

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ORCA SECURITY LTD,
Petitioner,

v.

WIZ, INC.,
Patent Owner.

IPR2025-01085
Patent 11,936,693

**PATENT OWNER WIZ, INC.'S
PRELIMINARY RESPONSE**

TABLE OF CONTENTS

	<u>Pages</u>
I. INTRODUCTION	1
II. CLAIM CONSTRUCTION	3
III. ANALYSIS.....	3
A. Ground 1: Petitioner Fails to Demonstrate that Calvo and Nguyen Render Obvious Claims 1-7, 9-18, and 20-21	3
1. Petitioner fails to demonstrate that the prior art taught or suggested <i>actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network</i> (limitation 1(b)/11(c)/12(d)).....	4
2. Petitioner fails to demonstrate that the prior art taught or suggested <i>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> (limitation 1(c)/11(d)/12(e)).....	7
a. Neither Calvo nor Nguyen teaches <i>storing an indicator to indicate that the network path is a valid path</i>	8
b. Neither Calvo nor Nguyen teach <i>in response to determining that the reachable resource is accessible from the external network</i>	10
3. Petitioner fails to demonstrate that the prior art taught or suggested <i>applying a policy on the valid path, wherein the policy includes a conditional rule</i> (limitation 1(d)/11(e)/12(f)).....	12
a. Petitioner acknowledges that a “ <i>network path</i> ” is a connection of two or more security objects	12
b. Neither Calvo nor Nguyen teaches <i>applying a policy on the [] path</i>	13
c. Neither Calvo nor Nguyen teaches <i>applying a policy on the valid path</i>	18
4. Petitioner fails to demonstrate that the prior art taught or suggested <i>applying the policy on another network path, in response to determining that the conditional rule is met</i> (limitation 1(f)/11(g)/12(h))	20

B. Ground 2: Petitioner Fails to Demonstrate that Calvo, Nguyen, and Datsenko Render Obvious Claims 8 and 19.....	23
IV. CONCLUSION.....	23

I. INTRODUCTION

Patent Owner Wiz, Inc. respectfully requests denial of *inter partes* review of the involved U.S. Patent No. 11,936,693 (“Reznik’693”). Petitioner Orca Security Ltd. has failed to demonstrate a reasonable likelihood that at least one of the claims challenged in the petition is unpatentable. 35 U.S.C. §324(a).

The petition fails to establish that the combination of Calvo and Nguyen teaches or suggests at least four separate limitations of Reznik’693. First, with respect to the claimed *actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network*,¹ Ground 1 of the petition relies solely on Nguyen as disclosing *active[] inspecti[on]*. Yet the petition does not allege that Nguyen, or any other grounds reference, teaches *actively inspecting the network path*, and Petitioner’s conclusory assertion that this would have been obvious lacks support in the cited evidence.

Second, Petitioner again relies on Nguyen as disclosing *storing an indicator to indicate that the network path is a valid path*. Yet, Nguyen never describes storing such an indicator. Rather Nguyen saves cyber security vulnerability

¹ For convenience, Wiz adopts Petitioner’s convention of denoting claim language with italics. Pet., 13 n.5.

information regarding specific cloud resources. Petitioner fails to establish why storing such information discloses storing an indicator to indicate that a network path is a valid path.

Third, the petition fails to demonstrate that the combination of references discloses *applying a policy on the valid path*. Petitioner's arguments on this point blur the distinctions between a *network path* and a *resource* and between a *policy* and a *mitigating action*. Petitioner's gap-filling attempt to sidestep the plain requirements of the claim is unsupported by either claim construction or the prior art disclosure.

Fourth, the petition fails to demonstrate that the prior art teaches *applying the policy on another network path*, specifically *in response to determining that the conditional rule is met*. For this limitation Petitioner relies on Calvo, in which the alleged *policy* is executed based on either a predetermined schedule or as a result of provisioning new resources. Calvo does **not** teach using the result of a conditional rule determination to trigger application of a policy on a subsequent network path. Petitioner fails to fill the gap between Calvo's teaching and that of the challenged Reznik'693 patent.

