

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ORCA SECURITY LTD.,)	
)	
Plaintiff,)	
)	
v.)	C.A. No. _____
)	
WIZ, INC.,)	DEMAND FOR JURY TRIAL
)	
Defendant.)	

COMPLAINT FOR PATENT INFRINGEMENT

INTRODUCTION AND SUMMARY OF THE ACTION

1. Plaintiff Orca Security Ltd. (“Orca”) brings this action against Wiz, Inc. (“Wiz”) to put an end to Wiz’s flagrant, ongoing, and unauthorized use of Orca’s patented technologies.

2. Wiz has built its business on a simple business plan: copy Orca. This copying is replete throughout Wiz’s business and has manifest in myriad ways. In its marketing, Wiz copies Orca’s imagery, its message, and even the coffee it uses at trade shows. In prosecuting patents, Wiz recruited away Orca’s former patent attorney to copy Orca’s intellectual property and even the figures from Orca’s patents. And, most importantly for this action, in its products and services, Wiz has embedded a number of revolutionary inventions developed and patented by Orca, passed those inventions off falsely as Wiz innovations, and forced Orca to compete against its own technological breakthroughs in the marketplace. Wiz’s conduct in this regard is illegal, unjust, and in violation of the United States patent laws. Orca thus brings this complaint to redress Wiz’s willful and deliberate infringement of Orca’s patents.

* * *

3. Modern cloud computing launched in 2006, and quickly evolved from an emerging fad to the predominant technology employed across the globe. By 2018, nearly half of all companies claimed that 31% to 60% of their IT systems were cloud-based.¹

4. With this widespread and rapid adoption came inevitable security threats that, if left unchecked, could threaten the industry. What made the cloud so attractive—the ability to quickly spin-up or tear-down assets on demand and expand at an unprecedented pace—also made cloud computing environments exceptionally challenging to protect.

5. Before Orca, stale security approaches and conventional wisdom from legacy technologies were employed. Those entrenched in the field adapted traditional security tools designed for on-premise physical computers to the cloud environment, either checking all traffic going in or going out (network security) or attempting to install agents within each virtual asset within the system (endpoint security). Those tools—effective for discrete numbers of physical machines or services—were woefully inadequate to protect cloud-computing environments with enormous and dynamically changing numbers of virtual assets. This led to multiplying vulnerabilities and tremendous uncertainty in that large organizations had little insight into which services operate in their environment, who owns those services, who is obligated to maintain them, and what risks attend them.

6. Enter Avi Shua, an Israeli-born cybersecurity technologist with a life-long fascination with ways to protect—or break into—computer systems. Even as a teen, Mr. Shua led corporate IT security for his high school. Mr. Shua then spent 10 years in the Israel Defense Forces as part of Unit 8200, an elite division of the Israel Intelligence Corps responsible for collecting signal intelligence and code decryption, counterintelligence, cyberwarfare, military intelligence,

¹ <https://www.comptia.org/content/research/2018-trends-in-cloud-computing>

and surveillance. Following his military service, Mr. Shua joined Check Point Software, an early pioneer in the computer security industry. Mr. Shua quickly rose through the ranks during his decade at Check Point, ultimately serving as its Chief Technologist for four years.

7. After leaving Check Point, Mr. Shua turned his sights toward addressing the many shortcomings he had observed in cloud computing security. Among other things, Mr. Shua realized that the transient nature of workloads in a virtual environment made it effectively impossible for traditional endpoint and network security to continuously map onto those workloads. The result was a whack-a-mole approach that looked to secure workloads by adjusting endpoint security dynamically as vulnerabilities arose. This approach resulted in long periods with no security visibility, gaping holes in protection, and prohibitive costs to implement.

8. Dissatisfied, Mr. Shua looked to develop a new platform that could provide frictionless and comprehensive security coverage to a constantly evolving cloud environment. He realized that there was a better way—a more effective choke point—for analyzing cloud security within a virtual environment: the virtualization itself held the answer. In general terms, Mr. Shua conceived of a revolutionary approach that analyzed virtual cloud assets using read-only access with no impact on performance, and without deploying agents or network scanners. The result was vastly improved visibility into a cloud environment, deeper and better results, and improved speed. Mr. Shua's innovations also enabled the integration of data into unified data models, to view cloud security threats in a context that was not possible before, and so to prioritize risks that endanger the organization's most critical assets.

9. Mr. Shua and his co-founders founded Orca in 2019 to create a cloud security tool that brought Mr. Shua's inventions to market. The company took off like a rocket ship: the year after it was founded, Orca Security achieved more than 1,000% year-over-year growth. As noted

by customers, this success was due to the genius of Orca’s Platform. As one customer noted, “Orca Security is unique in that it locates vulnerabilities with precision and delivers tangible, actionable results—without having to sift through all of the noise.”² And another customer echoed the sentiment, stating: “Orca is unique in that it doesn’t require the installation of cumbersome agents. This reduces integration costs, and eliminates the question we had always asked ourselves, ‘are agents installed on all resources?’”³

10. In the four years since its founding, Orca has raised substantial investment funds and grown from fewer than a dozen to more than 400 employees today. Orca has been recognized as one of the most innovative companies in cloud security and, in 2022, was the recipient of Amazon Web Services Global Security Partner of the Year Award.⁴ The U.S. Patent Office has awarded Orca several patents for Mr. Shua’s inventions, including U.S. Patent Nos. 11,663,031 (the “’031 patent”), and 11,663,032 (the “’032 patent”), among others.

11. Now, Orca is threatened because the Defendant, Wiz, Inc., has taken Orca’s revolutionary inventions and created a copycat cloud security platform, improperly trading off of Orca’s inventions, including those claimed in the ’031 and ’032 patents, without authorization.

WIZ AND ITS WIDESPREAD COPYING OF ORCA

12. Wiz was founded in January 2020 by Assaf Rappaport, Ami Luttwak, Yinon Costica, and Roy Reznikthat, a team that previously led the Cloud Security Group at Microsoft,

² <https://web.archive.org/web/20200930194127/https://orca.security/> (Aaron Brown, Senior Cloud Security Engineer, Sisense).

³ <https://web.archive.org/web/20200930194127/https://orca.security/> (Jonathan Jaffe, Head of Information Security, Legal Counsel, people.ai).

⁴ <https://finance.yahoo.com/news/orca-security-awarded-2022-regional-010000110.html>

one of the top providers of cloud computing environments in the world.⁵ According to those founders, it was their time at Microsoft that provided them the “insight” that current cloud security tools were too complicated, fragmented, and generate too many alerts.⁶ Wiz was thus founded to “build a platform that lets teams scan their environments across compute types and cloud services for vulnerabilities and configuration, network, and identity issues without agents”; *i.e.*, to do exactly what Orca had already been doing for over a year.⁷

13. This was not a coincidence or a simultaneous stroke of genius. On the contrary, Wiz was birthed from the very beginning as a counterfeit copy of *Orca*’s ideas—Mr. Shua had presented Orca’s Platform to Wiz’s founders at Microsoft in May 2019, and the so-called “insight” of which Wiz boasts was nothing more than the misappropriation of Mr. Shua’s ideas and Orca’s technology as presented to Wiz’s founders before they formed Wiz and sought to launch a copycat competitor to Orca. It was at this 2019 meeting that Mr. Shua explained how cloud security would forever be changed by his novel agentless cloud security platform as implemented in Orca’s cloud-native security platform. Within months, the Wiz founders left their lucrative careers at Microsoft to start Wiz, build a clone of Orca’s technology, and compete directly with Orca.

14. Because of the massive head start it received from Orca and Mr. Shua, it took Wiz just months from the time the company was founded before it had a fully functioning “cloud visibility solution for enterprises that provides a complete view of security risks across clouds,

⁵ <https://www.darkreading.com/cloud/former-microsoft-cloud-security-leads-unveil-new-startup>; <https://www.forbes.com/sites/davidjeans/2020/12/09/wiz-sequoia-index-cybersecurity-100-million-former-microsoft-executives/?sh=4414df63254c> (“At Microsoft, Rappaport says he became increasingly aware of a growing problem for large companies: managing cloud security threats was a fragmented process, with security teams becoming overwhelmed by alerts.”).

⁶ <https://www.darkreading.com/cloud/former-microsoft-cloud-security-leads-unveil-new-startup>

⁷ *Id.*

workloads and containers” that was “already used by Fortune 100 companies.”⁸ In August 2022, Wiz announced it had become the “fastest-growing software company ever” reaching “\$100M ARR [annual recurring revenue] in 18 months.”⁹ And just eight months later in February 2023, Wiz raised \$300 million and achieved a company valuation of \$10 billion.¹⁰

15. Wiz’s wholesale copying of Orca’s technology has been observed by third party industry analysts. For example, SOURCEFORGE’s comparison of Orca and Wiz lists identical “Cloud Security Features” for each platform:

⁸ <https://www.securityweek.com/cloud-security-firm-wiz-emerges-stealth-100m-funding/>

⁹ <https://www.wiz.io/blog/100m-arr-in-18-months-wiz-becomes-the-fastest-growing-software-company-ever>

¹⁰ <https://techcrunch.com/2023/02/27/cloud-security-startup-wiz-now-valued-at-10b-raises-300m/>

Product	Feature	Status
Orca Security	Antivirus	✓
	Application Security	✓
	Behavioral Analytics	✓
	Encryption	✓
	Endpoint Management	✓
	Incident Management	✓
	Intrusion Detection System	✓
	Threat Intelligence	✓
	Two-Factor Authentication	✗
	Vulnerability Management	✓
Wiz	Antivirus	✓
	Application Security	✓
	Behavioral Analytics	✓
	Encryption	✓
	Endpoint Management	✓
	Incident Management	✓
	Intrusion Detection System	✓
	Threat Intelligence	✓
	Two-Factor Authentication	✗
	Vulnerability Management	✓

<https://sourceforge.net/software/compare/Orca-Security-vs-Wiz/>.

