

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. IPR2025-01085
U.S. Patent No. 11,936,693

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,936,693**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	THE '693 PATENT.....	1
A.	THE '693 PATENT	1
B.	PROSECUTION HISTORY	5
C.	LEVEL OF SKILL OF A PERSON HAVING ORDINARY SKILL IN THE ART.....	7
III.	REQUIREMENTS UNDER 37 C.F.R. § 42.104	7
A.	GROUND FOR STANDING UNDER 37 C.F.R. § 42.104(A).....	7
B.	IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B)	8
C.	CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3).....	8
IV.	SHOWING OF ANALOGOUS, PRIOR ART	9
A.	CALVO	10
B.	NGUYEN.....	11
C.	DATSENKO	11
V.	OVERVIEW OF GROUNDS.....	12
VI.	GROUND 1: CLAIMS 1-7, 9-18, AND 20-21 ARE OBVIOUS OVER CALVO AND NGUYEN.....	13
A.	CLAIM 1	13
1.	<i>[1(P)] 1. A method for applying a policy on a network path, comprising:.....</i>	<i>13</i>
2.	<i>[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;</i>	<i>14</i>
3.	<i>[1(b)] actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;</i>	<i>21</i>
4.	<i>[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;</i>	<i>32</i>

5.	<i>[1(d)] applying a policy on the valid path, wherein the policy includes a conditional rule;</i>	<i>36</i>
6.	<i>[1(e)] initiating a mitigation action, in response to determining that the conditional rule is not met; and</i>	<i>39</i>
7.	<i>[1(f)] applying the policy on another network path, in response to determining that the conditional rule is met.</i>	<i>42</i>
B.	CLAIM 2	48
1.	2. The method of claim 1, further comprising: initiating active inspection for each network path of a plurality of network paths; and applying the policy only on a network path of the plurality of network paths which is a valid path.	48
C.	CLAIM 3	49
1.	3. The method of claim 2, further comprising: initiating active inspection by generating an access instruction for the reachable resource; and executing the access instruction on a network path.	49
D.	CLAIM 4	51
1.	4. The method of claim 2, further comprising: applying the policy only on each network path of the plurality of network paths which is a valid path.	51
E.	CLAIM 5	52
1.	5. The method of claim 4, further comprising: initiating active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.	52
F.	CLAIM 6	53
1.	6. The method of claim 1, further comprising: initiating the mitigation action on the reachable resource.	53
G.	CLAIM 7	53
1.	7. The method of claim 6, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.	53
H.	CLAIM 9	54
1.	9. The method of claim 1, further comprising: initiating active inspection of the network path to detect an application path.	54

I.	CLAIM 10	55
1.	10. The method of claim 9, further comprising: generating the mitigation action further based on the application path.	55
J.	CLAIM 11	56
1.	[11(P)] 11. A non-transitory computer-readable medium storing a set of instructions for applying a policy on a network path, the set of instructions comprising:.....	56
2.	[11(a)] one or more instructions that, when executed by one or more processors of a device, cause the device to:	57
3.	[11(b)] select 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;	58
4.	[11(c)] actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;	58
5.	[11(d)] 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;	58
6.	[11(e)] apply a policy on the valid path, wherein the policy includes a conditional rule;	58
7.	[11(f)] initiate a mitigation action, in response to determining that the conditional rule is not met; and	58
8.	[11(g)] apply the policy on another network path, in response to determining that the conditional rule is met.	58
K.	CLAIM 12	59
1.	[12(P)] 12. A system for applying a policy on a network path comprising:.....	59
2.	[12(a)] a processing circuitry; and.....	60
3.	[12(b)] a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to:	60
4.	[12(c)] select 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	

	<i>network which is external to the cloud computing environment;</i>	<i>60</i>
5.	<i>[12(d)] actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;</i>	<i>60</i>
6.	<i>[12(e)] store 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;</i>	<i>60</i>
7.	<i>[12(f)] apply a policy on the valid path, wherein the policy includes a conditional rule;</i>	<i>61</i>
8.	<i>[12(g)] initiate a mitigation action, in response to determining that the conditional rule is not met; and</i>	<i>61</i>
9.	<i>[12(h)] apply the policy on another network path, in response to determining that the conditional rule is met.</i>	<i>61</i>
L.	CLAIM 13	61
1.	<i>13. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection for each network path of a plurality of network paths; and apply the policy only on a network path of the plurality of network paths which is a valid path.</i>	<i>61</i>
M.	CLAIM 14	61
1.	<i>14. The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection by generating an access instruction for the reachable resource; and execute the access instruction on a network path.</i>	<i>61</i>
N.	CLAIM 15	62
1.	<i>15. The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: apply the policy only on each network path of the plurality of network paths which is a valid path.</i>	<i>62</i>
O.	CLAIM 16	62
1.	<i>16. The system of claim 15, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to:</i>	

	<i>initiate active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.</i>	<i>62</i>
P.	CLAIM 17	62
1.	<i>17. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate the mitigation action on the reachable resource.....</i>	<i>62</i>
Q.	CLAIM 18	62
1.	<i>18. The system of claim 17, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.....</i>	<i>62</i>
R.	CLAIM 20	63
1.	<i>20. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection of the network path to detect an application path.</i>	<i>63</i>
S.	CLAIM 21	63
1.	<i>21. The system of claim 20, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate the mitigation action further based on the application path.</i>	<i>63</i>
VII.	GROUND 2: CLAIMS 8 AND 19 ARE OBVIOUS OVER CALVO, NGUYEN, AND DATSENKO	63
A.	CLAIM 8	63
1.	<i>8. The method of claim 1, further comprising: generating an exception to the policy based on a valid network path.</i>	<i>63</i>
B.	CLAIM 19	67
1.	<i>19. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate an exception to the policy based on a valid network path.</i>	<i>67</i>
VIII.	CONCLUSION.....	67

IX.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)	68
A.	REAL PARTY-IN-INTEREST	68
B.	RELATED MATTERS	68
C.	LEAD AND BACK-UP COUNSEL	68
D.	37 C.F.R. § 42.8(B)(4) – SERVICE INFORMATION	69

TABLE OF AUTHORITIES

Cases:

<i>Elekta Ltd v. ZAP Surgical Sys., Inc.</i> , 81 F.4th 1368 (Fed. Cir. 2023).....	32
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	9

Statutes:

35 U.S.C. §§ 102(a)(1)	10, 11
35 U.S.C. §§ 102(a)(2)	10, 11
35 U.S.C. § 103	8

Regulations:

37 C.F.R. § 42.6(e)	79
37 C.F.R. §42.8.....	78
37 C.F.R. § 42.8(a)(1)	68
37 C.F.R. § 42.8(b)(1)	68
37 C.F.R. § 42.8(b)(3)	68
37 C.F.R. § 42.8(b)(4)	68, 69
37 C.F.R. §42.24.....	78
37 C.F.R. § 42.104.....	7
37 C.F.R. § 42.104(a)	7
37 C.F.R. § 42.104(b).....	8
37 C.F.R. § 42.104(b)(3)	8
37 C.F.R. § 42.105.....	79
37 C.F.R. § 42.105(B)	79

I. INTRODUCTION

Petitioner Orca Security Ltd. (“Petitioner”) requests *Inter Partes* Review of Claims 1-21 (the “Challenged Claims”) of U.S. Patent No. 11,936,693 (the “’693 Patent”) assigned to Wiz, Inc. (“Patent Owner”).

The ’693 Patent claims a broad, cybersecurity process that was well-known before 2022—protecting a cloud network from external attacks by applying policy rules. The ’693 Patent’s closest, alleged point of novelty is “storing an indicator” to ensure that a potential way into the cloud network represents a legitimate threat. As explained in this Petition, the prior art renders the Challenged Claims obvious.

II. THE ’693 PATENT

A. The ’693 Patent

The ’693 Patent is generally directed to cybersecurity and discloses cloud-computing environments. ’693 Patent, Title, Abstract, 1:20-32, 1:43-45, 5:37-51, Claims 1-21. An exemplary cloud-computing environment with access to a public network is provided by Figure 1:

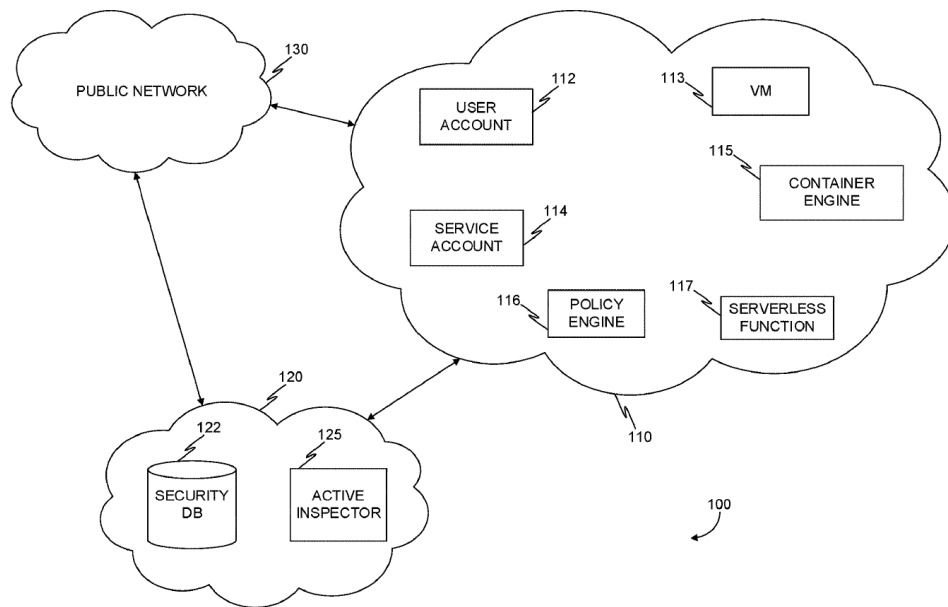


FIG. 1

'693 Patent, Fig. 1.

Regarding resource inspection, the '693 Patent describes “[e]xternal attack surface management (EASM)[,] ... [which] describe[s] what vulnerabilities an organization has within their network infrastructure[.]” ’693 Patent, 1:27-32. The ’693 Patent purports to disclose an “efficient way” of EASM through a process the ’693 Patent refers to as “active inspection.” ’693 Patent, 5:40-55. Per the ’693 Patent, “active inspection” determines which theoretical vulnerabilities are “indeed vulnerable” by trying to access internal cloud resources from an external network (’693 Patent, 10:66-11:6, 20:44-48), for example by sending instructions to and receiving responses from such resources (’693 Patent, 5:40-44, 8:2-7, 9:62-63, 9:64-10:6). If the resource can be successfully accessed from an external network, the

network path to such resource is determined to be valid/viable. '693 Patent, 10:50-53, 10:56-58, 11:10-14, 20:3-6, Claim 1.

After determining a network path is valid via active inspection, the '693 Patent discloses a process of policy application followed by checking for compliance of such policy; the process of checking for compliance includes either (A) **mitigating in a case of noncompliance** or (B) **continuing with policy application in the case of compliance**.¹

¹ All emphasis has been added by Petitioner unless stated otherwise.