Finally, the second ground fails for similar reasons as it relies on the first ground for the limitations discussed above.

Accordingly, for the reasons detailed below, the Board should deny

institution of the petition.

II. CLAIM CONSTRUCTION

In an IPR, claims are given their ordinary and customary meaning in light of the specification. 37 CFR §42.100(b). No constructions are necessary to deny institution because denial is warranted for numerous reasons that do not depend on claim construction, as further detailed below.

III. ANALYSIS

A. Ground 1: Petitioner Fails to Demonstrate that Calvo and Nguyen Render Obvious Claims 1-7, 9-18, and 20-21

Ground 1 challenges claims 1-7, 9-18, and 20-21 and relies on Calvo in view of Nguyen. Pet., 12. The Board should reject this ground because of several flaws with Petitioner's arguments. First, the petition fails to allege, let alone show, that either Calvo or Nguyen discloses *actively inspecting the network path*, and the bald assertion that this would have been obvious despite prior art disclosure lacks corroboration. Second, Petitioner fails to demonstrate that the combination renders obvious *storing an indicator to indicate that the network path is a valid path*. Third, neither Calvo nor Nguyen disclose *applying a policy on the valid path* and the petition fails to establish that it would have been obvious to modify Calvo to apply such a policy to a path. Fourth, Petitioner fails to identify prior art disclosure of *applying the policy on another network path, in response to determining that the conditional rule is met*.

1. Petitioner fails to demonstrate that the prior art taught or suggested *actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network* (limitation 1(b)/11(c)/12(d))²

Independent claims 1, 11, and 12 each require *actively inspect[ing] the network path to determine if the network path of the reachable resource is accessible from the external network*. EX1001, claim 1, claim 11, claim 12.

Petitioner does not assert that either Calvo or Nguyen discloses *actively inspecting the network path* as claimed. Rather, Petitioner asserts that a POSITA would have understood this claim element to result from combining the teachings of the two references. However, neither Petitioner's cited expert testimony nor the non-grounds reference used to gap-fill the missing limitation supports Petitioner's contention.

First, Petitioner acknowledges that Calvo does not disclose active inspection. Pet. 22 ("Calvo does not expressly provide details for *active[] inspecti[on]* as described in Reznik'693 (i.e., Claim 1[b]))."). Petitioner therefore relies on Nguyen as purportedly "rendering obvious *active[] inspecti[on]* as claimed." *Id.*; *see also id.*, 27 ("These Nguyen disclosures also teach *active[] inspecti[on]* under

² Petitioner's labeling for the claim limitations is used in this preliminary response.

each party's proffered constructions.”).

Yet, Petitioner never alleges that Nguyen describes *actively inspecting the network path*. See Pet. 22-25. Rather, Petitioner's discussion of Nguyen identifies disclosure of “identif[ying] potential targets” (*id.* 24) and running a penetration test in which “[a] potential vulnerability is determined to be an actual vulnerability” (*Id.*, 25-26). Critically absent from Petitioner's Nguyen disclosure is any allegation that Nguyen actively inspects ***a network path***, let alone explanation as to how this might be understood in view of Nguyen's focus on target assessments.

Finally, after nearly eight pages of citation to the challenged Reznik'693 patent, Calvo, and Nguyen, Petitioner's limitation 1(b) theory becomes clear in a single sentence before transitioning to motivation to combine:

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)).

Pet. 28. Thus, petitioner's theory is not that either Calvo or Nguyen discloses *actively inspecting the network path* as claimed, but rather that this would have been obvious in their combination due to general knowledge of a POSITA, with citation to expert testimony and an exhibit that is not a grounds reference.

Petitioner’s gap-filling is a sign of improper hindsight, using the claims as a template. *KSR International v. Teleflex Inc.*, 550 U.S. 398, 421 (2007) (“A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.”).

