

Filed on behalf of: Orca Security Ltd.

Entered: May 9, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-01109
U.S. Patent 11,726,809 B2

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The '809 Patent Improved Cloud Security Systems	4
A.	Problems with the Prior Art	4
B.	The '809 Patent's Innovative Cloud Security Systems.....	4
III.	Claim Construction.....	5
A.	“Analyzing the Snapshot”	6
IV.	Challenged Claims 1-10 and 12-23 Are Nonobvious Over Veselov and Mohanty (Ground 1)	8
A.	POSAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov and Mohanty	8
1.	Overview of Veselov	8
2.	Overview of Mohanty	9
3.	Wiz's Motivations To Combine Veselov and Mohanty Should Be Rejected.....	10
B.	Veselov and Mohanty Fail to Disclose or Suggest Multiple Limitations in the Challenged Claims.....	20
1.	The Veselov/Mohanty Combination Does Not Render Obvious Correlating Determined Cyber Vulnerabilities With a Network Location.....	20
2.	The Veselov/Mohanty Combination Does Not Render Obvious Reporting Vulnerabilities As Alerts Prioritized By Determined Risk.....	23
3.	The Veselov/Mohanty Combination Does Not Render Obvious Dependent Claims	26
C.	Objective Evidence Demonstrates and Confirms the Non- Obviousness of the Challenged Claims.....	30

1.	The Claimed Inventions Solved a Long-felt, Unmet Need With A “Genuinely Genius Innovation”	31
2.	Orca’s SideScanning™ Practices the ’809 Patent	34
3.	The Claimed Inventions Defied the Skeptics, and Became Widely Accepted in the Industry	38
4.	The Industry Praised Orca’s Revolutionary Inventions.....	41
5.	Wiz Copied Orca’s Inventions.....	45
6.	Orca’s And Wiz’s Commercial Success Demonstrates Non-obviousness.....	64
V.	Challenged Claims 1-10 and 12-23 Are Nonobvious Over Veselov, Mohanty, and Czarny (Ground 2).....	68
VI.	A POSA Would Not Have Combined Wiz’s Grounds 1 And 2 References (Grounds 3 and 4)	70
VII.	Conclusion	73

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

<i>Adidas AG v. Nike, Inc.</i> , 963 F.3d 1355 (Fed. Cir. 2020)	13
<i>Allen Archery, Inc. v. Browning Mfg. Co.</i> , 819 F.2d 1087 (Fed. Cir. 1987)	39
<i>Apple Inc. v. Samsung Elecs. Co.</i> , 839 F.3d 1034 (Fed. Cir. 2016) (en banc)	31, 41, 43
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	28
<i>Bettcher Indus., Inc. v. Bunzl USA, Inc.</i> , 661 F.3d 629 (Fed. Cir. 2011)	29
<i>Brown & Williamson Tobacco Corp. v. Philip Morris Inc.</i> , 229 F.3d 1120 (Fed. Cir. 2000)	67
<i>Chemours Co. FC, LLC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	66
<i>Fanduel, Inc. v. Interactive Games LLC</i> , 966 F.3d 1334 (Fed. Cir. 2020)	18
<i>Fromson v. Advance Offset Plate, Inc.</i> , 755 F.2d 1549 (Fed. Cir. 1985)	3
<i>In re Kotzab</i> , 217 F.3d 1365 (Fed. Cir. 2000)	25
<i>In re NTP</i> , 654 F.3d 1279 (Fed. Cir. 2011)	8, 19
<i>Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	19

<i>Iron Grip Barbell Co. v. USA Sports, Inc.</i> , 392 F.3d 1317 (Fed. Cir. 2004)	46
<i>Johns Manville Corp. v. Knauf Insulation, Inc.</i> , IPR2018-00827, Paper 9 (P.T.A.B. Oct. 16, 2018).....	11
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	3
<i>Liqwd, Inc. v. L'Oreal USA, Inc.</i> , 941 F.3d 1133 (Fed. Cir. 2019)	45
<i>Medtronic, Inc. v. Teleflex Innovations S.à.r.l.</i> , 70 F.4th 1331 (Fed. Cir. 2023)	31, 45, 46, 59
<i>Metalcraft of Mayville, Inc. v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	3, 8
<i>Orthocision, Inc. v. PTL OPCO LLC</i> , IPR2023-00625, Paper 34 (Sept. 18, 2024).....	18
<i>ParkerVision, Inc. v. Qualcomm Inc.</i> , 903 F.3d 1354 (Fed. Cir. 2018)	29
<i>Pentec, Inc. v. Graphic Controls Corp.</i> , 776 F.2d 309 (Fed. Cir. 1985)	66
<i>Personal Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	<i>passim</i>
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	15, 20, 64
<i>Power-One, Inc. v. Artesyn Techs., Inc.</i> , 599 F.3d 1343 (Fed. Cir. 2010)	68
<i>Rambus Inc. v. Rea</i> , 731 F.3d 1248 (Fed. Cir. 2013)	31
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	3, 59, 63

TriVascular, Inc. v. Samuels,
812 F.3d 1056 (Fed. Cir. 2016) 18

WBIP, LLC v. Kohler Co.,
829 F.3d 1317 (Fed. Cir. 2016)*passim*

STATUTES

35 U.S.C. § 312(a)(3).....18

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	RESERVED
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> ")
2008	RESERVED
2009	RESERVED

Exhibit	Description
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”)
2020	RESERVED
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, Characterizing Hypervisor Vulnerabilities”)

Exhibit	Description
2023-2024	RESERVED
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_Guideen-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”)
2027-2039	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”)
2041	Appendix D, Invalidity of United States Patent 11,726,809 (the “’809 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)
2042	Appendix D-1, Invalidity of United States Patent 11,726,809 (the “’809 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)
2043	Pallavi Vishwakarma, <i>Agent-Based Vs Network Based Internal Vulnerability Scanning</i> , SecOps Solution.com (July 2, 2023)
2044	<i>Agentless vs Agent-Based Scanning: A Comparative Analysis</i> , Runecast.com (July 20, 2023)
2045	Joint Claim Construction Chart, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Sept. 25, 2024) (“Jt. Claim Constr. Chart”)

Exhibit	Description
2046	Declaration of Douglas E. Lumish Pursuant to 37 C.F.R. § 42.10(c)(2)
2047	Declaration of Steven W. Peters In Response to Petitioner's First Objections to Evidence [<i>served, not filed</i>]
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
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/

Exhibit	Description
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)(2)
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, Containers vs. VMs: What's the difference? (Apr. 8, 2024) [Stavrou Dep. Ex. 2075]
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 ("1st Stavrou Tr.")

Exhibit	Description
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
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=tIS0A92IYm8
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

Exhibit	Description
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=QdBsE2VqipU (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)
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)

Exhibit	Description
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/
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/

Exhibit	Description
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/
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

Exhibit	Description
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/
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

Exhibit	Description
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</i> , 2024 (last visited Mar. 19, 2025), https://risingincyber.com/
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/

Exhibit	Description
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> , <i>ISSA Journal</i> (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</i> , <i>Channel</i> (Oct. 5, 2021), https://www.crn.com/news/security/orca-security-raises-340m-to-scale-platform-r-d-channel
2140	Elias Terman, <i>From Stealthy Startup to Cloud Security Innovation Leader</i> (Feb. 4, 2021), https://orca.security/resources/blog/2020-recap/

Exhibit	Description
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	RESERVED
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
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	RESERVED
2152-2157	RESERVED

Exhibit	Description
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	Alon Weiss & Jiong Liu, <i>Uncover What Is Really Deployed in Your Environment with the Enhanced Wiz Inventory</i> (Dec. 8, 2022), https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory
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	RESERVED
2167-2170	RESERVED
2171	RESERVED
2172	Transcript of Deposition of Angelos Stavrou, Ph.D., taken April 2, 2025 ("2nd Stavrou Tr.")
2173	Qualys, <i>Vulnerability Management</i> (2017). https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet.pdf

Exhibit	Description
2174	Jane Man, <i>Live Monitoring with Endpoint Agents</i> (Sept. 28, 2016), https://www.rapid7.com/blog/post/2016/09/28/live-monitoring-for-endpoints/)
2175	<i>Virus</i> , NIST Computer Resource Center Glossary (last visited May 7, 2025), https://csrc.nist.gov/glossary/term/virus
2176	<i>Vulnerability</i> , NIST Computer Resource Center Glossary (last visited May 7, 2025), https://csrc.nist.gov/glossary/term/vulnerability
2177	Wiz Experts Team, <i>What is Lateral Movement? Understanding Attacker Techniques</i> (Mar. 17, 2025), https://www.wiz.io/academy/what-is-lateral-movement#identify-and-stop-lateral-movement-with-wiz-82
2178	Yinon Costica, <i>A New Vision for Cloud Security Unites Builders and Defenders</i> (June 7, 2022), https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security
2179-2188	RESERVED
2189	U.S. Patent Application Pub. No. 2020/0244678 A1
2190	Karthik Muthukrishnan, <i>Automating Cloud Security Governance</i> (May 14, 2017) (Master's Thesis, Helsinki Metropolia University of Applied Sciences), https://www.theseus.fi/bitstream/handle/10024/130058/Muthukrishnan_Karthik.pdf?sequence=1

Exhibit	Description
2191	Ferda Özdemir Sönmez et al., Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation (2018) https://www.researchgate.net/profile/Ferda-Oezdemir-Soenmez/publication/328714022_Evaluation_of_Security_Information_and_Event_Management_Systems_for_Custom_Security_Visualization_Generation/links/66cb5356920e05672e503f60/Evaluation-of-Security-Information-and-Event-Management-Systems-for-Custom-Security-Visualization-Generation?__cf_chl_tk=GFDVvFCEO0W43yRmGpNuvRoYvLxLlf5MQty2WjCtIKQ-1746109122-1.0.1.1-9thX8K_E0POm9M_WksJEsfRdeg1KqYZ7qaqwHQ8.8yw
2192-2299	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]

Exhibit	Description
2308	REDACTED [PROTECTIVE ORDER MATERIAL]
2309	REDACTED [PROTECTIVE ORDER MATERIAL]
2310	RESERVED
2311	Excerpt from Orca Product Documentation (2024) Part 2 [PROTECTIVE ORDER MATERIAL]
2312	REDACTED [PROTECTIVE ORDER MATERIAL]
2313	Excerpt from Orca Product Documentation (2024) [PROTECTIVE ORDER MATERIAL]
2314-2399	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]

Exhibit	Description
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]
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]

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

I. Introduction

The '809 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.

