

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

PTAB Case No. IPR2026-00472

U.S. Patent No. 12,244,621

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 12,244,621**

TABLE OF CONTENTS

EXHIBIT LIST	viii
I. INTRODUCTION	1
II. MANDATORY NOTICES	2
A. Real party in interest.....	2
B. Related matters	2
C. Counsel and service information.....	2
D. Fees.....	3
III. IPR REQUIREMENTS—37 C.F.R. §42.104	3
A. Standing—37 C.F.R. §42.104	3
B. Challenged claims and relief requested.....	3
1. Challenged Claims	4
2. Prior art—Invalidity under 35 U.S.C. § 103.....	6
3. Grounds	8
4. No Discretionary Denial Factors Are Present	8
IV. TECHNOLOGY DESCRIPTION.....	9
A. Overview of the Underlying Technology Landscape	9
1. Audit Log Comparison	9
2. Shadow Information Technology	10
B. The '621 Patent	11
1. Alleged invention.....	11
2. Effective Filing Date of the Challenged Claims.....	13

3.	Prosecution history.....	19
V.	LEVEL OF ORDINARY SKILL	20
VI.	CLAIM CONSTRUCTION	21
VII.	SPECIFIC GROUNDS.....	21
A.	Ground 1: Karunakaran Renders Claims 1-3, 5-11, and 13-19 Obvious.	22
1.	Overview of Karunakaran.....	22
2.	Claims 1, 9, and 17.....	27
a.	1[pre]: “A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising” (See 9[pre] and 17[pre]/[a]/[b] below).....	27
b.	9[pre] / 17[pre], 17[a], 17[b]: “A non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to” / “A system comprising: a memory; and a processing device, operatively coupled to the memory, the processing device configured to”	29
c.	1[a] / 9[a] / 17[c]: “gathering [or gather], from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;”.....	30
d.	1[b] / 9[b] / 17[d]: “gathering [or gather], from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources;”	31
e.	1[c] / 9[c] / 17[e]: “identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at	

least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.”	33
3. Claims 2, 10, and 18	40
2 [“The method of claim 1”] / 10[“The non-transitory computer readable storage medium of claim 9”] / 18 [“The system of claim 17”] . . . “wherein the first information is gathered from one or more identity providers.”	40
4. Claims 3, 11, and 19	43
3 [“The method of claim 1”] / 11 [“The non-transitory computer readable storage medium of claim 9”] . . . “wherein the first information is gathered from one or more applications of the one or more resources or of the providers.”	43
19: “The system of claim 17 wherein the first information is gathered from one or more applications of the one or more resources or the providers of the one or more resources.”	43
5. Claims 5 and 13.....	44
5: “The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.”	44
13: “The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to generate an alert in response to identifying the one or more shadow systems.”	44

6.	Claims 6 and 14.....	44
6:	“The method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems.”	44
14:	“The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to direct the user to a remediation workflow in response to identifying the one or more shadow systems.”	44
7.	Claims 7 and 15.....	46
7:	“The method of claim 1 wherein the first information is not gathered from the one or more user devices.”	46
15:	“The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more resources or the providers of the one or more resources other than the one or more user devices.”	46
8.	Claims 8 and 16.....	47
8:	“The method of claim 1 wherein the second information is gathered via the one or more client applications including one or more proxy applications executed on the at least a subset of the one or more user devices.”	47
16:	“The non-transitory computer readable storage medium of claim 9 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices.”	47
B.	Ground 2: Combining Chien with Lipman Renders Claims 1-3, 5-11, and 13-19 Obvious.....	49
1.	Overview of Chien.....	49
2.	Overview of Lipman	53

3.	Motivation to Combine	56
4.	Claims 1, 9, and 17.....	60
a.	1[pre]: “A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising” (<i>See</i> 9[pre] and 17[pre] below)	60
b.	9[pre] / 17[pre], 17[a], 17[b]: “A non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to” / “A system comprising: a memory; and a processing device, operatively coupled to the memory, the processing device configured to”	61
c.	1[a] / 9[a] / 17[c]: “gathering [or gather], from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;”	62
d.	1[b] / 9[b] / 17[d]: “gathering [or gather], from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources;”	63
e.	1[c] / 9[c] / 17[e]: “identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.”	64
5.	Claims 2, 10, and 18	69

2	["The method of claim 1"] / 10["The non-transitory computer readable storage medium of claim 9"] / 18 ["The system of claim 17"] . . . "wherein the first information is gathered from one or more identity providers."	69
6.	Claims 3, 11, and 19	70
3	["The method of claim 1"] / 11 ["The non-transitory computer readable storage medium of claim 9"] . . . "wherein the first information is gathered from one or more applications of the one or more resources or of the providers."	70
19:	"The system of claim 17 wherein the first information is gathered from one or more applications of the one or more resources or the providers of the one or more resources."	70
7.	Claims 5 and 13	71
5:	"The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems."	71
13:	"The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to generate an alert in response to identifying the one or more shadow systems."	71
8.	Claims 6 and 14	73
6:	"The method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems."	73
14:	"The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to direct the user to a remediation workflow in response to identifying the one or more shadow systems."	73

9. Claims 7 and 15.....	75
7: “The method of claim 1 wherein the first information is not gathered from the one or more user devices.”	75
15: “The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more resources or the providers of the one or more resources other than the one or more user devices.”	75
10. Claims 8 and 16.....	75
8: “The method of claim 1 wherein the second information is gathered via the one or more client applications including one or more proxy applications executed on the at least a subset of the one or more user devices.”	75
16: “The non-transitory computer readable storage medium of claim 9 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices.”	75
VIII. CONCLUSION.....	79
IX. PAYMENT OF FEES	79

EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 12,244,621 (“the ’621 Patent”)
1002	File History of the ’621 Patent
1003	Declaration of Dr. Michael Franz
1004	Curriculum Vitae of Dr. Michael Franz
1005	U.S. Patent Publication No. 2018/0288045 A1 (“Karunakaran”), Mar. 27, 2018
1006	U.S. Patent Publication No. 2007/0220605 A1 (“Chien”), Mar. 15, 2007
1007	U.S. Patent No. 10,237,294 (“Zadeh”), filed Jan. 30, 2017
1008	U.S. Pat. Publication No. 2019/0199751 A1 (“Lipman”), filed Dec. 21, 2017
1009	Threat Intelligence Cloud, Leveraging the Global Threat Community to Prevent Known and Unknown Threats, Palo Alto Networks®, 2016
1010	Reserved
1011	Special Publication (SP) 800-92 “Guide to Computer Security Log Management,” September 2006.
1012	The Wayback Machine “Extended Log File Format, W3C Working Draft WD-logfile-960323,” 1997
1013	Snort (1999) Lightweight Intrusion Detection For Networks. The USENIX Association, Proceedings of LISA ‘1999: 13 th Systems Administration Conference.
1014	Suricata (2009) Intrusion Detection / Intrusion Prevention Systems

Exhibit No.	Description
	(IDS/IPS)
1015	Cisco, “The Shadow IT Dilemma,” https://blogs.cisco.com/cloud/the-shadow-it-dilemma , March 23, 2016, Stark, Joann.
1016	Gartner, “Top 10 Security Predictions”. https://web.archive.org/web/20160619165354/https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016?cm_mmc=social-_rm-_gart-_swg , June 15th, 2016.
1017	U.S. Patent Application 17/836,813, filed Jun. 9, 2022
1018	U.S. Patent 11,689,553, filed March 9, 2021
1019	U.S. Patent 10,986,114, filed July 1, 2019
1020	U.S. Patent 10,419,469, filed September 18, 2018
1021	U.S. Provisional Patent Application 62/590,986, filed on Nov. 27, 2017
1022	U.S. Provisional Patent Application 62/650,971, filed March 30, 2018.
1023	U.S. Provisional Patent Application 63/240,818, filed September 3, 2021.
1024	U.S. Provisional Patent Application 62/478,081, filed March 29, 2017 (“Karunakaran Provisional”)
1025	Generated Redline Comparison of the PDF Specification of the ‘621 Patent and U.S. Patent No. 10,419,469
1026	Generated Redline Comparison of the Text of the Specification of the ‘621 Patent and U.S. Patent No. 10,419,469

I. INTRODUCTION

U.S. Patent No. 12,244,621 (“the ’621 patent”) claims nothing more than comparing two pieces of information and flagging mismatches—a concept as old as balancing a checkbook or reconciling credit card statements. Here, the patent applies that same concept to network security—comparing an access log from a resource provider against a log from a user device to spot devices operating outside enterprise IT control, known as “shadow systems.” The term “shadow IT” was an established industry concern years before the patent’s earliest possible priority date. And the patent adds nothing to the underlying technology: it uses generic processors and memory to perform their standard functions.

The claims never should have issued. Every element recited in the challenged claims was well-known in the art years before the patent’s actual priority date (June 9, 2022). A single reference—U.S. Patent Publication No. 2018/0288045 A1 (“Karunakaran”)—alone renders every challenged claim obvious. Yet the examiner never even considered Karunakaran because the examiner relied on the priority date printed on the face of the patent (November 2017) without examining the priority chain. Ex-1002 at 178 (Feb. 1, 2024 Office Action). Had the examiner done so, it would have discovered that the ’621 patent is a continuation-in-part whose challenged claims find support only in material first disclosed on June 9, 2022. Under that later priority date, Karunakaran qualifies as

prior art—and by itself makes the claims obvious. Nor is Karunakaran the only reference the examiner missed. U.S. Patent Publication No. 2007/0220605 A1 (“Chien”) combined with U.S. Patent Publication No. 2019/0199751 A1 (“Lipman”) independently renders the claims obvious—both references predate even the patent’s earliest possible provisional application filing date of September 3, 2021.

Accordingly, Petitioner respectfully requests cancellation of claims 1–3, 5–11, and 13–19 of the ’621 patent under 35 U.S.C. §103.

II. MANDATORY NOTICES

A. Real party in interest

Netskope, Inc. is the sole real party-in-interest.

B. Related matters

Patentee originally asserted the ’621 Patent against Petitioner in the United States District Court for the Northern District of California, Case No. NDCA-4-25-cv-02360-HSG. That clam has now been severed into Case No. 4:26-cv-08886-HSG.

C. Counsel and service information

Lead Counsel: Thomas N. Millikan (Reg. No. 72,316).

Back-up counsel: Joseph P. Reid (Reg. No. 72,317), Andrew Klein (*pro hac vice* forthcoming), and Ericka Jacobs Schulz (Reg. No. 60,665).

These attorneys can be reached by mail at Sheppard, Mullin, Richter & Hampton LLP, 12275 El Camino Real, Suite 100, San Diego, California, 92130, by phone at (858) 720-8900, and by fax at (858) 509-3691.

Petitioner consents to electronic service. All services and communications to the attorneys listed above may be sent to:

LegalTm-NetskopeFortinetII-IPRs@sheppard.com.

A Power of Attorney for Petitioner is being filed concurrently.

D. Fees

Petitioner paid the required fees. The Office is authorized to charge any fee deficiency, or credit any overpayment, to Deposit Account No. 50-4561.

III. IPR REQUIREMENTS—37 C.F.R. §42.104

A. Standing—37 C.F.R. §42.104

Petitioner certifies the '621 Patent is available for *inter partes* review (“IPR”), and Petitioner is not barred or estopped from requesting IPR on the grounds herein.

B. Challenged claims and relief requested

Petitioner respectfully requests cancellation of the challenged claims 1-3, 5-11, and 13-19 under §103 on grounds 1 & 2 below.

1. Challenged Claims

Claim Element	Claim language
1[pre]	A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising:
1[a]	gathering, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;
1[b]	gathering, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and
1[c]	identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.
2	The method of claim 1 wherein the first information is gathered from one or more identity providers.
3	The method of claim 1 wherein the first information is gathered from one or more applications of the one or more resources or of the providers.
5	The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.
6	The method of claim 1 further comprising directing the user to a remediation workflow in response to identifying the one or more shadow systems.
7	The method of claim 1 wherein the first information is not gathered from the one or more user devices.
8	The method of claim 1 wherein the second information is gathered via the one or more client applications including one or more proxy applications executed on the at least a subset of the one or more user

	devices.
9[pre]	A non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to:
9[a]	gather, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;
9[b]	gather, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and
9[c]	identify one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.
10	The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from one or more identity providers.
11	The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from one or more applications of the one or more resources or providers.
13	The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to generate an alert in response to identifying the one or more shadow systems.
14	The non-transitory computer readable storage medium of claim 9 wherein the instructions, when executed, further cause the processing device to direct the user to a remediation workflow in response to identifying the one or more shadow systems.
15	The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more resources or the providers of the one or more resources other than the one or more user devices.

16	The non-transitory computer readable storage medium of claim 9 wherein the second information is gathered via one or more proxy applications executed on the at least a subset of the one or more user devices.
17[pre]	A system comprising:
17[a]	a memory; and
17[b]	a processing device, operatively coupled to the memory, the processing device configured to:
17[c]	gather, from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;
17[d]	gather, from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources; and
17[e]	identify one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT) activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.
18	The system of claim 17 wherein the first information is gathered from one or more identity providers.
19	The system of claim 17 wherein the first information is gathered from one or more applications of the one or more resources or the providers of the one or more resources.

2. Prior art—Invalidity under 35 U.S.C. § 103

Petitioner relies on the references listed in the Table of Exhibits, including:

Prior Art
U.S. Patent Publication No. 2018/0288045 A1 (“Karunakaran”); published

October 4, 2018, and was filed on March 27, 2018 (claiming priority to March 29, 2017 provisional); prior art under at least 35 U.S.C. § 102(a)(1) and § 102(a)(2), Ex-1005.
--

<u>U.S. Patent Publication No. 2007/0220605 A1</u> (“Chien”); published September 20, 2007; prior art under at least 35 U.S.C. § 102(a)(1) and § 102(a)(2), Ex-1006.

<u>U.S. Patent Publication No. 2019/0199751 A1</u> (“Lipman”); published June 27, 2019, and filed December 21, 2017; prior art under at least 35 U.S.C. § 102(a)(1) and § 102(a)(2), Ex-1008.
--

The ’621 Patent is not entitled to the earliest alleged priority date identified on the face of the patent (November 27, 2017). As detailed below (§IV.B.2), the Challenged Claims are only entitled to an effective filing date of no earlier than June 9, 2022—the filing date of U.S. Patent Application 17/836,813, Ex-1017—which is the *only* application to which the ’621 Patent claims priority that includes the disclosure supporting the Challenged Claims (*i.e.*, starting at column 91 and going forward). Each piece of prior art has a publication date prior to the actual priority date of the ’621 Patent.

Declaration of Michael Franz (“Franz Decl.”), Ex-1003. Petitioner relies on the declaration of Dr. Michael Franz, a Distinguished Professor of Computer Science at the University of California, Irvine, whose research focuses on software systems, computer security, and trustworthy computing. Ex-1003, ¶¶6-7, 14-16.

