

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-00863
Patent 11,663,031 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 1–16 of U.S. Patent No. 11,663,031 B2 (Ex. 1001, “the ’031 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 42, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 60, “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. For the reasons below, we also dismiss Petitioner’s Motion Exclude (Paper 52) as moot and grant the parties’ Motions to Seal (Papers 43, 51, 55, 58, 59, 64, and 67).

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.

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 38), Petitioner’s Reply (Paper 77), and Patent Owner’s Sur-reply (Paper 70).

B. Related Matters

The parties indicate that the '031 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). Pet. 2; Paper 3, 1.

C. The '031 Patent

The '031 patent generally relates to “cyber-security systems and, more specifically, to techniques for securing virtual machines.” Ex. 1001, 1:14–16. According to the '031 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 1:24–26. This is accomplished by using “virtual machines [VMs]” that “emulate[] a number of ‘computers’ or instances, all within a single physical device.” *Id.* at 1:28–30. The '031 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 1:39–46. 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 1:46–2:14. The '031 patent, however, explains how there are certain

disadvantages associated with each of these conventional ways of traffic inspection. *Id.*

The '031 patent ostensibly addresses these disadvantages by providing a method for “securing virtual cloud assets at rest against cyber threats.”

Ex. 1001, 2:56–57. Figure 1B of the '031 patent, reproduced below, illustrates a network diagram that implements various embodiments. *Id.* at 3:24–25.

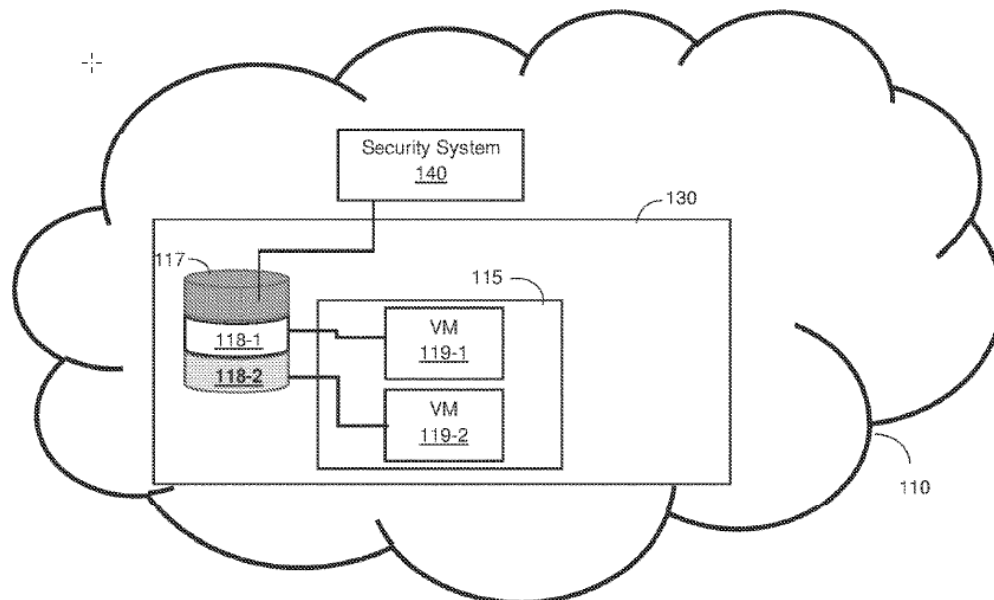


FIG. 1B

Figure 1B illustrates cloud computing platform 110 that includes client environment 130 with storage 117 containing virtual disks 118-1 and 118-2, server 115 hosting virtual machines 119-1 and 119-2, and security system 140. *Id.* at 3:60–4:50. “[S]ecurity system 140 is configured to detect vulnerabilities and other cyber threats related to the execution [of] VM 119-2.” *Id.* at 5:19–21. 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 5:24–30.

D. Challenged Claims

Of the challenged claims, claims 1, 9, and 16 are independent. Independent claim 1 is illustrative of the challenged claims and is reproduced below.

1. A system for inspecting data, the system comprising:
 - [1.i] at least one processor configured to:
 - [1.1] establish an interface between a client environment and security components;
 - [1.2] using the interface, utilize cloud computing platform [application programming interfaces (‘APIs’)] to identify virtual disks of a virtual machine in the client environment;
 - [1.3] use the computing platform APIs to query a location of at least one of the identified virtual disks;
 - [1.4] receive an identification of the location of the virtual disks of the virtual machine;
 - [1.5] perform at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time;
 - [1.6] analyze the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive; and
 - [1.7] report the detected vulnerabilities as alerts.

Id. at 10:44–64 (Petitioner’s element numbering added).

E. Asserted Prior Art References

Petitioner relies on the prior art references set forth in the tables below.

Name²	Reference	Dates	Exhibit No.
Veselov	US 11,216,563 B1	issued Jan 4, 2022; filed May 19, 2017	1007
Price	US 2013/0247133 A1	published Sept. 19, 2013; filed Oct. 13, 2011	1048
Hufsmith	US 2020/0097662 A1	published Mar. 26, 2020; filed Sept. 28, 2018	1078

Printed Publication	Exhibit No.
Alvin Huseinović & Samir Ribić, “ <i>Virtual Machine Memory Forensics</i> ” 2013 21st Telecommunications Forum Telfor (“Huseinović”).	1049

F. Asserted Grounds of Unpatentability

Petitioner challenges claims 1–16 of the ’031 patent based on the asserted grounds of unpatentability set forth in the table below. Pet. 3, 22–65.

