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.
13/559,707	03/24/2015	8990948	0079152-000015	1767

21839 7590 03/04/2015

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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 169 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 Application Information Retrieval (PAIR) WEB site (http://pair.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 Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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 including the Patent, advance orders and notification of maintenance fees 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.

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

21839 7590 12/24/2014
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015	1767

TITLE OF INVENTION: SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/24/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
BEHESHTI SHIRAZI, SAYED ARESH	2435	726-025000

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/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form 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 BUCHANAN INGERSOLL & ROONEY PC
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 has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: TAASERA, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): ERIE, PENNSYLVANIA

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

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☒ Payment by credit card.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 02-4800 (enclose an extra copy of this form).

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 February 16, 2015

Typed or printed name Charles F. Wieland III Registration No. 33,096

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 2 of 318

Electronic Patent Application Fee Transmittal

Application Number:	13559707
Filing Date:	27-Jul-2012
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Charles F. Wieland III/Mich Sok
Attorney Docket Number:	0079152-000015

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt	
EFS ID:	21507056
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/Mich Sok
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000015
Receipt Date:	16-FEB-2015
Filing Date:	27-JUL-2012
Time Stamp:	13:01:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$480
RAM confirmation Number	9238
Deposit Account	024800
Authorized User	WIELAND, CHARLES F.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Fees_Transmittal.pdf	955106 eeb2f92973eff20ff8db6e959bea1ba22e668024	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30669 01297659336a49992fb5520c42316dbd8e0bdd28	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	985775		

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.

Issue Classification CPC	Application_ID
	13559707
Document Date: 2/6/2015	**Document Code: IIFW**

APPLICATION_ID	SUBCLASS	MAINGROUP	SLASH	SUBGROUP	TYPE	VERSION
13559707	G06F	21	/	51	I	20130101
13559707	G06F	21	/	564	F	20130101
13559707	H04L	63	/	145	A	20130101

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

21839 7590 12/24/2014

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
BEHESHTI SHIRAZI, SAYED ARESH	
ART UNIT	PAPER NUMBER
2435	

DATE MAILED: 12/24/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015	1767

TITLE OF INVENTION: SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/24/2015

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 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity 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 and an extra copy of the form should be submitted. 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: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 8 of 318

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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 including the Patent, advance orders and notification of maintenance fees 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.

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

21839 7590 12/24/2014
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015	1767

TITLE OF INVENTION: SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/24/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
BEHESHTI SHIRAZI, SAYED ARESH	2435	726-025000

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/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form 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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 9 of 318

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.
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015	1767

21839 7590 12/24/2014

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
BEHESHTI SHIRAZI, SAYED ARESH	
ART UNIT	**PAPER NUMBER**
2435	

DATE MAILED: 12/24/2014

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.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 10 of 318

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 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, 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. 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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

Notice of Allowability	Application No. 13/559,707	Applicant(s) KUMAR ET AL.	
	Examiner SAYED ARESH BEHESHTI SHIRAZI	Art Unit 2435	AIA (First Inventor to File) Status No

-- 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 *11/13/2014*.
   ☐ 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 *5-9*. 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 *12/09/2014* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JOSEPH P. HIRL/
Supervisory Patent Examiner, Art Unit 2435

The present application is being examined under the pre-AIA first to invent provisions.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Derek P. Benke (Reg No. 56,944) on December 9, 2014.

During the interview Examiner indicated combination of limitations disclosed by amended claim 5 is allowable, and suggested cancelation of withdrawn claims. Applicant representative agreed.

AMEND THE FOLLOWING CLAIMS AS FOLLOWS:

1. (Canceled)

2. (Canceled)

3. (Canceled)

4. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Canceled)

13. (Canceled)

14. (Canceled)

Allowable Subject Matter

1. Claims 5-9 are allowed.

According to MPEP 1302.14 (I): "In most cases, the examiner's actions and the applicant's replies make evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule. This is particularly true when applicant fully complies with 37 CFR 1.111 (b) and (c) and 37 CFR 1.133(b). **Thus, where the examiner's actions clearly point out the reasons for rejection and the applicant's reply explicitly presents reasons why claims are patentable over the reference, the reasons for**

allowance are in all probability evident from the record and no statement should be necessary."

Cited prior art **Alperovitch et al. (U.S. 2008/0175266)** discloses methods and systems for assigning reputation to communications entities include collecting communications data from distributed agents, aggregating the communications data, analyzing the communications data and identifying relationships between communications entities based upon the communications data.

Further **Njemanze et al. (U.S. 2011/0145711)** discloses a selected time interval of previously stored events generated by a number of computer network devices are replayed and cross-correlated according to rules. Meta-events are generated when the events satisfy conditions associated with one or more of the rules. The rules used during replay may differ from prior rules used at a time when the events occurred within a computer network that included the computer network devices. In this way, new rules can be tested against true event data streams to determine whether or not the rules should be used in a live environment (i.e., the efficacy of the rules can be tested an tor debugged against actual event data).

Examiner notes combination of limitations disclosed by independent claim 5 would be allowable, none of the cited prior arts disclose the combination of limitations "**monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime**

configuration of the application resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events"

Dependent claims are allowed due to the dependency.

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"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAYED ARESH BEHESHTI SHIRAZI whose telephone number is (571)270-3396. The examiner can normally be reached on 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOSEPH P HIRL can be reached on 571-272-3685. 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.

/S. B./
Examiner, Art Unit 2435

/JOSEPH P. HIRL/
Supervisory Patent Examiner, Art Unit 2435

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/559,707	KUMAR ET AL.	
	Examiner	Art Unit	
	SAYED ARESH BEHESHTI SHIRAZI	2435	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SAYED ARESH BEHESHTI SHIRAZI*. (3) *Dereke P. Benke (Reg. No. 56,944)*.

(2) _____. (4)_____.

Date of Interview: *09 December 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1-4 and 10-14*.

Identification of prior art discussed: _____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

During the interview, Examiner requested cancelation of withdrawn claims. Applicant representative agreed.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of 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.

☐ Attachment

/SAYED ARESH BEHESHTI SHIRAZI/ Examiner, Art Unit 2435	/JOSEPH P. HIRL/ Supervisory Patent Examiner, Art Unit 2435

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 18 of 318

Notice of References Cited	Application/Control No. 13/559,707	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner SAYED ARESH BEHESHTI	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2008/0175266 A1	07-2008	Alperovitch et al.	370/465
*	B	US-2009/0328222 A1	12-2009	Helman et al.	726/25
*	C	US-2011/0145711 A1	06-2011	Njemanze et al.	715/736
*	D	US-8,214,497 B2	07-2012	Alperovitch et al.	709/226
*	E	US-2012/0284282 A9	11-2012	Ghosh et al.	707/748
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	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 MM-YYYY format are publication dates. Classifications may be US or foreign.

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

BIB DATA SHEET

CONFIRMATION NO. 1767

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/559,707	07/27/2012 RULE	726	2435	0079152-000015

APPLICANTS

INVENTORS

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/641,007 05/01/2012

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/08/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /SAYED BEHESHTI SHIRAZI/ Examiner's Signature	☐ Met after Allowance S.B Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	29	14	4

ADDRESS

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404
UNITED STATES

TITLE

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

FILING FEE RECEIVED		
1500	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	Art Unit
	SAYED BEHESHTI SHIRAZI	2435

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	25	7/1/2014	S.B
709	205, 206, 224, 226	7/1/2014	S.B
715	736	7/1/2014	S.B
345	440	7/1/2014	S.B
726	25	12/10/2014	S.B
709	205, 206, 224, 226	12/10/2014	S.B
715	736	12/10/2014	S.B
345	4400	12/10/2014	S.B

SEARCH NOTES		
Search Notes	Date	Examiner
Performed Inventor search	7/1/2014	S.B
Performed Assignee search	7/1/2014	S.B
Performed Double Patenting search	7/1/2014	S.B
Performed Classification search	7/1/2014	S.B
Performed CPC search	7/1/2014	S.B
Performed NPL search (Google Scholar)	7/1/2014	S.B
Performed EAST keyword search	7/1/2014	S.B
Consulted with Tod Swann 2430 QAS regarding 101, 112	7/3/2014	S.B
Consulted with Justin Rider 2430 QAS regarding 101, 112	7/3/2014	S.B
Performed Inventor search	12/10/2014	S.B
Performed Assignee search	12/10/2014	S.B
Performed Double Patenting search	12/10/2014	S.B

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
Performed Classification search combined with keyword search	12/10/2014	S.B
Performed EAST keyword search	12/10/2014	S.B
Performed NPL search (Google Scholar)	12/10/2014	S.B

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	Performed interferenc search (UPAD, US-PGPUB)e	12/10/2014	S.B

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	**Art Unit**
	SAYED BEHESHTI SHIRAZI	2435

CPC		
Symbol	**Type**	**Version**

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

/SAYED BEHESHTI SHIRAZI/ Examiner.Art Unit 2435	12/10/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	5	
/JOSEPH P HIRL/ Supervisory Patent Examiner.Art Unit 2435	12/15/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 23 of 318

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	**Art Unit**
	SAYED BEHESHTI SHIRAZI	2435

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	25	G	0	6	F	11 / 00 (2006.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
709	205	206	224	226	
715	736				
345	440				

/SAYED BEHESHTI SHIRAZI/ Examiner.Art Unit 2435	12/10/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	5	
/JOSEPH P HIRL/ Supervisory Patent Examiner.Art Unit 2435	12/15/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	**Art Unit**
	SAYED BEHESHTI SHIRAZI	2435

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1														
	2														
	3														
	4														
1	5														
2	6														
3	7														
4	8														
5	9														
	10														
	11														
	12														
	13														
	14														

/SAYED BEHESHTI SHIRAZI/ Examiner.Art Unit 2435	12/10/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	5	
/JOSEPH P HIRL/ Supervisory Patent Examiner.Art Unit 2435	12/15/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 25 of 318

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	"13559707"	USPAT	OR	OFF	2013/11/30 16:38
S2	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:38
S3	20273	orchestrat$3	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:39
S4	23	orchestrat$3 same security same assessment	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:39
S5	1	"20120284282"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:48
S6	0	"2009032822"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:49
S7	1	"20090328222"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:49
S8	1	"8214497".pn.	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:50
S9	1	quarantin$3 near20 (infected or attacked) same divert$3 near10 user$1 near20 transaction$1 near20 traffic	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:25
S10	1	quarantin$3 near20 (infected or attacked) same (divert$3 or direct$3 or re$1direct$3 or re$1rout$3) same user$1 same transaction$1 near20 traffic	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S11	75	quarantin$3 near20 (infected or attacked) same (divert$3 or direct$3 or re$1direct$3 or re$1rout$3) same (user$1 or transaction$1 or traffic)	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S12	45	quarantin$3 near20 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S13	45	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S14	1	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic)) same ((GUI or display or monitor or screen) near10 detail$1 near10 (malware or infection or malicious or virus))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:28
S15	1	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:28

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 26 of 318

		same5 ((GUI or display or monitor or screen) near10 detail$1 near10 (malware or infection or malicious or virus))				
S16	1	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic)) same5 ((GUI or display or monitor or screen) near10 (malware or infection or malicious or virus))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:28
S17	40	S13 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:29
S20	20	("20070143474" | "20080276317" | "6742128" | "20070185856" | "20080083039" | "7587607" | "8108536" | "20050289072" | "20120102458" | "8214497" | "20050283660" | "20090172814" | "20090178138" | "20090187988" | "20090204964" | "6990579" | "20090094584" | "20090144818" | "20090241170" | "20120216244" | "20120011590" | "8010469" | "20050138384" | "20080141027" | "20110154500" | "20110179477" | "7882221" | "7979696" | "20090133110" | "20090138939" | "20090328186" | "20110072506" | "20110276468" | "20120110174" | "7370359" | "20050132031" | "20080015808" | "20080244748" | "20100281273" | "20110173643" | "6760441" | "6996710" | "7797544" | "7984304" | "20090276204" | "20090328222" | "20120072968" | "20120137375" | "20060200680" | "20070005992" | "20110035577" | "20070174406" | "20060015942" | "7174566" | "20050132202" | "20050204404" | "20050221766" | "20080289028" | "20110185423" | "6091835" | "7013481" | "20110162073" | "20050033987" | "20120131334" | "7194759" | "7979544" | "20120260342" | "20060005009" | "20080235372" | "20090204806" | "20120084850" | "20120284282" | "6507904" | "8429454").PN.	USPAT	OR	OFF	2014/07/01 15:43
S21	74	("20070143474" | "20080276317" | "6742128" | "20070185856" | "20080083039" | "7587607" | "8108536" | "20050289072" | "20120102458" | "8214497" | "20050283660" | "20090172814" | "20090178138" | "20090187988" | "20090204964" | "6990579" | "20090094584" | "20090144818" | "20090241170" | "20120216244" | "20120011590" | "8010469" | "20050138384" | "20080141027" | "20110154500" | "20110179477" | "7882221" | "7979696" | "20090133110" | "20090138939" | "20090328186" | "20110072506" |	US-PGPUB; USPAT	OR	OFF	2014/07/01 15:49

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705

		"20110276468" | "20120110174" | "7370359" | "20050132031" | "20080015808" | "20080244748" | "20100281273" | "20110173643" | "6760441" | "6996710" | "7797544" | "7984304" | "20090276204" | "20090328222" | "20120072968" | "20120137375" | "20060200680" | "20070005992" | "20110035577" | "20070174406" | "20060015942" | "7174566" | "20050132202" | "20050204404" | "20050221766" | "20080289028" | "20110185423" | "6091835" | "7013481" | "20110162073" | "20050033987" | "20120131334" | "7194759" | "7979544" | "20120260342" | "20060005009" | "20080235372" | "20090204806" | "20120084850" | "20120284282" | "6507904" | "8429454").PN.				
S22	8	(dashboard or GUI) near10 display$3 near10 integrity near10 (application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:05
S23	0	(dashboard or GUI) same (real$1time or live) same display$3 near10 integrity near10 (application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S24	11	(dashboard or GUI) same (real$1time or live) same display$3 same integrity same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S25	234	(dashboard or GUI) same (real$1time or live) same display$3 same status same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S26	26	(dashboard or GUI) same (real$1time or live) same display$3 same status same (integrity or risk or security) same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S27	22	S26 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S28	35	(dashboard or GUI) same (real$1time or live) same display$3 same (status or state) same (integrity or risk or security) same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:46
S29	15	(plurality or many or multiple or multi) same (dashboard$1 or GUI$1) same (real$1time or live) same display$3 same (status or state) same (integrity or risk or security) same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:46
S30	9	S29 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:46
S31	63	(risk near20 score) same engine same (correlat$3 or aggregat$3)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:48
S32	4	(risk near20 score) same engine same (correlat$3 or aggregat$3) same (sensor$1 or agent$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:48
S33	3	S32 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:51
S34	1746	726/25.ccls.	USPAT	OR	OFF	2014/07/01 17:05

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 28 of 318

S35	26706	709/205,206,224,226.ccls.	USPAT	OR	OFF	2014/07/01 17:06
S36	734	715/736.ccls.	USPAT	OR	OFF	2014/07/01 17:06
S37	1595	345/440.ccls.	USPAT	OR	OFF	2014/07/01 17:06
S38	0	(security adj agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (correlat$3 or aggregat$3) same risk same (score or number)	USPAT	OR	OFF	2014/07/01 17:08
S39	0	(security adj agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (correlat$3 or aggregat$3) same risk same (score or number)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:08
S40	0	(security adj agent$1) same (sens$3 or monitor$3) same (correlat$3 or aggregat$3) same risk same (score or number)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:09
S41	21	(security adj agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1)	USPAT	OR	OFF	2014/07/01 17:09
S42	2452	(agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1)	USPAT	OR	OFF	2014/07/01 17:10
S43	3740	(agent$1) same (sens$3 or monitor$3) same (activity event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1)	USPAT	OR	OFF	2014/07/01 17:10
S44	4	(agent$1) same (sens$3 or monitor$3) same (activity event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1) same2 (risk adj (score or number))	USPAT	OR	OFF	2014/07/01 17:10
S45	11	(agent$1) same (sens$3 or monitor$3) same (activity event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1) same2 (risk adj (score or number))	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:10
S46	8	S45 AND ((G06F21/316 OR G06F21/577 OR G06F19/3431 OR G06F21/552 OR H04L63/14 OR H04L63/20).CPC.)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:15
S47	8	S31 AND ((G06F21/316 OR G06F21/577 OR G06F19/3431 OR G06F21/552 OR H04L63/14 OR H04L63/20).CPC.)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:17
S48	5	S25 AND ((G06F21/316 OR G06F21/577 OR G06F19/3431 OR G06F21/552 OR H04L63/14 OR H04L63/20).CPC.)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:17
S49	1	"20080175266"	USPAT	OR	OFF	2014/07/01 22:09
S50	3	"20080175266"	US-PGPUB; USPAT	OR	OFF	2014/07/01 22:09
S51	0	(scan$3 same per same schedule) same behavior$2 same risk$1	USPAT	OR	OFF	2014/07/02 18:56
S52	1	(scan$3 same per same schedule) same	US-PGPUB;	OR	OFF	2014/07/02

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 29 of 318

		behavior$2 same risk$1	USPAT			18:56
S53	0	(scan$3 same schedule same (hour$2 or Day or daily or week$2 or monthly)) same behavior$2 same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:58
S54	12	(scan$3 same (hour$2 or Day or daily or week$2 or monthly)) same behavior$2 same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:59
S55	12	(scan$4 same (hour$2 or Day or daily or week$2 or monthly)) same behavior$2 same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:59
S56	85	(scan$4 same (hour$2 or Day or daily or week$2 or monthly)) same (behavior$2 or risk or event or anomaly or abnormal$3) same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:00
S57	79	S56 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:01
S58	2	(scan$4 near4 (hour$2 or Day or daily or week$2 or monthly)) same (behavior$2 or risk or event or anomaly or abnormal$3) same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:02
S59	22	(scan$4 near4 (hour$2 or Day or daily or week$2 or monthly)) same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:03
S60	18	S59 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:03
S61	0	"13559707"	USPAT	OR	OFF	2014/07/03 09:51
S62	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2014/07/03 09:51
S63	17	"KUMAR, Srinivas".in.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:26
S64	18	"Pollutro, Dennis".in.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:26
S65	29	S63 or S64	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:26
S66	7	"TAASERA, INC".as.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:44
S67	7	"TAASERA".as.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:44
S68	74	("20070143474" | "20080276317" | "6742128" | "20070185856" | "20080083039" | "7587607" | "8108536" | "20050289072" | "20120102458" | "8214497" | "20050283660" | "20090172814" | "20090178138" | "20090187988" | "20090204964" | "6990579" | "20090094584" | "20090144818" | "20090241170" | "20120216244" | "20120011590" | "8010469" | "20050138384" | "20080141027" | "20110154500" | "20110179477" | "7882221" | "7979696" | "20090133110" | "20090138939" |	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:57

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 30 of 318

		"20090328186" | "20110072506" | "20110276468" | "20120110174" | "7370359" | "20050132031" | "20080015808" | "20080244748" | "20100281273" | "20110173643" | "6760441" | "6996710" | "7797544" | "7984304" | "20090276204" | "20090328222" | "20120072968" | "20120137375" | "20060200680" | "20070005992" | "20110035577" | "20070174406" | "20060015942" | "7174566" | "20050132202" | "20050204404" | "20050221766" | "20080289028" | "20110185423" | "6091835" | "7013481" | "20110162073" | "20050033987" | "20120131334" | "7194759" | "7979544" | "20120260342" | "20060005009" | "20080235372" | "20090204806" | "20120084850" | "20120284282" | "6507904" | "8429454").PN.				
S69	1	(security and end$1point and network and integrity and application and behavior and engine and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:59
S70	1	(security and end$1point and network and integrity and behavior and engine and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:59
S71	1	(security and end$1point and network and integrity and behavior and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:59
S72	4	(security and network and integrity and behavior and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S73	7	(security and network and integrity and behavior and correlat$3).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S74	78	(security and network and behavior and correlat$3).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S75	0	S68 and S74	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S76	1	S67 and S74	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:01
S77	29	S63 or S64	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:01
S78	1	S77 and S74	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:01
S79	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:13
S80	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2014/10/23 14:18
S81	0	correlat$3 same matrix same event$1 same classification same threat same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:27
S82	0	correlat$3 same matri$2 same event$1 same classification same threat same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR;	OR	OFF	2014/12/07 21:27

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 31 of 318

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S83	0	correlat$3 same matri$3 same event$1 same classification same threat same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:27
S84	0	matri$3 same event$1 same classification same threat same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:27
S85	0	matri$3 same (event$1 or incident$1 or action$1 or result$1) same classification same threat same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:27
S86	0	matri$3 same (event$1 or incident$1 or action$1 or result$1) same classif$7 same threat same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:28
S87	0	matri$3 same (event$1 or incident$1 or action$1 or result$1) same classif$7 same threat$1 same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:28
S88	7	(matri$3 or event$1 or incident$1 or action$1 or result$1) same classif$7 same threat$1 same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:31
S89	7	event near5 risk near5 correlation near5 matri$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 21:32
S90	2	"20090328222"	US-PGPUB; USPAT	OR	OFF	2014/12/07 21:44
S91	0	matri$3 same (event$1 or incident$1 or action$1 or result$1 or risk) same classif$7 same threat$1 same tempor$4 same behavior$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2014/12/07 22:05

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 32 of 318

			IBM_TDB			
S92	0	matri$3 same (event$1 or incident$1 or action$1 or result$1 or risk) same classif$7 same threat$1 same tempor$4 same behavior$2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 22:05
S93	0	matri$3 same (event$1 or incident$1 or action$1 or result$1 or risk) same classif$7 same threat$1 same (tempor$4 or live) same behavior$2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 22:09
S94	7	matri$3 same (event$1 or incident$1 or action$1 or result$1 or risk) same classif$7 same threat$1 same behavior$2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 22:09
S95	19	matri$3 same (event$1 or incident$1 or action$1 or result$1) same classif$7 same (threat$1 or malicious or malware or unauthorized or virus or risk) same behavior$2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/07 22:09
S96	8	S95 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/12/07 22:10
S97	11	"TAASERA".as.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:04
S98	22	"KUMAR, Srinivas".in.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:05
S99	21	"Pollutro, Dennis".in.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:05
S100	34	S98 or S99	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:05
S101	34	S97 or S100	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:05
S102	19	matri$3 same (event$1 or incident$1 or action$1 or result$1) same classif$7 same (threat$1 or malicious or malware or unauthorized or virus or risk) same behavior$2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/10 18:05
S103	246	matri$3 same (event$1 or incident$1 or action$1 or result$1) same classif$7 same (threat$1 or malicious or malware or unauthorized or virus or risk)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/10 18:05
S104	7	S101 and S103	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2014/12/10 18:07

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 33 of 318

			EPO; JPO; DERWENT; IBM_TDB			
S105	2996	726/25.ccls.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:18
S106	52932	709/205,206,224,226.ccls.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:18
S107	1331	715/736.ccls.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:18
S108	3020	345/440.ccls.	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:18
S109	59465	S105 or S106 or S107 or S108	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:19
S110	338	real$1time and behavior and event$1 and monitor$3 and (activit$3 or dialog$1) and (matrix or matrice) and risk and correlation and (classification or classif$4) and threat$1 and sequence and temporal	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:20
S111	17	S109 and S110	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:20
S112	11	S111 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/12/10 18:20

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S18	0	"13559707"	USPAT; UPAD	OR	OFF	2014/03/25 11:12
S19	1	"13559707"	US-PGPUB; USPAT; UPAD	OR	OFF	2014/03/25 11:12
S113	22	"KUMAR, Srinivas".in.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:11
S114	21	"Pollutro, Dennis".in.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:12
S115	11	"TAASERA".as.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:12
S116	34	S113 or S114 or S115	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:12
S117	0	(correlating and correlation and matri$3 and risk and threat$1 and classif$7 and sequence and temopral and real$1time and behavior and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:13
S118	0	(correlating and correlation and matri$3 and risk and threat$1 and classif$7 and real$1time and behavior and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:13

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 34 of 318

S119	0	(correlating and correlation and matri$3 and risk and threat$1 and classif$7 and real$1time and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:13
S120	0	(correlating and correlation and matri$3 and risk and classif$7 and real$1time and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:14
S124	0	(correlating and correlation and matri$3 and risk and threat$1 and sequence and temopral and real$1time and behavior and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:15
S125	0	(correlat$3 and matri$3 and risk and threat$1 and sequence and temopral and real$1time and behavior and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:15
S126	1	(correlat$3 and matri$3 and risk and threat$1 and real$1time and behavior and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:15
S127	1	(correlat$3 and matri$3 and risk and threat$1 and real$1time and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:15
S128	0	(correlating and correlation and matri$3 and risk and threat$1 and sequence and temopral and behavior and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:15
S130	31	(correlat$3 and risk and (matrix or matrices) and event$1).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:16
S131	3	S130 and S116	US-PGPUB; USPAT; UPAD	OR	OFF	2014/12/10 18:16

12/10/2014 8:24:50 PM
C:\Users\sbeheshtishirazi\Documents\EAST\Workspaces\13559707.wsp

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 35 of 318

Aggression toward female partners by at-**risk** young men: the contribution of male adolescent friendships.

DM Capaldi, TJ Dishion, M Stoolmiller… - Developmental …, 2001 - psycnet.apa.org

... the Couples Study were found to show significantly higher levels of **risk** than those ... The **correlation** between the observational and coder impression variables was .63. ... and psychological aggression indicators are shown in Table 2. All alphas and **correlations** between indicators ...

Cited by 207 Related articles All 8 versions Cite Save

Real-time visualization of network **behaviors** for situational awareness

DM Best, S Bohn, D Love, A Wynne… - Proceedings of the seventh …, 2010 - dl.acm.org

... The visual analysis tools themselves— **Correlation** Layers for Information Query and Exploration (CLIQUE) and Traffic Circle ... We then create a **matrix** that contains each channel for a given actor and each ... By having two **matrices**, one of a historic timeframe and one of the current ...

Cited by 24 Related articles All 4 versions Cite Save

Botnet detection based on network **behavior**

WT Strayer, D Lapsely, R Walsh, C Livadas - Botnet Detection, 2008 - Springer

... a deterministic decision, one is left with a probabilistic conclusion, complete with the **risk** of false ... The identification of clusters of **correlated** flows certainly suggest further inves- tigation, which is the ... This **correlation** stage does not prove the existence of a botnet — there is no test ...

Cited by 117 Related articles All 15 versions Cite Save

Insider **threat** detection using situation-aware MAS

JF Buford, L Lewis, G Jakobson - Information Fusion, 2008 11th …, 2008 - ieeexplore.ieee.org

... CERT's MERIT (Management and Education of the **Risks** and Insider **Threat**) workshop [5], which ... **Correlated** events are used by the situation manager to identify emerging situations and validate ... For example if two users have a high **correlation** of "unknown location" events, this ...

Cited by 17 Related articles All 3 versions Cite Save

A fusion model for network **threat** identification and **risk** assessment

J Ma, Z Li, H Zhang - Artificial Intelligence and Computational …, 2009 - ieeexplore.ieee.org

... us a good mechanism to meet needs of **real-time risk** processing, which combines the **risks** of individual ... The information of open ports in one host are also can be **correlated** with the port features ... Finally, the whole network **risk** distribution is described by using HMM approach. ...

Cited by 8 Related articles All 4 versions Cite Save

How optimists face skin cancer information: **Risk** assessment, attention, memory, and **behavior**

J Luo, DM Isaacowitz - Psychology and health, 2007 - Taylor & Francis

... variety of health **risks**, ranging from catching a cold to more serious **risks** such as ... health-related optimism, or unrealistic optimism (**risk** perception controlled for objective **risk**), respectively. ... Table I. **Correlation matrix** for optimism and measures of attention, memory, and **behavior**. ...

Cited by 26 Related articles Cite Save

Preparing for smart grid technologies: A **behavioral** decision research approach to understanding consumer expectations about smart meters

T Krishnamurti, D Schwartz, A Davis, B Fischhoff… - Energy Policy, 2012 - Elsevier

... Because **correlations** in the factor **correlation matrix** were less than a standard cutoff of 0.32 ... Given the potential for **risk** beliefs to increase when they are not addressed (Fischhoff, 1996 ... transparent and clarifies the **temporal** scope and primary recipients of those **risks** and benefits. ...

Cited by 36 Related articles All 9 versions Cite Save

Financial **risk** cover analysis, modeling control and monitoring system

J Barsade, JA Conlon, TJ Gutierez… - US Patent …, 2012 - Google Patents

... Over the counter derivatives undergo periods of **risk** during which either the instrument is not liquid, or ... 8 , if the **correlation** coefficient between the client portfolio and a particular FRC is specified to ... As appropriate, steps can be taken to offset the **risks** such outlier events may pose ...

Cited by 1 Related articles All 6 versions Cite Save

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 36 of 318

The role of information in mobile banking resistance

T Laukkanen, V Kiviniemi - International Journal of Bank …, 2010 - emeraldinsight.com

... This indicates **correlation** between these two constructs. ... increase the perceived value added provided by mobile banking and decrease the perceived **risks** related to ... and Sheth, 1989), our findings suggest that functional barriers, including usage, value and **risk**, are **correlated**. ...

Cited by 53 Related articles All 4 versions Cite Save

DRIVABILITY: a new concept for modelling driving performance

E Bekiaris, A Amditis, M Panou - Cognition, Technology & Work, 2003 - Springer

... Table 8 Indicative **correlation** of DRIVABILITY indexes and scale to the TRAINER failure criteria for ... Inappropriate driving **behaviour** and ignorance of basic **risks** (ie vehicle damage, traffic rules violation) RAI ... TTC<5 s, violation of traffic rules Driver misses a critical **risk** (on-coming ...

Cited by 17 Related articles All 5 versions Cite Save

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 37 of 318

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Kumar, Srinivas et al.	Group Art Unit: 2435
Application No.: 13/559,707	Examiner: Beheshti Shirazi, Syed Aresh
Filed: July 27, 2012	Confirmation No.: 1767
For: Systems and Methods for Orchestrating Runtime Operational Integrity	

AMENDMENT UNDER 37 C.F.R. § 1.111

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

Madam:

In response to the Office Action dated July 17, 2014, please amend the above-identified patent application as follows:

AMENDMENTS TO THE SPECIFICATION:

Please amend paragraph [0019] of the specification, as follows:

In other exemplary embodiments, methods, apparatuses, systems and computer readable media comprise a plurality of services that enable visibility, control, and/or compliance in a cloud computing environment with a runtime dashboard [[to]] capable of displaying operational integrity metrics of systems based on a plurality of threat vectors.

Please amend paragraph [0061] of the specification, as follows:

Referring to FIG. 3B, the exemplary method 310 may include determining or performing a calculus of risk 320 for the data center application and data silos, that receives sensory inputs 314 from instrumentation 313 including integrity measurement and verification scan correlation 315, network activity correlation 316 and endpoint event correlation 317, and may generate integrity metrics 312 for security orchestration 321, and may dispatch directives to an edge device 323 (for example, network firewall) for user access controls 322, to a load balancer 325 for session controls 324, or to a network fabric element 327 (for example, a switch or router) for flow controls 326.

Please amend paragraph [0075] of the specification, as follows:

As shown in FIG. 5, the exemplary application operational integrity system 500 includes an endpoint trust agent 510 on a device 560 comprising a process monitor 514 configured to observe local execution context of applications and services. The endpoint trust agent 510 further comprises a socket monitor 513 configured to observe network activities of applications and services and a system monitor 512 configured to observe system and platform resources consumed by applications and services. In the example embodiment provided in FIG. 5, the trust agent 510 also comprises an application integrity module 516 and a resource utilization module 515 configured to assess operational integrity based on rulesets 517. The trust agent 510 can also comprise native machine instrumentation 511 for a computing device being monitored by the application operational integrity system 500.

Please amend paragraph [0080] of the specification, as follows:

In the embodiment shown in FIG. 5, the endpoint events 520 are generated by a component of the endpoint trust agent 510, and represent alerts based ~~an~~ on endpoint sensor resident on the device 560. The alerts are mapped to a cell in the risk correlation matrix 411 grid by the system event correlator 410. In one embodiment, the format (schema) of the endpoint events 520 is a standard Extensible Markup Language (XML) notation. Additional features of the endpoint events 520 are described below with reference to FIG. 6.

Please amend paragraph [0116] of the specification, as follows:

A user's (1014) device D (560) may become infected with a form of an advanced persistent threat (e.g., malware M(benign)) while ~~he~~ the device D is still connected to an enterprise network of an organization 2303. The connection of the device D to the enterprise network can occur through user activity, for example, when the user 1014 connects a plug-and-play portable universal serial bus (USB) device with the malware M to the device D (benign) while it is connected to the enterprise network, as the result of the user 1014 opening an email attachment infected with the malware M(benign), when the user 1014 accesses a social network application from the device D, or when the user 1014 unwittingly transfers a file with the malware M(benign) to device D while accessing a file sharing service.

Please amend paragraph [0140] of the specification, as follows:

According to exemplary embodiments, the event correlator 1007 receives endpoint events 1033 from the event ~~correlator 1007,~~ processor 1006, maps the alerts 1032 using the event correlation matrix 1013, generates and sends endpoint warnings 1034 to the threat classifier 1008.

Please amend paragraph [0259] of the specification, as follows:

Referring to FIG. 23, the exemplary reputation scoring system 2300 computes a reputation score for a user 1014 that is employed by, a member of, or otherwise associated with an organization 2303. The user 1014 can be associated with the organization temporarily (i.e., as a contractor). The user 1014 uses one or more endpoint devices 560 to perform an online transaction 2304 with a service 2305 that is rendered by an application 2306 and managed by the organization 2303, to participate in an activity 2307. In embodiments, the activity 2307 is categorized as either social 2308 or professional **[[**1409**]]** 2309.

AMENDMENTS TO THE CLAIMS:

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

LISTING OF CLAIMS:

1. (Withdrawn-Currently Amended) A method for presenting a data center level runtime operational integrity dashboard for visibility at an application level and controls to remediate infected systems hosting applications engaging in malicious activities in a display of a computing platform having an integrity processor, a runtime event correlation matrix, a trust broker, a system event correlator, a network activity correlator, a trust supervisor, and a remediation controller ~~and remediation controls for infected systems in a display of a computing platform having a network trust agent, an endpoint trust agent, and a trust orchestrator~~, the method comprising:

receiving, from a plurality of endpoint assessment services, runtime integrity metrics for a plurality of trust vectors;

displaying, in a graphical user interface (GUI) on the display, risk indicators and impact analysis based on the confidence level of received integrity metrics;

providing, manual or automated remediation controls for threat containment and risk mitigation by performing one or more of:

taking a snapshot of the infected system,

restoring or reimaging the infected system from a trusted baseline configuration,

quarantining the infected system from a network fabric,

diverting users from the infected system,

diverting transactions from the infected system, and

diverting traffic from the infected system;

displaying, in the GUI, a status and progress of initiated remediation actions; and

displaying, in the GUI, details of malware analytics comprising one or more of:

infection summaries,

infection diagnosis,

threat categorization and identification based on a signature-less infection life-cycle model,

an address and geo-location for a source or attacker,

an identification of one or more infected victims,

forensic evidence chain of detected malicious activities and intent, and

compute, memory, storage and network level anomalies detected on the victim machine or infected system.

2. (Withdrawn) The method of claim 1, wherein the risk indicators are color-coded.

3. (Withdrawn) The method of claim 1, wherein the runtime operational integrity comprises execution anomalies and a threat posture.

4. (Withdrawn-Currently Amended) A method of orchestrating runtime operational integrity of a system executing on a computing platform using a network activity correlator ~~analyzer~~, an integrity processor ~~endpoint trust agent~~, a system event correlator, a trust broker, a remediation controller, a trust supervisor ~~orchestrator~~ and a plurality of network endpoint assessments, the method comprising:

determining, by the network activity correlator ~~analyzer~~, infection profiles based on network event correlation forensic evidence of malicious communications ~~anomalies based on network activity correlation and network malware detection~~;

determining, by the trust broker, system configuration anomalies based on system level normalization and collation of assessments;

determining, by the integrity processor ~~endpoint trust agent~~, resource utilization anomalies based on rulesets or alert expressions associated with processor, memory, and network resource usage;

determining, by the integrity processor ~~endpoint trust agent~~, at least one application integrity anomaly based on rulesets or alert expressions associated with static and dynamic image analysis;

determining, by the system event correlator, integrity profiles based on temporal and endpoint events associated with the application;

correlating, by the trust supervisor ~~orchestrator~~, integrity and infection profiles to characterize behaviors through continuous local and remote monitoring risk analysis and detection of malicious applications ~~network activity and endpoint events and behaviors characterized through continuous local and remote monitoring of network endpoints for risk analysis and detection of infected systems~~; and

mitigating, by the remediation controller ~~trust orchestrator~~, an infected system using inputs received from a real time threat visualization dashboard to implement flow level or transaction level remediation controls for the malicious applications.

5. (Currently Amended) A method of providing real-time ~~runtime~~ operational integrity of an application on a native computing environment ~~and a system using a computing platform comprising a network trust agent, an endpoint trust agent, an event and behavior correlation engine, and a trust orchestration server~~, the method comprising:

monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application ~~activity, system configuration for a system the application is executing on~~, resource utilization by the application, and integrity of the application;

generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;

correlating, by the event and risk correlation matrix, threat classifications ~~behavior correlation engine, risk~~ based on the temporal sequence of the generated real-time behavior based events ~~monitoring~~; and

displaying, in a plurality of runtime dashboards of an administrative console of the computing environment ~~platform~~, ~~real-time~~ real-time status indications for operational integrity of the ~~system and~~ application.

6. (Currently Amended) The method of claim 5, wherein the real-time operations of applications are monitored ~~monitoring is performed~~ continuously.

7. (Currently Amended) The method of claim 5, wherein the event and behavior correlation engine receives one or more of:

system events and infection profiles from [[the]] a network activity sensor;

integrity measurement and verification reports of scans from [[the]] a system configuration sensor;

system events pertaining to processor, network, memory, and storage resource consumption from [[the]] a resource utilization sensor; and

system events pertaining to image profiles and local execution context from [[the]] an application integrity sensor.

8. (Currently Amended) The method of claim 7, wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly, by a third party collaboration service to score the severity of an application based on the vulnerability, compliance, and patch status to affirm positive presence of a threat.

9. (Currently Amended) The method of claim 5, wherein the plurality of runtime dashboards are a plurality of application runtime reputation score ~~runtime~~ dashboards that comprise one or more of:

a global view dashboard;

a system configuration dashboard;

a resource utilization dashboard;

an application integrity dashboard; and

a network activity dashboard.

10. (Withdrawn) A system for orchestrating and displaying reputation scoring of a subject, the system comprising:

a display;

a reputation broker configured to:

process a query from a service provider for a reputation score of the subject, and

dispatch a request to generate a hierarchical reputation score for the subject;

a display module configured to render a graphical user interface (GUI) for an administration console comprising a plurality of dashboards in the display;

a trust orchestrator configured to:

process a received request from the reputation broker for a hierarchical reputation score by:

initiating a plurality of directed queries to information management systems external to an organization to interrogate attributes associated with the subject,

analyzing received query responses,

receiving a generated hierarchical reputation score for the subject based on a calculus of risk; and

sending the received hierarchical reputation score for the subject to the reputation broker;

receive a reputation token from the reputation broker for the subject in response to the dispatched request; and

send the reputation token to the service provider as a response to the query.

11. (Withdrawn-Currently Amended) The system of claim 10, wherein the ~~wherein the~~ query is received at a reputation broker configured to forward the query to

the trust broker, and wherein the query can be created, displayed, edited, and submitted using a dashboard of the administration console.

12. (Withdrawn-Currently Amended) The system of claim 10, wherein the ~~wherein the~~ response is displayed in a dashboard of the administration console.

13. (Withdrawn) The system of claim 10, wherein the hierarchical reputation is graphically depicted in a dashboard of the administration console.

14. (Withdrawn) The system of claim 10, wherein plurality of dashboards comprise one or more of:

a global view dashboard;

a system configuration dashboard;

a resource utilization dashboard;

an application integrity dashboard; and

a network activity dashboard.

AMENDMENTS TO THE DRAWINGS:

The attached sheets of drawings include changes to Figures 8 and 11. These sheets, which include Figures 8 and 11, replace the original sheets including Figures 8 and 11.

Replacement Sheets: 2 sheets

REMARKS

Favorable reconsideration of this application as presently amended, and in light of the following discussion, is respectfully requested.

Claims 5-9 are active in this application, Claims 1-4 and 10-14 having currently been withdrawn; and Claims 1, 4-9, 11, and 12 having been currently amended. Support for amended Claims 1, 4-9, 11 and 12 can be found in the original claims, drawings, and specification as-filled. No new matter has been added.

In the outstanding Office Action, the drawings were objected to due to informalities; Claims 5-9 were rejected under non-statutory double patenting; Claims 5-7 and 9 were rejected under 35 U.S.C. § 103(a) as unpatentable over Alperovitch et al. (U.S. Patent Publication No. 2008/0175266; hereinafter "Alperovitch") in view of Njemanze et al. (U.S. Patent Publication No. 2011/0145711; hereinafter "Njemanze"); and Claim 8 was rejected under 35 U.S.C. § 103(a) as unpatentable over Alperovitch in view of Njemanze and Midgely et al. (U.S. Patent No. 5,604,862; hereinafter "Midgely").

Applicants acknowledge with appreciation the courtesy of Examiner Shirazi in granting an interview in this application with Applicants' representative and the Applicant on October 23, 2014, during which time the art rejections were discussed. During the interview, proposed claim amendments were discussed which are substantially similar to the claim amendments included herewith, and the Examiner acknowledged that the proposed claim amendments overcome the current rejections. In light of this indication, the claims are amended as discussed during the interview.

In response to the objection to the drawings, Applicants have amended the specification to include the reference characters "312," "517," and "2309." Also,

Applicants have amended Figure 8 by removing reference character "845," and have amended Figure 11 by removing reference character "1114."

Accordingly, Applicants respectfully submit that the objection to the drawings has been overcome.

Regarding the double patenting rejection, a terminal disclaimer can be filed, if the claims in the present application remain obvious in view of the claims of the cited U.S. patent application at the time of allowance of the present application. Further amendments (if needed for allowance of these claims) may eliminate the double-patenting rejection, making the filing of a terminal disclaimer now premature. Indeed, MPEP § 804.02 VI states that, prior to issuance, it is necessary to disclaim the double patenting reference applied. Hence, Applicants respectfully request that the Examiner contact the undersigned should the present amendments and arguments be accepted and should the present application be otherwise in condition for allowance. At that time, a terminal disclaimer if warranted can be supplied to expedite issuance of this application.

In response to the rejection of Claims 5-7 and 9 under 35 U.S.C. § 103(a) as unpatentable over Alperovitch in view of Njemanze, Applicants respectfully submit that amended independent Claim 5 recites novel features not taught or rendered obvious by the applied references.

Independent Claim 5 is directed to a method of providing real-time operational integrity of an application on a native computing environment, the method including:

> monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime

configuration of the application, resource utilization by the application, and integrity of the application;

generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;

correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and

displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

Page 12 of the outstanding Office Action asserts that paragraphs [0030] and [0033] of Alperovitch describe "monitoring, by a plurality of sensory inputs, one or more of network activity, system configuration for a system the application is executing on, resource utilization by the application, and integrity of the application." However, as explained during the interview, Alperovitch fails to teach or suggest "monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application," as recited in Applicants' amended independent Claim 5.

Alperovitch describes methods and systems for assigning reputations to communications entities.[1] The methods described in Alperovitch are not able to authoritatively identify the application instances on the endpoint devices that may be

[1] See the Abstract of Alperovitch.

engaging in malicious activity, or make any determination about the runtime integrity of applications executing on the endpoint devices that may be responsible for the infection or may have been compromised because of threats undetected by the network based security controls.

Paragraph [0030] of Alperovitch states:

> The security agent 100 monitors communications entering and exiting the network 110. These communications are typically received though the internet 120 from many entities 130a-f that are connected to the internet 120. One or more of the entities 130a-f can be legitimate originators of communications traffic. However, one or more of the entities 130a-f can also be non-reputable entities originating unwanted communications. As such, the security agent 100 includes a reputation engine. The reputation engine can inspect a communication and to determine a reputation associated with an entity that originated the communication. The security agent 100 then performs an action on the communication based upon the reputation of the originating entity. If the reputation indicates that the originator of the communication is reputable, for example, the security agent can forward the communication to the recipient of the communication. However, if the reputation indicates that the originator of the communication is non-reputable, for example, the security agent can quarantine the communication, perform more tests on the message, or require authentication from the message originator, among many others....

Thus, the above paragraph of Alperovitch describes that a reputation engine can inspect a communication and determine a reputation associated with an entity that originated the communication. However, paragraph [0030] of Alperovitch fails to describe monitoring one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application,

resource utilization by the application, and integrity of the application, as recited in Applicants' amended independent Claim 5.

Further, Applicants respectfully submit that Alperovitch and Njemanze fail to teach or suggest "displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application," as recited in Applicants' amended independent Claim 5.

Page 13 of the outstanding Office Action acknowledges that Alperovitch fails to teach or suggest the above features, but asserts that paragraphs [0048] and [0049] of Njemanze describes the above features. Applicants respectfully disagree.

Paragraphs [0048] and [0049] of Njemanze describe a graphical user interface for a console 16. The graphical user interface includes a toolbar area that contains a file menu area as well as playback controls; a navigation panel that allows a user to view system assets; an inspect/edit panel through which a user can examine a specific event in great detail; a views panel that allows a user to view security events from heterogeneous sources; and a status bar that describes the current state of the time-based events selected by a user. However, the graphical user interface of Njemanze does not display in a plurality of runtime dashboards of an administrative console of a computing environment, ***real-time status indications*** for operational integrity of the application on ***a native computing environment***, as recited in Applicants' amended independent Claim 5.

Accordingly, Applicants respectfully submit that the cited references fail to teach or suggest "displaying, in a plurality of runtime dashboards of an administrative console

of the computing environment, real-time status indications for operational integrity of the application," as recited in Applicants' Claim 5.

Consequently, Alperovitch and Njemanze also fail to teach or suggest "generating real-time behavior based events for determining the real-time operational integrity of the application executing ***on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor***," as recited in Applicants' amended independent Claim 5.

Accordingly, Applicants respectfully request that the rejection of Claims 5-7 and 9 under 35 U.S.C. § 103(a) as unpatentable over Alperovitch in view of Njemanze be withdrawn.

In response to the rejection of Claim 8 under 35 U.S.C. § 103(a) as unpatentable over Alperovitch in view of Njemanze and Midgely, Applicants note that Claim 8 is dependent on Claim 5, and is believed to be patentable for at least the reasons discussed above. Further, Applicants respectfully submit that Midgely fails to cure the above-noted deficiencies of Alperovitch and Njemanze.

Accordingly, Applicants respectfully request the rejection of Claim 8 under 35 U.S.C. § 103(a) as unpatentable over Alperovitch in view of Njemanze and Midgely be withdrawn.

