UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	FORT-055460	4455

182115 7590 03/04/2025

Fortinet, Inc. (Lacework, Inc.)/JWHD
c/o Jaffery Watson Hamilton & DeSanctis LLP
7501 Village Square Drive, Suite 206
Castle Pines, CO 80108

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
03/04/2025	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

april.piepenburg@jwhdlaw.com
eofficeaction@appcoll.com
mike.desanctis@jwhdlaw.com

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00001

APPLICATION NO.	ISSUE DATE	PATENT NO.
17/858,866	04-Mar-2025	12244621

Fortinet, Inc. (Lacework, Inc.)/JWHD
c/o Jaffery Watson Hamilton & DeSanctis LLP
7501 Village Square Drive, Suite 206
Castle Pines, CO 80108

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00002

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	03/04/2025	12244621	FORT-055460	4455

182115 7590 02/12/2025

Fortinet, Inc. (Lacework, Inc.)/JWHD
c/o Jaffery Watson Hamilton & DeSanctis LLP
7501 Village Square Drive, Suite 206
Castle Pines, CO 80108

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 148 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (https://patentcenter.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional inventors):

VIKRAM KAPOOR, CUPERTINO, CA;
HARISH KUMAR BHARAT SINGH, PLEASANTON, CA;
WEIFEI ZENG, SUNNYVALE, CA;
VIMALKUMAR JEYAKUMAR, LOS ALTOS, CA;
THERON TOCK, MOUNTAIN VIEW, CA;

APPLICANT(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional applicants):

LACEWORK, INC., SAN JOSE, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

Change(s) applied to document, /J.G./ 10/30/2024	89	20220374800	A1	11-2022 ~~2023-09-26~~	Adinarayan et al.	
	90	20220376970	A1	2022-11-24	Chawathe et al.	
	91	20220382611	A1	12-2022 ~~2023-01-03~~	Kapish et al.	
	92	20220394082	A1	2022-12-08	Keren et al.	
	93	20220414072	A1	2022-12-29	Tandon et al.	
	94	20220414105	A1	2022-12-29	Umay et al.	
	95	20230025252	A1	2023-01-26	Erickson et al.	
	96	20230039566	A1	2023-02-09	Ghag et al.	
	97	20230052827	A1	2023-02-16	Araujo et al.	
	98	20230088960	A1	2023-03-23	Popelka et al.	
	99	20230096930	A1	2023-03-30	Dasdan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	78	20220050840	A1	2022-02-17	Parravicini et al.	
	79	20220058193	A1	02-2022 ~~2023-09-12~~	Smith Shawn et al.	
	80	20220067186	A1	2022-03-03	Thakur et al.	
	81	20220086179	A1	03-2022 ~~2023-05-09~~	Levin et al.	
	82	20220092481	A1	2022-03-24	Neithalath et al.	
	83	20220121741	A1	04-2022 ~~2023-09-05~~	Araujo et al.	
	84	20220124108	A1	2022-04-21	Gamble et al.	
	85	20220129803	A1	2022-04-28	Bikumala et al.	
	86	20220191226	A1	2022-06-16	Chan et al.	
	87	20220327119	A1	2022-10-13	Gasper et al.	
	88	20220350789	A1	11-2022 ~~2023-05-02~~	Yang et al.	

Change(s) applied to document, /J.G./ 10/30/2024

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00006

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	67	20200287923	A1	2020-09-10	Raghavendra et al.	
Change(s) applied to document. /J.G./ 10/30/2024	68	20200320106	A1	10-2020 ~~2022-04-28~~	Goldfarb	
	69	20200334293	A1	2020-10-22	Piechowicz et al.	
	70	20200351151	A1	2020-11-05	Dang et al.	
	71	20200412752	A1	2020-12-31	Shapoury	
	72	20210019209	A1	2021-01-21	Krishnaswamy et al.	
	73	20210232420	A1	2021-07-29	Dhruvakumar et al.	
	74	20210286798	A1	2021-09-16	Li et al.	
	75	20210294798	A1	2021-09-23	Binkley et al.	
	76	20210406917	A1	2021-12-30	Erickson et al.	
	77	20220004718	A1	2022-01-06	Quamar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	56	20190101622	A1	2019-04-04	Wilson	
	57	20190163555	A1	2019-05-30	Zheng et al.	
	58	20190227860	A1	2019-12-03	Gefen et al.	
	59	20190312898	A1	2019-10-10	Verma et al.	
	60	20190327251	A1	2019-10-24	Muddu et al.	
	61	20190342307	A1	2019-11-07	Gamble et al.	
	62	20190354554	A1	2019-11-21	Piechowicz et al.	
Change(s) applied to document. /J.G./ 10/30/2024	63	20190356555	A1	11-2019 ~~2020-08-25~~	Bai ~~Bai et al.~~	
	64	20200014718	A1	2020-01-09	DURAIRAJ et al.	
	65	20200021607	A1	2020-01-16	Muddu et al.	
	66	20200175361	A1	2020-06-04	Che et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	45	20180007145	A1	01-2018 ~~2019-10-29~~	Piechowicz et al.	
Change(s) applied to document. /J.G./ 10/30/2024	46	20180089132	A1	2018-03-29	Atta et al.	
	47	20180191781	A1	2018-07-05	Palani et al.	
	48	20180211425	A1	2018-07-26	Winternitz et al.	
	49	20180219888	A1	2018-08-02	Apostolopoulos	
	50	20180219897	A1	2018-08-02	Muddu et al.	
	51	20180359162	A1	2018-12-13	Savov et al.	
	52	20190042950	A1	2019-02-07	Lin et al.	
	53	20190050445	A1	02-2019 ~~2021-06-15~~	Griffith et al.	
	54	20190058626	A1	2019-02-21	Knowles et al.	
	55	20190075126	A1	2019-03-07	Muddu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	34	20170102961	A1	04-2017 ~~2020-01-14~~	Hilemon et al.	
Change(s) applied to ~~document~~, /J.G./ 10/30/2024	35	20170118099	A1	2017-04-27	HUANG	
	36	20170142140	A1	2017-05-18	Muddu et al.	
	37	20170148197	A1	2017-05-25	Winternitz et al.	
	38	20170155570	A1	2017-06-01	Maheshwari et al.	
	39	20170155672	A1	2017-06-01	Muthukrishnan et al.	
	40	20170223036	A1	2017-08-03	Muddu et al.	
	41	20170330096	A1	2017-11-16	Gupta et al.	
	42	20170346683	A1	11-2017 ~~2018-05-29~~	Li et al.	
	43	20180004835	A1	2018-01-04	Piechowicz et al.	
	44	20180004859	A1	01-2018 ~~2020-06-30~~	Piechowicz et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

Change(s) applied to document. /J.G./ 10/30/2024	23	20140125672	A1	05-2014 ~~2015-07-07~~	Winternitz et al.	
	24	20140279779	A1	09-2014 ~~2017-06-13~~	Zou et al.	
	25	20150310649	A1	10-2015 ~~2017-03-21~~	Winternitz et al.	
	26	20160120070	A1	2016-04-28	Myrah et al.	
	27	20160357521	A1	12-2016 ~~2019-07-02~~	Zhang et al.	
	28	20170063888	A1	2017-03-02	Muddu et al.	
	29	20170063903	A1	2017-03-02	Muddu et al.	
	30	20170063905	A1	2017-03-02	Muddu et al.	
	31	20170063909	A1	2017-03-02	Muddu et al.	
	32	20170063911	A1	2017-03-02	Muddu et al.	
	33	20170070594	A1	03-2017 ~~2019-11-26~~	Oetting et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	12	20090063857	A1	03-2009 ~~2010-04-27~~	Bade et al.	
Change(s) applied to document. /J.G./ 10/30/2024	13	20090307651	A1	2009-12-10	Senthil et al.	
	14	20090327328	A1	12-2009 ~~2015-08-18~~	Woodall et al.	
	15	20100042823	A1	02-2010 ~~2011-08-00~~	Arndt et al.	
	16	20110119100	A1	2011-05-19	Ruhl et al.	
	17	20110154287	A1	2011-06-23	Mukkamala et al.	
	18	20120143898	A1	2012-06-07	Bruno et al.	
	19	20120159333	A1	2012-06-21	Mital et al.	
	20	20130024412	A1	2013-01-24	Gong et al.	
	21	20130151453	A1	2013-06-13	Bhanot et al.	
	22	20140067750	A1	03-2014 ~~2015-05-26~~	Ranganathan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

Change(s) applied to document. /J.G./ 10/30/2024

	1	20040225929	A1	11-2004 ~~2007-01-23~~	Agha et al.	
	2	20050246521	A1	11-2005 ~~2009-01-27~~	Bade et al.	
	3	20060025987	A1	2006-02-02	Baisley et al.	
	4	20060026419	A1	02-2006 ~~2008-01-13~~	Arndt et al.	
	5	20060109271	A1	05-2006 ~~2007-06-10~~	Lomask	
	6	20070214111	A1	09-2007 ~~2017-08-08~~	Jin et al.	
	7	20070282916	A1	2007-12-06	Albahari et al.	
	8	20080109730	A1	2008-05-08	Coffman et al.	
	9	20080147707	A1	06-2008 ~~2012-04-17~~	Jin et al.	
	10	20090006843	A1	01-2009 ~~2011-12-27~~	Bade et al.	
	11	20090007010	A1	2009-01-01	Kriss et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**01/24/2025 02:47:59 PM Z ET**	**FORT-055460**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	April Piepenburg
PATENT CENTER #	68879289	AUTHORIZED BY	jeremy schweigert
CUSTOMER #	182115	FILING DATE	07/06/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	VIKRAM KAPOOR

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 9075	**E20251NE48485681**	**April Piepenburg**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1501	UTILITY ISSUE FEE	1200.00	1	1200.00
			TOTAL AMOUNT:	**$1,200.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**01/24/2025 02:47:59 PM Z ET**	**FORT-055460**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	April Piepenburg
PATENT CENTER #	68879289	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	jeremy schweigert

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
FORT-055460 ISSUE FEE.pdf	1	Issue Fee Payment (PTO-85B)	182 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
FORT-055460 ISSUE FEE.pdf	E1F9D26833673C62792CB373A5E5DA4F2030944A591EBA8DE148530585EFEC3A77FB0BE4704E4672CDC4403D203D652051D6737AB6FB05BAEB909FDF5726484D

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

182115 7590 10/29/2024
Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

April Piepenburg	(Typed or printed name)
/April Piepenburg/	(Signature)
1/23/25	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

TITLE OF INVENTION: Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	01/29/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
RAHMAN, MAHFUZUR	2498	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Jaffery Watson Hamilton & DeSanctis LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Fortinet, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Sunnyvale, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 60-6522

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Jeremy Schweigert/ Date 1/23/25

Typed or printed name Jeremy Schweigert Registration No. 56244

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

182115 7590 10/29/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
RAHMAN, MAHFUZUR	
ART UNIT	PAPER NUMBER
2498	

DATE MAILED: 10/29/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

TITLE OF INVENTION: Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	01/29/2025

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00019

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

182115 7590 10/29/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

TITLE OF INVENTION: Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	01/29/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
RAHMAN, MAHFUZUR	2498	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via the USPTO patent electronic filing system ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00020

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

182115 7590 10/29/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
RAHMAN, MAHFUZUR	
ART UNIT	**PAPER NUMBER**
2498	

DATE MAILED: 10/29/2024

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00021

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/ owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).
https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
2) a federal, state, local, or international agency, in response to its request;
3) a contractor of the USPTO having need for the information in order to perform a contract;
4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
9) the Office of Personnel Management (OPM) for personnel research purposes; and
10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 17/858,866	Applicant(s) KAPOOR et al.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2498	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 09/12/2024.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MAHFUZUR RAHMAN/
Primary Examiner, Art Unit 2498

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00023

DETAILED ACTION

This Office Action is in response to the request for continued examination (RCE) filed on 09/12/2024 in which Claims 1-20 are presented for examination on the merits.

Notice of Pre-AIA or AIA Status

The present application is being examined under the first inventor to file provisions of the AIA.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/12/2024 has been entered.

Response to Arguments

2. Applicant's arguments in pages 7-11 of the REMARKS filed on 09/12/2024 with respect to the rejection under 35 USC § 103(a) have been have been fully considered. Specially the following arguments in the remarks are persuasive: "..Thus, Giokas fails to disclose the limitations "identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information

and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses" of amended claim 1….Cudak has no disclosure of identifying one or more shadow systems as defined in amended claim 1 because in Cudak the shadow systems are intentionally deployed in a network to help determine if a security breach exists for active components of the network (Cudak, Abstract, [0008]-[0010], [0019]-[0020])."

In view of the aforesaid amendments and upon further search/consideration, the rejections to the respective claims under 35 U.S.C. 103(a) mailed on 06/12/2024 are hereby withdrawn.

Allowable Subject Matter

3. Claims 1-20 are allowed over prior art of record.

Reasons for Allowance

4. The following is an examiner's statement of reasons for allowance:

Independent claims 1, 9, and 17 are allowed and the corresponding dependent claims depend upon one of the above-mentioned allowed claims and are therefore allowed by virtue of their dependencies.

Giokas (US 20150033340 A1, prior art on the record) discloses a self-tuning network intrusion and detection system. In particular, systems and methods of the present disclosure provide a network security tool that protects a private network by monitoring the data packets flowing through the network. The data packets are compared against specific signatures of an intrusion detection and prevention system ("IDS/IPS") defense line of the private network and can thereby be identified as malicious. The tool can activate, deactivate, and generate signatures and alerts. The

signatures, which are relevant to the active network vulnerabilities, are activated within the tool, thereby improving the efficiency of the tool and the private network (Giokas, Paragraph 0004).

Further, Giokas discloses that an IDPS can be implemented via signature detection. In signature detection methodologies, the IDPS monitors data packets which are flowing through the network and compares this information with a pre-determined set of rules which identify known attack patterns. These attack patterns are known as signatures. As the IDPS monitors more signatures, the increased load upon the network and IDPS may increase the amount of time to analyze data packets due to the increase amount of patterns with which the IDPS compares packets. To reduce the load, the IDPS can be tuned to monitor for relevant attack patterns to protect the network are being monitored for by the IDPS. Since not all networks are the same, not all networks have the same vulnerabilities; e.g., a particular exploit for one network may not be viable on another network. Thus, it may be sufficient to maintain monitoring for attack patterns which can actually affect the network being protected (Giokas, Paragraph 0009).

Di Pietro et al. (US 20160028753 A1, prior art on the record) discloses that a computer network is a geographically distributed collection of nodes interconnected by communication links and segments for transporting data between end nodes, such as personal computers and workstations, or other devices, such as sensors, etc. Many types of networks are available, ranging from local area networks (LANs) to wide area networks (WANs). LANs typically connect the nodes over dedicated private communications links located in the same general physical location, such as a building

or campus. WANs, on the other hand, typically connect geographically dispersed nodes over long-distance communications links, such as common carrier telephone lines, optical lightpaths, synchronous optical networks (SONET), synchronous digital hierarchy (SDH) so links, or Powerline Communications (PLC) such as IEEE 61334, IEEE P1901.2, and others. In addition, a Mobile Ad-Hoc Network (MANET) is a kind of wireless ad-hoc network, which is generally considered a self-configuring network of mobile routers (and associated hosts) connected by wireless links, the union of which forms an arbitrary topology (Di Pietro, Paragraph 0021).

Furthermore, Di Pietro discloses that an approach to ensure the performance of an attack detection classifier remains above a threshold amount. For example, actual attacks may be launched against the network periodically, to assess the effectiveness and validity of a deployed attack detector. However, this may not be practical or feasible in a number of scenarios. Notably, initiating a realistic attack may require the non-trivial use of resources (e.g., attackers often leverage large botnets of compromised hosts spread across the globe). In addition, a realistic attack may seriously impair network and service availability within the up and running network (Di Pietro, Paragraph 0058).

Cudak et al. (US 20170310701 A1, prior art on the record) discloses a computer system to: deploy at least one shadow system in association with each of one or more components of a network environment; periodically record a state map of each active component of the network environment and a corresponding state map of the at least one shadow system associated therewith; periodically compare the recorded state map of each active component with the corresponding recorded state map of the at least one shadow system associated therewith; determine whether a deviation exists with respect

to the recorded state map of each active component and the corresponding recorded state map of the at least one shadow system associated therewith; in response to determining the deviation exists, determine whether the deviation is greater than a predetermined deviation threshold; and in response to determining the deviation is greater a the predetermined deviation threshold, declare a security breach regarding the active component(s) for which the deviation was determined to be greater than the predetermined deviation threshold.

Further, Cudak discloses a method includes: deploying at least one shadow system in association with each of one or more components of a network environment; periodically recording a state map of each active component of the network environment and a corresponding state map of the at least one shadow system associated therewith; periodically comparing the recorded state map of each active component with the corresponding recorded state map of the at least one shadow system associated therewith; determining whether a deviation exists with respect to the recorded state map of each active component and the corresponding recorded state map of the at least one shadow system associated therewith; in response to determining the deviation exists, determining whether the deviation is greater than a predetermined deviation threshold; and in response to determining the deviation is greater than the predetermined deviation threshold, declaring a security breach regarding the active component(s) for which the deviation was determined to be greater than the predetermined deviation threshold (Cudak, Para 0009).

Although, the cited references above are from same or similar fields of endeavor however, the Applicant's invention is directed towards data ingestion resources is

configured to ingest data from cloud environment into data platform wherein data ingestion resources is configured to receive the data from one or more agents deployed within cloud environment, utilize an event streaming platform (e.g., Kafika) to obtain the data, and/or pull data (e.g., configuration data) from cloud environment.

The subject matters of the independent claims 1, 9, and 17 are not taught or fairly suggested by the prior art of record, specifically the limitations in claim 1 that recite: ".. identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses..." in combination with the rest of the limitations recited in the independent claim 1.

Independent claims 9 and 17 recite similar subject matters as to those in claim 1.

The claimed subject matters are novel and non-obvious in scope over the prior art of record as the prior-art references fail to teach each and every features of the independent claim(s) including the limitations set forth above.

In view of the foregoing, the scope of claimed subject matters renders the invention patentably distinct as none of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Specifically, the substances of applicant's arguments in pages 7-11 of the REMARKS filed on 09/12/2024 as cited above (under "Response to Arguments" section) in view of the claim amendments has been fully considered and are persuasive. Therefore, all of the previous rejections have been removed and the current claims are in condition for allowance.

Furthermore, the Examiner performed updated search which does not yield other specific references that reasonably, either alone or in combination, would result a proper rejection of all the claimed features presented in each of the independent claims 1, 9, and 17 under 35 U.S.C 102 or 35 U.S.C.103 with proper motivation.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Yin-Chen Shaw can be reached on 571-272-8878. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MAHFUZUR RAHMAN/
Primary Examiner, Art Unit 2498

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2498

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/27/2024	06/07/2024	10/19/2024						
	1	✓	✓	=						
	2	✓	✓	=						
	3	✓	✓	=						
	4	✓	✓	=						
	5	✓	✓	=						
	6	✓	✓	=						
	7	✓	✓	=						
	8	✓	✓	=						
	9	✓	✓	=						
	10	✓	✓	=						
	11	✓	✓	=						
	12	✓	✓	=						
	13	✓	✓	=						
	14	✓	✓	=						
	15	✓	✓	=						
	16	✓	✓	=						
	17	✓	✓	=						
	18	✓	✓	=						
	19	✓	✓	=						
	20	✓	✓	=						

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00032

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2498

CPC - Searched*		
Symbol	**Date**	**Examiner**
(H04L63/1425 OR G06F9/455 OR G06F9/545 OR G06F16/9024 OR G06F16/9038 OR G06F16/9535 OR G06F16/9537 OR G06F21/57 OR H04L43/045 OR H04L43/06 OR H04L63/10 OR H04L67/306 OR H04L67/535 OR G06F16/2456).cpc.	10/19/2024	MR

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Search History Including CPC/Inventor/Assignee/NPL/Keywords Search Attached	10/19/2024	MR
Inventor/Assignee Search	10/19/2024	MR

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00033

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2498

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
(H04L63/1425	(H04L63	10/19/2024	MR
	((detect$3 identifying tdetermin$5) shadow WITH (class$5 subset group type) near10 (device system) with (discrepancy difference) same resource with access$3).clm.	10/19/2024	MR

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00034

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2498

CPC							
Symbol						**Type**	**Version**
H04L	/	63	/	1425		F	2013-01-01
G06F	/	16	/	9024		I	2019-01-01
G06F	/	9	/	545		I	2013-01-01
H04L	/	63	/	10		I	2013-01-01
H04L	/	43	/	06		I	2013-01-01
H04L	/	43	/	045		I	2013-01-01
G06F	/	16	/	9535		I	2019-01-01
G06F	/	21	/	57		I	2013-01-01
H04L	/	67	/	306		I	2013-01-01
H04L	/	67	/	535		I	2022-05-01
G06F	/	9	/	455		I	2013-01-01
G06F	/	16	/	9038		I	2019-01-01
G06F	/	16	/	9537		I	2019-01-01
G06F	/	16	/	2456		A	2019-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

Use images from artifact folder? ○ Yes ◉ No

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498 (Primary Examiner)	19 October 2024 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00035

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2498

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L	/	29	/	06

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

Use images from artifact folder? ○ Yes ◉ No

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498 (Primary Examiner)	19 October 2024 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00036

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2498

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19										
	2		11		20										
	3		12												
	4		13												
	5		14												
	6		15												
	7		16												
	8		17												
	9		18												

Use images from artifact folder? ○ Yes ◉ No

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498 (Primary Examiner)	19 October 2024 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00037

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1131	16	"20160163205"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/09/30 03:30 PM
L1133	16	"20160163205"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/09/30 03:30 PM
L1134	16	"20160163205"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1135	16	"20160163205"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1136	16	"20160163205"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1137	39	1110 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1138	79	(location geographic$2 OR gps shop place) WITH (anomalous behavior$2 detect$3 abnormal normal unauthorized activ$4) near7 (detect$3 determin$5 profile Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviat$3 alert$3 alarm$3 tolerance warning failure) AND device WITH user AND known near6 location AND activity AND device AND (polygraph polygraph OR (health	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM

		detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph)))					
L1139	75	((("Chen") near3 ("Yijou"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/10/05 03:31 PM
L1140	151	graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND software near4 service	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1141	2	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1142	208	device WITH location near8 (characterization character context usage utiliz$5) near10 (known unknown unauthorized) WITH (anomal$5 unauthor$5 flag$4)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1143	23	((Original OR initial OR first) WITH (session instance communication profile OR log$4 OR credential) WITH (monitor$3 OR track$3 audit$3 OR inspect$3) WITH (generat$3 OR creat$3 OR produc$3) WITH (graph OR pattern OR map$4) WITH (anomal$3 OR behavior OR intrusion OR threat OR attack$3 anomalous OR risk) AND (multiple OR plurality) WITH (machine OR device OR node) WITH model$4) AND edge WITH (connect$3 OR link$3 OR communicat$3) AND (alert$3 OR alarm$3).clm.	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1144	0	1040 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1145	1	"2004025026"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:31 PM

L1146	2	1046 AND user WITH model	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1147	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1148	1	(polygraph OR (health detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph))) WITH (destination OR target OR end OR recipient OR receiv$3 OR remot$2 server) WITH (brow$4 website program application remote) near10 (normal abnormal activit$3 risk malicious$4 OR anomal$3 OR threat OR risk intrusion OR threat vulnerabilities OR vulnerab$5 OR exploit unauthoriz$5 deviat$3) AND SaaS AND scor$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1149	2	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1150	2	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1151	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1152	68	((US-20080120721-A1 OR US-20170019487-A1 OR US-20190222597-A1 OR US-20090031423-A1 OR US-20160143570-A1 OR US-20150033340-A1 OR US-20100094767-A1 OR US-20130073387-A1 OR US-	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00040

		20140020102-A1 OR US-20160103883-A1 OR US-20130227691-A1 OR US-20160359872-A1 OR US-20180288063-A1 OR US-20160028753-A1 OR US-20080022405-A1 OR US-20170310701-A1 OR US-20150106140-A1 OR US-20130238555-A1 OR US-20120166393-A1 OR US-20120166493-A1 OR US-20120041933-A1 OR US-20100138440-A1 OR US-20030130985-A1 OR US-20180095743-A1 OR US-20130167207-A1 OR US-20120062389-A1 OR US-20120062390-A1 OR US-20160353245-A1 OR US-20140359558-A1 OR US-20160034305-A1 OR US-20140282586-A1 OR US-20180084012-A1 OR US-20190207955-A1 OR US-20190012457-A1 OR US-20180375882-A1 OR US-20140330960-A1 OR US-20160241705-A1 OR US-20200358804-A1 OR US-20180103052-A1 OR US-20100088281-A1 OR US-20160163205-A1 OR US-20100076952-A1 OR US-20160135751-A1 OR US-20140280952-A1 OR US-20150101050-A1 OR US-20150309813-A1 OR US-20220400130-A1 OR US-20230328086-A1).did. AND PGPB.dbnm.) OR ((US-10115111-B2 OR US-8880588-B2 OR US-9210183-B2 OR US-9519782-B2 OR					

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00041

		US-10142353-B2 OR US-9825989-B1 OR US-8443442-B2 OR US-9916763-B2 OR US-10419469-B1 OR US-9021583-B2 OR US-9378044-B1 OR US-9407754-B1 OR US-9071638-B1 OR US-4744029-A OR US-11044533-B1 OR US-9552354-B1 OR US-10986114-B1 OR US-11689553-B1 OR US-5371878-A).did. AND USPT.dbnm.) OR ((US-20110119085-A1).did. AND DWPI.dbnm.)					
L1153	68	((US-20080120721-A1 OR US-20170019487-A1 OR US-20190222597-A1 OR US-20090031423-A1 OR US-20160143570-A1 OR US-20150033340-A1 OR US-20100094767-A1 OR US-20130073387-A1 OR US-20140020102-A1 OR US-20160103883-A1 OR US-20130227691-A1 OR US-20160359872-A1 OR US-20180288063-A1 OR US-20160028753-A1 OR US-20080022405-A1 OR US-20170310701-A1 OR US-20150106140-A1 OR US-20130238555-A1 OR US-20120166393-A1 OR US-20120166493-A1 OR US-20120041933-A1 OR US-20100138440-A1 OR US-20030130985-A1 OR US-20180095743-A1 OR US-20130167207-A1 OR US-20120062389-A1 OR US-20120062390-A1 OR US-20160353245-A1 OR US-20140359558-A1 OR US-	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM

		20160034305-A1 OR US-20140282586-A1 OR US-20180084012-A1 OR US-20190207955-A1 OR US-20190012457-A1 OR US-20180375882-A1 OR US-20140330960-A1 OR US-20160241705-A1 OR US-20200358804-A1 OR US-20180103052-A1 OR US-20100088281-A1 OR US-20160163205-A1 OR US-20100076952-A1 OR US-20160135751-A1 OR US-20140280952-A1 OR US-20150101050-A1 OR US-20150309813-A1 OR US-20220400130-A1 OR US-20230328086-A1).did. AND PGPB.dbnm.) OR ((US-10115111-B2 OR US-8880588-B2 OR US-9210183-B2 OR US-9519782-B2 OR US-10142353-B2 OR US-9825989-B1 OR US-8443442-B2 OR US-9916763-B2 OR US-10419469-B1 OR US-9021583-B2 OR US-9378044-B1 OR US-9407754-B1 OR US-9071638-B1 OR US-4744029-A OR US-11044533-B1 OR US-9552354-B1 OR US-10986114-B1 OR US-11689553-B1 OR US-5371878-A).did. AND USPT.dbnm.) OR ((US-20110119085-A1).did. AND DWPI.dbnm.)					
L1154	32	874 AND shadow WITH access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1155	32	874 AND shadow WITH access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/10/05 03:31 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00043

			IBM_TDB)				
L1156	5	752 AND (compar$3 detect$3 match$3) WITH (Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviation alert$3 alarm$3 tolerance warning failure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1157	0	931 AND match$3 WITH (location region)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1158	0	931 AND match$3 WITH (location region)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1159	0	925 AND anomal$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1160	0	925 AND anomal$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1161	61	((US-20160103883-A1 OR US-20140020102-A1 OR US-20130073387-A1 OR US-20100094767-A1 OR US-20150033340-A1 OR US-20080120721-A1 OR US-20160143570-A1 OR US-20090031423-A1 OR US-20190222597-A1 OR US-20170019487-A1 OR US-20130227691-A1 OR US-20160359872-A1 OR US-20180288063-A1 OR US-20160028753-A1 OR US-20080022405-A1 OR US-20170310701-A1 OR US-20150106140-A1 OR US-20130238555-A1 OR	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00044

		US-20120166393-A1 OR US-20120166493-A1 OR US-20120041933-A1 OR US-20100138440-A1 OR US-20030130985-A1 OR US-20180095743-A1 OR US-20140359558-A1 OR US-20160034305-A1 OR US-20140282586-A1 OR US-20180084012-A1 OR US-20190207955-A1 OR US-20190012457-A1 OR US-20180375882-A1 OR US-20140330960-A1 OR US-20160241705-A1 OR US-20200358804-A1 OR US-20180103052-A1 OR US-20100088281-A1 OR US-20100076952-A1 OR US-20160135751-A1 OR US-20140280952-A1 OR US-20150101050-A1 OR US-20150309813-A1 OR US-20220400130-A1).did. AND PGPB.dbnm.) OR ((US-9210183-B2 OR US-8880588-B2 OR US-10115111-B2 OR US-9519782-B2 OR US-10142353-B2 OR US-9825989-B1 OR US-8443442-B2 OR US-10419469-B1 OR US-9021583-B2 OR US-9378044-B1 OR US-9407754-B1 OR US-9071638-B1 OR US-4744029-A OR US-11044533-B1 OR US-9552354-B1 OR US-10986114-B1 OR US-11689553-B1 OR US-5371878-A).did. AND USPT.dbnm.) OR ((US-20110119085-A1).did. AND DWPI.dbnm.)					
L1162	0	853 AND shadow ADJ system WITH (device hardware resource	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO;	OR	ON	ON	2024/10/05 03:31 PM

		system) near4 access$3	JPO; DERWENT; IBM_TDB)				
L1163	6	872 AND monitor$3 SAME shadow ADJ system WITH (device hardware resource system) WITH (activit$3 access$3)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1164	49	871 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1165	74	L274 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1166	74	L274 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1167	14	750 AND polygraph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1168	5	751 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:31 PM
L1169	75	((("Chen") near3 ("Yijou"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/10/05 03:32 PM
L1170	75	((("Chen") near3 ("Yijou"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/10/05 03:32 PM
L1171	0	L238 and ((@ad or @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1172	2	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1173	2	L191 and (valid or original or authorized) with session	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1174	4	"17810978"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1175	3	((US-20180288063-A1 OR US-20100094767-A1 OR US-	(US-PGPUB)	OR	ON	ON	2024/10/05 03:32 PM

		20130073387-A1).did. AND PGPB.dbnm.)					
L1176	139092069	369AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1177	13	443 AND polygraph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1178	7846	(polygraph OR (health detect$3 pulse) near4 network nea4 graph) WITH (destination OR target OR end OR recipient OR receiv$3 OR remot$2 server) WITH (brow$4 website program application remote) near10 (normail abnormal activit$3 risk malicious$4 OR anomal$3 OR threat OR risk intrusion OR threat vulnerabilities OR vulnerab$5 OR exploit unauthoriz$5)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1179	79	L229 and (Anomal$3 or behavior or intrusion or threat or attack$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1180	90	L169 and ((@ad or @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1181	17	"16459207"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1182	194	logical adj graph and log adj5 data	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1183	50	(US-20100076952-$ or US-20170019487-$ or US-20160103883-$ or US-20180288063-$ or US-20180084012-$ or US-20160028753-$ or US-20140020102-$ or US-20130073387-$ or US-20140282586-$ or US-20160034305-$ or	(US-PGPUB; USPAT; DERWENT)	OR	ON	ON	2024/10/05 03:32 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00047

		US-20150309813-$ or US-20150101050-$ or US-20140359558-$ or US-20140280952-$ or US-20100094767-$ or US-20150033340-$ or US-20080120721-$ or US-20160143570-$ or US-20160135751-$ or US-20090031423-$).did. or (US-9378044-$ or US-9210183-$ or US-8880588-$ or US-10115111-$ or US-8443442-$).did. or (US-20110119085-$).did.					
L1184	2	L181 and (detect$3 or indetif$4 or determin$5) with (Anomal$3 or behavior or intrusion or threat or attack$3 anomalous) with (stor$3 or database or table to record43 or log$4)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:32 PM
L1185	4	"17810978"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:41 PM
L1186	0	18/438,857	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 03:43 PM
L1187	208	(visual visualization) WITH graph$4 AND polygraph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:04 PM
L1188	75	1187 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:05 PM
L1189	11	1188 AND detect$3 WITH (unauthorized anomal$3 behavior$2)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:10 PM
L1190	4	((US-20180288063-A1 OR US-20180103052-A1 OR US-20130227691-A1 OR US-20160359872-A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:16 PM
L1191	2	1190 AND saas	(US-PGPUB; USPAT;	OR	ON	ON	2024/10/05

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00048

			USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				04:30 PM
L1192	2	1189 AND saas	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:31 PM
L1193	0	1188 AND detect$3 WITH (unauthorized anomal$3 behavior$2) WITH (target destination)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:32 PM
L1194	1	1191 AND detect$3 WITH (unauthorized anomal$3 behavior$2) WITH (target destination)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:32 PM
L1195	38	"20150033340"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 04:43 PM
L1196	0	1040 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 09:40 PM
L1197	6	1108 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 09:40 PM
L1198	31	(location geographic$2 OR gps shop place) WITH (anomalous behavior$2 detect$3 abnormal normal unauthorized activ$4) near7 (detect$3 determin$5 profile Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviat$3 alert$3 alarm$3 tolerance warning failure) AND device WITH user AND known near6 location AND activity AND device WITH (polygraph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 09:40 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00049

		polygraph OR (health detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph)))					
L1199	82	918 AND (location region area) WITH (profile account)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 09:40 PM
L1200	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/05 09:40 PM
L1201	82	918 AND (location region area) WITH (profile account)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:37 PM
L1202	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:37 PM
L1203	31	(location geographic$2 OR gps shop place) WITH (anomalous behavior$2 detect$3 abnormal normal unauthorized activ$4) near7 (detect$3 determin$5 profile Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviat$3 alert$3 alarm$3 tolerance warning failure) AND device WITH user AND known near6 location AND activity AND device WITH (polygraph polygraph OR (health detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph)))	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:37 PM
L1204	0	1040 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/10/19 08:37 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00050

			IBM_TDB)				
L1205	1	1191 AND detect$3 WITH (unauthorized anomal$3 behavior$2) WITH (target destination)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:37 PM
L1206	1	1191 AND detect$3 WITH (unauthorized anomal$3 behavior$2) WITH (target destination)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:37 PM
L1207	2	L191 and (valid or original or authorized) with session	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1208	0	853 AND shadow ADJ system WITH (device hardware resource system) near4 access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1209	49	871 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1210	209	device WITH location near8 (characterization character context usage utiliz$5) near10 (known unknown unauthorized) WITH (anomal$5 unauthor$5 flag$4)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1211	79	(location geographic$2 OR gps shop place) WITH (anomalous behavior$2 detect$3 abnormal normal unauthorized activ$4) near7 (detect$3 determin$5 profile Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviat$3 alert$3 alarm$3 tolerance warning failure) AND device WITH user AND known near6 location AND activity AND device	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00051

		AND (polygraph polygraph OR (health detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph)))					
L1212	209	device WITH location near8 (characterization character context usage utiliz$5) near10 (known unknown unauthorized) WITH (anomal$5 unauthor$5 flag$4)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1213	2	L191 and (valid or original or authorized) with session	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1214	155	graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND software near4 service	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1215	5	752 AND (compar$3 detect$3 match$3) WITH (Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviation alert$3 alarm$3 tolerance warning failure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1216	0	931 AND match$3 WITH (location region)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1217	204022	"7" and ((anomal$3 or behavior or intrusion or threat or attack$3 anomalous potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2 fraudster or fraudulent) near8 (machine or device or node or client terminal) and (detect$3 or indetif$4 or determin$5)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM

		with(Anomal$3 or behavior or intrusion or threat or attack$3))					
L1218	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1219	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1220	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1221	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1222	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:38 PM
L1223	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1224	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1225	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1226	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1227	2	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1228	76	L187 and (generat$3 or	(US-PGPUB; USPAT;	OR	ON	ON	2024/10/19

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00053

		creat$3) with (graph or model)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)				08:39 PM
L1229	2848	1053 AND context$2 WITH (parameter attribute propert$3 value) SAME user WITH model	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1230	36	1044 AND model AND context$4	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1232	56	1042 AND (approv$3 consent) WITH (workflow model polic$3) AND graph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1233	0	1042 AND (approv$3 consent) WITH (workflow model polic$3) AND log$4 WITH graph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1234	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1235	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1236	58	L205 and (previlege or permission or permit$4 or authoriz$5) same (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1237	2	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1238	17	937 AND device WITH location near8 (characterization character context usage utiliz$5) near10 (known unknown unauthorized) WITH (anomal$5 unauthor$5 flag$4)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:39 PM
L1239	1	L103 and (cluster or group$3 or class or classifying or classified)	(US-PGPUB)	OR	ON	ON	2024/10/19 08:39 PM

		with (machine or server or device or terminal) with resource$3					
L1240	0	L238 and ((@ad or @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 08:40 PM
L1241	38	"20150033340"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:12 PM
L1242	23	"20160028753"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:15 PM
L1243	0	"20170310701"1	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:19 PM
L1244	5	"20170310701"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:20 PM
L1245	0	"17858866"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:22 PM
L1246	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:45 PM
L1247	0	853 AND shadow ADJ system WITH (device hardware resource system) near4 access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:45 PM
L1248	0	1188 AND detect$3 WITH (unauthorized anomal$3 behavior$2) WITH (target destination)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:45 PM
L1249	0	1188 AND detect$3 WITH (unauthorized anomal$3 behavior$2) WITH (target destination)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/10/19 09:45 PM

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N542	4	N122 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with model$4).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N543	0	N85 and ((Original or initial or first) with (session) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4 or model) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2) and (hash or checksum) with (password or pin)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N544	20	((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4) and edge with	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00056

		(connect$3 or link$3 or communicat$3) and (alert$3 or alarm$3).clm.					
N545	16	N291 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N546	1	378 AND (graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND (software near4 service OR SaaS) AND access$3 WITH (target destination)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N547	0	(train$3 WITH model AND approv$3 NEAR5 workflow AND (HISTORY OR RECORD LOG) near8 (deviat$3 normal abnormal intrusion)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N548	2035	(polygraph OR (health detect$3 pulse) near4 network nea4 graph) WITH (destination OR target OR end OR recipient OR receiv$3 OR remot$2 server) WITH (brow$4 website program application remote) near10 (normail abnormal activit$3 risk malicious$4 OR anomal$3 OR threat OR risk intrusion OR threat vulnerabilities OR vulnerab$5 OR exploit unauthoriz$5)	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N549	2035	(polygraph OR (health	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00057

		detect$3 pulse) near4 network nea4 graph) WITH (destination OR target OR end OR recipient OR receiv$3 OR remot$2 server) WITH (brow$4 website program application remote) near10 (normail abnormal activit$3 risk malicious$4 OR anomal$3 OR threat OR risk intrusion OR threat vulnerabilities OR vulnerab$5 OR exploit unauthoriz$5)					03:32 PM
N550	64	("20060085437"|"20160080404"|"20180248901"|"9332020"|"9515999"|"9853968"|"20170118240"|"10033611"|"10142357"|"20030037136"|"20060259470"|"20110055138"|"20170279827"|"20180288063"|"20180367548"|"9021583"|"20070118909"|"20090271504"|"20120317151"|"20170163666"|"5806062"|"10389742"|"20180181750"|"20160149937"|"20050102284"|"20140359558"|"20170272344"|"20180020015"|"20180173789"|"8103906"|"9596253"|"20020184225"|"20090019160"|"20150135312"|"8122122"|"10115111"|"10127273"|"20040015470"|"20080148180"|"20100094767"|"20160078365"|"20160218911"|"20160359592"|"20180174062"|"20190132224"|"5584024"|"20100274785"|"20120005243"|"20180063178"|"20180115578"|"8443442"|"8862524"|"20140115001"|"20030179227"|"20100172261"|"20130304915"|"20150341379"|"20160205125"|"20180034840"|"9516053"|"9654503"|"20100114931"|"20190259033"|"20190222597").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM

N551	1	(US-9021583-$).did.	(USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N552	18	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N553	18	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N554	1	378 AND (graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND (software near4 service OR SaaS) AND access$3 WITH (target destination)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N555	1	378 AND (graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) near10 (personal individual$5 specific) AND (software near4 service OR SaaS) AND access$3 WITH (target destination)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N556	18208	(H04L63/1425 or G06F17/30958).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N557	18	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N558	1	378 AND graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) near10 (personal individual$5 specific) AND (alert$3 alarm$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N559	2	graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) near10 (personal individual$5 specific) AND (alert$3 alarm$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:32 PM
N560	0	18/438,857	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 03:43 PM
N561	4	((US-20180288063-A1 OR US-20180103052-A1 OR US-20130227691-A1 OR US-20160359872-	(US-PGPUB)	OR	ON	ON	2024/10/05 03:55 PM

		A1).did. AND PGPB.dbnm.)					
N562	49384	(visual visualization) WITH graph	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 04:02 PM
N563	251435	(visual visualization) WITH graph$4	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 04:04 PM
N564	157	(visual visualization) WITH graph$4 AND polygraph	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/05 04:04 PM
N565	0	"17858866"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:22 PM
N566	3283435	((detect$3 identifying tdetermin$5) shadow WITH (class$5 subset group type) near10 (device system) WITH (discrepancy difference) SAME resource WITH access$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:40 PM
N567	0	((detect$3 identifying tdetermin$5) WITH shadow WITH (class$5 subset group type) near10 (device system) WITH (discrepancy difference) SAME resource WITH access$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:41 PM
N568	0	(detect$3 identifying tdetermin$5) WITH shadow WITH (class$5 subset group type) near10 (device system) WITH (discrepancy difference) SAME (resource access$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:41 PM
N569	18303	(H04L63/1425 OR G06F17/30958).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM
N570	0	569 AND (detect$3 identifying tdetermin$5) WITH shadow WITH (class$5 subset group type) near10 (device system) WITH (discrepancy difference) SAME (resource access$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM
N571	0	566 AND (detect$3 identifying tdetermin$5) WITH shadow WITH (class$5 subset group type) near10 (device system) WITH	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM

		(discrepancy difference) SAME (resource access$3).clm.					
N572	1	378 AND graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) near10 (personal individual$5 specific) AND (alert$3 alarm$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM
N573	64	("20060085437"|"20160080404"|"20180248901"|"9332020"|"9515999"|"9853968"|"20170118240"|"10033611"|"10142357"|"20030037136"|"20060259470"|"20110055138"|"20170279827"|"20180288063"|"20180367548"|"9021583"|"20070118909"|"20090271504"|"20120317151"|"20170163666"|"5806062"|"10389742"|"20180181750"|"20160149937"|"20050102284"|"20140359558"|"20170272344"|"20180020015"|"20180173789"|"8103906"|"9596253"|"20020184225"|"20090019160"|"20150135312"|"8122122"|"10115111"|"10127273"|"20040015470"|"20080148180"|"20100094767"|"20160078365"|"20160218911"|"20160359592"|"20180174062"|"20190132224"|"5584024"|"20100274785"|"20120005243"|"20180063178"|"20180115578"|"8443442"|"8862524"|"20140115001"|"20030179227"|"20100172261"|"20130304915"|"20150341379"|"20160205125"|"20180034840"|"9516053"|"9654503"|"20100114931"|"20190259033"|"20190222597").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM
N574	0	N163 and ((Original or initial or first) with (session) with (generat$3 or creat$3	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM

		or produc$3) with (graph or pattern or map$4 or model) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2) and (hash or checksum) with (password or pin)).clm.					
N575	18303	(H04L63/1425 or G06F17/30958).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM
N576	19	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM
N577	111	("20030040942"|"20030135758"|"20040049698"|"20050044418"|"20050261943"|"20080167920"|"20090024663"|"20110313930"|"20140328179"|"20150088595"|"20160189301"|"20170085595"|"8973088"|"20030126049"|"20070294118"|"20100229187"|"20110161116"|"20120046989"|"20120215575"|"20120284158"|"20160205138"|"8448245"|"8744894"|"9521160"|"9699209"|"20060184473"|"20060265746"|"20120059779"|"20130239167"|"20130283336"|"20140067716"|"20140137257"|"20150188949"|"20150331932"|"20160234247"|"20170093904"|"20170116552"|"9253203"|"9373144"|"10230764"|"20090037323"|"20160099963"|"20030084349"|"20030154393"|"20040010709"|"20040024693"|"20050015624"|"20050278786"|"20130191829"|"20130346328"|"20150341389"|"20170093905"|"6374358"|"8468599"|"8494955"|"8577775"|"8699767"|"9031951"|"9292881"|"20020026335"|"20040064726"|"20080047016"|"20090319342"|	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/19 09:45 PM

		20100205014"|"201101 54497"|"20120041790"| "20120089617"|"20120 096558"|"20120239438 "|"20120300975"|"2013 0239177"|"2014001917 1"|"20140200930"|"201 70187745"|"7047419"|" 7324952"|"2002009155 1"|"20030014344"|"200 30236990"|"201100780 73"|"20140379708"|"20 160212169"|"6269349"| "7680659"|"7711646"|"2 0040260945"|"2008001 6563"|"20120011077"|" 20130055404"|"201303 47060"|"20140067713"| "20140142988"|"20150 373043"|"20160248799 "|"8484066"|"8601587"|" 20090063365"|"200300 28803"|"20040006532"| "20070192867"|"20080 250064"|"20100114634 "|"20130188475"|"2013 0239168"|"2014000719 0"|"20160248800"|"201 60294854"|"8332242"|" 9646428"|"2003001434 2"|"20080162377").PN.					

Google *" subset * shadow systems* discrepancy * resc

All Images Shopping News Videos Forums Web More Tools

No results found for *" subset * shadow systems* discrepancy * resource access*".

Results for * subset * shadow systems* discrepancy * resource access* (without quotes):

IData Insights
https://blog.idatainc.com › shadow-systems

Shadow Systems Explained

Feb 6, 2019 — In this post, when we say "shadow system" we mean a database or data set created and maintained outside of your systems of record.
Missing: discrepancy* | Show results with: discrepancy *

ResearchGate
https://www.researchgate.net › publication › 30368205...

(PDF) Why Do Shadow Systems Fail? An Expert Study on ...

May 31, 2016 — Our empirical data supports the argument that smaller shadow systems are more likely to disappear by exemplifying several small shadow systems ...
Missing: discrepancy* | Show results with: discrepancy *

People also ask

What is a shadow system?

What are data shadow systems also called?

What is a shadow spreadsheet?

How are shadow systems managed?

Feedback

ScienceDirect.com
https://www.sciencedirect.com › article › pii › pdf

Feral Information Systems, Shadow ...

by R Lund-Jensen · 2016 · Cited by 32 — The aim of this article is to explore and investigate the differences in the terms 'feral information systems' (FIS), 'shadow systems', and 'workarounds'.
8 pages

Elimity
https://elimity.com › blog › user-access-management-th...

User Access Management: The Fundamentals Explained

User access management (UAM) is the process of controlling who has access to an organization's resources, such as systems, data, and networks.
Missing: discrepancy* | Show results with: discrepancy *

ConductorOne
https://www.conductorone.com › guides › user-access-r...

User Access Reviews: Process & Best Practices Checklist

Mar 1, 2024 — A User Access Review (UAR) is a critical process that involves examining and validating user access rights within an organization's systems and applications.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00064

ResearchGate
https://www.researchgate.net › publication › 220421111...

Shadow Systems: The Good, The Bad and The Ugly

The ethnographic investigation of a shadow system used in a higher educations institution, Central Queensland University (CQU) was reported in the article.
Missing: ~~discrepancy~~ * | Show results with: discrepancy *

Google Patents
https://patents.google.com › patent

Base station for implementing inter-cell interference coordination ...

US8989752B2 - Base station for implementing inter-cell interference coordination and method for inter-cell interference coordination - Google Patents

Salesforce
https://help.salesforce.com › articleView

Use Filters to Aggregate a Subset of Records

Use filters with record aggregation to aggregate only the records that matter to your users. Apply filters on the aggregate-from object, the aggregate to...

Secure Controls Framework
https://securecontrolsframework.com › sum › scf... PDF

SCF Set Theory Relationship Mapping

Shadow ... ◦ Non-console access to critical systems or systems that store, transmit and/or ... remove or quarantine a resource's access to other resources.
Missing: ~~discrepancy~~ * | Show results with: discrepancy *

Stanford University
https://fingate.stanford.edu › newsroom › cardinal-planni...

Cardinal Planning & Budgeting Project - Fingate

The initiative features the development of the new Cardinal Planning & Budgeting system (that replaced Tidemark Budgeting, which sunset Sept. 29, 2024)

People also search for

* Subset * shadow systems * discrepancy * resource access * qui	What is a Shadow system gun
what are shadow systems?	how does metadata differ for different types of information?

1 2 3 4 5 6 7 8 9 10 Next

20770, Greenbelt, MD - Based on your places (Home) · Update location

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00065

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**09/12/2024 01:30:15 PM Z ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	April Piepenburg
PATENT CENTER #	67149345	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	jeremy schweigert

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
FORT-055460 Response to Final OA v1.pdf	11	Amendment Submitted/Entered with Filing of Continued Prosecution Application (CPA)/Request for Continued Examination(RCE)	63 KB
FORT-055460 RCE.pdf	1	Request for Continued Examination (RCE)	345 KB

Warning: This is not a USPTO supplied RCE fillable form. Data in the form cannot be automatically loaded to other USPTO systems.

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

FORT-055460 Response to Final OA v1.pdf	3A4B0B2BECE108957B154A3E38BE08397B8902C2D1225A98D73763051803AC5653DE859B0BD60909D4B61E6CE18D5CFBDB880825DD0C3A0CD3062A2905C5FE9B
FORT-055460 RCE.pdf	529475DF4C073DE1E26206632C39A7002CFEAF4CEA88310AD4A754F767C5E8BCFEDBE5D735133D26984A92BCDE813576D96023456452F65FF0A56E45B303CA9C

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/30 (11-17)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	17/858,866
Filing Date	2022-07-06
First Named Inventor	Kapoor
Art Unit	2498
Examiner Name	Mahfuzur Rahman
Attorney Docket Number	FORT-055460

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      Ii. ☐ Other _____

   b. ☑ Enclosed

      I. ☑ Amendment/Reply

      iii. ☐ Information Disclosure Statement (IDS)

      ii. ☐ Affidavit(s)/ Declaration(s)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☑ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 60-6522.

      i. ☑ RCE fee required under 37 CFR 1.17(e)

      ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

   d. ■ Payment by EFS-Web

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Jeremy Schweigert/	Date	2024-09-12
Name (Print/Type)	Jeremy Schweigert	Registration No.	56244

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being EFS-Web transmitted to the United States Patent and Trademark Office (USPTO), deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the USPTO on the date shown below.

Signature	/April Piepenburg/		
Name (Print/Type)	April Piepenburg	Date	2024-09-12

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 12 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **If filing this completed form by mail, send to:**

Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**09/12/2024 01:30:15 PM Z ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	April Piepenburg
PATENT CENTER #	67149345	AUTHORIZED BY	jeremy schweigert
CUSTOMER #	182115	FILING DATE	07/06/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	VIKRAM KAPOOR

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 9075	**E20249BD30497648**	**April Piepenburg**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1801	REQUEST FOR CONTINUED EXAMINATION (RCE) - 1ST REQUEST (SEE 37 CFR 1.114)	1360.00	1	1360.00
			TOTAL AMOUNT:	**$1,360.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C.

371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Kapoor	Examiner: Mahfuzur Rahman
Serial No.:	17/858,866	Group Art Unit: 2498
Filed:	July 6, 2022	Docket No.: FORT-055460 (24219)
		Confirmation No.: 4455

Title: Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

---

AMENDMENT AND RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

In response to the Final Office Action, mailed on June 12, 2024, please amend the above-identified patent application as follows. A request for continued examination (RCE) is being filed with this Amendment.

IN THE CLAIMS

Amendments to the Claims:

Amendments to the claims are listed herein. This Listing of Claims will replace all prior versions, and listings, of claims in the subject application. Any amendments or cancelations of claims made herein is done without prejudice, waiver, or disclaimer of or to the claimed or disclosed subject matter. Furthermore, the right to claim any of the amended or disclosed subject matter in a continuing or divisional application is hereby reserved.

Listing of Claims:

1. (Currently amended) A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising:

gathering, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;

gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

2. (Original) The method of claim 1 wherein the first information is gathered from one or more identity providers.

3. (Currently amended) The method of claim 1 wherein the first information is gathered from [[the]] one or more applications of the one or more resources or of the providers.

4. (Original) The method of claim 1 further comprising generating a polygraph indicating the one or more shadow systems.

5. (Original) The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.

6. (Original) The method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems.

7. (Currently amended) The method of claim 1 wherein the first information is not gathered from the one or more user devices ~~identifying the one or more shadow systems comprises:~~

~~identifying one or more accesses described in the first information but not described in the second information; and~~

~~identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses~~.

8. (Currently amended) The method of claim 1 wherein the second information is gathered via the one or more client applications including one or more proxy applications executed on the at least a subset of the one or more user devices.

9. (Currently amended) A non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to:

gather, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;

gather, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identify one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

10. (Previously Presented) The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from one or more identity providers.

11. (Currently amended) The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from [[the]] one or more applications of the one or more resources or providers.

12. (Previously Presented) The non-transitory computer readable storage medium of claim 9 further comprising generating a polygraph indicating the one or more shadow systems.

13. (Previously Presented) The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to generate an alert in response to identifying the one or more shadow systems.

14. (Previously Presented) The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to direct the user to a remediation workflow in response to identifying the one or more shadow systems.

15. (Currently amended) The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more resources or the providers of the one or more resources other than the one or more user devices~~, to identify the one or more shadow systems, the instructions, when executed, further cause the processing device to:~~

~~identify one or more accesses described in the first information but not described in the second information; and~~

~~identify, as one or more shadow systems, one or more user devices corresponding to the one or more accesses~~.

16. (Currently amended) The non-transitory computer readable storage medium of claim 9 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices.

17. (Currently amended) A system comprising:

a memory; and
a processing device, operatively coupled to the memory, the processing device configured to:

gather, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;

gather, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identify one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

18. (Original) The system of claim 17 wherein the first information is gathered from one or more identity providers.

19. (Currently amended) The system of claim 17 wherein the first information is gathered from [[the]] one or more applications of the one or more resources or the providers of the one or more resources.

20. (Previously Presented) The system of claim 17 wherein the processing device is further configured to generate a polygraph indicating the one or more shadow systems.

REMARKS

Applicant respectfully requests reconsideration of this application in view of the following remarks and the above amendments. Various claims are amended. The amendments are made without prejudice or disclaimer. Accordingly, the amendments are not intended and do not surrender claimed subject matter. No new matter is added. It is respectfully requested that the above referenced patent application be reconsidered in view of the following remarks.

35 USC §103 Rejection of the Claims

Claims 1-20 are rejected under 35 USC 103 as being unpatentable over Giokas (US2015/0033340) "Giokas" in view of Di Pietro et al. (US 2016/0028753) "Di Pietro" and Cudak et al. (US 2017/0310701) "Cudak".

Claim 1, as amended, includes the limitations "gathering, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user; gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

Both the first information and the second information describe access to the one or more resources from different perspectives. The first information is generated from the perspective of an identity provider or SaaS accessed via a user device, and the second information is generated from the perspective of a user device via a client application executed on the user device. Each access to a particular resource by a user device should be described in first information gathered from the identity provider, from the resource itself, or both. In contrast, access to a resource by a user device will only be described in second information from that user device if the access was performed via the client application (e.g., via a proxy application or by proxy functionality of that application). Thus, where a user device accesses a resource without using the client

application or otherwise circumventing the client application, that access will be described in the first information but not described in any second information from the user device. (Specification, [00792]).

The Office Action cites Giokas at [0069, 0071, 0074] as disclosing "gathering…second information describing access to the one or more resources." Applicant disagrees.

The cited portions of Giokas merely recite broad teachings describing the components of a "computing device," such as having "input and output" capabilities (Giokas at [0069]), "display devices" (Giokas at [0071]), and a "network interface" (Giokas at [0074]). These cited portions of Giokas only serve to describe the components and capabilities of a "computing device" at an extremely high level and do not recite nor relate in any way to the limitation "gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources." Therefore, Giokas fails to disclose this limitation.

Although Giokas does disclose that in signature detection methodologies, the IDPS monitors data packets which are flowing through the network and compares this information with a pre-determined set of rules which identify known attack patterns, Giokas fails to disclose identifying one or more shadow systems as defined in amended claim 1.

Thus, Giokas fails to disclose the limitations "identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses" of amended claim 1.

Di Pietro fails to cure the deficiencies of Giokas. The Office Action relies on Di Pietro at [0043] and [0070] as disclosing "at least a subset of the one or more user devices." Applicant

disagrees. The cited portions of Di Pietro merely describe the existence of Low-power and Lossy Networks (LLNs), a class of networks where the routers and interconnects of the network are constrained. Paragraph [0070] describes that previously collected traffic records may be mixed with currently monitored traffic, during a validation test. Such a mixing may be performed locally by the node hosting the attack detector.

Di Pietro fails to disclose the limitations "gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses."

Cudak has no disclosure of identifying one or more shadow systems as defined in amended claim 1 because in Cudak the shadow systems are intentionally deployed in a network to help determine if a security breach exists for active components of the network. (Cudak, Abstract, [0008]-[0010], [0019]-[0020]).

Thus, Cudak fails to disclose the limitations "gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses" of amended claim 1.

Furthermore, even if Giokas, Di Pietro, and Cudak were combined, such a combination would lack the limitations "gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses" of amended claim 1.

Therefore, in view of the above distinction, neither Giokas nor Di Pietro nor Cudak, individually or in combination, disclose each and every limitation of claim 1. As such, amended claim 1 and associated dependent claims 2-8 are patentable over Giokas, Di Pietro, and Cudak under 35 U.S.C. § 103.

Independent claims 9 and 17 have been amended in a similar manner in comparison to amended claim 1. Independent claims 9 and 17, as amended, contains similar limitations but not identical compared to the limitations of claim 1. For similar reasons, independent claims 9 and 17 and associated dependent claims 9-16 and 18-20 are patentable over Giokas, Di Pietro, and Cudak under 35 U.S.C. § 103.

Conclusion

For the foregoing reasons, reconsideration and allowance of the pending claims is requested. Amendments in this response are made without prejudice or disclaimer solely to expedite allowance. The right to pursue cancelled or amended subject matter in one or more continuation applications is explicitly reserved. It is respectfully submitted that the pending claims are patentable, and accordingly, the application is now in condition for allowance. Issuance of the Notice of Allowance is respectfully requested.

Any fees or extensions of time believed to be due in connection with this amendment are enclosed herein. However, please consider this a request for any extensions.

The undersigned representative authorizes the Commissioner to charge any additional fees that may be required, or credit any overpayment, to Deposit Account No.: **60-6522**, referencing Attorney Docket No.: **FORT-055460**.

The Examiner is invited to call the undersigned attorney at 833-596-4529 x708 if there remains any issue with allowance of this case.

Respectfully submitted,

Date 9/12/2024

By /Jeremy Schweigert/
Jeremy Schweigert, Reg. No. 56244
Telephone Number: 833-596-4529 x708

Jaffery Watson Hamilton & DeSanctis LLP
7501 Village Square, Suite 206
Castle Pines, CO 80108

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/858,866	Filing Date 07/06/2022	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $480 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	09/12/2024	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/DONNA D SMALLS LOGAN/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

182115 7590 06/12/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
06/12/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
kate@klspatents.com
office@klspatents.com

Office Action Summary	**Application No.** 17/858,866	**Applicant(s)** KAPOOR et al.	
	Examiner MAHFUZUR RAHMAN	**Art Unit** 2498	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 05/01/2024

.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 06 July 2022 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 05/01/2021.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the amendment filed on 05/01/2024 in which claims 1-20 are presented for examination on the merits.

Notice of Pre-AIA or AIA Status

The present application is being examined under the first inventor to file provisions of the AIA.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 05/01/2021 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Response to Arguments

1. Applicant's arguments in pages 7-12 of the REMARKS filed on 05/01/2024 with respect to the rejection under 35 USC § 103(a) have been considered but are moot in view of the new grounds of rejection. After careful review and in light of Applicant's amendments, remarks, and Examiner's newly performed search and consideration, claims 1-20 are now newly rejected under 35 U.S.C. 103(a) for the reasons specified below.

With regards to the rejection under 35 U.S.C. 35 U.S.C § 101, Applicants arguments in light of the claim amendments have been considered. As such, the Examiner hereby withdraws the rejections under 35 U.S.C. 35 U.S.C § 101.

With regards to the Claim Interpretation under 35 U.S.C. 112(f), Applicants arguments in light of the claim amendments have been considered. As such, the Examiner hereby withdraws Claim Interpretation under 35 U.S.C. 112(f).

Claim Rejections - 35 USC § 103

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

3. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in Graham **v.** John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1-20 are rejected under 35 U.S.C. 103 as being unpatentable over Giokas (US 20150033340 A1, hereinafter, Giokas) in view of Di Pietro et al. (US 20160028753 A1) and further in view of Cudak et al. (US 20170310701 A1, hereinafter, Cudak).

Regarding claim 1, Giokas discloses a method of using activity monitored by multiple data sources to identify shadow systems (Paragraph 0027: passive vulnerability assessor is further configured to receive a plurality of logs of network activity associated with computing devices of the protected network),

the method comprising: gathering first information describing access to one or more resources by one or more user devices of a user (Paragraphs 0029, 0093: clients 102a-n (e.g., end user devices, computing devices, administrator devices) or servers 106a-n that communicate via a private or protected network wherein system includes a plurality of modules to collect, analyze, store and process the vulnerability information);

gathering, [from at least a subset of the one or more user devices], second information describing access to the one or more resources (Paragraphs 0069, 0071. 0074: computing device includes any type and/or form of video adapter, video card, driver, and/or library to interface, communicate, connect or otherwise use the display devices 124a-124n to communicate with other computing devices via any type and/or form of gateway or tunneling protocol e.g. Secure Socket Layer (SSL) or Transport Layer Security (TLS), or the Citrix Gateway Protocol manufactured by Citrix Systems wherein group of devices are augment reality devices, for example); and

identifying one or more shadow systems based on a discrepancy between the first information and the second information (Paragraphs 0009, 0057: IDPS monitors data packets which are flowing through the network and compares this information with a pre-determined set of rules which identify known attack patterns. These attack patterns are known as signatures. As the IDPS monitors more signatures, the increased load upon the network and IDPS may increase the amount of time to analyze data packets due to the increase amount of patterns with which the IDPS compares packets) wherein [information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity]

Giokas does not explicitly states but Di Pietro from the same or similar fields of endeavor teaches a subset of the one or more user devices (Di Pietro, Paragraphs 0043, 0070: LLNs are comprised of anything from a few dozen and up to thousands or even millions of LLN routers, and support point-to-point traffic (between devices inside the LLN), point-to-multipoint traffic (from a central control point to a subset of devices inside the LLN)) wherein previously collected traffic records are mixed with currently monitored traffic, during a validation test. Such a mixing is performed locally by the node hosting the attack detector)

Therefore, it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to utilize user session associated with an original user as taught by Di Pietro in the teachings of Giokas for the advantage of detecting a potential network attack using clustering technique wherein clustering is

used in recommender systems (RS) for grouping objects that are similar in terms of user's selections (Di Pietro, Paragraph 0034).

The combination of Giokas and Di does not explicitly states but Cudak from the same or similar fields of endeavor teaches wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity (Cudak, Paragraphs 0072, 0052, 0054: a shadow system performing a corresponding, mirrored version of the workload(s) exhibit a deviation in execution time, memory usage, or network behavior wherein he period between recording state maps and/or comparing state maps of the active component(s) against the state maps of corresponding shadow system(s) may be determined based on the type of application(s) and/or workload(s) being handled by the network environment).

Therefore, it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity as taught by Cudak in the teachings of Giokas and Di for the advantage of determining whether the deviation is greater than a predetermined deviation threshold; and declaring a security breach regarding the active component(s) for which the deviation was determined (Cudak, Abstract).

Regarding claim 2, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 wherein the first information is gathered from one or more identity providers (Giokas, Paragraphs 0088, 0095: the network security tool of the present disclosure can automatically implement a plan of action to address findings of the VA

tool wherein the vulnerability assessor 210 can obtain data packets of a protected network, save the data packets to a data file or database, and analyze the data packets to identify stray IP addresses, spoofed packets, unnecessary packet drops, or suspicious packet generation from a single IP address).

Regarding claim 3, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 wherein the first information is gathered from the one or more applications (Giokas, Paragraph 0061: access SaaS resources through smartphone or tablet applications, including, e.g., Salesforce Sales Cloud, or Google Drive app. Clients 102 may also access SaaS resources through the client operating system, including, e.g., Windows file system for DROPBOX.).

Regarding claim 4, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 further comprising generating a polygraph indicating the one or more shadow systems (Giokas Paragraph 0114: signatures can be generated using various techniques including, e.g., statistical packet anomaly detection engine, Hamsa: fast signature generation for zero-day polymorphic worms with provable attack resilience, Polygraph).

Regarding claim 5, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems (Giokas Paragraphs 0008, 0019: an intrusion detection and prevention system (IDPS) combines these two functionalities, detecting potential attacks and both alerting system administrators and automatically moving to impede the attack.).

Regarding claim 6, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems (Giokas, Paragraphs 0083, 0010, 0032: a self-tuning network security tool that facilitates automatically identifying a current vulnerability of a computer system or network, and preventing an attack from exploiting the current vulnerability).

Regarding claim 7, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 wherein identifying the one or more shadow systems comprises: identifying one or more accesses described in the first information but not described in the second information (Giokas, Paragraph 0084: the tool can be configured to receive, access, look up, process, analyze or otherwise obtain and utilize information of one or more vulnerabilities lists or registries in one or more formats, standards, or schemes. The tool can be vulnerability scheme independent); and

identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses (Giokas Paragraphs 0011, 0049: network security tool may access or be otherwise communicate with a vulnerability assessment tool (e.g., via a network). The vulnerability assessment tool may detect vulnerabilities in the network, and feed them to the network security tool. The vulnerability assessment tool may feed the detected vulnerabilities in the form of a vulnerabilities list using a common scheme wherein network connection provide an access to Internet to allow the tool to get up to date with the latest exploits and signatures that are crowd-sourced).

Regarding claim 8, the combination of Giokas, Di Pietro, and Cudak discloses the method of claim 1 wherein the second information is gathered via one or more proxy

applications executed on the at least a subset of the one or more user devices (Giokas Paragraphs 0057, 0069: server 106 may be a file server, application server, web server, proxy server, appliance, network appliance, gateway, gateway server, virtualization server, deployment server, SSL VPN server, or firewall … interacting with group of electronic devices including augment reality devices).

Regarding claim 9; Claim 9 is similar in scope to claim 1, and is therefore rejected under similar rationale.

Regarding claim 10; Claim 10 is similar in scope to claim 2, and is therefore rejected under similar rationale.

Regarding claim 11; Claim 11 is similar in scope to claim 3, and is therefore rejected under similar rationale.

Regarding claim 12; Claim 12 is similar in scope to claim 4, and is therefore rejected under similar rationale.

Regarding claim 13; Claim 13 is similar in scope to claim 5, and is therefore rejected under similar rationale.

Regarding claim 14; Claim 14 is similar in scope to claim 6, and is therefore rejected under similar rationale.

Regarding claim 15; Claim 15 is similar in scope to claim 7, and is therefore rejected under similar rationale.

Regarding claim 16; Claim 16 is similar in scope to claim 8, and is therefore rejected under similar rationale.

Regarding claim 17; Claim 17 is similar in scope to claim 1, and is therefore rejected under similar rationale.

Regarding claim 18; Claim 18 is similar in scope to claim 2, and is therefore rejected under similar rationale.

Regarding claim 19; Claim 19 is similar in scope to claim 3, and is therefore rejected under similar rationale.

Regarding claim 20; Claim 20 is similar in scope to claim 4, and is therefore rejected under similar rationale.

Examiner Notes

7. The Examiner notes that incorporating the combined limitations of dependent claims 4, 6, and 7 **OR** dependent claims 6, 7, and 8 into independent claim 1 would better clarify the subject matter/embodiment of claimed invention. Similarly, amending independent claims 9 and 17 with aforesaid claim limitations would help advance the prosecution as it would clarify the claimed invention.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Seligman et al. (US 9552354 B1) discloses method for a highly interactive style of speech-to-speech translation is provided. The interactive procedures enable a user to recognize, and if necessary correct, errors in both speech recognition and translation, thus providing robust translation output than would otherwise be possible. The interactive techniques for monitoring and correcting word ambiguity errors during automatic translation, search, or other natural language processing tasks.

- Bentzien (US 20120166493 A1) discloses computer system that includes a program database module configured to define, at a shadow system, a shadow program database including data and a structure collectively defining an upgrade to an original program database on an original system. The computer system can include a basis module configured to define at the shadow system a shadow basis database related to start functionality of the shadow system.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- VEDANTHAM (US 20210049285 A1) discloses a manner of provide a time of life of data where a portion of the control parameters can be stored into a distributed ledger.

- Frei et al. (US 20190058996 A1) discloses methods for controlling access to and/or forwarding of communicated information, e.g. traffic, in a wireless communication system. The key, e.g., PSK, used to secure data that is transmitted to an access point for communication to a destination device is taken into consideration when deciding whether or not to provide the destination device access to the communicated content.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Yin-Chen Shaw can be reached on 571-272-8878. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MAHFUZUR RAHMAN/
Primary Examiner, Art Unit 2498

Notice of References Cited	Application/Control No. 17/858,866	Applicant(s)/Patent Under Reexamination KAPOOR et al.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20180095743-A1	2018-04-05	Specht; Juergen	G06F8/71	1/1
*	B	US-20170310701-A1	2017-10-26	Cudak; Gary David	H04L63/1441	1/1
*	C	US-9552354-B1	2017-01-24	Seligman; Mark	G06F40/51	1/1
*	D	US-20150106140-A1	2015-04-16	Biewald; Lars-Eric	G06Q10/06	705/7.12
*	E	US-20130238555-A1	2013-09-12	Driesen; Volker	G06F16/13	707/613
*	F	US-20120166393-A1	2012-06-28	Hoprich; Wieland	G06F16/21	707/634
*	G	US-20120166493-A1	2012-06-28	Bentzien; Levke	G06F16/27	707/E17.005
*	H	US-20120041933-A1	2012-02-16	Driesen; Volker	G06F16/214	707/E17.005
*	I	US-20100138440-A1	2010-06-03	Driesen; Volker	G06F16/2445	707/765
*	J	US-20100088281-A1	2010-04-08	Driesen; Volker	G06F11/1433	707/E17.007
*	K	US-20030130985-A1	2003-07-10	Driesen, Volker	G06F16/20	1/1
*	L	US-5371878-A	1994-12-06	Coker; Robert T.	G06F11/3664	714/E11.213
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00097

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2498

CPC - Searched*		
Symbol	**Date**	**Examiner**
(H04L63/1425 OR G06F9/455 OR G06F9/545 OR G06F16/9024 OR G06F16/9038 OR G06F16/9535 OR G06F16/9537 OR G06F21/57 OR H04L43/045 OR H04L43/06 OR H04L63/10 OR H04L67/306 OR H04L67/535 OR G06F16/2456).cpc.	06/07/2024	MR

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Search History Including CPC/Inventor/Assignee/NPL/Keywords Search Attached	06/07/2024	MR
Inventor/Assignee Search	06/07/2024	MR

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00098

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2498

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
(H04L63/1425	(H04L63	06/07/2024	MR
	((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4) and edge with (connect$3 or link$3 or communicat$3) and (alert$3 or alarm$3). clm.	06/07/2024	MR

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00099

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2498

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/27/2024	06/07/2024							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00100

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6347339	B1	2002-02-12	Morris et al.	
	2	6434663	B1	2002-08-13	Grimsrud et al.	
	3	6938084	B2	2005-08-30	Gamache et al.	
	4	7310733	B1	2007-12-18	Pearson et al.	
	5	7529801	B2	2009-05-05	Moore et al.	
	6	7562045	B2	2009-07-14	Beadle et al.	
	7	7743153	B2	2010-06-22	Hall et al.	
	8	7797548	B2	2010-09-14	Pearson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	9	7856544	B2	2010-12-21	Schenfeld et al.	
	10	7926026	B2	2011-04-12	Klein et al.	
	11	7962635	B2	2011-06-14	Naidu et al.	
	12	7996885	B2	2011-08-09	Jaiswal et al.	
	13	8032925	B2	2011-10-04	Cho	
	14	8037284	B2	2011-10-11	Schenfeld et al.	
	15	8037521	B2	2011-10-11	Minato	
	16	8151107	B2	2012-04-03	Song et al.	
	17	8276197	B1	2012-09-25	Mangal et al.	
	18	8291233	B2	2012-10-16	Pearson et al.	
	19	8341711	B1	2012-12-25	Pennington et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	20	8351456	B2	2013-01-08	Kadous et al.	
	21	8359584	B2	2013-01-22	Rao et al.	
	22	8497863	B2	2013-07-30	Xie et al.	
	23	8549002	B2	2013-10-01	Herter et al.	
	24	8561157	B2	2013-10-15	Ge	
	25	8595262	B1	2013-11-26	Hayden	
	26	8607306	B1	2013-12-10	Bridge et al.	
	27	8655989	B2	2014-02-18	Ritter et al.	
	28	8725587	B2	2014-05-13	Beadle et al.	
	29	8826403	B2	2014-09-02	Bhaskaran et al.	
	30	8843646	B2	2014-09-23	Kuzin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	31	8959608	B2	2015-02-17	Ahmed et al.	
	32	9053306	B2	2015-06-09	Yoshigaki et al.	
	33	9231935	B1	2016-01-05	Bridge et al.	
	34	9239873	B2	2016-01-19	Branch et al.	
	35	9246897	B2	2016-01-26	He	
	36	9323806	B2	2016-04-26	Sadikov et al.	
	37	9369450	B1	2016-06-14	Barak et al.	
	38	9391978	B2	2016-07-12	Burch et al.	
	39	9400882	B2	2016-07-26	Pearson et al.	
	40	9430830	B2	2016-08-30	Madabhushi et al.	
	41	9495522	B2	2016-11-15	Singh et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	42	9537851	B2	2017-01-03	Gordon et al.	
	43	9569869	B2	2017-02-14	Hesse et al.	
	44	9582766	B2	2017-02-28	Sadikov et al.	
	45	9596295	B2	2017-03-14	Banadaki et al.	
	46	9602506	B2	2017-03-21	Kang et al.	
	47	9602526	B2	2017-03-21	Liu et al.	
	48	9639676	B2	2017-05-02	Betz et al.	
	49	9652875	B2	2017-05-16	Vassilvitskii et al.	
	50	9659337	B2	2017-05-23	Lee et al.	
	51	9665660	B2	2017-05-30	Wensel	
	52	9740744	B2	2017-08-22	Stetson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	53	9741138	B2	2017-08-22	Friedlander et al.	
	54	9753960	B1	2017-09-05	Troyanovsky	
	55	9760619	B1	2017-09-12	Lattanzi et al.	
	56	9781115	B2	2017-10-03	Heise	
	57	9787705	B1	2017-10-10	Love et al.	
	58	9805080	B2	2017-10-31	Joshi et al.	
	59	9805140	B2	2017-10-31	Chakrabarti et al.	
	60	9819671	B2	2017-11-14	Ji	
	61	9830435	B2	2017-11-28	Haven	
	62	9836183	B1	2017-12-05	Love et al.	
	63	9852230	B2	2017-12-26	Fleury et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	64	9887999	B2	2018-02-06	Dong et al.	
	65	9942220	B2	2018-04-10	Bajenov et al.	
	66	9946800	B2	2018-04-17	Qian et al.	
	67	9954842	B2	2018-04-24	Huang	
	68	10104071	B2	2018-10-16	Gordon et al.	
	69	10121000	B1	2018-11-06	Rivlin et al.	
	70	10149148	B2	2018-12-04	Zha et al.	
	71	10182058	B2	2019-01-15	Xu	
	72	10237254	B2	2019-03-19	McDowell et al.	
	73	10249266	B2	2019-04-02	Zamir	
	74	10331659	B2	2019-06-25	Ahuja et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	75	10382529	B2	2019-08-13	Wan et al.	
	76	10419469	B1	2019-09-17	Singh et al.	
	77	10425437	B1	2019-09-24	Bog et al.	
	78	10454753	B2	2019-10-22	Sasturkar et al.	
	79	10496263	B2	2019-12-03	So et al.	
	80	10496678	B1	2019-12-03	Tang	
	81	10510007	B2	2019-12-17	Singhal et al.	
	82	10515095	B2	2019-12-24	Childress et al.	
	83	10581891	B1	2020-03-03	Kapoor et al.	
	84	10587609	B2	2020-03-10	Ebrahimi et al.	
	85	10592535	B2	2020-03-17	Ahn et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	86	10599718	B2	2020-03-24	Kumar et al.	
	87	10614200	B2	2020-04-07	Betz et al.	
	88	10642867	B2	2020-05-05	Palanciuc	
	89	10656979	B2	2020-05-19	Ishakian et al.	
	90	10664757	B2	2020-05-26	Lastras-Montano et al.	
	91	10685295	B1	2020-06-16	Ross et al.	
	92	10701051	B2	2020-06-30	Ohsumi	
	93	10754940	B2	2020-08-25	Ohsumi	
	94	10775183	B2	2020-09-15	Ho et al.	
	95	10824675	B2	2020-11-03	Alonso et al.	
	96	10824813	B2	2020-11-03	Smith et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	97	10885452	B1	2021-01-05	Garg	
	98	10904007	B2	2021-01-26	Kim et al.	
	99	10986114	B1	2021-04-20	Singh et al.	
	100	11036800	B1	2021-06-15	Kayyoor et al.	
	101	11048492	B2	2021-06-29	Jain et al.	
	102	11233821	B2	2022-01-25	Yadav et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	RE47937E1		2020-04-07	Ramachandran et al.	
	2	RE47952E1		2020-04-14	Ramachandran et al.	
	3	20020059531	A1	2002-05-16	Lai On, Warren Kwan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	4	20020161889	A1	2002-10-31	Gamache, Rod et al.	
	5	20030233361	A1	2003-12-18	Cady, C. Conrad	
	6	20050060287	A1	2005-03-17	Hellman, Ziv Z. et al.	
	7	20050102365	A1	2005-05-12	Moore, Jason Eric et al.	
	8	20050108142	A1	2005-05-19	Beadle, Alastair J.D. et al.	
	9	20050231760	A1	2005-10-20	Minato, Junichi	
	10	20050246288	A1	2005-11-03	Kimura, Daisuke et al.	
	11	20060036896	A1	2006-02-16	Gamache et al.	
	12	20060090095	A1	2006-04-27	Massa et al.	
	13	20070162605	A1	2007-07-12	Chalasani et al.	
	14	20070162963	A1	2007-07-12	PENET et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	15	20070169175	A1	2007-07-19	Hall et al.	
	16	20070225956	A1	2007-09-27	Pratt et al.	
	17	20070266425	A1	2007-11-15	Cho	
	18	20080034411	A1	2008-02-07	Aoyama	
	19	20080065879	A1	2008-03-13	Song et al.	
	20	20080072062	A1	2008-03-20	Pearson et al.	
	21	20080155335	A1	2008-06-26	Klein et al.	
	22	20080244718	A1	2008-10-02	Frost et al.	
	23	20080263643	A1	2008-10-23	Jaiswal et al.	
	24	20090165109	A1	2009-06-25	Hird	
	25	20090177573	A1	2009-07-09	Beadle et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	26	20090222740	A1	2009-09-03	YUAN	
	27	20090287720	A1	2009-11-19	Herter et al.	
	28	20100217860	A1	2010-08-26	Naidu et al.	
	29	20100309206	A1	2010-12-09	Xie et al.	
	30	20100329162	A1	2010-12-30	Kadous et al.	
	31	20110023098	A1	2011-01-27	Pearson et al.	
	32	20110029952	A1	2011-02-03	Harrington	
	33	20110302631	A1	2011-12-08	Sureshchandra et al.	
	34	20120054732	A1	2012-03-01	Jain et al.	
	35	20120089875	A1	2012-04-12	Faust et al.	
	36	20120102029	A1	2012-04-26	Larson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	37	20120158858	A1	2012-06-21	Gkantsidis et al.	
	38	20120173541	A1	2012-07-05	Venkataramani	
	39	20120317149	A1	2012-12-13	Jagota et al.	
	40	20130067100	A1	2013-03-14	Kuzin et al.	
	41	20130081118	A1	2013-03-28	Ge	
	42	20130086667	A1	2013-04-04	Haven	
	43	20130097320	A1	2013-04-18	Ritter et al.	
	44	20130173915	A1	2013-07-04	Haulund	
	45	20130219295	A1	2013-08-22	FELDMAN et al.	
	46	20130269007	A1	2013-10-10	Yoshigaki et al.	
	47	20140041005	A1	2014-02-06	HE	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	48	20140098101	A1	2014-04-10	FRIEDLANDER et al.	
	49	20140181944	A1	2014-06-26	AHMED et al.	
	50	20140325631	A1	2014-10-30	Pearson et al.	
	51	20140379716	A1	2014-12-25	Branch et al.	
	52	20150161201	A1	2015-06-11	Sadikov et al.	
	53	20150213598	A1	2015-07-30	Madabhushi et al.	
	54	20160063226	A1	2016-03-03	Singh et al.	
	55	20160203411	A1	2016-07-14	Sadikov et al.	
	56	20160261544	A1	2016-09-08	Conover	
	57	20160330183	A1	2016-11-10	McDowell et al.	
	58	20160330206	A1	2016-11-10	Xu	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	59	20160373428	A1	2016-12-22	Shi	
	60	20170063830	A1	2017-03-02	Huang	
	61	20170076206	A1	2017-03-16	Lastras-Montano et al.	
	62	20170085553	A1	2017-03-23	Gordon et al.	
	63	20170086069	A1	2017-03-23	Liu	
	64	20170111245	A1	2017-04-20	ISHAKIAN et al.	
	65	20170116315	A1	2017-04-27	Xiong et al.	
	66	20170249069	A1	2017-08-31	Zamir	
	67	20170257358	A1	2017-09-07	Ebrahimi et al.	
	68	20170262521	A1	2017-09-14	Cho et al.	
	69	20170277997	A1	2017-09-28	Zong et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	70	20170286190	A1	2017-10-05	ISHAKIAN et al.	
	71	20170337262	A1	2017-11-23	Smith et al.	
	72	20170353853	A1	2017-12-07	Zha et al.	
	73	20180025361	A1	2018-01-25	Ferrarons Llagostera et al.	
	74	20180039688	A1	2018-02-08	Ahn et al.	
	75	20180067981	A1	2018-03-08	Ahuja et al.	
	76	20180096047	A1	2018-04-05	Childress et al.	
	77	20180097793	A1	2018-04-05	AGARWAL et al.	
	78	20180139200	A1	2018-05-17	Gordon et al.	
	79	20180227286	A1	2018-08-09	OHSUMI	
	80	20190042879	A1	2019-02-07	Munoz	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	81	20190087480	A1	2019-03-21	Palanciuc	
	82	20190149553	A1	2019-05-16	XU	
	83	20190342282	A1	2019-11-07	Carbune et al.	
	84	20200074341	A1	2020-03-05	He et al.	
	85	20200080856	A1	2020-03-12	Ho et al.	
	86	20200175042	A1	2020-06-04	Batruni	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/MAHFUZUR RAHMAN/	Date Considered	06/07/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2024-05-01
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L818	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L819	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L820	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L821	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L822	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L823	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L824	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L825	1	L103 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 12:29 PM
L826	1	L103 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 12:29 PM
L827	1	L103 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 12:29 PM
L828	1	L103 and (cluster or group$3 or class or classifying or classified)	(US-PGPUB)	OR	ON	ON	2024/06/07 12:29 PM

		with (machine or server or device or terminal) with resource$3					
L829	52	L215 and logical adj graph same log adj5 data	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L830	52	L215 and logical adj graph same log adj5 data	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L831	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L832	73	L187 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:29 PM
L833	55	L205 and (previlege or permission or permit$4 or authoriz$5) same (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L834	429241	(H04L63/1425 OR G06F9/455 OR G06F9/545 OR G06F16/9024 OR G06F16/9038 OR G06F16/9535 OR G06F16/9537 OR G06F21/57 OR H04L43/045 OR H04L43/06 OR H04L63/10 OR H04L67/306 OR H04L67/535 OR G06F16/2456).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L835	429241	(H04L63/1425 OR G06F9/455 OR G06F9/545 OR G06F16/9024 OR G06F16/9038 OR G06F16/9535 OR G06F16/9537 OR G06F21/57 OR H04L43/045 OR H04L43/06 OR H04L63/10 OR H04L67/306 OR H04L67/535 OR G06F16/2456).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L836	20	((Original OR initial OR first) WITH (session instance communication	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO;	OR	ON	ON	2024/06/07 12:30 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00123

		profile OR log$4 OR credential) WITH (monitor$3 OR track$3 audit$3 OR inspect$3) WITH (generat$3 OR creat$3 OR produc$3) WITH (graph OR pattern OR map$4) WITH (anomal$3 OR behavior OR intrusion OR threat OR attack$3 anomalous OR risk) AND (multiple OR plurality) WITH (machine OR device OR node) WITH model$4) AND edge WITH (connect$3 OR link$3 OR communicat$3) AND (alert$3 OR alarm$3).clm.	JPO; DERWENT; IBM_TDB)				
L837	20	((Original OR initial OR first) WITH (session instance communication profile OR log$4 OR credential) WITH (monitor$3 OR track$3 audit$3 OR inspect$3) WITH (generat$3 OR creat$3 OR produc$3) WITH (graph OR pattern OR map$4) WITH (anomal$3 OR behavior OR intrusion OR threat OR attack$3 anomalous OR risk) AND (multiple OR plurality) WITH (machine OR device OR node) WITH model$4) AND edge WITH (connect$3 OR link$3 OR communicat$3) AND (alert$3 OR alarm$3).clm.	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L838	8	"20080022405"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L839	8	"20080022405"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L840	3	log WITH logical near4	(US-PGPUB)	OR	ON	ON	2024/06/07

		graph SAME anomal$3					12:30 PM
L841	3	log WITH logical near4 graph SAME anomal$3	(US-PGPUB)	OR	ON	ON	2024/06/07 12:30 PM
L842	2	L252 and graph with model	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L843	2	L252 and graph with model	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L844	2	L145 and (privilege or permission or restrict$3 or control$3 or chang$3 or modifying or modification) with (graph or model)	(US-PGPUB)	OR	ON	ON	2024/06/07 12:30 PM
L845	3	"17836558"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L846	3	"17836558"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L847	2138351	graph$3 SAME (generat$3 OR creat$3) (visual visualiz$5) near10 (personal individual$5 specific) AND (alert$3 alarm$3) AND device WITH location AND user WITH profile	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L848	78	L203 and (Anomal$3 or behavior or intrusion or threat or attack$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L849	78	L203 and (Anomal$3 or behavior or intrusion or threat or attack$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L850	78	L203 and (Anomal$3 or behavior or intrusion or threat or attack$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L851	78	L203 and (Anomal$3 or behavior or intrusion or threat or attack$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L852	47155	(H04L63/1425 or G06F17/30958).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	ON	2024/06/07 12:30 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00125

			JPO; DERWENT; IBM_TDB)				
L853	47155	(H04L63/1425 or G06F17/30958).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L854	73	L274 and (generat$3 or creat$3) with (graph or model)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L855	47155	(H04L63/1425 or G06F17/30958).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L856	47155	(H04L63/1425 or G06F17/30958).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L857	2	((US-20180288063-A1 OR US-20100094767-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/06/07 12:30 PM
L858	121	L251 and ((@ad or @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L859	1	L259 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 12:30 PM
L860	1	L259 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 12:30 PM
L861	11	(US-20100076952-$ or US-20170019487-$ or US-20160103883-$ or US-20180288063-$ or US-20180084012-$ or US-20160028753-$ or US-20140020102-$ or US-20130073387-$).did. or (US-9378044-$ or US-9210183-$ or US-8880588-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/07 12:30 PM
L862	28537	L173 and (detect$3 or indetif$4 or determin$5) with(Anomal$3 or behavior or intrusion or threat or attack$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM