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

Claim(s) Challenged	35 U.S.C. §	References/Basis
1, 3–9, 11–16	103 ³	Veselov, Price
2, 10	103	Veselov, Price, Hufsmith
6, 14	103	Veselov, Price, Hufsmith, Huseinović

II. DISCUSSION

A. Claim Construction

1. “analyz[ing] the at least one snapshot”

Independent claims 1, 9, and 16 each require “analyz[ing] the at least one 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. 10–11. Patent Owner disputes the latter approach, but not the former. *See* PO. Resp. 10–12.

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 ’031 patent’s specification includes similar passages. *See* Ex. 1001, 6:62–7:11; 8:45–59, Fig. 2 (step 240). For the same reason explained in IPR2024-00865, we agree with

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).

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))).

2. “(i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest”

Independent claims 1, 9, and 16 each recite “[perform/performing] at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest.” The parties dispute whether the phrase “of the virtual machine at rest” modifies both listed clauses—“(i) taking at least one snapshot” and “(ii) requesting taking at least one snapshot”—as Patent Owner contends (*see* PO Resp. 6–10), or only the second “requesting taking” clause, as Petitioner contends (*see* Pet. Reply 1–3).

We agree with Petitioner that “at rest” applies only to the second listed option because, as Petitioner notes, “[t]he claim language emphasizes the distinction between options (i) and (ii) with numbering, punctuation, and separate recitation of ‘at least one snapshot.’” Pet. Reply 1. Moreover, the prosecution history of the ’031 patent supports Petitioner’s construction

because older versions of the claim expressly added the “at rest” limitation in the first listed option, but that language was ultimately removed. *See* Ex. 1004, 123–127⁴; Pet. Reply 2–3 (citing *U.S. v. Telectronics, Inc.*, 857 F.2d 778, 782–83 (Fed. Cir. 1988) (holding that adding a limitation to a claim during prosecution and then removing it does not permit reading of limitation into claim when the claim issued without it)).

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,

⁴ All references to the page number in the prosecution history of the ’031 patent refer to the page numbers added by Petitioner in the bottom, right-hand corner of each page in Exhibit 1004.

malware analysis, security analysis of cloud computing systems,
and security analysis of virtual machines.

Pet. 8–9 (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 ’031 patent and the asserted prior art.

C. Description of 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”).

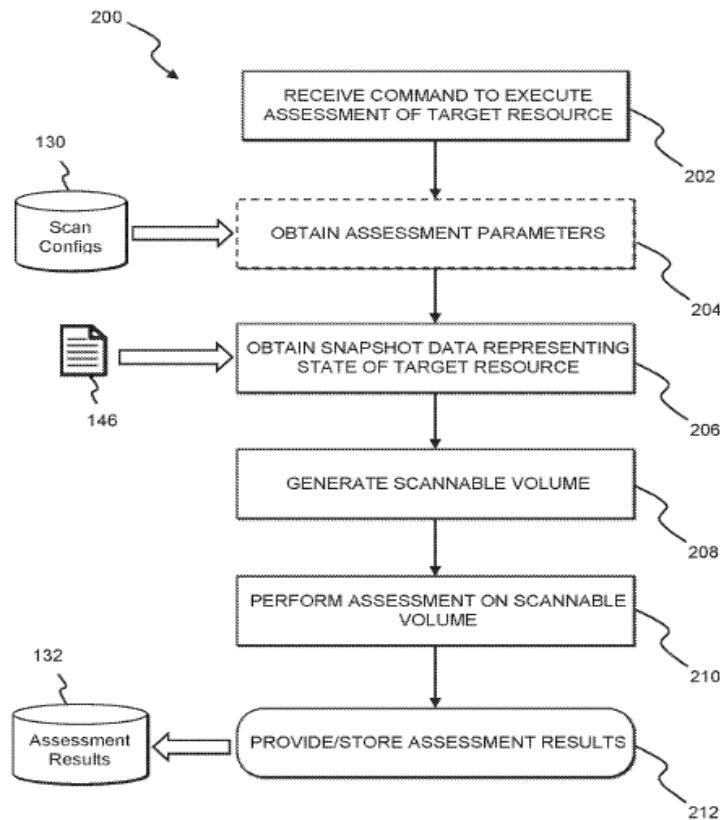


FIG. 2

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. Price (*Ex. 1048*)

Price generally relates to “computer security and, more particularly, to performing security tasks on virtual machines.” *Ex. 1048* ¶ 1. Price discloses a feature directed to collecting “[r]esult data . . . from the security assessment of . . . offline virtual machines.” *Id.* ¶ 14. Price accomplishes this collection of data using computer system 100 that is “configured to scan offline virtual appliances, including those virtual appliances which had already been powered down, for vulnerabilities and policy compliance violations.” *Id.* ¶ 29, Fig. 1.

4. *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.

