

Filed on behalf of: Orca Security Ltd.

Entered: April 7, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-00863
U.S. Patent 11,663,031 B2

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The '031 Patent Improved Cloud Security Systems	4
A.	Problems with the Prior Art	4
B.	The '031 Patent's Innovative Cloud Security Systems.....	4
III.	Claim Construction.....	6
A.	“(i) Taking at Least One Snapshot, and (ii) Requesting Taking at Least One Snapshot of the Virtual Machine at Rest”	6
B.	“Analyzing the At Least One Snapshot”	10
IV.	Challenged Claims 1, 3-9, and 11-16 Are Nonobvious Over Veselov and Price (Ground 1)	12
A.	POSAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov and Price	13
1.	Overview of Veselov	13
2.	Overview of Price	14
3.	Wiz Does Not Establish a Motivation for Combining Veselov's Multiple Distinct Embodiments.....	14
4.	Wiz's Motivations To Combine Veselov And Price Should Be Rejected.....	20
B.	Veselov and Price Fail to Disclose or Suggest Multiple Limitations.....	23
1.	The Veselov/Price Combination Does Not Render Obvious Using Cloud Computing Platform APIs to Identify and Locate Virtual Disks.....	24
2.	The Veselov/Price Combination Does Not Render Obvious Taking or Requesting the Taking of Snapshots of VMs At Rest, or Snapshot Analyses When VMs Are Inactive	31

3.	The Veselov/Price Combination Does Not Render Obvious Reporting Detected Vulnerabilities as Alerts.....	33
4.	The Veselov/Price Combination Does Not Render Obvious Dependent Claims 4 and 12	35
C.	Objective Evidence Demonstrates and Confirms the Non-obviousness of the Challenged Claims	35
1.	The Claimed Inventions Solved a Long-felt, Unmet Need With A “Genuinely Genius Innovation”	36
2.	Orca’s SideScanning™ Practices the ’031 Patent	40
3.	The Claimed Inventions Defied the Skeptics, and Became Widely Accepted in the Industry	42
4.	The Industry Praised Orca’s Revolutionary Inventions.....	45
5.	Wiz Copied Orca’s Inventions.....	49
6.	Orca’s And Wiz’s Commercial Success Demonstrates Non-obviousness.....	59
V.	Claims 2 and 10 Are Nonobvious Over Veselov, Price, and Hufsmith (Ground 2)	62
A.	POSAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov, Price, and Hufsmith	62
B.	Veselov, Price, and Hufsmith Fail to Render Obvious Claims 2 and 10	63
VI.	Claims 6 and 14 Are Nonobvious Over Veselov, Price, Hufsmith, and Huseinović (Ground 3)	65
VII.	Conclusion	65

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>Abiomed, Inc. v. Maquet Cardiovascular, LLC</i> , IPR2017-01204, Paper 9 (PTAB Oct. 23, 2017).....	26
<i>ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	29
<i>Allen Archery, Inc. v. Browning Mfg. Co.</i> , 819 F.2d 1087 (Fed. Cir. 1987)	42
<i>Apple Inc. v. Samsung Elecs. Co.</i> , 839 F.3d 1034 (Fed. Cir. 2016) (en banc)	36, 45, 46
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	28, 29
<i>BlephEx, LLC v. Myco Indus., Inc.</i> , 24 F.4th 1391 (Fed. Cir. 2022)	18, 20, 27
<i>Brown & Williamson Tobacco Corp. v. Philip Morris Inc.</i> , 229 F.3d 1120 (Fed. Cir. 2000)	61
<i>Chemours Co. FC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	61
<i>Fanduel, Inc. v. Interactive Games LLC</i> , 966 F.3d 1334 (Fed. Cir. 2020)	23
<i>Fromson v. Advance Offset Plate, Inc.</i> , 755 F.2d 1549 (Fed. Cir. 1985)	4
<i>In re Stepan Co.</i> , 868 F.3d 1342 (Fed. Cir. 2017)	15, 18, 20, 27
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	21, 23

<i>Iron Grip Barbell Co. v. USA Sports, Inc.</i> , 392 F.3d 1317 (Fed. Cir. 2004)	50
<i>K/S HIMPP v. Hear-Wear Techs., LLC</i> , 751 F.3d 1362 (Fed. Cir. 2014)	26
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	4
<i>Liqwd, Inc. v. L'Oreal USA, Inc.</i> , 941 F.3d 1133 (Fed. Cir. 2019)	49, 50
<i>MarkForged Inc. v. Continuous Composites, Inc.</i> , IPR2022-00679, Paper 24 (PTAB Sept. 26, 2023).....	20
<i>Medtronic, Inc. v. Teleflex Innovations S.a.r.l.</i> , 69 F.4th 1341 (Fed. Cir. 2023)	21
<i>Medtronic, Inc. v. Teleflex Innovations S.a.r.l.</i> , 70 F.4th 1331 (Fed. Cir. 2023)	36, 49, 50, 56
<i>Metalcraft of Mayville, Inc. v. The Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	3, 15
<i>Pentec, Inc. v. Graphic Controls Corp.</i> , 776 F.2d 309 (Fed. Cir. 1985)	60
<i>Personalized Media Commc'ns, LLC v. Apple Inc.</i> , 952 F.3d 1336 (Fed. Cir. 2020)	10
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	59
<i>Power-One, Inc. v. Artesyn Techs., Inc.</i> , 599 F.3d 1343 (Fed. Cir. 2010)	62
<i>Salazar v. AT&T Mobility LLC</i> , 64 F.4th 1311 (Fed. Cir. 2023)	8
<i>SkinMedica, Inc. v. Histogen Inc.</i> , 727 F.3d 1187 (Fed. Cir. 2013)	8

<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	4, 49, 59
<i>TQ Delta LLC v. CISCO Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	22
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	21
<i>Univ. of Strathclyde v. Clear-Vu Lighting LLC</i> , 17 F.4th 155 (Fed. Cir. 2021)	22
<i>Wastow Enters., LLC v. Truckmovers.com, Inc.</i> , 855 F. App'x 748 (Fed. Cir. 2021)	8
<i>WBIP, LLC v. Kohler Co.</i> , 829 F.3d 1317 (Fed. Cir. 2016)	<i>passim</i>

Exhibit List

Exhibit	Description
2001	Declaration of David R. Kaeli, Ph.D. (“Kaeli Decl.”)
2002	<i>Curriculum Vitae</i> of David R. Kaeli, Ph.D.
2003	Trend Micro™ vmware®, <i>Trend Micro Enterprise Security: Changing the Game for Anti-Virus in the Virtual Datacenter</i> (White Paper) (Sept. 2010), https://www.kennisportal.com/wp-content/uploads/2022/06/ChangingtheGameintheVirtualDatacenter.pdf (last visited Sept. 7, 2024) (“vmware, <i>Trend Micro Enterprise Security</i> ”)
2004	Red Hat, <i>Red Hat Virtualization 4.0: Technical Reference: The Technical Architecture of Red Hat Virtualization Environments</i> (updated Mar. 29, 2018), https://docs.redhat.com/en-us/documentation/red_hat_virtualization/4.0/pdf/technical_reference/Red_Hat_Virtualization-4.0-Technical_Reference-en-US.pdf (“Red Hat Virtualization 4.0”)
2005	U.S. Pat. App. Pub. No. 2008/0320583 A1 (“Sharma”)
2006	<i>Virtual Machine Snapshots, Red Hat Virtualization 4.3: Technical Reference: The Technical Architecture of Red Hat Virtualization Environments</i> (updated Apr. 20, 2020), https://docs.redhat.com/en-us/documentation/red_hat_virtualization/4.3/pdf/technical_reference/Red_Hat_Virtualization-4.3-Technical_Reference-en-US.pdf (excerpt) (“Red Hat Virtualization 4.3 – <i>Virtual Machine Snapshots</i> ”)
2007	Dominik Birk, <i>Technical Challenges of Forensic Investigations in Cloud Computing Environments</i> (Jan. 12, 2011), https://cachin.com/cc/csc2011/submissions/birk.pdf (last visited Sept. 7, 2024) (“Birk, <i>Technical Challenges</i> ”)

Exhibit	Description
2008	Sasa Mrdovic et al., <i>Combining Static and Live Digital Forensic Analysis in Virtual Environment</i> , 2009 XXII Int'l Symp. on Info., Commc'n & Automation Techs., Sarajevo, Bosnia & Herzegovina (Oct. 29–31, 2009) (“Mrdovic, <i>Combining Static and Live Digital Forensic Analysis</i> ”)
2009	RESERVED
2010	U.S. Pat. No. 9,467,465 B2 (“Hibbert”)
2011	U.S. Pat. No. 10,298,599 B1 (“Zhang”)
2012	U.S. Pat. No. 9,594,912 B1 (“Thioux”)
2013	RESERVED
2014	Complaint for Patent Infringement, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. July 12, 2023), ECF No. 1 (“Orca Compl.”)
2015	Oral Order (Joint Motion for Discovery Dispute Teleconference), <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. May 17, 2024), ECF No. 62 (“Oral Order”)
2016	Defendant Wiz, Inc.’s Initial Invalidity Contentions, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. June 7, 2024) (excerpt) (“Pet’r’s Invalidity Contentions”)
2017	RESERVED
2018	Abraham Silberschatz et al., <i>Operating System Concepts</i> (9th ed. 2013) (excerpt)
2019	Derek Uluski, Real Time Anti-Virus for a Virtualized Environment (2008) (M.S.E.E., Thesis, Northeastern University) (excerpt) (“Uluski Thesis”)

Exhibit	Description
2020	MahMush, <i>Snapshots vs. Images – Which One to Choose?</i> , Huawei (Sept. 15, 2021, 17:55:10), https://forum.huawei.com/enterprise/en/snapshots-vs-images-which-one-to-choose/thread/773699-893 (“Huawei - <i>Snapshots vs. Images</i> ”)
2021	Amazon Web Service (AWS), <i>What Is a Hypervisor?</i> (2024), https://aws.amazon.com/what-is/hypervisor/ (last visited Sept. 11, 2024)
2022	Diego Perez-Botero et al., <i>Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers</i> , Conference: Proceedings of the Workshop on Security in Cloud Computing (SCC), Hangzhou, China 1–8 (May 8, 2013) (“Perez-Botero, <i>Characterizing Hypervisor Vulnerabilities</i> ”)
2023	U.S. Pat. No. 8,220,053 B1 (“Sun”)
2024	Jinpeng Wei et al., <i>Managing Security of Virtual Machine Images in a Cold Environment</i> , Conference: Proceedings of the First ACM Cloud Computing Security Workshop (CCSW), Chicago, Illinois 1–6 (Nov. 13, 2009) (“Wei, <i>Managing Security of Virtual Machine Images</i> ”)
2025	Red Hat, <i>Red Hat OpenStack Platform 11: Instances and Images Guide – Managing Instances and Images</i> (updated Feb. 19, 2018), https://docs.redhat.com/en-us/documentation/red_hat_openstack_platform/11/pdf/instances_and_images_guide/Red_Hat_OpenStack_Platform-11-Instances_and_Images_Guide-en-US.pdf (“Red Hat Open Stack”)
2026	Greg Zemlin, <i>Agentless vs. Agent-Based Security: Which is Better for the Cloud?</i> , Wiz (Nov. 26, 2023), https://www.wiz.io/academy/agentless-vs-agent-based-security (“Wiz Marketing”)
2027	Steve Lasker, <i>Key Differences Between VM and Container Vulnerability Scanning</i> , stivelaskerblog.com (June 27, 2018), https://stivelasker.blog/2018/06/27/key-differences-between-vm-and-container-vulnerability-scanning/

Exhibit	Description
2028	Exhibit A-1, Invalidity of United States Patent 11,663,031 (the “’031 Patent”) by Veselov, attached to Defendant Wiz, Inc.’s Initial Invalidity Contentions, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. June 7, 2024) (excerpt) (Ex. 2016)
2029	Exhibit A-4, Invalidity of United States Patent 11,663,031 (the “’031 Patent”) by Price, attached to Defendant Wiz, Inc.’s Initial Invalidity Contentions, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. June 7, 2024) (excerpt) (Ex. 2016)
2030	Exhibit A-2, Invalidity of United States Patent 11,663,031 (the “’031 Patent”) by Hufsmith, attached to Defendant Wiz, Inc.’s Initial Invalidity Contentions, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. June 7, 2024) (excerpt) (Ex. 2016)
2031	RESERVED
2032	RESERVED
2033	RESERVED
2034	RESERVED
2035	RESERVED
2036	RESERVED
2037	Appendix A, Invalidity of United States Patent 11,663,031 (the “’031 Patent”), attached to Defendant Wiz, Inc.’s Initial Invalidity Contentions, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. June 7, 2024) (excerpt) (Ex. 2016)
2038	RESERVED
2039	RESERVED
2040	Stipulation and Order, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. June 25, 2024) (“Amended Scheduling Order”)

Exhibit	Description
2041	Declaration of Christopher Henry In Response to Petitioner's First Objections to Evidence [<i>served, not filed</i>]
2042	Declaration of Douglas E. Lumish Pursuant to 37 C.F.R. § 42.10(c)
2043-2047	RESERVED
2048	Wiz, Inc.'s Answering Claim Construction Brief, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Oct. 22, 2024) (excerpt) ("Answering Claim Constr. Chart")
2049-2052	RESERVED
2053	Listing of Requested Documents
2054	RESERVED
2055	RESERVED
2056	Orca Security Ltd.'s Eleventh Supplemental Responses and Objections to Defendant Wiz's First Set of Interrogatories, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Dec. 13, 2024) (excerpts)
2057	Stipulated Protective Order, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Mar. 15, 2024), ECF No. 38
2058	Email exchange between counsel for Wiz, Inc. and counsel for Orca Security Ltd. (Dec. 17-26, 2024)
2059	Email exchange between counsel for Wiz, Inc. and counsel for Orca Security Ltd. (Dec. 23, 2024 – Feb. 25, 2025)
2060-2064	RESERVED