Patent Owner Orca was co-founded in 2019 by Avi Shua, the sole inventor of the '809 Patent, to address shortcomings in preexisting security solutions for dynamic cloud environments. Ex.2074 (Declaration of Avi Shua, "Shua") ¶¶2-9. Mr. Shua secured his innovation in the claims of the '809 Patent, and unveiled the claimed inventions to the world in Orca's agentless SideScanning™ technology. *Id.* ¶¶9-13.

Orca's SideScanning technology defied skeptics and has been heralded in the industry as a "***genuinely genius innovation***" (Ex.2076, 7), 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 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. 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 securing 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.") (original emphasis).

REDACTED

¹ Exhibits 2400-2422 and 2425-2428 are Wiz's confidential documents produced pursuant to Paper 28.

REDACTED

As detailed below, Wiz's hindsight-driven obviousness combinations do not show that any challenged claim is unpatentable. 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. Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017). In the end, Wiz does nothing more than attempt, 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 was, independently, known in the prior art."); *see also id.* at 418-19 ("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* Sections IV.C.2, IV.C.6.

II. The '809 Patent Improved Cloud Security Systems

A. Problems with the Prior Art

The '809 Patent explains that as organizations “increasingly adapted their applications to be run from multiple cloud computing platforms,” security solutions struggled to adapt. '809 Patent (Ex.1001), 1:20-46. 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 various problems discussed in more detail in Section IV.C.1 below. *Id.* 1:49-2:14; *see also* Kaeli (Ex.2073) ¶¶35-41, 168-175.

B. The '809 Patent's Innovative Cloud Security Systems

The '809 Patent's inventions solved the problems faced by preexisting security systems. '809 Patent, 2:18-19. In particular, the problems discussed above motivated Mr. Shua to found Orca and develop agentless side scanning technology (SideScanning™) and the inventions disclosed and claimed in the '809 Patent (Shua¶¶2-9)—cloud security systems and methods that, among other things, “determine” and “access” using “an API or service provided by the cloud computing environment” a “snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment,” “analyze the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications” to determine “potential cyber vulnerabilities,” and use network locations of the

virtual cloud asset to determine risk and report vulnerabilities as “alerts prioritized according to the determined risk.” *See* ’809 Patent, cls. 1, 16, 19.

These inventions neither use nor suffer from the problems that plagued traffic inspection, traffic monitoring, and intrusive agent-based solutions, and the industry considered them “genuinely genius.” Ex.2076, 7. In fact, Orca’s inventions launched “the first version of agentless side scanning” that “leverage cloud APIs to snapshot underlying instance hard disks” that was recognized as “unique,” “like magic,” and “a big leap in cloud security,” including, as explained more below in Section IV.C.4, including with respect to specific claimed features in the ’809 Patent. *See, e.g.*, Ex.2076, 11-12, 31.

REDACTED

REDACTED

; *see also* Sections IV.C.1, IV.C.4;

Kaeli¶¶176-186.

III. Claim Construction

Wiz’s prior art fails to render obvious the challenged claims under any reasonable construction. Pet.10-11; *see* Kaeli¶¶42-47. Nevertheless, Wiz’s

interpretation of the “analyzing the snapshot” term should be rejected, for reasons discussed below.

A. “Analyzing the Snapshot”

Wiz argues that limitations in independent claims 1, 16, and 19 reciting “[analyze/analyzing] ...’ encompass[es] both [1] direct analysis of the snapshot data and [2] analysis of a VM instantiated from the snapshot.” Pet.11. Wiz is wrong as to [2].

Wiz does not dispute that the “ordinary and customary meaning of [analyzing a snapshot] encompasses direct analysis of the snapshot data (e.g., analyzing the snapshot as a data file without instantiating an assessment VM).” Pet.10. Wiz’s contention that “analyzing[] [a] snapshot” should also “encompass[] ... analysis of a VM instantiated from a snapshot” is based only on improper characterizations of Orca’s District Court complaint. *Id.* (citing Ex.1006, 23, 57-58). Orca’s allegations do not state or otherwise indicate that analyzing a VM instantiated from a snapshot is “analyzing [a] snapshot” as claimed. *See* Ex.1006, 23, 57-58. And POSAs would understand that limitations reciting “analyzing the snapshot” mean what they say and require analyzing snapshots (and snapshot data), not duplicate VMs instantiated from snapshots. Kaeli¶¶45-46.

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 ’809 Patent’s claims and specification. ’809 Patent, cls. 1, 16, 19 (separately reciting a “snapshot of the at least one virtual disk” and “a protected virtual cloud asset”), 4:60-61 (“A VM’s snapshot is a copy of the machine’s virtual disk (or disk file) at a given point in time.”); Kaeli ¶¶45-46 (“[A]n instantiated VM is not a snapshot.”). The specification also distinguishes analyzing a snapshot by a “security system 140 to detect vulnerabilities” (’809 Patent, 5:20-21), 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.* 5:55-67). *See also id.* 7:42-52.

Tellingly, Wiz’s expert, Dr. Stavrou, never supported and has now directly contradicted Wiz’s interpretation; he states only that he “*assume[d]* that ‘[analyze/analyzing] the 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 ¶82; Ex.2077 (“1st 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; *see also* Ex.2172 (“2nd Stavrou Tr.”) 38:7-20, 39:14-40:1. Dr. Stavrou appears to have adopted this construction in an attempt to expand his obviousness arguments based on inapposite disclosures in Veselov discussing analyzing duplicate VMs. But 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.” 1st Stavrou Tr.280:8-281:1; 2nd Stavrou Tr.12:5-12 (agreeing prior testimony regarding Veselov applies equally to the ’809 Patent). Wiz’s attempt to broaden the claims in an improper attempt to capture the prior art should be rejected. Kaeli ¶¶46-47.

IV. Challenged Claims 1-10 and 12-23 Are Nonobvious Over Veselov and Mohanty (Ground 1)

Wiz fails to show that claims 1-10 and 12-23 would have been obvious over Veselov and Mohanty for the reasons discussed below, including an unusual amount of objective indicia of non-obviousness that refutes Wiz’s hindsight-driven combination and improper piecemeal analysis. *See* Section IV.C; *Metalcraft*, 848 F.3d at 1367; *In re NTP*, 654 F.3d 1279, 1299 (Fed. Cir. 2011); *WBIP*, 829 F.3d at 1328.

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

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 ¶¶48-58; *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 '809 Patent. Kaeli¶¶48-58 (Veselov Overview); Shua¶¶152-159. The Petition disregards all such distinctions, improperly lumping all of Veselov's disclosures together and using the '809 Patent as a roadmap to select from among Veselov's myriad and disparate techniques. Yet, none of Veselov's embodiments teach correlating cyber vulnerabilities with a network location, determining risk, or reporting cyber vulnerabilities as alerts prioritized according to a determined risk. Kaeli¶¶48-58.

2. Overview of Mohanty

Mohanty disparages security techniques providing vulnerability assessments of network systems in the past, such as snapshot-based systems in Veselov, as those may become “obsolete within hours or minutes.” *Id.* 1:5-22; Kaeli¶¶59-62. Instead,

Mohanty encourages a “strong and continuous prioritization system to track critical vulnerabilities and take actions as changes occur.” Mohanty 1:17-22. Consistent with its goal of a “continuous prioritization system,” Mohanty relies on vulnerability assessment products that “perform vulnerability checks (i.e., scans) **on** the virtual machines,” i.e., agent-based systems such as from “QUALYS and RAPID7.” Mohanty, 1:11-14, 4:59-62, 6:54-58, Fig. 2; Kaeli¶¶60-62; Exs.2173-2174; Ex.2172, 239:3-240:9 (Stavrou “didn’t look at” whether Mohanty uses agent-based approaches); Shua¶¶160-161.

Mohanty uses the outputs of these agent-based VA products in a “three dimensional” algorithm that correlates vulnerabilities detected in real-time using agents with “contextual information such as threat data and virtualization tags.” Mohanty, 3:43-49. Unlike the claims of the ’809 Patent, Mohanty does not disclose or suggest snapshot-based analyses or facilitating those analyses using an API or service provided by the cloud computing environment.