L863	185	logical adj graph and log adj5 data	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L864	196300	"7" and ((anomal$3 or behavior or intrusion or threat or attack$3 anomalous potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2 fraudster or fraudulent) near8 (machine or device or node or client terminal) and (detect$3 or indetif$4 or determin$5) with(Anomal$3 or behavior or intrusion or threat or attack$3))	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L865	1	L40 and (privilege or permission or permit$4 or authoriz$5) with (model or table stor$3 or database or table to record$3 or log$4 repositor$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L866	89	L11 and ((@ad or @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 12:30 PM
L867	1803	shadow ADJ system WITH (device hardware resource system)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:14 PM
L868	0	853 AND shadow ADJ system WITH (device hardware resource system) near4 access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:15 PM
L869	0	853 AND shadow ADJ system WITH (device hardware resource system) WITH access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:15 PM
L870	0	853 AND shadow ADJ system WITH (device hardware resource system) WITH (activit$3 access$3)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:15 PM
L871	297	shadow ADJ system WITH (device hardware resource system) WITH	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO;	OR	ON	ON	2024/06/07 01:15 PM

		(activit$3 access$3)	JPO; DERWENT; IBM_TDB)				
L872	48	871 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:15 PM
L873	6	872 AND monitor$3 SAME shadow ADJ system WITH (device hardware resource system) WITH (activit$3 access$3)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:16 PM
L874	36	872 AND monitor$3 AND shadow ADJ system WITH (device hardware resource system) WITH (activit$3 access$3)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 01:20 PM
L875	31	874 AND shadow WITH access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 03:52 PM
L876	0	874 AND polygraph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 03:52 PM
L877	0	874 AND monitor$3 WITH activit$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 03:53 PM
L878	36	874 AND monitor$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 03:53 PM
L879	1	((US-20170310701-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/06/07 04:01 PM
L880	1	879 AND shadow WITH (device subset group type)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 04:01 PM
L881	35	"20150033340"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 04:06 PM
L882	0	853 AND shadow ADJ system WITH (device hardware resource	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO;	OR	ON	ON	2024/06/07 04:09 PM

		system) near4 access$3	JPO; DERWENT; IBM_TDB)				
L883	0	853 AND shadow ADJ system WITH (device hardware resource system) near4 access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 04:09 PM
L884	0	853 AND shadow ADJ system WITH (device hardware resource system) near4 access$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 04:09 PM
L885	1	L259 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 04:09 PM
L886	20	((Original OR initial OR first) WITH (session instance communication profile OR log$4 OR credential) WITH (monitor$3 OR track$3 audit$3 OR inspect$3) WITH (generat$3 OR creat$3 OR produc$3) WITH (graph OR pattern OR map$4) WITH (anomal$3 OR behavior OR intrusion OR threat OR attack$3 anomalous OR risk) AND (multiple OR plurality) WITH (machine OR device OR node) WITH model$4) AND edge WITH (connect$3 OR link$3 OR communicat$3) AND (alert$3 OR alarm$3).clm.	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 04:19 PM
L887	1	L103 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 04:19 PM
L888	1	L103 and (cluster or group$3 or class or classifying or classified) with (machine or server or device or terminal) with resource$3	(US-PGPUB)	OR	ON	ON	2024/06/07 04:19 PM

L889	5	752 AND (compar$3 detect$3 match$3) WITH (Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviation alert$3 alarm$3 tolerance warning failure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/06/07 04:19 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N509	64	("20060085437"|"20160080404"|"20180248901"|"9332020"|"9515999"|"9853968"|"20170118240"|"10033611"|"10142357"|"20030037136"|"20060259470"|"20110055138"|"20170279827"|"20180288063"|"20180367548"|"9021583"|"20070118909"|"20090271504"|"20120317151"|"20170163666"|"5806062"|"10389742"|"20180181750"|"20160149937"|"20050102284"|"20140359558"|"20170272344"|"20180020015"|"20180173789"|"8103906"|"9596253"|"20020184225"|"20090019160"|"20150135312"|"8122122"|"10115111"|"10127273"|"20040015470"|"20080148180"|"20100094767"|"20160078365"|"20160218911"|"20160359592"|"20180174062"|"20190132224"|"5584024"|"20100274785"|"20120005243"|"20180063178"|"20180115578"|"8443442"|"8862524"|"20140115001"|"20030179227"|"20100172261"|"20130304915"|"20150341379"|"20160205125"|"20180034	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/31 11:57 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00130

		840"|"9516053"|"9654503"|"20100114931"|"20190259033"|"20190222597").PN.					
N510	111	("20030040942"|"20030135758"|"20040049698"|"20050044418"|"20050261943"|"20080167920"|"20090024663"|"20110313930"|"20140328179"|"20150088595"|"20160189301"|"20170085595"|"8973088"|"20030126049"|"20070294118"|"20100229187"|"20110161116"|"20120046989"|"20120215575"|"20120284158"|"20160205138"|"8448245"|"8744894"|"9521160"|"9699209"|"20060184473"|"20060265746"|"20120059779"|"20130239167"|"20130283336"|"20140067716"|"20140137257"|"20150188949"|"20150331932"|"20160234247"|"20170093904"|"20170116552"|"9253203"|"9373144"|"10230764"|"20090037323"|"20160099963"|"20030084349"|"20030154393"|"20040010709"|"20040024693"|"20050015624"|"20050278786"|"20130191829"|"20130346328"|"20150341389"|"20170093905"|"6374358"|"8468599"|"8494955"|"8577775"|"8699767"|"9031951"|"9292881"|"20020026335"|"20040064726"|"20080047016"|"20090319342"|"20100205014"|"20110154497"|"20120041790"|"20120089617"|"20120096558"|"20120239438"|"20120300975"|"20130239177"|"20140019171"|"20140200930"|"20170187745"|"7047419"|"7324952"|"20020091551"|"20030014344"|"20030236990"|"20110078073"|"20140379708"|"20160212169"|"6269349"|	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/31 11:57 PM

		"7680659"|"7711646"|"20040260945"|"20080016563"|"20120011077"|"20130055404"|"20130347060"|"20140067713"|"20140142988"|"20150373043"|"20160248799"|"8484066"|"8601587"|"20090063365"|"20030028803"|"20040006532"|"20070192867"|"20080250064"|"20100114634"|"20130188475"|"20130239168"|"20140007190"|"20160248800"|"20160294854"|"8332242"|"9646428"|"20030014342"|"20080162377").PN.					
N511	111	("20030040942"|"20030135758"|"20040049698"|"20050044418"|"20050261943"|"20080167920"|"20090024663"|"20110313930"|"20140328179"|"20150088595"|"20160189301"|"20170085595"|"8973088"|"20030126049"|"20070294118"|"20100229187"|"20110161116"|"20120046989"|"20120215575"|"20120284158"|"20160205138"|"8448245"|"8744894"|"9521160"|"9699209"|"20060184473"|"20060265746"|"20120059779"|"20130239167"|"20130283336"|"20140067716"|"20140137257"|"20150188949"|"20150331932"|"20160234247"|"20170093904"|"20170116552"|"9253203"|"9373144"|"10230764"|"20090037323"|"20160099963"|"20030084349"|"20030154393"|"20040010709"|"20040024693"|"20050015624"|"20050278786"|"20130191829"|"20130346328"|"20150341389"|"20170093905"|"6374358"|"8468599"|"8494955"|"8577775"|"8699767"|"9031951"|"9292881"|"20020026335"|"20040064726"|"2008004	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/31 11:57 PM

		7016"|"20090319342"|"20100205014"|"20110154497"|"20120041790"|"20120089617"|"20120096558"|"20120239438"|"20120300975"|"20130239177"|"20140019171"|"20140200930"|"20170187745"|"7047419"|"7324952"|"20020091551"|"20030014344"|"20030236990"|"20110078073"|"20140379708"|"20160212169"|"6269349"|"7680659"|"7711646"|"20040260945"|"20080016563"|"20120011077"|"20130055404"|"20130347060"|"20140067713"|"20140142988"|"20150373043"|"20160248799"|"8484066"|"8601587"|"20090063365"|"20030028803"|"20040006532"|"20070192867"|"20080250064"|"20100114634"|"20130188475"|"20130239168"|"20140007190"|"20160248800"|"20160294854"|"8332242"|"9646428"|"20030014342"|"20080162377").PN.					
N512	18	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/07 12:30 PM

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**05/01/2024 02:12:33 PM Z ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	Ashley Jenkins
PATENT CENTER #	65336216	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2024-05-01_L0040B3CIP6C1_IDS.pdf	21	Information Disclosure Statement (IDS) Form (SB08)	1256 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2024-05-01_L0040B3CIP6C1_IDS.pdf	4B36BC0E3DD37C3637958CACD1CE869476495855F00AA3F781EB2258E56624ADC7ABB7404C010D7FBE611EA6C9DC6DFA0E740BF2FB20406519457CBEB116D78E

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	05/01/2024 02:12:33 PM Z ET	L0040B3CIP6C1

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	Ashley Jenkins
PATENT CENTER #	65336216	AUTHORIZED BY	Edward Lenart
CUSTOMER #	182115	FILING DATE	07/06/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	VIKRAM KAPOOR

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 2001	E202451E13046811	Ashley Jenkins

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1806	SUBMISSION OF AN INFORMATION DISCLOSURE STATEMENT	260.00	1	260.00
			TOTAL AMOUNT:	$260.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	2498
Examiner Name	Mahfuzur RAHMAN
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6347339	B1	2002-02-12	Morris et al.	
	2	6434663	B1	2002-08-13	Grimsrud et al.	
	3	6938084	B2	2005-08-30	Gamache et al.	
	4	7310733	B1	2007-12-18	Pearson et al.	
	5	7529801	B2	2009-05-05	Moore et al.	
	6	7562045	B2	2009-07-14	Beadle et al.	
	7	7743153	B2	2010-06-22	Hall et al.	
	8	7797548	B2	2010-09-14	Pearson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	9	7856544	B2	2010-12-21	Schenfeld et al.	
	10	7926026	B2	2011-04-12	Klein et al.	
	11	7962635	B2	2011-06-14	Naidu et al.	
	12	7996885	B2	2011-08-09	Jaiswal et al.	
	13	8032925	B2	2011-10-04	Cho	
	14	8037284	B2	2011-10-11	Schenfeld et al.	
	15	8037521	B2	2011-10-11	Minato	
	16	8151107	B2	2012-04-03	Song et al.	
	17	8276197	B1	2012-09-25	Mangal et al.	
	18	8291233	B2	2012-10-16	Pearson et al.	
	19	8341711	B1	2012-12-25	Pennington et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	20	8351456	B2	2013-01-08	Kadous et al.	
	21	8359584	B2	2013-01-22	Rao et al.	
	22	8497863	B2	2013-07-30	Xie et al.	
	23	8549002	B2	2013-10-01	Herter et al.	
	24	8561157	B2	2013-10-15	Ge	
	25	8595262	B1	2013-11-26	Hayden	
	26	8607306	B1	2013-12-10	Bridge et al.	
	27	8655989	B2	2014-02-18	Ritter et al.	
	28	8725587	B2	2014-05-13	Beadle et al.	
	29	8826403	B2	2014-09-02	Bhaskaran et al.	
	30	8843646	B2	2014-09-23	Kuzin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	31	8959608	B2	2015-02-17	Ahmed et al.	
	32	9053306	B2	2015-06-09	Yoshigaki et al.	
	33	9231935	B1	2016-01-05	Bridge et al.	
	34	9239873	B2	2016-01-19	Branch et al.	
	35	9246897	B2	2016-01-26	He	
	36	9323806	B2	2016-04-26	Sadikov et al.	
	37	9369450	B1	2016-06-14	Barak et al.	
	38	9391978	B2	2016-07-12	Burch et al.	
	39	9400882	B2	2016-07-26	Pearson et al.	
	40	9430830	B2	2016-08-30	Madabhushi et al.	
	41	9495522	B2	2016-11-15	Singh et al.	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00141

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	42	9537851	B2	2017-01-03	Gordon et al.	
	43	9569869	B2	2017-02-14	Hesse et al.	
	44	9582766	B2	2017-02-28	Sadikov et al.	
	45	9596295	B2	2017-03-14	Banadaki et al.	
	46	9602506	B2	2017-03-21	Kang et al.	
	47	9602526	B2	2017-03-21	Liu et al.	
	48	9639676	B2	2017-05-02	Betz et al.	
	49	9652875	B2	2017-05-16	Vassilvitskii et al.	
	50	9659337	B2	2017-05-23	Lee et al.	
	51	9665660	B2	2017-05-30	Wensel	
	52	9740744	B2	2017-08-22	Stetson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	53	9741138	B2	2017-08-22	Friedlander et al.	
	54	9753960	B1	2017-09-05	Troyanovsky	
	55	9760619	B1	2017-09-12	Lattanzi et al.	
	56	9781115	B2	2017-10-03	Heise	
	57	9787705	B1	2017-10-10	Love et al.	
	58	9805080	B2	2017-10-31	Joshi et al.	
	59	9805140	B2	2017-10-31	Chakrabarti et al.	
	60	9819671	B2	2017-11-14	Ji	
	61	9830435	B2	2017-11-28	Haven	
	62	9836183	B1	2017-12-05	Love et al.	
	63	9852230	B2	2017-12-26	Fleury et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	64	9887999	B2	2018-02-06	Dong et al.	
	65	9942220	B2	2018-04-10	Bajenov et al.	
	66	9946800	B2	2018-04-17	Qian et al.	
	67	9954842	B2	2018-04-24	Huang	
	68	10104071	B2	2018-10-16	Gordon et al.	
	69	10121000	B1	2018-11-06	Rivlin et al.	
	70	10149148	B2	2018-12-04	Zha et al.	
	71	10182058	B2	2019-01-15	Xu	
	72	10237254	B2	2019-03-19	McDowell et al.	
	73	10249266	B2	2019-04-02	Zamir	
	74	10331659	B2	2019-06-25	Ahuja et al.	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00144

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	75	10382529	B2	2019-08-13	Wan et al.	
	76	10419469	B1	2019-09-17	Singh et al.	
	77	10425437	B1	2019-09-24	Bog et al.	
	78	10454753	B2	2019-10-22	Sasturkar et al.	
	79	10496263	B2	2019-12-03	So et al.	
	80	10496678	B1	2019-12-03	Tang	
	81	10510007	B2	2019-12-17	Singhal et al.	
	82	10515095	B2	2019-12-24	Childress et al.	
	83	10581891	B1	2020-03-03	Kapoor et al.	
	84	10587609	B2	2020-03-10	Ebrahimi et al.	
	85	10592535	B2	2020-03-17	Ahn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	86	10599718	B2	2020-03-24	Kumar et al.	
	87	10614200	B2	2020-04-07	Betz et al.	
	88	10642867	B2	2020-05-05	Palanciuc	
	89	10656979	B2	2020-05-19	Ishakian et al.	
	90	10664757	B2	2020-05-26	Lastras-Montano et al.	
	91	10685295	B1	2020-06-16	Ross et al.	
	92	10701051	B2	2020-06-30	Ohsumi	
	93	10754940	B2	2020-08-25	Ohsumi	
	94	10775183	B2	2020-09-15	Ho et al.	
	95	10824675	B2	2020-11-03	Alonso et al.	
	96	10824813	B2	2020-11-03	Smith et al.	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00146

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	97	10885452	B1	2021-01-05	Garg	
	98	10904007	B2	2021-01-26	Kim et al.	
	99	10986114	B1	2021-04-20	Singh et al.	
	100	11036800	B1	2021-06-15	Kayyoor et al.	
	101	11048492	B2	2021-06-29	Jain et al.	
	102	11233821	B2	2022-01-25	Yadav et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	RE47937E1		2020-04-07	Ramachandran et al.	
	2	RE47952E1		2020-04-14	Ramachandran et al.	
	3	20020059531	A1	2002-05-16	Lai On, Warren Kwan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	4	20020161889	A1	2002-10-31	Gamache, Rod et al.	
	5	20030233361	A1	2003-12-18	Cady, C. Conrad	
	6	20050060287	A1	2005-03-17	Hellman, Ziv Z. et al.	
	7	20050102365	A1	2005-05-12	Moore, Jason Eric et al.	
	8	20050108142	A1	2005-05-19	Beadle, Alastair J.D. et al.	
	9	20050231760	A1	2005-10-20	Minato, Junichi	
	10	20050246288	A1	2005-11-03	Kimura, Daisuke et al.	
	11	20060036896	A1	2006-02-16	Gamache et al.	
	12	20060090095	A1	2006-04-27	Massa et al.	
	13	20070162605	A1	2007-07-12	Chalasani et al.	
	14	20070162963	A1	2007-07-12	PENET et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	15	20070169175	A1	2007-07-19	Hall et al.	
	16	20070225956	A1	2007-09-27	Pratt et al.	
	17	20070266425	A1	2007-11-15	Cho	
	18	20080034411	A1	2008-02-07	Aoyama	
	19	20080065879	A1	2008-03-13	Song et al.	
	20	20080072062	A1	2008-03-20	Pearson et al.	
	21	20080155335	A1	2008-06-26	Klein et al.	
	22	20080244718	A1	2008-10-02	Frost et al.	
	23	20080263643	A1	2008-10-23	Jaiswal et al.	
	24	20090165109	A1	2009-06-25	Hird	
	25	20090177573	A1	2009-07-09	Beadle et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	26	20090222740	A1	2009-09-03	YUAN	
	27	20090287720	A1	2009-11-19	Herter et al.	
	28	20100217860	A1	2010-08-26	Naidu et al.	
	29	20100309206	A1	2010-12-09	Xie et al.	
	30	20100329162	A1	2010-12-30	Kadous et al.	
	31	20110023098	A1	2011-01-27	Pearson et al.	
	32	20110029952	A1	2011-02-03	Harrington	
	33	20110302631	A1	2011-12-08	Sureshchandra et al.	
	34	20120054732	A1	2012-03-01	Jain et al.	
	35	20120089875	A1	2012-04-12	Faust et al.	
	36	20120102029	A1	2012-04-26	Larson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	37	20120158858	A1	2012-06-21	Gkantsidis et al.	
	38	20120173541	A1	2012-07-05	Venkataramani	
	39	20120317149	A1	2012-12-13	Jagota et al.	
	40	20130067100	A1	2013-03-14	Kuzin et al.	
	41	20130081118	A1	2013-03-28	Ge	
	42	20130086667	A1	2013-04-04	Haven	
	43	20130097320	A1	2013-04-18	Ritter et al.	
	44	20130173915	A1	2013-07-04	Haulund	
	45	20130219295	A1	2013-08-22	FELDMAN et al.	
	46	20130269007	A1	2013-10-10	Yoshigaki et al.	
	47	20140041005	A1	2014-02-06	HE	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	48	20140098101	A1	2014-04-10	FRIEDLANDER et al.	
	49	20140181944	A1	2014-06-26	AHMED et al.	
	50	20140325631	A1	2014-10-30	Pearson et al.	
	51	20140379716	A1	2014-12-25	Branch et al.	
	52	20150161201	A1	2015-06-11	Sadikov et al.	
	53	20150213598	A1	2015-07-30	Madabhushi et al.	
	54	20160063226	A1	2016-03-03	Singh et al.	
	55	20160203411	A1	2016-07-14	Sadikov et al.	
	56	20160261544	A1	2016-09-08	Conover	
	57	20160330183	A1	2016-11-10	McDowell et al.	
	58	20160330206	A1	2016-11-10	Xu	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	59	20160373428	A1	2016-12-22	Shi	
	60	20170063830	A1	2017-03-02	Huang	
	61	20170076206	A1	2017-03-16	Lastras-Montano et al.	
	62	20170085553	A1	2017-03-23	Gordon et al.	
	63	20170086069	A1	2017-03-23	Liu	
	64	20170111245	A1	2017-04-20	ISHAKIAN et al.	
	65	20170116315	A1	2017-04-27	Xiong et al.	
	66	20170249069	A1	2017-08-31	Zamir	
	67	20170257358	A1	2017-09-07	Ebrahimi et al.	
	68	20170262521	A1	2017-09-14	Cho et al.	
	69	20170277997	A1	2017-09-28	Zong et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	70	20170286190	A1	2017-10-05	ISHAKIAN et al.	
	71	20170337262	A1	2017-11-23	Smith et al.	
	72	20170353853	A1	2017-12-07	Zha et al.	
	73	20180025361	A1	2018-01-25	Ferrarons Llagostera et al.	
	74	20180039688	A1	2018-02-08	Ahn et al.	
	75	20180067981	A1	2018-03-08	Ahuja et al.	
	76	20180096047	A1	2018-04-05	Childress et al.	
	77	20180097793	A1	2018-04-05	AGARWAL et al.	
	78	20180139200	A1	2018-05-17	Gordon et al.	
	79	20180227286	A1	2018-08-09	OHSUMI	
	80	20190042879	A1	2019-02-07	Munoz	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	81	20190087480	A1	2019-03-21	Palanciuc	
	82	20190149553	A1	2019-05-16	XU	
	83	20190342282	A1	2019-11-07	Carbune et al.	
	84	20200074341	A1	2020-03-05	He et al.	
	85	20200080856	A1	2020-03-12	Ho et al.	
	86	20200175042	A1	2020-06-04	Batruni	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	2498
	Examiner Name	Mahfuzur RAHMAN
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2024-05-01
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00158

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor:	VIKRAM KAPOOR
Serial No.:	17/858,866
Atty Docket No.:	L0040B3CIP6C1
Group Art Unit:	2498
Filed:	07/06/2022
Customer No.:	182115
Confirmation No.:	4455
Examiner:	MAHFUZUR RAHMAN
Title:	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Mail Stop: Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

RESPONSE TO OFFICE ACTION DATED FEBRUARY 01, 2024

This is a Response to the Office Action dated February 01, 2024 (hereafter "the Office Action"). Applicant presents the following amendments and remarks demonstrating that the case is in condition for allowance.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00159

AMENDMENT

Amendments To The Claims:

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising:

gathering first information describing access to one or more resources by one or more user devices of a user;

gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity.

2. (Original) The method of claim 1 wherein the first information is gathered from one or more identity providers.

3. (Original) The method of claim 1 wherein the first information is gathered from the one or more applications.

4. (Original) The method of claim 1 further comprising generating a polygraph indicating the one or more shadow systems.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00160

5. (Original) The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.

6. (Original) The method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems.

7. (Original) The method of claim 1 wherein identifying the one or more shadow systems comprises:

identifying one or more accesses described in the first information but not described in the second information; and

identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

8. (Original) The method of claim 1 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices.

9. (Currently Amended) A ~~computer program product for using activity monitored by multiple data sources to identify shadow systems, the computer program product disposed on a computer readable medium, the computer program product including computer program instructions configurable to carry out the steps of~~ non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to:

~~gathering~~ gather first information describing access to one or more resources by one or more user devices of a user;

~~gathering~~ gather, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00161

~~identifying~~ identify one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity.

10. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from one or more identity providers.

11. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more applications.

12. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 further comprising generating a polygraph indicating the one or more shadow systems.

13. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 ~~wherein the steps further comprise further comprising generating~~ wherein the instructions, when executed, further cause the processing device to generate an alert in response to identifying the one or more shadow systems.

14. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 ~~wherein the steps further comprise directing~~ wherein the instructions, when executed, further cause the processing device to direct the user to a remediation workflow in response to identifying the one or more shadow systems.

15. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 wherein, to identify[[ing]] the one or more

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00162

shadow systems, the instructions, when executed, further cause the processing device to: ~~comprises;~~

identify[[ing]] one or more accesses described in the first information but not described in the second information; and

identify[[ing]], as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

16. (Currently Amended) The ~~computer program product~~ non-transitory computer readable storage medium of claim 9 wherein the second information is gathered via one or more proxy application executed on the at least a subset of the one or more user devices.

17. (Currently Amended) A system ~~for using activity monitored by multiple data sources to identify shadow systems, the system configurable to carry out the steps of~~ comprising:

a memory; and

a processing device, operatively coupled to the memory, the processing device configured to:

~~gathering~~ gather first information describing access to one or more resources by one or more user devices of a user;

~~gathering~~ gather, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and

~~identifying~~ identify one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00163

or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity.

18. (Original) The system of claim 17 wherein the first information is gathered from one or more identity providers.

19. (Original) The system of claim 17 wherein the first information is gathered from the one or more applications.

20. (Currently Amended) The system of claim 17 wherein ~~the steps further comprise generating~~ the processing device is further configured to generate a polygraph indicating the one or more shadow systems.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00164

REMARKS

Claims 1-20 are pending. In this Amendment, Applicants have amended claims 1, 9-17 20. Applicants are not conceding that the subject matter encompassed by the claims prior to this Amendment is unpatentable over the art cited by the Examiner. Applicants respectfully reserve the right to pursue claims in one or more continuing applications, including claims capturing the subject matter encompassed by the claims prior to this Amendment and additional claims. No new matter has been added.

Examiner Interview

Applicant thanks the Examiner for the time spent with Applicant's representative, Jason Fletcher (Reg. No. 68,044), during the telephonic interview held February 16, 2024. An agreement was reached regarding clarifying amendments to expedite prosecution. No further agreement was reached.

Claim Rejections – 35 U.S.C. § 101

Claims 9-16 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Particularly, the Office Action alleges that the claimed computer program product covers both transitory and non-transitory embodiments. Applicant has amended claims 9-16 to recite a "non-transitory computer readable storage medium." Accordingly, Applicant asserts that the rejection has been overcome and should be withdrawn.

Claim Interpretation – 35 U.S.C. § 112(f)

The Office Action alleges that claims 17-20 invoke interpretation under 35 U.S.C. § 112(f) due to allegedly reciting a generic placeholder followed by functional language without corresponding structure. Applicant has amended claim 17 to recite a "memory" and a "processing device" operatively coupled to the memory, therefore reciting sufficient structure and not invoking interpretation under 35 U.S.C. § 112(f).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00165

Claim Rejections – 35 U.S.C. § 103

Claims 1-20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Giokas (U.S. Patent Publication No. 2015/0033340) in view of Di Pietro (U.S. Patent Publication No. 2016/0028753).

Independent Claims 1, 9, and 17

Applicants respectfully note in response that no combination of only the cited references can be used to establish a prima facie case of obviousness against claims 1-20 of the present application under 35 U.S.C. § 103 because the cited references, individually or in combination, do not teach or suggest every element and limitation of independent claims 1, 9, and 17 of the present application. For example, the cited portions of the cited references, individually or in combination, do not teach or suggest at least the following limitations of independent claims 1, 9, and 17 of the present application: "gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources." The Office Action cites Giokas at [0069, 0071, 0074] as disclosing "gathering…second information describing access to the one or more resources." Applicant disagrees.

The cited portions of Giokas merely recite broad teachings describing the components of a "computing device," such as having "input and output" capabilities (Giokas at [0069]), "display devices" (Giokas at [0071]), and a "network interface" (Giokas at [0074]). These cited portions of Giokas only serve to describe the components and capabilities of a "computing device" at an extremely high level and do not recite nor relate in any way to gathering information related to the access of resources by those devices. Therefore, Giokas fails to disclose this element.

Di Pietro fails to cure the deficiencies of Giokas. The Office Action relies on Di Pietro at [0043] and [0070] as disclosing "at least a subset of the one or more user devices." Applicant disagrees. The cited portions of Di Pietro merely describe the existence of

Low-power and Lossy Networks (LLNs), a class of networks where the routers and interconnects of the network are constrained. Again, the cited portions of Di Pietro only serve to describe broad, high-level teachings that do not relate in any way to the claimed limitations.

This element recites that information related to the access of one or more resources is gathered from a subset of user devices. The cited portions of Giokas only describe broad teachings related to the existence of computing devices while the cited portions of Di Pietro only describe broad teachings related to the existence of LLNs. A combination of such broad teachings cannot rise to the level of disclosing "gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources" as claimed. Thus, the combined references fail to disclose this element.

The combined references also fail to disclose "identifying one or more shadow systems based on a discrepancy between the first information and the second information." The Office Action cites Giokas at [0009, 0057] as disclosing this element. Applicant disagrees. The cited portions of Giokas recite an "IDPS" that monitors data packets and compares the monitored information to pre-determined rules for identifying known attack patterns. Even if, for the sake of argument, identifying attack patterns disclosing identifying "shadow systems" as claimed, the cited reference relies on an approach whereby activity is monitored and compared to a set of known rules. In contrast, the claimed embodiments describe an approach whereby shadow systems are identified based on a discrepancy between two sets of information: first information gathered from some data source and second information gathered from the user devices themselves. The approaches described in Giokas do not rely on any such comparison. Put differently, one skilled in the art would appreciate the difference between detecting matches to activity patterns as described in Giokas and finding discrepancies between two different sets of information as claimed. Therefore, Giokas fails to disclose this element. As Di Pietro fails to cure the deficiencies of Giokas, the combined references fail to disclose this element.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00167

Because the cited references, individually or in combination, do not teach or suggest every element and limitation of independent claims 1, 9, and 17, no combination of only the cited references can be used to establish a prima facie case of obviousness, under 35 U.S.C. § 103, against claims 1, 9, and 17 of the present application. Claims 1, 9, 17, and their respective dependent claims are therefore allowable. Applicants therefore respectfully request that the § 103 rejections be withdrawn and the claims be allowed.

Dependent Claims 2, 10, and 18

The cited references also fail to disclose at least the following limitation of dependent claims 2, 10, and 18: "wherein the first information is gathered from one or more identity providers." The Office Action cites Giokas at [0088, 0095] as disclosing this element. Applicant disagrees. The cited portion of Giokas describes a "network security tool" that can address findings of a "vulnerability assessor" that analyzes data packets. Applicant notes that an "identity provider" is a term of art in computing for an entity that manages identify information and authentication as a service. Neither the "network security tool" nor the "vulnerability assessor" of Giokas serve these functions. Accordingly, absent any explicit disclosure of an "identity provider," Giokas fails to disclose this element. As Di Pietro fails to cure the deficiencies of Giokas, the combined references fail to disclose this element.

Furthermore, Applicant notes that Giokas is silent as to any information gathered from this "network security tool" or "vulnerability assessor" that is compared to information gathered from user devices in order to identify shadow systems. In combination with the independent claims from which they depend, the claimed embodiments are directed to approaches whereby information gathered from an identity provider is compared to information gathered from user devices in order to identify shadow systems based on some discrepancy between the gathered information. None of the cited references, individually or in combination, disclose these features. Therefore, the combined references fail to disclose this element. Accordingly, Applicant requests that the rejection of claims 2, 10, and 18 be withdrawn.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00168

Dependent Claims 3, 11, and 19

The cited references also fail to disclose at least the following limitation of dependent claims 3, 11, and 19: "wherein the first information is gathered from one or more identity providers." The Office Action cites Giokas at [0061] as disclosing this element. Applicant disagrees. The cited portion of Giokas describes that SaaS resources can be accessed through smartphone or tablet applications. Put differently, the cited portions of Giokas merely describe the existence of SaaS applications and that those applications can be accessed by devices. Giokas does not disclose or describe in any way gathering information from these applications that describes access to those applications, let alone for comparison to other information for the purposes of identifying shadow systems. Therefore, Giokas fails to disclose this element. As Di Pietro fails to cure the deficiencies of Giokas, the combined references fail to disclose this element.

In combination with the independent claims from which they depend, the claimed embodiments are directed to approaches whereby information gathered from applications is compared to information gathered from user devices in order to identify shadow systems based on some discrepancy between the gathered information. None of the cited references, individually or in combination, disclose these features. Therefore, the combined references fail to disclose this element. Accordingly, Applicant requests that the rejection of claims 3, 11, and 19 be withdrawn.

Dependent Claims 7 and 15

The cited references also fail to disclose at least the following limitation of dependent claims 7 and 15: "wherein identifying the one or more shadow systems comprises: identifying one or more accesses described in the first information but not described in the second information; and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses." The Office Action cites Giokas at [0084, 0011, 0049] as disclosing these elements. Applicant disagrees. For example, the Office Action relies on Giokas at [0084] as disclosing "identifying one or more accesses

described in the first information but not described in the second information." This portion of Giokas merely recites that a "tool" can be configured to use information from "vulnerabilities lists or registries" that may be formatted or scheme independent. Giokas is silent as to any identification of accesses found in one set of information but not another as claimed. The mere usage of "vulnerabilities lists" does not disclose "identifying one or more accesses described in the first information but not described in the second information" as claimed. Therefore, Giokas fails to disclose this element. As Di Pietro fails to cure the deficiencies of Giokas, the combined references fail to disclose this element.

As another example, Giokas at [0011, 0049] discloses a "network security tool" that may communicate with a "vulnerability assessment tool." Again, these cited portions of Giokas merely describe broad teachings relating to the existence of various tools. Giokas does not disclose any identification of accesses found in one set of information but not another and using those identified accesses to identify shadow systems. The broad, high-level teachings of the cited references again fail to rise to the level of the specific features found in the claims. Therefore, the cited references fail to disclose these elements. Accordingly, Applicant requests that the rejection of these claims be withdrawn.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 50-3082 for any fees required or overpaid.

Respectfully submitted,

Date: May 1, 2024

By: /Jason T. Fletcher/
Jason T. Fletcher, Reg. No. 68,044
Kennedy Lenart Spraggins LLP
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPLICANT

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**05/01/2024 01:44:01 PM Z ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	Ashley Jenkins
PATENT CENTER #	65334937	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Jason Fletcher

Documents

TOTAL DOCUMENTS: 3

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection.pdf		12	-	118 KB
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection-A....pdf	(1-1)	1	Amendment/Request for Reconsideration-After Non-Final Rejection	79 KB
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection-CLM.pdf	(2-6)	5	Claims	99 KB
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection-REM.pdf	(7-12)	6	Applicant Arguments/Remarks Made in an Amendment	90 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection.pdf	8CE75A2FD748CC0A804AC5EDC9523BE19E9D28C4F2EDE9D12169AE4ED8215C6A048BA4D788C7AC0943DF8CA6031E776832849F3DE68B52AACA5D1419F9477378
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection-A....pdf	885E26C0E7DDAA52072E0DF9608C2276501361C564C7BFCEEA90FB0838957548969BB99BCB18219202C55A18E1B57A1A01CF976EA6861C8B6190EB22C69BDC55
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection-CLM.pdf	0336EE61B6A28D0D68A2F475035533AF7388B989227D81F2FA370549A1F7A4CBABD460EE204BE30D77A344AA4909A6F0344DE05D921AA615EC81AC2F822A816F
2024-05-01_L0040B3CIP6C1_ResponsetoNFRejection-REM.pdf	C7DE07255522C41EFE28BD8E1F2C2B15BC7C68EA70E58D97FA3374BE749AB00141409C200B95D88EA1FE069E6F01FAD6F796B36A12F7A7DA70D5BAEE52EE824A

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/858,866	Filing Date 07/06/2022	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $480 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	05/01/2024	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	PSA
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/TAMMY D MCBETH/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

182115 7590 02/29/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
02/29/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
kate@klspatents.com
office@klspatents.com

Applicant-Initiated Interview Summary	**Application No.** 17/858,866	**Applicant(s)** KAPOOR et al.		
	Examiner MAHFUZUR RAHMAN	**Art Unit** 2498	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MAHFUZUR RAHMAN	Primary Examiner	Telephonic
Jason Fletcher	Attorney	

Date of Interview: 16 February 2024

Issues Discussed:

Other

Applicant's representative Jason Fletcher and the Examiner Mahfuzur Rahman were among the participants of the interview. Mr. Fletcher explained proposed claim amendments presented in the interview agenda and discussed the rejections under 35 USC 103. The Examiner respectfully suggested that claims be further amended for clarity especially "shadow systems". It was indicated that incorporating the combined limitations of claims 4, 6, and 8 or claims 6, 7, and 8 into respective independent claims would better clarify the subject matter/embodiment of claimed invention. The Examiner indicated that claim amendments would require a further review/search and consideration. No agreement was reached as to the allowability of the case at this time.

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/858,866	07/06/2022	VIKRAM KAPOOR	L0040B3CIP6C1	4455

182115 7590 02/01/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
02/01/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
kate@klspatents.com
office@klspatents.com

Office Action Summary	Application No. 17/858,866	Applicant(s) KAPOOR et al.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2498	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 07/06/2022

.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 06 July 2022 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 01/06/2023, 04/24/2023, 12/07/2023.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Claims 1-20 are presented for examination on the merits

Notice of Pre-AIA or AIA Status

The present application is being examined under the first inventor to file provisions of the AIA.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 01/06/2023, 04/24/2023, 12/07/2023 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Drawings

The drawings filed on 07/06/2022 are accepted by the examiner.

Priority

The application is filed on 07/06/2022 and claims an earlier priority date from provisional application filed on 11/27/2017.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 9 is rejected under 35 U.S.C. 101 because: the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

3. Claim 9 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Independent Claim 18 recites "a computer program product for using activity monitored by multiple data sources to identify shadow systems, the computer program product disposed on a computer readable medium….". Pending claims are interpreted as broadly as their terms reasonably allow (See In re Zletz, 893 F.2d 3 19 (Fed. Cir. 1989)). The broadest reasonable interpretation of a claim drawn to a computer readable storage medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media (See MPEP 2111.01). When the broadest reasonable interpretation of a claim covers a signal per se, the claim must be rejected under 35 U.S.C. §101 as covering non-statutory subject matter. See In re Nuijten, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter).

4. The Examiner suggests that a claim drawn to such a computer program product that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. §101 by adding the limitation "non-transitory" to the claim [or any similar limitations such as "computer usable memory", or "computer usable storage memory", or "computer readable memory", or "computer readable device", (i.e. any variations thereof, where "media" or "medium" is replaced by "device" or "memory")]. Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes signals per se. The limited situations in which such an amendment could raise issues of new matter occur, for example, when the specification does not support

a non-transitory embodiment because a signal per se is the only viable embodiment such that the amended claim is impermissibly broadened beyond the supporting disclosure. See, e.g., Gentqv Galleiy, Inc. v. Berkline Corp., 134 F.3d 1473 (Fed. Cir. 1998).

5. Claims 10-16 are also rejected under 101 because they inherit the deficiencies of the base claim 9.

Claim Interpretation

6. The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

7. Claim 17 is interpreted under 35 U.S.C. 112(f) or 35 U.S.C. 112(pre-AIA), sixth paragraph.

8. The limitations "a system for using activity monitored by multiple data sources to identify shadow systems, the system configurable to carry out the steps of: gathering first information ..." in claim 17 has been interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the "system" as claimed uses a generic placeholder coupled with functional language such as "gathering first information"

without reciting sufficient structure to achieve the function. Furthermore, the generic placeholder is not preceded by a structural modifier.

9. Since these claim limitation(s) invokes 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, claim(s) 16 has been interpreted to cover the corresponding structure described in the specification that achieves the claimed function, and equivalents thereof.

10. A review of the specification shows that the following appears to be the corresponding structure described in the specification for the 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph limitation: The blocks of FIG.5A and 5B illustrates "system" elements that gather information to enable the utilization of networking resources or network traffic to specific processes. This is useful in analyzing the behavior of a particular process, which is important for observability. See also the steps described in associated paragraphs 00199, 00232, 00250, 00630 of the specification.

If applicant wishes to provide further explanation or dispute the examiner's interpretation of the corresponding structure, applicant must identify the corresponding structure with reference to the specification by page and line number, and to the drawing, if any, by reference characters in response to this Office action.

If applicant does not intend to have the claim limitation(s) treated under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112 , sixth paragraph, applicant may amend the claim(s) so that it/they will clearly not invoke 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, or present a sufficient showing that the claim recites/recite sufficient structure, material, or acts for performing the claimed function to preclude application of 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

For more information, see MPEP § 2173 *et seq.* and *Supplementary Examination Guidelines for Determining Compliance With 35 U.S.C. 112 and for Treatment of Related Issues in Patent Applications*, 76 FR 7162, 7167 (Feb. 9, 2011).

Claim Rejections - 35 USC § 103

11. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

12. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

13. The factual inquiries set forth in Graham **v.** John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

15. Claims 1-20 are rejected under 35 U.S.C. 103 as being unpatentable over Giokas (US 20150033340 A1, hereinafter, Giokas) in view of Di Pietro et al. (US 20160028753 A1).

Regarding claim 1, Giokas discloses a method of using activity monitored by multiple data sources to identify shadow systems (Paragraph 0027: passive vulnerability assessor is further configured to receive a plurality of logs of network activity associated with computing devices of the protected network),

the method comprising: gathering first information describing access to one or more resources by one or more user devices of a user (Paragraphs 0029, 0093: clients 102a-n (e.g., end user devices, computing devices, administrator devices) or servers 106a-n that communicate via a private or protected network wherein system includes a plurality of modules to collect, analyze, store and process the vulnerability information);

gathering, [from at least a subset of the one or more user devices], second information describing access to the one or more resources (Paragraphs 0069, 0071. 0074: computing device includes any type and/or form of video adapter, video card, driver, and/or library to interface, communicate, connect or otherwise use the display devices 124a-124n to communicate with other computing devices via any type and/or

form of gateway or tunneling protocol e.g. Secure Socket Layer (SSL) or Transport Layer Security (TLS), or the Citrix Gateway Protocol manufactured by Citrix Systems wherein group of devices are augment reality devices, for example); and

identifying one or more shadow systems based on a discrepancy between the first information and the second information (Paragraphs 0009, 0057: IDPS monitors data packets which are flowing through the network and compares this information with a pre-determined set of rules which identify known attack patterns. These attack patterns are known as signatures. As the IDPS monitors more signatures, the increased load upon the network and IDPS may increase the amount of time to analyze data packets due to the increase amount of patterns with which the IDPS compares packets).

Giokas does not explicitly states but Di Pietro from the same or similar fields of endeavor teaches a subset of the one or more user devices (Di Pietro,Paragraphs 0043, 0070: LLNs are comprised of anything from a few dozen and up to thousands or even millions of LLN routers, and support point-to-point traffic (between devices inside the LLN), point-to-multipoint traffic (from a central control point to a subset of devices inside the LLN)) wherein previously collected traffic records are mixed with currently monitored traffic, during a validation test. Such a mixing is performed locally by the node hosting the attack detector)

Therefore, it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to utilize user session associated with an original user as taught by Di Pietro in the teachings of Giokas for the advantage of detecting a potential network attack using clustering technique wherein clustering is

used in recommender systems (RS) for grouping objects that are similar in terms of user's selections (Di Pietro, Paragraph 0034).

Regarding claim 2, the combination of Giokas and Di Pietro discloses the method of claim 1 wherein the first information is gathered from one or more identity providers (Giokas, Paragraphs 0088, 0095: the network security tool of the present disclosure can automatically implement a plan of action to address findings of the VA tool wherein the vulnerability assessor 210 can obtain data packets of a protected network, save the data packets to a data file or database, and analyze the data packets to identify stray IP addresses, spoofed packets, unnecessary packet drops, or suspicious packet generation from a single IP address).

Regarding claim 3, the combination of Giokas and Di Pietro discloses the method of claim 1 wherein the first information is gathered from the one or more applications (Giokas, Paragraph 0061: access SaaS resources through smartphone or tablet applications, including, e.g., Salesforce Sales Cloud, or Google Drive app. Clients 102 may also access SaaS resources through the client operating system, including, e.g., Windows file system for DROPBOX.).

Regarding claim 4, the combination of Giokas and Di Pietro discloses the method of claim 1 further comprising generating a polygraph indicating the one or more shadow systems (Giokas Paragraph 0114: signatures can be generated using various techniques including, e.g., statistical packet anomaly detection engine, Hamsa: fast signature generation for zero-day polymorphic worms with provable attack resilience, Polygraph).

Regarding claim 5, the combination of Giokas and Di Pietro discloses the method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems (Paragraphs 0008, 0019: an intrusion detection and prevention system (IDPS) combines these two functionalities, detecting potential attacks and both alerting system administrators and automatically moving to impede the attack.).

Regarding claim 6, the combination of Giokas and Di Pietro discloses the method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems Giokas (Paragraphs 0083, 0010, 0032: a self-tuning network security tool that facilitates automatically identifying a current vulnerability of a computer system or network, and preventing an attack from exploiting the current vulnerability).

Regarding claim 7, the combination of Giokas and Di Pietro discloses the method of claim 1 wherein identifying the one or more shadow systems comprises: identifying one or more accesses described in the first information but not described in the second information (Giokas, Paragraph 0084: the tool can be configured to receive, access, look up, process, analyze or otherwise obtain and utilize information of one or more vulnerabilities lists or registries in one or more formats, standards, or schemes. The tool can be vulnerability scheme independent); and

identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses (Giokas Paragraphs 0011, 0049: network security tool may access or be otherwise communicate with a vulnerability assessment tool (e.g., via a network). The vulnerability assessment tool may detect vulnerabilities in

the network, and feed them to the network security tool. The vulnerability assessment tool may feed the detected vulnerabilities in the form of a vulnerabilities list using a common scheme wherein network connection providea access to Internet to allow the tool to get up to date with the latest exploits and signatures that are crowd-sourced).

Regarding claim 8, the combination of Giokas and Di Pietro discloses the method of claim 1 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices (Giokas Paragraphs 0057, 0069: server 106 may be a file server, application server, web server, proxy server, appliance, network appliance, gateway, gateway server, virtualization server, deployment server, SSL VPN server, or firewall … interacting with group of electronic devices including augment reality devices).

Regarding claim 9; Claim 9 is similar in scope to claim 1, and is therefore rejected under similar rationale.

Regarding claim 10; Claim 10 is similar in scope to claim 2, and is therefore rejected under similar rationale.

Regarding claim 11; Claim 11 is similar in scope to claim 3, and is therefore rejected under similar rationale.

Regarding claim 12; Claim 12 is similar in scope to claim 4, and is therefore rejected under similar rationale.

Regarding claim 13; Claim 13 is similar in scope to claim 5, and is therefore rejected under similar rationale.

Regarding claim 14; Claim 14 is similar in scope to claim 6, and is therefore rejected under similar rationale.

Regarding claim 15; Claim 15 is similar in scope to claim 7, and is therefore rejected under similar rationale.

Regarding claim 16; Claim 16 is similar in scope to claim 8, and is therefore rejected under similar rationale.

Regarding claim 17; Claim 17 is similar in scope to claim 1, and is therefore rejected under similar rationale.

Regarding claim 18; Claim 18 is similar in scope to claim 2, and is therefore rejected under similar rationale.

Regarding claim 19; Claim 19 is similar in scope to claim 3, and is therefore rejected under similar rationale.

Regarding claim 20; Claim 20 is similar in scope to claim 4, and is therefore rejected under similar rationale.

Examiner Notes

16. The Examiner notes that incorporating the combined limitations of dependent claims 4, 6, and 7 **OR** dependent claims 6, 7, and 8 into independent claim 1 would better clarify the subject matter/embodiment of claimed invention. Similarly, amending independent claims 9 and 17 with aforesaid claim limitations would help advance the prosecution as it would clarify the claimed invention.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Koottayi (US 20180288063 A1) discloses techniques for managing user access to resources in an enterprise environment wherein managing access to a target resource based on a threat perception of a user that is calculated using a rule or policy based risk for the user and a behavior based risk for the user.

- Miltonberger (US 10115111 B2) discloses predicting expected behavior of a user in an account and automatically generate a causal model corresponding to a user.

18. In an effort to advance compact prosecution, with respect to any amendments to the claimed invention, the applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Moreover with respect to advancing compact prosecution, if the applicant intends to make numerous amendments, the examiner respectfully requests that applicant submit a clean copy of the claims in addition to the marked up copy of the claims in order to expedite the examination process by allowing for accurate optical character recognition (OCR) of the claims.

The prior art made of record and not relied upon, if any, is considered pertinent to applicant's disclosure and would be listed under PTO-Form 892.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Yin-Chen Shaw can be reached on 571-272-8878. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MAHFUZUR RAHMAN/
Primary Examiner, Art Unit 2498

Notice of References Cited	Application/Control No. 17/858,866	Applicant(s)/Patent Under Reexamination KAPOOR et al.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20190207955-A1	07-2019	EL-MOUSSA; Fadi	H04L63/1408	1/1
*	B	US-20190012457-A1	01-2019	EL-MOUSSA; Fadi	G06F21/56	1/1
*	C	US-20180375882-A1	12-2018	KALLOS; George	G06F21/566	1/1
*	D	US-20180288063-A1	10-2018	Koottayi; Vipin	H04L63/1416	1/1
*	E	US-20100094767-A1	04-2010	Miltonberger; Tom	G06Q10/10	705/348
*	F	US-20150033340-A1	2015-01-29	Giokas; Ioannis	H04L63/1433	726/23
*	G	US-20160103883-A1	2016-04-14	Ramani; Arun	G06F16/24573	707/725
*	H	US-20160028753-A1	2016-01-28	Di Pietro; Andrea	G06F21/577	726/23
*	I	US-20170019487-A1	2017-01-19	Maheshwari; Sonal	H04L67/51	1/1
*	J	US-10115111-B2	2018-10-30	Miltonberger; Tom	G06Q50/265	1/1
*	K	US-8443442-B2	2013-05-14	Wang; Xinran	H04L63/1441	709/233
*	L	US-20080022405-A1	2008-01-24	Wang; Xinran	H04L63/1441	726/23
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00191

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2498

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant			☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		**DATE**								
Final	Original	01/27/2024								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00192

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2498

CPC - Searched*		
Symbol	**Date**	**Examiner**
(H04L63/1425 OR G06F9/455 OR G06F9/545 OR G06F16/9024 OR G06F16/9038 OR G06F16/9535 OR G06F16/9537 OR G06F21/57 OR H04L43/045 OR H04L43/06 OR H04L63/10 OR H04L67/306 OR H04L67/535 OR G06F16/2456).cpc.	01/27/2024	MR

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Search History Including CPC/Inventor/Assignee/NPL/Keywords Search Attached	01/27/2024	MR
Inventor/Assignee Search	01/27/2024	MR

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00193

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/858,866	KAPOOR et al.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2498

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
(H04L63/1425	(H04L63	01/27/2024	MR
	((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4) and edge with (connect$3 or link$3 or communicat$3) and (alert$3 or alarm$3). clm.	01/27/2024	MR

/MAHFUZUR RAHMAN/ Primary Examiner, Art Unit 2498	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00194

Bibliographic Data

Application No: 17/858,866

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /MAHFUZUR RAHMAN/ (Examiner's Signature) | MR (Initials)

Title: Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
07/06/2022	726	2498	L0040B3CIP6C1
RULE			

APPLICANTS

LACEWORK, INC., SAN JOSE, CA, UNITED STATES

INVENTORS

VIKRAM KAPOOR, CUPERTINO, CA, UNITED STATES

HARISH KUMAR BHARAT SINGH, PLEASANTON, CA, UNITED STATES

WEIFEI ZENG, SUNNYVALE, CA, UNITED STATES

VIMALKUMAR JEYAKUMAR, LOS ALTOS, CA, UNITED STATES

THERON TOCK, MOUNTAIN VIEW, CA, UNITED STATES

YING XIE, CUPERTINO, CA, UNITED STATES

YIJOU CHEN, CUPERTINO, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 17836813 06/09/2022ABN

17836813 has PRO of 63240818 09/03/2021

This application has PRO of 63240818 09/03/2021

17836813 is a CIP of 17196887 03/09/2021 PAT 11689553

17196887 is a CON of 16459207 07/01/2019 PAT 10986114

16459207 is a CON of 16134821 09/18/2018 PAT 10419469

16134821 has PRO of 62650971 03/30/2018

16134821 has PRO of 62590986 11/27/2017

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

07/15/2022

STATE OR COUNTRY

UNITED STATES

ADDRESS

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681
UNITED STATES

FILING FEE RECEIVED

$2,240

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	
Examiner Name	
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10033611	B1	2018-07-24	Linkous et al.	
	2	10115111	B2	2018-10-30	Miltonberger	
	3	10127273	B2	2018-11-13	Dickey	
	4	10142357	B1	2018-11-27	Tamersoy et al.	
	5	10205736	B2	2019-02-12	Rieke et al.	
	6	10339309	B1	2019-07-02	Kling et al.	
	7	10389742	B2	2019-08-20	Reddy et al.	
	8	10594718	B1	2020-03-17	Deaguero et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	9	10708082	B1	2020-07-07	Bakiaraj et al.	
	10	10735329	B2	2020-08-04	WANG et al.	
	11	11431735	B2	2022-08-30	SHUA	
	12	11489863	B1	2022-11-01	Shua et al.	
	13	5584024	A	1996-12-10	Shwartz	
	14	5806062	A	1998-09-08	Chen et al.	
	15	8103906	B1	2012-01-24	Alibakhsh et al.	
	16	8122122	B1	2012-02-21	Clingenpeel et al.	
	17	8443442	B2	2013-05-14	Wang et al.	
	18	8671453	B2	2014-03-11	Underwood et al.	
	19	8862524	B2	2014-10-14	Zheng et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	20	9021583	B2	2015-04-28	Wittenstein et al.	
	21	9037273	B2	2015-05-19	Mikkelsen	
	22	9332020	B2	2016-05-03	Thomas et al.	
	23	9515999	B2	2016-12-06	Ylonen	
	24	9516053	B1	2016-12-06	Muddu et al.	
	25	9558265	B1	2017-01-31	Tacchi et al.	
	26	9596253	B2	2017-03-14	Chauhan et al.	
	27	9654503	B1	2017-05-16	Kowalyshyn	
	28	9734040	B2	2017-08-15	Gounares	
	29	9749339	B2	2017-08-29	Kadambe et al.	
	30	9853968	B2	2017-12-26	Shen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	31	9953014	B1	2018-04-24	Reshadi et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020184225	A1	2002-12-05	Ghukasyan	
	2	20030037136	A1	2003-02-20	Labovitz et al.	
	3	20030179227	A1	2003-09-25	Ahmad et al.	
	4	20040015470	A1	2004-01-22	Smith et al.	
	5	20050102284	A1	2005-05-12	Srinivasan et al.	
	6	20050188222	A1	2005-08-25	Motsinger et al.	
	7	20060085437	A1	2006-04-20	Brodhun et al.	
	8	20060259470	A1	2006-11-16	Chandrasekharan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	9	20060288415	A1	2006-12-21	Wong	
	10	20070050497	A1	2007-03-01	Haley et al.	
	11	20070118909	A1	2007-05-24	Hertzog et al.	
	12	20080148180	A1	2008-06-19	Liu et al.	
	13	20080151893	A1	2008-06-26	Nordmark et al.	
	14	20090019160	A1	2009-01-15	Schuler	
	15	20090228474	A1	2009-09-10	Chiu et al.	
	16	20090271504	A1	2009-10-29	Ginter et al.	
	17	20100094767	A1	2010-04-15	Miltonberger	
	18	20100114931	A1	2010-05-06	Xie et al.	
	19	20100172261	A1	2010-07-08	Shinbo et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	20	20100274785	A1	2010-10-28	Procopiuc et al.	
	21	20110055138	A1	2011-03-03	Khanduja et al.	
	22	20120005243	A1	2012-01-05	Merwe et al.	
	23	20120317151	A1	2012-12-13	Ruf et al.	
	24	20120323956	A1	2012-12-20	Dumitru et al.	
	25	20130304915	A1	2013-11-14	KAWAI	
	26	20130305357	A1	2013-11-14	Ayyagari et al.	
	27	20140115001	A1	2014-04-24	Arroyo et al.	
	28	20140115011	A1	2014-04-24	Buerner et al.	
	29	20140208191	A1	2014-07-24	Zaric et al.	
	30	20140245443	A1	2014-08-28	Chakraborty	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	31	20140280068	A1	2014-09-18	DHOOPAR et al.	
	32	20140359558	A1	2014-12-04	Chamberlain	
	33	20150135312	A1	2015-05-14	Wada et al.	
	34	20150188751	A1	2015-07-02	Vasseur et al.	
	35	20150341379	A1	2015-11-26	Lefebvre et al.	
	36	20150356144	A1	2015-12-10	Chawla et al.	
	37	20160078365	A1	2016-03-17	Baumard	
	38	20160080404	A1	2016-03-17	KOHOUT et al.	
	39	20160110434	A1	2016-04-21	Kakaraddi et al.	
	40	20160149937	A1	2016-05-26	KATMOR et al.	
	41	20160205125	A1	2016-07-14	Kim et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	42	20160218911	A1	2016-07-28	WESSELS et al.	
	43	20160359592	A1	2016-12-08	Kulshreshtha et al.	
	44	20160359872	A1	2016-12-08	Yadav et al.	
	45	20170118240	A1	2017-04-27	Reddy et al.	
	46	20170134240	A1	2017-05-11	Hévizi et al.	
	47	20170147646	A1	2017-05-25	LEE et al.	
	48	20170163666	A1	2017-06-08	Venkatramani et al.	
	49	20170251013	A1	2017-08-31	Kirti et al.	
	50	20170272344	A1	2017-09-21	Tang et al.	
	51	20170279827	A1	2017-09-28	Savalle et al.	
	52	20170288974	A1	2017-10-05	Yoshihira et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	53	20170359361	A1	2017-12-14	Modani et al.	
	54	20170366492	A1	2017-12-21	Ho et al.	
	55	20180020015	A1	2018-01-18	Munro et al.	
	56	20180034840	A1	2018-02-01	Marquardt et al.	
	57	20180063178	A1	2018-03-01	Jadhav et al.	
	58	20180103052	A1	2018-04-12	Choudhury et al.	
	59	20180115578	A1	2018-04-26	Subbarayan et al.	
	60	20180137858	A1	2018-05-17	Saxena et al.	
	61	20180173789	A1	2018-06-21	Llagostera et al.	
	62	20180174062	A1	2018-06-21	Simo et al.	
	63	20180181750	A1	2018-06-28	Lamothe-Brassard	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	64	20180248901	A1	2018-08-30	Rieke	
	65	20180268078	A1	2018-09-20	Gianetto et al.	
	66	20180288063	A1	2018-10-04	Koottayi et al.	
	67	20180329958	A1	2018-11-15	Choudhury et al.	
	68	20180336353	A1	2018-11-22	Manadhata et al.	
	69	20180357422	A1	2018-12-13	Telang et al.	
	70	20180367548	A1	2018-12-20	Stokes III et al.	
	71	20190028327	A1	2019-01-24	SILVA et al.	
	72	20190109870	A1	2019-04-11	BEDHAPUDI et al.	
	73	20190132224	A1	2019-05-02	VERMA et al.	
	74	20190222597	A1	2019-07-18	Crabtree et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	75	20190259033	A1	2019-08-22	Reddy et al.	
	76	20190339965	A1	2019-11-07	Garvey et al.	
	77	20190349305	A1	2019-11-14	WANG et al.	
	78	20190378050	A1	2019-12-12	Edkin et al.	
	79	20200076685	A1	2020-03-05	Vaidya et al.	
	80	20200192690	A1	2020-06-18	Gupta et al.	
	81	20200252376	A1	2020-08-06	Feng et al.	
	82	20200272740	A1	2020-08-27	Obee et al.	
	83	20200278892	A1	2020-09-03	Nainar et al.	
	84	20200280592	A1	2020-09-03	Ithal et al.	
	85	20200311644	A1	2020-10-01	WILLARD III et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	86	20200403860	A1	2020-12-24	Lewis et al.	
	87	20210329019	A1	2021-10-21	SHUA	
	88	20210336976	A1	2021-10-28	SHUA	
	89	20210377287	A1	2021-12-02	SHUA	
	90	20220342690	A1	2022-10-27	Shua	
	91	20220345480	A1	2022-10-27	Shua	
	92	20220345481	A1	2022-10-27	Shua	
	93	20220345483	A1	2022-10-27	Shua	
	94	20220350931	A1	2022-11-03	Shua	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	AI-YASEEN et al., "Real-Time Intrusion Detection System Using Multi-Agent System", IAENG International Journal of Computer Science, volume 43, no. 1, February 2016, pp. 80-90, International Association of Engineers (IAENG), Hong Kong.	
	2	AKOGLU et al., "Graph-based Anomaly Detection and Description: A Survey", April 28, 2014.	
	3	AMIDON et al., "Program Fracture and Recombination for Efficient Automatic Code Reuse", In 2015 IEEE High Performance Extreme Computing Conference (HPEC), September 2015, pp. 1-6, IEEE.org (online), DOI: 10.1109/HPEC.2015.7396314.	
	4	AMMAR et al., "Query Optimization Techniques in Graph Databases", International Journal of Database Management Systems (IIDMS), Vol. 8, No. 4, August 2016, pages 1-14 (Year: 2016).	
	5	BALASUBRAMANIYAN et al., "An Architecture For Intrusion Detection Using Autonomous Agents", In Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217), 19 pages, June 1998, IEEE, DOI: 10.1109/CSAC.1998.738563.	
	6	BEUTEL et al., "User Behavior Modeling with Large-Scale Graph Analysis", Computer Science Department, Carnegie Mellon University, May 2016.	
	7	BUGIEL et al., "Towards Taming Privilege-Escalation Attacks on Android", In NOSS (Vol. 17, p. 19), 2012, February.	
	8	CHANG et al., "Reality Bites - Progressive Querying and Result Visualization in Logical and VR Spaces", Proceedings of 1994 IEEE Symposium on Visual Languages, pp. 100-109, October 1994, IEEE, DOI: 10.1109NL.1994.363635.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	9	CHESSON, "Communication And Control In A Cluster Network", ACM '74: Proceedings of the 1974 annual ACM conference - Volume 2, January 1974, pp 509-514, http://doi.org/10.1145/1408839 (Year 1974).	
	10	CROSBIE et al., "Defending a Computer System using Autonomous Agents", docs.lib.purdue.edu (online), March 1995, 11 pages.	
	11	HAUTAMAKI et al., "Outlier Detection Using k-Nearest Neighbour Graph", Proceedings of the 17th International Conference on Pattern Recognition (ICPR 2004), Vol. 3, August 2004, IEEE, DOI: 10.1109/ICPR.2004.1334558.	
	12	HOOPER et al., "Medusa: a simple tool for interaction graph analysis", Bioinformatics, Vol. 21 no. 24, September 2005, pages 4432-4433, Oxford University Press (online), URL: https://academic.oup.com/bioinformatics/article/21/24/4432/179694.	
	13	KOUTRA et al., "Exploring and Making Sense of Large Graphs", Computer Science Department, Carnegie Mellon University, August 2015.	
	14	LEOPOLD et al., "A Visual Query System for the Specification and Scientific Analysis off Continual Queries", Proceedings, IEEE Symposia on Human-Centric Computing Languages and Environments (Cat. No.01TH8587), September 2001, pp. 203-211, IEEE, doi: 10.1109/HCC.2001.995260.	
	15	LIAO et al., "Visualizing Graph Dynamics And Similarity For Enterprise Network Security And Management", VizSec '10: Proceedings of the Seventh International Symposium on Visualization for Cyber Security, September 2010, pp. 34-45, URL: https://doi.org/10.1145/1850795.1850799.	
	16	LONG et al., "Automatic Input Rectification", 2012 34th International Conference on Software Engineering (ICSE), June 2012, pp. 80-90, IEEE.org (online), DOI: 10.1109/ICSE.2012.6227204.	
	17	MATEESCU et al., "Join-Graph Propagation Algorithms", Journal of Artificial Intelligence Research, vol. 37, March 2010, pages 279-328, AI Access Foundation, Inc. (online), URL: https://doi.org/10.1613/jair.2842.	
	18	MORIANO et al., "Insider Threat Event Detection in User-System Interactions", MIST '17: Proceedings of the 2017 International Workshop on Managing Insider Security Threats, October 2017, pp 1-12, ACM Digital Library (online), URL: https://doi.Jrg/10.1145/3139923.3139928.	
	19	PERKINS et al., "Automatically Patching Errors in Deployed Software", Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles, October 2009, pp 82-102, acm.org (online), URL: https://doi.org/10.1145/1629575.1629585.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	20	RANSHOUS et al., "Anomaly detection in dynamic networks: a survey", WIREs Computational Statistics, volume 7, May/June 2015, pp. 223-247, Wiley Periodicals, Inc, United States.	
	21	RINARD, "Living In The Comfort Zone", ACM SIGPLAN Notices, Volume 42, Issue 10, October 2007, pp. 611-622, acm.org (online), URL: https://doi.org/10.1145/1297105.1297072.	
	22	RINARD, "Manipulating Program Functionality to Eliminate Security Vulnerabilities", In Moving Target Defense, January 2011, pp. 109-115. Springer, New York, NY.	
	23	SAMUEL et al., "Let's Parse to Prevent Pwnage", Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET'12), April 2012, 3 pages, acm.org (online), URL: https://www.usenix.org/conference/leet12/workshop-program/presentation/samuel.	
	24	SHEN et al., "Active Learning for Inference and Regeneration of Applications that Access Databases", ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 42, Issue 4, Article 18, January 2021, pp. 1-119, acm.org (online), URL: https://doi.org/10.1145/3430952.	
	25	TAMASSIA et al., "Graph Drawing for Security Visualization", In: Graph Drawing (GD 2008), Lecture Notes in Computer Science, vol 5417, Springer, Berlin, Heidelberg (online), URL: https://doi.org/10.1007/978-3-642-00219-9_2.	
	26	VAAS et al., "Detecting disguised processes using Application-Behavior Profiling", In 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1-6, June 2017, IEEE, DOI: 10.1109/THS.2017.7943508.	
	27	VASILAKIS et al., "Supply-Chain Vulnerability Elimination via Active Learning and Regeneration", Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, November 2021, pp. 1755-1770, acm.org (online), URL: https://doi.org/10.1145/3460120.3484736.	
	28	YU et al., "Recommending Join Queries Based on Path Frequency", 2015 12th Web Information System and Application Conference (WISA), September 2015, pp. 21-26, IEEE, DOI: 10.1109/WISA.2015.52.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/MAHFUZUR RAHMAN/	Date Considered	01/27/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-01-06
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	OPAP
Examiner Name	DOCKET CENTRAL
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10003605	B2	2018-06-19	Muddu et al.	
	2	10116670	B2	2018-10-30	Muddu et al.	
	3	10148677	B2	2018-12-04	Muddu et al.	
	4	10158652	B2	2018-12-18	Muddu et al.	
	5	10205735	B2	2019-02-12	Apostolopoulos	
	6	10243970	B2	2019-03-26	Muddu et al.	
	7	10254848	B2	2019-04-09	Winternitz et al.	
	8	10338895	B2	2019-07-02	Zhang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	9	10389738	B2	2019-08-20	Muddu et al.	
	10	10419463	B2	2019-09-17	Muddu et al.	
	11	10419465	B2	2019-09-17	Muddu et al.	
	12	10432639	B1	2019-10-01	Bebee et al.	
	13	10454889	B2	2019-10-22	HUANG	
	14	10459979	B2	2019-10-29	Piechowicz et al.	
	15	10462169	B2	2019-10-29	DURAIRAJ et al.	
	16	10491705	B2	2019-11-26	Oetting et al.	
	17	10496468	B2	2019-12-03	Gefen et al.	
	18	10534633	B2	2020-01-14	Hilemon et al.	
	19	10666668	B2	2020-05-26	Muddu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	20	10673880	B1	2020-06-02	Pratt et al.	
	21	10693900	B2	2020-06-23	Zadeh et al.	
	22	10698954	B2	2020-06-30	Piechowicz et al.	
	23	10756982	B2	2020-08-25	Bai et al.	
	24	10771488	B2	2020-09-08	Verma et al.	
	25	10776191	B2	2020-09-15	Zheng et al.	
	26	10788570	B2	2020-09-29	Wilson	
	27	11036716	B2	2021-06-15	Griffith et al.	
	28	11044264	B2	2021-06-22	DURAIRAJ et al.	
	29	11082289	B2	2021-08-03	Dang et al.	
	30	11120343	B2	2021-09-14	Das et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	31	11126533	B2	2021-09-21	Knowles et al.	
	32	11194849	B2	2021-12-07	Lassoued et al.	
	33	11212299	B2	2021-12-28	Gamble et al.	
	34	11258807	B2	2022-02-22	Muddu et al.	
	35	11281519	B2	2022-03-22	Krishnaswamy et al.	
	36	11314789	B2	2022-04-26	Goldfarb	
	37	11411966	B2	2022-08-09	Muddu et al.	
	38	11463464	B2	2022-10-04	Zadeh et al.	
	39	11494787	B2	2022-11-08	Erickson et al.	
	40	11544138	B2	2023-01-03	Kapish et al.	
	41	11606272	B1	2023-03-14	Popelka et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	42	11636090	B2	2023-04-25	Li et al.	
	43	11640388	B2	2023-05-02	Yang et al.	
	44	11647034	B2	2023-05-09	Levin et al.	
	45	11658990	B2	2023-05-23	Shapoury	
	46	11669571	B2	2023-06-06	Binkley et al.	
	47	11693958	B1	2023-07-04	Steiman	
	48	11722554	B2	2023-08-08	Keren et al.	
	49	11734351	B2	2023-08-22	Binkley et al.	
	50	11734419	B1	2023-08-22	Mackle	
	51	11748473	B2	2023-09-05	Araujo et al.	
	52	11755576	B1	2023-09-12	Jiang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	53	11755602	B2	2023-09-12	Smith Shawn et al.	
	54	11769098	B2	2023-09-26	Adinarayan et al.	
	55	11770387	B1	2023-09-26	Shivamoggi et al.	
	56	7233333	B2	2007-06-19	Lomask	
	57	7478246	B2	2009-01-13	Arndt et al.	
	58	7484091	B2	2009-01-27	Bade et al.	
	59	7526501	B2	2009-04-28	Albahari et al.	
	60	7707411	B2	2010-04-27	Bade et al.	
	61	7739211	B2	2010-06-15	Coffman et al.	
	62	7747559	B2	2010-06-29	Leitner et al.	
	63	7765431	B2	2010-07-27	Agha et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	64	8050907	B2	2011-11-01	Baisley et al.	
	65	8086852	B2	2011-12-27	Bade et al.	
	66	8140977	B2	2012-03-20	Kriss et al.	
	67	8160999	B2	2012-04-17	Jin et al.	
	68	8209204	B2	2012-06-26	Adler et al.	
	69	8301660	B2	2012-10-30	Yalamanchi	
	70	8490055	B2	2013-07-16	Basak	
	71	9043764	B2	2015-05-26	Ranganathan et al.	
	72	9053437	B2	2015-06-09	Adler et al.	
	73	9064210	B1	2015-06-23	Hart	
	74	9075618	B2	2015-07-07	Winternitz et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	75	9110873	B2	2015-08-18	Woodall et al.	
	76	9159024	B2	2015-10-13	Bhanot et al.	
	77	9189623	B1	2015-11-17	Lin et al.	
	78	9589069	B2	2017-03-07	Yang et al.	
	79	9591010	B1	2017-03-07	Muddu et al.	
	80	9600915	B2	2017-03-21	Winternitz et al.	
	81	9667641	B2	2017-05-30	Muddu et al.	
	82	9679243	B2	2017-06-13	Zou et al.	
	83	9699205	B2	2017-07-04	Muddu et al.	
	84	9710332	B1	2017-07-18	Fan et al.	
	85	9720703	B2	2017-08-01	Reick et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	86	9720704	B2	2017-08-01	Reick et al.	
	87	9727441	B2	2017-08-08	Agarwal et al.	
	88	9727604	B2	2017-08-08	Jin et al.	
	89	9813435	B2	2017-11-07	Muddu et al.	
	90	9824473	B2	2017-11-21	Winternitz et al.	
	91	9838410	B2	2017-12-05	Muddu et al.	
	92	9843837	B2	2017-12-12	Gopalan	
	93	9864672	B2	2018-01-09	Seto et al.	
	94	9985827	B2	2018-05-29	Li et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	1	20040225929	A1	2007-01-23	Agha et al.	
	2	20050246521	A1	2009-01-27	Bade et al.	
	3	20060025987	A1	2006-02-02	Baisley et al.	
	4	20060026419	A1	2009-01-13	Arndt et al.	
	5	20060109271	A1	2007-06-19	Lomask	
	6	20070214111	A1	2017-08-08	Jin et al.	
	7	20070282916	A1	2007-12-06	Albahari et al.	
	8	20080109730	A1	2008-05-08	Coffman et al.	
	9	20080147707	A1	2012-04-17	Jin et al.	
	10	20090006843	A1	2011-12-27	Bade et al.	
	11	20090007010	A1	2009-01-01	Kriss et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	12	20090063857	A1	2010-04-27	Bade et al.	
	13	20090307651	A1	2009-12-10	Senthil et al.	
	14	20090327328	A1	2015-08-18	Woodall et al.	
	15	20100042823	A1	2011-08-09	Arndt et al.	
	16	20110119100	A1	2011-05-19	Ruhl et al.	
	17	20110154287	A1	2011-06-23	Mukkamala et al.	
	18	20120143898	A1	2012-06-07	Bruno et al.	
	19	20120159333	A1	2012-06-21	Mital et al.	
	20	20130024412	A1	2013-01-24	Gong et al.	
	21	20130151453	A1	2013-06-13	Bhanot et al.	
	22	20140067750	A1	2015-05-26	Ranganathan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	23	20140125672	A1	2015-07-07	Winternitz et al.	
	24	20140279779	A1	2017-06-13	Zou et al.	
	25	20150310649	A1	2017-03-21	Winternitz et al.	
	26	20160120070	A1	2016-04-28	Myrah et al.	
	27	20160357521	A1	2019-07-02	Zhang et al.	
	28	20170063888	A1	2017-03-02	Muddu et al.	
	29	20170063903	A1	2017-03-02	Muddu et al.	
	30	20170063905	A1	2017-03-02	Muddu et al.	
	31	20170063909	A1	2017-03-02	Muddu et al.	
	32	20170063911	A1	2017-03-02	Muddu et al.	
	33	20170070594	A1	2019-11-26	Oetting et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	34	20170102961	A1	2020-01-14	Hilemon et al.	
	35	20170118099	A1	2017-04-27	HUANG	
	36	20170142140	A1	2017-05-18	Muddu et al.	
	37	20170148197	A1	2017-05-25	Winternitz et al.	
	38	20170155570	A1	2017-06-01	Maheshwari et al.	
	39	20170155672	A1	2017-06-01	Muthukrishnan et al.	
	40	20170223036	A1	2017-08-03	Muddu et al.	
	41	20170330096	A1	2017-11-16	Gupta et al.	
	42	20170346683	A1	2018-05-29	Li et al.	
	43	20180004835	A1	2018-01-04	Piechowicz et al.	
	44	20180004859	A1	2020-06-30	Piechowicz et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	45	20180007145	A1	2019-10-29	Piechowicz et al.	
	46	20180089132	A1	2018-03-29	Atta et al.	
	47	20180191781	A1	2018-07-05	Palani et al.	
	48	20180211425	A1	2018-07-26	Winternitz et al.	
	49	20180219888	A1	2018-08-02	Apostolopoulos	
	50	20180219897	A1	2018-08-02	Muddu et al.	
	51	20180359162	A1	2018-12-13	Savov et al.	
	52	20190042950	A1	2019-02-07	Lin et al.	
	53	20190050445	A1	2021-06-15	Griffith et al.	
	54	20190058626	A1	2019-02-21	Knowles et al.	
	55	20190075126	A1	2019-03-07	Muddu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	56	20190101622	A1	2019-04-04	Wilson	
	57	20190163555	A1	2019-05-30	Zheng et al.	
	58	20190227860	A1	2019-12-03	Gefen et al.	
	59	20190312898	A1	2019-10-10	Verma et al.	
	60	20190327251	A1	2019-10-24	Muddu et al.	
	61	20190342307	A1	2019-11-07	Gamble et al.	
	62	20190354554	A1	2019-11-21	Piechowicz et al.	
	63	20190356555	A1	2020-08-25	Bai et al.	
	64	20200014718	A1	2020-01-09	DURAIRAJ et al.	
	65	20200021607	A1	2020-01-16	Muddu et al.	
	66	20200175361	A1	2020-06-04	Che et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	67	20200287923	A1	2020-09-10	Raghavendra et al.	
	68	20200320106	A1	2022-04-26	Goldfarb	
	69	20200334293	A1	2020-10-22	Piechowicz et al.	
	70	20200351151	A1	2020-11-05	Dang et al.	
	71	20200412752	A1	2020-12-31	Shapoury	
	72	20210019209	A1	2021-01-21	Krishnaswamy et al.	
	73	20210232420	A1	2021-07-29	Dhruvakumar et al.	
	74	20210286798	A1	2021-09-16	Li et al.	
	75	20210294798	A1	2021-09-23	Binkley et al.	
	76	20210406917	A1	2021-12-30	Erickson et al.	
	77	20220004718	A1	2022-01-06	Quamar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	78	20220050840	A1	2022-02-17	Parravicini et al.	
	79	20220058193	A1	2023-09-12	Smith Shawn et al.	
	80	20220067186	A1	2022-03-03	Thakur et al.	
	81	20220086179	A1	2023-05-09	Levin et al.	
	82	20220092481	A1	2022-03-24	Neithalath et al.	
	83	20220121741	A1	2023-09-05	Araujo et al.	
	84	20220124108	A1	2022-04-21	Gamble et al.	
	85	20220129803	A1	2022-04-28	Bikumala et al.	
	86	20220191226	A1	2022-06-16	Chan et al.	
	87	20220327119	A1	2022-10-13	Gasper et al.	
	88	20220350789	A1	2023-05-02	Yang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	89	20220374800	A1	2023-09-26	Adinarayan et al.	
	90	20220376970	A1	2022-11-24	Chawathe et al.	
	91	20220382611	A1	2023-01-03	Kapish et al.	
	92	20220394082	A1	2022-12-08	Keren et al.	
	93	20220414072	A1	2022-12-29	Tandon et al.	
	94	20220414105	A1	2022-12-29	Umay et al.	
	95	20230025252	A1	2023-01-26	Erickson et al.	
	96	20230039566	A1	2023-02-09	Ghag et al.	
	97	20230052827	A1	2023-02-16	Araujo et al.	
	98	20230088960	A1	2023-03-23	Popelka et al.	
	99	20230096930	A1	2023-03-30	Dasdan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	100	20230101773	A1	2023-03-30	Katahanas et al.	
	101	20230138371	A1	2023-05-04	Bandukwala et al.	
	102	20230244523	A1	2023-08-03	Gorantla et al.	
	103	20230251960	A1	2023-08-10	Sharma et al.	
	104	20230275909	A1	2023-08-31	Shivamoggi et al.	
	105	20230291755	A1	2023-09-14	Siebel et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/MAHFUZUR RAHMAN/	Date Considered	01/27/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-12-07
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L703	0	"17858949"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/13 11:49 PM
L704	0	"17858949"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/13 11:50 PM
L705	2	"17836558"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/13 11:51 PM
L706	0	"17858949"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/13 11:51 PM
L707	0	"17858949"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/13 11:52 PM
L708	2	"17836558"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/13 11:53 PM
L709	53	train$3 WITH model NEAR5 workflow AND (HISTORY OR RECORD LOG) near8 (deviat$3 normal abnormal intrusion)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/14 12:10 AM
L710	8	709 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/14 12:11 AM
L711	2	"17836558"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:58 PM
L712	2	"17836558"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/01/27 08:58 PM

			IBM_TDB)				
L713	1	365 AND device WITH (behavior$2 occurrence event interest activity abnormal trigger$3 potential threat condition environment$2 fire malicious)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L714	1	365 AND device WITH (behavior$2 occurrence event interest activity abnormal trigger$3 potential threat condition environment$2 fire malicious)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L715	1	365 AND device WITH (behavior$2 occurrence event interest activity abnormal trigger$3 potential threat condition environment$2 fire malicious)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L716	1	365 AND device WITH (behavior$2 occurrence event interest activity abnormal trigger$3 potential threat condition environment$2 fire malicious)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L717	1970	graph$3 SAME (visual visualiz$5) near10 (personal individual$5 specific) AND (alert$3 alarm$3) AND device WITH location	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L718	1970	graph$3 SAME (visual visualiz$5) near10 (personal individual$5 specific) AND (alert$3 alarm$3) AND device WITH location	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L719	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L720	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM

L721	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L722	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L723	57	((("Chen") near3 ("Yijou"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/01/27 08:59 PM
L724	57	((("Chen") near3 ("Yijou"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/01/27 08:59 PM
L725	2	L145 and (privilege or permission or restrict$3 or control$3 or chang$3 or modifying or modification) with (graph or model)	(US-PGPUB)	OR	ON	ON	2024/01/27 08:59 PM
L726	1	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L727	1	513 AND second WITH factor	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L728	1	513 AND second WITH factor	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L729	14	"17196887"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L730	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L731	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L732	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/01/27 08:59 PM

			IBM_TDB)				
L733	134	graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND software near4 service	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L734	134	graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND software near4 service	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L735	27	588 AND link$3 WITH (visual visualiz$5) AND (software near4 service OR SaaS) AND type WITH (target destination)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L737	1	L135 and (previlege or permission or permit$4 or authoriz$5) with (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L738	2	L252 and graph with model	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L740	55	L205 and (previlege or permission or permit$4 or authoriz$5) same (model or table database rule polic$3)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L741	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L742	1	511 AND (algorithm model module) near8 (workflow)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L743	362	L264 and ((@ad or @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L744	70	"20160359872"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L745	70	"20160359872"	(US-PGPUB; USPAT; USOCR; FIT (CN, FR,	OR	ON	ON	2024/01/27 08:59 PM

			WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L746	68	"20160359872"	(USPAT)	OR	ON	ON	2024/01/27 08:59 PM
L747	1	(polygraph OR (health detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph))) WITH (destination OR target OR end OR recipient OR receiv$3 OR remot$2 server) WITH (brow$4 website program application remote) near10 (normal abnormal activit$3 risk malicious$4 OR anomal$3 OR threat OR risk intrusion OR threat vulnerabilities OR vulnerab$5 OR exploit unauthoriz$5 deviat$3) AND SaaS AND scor$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L748	1	(polygraph OR (health detect$3 pulse) near4 ((network near4 graph) OR (logic$2 near4 graph))) WITH (destination OR target OR end OR recipient OR receiv$3 OR remot$2 server) WITH (brow$4 website program application remote) near10 (normal abnormal activit$3 risk malicious$4 OR anomal$3 OR threat OR risk intrusion OR threat vulnerabilities OR vulnerab$5 OR exploit unauthoriz$5 deviat$3) AND SaaS AND scor$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 08:59 PM
L749	2	log WITH logical near4 graph SAME anomal$3	(US-PGPUB)	OR	ON	ON	2024/01/27 08:59 PM
L750	45	((US-20160103883-A1 OR US-20190222597-A1 OR US-20090031423-A1 OR US-20160143570-A1 OR US-20080120721-A1 OR US-20150033340-A1 OR US-20100094767-A1	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:17 PM

		OR US-20130073387-A1 OR US-20140020102-A1 OR US-20170019487-A1 OR US-20130227691-A1 OR US-20160359872-A1 OR US-20180288063-A1 OR US-20160028753-A1 OR US-20180084012-A1 OR US-20140282586-A1 OR US-20160034305-A1 OR US-20140359558-A1 OR US-20190207955-A1 OR US-20190012457-A1 OR US-20180375882-A1 OR US-20140330960-A1 OR US-20160241705-A1 OR US-20160135751-A1 OR US-20140280952-A1 OR US-20150309813-A1 OR US-20100076952-A1 OR US-20150101050-A1 OR US-20220400130-A1).did. AND PGPB.dbnm.) OR ((US-10115111-B2 OR US-8880588-B2 OR US-9210183-B2 OR US-9519782-B2 OR US-10142353-B2 OR US-9825989-B1 OR US-9378044-B1 OR US-9021583-B2 OR US-8443442-B2 OR US-10419469-B1 OR US-9407754-B1 OR US-9071638-B1 OR US-4744029-A OR US-10986114-B1 OR US-11689553-B1).did. AND USPT.dbnm.) OR ((US-20110119085-A1).did. AND DWPI.dbnm.)					
L751	6	750 AND shadow	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:17 PM
L752	5	751 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/01/27 09:18 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00242

			IBM_TDB)				
L753	5	752 AND (compar$3 detect$3 match$3) WITH (Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviation alert$3 alarm$3 tolerance warning failure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:19 PM
L754	0	"17858866"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:20 PM
L755	14	750 AND polygraph	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:29 PM
L756	6	755 AND prox$3	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:30 PM
L757	2	756 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:30 PM
L758	8	"20080022405"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:31 PM
L759	0	755 AND subset WITH device	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:49 PM
L760	3	750 AND subset WITH device	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:50 PM
L761	3	760 AND ((@ad OR @rlad) <"20171127")	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 09:50 PM
L762	420580	(H04L63/1425 OR G06F9/455 OR G06F9/545 OR G06F16/9024 OR	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 10:44 PM

		G06F16/9038 OR G06F16/9535 OR G06F16/9537 OR G06F21/57 OR H04L43/045 OR H04L43/06 OR H04L63/10 OR H04L67/306 OR H04L67/535 OR G06F16/2456).cpc.					
L763	16280	762 AND subset WITH device	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 10:44 PM
L764	7700	763 AND (compar$3 detect$3 match$3) WITH (Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviation alert$3 alarm$3 tolerance warning failure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 10:44 PM
L765	6	764 AND ((Original OR initial OR first) WITH (session instance communication profile OR log$4 OR credential) WITH (monitor$3 OR track$3 audit$3 OR inspect$3) WITH (generat$3 OR creat$3 OR produc$3) WITH (graph OR pattern OR map$4) WITH (anomal$3 OR behavior OR intrusion OR threat OR attack$3 anomalous OR risk) AND (multiple OR plurality) WITH (machine OR device OR node) WITH model$4) AND edge WITH (connect$3 OR link$3 OR communicat$3) AND (alert$3 OR alarm$3)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 10:45 PM
L766	19	((Original OR initial OR first) WITH (session	(US-PGPUB; USPAT; USOCR; FIT (CN, FR,	OR	ON	ON	2024/01/27 10:46 PM

		instance communication profile OR log$4 OR credential) WITH (monitor$3 OR track$3 audit$3 OR inspect$3) WITH (generat$3 OR creat$3 OR produc$3) WITH (graph OR pattern OR map$4) WITH (anomal$3 OR behavior OR intrusion OR threat OR attack$3 anomalous OR risk) AND (multiple OR plurality) WITH (machine OR device OR node) WITH model$4) AND edge WITH (connect$3 OR link$3 OR communicat$3) AND (alert$3 OR alarm$3).clm.	WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L767	5	752 AND (compar$3 detect$3 match$3) WITH (Trojan suspicious Malware OR malicious OR worm OR infect$3 OR DoS OR virus OR anomal$3 OR contamin$5 OR malfunction$3 fault error defect$3 attack$3 intrusion discrepanc$3 distort$3 deviation alert$3 alarm$3 tolerance warning failure)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/01/27 10:48 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N420	4	N122 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00245

		or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with model$4).clm.					
N421	0	N122 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N422	64	("20060085437"|"20160080404"|"20180248901"|"9332020"|"9515999"|"9853968"|"20170118240"|"10033611"|"10142357"|"20030037136"|"20060259470"|"20110055138"|"20170279827"|"20180288063"|"20180367548"|"9021583"|"20070118909"|"20090271504"|"20120317151"|"20170163666"|"5806062"|"10389742"|"20180181750"|"20160149937"|"20050102284"|"20140359558"|"20170272344"|"20180020015"|"20180173789"|"8103906"|"9596253"|"20020184225"|"20090019160"|"20150135312"|"8122122"|"10115111"|"10127273"|"20040015470"|"20080148180"|"20100094767"|"20160078365"|"20160218911"|"20160359592"|"20180174062"|"20190132224"|"5584024"|"20100274785"|"20120005243"|"20180063178"|"20180115578"|"8443442"|"8862524"|"2014011500	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM

		1"|"20030179227"|"20100172261"|"20130304915"|"20150341379"|"20160205125"|"20180034840"|"9516053"|"9654503"|"20100114931"|"20190259033"|"20190222597").PN.					
N423	64	("20060085437"|"20160080404"|"20180248901"|"9332020"|"9515999"|"9853968"|"20170118240"|"10033611"|"10142357"|"20030037136"|"20060259470"|"20110055138"|"20170279827"|"20180288063"|"20180367548"|"9021583"|"20070118909"|"20090271504"|"20120317151"|"20170163666"|"5806062"|"10389742"|"20180181750"|"20160149937"|"20050102284"|"20140359558"|"20170272344"|"20180020015"|"20180173789"|"8103906"|"9596253"|"20020184225"|"20090019160"|"20150135312"|"8122122"|"10115111"|"10127273"|"20040015470"|"20080148180"|"20100094767"|"20160078365"|"20160218911"|"20160359592"|"20180174062"|"20190132224"|"5584024"|"20100274785"|"20120005243"|"20180063178"|"20180115578"|"8443442"|"8862524"|"20140115001"|"20030179227"|"20100172261"|"20130304915"|"20150341379"|"20160205125"|"20180034840"|"9516053"|"9654503"|"20100114931"|"20190259033"|"20190222597").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N424	0	378 AND (graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) near10 (personal individual$5 specific) AND (software near4	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM

		service OR SaaS) AND access$3 WITH (target destination)).clm.					
N425	0	378 AND (graph$3 SAME (destination target) WITH (type group$3 class) WITH (visual visualiz$5) AND (software near4 service OR SaaS) AND access$3 WITH (target destination)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N426	11143	N85 and ((anomal$3 or behavior or intrusion or threat or attack$3 anomalous potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2 fraudster or fraudulent) near8 (machine or device or node or client terminal) and (detect$3 or indetif$4 or determin$5) with(Anomal$3 or behavior or intrusion or threat or attack$3))	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N427	11143	N85 and ((anomal$3 or behavior or intrusion or threat or attack$3 anomalous potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2 fraudster or fraudulent) near8 (machine or device or node or client terminal) and (detect$3 or indetif$4 or determin$5) with(Anomal$3 or behavior or intrusion or threat or attack$3))	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N428	0	N193 and ((Original or initial or first) with (session) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4 or model) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM

		potential or suspicious or suspicion or violat$5 or unusual or intrusion or malicious or exploit behavior$2) and (hash or checksum) with (password or pin)).clm.					
N429	14	N291 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N430	14	N291 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:46 PM
N431	0	"17858949"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:49 PM
N432	0	"17858949"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/13 11:52 PM
N433	0	(train$3 WITH model AND approv$3 NEAR5 workflow AND (HISTORY OR RECORD LOG) near8 (deviat$3 normal abnormal intrusion)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/14 12:08 AM
N434	14	N291 and ((Original or initial or first) with (session instance	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM

		communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.					
N435	14	N291 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N436	14	N291 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N437	14	N291 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM

		or produc$3) with (logical or graph or pattern or map$4 or model or rout$3) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk)).clm.					
N438	0	N122 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N439	0	N122 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N440	12	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N441	12	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N442	12	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N443	12	"16134821"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N444	16575	(H04L63/1425 or	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27

		G06F17/30958).cpc.					08:59 PM
N445	0	N153 and ((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4) and edge with (connect$3 or link$3 or communicat$3) and (alert$3 or alarm$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 08:59 PM
N446	16	((Original or initial or first) with (session instance communication profile or log$4 or credential) with (monitor$3 or track$3 audit$3 or inspect$3) with (generat$3 or creat$3 or produc$3) with (graph or pattern or map$4) with (anomal$3 or behavior or intrusion or threat or attack$3 anomalous or risk) and (multiple or plurality) with (machine or device or node) with model$4) and edge with (connect$3 or link$3 or communicat$3) and (alert$3 or alarm$3).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 09:00 PM
N447	0	"17858866"	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 09:20 PM
N448	5	poligraph	(US-PGPUB; USPAT)	OR	ON	ON	2024/01/27 09:28 PM

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	OPAP
Examiner Name	DOCKET CENTRAL
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10122740	B1	2018-11-06	Finkelshtein et al.	
	2	10237294	B1	2019-03-19	Zadeh et al.	
	3	10367704	B2	2019-07-30	Giura et al.	
	4	10382303	B2	2019-08-13	Khanal et al.	
	5	10419468	B2	2019-09-17	Glatfelter et al.	
	6	10447526	B2	2019-10-15	Tucker et al.	
	7	10505818	B1	2019-12-10	Yona et al.	
	8	10521584	B1	2019-12-31	Mehr	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	9	10565373	B1	2020-02-18	Rao et al.	
	10	10791131	B2	2020-09-29	Nor et al.	
	11	10797974	B2	2020-10-06	Giura et al.	
	12	10812497	B2	2020-10-20	Venkatramani et al.	
	13	10904270	B2	2021-01-26	Muddu et al.	
	14	10911470	B2	2021-02-02	Muddu et al.	
	15	11575693	B1	2023-02-07	Muddu et al.	
	16	6363411	B1	2002-03-26	Dugan et al.	
	17	7054873	B2	2006-05-30	Nordström et al.	
	18	8352589	B2	2013-01-08	Ridel et al.	
	19	9225730	B1	2015-12-29	Brezinski	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	20	9497224	B2	2016-11-15	Sweet et al.	
	21	9596254	B1	2017-03-14	Muddu et al.	
	22	9729416	B1	2017-08-08	Khanal et al.	
	23	9811790	B2	2017-11-07	Ahern et al.	
	24	9923911	B2	2018-03-20	Vasseur et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070130330	A1	2007-06-07	Ridel et al.	
	2	20070168696	A1	2007-07-19	Ridel et al.	
	3	20080270451	A1	2008-10-30	Thomsen et al.	
	4	20150058619	A1	2015-02-26	Sweet et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	5	20170063906	A1	2017-03-02	Muddu et al.	
	6	20170063908	A1	2017-03-02	Muddu et al.	
	7	20170063910	A1	2017-03-02	Muddu et al.	
	8	20170063912	A1	2017-03-02	Muddu et al.	
	9	20170230183	A1	2017-08-10	Sweet et al.	
	10	20170277553	A1	2017-09-28	Zada et al.	
	11	20180013650	A1	2018-01-11	Khanal et al.	
	12	20180019932	A1	2018-01-18	Giura et al.	
	13	20180069885	A1	2018-03-08	Patterson et al.	
	14	20180123864	A1	2018-05-03	Tucker et al.	
	15	20190158524	A1	2019-05-23	Zadeh et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	16	20190312796	A1	2019-10-10	Giura et al.	
	17	20190342311	A1	2019-11-07	Muddu et al.	
	18	20190364067	A1	2019-11-28	Yona et al.	
	19	20200065857	A1	2020-02-27	Lagi et al.	
	20	20200228555	A1	2020-07-16	Wittenschlaeger	
	21	20200287927	A1	2020-09-10	Zadeh et al.	
	22	20200404008	A1	2020-12-24	Venkatramani et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/MAHFUZUR RAHMAN/	Date Considered	01/27/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-04-24
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R/

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**12/07/2023 03:26:29 PM Z ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	Ashley Jenkins
PATENT CENTER #	63530523	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2023-12-07_L0040B3CIP6C1_IDS.pdf	22	Information Disclosure Statement (IDS) Form (SB08)	1256 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2023-12-07_L0040B3CIP6C1_IDS.pdf	86A56886D1FCE15FBCAC5C5EB5B2F42BB7C126492A2DA7F6A2AC492B2AD280F762CFD0F6334DDC9D21D0DDCCF6B719C06849675DA452A862CDEED160708F54D5

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	OPAP
Examiner Name	DOCKET CENTRAL
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10003605	B2	2018-06-19	Muddu et al.	
	2	10116670	B2	2018-10-30	Muddu et al.	
	3	10148677	B2	2018-12-04	Muddu et al.	
	4	10158652	B2	2018-12-18	Muddu et al.	
	5	10205735	B2	2019-02-12	Apostolopoulos	
	6	10243970	B2	2019-03-26	Muddu et al.	
	7	10254848	B2	2019-04-09	Winternitz et al.	
	8	10338895	B2	2019-07-02	Zhang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	9	10389738	B2	2019-08-20	Muddu et al.	
	10	10419463	B2	2019-09-17	Muddu et al.	
	11	10419465	B2	2019-09-17	Muddu et al.	
	12	10432639	B1	2019-10-01	Bebee et al.	
	13	10454889	B2	2019-10-22	HUANG	
	14	10459979	B2	2019-10-29	Piechowicz et al.	
	15	10462169	B2	2019-10-29	DURAIRAJ et al.	
	16	10491705	B2	2019-11-26	Oetting et al.	
	17	10496468	B2	2019-12-03	Gefen et al.	
	18	10534633	B2	2020-01-14	Hilemon et al.	
	19	10666668	B2	2020-05-26	Muddu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	20	10673880	B1	2020-06-02	Pratt et al.	
	21	10693900	B2	2020-06-23	Zadeh et al.	
	22	10698954	B2	2020-06-30	Piechowicz et al.	
	23	10756982	B2	2020-08-25	Bai et al.	
	24	10771488	B2	2020-09-08	Verma et al.	
	25	10776191	B2	2020-09-15	Zheng et al.	
	26	10788570	B2	2020-09-29	Wilson	
	27	11036716	B2	2021-06-15	Griffith et al.	
	28	11044264	B2	2021-06-22	DURAIRAJ et al.	
	29	11082289	B2	2021-08-03	Dang et al.	
	30	11120343	B2	2021-09-14	Das et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	31	11126533	B2	2021-09-21	Knowles et al.	
	32	11194849	B2	2021-12-07	Lassoued et al.	
	33	11212299	B2	2021-12-28	Gamble et al.	
	34	11258807	B2	2022-02-22	Muddu et al.	
	35	11281519	B2	2022-03-22	Krishnaswamy et al.	
	36	11314789	B2	2022-04-26	Goldfarb	
	37	11411966	B2	2022-08-09	Muddu et al.	
	38	11463464	B2	2022-10-04	Zadeh et al.	
	39	11494787	B2	2022-11-08	Erickson et al.	
	40	11544138	B2	2023-01-03	Kapish et al.	
	41	11606272	B1	2023-03-14	Popelka et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	42	11636090	B2	2023-04-25	Li et al.	
	43	11640388	B2	2023-05-02	Yang et al.	
	44	11647034	B2	2023-05-09	Levin et al.	
	45	11658990	B2	2023-05-23	Shapoury	
	46	11669571	B2	2023-06-06	Binkley et al.	
	47	11693958	B1	2023-07-04	Steiman	
	48	11722554	B2	2023-08-08	Keren et al.	
	49	11734351	B2	2023-08-22	Binkley et al.	
	50	11734419	B1	2023-08-22	Mackle	
	51	11748473	B2	2023-09-05	Araujo et al.	
	52	11755576	B1	2023-09-12	Jiang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	53	11755602	B2	2023-09-12	Smith Shawn et al.	
	54	11769098	B2	2023-09-26	Adinarayan et al.	
	55	11770387	B1	2023-09-26	Shivamoggi et al.	
	56	7233333	B2	2007-06-19	Lomask	
	57	7478246	B2	2009-01-13	Arndt et al.	
	58	7484091	B2	2009-01-27	Bade et al.	
	59	7526501	B2	2009-04-28	Albahari et al.	
	60	7707411	B2	2010-04-27	Bade et al.	
	61	7739211	B2	2010-06-15	Coffman et al.	
	62	7747559	B2	2010-06-29	Leitner et al.	
	63	7765431	B2	2010-07-27	Agha et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	64	8050907	B2	2011-11-01	Baisley et al.	
	65	8086852	B2	2011-12-27	Bade et al.	
	66	8140977	B2	2012-03-20	Kriss et al.	
	67	8160999	B2	2012-04-17	Jin et al.	
	68	8209204	B2	2012-06-26	Adler et al.	
	69	8301660	B2	2012-10-30	Yalamanchi	
	70	8490055	B2	2013-07-16	Basak	
	71	9043764	B2	2015-05-26	Ranganathan et al.	
	72	9053437	B2	2015-06-09	Adler et al.	
	73	9064210	B1	2015-06-23	Hart	
	74	9075618	B2	2015-07-07	Winternitz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	75	9110873	B2	2015-08-18	Woodall et al.	
	76	9159024	B2	2015-10-13	Bhanot et al.	
	77	9189623	B1	2015-11-17	Lin et al.	
	78	9589069	B2	2017-03-07	Yang et al.	
	79	9591010	B1	2017-03-07	Muddu et al.	
	80	9600915	B2	2017-03-21	Winternitz et al.	
	81	9667641	B2	2017-05-30	Muddu et al.	
	82	9679243	B2	2017-06-13	Zou et al.	
	83	9699205	B2	2017-07-04	Muddu et al.	
	84	9710332	B1	2017-07-18	Fan et al.	
	85	9720703	B2	2017-08-01	Reick et al.	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00270

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	86	9720704	B2	2017-08-01	Reick et al.	
	87	9727441	B2	2017-08-08	Agarwal et al.	
	88	9727604	B2	2017-08-08	Jin et al.	
	89	9813435	B2	2017-11-07	Muddu et al.	
	90	9824473	B2	2017-11-21	Winternitz et al.	
	91	9838410	B2	2017-12-05	Muddu et al.	
	92	9843837	B2	2017-12-12	Gopalan	
	93	9864672	B2	2018-01-09	Seto et al.	
	94	9985827	B2	2018-05-29	Li et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	1	20040225929	A1	2007-01-23	Agha et al.	
	2	20050246521	A1	2009-01-27	Bade et al.	
	3	20060025987	A1	2006-02-02	Baisley et al.	
	4	20060026419	A1	2009-01-13	Arndt et al.	
	5	20060109271	A1	2007-06-19	Lomask	
	6	20070214111	A1	2017-08-08	Jin et al.	
	7	20070282916	A1	2007-12-06	Albahari et al.	
	8	20080109730	A1	2008-05-08	Coffman et al.	
	9	20080147707	A1	2012-04-17	Jin et al.	
	10	20090006843	A1	2011-12-27	Bade et al.	
	11	20090007010	A1	2009-01-01	Kriss et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	12	20090063857	A1	2010-04-27	Bade et al.	
	13	20090307651	A1	2009-12-10	Senthil et al.	
	14	20090327328	A1	2015-08-18	Woodall et al.	
	15	20100042823	A1	2011-08-09	Arndt et al.	
	16	20110119100	A1	2011-05-19	Ruhl et al.	
	17	20110154287	A1	2011-06-23	Mukkamala et al.	
	18	20120143898	A1	2012-06-07	Bruno et al.	
	19	20120159333	A1	2012-06-21	Mital et al.	
	20	20130024412	A1	2013-01-24	Gong et al.	
	21	20130151453	A1	2013-06-13	Bhanot et al.	
	22	20140067750	A1	2015-05-26	Ranganathan et al.	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00273

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	23	20140125672	A1	2015-07-07	Winternitz et al.	
	24	20140279779	A1	2017-06-13	Zou et al.	
	25	20150310649	A1	2017-03-21	Winternitz et al.	
	26	20160120070	A1	2016-04-28	Myrah et al.	
	27	20160357521	A1	2019-07-02	Zhang et al.	
	28	20170063888	A1	2017-03-02	Muddu et al.	
	29	20170063903	A1	2017-03-02	Muddu et al.	
	30	20170063905	A1	2017-03-02	Muddu et al.	
	31	20170063909	A1	2017-03-02	Muddu et al.	
	32	20170063911	A1	2017-03-02	Muddu et al.	
	33	20170070594	A1	2019-11-26	Oetting et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	34	20170102961	A1	2020-01-14	Hilemon et al.	
	35	20170118099	A1	2017-04-27	HUANG	
	36	20170142140	A1	2017-05-18	Muddu et al.	
	37	20170148197	A1	2017-05-25	Winternitz et al.	
	38	20170155570	A1	2017-06-01	Maheshwari et al.	
	39	20170155672	A1	2017-06-01	Muthukrishnan et al.	
	40	20170223036	A1	2017-08-03	Muddu et al.	
	41	20170330096	A1	2017-11-16	Gupta et al.	
	42	20170346683	A1	2018-05-29	Li et al.	
	43	20180004835	A1	2018-01-04	Piechowicz et al.	
	44	20180004859	A1	2020-06-30	Piechowicz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	45	20180007145	A1	2019-10-29	Piechowicz et al.	
	46	20180089132	A1	2018-03-29	Atta et al.	
	47	20180191781	A1	2018-07-05	Palani et al.	
	48	20180211425	A1	2018-07-26	Winternitz et al.	
	49	20180219888	A1	2018-08-02	Apostolopoulos	
	50	20180219897	A1	2018-08-02	Muddu et al.	
	51	20180359162	A1	2018-12-13	Savov et al.	
	52	20190042950	A1	2019-02-07	Lin et al.	
	53	20190050445	A1	2021-06-15	Griffith et al.	
	54	20190058626	A1	2019-02-21	Knowles et al.	
	55	20190075126	A1	2019-03-07	Muddu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	56	20190101622	A1	2019-04-04	Wilson	
	57	20190163555	A1	2019-05-30	Zheng et al.	
	58	20190227860	A1	2019-12-03	Gefen et al.	
	59	20190312898	A1	2019-10-10	Verma et al.	
	60	20190327251	A1	2019-10-24	Muddu et al.	
	61	20190342307	A1	2019-11-07	Gamble et al.	
	62	20190354554	A1	2019-11-21	Piechowicz et al.	
	63	20190356555	A1	2020-08-25	Bai et al.	
	64	20200014718	A1	2020-01-09	DURAIRAJ et al.	
	65	20200021607	A1	2020-01-16	Muddu et al.	
	66	20200175361	A1	2020-06-04	Che et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	67	20200287923	A1	2020-09-10	Raghavendra et al.	
	68	20200320106	A1	2022-04-26	Goldfarb	
	69	20200334293	A1	2020-10-22	Piechowicz et al.	
	70	20200351151	A1	2020-11-05	Dang et al.	
	71	20200412752	A1	2020-12-31	Shapoury	
	72	20210019209	A1	2021-01-21	Krishnaswamy et al.	
	73	20210232420	A1	2021-07-29	Dhruvakumar et al.	
	74	20210286798	A1	2021-09-16	Li et al.	
	75	20210294798	A1	2021-09-23	Binkley et al.	
	76	20210406917	A1	2021-12-30	Erickson et al.	
	77	20220004718	A1	2022-01-06	Quamar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	78	20220050840	A1	2022-02-17	Parravicini et al.	
	79	20220058193	A1	2023-09-12	Smith Shawn et al.	
	80	20220067186	A1	2022-03-03	Thakur et al.	
	81	20220086179	A1	2023-05-09	Levin et al.	
	82	20220092481	A1	2022-03-24	Neithalath et al.	
	83	20220121741	A1	2023-09-05	Araujo et al.	
	84	20220124108	A1	2022-04-21	Gamble et al.	
	85	20220129803	A1	2022-04-28	Bikumala et al.	
	86	20220191226	A1	2022-06-16	Chan et al.	
	87	20220327119	A1	2022-10-13	Gasper et al.	
	88	20220350789	A1	2023-05-02	Yang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	89	20220374800	A1	2023-09-26	Adinarayan et al.	
	90	20220376970	A1	2022-11-24	Chawathe et al.	
	91	20220382611	A1	2023-01-03	Kapish et al.	
	92	20220394082	A1	2022-12-08	Keren et al.	
	93	20220414072	A1	2022-12-29	Tandon et al.	
	94	20220414105	A1	2022-12-29	Umay et al.	
	95	20230025252	A1	2023-01-26	Erickson et al.	
	96	20230039566	A1	2023-02-09	Ghag et al.	
	97	20230052827	A1	2023-02-16	Araujo et al.	
	98	20230088960	A1	2023-03-23	Popelka et al.	
	99	20230096930	A1	2023-03-30	Dasdan	

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00280

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	100	20230101773	A1	2023-03-30	Katahanas et al.	
	101	20230138371	A1	2023-05-04	Bandukwala et al.	
	102	20230244523	A1	2023-08-03	Gorantla et al.	
	103	20230251960	A1	2023-08-10	Sharma et al.	
	104	20230275909	A1	2023-08-31	Shivamoggi et al.	
	105	20230291755	A1	2023-09-14	Siebel et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-12-07
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	OPAP
Examiner Name	DOCKET CENTRAL
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10122740	B1	2018-11-06	Finkelshtein et al.	
	2	10237294	B1	2019-03-19	Zadeh et al.	
	3	10367704	B2	2019-07-30	Giura et al.	
	4	10382303	B2	2019-08-13	Khanal et al.	
	5	10419468	B2	2019-09-17	Glatfelter et al.	
	6	10447526	B2	2019-10-15	Tucker et al.	
	7	10505818	B1	2019-12-10	Yona et al.	
	8	10521584	B1	2019-12-31	Mehr	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	9	10565373	B1	2020-02-18	Rao et al.	
	10	10791131	B2	2020-09-29	Nor et al.	
	11	10797974	B2	2020-10-06	Giura et al.	
	12	10812497	B2	2020-10-20	Venkatramani et al.	
	13	10904270	B2	2021-01-26	Muddu et al.	
	14	10911470	B2	2021-02-02	Muddu et al.	
	15	11575693	B1	2023-02-07	Muddu et al.	
	16	6363411	B1	2002-03-26	Dugan et al.	
	17	7054873	B2	2006-05-30	Nordström et al.	
	18	8352589	B2	2013-01-08	Ridel et al.	
	19	9225730	B1	2015-12-29	Brezinski	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	20	9497224	B2	2016-11-15	Sweet et al.	
	21	9596254	B1	2017-03-14	Muddu et al.	
	22	9729416	B1	2017-08-08	Khanal et al.	
	23	9811790	B2	2017-11-07	Ahern et al.	
	24	9923911	B2	2018-03-20	Vasseur et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070130330	A1	2007-06-07	Ridel et al.	
	2	20070168696	A1	2007-07-19	Ridel et al.	
	3	20080270451	A1	2008-10-30	Thomsen et al.	
	4	20150058619	A1	2015-02-26	Sweet et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	5	20170063906	A1	2017-03-02	Muddu et al.	
	6	20170063908	A1	2017-03-02	Muddu et al.	
	7	20170063910	A1	2017-03-02	Muddu et al.	
	8	20170063912	A1	2017-03-02	Muddu et al.	
	9	20170230183	A1	2017-08-10	Sweet et al.	
	10	20170277553	A1	2017-09-28	Zada et al.	
	11	20180013650	A1	2018-01-11	Khanal et al.	
	12	20180019932	A1	2018-01-18	Giura et al.	
	13	20180069885	A1	2018-03-08	Patterson et al.	
	14	20180123864	A1	2018-05-03	Tucker et al.	
	15	20190158524	A1	2019-05-23	Zadeh et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

	16	20190312796	A1	2019-10-10	Giura et al.	
	17	20190342311	A1	2019-11-07	Muddu et al.	
	18	20190364067	A1	2019-11-28	Yona et al.	
	19	20200065857	A1	2020-02-27	Lagi et al.	
	20	20200228555	A1	2020-07-16	Wittenschlaeger	
	21	20200287927	A1	2020-09-10	Zadeh et al.	
	22	20200404008	A1	2020-12-24	Venkatramani et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	OPAP
	Examiner Name	DOCKET CENTRAL
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-04-24
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**04/24/2023 04:52:00 PM ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	Laryssa Weiland
PATENT CENTER #	61974230	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
L0040B3CIP6C1_SuppIDS.pdf	8	Information Disclosure Statement (IDS) Form (SB08)	1253 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
L0040B3CIP6C1_SuppIDS.pdf	959E640A2C807EC4FF0A48EF57BD3628E70F1473C5FD20A49 E6C767318570C9CE5F376A1A39A0EE7E6A566D32BCC618B69 BD91A05424C3054073C21F90743128

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17858866
Filing Date	2022-07-06
First Named Inventor	VIKRAM KAPOOR
Art Unit	
Examiner Name	
Attorney Docket Number	L0040B3CIP6C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10033611	B1	2018-07-24	Linkous et al.	
	2	10115111	B2	2018-10-30	Miltonberger	
	3	10127273	B2	2018-11-13	Dickey	
	4	10142357	B1	2018-11-27	Tamersoy et al.	
	5	10205736	B2	2019-02-12	Rieke et al.	
	6	10339309	B1	2019-07-02	Kling et al.	
	7	10389742	B2	2019-08-20	Reddy et al.	
	8	10594718	B1	2020-03-17	Deaguero et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	9	10708082	B1	2020-07-07	Bakiaraj et al.	
	10	10735329	B2	2020-08-04	WANG et al.	
	11	11431735	B2	2022-08-30	SHUA	
	12	11489863	B1	2022-11-01	Shua et al.	
	13	5584024	A	1996-12-10	Shwartz	
	14	5806062	A	1998-09-08	Chen et al.	
	15	8103906	B1	2012-01-24	Alibakhsh et al.	
	16	8122122	B1	2012-02-21	Clingenpeel et al.	
	17	8443442	B2	2013-05-14	Wang et al.	
	18	8671453	B2	2014-03-11	Underwood et al.	
	19	8862524	B2	2014-10-14	Zheng et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	20	9021583	B2	2015-04-28	Wittenstein et al.	
	21	9037273	B2	2015-05-19	Mikkelsen	
	22	9332020	B2	2016-05-03	Thomas et al.	
	23	9515999	B2	2016-12-06	Ylonen	
	24	9516053	B1	2016-12-06	Muddu et al.	
	25	9558265	B1	2017-01-31	Tacchi et al.	
	26	9596253	B2	2017-03-14	Chauhan et al.	
	27	9654503	B1	2017-05-16	Kowalyshyn	
	28	9734040	B2	2017-08-15	Gounares	
	29	9749339	B2	2017-08-29	Kadambe et al.	
	30	9853968	B2	2017-12-26	Shen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	31	9953014	B1	2018-04-24	Reshadi et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020184225	A1	2002-12-05	Ghukasyan	
	2	20030037136	A1	2003-02-20	Labovitz et al.	
	3	20030179227	A1	2003-09-25	Ahmad et al.	
	4	20040015470	A1	2004-01-22	Smith et al.	
	5	20050102284	A1	2005-05-12	Srinivasan et al.	
	6	20050188222	A1	2005-08-25	Motsinger et al.	
	7	20060085437	A1	2006-04-20	Brodhun et al.	
	8	20060259470	A1	2006-11-16	Chandrasekharan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	9	20060288415	A1	2006-12-21	Wong	
	10	20070050497	A1	2007-03-01	Haley et al.	
	11	20070118909	A1	2007-05-24	Hertzog et al.	
	12	20080148180	A1	2008-06-19	Liu et al.	
	13	20080151893	A1	2008-06-26	Nordmark et al.	
	14	20090019160	A1	2009-01-15	Schuler	
	15	20090228474	A1	2009-09-10	Chiu et al.	
	16	20090271504	A1	2009-10-29	Ginter et al.	
	17	20100094767	A1	2010-04-15	Miltonberger	
	18	20100114931	A1	2010-05-06	Xie et al.	
	19	20100172261	A1	2010-07-08	Shinbo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	20	20100274785	A1	2010-10-28	Procopiuc et al.	
	21	20110055138	A1	2011-03-03	Khanduja et al.	
	22	20120005243	A1	2012-01-05	Merwe et al.	
	23	20120317151	A1	2012-12-13	Ruf et al.	
	24	20120323956	A1	2012-12-20	Dumitru et al.	
	25	20130304915	A1	2013-11-14	KAWAI	
	26	20130305357	A1	2013-11-14	Ayyagari et al.	
	27	20140115001	A1	2014-04-24	Arroyo et al.	
	28	20140115011	A1	2014-04-24	Buerner et al.	
	29	20140208191	A1	2014-07-24	Zaric et al.	
	30	20140245443	A1	2014-08-28	Chakraborty	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	31	20140280068	A1	2014-09-18	DHOOPAR et al.	
	32	20140359558	A1	2014-12-04	Chamberlain	
	33	20150135312	A1	2015-05-14	Wada et al.	
	34	20150188751	A1	2015-07-02	Vasseur et al.	
	35	20150341379	A1	2015-11-26	Lefebvre et al.	
	36	20150356144	A1	2015-12-10	Chawla et al.	
	37	20160078365	A1	2016-03-17	Baumard	
	38	20160080404	A1	2016-03-17	KOHOUT et al.	
	39	20160110434	A1	2016-04-21	Kakaraddi et al.	
	40	20160149937	A1	2016-05-26	KATMOR et al.	
	41	20160205125	A1	2016-07-14	Kim et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	42	20160218911	A1	2016-07-28	WESSELS et al.	
	43	20160359592	A1	2016-12-08	Kulshreshtha et al.	
	44	20160359872	A1	2016-12-08	Yadav et al.	
	45	20170118240	A1	2017-04-27	Reddy et al.	
	46	20170134240	A1	2017-05-11	Hévizi et al.	
	47	20170147646	A1	2017-05-25	LEE et al.	
	48	20170163666	A1	2017-06-08	Venkatramani et al.	
	49	20170251013	A1	2017-08-31	Kirti et al.	
	50	20170272344	A1	2017-09-21	Tang et al.	
	51	20170279827	A1	2017-09-28	Savalle et al.	
	52	20170288974	A1	2017-10-05	Yoshihira et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	53	20170359361	A1	2017-12-14	Modani et al.	
	54	20170366492	A1	2017-12-21	Ho et al.	
	55	20180020015	A1	2018-01-18	Munro et al.	
	56	20180034840	A1	2018-02-01	Marquardt et al.	
	57	20180063178	A1	2018-03-01	Jadhav et al.	
	58	20180103052	A1	2018-04-12	Choudhury et al.	
	59	20180115578	A1	2018-04-26	Subbarayan et al.	
	60	20180137858	A1	2018-05-17	Saxena et al.	
	61	20180173789	A1	2018-06-21	Llagostera et al.	
	62	20180174062	A1	2018-06-21	Simo et al.	
	63	20180181750	A1	2018-06-28	Lamothe-Brassard	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	64	20180248901	A1	2018-08-30	Rieke	
	65	20180268078	A1	2018-09-20	Gianetto et al.	
	66	20180288063	A1	2018-10-04	Koottayi et al.	
	67	20180329958	A1	2018-11-15	Choudhury et al.	
	68	20180336353	A1	2018-11-22	Manadhata et al.	
	69	20180357422	A1	2018-12-13	Telang et al.	
	70	20180367548	A1	2018-12-20	Stokes III et al.	
	71	20190028327	A1	2019-01-24	SILVA et al.	
	72	20190109870	A1	2019-04-11	BEDHAPUDI et al.	
	73	20190132224	A1	2019-05-02	VERMA et al.	
	74	20190222597	A1	2019-07-18	Crabtree et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	75	20190259033	A1	2019-08-22	Reddy et al.	
	76	20190339965	A1	2019-11-07	Garvey et al.	
	77	20190349305	A1	2019-11-14	WANG et al.	
	78	20190378050	A1	2019-12-12	Edkin et al.	
	79	20200076685	A1	2020-03-05	Vaidya et al.	
	80	20200192690	A1	2020-06-18	Gupta et al.	
	81	20200252376	A1	2020-08-06	Feng et al.	
	82	20200272740	A1	2020-08-27	Obee et al.	
	83	20200278892	A1	2020-09-03	Nainar et al.	
	84	20200280592	A1	2020-09-03	Ithal et al.	
	85	20200311644	A1	2020-10-01	WILLARD III et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	86	20200403860	A1	2020-12-24	Lewis et al.	
	87	20210329019	A1	2021-10-21	SHUA	
	88	20210336976	A1	2021-10-28	SHUA	
	89	20210377287	A1	2021-12-02	SHUA	
	90	20220342690	A1	2022-10-27	Shua	
	91	20220345480	A1	2022-10-27	Shua	
	92	20220345481	A1	2022-10-27	Shua	
	93	20220345483	A1	2022-10-27	Shua	
	94	20220350931	A1	2022-11-03	Shua	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	AI-YASEEN et al., "Real-Time Intrusion Detection System Using Multi-Agent System", IAENG International Journal of Computer Science, volume 43, no. 1, February 2016, pp. 80-90, International Association of Engineers (IAENG), Hong Kong.	
	2	AKOGLU et al., "Graph-based Anomaly Detection and Description: A Survey", April 28, 2014.	
	3	AMIDON et al., "Program Fracture and Recombination for Efficient Automatic Code Reuse", In 2015 IEEE High Performance Extreme Computing Conference (HPEC), September 2015, pp. 1-6, IEEE.org (online), DOI: 10.1109/HPEC.2015.7396314.	
	4	AMMAR et al., "Query Optimization Techniques in Graph Databases", International Journal of Database Management Systems (IIDMS), Vol. 8, No. 4, August 2016, pages 1-14 (Year: 2016).	
	5	BALASUBRAMANIYAN et al., "An Architecture For Intrusion Detection Using Autonomous Agents", In Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217), 19 pages, June 1998, IEEE, DOI: 10.1109/CSAC.1998.738563.	
	6	BEUTEL et al., "User Behavior Modeling with Large-Scale Graph Analysis", Computer Science Department, Carnegie Mellon University, May 2016.	
	7	BUGIEL et al., "Towards Taming Privilege-Escalation Attacks on Android", In NOSS (Vol. 17, p. 19), 2012, February.	
	8	CHANG et al., "Reality Bites - Progressive Querying and Result Visualization in Logical and VR Spaces", Proceedings of 1994 IEEE Symposium on Visual Languages, pp. 100-109, October 1994, IEEE, DOI: 10.1109NL.1994.363635.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	9	CHESSON, "Communication And Control In A Cluster Network", ACM '74: Proceedings of the 1974 annual ACM conference - Volume 2, January 1974, pp 509-514, http://doi.org/10.1145/1408839 (Year 1974).	
	10	CROSBIE et al., "Defending a Computer System using Autonomous Agents", docs.lib.purdue.edu (online), March 1995, 11 pages.	
	11	HAUTAMAKI et al., "Outlier Detection Using k-Nearest Neighbour Graph", Proceedings of the 17th International Conference on Pattern Recognition (ICPR 2004), Vol. 3, August 2004, IEEE, DOI: 10.1109/ICPR.2004.1334558.	
	12	HOOPER et al., "Medusa: a simple tool for interaction graph analysis", Bioinformatics, Vol. 21 no. 24, September 2005, pages 4432-4433, Oxford University Press (online), URL: https://academic.oup.com/bioinformatics/article/21/24/4432/179694.	
	13	KOUTRA et al., "Exploring and Making Sense of Large Graphs", Computer Science Department, Carnegie Mellon University, August 2015.	
	14	LEOPOLD et al., "A Visual Query System for the Specification and Scientific Analysis off Continual Queries", Proceedings, IEEE Symposia on Human-Centric Computing Languages and Environments (Cat. No.01TH8587), September 2001, pp. 203-211, IEEE, doi: 10.1109/HCC.2001.995260.	
	15	LIAO et al., "Visualizing Graph Dynamics And Similarity For Enterprise Network Security And Management", VizSec '10: Proceedings of the Seventh International Symposium on Visualization for Cyber Security, September 2010, pp. 34-45, URL: https://doi.org/10.1145/1850795.1850799.	
	16	LONG et al., "Automatic Input Rectification", 2012 34th International Conference on Software Engineering (ICSE), June 2012, pp. 80-90, IEEE.org (online), DOI: 10.1109/ICSE.2012.6227204.	
	17	MATEESCU et al., "Join-Graph Propagation Algorithms", Journal of Artificial Intelligence Research, vol. 37, March 2010, pages 279-328, AI Access Foundation, Inc. (online), URL: https://doi.org/10.1613/jair.2842.	
	18	MORIANO et al., "Insider Threat Event Detection in User-System Interactions", MIST '17: Proceedings of the 2017 International Workshop on Managing Insider Security Threats, October 2017, pp 1-12, ACM Digital Library (online), URL: https://doi.Jrg/10.1145/3139923.3139928.	
	19	PERKINS et al., "Automatically Patching Errors in Deployed Software", Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles, October 2009, pp 82-102, acm.org (online), URL: https://doi.org/10.1145/1629575.1629585.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

	20	RANSHOUS et al., "Anomaly detection in dynamic networks: a survey", WIREs Computational Statistics, volume 7, May/June 2015, pp. 223-247, Wiley Periodicals, Inc, United States.	
	21	RINARD, "Living In The Comfort Zone", ACM SIGPLAN Notices, Volume 42, Issue 10, October 2007, pp. 611-622, acm.org (online), URL: https://doi.org/10.1145/1297105.1297072.	
	22	RINARD, "Manipulating Program Functionality to Eliminate Security Vulnerabilities", In Moving Target Defense, January 2011, pp. 109-115. Springer, New York, NY.	
	23	SAMUEL et al., "Let's Parse to Prevent Pwnage", Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET'12), April 2012, 3 pages, acm.org (online), URL: https://www.usenix.org/conference/leet12/workshop-program/presentation/samuel.	
	24	SHEN et al., "Active Learning for Inference and Regeneration of Applications that Access Databases", ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 42, Issue 4, Article 18, January 2021, pp. 1-119, acm.org (online), URL: https://doi.org/10.1145/3430952.	
	25	TAMASSIA et al., "Graph Drawing for Security Visualization", In: Graph Drawing (GD 2008), Lecture Notes in Computer Science, vol 5417, Springer, Berlin, Heidelberg (online), URL: https://doi.org/10.1007/978-3-642-00219-9_2.	
	26	VAAS et al., "Detecting disguised processes using Application-Behavior Profiling", In 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1-6, June 2017, IEEE, DOI: 10.1109/THS.2017.7943508.	
	27	VASILAKIS et al., "Supply-Chain Vulnerability Elimination via Active Learning and Regeneration", Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, November 2021, pp. 1755-1770, acm.org (online), URL: https://doi.org/10.1145/3460120.3484736.	
	28	YU et al., "Recommending Join Queries Based on Path Frequency", 2015 12th Web Information System and Application Conference (WISA), September 2015, pp. 21-26, IEEE, DOI: 10.1109/WISA.2015.52.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17858866
	Filing Date	2022-07-06
	First Named Inventor	VIKRAM KAPOOR
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0040B3CIP6C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-01-06
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/858,866	**01/06/2023 05:08:20 PM ET**	**L0040B3CIP6C1**

Title of Invention

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4455	FILED BY	Laryssa Weiland
PATENT CENTER #	61401986	FILING DATE	07/06/2022
CUSTOMER #	182115	FIRST NAMED INVENTOR	VIKRAM KAPOOR
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 29

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2023-01-06_L0040B3CIP6C1_IDS.pdf	18	Information Disclosure Statement (IDS) Form (SB08)	1258 KB
NPL_BalasubramaniyanAnArchitectureForInIntrusion.pdf	19	Non Patent Literature	224 KB
NPL_Ammar_QueryOptimizationTechniques.pdf	14	Non Patent Literature	311 KB
NPL_Amidon_ProgramFracture.pdf	6	Non Patent Literature	144 KB
NPL_Akoglu_GraphBasedAnomalyDetection.pdf	68	Non Patent Literature	806 KB

NPL_Al-Yaseen_Real-timeIntrusion.pdf	11	Non Patent Literature	449 KB
NPL_Crosbie_DefendingAComputerSystem.pdf	11	Non Patent Literature	289 KB
NPL_Chesson_CommunicationAndControl.pdf	6	Non Patent Literature	702 KB
NPL_Chang_RealityBitesProgressiveQuerying.pdf	10	Non Patent Literature	742 KB
NPL_Hautamaki_OutlierDetectionUsingK-Nearest.pdf	4	Non Patent Literature	338 KB
NPL_Hooper_Medusa-ASimpleTool.pdf	2	Non Patent Literature	214 KB
NPL_Leopold_AVisualQuerySystem.pdf	9	Non Patent Literature	396 KB
NPL_Mateescu_Join-GraphPropogation.pdf	50	Non Patent Literature	701 KB
NPL_Long_AutomaticInputRectification.pdf	11	Non Patent Literature	1610 KB
NPL_Perkins_AutomaticallyPatchingErrors.pdf	16	Non Patent Literature	283 KB
NPL_Ranshous_AnomalyDetectionInDynamicNetworks.pdf	25	Non Patent Literature	493 KB
NPL_Moriano_InsiderThreatEvent.pdf	12	Non Patent Literature	2137 KB
NPL_Rinard_LivingInTheComfortZone.pdf	11	Non Patent Literature	213 KB
NPL_Koutra_ExploringAndM	232	Non Patent Literature	3825 KB

akingSense.pdf			
NPL_Beutel_UserBehaviorModeling.pdf	275	Non Patent Literature	5352 KB
NPL_Samuel_LetsParse.pdf	4	Non Patent Literature	141 KB
NPL_Rinard_ManipulatingProgramFunctionality.pdf	6	Non Patent Literature	79 KB
NPL_Bugiel_TowardsTamingPrivilege-Escalation.pdf	18	Non Patent Literature	5950 KB
NPL_Liao_VisualizingGraphDynamics.pdf	12	Non Patent Literature	4704 KB
NPL_Vaas_DetectingDisguisedProcesses.pdf	6	Non Patent Literature	1083 KB
NPL_Vasilakis_SupplyChainVulnerability.pdf	16	Non Patent Literature	1167 KB
NPL_Yu_RecommendingJoinQueries.pdf	6	Non Patent Literature	611 KB
NPL_Tamassia_GraphDrawingForSecurity.pdf	12	Non Patent Literature	2074 KB
NPL_Shen_ActiveLearningforInference.pdf	119	Non Patent Literature	23293 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2023-01-06_L0040B3CIP6C1_IDS.pdf	0DD4147021697C40F7E08719FAEC24CD828641FB1427A3B283F1AD98CAF27F4FB05489F560307DDE03773FB949C47AD7518709F519619BEE11F5726CB8067D62

NPL_Balasubramaniyan_AnArchitectureForIntrusion.pdf	89D89D9869DCBBE55A4153A48E1BD4CED5FBF83E3D42AD8A7E6B48D2EF1F5988072BCDF32F79A066A708CE2E85D2EC0FF4036FD1EDF166D17C684E4027B7A93F
NPL_Ammar_QueryOptimizationTechniques.pdf	5450BE9D00EE222F51311A0E76BDDA29E49D0D42E050CBAE2AF6F481B5E00200026AC4F585E30704A41547DE02453168F935F48B22D259DA9E0E4311B4869C20
NPL_Amidon_ProgramFracture.pdf	A5163B5F289074A5B578A5C69BAFF222532D61A7130F7D19055A80163749BE9D25BC499F5B5165D8FF879208EDB8AFBF53389FB1AD5E83A0D7842ECA4B4AD44C
NPL_Akoglu_GraphBasedAnomalyDetection.pdf	B29A5D3C6B5D2B61818CB3610CDFEA65FE981A62778C3C145BA31E27B69F0EDE7FA6CDDFFF259BF50B3655BFF1BD581567422EB6CB933ACBBE7BE1AAF7FD8838
NPL_Al-Yaseen_Real-timeIntrusion.pdf	410D4DC41C77675E56DA21A96B493CF00C08E22AAE966408AE09E7FFFF61E430D32F54CEE2A0ABB6D9190159EFD3B8DF0BC6AD0A7E2F05333B07625264CA9B41
NPL_Crosbie_DefendingAComputerSystem.pdf	D65F6310889E53834E679AF8C8296FDC35FDEF9839D7158ABE5F2A6BD9498927D6B700DE6CEA8D6C6B4677FD19DA3D5AAC1E8B976A4BD92A3E4BDDC62348BE7B
NPL_Chesson_CommunicationAndControl.pdf	72FF001DF810C923A0A811B06C6EB03B8DCB29812B2E5FC76F8AC800444F1E1AED684B9055EDCDFD41263868D809822463E745D5D187C4B9A49DB3380167958C
NPL_Chang_RealityBitesProgressiveQuerying.pdf	36FFFB3A06A3DD8F0977DF78B963E835CDBBFAA3F4C431BF41C6061D0A88FBC603019431A55DFF73C2E886FF223F487F0CFCBE6CFDF1E6AE13F907E045869F15
NPL_Hautamaki_OutlierDetectionUsingK-Nearest.pdf	8037EC36114C79375D3E058FD9739C2F3E8D02D00E4FA1A5C8902CC7711AFAE3651FE91633DB6A833E448F38163E626348404CADE416B2CE6362339C0CC6A057
NPL_Hooper_Medusa-ASimpleTool.pdf	BADCC82C81EB5A717282FE221B2DA79DDE5F844E1D77947C1B10A0172D6E1100A6FB314AF8BA7FA22B3A5A7BA555666C5C5E5399AE00399E9940DC3DE54E12A0

NPL_Leopold_AVisualQuerySystem.pdf	2DBBCB42678A322C54D58BBD9BF7D8B950B37B081928F4644496E5B65635F403C142238EE625447929582DA9A964465FC4CE86113C586524BB9D20F7B25B73ED
NPL_Mateescu_Join-GraphPropogation.pdf	240C1B56027F98F776F7616A57CA1C63F6B2B6FA985197300E22D2DFA92FB757D28DC00DA5E4EBFE2EA583872A966C02D95F06D45F08CC280D635635D5697732
NPL_Long_AutomaticInputRectification.pdf	5B5AFA0391B3825FC11AB42870AF9DEC8197A77FAB600BE67667A0367748B48A30231C16BD5934C4CE4E8504D6664F17BB5AAFF78B96BFB6AD7DA0D863E1F4A5
NPL_Perkins_AutomaticallyPatchingErrors.pdf	D1072E4E608A6280A3B1C10D8D2C06B5F60F52390F6038E98285E380686BC56C715EC8D507E016555EE6DBA51D70936B24F0184C8CBC44D1CF0852DF03C8F69C
NPL_Ranshous_AnomalyDetectionInDynamicNetworks.pdf	25E465CAC9E23F8E0F5C46C006FC398BBE2B21BE567F31704F18E9A79ADCCD956A6199D0C6D90B791E03075E18E95D90453E8B8FFFC84E6D495B0C48B3F692AB
NPL_Moriano_InsiderThreatEvent.pdf	883CDB3BE49DD3012BEB1F829023F06BB59D15BECEF2AB53AF27993E86FCA7363D8BF0600D1FFA9461393D0E3F69C7BCBA05F04BCC224A4DF995F22DB209A447
NPL_Rinard_LivingInTheComfortZone.pdf	C5BAED094A9AB1CB7181900E57C0F93EBBFECADCDCC79172AE1604E28E1FB8C83DA67111D5529EC8B4156AA832CBCD335B3FFFC17A1FA8A7F9CDBBC979E16056
NPL_Koutra_ExploringAndMakingSense.pdf	234A544FE73F84AE279FC4F0975B640DD129EBAA9AA8A2C6DDCA07BD85B273404CD7CB34F0F0C5C39400ABC08DE842231FCD82267321DE58B9615011EF49C8C7
NPL_Beutel_UserBehaviorModeling.pdf	F5DF9EE6942BFC7F40B394F4A813718E7C3FC191A3195EC077E7F91310D11ACB4DAB3D7D7BF9764D765C3331DF1669FA9FD2BD8F39B43A1ED3C0D1A00D3C2561
NPL_Samuel_LetsParse.pdf	4BD282FEA8C5BD2EFDB7EAE4091130539BA7AE2A70D87294C49985A95390F5484F7D8C8EA507D3FA761DF84D7FBCE018AA11B967DC7D4C1EF36D8C4B6ED5D88B

NPL_Rinard_ManipulatingProgramFunctionality.pdf	420C43E1D140EC3BA786F8D78B387BCE53926B56F6B13BD431759A7978999ACEFF6FCDC2DC304236927C722CCAED2A2E399BDCF020A0FD3857E84915B414997E
NPL_Bugiel_TowardsTamingPrivilege-Escalation.pdf	AB4A380C4B69D6746D2E55C35C8472398C45D815B9B14BA12ED45665EE24F28D6766733FFB6F9D371D9511FC8EB36DCC856F64F0C069B4818320B119E2488BB7
NPL_Liao_VisualizingGraphDynamics.pdf	655425F1461CA49285FC1541D4BC3C8213580A7412C032D76A7957A4F11F82BB8964C43BA5E0584A919AF7D9691F4CEAE02E75B735FB14DE75B16DE0B520832A
NPL_Vaas_DetectingDisguisedProcesses.pdf	A4CC045FC2C3A718E6D815CCEBC2F20E3B11D69453239F74EE37BC3FC19DF125DB1BB1431229BDAD797EC3B012247A6AE36D19EEE44FACA85710AA90F1F80C07
NPL_Vasilakis_SupplyChainVulnerability.pdf	9622653FABEEBC2BA0B3498E60500655B042037F55824FBF611E792B64A5023D444BDB15AC612E65512971211C6BF9AD675808C838CFD80F1E3F11C91E577A08
NPL_Yu_RecommendingJoinQueries.pdf	453387A31544F555B48A673B5B4BF42BB7A8247AC21511F5140B57B14F4D4E6F957DF84297CDFAA72436CC2B907AFC933F42BBBE4116C0858F35B25FE61D14C5
NPL_Tamassia_GraphDrawingForSecurity.pdf	50D27B55A1265D5471EA36A1A05254AB81F273FC80FDC0A0512A0958AB42CCDBF51B98BDE00A5938251DE58AAA00774A58494D97CFDE610EE76842E137049327
NPL_Shen_ActiveLearningforInference.pdf	982B2B58985D9117510766586BC7BCC699FD14BEF056536C729977E5FCA528984497775DA564A5F6D9107BD47132164756533 7288B06B5FDE2F34567F8B13F36

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C.

371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/858,866	07/06/2022	3656	2240	L0040B3CIP6C1	20	3

CONFIRMATION NO. 4455

FILING RECEIPT

182115
Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

OC000000135207202

Date Mailed: 07/19/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

VIKRAM KAPOOR, CUPERTINO, CA;
HARISH KUMAR BHARAT SINGH, PLEASANTON, CA;
WEIFEI ZENG, SUNNYVALE, CA;
VIMALKUMAR JEYAKUMAR, LOS ALTOS, CA;
THERON TOCK, MOUNTAIN VIEW, CA;
YING XIE, CUPERTINO, CA;
YIJOU CHEN, CUPERTINO, CA;

Applicant(s)

LACEWORK, INC., SAN JOSE, CA;

Power of Attorney: The patent practitioners associated with Customer Number 182115

Domestic Priority data as claimed by applicant

This application is a CON of 17/836,813 06/09/2022 ABN
which is a CIP of 17/196,887 03/09/2021
which is a CON of 16/459,207 07/01/2019 PAT 10986114
which is a CON of 16/134,821 09/18/2018 PAT 10419469
which claims benefit of 62/650,971 03/30/2018
and claims benefit of 62/590,986 11/27/2017
and said 17/836,813 06/09/2022
claims benefit of 63/240,818 09/03/2021
This application 17/858,866
claims benefit of 63/240,818 09/03/2021

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 07/15/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/858,866**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
Title

Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems

Preliminary Class

384

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00322

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00323

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/858,866

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	320
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	700
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	800
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 480 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						420
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2240

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT7418809

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
VIKRAM KAPOOR	06/08/2022
HARISH KUMAR BHARAT SINGH	06/06/2022
WEIFEI ZENG	06/06/2022
VIMALKUMAR JEYAKUMAR	06/08/2022
THERON TOCK	06/09/2022
YING XIE	06/07/2022
YIJOU CHEN	06/06/2022

RECEIVING PARTY DATA

Name:	LACEWORK, INC.
Street Address:	6201 AMERICA CENTER DRIVE
Internal Address:	SUITE 200
City:	SAN JOSE
State/Country:	CALIFORNIA
Postal Code:	95002

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	17858866

CORRESPONDENCE DATA

Fax Number: (512)472-9887

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 512-472-9881
Email: ashley@klspatents.com, kennedm9325@intake.appcoll.com
Correspondent Name: LACEWORK, INC. C/O KLS
Address Line 1: 797 SAM BASS ROAD #2559
Address Line 4: ROUND ROCK, TEXAS 78681

ATTORNEY DOCKET NUMBER:	L0040B3CIP6C1
NAME OF SUBMITTER:	ASHLEY JENKINS
SIGNATURE:	/Ashley Jenkins/

DATE SIGNED:	07/06/2022
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 3
source=2022-07-06_L0040B3CIP6C1_Assignment#page1.tif
source=2022-07-06_L0040B3CIP6C1_Assignment#page2.tif
source=2022-07-06_L0040B3CIP6C1_Assignment#page3.tif

DOCKET NUMBER: **L0040B3CIP6**

ASSIGNMENT-STATEMENT

Title of Invention: **USING ACTIVITY MONITORED BY MULTIPLE DATA SOURCES TO IDENTIFY SHADOW SYSTEMS**

As a below named inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked):

[✓] United States application or PCT international application number 17/858,866 filed on July 6, 2022.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR Section 1.56.

Whereas, I ("ASSIGNOR") have made certain inventions, improvements, and discoveries (herein referred to as the "Invention") disclosed in the above-identified patent application and further identified by the Docket Number provided above in the header of this document;

Whereas, Lacework, Inc., (herein referred to as the "ASSIGNEE"), a corporation organized and existing under the laws of the State of Delaware, with a principal office at 6201 America Center Drive, Suite 200, San Jose, CA 95002 (herein referred to as "Lacework"), desires to acquire, and each undersigned inventor desires to grant to Lacework, the entire worldwide right, title, and interest in and to the Invention and in and to any and all patent applications and patents directed thereto;

Now, therefore, for good and valuable consideration, the receipt and sufficiency thereof being hereby acknowledged, I hereby sell or have sold, assign or have assigned, and otherwise transfer or have transferred to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the Invention, the above-identified United States patent application, and any and all other patent applications and patents for the Invention which may be applied for or granted therefor in the United States and in all foreign countries and jurisdictions, including all divisions, continuations, reissues, reexaminations, renewals, extensions, counterparts, substitutes, and extensions thereof, and all rights of priority resulting from the filing of such applications and granting of such patents. In addition, I hereby authorize and request the Director of the United States Patent and Trademark Office to issue any United States Patent, and foreign patent authorities to issue any foreign patent, granted for the Invention, to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the same to be held and enjoyed by the ASSIGNEE, its successors, legal representatives, and assigns to the full end of the terms for which any and all such patents may be granted, as fully and entirely as would have been held and enjoyed by me had this Assignment not been made; and I agree to execute any and all documents and instruments and perform all lawful acts reasonably related to recording this Assignment or perfecting title to the Invention and all related patents and applications, in the ASSIGNEE, its successors, legal representatives, and assigns, whenever requested by the ASSIGNEE, its successors, legal representatives, or assigns.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00327

I acknowledge my prior and ongoing obligations to sell, assign, and transfer my rights under this Assignment to the ASSIGNEE and am unaware of any reason why I may not have the full and unencumbered right to sell, assign, and transfer my rights hereby sold, assigned, and transferred, and have not executed, and will not execute, any document or instrument in conflict herewith. I also hereby grant the ASSIGNEE, its successors, legal representatives, and assigns, the right to insert in this Assignment any further identification (including, but not limited to, patent Application Number) which may be necessary or desirable for recordation of this Assignment. This Assignment is governed by the substantive laws of the State of Delaware, and any disputes will be resolved in a Delaware state court or federal court sited in Delaware.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

Signature: / Vikram Kapoor / Date: 06/08/2022

(1) Legal Name of Inventor: **VIKRAM KAPOOR**

Signature: / Harish kumar Bharat Singh / Date: 06/06/2022

(2) Legal Name of Inventor: **HARISH KUMAR BHARAT SINGH**

Signature: / Weifei Zeng / Date: 06/06/2022

(3) Legal Name of Inventor: **WEIFEI ZENG**

Signature: / Vimalkumar Jeyakumar / Date: 06/08/2022

(4) Legal Name of Inventor: **VIMALKUMAR JEYAKUMAR**

Signature: / Theron Tock / Date: 06/09/2022

(5) Legal Name of Inventor: **THERON TOCK**

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00328

Signature: / Ying Xie / Date: 06/07/2022

(6) Legal Name of Inventor: **YING XIE**

Signature: / Yijou Chen / Date: 06/06/2022

(7) Legal Name of Inventor: **YIJOU CHEN**

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00329

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	UNKNOWN
Filing Date	HEREWITH
First Named Inventor	VIKRAM KAPOOR
Title	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems
Art Unit	UNKNOWN
Examiner Name	UNKNOWN
Attorney Docket Number	L0040B3CIP6C1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Edward Lenart/	Date (Optional)	2022-07-06
Name	Edward Lenart	Registration Number	63665
Title (if Applicant is a juristic entity)	Patent Practitioner for Applicant		
Applicant Name (if Applicant is a juristic entity)	Lacework, Inc.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 182115

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Lacework, Inc.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/Michael Moore/	Date (Optional)	
Name	Michael Moore		
Title	Vice President, Privacy and Intellectual Property		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	VIKRAM		KAPOOR	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	CUPERTINO	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	State/Province	CA
Postal Code	95002	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	HARISH KUMAR BHARAT		SINGH	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	PLEASANTON	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	State/Province	CA
Postal Code	95002	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	WEIFEI		ZENG	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

City	SUNNYVALE	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	State/Province	CA
Postal Code	95002	Country	US

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	VIMALKUMAR		JEYAKUMAR	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	LOS ALTOS	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	State/Province	CA
Postal Code	95002	Country	US

Inventor 5 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	THERON		TOCK	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	MOUNTAIN VIEW	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	State/Province	CA
Postal Code	95002	Country	US

Inventor 6 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	YING		XIE	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	CUPERTINO	State/Province	CA	Country of Residence	US

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	**State/Province**	CA
Postal Code	95002	**Country** i	US

Inventor 7 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	YIJOU		CHEN	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	CUPERTINO	**State/Province**	CA	**Country of Residence** i	US

Mailing Address of Inventor:

Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	**State/Province**	CA
Postal Code	95002	**Country** i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	182115		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems		
Attorney Docket Number	L0040B3CIP6C1	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	59	**Suggested Figure for Publication (if any)**	

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	182115		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	17836813	2022-06-09

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
17836813	Continuation in part of	17196887	2021-03-09
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17196887	Continuation of	16459207	2019-07-01	10986114	2021-04-20

Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16459207	Continuation of	16134821	2018-09-18	10419469	2019-09-17

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
16134821	Claims benefit of provisional	62650971	2018-03-30
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
16134821	Claims benefit of provisional	62590986	2017-11-27
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
17836813	Claims benefit of provisional	63240818	2021-09-03
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	63240818	2021-09-03
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	LACEWORK, INC.		
Mailing Address Information For Applicant:			
Address 1	6201 AMERICA CENTER DRIVE		
Address 2	SUITE 200		
City	SAN JOSE	**State/Province**	CA
Country	US	Postal Code	95002
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Edward Lenart/			Date (YYYY-MM-DD)	2022-07-06
First Name	Edward J.	Last Name	Lenart	Registration Number	63665

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0040B3CIP6C1
	Application Number	
Title of Invention	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00343

USING ACTIVITY MONITORED BY MULTIPLE DATA SOURCES TO IDENTIFY SHADOW SYSTEMS

BRIEF DESCRIPTION OF THE DRAWINGS

[0001] The accompanying drawings illustrate various embodiments and are a part of the specification. The illustrated embodiments are merely examples and do not limit the scope of the disclosure. Throughout the drawings, identical or similar reference numbers designate identical or similar elements.

[0002] Fig. 1A shows an illustrative configuration in which a data platform is configured to perform various operations with respect to a cloud environment that includes a plurality of compute assets.

[0003] Fig. 1B shows an illustrative implementation of the configuration of Fig. 1A.

[0004] Fig. 1C illustrates an example computing device.

[0005] Fig. 1D illustrates an example of an environment in which activities that occur within datacenters are modeled.

[0006] Fig. 2A illustrates an example of a process, used by an agent, to collect and report information about a client.

[0007] Fig. 2B illustrates a 5-tuple of data collected by an agent, physically and logically.

[0008] Fig. 2C illustrates a portion of a polygraph.

[0009] Fig. 2D illustrates a portion of a polygraph.

[0010] Fig. 2E illustrates an example of a communication polygraph.

[0011] Fig. 2F illustrates an example of a polygraph.

[0012] Fig. 2G illustrates an example of a polygraph as rendered in an interface.

[0013] Fig. 2H illustrates an example of a portion of a polygraph as rendered in an interface.

[0014] Fig. 2I illustrates an example of a portion of a polygraph as rendered in an interface.

[0015] Fig. 2J illustrates an example of a portion of a polygraph as rendered in an interface.

[0016] Fig. 2K illustrates an example of a portion of a polygraph as rendered in an interface.

[0017] Fig. 2L illustrates an example of an insider behavior graph as rendered in an interface.

[0018] Fig. 2M illustrates an example of a privilege change graph as rendered in an interface.

[0019] Fig. 2N illustrates an example of a user login graph as rendered in an interface.

[0020] Fig. 2O illustrates an example of a machine server graph as rendered in an interface.

[0021] Fig. 3A illustrates an example of a process for detecting anomalies in a network environment.

[0022] Fig. 3B depicts a set of example processes communicating with other processes.

[0023] Fig. 3C depicts a set of example processes communicating with other processes.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00344

[0024] Fig. 3D depicts a set of example processes communicating with other processes.

[0025] Fig. 3E depicts two pairs of clusters.

[0026] Fig. 3F is a representation of a user logging into a first machine, then into a second machine from the first machine, and then making an external connection.

[0027] Fig. 3G is an alternate representation of actions occurring in Fig. 3F.

[0028] Fig. 3H illustrates an example of a process for performing extended user tracking.

[0029] Fig. 3I is a representation of a user logging into a first machine, then into a second machine from the first machine, and then making an external connection.

[0030] Fig. 3J illustrates an example of a process for performing extended user tracking.

[0031] Fig. 3K illustrates example records.

[0032] Fig. 3L illustrates example output from performing an ssh connection match.

[0033] Fig. 3M illustrates example records.

[0034] Fig. 3N illustrates example records.

[0035] Fig. 3O illustrates example records.

[0036] Fig. 3P illustrates example records.

[0037] Fig. 3Q illustrates an adjacency relationship between two login sessions.

[0038] Fig. 3R illustrates example records.

[0039] Fig. 3S illustrates an example of a process for detecting anomalies.

[0040] Fig. 4A illustrates a representation of an embodiment of an insider behavior graph.

[0041] Fig. 4B illustrates an embodiment of a portion of an insider behavior graph.

[0042] Fig. 4C illustrates an embodiment of a portion of an insider behavior graph.

[0043] Fig. 4D illustrates an embodiment of a portion of an insider behavior graph.

[0044] Fig. 4E illustrates a representation of an embodiment of a user login graph.

[0045] Fig. 4F illustrates an example of a privilege change graph.

[0046] Fig. 4G illustrates an example of a privilege change graph.

[0047] Fig. 4H illustrates an example of a user interacting with a portion of an interface.

[0048] Fig. 4I illustrates an example of a dossier for an event.

[0049] Fig. 4J illustrates an example of a dossier for a domain.

[0050] Fig. 4K depicts an example of an Entity Join graph by FilterKey and FilterKey Group (implicit join).

[0051] Fig. 4L illustrates an example of a process for dynamically generating and executing a query.

[0052] Fig. 5A sets forth a system for providing many of the features described herein for user devices as a distributed edge service in accordance with some embodiments of the present disclosure.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00345

[0053] Fig. 5B sets forth a system for providing many of the features described herein for user devices as a distributed edge service in accordance with some embodiments of the present disclosure.

[0054] Fig. 6 sets forth a flow chart illustrating an example method of detecting deviations from typical user behavior in accordance with some embodiments of the present disclosure.

[0055] Fig. 7 sets forth a flow chart illustrating an additional example method of detecting deviations from typical behavior in accordance with some embodiments of the present disclosure.

[0056] Fig. 8 sets forth a flow chart illustrating an additional example method of detecting deviations from typical behavior in accordance with some embodiments of the present disclosure.

[0057] Fig. 9 sets forth a flow chart illustrating an example method of detecting a location of a user device in accordance with some embodiments of the present disclosure.

[0058] Fig. 10 sets forth a flow chart illustrating an additional example method of detecting a location of a user device in accordance with some embodiments of the present disclosure.

[0059] Fig. 11 sets forth a flow chart illustrating an additional example method of detecting a location of a user device in accordance with some embodiments of the present disclosure.

[0060] Fig. 12 sets forth a flow chart illustrating an example method of detecting deviation from normal behavior of a device in accordance with some embodiments of the present disclosure.

[0061] Fig. 13 sets forth a flow chart illustrating an additional example method of detecting deviation from normal behavior of a device according to embodiments of the present disclosure.

[0062] Fig. 14 sets forth a flow chart illustrating an additional example method of detecting deviation from normal behavior of a device in some embodiments of the present disclosure.

[0063] Fig. 15A sets forth an example of a user-specific polygraph in accordance with some embodiments of the present disclosure.

[0064] Fig. 15B sets forth an example of a user-specific polygraph in accordance with some embodiments of the present disclosure.

[0065] Fig. 16 sets forth a flowchart of an example method of using activity monitored by multiple data sources to identify shadow systems according to some embodiments of the present disclosure.

[0066] Fig. 17 sets forth a flowchart of another example method of using activity monitored by multiple data sources to identify shadow systems according to some embodiments of the present disclosure.

[0067] Fig. 18 sets forth a flowchart of another example method of using activity monitored by multiple data sources to identify shadow systems according to some embodiments of the present disclosure.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00346

[0068] Fig. 19 sets forth a flowchart of another example method of using activity monitored by multiple data sources to identify shadow systems according to some embodiments of the present disclosure.

[0069] Fig. 20 sets forth an example polygraph for identifying shadow systems according to some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0070] Various illustrative embodiments are described herein with reference to the accompanying drawings. It will, however, be evident that various modifications and changes may be made thereto, and additional embodiments may be implemented, without departing from the scope of the invention as set forth in the claims. For example, certain features of one embodiment described herein may be combined with or substituted for features of another embodiment described herein. The description and drawings are accordingly to be regarded in an illustrative rather than a restrictive sense.

[0071] Fig. 1A shows an illustrative configuration 10 in which a data platform 12 is configured to perform various operations with respect to a cloud environment 14 that includes a plurality of compute assets 16-1 through 16-N (collectively "compute assets 16). For example, data platform 12 may include data ingestion resources 18 configured to ingest data from cloud environment 14 into data platform 12, data processing resources 20 configured to perform data processing operations with respect to the data, user interface resources 22 configured to provide one or more external users and/or compute resources (e.g., computing device 24) with access to an output of data processing resources 20. Each of these resources are described in detail herein.

[0072] Cloud environment 14 may include any suitable network-based computing environment as may serve a particular application. For example, cloud environment 14 may be implemented by one or more compute resources provided and/or otherwise managed by one or more cloud service providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and/or any other cloud service provider configured to provide public and/or private access to network-based compute resources.

[0073] Compute assets 16 may include, but are not limited to, containers (e.g., container images, deployed and executing container instances, etc.), virtual machines, workloads, applications, processes, physical machines, compute nodes, clusters of compute nodes, software runtime environments (e.g., container runtime environments), and/or any other virtual and/or physical compute resource that may reside in and/or be executed by one or more computer resources in

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00347

cloud environment 14. In some examples, one or more compute assets 16 may reside in one or more datacenters.

[0074] A compute asset 16 may be associated with (e.g., owned, deployed, or managed by) a particular entity, such as a customer or client of cloud environment 14 and/or data platform 12. Accordingly, for purposes of the discussion herein, cloud environment 14 may be used by one or more entities.

[0075] Data platform 12 may be configured to perform one or more data security monitoring and/or remediation services, compliance monitoring services, anomaly detection services, DevOps services, compute asset management services, and/or any other type of data analytics service as may serve a particular implementation. Data platform 12 may be managed or otherwise associated with any suitable data platform provider, such as a provider of any of the data analytics services described herein. The various resources included in data platform 12 may reside in the cloud and/or be located on-premises and be implemented by any suitable combination of physical and/or virtual compute resources, such as one or more computing devices, microservices, applications, etc.

[0076] Data ingestion resources 18 may be configured to ingest data from cloud environment 14 into data platform 12. This may be performed in various ways, some of which are described in detail herein. For example, as illustrated by arrow 26, data ingestion resources 18 may be configured to receive the data from one or more agents deployed within cloud environment 14, utilize an event streaming platform (e.g., Kafka) to obtain the data, and/or pull data (e.g., configuration data) from cloud environment 14. In some examples, data ingestion resources 18 may obtain the data using one or more agentless configurations.

[0077] The data ingested by data ingestion resources 18 from cloud environment 14 may include any type of data as may serve a particular implementation. For example, the data may include data representative of configuration information associated with compute assets 16, information about one or more processes running on compute assets 16, network activity information, information about events (creation events, modification events, communication events, user-initiated events, etc.) that occur with respect to compute assets 16, etc. In some examples, the data may or may not include actual customer data processed or otherwise generated by compute assets 16.

[0078] As illustrated by arrow 28, data ingestion resources 18 may be configured to load the data ingested from cloud environment 14 into a data store 30. Data store 30 is illustrated in Fig. 1A as being separate from and communicatively coupled to data platform 12. However, in some alternative embodiments, data store 30 is included within data platform 12.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00348

[0079] Data store 30 may be implemented by any suitable data warehouse, data lake, data mart, and/or other type of database structure as may serve a particular implementation. Such data stores may be proprietary or may be embodied as vendor provided products or services such as, for example, Snowflake, Google BigQuery, Druid, Amazon Redshift, IBM Db2, Dremio, Databricks Lakehouse Platform, Cloudera, Azure Synapse Analytics, and others.

[0080] Although the examples described herein largely relate to embodiments where data is collected from agents and ultimately stored in a data store such as those provided by Snowflake, in other embodiments data that is collected from agents and other sources may be stored in different ways. For example, data that is collected from agents and other sources may be stored in a data warehouse, data lake, data mart, and/or any other data store.

[0081] A data warehouse may be embodied as an analytic database (e.g., a relational database) that is created from two or more data sources. Such a data warehouse may be leveraged to store historical data, often on the scale of petabytes. Data warehouses may have compute and memory resources for running complicated queries and generating reports. Data warehouses may be the data sources for business intelligence ('BI') systems, machine learning applications, and/or other applications. By leveraging a data warehouse, data that has been copied into the data warehouse may be indexed for good analytic query performance, without affecting the write performance of a database (e.g., an Online Transaction Processing ('OLTP') database). Data warehouses also enable the joining data from multiple sources for analysis. For example, a sales OLTP application probably has no need to know about the weather at various sales locations, but sales predictions could take advantage of that data. By adding historical weather data to a data warehouse, it would be possible to factor it into models of historical sales data.

[0082] Data lakes, which store files of data in their native format, may be considered as "schema on read" resources. As such, any application that reads data from the lake may impose its own types and relationships on the data. Data warehouses, on the other hand, are "schema on write," meaning that data types, indexes, and relationships are imposed on the data as it is stored in an enterprise data warehouse (EDW). "Schema on read" resources may be beneficial for data that may be used in several contexts and poses little risk of losing data. "Schema on write" resources may be beneficial for data that has a specific purpose, and good for data that must relate properly to data from other sources. Such data stores may include data that is encrypted using homomorphic encryption, data encrypted using privacy-preserving encryption, smart contracts, non-fungible tokens, decentralized finance, and other techniques.

[0083] Data marts may contain data oriented towards a specific business line whereas data warehouses contain enterprise-wide data. Data marts may be dependent on a data warehouse, independent of the data warehouse (e.g., drawn from an operational database or external source),

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00349

or a hybrid of the two. In embodiments described herein, different types of data stores (including combinations thereof) may be leveraged.

[0084] Data processing resources 20 may be configured to perform various data processing operations with respect to data ingested by data ingestion resources 18, including data ingested and stored in data store 30. For example, data processing resources 20 may be configured to perform one or more data security monitoring and/or remediation operations, compliance monitoring operations, anomaly detection operations, DevOps operations, compute asset management operations, and/or any other type of data analytics operation as may serve a particular implementation. Various examples of operations performed by data processing resources 20 are described herein.

[0085] As illustrated by arrow 32, data processing resources 20 may be configured to access data in data store 30 to perform the various operations described herein. In some examples, this may include performing one or more queries with respect to the data stored in data store 30. Such queries may be generated using any suitable query language.

[0086] In some examples, the queries provided by data processing resources 20 may be configured to direct data store 30 to perform one or more data analytics operations with respect to the data stored within data store 30. These data analytics operations may be with respect to data specific to a particular entity (e.g., data residing in one or more silos within data store 30 that are associated with a particular customer) and/or data associated with multiple entities. For example, data processing resources 20 may be configured to analyze data associated with a first entity and use the results of the analysis to perform one or more operations with respect to a second entity.

[0087] One or more operations performed by data processing resources 20 may be performed periodically according to a predetermined schedule. For example, one or more operations may be performed by processing resources 20 every hour or any other suitable time interval. Additionally or alternatively, one or more operations performed by data processing resources 20 may be performed in substantially real-time (or near real-time) as data is ingested into data platform 12. In this manner, the results of such operations (e.g., one or more detected anomalies in the data) may be provided to one or more external entities (e.g., computing device 24 and/or one or more users) in substantially real-time and/or in near real-time.

[0088] User interface resources 22 may be configured to perform one or more user interface operations, examples of which are described herein. For example, user interface resources 22 may be configured to present one or more results of the data processing performed by data processing resources 20 to one or more external entities (e.g., computing device 24 and/or one or more users), as illustrated by arrow 34. As illustrated by arrow 36, user interface resources 22 may access data in data store 30 to perform the one or more user interface operations

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00350

[0089] Fig. 1B illustrates an implementation of configuration 10 in which an agent 38 (e.g., agent 38-1 through agent 38-N) is installed on each of compute assets 16. As used herein, an agent may include a self-contained binary and/or other type of code or application that can be run on any appropriate platforms, including within containers and/or other virtual compute assets. Agents 38 may monitor the nodes on which they execute for a variety of different activities, including but not limited to, connection, process, user, machine, and file activities. In some examples, agents 38 can be executed in user space, and can use a variety of kernel modules (e.g., auditd, iptables, netfilter, pcap, etc.) to collect data. Agents can be implemented in any appropriate programming language, such as C or Golang, using applicable kernel APIs.

[0090] Agents 38 may be deployed in any suitable manner. For example, an agent 38 may be deployed as a containerized application or as part of a containerized application. As described herein, agents 38 may selectively report information to data platform 12 in varying amounts of detail and/or with variable frequency.

[0091] Also shown in Fig. 1B is a load balancer 40 configured to perform one or more load balancing operations with respect to data ingestion operations performed by data ingestion resources 18 and/or user interface operations performed by user interface resources 22. Load balancer 40 is shown to be included in data platform 12. However, load balancer 40 may alternatively be located external to data platform 12. Load balancer 40 may be implemented by any suitable microservice, application, and/or other computing resources. In some alternative examples, data platform 12 may not utilize a load balancer such as load balancer 40.

[0092] Also shown in Fig. 1B is long term storage 42 with which data ingestion resources may interface, as illustrated by arrow 44. Long term storage 42 may be implemented by any suitable type of storage resources, such as cloud-based storage (e.g., AWS S3, etc.) and/or on-premises storage and may be used by data ingestion resources 18 as part of the data ingestion process. Examples of this are described herein. In some examples, data platform 12 may not utilize long term storage 42.

[0093] The embodiments described herein can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the principles described herein. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a

specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0094] In some examples, a non-transitory computer-readable medium storing computer-readable instructions may be provided in accordance with the principles described herein. The instructions, when executed by a processor of a computing device, may direct the processor and/or computing device to perform one or more operations, including one or more of the operations described herein. Such instructions may be stored and/or transmitted using any of a variety of known computer-readable media.

[0095] A non-transitory computer-readable medium as referred to herein may include any non-transitory storage medium that participates in providing data (e.g., instructions) that may be read and/or executed by a computing device (e.g., by a processor of a computing device). For example, a non-transitory computer-readable medium may include, but is not limited to, any combination of non-volatile storage media and/or volatile storage media. Exemplary non-volatile storage media include, but are not limited to, read-only memory, flash memory, a solid-state drive, a magnetic storage device (e.g. a hard disk, a floppy disk, magnetic tape, etc.), ferroelectric random-access memory ("RAM"), and an optical disc (e.g., a compact disc, a digital video disc, a Blu-ray disc, etc.). Exemplary volatile storage media include, but are not limited to, RAM (e.g., dynamic RAM).

[0096] Fig. 1C illustrates an example computing device 50 that may be specifically configured to perform one or more of the processes described herein. Any of the systems, microservices, computing devices, and/or other components described herein may be implemented by computing device 50.

[0097] As shown in Fig. 1C, computing device 50 may include a communication interface 52, a processor 54, a storage device 56, and an input/output ("I/O") module 58 communicatively connected one to another via a communication infrastructure 60. While an exemplary computing device 50 is shown in Fig. 1C, the components illustrated in Fig. 1C are not intended to be limiting. Additional or alternative components may be used in other embodiments. Components of computing device 50 shown in Fig. 1C will now be described in additional detail.

[0098] Communication interface 52 may be configured to communicate with one or more computing devices. Examples of communication interface 52 include, without limitation, a wired network interface (such as a network interface card), a wireless network interface (such as a wireless network interface card), a modem, an audio/video connection, and any other suitable interface.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00352

[0099] Processor 54 generally represents any type or form of processing unit capable of processing data and/or interpreting, executing, and/or directing execution of one or more of the instructions, processes, and/or operations described herein. Processor 54 may perform operations by executing computer-executable instructions 62 (e.g., an application, software, code, and/or other executable data instance) stored in storage device 56.

[00100] Storage device 56 may include one or more data storage media, devices, or configurations and may employ any type, form, and combination of data storage media and/or device. For example, storage device 56 may include, but is not limited to, any combination of the non-volatile media and/or volatile media described herein. Electronic data, including data described herein, may be temporarily and/or permanently stored in storage device 56. For example, data representative of computer-executable instructions 62 configured to direct processor 54 to perform any of the operations described herein may be stored within storage device 56. In some examples, data may be arranged in one or more databases residing within storage device 56.

[00101] I/O module 58 may include one or more I/O modules configured to receive user input and provide user output. I/O module 58 may include any hardware, firmware, software, or combination thereof supportive of input and output capabilities. For example, I/O module 58 may include hardware and/or software for capturing user input, including, but not limited to, a keyboard or keypad, a touchscreen component (e.g., touchscreen display), a receiver (e.g., an RF or infrared receiver), motion sensors, and/or one or more input buttons.

[00102] I/O module 58 may include one or more devices for presenting output to a user, including, but not limited to, a graphics engine, a display (e.g., a display screen), one or more output drivers (e.g., display drivers), one or more audio speakers, and one or more audio drivers. In certain embodiments, I/O module 58 is configured to provide graphical data to a display for presentation to a user. The graphical data may be representative of one or more graphical user interfaces and/or any other graphical content as may serve a particular implementation.

[00103] Fig. 1D illustrates an example implementation 100 of configuration 10. As such, one more components shown in Fig. 1D may implement one or more components shown in Fig. 1A and/or Fig. 1B. In particular, implementation 100 illustrates an environment in which activities that occur within datacenters are modeled using data platform 12. Using techniques described herein, a baseline of datacenter activity can be modeled, and deviations from that baseline can be identified as anomalous. Anomaly detection can be beneficial in a security context, a compliance context, an asset management context, a DevOps context, and/or any other data analytics context as may serve a particular implementation.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00353

[00104] Two example datacenters (104 and 106) are shown in Fig. 1D, and are associated with (e.g., belong to) entities named entity A and entity B, respectively. A datacenter may include dedicated equipment (e.g., owned and operated by entity A, or owned/leased by entity A and operated exclusively on entity A's behalf by a third party). A datacenter can also include cloud-based resources, such as infrastructure as a service (IaaS), platform as a service (PaaS), and/or software as a service (SaaS) elements. The techniques described herein can be used in conjunction with multiple types of datacenters, including ones wholly using dedicated equipment, ones that are entirely cloud-based, and ones that use a mixture of both dedicated equipment and cloud-based resources.

[00105] Both datacenter 104 and datacenter 106 include a plurality of nodes, depicted collectively as set of nodes 108 and set of nodes 110, respectively, in Fig. 1D. These nodes may implement compute assets 16. Installed on each of the nodes are in-server / in-virtual machine (VM) / embedded in IoT device agents (e.g., agent 112), which are configured to collect data and report it to data platform 12 for analysis. As described herein, agents may be small, self-contained binaries that can be run on any appropriate platforms, including virtualized ones (and, as applicable, within containers). Agents may monitor the nodes on which they execute for a variety of different activities, including: connection, process, user, machine, and file activities. Agents can be executed in user space, and can use a variety of kernel modules (e.g., auditd, iptables, netfilter, pcap, etc.) to collect data. Agents can be implemented in any appropriate programming language, such as C or Golang, using applicable kernel APIs.

[00106] As described herein, agents can selectively report information to data platform 12 in varying amounts of detail and/or with variable frequency. As is also described herein, the data collected by agents may be used by data platform 12 to create polygraphs, which are graphs of logical entities, connected by behaviors. In some embodiments, agents report information directly to data platform 12. In other embodiments, at least some agents provide information to a data aggregator, such as data aggregator 114, which in turn provides information to data platform 12. The functionality of a data aggregator can be implemented as a separate binary or other application (distinct from an agent binary), and can also be implemented by having an agent execute in an "aggregator mode" in which the designated aggregator node acts as a Layer 7 proxy for other agents that do not have access to data platform 12. Further, a chain of multiple aggregators can be used, if applicable (e.g., with agent 112 providing data to data aggregator 114, which in turn provides data to another aggregator (not pictured) which provides data to data platform 12). An example way to implement an aggregator is through a program written in an appropriate language, such as C or Golang.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00354

[00107] Use of an aggregator can be beneficial in sensitive environments (e.g., involving financial or medical transactions) where various nodes are subject to regulatory or other architectural requirements (e.g., prohibiting a given node from communicating with systems outside of datacenter 104). Use of an aggregator can also help to minimize security exposure more generally. As one example, by limiting communications with data platform 12 to data aggregator 114, individual nodes in nodes 108 need not make external network connections (e.g., via Internet 124), which can potentially expose them to compromise (e.g., by other external devices, such as device 118, operated by a criminal). Similarly, data platform 12 can provide updates, configuration information, etc., to data aggregator 114 (which in turn distributes them to nodes 108), rather than requiring nodes 108 to allow incoming connections from data platform 12 directly.

[00108] Another benefit of an aggregator model is that network congestion can be reduced (e.g., with a single connection being made at any given time between data aggregator 114 and data platform 12, rather than potentially many different connections being open between various of nodes 108 and data platform 12). Similarly, network consumption can also be reduced (e.g., with the aggregator applying compression techniques/bundling data received from multiple agents).

[00109] One example way that an agent (e.g., agent 112, installed on node 116) can provide information to data aggregator 114 is via a REST API, formatted using data serialization protocols such as Apache Avro. One example type of information sent by agent 112 to data aggregator 114 is status information. Status information may be sent by an agent periodically (e.g., once an hour or once any other predetermined amount of time). Alternatively, status information may be sent continuously or in response to occurrence of one or more events. The status information may include, but is not limited to, a. an amount of event backlog (in bytes) that has not yet been transmitted, b. configuration information, c. any data loss period for which data was dropped, d. a cumulative count of errors encountered since the agent started, e. version information for the agent binary, and/or f. cumulative statistics on data collection (e.g., number of network packets processed, new processes seen, etc.).

[00110] A second example type of information that may be sent by agent 112 to data aggregator 114 is event data (described in more detail herein), which may include a UTC timestamp for each event. As applicable, the agent can control the amount of data that it sends to the data aggregator in each call (e.g., a maximum of 10MB) by adjusting the amount of data sent to manage the conflicting goals of transmitting data as soon as possible, and maximizing throughput. Data can also be compressed or uncompressed by the agent (as applicable) prior to sending the data.

[00111] Each data aggregator may run within a particular customer environment. A data aggregator (e.g., data aggregator 114) may facilitate data routing from many different agents

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00355

(e.g., agents executing on nodes 108) to data platform 12. In various embodiments, data aggregator 114 may implement a SOCKS 5 caching proxy through which agents can connect to data platform 12. As applicable, data aggregator 114 can encrypt (or otherwise obfuscate) sensitive information prior to transmitting it to data platform 12, and can also distribute key material to agents which can encrypt the information (as applicable). Data aggregator 114 may include a local storage, to which agents can upload data (e.g., pcap packets). The storage may have a key-value interface. The local storage can also be omitted, and agents configured to upload data to a cloud storage or other storage area, as applicable. Data aggregator 114 can, in some embodiments, also cache locally and distribute software upgrades, patches, or configuration information (e.g., as received from data platform 12).

[00112] Various examples associated with agent data collection and reporting will now be described.

[00113] In the following example, suppose that a user (e.g., a network administrator) at entity A (hereinafter "user A") has decided to begin using the services of data platform 12. In some embodiments, user A may access a web frontend (e.g., web app 120) using a computer 126 and enrolls (on behalf of entity A) an account with data platform 12. After enrollment is complete, user A may be presented with a set of installers, pre-built and customized for the environment of entity A, that user A can download from data platform 12 and deploy on nodes 108. Examples of such installers include, but are not limited to, a Windows executable file, an iOS app, a Linux package (e.g., .deb or .rpm), a binary, or a container (e.g., a Docker container). When a user (e.g., a network administrator) at entity B (hereinafter "user B") also signs up for the services of data platform 12, user B may be similarly presented with a set of installers that are pre-built and customized for the environment of entity B.

[00114] User A deploys an appropriate installer on each of nodes 108 (e.g., with a Windows executable file deployed on a Windows-based platform or a Linux package deployed on a Linux platform, as applicable). As applicable, the agent can be deployed in a container. Agent deployment can also be performed using one or more appropriate automation tools, such as Chef, Puppet, Salt, and Ansible. Deployment can also be performed using managed/hosted container management/orchestration frameworks such as Kubernetes, Mesos, and/or Docker Swarm.

[00115] In various embodiments, the agent may be installed in the user space (i.e., is not a kernel module), and the same binary is executed on each node of the same type (e.g., all Windows-based platforms have the same Windows-based binary installed on them). An illustrative function of an agent, such as agent 112, is to collect data (e.g., associated with node 116) and report it (e.g., to data aggregator 114). Other tasks that can be performed by agents include data configuration and upgrading.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00356

[00116] One approach to collecting data as described herein is to collect virtually all information available about a node (and, e.g., the processes running on it). Alternatively, the agent may monitor for network connections, and then begin collecting information about processes associated with the network connections, using the presence of a network packet associated with a process as a trigger for collecting additional information about the process. As an example, if a user of node 116 executes an application, such as a calculator application, which does not typically interact with the network, no information about use of that application may be collected by agent 112 and/or sent to data aggregator 114. If, however, the user of node 116 executes an ssh command (e.g., to ssh from node 116 to node 122), agent 112 may collect information about the process and provide associated information to data aggregator 114. In various embodiments, the agent may always collect/report information about certain events, such as privilege escalation, irrespective of whether the event is associated with network activity.

[00117] An approach to collecting information (e.g., by an agent) is as follows, and described in conjunction with process 200 depicted in Fig. 2A. An agent (e.g., agent 112) monitors its node (e.g., node 116) for network activity. One example way that agent 112 can monitor node 116 for network activity is by using a network packet capture tool (e.g., listening using libpcap). As packets are received (201), the agent obtains and maintains (e.g., in an in-memory cache) connection information associated with the network activity (202). Examples of such information include DNS query/response, TCP, UDP, and IP information.

[00118] The agent may also determine a process associated with the network connection (203). One example approach is for the agent to use a kernel network diagnostic API (e.g., netlink_diag) to obtain inode/process information from the kernel. Another example approach is for the agent to scan using netstat (e.g., on /proc/net/tcp, /proc/net/tcp6, /proc/net/udp, and /proc/net/udp6) to obtain sockets and relate them to processes. Information such as socket state (e.g., whether a socket is connected, listening, etc.) can also be collected by the agent.

[00119] One way an agent can obtain a mapping between a given inode and a process identifier is to scan within the /proc/pid directory. For each of the processes currently running, the agent examines each of their file descriptors. If a file descriptor is a match for the inode, the agent can determine that the process associated with the file descriptor owns the inode. Once a mapping is determined between an inode and a process identifier, the mapping is cached. As additional packets are received for the connection, the cached process information is used (rather than a new search being performed).

[00120] In some cases, exhaustively scanning for an inode match across every file descriptor may not be feasible (e.g., due to CPU limitations). In various embodiments, searching through file descriptors is accordingly optimized. User filtering is one example of such an optimization. A

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00357

given socket is owned by a user. Any processes associated with the socket will be owned by the same user as the socket. When matching an inode (identified as relating to a given socket) against processes, the agent can filter through the processes and only examine the file descriptors of processes sharing the same user owner as the socket. In various embodiments, processes owned by root are always searched against (e.g., even when user filtering is employed).

[00121] Another example of an optimization is to prioritize searching the file descriptors of certain processes over others. One such prioritization is to search through the subdirectories of /proc/ starting with the youngest process. One approximation of such a sort order is to search through /proc/ in reverse order (e.g., examining highest numbered processes first). Higher numbered processes are more likely to be newer (i.e., not long-standing processes), and thus more likely to be associated with new connections (i.e., ones for which inode-process mappings are not already cached). In some cases, the most recently created process may not have the highest process identifier (e.g., due to the kernel wrapping through process identifiers).

[00122] Another example prioritization is to query the kernel for an identification of the most recently created process and to search in a backward order through the directories in /proc/ (e.g., starting at the most recently created process and working backwards, then wrapping to the highest value (e.g., 32768) and continuing to work backward from there). An alternate approach is for the agent to keep track of the newest process that it has reported information on (e.g., to data aggregator 114), and begin its search of /proc/ in a forward order starting from the PID of that process.

[00123] Another example prioritization is to maintain, for each user actively using node 116, a list of the five (or any other number) most recently active processes. Those processes are more likely than other processes (less active, or passive) on node 116 to be involved with new connections, and can thus be searched first. For many processes, lower valued file descriptors tend to correspond to non-sockets (e.g., stdin, stdout, stderr). Yet another optimization is to preferentially search higher valued file descriptors (e.g., across processes) over lower valued file descriptors (that are less likely to yield matches).

[00124] In some cases, while attempting to locate a process identifier for a given inode, an agent may encounter a socket that does not correspond to the inode being matched against and is not already cached. The identity of that socket (and its corresponding inode) can be cached, once discovered, thus removing a future need to search for that pair.