16. SOURCEFORGE also notes that Wiz has the same “Cybersecurity Features” as

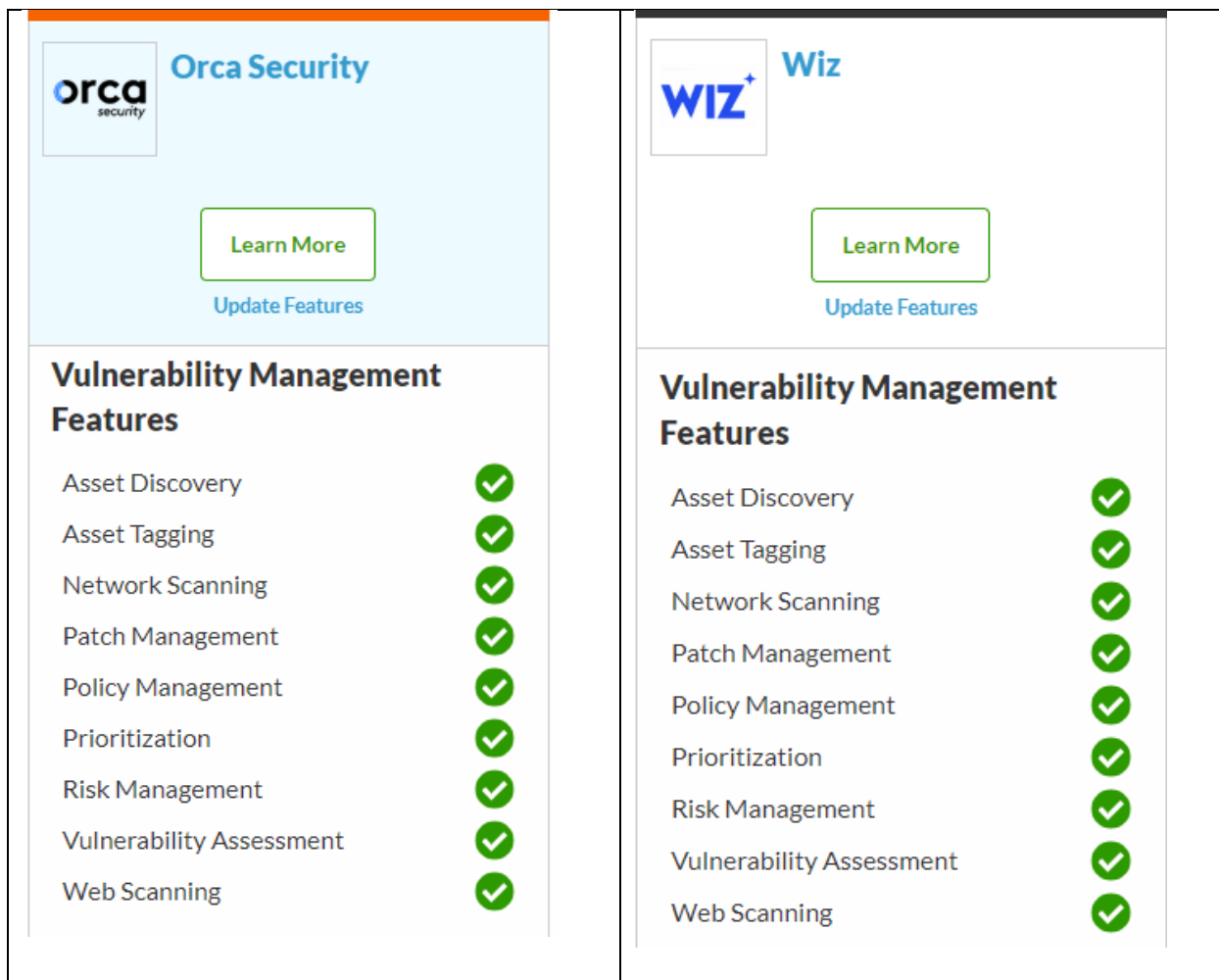
Orca:

The image displays two side-by-side panels comparing the cybersecurity features of Orca Security and Wiz. Each panel includes a header with the company logo and name, a 'Learn More' button, and an 'Update Features' link. Below this is a section titled 'Cybersecurity Features' with a list of features and their status, indicated by checkmarks in circles.

Feature	Orca Security Status	Wiz Status
AI / Machine Learning	Not Present (Grey Checkmark)	Present (Green Checkmark)
Behavioral Analytics	Not Present (Grey Checkmark)	Present (Green Checkmark)
Endpoint Management	Present (Green Checkmark)	Present (Green Checkmark)
Incident Management	Present (Green Checkmark)	Present (Green Checkmark)
IOC Verification	Present (Green Checkmark)	Present (Green Checkmark)
Tokenization	Not Present (Grey Checkmark)	Not Present (Grey Checkmark)
Vulnerability Scanning	Present (Green Checkmark)	Present (Green Checkmark)
Whitelisting / Blacklisting	Not Present (Grey Checkmark)	Not Present (Grey Checkmark)

Id.

17. SOURCEFORGE further shows that Wiz has the same “Vulnerability Management Features” as Orca:



Id.

18. Through all of its copying, Wiz has attributed none of its technology to Orca. In fact, Wiz has done the opposite. Wiz has claimed it was the “first cloud visibility solution”¹¹ and the “first full stack multi-cloud security platform.”¹² But even its “full stack” descriptor was copied from Orca. It was Orca that first announced its “Unprecedented Full Stack Cloud Visibility” platform in June 2019, months before Wiz was even founded.¹³ As another more recent example, Wiz announced in June 2022 that it had a “new vision for cloud security” with the “introduction

¹¹ <https://web.archive.org/web/20210128014251/https://wiz.io/>

¹² <https://web.archive.org/web/20210422201202/https://www.wiz.io/product>

¹³ <https://orca.security/resources/blog/orca-security-lands-6-5m-seed-round-to-deliver-it-security-teams-unprecedented-full-stack-cloud-visibility-securing-high-velocity-cloud-growth/>

of attack path analysis.”¹⁴ But Wiz’s “attack path analysis” was not new, and it wasn’t Wiz’s vision. It was Mr. Shua’s from just two months earlier. On March 31, 2022, Mr. Shua blogged about Orca’s new “Cloud Attack Path Analysis” dashboard, which Wiz copied.¹⁵

19. Wiz’s copying of Orca did not stop with the technology, but pervades Wiz’s business as a whole. For example, Orca realized early on that its cloud-native approach could be analogized to a medical MRI, providing a full model of the cloud environment without affecting it in any way. Early Orca marketing materials noted: “*An apt analogy is to think of a medical MRI. Instead of probing inside the body with needles and scalpels*, such imaging is an out-of-band method of obtaining a detailed picture of the organs and tissue within. *The person is never physically touched.*” Exhibit 3 (Orca SideScanning Technical Brief (2020)) at 15. Wiz copied this message: “Instead of using an intrusive agent, Wiz leverages cloud-native tools to perform scans without interrupting or impacting production workloads. *Just like an MRI performs a 3D scan of the body without affecting the body itself*, snapshot scanning achieves deep analysis of the workload without any impact or interruption to the live workload.” Exhibit 4 (Wiz “Agentless Scanning” (Jan. 19, 2022)).

20. As another example, Orca promoted its technology as assuming the “heavy lifting” of contextualizing detected security threats and prioritizing those that matter most. Exhibit 3 at 15 (“Context is critical; it’s the difference between effective security and dreaded analyst alert fatigue. *Orca assumes responsibility for the heavy lifting* associated with this additional context and assesses the real and effective risk. Orca’s mission is to provide the best contextualized security

¹⁴ <https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security>

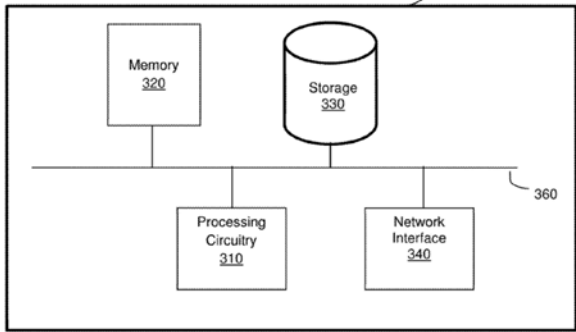
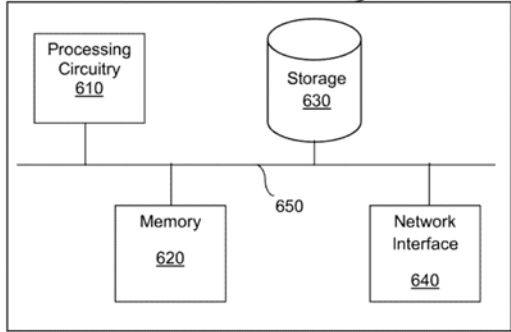
¹⁵ <https://orca.security/resources/blog/cloud-attack-path-analysis/>

intelligence possible.”). Wiz copied this too beginning with its very first website in 2020: “*We do the heavy lifting*, you get total visibility.”¹⁶

21. Wiz even copied the more mundane aspects of Orca’s marketing. For example, at a multi-day security conference in London, Orca decided that it would break away from typical technology booths and instead sponsor a coffee booth. Wiz attended the same conference. On the first day, Wiz sponsored a typical technology booth. The following day, Wiz showed up with its own coffee machine. Just like Orca.

