

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-00864
Patent 11,663,032 B2

Before MICHAEL R. ZECHER, GARTH D. BAER, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

BAER, *Administrative Patent Judge*.

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

I. INTRODUCTION

Petitioner, Wiz, Inc., filed a Petition requesting an *inter partes* review (“IPR”) of claims 1–25 of U.S. Patent No. 11,663,032 B2 (Ex. 1001, “the ’032 patent”). Paper 2 (“Pet.”). Patent Owner, Orca Security Ltd., filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). Based on the authority delegated to us by the Director under 37 C.F.R. § 42.4(a), we may not institute an IPR unless the information presented in the Petition and any preliminary response thereto shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Taking into account Patent Owner’s Preliminary Response, we conclude that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail in demonstrating at least one of claims 1–25 of the ’032 patent is unpatentable. Pursuant to § 314, we hereby institute an IPR as to these claims of the ’032 patent.

A. *Real Party in Interest (“RPI”)*

Petitioner identifies itself as an RPI. Pet. 1. Patent Owner identifies itself as an RPI. Paper 3 (Patent Owner’s Mandatory Notices), 1.

B. *Related Matters*

The parties indicate that the ’032 patent is the subject of a district court case titled *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23-cv-00758 (D. Del. filed July 12, 2023) (“Delaware Action”). Pet. 2; Paper 3, 1.

C. *The ’032 Patent*

The ’032 patent generally relates to “cyber-security systems and, more specifically, to techniques for securing virtual machines.” Ex. 1001, 1:17–

19. According to the '032 patent, organizations like Amazon, Microsoft, and Google “have increasingly adapted their applications to be run from multiple cloud computing platforms.” *Id.* at 1:23–26. “Virtualization [plays] a key role in a cloud computing” by “allowing multiple applications and users to share the same cloud computing infrastructure.” *Id.* at 1:27–29. This is accomplished by using “virtual machines [VMs]” that “emulate[] a number of ‘computers’ or instances, all within a single physical device.” *Id.* at 1:32–33. The '032 patent states that “virtual machines running on top of virtualization technologies are . . . vulnerable to some cyber threats,” but that “[p]rotection of a cloud computing infrastructure, and particularly of virtual machines can be achieved via inspection of traffic.” *Id.* at 1:39–49.

Conventionally, traffic inspection may be accomplished by “a network device connected between a client and a server . . . hosting virtual machines,” “a network scanner deployed out of path,” “a traffic monitor that listens to traffic flows between clients and the server,” or by using “vulnerability management and security assessment solutions . . . based on agents installed in each server in a cloud computing platform.” *Id.* at 1:49–2:9. The '032 patent, however, explains how there are certain disadvantages associated with each of these conventional ways of traffic inspection. *Id.*

The '032 patent ostensibly addresses these disadvantages by providing a method for “securing virtual cloud assets in a cloud computing environment against cyber threats.” Ex. 1001, 2:61–62. Figure 1B of the '032 patent, reproduced below, illustrates a network diagram that implements various embodiments. *Id.* at 3:14–15.

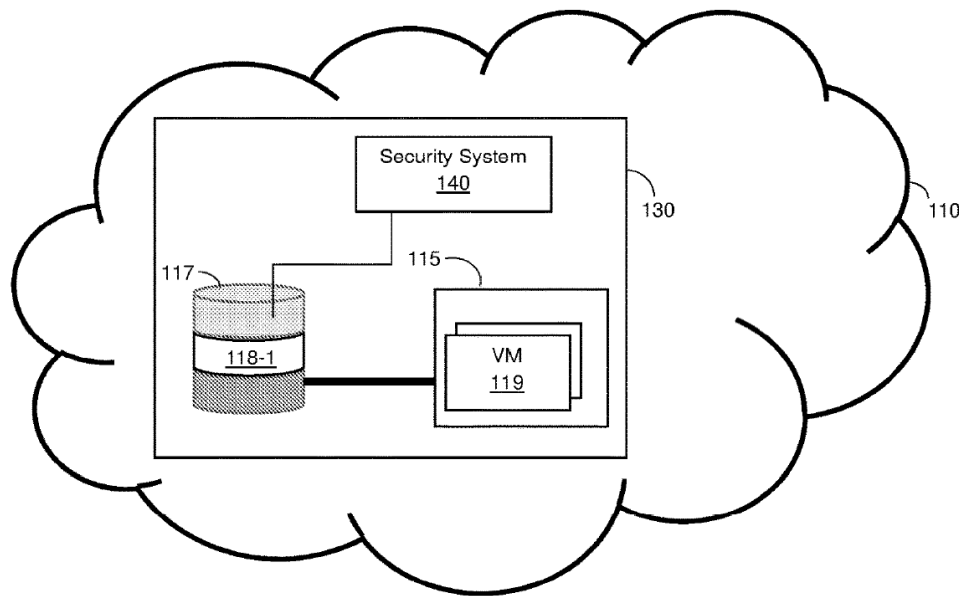


FIG. 1B

Figure 1B illustrates cloud computing platform 110 that includes client environment 130 with storage 117 containing virtual disk 118-1, server 115 hosting virtual machine 119, and security system 140. *Id.* at 3:35–4:23.

