

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

ORCA SECURITY LTD,  
Petitioner

v.

WIZ, INC.,  
Patent Owner

---

*Inter Partes* Review Case No. IPR2025-01083  
U.S. Patent No. 11,722,554

**PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 11,722,554**

## TABLE OF CONTENTS

|             |                                                                                                                                                                                                                                              |           |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>I.</b>   | <b>INTRODUCTION.....</b>                                                                                                                                                                                                                     | <b>1</b>  |
| <b>II.</b>  | <b>THE '554 PATENT.....</b>                                                                                                                                                                                                                  | <b>1</b>  |
| A.          | SUMMARY OF THE '554 PATENT.....                                                                                                                                                                                                              | 1         |
| B.          | FIELD OF ENDEAVOR.....                                                                                                                                                                                                                       | 3         |
| C.          | PROBLEM SOLVED BY INVENTOR .....                                                                                                                                                                                                             | 4         |
| D.          | PRIORITY DATE OF THE CHALLENGED CLAIMS .....                                                                                                                                                                                                 | 5         |
| E.          | SUMMARY OF THE PROSECUTION HISTORY .....                                                                                                                                                                                                     | 5         |
| F.          | LEVEL OF SKILL OF A PERSON HAVING ORDINARY SKILL IN THE<br>ART.....                                                                                                                                                                          | 6         |
| <b>III.</b> | <b>REQUIREMENTS UNDER 37 C.F.R. § 42.104 .....</b>                                                                                                                                                                                           | <b>6</b>  |
| A.          | GROUND FOR STANDING UNDER 37 C.F.R. § 42.104(A).....                                                                                                                                                                                         | 6         |
| B.          | IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B) .....                                                                                                                                                                                | 6         |
| C.          | CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3).....                                                                                                                                                                                       | 7         |
| <b>IV.</b>  | <b>SHOWING OF ANALOGOUS, PRIOR ART .....</b>                                                                                                                                                                                                 | <b>7</b>  |
| A.          | SHIVAMOGGI.....                                                                                                                                                                                                                              | 7         |
| B.          | ZHONG .....                                                                                                                                                                                                                                  | 8         |
| C.          | WOOLWARD.....                                                                                                                                                                                                                                | 9         |
| <b>V.</b>   | <b>GROUND 1: CLAIMS 1, 4, 7-12, 15, 18-21 ARE OBVIOUS<br/>OVER SHIVAMOGGI.....</b>                                                                                                                                                           | <b>10</b> |
| A.          | CLAIM 1 .....                                                                                                                                                                                                                                | 10        |
| 1.          | <i>Claim 1[Pre]: “A method for determining abnormal<br/>configuration of network objects deployed in a cloud<br/>computing environment comprising:” .....</i>                                                                                | <i>10</i> |
| 2.          | <i>Claim 1[a]: “collecting network object data on a<br/>plurality of network objects deployed in the cloud<br/>computing environment” .....</i>                                                                                              | <i>15</i> |
| 3.          | <i>Claim 1[b]: “constructing a network graph based on the<br/>collected network object data, wherein the network graph<br/>includes a visual representation of network objects<br/>identified in the cloud computing environment;” .....</i> | <i>18</i> |
| 4.          | <i>Claim 1[c]: “determining relationships between the<br/>identified network objects in the network graph, wherein<br/>the determined relationships between the identified</i>                                                               |           |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
|    | <i>network objects includes descriptions of connections between the identified network objects;”</i> .....                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 22 |
| 5. | <i>Claim 1[d]: “analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and”</i> .....                                                                                                                                                                                                                                                                                                                                 | 24 |
| 6. | <i>Claim 1[e]: “tagging network objects in the network graph for which the insight is generated.”</i> .....                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 28 |
| B. | CLAIM 4: “THE METHOD OF CLAIM 1, WHEREIN GENERATING INSIGHTS TO INCLUDE AT LEAST THE LIST OF ABNORMAL CONNECTIONS FURTHER COMPRISES: DETECTING ANY ONE OF: A RARE NETWORK CONFIGURATION, A NOVEL NETWORK CONFIGURATION, A RARE NETWORK EVENT, A NOVEL NETWORK EVENT, A CONNECTION OF A NEW DEVICE TO A NETWORK, AN UNAUTHORIZED CONNECTION, A RE-CONNECTION OF A USER DEVICE TO A SUBNET WHICH THE USER IS NOT PERMITTED TO ACCESS, A CONNECTION DEMONSTRATING ANOMALOUS BEHAVIOR OR MISCONFIGURATION, AND A CONNECTION DEMONSTRATING SPIKES OF NETWORK ACTIVITY.” ..... | 31 |
| C. | CLAIM 7: “THE METHOD OF CLAIM 1, WHEREIN DETERMINING THE RELATIONSHIPS BETWEEN THE IDENTIFIED NETWORK OBJECTS IN FURTHER COMPRISES: DETERMINING THE RELATIONSHIPS USING AT LEAST ONE OF: OBSERVATIONAL METHODS, AND ACTIVE LOGGING METHODS.” .....                                                                                                                                                                                                                                                                                                                       | 32 |
| D. | CLAIM 8: “THE METHOD OF CLAIM 1, FURTHER COMPRISING: ADDING VISUAL REPRESENTATIONS OF THE DETERMINED RELATIONSHIPS TO THE VISUAL REPRESENTATIONS OF THE NETWORK GRAPH.” .....                                                                                                                                                                                                                                                                                                                                                                                            | 34 |
| E. | CLAIM 9: “THE METHOD OF CLAIM 1, WHEREIN EACH OF THE PLURALITY OF NETWORK OBJECTS INCLUDES ANY ONE OF: A VIRTUAL NETWORK, A FIREWALL, A NETWORK INTERFACE CARD, A PROXY, A GATEWAY, A SOFTWARE CONTAINER, CONTAINER, A MANAGEMENT OBJECT, A VIRTUAL MACHINE, A SUBNET, A HUB, A VIRTUAL PRIVATE NETWORK (VPN).” .....                                                                                                                                                                                                                                                    | 36 |
| F. | CLAIM 10: “THE METHOD OF CLAIM 1, WHEREIN A GENERATED INSIGHT OF THE GENERATED INSIGHTS IS GENERATED UTILIZING NATURAL LANGUAGE REPRESENTATION.” .....                                                                                                                                                                                                                                                                                                                                                                                                                   | 37 |
| G. | CLAIM 11[PRE]: “A NON-TRANSITORY COMPUTER READABLE MEDIUM HAVING STORED THEREON INSTRUCTIONS FOR CAUSING A PROCESSING CIRCUITRY TO EXECUTE A PROCESS FOR                                                                                                                                                                                                                                                                                                                                                                                                                 |    |

|    |                                                                                                                                                                                                                                                                                  |    |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
|    | DETERMINING ABNORMAL CONFIGURATION OF NETWORK OBJECTS<br>DEPLOYED IN A CLOUD COMPUTING ENVIRONMENT, THE PROCESS<br>COMPRISING:” .....                                                                                                                                            | 39 |
| H. | CLAIM 11[A]: “COLLECTING NETWORK OBJECT DATA ON A<br>PLURALITY OF NETWORK OBJECTS DEPLOYED IN THE CLOUD<br>COMPUTING ENVIRONMENT;” .....                                                                                                                                         | 41 |
| I. | CLAIM 11[B]: “CONSTRUCTING A NETWORK GRAPH BASED ON THE<br>COLLECTED NETWORK OBJECT DATA, WHEREIN THE NETWORK<br>GRAPH INCLUDES A VISUAL REPRESENTATION OF NETWORK<br>OBJECTS IDENTIFIED IN THE CLOUD COMPUTING ENVIRONMENT;” .....                                              | 41 |
| J. | CLAIM 11[C]: “DETERMINING RELATIONSHIPS BETWEEN THE<br>IDENTIFIED NETWORK OBJECTS IN THE NETWORK GRAPH,<br>WHEREIN THE DETERMINED RELATIONSHIPS BETWEEN THE<br>IDENTIFIED NETWORK OBJECTS INCLUDES DESCRIPTIONS OF<br>CONNECTIONS BETWEEN THE IDENTIFIED NETWORK OBJECTS;” ..... | 41 |
| K. | CLAIM 11[D]: “ANALYZING THE NETWORK GRAPH AND THE<br>DETERMINED RELATIONSHIPS TO GENERATE INSIGHTS, WHEREIN<br>THE GENERATED INSIGHTS INCLUDE AT LEAST A LIST OF<br>ABNORMAL CONNECTIONS BETWEEN THE IDENTIFIED NETWORK<br>OBJECTS; AND” .....                                   | 41 |
| L. | CLAIM 11[E]: “TAGGING NETWORK OBJECTS IN THE NETWORK<br>GRAPH FOR WHICH THE INSIGHT IS GENERATED.” .....                                                                                                                                                                         | 41 |
| M. | CLAIM 12[PRE]: “A SYSTEM FOR DETERMINING ABNORMAL<br>CONFIGURATION OF NETWORK OBJECTS DEPLOYED IN A CLOUD<br>COMPUTING ENVIRONMENT, COMPRISING:” .....                                                                                                                           | 41 |
| N. | CLAIM 12[A]: “A PROCESSING CIRCUITRY; AND” .....                                                                                                                                                                                                                                 | 42 |
| O. | CLAIM 12[B]: “A MEMORY, THE MEMORY CONTAINING<br>INSTRUCTIONS THAT, WHEN EXECUTED BY THE PROCESSING<br>CIRCUITRY, CONFIGURE THE SYSTEM TO:” .....                                                                                                                                | 42 |
| P. | CLAIM 12[C]: “COLLECT NETWORK OBJECT DATA ON A<br>PLURALITY OF NETWORK OBJECTS DEPLOYED IN THE CLOUD<br>COMPUTING ENVIRONMENT;” .....                                                                                                                                            | 42 |
| Q. | CLAIM 12[D]: “CONSTRUCT A NETWORK GRAPH BASED ON THE<br>COLLECTED NETWORK OBJECT DATA, WHEREIN THE NETWORK<br>GRAPH INCLUDES A VISUAL REPRESENTATION OF NETWORK<br>OBJECTS IDENTIFIED IN THE CLOUD COMPUTING ENVIRONMENT;” .....                                                 | 42 |
| R. | CLAIM 12[E]: “DETERMINE RELATIONSHIPS BETWEEN THE<br>IDENTIFIED NETWORK OBJECTS IN THE NETWORK GRAPH,<br>WHEREIN THE DETERMINED RELATIONSHIPS BETWEEN THE                                                                                                                        |    |

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|     | IDENTIFIED NETWORK OBJECTS INCLUDES DESCRIPTIONS OF CONNECTIONS BETWEEN THE IDENTIFIED NETWORK OBJECTS;” .....                                                                                                                                                                                                                                                                                                                                                                                                   | 42        |
| S.  | CLAIM 12[F]: “ANALYZE THE NETWORK GRAPH AND THE DETERMINED RELATIONSHIPS TO GENERATE INSIGHTS, WHEREIN THE GENERATED INSIGHTS INCLUDE AT LEAST A LIST OF ABNORMAL CONNECTIONS BETWEEN THE IDENTIFIED NETWORK OBJECTS; AND” .....                                                                                                                                                                                                                                                                                 | 42        |
| T.  | CLAIM 12[G]: “TAGGING NETWORK OBJECTS IN THE NETWORK GRAPH FOR WHICH THE INSIGHT IS GENERATED.” .....                                                                                                                                                                                                                                                                                                                                                                                                            | 43        |
| U.  | CLAIM 15: “THE SYSTEM OF CLAIM 12, WHEREIN THE SYSTEM IS FURTHER CONFIGURED TO: DETECT ANY ONE OF: A RARE NETWORK CONFIGURATION, A NOVEL NETWORK CONFIGURATION, A RARE NETWORK EVENT, A NOVEL NETWORK EVENT, A CONNECTION OF A NEW DEVICE TO A NETWORK, AN UNAUTHORIZED CONNECTION, A RE-CONNECTION OF A USER DEVICE TO A SUBNET WHICH THE USER IS NOT PERMITTED TO ACCESS, A CONNECTION DEMONSTRATING ANOMALOUS BEHAVIOR OR MISCONFIGURATION, AND A CONNECTION DEMONSTRATING SPIKES OF NETWORK ACTIVITY.” ..... | 43        |
| V.  | CLAIM 18: “THE SYSTEM OF CLAIM 12, WHEREIN THE SYSTEM IS FURTHER CONFIGURED TO: DETERMINE THE RELATIONSHIPS USING AT LEAST ONE OF: OBSERVATIONAL METHODS, AND ACTIVE LOGGING METHODS.” .....                                                                                                                                                                                                                                                                                                                     | 43        |
| W.  | CLAIM 19: “THE SYSTEM OF CLAIM 12, WHEREIN THE SYSTEM IS FURTHER CONFIGURED TO: ADDING VISUAL REPRESENTATIONS OF THE DETERMINED RELATIONSHIPS TO THE VISUAL REPRESENTATIONS OF THE NETWORK GRAPH.” .....                                                                                                                                                                                                                                                                                                         | 43        |
| X.  | CLAIM 20: “THE SYSTEM OF CLAIM 12, WHEREIN EACH OF THE PLURALITY OF NETWORK OBJECTS INCLUDES ANY ONE OF: A VIRTUAL NETWORK, A FIREWALL, A NETWORK INTERFACE CARD, A PROXY, A GATEWAY, A SOFTWARE CONTAINER, CONTAINER, A MANAGEMENT OBJECT, A VIRTUAL MACHINE, A SUBNET, A HUB, A VIRTUAL PRIVATE NETWORK (VPN).” .....                                                                                                                                                                                          | 43        |
| Y.  | CLAIM 21: “THE SYSTEM OF CLAIM 12, WHEREIN A GENERATED INSIGHT OF THE GENERATED INSIGHTS IS GENERATED UTILIZING NATURAL LANGUAGE REPRESENTATION.” .....                                                                                                                                                                                                                                                                                                                                                          | 44        |
| VI. | <b>GROUND 2: CLAIMS 2, 3, 13, AND 14 ARE OBVIOUS OVER SHIVAMOGGI AND ZHONG .....</b>                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>44</b> |

