

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-00865
Patent 11,693,685 B2

Before MICHAEL R. ZECHER, GARTH D. BAER, and
BRENT M. DOUGAL, *Administrative Patent Judges*.

ZECHER, *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. (“Wiz”), filed a Petition requesting an *inter partes* review (“IPR”) of claims 1–22 of U.S. Patent No. 11,693,685 B2 (Ex. 1001, “the ’685 patent”). Paper 2 (“Pet.”). Patent Owner, Orca Security Ltd. (“Orca”), filed a Preliminary Response. Paper 6. Taking into account the arguments presented in Orca’s Preliminary Response, the Board determined that the information presented in the Petition established that there was a reasonable likelihood that Wiz would prevail with respect to challenging at least one of claims 1–22 of the ’685 patent. Pursuant to 35 U.S.C. § 314, we instituted this IPR on December 9, 2024, as to claims 1–22 of the ’685 patent based on all grounds raised in the Petition challenging these claims. Paper 8.

During trial, Orca filed unredacted and redacted versions of a Patent Owner Response (Papers 32 and 38, “PO Resp.”), Wiz filed unredacted and redacted versions of a Reply (Papers 42 and 76, “Pet. Reply”), and Orca filed unredacted and redacted versions of a Sur-reply (Papers 60 and 69, “PO Sur-reply”). We granted Orca’s Motion to Seal filed with its Patent Owner Response and entered a Joint Proposed Protective Order. Paper 37; Ex. 2161. The parties also filed Motions to Seal with the Reply and the Sur-reply. Papers 43, 59.

Wiz also filed unredacted and redacted versions of a Motion to Exclude that seeks to exclude Exhibits 2134–2137, 2148, 2152, and 2400–2428 (Papers 52 and 75, “Pet. Mot. to Exclude”), Orca filed unredacted and redacted versions of an Opposition to the Motion to Exclude (Papers 56 and 70), and Wiz filed unredacted and redacted versions of a

Reply to the Opposition to the Motion to Exclude (Papers 57 and 77). The parties also filed Motions to Seal with the Motion to Exclude, the Opposition to the Motion to Exclude, and the Reply to the Opposition to the Motion to Exclude. Papers 51, 55, 58.

In addition, an oral argument was held on September 15, 2025, and unredacted and redacted versions of the transcript of the hearing are included in the record. Papers 78 and 82 (“Tr.”). The parties filed unredacted and redacted versions of their demonstratives for the oral argument. Papers 65, 67, 71, 74. The parties also files Motions to Seal with their demonstratives. Papers 63, 66.

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of claims 1–22 of the ’685 patent. For the reasons we identify below, we hold that Wiz has demonstrated by a preponderance of the evidence that these claims are unpatentable. We also *dismiss* Wiz’s Motion to Exclude as moot. We also *grant* the parties’ Motions to Seal.

A. Real Party in Interest (“RPI”)

Wiz identifies itself as an RPI. Pet. 1; Paper 26 (Wiz’s Updated Mandatory Notices), 1. Orca identifies itself as an RPI. Paper 3 (Orca’s Mandatory Notices), 1.

B. Related Matters

The parties indicate that the ’685 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; Paper 26, 1. In addition to this Petition, Wiz filed another petition challenging a related patent owned by

IPR2024-00865
Patent 11,693,685 B2

Orca in a proceeding titled *Wiz, Inc. v. Orca Security Ltd.*, IPR2024-00220, Paper 2 (PTAB Jan. 8, 2024) (challenging claims 1–7, 9–17, and 19 of U.S. Patent No. 11,431,735 B2 (“the ’735 patent”)). Pet. 2; Paper 26, 1.

In IPR2024-00220, the Board denied institution because Orca disclaimed all the challenged claims of the ’735 patent. *Wiz, Inc. v. Orca Security Ltd.*, IPR2024-00220, Paper 7 (PTAB May 9, 2024) (Decision Denying Institution).

We also note that Wiz challenges related patents owned by Orca in the following five proceedings: (1) IPR2024-00863; (2) IPR2024-00864; (3) IPR2024-01109; (4) IPR2024-01190; and (5) IPR2024-01191. We entered Final Written Decision in IPR2024-00863 and IPR2024-00864 concurrently herewith.

C. The ’685 Patent

The ’685 patent, titled “Virtual Machine Vulnerabilities and Sensitive Data Analysis and Detection,” issued from U.S. Patent Application No. 17/361,861, filed on June 29, 2021. Ex. 1001, codes (54), (21), (22). The ’685 patent is a continuation of U.S. Patent Application No. 16/585,967, which was filed on September 27, 2019—now the ’735 patent—and it claims priority to U.S. Provisional Patent Application No. 62/797,718 (“the ’718 application”), which was filed on January 28, 2019. *Id.* at codes (63), (60).

The ’685 patent generally relates to “cyber-security systems and, more specifically, to techniques for securing virtual machines.” Ex. 1001, 1:14–16. According to the ’685 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” that “emulate[] a number of ‘computers’ or instances, all within a single physical device.” *Id.* at 1:28–30.

The ’685 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.” Ex. 1001, 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 ’685 patent, however, explains that there are certain disadvantages associated with each of these conventional ways of traffic inspection. *Id.*

The ’685 patent ostensibly addresses these disadvantages by providing a method, system, and non-transitory computer readable medium for “securing virtual cloud assets in a cloud computing environment against cyber threats.” Ex. 1001, 2:34–36, 2:45–48, 2:57–59. Figure 1B of the ’685 patent, reproduced below, illustrates a network diagram that implements various embodiments. *Id.* at 3:11–12.

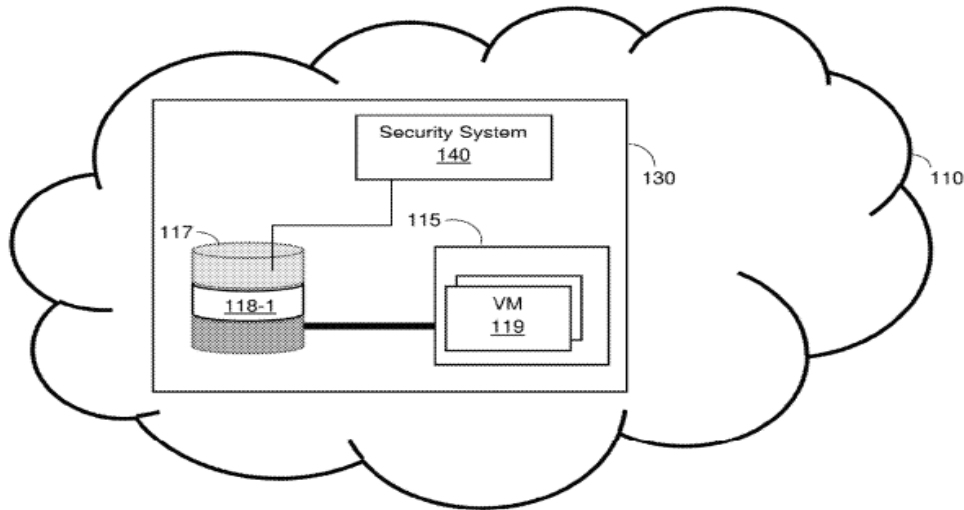


FIG. 1B

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 (“VM”) 119, and security system 140. *Id.* at 3:32–4:14. “[S]ecurity system 140 is configured to detect vulnerabilities and other cyber threats related to the execution of VM 119.” *Id.* at 4:43–45. More specifically, “security system 140 can scan and detect vulnerable software, non-secure configurations, exploitation attempts, compromised assets, data leaks, data mining, and so on,” as well as “provide security services, such as incident response, anti-ransomware, and cyber insurance by accessing the security posture.” *Id.* at 4:48–54.

D. Challenged Claims

Of the challenged claims, claims 1, 13, and 22 are independent. Ex. 1001, 9:33–54, 10:26–47, 11:9–30. Independent claim 1 is illustrative of the challenged claims and is reproduced below.

1. A system for inspecting data, the system comprising: 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] generate at least one snapshot of the virtual disks of the virtual machine;

[1.6] analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine;

[1.7] determine a risk level of the virtual machine; and

[1.8] report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.

Id. at 9:33–54 (with bracket annotations provided by Wiz in the Petition).

E. Asserted Prior Art References

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

IPR2024-00865
Patent 11,693,685 B2

Name ¹	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
Chari	US 2015/0033221 A1	published Jan. 29, 2015; filed July 24, 2013	1056
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

Wiz challenges claims 1–22 of the ’685 patent based on the asserted grounds of unpatentability set forth in the table below. Pet. 3, 21–71.

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–22	103 ²	Veselov, Hufsmith
1–22	103	Veselov, Hufsmith, Chari
2, 3, 14, 15	103	Veselov, Hufsmith, Chari, Price, Huseinović

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

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the ’685 patent claims the benefit of the ’718 application, which was filed after this date, the AIA version of § 103 applies. Ex. 1001, code (60).

II. ANALYSIS

A. Claim Construction

In this IPR, claim terms are construed using the same claim construction standard as in a civil action under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b). That is, claim terms generally are construed in accordance with their ordinary and customary meaning, as would have been understood by a person of ordinary skill in the art, in view of the specification and the prosecution history pertaining to the patent at issue. *See id.* The ordinary and customary meaning of a claim term “is its meaning to the ordinary artisan after reading the entire patent,” and “as of the effective filing date of the patent application.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, 1321 (Fed. Cir. 2005) (en banc).

In its Petition, Wiz proposes that two claim terms require construction. *See* Pet. 9–11. First, Wiz contends that each of independent claims 1, 13, and 22 require querying a “location” of at least one of the identified virtual disks, and that a person of ordinary skill in the art reading these claims in light of the specification of the ’685 would have understood that the claim term “location” “encompasses at least a virtual location and a non-virtual location.” *Id.* at 9; *see also id.* at 9–10 (relying on the specification of the ’685 patent and the supporting testimony of its declarant, Dr. Angelos Stavrou, to support its proposed construction (citing Ex. 1001, 4:27–30; Ex. 1002 ¶¶ 30, 45, 46, 78–80)).

In its Patent Owner Response, Orca does not address Wiz’s proposed construction of the claim term “location,” and we determine it is unnecessary to construe this term. *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))).

Second, Wiz contends that each of independent claims 1, 13, and 22 requires “[analyze/analyzing] the at least one snapshot.” Pet. 10. According to Wiz, the ordinary and customary meaning of this claim term “encompasses direct analysis of the snapshot data (e.g., analyzing the snapshot as a data file without instantiating an assessment VM).” *Id.* To support its proposed construction, Wiz directs us to the specification of the ’685 patent and the supporting testimony of its declarant, Dr. Stavrou. *Id.* (citing Ex. 1001, 5:19–20, 5:36–39, 6:4–11, 6:35–58; Ex. 1002 ¶¶ 81–84). In the related district court case between the parties, Wiz notes that “Orca appears to treat this limitation as also encompassing analysis of a VM instantiated from a snapshot.” *Id.* at 10–11 (citing Ex. 1006 (Second Amended Complaint For Patent Infringement), 23, 57–58). For purposes of this proceeding, Wiz also proposes applying Orca’s interpretation from the related district court case. *Id.* at 11 (citing Ex. 1002 ¶ 83). Accordingly, Wiz argues that we should construe the claim term “[analyze/analyzing] the at least one snapshot” as “encompassing both direct analysis of the snapshot data and analysis of a VM instantiated from the snapshot.” *Id.* (citing Ex. 1002 ¶ 84).

In its Patent Owner Response, Orca acknowledges that Wiz’s proposed construction relies on Orca’s amended complaint in the district court case between the parties, but contends that “[n]othing in Orca’s allegations

[presented in the district court case] indicate that analyzing a VM instantiated from a snapshot is ‘analyzing [a] snapshot’ as claimed.” PO Resp. at 5–6 (citing Ex. 1006, 23, 57–58). Orca argues that, “[o]nce a VM is instantiated from a snapshot, . . . the VM is not a ‘snapshot,’ and monitoring or assessing it is not ‘analyzing’ a ‘snapshot.’” *Id.* at 6. According to Orca, “[t]he specification . . . distinguishes analyzing a snapshot by a ‘security system 140 to detect vulnerabilities’, as claimed, from a system that ‘instantiate[s] a copy of the VM’ and performs ‘execution of the instance of the VM [in] an isolated sandbox.’” *Id.* (first quoting Ex. 1001, 5:19–20, then quoting Ex. 1001, 5:54–67)(citing Ex. 1001, 7:39–49; Ex. 2073 ¶ 46). In addition, Orca argues that Wiz’s declarant, Dr. Stavrou, never supports, and now directly contradicts, Wiz’s proposed construction of the claim term “[analyze/analyzing] the at least one snapshot.” *Id.* at 6–7 (citing Ex. 1002 ¶ 83; Ex. 2077, 265:17–266:4, 266:13–269:20, 280:8–281:1).

In its Reply, Wiz contends that Orca’s claim construction arguments directed to the claim term “[analyze/analyzing] the at least one snapshot” include “numerous contradictions.” Pet. Reply 1 (citing Ex. 1400 ¶ 10). Wiz contends that “[Orca] does not explain contrary positions in its district-court complaint, claim construction briefing, and the specification/provisional.” *Id.* at 1–2 (citing Pet. 10–11; Ex. 1006, 23, 57–58; Ex. 1117, 64, 67–68; Ex. 1001, 7:34–49; Ex. 2149 ¶¶ 22, 43; Ex. 1401, 33:12–36:11; Ex. 1402, 215:5–222:7). Wiz also argues that, in other documents, Orca takes the position that “‘examin[ing] the VMs spun up from the snapshot’ shows Wiz analyzing the snapshot.” *Id.* (citing IPR2024-00864, Paper 32, 54–55; Ex. 1401, 30:15–31:17, 127:7–131:8;

Ex. 1402, 187:2–203:14, 249:11–258:2). In any event, Wiz asserts that the arguments and evidence presented in the Petition do not depend solely on its alternative construction pertaining to the assessment-VM approach. *Id.* at 2.

In its Sur-reply, Orca contends that, if Wiz actually abandons its proposed construction of the claim term “[analyze/analyzing] the at least one snapshot” as encompassing analyzing VMs instantiated from snapshots, we should disregard Wiz’s reliance on Veselov’s assessment VM approach. PO Sur-reply 2 (citing Pet. Reply 1–2; Pet. 15–16, 17–18, 37–40, 67). Orca argues that, if Wiz did not abandon this claim construction position, Wiz’s assessment VM theories are wrong for the reasons it presents in its Patent Owner Response. *Id.* at 2 (citing PO Resp. 10–14).

Based on the complete record, we understand Wiz to propose a construction for the claim term “[analyze/analyzing] the at least one snapshot” that encompasses the following two alternative approaches: (1) “direct analysis of the snapshot data”; and (2) “analysis of a VM instantiated from the snapshot.” *See* Pet. 10–11; Pet. Reply 1–2. We understand Orca to dispute the latter approach, but not the former approach. *See* PO Resp. 5–7; PO Sur-reply 2.

We begin our analysis by reviewing the intrinsic evidence, which includes the specification of the ’685 patent. *See Phillips*, 415 F.3d at 1315 (stating that the specification “is ‘the single best guide to the meaning of a disputed term’” (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996))). The specification discloses that “[v]arious techniques can be utilized to analyze the snapshots, depending on the type of vulnerability and cyber threats to be detected.” Ex. 1001, 5:25–27. The

specification identifies snapshot analysis techniques that may be implemented by security system 140, where one embodiment includes configuring “security system 140 . . . to match the application files, either directly (using binary comparison) or by computing a cryptographic hash against database of files in vulnerable applications.” *Id.* at 5:36–37.

In another embodiment that performs snapshot analysis, the specification discloses that security system 140 “instantiate[s] a copy of the VM 119 and/or a subset of applications of the VM 119 on the server 115 or a separate server and monitor[s] all activity performed by the instance of the VM.” *Id.* at 5:54–58. According to the specification, “[t]he execution of the instance of the VM is an isolated sandbox” and “[t]he monitored activity may be further analyzed to determine abnormality,” where “[s]uch analysis” includes “monitoring of API activity, process creation, file activity, network communication, registry changes, and active probing of the said subset in order to assess its security posture.” *Id.* at 5:58–66.

Later, when describing flowchart 200 illustrated in Figure 2, the specification discloses that, “[a]t S240, the snapshot is analyzed to detect cyber threats and potential vulnerabilities.” Ex. 1001, 7:34–35, Fig. 2 (step 240). The specification discloses that step 240 may include the following:

comparing the snapshot to some baseline, which may include, but is not limited to, a copy of the image used to create the VM (e.g., lists of applications, previous snapshots), cryptographic hashes gathered in the previous scan, analyzing logs of the VMs, instantiating a copy of the VM and executing the instance or application executed by the VM in a sandbox, analyzing the machine memory, as reflected in the page file, or any combination of these techniques.

Id. at 7:39–47. This portion of the specification concludes by stating “[s]ome example embodiments for analyzing the snapshots . . . are provided above.” *Id.* at 7:47–49.

Based on our review of the specification of the ’685 patent, we find that it discloses more than one snapshot analysis technique. As one example, analyzing a snapshot may be done through direct analysis of snapshot data, such as by using binary comparison or computing a cryptographic hash to directly match application files against a database of files in vulnerable applications. As another example, analyzing a snapshot may be done through instantiating a copy of a VM or a subset of applications of the VM and monitoring all activity performed by the instance of the VM. Although the specification discloses executing the instance of the VM in a sandbox, there is nothing in the challenged claims that would suggest that analyzing a snapshot cannot be done in this way. In our view, these two embodiments disclosed in the specification of the ’685 patent support Wiz’s proposed construction of the claim term “[analyze/analyzing] the at least one snapshot” as encompassing the following two alternative approaches: (1) “direct analysis of the snapshot data”; and (2) “analysis of a VM instantiated from the snapshot.”

We do not agree with Orca’s argument that the specification of the ’685 patent distinguishes between security system 140 analyzing a snapshot to detect vulnerabilities and security system 140 instantiating a copy of the VM and performing execution of the instance of the VM in a sandbox. *See* PO Resp. 6. Although the specification discloses various snapshot analysis techniques implemented by security system 140, security system 140 is

capable of using all the disclosed techniques to analyze a snapshot. This notion is further reinforced through the specification's disclosure of step 240 in flowchart 200 illustrated in Figure 2. As we explain above, the specification describes step 240 by listing more than one snapshot analysis technique. *See* Ex. 1001, 7:39–49. Notably, those snapshot analysis techniques include at least two techniques that align with the two alternative approaches proposed by Wiz—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).

We also do not agree with Orca's argument that Wiz's declarant, Dr. Stavrou, never supports, and directly contradicts, Wiz's proposed construction of the claim term “[analyze/analyzing] the at least one snapshot.” *See* PO Resp. 6–7. Although Dr. Stavrou testifies that he assumes that the claim term “[analyze/analyzing] the at least one snapshot” encompasses analysis of a VM instantiated from the snapshot without providing further analysis, Orca does not direct us to, nor can we find, additional testimony from Dr. Stavrou that contradict Wiz's claim construction position. *See* Ex. 1002 ¶ 83. As we explain above, the specification of the '685 patent supports Wiz's two alternative approaches for “[analyze/analyzing] the at least one snapshot.” When, as here, the intrinsic evidence is sufficient to enable us to determine the scope and meaning of a particular claim term, we need not rely on extrinsic evidence, such as Dr. Stavrou's testimony. *See Vitronics Corp.*, 90 F.3d at 1583 (“In most situations, an analysis of the intrinsic evidence alone will resolve any

ambiguity in a disputed claim term. In such circumstances, it is improper to rely on extrinsic evidence.”); *see also id.* at 1584 (“[E]xtrinsic evidence in general, and expert testimony in particular, may be used only to help the court come to the proper understanding of the claims; it may not be used to vary or contradict the claim language.”).

In summary, upon weighing all the evidence bearing on the construction of the claim term “[analyze/analyzing] the at least one snapshot,” we determine that the intrinsic evidence supports Wiz’s proposed construction of this claim term as encompassing the following two alternative approaches: (1) “direct analysis of the snapshot data”; and (2) “analysis of a VM instantiated from the snapshot.”

B. Obviousness over the Combined Teachings of Veselov and Hufsmith

Wiz contends that claims 1–22 of the ’685 patent are unpatentable under 35 U.S.C. § 103 as obvious over the combined teachings of Veselov and Hufsmith. Pet. 21–59. Wiz contends that the combined teachings of Veselov and Hufsmith account for the subject matter of each challenged claim, and Wiz provides reasoning as to why a person of ordinary skill in the art would have been prompted to modify the teachings of these references. *Id.* To support its positions, Wiz submits a first Declaration of Dr. Stavrou with the Petition, a second Declaration of Dr. Stavrou with the Reply, and a Declaration of Amit Luttwak with the Reply. *See* Exs. 1002, 1400, 1414.

Orca contends that the combined teachings of Veselov and Hufsmith do not account for elements 1.1–1.4, 1.6, and 1.8. PO Resp. 20–33; PO Sur-reply 9–13. Orca also argues that Wiz improperly relies on a combination of Veselov’s embodiments, and it does not provide a sufficient

rationale to combine the teachings of Veselov and Hufsmith. PO Resp. 10–20; PO Sur-reply 2–9. In addition, Orca presents arguments and evidence of objective indicia of non-obviousness, which, according to Orca, confirms the patentability of the challenged claims. PO Resp. 34–62; PO Sur-reply 15–35. To support its positions, Orca submits the Declarations of Dr. David Kaeli and Mr. Avi Shua with the Patent Owner Response. *See* Exs. 2073, 2074.

Based on the complete record, we determine that Wiz has shown by a preponderance of the evidence that claims 1–22 of the '685 patent are unpatentable as obvious over the combined teachings of Veselov and Hufsmith. We begin our analysis with the principles of law that generally apply to an asserted ground based on obviousness, we then assess the level of skill in the art, next we provide overviews of Veselov and Hufsmith, and then we turn to the parties' contentions with respect to the challenged claims.

1. Principles of Law

A claim is unpatentable as obvious “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in

evidence, objective indicia of obviousness or non-obviousness (i.e., secondary considerations, such as commercial success, long-felt but unsolved need, failure of others, etc.). *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966). We analyze the asserted grounds based on obviousness with the principles we identify above in mind.

2. *Level of Skill in the Art*

In determining whether an invention would have been obvious, we consider the level of ordinary skill in the pertinent art at the relevant time. *Graham*, 383 U.S. at 17. “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The “person having ordinary skill in the art” is a hypothetical construct, from whose vantage point obviousness is assessed. *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998).

Factors pertinent to a determination of the level of ordinary skill in the art include “(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field.” *Env’t Designs, Ltd. v. Union Oil Co. of Cal.*, 713 F.2d 693, 696 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). “Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case.” *Id.* at 696–97.

Relying on the testimony of Dr. Stavrou, Wiz 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. 8 (citing Ex. 1002 ¶¶ 21, 22). In its Patent Owner Response, Orca does not provide its own assessment of the level of skill in the art, nor does Orca dispute Wiz's assessment of the level of skill in the art. *See* PO Resp.

We adopt Wiz's assessment of the level of skill in the art, 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. Without the qualifier, Wiz's assessment of the level of skill in the art is (1) consistent with the '685 patent and the asserted prior art; and (2) supported by the testimony of Dr. Stavrou.

3. Overview of Veselov

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”).

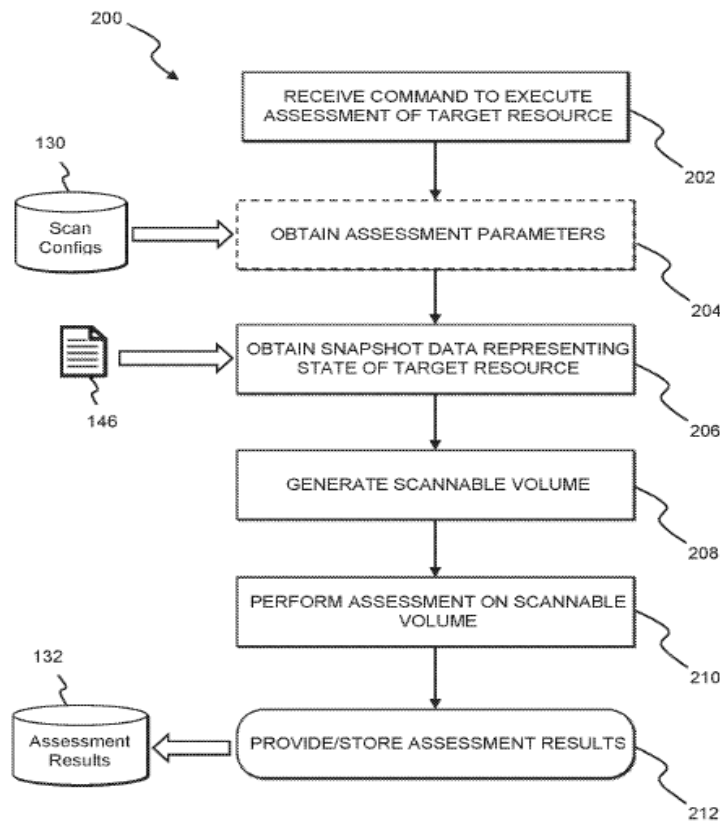


FIG. 2

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.