5. *Huseinović (Ex. 1049)*

Huseinović generally relates to obtaining and analyzing virtual machine physical memory “usually presented as a file on a host operating system.” Ex. 1049, 940. Huseinović discloses using “standard and built-in options . . . to collected physical memory data from virtual machines that are running in VMware and VirtualBox virtualization environments.” *Id.* Huseinović accomplishes this task by generating a snapshot while the VM is in a suspended state, and then analyzing a file from the snapshot. *Id.* at 940–41.

III. OBVIOUSNESS ANALYSIS

A. *Ground 1: Obviousness based on Veselov and Price*

Petitioner contends that claims 1, 3–9, and 11–16 are unpatentable under 35 U.S.C. § 103 as obvious over Veselov and Price. Pet. 22–54. 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 Price*

Petitioner relies on Veselov to teach the bulk of the independent claim elements. Petitioner maps Veselov’s network communication channels that facilitate a scanning service for a target resource (as depicted in Veselov’s Figure 1) to the claimed client-security interface and cloud computing API that identifies and queries a VMs’ virtual disks. Pet. 25–36. Petitioner further relies on Veselov’s service that “obtain[s] and analyze[s] snapshot data 146” for teaching taking and analyzing snapshots of the virtual disks to detect and report vulnerabilities, as the independent claims require. *Id.* at 37

(quoting Ex. 1007, 6:25–30); *see id.* at 36–45. Petitioner further explains that Veselov teaches the claimed reporting-vulnerabilities step because Veselov’s assessment results describe security vulnerabilities. *Id.* at 45.

Because Veselov “does not expressly describe the state of the VM at the time the snapshot is captured,” Petitioner relies on Price for teaching “obtaining and analyzing images of offline VMs.” *Id.* at 38. Price does so, Petitioner explains, by “determining whether VMs are online or offline and, for each offline VM, obtaining and scanning the VM’s image data to identify/report security issues.” *Id.* at 38 (citing Ex. 1048 ¶¶ 14, 21, 29, 42, 44, 45, Fig. 6). Citing relevant support from Price and its declarant, Dr. Stavrou, Petitioner contends that a skilled artisan would have been motivated to combine Price’s inactive/at rest security assessments with Veselov’s virtual computing security assessment system “to provide the well-known security benefit of preventing further damage that might otherwise be caused if a potentially compromised VM actively runs (e.g., a vulnerability could be exploited, or suspected malware could contaminate other resources).” *Id.* at 24 (citing Ex. 1048 ¶ 14; Ex. 1002 ¶ 105).

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

a) Patent Owner’s Challenge to Petitioner’s Rationale for Combining Veselov and Price

As noted above, Petitioner explains that a skilled artisan would have been motivated to combine Veselov’s virtual computing security assessment system with Price’s inactive/at rest security assessments “to provide the well-known security benefit of preventing further damage that might

otherwise be caused if a potentially compromised VM actively runs (e.g., a vulnerability could be exploited, or suspected malware could contaminate other resources).” Pet. 24 (citing Ex. 1048 ¶ 14; Ex. 1002 ¶ 105). Patent Owner asserts that Petitioner’s rationale for combining Veselov and Price is flawed because “Veselov never mentions offline VMs or analyzing offline VMs,” and Price’s inactive/at-rest scans are contrary to Veselov’s “purpose of keeping VMs active and running during security assessments.” PO Resp. 20; *see id.* at 31 (arguing that “Veselov’s invention and goal is for ‘the assessment’ to be ‘performed without impacting the customer’s virtual machine’” (quoting Ex. 1007, 12:21–43)); PO Sur-reply 6–7. Patent Owner further asserts “incompatibilities” and “differences” between Price’s agent-based scans for VM images and Veselov’s agentless, snapshot-based scans. PO Resp. 21–22; *see* PO Sur-reply 7–8.

We disagree with Patent Owner’s arguments. Given Petitioner’s rationale outlined above of preventing further damage, 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 Price’s offline/inactive scanning comes at a cost of keeping VMs active and running, that tradeoff would not necessarily undermine Petitioner’s proffered combination given Petitioner’s articulated benefits regarding preventing further damage. *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, “[o]ur precedent . . . does not require that the motivation be the best option, only that it be a suitable option from which the prior art did not teach away.” *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1197–98 (Fed. Cir. 2014). Although Veselov discloses some benefits of keeping VMs online/active when performing security assessments, it also discloses other examples of performing security assessments that are agnostic as to whether the VMs are active or inactive. *See* Ex. 1007, 3:44–67, 16:45–53, Fig. 4. Thus, Veselov does not preclude offline scans, 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.”). Last, Patent Owner’s arguments distinguishing Price’s agent-based image scans versus Veselov’s agentless snapshot scans likewise does not undermine Petitioner’s proffered combination because it incorrectly assumes that Petitioner proposes bodily incorporating Price’s agent-based image scan into Veselov. That is not what Petitioner proposes. *See* Pet. Reply 7–8 (explaining that Petitioner does not propose bodily incorporating Price’s agent-based or image-based approach); *see also* Pet. 23–25 (describing Veselov’s agentless, snapshot-based approach and Price’s offline analysis).