|              |                                                                                                                                                                                                                                                                                                                                    |           |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| A.           | CLAIM 2: “THE METHOD OF CLAIM 1, WHEREIN THE CLOUD COMPUTING ENVIRONMENT INCLUDES A PLURALITY OF DIFFERENT CLOUD COMPUTING PLATFORMS.” .....                                                                                                                                                                                       | 44        |
| 1.           | <i>Zhong’s Teachings</i> .....                                                                                                                                                                                                                                                                                                     | 44        |
| 2.           | <i>Motivation to Combine Shivamoggi and Zhong</i> .....                                                                                                                                                                                                                                                                            | 46        |
| B.           | CLAIM 3: “THE METHOD OF CLAIM 2, WHEREIN COLLECTING NETWORK OBJECT DATA FURTHER COMPRISES: CONNECTING THROUGH AN APPLICATION PROGRAMING INTERFACE (API) EACH OF THE PLURALITY OF DIFFERENT CLOUD COMPUTING PLATFORMS TO COLLECT NETWORK OBJECT DATA OF NETWORK OBJECTS DEPLOYED IN THE RESPECTIVE CLOUD COMPUTING PLATFORM.” ..... | 48        |
| 1.           | <i>Zhong’s Teachings</i> .....                                                                                                                                                                                                                                                                                                     | 48        |
| 2.           | <i>Motivation to Combine</i> .....                                                                                                                                                                                                                                                                                                 | 50        |
| C.           | CLAIM 13: “THE SYSTEM OF CLAIM 12, WHEREIN THE CLOUD COMPUTING ENVIRONMENT INCLUDES A PLURALITY OF DIFFERENT CLOUD COMPUTING PLATFORMS.” .....                                                                                                                                                                                     | 51        |
| D.           | CLAIM 14: “THE SYSTEM OF CLAIM 13, WHEREIN THE SYSTEM IS FURTHER CONFIGURED TO: CONNECT THROUGH AN APPLICATION PROGRAMING INTERFACE (API) EACH OF THE PLURALITY OF DIFFERENT CLOUD COMPUTING PLATFORMS TO COLLECT NETWORK OBJECT DATA OF NETWORK OBJECTS DEPLOYED IN THE RESPECTIVE CLOUD COMPUTING PLATFORM. ....                 | 52        |
| <b>VII.</b>  | <b>GROUND 3: CLAIMS 5 AND 16 ARE OBVIOUS OVER SHIVAMOGGI AND WOOLWARD .....</b>                                                                                                                                                                                                                                                    | <b>52</b> |
| A.           | CLAIM 5: “THE METHOD OF CLAIM 4, FURTHER COMPRISING: DETERMINING IMPERMISSIBLE RELATIONSHIPS BETWEEN THE NETWORK OBJECTS.” .....                                                                                                                                                                                                   | 52        |
| 1.           | <i>Woolward’s Teachings of Determining Impermissible Relationships</i> .....                                                                                                                                                                                                                                                       | 53        |
| 2.           | <i>Motivation to Combine</i> .....                                                                                                                                                                                                                                                                                                 | 55        |
| B.           | CLAIM 16: “THE SYSTEM OF CLAIM 12, WHEREIN THE SYSTEM IS FURTHER CONFIGURED TO: DETERMINE IMPERMISSIBLE RELATIONSHIPS BETWEEN THE NETWORK OBJECTS.” .....                                                                                                                                                                          | 57        |
| <b>VIII.</b> | <b>CONCLUSION.....</b>                                                                                                                                                                                                                                                                                                             | <b>57</b> |
| <b>IX.</b>   | <b>MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1) .....</b>                                                                                                                                                                                                                                                                        | <b>59</b> |
| A.           | REAL PARTY-IN-INTEREST.....                                                                                                                                                                                                                                                                                                        | 59        |
| B.           | RELATED MATTERS .....                                                                                                                                                                                                                                                                                                              | 59        |
| C.           | LEAD AND BACK-UP COUNSEL .....                                                                                                                                                                                                                                                                                                     | 59        |

|    |                                                    |    |
|----|----------------------------------------------------|----|
| D. | 37 C.F.R. § 42.8(B)(4) – SERVICE INFORMATION ..... | 60 |
|----|----------------------------------------------------|----|

## TABLE OF AUTHORITIES

### Cases:

|                                                                                        |   |
|----------------------------------------------------------------------------------------|---|
| <i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) .....                    | 7 |
| <i>Wellman, Inc. v. Eastman Chem. Co.</i> , 642 F.3d 1355, 1361 (Fed. Cir. 2011) ..... | 7 |

### Statutes:

|                      |     |
|----------------------|-----|
| 35 U.S.C. § 103..... | 6,7 |
|----------------------|-----|

### Regulations:

|                                |        |
|--------------------------------|--------|
| 37 C.F.R. § 42.6(e) .....      | 66     |
| 37 C.F.R. §42.8.....           | 65     |
| 37 C.F.R. § 42.8(a)(1) .....   | 57     |
| 37 C.F.R. § 42.8(b)(1) .....   | 57     |
| 37 C.F.R. § 42.8(b)(3) .....   | 57     |
| 37 C.F.R. § 42.8(b)(4) .....   | 57, 58 |
| 37 C.F.R. §42.24.....          | 65     |
| 37 C.F.R. §42.100.....         | 7      |
| 37 C.F.R. § 42.104.....        | 6      |
| 37 C.F.R. § 42.104(a) .....    | 6      |
| 37 C.F.R. § 42.104(b).....     | 6      |
| 37 C.F.R. § 42.104(b)(3) ..... | 7      |
| 37 C.F.R. § 42.105.....        | 66     |
| 37 C.F.R. § 42.105(b).....     | 66     |

## **I. INTRODUCTION**

Petitioner Orca Security Ltd. (“Petitioner”) requests *Inter Partes* Review of Claims 1-5, 7-16, and 18-21 (the “Challenged Claims”) of U.S. Patent No. 11,722,554 (“the ’554 Patent,” Ex. 1001) assigned to Wiz, Inc. (“Patent Owner”).

## **II. THE ’554 PATENT**

### **A. Summary of the ’554 Patent**

The ’554 Patent is directed to analyzing a network within a cloud computing environment to determine abnormal configurations of network objects. ’554 *Patent*, 1:16, 2:51-53, Fig. 1A. The ’554 Patent sought to address the problem of monitoring network objects, noting that manual monitoring is too time-consuming, and agent-based monitoring requires excessive computing resources. *Id.* 1:34-44; 2:9-33. Instead, the ’554 Patent proposed the use of graphical solutions to determine abnormal network configurations. However, these techniques were already well known in the art at the time of the earliest priority date of the ’554 Patent.

Specifically, the ’554 Patent describes a cloud computing environment that includes “network objects,” “applications,” and “subnets,” and the cloud computing environment provides connectivity between these various elements. ’554 *Patent*, 4:10-15, 4:27-31, 4:53-55, 4:62-63, 5:45-48, Fig. 1B. Exemplary cloud platforms in

the '554 Patent include “Amazon AWS®, Microsoft Azure®, and the like.” '554 Patent, 4:31-35.

The cloud computing environment in the '554 Patent can connect through a network to a cybersecurity system that provides “network analysis, traffic analysis, object querying, [and] graph generation[.]” '554 Patent, 4:14-16, 6:5-14; Fig. 2. The process of generating a graph is depicted in a flowchart in Figure 2:

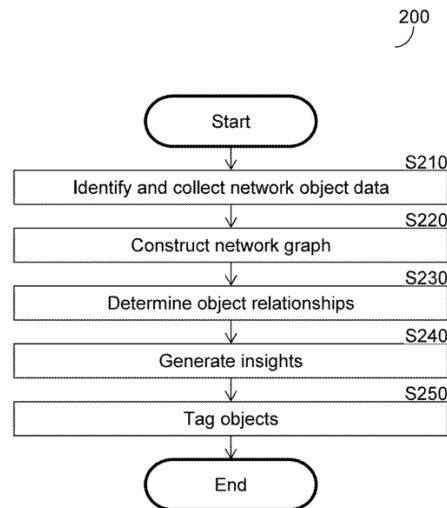


FIG. 2

*Id.*, Fig. 2.

This network graph describes the various objects in a network and the relationships between those objects. *Id.*, 7:43-45; 8:48-51. In constructing a network graph, “network objects are identified, and network object data is collected.” *Id.*, 7:46-47; *see also id.*, 5:4-44 (describing “examples of network objects 105” such as “objects providing support for application-layer communications and systems,”

“third-party containers and images,” and “virtual entities or instances of systems, devices, or components, including virtual systems, devices, or components, or any combination thereof.”). And this network graph can be constructed using data that describes the network objects, and the graph can further be comprised of a “visual ‘node and link’ graph.” *'554 Patent*, 8:48-63, Fig. 2.

The process of determining relationships between network objects includes “identify[ing] impermissible relationships.” *'554 Patent*, 9:3-4, 9:59-61, Fig. 2. After these relationships are generated, network insights are generated, including anomaly detection and natural-language representations of the network graph. *Id.*, 10:15-17, 50-52, Fig. 2. Finally, “network objects are tagged” using data label descriptions that allow for querying the network graph with a network graph utility. *'554 Patent*, 11:16, 11:21-24, 11:35-37, Fig. 2 (Step S250). Such a network graph utility (e.g., an “interface”) presents a network graph that is “a visual representation of a network” as described above. *'554 Patent*, 11:48-49, Fig. 3A.

## **B. Field of Endeavor**

The *'554 Patent* describes the technical field generally as “network administration, in particular, [] systems and methods for analyzing networks.” *'554 Patent*, 1:13-16; *see also id.*, 1:45-46 (“To address the need to manage large, distributed network systems....”), 2:51-53 (“...determining abnormal configuration of network objects deployed in a cloud computing environment.”), claims 1, 11, 12.

A POSITA would have thus understood the field of endeavor of the '554 Patent to be network administration and security. Ex. 1003, ¶ 51.

### **C. Problem Solved by Inventor**

The '554 Patent recognizes that organizations become “increasingly vulnerable to developing cyber-threats” when “implementing computing solutions at the individual, group, team, and cloud levels....” *'554 Patent*, 1:23-30. Given the complexity of modern, “large, multi-layered network systems, management of network access and use may be difficult or impossible for lone administrators or teams of administrators.” *'554 Patent*, 1:34-37. The '554 Patent outlines several alleged drawbacks with the existing network analysis solutions, including: (1) time- and effort-intensive manual review; (2) special-purpose solutions that monitor/manage only certain components or connections; and (3) protocol-agnostic solutions that provide over-broad connection information and fail to provide device-specific insights. *'554 Patent*, 1:47-54, 1:55-65, 1:65-2:7.

Thus, a POSITA would have understood that the '554 Patent is directed to solving the problem of monitoring devices and connections in large network systems. *'554 Patent*, 1:27-44. Ex. 1003, ¶¶ 24, 27, 31, 50.

**D. Priority Date of the Challenged Claims**

The '554 Patent claims priority to USPN 11,431,786 filed on Dec. 2, 2020. For purposes of this Petition only, Petitioner applies Dec. 2, 2020, as the priority date for the Challenged Claims.

**E. Summary of the Prosecution History**

The '554 Patent did not face any rejections during prosecution. *See '554 File History* (Ex. 1002). A single interview was conducted, where the “[t]he examiner and the applicant discussed the invention and the parent patents. The examiner suggests to incorporate ‘tagging network objects in the network graph for which the insight is generated’ in claims 1, 11, and 12, and a terminal disclaimer over the parent patent to place the application in condition for allowance.” *Id.*, 22. After this Interview, a Notice of Allowance issued, where the examiner stated that “the prior art of record does not teach or suggest, determining relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects, analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects, and tagging network objects in the network graph for which the insight is generated in light of other features described in independent claims 1, 11 and 12.”

'554 *File History*, 20. As demonstrated below, these limitations are taught by Shivamoggi alone or Shivamoggi in view of Zhong and Woolward.

**F. Level of Skill of a Person Having Ordinary Skill in the Art**

A POSITA at the time of the '554 Patent would have had a bachelor's degree in an academic area emphasizing computer science (i.e. computer science, computer information systems, computer engineering, etc.) or cybersecurity, with at least two years of experience in the field of cybersecurity; additional education or experience might substitute for these requirements. Ex. 1003, ¶ 49.

**III. REQUIREMENTS UNDER 37 C.F.R. § 42.104**

**A. Grounds for Standing Under 37 C.F.R. § 42.104(a)**

Petitioner certifies the '554 Patent is available for IPR and Petitioner is not barred/estopped from requesting IPR as set forth in this Petition.

**B. Identification of Challenge Under 37 C.F.R. § 42.104(b)**

Petitioner requests that the Challenged Claims be found unpatentable on the following grounds.

| <b>Proposed Grounds of Unpatentability</b>                                                                  | <b>Exhibits</b> |
|-------------------------------------------------------------------------------------------------------------|-----------------|
| <b><u>Ground 1:</u></b> Claims 1, 4, 7-12, 15, and 18-21 are obvious under 35 U.S.C. § 103 over Shivamoggi  | 1004            |
| <b><u>Ground 2:</u></b> Claims 2, 3, 13, and 14 are obvious under 35 U.S.C. § 103 over Shivamoggi and Zhong | 1004, 1005      |

|                                                                                                 |            |
|-------------------------------------------------------------------------------------------------|------------|
| <b>Ground 3:</b> Claims 5 and 16 are obvious under 35 U.S.C. § 103 over Shivamoggi and Woolward | 1004, 1006 |
|-------------------------------------------------------------------------------------------------|------------|

**C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)**

To the extent necessary, all claim terms should be construed according to the *Phillips* standard. 37 C.F.R. §42.100; *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). Here, no claim terms need to be construed to resolve any issues in controversy in the Petition. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

**IV. SHOWING OF ANALOGOUS, PRIOR ART**

**A. Shivamoggi**

U.S. Patent No. 11,770,387 to Shivamoggi (“Shivamoggi,” Ex. 1004) was neither cited nor discussed during the prosecution of the ’554 Patent. *See generally* Ex. 1002. Shivamoggi was filed July 17, 2020, and therefore qualifies as prior art under §102(a)(2).

Shivamoggi teaches monitoring a computer network for anomalous connections indicative of lateral movement through the network during a cyberattack. *Shivamoggi*, Abstract, 1:33-53, 2:48-54. Shivamoggi is in the same field of endeavor and is reasonably pertinent to at least one problem with which the inventors of the ’554 Patent were involved. Ex. 1003, ¶¶ 20-24. Like the ’554 Patent,

Shivamoggi is directed to a system that monitors a computer network to determine unwanted or abnormal configurations, i.e., “lateral movement” that is not authorized. *Cf. Shivamoggi*, 1:32-35 with ’554 Patent, 2:51-53.

Shivamoggi is also reasonably pertinent to a particular problem addressed by the ’554 Patent, which is the management and monitoring of individual devices and connections in large network systems. *Cf. Shivamoggi*, 2:55-60, 2:67–3:4 with ’554 Patent, 1:34-37, 1:50-54.

**B. Zhong**

U.S. Patent No. 10,693,743 to Zhong (“Zhong”, Ex. 1005) was neither cited nor considered during the prosecution of the ’554 Patent. Zhong was filed as a PCT application on September 21, 2015, therefore qualifying as prior art under §102(a)(2). Zhong teaches management and visualization of data acquired from multiple cloud computing services. *Zhong*, Abstract, 37:3-7, Figs. 18, 21; Ex. 1003, ¶¶ 25-27.

Zhong is analogous to the claimed invention of the ’554 Patent because Zhong is from the same field of endeavor: network administration, including security analysis through systems and methods for analyzing networks. *Cf. Zhong*, 37:7-11, 38:27-46, with ’554 Patent, 1:45-47.

Zhong is also reasonably pertinent to particular problems addressed by the ’554 Patent: managing and monitoring individual devices and connections in large,

multi-layered network systems. *Cf. Zhong*, Abstract, 38:21-26, with '554 Patent, 1:20-2:7.

### **C. Woolward**

U.S. Patent Application Publication No. 2020/0382560 to Woolward ("Woolward," Ex. 1006) was neither cited nor considered during the prosecution of the '554 Patent. Woolward was filed May 31, 2019, therefore qualifying as prior art under §102(a)(2). Woolward teaches determining violations in the relationships among workloads in a cloud-computing environment. *Woolward*, Abstract, [0006], Fig. 6; Ex. 1003, ¶¶ 28-31.