Dr. Franz holds a Dr. of Science in Computer Science and a Dipl. Informatik-Ing. ETH degree, both from ETH Zurich. He is a Fellow of AAAS,

ACM, IEEE, and IFIP, and has authored numerous publications and awards. Ex-1003, ¶¶5, 8-13; Ex-1004.

3. Grounds

Petitioner requests *inter partes* review and cancelation of the challenged claims on the following grounds:

Ground	Basis	Reference(s)	Challenged Claims
1	§103	Karunakaran	1-3, 5-11, 13-19
2	§103	Chien and Lipman	1-3, 5-11, 13-19

4. No Discretionary Denial Factors Are Present

Petitioner submits that *inter partes* review is warranted here because, in addition to the claimed invention being known before the '621 Patent, there are no discretionary factors that weigh against review. For example:

- None of the prior art discussed herein was before the Examiner during prosecution.
- There are no settled expectations because the '621 Patent issued about 1.5 years ago (March 4, 2025), and has a priority date of no earlier than June 9, 2022 due to new matter added in a continuation-in-part application.
- No schedule is set, including no set trial date, in the parallel district court proceeding.

- Petitioner has not taken inconsistent positions on claim construction—indeed, claim construction proceedings have not begun in the parallel district court proceeding.
- Netskope is a U.S.-based cloud security company.

IV. TECHNOLOGY DESCRIPTION

A. Overview of the Underlying Technology Landscape

1. Audit Log Comparison

Before the alleged invention in 2022 (even as early as 2007), audit logging was a mature computer security practice, and a POSITA would have been aware of techniques for capturing access events across file systems, networks, authentication services, cloud resources, and databases. Ex-1006, *see e.g.*, ¶¶0018, 0033-0039, 0041-0045, 0047, 0050-0052, Figs. 3, 5; Ex-1005; Ex-1011; Ex-1012. By no later than 2007, a POSITA would have understood that audit logs were the primary framework for both real-time anomaly detection and forensic investigations of unauthorized accesses. Ex-1006. Likewise, it was well-known by no later than 2017 that such logging could occur at a resource or its provider, within user devices, or within client applications. *Id.*, Ex-1005; Ex-1007. By 2017, an entire industry—including UEBA and SIEM solutions—offered tools to analyze audit logs and detect anomalous behaviors, building on earlier static approaches such as

Snort (1999) (Ex-1013) and Suricata (2009) (Ex-1014), as well as shared threat intelligence (Ex-1009) and then-emerging machine learning. Ex-1003, ¶¶42-46.

2. Shadow Information Technology

Shadow information technology (IT) refers to any use of computer systems, devices, applications, or services within an organization without its IT department's approval. Ex-1007 at 6:55-7:25, 44:36-51; *see also* Ex-1024 at 1. The concept originated in the 1990s and gained relevance through “bring your own device” policies and “roaming” users accessing enterprise networks from remote locations. Ex-1024 at 1; Ex-1005, ¶0002. As Cisco observed in March 2016, “Shadow IT is not a new topic.” Ex-1015 at 1. By at least 2016, IT departments were alerting users to risks from unauthorized cloud storage, personal devices, and unmanaged messaging applications. Ex-1024 at 1; Ex-1005 at 1:24-48; Ex-1007 at 6:55-7:25, 44:36-51. Gartner's 2016 “Top 10 Security Predictions” listed shadow IT as its #2 prediction, recommending that companies “find a way to track shadow IT.” Ex-1016 at 1-2. In January 2017, U.S. Patent No. 10,237,294 to Zadeh (“Zadeh”) identified shadow IT as a significant challenge, illustrating the problem with unauthorized biomedical devices on a hospital network, and disclosed analyzing IT environment events to detect and address shadow IT. Ex-1007 at 6:55-67, 7:1-14. Thus, well before the alleged invention, a POSITA would have

understood that detecting shadow IT was based on analyzing audit logs to find discrepancies between expected and reported resource accesses. Ex-1003, ¶¶48-54.

B. The '621 Patent

1. Alleged invention

The Challenged Claims are equivalent to comparing two pieces of information and flagging mismatches. This is the kind of discrepancy check anyone might perform when reviewing a credit card statement or a checkbook against saved receipts. Any “discrepancy” should be flagged as an unauthorized transaction. The '621 Patent applies this same well-known logic to network security.

Figure 18 of the '621 Patent generally illustrates the Challenged Claims' process (color added): the green indicates gathering a full set of access information from a provider of resources (first information), blue indicates gathering the subset of authorized access from the client's perspective (second information), and yellow indicates the resulting discrepancy of unauthorized access when the two logs are compared.

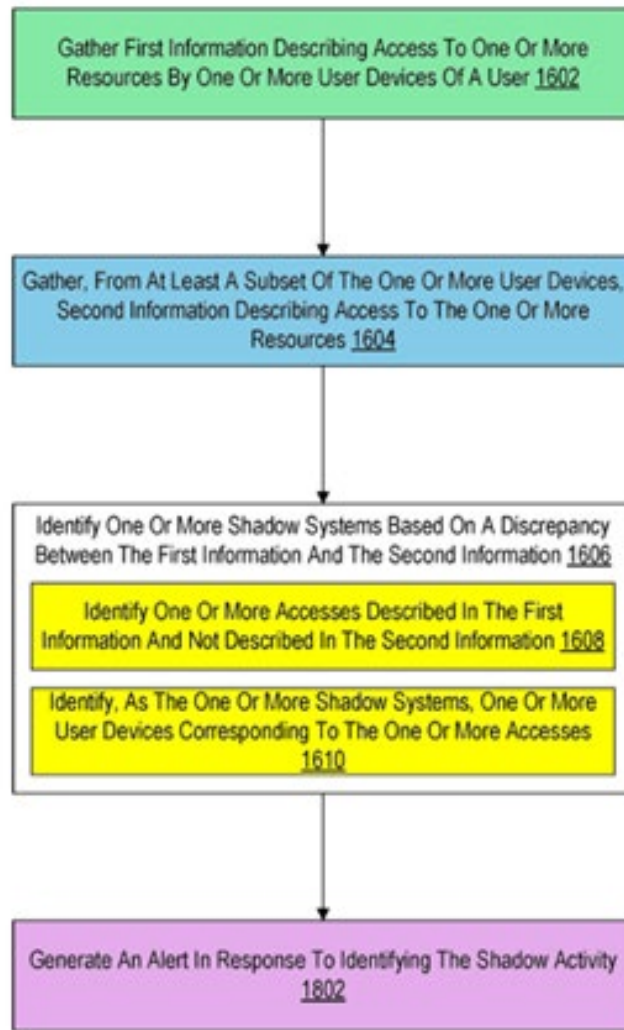


Fig. 18

Ex-1001, Fig. 18. Where an a discrepancy is detected, *e.g.*, an entry appears in the provider's log but has no corresponding entry in the client-side log, the system flags that device as a "shadow system"—a device accessing the resource outside the enterprise or organization's managed IT environment. Ex-1001 at 94:20-33,

98:20-100:34. If a discrepancy is found, the system may generate an alert or direct the user to a remediation workflow (represented in pink). Ex-1001 at 98:20-100:34; Ex-1003, ¶¶72-77. No particular hardware is disclosed for this process.

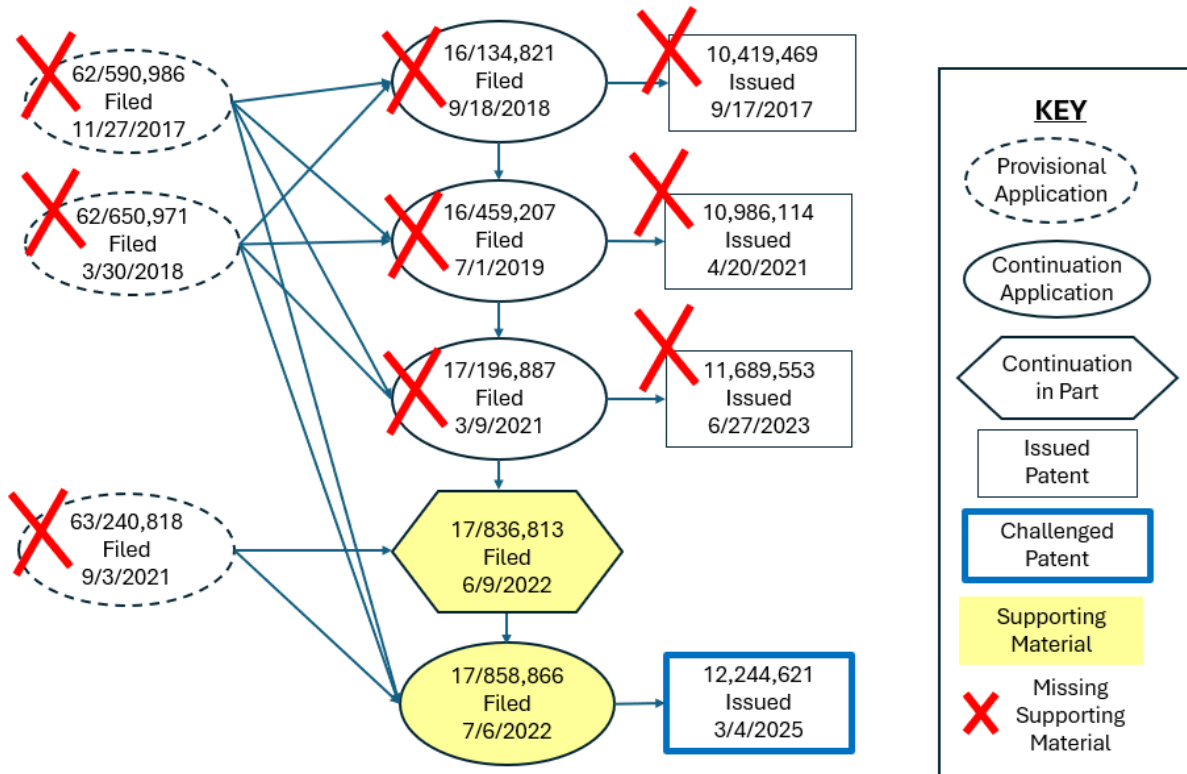
The '621 Patent specification and claims also reference a “proxy application” that both logs the resource access information and provides a redirecting proxy functionality. This proxy functionality is described as part of the client application (*i.e.*, an authorized application or part of an authorized application on a user device) that collects the second information in addition to redirecting the user’s network traffic through the managed application. Ex-1001 at 93:40-48; Ex-1003, ¶78.

Although the '621 Patent specification spans over 100 columns and almost 60 pages of figures, only columns 91-98 and Figures 16-19 describe the methods underlying the Challenged Claims. As discussed below, this material first appeared in the continuation-in-part application filed on June 9, 2022 (No. 17/836,813, now abandoned).

2. Effective Filing Date of the Challenged Claims

The examiner relied on the priority date printed on the face of the patent without examining the priority chain. Ex-1002 at 178 (Feb. 1, 2024 Office Action (reciting the priority date of November 27, 2017)). The '621 Patent claims priority

as a continuation to U.S. Patent Application No. 17/836,813, filed June 9, 2022 (now abandoned) (Ex-1017), which claimed priority as a ***continuation-in-part*** to application No. 17/196,887, filed on Mar. 9, 2021, now Pat. No. 11,689,553 (Ex-1018), which is a continuation of application No. 16/459,207, filed on Jul. 1, 2019, now Pat. No. 10,986,114 (Ex-1019), which is a continuation of application No. 16/134,821, filed on Sep. 18, 2018, now Pat. No. 10,419,469 (Ex-1020). The '621 Patent also claims priority to provisional applications 63/240,818, filed on September 3, 2021 (Ex-1023), 62/650,971, filed on Mar. 30, 2018 (Ex-1022), and 62/590,986, filed on Nov. 27, 2017 (Ex-1021). The Family Tree for the '621 Patent is illustrated below.



'621 Patent Claimed Priority Applications Family Tree

Two versions of a redline comparison were prepared, for demonstrative purposes, of the first filed/issued patent in the family, the '469 Patent (Ex-1020) and the '621 Patent (Ex-1001). Ex-1025, Ex-1026. The first is a comparison of the PDFs for the '469 Patent and the '621 Patent. Ex-1025. The second is a text-only comparison of the specifications extracted from Google Patents, shown as a Word redline. Ex-1026. Notably, the same comparison generally applies to the '114 Patent (Ex-1019) and the '553 Patent (Ex-1018) because, as continuation applications, they share the same specification as the '469 Patent. These comparisons confirm that the '621 Patent specification replaced a significant

portion of the '469 Patent specification with completely new material and adding new figures (*e.g.*, Figs. 16-19). *See e.g.*, Ex-1025 at 70-73, 106-112, 114-125; Ex-1026 at 2-9, 69-104. In addition to a portion at the beginning of the specification, the material starting at least at column 61, all the way through to the end at column 98, line 17 is ***all new material*** for the '621 Patent. *See* Ex-1025 at 106-124; Ex-1026 at 69-104; Ex-1003, ¶¶27-33.

The written description requirement under 35 U.S.C. § 112(a) demands that the specification of the earlier priority applications must convey to a POSITA that the inventor possessed the full scope of the claimed invention as of that earlier filing date. *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1571-72 (Fed. Cir. 1997). “When neither the PTO nor the Board has previously considered priority, there is simply no reason to presume that claims in a [continuation-in-part] application are entitled to the effective filing date of an earlier filed application.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1380 (Fed. Cir. 2015).

The Challenged Claims recite multiple limitations that were not disclosed by the patent owner until the filing of the June 9, 2022 priority patent application No. 17/836,813. Ex-1017. For example, as illustrated in Figure 18 and discussed further below, each independent claim requires at least (1) a multiple-source

architecture providing information related to users accessing resources—one from the resource provider perspective and one from the client perspective, (2) gathering of the resource access information from the multiple sources, (3) a comparison of the data gathered from the multiple sources, and (4) a detection of shadow IT based on a discrepancy between the two sources of data. Ex-1001 at the claims and 98:20-100:34, Fig. 18. The system and/or method for gathering resource access information from multiple sources, and performing a discrepancy comparison to detect “shadow IT,” was not disclosed until columns 91:53-98:16 and Figs. 16-20 of the ’621 Patent. *Compare* Ex-1001 and Ex-1017 *with* Ex-1018—Ex-1023. However, the Examiner never considered whether the priority applications provided written description for the ’621 Patent claims—neither the original claims nor as amended. Ex-1002 at 178 Ex-1003, ¶32.

More specifically, in the second narrowing of the claims (on September 12, 2024, discussed below), the patent owner narrowed *each* independent claim to include “*wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.*” Ex-1002 at 72 (amended claim 1), 74 (amended claim 9), and 76 (amended claim

17) (Request for Continued Examination, Sept. 12, 2024 (66-82)). The patent owner supported the inclusion of this element by citing to only the “Specification [0792],” which is found in the issued patent (Ex-1001) at 94:42-59. Ex-1002 at 78. None of this material was included in the alleged priority applications until the June 9, 2022 filing of U.S. Patent Application 17/836,813 (now abandoned).¹ Ex-1018—Ex-1023; Ex-1003, ¶¶32, 33.

