

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ORCA SECURITY LTD.,
Petitioner,

v.

WIZ, INC.,
Patent Owner.

IPR2025-01083
Patent 11,722,554 B2

Before KARL D. EASTHOM, NABEEL U. KHAN, and
LISA A. MURRAY, *Administrative Patent Judges*.

KHAN, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. *Background and Summary*

Orca Security Ltd. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–5, 7–16, and 18–21 (“the challenged claims”) of U.S. Patent No. 11,722,554 B2 (“the ’554 patent,” Ex. 1001). Wiz, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 9, “Prelim. Resp.”).

An *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Having considered the arguments and evidence presented by Petitioner and Patent Owner, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on at least one of the challenged claims of the ’554 patent. We do not institute *inter partes* review as to the challenged claims of the ’554 patent.

B. *Related Proceedings*

The parties identify the following matters as involving the ’554 patent: *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23-CV-00758 (D. Del.). Pet. 59; Paper 3, 1.

C. *The ’554 Patent (Ex. 1001)*

The challenged patent relates to a method and system for determining abnormal configuration of network objects deployed in a cloud computing environment. Ex. 1001, Abstract.

A cloud environment is depicted in Figure 1A, reproduced below.

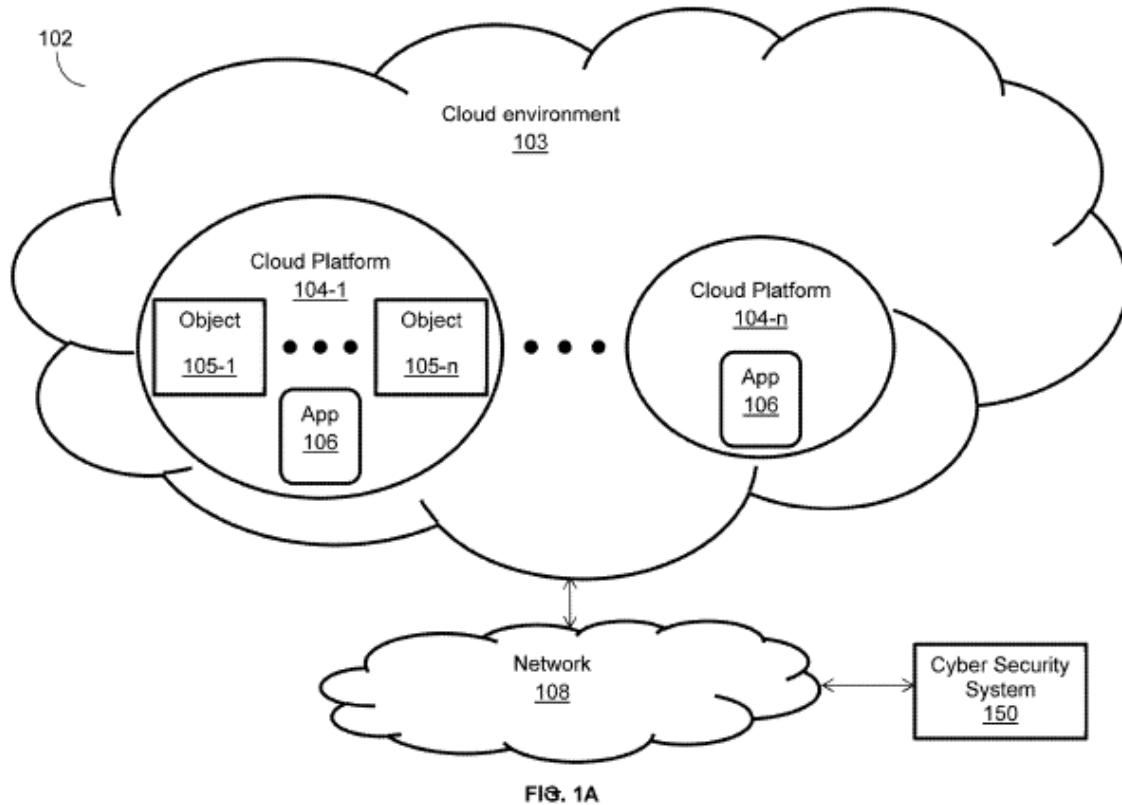


Figure 1A of the '554 patent, reproduced above, depicts a cloud environment 103 that includes a number of cloud computing platforms, 104-1 through 104-n. Ex. 1001, 4:7–9. Each cloud platform may include multiple network objects, 105-1 through 105-n and one or more applications 106. Ex. 1001, 4:9–14. The cloud environment may be configured to connect, via a network 108, with a cyber-security system 150. *Id.* at 4:14–16.

