IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ORCA SECURITY LTD.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 23-758 (GBW)
	)	
WIZ, INC.,	)	**DEMAND FOR JURY TRIAL**
	)	
Defendant.	)	

AMENDED 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 Amended 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"), 11,663,032 (the "'032 patent"), 11,693,685 (the "'685 patent"), 11,726,809 (the "'809 patent"), and 11,740,926 (the "'926 patent"), among others. Less than a month after the first of these patents issued on August 22, 2022, Orca announced to the public and its competitors that it had "secured a patent for its agentless SideScanning™ technology, providing visibility and risk coverage across the entire cloud estate."[5] Prior to issuance, Orca's marketing

---

[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

[5] https://orca.security/resources/press-releases/orca-security-innovation-patent-grant-sidescanning-technology/ (announcement dated November 10, 2022, and providing direct link to Orca's U.S. Patent No. 11,431,735 (https://patents.google.com/patent/US11431735)).

materials and publications dating back to June 2019 explained that the Orca Platform used a "patent-pending SideScanning™ technology."[6]

11. Orca's products, including the Orca Platform, and certain of Orca's services, practice the '031, '032, '685, '809, and '926 patents, among others. In accordance with 35 U.S.C. § 287(a), Orca virtually marks its products and maintains a webpage identifying a listing of patents applicable to those products. *See* https://orca.security/virtual-patent-marking/.

12. 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, '032, '685, '809, and '926 patents, without authorization.

WIZ AND ITS WIDESPREAD COPYING OF ORCA

13. Wiz was founded in January 2020 by Assaf Rappaport, Ami Luttwak, Yinon Costica, and Roy Reznik, a team that previously led the Cloud Security Group at Microsoft, one of the top providers of cloud computing environments in the world.[7] According to those founders, it was their time at Microsoft that provided them the "insight" that current cloud security tools

---

[6] 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/ (announcement dated June 12, 2019, "Patent-pending SideScanning™ technology deploys instantaneously without the impact and complexity of per-asset agents"); Exhibit 3 (Orca SideScanning Technical Brief (2020)) at 5 ("Orca Security uses our patent-pending SideScanning™ technology."), 15 ("Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads your cloud configuration and workloads' run-time block storage out-of-band. It detects vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and high-risk data such as PII.").

[7] 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.").

were too complicated, fragmented, and generate too many alerts.[8] 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.[9]

14. 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.

15. 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, workloads and containers" that was "already used by Fortune 100 companies."[10] In August 2022, Wiz announced it had become the "fastest-growing software company ever" reaching "$100M

---

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

9 *Id.*

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

ARR [annual recurring revenue] in 18 months."[11] And just eight months later in February 2023, Wiz raised $300 million and achieved a company valuation of $10 billion.[12]

16. 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:

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

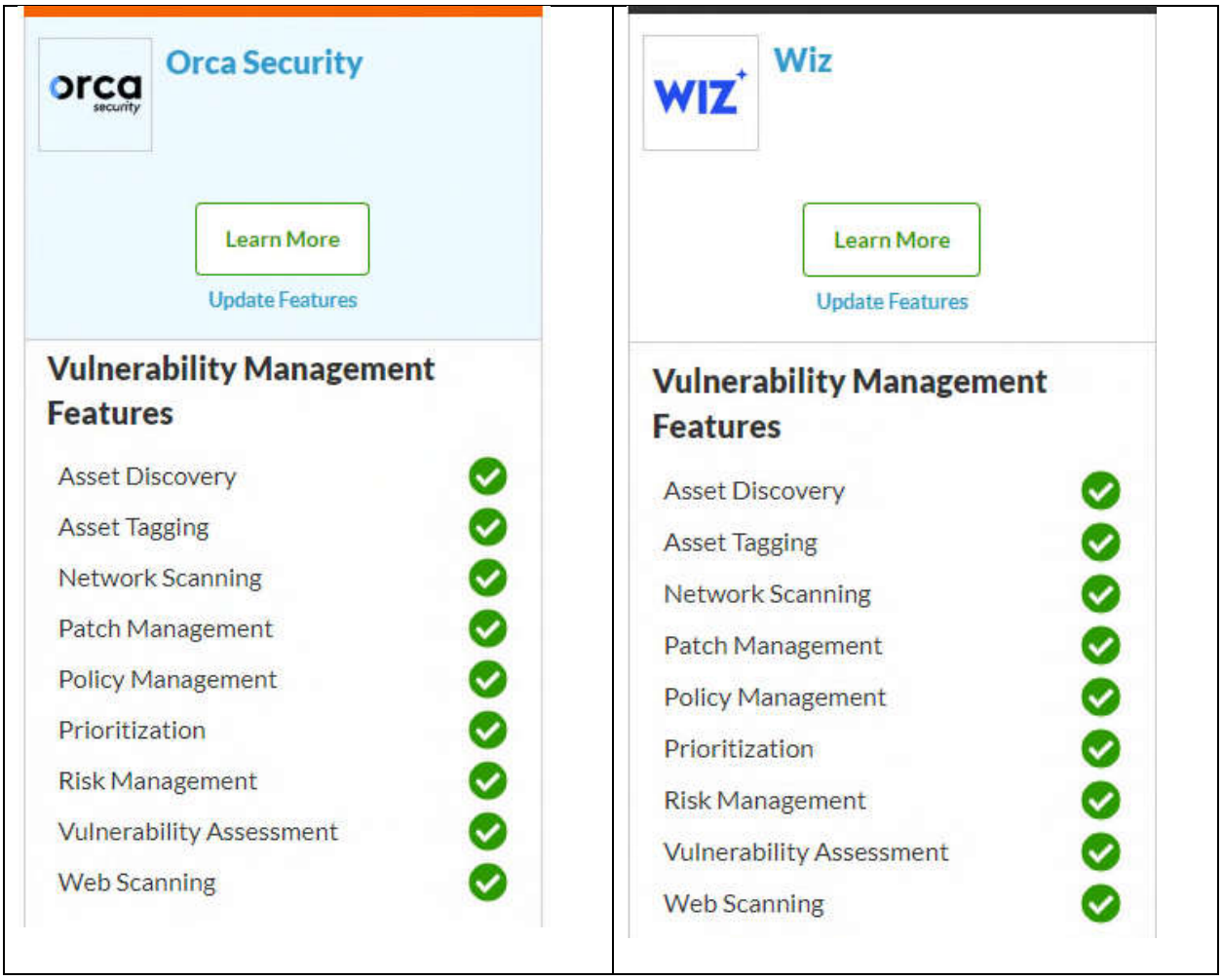
[11] https://www.wiz.io/blog/100m-arr-in-18-months-wiz-becomes-the-fastest-growing-software-company-ever

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

17. SOURCEFORGE also notes that Wiz has the same "Cybersecurity Features" as Orca:

Id.

18. SOURCEFORGE further shows that Wiz has the same "Vulnerability Management Features" as Orca:



Id.

19. 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"[13] and the "first full stack multi-cloud security platform."[14] 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.[15] As another more recent example,

[13] https://web.archive.org/web/20210128014251/https://wiz.io/

[14] https://web.archive.org/web/20210422201202/https://www.wiz.io/product

[15] 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/

Wiz announced in June 2022 that it had a "new vision for cloud security" with the "introduction of attack path analysis."[16] 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.[17]

20. 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 5. 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)). And Wiz knew, or should have known, that the technology Orca analogized to an "MRI" that Wiz copied would be protected by Orca's patent portfolio. Exhibit 3 (Orca SideScanning Technical Brief (2020) at 5 ("Orca Security uses our ***patent-pending SideScanning™ technology*** . . . [a]n apt analogy is to think of a medical MRI.").

21. 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

---

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

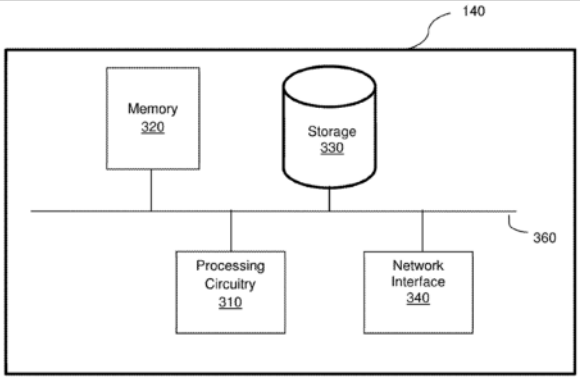
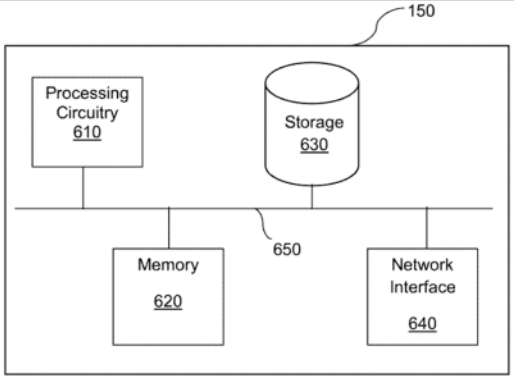
17 https://orca.security/resources/blog/cloud-attack-path-analysis/

("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 intelligence possible."). Wiz copied this too beginning with its very first website in 2020: "***We do the heavy lifting,*** you get total visibility."[18]

22. 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.

