

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
BRENT M. DOUGAL, *Administrative Patent Judges*.

BAER, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)
Dismissing Petitioner's Motion to Exclude
37 C.F.R. § 42.64(c)
Granting Petitioner's and Patent Owner's Motions to Seal
37 C.F.R. §§ 42.14 and 42.54

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. Pursuant to 35 U.S.C. § 314, we instituted *inter partes* review as to all of the challenged claims and all grounds raised in the Petition. Paper 8. Following institution, Patent Owner filed a Response. Paper 32 (“PO Resp.”). Petitioner filed a Reply to Patent Owner’s Response (Paper 43, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 61, “PO Sur-reply”).¹ On September 15, 2025, we held an oral hearing. A transcript of the hearing is included in the record. Paper 79.

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proven by a preponderance of the evidence that the challenged claims are unpatentable.

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

¹ In this decision, we cite the unredacted versions of the parties’ papers noted above. The parties also filed redacted versions of Patent Owner’s Response (Paper 39), Petitioner’s Reply (Paper 77), and Patent Owner’s Sur-reply (Paper 70).

court case titled *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23-cv-00758 (D. Del. filed July 12, 2023). 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 1:20–23. “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 1:43–49. 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 1:49–2:13. 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.

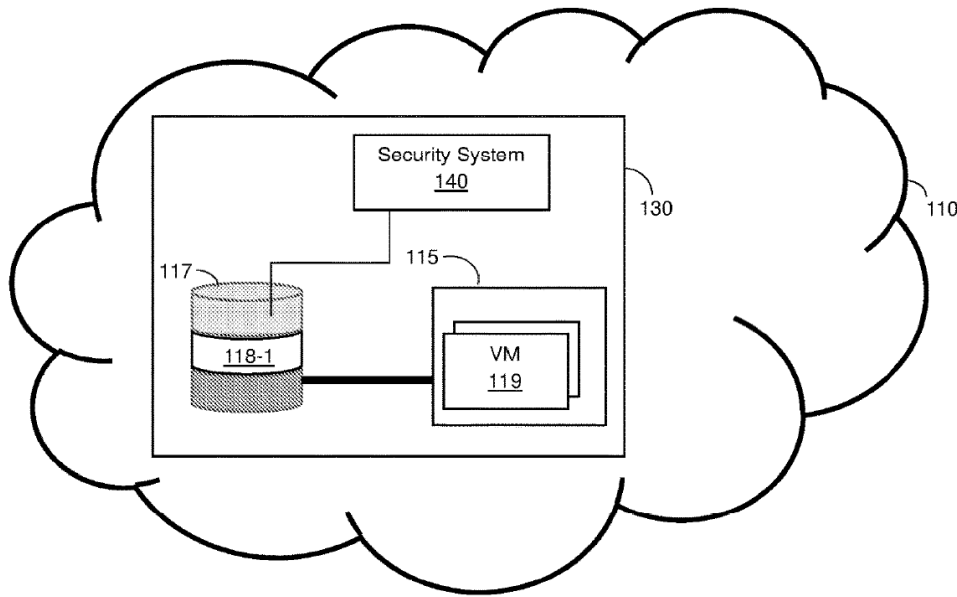


FIG. 1B

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 configuration[s], 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:

Name ²	Reference	Dates	Exhibit No.
Veselov	US 11,216,563 B1	issued Jan 4, 2022; filed May 19, 2017	1007
Hufsmith	US 2020/0097662 A1	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 ³	Veselov, Hufsmith
12	103	Veselov, Hufsmith, Hutchins

II. DISCUSSION

A. Claim Construction

Independent claims 1, 18, and 22 require “analyzing the snapshot.” Petitioner proposes we construe this term to encompass two alternative

² For clarity and ease of reference, we only list the first named inventor.

³ 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).

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 latter approach, but not the former. *See* PO. Resp. 7–9.

We addressed this same issue in our Final Written Decision in IPR2024-00865. IPR2024-00865, Paper 84 at 10–16. As we explained there, the intrinsic evidence supports that analyzing a snapshot includes analyzing a VM instantiated from a snapshot because the specification characterizes it as such. *Id.* at 13–16. The ’032 patent’s specification includes similar passages. *See* Ex. 1001, 5:55–6:4; 7:37–52, Fig. 2 (step 240). For the same reason explained in IPR2024-00865, we agree with Petitioner that snapshot analysis includes both techniques that Petitioner proposes—namely, (1) direct analysis of the snapshot data (i.e., comparing the snapshot to some baseline); and (2) analysis of a VM instantiated from the snapshot (i.e., instantiating a copy of the VM and executing that instance in a sandbox). IPR2024-00865 Paper 84 at 16; *see also SightSound Techs., LLC v. Apple Inc.*, 809 F.3d 1307, 1316 (Fed. Cir. 2015) (explaining that, “[w]here multiple patents ‘derive from the same parent application and share many common terms, we must interpret the claims consistently across all asserted patents’” (quoting *NTP, Inc. v. Rsch. In Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Circ. 2005))).