3. Wiz’s Motivations To Combine Veselov and Mohanty Should Be Rejected

The Board’s ID preliminarily found the Petition had “sufficient reasoning” for combining Veselov and Mohanty “to improve security analysis by presenting more accurate measures of risk, thus facilitating rapid identification of more critical security problems.” ID 15. The Board also preliminarily found that Wiz present[ed] “sufficient arguments and evidence” that a POSA would have had “a reasonable

expectation of success in” combining Veselov and Mohanty. *Id.* 17. On these issues, however, Wiz’s contentions fail on the facts and the law for the following six reasons. Kaeli¶¶67-105.

First, Wiz’s arguments why a POSA would be motivated to, and reasonably expect success, in combining Veselov and Mohanty to arrive at the claims is foundationally based on the argument that Veselov’s and Mohanty’s security assessment techniques “consider[] the same types of data.” Pet.22-23. But even if it were true that the security analyses described in Veselov and Mohanty resulted in similar “types of data” for VMs, that suggests at best the two references are analogous art, not that a POSA would have been motivated to combine them. *Johns Manville Corp. v. Knauf Insulation, Inc.*, IPR2018-00827, Paper 9 at 10 (P.T.A.B. Oct. 16, 2018) (informative).

But it is not true that Mohanty’s agent-based assessments and Veselov agentless snapshot-based assessments detect the same “types of data.” Kaeli¶¶88-92. Before Orca’s inventions—and for years afterwards—the industry believed agentless scanning using “snapshots” for security assessments were “lightweight” and could only deliver “rudimentary security capabilities.” Ex.2106, 1-2. Those in the industry believed only agent-based security analyses, like those proposed in Mohanty, could provide detailed monitoring and protection. *Id.* It was only after Orca introduced its patent-practicing SideScanning™ in 2019 (*see* Section IV.E.2),

that the industry recognized the deep security assessment possible by analyzing snapshots located using cloud computing APIs. Kaeli ¶¶168-186; Ex.2076, 7 (explaining it was “difficult ... for older providers to come to terms with the success of agentless scanning”), 31 (Orca “made a big leap in cloud security with the introduction of its patented agentless SideScanning Technique in 2019.”); *see* Section IV.C.3 (Orca overcame skepticism).

Veselov itself reflects the pre-Orca understanding that agent-based approaches provided more detailed security analyses than agentless approaches. Veselov taught two distinct embodiments that begin with snapshots, (1) a “security agent” based assessment, where an agent is installed “into” a duplicate VM instantiated from a snapshot (*e.g.*, Veselov, Figs. 3A/3B, 14:22-25, 15:31-33, 16:45-52, 21:3-8, 21:57-60), and (2) analyzing a snapshot as a “data file” without an instantiated VM and without agents (*e.g.*, *id.* Figs. 5A/5B, 16:59-17:8). Kaeli ¶¶72-87; *see* 2nd Stavrou Tr.49:11-20; Ex.1002 ¶89. In Veselov’s “security agent” based assessment described in Figures 3A-3B, the agent can “apply tasks of the security assessment to real-time dynamic and static data, network connections, communications to computing resources, and other computational activities of the assessment virtual machine 312A-B.” Veselov, 15:41-47, 15:60-16:14; *see also id.* 15:29-38 (“install the security agent program 330 in the assessment virtual machine’s 312A, B”), 14:22-36 (similar), 21:3-8 (similar). As explained in Section

III.A above, Veselov's agent-based analysis of instantiated VMs cannot satisfy the claimed "analyzing a snapshot."

In contrast, Veselov also teaches determining comparatively basic information when analyzing a snapshot as a data file, such as "to identify files, software packages, application versions, and the like, for software installed on the target virtual machine 312." Veselov, 18:34-38. Veselov does not teach that analyzing a snapshot itself would permit any analysis of "dynamic" data, "network connections" or "communications to computing resources," or any of the other information available in Veselov's agent-based VM analyses. *See id.*; Section III.A (Claim Construction); Kaeli ¶¶72-92.² Accordingly, the foundational aspects of Wiz's purported motivation to combine—i.e., that agent-based and snapshot-based assessments detect the same data—is wrong. Wiz's obviousness argument should be rejected because it does not address the "fundamental differences in [scanning] techniques" between Veselov and Mohanty or to "reconcile these differences" in its obviousness combination. *Adidas AG v. Nike, Inc.*, 963 F.3d 1355, 1359–60 (Fed. Cir. 2020) (affirming Board's nonobviousness determination).

² Wiz's cited background references indicate a difference between live VM analyses and agentless analyses too. *See* Ex.1038, 134; Ex.1043; Kaeli ¶¶88-89.

Second, Wiz ignores that Mohanty disparages vulnerability assessments that are based on reports of a system “provided in the past” because such systems “become[] obsolete within hours or minutes as virtual machines or workloads change positions within a virtualized environment.” Mohanty, 1:14-17, 2:13-35, 6:45-63; *see also, e.g., id.*, 1:19-22 (explaining that a “security operations team needs a strong and continuous prioritization system to track critical vulnerabilities and take actions as changes occur”), 3:3-8 (explaining how disclosed system should “rapidly updat[e]” prioritization scores); Kaeli¶¶59-62, 81-87, 97-98. These teachings in Mohanty would have led a POSA away from implementing Veselov’s security assessment techniques, which only discloses security assessments premised on “snapshots,” wherein snapshots contain data at a point in time in the past. Kaeli¶¶81-87, 97-98; Veselov, 3:25-26 (referring to a “snapshot” as “a state of the resource at a point in time”), 6:50 (“snapshot data ... may be point-in-time consistent”), 9:38 (same).

Third, Wiz argues that a POSA would have been motivated to apply Mohanty’s teachings to Veselov to “provide more accurate risk assessments,” e.g., so that “risk may be assessed more effectively by considering multiple factors such as the asset’s threats/vulnerabilities, network location, data, and importance.” Pet.23. But, Wiz’s Petition fails to explain *how* such a combination would have worked, such as how a POSA would have implemented Veselov’s snapshot analysis

embodiments such that it also gathered information about an asset's "threats/vulnerabilities" or "network location, data, and importance." *Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017). For example, unlike Mohanty's security assessment designed to have direct interaction with the machine being assessed and allowing real-time vulnerability detection, Veselov taught an entirely different approach where the security analysis is performed without interacting with the target VM using data in the past. *See* Veselov, 3:20-23; Mohanty, 6:54-58; Kaeli ¶¶81-87, 97-105. A POSA would not be motivated to modify Veselov to nevertheless interact with the VM as taught in Mohanty because that would require processing time and power from the target VM, which is contrary to Veselov's objective to "avoid[] consuming processing time, processing power, and storage space of the target computing resource." Veselov, Abstract, 12:21-43, 2:54-63, 17:9-12; Kaeli ¶¶81-87, 97-105, 48-58.

A POSA similarly would not have been motivated to add the complex multi-factor monitoring and assessment system of Mohanty to Veselov because Veselov counsels against it. Veselov, 2:42-46 (describing "complexity of installation and monitoring" of an assessment system as a problem of other systems); Mohanty, 3:43-67 (describing three factor algorithm); Kaeli ¶¶48-58, 81-97. Wiz's combination would thus run "contrary to one of [Veselov's] stated purposes," counseling against such a combination if not teaching away from it expressly. *Polaris Indus., Inc. v.*

Arctic Cat, Inc., 882 F.3d 1056, 1069 (Fed. Cir. 2018) (vacating obviousness finding where obviousness analysis did not consider “statements regarding preferences” of the prior art).

Fourth, Wiz contends that “a POSA would have been motivated to obtain known benefits of prioritization” and that it was “well known that prioritizing vulnerabilities/alerts facilitated rapid identification of more critical security problems and assets.” Pet.23-24. Wiz’s position is premised on its contention that “snapshot-based assessments ... typically address security issues of varying importance,” but that contention is not supported by the evidence it cites. *Id.* (citing portions of Exs.1025, 1044, 1046). The cited exhibits do not discuss “snapshot-based” assessments or that such assessments could provide information necessary for prioritization of vulnerabilities. Kaeli¶¶98-105; Ex.1025, 32 (discussing “Incident Prioritization” as part of an “incident handling process”), 36 (separately identifying snapshots as part of “Evidence Gathering” and only for “identifying the problem and its source”); Ex.1044, 6:9-18 (discussing “Classification of Assets”), 3:38-42 (identifying vulnerabilities using agents that “**run on** one or more of the computing systems 104” running the VMs), Fig. 1; Ex.1046, 11:52-12:14 (discussing prioritization of “exploits found in software in [a] sandbox environment”). And contrary to Wiz’s hindsight-based assertions, those in the industry even after the priority date of the ’809 Patent viewed snapshot-based

assessments as providing only “rudimentary security capabilities.” Ex.2106, 1-2. Kaeli¶¶90-91. Wiz also fails to address or explain why a POSA would have sought to prioritize or “alert” on Veselov’s assessment based on information gathered in the past, considering Mohanty taught that such information would be quickly rendered “obsolete.” Mohanty, 1:14-17, 1:17-22 (“in virtualized environments ... vulnerabilities are constantly changing”).