23. 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:

[18] https://web.archive.org/web/20201209145922/http://www.wiz.io/.

Orca	Wiz
 FIG. 3 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**. 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. '032 patent at Fig 3, 8:7-23; '031 patent at Fig. 3, 9:15-31.	 FIG. 6 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**. 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. Wiz's U.S. Patent No. 11,374,982 at Fig. 6, 20:61-21:12.

24. 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.

25. 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.

26. 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 collective pattern of efforts to copy and to compete unfairly with Orca.

27. Certain examples provided above may be explainable as an individual occurrence. But viewed collectively, they demonstrate a pattern of copying that pervades Wiz's business as a whole. This pattern leads to the further conclusion, on information and belief, that Wiz monitors virtually every aspect of Orca's business, from the mundane aspects of how it presents itself at conferences, to its marketing, and Orca's fundamental technology and patent portfolio. Wiz would have had reason to, and, on information and belief, does monitor Orca's patent portfolio because Orca's website and marketing materials—including those Wiz copies—explained the Orca Platform used "patent-pending" and "patented" technology. *See* Paragraphs 10-11, 20 above.[19] Wiz then copies, with intentional and/or reckless disregard for Orca's rights, anything it deems would give it an unfair advantage.

28. Wiz's continuous pattern of copying indicates, on information and belief, that Wiz had knowledge of the '031 patent, the '032 patent, the '685 patent, the '809 patent, and the '926

[19] *See also, e.g.,* https://orca.security/platform/ ("The Orca Cloud-Native Application Protection Platform (CNAPP) is built on Orca's patented SideScanning technology"); https://orca.security/platform/agentless-sidescanning/ ("Our patented SideScanning™ technology is at the heart of the Orca Platform . . ."); https://orca.security/platform/vulnerability-management/ ("Orca's patented SideScanning™ technology is a radical new approach that addresses the shortcomings of traditional vulnerability assessment and agent-based cloud security solutions.").

patent at or around the time that each patent issued, with knowledge or reckless disregard that its actions constituted infringement thereto.

29. 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, the '032 patent, the '685 patent, the '809 patent, and the '926 patent (collectively, the "Asserted Patents").

THE PARTIES

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

31. 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.[20]

JURISDICTION AND VENUE

32. 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).

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

34. 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.

[20] https://www.wiz.io/contact (Locations)

35. 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)

36. Orca incorporates all other allegations in this Amended Complaint.

37. 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.

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

39. The '031 patent is valid and enforceable.

40. 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

41. 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.

42. Claim 9 of the '031 patent recites:

> 9. 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.

43. 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.

44. 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").

45. 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").

46. 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.

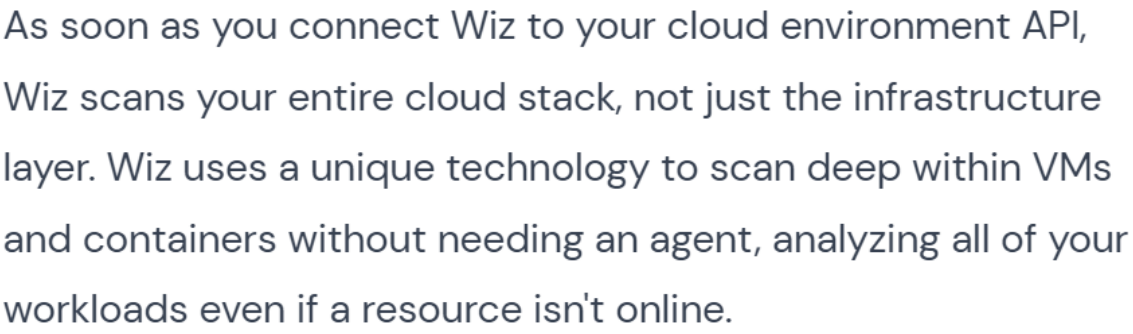
See Exhibit 5 at 13; Exhibit 6 (supported cloud computing platforms include AWS, Azure, and Google Cloud Platform (GCP)). Through the API, Wiz creates a graph of a client environment "with full context on the resource[s]," which includes identifying virtual disks of virtual machines. *See* https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-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.").

47. 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-

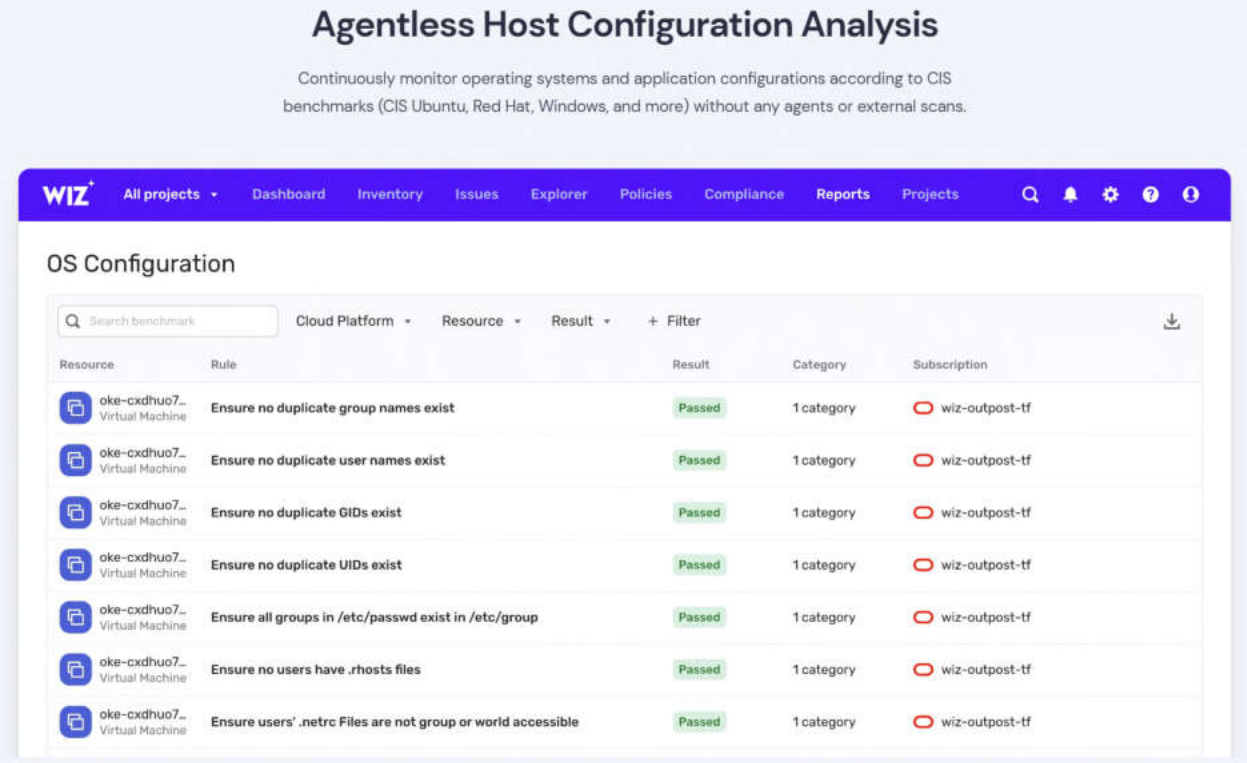
cisa-known-exploited-vulnerabilities-kev-with-wiz ("You can query and locate all the VMs, containers, and serverless functions in your cloud environment that are vulnerable to a specific CVE in the catalog with a simple query shortcut."); https://www.wiz.io/solutions/cnapp ("Scan buckets, data volumes, 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.").

48. 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").

49. 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://www.wiz.io/partners/gcp. 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.

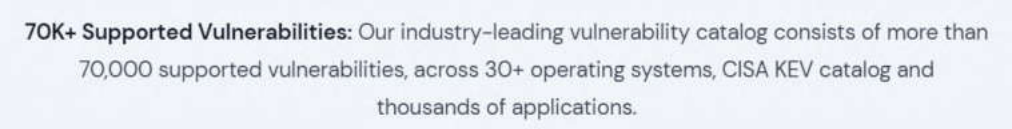


https://www.wiz.io/solutions/vulnerability-management.

50. 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://www.wiz.io/partners/gcp ("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.").