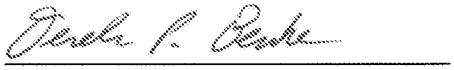
Consequently, in view of the present amendment, and in light of the above discussion, the pending claims as presented herewith are believed to be in condition for formal allowance, and an early and favorable action to that effect is respectfully requested.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: November 13, 2014 By: 

Derek P. Benke
Registration No. 56,944

Customer No. 21839
703 836 6620

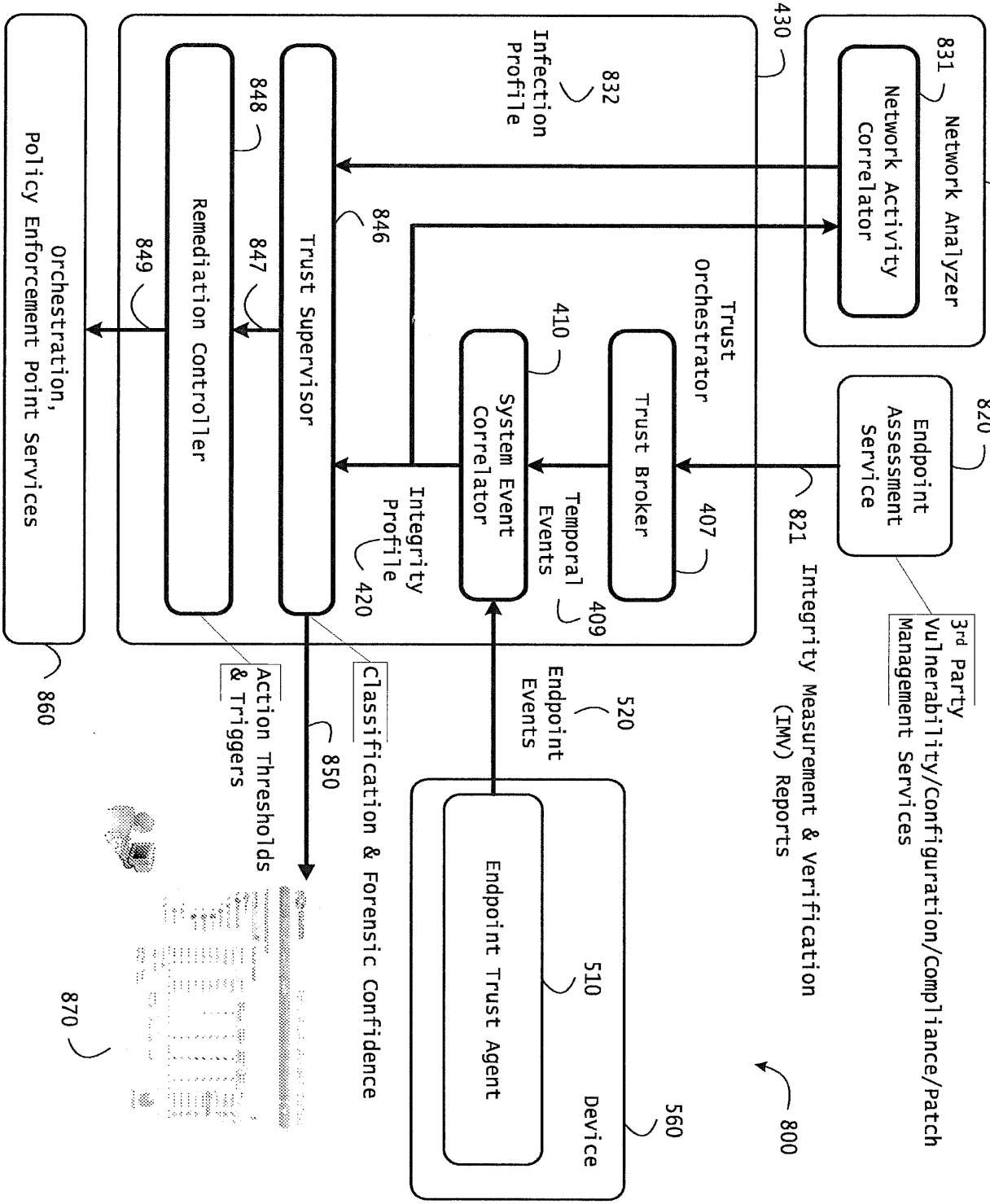

830
Network Analyzer
831
Network Activity Correlator
430
Infection Profile
832
848
Remediation Controller
849
Trust Supervisor
847
846
Trust Orchestrator
Trust Broker
407
410
System Event Correlator
Integrity Profile
420
Temporal Events
409
Orchestration, Policy Enforcement Point Services
860
820
Endpoint Assessment Service
821
Integrity Measurement & Verification (IMV) Reports
3rd Party Vulnerability/Configuration/Compliance/Patch Management Services
800
560
Device
510
Endpoint Trust Agent
520
Endpoint Events
Action Thresholds & Triggers
Classification & Forensic Confidence
850
870

FIG. 8

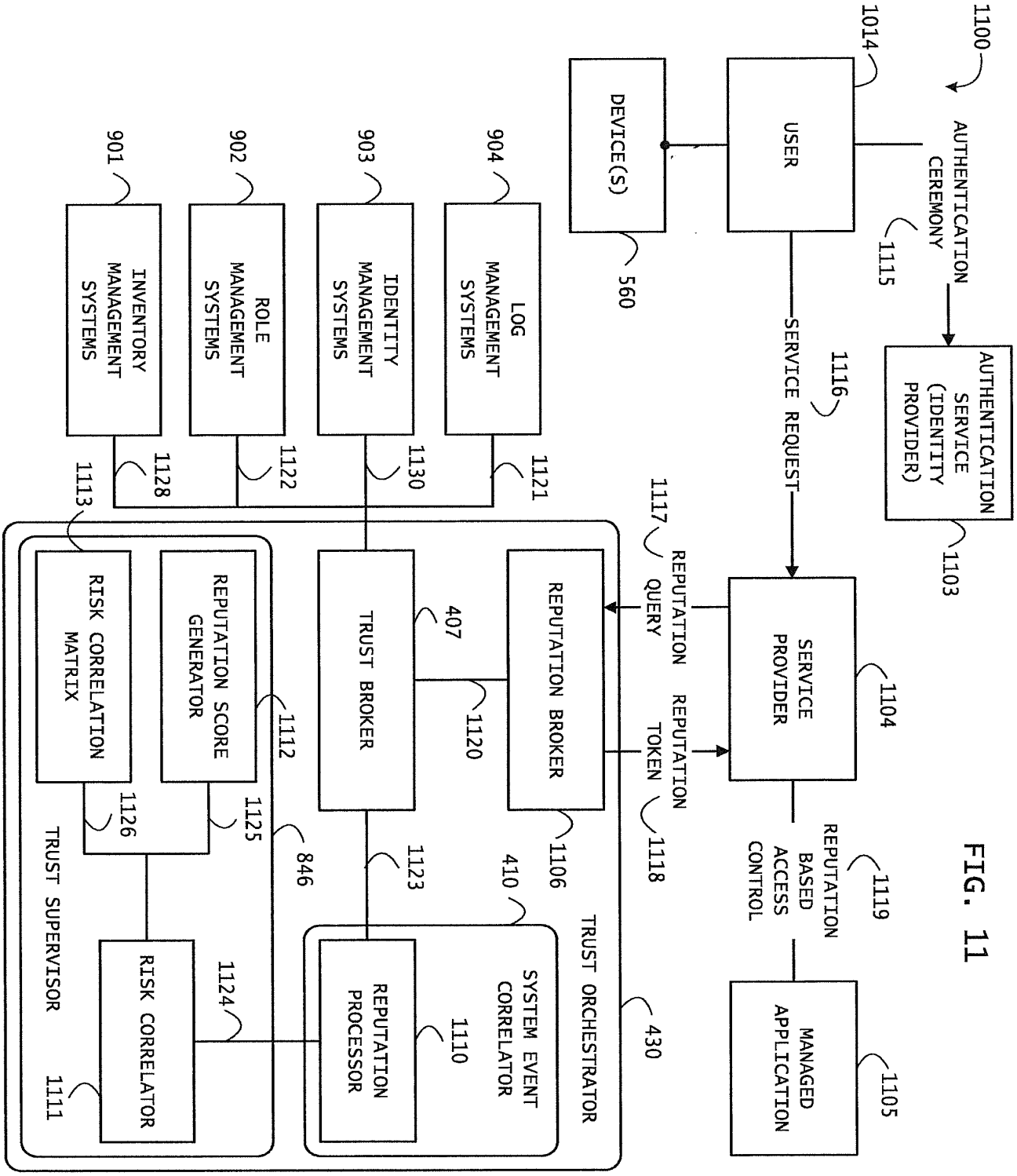

1100
AUTHENTICATION CEREMONY
1115
1014
USER
DEVICE(S)
560
AUTHENTICATION SERVICE (IDENTITY PROVIDER)
1103
1116
SERVICE REQUEST
1117
REPUTATION QUERY
REPUTATION TOKEN
1118
SERVICE PROVIDER
1104
REPUTATION BASED ACCESS CONTROL
1119
MANAGED APPLICATION
1105
901
INVENTORY MANAGEMENT SYSTEMS
902
ROLE MANAGEMENT SYSTEMS
903
IDENTITY MANAGEMENT SYSTEMS
904
LOG MANAGEMENT SYSTEMS
1128
1122
1130
1121
1113
TRUST ORCHESTRATOR
430
REPUTATION BROKER
1106
TRUST BROKER
407
1120
410
SYSTEM EVENT CORRELATOR
1110
REPUTATION PROCESSOR
1123
RISK CORRELATION MATRIX
REPUTATION SCORE GENERATOR
1112
1125
846
1126
RISK CORRELATOR
1124
TRUST SUPERVISOR
1111

FIG. 11

Electronic Patent Application Fee Transmittal

Application Number:	13559707
Filing Date:	27-Jul-2012
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Derek P. Benke/Shaunna Lloyd
Attorney Docket Number:	0079152-000015

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	100	100

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**100**

Electronic Acknowledgement Receipt	
EFS ID:	20690653
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna Lloyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000015
Receipt Date:	13-NOV-2014
Filing Date:	27-JUL-2012
Time Stamp:	16:38:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$100
RAM confirmation Number	3377
Deposit Account	024800
Authorized User	BENKE, DEREK
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	PET.pdf	674313 b29f05c5511bcc6de8891867d77b643519dbf35f	no	1
Warnings:					
Information:					
2		Amendment.pdf	746383 b4dd4c9729dc6f7878a2c6ce91f64e0561e8a9a2	yes	19

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	5
Claims	6	11
Drawings-only black and white line drawings	12	12
Applicant Arguments/Remarks Made in an Amendment	13	19

Warnings:					
Information:					
3	Drawings-only black and white line drawings	ReplacementSheets.pdf	95498 9d35003f758e73df8cbb62db12e92a08d74bdc07	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30256 94572675aa54d76d445a091bcd5140d654d9c82f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1546450		

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.

PTO/AIA/22 (03-132)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 0079152-000015
Application Number 13/559,707	Filed July 27, 2012
For Systems and Methods for Orchestrating Runtime Operational Integrity	
Art Unit 2435	Examiner Beheshti Shirazi, Syed Aresh

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Large Fee	Small Fee	Micro Fee	
☒ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 100.00
☐ Two month (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐ Three month (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four month (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five month (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☒ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☒ Payment by credit card.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number **02-4800**.

☒ Payment made via EFS-Web.

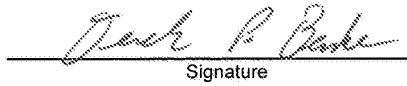
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☒ attorney or agent of record. Registration number **56944**.

☐ attorney or agent acting under 37 CFR 1.34. Registration number **56944**.



Signature

November 13, 2014
Date

Derek P. Benke
Type or printed name

703-836-6620
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required. See below*.

☐ Total of ___ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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.**

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 13/559,707	Filing Date 07/27/2012	☐ 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 $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ 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

AMENDMENT	11/13/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $210 =	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

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ 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.

** 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 number found in the appropriate box in column 1.

LIE
/JAMES TUNSTALL/

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.
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015	1767

21839 7590 07/17/2014

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
BEHESHTI SHIRAZI, SAYED ARESH	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
07/17/2014	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):

ADIPDOC1@BIPC.com

Office Action Summary	Application No. 13/559,707	Applicant(s) KUMAR ET AL.	
	Examiner SAYED ARESH BEHESHTI SHIRAZI	Art Unit 2435	AIA (First Inventor to File) Status No

-- 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 *04/11/2014*.

☐ 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) *5-9* 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) *5-9* 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 *07/27/2012* 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 *11/09/2012, 09/19/2013, 01/24/2014*.

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

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This action is in response to the applicant's communication filed on 04/28/2014. In virtue of this communication, claims 5-9 filed on 04/28/2014 are currently pending in the instant application.

Election/Restrictions

Applicant's election without traverse of claims of species III (i.e., claims 5-9) in the reply filed on 04/28/2014 is acknowledged.

Oath/Declaration

The instant application oath or declaration has been reviewed and accepted by Office.

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: Figure 3B, item 312, Figure 5, item 517, Figure 8, item 845, Figure11, item 1114, Figure 23, item 2039.

. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is

being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Information Disclosure Statement

The information Disclosure statement (IDS) form PTO-1449, filled on 11/09/2012, 09/19/2013, and 01/24/2014 are in compliance with the provisions of CFR 1.97. Accordingly, the information discloses therein was considered by the examiner.

Double Patenting

The non-statutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper time wise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A non-statutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*,

686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

4. Claims **5-9** are rejected on the ground of provisional nonstatutory double patenting as being unpatentable over claims **1, 3-7** of co-pending U.S. application **13/559,766**. Although the claims at issue are not identical, they are not patentably distinct from each other because the instant independent claim is directed to a A method of orchestrating runtime operational integrity of a system executing on a computing platform using a network analyzer, an endpoint trust agent, a trust broker, a trust orchestrator to perform the steps of claimed method/system of co-pending

application 13/559,766 which claims a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. Please refer to comparison table below for a better comparison of claims between claims **5-9,** of the instant application and claims **1-7** of the co-pending application 13/559,776.

13/559,707	**13/559,766**
5. A method of providing runtime operational integrity of an application and a system using a computing platform comprising a network trust agent, an endpoint trust agent, an event and behavior correlation engine, and a trust orchestration server, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network activity, system configuration for a system the application is executing on, resource utilization by the application, and integrity of the application; correlating, by the event and behavior correlation engine, risk based on the monitoring; and displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and application. 6. The method of claim 5, wherein the monitoring is performed continuously.	1. (Currently Amended) A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration

7. The method of claim 5, wherein the event and behavior correlation engine receives one or more of: system events and infection profiles from the network activity sensor; integrity measurement and verification reports of scans from the system configuration sensor; system events pertaining to processor, network, memory, and storage resource consumption from the resource utilization sensor; and system events pertaining to image profiles and local execution context from the application integrity sensor. 8. The method of claim 7, wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly. 9. The method of claim 5, wherein the plurality of runtime dashboards comprise one or more of: a global view dashboard; a system configuration dashboard; a resource utilization dashboard; an application integrity dashboard; and a network activity dashboard.	server, third party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system. 3. (Previously Presented) The method of claim 1, wherein the third party network endpoint assessments are received from an endpoint assessment service. 4. (Previously Presented) The method of claim 3, further comprising: receiving, by the trust orchestration server, integrity measurement and verification reports from the endpoint assessment service. 5. (Previously Presented) The method of claim 1, wherein the third party network endpoint assessments are received from one or more collaboration services. 6. (Previously Presented) The method of claim 5, further comprising: receiving, by the trust orchestration

	server, integrity measurement and verification reports from the one or more collaboration services. 7. (Previously Presented) The method of claim 1, wherein the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents, and the temporal events are generated by a trust broker of the trust orchestration server and are received by the system event correlator from the trust broker.

Claims **5-9** are rejected on the ground of provisional nonstatutory double patenting as being unpatentable over claims **1-6** of co-pending U.S. application **13/559,732**. Although the claims at issue are not identical, they are not patentably distinct from each other because the instant independent claim is directed to a method of orchestrating runtime operational integrity of a system executing on a computing platform using a network analyzer, an endpoint trust agent, a trust broker, a trust orchestrator to perform the steps of claimed method/system of co-pending application 13/559,732 which claims a system for providing network flow level remediation at a network element based upon a risk correlation for a computing device or an application executing on the computing device, the system comprising: a network trust agent.

Please refer to comparison table below for a better comparison of claims between claims **5-9,** of the instant application and claims **1-6** of the co-pending application 13/559,732.

13/559,707	**13/559,732**
5. A method of providing runtime operational integrity of an application and a system using a computing platform comprising a network trust agent, an endpoint trust agent, an event and behavior correlation engine, and a trust orchestration server, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network activity, system configuration for a system the application is executing on, resource utilization by the application, and integrity of the application; correlating, by the event and behavior correlation engine, risk based on the monitoring; and displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and application. 6. The method of claim 5, wherein the monitoring is performed continuously. 7. The method of claim 5, wherein the event and behavior correlation engine receives one or more of: system events and infection profiles from the network activity sensor; integrity measurement and verification reports of scans from the system configuration sensor; system events pertaining to processor, network,	1. (Currently Amended) A system for providing network flow level remediation at a network element based upon a risk correlation for a computing device or an application executing on the computing device, the system comprising: a network trust agent configured to subscribe to and receive security status posture updates and notifications of revised reputation scores for the computing device; an endpoint trust agent, on the computing device, configured to monitor local device activities and receive endpoint threat intelligence; an event and behavior correlation engine configured to correlate risk based on inputs received from a plurality of sensory inputs configured to monitor network activity of the computing device and applications executing thereon, system configuration for the computing device and applications executing thereon, resource utilization by the computing device and applications running thereon, and integrity of the computing device and applications running thereon; a trust orchestration server configured to: perform a calculus of risk on a global security context including endpoint assessment reports received from collaboration services, and

memory, and storage resource consumption from the resource utilization sensor; and system events pertaining to image profiles and local execution context from the application integrity sensor. 8. The method of claim 7, wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly. 9. The method of claim 5, wherein the plurality of runtime dashboards comprise one or more of: a global view dashboard; a system configuration dashboard; a resource utilization dashboard; an application integrity dashboard; and a network activity dashboard.	send system warnings based upon the endpoint threat intelligence to the network trust agent; and a remediation engine configured to receive real time directives for control of the computing device or applications running thereon and provide said security status posture updates and notifications of revised reputation scores for the computing device to orchestration or policy enforcement point services. 2. (Original) The system of claim 1, wherein the sensory inputs are configured to perform continuous monitoring. 3. (Original) The system of claim 1, wherein the event and behavior correlation engine are configured to receive one or more of: system events and infection profiles from the network activity sensor; integrity measurement and verification reports of scans from the system configuration sensor; system events pertaining to processor, network, memory, and storage resource consumption from the resource utilization sensor; and system events pertaining to image profiles and local execution context from the application integrity sensor. 4. (Currently Amended) The system of claim 3, wherein the scans are performed by a third party collaboration service at the application component and package level on the

	computing device to evaluate configuration, compliance, vulnerability and patch level posture per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly. 5. (Currently Amended) The system of claim 1, wherein the remediation engine is configured to perform actions on one or more of a virtual machine, a network flow controller, and a transaction. 6. (Original) The system of claim 5, wherein the actions are based on configured trigger controls.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

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 pre-AIA 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.

Claims 5-7 and 9 rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Alperovitch et al. (U.S. 2008/0175266,) in view of Njemanze et al. (U.S. 2011/0145711)

Regarding Claim 5, Alperovitch discloses "**a method of providing runtime operational integrity of an application and a system using a computing platform**" (refer to paragraph [0006] discloses systems and methods for a distributed reputation architecture are provided. A distributed reputation system can include a communications interface, a data aggregation engine, an analyzer, a correlation engine and a reputation engine. Further Figures 1, 2, and 3 discloses more detail.)

In addition discloses "**computing platform comprising a network trust agent, an endpoint trust agent, an event and behavior correlation engine, and a trust orchestration server, the method comprising**:" (refer to Figures 1, 2, and 3, further paragraphs [0031] and [0040] discloses multiple security agents 100a, 100b, which would be interpreted as an endpoint trust agent, further paragraph [0040] discloses the data can be aggregated and mined by a central system which receives identifiers and attributes associated with all entities 300a-c for which the security agents 100a, 100b

have received communications, which the central system 200 would be interpreted as a network trust agent, further paragraph [0007] discloses correlation engine that can correlate the attributes of the entities, further discloses reputation engine can identify relationships between the entities, paragraph [0030] discloses the security agent includes a reputation engine, and paragraph [0065] discloses the security agent can correlate the communication, therefore the combination of correlation engine, and reputation engine including at security agent would be interpreted as an event and behavior correlation engine, further paragraph [0065] discloses **a reputation score determinator** 745 can provide the engine for weighting 740 the aggregated reputation information 730, 735 and producing a global reputation vector. in addition paragraph [0060] discloses server 620 is operable to respond to the query with a global reputation determination. the central server can derive the global reputation using a global reputation aggregation 630, which server 620 would be interpreted as the trust orchestration server.)

Moreover discloses "**monitoring, by a plurality of sensory inputs, one or more of network activity, system configuration for a system the application is executing on, resource utilization by the application, and integrity of the application**;" (refer to paragraph [0030] discloses the security agent 100 monitors communications entering and exiting the network 110. These communications are typically received though the internet 120 from many entities 130a-f that are connected to the internet 120. Further paragraph [0033] discloses sophisticated security agents

100a-n can track entities and analyze the characteristics of the entities to help determine whether to allow a communication to enter a network 110a-n.)

Further discloses "**correlating, by the event and behavior correlation engine, risk based on the monitoring**;" paragraph [0007] discloses correlation engine that can correlate the attributes of the entities, further discloses reputation engine can identify relationships between the entities, paragraph [0030] discloses the security agent includes a reputation engine, and paragraph [0065] discloses the security agent can correlate the communication, therefore the combination of correlation engine, and reputation engine including at security agent would be interpreted as an event and behavior correlation engine, further paragraph [0065] discloses **a reputation score determinator** 745 can provide the engine for weighting 740 the aggregated reputation information 730, 735 and producing a global reputation vector. in addition paragraph [0060] discloses server 620 is operable to respond to the query with a global reputation determination. the central server can derive the global reputation using a global reputation aggregation 630, which server 620 would be interpreted as the trust orchestration server.)

Alperovitch does not explicitly disclose "**displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and application**"; however, Njemanze from similar field of endeavor discloses "**displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and**

application;" (refer to paragraph [0048] discloses view is provided through a graphical user interface (GUI). Further paragraph [0049] discloses GUI includes five configurable areas of interest: a toolbar area that contains a file menu area as well as the eve playback controls; a navigation panel that allows a user to view system assets (as well as dashboards).)

Therefore it would have been obvious to a person with ordinary skill in the art at the time the invention was made to incorporate Njemanze's technique of displaying using run-time dashboards a real time status indication for operational integrity into Alperovitch's technique with motivation to provides a centralized view into the security status of an enterprise and gives administrators, analysts, and operators an interface to perform security management tasks. Refer to Njemanze paragraph [0048]

Regarding Claim 6, in view of claim 5, Alperovitch as modified by Njemanze discloses "**wherein the monitoring is performed continuously**" (refer to Alperovitch paragraph [0093] discloses the monitoring is continuous.)

Regarding Claim 7, in view of claim 5, Alperovitch as modified by Njemanze discloses "**wherein the event and behavior correlation engine receives one or more of: system events and infection profiles from the network activity sensor; integrity measurement and verification reports of scans from the system**

configuration sensor; system events pertaining to processor, network, memory, and storage resource consumption from the resource utilization sensor; and system events pertaining to image profiles and local execution context from the application integrity sensor" (refer to Alperovitch paragraph [0007] discloses correlation engine that can correlate the attributes of the entities, further discloses reputation engine can identify relationships between the entities, paragraph [0030] discloses the security agent includes a reputation engine, and paragraph [0065] discloses the security agent can correlate the communication, therefore the combination of correlation engine, and reputation engine including at security agent would be interpreted as an event and behavior correlation engine, further paragraph [0065] discloses **a reputation score determinator** 745 can provide the engine for weighting 740 the aggregated reputation information 730, 735 and producing a global reputation vector. in addition paragraph [0060] discloses server 620 is operable to respond to the query with a global reputation determination. the central server can derive the global reputation using a global reputation aggregation 630, which server 620 would be interpreted as the trust orchestration server. Further paragraphs [0045] to [0048] disclose description about the attributes.)

Regarding Claim 9, in view of claim 5, Alperovitch as modified by Njemanze discloses "**wherein the plurality of runtime dashboards comprise one or more of: a global view dashboard; a system configuration dashboard; a resource utilization dashboard; an application integrity dashboard; and a network activity dashboard**"

(refer to Njemanze paragraph [0048] discloses view is provided through a graphical user interface (GUI). Further paragraph [0049] discloses GUI includes five configurable areas of interest: a toolbar area that contains a file menu area as well as the eve playback controls; a navigation panel that allows a user to view system assets (as well as dashboards).)

Claim 8 rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Alperovitch et al. (U.S. 2008/0175266,) in view of Njemanze et al. (U.S. 2011/0145711), further in view of Midgely et al. (U.S. Patent No. 5,604,862)

Regarding Claim 8, in view of claim 7, Alperovitch as modified by Njemanze does not explicitly disclose "**wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi- weekly, or monthly**"; however, Midgely from similar field of endeavor discloses "**wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi- weekly, or monthly**." (refer to Column 2, lines 60-63 discloses various scheduling policies are available for snapshotting: continuous scanning, at specified time of day, in response to specific system events, or on demand.)

Therefore it would have been obvious to a person with ordinary skill in the art at the time the invention was made to incorporate Midgely's technique of performing

scanning based on hourly, daily or etc. schedule into Alperovitch as modified by Njemanze's technique since the known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art.

Conclusion

Note: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or discloses by examiner.

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

Ghosh et al. (U.S. 2012.0284282,) discloses ranking and selecting entities based on calculated reputation or influence scores.

Helman et al. (U.S. 2009/0328222,) discloses mapping between users and machines in enterprise security assessment sharing system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAYED ARESH BEHESHTI SHIRAZI whose telephone number is (571)270-3396. The examiner can normally be reached on 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOSEPH P HIRL can be reached on 571-272-3685. 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.

/SAYED ARESH BEHESHTI SHIRAZI/

Examiner, Art Unit 2435

Notice of References Cited	Application/Control No. 13/559,707	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner SAYED ARESH BEHESHTI	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2008/0175266 A1	07-2008	Alperovitch et al.	370/465
*	B	US-2009/0328222 A1	12-2009	Helman et al.	726/25
*	C	US-2011/0145711 A1	06-2011	Njemanze et al.	715/736
*	D	US-8,214,497 B2	07-2012	Alperovitch et al.	709/226
*	E	US-2012/0284282 A9	11-2012	Ghosh et al.	707/748
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	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 MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	Art Unit
	SAYED BEHESHTI SHIRAZI	2435

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	25	7/1/2014	S.B
709	205, 206, 224, 226	7/1/2014	S.B
715	736	7/1/2014	S.B
345	440	7/1/2014	S.B

SEARCH NOTES		
Search Notes	Date	Examiner
Performed Inventor search	7/1/2014	S.B
Performed Assignee search	7/1/2014	S.B
Performed Double Patenting search	7/1/2014	S.B
Performed Classification search	7/1/2014	S.B
Performed CPC search	7/1/2014	S.B
Performed NPL search (Google Scholar)	7/1/2014	S.B
Performed EAST keyword search	7/1/2014	S.B
Consulted with Tod Swann 2430 QAS regarding 101, 112	7/3/2014	S.B
Consulted with Justin Rider 2430 QAS regarding 101, 112	7/3/2014	S.B

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 86 of 318

Method And Apparatus For Risk Visualization and Remediation

JS Gill, S Kakkera, IR Arora… - US Patent App. 12/ …, 2010 - Google Patents

... the right people have access to assets, eg job, certifications, background; Any suspicious **behavior** or activities; ... source systems for on need basis look up for the data, and (c) **event** mode in ... and rules **engine** 624, a controls, **risks**, and assets repository 626, an **events**, alerting and ...

Cited by 2 Related articles All 2 versions Cite Save

Magic quadrant for security information and event management

M Nicolett, KM Kavanagh - Gartner RAS Core Reasearch Note (May …, 2011 - arrowecs.ae

... Support the real-time collection and analysis of **events** from host systems, security ... CorreLog does not provide **event** source integration for third-party DLP or DAM ... integrity monitoring, operational performance monitoring functions, and some network **behavior** analysis capabilities ...

Cited by 35 Related articles All 9 versions Cite Save More

Systems, methods and devices for providing situational awareness, mitigation, risk analysis of assets, applications and infrastructure in the internet and cloud

JJ Donovan - US Patent App. 12/834,378, 2010 - Google Patents

... system of claim 56 , wherein the unauthorized usage is detected by **correlations** of unusual **behavior**. ... Meta-data and attribute data are both used for **event correlation**, for network management, and ... Finally, the analysis of a set of **correlated events** may lead to “resetting” (flip flop ...

Cited by 1 Related articles All 2 versions Cite Save

Monitoring web service event trails for business compliance

E Mulo, U Zdun, S Dustdar - Service-Oriented Computing and …, 2009 - ieeexplore.ieee.org

... **events** are recorded in audit logs (files) that can later be analyzed to identify anomalies in system **behavior**. ... **event** is fired, it is actually an instance of the ontology class representing the **event** type on ... [20] propose a framework to monitor and validate the runtime **behaviour** of web ...

Cited by 23 Related articles All 11 versions Cite Save

Driver Inattention Detection based on Eye Gaze—Road Event Correlation

L Fletcher, A Zelinsky - The international journal of robotics …, 2009 - ijr.sagepub.com

... Consistent, multitasking, servile Highly adaptable Limited programmed **behaviour** change High ambiguity and uncertainty tolerance ... Page 6. Fletcher and Zelinsky / Driver Inattention Detection based on Eye Gaze–Road **Event Correlation** 779 Fig. ... 2.5. Judging Driver **Behavior** ...

Cited by 22 Related articles All 3 versions Cite Save

Risk Analysis Engine

CM Gifford, JS Brush, MB Gabriele - US Patent App. 13/774,293, 2013 - Google Patents

... The observations are produced from **behavior** specifications that are based upon the **behavioral** patterns, estimated next occurrences or estimated probable activities. The **behavior** specifications may be based on precursor **behaviors**, indicator **behaviors**, asset-specific ...

All 2 versions Cite Save

Event Correlation Languages and Engines

FN Chase - chasegalleryconnect.org

... To **correlate** and filter this data, Veritas relies on configurable models of network and system **behavior**, called **behavior** models, for each type of ... As in the case of InCharge, the **event correlation** in the Veritas system is designed to handle only network **events**, and it does ...

Related articles Cite Save More

Event Correlation in Network Security to Reduce False Positive

MAR Zope, DR Ingle - ijcsn.com

... found neglected elements which are perhaps very useful for trends and decision-making **behavior**. ... of the path through the rule sets makes it so that **events** are may ... There are many different types of artificial intelligence, and **event correlation** techniques have been proposed ...

Related articles All 2 versions Cite Save More

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 87 of 318

Systems and methods for network flow remediation based on risk correlation
S Kumar, D Pollutro - US Patent App. 13/559,732, 2012 - Google Patents
... Irrespective of the method of break-in, the post-infection **behaviors** during the window of ... 1 , the **event** and **behavior correlation engine** 130 is also configured to receive endpoint **events** 116 of ... 400 further comprises a normalizer and collator 408 and a system **event** correlator 410 ...
All 2 versions Cite Save

Business Process Data Warehousing: Modeling and Integration Issues
U Dayal, F Casati, M Castellanos, MC Shan, N Salazar... - 2007 - Citeseer
Related articles All 2 versions Cite Save

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 88 of 318

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

BIB DATA SHEET

CONFIRMATION NO. 1767

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/559,707	07/27/2012 RULE	726	2435	0079152-000015

APPLICANTS

INVENTORS

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/641,007 05/01/2012

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/08/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /SAYED BEHESHTI SHIRAZI/ Examiner's Signature	☐ Met after Allowance S.B Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	29	14	4

ADDRESS

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404
UNITED STATES

TITLE

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

FILING FEE RECEIVED		
1500	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	"13559707"	USPAT	OR	OFF	2013/11/30 16:38
S2	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:38
S3	20273	orchestrat$3	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:39
S4	23	orchestrat$3 same security same assessment	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:39
S5	1	"20120284282"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:48
S6	0	"2009032822"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:49
S7	1	"20090328222"	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:49
S8	1	"8214497".pn.	US-PGPUB; USPAT	OR	OFF	2013/11/30 16:50
S9	1	quarantin$3 near20 (infected or attacked) same divert$3 near10 user$1 near20 transaction$1 near20 traffic	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:25
S10	1	quarantin$3 near20 (infected or attacked) same (divert$3 or direct$3 or re$1direct$3 or re$1rout$3) same user$1 same transaction$1 near20 traffic	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S11	75	quarantin$3 near20 (infected or attacked) same (divert$3 or direct$3 or re$1direct$3 or re$1rout$3) same (user$1 or transaction$1 or traffic)	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S12	45	quarantin$3 near20 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S13	45	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:27
S14	1	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic)) same ((GUI or display or monitor or screen) near10 detail$1 near10 (malware or infection or malicious or	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:28

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 90 of 318

		virus))				
S15	1	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic)) same5 ((GUI or display or monitor or screen) near10 detail$1 near10 (malware or infection or malicious or virus))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:28
S16	1	quarantin$3 near10 (infected or attacked) same ((divert$3 or direct$3 or re$1direct$3 or re$1rout$3) near5 (user$1 or transaction$1 or traffic)) same5 ((GUI or display or monitor or screen) near10 (malware or infection or malicious or virus))	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:28
S17	40	S13 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2013/12/03 14:29
S20	20	("20070143474" | "20080276317" | "6742128" | "20070185856" | "20080083039" | "7587607" | "8108536" | "20050289072" | "20120102458" | "8214497" | "20050283660" | "20090172814" | "20090178138" | "20090187988" | "20090204964" | "6990579" | "20090094584" | "20090144818" | "20090241170" | "20120216244" | "20120011590" | "8010469" | "20050138384" | "20080141027" | "20110154500" | "20110179477" | "7882221" | "7979696" | "20090133110" | "20090138939" | "20090328186" | "20110072506" | "20110276468" | "20120110174" | "7370359" | "20050132031" | "20080015808" | "20080244748" | "20100281273" | "20110173643" | "6760441" | "6996710" | "7797544" | "7984304" | "20090276204" | "20090328222" | "20120072968" | "20120137375" | "20060200680" | "20070005992" | "20110035577" | "20070174406" | "20060015942" | "7174566" | "20050132202" | "20050204404" | "20050221766" | "20080289028" | "20110185423" | "6091835" | "7013481" | "20110162073" | "20050033987" | "20120131334" | "7194759" | "7979544" | "20120260342" | "20060005009" | "20080235372" | "20090204806" | "20120084850" | "20120284282" | "6507904" | "8429454").PN.	USPAT	OR	OFF	2014/07/01 15:43
S21	74	("20070143474" | "20080276317" | "6742128" | "20070185856" | "20080083039" | "7587607" | "8108536" | "20050289072" | "20120102458" | "8214497" | "20050283660" | "20090172814" | "20090178138" | "20090187988" | "20090204964" | "6990579" | "20090094584" | "20090144818" | "20090241170" | "20120216244" | "20120011590" | "8010469" | "20050138384" | "20080141027" | "20110154500" | "20110179477" | "7882221" | "7979696" | "20090133110" | "20090138939" | "20090328186" | "20110072506" | "20110276468" | "20120110174" | "7370359"	US-PGPUB; USPAT	OR	OFF	2014/07/01 15:49

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 91 of 318

		| "20050132031" | "20080015808" | "20080244748" | "20100281273" | "20110173643" | "6760441" | "6996710" | "7797544" | "7984304" | "20090276204" | "20090328222" | "20120072968" | "20120137375" | "20060200680" | "20070005992" | "20110035577" | "20070174406" | "20060015942" | "7174566" | "20050132202" | "20050204404" | "20050221766" | "20080289028" | "20110185423" | "6091835" | "7013481" | "20110162073" | "20050033987" | "20120131334" | "7194759" | "7979544" | "20120260342" | "20060005009" | "20080235372" | "20090204806" | "20120084850" | "20120284282" | "6507904" | "8429454").PN.				
S22	8	(dashboard or GUI) near10 display$3 near10 integrity near10 (application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:05
S23	0	(dashboard or GUI) same (real$1time or live) same display$3 near10 integrity near10 (application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S24	11	(dashboard or GUI) same (real$1time or live) same display$3 same integrity same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S25	234	(dashboard or GUI) same (real$1time or live) same display$3 same status same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S26	26	(dashboard or GUI) same (real$1time or live) same display$3 same status same (integrity or risk or security) same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S27	22	S26 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:06
S28	35	(dashboard or GUI) same (real$1time or live) same display$3 same (status or state) same (integrity or risk or security) same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:46
S29	15	(plurality or many or multiple or multi) same (dashboard$1 or GUI$1) same (real$1time or live) same display$3 same (status or state) same (integrity or risk or security) same(application$1 or app$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:46
S30	9	S29 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:46
S31	63	(risk near20 score) same engine same (correlat$3 or aggregat$3)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:48
S32	4	(risk near20 score) same engine same (correlat$3 or aggregat$3) same (sensor$1 or agent$1)	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:48
S33	3	S32 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/01 16:51
S34	1746	726/25.ccls.	USPAT	OR	OFF	2014/07/01 17:05

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 92 of 318

S35	26706	709/205,206,224,226.ccls.	USPAT	OR	OFF	2014/07/01 17:06
S36	734	715/736.ccls.	USPAT	OR	OFF	2014/07/01 17:06
S37	1595	345/440.ccls.	USPAT	OR	OFF	2014/07/01 17:06
S38	0	(security adj agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (correlat$3 or aggregat$3) same risk same (score or number)	USPAT	OR	OFF	2014/07/01 17:08
S39	0	(security adj agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (correlat$3 or aggregat$3) same risk same (score or number)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:08
S40	0	(security adj agent$1) same (sens$3 or monitor$3) same (correlat$3 or aggregat$3) same risk same (score or number)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:09
S41	21	(security adj agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1)	USPAT	OR	OFF	2014/07/01 17:09
S42	2452	(agent$1) same (sens$3 or monitor$3) same (event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1)	USPAT	OR	OFF	2014/07/01 17:10
S43	3740	(agent$1) same (sens$3 or monitor$3) same (activity event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1)	USPAT	OR	OFF	2014/07/01 17:10
S44	4	(agent$1) same (sens$3 or monitor$3) same (activity event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1) same2 (risk adj (score or number))	USPAT	OR	OFF	2014/07/01 17:10
S45	11	(agent$1) same (sens$3 or monitor$3) same (activity event$1 or behavior$1) same (application$1 or app$1 or program$1 or software$1) same2 (risk adj (score or number))	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:10
S46	8	S45 AND ((G06F21/316 OR G06F21/577 OR G06F19/3431 OR G06F21/552 OR H04L63/14 OR H04L63/20).CPC.)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:15
S47	8	S31 AND ((G06F21/316 OR G06F21/577 OR G06F19/3431 OR G06F21/552 OR H04L63/14 OR H04L63/20).CPC.)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:17
S48	5	S25 AND ((G06F21/316 OR G06F21/577 OR G06F19/3431 OR G06F21/552 OR H04L63/14 OR H04L63/20).CPC.)	US-PGPUB; USPAT	OR	OFF	2014/07/01 17:17
S49	1	"20080175266"	USPAT	OR	OFF	2014/07/01 22:09
S50	3	"20080175266"	US-PGPUB; USPAT	OR	OFF	2014/07/01 22:09
S51	0	(scan$3 same per same schedule) same behavior$2 same risk$1	USPAT	OR	OFF	2014/07/02 18:56
S52	1	(scan$3 same per same schedule) same behavior$2 same risk$1	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:56

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 93 of 318

S53	0	(scan$3 same schedule same (hour$2 or Day or daily or week$2 or monthly)) same behavior$2 same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:58
S54	12	(scan$3 same (hour$2 or Day or daily or week$2 or monthly)) same behavior$2 same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:59
S55	12	(scan$4 same (hour$2 or Day or daily or week$2 or monthly)) same behavior$2 same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 18:59
S56	85	(scan$4 same (hour$2 or Day or daily or week$2 or monthly)) same (behavior$2 or risk or event or anomaly or abnormal$3) same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:00
S57	79	S56 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:01
S58	2	(scan$4 near4 (hour$2 or Day or daily or week$2 or monthly)) same (behavior$2 or risk or event or anomaly or abnormal$3) same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:02
S59	22	(scan$4 near4 (hour$2 or Day or daily or week$2 or monthly)) same network same (node$1 or entit$3 or terminal$1)	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:03
S60	18	S59 and @AD < "20120727"	US-PGPUB; USPAT	OR	OFF	2014/07/02 19:03
S61	0	"13559707"	USPAT	OR	OFF	2014/07/03 09:51
S62	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2014/07/03 09:51
S63	17	"KUMAR, Srinivas".in.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:26
S64	18	"Pollutro, Dennis".in.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:26
S65	29	S63 or S64	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:26
S66	7	"TAASERA, INC".as.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:44
S67	7	"TAASERA".as.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:44
S68	74	("20070143474" | "20080276317" | "6742128" | "20070185856" | "20080083039" | "7587607" | "8108536" | "20050289072" | "20120102458" | "8214497" | "20050283660" | "20090172814" | "20090178138" | "20090187988" | "20090204964" | "6990579" | "20090094584" | "20090144818" |	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:57

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 94 of 318

		"20090241170" | "20120216244" | "20120011590" | "8010469" | "20050138384" | "20080141027" | "20110154500" | "20110179477" | "7882221" | "7979696" | "20090133110" | "20090138939" | "20090328186" | "20110072506" | "20110276468" | "20120110174" | "7370359" | "20050132031" | "20080015808" | "20080244748" | "20100281273" | "20110173643" | "6760441" | "6996710" | "7797544" | "7984304" | "20090276204" | "20090328222" | "20120072968" | "20120137375" | "20060200680" | "20070005992" | "20110035577" | "20070174406" | "20060015942" | "7174566" | "20050132202" | "20050204404" | "20050221766" | "20080289028" | "20110185423" | "6091835" | "7013481" | "20110162073" | "20050033987" | "20120131334" | "7194759" | "7979544" | "20120260342" | "20060005009" | "20080235372" | "20090204806" | "20120084850" | "20120284282" | "6507904" | "8429454").PN.				
S69	1	(security and end$1point and network and integrity and application and behavior and engine and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:59
S70	1	(security and end$1point and network and integrity and behavior and engine and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:59
S71	1	(security and end$1point and network and integrity and behavior and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 11:59
S72	4	(security and network and integrity and behavior and correlation).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S73	7	(security and network and integrity and behavior and correlat$3).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S74	78	(security and network and behavior and correlat$3).clm.	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S75	0	S68 and S74	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:00
S76	1	S67 and S74	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:01
S77	29	S63 or S64	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:01
S78	1	S77 and S74	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:01
S79	1	"13559707"	US-PGPUB; USPAT	OR	OFF	2014/07/03 12:13

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S18	0	"13559707"	USPAT; UPAD	OR	OFF	2014/03/25 11:12
S19	1	"13559707"	US-PGPUB; USPAT; UPAD	OR	OFF	2014/03/25 11:12

7/3/2014 5:10:32 PM
C:\Users\sbeheshtishirazi\Documents\EAST\Workspaces\13559707.wsp

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 96 of 318

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	6742128	B1	2004-05-25	JOINER	
	2	7174566	B2	2007-02-06	YADAV	
	3	7370359	B2	2008-05-06	HRABIK et al.	
	4	8010469	B2	2011-08-30	KAPOOR et al.	
	5	8214497	B2	2012-07-03	ALPEROVITCH 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	20060015942	A1	2006-01-19	JUDGE et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Receipt date: 09/19/2013	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
(**Not for submission under 37 CFR 1.99)**	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

	2	20080276317	A1	2008-11-06	CHANDOLA et al.	
	3	20090328222	A1	2009-12-31	HELMAN et al.	
	4	20110072506	A1	2011-03-24	LAW et al.	
	5	20110162073	A1	2011-06-30	JESCHKE et al.	
	6	20110276468	A1	2011-11-10	LEWIS et al.	
	7	20120011590	A1	2012-01-12	DONOVAN	
	8	20120072968	A1	2012-03-22	WYSOPAL et al.	
	9	20120102458	A1	2012-04-26	MEIJER et al.	
	10	20120110174	A1	2012-05-03	WOOTTON et al.	
	11	20120137375	A1	2012-05-31	RAMACHANDRAN et al.	
	12	20120260342	A1	2012-10-11	DUBE et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Receipt date: 09/19/2013	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	20110027386	KR	A	2011-03-16	MOZENSOFT INC.		☒

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	Norton Antivirus Product Manual Copyright 2011 Symantec Corporation, 334 pp	☐
	2	J. Andrew Schafer "Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events", msdn magazine, http://msdn.microsoft.com/en-us/magazine/cc301317.aspx, September 2001, 5 pp	☐
	3	AUBREY-DERRICK SCHMIDT et al. "Static Analysis of Executables for Collaborative Malware Detection on Android" ICC'09 Proceedings of the 2009 IEEE International Conference on Communications, 5 pp	☐
	4	International Search Report and Written Opinion dated August 27, 2013, issued in corresponding International Application No. PCT/US2013/039033, 16 pp	☐
	5	Office Action issued in copending U.S. Patent Application No. 13/559,732, mailed June 20, 2013, 32 pp	☐
	6	Office Action issued in copending U.S. Patent Application No. 13/559,766, mailed July 18, 2013, 39 pp	☐

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Receipt date: 09/19/2013	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

EXAMINER SIGNATURE			
Examiner Signature	/Sayed Aresh Beheshti Shirazi/	Date Considered	07/03/2014

*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. /S.B./

Receipt date: 09/19/2013	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	/Jennifer A. Wilson/	Date (YYYY-MM-DD)	2013-09-19
Name/Print	Jennifer A. Wilson	Registration Number	62,604

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. /S.B./

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. /S.B./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed
PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

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					
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	20050289072	A1	2005-12-29	Sabharwal	
	2	20070143474	A1	2007-06-21	Sheng et al.	
	3	20070174406	A1	2007-07-26	Morris et al.	
	4	20090094584	A1	2009-04-09	Dheap et al.	
	5	20090144818	A1	2009-06-04	Kumar et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Receipt date: 11/09/2012	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

	6	20090138939	A1	2009-05-28	Kumar et al.	
	7	20090276204	A1	2009-11-05	Kumar et al.	
	8	20090241170	A1	2009-09-24	Kumar et al.	
	9	20090133110	A1	2009-05-21	Kumar et al.	
	10	20090328186	A1	2009-12-31	Pollutro et al.	
	11	20120216244	A1	2012-08-23	Kumar 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

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]

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Receipt date: 11/09/2012	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

	1		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Sayed Aresh Beheshti Shirazi/	Date Considered	07/03/2014

*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. /S.B./

Receipt date: 11/09/2012	Application Number	13559707 13559707 - GAU: 2435
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

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	/ R. K. Baldwin /	Date (YYYY-MM-DD)	2012-11-09
Name/Print	Randall K. Baldwin	Registration Number	59713

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. /S.B./

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. /S.B./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP IDS**
Kumar, Srinivas et al.	Group Art Unit: 2431
Application No.: 13/559,707	Examiner:
Filed: July 27, 2012	Confirmation No.: 1767
For: Systems and Methods for Orchestrating Runtime Operational Integrity	

INFORMATION DISCLOSURE STATEMENT

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

Madam:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

Pursuant to 37 C.F.R. § 1.98, a copy of each of the documents cited is enclosed. However, copies of the listed U.S. patents and U.S. patent application publications are not enclosed since it is no longer required.

The documents are being submitted within three (3) months of the filing or entry of the national stage of this application or before the first Office Action on the merits, whichever is later. Since these documents are being filed within the time period set forth in 37 C.F.R. § 1.97(b), no fee or statement is required.

To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: January 24, 2014

By: Derek P. Benke
Derek P. Benke
Registration No. 56,944

Customer No. 21839
703 836 6620

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,707**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
(Use as many sheets as necessary)				*Art Unit*	**2431**
				Examiner Name	
Sheet	1	of	3	*Attorney Docket Number*	**0079152-000015**

U.S. PATENT DOCUMENTS					
Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,091,835	7/18/2000	Smithies et al.	
		US-6,507,904 B1	1/14/2003	Ellison et al.	
		US-6,760,441 B1	7/6/2004	Ellison et al.	
		US-6,990,579 B1	1/24/2006	Herbert et al.	
		US-6,996,710 B1	2/7/2006	Ellison et al.	
		US-7,013,481 B1	3/14/2006	Ellison et al.	
		US-7,194,759 B1	3/20/2007	Chess et al.	
		US-7,587,607 B2	9/8/2009	Brickell et al.	
		US-7,797,544 B2	9/14/2010	Dillaway et al.	
		US-7,882,221 B2	2/1/2011	Sailer et al.	
		US-7,979,696 B2	7/12/2011	Kim et al.	
		US-7,984,304 B1	7/19/2011	Waldspurger et al.	
		US-8,108,536 B1	1/31/2012	Hernacki et al.	
		US-8,429,454 B2	4/23/2013	Yuan et al.	
		US-2005/0033987 A1	2/10/2005	Yan et al.	
		US-2005/0132202 A1	6/16/2005	Dillaway et al.	
		US-2005/0132031 A1	6/16/2005	Sailer et al.	
		US-2005/0138384 A1	6/23/2005	Brickell et al.	
		US-2005/0204404 A1	9/15/2005	Hrabik et al.	
		US-2005/0221766 A1	10/6/2005	Brizek et al.	
		US-2005/0283660 A1	12/22/2005	McKeen et al.	
		US-2006/0005009 A1	1/5/2006	Ball et al.	
		US-2006/0200680 A1	9/7/2006	Ellison et al.	
		US-2007/0005992 A1	1/4/2007	Schluessler et al.	
		US-2007/0185856 A1	8/9/2007	Mittal et al.	
		US-2008/0015808 A1	1/17/2008	Wilson et al.	
		US-2008/0083039 A1	4/3/2008	Choi et al.	
		US-2008/0141027 A1	6/12/2008	Kim et al.	
		US-2008/0235372 A1	9/25/2008	Sailer et al.	
		US-2008/0244748 Al	10/2/2008	Neystadt et al.	
		US-2008/0289028 A1	11/20/2008	Jansen et al.	
		US-2009/0172814 A1	7/2/2009	Khosravi et al.	
		US-2009/0178138 A1	7/9/2009	Weiss et al.	
		US-2009/0187988 A1	7/23/2009	Hulten et al.	
		US-2009/0204806 A1	8/13/2009	Kanemura et al.	
		US-2009/0204964 A1	8/13/2009	Foley et al.	
		US-2010/0281273 A1	11/4/2010	Lee et al.	
		US-2011/0035577 A1	2/10/2011	Lin et al.	

Examiner Signature	/Sayed Aresh Beheshti Shirazi/	Date Considered	07/03/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,707**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
(Use as many sheets as necessary)				*Art Unit*	**2431**
				Examiner Name	
Sheet	2	of	3	*Attorney Docket Number*	**0079152-000015**

U.S. PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2011/0154500 A1	6/23/2011	Sahita et al.	
		US-2011/0173643 A1	7/14/2011	Nicolson et al.	
		US-2011/0179477	7/21/2011	Starnes et al.	
		US-2011/0185423 A1	7/28/2011	Sallam	
		US-2012/0084850 A1	4/5/2012	Novak et al.	
		US-2012/0131334 A1	5/24/2012	Haikney et al.	
		US-2012/0284282 A9	11/8/2012	Ghosh et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		December 5, 2013 Office Action issued in U.S. Application No. 13/559,665.	
		December 10, 2013 Office Action issued in U.S. Application No. 13/559,732.	
		October 23, 2013 Office Action issued in U.S. Application No. 13/559,692.	
		January 17, 2014 Office Action issued in U.S. Application No. 13/559,766.	
		Event Tracker ver 7.0 Enterprise Users Guide. "Event Tracker ver 7.0 Enterprise User's; Guide. Prism Microsystems, 28 July 2010. Web. 29 Nov. 2013 <http://www.eventtracker.com/wp-content/uploads/EventTracker-v7.0-Enterprise-User-Guide.pdf>.	
		Statement of FIPS 140-2 Compliance. "Statement of FIPS 140-2 Compliance. Prism Microsystems, 6 Oct. 2010. Web 29 Nov. 2010. ,http://www.eventtracker.com/wp-content/uploads/2013/01/EventTracker_v7.0_FIPS_Compliance.pdf>.	
		Trend Micro, Inc.. "OfficeScan 10 Administrator/s Guide." docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf. N.p. 20 Apr. 2009. Web. 27 Nov. 2013 http://docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf.	
		August 27, 2012 International Search Report issued in PCT/US2012/025551.	
		August 27, 2012 Written Opinion issued in PCT/US2012/025551.	

Examiner Signature	/Sayed Aresh Beheshti Shirazi/	Date Considered	07/03/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,707**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
(Use as many sheets as necessary)				*Art Unit*	**2431**
				Examiner Name	
Sheet	3	of	3	*Attorney Docket Number*	**0079152-000015**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		August 21, 2013 International Preliminary Report on Patentability issued in PCT/US2012/025551.	

Examiner Signature	/Sayed Aresh Beheshti Shirazi/	Date Considered	07/03/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.B./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	Art Unit
	SAYED BEHESHTI SHIRAZI	2435

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

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

CLAIM		DATE								
Final	Original	03/25/2014	07/01/2014							
	1	÷	N							
	2	÷	N							
	3	÷	N							
	4	÷	N							
	5	÷	✓							
	6	÷	✓							
	7	÷	✓							
	8	÷	✓							
	9	÷	✓							
	10	÷	N							
	11	÷	N							
	12	÷	N							
	13	÷	N							
	14	÷	N							

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 112 of 318

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Kumar, Srinivas et al.	Group Art Unit: 2435
Application No.: 13/559,707	Examiner: Beheshti Shirazi, Sayed Aresh
Filed: July 27, 2012	Confirmation No.: 1767
For: Systems and Methods for Orchestrating Runtime Operational Integrity	

RESPONSE TO ELECTION OF SPECIES REQUIREMENT

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

Madam:

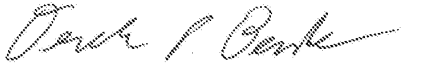
In response to the Election of Species Requirement dated April 11, 2014, Applicants elect without traverse Species III, Claims 5-9, for further examination on the merits. Applicants reserve the right to file one or more divisional applications directed to the non-elected species.

Accordingly, examination on the merits of Claims 5-9 is believed to be in order and an early and favorable action is respectfully requested. Should the Examiner have any comments or suggestions, he is invited to contact the undersigned at the number listed below.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date April 28, 2014 By: 

Derek P. Benke
Registration No. 56,944

Customer No. 21839
703 836 6620
Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

Electronic Acknowledgement Receipt

EFS ID:	18875492
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna Lloyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000015
Receipt Date:	28-APR-2014
Filing Date:	27-JUL-2012
Time Stamp:	14:35:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response to Election / Restriction Filed	Response.pdf	466444 fa0cca541ad7df05a5f02c4638f57d19b1a89178	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	466444

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.