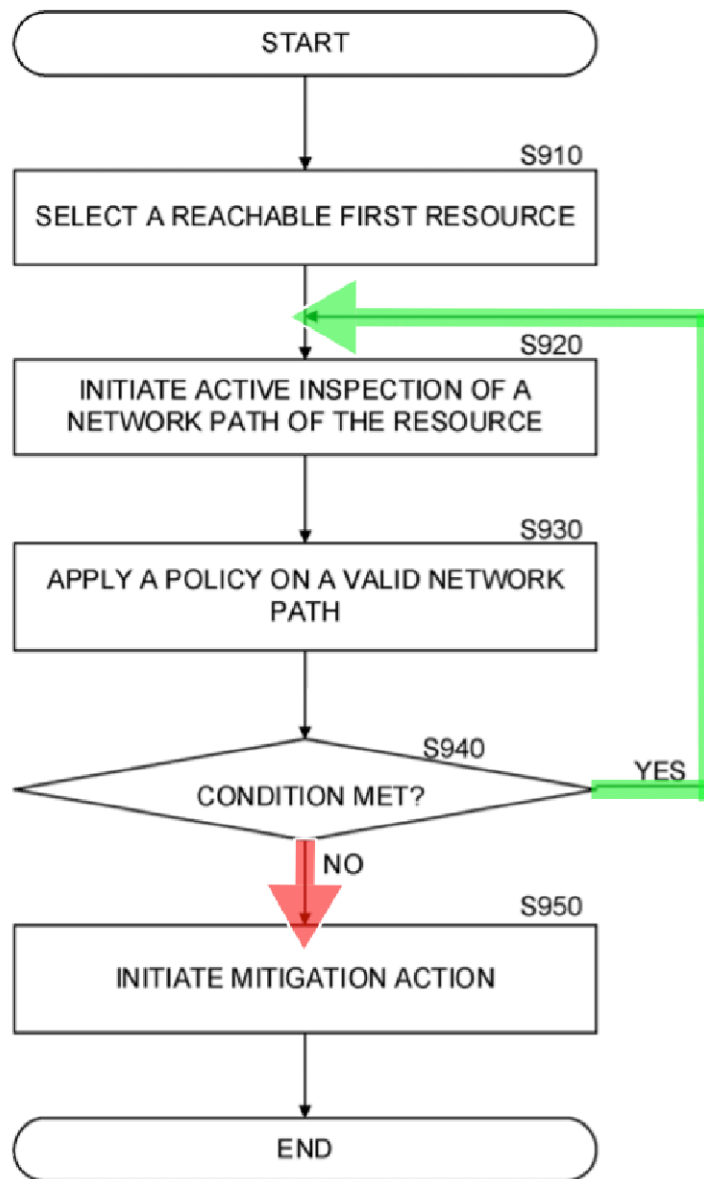


FIG. 9

'693 Patent, Fig. 9 (annotated), Claim 1, 5:21-22, 20:34-22:57.

In accordance with Figure 9, the '693 Patent provides the following exemplary scenario for “a policy [] applied on a valid network path” ('693 Patent, 21:56, Fig. 9 at S930): “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). 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.” ’693 Patent, 22:2-8, 5:43-51 (using “port 22” as an example).

B. Prosecution History

As explained in this Section, the Challenged Claims were allowed after the Examiner indicated in an interview that the “storing an indicator” limitation (limitations 1(c), 11(d), and 12(e) in the Challenged Claims, the “Storing Limitation”) would overcome the cited art and Applicant amended all independent claims to include the Storing Limitation.

In a Non-Final Office Action dated October 24, 2023, the Examiner rejected the then-pending claims as obvious over Sundararajan in view of Nickolov. Ex. 1002, 106-114. Examiner and Applicant then conducted an interview to “discuss[] the claim limitations of [then] dependent claim 2 which recite ‘storing an indicator to indicate that a first network path of the plurality of networks paths is a valid path, in response to determining that the reachable resource is accessible from the external network” (i.e., the Storing Limitation). Ex. 1002, 117.

Applicant responded to the Non-Final Office Action dated October 24, 2023 by amending the independent claims, largely to add the Storing Limitation. Ex. 1002,

122-134. Applicant noted: “During the interview, the **Examiner indicated that the limitation of [then] dependent claim 2 appears to overcome the cited art,** pending further search.” Ex. 1002, 123. Exemplary independent claim 1 after the amendment recited:

1. (Currently Amended) A method for applying a policy on a network path, comprising:

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;

actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;

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;

applying a policy on the ~~accessible network~~ valid path, wherein the policy includes a conditional rule;

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.

Ex. 1002, 124. Applicant went on to argue that Sundararajan in view of Nickolov did not disclose the Storing Limitation (because “Sundararajan does **not** teach or suggest that a network path is valid or not valid”), did not teach “selecting a reachable resource having a network path to access the reachable resource” (because the alleged resource was “external to the cloud computing environment), did not teach “initiating a mitigation action” (because “[t]here is **no** mitigation action in

Sundararajan at all”), did “not disclose active inspection of a network path” (because Nickolov instead disclosed “permission for sending a content over an external network portion”), and did not teach “applying the policy on a valid network path” (because “Nickolov teaches that confidential data should not be sent on an external network portion”). Ex. 1002, 130-133 (emphasis in original).

Applicant concluded by again noting: “In light of the above and **as mentioned by the Examiner during the interview summary**, it is believed that Claim 1 is allowable given the cited art.” Ex. 1002, 132-133. The claims were then allowed without any enumerated reasons for allowance. Ex. 1002, 149-153.

C. Level of Skill of a Person Having Ordinary Skill in the Art

A 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; Dr. Easttom is a POSITA for the ’693 Patent Ex. 1003, ¶¶ 63-64.

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

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

Petitioner certifies the ’693 Patent is available for IPR and Petitioner is not barred/estopped from requesting IPR.

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.

Grounds of Unpatentability	Exhibits
<u>Ground 1:</u> Claims 1-7, 9-18, 20-21 are obvious under 35 U.S.C. § 103 ² over Calvo and Nguyen	1004 1005
<u>Ground 2:</u> Claims 8 and 19 are obvious under 35 U.S.C. § 103 over Calvo, Nguyen, and Datsenko	1004 1005 1006

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

Petitioner notes that the parties have proffered the following constructions for two terms of the '693 Patent in the related—and stayed³— district court litigation:

Term/Phrase	Petitioner's Proposed Construction	Patent Owner's Proposed Construction
"actively inspect[ing] the network path" /	"sending a data packet over the network path"	No construction necessary.

² All references to Title 35 are to post-AIA Title 35 unless otherwise stated.

³ The district court litigation was stayed "through final written decision in each of the Wiz IPRs." Ex. 1047, Stay Order, 2. The "Wiz IPRs" refer to the instituted IPRs filed by Patent Owner against Petitioner's patents. *Id.*, 1.

“initiat[e/ing] active inspection”		“gathering information regarding the network path” not limited to sending a data packet.
“valid path”	“network path through which a resource is really reachable”	No construction necessary. Alternatively, “network path through which a resource is reachable”.

Ex. 1046, Amended Joint CC Chart, 13-14.

The district court’s *Markman* hearing “is CONTINUED” and has not been rescheduled in view of the instituted Wiz IPRs and related stay. *Orca Security Ltd. v. Wiz, Inc.*, 1:23-cv-00758-JLH-SFR, Dkt. 223, Oral Order (Dec. 17, 2024).

Because the proposed grounds below render the Challenged Claims obvious under each party’s proposed constructions and the ordinary/customary meaning (to the extent different), Petitioner does not contend that any claim construction is necessary. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (construction is required “only to the extent necessary to resolve the controversy”).

IV. SHOWING OF ANALOGOUS, PRIOR ART

The ’693 Patent was filed on July 24, 2023, and claims priority to Application Nos. 17/818,898, 17/659,163, 17/659,164, and 17/659,165 filed August 10, 2022

and April 13, 2022. Accordingly, the earliest possible priority date for the '693 Patent is **April 13, 2022**.⁴

A. Calvo

Calvo is prior art to the '693 Patent. Calvo was filed March 25, 2019 and issued as U.S. Patent No. 10,949,406 on March 16, 2021. Calvo therefore qualifies as prior art to the '693 Patent under 35 U.S.C. §§ 102(a)(1) and (2).

Calvo is analogous prior art to the '693 Patent because Calvo is in the same field of endeavor as the '693 Patent and is reasonably pertinent to a problem with which the inventors of the '693 Patent were involved. Ex. 1003, ¶¶ 20-23. Like the '693 Patent, Calvo is directed to cybersecurity.'693 Patent, Title, Abstract, 1:20-32, 5:37-39, Claims 1-21; Calvo, Title, Abstract, 1:5-22, 2:7-36. Additionally, like the '693 Patent, Calvo addresses problems related to policy application ('693 Patent, Title, Abstract, 2:44-62, 20:34-35, Fig. 9, Claims 1-21; Calvo, Title, Abstract, 1:6-22, 2:7-36) and managing networks at scale ('693 Patent, 1:59-2:17; Calvo, 1:19-22, 2:34-36). Calvo was neither cited nor discussed during the prosecution of the '693 Patent. *See generally* Ex. 1002.

⁴ For purposes of this Petition, Petitioner does not challenge the '693 Patent's priority claim.

B. Nguyen

Nguyen was filed on November 5, 2020, and issued as U.S. Patent No. 11,558,414 on January 17, 2023. Nguyen, therefore, qualifies as prior art to the '693 Patent under 35 U.S.C. § 102(a)(2).

Nguyen is analogous prior art to the '693 Patent because Nguyen is in the same field of endeavor as the '693 Patent and is reasonably pertinent to a problem with which the inventors of the '693 Patent were involved. Ex. 1003, ¶¶ 24-27. Like the '693 Patent, Nguyen is also directed to cybersecurity. '693 Patent, Title, Abstract, 1:20-32, 1:43-45, 5:40-51, Claims 1-21; Nguyen, Title, Abstract, 1:5-35. Additionally, like the '693 Patent, Nguyen addresses problems related to determining network vulnerabilities/improving scanning techniques for attempting to infiltrate a network ('693 Patent, 1:43-50, 1:53-2:17; Nguyen, Title, Abstract, 1:5-35, 1:56-2:14, 11:56-58) and reducing time/resources/labor for such ('693 Patent, 1:53-2:17; Nguyen, 1:18-25, 3:67). Nguyen was neither cited nor discussed during the prosecution of the '693 Patent. *See generally* Ex. 1002.

C. Datsenko

Datsenko was filed June 2, 2011, and published as U.S. Patent Application Publication No. 2012/0311696 on December 6, 2012. Datsenko therefore qualifies as prior art to the '693 Patent under 35 U.S.C. §§ 102(a)(1) and (2).

Datsenko is analogous prior art to the '693 Patent because Datsenko is in the same field of endeavor as the '693 Patent and is reasonably pertinent to a problem with which the inventors of the '693 Patent were involved. Ex. 1003, ¶¶ 28-31. Like the '693 Patent, Datsenko is also directed to cybersecurity.'693 Patent, Title, Abstract, 1:20-32, 5:37-39, 22:17-26, Claims 1-21; Datsenko, Title, Abstract, [0001]-[0003]. Additionally, like the '693 Patent, Datsenko addresses problems related to policy application. '693 Patent, Title, Abstract, 2:44-62, 20:34-35, 22:17-26, Fig. 9, Claims 1-21; Datsenko, Title, Abstract, [0001]-[0003], [0043]-[0044]. Datsenko was neither cited nor discussed during prosecution of the '693 Patent. *See generally* Ex. 1002.

V. OVERVIEW OF GROUNDS

Ground 1: As explained below, Calvo in view of Nguyen renders obvious each of the Challenged Claims except Claims 8 and 19. Specifically, Calvo teaches the core concepts of resource selection and policy application through Calvo's compliance pack disclosures, which include compliance with the Payment Card Industry Data Security Standard ("PCI DSS"). Calvo does not expressly discuss details for "active inspection" as described in the '693 Patent; however, Nguyen does describe such details via Nguyen's pen-testing disclosures. Pen-testing (or penetration testing) was a well-known technique used in the art to probe an internal network from outside to determine whether unwanted, outside access could be

achieved. A POSITA would have been motivated to incorporate Nguyen's pen-testing process into Calvo's method/system for all the reasons explained below; for example, **PCI DSS requires penetration testing**.

Ground 2: As also explained below, the Calvo-Nguyen combination in further view of Datsenko renders obvious Claims 8 and 19, which add a further limitation of generating an exception to the policy. Datsenko teaches such, and a POSITA would have been motivated to incorporate Datsenko's policy exception mechanism into the Calvo-Nguyen combination for all the reasons explained below; for example, users may need access to an internal network that is (otherwise properly) prohibiting such access through a working policy.

VI. GROUND 1: CLAIMS 1-7, 9-18, AND 20-21 ARE OBVIOUS OVER CALVO AND NGUYEN

A. Claim 1

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

To the extent the preamble is limiting, Calvo in view of Nguyen renders obvious *a method for applying a policy on a network path*⁵ (e.g., Calvo's method of applying compliance pack(s) to firewall port 22 to prevent access from the public

⁵ Requester denotes claim language in the mapping sections by italics.

Internet through port 22 to internal cloud-based resource(s)), as claimed. *See infra* Claims 1(a)-1(d).

