

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ORCA SECURITY LTD.,
Petitioner,

v.

WIZ, INC.,
Patent Owner.

IPR2025-01085
Patent 11,936,693 B2

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

EASTHOM, *Administrative Patent Judge*.

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

I. INTRODUCTION

Orca Security, Ltd., Petitioner, filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–21 (the “challenged claims”) of U.S. Patent No. 11,936,693 B2 (Ex. 1001, the “’693 patent”). Pet. 1. Wiz, Inc., Patent Owner, filed a Preliminary Response. Paper 9 (“Prelim. Resp.”).¹

Institution of an *inter partes* review requires that the information presented in a petition and preliminary response shows that “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a).

For the reasons explained below, we determine that Petitioner establishes a reasonable likelihood that it would prevail with respect to at least one challenged claim. Accordingly, we institute an *inter partes* review as to the challenged claims and the grounds raised in the Petition.

II. BACKGROUND

A. *Real Parties in Interest*

Each party identifies itself as the real party in interest. Pet. 68; Paper 3, 2. Paper 3, 1.

B. *Related Matters*

The parties identify the following pending litigation involving the ’693 patent: *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23CV-00758 (D. Del.) (stayed). Pet. 68; Paper 3, 1.

¹ The parties also filed briefing directed to discretionary denial issues pursuant to the Board’s bi-furcated *inter partes* review process, and the Director referred the institution decision to the Board. See Papers 7, 8, 10.

C. *The '693 Patent*

The '693 patent generally relates to cybersecurity in cloud computing environments. Ex. 1001, code (57). The '693 patent describes “[e]xternal attack surface management (EASM),” which “aim[s] to discover where an organization is vulnerable, in order for a network administrator to secure the discovered vulnerabilities.” *Id.* at 1:26–27, 53–45. The '693 patent describes an “efficient way” of using EASM through “active inspection.” *Id.* at 5:40–55. The “[a]ctive inspection” “generate[s] instructions” “over a network path” to a “reachable resource caus[ing] the reachable resource to send a response.” *Id.* at 5:40–44. “For example, the instruction may be to send a data packet to an IP address of the resource, and receive an acknowledgement (ACK) response.” *Id.* at 8:4–7. “In an embodiment a network path is determined to be viable (or accessible), if the access instruction, when executed does not return an error message.” *Id.* at 10:56–58. The access “instruction may be a ping, GET, CONNECT, or TRACE request over HTTP.” *Id.* at 10:3–5.

“In an embodiment, if the network path results in successfully reaching the resource, the network path is determined to be accessible (or viable). If the resource is not reachable by the network path, the network path is determined to be inaccessible (or unviable).” Ex. 1001, 11:10–14. After determining a network path is valid via active inspection, the system applies a policy and checks for compliance with the policy. *See id.* at 22:27–50.

D. Illustrative Claim

Independent claim 1 is illustrative of the challenged claims, and follows:

[1(P)] A method for applying a policy on a network path, comprising:

[1(a)] selecting a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment;

[1(b)] actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;

[1(c)] storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network;

[1(d)] applying a policy on the valid path, wherein the policy includes a conditional rule;

[1(e)] initiating a mitigation action, in response to determining that the conditional rule is not met; and

[1(f)] applying the policy on another network path, in response to determining that the conditional rule is met.

See Pet. 13–47 (alterations in original).

E. Asserted Grounds of Unpatentability

Petitioner contends that the challenged claims are unpatentable as follows:²

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–7, 9–18, 20–21	103	Calvo, ³ Nguyen ⁴
8, 19	103	Calvo, Nguyen, Datsenko ⁵

Pet. 8. Petitioner supports its Petition with the Declaration of Chuck Easttom Ph.D, D.Sc. Ex. 1003.

III. ANALYSIS OF PETITIONER’S CHALLENGES

A. The Obviousness Standard

Section 103(a) forbids issuance of a patent when “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.”

KSR Int’l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007).⁶ The obviousness question involves resolving underlying factual determinations including (1)

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. §§ 102, 103 effective March 16, 2013, prior to the ’693 patent’s effective filing date. *See* Ex. 1001, codes (22) (63). Therefore, the AIA versions of these sections apply.

³ Calvo et al., U.S. Pat. No. 10,949,406 B1, issued Mar. 16, 2021. Ex. 1004.

⁴ Nguyen, U.S. Pat. No. 11,558,414 B1, issued Jan.17, 2023. Ex. 1005.

⁵ Datsenko et al., U.S. Pub. No. 2012/0311696 A1, published Dec. 6, 2012. Ex. 1006.

⁶ Section 103(a) is materially the same as the AIA version of Section 103 for purposes of this trial.

the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and when presented (not here), (4) objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art (POSITA) at the time of the '693 Patent would have had a bachelor's degree in computer engineering, computer science, electrical engineering, or a similar degree, with at least two years of experience in the field of cybersecurity; additional education or experience might substitute for these requirements. Pet. 7 (citing Ex. 1003 ¶¶ 63–64). Patent Owner does not provide a level of ordinary skill in the art. *See generally* Prelim. Resp.

Based on a review of the record, we adopt Petitioner's proposed level of ordinary skill in the art because it is consistent with the evidence of record, including the asserted prior art and '693 patent specification.

C. Claim Construction

In *inter partes* reviews, the Board interprets claim language using the district-court-type standard, as described in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b) (2024). Under this standard, claim terms have their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the invention, in light of the language of the claims, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1313–14.

The parties agree no explicit claim construction is necessary for purposes of deciding whether to institute. Pet. 8; Prelim. Resp. 3. However,

as set forth below in the analysis of whether Petitioner satisfies the burden of showing obviousness for institution purposes, Patent Owner presents arguments that ultimately turn on claim construction.

Petitioner notes that the parties proffered claim constructions of several terms in preparation for the district court trial in Delaware (stayed prior to a *Markman* hearing) (“District Court litigation”). See Pet. 8–9 (citing Ex. 1046 (District Court litigation: Amended Joint Claim Construction Chart)); *supra* § II.B (Related Matters).

I. “network path”

Limitation 1(a) recites “selecting a reachable resource having a network path to access the reachable resource.”

Petitioner contends that “a POSITA would have understood ‘a network path to be merely a connection of two or more resource nodes in a computing network, including in or partially in a cloud network’ or in other words ‘a node-by-node specification of a link between two machines.’” Pet. 17 (citing Ex. 1003 ¶¶ 39–43; Exs. 1026–1028).

To support its claim construction, Petitioner notes that “the ’693 [p]atent explains that ‘[a] network path is a connection of two or more security objects.’” Pet. 16 (quoting Ex. 1001, 12:46–47; citing Ex. 1001 13:57–59 (“For exemplary purposes, a network path may be a path from a virtual machine (VM), connected to a NIC, connected to a load balancer, connected to a firewall.”)). The full sentence states that “[a] network path is a connection of two or more security objects accessible from an external or internal network, and/or an external or internal object.” Ex. 1001, 12:46–47.

