

Filed on behalf of: Wiz, Inc.

By: Matthew A. Argenti (margenti@wsgr.com)
Michael T. Rosato (mrosato@wsgr.com)
Wesley E. Derryberry (wderryberry@wsgr.com)
Tasha M. Thomas (tthomas@wsgr.com)
Joseph M. Baillargeon (jbaillargeon@wsgr.com)
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA 94304

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

Case IPR2025-00442
Patent No. 11,627,154

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,627,154**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	2
III.	CERTIFICATIONS.....	3
IV.	IDENTIFICATION OF CHALLENGE; STATEMENT OF PRECISE RELIEF REQUESTED	3
V.	THE '154 PATENT	3
A.	Prosecution History	5
VI.	NO BASIS EXISTS FOR DENIAL UNDER 35 U.S.C. §325(D)	6
VII.	LEVEL OF ORDINARY SKILL	7
VIII.	CLAIM CONSTRUCTION	8
IX.	STATE OF THE ART	8
X.	PRIOR ART.....	11
A.	Keren (U.S. Patent No. 11,374,982, EX1005).....	11
B.	Morgan (U.S. Patent No. 12,015,631, EX1006).....	14
XI.	GROUND 1: CLAIMS 1-20 WERE OBVIOUS OVER KEREN AND MORGAN.....	17
A.	Reasons to Combine Keren and Morgan	18
B.	Independent Claims.....	27
1.	Preambles	27
2.	Element 1.i	34
3.	Elements 1.1, 14.1, and 20.1.....	34
4.	Elements 1.2, 14.2, and 20.2.....	36
5.	Elements 1.3, 14.3, and 20.3.....	38
6.	Elements 1.4, 14.4, and 20.4.....	41
7.	Elements 1.5, 14.5, and 20.5.....	45
8.	Elements 1.6, 14.6, and 20.6.....	51
9.	Elements 1.7, 14.7, and 20.7.....	57

C.	Dependent Claims	62
1.	Claims 2 and 15.....	62
2.	Claims 3 and 16.....	63
3.	Claims 4 and 17.....	64
4.	Claims 5 and 18.....	67
5.	Claims 6 and 19.....	70
6.	Claim 7.....	70
7.	Claim 8.....	73
8.	Claim 9.....	75
9.	Claim 10.....	75
10.	Claim 11.....	76
11.	Claim 12.....	77
12.	Claim 13.....	78
XII.	CONCLUSION.....	79

LISTING OF CHALLENGED CLAIMS

1. A graphical user interface system for providing forward and backward facing attack vector visualizations, the system comprising:
 - [1.i] at least one processor configured to:
 - [1.1] identify assets in a cloud environment;
 - [1.2] identify risks associated with each of the identified asset;
 - [1.3] identify relationships between at least some of the identified assets, the relationships including at least one of a trust, a network connectivity, or a mechanism of network proxying;
 - [1.4] receive an identification of a specific asset under investigation;
 - [1.5] perform a forward analysis of the specific asset under investigation to identify at least one possible attack vector reaching the specific asset via a network outside the cloud environment;
 - [1.6] perform a backward analysis of the specific asset to identify at least one exposure risk to one or more assets that is in a downstream of the specific asset, wherein the at least one exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset; and
 - [1.7] output a signal to cause on a display to present a presentation of forward and backward paths associated with the specific asset, thereby enabling visualization of a plurality of entry points and lateral movement risks associated with the plurality of entry points.
2. The system of claim 1, wherein the network outside the cloud environment includes the Internet.
3. The system of claim 1, wherein the assets in the cloud environment include at least one of: a virtual machine, a network appliance, a storage appliance, a compute instance, or an engine instance.
4. The system of claim 1, wherein identifying the assets in a cloud environment includes identifying the assets based on at least one of: an

identity and access management policy, an organization policy, or an access policy.

5. The system of claim 1, wherein the presentation of the forward and backward paths indicates alternative paths connecting between the specific asset and an upstream asset or a downstream asset.

6. The system of claim 5, wherein the visualization includes a presentation of the alternative paths.

7. The system of claim 5, wherein the at least one processor is further configured to detect a potential risk associated with the specific asset based on the monitored network activities.

8. The system of claim 1, wherein the presentation of the forward and backward paths indicates port numbers for each pathway.

9. The system of claim 1, wherein the visualization of the entry points indicates at least one entry point at risk.

10. The system of claim 1, wherein the at least one processor is further configured to monitor network activities of the assets in a cloud environment.

11. The system of claim 1, the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of the specific asset.

12. The system of claim 1, the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of an upstream asset of the specific asset.

13. The system of claim 1, the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of a downstream asset of the specific asset.

14. A method for generating a graphical user interface for providing forward and backward facing attack vector visualizations, the method comprising:

[14.1] identifying assets in a cloud environment;

- [14.2] identifying risks associated with each of the identified asset;
- [14.3] identifying relationships between at least some of the identified assets, the relationships including at least one of a trust, a network connectivity, or a mechanism of network proxying;
- [14.4] receiving an identification of a specific asset under investigation;
- [14.5] performing a forward analysis of the specific asset under investigation to identify at least one possible attack vector reaching the specific asset via a network outside the cloud environment;
- [14.6] performing a backward analysis of the specific asset to identify at least one exposure risk to one or more assets that is in a downstream of the specific asset, wherein the at least one exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset; and
- [14.7] outputting a signal to cause on a display to present a presentation of forward and backward paths associated with the specific asset, thereby enabling visualization of a plurality of entry points and lateral movement risks associated with the plurality of entry points.

15. The method of claim 14, wherein the network outside the cloud environment includes the Internet.

16. The method of claim 14, wherein the assets in the cloud environment include at least one of: a virtual machine, a network appliance, a storage appliance, a compute instances, or an engine instance.

17. The method of claim 14, wherein identifying the assets in a cloud environment includes identifying the assets based on at least one of: an identity and access management policy, an organization policy, or an access policy.

18. The method of claim 14, wherein the presentation of the forward and backward paths indicates alternative paths connecting between the specific asset and an upstream asset or a downstream asset.

19. The method of claim 18, wherein the visualization includes a presentation of the alternative paths.

20. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations comprising:

[20.1] identifying assets in a cloud environment;

[20.2] identifying risks associated with each of the identified asset;

[20.3] identifying relationships between at least some of the identified assets, the relationships including at least one of a trust, a network connectivity, or a mechanism of network proxying;

[20.4] receiving an identification of a specific asset under investigation;

[20.5] performing a forward analysis of the specific asset under investigation to identify at least one possible attack vector reaching the specific asset via a network outside the cloud environment;

[20.6] performing a backward analysis of the specific asset to identify at least one exposure risk to one or more assets that is in a downstream of the specific asset, wherein the at least one exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset; and

[20.7] outputting a signal to cause on a display to present a presentation of forward and backward paths associated with the specific asset, thereby enabling visualization of a plurality of entry points and lateral movement risks associated with the plurality of entry points.

I. INTRODUCTION

Petitioner Wiz, Inc. (“Wiz”) respectfully requests review of U.S. Patent No. 11,627,154 (“the ’154 patent”), currently assigned to Orca Security Ltd. (“Orca”). This petition demonstrates claims 1-20 are unpatentable.

The ’154 claims describe well-known techniques for identifying the network paths within a cloud environment that an attacker could use to gain unauthorized access to assets and presenting those paths as visualizations in a graphical user interface system. These techniques involve identifying the assets in the cloud environment, risks associated with the assets, and the assets’ relationships. An identification of a specific asset under investigation is received and a forward and backward analysis is performed to identify an attack vector reaching the asset via a network outside the cloud environment and exposure risks to downstream assets. A signal is outputted to present the forward and backward paths associated with the asset to enable visualization of entry points and lateral movement risks.

These techniques of analyzing a cloud environment and its assets to identify and visualize the network paths that could serve as attack vectors were already well known prior to the ’154 patent’s priority date, as demonstrated by Keren and Morgan. Furthermore, the dependent claims describe other well-known features, as demonstrated below.

Accordingly, Wiz respectfully requests institution.

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Party-in-Interest (37 C.F.R. §42.8(b)(1)): Petitioner Wiz is the real party-in-interest.

Related Matters (37 C.F.R. § 42.8(b)(2)): Wiz is involved in litigation involving Orca patents from a different patent family than those of the '154 patent in *Orca Security Ltd. v. Wiz, Inc.*, No. 1-23-cv-00758 (DDE), filed and served on July 12, 2023. Wiz has also filed the following IPR petitions challenging Orca patents unrelated to the '154 patent: IPR2024-00220, IPR2024-00863, IPR2024-00864, IPR2024-00865, IPR2024-01109, IPR2024-01190, IPR2024-01191, and IPR2025-00092. In addition, Wiz has filed IPR petitions challenging two Orca patents claiming priority to the same provisional application as the '154 patent: IPR2025-00093 and IPR2025-00095.

Lead and Back-Up Counsel (37 C.F.R. §42.8(b)(3)):

Lead Counsel: Matthew A. Argenti (Reg. No. 61,836)

Back-Up Counsel: Michael T. Rosato (Reg. No. 52,182); Wesley E. Derryberry (Reg. No. 71,594); Tasha M. Thomas (Reg. No. 73,207); Joseph M. Baillargeon (Reg. No. 79,685).

Service Information—37 C.F.R. §42.8(b)(4): Wiz consents to electronic service. Please direct all correspondence to lead and back-up counsel at the contact information below. A power of attorney accompanies this petition.

E-mail: margenti@wsgr.com; mrosato@wsgr.com; wderryberry@wsgr.com;
tthomas@wsgr.com; jbaillargeon@wsgr.com

Post: WILSON SONSINI GOODRICH & ROSATI, 650 Page Mill Road,
Palo Alto, CA 94304

Tel.: 650-354-4154 Fax: 650-493-6811

III. CERTIFICATIONS

The '154 patent is available for IPR, and Wiz is not barred or estopped from requesting IPR on these grounds.

IV. IDENTIFICATION OF CHALLENGE; STATEMENT OF PRECISE RELIEF REQUESTED

Wiz seeks cancellation of the challenged claims for the reasons stated below, which are supported with exhibits, including the Declaration of Dr. Angelos Stavrou (EX1002). The claims are unpatentable under 35 U.S.C. §311 and AIA §6 based on at least the following grounds:

Ground	Claims	Basis
1	1-20	§103(a): obviousness over Keren and Morgan.

V. THE '154 PATENT

The '154 patent issued from U.S. Application No. 17/657,981 (“the '981 application”), filed April 5, 2022. EX1001, Face. The '981 application claims priority to Provisional Application No. 63/180,048, filed April 26, 2021. The '154

patent thus has an effective filing date no earlier than April 26, 2021, and is subject to AIA §102 and §103. *Id.*; EX1002, ¶20.

The '154 patent describes “a system for performing visualization of forward and backward facing threats” for a cloud infrastructure. EX1001, 1:15-18, 45:38-40, Fig. 8; EX1002, ¶23. The specification describes the well-known techniques of identifying assets in a cloud environment (e.g., virtual machines, network appliances, storage appliances, compute instances, and engine instances), identifying risks associated with the assets, and determining the relationships (e.g., trust, network connectivity, or proxying) between the assets. EX1001, 45:55-46:29, 47:25-42; *see also id.*, 10:26-30, 13:8-18, 47:43-54, 48:28-55, 49:3-17, 49:30-43, 65:11-21, Fig. 1, claim 3; EX1002, ¶¶24-26.

The specification further describes the well-known technique of performing an attack path analysis. EX1002, ¶¶27-28; *infra*, §IX. More specifically, the system is configured to “receive an identification ... of a specific asset under investigation” and perform “a forward analysis” and “a backward analysis” of the asset. EX1001, 46:30-47:4; *see also id.*, 49:44-52. A forward analysis “identif[ies] at least one possible attack vector reaching the specific asset via a network outside the cloud environment” (e.g., the internet) and “may involve those external entities that may access an analyzed asset.” *Id.*, 46:39-53; *see also id.*, 48:63-65, 47:19-21, 49:53-50:3; EX1002, ¶27. A backward analysis considers

“the possible impacts to an analyzed asset and those impacts’ possible effect” by identifying “at least one exposure risk” to a downstream asset, such as identifying an exposed asset, an entry point into it (e.g., a port of access), and lateral movement risks (e.g., potential movement between assets). EX1001, 46:54-67, 48:17-19, 48:65-67, 61:19-39; *see also id.*, 15:14-15, 46:67-47:4, 50:4-19, 69:26-28; EX1002, ¶28.

Finally, the system can display “a presentation of forward and backward paths associated with the specific asset” to “enabl[e] visualization of a plurality of entry points and lateral movement risks associated with the plurality of entry points,” which can be “graphical, sequential, or multi-dimensional displays of attack vectors.” EX1001, 45:41-54, 47:5-10; *see also id.*, 47:10-18; EX1002, ¶29.

The ’154 patent includes 20 claims. Claims 1, 14, and 20 are independent. Claims 14 and 20 essentially mirror claim 1, but whereas claim 1 is a system claim, claim 14 is directed to a method, and claim 20 is directed to a computer-readable medium. The dependent claims add other conventional aspects of cybersecurity and cloud computing. EX1002, ¶¶30-31.

A. Prosecution History

During prosecution, the ’981 application never received a rejection under §102 or §103. The first office action was an *Ex Parte Quayle* action that only objected to the specification and drawings. EX1004, 630-36. After addressing the

objections, a notice of allowance issued. *Id.*, 322-23. In allowing the claims, the Examiner identified a reference (CN 110708315 (Wang)) as the closest prior art, but only broadly indicated the supposedly lacking teachings by copying and pasting most of the independent claim language without explanation. *Id.*, 634-35; EX1002, ¶32.

VI. NO BASIS EXISTS FOR DENIAL UNDER 35 U.S.C. §325(d)

Under the two-part *Advanced Bionics* framework, §325(d) analysis considers several factors to determine:

(1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of [the] first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.

Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6 at 8 (precedential); 35 U.S.C. §325(d).

Keren was not presented to the Office nor considered by the Office during prosecution. *See* EX1001, (56); *see generally* EX1004. The reference is also not cumulative of references considered during prosecution. Keren was also never considered in combination with Morgan since that reference likewise was not disclosed. The Office thus did not consider any of the grounds presented herein.

The Office also lacked additional evidence discussed herein, including the declaration provided by Wiz's expert, Dr. Stavrou.

Allowance of the claims also constituted material error under part two of the *Advanced Bionics* test. The Examiner allowed the '154 patent claims without rejection and simply reproduced the claim language as a reason for allowance. See EX1004, 630-36; *supra*, §V.A. However, as discussed in more detail below, the combination of Keren and Morgan teaches each of these limitations. *Infra*, §§X-XI. The claims therefore should not have issued, and they would not have issued if the Examiner had considered the present grounds.

VII. LEVEL OF ORDINARY SKILL

For purposes of this petition, Wiz assumes a priority date of April 26, 2021. A POSA as of April 2021 would have held at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and would also have 2-3 years of professional experience working with cyber security analysis and virtualization. Additional experience could compensate for less education and vice versa. Relevant work experience includes, for example, malware analysis, security analysis of cloud computing systems, and security analysis of VMs. EX1002, ¶¶21-22. Dr. Stavrou meets these requirements and is qualified to credibly opine on the state of the art and the POSA's perspective. *Id.*, ¶¶1-19; see also *id.*, ¶¶2-5 (qualifications); EX1003 (Stavrou CV).

VIII. CLAIM CONSTRUCTION

Claim terms are given their ordinary and customary meaning, consistent with the specification, as a POSA understood them. 37 CFR §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc). This petition applies the ordinary and customary meaning of the claim terms. *See also* EX1002, ¶33.

IX. STATE OF THE ART

By April 26, 2021, cybersecurity systems for analyzing and visualizing the network paths that an outside attacker could traverse within a computing environment were well-known and predictable. EX1002, ¶34. These vector visualizations were commonly known as “attack graphs” or “attack trees.” EX1007, ¶¶5 (“to defend against cyber-attacks,” “analytical attack graphs (AAGs) can be generated, which represent potential lateral movements of adversaries within computing networks”), 26-29, Fig. 3; EX1009, iv (attack graphs “measure the security risk of enterprise systems”); EX1010, 1-2; EX1011, 2 (“attack graphs and attack trees are the most popular method of representing cyber-attacks”). Attack vector visualizations illustrated to network administrators how an attacker could leverage vulnerabilities in assets to enter and move within the network to achieve an attack. EX1007, ¶¶5 (attack graphs show “how a computer network can be hacked and undesirable consequences that can result”), 26-29; EX1008, 1:25-29, 1:44-58; EX1009, iv (attack graphs illustrate “how vulnerabilities can be

combined and exploited to stage an attack”), 6; EX1011, 2. Because attackers often targeted operationally sensitive or critical assets, POSAs recognized attack path visualizations as a useful tool to understanding how important assets could be at risk. EX1007, ¶¶4-5; EX1009, 6 (attackers “launch multistep and multi-host attacks that can incrementally penetrate the network with the goal of eventually compromising critical systems”); EX1010, Fig. 3 (illustrating attack path accessing protected internal servers).