2. ***[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;***

Calvo discloses, or otherwise renders obvious, *selecting a reachable resource* (e.g., Calvo's selecting one or more target cloud-based resources) *having a network path to access the reachable resource* (e.g., the network location(s) of Calvo's selected cloud-based resource(s), for example: public Internet>firewall>port 22>resource(s)), *wherein the reachable resource is a cloud object deployed in a cloud computing environment* (e.g., Calvo's cloud-based resource(s) hosted in the cloud), *having access to an external network which is external to the cloud computing environment* (e.g., Calvo's cloud-based resource(s) accessible from the public Internet outside Calvo's provider network), as claimed.

Calvo teaches *selecting a resource*. For example, Calvo generally discloses “[v]arious embodiments of methods, systems, and computer-readable media for compliance lifecycle management for cloud-based resources” (Calvo, 2:7-9) and specifically discloses “select[ing] target resources for deployment of the selected compliance pack.” Calvo, Fig. 2B, S210, Fig. 1A, 4:2-9 (“select the account(s) or 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”), 4:22-25 (“resource selection 130 may automatically select such resources”).

Regarding *a reachable resource having a network path to access the reachable resource*, the ’693 Patent explains that a resource having one or more “reachability parameters” (such as “protocols, IP addresses, ports”) which allows access from an external network (for example, through a “firewall”) teaches *a reachable resource having a network path to access the reachable resource*. ’693 Patent, 16:56-60 (“A reachable resource is a resource which includes at least a viable network path, having reachability parameters which allow access from an external network to the resource, the resource deployed in a cloud computing environment.”), 18:66-19:3, 5:66-6:2 (“Reachability properties, or parameters, may be utilized to establish a network path to the resource from an external network through the cloud computing environment.”), 7:50-53 (“a network path may be stored as a data string which includes one or more reachability parameters. Such parameters include host names, protocols, IP addresses, ports, usernames, passwords, and the like.”), 9:28-31 (“The network path, also known as object reachability, includes data (e.g., reachability parameters) for accessing the first resource from a public network”), 10:20-21 (“The IP address and ports would be reachability parameters”); 5:43-46, 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.”).

Specifically regarding *network path*, the '693 Patent explains that “[a] network path is a connection of two or more security objects[.]” '693 Patent, 12:46-47, 13:57-59. The '693 Patent’s “FIG. 2 is an example of a security graph 200 illustrating a network path ... [which] includes a plurality of nodes” (8:30-39):

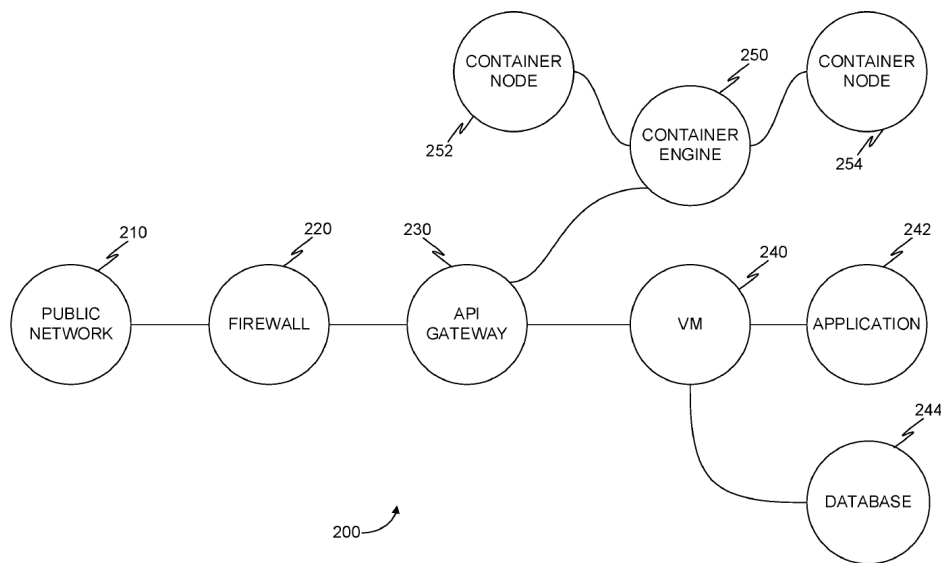


FIG. 2

'693 Patent, Fig. 2. The firewall, API gateway, container engine, and VM nodes seen in Figure 2 each depict a “resource” per the '693 Patent. '693 Patent, 6:37-40 (“A resource is a cloud entity which supplies functionality, such as processing power, memory, storage, communication, and the like.”), 6:41-44 (“Resources may include [] virtual machines (VMs) [] container engines [] serverless functions”), 8:57-59

(“firewall 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. An API gateway is a workload, for example a serverless function”).

Additionally, 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.” Ex. 1003, ¶¶ 39-43 (citing Exs. 1026-1028). A POSITA would have further understood that such “network path[s]” are identified by identifying resources via IP address/ports, for example as used in routing tables. Ex. 1003, ¶¶ 35-38 (citing Exs. 1019-1025), ¶¶ 44-46 (citing Exs. 1029-1034), ¶¶ 80-83.

Accordingly, an exemplary *network path* (in the ’693 Patent’s Figure 2) is: public network>firewall>API gateway>additional resources, where such nodes may have IP addresses or port numbers; this exemplary *network path* includes as few as two connected resource nodes.

Calvo likewise teaches *a reachable resource having a network path to access the reachable resource*. Specifically, Calvo teaches at least the following exemplary *network path to access the reachable resource*: public Internet>firewall>port 22>resource(s).

For example, Calvo provides the following example for evaluation of a rule in a deployed compliance pack for its selected target cloud-based resources: “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.” Calvo, 6:35-39. Calvo explains that this exemplary rule can be for “resources” (Calvo, 6:30-35), “resources [may be] termed ‘cloud-based’ and [] hosted in the cloud” (Calvo, 3:33-35), “[t]he resources [] may be accessed from inside or outside the provider networks (e.g., via one or more public networks such as the Internet...)” (Calvo, (3:37-41), and “a compliance package [can] be applied to one or more resources in one or more multi-tenant provider networks, including one or more regions of such networks.” (Calvo, 2:42-45).

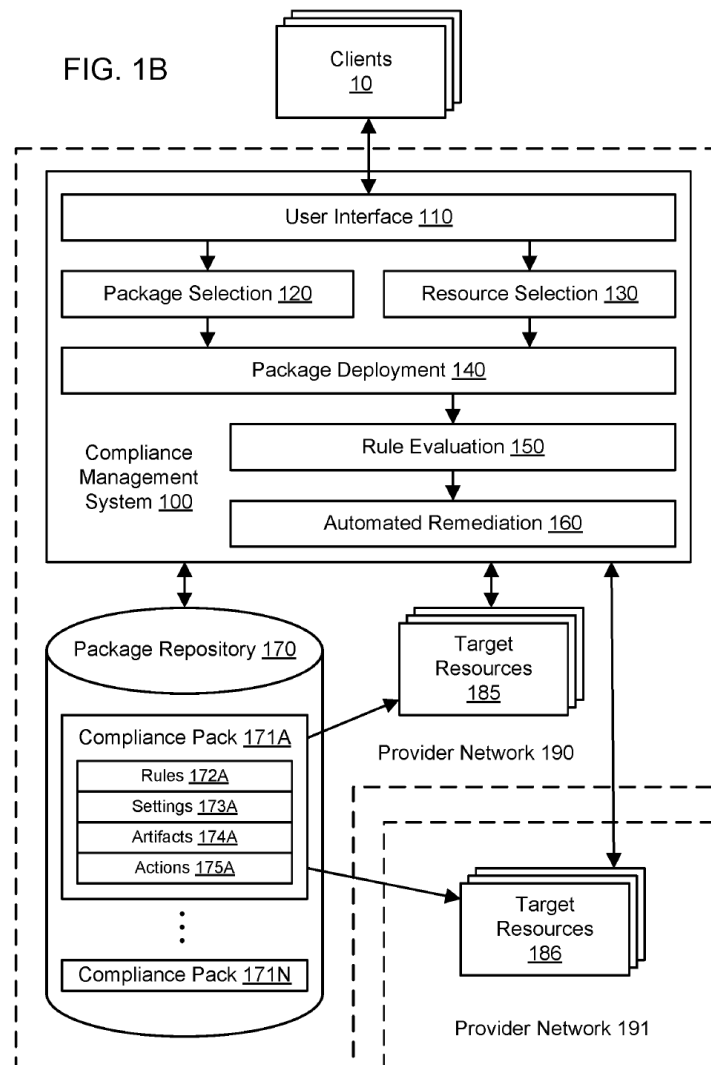
Calvo also teaches *a reachable resource having a network path to access the reachable resource* because (in addition to Calvo’s exemplary *network path*) Calvo teaches its selected target resources include one or more reachability parameters (e.g., Calvo’s port 22) which may provide access from an external network (e.g., through Calvo’s firewall from Calvo’s public Internet). Calvo, 6:35-39, 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.”).

Accordingly, Calvo's exemplary path from the public Internet through the firewall and port 22 to selected cloud-based target resources (where Calvo's target resources have one or more reachability parameters per the '693 Patent) teaches *a reachable resource having a network path to access the reachable resource*.

Calvo also teaches that *the reachable resource is a cloud object deployed in a cloud computing environment*. Calvo discloses methods and systems "for compliance lifecycle management for cloud-based resources[.]" Calvo, Abstract, Title. Calvo's "[c]loud-based resource may include computational resources (e.g., virtual compute instances), applications, services web servers, databases, and so on." Calvo, 2:9-12, 2:37-40, 3:24-41, Figs. 1A-1B. "The resources 180 may be 'cloud-based' and may be hosted in the cloud." Calvo, 3:33-35.

Calvo further teaches that its selected cloud-based target resources *hav[e] access to an external network which is external to the cloud computing environment*. Calvo's selected target resources are "cloud-based resources" "hosted in the cloud" and such resources may be "hosted in one or more provider networks" or "one or more multi-tenant provider networks, including one or more regions of such networks." Calvo, Abstract, 3:33-35, 2:44-45, 3:35-37 ("The resources 180 may be hosted in one or more multi-tenant provider networks such as networks 190 and 191."). **"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.” Calvo, 3:37-41, 9:3-8 (“A provider network may represent a network operated by an entity such as a business or public-sector organization to provide one or more services (such as various types of cloud-based computing or storage) accessible via the Internet and/or other networks to a distributed set of clients.”). Calvo’s Figures 1B “illustrate[s an] example system environment[] for compliance lifecycle management for cloud-based resources” (Calvo, 3:24-26):



Calvo, Fig. 1B.

3. ***[1(b)] actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;***

Calvo in view of Nguyen renders obvious *actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network* (e.g., Nguyen's process of pen-testing targets/potential

vulnerabilities to determine if such are actual vulnerabilities by sending instructions and receiving responses), as claimed.

Although Calvo teaches *selecting a reachable resource* (i.e., Claim 1(a)), as claimed, Calvo does not expressly provide details for *active[] inspecti[on]* as described in the '693 Patent (i.e., Claim 1(b)). However, Calvo discloses its compliance packs may be used for PCI DSS compliance. Calvo, 2:5-24. And it was well-known in the art that **PCI DDS compliance required pen-testing**. Ex. 1003, ¶¶ 55-61 (citing Exs. 1039-1044). Nguyen's pen-testing disclosures represent one example rendering obvious *active[] inspecti[on]* as claimed.

The '693 Patent explains that active inspection⁶ determines which theoretical vulnerabilities are real vulnerabilities. '693 Patent, 10:66-11:6 ("Performing an active inspection of a cloud environment allows to determine which of the reachability paths (i.e., network paths) are indeed vulnerable, meaning that paths that can be used to gain access into the cloud environment, and which reachability paths (network paths) are not vulnerabilities since the active inspector could not gain

⁶ During prosecution, Applicant stated "active inspection of a network path [is] defined in the specification in at least par. [0029], [0040]-[0043], [0050]-[0064], and [0098]-[0109]." Ex. 1002, 132. These paragraphs are 5:40-51, 7:48-8:29, 9:24-12:23, and 16:35-18:36 in the '693 Patent.

access to the resource, therefore the reachability path is not possible in practice.”), 20:44-48 (“According to some embodiments, 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.”).