We determine we do not need to construe any additional terms to determine whether Petitioner has shown the challenged claims are unpatentable. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those 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))).

B. Level of Skill in the Art

Relying on the testimony of 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 does not provide its own assessment of the level of skill in the art, nor does it dispute Petitioner's assessment. 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 Dr. Stavrou's testimony and it is consistent with the '032 patent and the asserted prior art.

C. 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”).

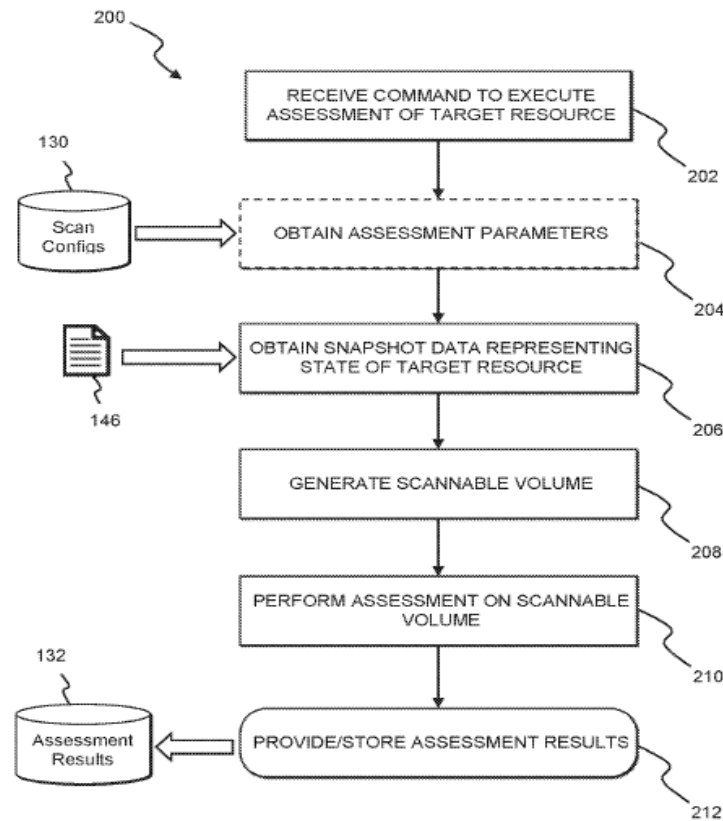


FIG. 2

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.* ¶ 91.

3. *Hutchins (Ex. 1070)*

Hutchens describes “[a] method for detecting malicious code within a first virtual machine” by “creating a snapshot of the first virtual machine and transferring the snapshot to a second machine.” Ex. 1070, code (57). “In response to detecting malicious code” during a scan operation of the snapshot run by the second machine, Hutchens teaches taking action at the first virtual machine, “includ[ing] placing the first virtual machine in quarantine.” *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. For the reasons explained below, we find that Petitioner has shown by a preponderance of evidence that these claims are unpatentable over the asserted references.

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 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 scanning 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.” *Id.* at 43. Hufsmith teaches these steps, Petitioner explains, because it discusses comparisons with CVE and malware repositories to determine potential cyber vulnerabilities. *Id.* at 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. *Id.* at 37–41. Last, Petitioner asserts that, together, Veselov and Hufsmith teach the claimed reporting the cyber vulnerabilities as prioritized alerts because Veselov 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.

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

2. Patent Owner's Challenge to Petitioner's Rationale for Combining Veselov and Hufsmith

Patent Owner asserts that Petitioner's rationale for combining Veselov and Hufsmith is flawed because the two references analyze different data (Veselov's snapshots/volume images vs. Hufsmith's container images) for different purposes (Veselov's post-deployment VM assessments for users/administrators vs. Hufsmith's pre-deployment assessments for developers). PO Resp. 13–15, *see* PO Sur-reply 3. Further, Patent Owner argues Hufsmith's score-based system would "increase[e] the complexity of Veselov's assessment system to include a multitude of separate scanners," and "Veselov expressly advised *against* the 'drawbacks' of systems that require 'complexity of installation and monitoring of the assessment system.'" *Id.* at 16 (quoting Ex. 1007, 2:42–54). We disagree with these arguments.