POSAs understood that a starting point to identifying attack vectors was knowledge of the overall network topology of the computing environment. EX1006, 2:1-5, 7:9-19 (collecting “knowledge of network architecture (e.g., device data, topology data, inter-device connection data)”), Fig. 2; EX1007, ¶35 (determining “network topology”); EX1008, Abstract, 2:4-30; EX1010, 2; EX1002, ¶35. This included identification of the environment’s assets and the network paths by which the assets were reachable. EX1006, 7:9-19; EX1009, 8; EX1010, 2, Fig. 2. POSAs appreciated that this information indicated an asset’s exposure to outside sources (e.g., the internet), which could be informative of risk. EX1005, 12:62-13:5, 19:34-20:12, Fig. 5; EX1017, 6:7-23 (cloud-based workloads “run a risk of being exposed to the external networks, such as the Internet”).

POSAs further understood that, while this information was relevant to assessing an asset’s exposure risk, the existence of a network path did not

necessarily mean an attacker could actually exploit that path. EX1006, 3:4-19 (“selectively identifying network pathways” that correspond to those that can be used by attacker); EX1007, ¶28 (consideration of topological connection alone is an “incomplete solution[] for addressing real attack scenarios”); EX1002, ¶36. To traverse a network path, it was understood that attackers also needed to successively exploit vulnerabilities present in assets along the path. EX1006, 2:1-7, 3:4-19, 7:20-27; EX1007, ¶36; EX1008, Abstract; EX1010, 2; *see also* EX1002, ¶¶37-38 (describing example attack path visualization from workstation to gain control of database server) (citing EX1009, 7-8, 13-20, Figs. 1-2; EX1010, 2), 39 (describing example attack path visualization of outside attacker gaining entry into internally protected servers through internet-facing servers) (citing EX1010, 2-3, Figs. 2-3). Thus, by analyzing the vulnerabilities along reachable paths between assets in a network, POSAs understood that assessments regarding the risk of attack could be beneficially improved. EX1002, ¶40. This, in turn, aided network administrators in remediation efforts because attack path visualizations allowed possible impacts to be better ascertained and gave improved insight into the fixes that would result in greater risk reduction to the network. EX1006, 14:46-15:2, 15:50-57 (attack graphs can “prioritize vulnerabilities and remediations”), 19:4-9; EX1007, ¶29 (attack graphs can “identify the most vulnerable components” and “be used to evaluate fixes”); EX1010, 2; EX1009, 20-22; EX1017, 6:20-23.

X. PRIOR ART

A. Keren (U.S. Patent No. 11,374,982, EX1005)

Keren was filed February 18, 2021, and is therefore prior art under 35 U.S.C. §102(a)(2).

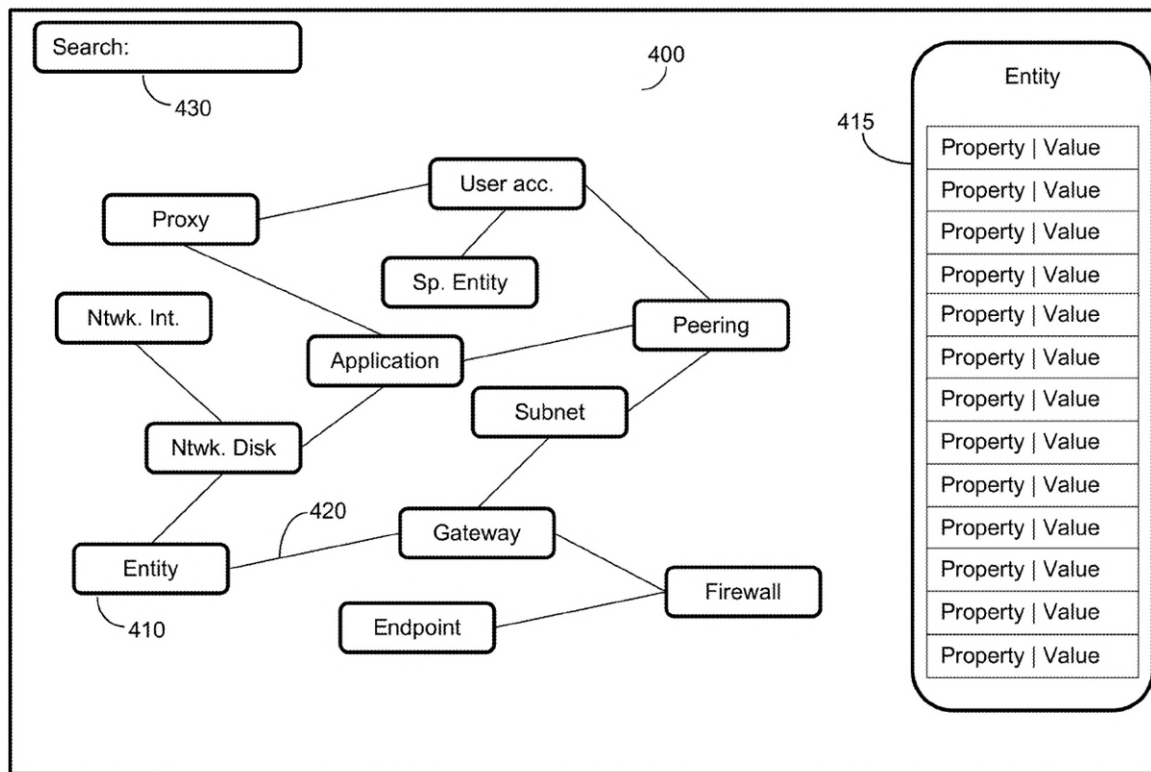
Keren relates to cybersecurity methods and systems “for automated generation of network analysis insights” in a cloud environment. EX1005, 1:16-18; *see also id.*, Abstract, 3:6-39, 4:31-55, Figs. 1A-B. The cloud environment includes “multiple security objects,” which are “objects, systems, devices, components, applications, entities, and the like, configured to operate within the cloud platform 104 and provide various functionalities therein.” *Id.*, 4:35-43, 5:20-44. The security objects may include, for example, proxies, firewalls, processing systems, databases, virtual machines, containers, and the like. *Id.*, 5:32-44, 6:13-19, 9:6-15; EX1002, ¶41.

The cloud environment connects with a cybersecurity system, which “provide[s] one or more network analysis functionalities including, without limitation, network analysis, traffic analysis, object querying, graph generation, and the like, as well as any combination thereof.” EX1005, 4:43-47, 6:47-51, Figs. 1A-1B; *see also id.*, 2:43-53 (system “provide[s] network information which describes the role of an individual entity within such a network or a cloud environment, as well as the vulnerabilities presented by the entities’ placements

within the network configuration”); EX1002, ¶42. To perform its analysis, Keren teaches that the cybersecurity system identifies the security objects and collects security object data. EX1005, 9:26-66, 10:11-14, Fig. 2; EX1002, ¶43. This collected data allows the system to determine the network connections, or relationships, between the security objects and construct a security graph describing the network topology of the cloud environment. *Id.*, 7:18-24, 10:27-57, Figs. 4A-4B; EX1002, ¶¶43-44. By analyzing the network, the system populates the security graph with properties describing cloud environment features. EX1002, ¶44. For example, the system can assess network paths and calculate a “reachability property” for each security object, which “defines if and how an object on the generated security graph can be reached from an external or internal network,” such as the internet. EX1005, Abstract, 11:61-12:10, 13:26-34, 15:15-24, Figs. 3A-3B. In addition, “security insights may be generated,” including descriptions of risky network configurations, such as rare or novel configurations or events, unauthorized connections, or connections displaying anomalous behavior. *Id.*, 12:11-14, 12:45-13:5; EX1002, ¶44.

Keren also teaches that the cybersecurity system includes a security graph utility for providing visualizations of the cloud environment. EX1005, 16:41-53; EX1002, ¶45. The security graph utility outputs a visual representation of the generated security graph (reproduced below) where security objects are

represented by vertex visualizations and relationships are represented by edge visualizations. EX1005, 16:54-67.



Id., Fig. 4A.

Keren teaches that the security graph utility includes interactive features.

Id., 17:1-3; EX1002, ¶46. For instance, a user may click on a vertex visualization to view information relating to the represented security object. EX1005, 17:3-18.

A user can also select to view a “security graph object list,” which lists selected security objects based on “mode-specific factors.” *Id.*, 17:52-18:1. As Keren explains, “[m]odes are selected list-organization profiles” that populate the security

graph object list in one or more configurations. *Id.*, 18:8-15. One example is “a ‘route’ mode,” which, when selected by the user, populates the security graph object list “to provide information describing a route between the specified objects.” *Id.*, 18:22-39, Fig. 4B; EX1002, ¶46.

B. Morgan (U.S. Patent No. 12,015,631, EX1006)

Morgan was filed March 30, 2021, and is therefore prior art under 35 U.S.C. §102(a)(2).

Morgan relates to systems and methods for “identifying instances of vulnerabilities on a computing network and generating a graph representing pathways that an attacking entity may take with respect to accessing one or more sensitive assets.” EX1006, Abstract; *see also id.*, 1:54-67, 5:54-63; EX1002, ¶47. To protect against the risk of outside entities gaining unauthorized access to information within a computing environment, Morgan teaches a risk management system that “receive[s] network information associated with a computing network including asset data, network architecture data, access rights data, and application configuration data.” EX1006, 1:6-18, 2:1-5; *see also id.*, 7:9-19, 11:48-56; EX1002, ¶¶48-49. The system also “receive[s] or otherwise identi[fies] a plurality of vulnerability instances for the computing network,” including “any problem or issue that has been called out with respect to a piece of software or a configuration (e.g., a device configuration, an account configuration, and application

configuration,” such as CVEs. EX1006, 2:5-7, 3:56-4:8; *see also id.*, 7:20-27, 11:66-12:12 (vulnerabilities can include “out of date software, vulnerable application policies, and any other network information that represents a known vulnerability”). Using this data, the risk management system builds a “threat graph” that includes “a plurality of pathways between an attacking entity (or multiple attacking entities) and one or more sensitive assets.” *Id.*, 2:7-15; *see also id.*, 14:46-60, 15:3-15, 15:50-57; EX1002, ¶50. The graph includes a plurality of nodes representing “a level of access or privilege” to an asset (e.g., user, group, or administrative access) and a plurality of edges connecting the nodes, which represent “escalations” that can be used by an attacker, such as a vulnerability instance. EX1006, 4:9-27, 4:36-49; *see also id.*, Abstract, 4:50-67, 6:11-21, 15:39-43, Figs. 3A-3C.

Morgan explains that the risk management system identifies attack paths “based on identified vulnerabilities that correspond to associated likelihoods that a given edge will be used by an attacker to potentially gain access to a sensitive asset.” *Id.*, 3:7-12; *see also id.*, 7:28-44; EX1002, ¶51. For example, one simplified example (reproduced below) identifies paths that an attacker can traverse within the network (e.g., red path) to gain access to an asset (e.g., first asset 308a). EX1006, 5:14-32, 12:44-13:43.

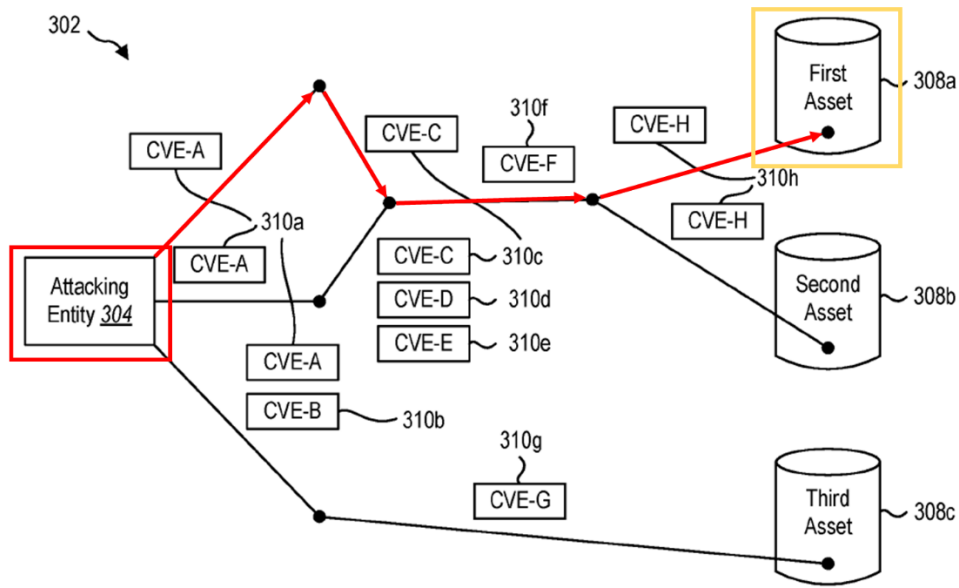


FIG. 3B

Id., Fig. 3B (annotated).

By successively exploiting vulnerabilities present in hosts on the network (e.g., the CVEs represented by edges), the attacker can gain increasing access (e.g., increasing privileges or permissions, represented by nodes) to access the target asset. *Id.*, 4:36-49, 13:8-31; *see also id.*, 13:66-14:17, 14:58-16:38, 16:57-66 (vulnerabilities are “associated with any level of access (represented as a node) within th[e] host that could be compromised by exploiting” vulnerable software on the host), Fig. 4A; EX1002, ¶52.

Morgan teaches presenting the threat graph in a graphical user interface, allowing a user to view the paths that an attacker can use to move within the computing network. EX1006, 14:18-35, Fig. 4B; EX1002, ¶53. By visualizing

attack paths, Morgan teaches the user can better understand where weaknesses exist in the network and where to efficiently focus remediation efforts. EX1006, 15:50-57, 19:15-34, 19:55-20:7; *see also id.*, 3:12-15 (system aids “in determining potential security risks to the computing network”), 10:63-11:29.

XI. GROUND 1: CLAIMS 1-20 WERE OBVIOUS OVER KEREN AND MORGAN

The combination of Keren and Morgan teaches, suggests, or makes obvious all limitations of claims 1-20 as a whole. Keren teaches a cybersecurity system that determines and analyzes the network topology of a cloud environment. *Supra*, §X.A (Keren summary); EX1002, ¶54. The system identifies security objects in the environment and determines their network relationships. *Id.* The system then uses this information to analyze network paths to calculate the reachability of the security objects and generate security insights describing risky network configurations. *Id.* The analysis is presented to a user in a graphical interface, which provides visualizations of the overall topology of the cloud environment, including the network paths to and from the security objects in the network. *Id.* The interface also includes interactive features that allow the user to select a security object to view object-specific properties of the selected security object, including visualizations that illustrate the network path for the selected object. *Id.*

Morgan teaches that analysis of risk present in a computing environment can be further improved by analyzing the environment’s network paths to identify the

specific paths an attacker can exploit. *Supra*, §X.B (Morgan summary); EX1002, ¶55. Morgan also teaches providing identified attack paths as visualizations to a user, which improves risk prioritization and remediation efforts for the user. *Id.* In view of Morgan's teachings, a POSA would have had reason to include attack path visualizations with Keren's system such that, when a user selected a security object to view object-specific information, the system would analyze the network paths to and from the selected security object to identify the paths that could be exploited by an attacker and output those paths as attack vector visualizations. *Infra*, §XI.A; EX1002, ¶56.

A. Reasons to Combine Keren and Morgan

As detailed more below, a POSA would have had reason to add functionality to a system like Keren's that would output visualizations of the specific network paths for a security object that could be compromised by an attacker outside of the cloud environment because it would enhance the system's ability to identify security risks by providing additional insight into how outside threats can enter a network and impact assets within network paths. EX1002, ¶57. The POSA also would have recognized that these attack path visualizations would aid the network administrator in deciding where remediation efforts can be efficiently focused. *Id.* The POSA would have understood that this functionality could be readily integrated into Keren's system by allowing the user to select a security object to

view the paths to and from the selected security object that the system identifies as possible attack vectors. *Id.*; *see also infra*, §§XI.B.7-9.

As an initial matter, the references are analogous art. Keren describes cybersecurity systems and methods for generating and outputting network graphs and path analysis to aid in the administration of security objects in a cloud environment. *See, e.g.*, EX1005, Abstract, 1:16-18, 2:34-53, 6:47-51. Morgan teaches systems and methods for generating visualizations of vulnerable pathways that an attacker may exploit to access assets in a network, such as a cloud environment. EX1006, Abstract, 1:54-67. Both references are thus in the same field as the '154 patent and are pertinent to issues addressed by the '154 patent. EX1001, 1:16-19, 45:36-57; EX1002, ¶58.