Petitioner also relies on Figure 2 of the ’693 patent, which follows (Pet. 16):

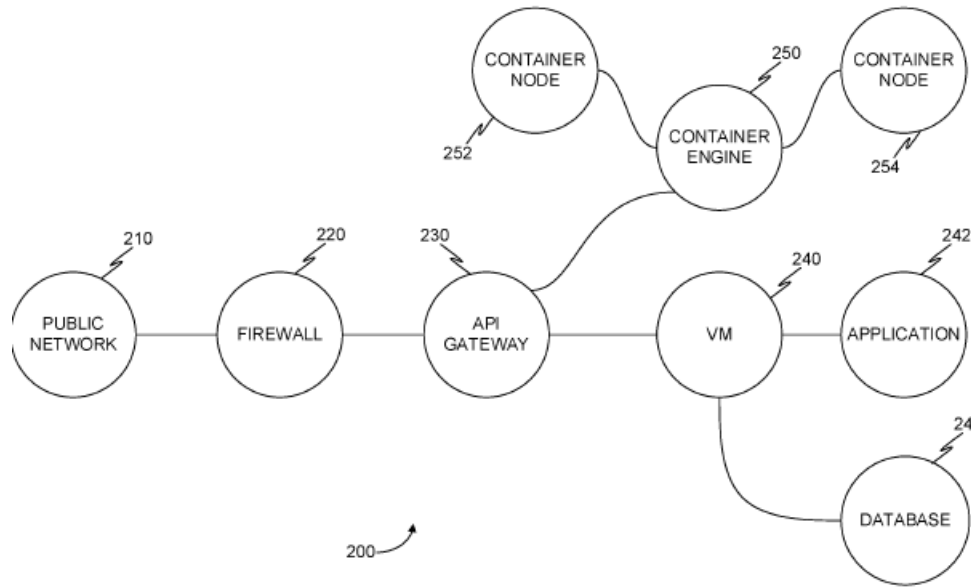


FIG. 2

Figure 2 illustrates a number of nodes, shown as labeled circles, connected by edges, shown as lines. The '693 patent states that “FIG. 2 is an example of a security graph 200 illustrating a network path . . . [which] includes a plurality of nodes, each node connected to at least another node by an edge.” Ex. 1001, 8:30–39. Petitioner also notes that “[t]he firewall, API gateway, container engine, and VM nodes seen in Figure 2 each depict a ‘resource’ per the ’693 [p]atent.” Pet. 16 . (citing Ex. 1001, 6:41–44 (“Resources may include, for example, virtual machines (VMs) such as VMs 113, container engines such as container engines 115, serverless functions such as serverless functions 117, and the like.”), 8:57–59 (“[F]irewall node 220 may be implemented, for example, as a virtual machine in the first cloud computing environment.”), 8:63–67 (“API gateway node 230 represents an API gateway.”)).

Patent Owner argues that “a network path is a connection (or series of connections) between *two or more* security objects.” See Prelim. Resp. 12–13. This construction is materially similar to Petitioner’s construction.

The '693 patent specification and the plain language of claim 1 support a construction that is similar to Petitioner's construction of a "network path" as "a link between two machines." *See* Pet. 17. That is, limitation 1(a) recites "selecting a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object . . . having access to an external network which is external to the cloud computing environment," and limitation 1(b) recites "actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network." This plain language shows that a network path is simply a connection (link) between an external network object and a resource in a cloud (or cloud object). The specification provides an example of accessing "port 22": "Active inspection allows to [sic] generate instructions directed at the reachable resource over a network path, which when received by the reachable resource cause the reachable resource to send a response." Ex. 1001, 5:40–45.

The specification also states that "a network path may include sequential representations of possible data/control flows between two or more objects in a graph." Ex. 1001, 12:49–52; *accord* Ex. 1001, 12:60–62 (describing "a path show[ing] a connection between security objects and/or computing objects that communicate over a network"), 12:42–44 ("A network path is a connection of two or more security objects accessible from an external or internal network, and/or an external or internal object."). In other words, the specification indicates that a transmitting testing object may be an object external to the cloud connected via a network path to another object (a cloud resource for testing).

The “network path” may also include resources/objects (represented as graph vertices) on the path. *See id.* at 12:51–59 (“A path may be a vertex-only path, describing a sequence of vertex-to-vertex ‘hops,’ an edge-only path, describing only the edges included in the sequence without description of the associated vertices, *or a combined edge-vertex path, describing both edges and vertexes included in the sequence.*” (emphasis added)).

Accordingly, for purposes of institution, we construe a “network path” as “a connection between an external object and a cloud resource, wherein the connection itself include objects and/or cloud resources.”

2. “valid path”

Limitation 1(c) recites “storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network.”

Petitioner shows that in the District Court litigation, the parties proposed the following constructions for “valid path” as recited in limitation 1(c): a “network path through which a resource is really reachable” (under Petitioner’s construction), and a “network path through which a resource is reachable” (under Patent Owner’s construction). Pet. 9 (quoting Ex. 1046 (District Court Amended Joint Claim Construction Chart), 13–14).

The ’693 patent specification supports both parties and indicates there is no material difference between the two constructions. That is, the ’693 patent states that “it is advantageous to determine if a network path is a valid network path, i.e., a network path through which a resource is really reachable, as opposed to an invalid network path, which seems reachable, but in practice cannot be used to access the resource.” Ex. 1001, 20:44–48; *accord* Ex. 1003 ¶ 89 (quoting Ex. 1001, 20:44–48). In addition, the

language of claim 1 supports the construction because it indicates that a “valid path” is one wherein “the reachable resource is accessible from the external network.”

We adopt both constructions and interpret them as materially the same. Accordingly, for purposes of institution, we construe a “valid path” as a “network path through which a resource is reachable or really reachable.”

3. *“actively inspecting the network path”*

Limitation 1(b) recites “actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network.”

In the District Court litigation, Petitioner proposed construing “actively inspecting the network path” as “sending a data packet over the network path.” Ex. 1046, 13 (citing Ex. 1001, 1:52–58, 5:40–051, 5:64–6:5, 7:48–64, 7:65– 8:2, 8:2–13, 9:24–26, 9:32–40, 9:62–10:58, 10:64–11:14, 11:6–14, 11:16–22, 11:31–37, 11:45–56, 12:3–8, 19:56–20:22, 20:44–56, 21:30–40, 21:49–61, 22:1–16, 22:17–26, 22:27–28, Figs. 3, 7, 8, 9); Pet. 9 (quoting Ex. 1046, 13). Patent Owner proposed that the term requires no construction. Ex. 1046, 8. Patent Owner also proposed construing a similar term, “initiating active inspection” (as recited in claim 2, which depends from claim 1) as “‘gathering information regarding the network path’ not limited to sending a data packet.” Ex. 1046, 13–14 (citing Ex. 1001, code (57), 1:21–23, 2:44–62, 2:63–3:23, 4:65–67, 5:3–5, 5:40–51, 6:36–8:29, 9:24–12:23, 15:54–18:36, 20:34–22:57, Figs. 1, 3, 6, 7); Pet. 9 (quoting Ex. 1046, 13).

Neither party offers another construction for the related terms here. *See generally* Prelim. Resp.; Pet. The ’693 patent specification supports the

broader construction as proposed by Patent Owner—i.e., not limiting the term to embodiments that involve “sending a data packet.” *See* Ex. 1001, code (57) (generally describing active inspection without mention of packets), 2:44–62 (same), 2:63–3:23 (same), 4:65–67 (same); 5:3–5 (same); 8:2–4 (“[T]he active inspector 125 may generate an instruction based on the network path to access the resource associated with the network path. *For example, the instruction may be to send a data packet to an IP address of the resource, and receive an acknowledgement (ACK) response.*” (emphases added)).