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 these rationales, 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). Even if Hufsmith's prioritized alerts come at a cost of increased complexity, that tradeoff would not necessarily undermine Petitioner's proffered combination given Petitioner's articulated benefits regarding rapid identification of higher-priority assets/risks and mitigated alert fatigue. *See Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000) ("The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another.").

In addition, Patent Owner's arguments highlighting mere differences between Veselov and Hufsmith do not undermine Petitioner's proffered rationales because they wrongly assume bodily incorporation of features like Hufsmith's pre-deployment data and container images that Petitioner does not propose combining without identifying any incompatibility in Petitioner's actual proposed combination. *See Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (explaining that physical combinability and bodily incorporation

are not the proper tests for obviousness).

Patent Owner also 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 because a skilled artisan would not “garner sufficient information from a snapshot to facilitate any type of application usage determination.” PO Resp. 18. We disagree. Petitioner explains, with relevant support from 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). Dr. Stavrou also explains that a skilled artisan would have expected that “well-known types of file-access data” would be “included in the snapshot data evaluated by Veselov” and “would have reasonably expected success in determining application usage based on such data” given Veselov’s teaching that a “snapshot includes various types of system data, including ‘system log properties.’” Ex. 1002 ¶ 176 (quoting Ex. 1007, 9:55–67). With this evidence, and absent any explanation why Hufsmith’s prioritized alerts and use determinations are incompatible with Veselov’s snapshot-based analysis, we find Petitioner has shown a skilled artisan would have a reasonable expectation of success in making the proposed combination.

3. Disputed Independent Claim Elements

a) Element [1.5]

Element [1.5] requires “determining whether the matching installed applications are used by the protected virtual cloud asset.” Ex. 1001, 9:61–

63. Independent claims 18 and 22 include parallel limitations. *Id.* at 11:42–43, 12:32–33. Petitioner asserts its proposed combination of Veselov and Hufsmith teaches this feature because “Veselov determines which applications are installed before running assessment tasks” and “Hufsmith teaches adjusting previously assigned threat levels based on whether the associated file/code is dormant or active.” Pet. 34 (citing Ex. 1007, 9:55–67, 18:32–53), 37–38 (citing Ex. 1078 ¶¶ 109, 113–128). Hufsmith also teaches the recited use determination, Petitioner explains, because its “malware evaluator considers ‘whether the file or code is executed’” as part of Hufsmith’s initial calculation of individual weights. *Id.* at 38–39 (quoting Ex. 1078 ¶ 121).”

Patent Owner argues Petitioner’s challenge fails because Hufsmith determines only whether “*subroutines*” of a single application are active or dormant, which “is different from, and does not render obvious, determining whether an installed application is used as required by the challenged claims.” PO Resp. 19–20 (citing Ex. 1078 ¶ 140). According to Patent Owner, “[t]he ’032 Patent itself differentiates between determining use of an ‘application’ and determining ‘modules executed in the protected virtual cloud asset.’” *Id.* at 20 (citing Ex. 1001, claims 1 and 10). In addition, Patent Owner asserts that “there are no disclosures of determining ‘application use’ in Hufsmith because its scans are directed to determining risks pre-deployment . . . , which is *before* virtual cloud assets might ‘use’ an application.” *Id.* at 21 (citing Ex. 1078 ¶¶ 108, 158, claim 1).

We disagree with Patent Owner’s argument first because it attacks Hufsmith individually, rather than the combination of Veselov and Hufsmith

that Petitioner asserts. *See In re Keller*, 642 F.2d 413, 426 (CCPA 1981). Even if Hufsmith did teach only determining whether subroutines or a component of application are in use and doing so only pre-deployment, that does not undermine Petitioner's challenge because Petitioner proposes combining Hufsmith's dormancy/activity determination with Veselov's installed applications. *See* Pet. 38 (asserting that Hufsmith's dormant-code analysis suggests "assessing the dormancy/activity of [Veselov's] matching installed applications"). Hufsmith does not preclude post-deployment application-use determinations, let alone disparage them. *See In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004) ("The prior art's mere disclosure of more than one alternative does not constitute a teaching away from . . . alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed."); *see* Ex. 1400 ¶ 30 (explaining that "Hufsmith teaches applicability to VMs . . . and teaches applicability during deployment" (citing Ex. 1078, ¶¶ 24, 108, 149, 154, 159)). Moreover, we agree with Petitioner that Patent Owner's argument mischaracterizes Hufsmith's disclosure as limited to assessing the activity of an application's subroutines, rather than the application itself. Pet. Reply 6–7. Rather, as Dr. Stavrou explains, because "malware was well known to encompass standalone applications," Hufsmith's malware evaluator that determines "whether the file or code is executed" encompasses determining whether the application itself used since that is one of [the] straightforward ways (if not the most straightforward way) of determining whether such malware is used." Ex. 1400 ¶ 29.