[00125] In some cases, a connection may terminate before the agent is able to determine its associated process (e.g., due to a very short-lived connection, due to a backlog in agent processing, etc.). One approach to addressing such a situation is to asynchronously collect information about the connection using the audit kernel API, which streams information to user

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00358

space. The information collected from the audit API (which can include PID/inode information) can be matched by the agent against pcap/inode information. In some embodiments, the audit API is always used, for all connections. However, due to CPU utilization considerations, use of the audit API can also be reserved for short/otherwise problematic connections (and/or omitted, as applicable).

[00126] Once the agent has determined which process is associated with the network connection (203), the agent can then collect additional information associated with the process (204). As will be described in more detail below, some of the collected information may include attributes of the process (e.g., a process parent hierarchy, and an identification of a binary associated with the process). As will also be described in more detail below, other of the collected information is derived (e.g., session summarization data and hash values).

[00127] The collected information is then transmitted (205), e.g., by an agent (e.g., agent 112) to a data aggregator (e.g., data aggregator 114), which in turn provides the information to data platform 12. In some embodiments, all information collected by an agent may be transmitted (e.g., to a data aggregator and/or to data platform 12). In other embodiments, the amount of data transmitted may be minimized (e.g., for efficiency reasons), using various techniques.

[00128] One approach to minimizing the amount of data flowing from agents (such as agents installed on nodes 108) to data platform 12 is to use a technique of implicit references with unique keys. The keys can be explicitly used by data platform 12 to extract/derive relationships, as necessary, in a data set at a later time, without impacting performance.

[00129] As previously mentioned, some data collected about a process is constant and does not change over the lifetime of the process (e.g., attributes), and some data changes (e.g., statistical information and other variable information). Constant data can be transmitted (210) once, when the agent first becomes aware of the process. And, if any changes to the constant data are detected (e.g., a process changes its parent), a refreshed version of the data can be transmitted (210) as applicable.

[00130] In some examples, an agent may collect variable data (e.g., data that may change over the lifetime of the process). In some examples, variable data can be transmitted (210) at periodic (or other) intervals. Alternatively, variable data may be transmitted in substantially real time as it is collected. In some examples, the variable data may indicate a thread count for a process, a total virtual memory used by the process, the total resident memory used by the process, the total time spent by the process executing in user space, and/or the total time spent by the process executing in kernel space. In some examples, the data may include a hash that may be used within data platform 12 to join process creation time attributes with runtime attributes to construct a full dataset.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00359

[00131] Below are additional examples of data that an agent, such as agent 112, can collect and provide to data platform 12.

[00132] 1. User Data

[00133] Core User Data: user name, UID (user ID), primary group, other groups, home directory.

[00134] Failed Login Data: IP address, hostname, username, count.

[00135] User Login Data: user name, hostname, IP address, start time, TTY (terminal), UID (user ID), GID (group ID), process, end time.

[00136] 2. Machine Data

[00137] Dropped Packet Data: source IP address, destination IP address, destination port, protocol, count.

[00138] Machine Data: hostname, domain name, architecture, kernel, kernel release, kernel version, OS, OS version, OS description, CPU, memory, model number, number of cores, last boot time, last boot reason, tags (e.g., Cloud provider tags such as AWS, GCP, or Azure tags), default router, interface name, interface hardware address, interface IP address and mask, promiscuous mode.

[00139] 3. Network Data

[00140] Network Connection Data: source IP address, destination IP address, source port, destination port, protocol, start time, end time, incoming and outgoing bytes, source process, destination process, direction of connection, histograms of packet length, inter packet delay, session lengths, etc.

[00141] Listening Ports in Server: source IP address, port number, protocol, process.

[00142] Dropped Packet Data: source IP address, destination IP address, destination port, protocol, count.

[00143] Arp Data: source hardware address, source IP address, destination hardware address, destination IP address.

[00144] DNS Data: source IP address, response code, response string, question (request), packet length, final answer (response).

[00145] 4. Application Data

[00146] Package Data: exe path, package name, architecture, version, package path, checksums (MD5, SHA-1, SHA-256), size, owner, owner ID.

[00147] Application Data: command line, PID (process ID), start time, UID (user ID), EUID (effective UID), PPID (parent process ID), PGID (process group ID), SID (session ID), exe path, username, container ID.

[00148] 5. Container Data

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00360

[00149] Container Image Data: image creation time, parent ID, author, container type, repo, (AWS) tags, size, virtual size, image version.

[00150] Container Data: container start time, container type, container name, container ID, network mode, privileged, PID mode, IP addresses, listening ports, volume map, process ID.

[00151] 6. File Data

[00152] File path, file data hash, symbolic links, file creation data, file change data, file metadata, file mode.

[00153] As mentioned above, an agent, such as agent 112, can be deployed in a container (e.g., a Docker container), and can also be used to collect information about containers. Collection about a container can be performed by an agent irrespective of whether the agent is itself deployed in a container or not (as the agent can be deployed in a container running in a privileged mode that allows for monitoring).

[00154] Agents can discover containers (e.g., for monitoring) by listening for container create events (e.g., provided by Docker), and can also perform periodic ordered discovery scans to determine whether containers are running on a node. When a container is discovered, the agent can obtain attributes of the container, e.g., using standard Docker API calls (e.g., to obtain IP addresses associated with the container, whether there's a server running inside, what port it is listening on, associated PIDs, etc.). Information such as the parent process that started the container can also be collected, as can information about the image (which comes from the Docker repository).

[00155] In various embodiments, agents may use namespaces to determine whether a process is associated with a container. Namespaces are a feature of the Linux kernel that can be used to isolate resources of a collection of processes. Examples of namespaces include process ID (PID) namespaces, network namespaces, and user namespaces. Given a process, the agent can perform a fast lookup to determine whether the process is part of the namespace the container claims to be its namespace.

[00156] As mentioned, agents can be configured to report certain types of information (e.g., attribute information) once, when the agent first becomes aware of a process. In various embodiments, such static information is not reported again (or is reported once a day, every twelve hours, etc.), unless it changes (e.g., a process changes its parent, changes its owner, or a SHA-1 of the binary associated with the process changes).

[00157] In contrast to static/attribute information, certain types of data change constantly (e.g., network-related data). In various embodiments, agents are configured to report a list of current connections every minute (or other appropriate time interval). In that connection list will be connections that started in that minute interval, connections that ended in that minute interval,

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00361

and connections that were ongoing throughout the minute interval (e.g., a one minute slice of a one hour connection).

[00158] In various embodiments, agents are configured to collect/compute statistical information about connections (e.g., at the one minute level of granularity and or at any other time interval). Examples of such information include, for the time interval, the number of bytes transferred, and in which direction. Another example of information collected by an agent about a connection is the length of time between packets. For connections that span multiple time intervals (e.g., a seven minute connection), statistics may be calculated for each minute of the connection. Such statistical information (for all connections) can be reported (e.g., to a data aggregator) once a minute.

[00159] In various embodiments, agents are also configured to maintain histogram data for a given network connection, and provide the histogram data (e.g., in the Apache Avro data exchange format) under the Connection event type data. Examples of such histograms include: 1. a packet length histogram (packet_len_hist), which characterizes network packet distribution; 2. a session length histogram (session_len_hist), which characterizes a network session length; 3. a session time histogram (session_time_hist), which characterizes a network session time; and 4. a session switch time histogram (session_switch_time_hist), which characterizes network session switch time (i.e., incoming->outgoing and vice versa). For example, histogram data may include one or more of the following fields: 1. count, which provides a count of the elements in the sampling; 2. sum, which provides a sum of elements in the sampling; 3. max, which provides the highest value element in the sampling; 4. std_dev, which provides the standard deviation of elements in the sampling; and 5. buckets, which provides a discrete sample bucket distribution of sampling data (if applicable).

[00160] For some protocols (e.g., HTTP), typically, a connection is opened, a string is sent, a string is received, and the connection is closed. For other protocols (e.g., NFS), both sides of the connection engage in a constant chatter. Histograms allow data platform 12 to model application behavior (e.g., using machine learning techniques), for establishing baselines, and for detecting deviations. As one example, suppose that a given HTTP server typically sends/receives 1,000 bytes (in each direction) whenever a connection is made with it. If a connection generates 500 bytes of traffic, or 2,000 bytes of traffic, such connections would be considered within the typical usage pattern of the server. Suppose, however, that a connection is made that results in 10G of traffic. Such a connection is anomalous and can be flagged accordingly.

[00161] Returning to Fig. 1D, as previously mentioned, data aggregator 114 may be configured to provide information (e.g., collected from nodes 108 by agents) to data platform 12. Data aggregator 128 may be similarly configured to provide information to data platform 12. As

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00362

shown in Fig. 1D, both aggregator 114 and aggregator 128 may connect to a load balancer 130, which accepts connections from aggregators (and/or as applicable, agents), as well as other devices, such as computer 126 (e.g., when it communicates with web app 120), and supports fair balancing. In various embodiments, load balancer 130 is a reverse proxy that load balances accepted connections internally to various microservices (described in more detail below), allowing for services provided by data platform 12 to scale up as more agents are added to the environment and/or as more entities subscribe to services provided by data platform 12. Example ways to implement load balancer 130 include, but are not limited to, using HaProxy, using nginx, and using elastic load balancing (ELB) services made available by Amazon.

[00162] Agent service 132 is a microservice that is responsible for accepting data collected from agents (e.g., provided by aggregator 114). In various embodiments, agent service 132 uses a standard secure protocol, such as HTTPS to communicate with aggregators (and as applicable agents), and receives data in an appropriate format such as Apache Avro. When agent service 132 receives an incoming connection, it can perform a variety of checks, such as to see whether the data is being provided by a current customer, and whether the data is being provided in an appropriate format. If the data is not appropriately formatted (and/or is not provided by a current customer), it may be rejected.

[00163] If the data is appropriately formatted, agent service 132 may facilitate copying the received data to a streaming data stable storage using a streaming service (e.g., Amazon Kinesis and/or any other suitable streaming service. Once the ingesting into the streaming service is complete, service 132 may send an acknowledgement to the data provider (e.g., data aggregator 114). If the agent does not receive such an acknowledgement, it is configured to retry sending the data to data platform 12. One way to implement agent service 132 is as a REST API server framework (e.g., Java DropWizard), configured to communicate with Kinesis (e.g., using a Kinesis library).

[00164] In various embodiments, data platform 12 uses one or more streams (e.g., Kinesis streams) for all incoming customer data (e.g., including data provided by data aggregator 114 and data aggregator 128), and the data is sharded based on the node (also referred to herein as a "machine") that originated the data (e.g., node 116 vs. node 122), with each node having a globally unique identifier within data platform 12. Multiple instances of agent service 132 can write to multiple shards.

[00165] Kinesis is a streaming service with a limited period (e.g., 1-7 days). To persist data longer than a day, the data may be copied to long term storage 42 (e.g., S3). Data loader 136 is a microservice that is responsible for picking up data from a data stream (e.g., a Kinesis stream) and persisting it in long term storage 42. In one example embodiment, files collected by data

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00363

loader 136 from the Kinesis stream are placed into one or more buckets, and segmented using a combination of a customer identifier and time slice. Given a particular time segment, and a given customer identifier, the corresponding file (stored in long term storage) contains five minutes (or another appropriate time slice) of data collected at that specific customer from all of the customer's nodes. Data loader 136 can be implemented in any appropriate programming language, such as Java or C, and can be configured to use a Kinesis library to interface with Kinesis. In various embodiments, data loader 136 uses the Amazon Simple Queue Service (SQS) (e.g., to alert DB loader 140 that there is work for it to do).

[00166] DB loader 140 is a microservice that is responsible for loading data into an appropriate data store 30, such as SnowflakeDB or Amazon Redshift, using individual per-customer databases. In particular, DB loader 140 is configured to periodically load data into a set of raw tables from files created by data loader 136 as per above. DB loader 140 manages throughput, errors, etc., to make sure that data is loaded consistently and continuously. Further, DB loader 140 can read incoming data and load into data store 30 data that is not already present in tables of data store 30 (also referred to herein as a database). DB loader 140 can be implemented in any appropriate programming language, such as Java or C, and an SQL framework such as jOOQ (e.g., to manage SQLs for insertion of data), and SQL/JDBC libraries. In some examples, DB loader 140 may use Amazon S3 and Amazon Simple Queue Service (SQS) to manage files being transferred to and from data store 30.

[00167] Customer data included in data store 30 can be augmented with data from additional data sources, such as AWS CloudTrail and/or other types of external tracking services. To this end, data platform may include a tracking service analyzer 144, which is another microservice. Tracking service analyzer 144 may pull data from an external tracking service (e.g., Amazon CloudTrail) for each applicable customer account, as soon as the data is available. Tracking service analyzer 144 may normalize the tracking data as applicable, so that it can be inserted into data store 30 for later querying/analysis. Tracking service analyzer 144 can be written in any appropriate programming language, such as Java or C. Tracking service analyzer 144 also makes use of SQL/JDBC libraries to interact with data store 30 to insert/query data.

[00168] As described herein, data platform 12 can model activities that occur within datacenters, such as datacenters 104 and 106. The model may be stable over time, and differences, even subtle ones (e.g., between a current state of the datacenter and the model) can be surfaced. The ability to surface such anomalies can be particularly beneficial in datacenter environments where rogue employees and/or external attackers may operate slowly (e.g., over a period of months), hoping that the elastic nature of typical resource use (e.g., virtualized servers) will help conceal their nefarious activities.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00364

[00169] Using techniques described herein, data platform 12 can automatically discover entities (which may implement compute assets 16) deployed in a given datacenter. Examples of entities include workloads, applications, processes, machines, virtual machines, containers, files, IP addresses, domain names, and users. The entities may be grouped together logically (into analysis groups) based on behaviors, and temporal behavior baselines can be established. In particular, using techniques described herein, periodic graphs can be constructed (also referred to herein as polygraphs), in which the nodes are applicable logical entities, and the edges represent behavioral relationships between the logical entities in the graph. Baselines can be created for every node and edge.

[00170] Communication (e.g., between applications/nodes) is one example of a behavior. A model of communications between processes is an example of a behavioral model. As another example, the launching of applications is another example of a behavior that can be modeled. The baselines may be periodically updated (e.g., hourly) for every entity. Additionally or alternatively, the baselines may be continuously updated in substantially real-time as data is collected by agents. Deviations from the expected normal behavior can then be detected and automatically reported (e.g., as anomalies or threats detected). Such deviations may be due to a desired change, a misconfiguration, or malicious activity. As applicable, data platform 12 can score the detected deviations (e.g., based on severity and threat posed). Additional examples of analysis groups include models of machine communications, models of privilege changes, and models of insider behaviors (monitoring the interactive behavior of human users as they operate within the datacenter).

[00171] Two example types of information collected by agents are network level information and process level information. As previously mentioned, agents may collect information about every connection involving their respective nodes. And, for each connection, information about both the server and the client may be collected (e.g., using the connection-to-process identification techniques described above). DNS queries and responses may also be collected. The DNS query information can be used in logical entity graphing (e.g., collapsing many different IP addresses to a single service – e.g., s3.amazon.com). Examples of process level information collected by agents include attributes (user ID, effective user ID, and command line). Information such as what user/application is responsible for launching a given process and the binary being executed (and its SHA-256 values) may also be provided by agents.

[00172] The dataset collected by agents across a datacenter can be very large, and many resources (e.g., virtual machines, IP addresses, etc.) are recycled very quickly. For example, an IP address and port number used at a first point in time by a first process on a first virtual machine may very rapidly be used (e.g., an hour later) by a different process/virtual machine.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00365

[00173] A dataset (and elements within it) can be considered at both a physical level, and a logical level, as illustrated in Fig. 2B. In particular, Fig. 2B illustrates an example 5-tuple of data 210 collected by an agent, represented physically (216) and logically (217). The 5-tuple includes a source address 211, a source port 212, a destination address 213, a destination port 214, and a protocol 215. In some cases, port numbers (e.g., 212, 214) may be indicative of the nature of a connection (e.g., with certain port usage standardized). However, in many cases, and in particular in datacenters, port usage is ephemeral. For example, a Docker container can listen on an ephemeral port, which is unrelated to the service it will run. When another Docker container starts (for the same service), the port may well be different. Similarly, particularly in a virtualized environment, IP addresses may be recycled frequently (and are thus also potentially ephemeral) or could be NATed, which makes identification difficult.

[00174] A physical representation of the 5-tuple is depicted in region 216. A process 218 (executing on machine 219) has opened a connection to machine 220. In particular, process 218 is in communication with process 221. Information such as the number of packets exchanged between the two machines over the respective ports can be recorded.

[00175] As previously mentioned, in a datacenter environment, portions of the 5-tuple may change – potentially frequently – but still be associated with the same behavior. Namely, one application (e.g., Apache) may frequently be in communication with another application (e.g., Oracle), using ephemeral datacenter resources. Further, either/both of Apache and Oracle may be multi-homed. This can lead to potentially thousands of 5-tuples (or more) that all correspond to Apache communicating with Oracle within a datacenter. For example, Apache could be executed on a single machine, and could also be executed across fifty machines, which are variously spun up and down (with different IP addresses each time). An alternate representation of the 5-tuple of data 210 is depicted in region 217, and is logical. The logical representation of the 5-tuple aggregates the 5-tuple (along with other connections between Apache and Oracle having other 5-tuples) as logically representing the same connection. By aggregating data from raw physical connection information into logical connection information, using techniques described herein, a size reduction of six orders of magnitude in the data set can be achieved.

[00176] Fig. 2C depicts a portion of a logical polygraph. Suppose a datacenter has seven instances of the application update_engine 225, executing as seven different processes on seven different machines, having seven different IP addresses, and using seven different ports. The instances of update_engine variously communicate with update.core-os.net 226, which may have a single IP address or many IP addresses itself, over the one hour time period represented in the polygraph. In the example shown in Fig. 2C, update_engine is a client, connecting to the server update.core-os.net, as indicated by arrow 228.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00366

[00177] Behaviors of the seven processes are clustered together, into a single summary. As indicated in region 227, statistical information about the connections is also maintained (e.g., number of connections, histogram information, etc.). A polygraph such as is depicted in Fig. 2C can be used to establish a baseline of behavior (e.g., at the one-hour level), allowing for the future detection of deviations from that baseline. As one example, suppose that statistically an update_engine instance transmits data at 11 bytes per second. If an instance were instead to transmit data at 1000 bytes per second, such behavior would represent a deviation from the baseline and could be flagged accordingly. Similarly, changes that are within the baseline (e.g., an eighth instance of update_engine appears, but otherwise behaves as the other instances; or one of the seven instances disappears) are not flagged as anomalous. Further, datacenter events, such as failover, autobalancing, and A-B refresh are unlikely to trigger false alarms in a polygraph, as at the logical level, the behaviors remain the same.

[00178] In various embodiments, polygraph data is maintained for every application in a datacenter, and such polygraph data can be combined to make a single datacenter view across all such applications. Fig. 2D illustrates a portion of a polygraph for a service that evidences more complex behaviors than are depicted in Fig. 2C. In particular, Fig. 2D illustrates the behaviors of S3 as a service (as used by a particular customer datacenter). Clients within the datacenter variously connect to the S3 service using one of five fully qualified domains (listed in region 230). Contact with any of the domains is aggregated as contact with S3 (as indicated in region 231). Depicted in region 232 are various containers which (as clients) connect with S3. Other containers (which do not connect with S3) are not included. As with the polygraph portion depicted in Fig. 2C, statistical information about the connections is known and summarized, such as the number of bytes transferred, histogram information, etc.

[00179] Fig. 2E illustrates a communication polygraph for a datacenter. In particular, the polygraph indicates a one hour summary of approximately 500 virtual machines, which collectively run one million processes, and make 100 million connections in that hour. As illustrated in Fig. 2E, a polygraph represents a drastic reduction in size (e.g., from tracking information on 100 million connections in an hour, to a few hundred nodes and a few hundred edges). Further, as a datacenter scales up (e.g., from using 10 virtual machines to 100 virtual machines as the datacenter uses more workers to support existing applications), the polygraph for the datacenter will tend to stay the same size (with the 100 virtual machines clustering into the same nodes that the 10 virtual machines previously clustered into). As new applications are added into the datacenter, the polygraph may automatically scale to include behaviors involving those applications.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00367

[00180] In the particular polygraph shown in Fig. 2E, nodes generally correspond to workers, and edges correspond to communications the workers engage in (with connection activity being the behavior modeled in polygraph 235). Another example polygraph could model other behavior, such as application launching. The communications graphed in Fig. 2E include traffic entering the datacenter, traffic exiting the datacenter, and traffic that stays wholly within the datacenter (e.g., traffic between workers). One example of a node included in polygraph 235 is the sshd application, depicted as node 236. As indicated in Fig. 2E, 421 instances of sshd were executing during the one hour time period of data represented in polygraph 235. As indicated in region 237, nodes within the datacenter communicated with a total of 1349 IP addresses outside of the datacenter (and not otherwise accounted for, e.g., as belonging to a service such as Amazon AWS 238 or Slack 239).

[00181] In the following examples, suppose that user B, an administrator of datacenter 106, is interacting with data platform 12 to view visualizations of polygraphs in a web browser (e.g., as served to user B via web app 120). One type of polygraph user B can view is an application-communication polygraph, which indicates, for a given one hour window (or any other suitable time interval), which applications communicated with which other applications. Another type of polygraph user B can view is an application launch polygraph. User B can also view graphs related to user behavior, such as an insider behavior graph which tracks user connections (e.g., to internal and external applications, including chains of such behavior), a privilege change graph which tracks how privileges change between processes, and a user login graph, which tracks which (logical) machines a user logs into.

[00182] Fig. 2F illustrates an example of an application-communication polygraph for a datacenter (e.g., datacenter 106) for the one hour period of 9am-10am on June 5. The time slice currently being viewed is indicated in region 240. If user B clicks his mouse in region 241, user B will be shown a representation of the application-communication polygraph as generated for the following hour (10am-11am on June 5).

[00183] Fig. 2G depicts what is shown in user B's browser after he has clicked on region 241, and has further clicked on region 242. The selection in region 242 turns on and off the ability to compare two time intervals to one another. User B can select from a variety of options when comparing the 9am-10am and 10am-11am time intervals. By clicking region 248, user B will be shown the union of both graphs (i.e., any connections that were present in either time interval). By clicking region 249, user B will be shown the intersection of both graphs (i.e., only those connections that were present in both time intervals).

[00184] As shown in Fig. 2G, user B has elected to click on region 250, which depicts connections that are only present in the 9am-10am polygraph in a first color 251, and depicts

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00368

connections that are only present in the 10am-11am polygraph in a second color 252. Connections present in both polygraphs are omitted from display. As one example, in the 9am-10am polygraph (corresponding to connections made during the 9am-10am time period at datacenter 106), a connection was made by a server to sshd (253) and also to systemd (254). Both of those connections ended prior to 10am and are thus depicted in the first color. As another example, in the 10am-11am polygraph (corresponding to connections made during the 10am-11am time period at datacenter 106), a connection was made from a known bad external IP to nginx (255). The connection was not present during the 9am-10am time slice and thus is depicted in the second color. As yet another example, two different connections were made to a Slack service between 9am and 11am. However, the first was made by a first client during the 9am-10am time slice (256) and the second was made by a different client during the 10am-11am slice (257), and so the two connections are depicted respectively in the first and second colors and blue.

[00185] Returning to the polygraph depicted in Fig. 2F, suppose user B enters "etcd" into the search box located in region 244. User B will then be presented with the interface illustrated in Fig. 2H. As shown in Fig. 2H, three applications containing the term "etcd" were engaged in communications during the 9am-10am window. One application is etcdctl, a command line client for etcd. As shown in Fig. 2H, a total of three different etcdctl processes were executed during the 9am-10am window, and were clustered together (260). Fig. 2H also depicts two different clusters that are both named etcd2. The first cluster includes (for the 9am-10am window) five members (261) and the second cluster includes (for the same window) eight members (262). The reason for these two distinct clusters is that the two groups of applications behave differently (e.g., they exhibit two distinct sets of communication patterns). Specifically, the instances of etcd2 in cluster 261 only communicate with locksmithctl (263) and other etcd2 instances (in both clusters 261 and 262). The instances of etcd2 in cluster 262 communicate with additional entities, such as etcdctl and Docker containers. As desired, user B can click on one of the clusters (e.g., cluster 261) and be presented with summary information about the applications included in the cluster, as is shown in Fig. 2I (e.g., in region 265). User B can also double click on a given cluster (e.g., cluster 261) to see details on each of the individual members of the cluster broken out.

[00186] Suppose user B now clicks on region 245 of the interface shown in Fig. 2F. User B will then be shown an application launch polygraph. Launching an application is another example of a behavior. The launch polygraph models how applications are launched by other applications. Fig. 2J illustrates an example of a portion of a launch polygraph. In particular, user B has typed "find" into region 266, to see how the "find" application is being launched. As shown in Fig. 2J,

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00369

in the launch polygraph for the 10am-11am time period, find applications (267) are always launched by bash (268), which is in turn always launched by systemd (269). If find is launched by a different application, this would be anomalous behavior.

[00187] Fig. 2K illustrates another example of a portion of an application launch polygraph. In Fig. 2K, user B has searched (270) for "python ma" to see how "python marathon_lb" (271) is launched. As shown in Fig. 2K, in each case (during the one hour time slice of 10am-11am), python marathon_lb is launched as a result of a chain of the same seven applications each time. If python marathon_lb is ever launched in a different manner, this indicates anomalous behavior. The behavior could be indicative of malicious activities, but could also be due to other reasons, such as a misconfiguration, a performance-related issue, and/or a failure, etc.

[00188] Suppose user B now clicks on region 246 of the interface shown in Fig. 2F. User B will then be shown an insider behavior graph. The insider behavior graph tracks information about behaviors such as processes started by a user interactively using protocols such as ssh or telnet, and any processes started by those processes. As one example, suppose an administrator logs into a first virtual machine in datacenter 106 (e.g., using sshd via an external connection he makes from a hotel), using a first set of credentials (e.g., first.last@example.com and an appropriate password). From the first virtual machine, the administrator connects to a second virtual machine (e.g., using the same credentials), then uses the sudo command to change identities to those of another user, and then launches a program. graphs built by data platform 12 can be used to associate the administrator with each of his actions, including launching the program using the identity of another user.

[00189] Fig. 2L illustrates an example of a portion of an insider behavior graph. In particular, in Fig. 2L, user B is viewing a graph that corresponds to the time slice of 3pm-4pm on June 1. Fig. 2L illustrates the internal/external applications that users connected to during the one hour time slice. If a user typically communicates with particular applications, that information will become part of a baseline. If the user deviates from his baseline behavior (e.g., using new applications, or changing privilege in anomalous ways), such anomalies can be surfaced.

[00190] Fig. 2M illustrates an example of a portion of a privilege change graph, which identifies how privileges are changed between processes. Typically, when a user launches a process (e.g., "ls"), the process inherits the same privileges that the user has. And, while a process can have fewer privileges than the user (i.e., go down in privilege), it is rare (and generally undesirable) for a user to escalate in privilege. Information included in the privilege change graph can be determined by examining the parent of each running process, and determining whether there is a match in privilege between the parent and the child. If the privileges are different, a privilege change has occurred (whether a change up or a change down). The application ntpd is one rare

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00370

example of a scenario in which a process escalates (272) to root, and then returns back (273). The sudo command is another example (e.g., used by an administrator to temporarily have a higher privilege). As with the other examples, ntpd's privilege change actions, and the legitimate actions of various administrators (e.g., using sudo) will be incorporated into a baseline model by data platform 12. When deviations occur, such as where a new application that is not ntpd escalates privilege, or where an individual that has not previously/does not routinely use sudo does so, such behaviors can be identified as anomalous.

[00191] Fig. 2N illustrates an example of a portion of a user login graph, which identifies which users log into which logical nodes. Physical nodes (whether bare metal or virtualized) are clustered into a logical machine cluster, for example, using yet another graph, a machine-server graph, an example of which is shown in Fig. 2O. For each machine, a determination is made as to what type of machine it is, based on what kind(s) of workflows it runs. As one example, some machines run as master nodes (having a typical set of workflows they run, as master nodes) and can thus be clustered as master nodes. Worker nodes are different from master nodes, for example, because they run Docker containers, and frequently change as containers move around. Worker nodes can similarly be clustered.

[00192] As previously mentioned, the polygraph depicted in Fig. 2E corresponds to activities in a datacenter in which, in a given hour, approximately 500 virtual machines collectively run one million processes, and make 100 million connections in that hour. The polygraph represents a drastic reduction in size (e.g., from tracking information on 100 million connections in an hour, to a few hundred nodes and a few hundred edges). Using techniques described herein, such a polygraph can be constructed (e.g., using commercially available computing infrastructure) in less than an hour (e.g., within a few minutes). Thus, ongoing hourly snapshots of a datacenter can be created within a two hour moving window (i.e., collecting data for the time period 8am-9am, while also generating a snapshot for the time previous time period 7am-8am). The following describes various example infrastructure that can be used in polygraph construction, and also describes various techniques that can be used to construct polygraphs.

[00193] Returning to Fig. 1D, embodiments of data platform 12 may be built using any suitable infrastructure as a service (IaaS) (e.g., AWS). For example, data platform 12 can use Simple Storage Service (S3) for data storage, Key Management Service (KMS) for managing secrets, Simple Queue Service (SQS) for managing messaging between applications, Simple Email Service (SES) for sending emails, and Route 53 for managing DNS. Other infrastructure tools can also be used. Examples include: orchestration tools (e.g., Kubernetes or Mesos/Marathon), service discovery tools (e.g., Mesos-DNS), service load balancing tools (e.g., marathon-LB), container tools (e.g., Docker or rkt), log/metric tools (e.g., collectd, fluentd, kibana, etc.), big data

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00371

processing systems (e.g., Spark, Hadoop, AWS Redshift, Snowflake etc.), and distributed key value stores (e.g., Apache Zookeeper or etcd2).

[00194] As previously mentioned, in various embodiments, data platform 12 may make use of a collection of microservices. Each microservice can have multiple instances, and may be configured to recover from failure, scale, and distribute work amongst various such instances, as applicable. For example, microservices are auto-balancing for new instances, and can distribute workload if new instances are started or existing instances are terminated. In various embodiments, microservices may be deployed as self-contained Docker containers. A Mesos-Marathon or Spark framework can be used to deploy the microservices (e.g., with Marathon monitoring and restarting failed instances of microservices as needed). The service etcd2 can be used by microservice instances to discover how many peer instances are running, and used for calculating a hash-based scheme for workload distribution. Microservices may be configured to publish various health/status metrics to either an SQS queue, or etcd2, as applicable. In some examples, Amazon DynamoDB can be used for state management.

[00195] Additional information on various microservices used in embodiments of data platform 12 is provided below.

[00196] Graph generator 146 is a microservice that may be responsible for generating raw behavior graphs on a per customer basis periodically (e.g., once an hour). In particular, graph generator 146 may generate graphs of entities (as the nodes in the graph) and activities between entities (as the edges). In various embodiments, graph generator 146 also performs other functions, such as aggregation, enrichment (e.g., geolocation and threat), reverse DNS resolution, TF-IDF based command line analysis for command type extraction, parent process tracking, etc.

[00197] Graph generator 146 may perform joins on data collected by the agents, so that both sides of a behavior are linked. For example, suppose a first process on a first virtual machine (e.g., having a first IP address) communicates with a second process on a second virtual machine (e.g., having a second IP address). Respective agents on the first and second virtual machines may each report information on their view of the communication (e.g., the PID of their respective processes, the amount of data exchanged and in which direction, etc.). When graph generator performs a join on the data provided by both agents, the graph will include a node for each of the processes, and an edge indicating communication between them (as well as other information, such as the directionality of the communication – i.e., which process acted as the server and which as the client in the communication).

[00198] In some cases, connections are process to process (e.g., from a process on one virtual machine within the cloud environment associated with entity A to another process on a virtual machine within the cloud environment associated with entity A). In other cases, a process may be

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00372

in communication with a node (e.g., outside of entity A) which does not have an agent deployed upon it. As one example, a node within entity A might be in communication with node 172, outside of entity A. In such a scenario, communications with node 172 are modeled (e.g., by graph generator 146) using the IP address of node 172. Similarly, where a node within entity A does not have an agent deployed upon it, the IP address of the node can be used by graph generator in modeling.

[00199] Graphs created by graph generator 146 may be written to data store 30 and cached for further processing. A graph may be a summary of all activity that happened in a particular time interval. As each graph corresponds to a distinct period of time, different rows can be aggregated to find summary information over a larger timestamp. In some examples, picking two different graphs from two different timestamps can be used to compare different periods. If necessary, graph generator can parallelize its workload (e.g., where its backlog cannot otherwise be handled within a particular time period, such as an hour, or if is required to process a graph spanning a long time period).

[00200] Graph generator 146 can be implemented in any appropriate programming language, such as Java or C, and machine learning libraries, such as Spark's MLLib. Example ways that graph generator computations can be implemented include using SQL or Map-R, using Spark or Hadoop.

[00201] SSH tracker 148 is a microservice that may be responsible for following ssh connections and process parent hierarchies to determine trails of user ssh activity. Identified ssh trails are placed by the SSH tracker 148 into data store 30 and cached for further processing.

[00202] SSH tracker 148 can be implemented in any appropriate programming language, such as Java or C, and machine libraries, such as Spark's MLLib. Example ways that SSH tracker computations can be implemented include using SQL or Map-R, using Spark or Hadoop.

[00203] Threat aggregator 150 is a microservice that may be responsible for obtaining third party threat information from various applicable sources, and making it available to other micro-services. Examples of such information include reverse DNS information, GeoIP information, lists of known bad domains/IP addresses, lists of known bad files etc. As applicable, the threat information is normalized before insertion into data store 30. Threat aggregator 150 can be implemented in any appropriate programming language, such as Java or C, using SQL/JDBC libraries to interact with data store 30 (e.g., for insertions and queries).

[00204] Scheduler 152 is a microservice that may act as a scheduler and that may run arbitrary jobs organized as a directed graph. In some examples, scheduler 152 ensures that all jobs for all customers are able to run during at a given time interval (e.g., every hour). Scheduler 152 may handle errors and retrying for failed jobs, track dependencies, manage appropriate resource

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00373

levels, and/or scale jobs as needed. Scheduler 152 can be implemented in any appropriate programming language, such as Java or C. A variety of components can also be used, such as open source scheduler frameworks (e.g., Airflow), or AWS services (e.g., the AWS Data pipeline) which can be used for managing schedules.

[00205] Graph Behavior Modeler (GBM) 154 is a microservice that may compute polygraphs. In particular, GBM 154 can be used to find clusters of nodes in a graph that should be considered similar based on some set of their properties and relationships to other nodes. As described herein, the clusters and their relationships can be used to provide visibility into a datacenter environment without requiring user specified labels. GBM 154 may track such clusters over time persistently, allowing for changes to be detected and alerts to be generated.

[00206] GBM 154 may take as input a raw graph (e.g., as generated by graph generator 146). Nodes are actors of a behavior, and edges are the behavior relationship itself. For example, in the case of communication, example actors include processes, which communicate with other processes. The GBM 154 clusters the raw graph based on behaviors of actors and produces a summary (the polygraph). The polygraph summarizes behavior at a datacenter level. The GBM also produces "observations" that represent changes detected in the datacenter. Such observations may be based on differences in cumulative behavior (e.g., the baseline) of the datacenter with its current behavior. The GBM 154 can be implemented in any appropriate programming language, such as Java, C, or Golang, using appropriate libraries (as applicable) to handle distributed graph computations (handling large amounts of data analysis in a short amount of time). Apache Spark is another example tool that can be used to compute polygraphs. The GBM can also take feedback from users and adjust the model according to that feedback. For example, if a given user is interested in relearning behavior for a particular entity, the GBM can be instructed to "forget" the implicated part of the polygraph.

[00207] GBM runner 156 is a microservice that may be responsible for interfacing with GBM 154 and providing GBM 154 with raw graphs (e.g., using a query language, such as SQL, to push any computations it can to data store 30). GBM runner 156 may also insert polygraph output from GBM 154 to data store 30. GBM runner 156 can be implemented in any appropriate programming language, such as Java or C, using SQL/JDBC libraries to interact with data store 30 to insert and query data.

[00208] Alert generator 158 is a microservice that may be responsible for generating alerts. Alert generator 158 may examine observations (e.g., produced by GBM 154) in aggregate, deduplicate them, and score them. Alerts may be generated for observations with a score exceeding a threshold. Alert generator 158 may also compute (or retrieves, as applicable) data that a customer (e.g., user A or user B) might need when reviewing the alert. Examples of events that can be

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00374

detected by data platform 12 (and alerted on by alert generator 158) include, but are not limited to the following:

[00209] new user: This event may be created the first time a user (e.g., of node 116) is first observed by an agent within a datacenter.

[00210] user launched new binary: This event may be generated when an interactive user launches an application for the first time.

[00211] new privilege escalation: This event may be generated when user privileges are escalated and a new application is run.

[00212] new application or container: This event may be generated when an application or container is seen for the first time.

[00213] new external connection: This event may be generated when a connection to an external IP/domain is made from a new application.

[00214] new external host or IP: This event may be generated when a new external host or IP is involved in a connection with a datacenter.

[00215] new internal connection: This event may be generated when a connection between internal-only applications is seen for the first time.

[00216] new external client: This event may be generated when a new external connection is seen for an application which typically does not have external connections.

[00217] new parent: This event may be generated when an application is launched by a different parent.

[00218] connection to known bad IP/domain: Data platform 12 maintains (or can otherwise access) one or more reputation feeds. If an environment makes a connection to a known bad IP or domain, an event will be generated.

[00219] login from a known bad IP/domain: An event may be generated when a successful connection to a datacenter from a known bad IP is observed by data platform 12.

[00220] Alert generator 158 can be implemented in any appropriate programming language, such as Java or C, using SQL/JDBC libraries to interact with data store 30 to insert and query data. In various embodiments, alert generator 158 also uses one or more machine learning libraries, such as Spark's MLLib (e.g., to compute scoring of various observations). Alert generator 158 can also take feedback from users about which kinds of events are of interest and which to suppress.

[00221] QsJobServer 160 is a microservice that may look at all the data produced by data platform 12 for an hour, and compile a materialized view (MV) out of the data to make queries faster. The MV helps make sure that the queries customers most frequently run, and data that they search for, can be easily queried and answered. QsJobServer 160 may also precompute and cache a variety of different metrics so that they can quickly be provided as answers at query time.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00375

QsJobServer 160 can be implemented using any appropriate programming language, such as Java or C, using SQL/JDBC libraries. In some examples, QsJobServer 160 is able to compute an MV efficiently at scale, where there could be a large number of joins. An SQL engine, such as Oracle, can be used to efficiently execute the SQL, as applicable.

[00222] Alert notifier 162 is a microservice that may take alerts produced by alert generator 158 and send them to customers' integrated Security Information and Event Management (SIEM) products (e.g., Splunk, Slack, etc.). Alert notifier 162 can be implemented using any appropriate programming language, such as Java or C. Alert notifier 162 can be configured to use an email service (e.g., AWS SES or pagerduty) to send emails. Alert notifier 162 may also provide templating support (e.g., Velocity or Moustache) to manage templates and structured notifications to SIEM products.

[00223] Reporting module 164 is a microservice that may be responsible for creating reports out of customer data (e.g., daily summaries of events, etc.) and providing those reports to customers (e.g., via email). Reporting module 164 can be implemented using any appropriate programming language, such as Java or C. Reporting module 164 can be configured to use an email service (e.g., AWS SES or pagerduty) to send emails. Reporting module 164 may also provide templating support (e.g., Velocity or Moustache) to manage templates (e.g., for constructing HTML-based email).

[00224] Web app 120 is a microservice that provides a user interface to data collected and processed on data platform 12. Web app 120 may provide login, authentication, query, data visualization, etc. features. Web app 120 may, in some embodiments, include both client and server elements. Example ways the server elements can be implemented are using Java DropWizard or Node.Js to serve business logic, and a combination of JSON/HTTP to manage the service. Example ways the client elements can be implemented are using frameworks such as React, Angular, or Backbone. JSON, jQuery, and JavaScript libraries (e.g., underscore) can also be used.

[00225] Query service 166 is a microservice that may manage all database access for web app 120. Query service 166 abstracts out data obtained from data store 30 and provides a JSON-based REST API service to web app 120. Query service 166 may generate SQL queries for the REST APIs that it receives at run time. Query service 166 can be implemented using any appropriate programming language, such as Java or C and SQL/JDBC libraries, or an SQL framework such as jOOQ. Query service 166 can internally make use of a variety of types of databases, including a relational database engine 168 (e.g., AWS Aurora) and/or data store 30 to manage data for clients. Examples of tables that query service 166 manages are OLTP tables and data warehousing tables.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00376

[00226] Cache 170 may be implemented by Redis and/or any other service that provides a key-value store. Data platform 12 can use cache 170 to keep information for frontend services about users. Examples of such information include valid tokens for a customer, valid cookies of customers, the last time a customer tried to login, etc.

[00227] Fig. 3A illustrates an example of a process for detecting anomalies in a network environment. In various embodiments, process 300 is performed by data platform 12. The process begins at 301 when data associated with activities occurring in a network environment (such as entity A's datacenter) is received. One example of such data that can be received at 301 is agent-collected data described above (e.g., in conjunction with process 200).

[00228] At 302, a logical graph model is generated, using at least a portion of the monitored activities. A variety of approaches can be used to generate such logical graph models, and a variety of logical graphs can be generated (whether using the same, or different approaches). The following is one example of how data received at 301 can be used to generate and maintain a model.

[00229] During bootstrap, data platform 12 creates an aggregate graph of physical connections (also referred to herein as an aggregated physical graph) by matching connections that occurred in the first hour into communication pairs. Clustering is then performed on the communication pairs. Examples of such clustering, described in more detail below, include performing Matching Neighbor clustering and similarity (e.g., SimRank) clustering. Additional processing can also be performed (and is described in more detail below), such as by splitting clusters based on application type, and annotating nodes with DNS query information. The resulting graph (also referred to herein as a base graph or common graph) can be used to generate a variety of models, where a subset of node and edge types (described in more detail below) and their properties are considered in a given model. One example of a model is a UID to UID model (also referred to herein as a Uid2Uid model) which clusters together processes that share a username and show similar privilege change behavior. Another example of a model is a CType model, which clusters together processes that share command line similarity. Yet another example of a model is a PType model, which clusters together processes that share behaviors over time.

[00230] Each hour (or any other predetermined time interval) after bootstrap, a new snapshot is taken (i.e., data collected about a datacenter in the last hour is processed) and information from the new snapshot is merged with existing data to create and (as additional data is collected/processed) maintain a cumulative graph. The cumulative graph (also referred to herein as a cumulative PType graph and a polygraph) is a running model of how processes behave over time. Nodes in the cumulative graph are PType nodes, and provide information such as a list of all active processes and PIDs in the last hour, the number of historic total processes, the average

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00377

number of active processes per hour, the application type of the process (e.g., the CType of the PType), and historic CType information/frequency. Edges in the cumulative graph can represent connectivity and provide information such as connectivity frequency. The edges can be weighted (e.g., based on number of connections, number of bytes exchanged, etc.). Edges in the cumulative graph (and snapshots) can also represent transitions.

[00231] One approach to merging a snapshot of the activity of the last hour into a cumulative graph is as follows. An aggregate graph of physical connections is made for the connections included in the snapshot (as was previously done for the original snapshot used during bootstrap). And, clustering/splitting is similarly performed on the snapshot's aggregate graph. Next, PType clusters in the snapshot's graph are compared against PType clusters in the cumulative graph to identify commonality.

[00232] One approach to determining commonality is, for any two nodes that are members of a given CmdType (described in more detail below), comparing internal neighbors and calculating a set membership Jaccard distance. The pairs of nodes are then ordered by decreasing similarity (i.e., with the most similar sets first). For nodes with a threshold amount of commonality (e.g., at least 66% members in common), any new nodes (i.e., appearing in the snapshot's graph but not the cumulative graph) are assigned the same PType identifier as is assigned to the corresponding node in the cumulative graph. For each node that is not classified (i.e., has not been assigned a PType identifier), a network signature is generated (i.e., indicative of the kinds of network connections the node makes, who the node communicates with, etc.). The following processing is then performed until convergence. If a match of the network signature is found in the cumulative graph, the unclassified node is assigned the PType identifier of the corresponding node in the cumulative graph. Any nodes which remain unclassified after convergence are new PTypes and are assigned new identifiers and added to the cumulative graph as new. As applicable, the detection of a new PType can be used to generate an alert. If the new PType has a new CmdType, a severity of the alert can be increased. If any surviving nodes (i.e., present in both the cumulative graph and the snapshot graph) change PTypes, such change is noted as a transition, and an alert can be generated. Further, if a surviving node changes PType and also changes CmdType, a severity of the alert can be increased.

[00233] Changes to the cumulative graph (e.g., a new PType or a new edge between two PTypes) can be used (e.g., at 303) to detect anomalies (described in more detail below). Two example kinds of anomalies that can be detected by data platform 12 include security anomalies (e.g., a user or process behaving in an unexpected manner) and devops/root cause anomalies (e.g., network congestion, application failure, etc.). Detected anomalies can be recorded and surfaced

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00378

(e.g., to administrators, auditors, etc.), such as through alerts which are generated at 304 based on anomaly detection.

[00234] Additional detail regarding processing performed, by various components depicted in Fig. 1D (whether performed individually or in combination), in conjunction with model/polygraph construction (e.g., as performed at 302) are provided below.

[00235] As explained above, an aggregated physical graph can be generated on a per customer basis periodically (e.g., once an hour) from raw physical graph information, by matching connections (e.g., between two processes on two virtual machines). In various embodiments, a deterministic fixed approach is used to cluster nodes in the aggregated physical graph (e.g., representing processes and their communications). As one example, Matching Neighbors Clustering (MNC) can be performed on the aggregated physical graph to determine which entities exhibit identical behavior and cluster such entities together.

[00236] Fig. 3B depicts a set of example processes (p1, p2, p3, and p4) communicating with other processes (p10 and p11). Fig. 3B is a graphical representation of a small portion of an aggregated physical graph showing (for a given time period, such as an hour) which processes in a datacenter communicate with which other processes. Using MNC, processes p1, p2, and p3 will be clustered together (305), as they exhibit identical behavior (they communicate with p10 and only p10). Process p4, which communicates with both p10 and p11, will be clustered separately.

[00237] In MNC, only those processes exhibiting identical (communication) behavior will be clustered. In various embodiments, an alternate clustering approach can also/instead be used, which uses a similarity measure (e.g., constrained by a threshold value, such as a 60% similarity) to cluster items. In some embodiments, the output of MNC is used as input to SimRank, in other embodiments, MNC is omitted.

[00238] Fig. 3C depicts a set of example processes (p4, p5, p6) communicating with other processes (p7, p8, p9). As illustrated, most of nodes p4, p5, and p6 communicate with most of nodes p7, p8, and p9 (as indicated in Fig. 3C with solid connection lines). As one example, process p4 communicates with process p7 (310), process p8 (311), and process p9 (312). An exception is process p6, which communicates with processes p7 and p8, but does not communicate with process p9 (as indicated by dashed line 313). If MNC were applied to the nodes depicted in Fig. 3C, nodes p4 and p5 would be clustered (and node p6 would not be included in their cluster).

[00239] One approach to similarity clustering is to use SimRank. In an embodiment of the SimRank approach, for a given node v in a directed graph, $I(v)$ and $O(v)$ denote the respective set of in-neighbors and out-neighbors of v. Individual in-neighbors are denoted as $I_i(v)$, for $1 \leq i \leq |I(v)|$, and individual out-neighbors are denoted as $O_i(v)$, for $1 \leq i \leq |O(v)|$. The similarity between two

objects a and b can be denoted by $s(a,b) \in [1,0]$. A recursive equation (hereinafter "the SimRank equation") can be written for $s(a,b)$, where, if a=b, then $s(a,b)$ is defined as 1, otherwise, $s(a,b)=\frac{C}{|I(a)||I(b)|}\sum_{i=1}^{|I(a)|}\sum_{j=1}^{|I(b)|}s(I_i(a),I_j(b))$ where C is a constant between 0 and 1. One example value for the decay factor C is 0.8 (and a fixed number of iterations such as five). Another example value for the decay factor C is 0.6 (and/or a different number of iterations). In the event that a or b has no in-neighbors, similarity is set to $s(a,b)=0$, so the summation is defined to be 0 when $I(a)=\emptyset$ or $I(b)=\emptyset$.

[00240] The SimRank equations for a graph G can be solved by iteration to a fixed point. Suppose n is the number of nodes in G. For each iteration k, n^2 entries $s_k(*,*)$ are kept, where $s_k(a,b)$ gives the score between a and b on iteration k. Successive computations of $s_{k+1}(*,*)$ are made based on $s_k(*,*)$. Starting with $s_0(*,*)$, where each $s_0(a,b)$ is a lower bound on the actual SimRank score $s(a,b)$: $s_0(a,b)=\begin{cases}1, \text{if } a=b,\\ 0, \text{if } a\neq b.\end{cases}$

[00241] The SimRank equation can be used to compute $s_{k+1}(a,b)$ from $s_k(*,*)$ with $s_{k+1}(a,b)=\frac{C}{|I(a)||I(b)|}\sum_{i=1}^{|I(a)|}\sum_{j=1}^{|I(b)|}s_k(I_i(a),I_j(b))$ for $a\neq b$, and $s_{k+1}(a,b)=1$ for $a=b$. On each iteration k+1, the similarity of (a,b) is updated using the similarity scores of the neighbors of (a,b) from the previous iteration k according to the SimRank equation. The values $s_k(*,*)$ are nondecreasing as k increases.

[00242] Returning to Fig. 3C, while MNC would cluster nodes p4 and p5 together (and not include node p6 in their cluster), application of SimRank would cluster nodes p4-p6 into one cluster (314) and also cluster nodes p7-p9 into another cluster (315).

[00243] Fig. 3D depicts a set of processes, and in particular server processes s1 and s2, and client processes c1, c2, c3, c4, c5, and c6. Suppose only nodes s1, s2, c1, and c2 are present in the graph depicted in Fig. 3D (and the other nodes depicted are omitted from consideration). Using MNC, nodes s1 and s2 would be clustered together, as would nodes c1 and c2. Performing SimRank clustering as described above would also result in those two clusters (s1 and s2, and c1 and c2). As previously mentioned, in MNC, identical behavior is required. Thus, if node c3 were now also present in the graph, MNC would not include c3 in a cluster with c2 and c1 because node c3 only communicates with node s2 and not node s1. In contrast, a SimRank clustering of a graph that includes nodes s1, s2, c1, c2, and c3 would result (based, e.g., on an applicable selected decay value and number of iterations) in a first cluster comprising nodes s1 and s2, and a second cluster of c1, c2, and c3. As an increasing number of nodes which communicate with server process s2, and do not also communicate with server process s1, are included in the graph (e.g., as c4, c5, and c6 are added), under SimRank, nodes s1 and s2 will become decreasingly similar (i.e., their intersection is reduced).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00380

[00244] In various embodiments, SimRank is modified (from what is described above) to accommodate differences between the asymmetry of client and server connections. As one example, SimRank can be modified to use different thresholds for client communications (e.g., an 80% match among nodes c1-c6) and for server communications (e.g., a 60% match among nodes s1 and s2). Such modification can also help achieve convergence in situations such as where a server process dies on one node and restarts on another node.

[00245] The application of MNC/SimRank to an aggregated physical graph results in a smaller graph, in which processes which are determined to be sufficiently similar are clustered together. Typically, clusters generated as output of MNC will be underinclusive. For example, for the nodes depicted in Fig. 3C, process p6 will not be included in a cluster with processes p4 and p5, despite substantial similarity in their communication behaviors. The application of SimRank (e.g., to the output of MNC) helps mitigate the underinclusiveness of MNC, but can result in overly inclusive clusters. As one example, suppose (returning to the nodes depicted in Fig. 3B) that as a result of applying SimRank to the depicted nodes, nodes p1-p4 are all included in a single cluster. Both MNC and SimRank operate agnostically of which application a given process belongs to. Suppose processes p1-p3 each correspond to a first application (e.g., an update engine), and process p4 corresponds to a second application (e.g., sshd). Further suppose process p10 corresponds to contact with AWS. Clustering all four of the processes together (e.g., as a result of SimRank) could be problematic, particularly in a security context (e.g., where granular information useful in detecting threats would be lost).

[00246] As previously mentioned, data platform 12 may maintain a mapping between processes and the applications to which they belong. In various embodiments, the output of SimRank (e.g., SimRank clusters) is split based on the applications to which cluster members belong (such a split is also referred to herein as a "CmdType split"). If all cluster members share a common application, the cluster remains. If different cluster members originate from different applications, the cluster members are split along application-type (CmdType) lines. Using the nodes depicted in Fig. 3D as an example, suppose that nodes c1, c2, c3, and c5 all share "update engine" as the type of application to which they belong (sharing a CmdType). Suppose that node c4 belongs to "ssh," and suppose that node c6 belongs to "bash." As a result of SimRank, all six nodes (c1-c6) might be clustered into a single cluster. After a CmdType split is performed on the cluster, however, the single cluster will be broken into three clusters (c1, c2, c3, c5; c4; and c6). Specifically, the resulting clusters comprise processes associated with the same type of application, which exhibit similar behaviors (e.g., communication behaviors). Each of the three clusters resulting from the CmdType split represents, respectively, a node (also referred to herein

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00381

as a PType) of a particular CmdType. Each PType is given a persistent identifier and stored persistently as a cumulative graph.

[00247] A variety of approaches can be used to determine a CmdType for a given process. As one example, for some applications (e.g., sshd), a one-to-one mapping exists between the CmdType and the application/binary name. Thus, processes corresponding to the execution of sshd will be classified using a CmdType of sshd. In various embodiments, a list of common application/binary names (e.g., sshd, apache, etc.) is maintained by data platform 12 and manually curated as applicable. Other types of applications (e.g., Java, Python, and Ruby) are multi-homed, meaning that several very different applications may all execute using the binary name, "java." For these types of applications, information such as command line / execution path information can be used in determining a CmdType. In particular, the subapplication can be used as the CmdType of the application, and/or term frequency analysis (e.g., TF/IDF) can be used on command line information to group, for example, any marathon related applications together (e.g., as a python.marathon CmdType) and separately from other Python applications (e.g., as a python.airflow CmdType).

[00248] In various embodiments, machine learning techniques are used to determine a CmdType. The CmdType model is constrained such that the execution path for each CmdType is unique. One example approach to making a CmdType model is a random forest based approach. An initial CmdType model is bootstrapped using process parameters (e.g., available within one minute of process startup) obtained using one hour of information for a given customer (e.g., entity A). Examples of such parameters include the command line of the process, the command line of the process's parent(s) (if applicable), the uptime of the process, UID/EUID and any change information, TTY and any change information, listening ports, and children (if any). Another approach is to perform term frequency clustering over command line information to convert command lines into cluster identifiers.

[00249] The random forest model can be used (e.g., in subsequent hours) to predict a CmdType for a process (e.g., based on features of the process). If a match is found, the process can be assigned the matching CmdType. If a match is not found, a comparison between features of the process and its nearest CmdType (e.g., as determined using a Levenstein distance) can be performed. The existing CmdType can be expanded to include the process, or, as applicable, a new CmdType can be created (and other actions taken, such as generating an alert). Another approach to handling processes which do not match an existing CmdType is to designate such processes as unclassified, and once an hour, create a new random forest seeded with process information from a sampling of classified processes (e.g., 10 or 100 processes per CmdType) and

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00382

the new processes. If a given new process winds up in an existing set, the process is given the corresponding CmdType. If a new cluster is created, a new CmdType can be created.

[00250] Conceptually, a polygraph represents the smallest possible graph of clusters that preserve a set of rules (e.g., in which nodes included in the cluster must share a CmdType and behavior). As a result of performing MNC, SimRank, and cluster splitting (e.g., CmdType splitting) many processes are clustered together based on commonality of behavior (e.g., communication behavior) and commonality of application type. Such clustering represents a significant reduction in graph size (e.g., compared to the original raw physical graph). Nonetheless, further clustering can be performed (e.g., by iterating on the graph data using the GBM to achieve such a polygraph). As more information within the graph is correlated, more nodes can be clustered together, reducing the size of the graph, until convergence is reached and no further clustering is possible.

[00251] Fig. 3E depicts two pairs of clusters. In particular, cluster 320 represents a set of client processes sharing the same CmdType ("a1"), communicating (collectively) with a server process having a CmdType ("a2"). Cluster 322 also represents a set of client processes having a CmdType a1 communicating with a server process having a CmdType a2. The nodes in clusters 320 and 322 (and similarly nodes in 321 and 323) remain separately clustered (as depicted) after MNC/SimRank/CmdType splitting – isolated islands. One reason this could occur is where server process 321 corresponds to processes executing on a first machine (having an IP address of 1.1.1.1). The machine fails and a new server process 323 starts, on a second machine (having an IP address of 2.2.2.2) and takes over for process 321.

[00252] Communications between a cluster of nodes (e.g., nodes of cluster 320) and the first IP address can be considered different behavior from communications between the same set of nodes and the second IP address, and thus communications 324 and 325 will not be combined by MNC/SimRank in various embodiments. Nonetheless, it could be desirable for nodes of clusters 320/322 to be combined (into cluster 326), and for nodes of clusters 321/323 to be combined (into cluster 327), as representing (collectively) communications between a1 and a2. One task that can be performed by data platform 12 is to use DNS query information to map IP addresses to logical entities. As will be described in more detail below, GBM 154 can make use of the DNS query information to determine that graph nodes of cluster 320 and graph nodes of cluster 322 both made DNS queries for "appserverabc.example.com," which first resolved to 1.1.1.1 and then to 2.2.2.2, and to combine nodes 320/322 and 321/323 together into a single pair of nodes (326 communicating with 327).

[00253] In various embodiments, GBM 154 operates in a batch manner in which it receives as input the nodes and edges of a graph for a particular time period along with its previous state, and

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00383

generates as output clustered nodes, cluster membership edges, cluster-to-cluster edges, events, and its next state.

[00254] GBM 154 may not try to consider all types of entities and their relationships that may be available in a conceptual common graph all at once. Instead, GBM uses a concept of models where a subset of node and edge types and their properties are considered in a given model. Such an approach is helpful for scalability, and also to help preserve detailed information (of particular importance in a security context) – as clustering entities in a more complex and larger graph could result in less useful results. In particular, such an approach allows for different types of relationships between entities to be preserved/more easily analyzed.

[00255] While GBM 154 can be used with different models corresponding to different subgraphs, core abstractions remain the same across types of models.

[00256] For example, each node type in a GBM model is considered to belong to a class. The class can be thought of as a way for the GBM to split nodes based on the criteria it uses for the model. The class for a node is represented as a string whose value is derived from the node's key and properties depending on the GBM Model. Note that different GBM models may create different class values for the same node. For each node type in a given GBM model, GBM 154 can generate clusters of nodes for that type. A GBM generated cluster for a given member node type cannot span more than one class for that node type. GBM 154 generates edges between clusters that have the same types as the edges between source and destination cluster node types.

[00257] Additionally or alternatively, the processes described herein as being used for a particular model can be used (can be the same) across models, and different models can also be configured with different settings.

[00258] Additionally or alternatively, the node types and the edge types may correspond to existing types in the common graph node and edge tables but this is not necessary. Even when there is a correspondence, the properties provided to GBM 154 are not limited to the properties that are stored in the corresponding graph table entries. They can be enriched with additional information before being passed to GBM 154.

[00259] Logically, the input for a GBM model can be characterized in a manner that is similar to other graphs. Edge triplets can be expressed, for example, as an array of source node type, edge type, and destination node type. And, each node type is associated with node properties, and each edge type is associated with edge properties. Other edge triplets can also be used (and/or edge triplets can be extended) in accordance with various embodiments.

[00260] Note that the physical input to the GBM model need not (and does not, in various embodiments) conform to the logical input. For example, the edges in the PtypeConn model correspond to edges between Matching Neighbors (MN) clusters, where each process node has

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00384

an MN cluster identifier property. In the User ID to User ID model (also referred to herein as the Uid2Uid model), edges are not explicitly provided separately from nodes (as the euid array in the node properties serves the same purpose). In both cases, however, the physical information provides the applicable information necessary for the logical input.

[00261] The state input for a particular GBM model can be stored in a file, a database, or other appropriate storage. The state file (from a previous run) is provided, along with graph data, except for when the first run for a given model is performed, or the model is reset. In some cases, no data may be available for a particular model in a given time period, and GBM may not be run for that time period. As data becomes available at a future time, GBM can run using the latest state file as input.

[00262] GBM 154 outputs cluster nodes, cluster membership edges, and inter-cluster relationship edges that are stored (in some embodiments) in the graph node tables: node_c, node_cm, and node_icr, respectively. The type names of nodes and edges may conform to the following rules:

[00263] * A given node type can be used in multiple different GBM models. The type names of the cluster nodes generated by two such models for that node type will be different. For instance, process type nodes will appear in both PtypeConn and Uid2Uid models, but their cluster nodes will have different type names.

[00264] * The membership edge type name is “MemberOf.”

[00265] * The edge type names for cluster-to-cluster edges will be the same as the edge type names in the underlying node-to-node edges in the input.

[00266] The following are example events GBM 154 can generate: new class, new cluster, new edge from class to class, split class (the notion that GBM 154 considers all nodes of a given type and class to be in the same cluster initially and if GBM 154 splits them into multiple clusters, it is splitting a class), new edge from cluster and class, new edge between cluster and cluster, and/or new edge from class to cluster.

[00267] One underlying node or edge in the logical input can cause multiple types of events to be generated. Conversely, one event can correspond to multiple nodes or edges in the input. Not every model generates every event type.

[00268] Additional information regarding examples of data structures/models that can be used in conjunction with models used by data platform 12 is now provided.

[00269] In some examples, a PTypeConn Model clusters nodes of the same class that have similar connectivity relationships. For example, if two processes had similar incoming neighbors of the same class and outgoing neighbors of the same class, they could be clustered.

[00270] The node input to the PTypeConn model for a given time period includes non-interactive (i.e., not associated with tty) process nodes that had connections in the time period and the base

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00385

graph nodes of other types (IP Service Endpoint (IPSep) comprising an IP address and a port), DNS Service Endpoint (DNSSep) and IPAddress) that have been involved in those connections. The base relationship is the connectivity relationship for the following type triplets:

[00271] * Process, ConnectedTo, Process

[00272] * Process, ConnectedTo, IP Service Endpoint (IPSep)

[00273] * Process, ConnectedTo, DNS Service Endpoint (DNSSep)

[00274] * IPAddress, ConnectedTo, ProcessProcess, DNS, ConnectedTo, Process

[00275] The edge inputs to this model are the ConnectedTo edges from the MN cluster, instead of individual node-to-node ConnectedTo edges from the base graph. The membership edges created by this model refer to the base graph node type provided in the input.

[00276] Class Values:

[00277] The class values of nodes are determined as follows depending on the node type (e.g., Process nodes, IPSep nodes, DNSSep nodes, and IP Address nodes).

[00278] Process nodes:

[00279] if exe_path contains java then "java <cmdline_term_1> ..."

[00280] else if exe_path contains python then "python <cmdline_term_1> ..."

[00281] else "last_part_of_exe_path"

[00282] IPSep nodes:

[00283] if IP_internal then "IntIPS"

[00284] else if severity = 0 then "<IP_addr>:<protocol>:<port>"

[00285] else "<IP_addr>:<port>_BadIP"

[00286] DNSSep nodes:

[00287] if IP_internal = 1 then "<hostname>"

[00288] else if severity = 0 then "<hostname>:<protocol>:port"

[00289] else "<hostname>:<port>_BadIP"

[00290] IPAddress nodes (will appear only on client side):

[00291] if IP_internal = 1 then "IPIntC"

[00292] else if severity = 0 then "ExtIPC"

[00293] else "ExtBadIPC"

[00294] Events:

[00295] A new class event in this model for a process node is equivalent to seeing a new CType being involved in a connection for the first time. Note that this does not mean the CType was not seen before. It is possible that it was previously seen but did not make a connection at that time.

[00296] A new class event in this model for an IPSep node with IP_internal = 0 is equivalent to seeing a connection to a new external IP address for the first time.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00386

[00297] A new class event in this model for a DNSSep node is equivalent to seeing a connection to a new domain for the first time.

[00298] A new class event in this model for an IPAddress node with IP_internal = 0 and severity = 0 is equivalent to seeing a connection from any external IP address for the first time.

[00299] A new class event in this model for an IPAddress node with IP_internal = 0 and severity > 0 is equivalent to seeing a connection from any bad external IP address for the first time.

[00300] A new class to class to edge from a class for a process node to a class for a process node is equivalent to seeing a communication from the source CType making a connection to the destination CType for the first time.

[00301] A new class to class to edge from a class for a process node to a class for a DNSSep node is equivalent to seeing a communication from the source CType making a connection to the destination domain name for the first time.

[00302] An IntPConn Model may be similar to the PtypeConn Model, except that connection edges between parent/child processes and connections between processes where both sides are not interactive are filtered out.

[00303] A Uid2Uid Model may cluster processes with the same username that show similar privilege change behavior. For instance, if two processes with the same username had similar effective user values, launched processes with similar usernames, and were launched by processes with similar usernames, then they could be clustered.

[00304] An edge between a source cluster and destination cluster generated by this model means that all of the processes in the source cluster had a privilege change relationship to at least one process in the destination cluster.

[00305] The node input to this model for a given time period includes process nodes that are running in that period. The value of a class of process nodes is "<username>".

[00306] The base relationship that is used for clustering is privilege change, either by the process changing its effective user ID, or by launching a child process which runs with a different user.

[00307] The physical input for this model includes process nodes (only), with the caveat that the complete ancestor hierarchy of process nodes active (i.e., running) for a given time period is provided as input even if an ancestor is not active in that time period. Note that effective user IDs of a process are represented as an array in the process node properties, and launch relationships are available from ppid_hash fields in the properties as well.

[00308] A new class event in this model is equivalent to seeing a user for the first time.

[00309] A new class to class edge event is equivalent to seeing the source user making a privilege change to the destination user for the first time.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00387

[00310] A Ct2Ct Model may cluster processes with the same CType that show similar launch behavior. For instance, if two processes with the same CType have launched processes with similar CTypes, then they could be clustered.

[00311] The node input to this model for a given time period includes process nodes that are running in that period. The value class of process nodes is CType (similar to how it is created for the PtypeConn Model).

[00312] The base relationship that is used for clustering is a parent process with a given CType launching a child process with another given destination CType.

[00313] The physical input for this model includes process nodes (only) with the caveat that the complete ancestor hierarchy active process nodes (i.e., that are running) for a given time period is provided as input even if an ancestor is not active in that time period. Note that launch relationships are available from ppid_hash fields in the process node properties.

[00314] An edge between a source cluster and destination cluster generated by this model means that all of the processes in the source cluster launched at least one process in the destination cluster.

[00315] A new class event in this model is equivalent to seeing a CType for the first time. Note that the same type of event will be generated by the PtypeConn Model as well.

[00316] A new class to class edge event is equivalent to seeing the source CType launching the destination CType for the first time.

[00317] An MTypeConn Model may cluster nodes of the same class that have similar connectivity relationships. For example, if two machines had similar incoming neighbors of the same class and outgoing neighbors of the same class, they could be clustered.

[00318] A new class event in this model will be generated for external IP addresses or (as applicable) domain names seen for the first time. Note that a new class to class to edge Machine, class to class for an IPSep or DNSName node will also be generated at the same time.

[00319] The membership edges generated by this model will refer to Machine, IPAddress, DNSName, and IPSep nodes in the base graph. Though the nodes provided to this model are IPAddress nodes instead of IPSep nodes, the membership edges it generates will refer to IPSep type nodes. Alternatively, the base graph can generate edges between Machine and IPSep node types. Note that the Machine to IPAddress edges have tcp_dst_ports/udp_dst_ports properties that can be used for this purpose.

[00320] The node input to this model for a given time period includes machine nodes that had connections in the time period and the base graph nodes of other types (IPAddress and DNSName) that were involved in those connections.

[00321] The base relationship is the connectivity relationship for the following type triplets:

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00388

[00322] * Machine, ConnectedTo, Machine

[00323] * Machine, ConnectedTo, IPAddress

[00324] * Machine, ConnectedTo, DNSName

[00325] * IPAddress, ConnectedTo, Machine, DNS, ConnectedTo, Machine

[00326] The edge inputs to this model are the corresponding ConnectedTo edges in the base graph.

[00327] Class Values:

[00328] Machine:

[00329] The class value for all Machine nodes is "Machine."

[00330] The machine_terms property in the Machine nodes is used, in various embodiments, for labeling machines that are clustered together. If a majority of the machines clustered together share a term in the machine_terms, that term can be used for labeling the cluster.

[00331] IPSep:

[00332] The class value for IPSep nodes is determined as follows:

[00333] if IP_internal then "IntIPS"

[00334] else

[00335] if severity = 0 then "<ip_addr>:<protocol>:<port>"

[00336] else "<IP_addr_BadIP>"

[00337] IPAddress:

[00338] The class value for IpAddress nodes is determined as follows:

[00339] if IP_internal then "IntIPC"

[00340] else

[00341] if severity = 0 then "ExtIPC"

[00342] else "ExtBadIPC"

[00343] DNSName:

[00344] The class value for DNSName nodes is determined as follows:

[00345] if severity = 0 then "<hostname>"

[00346] else then "<hostname>_BadIP"

[00347] An example structure for a New Class Event is now described.

[00348] The key field for this event type looks as follows (using the PtypeConn model as an example):

[00349] {

[00350] "node": {

[00351] "class": {

[00352] "cid": "httpd"

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00389

[00353] },

[00354] "key": {

[00355] "cid": "29654"

[00356] },

[00357] "type": "PtypeConn"

[00358] }

[00359] }

[00360] It contains the class value and also the ID of the cluster where that class value is observed. Multiple clusters can be observed with the same value in a given time period. It contains the class value and also the ID of the cluster where that class value is observed. Multiple clusters can be observed with the same value in a given time period. Accordingly, in some embodiments, GBM 154 generates multiple events of this type for the same class value.

[00361] The properties field looks as follows:

[00362] {

[00363] "set_size": 5

[00364] }

[00365] The set_size indicates the size of the cluster referenced in the keys field.

[00366] Conditions:

[00367] For a given model and time period, multiple NewClass events can be generated if there is more than one cluster in that class. NewNode events will not be generated separately in this case.

[00368] Example New Class to Class Edge Event structure:

[00369] The key field for this event type looks as follows (using the PtypeConn model as an example):

[00370] "edge": {

[00371] "dst_node": {

[00372] "class": {

[00373] "cid": "java war"

[00374] },

[00375] "key": {

[00376] "cid": "27635"

[00377] },

[00378] "type": "PtypeConn"

[00379] },

[00380] "src_node": {

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00390

[00381] "class": {

[00382] "cid": "IntIPC"

[00383] },

[00384] "key": {

[00385] "cid": "20881"

[00386] },

[00387] "type": "PtypeConn"

[00388] },

[00389] "type": "ConnectedTo"

[00390] }

[00391] }

[00392] The key field contains source and destination class values and also source and destination cluster identifiers (i.e., the src/dst_node:key.cid represents the src/dst cluster identifier).

[00393] In a given time period for a given model, an event of this type could involve multiple edges between different cluster pairs that have the same source and destination class values. GBM 154 can generate multiple events in this case with different source and destination cluster identifiers.

[00394] The props fields look as follows for this event type:

[00395] {

[00396] "dst_set_size": 2,

[00397] "src_set_size": 1

[00398] }

[00399] The source and destination sizes represent the sizes of the clusters given in the keys field.

[00400] Conditions:

[00401] For a given model and time period, multiple NewClassToClass events can be generated if there are more than one pair of clusters in that class pair. NewNodeToNode events are not generated separately in this case.

[00402] Combining Events at the Class Level: for a given model and time period, the following example types of events can represent multiple changes in the underlying GBM cluster level graph in terms of multiple new clusters or multiple new edges between clusters:

[00403] * NewClass

[00404] * NewEdgeClassToClass

[00405] * NewEdgeNodeToClass

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00391

[00406] * NewEdgeClassToNode

[00407] Multiple NewClass events with the same model and class can be output if there are multiple clusters in that new class.

[00408] Multiple NewEdgeClassToClass events with the same model and class pair can be output if there are multiple new cluster edges within that class pair.

[00409] Multiple NewEdgeNodeToClass events with the same model and destination class can be output if there are multiple new edges from the source cluster to the destination clusters in that destination class (the first time seeing this class as a destination cluster class for the source cluster).

[00410] Multiple NewEdgeClassToNode events with the same model and source class can be output if there are multiple new edges from source clusters to the destination clusters in that source class (the first time seeing this class as a source cluster class for the destination cluster).

[00411] These events may be combined at the class level and treated as a single event when it is desirable to view changes at the class level, e.g., when one wants to know when there is a new CType.

[00412] In some examples, different models may have partial overlap in the types of nodes they use from the base graph. Therefore, they can generate NewClass type events for the same class. NewClass events can also be combined across models when it is desirable to view changes at the class level.

[00413] Using techniques herein, actions can be associated with processes and (e.g., by associating processes with users) actions can thus also be associated with extended user sessions. Such information can be used to track user behavior correctly, even where a malicious user attempts to hide his trail by changing user identities (e.g., through lateral movement). Extended user session tracking can also be useful in operational use cases without malicious intent, e.g., where users make original logins with distinct usernames (e.g., “charlie” or “dave”) but then perform actions under a common username (e.g., “admin” or “support”). One such example is where multiple users with administrator privileges exist, and they need to gain superuser privilege to perform a particular type of maintenance. It may be desirable to know which operations are performed (as the superuser) by which original user when debugging issues. In the following examples describing extended user session tracking, reference is generally made to using the secure shell (ssh) protocol as implemented by openssh (on the server side) as the mechanism for logins. However, extended user session tracking is not limited to the ssh protocol or a particular limitation and the techniques described herein can be extended to other login mechanisms.

[00414] On any given machine, there will be a process that listens for and accepts ssh connections on a given port. This process can run the openssh server program running in daemon mode or it could be running another program (e.g., initd on a Linux system). In either case, a new process running openssh will be created for every new ssh login session and this process can be used to identify an ssh session on that machine. This process is called the "privileged" process in openssh.

[00415] After authentication of the ssh session, when an ssh client requests a shell or any other program to be run under that ssh session, a new process that runs that program will be created under (i.e., as a child of) the associated privileged process. If an ssh client requests port forwarding to be performed, the connections will be associated with the privileged process.

[00416] In modern operating systems such as Linux and Windows, each process has a parent process (except for the very first process) and when a new process is created the parent process is known. By tracking the parent-child hierarchy of processes, one can determine if a particular process is a descendant of a privileged openssh process and thus if it is associated with an ssh login session.

[00417] For user session tracking across machines (or on a single machine with multiple logins) in a distributed environment, it is established when two login sessions have a parent-child relationship. After that, the "original" login session, if any, for any given login session can be determined by following the parent relationship recursively.

[00418] Fig. 3F is a representation of a user logging into a first machine and then into a second machine from the first machine, as well as information associated with such actions. In the example of Fig. 3F, a user, Charlie, logs into Machine A (331) from a first IP address (332). As part of the login process, he provides a username (333). Once connected to Machine A, an openssh privileged process (334) is created to handle the connection for the user, and a terminal session is created and a bash process (335) is created as a child. Charlie launches an ssh client (336) from the shell, and uses it to connect (337) to Machine B (338). As with the connection he makes to Machine A, Charlie's connection to Machine B will have an associated incoming IP address (339), in this case, the IP address of Machine A. And, as part of the login process with Machine B, Charlie will provide a username (340) which need not be the same as username 333. An openssh privileged process (341) is created to handle the connection, and a terminal session and child bash process (342) will be created. From the command line of Machine B, Charlie launches a curl command (343), which opens an HTTP connection (2028) to an external Machine C (345).

[00419] Fig. 3G is an alternate representation of actions occurring in Fig. 3F, where events occurring on Machine A are indicated along line 350, and events occurring on Machine B are

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00393

indicated along line 351. As shown in Fig. 3G, an incoming ssh connection is received at Machine A (352). Charlie logs in (as user "x") and an ssh privileged process is created to handle Charlie's connection (353). A terminal session is created and a bash process is created (354) as a child of process 353. Charlie wants to ssh to Machine B, and so executes an ssh client on Machine A (355), providing credentials (as user "y") at 356. Charlie logs into Machine B, and an ssh privileged process is created to handle Charlie's connection (357). A terminal session is created and a bash process is created (358) as a child of process 357. Charlie then executes curl (359) to download content from an external domain (via connection 360).

[00420] The external domain could be a malicious domain, or it could be benign. Suppose the external domain is malicious (and, e.g., Charlie has malicious intent). It would be advantageous (e.g., for security reasons) to be able to trace the contact with the external domain back to Machine A, and then back to Charlie's IP address. Using techniques described herein (e.g., by correlating process information collected by various agents), such tracking of Charlie's activities back to his original login (330) can be accomplished. In particular, an extended user session can be tracked that associates Charlie's ssh processes together with a single original login and thus original user.

[00421] As described herein, software agents (such as agent 112) may run on machines (such as a machine that implements one of nodes 116) and detect new connections, processes, and/or logins. As also previously explained, such agents send associated records to data platform 12 which includes one or more datastores (e.g., data store 30) for persistently storing such data. Such data can be modeled using logical tables, also persisted in datastores (e.g., in a relational database that provides an SQL interface), allowing for querying of the data. Other datastores such as graph oriented databases and/or hybrid schemes can also be used.

[00422] The following identifiers are commonly used in the tables:

[00423] * MID

[00424] * PID_hash

[00425] An ssh login session can be identified uniquely by an (MID, PID_hash) tuple. The MID is a machine identifier that is unique to each machine, whether physical or virtual, across time and space. Operating systems use numbers called process identifiers (PIDs) to identify processes running at a given time. Over time processes may die and new processes may be started on a machine or the machine itself may restart. The PID is not necessarily unique across time in that the same PID value can be reused for different processes at different times. In order to track process descendants across time, one should therefore account for time as well. In order to be able to identify a process on a machine uniquely across time, another number called a PID_hash is generated for the process. In various embodiments, the PID_hash is generated using a

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00394

collision-resistant hash function that takes the PID, start time, and (in various embodiments, as applicable) other properties of a process.

[00426] Input data collected by agents comprises the input data model and is represented by the following logical tables:

[00427] * connections

[00428] * processes

[00429] * logins

[00430] A connections table may maintain records of TCP/IP connections observed on each machine. Example columns included in a connections table are as follows:

Column Name	Description
MID	Identifier of the machine that the connection was observed on.
start_time	Connection start time.
PID_hash	Identifier of the process that was associated with the connection.
src_IP_addr	Source IP address (the connection was initiated from this IP address).
src_port	Source port.
dst_IP_addr	Destination IP address (the connection was made to this IP address).
dst_port	Destination port.
Prot	Protocol (TCP or UDP).
Dir	Direction of the connection (incoming or outgoing) with respect to this machine.

[00431] The source fields (IP address and port) correspond to the side from which the connection was initiated. On the destination side, the agent associates an ssh connection with the privileged ssh process that is created for that connection.

[00432] For each connection in the system, there will be two records in the table, assuming that the machines on both sides of the connection capture the connection. These records can be matched based on equality of the tuple (src_IP_addr, src_port, dst_IP_addr, dst_port, Prot) and proximity of the start_time fields (e.g., with a one minute upper threshold between the start_time fields).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00395

[00433] A processes table maintains records of processes observed on each machine. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the process was observed on.
PID_hash	Identifier of the process.
start_time	Start time of the process.
exe_path	The executable path of the process.
PPID_hash	Identifier of the parent process.

[00434] A logins table may maintain records of logins to machines. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the login was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with login.
login_time	Time of login.
login_username	Username used in login.

[00435] Output data generated by session tracking is represented with the following logical tables:

[00436] * login-local-descendant

[00437] * login-connection

[00438] * login-lineage

[00439] Using data in these tables, it is possible to determine descendant processes of a given ssh login session across the environment (i.e., spanning machines). Conversely, given a process, it is possible to determine if it is an ssh login descendant as well as the original ssh login session for it if so.

[00440] A login-local-descendant table maintains the local (i.e., on the same machine) descendant processes of each ssh login session. It may have the following columns:

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00396

Column Name	Description
MID	Identifier of the machine that the login was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with login.
login_time	Time of login.
login_username	Username used in login.

[00441] A login-connections table may maintain the connections associated with ssh logins. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the process was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with the login.
login_time	Time of login.
login_username	The username used in the login.
src_IP_addr	Source IP address (connection was initiated from this IP address).
src_port	Source port.
dst_IP_addr	Destination IP address (connection was made to this IP address).
dst_port	Destination port.

[00442] A login-lineage table may maintain the lineage of ssh login sessions. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the ssh login was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with the login.
parent_MID	Identifier of the machine that the parent ssh login was observed on.
parent_sshd_PID_hash	Identifier of the sshd privileged process associated with the parent login.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00397

origin_MID	Identifier of the machine that the origin ssh login was observed on.
origin_sshd_PID_hash	Identifier of the sshd privileged process associated with the origin login.

[00443] The parent_MID and parent_sshd_PID_hash columns can be null if there is no parent ssh login. In that case, the (MID, sshd_PID_hash) tuple will be the same as the (origin_MID, origin_sshd_PID_hash) tuple.

[00444] Fig. 3H illustrates an example of a process for performing extended user tracking. In various embodiments, process 361 is performed by data platform 12. The process begins at 362 when data associated with activities occurring in a network environment (such as entity A's datacenter) is received. One example of such data that can be received at 362 is agent-collected data described above (e.g., in conjunction with process 200). At 363, the received network activity is used to identify user login activity. And, at 364, a logical graph that links the user login activity to at least one user and at least one process is generated (or updated, as applicable). Additional detail regarding process 361, and in particular, portions 363 and 364 of process 361 are described in more detail below (e.g., in conjunction with discussion of Fig. 3J).

[00445] Fig. 3I depicts a representation of a user logging into a first machine, then into a second machine from the first machine, and then making an external connection. The scenario depicted in Fig. 3I is used to describe an example of processing that can be performed on data collected by agents to generate extended user session tracking information. Fig. 3I is an alternate depiction of the information shown in Figs. 3F and 3G.

[00446] At time t1 (365), a first ssh connection is made to Machine A (366) from an external source (367) by a user having a username of "X." In the following example, suppose the external source has an IP address of 1.1.1.10 and uses source port 10000 to connect to Machine A (which has an IP address of 2.2.2.20 and a destination port 22). External source 367 is considered an external source because its IP address is outside of the environment being monitored (e.g., is a node outside of entity A's datacenter, connecting to a node inside of entity A's datacenter).

[00447] A first ssh login session LS1 is created on machine A for user X. The privileged openssh process for this login is A1 (368). Under the login session LS1, the user creates a bash shell process with PID_hash A2 (369).

[00448] At time t2 (370), inside the bash shell process A2, the user runs an ssh program under a new process A3 (371) to log in to machine B (372) with a different username ("Y"). In particular, an ssh connection is made from source IP address 2.2.2.20 and source port 10001 (Machine A's

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00398

source information) to destination IP address 2.2.2.21 and destination port 22 (Machine B's destination information).

[00449] A second ssh login session LS2 is created on machine B for user Y. The privileged openssh process for this login is B1 (373). Under the login session LS2, the user creates a bash shell process with PID_hash B2 (374).

[00450] At time t3 (376), inside the bash shell process B2, the user runs a curl command under a new process B3 (377) to download a file from an external destination (378). In particular, an HTTPS connection is made from source IP address 2.2.2.21 and source port 10002 (Machine B's source information) to external destination IP address 3.3.3.30 and destination port 443 (the external destination's information).

[00451] Using techniques described herein, it is possible to determine the original user who initiated the connection to external destination 378, which in this example is a user having the username X on machine A (where the extended user session can be determined to start with ssh login session LS1).

[00452] Based on local descendant tracking, the following determinations can be on machine A and B without yet having performed additional processing (described in more detail below):

[00453] * A3 is a descendant of A1 and thus associated with LS1.

[00454] * The connection to the external domain from machine B is initiated by B3.

[00455] * B3 is a descendant of B1 and is thus associated with LS2.

[00456] * Connection to the external domain is thus associated with LS2.

[00457] An association between A3 and LS2 can be established based on the fact that LS2 was created based on an ssh connection initiated from A3. Accordingly, it can be determined that LS2 is a child of LS1.

[00458] To determine the user responsible for making the connection to the external destination (e.g., if it were a known bad destination), first, the process that made the connection would be traced, i.e., from B3 to LS2. Then LS2 would be traced to LS1 (i.e., LS1 is the origin login session for LS2). Thus the user for this connection is the user for LS1, i.e., X. As represented in Fig. 3I, one can visualize the tracing by following the links (in the reverse direction of arrows) from external destination 378 to A1 (368).

[00459] In the example scenario, it is assumed that both ssh connections occur in the same analysis period. However, the approaches described herein will also work for connections and processes that are created in different time periods.

[00460] Fig. 3J illustrates an example of a process for performing extended user tracking. In various embodiments, process 380 is performed periodically (e.g., once an hour in a batch fashion) by ssh tracker 148 to generate new output data. In general, batch processing allows for

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00399

efficient analysis of large volumes of data. However, the approach can be adapted, as applicable, to process input data on a record-by-record fashion while maintaining the same logical data processing flow. As applicable the results of a given portion of process 380 are stored for use in a subsequent portion.

[00461] The process begins at 381 when new ssh connection records are identified. In particular, new ssh connections started during the current time period are identified by querying the connections table. The query uses filters on the start_time and dst_port columns. The values of the range filter on the start_time column are based on the current time period. The dst_port column is checked against ssh listening port(s). By default, the ssh listening port number is 22. However, as this could vary across environments, the port(s) that openssh servers are listening to in the environment can be determined by data collection agents dynamically and used as the filter value for the dst_port as applicable. In the scenario depicted in Fig. 3I, the query result will generate the records shown in Fig. 3K. Note that for the connection between machine A and B, the two machines are likely to report start_time values that are not exactly the same but close enough to be considered matching (e.g., within one minute or another appropriate amount of time). In the above table, they are shown to be the same for simplicity.

[00462] At 382, ssh connection records reported from source and destination sides of the same connection are matched. The ssh connection records (e.g., returned from the query at 381) are matched based on the following criteria:

[00463] * The five tuples (src_IP, dst_IP, IP_prot, src_port, dst_port) of the connection records must match.

[00464] * The delta between the start times of the connections must be within a limit that would account for the worst case clock difference expected between two machines in the environment and typical connection setup latency.

[00465] * If there are multiple matches possible, then the match with the smallest time delta is chosen.

[00466] Note that record 390 from machine A for the incoming connection from the external source cannot be matched with another record as there is an agent only on the destination side for this connection. Example output of portion 382 of process 380 is shown in Fig. 3L. The values in the dst_PID_hash column (391) are that of the sshd privileged process associated with ssh logins.

[00467] At 383, new logins during the current time period are identified by querying the logins table. The query uses a range filter on the login_time column with values based on the current time period. In the example depicted in Fig. 3I, the query result will generate the records depicted in Fig. 3M.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00400

[00468] At 384, matched ssh connection records created at 382 and new login records created at 383 are joined to create new records that will eventually be stored in the login-connection table. The join condition is that dst_MID of the matched connection record is equal to the MID of the login record and the dst_PID_hash of the matched connection record is equal to the sshd_PID_hash of the login record. In the example depicted in Fig. 3I, the processing performed at 384 will generate the records depicted in Fig. 3N.

[00469] At 385, login-local-descendant records in the lookback time period are identified. It is possible that a process that is created in a previous time period makes an ssh connection in the current analysis batch period. Although not depicted in the example illustrated in Fig. 3I, consider a case where bash process A2 does not create ssh process A3 right away but instead that the ssh connection A3 later makes to machine B is processed in a subsequent time period than the one where A2 was processed. While processing this subsequent time period in which processes A3 and B1 are seen, knowledge of A2 would be useful in establishing that B1 is associated with A3 (via ssh connection) which is associated with A2 (via process parentage) which in turn would be useful in establishing that the parent of the second ssh login is the first ssh login. The time period for which look back is performed can be limited to reduce the amount of historical data that is considered. However, this is not a requirement (and the amount of look back can be determined, e.g., based on available processing resources). The login local descendants in the lookback time period can be identified by querying the login-local-descendant table. The query uses a range filter on the login_time column where the range is from start_time_of_current_period - lookback_time to start_time_of_current_period. (No records as a result of performing 385 on the scenario depicted in Fig. 3I are obtained, as only a single time period is applicable in the example scenario.)

[00470] At 386, new processes that are started in the current time period are identified by querying the processes table. The query uses a range filter on the start_time column with values based on the current time period. In the example depicted in Fig. 3I, the processing performed at 386 will generate the records depicted in Fig. 3O.