Fifth, Wiz asserts “applying Mohanty’s prioritization techniques would similarly benefit snapshot-based assessments.” Pet.24. That argument, however, addresses only whether Mohanty and Veselov “would have allowed for” a combination or that they “could be combined,” which is “not enough.” *Personal Web*, 848 F.3d at 993 (emphases omitted). Indeed, while proof of physical or bodily incorporation of one reference into the other is not required, a satisfactory explanation of “how the combination of the ... references [is] supposed to work” is necessary to support “a conclusion that a relevant skilled artisan would have been motivated to make the combination and reasonably expect success in doing so.” *Id.*, 994 (emphasis omitted). Here, a POSA would have understood from Mohanty that it detects cyber threats using agent-based scanners that can analyze the real-time running processes on a virtual machine. Kaeli¶¶86-87. Wiz does not explain how or why a POSA would have taken these disclosures and adapted them to fit Veselov’s snapshot-based scanning. Kaeli¶¶88-105. Indeed, such a combination

would not have a reasonable expectation of success because, as Dr. Stavrou admitted, “an agent can only be installed on a virtual machine” and “I don’t think that an agent can be installed on a snapshot.” 2nd Stavrou Tr.53:14-20. The Board should not have to use their “imagination to fill in the many gaps in the Petition’s reasoning as they have been identified above.” *Orthocision, Inc. v. PTL OPCO LLC*, IPR2023-00625, Paper 34 at 62 (Sept. 18, 2024); *see also TriVascular, Inc. v. Samuels*, 812 F.3d 1056 at 1068 (Fed. Cir. 2016).

Sixth, Wiz argues that “[a]rriving at the claims involved using known elements according to their known functions to achieve predictable results” (Pet.22), but even if this is true (which it is not), Wiz’s position does not warrant a finding of obviousness. Wiz leaves a fatal “gap between the[se] concept[s]] ... [allegedly] being well-known and the[ir] beneficial application” to Veselov. *Fanduel, Inc. v. Interactive Games LLC*, 966 F.3d 1334, 1344 (Fed. Cir. 2020) (affirming Board rejection of obviousness challenge). None of the dozen or more references Wiz cites address whether a POSA would have reasonably expected security analyses of running VMs, as in Mohanty, to be applicable to systems utilizing a snapshot-based analysis, as in Veselov. *See* Pet.22; Kaeli¶¶93-96 (explaining inapplicability of references). And, Wiz’s retreat to over a dozen “background” references does not satisfy Wiz’s burden to identify “with particularity” the information it is relying on (35 U.S.C. § 312(a)(3)) and instead evidences Wiz’s improper, hindsight-based use

of the challenged claims “as a guide through [a] maze of prior art references.” *NTP*, 654 F.3d at 1299.

Seventh, with respect to reasonable expectation of success, Wiz contends that, “alert prioritization” was “well known and routinely implemented.” Pet.24-25. But even if that were true generally, Wiz’s burden here is to show “a reasonable expectation of achieving *what is claimed in the patent-at-issue*.” *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016). Wiz has failed to do so here. Wiz does not show that determining the network location of a virtual cloud asset was routine or well known in security systems that analyze *snapshots* in a cloud computing environment-based system, as opposed to security systems that utilize agents to perform security assessments. Kaeli ¶¶100-105. Nor would a POSA have understood such systems to be mutually applicable to the other. For example, an “agent” installed on a virtual cloud asset itself allows the network location of the asset to be determined based on the location of the agent. Those teachings are not applicable to a snapshot-based system. To the contrary, a POSA would have been led away from relying on the “network location” for any vulnerability correlation in a snapshot of a cloud-based virtual cloud asset in Veselov, as Veselov indicates that the target device undergoing an assessment may have a “network address[]” and “physical computing device[]” that “changes over time.” Veselov, 2:67-3:5; Kaeli ¶¶81-105.

In sum, Wiz's assertions under Ground 1 are improperly "focused on what a skilled artisan would have been able to do, rather than what a skilled artisan would have been motivated to do at the time of the invention." *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1068–69 (Fed. Cir. 2018). Wiz's hindsight based motivation to combine is also refuted by objective evidence discussed in Section IV.C below.

B. Veselov and Mohanty Fail to Disclose or Suggest Multiple Limitations in the Challenged Claims

Even if the Board were to accept Wiz's Veselov/Mohanty combination, that combination fails to disclose or suggest multiple limitations of the challenged claims discussed below. Kaeli ¶¶106-141.

1. The Veselov/Mohanty Combination Does Not Render Obvious Correlating Determined Cyber Vulnerabilities With a Network Location

Wiz fails to show how its combination of Veselov and Mohanty renders obvious limitations 1.5, 16.5, and 19.5 which recite "[correlating/correlate] the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset," and related limitations 1.6-1.7, 16.6-16.7, and 19.6-19.7 that recite "[using/use] the determined plurality of potential cyber vulnerabilities and the network location of the protected virtual cloud asset to determine a risk of the protected virtual cloud asset to the cloud computing environment" and

“[prioritizing/prioritize], by the determined risk, the plurality of potential cyber vulnerabilities.” Kaeli ¶¶107-112.

Wiz tacitly concedes that Veselov does not correlate cyber vulnerabilities with a network location of the protected virtual cloud asset. *See* Pet.39. Instead, Wiz asserts that Veselov explains its snapshots may include the “configurations of network protocols and services” or “properties of connections to other computing resources.” *Id.* Wiz fails to note, however, that Veselov indicates these “properties” are only included where “relevant to the security assessment.” Veselov, 9:55-58. And the only security assessments Veselov teaches where network protocols or connections to other computing resources are relevant are in the context of agent-based duplicate-VM assessments in its Figures 3A/3B embodiments. Veselov, 15:41-16:14, 21:3-23; Kaeli ¶¶107-108. In those duplicate-VM assessment embodiments, the configurations and connections are used to replicate the original machine including intercepting traffic. Veselov, 15:60-16:14; Kaeli ¶¶48-58, 107-108. Those embodiments, however, teach away from the challenged claims because analyzing a duplicate VM instantiated from a snapshot does not disclose or render obvious the claimed “analyz[e/ing] a snapshot.” *See* Section III.A; Kaeli ¶¶72-80.

In contrast, Veselov's Figures 5A/5B embodiments include analyzing a snapshot as a data file, but Veselov does not disclose using, analyzing, or determining network protocols and services or connections to other computing

resources. Kaeli ¶¶107-108; *see* Veselov, 16:56-18:56, Figs. 5A, 5B, 6. Indeed, Wiz does not cite to or rely on Veselov's snapshot analysis embodiments as disclosing limitations 1.5-1.7 or the corresponding limitations of claims 16 and 19. *See* Pet.38-42. In addition to Veselov failing itself to teach that analyzing a snapshot would include determining network location, that also would not have been obvious prior to the '809 Patent. As described in Section IV.A.3 above, those in the industry believed snapshot-based analyses only provided lightweight and "rudimentary" information in comparison with agent-based approaches. *See* Section IV.A.3; Kaeli ¶¶108-111; Ex.2106, 1-2.

To bridge the gap from Veselov to the challenged claim limitations, Wiz contends that Mohanty teaches "correlating the determined vulnerabilities with a network location of the protected virtual cloud asset." Pet.39. But, Wiz does not explain how the combination "was supposed to work."³ *Personal Web*, 848 F.3d at 993-94. It is "not enough," as Wiz does in the Petition, to say "no more than that a skilled artisan, once presented with the two references, would have understood that they could be combined." *Id.* For example, Wiz purports to rely on Mohanty's

³ Additionally, Wiz contends that it relies on Czarny for its discussion of an "asset-level risk" with no explanation as to how an "asset-level risk" is sufficient to address the claimed "risk of the ... asset to the cloud computing environment." Pet.65-68.

“workload context” that includes network location “tags” correlated with vulnerabilities determined from agent-based vulnerability assessment tools. Pet.40-41 (citing Ex.1075, 5:16-58, 8:19-59) (“tags 202 represent the ‘workload context,’ including the asset’s network location”). Wiz does not explain, however, how in the combination a POSA would have the same “workload context” in Veselov’s system. Wiz’s expert admitted, for example, that he did not offer any opinions that context “tags” would be applicable to a system based on analyzing a snapshot of a virtual cloud asset, as in Veselov, or that such a snapshot would include any of the tags that are discussed in Mohanty. 2nd Stavrou Tr.241:16-242:10 (“I’m not claiming either that it does or it doesn’t, because I don’t know what the snapshot data would look like.”). Wiz has therefore failed to provide “a clear, evidence-supported account of the contemplated workings of the combination,” and thus the Board should find Wiz failed to show that its combination renders obvious limitations 1.5-1.7, 16.5-16.7, or 19.5-19.7. *Personal Web*, 848 F.3d at 994; Kaeli ¶¶107-120.

2. The Veselov/Mohanty Combination Does Not Render Obvious Reporting Vulnerabilities As Alerts Prioritized By Determined Risk

Wiz fails to show that its proposed combination renders obvious limitations 1.8, 16.8, and 19.8 that require “[report/reporting] the determined plurality of potential cyber vulnerabilities as alerts prioritized according to the determined risk.” Kaeli ¶¶121-131.