In addition, a POSA would have had reason to include attack path visualizations, as taught by Morgan, in a graphical user interface system like Keren's to help improve the security posture of the cloud environment managed by the system by more accurately identifying the risks of an outside attacker entering and moving along assets in the network. EX1002, ¶59. Keren recognizes that organizations' networks have been "increasingly vulnerable to cyber-threats," which has led to a need for tools that allow for effective management of assets and "provide granular, comprehensible representations of network information." EX1005, 1:22-29, 1:36-49, 2:34-42; EX1002, ¶59. Keren therefore describes a

cybersecurity system that “provide[s] network information which describes the role of an individual entity within such a network or a cloud environment, as well as the vulnerabilities presented by the entities’ placements within the network configuration.” EX1005, 2:42-55.

The system taught by Keren identifies the assets (or “security objects”) within the cloud environment and their relationships and generates security graphs of the overall network topology. *Id.*, 9:22-27, 10:27-39, 10:49-57, Figs. 2, 4A; EX1002, ¶60. The system further analyzes the network paths to and from security objects to determine object-specific properties. EX1005, 11:61-12:12, 13:47-53, 14:31-33, 15:15-24, Figs. 3A-3B, 5. For example, Keren teaches the properties include an object’s “reachability property,” which can describe the communication paths that outside sources (e.g., the internet) can reach the object. EX1005, 12:4-10, 13:26-61, 19:66-20:12, Figs. 3A-3B. From these properties, Keren teaches that the system also generates security insights into the cloud environment’s current state to aid the network administrator. *Id.*, 2:34-55, 12:11-13:5.

As discussed above, a POSA would have appreciated that a security object’s reachability in a network path informed a network administrator of the object’s exposure to outside sources, such as the internet, which could indicate risk. See *id.*, 12:62-13:5, 19:34-20:12, Fig. 5; *supra*, §IX. However, the POSA also would have recognized that a reachable path did not necessarily mean that an outside

attacker could use the path to access objects within the path. *Supra*, §IX; *see also* EX1006, 3:4-19; EX1007, ¶28; EX1002, ¶¶35-36, 61.

Morgan teaches that risk assessments can be beneficially improved by identifying and providing as visualizations the specific paths that can be traversed by an attacker. EX1002, ¶62. Like Keren, Morgan acknowledges that the recent growth and complexity of computer networks has resulted in “increasing quantities of information, including sensitive information, [to] be at risk.” EX1006, 1:12-18. However, “[u]nderstanding where and how to implement ... security improvements” that better protect this information “can become complicated, particularly where a computer network may have hundreds of thousands of vulnerable points that need to be addressed.” *Id.*, 2:26-29. Morgan teaches that simply identifying vulnerabilities can be insufficient because “not all known vulnerabilities are necessarily important to fix or provide a significant boost to security of a network system.” *Id.*, 2:35-53. Thus, to improve risk evaluation, Morgan teaches analyzing the network paths within a computing environment and identifying the specific paths that, based on identified vulnerabilities, correspond to pathways that could be used in an attack. *Id.*, 1:60-67, 3:7-12, 12:44-63, Figs. 3A-3B; *see also id.*, 2:1-7, 7:9-27, 15:3-49. A POSA would have recognized that this identification would provide an improved assessment of risk because the analysis would illustrate the cumulative effects of vulnerabilities. *Id.*, 10:63-11:29 (attack

paths “represent material improvements to conventional network security systems that are often limited to diagnosing vulnerabilities to a network based on likelihood of infiltration of the particular vulnerabilities”), 15:54-57; *see also* EX1009, iv (attack path analysis “is used to maximize the security of enterprise systems” and “evaluate and strengthen the overall security of enterprise networks”); EX1002, ¶62.

More specifically, a POSA would have recognized that outputting attack vector visualizations would provide additional insight into how an attacker could access the cloud environment through a network path and the overall impacts to security objects along the path. EX1002, ¶63. Keren recognizes a need to inform administrators of potential risk to assets, including risks that “may not be detectable based on the analysis of individual objects.” EX1005, 12:62-13:5 (describing examples); *see also id.*, 1:22-35 (acknowledging “attackers may seek to identify and exploit [vulnerabilities] to gain access to sensitive systems and data”), 2:49-53; EX1002, ¶63. Keren also teaches that the properties of a security object affect how reachable a downstream object is from an outside network. *Id.*, 15:25-33 (object’s reachability depends on “reachable properties of all other objects in the path”), 18:59-19:18, 19:34-20:12, Fig. 5 (illustrating public proxy limits traffic forwarded to database). Thus, Keren teaches performing analyses that

comprehensively consider the properties of objects within a network path.

EX1002, ¶63.

Morgan teaches that attack vector visualizations enable the network administrator to understand how an attacker can both enter a network and move in it to access target assets. EX1006, Abstract (system “identif[ies] pathways that an attacker is likely to use in accessing the sensitive assets(s)”), 3:23-25, 5:14-32, 7:40-44, 8:40-56, 13:66-14:17, 20:3-7, 20:23-62 (identifying “possible attack vectors” to sensitive assets), Figs. 4A-4B; *see also* EX1009, 6; EX1010, Fig. 3; *supra*, §IX; EX1002, ¶¶64, 126 n.4. Thus, a POSA would have appreciated that providing attack path visualizations in Keren’s system would further Keren’s stated need of providing “granular, comprehensive representations of network information” because the visualizations would improve identification of specific paths, and the assets within those paths, that are at risk to outside attack. EX1005, 2:34-55 (stating desire to “describe[] the role of an individual entity within such a network or a cloud environment, as well as the vulnerabilities presented by the entities’ placements within the network configuration”); EX1002, ¶64; *see also* *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 420 (2007) (“[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.”).

A POSA would have also recognized that providing attack vector visualizations would enable better network administration by improving remediation activities. EX1002, ¶65. Morgan teaches that by visualizing possible attack paths and their overall impacts, the network administrator can make more informed decisions for remediation efforts. EX1006, 14:61-15:2, 15:54-57 (analysis may be used to “generally prioritize vulnerabilities and remediations”), 19:4-14; *see also id.*, 13:55-65 (providing example); EX1007, ¶29 (attack graphs “can be used to evaluate fixes of vulnerabilities”); EX1009, 20-22 (attack graphs enable “system administrators to decide among the different risk mitigation options”). For example, a POSA would have appreciated that knowledge of how an attacker could access a given security object and the downstream consequences to other objects would provide valuable insight into which fixes would result in better network protection. *See, e.g.*, EX1006, 13:55-65, 18:33-48 (teaching vulnerability remediation based on association with multiple pathways), 19:4-19 (deprioritizing vulnerability fix because it “is not located on a viable attack path leading to a sensitive asset”); EX1009, 20-21 (consideration of patches for a given asset and their effect on the risk of compromise for other assets); EX1002, ¶65.

Thus, a POSA would have been motivated to configure Keren’s system to allow the user to select a security object to view object-specific information visualizing the object’s network paths that the system identifies as attack vectors so

that the user can view how outside threats can access the security object and impact other objects within its network paths, which, in turn, would enable better insight for remediations. EX1002, ¶66.

Further, arriving at the claims involved using known elements according to known functions to achieve predictable results. *KSR*, 550 U.S. at 416-17. As explained above, calculating and providing visualizations of attack vectors, as taught by Morgan, was well-known and predictable. *Supra*, §IX; EX1002, ¶¶34, 37-39, 67. POSAs were familiar with the various modeling techniques and understood how to visualize identified paths to a network administrator. *See, e.g.*, EX1006, Abstract (systems “use graph theory to generate or otherwise identify pathways that an attacker is likely to use”), 8:27-30; EX1007, ¶73 (known processing data to generate visualizations); EX1009, 8-9 (known tools); EX1010, 4-10 (known analysis methods); EX1011, 2-11 (same); EX1002, ¶67. The combination uses these techniques to predictably perform their known functions since the references describe analogous systems for network analysis, and using Morgan’s techniques of analyzing network information to identify attack vectors and visualizing those paths in a graphical user interface like that of Keren would not meaningfully change their function or result. EX1002, ¶67.

A POSA would have reasonably expected success in combining the references to arrive at the claims. EX1002, ¶68. A POSA would have recognized

that Keren's system includes the foundational framework (e.g., network architecture identification, network path and reachability analysis, and an interactive graphical user interface) that would have been needed to identify and visualize likely attack paths for a security object. See EX1006, 14:46-60 (attack path analysis uses network architecture knowledge), 15:2-15, Fig. 2; EX1007, ¶35 (determining network topology to generate attack graphs); EX1009, 8 (known methods compute "network reachability"); EX1010, 2 (teaching "information about network topology, vulnerability, network configuration, and network connectivity should be first collected" and "reachability analysis" should be conducted), Fig. 2; EX1002, ¶68. As Morgan demonstrates, POSAs also appreciated additional data that would facilitate attack path analysis and were familiar with the routine methods for collecting the data. EX1006, 7:9-27, 12:3-7 (vulnerabilities can be identified using "a conventional or off-the-shelf vulnerability scanner"), 14:46-60; *see also* EX1010, 2-3 (collecting vulnerability information, such as CVEs). And, as explained above, POSAs were familiar with the known methods for analyzing network attack paths and visualizing the identified paths to a user. See, e.g., EX1006, Abstract, 8:27-30; EX1007, ¶73; EX1009, 8-9; EX1010, 4-10; EX1011, 2-11; *supra*, §IX. A POSA therefore would have been familiar with the applied techniques, and the combination would not

have presented meaningful technical challenges or produced unexpected results.
EX1002, ¶68.

B. Independent Claims

1. Preambles

To the extent the preambles are limiting, the combination of Keren and Morgan teaches them. EX1002, ¶¶69-70. Claim 1 recites a “graphical user interface system for providing forward and backward facing attack vector visualizations, the system comprising.” Claim 14 recites a “method for generating a graphical user interface for providing forward and backward facing attack vector visualizations, the method comprising.” The preamble of claim 20 recites a “non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations comprising.”

Keren teaches a graphical user interface system and corresponding methods for generating a graphical user interface in the form of a cybersecurity system, which “is a system, device, or component,” that “provide[s] one or more network analysis functionalities including, without limitation, network analysis, traffic analysis, object querying, graph generation, and the like....” EX1005, 6:47-56. As detailed more below, the cybersecurity system includes a security graph utility that

is used to output forward and backward facing vector visualizations of a cloud environment to a user. EX1002, ¶71.

Specifically, the cybersecurity system assesses “security objects” (e.g., virtual machines, databases, firewalls, load balancers, proxy servers, etc.) in a cloud environment. EX1005, Abstract; *see also id.*, 1:15-18, 3:6-39, 4:31-43, Figs. 1A-1B, claims 1, 11. The described system analyzes the security objects and their properties, automatically generates security graphs describing the objects and their relationships, and provides network insights of the cloud environment. *See id.*, Abstract, 1:15-18, 2:24-55, 4:53-55, 6:47-56; EX1002, ¶72.

The analyses performed by Keren’s system are visually outputted to a user. EX1002, ¶73. For example, Keren teaches the cybersecurity system generates visualizations that are “presented through a security graph utility,” which “may be an application, interface, or other, like means of providing a visual representation of a security graph, and the like, where the provided security graph visualization ... may include various interactive features.” *Id.*, 16:41-49, Fig. 4A; *see also id.*, 16:49-53, 21:59-62. As shown below, the security graph utility includes a “security graph visualization 400,” which is a “visualization representing a network” where “the various objects, systems, devices, components, and the like, of the network are represented as vertex visualizations 410” and their corresponding connections are shown by “edge visualizations 420.” *Id.*, 16:54-62;

EX1002, ¶74. The paths between security objects as illustrated in the figure would have been understood to be examples of vector visualizations of the possible communication paths within the cloud environment. EX1002, ¶74; *cf.* EX1001, 12:62-13:2 (describing vectors as “connecting the plurality of systems and devices” in a cloud infrastructure “based on the networking configuration”). These vector visualizations would have been understood to include forward and backward facing visualizations because they visualize the network paths to a given security object and from the object to other downstream objects within the path. EX1002, ¶74; *see also infra*, §§XI.B.7-8.

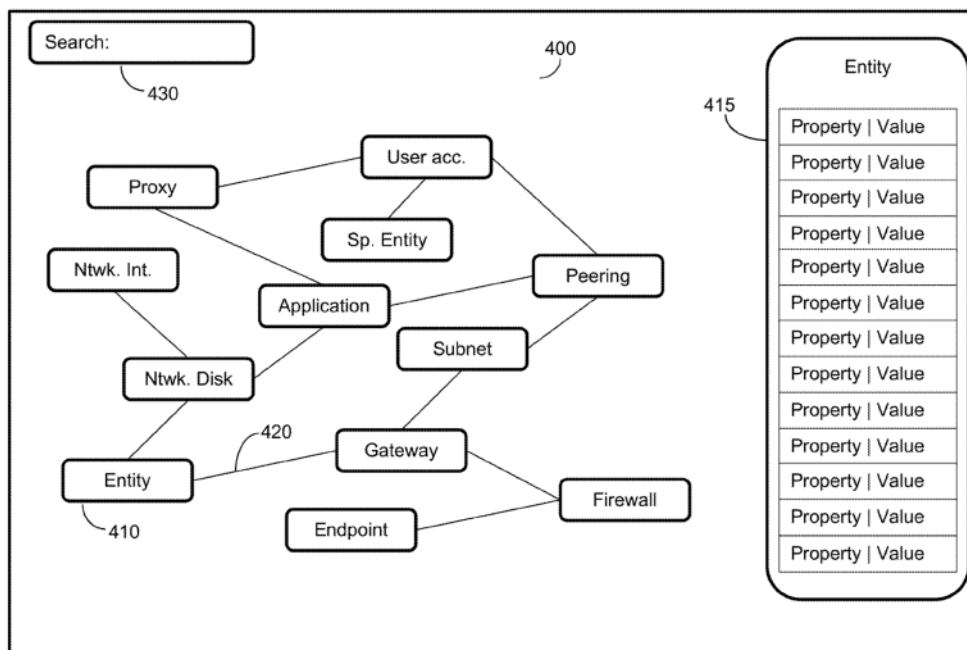


FIG. 4A

EX1005, Fig. 4A.

Keren also teaches the security graph utility can provide additional visualizations of specific network properties and paths through interactive features. *Id.*, 17:1-3; EX1002, ¶75. For example, a user may click on a vertex visualization 410 to display properties specific to the represented security object in a vertex overview pane 415. *Id.*, 17:3-18. The security graph utility may also include a “security graph object list 450” that “list[s] security objects 470” based on “mode-specific factors.” *Id.*, 17:39-18:1. “[W]here a mode is selected,” the security graph object list is “populated based on the specified mode or modes” relating to selected security objects, which can be “routing paths, object utilization or availability descriptions, other, like, configurations, and any combination thereof.” *Id.*, 18:1-22.

One example is shown below, where a user has selected “a ‘route’ mode,” resulting in a security graph object list 450 that shows “objects occupying a data path between a first object 470-1 and a destination object 470-n,” allowing the user to view the transmissions between the objects. *Id.*, 18:27-34. A POSA would have understood that this illustrated another example of forward and backward facing vector visualizations because it visualizes the network path connecting specific security objects from a destination or source. EX1002, ¶76; *cf.*, EX1001, 12:62-13:2.

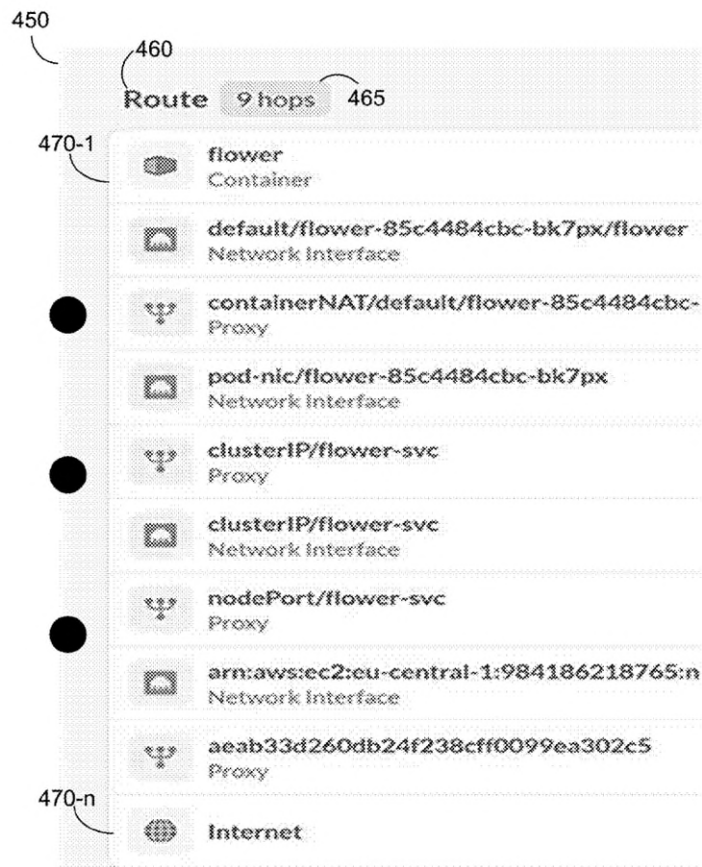


FIG. 4B

EX1005, Fig. 4B.