22. Wiz also has knowingly copied Orca’s patents, its prosecution strategy, and even its prosecuting attorney. Orca’s first patent applications were filed and prosecuted by a lawyer at a small boutique firm with less than 10 attorneys, with whom Mr. Shua worked directly and confidentially. That engagement was terminated in 2021 when Orca learned that Wiz had engaged the same lawyer to file patents for Wiz on overlapping technology. Wiz’s patent applications now include figures and descriptions that are nearly identical to those found in Orca’s ’031 and ’032 patents:

¹⁶ <https://web.archive.org/web/20201209145922/http://www.wiz.io/>.

Orca	Wiz
 <p style="text-align: center;">FIG. 3</p> <p>FIG. 3 is an example block diagram of the security system 140 according to an embodiment. The security system 140 includes a processing circuitry 310 coupled to a memory 320, a storage 330, and a network interface 340. In an embodiment, the components of the security system 140 may be communicatively connected via a bus 360.</p> <p>The processing circuitry 310 may be realized as one or more hardware logic components and circuits. For example, and without limitation, illustrative types of hardware logic components that can be used include field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), application-specific standard products (ASSPs), system-on-a-chip systems (SOCs), general-purpose microprocessors, microcontrollers, digital signal processors (DSPs), and the like, or any other hardware logic components that can perform calculations or other manipulations of information.</p> <p>'032 patent at Fig 3, 8:7-23; '031 patent at Fig. 3, 9:15-31.</p>	 <p style="text-align: center;">FIG. 6</p> <p>FIG. 6 is an example hardware block diagram 600 depicting a cyber-security system 150, according to an embodiment. The cyber-security system 150 includes a processing circuitry 610 coupled to a memory 620, a storage 630, and a network interface 640. In an embodiment, the components of the cyber-security system 150 may be communicatively connected via a bus 650.</p> <p>The processing circuitry 610 may be realized as one or more hardware logic components and circuits. For example, and without limitation, illustrative types of hardware logic components that can be used include field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), Application-specific standard products (ASSPs), system-on-a-chip systems (SOCs), graphics processing units (GPUs), tensor processing units (TPUs), general-purpose microprocessors, microcontrollers, digital signal processors (DSPs), and the like, or any other hardware logic components that can perform calculations or other manipulations of information.</p> <p>Wiz's U.S. Patent No. 11,374,982 at Fig. 6, 20:61-21:12.</p>

23. Again, this was no coincidence. On information and belief, Wiz knew that the lawyer it hired had prosecuted Orca's patent applications and hired him to assist Wiz in its attempts to pass off Orca's technology and intellectual property.

24. In furtherance of its scheme to copy Orca, Wiz also recruited Orca's outside corporate counsel to work for Wiz. That lawyer attended Orca's Board of Director meetings and, as a result, was exposed to Orca's highly confidential technology and business plans. Orca replaced its outside corporate counsel in November 2020 after it learned that Wiz had engaged the very same lawyer as its own corporate counsel. On information and belief, Wiz knew that the

lawyer it hired was Orca's outside corporate counsel and Wiz hired him to assist Wiz in its attempts to copy Orca.

25. Beyond the foregoing examples, on information and belief, Wiz has hired former Orca employees and worked with third parties to acquire Orca's confidential information relating to current and future product plans, marketing, sales, prospective customers, and prospective employees, and has used that confidential information in furtherance of its efforts to copy and to compete unfairly with Orca.

26. This action seeks to put an end to, and obtain relief for, this pattern of copying and Wiz's willful infringement of the '031 patent and the '032 patent (collectively, the "Asserted Patents").

THE PARTIES

27. Plaintiff Orca Security Ltd. is an Israeli company with a principal place of business at 3 Tushia St., Tel Aviv, Israel 6721803.

28. On information and belief, Defendant Wiz, Inc. is a Delaware company with a principal place of business at One Manhattan West, 57th Floor, New York, New York.¹⁷

JURISDICTION AND VENUE

29. This action arises under the patent laws of the United States, 35 U.S.C. § 1 et seq. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

30. This Court has personal jurisdiction over Wiz because Wiz is subject to general and specific jurisdiction in the state of Delaware. Wiz is subject to personal jurisdiction at least because Wiz is a Delaware corporation and resides in this District. Wiz has made certain minimum

¹⁷ <https://www.wiz.io/contact> (Locations)

contacts with Delaware such that the maintenance of this suit does not offend traditional notions of fair play and substantial justice.

31. The exercise of personal jurisdiction comports with Wiz's right to due process because, as described above, Wiz has purposefully availed itself of the privilege of Delaware corporate laws such that it should reasonably anticipate being haled into court here.

32. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391 and 1400(b) at least because Wiz is incorporated in the State of Delaware and is subject to personal jurisdiction in this District.

COUNT I
(Infringement of the '031 Patent)

33. Orca incorporates all other allegations in this Complaint.

34. The '031 patent is entitled "Techniques for Securing Virtual Cloud Assets at Rest Against Cyber Threats" and was duly and legally issued on May 30, 2023. A true and correct copy of the '031 patent is attached hereto as Exhibit 1.

35. Orca is the owner of all rights, title, and interest in the '031 patent.

36. The '031 patent is valid and enforceable.

37. The inventions claimed in the '031 patent improved on prior art cloud security systems and methods by, *inter alia*, taking at least one snapshot or requesting taking of at least one snapshot of a virtual machine at rest, and analyzing the at least one snapshot to detect vulnerabilities. *See, e.g.*, '031 patent at cls. 1-16. This snapshot-based analysis for inactive assets was not well understood, routine, or conventional. It is an inventive concept that allows virtual assets in a cloud computing platform to be analyzed and scanned for embedded vulnerabilities, at a time when the machine is inactive, because, among other things, the analysis does not require any interaction and/or information from a running virtual asset like agent-based solutions. By

analyzing virtual cloud assets at rest, the '031 patent provides greater context for detected vulnerabilities and more comprehensive security for a cloud computing platform, including protecting against assets that may have become unsafe after they were turned off due to newly disclosed vulnerabilities or infrastructure changes.

(a) Direct Infringement of the '031 Patent

38. Wiz, without authorization, directly infringes one or more claims of the '031 patent, literally and/or under the doctrine of equivalents. Wiz infringes under 35 U.S.C. § 271 including, without limitation, 35 U.S.C. § 271(a), by making, using, selling, offering to sell, and/or importing within the United States without authority, Wiz's CSP and/or other similar products or services, which include (or are otherwise referred to) but are not limited to Wiz's Cloud Native Application Protection Platform ("CNAPP"), Cloud Security Posture Management ("CSPM"), Cloud Infrastructure Entitlement Management ("CIEM"), Data Security Posture Management ("DSPM"), Infrastructure-as-code ("IaC") scanning (<https://www.wiz.io/solutions/iac>), and Cloud Detection and Response ("CDR") platforms and/or features. *See* <https://www.wiz.io/> (listing CNAPP, CSPM, CIEM, DSPM, IaC scanning, and CDR as "Product[s]"); *see also* <https://www.wiz.io/product> (same). Wiz's infringement includes infringement of, for example, claim 9 of the '031 patent.

39. Claim 9 of the '031 patent recites:

1. A computer-implemented method for inspecting data, the method comprising:

establishing an interface between a client environment and security components;

using the interface to utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment;

using the computing platform APIs to query a location of at least one of the identified virtual disks;

receiving an identification of the location of the virtual disks of the virtual machine;

emulating the virtual disks for the virtual machine;

performing at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time;

analyzing the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive; and

reporting the detected vulnerabilities as alerts.

40. On information and belief, Wiz practices each and every limitation of claim 9 of the '031 patent by and through the use of Wiz's CSP and/or other similar products or services for Wiz's clients or customers.

41. The preamble of claim 9 recites “[a] computer-implemented method for inspecting data, the method comprising. . . .” To the extent the preamble is limiting, Wiz practices this step by, for example, using its computer-implemented CSP to inspect data in clients' cloud computing environments, including inactive assets. *See, e.g.*, <https://www.wiz.io/solutions/cnapp> (“Wiz leverages unique technology to scan PaaS resources, Virtual Machines, Containers, Serverless Functions, . . . to identify the risks in each layer”); <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz> (“Detect and prioritize CISA Known Exploited Vulnerabilities in the cloud with Wiz”).