[00471] At 387, new login-local-descendant records are identified. The purpose is to determine whether any of the new processes in the current time period are descendants of an ssh login process and if so to create records that will be stored in the login-local-descendant table for them. In order to do so, the parent-child relationships between the processes are recursively followed. Either a top down or bottom up approach can be used. In a top down approach, the ssh local descendants in the lookback period identified at 385, along with new ssh login processes in the current period identified at 384 are considered as possible ancestors for the new processes in the current period identified at 386.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00401

[00472] Conceptually, the recursive approach can be considered to include multiple sub-steps where new processes that are identified to be ssh local descendants in the current sub-step are considered as ancestors for the next step. In the example scenario depicted in Fig. 3I, the following descendancy relationships will be established in two sub-steps:

[00473] Sub-step 1:

[00474] Process A2 is a local descendant of LS1 (i.e., MID = A, sshd_PID_hash = A1) because it is a child of process A1 which is the login process for LS1.

[00475] Process B2 is a local descendant of LS2 (i.e., MID = B, sshd_PID_hash = B1) because it is a child of process B1 which is the login process for LS2.

[00476] Sub-step 2:

[00477] Process A3 is a local descendant of LS1 because it is a child of process A2 which is associated to LS1 in sub-step 1.

[00478] Process B3 is a local descendant of LS2 because it is a child of process B1 which is associated to LS2 in sub-step 1.

[00479] Implementation portion 387 can use a datastore that supports recursive query capabilities, or, queries can be constructed to process multiple conceptual sub-steps at once. In the example depicted in Fig. 3I, the processing performed at 387 will generate the records depicted in Fig. 3P. Note that the ssh privileged processes associated with the logins are also included as they are part of the login session.

[00480] At 388, the lineage of new ssh logins created in the current time period is determined by associating their ssh connections to source processes that may be descendants of other ssh logins (which may have been created in the current period or previous time periods). In order to do so, first an attempt is made to join the new ssh login connections in the current period (identified at 384) with the combination of the login local descendants in the lookback period (identified at 385) and the login local descendants in the current time period (identified at 386). This will create adjacency relationships between child and parent logins. In the example depicted in Fig. 3I, the second ssh login connection will be associated with process A3 and an adjacency relationship between the two login sessions will be created (as illustrated in Fig. 3Q).

[00481] Next, the adjacency relationships are used to find the original login sessions. While not shown in the sample scenario, there could be multiple ssh logins in a chain in the current time period, in which case a recursive approach (as in 387) could be used. At the conclusion of portion 388, the login lineage records depicted in Fig. 3R will be generated.

[00482] Finally, at 389, output data is generated. In particular, the new login-connection, login-local-descendant, and login-lineage records generated at 384, 387, and 388 are inserted into their respective output tables (e.g., in a transaction manner).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00402

[00483] An alternate approach to matching TCP connections between machines running an agent is for the client to generate a connection GUID and send it in the connection request (e.g., the SYN packet) it sends and for the server to extract the GUID from the request. If two connection records from two machines have the same GUID, they are for the same connection. Both the client and server will store the GUID (if it exists) in the connection records they maintain and report. On the client side, the agent can configure the network stack (e.g., using IP tables functionality on Linux) to intercept an outgoing TCP SYN packet and modify it to add the generated GUID as a TCP option. On the server side, the agent already extracts TCP SYN packets and thus can look for this option and extract the GUID if it exists.

[00484] Example graph-based user tracking and threat detection embodiments associated with data platform 12 will now be described. Administrators and other users of network environments (e.g., entity A's datacenter 104) often change roles to perform tasks. As one example, suppose that at the start of a workday, an administrator (hereinafter "Joe Smith") logs in to a console, using an individualized account (e.g., username=joe.smith). Joe performs various tasks as himself (e.g., answering emails, generating status reports, writing code, etc.). For other tasks (e.g., performing updates), Joe may require different/additional permission than his individual account has (e.g., root privileges). One way Joe can gain access to such permissions is by using sudo, which will allow Joe to run a single command with root privileges. Another way Joe can gain access to such permissions is by su or otherwise logging into a shell as root. After gaining root privileges, another thing that Joe can do is switch identities. As one example, to perform administrative tasks, Joe may use "su help" or "su database-admin" to become (respectively) the help user or the database-admin user on a system. He may also connect from one machine to another, potentially changing identities along the way (e.g., logging in as joe.smith at a first console, and connecting to a database server as database-admin). When he's completed various administrative tasks, Joe can relinquish his root privileges by closing out of any additional shells created, reverting back to a shell created for user joe.smith.

[00485] While there are many legitimate reasons for Joe to change his identity throughout the day, such changes may also correspond to nefarious activity. Joe himself may be nefarious, or Joe's account (joe.smith) may have been compromised by a third party (whether an "outsider" outside of entity A's network, or an "insider"). Using techniques described herein, the behavior of users of the environment can be tracked (including across multiple accounts and/or multiple machines) and modeled (e.g., using various graphs described herein). Such models can be used to generate alerts (e.g., to anomalous user behavior). Such models can also be used forensically, e.g., helping an investigator visualize various aspects of a network and activities that have

occurred, and to attribute particular types of actions (e.g., network connections or file accesses) to specific users.

[00486] In a typical day in a datacenter, a user (e.g., Joe Smith) will log in, run various processes, and (optionally) log out. The user will typically log in from the same set of IP addresses, from IP addresses within the same geographical area (e.g., city or country), or from historically known IP addresses/geographical areas (i.e., ones the user has previously/occasionally used). A deviation from the user's typical (or historical) behavior indicates a change in login behavior. However, it does not necessarily mean that a breach has occurred. Once logged into a datacenter, a user may take a variety of actions. As a first example, a user might execute a binary/script. Such binary/script might communicate with other nodes in the datacenter, or outside of the datacenter, and transfer data to the user (e.g., executing "curl" to obtain data from a service external to the datacenter). As a second example, the user can similarly transfer data (e.g., out of the datacenter), such as by using POST. As a third example, a user might change privilege (one or more times), at which point the user can send/receive data as per above. As a fourth example, a user might connect to a different machine within the datacenter (one or more times), at which point the user can send/receive data as per the above.

[00487] In various embodiments, the above information associated with user behavior is broken into four tiers. The tiers represent example types of information that data platform 12 can use in modeling user behavior:

[00488] 1. The user's entry point (e.g., domains, IP addresses, and/or geolocation information such as country/city) from which a user logs in.

[00489] 2. The login user and machine class.

[00490] 3. Binaries, executables, processes, etc. a user launches.

[00491] 4. Internal servers with which the user (or any of the user's processes, child processes, etc.) communicates, and external contacts (e.g., domains, IP addresses, and/or geolocation information such as country/city) with which the user communicates (i.e., transfers data).

[00492] In the event of a security breach, being able to concretely answer questions about such information can be very important. And, collectively, such information is useful in providing an end-to-end path (e.g., for performing investigations).

[00493] In the following example, suppose a user ("UserA") logs into a machine ("Machine01") from a first IP address ("IP01"). Machine01 is inside a datacenter. UserA then launches a script ("runnable.sh") on Machine01. From Machine01, UserA next logs into a second machine ("Machine02") via ssh, also as UserA, also within the datacenter. On Machine02, UserA again launches a script ("new_runnable.sh"). On Machine02, UserA then changes privilege, becoming root on Machine02. From Machine02, UserA (now as root) logs into a third machine

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00404

("Machine03") in the datacenter via ssh, as root on Machine03. As root on Machine03, the user executes a script ("collect_data.sh") on Machine03. The script internally communicates (as root) to a MySQL-based service internal to the datacenter, and downloads data from the MySQL-based service. Finally, as root on Machine03, the user externally communicates with a server outside the datacenter ("External01"), using a POST command. To summarize what has occurred, in this example, the source/entry point is IP01. Data is transferred to an external server External01. The machine performing the transfer to External01 is Machine03. The user transferring the data is "root" (on Machine03), while the actual user (hiding behind root) is UserA.

[00494] In the above scenario, the "original user" (ultimately responsible for transmitting data to External01) is UserA, who logged in from IP01. Each of the processes ultimately started by UserA, whether started at the command line (tty) such as "runnable.sh" or started after an ssh connection such as "new_runnable.sh," and whether as UserA, or as a subsequent identity, are all examples of child processes which can be arranged into a process hierarchy.

[00495] As previously mentioned, machines can be clustered together logically into machine clusters. One approach to clustering is to classify machines based on information such as the types of services they provide/binaries they have installed upon them/processes they execute. Machines sharing a given machine class (as they share common binaries/services/etc.) will behave similarly to one another. Each machine in a datacenter can be assigned to a machine cluster, and each machine cluster can be assigned an identifier (also referred to herein as a machine class). One or more tags can also be assigned to a given machine class (e.g., database_servers_west or prod_web_frontend). One approach to assigning a tag to a machine class is to apply term frequency analysis (e.g., TF/IDF) to the applications run by a given machine class, selecting as tags those most unique to the class. Data platform 12 can use behavioral baselines taken for a class of machines to identify deviations from the baseline (e.g., by a particular machine in the class).

[00496] Fig. 3S illustrates an example of a process for detecting anomalies. In various embodiments, process 392 is performed by data platform 12. As explained above, a given session will have an original user. And, each action taken by the original user can be tied back to the original user, despite privilege changes and/or lateral movement throughout a datacenter. Process 392 begins at 393 when log data associated with a user session (and thus an original user) is received. At 394, a logical graph is generated, using at least a portion of the collected data. When an anomaly is detected (395), it can be recorded, and as applicable, an alert is generated (396). The following are examples of graphs that can be generated (e.g., at 394), with corresponding examples of anomalies that can be detected (e.g., at 395) and alerted upon (e.g., at 396).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00405

[00497] Fig. 4A illustrates a representation of an embodiment of an insider behavior graph. In the example of Fig. 4A, each node in the graph can be: (1) a cluster of users; (2) a cluster of launched processes; (3) a cluster of processes/servers running on a machine class; (4) a cluster of external IP addresses (of incoming clients); or (5) a cluster of external servers based on DNS/IP/etc. As depicted in Fig. 4A, graph data is vertically tiered into four tiers. Tier 0 (400) corresponds to entry point information (e.g., domains, IP addresses, and/or geolocation information) associated with a client entering the datacenter from an external entry point. Entry points are clustered together based on such information. Tier 1 (401) corresponds to a user on a machine class, with a given user on a given machine class represented as a node. Tier 2 (402) corresponds to launched processes, child processes, and/or interactive processes. Processes for a given user and having similar connectivity (e.g., sharing the processes they launch and the machines with which they communicate) are grouped into nodes. Finally, Tier 3 (403) corresponds to the services/servers/domains/IP addresses with which processes communicate. A relationship between the tiers can be stated as follows: Tier 0 nodes log in to tier 1 nodes. Tier 1 nodes launch tier 2 nodes. Tier 2 nodes connect to tier 3 nodes.

[00498] The inclusion of an original user in both Tier 1 and Tier 2 allows for horizontal tiering. Such horizontal tiering ensures that there is no overlap between any two users in Tier 1 and Tier 2. Such lack of overlap provides for faster searching of an end-to-end path (e.g., one starting with a Tier 0 node and terminating at a Tier 3 node). Horizontal tiering also helps in establishing baseline insider behavior. For example, by building an hourly insider behavior graph, new edges/changes in edges between nodes in Tier 1 and Tier 2 can be identified. Any such changes correspond to a change associated with the original user. And, any such changes can be surfaced as anomalous and alerts can be generated.

[00499] As explained above, Tier 1 corresponds to a user (e.g., user "U") logging into a machine having a particular machine class (e.g., machine class "M"). Tier 2 is a cluster of processes having command line similarity (e.g., CType "C"), having an original user "U," and running as a particular effective user (e.g., user "U1"). The value of U1 may be the same as U (e.g., joe.smith in both cases), or the value of U1 may be different (e.g., U=joe.smith and U1=root). Thus, while an edge may be present from a Tier 1 node to a Tier 2 node, the effective user in the Tier 2 node may or may not match the original user (while the original user in the Tier 2 node will match the original user in the Tier 1 node).

[00500] A change from a user U into a user U1 can take place in a variety of ways. Examples include where U becomes U1 on the same machine (e.g., via su), and also where U sshes to other machine(s). In both situations, U can perform multiple changes, and can combine approaches. For example, U can become U1 on a first machine, ssh to a second machine (as U1), become U2

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00406

on the second machine, and ssh to a third machine (whether as user U2 or user U3). In various embodiments, the complexity of how user U ultimately becomes U3 (or U5, etc.) is hidden from a viewer of an insider behavior graph, and only an original user (e.g., U) and the effective user of a given node (e.g., U5) are depicted. As applicable (e.g., if desired by a viewer of the insider behavior graph), additional detail about the path (e.g., an end-to-end path of edges from user U to user U5) can be surfaced (e.g., via user interactions with nodes).

[00501] Fig. 4B illustrates an example of a portion of an insider behavior graph (e.g., as rendered in a web browser). In the example shown, node 405 (the external IP address, 52.32.40.231) is an example of a Tier 0 node, and represents an entry point into a datacenter. As indicated by directional arrows 406 and 407, two users, "aruneli_prod" and "harish_prod," both made use of the source IP 52.32.40.231 when logging in between 5pm and 6pm on Sunday July 30 (408). Nodes 409 and 410 are examples of Tier 1 nodes, having aruneli_prod and harish_prod as associated respective original users. As previously mentioned, Tier 1 nodes correspond to a combination of a user and a machine class. In the example depicted in Fig. 4B, the machine class associated with nodes 409 and 410 is hidden from view to simplify visualization, but can be surfaced to a viewer of interface 404 (e.g., when the user clicks on node 409 or 410).

[00502] Nodes 414-423 are examples of Tier 2 nodes – processes that are launched by users in Tier 1 and their child, grandchild, etc. processes. Note that also depicted in Fig. 4B is a Tier 1 node 411 that corresponds to a user, "root," that logged in to a machine cluster from within the datacenter (i.e., has an entry point within the datacenter). Nodes 425-1 and 425-2 are examples of Tier 3 nodes – internal/external IP addresses, servers, etc., with which Tier 2 nodes communicate.

[00503] In the example shown in Fig. 4B, a viewer of interface 404 has clicked on node 423. As indicated in region 426, the user running the marathon container is "root." However, by following the directional arrows in the graph backwards from node 423 (i.e. from right to left), the viewer can determine that the original user, responsible for node 423, is "aruneli_prod," who logged into the datacenter from IP 52.32.40.231.

[00504] The following are examples of changes that can be tracked using an insider behavior graph model:

[00505] * A user logs in from a new IP address.

[00506] * A user logs in from a geolocation not previously used by that user.

[00507] * A user logs into a new machine class.

[00508] * A user launches a process not previously used by that user.

[00509] * A user connects to an internal server to which the user has not previously connected.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00407

[00510] * An original user communicates with an external server (or external server known to be malicious) with which that user has not previously communicated.

[00511] * A user communicates with an external server which has a geolocation not previously used by that user.

[00512] Such changes can be surfaced as alerts, e.g., to help an administrator determine when/what anomalous behavior occurs within a datacenter. Further, the behavior graph model can be used (e.g., during forensic analysis) to answer questions helpful during an investigation. Examples of such questions include:

[00513] * Was there any new login activity (Tier 0) in the timeframe being investigated? As one example, has a user logged in from an IP address with unknown geolocation information? Similarly, has a user started communicating externally with a new Tier 3 node (e.g., one with unknown geolocation information).

[00514] * Has there been any suspicious login activity (Tier 0) in the timeframe being investigated? As one example, has a user logged in from an IP address that corresponds to a known bad IP address as maintained by Threat aggregator 150? Similarly, has there been any suspicious Tier 3 activity?

[00515] * Were any anomalous connections made within the datacenter during the timeframe being investigated? As one example, suppose a given user ("Frank") typically enters a datacenter from a particular IP address (or range of IP addresses), and then connects to a first machine type (e.g., bastion), and then to a second machine type (e.g., database_prod). If Frank has directly connected to database_prod (instead of first going through bastion) during the timeframe, this can be surfaced using the insider graph.

[00516] * Who is (the original user) responsible for running a particular process?

[00517] An example of an insider behavior graph being used in an investigation is depicted in Figs. 4C and 4D. Fig. 4C depicts a baseline of behavior for a user, "Bill." As shown in Fig. 4C, Bill typically logs into a datacenter from the IP address, 71.198.44.40 (427). He typically makes use of ssh (428), and sudo (429), makes use of a set of typical applications (430) and connects (as root) with the external service, api.lacework.net (431).

[00518] Suppose Bill's credentials are compromised by a nefarious outsider ("Eve"). Fig. 4D depicts an embodiment of how the graph depicted in Fig. 4C would appear once Eve begins exfiltrating data from the datacenter. Eve logs into the datacenter (using Bill's credentials) from 52.5.66.8 (432). As Bill, Eve escalates her privilege to root (e.g., via su), and then becomes a different user, Alex (e.g., via su alex). As Alex, Eve executes a script, "sneak.sh" (433), which launches another script, "post.sh" (434), which contacts external server 435 which has an IP address of 52.5.66.7, and transmits data to it. Edges 436-439 each represent changes in Bill's

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00408

behavior. As previously mentioned, such changes can be detected as anomalies and associated alerts can be generated. As a first example, Bill logging in from an IP address he has not previously logged in from (436) can generate an alert. As a second example, while Bill does typically make use of sudo (429), he has not previously executed sneak.sh (433) or post.sh (434) and the execution of those scripts can generate alerts as well. As a third example, Bill has not previously communicated with server 435, and an alert can be generated when he does so (439). Considered individually, each of edges 436-439 may indicate nefarious behavior, or may be benign. As an example of a benign edge, suppose Bill begins working from a home office two days a week. The first time he logs in from his home office (i.e., from an IP address that is not 71.198.44.40), an alert can be generated that he has logged in from a new location. Over time, however, as Bill continues to log in from his home office but otherwise engages in typical activities, Bill's graph will evolve to include logins from both 71.198.44.40 and his home office as baseline behavior. Similarly, if Bill begins using a new tool in his job, an alert can be generated the first time he executes the tool, but over time will become part of his baseline.

[00519] In some cases, a single edge can indicate a serious threat. For example, if server 432 (or 435) is included in a known bad IP listing, edge 436 (or 439) indicates compromise. An alert that includes an appropriate severity level (e.g., "threat level high") can be generated. In other cases, a combination of edges could indicate a threat (where a single edge might otherwise result in a lesser warning). In the example shown in Fig. 4D, the presence of multiple new edges is indicative of a serious threat. Of note, even though "sneak.sh" and "post.sh" were executed by Alex, because data platform 12 also keeps track of an original user, the compromise of user B's account will be discovered.

[00520] Fig. 4E illustrates a representation of an embodiment of a user login graph. In the example of Fig. 4E, tier 0 (440) clusters source IP addresses as belonging to a particular country (including an "unknown" country) or as a known bad IP. Tier 1 (441) clusters user logins, and tier 2 (442) clusters type of machine class into which a user is logging in. The user login graph tracks the typical login behavior of users. By interacting with a representation of the graph, answers to questions such as the following can be obtained:

[00521] * Where is a user logging in from?

[00522] * Have any users logged in from a known bad address?

[00523] * Have any non-developer users accessed development machines?

[00524] * Which machines does a particular user access?

[00525] Examples of alerts that can be generated using the user login graph include:

[00526] * A user logs in from a known bad IP address.

[00527] * A user logs in from a new country for the first time.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00409

[00528] * A new user logs into the datacenter for the first time.

[00529] * A user accesses a machine class that the user has not previously accessed.

[00530] One way to track privilege changes in a datacenter is by monitoring a process hierarchy of processes. To help filter out noisy commands/processes such as "su –u," the hierarchy of processes can be constrained to those associated with network activity. In a *nix system, each process has two identifiers assigned to it, a process identifier (PID) and a parent process identifier (PPID). When such a system starts, the initial process is assigned a PID 0. Each user process has a corresponding parent process.

[00531] Using techniques described herein, a graph can be constructed (also referred to herein as a privilege change graph) which models privilege changes. In particular, a graph can be constructed which identifies where a process P1 launches a process P2, where P1 and P2 each have an associated user U1 and U2, with U1 being an original user, and U2 being an effective user. In the graph, each node is a cluster of processes (sharing a CType) executed by a particular (original) user. As all the processes in the cluster belong to the same user, a label that can be used for the cluster is the user's username. An edge in the graph, from a first node to a second node, indicates that a user of the first node changed its privilege to the user of the second node.

[00532] Fig. 4F illustrates an example of a privilege change graph. In the example shown in Fig. 4F, each node (e.g., nodes 444 and 445) represents a user. Privilege changes are indicated by edges, such as edge 446.

[00533] As with other graphs, anomalies in graph 443 can be used to generate alerts. Three examples of such alerts are as follows:

[00534] * New user entering the datacenter. Any time a new user enters the datacenter and runs a process, the graph will show a new node, with a new CType. This indicates a new user has been detected within the datacenter. Fig. 4F is a representation of an example of an interface that depicts such an alert. Specifically, as indicated in region 447, an alert for the time period 1pm-2pm on June 8 was generated. The alert identifies that a new user, Bill (448) executed a process.

[00535] *Privilege change. As explained above, a new edge, from a first node (user A) to a second node (user B) indicates that user A has changed privilege to user B.

[00536] * Privilege escalation. Privilege escalation is a particular case of privilege change, in which the first user becomes root.

[00537] An example of an anomalous privilege change and an example of an anomalous privilege escalation are each depicted in graph 450 of Fig. 4G. In particular, as indicated in region 451, two alerts for the time period 2pm-3pm on June 8 were generated (corresponding to the detection of the two anomalous events). In region 452, root has changed privilege to the user "daemon," which root has not previously done. This anomaly is indicated to the user by

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00410

highlighting the daemon node (e.g., outlining it in a particular color, e.g., red). As indicated by edge 453, Bill has escalated his privilege to the user root (which can similarly be highlighted in region 454). This action by Bill represents a privilege escalation.

[00538] An Extensible query interface for dynamic data compositions and filter applications will now be described.

[00539] As described herein, datacenters are highly dynamic environments. And, different customers of data platform 12 (e.g., entity A vs. entity B) may have different/disparate needs/requirements of data platform 12, e.g., due to having different types of assets, different applications, etc. Further, as time progresses, new software tools will be developed, new types of anomalous behavior will be possible (and should be detectable), etc. In various embodiments, data platform 12 makes use of predefined relational schema (including by having different predefined relational schema for different customers). However, the complexity and cost of maintaining/updating such predefined relational schema can rapidly become problematic – particularly where the schema includes a mix of relational, nested, and hierarchical (graph) datasets. In other embodiments, the data models and filtering applications used by data platform 12 are extensible. As will be described in more detail below, in various embodiments, data platform 12 supports dynamic query generation by automatic discovery of join relations via static or dynamic filtering key specifications among composable data sets. This allows a user of data platform 12 to be agnostic to modifications made to existing data sets as well as creation of new data sets. The extensible query interface also provides a declarative and configurable specification for optimizing internal data generation and derivations.

[00540] As will also be described in more detail below, data platform 12 is configured to dynamically translate user interactions (e.g., received via web app 120) into SQL queries (and without the user needing to know how to write queries). Such queries can then be performed (e.g., by query service 166) against any compatible backend (e.g., data store 30).

[00541] Fig. 4H illustrates an example of a user interacting with a portion of an interface. When a user visits data platform 12 (e.g., via web app 120 using a browser), data is extracted from data store 30 as needed (e.g., by query service 166), to provide the user with information, such as the visualizations depicted variously herein). As the user continues to interact with such visualizations (e.g., clicking on graph nodes, entering text into search boxes, navigating between tabs (e.g., tab 455 vs. 465)), such interactions act as triggers that cause query service 166 to continue to obtain information from data store 30 as needed (and as described in more detail below).

[00542] In the example shown in Fig. 4H, user A is viewing a dashboard that provides various information about entity A users (455), during the time period March 2 at midnight – March 25 at

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00411

7pm (which she selected by interacting with region 456). Various statistical information is presented to user A in region 457. Region 458 presents a timeline of events that occurred during the selected time period. User A has opted to list only the critical, high, and medium events during the time period by clicking on the associated boxes (459-461). A total of 55 low severity, and 155 info-only events also occurred during the time period. Each time user A interacts with an element in Fig. 4H (e.g., clicks on box 461, clicks on link 464-1, or clicks on tab 465), her actions are translated/formalized into filters on the data set and used to dynamically generate SQL queries. The SQL queries are generated transparently to user A (and also to a designer of the user interface shown in Fig. 4H).

[00543] User A notes in the timeline (462) that a user, Harish, connected to a known bad server (examplebad.com) using wget, an event that has a critical severity level. User A can click on region 463 to expand details about the event inline (which will display, for example, the text "External connection made to known bad host examplebad.com at port 80 from application 'wget' running on host dev1.lacework.internal as user harish") directly below line 462. User A can also click on link 464-1, which will take her to a dossier for the event (depicted in Fig. 4I). As will be described in more detail below, a dossier is a template for a collection of visualizations.

[00544] As shown in interface 466, the event of Harish using wget to contact examplebad.com on March 16 was assigned an event ID of 9291 by data platform 12 (467). For convenience to user A, the event is also added to her dashboard in region 476 as a bookmark (468). A summary of the event is depicted in region 469. By interacting with boxes shown in region 470, user A can see a timeline of related events. In this case, user A has indicated that she would like to see other events involving the wget application (by clicking box 471). Events of critical and medium security involving wget occurred during the one hour window selected in region 472.

[00545] Region 473 automatically provides user A with answers to questions that may be helpful to have answers to while investigating event 9291. If user A clicks on any of the links in the event description (474), she will be taken to a corresponding dossier for the link. As one example, suppose user A clicks on link 475. She will then be presented with interface 477 shown in Fig. 4J.

[00546] Interface 477 is an embodiment of a dossier for a domain. In this example, the domain is "examplebad.com," as shown in region 478. Suppose user A would like to track down more information about interactions entity A resources have made with examplebad.com between January 1 and March 20. She selects the appropriate time period in region 479 and information in the other portions of interface 477 automatically update to provide various information corresponding to the selected time frame. As one example, user A can see that contact was made

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00412

with examplebad.com a total of 17 times during the time period (480), as well as a list of each contact (481). Various statistical information is also included in the dossier for the time period (482). If she scrolls down in interface 477, user A will be able to view various polygraphs associated with examplebad.com, such as an application-communication polygraph (483).

[00547] Data stored in data store 30 can be internally organized as an activity graph. In the activity graph, nodes are also referred to as Entities. Activities generated by Entities are modeled as directional edges between nodes. Thus, each edge is an activity between two Entities. One example of an Activity is a "login" Activity, in which a user Entity logs into a machine Entity (with a directed edge from the user to the machine). A second example of an Activity is a "launch" Activity, in which a parent process launches a child process (with a directed edge from the parent to the child). A third example of an Activity is a "DNS query" Activity, in which either a process or a machine performs a query (with a directed edge from the requestor to the answer, e.g., an edge from a process to www.example.com). A fourth example of an Activity is a network "connected to" Activity, in which processes, IP addresses, and listen ports can connect to each other (with a directed edge from the initiator to the server).

[00548] As will be described in more detail below, query service 166 provides either relational views or graph views on top of data stored in data store 30. Typically, a user will want to see data filtered using the activity graph. For example, if an entity was not involved in an activity in a given time period, that entity should be filtered out of query results. Thus, a request to show "all machines" in a given time frame will be interpreted as "show distinct machines that were active" during the time frame.

[00549] Query service 166 relies on three main data model elements: fields, entities, and filters. As used herein, a field is a collection of values with the same type (logical and physical). A field can be represented in a variety of ways, including: 1. a column of relations (table/view), 2. a return field from another entity, 3. an SQL aggregation (e.g., COUNT, SUM, etc.), 4. an SQL expression with the references of other fields specified, and 5. a nested field of a JSON object. As viewed by query service 166, an entity is a collection of fields that describe a data set. The data set can be composed in a variety of ways, including: 1. a relational table, 2. a parameterized SQL statement, 3. DynamicSQL created by a Java function, and 4. join/project/aggregate/subclass of other entities. Some fields are common for all entities. One example of such a field is a "first observed" timestamp (when first use of the entity was detected). A second example of such a field is the entity classification type (e.g., one of: 1. Machine (on which an agent is installed), 2. Process, 3. Binary, 4. UID, 5. IP, 6. DNS Information, 7. ListenPort, and 8. PType). A third example of such a field is a "last observed" timestamp.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00413

[00550] A filter is an operator that: 1. takes an entity and field values as inputs, 2. a valid SQL expression with specific reference(s) of entity fields, or 3. is a conjunct/disjunct of filters. As will be described in more detail below, filters can be used to filter data in various ways, and limit data returned by query service 166 without changing the associated data set.

[00551] As mentioned above, a dossier is a template for a collection of visualizations. Each visualization (e.g., the box including chart 484) has a corresponding card, which identifies particular target information needed (e.g., from data store 30) to generate the visualization. In various embodiments, data platform 12 maintains a global set of dossiers/cards. Users of data platform 12 such as user A can build their own dashboard interfaces using preexisting dossiers/cards as components, and/or they can make use of a default dashboard (which incorporates various of such dossiers/cards).

[00552] A JSON file can be used to store multiple cards (e.g., as part of a query service catalog). A particular card is represented by a single JSON object with a unique name as a field name.

[00553] Each card may be described by the following named fields:

[00554] TYPE: the type of the card. Example values include:

[00555] * Entity (the default type)

[00556] * SQL

[00557] * Filters

[00558] * DynamicSQL

[00559] * graphFilter

[00560] * graph

[00561] * Function

[00562] * Template

[00563] PARAMETERS: a JSON array object that contains an array of parameter objects with the following fields:

[00564] * name (the name of the parameter)

[00565] * required (a Boolean flag indicating whether the parameter is required or not)

[00566] * default (a default value of the parameter)

[00567] * props (a generic JSON object for properties of the parameter. Possible values are: “utype” (a user defined type), and “scope” (an optional property to configure a namespace of the parameter))

[00568] * value (a value for the parameter - non-null to override the default value defined in nested source entities)

[00569] SOURCES: a JSON array object explicitly specifying references of input entities. Each source reference has the following attributes:

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00414

[00570] * name (the card/entity name or fully-qualified Table name)

[00571] * type (required for base Table entity)

[00572] * alias (an alias to access this source entity in other fields (e.g., returns, filters, groups, etc))

[00573] RETURNS: a required JSON array object of a return field object. A return field object can be described by the following attributes:

[00574] * field (a valid field name from a source entity)

[00575] * expr (a valid SQL scalar expression. References to input fields of source entities are specified in the format of #{Entity.Field}. Parameters can also be used in the expression in the format of ${ParameterName})

[00576] * type (the type of field, which is required for return fields specified by expr. It is also required for all return fields of an Entity with an SQL type)

[00577] * alias (the unique alias for return field)

[00578] * aggr (possible aggregations are: COUNT, COUNT_DISTINCT, DISTINCT, MAX, MIN, AVG, SUM, FIRST_VALUE, LAST_VALUE)

[00579] * case (JSON array object represents conditional expressions “when” and “expr”)

[00580] * fieldsFrom, and, except (specification for projections from a source entity with excluded fields)

[00581] * props (general JSON object for properties of the return field. Possible properties include: “filterGroup,” “title,” “format,” and “utype”)

[00582] PROPS: generic JSON objects for other entity properties

[00583] SQL: a JSON array of string literals for SQL statements. Each string literal can contain parameterized expressions ${ParameterName} and/or composable entity by #{EntityName}

[00584] GRAPH: required for graph entity. Has the following required fields:

[00585] * source (including “type,” “props,” and “keys”)

[00586] * target (including “type,” “props,” and “keys”)

[00587] * edge (including “type” and “props”)

[00588] JOINS: a JSON array of join operators. Possible fields for a join operator include:

[00589] * type (possible join types include: “loj” - Left Outer Join, “join” - Inner Join, “in” - Semi Join, “implicit” - Implicit Join)

[00590] * left (a left hand side field of join)

[00591] * right (a right hand side field of join)

[00592] * keys (key columns for multi-way joins)

[00593] * order (a join order of multi-way joins)

[00594] FKEYS: a JSON array of FilterKey(s). The fields for a FilterKey are:

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00415

[00595] * type (type of FilterKey)

[00596] * fieldRefs (reference(s) to return fields of an entity defined in the sources field)

[00597] * alias (an alias of the FilterKey, used in implicit join specification)

[00598] FILTERS: a JSON array of filters (conjunct). Possible fields for a filter include:

[00599] * type (types of filters, including: “eq” - equivalent to SQL =, “ne” - equivalent to SQL <>, “ge” - equivalent to SQL >=, “gt” - equivalent to SQL >, “le” - equivalent to SQL <=, “lt” - equivalent to SQL <, “like” - equivalent to SQL LIKE, “not_like” - equivalent to SQL NOT LIKE, “rlike” - equivalent to SQL RLIKE (Snowflake specific), “not_rlike” - equivalent to SQL NOT RLIKE (Snowflake specific), “in” - equivalent to SQL IN, “not_in” - equivalent to SQL NOT IN)

[00600] * expr (generic SQL expression)

[00601] * field (field name)

[00602] * value (single value)

[00603] * values (for both IN and NOT IN)

[00604] ORDERS: a JSON array of ORDER BY for returning fields. Possible attributes for the ORDER BY clause include:

[00605] * field (field ordinal index (1 based) or field alias)

[00606] * order (asc/desc, default is ascending order)

[00607] GROUPS: a JSON array of GROUP BY for returning fields. Field attributes are:

[00608] * field (ordinal index (1 based) or alias from the return fields)

[00609] LIMIT: a limit for the number of records to be returned

[00610] OFFSET: an offset of starting position of returned data. Used in combination with limit for pagination.

[00611] Suppose customers of data platform 12 (e.g., entity A and entity B) request new data transformations or a new aggregation of data from an existing data set (as well as a corresponding visualization for the newly defined data set). As mentioned above, the data models and filtering applications used by data platform 12 are extensible. Thus, two example scenarios of extensibility are (1) extending the filter data set, and (2) extending a FilterKey in the filter data set.

[00612] Data platform 12 includes a query service catalog that enumerates cards available to users of data platform 12. New cards can be included for use in data platform 12 by being added to the query service catalog (e.g., by an operator of data platform 12). For reusability and maintainability, a single external-facing card (e.g., available for use in a dossier) can be composed of multiple (nested) internal cards. Each newly added card (whether external or internal) will also have associated FilterKey(s) defined. A user interface (UI) developer can then

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00416

develop a visualization for the new data set in one or more dossier templates. The same external card can be used in multiple dossier templates, and a given external card can be used multiple times in the same dossier (e.g., after customization). Examples of external card customization include customization via parameters, ordering, and/or various mappings of external data fields (columns).

[00613] As mentioned above, a second extensibility scenario is one in which a FilterKey in the filter data set is extended (i.e., existing template functions are used to define a new data set). As also mentioned above, data sets used by data platform 12 are composable/reusable/extensible, irrespective of whether the data sets are relational or graph data sets. One example data set is the User Tracking polygraph, which is generated as a graph data set (comprising nodes and edges). Like other polygraphs, User Tracking is an external data set that can be visualized both as a graph (via the nodes and edges) and can also be used as a filter data set for other cards, via the cluster identifier (CID) field.

[00614] As mentioned above, as users such as user A navigate through/interact with interfaces provided by data platform 12 (e.g., as shown in Fig. 4H), such interactions trigger query service 166 to generate and perform queries against data store 30. Dynamic composition of filter datasets can be implemented using FilterKeys and FilterKey Types. A FilterKey can be defined as a list of columns and/or fields in a nested structure (e.g., JSON). Instances of the same FilterKey Type can be formed as an Implicit Join Group. The same instance of a FilterKey can participate in different Implicit Join Groups. A list of relationships among all possible Implicit Join Groups is represented as a Join graph for the entire search space to create a final data filter set by traversing edges and producing Join Path(s).

[00615] Each card (e.g., as stored in the query service catalog and used in a dossier) can be introspected by a /card/describe/CardID REST request.

[00616] At runtime (e.g., whenever it receives a request from web app 120), query service 166 parses the list of implicit joins and creates a Join graph to manifest relationships of FilterKeys among Entities. A Join graph (an example of which is depicted in Fig. 4K) comprises a list of Join Link(s). A Join Link represents each implicit join group by the same FilterKey type. A Join Link maintains a reverse map (Entity-to-FilterKey) of FilterKeys and their Entities. As previously mentioned, Entities can have more than one FilterKey defined. The reverse map guarantees one FilterKey per Entity can be used for each JoinLink. Each JoinLink also maintains a list of entities for the priority order of joins. Each JoinLink is also responsible for creating and adding directional edge(s) to graphs. An edge represents a possible join between two Entities.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00417

[00617] At runtime, each Implicit Join uses the Join graph to find all possible join paths. The search of possible join paths starts with the outer FilterKey of an implicit join. One approach is to use a shortest path approach, with breadth first traversal and subject to the following criteria:

[00618] * Use the priority order list of Join Links for all entities in the same implicit join group.

[00619] * Stop when a node (Entity) is reached which has local filter(s).

[00620] * Include all join paths at the same level (depth).

[00621] * Exclude join paths based on the predefined rules (path of edges).

[00622] Fig. 4L illustrates an example of a process for dynamically generating and executing a query. In various embodiments, process 485 is performed by data platform 12. The process begins at 486 when a request is received to filter information associated with activities within a network environment. One example of such a request occurs in response to user A clicking on tab 465. Another example of such a request occurs in response to user A clicking on link 464-1. Yet another example of such a request occurs in response to user A clicking on link 464-2 and selecting (e.g., from a dropdown) an option to filter (e.g., include, exclude) based on specific criteria that she provides (e.g., an IP address, a username, a range of criteria, etc.).

[00623] At 487, a query is generated based on an implicit join. One example of processing that can be performed at 487 is as follows. As explained above, one way dynamic composition of filter datasets can be implemented is by using FilterKeys and FilterKey Types. And, instances of the same FilterKey Type can be formed as an Implicit Join Group. A Join graph for the entire search space can be constructed from a list of all relationships among all possible Join Groups. And, a final data filter set can be created by traversing edges and producing one or more Join Paths. Finally, the shortest path in the join paths is used to generate an SQL query string.

[00624] One approach to generating an SQL query string is to use a query building library (authored in an appropriate language such as Java). For example, a common interface “sqlGen” may be used in conjunction with process 485 is as follows. First, a card/entity is composed by a list of input cards/entities, where each input card recursively is composed by its own list of input cards. This nested structure can be visualized as a tree of query blocks(SELECT) in standard SQL constructs. SQL generation can be performed as the traversal of the tree from root to leaf entities (top-down), calling the sqlGen of each entity. Each entity can be treated as a subclass of the Java class(Entity). An implicit join filter (EntityFilter) is implemented as a subclass of Entity, similar to the right hand side of a SQL semi-join operator. Unlike the static SQL semi-join construct, it is conditionally and recursively generated even if it is specified in the input sources of the JSON specification. Another recursive interface can also be used in conjunction with process 485, preSQLGen, which is primarily the entry point for EntityFilter to run a search and generate nested implicit join filters. During preSQLGen recursive invocations, the applicability

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00418

of implicit join filters is examined and pushed down to its input subquery list. Another top-down traversal, pullUpCachable, can be used to pull up common sub-query blocks, including those dynamically generated by preSQLGen, such that SELECT statements of those cacheable blocks are generated only once at top-level WITH clauses. A recursive interface, sqlWith, is used to generate nested subqueries inside WITH clauses. The recursive calls of a sqlWith function can generate nested WITH clauses as well. An sqlFrom function can be used to generate SQL FROM clauses by referencing those subquery blocks in the WITH clauses. It also produces INNER/OUTER join operators based on the joins in the specification. Another recursive interface, sqlWhere, can be used to generate conjuncts and disjuncts of local predicates and semi-join predicates based on implicit join transformations. Further, sqlProject, sqlGroupBy, sqlOrderBy, and sqlLimitOffset can respectively be used to translate the corresponding directives in JSON spec to SQL SELECT list, GROUP BY, ORDER BY, and LIMIT/OFFSET clauses.

[00625] Returning to process 485, at 488, the query (generated at 487) is used to respond to the request. As one example of the processing performed at 488, the generated query is used to query data store 30 and provide (e.g., to web app 120) fact data formatted in accordance with a schema (e.g., as associated with a card associated with the request received at 486).

[00626] Although the examples described herein largely relate to embodiments where data is collected from agents and ultimately stored in a data store such as those provided by Snowflake, in other embodiments data that is collected from agents and other sources may be stored in different ways. For example, data that is collected from agents and other sources may be stored in a data warehouse, data lake, data mart, and/or any other data store.

[00627] A data warehouse may be embodied as an analytic database (e.g., a relational database) that is created from two or more data sources. Such a data warehouse may be leveraged to store historical data, often on the scale of petabytes. Data warehouses may have compute and memory resources for running complicated queries and generating reports. Data warehouses may be the data sources for business intelligence ('BI') systems, machine learning applications, and/or other applications. By leveraging a data warehouse, data that has been copied into the data warehouse may be indexed for good analytic query performance, without affecting the write performance of a database (e.g., an Online Transaction Processing ('OLTP') database). Data warehouses also enable the joining data from multiple sources for analysis. For example, a sales OLTP application probably has no need to know about the weather at various sales locations, but sales predictions could take advantage of that data. By adding historical weather data to a data warehouse, it would be possible to factor it into models of historical sales data.

[00628] Data lakes, which store files of data in their native format, may be considered as "schema on read" resources. As such, any application that reads data from the lake may impose

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00419

its own types and relationships on the data. Data warehouses, on the other hand, are "schema on write," meaning that data types, indexes, and relationships are imposed on the data as it is stored in the EDW. "Schema on read" resources may be beneficial for data that may be used in several contexts and poses little risk of losing data. "Schema on write" resources may be beneficial for data that has a specific purpose, and good for data that must relate properly to data from other sources. Such data stores may include data that is encrypted using homomorphic encryption, data encrypted using privacy-preserving encryption, smart contracts, non-fungible tokens, decentralized finance, and other techniques.

[00629] Data marts may contain data oriented towards a specific business line whereas data warehouses contain enterprise-wide data. Data marts may be dependent on a data warehouse, independent of the data warehouse (e.g., drawn from an operational database or external source), or a hybrid of the two. In embodiments described herein, different types of data stores (including combinations thereof) may be leveraged. Such data stores may be proprietary or may be embodied as vendor provided products or services such as, for example, Google BigQuery, Druid, Amazon Redshift, IBM Db2, Dremio, Databricks Lakehouse Platform, Cloudera, Azure Synapse Analytics, and others.

[00630] The deployments (e.g., a customer's cloud deployment) that are analyzed, monitored, evaluated, or otherwise observed by the systems described herein (e.g., systems that include components such as the platform 12 of Fig. 1D, the data collection agents described herein, and/or other components) may be provisioned, deployed, and/or managed using infrastructure as code ('IaC'). IaC involves the managing and/or provisioning of infrastructure through code instead of through manual processes. With IaC, configuration files may be created that include infrastructure specifications. IaC can be beneficial as configurations may be edited and distributed, while also ensuring that environments are provisioned in a consistent manner. IaC approaches may be enabled in a variety of ways including, for example, using IaC software tools such as Terraform by HashiCorp. Through the usage of such tools, users may define and provide data center infrastructure using JavaScript Object Notation ('JSON'), YAML, proprietary formats, or some other format. In some embodiments, the configuration files may be used to emulate a cloud deployment for the purposes of analyzing the emulated cloud deployment using the systems described herein. Likewise, the configuration files themselves may be used as inputs to the systems described herein, such that the configuration files may be inspected to identify vulnerabilities, misconfigurations, violations of regulatory requirements, or other issues. In fact, configuration files for multiple cloud deployments may even be used by the systems described herein to identify best practices, to identify configuration files that deviate from typical configuration files, to identify configuration files with similarities to deployments that have been

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00420

determined to be deficient in some way, or the configuration files may be leveraged in some other ways to detect vulnerabilities, misconfigurations, violations of regulatory requirements, or other issues prior to deploying an infrastructure that is described in the configuration files. In some embodiments the techniques described herein may be use in multi-cloud, multi-tenant, cross-cloud, cross-tenant, cross-user, industry cloud, digital platform, and other scenarios depending on specific need or situation.

[00631] In some embodiments, the deployments that are analyzed, monitored, evaluated, or otherwise observed by the systems described herein (e.g., systems that include components such as the platform 12 of Fig. 1D, the data collection agents described herein, and/or other components) may be monitored to determine the extent to which a particular component has experienced "drift" relative to its associated IaC configuration. Discrepancies between how cloud resources were defined in an IaC configuration file and how they are currently configured in runtime may be identified and remediation workflows may be initiated to generate an alert, reconfigure the deployment, or take some other action. Such discrepancies may occur for a variety of reasons. Such discrepancies may occur, for example, due to maintenance operations being performed, due to incident response tasks being carried out, or for some other reason. Readers will appreciate that while IaC helps avoid initial misconfigurations of a deployment by codifying and enforcing resource creation, resource configuration, security policies, and so on, the systems described herein may prevent unwanted drift from occurring during runtime and after a deployment has been created in accordance with an IaC configuration.

[00632] In some embodiments, the deployments (e.g., a customer's cloud deployment) that are analyzed, monitored, evaluated, or otherwise observed by the systems described herein (e.g., systems that include components such as the platform 12 of Fig. 1D, the data collection agents described herein, and/or other components) may also be provisioned, deployed, and/or managed using security as code ('SaC'). SaC extends IaC concepts by defining cybersecurity policies and/or standards programmatically, so that the policies and/or standards can be referenced automatically in the configuration scripts used to provision cloud deployments. Stated differently, SaC can automate policy implementation and cloud deployments may even be compared with the policies to prevent "drift." For example, if a policy is created where all personally identifiable information ('PII') or personal health information ('PHI') must be encrypted when it is stored, that policy is translated into a process that is automatically launched whenever a developer submits code, and code that violates the policy may be automatically rejected.

[00633] In some embodiments, SaC may be implemented by initially classifying workloads (e.g., by sensitivity, by criticality, by deployment model, by segment). Policies that can be instantiated

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00421

as code may subsequently be designed. For example, compute-related policies may be designed, access-related policies may be designed, application-related policies may be designed, network-related policies may be designed, data-related policies may be designed, and so on. Security as code may then be instantiated through architecture and automation, as successful implementation of SaC can benefit from making key architectural-design decisions and executing the right automation capabilities. Next, operating model protections may be built and supported. For example, an operating model may "shift left" to maximize self-service and achieve full-life-cycle security automation (e.g., by standardizing common development toolchains, CI/CD pipelines, and the like). In such an example, security policies and access controls may be part of the pipeline, automatic code review and bug/defect detection may be performed, automated build processes may be performed, vulnerability scanning may be performed, checks against a risk-control framework may be made, and other tasks may be performed all before deploying an infrastructure or components thereof.

[00634] The systems described herein may be useful in analyzing, monitoring, evaluating, or otherwise observing a GitOps environment. In a GitOps environment, Git may be viewed as the one and only source of truth. As such, GitOps may require that the desired state of infrastructure (e.g., a customer's cloud deployment) be stored in version control such that the entire audit trail of changes to such infrastructure can be viewed or audited. In a GitOps environment, all changes to infrastructure are embodied as fully traceable commits that are associated with committer information, commit IDs, time stamps, and/or other information. In such an embodiment, both an application and the infrastructure (e.g., a customer's cloud deployment) that supports the execution of the application are therefore versioned artifacts and can be audited using the gold standards of software development and delivery. Readers will appreciate that while the systems described herein are described as analyzing, monitoring, evaluating, or otherwise observing a GitOps environment, in other embodiments other source control mechanisms may be utilized for creating infrastructure, making changes to infrastructure, and so on. In these embodiments, the systems described herein may similarly be used for analyzing, monitoring, evaluating, or otherwise observing such environments.

[00635] As described in other portions of the present disclosure, the systems described herein may be used to analyze, monitor, evaluate, or otherwise observe a customer's cloud deployment. While securing traditional datacenters requires managing and securing an IP-based perimeter with networks and firewalls, hardware security modules ('HSMs'), security information and event management ('SIEM') technologies, and other physical access restrictions, such solutions are not particularly useful when applied to cloud deployments. As such, the systems described

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00422

herein may be configured to interact with and even monitor other solutions that are appropriate for cloud deployments such as, for example, “zero trust” solutions.

[00636] A zero trust security model (a.k.a., zero trust architecture) describes an approach to the design and implementation of IT systems. A primary concept behind zero trust is that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified. Zero trust security models help prevent successful breaches by eliminating the concept of trust from an organization's network architecture. Zero trust security models can include multiple forms of authentication and authorization (e.g., machine authentication and authorization, human/user authentication and authorization) and can also be used to control multiple types of accesses or interactions (e.g., machine-to-machine access, human-to-machine access).

[00637] In some embodiments, the systems described herein may be configured to interact with zero trust solutions in a variety of ways. For example, agents that collect input data for the systems described herein (or other components of such systems) may be configured to access various machines, applications, data sources, or other entity through a zero trust solution, especially where local instances of the systems described herein are deployed at edge locations. Likewise, given that zero trust solutions may be part of a customer’s cloud deployment, the zero trust solution itself may be monitored to identify vulnerabilities, anomalies, and so on. For example, network traffic to and from the zero trust solution may be analyzed, the zero trust solution may be monitored to detect unusual interactions, log files generated by the zero trust solution may be gathered and analyzed, and so on.

[00638] In some embodiments, the systems described herein may leverage various tools and mechanisms in the process of performing its primary tasks (e.g., monitoring a cloud deployment). For example, Linux eBPF is mechanism for writing code to be executed in the Linux kernel space. Through the usage of eBPF, user mode processes can hook into specific trace points in the kernel and access data structures and other information. For example, eBPF may be used to gather information that enables the systems described herein to attribute the utilization of networking resources or network traffic to specific processes. This may be useful in analyzing the behavior of a particular process, which may be important for observability/SIEM.

[00639] The systems described may be configured to collect security event logs (or any other type of log or similar record of activity) and telemetry in real time for threat detection, for analyzing compliance requirements, or for other purposes. In such embodiments, the systems described herein may analyze telemetry in real time (or near real time), as well as historical telemetry, to detect attacks or other activities of interest. The attacks or activities of interest may be analyzed to determine their potential severity and impact on an organization. In fact, the

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00423

attacks or activities of interest may be reported, and relevant events, logs, or other information may be stored for subsequent examination.

[00640] In one embodiment, systems described herein may be configured to collect security event logs (or any other type of log or similar record of activity) and telemetry in real time to provide customers with a SIEM or SIEM-like solution. SIEM technology aggregates event data produced by security devices, network infrastructure, systems, applications, or other source. Centralizing all of the data that may be generated by a cloud deployment may be challenging for a traditional SIEM, however, as each component in a cloud deployment may generate log data or other forms of machine data, such that the collective amount of data that can be used to monitor the cloud deployment can grow to be quite large. A traditional SIEM architecture, where data is centralized and aggregated, can quickly result in large amounts of data that may be expensive to store, process, retain, and so on. As such, SIEM technologies may frequently be implemented such that silos are created to separate the data.

[00641] In some embodiments of the present disclosure, data that is ingested by the systems described herein may be stored in a cloud-based data warehouse such as those provided by Snowflake and others. Given that companies like Snowflake offer data analytics and other services to operate on data that is stored in their data warehouses, in some embodiments one or more of the components of the systems described herein may be deployed in or near Snowflake as part of a secure data lake architecture (a.k.a., a security data lake architecture, a security data lake/warehouse). In such an embodiment, components of the systems described herein may be deployed in or near Snowflake to collect data, transform data, analyze data for the purposes of detecting threats or vulnerabilities, initiate remediation workflows, generate alerts, or perform any of the other functions that can be performed by the systems described herein. In such embodiments, data may be received from a variety of sources (e.g., EDR or EDR-like tools that handle endpoint data, cloud access security broker ('CASB') or CASB-like tools that handle data describing interactions with cloud applications, Identity and Access Management ('IAM') or IAM-like tools, and many others), normalized for storage in a data warehouse, and such normalized data may be used by the systems described herein. In fact, the systems described herein may actually implement the data sources (e.g., an EDR tool, a CASB tool, an IAM tool) described above.

[00642] In some embodiments one data source that is ingested by the systems described herein is log data, although other forms of data such as network telemetry data (flows and packets) and/or many other forms of data may also be utilized. In some embodiments, event data can be combined with contextual information about users, assets, threats, vulnerabilities, and so on, for the purposes of scoring, prioritization and expediting investigations. In some embodiments, input

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00424

data may be normalized, so that events, data, contextual information, or other information from disparate sources can be analyzed more efficiently for specific purposes (e.g., network security event monitoring, user activity monitoring, compliance reporting). The embodiments described here offer real-time analysis of events for security monitoring, advanced analysis of user and entity behaviors, querying and long-range analytics for historical analysis, other support for incident investigation and management, reporting (for compliance requirements, for example), and other functionality.

[00643] In some embodiments, the systems described herein may be part of an application performance monitoring ('APM') solution. APM software and tools enable the observation of application behavior, observation of its infrastructure dependencies, observation of users and business key performance indicators ('KPIs') throughout the application's life cycle, and more. The applications being observed may be developed internally, as packaged applications, as software as a service ('SaaS'), or embodied in some other ways. In such embodiments, the systems described herein may provide one or more of the following capabilities:

[00644] The ability to operate as an analytics platform that ingests, analyzes, and builds context from traces, metrics, logs, and other sources.

[00645] Automated discovery and mapping of an application and its infrastructure components.

[00646] Observation of an application's complete transactional behavior, including interactions over a data communications network.

[00647] Monitoring of applications running on mobile (native and browser) and desktop devices.

[00648] Identification of probable root causes of an application's performance problems and their impact on business outcomes.

[00649] Integration capabilities with automation and service management tools.

[00650] Analysis of business KPIs and user journeys (for example, login to check-out).

[00651] Domain-agnostic analytics capabilities for integrating data from third-party sources.

[00652] Endpoint monitoring to understand the user experience and its impact on business outcomes.

[00653] Support for virtual desktop infrastructure ('VDI') monitoring.

[00654] In embodiments where the systems described herein are used for APM, some components of the system may be modified, other components may be added, some components may be removed, and other components may remain the same. In such an example, similar mechanisms as described elsewhere in this disclosure may be used to collect information from the applications, network resources used by the application, and so on. The graph based modelling techniques may also be leveraged to perform some of the functions mentioned above, or other functions as needed.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00425

[00655] In some embodiments, the systems described herein may be part of a solution for developing and/or managing artificial intelligence ('AI') or machine learning ('ML') applications. For example, the systems described herein may be part of an AutoML tool that automate the tasks associated with developing and deploying ML models. In such an example, the systems described herein may perform various functions as part of an AutoML tool such as, for example, monitoring the performance of a series of processes, microservices, and so on that are used to collectively form the AutoML tool. In other embodiments, the systems described herein may perform other functions as part of an AutoML tool or may be used to monitor, analyze, or otherwise observe an environment that the AutoML tool is deployed within.

[00656] In some embodiments, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include other forms of AI/ML tools. For example, the systems described herein may manage, analyze, or otherwise observe deployments that include AI services. AI services are, like other resources in an as-a-service model, ready-made models and AI applications that are consumable as services and made available through APIs. In such an example, rather than using their own data to build and train models for common activities, organizations may access pre-trained models that accomplish specific tasks. Whether an organization needs natural language processing ('NLP'), automatic speech recognition ('ASR'), image recognition, or some other capability, AI services simply plug-and-play into an application through an API. Likewise, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include other forms of AI/ML tools such as Amazon Sagemaker (or other cloud machine-learning platform that enables developers to create, train, and deploy ML models) and related services such as Data Wrangler (a service to accelerate data prep for ML) and Pipelines (a CI/CD service for ML).

[00657] In some embodiments, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include various data services. For example, data services may include secure data sharing services, data marketplace services, private data exchanges services, and others. Secure data sharing services can allow access to live data from its original location, where those who are granted access to the data simply reference the data in a controlled and secure manner, without latency or contention from concurrent users. Because changes to data are made to a single version, data remains up-to-date for all consumers, which ensures data models are always using the latest version of such data. Data marketplace services operate as a single location to access live, ready-to-query data (or data that is otherwise ready for some other use). A data marketplace can even include a "feature stores," which can allow data scientists to repurpose existing work. For example, once a data scientist has converted raw data into a metric

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00426

(e.g., costs of goods sold), this universal metric can be found quickly and used by other data scientists for quick analysis against that data.

[00658] In some embodiments, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include distributed training engines or similar mechanisms such as, for example, such as tools built on Dask. Dask is an open source library for parallel computing that is written in Python. Dask is designed to enable data scientists to improve model accuracy faster, as Dask enables data scientists can do everything in Python end-to-end, which means that they no longer need to convert their code to execute in environments like Apache Spark. The result is reduced complexity and increased efficiency. The systems described herein may also be used to manage, analyze, or otherwise observe deployments that include technologies such as RAPIDS (an open source Python framework which is built on top of Dask). RAPIDS optimizes compute time and speed by providing data pipelines and executing data science code entirely on graphics processing units (GPUs) rather than CPUs. Multi-cluster, shared data architecture, DataFrames, Java user-defined functions (UDF) are supported to enable trained models to run within a data warehouse.

[00659] In some embodiments, the systems described herein may be leveraged for the specific use case of detecting and/or remediating ransomware attacks and/or other malicious action taken with respect to data, systems, and/or other resources associated with one or more entities. Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to such data unless a ransom is paid. In such embodiments, ransomware attacks may be carried out in a manner such that patterns (e.g., specific process-to-process communications, specific data access patterns, unusual amounts of encryption/re-encryption activities) emerge, where the systems described herein may monitor for such patterns. Alternatively, ransomware attacks may involve behavior that deviates from normal behavior of a cloud deployment that is not experiencing a ransomware attack, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a ransomware attack.

[00660] In some embodiments, particular policies may be put in place the systems described herein may be configured to enforce such policies as part of an effort to thwart ransomware attacks. For example, particular network sharing protocols (e.g., Common Internet File System ('CIFS'), Network File System ('NFS')) may be avoided when implementing storage for backup data, policies that protect backup systems may be implemented and enforced to ensure that usable backups are always available, multifactor authentication for particular accounts may be utilized and accounts may be configured with the minimum privilege required to function,

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00427

isolated recovery environments may be created and isolation may be monitored and enforced to ensure the integrity of the recovery environment, and so on. As described in the present disclosure, the systems described herein may be configured to explicitly enforce such policies or may be configured to detect unusual activity that represents a violation of such policies, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a violation of a particular policy.

[00661] Readers will appreciate that ransomware attacks are often deployed as part of a larger attack that may involve, for example:

[00662] Penetration of the network through means such as, for example, stolen credentials and remote access malware.

[00663] Stealing of credentials for critical system accounts, including subverting critical administrative accounts that control systems such as backup, Active Directory ('AD'), DNS, storage admin consoles, and/or other key systems.

[00664] Attacks on a backup administration console to turn off or modify backup jobs, change retention policies, or even provide a roadmap to where sensitive application data is stored.

[00665] Data theft attacks.

[00666] As a result of the many aspects that are part of a ransomware attack, embodiments of the present disclosure may be configured as follows:

[00667] The systems may include one or more components that detect malicious activity based on the behavior of a process.

[00668] The systems may include one or more components that store indicator of compromise ('IOC') or indicator of attack ('IOA') data for retrospective analysis.

[00669] The systems may include one or more components that detect and block fileless malware attacks.

[00670] The systems may include one or more components that remove malware automatically when detected.

[00671] The systems may include a cloud-based, SaaS-style, multitenant infrastructure.

[00672] The systems may include one or more components that identify changes made by malware and provide the recommended remediation steps or a rollback capability.

[00673] The systems may include one or more components that detect various application vulnerabilities and memory exploit techniques.

[00674] The systems may include one or more components that continue to collect suspicious event data even when a managed endpoint is outside of an organization's network.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00428

[00675] The systems may include one or more components that perform static, on-demand malware detection scans of folders, drives, devices, or other entities.

[00676] The systems may include data loss prevention (DLP) functionality.

[00677] In some embodiments, the systems described herein may manage, analyze, or otherwise observe deployments that include deception technologies. Deception technologies allow for the use of decoys that may be generated based on scans of true network areas and data. Such decoys may be deployed as mock networks running on the same infrastructure as the real networks, but when an intruder attempts to enter the real network, they are directed to the false network and security is immediately notified. Such technologies may be useful for detecting and stopping various types of cyber threats such as, for example, Advanced Persistent Threats ('APTs'), malware, ransomware, credential dumping, lateral movement and malicious insiders. To continue to outsmart increasingly sophisticated attackers, these solutions may continuously deploy, support, refresh and respond to deception alerts.

[00678] In some embodiments, the systems described herein may manage, analyze, or otherwise observe deployments that include various authentication technologies, such as multi-factor authentication and role-based authentication. In fact, the authentication technologies may be included in the set of resources that are managed, analyzed, or otherwise observed as interactions with the authentication technologies may monitored. Likewise, log files or other information retained by the authentication technologies may be gathered by one or more agents and used as input to the systems described herein.

[00679] In some embodiments, the systems described herein may be leveraged for the specific use case of detecting supply chain attacks. More specifically, the systems described herein may be used to monitor a deployment that includes software components, virtualized hardware components, and other components of an organization's supply chain such that interactions with an outside partner or provider with access to an organization's systems and data can be monitored. In such embodiments, supply chain attacks may be carried out in a manner such that patterns (e.g., specific interactions between internal and external systems) emerge, where the systems described herein may monitor for such patterns. Alternatively, supply chain attacks may involve behavior that deviates from normal behavior of a cloud deployment that is not experiencing a supply chain attack, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a supply chain attack.

[00680] In some embodiments, the systems described herein may be leveraged for other specific use cases such as, for example, detecting the presence of (or preventing infiltration from) cryptocurrency miners (e.g., bitcoin miners), token miners, hashing activity, non-fungible token

activity, other viruses, other malware, and so on. As described in the present disclosure, the systems described herein may monitor for such threats using known patterns or by detecting unusual activity, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a particular type of threat, intrusion, vulnerability, and so on.

[00681] The systems described herein may also be leveraged for endpoint protection, such the systems described herein form all of or part of an endpoint protection platform. In such an embodiment, agents, sensors, or similar mechanisms may be deployed on or near managed endpoints such as computers, servers, virtualized hardware, internet of things ('IotT') devices, mobile devices, phones, tablets, watches, other personal digital devices, storage devices, thumb drives, secure data storage cards, or some other entity. In such an example, the endpoint protection platform may provide functionality such as:

[00682] Prevention and protection against security threats including malware that uses file-based and fileless exploits.

[00683] The ability to apply control (allow/block) to access of software, scripts, processes, microservices, and so on.

[00684] The ability to detect and prevent threats using behavioral analysis of device activity, application activity, user activity, and/or other data.

[00685] The ability for facilities to investigate incidents further and/or obtain guidance for remediation when exploits evade protection controls

[00686] The ability to collect and report on inventory, configuration and policy management of the endpoints.

[00687] The ability to manage and report on operating system security control status for the monitored endpoints.

[00688] The ability to scan systems for vulnerabilities and report/manage the installation of security patches.

[00689] The ability to report on internet, network and/or application activity to derive additional indications of potentially malicious activity.

[00690] Example embodiments are described in which policy enforcement, threat detection, or some other function is carried out by the systems described herein by detecting unusual activity, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a particular type of threat, intrusion, vulnerability, and so on. Although these examples are largely described in terms of identifying unusual activity, in these examples

the systems described herein may be configured to learn what constitutes 'normal activity' – where 'normal activity' is activity observed, modeled, or otherwise identified in the absence of a particular type of threat, intrusion, vulnerability, and so on. As such, detecting 'unusual activity' may alternatively be viewed as detecting a deviation from 'normal activity' such that 'unusual activity' does not need to be identified and sought out. Instead, deviations from 'normal activity' may be assumed to be 'unusual activity'.

[00691] Readers will appreciate that while specific examples of the functionality that the systems described herein can provide are included in the present disclosure, such examples are not to be interpreted as limitations as to the functionality that the systems described herein can provide. Other functionality may be provided by the systems described herein, all of which are within the scope of the present disclosure. For the purposes of illustration and not as a limitation, additional examples can include governance, risk, and compliance ('GRC'), threat detection and incident response, identity and access management, network and infrastructure security, data protection and privacy, identity and access management ('IAM'), and many others.

[00692] In order to provide the functionality described above, the systems described herein or the deployments that are monitored by such systems may implement a variety of techniques. For example, the systems described herein or the deployments that are monitored by such systems may tag data and logs to provide meaning or context, persistent monitoring techniques may be used to monitor a deployment at all times and in real time, custom alerts may be generated based on rules, tags, and/or known baselines from one or more polygraphs, and so on.

[00693] Although examples are described above where data may be collected from one or more agents, in some embodiments other methods and mechanisms for obtaining data may be utilized. For example, some embodiments may utilize agentless deployments where no agent (or similar mechanism) is deployed on one or more customer devices, deployed within a customer's cloud deployment, or deployed at another location that is external to the data platform. In such embodiments, the data platform may acquire data through one or more APIs such as the APIs that are available through various cloud services. For example, one or more APIs that enable a user to access data captured by Amazon CloudTrail may be utilized by the data platform to obtain data from a customer's cloud deployment without the use of an agent that is deployed on the customer's resources. In some embodiments, agents may be deployed as part of a data acquisition service or tool that does not utilize a customer's resources or environment. In some embodiments, agents (deployed on a customer's resources or elsewhere) and mechanisms in the data platform that can be used to obtain data from through one or more APIs such as the APIs that are available through various cloud services may be utilized. In some embodiments, one or more cloud services themselves may be configured to push data to some entity (deployed

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00431

anywhere), which may or may not be an agent. In some embodiments, other data acquisition techniques may be utilized, including combinations and variations of the techniques described above, each of which is within the scope of the present disclosure.

[00694] Readers will appreciate that while specific examples of the cloud deployments that may be monitored, analyzed, or otherwise observed by the systems described herein have been provided, such examples are not to be interpreted as limitations as to the types of deployments that may be monitored, analyzed, or otherwise observed by the systems described herein. Other deployments may be monitored, analyzed, or otherwise observed by the systems described herein, all of which are within the scope of the present disclosure. For the purposes of illustration and not as a limitation, additional examples can include multi-cloud deployments, on-premises environments, hybrid cloud environments, sovereign cloud environments, heterogeneous environments, DevOps environments, DevSecOps environments, GitOps environments, quantum computing environments, data fabrics, composable applications, composable networks, decentralized applications, and many others.

[00695] Readers will appreciate that while specific examples of the types of data that may be collected, transformed, stored, and/or analyzed by the systems described herein have been provided, such examples are not to be interpreted as limitations as to the types of data that may be collected, transformed, stored, and/or analyzed by the systems described herein. Other types of data can include, for example, data collected from different tools (e.g., DevOps tools, DevSecOps, GitOps tools), different forms of network data (e.g., routing data, network translation data, message payload data, Wi-Fi data, Bluetooth data, personal area networking data, payment device data, near field communication data, metadata describing interactions carried out over a network, and many others), data describing processes executing in a container, lambda, EC2 instance, virtual machine, or other execution environment), information describing the execution environment itself, and many other types of data.

[00696] For further explanation, Fig. 5A sets forth a system for providing many of the features described herein for user devices as a distributed edge service in accordance with some embodiments of the present disclosure. The system depicted in Fig. 5A includes a distributed edge platform 510. The distributed edge platform 510 may be similar to the systems described above where the distributed edge platform 510 can be used to perform tasks such as, for example, anomaly detection, threat detection, vulnerability detection, compliance monitoring, and many others. The distributed edge platform 510 may be deployed in a distributed fashion, such that instances of the distributed edge platform 510 are deployed on geographically distributed execution environments, as will be described in greater detail below.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00432

[00697] The distributed edge platform 510 depicted in Fig. 5A may be utilized to provide for continuous risk behavior based security to user devices. Such security is 'continuous' in the sense that data regarding the activity of a user device is continuously gathered and evaluated in real-time (or near real-time) rather than performing batch-based evaluation. Such security is 'behavior based' in the sense that various behaviors of the user device are used as the primary inputs into security evaluations. In many cases, such behaviors may not be concerning on their own, but instead may represent a deviation from typical device activity that warrants additional investigation. For example, if the user device is connecting to a cloud deployment, creating EC2 instances, and executing software on those EC2 instances, those steps alone may not be concerning. If this happens at hours when the user is known to be asleep and the user has never logged into the cloud deployment nor deployed software on EC2 instances in the cloud, however, this behavior may be deemed to be suspicious.

[00698] The example depicted in Fig. 5A includes a private environment 502 that is supporting a plurality of resources 504a-n. The private environment 502 may be embodied as a customer's datacenter, as a virtual private cloud for a particular customer, as co-located resources, or in some other way. The private environment 502 may include a collection of hardware resources, software resources, networking resources, and other resources so that the private environment 502 can be used to provide an organization or some other entity with an environment to execute their secure applications, store their secure data, and so on. In this example, the private environment 502 is 'private' in the sense that it is not available for public consumption. The private environment 502 depicted in Fig. 5A is supporting a plurality of resources 504a-n that may include, for example, software applications, databases, file systems, various services (e.g., whether local SaaS offerings), development tools (e.g., automation servers, code repositories, etc…), and so on.

[00699] The private environment 502 also includes a connector 506 that can be used to connect the private environment to the distributed edge platform 510 via a zero trust 508 authentication service. The connecter 506 may be embodied, for example, as one or more modules of computer program instructions executing on computer hardware, virtualized hardware, or in some other execution environment (including on resources in a dedicated networking components such as a router). The connector may be configured to act as a communications interface between the private environment 502 and the distributed edge platform 510. In such an example, access between the private environment 502 and the distributed edge platform 510 may involve the zero trust 508 authentication service, as any participants in data communications between the private environment 502, the distributed edge platform 510, and the user devices 512, 514, 522 that are monitored by the distributed edge platform 510 must be authenticated by the zero trust 508

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00433

authentication service. The zero trust 508 authentication service may be embodied, for example, as a third party authentication service such as Okta, or in some other way. In fact, readers will appreciate that the distributed edge platform 510 may be integrated with (and may leverage) a variety of third party tools such as identity and access management tools, Mobile device management ('MDM') tools, and so on.

[00700] In the example depicted in Fig. 5A, a user device 512 can access the resources 504a-n in the private environment 502 via the zero trust 508 authentication service. In such an example, because all access occurs through the zero trust 508 authentication service, the user device 512 need not connect to a VPN, go through a firewall, or use a similar mechanism in order to securely access the resources 504a-n in the private environment 502. In fact, the distributed edge platform 510 may implement policies that identify which users may access which resources 504a-n, what privileges each user has, and other policies so that the user device 512 is only routed to (and given access to) a particular resource 504a-n in the private environment 502 if the policies allow for such access. The distributed edge platform 510 can do all sorts of behavior analysis (i.e., analysis of device activity and user activity as described below) to add in anomaly detection capabilities, threat assessment, risk assessment, and other security related capabilities as described elsewhere in the present disclosure.

[00701] The example depicted in Fig. 5A also includes a SaaS environment 518 that is supporting a plurality of resources 520a-n. The SaaS environment 518 may be embodied, for example, as a public cloud that is accessible using a particular account, as an environment provided by the vendor of some SaaS offering, or in some other way. The SaaS environment 518 may include a collection of hardware resources, software resources, networking resources, and other resources so that the SaaS environment 518 can be used to provide a vendor of software that is consumed as-a-service to offer their SaaS products. The SaaS offerings can include any software offered as-a-service including, for example, Salesforce, Office365, and many others. In this example, the resources 520a-n that may include software applications, databases, file systems, or anything else offered as-a-service.

[00702] In the example depicted in Fig. 5A, a user device 514 can access the resources 520a-n in the SaaS environment 518 via a SaaS security 516 module. The SaaS security 516 module may be embodied, for example, as a login service or similar service that is implemented by a cloud computing environment or service vendor to control access to one or more SaaS offerings. In such a way, access to the SaaS environment 518 may only occur in accordance with the requirements put in place by the cloud computing environment, the service vendor, or similar entity that controls access to one or more SaaS offerings.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00434

[00703] The example depicted in Fig. 5A also includes a public internet 528 that is supporting a plurality of resources 526a-n. The public internet 528 may include a collection of hardware resources, software resources, networking resources, and other resources that can be used to offer resources 526a-n such as websites, social media platforms, and anything else publicly accessible via a web browser, mobile application, or other appropriate interface.

[00704] In the example depicted in Fig. 5A, a user device 522 can access the resources 526a-n in the public internet 528 via a network security 524 module. The network security 524 module may be embodied, for example, as one or more modules of computer program instructions that are configured to perform tasks such as SSL inspection, DNS inspection, and other tasks described in the present disclosure. In such an example, the network security module may be configured to protect the user device 522 from malware intrusions, computer viruses, or other threats that can originate from the public internet 528.

[00705] The distributed edge platform 510 may implement policies that identify which users may access which resources 520a-n, what privileges each user has, and other policies so that the user device 514 is only able to access various resources if the policies allow for such access. In fact, the distributed edge platform 510 can do all sorts of behavior analysis (i.e., analysis of device activity and user activity as described below) to add in anomaly detection capabilities, threat assessment, risk assessment, and other security related capabilities as described elsewhere in the present disclosure.

[00706] The distributed edge platform 510 depicted in Fig. 5A includes a real-time visibility and policy enforcement 530 module. The real-time visibility and policy enforcement 530 module may be embodied, for example, as one or more modules of computer program instructions executing on computer hardware, virtualized hardware, or in some other execution environment. The real-time visibility and policy enforcement 530 module may be configured to carry out many of the steps described above such as, for example, monitoring user activity (e.g., via data communications involving a user device or in some other way) to enforce various policies describing how the user devices may be utilized, what resources the user devices may access, what privileges the user device has, and so on. The real-time visibility and policy enforcement 530 module may also enable an administrator to have visibility into the activities associated with the monitored user devices. The real-time visibility and policy enforcement 530 module may be used to populate a monitoring interface used by the administrator, the real-time visibility and policy enforcement 530 module may enable the administrator to query the distributed edge platform 510 for information related to user activity or device activity, and so on.

[00707] The distributed edge platform 510 depicted in Fig. 5A also includes a user behavior anomaly detection 532 module. The user behavior anomaly detection 532 module may be

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00435

embodied, for example, as one or more modules of computer program instructions executing on computer hardware, virtualized hardware, or in some other execution environment. The user behavior anomaly detection 532 may be configured to analyze user behavior, user device activity, or other information to detect anomalous behavior as described in greater detail elsewhere in the present disclosure.

[00708] The distributed edge platform 510 depicted in Fig. 5A also includes an events, workflows, and auto management 534 module. The events, workflows, and auto management 534 module may be embodied, for example, as one or more modules of computer program instructions executing on computer hardware, virtualized hardware, or in some other execution environment. The events, workflows, and auto management 534 module may be configured to generate alerts, initiate a remediation workflow (or some other workflow), or perform other automatic remediation tasks as described in greater detail elsewhere in the present disclosure.

[00709] For further explanation, Fig. 5B sets forth a system for providing many of the features described herein for user devices as a distributed edge service in accordance with some embodiments of the present disclosure. The example depicted in Fig. 5B illustrates the distributed nature of the distributed edge service. The example depicted in Fig. 5B illustrates instances of the distributed edge platform 510a, 510b, 510c, 510d that are executing at distinct population centers 540a, 540b, 540c, 540d. Each of the population centers 540a, 540b, 540c, 540d may be embodied, for example, as a geographically distributed execution environment such as a distinct availability zone that is provided by a cloud services provider such as AWS, GCP, Azure, or others. In fact, the geographically distributed execution environments (represented here as population centers 540a, 540b, 540c, 540d) may even be provided by multiple cloud services providers (e.g., population center 540a is supported by AWS and population center 540b is supported by GCP).

[00710] Readers will appreciate that each instance of the distributed edge platform 510a, 510b, 510c, 510d may, in some embodiments, be deployed on a set of appliances that are deployed in various locations. Each appliance may include, for example, one or more servers or other computing devices, one or more networking devices, one or more storage devices, and so on. In such an example, each appliance may be configured to execute a particular instance of the distributed edge platform 510a, 510b, 510c, 510d.

[00711] In the example depicted in Fig. 5B, the instance of the distributed edge platform 510a, 510b, 510c, 510d that is accessed by a particular user device 512, 514, 522, 542 may be dependent upon the relative proximity between each population center 540a, 540b, 540c, 540d and each user device 512, 514, 522, 542. For example, each user device 512, 514, 522, 542 may connect to the instance of the distributed edge platform 510a, 510b, 510c, 510d that is supported

by the population center 540a, 540b, 540c, 540d that is most physically proximate to the user device 512, 514, 522, 542. The various instances of the distributed edge platform 510a, 510b, 510c, 510d may be updated in a coordinated fashion and may share access to the same information such that each instance operates in the same manner as any other instance, even if two instances are deployed in different ways (e.g., on different underlying resources).

[00712] For further explanation, Fig. 6 sets forth a flow chart illustrating an example method of detecting deviations from typical user behavior in accordance with some embodiments of the present disclosure. As will be described in greater detail below, detecting deviations from typical user behavior can be carried out with respect to end user devices. For example, detecting deviations from typical user behavior can include detecting typical user behavior as reflected by the manner in which a particular device (e.g., a laptop, a smartphone) is typically used and identifying situations in which the particular device is being used in a manner that deviates from the typical usage pattern. Although not expressly illustrated in Fig. 6, the methods described in Fig. 6 and elsewhere in the present disclosure may be carried out by one or more modules of computer program instructions executing on computer hardware, virtualized computer hardware, containers, or in some other execution environment.

[00713] The example method depicted in Fig. 6 includes identifying 602 a location of a device that is associated with a user. The device that is associated with a user may be embodied, for example, as a smartphone, as a tablet computer, as a laptop computer, or as some other device. The device may be associated with the user because the user is logged into the device, the device has been designated for use by the user (e.g., the device is a company issued laptop provided by the user's employer), or the device is otherwise associated with the user. The location of the device may be embodied, for example, as a city and state (e.g., Los Angeles, CA), as a label of a known location (e.g., 'home'), or designated in some other way.

[00714] Identifying 602 a location of a device that is associated with a user may be carried out in a variety of ways. In fact, identifying 602 a location of the device may be carried out using any of multiple mechanisms for determining a device's location and (in some embodiments) verifying that each mechanism yields the same outcome, or at least the same outcome within a predetermined threshold. For example, identifying 602 a location of the device may be carried out by identifying wireless networks or wireless access points that the device can connect to and determining the location of the available wireless networks or wireless access points. Once the locations of wireless networks or wireless access points that the device can connect to have been identified, other mechanisms may be used to verify the location of the device. For example, the source IP address of a data communications packet generated by the device may be used to determine the location of the device. In such an example, if the locations of wireless networks or

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00437

wireless access points that the device can connect to and the location of the source IP address of a data communications packet generated by the device match each other, the matching locations may be identified 602 as being the location of a device. The mechanisms for determining a device's location will be explained in greater detail below.

[00715] The example method depicted in Fig. 6 also includes determining 604 device activity associated with the user. The device activity associated with the user can include information describing the usage of the device. The device activity can include, for example, information describing applications that are being executed or utilized on the device, information describing how those applications are being utilized, information describing files being accessed via the device, information describing data sources being accessed via the device, information describing data communications coming into and flowing out of the device, and many others. In general, the device activity can be used to ascertain how a device is being used, when the device is being used, where the device is being used, or any other quantifiable aspect of device usage.

[00716] Determining 604 device activity associated with the user may be carried out, for example, by one or more data collection agents that are executing on the device, by one or more data collection agents that executing at some other location off of the device, or in some other way. That is, while some information describing device activity may come from the device (OS version, what apps are running locally, etc.), the information describing device activity may also come from outside the device. For example, other cloud services that report what users are doing may be leveraged (e.g., activity logs from Office 365 may be used, activity logs from Dropbox may be used). In such an example, even if no agents or other data collection programs were deployed on the device itself, information describing device activity may still be obtained. As such, determining 604 device activity associated with the user may be carried out by local agents executing on the monitored device itself, by agents executing elsewhere, or by combinations and variations thereof. The data collection agents (whether deployed on the user's device or elsewhere) may include, for example, one or more programs that can carry out a stream-based capture of network traffic in and out of the device (i.e., stream-oriented traffic processing), one or more programs that capture the usage of a device interface (e.g., a keystroke recorder, a recording program for capturing data acquired via a microphone), or other programs. In such a way, the agents may capture various aspects describing how the device is being used, when it is being used, by whom it is being used, where the device is located when being used, and so on.

[00717] The example method depicted in Fig. 6 also includes determining 606, based on a profile associated with the user, that the device activity associated with the user deviates from normal activity for the user. The profile associated with the user may include information describing normal activity for the user. The normal activity for the user may be determined, for example,

based on historical usage of the device (or some other device) associated with the user. That is, normal activity may be learned through an analysis of how the device has historically been used rather than being specified exclusively as a set of rules. The normal activity may include, for example, an identification of applications on the device that are accessed by the user, the times that those applications are accessed, the locations from which those applications are accessed, the order in which the applications on the device are typically accessed by the user, and so on. The particular mechanics of creating a user profile and learning what is normal activity for the device will be described in greater detail below.

[00718] In the example method depicted in Fig. 6, determining 606, based on a profile associated with the user, that the device activity associated with the user deviates from normal activity for the user may be carried out by comparing the device activity with the profile associated with the user. A comparison between the device activity and the profile associated with the user may reveal that device activity does not align with the profile associated with the user, which may be treated as a detection of abnormal activity.

[00719] Readers will appreciate that comparisons the device activity and the profile associated with the user may utilize ranges, thresholds, or similar concepts to allow for minor deviations between the device activity and the profile associated with the user. For example, if the profile associated with the user indicates that the device is typically located at the user's office between the hours of 9 AM and 5 PM on weekdays, but the device activity reveals that the user is still at the office at 6 PM on a particular Tuesday evening, this minor deviation may be tolerated and may not rise to the level of triggering an alarm. In contrast, if the device activity reveals that the user is at the office at 2:30 AM on a Sunday morning, this may be viewed as being a larger deviation. In this example, a threshold may be utilized such that the user deviating from their normal activity by 90 minutes (as a very simplified example used for ease of explanation) does not rise to the level of abnormal activity that would trigger an alarm or cause some other remediation workflow to be initiated. In other embodiments, other mechanisms may be used to allow for minor deviations between the device activity and the profile associated with the user, where such minor deviations do not result in determining 606 that the device activity associated with the user deviates from normal activity for the user.

[00720] For further explanation, Fig. 7 sets forth a flow chart illustrating an additional example method of detecting deviations from typical user behavior in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 7 is similar to the example method depicted in Fig. 6, as the example method depicted in Fig. 7 also includes identifying 602 a location of a device that is associated with a user, determining 604 device activity associated

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00439

with the user, and determining 606 that the device activity associated with the user deviates from normal activity for the user.

[00721] The example method depicted in Fig. 7 also includes generating 702 the profile associated with the user. Generating 702 the profile associated with the user may be carried out, for example, by utilizing data gathered by the agents described above as input to one or more machine learning algorithms. In such a way, patterns may be identified and correlations may be detected that represent the normal activity of the user. Such machine learning algorithms may detect, for example, that a particular application is normally only used at certain times and from certain locations. For example, the data gathered by the agents described above may reveal that a VPN client on the device is typically only used during traditional business hours (e.g., 8 AM – 6 PM) on weekdays and when the device is located at a location other than the user's office (as the private network may be directly accessible when the device is being used at the user's office). Readers will appreciate that in other embodiments, the profile associated with the user may be generated 702 in some other way. In such an example, the profile associated with the user may be expressed as a trained machine learning model that may be deployed to differentiate between normal activity and abnormal activity associated with a user (or a user device).

[00722] In the example method depicted in Fig. 7, determining 604 device activity associated with the user can include identifying 704 one or more applications being accessed on the device. Identifying 704 one or more applications being accessed on the device may be carried out, for example, by an agent that is executing on the device. For example, the agent may identify all running processes on the device and map (by the agent or by some other entity) the running processes to particular applications, the agent may identify all binaries that are loaded on the device and map (by the agent or by some other entity) the binaries to particular applications, the agent may query a device management application, or the agent may identify 704 one or more applications accessed by the device in some other way. In other embodiments, especially those in which the applications are SaaS offerings that are executed externally to the device (e.g., in a cloud environment), identifying 704 one or more applications being accessed on the device may be carried out in other ways such as, for example, by examining activity logs generated by the creator of the SaaS offering, by monitoring the device for calls to the application, through the use of an agent that monitors traffic in and out of the SaaS offering, or in some other way.

[00723] In the example method depicted in Fig. 7, determining 604 device activity associated with the user can also include identifying 706 application behavior for the one or more applications. Identifying 706 application behavior for the one or more applications can include, for example, identifying the data communications endpoints that the applications have communicated with, identifying data that has been accessed by the applications, identifying users

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00440

or accounts that have utilized the applications, identifying the time that the application was used, and so on. Such application behavior can include any quantifiable aspect describing how the application was used, when the application was used, by whom the application was used, and so on.

[00724] The example method depicted in Fig. 7 also includes, responsive to determining that the device activity associated with the user deviates from normal activity for the user, generating 708 an alert. The alert that is generated 708 may include contextual information including the specific actions (e.g., accessing a VPN client on a during non-business hours on a weekend from a previously unknown location) that caused the alert to be generated. In such an example, the alert may be issued to the user of the device, issued to a system administrator or similar entity that oversees a company's deployment, or issued elsewhere. In fact, the alert may be presented as part of a user-specific polygraph as will be described in greater detail herein.

[00725] For further explanation, Fig. 8 sets forth a flow chart illustrating an additional example method of detecting deviations from typical user behavior in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 8 is similar to the examples method depicted in Figures 6 and 7, as the example method depicted in Fig. 8 also includes identifying 602 a location of a device that is associated with a user, determining 604 device activity associated with the user, and determining 606 that the device activity associated with the user deviates from normal activity for the user.

[00726] The example method depicted in Fig. 8 also includes generating 802 a user-specific polygraph. The user-specific polygraph may be generated 802 in a manner that is similar to the manner in which polygraphs are created as described above. Although the user-specific polygraphs may be similar to the polygraphs described above, the user-specific polygraph may be distinct by virtue of each entity in the user-specific polygraph being specific to a particular user or user device. As one example of a user specific polygraph, Figures 15A and 15B include examples of a user-specific polygraph. As is depicted in greater detail below, the user-specific polygraph can include the geographic location of the device and the device activity associated with the user, among other possible entities. In some embodiments, the user-specific polygraph can also include one or more alerts, as described in greater detail below.

[00727] In the examples described herein, the device activity associated with the user may be continuously monitored for deviation from normal activity. The device activity may be continuously monitored for deviation from normal activity, for example, by determining whether device activity associated with the user deviates from normal activity for the user (as specified in a user profile) every time that a change to the device activity associated with the user occurs, as part of a process that is always executing on some computing resources, or in some other way. In

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00441

such a way, the systems described herein may be provide real-time or near real-time detection of a deviation from normal activity – rather than batch processing or other form of delayed processing of device activity to determine whether such activity deviates from normal activity.

[00728] In the examples described herein, the device activity associated with the user and the profile associated with the user include temporal information. The temporal information may be embodied, for example, as specific dates or times when some activity occurred or normally occurs, as relative times when some activity occurred or normally occurs, ranges of times when some activity occurred or normally occurs, as durations of time when some activity occurred or normally occurs, and so on. As such, the time at which some activity occurred may factor into an evaluation as to whether the activity represents normal activity.

[00729] For further explanation, Fig. 9 sets forth a flow chart illustrating an example method of establishing a location profile for a user device in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 9 includes gathering 902 information associated with the location of a user device. Gathering 902 information associated with the location of a user device may be carried out not only by gathering geolocation information, but also gathering information that may be useful in determining the nature of a particular location. For example, information may be gathered 902 to determine whether the location of the user device is a location where the user device is frequently utilized, information may be gathered 902 to determine whether the location of the user device is a location where utilizing the user device to perform certain functions is allowed or prohibited, and so on. As such, the information associated with the location of a user device may be gathered 902 not just for the purposes of determining where the device would be located on a map, but to use the location of the device as an input to determining whether a user or a user device is exhibiting anomalous behavior.

[00730] Readers will appreciate that many forms of information associated with the location of a user device may gathered 902 through a variety of mechanisms. Gathering 902 information associated with the location of a user device may be carried out, for example, using location-related capabilities of the user device such as a global positioning system (‘GPS’) receiver, an Assisted GPS (‘AGPS’) chip, and so on. In other embodiments, gathering 902 information associated with the location of a user device may be carried out using data communications related capabilities of the user device. For example, a Wi-Fi adapter in the user device may detect nearby networks and the Service Set Identifier (‘SSID’) associated with a detected network may be mapped to a geolocation through the use of tools such as Google Geolocation API. Likewise, examining data communications traffic sent by the user device and extracting the client IP address that is associated with the data communications traffic may be used in gathering 902 information associated with the location of the user device. In such an example, the client IP

address may be used to query one or more of a variety of services that convert IP addresses to geolocation information (e.g., a city/state, latitude and longitude, and so on). In fact, other embodiments could leverage image sensors or other capabilities of the user device to gather 902 information that may be informative for the purposes of identify a user device's location.

