

Filed on behalf of: Orca Security Ltd.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

Case IPR2024-01109
Patent 11,726,809

DECLARATION OF AVI SHUA

Contents

I.	Introduction.....	5
II.	Background.....	5
III.	Orca's SideScanning™ Uses The '809 Patent Inventions.....	17
A.	SideScanning™ Uses the Inventions Of Claims 1, 16, and 19.....	21
1.	Preambles 1, 16, and 19, Limitation 19.i: A Method For Securing Virtual Cloud Assets Against Cyber Vulnerabilities; A Computer Readable Medium Containing Instructions For Securing Virtual Cloud Assets Against Cyber Vulnerabilities; A System For Securing Virtual Cloud Assets Against Cyber Vulnerabilities Comprising a Processor	21
2.	Limitations 1.1, 16.1, 19.1: Determin[e/ing], Using An API Or Service Provided By The Cloud Computing Environment, A Location Of A Snapshot Of At Least One Virtual Disk Of A Protected Virtual Cloud Asset, Wherein The Protected Virtual Cloud Asset Is Instantiated In The Cloud Computing Environment	22
3.	Limitations 1.2, 16.2 19.2: Accessing, Based On The Determined Location And Using An API Or Service Provided By The Cloud Computing Environment, The Snapshot Of The Virtual Disk	25
4.	Limitations 1.3, 16.3, 19.3: Analyz[e/ing] The Snapshot Of The At Least One Virtual Disk By Matching Installed Applications With Applications On A Known List Of Vulnerable Applications	29
5.	Limitations 1.4, 16.4, 19.4: Determine[e/ing], Based On The Matching, An Existence Of A Plurality Of Potential Cyber Vulnerabilities Of The Protected Virtual Cloud Asset	31
6.	Limitations 1.5, 16.5, 19.5: Correlat[e/ing] The Determined Potential Cyber Vulnerabilities With A Network Location Of The Protected Virtual Cloud Asset	32
7.	Limitations 1.6, 16.6, 19.6: Us[e/ing] The Determined Plurality Of Potential Cyber Vulnerabilities And The Network Location Of The Protected Virtual Cloud Asset To Determine A Risk Of The Protected Cloud Asset To The Cloud Computing Environment	34
8.	Limitations 1.7, 16.7, 19.7: Prioritiz[e/ing], By The Determined Risk, The Plurality Of The Potential Cyber Vulnerabilities	35

9.	Limitations 1.8, 16.8, 19.8: Report[ing] The Determined Plurality Of Potential Cyber Vulnerabilities As Alerts Prioritized According To The Determined Risk.....	36
B.	SideScanning™ Uses The Inventions Of At Least Claims 2-8, 10, 12-15, 17-18, and 20-23	38
1.	Claim 2.....	38
2.	Claim 3.....	39
3.	Claim 4.....	40
4.	Claim 5.....	41
5.	Claims 6 and 17	42
6.	Claims 7 and 18	43
7.	Claim 8.....	44
8.	Claim 10.....	45
9.	Claim 12.....	45
10.	Claims 13 and 20	46
11.	Claims 14 and 21	47
12.	Claims 15 and 22	49
13.	Claim 23.....	50
IV.	Orca's SideScanning™ Solved Long-Standing Industry Problems	51
V.	Orca Overcame Skepticism About SideScanning™'s Efficacy	62
VI.	My SideScanning™ Inventions Drove Orca's Commercial Success	63
VII.	Wiz Copied Orca's SideScanning™.....	74
VIII.	Orca's SideScanning™ Inventions Were Widely Praised and Received Many Accolades.....	88
IX.	The Patents And Publications Relied On By Wiz Are Vastly Different Than Orca's SideScanning™ And '809 Patent Inventions.....	96
A.	Veselov (Ex.1007)	96

B.	Mohanty (Ex.1075).....	101
C.	Czarny (Ex.1084).....	102
D.	Hutchins (Ex.1070).....	103
X.	Conclusion	105

I. Introduction

1. I, Avi Shua, submit this declaration based upon my personal knowledge, and, if called upon to testify, would testify competently to the matters stated herein.

2. I am a co-founder of Orca Security, Ltd., and am currently Orca's Chief Innovation Officer. I am a named inventor on 20 United States Patents, including 18 as part of my work at Orca, and including as the sole inventor of U.S. Patent No. 11,762,809 (the "'809 Patent").

3. I understand this declaration will be filed in an *inter partes* review (or "IPR") before the Patent Trial and Appeal Board of the United States Patent and Trademark Office, which is a proceeding directed to assessing the validity of the inventions claimed in the '809 Patent. I also understand that this IPR was initiated by Wiz, Inc., a company against which Orca filed a patent litigation lawsuit in the United States District Court for the District of Delaware in July 2023, a suit in which Orca asserted the '809 Patent against Wiz.

II. Background

4. I have over 20 years of experience in the computer and cloud security industry.

5. I earned a Bachelor of Science degree in Computer Science & Philosophy from The Hebrew University in 2008.

6. After earning my degree, I served in Unit 8200 of the Israeli Intelligence Corps for around 4 years, followed by 4 years of consulting the same Unit 8200. During my tenure with Unit 8200, I gathered invaluable experience in a wide variety of cybersecurity-related fields. Additionally, I led several projects that became key pillars of Unit 8200's operations, and I was honored with multiple awards as part of my service.

7. After I left the Israeli Intelligence Corps, I joined Check Point Software. Check Point was an early pioneer in the computer security industry, and I worked there for 11 years. I was Check Point's Threat Prevention Chief Technologist for four of those years.

8. As a result of my experience in the military and at Check Point, as well as cybersecurity research that I did, I recognized that traditional computer security approaches faced major challenges in cloud computing environments, which are dynamic and include many transient workloads. For example, pre-Orca security solutions were often unable to adequately secure cloud-based dynamic computing environments' workloads against vulnerabilities, which led to gaping holes in protection and long periods without adequate security visibility. Such solutions were also very costly. I set out to invent a better way to provide comprehensive security coverage in evolving cloud environments.

9. In late 2018, I left full-time employment with Check Point with several colleagues to found Orca. I have been with Orca since we officially formed the company in January 2019. I served as Orca's Chief Executive Officer until March 2023, and as Chief Innovation Officer after that.

10. At Orca, I invented and developed new ways to analyze and protect cloud computing environments. In general terms, I conceived of new approaches that access and analyze snapshots of virtual assets, for example, virtual machines, in cloud computing environments using cloud computing platform APIs. With my new approaches, clients could secure their cloud computing environments without negative impacts on virtual asset performance, and without network scanners or agents, which had to be installed directly onto virtual assets to gather information for, and to perform, security assessments. My new approaches dramatically reduced the organizational friction and effort required to engineer security tools, vastly improved visibility into cloud environments, and provided deeper and better assessment results, as well as accurate risk prioritization (to protect an organization's critical assets), at greater speeds.

11. On January 28, 2019, Orca filed its first provisional patent application (No. 62/797,718) (the "'718 Provisional Application"), in which I described my new cloud security approaches.

12. On November 14, 2022, Orca filed the application (No. 18/055,201) that issued as the '809 Patent on which I focus in this declaration. I understand that the '809 Patent is a continuation of application No. 17/330,998, which is a continuation of application No. 16/585,967, and also is entitled to the benefit of the January 28, 2019 filing date of the '718 Provisional Application.

13. I also worked with the team at Orca to commercialize the technology described and inventions claimed in the '809 Patent. To facilitate that, in 2019, we named our technology "SideScanning," which Orca has now trademarked. SideScanning™ has been, and continues to be, the foundational technology that powers Orca's Cloud Computing Platform and differentiates Orca from its competitors.

14. In the last five years, I have spoken at multiple conferences and events, and in interviews, about Orca's patented SideScanning™ approaches, including: the 9th Annual International Cybersecurity Conference at Cyber Week 2019 (Ex.2078 (excerpted video of "The CISO - Startup Connection Powered by YL Ventures - Orca Security," <https://www.youtube.com/watch?v=h4x4zh1D-tw>); Ex.2079 (transcript of "The CISO - Startup Connection Powered by YL Ventures - Orca Security," <https://www.youtube.com/watch?v=h4x4zh1D-tw>)); an interview with Startup Daily in April 2021 (Ex.2084 (page capture of "Australian Business Interview with Avi Shua | Orca Security Through the Years,"

<https://www.youtube.com/watch?v=ne6biY89RyY>)); an interview on the Consumer News and Business Channel's (CNBC) TechCheck in April 2021 (Ex.2085 (page capture of "CNBC Interview with Avi Shua | Orca Security Through the Years," <https://www.youtube.com/watch?v=r9aBmLHpSnY>)); an interview with The Cube in June 2021 (Ex.2086 (page capture of "The CUBE Interview: Avi Shua Explains Orca Security and Its Value Proposition," <https://www.youtube.com/watch?v=tlS0A92IYm8>)); an interview with The Matias Experience (Ex.2087 (page capture of "Ep398: Avi Shua | CEO & Co-Founder, Orca Security," <https://www.youtube.com/watch?v=M58n3oE6E1Y>)); and an interview on CNBC's Squawk Box Asia (Ex.2088 (page capture of "CNBC Prime Time Interview on Orca Security's Series C Extension Led by Temasek," <https://orca.security/resources/video/cnbc-squawk-box-asia-avi-shua-interview-550m-series-c-extension/>)). And, as I explain more below, in Section III, Orca's agentless SideScanning™, which powers Orca's Cloud Security Platform, uses the inventions claimed in the '809 Patent.

15. Before I provide that explanation, though, it is worth further describing in general how Orca's Cloud Security Platform and agentless SideScanning™ work.

16. As an initial matter, I note that in virtually all of Orca's early marketing materials and presentations about its technology, Orca emphasized that its SideScanning™ used "patent-pending" techniques. And, until April 26, 2021, Orca

did not have any pending patent applications other than those claiming priority to the '718 Provisional Application discussed above. So “patent-pending” references in Orca’s marketing materials, presentations, and other documents from before April 2021 necessarily referred to the inventions described and claimed in the '718 Provisional Application’s patent family, including the '809 Patent. I discuss examples of early videos and marketing materials describing Orca’s SideScanning™ technology in the following paragraphs.

17. Exhibit 2080 is a true and correct copy of a video from as early as June 12, 2019, titled “Full Stack Visibility In Minutes,” which is available at https://www.youtube.com/watch?v=sxD14bRT_28, and which describes Orca’s SideScanning™ technology. Orca made this video publicly available by posting it online in June 2019, five months after the '718 Provisional Application was filed. I have personal knowledge of this video and confirm that it was published online by as early as June 12, 2019. Exhibit 2081 is a copy of a transcript of this video. As we explained in this video, “Orca’s patent-pending Orca SideScanning technology” “automatically discovers and performs full-stack scanning” of an organization’s cloud infrastructure to “deliver comprehensive and seamless visibility into” the organization’s “cloud inventory.” Ex.2081 (transcript of “Full Stack Visibility In Minutes,” https://www.youtube.com/watch?v=sxD14bRT_28); *see also* Ex.2080

(video of “Full Stack Visibility In Minutes,” https://www.youtube.com/watch?v=sxD14bRT_28), 0:48-1:24.

18. Exhibit 2078 is a true and correct copy of an excerpt of a video from as early as July 1, 2019, titled “The CISO – Startup Connection Powered by YL Ventures – Orca Security,” which is available at <https://www.youtube.com/watch?v=h4x4zh1D-tw>, and through which I presented on my patent-pending SideScanning™ inventions at the 9th Annual International Cybersecurity Conference, during Cyber Week 2019. I have personal knowledge of this video and confirm that it was publicly posted online by as early as July 1, 2019. Exhibit 2079 is a copy of a transcript of this video. In this video, I explained that “while all of our competitors require to install agents or to configure network scanners,” the “secret sauce” for Orca was its “patent-pending SideScanning technology” which “us[ed] low-level APIs that are open[] to the cloud infrastructure level to read the machine configuration and virtual disk...” Ex.2079 (transcript of “The CISO – Startup Connection Powered by YL Ventures – Orca Security, <https://www.youtube.com/watch?v=h4x4zh1D-tw>), 2; *see also* Ex.2078 (excerpted video of “The CISO – Startup Connection Powered by YL Ventures – Orca Security, <https://www.youtube.com/watch?v=h4x4zh1D-tw>), 6:26-7:01. I also explained that, after Orca’s Cloud Security Platform is integrated, in minutes, it uses read-only access to provide “full stack visibility of misconfiguration vulnerabilities into your

data[] without any change in the environment.” Ex.2079 (transcript of “The CISO – Startup Connection Powered by YL Ventures – Orca Security, <https://www.youtube.com/watch?v=h4x4zh1D-tw>), 2; *see also* Ex.2078 (excerpted video of “The CISO – Startup Connection Powered by YL Ventures – Orca Security, <https://www.youtube.com/watch?v=h4x4zh1D-tw>), 6:13-6:23.



Ex.2078 (excerpted video of “The CISO – Startup Connection Powered by YL Ventures – Orca Security, <https://www.youtube.com/watch?v=h4x4zh1D-tw>), 6:34.

19. Exhibit 2082 is a true and correct copy of a video from as early as August 9, 2020, titled “Orca Security – SideScanning vs Traditional Security Assessment Methods,” which is available at <https://www.youtube.com/watch?v=0SDwFzINzGM>, and in which I compared SideScanning™ against “Traditional Security Assessment Methods.” I have

personal knowledge of this video and confirm it was publicly posted online by as early as August 9, 2020. Exhibit 2083 is a copy of a transcript of this video. As I explained in this video, and like I explained in the '809 Patent, before my inventions, organizations secured their physical data center environments by “install[ing] security agents” that reside on the host resources or by deploying physical “network scanners” on the network that “try to probe things externally, either using authenticated or unauthenticated mechanisms.” Ex.2083 (transcript of “Orca Security – SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 1; *see also* Ex.2082 (video of “Orca Security – SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 0:30. When cloud computing environments were introduced, the industry applied these same, flawed techniques to those environments by installing agents on virtual machines in the environment or by using “virtual network scanners.” Ex.2083 (transcript of “Orca Security – SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 1; *see also* Ex.2082 (video of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 1:37. Two problems were immediately apparent. First, agent-based techniques did not scale because it is almost impossible to deploy agents “everywhere,” as it requires “huge intra-

organizational friction in order to get them deployed.” Ex.2083 (transcript of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 1; *see also* Ex.2082 (video of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 2:17. Second, agent-based techniques produce too many security alerts without context based on and appropriately tailored to the “overall picture” of the cloud environment. Ex.2083 (transcript of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 1; *see also* Ex.2082 (video of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 2:43. As I further explained in this video, Orca’s Cloud Security Platform does not “require any agents” or a “network scanner,” which “interfer[e] with the environment.” Ex.2083 (transcript of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 2; *see also* Ex.2082 (video of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 4:40-4:46. Instead, Orca’s Cloud Security Platform “detect[s] the risks within the workloads without any agent, without any scanners, [] without sending a single packet, [and] without running a

single opcode in the environment.” Ex.2083 (transcript of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 2; *see also* Ex.2082 (video of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), 4:46.

20. In addition to describing its patent-pending SideScanning™ in videos and at conferences, Orca published white papers and electronic books (“Ebooks”) about my SideScanning™ technology.

21. Exhibit 2066 is a true and correct copy of Orca Security’s Ebook titled “The Ultimate Guide to: Gaining Full Stack Visibility into Your Cloud Assets.” I have personal knowledge of this Ebook and confirm that the November 2019 date on the cover was around when Orca made this Ebook available to the public. That November 2019 Orca Ebook described the commercial implementation of my inventions and explained, for example, that Orca’s cloud security platform works by “utiliz[ing] the patent pending SideScanning™ technology.”

How it works: The platform utilizes the patent pending SideScanning™ technology. After a one-time, essentially instantaneous, impact free integration into the cloud infrastructure; it scans the configuration, network layout, security configuration, while reading into virtual machines disks, databases, and datastores, as well as cloud logs for all of the cloud assets. It then analyzes the data, building a full-stack inventory and automatically assessing the security state of every discovered asset throughout the entire technology stack - including all four cloud layers: I/S, OS, apps and data. It undertakes a comprehensive assessment of the security state of every discovered asset, with complete visibility into compromised resources, vulnerable software, and misconfigurations without impacting performance or availability.

Ex.2066 (The Ultimate Guide to: Gaining Full Stack Visibility into Your Cloud Assets (November 2019)), 16

22. Exhibit 2090 is a true and correct copy of an earlier version of Orca's "The Ultimate Guide to: Gaining Full Stack Visibility into Your Cloud Assets" Ebook. I have personal knowledge of this Ebook, which was made available to the public in June 2019.

23. Exhibit 2067 is a true and correct copy of an early version of the Orca SideScanning™ Technical Brief, which I helped draft and was made available to the public on Orca's website at least as early as June 2020. *See also* Ex.2067 (SideScanning Technical Brief (2020)), 19 ("Copyright Orca Security, 2020"). The SideScanning™ Technical Brief describes the commercial implementation of my inventions by Orca, and it also notes that Orca's Cloud Security Platform is "[p]ower[ed]" by Orca's "patent-pending SideScanning™." Ex.2067 (SideScanning Technical Brief (2020)), 1, 19.