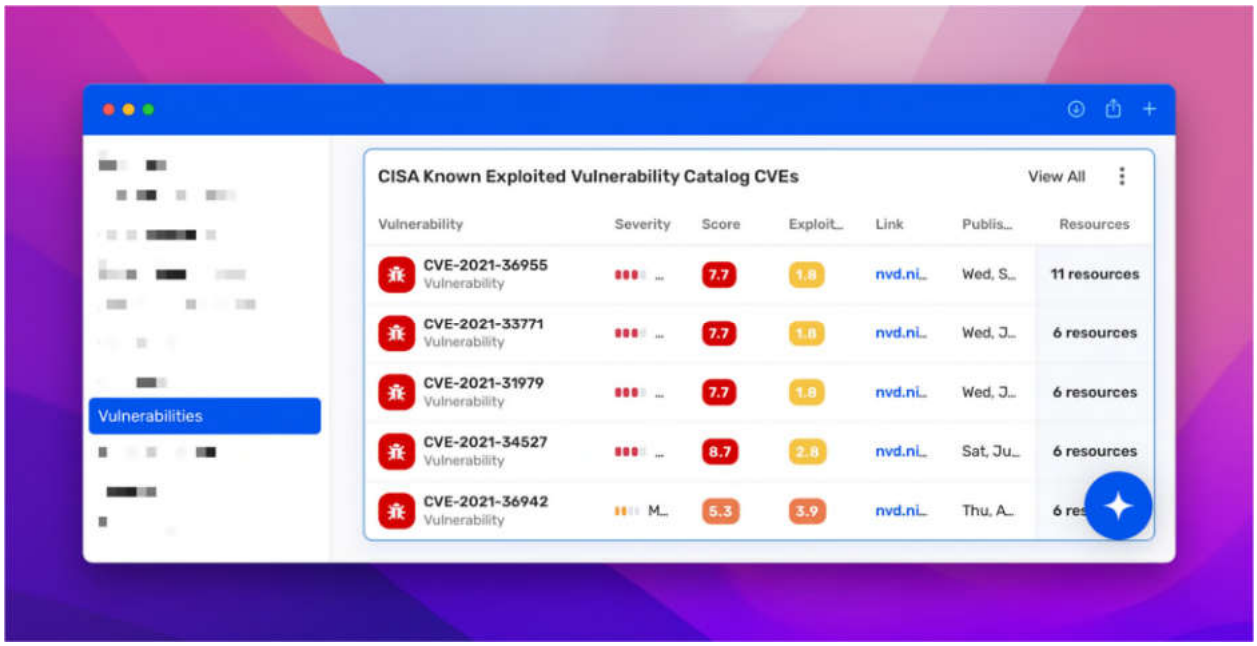
51. Claim 9 further recites "analyzing the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive . . . ." Wiz performs this step by, for example, analyzing the snapshot of a virtual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



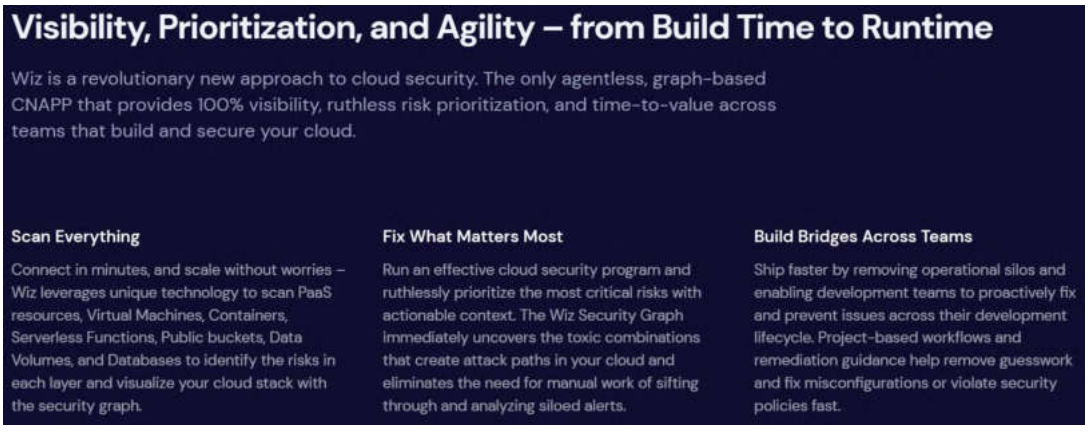
https://www.wiz.io/solutions/vulnerability-management.

52. 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://www.wiz.io/partners/gcp ("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").

53. 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."



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.").

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

55. 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

56. 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).

57. 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 collective pattern of efforts to copy Orca's technology and its patents as discussed

above in Paragraphs 13-29. 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 23, 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 the Original Complaint on July 12, 2023.

58. 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.

59. Wiz's specific intent to induce infringement is also demonstrated by its actions since the filing of the Original Complaint on July 12, 2023. As of September 15, 2023, despite the disclosure of its infringement in the Original Complaint, Wiz still maintains all the same pages on its website instructing its customers and potential customers on how the Wiz CSP can be used to infringe the '031 Patent that were identified in the Original Complaint. *See, e.g.*, https://www.wiz.io/solutions/iac (last accessed Sept. 15, 2023); https://www.wiz.io (last accessed Sept. 15, 2023); https://www.wiz.io/product (last accessed Sept. 15, 2023);

https://www.wiz.io/solutions/cnapp (last accessed Sept. 15, 2023); https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/vulnerability-management (last accessed Sept. 15, 2023); https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5643759466396-Security-Graph-Basics (last accessed Sept. 15, 2023); https://legacy.wiz.io/partners/google (now https://www.wiz.io/partners/gcp (last accessed Sept. 15, 2023)); https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning (last accessed Sept. 15, 2023).

60. In addition, after the filing of the Original Complaint, Wiz posted a video on August 11, 2023, specifically instructing users how Wiz "does agentless vulnerability scanning across every layer of your cloud environment including virtual machines," "detects" vulnerabilities, "generates a vulnerability finding" for each detected vulnerability, and how a customer is presented "with a prioritized list of issues related to vulnerabilities" in a manner intended to infringe at least claim 9 of the '031 patent. *See, e.g.*, https://www.youtube.com/watch?v=GP0NWZa_7vk ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023); *see also* https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

(c) Contributory Infringement of the '031 Patent

61. 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 collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. 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 23, 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 the Original Complaint on July 12, 2023.

62. 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.

63. Wiz's CSP, or any further component parts thereof, is not a staple article of commerce and has no substantial non-infringing use. On information and belief, Wiz's CSP cannot operate without incorporating technology claimed by the claims of the '031 patent. Specifically, as described above, Wiz's user guides, instructions, sales-related material, and/or

other supporting documentation state that Wiz's CSP is intended to be used to perform agentless scanning of virtual assets, including a virtual machine at rest, in a client environment through snapshot scanning, detect vulnerabilities, and report detected vulnerabilities as alerts, as claimed in the claims of the '031 patent. *See, e.g.*, Exhibit 4 at 1-2, 10-11; Exhibit 5 at 11-23; Exhibit 6. Its documentation do not advertise or otherwise suggest that Wiz's CSP is a staple article of commerce or has a substantial non-infringing use. *See generally* Exhibit 5; Exhibit 6. Furthermore, when used as shown in Wiz's documentation, Wiz's CSP directly infringes claims of the '031 patent as described above in Paragraphs 41-55.

64. On information and belief, Wiz has continued to contributorily infringe in the same way as set forth in the preceding paragraphs since the filing of the Original Complaint on July 12, 2023. As of September 15, 2023, despite the disclosure of its infringement in the Original Complaint, Wiz still maintains all the same pages on its website that were identified in the Original Complaint and are referenced herein. *See, e.g.*, https://www.wiz.io/solutions/iac (last accessed Sept. 15, 2023); https://www.wiz.io (last accessed Sept. 15, 2023); https://www.wiz.io/product (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/cnapp (last accessed Sept. 15, 2023); https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/vulnerability-management (last accessed Sept. 15, 2023); https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security (last accessed Sept. 15, 2023); https://legacy.wiz.io/partners/google (now https://www.wiz.io/partners/gcp (last accessed Sept. 15, 2023)); https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning (last accessed Sept. 15, 2023).

(d) *Willful Infringement of the '031 Patent*

65. 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 collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. 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 23, 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 the Original Complaint on July 12, 2023.

66. Wiz's intentional and deliberate infringement is also demonstrated by its actions since the filing of the Original Complaint on July 12, 2023, which show a continuing willful, deliberate, and consciously wrongful intent to infringe the '031 patent. As of September 15, 2023, despite the disclosure of its infringement in the Original Complaint, Wiz still maintains all the same pages on its website identified in the Original Complaint describing Wiz's infringement of the '031 patent. *See, e.g.,* Original Complaint ¶¶ 38-52; https://www.wiz.io/solutions/iac (last accessed Sept. 15, 2023); https://www.wiz.io (last accessed Sept. 15, 2023); https://www.wiz.io/product (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/cnapp (last accessed Sept. 15, 2023); https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/vulnerability-management (last

accessed Sept. 15, 2023); https://www.wiz.io/blog/uniting-builders-and-defenders-a-new-vision-for-cloud-security (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5643759466396-Security-Graph-Basics (last accessed Sept. 15, 2023); https://legacy.wiz.io/partners/google (now https://www.wiz.io/partners/gcp (last accessed Sept. 15, 2023)); https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning (last accessed Sept. 15, 2023).

67. Wiz also posted a video on August 11, 2023, describing how Wiz continues to use its Wiz CSP to do "agentless vulnerability scanning across every layer of your cloud environment including virtual machines," "detects" vulnerabilities, "generates a vulnerability finding" for each detected vulnerability, and presenting "a prioritized list of issues related to vulnerabilities" in a manner that demonstrates a conscious disregard for Orca's rights in the inventions claimed in the '031 patent. *See, e.g.*, https://www.youtube.com/watch?v=GP0NWZa_7vk ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023); *see also* https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

68. 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.

69. 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.

70. 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)

71. Orca incorporates all other allegations in this Amended Complaint.

72. 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.

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

74. The '032 patent is valid and enforceable.

75. 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.

76. 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*

77. 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.

78. 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.

79. 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.

80. 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").

81. 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.

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").

