

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.

Case IPR2024-01190
Patent No. 11,740,926

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The '926 Patent Improved Cloud Security Systems	3
A.	Problems with the Prior Art	3
B.	The '926 Patent's Innovative Cloud Security Systems.....	4
III.	Claim Construction.....	5
A.	“Analyzing the Snapshot”	5
IV.	Ground 1 Fails: Claims 1, 5-10, and 12-15 Are Nonobvious Over Veselov And Mohanty	7
A.	Overview of Veselov (Ex.1007).....	7
B.	Overview of Mohanty (Ex.1075)	8
C.	Wiz's Conclusory And Generic Motivations To Combine Should Be Rejected	9
D.	Wiz Fails To Show The Ground 1 Art Teaches Multiple Claim Limitations.....	15
1.	Limitations 1.4, 14.4, 15.4	15
2.	Limitations 1.5-1.6, 14.5-14.6, 15.5-15.6	26
3.	Limitations 1.7, 14.7, 15.7	27
4.	Dependent Claim 13	30
E.	Objective Evidence Demonstrates and Confirms the Nonobviousness of the Challenged Claims.....	33
1.	The Claimed Inventions Solved a Long-felt, Unmet Need With A “Genuinely Genius Innovation”	34
2.	Orca's SideScanning™ Practices the '926 Patent	35

3.	The Claimed Inventions Defied the Skeptics, and Became Widely Accepted in the Industry	39
4.	The Industry Praised Orca’s Revolutionary Inventions.....	41
5.	Wiz Copied Orca’s Inventions.....	43
6.	Orca’s And Wiz’s Commercial Success Demonstrates Nonobviousness	58
F.	Ground 2 Fails: Claims 1-10 and 12-15 Would Not Have Been Obvious Over Veselov, Mohanty, and Ranum	62
1.	Wiz’s Ground 2 Art Does Not Render Obvious Dependent Claims 2 and 4	66
G.	Grounds 3-6 fail for at least the reasons as Grounds 1-2	68
V.	CONCLUSION.....	69

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

<i>Abbott Laboratories v. Sandoz, Inc.</i> , 544 F.3d 1341 (Fed. Cir. 2008)	69
<i>Adidas AG v. Nike, Inc.</i> , 963 F.3d 1355 (Fed. Cir. 2020)	12
<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)	34, 41, 42
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	31
<i>Bettcher Indus., Inc. v. Bunzl USA, Inc.</i> , 661 F.3d 629 (Fed. Cir. 2011)	32
<i>Brown & Williamson Tobacco Corp. v. Philip Morris Inc.</i> , 229 F.3d 1120 (Fed. Cir. 2000)	61
<i>Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.</i> , 381 F.3d 1371 (Fed. Cir. 2004)	20
<i>Chemours Co. FC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	60
<i>Cisco Sys. Inc. v. C-Cation Techs., LLC</i> , IPR2014-00454, Paper 12 (P.T.A.B. Aug. 29, 2014).....	21
<i>Cont'l Can Co. USA, Inc. v. Monsanto Co.</i> , 948 F.2d 1264 (Fed. Cir. 1991)	19
<i>In re NTP, Inc.</i> , 654 F.3d 1279 (Fed. Cir. 2011)	14
<i>In re Oelrich</i> , 666 F.2d 578 (C.C.P.A. 1981)	19, 21

<i>Intel Corp. v. PACT XPP Schweiz AG</i> , No. 2022-1038, 2023 WL 2198649 (Fed. Cir. Feb. 24, 2023).....	64
<i>InTouch Techs., Inc. v. VGO Commc'ns, Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014)	68
<i>Iron Grip Barbell Co. v. USA Sports, Inc.</i> , 392 F.3d 1317 (Fed. Cir. 2004)	44
<i>Johns Manville Corp. v. Knauf Insulation, Inc.</i> , IPR2018-00827, Paper 9 (P.T.A.B. Oct. 16, 2018).....	10, 65
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	3, 9
<i>Liqwd, Inc. v. L'Oreal USA, Inc.</i> , 941 F.3d 1133 (Fed. Cir. 2019)	43, 44
<i>Medtronic, Inc. v. Teleflex Innovations S.à.r.l.</i> , 70 F.4th 1331 (Fed. Cir. 2023)	33, 44, 55
<i>Metalcraft of Mayville, Inc. v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	3
<i>Orthocision, Inc. v. PTL OPCO LLC</i> , IPR2023-00625, Paper 34 (P.T.A.B. Sept. 18, 2024).....	14
<i>PAR Pharm., Inc. v. TWI Pharms., Inc.</i> , 773 F.3d 1186 (Fed. Cir. 2014), <i>aff'd</i> , 624 F. App'x 756 (Fed. Cir. 2015) (per curiam)	19, 20
<i>ParkerVision, Inc. v. Qualcomm Inc.</i> , 903 F.3d 1354 (Fed. Cir. 2018)	32
<i>Pentec, Inc. v. Graphic Controls Corp.</i> , 776 F.2d 309 (Fed. Cir. 1985)	60
<i>Personal Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	13, 22, 26, 62
<i>Plas-Pak Indus., Inc. v. Sulzer Mixpac AG</i> , 600 F. App'x. 755 (Fed. Cir. 2015)	67

<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	13, 14, 58
<i>Power-One v. Artesyn Techs., Inc.</i> , 599 F.3d 1343 (Fed. Cir. 2010)	61
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	3, 55, 58
<i>TQ Delta LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	64, 65
<i>Trivascular, Inc. v. Samuels</i> , 812 F.3d 1056 (Fed. Cir. 2016)	14
<i>Unigene Laboratories, Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	9
<i>Univ. of Strathclyde v. Clear-Vu Lighting LLC</i> , 17 F.4th 155 (Fed. Cir. 2021)	64
<i>WBIP, LLC v. Kohler Co.</i> , 829 F.3d 1317 (Fed. Cir. 2016)	<i>passim</i>

STATUTES

35 U.S.C. § 312(a)(3).....	14, 16, 21
----------------------------	------------

OTHER AUTHORITIES

Giles S. Rich, <i>The Extent of Protection and Interpretation of Claims - American Perspectives</i> , 21 Int'l Rev. Indus. Prop. & Copyright L. (1990)	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> ”)
2008-2009	RESERVED
2010	U.S. Pat. No. 9,467,465 B2 (“Hibbert”)

Exhibit	Description
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, <i>Characterizing Hypervisor Vulnerabilities</i> ”)
2023-2024	RESERVED

Exhibit	Description
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”)
2041-2042	RESERVED
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”)
2046	Appendix E, Invalidity of United States Patent 11,740,926 (the “’926 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)
2047	Appendix E-1, Invalidity of United States Patent 11,740,926 (the “’926 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)

Exhibit	Description
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	Declaration of Douglas E. Lumish Pursuant to 37 C.F.R. § 42.10(c)(2)
2050	Declaration of Steven W. Peters In Response to Petitioner’s First Objections to Evidence [<i>served, not filed</i>]
2051-2052	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/
2146-2147	RESERVED
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	Citizens JMP Cyber 66 Report (2024), https://7938840.fs1.hubspotusercontent-na1.net/hubfs/7938840/2024_CJMP_Cyber_66.pdf

Exhibit	Description
2153	Julie Bort, <i>Wiz Hopes to Hit \$1B in ARR in 2025 Before an IPO, after Turning Down Google's \$23B</i> (Oct. 23, 2024), https://techcrunch.com/2024/10/23/wiz-hopes-to-hit-1b-in-arr-in-2025-before-an-ipo-after-turning-down-googles-23b/
2154	Ofir Dor, <i>Wiz Launches New Cloud Data Security Technology</i> (Nov. 22, 2022), https://en.globes.co.il/en/article-wiz-launchesnew-cloud-data-security-technology-1001430578
2155	George Pisha, <i>Wiz Becomes the First CNAPP to Deliver Integrated Data Security Posture Management</i> (Nov. 21, 2022), https://www.wiz.io/blog/wiz-becomes-first-cnapp-to-deliverintegrated-data-security-posture-management
2156	Wiz Experts Team, <i>CSPM vs. DSPM: Why You Need Both</i> (May 12, 2024), https://www.wiz.io/academy/cspm-vs-dspm
2157	Wiz Experts Team, <i>Sensitive Data Discovery</i> (Oct. 31, 2024), https://www.wiz.io/academy/sensitive-data-discovery
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

Exhibit	Description
2163-2171	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
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/)
2175-2178	RESERVED
2179	Orca Security, <i>Sensitive Data Detection</i> (last visited May 5, 2025), https://orca.security/solutions/sensitive-data-detection/
2180	Avi Shua, <i>How Orca’s Cloud Security Solution Detects Weak Passwords</i> (Feb. 13, 2020), https://orca.security/resources/blog/how-orcas-cloud-security-solution-detects-weak-passwords/
2181	Orca Security, <i>Orca Cloud Security Platform: Comprehensive Cloud Security – In Minutes</i> (2023)
2182	Matika Lidgi & Nicolas Ehrman, <i>Automatically Discover and Secure Your APIs with Wiz Dynamic Scanner</i> (Dec. 21, 2022), https://www.wiz.io/blog/automatically-discover-and-secure-your-apis-with-wiz-dynamic-scanner
2183	U.S. Patent No. 11,663,031
2184	U.S. Patent No. 11,663,032
2185	U.S. Patent No. 11,693,685
2186	U.S. Patent No. 11,775,326
2187	U.S. Patent No. 11,726,809