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.
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015	1767

21839 7590 04/11/2014

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
BEHESHTI SHIRAZI, SAYED ARESH	
ART UNIT	**PAPER NUMBER**
2435	

NOTIFICATION DATE	DELIVERY MODE
04/11/2014	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):

ADIPDOC1@BIPC.com

Office Action Summary	Application No. 13/559,707	Applicant(s) KUMAR ET AL.	
	Examiner SAYED ARESH BEHESHTI SHIRAZI	Art Unit 2435	AIA (First Inventor to File) Status No

-- 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 2 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 *07/27/2012*.

☐ 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) *1-14* 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) _____ is/are rejected.

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

9)☒ Claim(s) *1-14* 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 _____ 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 _____.

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

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

Election/Restrictions

This application contains claims directed to the following patentably distinct species:

Species I: Figure 1 associates with claims 1-3.

Species II: Figures 4 and 5 associate with claim 4.

Species III: Figures 2 and 13 associate with claims 5-9.

Species IV: Figures 23 and 24 associate with claims 10-14

The species are independent or distinct because **species I** discloses continuously monitor and dynamically analyze events and network activity to ascertain the integrity of a monitored system..., whereas **species II** discloses a method for orchestrating runtime operational integrity, a data flow for consolidating and normalizing network endpoint assessments as part of a configuration for an exemplary attestation system 400. The exemplary attestation system 400 includes a trust orchestrator 430, a trust broker 407 configured to receive integrity reports 406 published by endpoint assessment services 401. the method comprising: determining, by the network analyzer, anomalies based on network activity correlation and network malware detection; determining, by the trust broker, system configuration anomalies based on system level normalization and collation of assessments; determining, by the endpoint trust agent, resource utilization anomalies based on rule-sets or alert expressions

associated with processor, memory, and network resource usage; determining, by the endpoint trust agent, at least one application integrity anomaly based on rulesets or alert expressions associated with static and dynamic image analysis…, whereas **species III** discloses system for endpoint and network activity correlation. In particular, the system shown in FIG. 2 is configured to receive inputs for endpoint events, correlate the events, and generate outputs such as, but not limited to, warnings and reports, whereas **species IV** discloses an entity-relationship diagram (ERD) illustrating relationships between entities of a reputation scoring system, according to an embodiment of the present disclosure; FIG. 24 illustrates a hierarchical representation of a subject reputation score, according to an embodiment of the present disclosure.

The species are independent or distinct because claims to the different species recite the mutually exclusive characteristics of such species. In addition, these species are not obvious variants of each other based on the current record.

Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable.

There is an examination and search burden for these patentably distinct species due to their mutually exclusive characteristics. The species require a different field of search (e.g., searching different classes/subclasses or electronic resources, or employing different search queries); and/or the prior art applicable to one species would not likely be applicable to another species; and/or the species are likely to raise different non-prior art issues under 35 U.S.C. 101 and/or 35 U.S.C. 112, first paragraph.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a species or a grouping of patentably indistinct species to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected species or grouping of patentably indistinct species**, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.

The election may be made with or without traverse. To preserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the election of species requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable on the elected species or grouping of patentably indistinct species.

Should applicant traverse on the ground that the species, or groupings of patentably indistinct species from which election is required, are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing them to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the species unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other species.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which depend from or otherwise require all the limitations of an allowable generic claim as provided by 37 CFR 1.141.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAYED ARESH BEHESHTI SHIRAZI whose telephone number is (571)270-3396. The examiner can normally be reached on 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOSEPH P HIRL can be reached on 571-272-3685. 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.

/SAYED ARESH BEHESHTI SHIRAZI/

Examiner, Art Unit 2435

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559707	KUMAR ET AL.
	Examiner	Art Unit
	SAYED BEHESHTI SHIRAZI	2435

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

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

CLAIM		DATE								
Final	Original	03/25/2014								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 123 of 318

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of Kumar, Srinivas Application No.: 13/559,707 Filed: July 27, 2012 For: Systems and Methods for Orchestrating Runtime Operational Integrity	**MAIL STOP** Group Art Unit: 2435 Examiner: BEHESHTI SHIRAZI, Sayed Aresh Confirmation No.: 1767

ASSERTION UNDER 37 C.F.R. § 1.27(c) OF ENTITLEMENT TO CLAIM SMALL ENTITY STATUS

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

Madam:

Applicant is entitled to claim status as a small entity. The undersigned is a party authorized to sign under 37 C.F.R. § 1.33(b).

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 14, 2014

By: _____
Derek P. Benke
Registration No. 56944

Customer No. 21839
703 836 6620

Electronic Acknowledgement Receipt	
EFS ID:	18478423
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna Lloyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000015
Receipt Date:	14-MAR-2014
Filing Date:	27-JUL-2012
Time Stamp:	15:28:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assertion of entitlement to small entity status	SMALLENTITY.pdf	281040 b4a696e8bc03ec54aacfe84f7de699a5e7d2fb50	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	281040

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP IDS**
Kumar, Srinivas et al.	Group Art Unit: 2431
Application No.: 13/559,707	Examiner:
Filed: July 27, 2012	Confirmation No.: 1767
For: Systems and Methods for Orchestrating Runtime Operational Integrity	

INFORMATION DISCLOSURE STATEMENT

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

Madam:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

Pursuant to 37 C.F.R. § 1.98, a copy of each of the documents cited is enclosed. However, copies of the listed U.S. patents and U.S. patent application publications are not enclosed since it is no longer required.

The documents are being submitted within three (3) months of the filing or entry of the national stage of this application or before the first Office Action on the merits, whichever is later. Since these documents are being filed within the time period set forth in 37 C.F.R. § 1.97(b), no fee or statement is required.

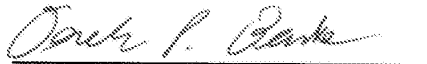
To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: January 24, 2014

By: 
Derek P. Benke
Registration No. 56,944

Customer No. 21839
703 836 6620

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,707**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
(Use as many sheets as necessary)				*Art Unit*	**2431**
				Examiner Name	
Sheet	1	of	3	*Attorney Docket Number*	**0079152-000015**

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,091,835	7/18/2000	Smithies et al.	
		US-6,507,904 B1	1/14/2003	Ellison et al.	
		US-6,760,441 B1	7/6/2004	Ellison et al.	
		US-6,990,579 B1	1/24/2006	Herbert et al.	
		US-6,996,710 B1	2/7/2006	Ellison et al.	
		US-7,013,481 B1	3/14/2006	Ellison et al.	
		US-7,194,759 B1	3/20/2007	Chess et al.	
		US-7,587,607 B2	9/8/2009	Brickell et al.	
		US-7,797,544 B2	9/14/2010	Dillaway et al.	
		US-7,882,221 B2	2/1/2011	Sailer et al.	
		US-7,979,696 B2	7/12/2011	Kim et al.	
		US-7,984,304 B1	7/19/2011	Waldspurger et al.	
		US-8,108,536 B1	1/31/2012	Hernacki et al.	
		US-8,429,454 B2	4/23/2013	Yuan et al.	
		US-2005/0033987 A1	2/10/2005	Yan et al.	
		US-2005/0132202 A1	6/16/2005	Dillaway et al.	
		US-2005/0132031 A1	6/16/2005	Sailer et al.	
		US-2005/0138384 A1	6/23/2005	Brickell et al.	
		US-2005/0204404 A1	9/15/2005	Hrabik et al.	
		US-2005/0221766 A1	10/6/2005	Brizek et al.	
		US-2005/0283660 A1	12/22/2005	McKeen et al.	
		US-2006/0005009 A1	1/5/2006	Ball et al.	
		US-2006/0200680 A1	9/7/2006	Ellison et al.	
		US-2007/0005992 A1	1/4/2007	Schluessler et al.	
		US-2007/0185856 A1	8/9/2007	Mittal et al.	
		US-2008/0015808 A1	1/17/2008	Wilson et al.	
		US-2008/0083039 A1	4/3/2008	Choi et al.	
		US-2008/0141027 A1	6/12/2008	Kim et al.	
		US-2008/0235372 A1	9/25/2008	Sailer et al.	
		US-2008/0244748 Al	10/2/2008	Neystadt et al.	
		US-2008/0289028 A1	11/20/2008	Jansen et al.	
		US-2009/0172814 A1	7/2/2009	Khosravi et al.	
		US-2009/0178138 A1	7/9/2009	Weiss et al.	
		US-2009/0187988 A1	7/23/2009	Hulten et al.	
		US-2009/0204806 A1	8/13/2009	Kanemura et al.	
		US-2009/0204964 A1	8/13/2009	Foley et al.	
		US-2010/0281273 A1	11/4/2010	Lee et al.	
		US-2011/0035577 A1	2/10/2011	Lin et al.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,707**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
(Use as many sheets as necessary)				*Art Unit*	**2431**
				Examiner Name	
Sheet	2	of	3	*Attorney Docket Number*	**0079152-000015**

U.S. PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2011/0154500 A1	6/23/2011	Sahita et al.	
		US-2011/0173643 A1	7/14/2011	Nicolson et al.	
		US-2011/0179477	7/21/2011	Starnes et al.	
		US-2011/0185423 A1	7/28/2011	Sallam	
		US-2012/0084850 A1	4/5/2012	Novak et al.	
		US-2012/0131334 A1	5/24/2012	Haikney et al.	
		US-2012/0284282 A9	11/8/2012	Ghosh et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		December 5, 2013 Office Action issued in U.S. Application No. 13/559,665.	
		December 10, 2013 Office Action issued in U.S. Application No. 13/559,732.	
		October 23, 2013 Office Action issued in U.S. Application No. 13/559,692.	
		January 17, 2014 Office Action issued in U.S. Application No. 13/559,766.	
		Event Tracker ver 7.0 Enterprise Users Guide. "Event Tracker ver 7.0 Enterprise User's; Guide. Prism Microsystems, 28 July 2010. Web. 29 Nov. 2013 <http://www.eventtracker.com/wp-content/uploads/EventTracker-v7.0-Enterprise-User-Guide.pdf>.	
		Statement of FIPS 140-2 Compliance. "Statement of FIPS 140-2 Compliance. Prism Microsystems, 6 Oct. 2010. Web 29 Nov. 2010. ,http://www.eventtracker.com/wp-content/uploads/2013/01/EventTracker_v7.0_FIPS_Compliance.pdf>.	
		Trend Micro, Inc.. "OfficeScan 10 Administrator/s Guide." docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf. N.p. 20 Apr. 2009. Web. 27 Nov. 2013 http://docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf.	
		August 27, 2012 International Search Report issued in PCT/US2012/025551.	
		August 27, 2012 Written Opinion issued in PCT/US2012/025551.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)* Sheet 3 of 3	*Complete if Known*	
	Application Number	**13/559,707**
	Filing Date	**July 27, 2012**
	First Named Inventor	**Kumar, Srinivas**
	Art Unit	**2431**
	Examiner Name	
	Attorney Docket Number	**0079152-000015**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		August 21, 2013 International Preliminary Report on Patentability issued in PCT/US2012/025551.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
0079152-0003		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)

Applicant

TAASERA, INC. et al

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of **3** sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of :
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. **1**
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 131 of 318

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/025551

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/22; G06F 15/16; G06F 15/173; G06F 9/44; G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: application, attestation, runtime, execute, server, remote, security, digital, sign, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007 See paragraphs [0024] - [0054]; figures 3-5.	1-26
A	US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005 See paragraphs [0110] - [0214]; figures 1,3.	1-26
A	US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009 See paragraphs [0017] - [0036]; figure 1-2.	1-26
A	US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007 See paragraphs [0033] - [0041], [0055] - [0067]; figures 2,4.	1-26

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JULY 2012 (30.07.2012)	**27 AUGUST 2012 (27.08.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Shin Sang Gil Telephone No. 82-42-481-8480

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2012/025551

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0143474 A1	21.06.2007	None	
US 2005-0289072 A1	29.12.2005	None	
US 2009-0094584 A1	09.04.2009	None	
US 2007-0174406 A1	26.07.2007	EP 1818850 A1 US 7574479 B2	15.08.2007 11.08.2009

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 133 of 318

PCT/US2012/025551

URGENT

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:

WIELAND CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC P. O. BOX 1404
ALEXANDRIA VA 22313-1404 USA

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 27 AUGUST 2012 (27.08.2012)
Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. **PCT/US2012/025551**	International filing date *(day/month/year)* **17 FEBRUARY 2012 (17.02.2012)**
Applicant **TAASERA, INC. et al**	

BUCHANAN INGERSOLL PC AUG 30 2012 LINKED

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 . 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer COMMISSIONER Telephone No. 82-42-481-8754

Form PCT/ISA/220 (July 2010)

* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

http://www.kipo.go.kr/en/ => PCT Services => PCT Services

ID : PCT international application number
PW : **9BZF99MH**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: http://www.ipkcenter.com
Email: ipkc@ipkcenter.com
Phone: +1 703 388 1066
Fax: +1 703 388 1084

Notes to Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
0079152-0003		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)
Applicant		
TAASERA, INC. et al		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 136 of 318

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/025551

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/22; G06F 15/16; G06F 15/173; G06F 9/44; G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: application, attestation, runtime, execute, server, remote, security, digital, sign, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007 See paragraphs [0024] - [0054]; figures 3-5.	1-26
A	US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005 See paragraphs [0110] - [0214]; figures 1,3.	1-26
A	US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009 See paragraphs [0017] - [0036]; figure 1-2.	1-26
A	US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007 See paragraphs [0033] - [0041], [0055] - [0067]; figures 2,4.	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JULY 2012 (30.07.2012)	**27 AUGUST 2012 (27.08.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Shin Sang Gil Telephone No. 82-42-481-8480

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2012/025551

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0143474 A1	21.06.2007	None	
US 2005-0289072 A1	29.12.2005	None	
US 2009-0094584 A1	09.04.2009	None	
US 2007-0174406 A1	26.07.2007	EP 1818850 A1 US 7574479 B2	15.08.2007 11.08.2009

Form PCT/ISA/210 (patent family annex) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC P. O. BOX
1404 ALEXANDRIA VA 22313-1404 USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	**27 AUGUST 2012 (27.08.2012)**
Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

Applicant

TAASERA, INC. et al

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	30 JULY 2012 (30.07.2012)	Shin Sang Gil Telephone No.82-42-481-8480

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioanl copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 140 of 318

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-26	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-26	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007
D2: US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005
D3: US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009
D4: US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007

1. Novelty and Inventive Step

1.1. Claims 1-12

The subject matter of claim 1 differs from these prior art documents in that the method of claim 1 includes steps of generating, by an attestation server, a report indicating security risks associated with an application based on a received runtime execution context and a received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 1 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 2-12 are dependent on claim 1 and therefore meet the requirements of PCT Article 33(2) and (3).

1.2. Claims 13-16

The subject matter of claim 13 differs from these prior art documents in that the non-transitory computer readable medium of claim 13 includes step of receiving and validating, by the attestation server form a server in a client server transaction or from a first peer in a peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 13 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

(Continued on Supplemental Box)

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 141 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of :

Box V

Claims 14-16 are dependent on claim 13 and therefore meet the requirements of PCT Article 33(2) and (3).

1.3. Claims 17-20
The subject matter of claim 17 differs from these prior art documents in that the method of claim 17 includes steps of generating assertions based on a received security context and a received local execution context; transmitting confidence metrics in a report to an identity provider; and providing attestation of a running web application or web servlet as a digital icon for rendering by a web browser. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 17 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 18-20 are dependent on claim 17 and therefore meet the requirements of PCT Article 33(2) and (3).

1.4. Claim 21-26
The subject matter of claim 21 differs from these prior art documents in that the system of claim 21 includes steps of requesting and receiving dynamic assertions form a metadata repository of an attestation service, a dynamic assertions pertaining to a local execution context an introspected security context of running application instances on instrumented target platforms; continuously displaying the dynamic assertions to a system administrator. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 21 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 22-26 are dependent on claim 21 and therefore meet the requirements of PCT Article 33(2) and (3).

2. Industrial Applicability
Claims 1-26 are industrially applicable under PCT Article 33(4).

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 142 of 318

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2012/025551	International filing date *(day/month/year)* 17 February 2012 (17.02.2012)	Priority date *(day/month/year)* 17 February 2011 (17.02.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TAASERA, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 21 August 2013 (21.08.2013)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Yukari Nakamura e-mail: pt07.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC P. O. BOX
1404 ALEXANDRIA VA 22313-1404 USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	**27 AUGUST 2012 (27.08.2012)**
Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

Applicant

TAASERA, INC. et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	30 JULY 2012 (30.07.2012)	Shin Sang Gil Telephone No.82-42-481-8480

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioanl copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 145 of 318

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-26	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-26	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007
D2: US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005
D3: US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009
D4: US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007

1. Novelty and Inventive Step

1.1. Claims 1-12

The subject matter of claim 1 differs from these prior art documents in that the method of claim 1 includes steps of generating, by an attestation server, a report indicating security risks associated with an application based on a received runtime execution context and a received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 1 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 2-12 are dependent on claim 1 and therefore meet the requirements of PCT Article 33(2) and (3).

1.2. Claims 13-16

The subject matter of claim 13 differs from these prior art documents in that the non-transitory computer readable medium of claim 13 includes step of receiving and validating, by the attestation server form a server in a client server transaction or from a first peer in a peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 13 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

(Continued on Supplemental Box)

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 146 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of :

Box V

Claims 14-16 are dependent on claim 13 and therefore meet the requirements of PCT Article 33(2) and (3).

1.3. Claims 17-20
The subject matter of claim 17 differs from these prior art documents in that the method of claim 17 includes steps of generating assertions based on a received security context and a received local execution context; transmitting confidence metrics in a report to an identity provider; and providing attestation of a running web application or web servlet as a digital icon for rendering by a web browser. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 17 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 18-20 are dependent on claim 17 and therefore meet the requirements of PCT Article 33(2) and (3).

1.4. Claim 21-26
The subject matter of claim 21 differs from these prior art documents in that the system of claim 21 includes steps of requesting and receiving dynamic assertions form a metadata repository of an attestation service, a dynamic assertions pertaining to a local execution context an introspected security context of running application instances on instrumented target platforms; continuously displaying the dynamic assertions to a system administrator. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 21 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 22-26 are dependent on claim 21 and therefore meet the requirements of PCT Article 33(2) and (3).

2. Industrial Applicability
Claims 1-26 are industrially applicable under PCT Article 33(4).

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 147 of 318

Electronic Acknowledgement Receipt

EFS ID:	18017872
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna LLoyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000015
Receipt Date:	24-JAN-2014
Filing Date:	27-JUL-2012
Time Stamp:	14:51:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_015.pdf	676761 25e04223510d7f120232405bf24c1e6457c532be	no	4

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	12_5_13_OA_665.pdf	1454882 9f7877d3233662e3e5e3a306c266e82f0966f335	no	15
Warnings:					
Information:					
3	Non Patent Literature	12_10_13_OA_732.pdf	2490430 bea7e19e8c3671444469941c0cac392606c5ec42	no	29
Warnings:					
Information:					
4	Non Patent Literature	10_23-13_OA_692.pdf	1338829 cedaa723010a9efac2173f0f01653fbc416542f1	no	12
Warnings:					
Information:					
5	Non Patent Literature	1_17_14OA_766.pdf	3502255 81149993dc6d411a6af6b55d5dd52f91c5ee8753	no	38
Warnings:					
Information:					
6	Non Patent Literature	Statement_ofFIPS.pdf	170829 0a6af5c16bd4c62a024849cac344342a8f859f41	no	1
Warnings:					
Information:					
7	Non Patent Literature	Trend_Micro.pdf	214710 516a6d79091df760128acd3972c8ca889da254ce	no	2
Warnings:					
Information:					
8	Non Patent Literature	ISR_551.pdf	339765 36bc512d2a9423c62b4edbfd1535554b27144fe5	no	3
Warnings:					
Information:					
9	Non Patent Literature	ISR_WO_551.pdf	1157331 ad87345d847c3f47aa48b38808fc24beab578c28	no	9
Warnings:					
Information:					
10	Non Patent Literature	IPRP_551.pdf	561947 50817d453d6a21f86f047a4e7e4065931fb17ece	no	5

Warnings:					
Information:					
11	Non Patent Literature	Event_Tracker_1pdf.pdf	15121555 2b263e6ca5aae1321f202eaf9a9bfcb7e42ca64d	no	200
Warnings:					
Information:					
12	Non Patent Literature	Event_Tracker_2pdf.pdf	15131181 139a5cd2abdf5cb715d796e8eb50696a9dac8a61	no	200
Warnings:					
Information:					
13	Non Patent Literature	Event_Tracker_3pdf.pdf	14129908 c2c37d0acf28e230d21fdeaff30909a26685ceb7	no	182
Warnings:					
Information:					
			Total Files Size (in bytes):	56290383	

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.

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/559,707	07/27/2012	Srinivas KUMAR	0079152-000015

CONFIRMATION NO. 1767

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

PUBLICATION NOTICE

OC000000064874152

Title:SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

Publication No.US-2013-0298243-A1
Publication Date:11/07/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 151 of 318

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	6742128	B1	2004-05-25	JOINER	
	2	7174566	B2	2007-02-06	YADAV	
	3	7370359	B2	2008-05-06	HRABIK et al.	
	4	8010469	B2	2011-08-30	KAPOOR et al.	
	5	8214497	B2	2012-07-03	ALPEROVITCH 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	20060015942	A1	2006-01-19	JUDGE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

	2	20080276317	A1	2008-11-06	CHANDOLA et al.	
	3	20090328222	A1	2009-12-31	HELMAN et al.	
	4	20110072506	A1	2011-03-24	LAW et al.	
	5	20110162073	A1	2011-06-30	JESCHKE et al.	
	6	20110276468	A1	2011-11-10	LEWIS et al.	
	7	20120011590	A1	2012-01-12	DONOVAN	
	8	20120072968	A1	2012-03-22	WYSOPAL et al.	
	9	20120102458	A1	2012-04-26	MEIJER et al.	
	10	20120110174	A1	2012-05-03	WOOTTON et al.	
	11	20120137375	A1	2012-05-31	RAMACHANDRAN et al.	
	12	20120260342	A1	2012-10-11	DUBE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	20110027386	KR	A	2011-03-16	MOZENSOFT INC.		☒

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	Norton Antivirus Product Manual Copyright 2011 Symantec Corporation, 334 pp	☐
	2	J. Andrew Schafer "Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events", msdn magazine, http://msdn.microsoft.com/en-us/magazine/cc301317.aspx, September 2001, 5 pp	☐
	3	AUBREY-DERRICK SCHMIDT et al. "Static Analysis of Executables for Collaborative Malware Detection on Android" ICC'09 Proceedings of the 2009 IEEE International Conference on Communications, 5 pp	☐
	4	International Search Report and Written Opinion dated August 27, 2013, issued in corresponding International Application No. PCT/US2013/039033, 16 pp	☐
	5	Office Action issued in copending U.S. Patent Application No. 13/559,732, mailed June 20, 2013, 32 pp	☐
	6	Office Action issued in copending U.S. Patent Application No. 13/559,766, mailed July 18, 2013, 39 pp	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2436
	Examiner Name	BEHESHTI SHIRAZI, SAYED ARESH
	Attorney Docket Number	0079152-000015

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	/Jennifer A. Wilson/	Date (YYYY-MM-DD)	2013-09-19
Name/Print	Jennifer A. Wilson	Registration Number	62,604

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.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 157 of 318

Espacenet

Bibliographic data: KR20110027386 (A) — 2011-03-16

APPARATUS, SYSTEM AND METHOD FOR PROTECTING MALICIOUS PACKETS TRANSMITTED OUTSIDE FROM USER TERMINAL

No documents available for this priority number.

Inventor(s): ROH CHUL HEE [KR] ± (ROH, CHUL HEE)

Applicant(s): MOZENSOFT INC [KR] ± (MOZENSOFT INC)

Classification: **- international:** ***G06F21/00; H04L12/22***
- cooperative:

Application number: KR20090085455 20090910

Priority number(s): KR20090085455 20090910

Abstract of KR20110027386 (A)

PURPOSE: An apparatus for blocking a malicious packet, a system thereof and a method thereof are provided to confirm a user about a protocol of a packet, which is not modulated, and to block the attack of DoS/DDoS or worm virus. CONSTITUTION: A user terminal(100) installs a malicious packet blocking unit. A central managing server collects log information of the user terminal. A log storing database calculates statics by using the stored log information.

Last updated: 13.03.2013 Worldwide Database 5.8.11.1; 92p

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 158 of 318

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0027386
(43) 공개일자 2011년03월16일

(51) Int. Cl.
H04L 12/22 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2009-0085455
(22) 출원일자 2009년09월10일
심사청구일자 2009년09월10일

(71) 출원인
모젠소프트 (주)
서울 광진구 군자동 98 세종대학교 충무관 311A
(72) 발명자
노철희
경기도 의정부시 호원동 현대아이파크 201-602
(74) 대리인
오세중

전체 청구항 수 : 총 17 항

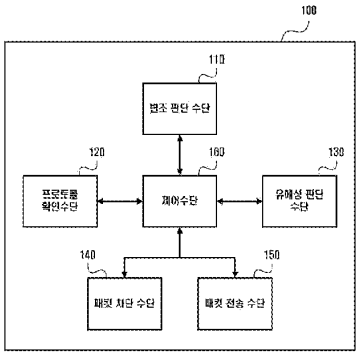
(54) 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법

(57) 요 약

사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법이 제공된다.

본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치는, 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단; 상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 패킷 차단 수단을 포함한다.

대 표 도 - 도2



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 159 of 318

특허청구의 범위

청구항 1

사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단;

상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 패킷 차단 수단을 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 2

제 1 항에 있어서,

상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 프로토콜 확인 수단;

상기 확인된 프로토콜 별로 유해성 여부를 판단하는 유해성 판단 수단;

상기 유해성 판단 수단의 판단 결과 유해하지 않은 경우에는 상기 패킷을 외부로 전송하는 패킷 전송 수단을 더 포함하며,

상기 유해성 판단 수단의 판단 결과 유해한 경우에는 상기 패킷 차단 수단이 상기 패킷을 차단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 3

제 2 항에 있어서,

상기 변조 판단 수단은,

상기 사용자 단말로부터 나가는 패킷의 헤더 영역의 인터넷 프로토콜 주소와 상기 사용자 단말에 설정되어 있는 인터넷 프로토콜 주소를 비교함으로써 변조되었는지 여부를 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 4

제 2 항 또는 제 3 항에 있어서,

상기 유해성 판단 수단은,

상기 사용자 단말로부터 분당 전송되는 패킷의 수가 임계치를 초과하는지 여부를 판단하여 상기 임계치를 초과하는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 임계치 이하인 경우에는 상기 패킷이 유해하지 않는 것으로 판단하는 임계치 초과 판단 수단;

상기 임계치 초과 판단 수단의 판단 결과 상기 임계치 이하인 경우 상기 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하여 상기 프래그먼트 공격이 있는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 패킷이 유해하지 않는 것으로 판단하는 프래그먼트 검사 수단을 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 5

제 4 항에 있어서,

상기 프로토콜 확인 수단의 확인 결과 상기 패킷이 UDP(User Datagram Protocol) 패킷인 경우에,

상기 임계치 초과 판단 수단은, 분당 전송되는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단하여 상기 UDP 임계치를 초과하는 경우 상기 UDP 패킷이 유해하다고 판단하며,

상기 프래그먼트 검사 수단은, 상기 임계치 초과 판단 수단의 판단 결과 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하는, 사용자 단말로부

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 160 of 318

터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 6

제 4 항에 있어서,

상기 프로토콜 확인 수단의 확인 결과 상기 패킷이 TCP 패킷인 경우에,

상기 임계치 초과 판단 수단은,

분당 전송되는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단하여 상기 TCP Syn/Ack 임계치를 초과하는 경우 상기 TCP Syn/Ack 패킷이 유해하다고 판단하며, 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단하여 상기 TCP Get 임계치를 초과하는 경우 상기 TCP Get 패킷이 유해하다고 판단하며, 상기 TCP Get 임계치 이하인 경우에는 분당 전송되는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단하여 상기 TCP RST/FIN 임계치를 초과하는 경우 상기 TCP RST/FIN 패킷이 유해하다고 판단하며,

상기 프래그먼트 검사 수단은, 상기 임계치 초과 판단 수단의 판단 결과 상기 TCP RST/FIN 임계치 이하인 경우에는 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 7

제 4 항에 있어서,

상기 프로토콜 확인 수단의 확인 결과 상기 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에,

상기 임계치 초과 판단 수단은, 분당 전송되는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단하여 상기 ICMP 임계치를 초과하는 경우 상기 ICMP 패킷이 유해하다고 판단하며,

상기 프래그먼트 검사 수단은, 상기 임계치 초과 판단 수단의 판단 결과 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 8

외부로 전송되는 패킷의 출발지 인터넷 프로토콜 주소의 변조 여부를 파악하여 변조된 패킷을 차단하고, 변조되지 않은 패킷의 전송 개수와 임계치의 비교 결과에 따라 유해한 패킷을 차단하는 유해 패킷 차단 장치가 설치된 사용자 단말;

복수의 사용자 단말에 각각 설치되어 있는 상기 유해 패킷 차단 장치를 관리하며, 상기 사용자 단말의 보안 정책을 설정하고, 상기 사용자 단말의 로그 정보를 수집하는 중앙 관리 서버;

상기 수집된 로그 정보를 저장하고, 상기 저장된 로그 정보를 이용하여 통계를 산출하는 로그 저장 데이터베이스를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 9

제 8 항에 있어서,

상기 유해 패킷 차단 장치는,

상기 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단;

상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 프로토콜 확인 수단;

상기 확인된 프로토콜 별로 유해성 여부를 판단하는 유해성 판단 수단;

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 161 of 318

상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우 또는 상기 유해성 판단 수단의 판단 결과 유해한 경우에는 상기 패킷을 차단하는 패킷 차단 수단;

상기 유해성 판단 수단의 판단 결과 유해하지 않은 경우에는 상기 패킷을 외부로 전송하는 패킷 전송 수단을 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 10

제 8 항에 있어서,

상기 변조 판단 수단은,

상기 사용자 단말로부터 나가는 패킷의 헤더 영역의 인터넷 프로토콜 주소와 상기 사용자 단말에 설정되어 있는 인터넷 프로토콜 주소를 비교함으로써 변조되었는지 여부를 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 11

제 8 항에 있어서,

상기 중앙 관리 서버는,

상기 출발지 인터넷 프로토콜 주소가 변조된 패킷 또는 상기 유해성 판단 수단의 판단 결과 유해하다고 판단된 패킷의 활동 통계를 산출하고, 상기 산출된 활동 통계의 분석 결과 위험하다고 판단되는 경우 상기 사용자 단말에게 실시간으로 통지하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 12

사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 단계;

상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 13

제 12 항에 있어서,

상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 단계;

상기 확인된 프로도콜 별로 유해성 여부를 판단하는 단계;

상기 유해성 여부의 판단 결과 유해한 경우에는 상기 패킷을 차단하고, 유해하지 않은 경우에는 상기 패킷을 외부로 전송하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 14

제 12 항 또는 제 13 항에 있어서,

상기 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 단계는,

상기 사용자 단말로부터 나가는 패킷의 헤더 영역의 인터넷 프로토콜 주소와 상기 사용자 단말에 설정되어 있는 인터넷 프로토콜 주소를 비교함으로써 변조되었는지 여부를 판단하는 단계인, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 15

제 13 항에 있어서,

상기 유해성 여부를 판단하는 단계는,

상기 패킷의 프로토콜을 확인한 결과 상기 패킷이 UDP(User Datagram Protocol) 패킷인 경우에는,

분당 전송되는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단하는 단계;

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 162 of 318

상기 UDP 임계치를 초과하는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 단계;

상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 16

제 13 항에 있어서,

상기 유해성 여부를 판단하는 단계는,

상기 패킷의 프로토콜을 확인한 결과 상기 패킷이 TCP 패킷인 경우에는,

분당 전송되는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단하는 단계;

상기 TCP Syn/Ack 임계치를 초과하는 경우에는 상기 TCP Syn/Ack 패킷이 유해하다고 판단하고, 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단하는 단계;

상기 TCP Get 임계치를 초과하는 경우에는 상기 TCP Get 패킷이 유해하다고 판단하고, 상기 TCP Get 임계치 이하인 경우에는 분당 전송되는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단하는 단계;

상기 TCP RST/FIN 임계치를 초과하는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 TCP RST/FIN 임계치 이하인 경우에는 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 단계;

상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 17

제 13 항에 있어서,

상기 유해성 여부를 판단하는 단계는,

상기 패킷의 프로토콜을 확인한 결과 상기 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에는,

분당 전송되는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단하는 단계;

상기 ICMP 임계치를 초과하는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 단계;

상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법에 관한 것으로서, 더욱 상세하게는, 사용자 단말로부터 나가는 패킷의 출발지 IP 주소가 변조되었는지 여부를 판단하여 출발지 IP 주소가 변조된 패킷을 차단하며, 변조되지 않은 패킷의 프로토콜을 확인하여 프로토콜 별로 유해성 여부를 판단하여 패킷을 차단할 수 있는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법에

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 163 of 318

관한 것이다.

배경 기술

[0002] 서비스 거부 공격(Denial of Service Attack, 이하 'DoS 공격'이라 한다)이란 외부 공격자가 특정 컴퓨터 시스템과 그 시스템이 속한 네트워크에 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 정상적인 운영을 방해하여 그 컴퓨터 시스템이 사용자에 대한 서비스의 제공을 거부하도록 하는 공격 방법이다.

[0003] 또한, 분산 서비스 거부 공격(Distributed Denial of Service Attack, 이하 'DDoS 공격'이라 한다)이란 많은 수의 호스트들에 패킷을 범람시킬 수 있는 서비스 거부 공격용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표의 컴퓨터 시스템이나 네트워크의 성능을 저하시키거나 시스템을 마비시키는 것을 말한다.

[0004] 이러한 DoS 및 DDoS 공격은 TCP SYN 플러딩 공격, UDP 플러딩 공격, ICMP(Internet Control Message Protocol) 반향 요구(echo requesting) 공격, ICMP 동보(broadcasting) 공격의 형태로 나뉘어 진다. 이를 다시 크게 분류하면 플러딩 공격, IP 패킷의 부적절한 단편화를 기반으로 하는 공격, 부적절한 패킷 헤더 포맷 기반 공격으로 나눌 수 있다.

[0005] 일반적으로, DoS 공격이 이루어지는 과정을 살펴보면, DoS 에이전트(Agent)가 실어진 컴퓨터(공격자)에서 대량의 패킷을 발생시켜 호스트 컴퓨터를 공격함으로써, 호스트 컴퓨터가 정당한 다른 사용자들에게 서비스를 제대로 제공하지 못하도록 하여 서비스 거부 공격이 이루어진다.

[0006] 이러한 서비스 거부 공격은 공격자 컴퓨터가 IP 주소를 위장하면서 공격 목표 호스트 컴퓨터에 TCP 접속을 위한 동기 신호를 무한으로 뒤폴이하여 보냄으로써 이루어지는데, 이 경우 호스트 컴퓨터는 이 위장된 IP 주소에 접속을 위한 신호를 응답하여 접속 준비가 되었음을 무한으로 뒤폴이하여 알리는 동작을 수행하므로 호스트 컴퓨터에 과부하가 걸려서 정당 사용자에게 서비스를 제공할 수 없게 된다.

[0007] 그런데, 기존의 DoS 또는 DDoS 방어 시스템 기술은 외부에서 내부 서버 또는 Victim 네트워크로 유입되는 공격을 차단하는 방향으로 개발되었다. 또한, IPS 시스템들도 외부에서 유입되는 Worm 바이러스 유입을 차단하도록 네트워크 경계선 상에서 방어를 한다. 하지만, 다양한 경로를 통해 Worm 바이러스에 감염되거나 부트 프로그램이 감염되어 대량의 좀비 PC가 양산되고 각 좀비 PC 단에서 공격이 시작되는 경우에는 효율적으로 대처하지 못하였다.

[0008] 이를 게이트웨이 보안의 측면에서 살펴보면, 변조된 IP 주소를 이용한 내부 사용자의 DoS 또는 DDoS 공격이나 웜 바이러스 확산을 원천적으로 탐지 및 차단하지 못하며, 이로 인하여 내부 네트워크의 안정성 확보가 어렵게 된다. 또한, 변조된 IP 주소를 이용한 내부 네트워크에서의 좀비 PC의 활동을 막기가 어렵다는 문제가 있었다.

[0009] 또한, 사용자 PC의 보안의 측면에서 살펴보면, 첫째, 기존의 백신 프로그램의 경우 DDoS 공격이나 웜 바이러스 공격이 발생한 후 활동 내역을 분석하여 백신이 개발되는 바, 이는 공격이 발생한 이후의 사후 처리를 위한 해결책은 되지만 사전에 DoS/DDoS나 웜 바이러스의 활동을 제한하거나 예방하는 역할은 못하였다. 둘째, 기존의 PC 방화벽의 경우 사용자 PC로부터 나가는 패킷에 대해서는 웹 서비스에 대한 접속을 무제한으로 허용하기 때문에 DoS/DDoS 공격에 가담하는 좀비 PC를 구분해 내지 못하였다.

발명의 내용

해결 하고자하는 과제

[0010] 따라서, 상술한 문제점을 해결하기 위하여 본 발명이 해결하고자 하는 과제는, 게이트웨이 단에서 방어하는 기존의 백신 프로그램의 한계를 극복하기 위해 공격에 가담하는 사용자 PC 단에서 원천적으로 DoS/DDoS나 웜 바이러스의 공격을 차단하고자 하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법을 제공하는 것이다.

[0011] 또한, 본 발명이 해결하고자 하는 다른 기술적 과제는, 자기 복제 기능을 통해 다른 컴퓨터나 내부 네트워크의 전산 시스템 등을 감염시키는 유해 트래픽의 확산을 사전에 감염된 PC에서 탐지하여 차단할 수 있는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법을 제공하는 것이다.

[0012] 본 발명이 해결하고자 하는 과제들은 이상에서 언급한 과제들로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 164 of 318

과제 해결수단

[0013] 전술한 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치는, 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단; 상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 패킷 차단 수단을 포함한다.

[0014] 또한, 전술한 기술적 과제를 달성하기 위한 본 발명의 다른 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템은, 외부로 전송되는 패킷의 출발지 인터넷 프로토콜 주소의 변조 여부를 파악하여 변조된 패킷을 차단하고, 변조되지 않은 패킷의 전송 개수와 임계치의 비교 결과에 따라 유해한 패킷을 차단하는 유해 패킷 차단 장치가 설치된 사용자 단말; 복수의 사용자 단말에 각각 설치되어 있는 상기 유해 패킷 차단 장치를 관리하며, 상기 사용자 단말의 보안 정책을 설정하고, 상기 사용자 단말의 로그 정보를 수집하는 중앙 관리 서버; 상기 수집된 로그 정보를 저장하고, 상기 저장된 로그 정보를 이용하여 통계를 산출하는 로그 저장 데이터베이스를 포함한다.

[0015] 또한, 전술한 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법은, 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 단계; 상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 단계를 포함한다.

[0016] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

효 과

[0017] 상기한 바와 같은 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법에 의하면, 다음과 같은 효과가 하나 이상 존재한다.

[0018] 첫째, 게이트웨이 단에서 방어하는 기존의 백신 프로그램의 한계를 극복하여 사용자 PC 단에서 원천적으로 DoS/DDoS나 웜 바이러스의 공격을 차단할 수 있다.

[0019] 둘째, 자기 복제 기능을 통해 다른 컴퓨터나 내부 네트워크의 전산 시스템 등을 감염시키는 유해 트래픽의 확산을 사전에 감염된 PC에서 탐지하여 차단할 수 있다.

[0020] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 실시를 위한 구체적인 내용

[0021] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0022] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소, 단계, 동작 및/또는 소자는 하나 이상의 다른 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다. 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0023] 이하, 본 발명을 보다 구체적으로 설명하기 위하여 본 발명에 따른 실시예들을 첨부 도면을 참조하면서 보다 상세하게 설명하고자 한다.

[0024] 도 1은 본 발명의 일 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템의 전체 구성도를 나타내는 도면이다.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 165 of 318

[0025] 도 1을 참조하면, 상기 시스템은 사용자 단말(100), 중앙 관리 서버(200), 관리 콘솔(300), 로그 저장 데이터베이스(400)을 포함하여 구성된다.

[0026] 사용자 단말(100)은 본 발명의 실시예에서의 유해 패킷 차단 장치가 구비된 단말로서, 네트워크의 종단에 위치한 개인용 컴퓨터나 네트워크 내부의 서버 등 네트워크에 연결되어 있는 전산 장치이기만 하면 되고, 연결 방식이 유선이든 무선이든 무관하다.

[0027] 본 발명에서 유해 패킷 차단 장치가 구비된 사용자 단말(100)은 자신에게서 외부로 나가는 패킷의 출발지 IP(Internet Protocol) 주소의 변조 여부를 파악하여 변조된 패킷에 대해서는 외부로 내보내지 않고 차단하며, 변조되지 않은 패킷에 대해서는 변조되지 않은 패킷의 분당 전송수가 소정의 임계치를 초과하는 경우에는 유해한 트래픽이 존재한다고 보아 차단하는 역할을 한다. 사용자 단말(100)에 구비된 유해 패킷 차단 장치의 구성과 역할에 대해서는 후술할 도 2에서 설명하기로 한다.

[0028] 그 밖에도 사용자 단말(100)은 자신의 네트워크 활동 상황을 모니터링하여 중앙 관리 서버(200)로 보고하며, 변조되지 않은 패킷의 전송에 대해서는 정상적인 연결을 보장하며, 보안 감사 기록을 중앙 관리 서버(200)로 전송할 수 있다.

[0029] 중앙 관리 서버(200)는 전술한 사용자 단말(100)에 각각 설치되어 있는 상기 유해 패킷 차단 장치를 관리하는 서버로서, 사용자 단말(100)의 보안 정책을 설정하여 제어하고, 사용자 단말(100)의 개별적인 로그 정보를 수집하여 통계를 산출할 수 있다. 또한, 사용자 단말(100)의 보안 상태를 실시간으로 모니터링하여 각 사용자 단말(100) 별 보고서를 작성할 수 있으며, 전사적으로 DDoS나 웜 바이러스와 같은 유해 트래픽의 활동을 기간별로 분석하여 기간별 보고서를 생성할 수도 있다.

[0030] 또한, 중앙 관리 서버(200)는 출발지 IP 주소가 변조된 패킷 또는 IP 주소가 변조되지 않았으나 유해하다고 판단된 패킷의 활동 통계를 산출하고, 상기 산출된 활동 통계의 분석 결과 위험하다고 판단되는 경우 사용자 단말(100)에게 실시간으로 통지할 수 있다.

[0031] 관리 콘솔(300)은 중앙 관리 서버(200)에 접근하기 위한 장치로서, 사용자 단말(100) 내부에 설치된 유해 패킷 차단 장치의 정책을 수립하는 역할을 할 수 있다.

[0032] 로그 저장 데이터베이스(400)는 중앙 관리 서버(200)에 의해 수집된 사용자 단말(100)의 로그 정보를 저장하고, 상기 저장된 로그 정보를 이용하여 통계를 산출하는 역할을 한다.

[0033] 도 2는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치의 구성을 나타내는 도면이다.

[0034] 상기 도 2를 참조하면, 유해 패킷을 차단하는 장치는 변조 판단 수단(110), 프로토콜 확인 수단(120), 유해성 판단 수단(130), 패킷 차단 수단(140), 패킷 전송 수단(150) 및 제어 수단(160)을 포함하여 구성된다.

[0035] 변조 판단 수단(110)은 사용자 단말(100)로부터 나가는 패킷의 출발지 IP 주소가 변조되었는지 여부를 판단하는 역할을 한다. 여기서, 패킷의 출발지 IP 주소의 변조 여부는 도 5를 참조하여 설명하기로 한다.

[0036] 도 5는 본 발명의 실시예에 따른 사용자 단말로부터 나가는 패킷의 출발지 IP 주소의 변조 여부를 판단하는 원리를 나타내는 도면이다. 즉, 도 5에서 알 수 있듯이, 사용자 단말로부터 나가는 패킷의 헤더 영역에는 출발지(Source) IP, 출발지 포트 번호, 목적지(Destination) IP, 및 목적지 포트 번호에 대한 정보가 기재되어 있는데, 이 중 출발지 IP 주소와 상기 사용자 단말에 설정되어 있는 IP 주소(도 5에서는 192.168.2.7)를 비교함으로써 변조되었는지 여부를 판단하게 된다.

[0037] 일반적으로, DDoS 공격이나 웜 바이러스의 확산시 발생하는 유해 트래픽의 내용 중 거의 대부분이 출발지 IP 주소를 변조하여 공격하므로 출발지 IP 주소가 변조되었는지 여부를 탐지하여 차단하는 것은 DDoS 공격이나 웜 바이러스의 확산에 대한 초기 대응에서 매우 중요하다고 할 수 있다.

[0038] 다시 도 2를 참조하면, 프로토콜 확인 수단(120)은 변조 판단 수단(110)의 확인 결과 상기 출발지 IP 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 역할을 한다.

[0039] 유해성 판단 수단(130)은 프로토콜 확인 수단(120)에 의해 확인된 프로토콜 별로 유해성 여부를 판단하는 역할을 한다.

[0040] 유해성 판단 수단의 구성을 나타내는 도 3을 참조하면, 유해성 판단 수단(130)은 임계치 초과 판단 수단(131)

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 166 of 318

및 프래그먼트 검사 수단(132)를 포함하여 구성됨을 알 수 있다.

[0041] 임계치 초과 판단 수단(131)은 사용자 단말로부터 분당 전송되는 패킷의 수가 임계치를 초과하는지 여부를 판단하여 상기 임계치를 초과하는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 임계치 이하인 경우에는 상기 패킷이 유해하지 않는 것으로 판단하게 된다. 여기서, 상기 임계치는 프로토콜 확인 수단(120)에 의해 확인된 프로토콜에 따른 통신에 대해 중앙 관리 서버(200)로부터 내려받은 정책을 기반으로 설정할 수 있다.

[0042] 프래그먼트 검사 수단(132)은 상기 임계치 초과 판단 수단(131)의 판단 결과 상기 임계치 이하인 경우 상기 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 역할을 하는데, 상기 프래그먼트 공격이 있는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 패킷이 유해하지 않는 것으로 판단하게 된다.

[0043] 여기서, 유해성 판단 수단(130)이 프로토콜 별로 유해성 여부를 판단하는 것을 좀 더 구체적으로 살펴보기로 한다.

[0044] 첫째, 프로토콜 확인 수단(120)의 확인 결과 사용자 단말(100)에서 나가는 패킷이 UDP(User Datagram Protocol) 패킷인 경우에는, 임계치 초과 판단 수단(131)은, 분당 전송되어 나가는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단하여 상기 UDP 임계치를 초과하는 경우 상기 UDP 패킷이 유해하다고 판단한다. 여기서, 상기 UDP 임계치는 UDP 통신에 대해 중앙 관리 서버(200)로부터 내려받은 정책을 기반으로 설정할 수 있다.

[0045] 또한, 프래그먼트 검사 수단(132)은, 임계치 초과 판단 수단(131)의 판단 결과 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하게 된다.

[0046] 둘째, 프로토콜 확인 수단(120)의 확인 결과 사용자 단말(100)에서 나가는 패킷이 TCP 패킷인 경우에는, 임계치 초과 판단 수단(131)은, 분당 전송되어 나가는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단하여 상기 TCP Syn/Ack 임계치를 초과하는 경우 상기 TCP Syn/Ack 패킷이 유해하다고 판단한다. 또한, 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되어 나가는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단하여 상기 TCP Get 임계치를 초과하는 경우 상기 TCP Get 패킷이 유해하다고 판단한다. 또한, 상기 TCP Get 임계치 이하인 경우에는 분당 전송되어 나가는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단하여 상기 TCP RST/FIN 임계치를 초과하는 경우 상기 TCP RST/FIN 패킷이 유해하다고 판단한다.

[0047] 이 경우, 상기 임계치 초과 판단 수단(131)의 판단 결과 상기 TCP RST/FIN 임계치 이하인 경우에는, 프래그먼트 검사 수단(132)이 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단한다.

[0048] 셋째, 프로토콜 확인 수단(120)의 확인 결과 사용자 단말(100)에서 나가는 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에는, 임계치 초과 판단 수단(131)은 분당 전송되어 나가는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단하여 상기 ICMP 임계치를 초과하는 경우 상기 ICMP 패킷이 유해하다고 판단한다. 여기서, 상기 ICMP 임계치는 ICMP 통신에 대해 중앙 관리 서버(200)로부터 내려받은 정책을 기반으로 설정할 수 있다.

[0049] 또한, 프래그먼트 검사 수단(132)은, 상기 임계치 초과 판단 수단(131)의 판단 결과 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하게 된다.

[0050] 다시 도 2로 돌아오면, 패킷 차단 수단(140)은 변조 판단 수단(110)의 판단 결과 상기 출발지 IP 주소가 변조된 경우 또는 상기 유해성 판단 수단(130)의 판단 결과 유해한 패킷이라고 판단된 경우에는 그 패킷을 차단하는 역할을 할 수 있다.

[0051] 패킷 전송 수단(150)은 유해성 판단 수단(130)의 판단 결과 유해하지 않다고 판단된 경우에는 상기 패킷을 외부로 전송하는 역할을 한다.

[0052] 제어 수단(160)은 전술한 각 수단들을 제어하고 각 수단들 간에 상호 작용할 수 있도록 신호를 전달하는 역할을

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 167 of 318

한다.

[0053] 도 4는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법의 전체 흐름을 나타내는 도면이다.

[0054] 먼저, 사용자 단말(100)로부터 나가는 패킷의 출발지 IP 주소가 변조되었는지 여부를 판단한다(S110).

[0055] 상기 판단 결과 변조된 경우에는 상기 패킷을 차단하고(S170), 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하여 프로토콜 별로 유해성 여부를 판단한다(S120).

[0056] 여기서, 패킷의 프로토콜로는 크게 3가지로 나눌 수 있는 바, UDP, TCP 및 ICMP로 분류할 수 있다.

[0057] 먼저, 상기 패킷이 UDP(User Datagram Protocol) 패킷인 경우에는, 분당 전송되는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단한다(S132). 상기 UDP 임계치를 초과하는 경우에는 상기 UDP 패킷이 유해하다고 판단하고(S170), 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지한다(S134). 상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고(S170), 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하여 패킷을 외부로 전송한다(S160).

[0058] 둘째, 상기 패킷이 TCP 패킷인 경우에는, 분당 전송되는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단한다(S142). 여기서, TCP Syn/Ack 패킷의 정상적인 통신 과정에서는 도 6a에서와 같이, 사용자 PC와 서버가 통신을 위해 TCP 연결을 위해 서로의 응답을 확인하고 다음 연결 단계를 거쳐 안전하게 통신을 하게 된다. 하지만, 비정상적인 통신 과정에서는 도 6b에서와 같이, Victim 서버로의 연결 시도 후 응답 확인 과정을 거치지 않고 대량의 연결 시도를 반복적으로 수행함으로써, Victim 서버의 대기 큐를 고갈시키는 피해가 발생된다.