While Keren teaches a graphical user interface system that provides visualization of a cloud environment's network configuration, including forward and backward facing vector visualizations illustrating network paths, Keren does not expressly disclose that the visualizations are "attack" vector visualizations. EX1002, ¶77. However, as discussed above, a POSA would have found it obvious to include attack vector visualizations in a graphical user interface system, as taught by Keren, that allow the user to selectively view the specific network paths

that the system identifies as attack vectors, as taught by Morgan, with respect to a specific security object. *Supra*, §XI.A; EX1002, ¶77.

Specifically, as explained more below (*infra*, §§XI.B.7-8), Morgan teaches analyzing objects in a computing environment to identify the network paths that an outside attacker would likely use to access assets. EX1006, Abstract, 5:14-32, 7:40-44, 8:40-56, 20:56-61 (identifying “possible attack vectors”), Fig. 4B; EX1002, ¶77. For example, as illustrated below, the analysis determines vectors by which an attacker can enter a host (e.g., host shown on the left) and move through the network toward other downstream hosts (e.g., host shown on the right). EX1006, 13:66-14:17, 20:3-7; *see also infra*, §§XI.B.7-8; EX1002, ¶78.

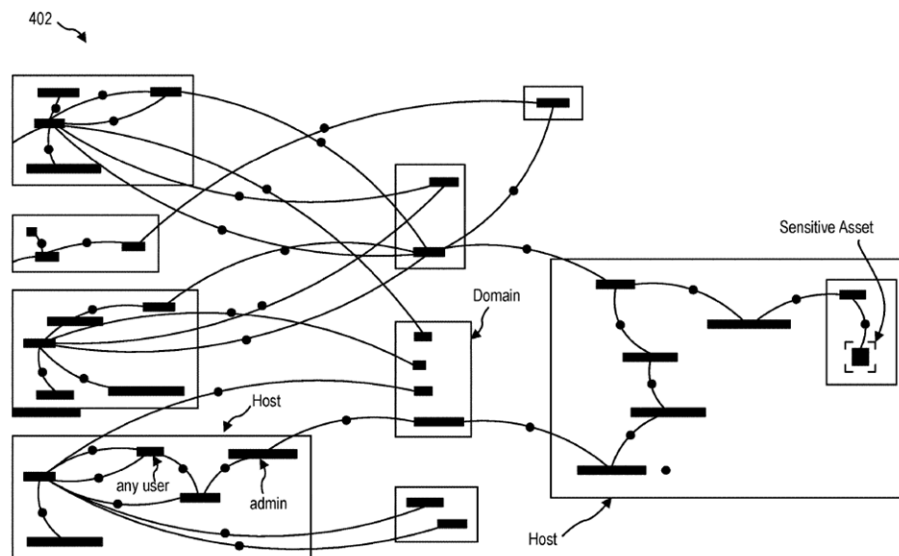


FIG. 4A

EX1006, Fig. 4A.

As further detailed below (*infra*, §XI.B.9), consistent with Keren’s teachings of visualizing network paths, Morgan teaches presenting attack vector visualizations to a user. EX1006, 19:55-20:7, Fig. 4B; EX1002, ¶79. As explained above, a POSA would have found it obvious to provide attack path visualizations, as taught by Morgan, for a security object selected by the user in Keren’s system so that the user can view the likely network paths that an attacker could take to compromise the selected object and the downstream impacts to other objects within the path. *Supra*, §XI.A. Thus, the combination of Keren and Morgan teaches a “graphical user interface system for providing forward and backward facing attack vector visualizations” and corresponding methods for generating the graphical user interface system, as recited. EX1002, ¶79.

The combination of Keren and Morgan also teaches a “non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform” the elements of claim 20. EX1002, ¶80. Keren teaches that the cybersecurity system can “execute one or more instructions, methods, processes, and the like.” EX1005, 6:51-56, Figs. 2-3B. The cybersecurity system includes a “processor circuitry 610 coupled to ... a storage 430.” *Id.*, 20:61-67; *see also id.*, 4:3-4, Fig. 6. Keren teaches that the processing circuitry may be “one or more hardware logic components and circuits,” such as a processor. *Id.*, 21:1-12. Moreover, the storage

may be a non-transitory computer-readable medium (e.g., “magnetic storage,” “optical storage,” or “any other medium which can be used to store the desired information”), which stores software instructions that “when executed by the processing circuitry 610, cause the processing circuitry 610 to perform the various processes” taught by Keren. *Id.*, 21:16-33. Therefore, a POSA would have understood that execution of the instructions contained on the medium would “cause the at least one processor to perform” each of the operations recited in claim 20. EX1002, ¶¶80-81; *infra*, §§XI.B.3-9.

2. Element 1.i

Keren teaches this element, which recites “at least one processor configured to....” As discussed above, Keren teaches that the cybersecurity system includes a processor used to execute instructions to perform the described methods. EX1005, 20:61-67, 21:1-12, 21:16-33; EX1002, ¶¶82-83.

3. Elements 1.1, 14.1, and 20.1

Keren teaches these elements, which recite “[identify/identifying] assets in a cloud environment.” EX1002, ¶84.

The ’154 patent explains that an “asset” is “a system or device” and may be “a virtual machine, a network appliance, a storage appliance, a computer instance, or an engine instance.” EX1001, 10:26-30, 47:25-42, claims 3, 16; EX1002, ¶85. The cybersecurity system of Keren identifies the same types of assets in the form

of “security objects.” EX1002, ¶86. Keren explains the system analyzes a “cloud environment” (illustrated below), which “may include a number of cloud computing platforms, 104-1 through 104-n ..., where a cloud platform may include multiple security objects, 105-1 through 105-n....” *Id.*, 4:33-43; *see also id.*, 4:60-65.

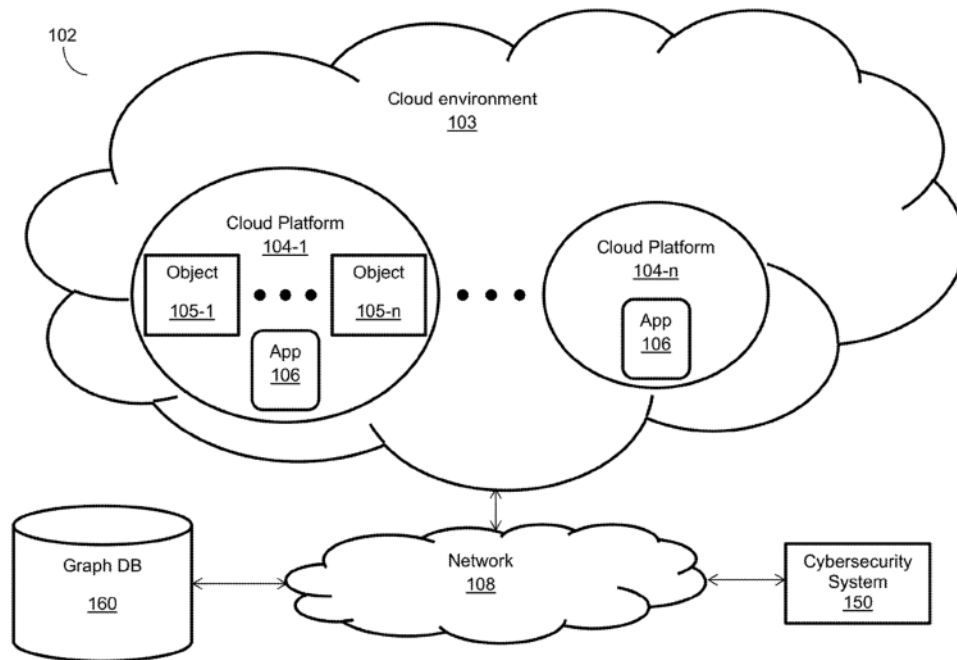


FIG. 1A

Id., Fig. 1A.

The security objects are “objects, systems, devices, components, applications, entities, and the like,” that operate within the cloud environment. *Id.*, 5:20-32; *see also id.*, 5:20-6:19; EX1002, ¶87. Examples of security objects include virtual machines and other compute and engine instances, such as containers, serverless applications, and other cloud processing and management

systems. EX1005, 4:27-51, 5:42-44, 6:13-18. The security objects also include network appliances, such as proxies, firewalls, gateways, and load balancers, and storage appliances, such as file servers and databases. *Id.*, 5:35-39, 5:42-44, 6:13-18; *cf.*, EX1001, 34:48-49 (a network appliance may be “a load balancer, a firewall, a proxy, or a router”).

Keren further teaches that the system identifies the security objects. EX1002, ¶88. To “construct[] security graphs,” “security objects are identified, and security object data is collected” through an API query. EX1005, 9:21-44, Fig. 2; *see also id.*, 9:56-10:10 (data includes “object types, object names or unique identifiers (IDs)”), 10:11-14 (collected data “may include collection of the identities of all objects”); EX1002, ¶¶88-89.

4. Elements 1.2, 14.2, and 20.2

The combination of Keren and Morgan teaches these elements, which recite “[identify/identifying] risks associated with each of the identified asset [*sic*].” EX1002, ¶90.

Keren teaches that the cybersecurity system identifies risks associated with the identified security objects. EX1002, ¶91. Specifically, the system generates “security insights,” which are “natural-language representations of aspects” of the constructed security graph. EX1005, 12:11-14. The security insights may describe risks associated with the security objects, such as rare or novel network

configurations or events, unauthorized connections, or anomalous connections. *Id.*, 12:26-55. For example, a security insight may describe that “VM thirty normally connects to load balancer twenty and firewall eight but is currently only connected to load balancer twenty.” *Id.*, 12:57-61. A POSA would have understood this insight as identifying a risk associated with the identified security object (VM thirty) because the virtual machine is no longer connected to a network security device designed to prevent unauthorized access to the asset. *See, e.g.*, EX1012, 17, 37 (firewalls strengthen network security perimeter); EX1013, ¶33 (using firewalls to prevent unauthorized asset exploitation); EX1014, ¶¶22-25 (discussing use of passive countermeasures, such as firewalls, to protect against vulnerability exploitation); EX1002, ¶91. Another example includes an insight notifying that “objects E, a database, and F, an administrator interface, are currently exposed to external networks.” EX1005, 12:61-13:5. A POSA would have understood this insight identified a risk that identified assets containing sensitive information or providing privileged access were exposed to an external network (e.g., the internet). EX1002, ¶91; *cf.*, EX1001, 37:25-27 (“[T]he Internet at large may be considered to be a potentially malicious source.”).

Morgan also teaches identifying risks, such as vulnerabilities like CVEs, that are associated with each of the devices in a computing environment. EX1002, ¶92. Specifically, Morgan teaches that, to identify attack paths, the system “identif[ies]

a plurality of vulnerability instances,” which include “any problem or issue that has been called out with respect to a piece of software or a configuration” on a host device. EX1006, 2:1-7, 3:56-62 (e.g., “a known problem that exists with respect to a particular browser or operating system”); *see also id.*, 19:46-54 (identifying hosts and “associat[ing] the hosts with the vulnerability data”); EX1002, ¶92. Morgan explains that the vulnerabilities can include CVEs that “are discovered by applying a vulnerability scanne[r] (e.g., a conventional or off-the-shelf vulnerability scanner) that scans the network architecture....” EX1006, 3:62-64, 11:66-12:12; *see also id.*, 16:34-38. Morgan teaches this vulnerability data facilitates the identification of attack paths. *Id.*, 16:27-38, 16:52-66 (“a host associated with software impacted by the [identified] vulnerability may be a target” for attack path analysis), Fig. 3B; *see also id.*, EX1010, 3, Fig. 3, Table 1; EX1002, ¶93; *supra*, §IX. Thus, in view of Morgan, a POSA would have also sought to identify risks that included vulnerabilities like CVEs associated with each of the identified security objects in Keren’s system to identify and output attack path visualizations to the user. *Supra*, §XI.A; EX1002, ¶¶93-94.

5. Elements 1.3, 14.3, and 20.3

The combination of Keren and Morgan teaches these elements, which recite “[identify/identifying] relationships between at least some of the identified assets,

the relationships including at least one of a trust, a network connectivity, or a mechanism of network proxying.” EX1002, ¶95.

Keren teaches that the system further identifies “relationships between security objects,” which “are descriptions of the various connections between the [identified] security objects.” EX1005, 10:49-52, Fig. 2 (step S230); EX1002, ¶96. These relationships include at least one of a trust, a network connectivity, or a mechanism of network proxying, as recited. EX1002, ¶¶96-97.

For example, Keren explains that the relationships “may describe aspects of the connections between objects” (i.e., network connectivity). EX1005, 10:52-57; EX1002, ¶96. The relationships may also be identified through “analysis of object and protocol code and rules.” EX1005, 10:58-11:10 (collected firewall data includes communication protocols), 11:56-60; EX1002, ¶97. As Dr. Stavrou explains, this analysis would further identify trust relationships or mechanisms of network proxying. EX1002, ¶97. For instance, by identifying protocol code and rules, the system would identify whether transmissions occurring between security objects were managed by secure communication protocols, such as encryption protocols (i.e., a trust relationship). *See, e.g.*, EX1017, 4:41-54; EX1018, ii-iii, 1; *cf.*, EX1001, 16:17-24 (a “trusted relationship ... may refer to a secure communication channel”); EX1002, ¶97. Moreover, as illustrated in Fig. 5 (reproduced below), the system may also identify mechanisms of network

proxying, such as a public proxy 540 that services traffic between the internet and a database 510 based on specific translation rules. EX1005, 18:40-43, 18:55-58, 19:56-20:12; EX1002, ¶¶98.

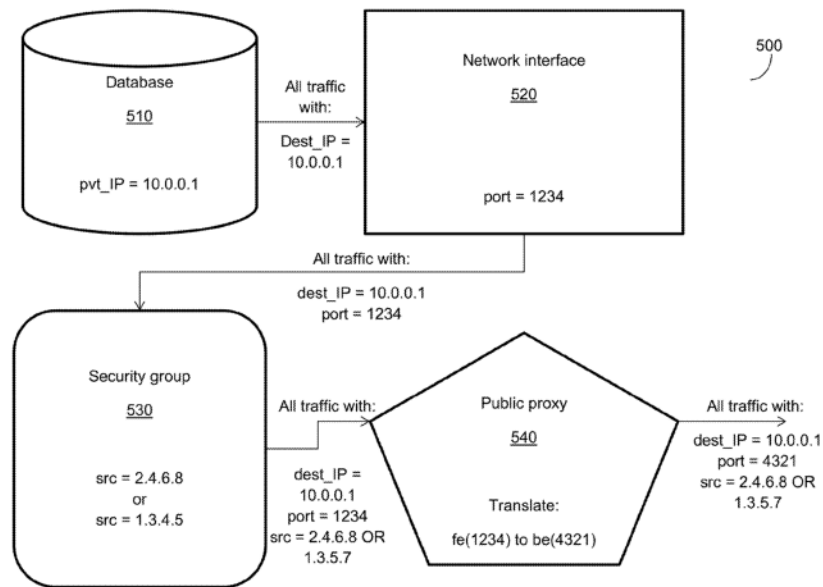


FIG. 5

EX1005, Fig. 5; *see also id.*, Figs. 3A (proxy mechanism between user account and application), 3B (proxy mechanisms between internet and container).

Morgan also teaches identifying relationships between network devices that include a trust relationship. EX1002, ¶¶99. To analyze attack paths, Morgan teaches gathering “access rights data,” such as “node data [and] permissions,” and “application configuration data,” such as “policies, application configurations, node configurations, [and] device configurations.” EX1006, 2:1-5, 7:9-19, Fig. 2. A POSA would have understood that this would include data relating to account

types (e.g., user or administrative accounts) and permissions for accessing or controlling an asset (i.e., a trust relationship). *Id.*, 5:14-32, 11:48-56, 14:46-54, 15:16-38, 23:20-23, claim 2; EX1002, ¶99. Morgan teaches that this information can be related as nodes in the attack vectors to show relationships between assets that an attacker can traverse. EX1006, 4:36-67, 15:16-20, 16:45-48. For example, a node may represent an administrator account on an asset that provides fully privileged access to other assets. *Id.*, 4:36-43, 4:54-57 (“[A]n administrator node that is fully connected may include edges connecting the administrator node to all or almost all nodes within a graph.”), Fig. 4B (illustrating connection between an administrator node of host to a domain). Thus, Morgan also teaches identifying relationships between assets that include a trust relationship, as recited. EX1002, ¶¶99-100; *cf.* EX1001, 16:15-27 (“trusted relationship” may be “an administration link”).

6. Elements 1.4, 14.4, and 20.4

Keren teaches these elements, which recite “[receive/receiving] an identification of a specific asset under investigation.” EX1002, ¶101.