42. Claim 9 further recites “establishing an interface between a client environment and security components” Wiz’s public presentations and technical documentation confirm that Wiz practices this step by, for example, using Wiz’s CSP to perform “[a]gentless scanning via API” provided by AWS, GCP, and Azure, among other cloud computing environments.



See Exhibit 5 (AWS re:Invent - Context is Everything: Join the CNAPP Revolution to Secure Your AWS Deployments) at 13; Exhibit 6 (Wiz Cloud Security Platform Datasheet) (supported cloud computing platforms include AWS, Azure, and Google Cloud Platform (GCP)); <https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics> (“Wiz connects to your cloud environment via your cloud service provider’s APIs in order to extract metadata and perform snapshot scans.”); <https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics> (same); <https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics> (same); <https://www.wiz.io/solutions/vulnerability-management> (“Using a one-time cloud native API deployment, continuously assess workloads without deploying agents”).

43. Claim 9 further recites “using the interface to utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment” Wiz practices this step by, for example, using Wiz’s CSP to provide “[f]ull visibility” of virtual cloud assets in a client environment using an API provided by AWS, GCP, and Azure, among other cloud computing environments.

Step 1: Full visibility in minutes across 60+ AWS services without agents

1 Agentless scan of cloud metadata and workloads

Frictionless visibility

- ✓ Agentless scanning via API
- ✓ Cloud and architecture agnostic
- ✓ Quick deployment, low maintenance

Serverless
Containers
VMs
PaaS

Compute

- Amazon EC2
- Amazon EKS
- AWS Fargate
- AWS Lambda
- Amazon ECS
- AWS Transient Gateway
- Amazon VPC
- Amazon Route 53
- Elastic Load Balancer
- Amazon ECR

Application and Data

- Amazon ElastiCache
- Amazon S3
- Amazon Neptune
- Amazon Redshift
- Amazon DynamoDB
- Amazon RDS
- Amazon SNS
- Amazon SQS
- Amazon SageMaker
- AWS Glue
- MQ
- Amazon CloudFront

Security and Identity

- Amazon Cognito
- IAM
- AWS KMS
- AWS Secrets Manager
- Amazon GuardDuty
- AWS CloudTrail
- AWS Systems Manager

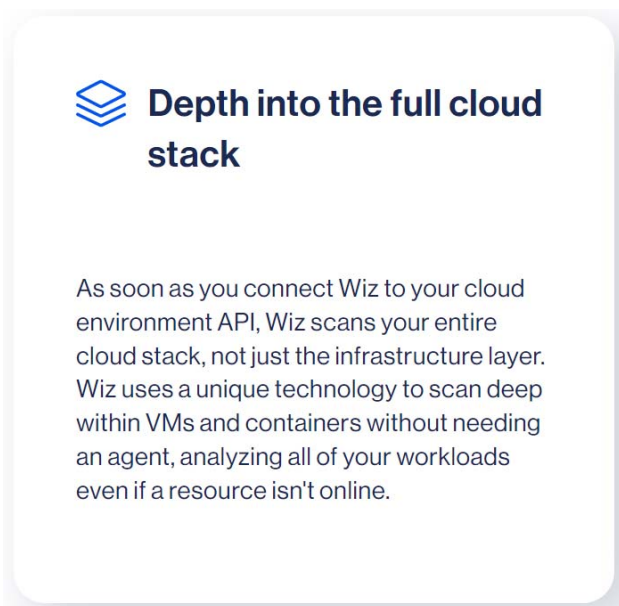
See Exhibit 5 at 13; Exhibit 6 (supported cloud computing platforms include AWS, Azure, and Google Cloud Platform (GCP)). Through the API, Wiz creates a graph of a client environment “with full context on the resource[s],” which includes identifying virtual disks of virtual machines. See <https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security>; Exhibit 6 at 3 (“Wiz uses the full context of your cloud and combines this information into a single graph in order to correlate related issues”), 4 (Wiz “takes a snapshot of each VM system volume and analyzes its operating system, application layer, and data layer statically with no performance impact.”).

44. Claim 9 further recites “using the computing platform APIs to query a location of at least one of the identified virtual disks” Wiz performs this step by, for example, using computing platform APIs to perform a query to locate virtual disks and other resources. *See* Exhibit 5 at 13 (“Agentless scanning via API”); <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz> (“You can query and locate all the VMs, containers, and serverless functions in your cloud environment that are vulnerable to a specific CVE in the catalog with a simple query shortcut.”); <https://www.wiz.io/solutions/cnapp> (“Scan buckets, data volumes, and databases and quickly classify the data to track wh[ere] data is located.”); <https://support.wiz.io/hc/en-us/articles/5643759466396-Security-Graph-Basics> (“[C]heck out our guide for optimizing your Security Graph queries.”).

45. Claim 9 further recites “receiving an identification of the location of the virtual disks of the virtual machine” Wiz practices this step by, for example, identifying virtual disks and other resources it locates when it performs a query. *See* <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz> (“You can query and locate all the VMs, containers, and serverless functions in your cloud environment that are vulnerable to a specific CVE in the catalog with a simple query shortcut.”). As another example, Wiz uses Wiz’s CSP to create a graph showing the locations of virtual cloud assets, including virtual machines and virtual disks, within a client environment. *See* Exhibit 6 at 3 (Wiz “uses the full context of your cloud and combines this information into a single graph in order to correlate related issues”); *see also* Exhibit 5 at 13 (“Full visibility in minutes . . . without agents”).

46. Claim 9 further recites “emulating the virtual disks for the virtual machine” On information and belief, Wiz practices this step by, for example, using Wiz’s CSP to scan “all

of [a customer's] workloads even if a resource isn't online" because an offline resource's virtual disks will need to be emulated before scanning.



<https://legacy.wiz.io/partners/google>. Wiz's website also promotes its platform as using agentless "snapshot" scanning. See <https://www.wiz.io/solutions/cnapp> ("Wiz deployment leverages a single cloud role to scan your entire cloud environment: PaaS, Virtual Machines, Containers, Serverless functions, Buckets, Data volumes and Databases."); <https://www.wiz.io/solutions/vulnerability-management>. As Wiz's blog posts explain, "volume snapshot approach" where snapshots are scanned "out of band, do not rely on the cloud environment's compute resources to run." <https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning>. Accordingly, on information and belief, Wiz uses its own separate compute resources to emulate virtual disks that it analyzes.

Agentless Host Configuration Analysis

Continuously monitor operating systems and application configurations according to CIS benchmarks (CIS Ubuntu, Red Hat, Windows, and more) without any agents or external scans.

The screenshot shows the Wiz.io interface for OS Configuration. The top navigation bar includes 'WIZ', 'All projects', 'Dashboard', 'Inventory', 'Issues', 'Explorer', 'Policies', 'Compliance', 'Reports', and 'Projects'. Below the navigation, the 'OS Configuration' section is visible, featuring a search bar and filters for 'Cloud Platform', 'Resource', 'Result', and '+ Filter'. The main content is a table with the following columns: Resource, Rule, Result, Category, and Subscription.

Resource	Rule	Result	Category	Subscription
oke-cxdhuo7... Virtual Machine	Ensure no duplicate group names exist	Passed	1 category	wiz-outpost-tf
oke-cxdhuo7... Virtual Machine	Ensure no duplicate user names exist	Passed	1 category	wiz-outpost-tf
oke-cxdhuo7... Virtual Machine	Ensure no duplicate GIDs exist	Passed	1 category	wiz-outpost-tf
oke-cxdhuo7... Virtual Machine	Ensure no duplicate UIDs exist	Passed	1 category	wiz-outpost-tf
oke-cxdhuo7... Virtual Machine	Ensure all groups in /etc/passwd exist in /etc/group	Passed	1 category	wiz-outpost-tf
oke-cxdhuo7... Virtual Machine	Ensure no users have .rhosts files	Passed	1 category	wiz-outpost-tf
oke-cxdhuo7... Virtual Machine	Ensure users' .netrc Files are not group or world accessible	Passed	1 category	wiz-outpost-tf

<https://www.wiz.io/solutions/vulnerability-management>.

47. Claim 9 further recites “performing at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time” Wiz performs this step by, for example, taking a snapshot of a virtual disk in order to “analyze[] [the] operating system, application layer, and data layer” of virtual machines in a client environment. *See* Exhibit 6 at 4, 3 (Wiz “[s]cans the workloads inside the container to determine . . . its vulnerabilities”); *see also* Exhibit 5 at 27. Wiz’s technical documentation explains that “Wiz connects to [a] cloud environment via [a] cloud service provider’s APIs in order to extract metadata and perform snapshot scans.” <https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics>; <https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics> (same); <https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics> (same). On information and belief, Wiz also requests taking a snapshot of

virtual disks on a virtual machine when it is offline. <https://legacy.wiz.io/partners/google> (“Wiz uses a unique technology to scan deep within VMs and containers without needing an agent, analyzing all of your workloads even if a resource isn’t online.”).