Woolward is analogous to the claimed invention of the '554 Patent because Woolward is from the same field of endeavor: network security, including security analysis through systems and methods for analyzing networks. *Cf. Woolward*, Abstract, [0004], [0024] with '554 Patent, 1:20-27.

Woolward is also reasonably pertinent to particular problems addressed by the '554 Patent: managing and monitoring individual devices and connections in large, multi-layered network systems. *Cf. Woolward*, [0006], [0013], [0017]-[0083] with '554 Patent, 1:20-2:7.

**V. GROUND 1: CLAIMS 1, 4, 7-12, 15, 18-21 ARE OBVIOUS OVER SHIVAMOGGI**

**A. Claim 1**

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

To the extent the preamble is limiting<sup>1</sup>, Shivamoggi teaches this limitation. For example, Shivamoggi teaches “methods [] to implement a cyberattack detection system that monitors a computer network for lateral movement” (i.e., *method for determining abnormal configuration*<sup>2</sup>) where the computer network includes virtual machine nodes (i.e., *network objects*) hosted on Amazon Web Services or Microsoft Azure cloud resources (i.e., *deployed in a cloud computing environment*). *Shivamoggi*, 1:33-36, 9:49-57, Fig. 2. Ex. 1003, ¶¶52-69.

In Shivamoggi, system 100 and service 230 monitor client networks for lateral movement, including network 212 of Fig. 2 (which may be an embodiment of client network 110 of Fig. 1). *Shivamoggi*, 1:6-8, 4:23-26, 5:11-13, 9:17-20, 9:47-49,<sup>3</sup>

---

<sup>1</sup>Petitioner contends that the Claim 1 preamble is not limiting.

<sup>2</sup>Claim language indicated by italics unless stated otherwise.

<sup>3</sup>A POSITA would have understood the disclosures at 9:17-20 and 9:47-49 to include a shared typographical error in that element 220 should refer instead to element 212.

FIGS. 1, 2. Ex. 1003, ¶¶ 55-56. Consistent with how the term was generally used in the field in December 2020, a POSITA would have understood that a “client network” in Shivamoggi is a network operated by a company, organization, group, or other type of entity and that the monitoring service 230 may monitor multiple client networks, each of which could be operated by a different such entity. *Shivamoggi*, 9:20-23; Ex. 1003, ¶ 57.

Shivamoggi teaches that each monitored client network can include virtual machines 214*d*, which can each be “an instance of an emulated computer that is

---

This is because: (1) element 220 references a public network, not a “client” network; and (2) while client network 212 is depicted to include elements 214*a-d* as described in the relevant text, public network 220 is not depicted as including these elements. *Shivamoggi*, 9:17-9:49; Ex. 1003, ¶ 67. Accordingly, a POSITA would have understood these disclosures to read respectively as follows: “The network monitoring service 230 is configured to monitor the remote client networks 210 and ~~220~~212, which may be embodiments of the client network 110 of FIG. 1;” and “[a]s shown, the client networks 210 and ~~220~~212 include different types of nodes, such as a workstation 214*a*, a server 214*b*, a printer 214*c*, and a virtual machine 214*d*.” *Id.*

**hosted on** a physical virtual machine host. The virtual machine host may implement virtualization hardware and/or software (*e.g.*, hypervisors) to execute and manage multiple instances of guest operating systems. Example implementations of such virtualization technologies include...AMAZON WEB SERVICES, and MICROSOFT AZURE.” *Shivamoggi*, 9:47-57,<sup>4,5</sup> Fig. 2. A POSITA would have understood that a virtual machine hosted in an AWS or Microsoft Azure environment is a cloud-based resource, because AWS and Microsoft Azure were well-known cloud-based resources at the time. Ex. 1003, ¶¶ 58-60. Further, AWS and Azure infrastructure were known to manage and provide the connections between hosted resources. Ex. 1003, ¶ 60 (citing *Beyer* (Ex. 1007), [0002], [0004]; *Huang* (Ex. 1008), 1:28-30).

A POSITA would have understood that these virtual machines in a client network are *network objects deployed in the cloud computing environment*, at least

---

<sup>4</sup>A POSITA would have understood the disclosure at 9:50 to include a typographical error in that element 130*d* should refer instead to 214*d*. This is clear from the context and also because element 130*d* does not appear in any figure, while the only element depicting virtual machines is element 214*d*. Ex. 1003, ¶ 68.

<sup>5</sup>All emphasis in quotes is added unless stated otherwise.

because the '554 Patent discloses that “network objects 105 include...virtual machines....” *'554 Patent*, 7:30-33; Ex. 1003, ¶ 61. The '554 Patent also describes an exemplary cloud computing environment as “represent[ing] an organization’s cloud-based resources, and the various connections between such resources.” *'554 Patent*, 4:4-7. Thus, client network 212 is a cloud computing environment that includes network objects. Ex. 1003, ¶ 61.

Shivamoggi also teaches “cyberattack detection system 100” and “network monitoring service 230” that monitor client networks for “lateral movement,” which is “a stage of cyberattacks where an attacker progressively moves through an organization’s network to search for high-value targets.” *Shivamoggi*, 1:6-8; *see also id.*, 4:23-26 (“In a typical lateral movement, an attacker first connects to one node in the network, and uses that node to connect to another node in the network, and so on.”). System 100 and service 230 each “use connection graphs to detect suspected lateral movements.” *Shivamoggi*, 5:7-9, 9:6-11, 10:27-32, FIGS. 1, 2. Namely, “[t]he connection graphs 140 will indicate distinct subsets of nodes in the network that made or attempted to make connections to each other during the time interval.” *Shivamoggi*, 7:5-7. Connection graphs are then analyzed to identify candidate attack paths, each of which “is a sequence of time-ordered connections that links a series of nodes in the connection graph.” *Shivamoggi*, 4:26-28, 8:15-24. Time-ordered

connection paths are evaluated and ranked based on, for example, “the length of the path, the number of connections in the path, the amount of data transmitted over all connections in the path, the number of distinct protocols indicated in the path,” in addition to, for example, “the presence or count of new nodes that used a communication protocol for a first time, or the presence or count of connections that represent a first-time connection between a source node and a destination node,” among other metrics. *Shivamoggi*, 8:36-63; *see also id.*, 3:21-36, 5:65-6:25, 10:26-34. The highest-ranking paths are identified as suspected attack paths. *Id.*

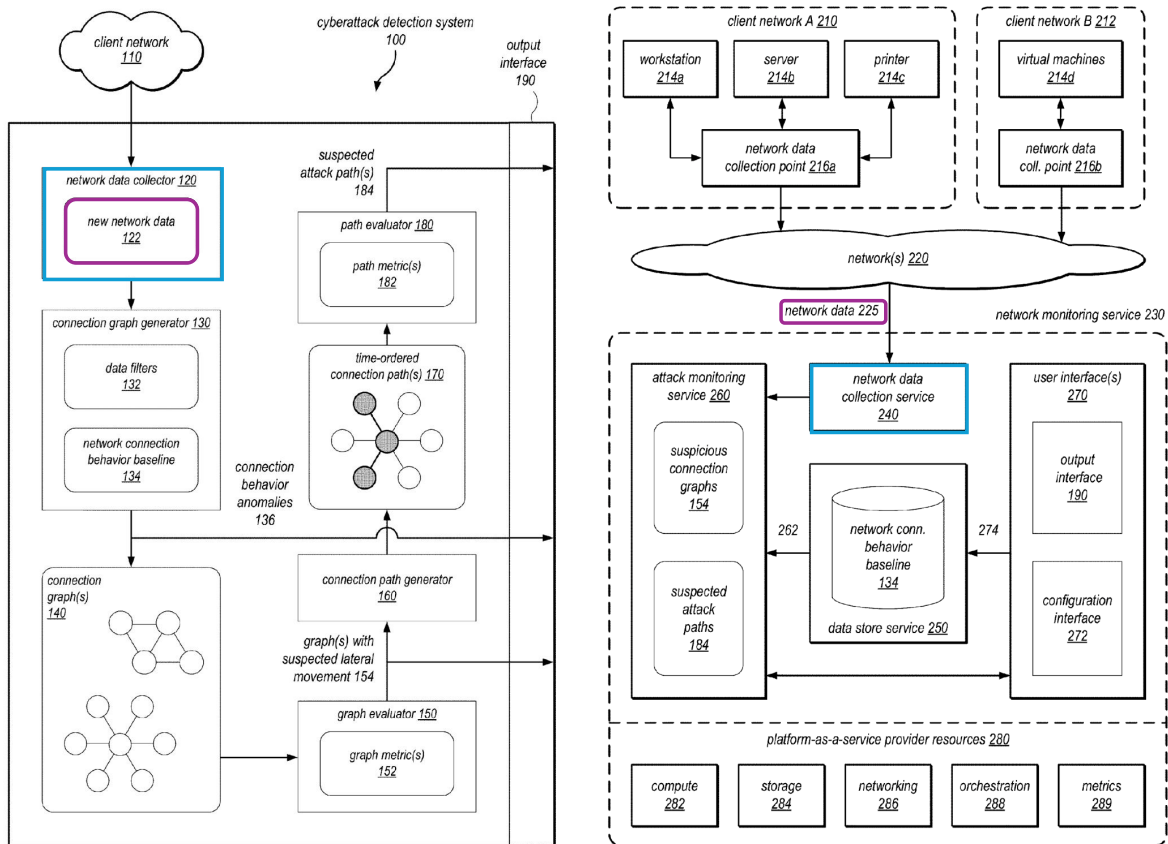
A POSITA would have understood that Shivamoggi’s detection of suspected lateral movement attack paths is the determination of an abnormal configuration of network objects within the meaning of the ’554 patent. Ex. 1003, ¶¶ 62-66. First, a sequence of time-ordered connections that links a series of nodes (i.e., *network objects*) is a “configuration” of the underlying network objects, at least because “configuration of network objects” as used in the ’554 patent describes the relative arrangement of network objects, including the connections linking them. *See, e.g., ’554 Patent*, 10:52-11:2 (providing examples of insights describing “network configurations or events which are rare or novel” as including insights describing connections of devices to and within a network); Ex. 1003, ¶ 64 (citing the Merriam-Webster’s Dictionary definition of “configuration”). Additionally, Shivamoggi

expressly teaches that its “network monitoring service may monitor the client networks for various types of conditions, including conditions regarding **network configuration....**” *Shivamoggi*, 9:23-27. Second, a POSITA would have understood that a suspected attack path is an *abnormal* configuration of network objects because suspected attack paths are identified, in part, based on the identification of abnormal or anomalous network object connection behavior. Ex. 1003, ¶¶ 65-66 (*Cf.*, *Shivamoggi*, 8:46-52 with ’554 Patent, 10:50-58); *see also Shivamoggi*, 3:21-36, 5:65-6:25, 10:26-34. Accordingly, *Shivamoggi* teaches the preamble. Ex. 1003, ¶ 69.

**2. Claim 1[a]: “collecting network object data on a plurality of network objects deployed in the cloud computing environment”**

*Shivamoggi* teaches or suggests *collecting network object data* (e.g., network data) *on a plurality of network objects* (e.g., virtual machines 214d nodes) *deployed in the cloud computing environment* (e.g., client network 212). *Shivamoggi* teaches *network objects* (i.e., virtual machines 214d nodes) *deployed in a cloud computing environment* (i.e., client network 212 including cloud-based resources within an AWS or Microsoft Azure infrastructure). *See* limitation 1[Pre], §V.A.1.

*Shivamoggi*’s cyber detection system 100 and network monitoring service 230 include a network data collection component/service (elements 120 and 240 of Figures 1 and 2):



Shivamoggi, Figs. 1 (left) and 2 (right); both annotated to show the analogous elements in system 100 and service 230); *see also id.*, 10:26-28 (“As shown in this example, the network data collection service 240 provides the **collected network data 225** to the attack monitoring service 260.”), 9:11-14, 5:13-23, 10:1-25; Ex. 1003, ¶ 72.

Regarding the collected “network object data,” the ’554 Patent teaches “network object data is data describing one or more network objects” and may include data describing, for example, object names or object network addresses or even a firewall event log. ’554 Patent, 8:10-20, 8:34-41. Ex. 1003, ¶¶ 70-71.

Similarly, Shivamoggi teaches that collected “network data may include **metadata** about internal connections that were made **among nodes** of the network during a time interval,” including among virtual machine 214d nodes (i.e., *network objects*). *Shivamoggi*, 3:13-15, 9:47-57, Fig. 2; *see also id.*, 5:52-54. Shivamoggi teaches exemplary types of metadata, including “**the source and destination nodes of the connection**, the communication protocol of the connection, the connection time and/or time length of the connection, the user that initiated the connection, the amount of data that was uploaded or downloaded over the connection, among other information.” *Shivamoggi*, 5:59-60; *see also id.*, 11:56-60; Fig. 3 (describing raw data attributes 330 that were collected from the network). A POSITA would have understood that each of these examples of metadata is data describing one or more network objects and, therefore, is “network object data” within the meaning of the ’554 Patent. Ex. 1003, ¶¶ 73-75. For example, a POSITA would have understood an identification of the source and destination nodes of a connection to include or suggest the network object addresses and the remaining examples of metadata to be information such as would be obtained from a firewall event log. *Id.* A POSITA would also have found it obvious to collect network object addresses because use of an object’s network address is the most ubiquitous means for identifying objects in a networked environment. Ex. 1003, ¶¶ 73-78

Moreover, the '554 Patent teaches that “[o]bject data may be collected [] from one or more sources including, ... network objects[.]” ’554 Patent, 8:20-31. Similarly, Shivamoggi teaches that “where the node is a virtual machine, the network data collection point may be implemented by the hypervisor running on the virtualization host.” *Shivamoggi*, 10:15-18; *see also id.*, 5:16-20, 10:1-25. Ex. 1003, ¶¶ 76-77.

3. ***Claim 1[b]: “constructing a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;”***

Shivamoggi teaches *constructing a network graph* (i.e., “connection graph”) *based on the collected network object data* (i.e., collected “network data,” *see* limitation 1[a], §V.A.2) *wherein the network graph includes a visual representation of network objects identified in the cloud computing environment*.