Exhibit	Description
2065	<i>Orca Security Lands \$6.5M Seed Round to Deliver IT Security Teams Unprecedented Full Stack Cloud Visibility, Securing High-Velocity Cloud Growth</i> , Orca Security Blog (June 12, 2019), https://orca.security/resources/blog/orca-security-lands-6-5m-seed-round-to-deliver-it-security-teams-unprecedented-full-stack-cloud-visibility-securing-high-velocity-cloud-growth/
2066	Orca Security, <i>The Ultimate Guide to: Gaining Full Stack Visibility Into Your Cloud Assets</i> (Nov. 2019)
2067	Orca Security Technical Brief, <i>SideScanning™ – Inside the Engine that Powers Orca Security</i> (2020)
2068	Letter from counsel for Orca Security Ltd. to counsel for Wiz, Inc. (May 20, 2024), filed in <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Sept. 10, 2024), ECF No. 140-2
2069	Letter to the Honorable Sherry R. Fallon from Rodger D. Smith Regarding Discovery Disputes, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Oct. 9, 2024), ECF No. 165
2070	Francis & James Berthoty, <i>Redefining CNAPP: A Complete Guide to the Future of Cloud Security</i> , Software Analyst Cyber Research, (Sept. 12, 2024), https://softwareanalyst.substack.com/p/redefining-cnapp-a-complete-guide
2071	Memorandum Order, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Oct. 22, 2024), ECF No. 182
2072	Declaration of Blake R. Davis Pursuant to 37 C.F.R. § 42.10(c)
2073	Declaration of Dr. David Kaeli in Support of Patent Owner's Response (“Kaeli”) [PROTECTIVE ORDER MATERIAL]
2074	Declaration of Avi Shua (“Shua”) [PROTECTIVE ORDER MATERIAL]
2075	Wiz Experts Team, <i>Containers vs. VMs: What’s the difference?</i> (Apr. 8, 2024) [Stavrou Dep. Ex. 2075]

Exhibit	Description
2076	Francis & James Berthoty, <i>Redefining CNAPP: A Complete Guide To the Future of Cloud Security</i> (Sept. 12, 2024) [Stavrou Dep. Ex. 2076]
2077	Transcript of Deposition of Angelos Stavrou, Ph.D., taken March 5, 2025
2078	Video of <i>The CISO – Startup Connection Powered by YL Ventures – Orca Security</i> , https://www.youtube.com/watch?v=h4x4zh1D-tw (excerpt)
2079	Transcript of <i>The CISO – Startup Connection Powered by YL Ventures - Orca Security</i> , https://www.youtube.com/watch?v=h4x4zh1D-tw
2080	Video of <i>Full Stack Visibility In Minutes</i> , https://www.youtube.com/watch?v=sxD14bRT_28
2081	Transcript of <i>Full Stack Visibility In Minutes</i> , https://www.youtube.com/watch?v=sxD14bRT_28
2082	Video of <i>Orca Security – SideScanning vs Traditional Security Assessment Methods</i> , https://www.youtube.com/watch?v=0SDwFzINzGM
2083	Transcript of <i>Orca Security – SideScanning vs Traditional Security Assessment Methods</i> , https://www.youtube.com/watch?v=0SDwFzINzGM
2084	<i>Australian Business Interview with Avi Shua Orca Security Through the Years</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=ne6biY89RyY
2085	Orca Security, <i>CNBC Interview with Avi Shua Orca Security Through the Years</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=r9aBmLHpSnY

Exhibit	Description
2086	Orca Security, <i>The CUBE Interview: Avi Shua Explains Orca Security and Its Value Proposition</i> (last visited Mar. 19, 2025) https://www.youtube.com/watch?v=tlS0A92IYm8
2087	The Matias Experiment, <i>Ep398: Avi Shua CEO & Co-Founder, Orca Security</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=M58n3oE6E1Y
2088	Orca Security, <i>CNBC Prime Time Interview on Orca Security's \$550 Series C Extension Led by Temask</i> (last visited Mar. 19, 2025) https://orca.security/resources/video/cnbc-squawk-box-asia-avi-shua-interview-550m-series-c-extension/
2089	RESERVED
2090	Orca Security, <i>The Ultimate Guide to: Gaining Full Stack Visibility Into Your Cloud Assets</i> (June 2019)
2091	RESERVED
2092	Orca Security SideScanning Technical Brief, ORCA_0049504 (2021)
2093	Orca Security SideScanning Technical Brief (2022), ORCAW_CP010_000581130
2094	Video of <i>Orca Pod (In-Account) Onboarding</i> , https://www.youtube.com/watch?v=FEvqhAktFS0 (first made available May 1, 2020)
2095	Video of <i>AWS Onboarding with Orca Security Orca Security and Its Partners</i> , https://www.youtube.com/watch?v=QdBsE2VqjpU (first made available Apr. 21, 2020)
2096	<i>Create AWS Policy</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=OdtXqrvbEdU (first made available June 11, 2019)

Exhibit	Description
2097	<i>Define AWS Role</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=SOw046Fnafo (first made available June 11, 2019)
2098	<i>GCP Onboarding, Walkthrough of How to Onboard a GCP Account for Orca to SideScan</i> (last visited Mar. 19, 2025), https://orca.security/resources/video/gcp-onboarding/ (first made available Apr. 21, 2020)
2099	<i>Orca Security-Deep Cloud Inspection</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=VwZ-7guGHw0
2100	<i>An MRI for Your Cloud Environment</i> (last visited Mar. 19, 2025), https://orca.security/resources/video/sidescanning-a-cloud-environment-mri/
2101	RESERVED
2102	Qualys, Inc., <i>Qualys Unveils Cloud Agent Platform for Continuous Asset Inventory, Security and Compliance</i> (Apr. 22, 2015), https://www.bankinfosecurity.com/press-releases/qualys-unveils-cloud-agent-platform-for-continuous-asset-p-223
2103	Saumitra Das, <i>Security Agents Don't Belong in Your Cloud!</i> (Aug. 18, 2021), https://cloudsecurityalliance.org/blog/2021/08/18/security-agents-don-t-belong-in-your-cloud
2104	Fortra, <i>Agent-Based vs. Agentless Scanning, Choosing the Right Vulnerability Scanning Method</i> (Aug. 27, 2021), https://www.fortra.com/blog/agent-based-vs-agent-less-scanning
2105	RESERVED
2106	Keith Mokris, <i>How Agentless Approaches Sideline Cloud Workload Protection Strategies</i> (Feb. 23, 2021), https://web.archive.org/web/20210727053930/https://www.paloaltonetworks.com/blog/prisma-cloud/agentless-approaches-sideline-cloud-workload-protection/

Exhibit	Description
2107	Orca Security, <i>Orca Security Lands \$6.5M Seed Round to Deliver IT Security Teams Unprecedented Full Stack Cloud Visibility, Securing High-Velocity Cloud Growth</i> (June 12, 219), https://orca.security/resources/blog/orca-security-lands-6-5m-seed-round-to-deliver-it-security-teams-unprecedented-full-stack-cloud-visibility-securing-high-velocity-cloud-growth/
2108	Orca Security, <i>Orca Security Lands \$20 Million Series A to Help More Global Enterprises Gain Deeper Multi-Cloud Visibility in Minutes, Not Months</i> (May 5, 2020), https://orca.security/resources/press-releases/orca-security-funding-20m-multi-cloud-visibility/
2109	TechCrunch, <i>Orca Security Raises \$20M Series A for Its Multi-Cloud Security Platform</i> (May 5, 2020), https://techcrunch.com/2020/05/05/orca-security-raises-20m-series-a-for-its-multi-cloud-security-platform/
2110	Orca Security, <i>Orca Security Lands \$55 Million Series B to Further Disrupt the Cloud Security Industry with Touchless, Deep, Context-Aware Security and Compliance</i> (Dec. 8, 2020), https://orca.security/resources/press-releases/iconiq-growth-orca-funding/
2111	Frederic Lardinois, <i>Orca Security Raises \$55M For Its Cloud-Native Security Platform</i> (Dec. 8, 2020), https://techcrunch.com/2020/12/08/orca-security-raises-55m-for-its-cloud-native-security-platform/
2112	Michael Novinson, <i>Upstart Orca Security Raises \$210M in Google-Backed Funding</i> (Mar. 23, 2021), https://www.crn.com/news/security/upstart-orca-security-raises-210m-in-google-backed-funding
2113	Orca Security, <i>Orca Security Extends Series C Round to \$550M, Boosting Valuation to \$1.8 Billion, to Further Accelerate Transformation of Cloud Security Industry</i> (Oct. 5, 2021), https://orca.security/resources/press-releases/orca-security-series-c-550-million-announcement/

Exhibit	Description
2114	RESERVED
2115	Ami Luttwak & Ryan Kazanciyan, <i>Securing Clouds, Securely</i> (Oct. 31, 2023), https://www.wiz.io/blog/the-wiz-approach-to-agentless-scanning
2116	Assaf Rappaport, <i>\$100M ARR in 18 Months: Wiz Becomes the Fastest-Growing Software Company Ever</i> (Aug. 10, 2022), https://www.wiz.io/blog/100m-arr-in-18-months-wiz-becomes-the-fastest-growing-software-company-ever
2117	Orca Security, <i>Unprecedented Holistic View of Cloud Security</i> (last visited Mar. 19, 2025), https://panoramait.com/en/solution-orca-security/
2118	Katie Teitler & Edward Amoroso, Tag Cyber, <i>Vendor Landscape and TCO Analysis for Achieving Cloud-Wide, Workload-Deep Security and Compliance for Public Cloud Environments</i> , ORCA_0261399-415
2119	Mark Haranas, <i>The 20 Coolest Tech Startups of 2020</i> (Nov. 19, 2020), https://www.crn.com/slide-shows/cloud/the-20-coolest-tech-startups-of-2020
2120	Louis Columbus, <i>The Top 20 Cybersecurity Startups to Watch in 2021</i> (Nov. 29, 2020), https://www.forbes.com/sites/louiscolumbus/2020/11/29/the-top-20-cybersecurity-startups-to-watch-in-2021-based-on-crunchbase/
2121	Orca Security, <i>Orca Security Named a 2021 Gartner Cool Vendor in Cloud Security Posture Management (CSPM)</i> (June 21, 2021), https://orca.security/resources/press-releases/press-release-cnapp-gartner-cool-vendor/
2122	Orca Security, <i>Orca Security Awarded 2022 Regional and Global AWS Partner Award</i> (Nov. 28, 2022), https://orca.security/resources/press-releases/orca-security-2022-regional-and-global-aws-partner-award/

Exhibit	Description
2123	SC Media, <i>SC Award Winners 2023 Orca Security – Best Cloud Security Workload Protection Solution</i> (Aug. 21, 2023), https://www.scworld.com/news/sc-award-winners-2023-orca-security-best-cloud-workload-protection-solution
2124	Avi Shua, <i>Orca Security Wins SC Award for Best Cloud Security Posture Management (CSPM) Solution</i> (Aug. 31, 2022), https://orca.security/resources/blog/orca-security-winner-sc-award-cspm-solution/
2125	Gil Geron, <i>Orca Security Wins 2023 SC Award for Best Cloud Workload Protection Platform (CWPP)</i> (Aug. 21, 2023), https://orca.security/resources/blog/orca-security-wins-sc-media-award-best-cwpp-2023/
2126	RESERVED
2127	Forbes, <i>Orca Security</i> (last visited Mar. 19, 2025), https://www.forbes.com/companies/orca-security/?list=cloud100&sh=482e6ca468be
2128	Orca Security, <i>Orca Security Named 2023 Forbes Cloud 100</i> (Aug. 8, 2023), https://orca.security/resources/press-releases/orca-security-2023-forbes-cloud-100/
2129	Orca Security, <i>Orca Security Named to Inaugural Redpoint InfraRed 100 List</i> (July 17, 2023), https://orca.security/resources/press-releases/orca-security-named-to-inaugural-redpoint-infrared-100-list/
2130	Orca Security, <i>Orca Security Named to Redpoint 2024 InfraRed 100 for Second Consecutive Year</i> (June 18, 2024), https://orca.security/resources/press-releases/orca-security-named-to-redpoint-2024-infrared-100-for-second-consecutive-year/
2131	<i>Rising in Cyber, 2024</i> (last visited Mar. 19, 2025), https://risingincyber.com/

Exhibit	Description
2132	Orca Security, <i>Orca Security Named to Notable Capital's Rising in Cyber 2024</i> (June 4, 2024), https://orca.security/resources/press-releases/orca-security-named-to-notable-capitals-rising-in-cyber-2024/
2133	Orca Security, <i>Orca Security: Deep Cloud Inspection</i> (last visited Mar. 19, 2025), https://orca.security/resources/product-info/sidescanning-deep-cloud-security-inspection-across-aws-azure-gcp/
2134	Vikki Davies, <i>The History of Cloud Computing</i> (Nov. 28, 2021), https://cybermagazine.com/cloud-security/history-cloud-computing
2135	Ankur Shah, <i>Palo Alto Networks Shifts Left with Prisma Cloud 3.0</i> (Nov. 16, 2021), https://www.paloaltonetworks.com/blog/2021/11/shift-left-with-prisma-cloud-3-0/
2136	Cybersecurity Insiders, <i>Cloud Security Report</i> (2018) https://static.carahsoft.com/concrete/files/5015/4532/6484/2018-cloud-security-report-palo-alto-networks.pdf
2137	Yuri Diogenes, <i>The Quest for Visibility and Control in the Cloud</i> , ISSA Journal (Mar. 20, 2019), https://issa.mydigitalpublication.com/articles/the-quest-for-visibility-and-control-in-the-cloud
2138	Josh Dreyfuss, <i>Agents Are Not Enough: Why Cloud Security Needs Agentless Deep Scanning</i> (Sept. 28, 2021), https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning
2139	Michael Novinson, <i>Orca Security Raises \$340M To Scale Platform R&D, Channel</i> (Oct. 5, 2021), https://www.crn.com/news/security/orca-security-raises-340m-to-scale-platform-r-d-channel