What’s more, the cited evidence does not support Petitioner’s argument. Petitioner’s stated basis for arriving at the claim language despite lack of prior art disclosure is that “pen-testing (for example as disclosed by Nguyen) was known to inspect such *network paths* by traversing resource nodes.” Pet. 28 (citing EX1003, ¶51; EX1007). However, the cited expert testimony does not say this. Rather, the claim element in question is conspicuously absent. The paragraph reads: “And penetration testing of internal networks on ‘paths’ was known to be accomplished by traversing resource nodes.” That the testing might take place “on ‘paths’” does not mean that constitutes *inspecting the network path*. Petitioner’s expert provides no analysis to bridge the gap, nor does Petitioner explain the difference between its expert’s testimony and the assertion in the petition. Petitioner’s citation to EX1007 fares no better, as it is not a grounds reference and Petitioner’s expert makes no effort to establish that its disclosures universally apply to all penetration testing or to Nguyen specifically.

Because Petitioner fails to show that either Calvo or Nguyen discloses *actively inspecting the network path to determine if the network path of the*

reachable resource is accessible from the external network, and Petitioner’s argument that this would be obvious is conclusory and unsupported by the underlying evidence, the petition fails to demonstrate that Nguyen discloses limitation 1(b).³

2. Petitioner fails to demonstrate that the prior art taught or suggested *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* (limitation 1(c)/11(d)/12(e))

Independent claims 1 11, and 12 require *stor[ing] 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*. EX1001, claim 1, claim 11, claim 12. Petitioner acknowledges that Calvo does not disclose storing such an indicator. Pet., 33 (“Calvo also does not expressly explain *storing an indicator* in response to *active[] inspecti[on]*.”). Instead, Petitioner relies on the combination of Calvo and Nguyen to meet this limitation. *Id.* However, Nguyen discloses neither storing an indicator that a path is valid nor doing so in response to determining that the reachable resource is accessible from the external network. Petitioner’s

³ The petition relies on its limitation 1(b) analysis for elements 11(c) and 12(d), and the challenge to those independent claims should thus be rejected for the same reason. Pet., 58, 60.

inability to specifically identify how Nguyen teaches this limitation is particularly striking in view of its express concession that Calvo lacks it.

a. Neither Calvo nor Nguyen teaches *storing an indicator to indicate that the network path is a valid path*

Element 1(c) requires, in part, *storing an indicator to indicate that the network path is a valid path*. For this limitation, Petitioner relies solely on Nguyen because Calvo “does not expressly explain *storing an indicator* in response to *active[] inspecti[on][.]*” Pet., 33.

Petitioner acknowledges that Nguyen teaches storing “results obtained from performing tests on targets.” Pet., 33 (citing EX1005, 11:16-17). That is, Nguyen discloses storing indicators regarding specific resource or “target” vulnerabilities, not “valid path” indicators. Petitioner tries to stretch the disclosure to meet the claim language by contending that Nguyen “rules out ‘false positives or potential vulnerabilities that are not actual vulnerabilities’ (i.e., resources that are not really reachable).” Pet., 34. But here Petitioner gives no explanation of why a “false positive” indicates a “not really reachable” resource, nor does Petitioner explain why ruling out false positives would indicate a *valid path*. In fact, Nguyen provides an example of a “false positive” where a test engine repeatedly enters text on a web page (through a valid path) and the backend system receives the input and “reacts appropriately.” EX1005, 13:33-44.

Finally, Petitioner fails to explain why a POSITA would have been

motivated to utilize Nguyen’s teaching of storing active inspection results.

Petitioner states that “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.’” Pet., 35. But beyond a conclusory “common sense” rationale, Petitioner provides no reason why the results need to be stored in order to be useful, or why storing the results eliminates false positives. Petitioner does not address readily apparent alternatives such as immediately remediating vulnerabilities or alerting a user with the relevant vulnerability information. Petitioner omits necessary analysis and instead relies on alleged common sense to fill in the gaps.