“[S]ecurity system 140 is configured to detect vulnerabilities and other cyber threats related to the execution [of] VM 119.” *Id.* at 4:45–47. More specifically, “security system 140 can scan and detect vulnerable software, non-secure configurations, exploitation attempts, compromised assets, data leaks, data mining, and so on,” as well as “provide security services, such as incident response, anti-ransomware, and cyber insurance by accessing the security posture.” *Id.* at 4:51–56.

D. Challenged Claims

Of the challenged claims, claims 1, 18, and 22 are independent. Independent claim 1 is illustrative of the challenged claims and is reproduced below.

1. A method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising:

[1.1] determining, using an [application programming interface ('API')] or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment;

[1.2] accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk;

[1.3] analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;

[1.4] determining, based on the matching, an existence of potential cyber vulnerabilities of the protected virtual cloud asset;

[1.5] determining whether the matching installed applications are used by the protected virtual cloud asset;

[1.6] prioritizing the potential cyber vulnerabilities based on the use determinations; and

[1.7] reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.

Id. at 9:37–60 (Petitioner’s element numbering added).

E. Asserted Prior Art References

Petitioner relies on the following prior art references:

Name¹	Reference	Dates	Exhibit No.
Veselov	US 11,216,563 B1	issued Jan 4, 2022; filed May 19, 2017	1007
Hufsmith	US 2020/0097662 A2	published Mar. 26, 2020; filed Sept. 28, 2018	1078
Hutchins	US 2013/0024940 A1	published Jan. 24, 2013; filed Sept. 20, 2012	1070

F. Asserted Grounds of Unpatentability

Petitioner challenges claims 1–25 of the '032 patent based on the asserted grounds of unpatentability set forth in the table below. Pet. 3, 20–72.

Claim(s) Challenged	35 U.S.C. §	References/Basis
1–11, 13–25	103 ²	Veselov, Hufsmith
12	103	Veselov, Hufsmith, Hutchins,

II. DISCUSSION

A. Discretionary Denial under § 314(a)

Patent Owner contends that we should exercise our discretion to deny the Petition under § 314(a) because “the overall balance of the *Fintiv* factors

¹ For clarity and ease of reference, we only list the first named inventor.

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the challenged patent claims the benefit of an application filed after this date, the post-AIA version of § 103 applies. Ex. 1001, code (60).

shows that ‘efficiency, fairness, and the merits support the exercise of authority to deny institution.’” Prelim. Resp. 45 (quoting *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 6 (PTAB Mar. 20, 2020) (Order Authorizing Supplemental Briefing on Discretionary Denial) (precedential). After Patent Owner filed its Preliminary Response, however, Petitioner filed a stipulation consistent with the stipulation filed in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (Decision Granting Institution) (precedential as to § II.A) (“*Sotera*”). Ex. 1083.

On June 21, 2022, the Director issued interim guidance in the form of a memo that further clarifies how we should approach analyzing the *Fintiv* factors. See Interim Procedure for Discretionary Denials in AIA Post-grant Proceedings with Parallel District Court Litigation, *available at* https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf. Notably, the Director stated that “the [Patent Trial and Appeal Board (‘PTAB’)] will not discretionarily deny institution in view of parallel district court litigation where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any ground that could have been reasonably raised before the PTAB.” *Id.* With this interim guidance in mind, we decline to exercise our discretion to deny institution of this proceeding under *Fintiv* because Petitioner filed a *Sotera* stipulation. Ex. 1083.

B. Discretionary Denial under § 325(d)

Patent Owner contends we should deny institution under 35 U.S.C. § 325(d) because “the same or substantially the same prior art . . . was previously were presented to the Patent Office.” Prelim. Resp. 53.

Specifically, Patent Owner explains, the Office previously considered Veselov during the '032 patent's prosecution. *Id.* (citing Ex. 1004, 108, 133³). For the reasons below, we are not persuaded to exercise our discretion to deny the Petition based on § 325(d).

In evaluating arguments under § 325(d), we use a two-part framework: (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of the first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8 (PTAB Feb. 13, 2020) (precedential).