To the extent that the Patent Owner points to U.S. Provisional Application 63/240,818, filed 9/3/2021 as support for the ’621 Patent claims because it mentions “shadow” once (Ex-1023 at 0032 (“NSaaS includes activity visibility to uncover shadow IT”)), the single mention of the term does not support the ’621 Patent claims. Even if aspects were mentioned or it may be possible to infer certain elements were obvious from the prior material, “[o]bviousness simply is not enough; the subject matter must be disclosed to establish possession.” *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1310 (Fed. Cir. 2008). Because no such disclosure existed until the June 9, 2022 filing (Ex-1017), the ’621 Patent’s effective filing date is no earlier than June 9, 2022. Even if that provisional application were found to provide adequate written description support for the

¹ The yellow highlighted boxes in the Family Tree illustrated above indicates the only two patent applications with the allegedly supporting material.

Challenged Claims, the prior art relied upon in Grounds 1 and 2 was published well before September 3, 2021, and the analysis would not change. Because the prior art references Karunakaran, Chien, and Lipman Petitioner identifies under grounds 1 and 2 predate the Challenged Claims actual priority date, the burden shifts to the patent owner to produce evidence that Challenged Claims are entitled to an earlier priority date. *Guest Tek Interactive Ent. Ltd. v. Nomadix, Inc.*, No. IPR2019-01191, 2019 WL 7212601, at *6-7 (P.T.A.B. Dec. 27, 2019); Ex-1003, ¶¶27-33.

3. Prosecution history

The claims were narrowed twice during prosecution. None of the prior art cited by the Examiner—Giokas (US 20150033340), Di Pietro (US 20160028753), or Cudak (US 20170310701)—is relied upon in this Petition, and none of those references is the same as or materially similar to the prior art presented here. Ex-1002 at 176-196, 83-96; Ex-1003, ¶¶34-38. The Examiner never considered the improper claim to the November 27, 2017 priority date, and thus, was unable to find art similar to Karunakaran or Lipman. Ex-1002 at 178.

In September 2024, the applicant filed a Request for Continued Examination and amended each independent claim to require that: (a) the first information be gathered “from one or more resources or providers of the one or more resources”;

(b) the second information be gathered “from one or more client applications of at least a subset of the one or more user devices”; and (c) the identification of shadow systems specifically comprise finding accesses “described in the first information but not described in the second information” and flagging the corresponding user devices as shadow systems. Ex-1002 at 72-76 (Request for Continued Examination, Sept. 12, 2024); Ex-1003, ¶37.

According to the Notice of Allowability, the Examiner relied on the claims based on the dual-perspective comparison/discrepancy and that an access appearing only in the first information, but not in the second information, indicates the user device circumvented the authorized client application—*e.g.*, shadow IT activity. The Examiner found that none of the cited prior art taught this resource-side versus client-side (dual-perspective) discrepancy framework, and allowed the amended claims. Ex-1002 at 25-30 (Notice of Allowability, Oct. 29, 2024 (23-32)); Ex-1003, ¶38.

V. LEVEL OF ORDINARY SKILL

A POSITA at the time of the alleged invention would have had at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and at least two years of work or research experience in the field of networking with exposure to network security issues.

Work experience can substitute for formal education and vice versa. Ex-1003, ¶¶24-26.

VI. CLAIM CONSTRUCTION

Petitioner has applied the claim terms' ordinary meanings as understood by a POSITA, which are consistent with the explanations provided in the specification and in the prosecution history.² 37 C.F.R. §42.100(b). For example, "shadow system" is described in the specification as "user devices engaging in 'shadow information technology (IT)' as would be appreciated by one skilled in the art, whereby access to a resource is performed outside of the operational control of an IT department." Ex. 1001, 94:21-25. The terms "shadow system" and "shadow IT" were well-known in the art at the time the '813 Application was filed in 2022, and the description provided in the specification falls within the plain and ordinary meaning as used in the industry at the time. Ex-1003, ¶40. The use of other certain technical terms in the context of the specification and claims are discussed below.

VII. SPECIFIC GROUNDS

A patent is invalid as obvious under Section 103 based on a single reference, or by combining references where there is a motivation to combine and a

² Petitioner reserves the right to respond to PO/Board constructions.

reasonable expectation of success. Petitioner reserves the right to address any secondary considerations Patent Owner may raise.

A. Ground 1: Karunakaran Renders Claims 1-3, 5-11, and 13-19 Obvious.

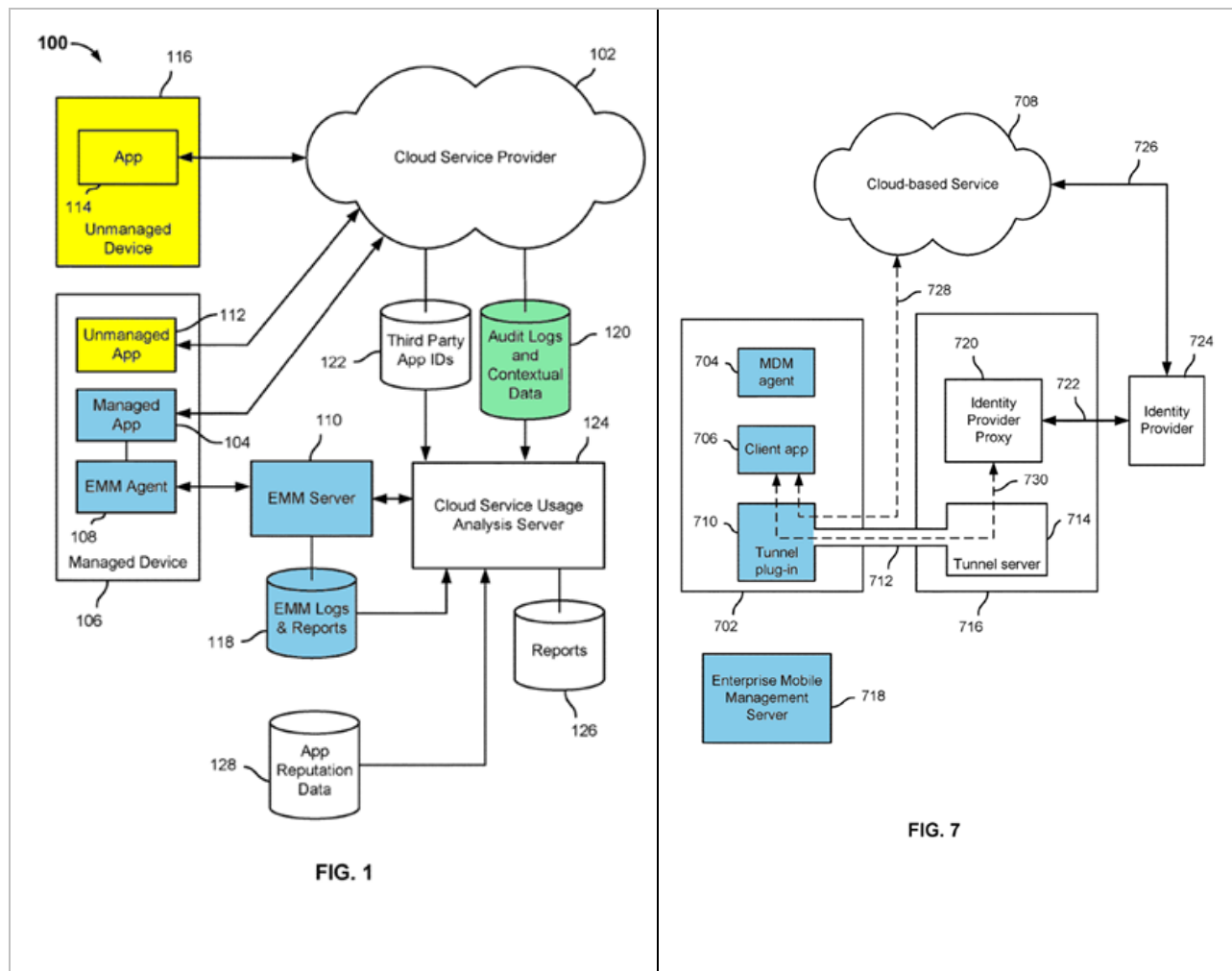
1. Overview of Karunakaran

Karunakaran addressed the Bring-Your-Own-Devices security challenge: “Unlike traditional desktop and other computers, which are managed and typically owned by the corporation, *mobile devices are typically owned by the employee (e.g., ‘bring your own device’ or BYOD)*. Even when the mobile device is managed by the Enterprise using an Enterprise Mobility Management (EMM) solution like that of Mobileiron®, *the applications that the employee uses to access the Cloud Services may not be a ‘sanctioned’ application.*” Ex-1005, ¶0002.

Karunakaran’s system is directed to solving this problem by implementing an Enterprise Mobility Management (“EMM”) Solution on a client/employee’s managed device 106 that logs resource access information through the EMM Solution and compares the EMM log 118 to cloud service provider’s 102 resource access logs 120. Through this comparison, Karunakaran’s system detects unauthorized access to enterprise cloud resources (*i.e.*, access that is performed outside of the operational control of an IT department)—the same dual-perspective

comparison/discrepancy framework that the '621 Patent Examiner had not found in the prior art. *See supra* §IV.B.3 (Ex-1002 at 25-30). Ex-1005, Abstract, ¶¶0002, 0015-0017, 0025, 0039, 0086, 0090, Figs. 1, 3, 7; Ex-1003, ¶¶59-78.

As shown in Figures 1 and 7 below, the first source of resource access information is provided by the cloud service provider 102, which generates and stores the “audit logs and contextual data 120,” (herein “audit log 120”, *see also* Fig. 4, log 400). Ex-1005, ¶¶0016, 0018, 0022, 0027; Fig. 1; Ex-1003, ¶¶62-69, 82.



Ex. 1005, Figs. 1 and 7.

Each audit log 120 entry captured “who logged into the service using which application and *from where and at what time, and in some cases with which device.*” Ex-1005, ¶0018. As seen in Figure 4, this included “for each access (e.g., login/attempt) . . . a date/time stamp, a user (e.g., username, display name, etc.) . . . a device type and/or identifier, a user email address, an IP address, an action (e.g., login, used new app to log in, etc.)” Ex-1005, ¶0049, Fig. 4. This confirmed the cloud service provider 102 also authenticated users and logged login/authentication events and failed login attempts. Ex-1005, ¶¶0027, 0049, Figs. 1, 4; Ex-1003, ¶¶65-70, 74, 82, 88-92.

The second source of access information is from the client/device side: the EMM Solution (comprising the EMM Agent 108 installed on managed user devices, and the EMM Server 110) that generates and stores EMM logs and reports 118 for each managed device. Ex-1005, ¶¶0026, 0050; Ex-1003, ¶¶63-65, 70-71, 83. These records include, for example, “identifying each *enterprise user and that user’s enterprise identity, associated device(s), app(s)*, etc.; records containing data for each managed device, including device type, *unique identifiers*, installed apps, *device location*, etc.; and *logs of cloud service access activity via managed and/or observed nodes or resources . . . including for each access event an*

identification of one or more of the user, device, and app involved in the event.”

Ex-1005, ¶¶0029, 0050, Fig. 5.

Karunakaran also disclosed integrating onto a mobile device 702 a tunnel plug-in 710 with the client application 706 and mobile device management agent 704 (“MDM Agent,” similar to an EMM Agent 108), all brought under management by the EMM Server 718. Ex-1005, ¶¶0094-0096, Fig. 7. The tunnel plug-in 710 is configured to work with the client app 706 “to *selectively direct traffic* associated with client app 706” to either the cloud-based service 708 or the security proxy server 716 (*i.e.*, acts as a proxy application). Ex-1005, ¶¶0094-0096, 0105, Fig. 7; Ex-1003, ¶¶69, 78, 97-98.

A cloud service usage analysis server 124 ingests both data sources (audit logs 120 and EMM logs 118), maps and normalizes the data to a common schema, and correlates the data. Ex-1005, ¶¶0028, 0033, 0034. The correlated data includes, for example, *user identity* (username, email, etc.) and *application identity* (*e.g.*, among multiple applications), timestamps, location. Ex-1005, ¶0034. Karunakaran disclosed that the correlated data was analyzed to, among other things, “[i]dentify *users who are accessing SP from mobile, but who do not have a device registered with EMM*” and “[d]etermine Apps which are sanctioned (configured in EMM to

be managed) vs. *unsanctioned for each SP.*” Ex-1005, ¶¶0037, 0039; Ex-1003, ¶¶63-66, 72-74, 84-87.

Karunakaran’s system generated alerts “when any of the above . . . matches certain conditions or exceeds a configured threshold,” and took responsive action including blocking unmanaged devices, quarantining unsanctioned apps, and migrating users to managed apps. Ex-1005, ¶¶0019, 0046, 0053-0054, Fig. 6. Karunakaran’s process at 202 is directed to identifying and blocking, based on a discrepancy in the audit logs 120 and EMM logs 118, specific instances of applications or devices accessing enterprise cloud service resources outside the operational control of the enterprise’s IT. Ex-1005, ¶¶0032, 0054; Ex-1003, ¶¶75-77, 94-95.

Where the disputed claim elements are disclosed together in a single embodiment of a single reference, no separate showing of motivation to combine or reasonable expectation of success is required. *See Gen. Elec. Co. v. Raytheon Techs. Corp.*, 983 F.3d 1334, 1352 (Fed. Cir. 2020); *see also Guardant Health, Inc. v. Univ. of Wash.*, No. 2024-1129, 2026 WL 184334, at *1, *4–5 (Fed. Cir. Jan. 23, 2026) (nonprecedential). Nonetheless, Karunakaran’s “embodiments are illustrative and not restrictive,” (Ex-1005, ¶0113) and are predictable variations of each other. Combining like-embodiments (*e.g.*, the EMM agent 108 and the MDM

agent 704) or combining functionally separate components into a single client application (e.g., the MDM Agent 704 and tunnel plug-in 710) requires only ordinary skill. *See Bos. Sci. Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (Fed. Cir. 2009); Ex-1003, ¶¶62, 78, 97–98.

2. Claims 1, 9, and 17

- a. 1[pre]: “A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising” (See 9[pre] and 17[pre]/[a]/[b] below)**

To the extent the preamble is limiting, Karunakaran disclosed or rendered obvious this limitation by identifying unmanaged applications 112, 114 and unmanaged devices 116 (*shadow systems*), using multiple data sources including audit logs 120 from the cloud service provider 102 (*first source*) and EMM logs 118 from the EMM agent 108 (*second source*). *See e.g.* Ex-1005, Abstract, ¶¶0002, 0015-0017, 0024-0029, 0032-0037, 0049-0054, 0094-0096, Figs. 1, 3, 4-8; Ex-1003, ¶¶40, 48-54, 59-63, 79-80.