Exhibit	Description
2140	Elias Terman, <i>From Stealthy Startup to Cloud Security Innovation Leader</i> (Feb. 4, 2021), https://orca.security/resources/blog/2020-recap/
2141	Kyle Wiggers, <i>Cloud Security Startup Wiz, Now Valued at \$10B, Raises \$300M</i> (Feb. 27, 2023), https://techcrunch.com/2023/02/27/cloud-security-startup-wiz-now-valued-at-10b-raises-300m/
2142	Rohan Goswami et al., <i>Wiz Walks Away from \$23 Billion Deal with Google, Will Pursue IPO</i> (July 22, 2024), https://www.cnbc.com/2024/07/23/google-wiz-deal-dead.html
2143	<i>SINET16 Previous Winners</i> (last visited Mar. 20, 2025), https://www.security-innovation.org/sinet16-award/past-award-winners/
2144	<i>SINET16 Innovator Award</i> (last visited Mar. 20, 2025), https://www.security-innovation.org/sinet16-award/
2145	<i>CISO Choice Award Winners 2020</i> (Nov. 19, 2020), https://securitycurrent.com/ciso-choice-awards-winners-2020/
2146	<i>Connect Wiz with Google Cloud (GCP)</i> (last visited Mar. 20 2025), https://web.archive.org/web/20221003171234/ https://www.wiz.io/partners/gcp
2147	Alan Schindel, <i>Detect and Prioritize CISA Known Exploited Vulnerabilities in the Cloud with Wiz</i> (Feb. 10, 2022), https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz
2148	Chris Ray, <i>GigaOm Radar for Cloud Workload Security</i> (Jan. 15, 2025), https://gigaom.com/reprint/gigaom-radar-for-cloud-workload-security-241089-check-point/
2149	Provisional Patent Application No. 62/797,718

Exhibit	Description
2150	<i>Azure Onboarding with Orca Security Orca Security and Its Partners</i> (last visited Mar. 23, 2025), https://www.youtube.com/watch?v=zw091YvbjsI
2151	U.S. Pat. App. Pub. No. 2020/0244692A1 A1
2152-2157	RESERVED
2158	Amazon Web Services, <i>Viewing Recent Management Events with the Console</i> (last visited Apr. 3, 2025), https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events-console.html
2159	Amazon Web Services, <i>Policies and Permissions in AWS Identity and Access Management</i> (last visited Apr. 3, 2025), https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
2160	RESERVED
2161	Joint Proposed Protective Order
2162	Redline Comparison between Joint Proposed Protective Order and Default Protective Order
2163	RESERVED
2164	RESERVED
2165	Wiz Experts Team, <i>Vulnerability Scanning: How It Works, Why It Matters, and What You'll Find</i> (Sept. 30, 2024), https://www.wiz.io/academy/vulnerability-scanning
2166	Nicolas Ehrman, <i>Containerization 101: Transforming Application and Deployment</i> (Feb. 6, 2025), https://www.wiz.io/academy/containerization
2167	Wiz, Inc., <i>CSPM Buyers Guide</i> (2023)
2168	Supplement to Declaration of Avi Shua

Exhibit	Description
2169-2299	RESERVED
2300	Excerpt from Orca Product Documentation (2024) [PROTECTIVE ORDER MATERIAL]
2301	<i>API Onboarding with GCP Multi Scanner for In-Account</i> [PROTECTIVE ORDER MATERIAL]
2302	REDACTED [PROTECTIVE ORDER MATERIAL]
2303	REDACTED PROTECTIVE ORDER MATERIAL]
2304	<i>AWS Permissions</i> [PROTECTIVE ORDER MATERIAL]
2305	RESERVED
2306	REDACTED [PROTECTIVE ORDER MATERIAL]
2307	REDACTED [PROTECTIVE ORDER MATERIAL]
2308	REDACTED [PROTECTIVE ORDER MATERIAL]
2309	REDACTED [PROTECTIVE ORDER MATERIAL]
2310	RESERVED
2311	RESERVED
2312	REDACTED [PROTECTIVE ORDER MATERIAL]

Exhibit	Description
2313-2399	RESERVED
2400	REDACTED [PROTECTIVE ORDER MATERIAL]
2401	REDACTED [PROTECTIVE ORDER MATERIAL]
2402	REDACTED [PROTECTIVE ORDER MATERIAL]
2403	REDACTED [PROTECTIVE ORDER MATERIAL]
2404	REDACTED [PROTECTIVE ORDER MATERIAL]
2405	REDACTED [PROTECTIVE ORDER MATERIAL]
2406	REDACTED [PROTECTIVE ORDER MATERIAL]
2407	REDACTED [PROTECTIVE ORDER MATERIAL]
2408	REDACTED [PROTECTIVE ORDER MATERIAL]
2409	REDACTED [PROTECTIVE ORDER MATERIAL]
2410	REDACTED [PROTECTIVE ORDER MATERIAL]
2411	REDACTED [PROTECTIVE ORDER MATERIAL]
2412	REDACTED [PROTECTIVE ORDER MATERIAL]

Exhibit	Description
2413	REDACTED [PROTECTIVE ORDER MATERIAL]
2414	REDACTED [PROTECTIVE ORDER MATERIAL]
2415	REDACTED [PROTECTIVE ORDER MATERIAL]
2416	REDACTED [PROTECTIVE ORDER MATERIAL]
2417	REDACTED [PROTECTIVE ORDER MATERIAL]
2418	REDACTED [PROTECTIVE ORDER MATERIAL]
2419	REDACTED [PROTECTIVE ORDER MATERIAL]
2420	REDACTED [PROTECTIVE ORDER MATERIAL]
2421	REDACTED [PROTECTIVE ORDER MATERIAL]
2422	REDACTED [PROTECTIVE ORDER MATERIAL]
2423	RESERVED
2424	RESERVED
2425	REDACTED [PROTECTIVE ORDER MATERIAL]
2426	REDACTED [PROTECTIVE ORDER MATERIAL]

Exhibit	Description
2427	REDACTED MATERIAL] [PROTECTIVE ORDER
2428	REDACTED [PROTECTIVE ORDER MATERIAL]

I. Introduction

The '031 Patent is a pioneering cybersecurity patent covering innovations that have been adopted by leading companies, recognized as a major milestone that redefined the industry, and widely praised and copied, including by Petitioner Wiz.

Drawing on decades of experience in the Israeli Intelligence Corps and the computer security industry, the inventor, Avi Shua, recognized significant shortcomings in preexisting cloud security solutions, including a failure to offer unobtrusive, comprehensive security solutions for dynamic cloud environments. Ex.2074 (Declaration of Avi Shua, "Shua")) ¶¶8-13. This motivated him to establish Orca (*id.*) and "[i]ntroduce[] the concept of agentless side scanning," which has been lauded in the industry as a "***genuinely genius innovation.***" Ex.2076, 7.¹ Mr. Shua secured his "genius innovation" in the claims of the '031 Patent and unveiled them commercially in Orca's agentless SideScanning™ technology. This technology defied skeptics, amassed extensive praise from the industry, and resulted in immense commercial success, including over \$600M in investments and REDACTED for Orca and far more for Wiz's copycat technology. *See* Section IV.C.6. Those in the industry praised Orca for having made a "big leap in cloud security with the

¹ Unless otherwise noted, emphasis is added and internal citations and quotations are omitted.

introduction of its patented agentless SideScanning technique,” calling it a “unique method” that “gather[s] crucial data through the cloud provider’s APIs, while scanning disk snapshots.” Ex.2076, 31. And still others explained Orca’s technology claimed in the ’031 Patent “transcends traditional solutions by inspecting data at rest.” Ex.2117, 1. Orca’s SideScanning™ redefined the cloud security industry to such an extent that the cloud security posture management (“CSPM”) market “can be defined by pre and post-Orca.” Ex.2076, 7.

Wiz’s petition looks to re-write this remarkable history and reduce Orca’s industry-changing inventions to nothing more than obvious combinations of known techniques. To this end, Wiz contends every challenged claim is obvious because it recites “well-known techniques for protecting virtual cloud assets.” Pet.1. But those arguments are driven by improper hindsight highlighted by the overwhelming objective indicia of non-obviousness Wiz failed to address or even mention in its Petition. *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1328 (Fed. Cir. 2016) (“[O]bjective indicia of non-obviousness play an important role as a guard against ... hindsight” and “must be considered in *every* case.”) (emphasis in original).

REDACTED

REDACTED

As detailed below, Wiz's hindsight-driven obviousness combinations do not show that any challenged claim is unpatentable. Wiz fails to show that POSAs would have made its combinations. Wiz's combinations fail to teach or suggest multiple claim limitations. And the objective evidence refutes Wiz's attempts to "stitch[] together prior art patches into something" like the claimed inventions. *Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017). In the end, Wiz does nothing more than attempt, albeit unsuccessfully, to show each individual element of Orca's claims can be found in the prior art. This is not enough. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007) ("A patent composed of several elements is not proved obvious merely by demonstrating that each element

² Exhibits 2400-2422 and 2425-2428 are Wiz's confidential documents produced pursuant to Paper 29.

was, independently, known in the prior art.”); *see also id.* at 418 (“claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.”); *see also Fromson v. Advance Offset Plate, Inc.*, 755 F.2d 1549, 1556 n.3 (Fed. Cir. 1985) (“Only God works from nothing. Men must work with old elements.”). Indeed, Wiz’s “lauding of all the available prior art” has “a hollow ring when played against its disregard of that art and its copying of” Orca’s patent-practicing SideScanning discussed below. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1541 (Fed. Cir. 1983); *see* Section IV.C.2, IV.C.5 below.

II. The ’031 Patent Improved Cloud Security Systems

A. Problems with the Prior Art

The ’031 Patent explains that as organizations “increasingly adapted their applications to be run from multiple cloud computing platforms,” security solutions struggled to adapt. ’031 Patent (Ex.1001), 1:20-27. Preexisting cloud security systems used, for example, “traffic inspection,” “traffic monitor[ing],” and “agents installed in each server in a cloud computing platform.” *Id.* 1:44-2:14. But those systems suffered from numerous problems discussed in greater detail in Section IV.C.1 (The Claimed Inventions Solved a Long-felt, Unmet Need). *Id.* 1:49-2:36, 3:53-55; Kaeli (Ex.2073) ¶¶35-38, 183-192.

B. The ’031 Patent’s Innovative Cloud Security Systems

The problems with prior art approaches motivated Mr. Shua to found Orca and develop agentless side scanning technology (SideScanning™) using the

inventions disclosed and claimed in the '031 Patent—cloud security systems and methods that, among other things, “utilize cloud computing platform APIs to identify virtual disks of a virtual machine,” use those APIs to “query a location of at least one of the identified virtual disks,” take or request the taking of “at least one snapshot of [a] virtual machine at rest,” “analyze the at least one snapshot to detect vulnerabilities [while] the virtual machine is inactive,” and “report the detected vulnerabilities as alerts.” *Id.* cls. 1, 9, 16; Shua¶¶13-14; Kaeli¶¶39-43.

These inventions neither use nor suffer from the problems that plagued traffic inspection, traffic monitoring, and intrusive agent-based solutions ('031 Patent, 2:37-38; Shua¶¶78-83), and the industry considered them “genuinely genius.” Ex.2076, 7. In fact, Orca's inventions were also recognized as “unique,” “like magic,” and “a big leap in cloud security” (*id.*, 11-12, 31) including, as explained more in Section IV.C.4 below, with respect to the novel combination of claimed features of the '031 Patent. As another example, Orca partners and customers recognized that Orca's technology “transcends traditional solutions by inspecting data at rest.” Ex.2117, 1;

REDACTED

REDACTED

; Kaeli ¶¶193-

197.

III. Claim Construction

Wiz's prior art fails to render obvious the subject matter of the challenged claims under any reasonable construction of their terms, including their plain meanings, as well as the constructions Wiz proposes (Pet.9-11). Kaeli ¶¶44-56. Nevertheless, two of Wiz's claim constructions should be rejected.

A. **“(i) Taking at Least One Snapshot, and (ii) Requesting Taking at Least One Snapshot of the Virtual Machine at Rest”**

Independent claims 1, 9, and 16 recite “[perform/performing] at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest.” The parties dispute whether the phrase “of the virtual machine at rest” modifies both listed clauses—“(i) taking at least one snapshot” and “(ii) requesting taking at least one snapshot”—as Orca contends, or only the second “requesting taking” clause, as Wiz contends. Wiz's attempt to broaden the claims so they do not require that claimed snapshots be taken of VMs “at rest” should be rejected. Kaeli ¶¶45-51.

First, the claim language establishes that “of the virtual machine at rest” applies to both “(i) taking at least one snapshot” and “(ii) requesting taking at least one snapshot.” For one, both clauses are in the same limitation which ends by

requiring “the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point of time.” This last clause referring to “the” snapshot tells POSAs there is only one snapshot, not two different snapshots of two different datasets. Subsequent limitations then refer back to the singular “at least one snapshot” without differentiating between the “taking” and “requesting taking” clauses. ’031 Patent, cl. 1 (“analyze *the at least one snapshot* to detect vulnerabilities, wherein ... the virtual machine is inactive”), cl. 5 (“The system of claim 1, wherein *the at least one snapshot* includes ...”), cls. 6-7 (same). Given that there is only “the” snapshot, the requirement that it be of “the virtual machine at rest” must apply to the snapshot regardless of whether it is taken or requested. Read as Wiz does, the claims would incoherently permit one snapshot to be taken of something other than the virtual machine at rest (which Wiz never identifies), while the requested snapshot must only be of the virtual machine at rest. This cannot be squared with the clear claim language. The snapshot of the claims must be of something, and the only something set forth in the claims is “the virtual machine at rest.” Kaeli¶48; cf. *Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1317 (Fed. Cir. 2023) (“For a dog owner to have ‘a dog that rolls over and fetches sticks,’ it does not suffice that he have two dogs, each able to perform just one of the tasks.”).