Keren teaches that the system is configured to receive an identification of a security object selected by a user to view detailed information of the selected object. EX1002, ¶102. For example, as explained above (*supra*, §XI.B.1), the

system includes a “security graph utility” (reproduced below), which generates a “security graph visualization 400” of the cloud environment:

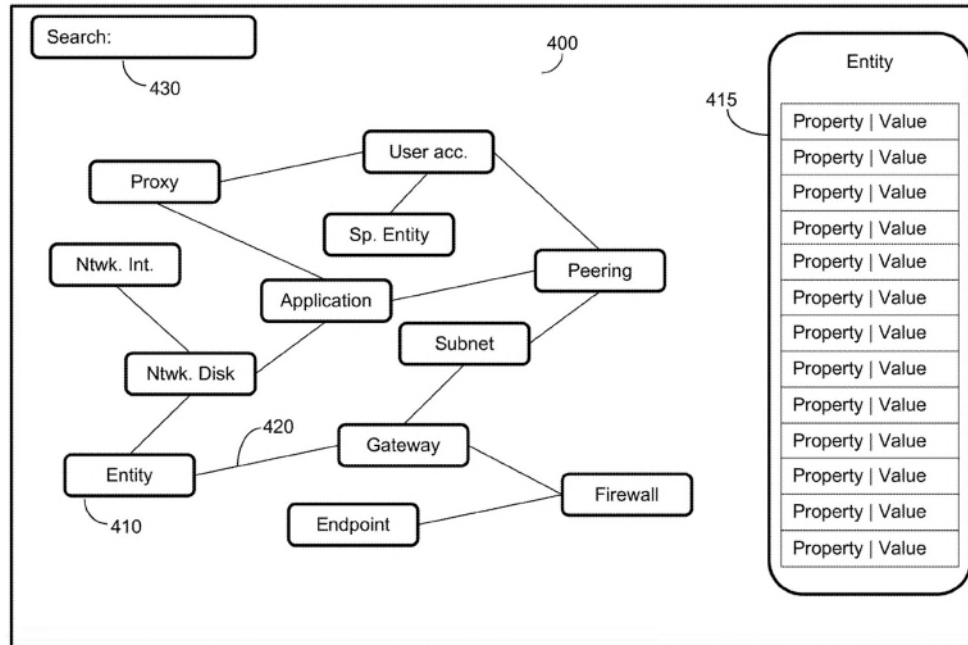


FIG. 4A

EX1005, 16:41-45, Fig. 4A.

The security graph visualization 400 allows the user to click on a vertex visualization 410, which represents a security object in the network (i.e., receiving an identification of a specific asset under investigation). EX1005, 16:54-17:8.

This may cause the system to generate a “vertex overview pane 415,” which “describ[es] various object data features” of the selected security object. *Id.*, 17:3-18; *see also id.*, 17:19-29 (system also includes “a search tool 300”); EX1002, ¶103.

The system also may provide a “security graph object list 450” as part of the security graph utility. EX1005, 17:58-63; EX1002, ¶104. The security graph object list can “list security objects 470 in one or more orders based on ... mode-specific factors” selected by the user. *Id.*, 17:63-18:1, 18:8-10. An example is reproduced below, in which a “route” mode has been selected:

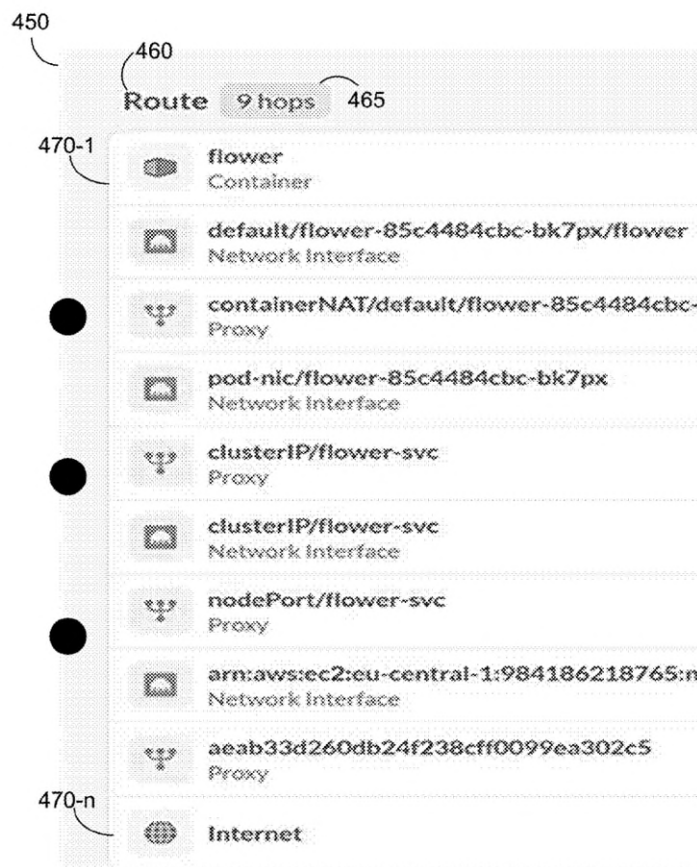


FIG. 4B

EX1005, 18:1-22, Fig. 4B.

As shown above, when a route mode is selected, a security graph object list is generated to show the network path between a first object 470-1 (a container)

and a destination object 470-n (the internet). *Id.*, 18:23-27; EX1002, ¶105. To generate this visualization, a POSA would have understood that, in addition to receiving the specific mode selected by the user, the system would also receive an identification of the security object selected by the user (e.g., the container) to view relevant network paths. *See* EX1005, 18:27-34 (“the security graph object list 450 is populated to provide information describing a route between the specified objects...”); EX1002, ¶105. Thus, Keren teaches that the system receives an identification of a specific asset under investigation (i.e., a security object selected by a user), as recited, so the user can view object-specific information, such as the object’s properties and network paths. EX1002, ¶106.

Keren contemplates that other types of object-specific network information may be outputted in response to a user’s selection. *See* EX1005, 17:46-51 (stating “other, like, modes and object 470 arrangements may be similarly applicable without loss of generality of departure from the scope of the disclosure”), 18:10-15 (modes may include “other, like, configurations”); EX1002, ¶106. As explained above, and detailed more below, a POSA would have had reason to output attack vector visualizations, such as taught by Morgan, in a system like Keren’s in response to receiving an identification of a security object under investigation so the user could view the identified attack paths to and from the selected security object. *Supra*, §XI.A; *infra*, §§XI.B.7-8; EX1002, ¶¶106-07.

7. Elements 1.5, 14.5, and 20.5

The combination of Keren and Morgan teaches these elements, which recite “[perform/performing] a forward analysis of the specific asset under investigation to identify at least one possible attack vector reaching the specific asset via a network outside the cloud environment.” EX1002, ¶108.

Keren teaches that the system performs a forward analysis of a specific security object to identify at least one possible vector reaching the object via an outside network in several ways. EX1002, ¶109. For example, Keren teaches that the system performs a forward analysis through the calculation of a security object’s “reachable” property, which “defines if and how an object on the generated security graph can be reached from an external or internal network, and/or an external or internal object.” EX1005, 13:26-31, Fig. 3A; *see also id.*, 12:4-7; EX1002, ¶109. “External means outside the cloud environment of the organization,” such as the internet. EX1005, 13:31-32, 13:66-14:1; *see also id.*, 15:50-58, 20:34-42. As one example, Keren teaches identifying a network path from a public proxy 540 to a database 510 and calculating the database’s reachability property with respect to the scope of internet-originating traffic that can reach the database. *Id.*, 18:40-58, 19:34-20:12, Fig. 5. Thus, Keren teaches performing a forward analysis of an asset to identify at least one possible vector

reaching the specific asset via a network outside the cloud environment. EX1002, ¶109.

In addition, as explained above in §XI.B.1, Keren's system provides forward and backward facing vector visualizations through the security graph utility. EX1002, ¶110. Specifically, the security graph visualization 400 provided by the utility shows forward facing vector visualizations of the network paths between security objects in the cloud environment. See EX1005, 16:54-67. As one example shown below, the visualization can include a forward network path (e.g., the red annotated path) reaching a specific object (e.g., an entity, annotated by the yellow box) from an object that is configured to service internet traffic (e.g., a proxy). EX1002, ¶¶110-11. A POSA would have understood, or at least found it obvious, that to provide these visualizations, the system would perform a forward analysis of the specific security objects in the visualization to identify at least one possible vector reaching the objects from outside sources. *Id.*, ¶111.

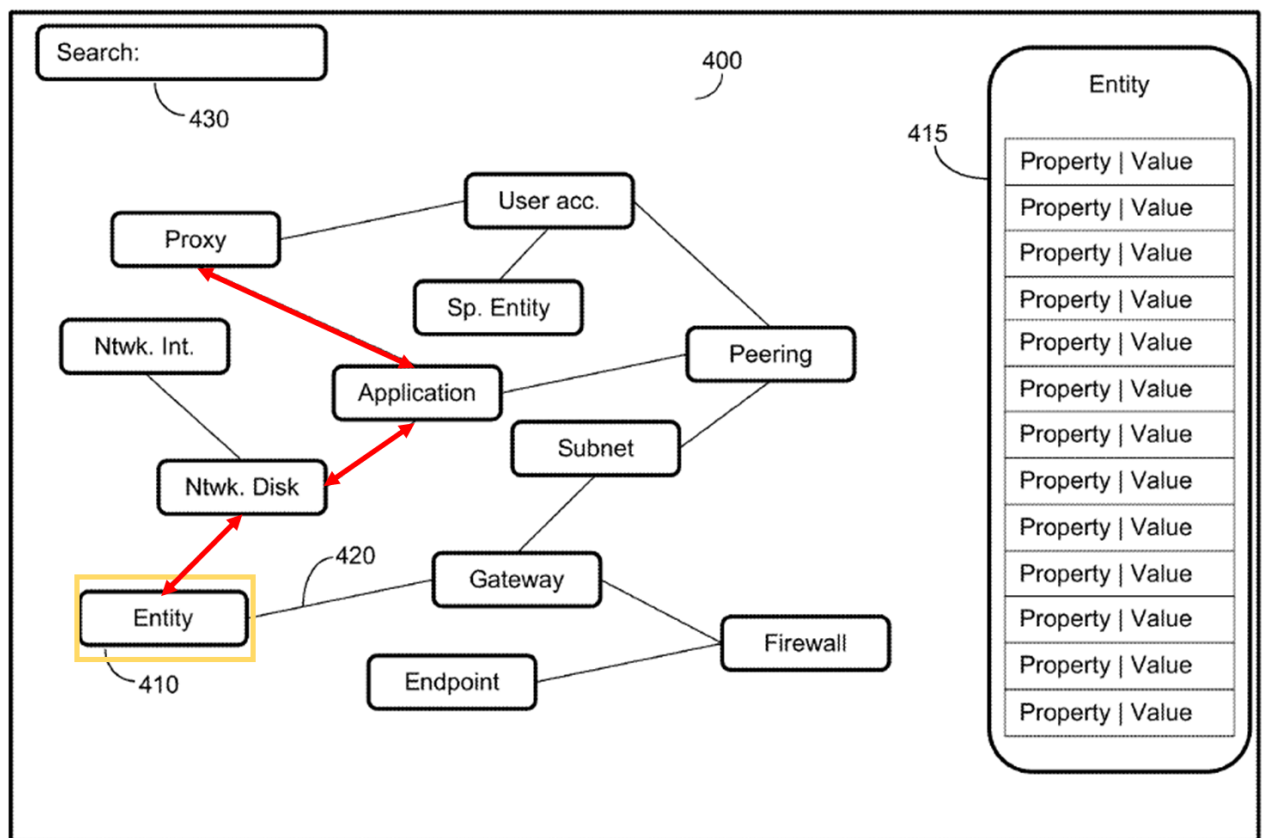


FIG. 4A

EX1005, Fig. 4A (annotated).

In addition, as explained above, Keren’s system may provide forward facing vector visualizations through a security graph object list that can visualize the route between the internet (i.e., a network outside the cloud environment) and selected security objects within a network path. EX1005, 18:23-34, Fig. 4B; *supra*, §§XI.B.1, XI.B.6. In response to the user’s selection, “the security graph object list 450 is populated to provide information describing a route between the specified objects.” EX1005, 18:27-30. To provide these visualizations, a POSA

would have understood, or at least found obvious, that when a user selected a security object to view the object's network paths, the system performs a forward analysis of the selected object to identify at least one vector reaching the selected object, including those reaching from an outside network, such as the internet. EX1002, ¶112.

As explained above, while the vectors identified by Keren show the paths by which a security object can be reached from an outside source (e.g., the internet), Keren does not explicitly disclose that the vectors are identified as “attack” vectors. EX1002, ¶113; *supra*, §XI.A. Nevertheless, a POA would have had reason to provide attack vector visualizations, such as a taught by Morgan, when a user selected a security object as taught by Keren. *Id.*

Morgan teaches performing an analysis that “define[s] pathways through which data may be processed or communicated and through which assets (e.g., sensitive assets) may be accessed by an attacking entity” (i.e., attack vectors). EX1006, 4:28-35; *see also id.*, 2:10-15 (identifying “a plurality of pathways between an attacking entity (or multiple attacking entities) and one or more sensitive assets”), 3:7-12 (identifying pathways that can “be used by an attacker to potentially gain access to a sensitive asset”); EX1002, ¶114. The analyses performed to identify these pathways include identifying pathways to a specific asset based on an attacking entity that is external to the network, which may be a

“cloud computing network.” EX1006, 1:54-60, 5:1-7, 11:57-65, 12:25-30, 16:52-66, 24:44-48 (attacking entity may be “an external attacking entity originating from outside the computing network”); EX1002, ¶115.

Morgan further teaches the analysis includes a forward analysis that identifies possible attack vectors reaching the specific asset from the external attacking entity. EX1002, ¶116. For example, as illustrated by the simplified attack graph reproduced below, the system can calculate a pathway (red annotation) from an attacking entity 304 (red box) to a first asset 308a (yellow box). EX1006, 12:44-50, Fig. 3A.

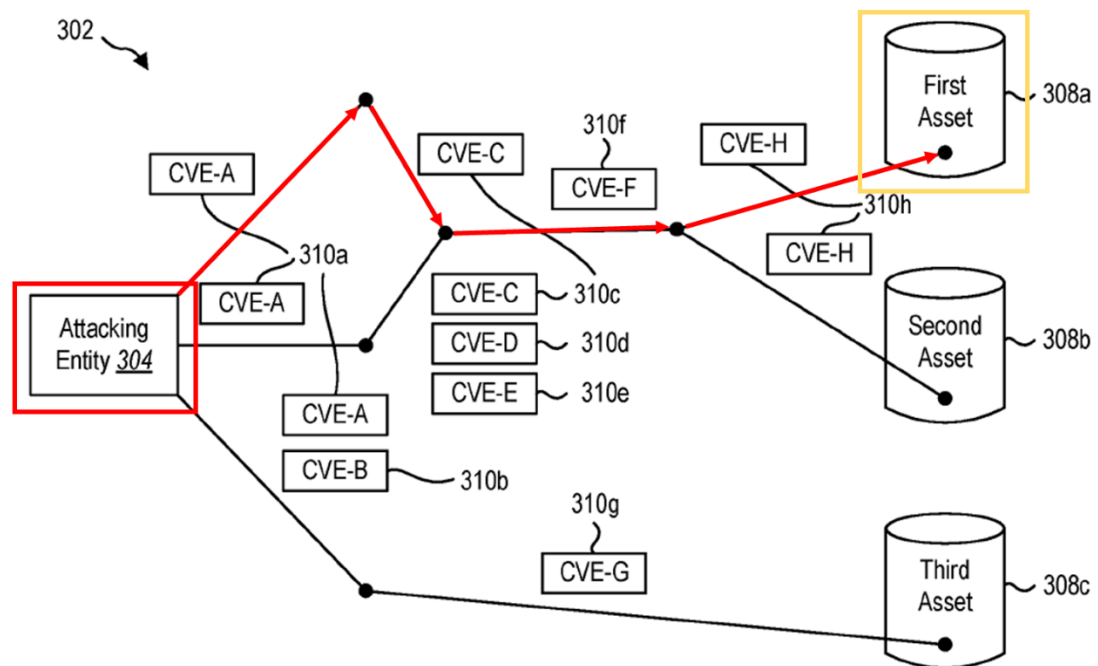


FIG. 3B

Id., Fig. 3B (annotated); EX1002, ¶116.

“[E]ach of the edges within the example graph may have an associated one or more escalations,” which represent successful exploitation of vulnerabilities.

EX1006, 13:8-17; EX1002, ¶117. Morgan teaches that a forward analysis is performed that identifies that an attacking entity can exploit a first vulnerability (e.g., CVE-A) to access a first node (e.g., a user account), and continue to exploit subsequent vulnerabilities until the entity gains access to the first asset 308a.

EX1006, 12:44-63, 14:7-9, 20:56-61. Thus, Morgan teaches performing a forward analysis to identify at least one possible attack vector reaching an asset via a network outside the computing network. EX1002, ¶117.