Petitioner relies solely on Nguyen’s testing results as disclosing *storing an indicator to indicate that the network path is a valid path*, yet Nguyen never describes its results as indicating that a network path is valid and Petitioner fails to explain why it should be interpreted as such. Accordingly, the petition fails to demonstrate that Nguyen discloses limitation 1(c).⁴

⁴ The petition relies on its limitation 1(c) analysis for elements 11(d) and 12(e), and the challenge to those independent claims should thus be rejected for the same reason. Pet., 58, 60.

b. Neither Calvo nor Nguyen teach *in response to determining that the reachable resource is accessible from the external network*

Element 1(c) further requires that the storage described above is done *in response to determining that the reachable resource is accessible from the external network*. As discussed above, Petitioner relies solely on Nguyen for this limitation because Calvo “does not expressly explain *storing an indicator* in response to *active[] inspecti[on][.]*” Pet., 33.

Here, Petitioner mistakenly equates storing an indicator “in response to *active[] inspecti[on]*,” with storing an indicator “*in response to determining that the reachable resource is accessible from the external network*.” Pet., 33; EX1001, claim 1. Importantly, the claim requires storing a specific indicator (that of a valid path) in response to a specific determination (that the resource is accessible from the external network).

For this limitation, Petitioner points to Nguyen’s disclosure of storing test results but provides no explanation as to how Nguyen might teach doing so in response to a specific determination of accessibility from the external network. Pet., 33. Petitioner quotes several passages of Nguyen, none of which disclose such a teaching. Pet., 33-34; EX1005, 11:16-17 (“vulnerabilities database 380 [] stores results obtained from performing tests on targets”), 16:12-13 (“The test results 390 may identify one or more actual vulnerability”), 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)”). In fact, these passages from Nguyen teach storage of test results “in response to the executed tests” themselves. That is, Nguyen teaches storage of test results **regardless** of the testing outcome or contents of those results. Petitioner does not, and cannot, explain how this disclosure maps to the limitation 1(c), which requires storage of results *in response to determining ... that the reachable resource is accessible*.

Because Petitioner relies solely on Nguyen’s storing of vulnerability testing results without explaining how such storage is *in response to determining that the reachable resource is accessible from the external network*, the petition further

fails to demonstrate that Nguyen discloses limitation 1(c).⁵

3. Petitioner fails to demonstrate that the prior art taught or suggested *applying a policy on the valid path, wherein the policy includes a conditional rule* (limitation 1(d)/11(e)/12(f))

Independent claims 1, 11, and 12 require *apply[ing] a policy on the valid path, wherein the policy includes a conditional rule*. EX1001, claim 1, claim 11, claim 12. For this limitation Petitioner relies on the combination of Calvo and Nguyen. Pet., 36. However, the combination discloses neither applying a policy on a network path nor doing so on a valid network path. Petitioner therefore fails to demonstrate that the combination of Calvo and Nguyen teaches this limitation.

a. Petitioner acknowledges that a “*network path*” is a connection of two or more security objects

Element 1(d) requires in part that the policy is applied on a *valid path* which is a type of network path. The challenged Reznik’693 patent explains that a network path is “a connection of two or more security objects accessible from an external or internal network, and/or an external or internal object.” EX1001, 12:46-48. That is, a network path is a connection (or series of connections) between **two**

⁵ The petition relies on its limitation 1(c) analysis for elements 11(d) and 12(e), and the challenge to those independent claims should thus be rejected for the same reason. Pet., 58, 60.

or more security objects.

Petitioner acknowledges this definition while discussing element 1(a). Pet., 16. Petitioner, quoting its own expert, goes on to state that a POSITA would have understood “‘a network path to be merely a connection of two or more resource nodes in a computing network, including in or partially in a cloud network’ or in other words ‘a node-by-node specification of a link between two machines.’” *Id.*, 17 (citing EX1003 (Easttom Dec.), ¶¶ 39-43). Thus, Petitioner agrees that element 1(d) requires a policy applied to a set of two or more security objects / resource nodes, i.e. a network path.

b. Neither Calvo nor Nguyen teaches applying a policy on the [] path

Petitioner fails to demonstrate that Calvo teaches *applying a policy on the [] path* where the path is two or more security objects as defined by the patent and Petitioner. Pet., 36-39.