Second, the specification repeatedly emphasizes that the claimed invention is applied to virtual machines “at rest.” The title of the ’031 Patent is “Techniques for

Securing Virtual Cloud Assets *at Rest* Against Cyber Threats.” *See Wastow Enters., LLC v. Truckmovers.com, Inc.*, 855 F. App’x 748, 750-51 (Fed. Cir. 2021) (construing “device” to mean “universal folding boom trailer” because, in part, the “patent’s title—‘Universal Folding Boom Trailer’—also indicates that a relevant artisan would understand that the claims require a universal folding boom trailer”). The written description consistently emphasizes VMs and other virtual cloud assets “at rest,” including in the Abstract, figures, problem to be solved, and disclosed embodiments. *See* ’031 Patent, Abstract (“securing virtual cloud assets *at rest*”), Fig. 2 (“scan a VM *at rest*”), 2:15-36 (identifying deficiencies in prior art approaches that they do not allow “detection of vulnerabilities in data *at rest*”), 2:56-67, 3:1-14, 3:45-59, 6:26-27, 8:42; Kaeli ¶49. These “clear, repeated, and consistent statements” support construing the claims to require snapshots of VMs “at rest” whether taken or requested. *SkinMedica, Inc. v. Histogen Inc.*, 727 F.3d 1187, 1203 (Fed. Cir. 2013).

Third, the prosecution history eliminates any doubt that “taking” the snapshot is also done on “the virtual machine at rest,” not just “requesting taking” that snapshot. Following a prior art rejection, Orca amended the originally-filed claims to recite “perform at least one of taking a snapshot of the virtual machine at rest, or requesting the snapshot of the virtual machine at rest.” As amended, the “virtual

machine at rest” was initially repeated twice to explicitly modify both the “taking” and “requesting” clauses:

~~generate~~perform at least one of taking a snapshot of the virtual machine at rest, or requesting the snapshot of the virtual disks of the virtual machine at rest, wherein the snapshot represents a copy of the virtual disks of the virtual machine at a point in time.

Ex.1004, 123 (underlining and strikethrough in original), 125, 127. In the arguments accompanying these amendments, Orca used the language now in the claims, referring three times to these claim amendments as:

perform[ing] at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time.

Id., 130-131. Orca then made clear this phraseology did not change the meaning of the amended limitation despite not repeating “virtual machine at rest” in the “taking” clause; rather, this phraseology still meant that the “taking” clause was also of the “virtual machine at rest.” In particular, Orca explained that Derbeko does not “describe *taking* and analyzing a snapshot *while the VM is at rest*,” because, in Derbeko, “*the VM is not at rest*, ... but is running (e.g., active),” and Bansal just “uses snapshots to backup a virtual machine” and thus does not “solve or attempt to

solve the problem addressed by the pending claims”—“analyz[ing] a snapshot taken *while the VM is at rest* to detect vulnerabilities.” *Id.*, 131. Following an Examiner interview, Orca amended the limitations to have the form repeatedly presented in its earlier arguments, which made clear that both the taking and requesting clauses were “of the virtual machine at rest.” *Id.*, 2, 20-21. The claims’ scope should be read consistently with prosecution: both “taking” and “requesting taking” of the snapshot must be of a VM at rest. *See Personalized Media Commc’ns, LLC v. Apple Inc.*, 952 F.3d 1336, 1345 (Fed. Cir. 2020) (recognizing the importance of “[a]n applicant’s repeated and consistent remarks during prosecution”); Kaeli¶50.

B. “Analyzing the At Least One Snapshot”

Wiz argues that limitations in independent claims 1, 9 and 16 reciting ““analyzing the snapshot’ encompass[] both [1] direct analysis of the snapshot data and [2] analysis of a VM instantiated from the snapshot.” Pet.10-11. Wiz is wrong as to [2]. The only support Wiz cites for its incorrect contention that “analyzing [a] snapshot” encompasses “analysis of a VM instantiated from a snapshot” are allegations in the Orca’s amended complaint from district court. Pet.11 (citing Ex.1006, 23, 57-58). Nothing in Orca’s allegations, however, states or otherwise indicates that analyzing a VM instantiated from a snapshot is “analyzing [a] snapshot” as claimed. Ex.1006, 23, 57-58. And POSAs would understand that limitations reciting “analyzing the at least one snapshot” mean what they say and

require analyzing snapshots (and snapshot data), not duplicate VMs instantiated from snapshots. Kaeli ¶¶52-56.

Once a VM is instantiated from a snapshot, e.g., for subsequent monitoring, the VM is not a “snapshot,” and monitoring or assessing it is not “analyzing” a “snapshot.” This would have been readily apparent to POSAs based on the claims, which recite that the “snapshot” that is analyzed “represents a copy of the virtual disks of the virtual machine at a point in time.” ’031 Patent, cls. 1, 9, 16; *id.* 5:35-36 (“A VM’s snapshot is a copy of the machine’s virtual disk (or disk file) at a given point in time.”); Kaeli ¶55 (“[A]n instantiated VM is not a snapshot.”). The specification also distinguishes analyzing a snapshot by a “security system 140 to detect vulnerabilities” (’031 Patent, 6:17-18), 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.* 6:62-7:11, 8:49-59).

Tellingly, Wiz’s expert, Dr. Stavrou, never supported and has now directly contradicted Wiz’s interpretation. Dr. Stavrou just “***assume[d]*** that ‘[analyze/analyzing] the at least one snapshot’ also encompasses analysis of a VM instantiated from the snapshot”—blindly and without any supporting evidence or analysis, because he was “instructed by [Wiz’s] counsel to assume this.” Ex.1002 ¶83; Ex.2077 (“Stavrou Tr.”), 265:17-266:4, 266:13-267:15 (Dr. Stavrou: “I didn’t ask why. I was asked to assume.”), 267:16-268:3 (“I didn’t ask why.

I don't have an opinion why that was included or not."), 268:4-269:20. And, Dr. Stavrou admitted that "[n]othing" in Veselov's description of "assessing or analyzing an actual running instantiated virtual machine" "refers to analyzing a snapshot." *Id.* 280:8-281:1.³ Wiz's errant interpretation—which, as discussed more below, is directed to improperly mixing and matching embodiments in Veselov—should be rejected. Kaeli¶¶52-56.

IV. Challenged Claims 1, 3-9, and 11-16 Are Nonobvious Over Veselov and Price (Ground 1)

Wiz fails to show that claims 1, 3-9, and 11-16 would have been obvious over Veselov and Price because (1) Wiz fails to demonstrate that POSAs would have been motivated to combine Veselov's embodiments or combine them with Price (Section IV.A), (2) the combination fails to teach or suggest multiple limitations in the challenged claims (Section IV.B), and (3) objective indicia of non-obviousness refute Wiz's hindsight-driven combination (Section IV.C). Kaeli¶¶92-94.

³ Notably, Dr. Stavrou resisted giving direct answers to questions throughout his deposition, frequently filibustering or providing nonresponsive answers in an effort to avoid addressing the shortcomings in the prior art. *See, e.g.*, Stavrou Tr.124:6-126:7; 131:12-132:14.

A. POSAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov and Price

Wiz's combination of different embodiments, systems and methods from Veselov and Price, with unrelated goals and contradictory teachings, should be rejected.

1. Overview of Veselov

Veselov's overarching goal is to perform security assessments of deployed and executing target VMs while avoiding downtime of those machines and reducing assessment complexity. Kaeli ¶¶57-67; *see, e.g.*, Veselov (Ex. 1007), 2:42-67. The crux of Veselov's disclosures are systems that "include a scanning service that facilitates duplication of all or a portion of the target computing resource," and "then performs the security assessment on the duplicate computing resource"—"to avoid consuming processing time, processing power, and storage space of the target computing resource." *Id.* Abstract, 12:21-43; *see also id.* 2:54-63, 17:9-12.

To facilitate its security assessment, Veselov's scanning system "obtains, or obtains access to a state of the resource at a point in time (e.g., a 'snapshot')," which is then "prepared so that the security assessment produces the result that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance." Veselov, 3:20-27, 4:1-4. Veselov illustrates five high level embodiments of its system in Figures 1, 3A, 3B, 5A and 5B, each with distinctly different features and/or techniques, none of which are arranged as

claimed in the '031 Patent. Kaeli¶¶57-67 (Veslov Overview), 95-103; Shua¶¶143-150 (explaining Veslov differs from the claimed inventions). The Petition disregards all such distinctions, improperly lumping all of Veslov's disclosures together and using the '031 Patent as a roadmap to select from among Veslov's myriad and disparate techniques. Yet none of Veslov's embodiments teach cloud computing APIs to identify and locate virtual disks or capturing and analyzing snapshots of offline VMs. Kaeli¶¶124-152; Shua¶¶144, 148; Stavrou Tr.97:13-98:10.

2. Overview of Price

Price discloses two different approaches to assess VMs. Price teaches that to assess security of "virtual machines identified as online," like every VM in Veslov, "an agent is loaded on each online virtual machine." Price (Ex.1048), Abstract, ¶12, Fig. 3B. For VMs "determined to be offline," unlike any VM in Veslov, Price discloses that "a machine image [i.e., VM image] is collected," and security is assessed from the VM image. *Id.* Abstract, ¶11, Fig. 4, Fig. 6 (depicting these two options), ¶9, ¶¶44-45; Kaeli¶¶68-77; Shua¶¶151-154; *see also* Stavrou Tr.244:10-246:2 (Dr. Stavrou agreeing Price discloses these two, distinct options).

3. Wiz Does Not Establish a Motivation for Combining Veslov's Multiple Distinct Embodiments

As discussed more below, including in Section IV.B.1, Wiz's analysis of the claims cites, interchangeably and without explanation, to discussions of Veslov's

embodiments corresponding to Figures 1, Figures 3A-3B, and Figure 5A-5B. *See, e.g.,* Pet.17-19, 28-30, 36, 38, 40-42; Kaeli ¶¶95-103. Wiz fails, however, to provide any motivation to combine these embodiments as required. *In re Stepan Co.*, 868 F.3d 1342, 1346 n.1 (Fed. Cir. 2017) (“combining multiple embodiments from a single reference” requires “a motivation to make the combination.”); *see also* Stavrou Tr.140:19-141:7 (“I don’t talk anywhere in my declaration about modifying Veselov.”). And the fact that Wiz is only able to map Veselov to the claims using selectively culled pieces from different embodiments is a hallmark of hindsight bias. *See Metalcraft*, 848 F.3d at 1367.

Initially, Veselov discusses “APIs” only in its Figure 1 and Figures 3A/3B embodiments, where computing environments are implemented by a “computing resource service provider.” Veselov, Figs. 1, 3A-3B, 4:59-5:8, 10:37-16:14; Kaeli ¶¶96-98. Those embodiments do not identify the APIs as “cloud computing platform APIs,” or suggest such APIs could be used to identify or query locations of virtual disks as claimed. Kaeli ¶¶96-98. And while Figure 1 and Figures 3A/3B include APIs, they differ in material ways with respect to the challenged claims.

Veselov’s Figure 1 embodiment involves a “snapshot storage service 108” used to store and “obtain the snapshot data,” where the snapshot storage is located separately from the virtual machines being assessed. Veselov, Fig. 1, 7:34-8:15; Kaeli ¶¶96-97. In these snapshot storage embodiments, the only “API calls” Veselov

discusses are ones that specify the “requestor, the user associated with the virtual machine 112, the on-demand storage service 108, and/or the particular virtual machine 112.” Veselov, 6:34-38; Kaeli¶¶96-97. And the only information that is received in response to those API calls is “snapshot data” or “access to snapshot data 146” that is “corresponding to the virtual machine 112.” Veselov, 6:38-49. There is no disclosure of identifying, querying, or returning the location of any virtual disk. Kaeli¶¶96-97. To the contrary, Veselov expressly states that when a snapshot is stored, it is only “queryable” by a “virtual machine identifier” or “snapshot identifier,” and specifically “non-queryable” when it is stored as “volume images.” Veselov, 7:50-61; *see also* 6:34-38 (discussing “API calls”). The Figure 1 embodiment thus cannot satisfy limitations [1.2]-[1.4], and corresponding limitations of claims 9 and 16, because there is no identification of, query for, or received location of, a virtual disk, let alone by utilizing “cloud computing platform APIs.” Kaeli¶¶96-97.

The Figures 3A/3B embodiments, on the other hand, do *not* include a “snapshot storage service” and include discussions regarding a “logical volume” of a virtual machine. *See, e.g.*, Veselov, 11:5-9, Figs. 3A-3B. But the Figures 3A/3B embodiments do not describe analyzing the “snapshot,” instead being limited to analyzing “duplicate” VMs, i.e., “assessment virtual machine[s].” Veselov, 12:1-5. Kaeli¶98. And while Figures 3A/3B refer to an “API 338,” that API is not used to

locate or query virtual disks. *See* Veselov, 14:3-65. The Figures 3A/3B embodiments thus cannot satisfy limitations [1.2]-[1.4], [1.6], and the corresponding limitations of claims 9 and 16.

The Figures 5A/5B embodiments have yet other problems for Wiz's theories. In these embodiments, Veselov discusses analyzing snapshots as "data files." However, the Figures 5A/5B embodiments are directed to systems that (i) are not implemented with a "Computing Resource Service Provider," which is what Wiz (incorrectly) maps to the claimed "cloud computing platform" (Pet.30), and (ii) do not use APIs, let alone cloud computing platform APIs operating as claimed. Veselov, Figs. 5A-5B, 16:56-18:15; Kaeli ¶¶95, 99-101.

The Board's ID found that Wiz was purportedly relying on "common features" across Veselov's different embodiments. ID 19. But Wiz is *not* relying on common features. Rather, Wiz picks out certain features that appear in some embodiments (e.g., a "computing resource service provider" and APIs from Figures 1 and 3A/3B), and other, distinct features from different embodiments (e.g., "logical volume 306/506" from Figs. 3A/3B and 5A/5B and assessing snapshots from the Figures 5A/5B embodiments), and uses those disparate features to try to manufacture what is claimed. Pet.27-34, 40-44 (relying on "computing resource provider [104/300/350]" and "API [120/338]" for elements 1.1-1.4, and Figs. 5A/5B to disclose analyzing snapshots for element 1.6). Wiz does not explain why POSAs

would have been motivated to modify or combine disparate embodiments of Veselov—switching midstream within the challenged claims—to make a combination that Veselov does not disclose. Kaeli¶¶95-103. That is fatal to Wiz's obviousness case. *In re Stepan Co.*, 868 F.3d 1342, 1346 n.1 (Fed. Cir. 2017); *BlephEx, LLC v. Myco Indus., Inc.*, 24 F.4th 1391, 1401 (Fed. Cir. 2022).