The ’693 Patent also explains that sending an instruction (for example GET, CONNECT, or TRACE, which may include an access parameter such as an IP address, a port, or HTTP/UDP communication protocol) to a resource and receiving a response is an exemplary way to accomplish active inspection. ’693 Patent, 5:40-44 (“Active inspection allows to 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. For example, a reachable resource may have indicated that port 22 is an open port.”), 8:2-7 (“the 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.”), 9:62-63 (“an access instruction is generated to access the first resource based on the network path.”), 9:64-10:6 (“In certain embodiments, **the instruction includes one or more access parameters. Such parameters may include**, but are not limited to, a host name, **an IP address, a communication protocol, a port**, a username, a

password, and the like, or combination thereof. **A communication protocol may be, for example, HTTP or UDP** (user datagram protocol). For example, **the instruction may be a ping, GET, CONNECT, or TRACE request over HTTP.**”), gu10:50-53 (“executing the access instruction provides a real result of an attempt to utilize the possible path, in order to determine which paths are really viable, and which are not.”), 10:56-58 (“a network path is determined to be viable (or accessible), if the access instruction, when executed does not return an error message.”), 11:10-14 (“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).”), 20:3-6 (“In an embodiment, a resource is accessible if, for example, it can be sent instructions which are then executed by the resource.”).

Nguyen teaches the same. For example, Ngueyn teaches determining which “targets” represent “actual vulnerabilities” by performing pen-testing (which includes sending instructions and receiving responses) to identify actual threats from external surfaces in the same manner as the ’693 Patent, as explained in the following paragraphs.

First, Nguyen teaches “reconnaissance [is performed] on a desired scope [] to map a relevant external surface [which] identifies the potential targets within the desired scope that are publically [sic] accessible (e.g., via a network, such as the

Internet)[.]” Nguyen, 5:15-21, 2:9-14, 2:45-51, 15:6-16. “The reconnaissance component 210 may use public information obtained from public sources to map the relevant external surface 244” and “may be characterized as identifying [] what the bad guys see[.]” Nguyen, 5:27-29, 6:50-51. In Nguyen, “‘target[s]’ refer[] to a public facing access point or endpoint” (Nguyen, 2:5-6) and “‘external surface’ refers to all of the targets within a particular scope through which an external actor may attempt to take advantage of a potential vulnerability” (Nguyen, 4:11-14). “Examples of targets include an IP address, an interface component[,], an [API] endpoint, a [URI] endpoint, and the like.” Nguyen, 2:6-9.

Next, Nguyen teaches generating and executing test plan instructions to “identify actual security risks and, at the same time, eliminate falsely identified potential vulnerabilities.” Nguyen, 4:46-50, 12:29-31, 12:57-58, 13:29-32, 16:1-4. **“A potential vulnerability is determined to be an actual vulnerability when the test elicits a specific response indicative of the presence of a particular vulnerability[.]”** Nguyen, 10:52-54. “In this manner, the test plan eliminates false positives or potential vulnerabilities that are not actual vulnerabilities.” Nguyen, 10:58-60. “The test plan(s) 350 may be configured to test portions of the relevant external surface[.]” Nguyen, 11:5-6.

Nguyen’s test plan instructions use the same exemplary “instructions” and “access parameters” as the ’693 Patent that would be “necessary for a potential actor

to take advantage of a potential vulnerability and potentially cause harm.” Nguyen, 11:1-4. For example, Nguyen’s processors (which execute the test plans) may be a web processor, mobile processor, and/or API processor, and **may be configured to communicate via IP addresses, ports, and/or UDP/HTTP protocols using instructions such as GET, TRACE, and/or CONNECT**. Nguyen, 13:14-16, 13:22-25 (“Similarly, an **IP address** may communicate via Transmission Control Protocol (‘TCP’) or User Datagram Protocol (‘UDP’) **and on different ports.**”), 13:25-27 (“Therefore, the web processor 420A must be configured to provide instructions using an appropriate protocol and over the correct port.”), 13:45-47 (“**The instructions sent to the web processor 420A may include HTTP methods, such as POST, GET, PUT, PATCH, DELETE, HEAD, TRACE, and CONNECT.**”), 19:25 (“UDP that transmits packets”).

Finally, Nguyen teaches that, based on the response from the executed instruction, actual vulnerabilities are determined. Nguyen, 10:52-54 (“**A potential vulnerability is determined to be an actual vulnerability when the test elicits a specific response indicative of the presences of a particular vulnerability**”), 13:38-44 (“If 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. On the other hand, if the web application 102A

reacts inappropriately, the potential vulnerability is determined to be an actual vulnerability.”).

These Nguyen disclosures also teach *active[] inspecti[on]* under each party’s proffered constructions in the stayed district court proceeding. *Supra* Section III.C. Nguyen’s disclosures teach “sending a data packet over the network” because Nguyen’s exemplary access parameter “UDP [protocol] transmits packets” (Nguyen, 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, Scott, Title, [0001]). 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. Nguyen, 4:46-50, 10:52-11:6, 12:29-13:44, 16:1-4.

In the present Calvo-Nguyen combination, Calvo teaches cloud-based resources hosted in an internal cloud network that has an accessible *network path* to an external public network (e.g., the Internet). *Supra* Claim 1(a). And Nguyen teaches vetting targets/potential vulnerabilities (which are akin to Calvo’s resources) to see if an actor could gain access to them from outside the network because Nguyen teaches pen-testing. Pen-testing (or penetration testing) is a well-known

cybersecurity process (particularly for cloud networks) involving attempts to gain access to (i.e., penetrate) a network from outside the network, as explained further in Dr. Easttom's Declaration. Ex. 1003, ¶¶ 48-51 (citing Exs. 1037-1039). Nguyen's "targets" are "public facing access point[s]" and Nguyen focuses on the "external surface ... through which an external actor may attempt to take advantage of a potential vulnerability." Nguyen, 2:5-9, 4:11-16. A POSITA would have understood the present Calvo-Nguyen combination to teach 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 (Ex. 1003, ¶ 51 (citing Ex. 1007, Deardorff, Title, Abstract, 8:64-9:9)). Accordingly, the Calvo-Nguyen combination teaches *actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network*, as claimed.

A POSITA would have been motivated to incorporate Nguyen's pen-testing process into Calvo's method/system with a reasonable expectation of success for multiple reasons. Ex. 1003, ¶¶ 98-104. First, 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" (Calvo, 2:7-24), and a POSITA would have known that "[o]ne of the **requirements** in the PCI DDS is performance of network-layer **penetration**

testing[.]” Ex. 1003, ¶ 99 (quoting Ex. 1039, Soh, 1:20-33). “Under Section 11.3.4.1 of the PCI DDS, this **penetration testing must be conducted at least annually[.]**” Ex. 1039, Soh, 1:28-30. Accordingly, 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.

Second, Calvo’s disclosures would have provided teaching/motivation/suggestion to make the proposed combination. Ex. 1003, ¶ 100. For example, Calvo discloses that “as the scale and scope of typical distributed systems has increased, the tasks of provisioning, administering, and managing the computing resources have become increasingly complicated” and that prior art approaches “were complex, time-consuming, resource-consuming, and potentially prone to human error when manually implemented.” Calvo, 1:19-22, 2:30-36. Accordingly, a POSITA reading Calvo would have been motivated to ensure that the selected resources for policy deployment posed true threats as opposed to merely theoretical threats and understood that Nguyen disclosed an exemplary process to determine which potential vulnerabilities are actual vulnerabilities. Ex. 1003, ¶ 100. Calvo also discloses that its “techniques ... may be used for managing the compliance lifecycle of resources hosted in the cloud in a simplified and efficient manner” (Calvo, 2:37-40) and that its disclosures provide the “technical advantage[.]” of “improving use of computation resources by providing simplified

selection.” Calvo, 3:6–10. Accordingly, a POSITA would have readily understood that Nguyen’s autonomous pen-testing process would have furthered Calvo’s desire for simplified and efficient policy applications and simplified selections because Ngueyn describes an automated process which can rule out “false positives or potential vulnerabilities that are not actual vulnerabilities[,]” thus allowing for future processing only on verified external attack vulnerabilities; such would have saved considerable processing power in large scale systems which continually check for policy compliance such as Calvo. Ex. 1003, ¶ 100. Finally, Calvo discloses that “resource selection 130 may be performed according to a scope” and “the scope may identify a class of resources to which the pack should be deployed, and the resource selection 130 may automatically select such resources that are accessible to the user account.” Calvo, 4:22-25. A POSITA would have understood that Nguyen’s autonomous pen-testing method would have been a known way to accomplish automatic resource selection, and indeed one which would focus on true external threats as opposed to theoretical threats. Ex. 1003, ¶ 100.

Third, Nguyen’s disclosures would have also provided teaching/motivation/suggestion to make the proposed combination. Ex. 1003, ¶ 101. For example, Ngueyn discloses a focused selection and verification of resources through testing, which “ensures that computing resources and/or testers are pentesting those of the applications that pose the greatest risk.” Nguyen, 3:4-12.

Accordingly, a POSITA would have understood that incorporating Nguyen's autonomous pen-testing process into Calvo's method/system would have provided the benefit of focusing on resources that posed the greatest risk. Ex. 1003, ¶ 101. Additionally, Nguyen discloses "[m]any companies own and operate hundreds or thousands of IP address that host multiple applications each" and that "companies may own and operate hundreds or thousands of publicly facing domain names. In other words, many companies have large external surfaces that would require a long time to properly pentest using prior art manual pentesting methods." Nguyen, 4:18-24. Accordingly, a POSITA would have understood that Nguyen's autonomous pen-testing process (which determines which targets/potential vulnerabilities are actual vulnerabilities) would have been beneficial in large internal/virtual networks with large surface exposures because such an automated pen-testing process would have identified only **actual, verified** vulnerabilities for policy application and potential remediation. Ex. 1003, ¶ 101.

Fourth, such a combination would have constituted combining prior art elements (Calvo's selecting of resources and Nguyen's pen-testing to verify that the selected resources correspond to actual vulnerabilities) according to known methods (pen-testing by sending instructions and receiving responses) to yield predictable results (determining which resources are actual vulnerabilities). Ex. 1003, ¶ 102.

Fifth, 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). Ex. 1003, ¶ 103.

For at least these same reasons, a POSITA would have enjoyed a reasonable expectation of success in making such combination. *Elekta Ltd v. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1377 (Fed. Cir. 2023) (“[E]vidence establishing a motivation to combine may establish a finding of reasonable expectation of success.”). Additionally, both references describe automated processes related to resource selection. Incorporating Nguyen’s process into Calvo’s process/system would have required at most minor modifications in software. Ex. 1003, ¶ 104. Finally, both Calvo and Nguyen matured into issued United States patents from applications filed by the same Amazon Technologies, Inc. entity, thus further evidencing their compatibility. *Id.*

4. [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;

Calvo in view of Nguyen renders obvious *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 (e.g., Nguyen’s storing of test results indicating which potential vulnerabilities are actual vulnerabilities), as claimed.

Because Calvo does not expressly explain *active[] inspecti[on]* as described in the ’693 Patent, Calvo also does not expressly explain *storing an indicator* in response to *active[] inspecti[on]*; however, Nguyen’s pen-testing process does.

The ’693 Patent explains that “if a resource is successfully accessed ... this result can be stored[.]” ’693 Patent, 11:40-44.

Nguyen teaches the same. As explained above, Nguyen teaches *active[] inspecti[on]* via Nguyen’s pen-testing process that determines which targets (potential vulnerabilities) are actual vulnerabilities by sending instructions to such targets and receiving responses. *Supra* Claim 1(b).

And like the ’693 Patent, Nguyen further teaches storing the results of such *active[] inspecti[on]*, which includes results indicating which targets (potential vulnerabilities) have been determined to be actual vulnerabilities based on instructions sent and responses received. For example, Nguyen teaches “vulnerabilities database 380 [] stores results obtained from performing tests on targets” (Nguyen, 11:16-17) and “[t]he test results 390 may identify one or more **actual vulnerability**.” Nguyen, 16:12-13, 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.**”), 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).”).