Patent Owner does not dispute that Veselov is the only reference that serves as the basis of Petitioner's obviousness grounds that was considered during prosecution of the '032 patent. *See* Prelim. Resp. 53; *see also* Ex. 1004, 59–62, 84–91. The Examiner, however, did not meaningfully address Veselov during prosecution of the '032 patent. Stated differently, the Examiner did not apply the teachings of Veselov to teach or suggest the limitations of the originally presented claims of the '032 patent. It is also undisputed that the Examiner did not consider the other references that serve as the basis of Petitioner's asserted obviousness grounds (i.e., Hufsmith and

³ All references to the page numbers in the prosecution history of the '032 patent refer to the page numbers inserted by Petitioner in the bottom, right-hand corner of each page in Exhibit 1004.

Hutchins) during prosecution. Nor did the Examiner have the benefit of Dr. Stavrou's testimony regarding the teachings of Petitioner's three asserted references. Accordingly, we are not persuaded by Petitioner's arguments that the Petition presents substantially the same art and arguments that were considered previously during prosecution of the '032 patent.

C. Claim Construction

Independent claims 11, 18, and 22 each require “analyz[ing] the snapshot.” Petitioner proposes we construe this term to encompass two alternative approaches: (1) “direct analysis of the snapshot data”; and (2) “analysis of a VM instantiated from the snapshot.” *See* Pet. 10. Patent Owner disputes the second approach, but not the former. *See* Prelim. Resp. 9–11. For purposes of institution, we agree with Petitioner's first alternative approach “analyz[ing] the snapshot” encompasses “direct analysis of the snapshot data.” This construction finds support in the specification of the '032 patent. *See e.g.*, Ex. 1001, 5:20–21 (“The snapshot is parsed and analyzed by the security system 140 to detect vulnerabilities.”), 5:37–40 (“[T]he security system 140 may be configured to match the application files, either directly (using binary comparison) or by computing a cryptographic hash against [a] database of files in vulnerable applications.”). Because, as we explain below, Petitioner's obviousness analysis is sufficient under this first approach, we take no position on Petitioner's second alternative approach, which Patent Owner disputes. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

Although Petitioner submits an additional term for construction, *see* Pet. 8–9, we do not need to further construe the claims to determine whether to institute IPR. *See Nidec Motor Corp.* 868 F.3d at 1017.

D. Level of Skill in the Art

Relying on the testimony of its declarant, Dr. Angelos Stavrou, Petitioner argues the following:

[a person of ordinary skill in the art] as of January 2019 would have held at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and would also have 2-3 years of professional experience working with cyber security analysis and virtualization. Additional experience could compensate for less education and vice versa. Relevant work experience includes, for example, malware analysis, security analysis of cloud computing systems, and security analysis of virtual machines.

Pet. 7–8 (citing Ex. 1002 ¶¶ 21, 22).

Patent Owner offers essentially the same assessment of the level of skill in the art as Petitioner, arguing the following:

[a person of ordinary skill in the art] as of the ’032 patent’s earliest priority date (January 28, 2019), would have had at least a Bachelor’s degree in computer science, computer engineering, or a related field, and two years of industry experience or academic research experience in cyber security and virtualization, including cloud computing cybersecurity. Additional education can compensate for less experience and vice-versa.

Prelim. Resp. 9 (citing Ex. 2001 ¶¶ 1–12, 19–26).

We do not discern a material difference between the assessments of the level of skill in the art advanced by either party, nor does either party premise its arguments exclusively on its own assessment. For purposes of institution, we adopt Petitioner’s assessment, except that we delete the

qualifier “at least” to eliminate vagueness as to the appropriate level of education. The qualifier expands the range without an upper bound (i.e., encompassing a Ph.D. degree and beyond), and does not meaningfully indicate the level of skill in the art. Petitioner’s assessment—without the qualifier—is supported by the testimony of Dr. Stavrou and it is consistent with the ’032 patent and the asserted prior art. We note, however, that our obviousness analysis would be the same under each party’s assessment.

E. Description of Primary Prior Art References

1. Veselov (Ex. 1007)

Veselov generally relates to “a scanning system and associated method for performing security assessments on virtualized reproductions of the computing resource(s) that is/are the target of the security assessment.” Ex. 1007, 3:20–23. According to Veselov, “the scanning system obtains, or obtains access to, a state of the resource at a point in time (e.g., a ‘snapshot’) prior to, or in conjunction with, initiating the security assessment.” *Id.* at 3:23–27. “The snapshot may” include “a copy of the state of memory, the state of any device (virtual or physical) allocated to the resource, block-level image of the entire logical volume; or . . . an image of only a portion of the logical volume containing the data required to embody an exact copy of the virtual machine instance; or . . . a copy of certain files of the target computing resource.” *Id.* at 3:32–40.