Based on Petitioner’s analysis outlined above, we agree with Petitioner that Hufsmith’s in-use determination applied to Veselov’s applications teaches “determining whether the matching installed applications are used by the protected virtual cloud asset,” as claimed.

b) Element [1.7]

Element [1.7] 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 its proposed combination of Veselov and Hufsmith teaches this additional feature because “Veselov’s assessment results describe the identified risks,” and “Hufsmith teaches, or at least suggests, that this reported information about individual vulnerabilities may include the previously discussed use-based priorities.” Pet. 41–42 (citing Exs. 1007, 1078). Specifically, Petitioner notes that Hufsmith teaches reporting “‘metrics’ with links to ‘descriptions of the potential vulnerabilities.’” *Id.* at 42 (citing Ex. 1078 ¶ 96). Petitioner asserts that Hufsmith also teaches the claimed prioritized alerts according to use determinations in its “discussion of presenting annotations in a development environment” that “display information about a single security vulnerability such as a classification or score.” *Id.* at 42–43 (citing 1078 ¶¶ 180–182 (quotation marks omitted)).

Patent Owner argues Petitioner’s challenge fails because Hufsmith teaches reporting only “overall scores” that “are related to the exposure of the entire *image*, not reporting the determined vulnerabilities found within a virtual cloud asset as prioritized alerts based on use determinations, as the

claims require.” PO Resp. 23. Patent Owner also asserts that Hufsmith’s source-code annotations are incompatible with Veselov, which involves read-only snapshots, rather than source code. *Id.* at 23–24.

We disagree with Patent Owner’s first argument because, once again, it attacks Hufsmith individually, rather than the combination of Veselov and Hufsmith that Petitioner asserts. *See In re Keller*, 642 F.2d at 426.

Petitioner does not map the claimed prioritized alerts to Hufsmith’s overall score, but rather to the combination of Veselov’s assessment results describing identified risks and Hufsmith’s “information about individual vulnerabilities.” Pet. 41–42; *see* Pet. Reply 8. In addition, Patent Owner’s argument that Hufsmith’s source-code annotations are incompatible with Veselov’s snapshots, which Patent Owner incorrectly characterizes as being limited to read-only (*see* Ex. 1007, 18:1–2) (describing that “the scanning service 510 *may* mount volume images as read only” (emphasis added)), incorrectly assumes that a skilled artisan could do no more than bodily incorporate Hufsmith’s source-code annotations to Veselov’s optional read-only snapshot embodiment. That, however, is neither what Petitioner proposes, nor is it the test for obviousness. *See* Ex. 1400 ¶ 36 (explaining that the combination does not involve does a wholesale incorporation of Hufsmith’s source-code annotations into Veselov’s read-only snapshot); *see also Allied Erecting & Dismantling Co.*, 825 F.3d at 1381 (explaining that physical combinability and bodily incorporation are not the proper tests for obviousness); *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (noting that “a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ”).

For the reasons outlined above, we agree with Petitioner that, given Hufsmith’s use-based prioritization Veselov’s assessment-results reporting, the asserted combination teaches “reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations,” as claimed.

4. Undisputed Independent Claim Limitations

Petitioner provides a detailed analysis demonstrating that its proposed combination teaches the remaining limitations of claim 1. *See* Pet. 20–43. Petitioner asserts Veselov’s scanning service that obtains/accesses “a state of the resource at a point in time (e.g., a **“snapshot”**)” teaches independent claim 1’s preamble and elements [1.1] and [1.2], which require 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 element [1.3]’s analyzing the snapshot, as well as element [1.4]’s determination of potential cyber vulnerabilities. *Id.* at 33; *see id.* at 34–35, 36–37. Petitioner explains that Hufsmith’s context evaluator and vulnerability weight assignment teach claim element [1.6]’s prioritizing vulnerabilities based on use determinations. *See id.* at 39–41. Petitioner’s analysis for independent claims 18 and 22 mirrors its claim 1 analysis as these three claims are substantively nearly the same. *See id.* at 24–43. Beyond the arguments above, Patent Owner does not challenge Petitioner’s analysis for elements [1.1]–[1.4] and [1.6] or the parallel limitations in independent claims 18 and 22. We have reviewed Petitioner’s arguments and evidence and, based on

that analysis, we find Petitioner has shown by a preponderance of the evidence its asserted combination of Veselov and Hufsmith teaches elements [1.1]–[1.4] and [1.6], as well as the parallel limitations in independent claims 18 and 22.

