

Filed on behalf of: Orca Security Ltd.

Entered: May 9, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-01191
U.S. Patent 11,775,326 B2

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The '326 Patent Improved Cloud Security Systems	4
A.	Problems with the Prior Art	4
B.	The '326 Patent's Innovative Cloud Security Systems.....	5
III.	Claim Construction.....	7
A.	“Analyzing the Snapshot”	7
IV.	Challenged Claims 1-21 and 28 Are Nonobvious Over Veselov and Basavapatna (Ground 1)	9
A.	POAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov and Basavapatna	9
1.	Overview of Veselov	10
2.	Overview of Basavapatna	11
3.	Wiz's Motivations To Combine Veselov and Basavapatna Should Be Rejected	12
B.	Veselov and Basavapatna Fail to Disclose or Suggest Multiple Limitations In Dependent Claims 6, 8 and 14.....	26
C.	Objective Evidence Demonstrates and Confirms the Non- obviousness 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 '326 Patent	37
3.	The Claimed Inventions Defied Skeptics, and Became Widely-Accepted in the Industry	41
4.	The Industry Praised Orca's Revolutionary Inventions.....	43
5.	Wiz Copied Orca's Inventions.....	48

6.	Orca's And Wiz's Commercial Success Demonstrates Non-obviousness	62
V.	Challenged Claims 4-5 and 17 Are Nonobvious Over Veselov, Basavapatna, and Czarny (Ground 2)	66
VI.	Challenged Claims 22-27 Are Nonobvious Over Veselov, Basavapatna, and Giakouminakis (Ground 3)	66
A.	POSAs Would Not Have Combined, or Reasonably Expected to Succeed in Combining, Veselov, Basavapatna, and Giakouminakis	67
B.	Ground 3 Does Not Show Obviousness of Challenged Claims 22-27	69
VII.	Conclusion	69

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

<i>ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	21, 23, 68
<i>Adidas AG v. Nike, Inc.</i> , 963 F.3d 1355 (Fed. Cir. 2020)	15
<i>Allen Archery, Inc. v. Browning Mfg. Co.</i> , 819 F.2d 1087 (Fed. Cir. 1987)	41
<i>Apple Inc. v. Samsung Elecs. Co.</i> , 839 F.3d 1034 (Fed. Cir. 2016) (en banc)	34, 43, 45
<i>Arctic Cat Inc. v. Polaris Indus., Inc.</i> , 795 F. App'x 827 (Fed. Cir. 2019)	23
<i>Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.</i> , 796 F.2d 443 (Fed. Cir. 1986)	23
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	18, 30
<i>Bettcher Indus., Inc. v. Bunzl USA, Inc.</i> , 661 F.3d 629 (Fed. Cir. 2011)	31
<i>Brown & Williamson Tobacco Corp. v. Philip Morris Inc.</i> , 229 F.3d 1120 (Fed. Cir. 2000)	65
<i>Chemours Co. FC, LLC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	65
<i>Fromson v. Advance Offset Plate, Inc.</i> , 755 F.2d 1549 (Fed. Cir. 1985)	4
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006)	17
<i>In re NTP, Inc.</i> , 654 F.3d 1279 (Fed. Cir. 2011)	24

<i>Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	25
<i>Iron Grip Barbell Co. v. USA Sports, Inc.</i> , 392 F.3d 1317 (Fed. Cir. 2004)	49
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	4, 13
<i>Liqwd, Inc. v. L'Oreal USA, Inc.</i> , 941 F.3d 1133 (Fed. Cir. 2019)	48
<i>Medtronic, Inc. v. Teleflex Innovations S.à.r.l.</i> , 70 F.4th 1331 (Fed. Cir. 2023)	33, 48, 49, 57
<i>Metalcraft of Mayville, Inc. v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	3
<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)	64
<i>Personal Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	16
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	24, 62, 69
<i>Power-One, Inc. v. Artesyn Techs., Inc.</i> , 599 F.3d 1343 (Fed. Cir. 2010)	66
<i>Rambus Inc. v. Rea</i> , 731 F.3d 1248 (Fed. Cir. 2013)	33
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	4, 57, 62
<i>Trivascular, Inc. v. Samuels</i> , 812 F.3d 1056 (Fed. Cir. 2016)	16

<i>Unigene Laboratories, Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	13
<i>WBIP, LLC v. Kohler Co.</i> , 829 F.3d 1317 (Fed. Cir. 2016)	<i>passim</i>

Exhibit List

Exhibit	Description
2001	Declaration of David R. Kaeli, Ph.D. (“Kaeli Decl.”)
2002	<i>Curriculum Vitae</i> of David R. Kaeli, Ph.D.
2003	Trend Micro™ vmware®, <i>Trend Micro Enterprise Security: Changing the Game for Anti-Virus in the Virtual Datacenter</i> (White Paper) (Sept. 2010), https://www.kennisportal.com/wp-content/uploads/2022/06/ChangingtheGameintheVirtualDatacenter.pdf (last visited Sept. 7, 2024) (“vmware, <i>Trend Micro Enterprise Security</i> ”)
2004	Red Hat, <i>Red Hat Virtualization 4.0: Technical Reference: The Technical Architecture of Red Hat Virtualization Environments</i> (updated Mar. 29, 2018), https://docs.redhat.com/en-us/documentation/red_hat_virtualization/4.0/pdf/technical_reference/Red_Hat_Virtualization-4.0-Technical_Reference-en-US.pdf (“Red Hat Virtualization 4.0”)
2005	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”)
2046-2047	RESERVED
2048	Wiz, Inc.’s Answering Claim Construction Brief, <i>Orca Sec. Ltd. v. Wiz, Inc.</i> , No. 1:23-cv-00758 (D. Del. Oct. 22, 2024) (excerpt) (“Answering Claim Constr. Chart”)
2049	Appendix F, Invalidity of United States Patent 11,775,326 (the “326 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
2050	Appendix F-1, Invalidity of United States Patent 11,775,326 (the “326 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)
2051	Declaration of Douglas E. Lumish Pursuant to 37 C.F.R. § 42.10(c)(2)
2052	Declaration of Steven W. Peters In Response to Petitioner’s First Objections to Evidence [<i>served, not filed</i>]
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=tlS0A92IYm8
2087	The Matias Experiment, <i>Ep398: Avi Shua CEO & Co-Founder, Orca Security</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=M58n3oE6E1Y

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=QdBsE2VqjpU (first made available Apr. 21, 2020)
2096	<i>Create AWS Policy</i> (last visited Mar. 19, 2025), https://www.youtube.com/watch?v=OdtXqrvbEdU (first made available June 11, 2019)
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> , ISSA Journal (Mar. 20, 2019), https://issa.mydigitalpublication.com/articles/the-quest-for-visibility-and-control-in-the-cloud
2138	Josh Dreyfuss, <i>Agents Are Not Enough: Why Cloud Security Needs Agentless Deep Scanning</i> (Sept. 28, 2021), https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning
2139	Michael Novinson, <i>Orca Security Raises \$340M To Scale Platform R&D</i> , Channel (Oct. 5, 2021), https://www.crn.com/news/security/orca-security-raises-340m-to-scale-platform-r-d-channel
2140	Elias Terman, <i>From Stealthy Startup to Cloud Security Innovation Leader</i> (Feb. 4, 2021), https://orca.security/resources/blog/2020-recap/

Exhibit	Description
2141	Kyle Wiggers, <i>Cloud Security Startup Wiz, Now Valued at \$10B, Raises \$300M</i> (Feb. 27, 2023), https://techcrunch.com/2023/02/27/cloud-security-startup-wiz-now-valued-at-10b-raises-300m/
2142	Rohan Goswami et al., <i>Wiz Walks Away from \$23 Billion Deal with Google, Will Pursue IPO</i> (July 22, 2024), https://www.cnbc.com/2024/07/23/google-wiz-deal-dead.html
2143	<i>SINET16 Previous Winners</i> (last visited Mar. 20, 2025), https://www.security-innovation.org/sinet16-award/past-award-winners/
2144	<i>SINET16 Innovator Award</i> (last visited Mar. 20, 2025), https://www.security-innovation.org/sinet16-award/
2145	<i>CISO Choice Award Winners 2020</i> (Nov. 19, 2020), https://securitycurrent.com/ciso-choice-awards-winners-2020/
2146	RESERVED
2147	Alan Schindel, <i>Detect and Prioritize CISA Known Exploited Vulnerabilities in the Cloud with Wiz</i> (Feb. 10, 2022), https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz
2148	Chris Ray, <i>GigaOm Radar for Cloud Workload Security</i> (Jan. 15, 2025), https://gigaom.com/reprint/gigaom-radar-for-cloud-workload-security-241089-check-point/
2149	Provisional Patent Application No. 62/797,718
2150	<i>Azure Onboarding with Orca Security Orca Security and Its Partners</i> (last visited Mar. 23, 2025), https://www.youtube.com/watch?v=zw091YvbjsI
2151-2157	RESERVED

Exhibit	Description
2158	Amazon Web Services, <i>Viewing Recent Management Events with the Console</i> (last visited Apr. 3, 2025), https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events-console.html
2159	Amazon Web Services, <i>Policies and Permissions in AWS Identity and Access Management</i> (last visited Apr. 3, 2025), https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
2160	Alon Weiss & Jiong Liu, <i>Uncover What Is Really Deployed in Your Environment with the Enhanced Wiz Inventory</i> (Dec. 8, 2022), https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory
2161	Joint Proposed Protective Order
2162	Redline Comparison between Joint Proposed Protective Order and Default Protective Order
2163-2164	RESERVED
2165	Wiz Experts Team, <i>Vulnerability Scanning: How It Works, Why It Matters, and What You'll Find</i> (Sept. 30, 2024), https://www.wiz.io/academy/vulnerability-scanning
2166-2167	RESERVED
2168	Wiz, <i>Agentless and Cloud-Native Vulnerability Management</i> (last visited May 5, 2025), https://www.wiz.io/solutions/vulnerability-management
2169	Thomas Nuth et al., <i>The Essential Steps for Cloud Vulnerability Management</i> (Oct. 30, 2024), https://www.wiz.io/blog/essential-steps-for-cloud-vulnerability-management
2170	Shaked Rotlevi, <i>Vulnerability Prioritization in the Cloud: Strategies + Steps</i> (Sept. 12, 2024), https://www.wiz.io/academy/vulnerability-prioritization