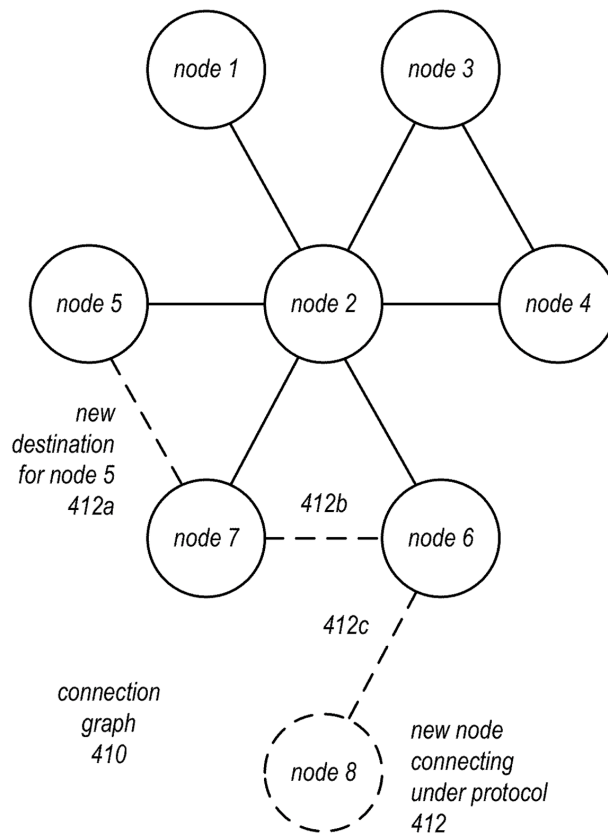
First, Shivamoggi’s connection graphs are based *on the collected network object data*. Specifically, Shivamoggi teaches that “**network data 122 collected** at each new time interval **will be processed** by a connection graph generator component 130 **to generate a set of connection graphs 140.**” *Shivamoggi*, 6:17-

20<sup>6</sup>; *see also id.*, Fig. 8 (step 820, “Generate connection graphs from the network data ...”), 17:30-52. Once generated, these connection graphs 140 are evaluated by a graph evaluator to determine which of the graphs indicate signs of suspected lateral movement. *Shivamoggi*, 7:28-33; *see also id.*, 8:1-4 (further describing the relationship between graphs 140 and 154), 8:15-19. Ex. 1003, ¶ 82. Accordingly, a POSITA would have understood that connection graphs 154 are a subset of connection graphs 140, specifically the subset of graphs that indicate signs of suspected lateral movement. Ex. 1003, ¶¶ 80-83. A POSITA would have also understood that system 100 and service 230 both generate connection graphs in the same way (i.e., using collected network data), since service 230 implements components of system 100. *See, e.g., Shivamoggi*, 9:9-27; Ex. 1003, ¶ 84 (citing *Shivamoggi*, 9:9-20, 10:26-32).

Second, *Shivamoggi*’s connection graphs each include a *visual representation of network objects* (i.e., nodes depicted as circles):

---

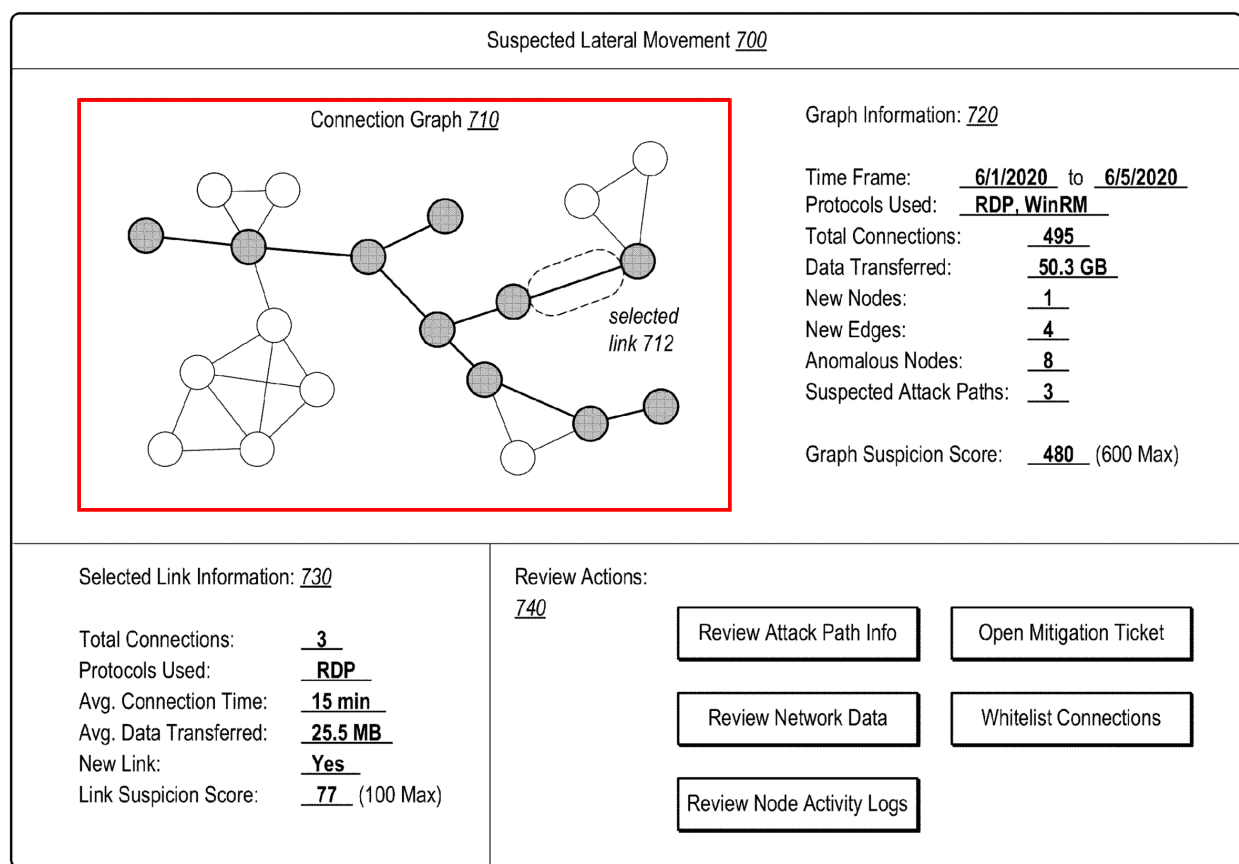
<sup>6</sup>For the reasons discussed in Claim 1[a], *Shivamoggi*’s collected “network data” is “network object data” within the meaning of the ’554 Patent.



*Shivamoggi*, Fig. 4 (excerpt); *see also id.*, 12:63-65 (“As shown, connection graph 410 indicates that eight nodes made or attempted connections to each other during a time interval.”), 12:59-60 (“connection graph 410 may be one of the connection graphs 140 of FIG. 1”), 17:31-34; *see also id.*, 12:57-13:4, 13:43-58, Fig. 5; Ex. 1003, ¶¶ 81, 85-88.

Shivamoggi also teaches that “candidate graphs 154 with suspected lateral movement are reported to the network administrator via the output interface 190.” *Shivamoggi*, 8:12-14, Fig. 7A; *see also id.*, 5:34-41 (describing how “system 100 may report its findings at different stages of the detection process to indicate things

such as connection behavior anomalies 136, connection graphs indicating suspected lateral movement attacks 154, and/or suspected attack paths 184” to the user interface 190). Shivamoggi further teaches GUI (graphical user interface) 700 “is one example of the output interface 190 of FIG. 1.” *Shivamoggi*, 15:15-19; Ex. 1003, ¶¶ 85-86. As shown in Fig. 7A “connection graph 710 associated with the detected lateral movement is displayed graphically.” *Shivamoggi*, 15:22-23, Fig. 7A:



*Shivamoggi*, Fig. 7A (annotated); *see also id.* 15:15-18. A POSITA would have understood that Shivamoggi’s connection graphs are visual “node and link” graphs as expressly contemplated by the ’554 Patent. For example, compare Shivamoggi’s

connection graphs depicted in Figs. 4, 5, 7A, 15:42-45 with those depicted in the '554 Patent at Fig 3A, 8:61-63. Ex. 1003, ¶¶ 87-88.

Third, the visually represented nodes (i.e., *network objects*) of Shivamoggi's connection graphs may be virtual machine nodes 214d of client network 212 that include cloud-based resources within an AWS or Microsoft Azure infrastructure (i.e., *network objects identified in the cloud computing environment*). See Fig. 2; limitation 1[Pre], §V.A.1.

4. ***Claim 1[c]: “determining relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects;”***

Shivamoggi teaches this limitation. The '554 Patent discloses that “descriptions of the various connections between the network objects” include “connection bandwidths, **connection durations, connection protocols**, connection names or IDs, **connection statuses....**” '554 Patent, 9:4-10. Shivamoggi teaches a network graph showing the *relationships between ... network objects*, including these “connection durations,” “connection protocols,” and “connection statuses.” Ex. 1003, ¶¶ 90-94.

First, Shivamoggi teaches a graphical display of connection statuses. *Shivamoggi*, 7:5-7 (teaching “connection graphs 140 will indicate distinct subsets of nodes in the network that **made or attempted to make connections** to each other

during the time interval.”) *Shivamoggi*, 7:5-7; *see* Claim 1[Pre], §V.A.1. Connection graphs include edges and nodes (i.e., *determin[ed] relationships between network objects in network graph*) that “may be associated with various **attributes obtained or inferred from the network data**, including various indicators of detected behavior anomalies 136” (i.e., *descriptions of connections between identified objects*). *Shivamoggi*, 7:13-16, Fig. 3. Specifically,

[a]n edge attribute may indicate that a **particular connection** is a first-time connection **between a source node to a new destination node**. In some embodiments, a graph node or edge may include an attribute that represents a negative indicator for lateral movement. For example, in some embodiments, a **graph edge may be tagged with an attribute** indicating that is consistent with the network’s baseline behavior and not likely part of a cyberattack.

*Shivamoggi*, 7:16-26; Ex. 1003, ¶¶ 90-93.

Second, *Shivamoggi* teaches that its graphically displayed connection attributes include connection protocols and connection durations. For example, *Shivamoggi* teaches the “**connection protocol** of the connection” along with “a user that initiated the connection, **the time length of the connection**, the amount of data uploaded or downloaded using the connection, etc.” *Shivamoggi*, 11:64-67, 12:19-21, Fig. 3; Ex. 1003, ¶ 92.

A POSITA would have understood the edges of Shivamoggi's connection graph themselves along with their associated attributes are *determin[ed] relationships between network objects in the network graph* at least because they are *descriptions of connections* between the nodes of the graph and include attributes describing aspects of the connections between the nodes of the graph. Ex. 1003, ¶ 93.

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

Shivamoggi teaches *analyzing the network graph and the determined relationships*. Ex. 1003, ¶¶ 95-103. For example, Shivamoggi teaches “candidate graphs 154 are further **analyzed** to determine suspected attack paths 184 in the graphs.” *Shivamoggi*, 8:15-17.<sup>7</sup>

Shivamoggi also teaches that candidates for suspected lateral movement are determined by ranking metrics in the connection graphs for a particular time interval. *Shivamoggi*, 8:1-4; *see also, Id.*, 7:33-41 (describing computation of graph metrics 152 based on “various properties of the graph,” such as the number of nodes and

---

<sup>7</sup>For the reasons discussed with respect to limitation 1[b], Shivamoggi's connection graphs 154 are a subset of connection graphs 140.

edges). As discussed above, Shivamoggi's connection graphs comprise *determined relationships* (i.e., connections) among nodes. *See* Claims 1[b], [c], §§V.A.3, V.A.4.; Ex. 1003, ¶ 96.

Subsequently, “time-ordered connection paths 170 are generated for a particular connection graph 154,” and these paths 170 “indicate a sequence of **connections** that were made in time order by a series of nodes in the candidate graph.” *Shivamoggi*, 8:22-24, 8:36-39. Then, “path evaluator 180 may generate respective path metrics 182 for each connection path 170 found in the graph,” wherein “the path metric may also take into account indicators of anomaly 136 included in the path[.]” *Shivamoggi*, 8:39-41, 8:46-51 (describing examples of anomalies 136). Finally, “path evaluator 180 will rank the path metrics 182 of all time-ordered connections in a graph, and determine a specified number of highest-ranking paths as the suspected attack paths 184,” which are then “reported” to an interface. *Shivamoggi*, 8:60-63, 9:1-2, Fig. 2; Ex. 1003, ¶¶ 96-97.

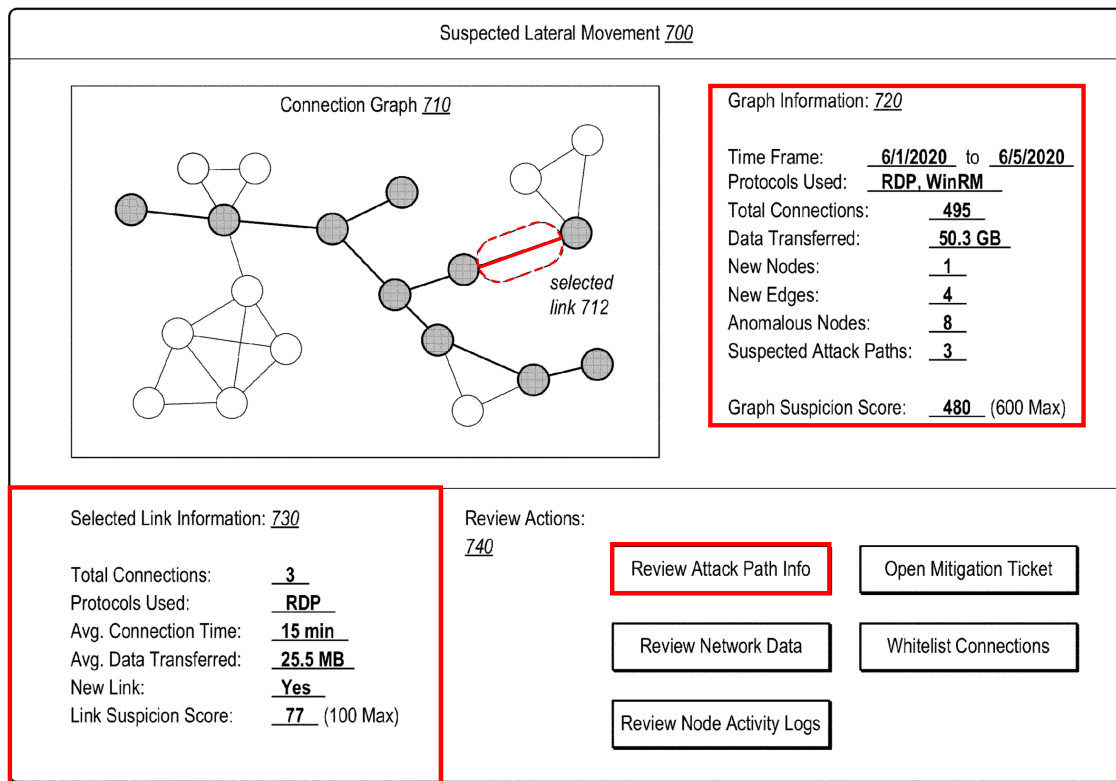
A POSITA would have understood “suspected attack paths” to be *generated insights* that *include a list of abnormal connections* within the meaning of the '554 Patent because the '554 Patent expressly teaches that *insights* may specify a path. *See, e.g., '554 Patent*, 10:31-49; Ex. 1003, ¶ 98. Likewise, Shivamoggi's attack paths demonstrate “suspected lateral movement of a cyberattack,” where “lateral

movement” is an abnormal connection path among network objects. *Shivamoggi*, 17:55-57, Figs. 3, 5; Ex. 1003, ¶¶ 62 (explaining that lateral movement is an abnormal configuration of a network), 99.

The '554 Patent also describes *insights* as “natural-language representations of aspects of the network graph[.]” ’554 Patent, 10:16-18. The '554 Patent further describes how insights include “object relationships,” and “descriptions of whether an object appears in another graph, object type counts, per-object connection counts, [and] graph connection counts....” ’554 Patent at 11:25-30. In the same way, Shivamoggi teaches “a graph information section 720 that provides a number of informational items about the graph 710....” *Shivamoggi*, 15:27-29. Such graph information includes natural-language representations of the network graph, such as “communication protocols used, the time frame of the connection behaviors shown, the total number of connections represented by the graph, the amount of data transferred within the graph, etc.” *Shivamoggi*, 15:29-32, Fig. 7A. Ex. 1003, ¶¶ 100-102.