In view of the references’ combined teachings, when a user selected a security object to view attack path information for that object, a POSA would have understood, or at least found it obvious, that the system would perform a forward analysis of the selected object to identify at least one possible attack vector reaching the security object via a network outside the cloud environment, as recited. *Supra*, §XI.A; EX1002, ¶118 (citing EX1005, 18:23-34; EX1006, 11:30-47). A POSA would have appreciated that this analysis would illustrate the network path that an outside attacker could use to access the selected security object. EX1002, ¶¶118-19.

8. Elements 1.6, 14.6, and 20.6

The combination of Keren and Morgan teaches these elements, which recite “[perform/performing] a backward analysis of the specific asset to identify at least one exposure risk to one or more assets that is in a downstream of the specific asset, wherein the at least one exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset.” EX1002, ¶120.

Keren teaches that the system performs a backward analysis of a specific security object that identifies vectors reaching security objects that are in a downstream of the specific object. *Id.*, ¶121. For example, as described above, Keren teaches that the system provides backward facing vector visualizations via a security graph visualization. *Supra*, §XI.B.1. As one example illustrated below, these visualizations show the network path (annotated in blue) extending from the specific security object (e.g., the entity) to other downstream objects (e.g., the endpoint). *See* EX1005, 16:54-67; *see also id.*, 18:23-39. As discussed above for the forward analysis (*supra*, §XI.B.7), a POSA would have understood, or at least found obvious, that to provide these visualizations, the system would perform a backward analysis of the security objects shown in the graph visualization to identify the paths reaching other downstream objects. EX1002, ¶121.

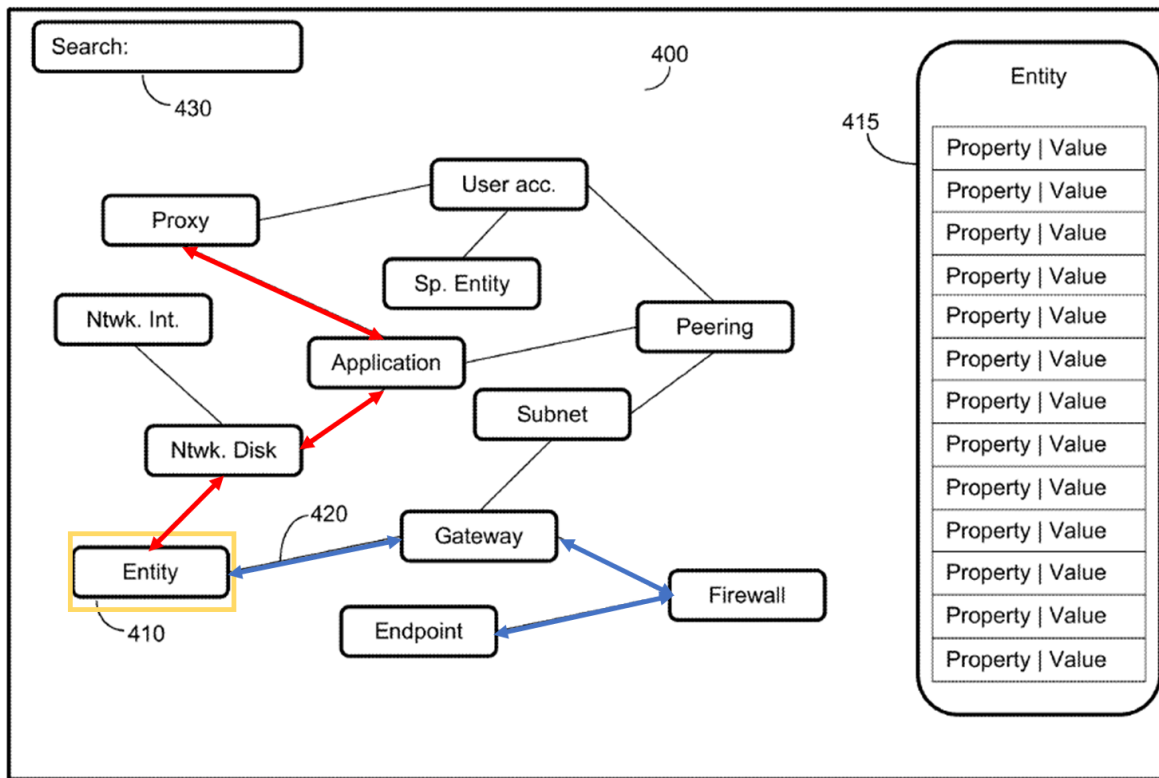


FIG. 4A

EX1005, Fig. 4A (annotated).

Further, as discussed above, Keren teaches determining reachable properties for security objects within the cloud environment, recognizing that the network properties of a specific security object in a network path affect the reachability of downstream security objects within the path. *Id.*, 18:44-58, 19:34-20:12; EX1002, ¶122 (detailing example shown in Fig. 5, where security objects inform the risk of exposure to external traffic for a downstream database object); *supra*, §§IX, XI.A, XI.B.7.

As additionally explained above, a POSA would have sought to include attack vector visualizations, as taught by Morgan, to allow a user to view the network paths that are identified as attack vectors for a selected security object in a system like Keren's. *Supra*, §XI.A; EX1002, ¶123. Morgan teaches that the identified attack vectors identify at least one exposure risk to one or more assets that is in a downstream of a specific asset, where the exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset. EX1002, ¶124.

Specifically, as Dr. Stavrou explains, based on the paths described in Morgan, a POSA would have understood that the identified attack vectors can include backward paths that an attacker can use to gain access into other assets exposed along the overall network path. *Id.* For example, as illustrated by the simplified attack graph reproduced below, after gaining access to the first asset 308a via a forward pathway (red annotation), a POSA would have understood that the attacking entity 304 may further leverage its position in the network to move from the first asset 308a to a second asset 308b by exploiting vulnerabilities along the network path (blue annotation). *Id.*

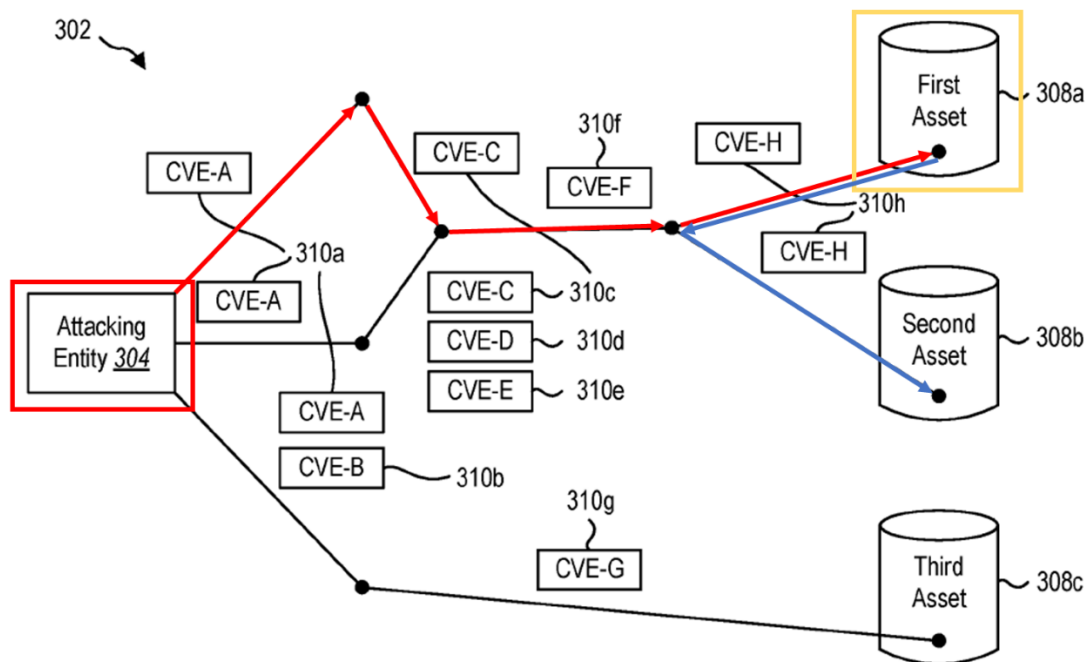


FIG. 3B

EX1006, Fig. 3B (annotated).

In addition, Morgan teaches that an attack vector may involve multiple “hops” across devices to reach a target asset. EX1006, 5:10-13, 8:19-26, 8:40-57, 14:7-17 (“The network pathway may traverse any number of edges via multiple nodes on one or multiples devices of the computing network.”), 18:22-32; EX1002, ¶125. This is evidenced by the example graph reproduced below, which illustrates how Morgan’s analysis identifies a number of attack paths that traverse multiple devices (as indicated by the black boxes in the figure) within the network. EX1006, 1:43-46, 13:66-14:17; EX1002, ¶125.

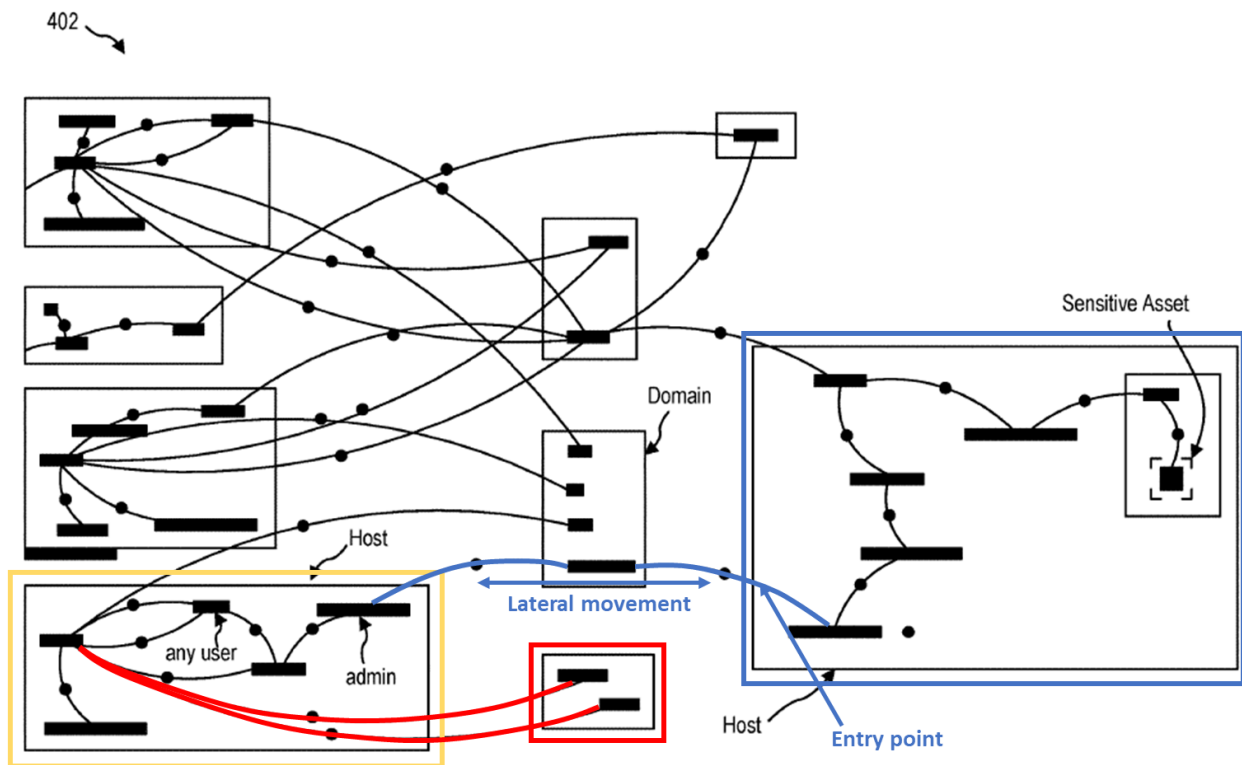


FIG. 4A

EX1006, Fig. 4A (annotated).

As demonstrated above, the attack vectors can identify at least one exposure risk to one or more downstream devices relative to a specific host device.

EX1002, ¶126. As Dr. Stavrou explains, a specific host under investigation (yellow box) may be associated with an attack vector in which an attacker (originating, e.g., from the red box) can traverse multiple nodes within the host by exploiting vulnerabilities to escalate the attacker's privileges to "any user" then to "admin." See EX1006, 14:12-13; EX1002, ¶126. Using admin access, the attacker can then move laterally in the network (blue path) to gain entry into another

downstream host (blue box), where the attacker can gain access to the sensitive asset contained on the host. EX1006, 14:1-12; EX1002, ¶126 & n.4 (noting broad application of “asset” as used in Morgan) (citing EX1006, 5:14-32). Thus, a POSA would have recognized Morgan as teaching that an identified attack vector can identify an exposure risk to a downstream host (blue) as indicated by the possible pathways an attacker can traverse to gain access to the downstream host. EX1002, ¶127. The exposure risk identifies the exposed asset (e.g., downstream host (blue)) and an entry point to the exposed asset (e.g., the node that can be accessed from the specific host (yellow)). *Id.* The exposure risk also identifies a lateral movement risk associated with the exposed asset (e.g., the identification of edges (blue path) from the upstream host (yellow) to the downstream host (blue)). EX1002, ¶¶128 (explaining lateral movement encompasses movement between network assets through, e.g., network connections or stored credentials/secrets) (citing EX1007, ¶¶5, 36; EX1017, 1:47-52, 4:30-40, 5:22-33), 129 (noting Morgan’s path identification consistent with lateral movement risk described by the ’154 patent) (citing EX1001, 15:14-15, 61:19-39, 69:26-28). Further, as explained more below, in addition to identifying a lateral movement risk as visualized by the paths that can be used by an attacker to laterally move between devices, Morgan also teaches that the lateral movement risk can be quantified to

provide an indication of the likelihood that an attacker will use the particular path.

Infra, §XI.B.9; EX1002, ¶129.

Thus, in view of the references’ combined teachings, a POSA would have readily adapted a system such that, when a user selected a security object to view attack path information for that object, the system would also perform a backward analysis of the selected object to identify at least one exposure risk to downstream security objects that is in a downstream of the selected object, as recited. EX1002, ¶¶118 (citing EX1005, 18:23-34; EX1006, 11:30-47), 130; *supra*, §XI.A. A POSA would have understood that this analysis would illustrate to the user the overall impacts to the network environment caused by an outside attacker traversing a network path of the selected security object. EX1002, ¶¶130-31.

9. Elements 1.7, 14.7, and 20.7

The combination of Keren and Morgan teaches these elements, which recite “[output/outputting] a signal to cause on a display to present a presentation of forward and backward paths associated with the specific asset, thereby enabling visualization of a plurality of entry points and lateral movement risks associated with the plurality of entry points.” EX1002, ¶132.

Keren teaches that the system outputs a presentation of forward and backward paths associated with security objects in the cloud environment. EX1002, ¶133. As explained above, Keren teaches that the system outputs a signal

to display the network paths to and from security objects (e.g., the forward (red) and backward (blue) paths annotated below) via a security graph visualization 400.

Supra, §§XI.B.1, XI.B.7-8.

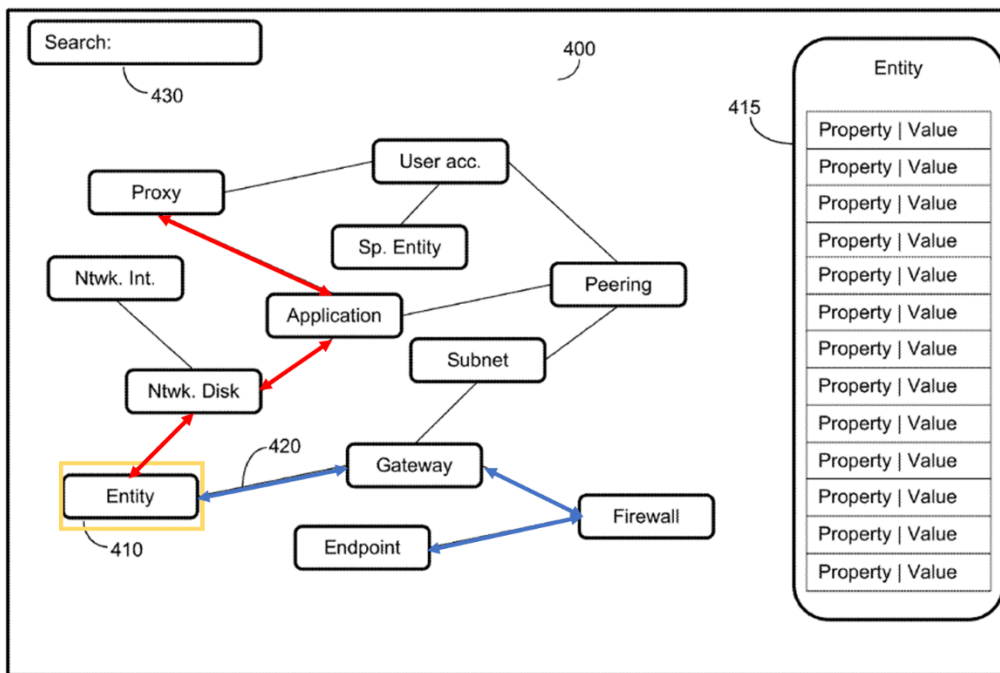


FIG. 4A

EX1005,

Fig. 4A (annotated).