Exhibit	Description
2171	RESERVED
2172	Transcript of Deposition of Angelos Stavrou, Ph.D., taken April 2, 2025 ("2nd Stavrou Tr.")
2173-2188	RESERVED
2189	U.S. Patent Application Pub. No. 2020/0244678 A1
2190-2299	RESERVED
2300	Excerpt from Orca Product Documentation (2024) [PROTECTIVE ORDER MATERIAL]
2301	<i>API Onboarding with GCP Multi Scanner for In-Account</i> [PROTECTIVE ORDER MATERIAL]
2302	REDACTED [PROTECTIVE ORDER MATERIAL]
2303	REDACTED [PROTECTIVE ORDER MATERIAL]
2304	<i>AWS Permissions</i> [PROTECTIVE ORDER MATERIAL]
2305	RESERVED
2306	REDACTED [PROTECTIVE ORDER MATERIAL]
2307	REDACTED (May 27, 2019) [PROTECTIVE ORDER MATERIAL]
2308	REDACTED [PROTECTIVE ORDER MATERIAL]

Exhibit	Description
2309	REDACTED [PROTECTIVE ORDER MATERIAL]
2310	RESERVED
2311	Excerpt from Orca Product Documentation (2024) Part 2 [PROTECTIVE ORDER MATERIAL]
2312	REDACTED [PROTECTIVE ORDER MATERIAL]
2313-2399	RESERVED
2400	REDACTED [PROTECTIVE ORDER MATERIAL]
2401	REDACTED [PROTECTIVE ORDER MATERIAL]
2402	REDACTED [PROTECTIVE ORDER MATERIAL]
2403	REDACTED [PROTECTIVE ORDER MATERIAL]
2404	REDACTED PROTECTIVE ORDER MATERIAL]
2405	REDACTED [PROTECTIVE ORDER MATERIAL]
2406	REDACTED PROTECTIVE ORDER MATERIAL]
2407	REDACTED [PROTECTIVE ORDER MATERIAL]
2408	REDACTED [PROTECTIVE ORDER MATERIAL]

Exhibit	Description
2409	REDACTED ROTECTIVE ORDER MATERIAL]
2410	REDACTED [PROTECTIVE ORDER MATERIAL]
2411	REDACTED [PROTECTIVE ORDER MATERIAL]
2412	REDACTED [PROTECTIVE ORDER MATERIAL]
2413	REDACTED [PROTECTIVE ORDER MATERIAL]
2414	REDACTED [PROTECTIVE ORDER MATERIAL]
2415	REDACTED [PROTECTIVE ORDER MATERIAL]
2416	REDACTED WIZ_0311825-833 [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]

Exhibit	Description
2422	REDACTED [PROTECTIVE ORDER MATERIAL]
2423	RESERVED
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 '326 Patent is a pioneering cybersecurity patent that Wiz argues—wrongly—would have been obvious. Contrary to Wiz's hindsight-driven reconstruction of the claimed inventions from the prior art, an unusual wealth of objective evidence demonstrates the '326 Patent claims novel inventions that have been adopted by leading companies, recognized as a major milestone that redefined the industry, and widely praised and copied, including by Petitioner Wiz.

Patent Owner Orca was founded in 2019 by Avi Shua, the sole inventor of the '326 Patent. Ex.2074 (Decl. of Avi Shua, "Shua") ¶¶2-3, 9-12. Drawing on decades of experience in the Israeli Intelligence Corps and the early computer security industry, Mr. Shua recognized significant shortcomings in preexisting cloud security solutions, including a failure to offer unobtrusive, comprehensive security solutions for dynamic cloud environments. *Id.* ¶¶4-8. This motivated him to establish Orca and "[i]ntroduce[] the concept of agentless side scanning," which was a "***genuinely genius innovation.***" Ex.2076, 7.¹ Mr. Shua secured his "genius" innovation in the '326 Patent's claims, and unveiled the claimed inventions to the world in Orca's agentless SideScanning™ technology. Shua ¶13.

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

This technology defied skeptics, amassed extensive praise from the industry, and resulted in immense commercial success, including over \$600M in investments and REDACTED for Orca and far more for Wiz's copycat technology. *See* §IV.C.6. Those in the industry praised Orca for having made a "big leap in cloud security with the introduction of its patented agentless SideScanning technique," calling it a "unique method" that "gather[s] crucial data through the cloud provider's APIs, while scanning disk snapshots." Ex.2076, 31. Orca's SideScanning™ redefined the cloud security industry to such an extent that the cloud security posture management ("CSPM") market "can be defined by pre and post-Orca." Ex.2076, 7. And Orca has been repeatedly recognized as one of the world's most innovative cloud security companies. *See* §IV.C.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) ("[O]bjective indicia of non-obviousness play an important role as a guard against ... hindsight" and "must be considered in *every* case.") (original emphasis).

REDACTED

As detailed below, Wiz's hindsight-driven obviousness combinations do not show the challenged claims are unpatentable because Wiz has not shown that a POSA would have and could have made its combinations. Even when combined, Wiz's combinations also fail to teach or suggest several challenged dependent claims. And the objective evidence refutes Wiz's attempts to "stitch[] together prior art patches into something" like the claimed inventions. *Metalcraft of Mayville, Inc.*

² Exhibits 2400-2422 and 2424-2428 are Wiz's confidential documents produced pursuant to Paper 27.

v. Toro Co., 848 F.3d 1358, 1367 (Fed. Cir. 2017). In the end, Wiz does nothing more than attempt, albeit unsuccessfully, to show each of the 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) ("A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art."); *see also id.* at 418-19 ("[I]nventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known."); *see also Fromson v. Advance Offset Plate, Inc.*, 755 F.2d 1549, 1556 n.3 (Fed. Cir. 1985) ("Only God works from nothing. Men must work with old elements."). Indeed, Wiz's "lauding of all the available prior art" has "a hollow ring when played against its disregard of that art and its copying of" Orca's patent-practicing SideScanning™ discussed below. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1541 (Fed. Cir. 1983); *see* §§IV.C.2, IV.C.5.

II. The '326 Patent Improved Cloud Security Systems

A. Problems with the Prior Art

The '326 Patent explains that as organizations "increasingly adapted their applications to be run from multiple cloud computing platforms," security solutions struggled to adapt. '326 Patent (Ex.1001), 1:21-46. 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 inaccuracies, a lack of access to data relevant to detecting security threats and vulnerabilities in dynamic cloud environments, a resulting inability to properly identify vulnerabilities and threats, and the time-consuming need to use cumbersome agents. *Id.*; *see also* Kaeli (Ex.2073) ¶¶35-42; §IV.C.1.

B. The '326 Patent's Innovative Cloud Security Systems

The '326 Patent's inventions solved the problems faced by preexisting security systems. '326 Patent, 2:18-19. In particular, the problems discussed above motivated Mr. Shua to found Orca and develop agentless side scanning technology (SideScanning™) and the inventions disclosed and claimed in the '326 Patent (Shua¶¶10-14)—cloud security systems and methods that, among other things, receive a request to scan a plurality of protected virtual cloud assets, and then, for each requested asset, determine “using an API or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a respective protected virtual cloud asset,” access “based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk,” analyze “the snapshot of the at least one virtual disk to determine existence of a plurality of cyber vulnerabilities,” determine “a risk associated with each of the determined potential cyber vulnerabilities,” determine “a risk level to the cloud computing environment,” and “report ... the

existence of potential cyber vulnerabilities” such that the assets “with the determined potential cyber vulnerabilities are prioritized based on associated risk levels.” *Id.* cls. 1, 15, 18.

These inventions neither use nor suffer from the problems that plagued traffic inspection, traffic monitoring, and intrusive agent-based solutions, and the industry considered them “genuinely genius.” Ex.2076, 7. In fact, Orca’s inventions were also recognized as “unique,” “like magic,” and “a big leap in cloud security,” including, as explained more below in §IV.C.4, with respect to the novel combination of claimed features in the ’326 Patent. *See, e.g.*, Ex.2076, 11 (“Orca launched the first version of agentless side scanning, which allowed deep visibility into cloud workloads without the need to install agents.”), 11-12 (“Agentless solutions ... leverage cloud APIs to snapshot underlying instance hard disks, copy them into the security vendor[']s account, where they’re hooked up on the vendor’s side and scanned,” which “creates an elegant ‘like magic’ approach.”), 31 (“Orca Security made a big leap in cloud security with the introduction of its patented agentless SideScanning technique,” a “unique method” that “gather[s] crucial data through the cloud provider’s APIs, while scanning disk snapshots”). REDACTED

REDACTED

see also §§IV.C.1, IV.C.4; Kaeli¶¶172-176.

III. Claim Construction

Wiz's prior art fails to render obvious the subject matter of the challenged claims under any reasonable construction of their terms, including their plain meanings, as well as the constructions Wiz proposes (Pet.8-10). *See* Kaeli¶¶70-155. Nevertheless, Wiz's interpretation of the "analyzing the at least one snapshot" term should be rejected.

A. "Analyzing the Snapshot"

Wiz argues that limitations in independent claims 1, 15, and 18 reciting "analyzing the snapshot" ... encompasses [1] direct analysis of the snapshot data ... and [2] analysis of a VM instantiated from a snapshot." Pet.10. Wiz is wrong as to [2]. The only support Wiz cites for its incorrect contention that "analyzing [a] snapshot" encompasses "analysis of a VM instantiated from a snapshot" are allegations in Orca's amended complaint from district court. *Id.* (citing Ex.1006, 23, 57-58). Nothing in Orca's allegations, however, states or otherwise indicates that analyzing a VM instantiated from a snapshot is "analyzing [a] snapshot" as claimed. *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 would have been readily apparent to POSAs based on the '326 Patent's claims and specification. '326 Patent, cls. 1, 15, 18 (“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 (“[A]n instantiated VM is not a snapshot.”). The specification also distinguishes analyzing a snapshot by a “security system 140 to detect vulnerabilities” ('326 Patent, 5:20-21), as claimed, from a system that “instantiate[s] a copy of the VM” and performs “execution of the instance of the VM [in] an isolated sandbox” (*id.* 5:56-6:5). *See also id.* 7:41-52.

Tellingly, Wiz's expert, Dr. Stavrou, never supported and has now directly contradicted Wiz's interpretation. Dr. Stavrou just “*assume[d]* that ‘[analyze/analyzing] the snapshot’ also encompasses analysis of a VM instantiated from the snapshot”—blindly and without any supporting evidence or analysis, because he was “instructed by [Wiz's] counsel to assume this.” Ex.1002 ¶82; Ex.2077 (“1st Stavrou Tr.”) 265:17-266:4, 266:13-267:15 (“I didn't ask why. I was asked to assume.”), 267:16-268:3 (“I don't have an opinion why that was included or not.”), 268:4-269:20; Ex.2172 (“2nd Stavrou Tr.”) 38:7-20 (“analyzing the

snapshot” meaning “direct analysis of the snapshot data” is “consistent with the ’926 specification”). And Dr. Stavrou admitted that “[n]othing” in Veselov’s description of “assessing or analyzing an actual running instantiated virtual machine” “refers to analyzing a snapshot.” 1st Stavrou Tr.280:8-281:1. Wiz’s errant interpretation should be rejected. Kaeli ¶¶44-48.