5. *Ground 1 Dependent Claims*

c) *Claim 2*

Claim 2 requires, in relevant part, “determining whether at least one of the matching installed applications is not in use by the protected virtual cloud asset, and wherein prioritizing reduces priority of potential cyber vulnerabilities for a matching installed application not in use.” Petitioner’s analysis for this limitation references its analysis for element [1.5]. *See* Pet. 44. There, Petitioner asserts its proposed combination of Veselov and Hufsmith teaches active/dormant application determination because “Veselov determines which applications are installed before running assessment tasks,” *id.* at 34 (citing Ex. 1007, 9:55–67, 18:32–53), and “Hufsmith teaches adjusting previously assigned threat levels based on whether the associated file/code is dormant or active,” *id.* at 37–38 (citing Ex. 1078 ¶¶ 109, 113–128). In challenging this element, Patent Owner reiterates its argument that Petitioner “wrongly conflates a *component* of an application (code or a file) with an actual application.” PO Resp. 26. We disagree with this argument for the reasons outlined above in Section III.A.3.a. Based on Petitioner’s analysis outlined above, we agree that the asserted combination of Veselov and Hufsmith teaches “determining whether at least one of the matching installed applications is not in use by the protected virtual cloud asset, and wherein prioritizing reduces priority of

potential cyber vulnerabilities for a matching installed application not in use,” as claimed.

d) Claim 3

As Petitioner explains, “[c]laim 3 depends from claim 1 and recites essentially the same language as claim 2 while adding that the recited use determination ‘includes checking configuration files of the matching installed applications’ to determine whether at least one of the matching installed applications is not in use by the protected virtual cloud asset.” Pet. 45. Petitioner asserts that Hufsmith accounts for this additional feature because it “explains that the environmental context used to make dormancy determinations may be inferred from a composition file or other ‘configuration data’ of a distributed application.” *Id.* (quoting Ex. 1078 ¶ 140). Other than the arguments above, Patent Owner does not additionally challenge Petitioner’s showing for claim 3. PO Resp. 26. Based on Petitioner’s analysis outlined above, we agree with Petitioner that the asserted combination of Veselov and Hufsmith teaches the additional limitation in claim 3.

e) Claims 4 and 5

Claim 4 depends from claim 1 and recites essentially the same language as claim 2, but adds that the recited use determination “includes verifying access times to files by an operating system” to determine whether the matching installed applications are not in use. Ex. 1001, 10:9–17. Claim 5 is similar, but requires that recited use determination “includes analyzing

application logs or system logs” to determine whether the matching installed applications are not in use. *Id.* at 10:18–25.

Petitioner asserts that these additional features would have been obvious because Hufsmith teaches “a variety of ways to determine whether the matching installed applications are used, including ‘[e]xecution environment records.’” Pet. 46 (quoting Ex. 1078 ¶ 140). Citing support from Dr. Stavrou and multiple prior-art references, Petitioner explains that while Hufsmith does not expressly state that its records include file access times, “this would have been obvious to a [person of ordinary skill in the art] because such access times were a common part of such records” and “use determinations such as those described in Hufsmith were routinely and predictably performed by verifying such access times.” *Id.* at 46–47 (citing Ex. 1002 ¶¶ 175–176 (citing Ex. 1063 ¶¶ 126, 184), Ex. 1007, 9:55–67, Ex. 1079, 31–36). Petitioner also explains, again with relevant support from Dr. Stavrou and multiple prior-art references, that “[r]ecords such as application logs and system logs were routinely kept in cloud systems such as those described in Veselov and Hufsmith, and they were also routinely analyzed during these types of security assessments.” *Id.* at 47 (citing Exs. 1002, 1007, 1078, 1079, 1063).