Lastly, 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 Price. PO Resp. 23. We disagree. Specifically, Petitioner explains, with relevant support from its expert and

the prior art, that “[o]ffline snapshotting and offline analysis were routine and predictable.” Pet. 25 (citing Exs. 1002, 1073, 1081). “Moreover,” Petitioner explains, “most of Veselov’s snapshot-generation and analysis techniques require no interaction with the original VM and, as a result, the state of the original VM could be inactive or at rest when the snapshot is taken and while the snapshot analysis is being performed.” *Id.* (citing Exs. 1002, 1007). Patent Owner’s argument that Petitioner ignores specific claim elements in its reasonable expectation of success analysis (*see* PO Resp. 23) does not undermine Petitioner’s showing because it incorrectly assumes that Petitioner proposes combining separate embodiments from Veselov. Given Petitioner’s evidence, we find Petitioner has shown a skilled artisan would have a reasonable expectation of success in making the proposed combination.

b) Element [1.i]

The preamble of independent claim 1 recites “[a] system for inspecting data, the system comprising: at least one processor configured to.” Ex. 1001, 10:44–45. Independent claims 9 and 16 include similar preambles requiring a “computer-implemented method for inspecting data” (claim 9) and a “non-transitory computer-readable medium storing instructions” (claim 16). *Id.* at 11:22–23; 12:22–23. Petitioner asserts that, to the extent these preambles are limiting, Veselov teaches them because Veselov’s system includes servers with processors and memory and computer-executable instructions configured to perform the described techniques. Pet. 25–26 (citing Ex. 1007, Abstract, Fig. 2, ¶¶ 108–114). Patent Owner does not challenge Petitioner’s showing in this regard. Based

on Petitioner’s analysis outlined above, we agree with Petitioner that Veselov teaches the independent claims’ preambles.

c) Element [1.1]

Element [1.1] recites “establish an interface between a client environment and security components.” Ex. 1001, 10:46–47. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:24–25, 12:24–25. Petitioner contends that Veselov teaches this limitation in at least two ways. Pet. 27. First, Petitioner argues that Veselov teaches this limitation by establishing communication channels between a scanning service and a client environment using an API-mediated interface. *Id.* at 27–28 (citing Ex. 1007, 4:19–29, 4:59–6:6, 8:52–62, 10:37–41, 10:48–53, 10:67–11:4, 16:15–18, 16:56–67, 18:16–18, 18:56–59, 24:54–25:2, Figs. 1, 3A, 3B, 5A, 5B; Ex. 1002 ¶¶ 91, 121–124). Second, Petitioner argues that Veselov teaches this limitation by establishing a user interface (“UI”) between a scanning service and an environment managed by the user, which includes the user’s device and the virtual computing environment in which the user’s VM resides. *Id.* at 28 (citing Ex. 1007, 4:11–5:8, 6:25–38, 10:30–32, 14:37–53; Ex. 1002 ¶ 129). According to Petitioner, “[t]his interface allows the user to configure/perform security scans and receive the assessment results.” *Id.* (citing Ex. 1007, 4:11–14, 5:5–8, 6:38–43, 8:48–51, 14:37–41, 15:3–27; Ex. 1002 ¶¶ 119–120).

Patent Owner does not challenge Petitioner’s showing for this element. Based on Petitioner’s analysis outlined above, we agree with Petitioner that Veselov teaches “establish[ing] an interface between a client environment and security components,” as claimed.

d) Element [1.2]

Element [1.2] requires “using the interface, utiliz[ing] cloud computing platform APIs to identify virtual disks of virtual machine.” Ex. 1001, 10:48–49. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:26–27, 12:27–28. Petitioner contends that Veselov teaches this limitation in at least two ways. Pet. 29. First, Veselov teaches this limitation because it discloses that “[u]sers can request a security assessment by identifying a target VM hosted in a virtual computer environment . . . and that VM can have multiple virtual disks.” Pet. 29 (citing Ex. 1007, 3:20–40, 6:30–43, 9:55–62, 11:31–32, 11:37–46, 16:21–23, Figs. 3A, 3B, 5A 5B). Petitioner asserts that Veselov’s “scanning service would first identify the virtual disks that will be part of the snapshot, particularly since the user may simply provide the scanning service with an identifier of the VM.” *Id.* at 30 (citing Ex. 1007, 6:30–43, Ex. 1002 ¶ 124). Second, Veselov also teaches this limitation because it discloses an “API-based UI [user interface] [that] can be used to select assessment targets and other assessment parameters,” and that through this UI, the user can “perform general management of ‘virtual resource allocations.’” *Id.* at 32 (citing Ex. 1007, 4:19–48, 5:1–8, 14:37–15:29). According to Petitioner, Veselov teaches or suggests the claimed “utiliz[ing] cloud computing platform APIs” to identify the virtual disks because Veselov teaches that the “[t]he scanning service communicates with the target resource’s environment via API calls” and “that the target environment can be part of a cloud computing platform.” *Id.* at 30 (citing Ex. 1007, 2:22–67, 5:1–5, 5:59–60); *see id.* at 32–33.