Petitioner relies on the idea that Calvo teaches applying “compliance packs.” *Id.*, 37. Importantly, Petitioner contends that these packs “can be evaluated to determine the policy compliance of **a resource**.” *Id.* (emphasis added). Petitioner fails to make any showing that Calvo teaches applying a policy on a network path as defined in Reznik’693. That is, applying a policy on a connection of **two or more** security objects.

This failure is exemplified by Petitioner’s cited example from Calvo in

which: “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.” Pet., 37; EX1004, 6:35-39. As this highlights, even if Calvo’s compliance packs are considered a policy, Calvo only teaches applying that policy on a specific resource or group of resources, not the path between resources. This is also shown in FIG. 2B at step 225.

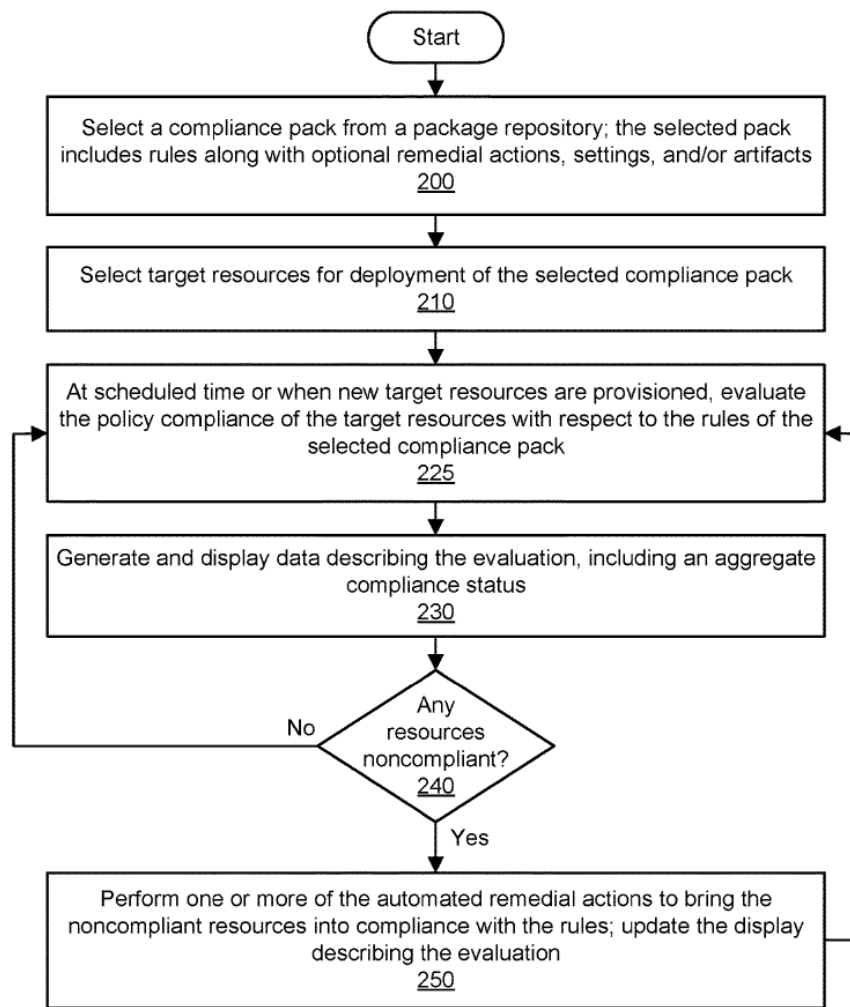


FIG. 2B

EX1004, FIG. 2B.