IV. Challenged Claims 1-21 and 28 Are Nonobvious Over Veselov and Basavapatna (Ground 1)

Wiz fails to show that claims 1-21 and 28 would have been obvious over Veselov and Basavapatna. First, Wiz fails to demonstrate both that POSAs would have been motivated to combine the teachings of Veselov and Basavapatna to achieve the claimed inventions of the ’326 Patent and would have had a reasonable expectation of success in doing so. *See* §IV.A. Second, even if Wiz’s Veselov-Basavapatna combination is accepted (it should not be), the combination fails to teach or suggest multiple limitations in the challenged claims. *See* §IV.B. Third, objective indicia of non-obviousness refute Wiz’s hindsight-driven combination and improper piecemeal analysis. *See* §IV.C.

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

Wiz’s combination of different systems and methods from Veselov and Basavapatna, with unrelated goals and contradictory teachings, is unsupported by

any rationale sufficiently demonstrating a POSA's motivation to combine these references.

1. Overview of Veselov

Veselov's overarching goal is to perform security assessments of target VMs while avoiding downtime of those machines and reducing assessment complexity. Kaeli¶¶49-59; *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." Veselov, Abstract, 12:21-43; *see also id.* 2:54-63, 17:9-12.

To facilitate its security assessment, Veselov's scanning system "obtains, or obtains access to a state of the resource at a point in time (e.g., a 'snapshot')," which is then "prepared so that the security assessment produces the result that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance." Veselov, 3:20-27, 4:1-4. Veselov illustrates five high level embodiments of its system in Figures 1, 3A, 3B, 5A and 5B, each with distinctly different features and/or techniques, none of which are arranged as claimed in the '326 Patent. Kaeli¶¶49-59 (Veselov Overview); Shua¶¶151-158 (explaining how Veselov differs from the claimed inventions). The Petition

disregards all such distinctions, improperly lumping all of Veselov's disclosures together and using the '326 Patent as a roadmap to select from among Veselov's myriad and disparate techniques. Yet, none of Veselov's embodiments teach determining a risk associated with potential cyber vulnerabilities, determining a risk level of a virtual cloud asset, or reporting the existence of potential cyber vulnerabilities prioritized by risk levels, among other features recited in the challenged dependent claims. Kaeli¶¶49-59; 1st Stavrou Tr.97:13-98:10.

2. Overview of Basavapatna

Unlike Veselov or the challenged '326 Patent, Basavapatna does not discuss snapshots, snapshot based security assessments, nor applying security assessments to any cloud based systems or "virtual" assets. 2nd Stavrou Tr.220:20-221:3 ("Q. ... Basavapatna is directed to security assessments of physical computing assets; right? A. Correct."), 221:15-222:12 (agreeing no disclosure of "virtual" assets); Kaeli¶¶60-67. Instead, Basavapatna discloses techniques for on-premises security assessments of physical assets in a network using "sensors" to "identify vulnerabilities" and "monitor the network traffic passing through the input/output subsystem." Basavapatna (Ex.1008), Cover, ¶¶2 (defining security assessments on "a computer or other electronic device"), 26-28.

Basavapatna's "sensors" used to detect vulnerabilities take one of two forms: (1) "host-based sensors" and/or (2) "network-based sensors." Basavapatna, ¶¶26-

28; 2nd Stavrou Tr.223:21-224:3, 228:9-16 (“A. These are the two types of sensors that are discussed. That’s correct.”). Basavapatna’s “host-based sensors” are security agents that are “actually installed on the machine being analyzed.” 2nd Stavrou Tr.224:20-225:2. And Basavapatna’s “network-based sensors” consist of hardware devices and/or software in “a data communication path between assets 104 protected by the sensor and the network resources that the asset is attempting to access” and which “monitor the network traffic passing through the input/output subsystem.” Basavapatna ¶¶26-28; 2nd Stavrou Tr.225:8-16. “The host-based sensors 108 and the network based sensors 110 monitor the assets themselves and/or network traffic to and from the assets.” Basavapatna ¶23. Tellingly, Basavapatna’s agent-based and network-scanner techniques are precisely the techniques that the ’326 Patent acknowledges as inadequate, and which the ’326 Patent improves upon. Kaeli¶¶60-67 (Basavapatna Overview); Shua¶¶159-161 (explaining how Basavapatna differs from the claimed inventions). Basavapatna also discusses techniques for determining a “risk metric for each asset and each threat,” but only in the context of analyzing information received from host-based or network-based sensors. Kaeli¶¶60-67.

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

Wiz argues arriving at the claims would have been obvious because Veselov taught “[l]ocating/accessing/analyzing a snapshot of a virtual disk to identify

vulnerabilities and reporting/mitigating identified security problems” and Basavapatna separately taught “[d]etermining vulnerability/asset risks, determining application usage, and reporting/prioritizing/filtering results based on associated risk levels.” Pet.21. It is black letter law, however, that even if “separate references cover[] each separate limitation in a claim under examination, 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 418, 421). Wiz has not made that showing here.

a. Basavapatna's Agent-Based Techniques are Incompatible with Veselov's Snapshot Assessments

First, Wiz contends that applying Basavapatna's techniques “in snapshot-based VM assessments would not meaningfully change their function or result.” Pet.22 (citing Ex.1002 ¶108). Dr. Stavrou asserts a “POSA would have recognized that Basavapatna's security-assessment techniques would operate similarly in the context of Veselov's snapshot-based security assessments of virtual cloud assets taught by Veselov.” Ex.1002 ¶108. Wiz and Dr. Stavrou are wrong.

POSAs would have understood that Basavapatna's “security-assessment techniques” are inapplicable to snapshot-based VM assessments. Kaeli¶¶75-101. As discussed in §IV.2, the only security assessment techniques disclosed by

Basavapatna are based on one of two types of “sensors,” (1) “host-based sensors 108” (i.e., security agents installed on the resource) that “monitor the assets themselves” and (2) “network-based sensors 110” (i.e., network scanners) that monitor “network traffic to and from the assets.” Basavapatna ¶23; 2nd Stavrou Tr.223:21-224:3, 228:9-16; Kaeli¶¶89-98. The “host-based sensors 108” “identify vulnerabilities on the assets 104 or ... identify viruses or other malware executing on the assets 104.” Basavapatna ¶26. The “network-based sensors” analyze “information being sent or received” when “an asset 104 tries to send information through the network 106 or receive information over the network 106.” Basavapatna ¶¶27-28.

Dr. Stavrou admitted on cross-examination that neither of Basavapatna's agent-based nor network scanner security assessments could be applied when analyzing a snapshot, as disclosed in Veselov's Figures 5A/5B embodiments and required by the claims of the '326 Patent. *First*, Dr. Stavrou admitted that “an agent can only be installed on a virtual machine” and “I don't think that an agent can be installed on a snapshot.” 2nd Stavrou Tr.53:14-20. So Basavapatna's security assessments using host-based sensors, which Dr. Stavrou conceded are security agents that are “actually installed on the machine being analyzed” (*Id.* 224:20-225:2), could not operate in the proposed combination. Kaeli¶¶86-98; Shua¶161. *Second*, Basavapatna's security assessment techniques using “network-based

sensors” analyze “information being sent or received” when “an asset 104 tries to send information through the network 106 or receive information over the network 106.” Basavapatna ¶¶27-28. But such techniques are entirely unavailable in snapshot based assessments, as Dr. Stavrou conceded: it “would not be possible to send or communicate packets or other messages to a snapshot” because a snapshot “doesn’t have active processing.” 2nd Stavrou Tr.256:21-257:3; Kaeli¶¶99-101; Shua¶¶150, 161.

As a result, a POSA reading Basavapatna would have understood its techniques relying on “host sensors” and “network sensor[s]” are inapplicable to snapshot-based analyses, which would have led a POSA away from the claimed inventions. Kaeli¶¶75-101. To the extent it would have been possible to modify Basavapatna’s techniques to be applied to snapshot based assessments, Wiz has entirely failed to acknowledge, let alone address, what those modifications would be as required. *Adidas AG v. Nike, Inc.*, 963 F.3d 1355, 1359-60 (Fed. Cir. 2020) (affirming Board’s nonobviousness determination where references described “fundamental differences in seaming techniques” and petitioner failed to “reconcile these differences” in its obviousness combination).

b. Wiz and Dr. Stavrou Do Not Demonstrate How the Purported Combination Would Work

Second, the Board found at institution that “Petitioner does not advocate for” a “bodily incorporation of Basavapatna’s specific agent-based analysis into

Veselov,” and instead seeks to add “Basavapatna’s teachings, for example, that ‘determining and reporting vulnerability/asset risks provides a more comprehensive risk assessment for the system.’” ID 24-25.³ Those assertions from Wiz, however, are inadequate because Wiz does not explain “*how* the combination of the two references was supposed to work.” *See Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 993-94 (Fed. Cir. 2017) (original emphasis); *see also Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016) (no error where Board required petitioner to explain how a POSA would have implemented combination).

Rather than addressing what its proposed combination entails, Wiz asserts that Veselov alone teaches the preambles, 18.i, 1.2.a-b, 15.2a-b, and 18.2a-b. Pet.25-31. Wiz then asserts Basavapatna alone teaches elements 1.2.c-d, 15.2.c-d, and 18.2.c-d. Pet.31-33. Wiz ostensibly asserts that “the combination” teaches elements 1.3, 15.3, and 18.3, but Wiz only discusses or cites to Basavapatna, without any reference to Veselov. Pet.34. Finally, for limitations 1.1, 1.4, 15.1, 15.4, 18.1 and 18.4, Wiz contends the “combination” teaches the elements, but Wiz simply separately

³ Orca does not suggest that Wiz must prove how a POSA would have “bodily incorporated” Basavapatna’s host/agent based sensors in Veselov, but rather that the differences between the references’ assessment techniques would counsel against combining them or arriving at the challenged claims. *Kaeli*, ¶¶85-103.

discusses each reference without identifying how the teachings of one apply to the other. Pet.34-36. This “mere identification in the prior art of each element is insufficient to defeat the patentability of the combined subject matter as a whole.” *In re Kahn*, 441 F.3d 977, 986 (Fed. Cir. 2006). Nor is it plain how such a combination would work, as Wiz’s reliance on Basavapatna’s “risk assessments” are inextricably tied to the outputs of host and network based sensors that could not be applied to a security system for analyzing snapshots as proposed in Wiz’s combination. *See, e.g.*, Basavapatna, Fig. 2, ¶¶34-36, 58, 65-66; Kaeli¶¶99-101.