A POSITA would have understood that a user selecting the “Review Attack Path Info” button (*see Shivamoggi*, Fig. 7A) would be provided with similar information to that provided in the “Graph Information” and “Selected Link Information” sections of Figure 7A. *Shivamoggi*, 15:51-58 (“In this example, the

user may **click on the buttons** to review additional information about the lateral movement, such as **information about a particular attack path** (e.g. the various factors that were used to compute the path metric), the underlying network data that was used to generate the connection graph 710, and also node activity logs associated with the period represented by connection graph.”), Fig. 7A; Ex. 1003, ¶ 101.

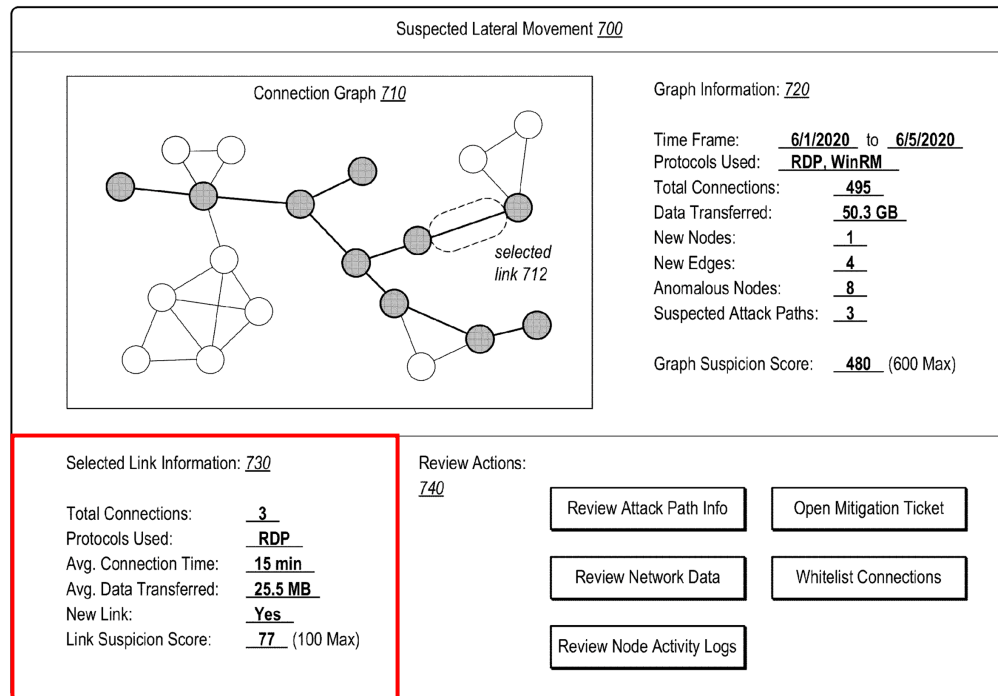


*Shivamoggi*, Fig. 7A, 15:46-47 (annotated to show generated information (i.e., *insights*) related to suspected lateral movement attack paths (i.e., *abnormal configuration*) in connection graphs (i.e., *network graphs*). Further, “path link 712 is selected, and information about that link is provided in section 730.”). A POSITA would have understood the *insights* provided in Fig. 7A, such as “Total

Connections” to match the *insights* of the ’554 Patent, which describes them as including “graph connection counts[.]” ’554 Patent, 11:25-29; Ex. 1003, ¶ 102.

6. ***Claim 1[e]: “tagging network objects in the network graph for which the insight is generated.”***

Shivamoggi teaches *tagging network objects in the network graph for which the insight is generated*. For example, Shivamoggi teaches that “GUI 700 displays a suspected lateral movement that is detected by the cyberattack detection system,” such as the connection graph 710, and “the GUI allows users to select elements within the displayed connection graph 710 (e.g. individual nodes, path links, or entire connection paths) in order to view **detailed information about the elements.**” *Shivamoggi*, 15:20-21, 15:42-45, Fig. 7A. This detailed information about the elements includes the information shown in section 730 (e.g., “Total Connections”, “Protocols Used”, etc.) of the exemplary GUI of Fig. 7A:



Shivamoggi, Fig. 7A (annotated); Ex. 1003, ¶¶ 104-106.

A POSITA would have understood that displaying detailed information about the elements in a connection graph is *tagging network objects in the network graph* as used in the '554 Patent, because the '554 Patent describes such tagging of network objects as “**association** of one or more data labels, tags, or other, like, features, **with graph entries** for one or more network objects,” just as in Shivamoggi. '554 Patent, 11:16-19, 11:21-24 (“The data labels, tags, or other, like, features, with graph entries, may include descriptions of aspects of relevant graphs, objects, relationships, and the like.”); Ex. 1003, ¶ 107. Like the “detailed information” provided in section 730 of Shivamoggi’s GUI 700, the '554 Patent provides examples of *tagging network objects* as describing “object type counts, per-object connection counts,

graph connection counts,” and “protocols relevant to an object[.]” ’554 Patent, 11:24-34; Ex. 1003, ¶ 107.

A POSITA would have further understood that the detailed information is for the *network graph for which the insight is generated* because “graph information section 720 [] provides a number of informational items **about** the graph 710[.]” *Shivamoggi*, 15:22-23; *see also id.*, 15:22-23 (describing how “the connection graph 710 **associated with the detected lateral movement** is displayed graphically....”). Ex. 1003, ¶ 104.

Additionally, the ’554 Patent discloses that “network graph schema 300, and corresponding network graph utility, may be configured to provide for various **interactive** functionalities” such as “a user interact[ing] with a node.” ’554 Patent, 12:5-8. In the same way, *Shivamoggi* teaches a GUI that “allows users to **select** elements within the displayed connection graph 710 (*e.g.*, individual nodes, path links, or entire connection paths) in order to view detailed information about the elements.” ’554 Patent, 12:5-8; *Shivamoggi*, 15:42-47; Ex. 1003, ¶ 106.

- B. Claim 4: “The method of claim 1, wherein generating insights to include at least the list of abnormal connections further comprises: detecting any one of: a rare network configuration, a novel network configuration, a rare network event, a novel network event, a connection of a new device to a network, an unauthorized connection, a re-connection of a user device to a subnet which the user is not permitted to access, a connection demonstrating anomalous behavior or misconfiguration, and a connection demonstrating spikes of network activity.”**

Shivamoggi teaches that *generating insights to include at least the list of abnormal connections further comprises: detecting a connection of a new device to a network*. As described above, Shivamoggi teaches generating time-ordered connection paths 170 from connection graphs 140, which are then evaluated and ranked (in part based on detected anomalies 136 in the path), with the highest ranked paths being reported as the suspicious attack paths 184. *Shivamoggi*, 8:22-24, 8:36-51, 8:60-63; *see* Claim 1[d], §V.A.5. Shivamoggi also teaches ranking connection graphs using graph metric 152 and path metric 182, each of which are computed based on, among other factors, “the presence or number of new edges in the graph (e.g. nodes connecting to a new destination node for a first time).” *Shivamoggi*, 4:4-16, 4:31-35; *see also*, *Shivamoggi*, 7:38-52, 8:15-58. Accordingly, a POSITA would have understood “nodes connecting to a new destination for a first time” to be *detecting a connection of a new device to a network*. *Id.*; Ex. 1003, ¶ 112.

Additionally, Shivamoggi teaches that *generating insights to include at least the list of abnormal connections further comprises: detecting a rare and/or novel*

*network event*. Ex. 1003, ¶¶ 109-111. A POSITA would have understood that the data (e.g., anomalies 136) included in generating suspected lateral movement attack paths 184 constitutes *detecting a novel and/or rare network event* within the meaning of the '554 Patent because the '554 Patent describes “events which are rare or novel” as the “connection of a new device to a network,...connections which display anomalous behavior, such as connections displaying spikes of network activity, and the like.” '554 Patent, 10:57-62; Ex. 1003, ¶¶ 113-114. In the same way, Shivamoggi teaches “indicators of detected behavior anomalies 136” (which are included in calculating the path and graph metrics) include “the presence or count of new nodes that used a communication protocol for a first time, or the presence or count of connections that represent a first-time connection between a source node and a destination node.” *Shivamoggi*, 7:15-18, 8:48-51. Additionally, Shivamoggi's connection graphs 140 are initially generated either on a schedule or in response to “triggering conditions” such as “a **spike** in the activity level of the **network (or a particular node)**, etc.” *Shivamoggi*, 6:61–7:2; Ex. 1003, ¶ 114.

**C. Claim 7: “The method of claim 1, wherein determining the relationships between the identified network objects in further comprises: determining the relationships using at least one of: observational methods, and active logging methods.”**

Shivamoggi teaches that *determining the relationships between the identified network objects in further comprises: determining the relationships using at least*

*one of: observational methods, and active logging methods* (i.e., cyberattack detection system monitoring a network and its data).

The '554 Patent describes “observational or active logging methods” “as methods providing for detection of object-to-object connections by monitoring traffic of a network in use.” ’554 Patent, 10:10-14; Ex. 1003, ¶ 116. In the same way, Shivamoggi teaches a cyberattack detection system that collects network data, including metadata about internal connections between nodes of the network during a time interval. *Shivamoggi*, 3:7-19 (exemplary metadata includes “which other nodes a node connected to....”); *see also id.*, 1:36-39 (“In one embodiment, the system collects network data from a computer network, which indicates connections among nodes in the network.”). Shivamoggi also teaches collecting network data to monitor a network by “using a network data collector component 120” or “network data collection points (e.g., networking switches or routers) in the client network[.]” *Shivamoggi*, 5:13-23; *see also, Shivamoggi*, 5:52-64, 6:17-34; 16:51-58; Fig. 7; Claim 14; Ex. 1003, ¶¶ 116-117.

A POSITA would have understood that Shivamoggi’s cyberattack system monitors “traffic of a network in use” as described in the '554 Patent as an example of an observational or active logging method because the Shivamoggi system collects “metadata about internal connections” during the monitoring period,

indicating the network is in use and collects “how much data was transmitted over the connections” in addition to other data about the relationship between objects in the network. *Shivamoggi*, 3:5-19; 3:47-59; ’554 *Patent*, 10:14; Ex. 1003, ¶¶ 118-120.

**D. Claim 8: “The method of claim 1, further comprising: adding visual representations of the determined relationships to the visual representations of the network graph.”**

*Shivamoggi* teaches *adding visual representations of the determined relationships* (i.e., highlighting suspected attack paths) *to the visual representations of the network graph* (i.e., connection graphs).

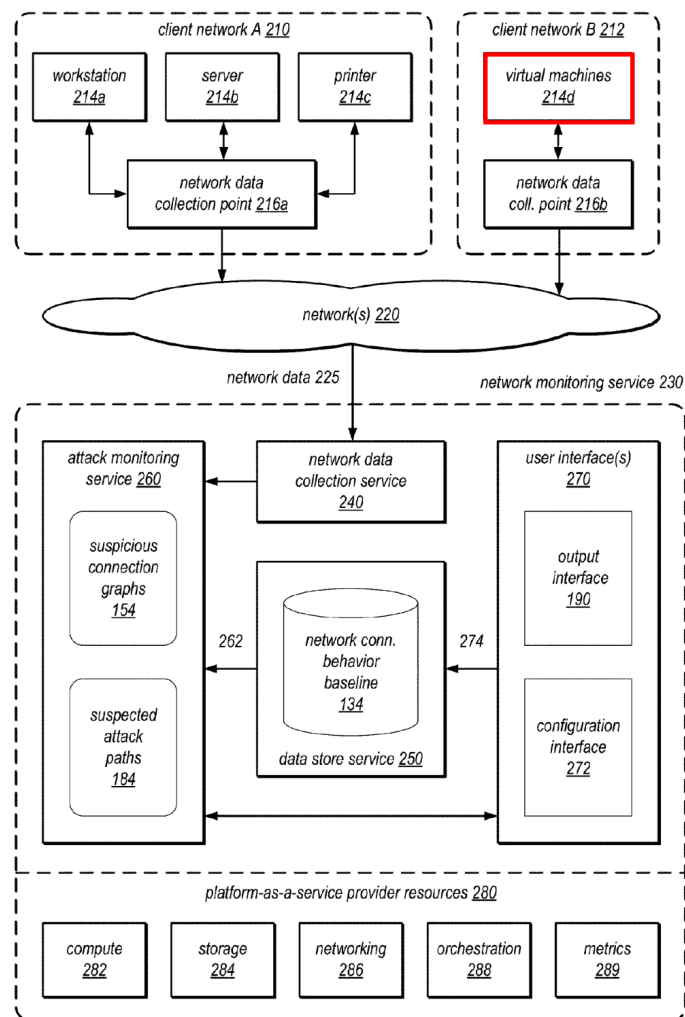
Specifically, *Shivamoggi* teaches that “**connection graph 710** associated with the detected lateral movement is **displayed graphically**” and that “graph 710 highlights certain nodes and edges to indicate the nodes and paths that are involved in suspected lateral movement attack paths.” *Shivamoggi*, 15:24-26. Ex. 1003, ¶¶ 122-123. Similarly, the ’554 *Patent* describes visualizing “a network system” using a visual ““node-and-link graph”” that is “update[ed] to include visible ‘links’ or connections between object ‘nodes’” ’554 *Patent*, 9:49-58 (further describing “updating the original visible graph to include such links, [by] adding a second, visible overlay to the graph, including the links....”), Fig. 2. A POSITA would have understood *Shivamoggi*’s graph 710 is a node-and-link graph as it comprises “individual nodes” and “path links” between them. *Shivamoggi*, 15:43-44; *cf.* ’554

*Patent*, Fig. 3A, with *Shivamoggi*, Fig. 7A; Ex. 1003, ¶¶ 87-88 (describing node-and-link graph), 123; see limitation 1[b], §V.A.3. *Shivamoggi* also teaches that findings can be reported at different stages of detecting lateral movement. *Shivamoggi*, 5:27-31, 5:34-41 (describing how “system 100 may report its findings at different stages of the detection process to indicate things such as connection behavior anomalies 136, **connection graphs indicating suspected lateral movement** attacks 154, and/or suspected attack paths 184” to the user interface 190). A POSITA would have understood *Shivamoggi*’s teachings to mean that a connection graph (without a suspected attack path highlighted) could be presented to a user and then that same graph could be presented to the user at a later stage with the attack path nodes and edges highlighted, thereby adding a visual representation of the determined relationships. Ex. 1003, ¶¶ 124-126.

To the extent Patent Owner argues this claim requires adding edges to a graph only after first visualizing nodes of the graph, such an implementation would have been obvious in view of *Shivamoggi*’s disclosure that it “may report its findings at different stages of the detection process[.]” *Shivamoggi*, 5:37-38; Ex. 1003, ¶ 126.

- E. **Claim 9: “The method of claim 1, wherein each of the plurality of network objects includes any one of: a virtual network, a firewall, a network interface card, a proxy, a gateway, a software container, container, a management object, a virtual machine, a subnet, a hub, a virtual private network (VPN).”**

Shivamoggi teaches that *each of the plurality of network objects includes a virtual machine* (i.e., virtual machine 214d nodes). See limitation 1[Pre], §V.A.1; Ex. 1003, ¶¶ 128-130.