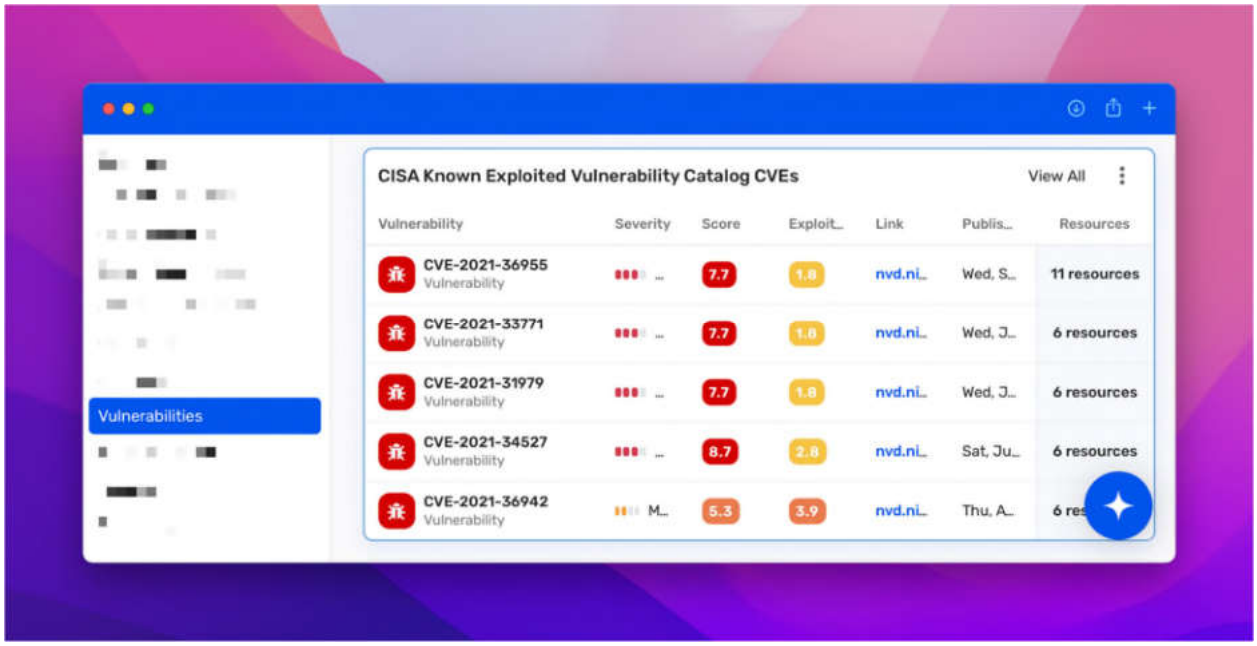
82. Claim 1 further recites "accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk . . . ." Wiz performs this step by, for example, accessing the snapshot of a virtual disk in order to "analyze[] [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).

83. 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."

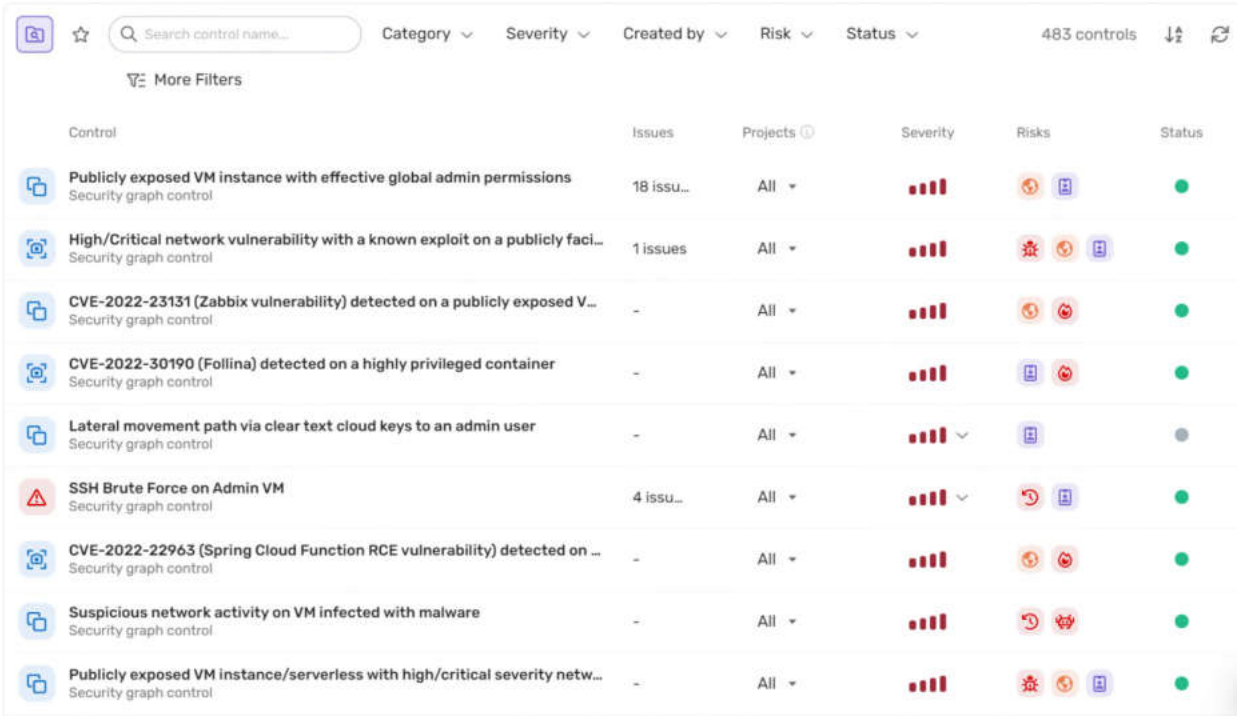
70K+ Supported Vulnerabilities: Our industry-leading vulnerability catalog consists of more than 70,000 supported vulnerabilities, across 30+ operating systems, CISA KEV catalog and thousands of applications.

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

84. 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.

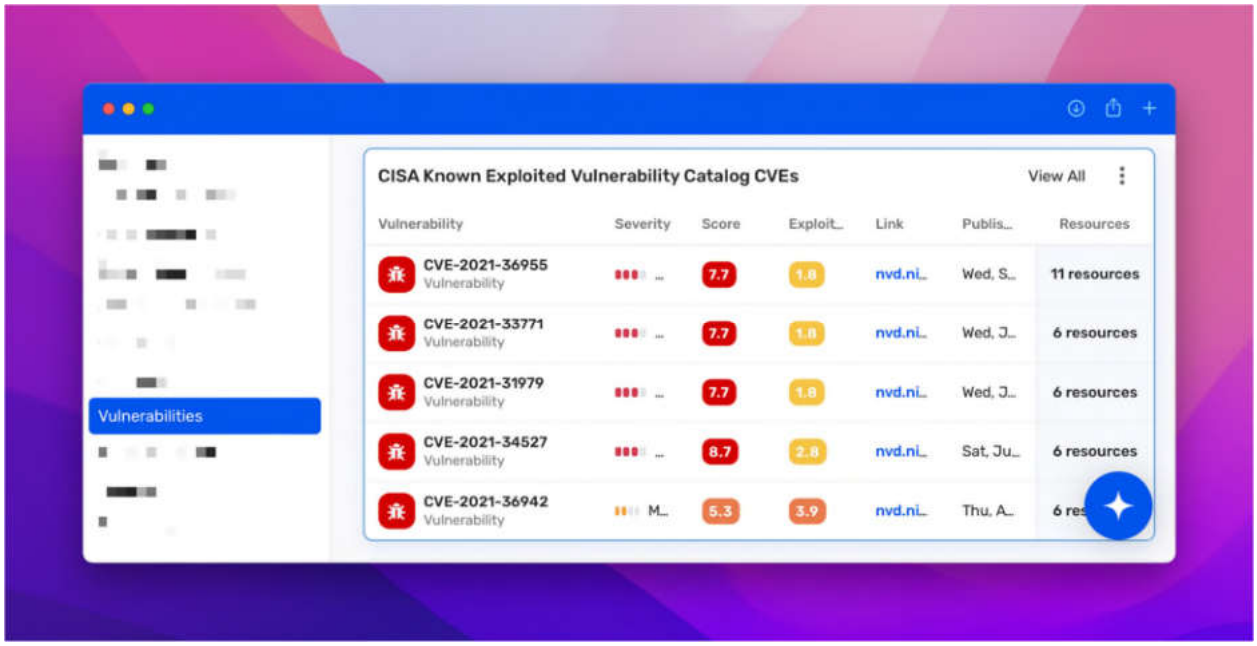


See id.