Initially, Wiz incorrectly conflates Veselov's reporting "assessment results" and reporting determined cyber vulnerabilities "as alerts." Pet.43. Merely reporting results does not constitute reporting determined vulnerabilities "as alerts," as claimed. Kaeli¶¶122-125. As Wiz admitted in the parties' related district court litigation, and Dr. Stavrou likewise repeatedly conceded, the "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; 1st Stavrou Tr.284:18-285:6, 286:9-287:21 (testifying "alerts are different than reports" and agreeing "it's not enough to just report, you have to report as alerts"). Instead, Dr. Stavrou explained that reporting results is a "more generic term" and does not constitute reporting vulnerabilities "as alerts," which is something that "potentially makes it stand out" as claimed. *Id.*, 287:4-12.

Veselov does not include any teaching of making any potential cyber vulnerabilities "stand out." Kaeli¶¶122-125. Nor would a POSA expect Veselov's "results" to amount to "alerts" in view of the finite universe of findings, based on snapshot data provided in the past, generated from Veselov's "rules of the assessment" that a user specifies in advance. *See* Veselov, 10:18-24, 2:42-46, 7:15-16, 14:66-15:23; Kaeli¶¶122-126. Indeed, Wiz does not contend Veselov teaches "prioritization" of alerts. *See* Pet.43-44.

Wiz next contends that Mohanty “further teaches reporting the vulnerabilities as alerts ‘prioritized according to the determined risk’” in “several ways.” Pet.43. But Wiz’s assertions merely refer to what Mohanty discloses alone, without providing any explanation how a POSA would have applied Mohanty’s teachings to Veselov in the combination. That is not enough: obviousness “cannot be predicated on the mere identification” of “individual components of claimed limitations” in the prior art. *Personal Web*, 848 F.3d at 991 (quoting *In re Kotzab*, 217 F.3d 1365, 1371 (Fed. Cir. 2000)). At bottom, Wiz’s recitation of how Veselov and Mohanty disclose parts of this limitation, at most, might demonstrate that a person of ordinary skill in the art could have combined the references’ disclosures, which does not support a conclusion of obviousness. *Id.* at 993. Similar to the deficient obviousness assertions in *Personal Web*, Wiz’s “reasoning seems to say no more than that a skilled artisan, once presented with the two references, would have understood that they could be combined.” *Id.* And there is good reason why a POSA would not have applied Mohanty’s “alerts” to Veselov. Mohanty bases its “alerts” on specific “prioritization scores” that are based on vulnerabilities detected *in real time* using an agent based approach. Mohanty, 1:19-22 (explaining need for “*continuous* prioritization system to track critical vulnerabilities and take actions *as changes occur*”), 6:54-58 (“a VA scanner by QUALYS or RAPID7, performs vulnerability checks (i.e., scans) *on* the virtual machines 318.”), 9:11-19 (“alert” is based on

“vulnerability data 210”); Kaeli ¶¶127-128. The opposite is true in Veselov. Veselov bases its assessments entirely on “snapshots” that provide data at a point in time, which Mohanty suggests would become “obsolete” within hours or minutes. Mohanty, 1:14-17. This would have suggested to a POSA that Veselov’s system should *not* issue “alerts” on the vulnerabilities it detects. Kaeli ¶¶122-128.

Objective evidence further refutes Wiz’s arguments based on hindsight that “[c]ommunicating scores/rankings was also a common way of reporting vulnerabilities as prioritized alerts according to [the cyber threat’s] determined risk” (Pet.44), because the evidence confirms prioritized alerts in the context of analyzing snapshots of a virtual disk, facilitated by a cloud computing environments API or services, to determine vulnerabilities garnered significant praise, and Wiz copied it. *See* Section IV.C; Kaeli ¶¶129-130.

3. The Veselov/Mohanty Combination Does Not Render Obvious Dependent Claims

For at least the reasons discussed with respect to the independent claims above, Wiz has not shown that any dependent claim is unpatentable. Furthermore, Wiz has failed to show that the additional requirements of the following dependent claims 15 and 22 would have been obvious.

a. Claims 15 and 22

Veselov is the only reference Wiz relies on for the additional requirements of dependent claims 15 and 22 (Pet.60-63), but Veselov neither teaches nor suggests

the additional requirements of “wherein determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the location of the virtual disk.” *See* Kaeli¶¶132-140.

Wiz concedes that Veselov only discloses computing environments that are implemented by a computing resource service provider (what Wiz contends is a “cloud computing environment”) in Figures 1 and 3A-B, but not in Figures 5A-B. Pet.60-61. In the admittedly non-cloud context of Figures 5A-B, however, Veselov explains that a snapshot of the virtual machine can be “obtain[ed].” Veselov, 18:18-21. Accordingly, a POSA would have understood that querying a cloud management console of the cloud computing environment for the location of a snapshot or the location of a virtual disk was neither necessary nor inherent. *See* Kaeli¶¶133-135. Nor would such a query be obvious in light of Veselov.

Wiz also concedes that Veselov does not disclose *any* embodiment where a cloud management console is queried to locate a “virtual disk.” Pet.62-64. Instead, Wiz contends this would have been obvious because certain embodiments teach that a “user” “can initiate the snapshot-analysis process” by “using the UI to identify the target VM.” Pet.62. But, “identifying the target VM” is not the same as, nor does it render obvious, querying the location of a virtual disk for at least two reasons. *See* Kaeli¶¶135-136, 139-140. First, a user identifying a target VM means that the user

already knows the location of the resource, and thus there is no reason to “query” for its location or the location of any of its components. *See* Kaeli ¶¶135-136, 139-140. Wiz contends that this was a “common feature” (Pet.63), but that at best only addresses whether a POSA “*could have*” modified Veselov to include such a step, while entirely failing to address how or why a POSA “*would have been motivated to make*” such a change. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (original emphases). Having failed to address any motivation in its Petition, Wiz’s obviousness argument fails.

Second, as Dr. Stavrou admitted at his deposition, “Virtual disks are different from virtual machines”—“[t]hey are definitely not synonymous.” 1st Stavrou Tr.97:13-98:10. And, as the ’809 Patent shows, VMs and virtual disks are typically in different locations. ’809 Patent, 3:55-63, Fig. 1B; Kaeli ¶¶136-140; 1st Stavrou Tr.92:4-93:19, 94:16-21. Thus, locating a VM does not necessarily or inherently specify the location of the virtual disk. *See* 1st 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”); Kaeli ¶¶136-140.

Wiz also argues, in the alternative, that Veselov locates a virtual disk because Veselov determines where a snapshot is, and “Veselov shows the snapshot and its associated virtual disk initially located in the same computing environment.” Pet.63. Wiz improperly relies exclusively on depictions in the figures to draw this

conclusion, without any supporting description in the text. Without such a description, Wiz's argument is essentially one of inherency, but Wiz does not (and cannot) show that a snapshot's location is "necessarily" stored in the same location as the virtual disk as required for inherency. *See Bettcher Indus., Inc. v. Bunzl USA, Inc.*, 661 F.3d 629, 639 (Fed. Cir. 2011). To the contrary, Veselov teaches in the context of Figure 1 that snapshots are located separately from any VM in an external "snapshot storage service." Veselov, 5:13-17, 6:43-49, 7:27-40; Kaeli ¶¶132-140. And in Figures 3A, 3B, 4, 5A, 5B, Veselov teaches that the volume image may be *provided to* a hypervisor or service that launches an assessment machine, or may be read by the hypervisor to launch the assessment machine. Veselov, 12:37-51; 18:16-21.

And even if Veselov's systems were *capable of* querying a "UI/API" to configure aspects of an "assessment target" (Pet.63), and that such a query *could* include requesting a virtual disk, Wiz does not make the required showing that a POSITA would have been motivated to query the location of the virtual disk itself. *See ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1363 (Fed. Cir. 2018) (holding claims not unpatentable because Petitioner failed that the prior art device, "even if capable of doing so, actually would [perform the claimed function], or why a person of ordinary skill in the art would have been motivated to use" the prior art device in the manner claimed).

And, locating virtual disks was important to the commercial success of Orca's patent-practicing SideScanning techniques because it enabled Orca to deploy its security components in the same location as the virtual disk, which was critical for performance. Ex.2133, 1; Ex.2082, 8:06-11:08 (video from A. Shua 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), 4 (describing performance benefits of determining location); Kaeli¶¶194-198; Shua¶¶19, 87 (discussing Exs.2082-2083).

REDACTED

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 (emphasis omitted). 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 (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257-58 (Fed. Cir. 2013)); *see also Medtronic, Inc. v. Teleflex Innovations S.à.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”).

Here, it is undisputed that the challenged claims were not anticipated by 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 demonstrate and confirm the non-obviousness of the ’809 Patent’s claimed combinations. Kaeli ¶¶166-167.

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 ¶¶84-94.

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.” ’809 Patent, 1:22-26; 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.” ’809 Patent, 1:39-46. Such technologies had computing advantages, but they were vulnerable to cyber threats. *Id.*; 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.” ’809 Patent, 1:47-2:17.