Calvo states that “[a]s shown in 225, for each of the *target resources*, the method may perform rule evaluation for all the rules in the compliance pack repeatedly at appropriate times.” EX1004, 10:67-11:2 (emphasis added). In this way, Calvo does not teach applying a policy on network paths, but rather applying “compliance packs to cloud-based resources to determine the policy compliance of

those **resources**.” EX1004 (Calvo), 2:64-3:1 (emphasis added). Unable to avoid this deficiency, Petitioner conflates FIG. 2B step 225 (“evaluate the policy compliance of the target resources”) and step 250 (“bring the noncompliant resources into compliance with the rules”). Petitioner does this in two steps.

First, Petitioner claims that “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.” Pet., 38 (emphasis added). But Petitioner fails to explain its modification of the claim language, i.e., explain why applying a policy on “part of” a network path (i.e. a single resource) teaches applying a policy on the path as claimed.

Petitioner then argues that because an instruction such as closing a port (i.e. a mitigation action) would be applied on a resource, the claimed *policy* must likewise be applied to a resource rather than a network path as claimed. Pet., 39. To support this misunderstanding, Petitioner contends:

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 POSITA 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).

Pet., 39 (citing EX1003 ¶ 119). Petitioner here reasons that because communication channels cannot execute instructions, they cannot have policies applied to them except indirectly via a resource. But this is contrary to the claims of Reznik’693 where a policy is applied to a valid path but mitigation actions are applied without restriction to a particular type of subject. *Compare* claim limitation 1(d) *with* limitation 1(e); *see also* EX1001, 3:11-12 (“initiating the mitigation action on the reachable resource”), 22:51-56 (“[T]he mitigation action includes generating a policy exemption ... [or] closing a port of the reachable resource.”). Petitioner cannot sidestep the literal claim language merely by identifying a purported *policy* in the prior art that it alleges cannot be applied to connections between nodes.

Dr. Easttom puts it slightly differently but still runs into the same issue. He states:

A POSITA would have understood that applying compliance rules (for example, to restrict external network access) would be applied on

nodes (i.e., resources) of a network because the nodes represent computing objects. Computing objects are the features in a network which can execute instructions. And the path is made up of a connection of resources. Instructions cannot be applied on simply the vertices between resource nodes. Rather, instructions are applied on the nodes to restrict aspects of network access.

EX1003, ¶ 119. This again confuses two separate elements of Reznik’693’s claims. Element 1(d) requires the application of a policy on a valid network path, while element 1(e) requires the initiation of a mitigation action (which may be applied to an individual resource). Petitioner does not explain why the “instructions” discussed by Petitioner and Dr. Easttom are a “policy” rather than a “mitigation action.” Petitioner provides no support for the idea that because mitigation actions may be applied at the resource level, policies are applied at the resource level as well, nor does Petitioner reconcile its assertions with claim elements 1(d) and 1(e).

Because Petitioner relies solely on Calvo’s application of a policy on an individual resource and Petitioners fail to explain why it should be interpreted as satisfying the claim requirement of applying a policy on a network path, the petition fails to demonstrate that Calvo discloses limitation 1(d).

c. Neither Calvo nor Nguyen teaches *applying a policy on the valid path*

Petitioner additionally fails to demonstrate that Calvo teaches *applying a policy on the valid path* where the path is found to be **valid**. Pet., 36-39.

Petitioner’s discussion of element 1(d) consistently ignores the limitation requiring the policy to be applied to a *valid path*. *Id.* The entirety of Petitioner’s discussion of this limitation is “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.” Pet., 39. This discussion is deficient and does not establish that the combination meets this limitation.

As discussed above with respect to element 1(c) (*supra*, §II.A.2.a), neither Calvo nor Nguyen disclose storing an indicator that a path is a valid path. For the same reasons, neither does the combination of Calvo and Nguyen teach applying a policy on a valid path. That is, the path itself has not been validated.

Further, even if Nguyen did teach storing an indicator that the network path is a valid path, Petitioner does not explain how Calvo teaches applying a policy on paths that have been found to be valid. Rather, as Petitioner stated, Calvo teaches applying compliance packs to whichever resources a user selects. Pet., 37-38. This omits a critical aspect of the claim.