Karunakaran’s system was directed to the same problem and solution disclosed in the ’621 Patent of detecting unauthorized access in an enterprise to cloud service resources or “shadow systems.” *See* Ex-1005, Abstract. Although the term “shadow system” is not used, Karunakaran’s system was configured to detect

the functional equivalent to “shadow IT”³—detecting unmanaged applications 112, 114 and unmanaged devices 106, “e.g., a device not under management of an EMM solution used by the enterprise, and/or an unmanaged mobile app.” Ex-1005, ¶0016, *see also* Abstract, ¶¶0002, 0024. A POSITA would have understood, given Karunakaran’s disclosure of “BYOD” security risks (*see* Ex-1005, ¶0002), that detecting unmanaged device 116 and unmanaged app 112, 114 was equivalent to detecting a “shadow system” as claimed in the ’621 Patent. Ex-1003, ¶¶40, 48-54.

To identify the shadow systems, Karunakaran gathered and correlated logs from multiple sources that provided the access information from different perspectives, including from (1) the audit logs and contextual data 120 storage (*e.g.*, data captured by the cloud service provider 102, *e.g.*, “cloud service provider audit log 400”) (Ex-1005, ¶0049) and (2) the EMM logs and reports 118 storage (*e.g.*, data captured from the EMM agent 108 and EMM server 110, *e.g.*, “mobile device app inventory 500”) (Ex-1005, ¶0050). Ex-1005, ¶¶0016-0017, 0024-0029, 0032-0037, 0049-0054, Figs. 1, 3, 4-8. Because the data from the two sources needed to be “mapped and normalized” (Ex-1005, ¶¶33-34, Fig. 3) before the logs

³ Zadeh’s discussion of shadow systems confirms Karunakaran’s unmanaged devices and apps engaged in the unauthorized use of organizational resources are shadow systems. Ex-1007, 6:55–67; Ex-1003, ¶¶40, 48-54.

could be “correlated,” a POSITA would have understood these logs came from different perspectives—but could be compared to detect any discrepancies. Ex-1003, ¶¶59-66, 80, 84.

- b. 9[pre] / 17[pre], 17[a], 17[b]: “A non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to” / “A system comprising: a memory; and a processing device, operatively coupled to the memory, the processing device configured to”

Karunakaran disclosed or rendered obvious this limitation because Karunakaran described the hardware used for implementing the system, including *e.g.*, the cloud service usage analysis server 124 and EMM logs & reports 118, audit logs and contextual data 120 (equivalent to “*non-transitory computer readable storage medium storing instructions*,” “*memory*,” and “*processing devices*”): “[t]he invention can be implemented in numerous ways, including . . . *a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor*. . . . As used herein, the term ‘*processor*’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.” Ex-1005, ¶0014; Figs. 1, 7; Ex-1003, ¶¶62, 65-67, 81.

- c. **1[a] / 9[a] / 17[c]: “gathering [or gather], from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;”**

Karunakaran disclosed or rendered obvious this limitation because the cloud service provider 102 generated resource access data stored in an audit log 120/400 (*first information*) for each access event and every user device (*one or more user devices of a user*), which is ingested (*gathered*) by the cloud service usage analysis server 124. Ex-1005, ¶¶0016, 0018, 0022, 0027-0028, 0033-0034, 0049, Figs. 1, 3, 4; Ex-1003, ¶¶62-65, 67, 82.

The Challenged Claims uses the terms “resources,” “providers,” and “application,” which are used throughout the ’621 Patent specification to refer to a variety of software functionality, cloud services, and service endpoints. Ex-1001; Ex-1003, ¶82. The cloud service providers 102 in Karunakaran employ, for example, server-side applications, such as “Office365, Box, Salesforce, Slack, etc. for their productivity, collaboration and business application workloads,” that provide or one or more resources. Ex-1005, ¶0002. Karunakaran disclosed that the “enterprise class Cloud Service Providers [102] provide *audit logs and contextual data* [120] *which contain information such as who logged into the service using which application and from where and at what time, and in some cases with*

which device.” Ex-1005, ¶0018, *see also* ¶¶0027, 0028, 0032-0033. Exemplary audit log 400 data “includes for each access (e.g., *login/attempt*) . . . a *date/time stamp, a user* (e.g., *username*, display name, etc.) . . . a device type and/or identifier, a user email address, an IP address, an action (e.g., login, used new app to log in, etc.).” Ex-1005, ¶0049, Fig. 4. The cloud service usage analysis server 124 ingests (gathers) these audit logs 120/400 (first information) at step 302 of Figure 3 and correlates them with the EMM logs 118/500 to “generate cloud service usage reports 126 . . . [that] may include data indicating and/or summarizing instances of cloud service access using *unmanaged devices and/or apps.*” Ex-1005, ¶¶0028, 0033-0034, Figs. 3, 4; Ex-1003, ¶¶62-65, 67, 73 82.

d. 1[b] / 9[b] / 17[d]: “gathering [or gather], from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources;”

Karunakaran disclosed or rendered obvious this limitation because Karunakaran’s EMM agent 108 (*client application*) is installed on a set of enterprise users or managed devices 106 (*subset of the one or more user devices*), wherein the EMM agent 108 captures resource access data in an EMM log 118 (*second information*) that is ingested into (*gathered* by) the cloud service usage analysis server 124. Ex-1005, Abstract, ¶¶0016-0017, 0022-0023, 0026, 0028, 0033, 0049, 0050, 0051, 0054, Figs. 1, 3, 5; Ex-1003, ¶¶63-65, 70-71, 83.

Karunakaran also described the MDM agent 704, client app 706, and tunnel plug-in 710, on a mobile device 702 with the EMM Server 718 (together “client application”) as a similar EMM solution capturing the same information. Ex-1005, ¶¶0094-0095, Fig. 7; Ex-1003, ¶¶69, 78, 97-98.

Karunakaran described the “managed app 104 [as] managed in part by a native or other EMM agent 108 on the device 106. *The EMM agent 108 in this example has been brought under management by an EMM solution that includes EMM server 110.* . . In some embodiments, the *EMM agent 108 may be a component and/or service of the device operating system.*” Ex-1005, ¶0022, Fig. 1. The EMM Solution generated EMM logs and reports 118 or mobile device app inventory 500. Ex-1005, ¶0050, Fig. 5.

500 ↗

App ID	Inventory ID	App Name	Platform Type	Version	VPN Name	Status

FIG. 5

Id.

Additionally, the EMM solution logged information similar to the that of the audit log 120/400, but from a different perspective, in the EMM log 118/500, which “include[d] one or more of the following: records identifying each enterprise user and that *user’s enterprise identity*, associated device(s), *app(s)*, etc.; records containing data for each managed device, including device type, unique identifiers, *installed apps, device location*, etc.; *and logs of cloud service access activity via managed and/or observed nodes or resources, . . . including for each access event an identification of one or more of the user, device, and app* involved in the event.” *Id.*, ¶¶0026, *see also* ¶¶0050-0051. Thus, the EMM log 118/500 described, from the subset of managed client/user’s perspective, the users’ access to one or more resources accessed through the cloud service provider 102. Ex-1003, ¶¶63-65, 70-71, 83.

Once this EMM log 118/500 is built, this “second information” is ingested into (or gathered by) the cloud service usage analysis server 124, and is mapped and normalized for and correlation with the cloud service data 120 (step 302 of process 202) to identify unmanaged devices or applications. Ex-1005, Figs. 1, 3, and 5, ¶¶0033, 0050, 0051, 0054, 0085-0090.

- e. **1[c] / 9[c] / 17[e]: “identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of**

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

Karunakaran disclosed or rendered obvious this limitation because Karunakaran disclosed (1) identifying a *subset* of an enterprise’s users with unmanaged devices 116 and unmanaged applications 112, 114 (*shadow system*), (2) identifying the unmanaged systems based on a correlation (a *discrepancy*) by the cloud service usage analysis server 124, where access data is logged (*described*) in the audit logs 120/400 (*first information*) but is not logged (*not described*) in the EMM logs 118/500 (*second information*); and (3) based on the discrepancy, identifying user devices corresponding to those unmatched accesses is an unmanaged device or app 116, 112, 114 (*one or more shadow systems, one or more user devices corresponding to the one or more accesses not described in the second information*) for blocking individual applications or devices (e.g., process 606). Ex-1005, ¶¶0002, 0016-0017, 0019, 0024-0025, 0032-0039, 0054, 0062, 0065, 0077-0080, 0083-0086, 0090, Figs. 1, 4, 5, 6; Ex-1003, ¶¶48-54, 59-66, 72-74, 84-87.

Identifying a Shadow System: As described above in §§ IV.A.2, VII.A.1 and VII.A.2.a, Karunakaran’s managed devices 106 running managed app 104 were registered with the EMM Solution (under the organization’s IT control), while unmanaged devices 116 and applications 112, 114 accessed the cloud service provider 102 outside the EMM Solution (or outside of the organization’s IT control). Ex-1005, ¶¶0022-0026, Fig. 1. Because the EMM solution did not log access by unmanaged devices/applications (which is a subset of all user devices in the enterprise), a POSITA would have understood that detecting unmanaged device 116 and unmanaged app 112, 114 is equivalent to detecting a “shadow system.” See Ex-1005, ¶¶0002, 0035 (“Determine the percentage of Users who are using a managed vs. unmanaged device to access an SP using an App.”), ¶0090 (“There are 5 executive level users (out of 10) using the unsanctioned ShareVault application.”); Ex-1003, ¶¶74-80, 84-85.

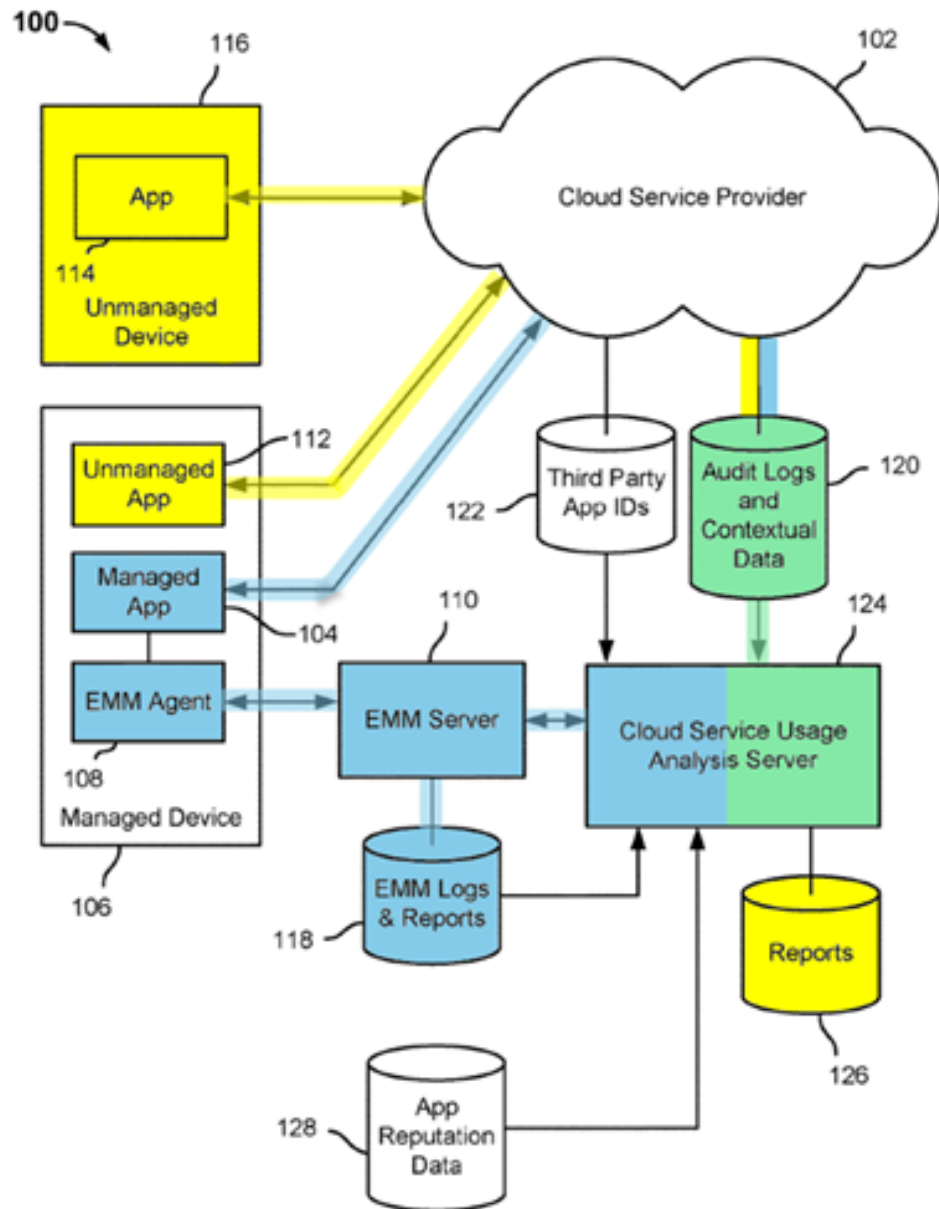


FIG. 1

Ex-1005, Fig. 1.

Discrepancy: Both the unmanaged devices/applications 112, 114, 116 as well as the managed devices/applications 104 and 106 access to enterprise

resources are logged by the cloud service provider 102 in audit log 120/400 (green for the first information), but the EMM agent 108/EMM Server 110 logged only the access of the *managed* devices/applications 104 and 106 in the EMM log 118/500 (blue for the second information). *See* Ex-1005, ¶¶0022-0026. Thus, after Karunakaran's system mapped and normalized the audit (120/400) and EMM logs (118/500) in process 202 to correlate the data (steps 302, 304, 306), the correlation would reveal a discrepancy (yellow for shadow IT), such as “[identifying] users who are accessing SP from mobile, but who do not have a device registered with EMM.” Ex-1005, ¶¶0002, 0016, 0022-0025, 0032-0037, Figs. 2-5; Ex-1003, ¶¶74-77, 84-86.

A POSITA would understand that identifying users who, for example, appear in the cloud service provider audit log 120/400 but who “do not have a device registered with EMM” (so do not appear in the EMM log 118/500), is identifying accesses described in the first information but not described in the second information, and is thus based on a discrepancy. Ex-1005, ¶¶ 00035-0050, Figs. 4 and 5; Ex-1003, ¶¶74-77, 86-87.

Karunakaran confirmed this discrepancy-based identification with an example. In an enterprise with 1000 users, the system determined from the Box SP logs (first information) that “150 users *not in EMM have used official Box app*

(most likely from an unmanaged mobile device)” and “50 users *not in EMM have used unsanctioned Box app* ‘ShareVault’ app (also most likely from an unmanaged mobile device).” Ex-1005, ¶¶0085, 0086; *see also* ¶0090 (“There are 5 executive level users (out of 10) using the unsanctioned ShareVault application.”); Ex-1003, ¶¶74-77, 79, 94-95.

Specific User Devices Engaging in Shadow Systems: Karunakaran’s remediation actions confirm that specific devices (*one or more user devices corresponding to the one or more [missing] accesses*) are identified through the unmatched access data in audit log 120/400 compared to the EMM log 118/500, because “in the case of access by one or more unmanaged device(s) 604, *access* to the cloud service by *that device* is *blocked* 606.” Ex-1005, ¶0054, Fig. 6; Ex-1003, ¶¶75-77, 94-95.