However, these methods suffered from multiple disadvantages, as Mr. Shua explained both in the ’809 Patent and at multiple conferences and videos prior to these IPR proceedings. Shua ¶¶85-89 (discussing ’809 Patent 1:47-2:17 and Exs.2082, 2083, 2099, 2100, 2133). “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. ’809 Patent, 1:52-55. With network

scanners deployed out of path, servers “may not respond” or “expose ... necessary data,” and network configuration- and credential-related issues can be problematic. *Id.*, 1:60-67. 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.” *Id.*, 2:1-9. And “[u]sing agents is a cumbersome solution for a number of reasons, including IT resource management, governance, and performance.” *Id.*, 2:10-17; Ex.2076, 11 (“Traditional agents struggle with complex deployment and maintenance.”). “For example, installing agents in a large data center may take months.” ’809 Patent, 2:16-17; Ex.2103, 2 (describing deployment and coverage problems with agents); 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 due to the tradeoff between performance and impact to the environment.”).

Accordingly, there was a long-felt, unmet need for a cloud security solution that could adequately address undetected vulnerabilities. ’809 Patent, 1:49-55, 1:60-67, 2:4-9, 2:18-19; Ex.2136, 2 (“Organizations continue to adopt cloud computing at a rapid pace,” but “traditional security tools are often not suited for the challenges of dynamic, virtual and distributed cloud environments.”), 3 (“Eighty-four percent [of respondents] say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.”); Ex.2137, 1 (“Although cloud

security has evolved over the years and is becoming more mature, the endless 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 the flaws in preexisting cloud security solutions motivated him to found Orca and develop Orca's SideScanning™, including as claimed in the '809 Patent (*see* Section IV.2 immediately below)—a “genuinely genius innovation” that redefined the industry. Ex.2076, 7-8, 11 (Orca's “agentless side scanning” “allowed deep visibility into cloud workloads without the need to install agents”) (original emphasis); *see also* Shua¶¶94-95, 14-25 (describing videos (Exs.2078-2087) and documentation (Exs.2066, 2067, 2090, 2092, 2093) regarding SideScanning development and operation); Ex.2103, 1; Ex.2104, 2; Ex.2148, 15; Kaeli¶¶168-175.

2. Orca's SideScanning™ Practices the '809 Patent

Orca's Cloud Security Platform, and in particular the SideScanning™ techniques that power the platform, have used the inventions in at least claims 1-8, 10, and 12-23 in the '809 Patent since 2019 when Orca first introduced Orca's Cloud Security Platform commercially. Shua¶¶13, 27; *see generally id.* ¶¶28-83; Kaeli¶¶167, 176-186, 214 (citing Ex.2074; Exs.2308-2309; Ex.2118, 1-5; Ex.2076, 7-12, 31;

REDACTED

Ex.2123; Ex.2120, 6-7; Ex.2119, 9-10; Ex.2103; Ex.2135, 2; Ex.2106,

1). For example, with respect to independent claims 1, 16, and 19, Orca's SideScanning:

- determines, REDACTED
location of a snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment ('809 Patent, cls. 1, 16, 19 (preambles and limitations 1.1, 16.1, 19.1)); *see* Shua¶¶31-36 (discussing Ex.2067, 5-6, 12, 15; Ex.2093, 7; Ex.2094; Ex.2095; Ex.2098; Ex.2150; Ex.2096; Ex.2097; Ex.2300, 1, 3-4; Exs.2301-2304; Ex.2067, 5, 8-9);
- accesses, REDACTED
the snapshot of the at least one virtual disk (limitations 1.2, 16.2, 19.2); *see* Shua¶¶37-40 (discussing Ex.2067, 5; Ex.2300, 5-6; Exs.2302-2303; Ex.2311, 3, 5);
- analyzes the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications, such as in a CVE database (limitations 1.3, 16.3, 19.3); *see* Shua¶¶41-43 (discussing Ex.2067, 3, 11; Ex.2300, 6, 10);

- determines, based on the matching, an existence of potential cyber vulnerabilities (e.g., CVEs) (limitations 1.4, 16.4, 19.4); *see* Shua¶¶44-46 (discussing Ex.2067, 11; Ex.2300, 6, 13);
- “shows what each vulnerability is [and] where it’s located” (limitations 1.5, 16.5, 19.5); *see* Shua¶¶47-48 (Ex.2300, 13; Ex.2067, 14-16; Ex.2093, 22);
- uses the determined plurality of potential cyber vulnerabilities and network location of the asset to “[d]etect [l]ateral [m]ovement [r]isk” (limitations 1.6, 16.6, 19.6); *see* Shua¶¶49-50 (Ex.2067, 14-16);
- “contextualizes” the “vulnerability data” and “scores it as” “High risk,” “Medium severity,” or “Low severity” (limitations 1.7, 16.7, 19.7); *see* Shua¶¶51-52 (Ex.2067, 16); and
- reports the determined potential cyber vulnerabilities as prioritized alerts according to the determined risk (limitations 1.8, 16.8, 19.8); *see* Shua¶¶53-55 (discussing Ex.2300, 9, 11, 14; Ex.2092, 20; Ex.2067, 16-17).

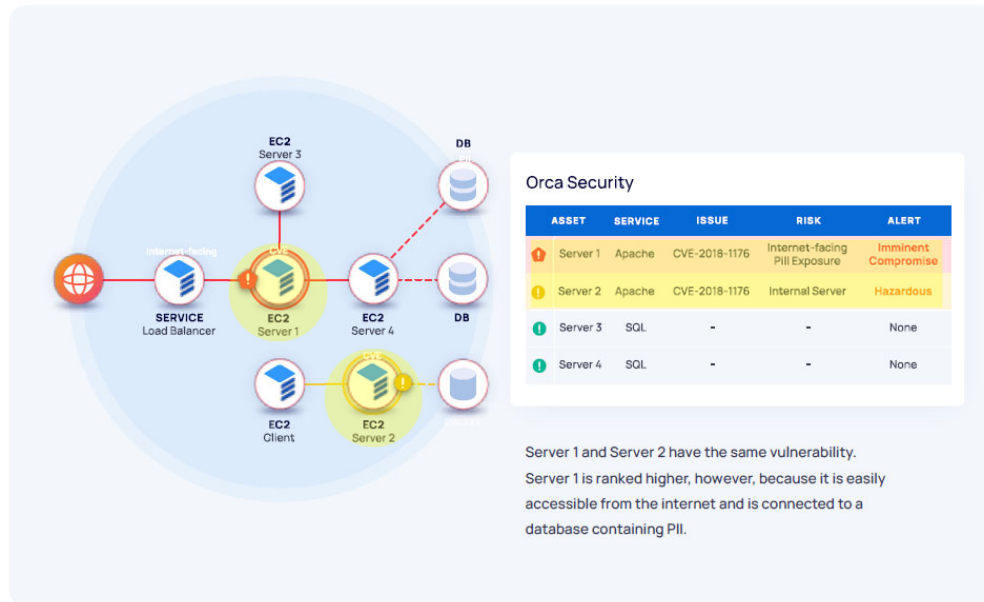


FIGURE 7: Orca combines asset and data characteristics with context information to prioritize risk and alerts in your environment.

Ex.2092 (SideScanning Technical Brief (2021)), 20.

Orca's SideScanning also practices dependent claims 2-8, 10, 12-15, 17-18, and 20-23. Shua¶¶56-83 (discussing Exs.2067, 2300, 2302-2304, 2311).

Orca's SideScanning™ solution was a “big leap in cloud security” because, using the above-discussed features, it “gather[ed] crucial data through the cloud provider's APIs, while scanning disk snapshots,”⁴ and “reconstructs file systems, scans operating systems, and applications ... for vulnerability assessments” and “allowed deep visibility into cloud workloads without the need to install agents.”⁵

Ex.2076, 11-12, 31.

REDACTED

⁴ See '809 Patent, limitations 1.1-1.2, 16.1-16.2, 19.1-19.2.

⁵ See '809 Patent, limitations 1.3-1.6, 16.3-16.6, 19.3-19.6.

REDACTED

see

also Kaeli¶¶182-187, 213-224; Shua¶¶93-94, 164 (discussing praise from others in, *e.g.*, Ex.2076, 31; Ex.2117, 1-2; Ex.2118, 5-7).

It is notable that, since its inception, Orca has attributed its success to its “patent pending” SideScanning™ techniques, which referred to the inventions claimed in the '809 Patent and related patents claiming priority to Orca's provisional patent application (No. 62/797,718). Shua¶¶16, 101; *see id.*¶¶17-23, 92, 101, 103, 111, 135, 139; Exs.2065-2067, 2080-2081, 2088, 2090, 2092-2093, 2107-2108, 2110, 2118,

REDACTED

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*,

⁶ *See* '809 Patent, limitations 1.7-1.8, 16.7-16.8, 19.7-19.8.

829 F.3d at 1335. And, if an invention achieves widespread industry acceptance, including after defying skeptics, that also evidences non-obviousness. *Allen Archery, Inc. v. Browning Mfg. Co.*, 819 F.2d 1087, 1092 (Fed. Cir. 1987).

Here, Orca's inventions defied skeptics and achieved widespread industry acceptance. Shua¶¶95-97; Ex.2076, 9, 11; Ex.2106, 1. REDACTED

This same skepticism was noted in the 2024 *Future of Cloud Security*, which remarked on “how difficult it was for older providers to come to terms with the success of agentless scanning” after Orca “[i]ntroduced 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 (Orca competitor publishing article “Agentless Solutions Fall Short” that claimed “side-scanning” only “delivers rudimentary security capabilities”); Kaeli¶¶176-181.