Exhibit	Description
2188	<i>Vulnerabilities</i> , NIST Vulnerability Database (last visited May 8, 2025), https://nvd.nist.gov/vuln
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
2191	Ferda Özdemir Sönmez et al., <i>Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation</i> (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_WksJEsRdeg1KqYZ7qaqwHQ8.8yw
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]

Exhibit	Description
2304	<i>AWS Permissions</i> [PROTECTIVE ORDER MATERIAL]
2305	RESERVED
2306	REDACTED [PROTECTIVE ORDER MATERIAL]
2307	REDACTED [PROTECTIVE ORDER MATERIAL]
2308	REDACTED [PROTECTIVE ORDER MATERIAL]
2309	REDACTED [PROTECTIVE ORDER MATERIAL]
2310	RESERVED
2311	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]

Exhibit	Description
2403	REDACTED [PROTECTIVE ORDER MATERIAL]
2404	REDACTED [PROTECTIVE ORDER MATERIAL]
2405	REDACTED [PROTECTIVE ORDER MATERIAL]
2406	REDACTED [PROTECTIVE ORDER MATERIAL]
2407	REDACTED [PROTECTIVE ORDER MATERIAL]
2408	REDACTED PROTECTIVE ORDER MATERIAL]
2409	REDACTED [PROTECTIVE ORDER MATERIAL]
2410	REDACTED [PROTECTIVE ORDER MATERIAL]
2411	REDACTED [PROTECTIVE ORDER MATERIAL]
2412	REDACTED ROTECTIVE ORDER MATERIAL]
2413	REDACTED [PROTECTIVE ORDER MATERIAL]
2414	REDACTED [PROTECTIVE ORDER MATERIAL]
2415	REDACTED [PROTECTIVE ORDER MATERIAL]

Exhibit	Description
2416	REDACTED [PROTECTIVE ORDER MATERIAL]
2417	REDACTED [PROTECTIVE ORDER MATERIAL]
2418	REDACTED [PROTECTIVE ORDER MATERIAL]
2419	REDACTED [PROTECTIVE ORDER MATERIAL]
2420	REDACTED [PROTECTIVE ORDER MATERIAL]
2421	REDACTED [PROTECTIVE ORDER MATERIAL]
2422	REDACTED [PROTECTIVE ORDER MATERIAL]
2423	REDACTED [PROTECTIVE ORDER MATERIAL]
2424	REDACTED [PROTECTIVE ORDER MATERIAL]
2425	REDACTED [PROTECTIVE ORDER MATERIAL]
2426	REDACTED [PROTECTIVE ORDER MATERIAL]
2427	REDACTED [PROTECTIVE ORDER MATERIAL]
2428	REDACTED [PROTECTIVE ORDER MATERIAL]

I. Introduction

The challenged '926 Patent is a pioneering cybersecurity patent that Petitioner (“Wiz”) argues—wrongly—would have been obvious.

Patent Owner Orca was cofounded in 2019 by Avi Shua, the sole inventor of the '926 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 '926 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* §IV.E.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. And Orca has been repeatedly recognized as one of the world’s most innovative cloud security

companies. *See* §IV.E.4.

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 merely recites “well-known” techniques. 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).

REDACTED

¹ Exhibits 2400-2428 are Wiz’s confidential documents produced pursuant to Paper 26.

REDACTED

As detailed below, Wiz’s hindsight-driven obviousness combinations do not show 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, albeit unsuccessfully, to show individual elements 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); *see also id.* at 418-19 (“claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.”). And, 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™. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1541 (Fed. Cir. 1983); *see* §§IV.E.2, IVE.5.

II. The ’926 Patent Improved Cloud Security Systems

A. Problems with the Prior Art

The ’926 Patent explains that as organizations “increasingly adapted their applications to be run from multiple cloud computing platforms,” security solutions struggled to adapt. ’926 Patent (Ex.1001), 1:23-46. Preexisting cloud security systems used, for example, “traffic inspection,” “traffic monitor[ing],” and “agents installed in each server in a cloud computing platform.” *Id.* 1:47-2:17. But those

systems suffered from various problems discussed in more detail in Section IV.E.1 below. *Id.* 1:51-2:17; *see also* Kaeli (Ex.2073) ¶¶35-42, 203-209.

B. The '926 Patent's Innovative Cloud Security Systems

The '926 Patent's inventions solved the problems faced by preexisting security systems. *See* '926 Patent, 2:18-19. In particular, the challenged claims are directed to cloud security systems and methods that, among other things, “locat[e]” and “access[]” a “snapshot of at least one virtual disk of a protected virtual cloud asset” using cloud computing environment (like AWS or Azure) APIs or services, and analyze the snapshot to “determine the existence of a plurality of potential cyber threats, each cyber threat based on data stored on the virtual disk.” *Id.*, cls. 1, 14, 15.

The '926 Patent claims are specifically directed to disclosed embodiments where “the security system 140 is configured to detect cyber threats ***that do not represent vulnerabilities.***” '926 Patent, 6:21-23, 4:45-47 (snapshot based analyses can be used to detect “[1] vulnerabilities,” and separately “[2] ***other*** cyber threats related to execution VM 119”). These embodiments detecting non-vulnerability cyber threats based on data, like “personally identifiable information” and “weak passwords,” are expressly recited in limitations 1.4, 14.4 and 15.4 of the challenged claims. *Compare* '926 Patent, 6:21-32, *with id.* limitations 1.4, 14.4, 15.4.

The '926 Patent's inventions as embodied in Orca's SideScanning were recognized as “unique,” “like magic,” and “a big leap in cloud security,” including,

as explained more below in Section IV.E.4, with respect to specific claimed features in the '926 Patent. *See, e.g.,* Ex.2076, 11-12, 31. REDACTED

; *see also* §§IV.E.1, IV.E.4; Kaeli¶¶35-42, 213-224.

III. Claim Construction

Wiz's prior art fails to render obvious the challenged claims under any reasonable construction (Pet.8-11). *See* Kaeli¶¶73-200. However, Wiz's construction of the "analyzing" term should be rejected.

A. "Analyzing the Snapshot"

Wiz argues "'analyzing[] the snapshot'" in claims 1, 14, 15, "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]. The only support Wiz cites to argue "analyzing [a] snapshot" encompasses "analysis of a VM instantiated from a snapshot" are allegations in Orca's amended complaint from district court. *See* Pet.10 (citing Ex.1006). Wiz is wrong. Nothing in those allegations indicates 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¶¶44-48.

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 is readily apparent from the ’926 Patent’s claims and specification. ’926 Patent, cls. 1, 14, 15 (“snapshot of at least one virtual disk”), 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 ¶47. The specification also distinguishes the claimed analyzing a “snapshot” that “does not require any interaction and/or information from the VM” (’926 Patent, 5:20-23), from unclaimed systems that “instantiate a copy of the VM” and performs “execution of the instance of the VM [in] an isolated sandbox.” *Id.* 5:55-67, 7:42-52.

Tellingly, Wiz’s expert, Dr. Stavrou, never supported and only “*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, 265:17-266:4, 266:13-267:15 (“I didn’t ask why.”), 267:16-268:3 (“I don’t have an opinion why that was included.”), 268:4-269:20; Ex.2172, 38:7-20 (“encompassing direct analysis of the snapshot data” as the meaning of analyzing the snapshot is “consistent with the ’926 specification”), 39:4-40:1. And Dr. Stavrou admitted “[n]othing” in Veselov’s description of “assessing or analyzing an actual running instantiated virtual machine” “refers to analyzing a snapshot.”

Ex.2077, 280:8-281:1. Wiz's errant interpretation should be rejected. Kaeli¶¶44-48.

IV. Ground 1 Fails: Claims 1, 5-10, and 12-15 Are Nonobvious Over Veselov And Mohanty

A. Overview of Veselov (Ex.1007)

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¶¶49-60; *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, 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 is arranged as claimed in the '926 Patent. Kaeli¶¶49-60, 78-86; Shua¶¶146-154. In particular,

none of Veselov's embodiments teach analyzing a snapshot to determine the "cyber threats based on data stored in the virtual disk" recited in the challenged claims, i.e., that include "at least one of" the types of data in limitations 1.4, 14.4 and 15.4, nor the remaining limitations that require determining a "risk" and reporting prioritized alerts based on those determined threats. Kaeli¶¶49-60, 78-86; Ex.2077, 97:13-98:10.

B. Overview of Mohanty (Ex.1075)

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." Mohanty, 1:5-22; Kaeli¶¶61-64. 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 or RAPID7." *Id.* 1:11-14, 4:59-62, 6:54-58, Fig. 2; Kaeli¶¶61-64; Ex.2173; Ex.2174; *see* Ex.2172, 239:3-240:9 (Stavrou "didn't look at" whether Mohanty uses agent-based approaches); Shua¶¶156, 88.

Mohanty uses the outputs of these agent-based VA products in a "three dimensional" algorithm that correlates vulnerabilities with "contextual information

such as threat data and virtualization tags.” Mohanty, 3:43-49. Unlike the cyber threats “based on data stored on the virtual disk” in the ’926 Patent, Mohanty’s “threats” are directed to “external threats.” *Id.* 3:60-67, 4:33-36, 6:64-7:5; Kaeli¶¶61-64, 132; Shua¶¶155-158.

C. Wiz’s Conclusory And Generic Motivations To Combine Should Be Rejected

Wiz contends that arriving at the claims would have been obvious because the prior art collectively taught the required elements of the claims. *See* Pet.22-23. It is black letter law, however, that even if “separate references cover[] each separate limitation in a claim under examination”—which is not the case here (§§IV.D.1-4)—“obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention.” *Unigene Laboratories, Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011) (citing *KSR*, 550 U.S. at 421). Wiz has not made that showing here for the following four reasons.