Accordingly, for purposes of institution, we construe “actively inspecting the network path” as “gathering information regarding the network path not limited to sending a data packet.”

4. *Remaining Terms*

No express construction of any other claim term is necessary to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. *Ground 1, Alleged Obviousness of Claims 1–3, 13, and 14 over Calvo and Nguyen.*

Petitioner contends that claims 1–7, 9–18, 20, and 21 would have been obvious over the combined teachings of Calvo, Stroud, and Nguyen. Pet. 13–53.

1. *Calvo*

Calvo relates to “compliance lifecycle management for cloud-based resources.” Ex. 1004, code (57). In Calvo, a “compliance package (also referred to as a compliance pack, policy compliance pack, conformance pack, or governance pack) may include settings, rules, artifacts (e.g., documentation of compliance standards), and remedial actions to be taken if resources are found to be noncompliant.” *Id.* at 2:46–51. “Remedial actions for noncompliance may include notifying relevant users, modifying a configuration of a resource, isolating a resource, and so on.” *Id.* at 2:62–64.

“Using the compliance management system described herein, users may easily select and deploy compliance packs to cloud-based resources to determine the policy compliance of those resources.” Ex. 1004, 2:64–3:1. Calvo provides data describing the evaluation of compliance of one or more resources. *Id.* code (57).

2. *Nguyen*

Nguyen describes a method of “obtaining threat model data associating at least one actor with an application,” wherein an actor is capable of “taking advantage of at least one potential vulnerability associated with the application.” Ex. 1005, code (57). Nguyen’s system employs “penetration testing,” known as “[p]en[-]testing,” “a systematic and safe cybersecurity technique that leverages tools, techniques, procedures, and processes in an attempt to compromise a system.” *Id.* at 1:5–11.⁷ “[P]en[-]testing is used to identify actual vulnerabilities that may lead to inappropriate use, if taken advantage of by an actor.” *Id.* at 2:40–42.

⁷ Nguyen refers to “pentesting” whereas Petitioner refers to “pen-testing.” We employ Petitioner’s spelling.

3. *Analysis of Claim 1*

a) *Preamble and Limitation 1(a)*

For independent claim 1’s preamble, “[a] method for applying a policy on a network path, comprising,” Petitioner relies on “Calvo’s method of applying compliance pack(s) to . . . prevent access from the public Internet through port 22 to internal cloud-based resource(s)).” Pet. 13–14.

For limitation 1(a), “selecting a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment,” Petitioner relies on Calvo’s method of selecting “cloud-based resource(s) accessible from the public Internet outside Calvo’s provider network.” *See* Pet. 14.

Regarding the selectable resource, Petitioner relies on Calvo’s disclosure of “[v]arious embodiments of methods, systems, and computer-readable media for compliance lifecycle management for cloud-based resources” and selecting target resources for deployment of the selected compliance pack. Pet. 14 (quoting Ex. 1004, 2:7–10, 4:6–7) (citing Ex. 1004, Fig. 2B, S210, Fig. 1A, 4:2–9 (“[S]elect the . . . target resources to which the compliance pack should be applied . . .”), 4:17–20 (“The client may also use a resource selection component 130 to select a set of target resources 185 from the resources 180 of the provider network 190.”), 4:22–25 (stating “resource selection 130 may automatically select such resources”)).

Patent Owner does not address Petitioner’s showing for the preamble or limitation 1(a). *See generally* Prelim. Resp.

On this preliminary record, Petitioner’s showing for the preamble and limitation 1(a), as summarized above, is sufficient for purposes of institution.

b) Limitation 1(b)

For limitation 1(b), “actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network,” Petitioner relies on the combined teachings of Calvo and Nguyen. Pet. 21–32. Petitioner contends that Calvo teaches selecting a reachable recourse as limitation 1(a) requires, but “Calvo does not expressly provide details for *active[] inspecti[on]* as described in the ’693 [p]atent (i.e., Claim 1(b)).” *Id.* at 22. According to Petitioner, “Calvo discloses its compliance packs may be used for PCI DSS compliance.” *Id.* (citing Ex. 1004, 2:5–24); *accord id.* at 28 (“Calvo discloses its compliance packs may be used for ‘compliance requirements’ such as those in ‘the Payment Card Industry Data Security Standard (PCI DDS) [] for companies that process credit card data.’” (quoting Ex. 1004, 2:7–24)).

According further to Petitioner, “a POSITA would have known that ‘[o]ne of the **requirements** in the PCI DDS is performance of network-layer **penetration testing**.’” Pet. 28–29 (citing Ex. 1003 ¶ 99; Ex. 1039, 1:20–33 (“Under Section 11.3.4.1 of the PCI DDS, this penetration testing must be conducted at least annually”). Petitioner also contends that Nguyen teaches “active[] inspection” because

Nguyen’s exemplary access parameter “UDP [protocol] transmits packets” ([Ex. 1005], 13:14–16, 13:22–25, 13:25–27, 19:25) and additionally because a POSITA would have understood that sending instructions (as disclosed by Nguyen) over/to/through a network would have been accomplished by sending data in the form of packets. Ex. 1003, ¶ 97 (citing Ex.

1045, . . . Title, [¶ 1]). Nguyen’s disclosures also teach “gathering information regarding the network” because Nguyen sends instructions over a network and receives responses back to determine which targets/potential vulnerabilities represent actual vulnerabilities in the target internal network. [Ex. 1005] . . . , 4:46–50, 10:52–11:6, 12:29–13:44, 16:1–4.

Id. at 27.

Petitioner further asserts that “Nguyen’s test plan instructions use the same exemplary ‘instructions’ and ‘access parameters’ as the ’693 [p]atent that would be ‘necessary for a potential actor to take advantage of a potential vulnerability and potentially cause harm.’” *Id.* at 25–26 (quoting Ex. 1005, 11:1–4). As an example, Petitioner notes that just like the ’693 patent, which employs instructions such as HTTP GET to access IP addresses, ports, etc., Nguyen’s pen-testing “communicate[s] via IP addresses, ports, and/or UDP/HTTP protocols using instructions such as GET, TRACE, and/or CONNECT.” *Id.* at 23–24 (citing Ex. 1001, 9:64–10:6), 26 (citing Ex. 1005, 13:14–16, 22–27, 45–47).

Based on this evidence, Petitioner argues that “a POSITA would have been motivated to incorporate Nguyen’s autonomous pen-testing process into Calvo’s method/system to comply with PCI DDS requirements.” *Id.* at 29. Petitioner summarizes that “it was well-known in the art that **PCI DDS compliance required pen-testing**,” and “Nguyen’s pen-testing disclosures represent one example rendering obvious *active[] inspecti[on]* as claimed.” *Id.* at 22 (citing Ex. 1003 ¶¶ 55–61; Exs. 1039–1044).

Dr. Easttom supports Petitioner and testifies that “Nguyen teaches determining which ‘targets’ represent ‘actual vulnerabilities’ by performing pen-testing,” and “Nguyen’s process includes sending instructions and receiving responses to identify actual threats from external surfaces in the

same manner as the '693 [p]atent.” Ex. 1003 ¶ 91 (citing Ex. 1005, 4:46–50, 10:52–11:6, 12:29–13:44, 16:1–4; Ex. 1001, 5:40–44, 8:2–7, 9:62–63).