[0059] 이러한 Syn/Ack 공격은 중앙 관리 서버(200)로부터 내려받은 임계치 정책을 기반으로 대량의 단 방향성 연결시도를 차단 할 수 있다. 즉, 상기 TCP Syn/Ack 임계치를 초과하는 경우에는 상기 TCP Syn/Ack 패킷이 유해하다고 판단하고(S170), 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단한다(S144).

[0060] 여기서, TCP Get 패킷의 정상적인 통신 과정에서는 도 7a에서와 같이, 사용자 PC와 서버가 통신을 위해 서로의 응답을 확인하고 다음 연결 단계를 거쳐 안전하게 통신을 하게 된다. 하지만, 비정상적인 통신 과정에서는 도 7b에서와 같이, Victim 서버로의 연결 시도 후 응답 확인 과정을 거치지 않고 데이터 요청을 반복적으로 수행함으로써 Victim 자원을 고갈시키게 된다.

[0061] 이러한 서버 부하 유발 공격에 대해 중앙 관리 서버(200)로부터 내려받은 Get 패킷에 대한 임계치 정책을 기반으로 대량의 데이터 요청 공격인 Get 플러딩 공격을 차단할 수 있다. 즉, 상기 TCP Get 임계치를 초과하는 경우에는 상기 TCP Get 패킷이 유해하다고 판단하고(S170), 상기 TCP Get 임계치 이하인 경우에는 분당 전송되는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단한다(S146).

[0062] 상기 TCP RST/FIN 임계치를 초과하는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고(S170), 상기 TCP RST/FIN 임계치 이하인 경우에는 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지 여부를 탐지한다(S148). 상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고(S170), 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단하여 패킷을 외부로 전송한다(S160).

[0063] 셋째, 상기 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에는, 분당 전송되는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단한다(S152). 상기 ICMP 임계치를 초과하는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고(S170), 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지한다(S154). 상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고(S170), 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하여 패킷을 외부로 전송한다(S160).

[0064] 한편, 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법은 이 방법을 실행하기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록매체에 저장되어 구현 가능하다.

[0065] 이상과 같이 본 발명을 도면에 도시한 실시예를 참고하여 설명하였으나, 이는 발명을 설명하기 위한 것일 뿐이

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 168 of 318

며, 본 발명이 속하는 기술 분야의 통상의 지식을 가진 자라면 발명의 상세한 설명으로부터 다양한 변형 또는 균등한 실시예가 가능하다는 것을 이해할 수 있을 것이다. 따라서 본 발명의 진정한 권리범위는 특허청구범위의 기술적 사상에 의해 결정되어야 한다.

도면의 간단한 설명

[0066] 도 1은 본 발명의 일 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템의 전체 구성도를 나타내는 도면이다.

[0067] 도 2는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치의 구성을 나타내는 도면이다.

[0068] 도 3은 상기 도 2에 도시된 유해성 판단 수단의 구성을 나타내는 도면이다.

[0069] 도 4는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법의 전체 흐름을 나타내는 도면이다.

[0070] 도 5는 본 발명의 실시예에 따른 사용자 단말로부터 나가는 패킷의 출발지 IP 주소의 변조 여부를 판단하는 원리를 나타내는 도면이다.

[0071] 도 6a는 TCP Syn/Ack 패킷의 정상적인 통신 과정을 나타내는 도면이다.

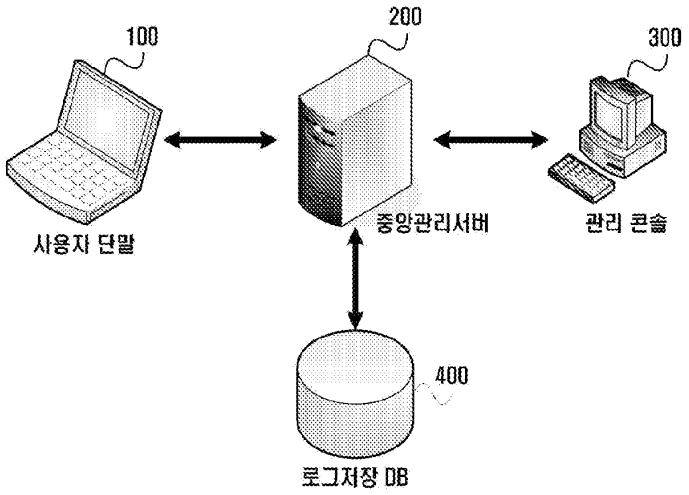
[0072] 도 6b는 TCP Syn/Ack 패킷의 공격 과정을 나타내는 도면이다.

[0073] 도 7a는 TCP Get 패킷의 정상적인 통신 과정을 나타내는 도면이다.

[0074] 도 7b는 TCP Get 패킷의 공격 과정을 나타내는 도면이다.

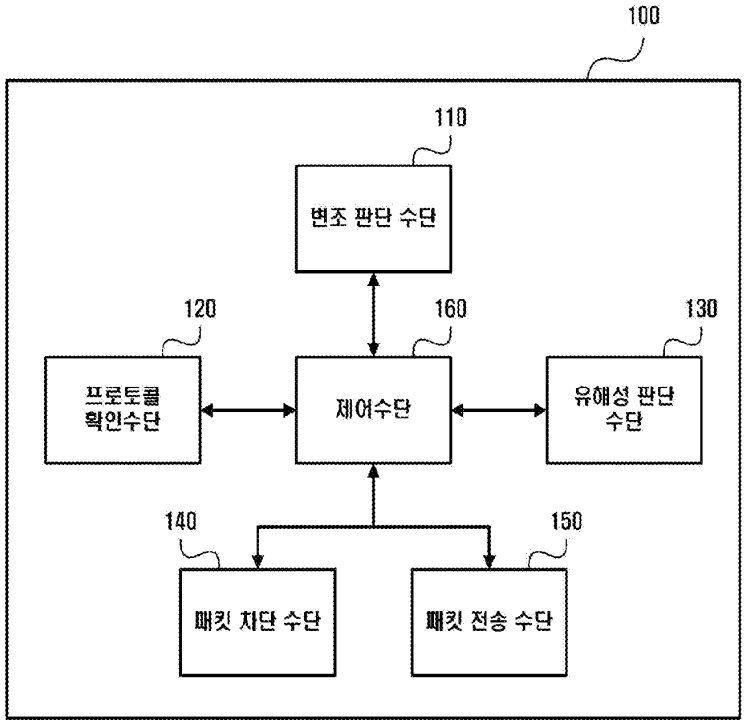
도면

도면1

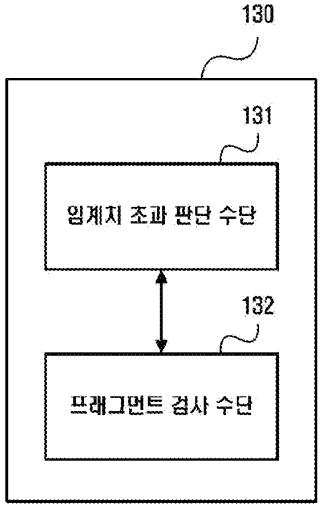


Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 169 of 318

도면2

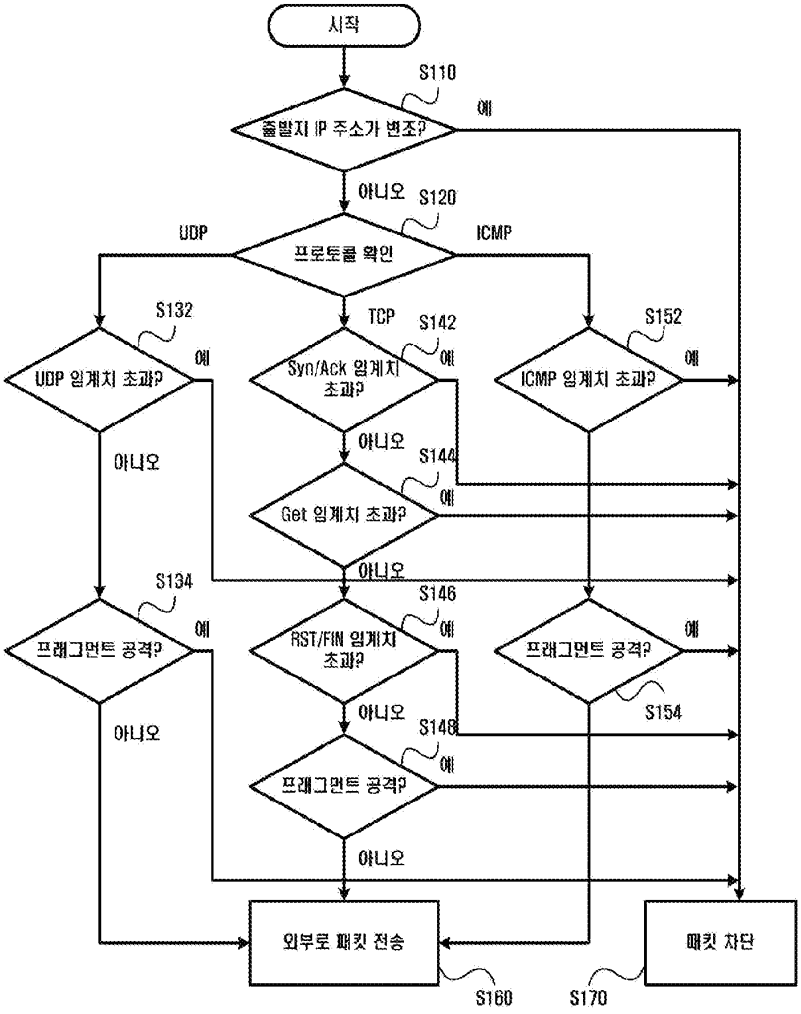


도면3

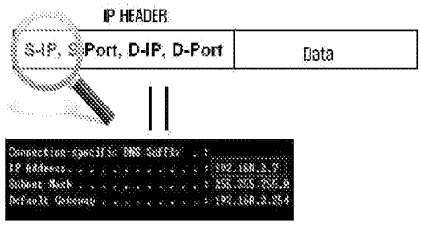


Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 170 of 318

도면4

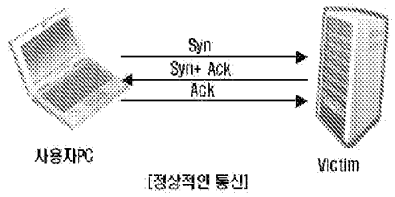


도면5

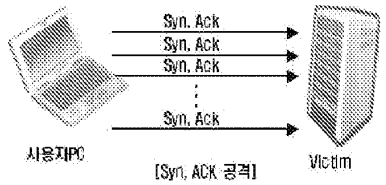


Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 171 of 318

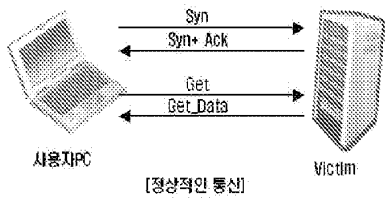
도 면6a



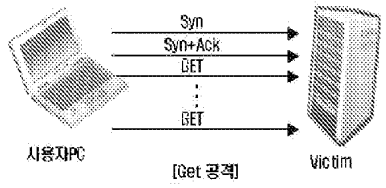
도 면6b



도 면7a



도 면7b



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 172 of 318

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND, CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC CUSTOMER NO. 21839 P. O. BOX 1404 ALEXANDRIA VA 22313-1404 USA

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing *(day/month/year)*	27 August 2013 (27.08.2013)
Applicant's or agent's file reference 0079152-0018	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. **PCT/US2013/039033**	International filing date *(day/month/year)* **01 May 2013 (01.05.2013)**

Applicant

TAASERA, INC.

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:

   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 . 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer COMMISSIONER Telephone No. 82-42-481-8753

Form PCT/ISA/220 (July 2010)

* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

http://www.kipo.go.kr/en/ => PCT Services => PCT Services

ID : PCT international application number
PW : **XF7ED7CJ**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: http://www.ipkcenter.com

Email: ipkc@ipkcenter.com

Notes to Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 0079152-0018	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. **PCT/US2013/039033**	International filing date *(day/month/year)* **01 May 2013 (01.05.2013)**	(Earliest) Priority Date *(day/month/year)* 01 May 2012 (01.05.2012)
Applicant **TAASERA, INC.**		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 175 of 318

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/039033

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/50(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/50; G06Q 40/00; G06F 11/00; G06F 21/00; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: cloud, mobile, integrity, alert, calculate, risk, rule, profile, trust, agent and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011-0162073 A1 (KONIKAYE JESCHKE) 30 June 2011 See paragraphs 20-49, 54; and figures 1-8.	1-106
A	US 2012-0011590 A1 (JOHN JOSEPH DONOVAN) 12 January 2012 See paragraphs 77-79; and figures 1, 8.	1-106
A	US 2011-0276468 A1 (MICHAEL LEWIS et al.) 10 November 2011 See paragraphs 44-49; and figure 3.	1-106
A	US 2011-0072506 A1 (GARY K. LAW et al.) 24 March 2011 See paragraphs 62-64; and figures 2, 15-16.	1-106
A	KR 10-2011-0027386 A (MOZENSOFT INC.) 16 March 2011 See paragraphs 33-35, 53-63; and figures 2-4.	1-106

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 August 2013 (26.08.2013)	**27 August 2013 (27.08.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	Authorized officer BYUN Sung Cheal Telephone No. +82-42-481-8262

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/039033

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0162073 A1	30/06/2011	AU 2007-349278 A1	25/09/2008
		CA 2681013 A1	25/09/2008
		CN 101681328 A	24/03/2010
		CN 101681328 B	21/03/2012
		EP 2137630 A1	30/12/2009
		EP 2137630 A4	13/04/2011
		US 2008-0229420 A1	18/09/2008
		US 7900259 B2	01/03/2011
		US 8141155 B2	20/03/2012
		WO 2008-115257 A1	25/09/2008
US 2012-0011590 A1	12/01/2012	None	
US 2011-0276468 A1	10/11/2011	US 2008-140576 A1	12/06/2008
		US 7403922 B1	22/07/2008
		US 7970701 B2	28/06/2011
		US 8244629 B2	14/08/2012
US 2011-0072506 A1	24/03/2011	CN 102299909 A	28/12/2011
		DE 102010037740 A1	05/05/2011
		GB 201015884 D0	27/10/2010
		GB 2474545 A	20/04/2011
		JP 2011-100443 A	19/05/2011
KR 10-2011-0027386 A	16/03/2011	None	

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 177 of 318

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND, CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC CUSTOMER
NO. 21839 P. O. BOX 1404 ALEXANDRIA VA 22313-1404
USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	**27 August 2013 (27.08.2013)**
Applicant's or agent's file reference 0079152-0018	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/039033	**01 May 2013 (01.05.2013)**	01 May 2012 (01.05.2012)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/50(2013.01)i

Applicant
TAASERA, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	26 August 2013 (26.08.2013)	BYUN Sung Cheal Telephone No. +82-42-481-8262

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/039033

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioanl copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 179 of 318

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/039033

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-106	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-106	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-106	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2011-0162073 A1 (KONIKAYE JESCHKE) 30 June 2011
D2: US 2012-0011590 A1 (JOHN JOSEPH DONOVAN) 12 January 2012
D3: US 2011-0276468 A1 (MICHAEL LEWIS et al.) 10 November 2011
D4: US 2011-0072506 A1 (GARY K. LAW et al.) 24 March 2011
D5: KR 10-2011-0027386 A (MOZENSOFT INC.) 16 March 2011

2.1 Novelty and Inventive Step (PCT Article 33(2) and (3))

2.1.1 Claims 1-19

The subject matter of claim 1 differs from these prior art documents in that a method comprises the steps of: determining a calculus of risk for a mobile device based at least upon integrity alerts and identified risks; sending, by an endpoint trust agent, a plurality of endpoints events comprising data and content of runtime integrity warnings to a trust orchestrator and generating, by the trust orchestrator, an integrity profile based on received endpoint events. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 1 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 2-19 are directly or indirectly dependent on claim 1. Consequently, claims 2-19 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.2 Claim 20

The subject matter of claim 20 differs from these prior art documents in that a system comprises: a computing platform including a network trust agent, and endpoint trust agent, and a trust orchestrator, wherein the computing platform is configured to: generate, by a trust orchestrator, an integrity profile for an endpoint based on received endpoint events pertaining to data and content; process and correlate, by the trust orchestrator one or more of: a system

Continued on Supplemental Box

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 180 of 318

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/039033

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Claim 38 is referring to itself, thereby rendering the definition of the subject matter of said claim unclear (PCT Article 6). (Note: This international search report and written opinion have been established on the assumption that claim 38 is dependent on claim 29.)

2. Claim 100 is unclear because "the trust orchestrator" has not been previously defined. Therefore, claim 100 does not meet the requirements of PCT Article 6. (Note: This international search report and written opinion have been established on the assumption that claim 100 is dependent on claim 94.)

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 181 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of : Box No. V

integrity profile generated based on a calculus of risk; a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports from a plurality of collaboration services; a system infection profile received from a network analyzer; send, by the trust orchestrator, system warnings based on an endpoint execution state of the mobile application or mobile computing device as a threat posture assesment to one or more of: a network trust agent, a mobile policy manager, and a mobile device manager; and send, by the network trust agent, messages or directives to network security frameworks and/or wireless access points to apply flow controls based on the received execution state of a mobile endpoint. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 20 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.1.3 Claim 21

The subject matter of claim 21 differs from these prior art documents in a non-transitory computer readable medium having instructions comprising: determining a predicate score based upon a deviation from a prescribed attribute constraint or metric; calculating a score that is inversely proportional to the deviation; determining a sample rate needed to achieve a required measurement frequency; determining a recurrence of successive deviations; identifying a weight for the attribute constraint; and identifying outlying integrity confidence scores as exceptions across a plurality of client applications or client mobile devices. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 21 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.1.4 Claims 22-28

The subject matter of claim 22 differs from these prior art documents in an architecture comprising: native machine instrumentation for a mobile device is configured to: represent event subscriptions, callbacks, notification mechanisms provided by an operating system (OS) on the mobile device, and generate raw events; extended trust instrumentation; a runtime monitor configured to: subscribe to and receive near real time asynchronous notifications of application events for the applications from the extended trust instrumentation, and generate and send dynamic expressions or rules as application filters linked to running instances of the applications; a system event correlator configured to correlate system events of the mobile device to determine a calculus of risk; a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the mobile device and the applications; and an endpoint trust sensor configured to measure runtime operational integrity of the mobile device by evaluating risk based on actions of an application

Continued on The Next Page

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 182 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of : Previous Page

executing on, or a user of, the mobile device and receiving the raw events from the native machine instrumentation. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 22 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 23-28 are directly or indirectly dependent on claim 22. Consequently, claims 23-28 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.5 Claims 29-48

The subject matter of claim 29 differs from these prior art documents in a system comprising a reputation broker configured to: process a query for a reputation score of the subject received at a trust broker from a service provider; and dispatch a request to a trust orchestrator to generate a hierarchical reputation score for the subject, wherein the trust orchestrator is configured to process a received request for a hierarchical reputation score by: initiating a plurality of directed queries to information management systems internal or external to an organization to interrogate attributes associated with the subject; analyzing received query responses; receiving a generated hierarchical reputation score for the subject based on a calculus of risk; and sending the received hierarchical reputation score for the subject to the reputation broker; receive a reputation token from the reputation broker for the subject in response to the dispatched request; and send the reputation token to the service provider as a response to the query. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 29 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 30-48 are directly or indirectly dependent on claim 29. Consequently, claims 30-48 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.6 Claims 49-52

The subject matter of claim 49 differs from these prior art documents in a method comprising: receiving, at the trust orchestrator by the reputation broker, from a service provider, a query for the reputation score of a subject; dispatching, at the trust orchestrator by the reputation broker, a request to generate a just-in-time reputation score for a subject; and processing, at the trust orchestrator by the trust broker, the received reputation request by: initiating, a plurality of directed queries to external information management systems to interrogate attributes associated with a subject, analyzing, received query responses and generate

Continued on The Next Page

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 183 of 318

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of : Previous Page

a reputation score for a subject based on a calculus of risk, sending, a reputation score for a subject to the reputation broker, and sending, by the reputation broker at the trust orchestrator, as a query response to a service provider, a reputation token for a subject. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 49 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 50-52 are directly or indirectly dependent on claim 49. Consequently, claims 50-52 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.7 Claims 53-58

The subject matter of claim 53 differs from these prior art documents in a system comprising: a trust orchestration server configured to: perform a calculus of risk on a global security context including endpoint assessment reports received from collaboration services, and send system warnings based upon the endpoint threat intelligence to the network trust agent; and a remediation engine configured to receive real time directives for control of the computing device or application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 53 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 54-58 are directly or indirectly dependent on claim 53. Consequently, claims 54-58 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.8 Claims 59-60

The subject matter of claim 59 differs from these prior art documents in a method comprising: determining, by the network analyzer, anomalies based on network activity correlation and network malware detection; determining, by the trust broker, system configuration anomalies based on system level normalization and collation of assessments; determining, by the endpoint trust agent, resource utilization anomalies based on rulesets associated with central processing unit(CPU), memory, storage, and network resources usage; determining, by the endpoint trust agent, application integrity anomalies based on the rulesets associated with static and dynamic image analysis; correlating, by the trust orchestrator, network activity and endpoint events and behaviors characterized through continuous local and remote monitoring of network endpoints for risk analysis and detection of infected systems; and mitigating, by the trust orchestrator, infected systems through automated machine, network flow,

Continued on The Next Page

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 184 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of: Previous Page

or transaction-level remediation controls. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 59 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claim 60 is dependent on claim 59. Consequently, claim 60 is also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.9 Claims 61-72

The subject matter of claim 61 differs from these prior art documents in a method comprising: generating, by a trust broker, temporal events related to an endpoint system; receiving, at the trust orchestrator, by the trust supervisor: infection profiles from the network analyzer, and integrity profiles from the system event correlator; identifying and categorizing, by the trust supervisor, threats and infections diagnosed at the endpoint system; receiving, by the remediation controller, at the trust orchestrator, directives from the trust supervisor to initiate a remediation sequence; and sending, by the remediation controller, at the trust orchestrator, actions to network elements for orchestration and policy enforcement services based on established thresholds and triggers. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 61 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 62-72 are directly or indirectly dependent on claim 61. Consequently, claims 62-72 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.10 Claims 73-75

The subject matter of claim 73 differs from these prior art documents in a method comprising: displaying, in the GUI, a status and progress of initiated remediation actions; and displaying, in the GUI, details of malware analytics comprising one or more of: infection summaries, infection diagnosis, threat categorization and identification based on a signatureless infection life-cycle model, an address and geo-location for a source or attacker, an identification of one or more infected victims, forensic evidence chain of detected malicious activities and intent, and compute, memory, storage and network level anomalies detected on the victim machine or infected system. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 73 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 74-75 are dependent on claim 73. Consequently, claims 74-75 are also considered to

Continued on The Next Page

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 185 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of : Previous Page

be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.11 Claim 76

The subject matter of claim 76 differs from these prior art documents in a method comprising: correlating, by a trust orchestrator, network activity and endpoint events and behaviors characterized through continuous local and remote monitoring of network endpoints for risk analysis and detection of infected systems; and mitigating, by the trust orchestrator, an infected system using inputs received from a real time threat visualization dashboard to implement flow level or transaction level remediation controls. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 76 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.1.12 Claims 77-81

The subject matter of claim 77 differs from these prior art documents in a method comprising: correlating, by an event and behavior correlation engine, risk based on monitoring; and displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 77 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 78-81 are directly or indirectly dependent on claim 77. Consequently, claims 78-81 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.13 Claims 82-86

The subject matter of claim 82 differs from these prior art documents in a system comporising: a reputation broker configured to: process a query from a service provider for a reputation score of the subject, and dispatch a request to generate a hierarchical reputation score for the subject; a trust orchestrator configured to: process a received request from the reputation broker for a hierarchical reputation score by: initiating a plurality of directed queries to information management systems external to an organization to interrogate attributes associated with the subject, analyzing received query responses, receiving a generated hierarchical reputation score for the subject based on a calculus of risk; and sending the received hierarchical reputation score for the subject to the reputation broker; receive a reputation token from the reputation broker for the subject in response to the dispatched

Continued on The Next Page

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 186 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of : Previous Page

request; and send the reputation token to the service provider as a response to the query. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 82 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 83-86 are dependent on claim 82. Consequently, claims 83-86 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.14 Claims 87-93

The subject matter of claim 87 differs from these prior art documents in a method comprising: generating temporal events based at least in part on analyzing network endpoint assessments; correlating received endpoint events and generated temporal events; and generating an integrity profile for the system. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 87 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 88-93 are directly or indirectly dependent on claim 87. Consequently, claims 88-93 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.15 Claims 94-105

The subject matter of claim 94 differs from these prior art documents in a method comprising: processing and correlating, by the trust orchestrator, one or more of: a system integrity profile generated based on a calculus of risk, a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and a system infection profile received from a network analyzer; sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments; and sending, by the network trust agent, messages or directives to OpenFlow security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 94 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 95-105 are directly or indirectly dependent on claim 94. Consequently, claims 95-105 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

Continued on The Next Page

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 187 of 318

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of : Previous Page

2.1.16 Claim 106

The features of independent claim 106 essentially correspond to those of claim 22. Thus, the same reasoning as in claim 22 applies to claim 106. Therefore, claim 106 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.2 Industrial Applicability (PCT Article 33(4))

Claims 1-106 are industrially applicable under PCT Article 33(4).

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 188 of 318

Electronic Acknowledgement Receipt

EFS ID:	16901155
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Jennifer A. Wilson/Taya M. Hawkins
Filer Authorized By:	Jennifer A. Wilson
Attorney Docket Number:	0079152-000015
Receipt Date:	19-SEP-2013
Filing Date:	27-JUL-2012
Time Stamp:	14:53:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_KUMAR015.PDF	613552 f66207d30f6e5cfa7a56f0211e6057aedcf18f36	no	6

Warnings:	
Information:	

2	Foreign Reference	KR_20110027386.PDF	1655084 43f263341030fce51de88d200f3464977aa389bc	no	15
Warnings:					
Information:					
3	Non Patent Literature	NortonManual.pdf	10376720 723c4cda750171fdf5b9d06ee0d4ffe77ced501b	no	334
Warnings:					
Information:					
4	Non Patent Literature	WindowsManagment.pdf	731559 748fc432c93f82ce893b85797a99b5c24e0b0148	no	5
Warnings:					
Information:					
5	Non Patent Literature	StaticAnalysis.pdf	520471 b302b3a912d74abca32c31de514681b683489a65	no	5
Warnings:					
Information:					
6	Non Patent Literature	ISR.PDF	620829 d9ea61b90857ebc6dd503f8edeae5784c1ae3404	no	16
Warnings:					
Information:					
7	Non Patent Literature	OA6202013.PDF	1098646 9a2b6a3acc32402c0a2bf484c6429694e03d8f71	no	32
Warnings:					
Information:					
8	Non Patent Literature	OA7182013.PDF	1506966 f294be13724724162bf4eae1223f317144dc0186	no	39
Warnings:					
Information:					
		Total Files Size (in bytes):	17123827		

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	13559707
Filing Date	2012-07-27
First Named Inventor	Srinivas KUMAR et al.
Art Unit	2431
Examiner Name	Unassigned
Attorney Docket Number	0079152-000015

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					

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	20050289072	A1	2005-12-29	Sabharwal	
	2	20070143474	A1	2007-06-21	Sheng et al.	
	3	20070174406	A1	2007-07-26	Morris et al.	
	4	20090094584	A1	2009-04-09	Dheap et al.	
	5	20090144818	A1	2009-06-04	Kumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

	6	20090138939	A1	2009-05-28	Kumar et al.	
	7	20090276204	A1	2009-11-05	Kumar et al.	
	8	20090241170	A1	2009-09-24	Kumar et al.	
	9	20090133110	A1	2009-05-21	Kumar et al.	
	10	20090328186	A1	2009-12-31	Pollutro et al.	
	11	20120216244	A1	2012-08-23	Kumar 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

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	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

	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	13559707
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000015

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	/ R. K. Baldwin /	Date (YYYY-MM-DD)	2012-11-09
Name/Print	Randall K. Baldwin	Registration Number	59713

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.

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 196 of 318

Electronic Acknowledgement Receipt

EFS ID:	14188780
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Randall K. Baldwin/Kevin Chanthakhoune
Filer Authorized By:	Randall K. Baldwin
Attorney Docket Number:	0079152-000015
Receipt Date:	09-NOV-2012
Filing Date:	27-JUL-2012
Time Stamp:	10:57:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	PTO_SB08.PDF	612594 68562ce17952416580ffd1fa9d58f7121577500b	no	5

Warnings:	
Information:	

Total Files Size (in bytes):	612594

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/559,707

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	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	14 minus 20 =	*			OR	x 60 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1				x 250 =	250
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).						0.00
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	1500

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.

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
13/559,707	07/27/2012	2431	1500	0079152-000015	14	4

CONFIRMATION NO. 1767

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

FILING RECEIPT

OC000000055850031

Date Mailed: 08/10/2012

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Applicant(s)

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

Assignment For Published Patent Application

Taasera, Inc., Erie, PA

Power of Attorney: The patent practitioners associated with Customer Number 21839

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/641,007 05/01/2012

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 08/08/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/559,707**

Projected Publication Date: 11/07/2013

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

Preliminary Class

713

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 (1-866-999-4158).

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).

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate 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.

Patent
Attorney Docket No. 0079152-000015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT APPLICATION TRANSMITTAL LETTER
FOR ELECTRONICALLY FILED UTILITY APPLICATION

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

Customer Number **2 1 8 3 9**

Sir:

Enclosed for filing is the utility patent application entitled:

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

by the following named inventor(s):

Srinivas KUMAR; and Dennis Vance POLLUTRO

☒ Applicant(s) suggests Figure __1__ for inclusion on the front page of the patent application publication and patent.

☒ Applicant(s) requests that the published application include the following assignment information: TAASERA, INC., Cupertino, California, USA.

☐ Small entity status is claimed.

Also enclosed are:

DRAWINGS: 29 sheets of drawings

DECLARATION: ☐ will follow ☒ executed, is enclosed ☐ unexecuted, is enclosed

ASSIGNMENT: ☒ is being filed electronically concurrent with the electronic filing of the application.
☐ will follow.

CLAIM FOR PRIORITY UNDER 35 USC § 119 and/or 365: ☐ is made in the declaration ☒ is hereby made as follows:

Country	Appl. No.	Filing Date MM-DD-YYYY
US	61/641,007	05-01-2012

OTHER PAPERS:
☒ A General Authorization for Petitions for Extensions of Time and Payment of Fees
☐ An Information Disclosure Statement
☒ An Application Data Sheet
☐ Other:

Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

(10/08)

☒ The filing fee has been calculated as follows:

☐ and in accordance with the enclosed Preliminary Amendment:

					FEES
Basic Patent Application Filing Fee (1011)					$380.00
Examination Fee (1311)					$250.00
Search Fee (1111)					$620.00
	No. of Claims		Extra Claims	Rate	
Total Claims	14	Minus 20=		x $ 60.00 (1202)	
Independent Claims	4	Minus 3=	1	x $ 250.00 (1201)	250.00
If multiple dependent claims are presented, add $450.00 (1203)					
App. Size Fee (app + dwgs. exceeding 100 sheets) - $310.00 / each add'l. 50 sheets (1081)					
TOTAL APPLICATION FEE DUE					**$1,500.00**

☒ Charge $1,500.00 to credit card. Filing fee is being paid electronically concurrent with filing of application.

☒ The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Please address all correspondence concerning this application to:

Buchanan Ingersoll & Rooney PC
Customer Number **2 1 8 3 9**

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 27, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Charles F. Wieland III/Beverly Caraway
Attorney Docket Number:	0079152-000015
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Independent claims in excess of 3	1201	1	250	250
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		1500

Electronic Acknowledgement Receipt

EFS ID:	13355414
Application Number:	13559707
International Application Number:	
Confirmation Number:	1767
Title of Invention:	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/Beverly Caraway
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000015
Receipt Date:	27-JUL-2012
Filing Date:	
Time Stamp:	10:26:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1500
RAM confirmation Number	9367
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		SPEC.pdf	312048 8efef67e667f0d3862411908fd6c3df46047cd1e	yes	71

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Specification	1	65
Claims	66	70
Abstract	71	71

Warnings:					
Information:					
2	Drawings-only black and white line drawings	DRAW.pdf	9379301 d565ca2657e4e78dd6ff606e370cc49c54fcb7ca	no	29
Warnings:					
Information:					
3	Oath or Declaration filed	DEC.pdf	196746 1c2931fd25946c08f8707cae500005de28f31040	no	4
Warnings:					
Information:					
4	Authorization for Extension of Time all replies	GENAUTH.pdf	35954 1185b9277d51bc8c2cc0914649e0135bef9fa1c9	no	1
Warnings:					
Information:					
5	Application Data Sheet	ADS.pdf	67752 6e9a500c5f07717a736d45aff387444fe5cefc14	no	3
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
6	Transmittal of New Application	TL.pdf	125718 3fc7ff50b81224f7cba9d2fa7d1c1354aa157f2f	no	2
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	36777 e7a5b65dd7225c2127237b63a874955a904e467e	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	10154296

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.

APPLICATION FOR
UNITED STATES LETTERS PATENT

FOR

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

by

SRINIVAS KUMAR
and
DENNIS POLLUTRO

Attorney Docket No. 0079152-000015
BUCHANAN INGERSOLL & ROONEY PC
CUSTOMER NO. 21839
P.O. Box 1404
Alexandria, VA 22313-1404

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of U.S. Provisional Appl. No. 61/641,007 entitled "System and Method for Operational Integrity Attestation," filed May 1, 2012, incorporated by reference herein in its entirety.

BACKGROUND OF THE DISCLOSURE

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to the field of data center virtualization and, more particularly, to systems and methods for providing dynamic operational integrity attestation of application security and a user reputation at runtime.

DESCRIPTION OF THE RELATED ART

[0003] One recent trend in computing is the trend towards virtualization and cloud computing in which, for example, enterprise software is no longer owned by the customer, but instead the enterprise's Information Technology (IT) infrastructure can be provided by a third party and enterprise software applications are sold as service offerings.

[0004] Traditional legacy and currently available security technologies, such as next-generation anti-virus software, network firewalls, and intrusion detection/prevention systems, operate based on signatures, protocol anomalies or virtual execution in a sandbox to monitor threats and attacks. However, once a target of an attack or threat (i.e., a 'target system' or 'target platform') becomes infected or compromised, many of these technologies have been proven relatively ineffective in protecting systems and preventing data breaches or service disruptions. Emerging threats and attacks can exhibit a low and slow mode of operation and can be signature-less in order to evade traditional detection and

defense technologies. Further, these technologies are often agnostic to the runtime operational integrity of computer workloads on the target (victim) systems and therefore often do not offer any level of remediation to service the affected target systems. As such, many traditional security technologies merely provide coarse-grained access controls limited to a simple allow or deny decision logic.

[0005] Many enterprises and organizations are moving there IT infrastructures to cloud computing environments (from self-managed on-premise data centers to service-provider managed outsourced virtual data centers), wherein which third parties may provide shared computing resources and applications running on those resources. They are being offered as services to a plurality of customers. The move by companies to cloud computing environments are increasing for various reasons, including the need for increased computing power, increased storage capacity, and/or increased network bandwidth, among others. Enterprise applications and mission critical applications may be executed in the cloud. Without adequate device, system, and application security, the cloud can compromise these applications, potentially causing large financial losses. Data confidentiality, data integrity and data availability can be maintained in the cloud computing environment even when such applications may be controlled by these third parties. The cloud may enable traditional information technology devices, systems and applications to transparently execute from these service-providers managed outsourced virtual data centers. As newer technologies emerge, the cloud infrastructure may evolve transparent to and scalable with enterprise operations. Security in such environments may be an emerging challenge. For example, virtualized, cloud computing on-demand, and elastic models require dynamic security orchestration at both the device and network level that is lacking in traditional security approaches and technologies.

[0006] A significant metric that relates to the lack of remediation controls in current security controls is the high rate of false positives and negatives in the detection of threats. False positives are unproductive and reduce operating capacity in data centers. False negatives lead to the bypass of security controls and compromise of the target systems and services. Existing signature-based approaches to security control are vulnerable to improvised attacks staged at targeted systems.

[0007] The proliferation of applications (business, social networking and gaming software) in Enterprise and cloud computing ecosystems has significantly increased the attack surface and window of exposure. Application runtime operational integrity is a critical factor in building end-to-end trust from device to service. The proliferation of unmanaged devices such as mobile computing devices (i.e., tablets and smart phones) and Bring Your Own Device (BYOD) policies in Enterprise network environments has increased the risk of advanced coordinated threats.

[0008] The current predominant security paradigm is based on a hard edge and soft core architecture. Security appliances such as network firewalls and intrusion detection/prevention systems deploy at the edge (perimeter). Antivirus and network based integrity measurement and verification services scan and audit the soft-core that comprises business critical systems, services and high value data silos. Once the edge is breached, defensive methods are largely ineffective in protecting vulnerable or compromised systems. In this paradigm, the hard edge does not generally provide any level of assurance of the runtime operational integrity of the soft core.

[0009] The heavy reliance on extensive application whitelists/blacklists(based on file hash digests and/or configuration), Internet Protocol (IP) address reputation lists, signatures, protocol anomalies and virtual execution in a sandbox, provides targeted and coordinated attacks a large staging surface to maneuver around with meticulously engineered evasion methods exploiting the gaps. Irrespective of the method of break-in, the post-infection behaviors during the window of exposure on a victim machine or environment are difficult to conceal, but may be obscured from timely detection and diagnosis by security administrators and virtual execution (sandbox) environments through evasion techniques. Various exemplary embodiments include an early warning system for threat identification and diagnosis with high forensic confidence and infection summaries for manual and/or automated intervention.

[0010] Current identity management (IdM) approaches are typically aimed at domain level authentication of users for the use of a security token in a transaction or business process wherein the issuance of the token is strictly based on proof of

possession of credentials and not the reputation of the user. While the industry has adopted multi-factor authentication technologies for increased protection from malicious users whose intent is to steal credentials for the purpose of impersonation or delegation, these security controls do not provide a means for incorporating attribution of an authenticated user's risk posture, independent of provisioned entitlements (i.e., user account privileges and roles). Thus, existing security controls do not incorporate a complete view of a user's risk posture as a component of an access policy, based on correlation of location and device agnostic global threat intelligence about the user. Accordingly, what is needed are systems and methods for runtime operational integrity monitoring of applications by providing dynamic operational integrity attestation of application security and user reputation at runtime that take into account a subject's (such as a device, application, or user) risk posture. What is further needed are systems and methods for performing post infection diagnoses, threat identification via signature-less anomalous behavior recognition using non-intrusive platform instrumentation without requiring 'hooks' into an operating system (OS) Kernel by security vendors that leverages OS vendor application programming interfaces (APIs).

[0011] The emerging cloud based application-hosting model requires a higher level of scrutiny of device and user security posture. Threats can be posed by both external and internal users, and therefore it has become harder to determine whether an authenticated user is a trustworthy operative. Application and network layer entitlements are largely static in nature. While role based access control (RBAC) systems are positioned to offer dynamic policies, these are not based on any form of aggregation of external threat intelligence in the context of the user in the transaction.

[0012] Tokenization of identities by Security Token Services (STS) intended to facilitate in Identity Federation and Single Sign On (SSO) for web and Enterprise applications have only aggravated the threat vectors by expanding the scope of resources that an authenticated user may access implicitly without granular context. Along with the coarse access policies offered by traditional security controls, such as firewalls and intrusion prevention systems, this increases the attack surface for

application exploits by malicious users leveraging the excessive privileges granted by default to most users (and groups) today, in the absence of strict Separation of Duties (SoD) and Principle of Least Privilege (PoLP) enforcement.

[0013] Several studies have uncovered conclusive evidence that the largest risk, associated with malicious activities resulting in theft of confidential data, intellectual property or financial losses for enterprises and consumers, arises from insider rather than outsider or man-in-the-middle attacks. Threat assessment systems have been predominantly focused on the means and methods rather than the adversary or operator (i.e., a user). There has been no emphasis on the reputation score of a user in the transaction or business process as a real time integrity metric for integration with access policy decision logic. Accordingly, what is further needed are systems and methods that employ a user reputation score that can serve either as a punitive or corrective method of intervention for the proactive prevention of exploits and data breaches.

[0014] One goal of trusted computing is to provide a resource owner or service provider with reliable knowledge about a target system. Current attestation systems are components of computer systems that permit reliable statements of evidence about those systems to be conveyed to remote parties, including other computers. Through evaluation of the identity and integrity of components of a system (i.e., a target system being evaluated), evidence is produced that the target system will not engage in defined classes of misbehaviors. As the users accessing a system and the requirements of applications running on a system generally cannot be known a priori, attestation systems and measurement systems alike must be flexible, providing for privacy, completeness of measurement, and trust in the basic collection and reporting mechanisms.

[0015] Existing attestation systems are often narrowly focused and generally aimed at specific use-cases limited to system components such as hardware and applications and therefore typically lack flexibility to dynamically address more general attestation problems. Further, existing definitions of attestation focus primarily on describing specific, narrow, and particular properties desirable in specific use-cases. Additionally, current attestation systems are created to work with one

particular measurement system targeting one particular system of interest without considering the reputations of users or operators of the system of interest.

[0016] Accordingly, what the present inventors have identified as desirable are technology based attestation architectures, systems, and methods that perform a calculus of risk to determine a level of trust of systems that are not necessarily monolithic and can be made up of diverse hardware and software platforms and can be accessed by users with varying credentials and reputations. Accordingly, what the inventors have identified as being desirable are attestation architectures, systems, and methods that can be flexible enough to accommodate varying concepts of attestation, including taking the reputation of users that access targeted systems into account. What the present inventors also see as desirable are attestation systems and architectures that can dynamically handle complex attestation scenarios and provide more complete runtime attestation than is currently achievable. What the present inventors additionally see as desirable are methods and systems for performing evidence based automated application binary analysis.

SUMMARY OF THE DISCLOSURE

[0017] Exemplary methods and systems are disclosed for continuously monitoring one or more systems and/or to correlate events and behavior of systems on an instrumented target platform at runtime using or based on a plurality of assertions (or statements).

[0018] In exemplary embodiments, methods, apparatus, systems and computer readable media perform infection diagnosis based on reconnaissance based intelligence correlation and a threat life cycle model of advanced low-and-slow attacks wherein malware may operate through a series of benign actions at an endpoint device.

[0019] In other exemplary embodiments, methods, apparatuses, systems and computer readable media comprise a plurality of services that enable visibility, control, and/or compliance in a cloud computing environment with a runtime dashboard to capable of displaying operational integrity metrics of systems based on a plurality of threat vectors.

[0020] In yet other exemplary embodiments, methods, apparatuses, systems and computer readable media establish device-to-network flows based on dynamic attestation of device integrity, and/or security controls provisioned based on integrity and context aware business logic instead of, for example, topology based coordinates associated with encapsulation headers in network packets.

[0021] Exemplary systems and methods for dynamic attestation of application integrity are described in U.S. Non-Provisional Patent Application No. 13/399,065 entitled "System and Method for Application Attestation," filed February 16, 2012, and U.S. Provisional Patent Application No. 61/443,854 entitled "System and Method for Application Attestation," filed February 17, 2011, both of which are incorporated herein by reference in their entireties.

[0022] According to exemplary embodiments, methods, apparatuses, systems and computer readable media authorize user-to-application transactions and/or data exchange in an established connection, during the authentication phase based on dynamic attestation of devices.

[0023] In accordance with further exemplary embodiments, methods, apparatuses, systems, and computer readable media determine a calculus of risk based on a plurality of sensory inputs from network and endpoint sensors to correlate network activity, system configuration, resource utilization and application integrity.

[0024] According to an exemplary embodiment, the network and endpoint sensors may be configured to measure runtime operational integrity and/or detect anomalous deviations in behavior from baseline based on rule sets to generate tiered alerts.

[0025] In accordance with exemplary embodiments, methods, apparatuses, systems and computer readable media comprise an event and behavior correlation engine configured to receive alerts, calculate risks and generate warnings.

[0026] In other exemplary embodiments, methods, apparatuses, systems and computer readable media remediate systems that are deviated, vulnerable, in duress or compromised based on a calculus of risk.

[0027] In accordance with yet other exemplary embodiments, methods, apparatuses, systems and computer readable media include: (1) a correlation engine configured to receive scan reports from vulnerability, configuration, compliance, and

patch scan services; (2) a risk correlation matrix configured to store elements of the scan reports that are used to analyze the elements; and (3) a module configured to generate an integrity profile of systems.

[0028] The presently disclosed exemplary technical solutions also may be embodied as methods, apparatuses, systems and computer readable media comprising: (1) event correlation logic that correlates temporal system events based on multiple predicate scores; (2) logic to determine a predicate score based upon a deviation from a prescribed value constraint per attribute (or metric, i.e., an attribute constraint); (3) logic for calculating a score that is inversely proportional to the deviation; (4) logic for determining a sample rate needed to achieve a required measurement frequency; (5) logic for determining a recurrence of successive deviations; (6) logic for identifying a weight for the attribute constraint; (7) logic for determining an integrity confidence for the system or process (or application) entity as a weighted average of predicate scores; and (8) logic for determining identifying outliers as exceptions (across multiple systems or processes).

[0029] The exemplary methods, apparatuses, architectures, systems and computer readable media disclosed herein may also use threat identification categories including, but not limited to:

[0030] (1) static image analysis (i.e., static analysis of binary files, intermediate code, and/or scripts);

[0031] (2) dynamic image (binary, intermediate code, or script) analysis with process, platform and network monitors;

[0032] (3) malware analysis for evasion techniques (multiple packing, obfuscated application programming interfaces (APIs), anti-debugging, anti-memory, anti-tracing, virtual machine monitor/manager (VMM) or hypervisor/emulator detection;

[0033] (4) dynamic system analysis of performance metrics harvested through native machine instrumentation, registry, and file system monitors; and

[0034] (5) temporal system analysis with consolidated integrity measurement and verification assessments and scan reports.

[0035] The presently disclosed exemplary technical solutions may be embodied as a method, apparatus and/or system for integrity confidence measurement including:

(1) a weighted average of system (or platform) predicate scores; (2) system (or platform) outliers; (3) weighted average of process (or application package) predicate scores; (4) process outliers.

[0036] The presently disclosed exemplary technical solutions also may be embodied methods, apparatuses, architectures, systems and computer readable media for generating user reputation scores for a plurality of users based on one or more of: (1) threat vectors modeled by actions of the plurality of users; (2) risk correlation with aggregation of intelligence related to accessed object (resource) attribution, subject roles, globally unique subject identifiers, security information and event management analytics, and geo-location services.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0037] The presently disclosed exemplary technical solutions are best understood from the following detailed description when read in connection with the accompanying drawings, to which the claimed invention is not limited. According to common practice, various features/elements of the drawings may not be drawn to scale. Common numerical references represent like features/elements. The following figures are included in the drawings:

FIG. 1 is an architecture diagram of an exemplary system for providing operational integrity attestation of application security and user reputation, according to an embodiment of the present disclosure;

FIG. 2 is a schematic diagram illustrating an exemplary system for endpoint and network activity correlation, according to an exemplary embodiment of the present disclosure;

FIG. 3A is a flowchart illustrating steps by which early warning and response automation is performed through monitoring, orchestration and remediation, according to an exemplary embodiment of the present disclosure;

FIG. 3B is a data flow diagram for intersystem risk assessment and remediation, according to an exemplary embodiment of the present disclosure;

FIG. 4 is a data flow diagram for configuring an attestation system by consolidating and normalizing network endpoint assessments, according to an exemplary embodiment of the present disclosure;

FIG. 5 illustrates communications between components of a system for measuring and evaluating application operational integrity, according to an exemplary embodiment of the present disclosure;

FIG. 6 is a block diagram illustrating data flows for instrumenting and measuring network endpoint risk, according to an exemplary embodiment of the present disclosure;

FIG. 7A depicts exemplary endpoint events that can be monitored by the systems and methods disclosed herein;

FIG. 7B depicts exemplary endpoint alerts that can be generated by the systems and methods disclosed herein;

FIG. 7C is a block diagram illustrating a method for correlating endpoint alerts and generating endpoint warnings, according to an exemplary embodiment of the present disclosure;

FIG. 8 is a block diagram of a trust orchestration architecture for correlating a plurality of events for determining operational integrity of a system, according to an exemplary embodiment of the present disclosure;

FIG. 9 is a block diagram of a system for consolidating and correlating a plurality of identity, inventory and log management systems for determining a reputation of a user, according to an exemplary embodiment of the present disclosure;

FIG. 10 is a block diagram of a system for determining a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIG. 11 is block diagram of a of a system for generating subject reputation scores based on a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIG. 12 is a block diagram of a system for network flow remediation based on a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIG. 13 a block diagram illustrating of a system for providing mobile security by remediating mobile devices and wireless network flows based on a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIGs. 14-18 depict a graphical user interface (GUI) for an exemplary trust management console including dashboards for operational runtime integrity, system configuration, resource, application integrity, and network activity, in accordance with various exemplary embodiments;

FIGs. 19-22 are flowcharts illustrating methods for threat identification and remediation, providing a user reputation service, and providing network flow level remediation in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 23 is an entity-relationship diagram (ERD) illustrating relationships between entities of a reputation scoring system, according to an embodiment of the present disclosure;

FIG. 24 illustrates a hierarchical representation of a subject reputation score, according to an embodiment of the present disclosure;

FIG. 25 is a block diagram of an architecture for monitoring application events with extensions to native machine instrumentation, according to an exemplary embodiment of the present disclosure; and

FIG. 26 is a diagram of an example computer system in which embodiments can be implemented.

DETAILED DESCRIPTION

[0038] Although the invention is illustrated and described herein with reference to certain exemplary embodiments, the invention is not intended to be limited thereto. Rather, various modifications may be made that are within the scope and range of equivalents of the claims and without departing from the invention. Various features, attributes and advantages described herein may or may not be present in various embodiments of the claimed invention.

[0039] In the detailed description herein, references to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every

embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0040] In certain exemplary embodiments, behavior deviations from a baseline healthy operational state to a vulnerable or compromised state may be detected, and the infection identified, before there is further propagation of the threat across interconnected systems, or information is exfiltrated resulting in data loss or theft.

[0041] The proliferation of unmanaged smart phones and Bring Your Own Device (BYOD) initiatives in the Enterprise ecosystem has increased the ability of advanced malware to evade traditional network and endpoint security controls and propagate to connected systems over standard protocols. Various exemplary embodiments include determination of the operational integrity of the device and/or the user in a transaction with an on-premise or off-premise service, based on the calculus of risk from a plurality of sensory inputs, for transaction and/or flow level remediation of infected devices.

Network for Monitoring and Dynamic Analysis of Events and Activities

[0042] FIG. 1 is an architecture diagram for an exemplary network 100 configured to continuously monitor and dynamically analyze events and network activity to ascertain the integrity of a monitored system (i.e., a target system).