First, Wiz’s combination is foundationally based on the assertion that Veselov’s and Mohanty’s security assessments would “typically consider[] the same types of data (e.g., applications, configurations, files, etc.).” Pet.23. Even if it were true that the references’ security assessments resulted in similar “types of data,” that suggests at best the two references are analogous art, and is legally deficient as a

motivation 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¶¶87-98. Before Orca’s inventions—and for years afterwards—the industry believed agentless scanning using “snapshots” was “lightweight” and could only deliver “rudimentary security capabilities.” Ex.2106, 1-2. Those in the industry believed only agent-based security analyses, like proposed in Mohanty, could provide detailed monitoring and protection. *Id.* It was only after Orca introduced its patent-practicing SideScanning in 2019 (*see* §IV.E.2), that the industry recognized the deep security assessment made possible by analyzing snapshots located using cloud computing APIs. Kaeli¶¶213-219; 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* §IV.E.3 (Orca overcame skepticism).

Veselov itself reflects the industry’s 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 of a duplicate VM instantiated from a snapshot (*e.g.*, Figs. 3A/3B), and (2) analyzing a snapshot as a “data file” without agents (*e.g.*, Figs.

5A/5B). Kaeli¶¶49-60, 78-86, 90-98; *see* Ex.2172, 49:11-20; Ex.1002 ¶89. In Veselov’s “security agent” based assessments, 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); Kaeli¶¶49-60, 78-86, 90-98;. As explained in Section III.A above, Veselov’s agent-based analysis of instantiated VMs cannot satisfy the claimed “analyzing a snapshot.”

In contrast with its agent-based approach, Veselov teaches obtaining 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 would permit any analysis of “dynamic” data, “network connections,” “communications to computing resources,” configurations, or any of the other information available in Veselov’s agent-based VM analyses. *See id.*; Kaeli¶¶97-98.² Accordingly, the foundational aspects of Wiz’s purported

² Wiz’s cited background references indicate a difference between live VM analyses and agentless analyses too. *See* Ex.1038, 134; Ex.1043; Kaeli¶94.

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).

Second, Wiz contends Mohanty attempts to solve a problem where “risk profiles may change frequently.” Pet.24. But that problem would have led a POSA *away* from implementing snapshot based approaches, as in Veselov, which do not provide continuous or real-time analyses of virtual cloud assets like Mohanty’s agent-based approaches. Kaeli¶¶90-98. Rather, Veselov only discloses security assessments based on “snapshots,” which is static data about a virtual machine at a past “point in time.” *See* Veselov, 6:50-53, 20:60-64; Kaeli¶¶90-98. These are the types of techniques that Mohanty disparaged, as they provide reports of a system “provided in the past” that could “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, 3:3-8; Kaeli¶¶87-98. Mohanty addresses these problems of information becoming “obsolete” by increasing the complexity of its monitoring and assessment system, i.e., a multi-dimensional model. Mohanty, 3:43-67, Fig. 2. But increasing the “complexity of

installation and monitoring” of an assessment is what *Veselov* describes as a problem. *Veselov*, 2:42-46; *Kaeli* ¶¶87-98. The competing preferences of Mohanty and *Veselov*, even if not teaching away, would have led a POSA away from combining them. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069 (Fed. Cir. 2018).

Third, Wiz asserts “applying Mohanty’s prioritization techniques would similarly benefit snapshot-based assessments.” Pet.25. That argument addresses only whether Mohanty and *Veselov* “would have allowed for” a combination or that they “could be combined,” which is “not enough.” *Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 993 (Fed. Cir. 2017) (emphases omitted). Although proof of 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 show a motivation to combine and expectation of success. *Id.* at 994 (emphases omitted). Here, Mohanty detects and provides context for vulnerabilities identified using agent-based scanners for real-time running processes on an asset. *Kaeli* ¶¶92-93. 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* ¶¶97-112. Nor would such a combination have a reasonable expectation of success because, as Dr. Stavrou admitted, “I don’t think that an agent can be installed on a snapshot.” Ex.2172, 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 (P.T.A.B. Sept. 18, 2024); *see also Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016).

Fourth, the above failings in Petitioner’s rationale for combining Veselov and Mohanty are not remedied by the Petition’s citations to over a dozen tertiary references. *See* Pet.23-25. None of these references address applying security techniques relying on agents and running VMs, as in Mohanty, to a snapshot-based analysis, as in Veselov. Kaeli¶¶99-105. And, Wiz’s retreat to a myriad of tertiary 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.” *In re NTP, Inc.*, 654 F.3d 1279, 1299 (Fed. Cir. 2011).

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*, 882 F.3d at 1068-69 (original emphases). Wiz’s hindsight based motivation to combine is also refuted by objective evidence discussed in Section IV.E below.

D. Wiz Fails To Show The Ground 1 Art Teaches Multiple Claim Limitations

1. Limitations 1.4, 14.4, 15.4

Wiz's Veselov/Mohanty combination fails to disclose or render obvious limitations 1.4, 14.4 and 15.4 because neither reference detects cyber threats that are "based" specifically on "at least one of" the expressly recited types of "data stored on the virtual disk." Kaeli ¶¶115-140. As Dr. Stavrou conceded, "**the data** includes" at least one in these limitations takes its antecedent basis from "cyber threat based on **data stored on the virtual disk.**" Ex.2172, 158:3-159:5. Accordingly, these limitation require a detection of cyber threats based specifically on "at least one of" the "listed types of data" in the claim. *See* Ex.2172, 158:22-159:5.

Of the specifically listed types of "data," Wiz only contends the Ground 1 combination taught: (1) unencrypted sensitive data; (2) weak encryption schemes; (3) personally identifiable information; (4) weak passwords; or (5) services run at startup. Pet.39-40; Ex.1002 ¶161; Ex.2172, 178:10-22 ("I don't opine on anything other than those.").³ Wiz is wrong.

³ The Board would be right to give little weight to Dr. Stavrou's testimony considering his attempts to evade questions confirming the scope of his declaration opinions. *See* Ex.2172, 182:2-2-185:5 (refusing to confirm no declaration opinion

The Petition asserts that both Veselov and Mohanty each separately disclose these limitations, but Wiz fails as a threshold matter to explain “with particularity ... the evidence that supports the grounds for the challenge to each claim.” 35 U.S.C. § 312(a)(3). Instead, Wiz merely provides general assertions about how *either* Veselov, *or* Mohanty, separately disclose limitations 1.4, 14.4 or 15.4, without clearly identifying how, or why, a POSITA would have been motivated to modify the processes disclosed in those references to arrive at the claimed invention. *See generally* Pet.34-40. Nevertheless, Wiz’s series of alternative arguments for how Veselov, Mohanty, or a “skilled artisan” would find the claim “routine” should be rejected for the reasons discussed below.

a. **Veselov Does Not Teach Limitations 1.4, 14.4 and 15.4**

Wiz alleges Veselov alone discloses analyzing snapshots to determine a plurality of cyber threats based on one or more of unencrypted sensitive data, weak encryption schemes, personally identifiable information, weak passwords, services run at startup. Pet.36-39. Wiz’s three alternative arguments fail.

First, Wiz argues that Veselov “teaches applying rule packages such as CVEs, which were known to identify cyber threats.” Pet.36 (citing Veselov, 2:22-54, 7:16-

on “disabled address space layout randomization”), 184:14-19 (similar); *see generally id.* 179:12-190:2.

22). “CVE” is an acronym for “Common Vulnerabilities Exposure,” and refers to a database of **vulnerabilities** that can be detected as part of a security assessment. Ex.2188 (<https://nvd.nist.gov/vuln>). While vulnerabilities may be one type of “potential cyber threat,” they are not cyber threats based on data expressly required by elements 1.4, 14.4, and 15.4. Kaeli¶¶119-129.

The ’926 Patent draws this distinction by separately describing analyzing a snapshot to (1) detect vulnerabilities, and (2) detect “cyber threats **that do not represent vulnerabilities.**” ’926 Patent, 6:20-32; *see also id.* 4:38-43 (discussing CVE databases for “vulnerabilities”). The former describes an embodiment that is not claimed in the ’926 Patent⁴, whereas the latter includes the data-based threats recited in limitations 1.4, 14.4, and 15.4. *Compare* ’926 Patent, 6:21-32 (listing examples of cyber threats that do not represent vulnerabilities), *with id.* cls. 1.4, 14.4, 15.4. Accordingly, Veselov and Mohanty’s respective discussions of detecting “vulnerabilities” or generalized assessments using a “CVE” database are not relevant to, and do not disclose or render obvious, limitations 1.4, 14.4 and 15.4. Kaeli¶¶119-131.

⁴ Analyzing snapshots to determine vulnerabilities is claimed in related patents. Kaeli¶123; Exs.2183-2187 (*e.g.*, cl.1).

As part of its “CVE” argument, Wiz asserts that “many CVEs were associated with [1] application features posing a threat to system security and [2] common startup services.” Pet.36-37. Wiz argues [1] is sufficient to satisfy the claim language because the ’926 Patent specification lists “risky application features” as a “cyber threats.” *Id.* (citing ’926 Patent, 6:21-32). But “the name of the game is the claim,” Giles S. Rich, *The Extent of Protection and Interpretation of Claims – American Perspectives*, 21 Int’l Rev. Indus. Prop. & Copyright L. 497, 499, 501 (1990), and “risky application features” in the specification are *not* one of the cyber threats based on types of data required by limitations 1.4, 14.4 or 15.4. Wiz’s attempt to map the prior art to an unclaimed specification embodiment should be rejected. Kaeli¶123.