Figure 2, reproduced below, is a flowchart depicting a method for constructing a network graph for a network system. Ex. 1001, 7:43–44.

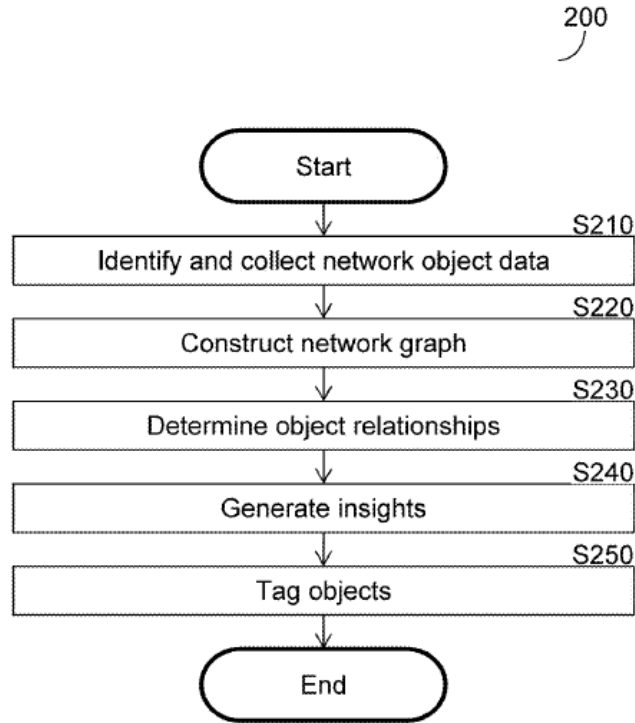


FIG. 2

Figure 2 of the '554 patent, reproduced above, depicts a flowchart 200 comprising five steps S210 – S250. At S210, network objects are identified, and network object data is collected. Ex. 1001, 7:46–47. In one embodiment, network objects may be identified by querying a cloud platform, through, for example, an orchestrator. *Id.* at 7:47–50. At S220, a network graph is constructed. *Id.* at 8:48. A network graph is a data feature describing the various objects included in, and adjacent to, a network, as well as the relationships between such objects. *Id.* at 8:48–51. At S230, relationships between network objects are determined. *Id.* at 9:3–4. Network object relationships are descriptions of the various connections between the network objects identified at S210. *Id.* at 9:4–6. At S240, network insights are generated. *Id.* at 10:15. Network insights are natural-language representations of aspects of the network graph constructed at S220. *Id.* at 10:15–17. At S250, network objects are tagged. *Id.* at 11:16.

Tagging of network objects at S250 may include association of one or more data labels, tags, or other, like, features, with graph entries for one or more network objects, including entries in graphs such as those described with respect to S220. *Id.* at 11:16–21.

D. Illustrative Claims

Claims 1, 11, and 12 are the only independent claims of the '554 patent. Claim 1 is reproduced below with limitation identifiers in brackets corresponding to claim analysis headings in the Petition. *See, e.g.*, Pet. 10–30.

1. [1[Pre]] A method for determining abnormal configuration of network objects deployed in a cloud computing environment, comprising:

[1[a]] collecting network object data on a plurality of network objects deployed in the cloud computing environment;

[1[b]] constructing a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;

[1[c]] determining relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects;

[1[d]] analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and

[1[e]] tagging network objects in the network graph for which the insight is generated.

Ex. 1001, 15:9–28.

E. Evidence

The Petition relies on the following references:

Reference	Exhibit No.
US 11,770,387 B1; filed July 17, 2020; issued Sept. 26, 2023 (“Shivamoggi”)	1004
US 10,693,743 B2; filed Sept. 21, 2015; issued June 23, 2020 (“Zhong”)	1005
US 2020/0382560 A1; filed May 31, 2019; published Dec. 3, 2020 (“Woolward”)	1006

Petitioner also relies on the Declaration of Dr. Chuck Easttom (Ex. 1003) in support of its arguments. The parties rely on other exhibits as discussed below.

F. Prior Art and Asserted Grounds

Petitioner sets forth the following challenges (Pet. 6–7):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 4, 7–12, 15, 18–21	103	Shivamoggi
2, 3, 13, 14	103	Shivamoggi, Zhong
5, 16	103	Shivamoggi, Woolward

II. ANALYSIS

A. Principles of Law

Petitioner bears the burden of persuasion to prove unpatentability of the claims challenged in the Petition, and that burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406

(2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) any objective evidence of obviousness or non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995).