4. Overview of Hufsmith

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 have different weights corresponding to different vulnerabilities or types of vulnerabilities in a taxonomy of vulnerabilities.” *Id.* ¶ 91.

5. Claims 1, 13, and 22

Our analysis below focuses on the limitations of independent claim 1 by relying on the bracketed annotations provided by Wiz in the Petition. *See* Pet. iv–vii, 26–45. For the most part, the same arguments and evidence Wiz provides to explain how the combined teachings of Veselov and Hufsmith account for all the limitations of independent claim 1 equally apply to the

corresponding limitations of independent claims 13 and 22. *See id.* at 26–45.

The preamble of claim 1 recites [1]—“[a] system for inspecting data, the system comprising.” Ex. 1001, 9:33. To the extent the preamble is treated as limiting, Wiz contends that Veselov teaches the features recited therein because it discloses “a system for performing a security assessment of a target VM, which includes analyzing snapshot data of a target VM (i.e., ‘inspecting data’).” Pet. 26 (citing Ex. 1007, code (57), Figs. 1–7; Ex. 1002 ¶¶ 114, 115).

Element 1.i recites “at least one processor configured to” perform certain steps. Ex. 1001, 9:33–34. Wiz contends that Veselov teaches this limitation because its system includes servers with one or more processors configured to perform security assessment techniques. Pet. 27 (citing Ex. 1007, 4:60–51, 5:23–40, 20:38–23:18, claim 1; Ex. 1002 ¶ 120).

Element 1.1 recites “establish an interface between a client environment and security components.” Ex. 1001, 9:35–36. Wiz contends that Veselov teaches this limitation in at least two ways. Pet. 27. First, Wiz argues that Veselov teaches this limitation by establishing communication channels between a scanning service and a client environment using an API-mediated interface (hereinafter referred to as “communication interface” mapping). *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, Wiz 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 (hereinafter referred to as "UI" mapping). *Id.* at 28–29 (citing Ex. 1007, 4:11–5:8, 6:25–38, 10:30–32, 14:37–53; Ex. 1002 ¶ 125). According to Wiz, "this interface allows the user to configure/perform security scans and receive 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 ¶¶ 125, 126).

Element 1.2 recites "using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment." Ex. 1001, 9:37–39. Consistent with its mapping of element 1.1, Wiz contends that Veselov teaches this limitation in at least two ways. Pet. 29. First, with respect to the communication interface mapping, Wiz argues that Veselov teaches this limitation because it discloses that the scanning service uses the communication interface to request a snapshot security assessment by identifying a target VM hosted in a virtual computer environment, which may have multiple logical volumes referred to as virtual disk drives. *Id.* at 29–30 (citing Ex. 1007, 3:20–40, 6:30–38, 9:55–62, 11:31–32, 11:37–46, 15:15–27, 16:21–23, Figs. 3A, 3B, 5A, 5B; Ex. 1002 ¶¶ 127, 128). Wiz asserts that Veselov's "scanning service would 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, 15:15–27; Ex. 1002 ¶¶ 129, 130). According to Wiz, Veselov teaches or suggests the claimed "utiliz[ing] cloud computing platform APIs" to identify the virtual disks because the scanning service communicates using API calls over the communication

interface, and “APIs for identifying a VM’s virtual disks were a well-known feature of virtualization platforms used in cloud [computing] systems.” *Id.* at 30–31 (citing Ex. 1007, 2:22–3:19, 5:1–5, 5:41–60, 19:30–37, 19:60–64, 20:46–56; Ex. 1002 ¶¶ 42, 45, 46, 125, 131, 132).

Second, with respect to the UI mapping, Wiz argues that Veselov teaches element 1.2 because it discloses that API-based UI selects assessment targets and other parameters, and the API-based UI performs general management of “virtual resource allocations.” Pet. 32–33 (quoting Ex. 1007, 4:19–48) (citing Ex. 1007, 5:1–8, 14:37–15:29; Ex. 1002 ¶¶ 136, 137). According to Wiz, a person of ordinary skill in the art would have understood that Veselov’s UI mapping uses APIs that amount to “cloud computing APIs” for the same reasons that Wiz identifies above with respect to its communication interface mapping. *Id.* at 33 (citing Ex. 1007, 2:22–3:19, 19:30–37, 19:60–64, 20:46–56; Ex. 1002 ¶¶ 135–138).

Element 1.3 recites “use the computer platform APIs to query a location of at least one of the identified virtual disks.” Ex. 1001, 9:40–41. Wiz 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, 9:9–28; Ex. 1002 ¶ 140). According to Wiz, “[d]isk-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.* (citing Ex. 1002 ¶ 141). Wiz also argues that

Veselov teaches or suggests using “APIs to query an endpoint/network address of the VM to which the disks are allocated.” *Id.* at 34. Wiz asserts that using APIs to query the VM’s endpoint/network address “was an obvious way to determine this information so that the scanning service can perform [certain] functions,” such as generating a snapshot or monitoring the VM’s activity/connections. *Id.* (citing Ex. 1002 ¶¶ 142, 143).

Element 1.4 recites “receive an identification of the location of the virtual disks of the virtual machine.” Ex. 1001, 9:42–43. Wiz contends that Veselov teaches this limitation in at least two ways. Pet. 34. First, Wiz argues that Veselov teaches this limitation (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.* at 34–35 (citing Ex. 1002 ¶¶ 144, 145). Second, Wiz 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.* at 35. According to Wiz, because Veselov’s scanning service may access the VM’s resources when generating a snapshot or when 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.* (citing Ex. 1007, 4:59–5:5, 10:48–11:4; Ex. 1002 ¶¶ 146, 147).

Element 1.5 recites “generate at least one snapshot of the virtual disks of the virtual machine.” Ex. 1001, 9:44–45. Wiz contends that Veselov teaches this limitation because it discloses generating and analyzing snapshots that include representations of the VM’s logical volumes, also

referred to as virtual disk drives. Pet. 35 (citing Ex. 1007, code (57), 2:27–35, 3:20–40, 8:52–9:25, 9:42–67, 11:5–67, 16:15–26, 16:56–17:8, 18:16–26, Figs. 2, 4, 6; Ex. 1002 ¶¶ 148, 149).

Element 1.6 recites “analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine.” Ex. 1001, 9:46–49. Wiz contends that the combination of Veselov and Hufsmith teaches or suggests this limitation. Pet. 37. Wiz argues that Veselov’s scanning service obtains and analyzes snapshot data. *Id.* (citing Ex. 1007, 4:49–54, 8:16–51, Figs. 1, 2, 3A, 3B, 4, 5A, 5B, 6). According to Wiz, Veselov discloses the following two ways to perform the snapshot analysis: (1) the scanning service analyzes a duplicate/assessment VM instantiated from the snapshot; and (2) the scanning service directly analyzes the snapshot data. *Id.* at 37–38 (citing Ex. 1007, 3:44–67, 8:30–45, 10:1–16, 12:1–20, 17:10–29, Figs. 3A, 3B; Ex. 1002 ¶¶ 153–157). Wiz asserts that both of Veselov’s ways of performing the snapshot analysis detects the claimed “vulnerabilities.” *Id.* at 38–39 (citing Ex. 1007, 1:46–49, 2:22–41, 2:46–54, 4:1–18, 4:57–59, 5:9–11, 7:1–4, 10:17–36, 14:41–15:3, 20:57–21:3, 23:19–24:4, claims 1, 16–18; Ex. 1002 ¶ 158).

Wiz also argues that the combination of Veselov and Hufsmith teaches or suggests snapshot analysis that results in detecting the claimed “sensitive data.” Pet. 39. According to Wiz, because Veselov’s scanning service can use “any suitable security assessment,” it is capable of implementing Hufsmith’s static and dynamic analysis of a container image. *Id.* (quoting Ex. 1007, 2:22–54) (citing Ex. 1007, 14:41–65; Ex. 1078 ¶¶ 82,

105, 149, 228, claim 9). Wiz further argues that Hufsmith’s security assessment “identifies potential exposure of various types of sensitive data such as ‘confidential information’ and ‘information about an encryption key.’” *Id.* (quoting Ex. 1078 ¶ 181) (citing Ex. 1078 ¶ 118; Ex. 1002 ¶ 160). Wiz asserts that it would have been obvious to analyze Veselov’s snapshot to detect sensitive data because, as evidenced by Hufsmith, the “detection of unsecured sensitive data was a common best practice that was routinely performed using static and runtime/dynamic analysis.” *Id.* at 39–40 (citing Ex. 1002 ¶¶ 34, 50, 54, 66, 160).

Lastly, Wiz contends that Veselov teaches the claimed “wherein analyzing the at least one snapshot requires no interactions with the virtual machine.” Pet. 40. Wiz argues that both of Veselov’s snapshot analysis techniques (i.e., analyzing an assessment VM instantiated from the snapshot and analyzing the snapshot data directly) “are performed independently of the original VM” and, therefore, require no interaction with the VM. *Id.* (citing Ex. 1007, 3:44–67, 15:60–16:3, 16:45–53, 18:32–53, Figs. 3A, 3B, 5A, 5B; Ex. 1002 ¶ 161). Wiz asserts that this applies equally to the combination of Veselov and Hufsmith because, similar to Veselov, Hufsmith also analyzes container image data without interacting with the target container/VM. *Id.* (citing Ex. 1078, code (57); Ex. 1002 ¶¶ 162, 163).

Element 1.7 recites “determine a risk level of the virtual machine.” Ex. 1001, 9:50. Wiz contends that the combination of Veselov and Hufsmith teaches or suggests this limitation because “Hufsmith provides a more accurate risk assessment by factoring in several types of ‘context’ of the virtual resource as a whole.” Pet. 41 (citing Ex. 1002 ¶¶ 164, 165).

Wiz argues that Hufsmith discloses “[a] context evaluator that determines global weights associated with context properties such as the virtual resource’s version history, score history, environment, and other context information.” *Id.* (citing Ex. 1078 ¶¶ 106, 135–142). According to Wiz, Hufsmith’s global weights teach or suggest the claimed “risk level” of the virtual resource because they are used “to adjust values for the identified security issues and calculate the resource’s overall risk.” *Id.* (citing Ex. 1078 ¶¶ 32, 34, 92–95, 106, 135–142; Ex. 1002 ¶ 165). More importantly, Wiz asserts that Hufsmith contemplates that its risk assessment techniques apply to VMs. *Id.* (citing Ex. 1078 ¶ 149; Ex. 1002 ¶¶ 166, 167).

Element 1.8 recites “report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.” Ex. 1001, 9:51–54. Wiz contends that the combination of Veselov and Hufsmith teaches this limitation because they collectively teach reporting the detected vulnerabilities and sensitive data as alerts. Pet. 42 (citing Ex. 1002 ¶¶ 168, 169). More specifically, Wiz argues that Veselov discloses “providing assessment results to a UI” and, similarly, that Hufsmith discloses “transmitting a report with alerts for each identified security issue.” *Id.* (citing Ex. 1007, 10:30–36, 18:53–56, Figs. 2, 4, 6; Ex. 1078 ¶ 96).

When considering the arguments and evidence that it identifies above for element 1.6, Wiz asserts it would have been obvious “for the reporting of the assessment results to include alerts for the detected vulnerabilities and sensitive data.” *Id.* (citing Ex. 1002 ¶¶ 64–66, 169). In addition, Wiz argues that Hufsmith explicitly contemplates “reporting alerts associated with both

vulnerabilities and sensitive data” because it discloses “reporting granular alerts via annotations in a development environment” that may apply to other reporting techniques, and “[t]hese notifications include specific alerts for identified vulnerabilities and sensitive data exposures.” *Id.* at 42–43 (citing Ex. 1078 ¶¶ 153, 154, 156, 180–182; Ex. 1002 ¶ 170).

Wiz further contends that Hufsmith teaches the claimed “wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine” because it discloses prioritizing alerts based on global weights. Pet. 43 (citing Ex. 1078 ¶¶ 34, 135–143). Wiz argues that alert prioritization would have been obvious in view of Hufsmith’s teachings because “alert prioritization was routinely used to bring higher priority alerts to the user’s attention.” *Id.* at 43–44 (citing Ex. 1002 ¶ 171). Wiz also argues that Hufsmith teaches the claimed “filter[ing]” of alerts based on the determined risk level of the VM because it discloses filtering detected security issues to reduce cognitive load (e.g., reducing cognitive load by presenting a partial report). *Id.* at 44 (citing Ex. 1078 ¶¶ 6, 154–156, 165, 183, 192, 196, 197; Ex. 1002 ¶ 172). Wiz further argues that filtering alerts based on the determined risk level would have been obvious in view of Hufsmith’s teachings because “[p]resenting partial reports that filter out low-priority alerts was a common way of addressing the cognitive-load issue” identified by Hufsmith. *Id.* (citing Ex. 1002 ¶ 173). Wiz asserts that Hufsmith’s individual weights would have provided “a straightforward basis” for accomplishing this filtering because “they indicate the associated threat levels.” *Id.* (citing Ex. 1078 ¶ 34; Ex. 1002 ¶ 174).

Turning to rationale to combine, Wiz contends that Veselov and Hufsmith are analogous art to the '685 patent because Veselov discloses “detecting and alerting security issues for VMs in cloud environments” and, similarly, Hufsmith discloses “detecting various security issues by analyzing images of virtual assets.” Pet. 22 (citing Ex. 1007, code (57), 4:5–8, 8:46–50; Ex. 1078, code (57), ¶¶ 8, 26, 33, 34, 149, 180). According to Wiz, both Veselov and Hufsmith are “in the same field [of endeavor] as the '685 patent and are reasonably pertinent to issues addressed by the '685 patent.” *Id.* (citing Ex. 1001, 1:14–16; Ex. 1002 ¶ 105).

Wiz contends that a person of ordinary skill in the art would have been motivated to combine the teachings of Veselov with those of Hufsmith “to improve security in multiple ways.” Pet. 23. First, Wiz argues that a person of ordinary skill in the art would have made the proposed combination “to provide a more complete assessment of potential security concerns” because Veselov addresses “a variety of security risks,” and Hufsmith provides a more detailed disclosure of “detecting and reporting particular types of security issues associated with malware, [Common Vulnerabilities and Exposures (‘CVEs’)], and sensitive data.” *Id.* (citing Ex. 1007, 2:35–41, 10:30–36, 18:53–56; Ex. 1078 ¶¶ 8, 28, 84, 104, 113–122; Ex. 1002 ¶ 108). For example, Wiz asserts that “Hufsmith recognizes the importance of avoiding the potential exposure of sensitive data.” *Id.* (citing Ex. 1078 ¶¶ 117, 118, 181; Ex. 1002 ¶ 108). In addition, Wiz argues that “[d]etermining a risk level and filtering/prioritizing alerts accordingly also would have furthered this benefit” of improved security because “the criticality of potentially exposed sensitive data was known to

depend on factors such as the type of data and the type of VM on which it is detected.” *Id.* at 24 (citing Ex. 1002 ¶ 109).

Second, Wiz argues that a person of ordinary skill in the art would have applied the teachings of Veselov and Hufsmith in combination “to improve security by facilitating a more efficient, targeted review of critical security issues.” Pet. 24. According to Wiz, “[i]t was well known that filtering and prioritizing alerts, as taught by Hufsmith, facilitated rapid identification of higher-priority assets/risks and mitigated alert fatigue.” *Id.* (citing Ex. 1002 ¶ 110). Wiz asserts that Hufsmith explains the benefits of these approaches. *Id.* (citing Ex. 1078 ¶¶ 6, 155, 165, 180, 183, 192). Wiz further argues that “[d]etermining risk levels of the VM provided a well-known, useful basis for filtering and prioritizing alerts associated with detected vulnerabilities and sensitive data.” *Id.* at 24–25 (citing Ex. 1002 ¶¶ 61, 111). Wiz asserts that a person of ordinary skill in the art would have been motivated to modify Veselov’s security scans to obtain these benefits because “such scans would typically detect numerous security issues of varying importance.” *Id.* at 25 (citing Ex. 1007, 2:21–41, 10:17–36, 14:34–36, 16:47–55; Ex. 1002 ¶¶ 110, 111).

Lastly, Wiz contends that a person of ordinary skill in the art would have had a reasonable expectation of success in making the proposed combination of Veselov and Hufsmith. Pet. 25 (citing Ex. 1002 ¶ 112). Wiz argues that “Veselov and Hufsmith have similar technical contexts” and they collectively demonstrate that “[s]ensitive-data detection, risk-level determination, and alert filtering/prioritization were well-understood, predictable techniques.” *Id.* (citing Ex. 1002 ¶¶ 50, 61, 65, 67, 68, 112).

According to Wiz, given that Veselov encourages “best practices” packages, and it discloses static/dynamic analysis, which is commonly used to detect sensitive data, a person of ordinary skill in the art would have understood that it was readily achievable in Veselov to detect sensitive data, determine a risk level of the VM, and filter/prioritize alerts based on the risk level because “these techniques were predictable and routinely practiced.” *Id.* (quoting Ex. 1007, 2:35–41) (citing Ex. 1078 ¶¶ 135–143; Ex. 1002 ¶ 112). Relying on the testimony of Dr. Stavrou, Wiz asserts that the proposed combination “would not have presented meaningful technical challenges or produced unexpected results.” *Id.* (citing Ex. 1002 ¶ 112).

During trial, Orca contends that the combined teachings of Veselov and Hufsmith do not account for elements 1.1–1.4, 1.6, and 1.8. PO Resp. 20–33; PO Sur-reply 9–13. Orca also argues that Wiz improperly relies on a combination of Veselov’s embodiments, and that it does not provide a sufficient rationale to combine the teachings of Veselov and Hufsmith. PO Resp. 10–20; PO Sur-reply 2–9. In addition, Orca presents arguments and evidence of objective indicia of non-obviousness, which, according to Orca, confirms the patentability of the challenged claims. PO Resp. 34–62; PO Sur-reply 15–35.

We begin our analysis by addressing Orca’s arguments directed to elements 1.1–1.4, 1.6, and 1.8, next we address Orca’s arguments directed to rationale to combine, and then we address Orca’s arguments and evidence of objective indicia of non-obviousness, which include long-felt but unsolved need, skepticism, praise, copying, and commercial success.

a. Element 1.2—“using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment”

In its Patent Owner Response, Orca contends that, at best, 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. 21 (citing Ex. 1007, 6:30–43, 9:55–62, 11:31–32, 11:34–36, 15:15–27, 16:21–23; Ex. 2073 ¶¶ 123–126; Ex. 2077, 97:13–98:10). Orca argues that the identification of a VM or snapshot in the context of Veselov’s Figure 1 “says nothing of the virtual disk location because Veselov’s snapshots are located separately in a ‘snapshot storage service.’” *Id.* at 21–22 (quoting Ex. 1007, 5:13–17, 6:43–49, 7:27–40). Orca also argues that, because the ’685 patent discloses that “VMs and virtual disks can be in different locations in cloud computing environments,” “locating a VM does not specify the location of the virtual disk.” *Id.* at 22 (citing Ex. 1001, 3:52–55, Fig. 1B; Ex. 2073 ¶¶ 127–129; Ex. 2074 ¶ 48; Ex. 2077 92:4–93:19, 94:16–21).

Orca further contends that Wiz’s claim mapping 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. 22–23 (citing Pet. 27–28; Ex. 2074 ¶¶ 86–94). For example, Orca argues that the embodiments illustrated in Veselov’s Figures 1, 3A, and 3B use APIs, “but they are not used to identify, query or locate virtual disks . . . or analyze snapshots.” *Id.* at 23 (citing Ex. 1007, 4:59–5:8, 10:37–41, 14:37–41, 15:23–27, Figs. 1, 3A, 3B;

Ex. 2073 ¶¶ 86–94). In contrast, Orca argues that the embodiments illustrated in Veselov’s Figures 5A and 5B “do not use APIs at all, let alone cloud computing APIs operating as claimed.” *Id.* (citing Ex. 1007, 15:56–17:66, Figs. 5A, 5B; Ex. 2073 ¶¶ 86–94; Ex. 2077 ¶¶ 154:2–155:22). In addition, Orca argues that, in the embodiments illustrated in Veselov’s Figures 1, 3A, and 3B that discuss APIs, these “APIs only provide interfaces to a user, or convey user-specific data”—they do not teach or suggest “using cloud computing platform APIs for identifying, querying, and receiving virtual disk location information.” *Id.* at 24 (citing Ex. 1007, 4:29–48, 5:1–8, 5:13–22, 6:34–38, 6:59–60, 8:46–51, 14:37–53, 15:23–38; Ex. 2073 ¶ 126); *see also id.* at 24–25 (arguing that Veselov’s tailoring of snapshots does not teach the claimed cloud computing APIs and their uses because, once again, Wiz improperly relies on distinct features of Veselov’s separate embodiments (citing Pet. 29–33; Ex. 1007, 8:16–45, 14:37–57; Ex. 2073 ¶¶ 127–130)). Orca also argues that Wiz’s reliance on tertiary references as evidence that identifying virtual disks using APIs was well known and routine fares no better because demonstrating that individual elements were independently known in the prior art is not enough, and Wiz fails to identify anything in the tertiary references that would have motivated a person of ordinary skill in the art to modify Veselov. *Id.* at 25 (citing Pet. 31–32; Exs. 1051, 1052, 1053, 1020; Ex. 2073 ¶¶ 128–130).

In its Reply, Wiz contends that Orca’s virtual disk identification arguments are misplaced because Wiz did not take the position that Veselov’s virtual disks and VMs are synonymous, nor did Wiz take the position that Veselov obtains snapshots from an optional snapshot storage

service. Pet. Reply 6–5 (citing PO Resp. 21–22; Pet. 26–35). Instead, Wiz argues that, in the Petition, it demonstrates that a person of ordinary skill in the art reading Veselov would have understood that obtaining or accessing a snapshot includes, or at least suggests, using cloud APIs to perform virtual disk identification. *Id.* at 7 (citing Pet. 30–31). That is, contrary to Orca’s arguments, Wiz asserts that it demonstrates how Veselov’s API-based virtual disk identification was a routine part of generating snapshots. *Id.* (citing PO Resp. 22 n.4; Pet. 31–32; Ex. 1400 ¶¶ 40, 41, 80–82). Wiz also disagrees with Orca’s argument that Veselov merely suggests user-provided disk locations because this argument fails to appreciate that “the claims don’t exclude user involvement.” *Id.* (citing PO Resp. 24–25). When viewing the claims in this light, Wiz asserts that “Veselov describes the *scanner* identifying data elements (e.g., a virtual disk) for the snapshot.” *Id.* According to Wiz, the arguments and evidence that it presents in the Petition do not rely on a modification to Veselov, and its actual analysis explaining what a person of ordinary skill in the art would have understood upon reading Veselov stands unrebutted. *Id.* at 7–8 (citing PO Resp. 24–25; Ex. 1400 ¶ 38).

Wiz further contends that Veselov “flatly contradicts” Orca’s argument that Wiz improperly relies on distinct features from the separate embodiments illustrated in Veselov’s Figures 1, 3A, 3B, 5A, and 5B. Pet. Reply 2. More specifically, Wiz argues that Veselov discloses that the embodiments illustrated in Veselov’s Figures 5A and 5B have the same “implementation” and “interactions” as the embodiments illustrated in Veselov’s Figures 3A and 3B, which Orca admits involve the use of APIs.

Id. at 2 (quoting Ex. 1007, 16:56–67) (citing Ex. 1007, 18:1–15; Ex. 1400 ¶¶ 11, 12; PO Resp. 10–13). Wiz also argues that, contrary to Orca’s assertion that Veselov’s Figure 1 is not suitable for snapshot analysis, Veselov indicates otherwise, including by teaching “API-mediated interactions between the scanning service and the environment/provider.” *Id.* at 3 (citing Ex. 1007, 3:20–4:29, 5:1–8, 8:34–45, 10:1–16; Ex. 1400 ¶ 3). Indeed, relying on the testimony of Dr. Stavrou, Wiz asserts “that is how virtually every cloud-security platform operate[s].” *Id.* (citing Ex. 1400 ¶¶ 14, 15, 80–82).

In its Sur-reply, Orca reiterates that Veselov’s disclosure of “identifying and querying locations of *VMs* (not disks)” does not amount to “using cloud APIs to identify and query locations of *virtual disks*,” as required by element 1.2. PO Sur-reply 9. Orca also argues that Wiz’s reply arguments turn on “improper embodiment mixing,” only citing to Veselov’s corresponding description of the embodiment illustrated in Figure 1. *Id.* (citing Pet. Reply 6–9). Orca then asserts that Wiz improperly relies on unsupported attorney argument, new arguments, impermissible hindsight reconstruction, and impermissible gap filling to demonstrate how Veselov teaches or suggests element 1.2. *Id.* at 9–11 (citing Pet. 30–32; Pet. Reply 7, 9; Ex. 2073 ¶¶ 123–127; Ex. 2172, 81:14–22, 82:12–21, 142:15–143:3).