Petitioner further contends that “the present Calvo-Nguyen combination . . . teach[es] inspecting *the network path* because the chain of resource nodes in Calvo teach a *network path* (*supra* Claim 1(a)) and pen-testing (for example as disclosed by Nguyen) was known to inspect such *network paths* by traversing resource nodes.” Pet. 28 (citing Ex. 1003, ¶ 51; Ex. 1007, code (51), code (57), 8:64–9:9).

Patent Owner responds that Petitioner performs “gap-filling[, which] is a sign of improper hindsight, using the claims as a template.” Prelim. Resp. 5–6 (citing *KSR*, 550 U.S. at 421 (“A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.”)). Patent Owner explains that “[P]etitioner’s theory is not that either Calvo or Nguyen discloses *actively inspecting the network path* as claimed, but rather that this would have been obvious in their combination due to general knowledge of a POSITA, with citation to expert testimony and an exhibit that is not a grounds reference.” *Id.* at 5. Patent Owner faults Petitioner’s argument that “pen-testing (for example as disclosed by Nguyen) was known to inspect such *network paths* by traversing resource nodes.” *Id.* at 6 (citing Pet. 28; Ex. 1003 ¶ 51; Ex. 1007). Patent Owner contends that “the [cited] paragraph [of Dr. Easttom’s declaration] reads: ‘And penetration testing of internal networks on “paths” was known to be accomplished by traversing resource nodes.’” *Id.* (quoting Ex. 1003 ¶ 51). However, Patent Owner contends that just because “the testing might take place ‘on “paths”’ does not mean that constitutes inspecting the network path.” *Id.* Patent Owner also faults Dr. Easttom’s

reliance on Exhibit 1007 because it is “not a grounds reference and Petitioner’s expert makes no effort to establish that its disclosures universally apply to all penetration testing or to Nguyen specifically.” *Id.* (citing Ex. 1003 ¶ 51; Ex. 1007, code (54), code (57), 8:64–9:9).

Patent Owner’s arguments are unavailing. Patent Owner does not explain why testing on a path is patentably distinct from inspecting the network path. Reaching or not reaching a network cloud resource via pen-testing as Petitioner shows necessarily involves inspecting connectivity of the network path from the pen-tester to the resource. Patent Owner also does not address or undermine Petitioner’s sufficient showing for institution purposes that Nguyen and the ’693 patent employ materially similar or the same methods of actively inspecting a network path, using *inter alia*, HTTP GET instructions, as summarized above.

Therefore, on this preliminary record, Petitioner sufficiently shows that “actively inspecting the network path” as limitation 1(b) requires (and as preliminarily construed herein) reads on Nguyen’s pen-testing procedure. *See supra* § II.C.3 (construing the term to mean “gathering information regarding the network path not limited to sending a data packet”). Patent Owner’s arguments do not address or undermine Petitioner’s related reliance on Nguyen’s general “teach[ing of] ‘gathering information regarding the network,’” wherein “Nguyen sends instructions over a network and receives responses back to determine which targets/potential vulnerabilities represent

actual vulnerabilities in the target internal network.” Pet. 27 (citing Ex. 1005, 4:46–50, 10:52–11:6, 12:29–13:44, 16:1–4).⁸

Patent Owner’s observation that Exhibit 1007 is “not a grounds reference” does not explain why Petitioner’s reliance thereon undermines Petitioner’s showing. *See* Prelim. Resp. 6. Exhibit 1007 describes, *inter alia*, “perform[ing] dynamic best path determination for penetration testing,” showing background knowledge of an artisan of ordinary skill with respect to pen-testing. *See* Ex. 1007, code (57). As outlined above, Petitioner relies on other evidence describing pen-testing as information gathering and as involving packets for active inspection, including Nguyen, which is “a grounds reference.”

Petitioner also sufficiently shows on this preliminary record that an artisan of ordinary skill would have considered evidence regarding known forms of pen-testing in interpreting Calvo’s PCI DDS disclosures. That is, as summarized above, Petitioner sufficiently shows that “a POSITA would have known that ‘[o]ne of the **requirements** in the PCI DDS is performance of network-layer **penetration testing**.’” Pet. 28–29 (citing Ex. 1003 ¶ 99; Ex. 1039, 1:20–33 (“Under Section 11.3.4.1 of the PCI DDS, this penetration testing must be conducted at least annually”)); *accord* Ex. 1003 ¶¶ 56–57 (testifying it was well-known that PCI DSS required penetration testing (citing Ex. 1039, 1:25–42; Exs. 1041–1043)).

⁸ As noted above, in the District Court litigation, Patent Owner proposed construing a similar term, “initiating active inspection,” as “‘gathering information regarding the network path’ not limited to sending a data packet.” Pet. 8 (quoting Ex. 1046, 13–14).

On this preliminary record, Petitioner’s showing for limitation 1(b), as summarized above and in light of Patent Owner’s arguments otherwise, is sufficient for purposes of institution.

c) Limitation 1(c)

(1) Petitioner’s Contentions

For limitation 1(c), “storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network,” Petitioner relies on the combined teachings of Calvo and Nguyen. Pet. 32–35. As discussed in the previous section, Petitioner contends that Calvo does not expressly disclose active inspection. Pet. 33. Petitioner also contends that Calvo does not disclose storing an indicator in response to such active inspection. *Id.* However, Petitioner asserts that “Nguyen’s pen-testing process does” disclose active inspection and storing an indicator (wherein such active inspection determines if the reachable resource is accessible from an external network according to limitation 1(b)). *Id.* (referring to its showing for limitation 1(b)). Petitioner explains that Nguyen teaches what the ’693 patent describes, namely, “if a resource is successfully accessed . . . this result can be stored.” *Id.* (quoting Ex. 1001, 11:40–44).

That is, Petitioner contends that similar to the ’693 patent, Nguyen’s pen-testing stores the results of active inspection, “which includes results indicating which targets (potential vulnerabilities) have been determined to be actual vulnerabilities based on instructions sent and responses received.” Pet. 33. As an example of storing test results, Petitioner asserts that “Nguyen teaches ‘vulnerabilities database 380 [] stores results obtained from performing tests on targets’ . . . and ‘[t]he test results 390 may identify one

or more actual vulnerability.” *Id.* (quoting Ex. 1005, 11:16–17, 16:12–13 (alterations except ellipses and emphasis in original)). Petitioner provides other citations to Nguyen to show storing of test results. *Id.* (citing Ex. 1005, 11:65–67 (“The test data source 330 may receive results 390 obtained in response to the executed tests from the execution module 140 and may store these results.”), 12:2–5 (“The execution module 140 and/or the test data source 330 may transmit the results 390 obtained in response to the executed tests to the vulnerabilities database 380 for storage thereby.”), 13:1–5 (“**The vulnerabilities database 380 may store the testing steps performed to take advantage of a potential vulnerability, the impact of the testing steps, and the severity of the potential vulnerability when the potential vulnerability is determined to be an actual vulnerability.**” (emphasis in original)), 13:52–54 (“The test engine saves the results in the test data source 330 (see FIG. 3) and/or the vulnerabilities database 380 (see FIG. 3).”).