REDACTED

Section IV.C.3 (Orca's SideScanning™ practices the challenged claims); Kaeli¶¶182-187, 213-224. And, ultimately, SideScanning™ was widely accepted—"everyone needed it in order to stay competitive." Ex.2076, 7; Ex.2113, 4 (describing exemplary Orca customers); Shua¶¶98-100, 105, 112 (describing exemplary customers and commercial success); Kaeli¶¶175, 180-186, 239-241.

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 '809 Patent, Orca received numerous awards due to the inventions claimed in the '809 Patent. Shua¶¶137-149 (discussing awards in Exs.2076, 2118-2125, 2127-2132, 2144-2145); Kaeli¶¶176-186. 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.2123, 2 (award noting customer praised Orca’s “agentless approach” as “both a major innovation and a game changer”); *id.*, 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 ’809 Patent. Shua¶¶149-150.

REDACTED

REDACTED

-

REDACTED

For example, as noted, Orca's innovative SideScanning™ was recognized as “genuinely genius,” “unique,” “elegant,” “like magic,” and “a big leap in cloud security,” including with respect to specific features in the '809 Patent's claimed combinations, such as using cloud computing platform APIs to determine locations of virtual disks and virtual disk snapshots and to facilitate snapshot analyses. *See* 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 disk snapshots.”); Ex.2118, 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.”);

REDACTED

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 “may be evidence that the patented invention is nonobvious.” *Liqwd, Inc. v. L’Oreal USA, Inc.*, 941 F.3d 1133, 1137 (Fed. Cir. 2019). And “[e]vidence of access and substantial similarity *is* evidence of copying.” *Medtronic*, 70 F.4th at 1340 (original emphasis).

REDACTED

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 at Microsoft in May 2019. Shua ¶¶114-118 (describing meeting and related emails Exs. 2307-2308); Kaeli ¶¶187-238. REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

-

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

⁷ See limitations 1.1-1.2, 16.1-16.2, 19.1-19.2.

⁸ See limitations 1.3-1.6, 16.3-16.6, 19.3-19.6.

⁹ See limitations 1.3-1.6, 16.3-16.6, 19.3-19.6.

REDACTED

¹⁰ *See* limitations 1.7-1.8, 16.7-16.8, 19.7-19.8.

¹¹ *See* cls. 15, 22.

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

..

REDACTED

REDACTED

REDACTED

As the above-discussed evidence shows, Wiz accessed and copied Orca's technology practicing the '809 Patent claims, which strongly supports that the claimed inventions were non-obvious. *See Stratoflex*, 713 F.2d at 1541; *WBIP*, 829 F.3d at 1336; *Kaeli*¶182.

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

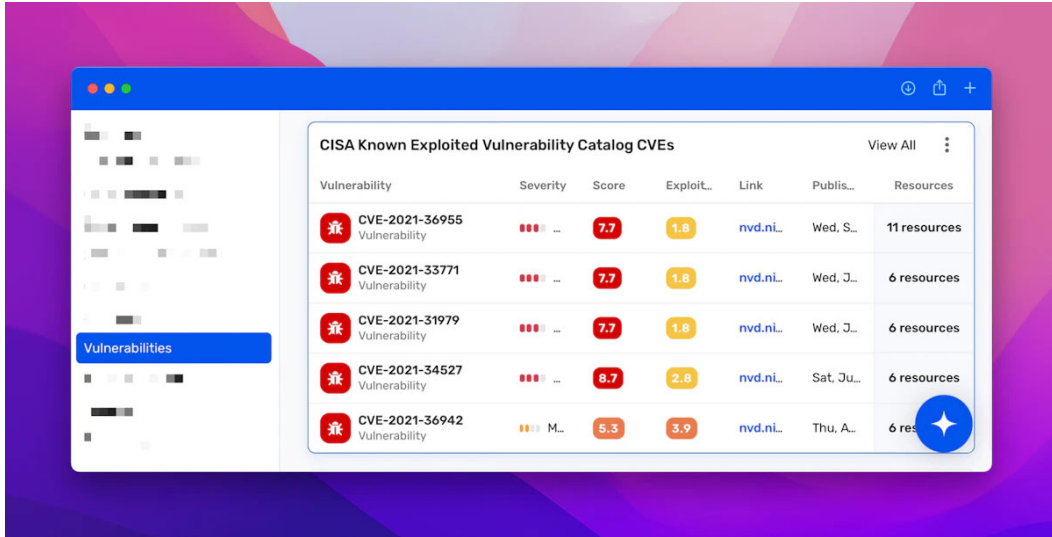
Wiz's copying of Orca's technology is further evidenced by Wiz's access to Orca's technology (discussed above), and the substantial similarity between Wiz's Cloud Security Platform and Orca's SideScanning™. *Medtronic*, 70 F.4th at 1340 ("Evidence of access and substantial similarity *is* evidence of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

Wiz's Cloud Security Platform uses what Wiz calls "workload scanning," which, like Orca's SideScanning™, practices the challenged claims. Kaeli¶¶187-238 (discussing Exs.2025-2026, 2074, 2115, 2158, 2308-2309, REDACTED). Wiz's "workload scanning":

- determines, REDACTED of a snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment (limitations 1.1, 16.1, 19.1); *see* Shua¶¶121-125 (discussing Ex.2308, 1-3; Ex.2309; Ex.2026, 1, 2-3, 7-8; Ex.2115, 1-2, 3); Kaeli¶¶226-231 (discussing Exs.2115, 2308-2309);
- accesses, REDACTED , the snapshot of the virtual disk (limitations 1.2, 16.2, 19.2); *see* Shua¶¶121-125 (discussing Ex.2308, 1-3; Ex.2309; Ex.2026, 1, 2-3, 7-8; Ex.2115, 1-2, 3); Kaeli¶¶226-231 (discussing Exs.2115, 2308-2309);
- analyzes the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications (limitations 1.3, 16.3, 19.3); *see* Shua¶¶123-127

(discussing Ex.2026, 2-3, 7-8; Ex.2115, 1-2, 3; Ex.2147, 2-3; Kaeli¶¶232-235 (discussing Exs.2115, 2147, 2165, 2178);

- determines, based on the matching, an existence of potential cyber vulnerabilities (e.g., CVEs) (limitations 1.4, 16.4, 19.4); *see* Shua¶¶126-127 (Ex.2147, 2; Kaeli¶¶232-235 (discussing Exs.2115, 2147, 2165, 2178);
- combines “external exposures and lateral movement paths” (limitations 1.5, 16.5, 19.5); *see* Shua¶¶128-132 (Ex.2147, 2-3; Ex.2177, 6-7, 10; Ex.2178, 1-2; Ex.2165, 8; Ex.2160, 2; Ex.2166, 2); Kaeli¶¶232-235 (Exs.2115, 2147, 2165, 2178);
- “performs a complete attack path analysis” (limitations 1.6, 16.6, 19.6); *see* Shua¶¶128-132 (Ex.2147, 2-3; Ex.2177, 6-7, 10; Ex.2178, 1-2; Ex.2165, 8; Ex.2160, 2; Ex.2166, 2); Kaeli¶¶236-238 (Ex.2165);
- “prioritize[es] critical risks” (limitations 1.7, 16.7, 19.7); *see* Shua¶¶126-132 (Ex.2147, 2-3; Ex.2177, 6-7, 10; Ex.2178, 1-2; Ex.2165, 8; Ex.2160, 2; Ex.2166, 2); Kaeli¶¶236-238 (Ex.2165); and
- reports the determined potential cyber vulnerabilities as prioritized alerts according to the determined risk (limitations 1.8, 16.8, 19.8); *see* Shua¶¶126, 129-130 (discussing Ex.2147, 2-3; Ex.2178, 1-2; Ex.2165, 8); Kaeli¶¶236-238 (discussing Ex.2165).



Ex.2147 (*Detect and Prioritize CISA Known Exploited Vulnerabilities in the Cloud with Wiz*), 2.

REDACTED

REDACTED

;

see also Shua¶114 (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¶220-224.

Wiz's copying of Orca's implementation of the inventions claimed in the '809 Patent plays the dual role of "praising" 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 demonstrated by Orca and Wiz's commercial success. *Polaris*, 882 F.3d at 1072.

After filing the provisional patent application that led to the '809 Patent in January 2019, and Orca introduced the claimed inventions in SideScanning later that year, Orca obtained a remarkable amount of investment. Shua¶¶98, 101-113 (discussing Exs.2065, 2108-2113, 2140 and explaining how funding was due to claimed inventions); Ex.2149, 24; Kaeli¶¶239-241. By June 2019, Orca raised \$6.5 million dollars in funding, with a direct nexus to the unique features of the challenged claims, including Orca's ability to read and analyze "virtual machine[s]" in the cloud and determine "[w]hich servers are vulnerable." Ex.2107, 2-3. One lead investor remarked about "Orca's unique approach and innovative solution" that provided "true, deep, and near instantaneous full stack visibility at a forensic level of detail." *Id.* 3.