Petitioner argues that a person of ordinary skill in the art (POSITA) “would have had a bachelor’s degree in an academic area emphasizing computer science (i.e. computer science, computer information systems, computer engineering, etc.) or cybersecurity, with at least two years of experience in the field of cybersecurity.” Pet. 6 (citing Ex. 1003 ¶ 49). Petitioner further argues that “additional education or experience might substitute for these requirements.” *Id.* Patent Owner does not contest Petitioner’s proposed definition of a POSITA at this stage of the proceeding. *See generally*, Prelim. Resp.

For purposes of this Decision, we adopt Petitioner’s proposed level of ordinary skill because it is consistent with the level of skill in the art at the time of the invention as reflected by the ’554 patent and the cited prior art.

C. Claim Construction

We apply the same claim construction standard used in district court actions under 35 U.S.C. § 282(b), namely that articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b).

In applying that standard, claim terms generally are given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Only claim terms in controversy require express construction, “and only to the extent necessary to resolve the controversy.” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *see also Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.”).

Petitioner asserts that “no claim terms need to be construed to resolve any issues in controversy in the Petition.” Pet. 7 (citing *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011)). Patent Owner asserts that “[n]o constructions are necessary to deny institution because denial is warranted for numerous reasons that do not depend on claim construction, as further detailed below.” Prelim. Resp. 2.

We determine that, at this stage of the proceeding, no explicit constructions are required to resolve the dispute between the parties.

D. Overview of Prior Art

Petitioner relies on Shivamoggi, Zhong, and Woolward in its asserted grounds. *See* § I.F. Below we provide an overview of the relied-upon references.

1. Overview of Shivamoggi

Shivamoggi describes “a cyberattack detection system that monitors a computer network for lateral movement.” Ex. 1004, Abstract. Shivamoggi explains that “[l]ateral movement is a stage of cyberattack where an attacker progressively moves through an organization’s network to search for high-value targets.” *Id.* at 2:48–50. Shivamoggi describes that conventional methods for detecting lateral movement attacks typically involve monitoring endpoint metadata such as endpoint authentication logs, which typically requires specialized data collection agents to be deployed on the network nodes, using up precious memory and storage capacity of the nodes, and interfering with nodes’ normal operations. *Id.* at 2:55–62. Shivamoggi’s Figure 1, below, shows a cyberattack detection system that uses connection graphs to detect suspected lateral movements in a computer network. *Id.* at 5:7–10.

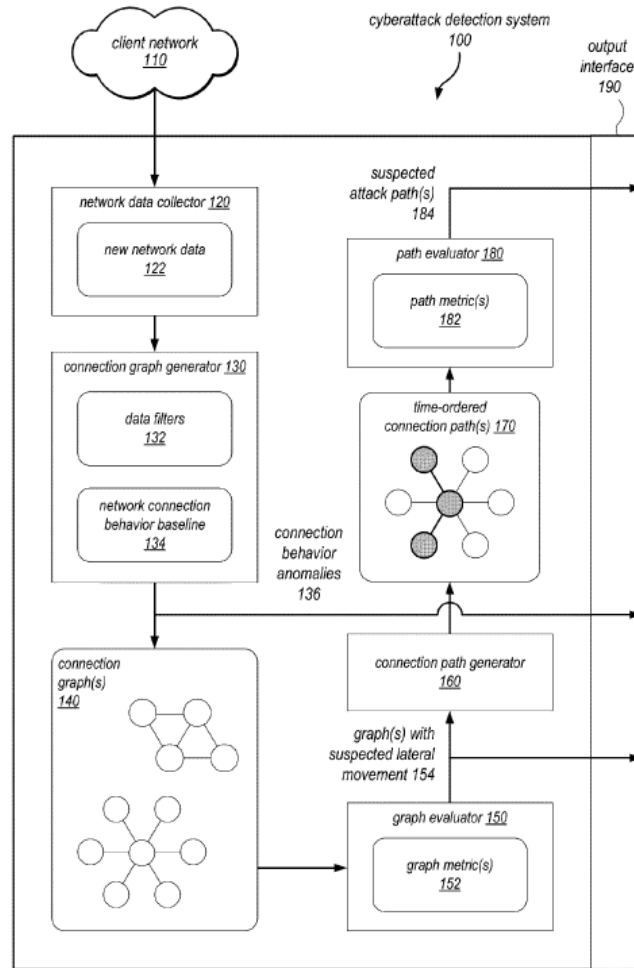


FIG. 1

Shivamoggi's Figure 1 shows a cyberattack attack system 100 that is configured to monitor a client network 110 for signs of lateral movement. Ex. 1004, 5:11–13. The monitoring may be performed by collecting network data 122 from the client network 110 using a network data collector component 120. *Id.* at 5:13–16. The network data may be collected at network data collection points (e.g. networking switches or routers) in the client network, so that no specialized data collection agents are deployed on the network nodes themselves. *Id.* at 5:16–20. Endpoint data collection agents may be used to collect endpoint metadata in addition to the network data, in order to augment the data used for lateral movement detection. *Id.* at

5:20–23. When a lateral movement is detected, the system 100 will generate an alert via an output interface 190. *Id.* at 5:31–33.