Petitioner also contends that the above disclosures teach a “valid path” as claimed and as construed by the parties in the District Court litigation (and as adopted here). *See* Pet. 8–9, 34; *supra* § III.C (i.e., construing a “valid path” as a “network path through which a resource is . . . reachable”). That is, Petitioner contends Nguyen teaches a valid path, namely a “network path through which a resource is really reachable” because “Nguyen’s pen-testing process determines which resources are actual vulnerabilities and rules out ‘false positives or potential vulnerabilities that are not actual vulnerabilities’ (i.e., resources that are not really reachable).” *Id.* at 34 (second quote quoting Ex. 1005, 10:58–60) (citing Ex. 1005, 11:16–17, 13:1–5, 16:12–13).

Petitioner further contends that based on these teachings, it would have been obvious “to incorporate the aspect of Nguyen’s pen-testing process that stores test results (indicating which potential vulnerabilities are actual vulnerabilities), so that the system could maintain a list of actual vulnerabilities for continuous policy application, compliance verification, and potential remediation, in addition to meeting PCI DSS requirements.” Pet. 35 (citing Ex. 1003 ¶¶ 111–113). Petitioner also contends that not storing pen-testing results including “false positives” that the system rules out as vulnerabilities would defeat the purpose of pen-testing—to identify actual vulnerabilities—because not storing the result would require redundant pen-testing to re-categorize the same resource. *See id.* (citing Ex. 1003 ¶¶ 114).

(2) Patent Owner’s First Arguments

Patent Owner responds that “Nguyen discloses neither storing an indicator that a path is valid nor doing so in response to determining that the reachable resource is accessible from the external network.” Prelim. Resp. 7. According to Patent Owner, “Nguyen discloses storing indicators regarding specific resource or ‘target’ vulnerabilities, not ‘valid path’ indicators.” *Id.* at 8. Patent Owner argues that Petitioner “tries to stretch the disclosure to meet the claim language by contending that Nguyen ‘rules out ‘false positives or potential vulnerabilities that are not actual vulnerabilities’” (i.e., resources that are not really reachable).” *Id.* According further to Patent Owner, “Petitioner gives no explanation of why a ‘false positive’ indicates a ‘not really reachable’ resource, nor does Petitioner explain why ruling out false positives would indicate a *valid path*.” *Id.* Patent Owner also contends that Nguyen provides insufficient

reasoning as to why Nguyen would store active inspection results “beyond a conclusory ‘common sense’ rationale.” *Id.* at 9. Patent Owner also argues that “Petitioner points to Nguyen’s disclosure of storing test results but provides no explanation as to how Nguyen might teach doing so in response to a specific determination of accessibility from the external network.” *Id.* at 10.

Patent Owner’s arguments are unavailing. Patent Owner agrees that “Nguyen discloses storing indicators regarding specific resource or ‘target’ vulnerabilities,” and merely denies that this is not storing “‘valid path’ indicators.” *See* Prelim. Resp. On this preliminary record, Petitioner sufficiently shows that storing indicators in response to determining vulnerabilities is not patentably distinct from storing indicators in response to determining a valid path exists. Determining a vulnerability is determining that it is an externally accessible reachable resource under Petitioner’s showing, which in turn verifies a valid path under the plain language of claim 1 and per the parties’ District Court claim construction adopted here (i.e., a “valid path” is a “network path through which a resource is . . . reachable”). *See supra* § III.C.2.

As summarized above, Petitioner sufficiently shows on this preliminary record that it would have been obvious “to incorporate the aspect of Nguyen’s pen-testing process that stores test results (indicating which potential vulnerabilities are actual vulnerabilities), so that the system could maintain a list of actual vulnerabilities for continuous policy application, compliance verification, and potential remediation, in addition to meeting PCI DSS requirements.” Pet. 35 (citing Ex. 1003 ¶¶ 111–113).

In addition, Petitioner sufficiently and generally explains that a false positive indicates the resource is not an “actual vulnerabilit[y]” so that it would have been obvious to store indications of actual vulnerabilities and indications of non-vulnerabilities to efficiently foster the goals of PCI DSS, including “continuous policy application, compliance verification, and potential remediation,” as opposed to, for example, re-testing the same resource. *See id.* (“If the results were not stored, such ‘false positives’ would not remain ruled out after being identified.”).

As Petitioner also sufficiently explains,

such a combination would have constituted the use of a known technique (Nguyen’s pen-testing to determine which resources correspond to actual vulnerabilities) to improve a similar device (Calvo’s device which selects resources for policy deployment) in the same way (Calvo’s process/system would be improved in the same way as Nguyen’s because false positive vulnerabilities would be eliminated from further cybersecurity processing).

Pet. 32 (citing Ex. 1003 ¶ 103).

(3) Patent Owner’s Second Argument

Patent Owner argues that “Nguyen teaches storage of test results *regardless* of the testing outcome or contents of those results.” Prelim. Resp. 11. Based on this premise, Patent Owner contends that Petitioner insufficiently shows that Nguyen teaches “storage of results *in response to determining . . . that the reachable resource is accessible.*” *Id.*

These arguments are unavailing. Even if Nguyen stores results regardless of the testing outcome, Petitioner sufficiently shows that Nguyen teaches “storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network” as outlined above.

In other words, claim 1 does not preclude storing different types of pen-testing results in response to those results. As preliminarily determined above, Petitioner sufficiently shows that Calvo-Nguyen’s combined system stores the results of pen-testing, which indicates if the path is valid. The ’693 patent states that its system “determine[s] which network paths, reachability paths, application paths, and the like, *are valid paths, for example by performing active inspection of the same.*” Ex. 1001, 20:54–56 (emphasis added).

As also preliminarily found above, Nguyen teaches “actively inspecting” as limitation 1(b) requires. That is, as Petitioner similarly points out as noted above, Nguyen teaches what the ’693 patent describes, namely, “if a resource is successfully accessed . . . this result can be stored.” Pet. 33 (quoting Ex. 1001, 11:40–44). In addition to Petitioner’s showing with respect to limitation 1(b) as summarized above, Petitioner sufficiently shows that the combined Calvo-Nguyen system includes using Nguyen’s pen-testing to send instructions and receive responses to identify “targets” or “actual vulnerabilities” (Ex. 1005, 5:15–21) “the bad guys see” (*id.* at 5:27–29) and “identifies the potential targets . . . that are public[ly] accessible (e.g., via a network, such as the Internet” (*id.* at 5:15–21) where “targets include an IP address, an interface component[,], an [API] endpoint, a [URI] endpoint, and the like” (*id.* at 2:6–9 (alterations in original). *See* Pet. 24–25 (quoting Ex. 1005 as noted), 26 (showing Nguyen communicates using standard UDP/HTTP protocols using instructions such as GET, TRACE, and/or CONNECT (citing Ex. 1005, 13:22–25)), 31–32 (citing Ex. 1003 ¶ 102)). As Petitioner also shows, as explained above, Nguyen’s instructions perform “active[] inspection” as recited in limitation 1(b) in the same

manner as the '693 patent, where for example, both systems use HTTP protocol GET instructions. Pet. 23–24, 26 (citing Ex. 1001, 9:61–10:6, Ex. 1004, 13:7–32, 45–47).

(4) Patent Owner's Third Argument

Patent Owner alleges that one of Nguyen's examples designates an application as a false positive even though "a test engine repeatedly enters text on a web page (through a valid path)." Prelim. Resp. 8 (citing Ex. 1005, 13:33–44). According to Patent Owner, this example undermines Petitioner's reasoning that Nguyen's false positives rule out a valid path. *Id.* However, Patent Owner's characterization omits the full description of the relied-upon example. In particular, Nguyen states that "[i]f the web application 102A reacts appropriately (e.g., the back end system or business logic filters the character strings) the potential vulnerability is determined to be a false positive." Ex. 1005, 13:38–41 (emphasis added).