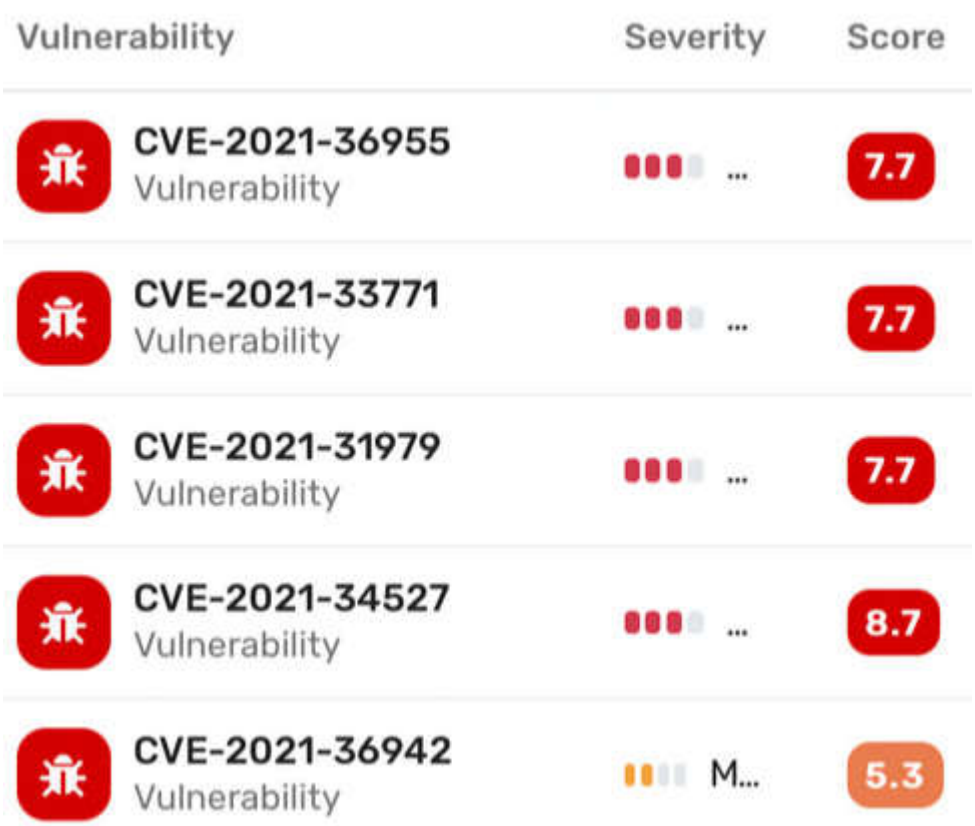
See also Exhibit 5 at 27 (listing "CVE" vulnerabilities, such as "CVE-2022-23131 (Zabbix Vulnerability)").

85. 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.



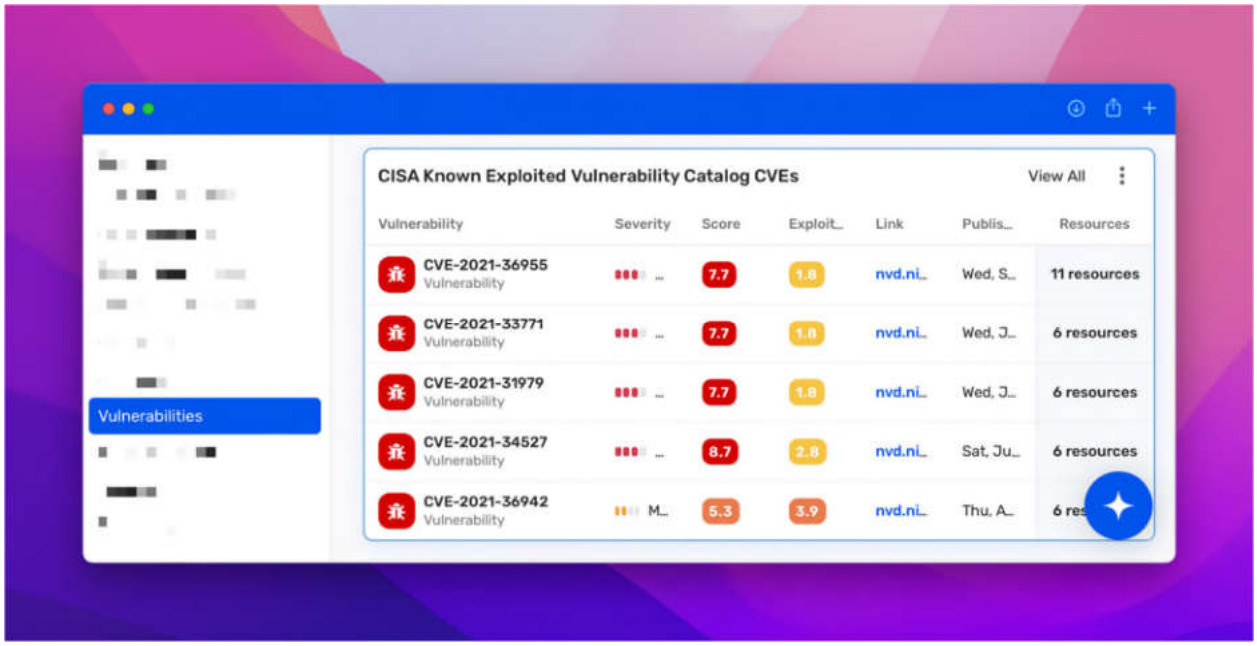
Id.; *see also* https://www.wiz.io/solutions/dspm ("Automatically correlate your sensitive data with underlying cloud context, including . . . how data assets are configured and used"); https://www.wiz.io/blog/monitor-detect-and-respond-to-cloud-data-risks-faster-with-built-in-security-controls ("[Y]ou 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").

86. 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.



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

87. 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-kev-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").

88. 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.

89. 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

90. 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).

91. 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 collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '032 patent's parent application, U.S. Patent Application No. 16/585,967 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 23, 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 the Original Complaint on July 12, 2023.

92. 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.

93. Wiz's specific intent to induce infringement is also demonstrated by its actions since the filing of the Original Complaint on July 12, 2023. As of September 15, 2023, despite the disclosure of its infringement in the Original Complaint, Wiz still maintains all the same pages on its website instructing its customers and potential customers on how the Wiz CSP can be used to infringe the '032 Patent that were identified in the Original Complaint. *See, e.g.*, https://www.wiz.io/ (last accessed Sept. 15, 2023); https://www.wiz.io/product (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/cnapp (last accessed Sept. 15, 2023); https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/vulnerability-management (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/dspm (last accessed Sept. 15, 2023); https://www.wiz.io/blog/monitor-detect-and-respond-to-cloud-data-risks-faster-with-built-in-security-controls (last accessed Sept. 15, 2023); https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory (last accessed Sept. 15, 2023).

94. In addition, after the filing of the Original Complaint, Wiz posted a video on August 11, 2023, specifically instructing users how to use Wiz's platform to perform agentless scanning of virtual cloud assets, vulnerability detection using a list of applications with known vulnerabilities, and reporting of vulnerabilities as prioritized alerts based on risk in a manner

specifically intended to infringe at least claim 1 of the '032 patent. *See, e.g.*, https://www.youtube.com/watch?v=GP0NWZa_7vk ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023); *see also* https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

(c) Contributory Infringement of the '032 Patent

95. 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 collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '032 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, 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 the Original Complaint on July 12, 2023.

96. 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.

97. Wiz's CSP, or any further component parts thereof, is not a staple article of commerce and has no substantial non-infringing use. On information and belief, Wiz's CSP cannot operate without incorporating technology claimed by the claims of the '032 patent. Specifically, as described above, Wiz's user guides, instructions, sales-related material, and/or other supporting documentation state that Wiz's CSP is intended to be used to perform agentless scanning of virtual assets in a client environment through snapshot scanning using an API provided by the cloud environment, match installed applications to a known list of vulnerabilities (such as vulnerabilities in the CISA KEV Catalog), and to determine, prioritize, and report potential vulnerabilities based on use determinations, as claimed in the claims of the '032 patent. *See, e.g.*, Exhibit 4 at 1-2; Exhibit 5 at 11-23; Exhibit 6; https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz. Its documentation do not advertise or otherwise suggest that Wiz's CSP is a staple article of commerce or has a substantial non-infringing use. *See generally* Exhibit 5; Exhibit 6. Furthermore, when used as shown in Wiz's documentation, Wiz's CSP directly infringes claims of the '032 patent as described above in Paragraphs 77-89.

98. On information and belief, Wiz has continued to contributorily infringe in the same way as set forth in the preceding paragraphs since the filing of the Original Complaint on July 12, 2023. As of September 15, 2023, despite the disclosure of its infringement in the Original Complaint, Wiz still maintains all the same pages on its website that were referenced in the Original Complaint and are referenced herein. *See, e.g.*, https://www.wiz.io/ (last accessed Sept. 15, 2023); https://www.wiz.io/product (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/cnapp (last accessed Sept. 15, 2023);

https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/vulnerability-management (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/dspm (last accessed Sept. 15, 2023); https://www.wiz.io/blog/monitor-detect-and-respond-to-cloud-data-risks-faster-with-built-in-security-controls (last accessed Sept. 15, 2023); https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory (last accessed Sept. 15, 2023).