Orca also reiterates that Wiz improperly relies on distinct features from the separate embodiments illustrated in Veselov’s Figures 1, 3A, 3B, 5A, and 5B. PO Sur-reply 2–3. Orca argues that the embodiments illustrated in Veselov’s Figures 5A and 5B do not have the same “implementation” and “interactions” as the embodiments illustrated in

Veselov's Figures 3A and 3B because Veselov expressly lists what features are shared between these embodiments, but expressly omits computer resource service provider 300, 350 and API 338. *Id.* at 3 (citing Ex. 1007, 16:56–67). According to Orca, even if a computer resource service provider were used in Veselov's Figures 5A and 5B, Wiz provides no motivation to modify these figures to use cloud APIs to identify and locate virtual disks. *Id.* (citing Ex. 2077, 142:15–143:3).

Based on the complete record, we agree with Wiz that Veselov teaches element 1.2—“using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment.” *See* Pet. 29–33, Pet. Reply 2–3, 6–8. Veselov clearly discloses that it provides security assessments of a service or distributed application using a distributed computing environment, such as “a ‘cloud’ computing environment.” Ex. 1007, 2:64–67. Veselov's Figure 1 illustrates that computing environment 100 includes scanning service 110 that may access “computer resource service provider 104, or any associated virtual computing environments and/or computing resources,” via API 120 or another API. *Id.* at 5:1–5. Similarly, Veselov's Figures 3A and 3B illustrate how an owner or administrator may configure one or more security assessments of virtual computing environment 304A or 304B so that user device 302 accesses “scanning service 310 via one or more APIs 338.” *Id.* at 14:37–41. Veselov discloses that “API 338 may be configured to receive the [security assessment] request, determine its content, and then control . . . scanning service 310 to implement the security assessment according to the user input.” *Id.* at 15:23–27. Based on these cited disclosures, we find that

Veselov's APIs (e.g., API 120 or APIs 338) constitute "cloud computing platform APIs" because, as we explain above, Veselov explicitly contemplates that a distributed computing environment may be a cloud computing environment.

In addition, Veselov discloses that "[t]he 'state' of the target resource [is] represented by snapshot data [that] may include any properties of the target resource," including "properties of logical volume(s) containing the target resource." Ex. 1007, 9:55–67. Veselov discloses that one example of a logical volume of a VM is a "virtual disk drive" (e.g., logical volume 306 of VM 312 illustrated in Figures 3A and 3B, logical volume 516 within volume image 508 of VM 512 or 512A, etc.). *Id.* at 11:28–33; *see also id.* at 11:5–9 ("[VM] 312 may be executed on a server and use a logical volume 306, which is composed of a fixed or variable allocation of physical data storage resources, such as data storage blocks selected from one or more hard disk drives of one or more server computers."). Based on these cited disclosures explaining how Veselov identifies a virtual disk of a VM, and taking into account our finding that Veselov's APIs (e.g., API 120 or APIs 338) constitute cloud computing platform APIs, we find that Veselov's APIs are used to "identify virtual disks of a virtual machine in client environment," as required by element 1.2.

Orca's arguments that Veselov's VMs and virtual disks are in different locations and, therefore, identifying locations of VMs is not the same as using APIs to identify the locations of virtual disks of the VMs, are misplaced. *See* PO Resp. 21–23; PO Sur-reply 9. Orca's arguments in this regard appear to be predicated on the notion that Veselov only obtains

snapshot data of a virtual disk drive from a snapshot storage service. *See, e.g.*, PO Resp. 21–22 (arguing “Veselov’s snapshots are located separately in a ‘snapshot storage service’” (quoting Ex. 1007, 5:13–17, 6:43–49, 7:27–40)). Veselov, however, distinguishes between scanning service 110 or virtualization layer 144 directly obtaining snapshot data of a virtual disk drive from a VM, and obtaining snapshot data of a virtual disk drive from an optional snapshot storage service 108. Ex. 1007, 5:13–17, 6:43–49, 7:27–40. We understand Wiz’s claim mapping to rely on the former and not the latter. *See, e.g.*, Pet. Reply 6 (referring to Veselov’s snapshot storage service and arguing the “Wiz did not rely on this optional component” (citing Pet. 26–35)).

We also do not agree with Orca’s argument that Wiz impermissibly combines distinct features from separate embodiments in Veselov, without providing a sufficient rationale to combine those embodiments. *See* PO Resp. 22–24; PO Sur-reply 9. We understand Wiz to rely upon common features across different embodiments illustrated in Figures 1, 3A, 3B, 5A, and 5B of Veselov. *See, e.g.*, Pet. 30 (relying on logical volume 306 of VM 312 illustrated in Figures 3A and 3B, as well as logical volume 506 of VM 512 illustrated in Figures 5A and 5B). That is, Veselov discloses exemplary embodiments, each of which executes a security assessment of a VM. Ex. 1007, 1:57–2:13, Figs. 1, 3A, 3B, 5A, 5B. These exemplary embodiments all have common features, such as user devices 102, 302, and 502, scanning services 110, 310, and 510, VMs 112, 312 and 512, and logical volumes 306 and 506. *Id.* at Figs. 1, 3A, 3B, 5A, 5B.

Moreover, Veselov discloses that the features of Figures 5A and 5B (e.g., user device 502, virtual computing environments 504A or 504B, logical volume 506, virtual image 508, VM 512 including operating system 560, runtime environment 562, software applications 564, and files/files system 566, etc.), “as well as their implementations and interactions, are the same as described above for associated components 302, 304A, 306, 308, 312, 360–366 of [Figures 3A and 3B].” Ex. 1007, 16:58–67. Contrary to Orca’s assertion, we do not view this cited disclosure in Veselov as being an exhaustive list of common features shared between the embodiments illustrated in Veselov’s Figures 3A, 3B, 5A, and 5B. Instead, we view this disclosure as sufficient support for Wiz’s position that the embodiments illustrated in Veselov’s Figures 3A, 3B, 5A, and 5B share common features, such that user device 502 is capable of accessing scanning service 510 via APIs in the same manner that user device 302 accesses scanning service 310 via APIs 338. *See* Pet. Reply 2; *see also Boston Scientific Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (Fed. Cir. 2009) (explaining that “[c]ombining two embodiments disclosed adjacent to each other in a prior art patent does not require a leap of inventiveness”).

Lastly, we do not agree with Orca’s arguments that it was improper for Wiz to introduce tertiary references with the Petition as evidence demonstrating that identifying virtual disks using APIs was well known and routine. *See* PO Resp. 25. Nor do we agree with Orca’s argument that Wiz fails to identify anything in the tertiary references that would have motivated a person of ordinary skill in the art to modify Veselov. *See* PO Resp. 25; PO Sur-reply 10–11. We need not rely on the tertiary references that Wiz

introduces with the Petition because we do not understand Wiz to rely on a modification to Veselov. *See* Pet. Reply 7–8; *see also* Ex. 1400 ¶ 38 (Dr. testifying that his initial “analysis explained what a [person of ordinary skill in the art] would have understood Veselov to teach or suggest . . . not modifications to Veselov’s broadly described process.”). Instead, as we explain above, we find that Veselov’s APIs (e.g., API 120 or APIs 338) are used to “identify virtual disks of a virtual machine in the client environment,” as required by element 1.2.

b. Element 1.3—“use the computer platform APIs to query a location of at least one of the identified virtual disks”

In its Patent Owner Response, Orca contends that Wiz’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. 25–26 (quoting Pet. 33) (citing Ex. 2073 ¶ 132; Ex. 1007, 9:9–25). According to Orca, “the only query disclosed in Veselov relates to querying a ‘snapshot storage service’ to find a stored snapshot, which obviates the need for the claimed cloud computing platform API querying for the location of a virtual disk.” *Id.* at 26 (citing Ex. 2073 ¶¶ 132–134). Orca also argues that Wiz’s fallback position that the features required by element 1.3 were individually “well-known” and “routine[]” is insufficient and “fraught with hindsight basis.” *Id.* (quoting Pet. 33–34) (citing Ex. 2073 ¶¶ 131–134).

In its Reply, Wiz contends that Orca and its declarant, Dr. Kaeli, “treat[] Veselov as limited to obtaining snapshots from storage, ignoring descriptions of taking new snapshots.” Pet. Reply 8 (citing Ex. 2073 ¶ 132; Ex. 1007, 5:1–9, 8:60–9:41). According to Wiz, Orca’s argument that the only disclosure of queries in Veselov involves the snapshot storage service is misplaced because “that service is optional” and “[Orca’s] focus on the word ‘query’ is misguided.” *Id.* (citing Ex. 1400 ¶¶ 44, 45). Wiz argues that the actual analysis presented in the Petition “explaining why the recited query was obvious because it was the well-known, routine way of doing what Veselov describes . . . stands un rebutted.” *Id.* (citing Pet. 33–34).

As an initial matter, Orca relies, at least in part, on the same arguments it presents for element 1.2 to support its position that Veselov does not teach or suggest element 1.3. For the same reasons we identify above, we do not agree with those arguments. *See supra* Section II.B.5.a.

Based on the complete record, we agree with Wiz that Veselov teaches element 1.3—“use the computer platform APIs to query a location of at least one of the identified virtual disks.” *See* Pet. 33–34; Pet. Reply 8. 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. Wiz’s declarant, Dr. Stavrou, testifies that “[i]t would have been apparent to a [person of ordinary skill in the art] that, for the scanning service to generate a snapshot of certain virtual disks . . . as described in Veselov, the scanning service would first determine the location

of the disks it will be including in the snapshot.” Ex. 1002 ¶ 140. We credit Dr. Stavrou’s testimony on this particular issue because it is consistent with Veselov’s disclosure that, prior to requesting a snapshot, the scanning service includes instructions identifying the data (i.e., the location of the virtual disk) to include in the snapshot. We find that Veselov’s cited disclosure, as further explained through the perspective of a person of ordinary skill in the art as evidenced by the supporting testimony of Dr. Stavrou, teaches that Veselov’s scanning services uses APIs (e.g., API 120 or APIs 338) “to query a location of at least one of the identified virtual disks,” as required by element 1.3.

We do not agree with Orca’s argument that the only disclosure of querying in Veselov is limited to querying a “snapshot storage service” to find a snapshot. *See* PO Resp. 26. As Wiz correctly notes in the Reply, Orca’s focus on the verbatim use of the word “query” in Veselov is “misguided.” Pet. Reply 8; *see also In re May*, 574 F.2d 1082, 1090 (CCPA 1978) (explaining that an obviousness analysis does not require an *ipsissimis verbis* test—that is, identity of terminology is not required). As we explain above, when viewing Veselov’s snapshot scanning service that “include[s] instructions identifying the data to include in the snapshot” (e.g., the location of the virtual disk drive of a VM to analyze) through the perspective of a person of ordinary skill in the art as evidenced by the supporting testimony of Dr. Stavrou (*see* Ex. 1007, 9:25–28; Ex. 1002 ¶ 140), we find that Veselov teaches the scanning service uses APIs (e.g., API 120 or APIs 338) to “query a location of at least one of the identified virtual disks,” as required by element 1.3.

c. Element 1.4—“receive an identification of the location of the virtual disks of the virtual machine”

In its Patent Owner Response, Orca contends that Wiz’s arguments and evidence for element 1.4 fail because it “rel[ies] on the prerequisite querying of[element] 1.3.” PO Resp. 26 (citing Pet. 34–35). Orca further argues that Wiz’s reliance on Veselov’s disclosure that a VM has a “virtual network address” to locate virtual disks of the VM improperly conflates identifying a VM generally and identifying the virtual disks of VM specifically. *Id.* at 26–27 (citing Ex. 2073 ¶¶ 135–137; Ex. 2077, 97:13–98:10).

In its Reply, Wiz disagrees with Orca’s arguments for element 1.4 because Orca repeats the same flawed arguments it presents for element 1.3. Pet. Reply 8 (citing PO Resp. 26). Wiz argues that Orca does not dispute that Veselov’s “[virtual network] address of the VM is a general location of the attached [virtual] disk.” *Id.* at 8–9 (citing PO Resp. 26–27; Pet. 12, 34–35, Ex. 1400 ¶ 46).

As an initial matter, Orca relies on the same arguments it presents for element 1.3 to support its position that Veselov does not teach or suggest element 1.4. For the same reasons we identify above, we do not agree with those arguments. *See supra* Section II.B.5.b.

Based on the complete record, we agree with Wiz that Veselov teaches element 1.4—“receive an identification of the location of the virtual disks of the virtual machine.” As we explain above when addressing the parties’ arguments and evidence for element 1.3, Veselov discloses one example where the scanning service queries a virtual disk drive of a VM for

analysis. *See* Ex. 1007, 9:25–32. Wiz’s declarant, Dr. Stavrou, testifies that it “would have been apparent to a [person of ordinary skill in the art] that the previously discussed location query would return an identification of the location of the virtual [disk drive] of the VM.” Ex. 1002 ¶ 145. We credit Dr. Stavrou’s testimony on this particular issue because, when Veselov’s scanning service queries the location of a virtual disk drive of a VM for analysis (i.e., a query that includes a location request), the response to the query would identify the location of the virtual disk drive of the VM so the scanning service can perform the analysis. *See KSR*, 550 U.S. at 418 (explaining that an obviousness evaluation “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ”).

We do not agree with Orca’s argument that Veselov’s disclosure of identifying a VM by using its virtual network address does not result in identifying the virtual disks of the VM. *See* PO Resp. 26–27. As we explain above when addressing the parties’ arguments and evidence for elements 1.2 and 1.3, we do not understand Wiz to rely on Veselov’s disclosure of the scanning service obtaining snapshot data of a virtual disk drive from a snapshot storage service. *See supra* Sections II.B.5.a and II.B.5.b. Instead, we understand Wiz to rely on Veselov’s disclosure of the scanning service directly obtaining snapshot data of a virtual disk drive by “includ[ing] instructions identifying the data to include in the snapshot” (e.g., the location of the virtual disk drive of a VM to analyze). *See* Ex. 1007, 9:25–28; Ex. 1002 ¶ 140. We find that, in the scenario where Veselov’s VM and its

attached virtual disks share the same general location, Veselov’s disclosure of identifying a VM by using its virtual network address would facilitate identifying the virtual disks of the VM. *See, e.g.*, Ex. 1133, 1 (acknowledging a scenario in Amazon’s cloud service called AWS where the “[t]he volume and instance must be in the same Availability zone”); *see also* Ex. 1007, code (71) (Veselov is assigned to Amazon Technologies, Inc.).

d. Element 1.6—“analyze the at least one snapshot to detect vulnerabilities and sensitive data”

In its Patent Owner Response, Orca contends that Wiz’s proposed combination of Veselov and Hufsmith fails to teach analyzing a snapshot to detect “vulnerabilities *and sensitive data*,” as required by element 1.6. PO Resp. 27–28. Orca argues that Hufsmith’s disclosure of “detecting the ‘potential exposure’ of sensitive data in a vulnerability or software weakness is distinct from detecting ‘sensitive data’ as claimed.” *Id.* at 28 (citing Ex. 2073 ¶¶ 140–143). According to Orca, the ’685 patent explains this distinction by disclosing that analyzing a snapshot can include detecting certain vulnerabilities identified in a CVE database and then, separately, detecting sensitive data (e.g., personally identifiable information or PII) on the VM that purportedly does not represent vulnerabilities. *Id.* (citing Ex. 1001, 4:32–42, 6:19–30, 6:44–53; Ex. 2073 ¶ 143. Orca asserts that Wiz’s proposed combination of Veselov and Hufsmith teaches a system “that only detects the *potential exposure* of sensitive data and flags risks regardless of whether sensitive data is actually present.” *Id.* (citing Ex. 2073 ¶¶ 140–144).

In its Reply, Wiz disagree with Orca’s argument that Hufsmith “does not detect sensitive data, just its potential exposure.” Pet. Reply 9. According to Wiz, Orca’s argument in this regard reverts to attacking Hufsmith individually rather than considering Hufsmith’s teachings of detecting sensitive data in the context of Veselov’s snapshot analysis. *Id.* at 9–10. Wiz argues that Orca’s semantic complaint does not respond to the showing in the Petition that detecting the potential exposure of sensitive data stored on a system at the very least suggests detecting the sensitive data itself. *Id.* at 10 (citing Pet. 39–40; Ex. 1002 ¶¶ 159, 160; Ex. 1400 ¶¶ 47–49).

In its Sur-reply, Orca contends that the proposed combination of Veselov and Hufsmith, at best, detects vulnerabilities or weaknesses showing the potential exposure of sensitive data, but this does not amount to “detecting vulnerabilities *and* sensitive data,” as required by element 1.6. PO Sur-reply 11. Orca disagrees with Wiz that the difference it outlines in the Patent Owner Response is a “semantic compliant,” arguing that it is critical in the context of the “prioritizing” and “alerting,” as required by element 1.8. *Id.* (citing Ex. 1001, 6:46–53).

Based on the complete record, we agree with Wiz that the proposed combination of Veselov and Hufsmith teaches element 1.6—“analyze the at least one snapshot to detect vulnerabilities and sensitive data.” *See* Pet. 37–40; Pet Reply 9–10. Veselov discloses that “scanning service 110 may obtain and analyze snapshot data 146” (Ex. 1007, 4:53–54) for purposes of evaluating “vulnerabilities of the target resources” (*id.* at 4:5–8). As one example of using snapshot analysis to detect vulnerabilities, Veselov

discloses that scanning service “transform[s] the snapshot into a data file” and “then perform[s] the security assessment of the data at the file system level.” *Id.* at 3:61–67. As another example of using snapshot analysis to detect vulnerabilities, Veselov discloses that scanning service “set[s] up and launch[es] an active virtual machine instance in the allocated computing resources” and then “perform[s] the security assessment on the active virtual machine instance in a static or runtime environment.” *Id.* at 3:54–61; *see also id.* at 10:1–16 (disclosing that, “[a]t step 208, the scanning service may generate a scannable volume,” which may “include launching a duplicate virtual machine instance in an allocated logical volume”). We find that these two ways of performing snapshot analysis are consistent with our construction of the claim term “[analyze/analyzing] the at least one snapshot” as encompassing the following two alternative approaches: (1) “direct analysis of the snapshot data”; and (2) “analysis of a VM instantiated from the snapshot.” *See supra* Section II.A.

Similar to Veselov, Hufsmith discloses a security assessment technique that provides annotations that “include an indication of a type of harm associated with a security vulnerability,” such as indicating that the vulnerability “potentially allows for the exfiltration of confidential information” or “leaks information about an encryption key.” Ex. 1078 ¶ 181; *see also id.* ¶ 166 (explaining that “annotations are in the form of an overlaid region like those described below with reference to [Figures] 3B and 3C that overlays portions of the user interface”). Hufsmith also discloses that its scans generate one or more metrics similar to a “confidentiality impact” by quantifying the exposure of “restricted

information.” *Id.* ¶ 118. Based on these cited disclosures, we find that Hufsmith teaches that detecting vulnerabilities includes detecting the potential exposure of sensitive data, such as confidential/restricted information or information pertaining to encryption keys. When combining Veselov’s scanning service that uses “any suitable security assessment,” including security assessments defined by rules packages like CVEs or “best practices” packages (Ex. 1007, 2:35–42), with Hufsmith’s ability to detect vulnerabilities that includes detecting the potential exposure of sensitive data, we find that this proposed combination fairly suggests to a person of ordinary skill in the art “analyz[ing] the at least one snapshot to detect vulnerabilities and sensitive data,” as required by element 1.6.

We do not agree with Orca’s argument that Hufsmith’s teaching of detecting the potential exposure of sensitive data in a security vulnerability or software weakness is distinct from the claimed “detect[ing] vulnerabilities and sensitive data.” *See* PO Resp. 28; PO Sur-reply 11. Orca does not explain, and we fail to see, how Hufsmith’s teaching of detecting vulnerabilities that includes detecting the potential exposure of sensitive data in a security vulnerability or software weakness would not suggest, at least in some instances, in detecting the sensitive data itself. *See* Pet. 39–40; Pet. Reply 10. This holds true in an obviousness evaluation, which does not require an asserted prior art reference to satisfy a claim limitation in every instance. *See, e.g., Unwired Planet, LLC v. Google Inc.*, 841 F.3d 995, 1002 (Fed. Cir. 2016) (explaining that prior art that “sometimes meet the claim elements” suffices “to show obviousness”); *Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1326 (Fed. Cir. 2003) (explaining that “a prior art

product that sometimes, but not always, embodies a claimed method nonetheless teaches that aspect of the invention”).

e. Element 1.8—“report the detected vulnerabilities and sensitive data as alerts”

In its Patent Owner Response, Orca contends that Wiz’s proposed combination of Veselov and Hufsmith does not teach detecting the claimed “sensitive data” for the same reasons it identifies above with respect to element 1.6 and, therefore, also fails to teach the reporting of “detected . . . sensitive data as alerts,” as required by element 1. 8. PO Resp. 30 (citing Ex. 2073 ¶ 149. Orca also argues that Wiz’s proposed combination of Veselov and Hufsmith does not teach the claimed “filtered and prioritized” alerts for vulnerabilities and sensitive data because Wiz conflates reporting of “assessment results” with reporting alerts. *Id.* at 30 (quoting Pet. 42) (citing Ex. 2073 ¶¶ 149–154). More specifically, Orca argues that Veselov’s disclosure of “[m]erely reporting results does not constitute reporting detected vulnerabilities or sensitive data ‘as alerts,’ as claimed.” *Id.* (citing Ex. 2073 ¶¶ 150, 151). To support this argument, Orca asserts that both the specification of the ’685 patent and Wiz’s declarant, Dr. Stavrou, differentiate between reporting results and reporting results “as alerts.” *Id.* at 30–31 (citing Ex. 1001, 7:50–51, 6:38–45; Ex. 2073 ¶¶ 150, 151; Ex. 2077, 287:4–12). In addition, Orca argues that Wiz’s reliance on Hufsmith’s “annotations in a development environment” to teach the claimed “alerts” is misplaced because these annotations are made by developers in the source code pre-deployment, and a person of ordinary skill in the art would not have found Hufsmith’s teaching in this regard to be

applicable to Veselov’s post-deployment assessments, which do not have source code available to annotate. *Id.* at 31 (quoting Pet. 43) (citing Ex. 1078 ¶¶ 153–155, 165, 168, 196, Figs. 3B–3C; Ex. 2078 ¶¶ 152, 153).

In its Reply, Wiz contends that Orca reiterates the same arguments regarding the “potential” exposure of sensitive data, which should be found unpersuasive for the same reasons Wiz identifies above with respect to element 1.6. Pet. Reply 11 (citing Ex. 1400 ¶ 51). Wiz also argues that Orca’s “alert” argument is unavailing because verbatim use of claims terms in the prior art is not required. *Id.* Wiz argues that, contrary to Orca’s “alert” argument, “Veselov does not describe reporting results generally,” but rather Veselov’s assessment results bring “specific problems/remediations to the user’s attention,” which is all that is required to teach the claimed “alerts.” *Id.* (citing Pet. 42; Ex. 1007, 10:17–36, 20:57–21:13, 23:19–47; Ex. 1400 ¶ 51; Ex. 2073 ¶ 151; Ex. 1401, 95:3–108:12). In addition, Wiz argues that Orca’s argument directed to Hufsmith’s source-code annotations is “misguided” because Wiz did not propose bodily incorporating Hufsmith’s source-code annotations in Veselov, nor is that the test for evaluating obviousness. *Id.* (citing Pet. 22–25, 42). According to Wiz, Orca does not dispute that Hufsmith’s development-environment techniques are applicable to other reporting techniques, such as those taught by Veselov. *Id.* at 11–12 (citing Pet. 22–25; Ex. 1400 ¶¶ 52, 53).

In its Sur-reply, Orca reiterates its position that Veselov sends assessment results to users without providing “alerts.” PO Sur-reply 12 (citing PO Resp. 29–33). Orca argues that, contrary to Wiz’s assertion that

element 1.8 may be satisfied by anything that “brings specific problems/remediation to the user’s attention,” Veselov’s assessment results report all assessment “findings”—not just “specific problems.” *Id.* (quoting Ex. 1007, 10:18–36) (citing Ex. 2073 ¶ 150). In addition, Orca argues that Hufsmith does not cure the deficiencies in Veselov because, as it explains in the Patent Owner Response, a person of ordinary skill in the art would not consider modifying Veselov’s post-deployment system to include Hufsmith’s pre-deployment code annotations, nor is there a reasonable expectation of success in doing so. *Id.* at 13 (citing PO Resp. 32). Orca asserts that, in the Reply, Wiz does not dispute that “Veselov’s post-deployment system doesn’t have source code available to annotate.” *Id.* (citing PO Resp. 16–17, 32–33).