24. Exhibits 2092 and 2093 are additional versions of the Orca SideScanning™ Technical Brief that were made available to the public on Orca's website in 2021 and 2022, respectively. Ex.2092 (SideScanning Technical Brief (2021)), 23 ("Copyright Orca Security 2021"); Ex.2093 (SideScanning Technical Brief (2022)), 26 ("Copyright Orca Security 2022").

25. Having provided this background, I turn to further explaining how Orca's SideScanning™ uses the inventions of the '809 Patent.

III. Orca's SideScanning™ Uses The '809 Patent Inventions

26. I have reproduced claims 1, 16, and 19 of the '809 Patent below with brackets that I understand Wiz uses to refer to different limitations of the claims:

'809 Patent, claim 1: A method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising:

[1.1] determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment;

[1.2] accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the virtual disk;

[1.3] analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;

[1.4] determining, based on the matching, an existence of a plurality of potential cyber vulnerabilities;

[1.5] correlating the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset;

[1.6] using the determined plurality of potential cyber vulnerabilities and the network location of the protected virtual cloud asset to determine a risk of the protected virtual cloud asset to the cloud computing environment;

[1.7] prioritizing, by the determined risk, the plurality of potential cyber vulnerabilities; and

[1.8] reporting the determined plurality of potential cyber vulnerabilities as alerts prioritized according to the determined risk.

'809 Patent, claim 16: A non-transitory computer readable medium containing instructions that when executed by at least one processor cause the at least one processor to perform operations for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the operations comprising:

[16.1] determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment;

[16.2] accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the virtual disk;

[16.3] analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;

[16.4] determining, based on the matching, an existence of a plurality of potential cyber vulnerabilities;

[16.5] correlating the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset;

[16.6] using the determined plurality of potential cyber vulnerabilities and the network location of the protected virtual cloud asset to determine a risk of the protected virtual cloud asset to the cloud computing environment;

[16.7] prioritizing, by the determined risk, the plurality of potential cyber vulnerabilities; and

[16.8] reporting, the determined plurality of potential cyber vulnerabilities as alerts prioritized according to the determined risk.

'809 Patent, claim 19: A system for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the system comprising:

[19.i] at least one processor configured to:

[19.1] 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 protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment;

[19.2] access, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the virtual disk;

[19.3] analyze the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;

[19.4] determine, based on the matching, an existence of a plurality of potential cyber vulnerabilities;

[19.5] correlate the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset;

[19.6] use the determined plurality of potential cyber vulnerabilities network location of the protected virtual cloud asset to determine a risk of the protected virtual cloud asset to the cloud computing environment;

[19.7] prioritize, by the determined risk, the plurality of potential cyber vulnerabilities; and

[19.8] report the determined plurality of potential cyber vulnerabilities as alerts prioritized according to the determined risk.

27. Since 2019 and continuing through today, Orca's Cloud Security Platform, and in particular the SideScanning™ techniques that power the platform, use the inventions claimed in the '809 Patent, as shown by the example public and confidential documents I discuss in the following subsections, which demonstrate how SideScanning™ operates. Unless otherwise noted, the SideScanning™ techniques I discuss were initially implemented and sold by Orca in 2019, and they are used and sold by Orca in substantially the same way today.

A. SideScanning™ Uses the Inventions Of Claims 1, 16, and 19

28. Orca SideScanning™ uses the inventions of claims 1, 16, and 19 of the '809 Patent.

1. Preambles 1, 16, and 19, Limitation 19.i: A Method For Securing Virtual Cloud Assets Against Cyber Vulnerabilities; A Computer Readable Medium Containing Instructions For Securing Virtual Cloud Assets Against

**Cyber Vulnerabilities; A System For Securing Virtual
Cloud Assets Against Cyber Vulnerabilities Comprising a
Processor**

29. Orca's SideScanning™ uses the features recited in the preambles and limitation of 19.i of claims 1, 16, and 19 of the '809 Patent (reproduced in full in paragraph 26).

30. Orca's SideScanning™ is the "Engine that Powers Orca Security." Ex.2067 (SideScanning Technical Brief (2020)), 1. It is a cloud-based, computer-implemented system and method for securing virtual cloud assets within the "cloud estate of an organization," including to detect and protect against cyber vulnerabilities, which uses processors and computer-readable media containing instructions for processors. Ex.2067 (SideScanning Technical Brief (2020)), 1, 3 ("Detect risks such as vulnerabilities"), 11 (describing "Vulnerability Scanning").

**2. Limitations 1.1, 16.1, 19.1: Determin[e/ing], Using An API
Or Service Provided By The Cloud Computing
Environment, A Location Of A Snapshot Of At Least One
Virtual Disk Of A Protected Virtual Cloud Asset, Wherein
The Protected Virtual Cloud Asset Is Instantiated In The
Cloud Computing Environment**

31. Orca's SideScanning™ uses the features recited in limitations 1.1, 16.1, and 19.1 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26).

32. As explained above, SideScanning™ has an "Onboarding" process for establishing an interface between a client organization's cloud computing

environment implemented by one or more cloud computing platforms, such as “AWS, Azure, or GCP,” and Orca’s backend security components. *See* Ex.2067 (SideScanning Technical Brief (2020)), 5-6.¹ As explained in the SideScanning™ Technical Brief, Orca uses its integration into AWS, Azure or GCP to “read[] into virtual machines” and “disks,” among other protected virtual cloud assets, to “build[] a full-stack inventory.” Ex.2067 (SideScanning Technical Brief (2020)), 5. Orca does this using “metadata gathered from cloud provider APIs.” Ex.2067 (SideScanning Technical Brief (2020)), 5.

33. Orca’s SideScanning™ uses APIs provided by the cloud computing environment, e.g., AWS, Azure or GCP, to determine locations of snapshots of

¹ To assist customers with Onboarding, Orca provides detailed videos that explain how to establish connections between their environment’s cloud security platform account and an Orca account. *See, e.g.,* Ex.2094; Ex.2095; Ex.2098, 1 (“Walkthrough of how to onboard a GCP account for Orca to SideScan”); Ex.2150;

[REDACTED]

[REDACTED]

[REDACTED]; *see also, e.g.,* Ex.2096; Ex.2097 (page capture of “Define AWS Role”).

virtual disks of protected virtual cloud assets, such as virtual disks of virtual machines, that are instantiated in the cloud computing environment.

34. This process is part of SideScanning™'s "Control Plane Path" where "Orca builds an infrastructure map that acts as a guide for its assessment and analysis processes." Ex.2067 (SideScanning Technical Brief (2020)), 8. The "control plane path yields a complete overview of the cloud estate" by "[l]ooking at all assets," and enumerates all "EC2 instances, volumes, snapshots," in addition to, for example, all "Databases," "Redshift and Kafka clusters," "ELB and ALB" instances, "ECS clusters, services, and tasks," "EKS" instances, and "S3 bucket and Glacier storage," that are instantiated in all regions of a client organization's "entire estate." Ex.2067 (SideScanning Technical Brief (2020)), 8-9.

35. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

36. SideScanning™ operates similarly for client environments implemented using other cloud computing platforms, such as GCP and/or Azure, and their respective APIs. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Ex.2094 (video of “Orca Pod (In-Account) Onboarding,” <https://www.youtube.com/watch?v=FEvqhAktFS0>); Ex.2095 (video of “AWS Onboarding with Orca Security,” <https://www.youtube.com/watch?v=QdBsE2VqipU>); Ex.2098 (page capture of “GCP Onboarding,” <https://orca.security/resources/video/gcp-onboarding/>), 1 (“Walkthrough of how to onboard a GCP account for Orca to SideScan”); Ex.2150 (page capture of “Azure Onboarding - Orca Security,” <https://www.youtube.com/watch?v=zw091YvbjsI>); *see also, e.g.*, Ex.2096 (page capture of “Create AWS policy,” <https://www.youtube.com/watch?v=OdtXqrvbEdU>); Ex.2097 (page capture of “Define AWS Role,” <https://www.youtube.com/watch?v=SOw046Fnafo>).

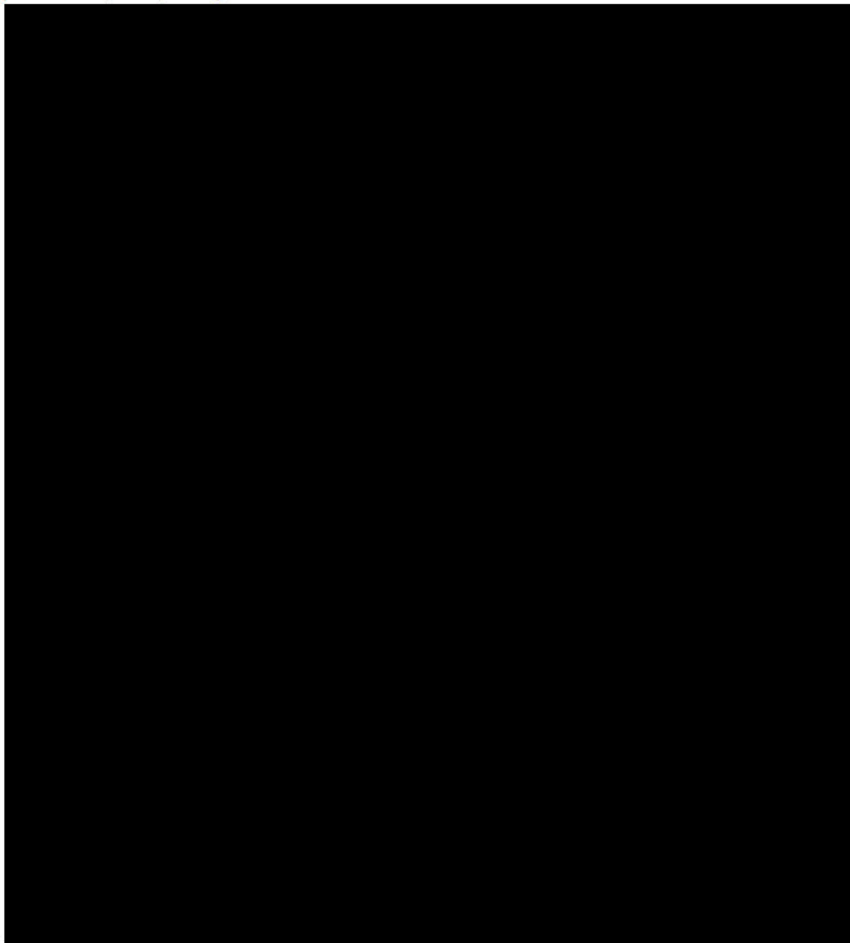
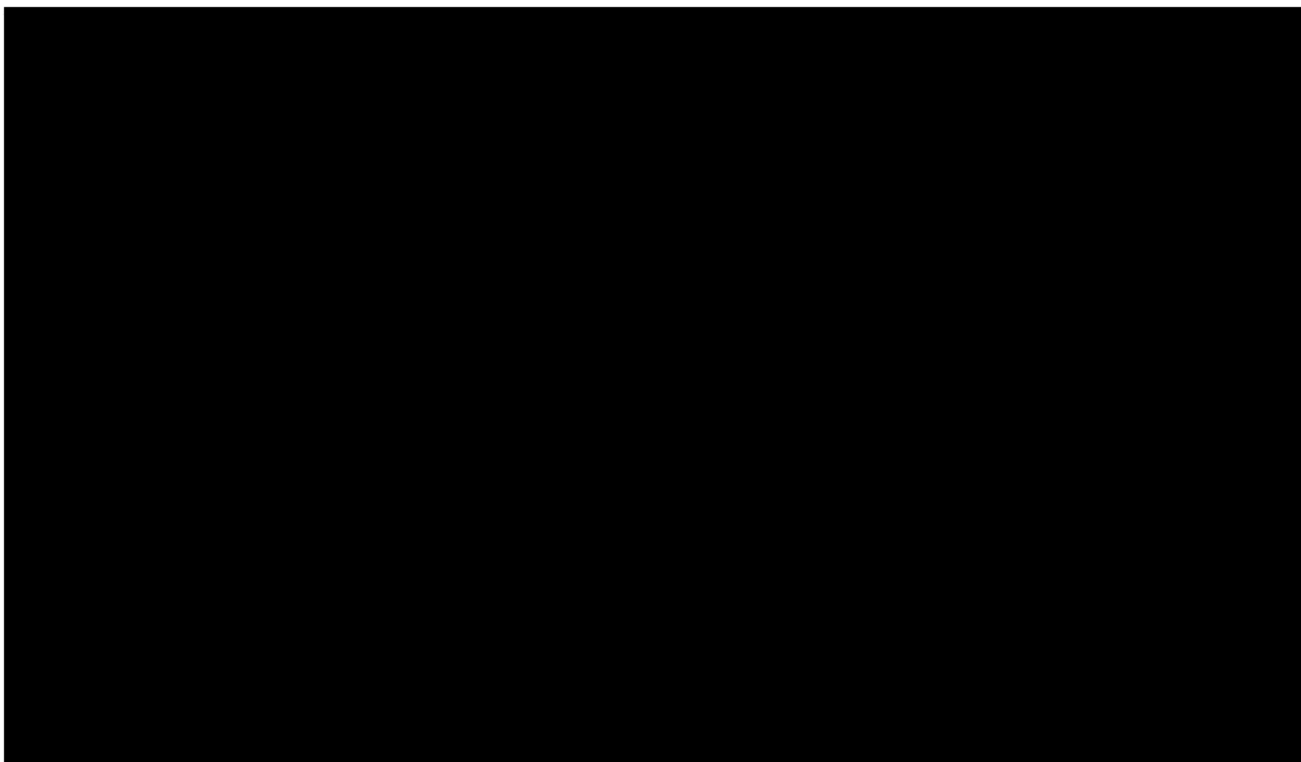
3. Limitations 1.2, 16.2 19.2: Accessing, Based On The Determined Location And Using An API Or Service

**Provided By The Cloud Computing Environment, The
Snapshot Of The Virtual Disk**

37. Orca's SideScanning™ uses the features recited in limitations 1.2, 16.2, and 19.2 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26). Orca's SideScanning™ uses the APIs provided by the cloud computing environment to access, based on the determined location of the snapshot, the snapshot of the at least one virtual disk.

38. The below diagram from Orca's product documentation for customers describes the SideScanning™ stages, [REDACTED]





[REDACTED]

[REDACTED]

[REDACTED]

40. As with the preceding limitations, SideScanning™ operates similarly for client environments implemented using other cloud computing platforms, such as GCP and/or Azure, and their respective APIs. *See, e.g.,* [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Ex.2094 (video of “Orca Pod (In-Account) Onboarding,” <https://www.youtube.com/watch?v=FEvqhAktFS0>); Ex.2095 (video of “AWS Onboarding with Orca Security,” <https://www.youtube.com/watch?v=QdBsE2VqipU>); Ex.2098 (page capture of “GCP Onboarding,” <https://orca.security/resources/video/gcp-onboarding/>), 1 (“Walkthrough of how to onboard a GCP account for Orca to SideScan”); Ex.2150 (page capture of “Azure Onboarding - Orca Security,” <https://www.youtube.com/watch?v=zw091YvbjsI>); *see also, e.g.,* Ex.2096 (page capture of “Create AWS policy,”

<https://www.youtube.com/watch?v=OdtXqrvbEdU>); Ex.2097 (page capture of “Define AWS Role,” <https://www.youtube.com/watch?v=SOw046Fnafo>)..

4. Limitations 1.3, 16.3, 19.3: Analyz[e/ing] The Snapshot Of The At Least One Virtual Disk By Matching Installed Applications With Applications On A Known List Of Vulnerable Applications

41. Orca’s SideScanning™ uses the features recited in limitations 1.3, 16.3, and 19.3 of claims 1, 16, and 19 of the ’809 Patent (reproduced in full above in Paragraph 26). Orca’s SideScanning™ will analyze a snapshot by matching installed applications with applications on a known list of vulnerable applications.