As to Wiz’s argument that there are CVEs corresponding to “common startup services,” Wiz’s argument fails factually and legally. Factually, none of the six “CVE” exhibits Wiz cites states the vulnerabilities are associated with “common startup services,” and neither the Petition nor Wiz’s expert provides any explanation supporting that assertion. Kaeli¶¶124-125; Exs.1090-1091, 1100-1103. Even if any of the identified CVEs actually relate to “common startup services,” that still is not enough because Veselov does not teach determining any of the particular CVEs Wiz identified. *See* Pet.36-37. At best, Wiz’s argument puts the cart before the horse. A CVE database is a glossary that classifies vulnerabilities, and thus represents what could theoretically be determined by a security assessment as an output. Kaeli¶122.

Just because a vulnerability *exists* in a database says nothing about whether the particular snapshot scanning technique taught by Veselov is capable of or would actually result in determining a particular vulnerability. Kaeli¶¶122-123.

Legally, because Wiz’s “CVE” argument fails to disclose the limitations expressly, Wiz is relying on inherency. But Wiz cannot meet the inherency standard. While in some instances “inherency may supply a missing claim limitation in an obviousness analysis,” Wiz must prove the missing claim limitation “*necessarily* must be present, or the natural result of the combination of elements explicitly disclosed by the prior art.” *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1194-96 (Fed. Cir. 2014) (explaining this is a “high standard”), *aff’d*, 624 F. App’x 756 (Fed. Cir. 2015) (per curiam); *Cont’l Can Co. USA, Inc. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991). Wiz, however, merely asserts that “evaluated data” in a CVE analysis “*typically* included common startup services.” Pet.40. That is not enough: “[t]he mere fact that a certain thing may result from a given set of circumstances is not sufficient” to find a limitation as inherent. *In re Oelrich*, 666 F.2d 578, 581 (C.C.P.A. 1981).

Second, Wiz argues Veselov “teaches identifying nonsecure system configurations, which also encompass ‘potential cyber threats.’” Pet.37. As with its CVE/vulnerability theory, Wiz’s “nonsecure configurations” theory fails because it is not “at least one of” the specific types of “cyber threats based on data” in

limitations 1.4, 14.4, and 15.4. Kaeli¶¶126-127. Wiz tries to get around this by arguing the claimed “weak passwords” and “weak encryption schemes” are taught by the ’926 Patent to be types of “nonsecure system configurations.” Pet.37 (citing ’926 Patent, 6:21-32). Wiz is wrong. The cited portion of the ’926 Patent never mentions “non-secure configurations,” let alone equating such configurations with “weak passwords” or “weak encryption schemes.” *See id.*; Kaeli¶¶126-127; *see also* ’926 Patent, 4:50-53 (referring to “non-secure configuration” without reference to passwords or encryption).⁵ Additionally, even if the ’926 Patent did draw that connection, obviousness “must not be derived by hindsight from knowledge” of the ’926 Patent. *See Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.*, 381 F.3d 1371, 1376 (Fed. Cir. 2004). Here, Wiz has not identified anything in Veselov teaching “configuration” assessments include weak passwords or weak encryption schemes as claimed. Kaeli¶¶126-127. Nor can Wiz rely on inherency, because nothing about “configuration assessments” *necessarily* requires a detection of weak passwords, weak encryption schemes, or any of the other expressly identified types of data in elements 1.4, 14.4 and 15.4. Kaeli¶¶126-127; *see, e.g., PAR Pharm.*, 773 F.3d at

⁵ Wiz’s hindsight reconstruction is reflected in its allegations that “weak passwords” are a type of “bad configuration[]” in one portion of the Petition (Pet.37), but a type of “sensitive data” in another. *Id.* 40.

1196; *Oelrich*, 666 F.2d at 581. Indeed, several of Wiz’s tertiary references describe analyzing “configurations” that have no disclosure “weak passwords” or “encryption schemes.” Kaeli ¶127; Ex.1008 ¶37; Ex.1020, 12:40-13:4.

Third, Wiz’s final argument is Veselov “contemplates implementation of any suitable security assessment” and “‘best practices’ packages.” Pet.36, 39 (citing Veselov, 2:35-41). From these statements, Wiz contends it has carte blanche to combine Veselov with *any* security assessment. *See id.* 37, 58, 68 (relying on same “suitable assessment” for combinations with all references). Wiz is wrong. In particular, Wiz fails to show evidence of what is (or is not) “suitable” in Veselov, and in particular determining the particular types of cyber threats based on data in the challenged claims. Snapshot assessments detecting that data is not supported in Veselov itself, which only teaches detecting “vulnerabilities” and “host configuration assessments.” *See* Veselov, 1:46-49, 2:35-41, 4:5-8, 4:14-18, 7:1-5, 10:24-36, 14:41-50, 14:63-65, 15:1-3, 21:1-2, 23:30-33, 23:40-47, 23:56-60; Kaeli ¶¶128-129. Finding no support in Veselov, Wiz cites its expert and cross references Section IX.B of the Petition, without explanation or elaboration, which is a section referring to over ***fifty (50) exhibits***. *See* Pet.39, 13-15 (§IX.B); Kaeli ¶¶135-136. Wiz’s citation to ***fifty*** exhibits cannot meet Wiz’s burden to identify “with particularity ... the evidence that supports the grounds for the challenge to each claim[.]” 35 U.S.C. § 312(a)(3); *see also Cisco Sys. Inc. v. C-Cation Techs., LLC*,

IPR2014-00454, Paper 12 at 10 (P.T.A.B. Aug. 29, 2014) (informative). Wiz’s assertion that detecting sensitive data in cloud systems was a “common best practice” before the ’926 Patent is also wrong. Articles from three years after the priority date in 2022, including from Wiz, explained “less than 1% of companies around the world use a DSPM solution,” i.e., a system that “identif[ies] where critical information – such as ... personal information ... is stored in the cloud,” and was a field that “only emerged in recent years.” Ex.2154, 3; Ex.2155, 2 (Wiz: “securing cloud data is a difficult problem.”); Kaeli¶¶135-136.

b. Mohanty Does Not Teach Limitations 1.4, 14.4 and 15.4

Separately from Veselov, Wiz argues Mohanty teaches the claimed determining “the existence of a plurality of potential cyber threats” in data. Pet.38-40. As an initial matter, the Board should reject Wiz’s Mohanty arguments because none of the “cyber threats” Wiz identifies are determined by analyzing “snapshots” as required by limitations 1.4, 14.4 and 15.4. Kaeli¶130. If Wiz is alleging a POSA would look to Veselov for analyzing snapshots, but detect Mohanty’s “cyber threats,” the Board should reject those arguments because Veselov and Mohanty disclose different security assessment techniques (*see* §§IV.A-C), and the Petition does not clearly explain “how the combination of the two references was supposed to work.” *Personal Web*, 848 F.3d at 994 (emphasis omitted). Wiz’s Mohanty arguments should also be rejected for three additional reasons.

First, Wiz contends Mohanty discusses “using CVE assessments like Veselov.” Pet.38; *id.* 37 (“Mohanty teaches performing a similar CVE assessment.”). Those arguments fail for at least the same reasons as for Veselov above. Mohanty does not disclose determining any of the particular CVEs Wiz relies on, otherwise suggest that such specific CVEs would be determined, and Mohanty’s CVE analysis does not inherently or necessarily disclose the claimed cyber threats. Kaeli¶131.

Second, Wiz misleadingly asserts that because Mohanty discusses analyzing “threats,” it discloses the claimed “potential cyber threats.” Pet.38. Wiz is wrong. Mohanty’s “threats” are *external* to an asset and categorically different than the claimed “threats based on data *stored on* the virtual disk.” Kaeli¶132. Mohanty explains that its “threat module” refers to an external “threat intelligence system” that provides “information 208 *about external threats*.” Mohanty, 3:60-67, 4:33-36, 6:64-7:5 (threat intelligence system ... reports latest lists of threats in a wild 208”). For example, an “external threat” may be that a known hacking group is currently targeting machines with a particular operating system (OS) using a specific exploitable vulnerability. *See* Mohanty, 6:64-7:5; Kaeli¶132. Mohanty never analyzes the virtual cloud asset to determine threats “in data stored on the virtual disk” as in the challenged claims. Kaeli¶132.

Third, although Mohanty discusses “sensitive data” (Pet.38), Mohanty does not “determine” sensitive data by “analyzing” a virtual cloud asset, let alone by analyzing a snapshot of its virtual disk. Kaeli¶133. Mohanty refers to “sensitive data” only as an example of a “static tag” set by a virtual cloud environment when “an asset (e.g., a virtual machine or a virtual application) is created and deployed in a virtual environment.” Mohanty, 4:4-8, 4:13-15, 5:50-54 (“*static tag information 204* could include indication of whether there is *sensitive data* in or handled by the asset 224”), 5:38-43; Kaeli¶133; Ex.2172, 209:12-19. Mohanty’s “static tags” are therefore a defined asset characteristic and not the result of “analyzing” to determine cyber threats based on data stored on the virtual disk. Kaeli¶133; Ex.2172, 212:6-10.