These Nguyen disclosures also teach *a valid path* under each party’s proffered constructions in the stayed district court proceeding. *Supra* Section III.C. Nguyen’s disclosures teach “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). Nguyen, 10:58-60, 11:16-17, 16:12-13, 13:1-5; *Supra* Claim 1(b). Nguyen’s disclosures also teach “network path through which a resource is reachable” for the same reasons. *Id.*

As explained above, a POSITA would have been motivated to incorporate Nguyen’s pen-testing process (to determine which targets/potential vulnerabilities are actual vulnerabilities) into Calvo’s method/system with a reasonable expectation

of success. *Supra* Claim 1(b). This incorporation/combination would have included Nguyen's storing of such determination for at least the same reasons explained above. *Supra* 1(b); Ex. 1003, ¶ 110. Additionally, a POSITA would have been specifically motivated 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. Ex. 1003, ¶ 111-113. It would have been common sense to store the results of the pen-testing process because the purpose of such a process is to determine actual vulnerabilities and eliminate "false positives." *Id.* If the results were not stored, such "false positives" would not remain ruled out after being identified. *Id.* A POSITA would have enjoyed a reasonable expectation of success in making such incorporation/combination for the same reasons explained in Claim 1(b), and also at least because a POSITA would have known how to store test results. Ex. 1003, ¶ 114.

Accordingly, the Calvo-Nguyen combination 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 claimed.

5. [1(d)] *applying a policy on the valid path, wherein the policy includes a conditional rule;*

Calvo in view of Nguyen renders obvious *applying a policy on the valid path* (e.g., applying 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.

The '693 Patent explains that *a policy* includes a statement and/or conditional rule, and that *applying a policy* can be accomplished by applying a conditional rule. '693 Patent, 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.").

The '693 Patent also explains "the condition [of a conditional rule] includes determining if the policy is adhered to by the network path. In some embodiments, this is determined [] by applying a rule and checking the result of the outcome[.]" '693 Patent, 22:39-45. The '693 Patent provides the following exemplary scenario for "a policy [] applied on a valid network path" ('693 Patent, 21:56, Fig. 9 at S930): "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). 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.” ’693 Patent, 22:2-8.

Calvo teaches the same. First, Calvo teaches *a policy that includes a conditional rule*. For example, Calvo discloses “compliance packs” and explains “[a] compliance pack 171A may include a plurality of rules 172A that can be evaluated to determine the policy compliance of a resource.” Calvo, 5:60-62. Additionally, Calvo discloses that its compliance packs may include “remedial actions to be taken if resources are found to be noncompliant.” Calvo, 2:46-51. 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. Ex. 1003, ¶ 118. Further, Calvo provides the following 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.” Calvo, 6:35-39. In this exemplary scenario, the conditional rule is “port 22 is not accessible to the Internet.”

Calvo also teaches *applying a policy on the [] path*. Calvo teaches *applying a policy* because Calvo teaches applying/deploying its compliance pack. Calvo, 2:42-45 (“A compliance management system may permit **a compliance package to be applied** to one or more resources in one or more multi-tenant provider networks,

including one or more regions of such networks.”), 4:2-9 (“select the account(s) or target resources **to which the compliance pack should be applied**, and **deploy the compliance pack** to the selected account(s) or resources.”), 2:64-3:1 (“users may easily select and **deploy compliance packs** to cloud-based resources to determine the policy compliance of those resources.”), 4:47-49 (“the selected **compliance pack 171A may be deployed** to the selected resources 185 using a package deployment component 140.”), Fig. 2B.

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. Calvo, 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.

Accordingly, because Calvo teaches *applying a policy on the [] path* and Nguyen teaches *that the network path is a valid path* (*supra* Claim 1(c)), the Calvo-Nguyen combination described above teaches *applying a policy on the valid path*, as claimed.

6. [1(e)] initiating a mitigation action, in response to determining that the conditional rule is not met; and

Calvo discloses, or otherwise renders obvious, *initiating a mitigation action, in response to determining that the conditional rule is not met* (e.g., Calvo’s remedial actions taken in response to a determination of rule noncompliance), as claimed.

The ’693 Patent explains “the mitigation action includes revoking access to the reachable resource, revoking access from the reachable resource, **closing a port**

of the reachable resource, **generating a notification**, generating an alert, any combination thereof, and the like.” ’693 Patent, 22:53-57.

Calvo teaches the same. As explained above, Calvo discloses deploying compliance packs that contain conditional rules. *Supra* Claim 1(d). Calvo also discloses that “[f]or each of the target resources 185, the system 100 may perform rule evaluation 150 for all the rules 172A in the compliance pack 171A. Rule evaluation 150 may include ... determining whether the resource is compliant or noncompliant with the rule.” Calvo, 4:52-58. “For resources found to be noncompliant, the system 100 may perform automated remediation 160.” Calvo, 4:58-60. “The automated remediation 160 may include performing one or more remedial actions[.]” Calvo, 4:60-61. **“Remedial actions for noncompliance may include notifying relevant users, modifying a configuration of a resource, isolating a resource, and so on.”** Calvo, 2:60-64, 4:9-13 (“Remedial actions 175A may result in notification of noncompliance to relevant users or other notification targets.”) Calvo, 4:63-65, (“system 100 may perform automated tasks to deploy a selected compliance pack, evaluate rules, potentially remediate any noncompliance”), 10:44–61. As can be seen in Calvo’s Figure 2B at steps 240-250, Calvo discloses that if a resource is noncompliant (i.e., a rule in the compliance pack is not met), then remedial actions are taken:

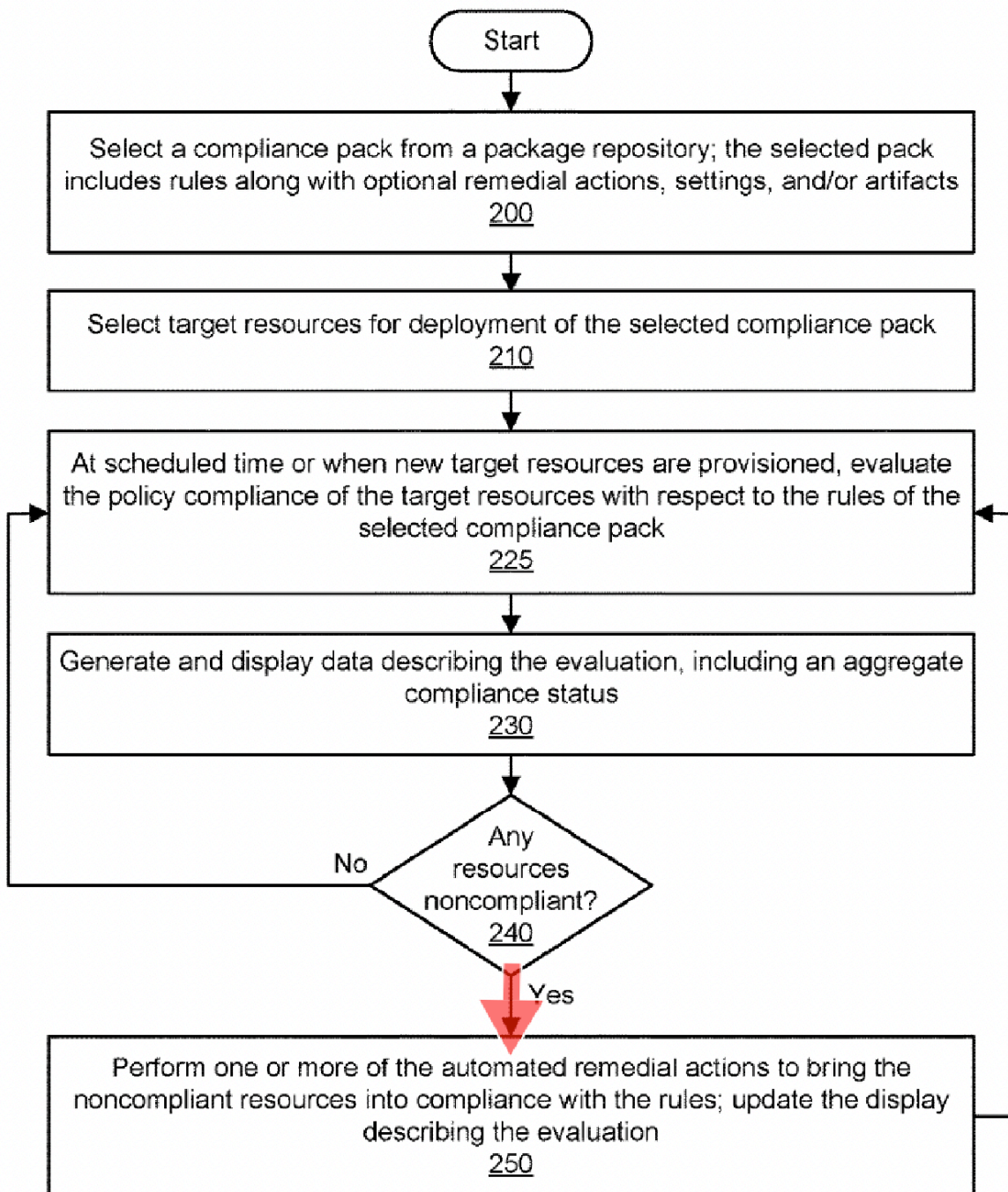


FIG. 2B

Calvo, Fig. 2B (annotated).

Additionally, in Calvo's exemplary scenario discussed above, the *mitigation action* is **closing port 22**. Calvo, 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.").

7. [1(f)] applying the policy on another network path, in response to determining that the conditional rule is met.

Calvo discloses, or otherwise renders obvious, *applying the policy on another network path, in response to determining that the conditional rule is met* (e.g., Calvo's continuous compliance verification process which 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.

The '693 Patent explains "FIG. 9 is a flowchart of a method for applying a policy on a network path[.]" '693 Patent, 5:21-22. As the Figure 9 disclosures explain, "[a]t S920, active inspection of a network path is initiated," "[a]t S930, a policy is applied on a valid network path," and "[a]t S940, a check is performed to determine if a condition is met." '693 Patent, 21:30-22:40. At this point, the Figure 9 disclosures then explain two options, as shown in the annotated figure below:

- (1) "[w]here the condition is satisfied (e.g., the network path adheres to the policy), execution continues at S920[;]"

- The first option is the subject of the present Claim 1(f) limitation.
- (2) “where the condition is not satisfied (e.g., the network path does not adhere to the policy), execution continues at S950.” ’693 Patent, 22:45-50.
- The second option is “S950, a mitigation action is initiated” (’693 Patent, 22:51-52) and is the subject of Claim 1(e).

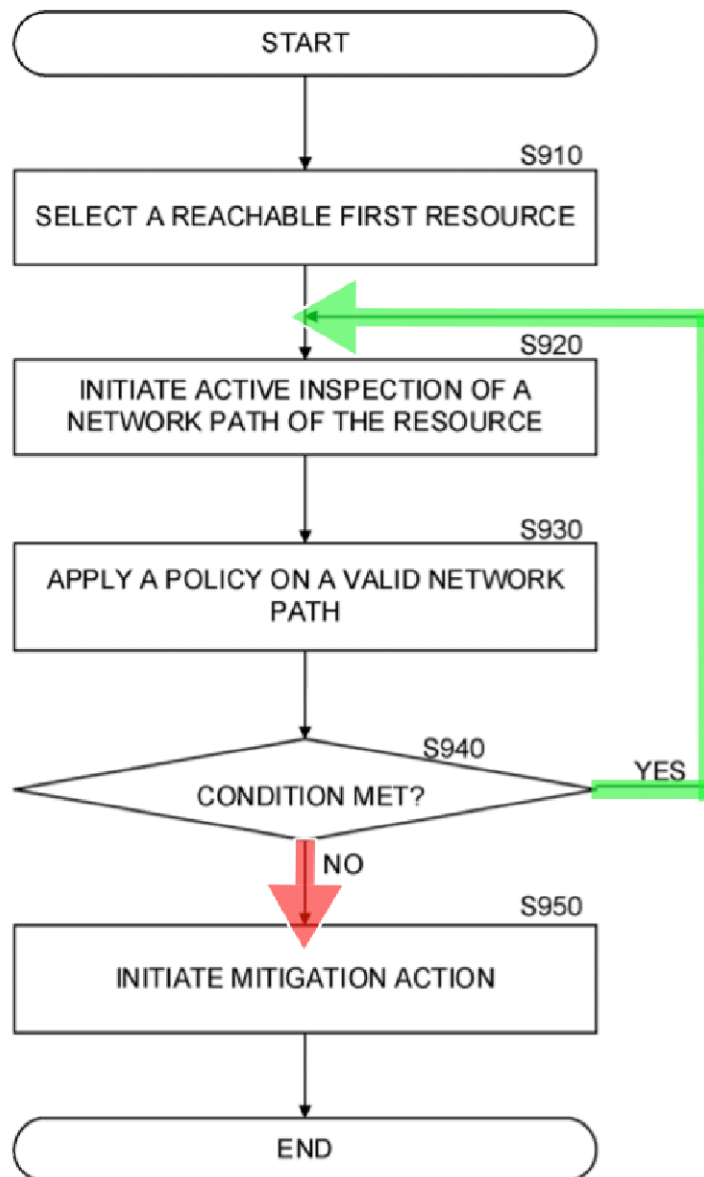


FIG. 9

'693 Patent, Fig. 9 (annotated). Accordingly, and in this manner, the '693 Patent teaches an iterative process for *applying the policy on another network path, in response to determining that the conditional rule is met*, as claimed.