Keren also teaches that the system can output a signal to display the network paths for a security object that has been selected by the user, as illustrated by the example shown in Fig. 4B below. *Supra*, §§XI.B.1, XI.B.7; EX1002, ¶134.



FIG. 4B

EX1005, Fig. 4B.

As explained above, while Keren teaches identifying the network paths (i.e., vectors) between security objects, it does not expressly disclose identifying the paths that can be attack vectors. EX1002, ¶135; *supra*, §XI.A. Nevertheless, a POSA would have sought to identify those paths and provide them as attack vector visualizations, as taught by Morgan. *Supra*, §XI.A. Specifically, as shown below, Morgan teaches visually presenting the attack vectors identified by the system for a specific host. EX1006, 14:18-35, 19:15-34 (system “provide[s] visualizations or

other data outputs that assist the user in understanding the comprehensive threat assessment”), 19:55-20:7 (users may view attack graphs for selected host with selectable granularity), Fig. 4B; EX1002, ¶135.

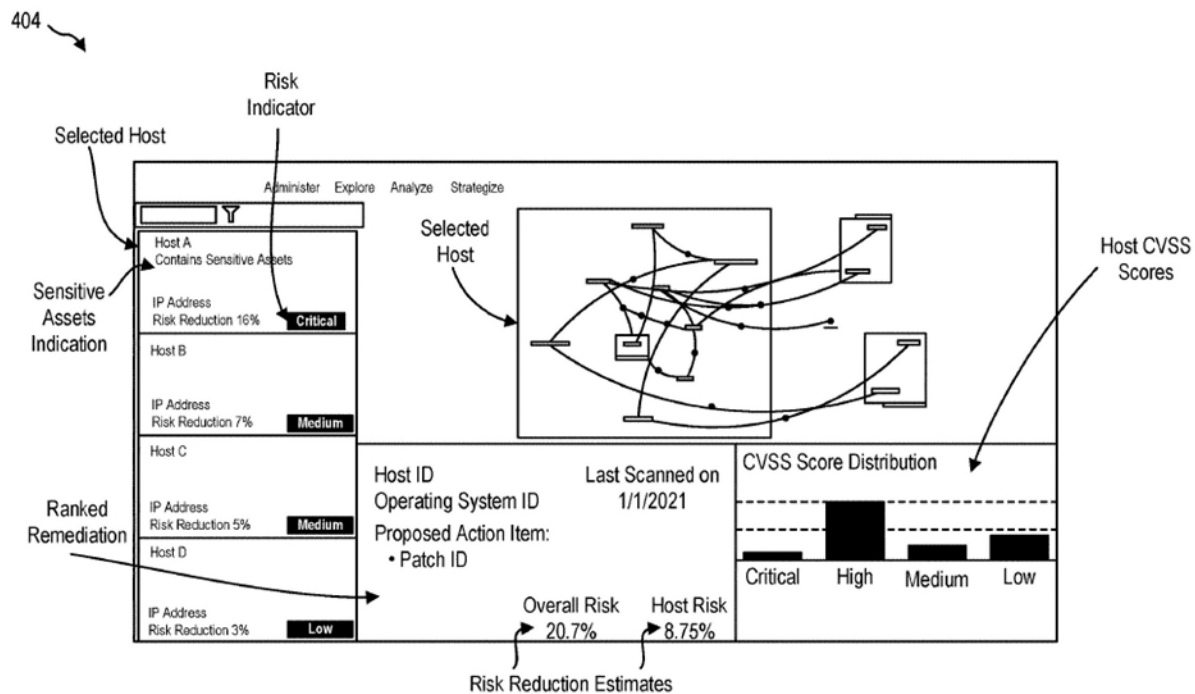


FIG. 4B

EX1006, Fig. 4B.

As detailed above, outputting the network paths identified as attack vectors for a selected security object would enable the user to view the entry points an attacker could access the selected security object, via the forward analysis, and the paths the attacker could move laterally to access entry points associated with downstream objects, via the backward analysis. See EX1006, 8:40-44 (system

identifies “multiple potential pathways”), 8:61-66, 11:16-21, 12:59-63, Fig. 4A; *supra*, §§XI.B.7-8; EX1002, ¶136. Thus, a POSA would have understood that the attack path visualizations displayed to the user for the selected security object would enable the visualization of a plurality of entry points (i.e., potential entry points into the selected security object and into downstream objects) and lateral movement risks associated with the plurality of entry points (i.e., the lateral paths connecting the selected security object to downstream objects), as recited. EX1002, ¶136.

Morgan further teaches that the lateral movement risks for an attack vector can also be quantified and presented to the user with the attack vector visualizations. EX1002, ¶137. Specifically, Morgan teaches that the system considers “a combination of factors” that are used “to determine risk scores associated with each edge,” resulting in “a numeric value (weight) that represents the likelihood an attacker would choose a given vulnerability to exploit a possible attack path.” EX1006, 3:20-36 (factors can include whether an edge is associated with multiple pathways, certain pathways include fewer edges, or a pathway would lead to higher impact), 9:31-46, 17:4-16; *see also id.*, 8:27-57, 10:4-16, 13:32-54, 17:23-35 (listing other attributes to calculate weight that edge will be traversed), Fig. 3C; EX1002, ¶¶137-38. Morgan teaches that this risk calculation is presented to the user along with the corresponding attack vectors so that the user can

visualize the pathways where remediation efforts will result in reduced overall risk to the network. EX1006, 10:63-11:29, 18:33-48 (teaching prioritization for remediation), 19:15-34 (user may select edge to view scoring reasoning), 20:55-21:10; EX1002, ¶139. Thus, Morgan also teaches enabling visualization of lateral movement risks by further presenting a quantification of the risk that an attacker will laterally move along a given pathway edge. EX1002, ¶139. Consistent with Morgan’s teachings, a POSA would have had reason to additionally include a risk quantification with the identified attack vectors outputted to the user upon selection of a security object in Keren’s system. EX1002, ¶¶139-41.

Accordingly, claims 1, 14, and 20 were obvious.

C. Dependent Claims

1. Claims 2 and 15

Claims 2 and 15 depend from claims 1 and 14, respectively, and further recite “wherein the network outside the cloud environment includes the Internet.” Keren and Morgan teach these limitations. EX1002, ¶142.

As explained above, Keren teaches analyzing the reachable paths of security objects relative to a network outside the cloud environment, including the internet. EX1005, 13:31-32, 13:66-14:1, 15:50-58, 20:34-42; *supra*, §XI.B.7; EX1002, ¶143. Similarly, Morgan teaches identifying attack paths originating external to the computing network, which may communicate over the internet. EX1006, 1:54-

60 (computing network may be a “cloud computing network”), 5:1-7, 6:23-43 (data may be transmitted to network devices through internet), 11:57-65, 12:25-30, 16:52-66, 24:44-48; §XI.B.7. Moreover, Keren and Morgan express a desire to prevent attackers from gaining unauthorized access into the network, which a POSA would have recognized included attackers originating from the internet. EX1005, 1:22-35 (increased digital presence exposes organizations to attackers); EX1006, 1:6-19 (recognizing increasing threat of “unauthorized entities gaining access to information maintained on computer networks”); *supra*, §XI.A. Thus, a POSA would have understood, or at minimum have found it obvious, that the attack path analysis, including the forward analysis discussed above (*supra*, §XI.B.7), would include identifying attack vectors reaching the selected security object via the internet. EX1002, ¶¶144-45.

Accordingly, claims 2 and 15 were obvious.

2. Claims 3 and 16

Claims 3 and 16 depend from claims 1 and 14, respectively, and further recite “wherein the assets in the cloud environment include at least one of: a virtual machine, a network appliance, a storage appliance, a compute instance[s], or an engine instance.” As explained above, Keren teaches the identified security objects can include virtual machines and other compute and engine instances (e.g., container, serverless applications, and other cloud processing and management

systems), network appliances (e.g., proxies, firewalls, gateways, and load balancers), and storage appliances (e.g., file servers and databases). EX1005, 4:27-51, 5:35-39, 5:42-44, 6:13-18; *supra*, §XI.B.3; EX1002, ¶146-48.

Accordingly, claims 3 and 16 were obvious.

3. Claims 4 and 17

Claims 4 and 17 depend from claims 1 and 14, respectively, and further recite “wherein identifying the assets in a cloud environment includes identifying the assets based on at least one of: an identity and access management policy, an organization policy, or an access policy.” Keren and Morgan teach these limitations. EX1002, ¶149.

Keren teaches that the system collects security object data as part of identifying the security objects in the cloud environment. *E.g.*, EX1005, 9:26-27, Fig. 2 (S210); *supra*, §XI.B.3; EX1002, ¶150. The data includes information that identifies the security objects and their properties, which is used to determine object relationships and network paths. *Id.*, 9:56-58 (“Security object data is data describing one or more security objects...”), 9:58-10:14; *supra*, §XI.B.5. Keren expressly teaches that the collected data may include data describing “object security or access configurations.” EX1005, 9:56-66 (emphasis added). Keren also teaches that the system may calculate reachable properties of security objects based on “various given accounts,” which a POSA would have understood assesses

whether a security object was reachable relative to a specific account. *Id.*, 15:44-58. To calculate this, a POSA would have understood, or at least found it obvious, that as part of identifying the security objects in the cloud environment, Keren's system would also identify the accounts that could access the security object, which would have been based on the object's access configurations (i.e., access policy). *Id.*, 9:56-66; *see also id.*, Fig. 4A; EX1002, ¶150.

Keren also teaches that security object data may be collected through "one or more API queries." EX1005, 10:6-10; EX1002, ¶151. These queries can be through "platform-specific APIs," such as those made available through Amazon AWS or Microsoft Azure. EX1005, 9:38-55. A POSA understood that such platform-specific APIs commonly provided network administrators with a service, known as "Identity and Access Management" or "IAM," to manage the relationships of users to cloud assets. *See* EX1015, 1 ("AWS Identity and Access Management (IAM) is a web service that you can use to manage users and user permissions under your AWS account."); EX1016, 181-82 ("Azure AD ... provides identity and access management in the cloud."); EX1002, ¶151. A POSA would have understood, or at least found obvious, that, as part of identifying security objects, Keren's system would also identify the users and permissions associated with a security object via an API query made to the cloud platform's IAM service (i.e., identity and access management policy). EX1002, ¶151. Thus,

Keren teaches identifying objects based on an access policy and/or an identity and access management policy, as recited, because Keren teaches identifying the accounts, users, and permissions associated with a security object. EX1002, ¶152; *cf.*, EX1001, 50:57-67 (“An identity and access management policy may comprise a software tool to verify identities of users and control access to an associated workload or system functionality. ... An access policy may determine the authorized users of an associated system.”).

Morgan also teaches identifying assets based on an access policy. EX1002, ¶153. Morgan teaches obtaining asset rights data and application configuration data, which a POSA would have understood included account types and permissions for accessing a given asset. EX1006, 2:1-5, 7:9-19, 15:16-38 (“automated queries may be used to obtain user account details (e.g., credentials), **access policies**, application configurations and the like” (emphasis added)), Fig. 2; *supra*, §XI.B.5. Morgan teaches that this information is related as nodes in the attack graph to show relationships between assets that an attacker can traverse by exploiting vulnerabilities. EX1006, 4:36-67, 15:16-20, 16:45-48. In further view of Morgan’s teachings, a POSA would have adapted a system such that, as part of identifying security objects as taught by Keren, the system would also collect data that would identify the accounts authorized to access the security objects (i.e., an access policy) to facilitate attack path analysis. EX1002, ¶¶153-54.

Accordingly, claims 4 and 17 were obvious.

4. Claims 5 and 18

Claims 5 and 18 depend from claims 1 and 14, respectively, and further recite “wherein the presentation of the forward and backward paths indicates alternative paths connecting between the specific asset and an upstream asset or a downstream asset.” Keren and Morgan teach these limitations. EX1002, ¶155.

Keren recognizes that security objects can be connected through alternative network paths. EX1002, ¶156. For example, as illustrated below, multiple network paths exist between a proxy and an endpoint (e.g., the additional green annotated path). *Id.*

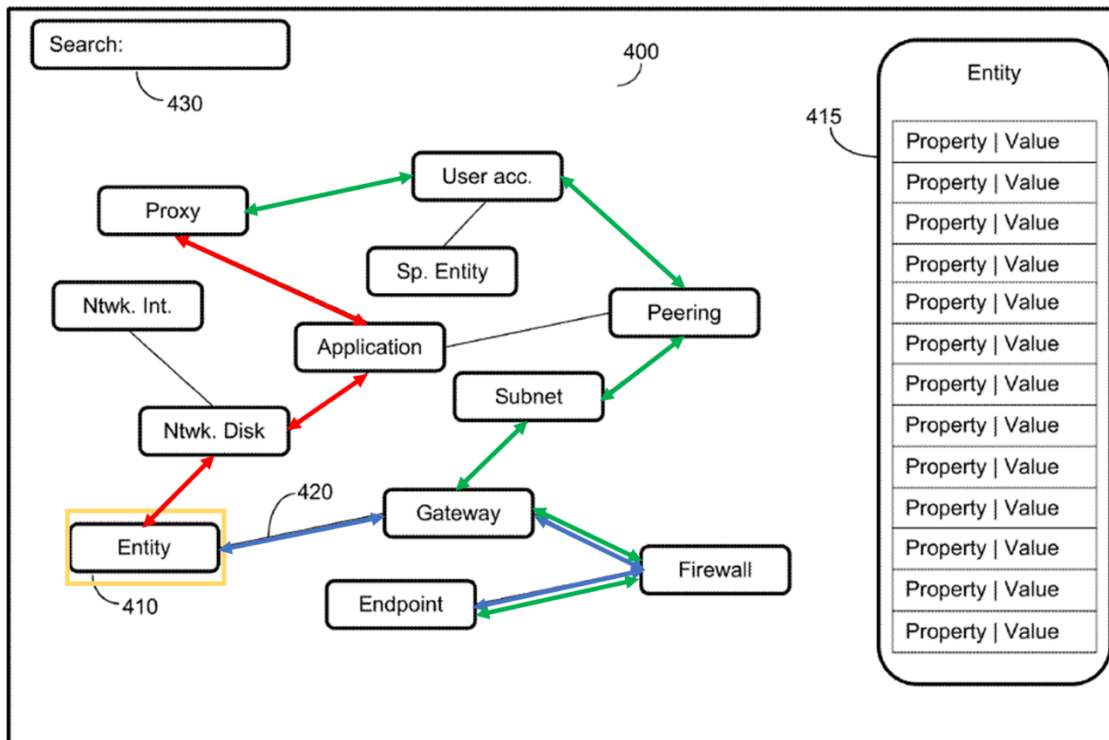


FIG. 4A

EX1005, Fig. 4A (annotated).

Morgan similarly recognizes that there may be multiple alternative pathways that an attacker can exploit to access an asset. EX1006, 8:40-44, 8:61-66 (system “may identify multiple pathways”), 11:16-21, 12:59-63. As illustrated below, Morgan teaches that the system can identify multiple alternative attack paths to a downstream host. EX1002, ¶157. For instance, as shown in the bottom leftmost host (yellow), an attacker (red) that has gained entry into the host can further exploit two alternative edges (orange and purple) that would lead to accessing the “any user” node, which can then be used to access the “admin” node. *Id.* Alternatively, a pathway exists (green) in which the attacker can bypass the “any user” node to directly access the “admin” node. *Id.* Each of these alternative pathways ultimately allow access to the downstream host containing the target sensitive asset (blue). *Id.*

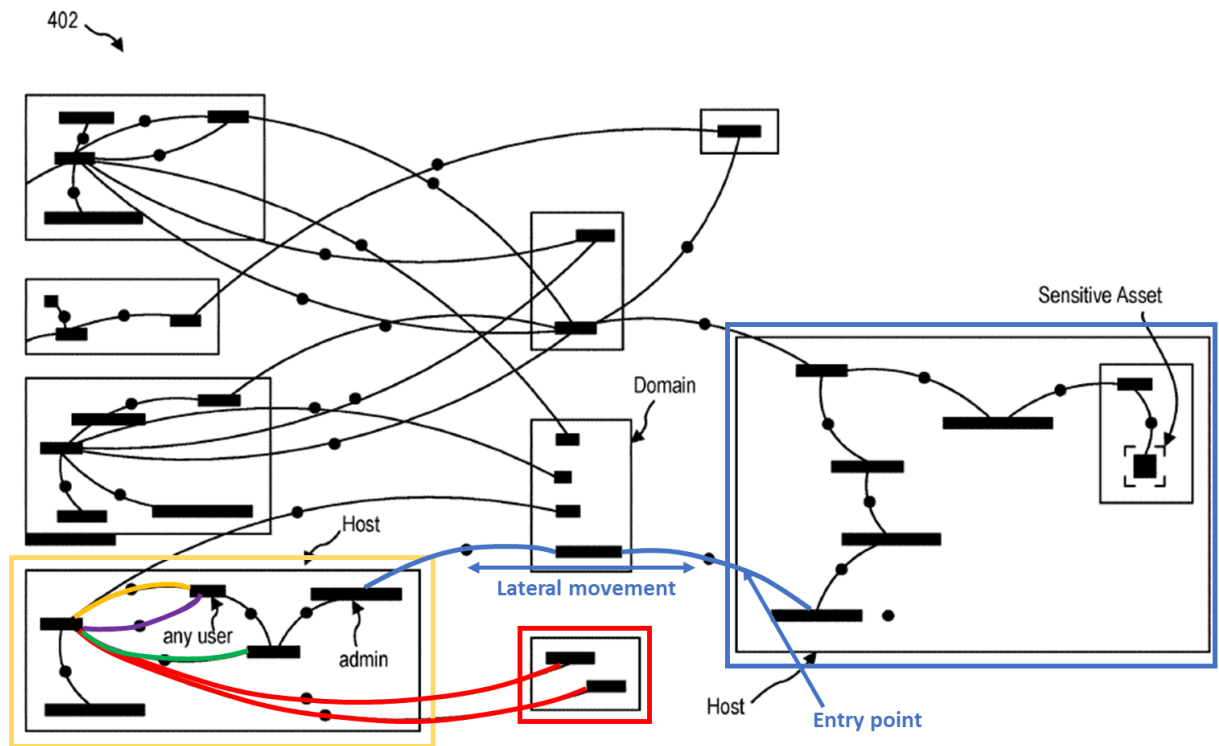


FIG. 4A

EX1006, Fig. 4A (annotated); *see also id.*, Fig. 3B.