Because Petitioner relies solely on Nguyen for teaching that a path is valid and Petitioner fails to explain why Calvo’s application of compliance packs on user-selected resources should be interpreted as application to a valid path, the petition fails to demonstrate that the combination of Calvo and Nguyen discloses

limitation 1(d).⁶

4. Petitioner fails to demonstrate that the prior art taught or suggested *applying the policy on another network path, in response to determining that the conditional rule is met* (limitation 1(f)/11(g)/12(h))

Independent claims 1, 11, and 12 require *applying the policy on another network path, in response to determining that the conditional rule is met*. EX1001, claim 1, claim 11, claim 12. For this limitation Petitioner relies on the teaching of Calvo. Pet., 42. However, Calvo does not teach that a subsequent application of the policy on another network path is *in response to determining that the conditional rule is met*. The claim language requires that the subsequent application of the policy on another network path is based on the results of the current application of the policy. In contrast, Calvo teaches applying a compliance pack (which Petitioner maps to the claimed *policy*) on all selected resources, regardless of any determination as to compliance with a rule. Calvo also teaches that any future application of the compliance pack is based on a scheduled time or the provisioning of a new resource.

⁶ The petition relies on its limitation 1(d) analysis for elements 11(e) and 12(f), and the challenge to those independent claims should thus be rejected for the same reasons. Pet., 58, 61.

Calvo's Figure 2B shows that the compliance pack is applied to all selected resources, regardless of outcome, in multiple ways.