[00731] Readers will appreciate that because the information associated with the location of a user device may be gathered 902 for reasons that extend well beyond the context of a geolocation, the information associated with the location of a user device may be information that is more useful in describing the nature of a location rather than an absolute physical location. For example, the particular set of device types that the user device can communicate with may be indicative of a location. Consider an example in which the user device can detect the presence of a thermostat, a smart refrigerator, multiple smart TVs, a router, and the entertainment system of an automobile via its Wi-Fi adapter or Bluetooth adapter. In such an example, this combination of reachable device types may be taken as an indication that the user device is at a private residence. In an example where the user device can only detect the presence of other personal communications devices and also detect the presence of a wireless network that includes a phrase such as "free," "public," or "starbucks" in its network name, this combination of reachable devices may be taken as an indication that the user device is at a public location (perhaps a coffee shop). In these examples, rather than attempting to determine a geolocation, information may be gathered 902 that can be used to determine a relative location, a type of location, characteristics of a location, or some other information that may be associated with a particular location.

[00732] The example method depicted in Fig. 9 also includes determining 904, based on the information associated with the location of a user device, whether the user device is being accessed at a known location. A 'known' location, as the term is used here, can refer to a location that is associated with an expected profile of device utilization based on previously observing how the user device (or some other device such as a similar device, a device that is associated with similar users, and so on) is utilized at the 'known' location. For example, a user device may be expected to be used in one way when the user device is located at the user's home, the user device may be expected to be used in another way when the user device is located at the user's office, the user device may be expected to be used in yet another way when the user device is located in the user's automobile, and so on. As such, in some embodiments a location may only be determined 904 to be a 'known location' if the location has an associated set of user behaviors that would be expected to be observed when the user device is located at the 'known location'.

[00733] Readers will appreciate that a location is not necessarily 'known' in the sense that the device's geolocation is known, although in some embodiments a known location may include a specific geolocation (e.g., 123 Avenue A, San Francisco, CA). For example, while it may not be

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00443

possible to determine the mailing address or street address where the user device is located, the detected presence of a particular set of other devices may be sufficient to determine that the user device is at a 'home' location, even if the exact street address of the home cannot be determined. Likewise, detecting that the user device is located at a particular set of GPS coordinates may be insufficient for determining that the location of the user device is 'known' if the set of GPS coordinates has no known relationship to a location where the user device has previously been used or is otherwise associated with a set of behaviors that would be expected to be observed when the user device is at the GPS coordinates. In fact, in some embodiments, the location of the user device may only be determined to be a 'known' location if the user device has previously been accessed at the location or at some other location where utilization of the user device would be expected to be similar. For example, if the location of the user device is at a hotel, this location may be determined to be a 'known' location by virtue of the fact that the user device has been used in the past at other hotels (even if the user device has not been previously used at the exact hotel that it is now located at).

[00734] The example method depicted in Fig. 9 also includes, responsive to affirmatively 906 determining that the user device is being accessed at a known location, determining 908 a characterization of the known location. A 'characterization' of the known location may be embodied as description of the location that can be associated with some set of behaviors that would be expected from the user device or the user by virtue of the user device being located at a location that is characterized in a certain way. Consider an example in which the characterization is a 'home' location. In this example, a set of expected behaviors may be associated with the user or the user device by virtue of the user device being at home. For example, it may be expected that the user device accesses streaming media services (e.g., Netflix) while the user device is at home, it may be expected that the user device accesses the public internet while the user device is at home, and so on. Alternatively, consider an example in which the characterization is a 'work' location. In this example, a set of expected behaviors may be associated with the user or the user device by virtue of the user device being at home. For example, it may be expected that the user device accesses their employer's internal bill payment systems, it may be expected that the user device accesses their employer's code repository and internal networks while at work, and so on.

[00735] In the example depicted in Figure 9, various 'characterizations' of locations may be generated through the use of one or more machine learning models. Machine learning models may be used, for example, to detect clusters (e.g., clusters of devices that can be reached via relatively short distance communications adapters in the devices) that can be identified as being at least a logical location. Such machine learning models may take data gathered by one or more devices to identify clusters that correspond to some location. For example, if information is

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00444

gathered indicating that a collection of user devices are located in a relatively small area and that a large percentage of those devices are connected to an internal corporate network for company ABC, the machine learning models may learn that the locations each device (and possibly some corresponding area surrounding each device) can be characterized as being an office for company ABC. Readers will appreciate that other 'characterizations' may be generated using a variety of information, machine learning techniques, other labelling techniques, or generated in some other way (e.g., by asking the user of the device or some administrator of the device to characterize their current location through some interface).

[00736] Determining 908 a characterization of the known location may be carried, for example, through the use of a table, database, or some other data structure/repository that associates known locations with characterizations of each known location. Such a repository can be constructed over time by monitoring the behavior of the user device and other devices. As part of a process of generating characterizations of various locations, the activity of the user device (and other devices) may also be monitored to learn what behavior constitutes 'normal' behavior for the user or user device in various locations, using techniques such as those described herein.

[00737] The example method depicted in Fig. 9 also includes determining 910, based on the characterization of the known location, whether device utilization is anomalous. Determining 910 whether device utilization is anomalous may be carried out as described above, generally by determining the extent to which device activity is consistent with normal activity that would be expected to be observed when the user device is at a known location that is characterized in a particular way. Readers will appreciate that a determination so to whether device utilization is anomalous may only be based in part on the characterization of the location, as other information may also be taken into consideration (e.g., information from other devices, specific details around how the device is being used, policies that restrict how a device should be utilized at certain locations, etc…).

[00738] The example method depicted in Fig. 9 also includes, responsive to determining that the user device is not 912 being accessed at a known location, determining 914 a characterization of the unknown location. Determining 914 a characterization of the unknown location may be carried out, for example, by performing some workflow to attempt to determine whether the unknown location is similar to a known characterization. For example, one characterization for various locations may be an 'in transit to work' (or something similar) characterization that is generally associated with locations between a user's home location and a user's work location, so long as there is some indication that the user device is moving at an appropriate rate from the user's home location and the user's work location. In such an example, if the workflow determines that the user device was located at the user's home 10 minutes ago, a route between

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00445

the user's home and the user's office takes 20 minutes to traverse, and the user device is currently located near a midpoint of that route, the unknown location may be characterized as being 'in transit to work' or something similar. Likewise, an unknown location may be characterized in accordance with various environmental attributes detected by the user device. For example, if the user device is at an unknown public location with no Wi-Fi networks that the user device is configured to access but the user device can access a cellular network, the unknown location may be consistent with a known characterization of a device being at a 'public location without secure Wi-Fi access,' such that the user device can be characterized as being at a 'public location without secure Wi-Fi access.'

[00739] In these examples, readers will appreciate that a library or catalog of known characterizations may be created by observing many devices over time. In fact, each entry (i.e., each known characterization of a location) in the catalog may associated with location information that tends to be associated with a particular characterization. For example, devices may be monitored to determine that when a device is placed in a silent mode between the hours of 8 AM – 1 PM on a Sunday, and a touch screen display for the device is not being interacted with by the user, and a microphone in the device detects periods of singing, the device is at a location that is characterized as a 'religious services' location. As such, information that was gathered 902 and is associated with an unknown location may be compared to signatures for the entries in the catalog of characterizations to determine whether the unknown location should be characterized using one of the entries in the catalog.

[00740] Readers will appreciate that the characterization of an unknown location may be associated with a set of expected device behaviors. For example, when a user device is characterized as being 'in transit to work', it may be expected that utilization of the user device may be extremely limited as the user may be operating a vehicle. Likewise, when a user device is characterized as being at a 'public location without secure Wi-Fi access', it may be expected that the user device will not be used to access sensitive financial data or initiate substantial monetary transactions on behalf of the user's employer.

[00741] The example method depicted in Fig. 9 also includes determining 916, based on the characterization of the unknown location, whether device utilization is anomalous. Determining 916 whether device utilization is anomalous may be carried out described above, generally by determining the extent to which device activity is consistent with normal activity that would be expected to occur when the user device is at an unknown location that is characterized in a particular way. Readers will appreciate that a determination so to whether device utilization is anomalous may only be based in part on the characterization of the location, as other information may also be taken into consideration (e.g., information from other devices, specific details

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00446

around how the device is being used, policies that restrict how a device should be utilized at certain locations, etc…).

[00742] For further explanation, Fig. 10 sets forth a flow chart illustrating an additional example method of establishing a location profile for a user device in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 10 is similar to the example method depicted in Fig. 9, as the example depicted in Fig. 10 also includes gathering 902 information associated with the location of a user device, determining 904 whether the user device is being accessed at a known location, determining 908 a characterization of a location, and determining 910 whether device utilization is anomalous.

[00743] In the example method depicted in Fig. 10, determining 904 whether the user device is being accessed at a known location can include determining 1002 whether the information associated with the location of a user device matches, at least within a predetermined threshold, location information associated with one or more location profiles. A location profile may be embodied, for example, as a data structure that associates one or more known locations with information associated with the known locations. The information that is associated with the known locations can include, for example, one or more device behaviors that are typically encountered when a device is at the known location, a geographic boundary that defines the known location, one or more characterizations of the known location, temporal aspects of device and user behavior that are typically observed at the known location, and so on. As such, the location profile may be used to correlate such information with a known location, so that the location profile can be used to determine whether a particular device is at the known location.

[00744] In the example method depicted in Fig. 10, the one or more location profiles may be created based on activity associated with the user device. For example, a location profile that is associated with the user device being at a hotel, on an airplane, at a coffee shop, at home, at work, or at some other location may be based on monitored or observed device activity or user activity associated with the user device itself. Alternatively, the one or more location profiles may be created based on activity associated with other devices. Such other devices may be embodied as, for example, similar devices for users that are part of the same organization (e.g., the same company, the same department within a company), devices for users that are determined to perform similar roles (e.g., engineers, accountants, legal team members) within an organization, and so on. In such a way, a particular user device may be monitored with the benefit of knowledge gleaned from monitoring other devices, which may be particularly useful when a particular user device is new and does not have a long history of monitored behavior.

[00745] In some embodiments, determining 910, 914 whether device utilization is anomalous may be further based on a temporal profile of device activity. The temporal profile of device

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00447

activity may include, for example, information describing days and times that particular applications are used on the user device, information describing days and times that the user device is typically being accessed or not being accessed, information describing the relative timing of different user or device activities (e.g., updated code is committed from the user's device to a code repository after text editing software or some other software used to write code has been utilized), or any other information that associates user behavior or device behavior with times at which such behavior is common, permitted, prohibited, and so on. The temporal profile may be embodied as a database, table, or some other data structure. In such embodiments, the relationship between times and device or user activities may be identified through the usage of one or more machine learning models that take activities (and the times associated with the activities) as inputs to the machine learning models.

[00746] For further explanation, Fig. 11 sets forth a flow chart illustrating an additional example method of establishing a location profile for a user device in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 11 is similar to the example methods depicted in Fig. 9 and Fig. 10, as the example depicted in Fig. 11 also includes gathering 902 information associated with the location of a user device, determining 904 whether the user device is being accessed at a known location, determining 908 a characterization of a location, and determining 910 whether device utilization is anomalous based on the characterization of the known location. The example method depicted in Fig. 11 also includes creating 1102 a polygraph associated with the user device. Creating 1102 a polygraph associated with the user device may be carried out as described elsewhere in the present disclosure. Examples of such device-specific polygraphs are included herein.

[00747] In the example depicted in Fig. 11, determining 904 whether the user device is being accessed at a known location can include determining 1104, based on one or more devices that are physically proximate to the user device, a location of the user device. Readers will appreciate that the exact distance between the user device and the one or more other devices (e.g., one or more routers that emit a Wi-Fi signal) may not be needed in order to determine 1104 a location of the user device. The term 'physically proximate' that is used here can be a threshold value that may even be a function of the particular wireless communications protocol that is being used. For example, if the user device can detect the presence of another device using a Bluetooth adapter, the user device may be assumed to be within 20 feet of the other device. If the user device can detect the presence of another device using a Wi-Fi adapter, however, the user device may be assumed to be within 100 feet of the other device. Readers will appreciate that these distance and technologies are included only as examples.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00448

[00748] Consider an example in which a user device is embodied as a laptop computer and the laptop computer can detect the presence of five distinct networks using its Wi-Fi adapter. In such an example, upon detecting the presence of each network, resources may be accessed that associate the access ID of the network with a physical location associated with the network. For example, Google maintains a database that can be accessed via various APIs to determine the latitude and longitude associated with a wireless network's access ID. In some examples, this database may be queried with the access ID of the detected network to receive latitude and longitude information associated with the network. Readers will appreciate that, over time, the results obtained from querying such a database may be cached such and reused. For example, if location information for each of the five distinct networks is obtained and the same user turns on a smartphone that detects the same five networks, the cached results of the previously executed queries may be utilized to determine the first geolocation of the smartphone. Cached results may similarly be used for other users whose devices detect the same networks.

[00749] In the example depicted in Fig. 11, determining 904 whether the user device is being accessed at a known location can include determining 1106, based on data communications involving the user device, a location of the user device. Determining 1106 a location of the user device based on data communications involving the user device may be carried out, for example, by examining data communications traffic sent by the device and extracting the client IP address that is associated with the data communications traffic. The client IP address may be used, for example, to query one or more of a variety of services that convert IP addresses to location information (e.g., a city/state, latitude and longitude, and so on). In an alternative embodiment, the IP address of the user device may be identified in other ways other than inspecting network traffic (e.g., through the use of CLI commands such as ipconfig).

[00750] Readers will appreciate that the location of a user device may be misidentified, for example, if the user device is connected to a virtual private network or if the user device is being operated in some other way where its IP address (or other data communications attribute) would not be an accurate representation of the device's location. As such, in some embodiments multiple pieces of information that are associated with a location can be used rather than relying exclusively on a single piece of information when determining a user device's location.

[00751] In some embodiments, a location cache may be maintained. As described above, as part of the process of determining a location of the user device, external resources may be accessed. For example, resources such as those maintained by Google may be accessed that associate the access ID of a network with a physical location associated with the network. Such resources, however, may not be free to access, may be timely to access, the resource may return location information in a less than ideal format (e.g., the resource return latitude and longitude

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00449

information when the desired format of the location is a zip code), or may be undesirable to access for other reasons. As such, the results obtained from querying such resources may be cached and reused in a local location cache.

[00752] Such a location cache may be a data repository such as a database, a file, a table, or embodied in some other way. In some embodiments, the location cache may be 'local' in the sense that it is stored on the user device itself or stored in some location that does not suffer from the same undesirable characteristics as the original resource. Continuing with the example where a Google database may be accessed (for a monetary charge) that associate the access ID of a network with a physical location associated with the network, after that initial access the location information associated with the access ID of the network may be maintained in a database that the user device can access free of charge. Readers will appreciate that in these examples, the content contained in the local location cache may be stored in the format desired by the user device (e.g., stored as city/state information rather than GPS coordinates).

[00753] Readers will appreciate that some embodiments may include a different combination of the steps described above, including variations of such steps. For example, some embodiments of establishing a location profile for a user device may include gathering information associated with a location of a user device, determining a characterization of the location, and determining, based on a characterization of the known location, whether device utilization is anomalous such that the step of determining whether a location is known is optional.

[00754] For further explanation, Fig. 12 sets forth a flow chart illustrating an example method of detecting deviation from normal behavior of a user device in accordance with some embodiments of the present disclosure.

[00755] The example method depicted in Fig. 12 includes generating 1202, using information describing historical activity associated with a user device, a trained model for detecting normal activity for the user device. The trained model may be embodied, for example, as a model artifact that is created by a training process in which machine learning algorithms are provided with training data to learn from. The trained model, once deployed, can make predictions, identify patterns, and perform other functions on new data (i.e., data that was not part of the training data). Generating 1202 a trained model for detecting normal activity for the user device using information describing historical activity associated with a user device may therefore be carried out, for example, by applying one or more machine learning algorithms to a training dataset that includes the information describing the historical activity associated with the user device. The information describing the historical activity associated with the user device can include, for example, information describing the locations at which the user device was utilized at some point in the past, information describing the applications on the user device that were executed at some

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00450

point in the past, information describing the dates and times the applications on the user device that were executed, and so on. In such an example, activity associated with the user device may be deemed to be 'historical' if the activity occurred at some point before training occurred.

[00756] Consider an example in which training occurred at time t_0. In such an example, any activity associated with the user device that occurred prior to time t_0 would be 'historical' activity associated with the user device. Further assume that additional training occurred at time t_1, which is later than time t_0. In this example, activity associated with the user device that occurred prior to time t_1 would be 'historical' activity associated with the user device, at least with respect to the additional training (whereas activity that occurred between time t_0 and time t_1 would not be 'historical' activity with respect to the original training that occurred at time t_0).

[00757] The example method depicted in Fig. 12 also includes gathering 1204 information describing current activity associated with the user device. The information current activity associated with the user device may be embodied, for example, as information describing activity associated with the user device that was gathered 1204 at a point in time such that it was not available for inclusion in the set of training data that was used to generate (or further refine via additional training) the trained model. The information describing current activity of the user device may include the types of information described above (e.g., location of the user device, applications executed by the user device, and much more). The information describing the current activity of the user device may be gathered 1204, for example, by the agents described above including agents that are executing on the user device itself.

[00758] The example method depicted in Fig. 12 also includes determining 1206, by using the information describing current activity associated with the user device as input to the trained model, whether the user device has deviated from normal activity. Determining 1206 whether the user device has deviated from normal activity by using the information describing current activity associated with the user device as input to the trained model may be carried out, for example, by executing the trained model on the user device and coupling the trained model to a data stream, data repository, or other source for the information describing current activity associated with the user device. In such an example, such information may describe 'current' activity in the sense that the information represents activity that has occurred in some recent period of time (e.g., the last minute, the last second), activity that is being monitored in real-time, activity that has occurred since the model was most recently trained, or activity that is 'current' as determined by some other rule or heuristic.

[00759] For further explanation, Fig. 13 sets forth a flow chart illustrating an example method of sets forth a flow chart illustrating an example method of detecting deviation from normal behavior of a user device in accordance with some embodiments of the present disclosure. The

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00451

example method depicted in Fig. 13 is similar to the example method depicted in Fig. 12, as Fig. 13 also includes generating 1202 a trained model for detecting normal activity for the user device, gathering 1204 information describing current activity associated with the user device, and determining 1206 whether the user device has deviated from normal activity.

[00760] In the example method depicted in Fig. 13, generating 1202 a trained model for detecting normal activity for the user device can include generating 1302 the trained model using information describing physical locations at which the user device was utilized. As described above, the physical locations at which the user device was utilized may be determined from a combination of sources (e.g., the location of physically proximate devices, data communications characteristics of the user device, user input, location-detecting devices that are embedded within the user device). Such locations at which the user device was utilized may be included in a training dataset that is used to generate the trained model. In fact, the trained model may ultimately identify density clusters such that locations that are not identical matches are determined to be the same location. For example, a cluster of locations at which the user device was utilized may be identified as locations within the user's office complex, such that the user being on the northeast side of the office building and the user being on the southwest side of the office building are not treated as distinct locations, but are instead treated as the user being within the same density area that represents a single logical location. Likewise, a cluster of locations that represent a commonly traversed path may be treated as a single entity. For example, the trained model may learn a user's daily route to work and may treat all of the individual locations along that route as a single entity. In some embodiments, particular locations may be labelled (e.g., home, office, etc…) as part of the training process or after the model has been trained.

[00761] In the example method depicted in Fig. 13, generating 1202 a trained model for detecting normal activity for the user device can include generating 1304 the trained model using information describing usage of one or more applications executed on the user device. The information describing usage of one or more applications executed on the user device may include, for example, information describing when the applications were used, information describing what features of the applications were used, information describing what external data sources were accessed when the applications were being used, information describing what data communications occurred when the applications were being used, and so on. Such information may be included in a training dataset that is used to generate the trained model. In fact, training the model using the training datasets may reveal relationships between different applications, patterns related to how the user utilizes the applications, actions that trigger the usage of the application (e.g., the user typically accesses an email application after receiving a notification),

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00452

and many other patterns that represent normal activity. As such, the trained model may be configured to identify deviations from normal activity.

[00762] In the example method depicted in Fig. 13, generating 1202 a trained model for detecting normal activity for the user device can include generating 1306 the trained model using information describing times at which activity previously occurred. The information describing times at which activity previously occurred may be embodied, for example, as absolute values (e.g., at 12:36 PM on a specific date), as relative values (e.g., after using application X, within 30 minutes after turning on the user device), as a value that is expressed in its relationship to some other activity or detected condition (e.g., while the user was in transit to work, while the user was at work), or in some other way. Such information may be included in a training dataset that is used to generate the trained model. In fact, training the model using the training datasets may reveal temporal relationships between different activities, patterns related to an ordering of a set of activities or detected conditions, and many other patterns that represent normal activity. As such, the trained model may be configured to identify deviations from normal activity.

[00763] Readers will appreciate that while the embodiments described above are largely described as individual types of information (e.g., location information, temporal information, device usage information) that may be used to generate 1202 a trained model for detecting normal activity for the user device, readers will appreciate that the process of generating 1202 a trained model for detecting normal activity for the user device may actually include one or more machine learning algorithms ingesting combinations of these types of information. In fact, other types of information may also be used in the process of generating 1202 a trained model for detecting normal activity for the user device. Readers will appreciate that any information that can be captured by an agent that is executing on the user device, including combinations thereof, can be used when generating 1202 a trained model for detecting normal activity for the user device.

[00764] In the example method depicted in Fig. 13, gathering 1204 information describing current activity associated with the user device can include gathering 1308 information describing a physical location at which the user device is currently being used. The information describing a physical location at which the user device is currently being used may be gathered 1308, for example, by one or more agents that are executing on the user device, by one or more agents that are executing on other devices (e.g., on a device that communicates with the user device over a local network). Such information may include, for example, information that itself does not represent a location of the user device but which may be used to determine the location of the user device as described above. Such information may include information describing other devices or network that are detected by the user device, information describing data

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00453

communications characteristics of the device, and so on. In other embodiments, the information itself may represent a location of the user device. For example, such information may include global positioning system ('GPS') coordinates obtained from a GPS receiver in the user device.

[00765] In the example method depicted in Fig. 13, gathering 1204 information describing current activity associated with the user device can include gathering 1310 information describing usage of applications that are being accessed by the user device. The information describing usage of applications that are being accessed by the user device may be gathered 1310, for example, by one or more agents that are executing on the user device, by one or more agents that are executing on a device/service that executes the application, or in other ways described above. Such information may include, for example, information describing which applications are being executed, information describing what data communications networks are being accessed when executing an application, information describing particular features of the application that are being utilized, and many others.

[00766] In the example method depicted in Fig. 13, gathering 1204 information describing current activity associated with the user device can include gathering 1312 information describing times at which current activity occurred on the device. The information describing times at which current activity occurred on the device may be gathered 1312, for example, by one or more agents that are executing on the user device, by one or more agents that are executing elsewhere, by inspecting activity logs, or in some other way. Such information may include, for example, information describing the exact time that some activity occurred, a range of times during which the activity occurred, a relative time during which the activity occurred, and so on.

[00767] For further explanation, Fig. 14 sets forth a flow chart illustrating an example method of sets forth a flow chart illustrating an example method of detecting deviation from normal behavior of a user device in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 14 is similar to the example method depicted in Figs. 12 and 13, as Fig. 14 also includes generating 1202 a trained model for detecting normal activity for the user device, gathering 1204 information describing current activity associated with the user device, and determining 1206 whether the user device has deviated from normal activity.

[00768] The example method depicted in Fig. 14 also includes periodically 1402 retraining the trained model. Periodically 1402 retraining the trained model may be carried out, for example, by including recently acquired data describing various aspects of the user device's operation and usage into a training data that is used to train the model. Such data may be 'recently acquired' in the sense that it was not included in training data that was previously used to train the model. The recently acquired data may be used either alone or in combination with training data that was previously used to train the model as part of a process to retraining the trained model, at which

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00454

point the retrained model may be deployed on the user device. Readers will appreciate that retraining the trained model periodically such as, for example, according to a predetermined schedule, upon the satisfaction of some condition (e.g., a threshold amount of new data has been acquired, sufficient resources to carry out the retraining have become available, alerts are being generated at a threshold level indicating that perhaps the trained model does not sufficiently understand normal behavior), upon request from a user or administrator, or in some other way. Through such periodically 1402 retraining the trained model, the trained model may be an evolving entity that can differentiate between normal and abnormal activity even as a user's interactions with the device or usage of the device change over time.

[00769] The example method depicted in Fig. 14 also includes generating 1404 an alert after determining that the user device has deviated from normal activity. The alert may be generated 1404 and expressed through one or more of the polygraphs described above. In other embodiments, alerts may be delivered in some other way (e.g., as a notification that is sent to some predetermined recipient using some predetermined delivery mechanism).

[00770] The example method depicted in Fig. 14 also includes initiating 1406 a remediation workflow after determining that the user device has deviated from normal activity. Initiating 1406 a remediation workflow may be carried out as part of an auto-remediation capability that may be provided to the monitored devices. The remediation workflow may be configured to perform a variety of tasks including, for example, restricting the access of the user device to certain data, restricting the usage of certain applications on the user device, enabling some feature on the user device (e.g., communications over an unsecured network is detected so a data encryption feature for data communications is enabled), or performing some other function. In some embodiments, the remediation workflow may be designed to either prevent the abnormal activity from occurring or even enabling the abnormal activity upon the satisfaction of some condition (e.g., an administrator approves the activity, the user authenticates their identity).

[00771] For further explanation, Fig. 15A sets forth an example of a user-specific polygraph 1500 in accordance with some embodiments of the present disclosure. The user-specific polygraph 1500 depicted in Fig. 15A may be generated in a similar manner as the polygraphs described above and may have similar features and capabilities. The user-specific polygraph 1500 depicted in Fig. 15A includes a representation of a user and information describing the user, in this case designated as User ABC 1502. The representation of the user may include, for example, a user's name, a user's handle, or any other information associated with the user. Such information associated with the user may be visible in the original presentation of the polygraph or may be accessible in other ways (e.g., hovering a mouse over the user icon).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00455

[00772] The user-specific polygraph 1500 depicted in Fig. 15A also includes information describing the location of the user (as represented by the location of the device that is being used by the user), depicted here as San Francisco, CA 1504. The location may be obtained as described in greater detail above. The representation of the location of the user may include, for example, an identification of a city, geographical coordinates, an identification of a known location (e.g., home, office), or any other location information associated with the user. Such location information associated with the user may be visible in the original presentation of the polygraph or may be accessible in other ways (e.g., hovering a mouse over the user icon).

[00773] The user-specific polygraph 1500 depicted in Fig. 15A also includes information describing the user device, depicted here as user device MRD1 1506. The information describing the user device may include, for example, a device name, a label for the device (e.g., phone, laptop, work laptop) or any other information describing the device. Such device information may be visible in the original presentation of the polygraph or may be accessible in other ways (e.g., hovering a mouse over the user icon).

[00774] The user-specific polygraph 1500 depicted in Fig. 15A also includes information describing applications accessed by the device, depicted here as internal sales application 1508, web browser application 1510, ad messaging application 1512. Information describing the applications that are accessed by the user device may be obtained as described in greater detail above. The representation of the applications may include, for example, a name of the application, a name of the binary, a custom label for the application, or any other information associated with the application including information describing the usage of the application. Such application-related information may be visible in the original presentation of the polygraph or may be accessible in other ways (e.g., hovering a mouse over the user icon).

[00775] The user-specific polygraph 1500 depicted in Fig. 15A also includes information describing specific details regarding how a particular application is being used. For example, the internal sales application 1508 is depicted as connecting to an internal sales database 1514. Information associated with the internal sales database (e.g., where the database is hosted, what credentials were used to access the database, how many queries have been directed to the database) may also be depicted or may be accessible in other ways (e.g., hovering a mouse over the user icon). Likewise, the web browser application 1510 is depicted as being connected to different endpoints, which may be carried out through the usage of different tabs or different instances of the web browser application 1510. For example, the web browser application 1510 is depicted as accessing a social media 1514 site, a productivity 1518 site (e.g., Salesforce, a web-based repository), a bandwidth intensive 1520 site such as a streaming video site, and a site that requires private information 1522 such as a banking site. In some embodiments, additional

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00456

information associated with each endpoint 1516, 1518, 1520, 1522 may be displayed or may be accessible in other ways (e.g., hovering a mouse over the user icon). In fact, the links between different icons in polygraph may also be enriched with data. For example, the links between the web browser application 1510 and the endpoints 1516, 1518, 1520, 1522 may include information describing how long the connection has been established, how much data has been transferred since the connection was established, and so on. In other embodiments, other data associated with the links between two icons may also be enriched with data that may be visible in the default view of the polygraph or accessible in some other way as described above.

[00776] For further explanation, Fig. 15B sets forth an example of a user-specific polygraph 1500 in accordance with some embodiments of the present disclosure. The example depicted in Fig. 15B illustrates an embodiment in which an alert 1526 is presented in the polygraph 1500. In this particular example, the alert 1526 is generated for a messaging application 1512 that is connected to an unknown network 1524. As illustrated in the alert 1526, a malicious IP address has been identified in the unknown network 1524. Although not illustrated in this example, the alert 1526 may be coupled with functionality that is accessible in the displayed 1526 alert, which such functionality can include ignoring the alert, terminating the application, initiating a remediation workflow, or taking some other action.

[00777] Readers will appreciate that the polygraph 1500 depicted in Fig. 15A and 15B is just one example of a user-specific polygraph that may be generated and utilized as described above. In other embodiments, less or additional information may be included in the polygraph 1500, different information may be included in the polygraph 1500, different actions may be initiated via the polygraph 1500, or the polygraph 1500 may otherwise differ from the depicted examples.

[00778] For further explanation, Fig. 16 sets forth an example method for using activity monitored by multiple data sources to identify shadow systems according to some embodiments of the present disclosure. The method of Fig. 16 may be performed, for example, in a distributed edge platform as described above, or another computing environment or execution environment as can be appreciated.

[00779] The method of Fig. 16 includes gathering 1602 first information describing access to one or more resources by one or more user devices of a user. The one or more user devices are associated with the user via a variety of approaches. For example, the one or more user devices may include one or more known user devices registered or having a profile that associates the user device with the user. As another example, the one or more user devices may be logged into a distributed edge platform or other service provider using authentication credentials for the user. As a further example, the one or more user devices may have accessed an identity provider using

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00457

authentication credentials for the user. The one or more user devices may be associated with a particular user by other approaches as can be appreciated.

[00780] The one or more resources accessed by the one or more user devices are remotely disposed resources accessible via a network. For example, the one or more resources may include one or more applications (e.g., software as a service (SaaS) applications from third party service providers deployed or managed by an organization including or overseeing the user), one or more private applications (e.g., applications deployed in a data center or other private computing environment controlled by an organization including or overseeing the user), one or more documents, one or more websites, and potentially other network-accessible resources as can be appreciated.

[00781] The first information is gathered 1602 from one or more data sources other than the one or more user devices. In some embodiments, the first information is gathered 1602 from the one or more resources or one or more providers of the one or more resources. In some embodiments, the first information may include log entries describing access to the particular resources. For example, the first information may include logs generated by the applications themselves or application service providers, by hosting services for particular webpages, by storage systems storing access documents or files, and the like. The first information may be gathered 1602 via exposed application program interfaces (APIs), by accessing one or more accessible files encoding the first information, and the like.

[00782] The first information may describe previous or historical access to the resources by particular users, by particular user devices, and the like. For example, the first information may describe an access to a resource and indicate particular authentication credentials, usernames, accounts, and the like used to access that resource. As another example, the first information may describe access to a resource and indicate device attributes for a device accessing the resource, including an internet protocol (IP) address, network interface address (e.g., a MAC address), a device identifier, and the like. As a further example, the first information may describe attributes of a network request or network address used to access a resource, including source and destination IP addresses, source and destination ports, particular protocols used to facilitate the request, descriptions of encryption protocols used to facilitate the request, certificates or keys used to facilitate the request, and the like. The first information may also include identifiers for particular accessed resources, including particular applications being accessed, particular websites, documents, or files being accessed, and the like. The first information may also indicate a particular type of transaction or access being performed via the request (e.g., a read access or a write access).

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00458

[00783] In some embodiments, the first information is gathered 1602 from an identity provider used to access the one or more resources. An identity provider allows access to multiple resources using a shared set of authentication credentials. For example, a user of a particular organization may log into the identity provider in order to access a variety of applications deployed or managed by the organization, rather than require the user to individually log into each of multiple applications. Accordingly, the identity provider may maintain logs describing particular

[00784] Accordingly, in some embodiments, the first information may describe uses of the identity provider by a particular user (e.g., using a particular set of authentication credentials). For example, the first information may include various attributes identifying a particular user device used to access the identity provider, including an IP address, network interface address, location information, or other information describing a device used to access the identity provider. The first information may also include times at which access to the identity provider was requested. The first information may also describe failed attempts to access the identity provider, including incorrect authentication credentials, device identifiers, and the like. Thus, portions of the first information describing a failed access to the identity provider may be associated with a particular user by virtue of using a user device known to be associated with the user.

[00785] In some embodiments, the first information from the identity provider may describe access to particular resources (e.g., SaaS applications or other resources) via the identity provider. Thus, access to a resource may be described using data from an identity provider, data from the resource itself, or both. Where two-factor authentication or other supplemental authentication schemes are used, the first information may describe a method of two-factor authentication used, values or data points used in the two-factor authentication, and so forth.

[00786] The first information may be requested on a per device basis using particular device attributes, on a per user basis using a username for the user, and combinations thereof. For example, an API request or other request may be provided to a particular data source (e.g., an identity provider, a SaaS application) to retrieve first information records having a particular username, a particular device identifier, or both. Such a request may also include other delimiters or filters, including particular time ranges, particular ranges of IP addresses, and so forth.

[00787] One skilled in the art will appreciate that the particular data included in the first information is dependent on what information is visible to the particular data source providing the first information. For example, a SaaS service provider may have access to particular data describing access to the SaaS service provider (e.g., logs of the SaaS application) that may differ from information accessible or visible to an identity provider.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00459

[00788] The method of Fig. 16 also includes gathering 1604, from at least a subset of the one or more user devices, second information describing access to the one or more resources. For example, assume that a user device is configurable to provide information (e.g., the second information) to a distributed edge platform or other computing environment using a client application executed on the user device. Such a client application may include, for example, a proxy application or an application implementing proxy functionality such that network traffic from the user device, including requests to access the one or more resources, is routed to the distributed edge platform or another destination.

[00789] Such a client application may also provide, to the distributed edge platform, metadata describing network requests or device attributes. In some embodiments, the metadata is generated by the client application and included with or appended to network requests routed to a proxy destination. In some embodiments, the metadata is generated by the client application and sent in a separate data payload or data stream. The second information may include a variety of data points or attributes as described above with respect to describing behavior of a user or a user device, including device identifiers, user identifiers, location identifiers, device attributes (e.g., an operating system or operating system version, a hardware configuration), device performance attributes (e.g., memory usage, processor usage, bandwidth usage, and the like), accessed resource identifiers, times at which particular network requests or resource accesses occurred, and the like. The second information may also describe network requests for accessing or logging into an identity provider, such as an identifier for the identity provider, a time at which the access occurred, authentication credentials used to access the identity provider, and the like.

[00790] The second information is gathered from at least a subset of the one or more user devices due to the second information being gathered via a client application. Where a user device does not use the client application, or use of the client application is circumvented somehow, second information may not be gathered from that user device. Although the present discussion describes gathering 1604 second information from at least a subset of the user devices, one skilled in the art will appreciate that, in some embodiments, no portions of second information may be gathered from any user devices. Accordingly, a lack of gathering any second information from any user device is also contemplated within the scope of the present disclosure. Thus, a null set of second information is also contemplated in the scope of the present disclosure.

[00791] The method of Fig. 16 also includes identifying 1606 one or more shadow systems based on a discrepancy between the first information and the second information. As described herein, “shadow systems” are user devices engaging in “shadow information technology (IT)” as would be appreciated by one skilled in the art, whereby access to a resource is performed outside of the operational control of an IT department. For example, in some embodiments, a user device

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00460

associated with a user of an organization may be used to access applications (e.g., SaaS applications, web-based applications) deployed or managed outside of the organization (e.g., "shadow applications"). As another example, a user device associated with the user may be used to access applications deployed or managed by the organization, but the user device is not accessing the application by a designated methodology. For example, the user device may be accessing the application without the use of a client application as described above that performs proxy functionality for redirecting network requests to a distributed edge platform or other execution environment. As a further example, the user device may be accessing the application using an unauthorized, unknown, or malicious virtual private network (VPN) or proxy service. Such user devices are hereinafter referred to as "shadow systems."

[00792] As is set forth above, both the first information and the second information describe access to the one or more resources from different perspectives. The first information is generated from the perspective of an identity provider or SaaS accessed via a user device, and the second information is generated from the perspective of a user device via a client application executed on the user device. Each access to a particular resource by a user device should be described in first information gathered from the identity provider, from the resource itself, or both. In contrast, access to a resource by a user device will only be described in second information from that user device if the access was performed via the client application (e.g., via a proxy application or by proxy functionality of that application). Thus, where a user device accesses a resource without using the client application or otherwise circumventing the client application, that access will be described in the first information but not described in any second information from the user device.

[00793] Accordingly, in some embodiments, identifying 1608 the shadow systems includes identifying 1608 accesses described in the first information and not described in the second information and identifying 1610, as one or more shadow systems, one or more user devices corresponding to the one or more accesses. A user device that performed the identified 1608 accesses is thus identified as a "shadow system." In other words, identifying 1606 the shadow systems includes identifying one or more shadow systems by identifying 1608 accesses described in the first information and not described in the second information and identifying, as a shadow system, one or more devices that performed the identified 1608 accesses.

[00794] In response to identifying 1606 the shadow systems, various remedial actions may be performed as is described in further detail below. One skilled in the art will appreciate that identifying 1606 one or more shadow systems improves security by identifying those user devices circumventing organizational policies or security monitoring systems in order to access organizational resources.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00461

[00795] A designation of a user device as a shadow system may affect detections of abnormal or risky user behavior according to the approaches described above. For example, a designation of a user device as a shadow system may factor in a composite score used to evaluate whether some use of the user device (e.g., some network activity) deviates from normal behavior of the user. As another example, designation of a user device as a shadow system may be provided as input to a model that identifies abnormal behavior for a user.

[00796] For further explanation, Fig. 17 sets forth a flowchart of another example method of using activity from multiple data sources to identify shadow systems according to some embodiments of the present disclosure. The method of Fig. 17 is similar to Fig. 16 in that the method of Fig. 17 includes gathering 1602 first information describing access to one or more resources by one or more user devices of a user; gathering 1604, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying 1606 one or more shadow systems based on a discrepancy between the first information and the second information by identifying 1608 accesses described in the first information and not described in the second information and identifying 1610, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

[00797] The method of Fig. 17 differs from Fig. 16 in that the method of Fig. 17 also includes generating 1702 a polygraph indicating the one or more shadow systems. Such a polygraph may be generated according to any approach for generating polygraphs as described above. An example polygraph 2000 for indicating shadow systems is set forth in Fig. 20. The polygraph 2000 of Fig. 20 describes network activity with respect to a user, represented in the polygraph 2000 as User ABC 2002.

[00798] The polygraph 2000 also includes a representation of a location associated with the user, shown as San Francisco, CA 2004. The location of the user may be determined using similar approaches as are set forth above. The polygraph 2000 also includes representations of user devices associated with the user, shown as primary device 2006 and other device 2008.

[00799] The polygraph 2000 also includes representations for executable applications (e.g., executables on the primary device 2006 or other device 2008) used to access particular resources, shown as web browser application 2010 and web browser application 2012. The polygraph 2000 also includes representations of SaaS applications accessed by the user via the user devices, shown as application 2014 and application 2016.

[00800] Here, the one or more shadow systems are indicated in the polygraph using an alert 2018 included in the polygraph 2000. The alert 2018 is anchored to the representation of the other device 2008, indicating that the other device 2008 has been identified as a shadow system. As the polygraph 2000 only shows the other device 2008 accessing the application 2016, it is

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00462

understood that, in this example, the other device 2008 is identified as a shadow system by accessing the application 2016 in an unauthorized manor, such as without using a client application (e.g., a proxy application) that would generate second information describing access to the application 2016 by the other device 2008.

[00801] Although the polygraph 2000 indicates shadow systems by anchoring an alert 2018 to an identified shadow system, one skilled in the art will appreciate that other approaches for indicating shadow systems may also be used. For example, an alert 2018 may be anchored to another node or to a connection between nodes. As another example, the representation of the other device 2008 may include a label, highlighting, flag, icon, or other distinguishing mark signifying that the other device 2008 has been identified as a shadow system. As another example, one or more connections between nodes (e.g., between the other device 2008, web browser application 2012, or application 2016 may be highlighted or otherwise designated, thereby indicating that some access was performed by a shadow system.

[00802] For further explanation, Fig. 18 sets forth a flowchart of another example method of using activity from multiple data sources to identify shadow systems according to some embodiments of the present disclosure. The method of Fig. 18 is similar to Fig. 16 in that the method of Fig. 18 includes gathering 1602 first information describing access to one or more resources by one or more user devices of a user; gathering 1604, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying 1606 one or more shadow systems based on a discrepancy between the first information and the second information by identifying 1608 accesses described in the first information and not described in the second information and identifying 1610, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

[00803] The method of Fig. 18 differs from Fig. 16 in that the method of Fig. 18 also includes generating 1802 an alert in response to identifying the one or more shadow systems. The alert may be embodied in a variety of approaches. For example, the alert may be presented as an alert 2018 in a polygraph 2000 as set forth above. As another example, the alert may be embodied as a notification, text message, email, chat message, or other message sent to one or more recipients. Such recipients may include, the user, the shadow system, a manager, administrator, or other supervisor of the user, a security team member, or other recipients as can be appreciated.

[00804] In some embodiments, the alert may identify the shadow system. As another example, the alert may describe one or more accesses that caused the device to be identified as a shadow system. As another example, the alert may include links to polygraphs or other visualizations describing the shadow systems. As will be described in further detail below, the alert may be used to direct the user to a remediation workflow by including one or more links or other user

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00463

interface elements that, when selected, cause a user device (e.g., a shadow system) to access a remediation workflow.

[00805] For further explanation, Fig. 19 sets forth a flowchart of another example method of using activity from multiple data sources to identify shadow systems according to some embodiments of the present disclosure. The method of Fig. 19 is similar to Fig. 16 in that the method of Fig. 19 includes gathering 1602 first information describing access to one or more resources by one or more user devices of a user; gathering 1604, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying 1606 one or more shadow systems based on a discrepancy between the first information and the second information by identifying 1608 accesses described in the first information and not described in the second information and identifying 1610, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

[00806] The method of Fig. 19 differs from Fig. 16 in that the method of Fig. 19 also includes directing 1902 the user to a remediation workflow in response to identifying the one or more shadow systems. A remediation workflow is one or more steps performed by a user device in order to remediate past shadow activity (e.g., activity that caused a user device to be identified as a shadow system), such as by preventing subsequent shadow activity or mitigating any potential harm that may have resulted from the shadow activity. For example, in some embodiments, a user may be directed 1902 to a remediation workflow by sending an alert, link, message, and the like to an identified shadow system or other user device associated with the user.

[00807] In some embodiments, the remediation workflow may facilitate installation or repair of an existing installation of a client application used to access remote resources, such as a client application that performs proxy functions on the installed user device. Accordingly, in some embodiments, the remediation workflow may include links to download the client application for installation, descriptions for installation of the client application, and the like. In some embodiments, the remediation workflow may facilitate identification and remediation of potential harm from the shadow activity. For example, the remediation workflow may include links to malware detection or remediation software, instructions for installation and use of such software, and the like. The remediation workflow may also include steps for confirming completion of prior steps in the remediation workflow. For example, the remediation workflow may include a link that when selected, causes the user device to send a network request. The network request may then be analyzed by a recipient to determine if the network request was received via a particular proxy, indicating that the user successfully installed or repaired an instance of the client application. As another example, the remediation workflow may include a link or user interface element that causes malware detection or remediation software to execute,

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00464

thereby ensuring that the software was run on the user device. One skilled in the art will appreciate that other remediation approaches may also be facilitated by a remediation workflow to which the user is directed 1902.

[00808] One or more embodiments may be described herein with the aid of method steps illustrating the performance of specified functions and relationships thereof. The boundaries and sequence of these functional building blocks and method steps have been arbitrarily defined herein for convenience of description. Alternate boundaries and sequences can be defined so long as the specified functions and relationships are appropriately performed. Any such alternate boundaries or sequences are thus within the scope and spirit of the claims. Further, the boundaries of these functional building blocks have been arbitrarily defined for convenience of description. Alternate boundaries could be defined as long as the certain significant functions are appropriately performed. Similarly, flow diagram blocks may also have been arbitrarily defined herein to illustrate certain significant functionality.

[00809] To the extent used, the flow diagram block boundaries and sequence could have been defined otherwise and still perform the certain significant functionality. Such alternate definitions of both functional building blocks and flow diagram blocks and sequences are thus within the scope and spirit of the claims. One of average skill in the art will also recognize that the functional building blocks, and other illustrative blocks, modules and components herein, can be implemented as illustrated or by discrete components, application specific integrated circuits, processors executing appropriate software and the like or any combination thereof.

[00810] While particular combinations of various functions and features of the one or more embodiments are expressly described herein, other combinations of these features and functions are likewise possible. The present disclosure is not limited by the particular examples disclosed herein and expressly incorporates these other combinations.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00465

CLAIMS

What is claimed is:

1. A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising:

gathering first information describing access to one or more resources by one or more user devices of a user;

gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identifying one or more shadow systems based on a discrepancy between the first information and the second information.

2. The method of claim 1 wherein the first information is gathered from one or more identity providers.

3. The method of claim 1 wherein the first information is gathered from the one or more applications.

4. The method of claim 1 further comprising generating a polygraph indicating the one or more shadow systems.

5. The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.

6. The method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems.

7. The method of claim 1 wherein identifying the one or more shadow systems comprises:

identifying one or more accesses described in the first information but not described in the second information; and

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00466

identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

8. The method of claim 1 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices.

9. A computer program product for using activity monitored by multiple data sources to identify shadow systems, the computer program product disposed on a computer readable medium, the computer program product including computer program instructions configurable to carry out the steps of:

gathering first information describing access to one or more resources by one or more user devices of a user;

gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identifying one or more shadow systems based on a discrepancy between the first information and the second information.

10. The computer program product of claim 9 wherein the first information is gathered from one or more identity providers.

11. The computer program product of claim 9 wherein the first information is gathered from the one or more applications.

12. The computer program product of claim 9 further comprising generating a polygraph indicating the one or more shadow systems.

13. The computer program product of claim 9 wherein the steps further comprise further comprising generating an alert in response to identifying the one or more shadow systems.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00467

14. The computer program product of claim 9 wherein the steps further comprise directing the user to a remediation workflow in response to identifying the one or more shadow systems.

15. The computer program product of claim 9 wherein identifying the one or more shadow systems comprises;

identifying one or more accesses described in the first information but not described in the second information; and

identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.

16. The computer program product of claim 9 wherein the second information is gathered via one or more proxy application executed on the at least a subset of the one or more user devices.

17. A system for using activity monitored by multiple data sources to identify shadow systems, the system configurable to carry out the steps of:

gathering first information describing access to one or more resources by one or more user devices of a user;

gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and

identifying one or more shadow systems based on a discrepancy between the first information and the second information.

18. The system of claim 17 wherein the first information is gathered from one or more identity providers.

19. The system of claim 17 wherein the first information is gathered from the one or more applications.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00468

20. The system of claim 17 wherein the steps further comprise generating a polygraph indicating the one or more shadow systems.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00469

ABSTRACT

Using activity monitored by multiple data sources to identify shadow systems, the method comprising: gathering first information describing access to one or more resources by one or more user devices of a user; gathering, from at least a subset of the one or more user devices, second information describing access to the one or more resources; and identifying one or more shadow systems based on a discrepancy between the first information and the second information.

Netskope Ex-1002
Netskope v. Fortinet IPR2026-00472
Page 00470

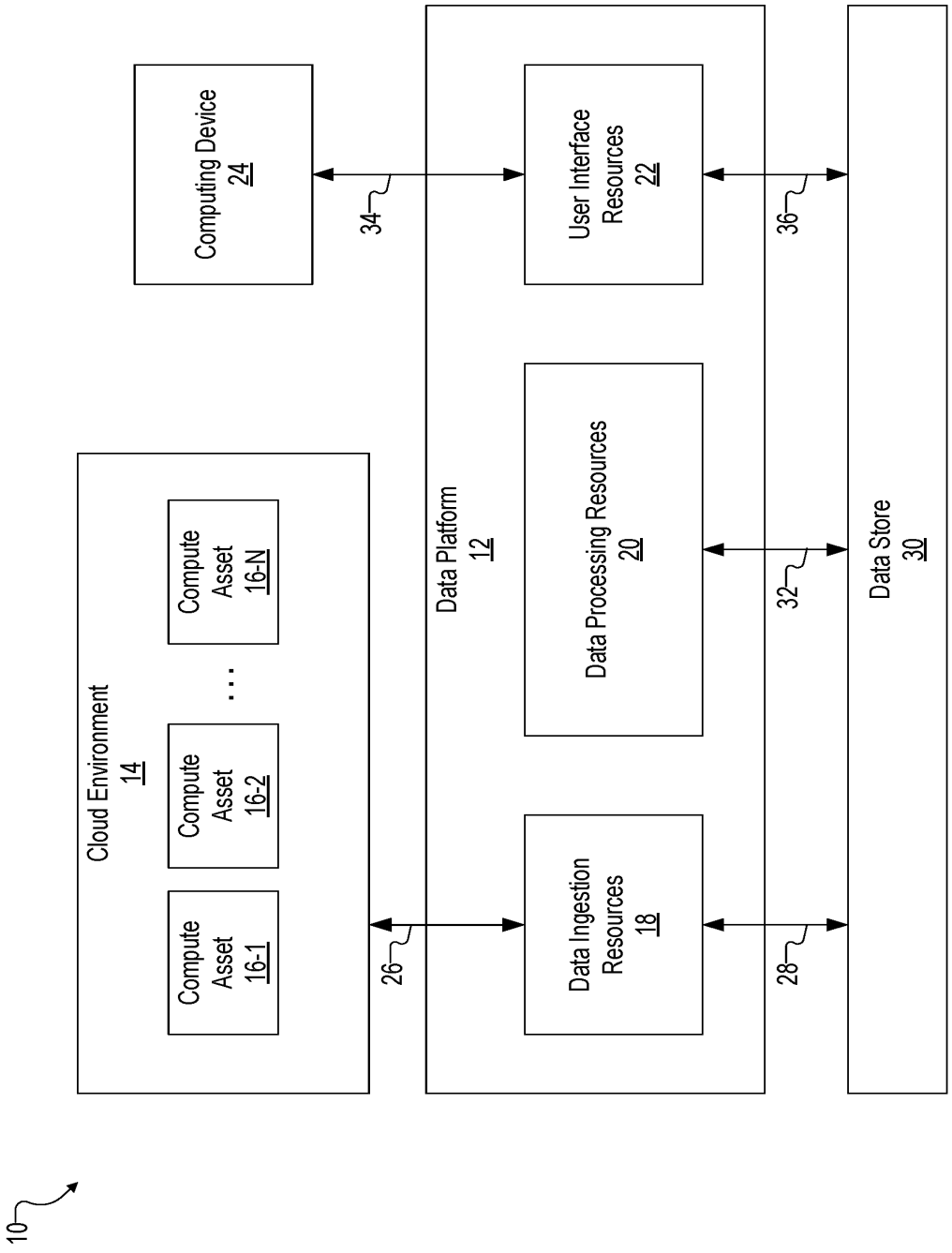

10
Cloud Environment
14
Compute Asset 16-1
Compute Asset 16-2
Compute Asset 16-N
Computing Device
24
Data Platform
12
Data Ingestion Resources
18
Data Processing Resources
20
User Interface Resources
22
Data Store
30
26
28
32
34
36

Fig. 1A

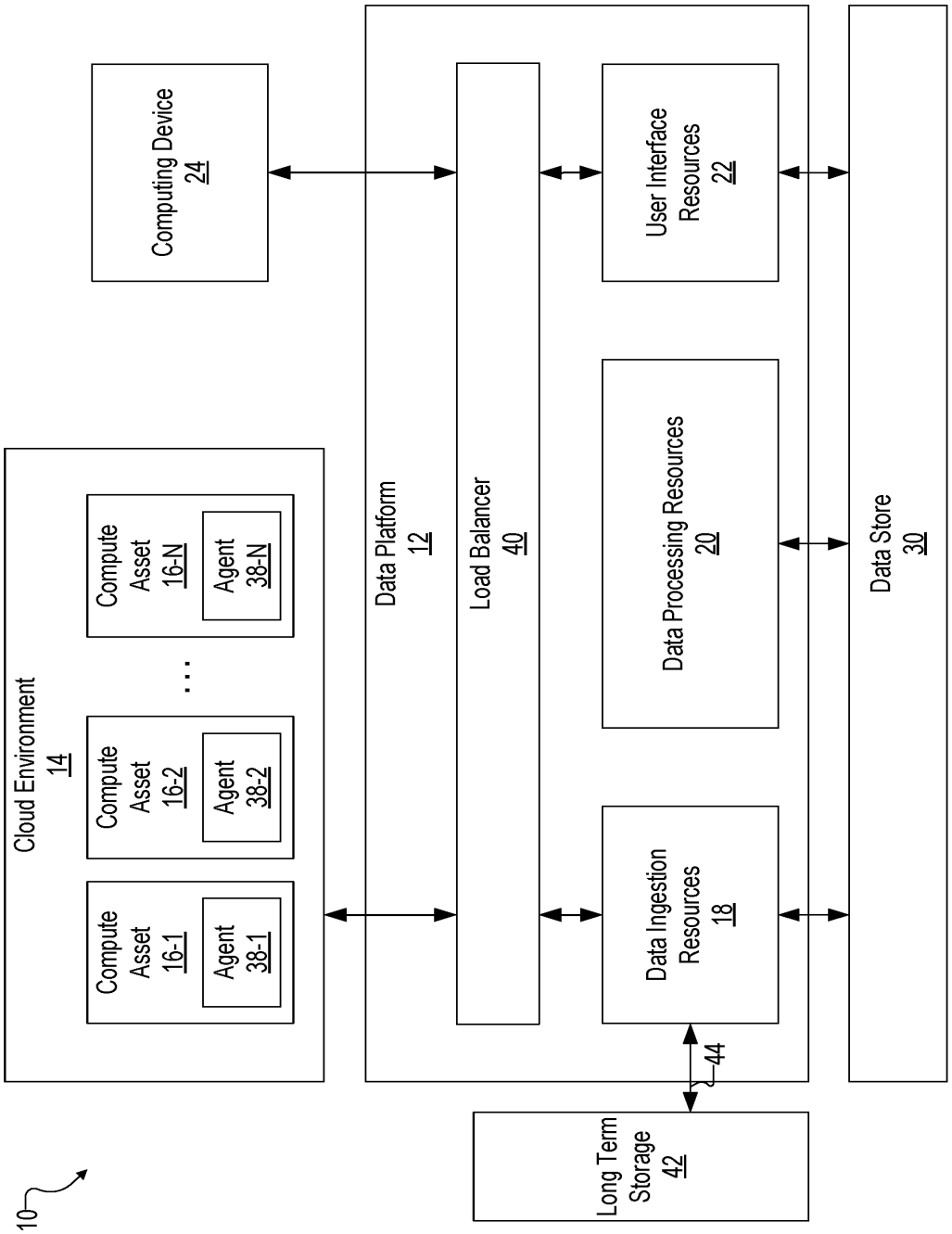

10
Cloud Environment
14
Compute Asset 16-1
Agent 38-1
Compute Asset 16-2
Agent 38-2
Compute Asset 16-N
Agent 38-N
Computing Device
24
Data Platform
12
Load Balancer
40
Data Ingestion Resources
18
Data Processing Resources
20
User Interface Resources
22
Data Store
30
44
Long Term Storage
42

Fig. 1B

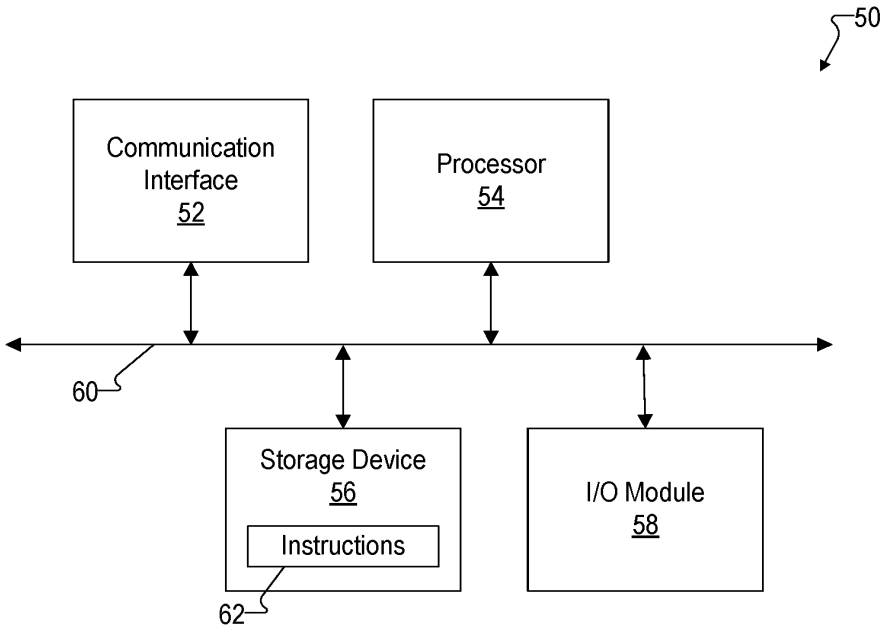

50
Communication Interface 52
Processor 54
60
Storage Device 56
Instructions
62
I/O Module 58

Fig. 1C

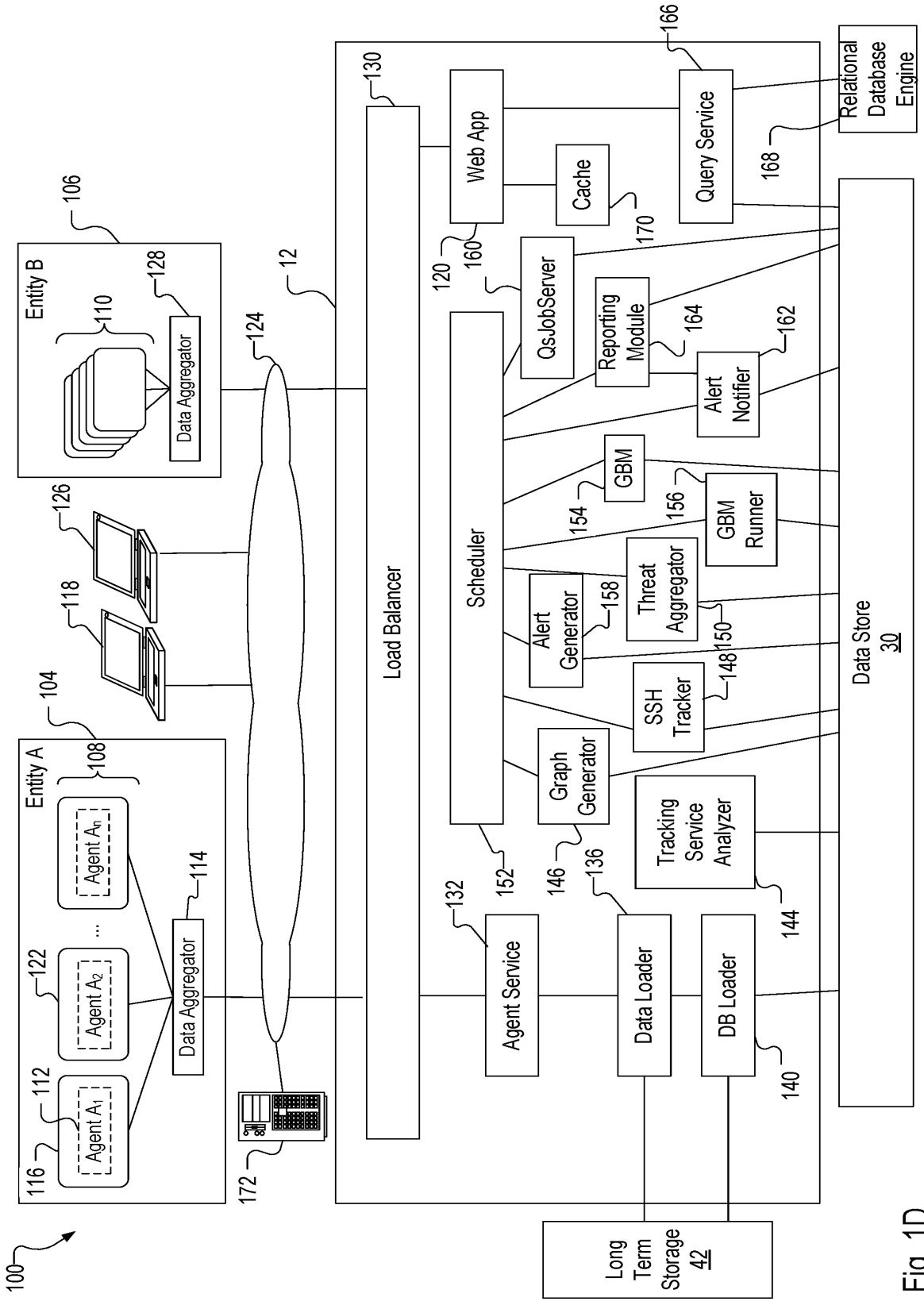

100
Entity A
104
108
Agent A_1
112
116
Agent A_2
122
Agent A_n
...
Data Aggregator
114
118
126
Entity B
106
110
128
Data Aggregator
12
124
172
Load Balancer
130
Web App
Cache
Query Service
166
Relational Database Engine
168
170
120
160
QsJobServer
Reporting Module
164
Alert Notifier
162
Scheduler
GBM
154
GBM Runner
156
Alert Generator
158
Threat Aggregator
150
SSH Tracker
148
Graph Generator
146
Tracking Service Analyzer
144
Agent Service
132
152
Data Loader
136
DB Loader
140
Data Store
30
Long Term Storage
42

Fig. 1D

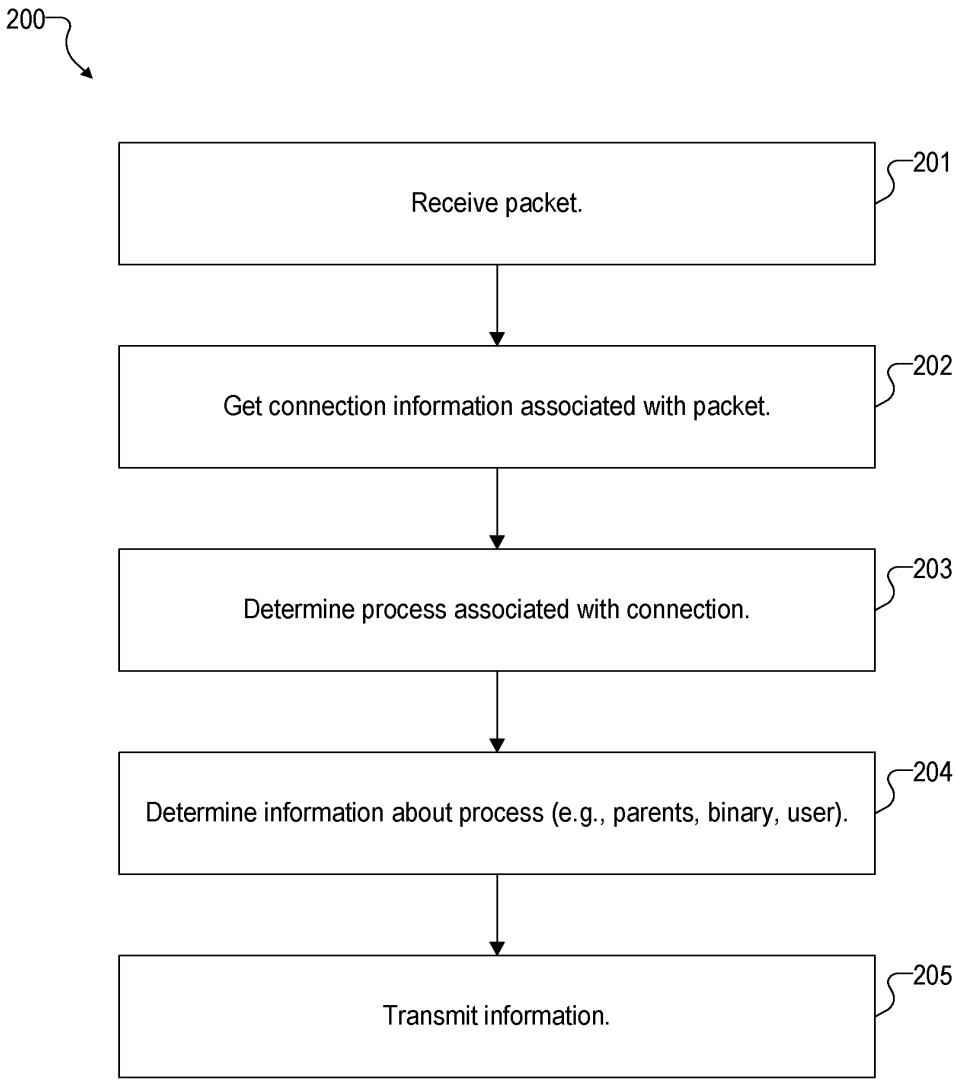

200
Receive packet.
201
Get connection information associated with packet.
202
Determine process associated with connection.
203
Determine information about process (e.g., parents, binary, user).
204
Transmit information.
205

Fig. 2A

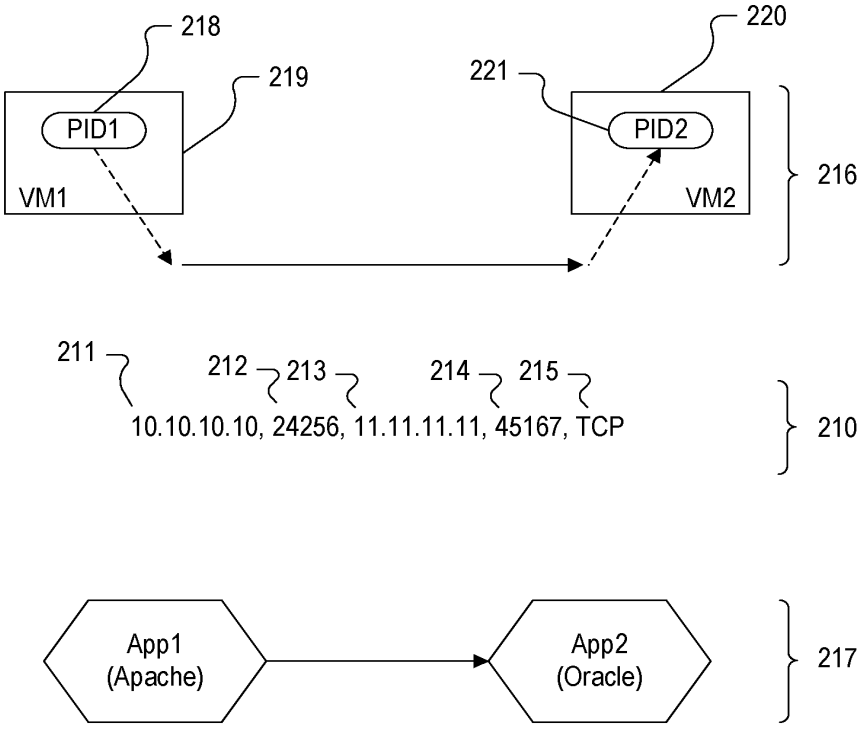

218
219
220
221
PID1
PID2
VM1
VM2
216
211
212
213
214
215
10.10.10.10, 24256, 11.11.11.11, 45167, TCP
210
App1
(Apache)
App2
(Oracle)
217

Fig. 2B

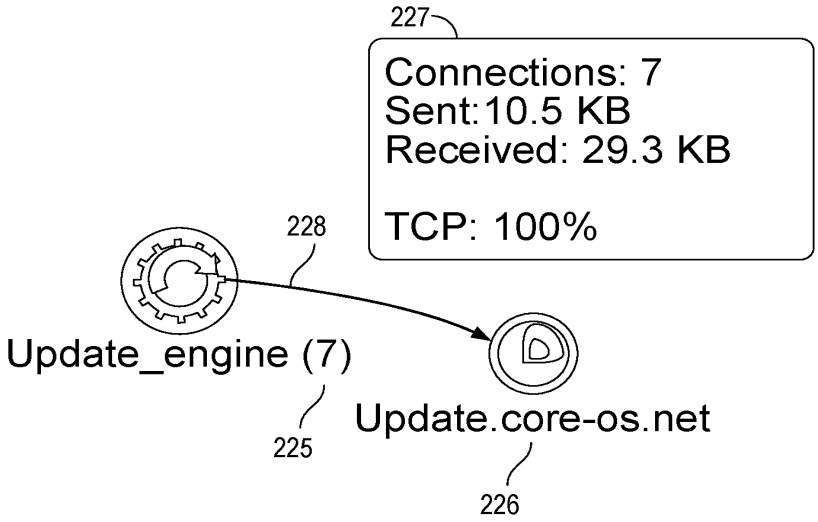

227
Connections: 7
Sent:10.5 KB
Received: 29.3 KB
TCP: 100%
228
Update_engine (7)
225
Update.core-os.net
226

Fig. 2C

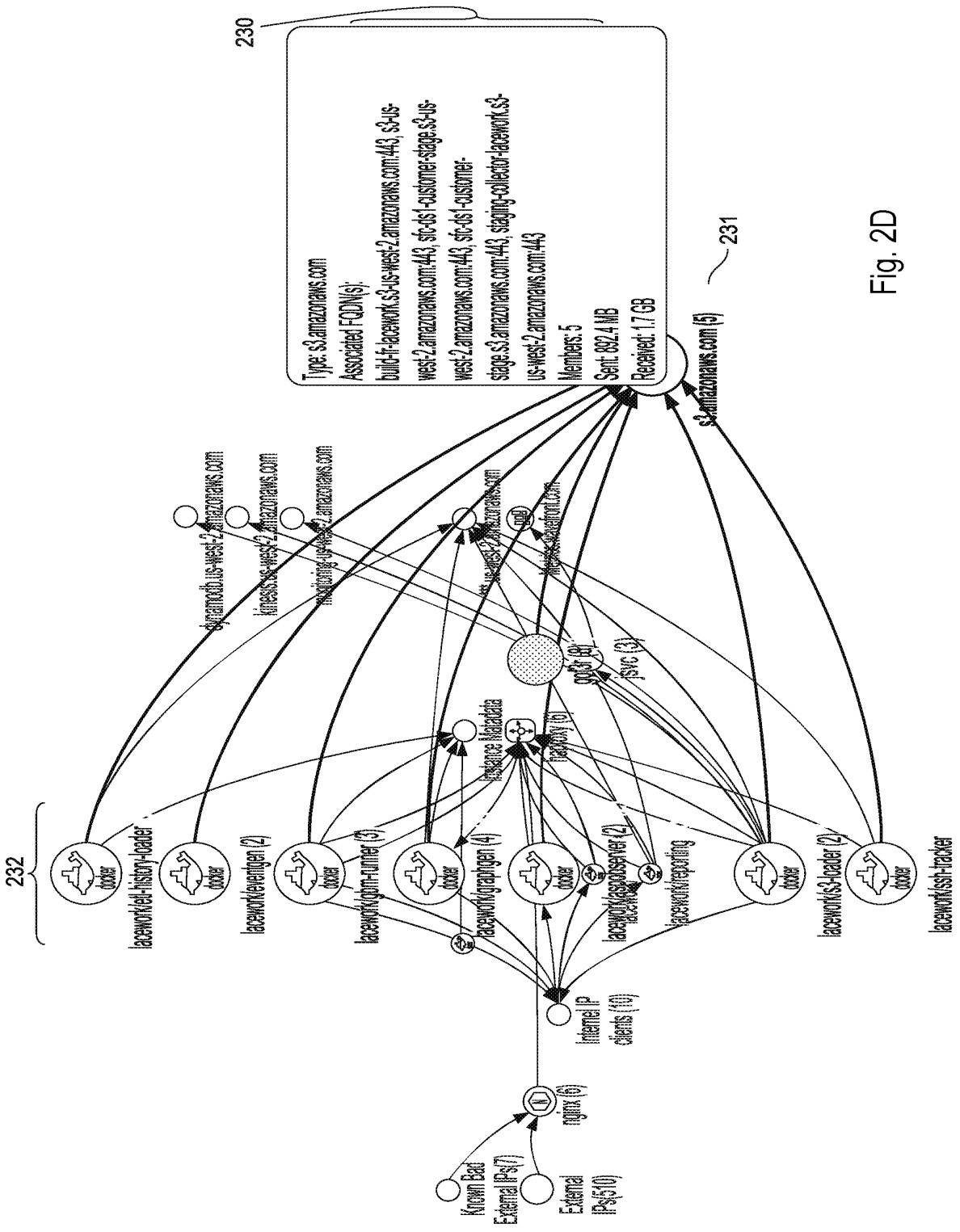

230
Type: s3.amazonaws.com
Associated FQDN(s):
build-fr-lacework.s3-us-west-2.amazonaws.com:443, s3-us-west-2.amazonaws.com:443, sfc-ds1-customer-stage.s3-us-west-2.amazonaws.com:443, sfc-ds1-customer-stage.s3.amazonaws.com:443, staging-collector-lacework.s3-us-west-2.amazonaws.com:443
Members: 5
Sent: 892.4 MB
Received: 1.7 GB
231
s3.amazonaws.com (5)
232
lacework/ecr-tracker
lacework/s3-loader (2)
lacework/reporting
lacework/cassdbserver (2)
lacework/graphgen (4)
lacework/cqlm-runner (3)
lacework/eventgen (2)
lacework/ecl-history-loader
Internal IP clients (10)
nginx (6)
External IPs (10)
Known Bad External IPs (7)
Instance Metadata
dynamodb.us-west-2.amazonaws.com
kinesis.us-west-2.amazonaws.com
monitoring.us-west-2.amazonaws.com
docker

Fig. 2D

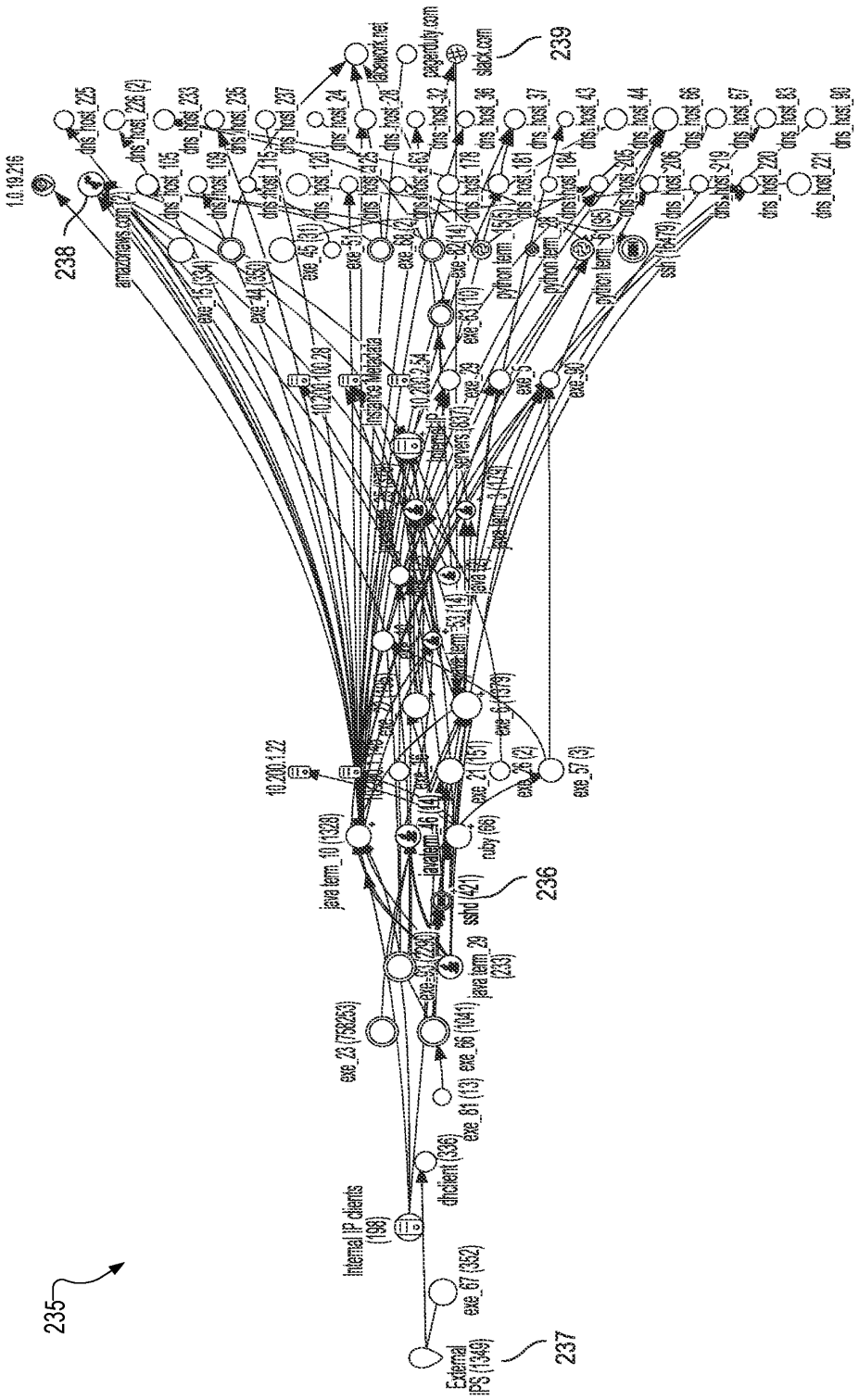

238
239
236
235
237
internal IP clients (196)
External IPS (1349)
java term_10 (1328)
sshd (421)
ruby (66)
python term_28 (1616)
python term_29 (1616)
python term_31 (1616)
ssh (1647)
slack.com
pagerduty.com
amazonaws.com (2)
10.200.1.22
10.200.100.28
10.200.2.24
InstanceIP
InstanceMetadata
servers (837)
invclient (336)
exe_67 (3352)
exe_23 (7502253)
exe_66 (1041)
exe_81 (13)
java term_29 (233)

Fig. 2E

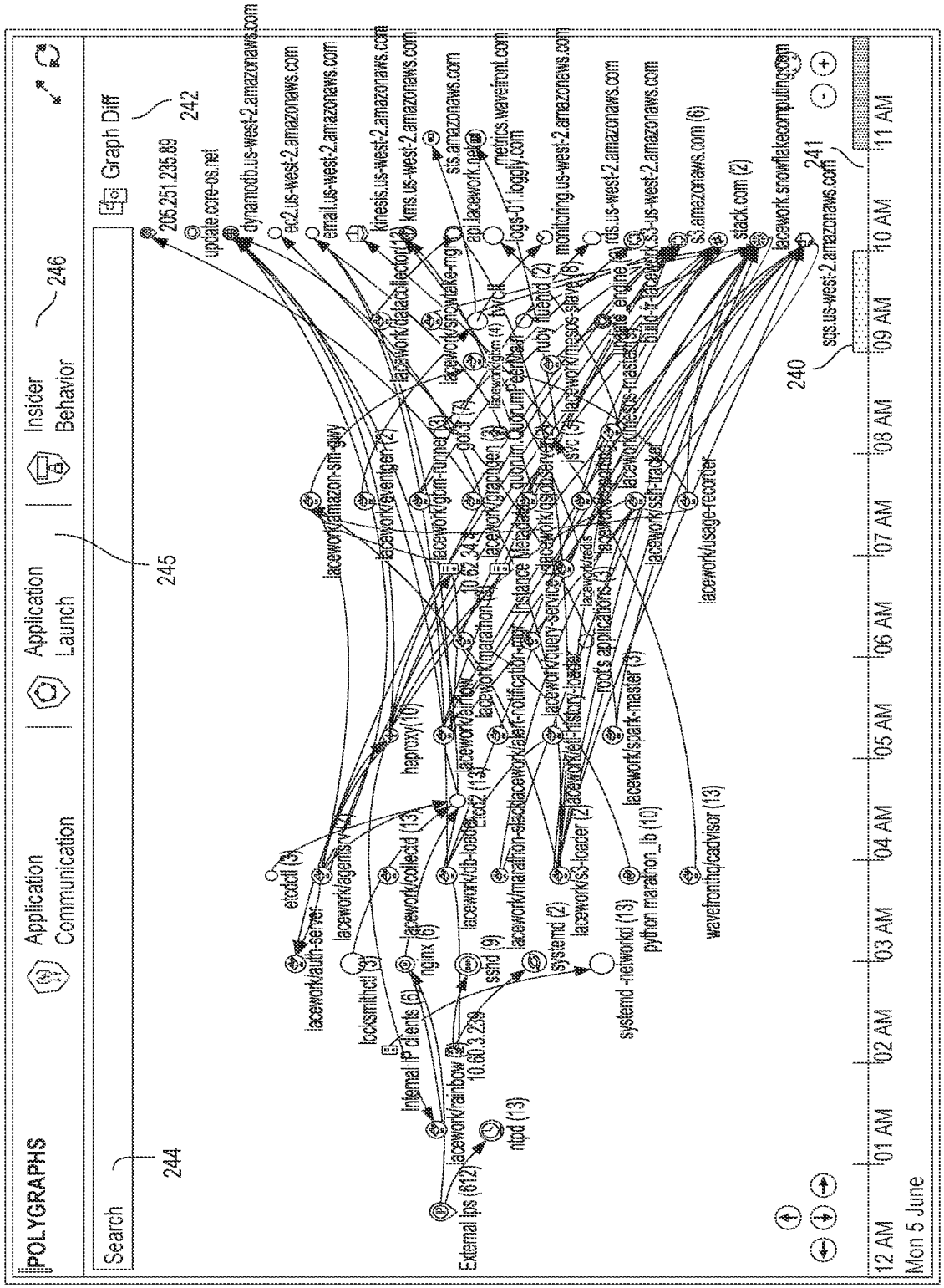

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
246
Graph Diff
242
Search
244
245
205.251.235.89
update.core-os.net
dynamodb.us-west-2.amazonaws.com
ec2.us-west-2.amazonaws.com
email.us-west-2.amazonaws.com
kinesis.us-west-2.amazonaws.com
kms.us-west-2.amazonaws.com
sts.amazonaws.com
api.lacework.net
metrics.wavefront.com
logs-01.loggly.com
monitoring.us-west-2.amazonaws.com
rds.us-west-2.amazonaws.com
s3.us-west-2.amazonaws.com
s3.amazonaws.com (6)
slack.com (2)
lacework.snowflakecomputing.com
sqs.us-west-2.amazonaws.com
241
240
lacework/amazon-sn-guy
lacework/aven-agen (12)
lacework/datacollector (13)
lacework/snowflake-mgr
lacework/dsm (4)
lacework/dsm-runner (13)
lacework/graphgen (4)
lacework/marathon-lb
10.62.34.4
lacework/query-service
lacework/discovery
lacework/redis
lacework/alert-history-loader
lacework/spark-master (3)
lacework/ssh-tracker
lacework/usage-recorder
lacework/auth-server
lacework/agentsvr
lacework/collectd (13)
lacework/db-loader
lacework/marathon-sec
lacework/marathon-sec
lacework/alert-notification-mgr
lacework/s3-loader (2)
root's applications (3)
python marathon_lb (10)
waveformhq/cadvisor (13)
etcdctl (3)
locksmithctl (3)
internal IP clients (6)
External ips (612)
10.60.3.239
haproxy (10)
nginx (6)
ssmd (9)
systemd (2)
systemd -networkd (13)
ntpd (13)
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 AM
Mon 5 June

Fig. 2F

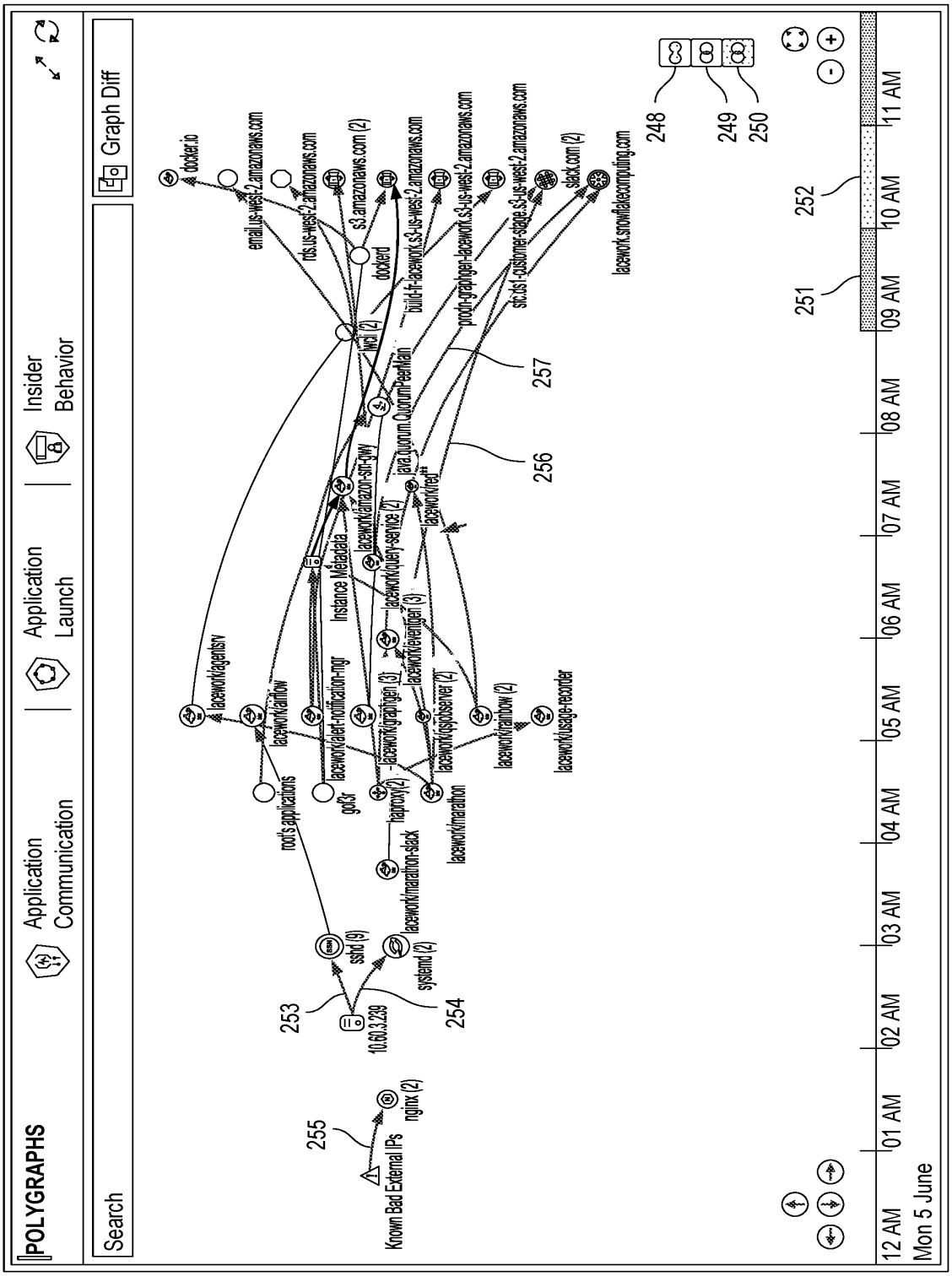

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Search
Graph Diff
docker.io
email.us-west-2.amazonaws.com
rds.us-west-2.amazonaws.com
s3.amazonaws.com (2)
dockerd
build-tf-lacework.s3-us-west-2.amazonaws.com
prodn-graphgen-lacework.s3-us-west-2.amazonaws.com
stc.cbs1-customer-stage.s3-us-west-2.amazonaws.com
slack.com (2)
lacework.snowflakecomputing.com
lacework/agentsrv
lacework/airflow
lacework/alert-notification-mgr
Instance Metadata
lacework/amazon-stir-gw
lacework/query-service (2)
lacework/reg*
java.lwquorum.QuorumPeerMain
lacework/graphgen (3)
lacework/eventgen (3)
lacework/gpsobserver (2)
lacework/marathon
lacework/rainbow (2)
lacework/usage-recorder
root's applications
got3r
haproxy (2)
lacework/marathon-slack
sshd (9)
systemd (2)
10.60.3.239
Known Bad External IPs
nginx (2)
253
254
255
256
257
248
249
250
251
252
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2G