As an initial matter, Orca relies on the same arguments it presents for element 1.6 to support its position that Wiz’s proposed combination of Veselov and Hufsmith does not teach detecting the claimed “sensitive data” required by element 1.8. For the same reasons we identify above, we do not agree with those arguments. *See supra* Section II.B.5.d.

Based on the complete record, we agree with Wiz that the proposed combination of Veselov and Hufsmith teaches “report[ing] the detected vulnerabilities and sensitive data as alerts,” as required by element 1.8. *See* Pet. 42–45; Pet. Reply 11–12. Veselov discloses that, after the scanning service “perform[s] a security assessment on the scannable volume,” it “produce[s] assessment results that describe ‘findings’ related to the assessed properties.” Ex. 1007, 10:17–24. Veselov further discloses that the scanning service takes various actions based on the assessment results,

including, among other things, “providing the assessment results in a user-readable format to a user interface to be displayed on the user device.” *Id.* at 10:24–36; *see also id.* at 18:53–56 (disclosing method 600 for performing a security assessment that includes, among other things, the scanning service “delivering the [assessment] results”). Based on these cited disclosures, we find that Veselov teaches reporting assessment results that include various findings regarding security vulnerabilities.

Wiz turns to Hufsmith to more clearly teach reporting Veselov’s assessment results regarding security vulnerabilities as alerts. *See* Pet. 42–43. Hufsmith discloses providing “alerts relating to potential security vulnerabilities” (Ex. 1078 ¶ 15) and, as one example, discloses providing annotations that identify potential exposure of sensitive data, such as “confidential information” and “information about an encryption key” (*id.* ¶ 181). Although Hufsmith describes its reporting technique in the context of a “[d]evelopment [e]nvironment” (*id.* ¶ 153), it also discloses that this reporting technique may be used “in conjunction with the approaches above” and should not be treated as “limiting” (*id.* ¶ 154). As one example, Hufsmith discloses that results engines 54 scans “a distributed application or container image” and “determine[s] combined threat scores for the distributed applications or container images,” and that the combined threat scores may be considered “during application or container development and deployment.” *Id.* ¶ 108. Based on these cited disclosures, we find that Hufsmith teaches reporting security vulnerabilities and the potential exposure of sensitive data as alerts, and Hufsmith does not limit this reporting technique to a particular environment. Taking into account Wiz’s

proposed combination of Veselov and Hufsmith, which includes Veselov's teaching of reporting assessment results that include various findings regarding security vulnerabilities, together with Hufsmith's more specific disclosure of reporting security vulnerabilities and the potential exposure of sensitive data as alerts, we find that this proposed combination fairly suggests "report[ing] the detected vulnerabilities and sensitive data as alerts," as required by element 1.8.

We do not agree with Orca's argument that that Wiz conflates Veselov's reporting of assessment results with reporting of the claimed "alerts," as required by element 1.8. *See* PO Resp. 30–31; PO Sur-reply 12. We fail to see the distinction Orca attempts to draw between Veselov's reporting of assessment results that include various findings regarding security vulnerabilities and the requirement in element 1.8 of reporting "alerts" because they both appear to accomplish a primary objective of a security assessment, which is to provide notification of situations that require attention, such as identifying security vulnerabilities and the potential exposure of sensitive data.

Our view in this regard is consistent with both (1) Dr. Kaeli's testimony that "[a]lerts serve to notify stakeholders of situations that require attention" (Ex. 2073 ¶ 151); and (2) the general background knowledge in the art as evidenced by Computer Security Incident Handling Guide issued by the National Institute of Standards and Technology, U.S. Department of Commerce, which states, in relevant part, that "[d]etection of security breaches is thus necessary to alert the organization whenever incidents occur" (Ex. 1025, 21). In our view, Veselov's reporting of assessment

results provides notification of situations that require attention. *See* Ex. 1007, 10:17–36. Nevertheless, as we explain above, Wiz relies on Hufsmith’s disclosure of providing “alerts relating to potential security vulnerabilities” (Ex. 1078 ¶ 15) to more clearly teach reporting alerts, which obviates the need for Veselov to provide essentially the same teaching.

We also do not agree with Orca’s argument that Wiz improperly relies on Hufsmith’s annotations that occur in a development environment because the annotations are made by developers in the source code pre-deployment and, therefore, Hufsmith’s reporting technique cannot be applied to Veselov’s post-deployment system. *See* PO Resp. 31; PO Sur-reply 13. Orca’s argument in this regard improperly seeks to limit Hufsmith’s reporting technique in a manner not contemplated by Hufsmith itself. A proper obviousness evaluation requires us to consider Hufsmith for everything it teaches by way of technology. *See EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 907 (Fed. Cir. 1985) (“A reference must be considered for everything it *teaches* by way of technology and is not limited to the particular invention it is describing and attempting to protect.”). As we explain above, Hufsmith does not limit its technique for reporting security vulnerabilities and the potential exposure of sensitive data as alerts to a particular environment. *See* Ex. 1078 ¶¶ 108, 149, 153, 154.

f. Rationale to Combine and Reasonable Expectation of Success

In its Patent Owner Response, Orca asserts that Wiz’s motivations to combine the teachings of Veselov and Hufsmith are insufficient for eight separate reasons. PO Resp. 14. First, Orca argues that “[persons of ordinary skill in the art] reading Veselov would not have found that a combination

with Hufsmith would permit a ‘more complete’ and ‘more efficient’ assessment” because Veselov and Hufsmith are not analogous art. *Id.* at 15 (quoting Pet. 23–24). According to Orca, Hufsmith’s security assessments are directed to container or VM images, whereas Veselov’s analysis is directed to snapshots (i.e., volume images). *Id.* (citing Pet. 22; Ex. 2073 ¶¶ 97–99; Ex. 2077, 272:7–13). Second, Orca argues that “[a person of ordinary skill in the art] would have understood that Hufsmith’s security assessments of container images and Veselov’s snapshot-based security assessments of VMs are different concepts and would not lend themselves to combination.” *Id.* at 15–16 (citing Ex. 2073 ¶¶ 100, 101; Ex. 2074 ¶¶ 167, 168; Ex. 2075, 6). Third, Orca argues that Wiz’s proposed combination of Veselov and Hufsmith is based on “mistaken characterizations and overextensions” of their respective teachings. *Id.* at 16. As one example, Orca asserts that Hufsmith only discloses indicators of potential exposure of sensitive data; it does not disclose actually detecting and reporting on sensitive data. *Id.* at (citing Pet. 23; Ex. 2073 ¶ 105; Ex. 1078 ¶¶ 111, 116, 126, 132). As another example, Orca asserts that Hufsmith provides “alerts” using annotations made by developers in the source code pre-deployment that would be inapplicable to Veselov’s post-deployment VM assessments. *Id.* at 16–17 (quoting Ex. 1078 ¶ 15) (citing Ex. 1078 ¶¶ 153–197; Ex. 2073 ¶¶ 102–108).

Fourth, Orca argues that Wiz fails to explain adequately why Hufsmith’s benefits relating to “rapid identification of higher-priority assets/risks” and mitigation of “alert fatigue” would be applicable to Veselov’s scanning system for VMs. PO Resp. 17–18 (quoting Pet. 24–25;

Ex. 1007, 4:5–8, 10:17–36, 16:47–55; Ex. 1078 ¶¶ 153–197; Ex. 2073 ¶¶ 106–113; Ex. 2074, 6). Fifth, Orca argues that Wiz’s assertion that combining the teachings of Veselov and Hufsmith is nothing more than the combination of familiar elements according to their known methods to yield predictable results includes “a fatal gap,” and Wiz’s reliance on multiple tertiary references to support this motivation to combine amounts to improper hindsight reconstruction. *Id.* at 18–19 (citing Pet. 22–25; Ex. 2073 ¶¶ 109–114). Sixth, Orca argues that Wiz’s assertion that combining the teachings of Veselov and Hufsmith “provide[s] a more complete assessment of potential security concerns” and “facilitate[es] a more efficient, targeted review of critical security issues” are generic statements that are frequently found to be insufficient to show motivation to combine. *Id.* 19 (quoting Pet. 23–24).

Seventh, Orca argues that Wiz’s assertion that there is a reasonable expectation of success in combining the teachings of Veselov and Hufsmith fails to achieve what is claimed in the ’685 patent, is contradicted by Wiz’s own public announcement, and is fraught with hindsight bias. PO Resp. 19–20 (citing Pet. 25; Ex. 1001, claims 1, 13, 22; Ex. 2155, 2; Ex. 2154; Ex. 2073 ¶¶ 114–117). Eighth, Orca argues that Wiz fails to show that a person of ordinary skill in the art “would reasonably expect to be able to gather sufficient information from snapshots facilitated by a cloud computing platform in order to determine risk levels of a VM, or to filter or prioritize alerts on that basis.” *Id.* at 20 (citing Ex. 2073 ¶¶ 181–185; Ex. 2412, 11).

In its Reply, Wiz contends that Orca's attacks on the proposed combination of Veselov and Hufsmith fail for several reasons. Pet. Reply 3. Wiz disagrees with Orca's argument that Veselov and Hufsmith are not analogous because Orca "identifies no relevant technical distinctions" between Hufsmith's container or VM images and Veselov's volume images or snapshots. *Id.* at 3–4 (citing PO Resp. 15; Ex. 1400 ¶¶ 16, 18–21). In any event, Wiz argues that Veselov and Hufsmith both analyze the same underlying data (e.g., files, applications, etc.). *Id.* at 4. Wiz also disagrees with Orca's argument that Hufsmith is limited to pre-deployment source-code analysis because "this mischaracterizes Hufsmith and improperly attacks bodily incorporation." *Id.* (citing Ex. 1400 ¶¶ 17, 18, 20, 21, 28; Ex. 1078 ¶¶ 108, 154).

Wiz contends that the "demonstrated benefit[s]" realized by its proposed combination of Veselov and Hufsmith go beyond generic statements. Pet. Reply 4 (citing Pet. 23–25; PO Resp. 19). Wiz also argues that Orca's conclusory denial of Wiz's assertion that combining the teachings of Veselov and Hufsmith is nothing more than the combination of familiar elements according to their known methods to yield predictable results "does not substantively dispute this point." *Id.* at 5 (citing Pet. 22–23; PO Resp. 18–19; *KSR*, 550 U.S. at 416).

In addition, Wiz argues that Orca fails to rebut that there would have been a reasonable expectation of success in making the proposed combination of Veselov and Hufsmith because, in the Petition, Wiz sufficiently addresses the requirement in the challenged claims of detecting sensitive data, without interacting with the VM. Pet. Reply 5 (citing Pet. 25,

40; PO Resp. 19). Wiz also argues that its declarant, Dr. Stavrou, confirms that detecting sensitive data was common practice in the relevant art, with his testimony on this issue being reinforced by the lack of explanation in the specification of the '685 patent regarding how to detect sensitive data. *Id.* at 5–6 (Ex. 1400 ¶¶ 31, 32, 86–88; Ex. 1002 ¶ 55; Ex. 1001; Ex. 1401, 141:11–155:2). Wiz also argues that Orca ignores the evidence of record demonstrating that a person of ordinary skill in the art would have understood that snapshots provided sufficient information, which, according to Wiz, contradicts Orca's assertion that customers thought this was impossible. *Id.* at 6 (citing Ex. 2073 ¶¶ 181–185; Pet. 25; Ex. 1078 ¶¶ 135–143; Ex. 1002 ¶ 112).

In its Sur-reply, Orca maintains that Wiz provides generic motivations to combine the teachings of Veselov and Hufsmith that are “hindsight-plagued.” PO Sur-reply 4 (citing Pet. 23–25; Pet. Reply 4; PO Resp. 14–20). According to Orca, it explains in the Patent Owner Response why a person of ordinary skill in the art would not have selected certain features from Veselov and Hufsmith and combined them “in the normal course.” *Id.* at 4–5 (citing PO Resp. 15–16). More specifically, Orca argues that Veselov and Hufsmith analyze different data for different purposes and “Wiz side-steps these differences.” *Id.* at 5 (citing PO Resp. 15; Ex. 2073 ¶¶ 98, 99, 104, 106–108; Pet. Reply 4–5). Orca asserts that, at best, Wiz demonstrates that Veselov and Hufsmith “*could* be combined, not whether [a person of ordinary skill in the art] *would* have as required.” *Id.* Orca also argues that “Veselov criticizes ‘drawbacks’ of systems requiring ‘complexity of installation and monitoring of the assessment system,’ which is what results

from combining with Hufsmith’s complex multi-scanner system.” *Id.* at 7 (quoting Ex. 1007, 2:42–54) (citing PO Resp. 7–8, 14–20).

Orca contends that Wiz fails to show a reasonable expectation of success in making its proposed combination of Veselov and Hufsmith in the following two additional ways: (1) Wiz does not demonstrate that Veselov’s snapshot analysis would result in generating the same amount of issues as Hufsmith’s container images in a pre-deployment environment, which, according to Orca, undermines Wiz’s motivation to combine relating to “alert fatigue”; and (2) Wiz does not demonstrate that a person of ordinary skill in the art would expect success in analyzing snapshots for sensitive data using cloud computing APIs because Hufsmith only detects vulnerabilities or weaknesses regarding the potential exposure of sensitive data—not the sensitive data itself. PO Sur-reply 7–9 (citing PO Resp. 15–20, Pet. Reply 3–6; Ex. 1400 ¶ 21; Ex. 2154, 2155, 2).

Based on the complete record, Wiz provides at least two reasons as to why a person of ordinary skill in the art would have been motivated to combine the relevant teachings of Veselov and Hufsmith that support a conclusion of obviousness. *See* Pet. 22–25. First, Wiz argues—and we agree—that a person of ordinary skill in the art would have combined the teachings of Veselov and Hufsmith “to provide a more complete assessment of potential security concerns.” *Id.* at 23. As Wiz recognizes in the Petition, Veselov contemplates implementing “any suitable security assessment,” including security assessments defined by rules packages like CVEs or “best practices” packages. Ex. 1007, 2:35–42. Hufsmith provides a more detailed disclosure of a suitable security assessment that would be implemented by

Veselov, such as one that is capable of detecting and reporting security vulnerabilities (e.g., CVEs (Ex. 1078 ¶¶ 8, 84, 104, 113–120)) and the potential exposure of sensitive data (e.g., confidential/restricted information or information pertaining to encryption keys (*id.* ¶¶ 118, 181)).

This particular motivation to combine the teachings of Veselov and Hufsmith also is supported by the testimony of Wiz’s declarant, Dr. Stavrou. Dr. Stavrou testifies that CVEs represent a published set of “vulnerabilities [that] were catalogued by individuals and organizations in the field . . . to facilitate identification and mitigation of . . . known threats.” Ex. 1002 ¶ 50. Dr. Stavrou further testifies that the risks posed by the potential exposure of sensitive data “were well known and routinely mitigated by detecting and reporting unencrypted sensitive data using static and dynamic analysis.” *Id.* ¶ 108. We credit Dr. Stavrou’s testimony on these issues because it is consistent with (1) both Veselov’s and Hufsmith’s disclosures of using security assessments like CVEs (*see* Ex. 1007, 2:35–42; Ex. 1078 ¶¶ 8, 84, 104, 113–120); and (2) Hufsmith’s guidance to avoid the potential exposure of sensitive data (*see* Ex. 1078 ¶¶ 118, 181).

Second, Wiz argues—and we agree—that a person of ordinary skill in the art would have combined the teachings of Veselov and Hufsmith “to improve security by facilitating a more efficient, targeted review of critical security issues.” Pet. 24. Dr. Stavrou testifies that “[i]t was well known that prioritizing and filtering alerts allowed for the rapid identification of which vulnerabilities are the most dangerous to a virtual asset.” Ex. 1002 ¶ 110. Dr. Stavrou further testifies that “it was also well known that prioritizing and filtering alerts allowed determination of which virtual assets are most at

risk.” *Id.* We credit Dr. Stavrou’s testimony in both regards because it consistent with (1) Hufsmith’s disclosure of providing “one or more classifications of the security vulnerability according to various criteria,” which, in turn, “make the security vulnerability faster . . . to assess” (Ex. 1078 ¶ 180); and (2) the general background knowledge in the art pertaining to CVEs (*see, e.g.*, Ex. 1023, 4 (“Agencies should use CVE in . . . alerts identifying the vulnerabilities targeted by active exploits.”)).

Wiz also provides sufficient evidentiary support for its assertion that there would have been a reasonable expectation of success in combining the teachings of Veselov and Hufsmith. *See* Pet. 25; Pet. Reply 5–6. More specifically, we agree with Wiz that modifying Veselov by incorporating Hufsmith’s teaching of detecting vulnerabilities includes detecting the potential exposure of sensitive data was “readily achievable” (*id.*) because Veselov explicitly contemplates implementing “any suitable security assessment,” including security assessments that are defined by “best practices” packages (Ex. 1007, 2:35–41). We also agree with Wiz that modifying Veselov by incorporating both Hufsmith’s risk level assessment (i.e., global weights representing overall risk) and Hufsmith’s filtering and prioritizing of alerts based on the risk level was “readily achievable” (Pet. 25) because Hufsmith discloses advantages associated with providing “alerts relating to potential security vulnerabilities” (Ex. 1078 ¶ 15), and using classification of security vulnerabilities to make them “faster . . . to assess” (*id.* ¶ 180).

We do not agree with the eight reasons Orca provides to support its position that Wiz’s motivations to combine the teachings of Veselov and

Hufsmith are insufficient. *See* PO Resp. 14–20. Rather than address each of the eight reasons identified by Orca separately, we address a few exemplary arguments below.

We do not agree with Orca’s argument that Veselov and Hufsmith are not analogous because Hufsmith’s security assessment is directed to container or VM images, whereas Veselov’s analysis is directed to snapshots (i.e., volume images). *See* PO Resp. 14; PO Sur-reply 4–5. Nor do we agree with Orca’s argument that Hufsmith’s security assessment of container images is incompatible with Veselov’s snapshot-based security assessments of VMs. PO Resp. 15. Veselov generally relates to “performing security assessments of virtualized compute resources,” which Veselov states “are particularly suited for security assessments” of VMs. Ex. 1007, 2:22–25. Veselov correlates VMs with containers by disclosing how “[VMs] themselves may be partitioned into multiple isolated virtual systems, called ‘containers.’” *Id.* at 1:34–36.

Similarly, Hufsmith generally relates to “vulnerability scans of container images.” Ex. 1078 ¶ 2. Although Hufsmith describes its scanning technique “with reference to containers,” Hufsmith discloses that “[these] techniques are applicable to other forms of encapsulated functionality, including virtual machine images.” *Id.* ¶ 149. Orca appears to ignore these overlapping disclosures in Veselov and Hufsmith and, instead, narrowly focuses on Hufsmith’s lack of disclosure regarding snapshot-based assessments. Orca, however, does not explain why Hufsmith’s lack of disclosure regarding snapshot-based assessments would preclude combining the teachings of Veselov and Hufsmith in the manner proposed by Wiz.

We do not agree with Orca's argument that Wiz's proposed combination of Veselov and Hufsmith is based on mischaracterizations, including that Hufsmith only discloses the potential exposure of sensitive data. *See* PO Resp. 15; PO Sur-reply 8–9. As we explain previously when addressing Orca's arguments for element 1.6, we find that Hufsmith's teaching of detecting vulnerabilities includes detecting the potential exposure of sensitive data in a security vulnerability or software weakness would not suggest, at least in some instances, in detecting sensitive data itself. *See supra* Section II.B.5.d. Once again, this holds true in an obviousness evaluation, which does not require an asserted prior art reference to satisfy a claim limitation in every instance. *See Unwired Planet*, 841 F.3d at 1002; *Hewlett-Packard*, 340 F.3d at 1326 (Fed. Cir. 2003).

We also do not agree with Orca's argument that Wiz's proposed combination of Veselov and Hufsmith is based on mischaracterizations, including that Hufsmith provides “alerts” using annotations made by developers in the source code pre-deployment that would be inapplicable to Veselov's post-deployment VM assessments. *See* PO Resp. 16–17; PO Sur-reply 7–8. As we explain previously when addressing Orca's arguments for element 1.8, we find that Hufsmith does not limit its technique for reporting security vulnerabilities and the potential exposure of sensitive data as alerts to a particular environment. *See supra* Section II.B.5.e. As one example, Hufsmith discloses that results engines 54 scans “a distributed application or container image” and “determines combined threat scores for the distributed applications for container images,” and that

the combined threat scores may be considered “during application or container development and deployment.” Ex. 1078 ¶ 108.

Nor do we agree with Orca’s argument that Hufsmith’s benefits relating to “rapid identification of higher-priority assets/risks” and mitigation of “alert fatigue” would be inapplicable to Veselov’s scanning system. *See* PO Resp. 17–18. This argument, once again, attempts to limit Hufsmith’s technique for reporting security vulnerabilities and the potential exposure of sensitive data as alerts to a particular environment, which, as we explain above, contravenes Hufsmith’s actual disclosure. *See* Ex. 1078 ¶¶ 108, 149, 153, 154. This argument also fails to recognize that Hufsmith explicitly discloses providing “alerts relating to potential security vulnerabilities” (Ex. 1078 ¶ 15), and using classification of security vulnerabilities to make them “faster . . . to assess” (*id.* ¶ 180).

Nor do we agree with Orca’s arguments that Wiz merely provides generic statements for combining the teachings of Veselov and Hufsmith that are frequently found insufficient to show motivation to combine. *See* PO Resp. 19. We are mindful of the guidance from the U.S. Court of Appeals for the Federal Circuit that rationales to combine cannot focus on generic statements divorced from the prior art elements, such as testimony indicating the generic desire to “build something better” or to make it “more efficient, cheaper, or . . . more attractive to your customers.” *ActiveVideo Networks, Inc. v. Verizon Comms., Inc.*, 694 F.3d. 1312, 1328 (Fed. Cir. 2012). But as we explain previously, Wiz’s rationales to combine the teachings of Veselov and Hufsmith go beyond such generic statements. As one example, Wiz’s assertion that a person of ordinary skill in the art

would have combined the teachings of Veselov and Hufsmith “to provide a more complete assessment of potential security concerns” takes into account that Veselov explicitly discloses implementing “any suitable security assessment” (Ex. 1007, 2:35–42), such as Hufsmith’s security assessment that detects and reports security vulnerabilities (e.g., CVEs (Ex. 1078 ¶¶ 8, 84, 104, 113–120)) and the potential exposure of sensitive data (e.g., confidential/restricted information or information pertaining to encryption keys (*id.* ¶¶ 118, 181)). *See* Ex. 1002 ¶¶ 50, 108.

Lastly, we do not agree with Orca that Wiz fails to show that there would have been a reasonable expectation of success in making the proposed combination of Veselov and Hufsmith. *See* PO Resp. 20; PO Sur-reply 7–9. To support this argument, Orca directs us to a document indicating that,

[REDACTED]
[REDACTED]
[REDACTED] (Ex. 2412, 11), but it is not clear to us how this [REDACTED]
[REDACTED] bears on Wiz’s proposed combination of Veselov and Hufsmith. Stated differently, Orca does not direct us to, nor can we find, evidence that undermines Wiz’s assertion that there was a reasonable expectation of success in combining the relevant teachings of Veselov and Hufsmith. *See* Pet. 25; Pet Reply 5–6.

*g. Objective Indicia of Non-Obviousness or Secondary Considerations*³

Notwithstanding what the combined teachings of Veselov and Hufsmith fairly suggest to a person of ordinary skill in the art, objective evidence of non-obviousness (so called “secondary considerations”) may lead to a conclusion that the challenged claims would not have been obvious. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Objective evidence of non-obviousness “play[s] an important role as a guard against the statutorily proscribed hindsight reasoning in the obviousness analysis.” *WBIP, LLC v. Kohler, Co.*, 829 F.3d 1317, 1328 (Fed. Cir. 2016). Indeed, objective evidence of non-obviousness “may often be the most probative and cogent evidence in the record” and “must be considered in every case.” *Id.* (first quoting *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1538 (Fed. Cir. 1983), then citing *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling USA, Inc.*, 699 F.3d 1340, 1349 (Fed. Cir. 2012)).

During trial, Orca presents extensive arguments and evidence directed to “long-felt, [but] unresolved need, skepticism regarding the inventions, industry acceptance, industry praise, commercial success, and copying,” which, according to Orca, confirms the non-obviousness of the challenged claims of ’685 patent. PO Resp. 34–62; PO Sur-reply 15–35. In response, Wiz contends that Orca’s arguments and evidence regarding objective indicia of non-obviousness “fail[] at every level” and, therefore, do not

³ Organizationally, we address the various elements of independent claim 1 and the parties’ arguments separately. However, we note that the final determination of obviousness is made with consideration of the claim, as a whole, and in view of Orca’s objective evidence of non-obviousness.

overcome the strong case of obviousness presented in the Petition.