Patent Owner argues that Petitioner’s arguments for claims 4 and 5 “leave a fatal gap between these concepts allegedly being well-known and their beneficial application to Veselov or Hufsmith.” PO Resp. 27 (quoting *Fanduel, Inc. v. Interactive Games LLC*, 966 F.3d 1334, 1344 (Fed. Cir. 2020) (internal quotations and alterations omitted)). We disagree. Petitioner did not merely allege that the additional features in claims 4 and 5 were well

known. Rather, Petitioner explained that Hufsmith teaches application-usage determinations based on execution-environment records and provided un rebutted evidence showing that application/system logs and records with corresponding file access times were known and “were routinely and predictably used to perform the application-usage techniques taught by Hufsmith.” Pet. Reply 9; *see* Pet. 46–47 (citing Exs. 1002, 1007, 1078, 1079, 1063). Patent Owner also argues that “application use analyses are not applicable or detected in Hufsmith’s pre-deployment container images,” and that analyzing application/system logs “would increase the complexity and installation of Veselov’s monitoring system, which Veselov advises against.” PO Resp. 27. We disagree with these arguments because they once again attack Hufsmith individually without identifying incompatibles, and ignore the risk-assessment benefits that come with use determinations, even if such use determinations may increase complexity. *See, e.g., Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000) (“The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another. Instead, the benefits, both lost and gained, should be weighed against one another.”).

Based on Petitioner’s analysis above, we agree with Petitioner that the asserted prior art teaches use determinations based on access times and application/system, as required in claims 4 and 5.

f) Claims 16 and 20

Dependent claims 16 and 20 each require “wherein determining the location of the snapshot of at least one virtual disk further includes querying

a cloud management console of the cloud computing environment for the location of the snapshot and the location of the virtual disk.” Ex. 1001, 11:12–17, 12:2–6. Petitioner asserts that Veselov teaches this additional feature. Specifically, Petitioner explains Veselov’s “[user interface (‘UI’)] (alone or in conjunction with its associated API) operates as a ‘cloud management console’” and that Veselov’s “target resources are part of a cloud system.” Pet. 64–65. Veselov teaches querying for the location of the snapshot 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.” *Id.* at 28 (quoting Ex. 1007, 6:25–49); *see id.* at 66. 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). “Moreover,” Petitioner explains, “this is a location *of the snapshot* because, except for optional embodiments in which the snapshot is stored in an external snapshot storage service, the snapshot is stored by and obtained/accessed via the virtualization layer.” *Id.* at 28 (citing Ex. 1007, 5:18–6:6, 6:25–49). Second, Petitioner asserts that Veselov’s discussion of Figure 2 teaches querying/determining a snapshot’s location because it teaches “determining a specific location within the virtual environment or data store” to access a snapshot stored there. *Id.* at 29; *see id.* at 66.

Next, Petitioner asserts Veselov suggests querying a location of the virtual disk because “Veselov shows the snapshot and its associated virtual

disk initially located in the same computing environment.” *Id.* at 66–67. Further, “Veslov also teaches using the UI/API to display and configure aspects of the assessment, including selection of the assessment target (e.g., the virtual disk),” which “teaches or at a minimum suggests” querying the virtual disk’s location “because that location would facilitate the subsequent assessment and because determining the location of such virtual resources was a common feature of these consoles.” *Id.* at 67 (citing Ex. 1002, ¶¶ 38, 45–46, 233–34; Ex. 1015, 16–23, 55–58, 115–20, 124–26, 150–52, 155–56; Ex. 1031, 1–4).

Patent Owner raises several arguments in contesting this limitation. First, Patent Owner argues “querying a cloud management console of the cloud computing environment for the location of a snapshot or the location of a virtual disk was neither necessary nor inherent” in Veslov because Veslov teaches obtaining snapshots in its Figure 5 embodiment, which lacks the computing resource service provider that Petitioner contends is a cloud computing environment. PO Resp. 28. We disagree with this argument because we do not understand Petitioner to be relying on inherency. We also disagree with Patent Owner that Veslov’s Figure-5 embodiment involves only a non-cloud provider because, as Petitioner notes, Veslov teaches in its background that its “techniques are particularly useful in a ‘distributed computing environment (e.g., a **“cloud” computing environment**),” and that its Figure-5 embodiment has the same “implementation and interactions” as Veslov’s Figure-3 embodiment, which includes a computing resource service provider. Pet. 25 (citing Ex. 1007, 2:42–3:19), 64 (citing Ex. 1007, 16:56–17:8).