In that example, Nguyen implies that the application does not allow execution of unfiltered text strings, but if it does, it is not a false positive and is accessible as a vulnerability because it does not "react[] appropriately." *See* Ex. 1005, 13:33–41. This is consistent with the '693 patent, which states that "[i]n an embodiment, a resource is accessible if, for example, it can be sent instructions which are then executed by the resource." *See* Pet. 24 (quoting Ex. 1005, 20:3–6).

(5) Summary of Limitation 1(c)

On this preliminary record, Petitioner's showing for limitation 1(c), as summarized above and in light of Patent Owner's arguments otherwise, is sufficient for purposes of institution.

d) Limitation 1(d)

(1) Petitioner's Contentions

For limitation 1(d), “applying a policy on the valid path, wherein the policy includes a conditional rule,” Petitioner relies on the combined teachings of Calvo and Nguyen. Pet. 36–39. Petitioner applies “Calvo’s compliance pack to prevent access from the public Internet to internal cloud-based resource(s) through firewall port 22, where such has been stored as an actual vulnerability via Nguyen’s pen-testing process[], *wherein the policy includes a conditional rule* (e.g., Calvo’s rules in Calvo’s compliance pack), as claimed.” *Id.* at 36. According to Petitioner, the ’693 patent describes applying a policy by applying a conditional rule. *Id.* (citing Ex. 1001, 8:22–29 (“In some embodiments, a policy includes a statement, a conditional rule, a combination thereof, and the like.”), 21:62–67 (“In some embodiments, applying a policy on a network path includes applying a conditional rule.”)).

Petitioner also contends that the “’693 [p]atent provides the following exemplary scenario for ‘a policy [] applied on a valid network path’”: “[A] policy includes a statement that a network path to/from a first reachable resource should only be accessible via a predefined port (e.g., port 80) using a predefined protocol (e.g., HTTPS).” Pet. 36–37 (quoting Ex. 1001, 21:56 (alteration in original)) (citing Ex. 1001, Fig. 9, S930). “In some embodiments, where a viable network path is detected, the policy is applied to determine if the network path adheres to the policy or not.” *Id.* (quoting Ex. 1001, 22:2–8).

Based on this and other evidence, Petitioner reads limitation 1(d)’s “wherein the policy includes a conditional rule” onto Calvo’s “compliance packs.” Pet. 36–37. Petitioner relies on Calvo’s disclosure that “[a]

compliance pack 171A may include a plurality of rules 172A that can be evaluated to determine the policy compliance of a resource.” *Id.* (quoting Ex. 1004, 5:60–62). Petitioner also relies on Calvo’s teaching that “its compliance packs may include ‘remedial actions to be taken if resources are found to be noncompliant.’” *Id.* (quoting Ex. 1004, 2:49–51).

Petitioner explains that a “POSITA would have understood that rule evaluation and compliance determination of a rule would be the result of a condition being present or absent.” Pet. 37 (citing Ex. 1003 ¶ 118). Petitioner relies on Calvo’s “exemplary scenario: ‘a rule in an InfoSec compliance pack may be used to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the relevant rule.’” *Id.* (quoting Ex. 1004, 6:35–39). According to Petitioner for this exemplary scenario, the conditional rule is “port 22 . . . is not accessible to the Internet.” *Id.* (quoting Ex. 1004, 6:36–37) (alteration added). Calvo supports Petitioner, stating that “the port may be closed if it is found to be noncompliant with the relevant rule,” and in general, “[u]sing a single compliance pack, such rules may be applied to disparate resources throughout an enterprise in a consistent manner.” Ex. 1001, 6:38–41.

With respect to limitation 1(d)’s “applying a policy on the valid path,” Petitioner relies on Nguyen’s teaching of modifying Calvo’s compliance packs using Nguyen’s pen-testing to detect and store an indication of a valid network path in order to comply with Calvo’s PCI DSS requirements as discussed in connection with limitations 1(b) and 1(c) above (*see* Pet. 21–35), and then Petitioner turns to Calvo’s compliance pack teachings:

Calvo’s disclosures of applying/deploying its compliance pack to selected cloud-based resources teach *applying a policy*

on the [] path because such resources are part of a *network path* from the public Internet to the selected cloud-based resources, and Calvo’s exemplary rule (which is applied for subsequent compliance determination) is to prevent access from the public Internet to the selected target cloud-based resource(s) through port 22 on Calvo’s firewall. [Ex. 1004], 6:35–39 (“For example, a rule in an InfoSec compliance pack may be used to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the relevant rule.”), 3:37–41 (“The resources 180 may be accessed from inside or outside the provider networks (e.g., via one or more public networks such as the Internet and/or one or more private networks) by resource owners or other provider network clients, such as client 10.”), 4:35–37 (“a compliance pack may be deployed to particular regions or divisions of a provider network or other enterprise.”), 2:46–51, 2:60–62, 5:60–62. A POSITA would have understood that applying a rule on a firewall port that is meant to prevent access through such firewall from the public Internet to an internal cloud-based resource teaches policy application *on the [] path* because a POSTIA would have understood that applying compliance rules (to restrict outside network access for example) would be applied on nodes (i.e., resources) of a network because the nodes represent computing objects (which can execute instructions) while connections between nodes represent communication channels (which themselves do not execute instructions). Ex. 1003, ¶ 119.

Pet. 38–39.

(2) Patent Owner’s First Argument

Patent Owner responds that “Petitioner . . . fails to demonstrate that the combination of Calvo and Nguyen teaches” “applying a policy on a network path []or doing so on a valid network path.” Prelim. Resp. 12. Patent Owner argues that “Petitioner agrees that element 1(d) requires a policy applied to a set of two or more security objects / resource nodes, i.e. a network path.” *Id.* at 13. Based on this alleged agreement, Patent Owner

argues that Petitioner fails to show “applying a policy on a connection of *two or more* security objects.” *Id.*

These arguments are not clear. Specifically, Patent Owner appears to contradict itself by arguing that “element 1(d) requires a policy applied to *a set of two or more security objects / resource nodes*, i.e. a network path” and also that it requires “applying a policy on *a connection* of two or more security objects.” *See* Prelim. Resp. 13 (emphasis added and omitted). As construed above, and as Patent Owner otherwise agrees, a “network path” is not “a set of two or more security objects / resource nodes,” but it may include two or more security objects/resource nodes. *See supra* § III.C.1.

Therefore, contrary to Patent Owner’s characterization, on this preliminary record, Petitioner does not agree that limitation 1(d) requires, applying a policy to “a set of two or more security objects / resource nodes.” Rather, limitation 1(d) recites “applying a policy *on* the valid path.” It follows that limitation 1(d) does not preclude applying “a policy [to a resource] on the valid path.” *See supra* §§ III.C.1 (construing a “network path” as not precluding a resource or object on the path), III.C.2 (construing a “valid path”). The parties will have the opportunity during trial to clarify any claim construction issues.