A POSA would have particularly understood Mohanty’s “static tags”—including “sensitive data”—are not determined as part of a security assessment in view of Mohanty’s discussion of “dynamic tags.” Kaeli¶133; Ex.2172, 194:15-18 (Stavrou agreeing Mohanty has “two types of context tags,” “static tags” and “dynamic tags”), 199:10-12. Mohanty explains “dynamic” tags relate to information “that is subject to change during the lifespan of the asset,” and can also be referred to as “security tags, since the changing information is of interest regarding security of the asset.” Mohanty, 4:15-23. Mohanty’s “dynamic” or “security” tags include information that is determined “by security technologies monitoring the same

systems.” *Id.* 5:38-48 (“sensitive data” is something a virtual machine is “mark[ed]” with); Kaeli¶133. In contrast, Mohanty does not teach using security technologies” or “monitoring” system to determine “static tags,” like “sensitive data.” Kaeli¶133. Mohanty also does not teach that “dynamic tags” would (or should) include any of the “cyber threats based on data stored on the virtual disk” recited in the challenged claims. Kaeli¶¶138-139.⁶

**c. Wiz Fails to Explain How Or Why A POSA Would
Combine Mohanty Or Veselov To Arrive At Limitations
1.4, 14.4 and 15.4**

As discussed above, Wiz layers a variety of alternative (and incorrect) arguments regarding how Veselov and Mohanty separately disclose limitations 1.4,

⁶ Mohanty states that a “dynamic tag” could include “whether or not suspicious data has been transferred into or out of the asset.” Mohanty, 5:54-59. Suspicious “transfers” of data into or out of the asset is different in kind from determining the challenged claims cyber threats “stored on the virtual cloud asset.” Kaeli¶139; *see* Mohanty, 5:50-58 (using “sensitive data” and “suspicious data” separately). For example, “suspicious data” could include transfer of *any* data from a networked computer to a computer located in a foreign country. Kaeli¶139; *see also* Ex.2172, 200:18-201:6 (POSA “cannot” confirm Mohanty’s “suspicious data” is “sensitive data” without further context).

14.4, and 15.4. As to the references combined, Wiz does not explain “how the combination of the two references was supposed to work.” *See Personal Web*, 848 F.3d at 994 (emphasis omitted). Wiz’s expert was unable to explain, for example, how Mohanty or Veselov could be combined to “analyz[e] a snapshot” to determine Mohanty’s “tags,” beyond generalities that “you can apply teachings from one – Mohanty in this case – to Veselov’s scanning.” Ex.2172, 206:4-16. Wiz’s arguments thus boil down to a contention that a “skilled artisan, once presented with the two references, would have understood that they could be combined,” which the Federal Circuit instructs is “not enough.” *Personal Web*, 848 F.3d at 993-94 (emphasis omitted). It is particularly not enough here when considering the objective evidence demonstrating Orca’s inventions analyzing snapshots to determine threats based on data stored on a virtual disk, like sensitive data and PII, in cloud environments garnered significant praise and commercial success, and Wiz copied those features from Orca. *See* §IV.E; REDACTED

2. Limitations 1.5-1.6, 14.5-14.6, 15.5-15.6

Wiz contends Mohanty alone satisfies limitations 1.5-1.6, 14.5-14.6 and 15.5-15.6, which require “[determine/determining] a risk associated with each of the determined plurality of potential cyber threats,” and prioritizing the determined threats according to the risk. Pet.41. Wiz’s mapping of Mohanty to these limitations, however, is inconsistent with its analysis of limitations 1.4, 14.4, and 15.4. Ex.2172,

217:4-14 (agreeing elements 1.5 and 1.6 are “referring to the same cyber threats” as element 1.4). What Wiz maps to the “threat” in limitation 1.5-1.6 is a “threat score” that quantifies the magnitude of impact of an *external* threat, i.e., a threat that is *not* “based on data stored on the virtual disk. Pet.41; *see* Mohanty, 4:38-58, cl. 14; *see also id.* cl. 17, 8:14-18; Kaeli¶¶141-147; *see* Ex.2172, 215:7-22 (testifying for the “risk” in elements 1.5, 14.5 and 15.5, “we use a threat score. Yes.”).

Mohanty’s “external threats” are *not* the alleged cyber threats based on at least one of “unencrypted sensitive data, weak encryption schemes, weak passwords ... personally identifiable information ... [or] services run at startup” that Wiz relies on for limitations 1.4, 14.4 and 15.4. Pet.41 (citing Mohanty, 7:30-56). Wiz has therefore failed to show how its proposed combination renders obvious the challenged claims as a whole. Kaeli¶¶141-147.

3. Limitations 1.7, 14.7, 15.7

Limitations 1.7, 14.7, and 15.7 further require “reporting the at least some of the determined plurality of potential cyber threats as alerts prioritized according to their associated risks.” Kaeli¶¶148-160. The antecedent basis for “the determined plurality of potential cyber threats” in these limitations is “a plurality of potential cyber threats, each cyber threat based on data stored on the virtual disk, wherein the data includes ...” in limitations 1.4, 14.4, and 15.4. *See* Ex.2172, 217:4-14. As discussed in the preceding sections, Wiz’s Ground 1 does not render obvious

determining the claimed “potential cyber threats,” and for the same reason does not render obvious reporting such threats as prioritized alerts. Kaeli¶¶148-160.

Furthermore, Wiz argues Veselov “reports assessment results describing the identified risks.” Pet.42. The only “identified risks” in Wiz’s cited portions of Veselov are “vulnerabilities.” *See id.* (citing Veselov, 10:17-36 (“if vulnerabilities are identified in the assessment results”), 18:53-56 (“the results, as described above”), 20:57-21:13 (“assessment result describing a security vulnerability”), 23:19-47 (“assessment result describing one or more security vulnerabilities”)). Vulnerabilities are different than, and do not disclose, the claimed “plurality of potential cyber threats” as discussed above for limitations 1.4, 14.4 and 15.4. Kaeli¶¶149-153; Shua¶44.

Even if Veselov’s vulnerabilities could satisfy the claimed “cyber threats” (they cannot), Veselov does not report those vulnerabilities “as alerts.” *Cf.* Pet.43. Instead, Veselov provides “assessment results that describe ‘findings’ relative to the assessed properties” (Veselov, 10:17-22), but a generic report listing all “findings” does not disclose reporting cyber threats “*as alerts*” as claimed. Kaeli¶¶149-153. For example, nothing in Veselov discloses reporting vulnerabilities such that they “stand out.” Ex.2077, 287:4-12 (Stavrou: “a report is a little bit more generic term. An alert is something that potentially makes it stand out.”); Ex.2048, 12 (Wiz: “[a] report and an alert *must mean different things* to give meaning to all the claim

language.”); *see* ’926 Patent, 7:53-55, 6:40-43; Ex.2077, 284:18-285:6, 286:9-287:21 (Stavrou: “alerts are different than reports” and “it’s not enough to just report, you have to report as alerts”).

Wiz also does not argue that Veselov teaches the claimed “prioritization,” *see* Pet.43, but contends instead only that Mohanty provides this missing limitation. *Id.* (Mohanty “further teaches reporting the cyber threats as alerts ‘prioritized according to their associated risks.’”). Wiz is wrong in both of its alternative arguments.

First, Wiz argues Mohanty’s alerts are directed to “**one or more applicable threats**.” Pet.43 (original emphasis) (quoting Mohanty, 9:16-26). But, as discussed above, Mohanty’s “threats” are *external* threats, not threats “based on data stored on the virtual disk” of an asset. Kaeli¶¶154-156; Mohanty, 4:33-35, 4:41-46, cls. 14, 17; *see* §IV.D.1.b.

Second, Wiz contends Mohanty “sends its alerts in response to determining prioritization scores.” Pet.44. The “prioritization score[s]” do not relate to “cyber threats based on data stored on a virtual disk” as claimed, instead being associated with “a specific **vulnerability** of a specific asset.” Mohanty, 9:6-19; Kaeli¶¶154-156; *see* §IV.D.1 (vulnerabilities do not satisfy claimed “cyber threats”). And, the Petition does not detail any theory in limitations 1.7, 14.7 and 15.7 where Mohanty discloses alerting for a cyber threat based on (for example) unencrypted sensitive

data (as in limitation 1.4, 14.4, and 15.4 (*see* Pet.39-40)), or prioritized according to its determined risk. *See* Pet.42-44.

Objective evidence further refutes Wiz’s hindsight-based arguments that “[c]ommunicating scores/rankings was also a common way of reporting prioritized alerts according to the cyber threat’s associated risk” (Pet.44), by showing Orca’s implementation of prioritized alerts in the context of analyzing snapshots of a virtual disk to determine cyber threats based on data in cloud environments resulted in great commercial success, praise by the industry, and Wiz’s copying. *See* §IV.E; Kaeli¶157.

4. Dependent Claim 13

Wiz relies on Veselov alone for the additional requirements of claim 13 (Pet.53-57), but Veselov does not teach “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¶¶161-168.

Wiz argues that Veselov discloses querying a cloud management console for the location of a snapshot (Pet.55-56), but Wiz concedes that Veselov does *not* disclose any embodiment where a cloud management console is additionally queried to locate a “virtual disk” as recited. *See id.*56. Instead, Wiz contends location a virtual disk would have been obvious because certain embodiments teach a “user” “can initiate the snapshot-analysis process” by “using the UI to make an API call

identifying the target VM.” *Id.* 55-56. But, an API call “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¶¶162-165.

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¶¶162-165. Wiz contends that locating virtual resources was “a common feature of these consoles” (Pet.57), but that at best only addresses whether a POSA “*could* have” modified Veselov to include such a step, without explaining 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).

Second, as Dr. Stavrou admitted at his deposition, “Virtual disks are different from virtual machines”—“[t]hey are definitely not synonymous.” Ex.2077, 97:13-98:10. And, as the ’926 Patent explains, VMs and virtual disks are typically in different locations. ’926 Patent, 3:56-58, Fig. 1B; Kaeli¶¶162-165; Ex.2077, 92:4-93:19, 94:16-21. Thus, locating a VM does not necessarily or inherently specify the location of the virtual disk. *See* Ex.2077, 142:15-143:3 (Stavrou: conceding no Veselov disclosure “identifies or describes an identifier for a virtual disk”); Kaeli¶¶162-165.