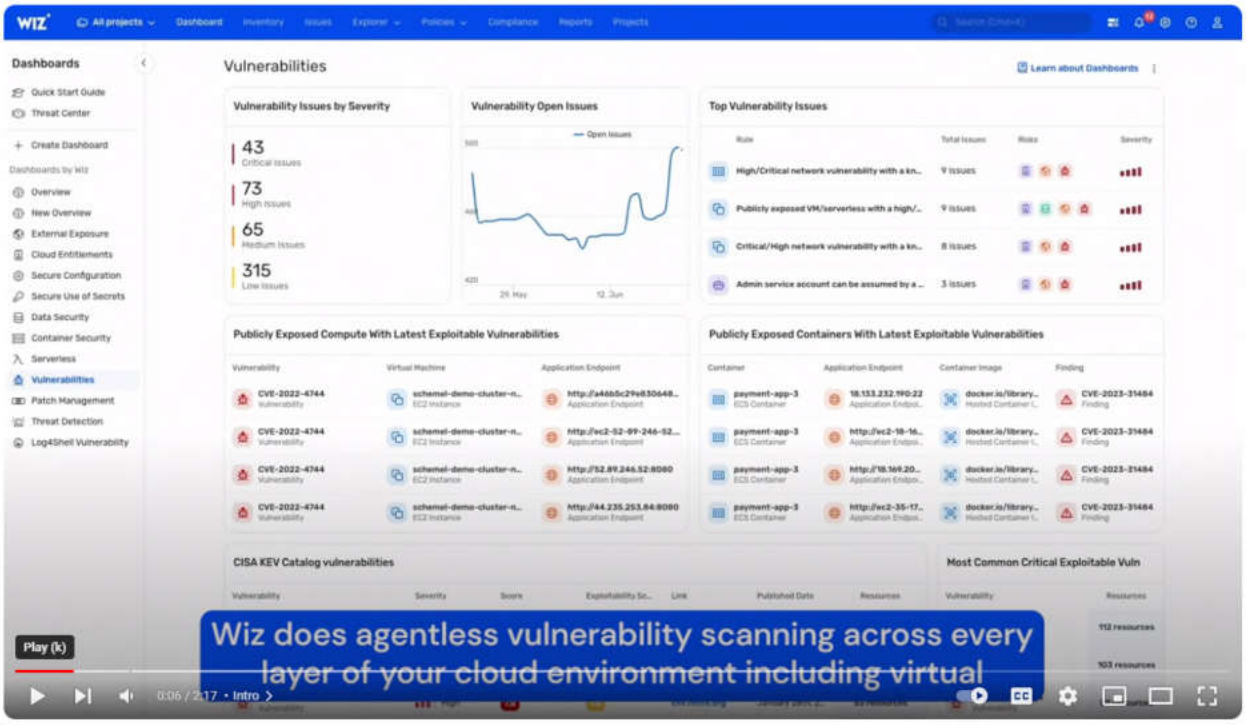
(d) Willful Infringement of the '032 Patent

99. 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 collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '032 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, 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 the Original Complaint on July 12, 2023.

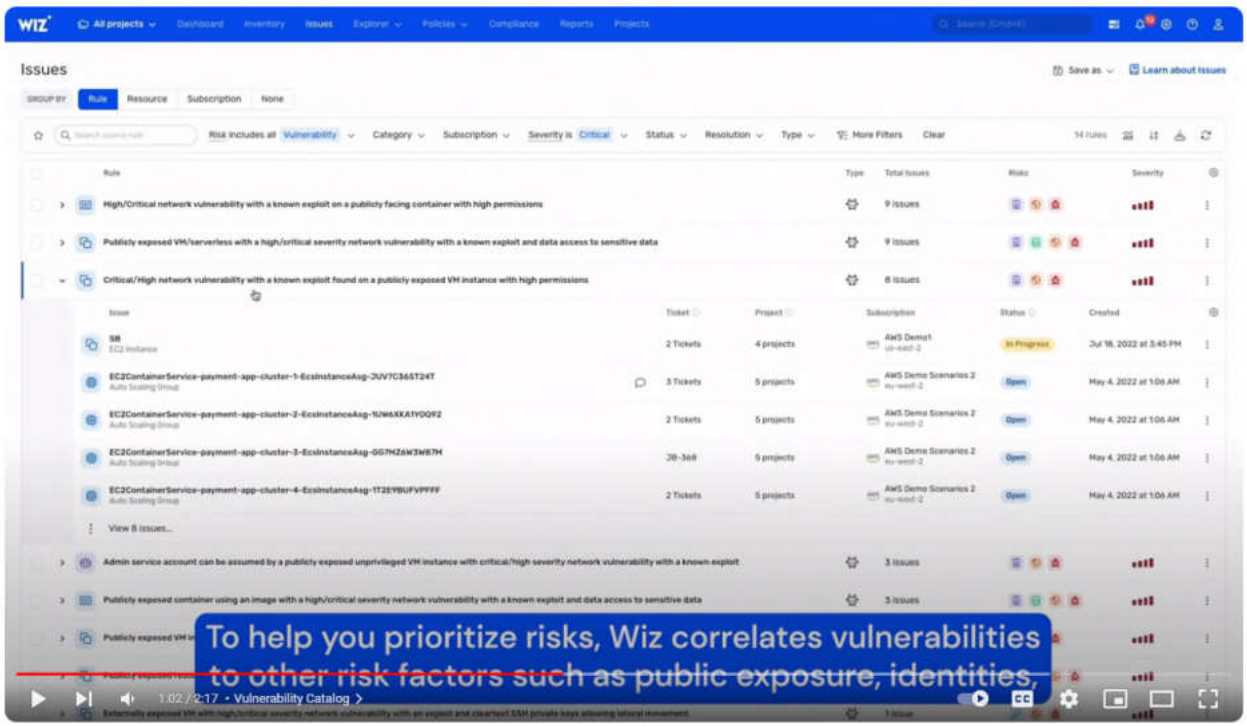
100. Wiz's intentional and deliberate infringement is also demonstrated by its actions since the filing of the Original Complaint on July 12, 2023, which show a continuing willful, deliberate, and consciously wrongful intent to infringe the '032 patent. As of September 15, 2023, despite the disclosure of its infringement in the Original Complaint, Wiz still maintains all the same pages on its website identified in the Original Complaint describing Wiz's infringement of the '032 patent. *See, e.g.,* Original Complaint ¶¶ 62-89; https://www.wiz.io/ (last accessed

Sept. 15, 2023); https://www.wiz.io/product (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/cnapp (last accessed Sept. 15, 2023); https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5641497256860-Azure-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5449816387100-AWS-Connector-Basics (last accessed Sept. 15, 2023); https://support.wiz.io/hc/en-us/articles/5642208092572-GCP-Connector-Basics (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/vulnerability-management (last accessed Sept. 15, 2023); https://www.wiz.io/solutions/dspm (last accessed Sept. 15, 2023); https://www.wiz.io/blog/monitor-detect-and-respond-to-cloud-data-risks-faster-with-built-in-security-controls (last accessed Sept. 15, 2023); https://www.wiz.io/blog/uncover-what-is-deployed-in-your-environment-with-enhanced-wiz-inventory (last accessed Sept. 15, 2023).

101. Wiz also posted a video on August 11, 2023, describing how Wiz continues to use its Wiz CSP to infringe the ’032 patent, including by promoting Wiz’s agentless scanning of virtual cloud assets, vulnerability detection using a list of applications with known vulnerabilities, and reporting of vulnerabilities as prioritized alerts based on risk.



See, e.g., https://www.youtube.com/watch?v=GP0NWZa_7vk ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) at 0:06 (last accessed Sept. 15, 2023).



Id. at 1:02; *see also* https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

102. 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.

103. 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.

104. 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 III
(INFRINGEMENT OF THE '685 PATENT)

105. Orca incorporates all other allegations in this Amended Complaint.

106. The '685 patent is entitled "Virtual Machine Vulnerabilities and Sensitive Data Analysis and Detection" and was duly and legally issued on July 4, 2023. A true and correct copy of the '685 patent is attached hereto as Exhibit 7.

107. Orca is the owner of all rights, title, and interest in the '685 patent.

108. The '685 patent is valid and enforceable.

109. The inventions claimed in the '685 patent improved on prior art cloud security systems and methods by, *inter alia*, using an interface to identify virtual disks of a virtual machine,

generating at least one snapshot of the virtual disks, analyzing the at least one snapshot to detect vulnerabilities and sensitive data wherein analyzing the at least one snapshot requires no interaction with the virtual machine, determining a risk level of the virtual machine, and reporting said vulnerabilities and sensitive data. *See, e.g.*, '685 patent at cls. 1-22. This novel analysis of snapshots and data requiring no interaction with the virtual machine was not well understood, routine, or conventional. It is an inventive concept that enables agentless security assessments, and improves the practicality and effectiveness of protecting cloud computing infrastructure and virtual machines by reducing costs typically associated with such protection, including the cost of licensing, deployment, integration, training, and support. By analyzing virtual assets without interaction with the virtual machine, the '685 patent provided improved security for a cloud computing platform because virtual machines can be analyzed more easily, quickly, and comprehensively than previous strategies allowed.

(a) Direct Infringement of the '685 Patent

110. Wiz, without authorization, directly infringes one or more claims of the '685 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 '685 patent.

111. Claim 1 of the '685 patent recites:

1. A system for inspecting data, the system comprising: at least one processor configured to:

establish an interface between a client environment and security components;

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

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

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

generate at least one snapshot of the virtual disks of the virtual machine;

analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine;

determine a risk level of the virtual machine; and

report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.

112. On information and belief, Wiz practices each and every limitation of claim 1 of the ’685 patent by and through the use of Wiz’s CSP and/or other similar products or services for Wiz’s clients or customers.