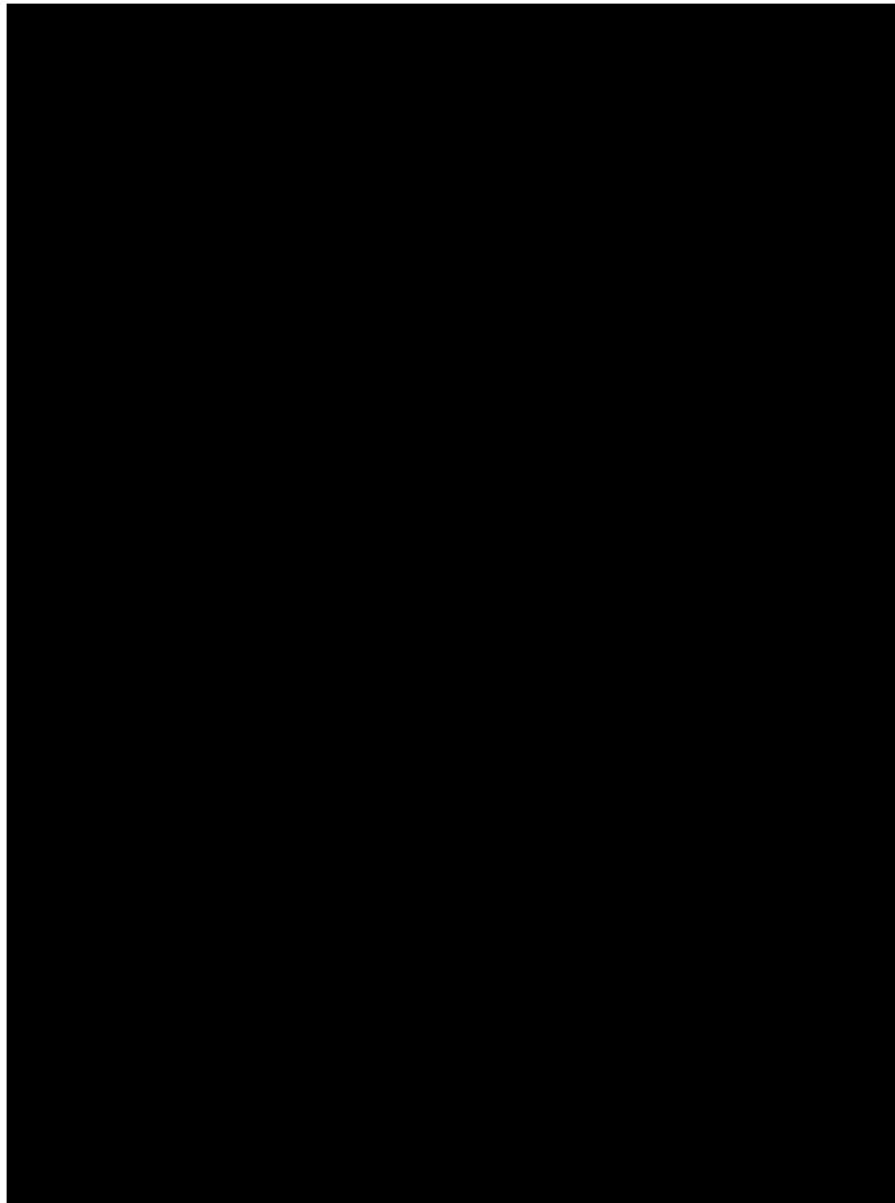
42. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Ex.2067 (SideScanning Technical Brief (2020)), 3 (“Detect risks such as vulnerabilities”), 11 (describing “Vulnerability Scanning”).



43. During “Vulnerability Scanning,” SideScanning™ “extracts all the OS packages, libraries, and program libraries” and “gathers library versions and other identifying characteristics,” then “tries matching them to known vulnerabilities in its vulnerability database.” Ex.2067 (SideScanning Technical Brief 2020), 11; [REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

5. Limitations 1.4, 16.4, 19.4: Determine[e/ing], Based On The Matching, An Existence Of A Plurality Of Potential Cyber Vulnerabilities Of The Protected Virtual Cloud Asset

44. Orca's SideScanning™ uses the features recited in limitations 1.4, 16.4, and 19.4 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26). Orca's SideScanning™ will determine the existence of a plurality of potential cyber vulnerabilities based on matching installed applications with applications on a known list of vulnerable applications.

45. For example, SideScanning™ matches applications installed on the protected virtual cloud asset to applications in Orca's "vulnerability database."

Ex.2067 (SideScanning Technical Brief 2020), 11; [REDACTED]

[REDACTED]

46. [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

6. Limitations 1.5, 16.5, 19.5: Correlat[e/ing] The Determined Potential Cyber Vulnerabilities With A Network Location Of The Protected Virtual Cloud Asset

47. Orca's SideScanning™ uses the features in limitations 1.5, 16.5, and 19.5 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26).

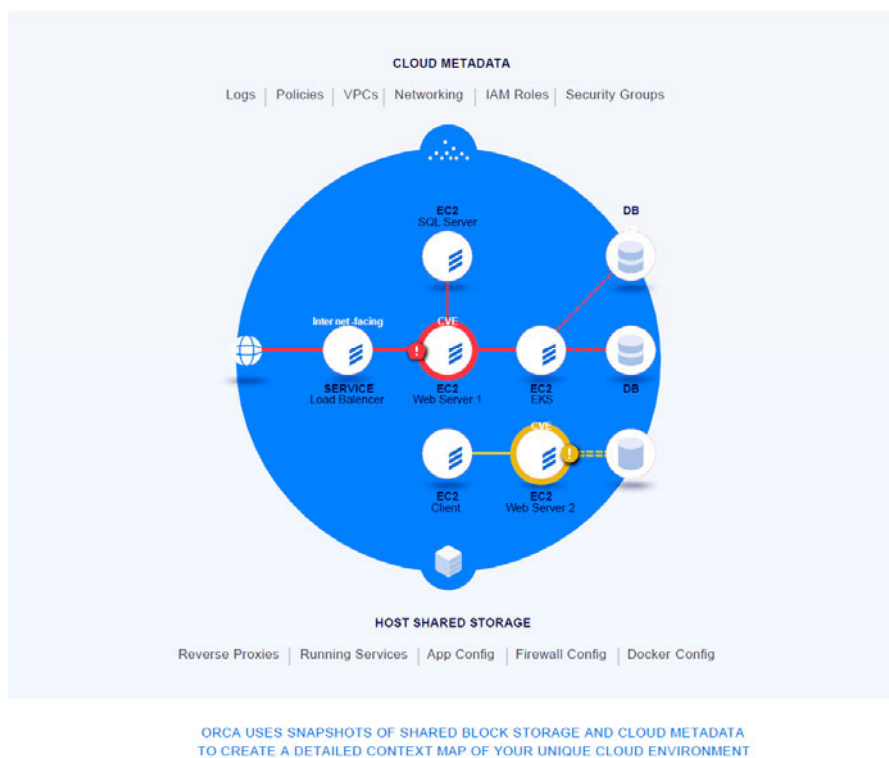
48. For example, Orca's SideScanning™ will correlate determined potential cyber vulnerabilities with a network location of the protected cloud asset

as part of creating a contextual map of the virtual network. [REDACTED]

[REDACTED]

[REDACTED]

SideScanning™ also “reads” the “network configuration” of the protected virtual cloud asset to “extend the contextual map built during the SideScanning control plane assessment phase,” which “shows what each vulnerability is [and] where it’s located.” Ex.2067 (SideScanning Technical Brief (2020)), 14, 16; *see also* Ex.2093 (SideScanning Technical Brief (2022)), 22 (“Vulnerabilities are grouped by type, location, and priority.”).



Ex.2093 (SideScanning Technical Brief (2022)), 12.

7. Limitations 1.6, 16.6, 19.6: Us[e/ing] The Determined Plurality Of Potential Cyber Vulnerabilities And The Network Location Of The Protected Virtual Cloud Asset To Determine A Risk Of The Protected Cloud Asset To The Cloud Computing Environment

49. Orca's SideScanning™ uses the features in limitations 1.6, 16.6, and 19.6 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26).

50. For example, SideScanning™ will use the vulnerabilities on the machine and its network location to determine lateral movement risks to the cloud computing environment. As we explained in the SideScanning Technical Brief, SideScanning™ uses the determined plurality of potential cyber vulnerabilities and network location of the asset to “[d]etect [l]ateral [m]ovement [r]isk” and “searches for” everything that would enable an attacker to “move laterally from one resource to another.” Ex.2067 (SideScanning Technical Brief (2020)), 15, 14 (SideScanning™ determines “bugs or other configuration risks that might only be exploitable from internal machines yet still facilitate an attacker’s lateral movement” to other protected cloud assets within the cloud computing environment.). In another example, SideScanning™ “takes a customer’s instance, maps the running services on it, then takes into consideration the vulnerability data collected in the data path” to determine a risk of the protected cloud asset to the cloud computing environment. Ex.2067 (SideScanning Technical Brief (2020)), 16.

8. Limitations 1.7, 16.7, 19.7: Prioritiz[e/ing], By The Determined Risk, The Plurality Of The Potential Cyber Vulnerabilities

51. Orca's SideScanning™ uses the features in limitations 1.7, 16.7, and 19.7 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26).

52. For example, Orca's SideScanning™ prioritizes potential cyber vulnerabilities to show “what each vulnerability is, where it's located, and its priority.” Ex.2067 (SideScanning Technical Brief (2020)), 16. Thus, “unlike legacy tools that operate in silos, Orca treats your cloud as an interconnected web of assets, prioritizing risk based on environmental context.” Ex.2067 (SideScanning Technical Brief (2020)), 16. An example of how Orca contextualizes and prioritizes potential cyber vulnerabilities based on a determined risk that is based on network locations is shown below:

vulnerability data collected in the data path. Orca contextualizes the information to establish whether an asset is internet-facing and easily accessible to attackers, or if it's private and hence a less important vulnerability. (A resource that isn't accessible by any other machine in the account represents less risk than one that's internet-facing.)

Consider a vulnerability in a web service. Orca scores it as:

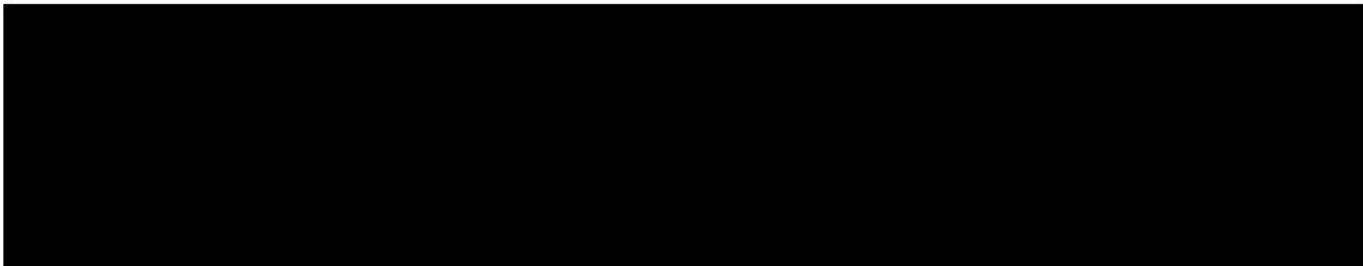
- High risk if it's connected to the internet, either directly or indirectly via a load balancer or reverse proxy
- Medium severity if it's only accessible internally
- Low severity if it's blocked by a security group configuration of the cloud provider

Ex.2067 (SideScanning Technical Brief (2020)), 16.

9. Limitations 1.8, 16.8, 19.8: Report[ing] The Determined Plurality Of Potential Cyber Vulnerabilities As Alerts Prioritized According To The Determined Risk

53. Orca's SideScanning™ uses the features in limitations 1.8, 16.8, and 19.8 of claims 1, 16, and 19 of the '809 Patent (reproduced in full above in Paragraph 26).

54. Orca's SideScanning™ reports determined cyber vulnerabilities as alerts. In particular, SideScanning™ analyzes “[a]ll the gathered information” from the Control Plane and Data Plane paths to “produce actionable, context-based alerts.” Ex.2067 (SideScanning Technical Brief (2020)), 16. The alerts are brief technical notifications that show, for example, “what each vulnerability is, where it's located, and its priority.” Ex.2067 (SideScanning Technical Brief (2020)), 16.



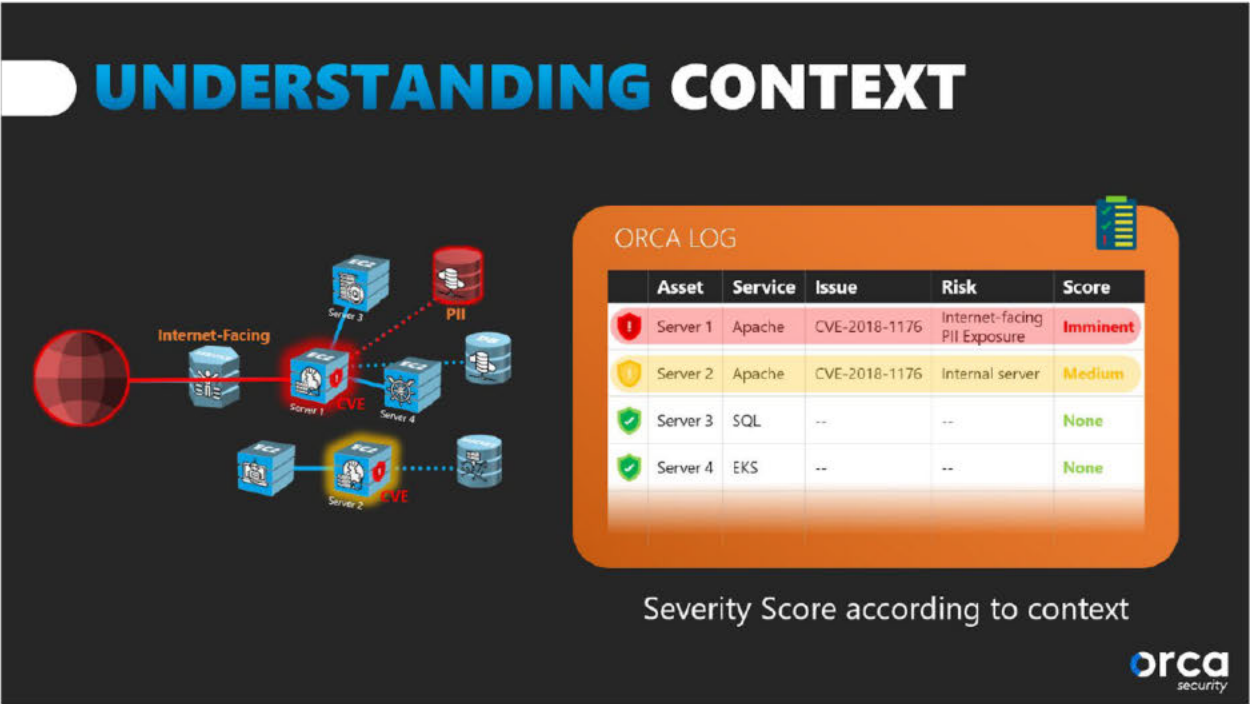
Showing Alerts in Context

Orca combines conclusions from different environmental perspectives into a single model. It takes the asset map from the control plane—where the service meshes and containers talk to each other—and enriches this information with the risk data gathered from the workload deep scanning. For example,

Ex.2067 (SideScanning Technical Brief (2020)), 16 (highlighted).

55. Orca's SideScanning™ Technical Brief provides examples of such SideScanning™ alerts prioritized according to the determined risk. For example, an

alert regarding a vulnerability on Server 1 is prioritized over the same vulnerability on Server 2 because Server 1 is internet-facing whereas Server 2 is an internal server.



Ex.2067 (SideScanning Technical Brief (2020)), 17.

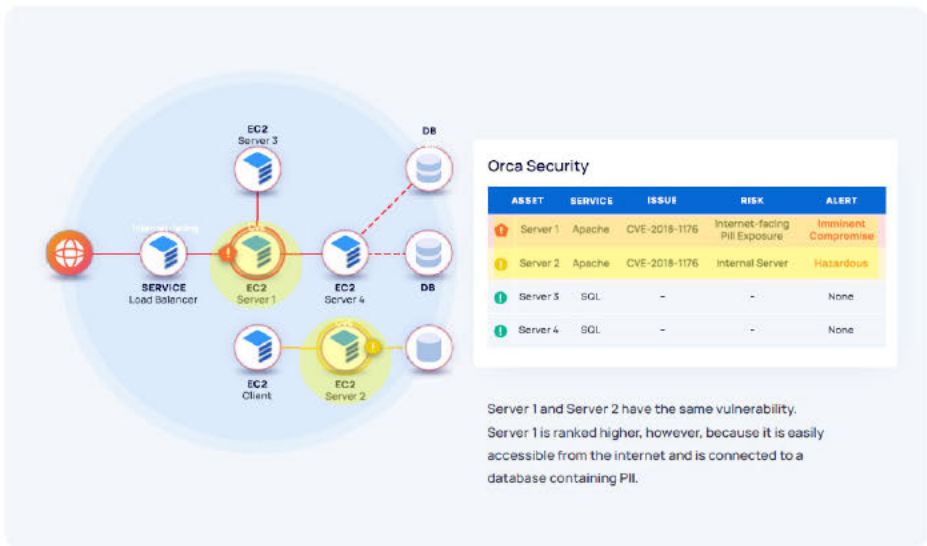


FIGURE 7: Orca combines asset and data characteristics with context information to prioritize risk and alerts in your environment.