Patent Owner contends that Veselov does not teach this element because Veselov separately discloses “the identification of a VM,” “the identification of a snapshot,” and “what a snapshot can contain,” but Veselov “never discloses identifying a virtual disk of a VM using cloud computing platform APIs.” PO Resp. 24. Patent Owner also asserts Petitioner’s analysis improperly relies on distinct features from the embodiments illustrated in Veselov’s Figures 1, 3A, 3B, 5A, and 5B, without providing a sufficient rationale to combine these separate embodiments. PO Resp. 14–20. 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 34–42; *compare* PO Resp. 14–20, 24–29 *with* IPR2024-00865, Paper 32 at 10–14, 21–25. For the same reasons explained in IPR2024-00865, we agree with Petitioner that Veselov teaches “using the interface, utiliz[ing] cloud computing platform APIs to identify virtual disks of virtual machine,” as claimed. IPR2024-00865, Paper 84 at 38–42.

e) Element [1.3]

Element [1.3] requires “us[ing] the computer platform APIs to query a location of at least one of the identified virtual disks.” Ex. 1001, 10:51–52. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:29–30, 12:30–31. Petitioner contends that Veselov teaches this limitation because a person of ordinary skill in the art would have understood that “Veselov’s scanning service . . . queries the location of the identified virtual disks so that it can locate them when generating a snapshot that includes those disks.” Pet. 33 (citing Ex. 1007, 9:25–28; Ex. 1002 ¶ 134). According to Petitioner,

these “disk-location queries were a well-known feature of standard cloud computing platform APIs . . . and virtual-disk locations were routinely determined using such queries for snapshot-generation purposes and for VM management generally.” *Id.* at 33–34 (citing Ex. 1002 ¶ 135). Petitioner also asserts that using APIs to query the VM’s endpoint/network address “was an obvious way to determine that information so that the scanning service can perform [certain] functions,” such as generating a snapshot or monitoring the VM’s activity/connections. *Id.* at 34 (citing Ex. 1007, 9:17–25, 10:48–11:4, 15:41–16:14; Ex. 1002 ¶¶ 136, 137).

Patent Owner contends that Petitioner’s position that Veselov’s scanning service may “generate the snapshot itself” is inapposite because, if correct, “[the scanning service] does not query the location of any disk using cloud APIs as claimed.” PO Resp. 29. We addressed this same issue based on the same arguments and evidence in our Final Written Decision in IPR2024-00865. IPR2024-00865, Paper 84 at 42–44; *compare* PO Resp. 29 *with* IPR2024-00865, Paper 32 at 25–26. For the same reasons explained in IPR2024-00865, we agree with Petitioner that Veselov teaches “us[ing] the computer platform APIs to query a location of at least one of the identified virtual disks,” as claimed. IPR2024-00865, Paper 84 at 43–44.

f) Element [1.4]

Element [1.4] requires “receiv[ing] an identification of the location of the virtual disks of the virtual machine.” Ex. 1001, 10:53–54. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:31–32, 12:32–33. Petitioner contends that Veselov teaches this limitation in at least two ways. Pet. 35. First, Petitioner contends that Veselov teaches this limitation

because it discloses receiving the identification of the location of the virtual disks (e.g., an address or endpoint of the virtual disks) in response to a location query as “[disk-location] queries routinely returned an identification of the requested disk location.” *Id.* (citing Ex. 1002 ¶ 139). Second, Petitioner argues that Veselov teaches this limitation because it discloses receiving the identification of the location of the virtual disks as a result of facilitating various communications with the VM. *Id.* According to Petitioner, because Veselov’s scanning service may access the VM’s resources when generating a snapshot or monitoring the VM’s activity/traffic, it would have been obvious for the scanning service to receive an identification of the VM’s virtual network address to facilitate these interactions. *Id.* at 35–36 (citing Ex. 1007, 4:59–5:5, 10:48–11:4; Ex. 1002 ¶¶ 140, 141).

Patent Owner disputes this limitation by reiterating its argument that Veselov’s general disclosure of querying and identifying a virtual network address of a VM does not result in querying and identifying the location of a virtual disk of the VM. PO Resp. 29–30. We addressed this same issue based on the same arguments and evidence in our Final Written Decision in IPR2024-00865. *See* IPR2024-00865, Paper 84 at 45–47; *compare* PO Resp. 29–30 *with* IPR2024-00865, Paper 32 at 26–27. For the same reasons explained in IPR2024-00865, we agree with Petitioner that Veselov teaches “receiv[ing] an identification of the location of the virtual disks of the virtual machine,” as claimed. IPR2024-00865, Paper 84 at 45–47.

g) Element [1.5]

Element [1.5] requires “perform[ing] at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time.” Ex. 1001, 10:55–59. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:34–38, 12:35–39. Petitioner asserts that Veselov teaches the first alternative because it teaches a service that “obtain[s] and analyze[s] snapshot data 146.” Pet. 37 (quoting Ex. 1007, 6:25–30); *see id.* at 37–38. In addition, Petitioner asserts that even under Patent Owner’s construction requiring the VM to be at rest in the first alternative, the combination of Veselov and Price teaches this feature because Veselov teaches taking a “snapshot” of a VM, whereas Price teaches “obtaining and analyzing images of offline [i.e., at rest] VMs.” Pet. 37–38 (citing Ex. 1007, 3:20–27, 9:14–16, 16:15–26; Ex. 1048 Abstract, ¶¶ 14, 29, 32, 42, 45, Figs. 1–6). Further, Petitioner explains that together, Veselov and Price teach the second “requesting” alternative because “Veselov’s scanning service can obtain the snapshot ‘by requesting another service to capture the snapshot and provide it to the scanning service,’” and, as outlined above, Price teaches analyzing VMs at rest. *Id.* at 39 (quoting Ex. 1007, 9:19–22). Last, Petitioner explains that “Veselov teaches ‘wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time’” because Veselov’s “snapshot represents the ‘state of the resource at a point in time.’” *Id.* at 40 (citing Ex. 1007 3:22–40, 9:14–16, 9:42–55).