Calvo teaches the same. Calvo discloses a “continuous compliance verification” process (i.e., applying Calvo’s rule(s) on a resource with one path, checking for rule compliance, **remediating in an instance of non-compliance** or alternatively **repeating policy application for subsequent resources with subsequent paths in an instance of compliance**), for example, as seen in the annotated figure below:

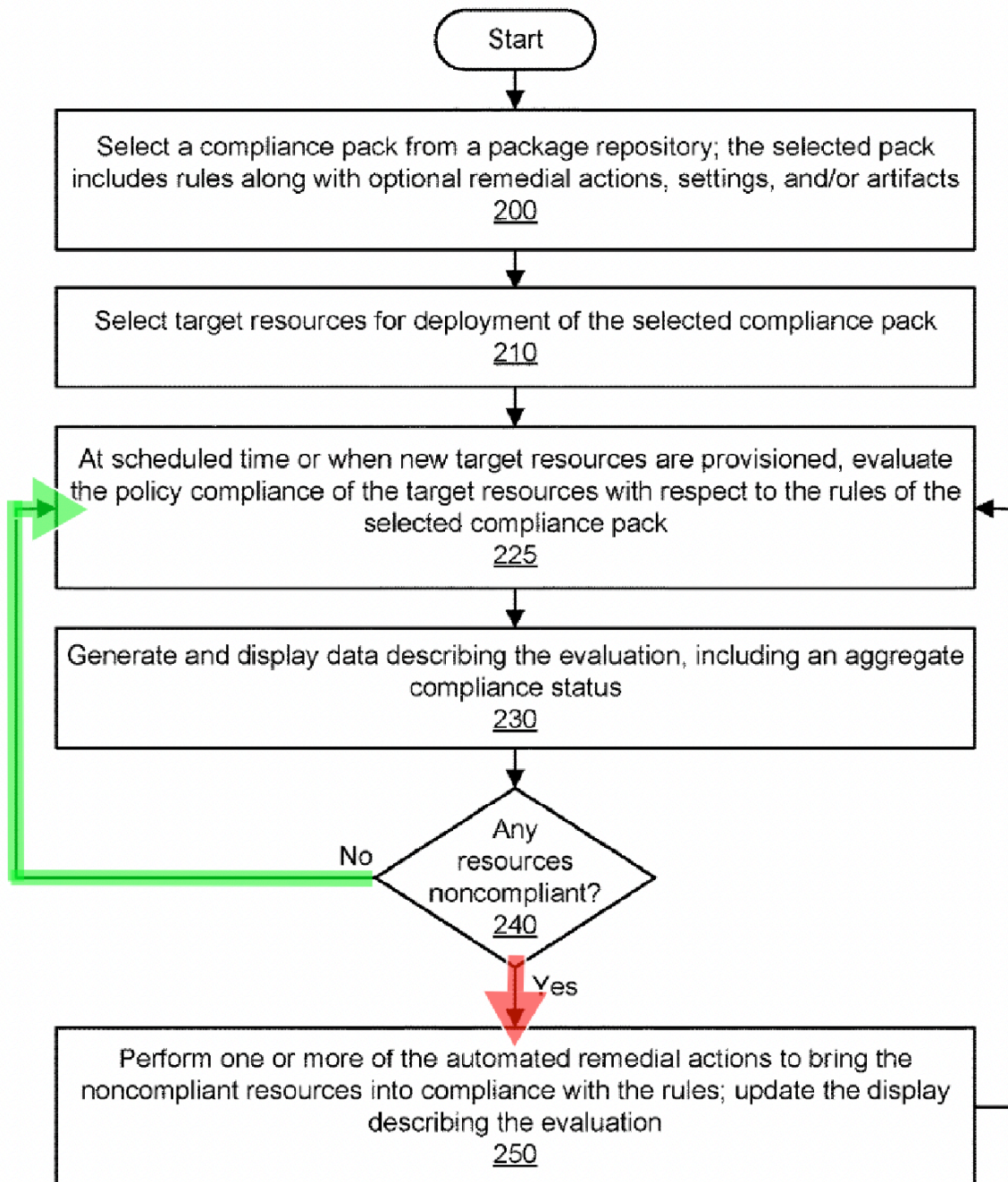


FIG. 2B

Calvo, Fig. 2B (annotated), 4:35-37 (“a compliance pack may be deployed to particular regions or divisions of a provider network or other enterprise.”), 4:52-54

(“For each of the target resources 185, the system 100 may perform rule evaluation 150”), 5:1-9 (“In the case of continuous compliance management, the stored association between the compliance pack 171A and the target resources 185 may be re-used in performing the rule evaluation 150 (and automated remediation 160) repeatedly over time. In various embodiments, the rule evaluation 150 may be performed . . . when a new resource is provisioned in the target resources”), 7:33-36 (“The results may include an aggregate compliance score or status for multiple resources [] for an individual rule.”), 7:51-60, 10:41-43.

As seen in Calvo’s Figure 9, after a compliance pack is deployed and rule evaluation for a resource (with one *network path* per the ’693 Patent) is performed, there are two options (just like the ’693 Patent) at step 240: (1) if the resource complies with the rule, follow the green annotated route back up in the iterative process and apply the rule/check for compliance on another resource with another *network path*; or (2) if the resource is noncompliant with the rule, follow the red annotated path and perform remediation actions. This second option is the subject of Claim 1(e), and the first option teaches Claim 1(f) because it teaches applying the same compliance pack (with the same at least one conditional rule) to another resource with another *network path* in response to determining the rule was complied with for a previous resource (the green annotated path from step 240).

Calvo's application of the same rule on a subsequent resource teaches *applying the policy on another network path* because the subsequent resource has a different *network path* than the first resource per the '693 Patent. As explained above, two resource nodes communicatively connected together represent a *network path* per the '693 Patent (and also how a POSITA would have understood *network path*). *Supra* Claim 1(a); '693 Patent, 12:46-47 ("A network path is a connection of two or more security objects"), 8:30-39; Ex. 1003, ¶¶ 39-43. And Calvo teaches "a user may deploy a compliance pack ... even across an entire enterprise and have access to a unified view of compliance across the target resources." Calvo, 3:1-5, 3:67-4:2, 6:39-41 ("Using a single compliance pack, such rules may be applied to disparate resources throughout an enterprise in a consistent manner."). Each of Calvo's resources has a distinct *network path* per the '693 Patent and as would have been understood by a POSITA.

Accordingly, Calvo's continuous compliance verification process, which applies the same compliance pack (containing the same conditional rule(s)) to subsequent resources (which have subsequent *network paths*) after confirming compliance for a previous resource (which has a previous *network path*) teaches *applying the policy on another network path, in response to determining that the conditional rule is met*, as claimed.

B. Claim 2

1. ***2. The method of claim 1, further comprising: initiating active inspection for each network path of a plurality of network paths; and applying the policy only on a network path of the plurality of network paths which is a valid path.***

Calvo in view of Nguyen renders obvious *the method of claim 1, further comprising: initiating active inspection for each network path of a plurality of network paths* (e.g., Nguyen’s process of pen-testing multiple resources/targets/potential vulnerabilities with multiple paths to determine if such are actual vulnerabilities by sending instructions to the such and receiving responses); *and applying the policy only on a network path of the plurality of network paths which is a valid path* (e.g., applying Calvo’s compliance pack on a resource with a path which Nguyen has verified is an actual vulnerability and not false positive potential vulnerabilities ruled out by Nguyen), as claimed.

As explained above, Nguyen’s pen-testing process teaches *active inspection* as claimed. *Supra* Claim 1(b). In the Calvo-Nguyen combination described above, there are multiple of Calvo’s resources (with multiple paths) selected for Nguyen’s pen-testing. *Supra* Claims 1(a)-1(b). As also explained above, because each such resource has its own *network path* per the ’693 Patent and as a POSITA would have understood, Nguyen’s pen-testing of such multiple resources teaches *active inspection for each network path of a plurality of network paths*. *Id.* For example, Nguyen’s process includes “reconnaissance [which] identifies all of the potential

targets within the desired scope.” Nguyen, 2:47-51, 2:54-57, 4:46-50, 9:18-23, 14:44-46 (“A chained test is a test that takes advantage of multiple potential vulnerabilities, including potential vulnerabilities that are deeper in a computing system.”), 15:67-16:5; *supra* Claim 1(b).

The Calvo-Ngueyn combination described above teaches *applying the policy only on a network path of the plurality of network paths which is a valid path* because the combination performs *active inspection* on multiple *network paths*, and Calvo’s compliance pack is applied only on a *network path that* has been verified as an actual vulnerability because Nguyen’s pen-testing process “eliminate[s] falsely identified potential vulnerabilities.” Nguyen, 4:46-50, 12:29-31, 12:57-58, 13:29-32, 16:1-4, 10:58-60 (“the test plan eliminates false positives or potential vulnerabilities that are not actual vulnerabilities.”), 13:38-44 (“If the web application 102A reacts appropriately ... the potential vulnerability is determined to be a false positive”).

C. Claim 3

1. ***3. The method of claim 2, further comprising: initiating active inspection by generating an access instruction for the reachable resource; and executing the access instruction on a network path.***

Calvo in view of Nguyen renders obvious *the method of claim 2, further comprising: initiating active inspection by generating an access instruction for the reachable resource and executing the access instruction on a network path* (e.g.,

Nguyen's generating and executing of test instructions to determine which potential vulnerabilities are actual vulnerabilities), as claimed.

As explained above, Nguyen's teaches *active inspection* in the same manner as the '693 Patent because Nguyen discloses generating and executing test plan instructions to accomplish such using the same exemplary instructions and parameters as the '693 Patent. *Supra* Claim 1(b).

For example, Nguyen discloses that its system "is configured to automatically generate one or more test plans and automatically execute the test plan(s) against the portion 102 of the applications 104 to automatically identify actual security risks and, at the same time, eliminate falsely identified potential vulnerabilities." Nguyen, 4:46-50. And Nguyen's test plan(s) includes the same exemplary instructions and parameters as the '693 Patent. *Compare* '693 Patent, 9:61-10:6 ("an access instruction is generated ... the instruction includes one or more access parameters. Such parameters [] include [] an IP address, a communication protocol, a port ... A communication protocol may be [] HTTP or UDP ... the instruction may be [] GET, CONNECT, or TRACE") *with* Nguyen, 13:7-32 ("the processor(s) 420 is/are configured to interface with the targets [] and test at least one application in the portion 102 of the applications 104. In other words, the processor(s) 420 are configured to translate the instructions received from the test engine(s) 410 into commands the portion 102 of the applications 104 understands and can execute. ...

the processor(s) 420 include a web processor 420A, a mobile processor 420B, and an API processor 420C ... an IP address may communicate via [TCP] or [UDP] on different ports ... web processor 420A must be configured to provide instructions using an appropriate protocol and over the correct port ... processor(s) 420 may be characterized as being tools configured to launch a test based on the instructions received from the test engine(s).”), 13:45-47 (“The instructions sent to the web processor 420A may include HTTP methods, such as [] GET, [] TRACE, and CONNECT.”).

D. Claim 4

1. ***4. The method of claim 2, further comprising: applying the policy only on each network path of the plurality of network paths which is a valid path.***

Calvo in view of Nguyen renders obvious *the method of claim 2, further comprising: applying the policy only on each network path of the plurality of network paths which is a valid path* (e.g., applying Calvo’s compliance pack on Nguyen’s actual vulnerabilities and not the false positive potential vulnerabilities ruled out by Nguyen), as claimed.