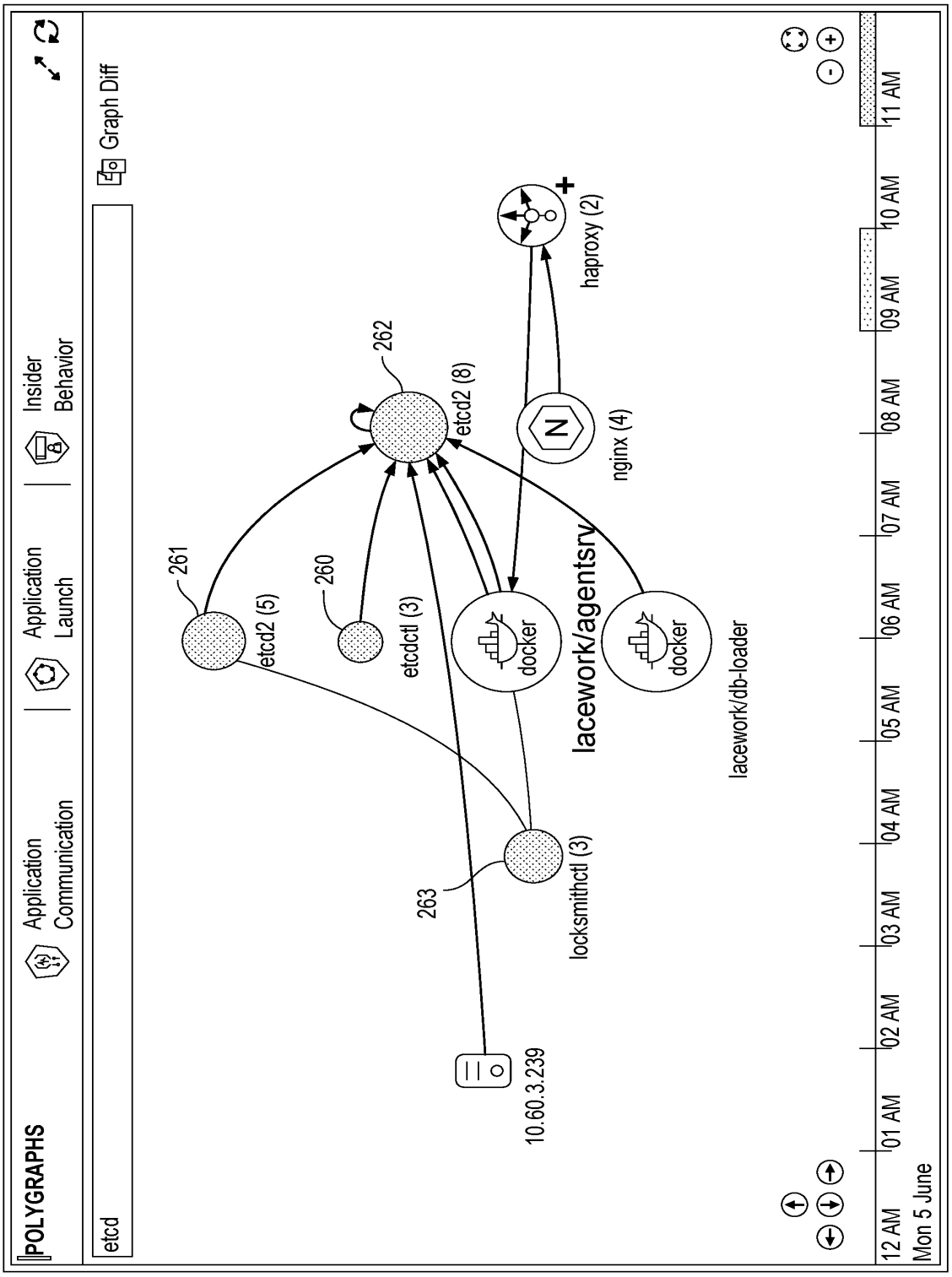

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
etcd
261
etcd2 (5)
260
etcdctl (3)
262
etcd2 (8)
haproxy (2)
nginx (4)
docker
docker
lacework/agentsrv
lacework/db-loader
263
locksmithctl (3)
10.60.3.239
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2H

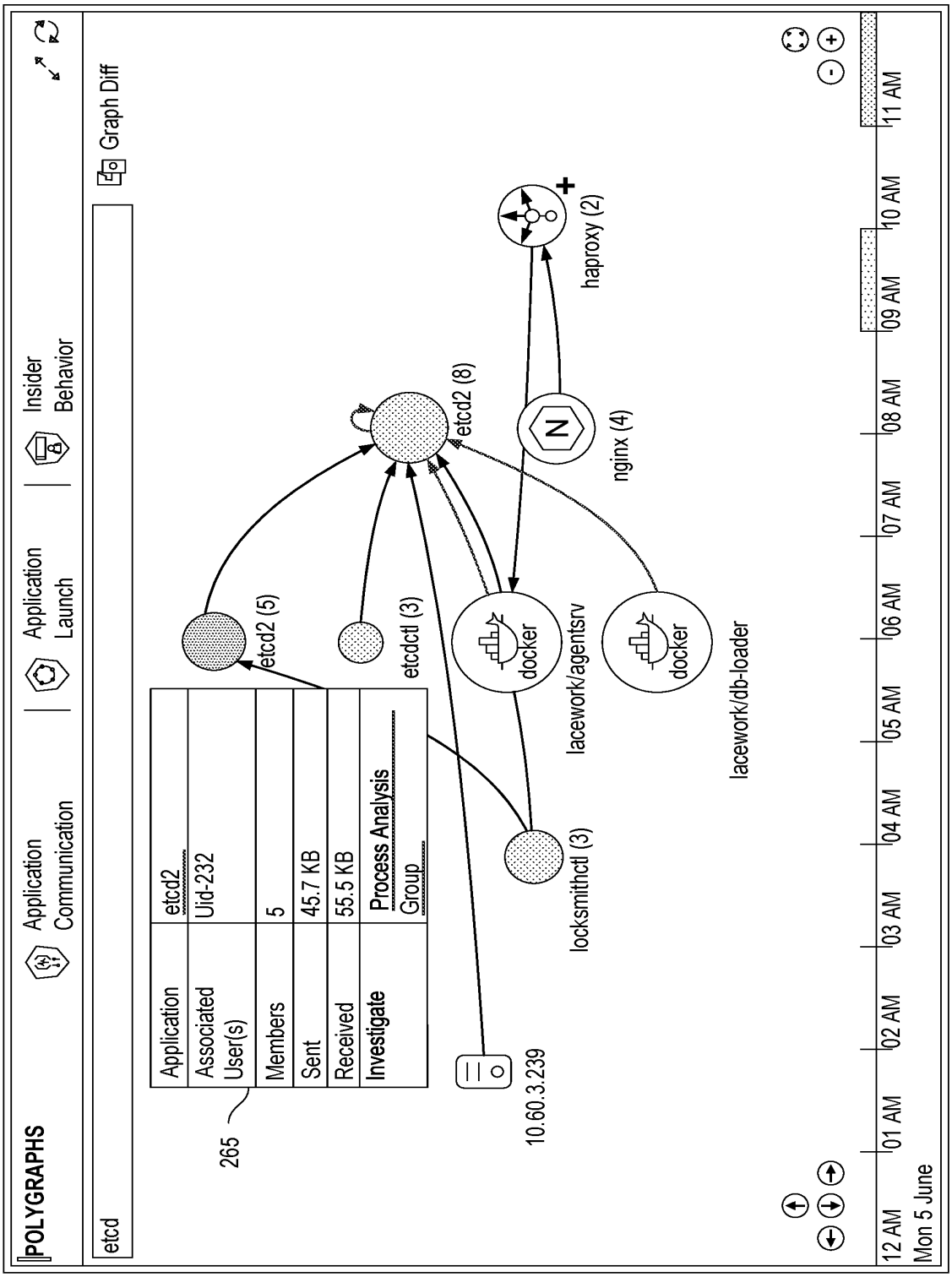

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
etcd
Application
Associated User(s)
Members
Sent
Received
Investigate
etcd2
Uid-232
5
45.7 KB
55.5 KB
Process Analysis
Group
265
etcd2 (5)
etcdctl (3)
etcd2 (8)
haproxy (2)
nginx (4)
docker
docker
lacework/agentsrv
lacework/db-loader
locksmithctl (3)
10.60.3.239
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2I

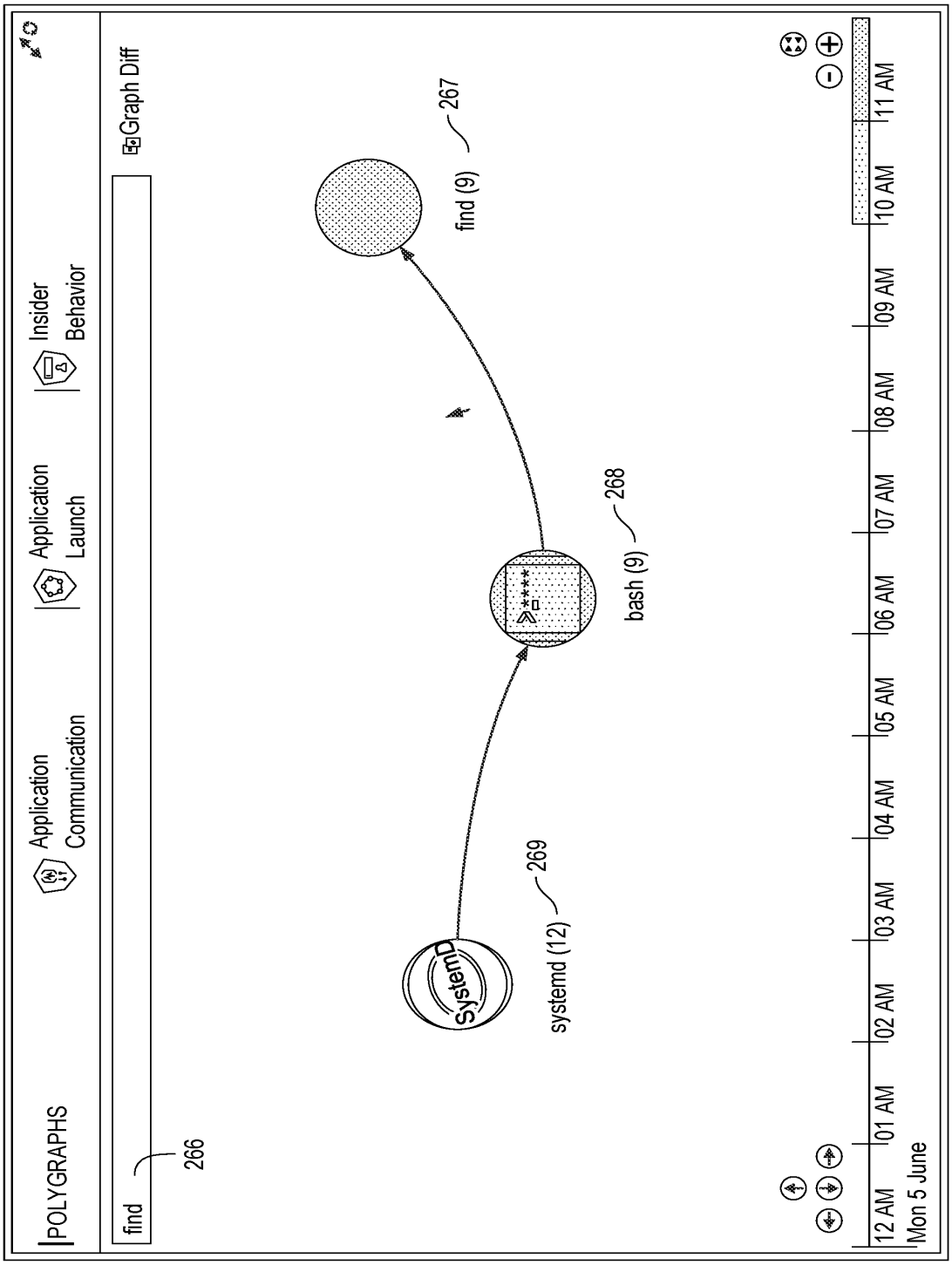

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
find
266
267
find (9)
268
bash (9)
269
systemd (12)
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2J

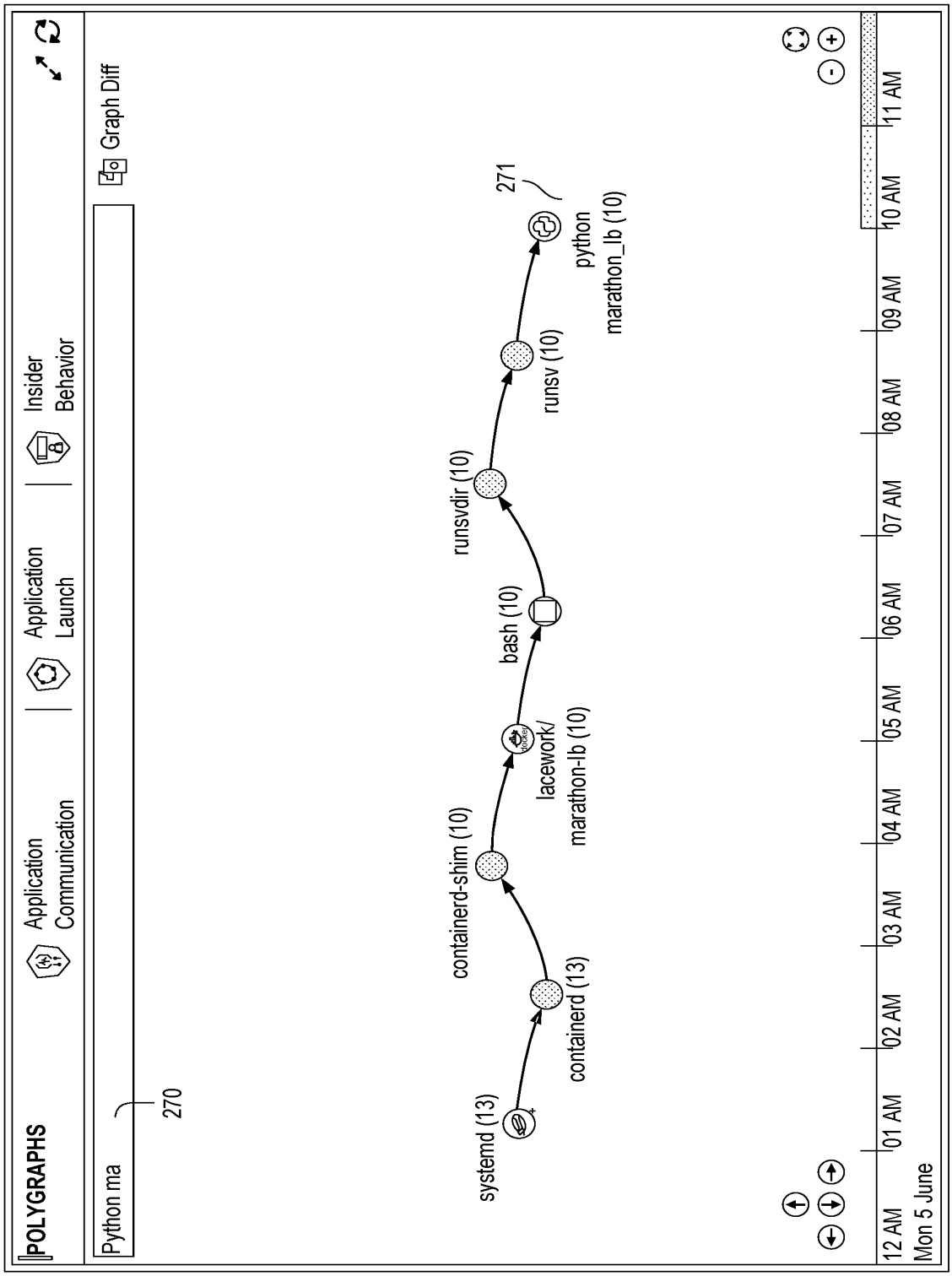

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
Python ma
270
systemd (13)
containerd (13)
containerd-shim (10)
lacework/ marathon-lb (10)
bash (10)
runsvdir (10)
runsv (10)
271
python marathon_lb (10)
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2K

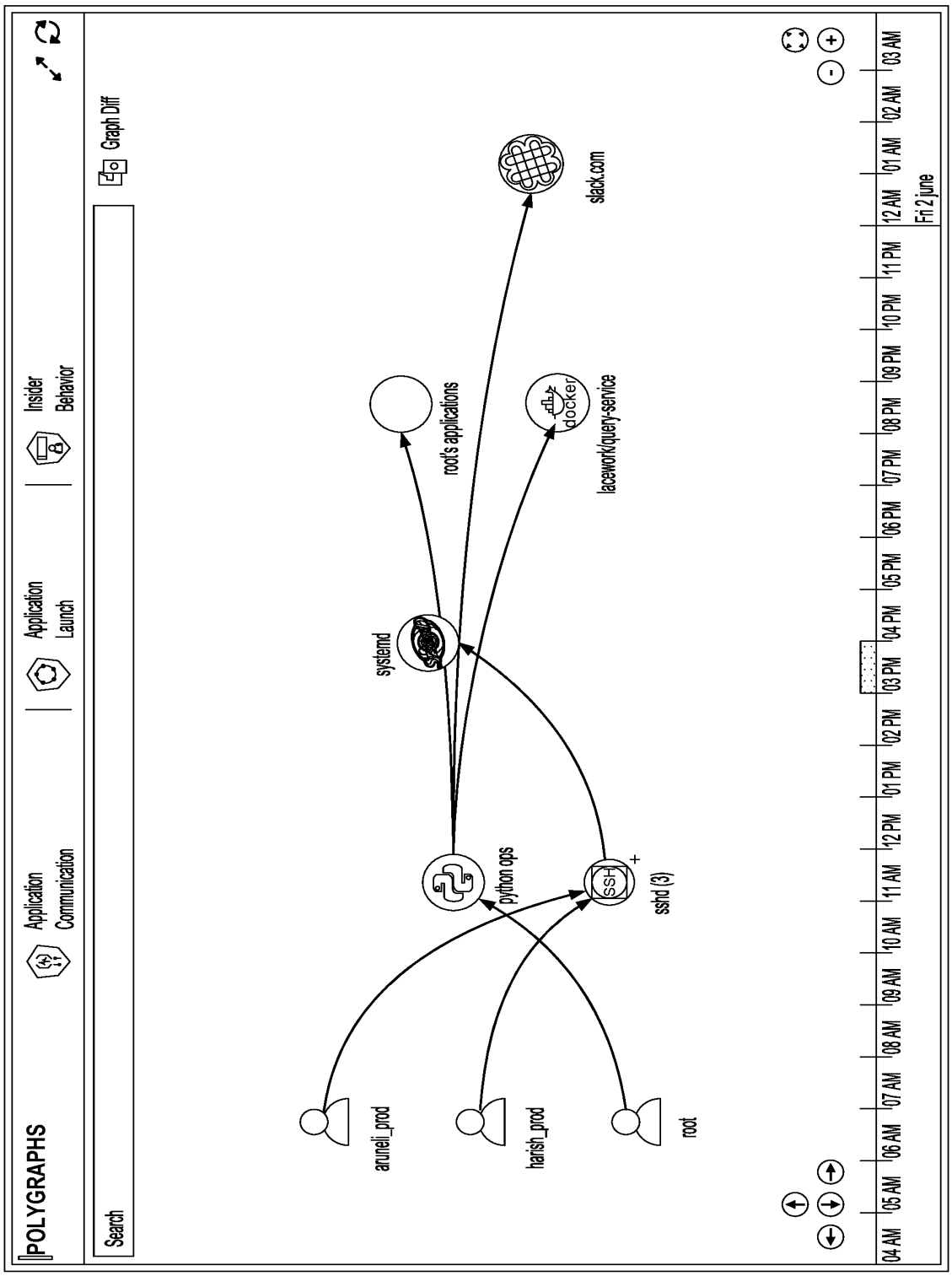

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
Search
aruneli_prod
harish_prod
root
python ops
sshd (3)
systemd
root's applications
slack.com
docker
lacework/query-service
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
07 PM
08 PM
09 PM
10 PM
11 PM
12 AM
01 AM
02 AM
03 AM
Fri 2 june

Fig. 2L

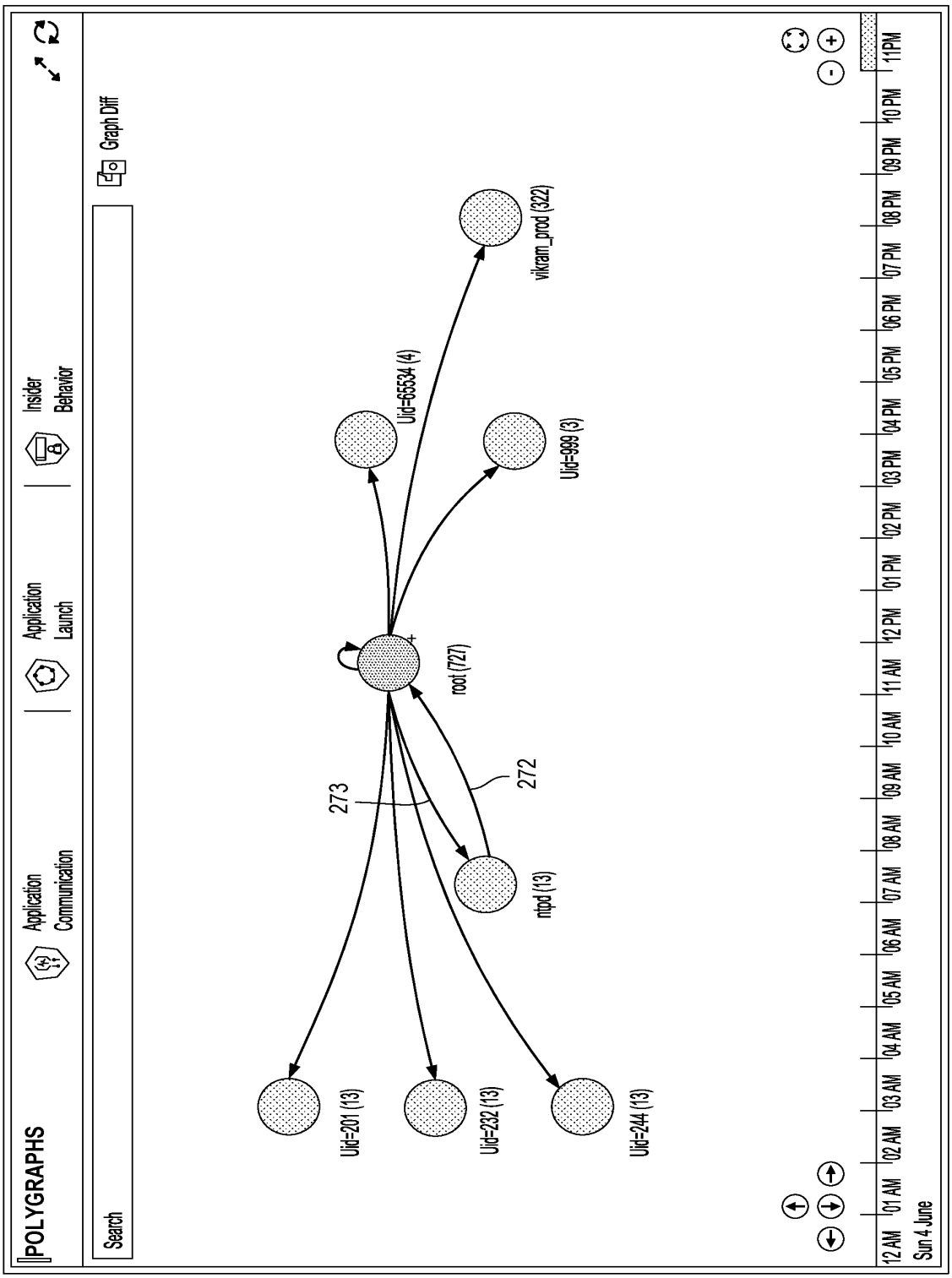

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
Search
Uid=201 (13)
Uid=232 (13)
Uid=244 (13)
ntpd (13)
root (727)
Uid=65534 (4)
vikram_prod (322)
Uid=999 (3)
273
272
12 AM
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
07 PM
08 PM
09 PM
10 PM
11PM
Sun 4 June

Fig. 2M

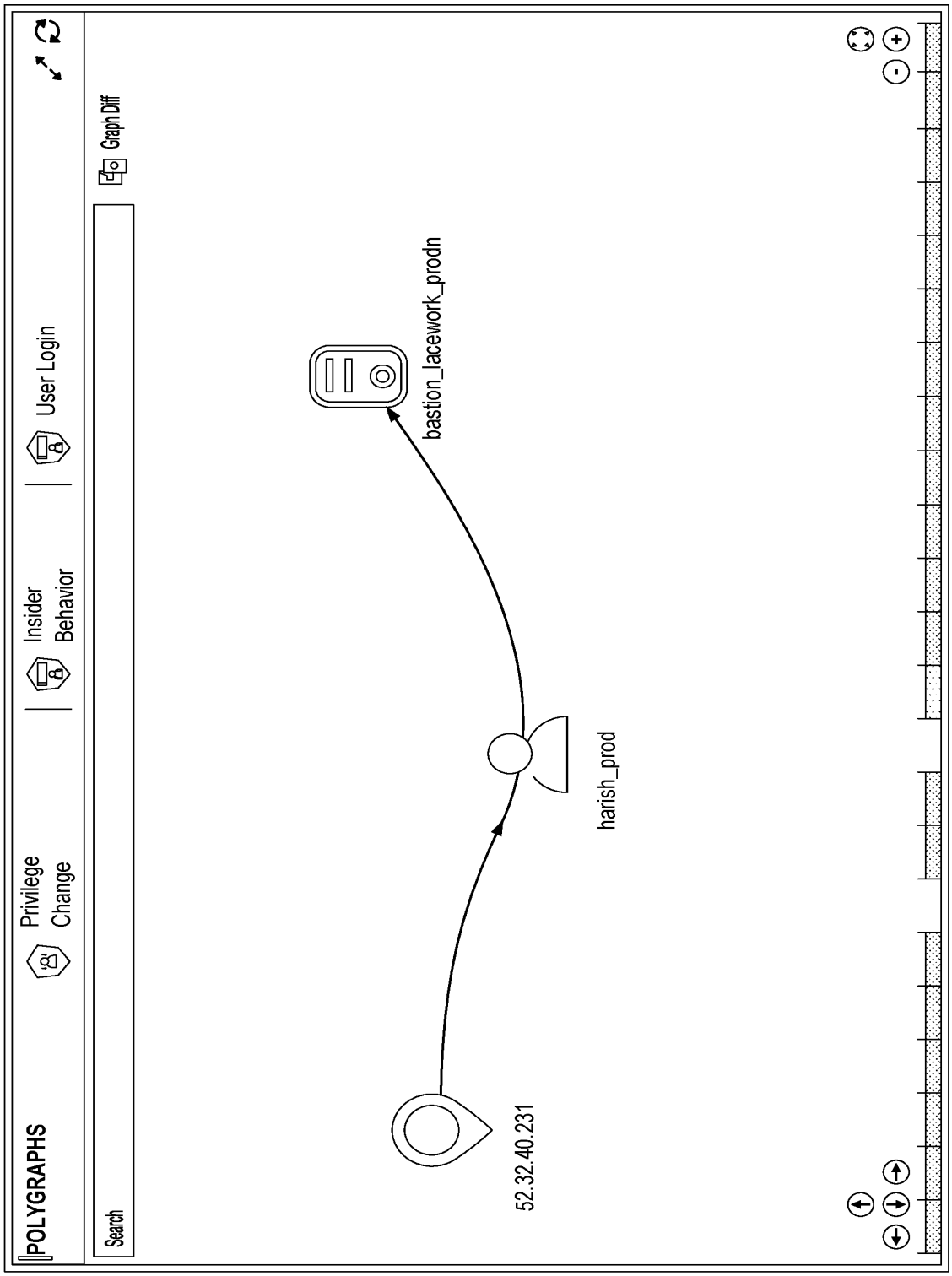

POLYGRAPHS
Privilege Change
Insider Behavior
User Login
Search
Graph Diff
bastion_lacework_prodn
harish_prod
52.32.40.231

Fig. 2N

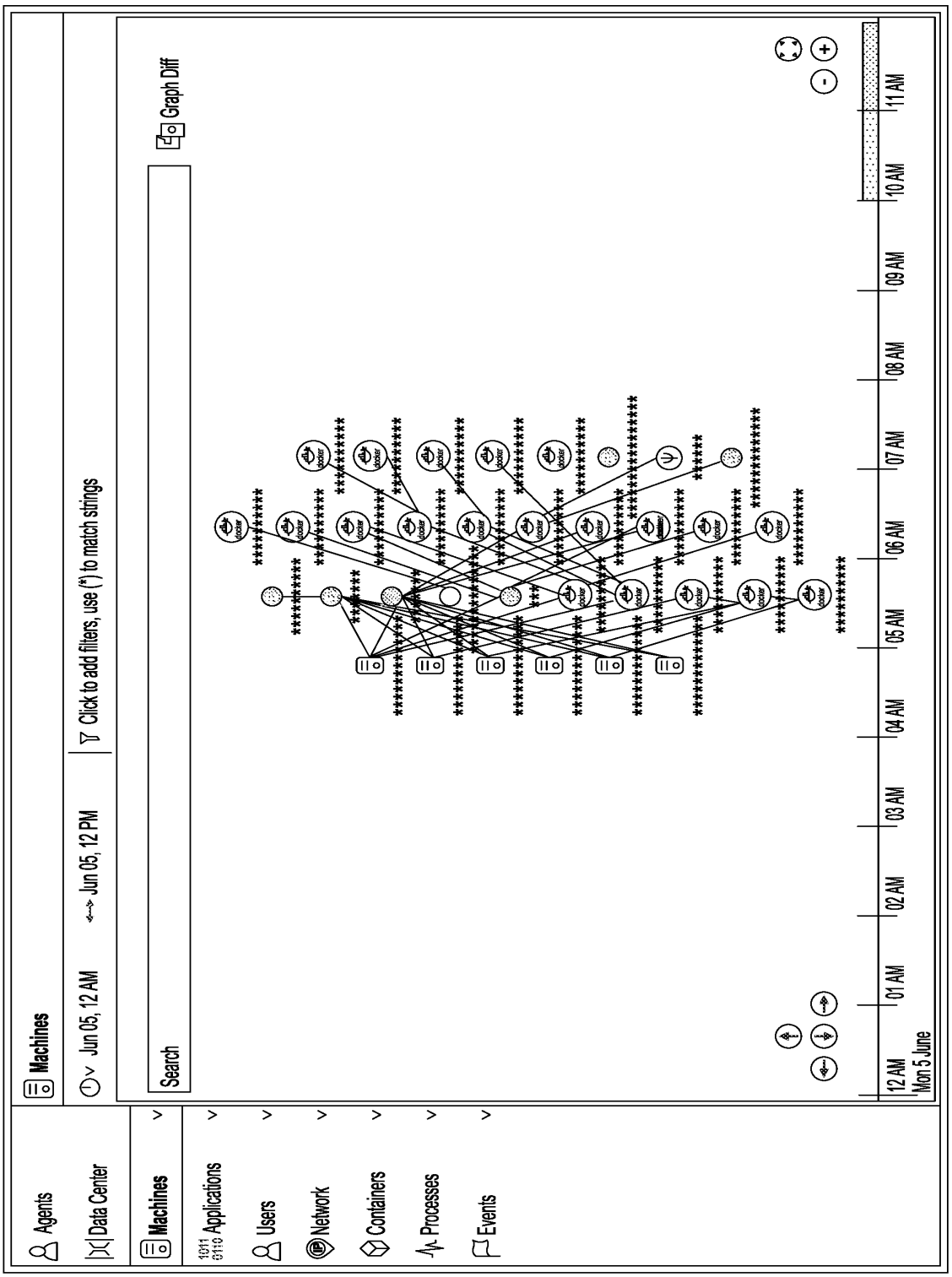

Agents
Data Center
Machines
Applications
Users
Network
Containers
Processes
Events
Machines
Jun 05, 12 AM
Jun 05, 12 PM
Click to add filters, use (*) to match strings
Search
Graph Diff
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 20

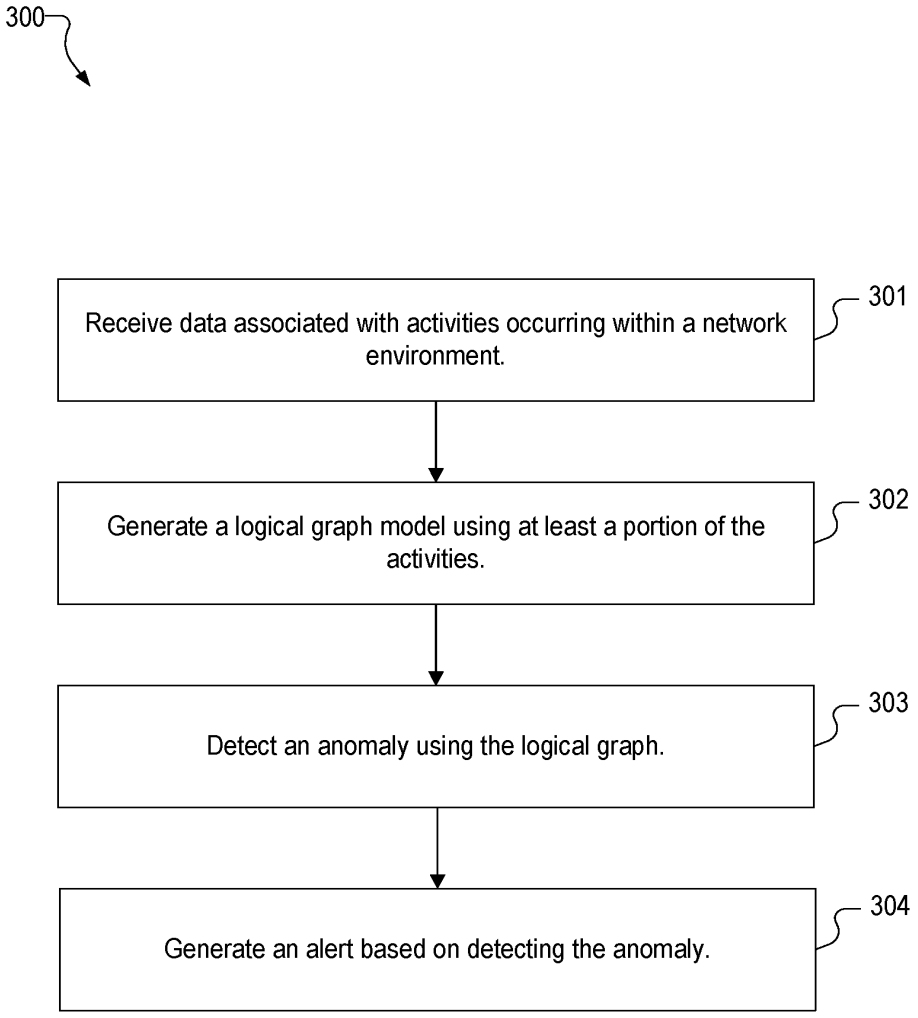

300
Receive data associated with activities occurring within a network environment.
301
Generate a logical graph model using at least a portion of the activities.
302
Detect an anomaly using the logical graph.
303
Generate an alert based on detecting the anomaly.
304

Fig. 3A

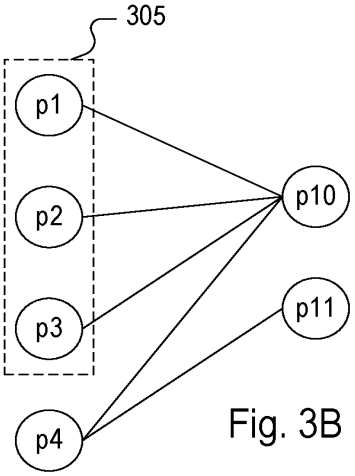


Fig. 3B

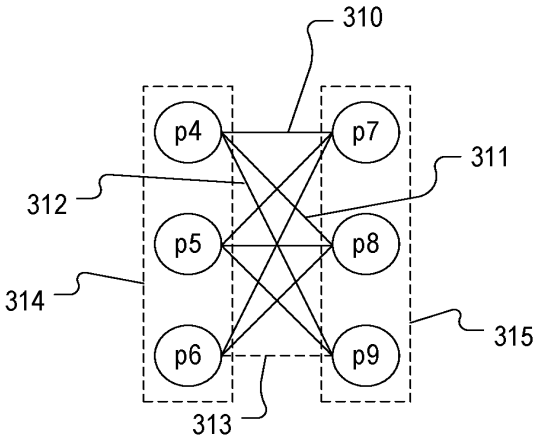


Fig. 3C

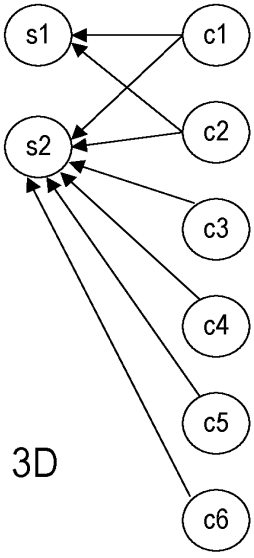


Fig. 3D

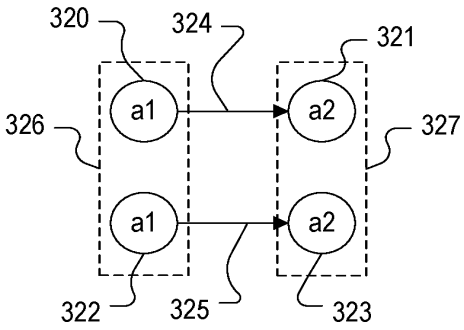


Fig. 3E

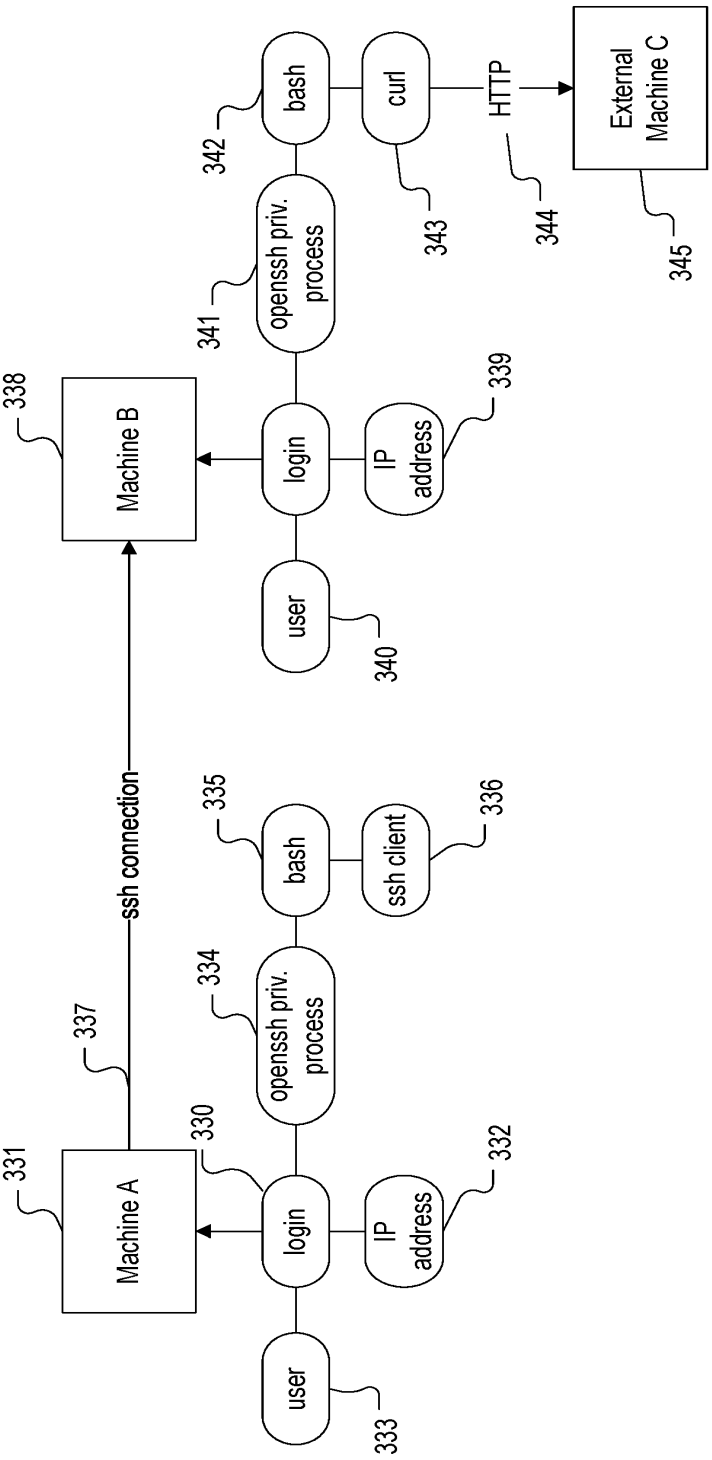

Machine A
331
user
333
login
330
IP address
332
openssh priv. process
334
bash
335
ssh client
336
ssh connection
337
Machine B
338
user
340
login
IP address
339
openssh priv. process
341
bash
342
curl
343
HTTP
344
External Machine C
345

Fig. 3F

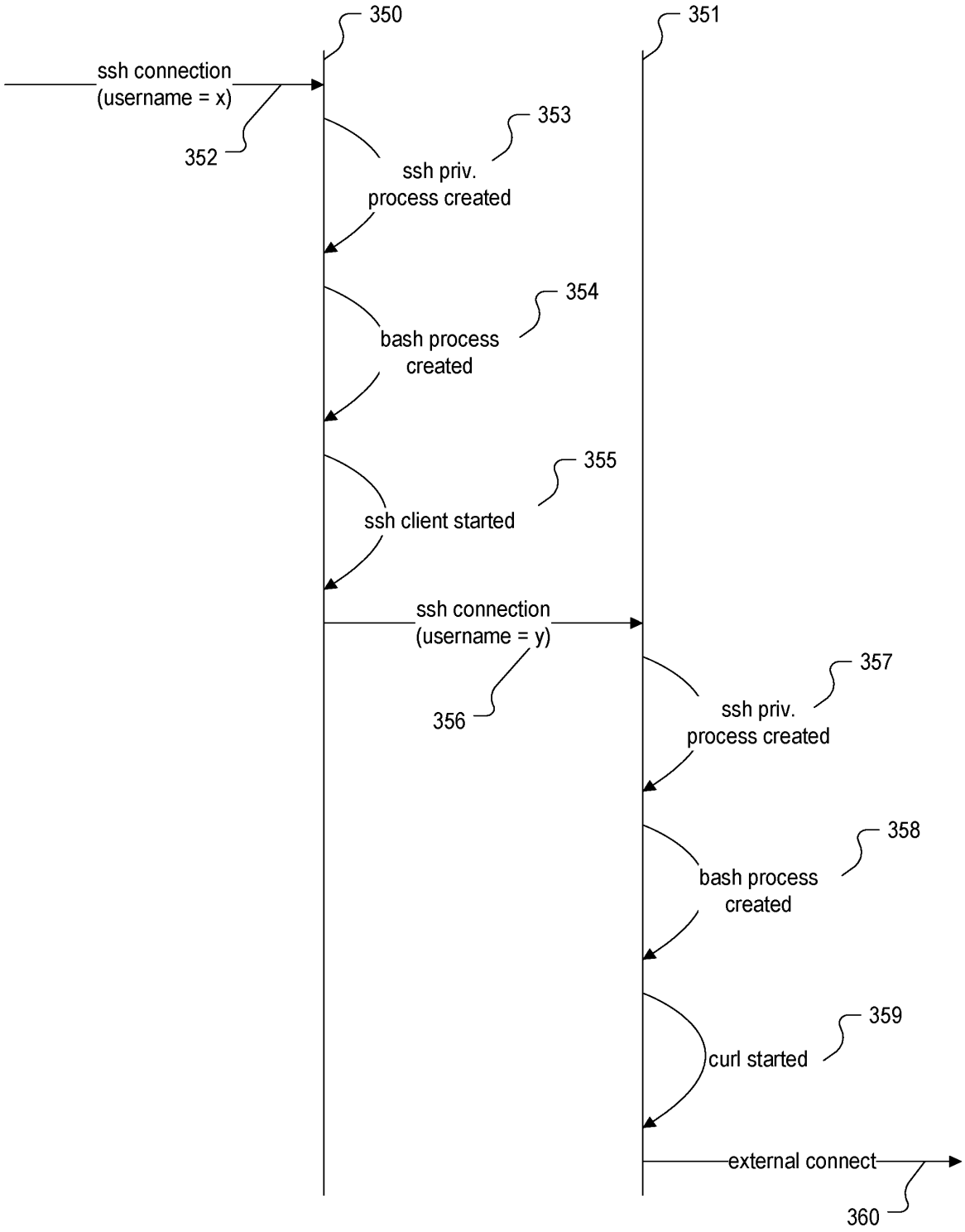

350
351
ssh connection
(username = x)
352
353
ssh priv.
process created
354
bash process
created
355
ssh client started
ssh connection
(username = y)
356
357
ssh priv.
process created
358
bash process
created
359
curl started
external connect
360

Fig. 3G

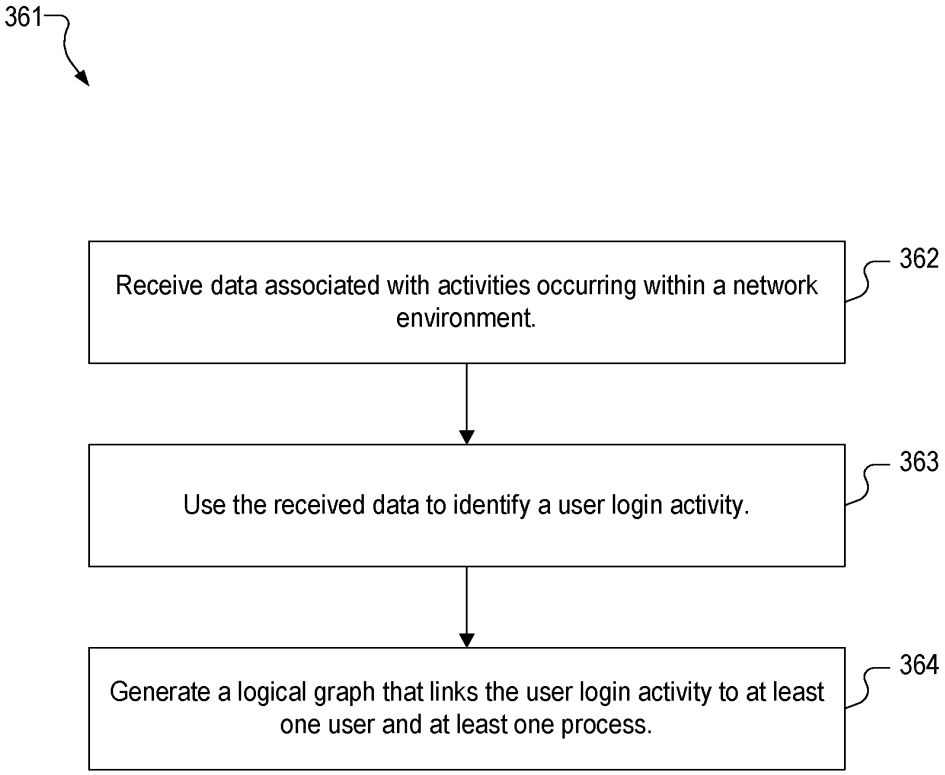

361
Receive data associated with activities occurring within a network environment.
362
Use the received data to identify a user login activity.
363
Generate a logical graph that links the user login activity to at least one user and at least one process.
364

Fig. 3H

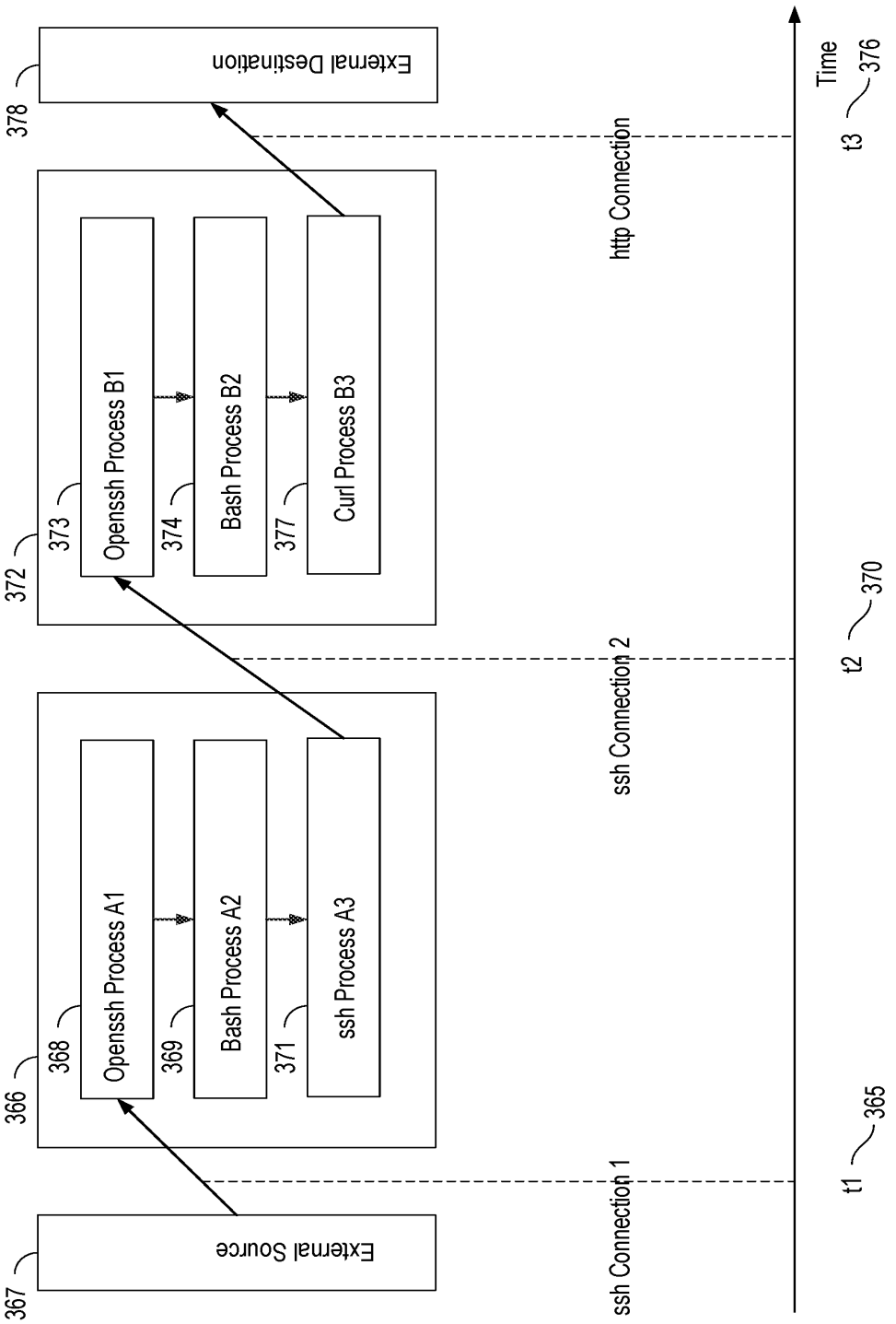

External Source
367
ssh Connection 1
t1
365
366
368
Openssh Process A1
369
Bash Process A2
371
ssh Process A3
ssh Connection 2
t2
370
372
373
Openssh Process B1
374
Bash Process B2
377
Curl Process B3
http Connection
t3
Time
376
378
External Destination

Fig. 3I

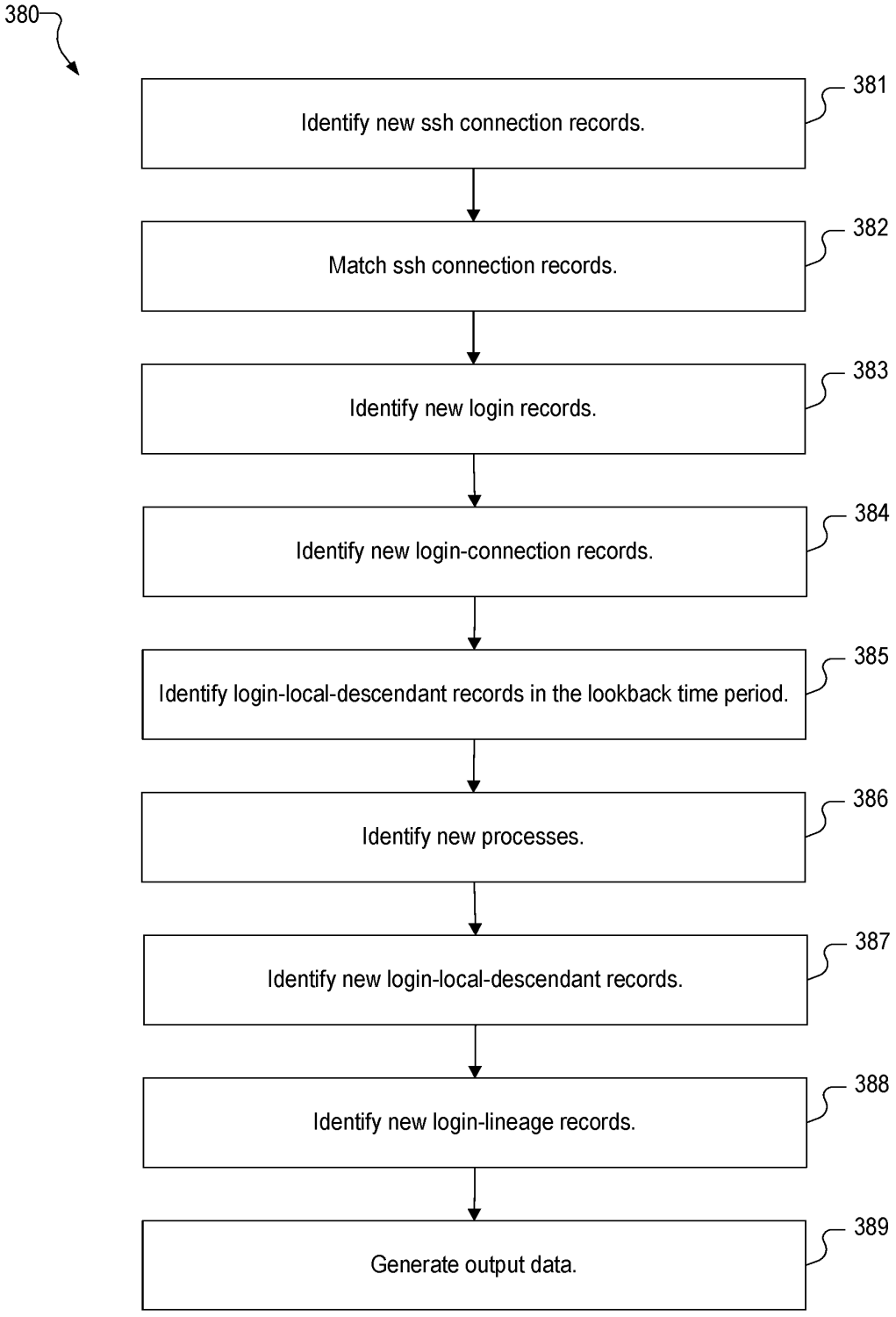

380
Identify new ssh connection records.
381
Match ssh connection records.
382
Identify new login records.
383
Identify new login-connection records.
384
Identify login-local-descendant records in the lookback time period.
385
Identify new processes.
386
Identify new login-local-descendant records.
387
Identify new login-lineage records.
388
Generate output data.
389

Fig. 3J

MID	start_time	PID_hash	src_IP_addr	src_port	dst_IP_addr	dst_port	prot	dir
A	t1	A1	1.1.1.10	10000	2.2.2.20	22	TCP	Incoming
A	t2	A3	2.2.2.20	10001	2.2.2.21	22	TCP	Outgoing
B	t2	B1	2.2.2.20	10001	2.2.2.21	22	TCP	Incoming

390

Fig. 3K

391

src_MID	src_PID_hash	dst_MID	dst_PID_hash	dst_start_time	src_IP_addr	src_port	dst_IP_addr	dst_port
null	null	A	A1	t1	1.1.1.10	10000	2.2.2.20	22
A	A3	B	B1	t2	2.2.2.20	10001	2.2.2.21	22

Fig. 3L

MID	login_time	sshd_PID_hash
A	t1	A1
B	t2	B1

Fig. 3M

MID	sshd_PID_hash	login_time	login_username	src_IP_addr	src_port	dst_IP_addr	dst_port
A	A1	t1	X	1.1.1.10	10000	2.2.2.20	22
B	B1	t2	Y	2.2.2.20	10001	2.2.2.21	22

Fig. 3N

MID	start_time	PID_hash	exe_path	parent_PID_hash
A	t1	A1	/usr/sbin/sshd	A0
A	t1	A2	/bin/bash	A1
A	t2	A3	/usr/bin/ssh	A2
B	t2	B1	/usr/sbin/sshd	B0
B	t2	B2	/bin/bash	B1
B	t3	B3	/usr/bin/curl	B2

Fig. 3O

MID	sshd_PID_hash	PID_hash
A	A1	A1
A	A1	A2
A	A1	A3
B	B1	B1
B	B1	B2
B	B1	B3

Fig. 3P

parent_MID	parent_sshd_PID_hash	child_MID	origin_sshd_PID_hash
A	A1	B	B1

Fig. 3Q

MID	sshd_PID_hash	parent_MID	parent_sshd_PID_hash	origin_MID	origin_sshd_PID_hash
A	A1	null	null	A	A1
B	B1	A	A1	A	A1

Fig. 3R

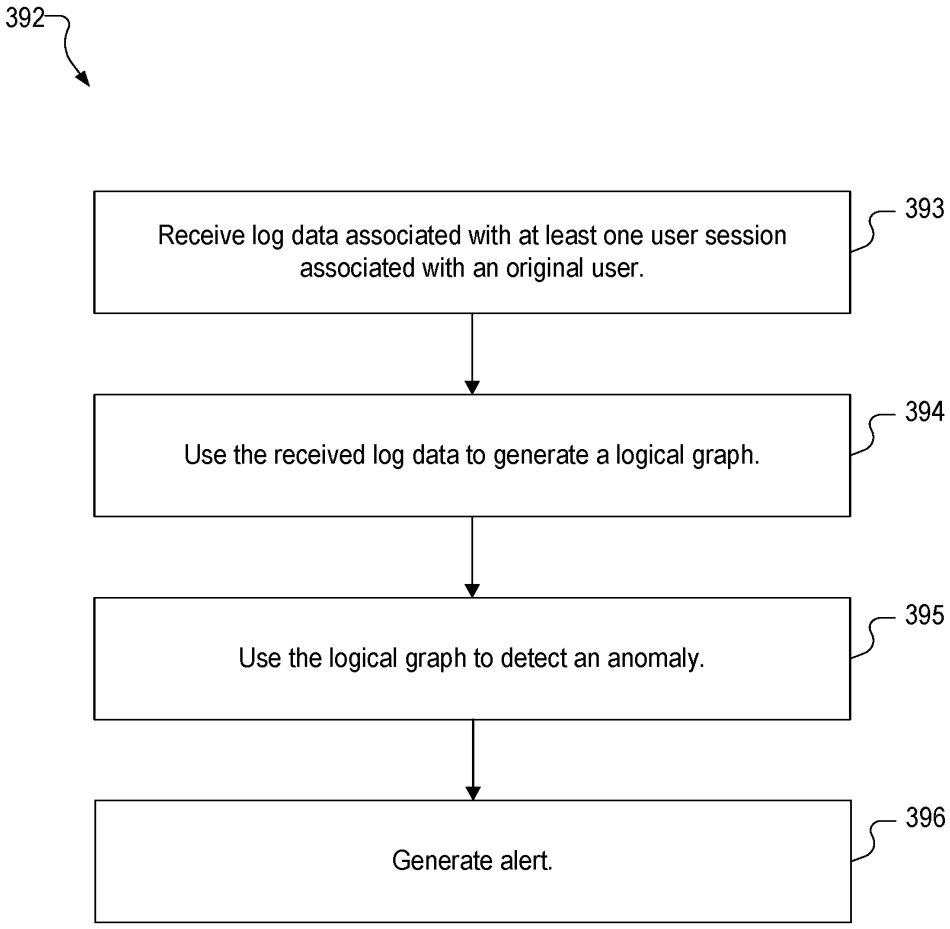

392
Receive log data associated with at least one user session associated with an original user.
393
Use the received log data to generate a logical graph.
394
Use the logical graph to detect an anomaly.
395
Generate alert.
396

Fig. 3S

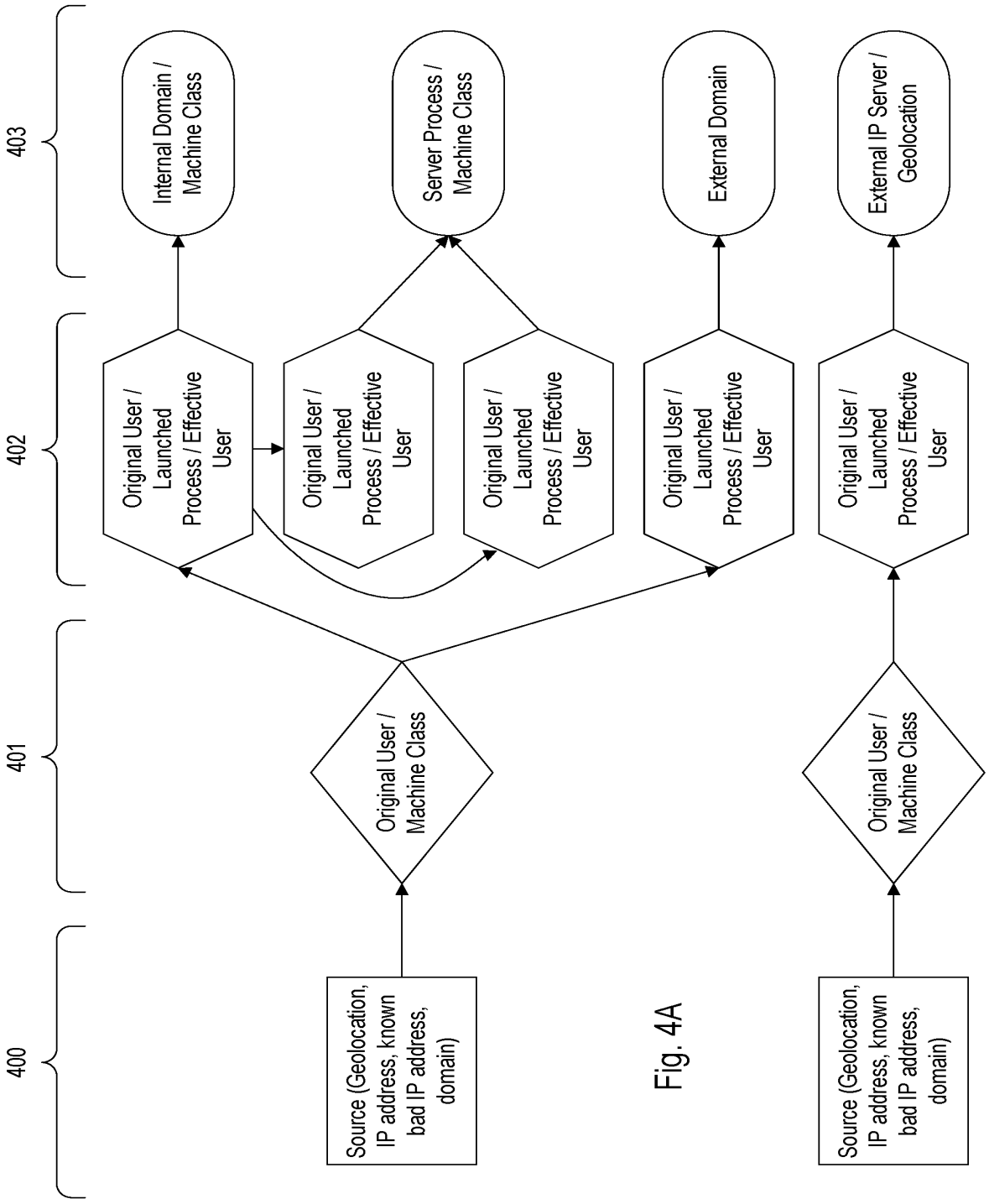

400
401
402
403
Source (Geolocation, IP address, known bad IP address, domain)
Original User / Machine Class
Original User / Launched Process / Effective User
Original User / Launched Process / Effective User
Original User / Launched Process / Effective User
Internal Domain / Machine Class
Server Process / Machine Class
Source (Geolocation, IP address, known bad IP address, domain)
Original User / Machine Class
Original User / Launched Process / Effective User
External Domain
Original User / Launched Process / Effective User
External IP Server / Geolocation

Fig. 4A

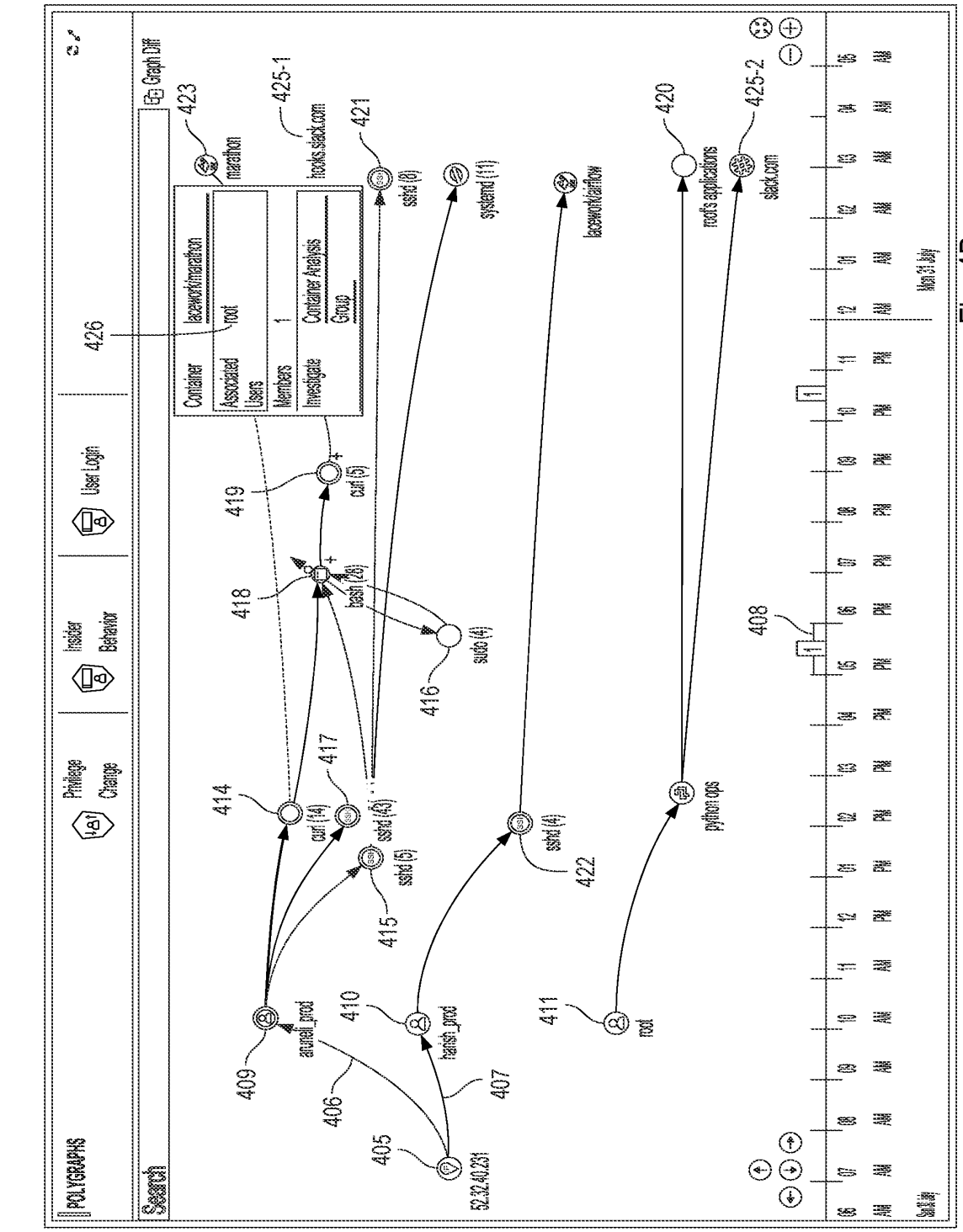

POLYGRAPHS
Search
Graph Diff
Privilege Change
Insider Behavior
User Login
426
Container
lacework/marathon
Associated Users
root
Members
1
Investigate
Container Analysis Group
423
marathon
425-1
hooks.slack.com
421
sshd (8)
systemd (11)
lacework/airflow
420
node applications
425-2
slack.com
419
curl (5)
418
bash (26)
sudo (4)
416
414
curl (14)
417
sshd (43)
sshd (5)
415
sshd (4)
422
python ops
408
409
anaheil_prod
406
405
52.32.40.231
410
hanish_prod
407
411
root
Mon 31 July

Fig. 4B

404

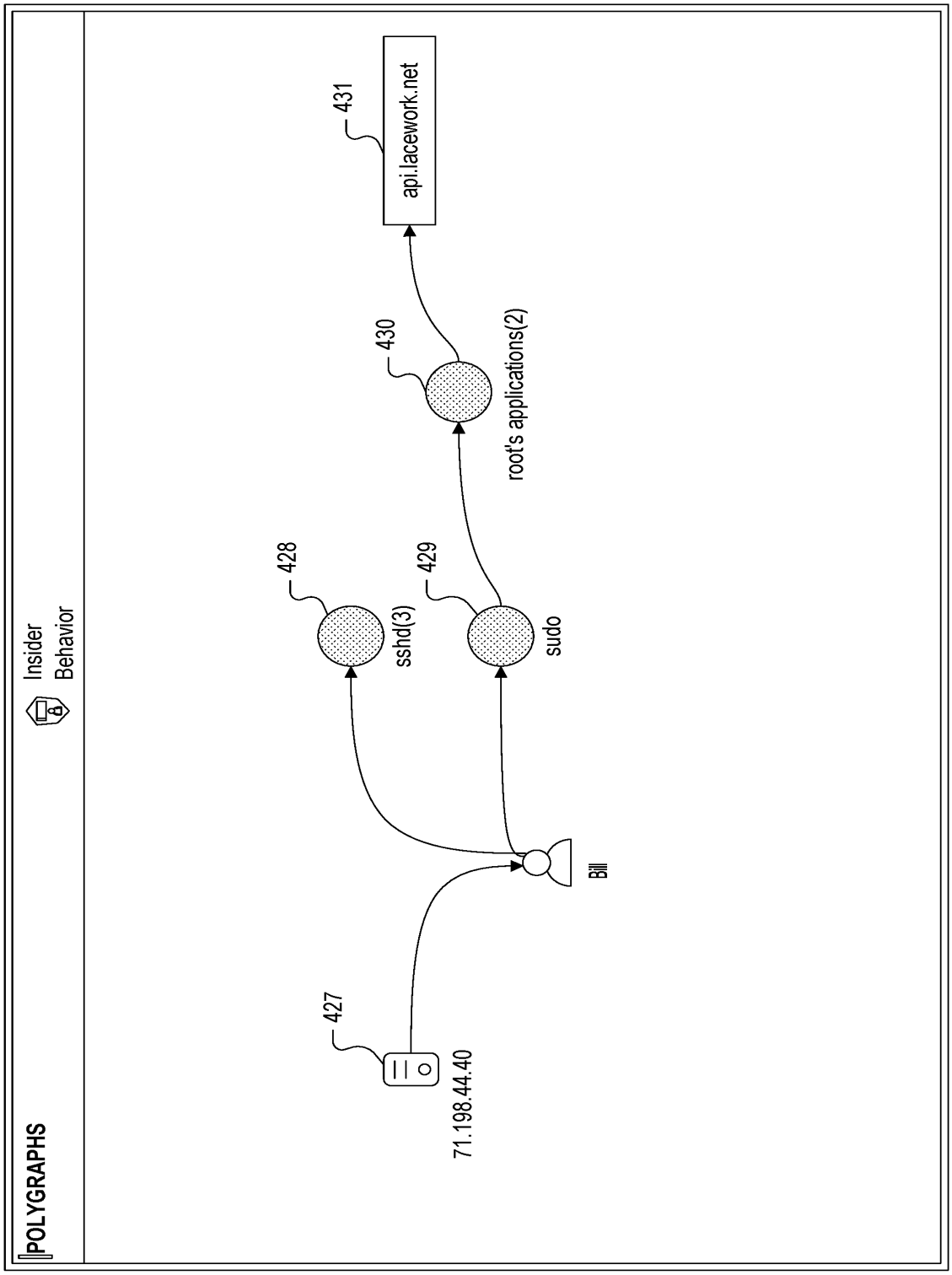

POLYGRAPHS
Insider Behavior
71.198.44.40
427
Bill
sshd(3)
428
sudo
429
root's applications(2)
430
api.lacework.net
431

Fig. 4C

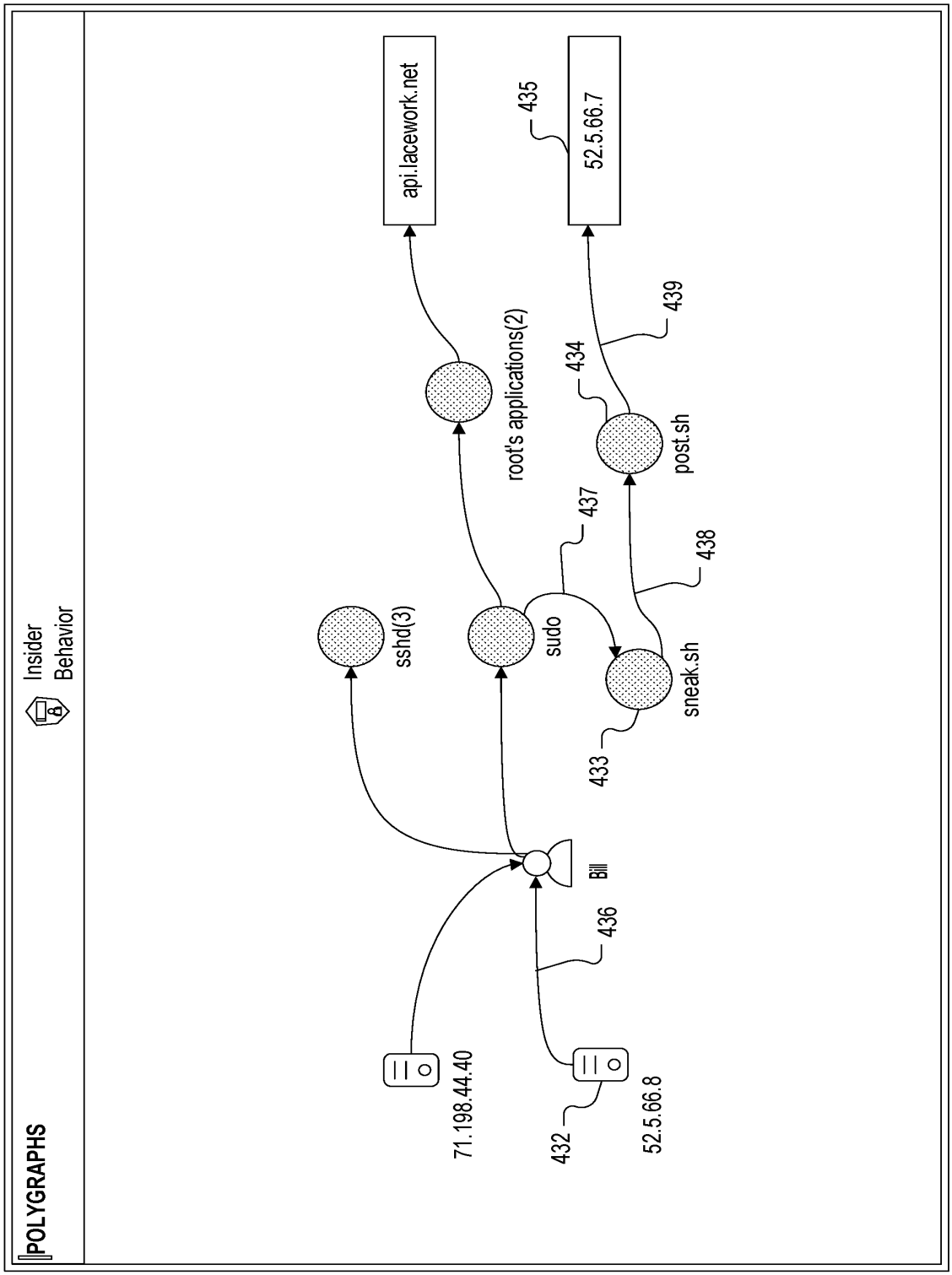

POLYGRAPHS
Insider Behavior
71.198.44.40
52.5.66.8
Bill
sshd(3)
sudo
root's applications(2)
sneak.sh
post.sh
api.lacework.net
52.5.66.7
432
433
434
435
436
437
438
439

Fig. 4D

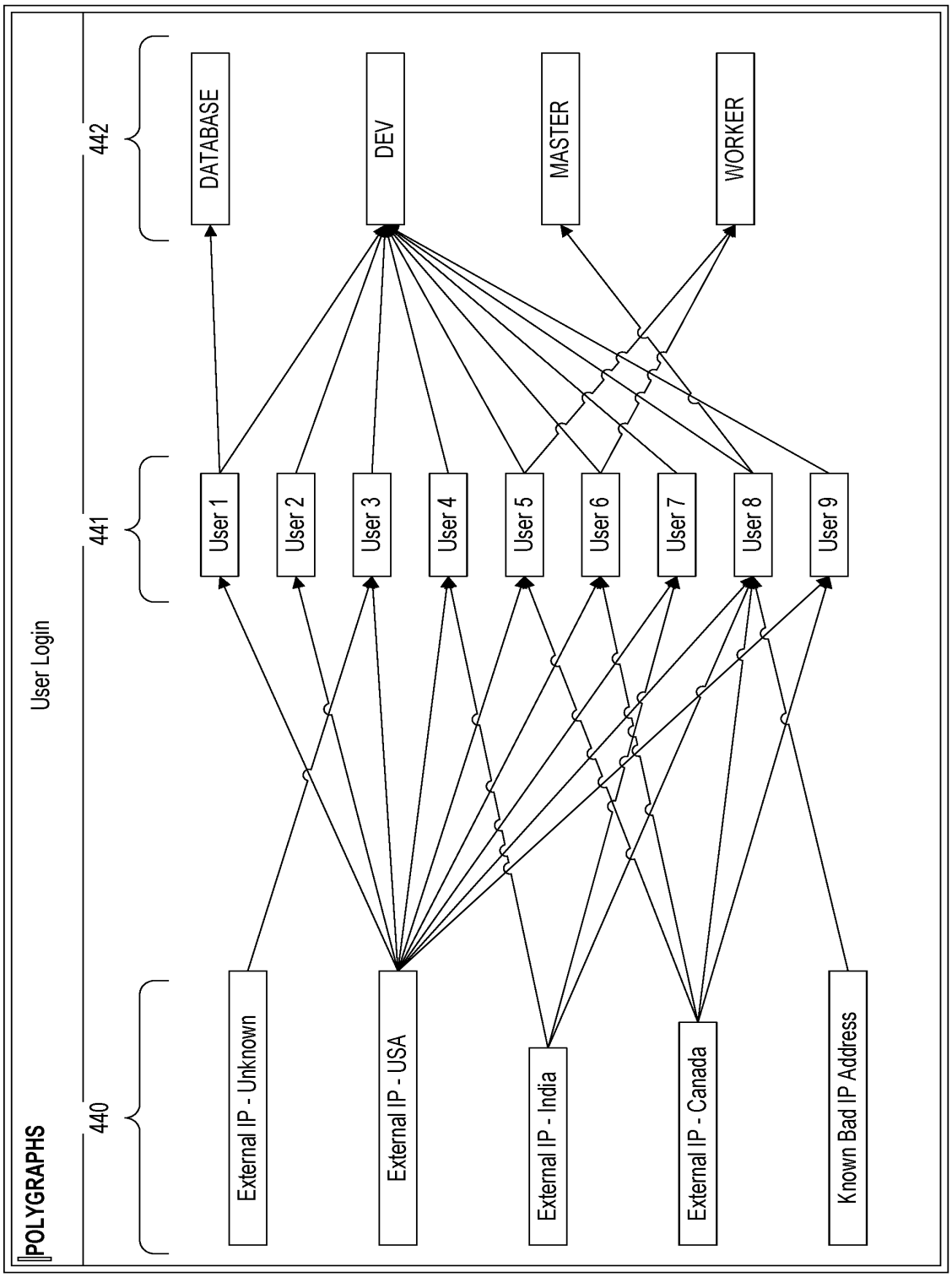

POLYGRAPHS
User Login
440
441
442
External IP - Unknown
External IP - USA
External IP - India
External IP - Canada
Known Bad IP Address
User 1
User 2
User 3
User 4
User 5
User 6
User 7
User 8
User 9
DATABASE
DEV
MASTER
WORKER

Fig. 4E

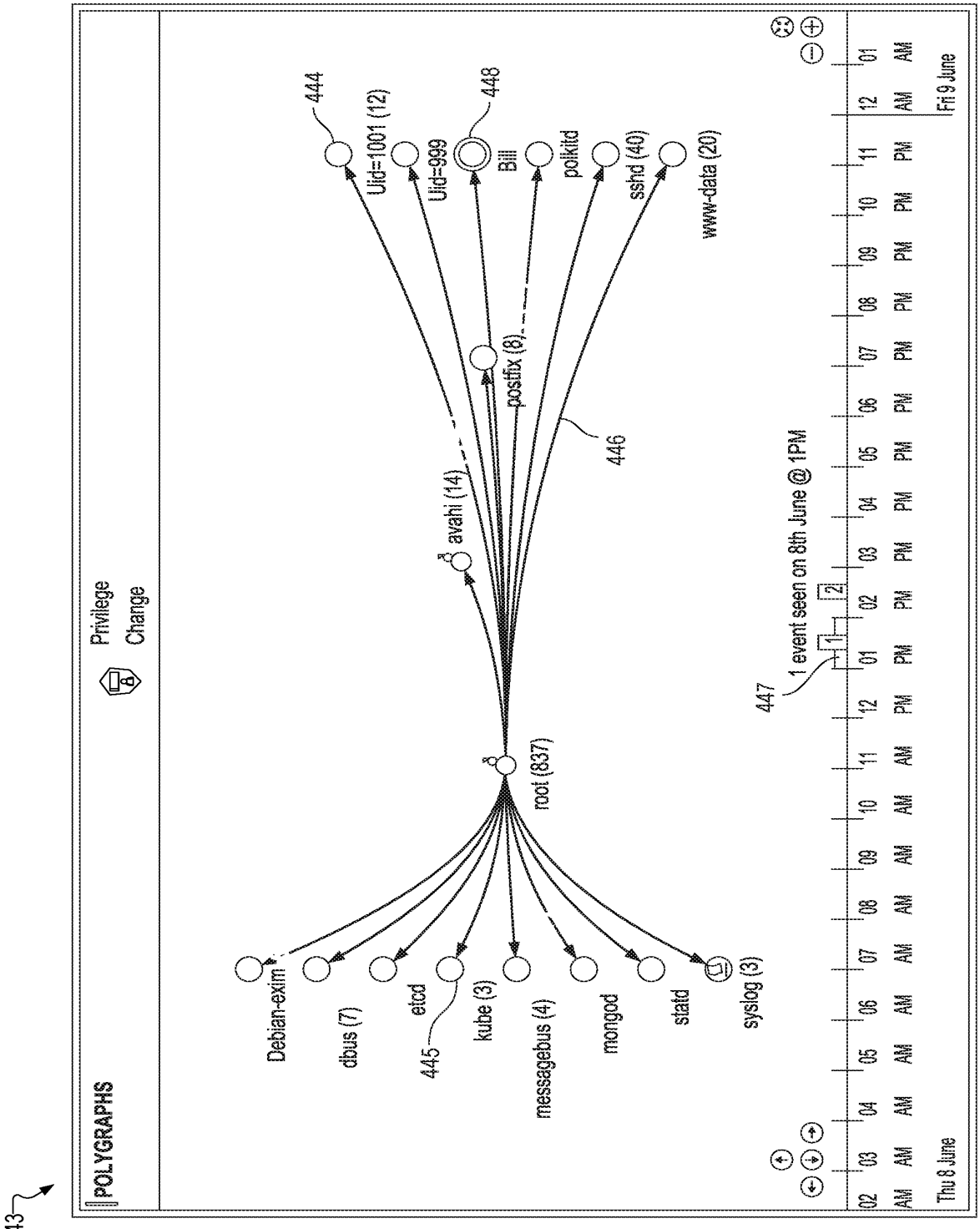

443
POLYGRAPHS
Privilege
Change
444
Uid=1001 (12)
Uid=999
448
Bill
polkitd
sshd (40)
www-data (20)
posfix (8)
avahi (14)
446
root (837)
Debian-exim
dbus (7)
etcd
445
kube (3)
messagebus (4)
mongod
statd
syslog (3)
447
1 event seen on 8th June @ 1PM
Thu 8 June
Fri 9 June

Fig. 4F

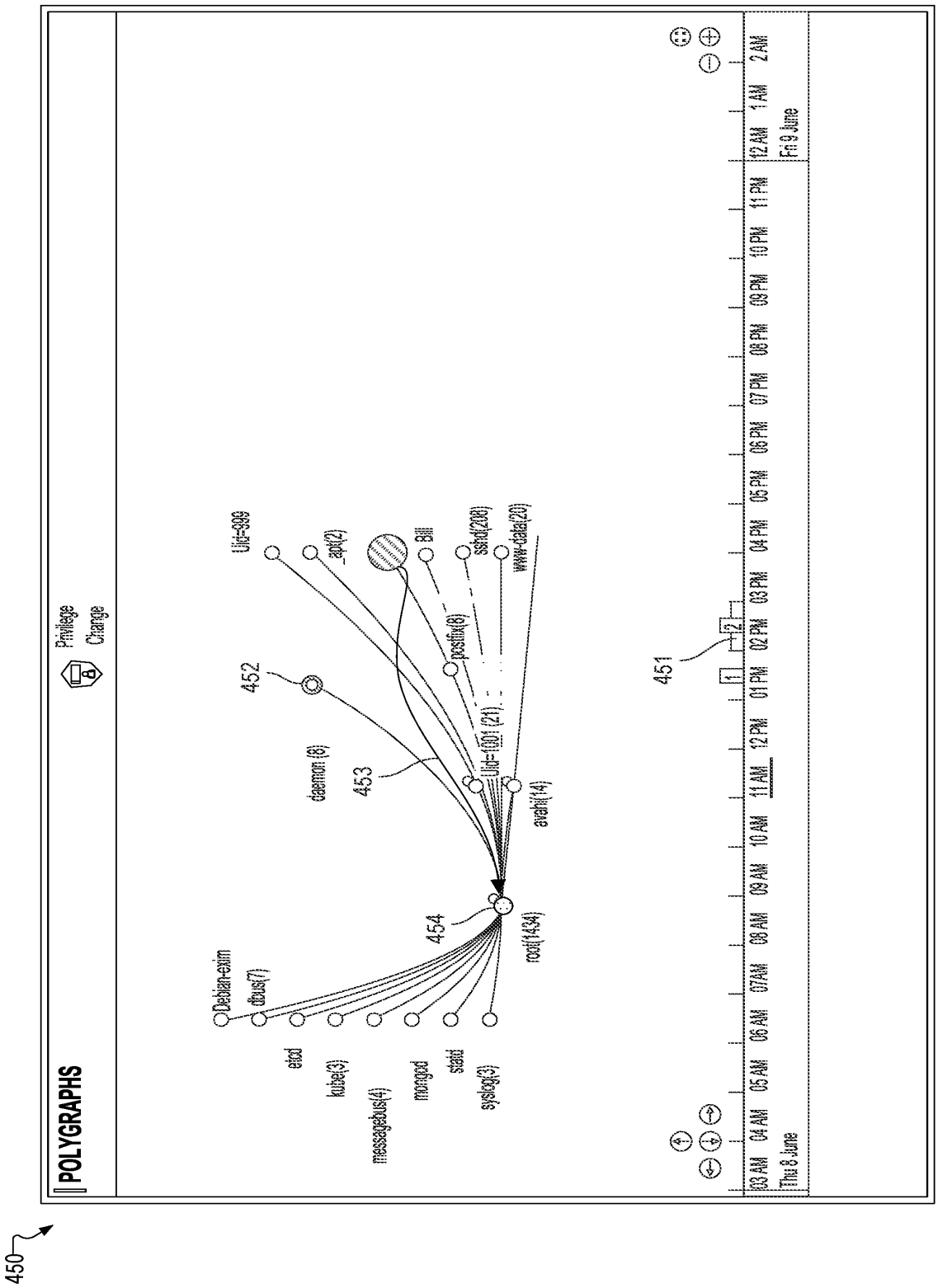

450
POLYGRAPHS
Privilege Change
Debian-exim
dbus(7)
etod
kube(3)
messagebus(4)
mongod
statd
syslog(3)
454
root(1434)
452
daemon (8)
453
Uid=999
_apt(2)
Bill
postfix(8)
Uid=1001 (21)
sshd(208)
www-data(20)
avahi(14)
451
12
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
07 PM
08 PM
09 PM
10 PM
11 PM
12 AM
1 AM
2 AM
Thu 8 June
Fri 9 June