Wiz leaves unaddressed the fact that Veselov teaches that APIs are used in only “some embodiments,” and does not disclose API use in embodiments implemented without “computing resource service provider[s]” like typical on-premises computing environments. Veselov, 4:29-35, 5:5-8, 5:13-15; *compare id.* Figs. 1, 3A-3B (“API 120” and “API 338”), *with id.* Figs. 5A-5B (no API); *compare id.* 3:11-16 (explaining certain security assessments can only be performed in “a virtual network effectuated by the service provider”), *with id.* 16:56-67 (listing components common to Figures 3A/3B, on one hand, and Figures 5A/5B, on the other, but not listing API 338 or computing resource provider 300/350 of Figures 3A/3B in Figures 5A/5B); Kaeli¶¶99-101. Further, even if Veselov's distinct embodiments could have been combined, Wiz has not shown (and cannot show) that POSAs applying the teachings of the Figures 3A/3B embodiments would have incorporated into the Figures 5A/5B embodiments computing resource service providers and APIs, but not the duplicate-VM assessments Veselov teaches for such systems, which are not the claimed snapshot-based analyses. Kaeli¶¶99-101.

Wiz argues all of Veselov's teachings "broadly apply to other embodiments," relying on Dr. Stavrou. Pet.17 (citing Ex.1002 ¶91), 28 (same). But Dr. Stavrou is wrong. For example, Dr. Stavrou asserts that Veselov teaches that "techniques discussed in the context of Fig. 2 can be performed by" any of Veselov's embodiments (Ex.1002 ¶91). But what Veselov says is "process 200 may be performed by any suitable system," with the Figure 1 system listed as an example. Veselov, 8:52-62. Neither Dr. Stavrou nor the Petition show that systems like those depicted and described in connection with Figures 5A/5B would be such "suitable system[s]." Kaeli¶102. Nor could they; the Figures 5A/5B embodiments are not implemented using a computing resource service provider or APIs. *Id.*¶102; *compare* Veselov, 4:19-48 ("Referring to FIG. 1" with "a virtual computing environment implemented by [a] computing resource service provider" that "may provide" an "API"), 10:37-39 (Figs. 3A-3B use "computing environments implemented by a computing resource service provider"), *with* 16:56-57 (Figs. 5A-B illustrate "additional embodiments" without computing resource service providers or APIs). Further, Dr. Stavrou's retreat to boilerplate that certain operations could apply to "various embodiments" and that embodiments are not "necessarily" limited do not establish a motivation to modify and combine disparate embodiments. *Stepan*, 868 F.3d at 1346 n.1; *BlephEx*, 24 F.4th at 1401; *MarkForged Inc. v. Continuous Composites, Inc.*, IPR2022-00679, Paper 24 at 15-16 (PTAB Sept. 26,

2023) (finding no motivation to combine based on reference's "generic passage regarding 'various features' that 'may' be provided in a single embodiment").

4. Wiz's Motivations To Combine Veselov And Price Should Be Rejected

In addition to mixing embodiments in Veselov, Wiz's arguments for combining Veselov and Price should be rejected for the following five reasons.

First, Wiz has not shown—and cannot show—that POSAs would have combined Veselov and Price to “prevent[] further damage that might otherwise be caused if a potentially compromised VM actively runs.” Pet.24. To make Wiz's combination, POSAs would have to take Veselov's active VMs offline for Price's assessment, ignoring Veselov's contrary purpose of keeping VMs active and running during security assessments. Kaeli¶¶104-106. Because Veselov's system is designed to keep VM's active, Veselov never mentions offline VMs or analyzing offline VMs, as Wiz's expert concedes. Stavrou Tr.203:21-205:7 (admitting there is “no reference in Veselov Exhibit 1007 to a virtual machine being offline when the snapshot is taken”), 242:8-12, 243:11-16; Kaeli¶¶106. Moreover, Veselov disparages the use of “existing security assessment systems” that would add “complexity of installation and monitoring of the assessment system,” Veselov, 2:42-46, which is what Wiz's combination that takes Veselov's machine's offline in view of Price would require. Kaeli¶¶107-108; *Medtronic, Inc. v. Teleflex Innovations S.a.r.l.*, 69 F.4th 1341, 1349 (Fed. Cir. 2023) (“[I]gnor[ing] evidence that a proposed

modification would interfere with a reference's stated purpose ... gives in to the very hindsight bias the obviousness inquiry is designed to avoid.").

Second, a POSA wouldn't have combined Price when implementing Veselov's system because of incompatibilities with how the two references assess security of active VMs. Price discloses using agents for active VMs (again, the only VMs Veselov discusses), (Price ¶45), which require installation on, and interfere with, target VMs. Kaeli ¶¶107-113; Stavrou Tr.245:3-11 (admitting Price uses agents for active VMs). That contradicts Veselov, which cautions against a "security assessment executed using the computing resources" of a target computing device. Veselov, 3:8-11. These differences would have steered a POSA away from combining Veselov and Price "in the normal course of research and development." *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360, 1363 (Fed. Cir. 2011); Kaeli ¶¶107-113.

Third, it is Wiz's burden to show that POSAs would have been motivated to combine Veselov and Price to achieve the claimed inventions. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1362, 1367-68 (Fed. Cir. 2016). But Wiz fails to explain why POSAs would have reasonably expected to achieve what is claimed by adding Price's techniques for assessments conducted with *VM images* to the alleged *VM snapshot*-based system it manufactures from Veselov. Price, Abstract ("For at least the virtual machines determined to be offline, a machine

image is collected.”), ¶14 (“[a]ssessing security of the offline virtual machines from the collected *images*”); Kaeli ¶¶111-113; Stavrou Tr.272:7-13 (agreeing “snapshots and images are different”). Wiz tries to skirt these differences by arguing “[o]ffline snapshotting and offline analysis were routine and predictable.” Pet.25. But these type of boilerplate statements—like Wiz’s assertion that its combination would have been “straightforward” and “routine” (*id.*)—are “the impermissible *ex post* reasoning and hindsight bias that *KSR* warned against.” *TQ Delta LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1361 (Fed. Cir. 2019); *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 165 (Fed. Cir. 2021); Kaeli ¶¶121.

Fourth, Wiz has not demonstrated that offline snapshotting and offline analyses were routine in the relevant context of cloud security analyses of the asserted claims. The tertiary references Wiz tries to use to show as much (*see* Pet.23) merely discuss applying software patches for active and offline VMs (Zhou, Ex.1066, 1-2; Jeswani, Ex.1067, 390-92) and note that VMs recently exposed to vulnerabilities could require offline scanning and quarantining (Budko, Ex.1081 ¶¶29-31, 37, 69). None of those references, including Ex.1015 (cited in Ex.1002 ¶33), which is the only record reference mentioning offline snapshotting, demonstrate that POSAs would have modified Veselov to contravene its purpose and shutdown target VMs to take snapshots. Kaeli ¶¶114-120. Moreover, even if Wiz *had* shown offline snapshotting and analyses were routine, Wiz leaves a fatal

gap between being well known and the “beneficial application” to Veselov, which, teaches that assessed VMs should remain online. *Fanduel, Inc. v. Interactive Games LLC*, 966 F.3d 1334, 1344 (Fed. Cir. 2020) (affirming nonobviousness because “[t]he Board reasonably identified a gap between the concept of a look-up table being well-known and the beneficial application of that concept to” a primary reference).

Fifth, Wiz has not sufficiently shown that a POSA would have “a reasonable expectation of achieving *what is claimed in the patent-at-issue*.” *Intelligent Bio-Sys.*, 821 F.3d at 1367. In particular, Wiz only attempts to address whether POSAs would have a reasonable expectation of success in “[o]ffline snapshotting and offline analyses” (Pet.25), ignoring whether POSAs would have expected to be able to “utilize cloud computing platform APIs” to identify and query “virtual disks of a virtual machine,” take or request the taking of “at least one snapshot of [a] virtual machine at rest,” and “analyze the at least one snapshot to detect vulnerabilities.” ’031 Patent, cls. 1, 9, 16. Wiz has not shown, and cannot show, they would have. Kaeli¶¶104-122.

B. Veselov and Price Fail to Disclose or Suggest Multiple Limitations

Wiz’s obviousness arguments also fail because the combination does not teach multiple claim limitations. Kaeli¶123.

1. The Veselov/Price Combination Does Not Render Obvious Using Cloud Computing Platform APIs to Identify and Locate Virtual Disks

Limitations 1.2 through 1.4, and their corresponding limitations in independent claims 9 and 16 require “utiliz[ing] cloud computing platform APIs to identify virtual disks of a virtual machine” and “us[ing] the computing platform APIs” to query and receive the location of at least one such virtual disk, which facilitate the taking or requesting the taking of snapshots and the analysis of such snapshots for vulnerabilities recited in other limitations. ’031 Patent, cls. 1, 9, 16. Veselov is the only reference Wiz relies on for these limitations (Pet.28-33), but it neither teaches nor suggests these features. Kaeli¶¶124-143.

Wiz asserts that “Veselov teaches that [its] scanning service uses [a communication] interface to ‘identify virtual disks of a virtual machine in the client environment’ in order to facilitate its generation of a snapshot of such disks.” Pet.29. Not so. At most, Veselov discloses, including in the portions Wiz cites, the identification of a VM (e.g., Veselov, 6:30-43), the identification of a snapshot (e.g., *id.*, 11:34-36, 16:21-23), or describes what a snapshot can contain (e.g., *id.* 9:55-62, 11:31-32, 11:37-46). But Veselov never discloses identifying a virtual disk of a VM using cloud computing platform APIs. Kaeli¶¶125-134. As Dr. Stavrou conceded, “Virtual disks are different from virtual machines”—“[t]hey are definitely not synonymous.” Stavrou Tr.97:13-98:10. Likewise, Veselov’s identification of a

virtual machine or snapshot in the context of Figure 1, says nothing of the virtual disk location because Veselov's snapshots can be located separately in a "snapshot storage service." Veselov, 5:13-17, 6:43-49, 7:27-40; Kaeli¶¶127-128. Veselov teaches that "volume images" are "non-queryable" in this embodiment. Veselov, 7:55-61.

Furthermore, the '031 Patent explains that in cloud computing environments, VMs and virtual disks are typically separate and in different locations. '031 Patent, 4:20-24, Fig. 1B; Kaeli¶¶133; Stavrou Tr.92:4-93:19, 94:16-21. Accordingly, Wiz's mapping of Veselov's disclosures identifying virtual machines to the claimed use of cloud computing platform APIs for identifying, querying, and receiving virtual disk location information fails. Kaeli¶¶129-134; *see also* Stavrou Tr.142:15-143:3 (Dr. Stavrou conceding he could not identify and was not aware of any disclosure in Veselov that "identifies or describes an identifier for a virtual disk").⁴

⁴ Wiz falls back on an assertion that APIs and the identification of virtual disks were "well-known" and "routine." Pet.29-31. But Wiz provides no basis to suggest that identifying a VM is obviously or necessarily an identification of any component thereof, where the prior art (Veselov) lacks such disclosure. *K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1366 (Fed. Cir. 2014).

Furthermore, for its Veselov mapping, as noted above (Section IV.A), Wiz improperly relies on distinct features from multiple embodiments—e.g., the embodiments depicted and described in connection with Figures 1 & 2, 3A-3B & 4, and 5A-5B & 6—without “establish[ing] sufficiently that the features of those different embodiments are interchangeable or provid[ing] sufficient rationale to combine the teachings of those different embodiments.” *Abiomed, Inc. v. Maquet Cardiovascular, LLC*, IPR2017-01204, Paper 9 at 9 (PTAB Oct. 23, 2017); Pet.27 (citing Veselov, Figs. “1, 3A-B, 5A-B”), 28 (citing “Figs. 3A-B, 5A-B” as “analogous communication interfaces”). POSAs would not have understood features from these embodiments to be interchangeable. Kaeli¶¶95-103, 128. The Figures 1, 3A/3B embodiments involve “computing environments implemented by a computing resource provider [104,] 300, 350,” which “may” provide users access to scanning services within virtual computing environments using APIs, but they do not locate disks (Figs. 1, 3A/3B) or analyze snapshots (Figs. 3A/3B). Veselov, 4:59-5:8, 10:37-41, 14:37-41, 15:23-27, Figs. 1, 3A-3B; Kaeli¶128; see Section IV.A.C above. Veselov’s APIs only provide interfaces to a user, convey user-specific data, or allow users to specify information for the system; these APIs are never used for

identifying, querying, and receiving virtual disk location information. *See* Veselov, 4:29-48, 5:1-8, 5:13-22, 6:34-38, 6:59-60, 8:46-51, 14:37-53, 15:23-38; Kaeli¶128.⁵

Wiz's citations to Veselov's Figures 5A/5B embodiments, in contrast to Figures 1 and 3A/3B, involve computing environments that are not effectuated by computing resource service providers, such as typical on-premises systems, and do not use APIs at all, let alone cloud computing platform APIs operating as claimed. Veselov, Figs. 5A-5B, 15:56-17:66; Kaeli¶129; *see also* Stavrou Tr.154:2-155:22. Wiz cannot meet its burden in this proceeding by invoking disclosures from different embodiments while ignoring those embodiments' distinctions and failing to explain why the embodiments are interchangeable and would have been modified and combined. *Stepan*, 868 F.3d at 1346 n.1; *BlephEx*, 24 F.4th at 1401; Kaeli¶¶95-103, 128-129.

Wiz also argues that the claimed cloud computing platform APIs and their uses are "taught or suggested by Veselov's discussion of tailoring snapshots." Pet.32. But this argument again relies on Veselov's separate embodiments—8:16-

⁵ Wiz turns to tertiary references not asserted in Ground 1 for evidence that API's for identifying virtual disks was well-known and routine. Pet.31. But Wiz fails to identify anything in those references that would motivate POSAs to modify Veselov's systems to do more than identify a "VM generally." Kaeli¶¶132-133.