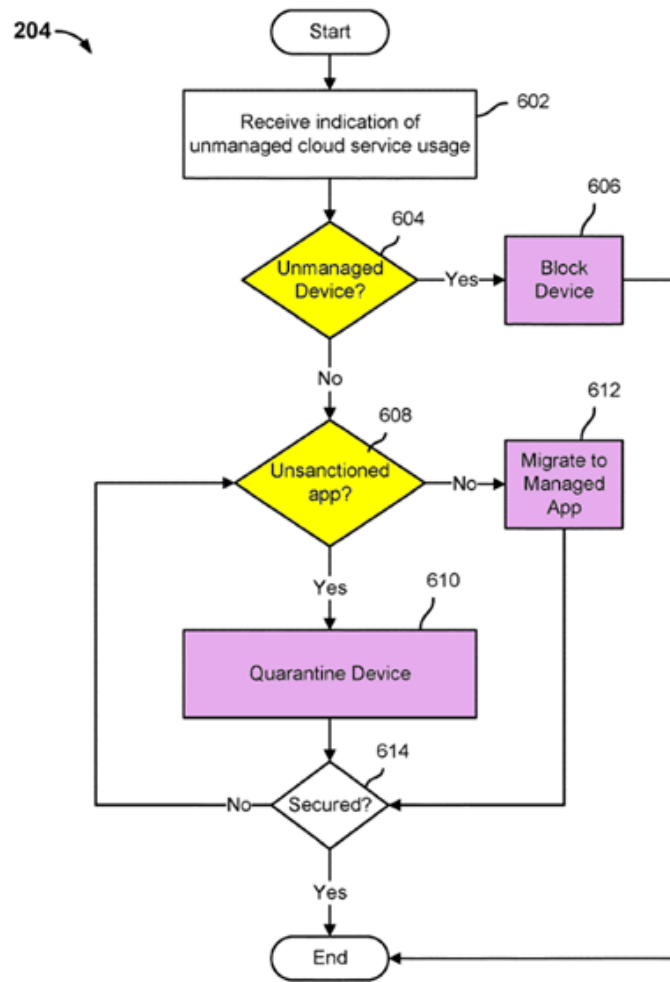


FIG. 6

Ex-1005, Fig. 6.

To block “that device,” Karunakaran’s system would have to first identify the specific device or application from the audit log 120/400 access data. Ex-1005, ¶¶0054, 0019 (actions include “blocking one or more users, blocking one or more apps”). The risk score factors further confirm device-level granularity, including

“geographic location of the users/devices” and “type of device used.” Ex-1005, ¶¶0062, 0065; Ex-1003, ¶¶84-87.

3. Claims 2, 10, and 18

2 [“The method of claim 1”] / 10[“The non-transitory computer readable storage medium of claim 9”] / 18 [“The system of claim 17”] . . . “wherein the first information is gathered from one or more identity providers.”

Karunakaran disclosed or rendered obvious the claim limitations of claims 1, 9, and 17, as seen above, and the remaining limitations because the cloud service provider 102 contained *identity provider* functionality that verified a user’s identity and gathered user device access information to *one or more resources* for inclusion in the audit log 120/400 (*first information*). Ex-1005, ¶¶0016, 0022, 0035-0037, 0049; Ex-1003, ¶¶67-70, 89-92.

As explained above in §VII.A.2.c, the Challenged Claims and specification use the term “provider” in various ways. For example, the ’621 Patent describes an identity provider as a resource, service, or a server-side application that a user logs *into* to verify a user’s identity that also gathers information including and *IP address, location information*, and *other device*-identifying information. Ex-1001, 92:52-93:2, Ex-1003, ¶¶82, 88.

Since many cloud service providers offer both their own local identity verification (by which a user can log in using credentials dedicated to that service) while simultaneously allowing access via federated or single-sign-on schemes, a POSITA would have understood that the term “identity provider” encompasses at least a single-resource identity provider and/or a centralized or federated identity provider. Ex-1003, ¶¶89-92. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (a more narrow embodiment disclosed in the specification does not limit claim language absent lexicography or disavowal). Given that claims 2, 10, and 18 rely on independent claims 1, 9, and 17, which require gathering “information describing access to the *one* or more resources by *one* or more user devices of a user,” Karunakaran’s cloud service provider 102 that verified a user’s identity and gathered user- and device-identifying information for at least one resource met this requirement. Ex-1005, ¶0002 (implementing “Cloud Service Providers (SPs) like Office365, Box, Salesforce, Slack, etc. for . . . collaboration and business application workloads.”), 0022; Ex-1003, ¶¶59, 89-92.

Karunakaran’s cloud service provider 102 required users to enter “*enterprise credentials* (e.g., username and password)” to access the cloud service provider 102. Ex-1005, ¶0022. Moreover, the audit log 120/400 recorded “*login sessions for a user*”—including failed login attempts—not merely recorded resource usage.

(Ex-1005, ¶0049, Fig. 4 Ex-1005, ¶0016). Logging of unsuccessful login attempts further indicates that the cloud service provider 102 is performing identity verification through an integrated server-side application or service, as a separate SSO-based identity provider would not typically relay such information back to the service provider. Ex-1003, ¶92. The audit log 120/400 further captured for each access a date/time stamp, *username*, *user email address*, *IP address*, and action type. Ex-1005, ¶0049, Fig. 4. A POSITA would have recognized that logging login sessions and authentication credentials tied to each login is the hallmark of an identity provider as described in the '621 Patent. *See* Ex-1001 at 92:60-93:2; *see also* Ex-1005, ¶¶0035, 0037; Ex-1003, ¶¶67, 88-92.

Notably, although Karunakaran's Figure 7 shows a separate Identity Provider 724 and Identity Provider Proxy 720, the specification does not require the IdP be separate. Ex-1005, Fig. 7. Moreover, Figure 7 shows a direct pathway from the MDM Agent 704/client application 706/tunnel plug-in 710 to the cloud-based service 708—without passing through the separate Identity Provider 724—further supporting that the cloud service provider 102/708 itself provides the functions of an identity provider in some instances. Ex-1005, Figs. 1, 7; Ex-1003, ¶98.

4. **Claims 3, 11, and 19**

3 [“The method of claim 1”] / **11** [“The non-transitory computer readable storage medium of claim 9”] . . .
“wherein the first information is gathered from one or more applications of the one or more resources or of the providers.”

19: “The system of claim 17 wherein the first information is gathered from one or more applications of the one or more resources or the providers of the one or more resources.”

Karunakaran disclosed or rendered obvious the claim limitations of claims 1, 9, and 17 as seen above and the remaining limitation because the cloud service provider 102 performed the identity verification function (*application of the one or more resources or of the providers*) and logged resource access information in the audit log 120/400 (*first information*).

As described above in §VII.A.3, Karunakaran’s cloud service provider 102 is a provider of resources whose authentication function verifies the identity of users, *e.g.*, it functions as both an “identity provider” (satisfying claims 2, 10, 18) and a server-side software “*application[] of the one or more resources or of the providers*” (satisfying claims 3, 11, 19). Moreover, as described above, the same authentication function also generates the audit logs 120/400 (*i.e.*, the *first information*)—which is another function or server-side application. Thus, Karunakaran’s cloud service provider 102 disclosed or rendered obvious these claims.. Ex-1005, ¶¶0018, 0034, 0049; Ex-1003, ¶¶82, 88-93.

5. Claims 5 and 13

5: “The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.”

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

Karunakaran disclosed or rendered obvious the claim limitations of claims 1 and 9 and the remaining limitation because Karunakaran disclosed generating an *alert* when the cloud service usage analysis server 124 *identifies* unmanaged devices 116 and unmanaged applications 112, 114 (*shadow systems*). Karunakaran’s system is configured to “[g]enerate an Alert when any of the above . . . matches certain conditions or exceeds a configured threshold.” Ex-1005, ¶¶0035-0048, 0055-0066, 0071; Ex-1003, ¶¶75-77, 94.

6. Claims 6 and 14

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

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

Karunakaran disclosed or rendered obvious the claim limitations of claims 1 and 9 as seen above and the remaining limitation because Karunakaran directed the

user to “[r]esponsive action . . . required to mitigate the security risk associated with accessing enterprise cloud service data or other resources using unmanaged devices and/or apps (204).” Ex-1005, ¶¶0032, 0019, 0054, 0071-0075; Ex-1003, ¶¶75-78, 95. The actions included migrating users to managed apps, logging out user sessions, *providing corrective actions via an interaction page*, warning users about unapproved actions, and stepping up authentication. Ex-1005, ¶0019.

A POSITA would have found it obvious that detecting a shadow system would include remediating the problem, whether by automating a remediation or engaging the user in pre-constructed remediation workflows. Ex-1003, ¶¶47, 76-78, 95. Figure 6 illustrates how a user was directed to remediate the use of an unmanaged application (shadow system), where the EMM solution informed *the user to uninstall the offending unmanaged app and install the managed app*. Ex-1005, ¶¶0054, 0071-0075 (mitigation actions including changing acceptable usage policies and managing notifications), Fig. 6; Ex-1003, ¶95.

7. Claims 7 and 15

7: “The method of claim 1 wherein the first information is not gathered from the one or more user devices.”

15: “The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more resources or the providers of the one or more resources other than the one or more user devices.”

Karunakaran disclosed or rendered obvious the claim limitations of claims 1 and 9 as seen above and the remaining limitation because the cloud service provider 102 (*the one or more providers of the one or more resources other than the one or more user devices*) generated the audit log 120/400 (*first information*). *See supra* §VII.A.2.c-d; Ex-1005, ¶¶0016, 0018, 0022, 0027-0031, 0034-0037, 0049; Ex-1003, ¶¶65-70, 82, 88-92, 96. In Karunakaran, the user device is the subject of, not the source of, the first information in the audit log 120/400. Notably, the '621 Patent specification never described user devices monitoring or gathering the “first information,” never described user devices acting as a “provider of one or more resources,” and never described the resource provider as monitoring or gathering the “second information” from the user’s perspective. Ex-1001. Thus, these dependent claims merely restate limitations already inherent in the independent claims—and do not actually narrow the claims.

8. Claims 8 and 16

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

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

Karunakaran disclosed or rendered obvious the claim limitations of claims 1 and 9 as seen above and the remaining limitation because Karunakaran integrated the client application 706, MDM Agent 704, and tunnel plug-in 710 on mobile device 702 (together reasonably combined as the *client application*) under management by the EMM Server 718, which collectively logged resource access information (*second information*) and acted as a proxy to forward and direct network traffic (*proxy application executed on at least a subset of the one or more user devices*). Ex-1005, ¶¶0094-0096, Fig. 7; Ex-1003, ¶¶69, 82, 78, 97-98.

As described above §VII.A.1.c, the term “application” is used throughout the ’621 Patent specification to refer to a variety of software functionality, cloud services, and service endpoints. *See e.g.*, Ex-1001 3:64-4:58, 6:45-64, *passim* (numerous uses of the term “application”). Similarly, the ’621 Patent describes the proxy functionality as part of the client application (*i.e.*, an authorized application or part of an authorized application on a user device) that “may include, for

example, a proxy application or an application implementing proxy functionality such that network traffic from the user device, including requests to access the one or more resources, is routed to the distributed edge platform or another destination.” Ex-1001 at 93:40-48; *see also* 94:51-55, 96:2-7. Accordingly, a POSITA would have understood that because the Karunakaran integrated a tunnel plug-in 710, client app 706, and MDM agent 704 as a single unit that both logs the resource access information and provides a redirecting proxy functionality, it would satisfy this claim. *See* Ex-1001 at 93:40–48, 94:51–55, Ex-1003, ¶¶82, 97-98.

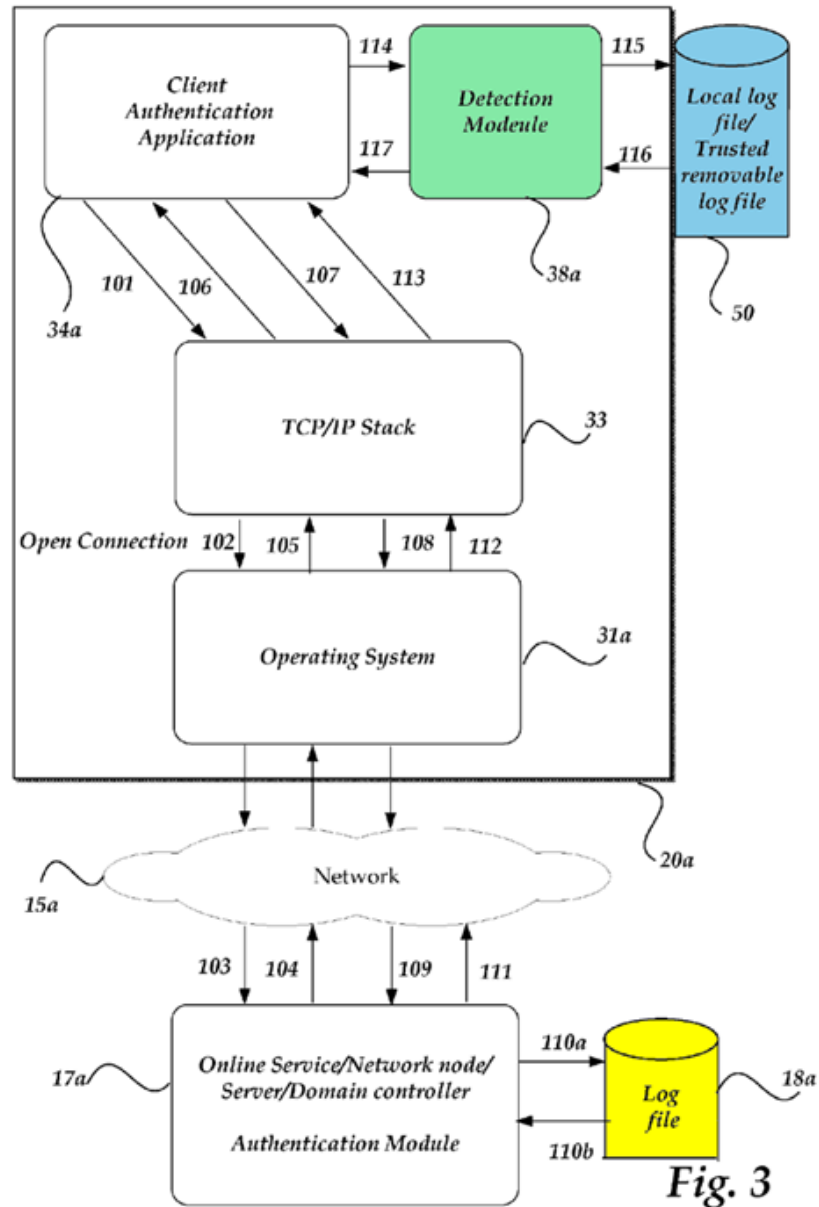
In Karunakaran, the tunnel plug-in 710 was configured to “forward traffic addressed by client app 706 to cloud-based service 708 directly,” while sending other traffic via tunnel 712 to the security proxy server 716. Ex-1005, ¶0096. Moreover, Karunakaran disclosed that “[t]he managed app 104 is managed in part by a *native or other* EMM agent 108 on the device 106. . . . In some embodiments, the EMM agent 108 may be a component and/or service of the device operating system.” Ex-1005, ¶0022. The phrase “native or other” directly indicates that there are multiple ways to implement the architecture, including integrating the MDM agent 704 with the client application 706 itself. It would have been straightforward for a POSITA to combine the proxy tunnel plug-in 710 with the client application

706 to produce a single binary component. A POSITA would have understood this combination of components—which collectively intercept, route, and log the user device’s traffic—fall within the meaning of “proxy application” as described in the ’621 Patent. Ex-1005, ¶¶0022, 0094-0096, Fig. 7; Ex-1003, ¶¶97-98.