In challenging element [1.5], Patent Owner reiterates its argument that Petitioner’s rationale for combining Veselov and Price fails. *See* PO Resp. 31 (arguing that “Wiz’s failure to show obviousness of these limitations directly follows from its inability to show a motivation to combine Veselov and Price”); *see id.* at 32–33; *see also* PO Sur-reply 11. Patent Owner’s arguments do not undermine Petitioner’s obviousness showing for two reasons. First, we disagree with Patent Owner’s challenge to Petitioner’s rationale for combining Veselov and Price for the reasons explained above in Section III.A.1.a. Second, even if Patent Owner is correct that skilled artisans would not combine Veselov and Price, that does not undermine Petitioner’s showing that Veselov alone teaches the first alternative under our claim construction, which does not require the VM to be at rest.

Based on Petitioner’s analysis outlined above, we agree with Petitioner that Veselov teaches taking at least one snapshot, as claimed in the first alternative of element [1.5]. We further agree with Petitioner that its asserted combination of Veselov and Price teaches the second alternative requiring requesting taking a snapshot of a VM at rest. Thus, we agree with Petitioner that the asserted combination of Veselov and Price teaches “perform[ing] at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time,” as claimed.

h) Element [1.6]

Element [1.6] requires “analyz[ing] the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive.”

Ex. 1001, 10:60–63. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:39–42, 12:40–43. Petitioner asserts that, together, Veselov and Price teach this limitation because Veselov teaches “the scanning service 110 may obtain and **analyze snapshot data**,” to identify “vulnerabilities, bad configurations, and the like.” Pet. 41, 42 (quoting Ex. 1007, 4:49–54, then quoting *id.* at 1:46–49). In addition, “Price expressly teaches obtaining and analyzing images of offline VMs.” *Id.* at 44.

Other than the arguments already addressed above, Patent Owner does not additionally challenge Petitioner’s showing for element [1.6]. *See* PO Resp. 32–33. Based on Petitioner’s analysis outlined above, we agree with Petitioner that the asserted combination of Veselov and Price teaches the claimed “[analyze/analyzing] the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive,” as claimed.

i) Element [1.7]

Element [1.7] requires “report[ing] the detected vulnerabilities as alerts.” Ex. 1001, 10:64. Independent claims 9 and 16 include parallel limitations. *Id.* at 11:43, 12:44. Petitioner asserts that Veselov teaches this limitation because Veselov “produces assessment results describing the

identified risks” and “provid[es] these assessment results to the user. Pet. 45 (citing Ex. 1007, 10:17–36). Patent Owner argues Veselov’s assessment reporting is not an alert because reports and alerts are distinct. *See* PO Resp. 34 (arguing that “[a] report and an alert ***must mean different things***” and “alerts are different than reports”).

We agree with Petitioner that Veselov’s assessment results teach the claimed alerts. Beyond a generic assessment, Veselov teaches producing an “assessment result *describing a security vulnerability*.” Ex. 1007, 20:67–21:1. Thus, even if Patent Owner is correct that “reporting results does not constitute reporting vulnerabilities ‘as alerts,’” PO Resp. 34, we agree with Petitioner that Veselov’s specific report describing a security vulnerability is an alert, as claimed. Thus, based on Petitioner’s analysis outlined above, we agree with Petitioner that Veselov teaches “report[ing] the detected vulnerabilities as alerts,” as claimed.

j) *Elements [9.5] and [16.5]*

In addition to limitations that parallel independent claim 1, independent claims 9 and 16 also require “[emulating/emulate] the virtual disks for the virtual machine.” Ex. 1001, 11:33, 12:34. Petitioner asserts Veselov teaches this feature because in Veselov, “the virtual disks are emulated by the system by virtualizing the underlying physical memory and assigning it to the VM,” which is “consistent with the ’031 patent specification’s discussion of emulating.” Pet. 36–37 (citing Exs. 1001, 1002, 1007). Patent Owner does not challenge Petitioner’s showing in this regard. Based on Petitioner’s analysis outlined above, we agree with

Petitioner that Veselov teaches “[emulating/emulate] the virtual disks for the virtual machine,” as claimed.

k) Dependent Claims 4 and 12

Dependent claims 4 and 12 recite “wherein the identification of the location of the virtual disks of the virtual machine includes a virtual address of at least one of the virtual disks.” Ex. 1001, 11:4–6, 12:6–8. Petitioner contends that Veselov teaches this limitation because it discloses that the “scanning service receives an identification of the virtual disks’ location in order to access those disks.” Pet. 47 (citing Ex. 1007, 8:16–45, 9:17–25). Petitioner further argues that Veselov teaches that the identification of the virtual disks’ location includes a virtual address in the following ways: (1) Veselov’s scanning service obtains the virtual network address of a targeted VM, to which the virtual disks are allocated, to facilitate communicate between the scanning service and the targeted VM; and (2) it would have been obvious for the identification of the targeted VM to include “more particularized” locations of the virtual disks that are included in a snapshot because it was commonplace to provide the virtual network addresses of virtual disks associated with managed VMs as part of the snapshot-generation process. *Id.* at 47–48 (citing Ex. 1007, 4:19–5:5, 9:17–25, 10:48–11:4, 15:41–59, 16:3–14; Ex. 1002 ¶¶ 28–30, 179–182).