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.56. Wiz improperly relies exclusively on depictions in the figures to draw this conclusion, without any supporting description in the text. *Id.* 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. *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 ¶¶162-165. And in Figures 3A, 3B, 4, 5A, 5B, Veselov teaches *providing* a volume image *to* a hypervisor or service. Veselov, 12:37-51; 18:16-21.

Regardless, even if Veselov’s system were *capable of* querying a “UI/API” to configure aspects of an “assessment target” (Pet.56), 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 as claimed. *See ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1363 (Fed. Cir. 2018). And objective evidence establishes that using a cloud management console to locate virtual disks was not obvious. Orca implemented it with great success because it allowed Orca to install security components in the same location as the

virtual disk, which was critical for performance. Ex.2133, 1; Ex.2082, 8:06-11:08 (Shua video describing how “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¶¶245; Shua¶¶19, 83 (discussing Exs.2082-2083).

REDACTED

E. Objective Evidence Demonstrates and Confirms the Nonobviousness 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. Accordingly, objective nonobviousness evidence may either be “linked to an individual element or, in other circumstances, it could be linked to the inventive combination of known elements.” *WBIP*, 829 F.3d at 1332; *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 combinations claimed were *not* taught in the prior art—Wiz relies on only (hindsight-driven) obviousness challenges. And evidence of long-felt, unsolved need, skepticism regarding the inventions, industry acceptance, industry praise, commercial success, and copying demonstrates and confirms the non-obviousness of the ’926 Patent’s claimed combinations. *See* §§IV.E.1-IV.E.5; Kaeli¶¶201-286.

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¶¶80-91.

Prior art techniques for analyzing cloud architectures before the ’926 Patent included (1) “traffic inspection,” (2) using “network scanner[s] deployed out of path,” (3) “traffic monitor[ing],” and (4) using “agents installed in each server.” ’926 Patent, 1:47-2:17. As Mr. Shua explained, both in the ’926 Patent and in various pre-IPR conferences and videos, these prior art techniques suffered from numerous problems. Shua¶¶81-85 (discussing ’926 Patent, 1:52-2:17; Exs.2082, 2083, 2099,

2100, 2133); *see also* Ex.2076, 11 (“Traditional agents struggle with complex deployment and maintenance.”); Ex.2103, 2 (describing deployment and coverage problems with agents). In particular, they failed to provide adequate detection of and protection for cyber threats based on data stored on a virtual disk, such as sensitive data. Shua¶86; *see also* Ex.2152, 5 (“locating” sensitive data “is generally proving unmanageable for legacy solutions”).

Accordingly, there was a long-felt, unmet need for a cloud security solution that could adequately address undetected cyber threats based on data stored on a virtual disk. ’926 Patent, 1:49-2:16; Shua¶86; Ex.2137, 1. Mr. Shua cofounded Orca to solve this need with SideScanning™, including as claimed in the ’926 Patent (*see* §IV.E.2 below)—which has been heralded as a “genuinely genius innovation” that redefined the industry. Ex.2076, 7; Shua¶¶90-91; Ex.2103, 1; Ex.2104, 2; Ex.2148, 15; *see also* Shua¶¶14-25 (describing videos (Exs.2078-2087) and documentation (Exs.2066, 2067, 2090, 2092, 2093) regarding SideScanning development and operation); Kaeli¶¶203-212.

2. Orca’s SideScanning™ Practices the ’926 Patent

Orca’s SideScanning™ has practiced the challenged claims of the ’926 Patent since 2019. Shua¶27; *see generally id.* ¶¶28-79; Kaeli¶202. For example, with respect to independent claims 1, 14, and 15, Orca’s SideScanning:

- Includes an “Onboarding” process and receives a request to scan a protected virtual cloud asset in the cloud computing environment (preambles and limitations 1.1, 14.1, 15.1); *see* Shua ¶¶29-33 (discussing Ex.2067, 1, 5-6, 8, 9-11, 13; Ex.2094; Ex.2095; Ex.2098, 1; Ex.2150; Ex.2300, 3-4; Ex.2096; Ex.2097);
- locates, using an API REDACTED, a REDACTED of a snapshot of at least one virtual disk of a protected virtual cloud asset (limitations 1.2, 14.2, 15.2); Shua ¶¶34-39 (discussing Ex.2067, 3, 10, 14, 17, 19; Ex.2300, 5-6, 11; Ex.2179, 1, 3);
- accesses the snapshot of the at least one virtual disk based on the snapshots REDACTED (limitations 1.3, 14.3, 15.3), Shua ¶¶40-43 (discussing Ex.2067, 14, 16; Ex.2300, 4, 5-6, 9, 11; Ex.2092, 20; Ex.2179, 1, 2; Ex.2301, 1; Ex.2302, 1; Ex.2303, 1-2; Ex.2311, 3, 5; Ex.2150; Ex.2097);
- analyzes such snapshots to detect “risks such as ... unsecured sensitive data” stored on the virtual disk (Ex.2067, 3) (limitations 1.4, 14.4, 15.4); Shua ¶¶44-45: (discussing Ex.2067, 3, 10, 14, 19; Ex.2300, 5-6);

- determines “risk” associated with each of the determined potential cyber threats including based on context such as whether the asset is internet facing (limitations 1.5, 14.5, 15.5); Shua ¶¶46-50 (discussing Ex.2067, 5, 16, 17; Ex.2092, 20; Ex.2313, 2, 4-5; Ex.2180, 3; Ex.2179, 1, 3);
- prioritizes the potential cyber threats, like unsecured sensitive data, based on the determined risk of the potential cyber threat (limitations 1.6, 14.6, 15.6); Shua ¶¶51-54 (discussing Ex.2092, 19-20; Ex.2067, 16; Ex.2179, 1, 3); and
- reports at least some of the determined cyber threats as alerts prioritized according to their associated risks (limitations 1.7, 14.7, 15.7); Shua ¶¶55-60 (discussing Ex.2067, 14, 16; Ex.2300, 9, 11; Ex.2092, 20; Ex.2179, 1, 2).

Orca’s SideScanning™ also practices dependent claims 2-13. Shua ¶¶61-79 (discussing Ex.2181, 13; Ex.2302, 1; Ex.2303, 1-2; Ex.2304; Ex.2311, 2, 3, 4, 5; Ex.2092, 20; Ex.2300, 7, 9, 11, 14; Ex.2180, 3-4; Ex.2067, 3, 10, 12, 13, 19; Ex.2313, 3). 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,” and “allowed deep visibility into cloud workloads without the need to install agents.” Ex.2076, 11-12, 31;

Shua¶¶91 (discussing Exs.2076, 2148); *see* '926 Patent, limitations 1.1-1.3, 14.1-14.3, 15.1-15.3. **REDACTED**

; *see* '926 Patent, limitations 1.7, 14.7, 15.7; *see also* Kaeli¶¶212; Shua¶¶¶128-130 (discussing 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 '926 Patent and related patents claiming priority to Orca's provisional patent application (No. 62/797,718). Shua¶¶¶16, 98; *see id.*¶¶¶17-23, 100, 128-129; 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*, 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¶¶90-94; Ex.2076, 8, 11; Ex.2106, 1; Ex.2148, 15. 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,” and 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.2103, 1 (“[A] new

‘agent-less’ approach to cloud security has recently become possible” and “provides security in a fundamentally different way.”); Kaeli¶¶213-219.

REDACTED

§IV.E.2 (Orca’s SideScanning™ practices the challenged claims); Kaeli¶¶213-219. And, ultimately, SideScanning™ was widely accepted—“everyone needed it in order to stay competitive.” Ex.2076, 7; *see also* Ex.2113, 4; Shua¶¶95-97, 101-102, 109-110 (describing exemplary customers and commercial success); Kaeli¶¶213-219.

4. The Industry Praised Orca's Revolutionary Inventions

Evidence of industry praise shows nonobviousness 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 '926 Patent, Orca received numerous awards for its inventions. Shua¶¶131-142 (discussing awards in Exs.2119-2132, 2144-2145); Kaeli¶¶220-224. 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” 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.2144; Ex.2145, 2; Ex.2121. In 2022, AWS awarded Orca “global Security Partner of the Year.” Ex.2122, 1-2. SC Media named Orca the “Best Cloud Security Posture Management (CSPM) solution” in 2022-2023 and a finalist in other categories. Ex.2124, 1; *see also* Ex.2123, 2 (award noting customer

praised Orca’s “agentless approach” as “both a major innovation and a game changer”); Ex.2125, 1-2. Orca was named on 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, the technology powering Orca’s product, embodying the inventions claimed in the ’926 Patent. Shua¶¶143-144.

REDACTED

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 ’926 Patent’s claimed combinations, such as using cloud computing platform APIs to facilitate snapshot analyses, detecting cyber threats based on data stored on a virtual disk, and reporting them as alerts prioritized based on risk. *See* Ex.2076, 7, 11-12, 31; 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.”), 4 (customer reporting Orca is “unique” because it “delivers tangible, actionable results”); REDACTED

The foregoing praise strongly supports 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

a. Wiz Copied Orca’s Patent-Practicing SideScanning™

Wiz knew of and had access to Orca’s technology before Wiz was founded. Mr. Shua presented Orca’s SideScanning™ technology to Wiz’s founder Yinon Costica when he still worked at Microsoft in May 2019. Shua¶¶111-115(discussing meeting and related emails Exs.2306, 2307).