For example, Wiz relies exclusively on Basavapatna’s “vulnerability-centric risk metric” and “threat-centric risk metric” to render obvious limitations 1.2.d, 15.2.d, and 18.2.d. Pet.33-34. But Wiz does not explain how or why (in the absence of hindsight) the data relied on in Basavapatna to generate risk metrics would be available in Veselov’s snapshot assessments that Wiz relies on for limitations 1.2a-b, 15.2.a-b, and 18.2.a-b. Kaeli¶¶99-103, 105. In particular, Basavapatna discloses that determining “vulnerability/asset risks” is dependent on processing by its “network monitor 102” which receives, e.g., “vulnerability detection data 206” and “configuration data 207” from “the assets and/or sensors themselves.” Basavapatna, ¶¶34, 36; 2nd Stavrou Tr.224:20-225:2 (Dr. Stavrou admitting Basavapatna’s host-based sensors are installed on the machine being analyzed). Without this host or network sensor-derived data, Basavapatna’s network monitor cannot perform its

“example process 300 for generating a threat-centric risk metric for an asset and a threat” or its “example process 350 for generating a vulnerability-centric risk metric for an asset and a vulnerability.” Basavapatna ¶¶72-119; Kaeli¶¶99-101.

Accordingly, Wiz has not shown how a POSA both could have and would have, in the proposed combination, arrived at limitations 1.2.d, 15.2.d, and 18.2.d. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015). This failure cascades to limitations 1.3, 15.3, and 18.3, for which Wiz relies on Basavapatna's “asset-level risk metric” which results from “aggregating the respective vulnerability-centric or threat-centric risk metrics” (Pet.34)—the underlying data needed to generate this asset-level metric is not available in Veselov's snapshot analyses. Kaeli¶¶99-101.

c. Basavapatna and Veselov Do Not Analyze Similar Data

Third, Wiz contends a POSA would have combined Veselov and Basavapatna because the references analyze “similar data” and thus would have “reasonably expected success” combining them. Pet.23. Wiz is wrong. It is *not* true that a POSA would have understood, prior to the '326 Patent, that Basavapatna's network sensor and agent-based techniques detect the same data as Veselov's agentless snapshot-based assessment techniques. Kaeli¶¶102-104. To the contrary, before Orca's inventions—and for years afterwards—the industry believed agentless scanning techniques that relied on “snapshot[s]” for security assessments were

“lightweight” and could only deliver “rudimentary security capabilities” in comparison with agent-based approaches. Ex.2106, 1-2. Those in the industry believed only agent-based security analyses, like proposed in Basavapatna, could provide detailed monitoring and protection. *Id.* It was only after Orca introduced its patent-practicing SideScanning technology in 2019 (*see* §IV.B) that the industry recognized the deep security assessment possible by analyzing snapshots located using cloud computing APIs. Kaeli ¶¶102-104; Ex.2076, 7 (explaining it was “difficult ... for older providers to come to terms with the success of agentless scanning” because they “didn’t know what they didn’t know”), 31 (Orca “made a big leap in cloud security with the introduction of its patented agentless SideScanning Technique in 2019” that gathered “crucial data through the cloud provider’s APIs, while scanning disk snapshots”); *see* §IV.C.3.

This understanding that agent-based approaches (e.g., Basavapatna) provided more detailed security analyses than agentless approaches is reflected in Veselov itself. Veselov teaches 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 ¶¶102-105; 2nd Stavrou Tr.49:11-20 (testifying only embodiments in Veselov that analyze the “snapshot itself” are Figures 5A-5B in columns 16-17); Ex.1002 ¶89.

In Veselov's "security agent" based assessment described in Figures 3A-3B, the agent can "apply tasks of the security assessment to real-time dynamic and static data, network connections, communications to computing resources, and other computational activities of the assessment virtual machine 312A-B." Veselov, 15:41-47; *see also id.* 15:29-38 ("install the security agent program 330 in the assessment virtual machine's 312A, B"), 14:22-36 ("installs a security agent program 330 into the assessment virtual machine 312A-B"). A security-agent based analysis of a duplicate VM can also include "intercept[ing] traffic" and "stimulat[ing] activity in the assessment virtual machine" allowing generation of "profile of the traffic to the target virtual machine." *Id.* 15:60-16:14. But, as discussed in §III.A above, analyzing an instantiated virtual machine cannot satisfy the claimed "analyzing a snapshot." 2nd Stavrou Tr.38:7-20 ("analyzing the snapshot" meaning "direct analysis of the snapshot data" is "consistent with the" '326 patent), 39:4-40:1 (no opinion that claimed "analyzing the snapshot" encompasses analyzing virtual machines instantiated from a snapshot).

In contrast, Veselov teaches determining comparatively basic information when analyzing a snapshot, e.g., in Veselov's Figures 5A/5B embodiments, such as to "use string or other pattern comparisons 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, would not result in understanding the “network connections” or “communications to computing resources,” or any of the other “configuration” information Veselov teaches is available in an agent-based system. Kaeli¶100; *cf.* Veselov, 13:53-58, 15:41-47. Yet, it is this data that is absent from Veselov’s snapshot-based assessment techniques that Basavapatna’s risk assessments rely on. *See* Basavapatna ¶¶36-37; Kaeli¶100. Accordingly, the foundational aspects of Wiz’s contentions that the references would be combined—i.e., that snapshot-based assessments would provide “similar data” to an agent and network-sensor based approach of instantiated machines—are unsupported and Wiz’s obviousness argument should be rejected. *ActiveVideo Networks, Inc. v. Verizon Commc’ns, Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012).⁴

d. Wiz’s Hindsight-Tainted Picking and Choosing is Insufficient to Establish Obviousness

Fourth, even if a POSA would have been motivated to combine Veselov and Basavapatna generally, Wiz has failed to show why, in such a combination, a POSA would have cherry-picked the particular disclosures from each reference that would have resulted in a POSA arriving at the challenged claims. In particular, to the extent

⁴ Wiz’s references similarly indicate a difference between the data considered by live VM analyses compared to snapshot-based analyses. *See* Ex.1038, 134; Ex.1043 (comparing “in-the-box” and “out-of-the-box” approaches); Kaeli¶103.

Veselov and Basavapatna describe “analogous security assessments” (Pet.22), it is in the context of Veselov’s Figures 3A/3B embodiments that use “security agents” installed on an instantiated virtual machine to perform security assessments *instead of* analyzing a snapshot as discussed above. Veselov, 14:22-27 (“security agent program 330” installed into “assessment virtual machine 312A-B ... to monitor activity”), 14:41-53, 15:29-34, 16:45-53; Kaeli¶102. But a POSA considering Veselov and Basavapatna because of their “analogous security assessments” would have therefore been led *away* from the challenged claims, as it would have motivated a POSA to implement an agent-based security assessment technique of instantiated VMs. Kaeli¶102.

Wiz does not provide any basis why a POSA would have ignored what is purportedly “analogous” in the references, and in a combination instead cherry-pick portions of Veselov directed to alternative, non-analogous, techniques of analyzing snapshots *without* agents that would be incompatible with Basavapatna’s risk assessment techniques that rely on information *from* agents. Lacking any such explanation, the Board should conclude that Wiz’s obviousness arguments are the product of improper hindsight reconstruction using the challenged claims as a roadmap through the prior art. Kaeli¶102. Indeed, Wiz’s arguments relative to Basavapatna “ignore[] those portions of the reference that argue[] against

obviousness” and fail to appreciate the reference “in its entirety.” *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 448-49 (Fed. Cir. 1986).

e. Wiz's Motivation is Legally and Factually Inadequate

Fifth, Wiz's contention that a POSA “would have been motivated to provide more robust and accurate risk assessments” (Pet.22), is nothing more than an attempt to “create a problem with the prior art in hopes of creating a motivation to combine.” *Arctic Cat Inc. v. Polaris Indus., Inc.*, 795 F. App'x 827, 833 (Fed. Cir. 2019). Nothing in Veselov suggests that its system's reported “‘findings’ relative to the assessed properties” are inaccurate or lack robustness. Kaeli¶101. Veselov's “assessment results” can be evaluated by an “owner or administrator of the virtual machine” without issue and without any suggestion that such results are inadequate. Veselov, 4:5-8. The Federal Circuit has found similar contentions, e.g., that a proposed combination was “better” or “more efficient,” to be insufficient under *KSR* to show a motivation to combine. *ActiveVideo*, 694 F.3d at 1328. The same applies here. Wiz's arguments are “generic and bear[] no relation to any specific combination of prior art elements” (*id.*), and should thus be rejected.

Additionally, modifying Basavapatna's teachings so that it could be added to and operate with Veselov's system, even if technically possible, would add complexity to Veselov's system, which Veselov derides as a “drawback[] of existing security assessment systems.” Veselov, 2:42-46. Veselov's preferences for less

complex monitoring and assessment systems would have counseled against adding Basavapatna's risk assessments using host and network-based sensors. Kaeli¶101; *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069 (Fed. Cir. 2018) (“[E]ven if a reference is not found to teach away, its statements regarding preferences are relevant” to whether there is motivation to combine.).

f. Dr. Stavrou's Background References Fail to Bridge the Gap

Sixth, Wiz cites to thirteen tertiary references as purportedly supporting that the individual elements of the challenged claims were “known elements.” Kaeli¶¶106-122; *see* Pet.21-23 (citing myriad and disparate portions of Exs.1014, 1025, 1034, 1036, 1040, 1044, 1045, 1046, 1048, 1063, 1076, 1077, 1078). As Dr. Kaeli explains, none of these background references support Wiz's fundamental assertions that a POSA could have or would have applied Basavapatna's agent and network sensor-based risk assessments to Veselov's agentless snapshot-based assessments. And Wiz's retreat to a laundry list of background references simply reinforces that Wiz's obviousness rationales are based on an improper, hindsight-based use of the challenged claims “as a guide through [a] maze of prior art references.” *In re NTP*, 654 F.3d 1279, 1299 (Fed. Cir. 2011).

g. POSAs Would Not Have Expected Success in Combining Basavapatna and Veselov

Seventh, with respect to reasonable expectation of success, Wiz contends that, separately, “snapshot-based analysis, vulnerability detection, risk assessments, reporting, and risk-based prioritization were well known and routinely implemented.” Pet.23. But, Wiz bears the burden of demonstrating that POSAs would have had “a reasonable expectation of achieving *what is claimed in the patent-at-issue*” (*Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016))—i.e., cloud API or service based systems and methods that “determin[e] a risk associated with” multiple cyber vulnerabilities **from analyzing a snapshot** and “report[] ... the existence of the potential cyber vulnerabilities, such that the plurality of protected virtual cloud assets with the determined potential cyber vulnerabilities are prioritized based on associated risk levels.” ’326 Patent, cls. 1, 15, 18. In particular, as explained above, Wiz has not shown that a POSA would have reasonably expected to garner sufficient information from a snapshot to facilitate any type of cyber vulnerability risk determination, and Wiz has not shown that a POSA would have and could have modified Veselov’s snapshot-assessment embodiments to collect the data needed to apply Basavapatna’s teachings. Kaeli¶123.