B. Ground 2: Combining Chien with Lipman Renders Claims 1-3, 5-11, and 13-19 Obvious.

1. Overview of Chien

Chien disclosed a system and method for detecting unauthorized access to online accounts by gathering and comparing access information from two sources: an online service or network node 17a, and a trusted log file 50 from the client device 20a. Ex-1006, Abstract, ¶¶0018, 0033, 0037, 0041, 0047, 0048; Ex-1003, ¶¶99-105. As shown below in Figure 3, Chien’s system provided user device 20a access to “resources” through a network 15a, including “a legitimate website, an email service, a file storage service, a domain name assignment service, a network address identification service, and the like.” Ex-1006, ¶0020; Ex-1003, ¶¶100-101.



Ex-1006, Fig. 3.

When the client 20a accesses the network, “[a]n *online service gathers information about a user’s access to an online account* and makes that information available to the account owner and/or other authorized user. When an

online account is accessed, the online service *logs [in log file 18a] a time stamp, a network address from which the account was accessed [(e.g., IP address)], [TCP/UDP] port number, a user ID, routing data, and/or other access data. . . The accessing client also stores access data. The client, account owner, and/or another decision maker evaluates all, or portions of information to detect unauthorized access to the account.*” Ex-1006, Abstract, ¶0033, Fig. 3. Next, “[a] copy of this information will also be returned to the client and stored on a trusted log file [local log file 50]. In general, these two log files [(log file 18a and local log file 50)] will be the same and synchronized. Any accesses by an unauthorized client will be recorded in the server log of the authentication service [(log file 18a)], but will not be collected by the account owner or other authorized user of the account [(local/trusted log file 50)]. *A comparison will then reveal the unauthorized accesses and/or unauthorized client(s).*” Ex-1006, ¶0033, Figs. 3, 5; Ex-1003, ¶¶100-103.

The logs are compared to determine any discrepancies where accesses by unauthorized users are recorded in the server log but are absent from the authorized user’s trusted log, creating a discrepancy: “At a decision operation 216, decision maker compares the server log data with the trusted access data gathered by the account owner or by the client device. The decision maker can be a human account

owner, a pre-authorized client, the server, and/or a remote decision maker. If all data matches, normal processing continues. However, if an unacceptable difference exists between the server log file and client-side trusted data, the difference is reported to the account owner, at an operation 218.” Ex-1006, ¶0052, *see also* ¶0047 (“the copy of the received access information, for the unauthorized access, would not be included in a trusted log file of trusted access information.”); Ex-1003, ¶¶100-102.

“In certain embodiments, *comparing timestamp, IP address, port number, and/or other data from both log files, a discrepancy can be determined and an unauthorized access can be found*. From the timestamp, IP address, port number, and/or other data, an intruder, hacker, or other unauthorized user can be tracked down.” *Id.*, ¶121. Upon detecting a “*discrepancy, the Client Authentication Application may issue a warning and may report this to the account owner with the timestamp, IP address, TCP/UDP port number, and/or other information about the suspected unauthorized access*. The account owner may use this information to find an intruder, hacker, or other unauthorized user.” Ex-1006, ¶0048, *see also* ¶0037. Chien’s system will also generate alerts to the user where “an optional warning may be displayed in another browser field 124, in a pop-up window, and/or in another way. . . . In addition, or alternatively, additional

validation information may be requested, or the account access can be denied or terminated. . . . [A] report may be made to a file, sent as an instant message, sent as an email, or otherwise provided to the account owner, administrator, security personnel, or the like.” Ex-1006, ¶50; Ex-1003, ¶¶103-104, 134.

Chien’s core dual-log comparison mechanism addresses the same fundamental problem as the ’621 Patent—detecting unauthorized access by gathering and comparing access information from multiple sources. However, Chien does not clearly disclose that the originating source of the second (client-side) log is independent from the source of the first (network-side) log, since Chien’s trusted client-side log (trusted log 50) was populated (at least in part) from a copy of information the network node 17a (log file 18a) returns to the client. Ex-1006, ¶¶0033, 0045. Additionally, Chien does not frame the security issues in an environment where shadow systems are detected. For these reasons, as discussed below, Petitioner considers Chien in combination with Lipman. Ex-1003, ¶105.

2. Overview of Lipman

Lipman described a system directed to discovering “shadow IT,” or “the implementation and use of certain systems, services, operations, processes, and data, or a combination thereof, inside an organization without explicit organizational authorization.” Ex-1008, ¶0021. Lipman implemented shadow IT

discovery by monitoring interactions between endpoint devices 204 and cloud-based services 216—through an edge device 320—to determine if the interaction was authorized. Ex-1008, Abstract, ¶¶0005, 0012, 0021; Ex-1003, ¶106.

Lipman's endpoint devices 204 were configured with an endpoint agent 206 and pluggable feature packs, including a shadow IT discovery feature pack 210. Ex-1008, ¶¶0020, 0021, 0030, Figs. 2-4; Ex-1003, ¶¶106-109. The endpoint agent 206 performed user behavior monitoring at the operating system level, correlating user activity/events with individual device accessing cloud service. Ex-1008, ¶0028. The shadow IT discovery feature pack 210 comprised a data stream collector 412, a cloud services request detector 414, and a cyber behavior collector 416, which collectively gathered cyber behavior factors 212—including user authentication factors 420, user interactions 426, date/time/frequency 428, and user location 430. Ex-1008, ¶¶0030, 0046, 0047, 0049, Fig. 4; Ex-1003, ¶¶106-112. Several of these cyber behavior factors overlap with data fields logged by Chien's network node 17a, such as date/timestamps, location, and user identity information (including login). Ex-1006, ¶0044; Ex-1008, ¶¶0027-0028, 0049.

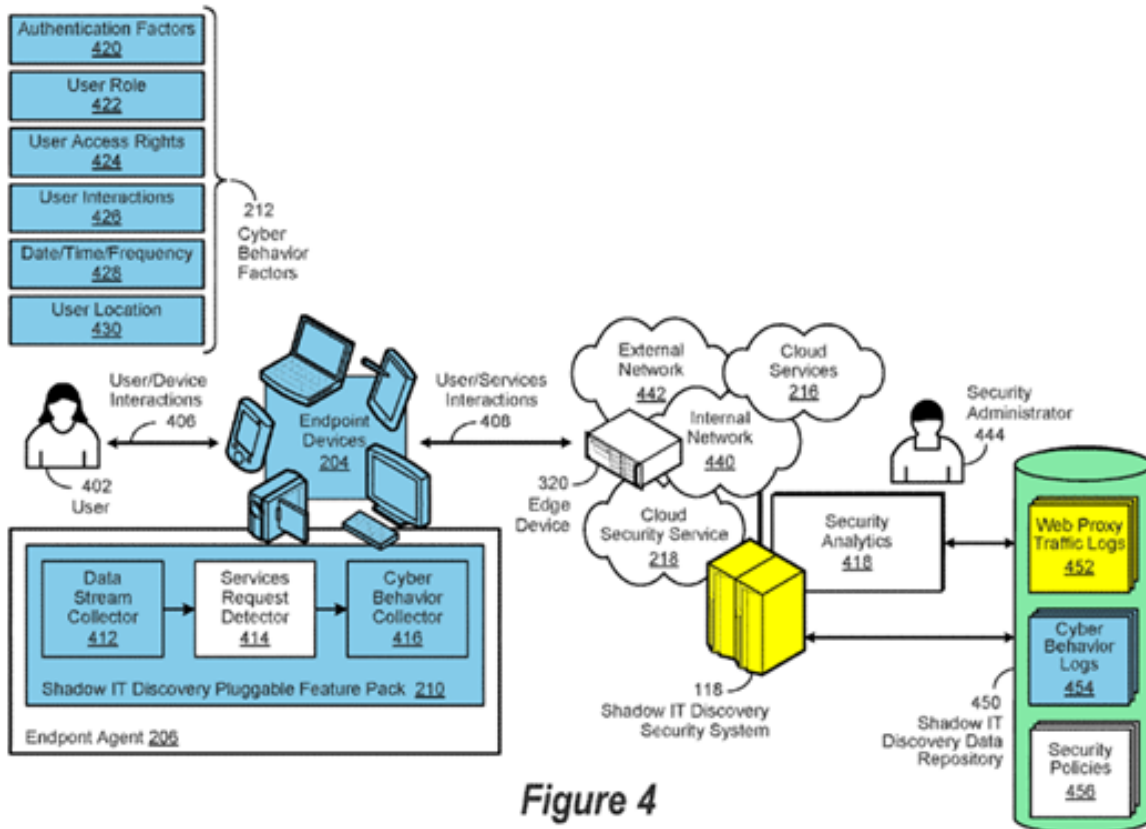


Figure 4

Ex-1008, Fig. 4.

In parallel, a shadow IT discovery system 118 on edge device 320 maintained web proxy traffic logs 324/452/454 recording information about the users' access to cloud-based services. Ex-1008, ¶¶0035, 0036, 0037, 0038, 0051, 0052, Figs. 2-4; Ex-1003, ¶¶106-112. Similar to Chien, Lipman's system performed a comparison between the cloud service request data gathered from the resource side (web proxy traffic logs 452) and the user's cyber behavior data 212 gathered from the client side (endpoint agent 206) to determine whether the user's interactions with a cloud service represented non-authorized use. Ex-1008, ¶¶0050,

0051, 0052, 0053, 0054, 0055; Ex-1003, ¶¶111-112. Upon identifying non-authorized use, Lipman disclosed enforcing a security policy that may block the user's access, restrict access, or allow unrestricted use, and further disclosed a multi-step remediation workflow—retrieve security policy, perform analytics, determine risk, decide whether to restrict use—triggered in response to identifying shadow IT. Ex-1008, ¶¶0053, 0054, 0055, 0056, 0057, Figs. 5a–5b; Ex-1003, ¶¶111-112.

3. Motivation to Combine

A POSITA at the time of the alleged invention would have been motivated to combine Chien and Lipman, with a reasonable expectation of success. Both references confront the same core technical challenge—identifying unauthorized or unsanctioned access to network resources—and both employ a similar approach of monitoring and comparing logged access information across multiple data sources. Ex-1006, Abstract, ¶¶0018, 0033; Ex-1008, Abstract, ¶¶0005, 0012, 0050. Lipman's teachings complement Chien's and provide several reasons to bring the two references together at the time the priority application for the '621 Patent was filed (in 2022). Ex-1003, ¶¶113-120.

First, although Chien predated the wave of BYOD personal mobile devices that reshaped the network security landscape, its foundational premise—flagging

unauthorized access—remained relevant. In 2007, modern mobile devices were just entering the market with limited processing power, so unsanctioned apps on mobile devices were not yet a significant concern, but unauthorized access to enterprise accounts was already a recognized problem. By approximately 2016, organizational IT security had expanded its focus to a then-emerging threat: unauthorized access through unsanctioned devices or applications (*i.e.*, the shadow IT problem). Ex-1006; Ex-1005, ¶¶0002; Ex-1016; Ex-1003, ¶¶48-54, 113-115. A POSITA would have appreciated that Chien’s client-side log—populated with a copy of information the server returned (Ex-1006, ¶¶0033, 0045)—would yield more complete and independently valuable data if the client application instead produced its own record of resource-access activity from the client’s vantage point, as Lipman’s endpoint agent does this through its data stream collector and cyber behavior collector modules—a natural progression given the substantial growth in mobile-device processing power since Chien. Ex-1006, ¶¶0037, 0047, 0048; Ex-1008, ¶¶0030, 0046, 0047, 0049-0051; Ex-1003, ¶¶113-114.

Second, BYOD policies and cloud-based enterprise services created an inherent conflict of interest: users could not be expected to self-report their own unsanctioned device use when doing so conflicted with their employer’s policies. A POSITA would therefore have recognized the need to automate the comparison

process rather than rely on user self-reporting, and Lipman's shadow IT discovery system supplied precisely such an automated, system-driven framework—offering a more efficient means of both collecting client-side resource-access data and performing the comparison in an automated manner. Ex-1008, ¶¶0050, 0051; Ex-1006, ¶¶0037, 0047, 0048; Ex-1003, ¶115.

Third, a POSITA would have appreciated that Lipman's method of collecting genuinely independent log data through its endpoint agent was both conceptually simpler and more dependable than Chien's approach of copying server-side information to the client. Ex-1008, ¶0030. Under Lipman's design, the client-side record is generated entirely from the endpoint's own observation of resource-access activity, rather than depending on the server to transmit a copy of access data. Ex-1008, ¶0030. Moreover, the growth in endpoint processing power between Chien's and Lipman's respective disclosures made the additional resource demands of a continuously operating endpoint agent far less of a practical concern. A POSITA would have recognized that integrating Lipman's endpoint agent into Chien's system would improve the reliability and completeness of the client-side information gathered, with a reasonable expectation of success. Ex-1003, ¶116.

Fourth, Lipman supplied a structured, policy-driven remediation workflow that addressed a gap in Chien's response to detected unauthorized access. While

Chien disclosed generating a warning and optionally requesting further validation or denying access, it did not set out a formalized remediation workflow. Ex-1006, ¶¶0048, 0050; Ex-1003, ¶117. Lipman filled that gap with a concrete, automated, multi-step remediation architecture that a POSITA would have viewed as a natural and desirable extension of any unauthorized-access detection system. Ex-1008, ¶¶0053–0057, Figs. 5a–5b; Ex-1003, ¶117.

Fifth, both Chien and Lipman employed modular, plug-in client-side architectures that would have made integrating the two systems—including a proxy application on the client side—straightforward for a POSITA. Chien disclosed that its Detection Module 38a and Client Authentication Application 34a could be deployed as plug-in modules that intercepted network requests, passed credentials, and stored access information in local log file 50—functions architecturally analogous to those of a proxy application. Ex-1006, ¶¶0029, 0041–0045, Fig. 3; Ex-1003, ¶118. Lipman’s endpoint agent 206 used a substantially similar plug-in design with pluggable feature packs 208, interfacing with the device through low-level OS hooks to intercept network traffic and wrap requests to be “handled by proxy.” Ex-1008, ¶¶0030, 0031–0032, 0036, 0043. Because both references already relied on plug-in designs, incorporating Lipman’s endpoint agent into Chien’s existing client-side framework would have required little more

than substituting one pluggable module for another—a routine design choice well within the capability of a POSITA. Ex-1003, ¶¶118–119.