113. The preamble of claim 1 recites “[a] system for inspecting data, the system comprising: at least one processor configured to . . . .” Wiz’s public presentations and technical documentation confirm that Wiz’s CSP system is a system for inspecting data. *See, e.g.*, Exhibit 5 at 13 (Wiz performs an “[a]gentless scan of cloud metadata and workloads,” including

"Application and Data"), 20 (Wiz performs "[s]ecrets scanning in data assets"), 21 (Wiz performs "[d]ata scanning"); Exhibit 6 at 2 ("Wiz analyzes the operating system, applications, code libraries, and secrets. Wiz also scans your cloud configuration and metadata."). On information and belief, Wiz's CSP is implemented in software running on at least one processor including to "scan everything, provide context and prioritization on the most pressing risks, and enable secure practice practices." https://www.wiz.io/solutions/cnapp; *see id.* ("Wiz leverages unique technology to scan PaaS resources, Virtual Machines, Containers, Serverless Functions, . . . to identify the risks in each layer").

114. Claim 1 further recites "establish an interface between a client environment and security components . . . ." Wiz's CSP practices this element by, for example, establishing an interface "via API" to a client environment and security components.

See Exhibit 5 at 13; Exhibit 6 (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").

115. Claim 1 further recites "using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment . . . ." Wiz's CSP satisfies this limitation because, for example, it utilizes APIs provided by AWS, GCP, and Azure, among other cloud computing environments, to identify virtual disks of a virtual machine in the client environment.

See Exhibit 5 at 13; Exhibit 6 (supported cloud computing platforms include AWS, Azure, and Google Cloud Platform (GCP)). Through the API, Wiz's system 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.").

116. Claim 1 further recites "use the computing platform APIs to query a location of at least one of the identified virtual disks . . . ." Wiz's CSP satisfies this limitation because, for example, it uses computing platform APIs from AWS, GCP, Azure, and other providers, 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."); 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").

117. Claim 1 further recites "receive an identification of the location of the virtual disks of the virtual machine . . . ." Wiz's CSP satisfies this limitation because, for example, it identifies

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's CSP system creates 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").

118. Claim 1 further recites "generate at least one snapshot of the virtual disks of the virtual machine . . . ." Wiz's CSP satisfies this limitation because, for example, it generates 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, 2 ("Wiz scans all the resources and workloads in your cloud environment using a unique snapshot technology that covers more than an agent can."). 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).

119. Claim 1 further recites "analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the

virtual machine . . . ." Wiz's CSP satisfies this limitation because, for example, it analyzes the snapshot of a virtual disk to determine cyber vulnerabilities affecting the virtual disk.

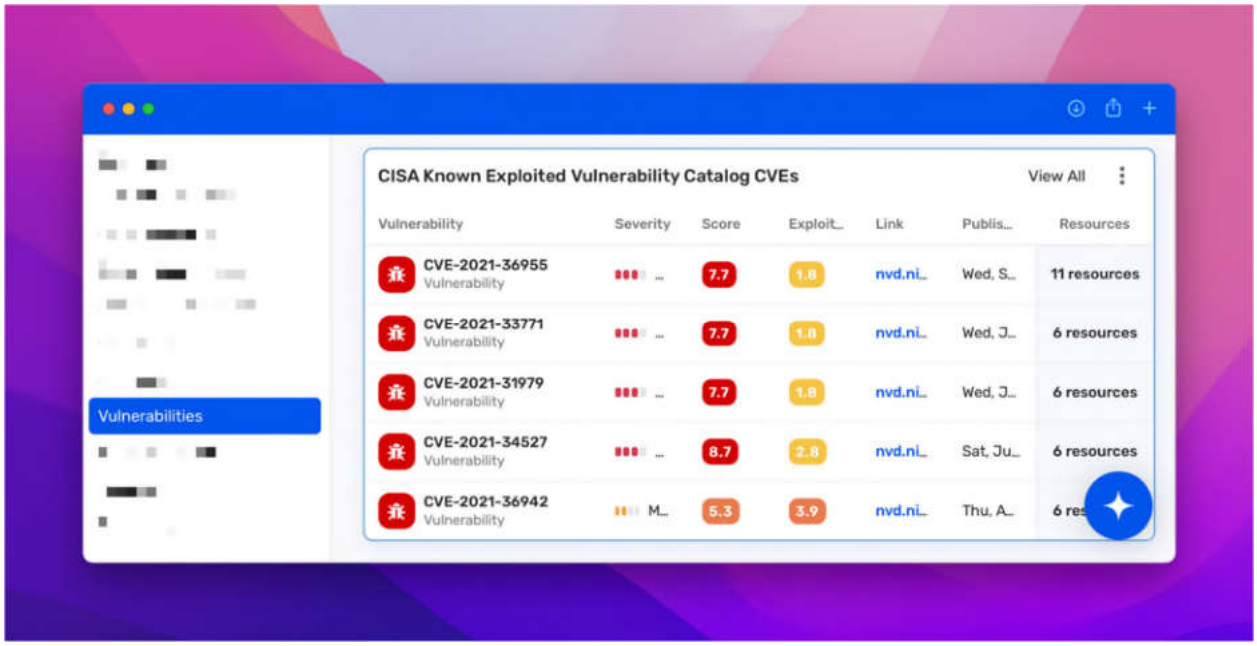
> **70K+ Supported Vulnerabilities:** Our industry-leading vulnerability catalog consists of more than 70,000 supported vulnerabilities, across 30+ operating systems, CISA KEV catalog and thousands of applications.

https://www.wiz.io/solutions/vulnerability-management. Wiz's CSP also "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."). Wiz's CSP also detects "sensitive data and secrets exposure." *See, e.g.,* https://www.wiz.io/solutions/dspm. Furthermore, Wiz's CSP analyzes snapshots without "deploying agents." *See, e.g.,* https://www.wiz.io/solutions/vulnerability-management ("Using a one-time cloud native API deployment, continuously assess workloads without deploying agent").

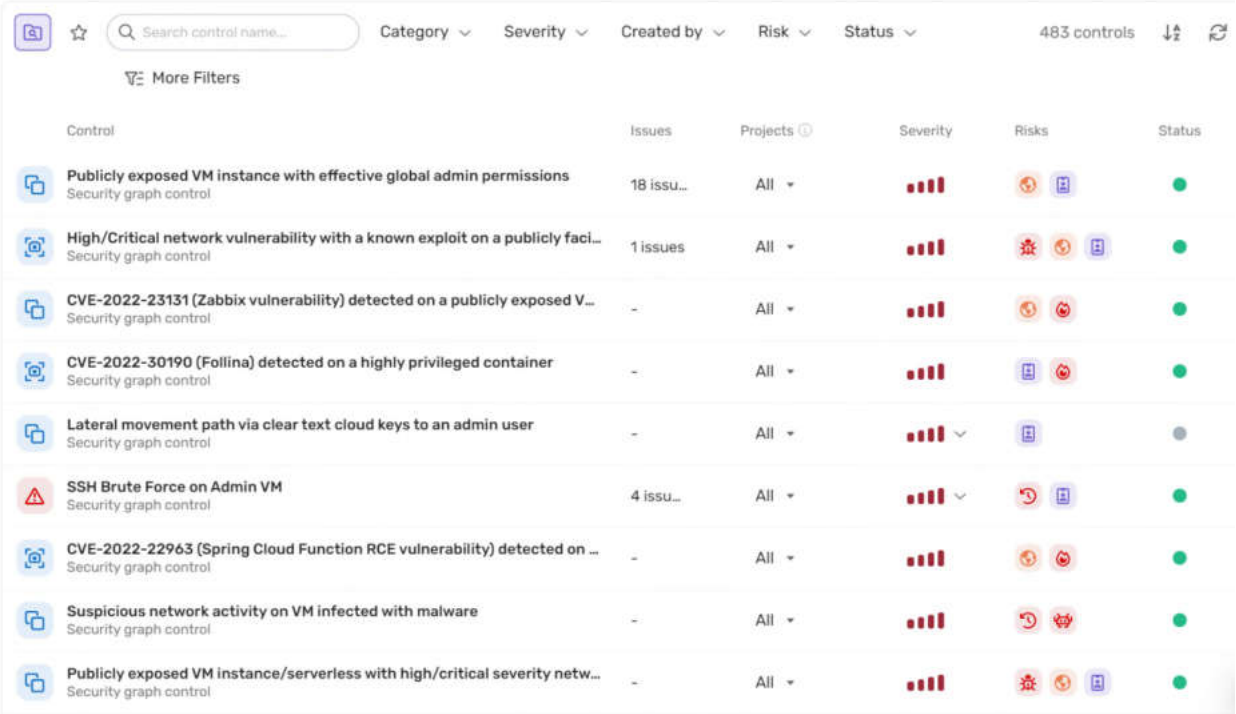
120. Claim 1 further recites "determine a risk level of the virtual machine . . . ." Wiz's CSP satisfies this limitation because, for example, it identifies assets with "toxic combinations" and "finding the resources that pose the highest risk in [a] cloud environment."