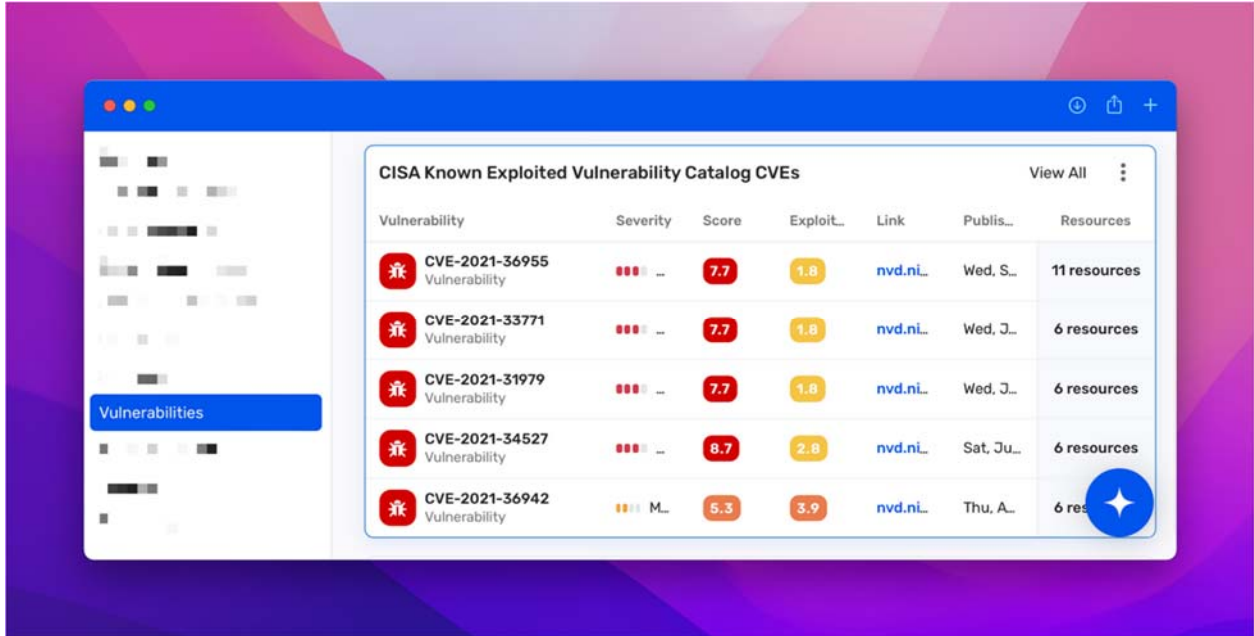
48. Claim 9 further recites “analyzing the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive” Wiz performs this step by, for example, analyzing the snapshot of a virtual disk to determine cyber vulnerabilities affecting the virtual disk. For example, Wiz analyzes the snapshot of a virtual disk to identify potential vulnerabilities.

70K+ Supported Vulnerabilities: Our industry-leading vulnerability catalog consists of more than 70,000 supported vulnerabilities, across 30+ operating systems, CISA KEV catalog and thousands of applications.

<https://www.wiz.io/solutions/vulnerability-management>.

49. As another example, Wiz “analyzes [the] operating system, application layer, and data layer” of virtual machines to provide full visibility into vulnerabilities across the cloud computing environment. *See* Exhibit 6 at 4 (Wiz “[s]cans the workloads inside the container to determine . . . its vulnerabilities”); <https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security> (“[D]efenders can now analyze activities and review timelines within the graph, with full context on the resource, roles, vulnerabilities, and potential impact.”). Furthermore, Wiz analyzes snapshots of machines that are not online and/or “before deployment to the runtime environment.” *See, e.g.*, <https://legacy.wiz.io/partners/google> (“Wiz uses a unique technology to scan deep within VMs and containers without needing an agent, analyzing all of your workloads even if a resource isn’t online.”); <https://www.wiz.io/solutions/vulnerability-management>; <https://www.wiz.io/solutions/iac> (“scan images continuously before deployment”).

50. Claim 9 further recites “reporting the detected vulnerabilities as alerts.” Wiz performs this step by, for example, reporting vulnerabilities in a client environment as alerts in Wiz’s CSP.



<https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz> (“CISA Known Exploited Vulnerability Catalog CVEs dashboard in Wiz”); *see also* Exhibit 6 at 3 (“Scan for vulnerable and unpatched operating systems, installed software, and code libraries in your workloads prioritized by risk.”). Wiz reports a “graph” to show “toxic combinations that create attack paths in [a] cloud.”

Visibility, Prioritization, and Agility – from Build Time to Runtime

Wiz is a revolutionary new approach to cloud security. The only agentless, graph-based CNAPP that provides 100% visibility, ruthless risk prioritization, and time-to-value across teams that build and secure your cloud.

Scan Everything

Connect in minutes, and scale without worries – Wiz leverages unique technology to scan PaaS resources, Virtual Machines, Containers, Serverless Functions, Public buckets, Data Volumes, and Databases to identify the risks in each layer and visualize your cloud stack with the security graph.

Fix What Matters Most

Run an effective cloud security program and ruthlessly prioritize the most critical risks with actionable context. The Wiz Security Graph immediately uncovers the toxic combinations that create attack paths in your cloud and eliminates the need for manual work of sifting through and analyzing siloed alerts.

Build Bridges Across Teams

Ship faster by removing operational silos and enabling development teams to proactively fix and prevent issues across their development lifecycle. Project-based workflows and remediation guidance help remove guesswork and fix misconfigurations or violate security policies fast.

See, e.g., <https://www.wiz.io/solutions/cnapp>; <https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security> (“[D]efenders can now analyze activities and review timelines within the graph, with full context on the resource, roles, vulnerabilities, and potential impact.”); Exhibit 6 at 3 (“Wiz uses the full context of your cloud and combines this information into a single graph in order to correlate related issues”); <https://www.wiz.io/solutions/vulnerability-management> (“Use the Threat Center to immediately identify workload exposure to the latest vulnerabilities sourced from Wiz Research along with numerous third-party threat intelligence feeds.”).

51. As described in the preceding paragraphs, Wiz infringes claim 9 of the ’031 patent, either literally or under the doctrine of equivalents.

52. The above examples of how Wiz directly infringes claim 9 of the ’031 patent are non-limiting and based on information currently available to Orca. In particular, additional or different aspects of Wiz’s products or services may be identified that meet the limitations of claim 9 of the ’031 patent, additional claims of the ’031 patent may be determined to be infringed, and additional Wiz products or services may be identified as infringing once additional nonpublic information is provided through the course of discovery.

(b) Induced Infringement of the ’031 Patent

53. On information and belief, in providing Wiz’s CSP to its customers, Wiz has induced, and continues to induce, direct infringement of one or more claims of the ’031 patent, including at least claim 9, literally and/or under the doctrine of equivalents pursuant to 35 U.S.C. § 271(b).

54. On information and belief, Wiz monitors Orca’s patent portfolio and was aware of the ’031 patent and its infringement thereof when the ’031 patent issued or soon thereafter at least

as a result of its efforts to copy Orca's technology and its patents. For example, Wiz by and through its patent prosecution counsel had knowledge of the '031 patent's parent application, U.S. Patent Application No. 16/750,556, and its provisional application, U.S. Provisional Application No. 62/797,718, because Wiz's patent prosecution counsel is the same lawyer that filed those applications on behalf of Orca. As described above in Paragraph 22, Wiz's patents also include nearly identical figures and descriptions as those found in the '031 patent. In any event, Wiz has had knowledge of the '031 patent and its infringement thereof since at least as early as the filing of this Complaint.

55. On information and belief, Wiz possesses a specific intent to induce infringement by, at a minimum, providing user guides, instructions, sales-related material, and/or other supporting documentation, and by way of advertising, solicitation, and provision of product instruction materials, that instruct its customers on the normal operation of Wiz's CSP in a manner that infringes one or more claims of the '031 patent, including at least claim 9 of the '031 patent, or Wiz believed there was a high probability that the acts of its customers would infringe one or more claims of the '031 patent, including at least claim 9, and took deliberate steps to avoid learning of that infringement.

(c) Contributory Infringement of the '031 Patent

56. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '031 patent and its infringement thereof when the '031 patent issued or soon thereafter at least as a result of its efforts to copy Orca's technology and its patents. For example, Wiz by and through its patent prosecution counsel had knowledge of the '031 patent's parent application, U.S. Patent Application No. 16/750,556, and its provisional application, U.S. Provisional Application No. 62/797,718, because Wiz's patent prosecution counsel is the same lawyer that filed those

applications on behalf of Orca. As described above in Paragraph 22, Wiz's patents also include nearly identical figures and descriptions as those found in the '031 patent. In any event, Wiz has had knowledge of the '031 patent and its infringement thereof since at least as early as the filing of this Complaint.

57. On information and belief, by providing Wiz's CSP to its customers, Wiz has in the past contributed, and continues to contribute, to the direct infringement of one or more claims of the '031 patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(c), including at least claim 9 of the '031 patent. Wiz has contributorily infringed and continues to contribute to the infringement of one or more claims of the '031 patent by offering to sell or selling Wiz's CSP, which is a patented component, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement and not a staple article or commodity of commerce suitable for substantial non-infringing use.