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



B. SideScanning™ Uses The Inventions Of At Least Claims 2-8, 10, 12-15, 17-18, and 20-23

1. Claim 2

56. Orca's SideScanning™ uses the features recited in the additional limitations of claim 2 of the '809 Patent (reproduced below):

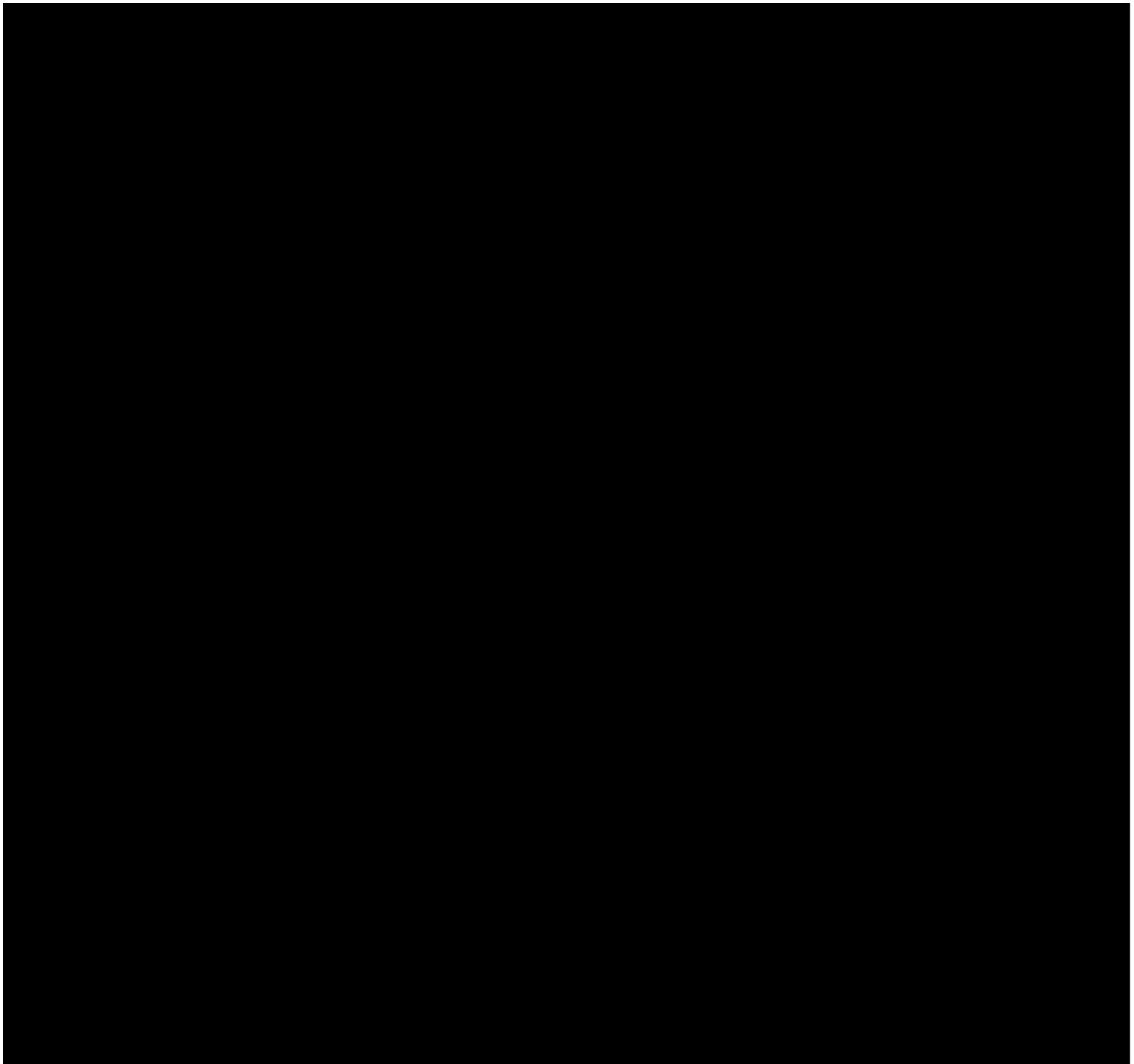
Claim 2: The method of claim 1, wherein reporting the determined potential cyber vulnerabilities includes communicating the prioritized alerts to a user console or a security information and event management (SIEM) system.

57. As explained above, Orca's SideScanning™ reports determined cyber vulnerabilities as alerts. These alerts are accessible via a user console or a SIEM system, including in Orca dashboards accessible to users.

Showing Alerts in Context

Orca combines conclusions from different environmental perspectives into a single model. It takes the asset map from the control plane—where the service meshes and containers talk to each other—and enriches this information with the risk data gathered from the workload deep scanning. For example,

Ex.2067 (SideScanning Technical Brief (2020)), 16 (highlighted).

**2. Claim 3**

58. Orca's SideScanning™ uses the features recited in the additional limitations of claim 3 of the '809 Patent (reproduced below):

Claim 3: The method of claim 2, further comprising filtering the determined potential cyber vulnerabilities based on a determined risk level associated with each determined potential alerts reports to a user console or a SIEM system is less than a total number of the determined potential cyber vulnerabilities.

59. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

This allows SideScanning™ to “do[] away with thousands of meaningless security alerts to provide just the critical few that matter, along with their precise path to remediation. Ex.2067 (SideScanning Technical Brief (2020)), 19, 18 (“Combining Low Severity Issues into Larger Alerts”).

3. Claim 4

60. Orca’s SideScanning™ uses the features recited in the additional limitations of claim 4 of the ’809 Patent (reproduced below):

Claim 4: The Method of claim 3, wherein determining the risk of the protected virtual cloud asset to the cloud computing environment is based on external intelligence on the likelihood of the determined potential cyber vulnerabilities being exploited.

61. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4. Claim 5

62. Orca's SideScanning™ uses the features recited in the additional limitations of claim 5 of the '809 Patent (reproduced below):

Claim 5: The method of claim 4, wherein determining a risk of the protected virtual cloud asset to the cloud computing environment includes: analyzing a configuration of the protected virtual cloud asset, and wherein the method further comprises: weighting a takeover risk of the protected virtual cloud asset.

63. For example, SideScanning™ analyzes “configuration information” to determine a risk of the protected cloud asset to the cloud computing environment that is “only [] vulnerable in specific configurations.” Ex.2067 (SideScanning Technical Brief (2020)), 12. SideScanning™ will also “augment[]” its “vulnerability scanning results” “with configuration-specific details,” such as

“which user is on a machine, its services . . . in addition to application-specific configurations” and “lateral-movement risks” that are part of weighting a takeover risk of the protected virtual cloud asset. Ex.2067 (SideScanning Technical Brief (2020), 12, 13-14.

5. Claims 6 and 17

64. Orca’s SideScanning™ uses the features recited in the additional limitations of claims 6 and 17 of the ’809 Patent (reproduced below):

Claim 6: The method of claim 1, wherein analyzing the snapshot of the at least one virtual disk includes matching application files on the snapshot of the at least one virtual disk directly against application files associated with a known list of vulnerable applications.

Claim 17: The non-transitory computer readable medium of claim 16, wherein analyzing the snapshot of the at least one virtual disk further includes matching application files on the snapshot of the at least one virtual disk directly against application files associated with a known list of vulnerable applications.

65. For example, during “Vulnerability Scanning,” SideScanning™ “extracts all the OS packages, libraries, and program libraries” and “gathers library versions and other identifying characteristics,” then “tries matching them to known vulnerabilities in its vulnerability database.” Ex.2067 (SideScanning Technical

Brief 2020), 11; [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

6. Claims 7 and 18

66. Orca's SideScanning™ uses the features recited in the additional limitations of claims 7 and 18 of the '809 Patent (reproduced below):

Claim 7: The method of claim 1, wherein analyzing the snapshot of the at least one virtual disk includes matching application files on the snapshot of the at least one virtual disk by: computing a cryptographic hash against at least one application file to be matched; and matching the computed cryptographic hash against a database of files associated with a known list of vulnerable applications.

Claim 18: The non-transitory computer readable medium of claim 16, wherein analyzing the snapshot of the at least one virtual disk further includes matching application files on the snapshot of the at least one virtual disk by: computing a cryptographic hash against at least one application file to be matched; and matching the computed

cryptographic hash against a database of files associated with a known list of vulnerable applications.

67. As explained above, SideScanning™ “extracts all the OS packages, libraries, and program libraries” and “gathers library versions and other identifying characteristics,” then “tries matching them to known vulnerabilities in its vulnerability database.” Ex.2067 (SideScanning Technical Brief 2020), 11; [REDACTED]

[REDACTED] As part of its analysis, SideScanning™ computes a hash for an application file and matches that hash against its vulnerability database. For example, SideScanning™ matches hashes against known vulnerabilities in its vulnerability database that includes “aggregated vulnerability data from” “OVAL.” Ex.2067 (SideScanning Technical Brief (2020)), 11.

7. Claim 8

68. Orca’s SideScanning™ uses the features recited in the additional limitations of claim 8 of the ’809 Patent (reproduced below):

Claim 8: The method of claim 1, wherein analyzing the snapshot of the at least one virtual disk includes: parsing the snapshot of the at least one

virtual disk; and scanning the parsed snapshot of the at least one virtual disk to detect the potential cyber vulnerabilities.

69. For example, SideScanning™'s “Data Plane Path” and “Analysis” parses snapshots to extract “OS packages, libraries, and program language libraries,” and scans the parsed snapshot as part of “Vulnerability Scanning.” Ex.2067 (SideScanning Technical Brief (2020)), 3 (“Detect risks such as vulnerabilities”), 11 (describing “Vulnerability Scanning”).

8. Claim 10

70. Orca's SideScanning™ uses the features recited in the additional limitations of claim 10 of the '809 Patent (reproduced below):

Claim 10: The method of claim 1, further comprising mitigating a potential cyber vulnerability posing a risk to the protected virtual cloud asset.

71. For example, SideScanning™ provides a “precise path to remediation” to mitigate vulnerabilities affecting virtual machines and other cloud assets in a cloud environment. Ex.2067 (SideScanning Technical Brief (2020)), 19.

9. Claim 12

72. Orca's SideScanning™ uses the features recited in the additional limitations of claim 12 of the '809 Patent (reproduced below):

Claim 12: The method of claim 1, wherein determining the location of the snapshot of at least one virtual disk further includes determining a virtual disk allocated to the protected virtual cloud asset.

73. [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10. Claims 13 and 20

74. Orca's SideScanning™ uses the features recited in the additional limitations of claims 13 and 20 of the '809 Patent (reproduced below):

Claim 13: The method of claim 1, wherein determining the location of the snapshot of at least one virtual disk further includes: using an API or service provided by the cloud computing environment for taking the snapshot or requesting the taking of the snapshot.

Claim 20: The system of claim 19, wherein determining the location of the snapshot of at least one virtual disk further includes: using an API or service provided by the cloud computing environment for taking the snapshot or requesting the taking of the snapshot.

75. [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11. Claims 14 and 21

76. Orca's SideScanning™ uses the features recited in the additional limitations of claims 14 and 21 of the '809 Patent (reproduced below):

Claim 14: The method of claim 13, wherein determining the location of the snapshot of at least one virtual disk further includes obtaining the location of the snapshot after the snapshot is taken.

Claim 21: The system of claim 20, wherein determining the location of the snapshot of at least one virtual disk further includes obtaining the location of the snapshot that is taken.

77.

12. Claims 15 and 22

78. Orca's SideScanning™ uses the features recited in the additional limitations of claims 15 and 22 of the '809 Patent (reproduced below):

Claim 15: The method of claim 1, wherein determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the location so the virtual disk.

Claim 22: The system of claim 19, wherein determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the location of the virtual disk.

79. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

80. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13. Claim 23

81. Orca's SideScanningTM uses the features recited in the additional limitations of claim 23 of the '809 Patent (reproduced below):

Claim 23: The method of claim 1, further comprising copying the snapshot of the at least one virtual disk; and further wherein analyzing the snapshots of the at least one virtual disk comprises analyzing the copy of the snapshot.

82. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

83. SideScanning™ analyzes copies of a snapshot to, for example, “extract[] all the OS packages, libraries, and program libraries” and “gather[] library versions and other identifying characteristics,” then “tries matching them to known vulnerabilities in its vulnerability database.” Ex.2067 (SideScanning Technical Brief 2020), 11; [REDACTED]

[REDACTED]

[REDACTED]

IV. Orca’s SideScanning™ Solved Long-Standing Industry Problems

84. Before Orca, I had never seen or heard of a person or company analyzing snapshots of virtual disks to conduct security assessments of, and detect vulnerabilities in, virtual assets in cloud environments, including by using existing cloud computing service platform APIs, with the other elements claimed in the ’809

Patent. I do not believe there was ever such a cloud security system before Orca's, and multiple people in the industry and Orca customers have recognized this, for example, by commenting that SideScanning™ was novel and ushered in a new era of agentless cloud security.

85. Before I filed the '718 Provisional Application in January 2019, it was my experience that companies in the cloud security industry had tried to adapt on-premises security approaches and apply conventional wisdom from legacy technologies to cloud technologies. For example, companies in the industry were trying to adapt traditional security tools designed for on-premise physical computers to the cloud environment, either checking all traffic going in or going out (network security), attempting to install agents within each virtual asset within the system (endpoint security), or using network scanners to probe the virtual assets. I determined that, while those tools may have been effective for discrete numbers of physical machines or services, they were not adequate for enormous and dynamically changing numbers of virtual assets in cloud environments. This led to multiplying vulnerabilities and tremendous uncertainty in that large organizations had little insight into which services operated in their environment, who owned those services, who was obligated to maintain them, and the risks associated with them. It was not practical to use the conventional approaches on these environments.

86. I describe these conventional approaches, and the disadvantages that I determined with those conventional approaches, in the background of the '809 Patent. *See, e.g.*, '809 Patent, 1:47-2:17 (describing “traffic inspection,” “network scanner[s] deployed out of path,” “traffic monitor[ing],” and “agents installed in each server”); '809 Patent, 1:49-55 (explaining that traffic inspection is traditionally “performed by a network device connected between a client and a server . . . hosting virtual machines,” and “may not provide an accurate indication of the security status of the server due to inherent limitations, such as encryption and whether the necessary data is exposed in the communication”); '809 Patent, 1:56-60 (describing “network scanner[s] deployed out of path,” which include a “scanner [that] queries the server to determine if the server executes an application that possess[es] a security threat, such as [a] vulnerability in the application”); '809 Patent, 1:60-62 (explaining that a “disadvantage” of network scanners is that “the server may not respond to all queries by the scanner” or that the server may “not expose the necessary data in the response”); '809 Patent, 1:63-67 (explaining that “the network configuration may prevent” the network scanner from “communicat[ing] with the server,” and “some types of queries may require credentials,” which “may not be available to the scanner,” “to access the server.”); '809 Patent, 2:1-:4 (describing “traffic monitor[ing],” which includes a “traffic monitor that listens to traffic flows between clients and the server” to “detect some cyber threats, e.g., based on the

volume of traffic.”); ’809 Patent, 2:4-9 (explaining that “the monitor can detect threats only based on the monitored traffic” and “may not [] detect[]” “misconfiguration of the server,” which “would not allow detection of vulnerabilities in software executed by the server.”); ’809 Patent, 2:11-17 (describing methods “based on agents installed in each server in a cloud computing platform or data center,” which are “cumbersome [] for a number of reasons, including IT resources management, governance, and performance. For example, installing agents in a large data center may take months.”).

87. I also discussed these same problems at multiple conferences and videos after I filed the ’718 Provisional Application. For example, in Ex.2082 (video of “Orca Security - SideScanning vs Traditional Security Assessment Methods,” <https://www.youtube.com/watch?v=0SDwFzINzGM>), I explained the following:

[S]o in order to answer that I’d like to explain a bit how we did in fact security posture monitoring before Orca and what are the problems that we are trying to solve. So back in the day before the cloud environments we had hosts. We wanted to secure hosts, and the most trivial answer is to install security agents on them. Naturally they reside on hosts. They can have full visibility to anything that is running on them, detect any rogue activity in the OS, application, detect data that shouldn’t be there etc. The main issue, that I’m sure all of you know, is that you need to install them. You need to install, you

need to maintain, you need to upgrade them. And if they are not installed and maintained they are simply invisible to you. So, a different approach that we used to have is to try to scan from the network, deploy network scanners. They try to probe things externally, either using authenticated and unauthenticated mechanisms. And these were basically the options that we have on the pre-cloud world. If you think about it, if you want to scan physical machines there's absolutely no alternative rather than installing agents or scanning from the network. So, we've used these two mechanisms, although they are far from perfect. When the cloud came what we actually did as an industry is to copy what we had. We had network scanners -- physical network scanners -- now we have virtual network scanners. We had agents that ran on the environment, on the physical machine, now, they are running on the virtual machines. And we simply added another beast, the cloud security posture manager tools that monitor the cloud configuration itself. So, things like the networks the machines are sitting in, the roles, etcetera. And we basically ended up with having the pre-cloud tools moved to the cloud augmented by the cloud security posture managers, tools like RedLock, Dome 9 etc. But we saw two main problems that we wanted to solve. First is the problem of agent deployment, that it does not scale. On average, we saw that organizations have less than 50 percent of their assets are covered by all

security solutions. It's almost impossible to deploy everywhere. There is a huge intra-organizational friction in order to get them deployed, and even organizations that put people working full-time to deploy that resulted in a very, very limited deployment. And the second problem is there are simply too many security alerts. On average you can see approximately 10,000 vulnerabilities to every 100 assets. And the reason for that is simply because these tools work in silos. They don't really know the overall picture.

Ex.2083 (transcript of "Orca Security - SideScanning vs Traditional Security Assessment Methods," <https://www.youtube.com/watch?v=0SDwFzINzGM>), 1; *see also* Ex.2082 (video of "Orca Security - SideScanning vs Traditional Security Assessment Methods," <https://www.youtube.com/watch?v=0SDwFzINzGM>), 0:10-3:00.

88. As another example, in Exhibit 2100 (page capture of "An MRI for Your Cloud Environment," <https://orca.security/resources/video/sidescanning-a-cloud-environment-mri/>), I explained that, "[b]efore SideScanning, security teams had no choice but to invest numerous resources into installing invasive security agents and still suffered from breaches on account of partial visibility." Ex.2100 (page capture of "An MRI for Your Cloud Environment," <https://orca.security/resources/video/sidescanning-a-cloud-environment-mri/>), 2.