[0043] Referring to the exemplary embodiment provided in FIG. 1, the network 100 includes an event and behavior correlation engine 130 configured to perform risk correlation 120 based on continuous monitoring 110 using a plurality of sensory inputs. In the embodiment of FIG. 1, the sensory inputs can include, but are not limited to, one or more of: network activity 111; system configuration 113; resource utilization 115; and application integrity 117. The network 100 also comprises a runtime dashboard 150 configured to receive real time status indications 131 for visibility of operational integrity of systems and a remediation engine 170 configured to receive real time directives 132 for control of infected systems.

[0044] The event and behavior correlation engine 130 is configured to receive network events and infection profiles 112 from a network activity sensor 111, integrity measurement and verification reports 114 of scans performed by a system configuration sensor 113. According to an embodiment, the scans are performed by the configuration sensor 113 according to a schedule. In embodiments, the scans can be scheduled to run daily, weekly, bi-weekly, monthly, or at other time increments as needed.

[0045] As shown in FIG. 1, the event and behavior correlation engine 130 is also configured to receive endpoint events 116 of computing, network and storage resource consumption from a resource utilization sensor 115, and endpoint events of image profiles and local execution context 118 from an application integrity sensor 117. Details of exemplary implementations of the system configuration sensor 113, the resource utilization sensor 115, the application integrity sensor 117, and the endpoint events 116, 118 are described below with reference to FIGs. 4-7.

[0046] The remediation engine 170 may perform actions 171 on a virtual machine (VM) 172, actions 173 on a network flow controller 174, or actions 175 on a transaction 176 based on configured trigger controls.

[0047] As will be appreciated by persons skilled in the relevant art(s), a VM is a software implementation of a machine such as a server, personal computer, mobile computing device, or other computing device that supports the execution of an operating system (OS) and executes applications as a physical machine running that OS would. A VM is a software implementation that duplicates the functionality of a physical machine implemented in hardware and software. Software applications and the OS running on a VM are limited to the resources and abstractions provided by the VM. Virtual machines (VMs) can be viewable within an overall virtual infrastructure. As will be appreciated by those skilled in the relevant art, a VMM or hypervisor can be used to start up, monitor, and manage VMs. Such hypervisors can be, but are not limited to VMMs such as the VMWARE™ Player, MICROSOFT™ VirtualPC, SUN™ VirtualBox, VMWARE™ ESX/ESXi, MICROSOFT™ Hyper-V, CITRIX™ XENServer, PARALLELS™ and others. As it would be apparent to one of

skill in the art, other hypervisors and VMs/virtualization solutions can be used for VM 172 in network 100 as well.

Example System and Method for Endpoint and Network Activity Correlation

[0048] FIG. 2 is a schematic diagram illustrating an exemplary system 200 for endpoint and network activity correlation. In particular, the system 200 shown in FIG. 2 is configured to receive inputs for endpoint events, correlate the events, and generate outputs such as, but not limited to, warnings and reports.

[0049] As shown in FIG. 2, the exemplary system 200 may include an endpoint event correlation module 240 configured to receive endpoint alerts 230 from an instrumented system 210 with a plurality of sensors configured to detect endpoint events related to one or more of application integrity 211, resource utilization 212, and system configuration 213. The system 200 also comprises a network activity correlation module 260 configured to receive network alerts 250 from a network activity sensor 220.

[0050] With continued reference to FIG. 2, the network activity correlation module 260 is further configured to produce network warnings 270 resulting from the network activity correlation and output the network warnings 270 to an orchestrator 290. The orchestrator 290 is configured to receive network warnings 270 from network activity correlation module 260 and endpoint warnings 280 from the endpoint event correlation module 240. According to embodiments depicted in FIG. 2, the received network warnings 270 and endpoint warnings 280 can be used by orchestrator 290 to coordinate manual or automated actions on infected systems.

[0051] With continued reference to FIG. 2, the orchestrator 290 can similarly receive warnings produced by one or more additional instrumented systems (see, e.g., VM #N) with respective pluralities of sensors and endpoint event correlation modules.

[0052] As shown in FIG. 2, the instrumented systems can include multiple virtual machines (VMs, i.e., VM 1 … VM #N) with respective pluralities of sensors configured to detect endpoint events related to one or more of application integrity 211, resource utilization 212, and system configuration 213.

[0053] FIG. 3A is a flowchart illustrating steps by which early warning and response automation is performed using monitoring, orchestration and remediation, in accordance with an exemplary method.

[0054] As shown in FIG. 3A, an exemplary method 300 comprises receiving communications from an early warning system 301 configured to continuously monitor the runtime integrity of systems. This continuous monitoring enables near-real time determinations and detections of deviated, vulnerable, in duress, and compromised systems 307.

[0055] The method 300 can operate in conjunction with legacy security technologies 305 to fill in the security holes or gaps inherent in traditional security solutions. As illustrated in FIG. 3A, such legacy security technologies 305 can include anti-virus software, network firewalls, and intrusion detection/prevention systems (IDS/IPS). Unlike the early warning system 301 and the automated and rapid response 303, the legacy security technologies 305 are limited to using signatures, detecting protocol anomalies or virtual execution in a sandbox to monitor threats and attacks. As shown in FIG. 3A once a target of an attack or threat (i.e., a 'target system' or vulnerable system 307) becomes infected or compromised, these technologies 305 can be ineffective in protecting the compromised/infected systems 307 and preventing data breaches or service disruptions.

[0056] Example limitations of legacy security technologies 305 are shown in FIG. 3A. For example, as depicted in FIG. 3A, a traditional network firewall technology 305 using access control lists (ACLs) cannot reliably block every threat. This is because firewalls are typically limited to monitoring well-known, default open ports used as listening ports for web protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP), email protocols such as the Simple Mail Transfer Protocol (SMTP) and the Post Office Protocol (POP), and other protocols such as the File Transfer Protocol (FTP), the Secret File Transfer Protocol (SSH), Secure FTP (SFTP), telnet, and the Remote Desktop Protocol (RDP). IDS and IDP technologies using rulesets cannot detect every zero-day signature/anomaly attack and have issues with regarding false negatives and leaving platforms/systems

vulnerable to backdoor attacks. Similarly, anti-virus software cannot detect zero-day, mutant, and low-and-slow infections.

[0057] The method 300 can also supplement security audit scans 308 and manual IT process that may be in place. For example, an organization may periodically run security audit scans (i.e., on a weekly or bi-weekly basis). Such security audit scans may be National Institute of Standards and Technology (NIST)/Security Content Automation Protocol (SCAP) compliant checks for common vulnerability exposures to identify deviated and vulnerable systems 307. The results from these scans may be used as part of manual IT processes for ticketing (i.e., creating 'trouble tickets' for deviated/vulnerable systems 307) and security/compliance review boards. However, as shown in FIG. 3A these manual processes triggered by merely periodic scans can takes days or weeks to react to threats, thus leaving target systems open to a long window of exposure.

[0058] The method 300 improves upon the legacy technologies 305, periodic audit scans 308, and manual IT processes 309 and makes up for their above-noted shortcomings by carrying out an automated and rapid response 303 for orchestration and remediation of infected systems 307. In an embodiment, automated and rapid response 303 can be performed by monitoring and orchestration systems (not shown). In the example of FIG. 3, a protocol 302 is used for data exchange between the early warning system 301 and monitoring and orchestration systems.

[0059] In an embodiment, the early warning system 301 monitors instrumented systems to measure and evaluate runtime operational integrity to determine whether a system 307 has deviated, become vulnerable, is in duress or has been compromised. Once this determination has been made, the system 307 is marked by the early warning system 301 as one or more of a deviated system, a vulnerable system, an in duress system, or a compromised/infected system. The early warning system 301 can then issue warnings regarding the system 307 via the protocol 302 so that an automated and rapid response 303 can be carried out by monitoring and orchestration systems.

[0060] FIG. 3B is a schematic diagram illustrating an exemplary method 310 for determining a calculus of risk, in accordance with exemplary embodiments.

[0061] Referring to FIG. 3B, the exemplary method 310 may include determining or performing a calculus of risk 320 for the data center application and data silos, that receives sensory inputs 314 from instrumentation 313 including integrity measurement and verification scan correlation 315, network activity correlation 316 and endpoint event correlation 317, and may generate integrity metrics for security orchestration 321, and may dispatch directives to an edge device 323 (for example, network firewall) for user access controls 322, to a load balancer 325 for session controls 324, or to a network fabric element 327 (for example, a switch or router) for flow controls 326.

[0062] With continued reference to FIG. 3B, the security orchestration 321 may include user access controls 322 as a remediation or mitigation means to block the infected device or malicious user from accessing protected data center centers, session controls 324 to divert users from infected systems or infected devices from protected systems, flow controls 326 to quarantine infected systems, divert traffic away from protected systems, or redirect traffic from attackers to pure, high-interaction or low-interaction honeypots.

[0063] FIG. 4 illustrates data flows used to configure an attestation system. In particular, FIG. 4 depicts a data flow for consolidating and normalizing network endpoint assessments as part of a configuration for an exemplary attestation system 400.

[0064] Referring to FIG. 4, the exemplary attestation system 400 includes a trust orchestrator 430, a trust broker 407 configured to receive integrity reports 406 published by endpoint assessment services 401.

Trust Broker and Integrity Report

[0065] With continued reference to FIG. 4, the trust broker 407 can be configured to receive sensory data feeds that represent the configuration state of the system based on a remotely administered scan of a device, such as device 560 described with reference to FIG. 5 below, by endpoint assessment services 401. These scans provide a snapshot in time of the state of the system and are agnostic to runtime aspects of the system including applications thereon.

[0066] In an embodiment, the sensory data is represented in a markup language such as, but not limited to, Extensible Markup Language (XML). An integrity report 406 incudes this sensory data. In embodiments, the integrity report 406 is generated by third party endpoint assessment services at platform- and application-level granularities. According to embodiments, the integrity report 406 may be received by the trust broker 407 either: (a) programmatically through outbound application programming interfaces (APIs) provided by respective application vendors; or (b) manually through importing the integrity report 406 as a file provided by an administrator through a dashboard of an administrative console user interface (UI) in a specified file format. Examples of an administrative console UI are discussed below with reference to FIGs. 14-18.

[0067] The trust broker 407 can also be configured to parse, normalize and collate received integrity reports 406. In accordance with embodiments, the parsing, normalizing, and/or collating can be based on one or more object identifiers. Exemplary object identifiers can include, but are not limited to, machine hostnames, IP addresses, application names, and package names. This parsing, normalization, and collation (collectively, processing) generates temporal events 409 that annotate the state of the endpoints (devices) at scan time. Additional embodiments of the trust broker are described with reference to FIGs. 5, 9, and 11 below.

Temporal Events

[0068] According to embodiments, the temporal events 409 can be expressed as assertions about operational parameters (e.g., vulnerabilities, compliance, patch level, etc.) based on enterprise policies established for a baseline configuration. The trust broker 407 serves as a moderator that aggregates endpoint operational state measurements for situation awareness and threat identification by the trust orchestrator 430.

[0069] With continued reference to FIG. 4, the temporal events 409 can be an annotation (e.g., an XML representation) of the configuration state of the system (including device, application and package) and include trust and severity scores as generated by third party security vendors based on integrity measurement and verification, in accordance with standards established by organizations. These

organizations can include NIST, the MITRE Corporation, and the United States Computer Emergency Readiness Team (US-CERT). The temporal events can be assertions about operational parameters expressed in the Open Vulnerability and Assessment Language (OVAL) to convey system details representing configuration information and a system/machine state including vulnerability, configuration, patch level, etc. Alternatively, the system details can be conveyed using the SCAP protocol. According to embodiments, the state representation includes schema attributes to measure configuration, vulnerability (exposures), compliance, and patch level based on severity. Compliance can be expressed in terms of the Extensible Configuration Checklist Description Format (XCCDF) using XCCDF checklists for devices attached to a system's Peripheral Component Interconnect (PCI) bus, and data security/system integrity compliance with the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and/or the Gramm–Leach–Bliley Act (GLBA).

[0070] As shown in FIG. 4, the integrity reports 406 can be generated by performing one or more scans, including, but not limited to, a vulnerability scan 402, a configuration scan 403, a compliance scan 404, and a patch scan 405 of networked endpoints. In an embodiment, the trust broker 407 can be implemented as the Trust-as-a-Service (TaaS) Broker from TAASERA, Inc. In one exemplary embodiment, the trust orchestrator 430 can be implemented as the TaaS Orchestrator from TAASERA, Inc.

[0071] With continued reference to FIG. 4, the attestation system 400 further comprises a normalizer and collator 408 and a system event correlator 410 configured to receive temporal events 409 associated with an endpoint and use a risk correlation matrix 411 to correlate and generate an integrity profile 420 for an endpoint. According to embodiments, the system event correlator 410 shown in FIG. 4 can be configured to receive temporal events 409 generated by the trust broker 407 that measure the integrity of the system at last scan. Additional exemplary features of the system event correlator 410 are described below with reference to FIG. 5.

Integrity Profile

[0072] In the embodiments of FIGs. 4-6, the integrity profile 420 represents an aggregation of system warnings (threats such as malware) identified based on the received temporal 409 and endpoint 520 events. In one embodiment, the format (schema) of the integrity profile 420 is a standard Extensible Markup Language (XML) notation.

Risk Correlation Matrix

[0073] In embodiments, the risk correlation matrix 411 depicted in FIGs 4-6 and the risk correlation matrix 721 described with reference to 7A-7C are embodied as grids that represent an exemplary dynamic model of measurement and identification based on clustering and classification of independent endpoint events (alerts) to generate system warnings that may be mapped to warning categories or classes. Additional details of the risk correlation matrices 411 and 721 are provided below with reference to FIGs. 6, 7B, and 7C.

System for Evaluating Operational Integrity of Applications

[0074] FIG. 5 illustrates communications between components of a system 500 for measuring and evaluating application operational integrity. In particular, FIG. 5 depicts communications between components of the application operational integrity system 500 used to evaluate application integrity based upon executable image profiles and process monitoring, and evaluate resource utilization based upon process and system monitoring. In embodiments, image profiles are generated for executable images such as, but not limited to, binary images, intermediate images, or scripts. FIG. 5 is described with continued reference to the embodiment illustrated in FIG. 4. However, FIG. 5 is not limited to that embodiment.

[0075] As shown in FIG. 5, the exemplary application operational integrity system 500 includes an endpoint trust agent 510 on a device 560 comprising a process monitor 514 configured to observe local execution context of applications and services. The endpoint trust agent 510 further comprises a socket monitor 513 configured to observe network activities of applications and services and a system monitor 512 configured to observe system and platform resources consumed by applications and services. In the example embodiment provided in FIG. 5, the trust

agent 510 also comprises an application integrity module 516 and a resource utilization module 515 configured to assess operational integrity based on rulesets. The trust agent 510 can also comprise native machine instrumentation 511 for a computing device being monitored by the application operational integrity system 500.

Device

[0076] In embodiments, the device 560 depicted in FIG. 5 may be a desktop, server, laptop, a mobile computing device such as a smart phone or tablet, or other types of mobile computing platforms that comprise (a) an operating system (OS); (b) a user operating the device to access a service or another device 560 over a network; and (c) application packages, applications or application components that may be downloaded and installed either with or without user intervention for later execution. Non-limiting examples of the device 560 include a personal computer, server, laptop, or tablet device running a MICROSOFT™ WINDOWS® operating system (OS), a personal computer, server, or laptop running an OSX OS from Apple Inc., a personal computer, server, or laptop running a UNIX or Linux OS, a personal digital assistant (PDA), an iPhone™, an iPod™ touch, or iPad™ tablet device running an iOS from Apple Inc., a device operating the Android OS from Google Inc., device running the MICROSOFT™ WINDOWS® Mobile or Phone OS, a device running a Symbian OS, a device running a PALM OS®, a BLACKBERRY® device running a Blackberry OS from Research In Motion ("RIM"), a mobile phone, a portable game device, a gaming console, a hand held computer, a netbook computer, a palmtop computer, an ultra-mobile PC, or another similar type of computing device capable of processing instructions and receiving and transmitting data to and from users and other computing devices.

Native Machine Instrumentation

[0077] In embodiments, the native machine instrumentation 511 can represent any event subscription, callback, notification mechanism provided by the supported operating system (OS) on the device 560 (e.g., MICROSOFT™ WINDOWS® Machine Instrumentation (WMI), Transport Filter Drivers, Application Layer Enforcement Callout Drivers, Linux/Unix Network Filter Drivers, etc.). The native

machine instrumentation 511 can generate raw events, as described below with reference to the illustrative example in FIG. 7A, that may appear insignificant as an isolated occurrence, but may include notable data points as forensic evidence of behavior anomalies or malicious activity to the event and risk correlation system.

[0078] Referring to FIG. 5, the trust broker 407 can be configured to receive one or more state attributes pertaining to applications running on a device 560 and components from the endpoint trust agent 510. The trust broker 407 serves as an arbitrator configured to dispatch a request for image analysis to one or more third party malware analyzers 540. In one embodiment, the dispatch mechanism uses trigger filter expressions that specify the set of criteria that warrant initiation of image analysis (e.g., frequency and volume of requests for analysis associated with the image across deployed endpoint trust agents), and parameters configured for each available connector to a third party malware analyzer 540. According to an embodiment, the parameters include cost, latency, and platform specific analysis capabilities. Such platform specific analysis capabilities can include static and dynamic analysis of applications on mobile platforms such as, but not limited to, devices 560 running an Android operating system (OS) from Google Inc., a PALM OS®, a MICROSOFT™ WINDOWS® Mobile or Phone OS, a Symbian OS, a Blackberry OS from Research In Motion (i.e., a BLACKBERRY® device 560), or an iOS (i.e., iPhone™, an iPod™ touch, or iPad™ devices 560).

[0079] The third party malware analyzers 540 perform static and dynamic analysis of the application images based on policies specified by the trust broker. The result of the malware analysis is a set of threats identified based on the analysis. The trust broker caches the results of the analysis indexed by a unique identifier for the image. The trust broker generates and returns an image profile 519 to the endpoint trust agent 510 which comprises assertions of malicious capabilities of the image that must be monitored at runtime for subsequent generation of endpoint events 520 by the endpoint trust agent 510.

Endpoint Events

[0080] In the embodiment shown in FIG. 5, the endpoint events 520 are generated by a component of the endpoint trust agent 510, and represent alerts based an

endpoint sensor resident on the device 560. The alerts are mapped to a cell in the risk correlation matrix 411 grid by the system event correlator 410. In one embodiment, the format (schema) of the endpoint events 520 is a standard Extensible Markup Language (XML) notation. Additional features of the endpoint events 520 are described below with reference to FIG. 6

[0081] With continued reference to FIG. 5, the application operational integrity system 500 can include a trust orchestrator 430 comprising a system event correlator 410 and a trust broker 407. The application operational integrity system 500 can further include a malware analyzer 540. In an embodiment, the trust orchestrator 430 can be implemented as the TaaS Orchestrator from TAASERA, Inc.

[0082] According to the exemplary embodiment depicted in FIG. 5, the system event correlator 410 can be configured to receive endpoint events 520 from the endpoint trust agent 510 as sensory inputs to a calculus of risk. The trust broker 407 is configured to receive an image file and image attributes 518 and then send the received image file to the malware analyzer 540 for diagnosis. The trust broker can also receive an asynchronous prognosis 533 and forward an asynchronous image profile 519 to the process monitor 514 to include in ruleset processing for diagnosis at the application integrity module 516.

System Event Correlator

[0083] According to embodiments, the system event correlator 410 shown in FIG. 5 can be configured to receive temporal events 409 generated by the trust broker 407 that measure the integrity of the system at last scan, and endpoint events 520 from the endpoint trust agent 510 that measure the runtime execution state of applications. The system event correlator 410 can be further configured to map the events to a cell in the risk correlation matrix 411 grid and processes the triggered system warnings to evaluate threats by category (or vectors). In one embodiment, the categories include at least resource utilization, system configuration, and application integrity. Each category is assigned a metric that is an indicator of the level of runtime operational integrity that may be asserted based on the system warnings and threat classification produced by the risk correlation matrix 411. The system event correlator 410 can also be configured to generate an integrity profile

420 for the device 560 that describes the security risks and threats posed by the measured execution state of running applications on the device 560.

[0084] FIG. 6 depicts data flows between components of an exemplary system for correlating endpoint events. In particular, FIG. 6 illustrates data flows between components and modules of a system event correlation system 600. FIG. 6 is described with continued reference to the embodiments illustrated in FIGs. 4 and 5. However, FIG. 6 is not limited to those embodiments.

[0085] Referring to FIG. 6, the exemplary correlation system 600 includes an endpoint trust agent 510 on a device 560 that comprises runtime monitor 620 configured to register for and receive a plurality of raw events 611 from native machine instrumentation 511 on the device 560. The runtime monitor 620 is further configured to raise integrity events 621 to an integrity processor 630 that may apply rulesets 631 to generate integrity alerts 632 and generate or populate an event correlation matrix 633 that maps integrity warnings 634 to endpoint events 520 for dispatch to a trust orchestrator 430.

[0086] In the embodiments shown in FIGs. 6 and 7A-7C, the endpoint events 520 are generated by the integrity processor 630, which is a component of the endpoint trust agent 510, and represent alerts based an endpoint sensor resident on the device 560. As described above with reference to FIG. 5, the alerts can then be mapped to a cell in the risk correlation matrix 411 grid by the system event correlator 410, which can be configured to read endpoint events 520 expressed in XML notation.

[0087] With continued reference to the exemplary embodiment provided in FIG. 6, the trust orchestrator 430 comprises a system event correlator 410 configured to use a risk correlation matrix 411 to generate an integrity profile 420 for the monitored system (i.e., the target system). In one embodiment, the system event correlator 410 can be implemented as a correlation engine. In another embodiment, the trust orchestrator 430 can be implemented as the TaaS Orchestrator from TAASERA, Inc.

[0088] For the risk correlation matrix 411 shown in FIG. 6, each cell in the grid is a set of alerts triggered through an event correlation matrix 633 and rulesets 631 (rule expressions) by the endpoint trust agent 510.

[0089] In certain exemplary embodiments, the application integrity module 516 and the resource utilization module 515 described above with reference to FIG. 5 may be included as a subcomponent or module of the integrity processor 630 depicted in FIG. 6.

[0090] In certain exemplary embodiments, the process monitor 514, system monitor 512 and socket monitor 513 depicted in FIG. 5 and described above may be included as subcomponents or modules of the runtime monitor 620.

[0091] FIG. 7A is a diagram indicating groupings of exemplary endpoint events 700 that can be monitored and analyzed by the presently disclosed methods and systems to determine a system integrity profile. In particular, the endpoint events 700 shown in FIG. 7A can be used to determine what an attestation system can assert about the integrity of a monitored system (i.e., a target system). FIG. 7A is described with continued reference to the embodiments illustrated in FIGs. 1, 4, 5, and 6. However, FIG. 7A is not limited to those embodiments.

[0092] By continuously monitoring for the endpoint events 700 and performing dynamic analysis of detected endpoint events 700, assertions about the integrity of a target system can be made. For example, the endpoint events 700 can be included in the endpoint events 116, 118 received by the event and behavior correlation engine 130 in the network 100 described above with reference to FIG. 1.

[0093] In one embodiment, one or more of the endpoint events 700 can be included in the endpoint events 520 used by the attestation system 500, described above with reference to FIG. 5. In other embodiments, the endpoint events 700 can be included in the endpoint events 520 used by the system event correlator 410 of the correlation system 600 depicted in FIG. 6.

[0094] Referring to FIG. 7A, the exemplary endpoint events 700 may include per process events 701, per processor events 702, system events 703, and per image binary analysis events 704. According to an embodiment, the events 701-704 can include, but are not limited to, all events available through native machine instrumentation and extensible on the platform with provider plug-ins.

[0095] FIG. 7B is a block diagram 710 illustrating exemplary alerts that can be generated by the methods and systems discussed herein.

[0096] As shown in FIG. 7B, in embodiments, alerts may include platform alerts 711, per image alerts 712, grayware alerts 713 (i.e., for a watch list), and per application alerts 714. The alerts are configurable and extensible, and not limited to the alerts illustrated in FIG. 7B.

[0097] FIG. 7C is a block diagram illustrating an exemplary method 720 for correlating endpoint alerts and generating endpoint warnings using a correlation matrix. FIG. 7C is described with continued reference to the embodiments illustrated in FIGs. 4-6. However, FIG. 7C is not limited to those embodiments.

[0098] Referring to FIG. 7C, the method 720 populates a risk correlation matrix 721 based upon one or more of system warning classes 722, system warnings 723, and integrity warnings 724. As shown in FIG. 7C, an alert expression can be expressed as a function 725 of at least an attribute, an attribute value constraint, a sample rate, a recurrence, a score and a weight. The function may be specified in any programming language or construct, as compiled, intermediate or interpreted code.

[0099] The risk correlation matrix 721 can comprise a universally unique identifier (UUID) for the system, system warnings 723 mapped to at least one system warning class 722, and at least a system warning class 722 to diagnose system deviations (i.e., system deviated integrity warnings 724), system duress, system vulnerable and system infections (i.e., system infected integrity warnings 724).

[0100] In the embodiment of FIG. 7C, each alert for the risk correlation matrix 721 is generated by a program function 725 that evaluates expressions that are specific for each attribute of the device 560. Based on the occurrence of a qualifying set of alerts in each cell, the corresponding system warning is triggered. In FIG. 7C, the exemplary risk correlation matrix 721 illustrates that for each device 560 (or application) uniquely identified by a machine identifier (e.g., a virtual machine universally unique identifier (UUID), IP address) or application instance identifier (application UUID), a different set of alerts may trigger different system warnings that map to a common system warning class. By mapping alerts to a behavior model (or cluster), unknown (such as emerging or polymorphic) threats may be classified and identified without requiring image or wire level signatures. The alerts may be grouped as illustrated in FIG. 7B to represent a category of alerts (e.g., platform,

application, grayware - that includes applications that are placed on a watch list based on reports generated by third party malware analyzers, image – that are weighted by threat level based on inspections performed by the endpoint trust agent 510 or malware analyzers 540). In an embodiment, the program function 725 can be configured to use conditional expressions (operators) to generate an alert based on value constraints, sample rate for the measurement, recurrence of measured values, an assigned score and weight for the attribute. According to embodiments, the score and weight can be predefined or customizable through a graphical user interface GUI or dashboard, such as the GUIs described below with reference to FIGs. 14-18.

[0101] In accordance with embodiments, a plurality of timers may be associated in the evaluation of system warnings and system warning classes, the calculus of risk, and generation of an integrity profile for the system.

[0102] According to embodiments, the integrity profile 420 comprises at least the endpoint address and one or more of system warning class, forensic confidence of the declared warning, and the full evidence chain.

Integrity Processor

[0103] With reference to FIGs. 6 and 7A-7C, the integrity processor 630 is a functional component of the endpoint trust agent 510. The integrity processor 630 can be configured to receive integrity events 621 from the runtime monitor 620 that describes process, processor, system and binary analysis events illustrated in FIG. 7A. Applying qualifying rule expressions (illustrated in FIG. 7B) in the rulesets 631, integrity alerts 632 are generated and mapped to a cell in an event correlation matrix grid 633 (analogous to the risk correlation matrix 411 of FIG. 4 and grid 721 of FIG. 7C) to generate system level integrity warnings 634. The rows in the event correlation matrix 633 represent an application instance on the device 560 (analogous to rows in the risk correlation matrix 411 that represent a device by machine identifier). The integrity warnings 634 can be formatted as endpoint events 520 for dispatch to the system event correlator 410 of the trust orchestrator 430 for threat classification and identification and subsequent remediation.

[0104] In accordance with embodiments, a plurality of alerts 711-714 in a variety of user configurable combinations (for example, as editable settings in an XML or text

format configuration file, or through a graphical administrative dashboard or user interface) constitute a system warning, and a system warning maps to a system warning class.

[0105] In accordance with embodiments, a plurality of system warning classes can be included in the integrity profiles 420 of the attestation system 400 and correlation system 600 depicted in FIGs. 4 and 6 respectively.

Example Trust Orchestration Architecture

[0106] FIG. 8 is a block diagram of an exemplary architecture 800 for trust orchestration including a trust orchestrator 430, a network analyzer 830, and a device 560. The architecture 800 can be used to correlate a plurality of events for determining runtime operational integrity of a system. FIG. 8 is described with continued reference to the embodiments illustrated in FIGs. 4, 5, and 7C and with reference to FIGs. 12 and 13. However, FIG. 8 is not limited to those embodiments.

[0107] As shown in FIG. 8, the trust orchestration architecture 800 may include an endpoint trust agent 510 on a device 560, a network analyzer 830 that may include a network activity correlator 831, an endpoint assessment service 820, a service provider for orchestration and/or policy enforcement point services 860, and a trust orchestrator 430 that may include a trust broker 407, a system event correlator 410, a trust supervisor 846, and a remediation controller 848.

Trust Orchestrator

[0108] According to the embodiments of FIGs. 4 and 8, the trust orchestrator 430 is an aggregation that includes functional components such as the trust broker 407, system event correlator 410, the trust supervisor 846, and remediation controller 848. In embodiments, the trust orchestrator 430 is configured to receive sensory threat intelligence from network analyzers 830, endpoint assessment services 820 and endpoint trust agents 510 on devices 560. Through a sequence of normalization, collation and risk correlation of events, directives 849 in the form of directives are dispatched to orchestration services to initiate remediation actions to deal with identified threats on devices 560. The directives are specific to the orchestration service and can include the use of vendor APIs. Examples of such vendor APIs include VMWARE™ vCloud APIs, BMC Atrium™ APIs for accessing a

BMC Atrium™ configuration management database (CMDB) from BMC Software, Inc., Hewlett Packard Software Operations Orchestration (HP-OO) APIs, and standard protocols such as OpenFlow.

[0109] In certain exemplary embodiments, the system event correlator 410 receives endpoint events 520 from the endpoint trust agent 510, temporal events 409 from the trust broker 407, correlates and sends an integrity profile for a network endpoint to the trust supervisor 846 and the network activity correlator 831.

[0110] In certain exemplary embodiments, the trust supervisor 848 receives an infection profile 832 for a network endpoint from the network activity correlator 831, an integrity profile 420 for a network endpoint from the system event correlator 410, analyzes and classifies threats along with a forensic confidence score, sends real time actions 847 to the remediation controller 848, and real time status indications 850 to a dashboard controller 870. The remediation controller 848 sends directives 849 to orchestration and/or policy enforcement point services 860 for machine, flow or transaction level remediation.

Remediation Controller

[0111] In embodiments, the remediation controller 848 can be configured to receive action requests 847 from the trust supervisor 846. The remediation controller 848 can also be configured to process the received requests and perform appropriate operations on orchestration services. According to embodiments, upon processing a received action request the remediation controller 848 may perform (a) a flow level operation on a network element 1216 (e.g., a physical or virtual switch or a firewall) or wireless access point 1320; (b) a machine level operation on a device 560 (e.g., a web or database server); (c) a transaction level operation to restrict access to a service or device 560; and/or (d) an update notification to a network trust agent (see, e.g., network trust agents 1209 and 1315 depicted in FIGs. 12 and 13, respectively) to indicate a revised reputation score for a device 560.

[0112] In embodiments, the infection profile 832 comprises at least the victim endpoint address and one or more of a forensic confidence of the declared infection, the attacker source, the command and control source, the full evidence chain, and the infection time range (onset, duration).

[0113] According to embodiments, the integrity profile 420 comprises at least the endpoint address and one or more of system warning class, forensic confidence of the declared warning, and the full evidence chain.

[0114] In accordance with embodiments, the risk correlation matrices 411 and 721 of FIGs. 4 and 7C, respectively, may be included in the trust supervisor 846 to consolidate and correlate integrity profile 420 and infection profile 832 of FIG. 8.

Example Threat Detection and Mitigation Scenario

[0115] An exemplary flow of a threat detection and mitigation sequence is described below with reference to FIGs. 3A, 4-6, 7B, 8, 10, 12, 13, and 23. In the example scenario below, the exemplary threat is a user device infected with malware. The paragraphs below detail how exemplary embodiments described herein with reference to FIGs. 4-6, 7B, 8, 10, 12 and 13 can handle such 'real world' threat vectors. The multi-dimensional event and risk correlation model described in the following paragraphs illustrates an exemplary method of detecting low and slow signature-less threats that are characteristic of emerging malware and advanced persistent threats.

[0116] A user's (1014) device D (560) may become infected with a form of an advanced persistent threat (e.g., malware $M_{(benign)}$) while he device D is still connected to an enterprise network of an organization 2303. The connection of the device D to the enterprise network can occur through user activity, for example, when the user 1014 connects a plug-and-play portable universal serial bus (USB) device with the malware $M_{(benign)}$ to the device D while it is connected to the enterprise network, as the result of the user 1014 opening an email attachment infected with the malware $M_{(benign)}$, when the user 1014 accesses a social network application from the device D, or when the user 1014 unwittingly transfers a file with the malware $M_{(benign)}$ to device D while accessing a file sharing service.

[0117] The device D can also become infected with malware $M_{(benign)}$ while the device D is disconnected from the enterprise network of the organization 2303. For example, the device D can become infected as a result of user activity on a home network, or external wireless or wired network not managed by an enterprise IT administrator of the organization 2303, such as a mobile network or the Internet.

[0118] Once the device D is infected, an egg download (i.e., download of an .egg compressed archive file) that evaded traditional network edge protections (e.g., legacy security technologies 305 such as firewalls and network IPS/IDS systems) has occurred. At this stage of infection, legacy security technologies 305 such as traditional antivirus programs installed on the device D are unlikely to detect the targeted malware $M_{(benign)}$ because no signature or blacklist already exists for this threat. The malware $M_{(benign)}$ may then perform discrete (and apparently benign) surveillance operations on the device D, such as periodic process restarts, executable file property modifications (i.e., changes to file name and/or size attributes) to introduce entropy and evade detection. The malware $M_{(benign)}$ may also make registry modifications, perform keyboard/input device monitoring, screen level monitoring, memory dumps, disk navigation to inspect files without excessive resource (CPU) utilization on the device D.

[0119] At this post-infection stage, the endpoint trust agent 510 monitors the executing malware process $P_{(benign)}$, performs file and component (e.g., dynamic link library(DLL)) level integrity checks including checking a file hash digest, digital signature, and certificate chain verification by leveraging collaboration services, such as the collaboration services 1207 and 1312, described below with reference to FIGs. 12 and 13, respectively, to access intelligent whitelisting services. These collaboration services are accessed through the trust orchestrator 430. Failure of one or more of these checks immediately places process $P_{(benign)}$ on a grayware alert 713 (i.e., a watch list).

[0120] Assuming no checks fail at this stage, the process $P_{(benign)}$ is continuously monitored by the integrity processor 630 for explicit rule violations. In an embodiment, violations of a rule in a ruleset 631 are continuously monitored for and detected. These rules detect anomalous behaviors in benign processes. Once a rule trigger criteria is reached, the endpoint trust agent 410 initiates an image integrity check and leverages a remote malware analyzer 540 through the trust orchestrator 430. The purpose of this check is to avoid complete reliance on supply chain provenance and locally available evidence. The image profile 519 generated

from malware binary analysis provides the integrity processor additional local events to monitor for process $P_{(suspect)}$.

[0121] At this point, the malware analyzer 540 reports capabilities detected (present in reverse engineered code) through static and dynamic analysis of the image. Such image analysis can look for code obfuscation techniques in the reverse engineered code such as anti-debug, anti-trace, anti-memory, and anti-emulation, use of network communication protocols like SMTP, FTP or HTTP, use of embedded uniform resource locators (URLs) or IP addresses, use of encryption methods such as use of the secure sockets layer (SSL) protocol, listening on local ports, remote ports accessed, file system operations, registry operations, operations in temporary, system or non-program folders, memory peek or poke operations, and remote thread creation.

[0122] The integrity processor 630 then monitors process $P_{(suspect)}$ for related warnings 721 and triggers endpoint events such as alerts 711-714 to the system event correlator 410. Multiple endpoint assessment services 820 may be deployed in the enterprise network to perform scheduled policy based scans to detect known exposures (vulnerability, configuration, compliance and patch level exploits). The respective integrity reports 821 may contain indications of exposures on the device D. However, these reports do not affirm positive presence of a threat or an infection on the device D and may be unaware of the existence and runtime activities of process $P_{(suspect)}$. The trust broker 407 generates temporal events 409 that inform the system event correlator 410 of the damage potential (severity) on the device D should any malicious program be active on the device (e.g., a personally identifiable information (PII) violation on a database server, a buffer overflow attack on an application server, a structured query language (SQL) injection attack on a database server, a keystroke or screen element capture, a microphone or camera hijack, etc.) based on authoritative state (snapshot) information and scan policies applied in the assessment of device D.

[0123] Based on risk analysis triggered by endpoint and temporal events, an integrity profile is generated by the system event correlator 410 for the device D. The network activity correlator 831 concurrently monitors all network traffic and

activities of device D and dispatches infection profiles 832 based on forensic evidence of malicious network dialogs indicative of an infected victim (device D). The evidence may be indicative of malicious activities such as peer-to-peer propagation, command and control communications, or data exfiltration to an attacker. The trust supervisor 846 classifies the forensic evidence based on the integrity and infection profiles generated independently by the endpoint, network, and scan based assessment sensors to determine the threat risk level of the device D with high forensic confidence to warrant an immediate manual or automated remediation action to mitigate the detected infection.

System for Integrity Profile Generation

[0124] FIG. 9 is block diagram illustrating an exemplary system for generating a subject integrity profile. The system 900 shown in FIG. 9 can be used to consolidate and correlate a plurality of identity, inventory and log management systems in order to determine a reputation of a subject (e.g., a user, device, transaction, service, or organization/company). FIG. 9 is described with continued reference to the embodiments illustrated in FIGs. 4 and 5. However, FIG. 9 is not limited to those embodiments.

[0125] Referring to FIG. 9, the exemplary subject integrity profile system 900 includes a trust orchestrator 430, a trust broker 407 that can be configured to query and receive an associated response 905 from a plurality of management systems.

[0126] With continued reference to FIG. 9, the integrity profile system 900 can include a plurality of subsystems, including an inventory management system 901 configured to provide resource object attributes, a role management system 902 configured to provide subject (or user) attributes (e.g., roles and entitlements), an identity management system 903 configured to provide aggregated subject attributes, a log management system 904 configured to provide information and events categorized by subject, a system event correlator 410 that receives temporal events 409 categorized by subject, and a risk correlation matrix to generate an integrity profile 420 for a subject that comprises a unique subject identifier and a reputation score.

[0127] Within the context of the subject integrity profile system 900, the trust broker 407 is configured to query and receive responses from third party management systems regarding inventory, role, identity and logs.

Inventory Management System

[0128] The inventory management system 901 shown in FIG. 9 is configured to provide information pertinent to devices 560 (e.g., mobile devices 560, mobile applications, enterprise desktops, servers, etc.). Examples of inventory management systems 901 include commercial products available from the IBM and Oracle Corporations used for managing an inventory of Enterprise IT managed assets.

Role Management System

[0129] According to embodiments, the role management systems 902 shown in FIG. 9 can be configured to provide information pertinent to a user's organizational roles, resource level privileges, application level entitlements, and extended group memberships (i.e., project level privileges and roles). Examples of role management systems include commercial products available from Oracle, Computer Associates, IBM, and SAP for role based access controls to database objects, files, servers, directories/folders, web servers, applications, network domains/subdomains, printers, and other resources. In some of these systems, users are assigned one or more roles that aggregate a set of privileges and permissions. For example, roles in an Oracle or IBM relational database environment represent different tiers or levels of access to database objects. For example, a user account with a 'database administrator' (DBA) role may have privileges and permissions needed to delete (i.e., drop), create, and alter database objects such as tables, views, synonyms, stored procedures, triggers, user accounts, entire databases, and other roles. In contrast user accounts with lesser roles, such as a developer or user role may only be able to insert and update data in database tables and views and revise existing stored procedure and trigger code. Yet other roles may be restricted to 'read only' access to select records from database tables and views as needed to generate reports and run queries.

Identity Management System

[0130] In accordance with embodiments, the identity management systems 903 shown in FIG. 9 can be configured to provide information pertinent to a user's organizational domain accounts and group level memberships (e.g., MICROSOFT™ Active Directory, Oracle Internet Identity).

Log Management System

[0131] In embodiments, the log management systems 904 shown in FIG. 9 can be configured provide information pertinent to a user's activities at the endpoint device and at the network level of operations based on logs generated by endpoint and network elements and reported through standard system information and event management protocols (e.g., SYSLOG) and formats such as the WebTrends Enhanced Log file Format (WELF) or the Common Event Format (CEF) used for network security applications.

Systems for Determining Calculus of Risk and Subject Reputation Scores

[0132] FIG. 10 is a block diagram illustrating an exemplary system for determining a calculus of risk. FIG. 10 is described with continued reference to the embodiments illustrated in FIGs. 4, 5 and 8. However, FIG. 10 is not limited to those embodiments.

[0133] Referring to FIG. 10, the exemplary calculus of risk system 1000 includes a network endpoint assessment 1001 configured to generate a network security scan report 1025, an endpoint collator 1002 to parse a plurality of received reports for categorization by address or geo-location, a normalizer 1003 for report consolidation, an object collator 1004 for categorization by package and component, an integrity processor 630 on a device 560, for runtime system 1016, application 1015 and user 1014 context, an endpoint trust agent 510, a global object context generator 1005 for aggregation of context, an event processor 1006 for evaluation of context, a rules repository 1012 of object attributes configured to include at least constraints 1023, a sample rate 1022, a recurrence 1021, a score 1020 and a weight 1019 for integrity assessments, an event correlator 1007, an event correlation matrix 1013, a threat classifier 1008, a dashboard controller 1009, and a remediation controller 848.

Trust Supervisor

[0134] According to the exemplary embodiments of FIG. 8 and FIG. 10, the trust supervisor 846 can be configured to receive infection profiles 832 from the network analyzers 830 and integrity profiles 420 from the system event correlator 410. The trust supervisor 846 uses an event processor 1006, an event correlator 1007, a threat classifier 1008, an event correlation matrix 1013 and a rules repository 1012 to correlate events associated to a device 560 for the classification and identification of threats based on the forensic confidence of leading indicators.

[0135] In an embodiment, the network endpoint assessment 1001 comprises performing a security scan of network endpoints for vulnerability, configuration, compliance, and patch management and use the results of these scans to generate a security assessment report 1026. As shown in FIG. 10, an endpoint collator 1002 is configured to receive the generated security assessment report 1026. In embodiments depicted in FIG. 10, at this point, the endpoint collator 1002 can then sort the security assessment report 1026 by endpoint address and/or geo-location to produce categorized reports 1027.

[0136] A normalizer 1003 is configured to receive the categorized reports 1027 and then normalize the elements therein to produce normalized reports 1028.

[0137] An object collator 1004 is configured to receive the normalized reports 1028 and then sort the elements therein by object package and component to produce temporal events 1029 for the global object context generator 1005.

[0138] In certain exemplary embodiments, the global object context generator 1005 receives endpoint events 1018 that may include the local runtime object execution context from the integrity processor 630 on a device 1017, and temporal events 1029 that may include endpoint security context from the object collator 1004.

[0139] In exemplary embodiments, the event processor 1006 receives endpoint integrity profiles 420 from the global object context generator 1005, retrieves associated endpoint rules 1031 from the rules repository 1012, generates and sends endpoint alerts 1033 to the event correlator 1007.

[0140] According to exemplary embodiments, the event correlator 1007 receives endpoint events 1033 from the event correlator 1007, maps the alerts 1032 using the

event correlation matrix 1013, generates and sends endpoint warnings 1034 to the threat classifier 1008.

[0141] In accordance with exemplary embodiments, the threat classifier 1008 may categorize threats, send status indications 1024 to the dashboard controller 1009 for real time visibility of endpoint integrity, and send action requests 1025 to the remediation controller 848.

[0142] In certain exemplary embodiments, the endpoint collator 1002, normalizer 1003 and object collator 1004 may be included in the trust broker 407 as described above with reference to FIG. 4.

[0143] In certain exemplary embodiments, the global object context generator 1005 may be included in the system event correlator 410 described in FIG. 4.

[0144] In certain exemplary embodiments, the event processor 1006, event correlator 1007 and threat classifier 1008 may be included in the trust supervisor 846 as described in FIG. 8.

[0145] FIG. 11 is a block diagram illustrating an exemplary system for determining a subject reputation. FIG. 11 is described with continued reference to the embodiments illustrated in FIGs. 4, 5, 7C, and 8-10. However, FIG. 11 is not limited to those embodiments. For example, the system 1100 can be used to generate subject reputation scores based on a calculus of risk, such as the calculus of risk determined by system 1000 described above with reference to FIG. 10.

[0146] Referring to FIG. 11, the exemplary subject reputation system 1100 includes a user 1014 authenticated on a device 560 through an authentication process/ceremony 1115 with an authentication service 1103, a service provider 1104 configured to receive a service request, a managed application 1105 that may be the target service, a reputation broker 1106, a trust broker 407, a log management system 904, a role management system 902 and an identity management system 903.

[0147] Unless specifically stated differently, a user is interchangeably used herein to identify a human user, a software agent, or a group of users and/or software agents. Besides a human user who needs use devices 560 and the attestation systems described herein, a software application or agent sometimes needs to run

applications, access services or social networks, conduct online transactions, review, update, or analyze security data, and process events, alerts and warnings. Accordingly, unless specifically stated, the term "user" as used herein does not necessarily pertain to a human being.

[0148] With continued reference to FIG. 11, the exemplary subject reputation system 1100 also includes an inventory management system 901, a reputation processor 1110, a risk correlator 1111, a risk correlation matrix 1113, and a reputation score generator 1112.

[0149] In an embodiment, the reputation processor 1110 is a component of the system event correlator 410 configured to receive subject events 1123 from the trust broker 407 and includes user alerts 1124 that are analogous to integrity profiles 420 of a user 1101.

[0150] As shown in FIG. 11, the risk correlator 1111 can be configured to receive subject alerts 1124 such as alerts for a user 1014 or a device 560, and map the subject alerts 1124 to a cell in the risk correlation matrix 1113 grid analogous to the risk correlation matrix 721 in FIG. 7C. The subject warnings 1126 (i.e., user 1014 or device 560 warnings) triggered can then be processed by the reputation score generator 1112 to determine the user's 1014 reputation score 1125.

Subject Events

[0151] In embodiments, the subject events 1123 shown in FIG. 11 can be assertions about provisioned attributes, endpoint and network level activities associated with a subject, received as a response to a directed query from the respective management systems. The subject can be a user 1014, a device 560, a transaction, or an organization such as a company.

[0152] In certain exemplary embodiments, a device 560 sends a service request 1116 on behalf of a user 1014 to a service provider 1104 to access a managed application 1105. The service provider 1104 sends a reputation query 1117 to the reputation broker 1106, receives a reputation token 1118 that may include at least a reputation score for the user 1014 or device 560, and enforces a reputation-based access control 1119 to permit or deny the service request 1116 to access the managed application 1105.

[0153] Within the context of the subject reputation system 1100, the trust broker 407 is configured to process received subject attributes (e.g., entitlements, memberships of users 1014, roles for users 1014, activity information), to generate and dispatch subject events to the reputation processor 1110. The subject events represent assertions about the subject that may determine a level of security risk in a transaction (e.g., static and dynamic separation of duties, principle of least privilege, observed resource usage patterns, observed activities on the internal and external networks, etc.). In one embodiment, the queries 1121, 1130, 1122, 1128 issued by the trust broker 407 are preconfigured, but can be customized by the administrator from a graphical user interface (GUI) or dashboard, such as the exemplary GUI described below with reference to FIGs. 14-18. In embodiments, the management systems may include information systems hosted by social networking vendors such as FACEBOOK® operated by Facebook, Inc., Twitter operated by Twitter, Inc., and LinkedIn.

[0154] According to exemplary embodiments, the trust broker 407 receives a query 1120 for a reputation score for a subject (i.e., a user, device, transaction, service, or organization), sends a subject activity query 1121 to log management systems 904, sends a subject attribute query to role management systems 902 and identity management systems 903, sends a device attribute query to inventory management systems 1128, generates and sends subject events 1123 to the reputation processor 1110.

[0155] In the context of the subject reputation system 1100, the inventory management system 901 shown in FIG. 9 can be configured to provide information pertinent to subjects that are devices 560, including mobile devices 560, mobile applications, enterprise desktops, servers, etc.

[0156] With continued reference to FIG. 11, in an embodiment, associated device attributes include at least a device 560 geo-location, a device provisioned state, enabled/disabled device 560 functions, and an owner registration (i.e., a user 1014 registration or an organization registration).

[0157] In accordance with embodiments, the risk correlator 1111 is configured to receive subject alerts 1124, use the risk correlation matrix 1113 to map the subject

alerts 1124 to subject warnings 1126, and invoke the reputation score generator 1112 to establish a subject reputation score 1125, which can be included in the reputation token 1118 by the reputation broker 1106.

[0158] In the exemplary embodiment of FIG. 11, the subject alerts 1124 can be user 1014 alerts (i.e., user 1014 integrity profiles), device 560 alerts, or application alerts for an application executing on the device 560. In certain exemplary embodiments, the reputation processor 1110 may be included in the system event correlator 410 described in FIG. 4.

[0159] According to exemplary embodiments, the risk correlator 1111, the risk correlation matrix 1113 and the reputation score generator 1112, may be included in the trust supervisor 846 described in FIG. 8.

Systems for Providing Network Flow Remediation and Mobile Security

[0160] FIG. 12 is a block diagram illustrating an exemplary system for network flow remediation. FIG. 12 is described with continued reference to the embodiment illustrated in FIG. 5. However, FIG. 12 is not limited to that embodiment. The system 1200 can perform network flow remediation based on a calculus of risk.

[0161] Referring to FIG. 12, the exemplary network flow remediation system1200 may include an endpoint trust agent 1201 on a device 560 that may execute an application 1203, a trust orchestrator 1205, a plurality of collaboration services 1207 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1230 that may include a network trust agent 1209 and an OpenFlow security framework 1211, an OpenFlow controller 1214, and an OpenFlow enabled network element 1216 (for example, a switch or router).

[0162] In certain exemplary embodiments, the endpoint trust agent 1201 sends a dynamic context 1204 that may include the local runtime execution context of an application 1203 to the trust orchestrator 1205 that may perform a calculus of risk on a global security context, that may include endpoint assessment reports 1206 received from collaboration services 1207, and sends a system warning 1208 (endpoint threat intelligence) as a subscription based reputation service to a network trust agent 1209 for network flow remediation.

[0163] In certain exemplary embodiments, the network trust agent 1209 sends messages 1210 to the OpenFlow security framework 1211 middleware to send directives 1213 to an OpenFlow controller 1214, or send directives 1212 to an OpenFlow controller 1214, to notify by means of a protocol 1215 an OpenFlow enabled network element 1216 to apply access controls 1217 to block or divert traffic flows.

[0164] FIG. 13 is a block diagram illustrating an exemplary system for providing mobile security. FIG. 13 is described with continued reference to the embodiments illustrated in FIGs. 4-6. However, FIG. 13 is not limited to those embodiments. System 1300 can provide mobile security by remediating mobile devices and wireless network flows based on a calculus of risk.