Neither Chien nor Lipman taught away from this combination. Both references addressed the same general problem of detecting and responding to unauthorized access to computing resources, and their respective teachings were complementary rather than contradictory. A POSITA would have had a reasonable expectation of success because the underlying techniques—dual-source log comparison and shadow IT discovery analytics—were each individually well understood in the art, and combining them required no more than routine skill and ordinary creativity. Ex-1003, ¶120.

4. Claims 1, 9, and 17

- a. 1[pre]: “A method of using activity monitored by multiple data sources to identify shadow systems, the method comprising” (*See* 9[pre] and 17[pre] below)

To the extent the preamble is limiting, Chien in combination with Lipman disclosed or rendered obvious this limitation by detecting unauthorized access to online accounts and/or shadow systems by gathering and comparing access information from (*multiple data sources*) (1) log file 18a from network node 17a and (2) Lipman’s client-side data captured from endpoint agent 206, and *identifying* discrepancies in the logs to detect *shadow systems* as disclosed in

Lipman. Ex-1006, Abstract, ¶¶0018, 0026, 0037, 0041, 0044, 0051, Fig. 3; Ex-1008, Abstract, ¶¶0005, 0012, 0021, 0050. A POSITA would have understood the logs in Chien (first information) could be compared to the logs in Lipman (second information) because there is overlapping access information captured from different perspectives including, for example, the *timestamp*, client *identity information*, *location*, etc. Ex-1006, ¶0044; Ex-1008, ¶¶0028, 0049; Ex-1003, ¶¶40, 48-54, 99-112, 121; *see also infra* §VII.B.4.e.

For the reasons set forth in Section VII.B.3, *supra*, a POSITA would have been motivated to combine Chien and Lipman because both references address the same technical problem—detecting unauthorized access by comparing logged access information from multiple data sources—and the combination would have been a straightforward application of known techniques with a reasonable expectation of success. Ex-1003, ¶¶113-123.

- b. 9[pre] / 17[pre], 17[a], 17[b]: “A non-transitory computer readable storage medium storing instructions which, when executed, cause a processing device to” / “A system comprising: a memory; and a processing device, operatively coupled to the memory, the processing device configured to”

Chien alone or in combination with Lipman disclosed or rendered obvious this limitation because Chien at least described the hardware “processors,” “computer readable storage medium,” “memory” and “computer instructions” for

implementing the '621 systems of claims 9 and 17: “*client device 20 includes a processing unit 22 in communication with a mass memory 24 via a bus 23. . . .*

Mass memory 24 illustrates a type of *computer-readable media, namely computer storage media. Computer storage media . . . for storage of information such as computer readable instructions, ...* Other examples of computer storage media include EEPROM, flash memory . . . any other medium which can be used to store the desired information and which can be accessed by a computing device.” Ex-1006, ¶¶0024, 0026-0029, 0040, Figs. 2, 3; Ex-1003, ¶¶101-102, 104, 122.

- c. **1[a] / 9[a] / 17[c]: “gathering [or gather], from one or more resources or providers of the one or more resources, first information describing access to the one or more resources by one or more user devices of a user;”**

Chien alone or in combination with Lipman disclosed or rendered obvious this limitation because Chien disclosed the network node 17a gathering cloud resource access information in log file 18a (*first information*)—including a time stamp, IP network address, user ID, client identifier, routing data, and other access data (*access to the one or more resources*)—regarding a user device’s 20a (*one or more user devices of a user*) access to resources. Ex-1006, Abstract, ¶¶0018, 0020, 0033-0035, 0037-0038, 0041-0042, 0044, 0051, Fig. 3; Ex-1003, ¶¶101, 107, 123-124.

As described above in §VII.A.2.c, the '621 Patent describes the resource “provider” provides a variety of software functionality remotely (*i.e.*, server-side applications). As shown in Fig.1, Chien’s online service 16 provided resources to clients through the network: “Network 15 is in communication with and enables communication between each of client devices 12-14, online service 16, and network node 17.” Ex-1006, ¶0020, Fig. 1. The network node/authentication module 17a was a server-side application that authenticated users and “stored in a server log file or database” or log file 18a resource access information such as “a timestamp, the client IP address, the client port number and/or other access information to a network node log file 18a.” Ex-1006, ¶¶0018, 0033, 0044, 0051.

- d. 1[b] / 9[b] / 17[d]: **“gathering [or gather], from one or more client applications of at least a subset of the one or more user devices, second information describing access to the one or more resources;”**

Chien in combination with Lipman disclosed or rendered obvious this limitation because Lipman’s endpoint agent 206 with the shadow IT discovery pluggable feature pack 210 comprising a data stream collector 412, a cloud services request detector 414, and a cyber behavior collector 416 (*one or more client applications*), deployed on the user’s endpoint device 204 (*one or more user devices*), collected (*gathered*) cyber behavior factors 212 (*second information*)

describing access to one or more resources. Ex-1008, ¶¶0046, 0047, 0049; Ex-1003, ¶¶102, 109-111, 125.

The Shadow IT Discovery Pluggable Feature Pack 210 and related modules disclosed in Lipman collectively gathered information describing access to the cloud service resources from the client perspective (at the operating system level)—including the identity of the cloud service requested, the user’s authentication factors 420, user access rights 424, user interactions 426, date/time/frequency 428, and user location 428. Ex-1008, ¶¶0030, 0046-0047, 0049, Fig. 4; Ex-1003, ¶¶110, 125. This gathered second information overlapped Chien’s dual-log framework that gathered authentication data, timestamp, IP address, port number, and/or other data in Chien’s log file 18a. Ex-1006, ¶¶0018, 0033, 0037. Thus, combining Chien and Lipman would have been natural, and yield a predictable improvement in the reliability and completeness of the second information. For the reasons set forth in Section VII.B.3, *supra*, a POSITA would have been motivated to combine these references with a reasonable expectation of success. Ex-1003, ¶¶102, 109-111, 113-120, 125.

- e. **1[c] / 9[c] / 17[e]: “identifying one or more shadow systems based on a discrepancy between the first information and the second information, wherein the one or more shadow systems comprise one or more of the at least a subset of the one or more user devices engaging in shadow information technology (IT)**

activity, wherein identifying the one or more shadow systems comprises identifying one or more accesses described in the first information but not described in the second information and identifying, as one or more shadow systems, one or more user devices corresponding to the one or more accesses.”

Chien in combination with Lipman disclosed or rendered obvious this limitation because Lipman disclosed identifying *shadow systems*, while Chien disclosed the mechanism of comparing two access logs to determine *discrepancies* in the logs to identify unauthorized access, and Chien and Lipman disclosed identifying the user devices corresponding to those unmatched accesses as shadow systems. Ex-1006, Abstract, ¶¶0018, 0033, 0037, 0047–48, Fig. 5; Ex-1008, Abstract, ¶¶0005, 0012, 0050; Ex-1003, ¶¶40, 48-54, 99-100, 103-111, 125-129.

Shadow System: As described above in §§VII.B.4.a and VII.B.1-3, *supra*, Chien disclosed a system for detecting unauthorized access to online accounts, while Lipman described unauthorized access as “shadow IT.” Ex-1008, ¶¶0012, 0021; Ex-1003, ¶127. A POSITA would have been motivated to combine Chien’s detection of unauthorized accesses through log discrepancies with Lipman’s shadow IT discovery framework, predictably resulting in identifying shadow systems within the meaning of the ’621 Patent. Ex-1006, ¶¶0018, 0037, 0047, 0048; Ex-1008, ¶¶0012, 0021; Ex-1003, ¶¶48-54, 113-121, 127.

Comparison/Discrepancy Mechanism: Chien disclosed a discrepancy-based system for detecting unauthorized access by “comparing the log file [18a] on the server against the trusted log file [50]. If there [was a] discrepancy, there has likely been an unauthorized accessed to the account.” Ex-1006, ¶¶0037; *see also* Abstract, ¶¶0047, 0048 (“*If there is discrepancy, the Client Authentication Application may issue a warning and may report this to the account owner with the timestamp, IP address, TCP/UDP port number, and/or other information about the suspected unauthorized access.*”), *see also* Abstract, Fig. 5; Ex-1003, ¶¶127-128.

Chien disclosed that a discrepancy arises because unauthorized users are recorded on the log file 18a as accessing the server, but are absent from the authorized user’s trusted log 50—“the *copy of the received access information, for the unauthorized access, would not be included in a trusted log file of trusted access information.*” Ex-1006, ¶¶0047; *see also* ¶¶0033, 0037, 0048, Fig. 5; Ex-1003, ¶¶103, 128. Because Chien’s trusted client-side log was populated from a copy of server-side information (Ex-1006, ¶¶0033, 0045), a POSITA would combine Chien with Lipman to create an independent multi-source log discrepancy framework. Ex-1003, ¶¶113-120, 128.

A POSITA would have recognized that at least some of the cyber behavior factors 212 collected by Lipman’s endpoint agent—including timestamps, user identity information, and user location—align and overlap with the data fields logged by Chien’s network node 17a in log file 18a, such as the ***timestamp***, client ***identity information***, ***location***, for each access event. Ex-1006, ¶0044; Ex-1008, ¶¶0028, 0049. Thus, a comparison of the data collected by Chien (log file 18a) and Lipman (cyber behavior factors 212) would have been a straightforward task for a POSITA. Ex-1003, ¶¶113-120, 128.

Identifying the User Devices Corresponding to the Unmatched Accesses as Shadow Systems

Chien disclosed that “[t]he network node authentication module verifies the user credentials and writes a timestamp, the ***client IP address***, the ***client port number*** and/or other access information to a network node log file 18a.” Ex-1006, ¶0044. Lipman similarly disclosed that “the cyber behavior may likewise include information associated with a user submitting an HTTP request for a particular cloud service 216 . . . [which] may likewise include a user’s interactions . . . the date, time and frequency of such interactions, ***and data associated with the location of the user***.” Ex-1008, ¶0028; see also ¶0049; Ex-1003, ¶¶40, 48-54, 110-111, 129. Lipman further disclosed that the endpoint agent 206 is deployed in

combination with the endpoint device 204 to perform user behavior monitoring, confirming that Lipman’s collected activity data is tied to individual endpoint devices. Ex-1008, ¶0028. Thus, the information Chien and Lipman disclosed as logged would provide the specific identities of users and devices engaging in shadow IT. Ex-1006, ¶¶0044, 0047, 0048; Ex-1008, ¶¶0022, 0023, 0028, 0049; Ex-1003, ¶129.

Accordingly, a POSITA would have understood that when an access appears in the resource-side log (first information) but has no corresponding entry in the client-side log (second information), the *specific* user device responsible for that access is identifiable from the resource-side log entry—and that device is a “shadow system” within the meaning of the claims. Ex-1003, ¶129.

For the reasons set forth in §VII.B.3, *supra*, combining Chien’s dual-log discrepancy comparison with Lipman’s independently gathered client-side data and shadow IT discovery framework involves no more than applying known techniques to achieve predictable results, with a reasonable expectation of success. Ex-1003, ¶¶113-123, 126-129.

5. Claims 2, 10, and 18

2 [“The method of claim 1”] / 10[“The non-transitory computer readable storage medium of claim 9”] / 18 [“The system of claim 17”] . . . “wherein the first information is gathered from one or more identity providers.”

As explained above in §VII.A.3, a POSITA would have understood the identity provider verifies the identity of the user for at least one resource and gathers access information from the provider’s perspective. Ex-1001, 92:52-93:2, claims 1, 9, and 17. Chien disclosed or rendered obvious the claim limitations of claim 1, 9, and 17 as seen above and the remaining limitation because the network node/authentication module 17a (*identity provider*) both verified a user’s identity and gathered user device access information (*first information*) to *one or more resources* for inclusion in the log file 18a. Ex-1006, ¶¶0020, 0033, 0041, 0044, 0051, 0055, Ex-1003, ¶¶82, 88-92, 101, 123-124, 130-131.

Chien’s network node 17a was configured to provide access to resources while it also “verifies the user credentials and writes a timestamp, the *client IP address*, the *client port number* and/or other access information to a network node log file 18a”—the same information logged in the ’621 Patent. Ex-1006, ¶¶0044. Chien confirmed the network node 18a verified a clients identity because a “copy of the received access information may indicate a successful authentication with network node 17 a for access to the email account or other account.” *Id.*, *see also*

¶¶0033 (“Network node 17 a also *generally provides an authentication function to check online user identifiers and passwords of clients that access the network node.*”), 0020, 0041, 0043, 0051, 0055. Ex-1003, ¶¶130-131.

6. **Claims 3, 11, and 19**

3 [“The method of claim 1”] / 11 [“The non-transitory computer readable storage medium of claim 9”] . . . “wherein the first information is gathered from one or more applications of the one or more resources or of the providers.”

19: “The system of claim 17 wherein the first information is gathered from one or more applications of the one or more resources or the providers of the one or more resources.”

Chien disclosed or rendered obvious the claim limitations of claims 1, 9, and 17 as seen above and the remaining limitation because the network node 17a (*one or more resources or of the providers*) comprises an *application* that provides at least an authentication (identity verification) resource. Ex-1006, ¶¶0020, 0033, 0041, 0043-0044, 0051, 0055; Ex-1003, ¶¶82, 88, 97-98, 130-133.

Claims 2, 10, and 18 are actually more narrow than claims 3, 11, and 19, because an “identity provider” is a *type* of “application” on a resource or provider. *See supra* §VII.A.4.c. and VII.A.8. Thus, Chien’s network node 17a, which provides resource and comprises the server-side application of authenticating and verifying the identity of users (as well as logging access data), is both an “identity provider” and a server-side “application[] of the one or more resources or of the

providers”—that also logs the access information (*i.e.*, the first information). Ex-1003, ¶¶130-133.

7. Claims 5 and 13

5: “The method of claim 1 further comprising generating an alert in response to identifying the one or more shadow systems.”

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

Chien alone or in combination with Lipman disclosed or rendered obvious the claim limitations of claims 1 and 9 as seen above and the remaining limitation because Chien generates various warnings 220, 22, 224 (*alerts*) to the users upon identifying unauthorized access—and Lipman disclosed generating a notification upon a match of a shadow system. Ex-1006, ¶¶0048, 0050, 0052, Fig. 6; Ex-1008, ¶¶0014, 0055-56. Ex-1003, ¶¶102, 112, 134.

Chien disclosed that upon the discovery of a unauthorized access, the user may be warned: “*If there is discrepancy, the Client Authentication Application may issue a warning and may report this to the account owner . . . about the suspected unauthorized access.*” Ex-1006, ¶48. Chien disclosed the types of warnings be “a report may be made to a file, *sent as an instant message, sent as an email, or otherwise provided to the account owner, administrator, security*

personnel, or the like.” Ex-1006, ¶50; *see also* ¶52 (“*the difference is reported to the account owner, at an operation 218.*”). A POSITA would understand these are instructions processed by a processing device. Figure 6 of Chien provides the visual example of this warning. Ex-1003, ¶¶103, 134.