As explained above, Calvo in view of Nguyen teaches *active inspection* on a plurality of *network paths* and deploying Calvo’s compliance packs only on a *network path* that has not been eliminated as a “false positive.” *Supra* Claim 2. These teachings further teach the claimed scenario of Claim 4, where *each network path*

out of multiple *network paths* is determined to be a *valid path* because the false positives have been eliminated, at least because Nguyen’s disclosures teach that more than one *network path* may be determined to be an actual vulnerability. For example, Nguyen teaches “vulnerabilities database 380 [] stores results obtained from performing tests on targets” (Nguyen, 11:16-17) and “[t]he test results 390 may identify one or more actual vulnerability.” Nguyen, 16:12-13. Accordingly, “false positives” are ruled out by Nguyen, and Calvo’s policy application is only done on the remaining verified threats.

E. Claim 5

1. ***5. The method of claim 4, further comprising: initiating active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.***

Calvo in view of Nguyen renders obvious *the method of claim 4, further comprising: initiating active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path* (e.g., Nguyen’s process of pen-testing multiple potential vulnerabilities paths to determine if such are actual vulnerabilities by sending instructions to such and receiving responses), as claimed.

As explained for the previous claims, the Calvo-Nguyen combination teaches *active inspection* for a plurality of *network paths* to determine which are *valid network paths*. *Supra* Claims 1-4.

F. Claim 6

- 1. 6. The method of claim 1, further comprising: initiating the mitigation action on the reachable resource.**

Calvo in view of Nguyen renders obvious *the method of claim 1, further comprising: initiating the mitigation action on the reachable resource* (e.g., Calvo’s remedial actions including modifying a resource, isolating a resource, and closing a port), as claimed.

As explained above, Calvo discloses that its “[r]emedial actions for noncompliance may include notifying relevant users, **modifying a configuration of a resource, isolating a resource, and so on.**” Calvo, 2:60-64. Additionally, in Calvo’s exemplary scenario discussed above, the *mitigation action* is closing port 22. Calvo, 6:35-39, 3:6-17 (explaining that “technical advantages” of Calvo’s disclosures include “improved security and policy compliance through automated remediation of noncompliant resources”).

G. Claim 7

- 1. 7. The method of claim 6, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.**

Calvo in view of Nguyen render obvious *the method of claim 6, wherein the mitigation action includes any one of: revoking access to the reachable resource,*

revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof (e.g., Calvo’s remediation actions which include notifying users, modifying a configuration of the resource, isolating the resource, and closing a port), as claimed.

As explained above (*supra* Claim 1(e)), Calvo’s remedial actions include “notifying relevant users, modifying a configuration of a resource, isolating a resource, and so on.” Calvo, 2:60-64. Additionally, in Calvo’s exemplary scenario discussed above, the *mitigation action* is closing port 22. Calvo, 6:35-39.

H. Claim 9

1. 9. *The method of claim 1, further comprising: initiating active inspection of the network path to detect an application path.*

Calvo in view of Nguyen renders obvious *the method of claim 1, further comprising: initiating active inspection of the network path to detect an application path* (e.g., Nguyen’s pen-testing process which includes reconnaissance on a scope of targets including applications), as claimed.

As explained above, the Calvo-Nguyen combination renders obvious *actively inspecting the network path* per the ’693 Patent via Nguyen’s pen-testing process. *Supra* Claim 1(b). The Calvo-Nguyen combination also teaches *initiating active inspection of the network path to detect an application path* because Nguyen’s pen-testing process includes reconnaissance on a scope of potential targets, and this

scope includes applications. Nguyen, 5:15-21 (“reconnaissance [is performed] on a desired scope [] to map a relevant external surface [which] identifies the potential targets within the desired scope that are publically [sic] accessible (e.g., via a network, such as the Internet)”); 2:9-14, 2:45-51, 15:6-16, 4:11-18 (“The term ‘external surface’ refers to all of the targets within a particular scope through which an external actor may attempt to take advantage of a potential vulnerability. The scope may include an application, a subcomponent of an application An IP address, for example, can host multiple applications and therefore can present a large external surface.”); 2:9-14 (“A target provides external or public access to application, such as a web application executing on an internal computing device, an API, a web service executing on an internal computing device, an application executing on an external computing device (e.g., a mobile device), and the like.”), Fig. 5. Additionally, Calvo teaches that its resources include applications. Calvo, 2:9-12 (“Cloud-based resources may include computational resources (e.g., virtual compute instances), applications, services, web servers, databases, and so on.”), 3:29-33, 9:48-53 (“Resources may include ... applications”).

I. Claim 10

1. 10. The method of claim 9, further comprising: generating the mitigation action further based on the application path.

Calvo in view of Nguyen renders obvious *the method of claim 9, further comprising: generating the mitigation action further based on the application path*

(e.g., Calvo’s continuous compliance verification process which includes automated remediation for target paths vetted by Nguyen’s pen-testing process which includes applications), as claimed.

As explained above, the Calvo-Nguyen combination teaches policy application on multiple resources that have corresponding multiple *network paths* via Calvo’s “continuous compliance verification” process and automatic remediation of noncompliance. *Supra* Claims 1(e)-1(f). As also explained above, the Calvo-Nguyen combination teaches *active inspection of the network path to detect an application path* via Nguyen’s pen-testing process, which includes reconnaissance on a scope of potential targets (where this scope includes applications). *Supra* Claim 9.

Accordingly, the Calvo-Nguyen combination described above teaches *generating the mitigation action further based on the application path* because Calvo continues to apply compliance packs and remedial actions based on the reconnaissance scope of Nguyen’s targets, which include applications.

J. Claim 11

- 1. [11(P)] 11. A non-transitory computer-readable medium storing a set of instructions for applying a policy on a network path, the set of instructions comprising:**

To the extent the preamble is limiting, Calvo discloses, or otherwise renders obvious, *a non-transitory computer-readable medium storing a set of instructions*

(e.g., Calvo's non-transitory computer-readable medium storing program instructions) *for applying a policy on a network path* (e.g., applying Calvo's compliance pack to firewall port 22 to prevent access from the public Internet through firewall port 22 to internal cloud-based resource(s)), as claimed.

Calvo teaches *applying a policy on a network path*. *Supra* Claims 1(a)-1(d). Calvo also teaches *a non-transitory computer-readable medium storing a set of instructions for* such. Calvo discloses “a computer system that implements a portion or all of the one or more of the technologies described herein may include a computer system that includes or is configured to access one or more computer-readable media,” Calvo's “FIG. 8 illustrates such a computing device 3000,” and “computing device 3000 includes one or more processors 3010A-3010N coupled to system memory 3020.” Calvo, 14:5-15. “[S]ystem memory 3020 may be one embodiment of a computer-readable (i.e., computer-accessible) medium configured to store program instructions and data as described above for implementing embodiments of the corresponding methods and apparatus[,]” and “computer-readable medium may include non-transitory storage media or memory.” Calvo, 15:7-15.

2. [11(a)] one or more instructions that, when executed by one or more processors of a device, cause the device to:

Calvo discloses, or otherwise renders obvious, *one or more instructions* (e.g., Calvo's program instructions) *that, when executed by one or more processors* (e.g.,

Calvo's one or more processors) of a device (e.g., Calvo's computing device), as claimed. *Supra* Claim 11(P).

3. ***[11(b)] select 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;***

Supra Claim 1(a).

4. ***[11(c)] actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;***

Supra Claim 1(b).

5. ***[11(d)] 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;***

Supra Claim 1(c).

6. ***[11(e)] apply a policy on the valid path, wherein the policy includes a conditional rule;***

Supra Claim 1(d).

7. ***[11(f)] initiate a mitigation action, in response to determining that the conditional rule is not met; and***

Supra Claim 1(e).

8. ***[11(g)] apply the policy on another network path, in response to determining that the conditional rule is met.***

Supra Claim 1(f).

K. Claim 12

1. [12(P)] 12. A system for applying a policy on a network path comprising:

Calvo in view of Ngueyn renders obvious *a system* (e.g., Calvo's computer system) *for applying a policy on a network path* (e.g., applying Calvo's compliance pack to firewall port 22 to prevent access from the public Internet through firewall port 22 to internal cloud-based resource(s)), as claimed.

Calvo teaches *applying a policy on a network path*. *Supra* Claims 1(a)-1(d). Calvo also teaches *a system for* such. Calvo discloses “a computer system that implements a portion or all of the one or more of the technologies described herein may include a computer system that includes or is configured to access one or more computer-readable media,” Calvo's “FIG. 8 illustrates such a computing device 3000,” and “computing device 3000 includes one or more processors 3010A-3010N coupled to system memory 3020.” Calvo, 14:5-15. “[P]rocessors 3010A-3010N may include any suitable processors capable of executing instructions.” Calvo, 14:20-21. “[S]ystem memory 3020 may be configured to store program instructions and data accessible by processor(s) 3010A-3010N.” Calvo, 14:29-31. “[S]ystem memory 3020 may be one embodiment of a computer-readable (i.e., computer-accessible) medium configured to store program instructions and data as described above for implementing embodiments of the corresponding methods and apparatus[,]” and

“computer-readable medium may include non-transitory storage media or memory.”

Calvo, 15:7-15

2. [12(a)] a processing circuitry; and

Calvo discloses, or at least renders obvious, *a processing circuitry* (e.g., Calvo’s one or more processors), as claimed. *Supra* Claim 12(P).

3. [12(b)] a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to:

Calvo discloses, or otherwise renders obvious, *a memory* (e.g., Calvo’s system memory), *the memory containing instructions* (e.g., Calvo’s program instructions) *that, when executed by the processing circuitry* (e.g., Calvo’s one or more processors execute Calvo’s program instructions), as claimed. *Supra* Claim 12(P).

4. [12(c)] select 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;

Supra Claim 1(a).

5. [12(d)] actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;

Supra Claim 1(b).

6. [12(e)] store 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;

Supra Claim 1(c).

7. *[12(f)] apply a policy on the valid path, wherein the policy includes a conditional rule;*

Supra Claim 1(d).

8. *[12(g)] initiate a mitigation action, in response to determining that the conditional rule is not met; and*

Supra Claim 1(e).

9. *[12(h)] apply the policy on another network path, in response to determining that the conditional rule is met.*

Supra Claim 1(f).

L. Claim 13

1. *13. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection for each network path of a plurality of network paths; and apply the policy only on a network path of the plurality of network paths which is a valid path.*

Supra Claims 12, 2.

M. Claim 14

1. *14. The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection by generating an access instruction for the reachable resource; and execute the access instruction on a network path.*

Supra Claims 13, 3.

N. Claim 15

1. *15. The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: apply the policy only on each network path of the plurality of network paths which is a valid path.*

Supra Claims 13, 4.

O. Claim 16

1. *16. The system of claim 15, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.*

Supra Claims 15, 5.

P. Claim 17

1. *17. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate the mitigation action on the reachable resource.*

Supra Claims 12, 6.

Q. Claim 18

1. *18. The system of claim 17, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.*

Supra Claims 17, 7.

R. Claim 20

- 1. 20. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection of the network path to detect an application path.**

Supra Claims 12, 9.

S. Claim 21

- 1. 21. The system of claim 20, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate the mitigation action further based on the application path.**

Supra Claims 20, 10.

VII. GROUND 2: CLAIMS 8 AND 19 ARE OBVIOUS OVER CALVO, NGUYEN, AND DATSENKO

A. Claim 8

- 1. 8. The method of claim 1, further comprising: generating an exception to the policy based on a valid network path.**

Calvo in view of Nguyen and Datsenko renders obvious *generating an exception to the policy based on a valid network path* (e.g., Datsenko's generating of an exception to a policy), as claimed.

As explained above, the Calvo-Nguyen combination teaches *applying a policy on the valid path*. *Supra* Claim 1(d). The Calvo-Nguyen combination does not expressly disclose *generating an exception to the policy based on a valid network path*. However, Datsenko does.

Datsenko teaches *generating an exception to the policy*. Datsenko teaches an “Override for Policy Enforcement System,” which includes “a mechanism for assisting a user in obtaining an exception to a given policy.” Datsenko, Title, Abstract, [0003], [0009], [0021] (“Embodiment 100 is an example of a device that may monitor access to a resource, then launch an exception management system that may or may not issue an exception to the access policy.”), [0023] (“The exception management system may provide a work around or exceptions to the access control policy for certain situations.”), [0037], [0048] (“exception management system 126 may generate an exception”).