Shivamoggi’s Figure 2, below, shows a graph-based attack monitoring service that is implemented on a platform-as-a-service provider network. *Id.* at 9:6–8.

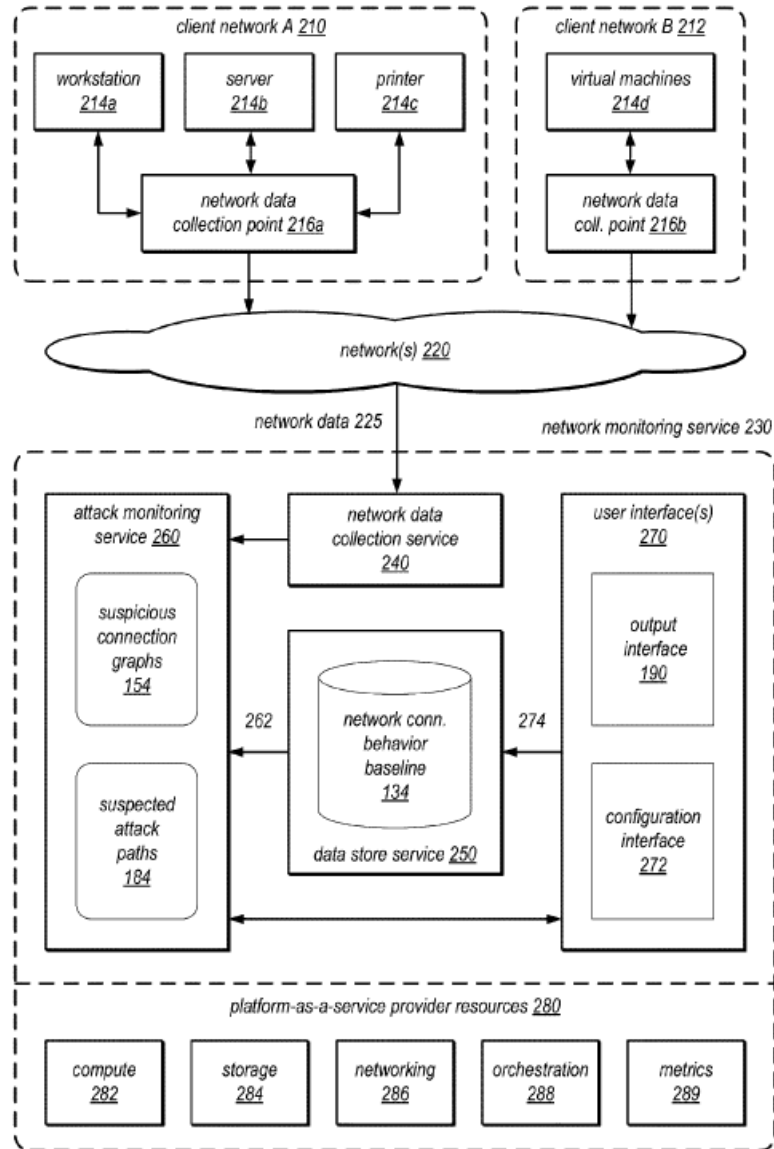


FIG. 2

Shivamoggi’s Figure 2 shows a network data collection service 240 and an attack monitoring service 260 implemented as part a network

monitoring service 230. Ex. 1004, 9:9–11. The network data collection service 240 may be configured to implement the network data collector 120 of Figure 1, and the attack monitoring service 260 may be configured to implement the connection graph generator 130, connection graph evaluator 150, connection path generator 160, and connection path evaluator 180. *Id.* at 9:11–17. The network monitoring service 230 is configured to monitor the remote client networks 210 and 220, which may be embodiments of the client network 110 of Figure 1. *Id.* at 9:17–20. The client networks 210 and 220 include different types of nodes, such as a workstation 214*a*, a server 214*b*, a printer 214*c*, and a virtual machine 214*d*. *Id.* at 9:47–49. Each client network may implement one or more network data collection points 216, which are configured to collect network data 225 from the client networks. *Id.* at 10:1–3. In some embodiments, these network data collection points 216 are distinct from the nodes 214*a-d* themselves, and may be implemented as a separate network entity, device, or host in the client network. *Id.* at 10:3–7.

Figure 7A of Shivamoggi, reproduced below, illustrates an example graphical user interface of the cyberattack detection system that provides information about a suspected lateral movement in a computer network. Ex. 1004, 2:10–13.