B. Veselov and Basavapatna Fail to Disclose or Suggest Multiple Limitations In Dependent Claims 6, 8 and 14

In addition to the foregoing reasons why a POSA would not have been motivated to combine Veselov and Basavapatna to arrive at the challenged independent claims, Wiz has also failed to show that the combination renders obvious the additional requirements of dependent claims 6, 8, and 14.

a. Claim 6

Wiz fails to show that claim 6, which recites “determining the risk associated with one of the plurality of cyber vulnerabilities further comprises determining whether the one of the potential cyber vulnerabilities corresponds to an application that is in use by the respective protected virtual cloud asset” would have been obvious. Wiz relies exclusively on Basavapatna, which fails to render obvious this limitation. Pet.44-45.

Wiz alleges Basavapatna's “vulnerability-centric risk metric ... is based on a vulnerability detection score that may indicate whether the asset ‘is running’ the relevant software” and Basavapatna's “applicability score” indicates ““when the asset **is running** software’ exploited by the threat.” *Id.* 44. But Wiz ignores that a determination that an asset is “running” or “executing” software in Basavapatna is based on analyzing agent-based data of an executing physical machine. Basavapatna ¶26 (“host-based sensor 108b is installed on asset 104c ... run various analyses **on** their respective assets 104 ... to identify viruses or other malware **executing** on the

assets”); Kaeli¶¶127-133. Wiz’s proposed combination, however, requires Veselov analyzing the *snapshot* of a virtual machine (*see* Pet.32 (discussing Veselov, 17:10-29)), which Dr. Stavrou admitted has no “active processing” to analyze. 2nd Stavrou Tr.256:21-257:3. Wiz has not explained or shown how a POSA in the proposed combination would have therefore determined whether an application is “in use” as claim 6 requires.

Wiz then relies on a fallback argument that “[a]t a minimum, determining the risk based on application usage would have been obvious” citing tertiary references. Pet.44. Neither tertiary reference is part of Wiz’s ground and therefore should not be considered. Moreover, neither reference explains how analyzing a snapshot, as in the proposed combination, could be used to determine whether an application is used as part of a risk assessment of a snapshot-based analysis. Kaeli¶131 (explaining Hibbert (Ex.1063) relies on agents, like Basavapatna, and Hufsmith (Ex.1078) relates to pre-deployment container image analysis, not executing machines).

b. Claim 8

Wiz fails to show that claim 8, which recites “determining whether the matching installed applications are used by the respective protected virtual cloud asset includes checking configuration files of the matching installed applications to determine whether at least one of the matching installed applications is not in use,” would have been obvious. Wiz relies on Veselov and Basavapatna, but neither

reference individually or in combination renders obvious this claim. Pet.45-47. In particular, Wiz argues Veselov's assessment "considers configuration files of installed applications" citing multiple passages. But mere consideration of configuration files does not teach or suggest using configuration files "to determine whether at least one of the matching installed applications is not in use" as the claim requires. Kaeli¶138.

Recognizing this deficiency, Wiz turns to Basavapatna, alleging Basavapatna "teaches that the application-usage determination involves checking application configuration files." Pet.46. Wiz extends Basavapatna's teachings too far: while Basavapatna teaches that the "configuration of the asset can include ... the configuration of the software running on the asset" (Basavapatna ¶37), Wiz points to nothing in Basavapatna that mentions "configuration files of ... installed applications," nothing that teaches examining "configuration files" of applications, and nothing in Basavapatna that teaches examining "configuration files" to determine application usage. Kaeli¶139.

As its fallback, Wiz argues "[a]t a minimum, this would have been obvious since it was well known that systems typically stored configuration files indicating application usage." Pet.47 (citing Ex.1002 ¶216). But this too misses the mark: whether systems "typically stored configuration files" doesn't mean it was obvious to check such configuration files "to determine whether at least one of the matching

installed applications is not in use” as claimed, and Dr. Stavrou’s citation to a tertiary reference about the Windows registry does not read on the claim language or advocate that those teachings would have been obvious to incorporate into the Veselov-Basavapatna combination. Kaeli ¶¶140, 134-141.

c. Claim 14

Veselov is the only reference Wiz relies on for the additional requirements of dependent claim 14 (Pet.54-57), but Veselov neither teaches nor suggests “determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the location of a specific virtual disk of the respective protected virtual cloud asset.” *See* Kaeli ¶¶142-149.

Wiz concedes that Veselov only discloses computing environments that are implemented by a computing resource service provider (what Wiz contends is a “cloud computing environment”) in Figures 1 and 3A-B, but not in Figures 5A-B. Pet.54-55. Figures 5A and 5B, however, are the Veselov embodiment that analyzes a snapshot rather than an instantiated VM. In the non-cloud context of Figures 5A-B, where no computing resource service provider is depicted, however, Veselov explains that a snapshot of the virtual machine can be “obtained.” Veselov 18:18-21. Accordingly, a POSA would have understood that obtaining a snapshot is not itself a disclosure of “querying a cloud management console” for a snapshot, as there

is nothing inherent to locating a snapshot requiring a cloud environment. *See* Kaeli¶143. Wiz also does not provide any reason why a POSA would have been motivated to modify Veselov's snapshot-analysis embodiments to specifically query such information from a cloud management console.

Moreover, Wiz concedes that Veselov does not disclose *any* embodiment where a cloud management console is queried to locate a "specific virtual disk" as recited. Pet.56-57. Instead, Wiz contends this would have been obvious because certain embodiments teach that a "user" "can initiate the snapshot-analysis process" "using the UI to identify the target VM." *Id.* But "identifying the target VM" is not the same as, nor does it render obvious, querying the location of a virtual disk for at least two reasons. *See* Kaeli¶144.

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¶¶145-146. Wiz contends that "[m]anaging security [of] computer resources" "routinely involved querying consoles to determine resource locations" and was a "common step" (Pet.56), but that at best only addresses whether a POSA "*could* have" modified Veselov to include such a step, while entirely failing to address how or why a POSA "*would have been motivated to make*" such a change. *See Belden*, 805 F.3d at 1073 (original

emphases). Having failed to address any motivation in its Petition, Wiz's obviousness argument fails.

Second, as Dr. Stavrou admitted, "Virtual disks are different from virtual machines"—"[t]hey are definitely not synonymous." 1st Stavrou Tr.97:13-98:10. And, as the '326 Patent shows, VMs and virtual disks are typically in different locations. '326 Patent, 3:55-58, Fig. 1B; Kaeli¶146; 1st Stavrou Tr.92:4-93:19, 94:16-21. Thus, locating a VM does not necessarily or inherently specify the location of the virtual disk. *See* 1st Stavrou Tr.142:15-143:3 (Dr. Stavrou conceding he could not identify and was not aware of any disclosure in Veselov that "identifies or describes an identifier for a virtual disk"); Kaeli¶146.

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 (i.e., specific 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. Without such a description, Wiz's argument is essentially one of inherency, but Wiz does not (and cannot) show that a snapshot's location is "necessarily" stored in the same location as the virtual disk as required for inherency. *See Bettcher Indus., Inc. v. Bunzl USA, Inc.*, 661 F.3d 629, 639 (Fed. Cir. 2011). To the contrary, Veselov teaches in Figure 1's context 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¶¶143-144. And in Figures 3A, 3B, 4, 5A, 5B, Veselov teaches that the volume image may be *provided to* a hypervisor or service that launches an assessment machine, or may be read by the hypervisor to launch the assessment machine. Veselov, 12:37-51, 18:16-21.

And even if Veselov's 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 itself. *See ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1363 (Fed. Cir. 2018).

And, locating virtual disks was important to the commercial success of Orca's patent-practicing SideScanning techniques because it enabled Orca to deploy its security components in the same location as the virtual disk, which was critical for performance. Ex.2133, 1; Ex.2082, 8:06-11:08 (video from A. Shua describing how cloud “manufacturers moved to an architecture where the storage in fact sits physically on a different box”); Ex.2083 (transcript of Ex.2082); Ex.2099, 9:40-14:00; Ex.2133 (transcript of Ex.2099), 4 (describing performance benefits of determining location); Kaeli¶¶186-187, 194; Shua¶¶19, 88 (discussing Exs.2082-2083).

REDACTED

REDACTED

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

Objective evidence of non-obviousness “play[s] an important role as a guard against the statutorily proscribed hindsight reasoning in the obviousness analysis.” *WBIP*, 829 F.3d at 1328-30. Indeed, it “may often be the most probative and cogent evidence in the record,” and “must be considered in every case.” *Id.* at 1328 (emphasis omitted). While “objective evidence of nonobviousness lacks a nexus if it exclusively relates to a feature that was ‘known in the prior art,’ the obviousness inquiry centers on whether ‘the claimed invention as a whole’ would have been obvious.” *Id.* at 1330 (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257-58 (Fed. Cir. 2013)); *see also Medtronic, Inc. v. Teleflex Innovations S.à.r.l.*, 70 F.4th 1331, 1337 (Fed. Cir. 2023) (agreeing with the Board that demonstrating “every element” of the challenged claims “was individually known in the prior art” does “not preclude nexus where the evidence was ‘tied to the combination of features as a whole’ and the combination was not previously known) (quoting *WBIP*, 829 F.3d at 1331-32).

Here, it is undisputed that the challenged claims were not anticipated by the prior art—Wiz relies on only (hindsight-driven) obviousness challenges.

And evidence of long-felt, unsolved need, skepticism regarding the inventions, industry acceptance, industry praise, commercial success, and copying demonstrate and confirm the non-obviousness of the '326 Patent's claimed combinations. *See* §§IV.C.1-IV.C.5; *WBIP*, 829 F.3d at 1330 (“[W]e have explained that the patent owner can show that it is the claimed combination as a whole that serves as a nexus for the objective evidence; proof of nexus is not limited to only when objective evidence is tied to the supposedly ‘new’ feature(s).”).

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. *See generally* Shua¶¶85-95.

As leading technology companies like Amazon, Microsoft, and Google began providing and developing their public cloud services, many “[o]rganizations ... increasingly adapted their applications to be run from multiple cloud computing platforms.” ’326 Patent, 1:21-25; Ex.2076, 5-6 (describing “Shift to Cloud” beginning in 2010-2014); Ex.2134, 2 (“Cloud adoption takes off” around 2012). And, “virtualization technologies,” such as “virtual machines, software containers, and serverless functions,” were also “adapted by cloud computing platforms.” ’326

Patent, 1:39-46. Such technologies had computing advantages, but they were vulnerable to cyber threats. *Id.*; Ex.2136, 2 (“As more workloads are shifting to the cloud, cybersecurity professionals remain concerned about security of data, systems, and services in the cloud.”); Ex.1029, 1 (“[S]ecurity is the biggest problem of” cloud computing systems.). Accordingly, the cloud security industry developed various methods for protecting cloud computing infrastructures, including: (1) “traffic inspection,” (2) using “network scanner[s] deployed out of path,” (3) “traffic monitor[ing],” and (4) using “agents installed in each server.” ’326 Patent, 1:47-2:17.