Figure 2 of Veselov, reproduced below, illustrates “a flow diagram of an example method for executing the security assessment of one or more virtual machines in [a] virtual computing environment.” Ex. 1007, 1:61–63; *see also id.* at 2:64–67 (stating that an example of “a distributed computing environment” is “a ‘cloud’ computing environment”).

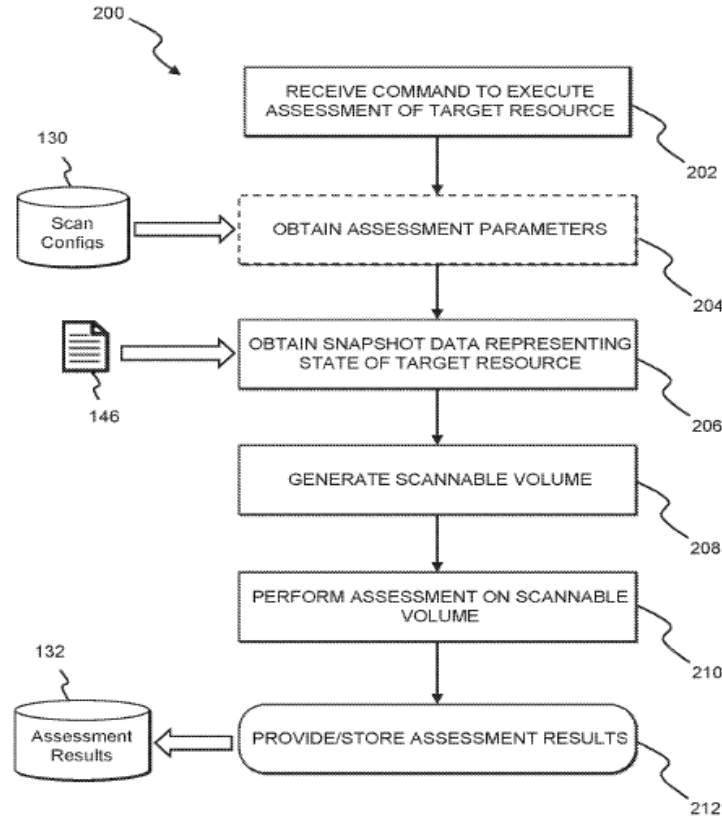


FIG. 2

Figure 2 illustrates process 200 that begins at step 202 where “the scanning service may receive a signal to execute a security assessment of the target resource.” *Id.* at 8:62–64. “At step 204, the scanning service may optionally obtain scan data describing the parameters of the security assessment to be performed.” *Id.* at 9:9–11. “At step 206, the scanning service may obtain snapshot data representing the state of the target resource at the time the snapshot was captured.” *Id.* at 9:14–16. “At step 208, the scanning service may generate a scannable volume, or cause a scannable volume to be generated, based at least in part on the snapshot data.” *Id.* at 10:1–3. One example of generating a scannable volume includes “launching a duplicate virtual machine instance in an allocated logical volume.” *Id.* at

10:9–16. “At step 210, the scanning service may perform the security assessment on the scannable volume.” *Id.* at 10:17–18. “At step 212, the scanning service may associate the assessment results with the target resource . . . and then may take various actions on the assessment results,” including “if vulnerabilities are identified in the assessment results, comparing the assessment results to a remediation framework to identify one or more actions the user can take to address the vulnerabilities.” *Id.* at 10:24–36.

2. *Hufsmith (Ex. 1078)*

Hufsmith generally relates to “tooling for software development related to distributed applications and, more specifically, to techniques that combine metrics of heterogeneous vulnerability scans of container images.” Ex. 1078 ¶ 2. Although Hufsmith primarily focuses on containers, it also discloses that “some implementations may include one or more containers executed within a virtual machine, which may be one of several virtual machines on a given computing device.” *Id.* ¶ 26; *see also id.* ¶ 149 (“The present techniques . . . are, in many cases, described with reference to containers, but it should be emphasized that the present techniques are applicable to other forms of encapsulated functionality, including virtual machine images.”). Hufsmith employs “scanner applications [that] may instantiate an intermediate container image and execute code of the intermediate container image, or execute code of an application therein, to dynamically test the body of code for vulnerabilities.” *Id.* ¶ 83.