Accordingly, the Calvo-Nguyen combination in further view of Datsenko teaches *generating an exception to the policy based on a valid network path* because Calvo-Nguyen teaches determination of *a valid network path* and Datsenko teaches *an exception to the policy* based on such a *path*. *Supra* Claim 1; Datsenko, [0003] (“each exception may have one or more paths by which the exception may be granted. The policy enforcement system may be used for any type of access control to any resource, including URL resources, physical peripherals or networks, data or applications, or any other resource”), [0013] (“policy enforcement system may operate at a resource or at a gateway to a resource. For example, a network may have a gateway through which devices on the outside of the network may request access to the network.”).

A POSITA would have been motivated to incorporate Datsenko's policy exception mechanism into the Calvo-Nguyen method/system described above with a reasonable expectation of success for multiple reasons. Ex. 1003, ¶¶ 186-187.

First, Datsenko's disclosures provide teaching/suggestion/motivation to do so. For example, Datsenko discloses that "[t]he exception mechanism may capture a reason or set of reasons why a user wishes to access the resource that is otherwise restricted." Datsenko, [0010]. "For example, a marketing professional may wish to access a social network website that may be normally blocked within a corporation. Because the marketing professional may have a business need to access the social network website, the exception policy 128 may create an exception when the marketing professional self-certifies that the access is for a business need." Datsenko, [0043]. Additionally, a POSITA would have understood that compliance requirements change over time, and therefore policy exceptions may be needed. Ex. 1003, ¶ 186 (citing Exs. 1041-1044). Accordingly, a POSITA would have understood that there may be reasons why an exception to an otherwise valid policy may be needed, and Datsenko's exception mechanism would have been one way to satisfy such a need. *Id.*

Second, such a combination would have constituted combining prior art elements (the network path policy applications of the Calvo-Nguyen system and policy exception mechanism of Datsenko) according to known methods (software

implementations) to yield predictable results (allow exceptions to otherwise valid policies when needed). *Id.*

Third, such a combination would have constituted the use of a known technique (updating policy compliance software to allow for needed exceptions) to improve a similar device (the policy compliance devices of the Calvo-Nguyen system and Datsenko system) in the same way (the Calvo-Nguyen system would benefit from necessary exceptions the same way Datsenko does). *Id.*

A POSITA would have enjoyed a reasonable expectation of success in making such incorporation/combination. *Id.*, ¶ 187. For example, Datsenko discloses that its “policy enforcement system may operate at a resource or at a gateway to a resource. For example, a network may have a gateway through which devices on the outside of the network may request access to the network.” Datsenko, [0013]. And Datsenko discloses that its “policy enforcement system may be used for any type of access control to any resource, including URL resources, physical peripherals or networks, data or applications, or any other resource.” Datsenko, [0003], [0035]. Accordingly, a POSITA would have recognized that Datsenko’s policy exception mechanism could have been readily implemented into the Calvo-Nguyen method/system described above because each represents a working example of using policies/rules to enforce/allow/restrict access from an external network to an internal network. Ex. 1003, ¶ 187. Additionally, such an incorporation/combination would represent

trivial modifications in software that would have been well within the skill set of a POSITA before the '693 Patent. *Id.*; Datsenko, [0016] (“some or all of the subject matter may be embodied in hardware and/or software (including firmware, resident software, micro-code, state machines, gate arrays, etc.)”).

B. Claim 19

- 1. 19. The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate an exception to the policy based on a valid network path.***

Supra Claims 12, 8.

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

B. Related Matters

The '693 Patent is presently asserted in the stayed district court litigation: *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23-CV-00758 (D. Del.). The '693 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) robin.snader@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	Eric A. Buresh (Reg. No. 50,394) eric.buresh@eriseip.com Kathleen Fitterling (Reg. No 62,950) kathleen.fitterling@eriseip.com Christopher Schmidt (Reg. No. 63,982) chris.schmidt@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 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. 11,936,693 for Claims 1-21

Claim Designation	Claim Language
Claim 1(P)	A method for applying a policy on a network path, comprising:
Claim 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;
Claim 1(b)	actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;
Claim 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;
Claim 1(d)	applying a policy on the valid path, wherein the policy includes a conditional rule;
Claim 1(e)	initiating a mitigation action, in response to determining that the conditional rule is not met; and
Claim 1(f)	applying the policy on another network path, in response to determining that the conditional rule is met.
Claim 2	The method of claim 1, further comprising: initiating active inspection for each network path of a plurality of network paths; and applying the policy only on a network path of the plurality of network paths which is a valid path.
Claim 3	The method of claim 2, further comprising: initiating active inspection by generating an access instruction for the reachable resource; and executing the access instruction on a network path.
Claim 4	The method of claim 2, further comprising: applying the policy only on each network path of the plurality of network paths which is a valid path.

Claim Designation	Claim Language
Claim 5	The method of claim 4, further comprising: initiating active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.
Claim 6	The method of claim 1, further comprising: initiating the mitigation action on the reachable resource.
Claim 7	The method of claim 6, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.
Claim 8	The method of claim 1, further comprising: generating an exception to the policy based on a valid network path.
Claim 9	The method of claim 1, further comprising: initiating active inspection of the network path to detect an application path.
Claim 10	The method of claim 9, further comprising: generating the mitigation action further based on the application path.
Claim 11(P)	A non-transitory computer-readable medium storing a set of instructions for applying a policy on a network path, the set of instructions comprising:
Claim 11(a)	one or more instructions that, when executed by one or more processors of a device, cause the device to:
Claim 11(b)	select 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;
Claim 11(c)	actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;

Claim Designation	Claim Language
Claim 11(d)	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;
Claim 11(e)	apply a policy on the valid path, wherein the policy includes a conditional rule;
Claim 11(f)	initiate a mitigation action, in response to determining that the conditional rule is not met; and
Claim 11(g)	apply the policy on another network path, in response to determining that the conditional rule is met.
Claim 12(P)	A system for applying a policy on a network path 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)	select 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;
Claim 12(d)	actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;
Claim 12(e)	store 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;
Claim 12(f)	apply a policy on the valid path, wherein the policy includes a conditional rule;
Claim 12(g)	initiate a mitigation action, in response to determining that the conditional rule is not met; and
Claim 12(h)	apply the policy on another network path, in response to determining that the conditional rule is met.

Claim Designation	Claim Language
Claim 13	The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection for each network path of a plurality of network paths; and apply the policy only on a network path of the plurality of network paths which is a valid path.
Claim 14	The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection by generating an access instruction for the reachable resource; and execute the access instruction on a network path.
Claim 15	The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: apply the policy only on each network path of the plurality of network paths which is a valid path.
Claim 16	The system of claim 15, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.
Claim 17	The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate the mitigation action on the reachable resource.
Claim 18	The system of claim 17, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.

Claim Designation	Claim Language
Claim 19	The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate an exception to the policy based on a valid network path.
Claim 20	The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection of the network path to detect an application path.
Claim 21	The system of claim 20, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate the mitigation action further based on the application path.

APPENDIX OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 11,936,693 (“’693 Patent”)
1002	Prosecution History for U.S. Patent No. 11,936,693 (“’693 Prosecution History”)
1003	Declaration of Dr. Easttom, CV attached as Appendix A
1004	U.S. Patent No. 10,949,406 to Calvo et al. (“Calvo”)
1005	U.S. Patent No. 11,558,414 to Nguyen (“Nguyen”)
1006	U.S. Patent Application Publication No. 2012/0311696 (“Datsenko”)
1007	U.S. Patent No. 11,418,528 to Deardorff et al. (“Deardorff”)
1008	Understanding Cloud Computing Basics, October 9, 2020, EU Online (“Cloud Computing Basics”)
1009	Introduction to Cloud Computing, Cloud Computing I, 15-319, Spring 2010, Majd F. Sakr (“Sakr”)
1010	Cloud Computing: An Overview, Ling Qian et al., 2009, LNCS 5931, 626-631 (“Qian”)
1011	The Introduction of Big Data in Cloud Computing, Austin Gruenberg, Minnesota State University Moorhead (“Gruenberg”)
1012	Cloud Computing Explained, Vangie Beal, May 21, 2010 (“Beal”)
1013	Study: Cloud Computing to Brighten Future of Data Centers, Martin LaMonica, March 10, 2008, CNET (“LaMonica”)
1014	Energy Aware Consolidation for Cloud Computing, Shekhar Srikantaiah et al. (“Srikantaiah”)
1015	Above the Clouds: A Berkeley View of Cloud Computing, Michael Armbrust et al, February 10, 2009 (“Armbrust”)
1016	Use of Cloud Computing Applications and Services, John Horrigan, September 12, 2008 (“Horrigan”)
1017	The NIST Definition of Cloud Computing, Publication 800-145, Peter Mell and Timoth Grance, U.S. Department of Commerce (“Mell”)

Exhibit	Description
1018	NIST Cloud Computing Standards Roadmap, Publication 500-291, Version 2 (“Gallagher”)
1019	No Vacancy: IPv4 Address Depletion and Possible Solutions for the Expanding Internet, Illumin Magazine, June 27, 2011, Steve Wolfsohn (“Wolfsohn”)
1020	Internet Protocol, DARPA Internet Program Protocol Specification, September 1981, RFC: 791(“RFC 791”)
1021	Internet Protocol, Version 6 Specification, December 1995 (“RFC 1883”)
1022	A Brief History of the Internet and Related Networks, Internet Histories, https://www.cs.kent.edu/~javed/internetbook/cerfs/cerf.html (“A Brief History of the Internet and Related Networks”)
1023	A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures, Zhijiang Chen et al., Big Data Research, 2015 (“Chen”)
1024	U.S. Patent Application Publication No. 2022/0360958 (“Cui”)
1025	Transmission Control Protocol, DARPA Internet Program Protocol Specification, September 1981, RFC: 793 (“RFC 793”)
1026	MegaLexica, Computer Dictionary of Information Technology (“MegaLexica”)
1027	U.S. Patent No. 10,205,638 to Angrish et al. (“Angrish”)
1028	European Patent Specification No. EP 3 013 016 to Murthy (“Murthy”)
1029	Cisco Configure Static Routing, Nexus 3000 Series Switches (“Cisco Static Routing”)
1030	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7 (“Cisco Firepower”)
1031	Cisco Routing Concepts (“Cisco Routing Concepts”)
1032	Analyzing the Internet’s BGP Routing Table, Geoff Huston, January 2001 (“Huston”)

Exhibit	Description
1033	How Does the Internet Work? Rus Shuler, Pomeroy IT Solutions, 2002 (“Shuler”)
1034	Unicast Routing Principles, Microsoft TechNet (“Unicast Routing Principles”)
1035	Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networks’ Resilience Against Zero-Day Attacks, Mengyuan Zhang et al., IEEE Vol. 18, No. 1, January/February 2021 (“Zhang”)
1036	U.S. Patent Application Publication No. 2015/0058993 (“Choi”)
1037	U.S. Patent No. 10,509,909 to Andriani (“Andriani”)
1038	U.S. Patent No. 11,720,685 to Gwilliams (“Gwilliams”)
1039	U.S. Patent No. 11,336,555 to Soh et al. (“Soh”)
1040	U.S. Patent No. 9,621,595 to Lian et al. (“Lian”)
1041	PCI Data Security Standard (PCI DSS), Version 1.1, September 2017 (“PCI DSS 1.1”)
1042	PCI Data Security Standard (PCI DSS), Version 1.2, March 2008 (“PCI DSS 1.2”)
1043	PCI Data Security Standard Requirements and Testing Procedures, Version 4.0, March 2022 (“PCI DSS 4.0”)
1044	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Matthew Scholl et al. (“Scholl”)
1045	European Patent Specification EP 2 869 535 to Scott et al. (“Scott”)
1046	Orca Security Ltd. v. Wiz, Inc., No. 23-758, Dkt. 222 (D. Del.) (“Amended Joint CC Chart”)
1047	Orca Security Ltd. v. Wiz, Inc., No. 23-758, Dkt. 233 (D. Del.) (“Stay Order”)

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, table of authorities, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits or claim listings, contains 12,766 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
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 June 4, 2025, 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 '693 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
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601
COUNSEL FOR PETITIONERS