[0165] Referring to FIG. 13, the exemplary mobile security system1300 includes an endpoint trust agent 1301 on a mobile device 560 that may execute a mobile application 1303, a trust orchestrator 1310, a plurality of collaboration services 1312 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1350 that may include a network trust agent 1315 and an network security framework 1318, a network element 1320 (for example, a switch or router), a wireless access point 1322, a mobile policy manager 1313 and a mobile device manager 1324.

Endpoint Trust Agent

[0166] Referring to FIGs. 5, 6 and 13, in an embodiment, the endpoint trust agent 510 resides on a device 560. The endpoint trust agent 510 can be configured to monitor all operations performed on the device 560 at runtime, including running applications and device functions (e.g., microphone, camera, keyboard, or display functions), and dispatches endpoint events 520 and security service requests 518 to the trust orchestrator 430. The runtime monitor 620, a functional component of the endpoint trust agent 510, includes a system monitor 512, a socket monitor 513, and a process monitor 514 that receive raw events 611 from native machine instrumentation 511 using a notification mechanism (e.g., MICROSOFT™ WINDOWS® Management Instrumentation (WMI) or the Android Application Manager). In certain exemplary embodiments, the endpoint trust agent 520 may

also receive and process messages from a mobile device manager 1324 or mobile policy manager 1313 to control device operations and/or settings. The endpoint trust agent 510 is risk and threat agnostic and merely generates events based on the evaluation of rulesets 631 and assessment of runtime behavior based on the threat correlation matrix 633. The assessment of risk, and classification and identification of threats can be delegated to the trust orchestrator 430.

[0167] In certain exemplary embodiments, the endpoint trust agent 1301 sends a dynamic context 1304 that may include the local runtime execution context of a mobile application 1303 to the trust orchestrator 1310 that may perform a calculus of risk on a global security context, that may include endpoint assessment reports 1311 received from collaboration services 1312, and sends threat intelligence as a subscription based reputation service 1314 to a network trust agent 1315 for network flow remediation.

[0168] In certain exemplary embodiments, the network trust agent 1315 sends messages 1316 to the network security framework 1318 middleware to send policies 1319 to a wireless access point 1320, or send policies 1317 to a wireless access point 1320, to apply access controls 1321 to block or divert traffic flows.

[0169] In certain exemplary embodiments, the trust orchestrator 1310 sends messages 1307 to the mobile policy manager 1313 to send directives 1308 to the mobile device manager 1324 to set feature controls 1306 on the mobile device 560 or send directives 1305 to the endpoint trust agent 1301 for the integrity processor 630 and runtime monitor 620 of FIG. 6.

[0170] In certain exemplary embodiments, the trust orchestrator 1310 is configured to send messages 1309 to the mobile device manager 1324 to set feature controls 1306 on the mobile device 560.

Example User Interface Dashboards for an Administration Console

[0171] FIGs. 14-18 illustrate exemplary graphical user interfaces (GUIs) according to embodiments of the present disclosure. The GUIs depicted in FIGs. 14-18 are described with reference to the embodiments of FIGs. 1-13. However, the GUIs are not limited to those example embodiments. FIGS. 14-18 illustrate an exemplary data center administration console interface comprising various dashboards for displaying

data related to operational integrity, resource utilization, application integrity, and network activity, in accordance with embodiments of the invention.

[0172] The terms “console display,” “display,” “display screen,” and “screen” are used interchangeably herein to refer broadly and inclusively to any type of display device or screen coupled to or integrated with a computing device for displaying content viewable by a user of the computing device, such as administrators for the systems describe herein or a user 1014 of a device 560. In an embodiment, the device 560 is a mobile computing device 560. Such a display screen can include, for example and without limitation, a touch-screen liquid crystal display (LCD). In embodiments of the invention, the GUIs of a mobile device 560 is viewed on a display. In other embodiments, the GUIs shown in FIGs. 14-18 are viewed on a display of a server (i.e., a server console), a desktop computer (i.e., a PC monitor), or a laptop display.

[0173] In the example GUIs shown in FIGs. 14-18, the console interface and dashboards are rendered in a dedicated, native interface. In alternative embodiments, the console interface can be web based and rendered within a web browser. In other embodiments, the console interface and dashboards illustrated in FIGs. 14-18 can be displayed on server or workstation displays having a touch sensitive (i.e., touch screen) display. For ease of explanation, the operation of the console interface is discussed in the context of a computing device platform with an input device such as a mouse or pointing device (including a touch-screen), but is not intended to be limited thereto. Examples of such computing device platforms include, but are not limited to, OSX server and workstation operating systems (OSs) from Apple, Inc.; WINDOWS® server and workstation OSs from the MICROSOFT™ Corporation; UNIX-based OSs, and Linux OSs, such as, but not limited to, Linux from RedHat™ Inc.

[0174] In alternative embodiments, the GUIs of FIGs. 14-18 can be rendered on a display of a mobile computing device such as, but not limited to a personal digital assistant (PDA), an iPhone™, an iPod™ touch, or iPad™ tablet device, a device operating the Android operating system (OS) from Google Inc., a device running a MICROSOFT™ WINDOWS® Mobile or Phone OS, a device running a Symbian OS,

a device running a PALM OS®, a BLACKBERRY® device running a Blackberry OS from Research In Motion ("RIM"), a smart phone, a hand held computer, a netbook computer, a palmtop computer, a laptop computer, an ultra-mobile PC, or another similar type of mobile device capable of processing instructions and receiving and transmitting data to and from users and other computing devices.

[0175] It is to be understood that the console interface and dashboards illustrated in the exemplary embodiments of FIGs. 14-18 can be readily adapted to execute on a display of mobile device platforms and operating systems, a computer terminal, a display of a client device, a display console of a server, a display console of a monitoring device, a display of a target or subject device, or other display of a computing device. Thus, the exemplary GUIs illustrated in FIGs. 14-18 can be rendered on a display of a mobile device using an attestation application, within a web browser session, on a display console of an attestation server, or on a display of a client device running an attestation application.

[0176] Throughout FIGs. 14-18, displays are shown with various icons, folders, panes, command regions, interfaces, windows, tabs, tiles, data entry fields, drop down menus, and buttons that are used to initiate action, invoke routines, monitor and display data related to operational integrity of, monitor resource utilization, or invoke other functionality. The initiated actions include, but are not limited to, viewing events, editing events, inputting calendar preferences, a backward scroll, a forward scroll, and other calendar view navigation inputs and gestures. For brevity, only the differences occurring within the figures, as compared to previous or subsequent ones of the figures, are described below.

[0177] In an embodiment, the display used to display the GUIs and dashboards shown in FIGs. 14-18 may be a computer display 2630 shown in FIG. 26, and the console interface may be display interface 2602. According to embodiments of the present invention, a user can interact with the console interface and dashboards using input devices such as, but not limited to, a touch screen, a pointing device, a stylus, a track ball, a touch pad, a mouse, a keyboard, a keypad, a joy stick, a voice activated control system, or other input devices used to provide interaction between a user and a GUI.

[0178] FIG. 14 depicts an exemplary GUI for a data center administration console 1400 including an operational integrity dashboard 1450.

[0179] Referring to FIG. 14, the exemplary data center administration console 1400 may visually display as a single pane an operational integrity dashboard or display window 1450 to provide a 'global view' of the data center inventory 1401 (i.e., a 'global view dashboard'). The display window 1450 can include information fields including the global view of the data center inventory 1401 in a hierarchical tree view of resources, a component level view of a resource 1402, a resource name 1403, a resource platform type 1404, integrity metrics for a plurality of trust vectors that include at least the system configuration 1405, resource utilization 1406, application integrity 1407, network activity 1408, a remediation action 1409, a remediation control 1410 that may include at least a restore, quarantine and divert users function, an action summary 1413, a details pane 1411, a status pane 1412, and color coded runtime integrity indicators 1440. The console 1400 can also graphically display risk indicators as integrity indicators 1440 and indications of impact analysis based on a confidence level of received integrity metrics for the trust vectors.

[0180] The information fields may be displayed and/or updated in real time or near real time. The color coded runtime integrity indicators 1440 for each displayed trust vector 1405, 1406, 1407 and 1408 may be animated and include audio-visual effects. For example, the integrity indicators 1440 can be animated with location changes, color changes, size changes, cross-fading, blinking, beeping, or vibration (i.e., when displayed on a mobile client device). In embodiments, some or all of the integrity indicators 1440 may be hyperlinked graphics with links to detailed dialog boxes, expanded views, or reports for a drill-down or detailed view of the corresponding trust vector.

[0181] Although the integrity dashboard 1450 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible. For example, additional trust vectors or a custom filter based perspective view may be displayed, or the dashboard may be embedded as a plug-in control and streamlined in a third party management console.

[0182] FIG. 15 depicts an exemplary GUI for a runtime operational integrity monitoring console 1500 including a system configuration dashboard 1550.

[0183] Referring to FIG. 15, the exemplary runtime operational integrity monitoring console 1500 may visually display a system configuration dashboard or display window 1550 in a single pane. The display window 1550 may include information fields including a severity 1501, a warning or observed activity 1502, a timestamp 1503, an evaluation status 1504, a recommended action 1505, advanced details 1506 that may include a timestamp corresponding to the displayed threat details pane 1507, source location, threat identifier and victim identifier, threat details pane 1507, and machine history 1508 that may pertain to infection history.

[0184] The threat details pane 1507 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0185] Although the system configuration dashboard 1550 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[0186] FIG. 16 depicts an exemplary GUI for a runtime operational integrity monitoring console 1600 including a resource utilization dashboard 1650.

[0187] Referring to FIG. 16, the exemplary runtime operational integrity monitoring console 1600 may visually display a resource utilization dashboard or display window 1650. The display window 1650 may include information fields including a severity 1601, a warning or observed activity 1602, a timestamp 1603, an evaluation status 1604, a recommended action 1605, advanced details 1606 that may include a timestamp corresponding to the displayed threat details pane 1607, source location, threat (or malware) identifier and victim identifier, threat details pane 1607, and machine history 1608 that may pertain to infection history.

[0188] The threat details pane 1607 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0189] Although the resource utilization dashboard 1650 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[0190] FIG. 17 depicts an exemplary GUI for a runtime operational integrity monitoring console 1700 including an application integrity dashboard 1750.

[0191] Referring to FIG. 17, the exemplary runtime operational integrity monitoring console 1700 may visually display an application integrity dashboard or display window 1750. The display window 1750 may include information fields including a severity 1701, a warning or observed activity 1702, a timestamp 1703, an evaluation status 1704, a recommended action 1705, advanced details 1706 that may include a timestamp corresponding to the displayed threat details pane 1707, source location, threat (or malware) identifier and victim identifier, threat details pane 1707, and machine history 1708 that may pertain to infection history.

[0192] The threat details pane 1707 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0193] Although the application integrity dashboard 1750 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[0194] FIG. 18 depicts an exemplary GUI for runtime operational integrity monitoring console 1800 including a network activity dashboard 1850.

[0195] As shown in FIG. 18, an exemplary runtime operational integrity-monitoring console 1800 may visually display a network activity dashboard or display window 1850. The display window 1850 may include information fields including a severity 1801, a warning or observed activity 1802, a timestamp 1803, an evaluation status 1804, a recommended action 1805, advanced details 1806 that may include a timestamp corresponding to the displayed threat details pane 1807, source location, threat (or malware) identifier and victim identifier, threat details pane 1807, and machine history 1808 that may pertain to infection history.

[0196] The threat details pane 1807 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0197] Although the network activity dashboard 1850 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

Methods for Threat Identification and Remediation and Subject Reputation

[0198] FIGs. 19-22 are flowcharts illustrating exemplary methods for threat identification and remediation, providing a subject reputation service, and providing network flow level remediation.

[0199] The flowcharts depicted in FIGs. 19-22 are described with reference to the embodiments of FIGs. 1-8 and 11. However, the methods 1900-2200 shown in FIGs. 1900-2200 are not limited to those example embodiments. The steps of the methods 1900-2200 shown in FIGs. 19-22 do not necessarily have to occur in the order described below. According to embodiments, some of the steps of the methods 1900-2200 are optional.

[0200] FIG. 19 is a flowchart illustrating an exemplary method for threat identification and remediation. Referring to FIG. 19, the method 1900 may provide threat identification and remediation for an infected device 560 using a trust orchestrator 430, an endpoint trust agent 510, a network analyzer 830 and an endpoint assessment service 820.

[0201] In step 1901, raw events 611 from the native device and/or platform instrumentation 610 are received. In an embodiment, the endpoint runtime monitor 620 described with reference to FIG. 6 above receives the raw events 611. After the raw events 611 are received, control is passed to step 1902.

[0202] In step 1902, image file and attributes are sent to a trust broker. According to an embodiment, this step is performed by the process monitor 514 described with reference to FIG. 5 above, that is included in the endpoint runtime monitor 620 described with reference to FIG. 6 above. In this embodiment, the process monitor 514 included in the endpoint runtime monitor 620 sends image file and attributes 518 to the trust broker 407 at the trust orchestrator 430 described with reference to FIG.

8 above so that specialized image analysis can be performed. After the image file and attributes 518 are sent, the method 1900 continues with step 1903.

[0203] In step 1903, the trust broker validates the image file based on received image attributes before passing control to step 1904. In accordance with an embodiment, the validation in step 1903 can be performed by the trust broker 407 described with reference to FIG. 5 above.

[0204] In step 1904, the trust broker (i.e., trust broker 407) sends the received image file to a malware analyzer. In one embodiment, the malware analyzer is malware analyzer 540 described with reference to FIG. 5 above and the malware analyzer is configured to perform specialized static and dynamic image introspection of the received image file.

[0205] In step 1905, a trust broker, such as, but not limited to, the trust broker 407, generates and sends, based on a received diagnosis, an image profile to an endpoint process monitor. In an embodiment, this step comprises sending an image profile 519 to the endpoint process monitor 514 described above with reference to FIG. 5. After the image profile is sent, control is passed to step 1906.

[0206] In step 1906, the endpoint runtime monitor 620 generates and sends integrity events, such as, but not limited to, integrity events 621, to an integrity processor, such as, but not limited to, the integrity processor 630 described above with reference to FIG. 6.

[0207] In step 1907, the endpoint integrity processor 630 may process and map received events to alerts using rulesets 631. In step 1908, the endpoint integrity processor 630 may generate and send warnings 634 using an event correlation matrix 633 to the trust orchestrator 430 as endpoint events 520.

[0208] In step 1909, a system event correlator, such as, but not limited to, the system event correlator 410, receives endpoint events 520 from the endpoint integrity processor 630.

[0209] In step 1910, the trust broker 407 receives network endpoint integrity measurement and verification reports 821 from an endpoint assessment service 820.

[0210] In step 1911, the system event correlator 410 receives temporal events 409 from the trust broker 407.

[0211] In step 1912, a system event correlator 410 may correlate the received endpoint and temporal events and generate an integrity profile 420 for the device 560 before passing control to step 1913.

[0212] In step 1913, the system event correlator 410 sends an integrity profile 420 of the device 560 to the trust supervisor 846.

[0213] In step 1914, the network activity correlator 831 sends infection profiles 831 to a trust supervisor, the trust supervisor 846.

[0214] In step 1915, the trust supervisor 846 may process the received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification on the device 560.

[0215] In step 1916, the trust supervisor 846 sends to the remediation controller 848 actions 847 to perform on the infected device 560. In step 1917, the remediation controller 848 may process the received action request on the infected device 560 and send directives 849 based on configured thresholds and triggers to system orchestration and policy enforcement point (or network security) services 860.

[0216] FIG. 20 is a flowchart illustrating an exemplary method for providing a subject reputation service to a service provider. In the example embodiment of FIG. 20, the subject is a user and the method 2000 provides a user reputation service. However, as discussed above with reference to FIGs. 9 and 11, in alternative embodiments, the subject can also be a device, transaction, service, or an organization, such as a company.

[0217] In particular, FIG. 20 illustrates the steps by which a method 2000 provides a user reputation service for a service provider. In one embodiment, the service provider is the service provider 1104 described above with reference to FIG. 11 and the method 2000 can use a trust orchestrator, such as, but not limited to, the trust orchestrator 430 described above with reference to FIG. 8.

[0218] According to embodiments, steps of the method 2000 can also be performed using an endpoint trust agent, a network analyzer , and a network analyzer, such as, but not limited to, the endpoint trust agent 510, network analyzer

830, and the endpoint assessment service 820 described above with reference to FIG. 8.

[0219] In step 2001, an endpoint runtime monitor, such as, but not limited to, the endpoint runtime monitor 620 described above with reference to FIG. 6, receives raw events 611 from the native device and/or platform instrumentation 610, detect and identify the user 1014 authenticated by the authentication service 1103 at the device 560.

[0220] In step 2002, the endpoint runtime monitor 620 receives user activity events from the native device and/or platform instrumentation 610. After the user activity events have been received, control is passed to step 2003.

[0221] In step 2003, the endpoint runtime monitor 620 may generate and send integrity events 621 to the endpoint integrity processor 630.

[0222] In step 2004, the endpoint integrity processor 630 may process and map received events to alerts using rulesets 631.

[0223] In step 2005, the endpoint integrity processor 630 may generate and send warnings 634 using an event correlation matrix 633 to the trust orchestrator 430 as endpoint events 520. After the warnings and event correlation matrix have been generated and sent, the method 2000 continues with step 2006.

[0224] In step 2006, the trust broker 407 may query and receive user and resource attributes 1121, 1130, 1122, and 1128 from a plurality of collaboration services 904, 903, 902, 901 and generate subject events 1123. In step 2007, the reputation processor 1110 may analyze received subject events 1123 and generate subject alerts 1124 (i.e., user alerts or integrity profiles).

[0225] In step 2008, the risk correlator 1111 may correlate received subject alerts 1124, such as user 1014 alerts, to generate user warnings 1126 using the risk correlation matrix 721, and user reputation score 1125 using the reputation score generator 1112.

[0226] In step 2009, the trust supervisor 846 may process the received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification of a user 1014 of the device 560. The user 1014 may be associated with the device due to currently being logged into the device 560, running

an application on the device 560, or by virtue of having account/user ID privileges to access resources such as files, data, applications, or web pages on the device 560.

[0227] In step 2010, the reputation broker 1106 receives a reputation query 1117 for the user 1014 of the device 560 from a service provider 1104.

[0228] In step 2011, the reputation broker 1106 sends a reputation token 1118 for the user 1014 of the device 560. In an embodiment, the reputation token 1118 sent in this step includes at least a user reputation score 1125. After the reputation token 1118 is sent, control is passed to step 2012.

[0229] In step 2012, the service provider 1104 applies a reputation-based access control 1119 in processing a service request 1116 received from the device 560 for the user 1014 to access a managed application 1105. After the reputation-based access control has been applied, control is passed to step 2013.

[0230] In step 2013, the trust supervisor 846 sends to the remediation controller 848 actions 847 to perform on the network fabric for sessions of the user 1014 of the device 560.

[0231] In step 2014, the remediation controller 848 may process received action request for sessions of the user 1014 of the device 560 and send directives 849 based on configured thresholds and triggers to system orchestration and policy enforcement point (network security) services 860.

[0232] FIG. 21 is a flowchart illustrating steps by which an attestation service for runtime operational integrity of systems executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server can be provided. The steps of the method 2100 shown in FIG. 21 do not necessarily have to occur in the order described.

[0233] Referring to FIG. 21, the method 2100 can provide network flow level remediation for an infected device 560 at a network element 1216 using a trust orchestrator 1205, an endpoint trust agent 1201, a network trust agent 1209 and collaboration services 1207.

[0234] In step 2101, the endpoint runtime monitor 620 at the endpoint trust agent 1201 on the device 560 sends a dynamic context 1204 that may include endpoint events 520 to the trust orchestrator 1205.

[0235] In step 2102, the trust orchestrator 430 may analyze received endpoint events 520 from the endpoint trust agent 1201 on the device 560 before passing control to step 2103.

[0236] In step 2103, the trust broker 407 receives and analyzes network endpoint assessments (or integrity measurement and verification reports) 821 from an endpoint assessment service (or collaboration services) 820 and generate temporal events 409.

[0237] In step 2104, the system event correlator 410 may correlate endpoint 520 and temporal 409 events and generate an integrity profile 420 for the device 560.

[0238] In step 2105, the trust supervisor 846 may generate and send to the remediation controller 848 flow remediation actions 847 to perform on the network fabric.

[0239] In step 2106, the remediation controller 848 at the trust orchestrator 1205 sends to the network trust agent 1209 a system warning 1208 for the network device 560. In step 2107, the network trust agent 1209 may generate and send to the OpenFlow security framework 1211 directives 1210 to formulate commands 1213 for the OpenFlow controller 1214.

[0240] In step 2108, the OpenFlow controller 1214 sends rules 1215 to the OpenFlow enabled network element (switch) 1216 to divert or block traffic flows to/from the forewarned network device 560.

[0241] In step 2109, the OpenFlow enabled network element (switch) 1216 may enforce received access restrictions (controls) 1217 for the forewarned network device 560 before control is passed to step 2110.

[0242] In step 2110, the trust supervisor 846 may monitor and send reputation score updates 847 for the forewarned network device 560 to the remediation controller 848. In step 2111, the remediation controller 848 at the trust orchestrator 1205 sends system security posture status updates 1208 for the forewarned network device 560 to the network trust agent 1209. After the reputation score updates are monitored and sent, the method 2100 proceeds to step 2112.

[0243] In step 2112, the network trust agent 1209 may generate and send to the OpenFlow security framework 1211 directives 1210 to formulate commands 1213 for

the OpenFlow controller 1214 to restore normal flows to/from the forewarned network device 560.

[0244] FIG. 22 is a flowchart illustrating a method in accordance with various exemplary embodiments.

[0245] Referring to FIG. 22, the method 2200 can provide network flow level remediation for an infected mobile device 560 at a wireless access point 1320 using a trust orchestrator 1310, an endpoint trust agent 1301, a network trust agent 1315 and an endpoint assessment service 1312.

[0246] In step 2201, the endpoint runtime monitor 620 at the endpoint trust agent 1301 on the mobile device 560 sends a dynamic context 1304 that may include endpoint events 520 to the trust orchestrator 1310 before passing control to step 2202.

[0247] In step 2202, the trust orchestrator 430 may analyze received endpoint events 520 from the endpoint trust agent 1301 on the mobile device 560.

[0248] In step 2203, the trust broker 407 receives and analyzes network endpoint assessments (or integrity measurement and verification reports) 821 from an endpoint assessment service (or collaboration services) 820 and generate temporal events 409. After the network endpoint assessments are analyzed and the temporal events are generated, the method 2200 proceeds to step 2204.

[0249] In step 2204, the system event correlator 410 may correlate endpoint 520 and temporal 409 events and generate an integrity profile 420 for the mobile device 560.

[0250] In step 2205, the trust supervisor 846 may generate and send to the remediation controller 848 flow remediation actions 847 to perform on the network fabric.

[0251] In step 2206, the remediation controller 848 at the trust orchestrator 1310 sends to the network trust agent 1209 a system warning 1208 for the mobile device 560 before control is passed to step 2207.

[0252] In step 2207, the network trust agent 1209 generates and sends to the wireless access point 1320 policies 1317 to apply access controls 1321 for the mobile device 560, at which point control is passed to step 2208.

[0253] In step 2208, the remediation controller 848 at the trust orchestrator 1310 sends to the mobile policy manager 1313 a system warning 1307 for the mobile device 560 or to the mobile device manager 1324 directives 1309 to set feature controls on the mobile device 560.

[0254] In step 2209, the mobile policy manager 1313 generate and send to the mobile device manager 1324 directives 1309 to formulate advisories and security settings for the registered user (service subscriber) and the mobile device 560 or set feature controls on the mobile device 560.

[0255] In step 2210, the reputation broker 1106 receives a reputation query 1117 for a mobile device 560 from a service provider 1104.

[0256] In step 2211, the reputation broker 1106 sends a reputation token 1118 for the device 560 that may include at least a security posture established by the trust supervisor 846 based on the received infection 832 and integrity 420 profiles for the device 560.

[0257] In step 2212, the service provider 1104 may apply a reputation-based access control 1119 in processing a service request 1116 received from the device 560 to access a managed application 1105.

Entity Relationship Model and Hierarchical Subject Reputation

[0258] FIG. 23 is an entity relationship diagram illustrating exemplary relationships between entities and components used in a system for the calculus of a subject reputation score. For example, the entities and components depicted in the entity model 2300 can be used to generate reputation scores by the system 1100 described above with reference to FIG. 11.

[0259] Referring to FIG. 23, the exemplary reputation scoring system 2300 computes a reputation score for a user 1014 that is employed by, a member of, or otherwise associated with an organization 2303. The user 1014 can be associated with the organization temporarily (i.e., as a contractor). The user 1014 uses one or more endpoint devices 560 to perform an online transaction 2304 with a service 2305 that is rendered by an application 2306 and managed by the organization 2303, to participate in an activity 2307. In embodiments, the activity 2307 is categorized as either social 2308 or professional 1409.

[0260] According to embodiments, the organization 2303 can be, but is not limited to, a company, a government agency/division, a university or school, a hospital, a non-profit firm, or any other group that needs to secure systems, platforms, mobile computing devices, or other IT assets on behalf of its employees/members (i.e., users 1014 of devices 560). The organization's 2303 IT assets can include, but are not limited to, servers, desktop computers, laptops, tablet computers, multi-function printers/scanners/fax machines, and network devices. The IT assets can be devices 560 owned or leased by the organization and directly controlled by the organization 2303.

[0261] The IT assets can include devices 560 owned and managed by users 1014 (i.e., a user-owned mobile computing device in a BYOD environment) or the organization 2303 (i.e., a 'corporate' IT asset owned or leased by the organization 2303). In an embodiment, the reputation scoring system 2300 can operate in a mixed environment of IT assets wherein the organization 2303 owns some devices 560, leases some devices 560, and users 1014 own other devices 560. For example the organization 2303 may own enterprise servers and network devices (not shown), lease laptops, desktop computers/personal computers (PCs), and other endpoint devices 560 for users 1014 and simultaneously allow user 1014-owned mobile computing devices 560 (i.e., smart phones, laptops, and tablets in a BYOD environment) to access the organization's 2303 domain via internal or external networks. The internal networks can be, but are not limited to, an intranet, a LAN, or a WAN. The external networks can be, but are not limited to, an extranet, a wireless data networks such as Wi-Fi, and the Internet.

[0262] The servers (not shown) in the reputation scoring system 2300 may be part of a server farm and can be, but are not limited to, application servers hosting applications 2306, file servers, mail servers, database servers, proxy servers, and web servers. These servers can be enterprise servers owned by the organization 2303 or servers under a corporate lease. Alternatively, the servers can also be part of a remote, service-provider managed outsourced virtual data center (i.e., a cloud computing environment). The network devices can be networked storage devices,

routers, switches, hubs, and firewalls. These network devices can be part of the organization's 2303 local area network (LAN) or wide area network (WAN).

[0263] FIG. 24 is a block diagram illustrating an exemplary hierarchical representation of a subject reputation score. The hierarchical representation 2400 can be used to report reputation scores generated by system 1100 described above with reference to FIG. 11.

[0264] Referring to FIG. 24, the exemplary hierarchical representation of a subject reputation score 2400 includes a reputation score 2401, a transaction score 2409, a user score 2407, a service score 2408, a social score 2402, a professional score 2403, a device score 2404, an organization score 2405, and an application score 2406. In the exemplary embodiment of FIG. 24, the organization score 2405 can be, for example a company score 2405.

[0265] A reputation score may comprise one or more component scores (as an aggregation), where a component score is illustrated in FIG. 24 below an aggregate score (for example, a service score may be a component score of a transaction score). An aggregate reputation score may provide an enumerated list to annotate component scores included.

Application Event Monitoring Architecture

[0266] FIG. 25 is a block diagram illustrating an exemplary computing system architecture 2500 for monitoring application events for trusted execution with layered extensions to native machine instrumentation mechanisms. FIG. 25 is described with continued reference to the embodiments illustrated in FIGs. 4-6. However, FIG. 25 is not limited to those embodiments.

[0267] Referring to FIG. 25, the exemplary representation of the architecture 2500 instrumented for trust includes a device 560, an endpoint trust agent 510, native machine instrumentation 610, extended trust instrumentation 2501, a runtime monitor 620, a system event correlator 410, and a trust orchestrator 430.

[0268] The runtime monitor 620 subscribes for, and receives, near real time asynchronous notifications of application events 2502 from the extended trust instrumentation 2501. The application events 2502 may include registry, file system, network, storage, input (for example, keyboard), output (for example, screen

display), memory (for example, peek or poke) and process operations (for example, thread creation), and usage of any system resource (for example, microphone or camera) by running applications on the target instrumented device 560.

[0269] The extended trust instrumentation 2501 may be layered extensions to native machine instrumentation 610, such as, for example, the WINDOWS® Management Instrumentation (WMI) on MICROSOFT™ WINDOWS® platforms.

[0270] As will be appreciated by persons skilled in the relevant art, WMI is a set of extensions to the MICROSOFT™ WINDOWS® Driver Model (WDM), which is a framework for device drivers that provides an operating system interface through which instrumented components (i.e., components of an instrumented platform) provide information and notification. WMI is a MICROSOFT™ implementation of the Distributed Management Task Force (DMTF) Web-Based Enterprise Management (WBEM) and the DMTF Common Information Model (CIM) standards. WMI is preinstalled on some MICROSOFT™ WINDOWS® Operating Systems (OSs) and allows scripting languages like Visual Basic Scripting Edition (VBScript) or Windows PowerShell to manage computing devices and platforms running a MICROSOFT™ WINDOWS® OS. Such management can be performed locally (i.e., on the server or platform being managed) or remotely from a computing device external to the managed platform/device.

[0271] In certain exemplary embodiments, the runtime monitor 620 may generate and send dynamic expressions or rules as application filters 2503 linked to one or more running instances of applications on the target instrumented device 560.

[0272] The application events 2502 and application filters 2503 may be expressed using standards based schema definitions, such as for example the DMTF CIM specification. In a non-limiting embodiment, the CIM schema can be used to provide Trust-as-a-Service (TaaS).

[0273] In embodiments, the architecture 2500 can be used with APIs to subscribe for asynchronous application events such as, but not limited to, registry, file system, network, and process operations (e.g., Load Library, Remote Thread Attach, Peek/Poke Memory operations).

[0274] Embodiments of the architecture 2500 can include packaging of a TaaS endpoint comprising an endpoint trust sensor with OS updates, such as, but not limited to, MICROSOFT™ WINDOWS®, UNIX, Linux, and Apple OSX updates (i.e., OS and application upgrades and security patches for browsers, business productivity suites, device drivers, and other platform components). By using the architecture 2500, an endpoint trust sensor can measure runtime operational integrity by evaluating risk based on 'actions' and leveraging the native machine instrumentation 610.

[0275] In embodiments, the architecture 2500 also enables a network trust sensor to perform signature-less network activity correlation using a threat 'life cycle model' for clustering and classification of malware.

[0276] According to embodiments, the architecture 2500 enables trust orchestration for actionable intelligence based on real-time event correlation (i.e., a calculus of risk) by using an API collaboration bus for integration of security intelligence.

Example Computer System Implementation

[0277] Although exemplary embodiments have been described in terms of a computing device or instrumented platform, it is contemplated that it may be implemented in software on microprocessors/general purpose computers such as the computer system 2600 illustrated in FIG. 26. In various embodiments, one or more of the functions of the various components may be implemented in software that controls a computing device, such as computer system 2600, which is described below with reference to FIG. 26.

[0278] Aspects of the present invention shown in FIGS. 1-25, or any part(s) or function(s) thereof, may be implemented using hardware, software modules, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems.

[0279] FIG. 26 illustrates an example computer system 2600 in which embodiments of the present invention, or portions thereof, may be implemented as computer-readable code. For example, the network systems and architectures of FIGS. 1, 4-6,

8-13 and 25 can be implemented in computer system 2600 using hardware, software, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Hardware, software, or any combination of such may embody any of the modules and components used to implement the architectures and systems 100, 400, 500, 600, 800, 900, 1000, 1100, 1200, 1300 and 2500 of FIGS. 1, 4-6, 8-13 and 25.

[0280] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. One of ordinary skill in the art may appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device.

[0281] For instance, at least one processor device and a memory may be used to implement the above-described embodiments. A processor device may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor "cores."

[0282] Various embodiments of the invention are described in terms of this example computer system 2600. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0283] Processor device 2604 may be a special purpose or a general-purpose processor device. As will be appreciated by persons skilled in the relevant art, processor device 2604 may also be a single processor in a multi-core/multiprocessor system, such system operating alone, or in a cluster of computing devices operating

in a cluster or server farm. Processor device 2604 is connected to a communication infrastructure 2606, for example, a bus, message queue, network, or multi-core message-passing scheme.

[0284] The computer system 2600 also includes a main memory 2608, for example, random access memory (RAM), and may also include a secondary memory 2610. Secondary memory 2610 may include, for example, a hard disk drive 2612, removable storage drive 2614. Removable storage drive 2614 may comprise a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, or the like.

[0285] The removable storage drive 2614 reads from and/or writes to a removable storage unit 2618 in a well-known manner. Removable storage unit 2618 may comprise a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 2614. As will be appreciated by persons skilled in the relevant art, removable storage unit 2618 includes a non-transitory computer usable storage medium having stored therein computer software and/or data.

[0286] In alternative implementations, secondary memory 2610 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 2600. Such means may include, for example, a removable storage unit 2622 and an interface 2620. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 2622 and interfaces 2620 which allow software and data to be transferred from the removable storage unit 2622 to computer system 2300.

[0287] The computer system 2600 may also include a communications interface 2624. Communications interface 2624 allows software and data to be transferred between computer system 2600 and external devices. Communications interface 2624 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, or the like. Software and data transferred via communications interface 2624 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals capable of being

received by communications interface 2624. These signals may be provided to communications interface 2324 via a communications path 2626. Communications path 2626 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link or other communications channels.

[0288] The computer system 2600 may also include a computer display 2630 and a display interface 2602. According to embodiments, the display used to display the GUIs and dashboards shown in FIGs. 14-18 and described above may be the computer display 2630, and the console interface may be display interface 2602.

[0289] In this document, the terms "computer program medium," "non-transitory computer readable medium," and "computer usable medium" are used to generally refer to media such as removable storage unit 2618, removable storage unit 2622, and a hard disk installed in hard disk drive 2612. Signals carried over communications path 2626 can also embody the logic described herein. Computer program medium and computer usable medium can also refer to memories, such as main memory 2608 and secondary memory 2610, which can be memory semiconductors (e.g., DRAMs, etc.). These computer program products are means for providing software to computer system 2600.

[0290] Computer programs (also called computer control logic) are stored in main memory 2608 and/or secondary memory 2610. Computer programs may also be received via communications interface 2624. Such computer programs, when executed, enable computer system 2600 to implement the present invention as discussed herein. In particular, the computer programs, when executed, enable processor device 2604 to implement the processes of the present invention, such as the stages in the methods illustrated by the flowcharts 1900, 2000, 2100 and 2200 of FIGS. 19-22, discussed above. Accordingly, such computer programs represent controllers of the computer system 2600. Where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 2600 using removable storage drive 2614, interface 2620, and hard disk drive 2612, or communications interface 2624.

[0291] Embodiments of the invention also may be directed to computer program products comprising software stored on any computer useable medium. Such

software, when executed in one or more data processing device, causes a data processing device(s) to operate as described herein. Embodiments of the invention employ any computer useable or readable medium. Examples of computer useable mediums include, but are not limited to, primary storage devices (e.g., any type of random access memory), secondary storage devices (e.g., hard drives, floppy disks, CD ROMS, ZIP disks, tapes, magnetic storage devices, and optical storage devices, MEMS, nanotechnological storage device, etc.), and communication mediums (e.g., wired and wireless communications networks, local area networks, wide area networks, intranets, etc.).

Conclusion

[0292] It is to be appreciated that the Detailed Description section, and not the Summary and Abstract sections, is intended to be used to interpret the claims. The Summary and Abstract sections may set forth one or more but not all exemplary embodiments of the present invention as contemplated by the inventor(s), and thus, are not intended to limit the present invention and the appended claims in any way.

[0293] Embodiments of the present invention have been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

[0294] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the

present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

[0295] Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range equivalents of the claims and without departing from the invention.

What is claimed is:

1. A method for presenting a data center level runtime operational integrity dashboard and remediation controls for infected systems in a display of a computing platform having a network trust agent, an endpoint trust agent, and a trust orchestrator, the method comprising:

receiving, from a plurality of endpoint assessment services, runtime integrity metrics for a plurality of trust vectors;

displaying, in a graphical user interface (GUI) on the display, risk indicators and impact analysis based on the confidence level of received integrity metrics;

providing, manual or automated remediation controls for threat containment and risk mitigation by performing one or more of:

taking a snapshot of the infected system,

restoring or reimaging the infected system from a trusted baseline configuration,

quarantining the infected system from a network fabric,

diverting users from the infected system,

diverting transactions from the infected system, and

diverting traffic from the infected system;

displaying, in the GUI, a status and progress of initiated remediation actions; and

displaying, in the GUI, details of malware analytics comprising one or more of:

infection summaries,

infection diagnosis,

threat categorization and identification based on a signature-less infection life-cycle model,

an address and geo-location for a source or attacker,

an identification of one or more infected victims,

forensic evidence chain of detected malicious activities and intent, and

compute, memory, storage and network level anomalies detected on the victim machine or infected system.

2. The method of claim 1, wherein the risk indicators are color-coded.

3. The method of claim 1, wherein the runtime operational integrity comprises execution anomalies and a threat posture.

4. A method of orchestrating runtime operational integrity of a system executing on a computing platform using a network analyzer, an endpoint trust agent, a trust broker, a trust orchestrator and a plurality of network endpoint assessments, the method comprising:

determining, by the network analyzer, anomalies based on network activity correlation and network malware detection;

determining, by the trust broker, system configuration anomalies based on system level normalization and collation of assessments;

determining, by the endpoint trust agent, resource utilization anomalies based on rulesets or alert expressions associated with processor, memory, and network resource usage;

determining, by the endpoint trust agent, at least one application integrity anomaly based on rulesets or alert expressions associated with static and dynamic image analysis;

correlating, by the trust orchestrator, network activity and endpoint events and behaviors characterized through continuous local and remote monitoring of network endpoints for risk analysis and detection of infected systems; and

mitigating, by the trust orchestrator, an infected system using inputs received from a real time threat visualization dashboard to implement flow level or transaction level remediation controls.

5. A method of providing runtime operational integrity of an application and a system using a computing platform comprising a network trust agent, an endpoint trust agent, an event and behavior correlation engine, and a trust orchestration server, the method comprising:

monitoring, by a plurality of sensory inputs, one or more of network activity, system configuration for a system the application is executing on, resource utilization by the application, and integrity of the application;

correlating, by the event and behavior correlation engine, risk based on the monitoring; and

displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and application.

6. The method of claim 5, wherein the monitoring is performed continuously.

7. The method of claim 5, wherein the event and behavior correlation engine receives one or more of:

system events and infection profiles from the network activity sensor;

integrity measurement and verification reports of scans from the system configuration sensor;

system events pertaining to processor, network, memory, and storage resource consumption from the resource utilization sensor; and

system events pertaining to image profiles and local execution context from the application integrity sensor.

8. The method of claim 7, wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly.

9. The method of claim 5, wherein the plurality of runtime dashboards comprise one or more of:

a global view dashboard;

a system configuration dashboard;

a resource utilization dashboard;

an application integrity dashboard; and

a network activity dashboard.

10. A system for orchestrating and displaying reputation scoring of a subject, the system comprising:

a display;

a reputation broker configured to:

process a query from a service provider for a reputation score of the subject, and

dispatch a request to generate a hierarchical reputation score for the subject;

a display module configured to render a graphical user interface (GUI) for an administration console comprising a plurality of dashboards in the display;

a trust orchestrator configured to:

process a received request from the reputation broker for a hierarchical reputation score by:

initiating a plurality of directed queries to information management systems external to an organization to interrogate attributes associated with the subject,

analyzing received query responses,

receiving a generated hierarchical reputation score for the subject based on a calculus of risk; and

sending the received hierarchical reputation score for the subject to the reputation broker;

receive a reputation token from the reputation broker for the subject in response to the dispatched request; and

send the reputation token to the service provider as a response to the query.

11. The system of claim 10, wherein the wherein the query is received at a reputation broker configured to forward the query to the trust broker, and wherein the query can be created, displayed, edited, and submitted using a dashboard of the administration console.

12. The system of claim 10, wherein the wherein the response is displayed in a dashboard of the administration console.

13. The system of claim 10, wherein the hierarchical reputation is graphically depicted in a dashboard of the administration console.

14. The system of claim 10, wherein plurality of dashboards comprise one or more of:

a global view dashboard;

a system configuration dashboard;

a resource utilization dashboard;

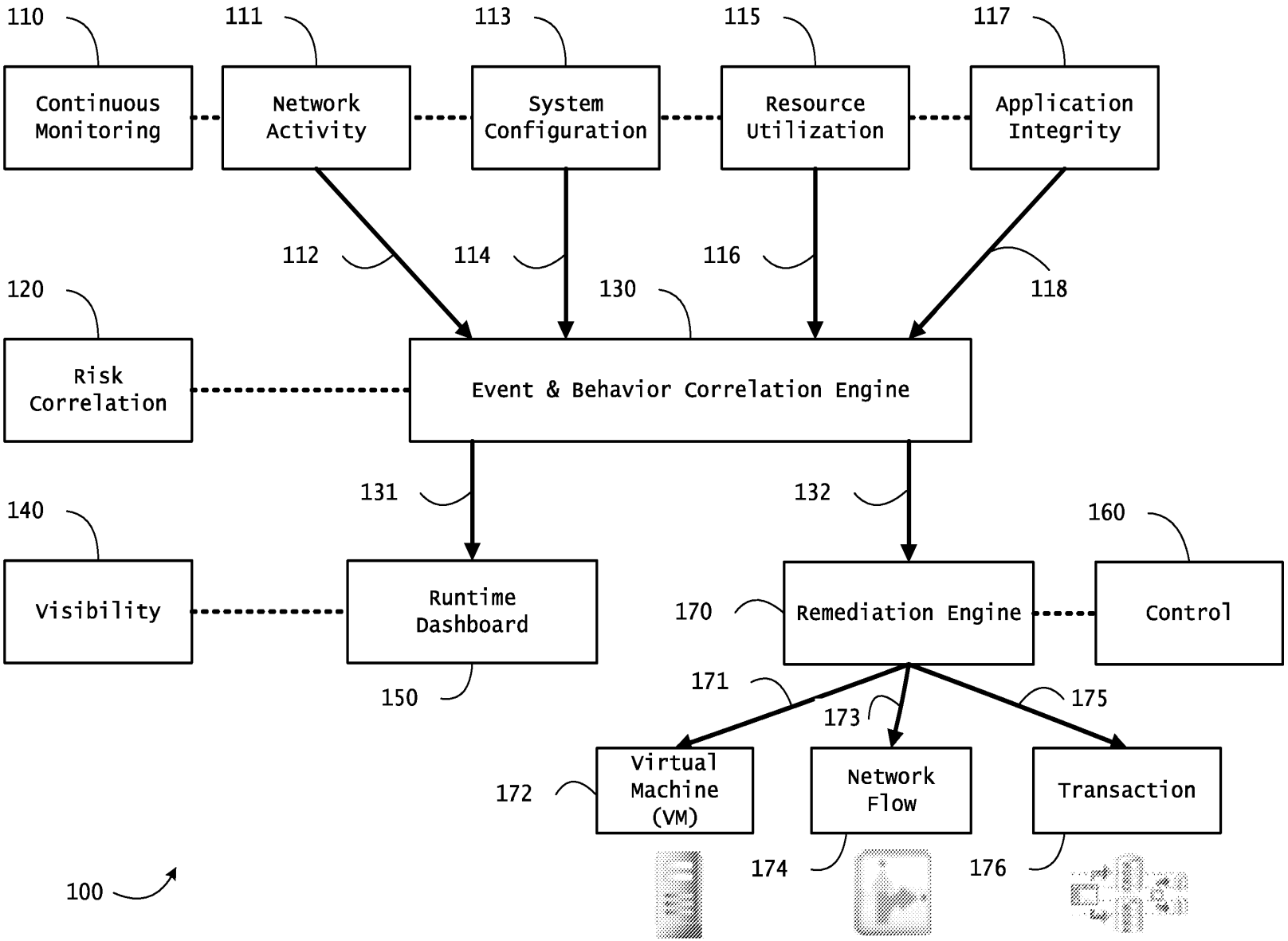
an application integrity dashboard; and

a network activity dashboard.

ABSTRACT OF THE DISCLOSURE

Instrumented networks and platforms having target subjects (devices, transactions, services, users, organizations) are disclosed. A security orchestration service generates runtime operational integrity profiles representing and identifying a level of threat or contextual trustworthiness, at near real time, of subjects and applications on the instrumented target platform. Systems and methods use a graphical user interface (GUI) console to orchestrate operational integrity of a platform. In an embodiment, a method presents a data center-level runtime operational integrity dashboard and remediation controls for infected systems in a display of a platform having a network trust agent, an endpoint trust agent, and a trust orchestrator. The method receives runtime integrity metrics for trust vectors and displays risk indicators based on the confidence level of received integrity metrics in the GUI. The method provides remediation controls for threat containment and risk mitigation and displays remediation status and progress results and malware analytics in the GUI.