45 and 14:37-57—which do not disclose using cloud computing platform APIs to identify, query, or receive virtual disk location information. Kaeli¶131. And, the fact that Veselov's systems may (i) configure a scan environment, including to “identify the data elements of the virtual machine 112 that are needed to perform the security assessment” (Veselov, 8:16-45), and (ii) be configured by an owner or administrator, including with respect to what is sent to the user “to be displayed, selected, changed, etc.” (*id.* 14:37-57), does not demonstrate that POSAs would have been motivated to modify Veselov's systems to locate or query virtual disk locations using cloud computing platform APIs as claimed. Kaeli¶131. Wiz also asserts “disk-identification tools” were “commonplace” (Pet.32), but that at best shows what a POSA *could have* made, but says nothing for why a POSA “*would have been motivated to make* the combinations or modifications” to Veselov “to arrive at the claimed invention. *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (emphasis original); Kaeli¶¶132-133.

Wiz also asserts that Veselov suggests the identification of virtual disks because Veselov's “API-based UI can be used to select assessment targets and other assessment parameters” and “perform general management of ‘virtual resource allocations.’” Pet.32. But, as described above, none of the Veselov disclosures Wiz relies on suggests using cloud computing platform APIs as claimed, and Wiz fails to explain why POSAs would have modified Veselov to include these features. *See*

Pet.32-33 (citing Veselov, 2:22-3:19, 5:1-8, 14:37-15:29, 19:30-37, 19:60-64, 20:46-56); Kaeli¶134.

With respect to limitations 1.3, 9.3, and 16.3, which require using cloud APIs to query for “a location of at least one of the identified virtual disks,” Wiz argues POSAs 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. Wiz argues that the scanning service may “generate the snapshot itself” (Pet. 33 (citing Veselov, 9:9-25)), but that is inapposite because if the service generates the snapshot “itself,” it does not query the location of any disk using cloud APIs as claimed. Kaeli¶¶135-137; Veselov, 9:9-25 (no discussion of APIs). However, the only “query” disclosed in Veselov relates to querying a “snapshot storage service” to find a stored snapshot based on a “VM identifier,” “identifier of the virtual machine instance,” “file name,” or “key,” none of which require a cloud computing platform API querying for the location of a virtual disk. Veselov, 7:34-61; Kaeli¶137. And Wiz’s fallback that these individual claim elements are “well-known” and “routine[]” (Pet.33-34) are insufficient and “fraught with hindsight bias.” *ActiveVideo Networks, Inc. v. Verizon Commc’ns, Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012); *Belden*, 805 F.3d at 1073; Kaeli¶¶138-139.

With respect to limitations 1.4, 9.4, and 16.4, which recite “receive an

identification of the location of the virtual disks of the virtual machine,” Wiz contends that Veselov suggests receiving identifications of the locations of virtual disks of VMs because “making a query typically result[s] in receiving ... requested information” (Pet.35). This contention relies on and fails on Wiz’s argument for limitations 1.3, 9.3, and 16.3. Further, Wiz’s assertion that Veselov renders obvious limitations 1.4, 9.4, and 16.4 because it discloses that a VM has a “virtual network address” again improperly and wrongly conflates (i) the identification of a VM generally and (ii) the challenged claims’ virtual disk-specific recitations. Kaeli¶¶140-142.

Objective evidence also supports these limitations were nonobvious. *See* Section IV.C. For example, Mr. Shua explains, including in videos pre-dating these proceedings, how using cloud APIs to identify the location of specific virtual disks before analyzing a snapshot was critical to SideScanning™ performance and Orca’s commercial success. Shua¶48; Ex. 2133, 1; Ex.2082, 8:06-11:08 (describing how cloud “manufacturers moved to an architecture where the storage in fact sits physically on a different box”); Ex.2083 (transcript of Ex.2082); Ex.2099, 9:40-14:00; Ex.2133 (transcript of Ex.2099) at 4 (describing performance benefits of determining location); Kaeli¶¶212-213. Simply identifying a VM (as in Veselov) does not support such functionalities, as Mr. Shua and Orca recognized. Shua¶48; Kaeli¶¶212-213.

REDACTED

REDACTED

2. The Veselov/Price Combination Does Not Render Obvious Taking or Requesting the Taking of Snapshots of VMs At Rest, or Snapshot Analyses When VMs Are Inactive

Limitations 1.5, 9.6, and 16.6 require taking a snapshot of a “virtual machine at rest” or requesting the taking of a snapshot of a “virtual machine at rest.” *See* Section III.A above (Claim Construction). Limitations 1.6, 9.7, and 16.7 require analysis of such a snapshot when “the virtual machine is inactive.” The teachings of Veselov and Price do not render these limitations obvious. Kaeli¶¶144-152.

Wiz’s failure to show obviousness of these limitations directly follows from its inability to show a motivation to combine Veselov and Price. Wiz incorrectly asserts Veselov “does not expressly describe the state of the VM at the time the snapshot is captured” (Pet.38) and that Veselov’s “analysis does not depend on the state of the original VM during the analysis step” (Pet.43), but as discussed above, Veselov does expressly describe its VMs state: active. Kaeli¶¶146, 60, 150. Indeed, Veselov’s invention and goal is for “the assessment” to be “performed without impacting the customer’s virtual machine, which may be servicing requests from its customers or performing other useful work.” Veselov, 12:21-43. For a customer’s

VM to “perform[] other useful work” and not be impacted by an assessment, it must stay active during the capture of a snapshot and the assessment process. Kaeli¶¶60, 150.

Thus, even if (as Wiz contends) a POSA would have known “many VMs would be at rest when security assessments were initiated” and “[t]aking a snapshot of a VM at rest was also consistent with common practice in the field” (Pet.39), neither assertion is consistent with Veselov itself, and no motivation has been shown to modify Veselov to operate counter to its purpose of maintaining VM activity. Stavrou Tr.140:19-141:7 (“I don’t talk anywhere in my declaration about modifying Veselov, sir.”). Nor is there a motivation to modify Veselov to combine Price’s teachings of offline VM *imaging*. In fact, the claimed taking or requesting taking of a *snapshot* of a VM “at rest” ran counter to conventional wisdom. Ex.2117, 1 (third party remarking Orca “transcends traditional solutions by inspecting data at rest.”); see Section IV.C below; Kaeli¶¶147. Thus, Wiz’s Veselov/Price combination does not render limitations 1.5, 9.6, and 16.6 obvious. Kaeli¶¶144-152.

Likewise, the combination does not render obvious limitations 1.6, 9.7, and 16.7 requiring that, “during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive.” Wiz wrongly argues Veselov “at least suggests analyzing the snapshot while the VM is inactive, since its analysis does not depend on the state of the original VM during the analysis step” (Pet.43)

because that would preclude Veselov's machine from "performing other useful work" during the analysis. Veselov, 12:21-43; Kaeli¶¶60, 150. And, while Wiz contends "this would have been a readily apparent option consistent with common practice in the field," that option is *inconsistent* with Veselov.

It would not have been obvious "for the VM to be inactive during the detection of the vulnerabilities in some situations" (Pet.44) because Veselov proscribes such inactivity. Kaeli¶¶146-148; *see also* Stavrou Tr.263:16-264:10 (conceding an offline VM "wouldn't be running its normal workload," "wouldn't be free or able to continue servicing requests," and "wouldn't be able to perform other work"). Wiz also overlooks the different classes of data analyzed with Price's offline VM *imaging* and Veselov's online VM *snapshotting*, which would lead a POSA away from the Veselov/Price combination. Kaeli¶¶147-148; *see also* Stavrou Tr.272:7-13.

Furthermore, objective evidence refutes Wiz's hindsight-based arguments that taking snapshots of a VM at rest was "common practice in the field" (Pet. ^{REDACTED}

. *See* Section IV.C; ^{REDACTED}

3. The Veselov/Price Combination Does Not Render Obvious Reporting Detected Vulnerabilities as Alerts

Wiz fails to show that limitations 1.7, 9.8, and 16.8, requiring "report[/ing] the detected vulnerabilities as alerts," would have been obvious. Wiz relies on only Veselov for these limitations (Pet.45), but Veselov does not mention alerts.

Kaeli¶¶153-158. Wiz therefore incorrectly argues that reporting “assessment results” and reporting detected vulnerabilities “as alerts” are equivalent. Pet.45. Wiz’s argument contradicts the language of these limitations, which do not end after reciting “report the detected vulnerabilities,” but continue and require that detected vulnerabilities be reported “as alerts.” ’031 Patent, 8:60-61, 7:40-47; Kaeli¶¶156-157. As Dr. Stavrou admitted, reporting results does not constitute reporting vulnerabilities “as alerts” as claimed. Kaeli¶157; Stavrou Tr.287:4-12 (“a report is a little bit more generic term. An alert is something that potentially makes it stand out.”).

Indeed, as Wiz admitted in the parties’ related district court litigation, and Dr. Stavrou repeatedly conceded, the ’031 Patent’s “claims presuppose that one would be able to report results without using alerts,” and “[a] report and an alert ***must mean different things*** to give meaning to all the claim language.” Ex.2048, 12; Stavrou Tr.284:18-285:6, 286:9-287:21 (Dr. Stavrou testifying that “alerts are different than reports” and agreeing that “it’s not enough to just report, you have to report as alerts” to “meet the requirement of the claims”). Further, POSAs would not expect Veselov’s “results” to amount to “alerts” in view of the finite universe of findings generated from Veselov’s analysis and because such findings include benign data that would not make sense to treat as an “alert.” See Veselov, 10:18-22, 2:42-46, 7:15-16; Kaeli¶156.

Because Wiz's Veselov/Price combination fails to teach or suggest multiple limitations in the independent claims, all challenged claims should be found not unpatentable. Kaeli¶¶164.

4. The Veselov/Price Combination Does Not Render Obvious Dependent Claims 4 and 12

Dependent claims 4 and 12 recite, “wherein the identification of the location of the virtual disks of the virtual machine includes a virtual address of at least one of the virtual disks.” Wiz's failure to show that Veselov and Price render obvious the virtual disk identification-related limitations of claims 1 and 9 applies equally to its obviousness contentions for claims 4 and 12. *See* Section IV.B.1; Kaeli¶¶159-164. Additionally, none of the disclosures that Wiz relies on for the additional limitation of dependent claims 4 and 12—including the “identification of *VM* virtual addresses” that Wiz argues Price discloses (Pet.47)—renders obvious the claimed identification of “a virtual address of at least one of the virtual disks.” *See* Kaeli¶¶159-163.

C. Objective Evidence Demonstrates and Confirms the Non-obviousness of the Challenged Claims

Objective evidence of non-obviousness “play[s] an important role as a guard against the statutorily proscribed hindsight reasoning in the obviousness analysis.” *WBIP*, 829 F.3d at 1328-30. Indeed, it “may often be the most probative and cogent evidence in the record,” and “must be considered in every case.” *Id.* at 1328.

While “objective evidence of nonobviousness lacks a nexus if it exclusively relates to a feature that was ‘known in the prior art,’ the obviousness inquiry centers on whether ‘the claimed invention as a whole’ would have been obvious.” *Id.* at 1330; *see also Medtronic, Inc. v. Teleflex Innovations S.a.r.l.*, 70 F.4th 1331, 1337 (Fed. Cir. 2023) (finding nexus “tied to the combination of features as a whole” even though “every element” of the challenged claims was “individually known in the prior art”). Accordingly, objective nonobviousness evidence may either be “linked to an individual element, or, in other circumstances, it could be linked to the inventive combination of known elements.” *WBIP*, 829 F.3d at 133.

Here, it is undisputed that the combinations of elements claimed were not taught in the prior art—Wiz relies on only (hindsight-driven) obviousness challenges. And evidence of long-felt, unsolved need, skepticism regarding the inventions, industry acceptance, industry praise, commercial success, and copying demonstrates and confirms the non-obviousness of the '031 Patent's claimed combinations. *See* Sections IV.C.1-IV.C.5; Kaeli¶181.

1. The Claimed Inventions Solved a Long-felt, Unmet Need With A “Genuinely Genius Innovation”

A long-felt but unresolved need shows non-obviousness because “the need would not have persisted had the solution been obvious.” *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1054-56 (Fed. Cir. 2016) (en banc). Here, Orca's

inventions solved a long-felt but unmet need for an unobtrusive, comprehensive security solution for dynamic cloud environments. Shua¶¶78-88.

As leading technology companies like Amazon, Microsoft, and Google began providing and developing their public cloud services, many “[o]rganizations ... increasingly adapted their applications to be run from multiple cloud computing platforms.” ’031 Patent, 1:20-23; Ex.2076, 5-6 (describing the “Shift to Cloud” beginning in 2010-2014); Ex.2134, 2 (“Cloud adoption takes off” around 2012). And, “virtualization technologies,” such as “virtual machines, software containers, and serverless functions,” were also “adapted by cloud computing platforms.” ’031 Patent, 1:36-39. Such technologies had computing advantages, but they were vulnerable to cyber threats. ’031 Patent, 1:36-39; Ex.2136, 2 (“As more workloads are shifting to the cloud, cybersecurity professionals remain concerned about security of data, systems, and services in the cloud.”); Ex.1029, 1 (“[S]ecurity is the biggest problem of” cloud computing systems.). Accordingly, the cloud security industry developed various methods for protecting cloud computing infrastructures, including: (1) “traffic inspection,” (2) using “network scanner[s] deployed out of path,” (3) “traffic monitor[ing],” and (4) using “agents installed in each server.” ’031 Patent, 1:44-2:14; Shua¶¶79-85; Ex.2102, 1 (describing challenges of establishing network scans and agents in cloud environments).