However, these methods suffered from multiple disadvantages, as Mr. Shua explained both in the ’326 Patent and at multiple conferences and videos prior to these IPR proceedings. Shua¶¶87-90 (discussing ’326 Patent, 1:47-2:17 and Exs. 2082, 2083, 2099, 2100, 2133). “Traffic inspection may not provide an accurate indication of the security status of [a] server due to inherent limitations, such as encryption” and lack of access to pertinent data. ’326 Patent, 1:49-55. With network scanners deployed out of path, servers “may not respond” or “expose ... necessary data,” and network configuration- and credential-related issues can be problematic. *Id.*, 1:56-67. Traffic monitoring “detect[s] threats only based on the monitored traffic” and thus can miss server “misconfiguration[s]” and “vulnerabilities in software executed by the server.” *Id.*, 2:1-9. And “[u]sing agents is a cumbersome

solution for a number of reasons, including IT resource management, governance, and performance.” *Id.*, 2:10-17; Ex.2076, 11 (“Traditional agents struggle with complex deployment and maintenance.”). “For example, installing agents in a large data center may take months.” ’326 Patent, 2:16-17; Ex.2103, 2 (“Customers tell me that agent-based approaches are only able to cover up to 50% of the cloud real estate even after several months of deployment.”).

Accordingly, there was a long-felt, unmet need for a cloud security solution that could adequately address undetected vulnerabilities. ’326 Patent, 1:52-55, 1:60-67, 2:4-9, 2:14-17; Ex.2136, 2 (“Organizations continue to adopt cloud computing at a rapid pace,” but “traditional security tools are often not suited for the challenges of dynamic, virtual and distributed cloud environments.”), 3 (“Eighty-four percent [of respondents] say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.”); Ex.2137, 1 (“Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge.”).

Mr. Shua’s recognition of this need and the flaws in preexisting cloud security solutions motivated him to found Orca and develop Orca’s SideScanning™, including as claimed in the ’326 Patent (*see* §IV.C.2)—a “genuinely genius innovation” that redefined the industry. Ex.2076, 7-8, 11 (“Orca launched the first

version of **agentless side scanning**, which allowed deep visibility into cloud workloads without the need to install agents.”) (original emphasis); *see also* Shua¶¶2, 8-9; Ex.2103, 1; Ex.2104, 2; Ex.2148, 15; Kaeli¶¶158-165; Ex.2138, 4 (Wiz: “[A]gentless deep scanning approaches ... achieve a level of comprehensiveness in terms of coverage and features that is not possible with agent-based approaches due to the tradeoff between performance and impact to the environment.”).

2. Orca's SideScanning™ Practices the '326 Patent

Orca's Cloud Security Platform, and in particular the SideScanning™ techniques that power the platform, have used the inventions in at least claims 1-28 of the '326 Patent since 2019 when Orca first introduced Orca's Cloud Security Platform commercially. Shua¶¶27-28; *see generally id.*¶¶27-84; Kaeli¶157. For example, with respect to independent claims 1, 15, and 18, Orca's SideScanning:

- receives a request to scan protected virtual cloud assets in a cloud computing environment (preambles and limitations 1.1, 15.1, 18.1); *see* Shua¶¶29-33 (discussing Orca's “onboarding” process including Exs.2067, 5-8 (“build[] a full-stack inventory” and “map of your entire environment”), 9-11; Ex.2300, 5, 8

REDACTED

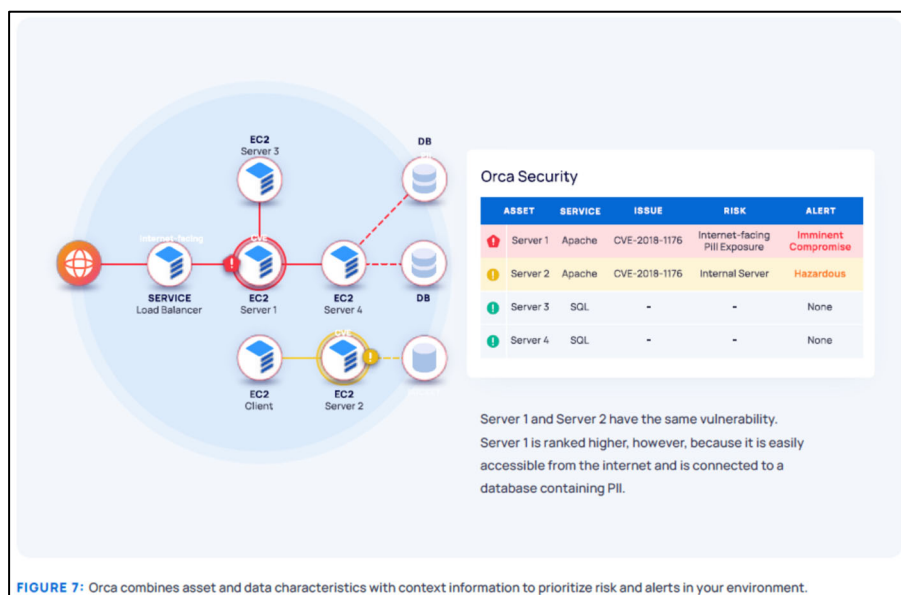
Ex.2094; Exs.2095-2098; Ex.2150; Ex.2300, 3-4); and, for each of the requested assets:

- determines, REDACTED of a snapshot of at least one virtual disk of a protected virtual cloud asset (limitations 1.2-1.2.a, 15.2-15.2.a, 18.2-18.2.a); *see* Shua¶¶34-39 (discussing Ex.2067, 5-6, 8-9; Ex.2093, 7; Ex.2302, 1; Ex.2303, 2; Ex.2301, 1; Ex.2300, 4; Exs.2094-2098, Ex.2150);
- accesses the snapshot of the at least one virtual disk REDACTED (limitations 1.2.b, 15.2.b, 18.2.b); *see* Shua¶¶41-44 (discussing Ex.2300, 5-6; Ex.2302, 1; Ex.2303, 2; Ex.2311, 3, 5; Ex.2301, 1; Ex.2300, 4; Exs.2094-2098, Ex.2150);
- analyzes as part of “Data Plane Path” the snapshot of the at least one virtual disk to determine an existence of potential cyber vulnerabilities (limitations 1.2.c, 15.2.c, 18.2.c), *see* Shua¶¶45-48 (discussing Ex.2067, 1, 3, 11, 19; Ex.2093, 7; Ex.2300, 5, 6);
- determines a risk associated with each of the determined potential cyber vulnerabilities (limitations 1.2.d, 15.2.d, 18.2.d); *see* Shua¶¶49-51

(discussing Ex.2067, 17, 11; Ex.2300, 14 REDACTED

;

- for each of the assets with the potential cyber vulnerabilities, determines a risk level to the cloud environment (limitations 1.3, 15.3, 18.3), *see* Shua¶¶52-53 (discussing Ex.2067, 19 (“report[] all issues in full context”); Ex.2093, 20, 22 (different risk levels for servers based on accessibility from Internet));
- reports the existence of the potential cyber vulnerabilities, such that the assets with the potential cyber vulnerabilities are prioritized based on associated risk levels as shown below (limitations 1.4, 15.4, 18.4), *see* Shua¶¶54-56 (discussing Ex.2300, 9; Ex.2067, 16; Ex.2092, 20); *see also, e.g.,*



Ex.2092, 20.

Orca's SideScanning also practices dependent claims 2-11, 13-14, 16-17, and 19-28. Shua¶¶57-82 (discussing Exs.2067, 2092, 2300, 2302, 2303, 2304, 2311).

Orca's SideScanning™ solution was a “big leap in cloud security” because, using the above-discussed features, it “gather[ed] crucial data through the cloud provider's APIs, while scanning disk snapshots,”⁵ and “reconstructs file systems, scans operating systems, and applications in a read-only mode ... for vulnerability assessments.”⁶ Ex.2076, 11-12, 31; Shua¶¶93-95.

^{REDACTED}
see also Kaeli¶¶172-176; Shua¶¶132-149 (discussing praise

⁵ See limitations 1.2.a-1.2.b, 15.2.a-15.2.b, 18.2.a-18.2.b.

⁶ See limitations 1.2.c-d, 1.3, 15.2.c-d, 15.3, 18.2.c-d, 18.3.

⁷ See limitations 1.4, 15.4, 18.4.

from others in, *e.g.*, Ex.2076, 31; Ex.2117, 1-2; Ex.2118, 5-7).⁸

3. The Claimed Inventions Defied 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¶¶96-98; Ex.2076, 9, 11; Ex.2106, 1 (industry skepticism that “side-scanning” could only provide “lightweight” and “rudimentary security capabilities”).

REDACTED

⁸ Since its inception, Orca has attributed its success to its “patent pending” SideScanning™ techniques, which referred to the inventions claimed in the '326 Patent and related patents claiming priority to Orca's provisional patent application (No. 62/797,718). Shua¶¶16; *see id.* ¶¶17, 18, 20, 23, 103-104, 111, 125, 134 (discussing references to “patent-pending SideScanning”); Exs.2065-2067, 2080-2081, 2088, 2090, 2092-2100, 2107-2108, 2110, 2118, REDACTED

REDACTED

This same skepticism was noted in the 2024 *Future of Cloud Security*, which remarked “how difficult it was for older providers to come to terms with the success of agentless scanning” after Orca “[i]ntroduced the concept.” Ex.2076, 7. In fact, that report explicitly states that industry participants were “skeptics” because “from a security perspective, agentless scanning was nothing compared to what attacks they were able to detect and protect.” *Id.* “They missed however that security teams were not yet in the weeds of these architectures,” so before Orca, they “didn’t know what they didn’t know.” *Id.* 7, 8 (“[T]he pivotal moment was the introduction of agentless scanning,” “but anyone who tells you they knew it at the time is lying.”); Ex.2106, 1 (Orca competitor publishing article with heading “Agentless Solutions Fall Short” that claimed “side-scanning” only “delivers rudimentary security capabilities”); Shua¶98; Kaeli¶¶166-171.

REDACTED

REDACTED

§IV.C.2 (Orca's SideScanning™ practices the challenged claims); Kaeli¶¶166-171. And, ultimately, SideScanning™ was widely accepted—"everyone needed it in order to stay competitive." Ex.2076, 7; Ex.2113, 4 ("Global innovators such as Databricks, Robinhood, Autodesk, News Corp, NCR, Duolingo, Unity Technologies, Druva and many more trust Orca Security to protect their public cloud estates."); Shua¶¶99-101, 106, 113 (describing customers and commercial success); Kaeli¶¶166-172; Ex.2103, 1 (article post-dating Orca's priority date remarking, ostensibly about Orca, about "a new 'agent-less' approach to cloud security has recently become possible due to cloud-native APIs," which provides security "in a fundamentally different way").