Shivamoggi, Fig. 2 (annotated).

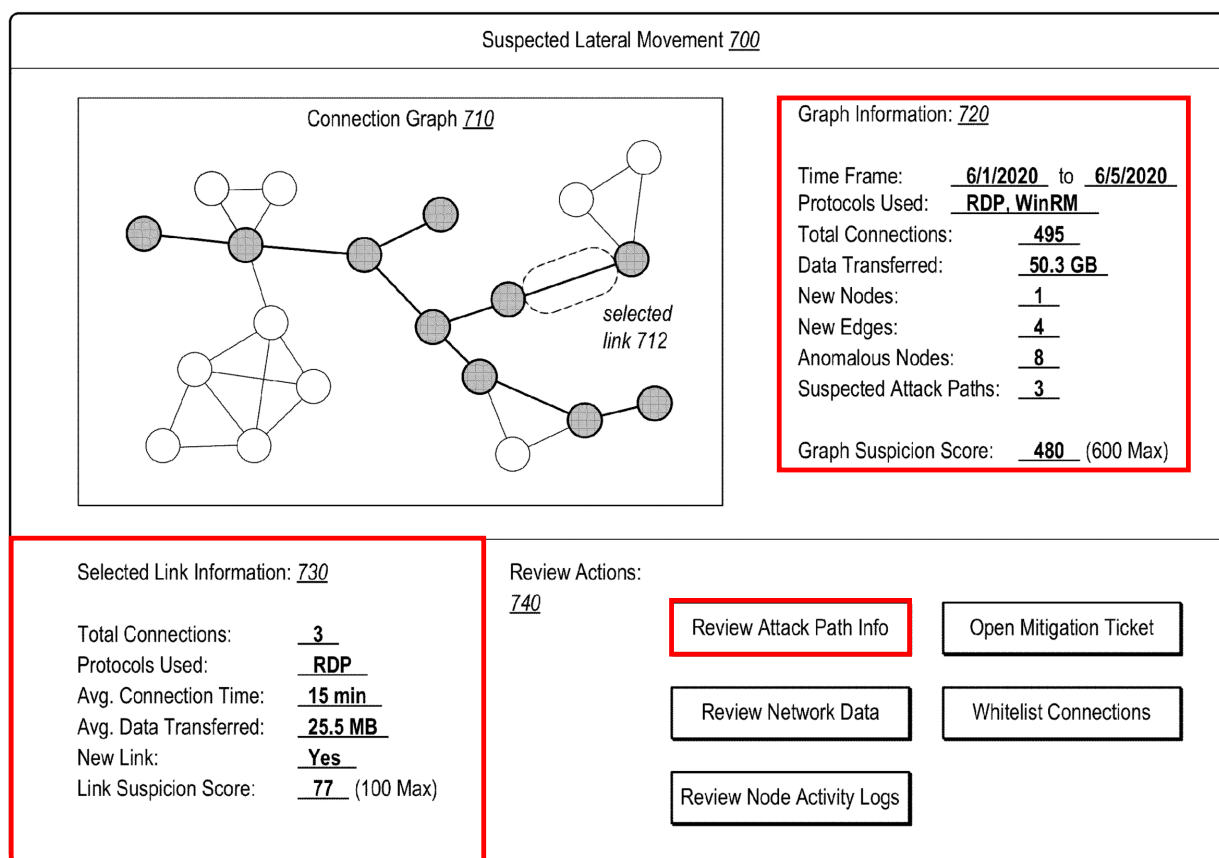
**F. Claim 10: “The method of claim 1, wherein a generated insight of the generated insights is generated utilizing natural language representation.”**

Shivamoggi teaches that *a generated insight of the generated insights is generated utilizing natural language representation.*

The '554 Patent describes *insights* as “natural-language representations,” and states that “insights may include pure-text descriptions of objects and relationships.” ’554 Patent, 10:17-20. Thus, a POSITA would have understood natural language representations to at least include pure-text descriptions of network objects and their relationships. *Id.* Ex. 1003, ¶ 131.

Shivamoggi teaches providing pure-text descriptions of connection graphs, selected link information, and overall attack path information. *See, e.g., Shivamoggi*, 15:27-41 (describing the information provided in graph information section 720 about graph 710 including “communication protocols used” and “the amount of data transferred within the graph, etc.”), 15:42-47 (describing when “a particular path link 712 is selected” “information about that link is provided in section 730.”), 15:48-61 (describing “review actions section 740, which provides a number of control elements to allow the user to perform a variety of actions when reviewing the reported lateral movement.”), Fig. 7A; Ex. 1003, ¶ 132. Pure-text *insights* can include at least listing of “Protocols Used” as shown in Fig. 7A, along with “the number of new nodes using a new protocol included in the graph” “and the total

number of anomalous nodes in the graph.” *Shivamoggi*, 15:29-38, Fig. 7A; Ex. 1003,  
¶ 133. A POSITA would have understood that a user selecting the “Review Attack  
Path Info” button would provide the user with similar information to that provided  
in the Graph Information 720 and Selected Link Information 730 sections of Fig.  
7A:



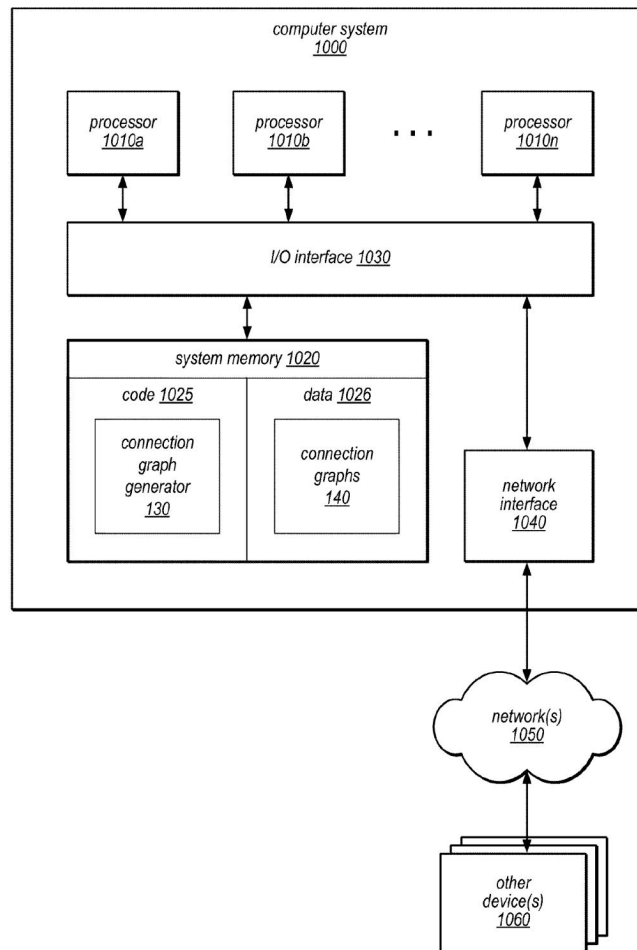
*Shivamoggi*, Fig. 7A (annotated); Ex. 1003, ¶¶ 134-135.

**G. Claim 11[Pre]: “A non-transitory computer readable medium having stored thereon instructions for causing a processing circuitry to execute a process for determining abnormal configuration of network objects deployed in a cloud computing environment, the process comprising:”**

To the extent the preamble is limiting, Shivamoggi alone teaches or suggests *a non-transitory computer readable medium having stored thereon instructions for causing a processing circuitry to execute a process for determining abnormal configuration of network objects deployed in a cloud computing environment (i.e., cyberattack detection system). See Claim 1[Pre].*

Shivamoggi expressly teaches “system memory 1020 may be used to store code 1025 or **executable instructions to implement the methods** and techniques described herein” such as “instructions to implement connection graph generator 130” of the cyberattack detection system. *Shivamoggi*, 20:42-46, Fig. 10. Shivamoggi also expressly teaches that “some of the code 1025 or executable instructions may be persistently **stored** on the computer system 1000 and may have been loaded from external storage media. The persistent storage of the computer system 1000 and the external media are examples of **non-transitory computer-readable storage media**, which may be used to **store program instructions to be executed by the computer system 1000.**” *Shivamoggi*, 20:52-54; *see also id.*, 20:61-64 (providing examples of non-transitory computer-readable storage media including “DVD/CD-ROM devices” and “network-attached storage systems[.]”).

Further, Shivamoggi's "computer system 1000 includes one or more processors 1010" "capable of executing instructions." *Shivamoggi*, 20:1-2, 20:9-10, Fig. 10; Ex. 1003, ¶¶ 137-138.



*Shivamoggi*, Fig. 10.

The process for determining abnormal configuration of network objects deployed in a cloud computing environment is as described above in limitation 1[Pre]. See *supra*, §V.A.1; Ex. 1003, ¶ 139.

**H. Claim 11[a]: “collecting network object data on a plurality of network objects deployed in the cloud computing environment;”**

*See* limitation 1[a], §V.A.2; Ex. 1003, ¶¶ 159-169.

**I. Claim 11[b]: “constructing a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;”**

*See* limitation 1[b], §V.A.3; Ex. 1003, ¶¶ 170-180.

**J. Claim 11[c]: “determining relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects;”**

*See* limitation 1[c], §V.A.4; Ex. 1003, ¶¶ 181-186.

**K. Claim 11[d]: “analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and”**

*See* limitation 1[d], §V.A.5; Ex. 1003, ¶¶ 187-196.

**L. Claim 11[e]: “tagging network objects in the network graph for which the insight is generated.”**

*See* limitation 1[e], §V.A.6; Ex. 1003, ¶¶ 197-202.

**M. Claim 12[Pre]: “A system for determining abnormal configuration of network objects deployed in a cloud computing environment, comprising:”**

*See* limitation 11[Pre], §V.G; Ex. 1003, ¶¶ 203-224.

**N. Claim 12[a]: “a processing circuitry; and”**

*See* limitation 11[Pre], §V.G; Ex. 1003, ¶¶ 203-224.

**O. Claim 12[b]: “a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to:”**

*See* limitation 11[Pre], §V.G; Ex. 1003, ¶¶ 203-224.

**P. Claim 12[c]: “collect network object data on a plurality of network objects deployed in the cloud computing environment;”**

*See* limitations 1[a], §V.A.2; Ex. 1003, ¶¶ 225-235.

**Q. Claim 12[d]: “construct a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;”**

*See* limitations 1[b], §V.A.3; Ex. 1003, ¶¶ 236-246.

**R. Claim 12[e]: “determine relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects;”**

*See* limitations 1[c], §V.A.4; Ex. 1003, ¶¶ 247-252.

**S. Claim 12[f]: “analyze the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and”**

*See* limitations 1[d], §V.A.5; Ex. 1003, ¶¶ 253-262.

- T. Claim 12[g]: “tagging network objects in the network graph for which the insight is generated.”**

*See* limitations 1[e], §V.A.6; Ex. 1003, ¶¶ 263-268.

- U. Claim 15: “The system of claim 12, wherein the system is further configured to: detect any one of: a rare network configuration, a novel network configuration, a rare network event, a novel network event, a connection of a new device to a network, an unauthorized connection, a re-connection of a user device to a subnet which the user is not permitted to access, a connection demonstrating anomalous behavior or misconfiguration, and a connection demonstrating spikes of network activity.”**

*See* Claim 4, §V.B; Ex. 1003, ¶¶ 269-276.

- V. Claim 18: “The system of claim 12, wherein the system is further configured to: determine the relationships using at least one of: observational methods, and active logging methods.”**

*See* Claim 7, §V.C; Ex. 1003, ¶¶ 277-282.

- W. Claim 19: “The system of claim 12, wherein the system is further configured to: adding visual representations of the determined relationships to the visual representations of the network graph.”**

*See* Claim 8, §V.D; Ex. 1003, ¶¶ 283-289.

- X. Claim 20: “The system of claim 12, wherein each of the plurality of network objects includes any one of: a virtual network, a firewall, a network interface card, a proxy, a gateway, a software container, container, a management object, a virtual machine, a subnet, a hub, a virtual private network (VPN).”**

*See* Claim 9, §V.E; Ex. 1003, ¶¶ 290-293.

- Y. **Claim 21: “The system of claim 12, wherein a generated insight of the generated insights is generated utilizing natural language representation.”**

*See* Claim 10, §V.F; Ex. 1003, ¶¶ 294-300.

## **VI. GROUND 2: CLAIMS 2, 3, 13, AND 14 ARE OBVIOUS OVER SHIVAMOGGI AND ZHONG**

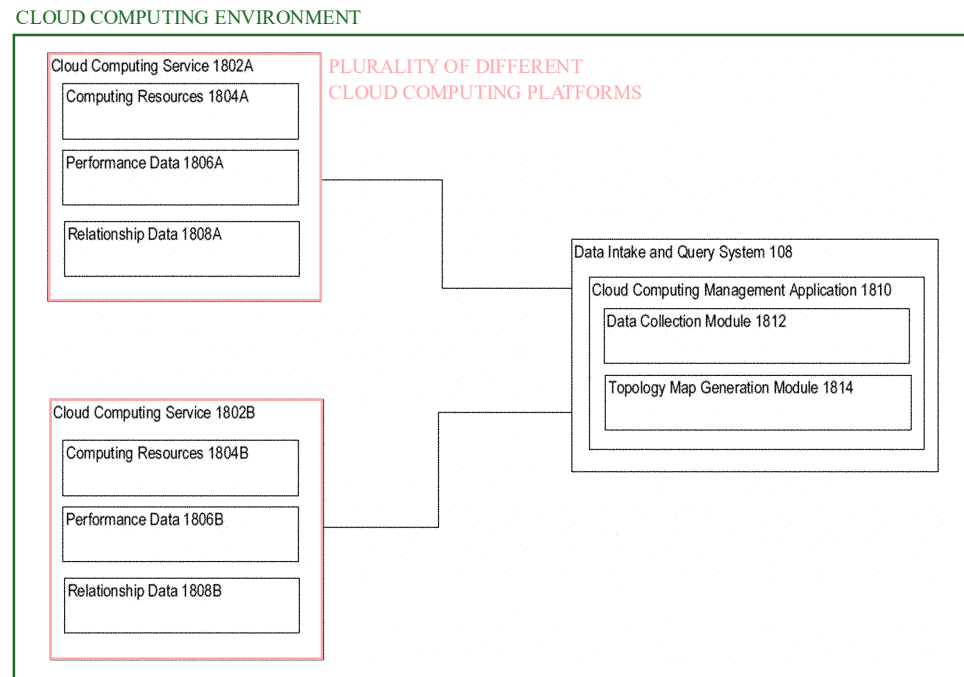
- A. **Claim 2: “The method of claim 1, wherein the cloud computing environment includes a plurality of different cloud computing platforms.”**

Shivamoggi does not expressly teach a client network that includes cloud-based resources of a plurality of different cloud computing platforms. The Shivamoggi-Zhong combination teaches that *the cloud computing environment includes a plurality of different cloud computing platforms*, as taught by Zhong. Ex. 1003, ¶¶ 301-315.

### ***1. Zhong’s Teachings***

Zhong teaches *a cloud computing environment* (i.e., networked computer environment) that *includes a plurality of different cloud computing platforms* (i.e., cloud computing services). Namely, Zhong teaches that cloud computing management application 1810 permits users to collect and manage data from a networked computing environment comprising “**any number** of separate cloud computing services” including at least Amazon Web Services (AWS), Microsoft

Azure, or Google Cloud. *Zhong*, 38:65–39:3; 39:40–42, Fig. 18; Ex. 1003, ¶¶ 301–306.