Hufsmith also discloses a results engine that “may calculate a combined threat score (e.g., single score, [such as] a one-dimensional, cardinal or ordinal value with three, five, ten, a hundred or more possible values in a scoring range from a maximum to a minimum) for a container image.” Ex. 1078 ¶ 91, Figs. 1A, 1B (results engine 54). “The combined threat score may be based on a weighted sum of detected potential vulnerabilities,” where “[d]ifferent detected potential vulnerabilities may have different weights corresponding to different vulnerabilities or types of vulnerabilities in a taxonomy of vulnerabilities.” *Id.*

III. OBVIOUSNESS ANALYSIS

A. Ground 1: Obviousness based on Veselov and Hufsmith

Petitioner contends that claims 1–11 and 13–25 are unpatentable under 35 U.S.C. § 103 as obvious over Veselov and Hufsmith. Pet. 20–69. Based on the present record and for the reasons explained below, we determine that Petitioner has demonstrated a reasonable likelihood of success in demonstrating that at least one of claims 1–11 and 13–25 would have been obvious over Veselov and Hufsmith.

1. Petitioner’s Proposed Combination of Veselov and Hufsmith

Petitioner asserts Veselov’s scanning system that obtains/accesses ““a state of the resource at a point in time (e.g., a **“snapshot”**)”” teaches the first two claim elements requiring determining a snapshot’s location and accessing the snapshot. Pet. 26 (quoting Ex. 1007 3:20–27); *see id.* at 26–33. Petitioner further relies on Veselov’s service that “obtain[s] and **analyze[s] snapshot data** 146” using Common Vulnerabilities and Exposures (CVE) analysis for teaching the claimed “analyzing the snapshot.” *Id.* at 33; *see id.* at 34–35.

Petitioner relies on Hufsmith for teaching analyzing the snapshot “by matching installed applications with applications on a known list of vulnerable applications,” as well as “determining whether the matching installed applications are used by the protected virtual cloud asset.” Hufsmith teaches these steps, Petitioner explains, because it discusses comparisons with CVE and malware repositories to determine potential cyber vulnerabilities. Pet. 34–37. Hufsmith also teaches “determining whether the matching installed applications are used by the protected virtual cloud asset,” and prioritizing cyber vulnerabilities based on those determinations, because Hufsmith adjusts threat levels based on whether the associated file/code is dormant or active. Pet. 37–41. Last, Petitioner asserts that, together, Veselov and Hufsmith teach the claimed reporting the cyber vulnerabilities as prioritized alerts because Veselov’s teaches reporting assessment results, whereas Hufsmith teaches scoring information and weights for vulnerabilities. *Id.* at 41–43.

Citing relevant support from Hufsmith and its declarant, Dr. Stavrou, Petitioner contends that a skilled artisan would have been motivated to combine Veselov’s and Hufsmith’s teachings because “Veselov provides a high-level description of CVE analysis and alert reporting, while Hufsmith provides further details that are directly applicable to Veselov’s approach.” Pet. 22. In addition, Petitioner explains that skilled artisans would have been motivated to employ Hufsmith’s prioritized alerts in Veselov’s system because “these common techniques facilitated rapid identification of higher-priority assets/risks and mitigated alert fatigue.” *Id.* at 22.

Beyond the independent claims, Petitioner asserts that Veselov and Hufsmith teach the additional limitations in dependent claims 2–11, 13–17,

19–21, and 23–25 including determining whether matching installed applications are not in use (claim 2), checking/verifying configuration files, access times, and application/system logs (claims 3, 4, 5, and 10), reporting vulnerabilities to a user console (claim 6), matching application files against a known list of vulnerable applications (claims 7 and 19), computing/matching a cryptographic hash (claim 8) parsing the snapshot (claim 9), mitigating vulnerabilities (claim 11), determining a virtual disk (claim 13), taking a new snapshot (claims 14, 15, 23, and 24), querying for a snapshot’s location (claim 16 and 20), and making/analyzing a copy a snapshot (claims 17, 21, and 25). Pet 43–69.

Patent Owner challenges several aspects of Petitioner’s obviousness challenge. We address those issues below.

2. *Whether Hufsmith is Analogous Art*

Patent Owner asserts that Petitioner’s rationale for combining Veselov and Hufsmith is flawed because Hufsmith is not in the same field of endeavor and, thus, is not analogous art to the ’032 patent. Prelim. Resp. 24–29. According to Patent Owner, the ’032 patent is directed, “‘specifically, to techniques for securing virtual machines’ that involve, *inter alia*, determining ‘a location of a snapshot of at least one virtual disk of a protected virtual cloud asset,’ accessing, based on the determined location, the ‘snapshot of the at least one virtual disk,’ and analyzing the ‘snapshot of the at least one virtual disk’ to determine vulnerabilities that can be reported as ‘prioritized alerts.’” *Id.* at 25 (quoting Ex. 1001). In contrast, Patent Owner argues that Hufsmith “is directed to ‘tooling for software development related to distributed applications and, more specifically, to techniques that combine metrics of heterogeneous vulnerability scans of

container images.” *Id.* at 25–26 (quoting Ex. 1078). Patent Owner further argues that Hufsmith “does not mention snapshots, analyzing snapshots of virtual disks, or using snapshot-based analyses of virtual disks to secure VMs.” *Id.* at 26.