89. In an interview, I explained that companies had employed solutions using “network scanners” and “authenticated, unauthenticated agents” “for the last 20 years.” Ex.2133 (page capture of “Orca Security: Deep Cloud Inspection,” <https://orca.security/resources/product-info/sidescanning-deep-cloud-security-inspection-across-aws-azure-gcp/>), 3; *see also* Ex.2099 (page capture of “Orca Security - Deep Cloud Inspection,” <https://www.youtube.com/watch?v=VwZ-7guGHw0>). I also explained that Orca “run[s] on the same data center via APIs and read[s] the same data that the workload reads,” unlike “20 years ago” when “you had another interface in each server that the scanner and a magic cable connected to.” Ex.2133 (page capture of “Orca Security: Deep Cloud Inspection,” <https://orca.security/resources/product-info/sidescanning-deep-cloud-security-inspection-across-aws-azure-gcp/>), 4. I further explained:

[W]hen I looked at this product together with the other co-founders, we haven’t asked how many companies out there this question, but a more basic question, is there a solution that they can simply deploy? And will alert if I have, let’s say, a vulnerable asset in my environment? And it must always work, not after I run through four months deployment, it will cover 80%. Is there a solution that can alert if I have a machine with even known malware in my organization that I can trust it will always work? And unfortunately, the answer is no. There is no single solution out there that can generally

answer this question for all of your cloud environment. All of them overlook disclaimers. It will work if you've done that, it will work if you integrated that, and these are the processes that organizations simply cannot follow. So we wanted to create something really unique that can answer this question and work 100% of the time for all of the assets.

Ex.2133 (page capture of "Orca Security: Deep Cloud Inspection," <https://orca.security/resources/product-info/sidescanning-deep-cloud-security-inspection-across-aws-azure-gcp/>), 2.

90. When I filed the '718 Provisional Application in January 2019, and for years afterwards, many people in the industry disagreed that network scanners and agent-based solutions were inadequate for cloud security. There were many companies at the time that were developing, and had created successful businesses, with agent-based solutions.

91. For example, Qualys released its Cloud Agent Platform. Ex.2102 (<https://www.bankinfosecurity.com/press-releases/qualys-unveils-cloud-agent-platform-for-continuous-asset-p-223>), 1 ("Qualys, Inc. . . . announced the launch of Qualys Cloud Agent Platform (CAP), a revolutionary new platform that extends Qualys' industry-leading Cloud Security and Compliance Platform with lightweight agents to continuously assess security and compliance of organizations' global IT infrastructure and applications. . . . [T]he challenges of establishing scanning

windows and authenticated scans, managing and updating heavyweight agents, and the rise of cloud and mobile environments, have proven difficult and cost prohibitive for most companies. The Qualys Cloud Agent Platform resolves this conundrum by combining the power of its Cloud Platform with lightweight agents that are extensible, centrally managed and self-updating.”). And, as another example, as of 2018, Twistlock and Aqua Security offered security agents to secure organizations’ networks.

92. Therefore, at Orca, we had to show companies that their existing solutions had major problems, and that we had solved those problems with my patent-pending SideScanning™ inventions.

93. After my patent applications were filed, and we began describing our inventions to the industry, other companies began copying our messaging, similarly emphasizing the problems with conventional approaches that my inventions solved. I provide two examples of this below.

Traditional approaches used for on-premises, like security agents, have significant limitations in the cloud. However, a new “agent-less” approach to cloud security has recently become possible due to cloud-native APIs now available from CSPs. This approach provides security in a fundamentally different way – taking advantage of the unique characteristics of the cloud while being best suited to the dynamic nature of the cloud.

Ex.2103 (Security Agents Don’t Belong in Your Cloud!), 1.

Challenges with Agent-Based Vulnerability Scanning

One of the drawbacks of agent-based vulnerability scanning is that they are operating system (OS) dependent and generally can't scan network assets like routers, switches, and firewalls. However, most agent-based scanning solutions will have support for multiple common OSes.

Agent-based scanning also comes with administrative overhead as new devices added to the network must have agents installed. While updates of agents are usually automated, new installs and changes in scanners will require extra work for IT staff.

Ex.2104 (Agent-Based vs. Agentless Scanning: Choosing the Right Vulnerability Scanning Method), 2.

94. Security industry specialists remarked that Orca “introduced the concept of agentless side scanning” and helped redefine the cloud security posture management (CSPM) market.

- **Orca:** Introduced the concept of **agentless side scanning**, which allowed for deep visibility into cloud environments, and workloads, without the need to install agents on each workload. CSPM can be defined by pre and post-Orca: the ability to view workload data without an agent was a genuinely genius innovation - utilizing the nature of cloud APIs being accessible to vendors.

Ex.2076 (Guide to the Future of Cloud Security), 7.

Deployment options for cloud security (Agent vs Agentless)

One of the central discussion points about the evolution of cloud security is how much the role of agents and agentless played throughout the history, and how relevant the question is today. There is no doubt, the pivotal moment was the introduction of **agentless** scanning by companies like Orca and Wiz. Agentless scanning was a turning point - but anyone who tells you they knew it at the time is lying. We're old enough to remember when these tools were finding their messaging foothold - trying everything from risk based prioritization to compliance scanning. This was a subtle industry move that wasn't appreciated until years later, in no small part due to how Wiz used it to define the CNAPP conversation.

Ex.2076 (Guide to the Future of Cloud Security), 8.

How Agentless Scanning Emerged

As discussed earlier, Orca launched the first version of **agentless side scanning**, which allowed deep visibility into cloud workloads without the need to install agents. Subsequently, Wiz was able to make the experience more intuitive with the graph and more fully bring the approach to market. There's a lot you can do without an agent, and with most security teams already overwhelmed by that work, it's hard to argue they're looking for even more to do.

Ex.2076 (Guide to the Future of Cloud Security), 11.

Orca Security

Solution Overview

Orca Security delivers security through its agentless platform, focusing on visibility and risk management across cloud environments. The company's innovative SideScanning technology enables deep workload inspection without requiring agent deployment.

The Orca Cloud Security Platform operates as a unified solution, offering integrated capabilities for workload protection, vulnerability management, compliance monitoring, and cloud security posture management. The platform's architecture leverages read-only access to cloud provider APIs and workload runtime block storage, enabling comprehensive security coverage without operational impact.

Orca's approach emphasizes simplified deployment and reduced operational overhead through its agentless architecture while maintaining visibility into CWS risks.

Positioned in the Maturity half of the Radar chart, Orca Security demonstrates a steady progression of features and enhancements that looks and feels the same year over year. The platform's continuous evolution focuses primarily on expanding cloud provider coverage, enhancing detection capabilities, and strengthening integration with enterprise security workflows, demonstrating Orca's commitment to innovation in CWS.

Orca is positioned as a Leader and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Ex.2148 (GigaOm Radar for Cloud Workload Security), 15.

V. Orca Overcame Skepticism About SideScanning™'s Efficacy

95. As discussed above, when Orca introduced SideScanning™, many people did not believe there were problems with agent-based or network scanning approaches, and they did not believe that my agentless SideScanning™ approach would work.

96. Palo Alto Networks (“PAN”), for example, was and continues to be a very well-known company in cloud security. Two years after we introduced our patent-practicing agentless SideScanning™, in February 2021, PAN published an article where they used “agentless” and “side-scanning” (Orca’s trademark) interchangeably, and wrote that agentless scanning of cloud native workloads, because it relied on snapshots, could only deliver “rudimentary security capabilities.”

Recently, new agentless or ‘side-scanning’ solutions have emerged claiming to provide a lightweight design that delivers security for cloud native workloads. Unfortunately, this lightweight architecture only delivers rudimentary security capabilities, mostly useful for compliance. These solutions fail to take advantage of immutable infrastructure principles and only offer a ‘point-in-time’ view, or ‘snapshot’ of what’s running at any given time. They cannot capture the dynamic evolution of workloads or provide

runtime attack prevention and policy enforcement. Here we present a few scenarios that demonstrate this shortcoming.

Ex.2106 (How Agentless Approaches Sideline Cloud Workload Protection Strategies), 1.

97. Industry reports have acknowledged how difficult it was for Orca to overcome this type of skepticism, because the way Orca implemented agentless scanning was entirely different from what came before.

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

Ex.2076 (Guide to the Future of Cloud Security), 7.

VI. My SideScanning™ Inventions Drove Orca's Commercial Success

98. Orca first introduced its Orca Cloud Security Platform, which is powered and driven by my SideScanning™ inventions, including the claimed inventions of the '809 Patent, in early 2019, and, as I explained above, Orca's SideScanning™ continues to use those inventions today.

99. In the five years since Orca first introduced SideScanning™, Orca has had investment rounds totaling over \$600 million, earned over [REDACTED]

██████████ from SideScanning™, and grown from fewer than a dozen to more than 400 employees. Orca has only sold products that are powered and driven by SideScanning™, including the inventions of the '809 Patent.

100. Orca also has earned significant revenues from sales of the Orca Cloud Security Platform using SideScanning™, ██████████

██

██

██

██

██

██

101. Orca, its investors, and third-party commentators have attributed Orca's success to Orca's "patent-pending SideScanning™ technology," which, as I have explained, refer to the inventions described in my '718 Provisional Application, including those recited in the claims of the '809 Patent. Orca's revenues and ability to raise outside investment are a direct result of the unique characteristics of the claimed inventions of the '809 patent.

102. Orca's first fundraising round, in June 2019, raised \$6.5 million in external investments. Attached as Exhibit 2065 is a true and correct copy of Orca's press release about that fundraising. As that press release shows, this success was attributable to unique features claimed in the '809 Patent. For example, the press

release explained that “[t]he Orca Cloud Visibility Platform leverages Orca’s patent-pending SideScanning technology to deliver comprehensive and seamless visibility into the security posture of an organization’s complete cloud footprint in a matter of minutes.” Ex.2065 (*Orca Security Lands \$6.5M Seed Round*), 2. The press release emphasized the “single and simple integration into the cloud infrastructure layer to automatically assess the security state of every discovered asset throughout the entire technology stack,” and that Orca’s SideScanning™ technology “expose[s] issues such as operating system and application level vulnerabilities and compromises.” Ex.2065 (*Orca Security Lands \$6.5M Seed Round*), 3. We secured this original funding because SideScanning could analyze assets and determine “[w]hich servers are vulnerable,” which is what is claimed in the ’809 patent. Ex.2065 (*Orca Security Lands \$6.5M Seed Round*), 4. 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.” Ex.2065 (*Orca Security Lands \$6.5M Seed Round*), 4; ’809 Patent, limitations 1.1, 1.3, 16.1, 16.3, 19.1, 19.3. The press release also emphasized Orca’s ability to integrate with cloud computing service platforms to allow “complete visibility into compromised resources [and] vulnerable software,” all without agents or network scanners. Ex.2065 (*Orca Security Lands \$6.5M Seed Round*), 3; ’809 Patent, limitations 1.1, 1.3, 16.1, 16.3, 19.1, 19.3.



Ex.2065 (Orca Security Lands \$6.5M Seed Round), 4.

103. Orca’s next funding round, around May 2020, included investments totaling another \$20M. Attached as Exhibit 2108 is a true and correct copy of the press release about this fundraising. This press release explained that Orca “created the first and only cloud security solution that can find vulnerabilities ... lateral movement risk, and high-risk data without agents or per asset integrations, literally within minutes.” Ex.2108 (*Orca Security Lands \$20 Million Series A*), 1. The press release also explained that “[t]his unique ability is achieved using Orca Security’s patent-pending SideScanning™ technology, which is based on reading the workloads’ run time block storage out of band, and cross-referencing this with cloud

context pulled directly from the cloud vendors' APIs." Ex.2108 (*Orca Security Lands \$20 Million Series A*), 1; '809 Patent, claims 1, 16, 19. The press release explained that "unlike point solutions that work in silos, Orca treats a customer's cloud estate as an interconnected web of assets, prioritizing risk based on environmental context." Ex.2108 (*Orca Security Lands \$20 Million Series A*), 1; '809 Patent, claims 1.5-1.7, 16.5-16.7, 19.5-19.7.

104. As another example, a third-party article about Orca's second funding round emphasized that Orca's success was attributable to using "low-level APIs," i.e., the use of cloud-computing platform APIs, to gain visibility into what is running in a customer's cloud, which provided "unparalleled visibility":

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 that allow it to gain visibility into what exactly is running in your cloud.

Ex.2109 (Orca Security raises \$20M Series A for its multi-cloud security platform (TechCrunch)), 1.

“In a software-driven world that is moving faster than ever before, it’s extremely difficult for security teams to properly discover and protect every cloud asset,” said GGV managing partner Glenn Solomon. “Orca Security’s novel approach provides unparalleled visibility into these assets and brings this power back to the CISO without slowing down engineering.”

Ex.2109 (*Orca Security raises \$20M Series A for its multi-cloud security platform (TechCrunch)*), 2 (highlighted); ’809 Patent, limitations 1.1, 1.2, 16.1, 16.2, 19.1, 19.2.

105. Orca also landed several notable companies as customers because of its SideScanning™, including Flexport, Fiverr, Sisense, and Qubole. Ex.2109 (*Orca Security raises \$20M Series A for its multi-cloud security platform (TechCrunch)*), 2.

106. Orca’s third funding round, around December 2020, included investments totaling \$55M. Attached as Exhibit 2110 is a true and correct copy of Orca’s press release about this fundraising. As that article explained, this funding “fuel[ed] Orca Security’s further disruption of the cloud security industry with touchless, workload-deep, context-aware security and compliance” that, for example, “helps to reduce thousands of security alerts to the critical few that matter, along with their precise path to remediation.” Ex.2110 (*Orca Security Lands \$55 Million Series B*), 1. One lead investor remarked “[SideScanning™] not only depicts vulnerabilities, but also outlines the full context of the business and cloud

environment.” Ex.2110 (*Orca Security Lands \$55 Million Series B*), 2; '809 Patent, limitations 1.5-1.6, 16.5-16.6, 19.5-19.6.

107. We were able to get these investments because of the novel aspects of SideScanning™ that are claimed in the '809 Patent. And, as we noted in a press release at the beginning of 2021, Orca achieved “historic” success in 2020 as we were able to secure “both our series A and B funding rounds.” Ex.2140 (*From Stealthy Startup to Cloud Security Innovation Leader*), 1-2. Exhibit 2140 is a true and correct copy of that press release.

108. Investors and security professionals remarked, for example, that “[w]hat 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.” Ex.2111 (*Orca Security Raises \$55M for Its Cloud-Native Security Platform (TechCrunch)*), 1. Furthermore, “[b]ased on this, in combination with the cloud metadata it collects, it can map and scan a company’s entire data estate and its cloud assets — and find potential security issues,” relevant to '809 Patent limitations 1.1-1.5, 16.1-16.5, and 19.1-19.5. Also, “Orca [] aims to provide security practitioners with relevant alerts based on the context of the exposure and business impact.” Ex.2111 (*Orca Security Raises \$55M for Its Cloud-*

Native Security Platform (TechCrunch)), 2; '809 Patent, limitations 1.6-1.8, 16.6-16.8, 19.6-19.8. The article further recognized, for example:

Clearly, Orca has hit on a winning formula here. Shua tells me that the company grew more than 10x this year already and instead of growing the team to about 50 employees, it's already at 70 now. At one point this summer, simply scheduling a call with a salesperson at Orca could take three weeks. Given this, it's maybe no surprise that Orca wanted to raise to continue to accelerate this growth (and that VCs would want to put more money into the company).

Ex.2111 (Orca Security Raises \$55M for Its Cloud-Native Security Platform (TechCrunch)), 4.

109. Orca's next funding round, around March 2021, included investments totaling another \$210M, and made Orca one of the fastest cybersecurity companies in history to achieve a \$1 billion valuation. Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 1. As the CRN press release attached as Exhibit 2112 explains, Orca secured this funding as Orca was “looking to expand its presence [] internationally” “after closing a monster Series C round.” Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 1-2 (also noting “Orca Security has become the fastest cybersecurity company in history to achieve a \$1 billion valuation.”). The press release explains that Orca sought to utilize the inventions present in the '809 Patent to focus on “detecting attacks as they unfold by examining the risk around critical attack vectors.” Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 2; '809 Patent, limitations 1.5-

1.6, 16.5-16.6, 19.5-19.6. As we explained in the press release, SideScanning™ “prioritizes risks based on the underlying security issue combined with environmental context, including its accessibility and potential damage to the business. Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 3.

110. Orca’s rapid growth to a valuation of over \$1 billion in less than two years was because the industry recognized the value and novelty of my SideScanning™ inventions, including those directly attributable to the ’809 patent claims. As CapitalG General Partner Gene Frantz put it, “Orca Security represents a revolutionary step forward in optimizing cloud environments . . . Their touchless SideScanning technology is best in class.” Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 1-2. And, the industry recognized that, “Orca’s foundational SideScanning technology can detect vulnerabilities.” Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 3; ’809 Patent, limitations 1.3-1.4, 16.3-16.4, 19.3-19.4. Orca was “the first cloud security provider to address these risks without agents or per asset integration, giving enterprises complete visibility and coverage within minutes.” Ex.2112 (*CRN – Upstart Orca Security Raises \$210M in Google-Backed Funding*), 4.