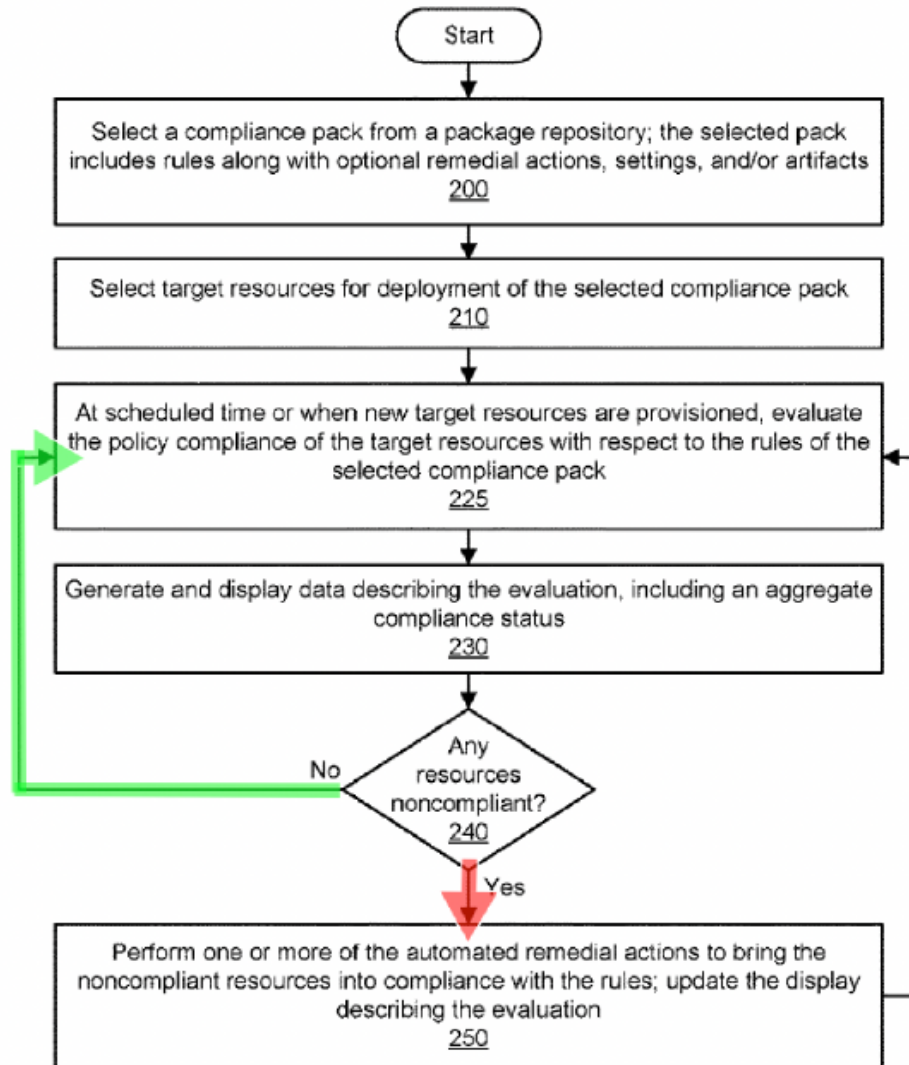


FIG. 2B

Pet., 45 (citing annotated EX1004, FIG. 2B).

As shown at step 210 in figure 2B a user “select[s] target *resources* for deployment of the selected compliance pack[.]” EX1004, FIG. 2B. Then, at step 225, Calvo teaches “evaluat[ing] the policy compliance of the ***target resources***

with respect to the rules of the selected compliance pack[.]” EX1004, FIG. 2B (emphasis added). Here Calvo evaluates the policy on ***all selected resources***. It is not until step 240 that Calvo asks if “any of the resources are noncompliant[.]” *Id.* In other words, all resources are evaluated, regardless of the compliance of any other resource.

Petitioner’s description of FIG. 2B misstates how the policy is applied to another network path. Petitioner states that the flow chart shows that “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*[.]” Pet., 46. But as FIG. 2B shows, if multiple resources were selected they are all evaluated at step 225, before the flowchart reaches step 240. EX1004, FIG. 2B

Even in a case where the flowchart reaches step 240 and follows the “no” path back to step 225, no subsequent application of the policy is triggered based on this determination. Instead, Calvo teaches that the application of the policy on another resource is based on a “scheduled time” or “when new target resources are provisioned[.]” EX1004, FIG. 2B. Neither of these triggering events is “in response to determining that the conditional rule is met,” as required by the claim.

Petitioner relies solely on Calvo’s teaching of continuous compliance as disclosing “applying the policy on another network path, in response to

determining that the conditional rule is met,” yet Calvo teaches only evaluating the alleged policy on all selected resources and triggering subsequent evaluations based on a schedule or the provisioning of a new resource. Thus, the petition fails to demonstrate that Calvo discloses limitation 1(f).⁷

B. Ground 2: Petitioner Fails to Demonstrate that Calvo, Nguyen, and Datsenko Render Obvious Claims 8 and 19

Ground 2 challenges claims 8 and 19 in view of the combination of “Calvo, Nguyen and Datsenko.” Pet., 63. Petitioner’s argument for this ground relies explicitly on the same analysis for claim 1 in Ground 1 and therefore fails for the same reasons discussed above. Pet., 63; *supra* §A.

IV. CONCLUSION

Petitioner has failed to make a facial case of unpatentability for any challenged claim, so institution is unwarranted and should be denied.

Respectfully submitted,

Date: September 26, 2025

/ Matthew A. Argenti /
Matthew A. Argenti
Reg. No. 61,836
Counsel for Wiz, Inc.

⁷ The petition relies on its limitation 1(f) analysis for elements 11(g) and 12(h), and the challenge to those independent claims should thus be rejected for the same reason. Pet., 58, 61.

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

I certify the word count for this reply is 4628 words, excluding any table of contents, table of authorities, mandatory notices, certificate of service or word count, and appendix of exhibits or claim listing.

Date: September 26, 2025

/ Matthew A. Argenti /
Matthew A. Argenti
Reg. No. 61,836
Counsel for Wiz, Inc.

CERTIFICATE OF SERVICE

I certify a true and correct copy of this paper was served today to the email correspondence addresses of the patent owner as follows:

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

Respectfully submitted,

Date: September 26, 2025

/ Matthew A. Argenti /
Matthew A. Argenti
Reg. No. 61,836
Counsel for Wiz, Inc.