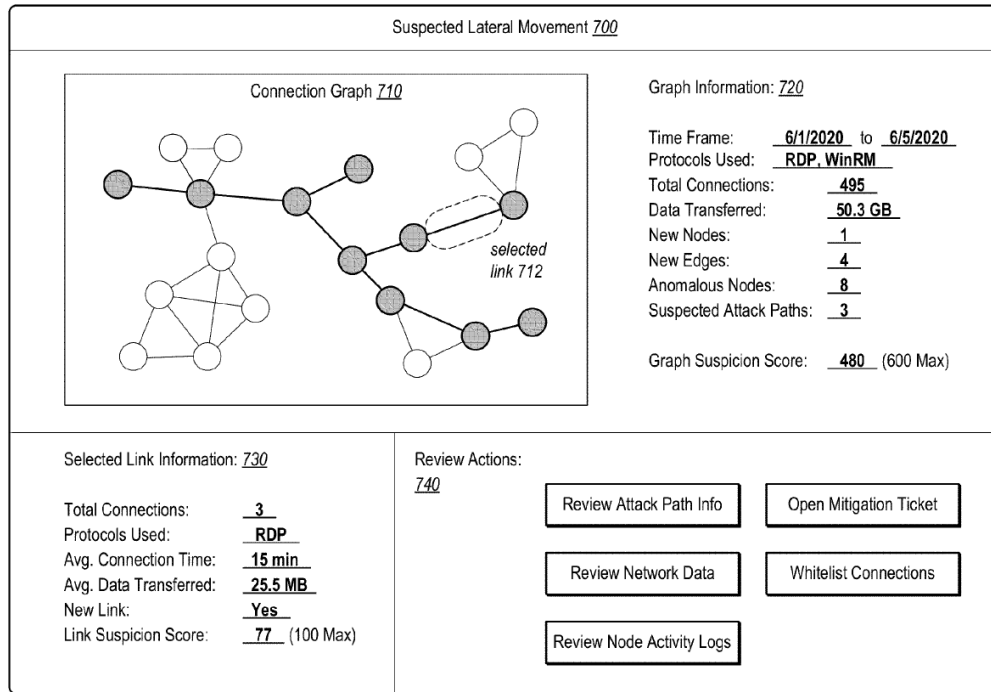


FIG. 7A

In Shivamoggi's Figure 7A above, the connection graph 710 is associated with the detected lateral movement and is displayed graphically. Ex. 1004, 15:22–23. Graph information section 720 provides a number of informational items about the graph 710, such as the communication protocols used, the time frame of the connection behaviors shown, the total number of connections represented by the graph, the amount of data transferred within the graph, etc. *Id.* at 15:27–32. Anomaly indicators are also shown, such as the number of new nodes using a new protocol included in the graph, the number of new edges that include first time connections between two nodes, and the total number of anomalous nodes in the graph. *Id.* at 15:33–38. In the example depicted in Figure 7A, a particular link 712 is selected and information about that link is provided in section 730. *Id.* at 15:45–47. Review Actions section 740 provides a number of control elements to allow the user to perform a variety of actions when examining the reported lateral movement, such as reviewing information about a

particular attack path (e.g. the various factors that were used to compute the path metric), reviewing the underlying network data that was used to generate the connection graph 710, and also reviewing node activity logs associated with the period represented by the connection graph. *Id.* at 15:49–58.

2. *Overview of Zhong*

Zhong relates to “techniques for displaying information related to a collection of cloud computing resources.” Ex. 1005, 1:16–18. Zhong describes the “collection of various types of data from cloud computing services and the generation of various dashboards and visualizations to view information about collections of cloud computing resources.” *Id.*, Abstract.

Zhong’s Figure 18, below, shows a networked computer environment that enables a cloud computing management application to collect data related to a collection of cloud computing resources and to display various visualizations related to the cloud computing resources. *Id.* at 38:54–58.