It was well understood that attackers could string together multiple vulnerabilities along different network paths to access the same target asset. *See, e.g.*, EX1009, 7-8, Fig. 1 (illustrating three alternative attack paths to gaining full privileges on database server); EX1010, Fig. 3; EX1011, Fig. 3 (showing two alternative paths leading to host user privileges). Thus, consistent with the references' teachings, a POSA would have presented forward and backward paths that identified alternative attack paths between the selected security object and any

upstream or downstream objects. EX1002, ¶158. A POSA would have appreciated that this would allow the user to visualize the different ways in which an attacker could accomplish an attack. *Id.*, ¶¶158-59.

Accordingly, claims 5 and 18 were obvious.

5. Claims 6 and 19

Claims 6 and 19 depend from claims 5 and 18, respectively, and further recite “wherein the visualization includes a presentation of the alternative paths.” As explained above, a POSA would have sought to present forward and backward paths that indicated alternative paths connecting the selected security object and any upstream or downstream objects. EX1002, ¶¶160-61; *supra*, §XI.C.4. Keren and Morgan teach presenting identified pathways as a visualization to the user. EX1005, Figs. 4A-4B; EX1006, Fig. 4B. Thus, a POSA would have included in the attack path visualization outputted to the user a presentation of the alternative paths identified by the system. EX1002, ¶¶161-62.

Accordingly, claims 6 and 19 were obvious.

6. Claim 7

Claim 7 depends from claim 5 and further recites “wherein the at least one processor is further configured to detect a potential risk associated with the specific

asset based on the monitored network activities.”¹ Keren and Morgan teach this limitation.

Keren teaches monitoring network activities to detect potential risks associated with specific security objects. EX1002, ¶164. As explained above, Keren’s system generates security insights describing the network, including risky network configurations. EX1005, 12:11-16, 12:45-13:5; *supra*, §XI.B.4. These security insights may be generated based on monitored network activities. EX1002, ¶164. For example, the security insights can describe “network management or anomaly detection data,” such as “descriptions of network configurations or **events** which are rare or novel,” descriptions of the “**re-connection** of a user’s device to a subnet which the user is not permitted to access,” or “descriptions of **connections which display anomalous behavior**,” such as “spikes of network activity.” EX1005, 12:45-55 (emphasis added); *see also id.*, 11:56-60 (system monitors network activity through “observational or active logging methods”). As Dr. Stavrou notes, each of these examples describes a risk associated with a specific security object based on monitored network activities (e.g., new or unauthorized connection of a user device or increased

¹ There is no antecedent basis for “the monitored network activities.”

Nevertheless, Keren and Morgan teach this limitation. EX1002, ¶163.

network activity associated with an asset) because they can suggest that an outside attacker is actively attempting to enter the network. EX1002, ¶164. Thus, Keren teaches that the system (and its processor) is further configured to detect a potential risk associated with the specific asset based on the monitored network activities, as recited. *Id.*

Morgan also teaches detecting a potential risk relating to an identified attack path for a specific asset based on monitored network activities. EX1002, ¶165. Specifically, as part of quantifying risk (*supra*, §XI.B.9), Morgan teaches that “recent use” of a network device may be used in weighing the risk that a path edge will be exploited by an attacker. EX1006, 17:49-52. For example, “it may be known from customer security architecture that a first device, having a vulnerability A, is not frequently used, whereas a second device, having vulnerability B, is used frequently” (i.e., monitored network activities). *Id.*, 17:52-55. Morgan explains that, if both vulnerabilities require user interaction for exploitation, then the risk associated with the edge corresponding to vulnerability B will be weighted higher than the edge for vulnerability A. *Id.*, 17:55-63. Thus, Morgan also teaches detecting a potential risk associated with the specific asset (e.g., a risk that an edge will be used by an attacker) based on monitored network activities, as recited. EX1002, ¶¶165-66.

Accordingly, claim 7 was obvious.

7. Claim 8

Claim 8 depends from claim 1 and recites “wherein the presentation of the forward and backward paths indicates port numbers for each pathway.” The combination of Keren and Morgan teaches this limitation. EX1002, ¶167.

Keren teaches that its system collects security object data, which includes the port configurations of security objects, such as the objects’ port numbers and statuses. EX1005, 6:5-9, 9:56-66 (collected data includes “object port configurations”), 10:52-57 (network relationships describe “relevant ports of connected objects”), Fig. 5 (illustrating port numbers as part of pathway); EX1002, ¶168. Keren teaches that the identified port numbers can be presented to the user. EX1005, 11:66-12:11 (descriptions of reachable properties may be included in the security graph, including “a port number”), 12:26-44 (describing security insights that detail port numbers used for data transmissions), 17:1-18 (vertex overview pane of security graph utility presents “object data features,” including collected security object data), claim 7.

A POSA would have further understood that the port numbers used by a security object were relevant to an attack path analysis. EX1002, ¶169. Specifically, POSAs were aware that, to exploit a vulnerability present on an asset, an attacker would need to use an open port that was in communication with the vulnerability. *Id.* This is evidenced below, where Table 1 lists the vulnerabilities

on certain network assets, Table 2 lists the communication rules between the assets, and Figure 3 illustrates a graph illustrating possible attack paths:

TABLE 1: Vulnerabilities on each server.

Server	Vulnerabilities	CVE ID
WS	Allow remote execution of code	CVE-2015-1635
DBS	Remote execution of SQL command	CVE-2014-1466
FS	Allow remote execution of code	CVE-2013-4465
	Allow remote execution of code	CVE-2012-2526
AS	Allow remote execution of code	CVE-2009-0241

TABLE 2: Communication rules between servers.

Source server	Destination server	Protocol and port
202.120.234.6	WS	HTTP (80)
WS	DBS	SQL (1433)
	DBS	SQL (1433)
	FS	FTP (21)
AS	WS	HTTP (80)
	DS	DNS (1024)

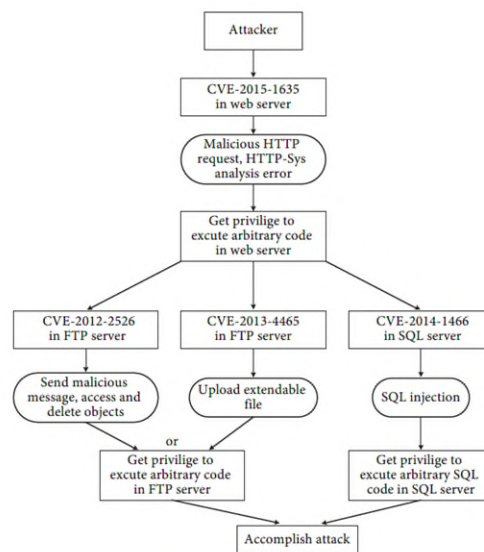


FIGURE 3: The corresponding attack graph.

EX1010, 3.

As Dr. Stavrou explains, to exploit a vulnerability found on the web server (CVE-2015-1635), the attacker would need to send a malicious HTTP request through the web server's port configured to receive HTTP requests (port 80). EX1002, ¶169 (describing additional ports used to exploit other vulnerabilities along the path). Because Keren teaches presenting to the user the port numbers associated with security objects and because POSAs appreciated that port numbers were relevant to an attack path analysis, a POSA would have had reason to also indicate the port numbers that an attacker would use in an attack path visualization so that the user could better visualize the communication means through which an

attack could be accomplished. EX1002, ¶¶170-71 (further noting that information would be especially important where non-standard service ports are used).

Accordingly, claim 8 was obvious.

8. Claim 9

Claim 9 depends from claim 1 and further recites “wherein the visualization of the entry points indicates at least one entry point at risk.” As explained above, a POSA would have sought to present identified attack paths as visualizations to a user, which would have visualized a plurality of entry points for an attacker to access a security object. *Supra*, §XI.B.9; EX1002, ¶¶172-73. As also explained above, Morgan teaches quantifying the risk that an attacker will exploit an identified attack path, which a POSA would have found obvious to include in the corresponding attack path visualization. EX1002, ¶173. Thus, because Morgan teaches quantifying a risk associated with an identified attack path, a POSA would have understood that this would indicate the entry points associated with that path that are at risk. *Id.*, ¶¶173-74.

Accordingly, claim 9 was obvious.

9. Claim 10

Claim 10 depends from claim 1 and further recites “wherein the at least one processor is further configured to monitor network activities of the assets in a cloud environment.” As explained above, Keren teaches that its system detects

risk based on monitored network activities of the security objects. EX1005, 12:45-61; *supra*, §XI.C.6; EX1002, ¶¶175-76. Keren further teaches that its system is configured to monitor those network activities. EX1005, 6:47-51 (system provides functionalities such as “network analysis” and “traffic analysis”), 11:56-60 (system applies “observational or active logging methods, such as those methods for detection of object-to-object connections by monitoring traffic of a network in use”); EX1002, ¶¶176-77.

Accordingly, claim 10 was obvious.

10. Claim 11

Claim 11 depends from claim 1 and further recites “the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of the specific asset.” As explained above, Keren teaches that the system detects potential risks associated with a specific asset based on the asset’s monitored network activities (e.g., new or unauthorized connections or abnormal activity). *Supra*, §XI.C.6; EX1002, ¶¶178-79. Similarly, Morgan teaches detecting a potential risk associated with a specific asset based on the asset’s frequency of use. *Supra*, §XI.C.6; EX1002, ¶¶179-80.

Accordingly, claim 11 was obvious.

11. Claim 12

Claim 12 depends from claim 1 and further recites “the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of an upstream asset of the specific asset.”

Morgan teaches this limitation. EX1002, ¶181.

As explained above, Morgan teaches quantifying a risk that an attacker will use an identified pathway to access an asset. *Supra*, §XI.B.9; EX1002, ¶182. This risk analysis can include consideration of the network activity of an asset within the path, such as whether an asset is frequently used. EX1006, 17:49-63; *supra*, §XI.C.6. Morgan teaches that, based on this network activity, a weight may be assigned to an attack path edge, which “reflects the likelihood of a successful exploitation of the vulnerability impacting the edge.” EX1006, 18:4-8. “Each edge in a potential path, once assigned a weight, is aggregated along with the other edges to assign a likelihood score for the overall given path, which can then be prioritized and provided to the user.” *Id.*, 18:8-11. Thus, Morgan teaches that the potential risk associated with a specific asset is based on the aggregated risk that an attacker will exploit each of the edges that make up a path for the specific asset. EX1002, ¶182. Based on these teachings, a POSA would have understood that the potential risk calculated for the specific security object in Keren’s system would include the weight assigned to the edge associated with an upstream object (e.g.,

the likelihood that a vulnerability of the upstream object will be exploited) based on that object's network activity (e.g., frequency of use). *Id.*, ¶¶182-83.

Accordingly, claim 12 was obvious.

12. Claim 13

Claim 13 depends from claim 1 and further recites “the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of a downstream asset of the specific asset.”

As explained above, a POSA had reason to present attack path visualizations for a selected security object to allow the user to visualize how an attacker could potentially use the selected security object to impact downstream objects. *Supra*, §§XI.A, XI.B.8; EX1002, ¶¶184-85. A POSA also had reason to include calculations of potential risk that an attacker would use an identified pathway as part of the outputted visualization, as taught by Morgan. *Supra*, §XI.B.9. As discussed previously, Morgan teaches that the calculations include assessing the risk that an attacker would exploit a vulnerability associated with a path edge based on the network activity of the asset having the vulnerability. EX1006, 17:49-18:21; *supra*, §XI.C.6.

A POSA would have recognized that Morgan's teachings regarding risk would equally apply to objects located downstream from the selected security object. EX1002, ¶186. For example, if a downstream object was not frequently

used, then the potential risk that an attacker could leverage the selected security object to move toward the downstream object would be diminished. *Id.* Thus, a POSA would have further included as part of the risk calculation for the selected security object the likelihood that an edge associated with a downstream object will be traversed based on that object's network activity. *Id.*, ¶¶186-87.

Accordingly, claim 13 was obvious.

XII. CONCLUSION

The challenged claims are unpatentable. Wiz respectfully requests that IPR be instituted.

Dated: January 17, 2025

Respectfully submitted,

/Matthew A. Argenti /
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836

CERTIFICATION UNDER 37 C.F.R. §42.24(d)

Under the provisions of 37 C.F.R. §42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,985 which is less than the 14,000 allowed under 37 C.F.R. 42.24(a)(i). In accordance with 37 C.F.R. 42.24(a), this word count does not include any table of contents, table of authorities, mandatory notices under §42.8, certificate of service or word count, or appendix of exhibits or claim listing.

Dated: January 17, 2025

Respectfully submitted,

/Matthew A. Argenti /
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836

PAYMENT OF FEES UNDER 37 C.F.R. §§42.15(A) AND 42.103

The required fees are submitted herewith. If any additional fees are due at any time during this proceeding, the Office is authorized to charge such fees to Deposit Account No. 23-2415.

LIST OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 11,627,154 to Shua
1002	Declaration of Dr. Angelos Stavrou
1003	<i>Curriculum Vitae</i> of Dr. Angelos Stavrou
1004	File History of U.S. Patent Application No. 17/657,981 ('154 Pat.)
1005	U.S. Patent No. 11,374,982 to Keren
1006	U.S. Patent No. 12,015,631 to Morgan
1007	U.S. Publication No. 2022/0263855 to Engelberg
1008	U.S. Patent No. 11,831,671 to Bruttomesso
1009	Singhal, "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs," NIST Interagency Report 7788 (Aug. 2011) https://doi.org/10.6028/NIST.IR.7788
1010	Zeng et al., "Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing," Security and Communication Networks (Dec. 2019)
1011	Lallie et al., "A Review of Attack Graph and Attack Tree Visual Syntax in Cyber Security," Elsevier Computer Science (2019)
1012	Cichonski, "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology," NIST Special Publication 800-61, Rev. 2 (Aug. 2012) http://dx.doi.org/10.6028/NIST.SP.800-61r2
1013	EP Patent No. 3,360,071 B1 to Li
1014	U.S. Publication No. 2013/0191919 A1, published July 25, 2013, to Basavapatna

Exhibit No.	Description
1015	Amazon Web Services, Inc., “AWS Identity and Access Management: API Reference,” available at: https://web.archive.org/web/20141225215104/https://docs.aws.amazon.com/IAM/latest/APIReference/iam-api.pdf , archived December 25, 2014
1016	Collier M. and Shahan R., “Fundamentals of Azure: Microsoft Azure Essentials,” 2nd Edition, Microsoft Press (2016), available at: https://web.archive.org/web/20210413101249/https://download.microsoft.com/download/6/6/2/662DD05E-BAD7-46EF-9431-135F9BAE6332/9781509302963_Microsoft%20Azure%20Essentials%20Fundamentals%20of%20Azure%202nd%20ed%20pdf.pdf , archived April 13, 2021
1017	U.S. Patent No. 11,799,874 to Lichtenstein
1018	McKay, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,” NIST Special Publication 800-52, Rev. 2 (Aug. 2019) https://doi.org/10.6028/NIST.SP.800-52r2

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e) and 42.105, I certify that I caused to be served true and correct copies of the foregoing: **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,627,154 and Exhibits 1001 - 1018** by Federal Express Next Business Day Delivery on January 17, 2025, on the Patent Owner's correspondence address of record for the subject patent as follows:

Finnegan, Henderson, Farabow,
Garrett & Dunner LLP
Attn: Christopher C. Johns
901 New York Avenue, N.W.
Washington, DC 20001-4413

Dated: January 17, 2025

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836