REDACTED

REDACTED

Particularly relevant to the challenged claims, Orca introduced analyzing snapshots for cyber threats based on data, including “PII” and “weak passwords,” in SideScanning in 2019. Shua¶120; *see, e.g.*, Ex.2090, 4, 16; Ex.2067, 14. ^{REDACTED}

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

PII and “weak passwords” are the specific types of “cyber threats based on data” that are uniquely claimed in the ’926 Patent (limitations 1.4, 14.4, and 15.4).

REDACTED

REDACTED

REDACTED

Additionally, if scanning virtual disk snapshots to determine sensitive data would have been obvious and “routine” as Wiz now contends, Wiz would not have needed to copy that functionality from Orca. REDACTED

REDACTED

REDACTED

Less than 12 months later, Wiz launched its copycat “Data Security Posture Management” feature that “now detects [sensitive] data such as PII, PHI, and PCI.” Ex.2155, 1, 3; Shua¶121. In that presentation, Wiz emphasized that “securing cloud data is a difficult problem”—squarely contradicting its position here that detecting cloud data was “routine” and “well known.” Ex.2155, 2; Pet.23; Kaeli¶136.

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

; Shua¶¶38, 42, 71 (describing
Orca’s use of AWS API’s for SideScanning), 118-119 (discussing Exs.2308).

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

The evidence shows Wiz accessed and copied Orca's SideScanning™ technology embodying the '926 Patent, which strongly supports the claimed inventions were non-obvious. *See Stratoflex*, 713 F.2d at 1541; *WBIP*, 829 F.3d at 1336.

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.

Wiz's Cloud Security Platform uses what Wiz calls "workload scanning," which practices the challenged claims in the same way as Orca's SideScanning. Kaeli¶¶260-283 (discussing Exs.2025-2026, 2074, 2115, 2155-2158, 2308-2309,

REDACTED

). Wiz's "workload scanning":

- receives a request to scan a protected virtual cloud asset in the cloud computing environment (limitations 1.1, 14.1, 15.1); Shua¶¶118-119 (discussing Ex.2308, 1); Kaeli¶¶278-283;
- locates, REDACTED

of a snapshot of at least one virtual disk of a

protected virtual cloud asset (limitations 1.2, 14.2, 15.2); Shua¶¶118-119 (discussing Ex.2308, 1-2), 124 (discussing Ex.2115, 1-2); Kaeli¶¶278-283;

- accesses the snapshot REDACTED
(limitations 1.3, 14.3, 15.3);
Shua¶¶118-119 (discussing Ex.2308, 3), 124 (discussing Ex.2115, 1-2); Kaeli¶¶278-283;
- analyzes the snapshot of the at least one virtual disk to determine the existence of “data security” cyber threats, like unsecured “personally identifiable information (PII)” (Ex.2157, 1; Ex.2155, 3-4) (limitations 1.4, 14.4, 15.4); Shua¶¶118-119 (discussing Ex.2308, 3), 121 (Ex.2155, Ex.2154); Kaeli¶284-287;
- determines a risk associated with each of the determined cyber threats and “automatically correlates data risks with other cloud risks” (Ex.2155, 3-4; Ex.2160) (limitations 1.5, 14.5, 15.5); *see* Shua¶125; Kaeli¶¶288-291;
- prioritizes the potential cyber threats for “prioritization of critical data exposure” and “to build a single prioritized queue of attack paths and toxic combinations of risk” (Ex.2155, 3-4; Ex.2154, 3) (limitations 1.6, 14.6, 15.6); *see* Shua¶¶121, 124-125; ¶¶288-291;

- reports potential cyber threats based on data “such as PII” as alerts “with laser precision” (Ex.2155, 3), which are prioritized according to their “data risks” (Ex.2155, 3-5) (limitations 1.7, 14.7, 15.7), *see* Shua¶¶121, 124-125; ¶¶288-291.

REDACTED

REDACTED

Kaeli¶276; *see also* Shua¶111 (explaining frequent customer remarks Wiz’s core product functionality is same as SideScanning).

Wiz’s copying of Orca’s implementation of the inventions claimed in the ’926 Patent shows those claims are nonobvious because it both “praises” Orca’s invention and shows 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 Nonobviousness

The non-obviousness of the challenged claims is further demonstrated by Orca and Wiz’s commercial success. *Polaris*, 882 F.3d at 1072.

After the provisional patent application that led to the ’926 Patent was filed in January 2019, and Orca introduced the claimed inventions in SideScanning later that year, Orca obtained substantial outside investment. Shua¶¶96, 98-110 (discussing Exs.2065, 2108-2113, 2140 and how funding due to claimed inventions); Ex.2149, 24; Kaeli¶¶292-294. By June 2019, Orca raised \$6.5 million dollars with a direct nexus to the challenged claims, including Orca’s ability to determine “[w]here is my

sensitive data stored,” Ex.2107, 2-3, with one investor remarking about “Orca’s unique approach and innovative solution.” Ex.2107, 3; Ex.2065, 2-4; Shua¶¶99.

In 2020, Orca raised another \$75 million, notably because of the claimed combination of elements in the ’926 Patent: “[o]ne feature that makes Orca stand out is its ability to quickly provide workload-level visibility ... us[ing] low-level APIs that allow it to gain visibility into what exactly is running in your cloud.” Ex.2109, 1-2 (“Orca ... offers security tools that scan for ... personally identifiable information.”); Ex.2111, 1-2 (“What makes Orca stand out is ... what it calls its SideScanning technology.”), 4; Ex.2110, 1; Ex.2140, 1-2; Shua¶¶98-99, 104 (investments due to “novel aspects of SideScanning™ that are claimed in the ’926 Patent”).

And in 2021, just two years after introducing the Orca Cloud Security Platform powered by its patented SideScanning technique embodied in the ’926 Patent—Orca’s only product—Orca raised investments totaling \$550 million and was valued over \$1 billion. Shua¶¶107-109; Ex.2112, 1-2 (“Orca Security represents a revolutionary step forward in optimizing cloud environments Their touchless SideScanning technology is best in class.”), 3-4; Ex.2113 1-2; Ex.2139, 2. These funding announcements highlight Orca’s commercial success is attributable to the cloud computing provider API-based techniques for analyzing snapshots for cyber threats stored on virtual disks, such as sensitive data, in the ’926 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 “misplaced PII”), 3 (praise from industry), 4 (Orca “[p]rioritize[s] risk” and reports issues as “alerts.”).

Importantly, Orca did not enjoy this success because it was *already* a market leader and simply introduced a new product, which is due less weight. *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¶¶95-98 REDACTED Ex.2312 REDACTED Ex.2067, 1, 3. REDACTED

Chemours Co. FC v. Daikin Indus., Ltd., 4 F.4th

⁷ Cloud Workload Protection Platform.

1370, 1378 (Fed. Cir. 2021) (“significant sales” are evidence of commercial success). Orca would have certainly earned even more, but for Wiz’s copying. *See* Shua¶111.

The commercial success of Wiz’s infringing product 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., when Orca confirmed Wiz had copied SideScanning’s agentless snapshot functionality (§§IV.E.5.a-b; 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.2142.⁸ And after Wiz introduced sensitive data

⁸ Wiz’s public remarks about cloud APIs used for agentless security assessments being “new” in 2020 also undercut its obviousness arguments that the same were “obvious” before January 2019. *See* Pet.14, 18; *Power-One v. Artesyn Techs., Inc.*, 599 F.3d 1343, 1352 (Fed. Cir. 2010).

scanning in its “DSPM” feature in November 2022, which it also copied from Orca, Wiz’s annual recurring revenue purportedly grew from ~\$100M to \$500M in the next two years. Ex.2153; §§IV.E.5.a-b.

The above-discussed objective evidence demonstrates the nonobviousness of all challenged claims.

F. Ground 2 Fails: Claims 1-10 and 12-15 Would Not Have Been Obvious Over Veselov, Mohanty, and Ranum

Ground 2 “builds upon” Ground 1 (Pet.57), and purports to add “Ranum’s [alleged] teachings of determining cyber threats based on stored disk data, reporting associated risks of assets, and cryptograph-hash comparison.” *Id.* 57-66. The Board should find Ground 2 fails for the reasons in Ground 1, including that POSAs would not have combined Veselov and Mohanty as proposed. The Board should also reject Wiz’s reliance on Ranum for the additional reasons discussed below.

For the challenged independent claims, Wiz relies on Ranum only for limitations 1.4, 14.4, 15.4 and 1.7, 14.7, 15.7. Pet.61-63. But like its Ground 1 combination, Wiz’s Ground 2 combination does not “clearly explain[], or cite[] evidence showing, how the combination of” Veselov, Mohanty, and Ranum “was supposed to work.” *Personal Web*, 848 F.3d at 994 (emphasis omitted). Instead, Wiz merely contends generally that “[a]rriving at the claims involved using known elements according to their known functions to achieve predictable results.” Pet.58. Wiz is wrong.

A POSA would have understood that using the relied-upon elements in Ranum “according to their known functions,” would have led a POSA *away* from the claimed inventions, because the described functions are exclusively in the context of what can be detected by “active scanners.” Pet.61; Ranum (Ex.1093), 13:41-44 (“the active scanners 210 may generally scan ...”), 13:48-49 (“active scanners”), 14:3-11 (“the information provided by the active scanners”). Dr. Stavrou admitted Ranum does not teach snapshot scanning. *See* Ex.2172, 251:8-252:2 (conceding Ranum’s “active network scanning” is different than Veselov’s snapshot assessments), 276:17-20 (no opinions that “Ranum is analyzing snapshots of a virtual cloud asset.”).