4. The Industry Praised Orca's Revolutionary Inventions

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

Following Orca's introduction of SideScanning™ and its 2019 filing of the provisional application that led to the '326 Patent, Orca received numerous awards

due to the inventions claimed in the '326 Patent. Shua¶¶136-149 (discussing awards in Exs.2076, 2117-2132). In 2020, Orca won CRN's "20 Coolest Tech Startups of 2020." Ex.2119, 6-7. CRN touted "Orca's SideScanning technology" which "automatically assesses the security state of every discovered asset" to provide "complete visibility." *Id.* The same year, Orca won Forbes's "Top 20 Cybersecurity Startups to Watch in 2021," the SINET16 Innovator Award, was named a "Visionary Vendor" by Security Current, and a "Gartner Cool Vendor" in the CSPM category. Ex.2120, 7 (Forbes finding Orca "noteworthy for its innovative approach to providing instant-on, workload-deep security" for cloud computing systems, emphasizing Orca's "patent-pending SideScanning™ technology" that "reads cloud configuration and workloads' runtime block storage out-of-band."); Ex.2143, 3; Ex.2145, 2; Ex.2121. In 2022, AWS awarded Orca "global Security Partner of the Year." Ex.2122, 1-2. And in both 2022 and 2023 SC Media named Orca the "Best Cloud Security Posture Management (CSPM) solution" and a finalist in other categories. Ex.2124, 1, Ex.2123, 2 (award noting customer praised Orca's "agentless approach" as "both a major innovation and a game changer"); Ex.2123, 1-2 ("After years of dealing with agents, then seeing how easy it is to install and use Orca, I knew that its agentless approach was both a major innovation and a game changer."); Ex.2125, 1-2. Orca was also named to Forbes' 2023 Cloud 100 list, the 2023 and 2024 Redpoint InfraRed 100 List, and a "most innovative startup" by

Cyber 2024. Exs.2127-2132. Orca received those awards because of SideScanning, which is the technology powering Orca's product, and the inventions claimed in the '326 Patent. Shua¶¶148-149; *see also id.* ¶¶100-101 REDACTED

REDACTED

REDACTED

-

REDACTED

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 '326 Patent's claimed combinations, such as using cloud computing platform APIs to determine locations of virtual disks and virtual disk snapshots and to facilitate snapshot analyses. *See* Ex.2076, 7 (“[T]he ability to view workload data without an agent was a genuinely genius innovation – utilizing the nature of cloud APIs being accessible to vendors.”), 11 (“Orca launched the first version of agentless side scanning, which allowed deep visibility into cloud workloads without the need to install agents.”), 11-12 (“Agentless solutions ... leverage cloud APIs to snapshot underlying instance hard disks, copy them into the security vendor[']s account, where they're hooked up on the vendor's side and scanned,” which “creates an elegant ‘like magic’ approach”), 31 (“Orca Security made a big leap in cloud security with the introduction of its patented agentless SideScanning technique,” a “unique method” that “gather[s] crucial data through the cloud provider's APIs, while scanning disk snapshots”); Ex.2118, 5 (“Orca uses a

patent-pending technique called SideScanning™, ... which unobtrusively scans the run-time block storage layer—out of band—to extract valuable data about the environment and the assets communicating in it.”), 4 (customer reporting Orca’s solution is “unique” because it “locates vulnerabilities with precision and delivers tangible, actionable results—without having to sift through all of the noise.”);

REDACTED

Shua¶¶133-136 (discussing Exs.2076, 2118); Kaeli¶175.

Industry praise demonstrates the challenged claims’ non-obviousness.

5. Wiz Copied Orca’s Inventions

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

REDACTED

REDACTED

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

Wiz knew of and had access to Orca's technology before Wiz was even founded because Mr. Shua presented Orca's SideScanning™ technology to Wiz's founder Yinon Costica at Microsoft in May 2019. Shua ¶¶ 115-119 (describing meeting and related emails in Exs.2306, 2307). REDACTED

REDACTED

REDACTED

⁹ *See* limitations 1.2.a-1.2.b, 15.2.a-15.2.b, 18.2.a-18.2.b.

¹⁰ *See* limitations 1.2.c-1.2.d, 15.2.c-15.2.d, 18.2.c-18.2.d.

¹¹ *See* limitations 1.3-1.4, 15.3-15.4, 18.3-18.4.

REDACTED

¹² AWS is an acronym for Amazon Web Services, a cloud computing platform. As the '326 Patent's claims recite, Orca's SideScanning™ utilizes AWS APIs ("API ... provided by [a] cloud computing environment"), to scan snapshots of virtual disks of VMs implemented on AWS to detect vulnerabilities, and an AWS policy provides

REDACTED

access permissions to AWS resources required for such scanning. Shua¶138;
Kaeli¶193.

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

As the above-discussed evidence shows, Wiz accessed and copied Orca's technology practicing the '326 Patent claims, which strongly supports that the claimed inventions were non-obvious. *See Stratoflex*, 713 F.2d at 1541; *WBIP*, 829 F.3d at 1336; *Kaeli* ¶¶182-201.

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

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

Wiz's Cloud Security Platform uses what Wiz calls "workload scanning," which, like Orca's SideScanning™, practices the challenged claims. *Kaeli* ¶¶202-232 (discussing Exs. 2026, 2074, 2115, 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, 15.1, 18.1); *see Shua* ¶¶122-

123 (discussing Ex.2308, 1); Kaeli¶¶215-221 (discussing Exs.2067, 2094-2097, 2115);

- for each of the requested plurality of protected virtual cloud assets in the cloud computing environment:

- determines, REDACTED

of

a snapshot of at least one virtual disk of a respective protected virtual cloud asset (limitations 1.2.a, 15.2.a, 18.2.a); *see* Shua¶¶122-123 (discussing Ex.2308, 1-2), 124 (discussing Ex.2026, 2-3), 127 (discussing Wiz's "workload scanner" using "cloud APIs" in Ex.2115); Kaeli¶¶215-221 (discussing Exs.2115, 2308-2309);

- accesses the snapshot of the at least one virtual disk using the

REDACTED (limitations 1.2.b, 15.2.b,

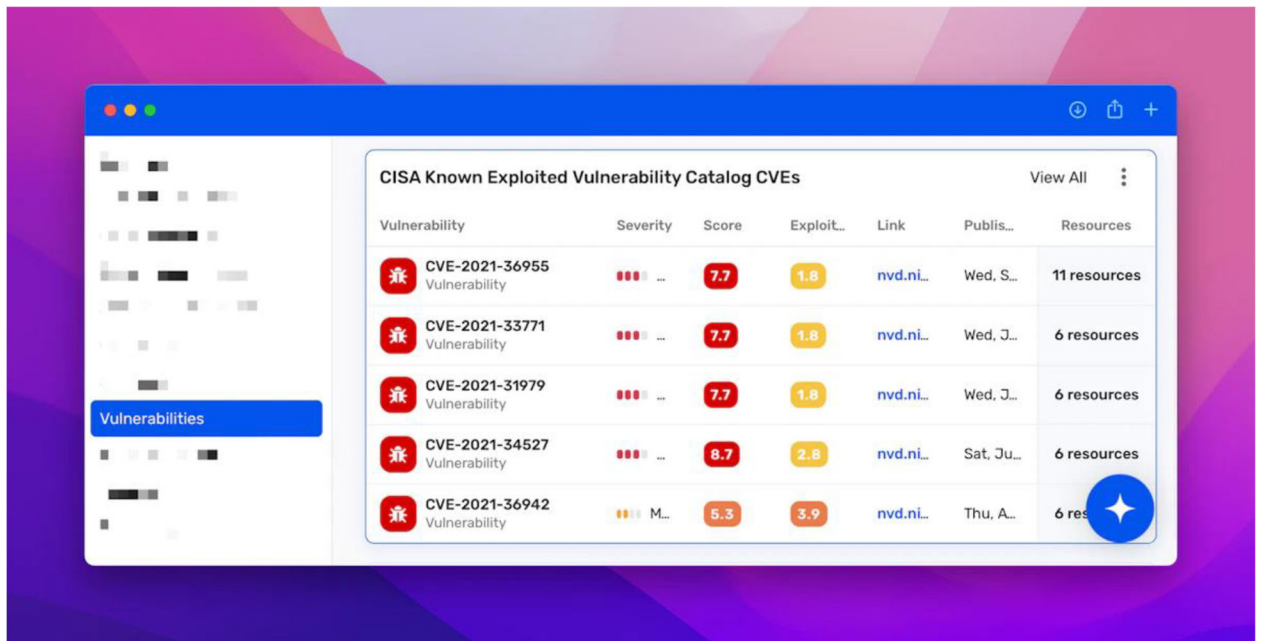
18.2.b), *see* Shua¶¶122-123 (discussing Ex.2308, 3), 124 (discussing Ex.2026, 2-3), 127 (discussing Ex.2115); Kaeli¶¶215-221 (discussing Exs.2115, 2308-2309);

- analyzes the snapshot to determine an existence of potential cyber vulnerabilities (limitations 1.2.c, 15.2.c, 18.2.c), *see* Shua¶¶124 (discussing Ex.2026, 2-3 ("[s]napshot scanning"),

127 (discussing Wiz's "workload scanner" in Ex.2115), 128-129 (Wiz "lists all resources ... vulnerable to one or more vulnerabilities" in Ex.2147); Kaeli¶¶222-224 (discussing Exs.2115, 2147, 2165);

- determines a risk associated with each of the determined potential cyber vulnerabilities (limitations 1.2.d, 15.2.d, 18.2.d)); *see* Shua¶¶127-130 (discussing Ex.2147, 2 (determining "one or more vulnerabilities"), Ex.2160, 2); Kaeli¶¶222-224 (discussing Exs.2115, 2147, 2165); Ex.2169, 3 ("breakdown of each vulnerability's risk impact");
- determines a risk level to the cloud computing environment (limitations 1.3, 15.3, 18.3), *see* Shua¶¶128-130 (discussing Ex.2160, 2 ("full visibility into what cloud services are in use and where"); Ex.2147, 2-3 ("find[] the resources that pose the highest risk"); Kaeli¶¶225-232 (discussing Exs.2115, 2147, 2165); Ex.2168 ("Prioritize remediation"); Ex.2070 ("Automated prioritization[:] Filters out irrelevant vulnerabilities and reports on those with the biggest blast radius."); Ex.2169, 3;
- reports the determined potential cyber vulnerabilities prioritizing the assets with the determined potential cyber vulnerabilities based on risk

levels (limitations 1.4, 15.4, 18.4), *see* Shua¶¶128-130 (discussing Ex.2147, 2; Ex.2160, 2); Kaeli¶¶225-232 (discussing Ex.2165); Ex.2169, 3 (“Wiz Issues correlates vulnerabilities to risks ... so they can focus on the vulnerabilities that truly have an impact to the business.”); Ex.2170, 11-12 (“Wiz analyzes your entire cloud environment to identify which resources are vulnerable and then ranks their severity and exploitability.”);



Ex.2147, 2.