We preliminarily disagree. The U.S. Court of Appeals for the Federal Circuit has explained that “the field-of-end endeavor test does not look to the problem that the patent purports to address,” and is also “not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field.” *Netflix, Inc. v. DivX LLC*, 80 F.4th 1352, 1359 (Fed. Cir. 2023). At this stage in the proceeding, Petitioner has presented sufficient evidence that Hufsmith is analogous art to the ’032 patent because both are directed to the same field of endeavor of security analysis for virtual resources to detect and report security issues. *See* Pet. 20. The ’032 patent generally relates to “cyber-security systems and, more specifically, to techniques for securing virtual machines.” Ex. 1001, 1:14–16. Similarly, Hufsmith generally relates to “techniques that combine metrics of heterogeneous vulnerability scans of container images.” Ex. 1078 ¶ 2. Hufsmith makes clear that its “[scanning] techniques are applicable to . . . virtual machine images.” *Id.* ¶ 149.

Moreover, even if we were to agree with Patent Owner that the field of endeavor of the ’032 patent should be limited to the particular focus of “snapshot-based analyses to secure VMs,” Hufsmith would likely still qualify as analogous art within that same field of endeavor. *See* Prelim. Resp. 25. Hufsmith discloses that its controller 42 can “scan a container image . . . by streaming a copy of the container image” *Id.* ¶ 69; *see also id.* ¶¶ 68, 55 (disclosing that “[c]ontainers may run within a virtual machine”).

In our view, Hufsmith's copy of the container image running within a VM amounts to a snapshot because it is nothing more than a copy of the container image within a VM at a given point in time. With this in mind, we view Hufsmith's controller 42 as capable of receiving a request to scan a VM by streaming a copy of the VM image. *See id.* ¶¶ 55, 69, 149. Consequently, even if the '032 patent's field of endeavor were limited to snapshot-based analyses to secure VMs, Hufsmith would likely still be directed to the same field of endeavor because it contemplates analyzing copies of VM images to secure VMs.

3. Petitioner's Rationale for Combining Veselov and Hufsmith

Patent Owner asserts that Petitioner's rationale for combining Veselov and Hufsmith is flawed because Veselov discloses performing analysis on snapshot data, whereas Hufsmith performs analysis on images Prelim. Resp. 31–32. In addition, Patent Owner asserts Petitioner does not meet its burden of demonstrating that there is a reasonable expectation of success in combining the teachings of Veselov and Hufsmith. *Id.* at 34–35. We preliminarily disagree.

As noted above, Petitioner explains that a skilled artisan would have been motivated to combine Hufsmith's security assessment technique with Veselov's security assessment system because Hufsmith provides further details that are directly applicable to Veselov's approach and Hufsmith's prioritized alerts facilitated rapid identification of higher-priority assets/risks and mitigated alert fatigue. Pet. 22–23. With this rationale, Petitioner has articulated sufficient reasoning with rational underpinning to support the legal conclusion that its proffered combination would have been obvious to one skilled in the art. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418

(2007). Patent Owner’s argument highlighting differences between Veselov and Hufsmith—i.e., Veselov’s snapshot analysis versus Hufsmith’s image analysis—does not undermine Petitioner’s proffered rationale and does not persuade us at this stage that Hufsmith’s security assessment techniques are incompatible with Veselov’s general security-assessment structure.

In addition, Petitioner presents sufficient arguments and evidence for purposes of institution that a skilled artisan would have a reasonable expectation of success in making the proposed combination. Specifically, Petitioner explains, with relevant support from its declarant, Dr. Stavrou, and the prior art that “Veselov’s snapshot-based techniques were well understood and routinely practiced,” and that “[a]lert prioritization (including usage-based prioritizing), as taught by Hufsmith, was similarly routine and predictable.” Pet. 23 (citing Exs. 1002, 1078, 1025). Patent Owner’s characterization of Petitioner’s arguments as “contrary say-so” (*see* Prelim. Resp. 34) does not undermine that one skilled in the art would have a reasonable expectation of success in employing Hufsmith’s security assessment techniques using Veselov’s snapshots.