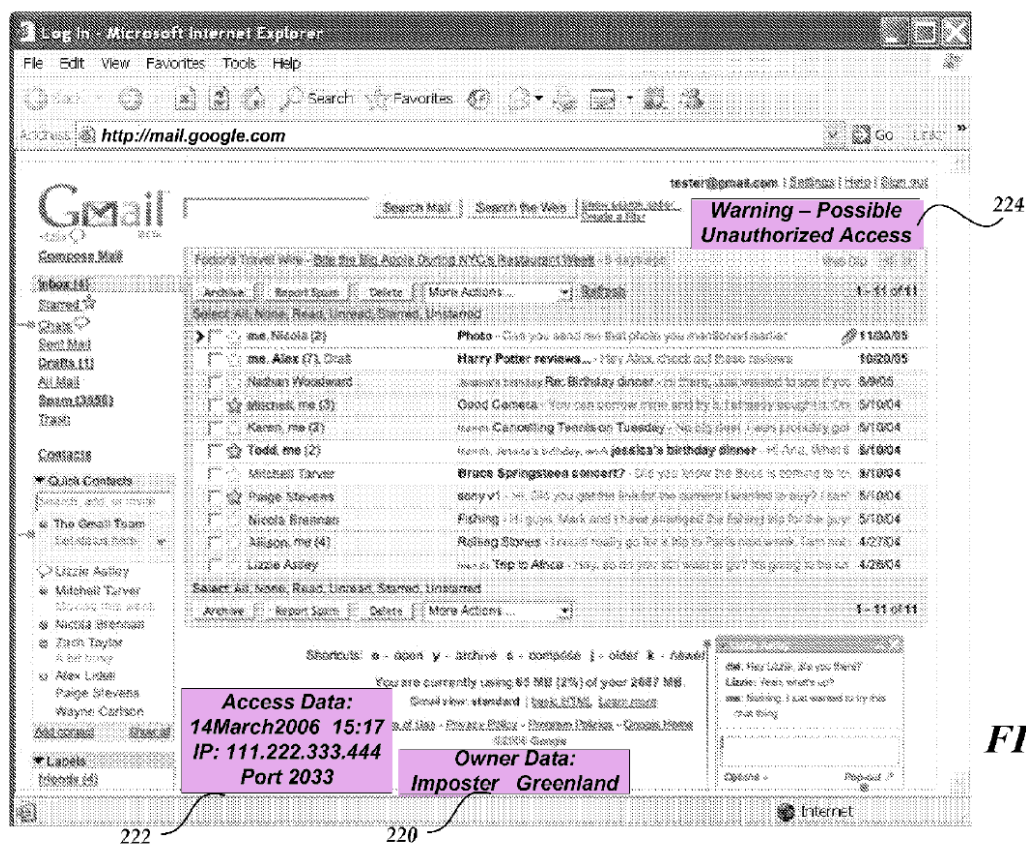


FIG. 6

Ex-1006, Fig. 6.

Lipman also discloses providing alerts. Ex-1003, ¶¶111, 133-137. For the reasons set forth in Section VII.B.3, *supra*, a POSITA would have been motivated to incorporate the warnings provided in Chien with the notifications provided in

Lipman to alert the system of the shadow system with a reasonable expectation of success. Ex-1003, ¶¶113-120, 134.

8. Claims 6 and 14

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

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

Chien and Lipman disclosed or rendered obvious the claim limitations of claims 1 and 9 as seen above and the remaining limitations because Chien disclosed both an automated remediation workflow (deny or terminate) or a human-in-the-loop remediation workflow (request additional validation information, issue a warning) (Ex-1006, ¶48) and Lipman disclosed a multi-step, policy-driven remediation workflow triggered in response to identifying non-authorized cloud service use. Ex-1008, ¶¶0053–0057, Figs. 5a–5b; Ex-1003, ¶¶47, 103, 112, 135-138.

Chien disclosed that where “there is discrepancy, the Client Authentication Application may issue a warning and may report this to the account owner . . . The account owner may use this information to find an intruder, hacker, or other unauthorized user. This information can also be returned to the network server

authentication module for further investigation.” Ex-1006, ¶0048. “In addition, or alternatively, *additional validation* information may be requested, or the account access can be denied or terminated.” Ex-1006, ¶0050, *see also* ¶0052 (“At a decision operation 210, the server may require *an additional password, and/or other information to authenticate the requester.*”) A POSITA would have understood that there are multiple remediation workflows available and that the user in Chien could have been embedded into the decision loop for “directing a user to a remediation workflow” as is required by claims 6 and 14. Ex-1006, ¶¶0048, 0050, 0052; Ex-1003, ¶¶135-138.

Lipman disclosed a multi-step, policy-driven remediation workflow triggered in response to identifying shadow systems—retrieving the applicable security policy, performing shadow IT discovery analytics, determining risk, and deciding whether to restrict access. Ex-1008, ¶¶0053–0057, Figs. 5a–5b. For the reasons set forth in Section VII.B.3, *supra*, a POSITA would have been motivated to incorporate Lipman’s structured remediation workflow into Chien’s detection system, with a reasonable expectation of success. Ex-1003, ¶¶113-120, 135-138.

9. Claims 7 and 15

7: “The method of claim 1 wherein the first information is not gathered from the one or more user devices.”

15: “The non-transitory computer readable storage medium of claim 9 wherein the first information is gathered from the one or more resources or the providers of the one or more resources other than the one or more user devices.”

Chien either alone or in combination with Lipman disclosed or rendered obvious the claim limitations of claim 1 and 9 as seen above and the remaining limitation because Chien’s network node 17a (*not the user devices*) gathers the first information. As described above in §§VII.B.4.c and VII.B.5 and 6, in the Chien system, the first information is collected by the network node 17a—a resource provider that is separate from the user devices. Ex-1006, ¶¶0033, 0020, 0041, 0043, 0044, 0051, 0055, Figs. 3 and 5; Ex-1003, ¶¶101, 123-124, 130-131, 139. As with Ground 1 (§VII.A.7), these dependent claims do not narrow the independent claims because the specification never disclosed the user devices gathering the first information nor acting as a provider of one or more resources.

10. Claims 8 and 16

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

16: “The non-transitory computer readable storage medium of claim 9 wherein the second information is gathered via

one or more proxy applications executed on the at least a subset of the one or more user devices.”

As described above in §VII.A.8, the '621 Patent describes “proxy application” as both logging resource access information and provide a redirecting proxy functionality on the client side. Ex-1001 at 93:40-48, 94:51-55, 96:2-7. Chien in combination with Lipman disclosed or rendered obvious the claim limitations of claims 1 and 9 as seen above and the remaining limitation because Chien disclosed client authentication applications 34a with proxy functionality and Lipman disclosed deploying an endpoint agent 206 on the user’s endpoint device 204 (*one or more user devices*) that functions as a *proxy application*. Ex-1006, ¶¶29, 41, Fig. 3; Ex-1008, ¶¶0030, 0040, 0043, 0046; Ex-1003, ¶¶43, 97, 109-110, 118-119, 140-143.

As shown in Fig. 3 in Chien, client 20a comprises a Client Authentication Application 34a (*e.g.*, an email application or browser) that already performed proxy-like functions (see steps 101-103, 113, 115), and a Detection Module 38a, which together gather and store “timestamps, IP addresses, TCP/UDP port numbers, or other data associated with accesses to an account that corresponds to a network resource” in a local log file 50. Ex-1006, Fig. 3, ¶¶0041-0045. Chien further disclosed that these modules may be “implemented as a plug-in” modules. Ex-1006, ¶¶0029; Ex-1003, ¶¶140-143.

As shown in Figure 4 of Lipman, the endpoint agent 206, deployed on the user's endpoint device 204, functions as a proxy application executed on the user device that also collects and logs access information:

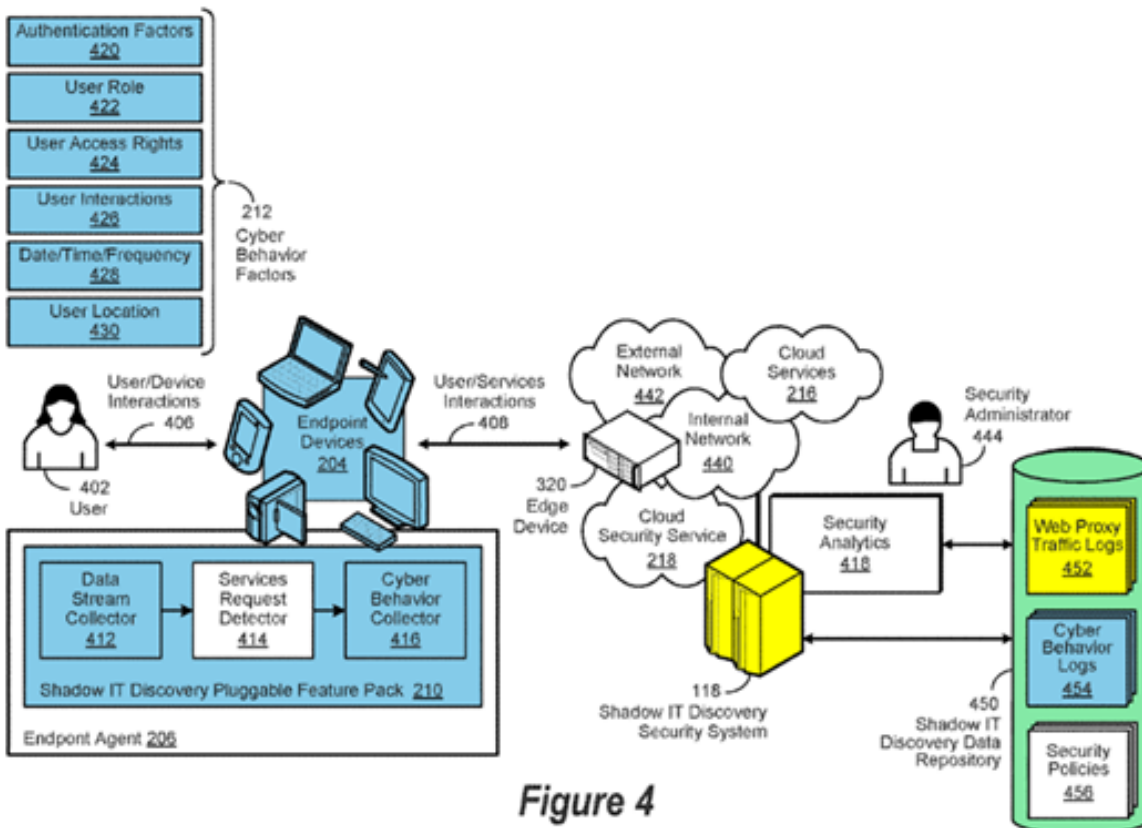


Figure 4

The endpoint agent 206 in Lipman included a shadow IT discovery pluggable feature pack 210 comprising a data stream collector 412 module, a cloud services request detector 414 module, and a cyber behavior collector 416 module. Ex-1008, ¶0046, Fig. 4. Lipman also explained that “[s]killed practitioners of the art” are “familiar with proxy servers, which may be *implemented as a specialized information handling system or as a software application, to act as an*

intermediary for requests from client devices seeking resources from other servers.” Ex-1008, ¶0036. Lipman disclosed that the endpoint agent 206 performed this same intermediary function on the endpoint device itself—intercepting network service requests, attaching contextual access information to cloud service requests, and wrapping requests to be “handled by proxy” via OS-level hooks before the request left the device. Ex-1008, ¶¶0030, 0040, 0043; Ex-1003, ¶140-143.

Together, the data stream collector 412, cloud services request detector 414, and cyber behavior collector 416 capture data streams from user/device interactions, identify cloud service requests, and gather associated cyber behavior factors—including user authentication factors, access rights, individual interactions, date/time/frequency, and user location. Ex-1008, ¶¶0047, 0049. Lipman’s endpoint agent thus operates as a client-resident proxy application that intercepts, monitors, and logs the user device’s outbound access requests to cloud service resources, and its modular plug-in architecture makes integration with Chien’s client-side framework straightforward. Ex-1008, ¶¶0030, 0040, 0043, 0046; Ex-1003, ¶¶140-143. For the reasons set forth in Section VII.B.3, *supra*, a POSITA would have been motivated to combine these references with a reasonable

expectation of success, yielding independently generated client-side logs gathered via a proxy application on the user device. Ex-1003, ¶¶113-123, 140-143.

VIII. CONCLUSION

Accordingly, the Board should institute IPR and cancel the challenged claims.

IX. PAYMENT OF FEES

The undersigned authorizes the Office to charge the fee required by §42.15(a) and any additional fees that might be due to Deposit Account No. 50-4561.

Dated: September 15, 2026

12275 El Camino Real, Ste 100
San Diego, California, 92130
Phone: (858) 720-8900
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,
RICHTER & HAMPTON LLP

/s/ Thomas Millikan

Thomas Millikan (Reg. No. 72,316)

Back-up Counsel

Joseph P. Reid (Reg. No. 72, 317)

Andrew Klein (*PHV* forthcoming)

Ericka Jacobs Schulz (Reg. No. 60,665)

Attorneys for Netskope, Inc.

CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(D)

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this Petition for *Inter Partes* Review totals 13,930 words, excluding the parts exempted by 37 C.F.R. §42.24(a). The word count was made using the built-in word count function in the Microsoft® Word 365 software used to prepare this document.

Dated: September 15, 2026

12275 El Camino Real, Ste 100
San Diego, California, 92130
Phone: (858) 720-8900
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,
RICHTER & HAMPTON LLP

/s/ Thomas Millikan

Thomas Millikan (Reg. No. 72,316)

Back-up Counsel

Joseph P. Reid (Reg. No. 72, 317)

Andrew Klein (*PHV* forthcoming)

Ericka Jacobs Schulz (Reg. No. 60,665)

Attorneys for Netskope, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that true copies of this PETITION FOR *INTER PARTES* REVIEW and supporting materials (Exhibits 1001-1026 and Power of Attorney) have been served via USPS Express Mail and electronically on counsel for patent owner as follows:

Law Office of Dorian Cartwright
P.O. Box 6629
San Jose, CA 95150
UNITED STATES
info@cartwrightesq.com

In addition, the undersigned certifies that a true copy of the petition and supporting materials have been served via email to Patent Owner's legal counsel:

Andrew Michael Holmes - drewholmes@quinnemanuel.com
Jordan Brock Kaericher - jordankaericher@quinnemanuel.com
Sean S. Pak - seanpak@quinnemanuel.com
Tigran Guledjian - tigranguledjian@quinnemanuel.com

Dated: September 15, 2026

12275 El Camino Real, Ste 100
San Diego, California, 92130
Phone: (858) 720-8900
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,
RICHTER & HAMPTON LLP

/s/ Thomas Millikan

Thomas Millikan (Reg. No. 72,316)

Back-up Counsel

Joseph P. Reid (Reg. No. 72, 317)

Andrew Klein (*PHV* forthcoming)

Ericka Jacobs Schulz (Reg. No. 60,665)

Attorneys for Netskope, Inc.