*Zhong*, Fig. 18 (annotated to show *a plurality of different cloud computing platforms* (i.e., cloud computing services 1802A and 1802B) in *a cloud computing environment* (i.e., networked computing environment)), 38:54–39:7 (“The networked computer environment of Fig. 18 includes cloud computing services 1802A and 1802B and data intake and query system 108” wherein “each of cloud computing services 1802A and 1802B generally represents **any collection** of remote computing services offered by a cloud computing service provider.”).

Like Shivamoggi, *Zhong* teaches collecting data from and about the networked computing environment, including “data related to a collection of cloud

computing resources **from one or more** cloud computing services” comprising at least “information about” “relationships with other resources” among other “attributes of the resources.” *Zhong*, 41:7-19 (further describing how “data related to the cloud computing resources may originate from **one or more** cloud computing service providers....”); *see also*, *Zhong*, 39:8-34 (describing the data collected); Ex. 1003, ¶ 307.

## **2. Motivation to Combine Shivamoggi and Zhong**

A POSITA would have been motivated to modify Shivamoggi’s *cloud computing environment* to include[] *a plurality of different cloud computing platforms*, as taught by *Zhong*. Ex. 1003, ¶¶ 308-315. *Zhong* provides an express motivation to combine its disclosures with Shivamoggi by noting that “conventional cloud computing service management consoles enable users to view some information related to the user’s cloud computing resources, the disconnected nature of such interfaces may present challenges when attempting to obtain broader information about an entire collection of resources.” *Zhong*, 38:6-11. *Zhong* goes on to describe the benefits of collecting and jointly analyzing the information for all of a client’s cloud computing providers together:

In one embodiment, a cloud computing management application is configured to **collect data related to a collection of cloud computing resources** and to store the data in a format that enables **more efficient**

**analysis**, for example, as event data stored by a data intake and query system. **The collected data** generally may comprise any available information related to the computing resources, including performance data, relationship data, state data, log data, etc., and may originate from **cloud computing service providers** or any other source. In an embodiment, **a cloud computing management application is further configured to generate and cause display of interactive topology map representations of cloud computing resources** based on the collected data.

*Zhong*, 38:27-40. Ex. 1003, ¶¶ 308-311. A POSITA would have valued the improvement in efficiency and holistic view provided by a multi-cloud platform approach, as taught by *Zhong*, because the improved efficiency and ability to analyze data in “ways not possible using conventional cloud computing service management consoles” were known to be desirable goals at the time. *Zhong*, 38:45-46; Ex. 1003, ¶ 312 (citing Ex. 1009 to Lotem).

Additionally, a POSITA would have had a reasonable expectation of success in modifying *Shivamoggi* with *Zhong* at least because *Shivamoggi* contemplates using the same cloud computing services as taught by *Zhong*, including AWS and Microsoft Azure and the only modification required is collection of data from the multiple service providers. *Shivamoggi*, 9:56-57; Ex. 1003, ¶ 313. Further, it was well-known that it was desirable for cloud monitoring systems (like *Shivamoggi*’s cyberattack detection system) to jointly monitor all of the cloud resources across the

various cloud providers to improve security and ease administrative workload. Ex. 1003, ¶ 312 (citing Ex. 1009 to Lotem).

The modification of Shivamoggi with Zhong would also have been a simple substitution of one known element (i.e., the use of a single cloud platform such as AWS or Azure within an environment) for another (i.e., the use of multiple cloud platforms such as AWS and Azure within an environment) to obtain the predictable result of improved efficiency and ability to analyze data, as taught by Zhong. Ex. 1003, ¶ 314. Adding the multiple cloud platforms of Zhong to Shivamoggi would have also been obvious to try, since demands for a single system to monitor cross-platform data were well understood at the time. *Id.*

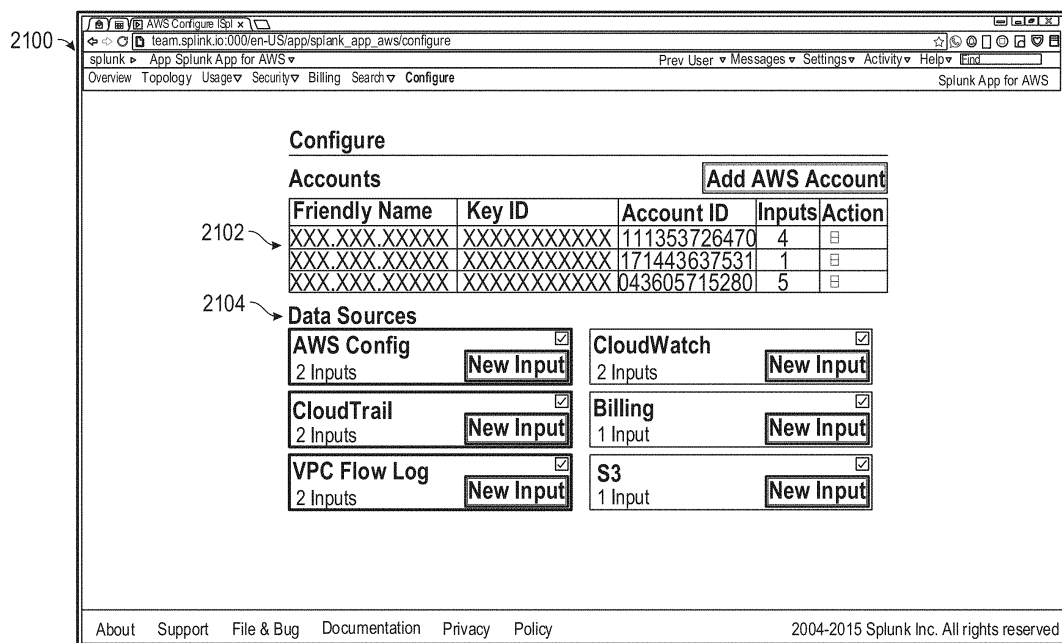
**B. Claim 3: “The method of claim 2, wherein collecting network object data further comprises: connecting through an application programing interface (API) each of the plurality of different cloud computing platforms to collect network object data of network objects deployed in the respective cloud computing platform.”**

Shivamoggi-Zhong further modified to include *an application programing interface (API)*, per Zhong, teaches Claim 3.

### ***1. Zhong’s Teachings***

Zhong expressly teaches “a particular cloud computing service may provide one or more **APIs** or other services that enable users to **retrieve various types of data** generated by the service” such as “a log file that records each time a resource is created, modified, deleted, etc.” *Zhong*, 41:67–42:2, 42:38-42. As described

above, cloud computing services comprise “any number of” services, including Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. *Zhong*, 38:66–39:5; *see* Claim 2, §VI.A; Ex. 1003, ¶¶ 316-317. *Zhong* teaches collecting relationship data from data sources, such as “a web service provided by a cloud computing service that includes an **API** for retrieving log files and/or other data related to a user’s cloud computing resources managed by the service.” *Zhong*, 41:59-62, 42:38-42. Ex. 1003, ¶¶ 318-323.



*Zhong*, Fig. 21 demonstrating multiple cloud computing platform data sources, which would each have their own *respective* API for enabling data collection. Ex. 1003, ¶ 324 (citing *Zhong*, 42:14-22).

## 2. *Motivation to Combine*

See §VI.A.2 above. Additionally, a POSITA would have been motivated to modify Shivamoggi *to collect network object data of network objects deployed in the respective cloud computing platform by connecting through an API*, in accordance with the teachings of Zhong. For example, the Shivamoggi-Zhong combination includes a cloud computing environment with multiple cloud computing platforms in the same system. See Claim 2, §VI.A. A POSITA would have also understood that “APIs...enable users to retrieve various types of data generated by the service.” Zhong, 42:1-2. Ex. 1003, ¶¶ 325-327. A POSITA would have been motivated to improve the integration between Shivamoggi’s cyberattack detection system and the respective cloud computing platforms by connecting them using an API, which was a well-known technique for connecting two different systems. Ex. 1003, ¶ 327 (citing Ex. 1010 to Pogrebinsky).

Shivamoggi already teaches a graphical user interface (GUI) 700 that permits administrators to review collected network data from network objects deployed in the cloud computing environment. Shivamoggi, 15:15-23, Fig. 7A, Fig. 10. Zhong teaches interface screen 2100 that “enables a user to configure one or more data sources for collection of data related to one or more cloud computing resources” through APIs for multiple cloud computing services. Zhong, 42:14-17, 42:39-40. It would have been well within the knowledge of a POSITA to integrate Shivamoggi’s

cyberattack detection system with an API *connect[ed]* to a *respective* cloud computing platform among the *plurality of cloud computing platforms*, as taught by Zhong. Ex. 1003, ¶¶ 328-329. Further, it was well-known that a “UI [(user interface)] and API integration allows users to see resources and services coming from different clouds as if they came from one ‘integrated’ or hybrid cloud.” *See, e.g.*, Ex. 1010, [0005]. Indeed, using an API is a ubiquitous technique that is employed throughout the field of computing and networks to share data across systems and networks. Ex. 1003, ¶¶ 327-330. For at least these reasons, a POSITA would have had a reasonable expectation of success in modifying Shivamoggi with the teachings of Zhong. *Id.*

The combination of Shivamoggi and Zhong would have also been the combination of known elements (i.e., cloud platform APIs and network monitoring systems) to yield the predictable results of efficient exchange of data between a cloud computing platform and a network monitoring system. Ex. 1003, ¶ 330.

**C. Claim 13: “The system of claim 12, wherein the cloud computing environment includes a plurality of different cloud computing platforms.”**

*See* limitations 12[Pre]-12[g] and Claim 2, §§V.M-V.T, VI.A (teachings and motivations to combine incorporated therein); Ex. 1003, ¶¶ 301-315.

- D. Claim 14: “The system of claim 13, wherein the system is further configured to: connect through an application programming interface (API) each of the plurality of different cloud computing platforms to collect network object data of network objects deployed in the respective cloud computing platform.**

*See* limitations 12[Pre]-12[g] and Claim 3, §§V.M-V.T, VI.B (teachings and motivations to combine incorporated therein); Ex. 1003, ¶¶ 316-331.

## **VII. GROUND 3: CLAIMS 5 AND 16 ARE OBVIOUS OVER SHIVAMOGGI AND WOOLWARD**

- A. Claim 5: “The method of claim 4, further comprising: determining impermissible relationships between the network objects.”**

Shivamoggi-Woolward teaches, suggests, or renders obvious Claim 5. In the combination, Shivamoggi’s cyberattack detection system is modified to include determining impermissible relationships between network objects, as taught by Woolward’s system 200.

The ’554 Patent describes the “permissibility analysis” for identifying impermissible network object relationships as the

comparison of determined relationships with one or more dictionaries, or other, like, repositories of object relationship information, to determine whether a given relationship matches a predefined relationship included in the dictionary, where such a predefined relationship may be pre-tagged as ‘permissible,’ ‘not permissible,’ or the like.

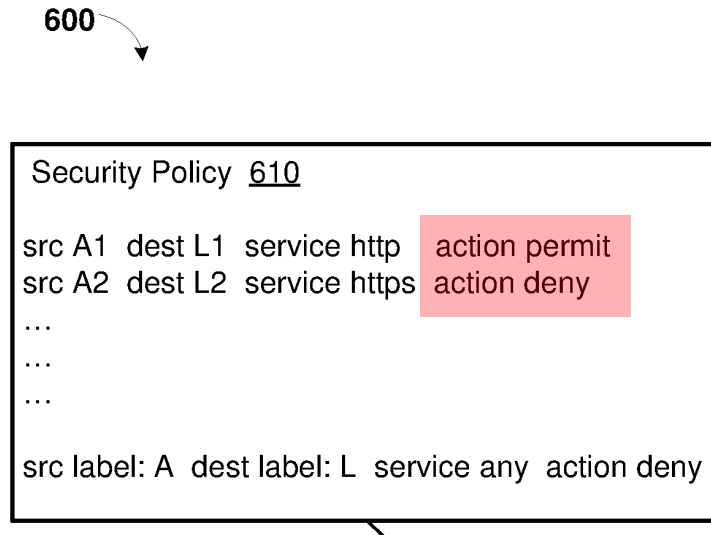
'554 Patent, 9:62–10:2, Fig. 2. Accordingly, a POSITA would have understood that a method performing a “comparison of determined relationships with one or more dictionaries or” “repositories” constitutes *determining impermissible relationships between network objects*, as claimed. *Id*; Ex. 1003, ¶ 332.

**1. *Woolward's Teachings of Determining Impermissible Relationships***

Like Shivamoggi, Woolward teaches *network objects*; namely, workloads 110<sub>1,1</sub>-110<sub>X,Y</sub>, each of which “can be a unit of computing resource, such as a...**virtual machine**[.]” *Woolward*, [0018]. Woolward also teaches identifying the relationships between network objects (i.e., workloads). Specifically, Woolward teaches “a method for validating security policy in a cloud computing environment,” comprising “providing a graph database” that “may represent workloads of the cloud computing environment as nodes and **relationships** between the workloads as edges.” *Woolward*, [0006], [0029]. Ex. 1003, ¶ 333.

Woolward further teaches *determining impermissible relationships* (i.e., relationship “violations”) *between network objects* (i.e., workloads including virtual machines) by comparing determined relationships among nodes with a “repository” (i.e., a security policy which “may logically describe rules for the relationships between the workloads”). *Woolward*, [0006]; Ex. 1003, ¶ 334 (citing *Woolward*, [0067] describing the generation of the security policy by the user.) Specifically,

Woolward teaches a graph database 225 that shows relationships (“edges”) between workloads (“nodes”). *See, e.g., Woolward*, [0006], [0029] (“Graph database 225 uses a graph data model comprised of nodes (also referred to as vertices), which is an entity such as a workload (e.g., of workloads 110<sub>1,1</sub>-110<sub>X-Y</sub> in Fig. 1), and edges, which represent the relationship between two nodes. Edges can be referred to as relationships.”). Woolward teaches pairing the security policy to the graph database and “simulating the security policy using the graph database by traversing the nodes and edges in the graph database” to determine and produce “a list of violations” for the user to review. *Woolward*, [0068]-[0069]; Ex. 1003, ¶ 335. Violations include connections between workloads that are deemed “not allowed” (e.g., *impermissible*) per “rules of the security policy.” *Woolward*, [0064], [0068], Figs. 6, 7. A POSITA would have understood Woolward’s security policy to be a “dictionary” or “repository” within the meaning of the ’554 Patent at least because workload relationships are “pre-tagged” as “action permit” (e.g., “permissible”) or “action deny” (e.g., “impermissible”), for example, as shown in Fig. 6:



*Woolward*, Fig. 6 (excerpt, annotated), [0060]; *Cf. Woolward*, [0068] with ’554 Patent, 9:62–10:2; Ex. 1003, ¶¶ 335-337.

## 2. *Motivation to Combine*

A POSITA would have been motivated to incorporate *Woolward*’s “method for validating security policies in a cloud computing environment” into *Shivamoggi*’s cyberattack detection system for several reasons. *Woolward*, [0006], Fig. 7.