However, these methods suffered from multiple disadvantages, as Mr. Shua explained both in the '031 patent and at multiple conferences and videos prior to these IPR proceedings. Shua ¶¶80-83 (discussing '031 Patent 1:44-2:28 and Exs. 2082, 2083, 2099, 2100). “Traffic inspection may not provide an accurate indication of the security status of [a] server due to inherent limitations, such as encryption” and lack of access to pertinent data. '031 Patent, 1:49-52. With network scanners deployed out of path, servers “may not respond” or “expose ... necessary data,” and network configuration- and credential-related issues were problematic. '031 Patent, 1:57-64. Traffic monitoring “detect[s] threats only based on the monitored traffic” and thus can miss server “misconfiguration[s]” and “vulnerabilities in software executed by the server.” '031 Patent, 2:1-6. And “[u]sing agents is a cumbersome solution for a number of reasons, including IT resource management, governance, and performance.” '031 Patent, 2:11-13; Ex.2076, 11 (“Traditional agents struggle with complex deployment and maintenance.”). “For example, installing agents in a large data center may take months.” '031 Patent, 2:14-15; Ex.2103, 2 (“Customers tell me that agent-based approaches are only able to cover up to 50% of the cloud real estate even after several months of deployment.”).

Prior methods for protecting cloud computing infrastructures failed to adequately address the security of VMs at rest, i.e., VMs that are “powered off.” '031 Patent, 2:15-26, 3:53-55; Ex.2135, 3 (recognizing, post '031 Patent priority

date, that “[a]gentless scanning works” to “extend[] coverage to both active *and dormant* virtual machines.”). Previously, VMs at rest “[we]re not inspected for vulnerabilities, simply because scanners and/or installed monitoring agents cannot operate on a powered-off machine,” or only past, potentially out-of-date information for such machines was scanned. ’031 Patent, 2:25-32; REDACTED

Accordingly, there was a long-felt, unmet need for a cloud security solution that could adequately address “constantly evol[ing]” threats and “undetected vulnerabilities [that] can pose cyber threats,” including for “data or a machine at rest.” ’031 Patent, 2:33-36; Ex.2136, 2 (“traditional security tools are often not suited for the challenges of dynamic, virtual and distributed cloud environments.”), 14 (“traditional security solutions either don’t work at all in cloud environments or have only limited functionality.”); Ex.2137, 1 (“the journey to obtain the right level of visibility and control over the cloud workloads is still a challenge.”).

Mr. Shua’s recognition of this need and flaws in preexisting cloud security solutions motivated him to found Orca and develop a new agentless deep scanning technique in Orca’s SideScanning™, including as claimed in the ’031 Patent (*see* Section IV.C.2 immediately below)—a “genuinely genius innovation” that redefined the industry. Ex.2076, 7-8, 11; *see also* Shua¶¶12-16, 85-88; Ex.2103, 1; Ex.104, 2; Ex.2148, 15; Kaeli¶182; Ex.2138, 4 (Wiz: “[A]gentless deep scanning

approaches ... achieve a level of comprehensiveness in terms of coverage and features that is not possible with agent-based approaches.”).

2. Orca's SideScanning™ Practices the '031 Patent

Orca's Cloud Security Platform, and in particular the SideScanning™ techniques that power the platform, have used the inventions claimed in the '031 since 2019 when Orca first introduced Orca's Cloud Security Platform commercially. Shua¶27; *see also id.* ¶¶28-77 (explaining how SideScanning practices claims 1-16); Kaeli¶182. For example, with respect to independent claims 1, 9, and 16, Orca's SideScanning:

- establishes interfaces between client environments and Orca's back-end security components, e.g., Orca's “Onboarding” process where a client environment provides Orca's SideScanning™ with a role that “establishes trust between [the client environment's] account and Orca's production account.” (Preambles, limitations 1.i, 1.1, 9.1, and 16.1), *see, e.g.*, Shua¶¶29-35 (discussing Ex.2067, 1, 5-7, 12, 15; Ex.2094; Ex.2095; Ex.2096; Ex.2097; Ex.2098; Ex.2150; Ex.2300; Ex.2301)
- uses cloud computing platform APIs ^{REDACTED} to identify virtual disks of VMs and to query and receive their ^{REDACTED} (limitations 1.2-1.4, 9.2-9.4, and

16.2-16.4), *see, e.g.*, Shua¶¶36-41 (discussing Ex.2302; Ex.2303; Ex.2304; Ex.2067, 5, 8-9; Ex.2099, 9:40-14:00);

- emulates virtual disks of VMs (limitations 9.5 and 16.5), *see, e.g.*, Shua¶¶49-50 (discussing Ex.2067, 10);
- takes snapshots of VMs at rest (limitations 1.5, 9.6, and 16.6), *see, e.g.*, Shua¶¶51-54 (discussing Ex.2067, 1, 7, 10; Ex.2300, 5-6, 12; Ex.2093, 7);
- analyzes such snapshots to detect vulnerabilities while target VMs are inactive (limitations 1.6, 9.7, and 16.7), *see, e.g.*, Shua¶¶55-58 (discussing Ex.2067, 1, 3, 11, 19; Ex.2300, 5; Ex.2093, 7, 16); and
- reports detected vulnerabilities as alerts (limitations 1.7, 9.8, and 16.8, claims 2, 10), *see, e.g.*, Shua¶¶59-62 (discussing Ex.2067, 16; Ex.2093, 22).

Orca's SideScanning also practices dependent claims 2-8 and 10-15. Shua¶¶63-77 (discussing Ex. 2067, Ex.2300); Ex.2168, ¶163.

Orca's SideScanning™ solution was a “big leap in cloud security” because, by using the above-discussed features, it “gather[ed] crucial data through the cloud provider's APIs, while scanning snapshots,”⁶ “allowed deep visibility into cloud

⁶ *See* limitations 1.2-1.5, 9.2-9.4, 9.6, 16.2-16.4, 16.6.

workloads without the need to install agents,” including for machines at rest,⁷ and provided “[t]argeted vulnerability alerts”⁸ that drew attention to what really mattered. Ex.2076, 11-12, 31; REDACTED

Kaeli¶¶183-192;

Shua¶¶124-128; Ex.2118, 4-8.⁹

3. The Claimed Inventions Defied the Skeptics, and Became Widely Accepted in the Industry

“Evidence of industry skepticism weighs in favor of non-obviousness.” *WBIP*, 829 F.3d at 1335. And, if an invention achieves widespread industry acceptance, including after defying skeptics, that also evidences non-obviousness. *Allen Archery*,

⁷ See limitations 1.6, 9.7, 16.7.

⁸ See limitations 1.7, 9.8, 16.8.

⁹ Since its inception, Orca has attributed its success to its “patent pending” SideScanning™ techniques, which referred to the inventions claimed in the '031 patent and related patents claiming priority to Orca's provisional patent application (No. 62/797,718). Shua¶¶16-24; Exs.2065-2067, 2080-2081, 2088, 2090, 2092-2100, 2107-2108, 2110, 2118, REDACTED

Inc. v. Browning Mfg. Co., 819 F.2d 1087, 1092 (Fed. Cir. 1987).

Here, Orca's inventions defied skeptics and achieved widespread industry acceptance.

REDACTED

This same skepticism was noted in the 2024 *Future of Cloud Security* report, which remarked on “how difficult it was for older providers to come to terms with the success of agentless scanning” after Orca “introduced the concept.” Ex.2076, 7. In fact, that report explicitly states that industry participants were “skeptics” because “from a security perspective, agentless scanning was nothing compared to what attacks they were able to detect and protect.” *Id.* “They missed however that security teams were not yet in the weeds of these architectures,” so before Orca, they “didn’t know what they didn’t know.” *Id.* 7, 8 (“[T]he pivotal moment was the introduction of agentless scanning,” “but anyone who tells you they knew it at the time is lying”); Ex.2106, 1 (“Agentless Solutions Fall Short”); Shua¶¶89-91; Kaeli¶¶193-197.

REDACTED

REDACTED

Shua¶¶89-91; Section IV.C.2 (Orca's SideScanning™ practices the challenged claims); Kaeli¶¶193-197. And, ultimately, SideScanning™ was widely accepted—"everyone needed it in order to stay competitive." Ex.2076, 7; *see also* Ex.2113, 4 ("Global innovators such as Databricks, Robinhood, Autodesk, News Corp, NCR, Duolingo, Unity Technologies, Druva and many more trust Orca Security to protect their public cloud estates"); Shua¶¶99, 106 (describing customers and commercial success); Kaeli¶¶193-197; Ex.2103, 1 ("[A] new 'agent-less' approach to cloud security has recently become possible due to cloud-native APIs now available from CSPs. This approach provides security in a fundamentally different way.").

4. The Industry Praised Orca's Revolutionary Inventions

Evidence of industry praise shows non-obviousness because “[i]ndustry participants, especially competitors, are not likely to praise an obvious advance.” *Apple*, 839 F.3d at 1053.

Following Orca's introduction of SideScanning™ and its 2019 filing of the provisional application that led to the '031 Patent, Orca received numerous awards for its inventions. Shua¶¶124-141 (discussing awards in Exs.2076, 2117-2132); Kaeli¶198. In 2020, Orca won CRN's "20 Coolest Tech Startups of 2020." Ex.2119, 6-7. CRN touted "Orca's SideScanning technology" which "automatically assesses the security state of every discovered asset" to provide "complete visibility." *Id.* The same year, Orca won Forbes's "Top 20 Cybersecurity Startups to Watch in 2021," the SINET16 Innovator Award, was named a "Visionary Vendor" by Security Current and a "Gartner Cool Vendor" in the CSPM category. Ex.2120, 7 (Forbes finding Orca "noteworthy for its innovative approach to providing instant-on, workload-deep security" for cloud computing systems, emphasizing Orca's "patent-pending SideScanning™ technology" that "reads cloud configuration and workloads' runtime block storage out-of-band."); Ex.2143, 3; Ex.2145, 2; Ex. 2121. In 2022, AWS awarded Orca "global Security Partner of the Year." Ex.2122, 1-2. And in both 2022 and 2023 SC Media named Orca the "Best Cloud Security Posture Management (CSPM) solution" and a finalist in other categories. Ex.2124, 1 (award

noting customer praised Orca's "agentless approach" as "both a major innovation and a game changer"); Ex.2123, 1-2 ("After years of dealing with agents, then seeing how easy it is to install and use Orca, I knew that its agentless approach was both a major innovation and a game changer."); Ex.2125, 1-2. Orca was also named to Forbes' 2023 Cloud 100 list, the 2023 and 2024 Redpoint InfraRed 100 List, and a "most innovative startup" by Cyber 2024. Exs.2127-2132. Orca received those awards because of SideScanning, which is the technology powering Orca's product, and the inventions claimed in the '031 Patent. Shua¶¶141, 93.

REDACTED

REDACTED

-

REDACTED

REDACTED

As discussed, Orca's

SideScanning™ was recognized as “genuinely genius,” “unique,” “like magic,” and “a big leap in cloud security,” including with respect to specific features in the '031 Patent's claimed combinations, such as using cloud computing platform APIs to facilitate snapshot analyses and inspecting data at rest. Ex.2076, 7 (“[T]he ability to view workload data without an agent was a genuinely genius innovation – utilizing the nature of cloud APIs being accessible to vendors.”), 11 (“Orca launched the first version of agentless side scanning, which allowed deep visibility into cloud workloads without the need to install agents.”), 11-12 (“Agentless solutions ... leverage cloud APIs to snapshot underlying instance hard disks, copy them into the security vendor[']s account, where they're hooked up on the vendor's side and scanned,” which “creates an elegant ‘like magic’ approach”), 31 (“Orca Security made a big leap in cloud security with the introduction of its patented agentless SideScanning technique,” a “unique method” that “gather[s] crucial data

through the cloud provider's APIs, while scanning snapshots"); Ex.2117, 1 (Orca "transcends traditional solutions by inspecting data at rest"); REDACTED

; Kaeli ¶¶200-202.¹⁰

Industry praise demonstrates the challenged claims' non-obviousness.

5. Wiz Copied Orca's Inventions

"[C]opying by a competitor is a relevant consideration in the objective indicia analysis" and "evidence that the patented invention is nonobvious." *Liqwd, Inc. v. L'Oreal USA, Inc.*, 941 F.3d 1133, 1137 (Fed. Cir. 2019). In particular, copying plays a dual role of "prais[ing]" the invention and suggesting that the prior art was insufficient. *See Stratoflex*, 713 F.2d at 1541; *WBIP*, 829 F.3d at 1336. And "[e]vidence of access and substantial similarity *is* evidence of copying." *Medtronic, Inc. v. Teleflex Innovations S.a.r.l.*, 70 F.4th 1331, 1340 (Fed. Cir. 2023) (emphasis

¹⁰ *See also* Ex.2118, *Vendor Landscape and TCO Analysis*, 5 ("Orca uses a patent-pending technique called SideScanning™, ... which unobtrusively scans the run-time block storage layer—out of band—to extract valuable data about the environment and the assets communicating in it."), 4 (customer reporting Orca's solution is "unique" because it "locates vulnerabilities with precision and delivers tangible, actionable results—without having to sift through all of the noise").

in original).

REDACTED

**a. Wiz Copied Orca's Patent-Practicing SideScanning™
Invention**

Wiz knew of and had access to Orca's technology before Wiz was even founded because Mr. Shua presented Orca's SideScanning™ technology to Wiz's founder Yinon Costica when he still worked at Microsoft in May 2019. Shua¶¶108-112.

REDACTED

REDACTED

see also

Shua¶¶113-114 (describing competition with Wiz indicating they had copied Orca's technology); Kaeli¶¶203-227.

REDACTED

REDACTED

REDACTED

REDACTED

¹¹ As the '031 Patent's claims recite, Orca's SideScanning™ utilizes Amazon Web Services (AWS) APIs ("cloud computing platform APIs") to identify, query, and locate virtual disks of VMs implemented on AWS to facilitate snapshot analyses to detect vulnerabilities, and Orca's AWS policy provides access permissions to AWS resources required for such scanning. Shua¶¶32-34, 36-41, 43-44, 46-47.

REDACTED

Shua^{¶¶} 32-47

(explaining how Orca uses AWS API calls in practicing the challenged claims), 115-

116

REDACTED

REDACTED

As the above-discussed evidence shows, Wiz accessed and copied Orca's claimed inventions.

b. Wiz's "Workload Scanning" Is Substantially Similar To Orca's SideScanning™

Wiz's copying of Orca's technology is further evidenced by Wiz's access to Orca's technology (discussed above) and the substantial similarity between Wiz's Cloud Security Platform and Orca's SideScanning™. *Medtronic*, 70 F.4th at 1340 ("Evidence of access and substantial similarity *is* evidence of copying.") (emphasis in original).