Fig. 4G

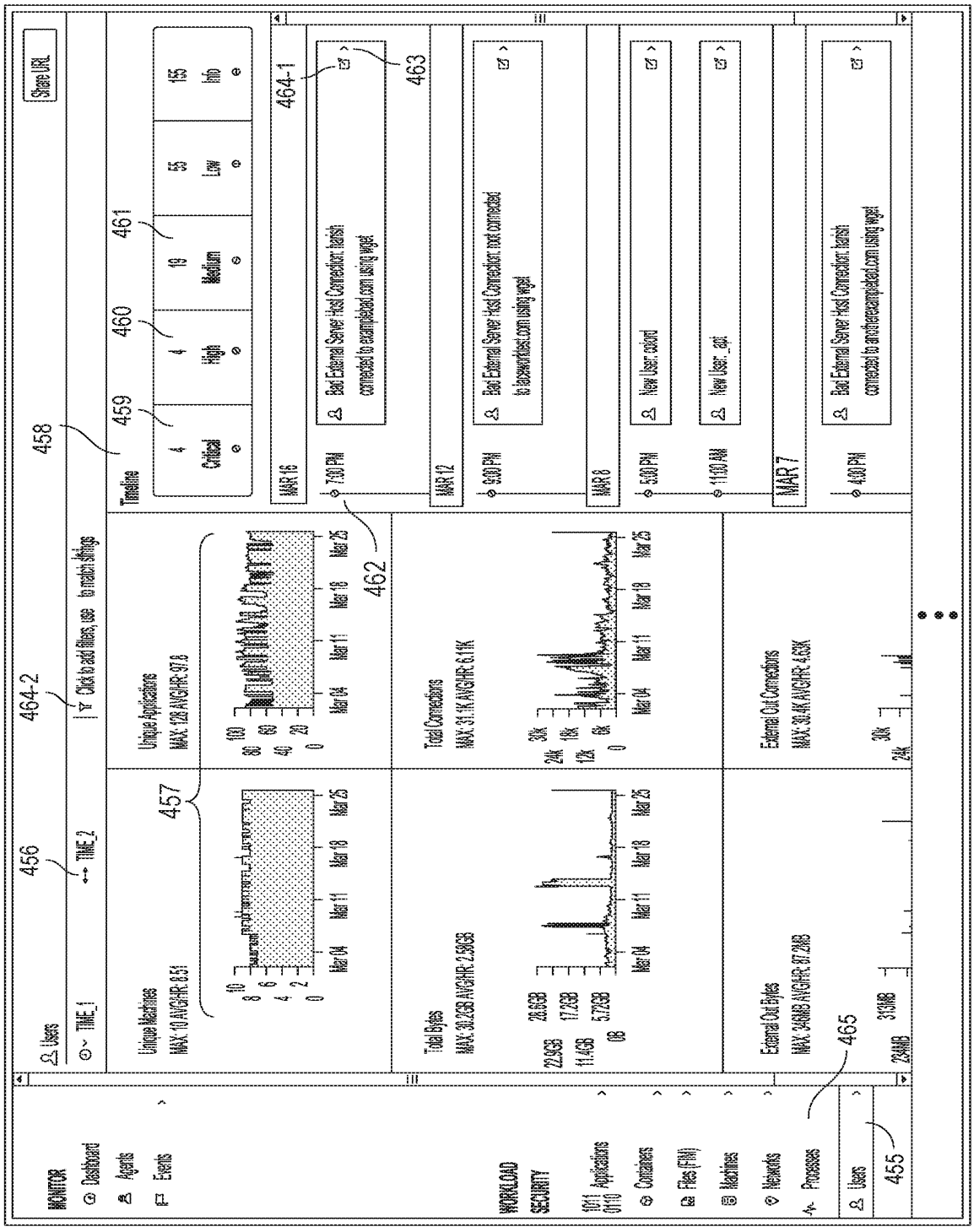

MONITOR
Dashboard
Agents
Events
WORKLOAD SECURITY
1911 Applications
0110
Containers
Files (FIM)
Machines
Networks
Processes
Users
455
456
TIME_1
TIME_2
Users
Click to add filters, use to match Strings
Share URL
458
464-2
457
Unique Machines
MAX: 10 AVG/HR: 0.51
Unique Applications
MAX: 128 AVG/HR: 97.6
462
Total Bytes
MAX: 31.23B AVG/HR: 2.86GB
Total Connections
MAX: 31.1K AVG/HR: 6.11K
External Out Bytes
MAX: 24MB AVG/HR: 87.2MB
External Out Connections
MAX: 30.4K AVG/HR: 4.63K
465
Timeline
459
4
Critical
460
4
High
461
19
Medium
55
Low
155
Info
464-1
463
MAR 16
7:00 PM
Bad External Server Host Connection: Ikarish connected to examplebad.com using wget
MAR 12
9:00 PM
Bad External Server Host Connection: root connected to badworldtest.com using wget
MAR 8
5:00 PM
New User: sciord
11:00 AM
New User: _apt
MAR 7
4:00 PM
Bad External Server Host Connection: Ikarish connected to anotherexampletest.com using wget

Fig. 4H

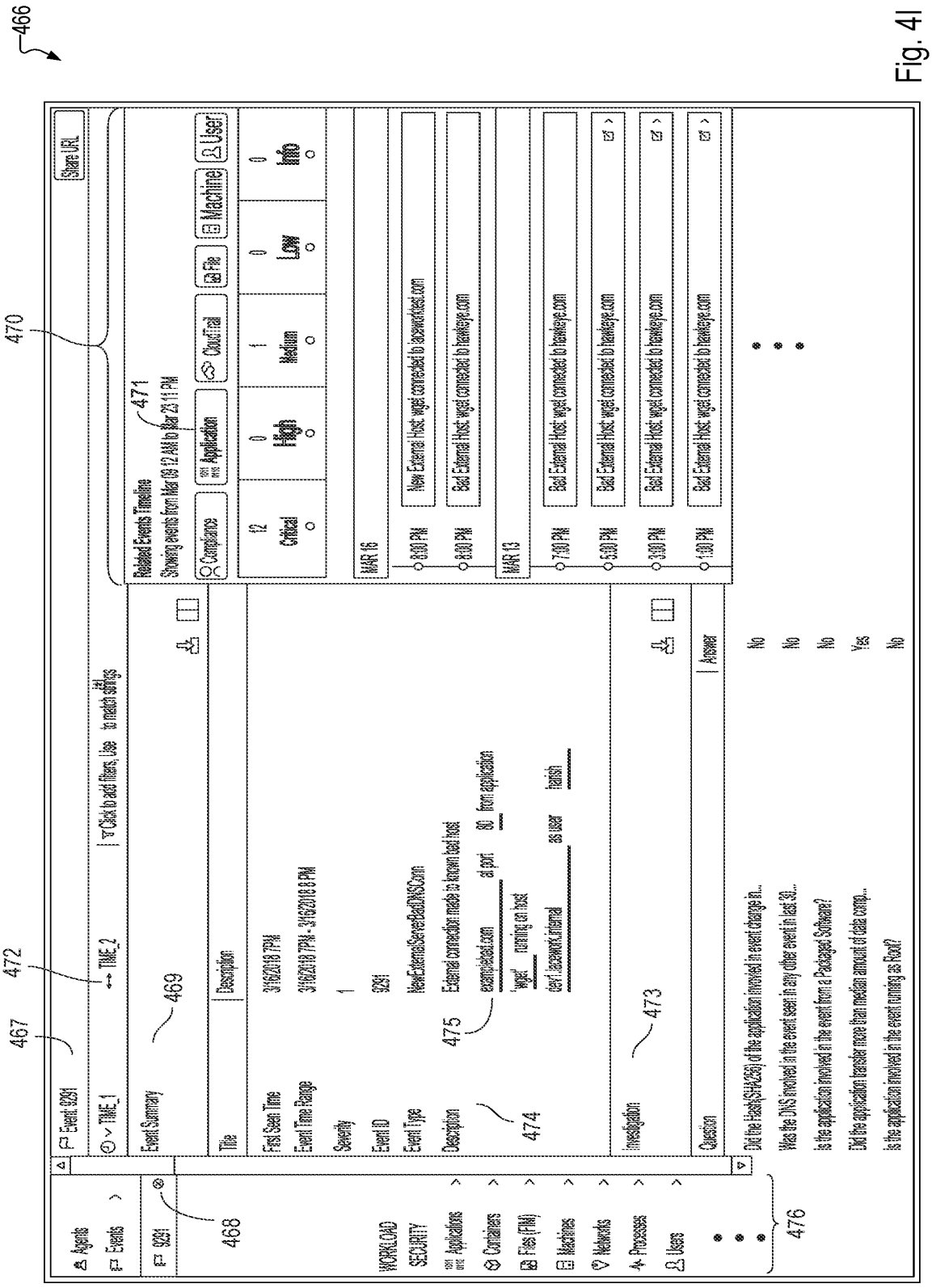

466
470
472
467
469
471
468
475
474
473
476
Agents
Events
9291
Event 9291
TIME_1
TIME_2
Click to add filters, Use to match strings
Share URL
Event Summary
Related Events Timeline
Showing events from Mar 09 12 AM to Mar 23 11 PM
Compliance
Application
CloudTrail
File
Machine
User
12 Critical
0 High
1 Medium
0 Low
0 Info
Title
Description
First Seen Time
Event Time Range
Severity
Event ID
Event Type
Description
3/16/2018 7PM
3/16/2018 7PM - 3/16/2018 8 PM
1
9291
NewExternalServerBadDNSCom
External connection made to known bad host
examplebad.com at port 80 from application
'wget' running on host
doe\ lacoewck.internal as user hanish
MAR 16
MAR 13
8:00 PM
New External Host: wget connected to badexample.com
7:00 PM
6:00 PM
5:00 PM
4:00 PM
Bad External Host: wget connected to hawkeye.com
Investigation
Question
Answer
Did the Hash(SHA256) of the application involved in event change in...
Was the DNS involved in the event seen in any other event in last 30...
Is the application involved in the event from a Privileged Software?
Did the application transfer more than median amount of data comp...
Is the application involved in the event running as Root?
No
No
No
Yes
No

Fig. 4I

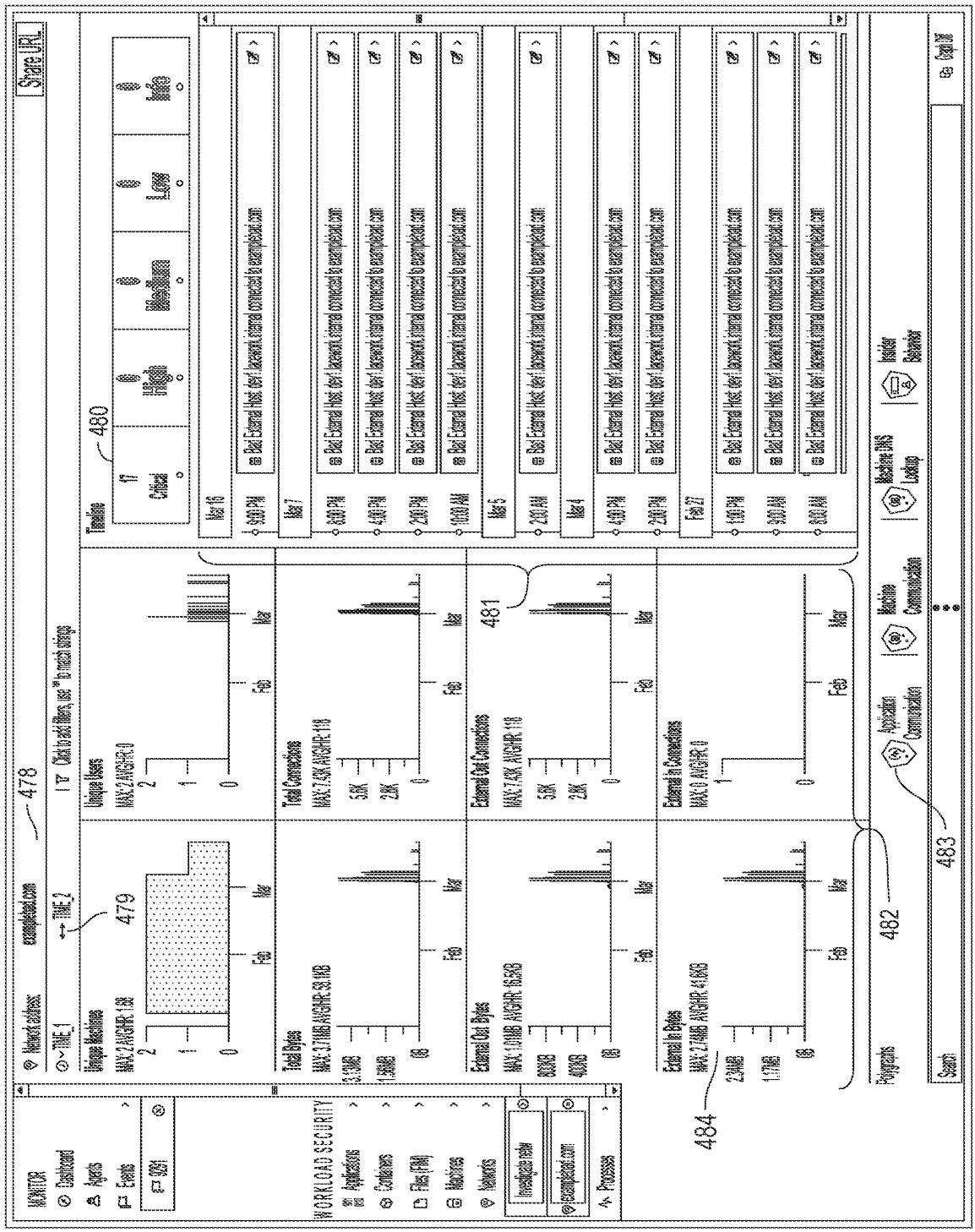

477
478
479
480
481
482
483
484
Share URL
MONITOR
Dashboard
Agents
Events
WORKLOAD SECURITY
Applications
Containers
Files (FIM)
Machines
Networks
Processes
Network address
examplebad.com
TIME_1
TIME_2
Click to add filters, use * to match strings
Unique Machines
Unique Users
Total Bytes
Total Connections
External Out Bytes
External Out Connections
External In Bytes
External In Connections
Timeline
17 Critical
0 High
0 Medium
0 Low
0 Info
Bad External Host: dest. descend. internal connected to examplebad.com
Polygraphs
Application Communication
Machine Communication
Machine DNS Lookup
Insider Behavior
Search

Fig. 4J

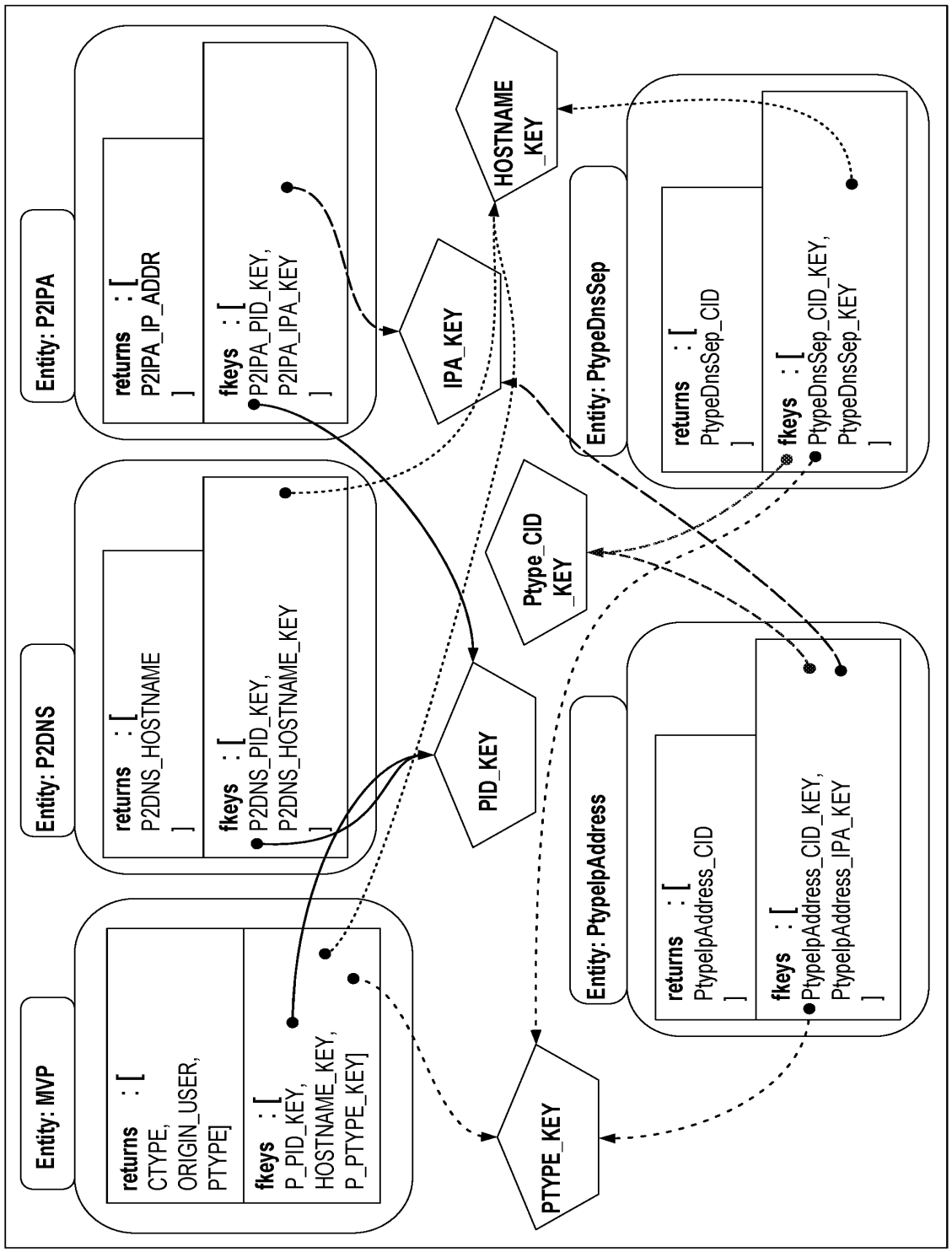

Entity: MVP
returns : [
CTYPE,
ORIGIN_USER,
PTYPE]
fkeys : [
P_PID_KEY,
HOSTNAME_KEY,
P_PTYPE_KEY]
Entity: P2DNS
returns : [
P2DNS_HOSTNAME
]
fkeys : [
P2DNS_PID_KEY,
P2DNS_HOSTNAME_KEY
]
Entity: P2IPA
returns : [
P2IPA_IP_ADDR
]
fkeys : [
P2IPA_PID_KEY,
P2IPA_IPA_KEY
]
Entity: PtypeIpAddress
returns : [
PtypeIpAddress_CID
]
fkeys : [
PtypeIpAddress_CID_KEY,
PtypeIpAddress_IPA_KEY
]
Entity: PtypeDnsSep
returns : [
PtypeDnsSep_CID
]
fkeys : [
PtypeDnsSep_CID_KEY,
PtypeDnsSep_KEY
]
PID_KEY
IPA_KEY
HOSTNAME_KEY
Ptype_CID_KEY
PTYPE_KEY

Fig. 4K

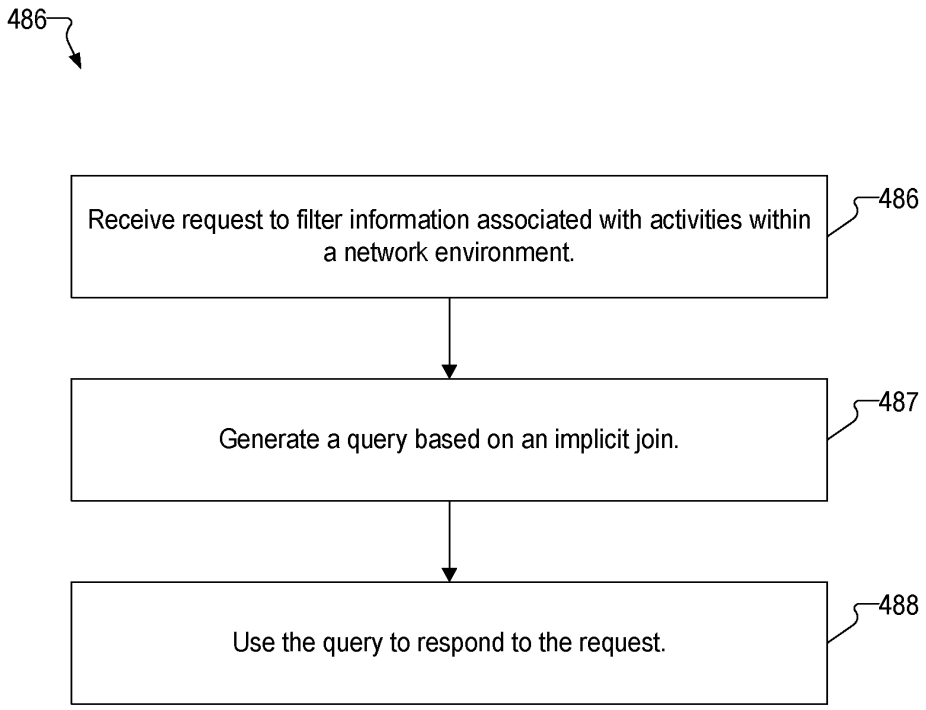

486
Receive request to filter information associated with activities within a network environment.
486
Generate a query based on an implicit join.
487
Use the query to respond to the request.
488

Fig. 4L

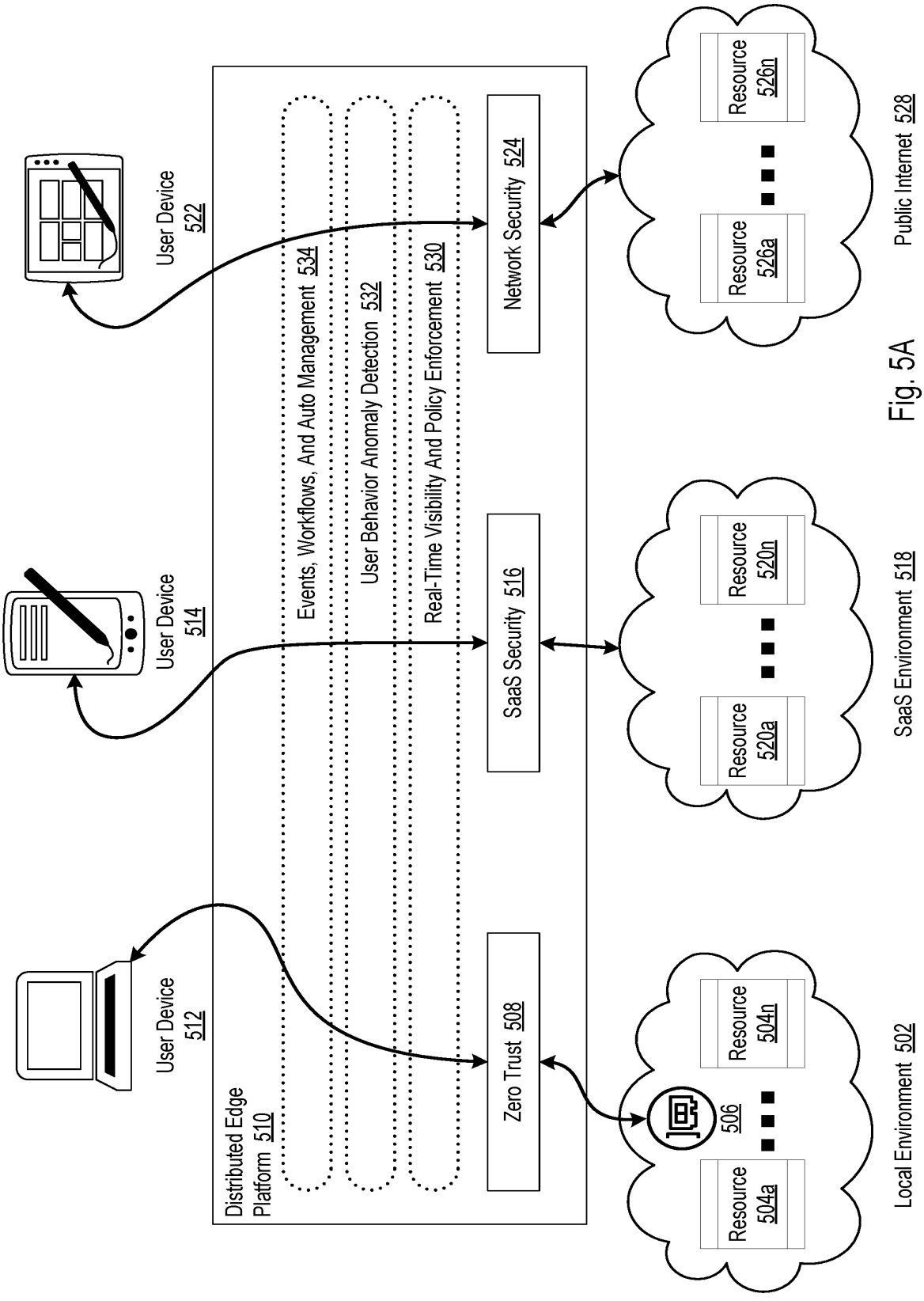

User Device 522
User Device 514
User Device 512
Distributed Edge Platform 510
Events, Workflows, And Auto Management 534
User Behavior Anomaly Detection 532
Real-Time Visibility And Policy Enforcement 530
Network Security 524
SaaS Security 516
Zero Trust 508
506
Resource 504a
Resource 504n
Resource 520a
Resource 520n
Resource 526a
Resource 526n
Local Environment 502
SaaS Environment 518
Public Internet 528

Fig. 5A

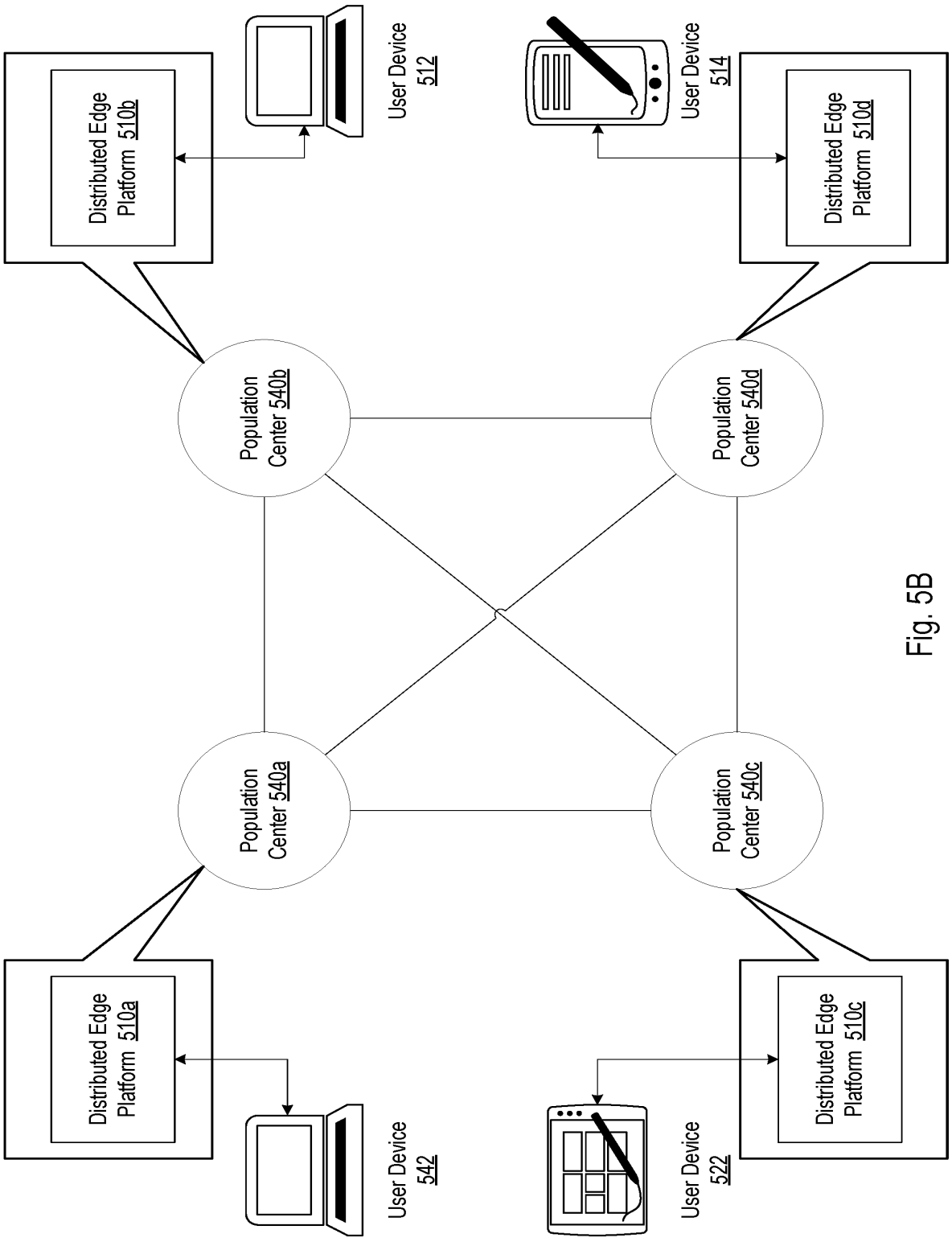

Distributed Edge Platform 510b
User Device 512
User Device 514
Distributed Edge Platform 510d
Population Center 540b
Population Center 540d
Population Center 540a
Population Center 540c
Distributed Edge Platform 510a
User Device 542
User Device 522
Distributed Edge Platform 510c

Fig. 5B

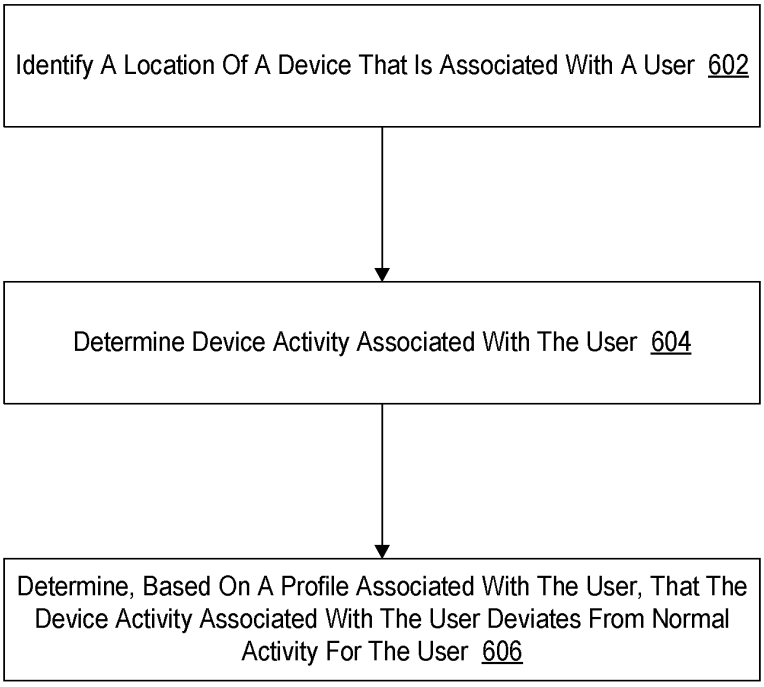

Identify A Location Of A Device That Is Associated With A User 602
Determine Device Activity Associated With The User 604
Determine, Based On A Profile Associated With The User, That The Device Activity Associated With The User Deviates From Normal Activity For The User 606

Fig. 6

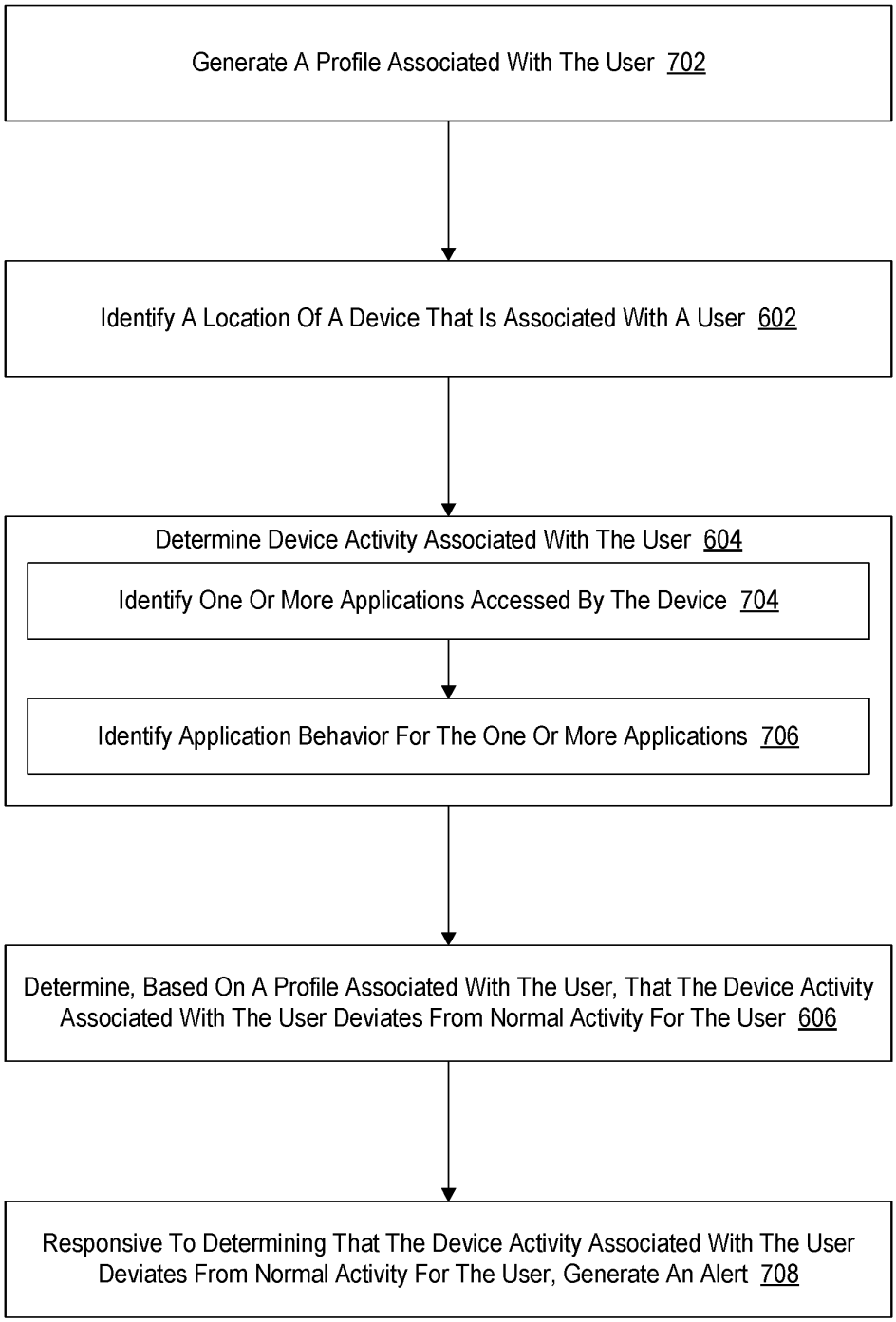

Generate A Profile Associated With The User 702
Identify A Location Of A Device That Is Associated With A User 602
Determine Device Activity Associated With The User 604
Identify One Or More Applications Accessed By The Device 704
Identify Application Behavior For The One Or More Applications 706
Determine, Based On A Profile Associated With The User, That The Device Activity Associated With The User Deviates From Normal Activity For The User 606
Responsive To Determining That The Device Activity Associated With The User Deviates From Normal Activity For The User, Generate An Alert 708

Fig. 7

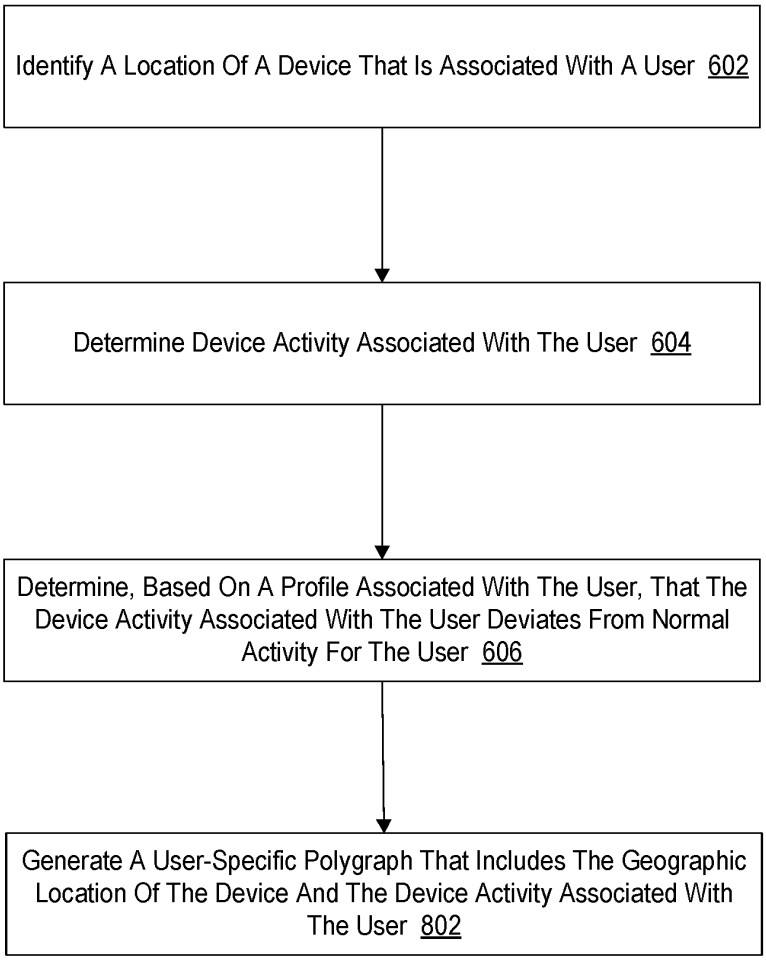

Identify A Location Of A Device That Is Associated With A User 602
Determine Device Activity Associated With The User 604
Determine, Based On A Profile Associated With The User, That The Device Activity Associated With The User Deviates From Normal Activity For The User 606
Generate A User-Specific Polygraph That Includes The Geographic Location Of The Device And The Device Activity Associated With The User 802

Fig. 8

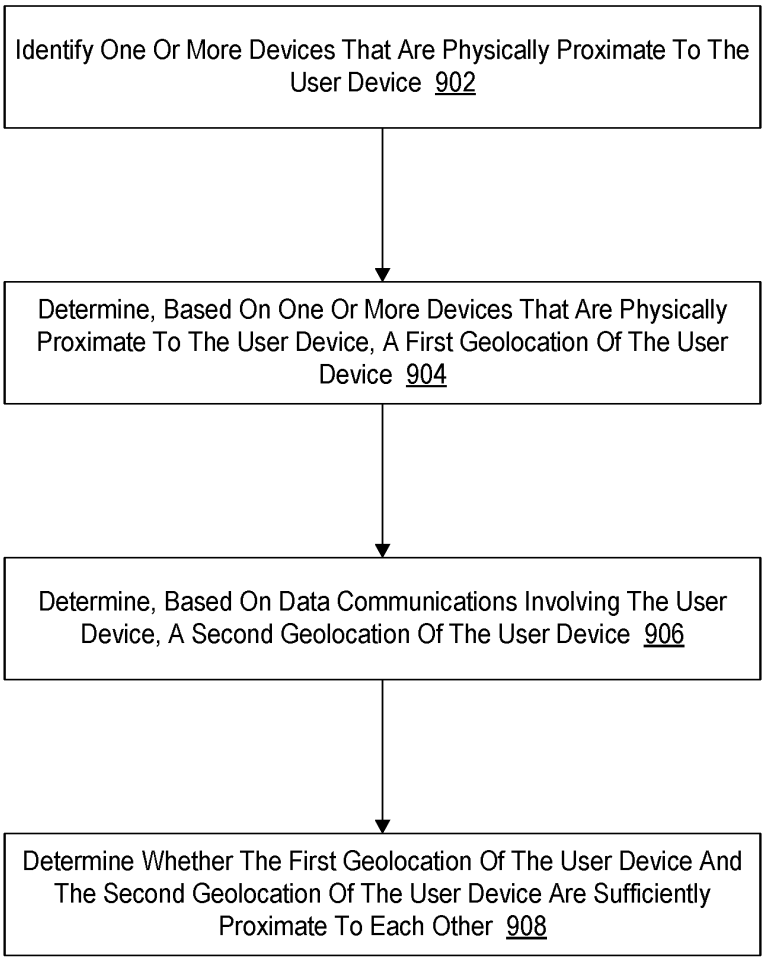

Identify One Or More Devices That Are Physically Proximate To The User Device 902
Determine, Based On One Or More Devices That Are Physically Proximate To The User Device, A First Geolocation Of The User Device 904
Determine, Based On Data Communications Involving The User Device, A Second Geolocation Of The User Device 906
Determine Whether The First Geolocation Of The User Device And The Second Geolocation Of The User Device Are Sufficiently Proximate To Each Other 908

Fig. 9

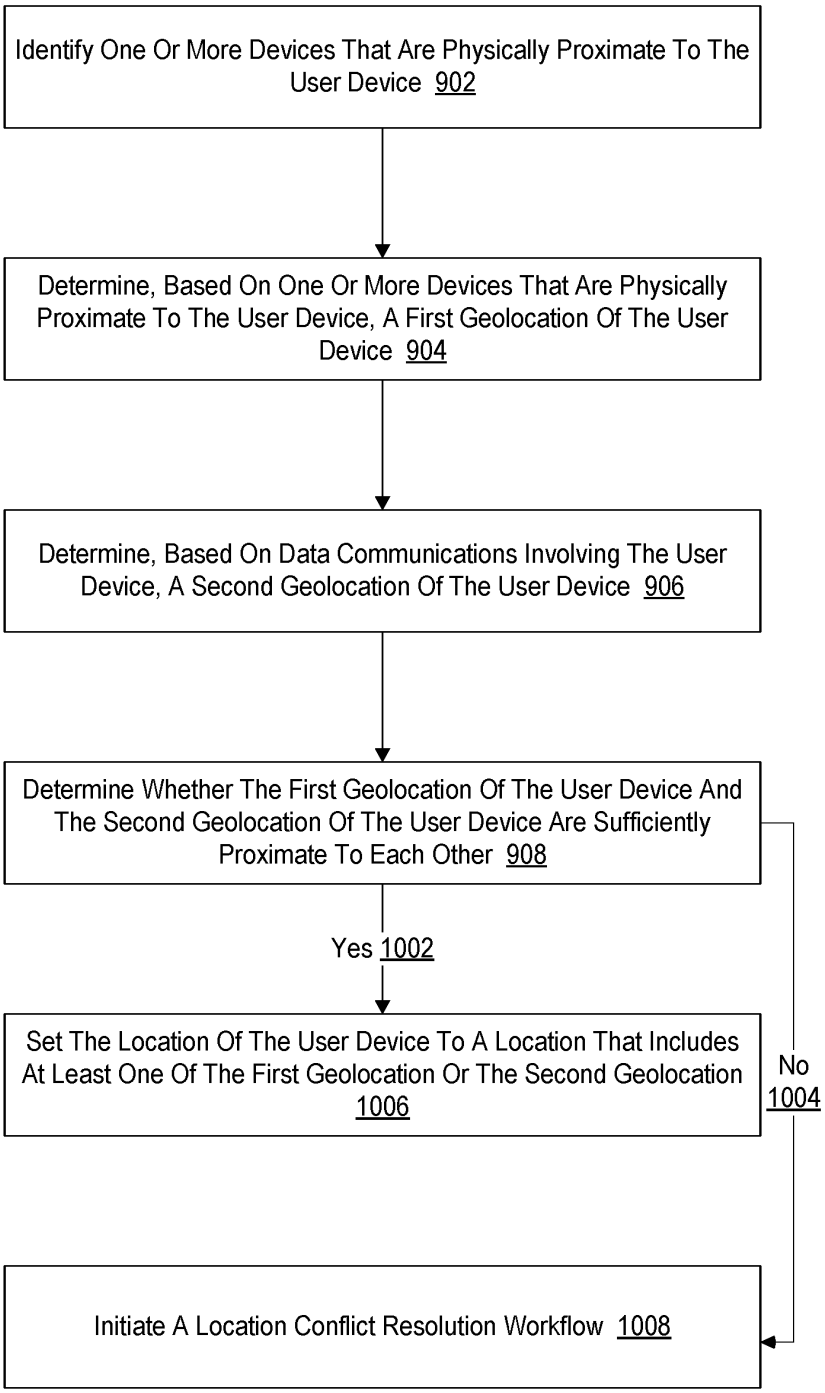

Identify One Or More Devices That Are Physically Proximate To The User Device 902
Determine, Based On One Or More Devices That Are Physically Proximate To The User Device, A First Geolocation Of The User Device 904
Determine, Based On Data Communications Involving The User Device, A Second Geolocation Of The User Device 906
Determine Whether The First Geolocation Of The User Device And The Second Geolocation Of The User Device Are Sufficiently Proximate To Each Other 908
Yes 1002
Set The Location Of The User Device To A Location That Includes At Least One Of The First Geolocation Or The Second Geolocation 1006
No 1004
Initiate A Location Conflict Resolution Workflow 1008

Fig. 10

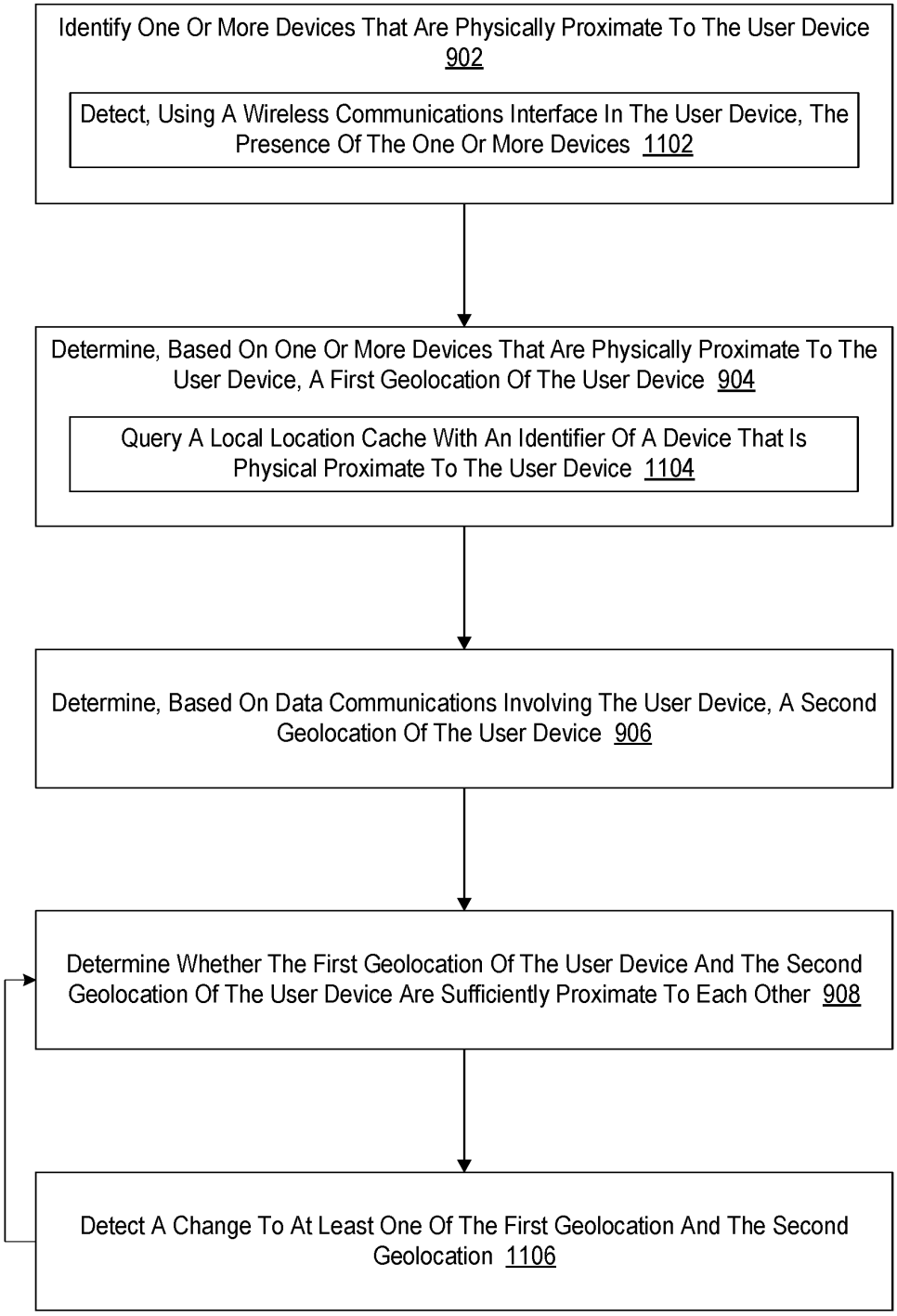

Identify One Or More Devices That Are Physically Proximate To The User Device 902
Detect, Using A Wireless Communications Interface In The User Device, The Presence Of The One Or More Devices 1102
Determine, Based On One Or More Devices That Are Physically Proximate To The User Device, A First Geolocation Of The User Device 904
Query A Local Location Cache With An Identifier Of A Device That Is Physical Proximate To The User Device 1104
Determine, Based On Data Communications Involving The User Device, A Second Geolocation Of The User Device 906
Determine Whether The First Geolocation Of The User Device And The Second Geolocation Of The User Device Are Sufficiently Proximate To Each Other 908
Detect A Change To At Least One Of The First Geolocation And The Second Geolocation 1106

Fig. 11

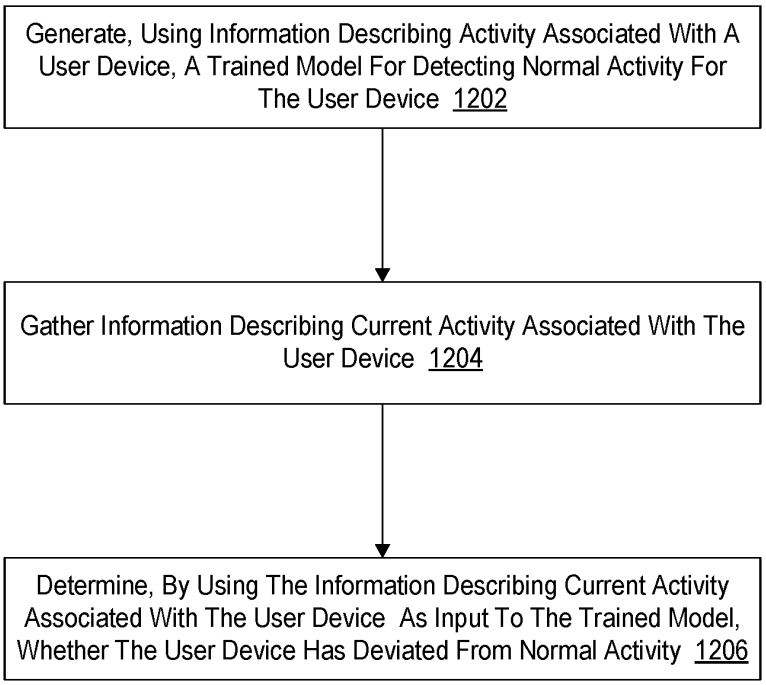

Generate, Using Information Describing Activity Associated With A User Device, A Trained Model For Detecting Normal Activity For The User Device 1202
Gather Information Describing Current Activity Associated With The User Device 1204
Determine, By Using The Information Describing Current Activity Associated With The User Device As Input To The Trained Model, Whether The User Device Has Deviated From Normal Activity 1206

Fig. 12

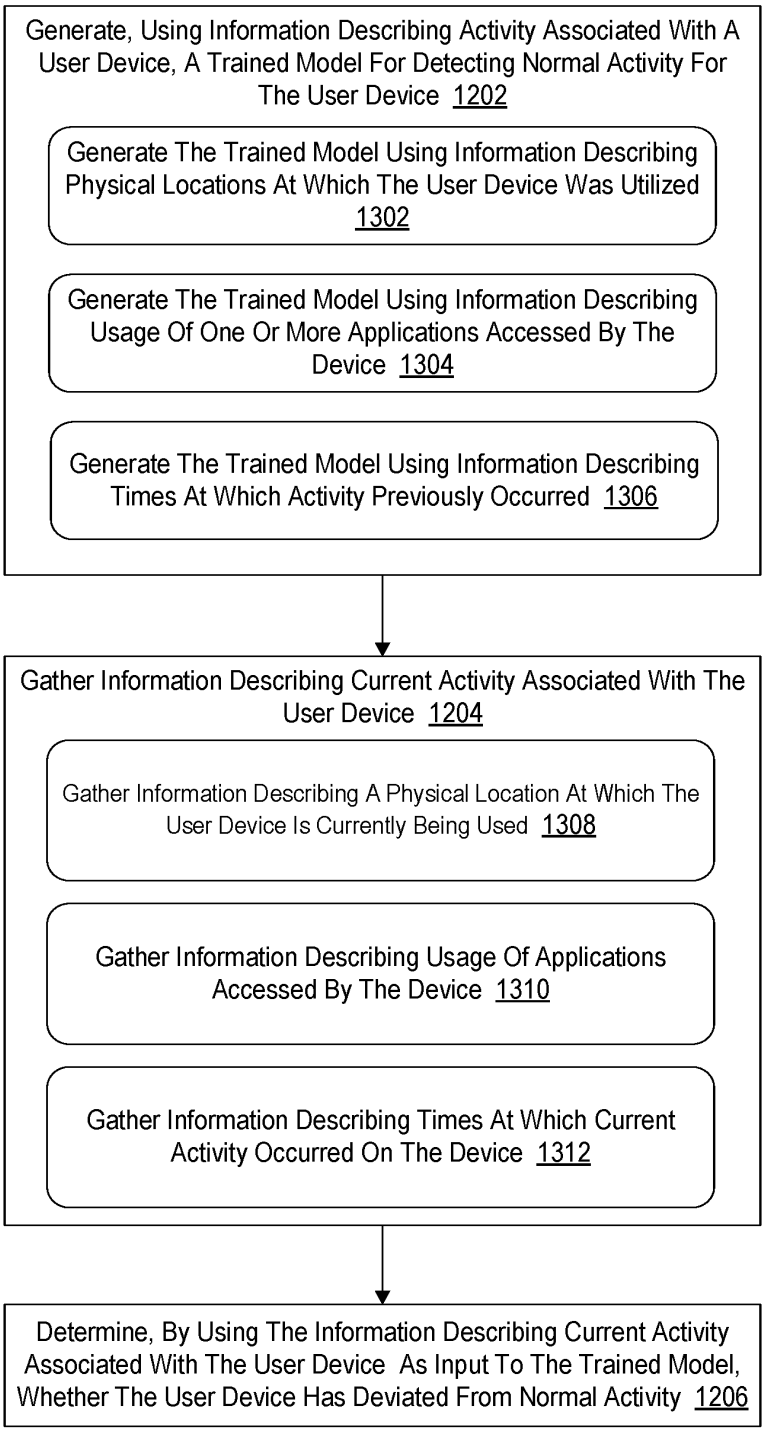

Generate, Using Information Describing Activity Associated With A User Device, A Trained Model For Detecting Normal Activity For The User Device 1202
Generate The Trained Model Using Information Describing Physical Locations At Which The User Device Was Utilized 1302
Generate The Trained Model Using Information Describing Usage Of One Or More Applications Accessed By The Device 1304
Generate The Trained Model Using Information Describing Times At Which Activity Previously Occurred 1306
Gather Information Describing Current Activity Associated With The User Device 1204
Gather Information Describing A Physical Location At Which The User Device Is Currently Being Used 1308
Gather Information Describing Usage Of Applications Accessed By The Device 1310
Gather Information Describing Times At Which Current Activity Occurred On The Device 1312
Determine, By Using The Information Describing Current Activity Associated With The User Device As Input To The Trained Model, Whether The User Device Has Deviated From Normal Activity 1206

Fig. 13

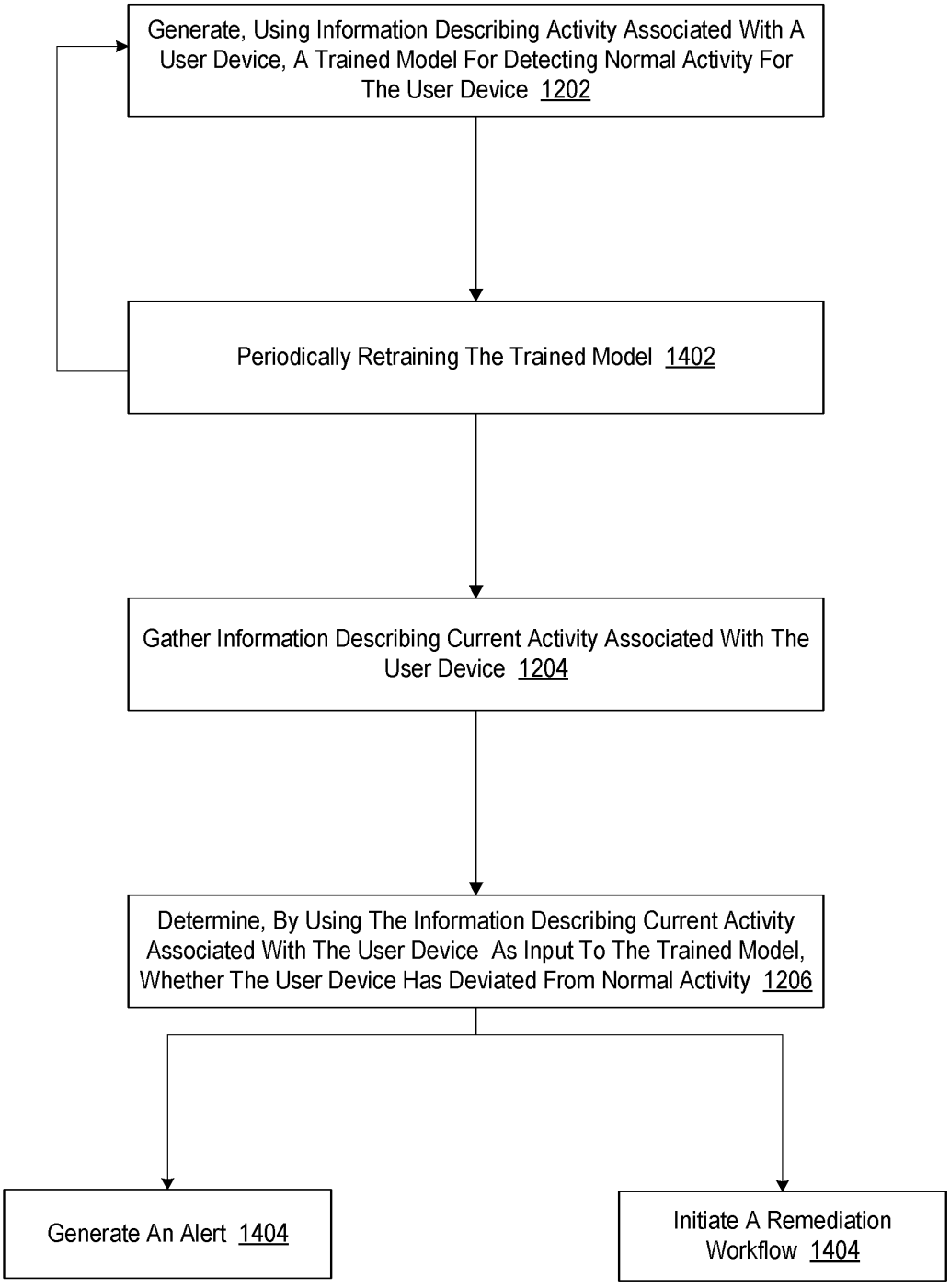

Generate, Using Information Describing Activity Associated With A User Device, A Trained Model For Detecting Normal Activity For The User Device 1202
Periodically Retraining The Trained Model 1402
Gather Information Describing Current Activity Associated With The User Device 1204
Determine, By Using The Information Describing Current Activity Associated With The User Device As Input To The Trained Model, Whether The User Device Has Deviated From Normal Activity 1206
Generate An Alert 1404
Initiate A Remediation Workflow 1404

Fig. 14

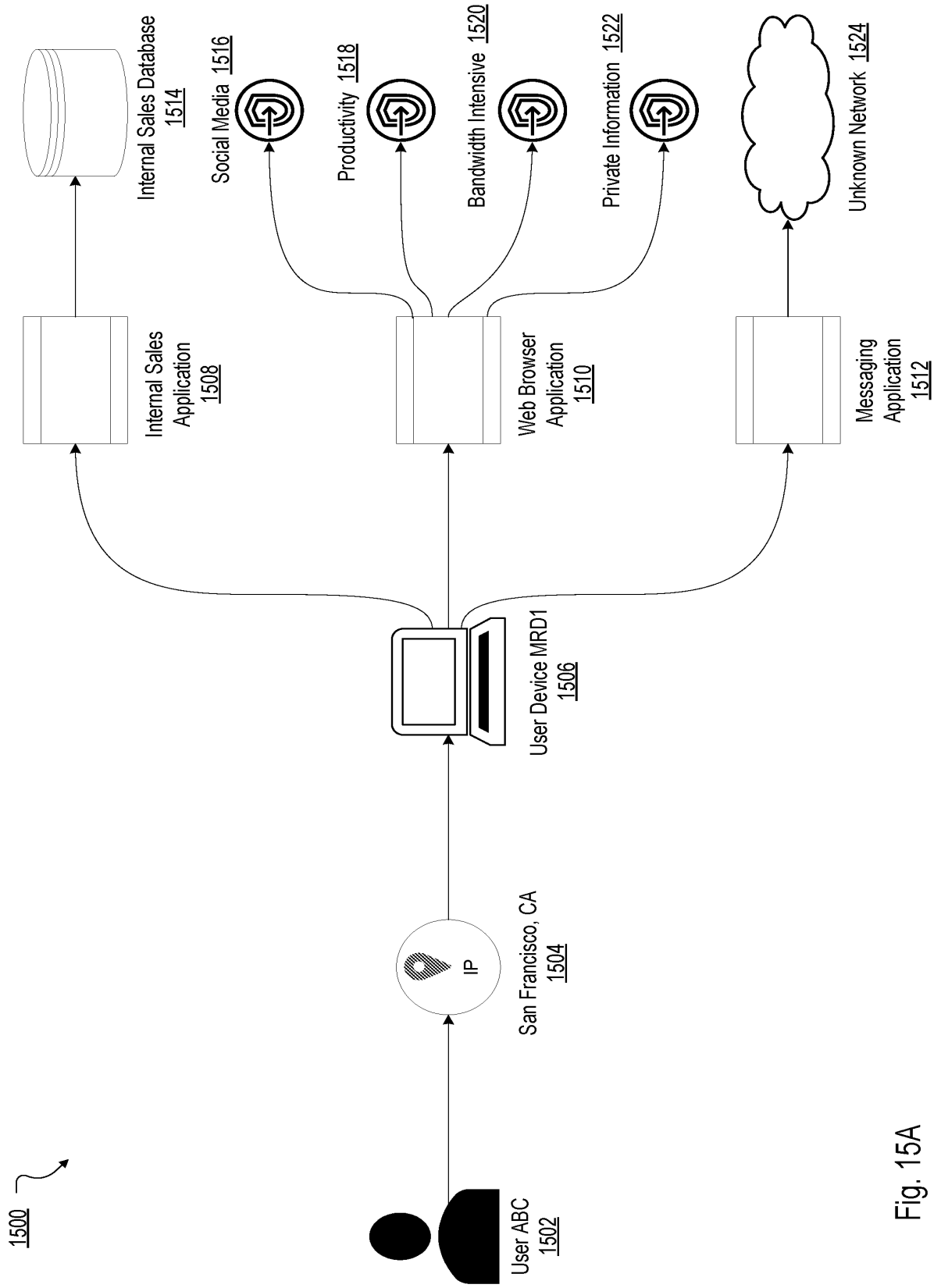

1500
User ABC
1502
IP
San Francisco, CA
1504
User Device MRD1
1506
Internal Sales Application
1508
Web Browser Application
1510
Messaging Application
1512
Internal Sales Database
1514
Social Media 1516
Productivity 1518
Bandwidth Intensive 1520
Private Information 1522
Unknown Network 1524

Fig. 15A

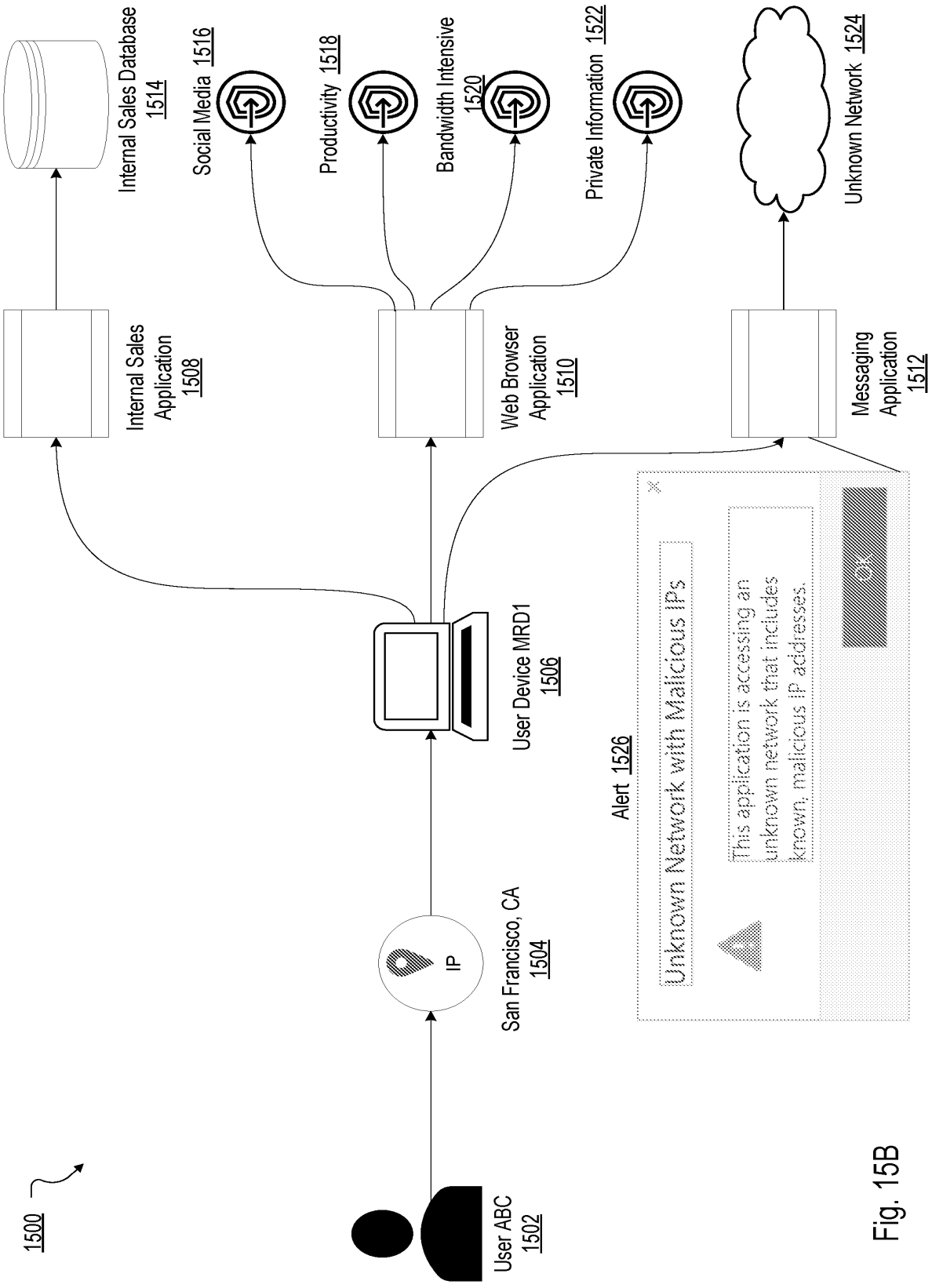

1500
User ABC
1502
IP
San Francisco, CA
1504
User Device MRD1
1506
Internal Sales Application
1508
Web Browser Application
1510
Messaging Application
1512
Internal Sales Database
1514
Social Media 1516
Productivity 1518
Bandwidth Intensive
1520
Private Information 1522
Unknown Network 1524
Alert 1526
Unknown Network with Malicious IPs
This application is accessing an unknown network that includes known, malicious IP addresses.
OK

Fig. 15B

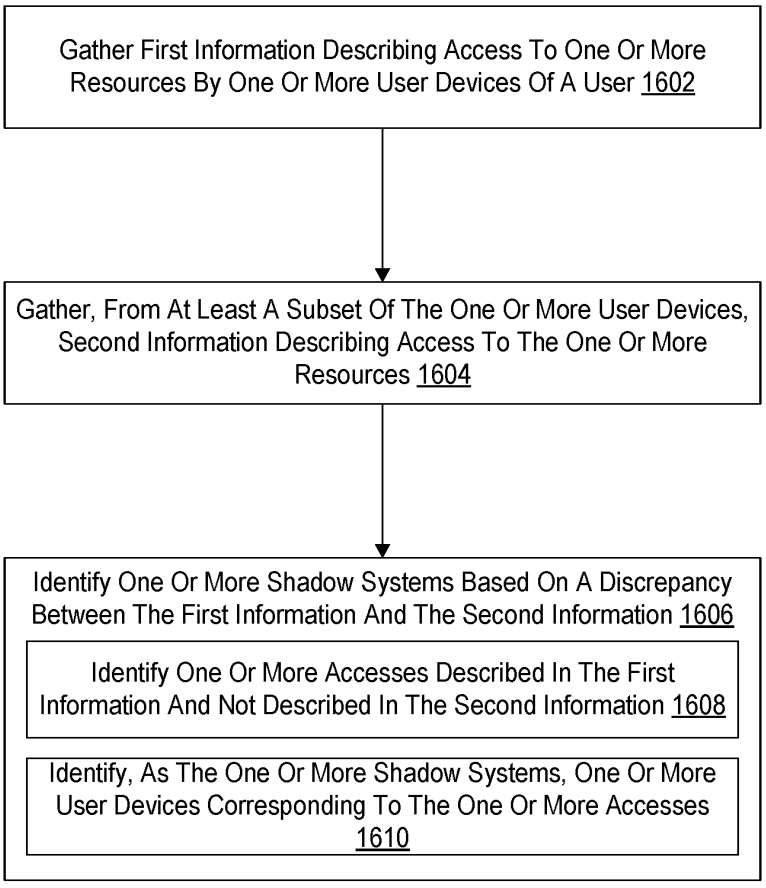

Gather First Information Describing Access To One Or More Resources By One Or More User Devices Of A User 1602
Gather, From At Least A Subset Of The One Or More User Devices, Second Information Describing Access To The One Or More Resources 1604
Identify One Or More Shadow Systems Based On A Discrepancy Between The First Information And The Second Information 1606
Identify One Or More Accesses Described In The First Information And Not Described In The Second Information 1608
Identify, As The One Or More Shadow Systems, One Or More User Devices Corresponding To The One Or More Accesses 1610

Fig. 16

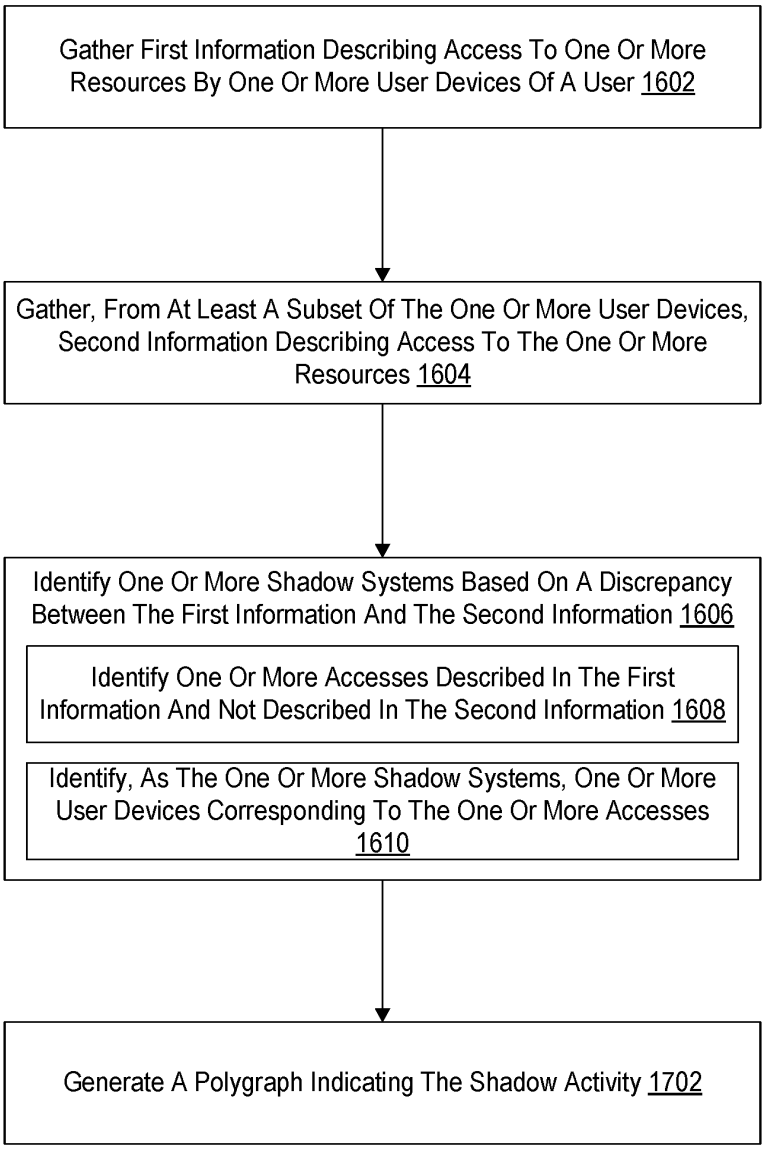

Gather First Information Describing Access To One Or More Resources By One Or More User Devices Of A User 1602
Gather, From At Least A Subset Of The One Or More User Devices, Second Information Describing Access To The One Or More Resources 1604
Identify One Or More Shadow Systems Based On A Discrepancy Between The First Information And The Second Information 1606
Identify One Or More Accesses Described In The First Information And Not Described In The Second Information 1608
Identify, As The One Or More Shadow Systems, One Or More User Devices Corresponding To The One Or More Accesses 1610
Generate A Polygraph Indicating The Shadow Activity 1702

Fig. 17

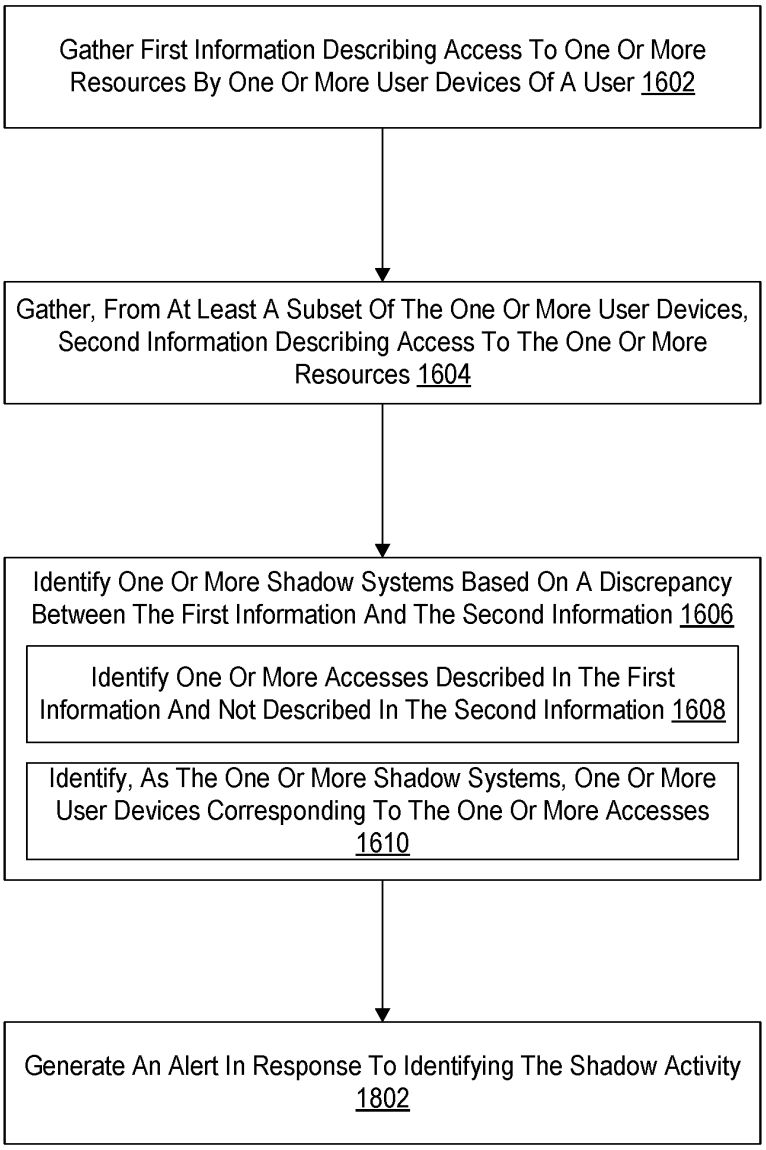

Gather First Information Describing Access To One Or More Resources By One Or More User Devices Of A User 1602
Gather, From At Least A Subset Of The One Or More User Devices, Second Information Describing Access To The One Or More Resources 1604
Identify One Or More Shadow Systems Based On A Discrepancy Between The First Information And The Second Information 1606
Identify One Or More Accesses Described In The First Information And Not Described In The Second Information 1608
Identify, As The One Or More Shadow Systems, One Or More User Devices Corresponding To The One Or More Accesses 1610
Generate An Alert In Response To Identifying The Shadow Activity 1802

Fig. 18

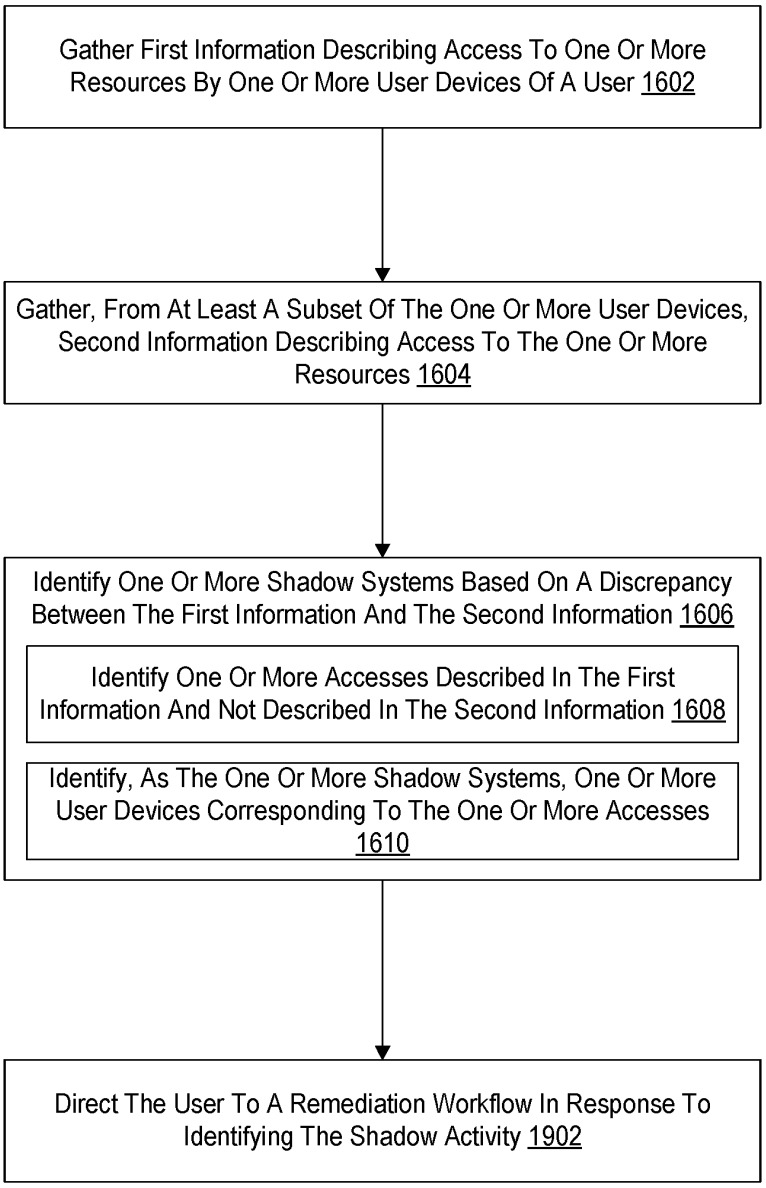

Gather First Information Describing Access To One Or More Resources By One Or More User Devices Of A User 1602
Gather, From At Least A Subset Of The One Or More User Devices, Second Information Describing Access To The One Or More Resources 1604
Identify One Or More Shadow Systems Based On A Discrepancy Between The First Information And The Second Information 1606
Identify One Or More Accesses Described In The First Information And Not Described In The Second Information 1608
Identify, As The One Or More Shadow Systems, One Or More User Devices Corresponding To The One Or More Accesses 1610
Direct The User To A Remediation Workflow In Response To Identifying The Shadow Activity 1902

Fig. 19

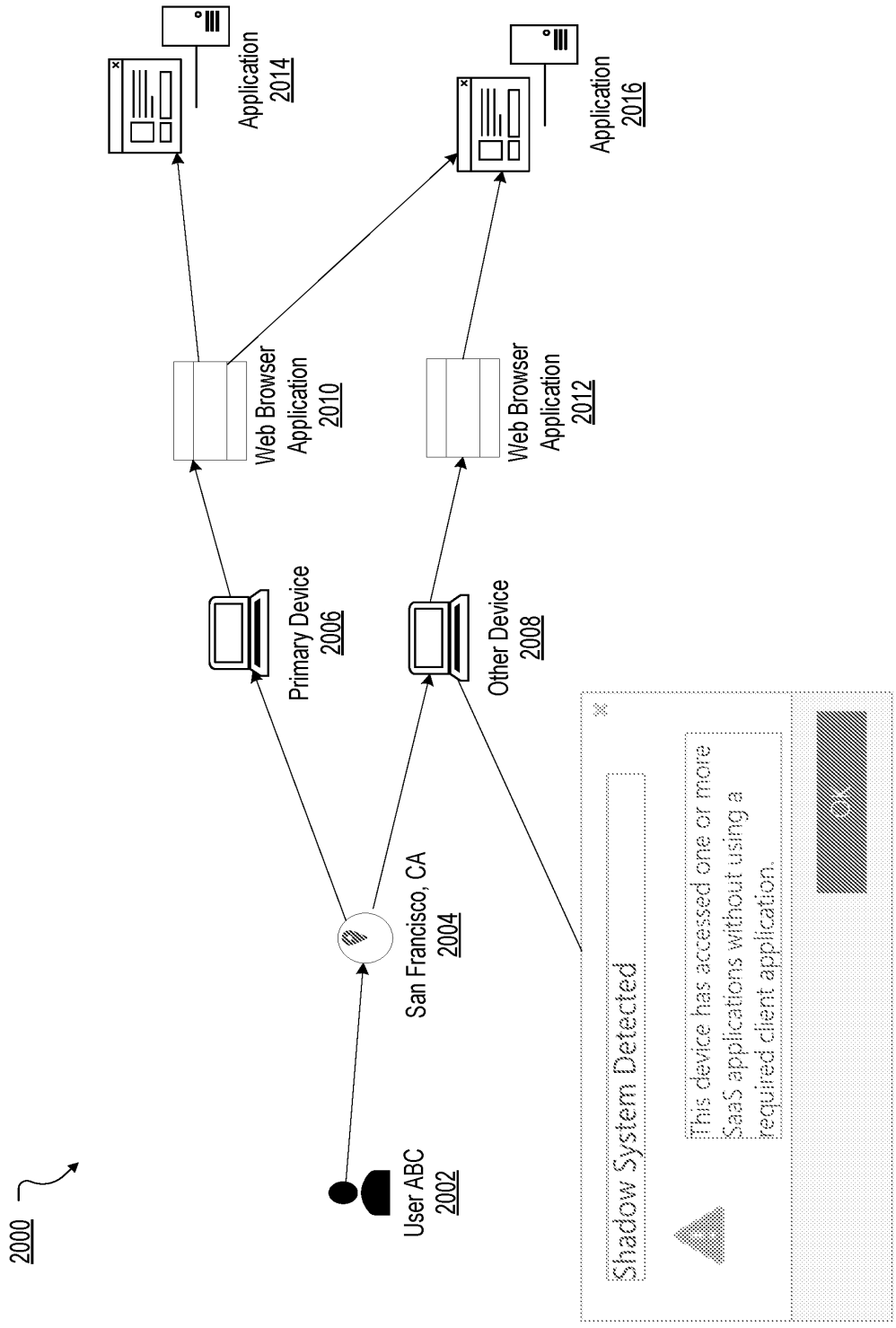

2000
User ABC
2002
San Francisco, CA
2004
Primary Device
2006
Other Device
2008
Web Browser
Application
2010
Web Browser
Application
2012
Application
2014
Application
2016
Shadow System Detected
This device has accessed one or more SaaS applications without using a required client application.
OK
Alert 2018

Fig. 20

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems
First Named Inventor/Applicant Name:	VIKRAM KAPOOR
Filer:	Edward Joseph Lenart/Ashley Jenkins
Attorney Docket Number:	L0040B3CIP6C1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	320	320
UTILITY SEARCH FEE	1111	1	700	700
UTILITY EXAMINATION FEE	1311	1	800	800
Pages:				
UTILITY APPL SIZE FEE PER 50 SHEETS >100	1081	1	420	420
Claims:				
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2240**

Electronic Acknowledgement Receipt

EFS ID:	46129807
Application Number:	17858866
International Application Number:	
Confirmation Number:	4455
Title of Invention:	Using Activity Monitored By Multiple Data Sources To Identify Shadow Systems
First Named Inventor/Applicant Name:	VIKRAM KAPOOR
Customer Number:	182115
Filer:	Edward Joseph Lenart/Ashley Jenkins
Filer Authorized By:	Edward Joseph Lenart
Attorney Docket Number:	L0040B3CIP6C1
Receipt Date:	06-JUL-2022
Filing Date:	
Time Stamp:	19:15:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2240
RAM confirmation Number	E202276J17362475
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	2022-07-06_L0040B3CIP6_POA.pdf	305425 8493d46c18d928616b565474e7c55a4b9d7715ad	no	3
Warnings:					
Information:					
2	Application Data Sheet	2022-07-06_L0040B3CIP6_ADS.pdf	2278602 4c6062e7c5bd4083d315968a281197a1b98fa288	no	11
Warnings:					
Information:					
3		2022-07-06_L0040B3CIP6C1_ContinuationApplication.pdf	722982 cff7a51a1d3772ffbc63727a6d2fc180a5b950d1	yes	127

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	122
Claims	123	126
Abstract	127	127

Warnings:					
Information:					
4	Drawings-only black and white line drawings	2022-07-06_L0040B3CIP6_ContinuationDrawings.pdf	2166137 3f566ec44953ad601791e25d3a6d817f6cf5974a	no	59
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	46994 ae20d2c626496d1960800dd828b27b42b364bc85	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	5520140

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.