(d) Willful Infringement of the '031 Patent

58. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '031 patent and its infringement thereof when the '031 patent issued or soon thereafter at least as a result of its efforts to copy Orca's technology and its patents. For example, Wiz by and through its patent prosecution counsel had knowledge of the '031 patent's parent application, U.S. Patent Application No. 16/750,556, and its provisional application, U.S. Provisional Application No. 62/797,718, because Wiz's patent prosecution counsel is the same lawyer that filed those applications on behalf of Orca. As described above in Paragraph 22, Wiz's patents also include nearly identical figures and descriptions as those found in the '031 patent. In any event, Wiz has had knowledge of the '031 patent and its infringement thereof since at least as early as the filing of this Complaint.

59. Wiz's infringement has been and continues to be intentional and deliberate, entitling Orca to enhanced damages under 35 U.S.C. § 284 and a finding that this case is exceptional, entitling Orca to an award of reasonable attorneys' fees under 35 U.S.C. § 285.

60. On information and belief, Wiz has profited from and will continue to profit from its infringing activities. Orca has been and will continue to be damaged and irreparably harmed by Wiz's infringing activities. As a result, Orca is entitled to injunctive relief and damages adequate to compensate it for such infringement, in no event less than a reasonable royalty, in accordance with 35 U.S.C. §§ 271, 281, 283, and 284. The amount of monetary damages Wiz's acts of infringement have caused to Orca cannot be determined without an accounting.

61. The harm to Orca from Wiz's ongoing infringing activity is irreparable, continuing, and not fully compensable by money damages, and will continue unless Wiz's infringing activities are enjoined.

COUNT II
(Infringement of the '032 Patent)

62. Orca incorporates all other allegations in this Complaint.

63. The '032 patent is entitled "Techniques for Securing Virtual Machines by Application Use Analysis," and was duly and legally issued on May 30, 2023. A true and correct copy of the '032 patent is attached hereto as Exhibit 2.

64. Orca is the current owner of all rights, title, and interest in the '032 patent.

65. The '032 patent is valid and enforceable.

66. The inventions claimed in the '032 patent improve on prior art systems by, *inter alia*, accessing the snapshot of at least one virtual disk of a protected virtual cloud asset, analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications, and determining, based on the matching, an existence of

potential cyber vulnerabilities of the protected virtual cloud asset. *See, e.g.*, '032 patent at cls. 1-25. This novel analysis of snapshots for potential cyber vulnerabilities was not well understood, routine, or conventional. It is an inventive concept that allows, for example, practical implementations of vulnerability detection for virtual cloud assets in large data centers because it does not require the cumbersome installation of agents. This reduces the costs of licensing, deployment, integration, training, and support for a cloud security platform. Additionally, analyzing snapshots as provided in the claims of the '032 patent achieved unconventional performance, including (1) the ability to scan virtual cloud assets across an entire cloud environment in a matter of minutes compared to months-long installations of agent-based solutions, and (2) achieving comprehensive coverage and features that are not possible using agent-based approaches due to the tradeoff between performance and impact to the environment.

67. The claims of the '032 patent also recite inventive concepts for prioritizing potential cyber vulnerabilities based on use determinations and reporting prioritized alerts according to the use determinations. *See, e.g., id.* Prioritizing based on use determinations was not well understood, routine, or conventional, and improves on prior art techniques by putting potential cyber vulnerabilities in context. The novel limitations of the '032 patent invention, including analyzing snapshots and prioritizing potential cyber vulnerabilities based on use determinations, improve the implementation of a security system for cloud environments because the gathered information can be analyzed to produce actionable, context-based alerts and reports without relying on agents or network scanners.

(a) Direct Infringement of the '032 Patent

68. Wiz, without authorization, directly infringes one or more claims of the '032 patent, literally and/or under the doctrine of equivalents. Wiz infringes under 35 U.S.C. § 271 including,

without limitation, 35 U.S.C. § 271(a), by making, using, selling, offering to sell, and/or importing within the United States without authority, Wiz's CSP and other similar products or services, which includes (or is otherwise referred to) but is not limited to Wiz's CNAPP, CSPM, CIEM, DSPM, IaC scanning, and CDR platforms and/or features. *See* <https://www.wiz.io/>; *see also* <https://www.wiz.io/product>. Wiz's infringement includes infringement of, for example, claim 1 of the '032 patent,

69. Claim 1 of the '032 patent recites:

1. A method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising:
 - 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;
 - accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk;
 - analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;
 - determining, based on the matching, an existence of potential cyber vulnerabilities of the protected virtual cloud asset;
 - determining whether the matching installed applications are used by the protected virtual cloud asset;
 - prioritizing the potential cyber vulnerabilities based on the use determinations; and
 - reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.

70. On information and belief, Wiz practices each and every limitation of claim 1 of the '032 patent by and through the use of Wiz's CSP and/or other similar products or services for Wiz's clients or customers.

71. The preamble of claim 1 recites “[a] method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising” To the extent the preamble is limiting, Wiz practices this step by, for example, using Wiz's CSP to detect cyber vulnerabilities in cloud computing environments and secure virtual cloud assets within those environments against said vulnerabilities. *See, e.g.*, <https://www.wiz.io/solutions/cnapp> (advertising that Wiz “identif[ies] and remediate[s] risks and respond[s] to threats in [] cloud environments”); <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz> (“Detect and prioritize CISA Known Exploited Vulnerabilities in the cloud with Wiz”).

72. Claim 1 further recites “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” Wiz's public presentations and technical documentation confirm that Wiz practices this step by, for example, using Wiz's CSP to perform “[a]gentless scanning via API” provided by AWS, GCP, and Azure, among other cloud computing environments.

Step 1: Full visibility in minutes across 60+ AWS services without agents

1 Agentless scan of cloud metadata and workloads

Frictionless visibility

- ✓ Agentless scanning via API
- ✓ Cloud and architecture agnostic
- ✓ Quick deployment, low maintenance

Serverless
Containers
VMs
PaaS

WIZ

Compute

- Amazon EC2
- Amazon EKS
- AWS Fargate
- AWS Lambda function
- Amazon ECS
- AWS Transit Gateway
- Amazon VPC
- Amazon Route 53
- Elastic Load Balancer
- Amazon ECR

Application and Data

- Amazon ElastiCache
- Amazon S3
- Amazon Neptune
- Amazon Redshift
- Amazon DynamoDB
- Amazon RDS
- Amazon SNS
- Amazon SQS
- Amazon SageMaker
- AWS Glue
- MQ
- Amazon CloudFront

Security and Identity

- Amazon Cognito
- IAM
- AWS KMS
- AWS Secrets Manager
- Amazon GuardDuty
- AWS CloudTrail
- AWS Systems Manager

See Exhibit 5 at 13; Exhibit 6 (supported cloud computing platforms include AWS, Azure, and Google Cloud Platform (GCP)). Wiz’s technical documentation confirms that its agentless scanning includes “snapshot scanning” of instantiated virtual cloud assets, wherein Wiz “takes a snapshot of each VM system volume and analyzes its operating system, application layer, and data layer statically with no performance impact.” Exhibit 6 at 4, 2 (“Wiz scans all the resources and workloads in your cloud environment using a unique snapshot technology that covers more than an agent can.”); <https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics> (“Wiz connects to your cloud environment via your cloud service provider’s APIs in order to extract metadata and perform snapshot scans.”); <https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics> (same); <https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics> (same); <https://www.wiz.io/solutions/vulnerability-management> (“Using a one-time cloud native API deployment, continuously assess workloads without deploying agents”).

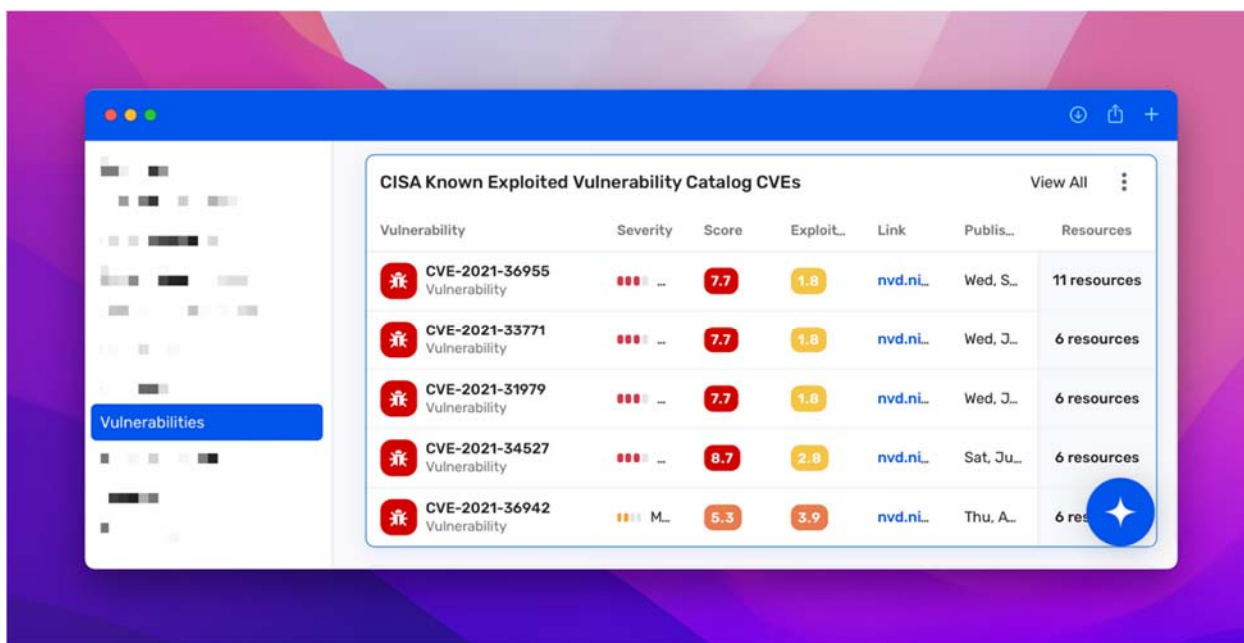
73. Claim 1 further recites “accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk” Wiz performs this step by, for example, accessing the snapshot of a virtual disk in order to “analyze[] [the] operating system, application layer, and data layer” of virtual cloud assets. *See* Exhibit 6 at 4, 3 (Wiz “[s]cans the workloads inside the container to determine . . . its vulnerabilities”). Wiz’s technical documentation explains that “Wiz connects to [a] cloud environment via [a] cloud service provider’s APIs in order to extract metadata and perform snapshot scans.” <https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics>; <https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics> (same); <https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics> (same).