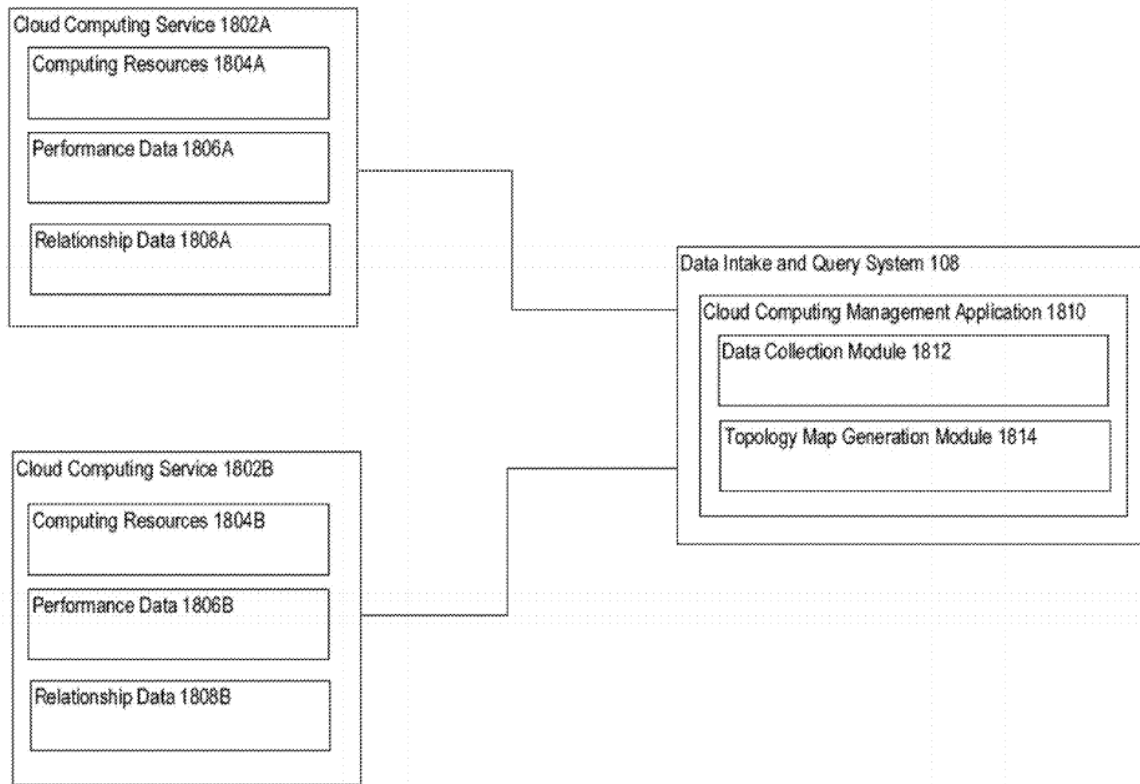


FIG. 18

Zhong's Figure 18 shows cloud computing services 1802A and 1802B and data intake and query system 108. Ex. 1005, 38:59–61. Each of cloud computing services 1802A and 1802B generally represents any collection of remote computing services offered by a cloud computing service provider. *Id.* at 38:62–65. Each of cloud computing services 1802A, 1802B includes a collection of computing resources 1804A, 1804B, performance data 1806A, 1806B, and relationship data 1808A, 1808B, respectively. *Id.* at 39:8–11. Performance data may include, for example, activity log files, configuration data, operating status information, performance metrics, or any other data that is generated by the cloud computing services related to computing services under management. *Id.* at 39:23–27. Relationship data generally may include any data that relates to relationships among the computing resources (e.g., relationship data may indicate that a particular storage

volume is attached to a particular server instance, that a particular server instance is a member of a particular subnet, etc.). *Id.* at 39:27–32. Zhong describes that cloud computing management application 1810 enables users to configure collection of data from any number of cloud computing services and further includes various interfaces for displaying information related to a user’s cloud computing resources. *Id.* at 39:40–44.

3. *Overview of Woolward*

Woolward relates “to communications networks, and more specifically to security in cloud computing environments.” Ex. 1006 ¶ 2. Woolward describes “methods and systems for validating [a] security policy in a cloud computing environment” and “[s]pecifically, a method for validating security policy in a cloud computing environment” that “may include providing a graph database.” *Id.* ¶ 6. The graph database may represent workloads of the cloud computing environment as nodes and relationships between the workloads as edges, and the security policy may logically describe rules for the relationships between the workloads. *Id.* The method may include determining, based on the security policy and the graph database, a list of violations and providing the list of violations to a user. *Id.*

E. *Ground 1 – Obviousness over Shivamoggi*

Petitioner contends that claims 1, 4, 7–12, 15, 18–21 are unpatentable as obvious over Shivamoggi. Pet. 10–44. Below we analyze Petitioner’s contentions in light of Patent Owner’s arguments.

1. *Analysis of Claim 1*

Petitioner contends that Shivamoggi teaches or suggests each of the limitations of claim 1. Pet. 10–30. Patent Owner disputes Petitioner’s contentions for limitations 1[a], 1[d], and 1[e]. Prelim. Resp. 3–13. We

analyze Patent Owner’s argument for limitation 1[d] below, which is dispositive for purposes of this Decision.