(3) Patent Owner’s Second Argument

Patent Owner correctly notes that Petitioner applies Calvo’s compliance pack “to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the relevant rule.” Prelim. Resp. 14 (quoting Pet. 37) (citing Ex. 1004, 6:35–39). According to Patent Owner, “even if Calvo’s compliance packs are considered a policy,

Calvo only teaches applying that policy on a specific resource or group of resources, *not the path between resources.*” *Id.* (emphasis added).

This claim construction argument is unavailing. For the reasons indicated above, “applying a policy on the valid path” does not preclude applying it to a resource on the path. *See supra* §§ III.C.1 (construing a “network path” as not precluding a resource or object on the path), III.C.2 (construing a “valid path”). As also indicated above, the parties will have the opportunity during trial to clarify any claim construction issues.

(4) Patent Owner’s Third Argument

As Patent Owner acknowledges, Petitioner relies on Calvo’s application of a compliance pack on a network path because resources on the path are part of the network path from the public Internet to the selected cloud-based resources. Prelim. Resp. 16. But according to Patent Owner, Petitioner does not “explain why applying a policy on ‘part of’ a network path (i.e. a single resource) teaches applying a policy on the path as claimed.” *Id.* at 16. Patent Owner similarly faults Petitioner for applying the policy “to a resource rather than a network path as claimed” (*id.*) and contends that Petitioner “confuses two separate elements” of claim 1: “Element 1(d) requires the application of a policy on a valid network path, while element 1(e) requires the initiation of a mitigation action (which may be applied to an individual resource).” *Id.* at 18.

Again, these claim construction arguments are unavailing largely for the reasons outlined above. Specifically, limitation 1(d) recites “applying a policy on the valid path,” which does not preclude “applying a policy [to a resource] on the valid path.” *See supra* §§ III.C.1 (construing a “network path” to include a resource on the path), III.C.2 (construing a “valid path”).

It is also not clear how limitation 1(e) (addressed in the next section) impacts the analysis of limitation 1(d) or how Petitioner “confuses” the two limitations, contrary to Patent Owner’s arguments. *See* Prelim. Resp. 18. As Patent Owner notes, limitation 1(e), “initiating a mitigation action, in response to determining that the conditional rule is not met,” does not preclude “initiating a mitigation action” to a resource on a network path. *See id.* But limitation 1(e) also does not preclude “applying a policy [to a resource] on a valid path.”

(5) Patent Owner’s Fourth Argument

Patent Owner also argues that “the combination of Calvo and Nguyen” does not “teach applying a policy on a valid path,” because “the path itself has not been validated.” Prelim. Resp. 19. Patent Owner further argues that “Petitioner does not explain how Calvo teaches applying a policy on paths that have been found to be valid,” where Petitioner states that “Calvo teaches applying compliance packs to whichever resources a user selects.” *Id.*

Patent Owner’s arguments are unavailing. On this preliminary record, limitation 1(d) does not require applying a policy to paths “that have been found to be valid.” Rather, it requires “applying a policy to the valid path.” The specification supports this interpretation by stating that “a policy is applied on a valid network path” in some embodiments without determining that it is a valid path prior to the policy application. *See* Ex. 1001, 21:56–61 (“At S930, a policy is applied on a valid network path. In some embodiments, an active inspector is configured to determine that a network path is a valid network path. In certain embodiments, in response to determining that a network path is a valid network path, the active inspector

is further configured to apply a policy to the network path.” (emphases added)). In contrast, limitation 1(d) does not recite “*in response to determining that a network path is a valid network path, applying a policy on the valid path.*”

The specification describes other embodiments that “apply such a policy . . . *only on a network path which is a valid network path* in order to reduce a number of alerts which are generated by cybersecurity system” because unreachable paths do “not currently pose a security threat.” *See id.* at 12:61–62 (emphasis added). In contrast, limitation 1(d) does not recite “applying a policy *only* on a valid path.” As noted, the parties will have the opportunity to clarify any claim construction issues during trial.

Even if claim 1 does require determining the path is valid prior to applying a policy (to a resource) on it, as noted above, a valid path is a “network path through which a resource is reachable” according to the parties’ District Court claim construction positions and as adopted here. *See supra* § III.C.2. As summarized above, Petitioner relies on the combined Calvo-Nguyen system, including Nguyen’s pen-testing system, to determine, by receiving information from a reachable network resource prior to applying Calvo’s compliance pack policy, “if the network path of the reachable resource is accessible from the external network” and thereby is a “valid path.” *See supra* § III.D.3.b–c (addressing limitations 1(b), 1(c)).

Moreover, on the preliminary record, determining that a resource is externally reachable on a path via Nguyen’s pen-testing procedure is a determination that it is valid according to the ’693 patent: “In an embodiment, *if the network path results in successfully reaching the resource, the network path is determined to be accessible (or viable).*” If the

resource is not reachable by the network path, the network path is determined to be inaccessible (or unviable).” Ex. 1001, 11:10–14 (emphasis added). By way of summary, under the theory advanced by Petitioner and similar to the ’693 patent’s disclosure, the Calvo-Nguyen system uses pen-testing to determine if a path is valid and then applies policies to valid path (reachable) resources. The combined system does not (and cannot) apply policies to invalid path (unreachable) resources.

(6) *Summary of Limitation 1(d)*

On this preliminary record, Petitioner’s showing for limitation 1(d), as summarized above and in light of Patent Owner’s arguments otherwise, is sufficient for purposes of institution.

e) *Limitations 1(e) and 1(f)*

Limitations 1(e) and 1(f) recite “initiating a mitigation action, in response to determining that the conditional rule is not met,” and “applying the policy on another network path, in response to determining that the conditional rule is met,” respectively. For these limitations, Petitioner relies on its annotated version of Calvo’s Figure 2b, as follows (Pet. 43):

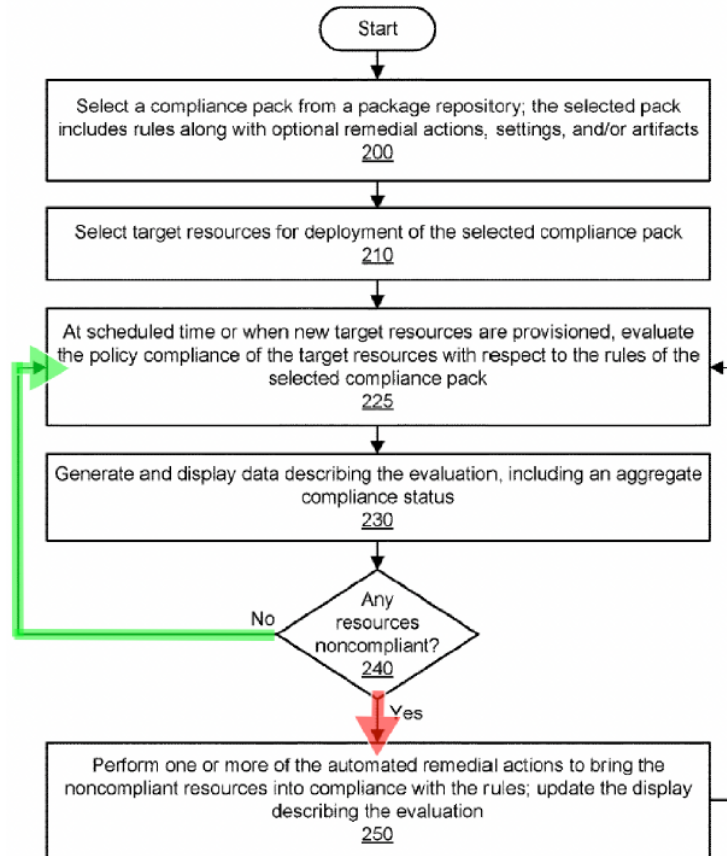


FIG. 2B

Calvo's Figure 2B above is a flow diagram illustrating Calvo's process of applying compliance packs to cloud resources. Petitioner annotates Figure 2B with red (Yes) and green (No) arrows at decision box 240 to indicate how limitations 1(e) and 1(f) read on Calvo's process, respectively. *See* Pet. 39–47.