FIG. 1

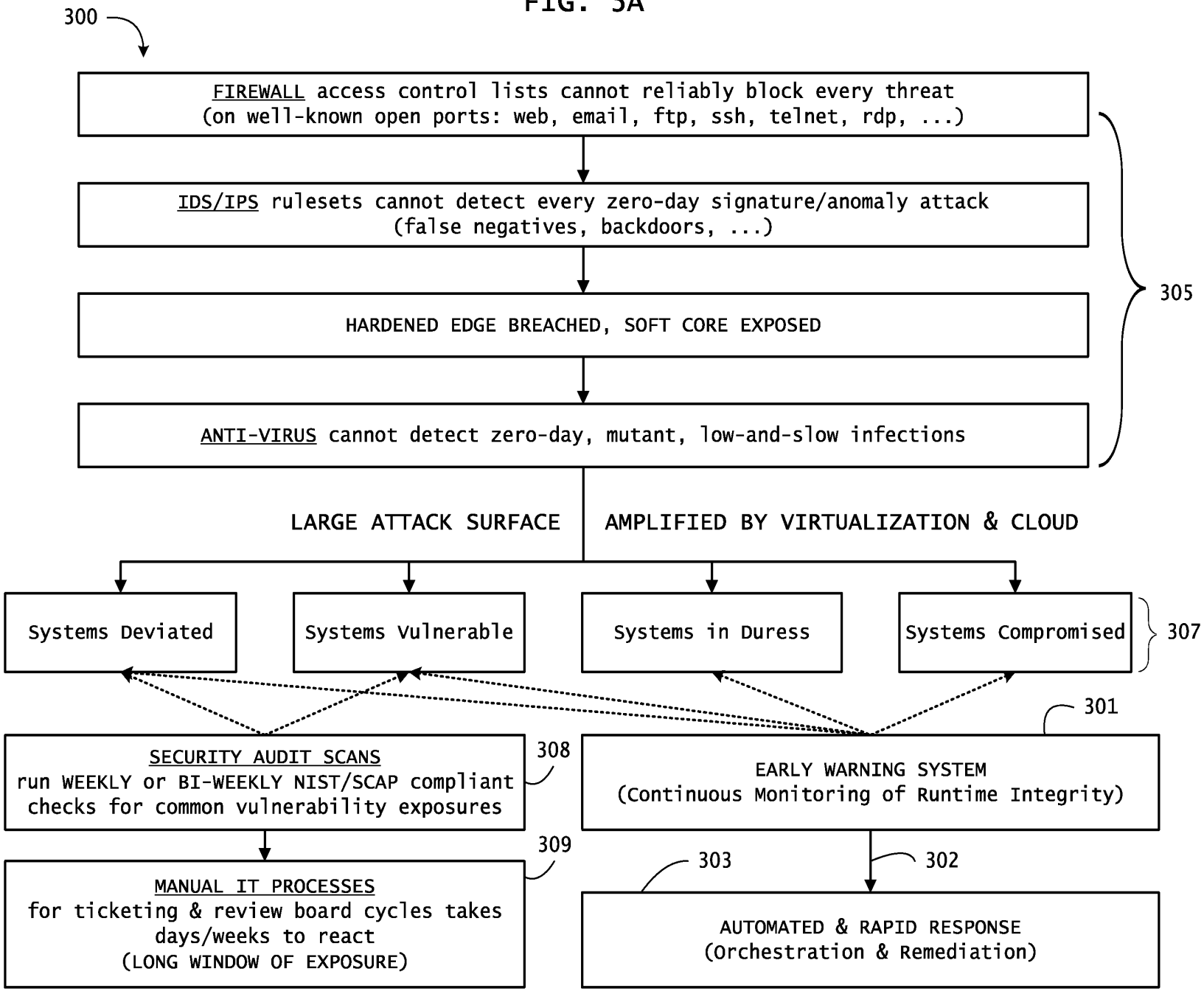


Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 281 of 318

FIG. 2

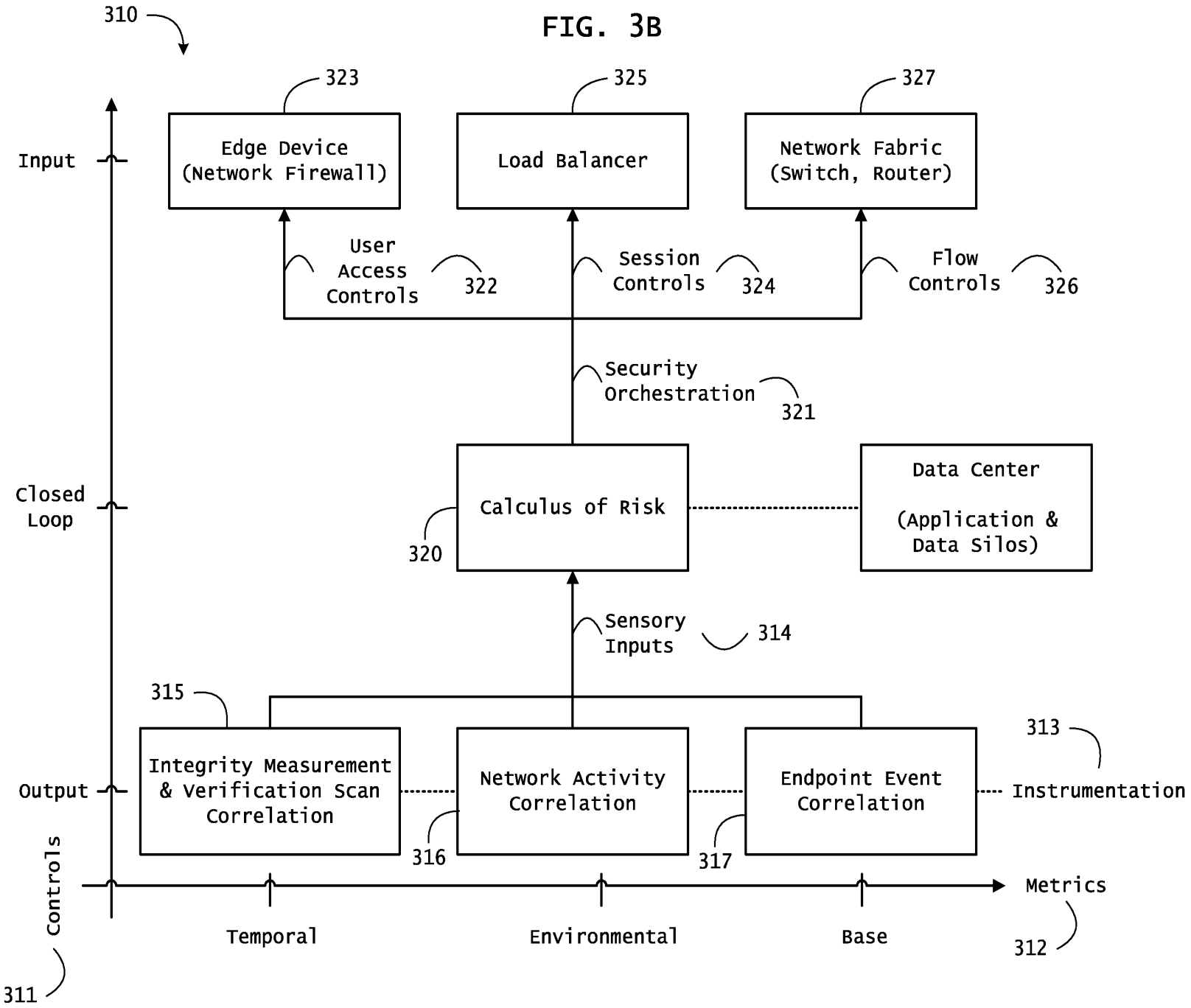
290
Orchestrator
(Manual or Automated)
WARNINGS
280
270
260
Network
Activity
Correlation
250
240
Endpoint Event
Correlation
Endpoint Event
Correlation
ALERTS
230
210
VM #1
Application
Integrity
Resource
Utilization
System
Configuration
Network
Activity
Network
Activity
VM #N
Application
Integrity
Resource
Utilization
System
Configuration
Sensor
211
212
213
220
200

FIG. 3A



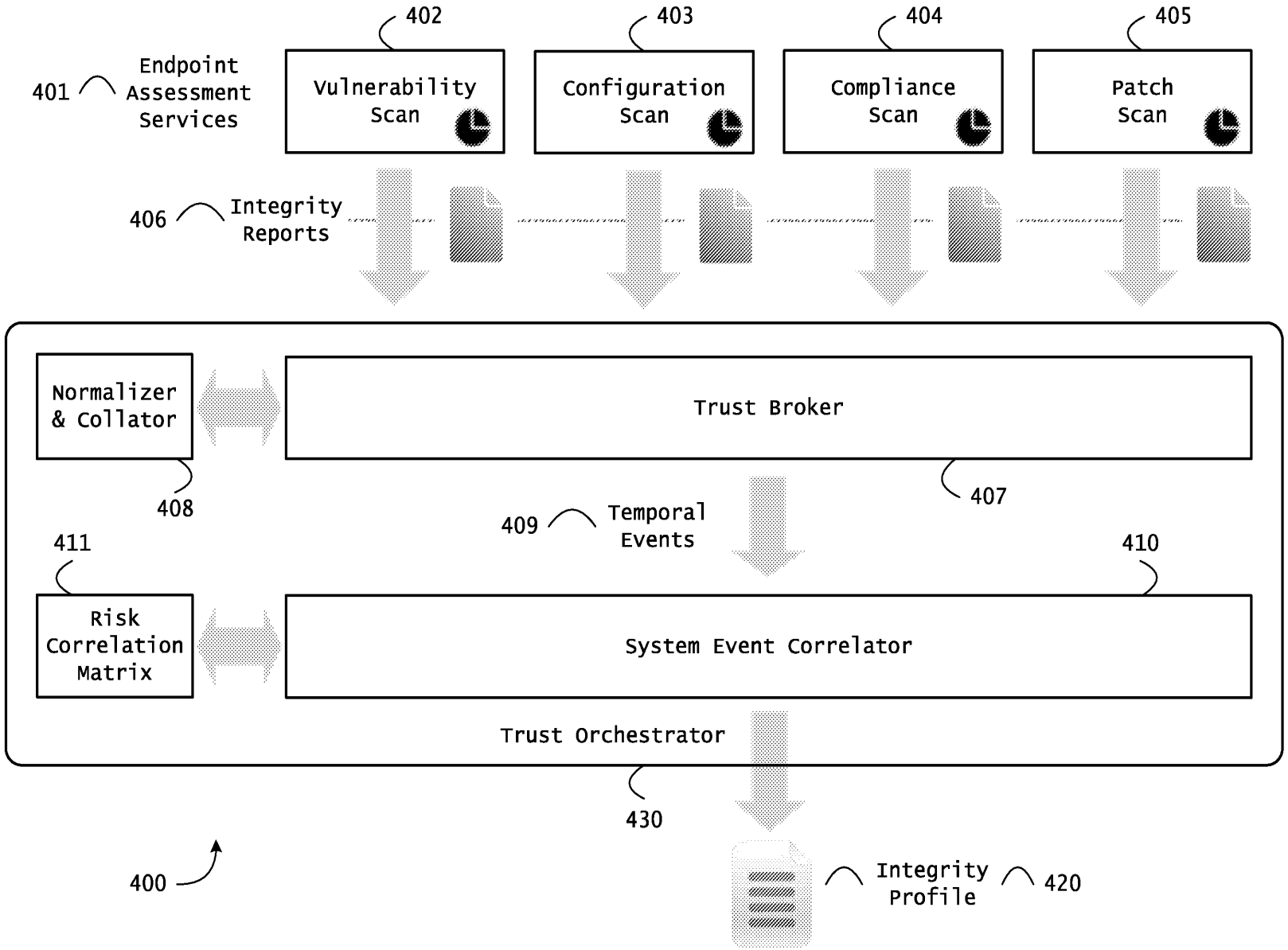
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 283 of 318

FIG. 3B



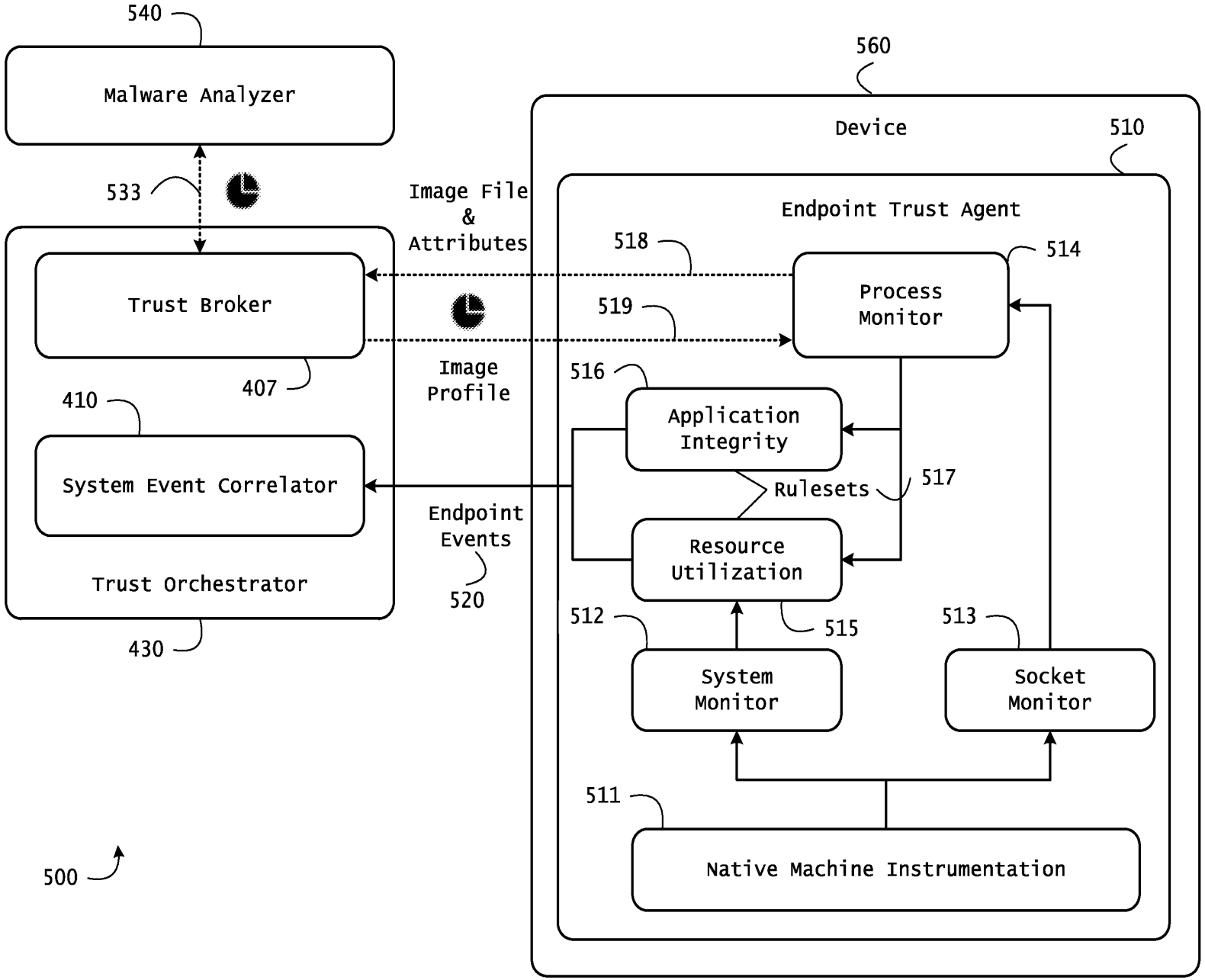
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 284 of 318

FIG. 4



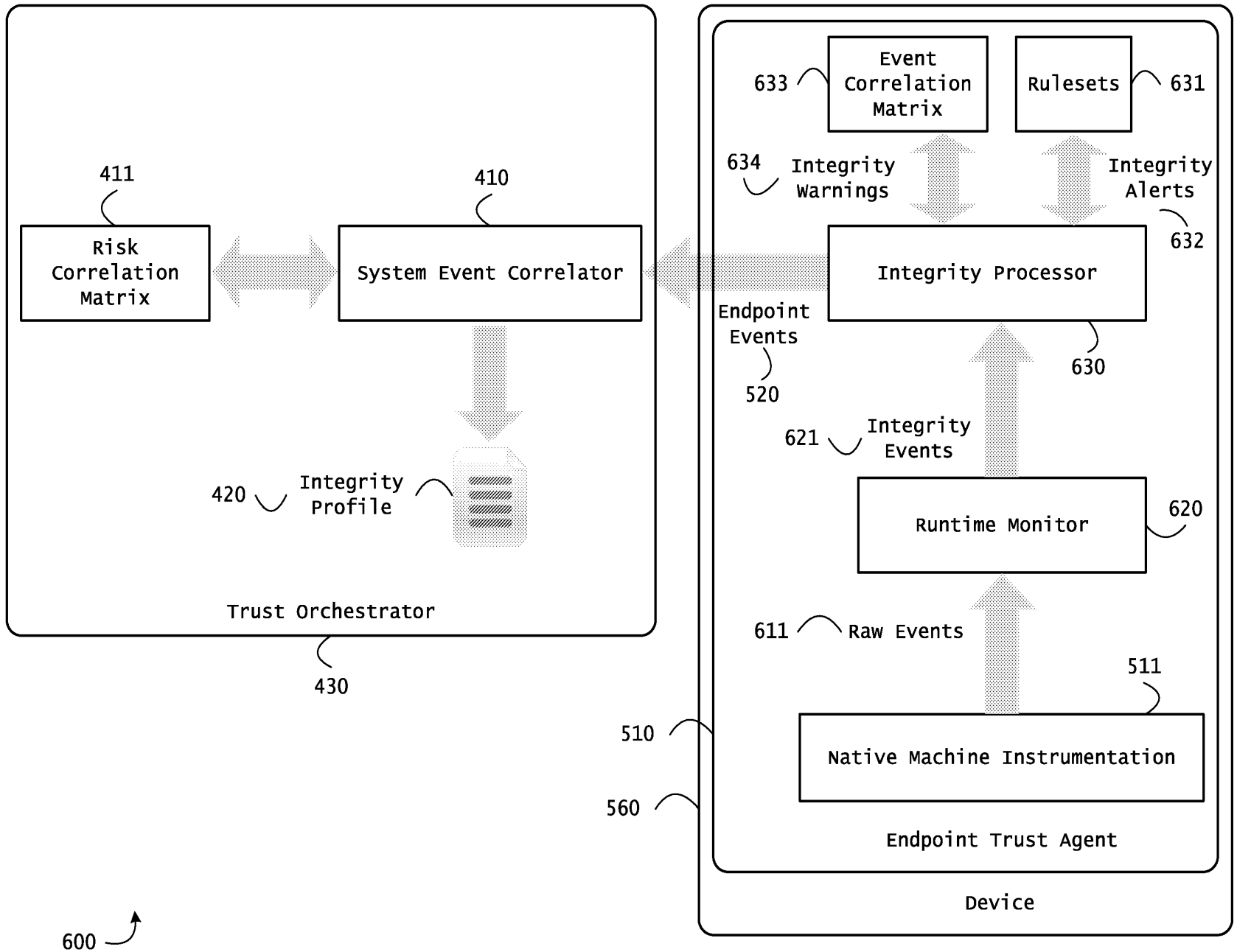
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 285 of 318

FIG. 5



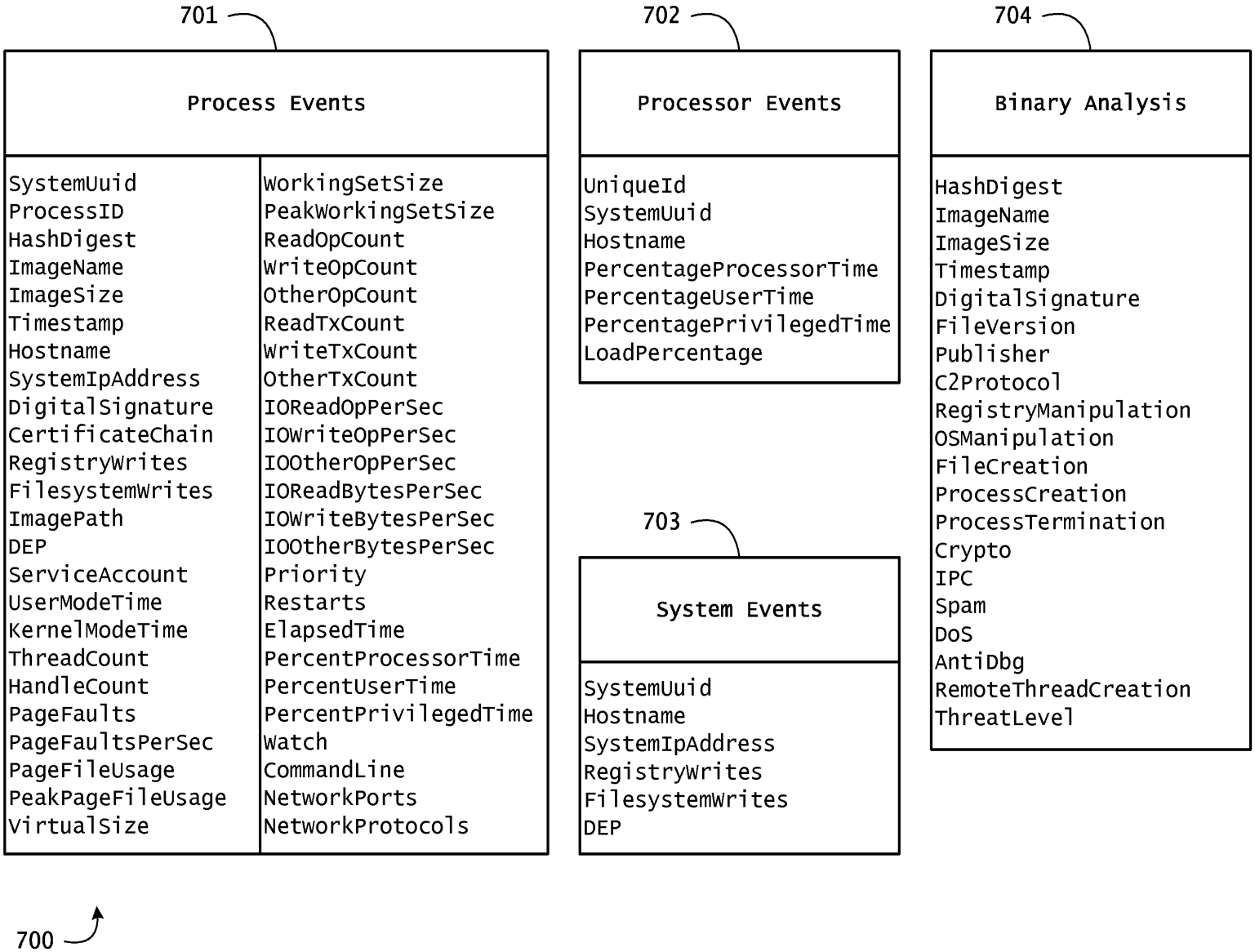
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 286 of 318

FIG. 6



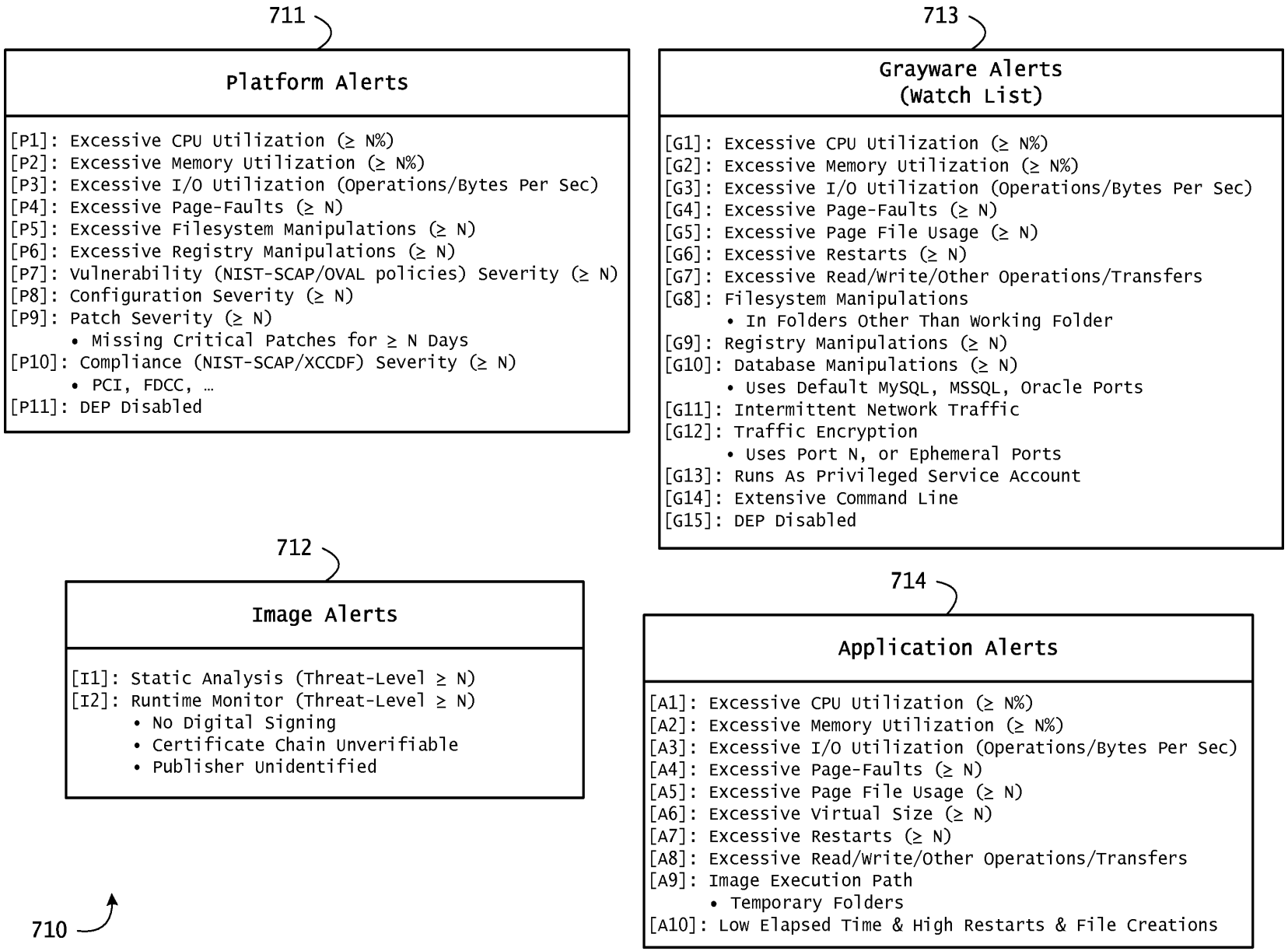
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 287 of 318

FIG. 7A



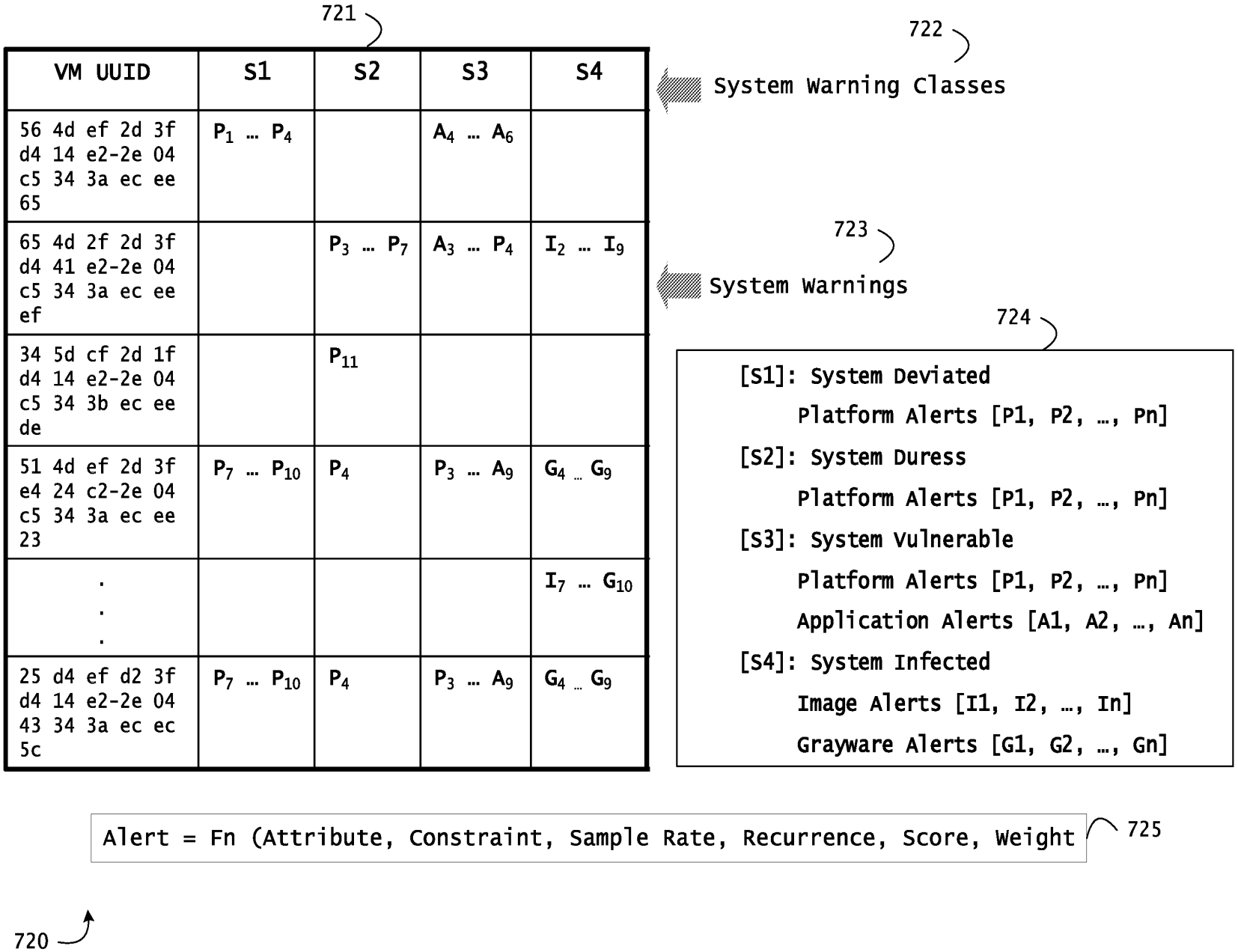
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 288 of 318

FIG. 7B



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 289 of 318

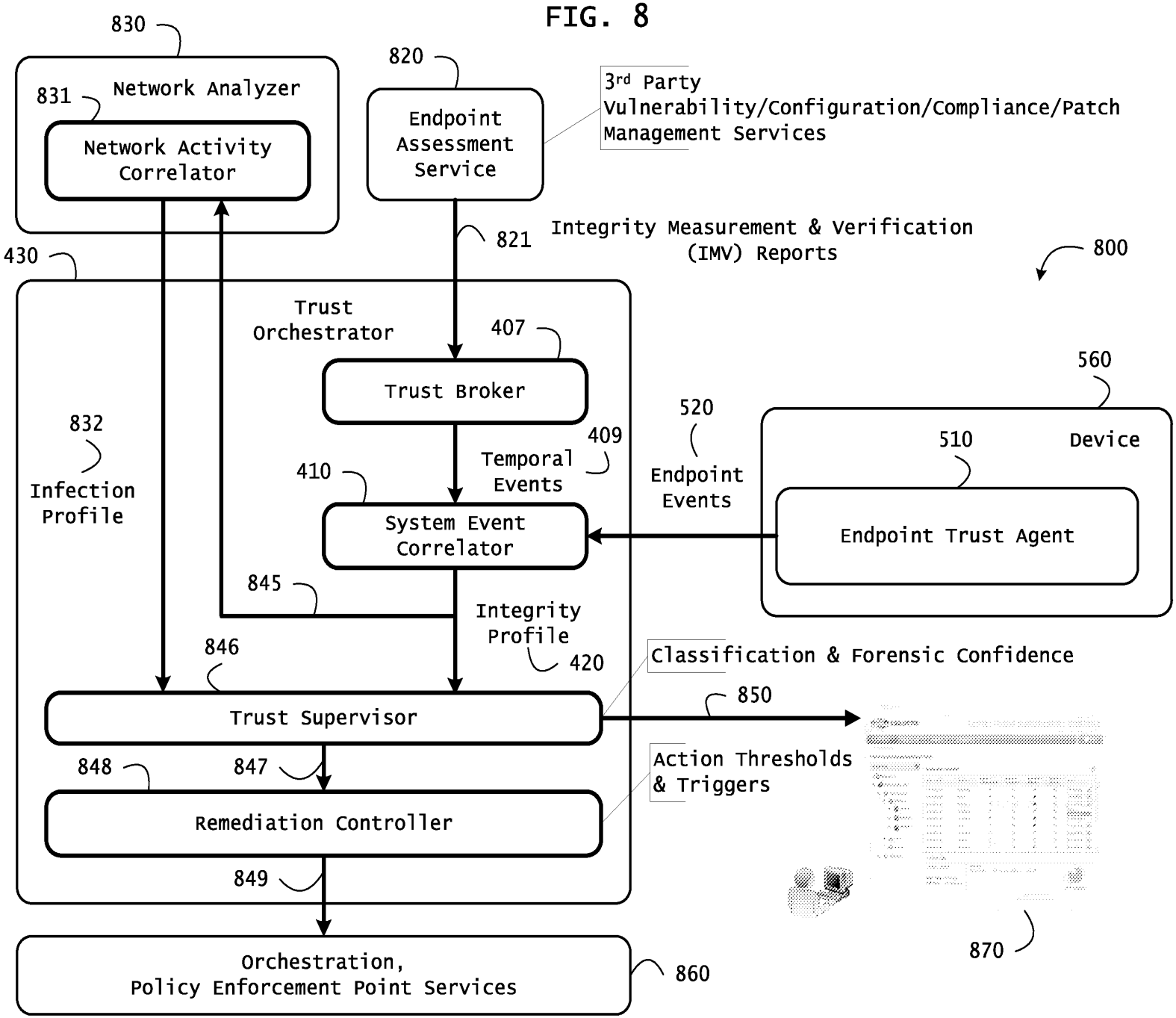
FIG. 7C



VM UUID	S1	S2	S3	S4
56 4d ef 2d 3f d4 14 e2-2e 04 c5 34 3a ec ee 65	P_1 … P_4		A_4 … A_6	
65 4d 2f 2d 3f d4 41 e2-2e 04 c5 34 3a ec ee ef		P_3 … P_7	A_3 … P_4	I_2 … I_9
34 5d cf 2d 1f d4 14 e2-2e 04 c5 34 3b ec ee de		P_{11}		
51 4d ef 2d 3f e4 24 c2-2e 04 c5 34 3a ec ee 23	P_7 … P_{10}	P_4	P_3 … A_9	G_4 … G_9
. . .				I_7 … G_{10}
25 d4 ef d2 3f d4 14 e2-2e 04 43 34 3a ec ec 5c	P_7 … P_{10}	P_4	P_3 … A_9	G_4 … G_9

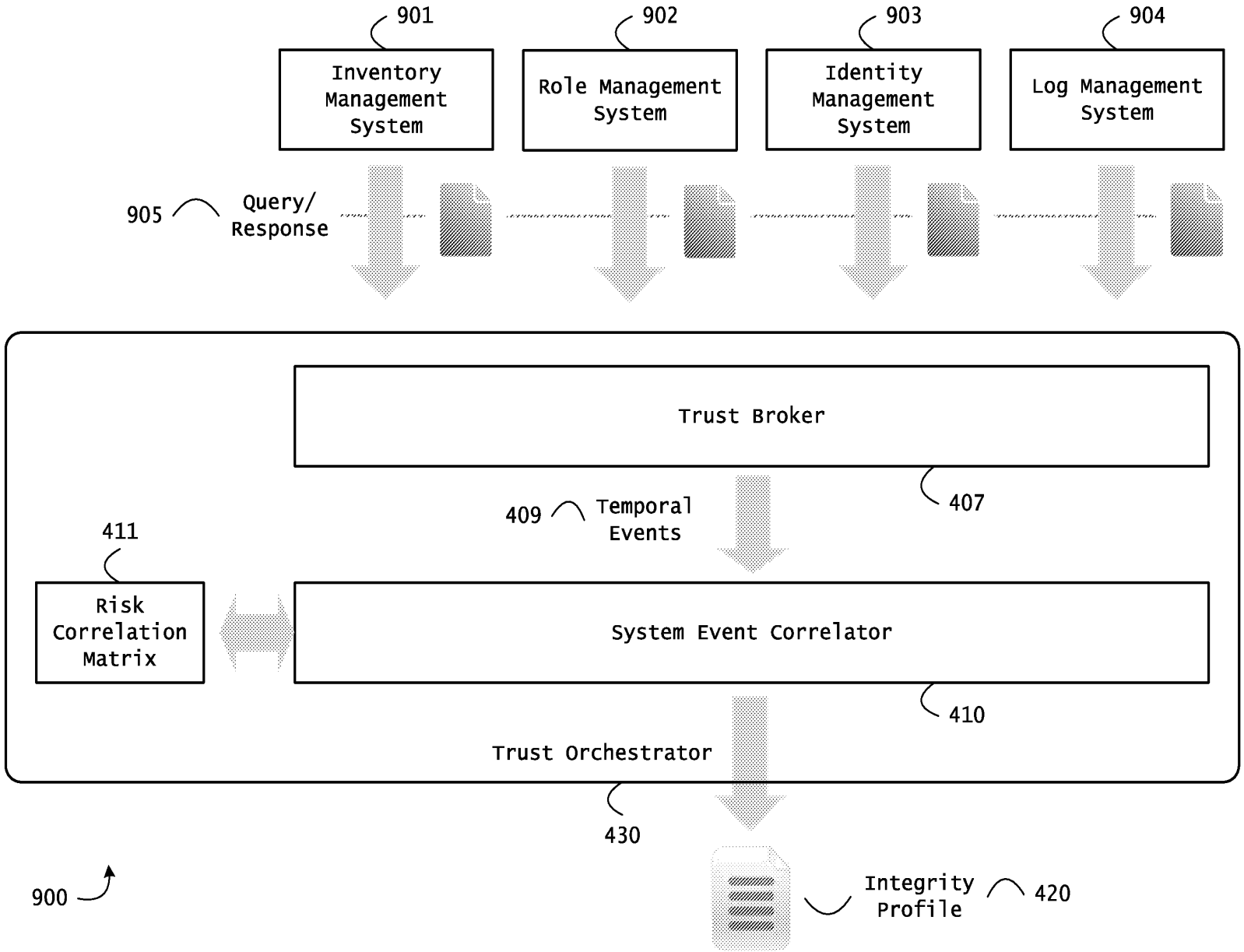
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 290 of 318

FIG. 8

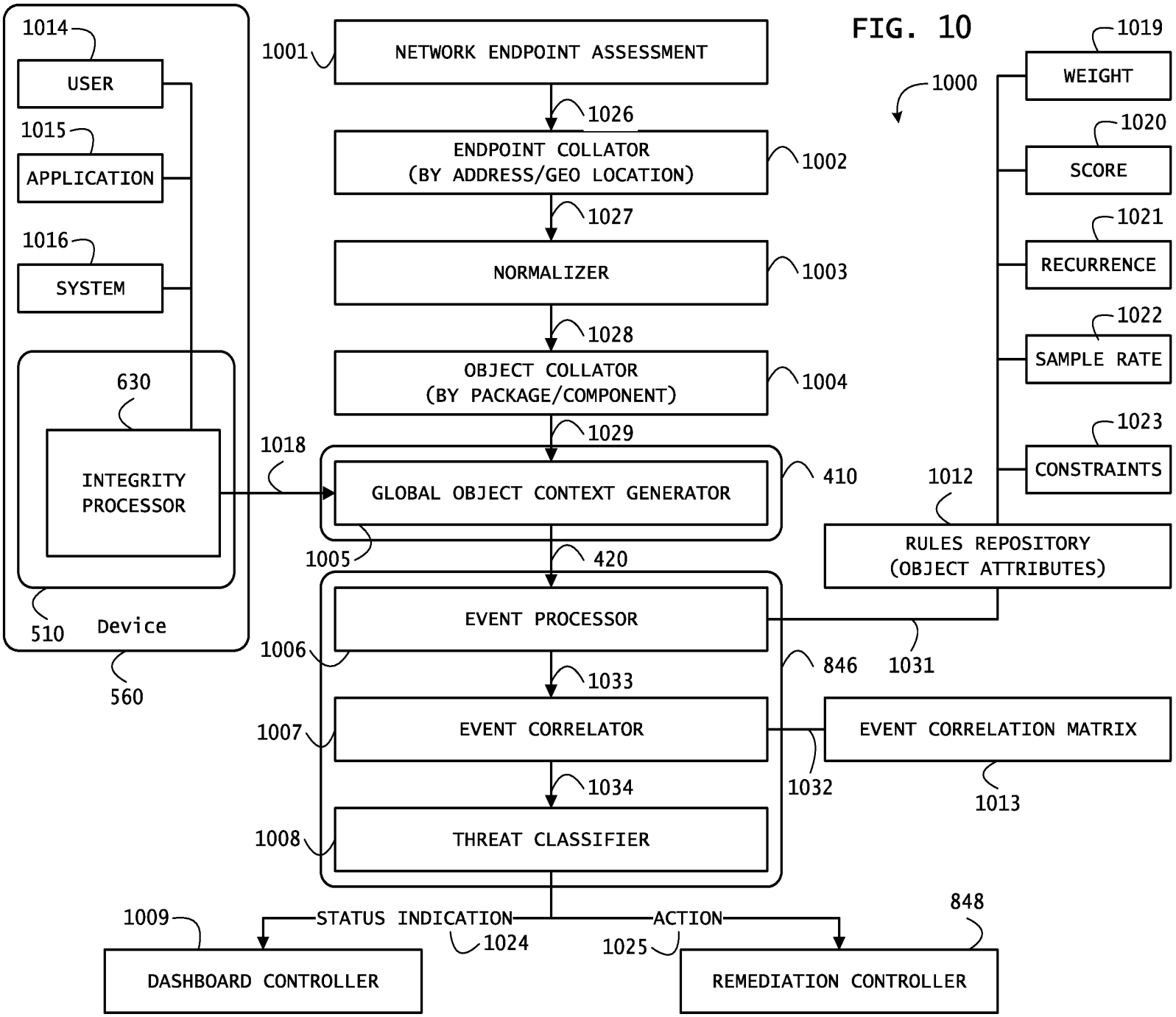


Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 291 of 318

FIG. 9



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 292 of 318



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 293 of 318

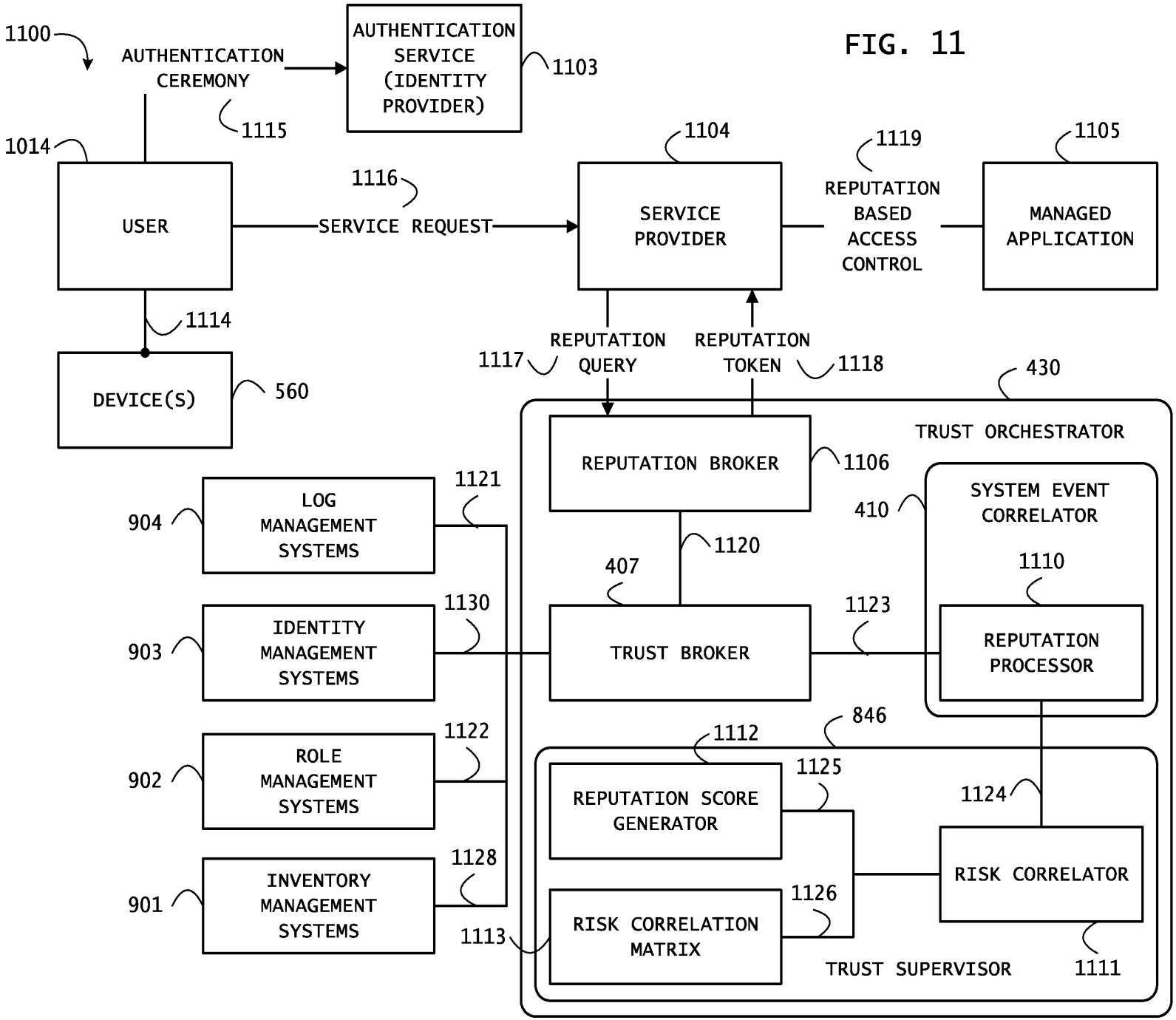
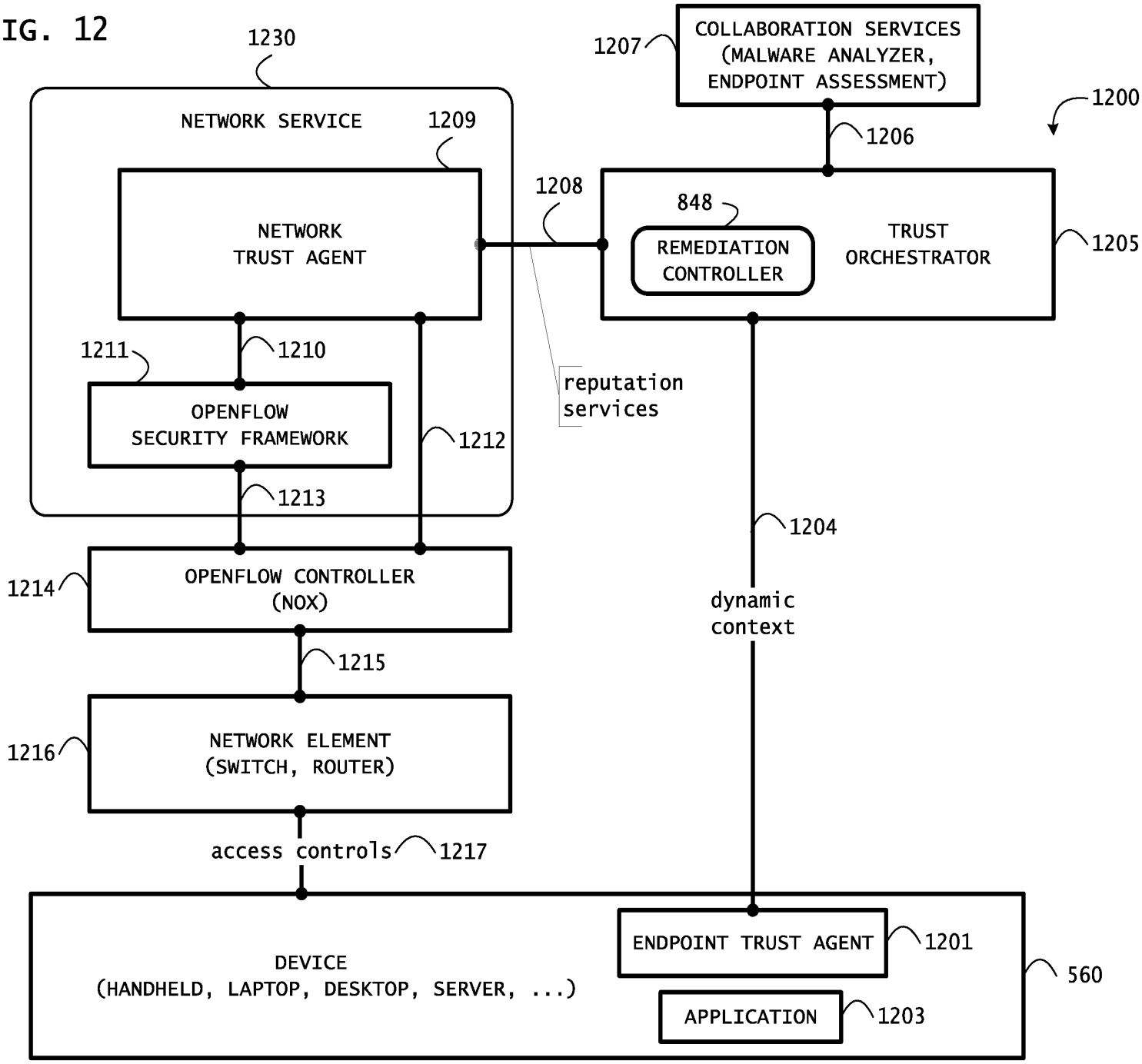


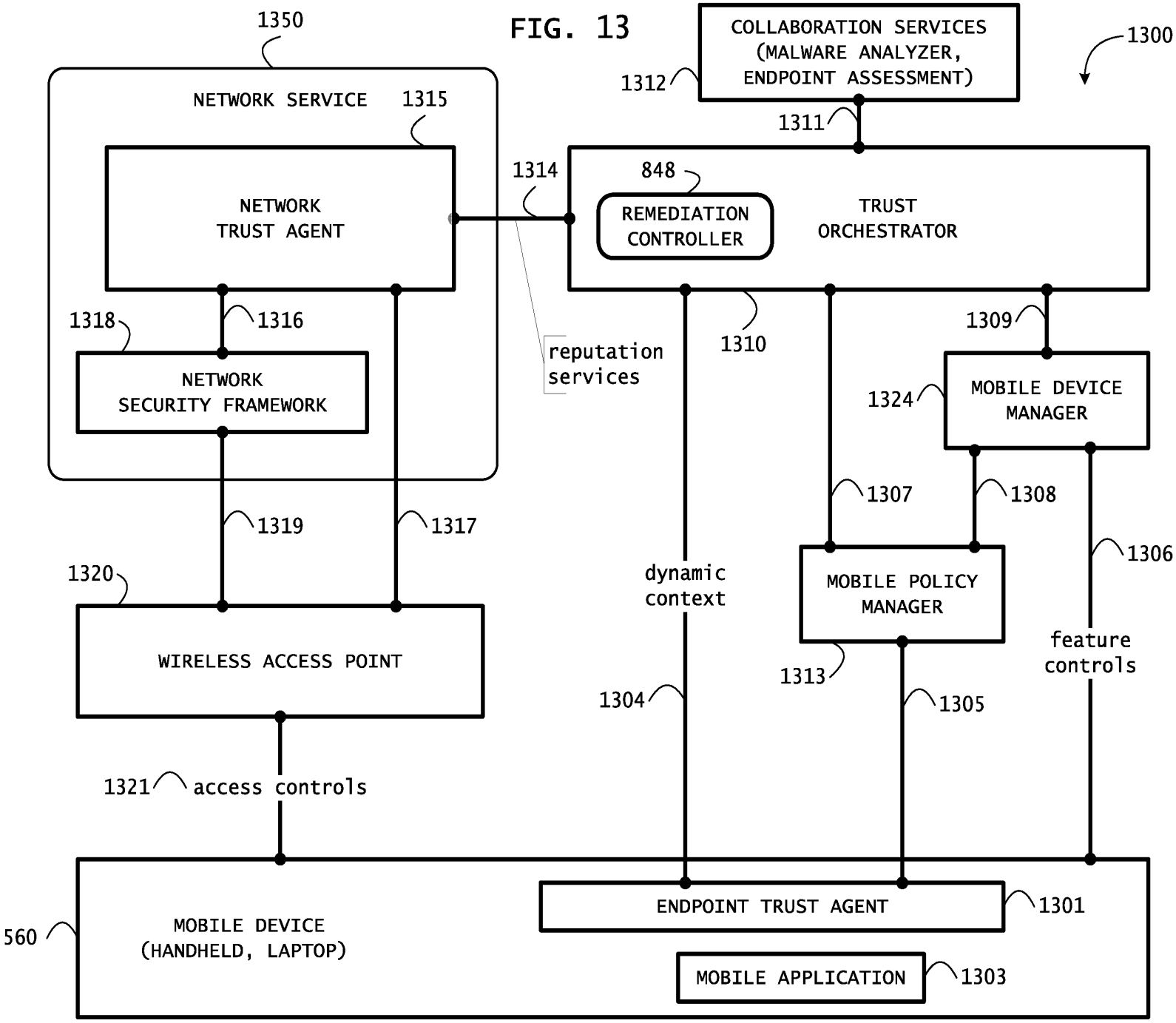
FIG. 11

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 294 of 318

FIG. 12

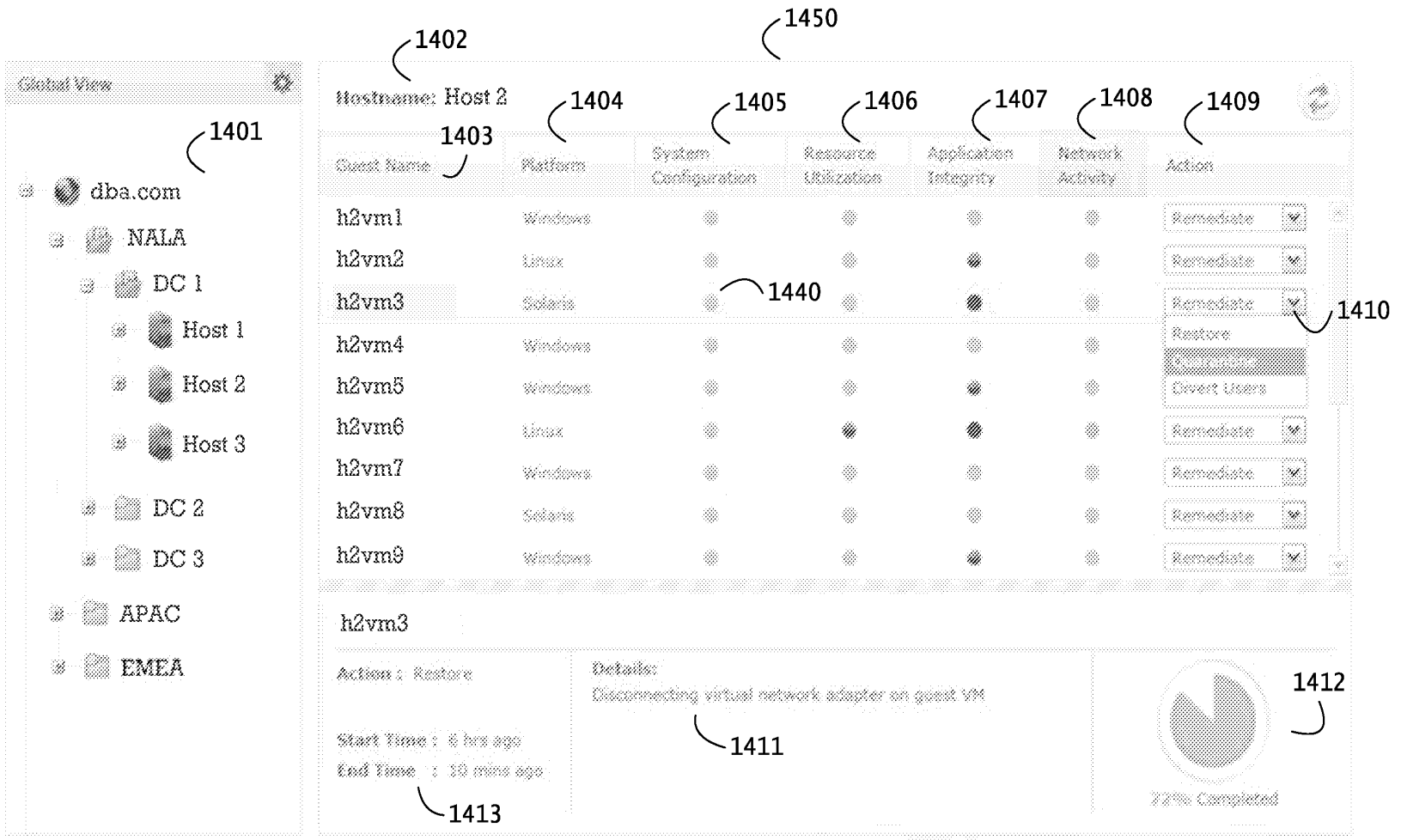


Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 295 of 318



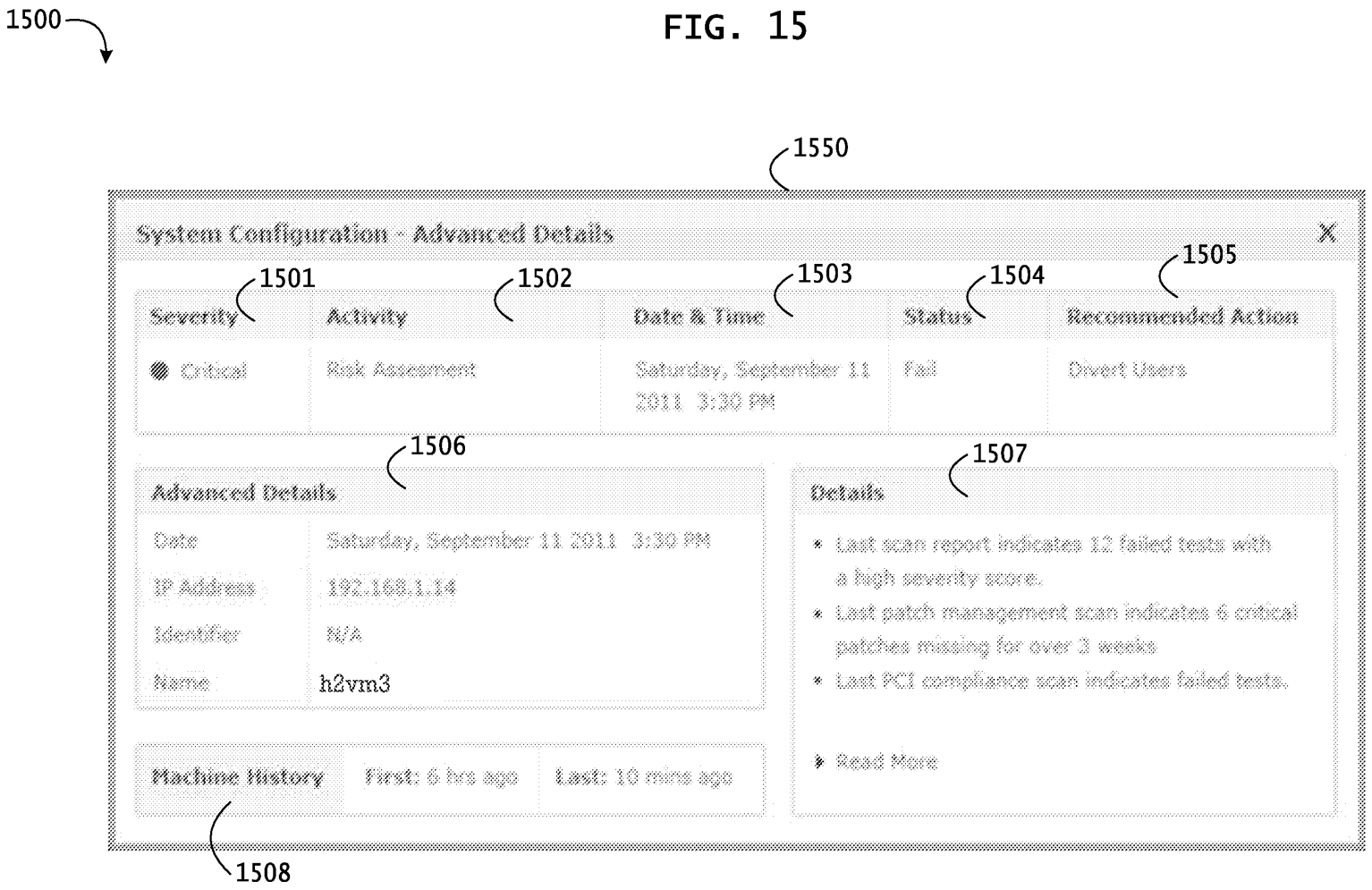
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 296 of 318