111. Around October 5, 2021, Orca extended its Series C funding round to include investments totaling \$550M. Ex.2113 (*Orca Security Extends Series C*

Round to \$550M Boosting Valuation to \$1.8 Billion), 1. Attached as Exhibit 2113 is a true and correct copy of that press release. As we explained, Orca's "800 percent year-over-year growth" was because "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," which is the technology using, for example, the features of limitations 1.1-1.4, 16.1-16.4, and 19.1-19.4 of the '809 Patent. Ex.2113 (*Orca Security Extends Series C Round to \$550M Boosting Valuation to \$1.8 Billion*), 1. We also explained that "[t]his means that after a quick and easy one-time deployment, Orca Security surfaces critical attack vectors, composed of the most serious risks such as vulnerabilities ... while guaranteeing 100 percent security coverage for all cloud assets," which is the technology using, for example, the features of limitations 1.5-1.8, 16.5-16.8, 19.5-19.8. Ex.2113 (*Orca Security Extends Series C Round to \$550M Boosting Valuation to \$1.8 Billion*), 1. And we explained that the reason our growth is exploding is because of our ability to provide "100 percent coverage of all cloud assets" and provide "automatic prioritization of the alerts that demand quick action," which is the technology using, for example, the feature of limitations 1.7-1.8, 16.7-16.8, and 19.7-19.8. Ex.2113 (*Orca Security Extends Series C Round to \$550M Boosting Valuation to \$1.8 Billion*), 1.

112. Additionally, as noted in the press release, Orca had significantly expanded its customer base to include “BeyondTrust, Hunters, Very Good Security, BigID, and many more.” Ex.2113 (*Orca Security Extends Series C Round to \$550M Boosting Valuation to \$1.8 Billion*), 2. And, Orca was “continuing to build rapid customer traction with partners in the U.S., Europe, India, Australia, New Zealand, Latin America, and Japan.” Ex.2113 (*Orca Security Extends Series C Round to \$550M Boosting Valuation to \$1.8 Billion*), 2.

113. Industry experts also attributed Orca’s commercial success to my SideScanning™ inventions:

“Security is one of the largest challenges associated with cloud adoption. Avi and the Orca Security team have built a next-generation solution that is redefining cloud security best practices,” said Fred Wang, partner, Adams Street. “Not only does the Orca Security platform provide end-to-end visibility across a company’s cloud environment, but it can be deployed in minutes and is effortless to maintain. Orca Security’s tremendous traction across industries is a testament to the value that they are delivering to customers.”

“Orca Security’s rapid emergence as a cloud security leader is driven by customer love for its product, which is the foundation of all of our investments,” said Ken Fox, partner and founder, Stripes. “Orca Security’s SideScanning technology enables unparalleled coverage, visibility, and context with incredibly low friction. We are thrilled to partner with Avi and the Orca Security team.”

“Orca Security’s skyrocketing success has cemented its place as a category leader in a multi-billion dollar industry,” said YL Ventures managing partner, Yoav Leitersdorf. “Orca has transformed cloud security, combining best-in-class technology, high caliber human capital and a customer-verified solution to a fundamental problem. YL Ventures has supported Orca Security since its seed round, and continues to do so as Orca becomes a veritable cybersecurity heavyweight.”

Ex.2113 (*Orca Security Extends Series C Round to \$550M Boosting Valuation to \$1.8 Billion*), 3.

VII. Wiz Copied Orca's SideScanning™

114. Wiz was founded in 2020, a year after Orca, and I have been involved with dozens, if not hundreds, of competing proof of concepts for potential customers against Wiz, and customers frequently remark that the agentless snapshotting using cloud computing API core of our products are extremely similar and almost identical. I believe that Wiz copied Orca's SideScanning, and they have improperly stolen Orca's market share by forcing Orca to compete with my inventions.

115. Wiz's founders were aware of Orca's SideScanning before Wiz was founded. That is because Gil Geron, another of Orca's co-founders and current CEO, and I presented Orca's Cloud Security Platform to Wiz's founder [REDACTED]

[REDACTED] after I filed the '718 Provisional Application from which the '809 Patent claims are derived. At the time, I understood [REDACTED]

[REDACTED] Wiz's other three founders, Assaf Rapport, Roy Reznik, and Ami Luttwak were also Microsoft employees.

116. At this May 2019 meeting, we explained to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

117. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

118. The purpose of the May 2019 Microsoft meeting was to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

119. In early 2020, I began hearing rumors that there was a new company in “stealth mode” that was developing an agentless cloud computing platform that was very similar to Orca’s. That company turned out to be Wiz, which emerged from stealth on December 9, 2020, but was competing for the same customers as Orca even earlier. Based on our direct competition with Wiz and the feedback we received from potential customers, it appeared that Wiz had copied Orca’s SideScanning™ techniques, including those claimed in the ’809 Patent.

120. [REDACTED]

[REDACTED]

121. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

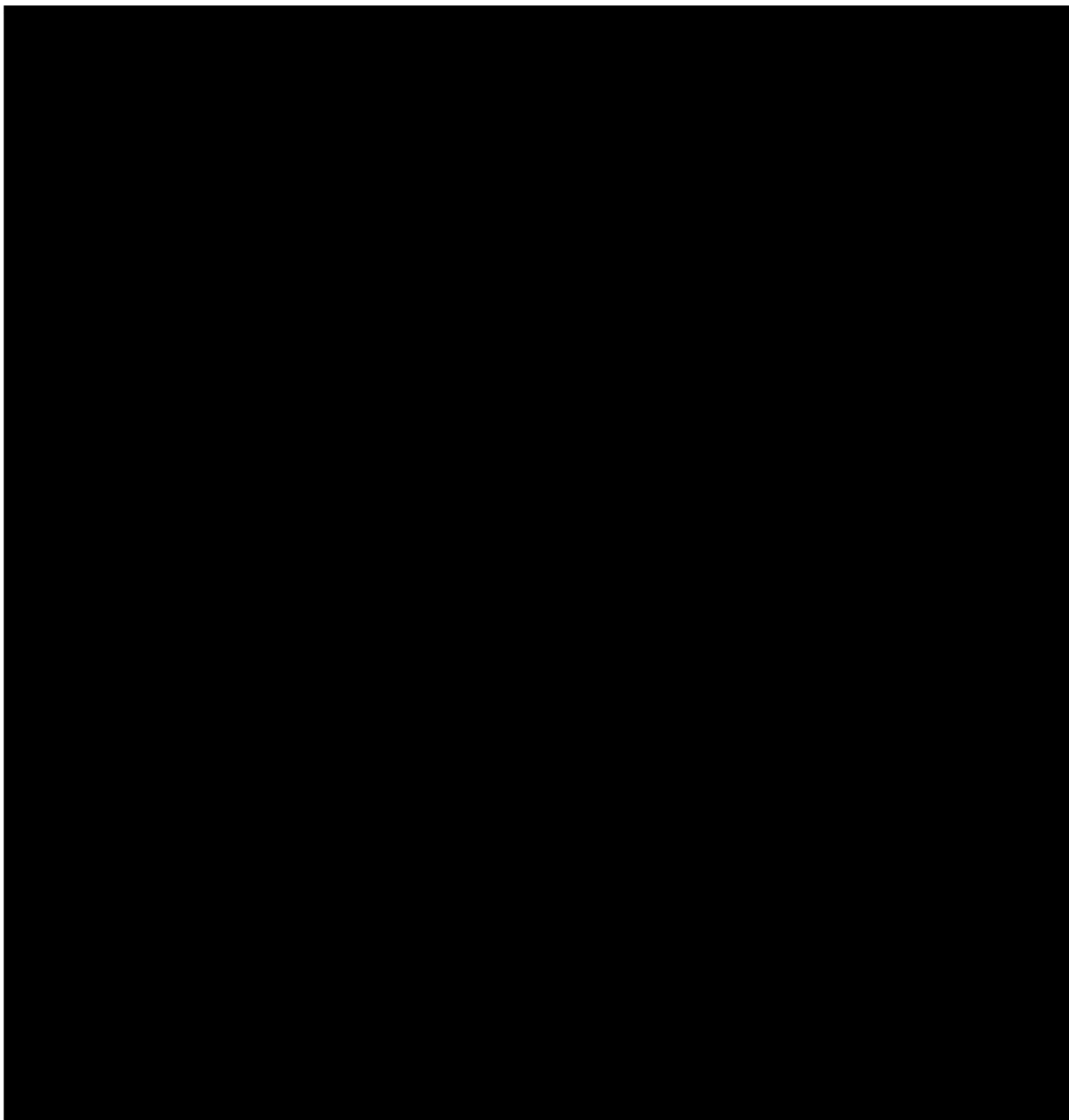
[REDACTED]

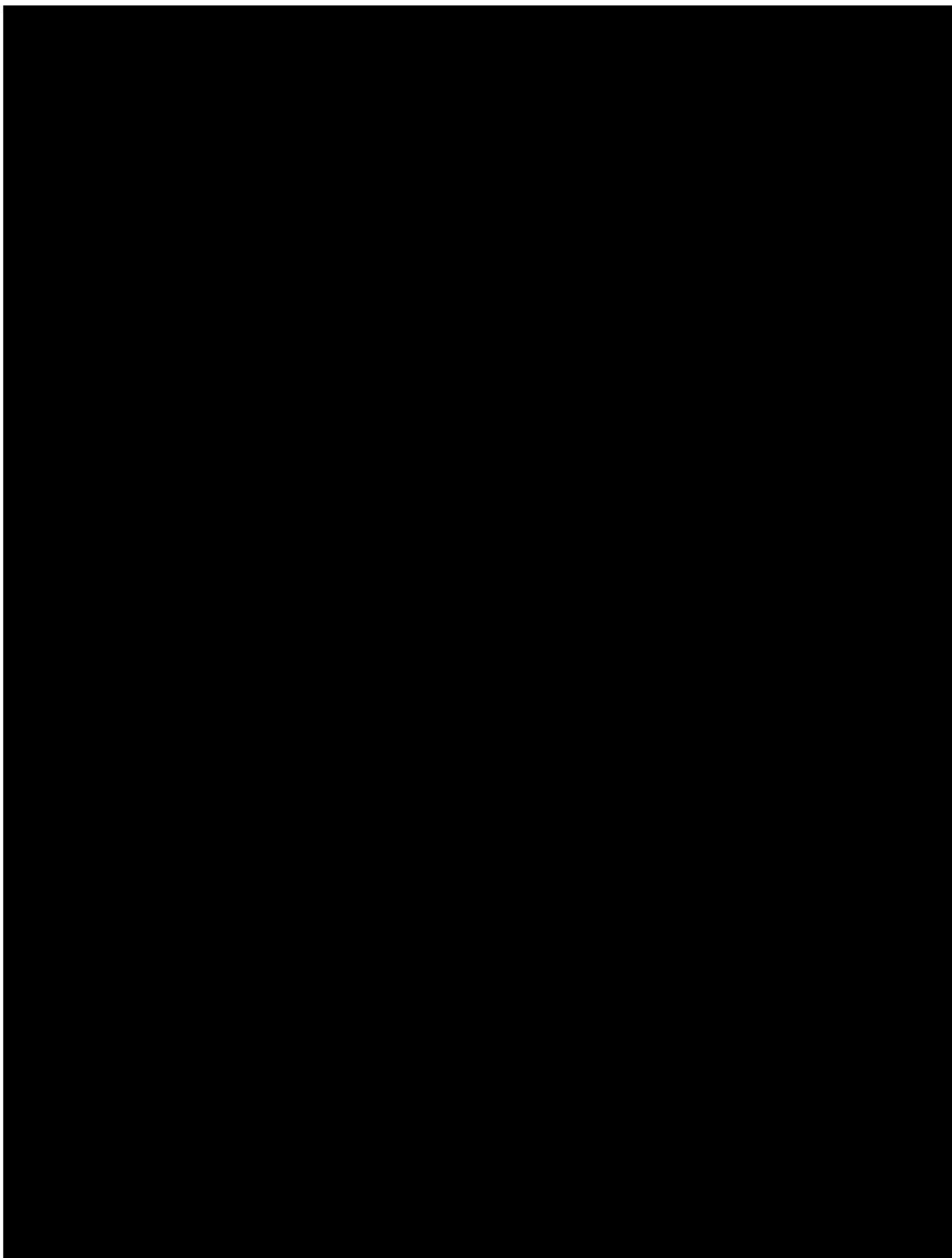
[REDACTED]

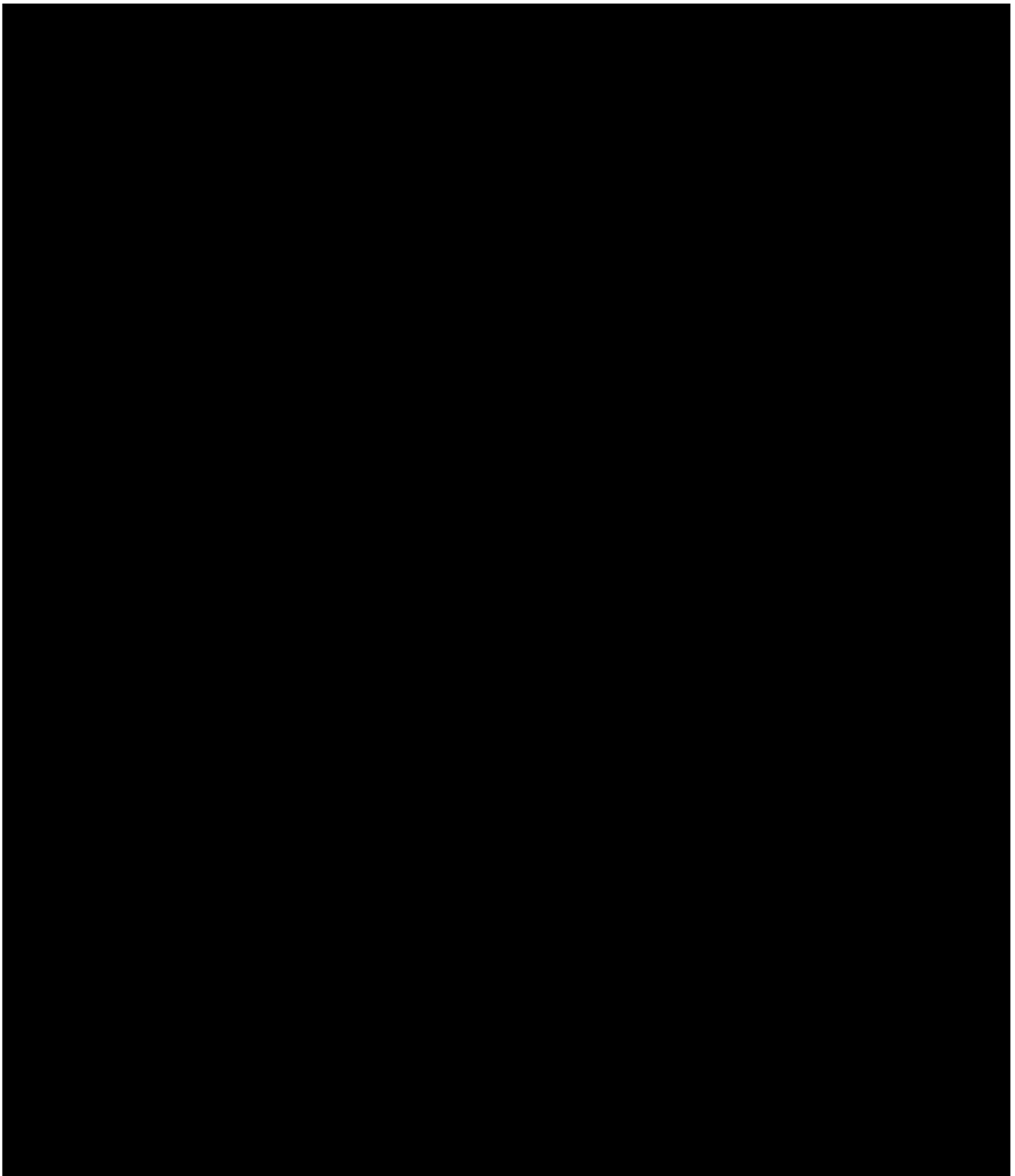
[REDACTED]

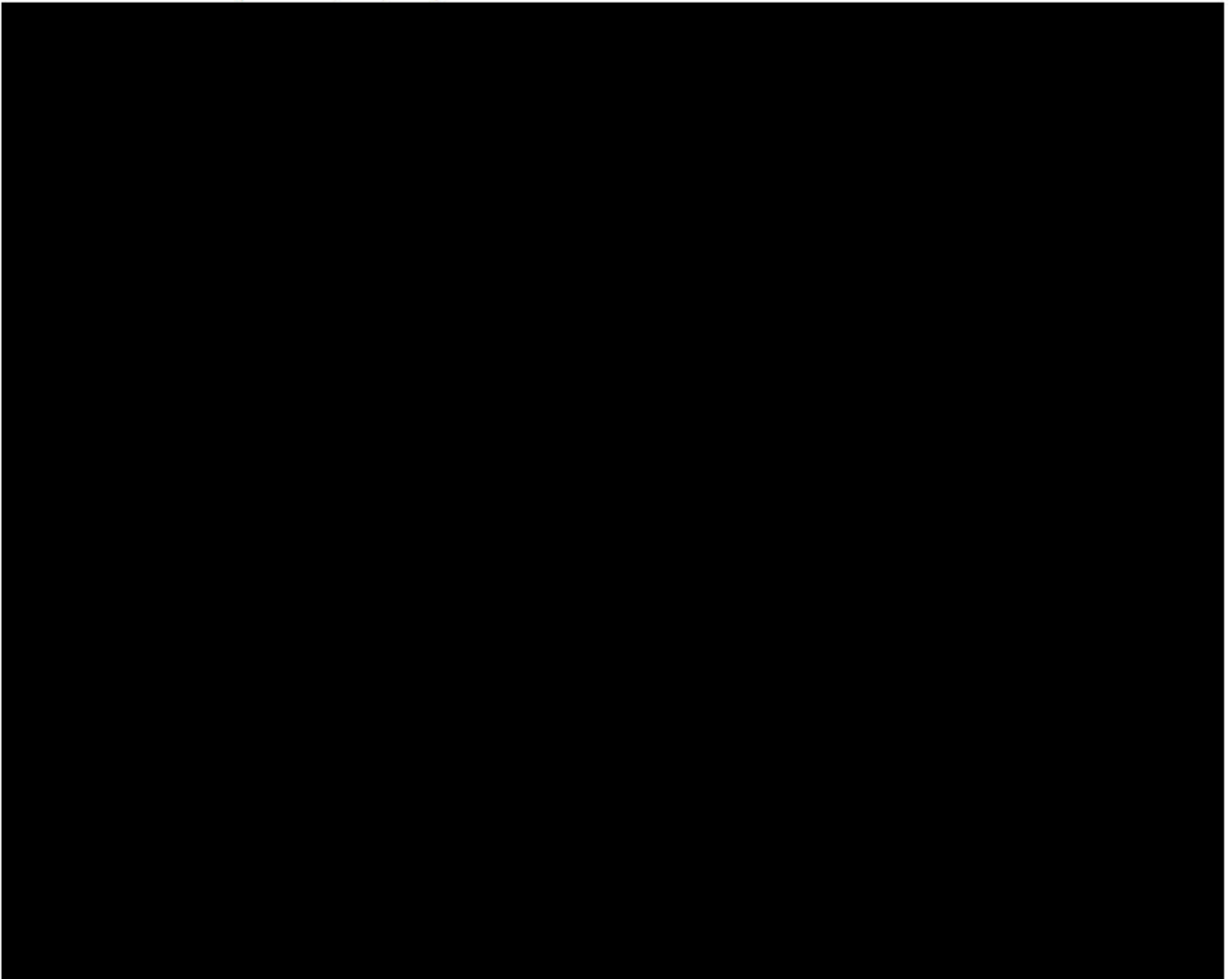
[REDACTED]

[REDACTED]









122. As of February 2021, Orca was the only company that I am aware of that used these cloud computing service platform API calls to perform security analyses of snapshots of protected virtual cloud assets (as claimed in the '809 Patent



123. In addition to the above, Wiz's marketing materials and blog posts describing Wiz's product emphasized that the "fundamental principles" that it operated on were the same as SideScanning™ and what is claimed in the '809 Patent,



such as “privileged access to the customer’s cloud environment via APIs” and “snapshot scanning.”