Next, Patent Owner asserts that locating a VM and locating a virtual disk are not the same because VMs and virtual disks are not synonymous and typically have different locations. PO Resp. 29. We disagree with this argument because Petitioner has not argued that VMs and the virtual disks are synonyms or co-located. *See* Pet. 66–67. In addition, beyond merely requesting VM snapshots, Veselov discloses that “[w]hen . . . requesting the snapshot, the scanning service may include instructions identifying the data to include in the snapshot,” such as which “file system of a virtual machine instance” to analyze (e.g., the location of the virtual disk drive of a VM to analyze). Ex. 1007, 9:25–32. Thus, even if querying a VM’s location is insufficient as Patent Owner contends, we agree with Petitioner that Veselov further teaches querying for the location of a virtual disk, as claimed.

Last, Patent Owner criticizes Petitioner for merely arguing that Veselov’s system is “*capable of*” a query that “*could* include requesting a virtual disk.” PO Resp. 30. We disagree with this argument because it mischaracterizes Petitioner’s position. Beyond arguing that Veselov could query a virtual disk’s location, Petitioner explains, with relevant, uncontested support from Dr. Stavrou and the prior art, that such queries (and their utility) were known in the art. Pet. 67 (citing Ex. 1002 ¶¶ 38, 45–46, 233–34; Ex. 1015, 16–23, 55–58, 115–20, 124–26, 150–52, 155–56; Ex. 1031, ii, 1–4). Petitioner also explains, again with uncontested support, why skilled artisans would have included them in Veselov—i.e., to “facilitate [Veselov’s] subsequent assessment.” *Id.*

Based on Petitioner’s analysis above, we agree with Petitioner that the asserted prior art teaches “wherein determining the location of the snapshot

of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the location of the virtual disk,” as each of dependent claims 16 and 20 require.

g) Remaining Dependent Claim Limitations

Petitioner provides a detailed analysis demonstrating that its proposed combination teaches the dependent claim limitations for claims 6–11, 13–15, 17, 19, 21, and 23–25 including 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), checking applications’ configuration files (claim 10), mitigating vulnerabilities (claim 11), determining an allocated virtual disk (claim 13), taking a new snapshot (claims 14, 15, 23, and 24), and making/analyzing a copy of a snapshot (claims 17, 21, and 25). Pet 43–69. Other than the arguments addressed above, Patent Owner does not additionally challenge Petitioner’s obviousness analysis for dependent claims 6–11, 13–15, 17, 19, 21, and 23–25 based on Veselov and Hufsmith. We have reviewed Petitioner’s arguments and evidence and, based on that analysis, we find Petitioner has shown that Veselov and Hufsmith teach the additional limitations in claims 6–11, 13–15, 17, 19, 21, and 23–25.

B. Ground 2: Obviousness of Claim 12 based on Veselov, Hufsmith, and Hutchins

In its second 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 71 (citing Ex. 1002 ¶¶ 70, 249).

Patent Owner asserts that Petitioner’s rationale for combining the teachings of Hutchins with those of Veselov/Hufsmith is flawed because Hutchins describes snapshot-based techniques, whereas Hufsmith teaches scanning offline container images. PO Resp. 62. Patent Owner also argues that Hutchins teaches scanning a replicated VM, rather than analyzing the snapshots themselves. *Id.* at 62–63. We disagree with these arguments. Given Petitioner’s rationale outlined above (i.e., minimizing further attacks to the VM and to minimizing contaminating other network resources), 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. Patent Owner’s arguments highlighting mere differences between Hutchins and Hufsmith—i.e., Hutchins’s snapshot scan versus Hufsmith’s container-image scan—do not undermine Petitioner’s proffered rationale and do not identify incompatibilities in Petitioner’s proposed combination. In addition, we disagree with Patent Owner’s argument regarding Hutchins replicated VM both because it relies

on Patent Owner’s “analyz[ing] the snapshot” claim construction (precluding analysis of a VM instantiated from a snapshot) that we do not adopt and because it incorrectly assumes Petitioner proposes bodily incorporating Hutchins’s VM replication, which is not what Petitioner proposes. *See* Pet. 71–72.

Other than the arguments above, Patent Owner does not additionally challenge Petitioner’s showing for claim 12. Based on Petitioner’s analysis outlined above, we agree with Petitioner that Hutchins teaches the additional feature of dependent claim 12. In addition, given Petitioner’s minimizing-exposure rationale outlined above, 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.