REDACTED

REDACTED

see also Shua¶¶125 (comparing Wiz blog Ex.2138 to Orca's SideScanning White Paper Ex.2067), 115 (explaining Orca has had dozens or hundreds of competing proof-of-concepts against Wiz, and customers frequently remark that Wiz's core product functionality is the same as SideScanning); Kaeli¶¶206-214.

Wiz's copying of Orca's implementation of the inventions claimed in the '326 Patent plays the dual role of "praising" the invention and suggesting that the prior art was insufficient. *See Stratoflex*, 713 F.2d at 1541; *WBIP*, 829 F.3d at 1336.

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

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

After filing the provisional patent application that led to the '326 Patent in January 2019, and Orca introduced the claimed inventions in SideScanning later that year, Orca obtained a remarkable amount of investment. Shua¶¶99-114 (discussing Exs.2065, 2108-2113, 2140 and explaining how funding was due to claimed inventions); Ex.2149, 24; Kaeli¶¶233-235. By June 2019, Orca raised \$6.5 million dollars in funding, with a direct nexus to the unique features of the challenged claims, including Orca's ability to read and analyze "virtual machine[s]" in the cloud and determine "[w]hich servers are vulnerable." Ex.2107, 2-3. One lead investor remarked about "Orca's unique approach and innovative solution" that provided "true, deep, and near instantaneous full stack visibility at a forensic level of detail."

Id., 3. In 2020, Orca raised another \$75 million in funding. Shua¶108 (explaining Orca was able to get these investments “because of the novel aspects of SideScanning™ that are claimed in the ’326 Patent”); Exs.2109-2110; Ex.2140, 2. For example, Orca explained that the money it raised would “fuel Orca Security’s further disruption of the cloud security industry with touchless, workload-deep, context-aware security and compliance” that “helps to reduce thousands of security alerts to the critical few that matter, along with their precise path to remediation.” Ex.2110, 1; *see also, e.g.*, Ex.2109, 1 (“One feature that makes Orca stand out is its ability to quickly provide workload-level visibility without the need for an agent or network scanner. Instead, Orca uses low-level APIs.”); Ex.2111, 1 (“What makes Orca stand out is not just its focus on cloud-native technologies but what it calls SideScanning technology. This enables it to map a company’s cloud environment and reconstruct its file system by looking at how workloads interact with the block storage services they use.”). And in 2021, just two years after introducing the Orca Cloud Security Platform powered by its patented SideScanning technique embodied in the ’326 Patent—Orca’s only product—Orca raised additional investments of over \$550 million, marking Orca as the fastest cloud security company to reach a valuation over \$1 billion. Ex.2112, 1-2; Ex.2139, 1; Shua¶¶110-111. These funding announcements again demonstrated how Orca’s commercial success was attributable to the inventions claimed in the ’326 Patent. Ex.2113, 1 (“Orca

Security's patent-pending SideScanning™ technology collects data directly from cloud provider APIs and the workload's runtime block storage out-of-band" and detects "vulnerabilities"), 4 (Orca "[p]rioritize[s] risk based on the severity of the underlying security issue, its accessibility, and business impact" and reports issues as "alerts"), 3 ("Orca Security's rapid emergence as a cloud security leader is driven by customer love for its product.").

Importantly, Orca did not enjoy this success because it was *already* a market leader and simply introduced a new product, which is due less weight. *See Pentec, Inc. v. Graphic Controls Corp.*, 776 F.2d 309, 316 (Fed. Cir. 1985). REDACTED

; Ex.2076, 7 ("CSPM can be defined by pre and post-Orca.").

Orca also earned significant revenues from its Cloud Security Platform "power[ed]" by SideScanning™. Shua¶¶99-100; Ex.2067, 1, 3. From introducing SideScanning in 2019 to the end of 2024, Orca earned REDACTED in revenue. Shua¶101; Ex.2312

REDACTED

¹³ Cloud Workload Protection Platform.

REDACTED

. *Id.*; *Chemours Co. FC, LLC v. Daikin Indus., Ltd.*, 4 F.4th 1370, 1378 (Fed. Cir. 2021) (“significant sales” are evidence of commercial success). Orca would have earned even more, but for Wiz copying Orca’s technology and forcing Orca to compete with it for customers. *See Shua*¶115.

The commercial success of Wiz’s infringing Cloud Security Platform further demonstrates nonobviousness. *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1130 (Fed. Cir. 2000) (“[T]he success of an infringing product is considered to be evidence of the commercial success of the claimed invention.”). Wiz reports that after February 2021—i.e., after Wiz copied Orca’s inventions (§IV.C.5)—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.2142.¹⁴

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

V. Challenged Claims 4-5 and 17 Are Nonobvious Over Veselov, Basavapatna, and Czarny (Ground 2)

Wiz's Ground 2 combination adds Czarny (Ex.1084) to its Ground 1 combination, but Wiz admits that its proposed combination "does not impact the previous obviousness arguments" in Ground 1 for the independent claims. Pet.60; *see id.* 60-64. Accordingly, Wiz's Ground 2 fails for the same reasons as Ground 1.

VI. Challenged Claims 22-27 Are Nonobvious Over Veselov, Basavapatna, and Giakouminakis (Ground 3)

Wiz's Ground 3 "builds upon Ground 1" and adds Giakouminakis as purportedly relating to claims 22-27. Pet.64. Wiz's Ground 3 does not address any

¹⁴ Wiz's public remarks about the use of cloud APIs in its infringing product being "new" when it was introduced in 2020-2021 also undercut its pre-2019 obviousness arguments. *See* Pet.29 (arguing it "would have been obvious" for security systems to use cloud APIs); *see Power-One, Inc. v. Artesyn Techs., Inc.*, 599 F.3d 1343, 1352 (Fed. Cir. 2010) ("Artesyn's position that Power-One's invention was obvious is inconsistent with its position that its own infringing product was an advancement in the industry.").

independent claim, and thus fails for the same reasons as Ground 1 and the additional reasons below.

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

POSAs would not have combined, or reasonably expected to succeed in combining, Veselov, Basavapatna, and Giakouminakis for at least the same reasons they would not have combined, or reasonably expected to succeed in combining, Veselov and Basavapatna. *See* §IV.A. Additionally, even assuming *arguendo* that POSAs would have combined Veselov and Basavapatna, POSAs would not have been motivated to modify Wiz's Veselov-Basavapatna combination with teachings from Giakouminakis to achieve what is claimed.

Giakouminakis describes a “security tool” to “identify vulnerabilities in a computing system and determine a risk level of the vulnerabilities.” Giakouminakis (Ex.1044), Abstract. But like Basavapatna (and unlike the challenged claims or the proposed combination), Giakouminakis's security tool is “implemented and executed on ... computing systems ... in order to test and analyze the security of a computing system,” i.e., Giakouminakis utilizes agents on executing computing devices to identify vulnerabilities. Giakouminakis, 12:31-36; Kaeli¶¶154-155; Shua¶¶150, 165-166. Giakouminakis does not contemplate snapshots or snapshot-based analyses. Thus, just like Wiz's failure to explain how the Veselov-Basavapatna combination would work, with a reasonable expectation of success,

Wiz fails to show how its purported Veselov-Basavapatna-Giakouminakis combination would work, and that a POSA would have had a reasonable expectation of success in combining the teachings. This is particularly true where Veselov's snapshot-based analyses do not provide the types of data required by the agent-based analyses of Basavapatna and Giakouminakis, contrary to Dr. Stavrou's unsupported opinion that the two different types of analyses involve "comparable data" (*see* Ex.1002 ¶291). Kaeli¶¶152-155; *see* §IV.A.3 (explaining POSAs understood agent-based approaches gather different data than agentless approaches).

Additionally, Wiz's generic rationale supporting the combination is insufficient to demonstrate obviousness. For example, Wiz asserts a motivation to combine the three references "to improve security by more accurately measuring risk" or to provide "more useful information" (Pet.65), yet this is virtually the same motivation asserted for combining Veselov and Basavapatna (*id.* 22: "more robust and accurate risk assessments"). *See ActiveVideo*, 694 F.3d at 1328. Wiz does not explain how Basavapatna's purported increased accuracy with respect to the independent claims somehow becomes deficient and in need of even more accuracy when arriving at claims 22-27, absent hindsight. To the contrary, Wiz's addition of Giakouminakis to provide what it generically calls a "multi-factorial risk assessment[]" in the combination (Pet.64-65), would further increase the complexity of monitoring or assessing the security posture of, which were the "drawbacks of

existing security systems” that Veselov was trying to overcome. Veselov, 2:42-46; Kaeli ¶¶152-155; *Polaris*, 882 F.3d at 1069. Wiz’s hindsight-driven combination is also refuted by the abundance of objective evidence supporting the nonobviousness of the challenged claims described above. *See* §IV.C.

B. Ground 3 Does Not Show Obviousness of Challenged Claims 22-27

Even if the Board were to accept Wiz’s Veselov-Basavapatna-Giakouminakis combination, it fails to render obvious claims 22-27 for at least the reasons discussed in the preceding section and because Wiz does not contend Giakouminakis addresses the deficiencies in Wiz’s Veselov-Basavapatna combination for independent claim 1. *See* §IV.B.

VII. Conclusion

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

Respectfully submitted,

Dated: May 9, 2025

By: / Blake R. Davis /

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

*Counsel for Patent Owner
Orca Security Ltd.*

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

I hereby certify that this Patent Owner's Response complies with the word count limitation of 37 C.F.R. § 42.24(b)(2) because the Patent Owner's Response contains 13,990 words using Microsoft Word's counting feature, excluding the cover page, signature block, and the parts of the Patent Owner's Response exempted by 37 C.F.R. § 42.24(b)(2).

By: / Blake R. Davis /

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

*Counsel for Patent Owner
Orca Security Ltd.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that on this 9th day of May, 2025, a true and correct copy of the foregoing **Patent Owner's Response and all Exhibits** were served by electronic mail on Petitioner's lead and backup counsel at the following email addresses:

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

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

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

By: / Blake R. Davis /

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

blake.davis@lw.com

Latham & Watkins LLP

505 Montgomery Street, Ste. 2000

San Francisco, CA 94111-6538

Telephone: 415.395.8033

Fax: 415.395.8095

Counsel for Patent Owner

Orca Security Ltd.