- a) *1[d] analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects;*

Petitioner contends that Shivamoggi’s “suspected attack paths” teach the recited “generated insights that include at least a list of abnormal connections” because the suspected attack paths demonstrate suspected lateral movement of a cyberattack where the lateral movement is an abnormal connection path among network objects. Pet. 25–26 (citing Ex. 1004, 17:55–57, Figs. 3, 5; Ex. 1003 ¶¶ 62, 98, 99.) Petitioner contends that a POSITA would have understood ‘suspected attack paths’ to be *generated insights* that *include a list of abnormal connections* within the meaning of the ’554 Patent because the ’554 Patent expressly teaches that *insights* may specify a path.” *Id.* at 25 (citing Ex. 1001, 10:31–49). Acknowledging that “[t]he ’554 [p]atent . . . describes *insights* as ‘natural-language representations of aspects of the network graph,” Petitioner argues that Figure 7A of Shivamoggi displays natural-language representations of the network graph and that a POSITA would have understood that, when selecting the “Review Attack Path Info” button in the graphical interface of Figure 7A, a user would be provided with similar information about a particular attack path. Pet. 26–27 (citing Ex. 1004, 15:27–32, 46–47, 51–58; Ex. 1003 ¶¶ 100–102).

Patent Owner argues that “the petition fails to show that Shivamoggi teaches generating insights that include *a list of abnormal connections between the identified network objects.*” Prelim. Resp. 8. Specifically, Patent Owner argues that Shivamoggi’s suspected attack paths do not

constitute a list of abnormal connections because Shivamoggi does not make clear that its suspected attack paths are provided in the form of a list rather than in another format such as a graphical format. Prelim. Resp. 9–10 (citing Ex. 1004, 8:60–63, 9:1–3; Pet. 25).

Having reviewed the record presently before us, we agree with Patent Owner. Limitation 1[d] requires generating “insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects.” The ’554 patent states that “[n]etwork insights are natural-language representations of aspects of the network graph.”¹ Ex. 1001, 10:15–17. Petitioner acknowledges that the recited “insights” are “natural-language representations.” Pet. 26 (citing Ex. 1001, 10:16–18). Dr. Easttom also agrees that insights are natural-language representations. Ex. 1003 ¶ 100 (testifying that “Shivamoggi’s insights are provided to the user as textual descriptions (i.e. natural-language representations).”). As an

¹ The parties do not address whether the “wherein” clause of limitation 1[d] runs afoul of the printed matter doctrine. “[T]he petition must set forth . . . [h]ow the challenged claim is to be construed.” 37 C.F.R. § 42.104. Even though “insights” are described in the ’554 patent as “natural-language representations of aspects of the network graph” (Ex. 1001, 10:15–17), Petitioner does not construe “insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects,” as “printed matter” that may be disregarded because it is “not functionally related to the substrate.” *See Praxair Distribution, Inc. v. Mallinckrodt Hosp. Prods. IP Ltd.*, 890 F.3d 1024, 1032 (Fed. Cir. 2018) (“Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability.” . . . For example, in *In re Ngai*, 367 F.3d 1336, 1339 (Fed. Cir. 2004) there was no functional relationship between claimed instructions and a diagnostic kit, as the instructions ‘in no way depend[ed] on the kit, and the kit [did] not depend on the’ instructions.” (quoting *Ngai*, 367 F.3d 1336, 1339 (Fed. Cir. 2004)). Because the parties have not addressed it, we decline to consider if the printed matter doctrine applies here.

example of an insight that specifies a path, the '554 patent discloses:

“virtual machine one to load balancer five, where port eighty is routed to port 1337 on virtual machine one, then from load balancer five to firewall two, where port eighty of firewall two is open, then from firewall two to subnet sixteen, where subnet sixteen has a network address of 10.0.1.0/24, then from subnet sixteen virtual network ten, where virtual network ten has a network address of 10.0.0.0/16, then from virtual network ten to virtual network eleven, via peering connection twelve, where peering connection twelve includes a routing rule to virtual network twelve, specifying virtual network twelve's network address, where virtual network twelve's network address is 172.31.0.0/16.”

Ex. 1001, 10:31–45 (quotation marks in original). This example illustrates that an insight is provided in natural-language, or textual, format, consistent with the description of an insight in the '554 patent and the testimony of Dr. Easttom. The limitation, which recites “the generated insights include at least a list of abnormal connections,” therefore requires generating a natural-language representation of a list of abnormal connections.