4. Element [1.1]

Claim 1 requires “determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a protected virtual cloud asset.” Ex. 1001, 9:40–44. Independent claims 18 and 22 include parallel limitations. *Id.* at 11:29–32, 12:19–22. Petitioner contends that Veselov teaches the claimed “determining” feature in two ways. First, Veselov’s scanning service “may ‘determine the corresponding virtualization layer 144’ for the VM before transmitting a command to provide snapshot data or to provide access to the

snapshot data.” Pet. 28 (quoting Ex. 1007, 6:25–49). According to Petitioner, “[t]his teaches, or at least suggests, determining a location such as a virtual or nonvirtual endpoint (e.g., a [uniform resource locator], [Internet protocol] address, or other endpoint) since this is how virtualization layers were typically reached.” *Id.* (citing Ex. 1002 ¶ 123). Second, Petitioner asserts that Veselov’s discussion of Figure 2 teaches this feature because it “teaches determining a specific location within the virtual environment or data store.” *Id.* at 29. In either case, Petitioner explains, “Veselov further teaches or suggests that this determination would use an API or service provided by the cloud environment, since communication between the scanning service and the host environment (which includes the virtualization layer) is mediated by APIs provided by the host environment, which is part of a cloud system.” *Id.* at 28–29; *see id.* at 30.

Patent Owner contends that Veselov does not teach this element because Veselov “only uses the word ‘cloud’ once, where it provides that ‘a cloud computing environment’ is a type of ‘distributed computing environment.’” Prelim. Resp. 36 (quoting Ex. 1007, 2:64–67) (internal quotations omitted). Patent Owner further argues that Veselov only discloses identifying a VM generally—“not the claimed determination of a location of a snapshot of a virtual disk made using an API or service provided by a cloud computing environment.” *Id.* Patent Owner asserts that Veselov’s disclosure of simply identifying a VM generally is not, by itself, a sufficient disclosure to support Petitioner’s positions of identifying any components thereof, including virtual disks of the VM. *Id.* at 37. In addition, Patent Owner contends that Petitioner relies on different embodiments in Veselov as illustrated in Figures 3A, 3B, 5A, and 5B, but

Petitioner fails to appreciate “those embodiments’ distinctions and fail[s] to explain why the embodiments are interchangeable.” *Id.* at 38–39 (citing Pet. 28, 30; Ex. 1007, 10:37–41, 14:37–41, Figs. 3A, 3B, 5A, 5B).

Based on the preliminary record, we agree with Petitioner that Veselov teaches “determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a protected virtual cloud asset.” As an initial matter, Veselov provides security assessments of a service or distributed application using a distributed computing environment, such as “a ‘cloud’ computing environment.” Ex. 1007, 2:64–67. Figure 1 of Veselov illustrates that computing environment 100 includes scanning service 110 that targets computing resources via API 120 or another API. *Id.* at 5:1–5. In our view, these APIs may constitute “an API or service provided by the cloud computing environment” because, as we explain above, Veselov explicitly contemplates that its computing environment 110 may be “a ‘cloud’ computing environment.” *Id.* at 2:64–67.

Veselov further discloses that “[t]he ‘state’ of the target resource represented by snapshot data may include any properties of the target resource,” including “properties of logical volume(s) containing the target resource.” Ex. 1007, 9:55–60. Veselov discloses that one example of these logical volumes is a “virtual disk drive” of a VM (e.g., logical volume 306 of VM 312 illustrated in Figures 3A and 3B). *Id.* at 11:28–33; *see also id.* at 11:5–9 (“[V]irtual machine 312 may be executed on a server and use a logical volume 306, which is composed of a fixed or variable allocation of physical data storage resources, such as data storage blocks selected from one or more hard disk drives of one or more server computers.”). With this

in mind, there appears to be sufficient evidence to support Petitioner’s argument that these APIs are used to “determin[e] . . . a location of a snapshot of at least one virtual disk,” as the challenged claims require.

In addition, at this stage in the proceeding, we are not persuaded by Patent Owner’s further argument that Petitioner relies on different embodiments in Veselov as illustrated in Figures 3A, 3B, 5A, and 5B, but fails to appreciate “those embodiments’ distinctions and fail[s] to explain why the embodiments are interchangeable.” Prelim. Resp. 38–39 (citing Pet. 28, 30). Instead, it appears that Petitioner relies upon common features across different exemplary systems illustrated in Veselov’s Figures 3A, 3B, 5A, and 5B. *See, e.g.*, Pet. 28 (relying on Figures 3A, 3B, 5A, and 5B—all of which show the volume image 308/508 in a virtualization layer—to support that “the snapshot is stored by and obtained/accessed via the virtualization layer”). That is, Veselov discloses exemplary systems, each of which executes a security assessment of a virtual machine. Ex. 1007, 1:64–2:13, Figs. 3A, 3B, 5A, 5B. These exemplary systems all have common features, such as volume image 308 and 508, and virtual computing environment 304 and 504. *Id.* at Figs. 3A, 3B, 5A, 5B. We do not fault Petitioner for relying on those features, even though they appear in multiple figures.