Pet. Reply 14–29. We address the parties’ arguments in turn.

i. Nexus

For us to accord substantial weight to objective indicia of non-obvious or secondary considerations, “the evidence of secondary considerations must have a ‘nexus’ to the claims” (i.e., “there must be ‘a legally and factually sufficient connection’ between the evidence and the patented invention.”) *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (citing *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019)). “The patentee bears the burden of showing that a nexus exists.” *WMS Gaming Inc. v. Int’l Game Tech.*, 184 F.3d 1339, 1359 (Fed. Cir. 1999). Presuming nexus is appropriate when “the patentee shows that the asserted objective evidence is tied to a specific product and that product ‘embodies the claimed features, and is coextensive with them.’” *Fox Factory*, 944 F.3d at 1373 (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). “A finding that a presumption of nexus is inappropriate does not end the inquiry into secondary considerations,” as “the patent owner is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the ‘direct result of the unique characteristics of the claimed invention.’” *Id.* at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)).

In its Patent Owner Response, Orca contends that its “SideScanning™ [technology] practices the challenged claims of the ’685 [p]atent.” PO Resp. 38 (citing Ex. 2074 ¶¶ 26–89; Ex. 2073 ¶ 170). Orca turns to the testimony of Mr. Shua, together with citations to roughly 20 additional documents in

the record, to demonstrate nexus between its SideScanning technology and the limitations of independent claims 1, 13, and 22. *Id.* at 38–39 (citing Ex. 2074 ¶¶ 29–64; Ex. 2067). Orca also asserts nexus between its SideScanning technology and the limitations of dependent claims 2–12 and 14–21. *Id.* at 39–40 (citing Ex. 2074 ¶¶ 65–89).

In its Reply, Wiz contends that the presumption of nexus to Orca’s SideScanning technology “is open and shut” because “[Orca] never addresses coextensiveness.” Pet. Reply 15. Wiz also argues that most of Orca’s nexus arguments either address the SideScanning technology generally or address unrecited/known features, each of which is insufficient to establish nexus by demonstrating that the evidence of non-obviousness is direct result of the unique characteristics of the claimed invention. *Id.* at 17. In particular, Wiz asserts that most of the evidence presented by Orca in support of its nexus arguments addresses agentless scanning, yet Orca does not demonstrate that this feature is required by the challenged claims. *Id.* Wiz asserts that, even if the challenged claims require agentless scanning, there is extensive evidence in the record demonstrating that it was a known feature. *Id.* at 17–18 (*see, e.g.*, Ex. 1002 ¶¶ 57, 88, 89, Ex. 1040, Abstract, ¶¶ 8–12, 23, 43–48, 52; Ex. 1073, 1; Ex. 1400 ¶¶ 78, 79).

In its Sur-reply, Orca clarifies that “[it] doesn’t rely on a presumption [of nexus],” but rather seeks to establish nexus by demonstrating that the secondary considerations are the direct result of the unique characteristics of the claimed invention. PO Sur-reply 15–16 (citing *Fox Factory*, 944 F.3d at 1373–74). Orca asserts that Wiz’s “[o]ther nexus arguments reduce to assertions that each limitation can be individually found in the art,” but

“[o]bjective indicia protects against exactly these hindsight-driven arguments.” *Id.* at 16.

As an initial matter, we need not address whether Orca establishes a presumption of nexus between its evidence based on SideScanning technology and the challenged claims of the ’685 patent because Orca readily admits in its Sur-reply that “[it] doesn’t rely on a presumption [of nexus].” PO Sur-reply 15. Absent a presumption of nexus, we turn to whether Orca sufficiently establishes nexus between its evidence based on SideScanning technology and the challenged claims of the ’685 patent by showing that this evidence is the “direct result of the unique characteristics of the claimed invention.” *Huang*, 100 F.3d at 140. We do not agree with Orca’s nexus arguments for two reasons.

First, rather than provide a detailed explanation of the significance of the evidence bearing on the alleged nexus between its SideScanning technology and the challenged claims of the ’685 patent in the Patent Owner Response itself, Orca merely provides numerous citations to the evidence of record. *See* PO Resp. 38–41. This violates our rule against improper incorporation by reference.⁴ The Board’s informative decision in *Cisco Systems, Inc. v. C-Cation Techs., LLC*, IPR2014-00454 (PTAB Aug. 29, 2014) (Paper 12) (informative) is instructive on this matter. In *Cisco*, the

⁴ In our Order Granting Patent Owner’s Motion for Additional Discovery, we specifically addressed this issue, stating that “[a]lthough establishing nexus will ultimately require a more fulsome analysis, we decline to fault Orca for deferring that full analysis until its Patent Owner Response.” Paper 29, 4.

Board panel explained that citations to “large portions of another document, without sufficient explanation of those portions, amounts to incorporation by reference.” *Cisco*, Paper 12 at 8. Similarly, the Board panel explained that the “practice of citing [a] Declaration to support conclusory statements that are not otherwise supported in the Petition also amounts to incorporation by reference.” *Id.* at 9. Such incorporation by reference is improper because “[a]rguments must not be incorporated by reference from one document into another document.” 37 C.F.R. § 42.6(a)(3); *see also DeSilva v. DiLeonardi*, 181 F.3d 865, 866–67 (7th Cir. 1999) (Incorporation by reference “amounts to a self-help increase in the length of the [] brief. . . . A brief must make all arguments accessible to the judges, rather than ask them to play archaeologist with the record.”).

Upon reviewing the four pages in the Patent Owner Response where Orca presents arguments and evidence pertaining to nexus, Orca attempts to incorporate by reference the following: (1) 63 paragraphs spanning roughly 29 pages of Mr. Shua’s Declaration; and (2) roughly 20 additional documents in the record varying in length. *See* PO Resp. 38–41. Put simply, Orca’s nexus arguments leave us “to play archaeologist with the record.” *DeSilva*, 181 F.3d, at 866–67; *see also Parus Holdings, Inc. v. Google LLC*, 70 F.4th 1365, 1371 (Fed. Cir. 2023) (“It is true that patent owners have no requirement to respond to petitions. However, here, [patent owner] chose to take on an affirmative burden to show that it was the first to make its claimed inventions. Once [patent owner] chose to submit a response and assume that burden, it bore the responsibilities that came with it—including submitting a response that complied with the rules and

regulations of the [U.S. Patent and Trademark Office]. And that includes not incorporating material by reference pursuant to 37 C.F.R. § 42.6(a)(3) and the inclusion of ‘a detailed explanation of the significance of the evidence including material facts’ pursuant to 37 C.F.R. § 42.22.”).

Second, even after reviewing the relevant paragraphs in Mr. Shua’s Declaration and the roughly 20 additional documents in the record, most of the evidence relating to what Orca asserts is embodied in the challenged claims of the ’685 patent turns on the concept of agentless scanning (also referred to as agentless side scanning). *See, e.g.*, Ex. 2076, 7⁵ (“Orca: Introduced the concept agentless side scanning, which allowed for deep visibility into cloud environments, and workloads, without the need to install agents on each workload.” (emphasis omitted)). We understand agentless scanning to require the following two fundamental principles:

(1) “[p]rivileged access to customer’s cloud environment via APIs”; and
(2) “[s]napshot scanning.” Ex. 2026, 3; *see also* Ex. 2074 ¶ 132 (testifying to the same); Tr. 80:10–81:15 (counsel for Orca agreeing that agentless scanning requires two fundamental principles).

Nevertheless, we agree with Wiz’s argument presented in its Reply that the two fundamental principles of agentless scanning were already known in the prior art. *See* Pet. Reply 17–18. For example, as we explain

⁵ Exhibit 2076 is an article titled “Redefining CNAPP: A Complete Guide To the Future of Cloud Security” authored by Francis Odum and James Berthoty, dated September 12, 2024. Wiz filed a verbatim copy of this article as Exhibit 1125. Unless otherwise noted, we refer to the version of this article that is Exhibit 2076.

above in our obviousness analysis of independent claims 1, 13, and 22, Veselov’s snapshot-based scanning service gains access to a virtual computing environment using cloud computing APIs (e.g., API 120 or APIs 338). Ex. 1007 2:64–67, 3:23–27. 5:1–5. Because the two fundamental principles of agentless scanning were already known in the prior art, we find that they do not represent a novel combination or arrangement of known individual elements that would suffice to establish nexus. *See Novartis AG v. Torrent Pharm. Ltd.*, 853 F.3d 1316, 1331 (Fed. Cir. 2017) (stating “the identified objective indicia must be directed to what was not known in the prior art,” “which may well be the novel combination or arrangement of known individual elements”); *Yita LLC v. MacNeil IP LLC*, 69 F. 4th 1356, 1364 (Fed. Cir. 2023) (stating that “case law makes clear that objective evidence of nonobviousness lacks a nexus if it exclusively relates to a feature that was *known* in the prior art—not necessarily well-known” (first and second quotations omitted)).

Independent of the general nexus problem between agentless scanning and the features of the challenged claims of the ’685 patent, Orca’s evidence of non-obviousness is, on balance, relatively weak. We address those issues below.

ii. Long-felt need

“Evidence of a long felt but unresolved need tends to show non-obviousness because it is reasonable to infer that the need would have not persisted had the solution been obvious.” *WBIP*, 829 F.3d at 1332 (citing *Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1325 (Fed. Cir. 2004) (“Absent a showing of long-felt need or the failure of others, the mere

passage of time without the claimed invention is not evidence of nonobviousness.”)).

In its Patent Owner Response, Orca contends that the claimed invention of the '685 patent “solved a long-felt but unmet need for an unobtrusive, comprehensive security solution for dynamic cloud environments.” PO Resp. 35 (citing Ex. 2074 ¶¶ 90–101). Orca argues that conventional methods for protecting cloud computing infrastructures suffered from multiple disadvantages, including that they “failed to adequately address the security of VMs while those VMs were inactive,” and they “failed to provide adequate detection of and protection for sensitive data.” *Id.* at 35–37 (citing Ex. 1001, 1:20–23, 1:36–2:14; Ex. 2078, 5–6, 11; Ex. 2134, 2; Ex. 2136, 2; Ex. 1029, 1; Ex. 2102, 1; Ex. 2103, 2; Ex. 2135, 3; Ex. 2414, 17; Ex. 2152, 5; Ex. 2074 ¶¶ 56, 80–83, 90–101, 118). According to Orca, “there was a long-felt, unmet need for a cloud security solution that could adequately address undetected vulnerabilities and sensitive data.” *Id.* at 37 (citing Ex. 1001, 1:46–52, 1:57–59, 2:1–6, 2:15–16; Ex. 2136, 2–3; Ex. 2137, 1). Orca asserts that Mr. Shua’s recognition of this need motivated him “to found Orca and develop a new agentless deep scanning technique in Orca’s SideScanning™[technology], including as claimed in the '685 [p]atent.” *Id.* at 37–38 (citing Ex. 2076, 7; Ex. 2074 ¶¶ 13–24, 100, 101; Ex. 2104, 2; Ex. 2148, 15; Ex. 2073 ¶¶ 171–180; Ex. 2138, 4).

In its Reply, Wiz contends that Orca’s assertion that it solved “a vague need for ‘unobtrusive, comprehensive’ cloud security and a need for at-rest protection” “[b]oth fall flat.” Pet. Reply 18 (quoting PO Resp. 35–38). Wiz argues that Orca’s purported solution of agentless scanning

was known, and “[t]here is little daylight between the touted features and Veselov.” *Id.* at 18–19 (citing PO Resp. 36–38; Ex. 1400 ¶¶ 79–92). Wiz also argues that the Orca’s assertion regarding the need for sensitive data detection “fails to withstand scrutiny” because companies addressed this need in 2018, and Wiz’s declarant, Dr. Stavrou, confirms that detecting sensitive data was “commonplace.” *Id.* at 19 (citing Ex. 2152, 5, 34, 51; Ex. 1400 ¶¶ 86–88). Wiz asserts that Orca’s other evidence regarding long-felt need has other flaws, including that Orca’s high-level comments about security are not commensurate in scope with the challenged claims, self-interested statements from Mr. Shua are insufficient, and Orca fails to demonstrate that it actually solved the purported need. *Id.* at 19–20 (citing PO Resp. 35–38; Ex. 2074 ¶¶ 97–99; Ex. 2102, 1–2; Ex. 2076, 2, 10, 12–13, 23; Ex. 1400 ¶¶ 93, 94; Ex. 1402, 128:16–129:19).

In its Sur-reply, Orca maintains that, prior to the ’685 patent, there was a long-felt need “for an unobtrusive, comprehensive security solution that also adequately addressed needs for sensitive-data detection and security of inactive VMs.” PO Sur-reply 16 (citing PO Resp. 35–38). Contrary to Wiz’s assertions, Orca argues that it solved this need by pioneering the “concept of agentless sidescanning.” *Id.* (quoting Ex. 2076, 5–7).

According to Orca, [REDACTED]

[REDACTED]

[REDACTED].

Id. at 17–18 (citing Ex. 2406, 12;

Ex. 2400; Ex. 2076, 7; Ex. 2424, 7,⁶ 9). According to Orca, industry reports and Orca's success corroborate prior system failures in solving this long-felt need. *Id.* at 18 (citing Ex. 2152, 5).

Based on the complete record, Orca's arguments and evidence that the claimed invention of the '685 patent solved the long-felt need for an unobtrusive, comprehensive security solution for dynamic cloud environments is weak. *See* PO Resp. 35; PO Sur-reply 16. As we explain above in our obviousness analysis of independent claims 1, 13, and 22, Veselov already teaches the two fundamental principles of agentless scanning required by Orca's SideScanning technology because Veselov discloses how its snapshot-based scanning service gains access to a virtual computing environment using cloud computing APIs (e.g., API 120 or APIs 338). Ex. 1007 2:64–67, 3:23–27. 5:1–5. As a result, the record before us demonstrates that the alleged long-felt need identified by Orca was already met by Veselov. *See Geo. M. Martin Co. v. All. Mach. Sys. Int'l LLC*, 618 F.3d 1294, 1304 (Fed. Cir. 2010) (“Where the differences between the prior art and the claimed invention are as minimal as they are here, . . . it cannot be said that any long-felt need was unsolved.”).

To the extent Orca argues that the long-felt need purportedly solved by the claimed invention of the '685 patent also addresses detecting sensitive data and the security assessment of an inactive VM, these two features were either already known in the prior art or not commensurate in scope with the

⁶ Orca's citation to page 7 of Exhibit 2024 appears to be an inadvertent mistake because the

appears on page 5 of Exhibit 2424.

challenged claims of the '685 patent. *See* PO Resp. 35–37; PO Sur-reply 16–18. Beginning with detecting sensitive data, as we explain above, Hufsmith fairly suggests that detecting vulnerabilities includes detecting the potential exposure of sensitive data in a security vulnerability or software weakness would result, at least in some instances, in detecting sensitive data itself. *See supra* Section II.B.5.d. There is additional evidence in the record confirming that detecting sensitive data within a snapshot of a VM was old and well known at the time of the '685 patent. *See, e.g.*, Ex. 1056 ¶¶ 39 (disclosing “identify[ing] and label[ing] sensitive data contained within a [VM]”), 94 (disclosing “label[ing] and sanitiz[ing] the snapshot of a specific instance of the [VM]”); Ex. 2152, 5⁷ (stating that “[p]erhaps one of the most critical risk vectors when it comes to an organizations cyber exposure is the sensitive data (customer, employee, intellectual property, etc.) that resides within their . . . cloud environments”).

Turning to the security assessment of an inactive VM, this feature is not commensurate in scope with independent claims 1, 13, and 22 of the '685 patent because these claims do not require an inactive VM. *See* Ex. 1001, 9:37–48 (claim 1), 10:29–42 (claim 13), 11:13–25 (claim 22). Only dependent claims 2 and 14 of the '685 patent, and by virtue of dependency, dependent claims 3 and 15, require an inactive VM. *See id.* at 9:55–58 (claim 2—“the virtual machine is inactive”), 10:48–51 (claim 14—“the virtual machine is inactive”). Nevertheless, Wiz argues—and we

⁷ All references to the page numbers in this exhibit from Citizens JPM titled “Cyber 66” Report refer to the page number inserted by Orca in the bottom, right-hand corner of each page in Exhibit 2152.

agree—that Price demonstrates that performing a security assessment on an inactive VM was well known at the time of the ’685 patent because it discloses performing offline analysis of VMs. Pet. 68 (citing Ex. 1048, code (57), ¶¶ 14, 26–29, 32, 42, 45; Ex. 1002 ¶¶ 62, 245, 246).

iii. Skepticism

“Doubt or disbelief by [a person of ordinary skill in the art] regarding the likely success of a combination or solution weighs against the notion that one would combine elements in references to achieve the claimed invention.” *WBIP*, 829 F.3d at 1335. Evidence of skepticism, however, “must be specific to the invention, not generic to the field.” *Auris Health, Inc. v. Intuitive Surgical Operations, Inc.*, 32 F.4th 1154, 1159 (Fed. Cir. 2022) (citing *WBIP*, 829 F.3d at 1335–36).

In its Patent Owner Response, Orca contends that the claimed invention of the ’685 patent “defied skeptics and achieved widespread industry acceptance.” PO Resp. 41 (citing Ex. 2074 ¶¶ 99–104, Ex. 2076, 8, 11; Ex. 2148, 15). According to Orca, [REDACTED] and an article pertaining to the future of cloud security both viewed Orca’s SideScanning technology with skepticism. *Id.* at 41–42 (citing Ex. 2406, 5, 14–15; Ex. 2076, 7, 8; Ex. 2074 ¶¶ 102–104; Ex. 2073 ¶¶ 181–185). Orca further argues [REDACTED]

[REDACTED] its SideScanning technology became widely accepted such that “everyone needed it in order to stay competitive.” *Id.* at 42–43 (first quoting Ex. 2406, 5, then quoting Ex. 2076, 7) (citing Ex. 2406, 12; Ex. 2412, 9, 11;

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

Ex. 2113, 4; Ex. 2074 ¶¶ 99, 106, 107, 112, 119, 120; Ex. 2073 ¶¶ 181–185, 256, 257; Ex. 2103, 1).

In its Reply, Wiz contends that Orca’s evidence of skepticism related to agentless scanning focuses on an “unrecited aspect” of the claimed invention of the ’685 patent that “was known.” Pet. Reply 20 (citing PO Resp. 41–43; Ex. 2076, 7–8, 11; Ex. 2106, 1; Ex. 2406, 5, 12; Ex. 2412, 9–11; Ex. 1400 ¶¶ 95–99). Wiz argues that Orca’s evidence [REDACTED]

[REDACTED] *Id.* at 20 (citing Ex. 2406, 5, 14–15). Wiz argues that Orca’s other evidence of skepticism [REDACTED]

[REDACTED]. *Id.* at 21 (citing, e.g., Ex. 2418, 15).

In its Sur-reply, Orca maintains that it provides evidence of skepticism that was tied directly to the challenged claims of the ’685 patent using [REDACTED] other reports. PO Sur-reply 19 (citing PO Resp. 41–43). For example, Wiz argues that there is nexus with skepticism and the agentless scanning embodied in the challenged claims of the ’685 patent, as evidenced by [REDACTED]

[REDACTED] *Id.* at 19–20 (quoting Ex. 2406, 14) (citing Ex. 2406, 16; PO Resp. 41–42, 45, 60). Orca also argues that Wiz’s assertions that certain documents and testimony are “self-interested” or “hearsay” are erroneous for the following three reasons: (1) the testimony of the named inventor of the ’685 patent—Mr. Shua—is “substantial evidence” of non-obviousness; (2) Wiz ignores the numerous other exhibits and

testimony corroborating Mr. Shua's purported "self-interested" testimony; and (3) Wiz overlooks the significant amount of non-hearsay evidence from Wiz's internal documents. *Id.* at 20–21 (citing, e.g., Exs. 2103, 2104, 2106, 2073, 2135, 2137, 2406, 2412, 2074; Paper 56).

Based on the complete record, Orca's arguments that its evidence of skepticism is specific to the claimed invention of the '685 patent is weak. *See* PO Resp. 41–43; PO Sur-reply 19–21. As one example, Orca directs us to an article stating the following:

There's a conversation worth having about how difficult it was for older providers to come to terms with the success of agentless scanning. They were absolutely right to be skeptics: from a security prospective, agentless scanning was nothing compared to what attacks they were able to detect and protect. They missed however that security teams were not yet in the weeds on these architectures, and didn't know what they didn't know. Agentless scanning was the first step of a security journey, and that's why everyone needed it in order to say competitive.

Ex. 2076, 7.⁸ This alleged skepticism is not particularly helpful to Orca because it does not involve general skepticism regarding whether agentless scanning, which was already known in the art, was feasible. Instead, it reflects skepticism for unclaimed features, such as how well agentless scanning could detect and protect against potential attacks from a security

⁸ Although obscured by the copy of this article filed by Orca as Exhibit 2076, this article also states the following: "Agentless v. agents: Companies that once championed agentless solutions are now all building agents." *Compare* Ex. 2076, 2 (emphasis omitted), *with* Ex. 1125, 2 (emphasis omitted). This statement appears to undermine Orca's assertions that the industry was skeptical of moving towards agentless scanning.

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

iv. Industry Praise

“Evidence that the industry praised a claimed invention or a product which embodies the patent claims weighs against an assertion that the same claim would have been obvious.” *WBIP*, 829, F.3d at 1334. “Industry participants, especially competitors, are not likely to praise an obvious advance over the known art.” *Id.*

In its Patent Owner Response, Orca contends that, following Orca’s introduction of its SideScanning technology and the filing of the patent application that issued as the ’685 patent, Orca received numerous awards for its inventions. PO Resp. 43 (citing Ex. 2074 ¶¶ 144–155; Ex. 2073 ¶ 186). As one example, Orca argues that it won Computer Retail News’s (“CRN’s”) “*20 Coolest Tech Startups of 2020*,” which touted the SideScanning technology as “automatically assess[ing] the security state of every discovered asset” to provide “complete visibility.” *Id.* at 43–44 (quoting Ex. 2119, 6–7). As another example, Orca argues that it won *Forbe’s “Top 20 Cybersecurity Startups to Watch in 2021,”* with *Forbes* stating that Orca is “noteworthy for its innovative approach to providing instant-on, workload-deep security,” and emphasizing Orca’s “patent-

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

pending SideScanning™ technology” that “reads cloud configuration and workloads’ runtime block storage out-of-band.” *Id.* at 44 (quoting Ex. 2120, 7). According to Orca, it received these awards because of its SideScanning technology that is embodied in the challenged claims of the ’685 patent. *Id.* (citing Ex. 2074 ¶¶ 156, 105–108).

Orca further argues that, even more telling of industry praise, is [REDACTED]
[REDACTED]. PO Resp. 45 (citing Ex. 2073 ¶¶ 187–189).

As one example, Orca argues that [REDACTED]
[REDACTED]
[REDACTED] *Id.*

(quoting Ex. 2406, 14–15). As another example, Orca argues that, [REDACTED]
[REDACTED]

[REDACTED] *Id.* (emphasis omitted) (quoting Ex. 2419, 1).

Moreover, Orca asserts that [REDACTED]
[REDACTED]
[REDACTED] *Id.* at 46–47 (citing Ex. 2412, 2–4, 9–11;

Ex. 2414, 18–19). Lastly, Orca asserts that its SideScanning technology was praised outside of Wiz as being “genuinely genius,” “unique,” “elegant,” “like magic,” and “a big leap in cloud security.” *Id.* at 47 (quoting Ex. 2076, 7, 11–12, 31) (citing Ex. 2118, 4, 5; Ex. 2117, 1; Ex. 2414, 18–19).

In its Reply, Wiz contends that Orca’s evidence of industry praise “largely consist of self-interested statements” from Orca’s own press releases or from Orca’s investors and partners. Pet. Reply 21 (citing Ex. 2117; Ex. 2121; Ex. 2122; Exs. 2123–2125; Exs. 2128–2130; Ex. 2132). Wiz argues that several of the awards relied on by Orca to demonstrate

industry praise were also sponsored by Orca’s own investors and at least one award was commissioned by Orca itself. *Id.* (citing Ex. 1400 ¶¶ 100–102; Ex. 1402, 177:3–184:1; Ex. 2128). Wiz also argues that Orca’s reliance on Wiz’s own documents to demonstrate industry praise “falls flat” because

[REDACTED]
[REDACTED]
[REDACTED] *Id.* at 22 (citing Ex. 2400; Ex. 2401; Ex. 2406; Ex. 2419; Ex. 2424, 9; Ex. 1007, 2:27–41, 3:29–4:4, 5:1–5; Ex. 1400 ¶¶ 79–83, 86–88, 105; Pet. 39–40; Ex. 1056 ¶¶ 38, 60, 61; Ex. 1078 ¶¶ 118, 181). Wiz argues that Orca’s reliance on [REDACTED]

[REDACTED] *Id.* (citing PO Resp. 46–47; [REDACTED]; Ex. 1400 ¶¶ 79, 106; Pet. 45–48; Ex. 1002 ¶¶ 157, 178–180).