Wiz's Cloud Security Platform uses what Wiz calls "workload scanning," which, like Orca's SideScanning™, practices the challenged claims. Kaeli¶¶228-240 (discussing Exs. 2026, 2115, 2158, 2308-2309, 2074, REDACTED, 241-260. Wiz's "workload scanning":

- establishes interfaces between client environments and Wiz's back-end security components (limitations 1.1, 9.1, 16.1); *see also* Shua¶¶115-117 (discussing Ex.2308, 1, 3; Ex.2309, 21); Kaeli¶¶241-244 (discussing Exs.2308-2309, 2115);
- uses cloud computing platform APIs, e.g., ec2:DescribeInstances, to identify virtual disks of VMs and to query and receive location information about such disks (limitations 1.2-1.4, 9.2-9.4, 16.2-16.4), *see also* Shua¶¶115, 118-119 (discussing Ex.2309, 21; Ex.2026, 7-8; Ex.2115, 1-2); Kaeli¶¶245-248 (discussing Exs.2308-2309, 2115);

- emulates virtual disks of VMs so the “scanner has read-only access to the scanned disk” (limitations 9.5, 16.5), *see, e.g.*, Shua¶¶120 (discussing Ex.2115, 3); Kaeli¶¶259-260 (discussing Ex.2075);
- takes snapshots of VMs at rest (limitations 1.5, 9.6, 16.6); *see, e.g.*, Shua¶¶121 (discussing Ex.2146, 1); Kaeli¶¶249-252 (discussing Exs.2308, 2165, 2167);
- analyzes snapshots as a “fundamental principle” of agentless scanning to detect vulnerabilities while VMs are inactive (limitations 1.6, 9.7, 16.7), *see, e.g.*, Shua¶¶116-118, 121 (discussing Ex.2026, 2-3, 7-8; Ex.2146, 1; Ex.2115, 1-2); Kaeli¶¶253-255 (discussing Exs.2115, 2165, 2167); and
- reports detected vulnerabilities as alerts ('031 Patent, cls. 1, 9, 16 (limitations 1.7, 9.8, 16.8)), *see, e.g.*, Shua¶¶122 (discussing Ex.2147, 2); Kaeli¶¶256-258 (discussing Ex.2165).

REDACTED

REDACTED

see also Shua¶¶108

(explaining Orca has had dozens or hundreds of competing proof of concepts against

Wiz, and customers frequently remark that Wiz's core product functionality is the same as SideScanning); Kaeli¶¶228-239.

Wiz's copying of Orca's implementation of the inventions claimed in the '031 Patent plays the dual role of "prais[ing]" the invention and suggesting that the prior art was insufficient. *See Stratoflex*, 713 F.2d at 1541; *WBIP*, 829 F.3d at 1336.

6. Orca's And Wiz's Commercial Success Demonstrates Non-obviousness

The non-obviousness of the challenged claims is further reinforced by Orca and Wiz's commercial success. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018).

After filing the provisional patent application that led to the '031 Patent in January 2019, Orca obtained a remarkable amount of investment. Shua¶¶93, 95-107 (discussing Exs.2065, 2108-2113, 2140 and explaining how funding was due to claimed inventions); Ex.2149, 24; '031 Patent, Cover; Kaeli¶¶261. By June 2019, Orca raised \$6.5 million in funding due to SideScanning™ technology that "collects cloud configuration and integrates with the cloud infrastructure to read virtual machine disks," with one investor remarking about "Orca's unique approach and innovative solution." Ex.2065, 2-4; Ex.2107, 3. In 2020, Orca raised another \$75 million in funding. Shua¶¶97-102; Ex.2108, 1 (funding raised based on "unique ability [] achieved using Orca' Security's patent-pending SideScanning™ technology"); Ex.2109, 1-2; Ex.2110, 1; Ex.2111, 1-2 Ex.2140, 2. And by 2021,

Orca had raised another \$550 million and was valued at between \$1.2-\$1.8 billion. Ex.2112, 1-2; Ex.2113, 1; Ex.2139, 1. These funding announcements showed that Orca's commercial success is attributable to the cloud computing provider API-based techniques to facilitate analyzing snapshots for vulnerabilities claimed in the '031 Patent. Shua¶¶95-107; *see also, e.g.*, Ex.2113, 1 (“Orca Security’s patent-pending SideScanning™ technology collects data directly from cloud provider APIs and the workload’s runtime block storage out-of-band” and detects “vulnerabilities”), 3 (praise from industry participants and investors), 4 (Orca “[p]rioritize[s] risk based on the severity of the underlying security issue, its accessibility, and business impact” and reports issues as “alerts”). Importantly, Orca did not enjoy this success because it was *already* a market leader and simply introduced a new product, which is due less weight. *Pentec, Inc. v. Graphic Controls Corp.*, 776 F.2d 309, 316 (Fed. Cir. 1985).

REDACTED

Ex.2076, 7 (“CSPM

can be defined by pre and post-Orca”).

¹² Cloud Workload Protection Platform.

Orca also earned significant revenues from its Cloud Security Platform “power[ed]” by SideScanning™. Shua¶¶93-94; Ex.2067, 1, 3. Since introducing SideScanning in 2019 through the end of 2024, REDACTED . Shua¶¶94; Ex.2312 (Orca Revenue 2019-2024). REDACTED

Shua¶¶94-95; *Chemours Co. FC v. Daikin Indus., Ltd.*, 4 F.4th 1370, 1378 (Fed. Cir. 2021) (“significant sales” are evidence of commercial success).

The commercial success of Wiz’s infringing Cloud Security Platform further demonstrates non-obviousness. *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1130 (Fed. Cir. 2000) (“[T]he success of an infringing product is considered to be evidence of the commercial success of the claimed invention.”). Wiz reports that after February 2021—i.e., after Wiz copied Orca’s inventions (Section IV.C.5; Ex.2308; Ex.2309—its annual recurring revenue (“ARR”) grew 100X in 18 months, making it the “fastest software company to achieve this feat.” Ex.2116, 1. Wiz attributed this success to its platform’s alleged “new approach” (i.e., Orca’s approach), which allowed Wiz’s platform to “be rolled

out in minutes via an agentless, API-centered approach to seamlessly scan workloads and give organizations full visibility of their cloud environment.” *Id.* 2.¹³ Wiz has since announced even higher revenues and valuations due to its copying of Orca’s technology. *See, e.g.*, Ex.2141, 2; Ex.2142; Kaeli ¶¶262-263.

The above-discussed objective evidence demonstrates and confirms the non-obviousness of all challenged claims.¹⁴

V. Claims 2 and 10 Are Nonobvious Over Veselov, Price, and Hufsmith (Ground 2)

A. POSAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov, Price, and Hufsmith

Even assuming *arguendo* that POSAs would have combined Veselov and Price (they would not have, *see* Section IV.A), POSAs would not have been motivated to modify Wiz’s Veselov/Price combination with teachings from

¹³ Wiz’s public remarks about the use of APIs in its infringing product being “new” also undercut its obviousness arguments. *See Power-One, Inc. v. Artesyn Techs., Inc.*, 599 F.3d 1343, 1352 (Fed. Cir. 2010) (“Artesyn’s position that Power-One’s invention was obvious is inconsistent with its position that its own infringing product was an advancement in the industry.”).

¹⁴ Wiz and Dr. Stavrou have not addressed any of the above-discussed objective evidence of non-obviousness. *See, e.g.*, Stavrou Tr.340:1-341:8.

Hufsmith to achieve what is claimed or expected success in doing so, including because Hufsmith is directed to methods for “determining combined threat score[s] for container images,” not snapshot-based assessments of VMs. *See* Hufsmith (Ex.1078), Title, ¶¶2, 4-6; Kaeli¶¶78-90, 165-172; Shua¶¶155-159; *see also* Stavrou Tr.300:13-22, 306:1-308:20 (agreeing VMs and containers are “not the same thing” and “distinct entities”), 302:2-5 (“Q. You don’t recall ever citing to a reference in Hufsmith to snapshot, though; is that fair? A. I would say it’s fair, yes.”).

Further, with respect to the alerts for which Wiz turns to Hufsmith specifically, Hufsmith describes ways to “annotate code specifying container images” for developers actively working in an “integrated development environment” (or “IDE”). Hufsmith ¶¶15, 153-197; Kaeli¶¶170-171. POSAs would have known and understood this context to be describing *pre-deployment* analyses of container images, which is vastly different from security assessments of running VMs contemplated by Wiz’s proposed Veselov/Price combination. Kaeli¶¶170-171. In short, Wiz once again relies on improper hindsight to try to reconstruct the claimed inventions.

B. Veselov, Price, and Hufsmith Fail to Render Obvious Claims 2 and 10

Setting aside the Veselov/Price combination’s failure to render obvious independent claims 1 and 9 (Section IV.B), adding Hufsmith does not render obvious “the reporting the detected vulnerabilities as alerts includes indicating

priority levels associated with the detected vulnerabilities” as recited. Kaeli¶¶173-178.

Wiz incorrectly contends there are “several ways” Hufsmith discloses these limitations. Pet.58. First, Wiz relies on “weights” determined by CVE and CWE evaluators sent to a “results engine.” Pet.58. But those weights represent only a type of “count of the number of potential vulnerabilities detected.” Hufsmith ¶90; Kaeli¶175. The weights are not reported as alerts, nor are they “priority levels associated with the detected vulnerabilities.” Kaeli¶175.

Second, Wiz argues Hufsmith teaches “report[s] sent to the user” can have “links” that allow users to see the “metrics,” which Wiz contends are “weights”, from the CVE/CWE evaluators. Pet.59-60. But Hufsmith’s “metrics” simply *include* weights, which, as discussed above, do not reflect “priority levels” for detected vulnerabilities. Hufsmith ¶¶90, 96; Kaeli¶176.

Third, Wiz points to Hufsmith’s disclosure that its system “may display information about a single security vulnerability.” Pet.59. But Wiz concedes these disclosures relate to “annotations in a development environment” (*id.*), i.e., displaying information about a vulnerability for particular lines of source code in a pre-deployment container image. Hufsmith ¶¶165, 168, 196; Kaeli¶177. This is inapplicable to Veselov (and Wiz’s hindsight-driven Veselov/Price combination), which only analyzes deployed VMs where source code would be unavailable for

such annotating. Kaeli¶177. And Wiz fails to explain how or why POSAs could have or would have implemented this feature in the proposed Veselov/Price combination. *Id.*

Fourth, Wiz argues that Hufsmith's "global weights" are the claimed priority levels. Pet.60. Hufsmith, however, explains that its global weights are a single aggregate score for all detected vulnerabilities for a given container image. *See* Hufsmith Figs. 3A/3B, ¶138; Kaeli¶178. Such weights are not the claimed "priority levels" (plural) "associated with the detected vulnerabilities" (plural). Kaeli¶178.

VI. Claims 6 and 14 Are Nonobvious Over Veselov, Price, Hufsmith, and Huseinović (Ground 3)

Wiz fails to show that claims 6 and 14 would have been obvious over the Ground 3 art for at least the same reasons as Grounds 1 and 2. Section IV.B. Furthermore, POSAs would not have been motivated to further modify Wiz's Veselov/Price/Hufsmith combination with Huseinović's teachings, which counsel against collecting offline data. Huseinović (Ex.1049) at 1 ("If the computer is set to off, the data are lost and cannot be retrieved for later analysis."); Kaeli¶¶179-180; Shua¶¶160-162.

VII. Conclusion

Orca respectfully requests that the Board confirm the patentability of every challenged claim.

Respectfully submitted,

Dated: April 7, 2025

By: / Blake R. Davis /

Blake R. Davis (admitted *pro hac vice*)

blake.davis@lw.com

Latham & Watkins LLP

505 Montgomery Street, Ste. 2000

San Francisco, CA 94111-6538

Telephone: 415.395.8033

Fax: 415.395.8095

Counsel for Patent Owner

Orca Security Ltd.

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

I hereby certify that this Patent Owner's Response complies with the word count limitation of 37 C.F.R. § 42.24(b)(2) because the Patent Owner's Response contains 13,970 words using Microsoft Word's counting feature, excluding the cover page, signature block, and the parts of the Patent Owner's Response exempted by 37 C.F.R. § 42.24(b)(2).

By: / Blake R. Davis /

Blake R. Davis (admitted *pro hac vice*)
blake.davis@lw.com
Latham & Watkins LLP
505 Montgomery Street, Ste. 2000
San Francisco, CA 94111-6538
Telephone: 415.395.8033
Fax: 415.395.8095

*Counsel for Patent Owner
Orca Security Ltd.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that on this 7th day of April, 2025, a true and correct copy of the foregoing **Patent Owner's Response and all Exhibits** were served by electronic mail on Petitioner's lead and backup counsel at the following email addresses:

Matthew A. Argenti (Reg. No. 61,836)
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA 94304
Tel.: 650.354.4154
Fax: 650.493.6811
margenti@wsgr.com

Michael T. Rosato (Reg. No. 52,182)
WILSON SONSINI GOODRICH & ROSATI
701 Fifth Avenue, Suite 5100
Seattle, WA 98104
Tel.: 206-883-2529
Fax: 206-883-2699
mrosato@wsgr.com

Wesley E. Derryberry (Reg. No. 71,594)
Tasha M. Thomas (Reg. No. 73,207)
Joseph M. Baillargeon (Reg. No. 79,685)
WILSON SONSINI GOODRICH & ROSATI
1700 K Street, NW, Fifth Floor
Washington, DC 20006
Tel.: 202-973-8947
Fax: 202-973-8899
wderryberry@wsgr.com
tthomas@wsgr.com
jbailargeon@wsgr.com

By: / Blake R. Davis /

Blake R. Davis (admitted *pro hac vice*)

blake.davis@lw.com

Latham & Watkins LLP

505 Montgomery Street, Ste. 2000

San Francisco, CA 94111-6538

Telephone: 415.395.8033

Fax: 415.395.8095

Counsel for Patent Owner

Orca Security Ltd.