For limitation 1(e), Petitioner contends that Calvo discloses deploying compliance packs that contain conditional rules as set forth in the discussion of limitation 1(d) above. Pet. 40. Petitioner further contends that as “Calvo's Figure 2B at steps 240–250,” illustrates, “Calvo discloses that if a resource is noncompliant (i.e., a rule in the compliance pack is not met), then remedial actions are taken” at step 250. *See id.* at 40–41 (referring to the red

arrow of Figure 2B pointing to step 250 from decision box 240). Petitioner adds that “in Calvo’s exemplary scenario discussed above, the *mitigation action* is **closing port 22.**” *Id.* at 42 (citing Ex. 1004, 6:35–39 (“For example, a rule in an InfoSec compliance pack may be used to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the relevant rule.”))).

For limitation 1(f), still relying on Calvo’s Figure 2B above, Petitioner contends that “Calvo’s continuous compliance verification process . . . applies the compliance pack on a subsequent resource, via a subsequent path, in response to compliance being confirmed for a previous resource/path, where each resource represents a separate network node with a separate network path), as claimed.” Pet. 42. Petitioner notes that Calvo teaches that “[i]n various embodiments, the rule evaluation 150 may be performed . . . when a new resource is provisioned in the target resources.” *Id.* at 46 (quoting Ex. 1001, 5:5–9).

Other than as discussed in the previous section, Patent Owner does not address Petitioner’s showing for limitation 1(e). Based on the record and summary above, Petitioner’s showing for limitation 1(e) is sufficient for institution purposes. *See* Pet. 39–42.

With respect to limitation 1(f), Patent Owner responds that “Calvo does not teach that a subsequent application of the policy on another network path is *in response to determining that the conditional rule is met.*” Prelim. Resp. 20. In support of this argument, Patent Owner maintains that in Calvo’s system, “all resources are evaluated, regardless of the compliance of any other resource.” *Id.* at 22. Patent Owner adds that “[e]ven . . . where

the flowchart reaches step 240 and follows the ‘no’ path back to step 225, no subsequent application of the policy is triggered based on this determination” because “[i]nstead, Calvo teaches that the application of the policy on another resource is based on a ‘scheduled time’ or ‘when new target resources are provisioned.’” *Id.* at 22 (quoting Ex. 1004, Fig. 2B, step 225).

This line of argument is unavailing. As Patent Owner recognizes by the latter argument, Petitioner’s shows that at step 225, after Calvo’s system at step 240 determines that *current* resources are compliant (i.e., follows the “No” path back to step 225), Calvo’s system evaluates “new target resources” for “policy compliance” when “provisioned.” *See* Ex. 1004, Fig. 2B, S225; Pet. 46 (noting that Calvo teaches that “[i]n various embodiments, the rule evaluation 150 may be performed . . . when a new resource is provisioned in the target resources” (quoting Ex. 1004, 5:5–9)). Therefore, Calvo’s system “appl[ies] the policy on another network path, in response to determining that the conditional rule is met,” as limitation 1(f) requires, even though it applies the policy to newly provisioned resources “on another network path.”⁹

On this preliminary record, Petitioner’s showing for limitations 1(e) and 1(f), as summarized above and in light of Patent Owner’s arguments otherwise, is sufficient for purposes of institution.

⁹ Calvo also teaches applying the policy to all new resources even if not “provisioned.” Ex. 1004, 11:9–12 (“Continuous compliance may include compliance verification of existing resources as well as preventative compliance verification of new resources, e.g., before the new resources are provisioned.”).

f) Summary for Claim 1

Based on our analysis set forth above and the current record, we determine that the information presented in the Petition, in light of the Preliminary Response, demonstrates a reasonable likelihood that Petitioner will prevail in establishing that claim 1 is unpatentable under 35 U.S.C. § 103 over the combination of Calvo and Nguyen.

4. Analysis of Claims 2–7, 9–18, 20, and 21

Independent claims 11 and 12 are similar to independent claim 1. Claims 2–7, 9, and 10 depend directly or indirectly from claim 1. Claims 13–18, 20, and 21 depend directly or indirectly from claim 12.

Petitioner contends that claims 2–7, 9–18, 20, and 21 would have been obvious over the combined teachings of Calvo and Nguyen. *See* Pet. 48–63. Petitioner sufficiently maps the prior art combination to the limitations of these claims and presents contentions and evidence concerning why an ordinarily skilled artisan would have combined Calvo and Nguyen with a reasonable expectation of success. *Id.* Patent Owner does not address Petitioner’s showing. *See generally* Prelim. Resp.

Accordingly, we determine on this record that the information presented in the Petition, in light of the Preliminary Response, demonstrates a reasonable likelihood that Petitioner will prevail in establishing that claim 2–7, 9–18, 20, and 21 are unpatentable under 35 U.S.C. § 103 over the combination of Calvo and Nguyen.

E. Ground 2, Alleged Obviousness of Claims 8 and 19 over Calvo, Nguyen, and Datsenko

Petitioner contends that claims 8 and 19 would have been obvious over the combined teachings of Calvo, Nguyen, and Datsenko. Pet. 63–67.

Petitioner sufficiently maps the prior art to the limitations of these claims and presents contentions and evidence concerning why an ordinarily skilled artisan would have combined Calvo, Nguyen, and Datsenko with a reasonable expectation of success. *Id.* Patent Owner does not address Petitioner’s showing for these claims separately. *See* Prelim. Resp. 13 (relying on arguments presented for claim 1).

Accordingly, we determine on this record that the information presented in the Petition, in light of the Preliminary Response, demonstrates a reasonable likelihood that Petitioner will prevail in establishing that claims 8 and 19 are unpatentable under 35 U.S.C. § 103 over the combination of Calvo, Nguyen, and Datsenko.

IV. CONCLUSION

After considering the evidence and arguments presented in the Petition and the Preliminary Response, we determine that Petitioner demonstrates a reasonable likelihood of prevailing on its assertion that at least one claim of the ’693 patent is unpatentable. Accordingly, we institute an *inter partes* review of the challenged claims on all of the grounds presented in the Petition. *See* 37 C.F.R. § 42.108(a); *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018); *AC Techs. S.A. v. Amazon.com, Inc.*, 912 F.3d 1358, 1364 (Fed. Cir. 2019) (“[I]f the Board institutes an IPR, it must . . . address all grounds of unpatentability raised by the petitioner.”). At this stage of the proceeding, we have not made a final determination as to the patentability of these challenged claims.

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that pursuant to 35 U.S.C. § 314, *inter partes* review is instituted as to claims 1–21 of the '693 patent with respect to all grounds of unpatentability presented in the Petition; and

FURTHER ORDERED that *inter partes* review is commenced on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

IPR2025-01085
Patent 11,936,693 B2

FOR PETITIONER:

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

FOR PATENT OWNER:

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