In its Sur-reply, Orca contends that Wiz’s piecemeal arguments regarding industry praise fail for the following reasons: (1) the press releases cannot be considered “self-interested” statements because they describe “awards *Orca received* from **outside** sources”; (2) Orca demonstrates that the awards were the result of a novel combination or arrangement of claimed features; (3) many of the awards received by Orca were from third parties—not investors and partners; (4) the testimony of Wiz’s declarant, Dr. Stavrou, characterizing Orca’s documents as “competitor overviews summarizing [Orca’s] marketing” or “diplomatic sales-pitch phrasing” should be entitled to little, if any, weight because Dr. Stavrou is not a marketing expert; and (5) [REDACTED]

PO Sur-reply 30–33 (quoting Pet Reply 22) (citing Exs. 2121–2125, 2128, 2129; PO Resp. 43–47; Ex. 2172, 8:5–9, 15:11–13, 20:11–17, 21:9–13, 30:3–10, 31:1–9, 67:10–68:1, 69:4–17, 112:1–17, 114:20–115:11, 132:15–17; Ex. 2120, 7; Ex. 2119, 6–10; Ex. 2400; Ex. 2401; Ex. 2419; Ex. 2416, 1, 4).

Based on the complete record, we agree with Orca’s arguments and evidence that there was some evidence of industry praise for its SideScanning technology. *See* PO Resp. 43–47; PO Sur-reply 30–34. As Orca correctly notes in its Patent Owner Response, its SideScanning technology received recognition from both CRN and Forbes. *See* Ex. 2119, 6–7; Ex. 2120, 7. More importantly, the recognition from Forbes regarding Orca’s SideScanning technology appears to implicate specific claimed features in the ’685 patent, such as “read[ing] cloud configuration,” “detecting vulnerabilities,” and detecting “weak or leaked passwords and unsured PII.” Ex. 2120, 7. Contrary to Wiz’s assertions, this recognition from both CRN and Forbes does not appear to have a connection with Orca’s own marketing material. *See, e.g.,* Exs. 2121, 2122, 2124, 2125, 2128–2130, 2132 (each of which includes an “Orca Security” label in the top, left-hand corner of the title page); *see also Bayer Healthcare Pharms. V. Watson Pharms., Inc.*, 713 F.3d 1369, 1377 (Fed. Cir. 2013) (explaining that “self-referential commendation fall[s] well short of demonstrating true industry praise”). Nor do CRN and Forbes appear to have a connection with Orca’s investors and partners. *See, e.g.,* Exs. 2129, 2132, 2145 (identifying

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

Redpoint Ventures, Notable Capital, and YL Ventures as investors); *see also* Ex. 1402, 177:3–184:1 (Mr. Shua confirming that Redpoint Ventures, Notable Capital partner, and YL Ventures are all investors in Orca).

We also agree with Orca that there is some evidence indicating [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. *See, e.g.,* *Power–One, Inc. v. Artesyn Techs., Inc.*, 599 F.3d 1343, 1352 (Fed. Cir. 2010) (explaining that industry praise and, more specifically, praise from a competitor, tends to indicate that the claimed invention would not have been obvious).

Lastly, we agree with Orca that it introduces some evidence that its SideScanning technology was well-received in the industry of cloud computing security. Orca provides an article that refers to Orca’s “agentless side scanning” as “a genuinely genius innovation.” Ex. 2076, 7. This same article states that “Orca Security made a big leap in cloud security with the introduction of its patented agentless SideScanning technique” by providing a “unique method.” *Id.* at 31. More importantly, this recognition of Orca’s SideScanning technology appears to implicate specific claimed features in

the '685 patent, such as indicating that it “has proven highly effectively for vulnerability assessments and scanning.” *Id.*

Bottom line, there is some evidence to suggest that the industry praised Orca and its SideScanning technology.

v. Copying

“Copying may indeed be another form of flattering praise for inventive features.” *Crocs, Inc. v. Int’l Trade Comm’n*, 598 F.3d 1294, 1311 (Fed. Cir. 2010). “[C]opying requires evidence of efforts to replicate a specific product.” *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010). “This may be demonstrated either through internal documents; direct evidence such as disassembling a patented prototype, photographing its features, and using the photograph as a blueprint to build a virtually identical replica; or access to, and substantial similarity to, the patented product (as opposed to the patent).” *Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1325 (Fed. Cir. 2004) (internal citations omitted).

“We note, however, that a showing of copying is only equivocal evidence of non-obviousness in the absence of more compelling objective indicia of other secondary considerations.” *Ecolochem, Inc. v. S. Cal. Edison Co.*, 227 F.3d 1361, 1380 (Fed. Cir. 2000); *see also In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995) (“[M]ore than the mere fact of copying by an accused infringer is needed to make that action significant to a determination of the obviousness issue.” (quoting *Cable Elec. Prods. v. Genmark, Inc.*, 770 F.2d 1015, 1028 (Fed. Cir. 1985))).

In its Patent Owner Response, Orca contends that Wiz copied Orca’s SideScanning technology. *See* PO Resp. 48–58; PO Sur-reply 21–30. Orca

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

argues that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] *Id.*

Based on the complete record, Orca’s arguments demonstrate that the evidence of copying is weak. We begin our copying analysis by first addressing Orca’s evidence of access, and then we turn to its evidence of substantial similarity.

I. Access

Orca contends that Wiz’s knowledge of, and access to, Orca’s SideScanning technology began when Mr. Avi Shua, the named inventor of the ’685 patent, met with Wiz’s co-founder, [REDACTED]. PO Resp. 50 (citing Ex. 2074 ¶¶ 121–125). The meeting occurred on May 27, 2019, [REDACTED] (“the May 2019 meeting”). Ex. 2074 ¶ 122; [REDACTED]. Mr. Shua testifies that “Gil Geron, another of Orca’s co-founders and current [Chief Executive Officer], and I presented Orca’s Cloud Security Platform to Wiz’s founder [REDACTED] [REDACTED] after I filed the ’718 [p]rovisional [a]pplication from which the ’685 [p]atent claims are derived.” Ex. 2074 ¶ 122.

As to the substance of what was discussed at the May 2019 meeting, Mr. Shua provides the following testimony:

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

At this May 2019 meeting, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Ex. 2074 ¶¶ 123–124

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] We have no evidence to contradict this testimony, and we find it credible for what it says. Yet, Mr. Shua’s testimony says little more than Orca’s SideScanning technology enabled agentless scanning. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

[REDACTED] Based on Mr. Shua's cited testimony, we find that one of Wiz's founders had access to the idea of agentless scanning in May 2019. We decline, however, to speculate that anything additional was disclosed at the May 2019 meeting.

Fast forward over a year, and [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Orca asserts that, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁹ [REDACTED] Beyond Networks was the original name for Wiz. Ex. 1414 ¶ 5.

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] As we note above, the details of the May 2019 meeting are sparse.

Wiz, for its part, introduces testimony and documentary evidence to show that [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Mr. Luttwak testifies that

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Mr. Luttwak testifies that

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Mr. Luttwak testifies that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In its Sur-reply, Orca counters that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] As another example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

We have reviewed Mr. Luttwak's deposition testimony, in which he explains that [REDACTED]

[REDACTED]. Mr. Luttwak testifies that [REDACTED]

[REDACTED].
Mr. Luttwak also testified that [REDACTED]

[REDACTED]. In light of Mr. Luttwak's cited deposition testimony, we can understand why [REDACTED]

[REDACTED]. Even assuming, however, that [REDACTED] which the evidence does not show, Wiz's documentary evidence still shows Wiz's development of its own product, including particular API calls, before [REDACTED].

Regarding the May 2019 meeting between Mr. Shua and Mr. Costica, Orca asserts that Wiz "doesn't dispute the meeting happened, challenge Mr. Shua's credibility, or introduce evidence contradicting Mr. Shua's testimony [that he] presented SideScanning and its implementation aspects." PO Sur-reply 23 (citing Ex. 2173, 46:22–47:21; Ex. 1402, 197:6–19; Ex. 2074 ¶¶ 122–125). The problem with this argument is that Mr. Shua's testimony [REDACTED]

[REDACTED] other than that it "enabled agentless cloud security, avoiding the need for installation of agents" and "us[ed] cloud

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

computing APIs.” Ex. 2074 ¶¶ 123, 124. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Orca also criticizes Wiz for “with[holding] Exhibits 1404-1413 until its Reply,” thereby “precluding Orca from addressing them.” PO Sur-reply 22. Orca, however, argued objective indicia of non-obviousness for the first time in its Patent Owner Response and our rules governing this proceeding permits Wiz to address those arguments. 37 C.F.R. § 42.23(b) (“A reply may only respond to arguments raised in the corresponding opposition, patent owner preliminary response, patent owner response, or decision on institution.”); *Anacor Pharm., Inc. v. Iancu*, 889 F.3d 1372, 1380–81 (Fed. Cir. 2018) (“[T]he petitioner in an [IPR] proceeding may introduce new evidence after the petition stage if the evidence is a legitimate reply to evidence introduced by the patent owner”). Wiz was not required to anticipate Orca’s copying arguments and produce, in the first instance with the Petition, all evidence showing how it developed its accused products.

Orca also argues that [REDACTED]

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

[REDACTED]. Although some of the documents [REDACTED], as evidenced by Exhibits 2404 and 2405, are dated before [REDACTED], the evidence shows that the earliest that Wiz accessed those documents was [REDACTED]. Ex. 2404 (email timestamp).

Orca argues that, [REDACTED], still other materials describing Orca's SideScanning were unquestionably 'publicly available . . . and accessible to [Wiz] [REDACTED].'" PO Sur-reply 28 (alterations by Orca) (quoting *Medtronic Inc. v. Teleflex Innovations S.a.r.l.*, 70 F.4th 1331, 1340 n.7 (Fed. Cir. 2023)). In support of this argument, Orca contends that an "Orca-published video in October 2019 described implementation of Mr. Shua's 'patent-pending' technology in SideScanning, with cloud 'APIs that we are using in quite a novel way that read the underlying block storage,' . . . where 'vulnerability management is a critical part' Orca is able to 'alert on.'" *Id.* at 28–29 (citing Ex. 2133, 3, 5; Ex. 2074 ¶ 48).

This evidence shows that Mr. Shua discussed SideScanning technology in the public domain, but it does not appear to mention "snapshots," which are at the heart of the challenged claims of the '685 patent. Ex. 2133 (transcript of YouTube video at Ex. 2099 (*see* PO Resp. 27)). Also, this document touts features of SideScanning technology other than performing snapshot analysis to detect vulnerabilities and sensitive data that is required by the challenged claims of the '685 patent, such as looking for misconfigurations. Ex. 2133, 6 ("The SideScanning is the enabling

technology that gives you access to the underlying bits and bytes that describe the running cloud environment. And then from that, you can reconstruct a model of everything, even the instances or cloud assets that the company might not even know about. And then run a series of best-of-breed tests on that model to look for misconfigurations, vulnerabilities, etc. Do I have it right?” “Yes, you have it exactly right.”); *see also* Ex. 2133, 8 (noting a “very beautiful, very polished” user interface). Thus, even if Wiz accessed this YouTube video, it is not clear that copying everything that’s described in the video would result in copying “the unique characteristics of the claimed invention,” as asserted by Orca. PO Sur-reply 15–16 (citing *Fox Factory*, 944 F.3d at 1373–74).

At best, the evidence of record prior to [REDACTED] shows that one of Orca’s co-founders heard about SideScanning technology, which “enabled agentless cloud security, avoiding the need for installation of agents” and “us[ed] cloud computing APIs.” Ex. 2074 ¶¶ 123, 124. The evidence also shows that some high level overviews of the SideScanning technology were available publicly. *See* Ex. 2133.

Wiz’s documentary evidence also contradicts Orca’s assertions that Wiz’s purported [REDACTED] demonstrates copying. *See* PO Resp. 51–52. For example, Dr. Kaeli testifies as follows:

[REDACTED]

[REDACTED]
[REDACTED]. In AWS, a policy “is an object... that, when associated with an identity or resource, defines their permissions.” Ex.2159 at 1. [REDACTED]
[REDACTED]

[REDACTED].

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]. Although Dr. Kaeli focuses on particular API calls and policies, the '685 patent itself provides no detail on what actions must be included in a policy in order to implement the claimed inventions. Instead, it simply says that “in AWS, a cross account policy service can be utilized to allow interfacing the client environment 130 with the security system 140.”

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

does not mention any particular API calls [REDACTED]

[REDACTED].”

Furthermore, Orca argues that Wiz initially started down one path and then “quickly pivoted to copying Orca’s inventions, deliberately and expressly.” PO Resp. 48–49 (citing Ex. 2406, 14; Ex. 2402, 1; Ex. 2403, 2). More specifically, Orca argues that [REDACTED]

[REDACTED]. To support this argument, Orca relies on [REDACTED]

[REDACTED]. Mr. Shua, however, testifies that “[i]n early 2020, [he] began hearing rumors that there was a new company in ‘stealth mode’ that was developing an agentless cloud computing platform that was very similar to Orca’s” and that this “company turned out to be Wiz.” Ex. 2074 ¶ 126. And as we identify previously, Orca asserts that [REDACTED]

[REDACTED]. PO Resp. 53 (citing Ex. 2308, 1–2). Thus, the evidence of record does not appear to show Wiz pivoting from one technology in [REDACTED] to another technology later. Further, the two other documents cited by Orca do not support its argument in this regard because they are from [REDACTED], respectively. Exs. 2402, 2403.

2. Substantial Similarity

Orca argues substantial similarity first by explaining how Wiz’s cloud computing platform purportedly “practices the challenged claims,” like Orca’s SideScanning technology. PO Resp. 54. Orca then proceeds to cite

various documents that purportedly show similarities because Wiz's and Orca's products. *Id.* at 54–56.

We take this opportunity to note that Orca's arguments for substantial similarity are presented at a high level. For example, to show that Wiz's cloud computing platform that uses “workload scanning” purportedly practices the challenged claims of the '685 patent, Orca provides a brief statement for each limitation or group of limitations that require us to cull through citations to Mr. Shua's and Dr. Kaeli's Declarations for more explanation. PO Resp. 54–56. In particular, Orca argues that Wiz's “workload scanning” includes the following functionality:

- establishes interfaces between client environments and Wiz's back-end security components ([elements] 1.1, 13.1, 22.1);
- uses cloud computing platform APIs to identify virtual disks of VMs and to query and receive location information about such disks ([elements] 1.2–1.4, 13.2–13.3, 22.2–22.3);
- generates at least one snapshot of the virtual disks of the VM ([element] 1.5);
- emulates virtual disks of VMs so the “scanner has read-only access to the scanned disk” ([elements] 13.4, 22.4);
- analyzes snapshots to detect vulnerabilities and sensitive data while requiring no interaction with the VM ([elements] 1.6, 13.5, 22.5);
- determines risk level of a VM ([elements] 1.7, 13.6, 22.6); and
- reports detected vulnerabilities and sensitive data “such as PII” and “alerts with laser precision” . . . , which are

filtered and prioritized based on the determined risk level of the VM . . . ([elements] 1.8, 13.7, 22.7).

PO Resp. 54–5567 (citations omitted). Orca’s analysis as to how its SideScanning technology practices independent claims 1, 13, and 22 of the ’685 patent uses similar, broad allegations, which, as we explain above, amounts to improper incorporation by reference. *See* PO Resp. 38–39. Putting aside the lack of a detailed explanation in the Patent Owner Response itself, the string-cited evidence largely identifies functionality

As one example, for elements 1.1, 13.1, and 22.1, Dr. Kaeli testifies that “Wiz’s Workload Scanner is based on assigning privileges to access and scan an environment using cloud APIs,” and that it “includes an onboarding process where a client environment provides Wiz’s Workload Scanner with ‘privileges’ that allow access to an environment and to scan the environment using cloud APIs,” which “establishes an interface between a client organization’s cloud computing environment implemented by one or more cloud computing platforms.” Ex. 2073 ¶¶ 234, 235.

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

[REDACTED]

[REDACTED].

As another example, for elements 1.2–1.4, 13.2–13.3, and 22.2–22.3,

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

As yet another example, for element 1.5, Dr. Kaeli cites [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. In

addition, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

[REDACTED]

For element 1.6, Dr. Kaeli testifies that “Wiz performs ‘vulnerability analysis’ based on the snapshot.” Ex. 2073 ¶ 246. For element 1.7, Dr. Kaeli testifies that Wiz’s cloud computing platform “provides vulnerability analysis identifying . . . numbers of ‘critical issues,’ ‘high issues,’ ‘medium issues,’ and ‘low issues.’” *Id.* ¶ 250 (citing Ex. 2165, 8).

For element 1.8, Dr. Kaeli testifies that “Wiz’s Workload Scanner performs ‘Risk-based prioritization’ of vulnerabilities,” “Wiz’s [cloud computing] platform . . . reports sensitive data.” and that “Wiz’s Workload Scanner reports issues as alerts.” Ex. 2073 ¶¶ 253–255 (citing Ex. 2165, 8, 14–15; Ex. 2155, 1, 3; Ex. 2157, 4). Dr. Kaeli’s cited support includes a screenshot titled “Stage 6: Vulnerability analysis” and captioned as follows: “Example vulnerability dashboard that prioritizes issues by contextual severity.” Ex. 2165, 8. The document further states: “[a]fter scanning, the tool will generate a comprehensive list of identified vulnerabilities, order them based on severity, filter away false positives, and provide options for remediation.” *Id.*

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

We also reviewed Mr. Shua’s string-cited testimony about how Wiz’s cloud computing platform that uses “workload scanning” purportedly practices the challenged claims of the ’685 patent, and his testimony similarly relies on high-level disclosures of API calls and vulnerability scanning that [REDACTED]

[REDACTED] Ex. 2074 ¶¶ 128–137. For example, Mr. Shua testifies that “Wiz says its workload scanner uses cloud computing APIs and is for ‘creating, sharing, and deleting snapshots’ where the ‘scanner has read-only access to the scanned disk.’” *Id.* ¶ 135. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In addition, Mr. Shua cites “an exemplary image showing Wiz’s ‘CISA Known Exploit Vulnerabilities Catalog CVEs dashboard’” as evidence of copying. Ex. 2074 ¶ 137 (citing Ex. 2147, 2). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Moreover, the document cited by

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

Mr. Shua states that “Wiz supports the new CISA Known Exploited Vulnerabilities (KEV) Catalog as a source of exploit intelligence to vulnerability findings, on top of other sources,” and that “CISA, the Cybersecurity & Infrastructure Security Agency, released a binding operational directive to reduce the significant risk of known exploited vulnerabilities.” Ex. 2147, 1. It is not clear to us how Wiz’s compliance with “binding operational directive” from a United States government agency is indicative of Wiz copying Orca’s SideScanning technology.

Orca also relies on other documents that purportedly show substantial product similarity. PO Resp. 56–59. One document relied on by Orca includes [REDACTED]

[REDACTED]. Orca argues that another document it relies on shows that a [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]. Orca also relies on other documents that [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]. Although the presentation of this evidence may show that there were some similarities between Wiz’s and Orca’s products, Orca does not tie this evidence specifically to the challenged claims of the ’685

patent. *Cf.* PO Sur-reply 15 (“Orca showed how objective evidence ‘tied to the combination of features’ claimed “as a whole” demonstrated Wiz’s piecemeal obviousness arguments were hindsight-biased.”).

3. *Summary of Copying Evidence*

In summary, we find that one of Wiz’s founders had access to the idea of agentless scanning from Mr. Shua in May 2019. *See supra* Section II.B.5.g.v.1. It may have been that Wiz took this broad concept of agentless scanning from a meeting with Mr. Shua in May 2019, and began developing its own product based on that idea. But even if Wiz copied an “‘API-centered approach’ for agentless security from Orca’s SideScanning™ [technology]” (Ex. 2074 ¶ 138), this does not “show that it is the claimed combination as a whole that serves as a nexus for the objective evidence.” *WBIP*, 829 F. 3d at 1330; *cf.* PO Sur-reply 16 (“And here the ‘claimed combination as a whole [] serves as nexus for the objective evidence.’” (quoting *WBIP*)).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] That is, the evidence of record shows “a competitor’s independent and contemporaneous development of a similar product,” which “may, in some cases, even suggest the patented product *would* have been obvious.” *Medtronic*, 70 F.4th at 1339.

Moreover, as we explain above in our obviousness analysis of independent claims 1, 13, and 22, Veselov already teaches the two

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

fundamental principles of agentless scanning required by Orca’s SideScanning technology because Veselov discloses how its snapshot-based scanning service gains access to a virtual computing environment using cloud computing APIs (e.g., API 120 or APIs 338). Ex. 1007 2:64–67, 3:23–27, 5:1–5. To the extent Wiz copied this idea of agentless scanning based on the May 2019 meeting, the copying would not be tied to “unique characteristics of the claimed invention” (*Fox Factory*, 944 F.3d at 1373–74), but rather to an idea already “within the public domain” (*Medtronic*, 70 F.4th at 1339). *See Yita*, 69 F.4th at 1364.

Lastly, Wiz argues—and we agree—that Orca’s evidence in support of copying shows “market monitoring,” which Wiz asserts is “a standard competitive practice” and “not indicative of copying patents/product.” Pet. Reply 25. For example, referring to Exhibit 2308, Mr. Shua testifies as follows:

[REDACTED]

Ex. 2074 ¶ 128; *see also id.* ¶ 126 (Mr. Shua also testifies that, based on “direct competition” between Wiz and Orca, Wiz “appeared” to copy Orca’s SideScanning technology). This cited testimony appears to support Wiz’s assertion [REDACTED]

[REDACTED] suggesting a market in which parties “typically copy any

development by their competitors, whether patented or not.” *Wm. Wrigley Jr. Co. v. Cadbury Adams USA LLC*, 683 F.3d 1356, 1364 (Fed. Cir. 2012).

vi. Commercial Success

When “a product attains a high degree of commercial success, there is a basis for inferring that [attempts to a solution] have been made and have failed.” *Merck & Co. v. Teva Pharm. USA, Inc.*, 395 F.3d 1364, 1376 (Fed. Cir. 2005). Evidence of commercial success, however, “must be due to the merits of the claimed invention beyond what was readily available in the prior art.” *J.T. Eaton & Co. v. Atl. Paste & Glue, Co.*, 106 F.3d 1563, 1571 (Fed. Cir. 1997) (citing *Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1580, (Fed. Cir. 1983)).

In its Patent Owner Response, Orca contends that, after filing a provisional application in January 2019 that ultimately led to the ’685 patent and introducing its SideScanning technology later that year, “Orca obtained a remarkable amount of investment.” PO Resp. 58 (citing Ex. 2074 ¶¶ 105, 106, 108–120; Ex. 2149; Ex. 2073 ¶¶ 256–258). According to Orca, it raised \$6.5 million dollars of funding in June 2019, it raised another \$75 million dollars of funding in 2020, and it raised investments totaling \$550 million in 2021, thereby making Orca’s overall value as a company over \$1 billion. *Id.* at 58–59 (citing Ex. 2107, 2–3; Ex. 2109, 1–2; Ex. 2110, 1; Ex. 2111, 1–2, 4; Ex. 2112, 1–4; Ex. 2113, 1–2; Ex. 2139, Ex. 2140, 1–2; Ex. 2065, 2–4; Ex. 2074 ¶¶ 109–120). Orca asserts that these funding announcements demonstrate that Orca’s commercial success is attributable to “the cloud computing provider API-based technique for analyzing

snapshots for vulnerabilities and sensitive data” that is claimed in the ’685 patent. *Id.* at 59–60 (citing Ex. 2113, 1, 3, 4).

Orca further contends that, from 2019 to 2024, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] PO Resp. 60–61 (citing Ex. 2074 ¶¶ 106, 107, 121; Ex. 2067, 1, 3; Ex. 2312). Orca also argues that the significant commercial success of Wiz’s cloud computing platform should be attributed to Orca because, after Wiz purportedly copied Orca’s “sensitive data scanning” and introduced this feature in November 2022, Wiz’s annual revenue grew from \$100 million to \$500 million over the next two years. *Id.* at 61–62 (citing Ex. 2116, 1, 2; Ex. 2141, 2; Ex. 2142; Ex. 2153).

In its Reply, Wiz contends that Orca fails to demonstrate commercial success because its “startup financing evidence consists of self-interested statements and articles quoting [the same].” Pet. Reply 27 (citing PO Resp. 58–60). Wiz argues that Orca’s revenue arguments also fail because Orca provides no market share data, nor does Orca discuss sales as compared to the relevant market. *Id.* at 27 (citing PO Resp. 60–61; Ex. 1402, 107:18–113:8, 118:17–123:10). Wiz asserts that, setting aside the apparent inflation of Orca’s annual revenue resulting from the sales of its SideScanning technology, the evidence of record demonstrates [REDACTED] [REDACTED]. *Id.* at 27–28 (citing Ex. 2076, 21; Ex. 2312). Lastly, Wiz argues that Orca’s cursory discussion of Wiz’s cloud computing

platform falls short because it does not demonstrate nexus, and it overlooks that “Wiz’s true strength” was not agentless scanning, but rather meeting its customer’s evolving needs. *Id.* at 28 (quoting Ex. 2076, 7–8) (citing PO Resp. 61–62; Ex. 1400 ¶¶ 7–8).