74. Claim 1 further recites “analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications” Wiz practices this step by, for example, analyzing the snapshot of a virtual disk by matching installed applications to a known list of vulnerabilities in the “CISA Known Exploited Vulnerability (KEV) Catalog,” which is “a catalog of known exploited vulnerabilities that carry significant risk,” including “vulnerabilities in . . . proprietary applications.” *See* <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz>. Wiz employs “agentless scanning” to “identify [] toxic combinations” between applications installed on a virtual disk and known vulnerable applications in Wiz’s “vulnerability catalog consist[ing] of more than 70,000 supported vulnerabilities, across 30+ operating systems, CISA KEV catalog and thousands of applications.”

70K+ Supported Vulnerabilities: Our industry-leading vulnerability catalog consists of more than 70,000 supported vulnerabilities, across 30+ operating systems, CISA KEV catalog and thousands of applications.

<https://www.wiz.io/solutions/vulnerability-management>; *see also id.*

75. Claim 1 further recites “determining, based on the matching, an existence of potential cyber vulnerabilities of the protected virtual cloud asset” Wiz practices this step because, for example, it uses results of its agentless scanning to “list[] all the resources . . . that are currently vulnerable to one or more vulnerabilities in the catalog.” *See* <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz>.

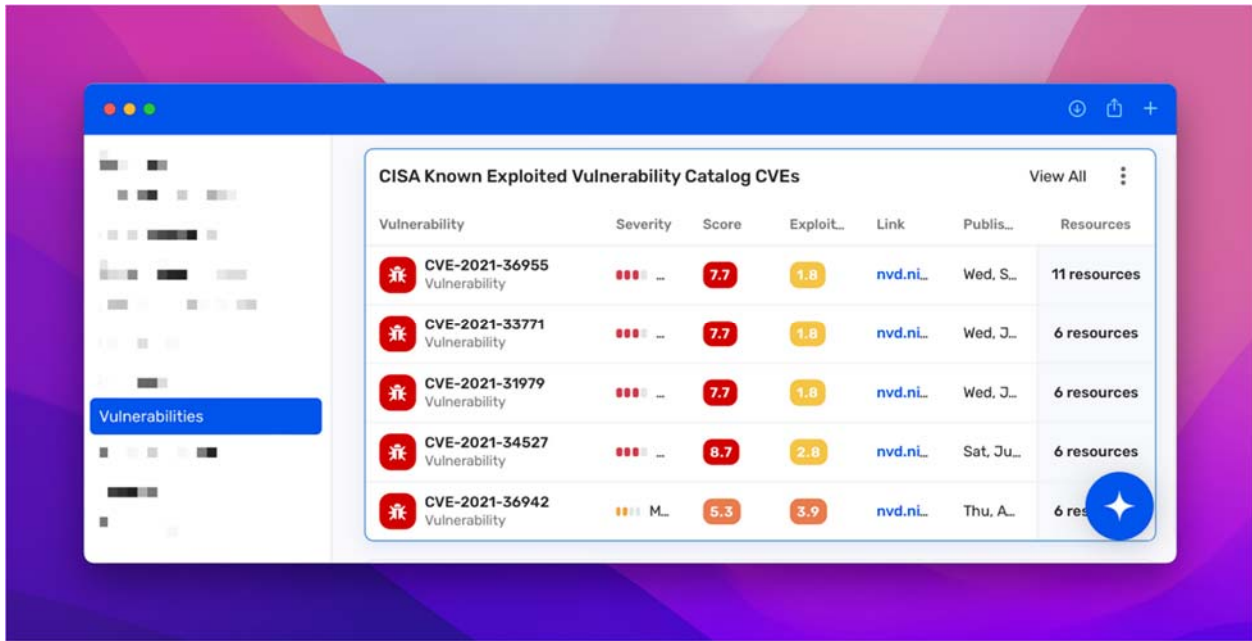


See id.

Control	Issues	Projects	Severity	Risks	Status
Publicly exposed VM instance with effective global admin permissions Security graph control	18 Issu...	All	High	High	Green
High/Critical network vulnerability with a known exploit on a publicly faci... Security graph control	1 issues	All	High	High	Green
CVE-2022-23131 (Zabbix vulnerability) detected on a publicly exposed V... Security graph control	-	All	High	High	Green
CVE-2022-30190 (Follina) detected on a highly privileged container Security graph control	-	All	High	High	Green
Lateral movement path via clear text cloud keys to an admin user Security graph control	-	All	High	High	Grey
SSH Brute Force on Admin VM Security graph control	4 issu...	All	High	High	Green
CVE-2022-22963 (Spring Cloud Function RCE vulnerability) detected on ... Security graph control	-	All	High	High	Green
Suspicious network activity on VM infected with malware Security graph control	-	All	High	High	Green
Publicly exposed VM instance/serverless with high/critical severity netw... Security graph control	-	All	High	High	Green
















See also Exhibit 5 at 27 (listing “CVE” vulnerabilities, such as “CVE-2022-23131 (Zabbix Vulnerability)”).

76. Claim 1 further recites “determining whether the matching installed applications are used by the protected virtual cloud asset” Wiz practices this step by, for example, determining whether applications in Wiz’s vulnerability catalog are used by virtual cloud assets to determine what vulnerabilities “pose the highest risk to [a] cloud environment.” See <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz>.



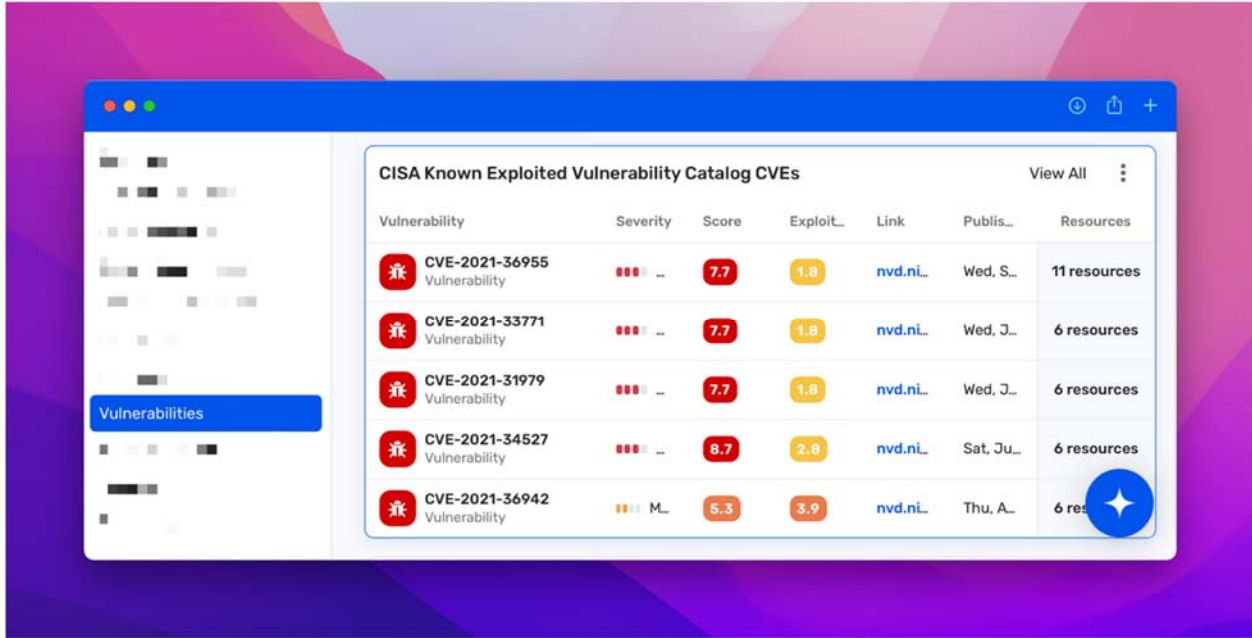
Id.; see also <https://www.wiz.io/solutions/dspm> (“Automatically correlate your sensitive data with underlying cloud context, including . . . how data assets are configured and used”); <https://www.wiz.io/blog/monitor-detect-and-respond-to-cloud-data-risks-faster-with-built-in-security-controls> (“[Y]ou can easily identify data resources with sensitive data that has traffic from an unrecommended IP.”); <https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory> (“The Wiz inventory already gives customers deep visibility into what cloud resources, applications, operating systems, and packages exist in their environment in minutes.”); Exhibit 6 at 3 (“Wiz uses the full context of your cloud and combines this information into a single graph in order to correlate related issues”).