Patent Owner contests that Veselov’s disclosure of obtaining the virtual network addresses of VMs does not teach identifying “a virtual address of at least one of the virtual disks,” as claims 4 and 12 require. PO Resp. 35 (citing Ex. 2073 ¶¶ 157–159). We addressed this same issue based on the same arguments and evidence in our Final Written Decision in

IPR2024-00865. *See* IPR2024-00865, Paper 84 at 120–122; *compare* PO Resp. 35 *with* IPR2024-00865, Paper 32 at 34. For the same reasons explained in IPR2024-00865, we agree with Petitioner that the additional limitation in dependent claims 4 and 12 would have been obvious over Veselov. IPR2024-00865, Paper 84 at 121–122.

l) Remaining Dependent Claim Limitations

Petitioner asserts that Veselov also teaches the limitations in dependent claims 3, 5–8 and 11, and 13–15 including implementing a remedial action (claims 3 and 11), a change log to restore the virtual machine to a particular point in time (claims 5 and 13), generating a plurality of snapshots according to a predetermined schedule (claims 7 and 15), and generating a snapshot in response to a predetermined trigger event (claim 8). Pet. 46–54. Other than the arguments addressed above, Patent Owner does not additionally challenge Petitioner’s obviousness analysis for claims 3–8 and 11–15. *See, e.g.*, PO Resp. 35. We have reviewed Petitioner’s arguments and evidence and, based on that analysis, we agree with Petitioner that the asserted combination of Veselov and Price teaches the additional limitations in dependent claims 3–8 and 11–15.

B. Ground 2: Obviousness of Claims 2 and 10 based on Veselov, Price, and Hufsmith

Dependent claim 2 requires “wherein reporting the detected vulnerabilities as alerts includes indicating priority levels associated with the detected vulnerabilities.” Ex. 1001, 10:65–67. Dependent claim 10 includes a parallel limitation. *Id.* at 10:44–12:2. Petitioner asserts that Hufsmith teaches this additional feature in several ways, including “[Common

Vulnerabilities and Exposures] and [Common Weakness Enumeration] evaluators” that “report[] the identified vulnerabilities data to the results engine along with respective weights.” Pet. 58. In addition, Hufsmith also teaches “reporting alerts as annotations in a development environment” and that “each annotation ‘may display information about a single security vulnerability’ such as a classification or score indicating the vulnerability’s priority level.” *Id.* at 59 (citing Ex. 1078 ¶¶ 154, 156, 180–182). Petitioner explains that skilled artisans would have been motivated to combine Hufsmith’s prioritized alerts “to obtain known benefits of prioritized alerts” including “rapid identification of which assets are most at risk and which threats and vulnerabilities are the most dangerous.” *Id.* at 57 (citing Ex. 1078 ¶ 138; Ex. ¶ 205).

Patent Owner argues skilled artisans would not have combined Hufsmith’s prioritized alerts with Veselov because Hufsmith is directed to “*pre-deployment* analyses of container images, which is vastly different from security assessments of running VMs.” PO Resp. 63. We disagree with Patent Owner’s argument because highlighting mere differences between Veselov and Hufsmith—i.e., Veselov’s running VMs versus Hufsmith’s pre-deployment analysis of container images—does not undermine Petitioner’s proffered rationale, nor does it suggest that Hufsmith’s prioritized alerts are incompatible with Veselov’s general security-assessment structure. To the contrary, as Dr. Stavrou explains, “containers and VMs are closely related resources, and a POSA would have recognized that the relevant underlying data in container images and VM images—e.g., files, applications, configurations, etc.—and VM snapshots

are analogous, as are the relevant techniques for detecting security issues such as vulnerabilities based on that data, making the aspects of Hufsmith . . . readily applicable to the snapshot-based analysis taught by Veselov.” Ex. 1014 ¶ 53 (citing Ex. 2001 ¶ 201–204) *see also* Ex. 2001, 204 (explaining that “Hufsmith’s prioritization techniques were a natural fit and directly applicable to Veselov’s teachings regarding snapshot-based security assessments” because “Veselov provides a high-level description of detecting security problems and reporting alerts, while Hufsmith elaborates on the detection and reporting of vulnerabilities using similar techniques”). Given Petitioner’s rationale outlined above (i.e., known benefits of prioritized alerts including rapid identification of which assets are most at risk and which threats and vulnerabilities are the most dangerous), 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. *KSR*, 550 U.S. at 418.