FIG. 14



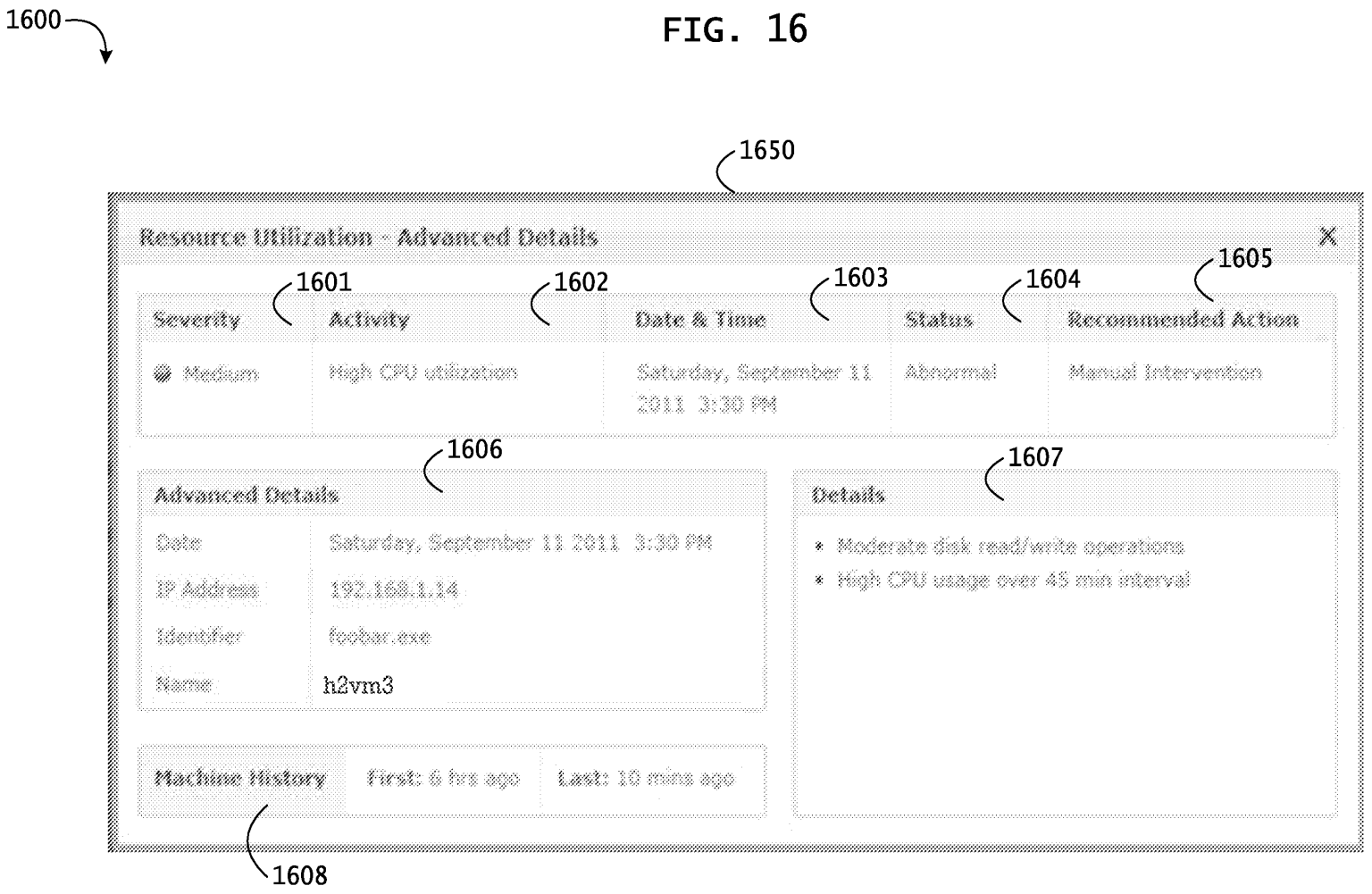
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 297 of 318

FIG. 15



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 298 of 318

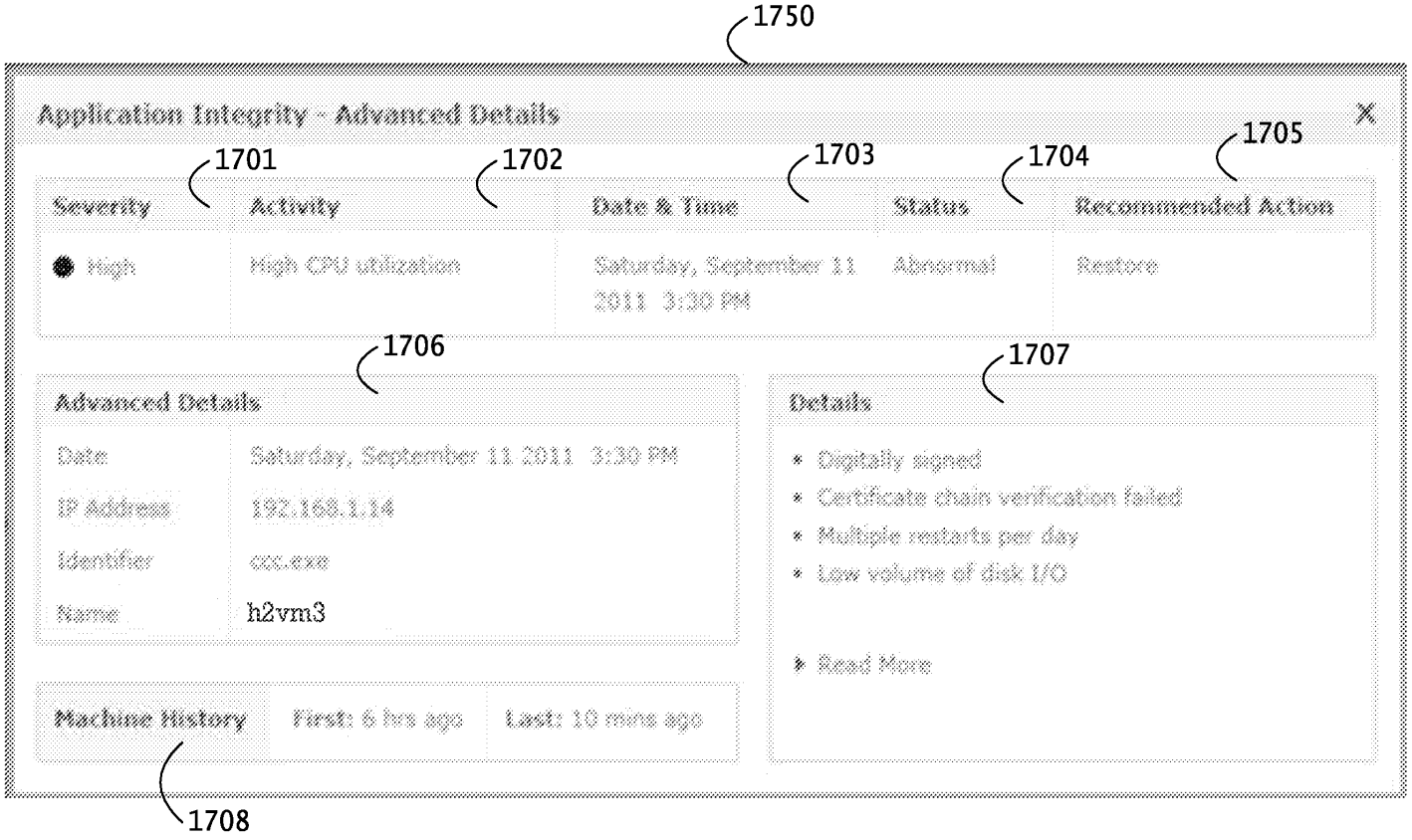
FIG. 16



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 299 of 318

1700

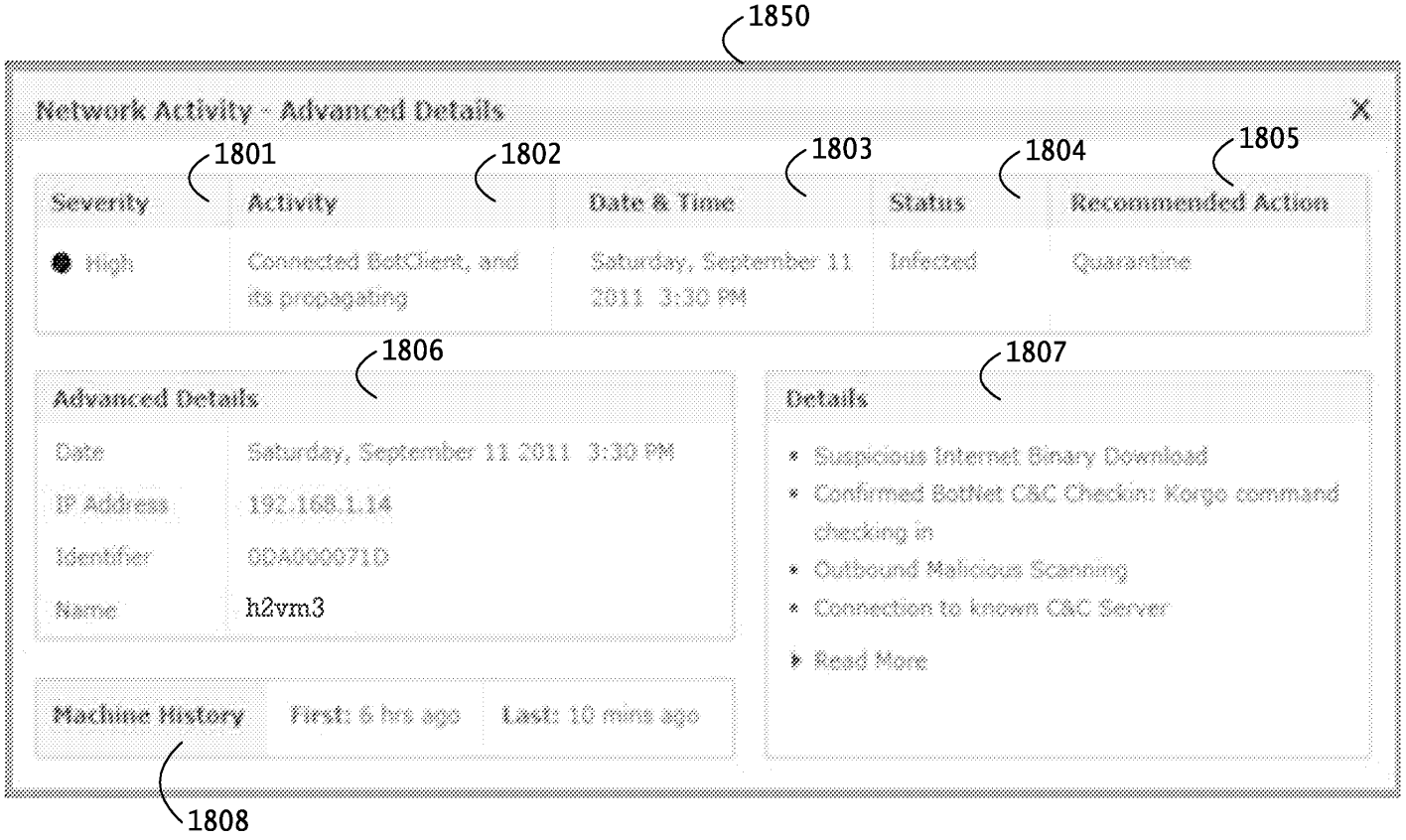
FIG. 17



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 300 of 318

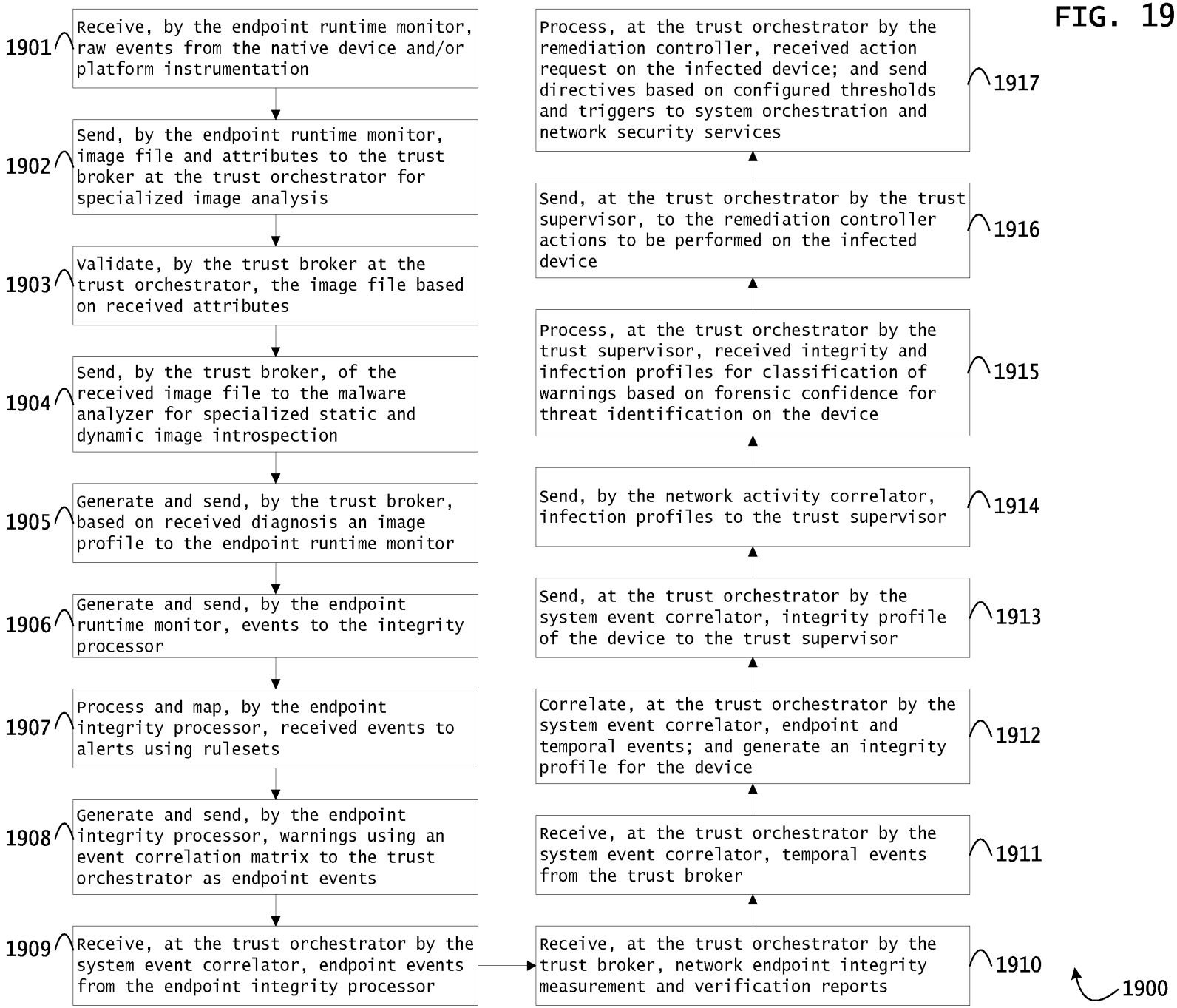
1800

FIG. 18



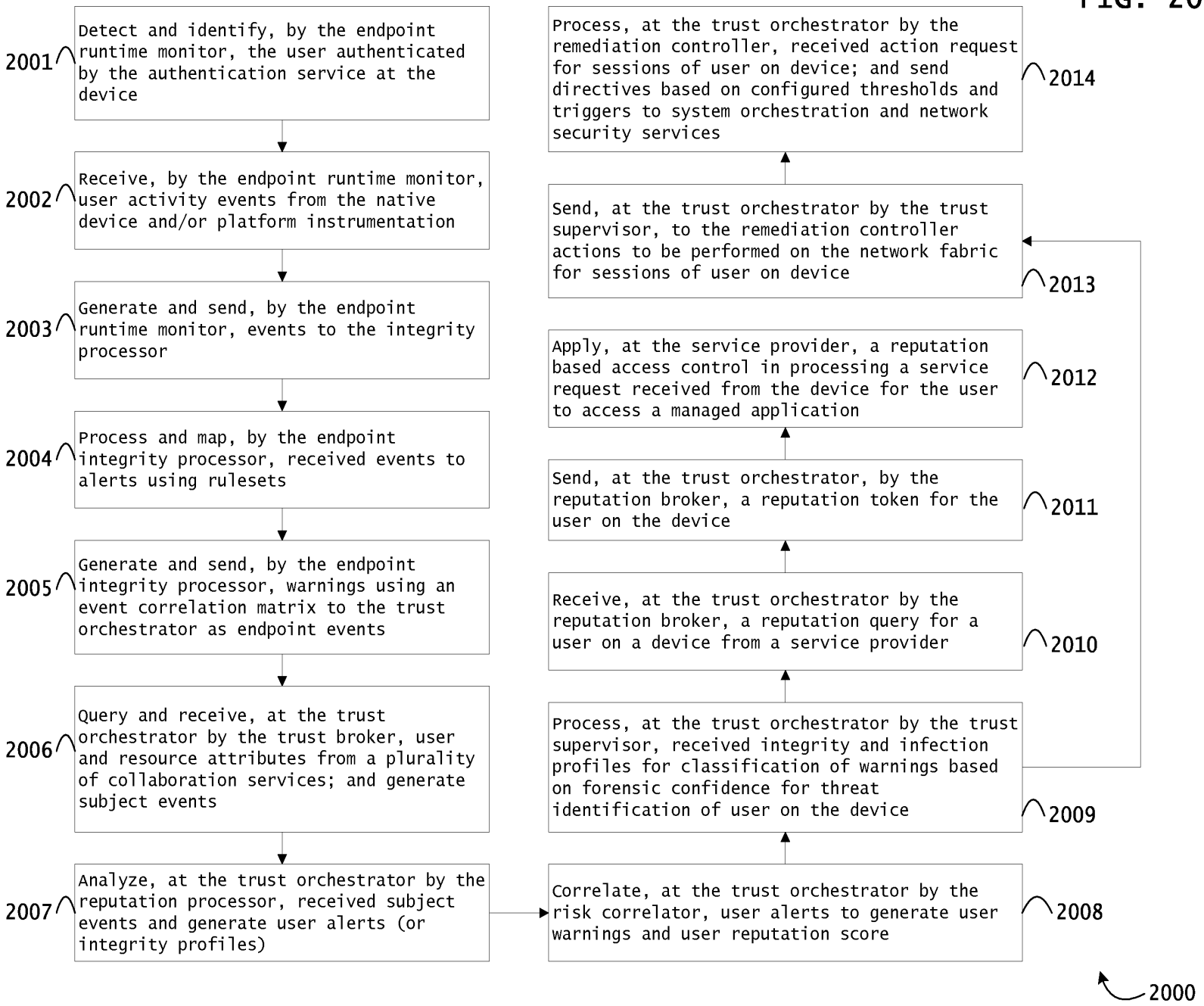
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 301 of 318

FIG. 19



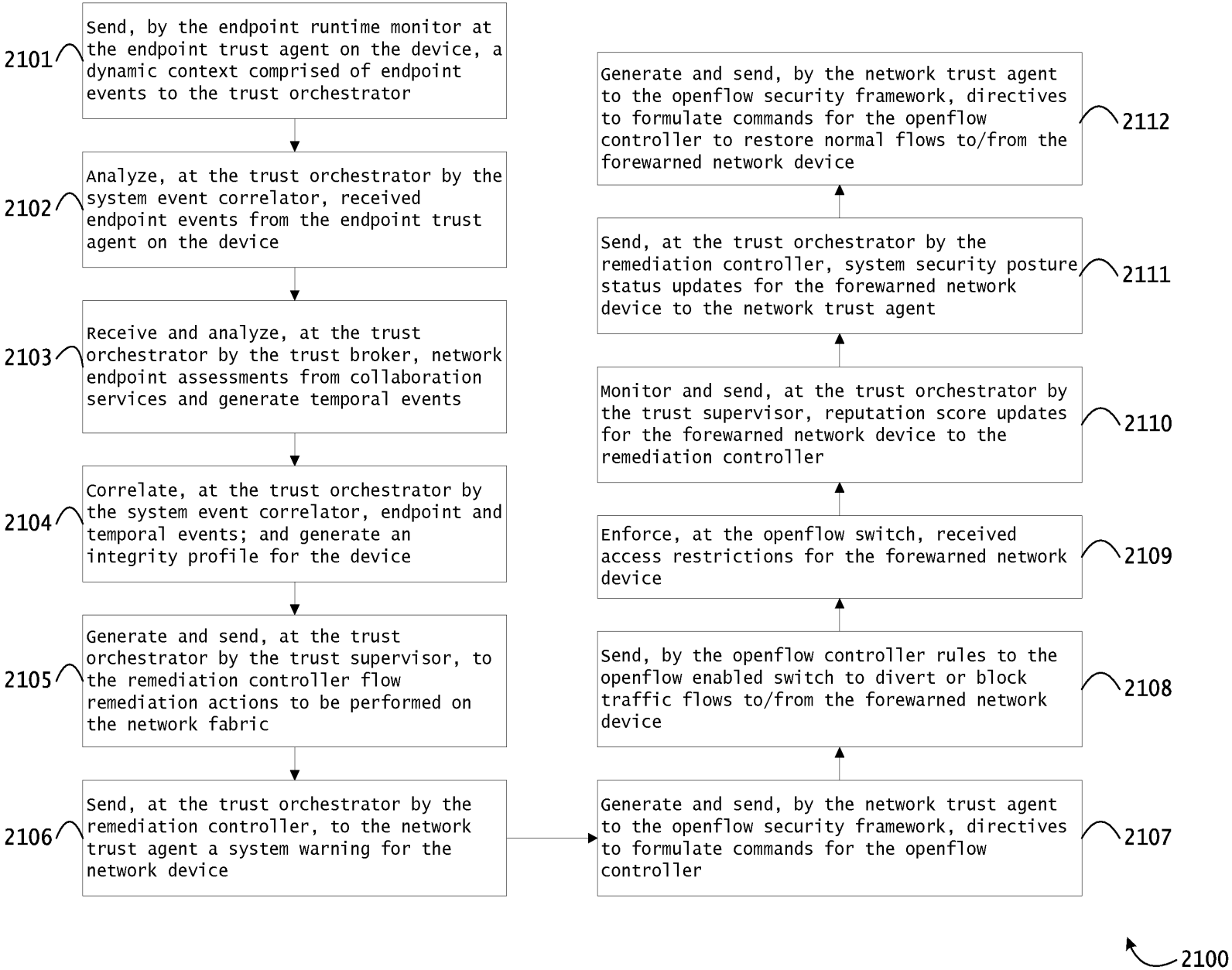
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 302 of 318

FIG. 20



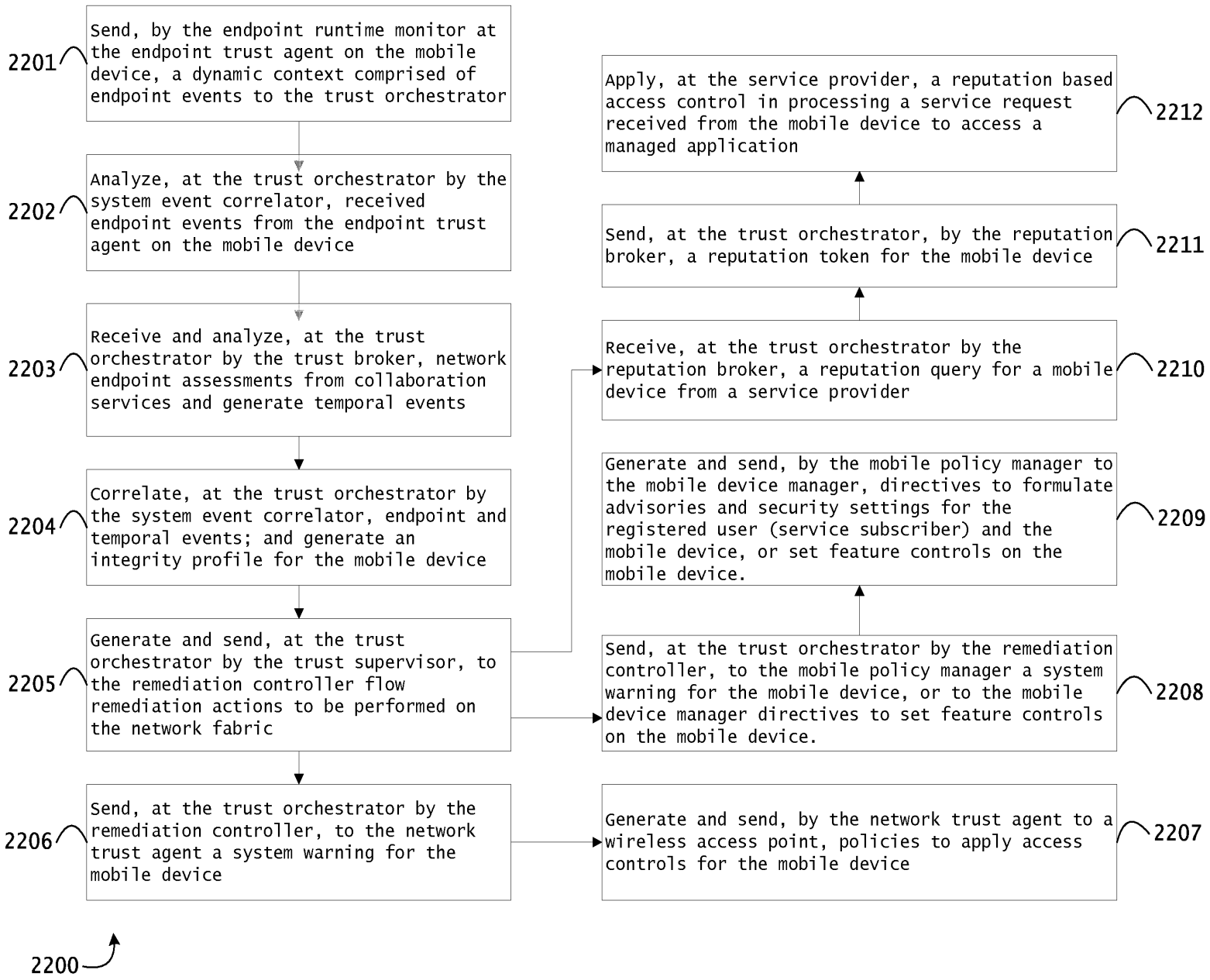
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 303 of 318

FIG. 21



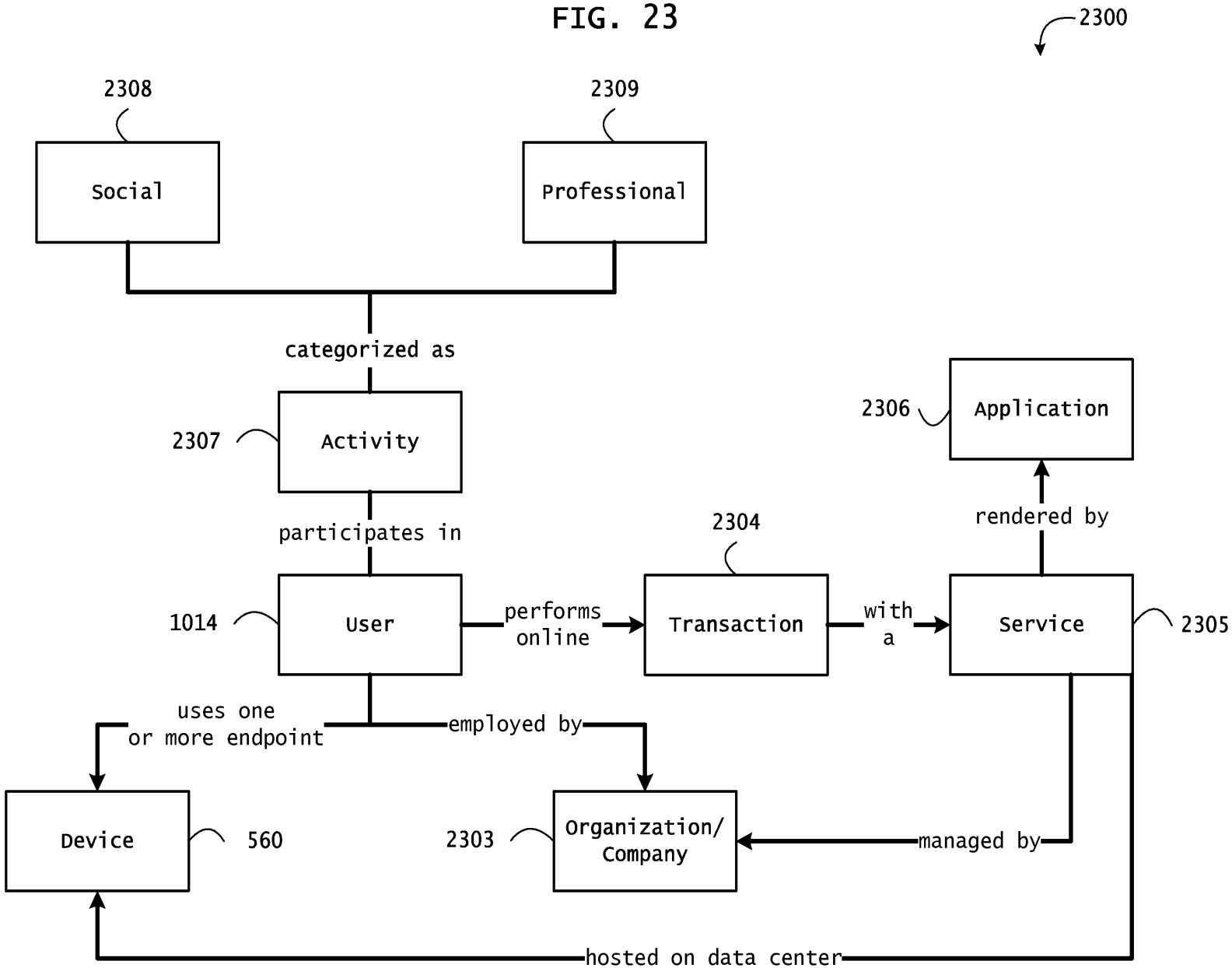
Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 304 of 318

FIG. 22



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 305 of 318

FIG. 23



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 306 of 318

FIG. 24

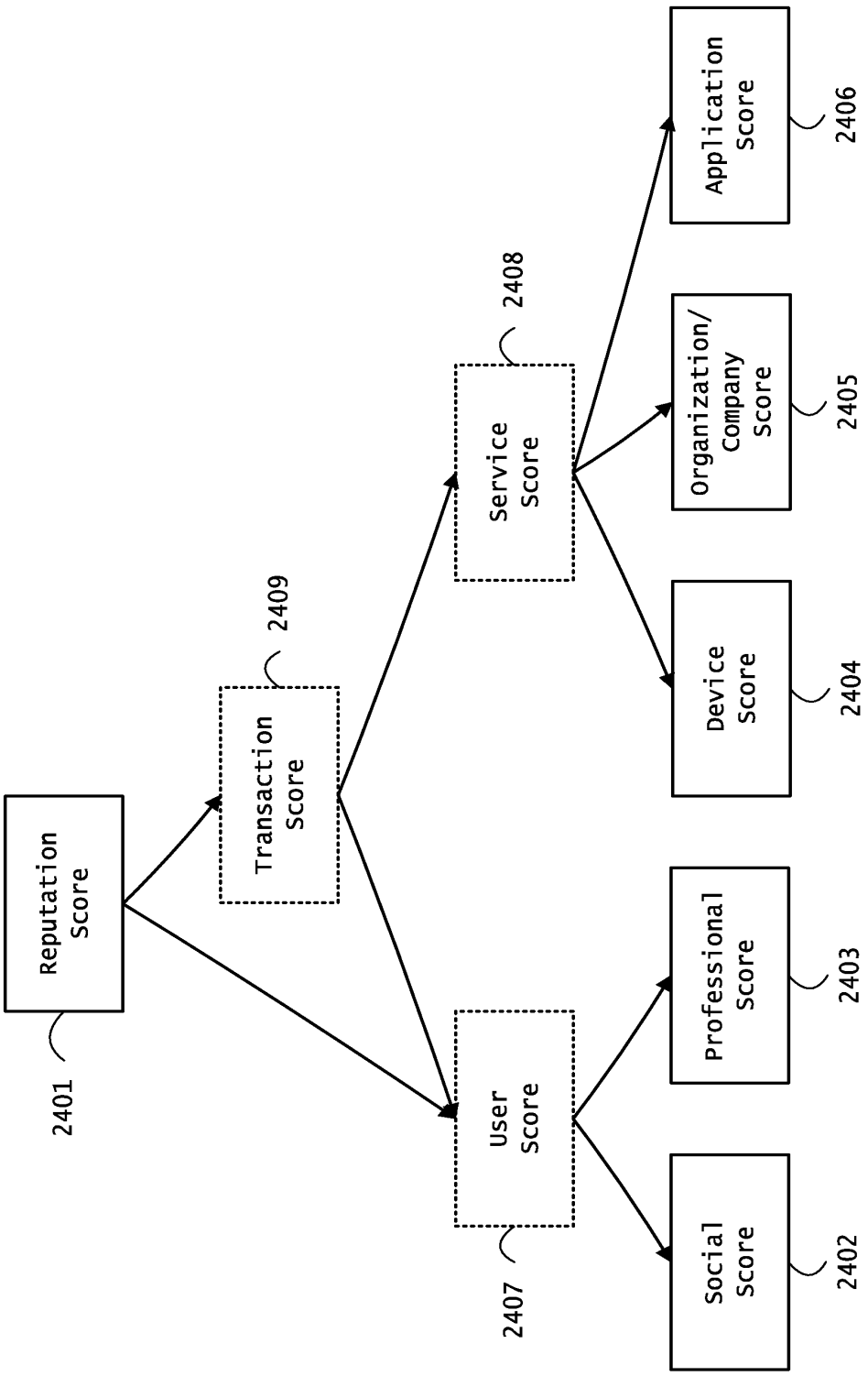
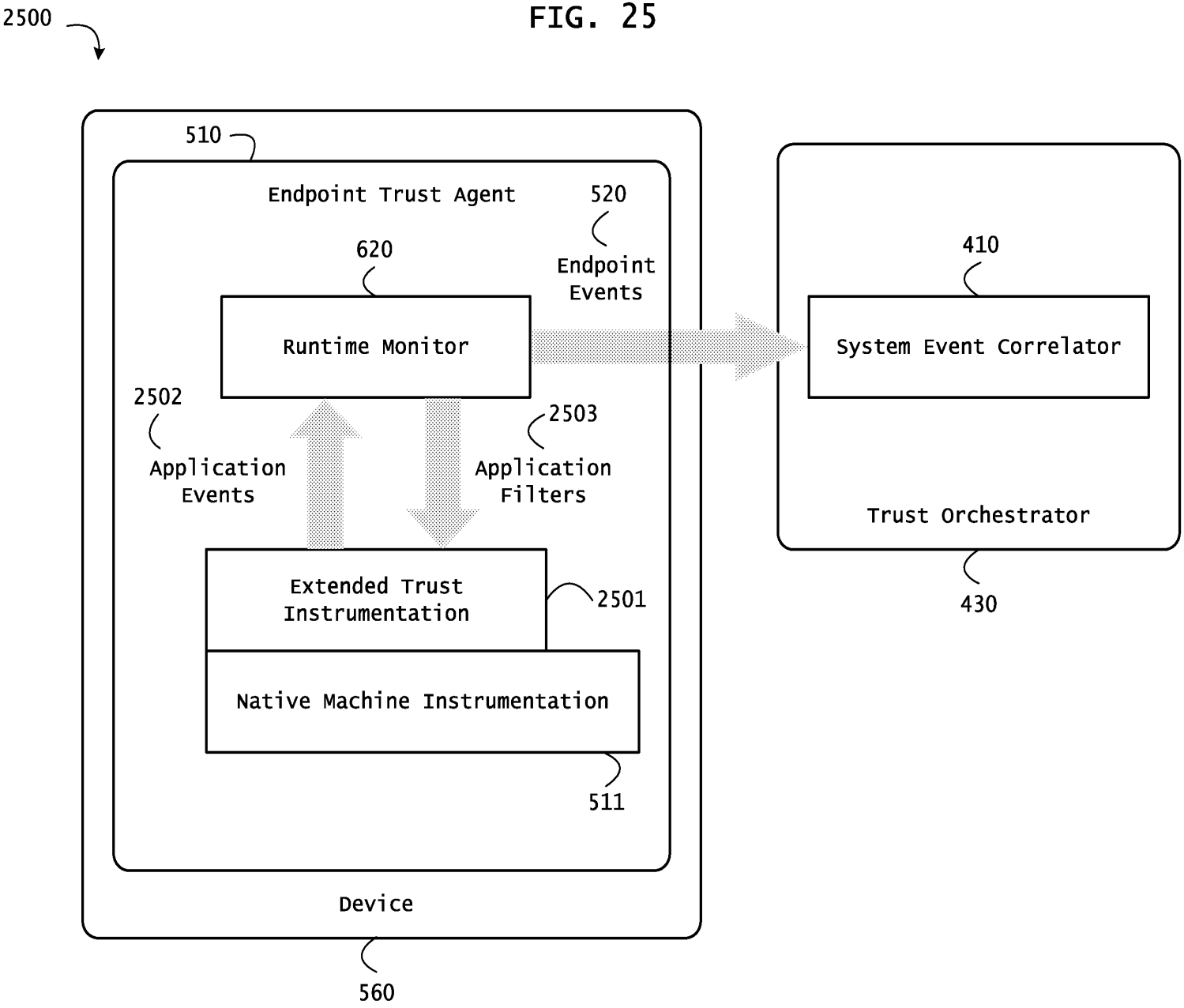
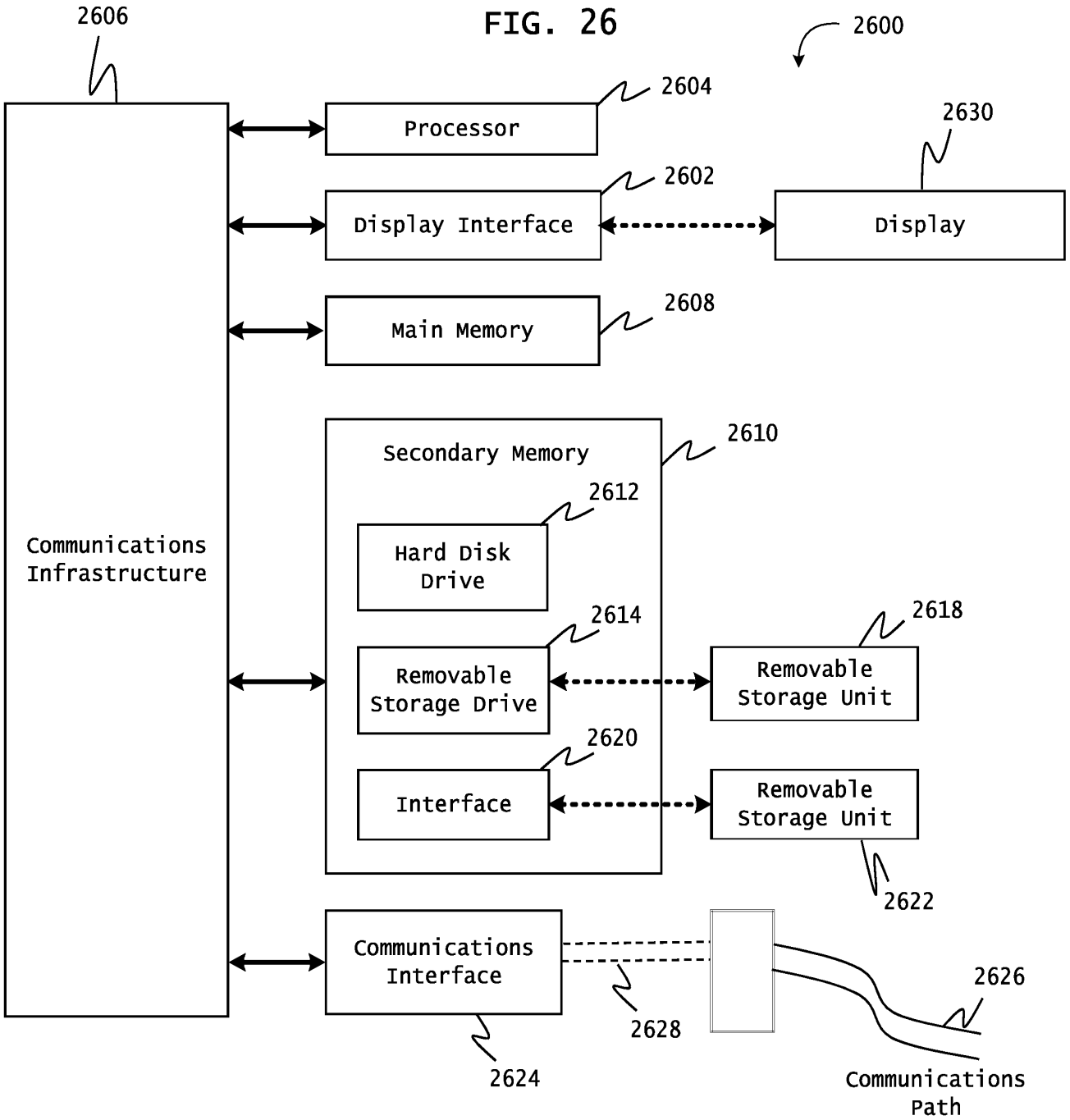

2400
Reputation Score
2401
Transaction Score
2409
User Score
2407
Service Score
2408
Social Score
2402
Professional Score
2403
Device Score
2404
Organization/ Company Score
2405
Application Score
2406

FIG. 25



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 308 of 318

FIG. 26



Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 309 of 318

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

the application of which **(check only one item below)**:

☐ is attached hereto.

☐ was filed as United States Patent application Number _____ on _____ and was amended on _____ (if applicable).

☐ was filed as PCT International application Number _____ on _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims, and drawings (if any), as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(d), 172 or 365(a) of any foreign application(s) for patent or inventor's certificate or of any international (PCT) application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international (PCT) application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §§119(a)-(d), 172 or 365(a):				
COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (MM/DD/YYYY)	PRIORITY CLAIMED UNDER 35 U.S.C. §§119, 172 OR 365(a)	
			Yes	No

(7/06)

I hereby appoint the attorneys and agents associated with the following PTO Customer Number of Buchanan Ingersoll & Rooney PC to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and transact all business in connection with international applications directed to said invention:

Customer Number **21839**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	Srinivas KUMAR
Signature	S Kumar
Date	7/25/2012
Residence (City, State, Country)	Cupertino, CA, US
Citizenship	US
Mailing Address	10926 Northridge Square
City, State, ZIP, Country	Cupertino, CA 95014, US
FULL NAME SECOND INVENTOR, IF ANY	Dennis POLLUTRO
Signature	
Date	
Residence (City, State, Country)	Clymer, NY, US
Citizenship	US
Mailing Address	8613 Knowlton Road
City, State, ZIP, Country	Clymer, NY 14724, US

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY

the application of which **(check only one item below)**:

☐ is attached hereto.

☐ was filed as United States Patent application Number _____ on _____ and was amended on _____ (if applicable).

☐ was filed as PCT International application Number _____ on _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims, and drawings (if any), as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(d), 172 or 365(a) of any foreign application(s) for patent or inventor's certificate or of any international (PCT) application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international (PCT) application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §§119(a)-(d), 172 or 365(a):				
COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (MM/DD/YYYY)	PRIORITY CLAIMED UNDER 35 U.S.C. §§119, 172 OR 365(a)	
			Yes	No

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 312 of 318

I hereby appoint the attorneys and agents associated with the following PTO Customer Number of Buchanan Ingersoll & Rooney PC to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and transact all business in connection with international applications directed to said invention:

Customer Number **21839**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	Srinivas KUMAR
Signature	
Date	
Residence (City, State, Country)	Cupertino, CA, US
Citizenship	US
Mailing Address	10926 Northridge Square
City, State, ZIP, Country	Cupertino, CA 95014, US
FULL NAME SECOND INVENTOR, IF ANY	Dennis POLOTRO
Signature	
Date	7/26/12
Residence (City, State, Country)	Clymer, NY, US
Citizenship	US
Mailing Address	8613 Knowlton Road
City, State, ZIP, Country	Clymer, NY 14724, US

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 313 of 318

Attorney Docket No. 0079152-000015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Srinivas KUMAR et al.	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Confirmation No.: Unassigned
	)	
Filed: July 27, 2012	)	
	)	
For: SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY	)	
	)	

GENERAL AUTHORIZATION FOR PETITIONS FOR EXTENSIONS OF TIME AND PAYMENT OF FEES

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

Sir:

In accordance with 37 C.F.R. § 1.136(a)(3), the U.S. Patent and Trademark Office is hereby provided with a general authorization to treat any concurrent or future reply requiring a petition for an extension of time for its timely submission as containing a request therefor for the appropriate length of time.

The Commissioner is hereby authorized to charge any appropriate fees that may be required by this paper, or any other submissions in this application, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 27, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

APPLICATION DATA SHEET

Application Information

Application Number::	
Filing Date::	
Application Type::	Nonprovisional
Subject Matter::	Utility
CD-ROM or CD-R?::	None
Computer Readable Form (CRF)?::	No
Title::	SYSTEMS AND METHODS FOR ORCHESTRATING RUNTIME OPERATIONAL INTEGRITY
Attorney Docket Number::	0079152-000015
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	29
Small Entity?::	No
Petition Included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Srinivas
Family Name::	KUMAR
City of Residence::	Cupertino

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 315 of 318

State or Province of Residence::	California
Country of Residence::	USA
Street of Mailing Address::	10926 Northridge Square
City of Mailing Address::	Cupertino
State or Province of Mailing Address::	California
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	95014
Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Dennis
Middle Name::	Vance
Family Name::	POLLUTRO
City of Residence::	Clymer
State or Province of Residence::	New York
Country of Residence::	USA
Street of Mailing Address::	8613 Knowlton Road
City of Mailing Address::	Clymer
State or Province of Mailing Address::	New York
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	14724

Palo Alto Networks - Exhibit 1002
Palo Alto Networks v. Taasera - IPR2023-00705
Page 316 of 318

Correspondence Information

Correspondence Customer Number:: 21839

Phone Number:: (703) 836-6620

Fax Number: (703) 836-2021

Representative Information

Representative Customer Number:: 21839

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Claiming benefit under 35 USC 119(e)	61/641,007	05/01/12

Assignee Information

Assignee Name:: Taasera, Inc.

Street of Mailing Address:: 1030 State Street

City of Mailing Address:: Erie

State or Province of Mailing Address:: Pennsylvania

Country of Mailing Address:: USA

Postal or Zip Code of Mailing Address:: 16501

Signature		Date	July 27, 2012
Name	Charles F. Wieland III	Registration No.	33,096

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 13559707 Document Date: 7/27/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006