In its Sur-reply, Orca maintains that the evidence of commercial success demonstrates that it achieved a \$1 billion plus valuation less than two years after the introduction of the SideScanning technology, which, in turn, powered [REDACTED] in revenue. PO Sur-reply 34 (citing PO Resp. 58–62). Orca also argues that it provided market share data that confirms Orca invented the agentless scanning market, Wiz’s purported copycat product was the only competitor in 2021, and, 5 years after commercialization, Orca’s revenue placed it in the top five cloud computing companies. *Id.* at 34–35 (citing PO Resp. 60; Pet. Reply 27–28; Ex. 2076, 21). Lastly, Orca argues that Wiz’s own press releases attributed Wiz’s commercial success to a feature it copied from Orca. *Id.* at 35 (citing PO Resp. 54–58, 60–62; Ex. 22172, 112:1–17, 112:20–113:4, 113:18–21; Ex. 2400).

Based on the complete record, Orca’s evidence demonstrates that it achieved some commercial success in the relevant market. Orca, however, has not established the requisite connection between that commercial success and claimed features that were not already known in the art. Beginning with Orca’s funding/investment arguments (*see* PO Resp. 58–60; PO Sur-reply 24), Orca does not direct us to, nor can we find, case law indicating how we should weigh third party funding/investment in the context of commercial success. *See* Tr. 137:18–138:13 (counsel for Orca

[REDACTED]

IPR2024-00865
Patent 11,693,685 B2

acknowledging that there isn't "a lot of cases where they talk about the investment"). Nevertheless, Orca does not establish that the third party funding/investment obtained by Orca was due to the actual merits of the claimed invention of the '685 patent beyond what was already known in the prior art. *See J.T. Eaton*, 106 F.3d at 1571.

Turning to Orca's revenue arguments (*see* PO Resp. 60–61; PO Sur-reply 34), the only evidence that Orca provides to demonstrate [REDACTED] [REDACTED] revenue purportedly generated from sales of its SideScanning technology is Exhibit 2312, which, on its face, appears to corroborate Orca's assertions that it generated [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

At best, Orca introduces an article into evidence that indicates that Orca was one of at least seven "major players" in the relevant market. Ex. 2076, 20–21 [REDACTED]

[REDACTED]

[REDACTED]. The article estimates that Orca only generated \$110 million of revenue [REDACTED]

[REDACTED] which amounts to roughly 19.6% of the relevant market that generated total sales exceeding \$2.15 billion. Ex. 2076, 21. When considering the limited evidence of market share in this record, we are of the view that Orca achieved some level of commercial success. Here again, however, Orca has not established that its general commercial success as a

company is tied to its SideScanning technology, nor has it established that it is due to claimed features that were not already known in the prior art.

Lastly, we do not agree with Orca’s argument that commercial success of Wiz’s cloud computing platform should be attributed to Orca because Wiz purportedly copied the feature of “sensitive data scanning” from Orca. *See* PO Resp. 61–62; PO Sur-reply 35. The particular feature of “sensitive data scanning” was already known in the prior art before the effective filing date of the ’685 patent. *See Ormco Corp. v. Align Technology, Inc.*, 463 F.3d 1299, 1312 (Fed. Cir. 2006) (“[I]f the feature that creates the commercial success was known in the prior art, the success is not pertinent.”). As we explain above, we find that Hufsmith fairly suggests that detecting vulnerabilities includes detecting the potential exposure of sensitive data in a security vulnerability or software weakness would result, at least in some instances, in detecting sensitive data itself. *See supra* Sections II.B.5.d and II.B.5.g.ii. There is additional evidence in the record confirming that detecting sensitive data within a snapshot of a VM was old and well known at the time of the ’685 patent. *See* Ex. 1002 ¶ 108; Ex. 1056 ¶¶ 39, 94; Ex. 1078, 118, 181; Ex. 2152, 5. Furthermore, we disagree with Orca’s assertion that Wiz copied the “sensitive data scanning” feature from Orca because [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

h. Summary

In summary, absent a presumption of nexus, Orca does not establish nexus between its evidence based on SideScanning technology and the challenged claims of the '685 patent by showing that this evidence of non-obviousness is the “direct result of the unique characteristics of the claimed invention.” *Huang*, 100 F.3d at 140. Independently of establishing nexus between its SideScanning technology and the challenged claims of the '685 patent, we find that the evidence of long-felt need, skepticism, and copying is weak, and despite there being some evidence of industry praise and commercial success, Orca has not shown that the evidence of industry praise and commercial success is connected to claimed features that were unknown in the prior art.

On balance, Orca’s evidence of non-obviousness does not overcome Wiz’s strong case of obviousness as to independent claims 1, 13, and 22. *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). Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the evidence that independent claims 1, 13, and 22 would have been obvious over the combined teachings of Veselov and Hufsmith.

6. Claims 2 and 14

Claim 2 depends from independent claim 1, and further recites “wherein during the analysis of the at least one snapshot, the virtual machine is inactive wherein the snapshot includes a page file of memory associated

with the virtual machine.” Ex. 1001, 9:55–58. Claim 14 recites the same limitation, but it depends from independent claim 13. *Id.* at 10:48–51.

In its Petition, Wiz contends that Veselov teaches the claimed “wherein during the analysis of the at least one snapshot, the virtual machine is inactive” because it suggests analyzing the VM while it is inactive because “most of Veselov’s snapshot-based assessment techniques require no interaction with the original VM.” Pet. 45. According to Wiz, this “at least suggests analyzing the snapshot while the VM is inactive, [because] its analysis does not depend on the state of the original VM during the analysis step.” *Id.* at 45–46 (citing Ex. 1002 ¶¶ 177, 178). Wiz argues that it would have been readily apparent to analyze Veselov’s snapshot while the VM is inactive because this “option [is] consistent with common practice in the field,” and “snapshot-based security assessments were routinely performed while the target resource was powered off or suspended (two types of ‘inactive’ states).” *Id.* at 46 (citing Ex. 1002 ¶¶ 178, 179).

Wiz also contends that Veselov teaches the claimed “wherein the snapshot includes a page file of memory associated with the virtual machine” for two reasons. *See* Pet. 46–48. First, Wiz argues that, even when powered off, “[a] VM’s operation system would . . . typically maintain [a page file] on a virtual disk,” “meaning this type of page file would typically be included in the disk image for snapshots captured in such situations.” *Id.* at 47 (citing Ex. 1002 ¶¶ 24–28, 182). Second, Wiz argues that “a [person of ordinary skill in the art] would have known that the snapshots of running/suspended VMs in common virtualization platforms typically included a page file representing the state of machine memory.”

Id. at 47 (citing Ex. 1002 ¶¶ 36, 183; Ex. 1049, 940–942). Wiz asserts that Veselov’s snapshot includes “this type of page file” because “[Veselov] notes that the snapshot can include machine memory (not just the virtual-disk data).” *Id.* (citing Ex. 1007, 3:32–40; Ex. 1002 ¶ 183).

In its Patent Owner Response, Orca contends that Wiz purportedly admitted in a related proceedings involving U.S. Patent No. 11,663,031 B2 owned by Orca that “Veselov does not expressly describe . . . detecting vulnerabilities while the VM is ‘inactive.’” PO Resp. 33 (quoting IPR2024-00863, Paper 2, 22). According to Orca, Wiz’s argument in this proceeding that a person of ordinary skill in the art would have expected many of Veselov’s targeted VMs to be inactive should be rejected because it contradicts “Veselov’s overarching goals of keeping target VMs active and minimizing any reductions in such devices’ computing capabilities.” *Id.* at 33–34 (citing Ex. 1007, 2:45–47; Ex. 2073 ¶¶ 155, 156; Ex. 2077, 203:21–205:7, 263:16–264:10).

In its Reply, Wiz contends that, contrary to Orca’s assertion, Veselov need not expressly describe inactive analysis to render this feature obvious. Pet. Reply 12 (citing PO Resp. 33–34). Wiz maintains that it explained in the Petition how “Veselov’s state-independent technique suggests analyzing the snapshot while the VM is inactive.” *Id.* (citing Pet. 45–46). Wiz further argues that Veselov merely discloses drawbacks of existing systems—not that all cloud assets are always active. *Id.* (citing Ex. 1007, 2:45–47). According to Wiz, the evidence of record supports that a person of ordinary skill in the art would have understood that “many target VMs would already

be inactive.” *Id.* at 12–13 (citing Ex. 1002 ¶¶ 178–180; Ex. 1400 ¶¶ 55, 56; Ex. 2414, 17; Ex. 1402, 106:18–107:17; Ex. 1401, 109:18–112:19).

In its Sur-reply, Orca contends that Wiz relies on improper gap filling to explain how Veselov teaches an inactive VM. PO Sur-reply 13. Orca argues that Wiz’s assertion that a person of ordinary skill in the art would have “‘expected many target VMs’ to be inactive” “doesn’t address why [a person of ordinary skill in the art] *would have* been motivated to modify Veselov to analyze inactive VMs.” *Id.* (quoting Pet. Reply 12) (citing Pet. 45–46).

Based on the complete record, we agree with Wiz that Veselov, together with the general background knowledge in the art, teaches or fairly suggests “wherein during the analysis of the at least one snapshot, the virtual machine is inactive,” as required by each of dependent claims 2 and 14. Veselov discloses that the scanning service performs a security assessment by “obtain[ing] the computing resources needed to implement a copy of the virtual machine instance” and implementing this duplicate of the virtual machine instance “outside of the original virtual computing environment.” Ex. 1007, 3:44–67. Later, when describing step 414 in Figure 4, Veselov discloses that “the scanning service may perform a security assessment on the assessment VM instance” independently of the original VM. *Id.* at 16:45–53, Fig. 4. Wiz’s declarant, Dr. Stavrou, testifies that “most of Veselov’s snapshot-based assessment techniques require no interaction with the original VM” and, therefore, the snapshot scanning analysis “does not depend on the state of the original VM.” Ex. 1002 ¶ 178. We credit Dr. Stavrou’s testimony on this particular issue because it is consistent with

Veselov's disclosure of performing its snapshot analysis independently of the VM. *See* Ex. 1007, 3:44–67, 16:45–53, Figs. 3A, 3B, 4, 5A, 5B.

Given that Veselov discloses some examples of performing its snapshot analysis independent of the VM, it follows that Veselov is agnostic as to whether the VM is active or inactive. Moreover, Dr. Stavrou testifies that “a [person of ordinary skill in the art] would have expected that many target VMs to already be inactive at the time of the security assessment because a ‘significant portion of VM images are mostly offline and infrequently booted’ due to increased cost.” Ex. 1002 ¶ 78 (quoting Ex. 1066, 2). We credit Dr. Stavrou's testimony on this particular issue because it is consistent with the general background knowledge in the art. *See* Ex. 1066, 2; *see also* Ex. 1067, 392 (stating that “[v]irtualized data centers have a large number of dormant VMs”).

We do not agree with Orca's argument that one of Veselov's stated objectives is to keep VMs active. *See* PO Resp. 33–34. Although Veselov discloses that it “overcome[s] drawbacks of existing security systems, such as . . . unavailability of resource services that are part of the assessment,” we do not view this cited disclosure as requiring the VM to be active when performing snapshot analysis. Ex. 1007, 2:42–47. Instead, as we explain above, because Veselov discloses performing its snapshot analysis independent of the VM, it is agnostic as to whether the VM is active or inactive.

Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the

evidence that dependent claims 2 and 14 would have been obvious over the combined teachings of Veselov and Hufsmith.

7. Claims 7 and 19

Claim 7 depends from independent claim 1, and further recites “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, 10:5–7. Claim 19 recites the same limitation, but it depends from independent claim 13. *Id.* at 10:65–67.

In its Petition, Wiz contends that Veselov teaches these limitations because it discloses that the “scanning service receives an identification of the virtual disks’ location in order to access those disks.” Pet. 53 (citing Ex. 1007, 8:16–45, 9:17–25). Wiz further argues that Veselov teaches that the identification of the location of virtual disks 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 communication 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 53–54 (citing Ex. 1007, 4:19–5:5, 9:17–25, 10:48–11:4, 15:41–59, 16:3–14; Ex. 1002 ¶¶ 28–30, 201–204).

In its Patent Owner Response, Orca contends Veselov’s disclosure of obtaining the virtual network addresses of VMs does not teach “the identification of . . . a virtual address of at least one of the virtual disks,” as

required by each of dependent claims 7 and 19. *See* PO Resp. 34 (citing Pet. 53–54; Ex. 2073 ¶¶ 157–159). In its Reply, Wiz contends that Orca relies solely on its flawed arguments for independent claims 1, 13, and 22, thereby leaving Wiz’s obviousness analysis regarding dependent claims 7 and 19 “unrebutted.” Pet. Reply 13 (citing PO Resp. 34; Ex. 1400 ¶ 57).

Based on the complete record, we agree with Wiz that Veselov teaches or fairly suggests “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,” as required by each of dependent claims 7 and 19. *See* Pet. 53–54; Pet. Reply 13. When describing Figures 3A and 3B, Veselov discloses that computing resource service providers 300, 350 communicate with virtual machine 312 so that scanning service 310 may perform a security assessment of a target resource (i.e., one or more executing instances of VM 312) using “a virtual network address” associated with VM 310. Ex. 1007, 10:37–11:4. Based on this cited disclosure, we find that Veselov’s scanning service 310 obtains the virtual network address of VM 312 to facilitate communication.

Although Veselov does not disclose explicitly that scanning service 310 obtains a virtual address of a virtual disk associated with VM 312, it would have been obvious to a person of ordinary skill in the art to do so, especially because, in some embodiments, Veselov’s scanning service is capable of generating a tailored snapshot containing “only the subset of virtual machine instance data needed to perform the security assessment” (i.e., a virtual disk). Ex. 1007, 8:16–45; *see also id.* at 11:5–9 (“[VM] 312 may be executed on a server and use a logical volume 306, which is

composed of a fixed or variable allocation of physical data storage resources, such as data storage blocks selected from one or more hard disk drives of one or more server computers.”).

Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the evidence that dependent claims 7 and 19 would have been obvious over the combined teachings of Veselov and Hufsmith.

8. Claims 3–6, 8–12, 15–18, 20, and 21

During trial, Orca does not address separately Wiz’s arguments and supporting evidence explaining how the combined teachings of Veselov and Hufsmith account for the additional limitation of dependents claims 3–6, 8–12, 15–18, 20, and 21. *See* PO Resp. 33–34. We have reviewed Wiz’s arguments and supporting evidence explaining how the combined teachings of Veselov and Hufsmith account for the additional limitation of these dependent claims, and we agree with and adopt Wiz’s analysis. *See* Pet. 48–52, 54–59. Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the evidence that the subject matter of dependent claims 3–6, 8–12, 15–18, 20, and 21 would have been obvious over the combined teachings of Veselov and Hufsmith.

C. Obviousness over the Combined Teachings of Veselov, Hufsmith, and Chari

Wiz contends that claims 1–22 of the ’685 patent are unpatentable under 35 U.S.C. § 103 as obvious over the combined teachings of Veselov, Hufsmith, and Chari. Pet. 59–64. Wiz contends that the combined

teachings of Veselov, Hufsmith, and Chari account for the subject matter of each challenged claim, and Wiz provides reasoning as to why a person of ordinary skill in the art would have been prompted to modify the teachings of these references. *Id.* To support its positions, Wiz submits a first Declaration of Dr. Stavrou with the Petition, a second Declaration of Dr. Stavrou with the Reply, and a Declaration of Mr. Luttwak with the Reply. *See* Exs. 1002, 1400, 1414.

Orca contends that Wiz does not provide a sufficient rationale to combine the teachings of Veselov, Hufsmith, and Chari. PO Resp. 62–65; PO Sur-reply 14. To support its positions, Orca submits the Declarations of Dr. Kaeli and Mr. Shua with the Patent Owner Response. *See* Exs. 2073, 2074.

Based on the complete record, we determine that Wiz has shown by a preponderance of the evidence that claims 1–22 of the ’685 patent are unpatentable as obvious over the combined teachings of Veselov, Hufsmith, and Chari. We begin by providing an overview of Chari, and then we turn to the parties’ contentions with respect to the challenged claims.

1. Overview of Chari

Chari generally relates to “virtual machines and[,] more specifically[,] to sanitizing a virtual machine image of sensitive data contained within a plurality of different software components of a software stack installed on the virtual machine image.” Ex. 1056 ¶ 2. Chari discloses that “[v]irtual machine images may contain substantial amounts of sensitive data belonging to a cloud computing environment,” including applications and services installed in the cloud computing environment, as well as user accounts

stored in the cloud computing environment. *Id.* ¶ 61. Some examples of this sensitive data include “raw information in the virtual disk blocks; sensitive details in system configuration files including network topology information and administrator accounts and passwords; sensitive details in system logs, such as administrator passwords; application data, such as raw data in database files; and application credentials, such as default passwords for applications.” *Id.* In one embodiment, Chari discloses a virtual machine image labeling and sanitization process that includes, among other steps, “virtual machine image manager generat[ing] a snapshot of the specific instance of the virtual machine at [step] 914.” *Id.* ¶ 94, Fig. 9.

2. Claims 1, 13, and 22

Once again, our analysis below focuses on the limitations of independent claim 1. For the most part, the same arguments and evidence Wiz provides to explain how the combined teachings of Veselov, Hufsmith, and Chari account for all the limitations of independent claim 1 equally apply to all the limitations of independent claims 13 and 22. *See* Pet. 26–45, 62–65. In addition, with the exception of elements 1.6/13.6/22.6 and 1.8/13.8/22.8, Wiz’s arguments and evidence it identifies above with respect to its obviousness ground based on the combined teachings of Veselov and Hufsmith equally apply to its obviousness ground challenging these same claims based on the combined teachings of Veselov, Hufsmith, and Chari. *See id.* at 59 (arguing “[t]his combination builds upon [the obviousness ground based on the combined teachings of Veselov and Hufsmith] and further applies Chari’s express disclosure of detecting and remediating

sensitive data, including encryption keys”). We address elements 1.6 and 1.8 below.

Element 1.6 recites “analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine.” Ex. 1001, 9:46–49. Wiz contends that Chari teaches the claimed “analyz[ing] the at least one snapshot to detect . . . sensitive data” because it discloses “analyz[ing] virtual resources to detect specific instances of sensitive data.” Pet. 62 (citing Ex. 1056, code (57), ¶¶ 5, 38, 39, 64–66, 75, 76, claim 1, Figs. 1, 2, 7). Wiz argues that, similar to Veselov, Chari’s “analysis may be performed on images/snapshots [of VMs] or on instantiated VMs.” *Id.* (citing Ex. 1056 ¶¶ 66, 72, 73, 92–94; Ex. 1002 ¶ 230). Wiz asserts that “[t]his facilitates particularized remediation to prevent unwanted data exposure.” *Id.* (citing Ex. 1056 ¶¶ 40–42, 66, 84, 85; Ex. 1002 ¶ 230).

Element 1.8 recites “report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.” Ex. 1001, 9:51–54. Wiz contends that “Hufsmith teaches filtering and prioritizing alerts for identified security issues based on a determined risk level.” Pet. 62. Wiz argues that, consistent with Hufsmith’s technique for filtering or prioritizing alerts associated with the exposure of sensitive data, “Chari teaches associating each detected item with sensitivity levels comparable to the various priority levels discussed in Hufsmith.” *Id.* at 62–63 (citing Ex. 1056 ¶¶ 39–41, 77–80; Ex. 1078 ¶¶ 180–182; Ex. 1002 ¶ 231). Based on the disclosures of Hufsmith and Chari, Wiz asserts that it “would have been obvious to filter

and prioritize alerts for the detected sensitive data based on the determined risk level.” *Id.* at 62 (citing Ex. 1002 ¶¶ 232, 233).

Turning to rationale to combine, Wiz contends that a person of ordinary skill in the art would have been motivated to combine the teachings of Veselov and Hufsmith with those of Chari “to provide a more complete identification/mitigation of security risks.” Pet. 60. According to Wiz, “[t]he presence of unsecured sensitive data was a common concern in security assessments,” and “Chari mitigates this issue by scanning images/snapshots to detect and sanitize such data, which a [person of ordinary skill in the art] would have recognized was equally beneficial in the security assessments taught by Veselov and Hufsmith.” *Id.* (citing Ex. 1056 ¶¶ 63–66; Ex. 1002 ¶ 227). Wiz further argues that, “consistent with Hufsmith’s general teachings of reporting the potential exposure of sensitive data, Chari expressly discloses detecting specific instances of sensitive data (e.g., passwords, account numbers, and encryption keys) in an image/snapshot” of a VM. *Id.* (citing Ex. 1056, code (57), ¶¶ 14, 38, 76–80). Wiz asserts that “[r]eporting filtered/prioritized alerts for the detected sensitive data also would have furthered this benefit, [because] it would bring more critical sensitive data to the user’s attention and improve remediation efforts.” *Id.* at 60–61 (citing Ex. 1056 ¶¶ 39–42, 77–80; Ex. 1078 ¶¶ 116–118, 180–183; Ex. 1002 ¶ 228).

Lastly, Wiz contends that a person of ordinary skill in the art would have had a reasonable expectation of success in making the proposed combination of Veselov, Hufsmith, and Chari. Pet. 61. Wiz argues that “[d]etecting sensitive data, as taught by Chari, was routinely and predictably

performed as part of security assessments,” such as in Veselov’s and Hufsmith’s security assessments. *Id.* (citing Ex. 1002 ¶¶ 50, 54, 229). According to Wiz, “[a]pplying these teachings is consistent with and readily implemented in combination with Veselov and Hufsmith,” and “Chari’s teachings are also consistent with and readily combined with Hufsmith’s filtering/prioritizing teachings [because], like Hufsmith, Chari teaches associating detected security issues with priority levels.” *Id.* (citing Ex. 1007, 2:35–41, 14:13–22; Ex. 1056 ¶¶ 39–41, 65; Ex. 1078 ¶¶ 82, 118, 180–183; Ex. 1002 ¶ 229). Relying on the testimony of Dr. Stavrou, Wiz asserts that the proposed combination “would not have presented meaningful technical challenges or produced unexpected results.” *Id.* (citing Ex. 1002 ¶ 229).

a. Orca’s Arguments

In its Patent Owner Response, Orca relies on the same arguments it identifies above when addressing Wiz’s proposed combination of Veselov and Hufsmith to support its assertions that a person of ordinary skill in the art would not have combined the teachings of Veselov, Hufsmith, and Chari, nor was there a reasonable expectation of success in doing so. PO Resp. 62. Orca also contends that a person of ordinary skill in the art would not have been motivated to modify Wiz’s proposed combination of Veselov and Hufsmith to include the teachings of Chari because Chari’s system identifies sensitive data through interactions with the target VM, whereas the challenged claims of the ’685 patent require detecting sensitive data through analysis that “requires no interaction with the [VM].” *Id.* at 62–63 (citing Ex. 1056 ¶¶ 37, 39; Ex. 2073 ¶¶ 161–163; Ex. 2074 ¶¶ 179, 180; Ex. 1001,

elements 1.6, 13.5, 22.5). More specifically, Orca argues that Chari's snapshots are used exclusively for "rollback purposes" and they can be "label[ed] and sanitize[d]," but Chari never discloses analyzing a snapshot to detect sensitive data. *Id.* at 63 (quoting Ex. 1056 ¶ 94) (citing Ex. 1056 ¶¶ 73, 92–96, Fig. 9; Ex. 2073 ¶¶ 161–163). Orca asserts that, because Chari's solution is the opposite of what is required by the challenged claims of the '685 patent, a person of ordinary skill in the art would not have been motivated "to add such a complex system to Veselov [as] Veselov counsels *against* 'complexity of installation and monitoring' of an assessment system." *Id.* at 64 (quoting Ex. 1007, 2:42–46) (citing Ex. 2073 ¶¶ 161–163).

In addition, Orca contends that there would be no reasonable expectation of success in combining the teachings of Veselov and Chari in the manner proposed by Wiz because these references include incompatible teachings. PO Resp. 64–65 (citing Ex. 1007, 17:23–29, 18:1–3, 18:26–29, 18:38–39, Fig. 6; Ex. 2073 ¶¶ 161–163). Orca asserts that, by ignoring these incompatible teachings, Wiz engages in impermissible hindsight reconstruction. *Id.* at 65.

In its Reply, Wiz contends that Orca's argument that there is no motivation to combine the teachings of Veselov and Chari "attacks the references individually and mischaracterizes Chari as limited to running VMs." Pet. Reply 13 (citing PO Resp. 62; Ex. 1056 ¶ 94; Ex. 1400 ¶¶ 58–60). Wiz asserts that Orca's insistence that Chari's disclosure of "label[ing] and santiz[ing]" a snapshot does not involve detecting sensitive data lacks merit because Orca cannot explain how Chari's system labels and

sanitizes data in snapshot, without first detecting the data. *Id.* (quoting Ex. 1056 ¶ 94) (citing PO Resp. 63; Ex. 1400 ¶¶ 61, 62).