5. *Element [1.2]*

Claim 1 requires “accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk.” Ex. 1001, 9:45–47. Independent claims 18 and 22 include parallel limitations. *Id.* at 11:34–36, 12:24–26. Petitioner contends that Veselov teaches this limitation because Veselov

teaches accessing snapshot data for snapshots in the determined location, as explained in Petitioner's Element [1.1] analysis. Pet. 31–33.

Although Patent Owner does not contest that Veselov accesses virtual disks' snapshots, Patent Owner asserts that, because Veselov does not determine a snapshot's location for the reasons outlined above for Element [1.1], Veselov does access the snapshot based on that determination. *See* Prelim. Resp. 40–41. We are not persuaded at this stage by Patent Owner's arguments for the same reasons we explain above for Element [1.1]. Thus, on the current record, we agree with Petitioner that Veselov's snapshot access teaches element [1.2].

6. Element [1.7]

Claim 1 requires “reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.” Ex. 1001, 9:58–60. Independent claims 18 and 22 include parallel limitations. *Id.* at 11:46–48, 12:36–38. Petitioner asserts that, together, Veselov and Hufsmith teach this limitation because Veselov's “assessment results describe the identified risks,” whereas Hufsmith teaches reporting use-based priorities—i.e., scoring information and weights for vulnerabilities. Pet. 41–43. Patent Owner argues Veselov's assessment reporting is not an alert, as evidenced by the distinction drawn between reporting results and alerts in the '032 patent's specification and claims. Prelim. Resp. 42 (citing Ex. 1001, 7:53–54, 6:40–47).

On this record, we preliminarily agree with Petitioner that Veselov's and Hufsmith's assessment results are “alerts.” Beyond a generic assessment, Veselov teaches producing an “assessment result describing a security vulnerability.” Ex. 1007, 20:67–21:1. Similarly, Hufsmith teaches

reporting “display information about a single security vulnerability,” as well as “an indication of a type of harm associated with the security vulnerability.” Ex. 1078 ¶¶ 180, 181. Thus, even if Patent Owner is correct that “that not all reported results are alerts,” Prelim. Resp. 42, we agree with Petitioner that that Veselov’s and Hufsmith’s specific reports that describe security vulnerabilities are alerts, as the challenged claims require.

7. Ground 1 Summary

Other than as outlined above, Patent Owner does not additionally challenge Petitioner’s obviousness analysis based on Veselov and Hufsmith at this stage. We have reviewed Petitioner’s arguments and the underlying evidence cited in support and we are persuaded that, at this stage, Petitioner sufficiently demonstrates a reasonable likelihood of succeeding in its challenge to claims 1–11 and 13–25 based on Veselov and Hufsmith.

B. Additional Obviousness Ground

In its additional obviousness ground, Petitioner adds Hutchins for teaching “quarantining the protected virtual cloud asset” as dependent claim 12 requires. Pet. 71–72. Hutchins does so, Petitioner explains, because it teaches “placing [a] virtual machine **in quarantine**” in response to detecting malicious code. *Id.* at 72 (quoting Ex. 1070, Abstract). Petitioner further explains that a skilled artisan would have been motivated to employ Hutchins’ quarantine response because it “minimizes [a VM’s] exposure to attacks that might exploit an identified vulnerability and minimizes contamination of other resources in the network/system by malicious/infected programs on the asset.” *Id.* at 70 (citing Ex. 1002, ¶¶ 70, 249). Other than as outlined above, Patent Owner does not additionally

challenge Petitioner's additional obviousness ground involving Hutchins. *See* Prelim Resp. 44. We have reviewed Petitioner's arguments and the underlying evidence cited in support and we are persuaded that, at this stage, Petitioner sufficiently demonstrates a reasonable likelihood of succeeding in obviousness challenge to claim 12 based on Veselov, Hufsmith, and Hutchins.

IV. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has demonstrated a reasonable likelihood of success in proving that at least one of the challenged claims of the '032 patent is unpatentable. We therefore institute trial on all challenged claims and grounds raised in the Petition. 37 C.F.R. § 42.108(a). At this stage of the proceeding, we have not made a final determination as to the patentability of any challenged claim or as to the construction of any claim term. Any final determination will be based on the record developed during trial. We place Patent Owner on express notice that any argument not asserted in a timely-filed Response to the Petition, or in another manner permitted during trial, shall be deemed waived, even if that argument was presented in the Preliminary Response.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an IPR of claims 1–25 of the '032 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), IPR of the '032 patent shall commence on the entry date of this Decision, and notice is hereby given of the institution of a trial.

For PETITIONER:

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

For PATENT OWNER:

Christopher Henry
Kristina McKenna
Steven W. Peters
LATHAM & WATKINS LLP
christopher.henry@lw.com
krissy.mckenna@lw.com
steven.peters@lw.com