Petitioner points to Figure 7A of Shivamoggi as providing a “graph information section [that] includes natural-language representations of the network graph, such ‘communication protocols used, the time frame of the connection behaviors shown, the total number of connections represented by the graph, the amount of data transferred within the graph, etc.’” Pet. 26 (citing Ex. 1004, 15:29–32, Fig. 7A; Ex. 1003 ¶¶ 100–102). Petitioner also argues that “[a] POSITA would have understood that a user selecting the ‘Review Attack Path Info’ button . . . would be provided with similar information to that provided in the ‘Graph Information’ and ‘Selected Link Information’ sections of Figure 7A.” *Id.* at 26–27 (citing Ex. 1004, 15:51–58). But as Patent Owner points out (Prelim. Resp. 11), none of these

examples (e.g. communication protocols used, the time frame of the connection behaviors shown, the total number of connections represented by the graph, the amount of data transferred within the graph, etc.), and none of the information in elements 720 and 730 of Figure 7A, are a “list of abnormal connections.” Similarly, Shivamoggi discloses that selecting the “Review Attack Path” button would allow the user to review information such as “the various factors that were used to compute the path metric,” but does not disclose that a list of abnormal connections would be displayed. Ex. 1004, 15:54–55.

The closest Figure 7A comes to disclosing a “list of abnormal connections” is in the element labeled “Connection Graph 710,” which displays the nodes and edges that are involved in the suspected lateral movement attack path. Ex. 1004, 15:23–26. But, this element displays “the detected lateral movement . . . *graphically*.” *Id.* at 15:23 (emphasis added). A graphical representation of the lateral movement, or of a suspected attack path, is not a natural-language representation, and therefore is not an “insight” as recited in limitation 1[d]. Nor does Petitioner allege that a person of ordinary skill would have been motivated to modify Shivamoggi to display the suspected attack path in textual or natural-language form. *See* Pet. 8–11.

Accordingly, we determine Petitioner has not demonstrated a reasonable likelihood that Shivamoggi teaches limitation 1[d].

b) Conclusion – Claim 1

Because Petitioner has not demonstrated a reasonable likelihood that Shivamoggi teaches limitation 1[d], Petitioner has not demonstrated a reasonable likelihood that claim 1 is unpatentable as obvious over Shivamoggi.

2. *Conclusion – Ground 1*

Limitations 11[d] and 12[f] are similar in scope to limitation 1[d] and Petitioner relies on the same contentions for limitations 11[d] and 12[f] as it did for limitation 1[d]. Pet. 41–42. For the same reasons explained in our analysis of limitation 1[d], we determine Petitioner has not demonstrated a reasonable likelihood that Shivamoggi teaches limitations 11[d] and 12[f] and thus has not demonstrated a reasonable likelihood that claims 11 and 12 are unpatentable as obvious over Shivamoggi. Dependent claims 4, 7–11, 15, and 18–21 each depend from one of claims 1 and 12. For the same reasons, we determine Petitioner has not demonstrated a reasonable likelihood that these dependent claims are unpatentable as obvious over Shivamoggi.

F. *Grounds 2 and 3 – Obviousness over the Combination of Shivamoggi and Zhong and the Combination of Shivamoggi and Woolward*

Petitioner challenges dependent claims 2, 3, 5, 13, 14, and 16 based, in part, on its contentions for independent claims 1 and 12. Pet. 44–57. Petitioner’s reliance on Zhong and Woolward do not remedy the deficiencies we identified regarding limitations 1[d] and 12[f] above. We, therefore, determine that Petitioner has not demonstrated a reasonable likelihood that dependent claims 2, 3, 5, 13, 14, and 16 are unpatentable as obvious over the combination of Shivamoggi and Zhong or the combination of Shivamoggi and Woolward.

III. CONCLUSION

Petitioner has not demonstrated a reasonable likelihood of prevailing in showing the unpatentability of any of the challenged claims. Consequently, we do not institute an *inter partes* review on any grounds or claims raised in the Petition. See 37 C.F.R. § 42.108(a).

IV. ORDER

For the foregoing reasons, it is

ORDERED that, pursuant to 35 U.S.C. § 314(a), the Petition is denied and an *inter partes* review of claims 1–5, 7–16, and 18–21 of the '554 patent is not instituted.

IPR2025-01083
Patent 11,722,554 B2

FOR PETITIONER:

Robin Snader
Eric Buresh
Kathleen Fitterling
Chris Schmidt
ERISE IP, P.A.
robin.snader@eriseip.com
eric.buresh@eriseip.com
kathleen.fitterling@eriseip.com
chris.schmidt@eriseip.com

FOR PATENT OWNER:

Matthew Argenti
Michael Rosato
Wesley Derryberry
Joseph Baillargeon
WILSON SONSINI GOODRICH & ROSATI
margenti@wsgr.com
mrosato@wsgr.com
wderryberry@wsgr.com
jbaillargeon@wsgr.com