In 2020, Orca raised another \$75 million in funding because of the claimed combination of elements in the '809 Patent. Shua¶¶107-110 (explaining Orca was able to get these investments "because of the novel aspects of SideScanning™ that are claimed in the '809 Patent"); Exs.2109-2110; Ex.2140, 2. For example, Orca "st[oo]d out" for "its ability to quickly provide workload-level visibility ... us[ing] low-level APIs that allow[ed] it to gain visibility into what exactly is running in [the]

cloud,” all “without slowing down engineering.” Ex.2109, 1-2 (“Orca ... offers security tools that scan for vulnerabilities.”). And, Orca was also known for its “SideScanning technology” that could “find potential security issues” without “introducing any additional overhead.” Ex.2111, 1-2. Orca explained at the time that the money it raised would “fuel Orca Security’s further disruption of the cloud security industry with touchless, workload-deep, context-aware security and compliance” that “helps to reduce thousands of security alerts to the critical few that matter, along with their precise path to remediation.” Ex.2110, 1; Ex.2111, 1 (“[Orca’s] SideScanning technology ... enables it to map a company’s cloud environment and reconstruct its file system by looking at how workloads interact with the block storage services they use.”).

In 2021, just two years after introducing the Orca Cloud Security Platform powered by its patented SideScanning technique embodied in the ’809 Patent—Orca’s only product—Orca raised additional investments of over \$550 million, marking Orca as the fastest cloud security company to reach a valuation over \$1 billion. Ex.2112, 1-2; Ex.2139, 1; Shua¶¶109-111. These funding announcements again demonstrated how Orca’s commercial success was attributable to the inventions claimed in the ’809 Patent. 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”), 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”), 3 (“Orca Security’s rapid emergence as a cloud security leader is driven by customer love for its product.”).

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. *See 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”).

Orca also earned significant revenues, REDACTED, from SideScanning™. Shua¶¶98-100 REDACTED; Ex.2312 REDACTED Ex.2067, 1, 3. REDACTED

Id.; *Chemours Co. FC, LLC v.*

¹² CWPP is an acronym for Cloud Workload Protection Platform.

Daikin Indus., Ltd., 4 F.4th 1370, 1378 (Fed. Cir. 2021) (“significant sales” are evidence of commercial success). Orca would have earned even more, but for Wiz copying Orca’s technology and forcing Orca to compete with it for customers. *See* Shua^{¶¶}114.

The commercial success of Wiz’s infringing Cloud Security Platform further demonstrates nonobviousness. *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.a; ^{REDACTED})—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; Ex.2141, 2; Ex.2142.¹³

¹³ Wiz’s public remarks about the use of cloud APIs in its infringing product being “new” when it was introduced in 2020-2021 also undercut its pre-2019 obviousness arguments. *See* Pet.30-31 (arguing it would have been “obvious” for security

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

V. Challenged Claims 1-10 and 12-23 Are Nonobvious Over Veselov, Mohanty, and Czarny (Ground 2)

Wiz fails to show that challenged claims 1-10 and 12-23 would have been obvious over the Ground 2 art, Veselov, Mohanty, and Czarny. Wiz relies on Czarny for its alleged disclosure of “determining and reporting a risk level for the asset as a whole to facilitate responsive action by security personnel,” which Wiz contends is relevant to limitations 1.8, 16.8 and 19.8. Pet.68-69. Wiz also relies on Czarny for dependent claims 6-7 and 17-18. Wiz does not rely on Czarny to address any of the failures in its motivations to combine Veselov and Mohanty discussed in Ground 1, and Ground 2 should be rejected for at least those same reasons. Furthermore, POSAs would not have been motivated to modify Wiz’s Veselov-Mohanty combination with teachings from Czarny. 2nd Stavrou Tr.32:7-11 (confirming that Dr. Stavrou was not aware of anyone who had ever looked at Veselov, Mohanty, and Czarny in combination together). As described above, Veselov and Mohanty

systems to use cloud APIs), 65; 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.”).

involve security assessments of virtual machines via analyses of snapshots or instantiated VMs (Veselov) or via agent-based monitoring (Mohanty). *See* Section IV.A. Czarny concerns assessments of electronic devices – *not* virtualized resources, and does not involve either snapshot analyses, instantiated VM analyses, or agent-based analyses of VMs, as in Veselov and Mohanty. Czarny (Ex.1084), Abstract, 1:39-56; *see also* Kaeli¶¶63 (Overview of Czarny); *id.*¶¶142-147 (explaining that POSAs would not combine Czarny's teachings with Veselov or Mohanty); Shua¶¶151, 162-164 (explaining how Czarny differs from the claimed inventions). Instead, Czarny relies on receiving "product binary data" and using that "binary data" for a security assessment. Neither Mohanty nor Veselov discuss any similar "binary data," and Wiz does not explain how or why a technique relying on such binary data was "supposed to work" in the combination. *Personal Web*, 848 F.3d at 994.

In particular, Wiz contends that it relies on Czarny for its discussion of an "asset-level risk," but Wiz does not how an "asset-level risk" is sufficient to address the claimed "risk of the ... asset to the cloud computing environment." Pet.65-68. Czarny's risk assessment is also in an unrelated context, attempting to determine whether target device should be granted or denied *access* to a secure environment based on the target device's "security vulnerability level." Czarny, 7:46-67; 2nd Stavrou Tr.244:11-245:1; *id.* 245:18-246:5 (agreeing that Czarny determines risk

before the asset becomes part of a distributed environment). Accordingly, Czarny is not related to determining a risk of a protected virtual cloud asset that is “instantiated *in*” a cloud computing environment, as in the challenged claims. *See* ’809 Patent, limitations 1.1, 16.1, 19.1; Kaeli¶¶148-149.

Wiz’s arguments for dependent claims 6-7 and 17-18 do not remedy the deficiencies described above with respect to independent claims 1 and 16, and claims 6-7 and 17-18 should be found not unpatentable for at least those reasons. Kaeli¶150.

VI. A POSA Would Not Have Combined Wiz’s Grounds 1 And 2 References (Grounds 3 and 4)

Wiz’s Grounds 3 and 4 challenge only claim 11 and purport to “build upon” Wiz’s Grounds 1 and 2, respectively, by adding Hutchins to the proposed combinations solely for its “teachings of quarantining VMs.” Pet.71. Wiz does not contend that Hutchins alone or in combination teaches any aspect of independent claim 1 from which claim 11 depends. Accordingly, if the Board finds that a POSA would not have been motivated to combine Wiz’s Grounds 1-2 art, or otherwise that claim 1 not unpatentable in Grounds 1 and 2, Wiz’s Grounds 3-4 should be rejected for the same reasons including in view of the unusual wealth of objective indicia supporting nonobviousness. Kaeli¶¶151-165.

Wiz’s Grounds 3-4 should be rejected for the additional reason that Wiz fails to explain why a POSA could have or would have looked to Hutchins for

remediation techniques in response to the detection of “potential cyber vulnerability[ies]” as required by claim 11. *See* '809 Patent, cl. 11; Kaeli¶¶153-156, 161-163. Indeed, Hutchins does not describe “vulnerabilities,” let alone recommending any remedial steps in response to detected vulnerabilities. Instead, Hutchins exclusively discusses quarantining a VM when a **virus** is detected, and viruses and potential cyber vulnerabilities are not the same. A virus is a significant cyber threat such as “[a] computer program that can copy itself and infect a computer without permission or knowledge of the user” and may “corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.” Ex.2175; Kaeli¶¶157-158. In contrast, a “vulnerability” is a “[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.” Ex.2176. As Wiz's own references indicate, “[v]ulnerability assessment” and virus or “malware detection” are different “fields or industries.” Czarny, 1:6-7. Kaeli¶¶157-158, 162-163.

Wiz's Grounds 3 and 4 fail because they do not explain why a POSA would have looked to virus scanning remediation steps (in Hutchins) for security analyses directed at detecting “vulnerabilities” as in Wiz's proposed combination. *See* Pet.71-74. A POSA would not have. As Wiz's Czarny reference explains, the typical response for “malware” requires “immediate response to eliminate a threat”

including “to quarantine.” Czarny, 1:8-12. But Czarny directly contradicts that “quarantining” is needed for detected “vulnerabilities,” explaining “[w]ith a positive vulnerability assessment, on the other hand, the computer device *can usually continue to operate without concern for a threat to the computer device*, since a malicious event is not necessarily imminent.” *Id.*, 1:12-15.

Wiz asserts that Hutchins describes a “similar snapshot-based security assessment” to Veselov. Pet.72. But Hutchins does not describe a similar snapshot-based security assessment *required by the challenged claims*. To the contrary, the “snapshot-based” approach described by Hutchins would have led a POSA *away* from the claimed invention because, in Hutchins, a snapshot is used to “create a new virtual machine” otherwise referred to as a “replicated virtual machine” that is then analyzed for viruses. Ex.1070, ¶¶17, 53; Kaeli¶¶155-156, 64-66; Shua¶¶165-167. For the reasons discussed in Section III, analyzing an executing virtual machine that is instantiated *from* a snapshot is not the same as “analyzing a snapshot” as required in is not analyzed. Wiz does not provide any basis for cherry picking only the portion of Hutchins describing quarantining a virtual machine, while ignoring the portions of the reference that would have directed a POSA away from the inventions of the challenged claims.

VII. Conclusion

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

Respectfully submitted,

Dated: May 9, 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 13,755 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 9th day of May, 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
jbaillargeon@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.