A POSA also would have understood Ranum’s “active scanner” teachings are *incompatible* with analyzing snapshots as claimed in the ’926 Patent, and with the embodiments analyzing snapshots in Veselov. Kaeli¶¶173-178; Shua¶¶159-161; *see also* ’926 Patent, 1:56-2:9 (describing problems with prior art “network scanner[s]” and “[t]raffic inspection”). Ranum discloses that “active scanners” detect vulnerabilities and other cyber threats by “communicat[ing] packets or other messages within the network to detect new or changed information describing various routers, hosts, servers, or other devices in the networks.” Ranum 4:36-57, 10:34-41 (same); *see* Pet.61. These teachings **cannot** be applied to analyzing a snapshot. Kaeli¶¶173-178; Shua¶¶161. As Dr. Stavrou admitted, when a snapshot is

analyzed it “doesn’t have active processing” and so “it would not be possible to communicate messages or packets to it as described in Ranum.” Ex.2172, 256:11-257:17, 257:20-258:6 (“because a snapshot is a data file, does not have any active processing, it would not be possible to communicate messages or packets to it as described in Ranum? A. **That is correct.**”), 276:21-277:2 (no declaration opinion Ranum’s “active scanners can be used to analyze snapshots”).

As Dr. Stavrou testified, a POSA would have known that Veselov “happens differently” than Ranum, and the best Dr. Stavrou could come up with was that “it doesn’t mean that [combining with Ranum] cannot happen.” Ex.2172, 257:13-19. That is not the standard. Wiz’s failure to address Ranum’s incompatibility with snapshot based assessments as claimed demonstrates Wiz’s “impermissible *ex post* reasoning” to try to reconstruct the challenged claims. *TQ Delta LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1361 (Fed. Cir. 2019); *Intel Corp. v. PACT XPP Schweiz AG*, No. 2022-1038, 2023 WL 2198649, at *3 (Fed. Cir. Feb. 24, 2023); *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 165 (Fed. Cir. 2021); *Kaeli* ¶¶173-178.

Wiz asserts “snapshot-based VM assessments typically analyzed the same types of data as in Ranum’s network scan (e.g., files)” and “Veselov and Mohanty teach similar comparison techniques.” Pet.58-59 (citing Ex.1002 ¶¶240-241). Wiz relies on Dr. Stavrou, whose testimony should be given little weight considering his

attempts to evade answering as to his declaration opinions. *See, e.g.,* Ex.2172, 272:21-273:18 (Stavrou: “*I don’t want to give you any precise answer* in the sake of saving time”), 274:12-18 (“my declaration is not meant to be inclusive”), 274:20-276:2. Even if credited, Dr. Stavrou’s testimony at best suggests Veselov, Mohanty and Ranum are analogous art, not a sufficient motivation to combine them. *Johns Manville*, IPR2018-00827, Paper 9 at 10; *see TQ Delta*, 942 F.3d at 1360.

Further, Wiz and Dr. Stavrou’s assertion that Veselov, Mohanty and Ranum detect the “same types of data” is not true. Pet.58; Kaeli¶177. POSAs would have understood Mohanty’s agent-based “vulnerability assessment tools,” Ranum’s “network scanners,” and Veselov’s agentless “snapshot” based analyses inspect virtual cloud assets in fundamentally different ways. Kaeli¶177; *see* Ex.2172, 252:11-18 (admitting “some of” the data “Veselov analyzes and what Ranum is talking about” are not “similar,” and the data is “not identical”) *see* §IV.C (discussing Mohanty/Veselov). Wiz itself has, outside of this IPR, remarked how “Agents” and “Network Scanners” were “existing solutions” that were “very complicated to get complete visibility,” in contrast with “agentless scanning” that was a “different approach” Ex.2182. And both Ranum and Mohanty’s techniques require interactions with the running asset being analyzed, 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¶¶177.

1. Wiz’s Ground 2 Art Does Not Render Obvious Dependent Claims 2 and 4

Wiz argues that a POSA would have combined Veselov and Mohanty with Ranum to arrive at the additional requirements of claims 2 and 4. Wiz is wrong.

For Claim 2, Wiz contends Ranum teaches “determining an unexpected change in the data stored on the virtual disk.” Pet.63. But Ranum performs that comparison to identify “malware signatures,” which is not “**the** data stored on the virtual disk” that takes its antecedent basis from limitations 1.4, 14.4, 15.4. *Compare* Pet.63-64, *with id.* 61-62 (no reliance on “malware” for limitations 1.4, 14.4, 15.4). Wiz does not explain why a POSA would have or could have applied malware signature techniques to arrive at the claims. Kaeli¶¶180-182.

Claim 4 recites “detecting **the** data stored on **the** virtual disk by computing a cryptographic hash ...,” which takes its antecedent from the virtual disk in claim 1 undergoing a snapshot analysis. Kaeli¶¶180-182. That differs from Wiz’s cited portions of Ranum, which use “cryptographic hashes” to “index[] one or more **trusted file systems** ... known to have no malware infections.” Ranum, 17:1-9; *see*

also id. 17:9-20⁹, 17:21-23, 17:49-54. Dr. Stavrou admitted those trusted file systems “aren’t the running systems in the network.” Ex.2172, 261:18-22. Thus, they are not relevant to claim 4, because they are not cryptographic hashes of a virtual cloud asset undergoing a security assessment. Kaeli¶¶180-182.

Ranum also discusses using “hashes” in the context of “active scanners” that “perform a credentialed scan.” Ranum, 17:54-63. But the purpose of these scans is to detect processes “**running** on managed hosts.” *Id.*; Ex.2172, 259:13-17. That is not applicable to Veselov’s teachings about analyzing snapshots, as in the proposed combination, because a POSA would have understood the snapshots have no active processing to detect using Ranum’s techniques. Ex.2172, 256:11-258:6; Kaeli¶¶180-182. To the extent active scanners could be applied to Veselov, which Wiz does not articulate, a POSA would not have had a reasonable expectation of success in the combination because it would change the basic principles of Veselov and require interactions with an active machine Veselov seeks to avoid. Veselov, Abstract, 12:21-43, 2:54-63, 17:9-12; Kaeli¶¶173-178; *Plas-Pak Indus., Inc. v. Sulzer Mixpac*

⁹ Dr. Stavrou showed his lack of credibility on this subject, testifying Ranum’s statement “**clean** system shipped from a suitable vendor that can be **trusted to have no malware** on it” (Ranum 17:9-20) “doesn’t say if it does or doesn’t” have malware. Ex.2172, 264:6-265:7; *see also id.* 265:15-266:18.

AG, 600 F. App'x. 755, 759 (Fed. Cir. 2015). Accordingly, a POSA would have been led away from combining Ranum's teachings with the "snapshot-based virtual disk analysis" in Wiz's proposed combination. Pet.64; Ex.2172, 256:11-258:6; Kaeli¶¶173-178.

G. Grounds 3-6 fail for at least the reasons as Grounds 1-2

Grounds 3-4 addresses only dependent claim 3, and Grounds 5-6 address only the requirements of dependent claim 11, and otherwise rely on Wiz's arguments and motivations to combine for Grounds 1-2. Pet.57, 70. Thus, if Grounds 1-2 are rejected, Grounds 3-6 should be rejected too.

Wiz's Ground 3-4 arguments should also be rejected because the combination pieces disparate teachings of three or four references together without sufficient articulated rationale. *See InTouch Techs., Inc. v. VGO Commc'ns, Inc.*, 751 F.3d 1327, 1349 (Fed. Cir. 2014). Wiz's generic motivations to combine do little other than look at all of the prior art "like separate pieces of a simple jigsaw puzzle" without sufficiently "explain[ing] what reason or motivation one of ordinary skill in the art at the time of the invention would have had to place these pieces together." *Id.* Contrary to Wiz's assertion that Seo is just like Mohanty, Veselov and Ranum (which references are not similar as discussed in Grounds 1-2), Seo principally discusses "an artificial intelligence (AI) system which mimics recognition and judgment of the human brain." Seo (Ex.1094) ¶2; *see also id.* ¶¶3-8; Kaeli¶163. Seo

describes applicability of its AI model to “cyber security threats such as malware” (see Pet.66), but “malware” is not one of the cyber threats based on data recited in the challenged claims. In Wiz’s combination, Wiz appears to disregard the focus of Seo’s disclosures (an AI model), instead taking only the portion of the reference that relates to analyzing “installation records.” Pet.66-69. Kaeli¶183-191. Such an analysis is improperly rooted in hindsight and the “temptation to read into the prior art the teachings of the invention in issue.” *Abbott Laboratories v. Sandoz, Inc.*, 544 F.3d 1341, 1348 (Fed. Cir. 2008).

As to Grounds 5-6, Wiz turns to Hutchins for “quarantining VMs.” Pet.70. But, POSAs looking to Hutchins would have been led away from what is claimed. Hutchins describes offloading resource-intensive virus scanning assessments applications to replicated VMs, not analyzing a snapshot to determine cyber threats based on data. *See, e.g.*, Hutchins, Abstract, ¶¶7, 20; *see also* Kaeli¶¶194-196; Shua¶¶164-166. Wiz does not sufficiently explain why a POSA would have disregarded Hutchins virus inspection technique and selectively applied only the “quarantining” aspect of the reference to its proposed three and four reference combination in the absence of hindsight. *Abbott*, 544 F.3d at 1348.

V. CONCLUSION

Orca respectfully requests 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)(1) because the Patent Owner's Response contains 13,974 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)(1).

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.