In its Sur-reply, Orca disagrees with Wiz’s assertion that it is attacking the references individually, instead arguing that Wiz cherry-picks helpful portions of Veselov and Chari while ignoring contrary disclosures that would lead a person of ordinary skill in the art away from the proposed combination. PO Sur-reply 14. Orca argues that Wiz’s assertion that Chari’s system could not label and sanitize sensitive data in snapshot, without first detecting the data, “misses the mark” because Chari requires an initial determination of sensitive data using VM interactions to create a labeling script, which stands in contrast to the challenged claims of the ’685 patent. *Id.* Orca also argues that Chari requires write access to target resources to run the labeling script, which is incompatible with Veselov’s read-only snapshots. *Id.* (citing PO Resp. 63–65).

Based on the complete record, Wiz provides sufficient reasons as to why a person of ordinary skill in the art would have been motivated to combine the teachings of Veselov, Hufsmith, and Chari with a reasonable expectation of success in doing so. *See* Pet. 59–61. More specifically, we agree with Wiz that, although Hufsmith teaches the potential exposure of sensitive data (Ex. 1078 ¶¶ 118, 181)), Chari more clearly teaches detecting specific instances of sensitive data (e.g., passwords, account numbers, and encryption keys) in a VM (Ex. 1056, code (57), ¶¶ 14, 38, 76–80). In our view, the added clarity provided by Chari’s explicit teaching of detecting sensitive data in a VM supports Wiz’s assertion that a person of ordinary skill in the art would have been motivated to apply this particular teaching

from Chari to its proposed combination of Veselov and Hufsmith “to provide a more complete identification/mitigation of security risks.” Pet. 60. We also agree with Wiz that there was a reasonable expectation of success in making the proposed combination of Veselov, Hufsmith, and Chari because Chari’s explicit teaching of detecting sensitive data “was routinely and predictably performed as part of security assessments,” such as in Veselov’s and Hufsmith’s security assessments. *Id.* at 61 (citing Ex. 1002 ¶¶ 50, 54, 229).

We do not agree with Orca’s arguments for two reasons. First, Orca relies, at least in part, on the same arguments it identifies above when addressing Wiz’s proposed combination of Veselov and Hufsmith to support its assertions that a person of ordinary skill in the art would not have combined the teachings of Veselov, Hufsmith, and Chari, nor was there a reasonable expectation of success in doing so. *See* PO Resp. 62. For the same reasons we identify above, we do not agree with those arguments. *See supra* Section II.B.5.f.

Second, we do not agree with Orca’s arguments because they improperly focus on disparate teachings of Veselov and Chari, and they attack the asserted references individually. *See* PO Resp. 62–65. It is well-settled that “non-obviousness [cannot be established] by attacking references individually,” when, as here, the asserted obviousness ground is based upon the combined teachings of Veselov, Hufsmith, and Chari. *In re Keller*, 642 F.2d 413, 426 (CCPA 1981). Instead, the test is what the combined teachings of these three references would have taught or suggested to a person of ordinary skill in the art. *In re Young*, 927 F.2d 588, 591 (Fed. Cir.

1991). As one example, we understand Wiz to rely on Veselov to teach the claimed “analyze at least one snapshot to detect vulnerabilities” (*see supra* Section II.B.5.d), and then Wiz turns to Chari to more clearly teach the claimed “detect[ing] . . . sensitive data” (*see* Pet. 60). As another example, we understand Wiz to rely on Veselov—not Chari—to teach or suggest the claimed “analyzing the at least one snapshot requires no interaction with the virtual machine.” *See id.* 40.

b. Objective Indicia of Non-Obviousness or Secondary Considerations

In its Patent Owner Response, Orca contends that the same objective indicia of non-obviousness that it identifies above when addressing Wiz’s proposed combination of Veselov and Hufsmith equally applies to Wiz’s proposed combination of Veselov, Hufsmith, and Chari. PO Resp. 65. For the same reasons we identify above, absent a presumption of nexus, Orca does not establish nexus between its evidence based on SideScanning technology and the challenged claims of the ’685 patent by showing that the evidence of non-obviousness is the “direct result of the unique characteristics of the claimed invention.” *Huang*, 100 F.3d at 140. Independently of establishing nexus between its evidence of non-obviousness and the challenged claims of the ’685 patent, we find that Orca’s evidence of long-felt need, skepticism, and copying is weak, and despite there being some evidence of industry praise and commercial success, Orca has not shown that the evidence of industry praise and commercial success is connected to claimed features that were unknown in the prior art. *See supra* Sections II.B.5.g.i–vi.

c. Summary

In summary, Orca's evidence of non-obviousness does not overcome Wiz's strong case of obviousness as to independent claims 1, 13, and 22. *See, e.g., Intercontinental Great Brands*, 869 F.3d at 1342–47 (Fed. Cir. 2017) (determining that the strong case of obviousness as to the independent claims at issue outweighs the objective indicia of non-obviousness). Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the evidence that independent claims 1, 13, and 22 would have been obvious over the combined teachings of Veselov, Hufsmith, and Chari.

3. Claims 2–12 and 14–21

During trial, Orca does not address separately Wiz's arguments and supporting evidence explaining how the combined teachings of Veselov, Hufsmith, and Chari account for the additional limitation of dependents claims 2–12 and 14–21. *See* PO Resp. 62–65. We have reviewed Wiz's arguments and supporting evidence explaining how the combined teachings of Veselov, Hufsmith, and Chari account for the additional limitations of these dependent claims, and we agree with and adopt Wiz's analysis. *See* Pet. 59, 63–64. Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the evidence that the subject matter of dependent claims 2–12 and 14–21 would have been obvious over the combined teachings of Veselov, Hufsmith, and Chari.

D. Obviousness over the Combined Teachings of Veselov, Hufsmith, Chari, Price, and Huseinović

Wiz contends that claims 2, 3, 14, and 15 of the '685 patent are unpatentable under 35 U.S.C. § 103 as obvious over the combined teachings of Veselov, Hufsmith, Chari, Price, and Huseinović. Pet. 64–71.

Wiz contends that the combined teachings of Veselov, Hufsmith, Chari, Price, and Huseinović account for the subject matter of each challenged claim, and Wiz provides reasoning as to why a person of ordinary skill in the art would have been prompted to modify the teachings of these references. *Id.* To support its positions, Wiz submits a first Declaration of Dr. Stavrou with the Petition, a second Declaration of Dr. Stavrou with the Reply, and a Declaration of Mr. Luttwak with the Reply. *See* Exs. 1002, 1400, 1414. *See* Exs. 1002, 1400, 1414.

Orca contends that Wiz does not provide a sufficient rationale to combine the teachings of Veselov, Hufsmith, Chari, Price, and Huseinović. PO Resp. 65–67; PO Sur-reply 15. To support its positions, Orca submits the Declarations of Dr. Kaeli and Mr. Shua with the Patent Owner Response. *See* Exs. 2073, 2074.

Based on the complete record, we determine that Wiz has shown by a preponderance of the evidence that claims 2, 3, 14, and 15 of the '685 patent are unpatentable as obvious over the combined teachings of Veselov, Hufsmith, Chari, Price, and Huseinović. We begin by providing overviews of Price and Huseinović, and then we turn to the parties' contentions with respect to the challenged claims.

1. Overview of Price

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.

2. Overview of Huseinović

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 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 940–941.

3. Claims 2, 3, 14, and 15

Claim 2 depends from independent claim 1, and further recites “wherein during the analysis of the at least one snapshot, the virtual machine is inactive wherein the snapshot includes a page file of memory associated with the virtual machine.” Ex. 1001, 9:55–58. Claim 14 recites the same limitation, but it depends from independent claim 13. *Id.* at 10:48–51.

Wiz contends that Price teaches the claimed “wherein during the analysis of the at least one snapshot, the virtual machine is inactive” because

Price discloses performing a security assessment by analyzing image data while the VM is powered off. Pet. 68 (citing Ex. 1048, code (57), ¶¶ 14, 26–29, 32, 42, 45; Ex. 1002 ¶¶ 62, 245, 246). Wiz argues that Price also discloses remediating the security issues identified before the VM resumes online operations. *Id.* (citing Ex. 1048 ¶ 14, claim 17; Ex. 1002 ¶¶ 70, 246). Wiz then contends that Huseinović teaches the claimed “snapshot includes a page file of memory associated with the virtual machine” because Huseinović discloses that, in common platforms such as VMware, taking a snapshot while a VM is suspended typically includes a page file representing the state of machine memory. *Id.* at 69 (citing Ex. 1049, 940, 941; Ex. 1002 ¶ 248). According to Wiz, Huseinović’s “page file provides useful security information, [because] it is easily interpreted to identify running processes.” *Id.* (citing Ex. 1049, 940–942; Ex. 1002 ¶ 248).

Claim 3 depends from independent claim 1, and further recites “wherein the page file is configured to allow deduction of one or more applications running on the virtual machine.” Ex. 1001, 9:59–61. Claim 15 recites the same limitation, but it depends from independent claim 13. *Id.* at 10:52–54.

Wiz contends that Huseinović teaches these limitations because, as it identifies above in its arguments and evidence for dependent claims 2 and 14, Huseinović discloses conventional generation of snapshots containing page files of memory. Pet. 70 (citing Ex. 1049, 940; Ex. 1002 ¶¶ 252, 253). Wiz argues that each of Huseinović’s page files are configured to allow deduction of the VM’s running applications because “the VM’s processes are readily determined from the page file[s] using common, well-understood

data-analysis tools.” *Id.* at 70–71 (citing Ex. 1049, 940–942; Ex. 1002 ¶¶ 252, 253).

Turning to rationale to combine, Wiz contends that a person of ordinary skill in the art would have been motivated to combine the teachings of Veselov, Hufsmith, and Chari with those of Price and Huseinović “to improve computer security in several ways.” Pet. 66. Wiz argues that “Price recognizes well-understood advantages of performing image analysis while a VM is inactive, [because] actively running a potentially compromised VM could cause further damage.” *Id.* (citing Ex. 1048, claim 17; Ex. 1002 ¶ 242). According to Wiz, Price’s offline analysis “help[s] minimize delays/costs associated with actively running VMs.” *Id.* (citing Ex. 1002 ¶ 242). Wiz also argues that a person of ordinary skill in the art would have had reasons to obtain Huseinović’s snapshot “to facilitate more accurate security-risk assessments.” *Id.* Wiz asserts that Huseinović discloses “obtaining this beneficial application-usage information by generating a snapshot while the VM is in a suspended state such that it contains a page file of the VM’s machine memory.” *Id.* at 67 (citing Ex. 1049, 940–942; Ex. 1002 ¶ 243).

Lastly, Wiz contends that a person of ordinary skill in the art would have had a reasonable expectation of success in making the proposed combination of Veselov, Hufsmith, Chari, Price, and Huseinović. Pet. 67. Wiz argues that Price’s offline analysis of VMs “was well understood and routinely practiced.” *Id.* (citing Ex. 1002 ¶ 244). According to Wiz, “[m]ost of Veselov’s snapshot-based assessment techniques require no interaction with the original VM, so the original VM’s state during the analysis step

would not affect the snapshot analysis or produce unexpected results.” *Id.* (citing Ex. 1007, 16:45–53, 18:32–53, Figs. 3A, 3B, 5A, 5B; Ex. 1048 ¶¶ 32, 42; Ex. 1002 ¶ 244). Next, Wiz argues Huseinović’s “[g]enerating and analyzing snapshots that include page files was also consistent with Veselov’s teachings.” *Id.* (citing Ex. 1007, 2:30–40; Ex. 1049, 940–942; Ex. 1002 ¶ 244). Relying on the testimony of Dr. Stavrou, Wiz asserts that interpreting Huseinović’s page files using common analysis tools would have been readily appreciated by a person of ordinary skill in the art “so applying Huseinović’s teachings would not have presented meaningful technical challenges or produced unexpected results.” *Id.* (citing Ex. 1002 ¶ 244).

a. Orca’s Arguments

In its Patent Owner Response, Orca relies on the same arguments it identifies above when addressing Wiz’s proposed combinations of Veselov and Hufsmith, with or without Chari, to support its assertions that a person of ordinary skill in the art would not have combined the teachings of Veselov, Hufsmith, Chari, Price, and Huseinović, nor was there a reasonable expectation of success in doing so. PO Resp. 65. Orca also contends that a person of ordinary skill in the art would not have been motivated to modify Wiz’s proposed combinations of Veselov and Hufsmith, with or with Chari, with the teachings of Price because “Price is directed to assessments with VM *images*, not *snapshots*.” *Id.* at 66 (citing Pet. 68–70; Ex. 1007, 2:56–67; Ex. 1048, Fig. 6; Ex. 2073 ¶¶ 73–81, 165). Indeed, Orca asserts that “Price does not even mention snapshots,” which, according to Orca, a person of

ordinary skill in the art would have understood “present a different class of security concerns from VM images.” *Id.* (citing Ex. 2073 ¶¶ 81, 166).

Moreover, Orca contends that a person of ordinary skill in the art would not have been motivated to modify Wiz’s proposed combinations of Veselov and Hufsmith, with or with Chari, with the teachings of Huseinović because “Huseinović is directed to a particular scenario where ‘VM workstation’ is used, and explains that preserving a ‘vmem file’ in a suspended state is an *alternative* to a ‘snapshot.’” PO Resp. 66 (quoting Ex. 1049, 940). Orca argues that Wiz does not explain why a person of ordinary skill in the art would have implemented any of the asserted prior art systems in “VMware workstation,” much less why such a person would have combined different alternative approaches. *Id.* at 66–67 (citing Ex. 2073 ¶ 167). In addition, Orca asserts that Huseinović “counsels *against* Wiz’s reliance on Price by discouraging powering down a VM.” *Id.* at 67 (citing Ex. 1049, 940; Ex. 2073 ¶ 165; Ex. 2074 ¶¶ 172–78).

In its Reply, Wiz disagrees with Orca’s assertion that Price’s inactive VM analysis contradicts Veselov’s purported goal of keeping VMs active because Veselov does not teach away from inactive VM analysis. Pet. Reply 13 (citing Pet. 65–67; Ex. 1400 ¶¶ 63, 64). Wiz asserts that both the Petition and the evidence of record demonstrate that Veselov’s snapshots may be used in the analysis of inactive VMs. *Id.* at 13–14 (citing Pet. 45–46, 66–67, 69; Ex. 1002 ¶¶ 33–36, 181, 240–244, 247–250; Ex. 1400 ¶ 66; Ex. 1402, 160:18–161:20). Wiz further argues that Orca’s assertion that Price analyzes VM images—not snapshots—attacks the reference individually. *Id.* at 14 (citing PO Resp. 66).

Wiz contends that Orca's arguments attacking Huseinović "fare no better" because Huseinović is evidence of the standard practice in many cloud computing platforms of capturing the same page file from the suspended machine and from suspended-state snapshotting. Pet. Reply 14 (citing Ex. 1049, 941; Ex. 1002 ¶¶ 33–36, 181–183, 240–244, 247–250; Ex. 1400 ¶ 65). Wiz disagrees with Orca's assertion discounting the use of Huseinović's VMware in Veselov because bodily incorporation is not the proper test for evaluating obviousness. *Id.* (citing PO Resp. 66–67). Wiz disagrees with Orca's assertion that Huseinović discourages powering down VMs because Orca does not address its alternative arguments that involve suspended VMs or already powered off VMs. *Id.* (citing PO Resp 67; Ex. Pet. 69–70; Ex. 1400 ¶ 64).

In its Sur-reply, Orca contends that Wiz's reply arguments do not fix the problems associated with "Price and Huseinović contradict[ing] Veselov's objectives and goals." PO Sur-reply 15 (citing PO Resp. 65–67). Orca argues that, in the Patent Owner Response, it does not rely on bodily incorporation arguments, but rather seeks to highlight how Wiz engages in impermissible hindsight reconstruction, and that Wiz ignores each asserted reference's scope and conflicting teachings that would lead a person of ordinary skill in the art away from the challenged claims of the '685 patent. *Id.*

Based on the complete record, Wiz provides sufficient reasons as to why a person of ordinary skill in the art would have been motivated to combine the teachings of Veselov, Hufsmith, Chari, Price, and Huseinović with a reasonable expectation of success in doing so. *See* Pet. 65–67. More

specifically, we agree with Wiz that a person of ordinary skill in the art would have understood that modifying Veselov to include Price's offline VM analysis improves computer security because "actively running a potentially compromised VM could cause further damage" (Pet. 66 (citing Ex. 1048 ¶ 14, claim 17)), and performing offline VM analysis would "help[] minimize delays/costs associated with actively running VMs" (Pet. 66 (citing Ex. 1002 ¶ 242)). We also agree with Wiz that that a person of ordinary skill in the art would have understood that modifying Veselov to include Huseinović's generation of a snapshot, which includes a page file configured to allow for the deduction of running applications on a VM, would result in obtaining "beneficial application-usage information." *Id.* at 67 (citing Ex. 1049, 940–942; Ex. 1002 ¶ 243). Lastly, we agree with Wiz that there was a reasonable expectation of success in making the proposed combination of Veselov, Hufsmith, Chari, Price, and Huseinović because Price's offline VM analysis "was well understood and routinely practiced," and Huseinović's generation and analysis of snapshots that include page files was "predictable and consistent with Veselov's teachings." *Id.* at 67 (citing Ex. 1002 ¶ 244; Ex. 1049, 940–942; Ex. 1007, 3:20–40).

We do not agree with Orca's arguments for two reasons. First, Orca relies, at least in part, on the same arguments it identifies above when addressing Wiz's proposed combination of Veselov and Hufsmith, with or without Chari, to support its assertions that a person of ordinary skill in the art would not have combined the teachings of Veselov, Hufsmith, Chari, Price, and Huseinović, nor was there a reasonable expectation of success in

doing so. *See* PO Resp. 65. For the same reasons we identify above, we do not agree with those arguments. *See supra* Sections II.B.5.f and II.C.2.a.

Second, we do not agree with Orca’s arguments because they improperly focus on the disparate teachings in Veselov, Price, and Huseinović, and they attack the asserted references individually. *See* PO Resp. 66–67; *In re Keller*, 642 F.2d at 426; *In re Young*, 927 F.2d at 591. As one example, we understand Wiz to rely on Veselov to teach the claimed “snapshot” (*see supra* Section II.B.5.d), and then Wiz turns to Price’s offline VM analysis to more clearly teach performing snapshot analysis when the claimed “the virtual machine is inactive” (*see* Pet. 68). As another example, we understand Wiz to rely on Veselov to teach the claimed “snapshot” (*see supra* Section II.B.5.d), and then Wiz turns to Huseinović’s snapshot that includes a page file representing the state of machine memory to more clearly teach the claimed “snapshot includes a page file of memory associated with the virtual machine” (*see* Pet. 69).

b. Objective Indicia of Non-Obviousness or Secondary Considerations

In its Patent Owner Response, we understand Orca to contend that the same objective indicia of non-obviousness that it identifies above when addressing Wiz’s proposed combination of Veselov and Hufsmith equally applies to Wiz’s proposed combination of Veselov, Hufsmith, Chari, Price, and Huseinović. *See* PO Resp. 67. For the same reasons we identify above, absent a presumption of nexus, Orca does not establish nexus between its evidence based on SideScanning technology and the challenged claims of the ’685 patent by showing that the evidence of non-obviousness is the “direct result of the unique characteristics of the claimed invention.” *Huang*,

100 F.3d at 140. Independently of establishing nexus between its evidence of non-obviousness and the challenged claims of the '685 patent, we find that Orca's evidence of long-felt need, skepticism, and copying is weak, and despite there being some evidence of industry praise and commercial success, Orca has not shown that the evidence of industry praise and commercial success is connected to claimed features that were unknown in the prior art. *See supra* Sections II.B.5.g.i–vi.

c. Summary

In summary, Orca's objective evidence of non-obviousness does not overcome Wiz's strong case of obviousness as to dependent claims 2, 3, 14, and 15. *See, e.g., Intercontinental Great Brands*, 869 F.3d at 1342–47 (Fed. Cir. 2017) (determining that the strong case of obviousness as to the independent claims at issue outweighs the objective indicia of non-obviousness). Accordingly, after weighing all the evidence bearing on obviousness and non-obviousness, Wiz has demonstrated by a preponderance of the evidence that dependent claims 2, 3, 14, and 15 would have been obvious over the combined teachings of Veselov, Hufsmith, Chari, Price, and Huseinović.

E. Wiz's Motion to Exclude

Wiz filed a Motion to Exclude that seeks to exclude Exhibits 2134–2137, 2148, 2152, and 2400–2428 as being inadmissible under the Federal Rules of Evidence (“FRE”) for the following reasons: (1) Exhibits 2134–2137, 2148, 2152, 2406, 2412, 2414, and 2416 should be excluded on FRE 801–805 because certain statements in these exhibits relied on by Orca to demonstrate objective indicia of non-obviousness constitute inadmissible

hearsay; (2) these same exhibits remain inadmissible hearsay under FRE 601 and 701–703; and (3) Exhibits 2400–2428 should be excluded under FRE 403 because they unfairly prejudice Wiz, confuse the issues, and waste time. Pet. Mot. to Exclude 1–15.

Of the exhibits that Wiz seeks to exclude, we rely on some, but not all, of Exhibits 2134–2137, 2148, 2152, and 2400–2428 in the context of considering Orca’s arguments and evidence regarding objective indicia of non-obviousness. *See supra* Sections II.B.5.g.i–vi. In any event, because we ultimately determine that Wiz demonstrates by a preponderance of the evidence that all challenged claims of the ’685 patent are unpatentable, the grant or denial of Wiz’s Motion to Exclude would have no impact on the outcome of this proceeding. Accordingly, we *dismiss* Wiz’s Motion to Exclude as moot.

F. Motions to Seal

In the Motion to Seal accompanying its Reply, Wiz requests to seal the non-public, unredacted version of the Reply (Paper 42), together with Exhibits 1400–1414, because they contain information that Orca previously designated as business confidential, or they contain business confidential information that would significantly harm Wiz’s competitive position, if made public. Paper 43, 1. In the Motion to Seal accompanying its Sur-reply, Orca requests to seal the non-public, unredacted version of the Sur-reply (Paper 60), together with Exhibits 2172 and 2173, because they contain the business confidential information of both parties. Paper 59, 1. The remaining Motions to Seal all request to seal the same business confidential information the parties previously designated in the Patent

Owner Response, Reply, and Sur-reply that also was included in the non-public, unredacted version of the Motion to Exclude (Paper 52), the non-public, unredacted version of the Opposition to the Motion to Exclude (Paper 56), the non-public, unredacted version of the Reply to the Opposition to the Motion to Exclude (Paper 57), and the non-public, unredacted versions of the parties' demonstratives (Papers 65, 67). Papers 51, 55, 58, 63, 66.

After reviewing Exhibits 1400–1414, 2172, 2173, together with the relevant quotes, discussions, and citations in the non-public, unredacted versions of the Reply, Sur-reply, Motion to Exclude, Opposition to the Motion to Exclude, Reply to the Opposition to the Motion to Exclude, and the parties' demonstratives, we agree that these documents and exhibits contain business confidential information. We also are mindful of Orca's representation that there is a genuine need to rely on this information to demonstrate objective indicia of non-obviousness, as well as for Wiz to provide arguments and evidence in rebuttal. *See* PO Resp. 35–62; Pet. Reply 14–29; PO Sur-reply 15–35. Accordingly, Exhibits 1400–1414, 2172, and 2173, and the non-public, unredacted versions of the Reply (Paper 42), Sur-reply (Paper 60), Motion to Exclude (Paper 52), Opposition to the Motion to Exclude (Paper 56), Reply to the Opposition to the Motion to Exclude (Paper 57), and the parties' demonstratives (Papers 65, 67), 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.

III. CONCLUSIONS

Based on the fully developed trial record, Wiz demonstrates by a preponderance of the evidence that claims 1–22 of the '685 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
1–22	103	Veselov, Hufsmith	1–22	
1–22	103	Veselov, Hufsmith, Chari	1–22	
2, 3, 14, 15	103	Veselov, Hufsmith, Chari, Price, Huseinović	2, 3, 14, 15	
Overall Outcome			1–22	

IV. ORDER

Accordingly, it is

ORDERED that claims 1–22 of the '685 patent have been shown to be unpatentable;

FURTHER ORDERED that we *dismiss* Wiz'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.

IPR2024-00865
Patent 11,693,685 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
jbailargeon@wsgr.com
tthomas@wsgr.com

For PATENT OWNER

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

Douglas E. Lumish (admitted *pro hac vice*)
WEIL, GOTSHAL & MANGES
doug.lumish@weil.com