*Shivamoggi*’s cyberattack detection system determines relationships between network objects. *See* limitation 1[Pre], §V.A.1. *Shivamoggi*’s system also employs methods of determining abnormal configurations of network objects. *Id.* *Woolward* expands on this concept by teaching an additional method of comparing connection graphs of virtual machine nodes to a “dictionary” like a security policy to *determine*

*impermissible relationships between the network objects* (i.e., relationship violations with the policy). Ex. 1003, ¶ 338.

Shivamoggi also notes that “human analysis to verify detected attack signals” “can be extremely labor-intensive, time-consuming, and error-prone for large networks.” *Shivamoggi*, 1:21-23. Therefore, a POSITA would have appreciated that automated methods detecting unwanted connections between nodes (which could be indicative of lateral movement attack paths) in a cyberattack detection system would have improved the ease and accuracy of network management and security. Ex. 1003, ¶¶ 339-340. Indeed, Shivamoggi acknowledges that “lateral movement is notoriously hard to detect” and thus a POSITA would have appreciated that using a security policy, as taught by Woolward, would further improve the efficiency of detecting undesirable connections and help prevent network data and resources potentially being stolen or compromised through an attack. *Shivamoggi*, 1:9-12; Ex. 1003, ¶ 340.

Such a combination would have had a reasonable expectation of success because Woolward teaches that its security policy can be deployed “in one or more cloud computing environments of cloud services 260<sub>1</sub>-260<sub>Z</sub> (e.g., Amazon Web Services (AWS), Microsoft Azure,” and Shivamoggi’s nodes are deployed in these same cloud services. *Woolward*, [0044]; *Shivamoggi*, 9:49-57. Further, network

management systems were generally well-known in the art, and combining these known methods of network management would have yielded the predictable result of improving the efficiency of detecting abnormal configurations. Ex. 1003, ¶¶ 341-342.

Shivamoggi's system determines relationships between network objects. Therefore, it would have been obvious to try to determine the impermissibility of these relationships, especially given Shivamoggi's intent to "detect an attacker's lateral movement in the network as it is happening," at least because identifying impermissible relationships as they are established would in turn prevent such lateral movement. *Shivamoggi*, 1:9-11; Ex. 1003, ¶ 343.

**B. Claim 16: "The system of claim 12, wherein the system is further configured to: determine impermissible relationships between the network objects."**

*See* limitations 12[Pre]-12[g] and Claim 5, §§V.M-V.T, VII.A (teachings and motivation to combine incorporated therein); Ex. 1003, ¶¶ 332-344.

## **VIII. CONCLUSION**

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Robin A. Snader  
Robin A. Snader, Reg. No. 66,085  
robin.snader@eriseip.com  
7015 College Boulevard, Suite 700  
Overland Park, Kansas 66211  
(913) 777-5600 Telephone  
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

**IX. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)**

**A. Real Party-In-Interest**

Petitioner is the real party-in-interest. 37 C.F.R. § 42.8(b)(1).

**B. Related Matters**

The '554 Patent is presently asserted in the stayed district court litigation: *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23-CV-00758 (D. Del.). The '554 Patent is not currently and has not been subject to any other district court litigation, *inter partes* review, reexamination, or other post-grant proceeding.

**C. Lead and Back-Up Counsel**

Petitioners provide the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

| Lead Counsel                                                                                                                                                                                                                                                            | Back-Up Counsel                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Robin A. Snader (Reg. No. 66,085)<br>robin.snader@eriseip.com<br>PTAB@eriseip.com<br><br><u>Postal and Hand-Delivery Address:</u><br>ERISE IP, P.A.<br>7015 College Blvd., Suite 700<br>Overland Park, Kansas 66211<br>Telephone: (913) 777-5600<br>Fax: (913) 777-5601 | Eric A. Buresh (Reg. No. 50,394)<br>eric.buresh@eriseip.com<br><br>Kathleen Fitterling (Reg. No 62,950)<br>kathleen.fitterling@eriseip.com<br><br>Christopher Schmidt (Reg. No. 63,982)<br>chris.schmidt@eriseip.com<br><br><u>Postal and Hand-Delivery Address:</u><br>ERISE IP, P.A.<br>7015 College Blvd., Suite 700<br>Overland Park, Kansas 66211<br>Telephone: (913) 777-5600<br>Fax: (913) 777-5601 |

**D. 37 C.F.R. § 42.8(b)(4) – Service Information**

Please address all correspondence to the lead and back-up counsel as shown above. Petitioner consents to electronic service by e-mail at the e-mail addresses provided above.

**CLAIM LISTING APPENDIX**  
**U.S. Patent No. 11,722,554 for Claims 1-5, 7-16, 18-21**

| <b>Claim Designation</b> | <b>Claim Language</b>                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim 1[P]               | A method for determining abnormal configuration of network objects deployed in a cloud computing environment, comprising:                                                                                                                       |
| Claim 1[a]               | collecting network object data on a plurality of network objects deployed in the cloud computing environment;                                                                                                                                   |
| Claim 1[b]               | constructing a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;                                           |
| Claim 1[c]               | determining relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects; |
| Claim 1[d]               | analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and                                   |
| Claim 1[e]               | tagging network objects in the network graph for which the insight is generated.                                                                                                                                                                |
| Claim 2                  | The method of claim 1, wherein the cloud computing environment includes a plurality of different cloud computing platforms.                                                                                                                     |
| Claim 3[P]               | The method of claim 2, wherein collecting network object data further comprises:                                                                                                                                                                |
| Claim 3[a]               | connecting through an application programming interface (API) each of the plurality of different cloud computing platforms to collect network object data of network objects deployed in the respective cloud computing platform.               |
| Claim 4[P]               | The method of claim 1, wherein generating insights to include at least the list of abnormal connections further comprises:                                                                                                                      |

| Claim Designation | Claim Language                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim 4[a]        | detecting any one of: a rare network configuration, a novel network configuration, a rare network event, a novel network event, a connection of a new device to a network, an unauthorized connection, a re-connection of a user device to a subnet which the user is not permitted to access, a connection demonstrating anomalous behavior or misconfiguration, and a connection demonstrating spikes of network activity. |
| Claim 5[P]        | The method of claim 4, further comprising:                                                                                                                                                                                                                                                                                                                                                                                   |
| Claim 5[a]        | determining impermissible relationships between the network objects.                                                                                                                                                                                                                                                                                                                                                         |
| Claim 7[P]        | The method of claim 1, wherein determining the relationships between the identified network objects in further comprises:                                                                                                                                                                                                                                                                                                    |
| Claim 7[a]        | determining the relationships using at least one of: observational methods, and active logging methods.                                                                                                                                                                                                                                                                                                                      |
| Claim 8[P]        | The method of claim 1, further comprising:                                                                                                                                                                                                                                                                                                                                                                                   |
| Claim 8[a]        | adding visual representations of the determined relationships to the visual representations of the network graph.                                                                                                                                                                                                                                                                                                            |
| Claim 9           | The method of claim 1, wherein each of the plurality of network objects includes any one of: a virtual network, a firewall, a network interface card, a proxy, a gateway, a software container, container, a management object, a virtual machine, a subnet, a hub, a virtual private network (VPN).                                                                                                                         |
| Claim 10          | The method of claim 1, wherein a generated insight of the generated insights is generated utilizing natural language representation.                                                                                                                                                                                                                                                                                         |
| Claim 11[P]       | A non-transitory computer readable medium having stored thereon instructions for causing a processing circuitry to execute a process for determining abnormal configuration of network objects deployed in a cloud computing environment, the process comprising:                                                                                                                                                            |
| Claim 11[a]       | collecting network object data on a plurality of network objects deployed in the cloud computing environment;                                                                                                                                                                                                                                                                                                                |
| Claim 11[b]       | constructing a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;                                                                                                                                                                                                                        |

| Claim Designation | Claim Language                                                                                                                                                                                                                                  |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim 11[c]       | determining relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects; |
| Claim 11[d]       | analyzing the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and                                   |
| Claim 11[e]       | tagging network objects in the network graph for which the insight is generated.                                                                                                                                                                |
| Claim 12[P]       | A system for determining abnormal configuration of network objects deployed in a cloud computing environment, comprising:                                                                                                                       |
| Claim 12[a]       | a processing circuitry; and                                                                                                                                                                                                                     |
| Claim 12[b]       | a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to:                                                                                                                          |
| Claim 12[c]       | collect network object data on a plurality of network objects deployed in the cloud computing environment;                                                                                                                                      |
| Claim 12[d]       | construct a network graph based on the collected network object data, wherein the network graph includes a visual representation of network objects identified in the cloud computing environment;                                              |
| Claim 12[e]       | determine relationships between the identified network objects in the network graph, wherein the determined relationships between the identified network objects includes descriptions of connections between the identified network objects;   |
| Claim 12[f]       | analyze the network graph and the determined relationships to generate insights, wherein the generated insights include at least a list of abnormal connections between the identified network objects; and                                     |
| Claim 12[g]       | tagging network objects in the network graph for which the insight is generated.                                                                                                                                                                |
| Claim 13          | The system of claim 12, wherein the cloud computing environment includes a plurality of different cloud computing platforms.                                                                                                                    |

| <b>Claim Designation</b> | <b>Claim Language</b>                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim 14[P]              | The system of claim 13, wherein the system is further configured to:                                                                                                                                                                                                                                                                                                                                                      |
| Claim 14[a]              | connect through an application programming interface (API) each of the plurality of different cloud computing platforms to collect network object data of network objects deployed in the respective cloud computing platform.                                                                                                                                                                                            |
| Claim 15[P]              | The system of claim 12, wherein the system is further configured to:                                                                                                                                                                                                                                                                                                                                                      |
| Claim 15[a]              | detect any one of: a rare network configuration, a novel network configuration, a rare network event, a novel network event, a connection of a new device to a network, an unauthorized connection, a re-connection of a user device to a subnet which the user is not permitted to access, a connection demonstrating anomalous behavior or misconfiguration, and a connection demonstrating spikes of network activity. |
| Claim 16[P]              | The system of claim 12, wherein the system is further configured to:                                                                                                                                                                                                                                                                                                                                                      |
| Claim 16[a]              | determine impermissible relationships between the network objects.                                                                                                                                                                                                                                                                                                                                                        |
| Claim 18[P]              | The system of claim 12, wherein the system is further configured to:                                                                                                                                                                                                                                                                                                                                                      |
| Claim 18[a]              | determine the relationships using at least one of: observational methods, and active logging methods.                                                                                                                                                                                                                                                                                                                     |
| Claim 19[P]              | The system of claim 12, wherein the system is further configured to:                                                                                                                                                                                                                                                                                                                                                      |
| Claim 19[a]              | adding visual representations of the determined relationships to the visual representations of the network graph.                                                                                                                                                                                                                                                                                                         |
| Claim 20                 | The system of claim 12, wherein each of the plurality of network objects includes any one of: a virtual network, a firewall, a network interface card, a proxy, a gateway, a software container, container, a management object, a virtual machine, a subnet, a hub, a virtual private network (VPN).                                                                                                                     |
| Claim 21                 | The system of claim 12, wherein a generated insight of the generated insights is generated utilizing natural language representation.                                                                                                                                                                                                                                                                                     |

## APPENDIX OF EXHIBITS

|                     |                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Exhibit 1001</b> | U.S. Patent No. 11,722,554                                                                                                                                                                                   |
| <b>Exhibit 1002</b> | File History of U.S. Patent No. 11,722,554—Application No. 17/819,442                                                                                                                                        |
| <b>Exhibit 1003</b> | Declaration of William Easttom, Ph.D., CV attached as appendix                                                                                                                                               |
| <b>Exhibit 1004</b> | U.S. Patent No. 11,770,381 to Shivamoggi et al. (“Shivamoggi”)                                                                                                                                               |
| <b>Exhibit 1005</b> | U.S. Patent No. 10,693,743 to Zhong et al. (“Zhong”)                                                                                                                                                         |
| <b>Exhibit 1006</b> | U.S. Patent Application Publication No. 2020/0382560 to Woolward et al. (“Woolward”)                                                                                                                         |
| <b>Exhibit 1007</b> | U.S. Patent Publication No. U.S. 2020/089518 to Beyer et al. (“Beyer”)                                                                                                                                       |
| <b>Exhibit 1008</b> | U.S. Patent No. US 8,650,299 to Huang et al. (“Huang”)                                                                                                                                                       |
| <b>Exhibit 1009</b> | U.S. Patent No. U.S. 11,146,581 to Lotem et al. (“Lotem”)                                                                                                                                                    |
| <b>Exhibit 1010</b> | U.S. Patent Application Publication No. 2017/0006119 to Pogrebinsky et al. (“Pogrebinsky”)                                                                                                                   |
| <b>Exhibit 1011</b> | Zimba, A., Chama, V., “Cyber Attacks in Cloud Computing: Modelling Multi-stage Attacks using Probability Density Curves.” <i>I. J. Computer Network and Information Security</i> , 2018, 3, 25-36. (“Zimba”) |
| <b>Exhibit 1012</b> | Merriam-Webster’s Collegiate Dictionary Tenth Edition (1998).                                                                                                                                                |
| <b>Exhibit 1013</b> | Peterson, L.L., Davie, B.S. “Computer Networks: A Systems Approach.” Fifth Edition. (2012) pp. 1-69. (“Computer Networks - A Systems Approach”)                                                              |
| <b>Exhibit 1014</b> | Easley, D., L.L., Davie, B.S. “Networks, Crowds, and Markets: Reasoning about a Highly Connected World.” (2010) Chapter 2. (“Easley”)                                                                        |
| <b>Exhibit 1015</b> | <a href="https://www.armadalabs.com/blog/amazon-aws-vs-microsoft-azure-a-zero-sum-game">https://www.armadalabs.com/blog/amazon-aws-vs-microsoft-azure-a-zero-sum-game</a> (“Armada Labs”)                    |

**CERTIFICATION OF WORD COUNT**

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 10,272 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: June 4, 2025

ERISE IP, P.A.

BY: /s/ Robin A. Snader  
Robin A. Snader, Reg. No. 66,085  
robin.snader@eriseip.com  
7015 College Blvd., Suite 700  
Overland Park, KS 66211  
P: (913) 777-5600  
F: (913) 777-5601

*COUNSEL FOR PETITIONER*

**CERTIFICATE OF SERVICE ON PATENT OWNER  
UNDER 37 C.F.R. § 42.105**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on March 21, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '554 Patent:

**M&B IP Analysts, LLC**  
150 Morristown Road  
Suite 205  
Bernardsville, NJ 07924-2626

Further, a courtesy copy of this Petition for *Inter Partes* Review was sent via email to Patent Owner's litigation counsel:

Frederick L. Cottrell, III (cottrell@rlf.com)  
Kelly E. Farnan (farnan@rlf.com)  
Christine Dealy Haynes (haynes@rlf.com)  
Alex Miller (alex.miller@wsgr.com)  
Callie Davidson (ccdavidson@wsgr.com)  
Jordan R. Jaffe (jjaffe@wsgr.com)  
Lisa D. Zang (lzang@wsgr.com)  
Praatika Prasad (pprasad@wsgr.com)

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Robin A. Snader  
Robin A. Snader, Reg. No. 66,085  
robin.snader@eriseip.com

7015 College Blvd., Suite 700  
Overland Park, KS 66211  
P: (913) 777-5600  
F: (913) 777-5601

*COUNSEL FOR PETITIONERS*