What is agentless security?

Agentless security provides visibility into the threats in your environments, without requiring the installation of software-driven agents.

Under the agent-based model, each of your hosts must run a monitoring process that collects data from the host’s environment and sends it to your security service. Agentless security removes this requirement by having the service collect data itself, using cloud provider APIs and metadata.

Agentless analysis approaches are based on two fundamental principles:

- Privileged access to customer’s cloud environment via APIs
- Snapshot scanning

Privileged access assigned to the security vendor enables discovery of all resources and services used in the cloud environment. This information is then processed to determine the list of workloads to be scanned.

Ex.2026 (*Agentless vs Agent-based Security*,

<https://www.wiz.io/academy/agentless-vs-agent-based-security>), 2-3.

124. Wiz also stated that using “cloud APIs” for agentless snapshot scanning is what “maximizes security coverage” and provides “compelling advantages.”

Advantages of agentless security

Agentless security solves most of the problems associated with agents. Instead of running an agent in each of your environments, agentless services sit *outside* your resources. They collate security information by monitoring data provided by cloud APIs and infrastructure services. This model presents several compelling advantages for security teams and administrators.

Simple, automatic coverage

Agentless platforms automatically monitor the resources in your cloud provider accounts.

By connecting to cloud APIs, they can discover new resources as they're created, without requiring manual installation of an agent process. This maximizes security coverage from day one, improving the visibility of security issues.

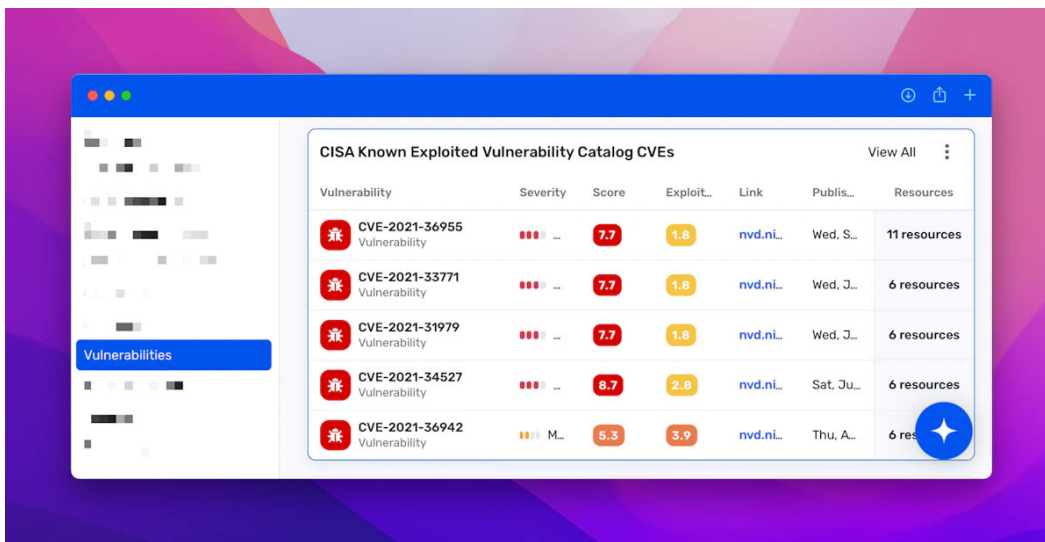
Ex.2026 (*Agentless vs Agent-based Security*,

<https://www.wiz.io/academy/agentless-vs-agent-based-security>), 7-8.

125. Wiz's scanning technology is a copy of Orca's SideScanning™, which Wiz renamed "workload scanner." Ex.2115 (*The Wiz Approach to Agentless Scanning*, <https://www.wiz.io/blog/the-wiz-approach-to-agentless-scanning>), 1. For example, in a blog post from October 2023, Wiz explained that its workload scanner does agentless scanning "using cloud APIs" and that being "API-based" is a "cornerstone of our [Wiz's] scanning technology." Ex.2115 (*The Wiz Approach to Agentless Scanning*, <https://www.wiz.io/blog/the-wiz-approach-to-agentless-scanning>), 1-2. And, like what is claimed in the '809 Patent and practiced by SideScanning™ since 2019, Wiz says its workload scanner uses cloud computing APIs and is for "creating, sharing, and deleting snapshots" where the "scanner has

read-only access to the scanned disk.” Ex.2115 (*The Wiz Approach to Agentless Scanning*, <https://www.wiz.io/blog/the-wiz-approach-to-agentless-scanning>), 3.

126. As yet another example of Wiz’s copying Orca’s SideScanning™, in a 2022 blog post, Wiz explained that it “lists all the resources in your cloud environment that are currently vulnerable to one or more vulnerabilities” and “find[s] the resources that pose the highest risk in your cloud environment,” Ex.2147 (*Detect and Prioritize CISA Known Exploited Vulnerabilities in the Cloud with Wiz*), 2-3, relevant to what is claimed in the ’809 Patent. ’809 Patent, limitations 1.8, 16.8, 19.8. I have reproduced an exemplary image showing Wiz’s “CISA Known Exploit Vulnerabilities Catalog CVEs dashboard” from that blog post below.



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

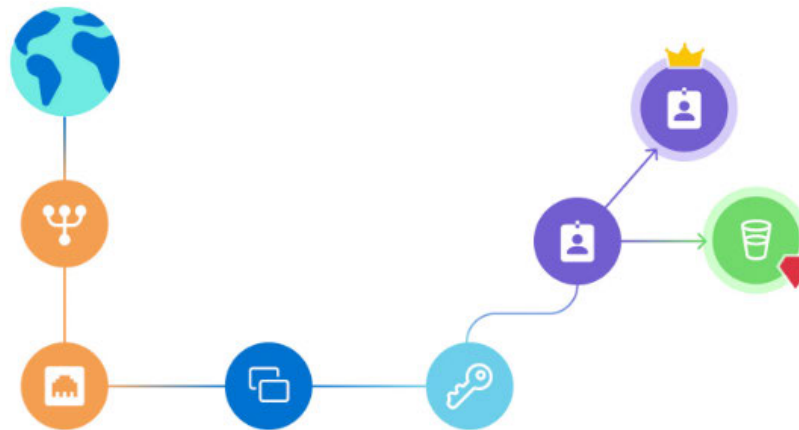
127. In the same blog post, Wiz explained that, “[f]or each CVE, the Wiz Research team maintains data from multiple threat intelligence sources and [Wiz’s] own independent research,” and “lists all the resources in [a client’s] cloud environment that are currently vulnerable to one or more vulnerabilities in the catalog,” like what is claimed in limitations 1.3-1.4, 16.3-16.4, and 19.3-19.4 of the ’809 Patent. Ex.2147 (*Detect and Prioritize CISA Known Exploited Vulnerabilities in the Cloud with Wiz*), 2.

128. In another blog post, Wiz explained that its platform can “[i]dentify and stop lateral movement” because it “provides direct visibility into your cloud environment, prioritizes risks, and offers remediation guidance,” like what is claimed in limitations 1.5-1.7, 16.5-16.7, and 19.5-19.7 of the ’809 Patent. Ex.2177 (*Wiz What Is Lateral Movement*), 10. The article explains that Wiz is capable of detecting lateral movement by “[m]ap[ping] lateral movement paths” including “[u]s[ing] attack path mapping tools to visualize relationships between compromised endpoints” like what is claimed in limitation 1.5, 16.5, and 19.5 of the ’809 Patent. Ex.2177 (*Wiz What Is Lateral Movement*), 6-7.

129. In another blog post, Wiz explained that its “approach to cloud security” is “different” from traditional solutions because it provides “Security Graph powered correlation; and prioritization of critical risks and contextual alerts” like what is claimed in limitations 1.5-1.8, 16.5-16.8, and 19.5-19.8 of the

'809 Patent. Ex.2178 (*Wiz Attack Path Analysis*), 1. Indeed Wiz describes these aspects of its platform as “the *foundation* of what makes Wiz so unique.” Ex.2178 (*Wiz Attack Path Analysis*) (emphasis added), 1. In its own words, the foundation of Wiz’s platform was a copy of the novel invention claimed in the '809 patent. The blog post explains that Wiz leveraged its “Security Graph” to “correlate dozens of disparate signals into a single prioritized risk assessment across the entire security stack,” like what is claimed in limitations 1.5-1.7, 16.5-16.7, and 19.5-19.7 of the '809 Patent. Ex.2178 (*Wiz Attack Path Analysis*), 2. I have reproduced an exemplary image showing Wiz’s contextual analysis from the blog post below:

Identify critical risks before they become threats with automated attack path analysis

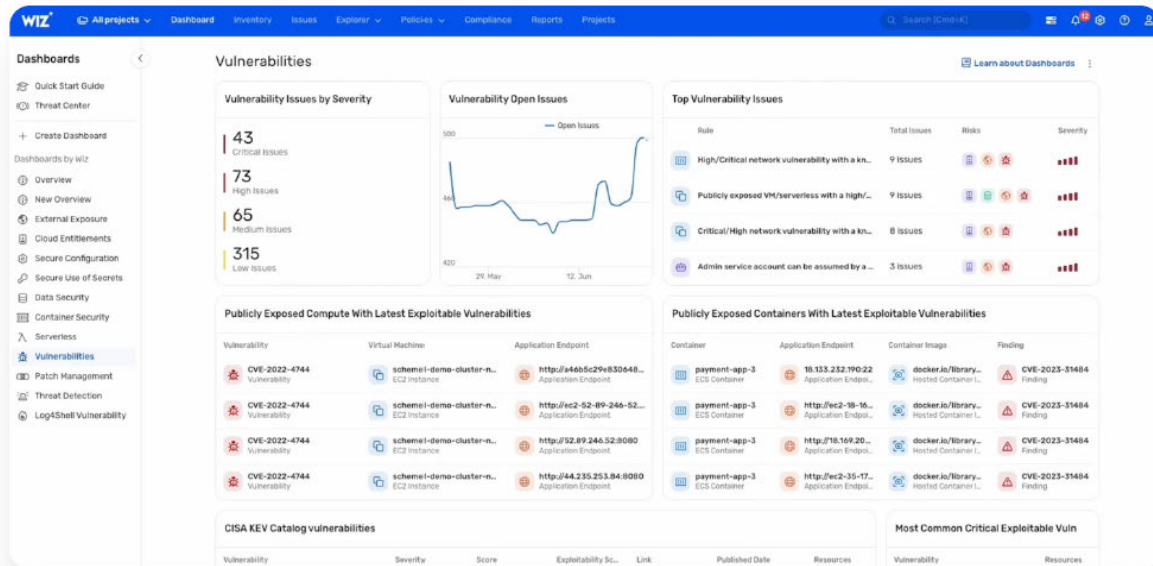


Wiz performs a complete attack path analysis, combining external exposures and lateral movement paths with access to high value assets. This analysis illustrates how threat actors may gain access to high-value assets through these paths.

Ex.2178 (*Wiz Attack Path Analysis*), 2.

130. In another blog post discussing Wiz’s vulnerability scanning, they include screenshots of their “vulnerabilities” dashboard that reports vulnerabilities as alerts prioritized based on risk, like Orca’s.

Stage 6: Vulnerability analysis



Example vulnerability dashboard that prioritizes issues by contextual severity

After scanning, the tool will generate a comprehensive list of identified vulnerabilities, order them based on severity, filter away false positives, and provide options for remediation.

Ex.2165 (*Vulnerability Scanning_ How It Works, Why It Matters, What It Finds*),

8.

131. In another blog post, Wiz explained that it provides “[f]ull visibility into what cloud services are in use and where” and “gives customers deep visibility into what cloud resources, applications, operating systems, and packages exist in their environment,” relevant to limitations 1.5, 16.5, and 19.5. Ex.2160 (Wiz, *Uncover What Is Really Deployed In Your Environment With The Enhanced Wiz*

Inventory, <https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory>), 2.

132. I note that, in August 2022, Wiz's press releases said that providing "an agentless, API-centered approach to seamlessly scan workloads and give organizations full visibility of their cloud environment" was a "new approach" when Wiz introduced its product in 2020. Ex.2116 (*\$100M ARR in 18 Months*, <https://www.wiz.io/blog/100m-arr-in-18-months-wiz-becomes-the-fastest-growing-software-company-ever>), 2. While I agree that agentless API-centered approaches were relatively new in 2020, it was Orca that introduced it and Wiz copied it from our SideScanning™.

VIII. Orca's SideScanning™ Inventions Were Widely Praised and Received Many Accolades

133. Orca's SideScanning™ inventions were widely praised and received many accolades.

134. For example, Orca's Cloud Security platform and my patent practicing SideScanning™ inventions were described as "unique" and a "big leap in cloud security" in the Complete Guide to the Future of Cloud Security. Ex.2076 (*Guide to the Future of Cloud Security*), 31. That guide also stated that Orca's "innovation introduced workload visibility without needing security teams to install an agent on endpoints or installing software on workloads for assessments." Ex.2076 (*Guide to the Future of Cloud Security*), 31.

135. TAG Cyber also published a report that provides that Orca's Cloud Security Platform and "patent-pending technique called SideScanning™" was a "next-gen platform" that employs "a read-only view of cloud workloads, 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." Ex.2118 (*TAG Cyber Report*), 5. This report also noted that Orca's SideScanning™ "produces a full snapshot of the environment ... that is used for correlation, contextualization, and analysis." Ex.2118 (*TAG Cyber Report*), 5. And the report explains that "Orca SideScanning bypasses the typical problems of better-known scanning methods like agent-based scanning and authenticated and unauthenticated scanning." Ex.2118 (*TAG Cyber Report*), 6. The report also specifically praised SideScanning™ because it "collects metadata from the cloud providers' APIs," and "enriches and contextualizes [] data with third-party threat intelligence, vulnerability, and exploit information and then uses advanced algorithms to assess the risk posture of every asset in the environment." Ex.2118 (*TAG Cyber Report*), 6. The report explains that "SideScanning ... quickly gathers all relevant data about deployed assets, including . . . vulnerabilities in software" and "risks of lateral movement." Ex.2118 (*TAG Cyber Report*), 6. The report called Orca's SideScanning™ a "unique[]" "patented technology" that "no other commercially available product can claim." Ex.2118 (*TAG Cyber Report*), 7.

136. The TAG Cyber report also presents praise from Orca customers. *See generally* Ex.2118 (*TAG Cyber Report*). For example, Aaron Brown from Sisense is quoted as saying Orca's Cloud Security Platform as "unique in that it locates vulnerabilities with precision and delivers tangible, actionable results." Ex.2118 (*TAG Cyber Report*), 4. As another example, Morey Haber from BeyondTrust is quoted as saying he had "never seen anything like the Orca Security platform before" and that Orca's platform was "a gem and must-have solution for businesses operating in the cloud." Ex.2118 (*TAG Cyber Report*), 5. As a third example, Drew Daniels from Druva, Inc. explained that he "tried numerous agent-based tools and they all failed miserably," but "Orca provide[d] 100% coverage without burdening our DevOps team" and "just works." Ex.2118 (*TAG Cyber Report*), 3.