77. Claim 1 further recites “prioritizing the potential cyber vulnerabilities based on the use determinations” Wiz performs this step by, for example, using its vulnerability “catalog input . . . to better prioritize and mitigate the critical risks.” See <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz>. Wiz also prioritizes cyber vulnerabilities based on one or more of “Severity,” “Score,” and “exploitability” ratings.

Vulnerability	Severity	Score
 CVE-2021-36955 Vulnerability		
 CVE-2021-33771 Vulnerability		
 CVE-2021-31979 Vulnerability		
 CVE-2021-34527 Vulnerability		
 CVE-2021-36942 Vulnerability		

See *id.*; see also Exhibit 5 at 27 (same).

78. Claim 1 further recites “reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.” Wiz performs this step by, for example, reporting “Vulnerabilit[ies],” prioritized according to “Severity,” “Score,” and/or “exploitability” through its “CISA Known Exploited Vulnerability Catalog CVEs dashboard.”



See <https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-key-with-wiz>; see also Exhibit 5 at 27 (prioritizing vulnerabilities according to “Severity”); <https://www.wiz.io/blog/monitor-detect-and-respond-to-cloud-data-risks-faster-with-built-in-security-controls> (Wiz “detect[s] and alert[s] on suspicious events and threats using rules continuously updated by Wiz Research.”); <https://www.wiz.io/solutions/dspm> (“Automatically correlate your sensitive data with underlying cloud context, including . . . how data assets are configured and used”).

79. As described in the preceding paragraphs, Wiz practices each limitation of claim 1 of the ’032 patent, either literally or under the doctrine of equivalents.

80. The above examples of how Wiz directly infringes claim 1 of the ’032 patent are non-limiting and based on information currently available to Orca. In particular, additional or different aspects of Wiz’s products or services may be identified that meet the limitations of claim 1 of the ’032 patent, additional claims of the ’032 patent may be determined to be infringed, and

additional Wiz products or services may be identified as infringing once additional nonpublic information is provided through the course of discovery.

(b) Induced Infringement of the '032 Patent

81. On information and belief, in providing Wiz's CSP to its customers, Wiz has induced, and continues to induce, direct infringement of one or more claims of the '032 patent, including at least claim 1, literally and/or under the doctrine of equivalents pursuant to 35 U.S.C. § 271(b).

82. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '032 patent and its infringement thereof when the '032 patent issued or soon thereafter at least as a result of its efforts to copy Orca's technology and its patents. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '032 patent's parent application, U.S. Patent Application No. 17/330,998, and its provisional application, U.S. Provisional Application No. 62/797,718, because Wiz's patent prosecution counsel is the same lawyer that filed those applications on behalf of Orca. As described above in Paragraph 22, Wiz's patents also include nearly identical figures and descriptions as those found in the '032 patent. In any event, Wiz has had knowledge of the '032 patent and its infringement thereof since at least as early as the filing of this Complaint.

83. On information and belief, Wiz possesses a specific intent to induce infringement by, at a minimum, providing user guides, instructions, sales-related material, and/or other supporting documentation, and by way of advertising, solicitation, and provision of product instruction materials, that instruct its customers on the normal operation of Wiz's CSP in a manner that infringes one or more claims of the '032 patent, including at least claim 1 of the '032 patent, or, in the alternative, Wiz believed there was a high probability that the acts of its customers would

infringe one or more claims of the '032 patent, including at least claim 1, and took deliberate steps to avoid learning of that infringement.

(c) Contributory Infringement of the '032 Patent

84. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '032 patent and its infringement thereof when the '032 patent issued or soon thereafter at least as a result of its efforts to copy Orca's technology and its patents. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '032 patent's parent application, U.S. Patent Application No. 17/330,998, and its provisional application, U.S. Provisional Application No. 62/797,718, because Wiz's patent prosecution counsel is the same lawyer that filed those applications on behalf of Orca. As described above in Paragraph 22, Wiz's patents also include nearly identical figures and descriptions as those found in the '032 patent. In any event, Wiz has had knowledge of the '032 patent and its infringement thereof since at least as early as the filing of this Complaint.

85. By providing Wiz's CSP to its customers, Wiz has in the past contributed, and continues to contribute, to the direct infringement of one or more claims of the '032 patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(c), including at least claim 1 of the '032 patent. Wiz has contributorily infringed and continues to contribute to the infringement of one or more claims of the '032 patent by offering to sell or selling Wiz's CSP, which is a patented component, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement and not a staple article or commodity of commerce suitable for substantial non-infringing use.

(d) Willful Infringement of the '032 Patent

86. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '032 patent and its infringement thereof when the '032 patent issued or soon thereafter at least as a result of its efforts to copy Orca's technology and its patents. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '032 patent's parent application, U.S. Patent Application No. 17/330,998, and its provisional application, U.S. Provisional Application No. 62/797,718, because Wiz's patent prosecution counsel is the same lawyer that filed those applications on behalf of Orca. As described above in Paragraph 22, Wiz's patents also include nearly identical figures and descriptions as those found in the '032 patent. In any event, Wiz has had knowledge of the '032 patent and its infringement thereof since at least as early as the filing of this Complaint.

87. Wiz's infringement has been and continues to be intentional and deliberate, entitling Orca to enhanced damages under 35 U.S.C. § 284 and a finding that this case is exceptional, entitling Orca to an award of reasonable attorneys' fees under 35 U.S.C. § 285.

88. On information and belief, Wiz has profited from and will continue to profit from its infringing activities. Orca has been and will continue to be damaged and irreparably harmed by Wiz's infringing activities. As a result, Orca is entitled to injunctive relief and damages adequate to compensate it for such infringement, in no event less than a reasonable royalty, in accordance with 35 U.S.C. §§ 271, 281, 283, and 284. The full amount of monetary damages Wiz's acts of infringement have caused to Orca cannot be determined without an accounting.

89. The harm to Orca from Wiz's ongoing infringing activity is irreparable, continuing, and not fully compensable by money damages, and will continue unless Wiz's infringing activities are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Orca respectfully asks that the Court enter judgment against Wiz and in favor of Orca as follows:

90. A judgment that Wiz has infringed and continues to infringe (either literally or under the doctrine of equivalents) one or more claims of the Asserted Patents under at least 35 U.S.C. § 271(a);

91. A judgment that Wiz has induced and continues to induce others to infringe one or more claims of the Asserted Patents under at least 35 U.S.C. § 271(b);

92. A judgment that Wiz has contributorily infringed and continues to contribute to the infringement of one or more claims of the Asserted Patents under at least 35 U.S.C. § 271(c);

93. A judgment that Wiz's infringement of the Asserted Patents has been and continues to be willful;

94. An award of monetary damages sufficient to compensate Orca for Wiz's patent infringement, with interest, pursuant to at least 35 U.S.C. § 284;

95. A preliminary and permanent injunction prohibiting Wiz and its officers, agents, representatives, assigns, licenses, distributors, servants, employees, related entities, attorneys, and all those acting in concert, privity, or participation with them, from:

- A. infringing or inducing the infringement of any claim of the Asserted Patents;
and
- B. soliciting any new business or new customers using any information or materials that Orca derived from its infringement of the Asserted Patents;

96. An award of enhanced damages of three times the amount found or assessed for Wiz's willful patent infringement, pursuant to at least 35 U.S.C. § 284, including interest on such damages;

97. An order finding this case exceptional and awarding Orca its attorneys' fees, to be obtained from any and all of Wiz's assets, pursuant to 35 U.S.C. § 285, including prejudgment interest on such fees;

98. An accounting and supplemental damages for all damages occurring after the period for which discovery is taken, and after discovery closes, through the Court's decision regarding the imposition of a permanent injunction;

99. An award of Orca's costs and expenses of this suit as the prevailing party; and

100. Any and all other relief that the Court deems just and proper.

JURY DEMAND

Orca hereby demands a trial by jury on all issues so triable.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jack B. Blumenfeld

OF COUNSEL:

Douglas E. Lumish
Lucas Lonergan
LATHAM & WATKINS LLP
140 Scott Drive
Menlo Park, CA 94025
(650) 328-4600

Blake R. Davis
LATHAM & WATKINS LLP
505 Montgomery Street, Suite 2000
San Francisco, CA 94111
(415) 391-0600

Jack B. Blumenfeld (#1014)
Rodger D. Smith II (#3778)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
jblumenfeld@morrisonichols.com
rsmith@morrisonichols.com

Attorneys for Plaintiff Orca Security Ltd.

July 12, 2023