Beyond challenging Petitioner’s rationale for its combination, Patent Owner argues Hufsmith does not teach reporting the detected vulnerabilities as alerts as claimed because Hufsmith’s “weights represent only a type of ‘count of the number of potential vulnerabilities detected,’” rather than priority levels. PO Resp. 64. We disagree. Patent Owner does not explain why a detected vulnerabilities count does not fall within the relatively broad claim term at issue—“priority levels associated with the detected vulnerabilities.” Because a higher count would, for example, reasonably reflect a higher priority level, *see* Ex. 1400 ¶ 58, we agree with Petitioner that Hufsmith’s weights teach the additional feature recited in dependent

claims 2 and 10. In addition, Patent Owner’s only challenge to Petitioner’s alternative mapping of Hufsmith’s classifications/scores to the claimed priority levels is that they relate to “annotations in a development environment” rather than to deployed VMs, as in Veselov. *Id.* at 64–65. We disagree with this argument because it assumes bodily incorporating Hufsmith’s source-code annotations with Veselov’s optional read-only snapshot embodiment (*see* Ex. 1007, 18:1–2) and identifies differences in the references (Hufsmith’s development environment vs. Veselov’s running VM) without explaining why Hufsmith’s reporting of priority-level scores for individual vulnerabilities would be incompatible with Veselov’s general security-assessment structure. *See* Ex. 1400 ¶ 59 (explaining that “the combination does not involve a wholesale incorporation of the embodiment into Veselov”). That, however, is neither what Petitioner proposes, nor is it the test for obviousness. *See Allied Erecting & Dismantling Co.*, 825 F.3d at 1381 (explaining that physical combinability and bodily incorporation are not the proper tests for obviousness).

Based on Petitioner’s analysis outlined above, we agree with Petitioner that Hufsmith accounts for the additional limitation of dependent claims 2 and 10 requiring indicating priority levels associated with the detected vulnerabilities. In addition, Petitioner has explained sufficiently why skilled artisans would have included that feature in its Veselov/Price combination, as outlined above.

C. Ground 3: Obviousness of Claims 6 and 14 based on Veselov, Price, Hufsmith, and Huseinović

Dependent claim 6 requires “wherein the snapshot includes a page file of memory associated with the virtual machine, the page file being configured to allow deduction of one or more applications running on the virtual machine.” Ex. 1001, 11:11–14. Dependent claim 14 includes a parallel limitation. *Id.* at 12:14–17. Petitioner asserts Huseinović teaches this additional feature because “Huseinović expressly teaches taking a VM snapshot that includes a page file representing the state of machine memory and using that page file to determine which applications are running.” Pet. 63 (citing Ex. 1049, 940, 941). Petitioner explains that a skilled artisan would have been motivated to apply Huseinović’s teaching to the asserted Veselov-Price-Hufsmith combination “to provide a straightforward way of obtaining information that is useful to the security assessment,” and to facilitate “adjusting risk levels based on application usage.” *Id.* at 62 (citing Ex. 1049, 940–42; Ex. 1002 ¶ 218).

Patent Owner’s only additional challenge to this ground is a one-sentence assertion that skilled artisans would not “further modify [Petitioner’s] Veselov/Price/Hufsmith combination with Huseinović’s teachings, which counsel against collecting offline data.” PO Resp. 65 (citing Ex. 1049, 1). We disagree. To the extent Patent Owner is reiterating that offline scanning comes at a cost to keeping VMs active and running, as we explained above, that tradeoff does not undermine Petitioner’s proffered combination given Petitioner’s articulated benefits related to offline scans, including preventing further damage.

Based on Petitioner's analysis outlined above, we agree with Petitioner that Huseinović teaches the additional feature of dependent claims 6 and 14. In addition, given Petitioner's rationale that Huseinović's machine-memory page file would facilitate adjusting risk levels based on application usage, 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.

D. Objective Indicia

Patent Owner asserts that objective-indicia evidence confirms the non-obviousness of the challenged claims of the '031 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, Orca 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 of the '031 patent, 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 overcomes Petitioner's strong obviousness showing. *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).

E. 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, 3–9, and 11–16 are unpatentable as obvious over Veselov and Price (ground 1), that claims 2 and 10 are unpatentable as obvious over Veselov, Price, and that Hufsmith (ground 2), and that claims 6 and 14 are unpatentable as obvious over Veselov, Price, Hufsmith, and Huseinović (ground 3).

IV. PETITIONER’S MOTION TO EXCLUDE

Petitioner filed a Motion to Exclude that seeks to exclude Exhibits 2134–2137, 2148, 2400–2422, and 2425–2428 as inadmissible under the Federal Rules of Evidence. Paper 52, 1–15.⁵ 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.

V. MOTIONS TO SEAL

Petitioner and Patent Owner request to seal Papers 42, 52, 56, 57, 60, 65, 66, and 68 and Exhibits 1400–1414, 2172, and 2173. Papers 43, 51, 55, 58, 59, 64, 67. After reviewing the Papers and Exhibits, we agree that they

⁵ Paper 52 is the unredacted version of Petitioner’s Motion to Exclude. Petitioner also filed a redacted version of its Motion as Paper 76.

contain business confidential information. Accordingly, Papers 42, 52, 56, 57, 60, 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 1–16 of the ’031 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, 3–9, 11–16	103	Veselov, Price	1, 3–9, 11–16	
2, 10	103	Veselov, Price, Hufsmith	2, 10	
6, 14	103	Veselov, Price, Hufsmith, Huseinović	6, 14	
Overall Outcome			1–16	

VII. IV. ORDER

Accordingly, it is

ORDERED that claims 1–16 of the 031 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.

IPR2024-00863
Patent 11,663,031 B2

For PETITIONER

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

For PATENT OWNER

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