137. Orca also received numerous industry awards since introducing its SideScanning™ inventions to the market.

138. For example, in 2020, Orca won a spot on CRN's list of "20 Coolest Tech Startups Of 2020," which identified "20 of the hottest technology startups in 2020 ... that solution providers should know about." Ex.2119 (*The 20 Coolest Tech Startups of 2020*), 1-2, 9-10. CRN highlighted that Orca's SideScanning™ "automatically assesses the security state of every discovered asset ... ultimately delivering complete visibility into issues such as vulnerabilities." Ex.2119 (*The 20 Coolest Tech Startups of 2020*), 6-7.

139. The same year, Orca was named to Forbes' "Top 20 Cybersecurity Startups to Watch in 2021," which selects companies "[b]ased on a methodology that equally weighs a startup's ability to attract new customers, current and projected revenue growth, ability to adapt their solutions to growing industries and position in their chosen markets." Ex.2120 (*The Top 20 Cybersecurity Startups to Watch in 2021 Based on Crunchbase*), 2-3. Forbes found Orca "noteworthy for its innovative approach to providing instant-on, workload-deep security for AWS, Azure and GCP without the gaps in agents' coverage and operational costs." Ex.2120 (*The Top 20 Cybersecurity Startups to Watch in 2021 Based on Crunchbase*), 7. Forbes explained that "Orca Security's patent-pending SideScanning™ technology . . . detect[s] vulnerabilities" and "lateral movement risk." Ex.2120 (*The Top 20 Cybersecurity Startups to Watch in 2021 Based on Crunchbase*), 7.

140. Also, in 2020, Orca won Security Innovation Network's SINET16 award. Ex.2143 (*SINET16 Previous Winners*), 3. Each year, Security Innovation Network "selects the 16 most innovative and compelling" cybersecurity companies and invites them to a conference "to present their products and solutions." Ex.2144 (*SINET16 Innovator Award*), 1.

141. As another example, in the same year, Orca was a named a winner of Security Current's CISO Choice Awards and was recognized as a "Visionary Vendor." Ex.2145 (*Security Current's CISO Choice Awards Winners 2020*), 2.

142. In 2021, Orca was named a Gartner Cool Vendor in Cloud Security Posture Management (CSPM). Exhibit 2121 is a true and correct copy of Orca's press release announcing the award. Gartner explained that SideScanning™ "surfaces the most important risks such as vulnerabilities" and "lateral movement risk." Ex.2121 (*Orca Security Named A 2021 Gartner Cool Vendor in Cloud Security Posture Management (CSPM)*), 1.

143. In 2022, Orca received a 2022 Regional and Global AWS Partner Award for global Security Partner of the Year, which "recognize[s] leaders around the globe playing a key role helping customers drive innovation and building solutions on Amazon Web Services (AWS)." Ex.2122 (*Orca Security Awarded 2022 Regional and Global AWS Partner Award*), 1. Attached as Exhibit 2122 is a true and correct copy of Orca's press release announcing its receipt of the 2022 Regional and Global AWS Partner Award. As Orca explained in that press release, the award "recognizes an AWS Partner who has proven customer success in securing every stage of cloud adoption, from initial migration through ongoing day-to-day management," and Orca was selected by "[a] panel of AWS experts." Ex.2122 (*Orca Security Awarded 2022 Regional and Global AWS Partner Award*), 2.

144. In the same year, Orca won SC Media's Best Cloud Security Posture Management (CSPM) solution. Ex.2124 (*SC Media Best Cloud Security Posture Management Solution Orca Security Platform*), 1. Attached as Exhibit 2124 is a

true and correct copy of Orca's press release describing its receipt of the award. Ex.2124 (*Orca Security Wins SC Award for Best Cloud Security Posture Management (CSPM) Solution*), 1-2. As the press release explains, "SC Media reported that the 2022 SC Awards were the most competitive to date." Ex.2124 (*Orca Security Wins SC Award for Best Cloud Security Posture Management (CSPM) Solution*), 1. Orca was "also chosen as a finalist in the Best Cloud Workload Protection Platform (CWPP) category." Ex.2124 (*Orca Security Wins SC Award for Best Cloud Security Posture Management (CSPM) Solution*), 1. SC Media explained that "SideScanning™ is at the heart of the Orca platform" which "detects risks at every layer of the tech stack, including vulnerabilities, . . . and lateral movement risk." Ex.2124 (*Orca Security Wins SC Award for Best Cloud Security Posture Management (CSPM) Solution*), 2.

145. In 2023, Orca won SC Media's Best Cloud Workload Protection Solution award. Ex.2123 (*SC Award Winners 2023 Orca Security – Best Cloud Workload Protection Solution*), 1-2. Paidy, a Japanese payment service company, told SC Media that Orca saved it "\$500,000 a year," and praised Orca's "agentless approach" as "both a major innovation and a game changer." Ex.2123 (*SC Award Winners 2023 Orca Security – Best Cloud Workload Protection Solution*), 1-2. Attached as Exhibit 2123 is a true and correct copy of Orca's press release announcing its receipt of the 2023 SC Award for Best Cloud Workload Protection

Platform (CWPP). As Orca explained, “[t]he SC Awards are cybersecurity’s most prestigious awards program honoring outstanding innovations, organizations and leaders that are advancing the practice of information security.” Ex.2125 (*Orca Security Wins 2023 SC Award for Best Cloud Workload Protection Platform (CWPP)*), 1. We were “also named a finalist in the Cloud Security Posture Management (CSPM) category.” Ex.2125 (*Orca Security Wins 2023 SC Award for Best Cloud Workload Protection Platform (CWPP)*), 2.

146. Also in 2023, Orca was named to Forbes’ 2023 Cloud 100 list and Redpoint InfraRed 100 List. Ex.2127 (*Forbes Cloud 100 Orca Security*), 2 (“#95 Cloud 100 (2023)”). Attached as Exhibit 2128 is a true and correct copy of Orca’s press release announcing its placement. Forbes’ Cloud 100 list “serves as the definitive ranking of the top 100 private cloud companies in the world.” Ex.2128 (*Orca Security Named 2023 Forbes Cloud 100*), 1. To select winners, “a judging panel of public cloud company CEOs” evaluated four factors: “market leadership,” “estimated valuation,” “operating metrics,” and “people & culture.” Ex.2128 (*Orca Security Named 2023 Forbes Cloud 100*), 1. And the Redpoint InfraRed 100 List is “a comprehensive list of the next 100 promising private companies in Cloud Infrastructure.” Ex.2129 (*Orca Security Named to Inaugural Redpoint InfraRed*), 1. Attached as Exhibit 2129 is a true and correct copy of Orca’s press release announcing the award.

147. In 2024, Orca was again awarded a place on the Redpoint InfraRed 100 List. Ex.2130 (*Orca Security Named to Redpoint 2024 InfraRed 100 for Second Consecutive Year*), 1. Attached as Exhibit 2130 is a true and correct copy of Orca's press release announcing the award.

148. In the same year, Orca was named to Notable Capital's Rising in Cyber 2024, "an inaugural list" "recogniz[ing] the most innovative startups in cybersecurity." Ex.2132 (*Orca Security Named to Notable Capital's Rising in 2024*), 1; Ex.2131 (*Rising in Cyber*), 2 (listing Orca). Exhibit 2132 is a true and correct copy of Orca's press release announcing the honor. As our press release explains, "Notable Capital partnered with over 100 CISOs, VPs of Security from companies such as Amazon, Atlassian, Coupang, and Netflix, and prominent venture capital firms to nominate and vote on approximately 200 companies to select the 30 honorees. Winners were chosen based on their proven ability to solve critical problems for security teams." Ex.2132 (*Orca Security Named to Notable Capital's Rising in 2024*), 1. The honorees were "recognized [on June 4, 2024] at the New York Stock Exchange." Ex.2132 (*Orca Security Named to Notable Capital's Rising in 2024*), 1.

149. I believe Orca received the above awards because of the unique inventions claimed in the '809 Patent and used in SideScanning™.

150. It is my opinion that Orca would not have received the above awards without the inventions claimed in the '809 Patent and used in SideScanning™.

IX. The Patents And Publications Relied On By Wiz Are Vastly Different Than Orca's SideScanning™ And '809 Patent Inventions

151. I understand that Wiz contends that claims 1-23 of the '809 Patent would have been obvious before January 2019, when the '718 Provisional Application was filed, in view of certain patents and publications, including U.S. Patent No. 11,216,563 ("Veselov") (Ex.1007), U.S. Patent No. 9,692,778 ("Mohanty") (Ex.1075), U.S. Patent No. 9,749,349 ("Czarny") (Ex.1084), and U.S. Publication No. US 2013/0024940 ("Hutchins") (Ex.1070). I disagree. In my view, none of the claims of the '809 Patent would have been obvious over the patents and publications that Wiz relies on for at least the reasons discussed below. It is also my opinion that a POSA would not have combined the references Wiz relies on because they are directed to entirely different techniques for security assessments that are not compatible with one another and would not have led a POSA to the inventions of the '926 Patent.

A. Veselov (Ex.1007)

152. I have reviewed Veselov, and in my view, Veselov is fundamentally different than the inventions of the '809 Patent.

153. For example, Veselov is different than my inventions because it focuses on systems for security assessments that use snapshots to instantiate functional, working “duplicate” resources, and then scans those resources. *See, e.g.,*

- Veselov, 3:20-23 (“The present disclosure describes a scanning system and associated methods for performing security assessments on virtualized reproductions of the computing resource(s) that is/are the target of the security assessment.”)
- Veselov, Abstract (“snapshot of the target computing resource, containing the data necessary to reproduce the portion to be assessed, is captured and used **to implement the duplicate computing resource in newly allocated resources**” ... “**To reproduce** a target virtual machine, the snapshot may include a configuration used to **instantiate the target virtual machine**; the scanning service may implement a duplicate virtual machine that is instantiated with the same configuration.”)
- Veselov, Fig. 4 (“install assessment agent in assessment VM”)
- Veselov, 3:27-29 (“The snapshot may include all of the data needed to **recreate** the state of the computing resource within a duplicate, virtual computing resource.”)
- Veselov, 3:54-61 (“In one embodiment, the scanning system **may set up and launch an active virtual machine** instance in the allocated

computing resources, the active virtual machine instance having the same configuration as the original virtual machine instance had at the time the snapshot was captured; the system may then perform the security assessment on the active virtual machine instance in a static or runtime environment.”)

- Veselov, 4:1-4 (“**In any case**, the snapshot is prepared so that the security assessment produces the results that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance”)
- Veselov, 12:21-27 (“Referring to FIG. 3A, in some embodiments it may be suitable or advantageous to perform the security assessment on a different **but similar** virtual machine than the customer's virtual machine because the assessment can be performed without impacting the customer's virtual machine”)
- Veselov, 17:9-12 (“Referring to FIG. 5A, the ‘duplicate’ of the virtual machine 512 may be created in a test environment 505 outside of the virtual computing environment 504A for the reasons stated above.”)

154. These types of resource cloning techniques are not the same as my inventions and would not work in modern cloud computing systems, especially those using containerized resources, which rely heavily on interactions with cloud services

that cannot be run in a reproduced environment without huge risk of negative impact to the system. In contrast, as I discussed above, SideScanning™, and the '809 Patent inventions, analyze a snapshot—a copy of data of the virtual disk at a point in time ('809 Patent, 4:60-61)—which Orca has consistently distinguished from “run[ning] a clone” of a workload as in Veselov. For example, the SideScanning Technical Brief explains:

Orca doesn't run a clone of your workload. Rather, the collector rebuilds the correct configuration and mounts the volumes in their native file systems in Orca's collection machine. This is done to ensure that Orca—and not any other entity—controls the scanning process. Also, this assists it in being more deliberate about the information it gathered from the machine.

AWS and all other cloud providers allow Orca to create a snapshot of the disk state while the machine is running. The process can snapshot multiple volumes at the same point in time, resulting in deep and consistent visibility.

Ex.2067 (SideScanning Technical Brief (2020)), 10 (highlighted).

155. I note that all of Veselov's claims are directed to creating a duplicate virtual machine instance and performing a security assessment on that running virtual machine. *See, e.g.* Ex.1007 (Veselov), cl. 1 (“cause a second virtual machine instance to be run, using the first volume image, in the virtual network of the user ... perform the security assessment on the second virtual machine instance”), cl. 6 (“use the first data to launch a second computing resource ... analyzing a connection of the second computing resource to a restricted resource associated with the user account”), cl. 16 (“configuring, based at least in part on the first data file, a second computing resource comprising a representation of the first computing resource in

the first state; causing the second computing resource to operate in the virtual computing environment”).

156. Additionally, the '809 Patent inventions require querying a cloud management console of the cloud computing environment for both a location of a snapshot *and* a location of a virtual disk. '809 Patent, cls. 15, 22. Persons in the industry understand that the determination of a snapshot location is different than the determination of a virtual disk location. I note that Veselov does not query a cloud management console of a cloud computing environment to determine a location of virtual disks associated with virtual machines.

157. I note that the use of cloud computing APIs is a critical element of the '809 Patent's claimed inventions and led others to recognize my inventions as “genuinely genius.” Ex.2076 (*Guide to the Future of Cloud Security*), 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.”). Veselov only uses the word “cloud” once, and only in describing problems associated with targets of security assessments. Ex.1007 (Veselov), 2:63-67.

158. Veselov also describes in its Figures 5A and 5B that “rather than recreating and instantiating a duplicate VM, the scanning service 510 is configured to analyze the volume image as a data file.” *See* Ex.1007 (Veselov), 16:67-17:3, Figs. 5A-5B. These discussions are not relevant to my claimed inventions because

they are discussing virtual computing environments that are implemented as an on-premises virtual computing environment. There is no “computing resource service provider” or any APIs that are used. *Compare* Ex.1007 (Veselov), Figs. 5A-5B with Figs. 3A-3B.

159. Veselov also does not disclose reporting any detected information as alerts, let alone ones that are prioritized according to a determination of matching installed applications that are used by a protected virtual cloud asset. This makes sense, as Veselov is describing individualized assessments of virtual machines, unlike my inventions.

B. Mohanty (Ex.1075)

160. I have reviewed Mohanty, and in my view, Mohanty is fundamentally different than the inventions of the '809 Patent.

161. For example, Mohanty does not discuss locating or accessing snapshots using APIs or services of a cloud computing environment, or analyzing any such snapshots. Instead, Mohanty discusses detecting vulnerabilities by analyzing instantiated machines using agent-based scanning technologies like “Qualys” and “Rapid7.” Ex.1075 (Mohanty), 6:54-58, Fig. 2. Mohanty also suggests that technology for assessing virtual machines in the past, e.g., using snapshots, should not be used because the corresponding data may become “obsolete within hours or minutes.” Ex.1075 (Mohanty), 1:7-23. Mohanty also discusses using “static” and

“dynamic” tags that are set by a “virtualization environment,” and does not teach how such tags would be applied to or available in a snapshot based analysis. *See* Ex.1075 (Mohanty), 3:60-4:23.

C. Czarny (Ex.1084)

162. I have reviewed Czarny and, in my view, Czarny is fundamentally different than the inventions of '809 Patent.

163. For example, Czarny does not teach or discuss any snapshot based assessment of virtual cloud assets like the '809 Patent claims. Instead, Czarny describes binary data scans of target electronic devices to “determine[] a correspondence between [] product binary data and [] product vulnerability data.” Ex.1084 (Czarny), 1:39-56.

164. As another example, Czarny’s assessments involve a determination of whether a target electronic device should be granted access to a secure environment based on whether a determined vulnerability level of the target electronic device exceeds a threshold. Ex.1084 (Czarny), 7:46-67. Accordingly, Czarny’s assessments are of any computing assets that are *outside* of a computing environment, not of a virtual cloud asset that is instantiated in a cloud computing environment as claimed, nor is there any determination of a risk of a protected virtual cloud asset based on its network location in such an environment like in the claims of the '809 patent. As I discuss above, Orca has been praised as “a leader in the field

of cloud security” based at least in part on how it has “excel[led] in contextual risk prioritization, allowing [users] to optimize [their] resources and ensure effective protection with the least amount of effort.” Ex.2117 (Panorama IT, Unprecedented Holistic View), 1.

D. Hutchins (Ex.1070)

165. I have reviewed Hutchins, and in my view, Hutchins is fundamentally different than the inventions of the '809 Patent.

166. For example, Hutchins does not discuss locating or accessing snapshots using APIs or services of a cloud computing environment, or prioritizing according to a determined risk or reporting the claimed determined plurality of potential cyber vulnerabilities as alerts. Instead, where Hutchins talks about snapshots, it is in the context of using snapshots to create duplicate VMs for analysis. Ex.1070 (Hutchins) ¶¶17, 53. Hutchins does not appear to include any discussion of cloud computing environments.

167. Furthermore, Hutchins discuss creating a duplicate VM that runs the same state of the scanned VM, trying to use the resources of the second VM to detect malicious code. It relies on cloning the main memory and resuming the clone including the memory, within the operation system of the original VM. This is not possible in cloud environment, not feasible in modern applications, and materially

different from the '926 patent that does not require the ability to launch the scanned asset at all, specifically not in the state where it was scanned.

X. Conclusion

All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true. Further, I am aware that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001. I declare under penalty of perjury that the foregoing is true and correct.

Executed on May-7-2025 (date), in Sydney, Australia (city, state).



Avi Shua