C. Objective Indicia

Patent Owner asserts that objective-indicia evidence confirms the non-obviousness of the challenged claims of the ’032 patent. PO Resp. 35–62. We addressed these same issues based on the same arguments and evidence in our Final Written Decision in IPR2024-00865. *See* IPR2024-00865, Paper 84 at 68–115; *compare* PO Resp. 35–62 *with* IPR2024-00865, Paper 32 at 34–62. As we explained there, Patent Owner did not establish a sufficient nexus between the asserted evidence based on its SideScanning technology and claimed features that were unknown in the prior art. *See* IPR2024-00865, Paper 84 at 115. Independently of establishing nexus between its SideScanning technology and the challenged claims, the evidence of long-felt need, skepticism, and copying is weak, and despite there being some evidence of industry praise and commercial success, Patent

Owner has not shown that the evidence of industry praise and commercial success is connected to claimed features that were unknown in the prior art. *Id.* For the same reasons explained in IPR2024-00865, we find that Patent Owner has not shown that its evidence of secondary considerations overcome Petitioner’s strong obviousness showing. *See* IPR2024-00865, Paper 84 at 118–119. *See, e.g., Intercontinental Great Brands LLC v. Kellogg North America Co.*, 869 F.3d 1336, 1342–47 (Fed. Cir. 2017) (determining that the strong case of obviousness as to the independent claims at issue outweighs the evidence of non-obviousness).

D. Obviousness Summary

Based on Petitioner’s analysis and for the reasons above, we find Petitioner has shown by a preponderance of the evidence that claims 1–11 and 13–25 are unpatentable as obvious over Veselov and Hufsmith (ground 1), and that claim 12 is unpatentable as obvious over Veselov, Hufsmith, and Hutchins (ground 2).

IV. PETITIONER’S MOTION TO EXCLUDE

Petitioner filed a Motion to Exclude 2134, 2136, 2137, 2148, 2400–2422, and 2425–2428 as inadmissible under the Federal Rules of Evidence. Paper 53, 1–15.⁴ Because we have determined that all challenged claims are unpatentable without excluding the evidence Petitioner seeks to exclude, Petitioner’s motion is moot. Accordingly, we *dismiss* Petitioner’s Motion as moot.

⁴ Paper 53 is the unredacted version of Petitioner’s Motion to Exclude. Petitioner also filed a redacted version of its Motion as Paper 76.

V. MOTIONS TO SEAL

Petitioner and Patent Owner request to seal Papers 43, 53, 57, 58, 61, 65, 66, and 68 and Exhibits 1400–1414, 2172, and 2173. Papers 44, 52, 56, 59, 60, 64, 67. After reviewing the Papers and Exhibits, we agree that they contain business confidential information. Accordingly, Papers 43, 53, 57, 58, 61, 65, 66, and 68 and Exhibits 1400–1414, 2172, and 2173 will continue to be maintained under seal, and these documents and exhibits will be governed by the terms of the parties’ Joint Proposed Protective Order entered in this proceeding. *See* Ex. 2161.

VI. CONCLUSION

Based on the fully developed trial record, Petitioner demonstrates by a preponderance of the evidence that claims 1–25 of the ’032 patent are unpatentable. A summary of our conclusions is set forth in the table below.

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–11, 13–25	103	Veselov, Hufsmith	1–11, 13–25	
12	103	Veselov, Hufsmith, Hutchins	12	
Overall Outcome			1–25	

VII. IV. ORDER

Accordingly, it is

ORDERED that claims 1–25 of the '032 patent have been shown to be unpatentable;

FURTHER ORDERED that we *dismiss* Petitioner's Motion to Exclude as moot;

FURTHER ORDERED that we *grant* the parties' Motions to Seal;

FURTHER ORDERED that all the papers and exhibits filed under seal will continue to be maintained under seal;

FURTHER ORDERED that, because this Final Written Decision discusses some of the business confidential information previously designated by the parties, it will be filed under seal;

FURTHER ORDERED that, no later than (10) business days of entry of this Final Written Decision, the parties must file a public, redacted version of the Final Written Decision that strikes the appropriate balance between the public's interest in maintaining a complete and understandable file history and the parties' interest in protecting their business confidential information; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. ¶ 90.2.

IPR2024-00864
Patent 11,663,032 B2

FOR PETITIONER

Matthew Argenti
Michael Rosato
Wesley Derryberry
Joseph Baillargeon
Tasha Thomas
WILSON SONSINI GOODRICH & ROSATI
margenti@wsgr.com
mrosato@wsgr.com
wderryberry@wsgr.com
jbaillargeon@wsgr.com
tthomas@wsgr.com

FORPATENT OWNER

Raghav Bajaj
Kristina McKenna
Douglas Lumish
Blake Davis (admitted *pro hac vice*)
LATHAM & WATKINS LLP
raghav.bajaj@lw.com
krissy.mckenna@lw.com
douglas.lumish@lw.com
blake.davis@lw.com