> Wiz scans the entire stack to identify the toxic combinations that represent real risk to your environment. Using the Wiz contextual security graph, you can prioritize patching by focusing on these toxic combinations and finding the resources that pose the highest risk in your cloud environment. For example:

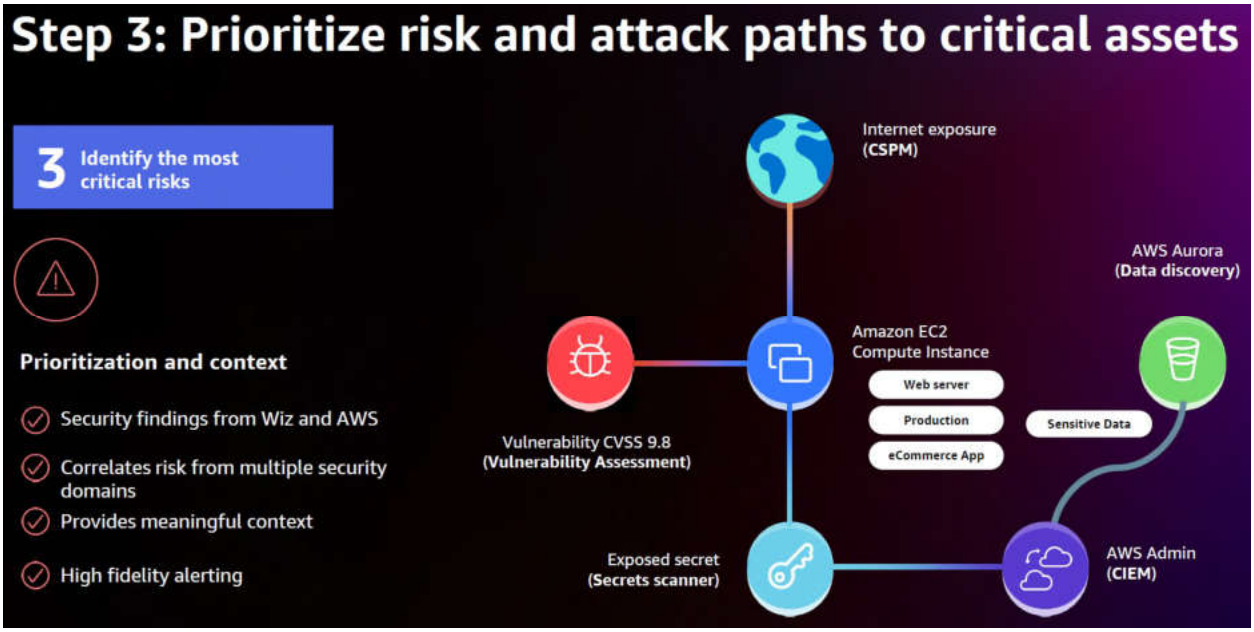
https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz.



Id.

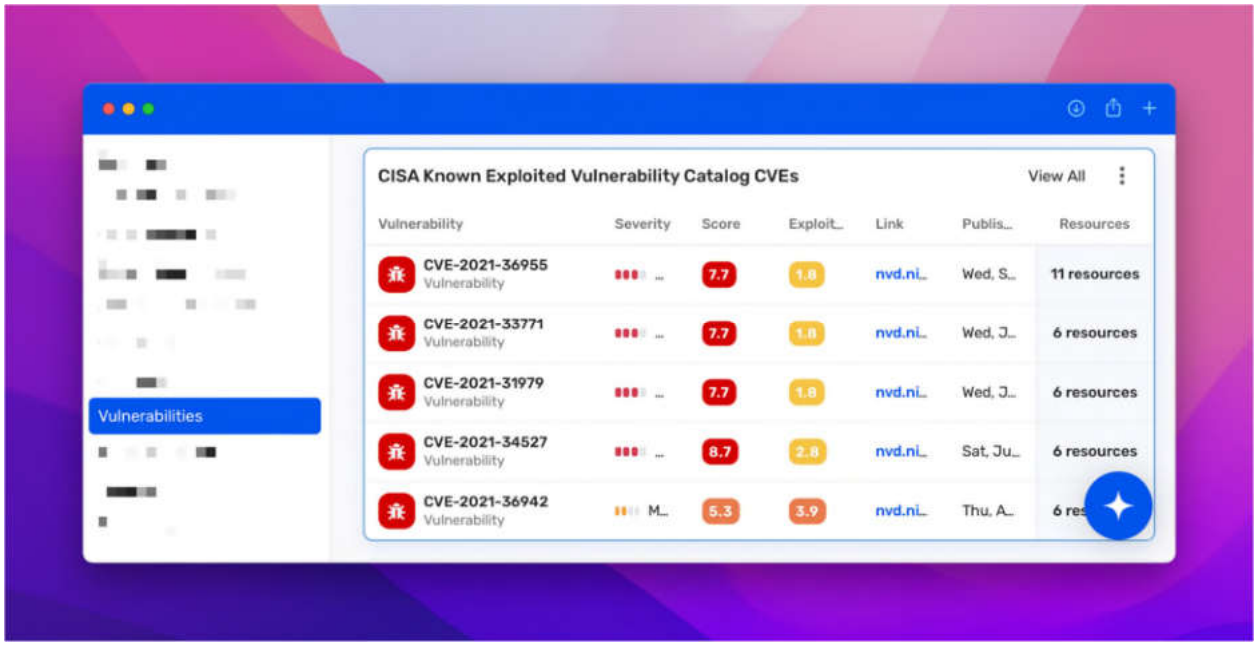


See also Exhibit 5 at 27. Wiz also states that it "[p]rioritize[s] risk and attack paths to critical assets" within the cloud computing environment.



Id. at 17; *see also* Exhibit 6 at 3 ("Scan for vulnerable and unpatched operating systems, installed software, and code libraries in your workloads prioritized by risk."); https://www.wiz.io/solutions/cnapp ("ruthless risk prioritization", "prioritize the most critical risks").

121. Claim 1 further recites "report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine." Wiz's CSP satisfies this element because, for example, it reports detected vulnerabilities and sensitive data and "prioritize[s] the most critical risks." *See, e.g.,* https://www.wiz.io/solutions/cnapp ("ruthless risk prioritization", "prioritize the most critical risks").



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.").

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.").

122. As described in the preceding paragraphs, Wiz's CSP satisfies each limitation of claim 1 of the '685 patent, either literally or under the doctrine of equivalents.

123. The above examples of how Wiz's CSP directly infringes claim 1 of the '685 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 '685 patent, additional claims of the '685 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 '685 Patent

124. 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 '685 patent, including at least claim 1, literally and/or under the doctrine of equivalents pursuant to 35 U.S.C. § 271(b).

125. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '685 patent and its infringement thereof when the '685 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '685 patent's parent application, U.S. Patent Application No. 16/585,967 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '685 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '685 patent through a cease-and-desist letter, attached hereto as Exhibit 10. Accordingly, Wiz has had knowledge of the '685 patent since at least September 12, 2023. In any event, Wiz has had knowledge of the '685 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

126. 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 '685 patent, including at least claim 1 of the '685 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 '685 patent, including at least claim 1, and took deliberate steps to avoid learning of that infringement.

127. Wiz's specific intent to induce is demonstrated by its public instructions and other documentation. For example, in a video titled "Wiz for Vulnerability Management," posted by Wiz on August 11, 2023, Wiz specifically instructs users on how to use Wiz's platform to perform "agentless vulnerability scanning across every layer of your cloud environment," identify "the threats you need to pay attention to right now . . . and what resources are at risk," and "generate a vulnerability report" in a manner specifically intended to infringe at least claim 1 of the '685 patent. *See, e.g.*, https://www.youtube.com/watch?v=GP0NWZa_7vk at 0:05, 1:50, 2:00 ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023); *see also*

https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

(c) Contributory Infringement of the '685 Patent

128. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '685 patent and its infringement thereof when the '685 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '685 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '685 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '685 patent through a cease-and-desist letter, attached hereto as Exhibit 10. In any event, Wiz has had knowledge of the '685 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

129. 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 '685 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 '685 patent. Wiz has contributorily infringed and continues to contribute to the infringement of one or more claims of the '685 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.

130. Wiz's CSP, or any further component parts thereof, is not a staple article of commerce and has no substantial non-infringing use. On information and belief, Wiz's CSP cannot operate without incorporating technology claimed by the claims of the '685 patent. Specifically, as described above, Wiz's user guides, instructions, sales-related material, and/or other supporting documentation state that Wiz's CSP establishes an interface between a client environment and security component using an API(s), which it uses to identify a virtual disk in a client environment, receives an identification of the location of the virtual disk when it performs a query, generates a snapshot of the virtual disk using snapshot technology, analyzes the snapshot to detect vulnerabilities, and reports the vulnerabilities prioritized based risk, as claimed in the claims of the '685 patent. *See, e.g.*, Exhibit 4 at 1-2; Exhibit 5 at 11-23; Exhibit 6. Its documentation do not advertise or otherwise suggest that Wiz's CSP is a staple article of commerce or has a substantial non-infringing use. *See generally* Exhibit 5; Exhibit 6. Furthermore, when used as shown in Wiz's documentation, Wiz's CSP directly infringes claims of the '685 patent as described above in Paragraphs 110-123.

(d) *Willful Infringement of the '685 Patent*

131. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '685 patent and its infringement thereof when the '685 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '685 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '685 patent. Furthermore, on September 12, 2023, Orca notified

Wiz of its infringement of the '685 patent through a cease-and-desist letter, attached hereto as Exhibit 10. In any event, Wiz has had knowledge of the '685 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

132. 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.

133. 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.

134. 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 IV
(INFRINGEMENT OF THE '809 PATENT)

135. Orca incorporates all other allegations in this Amended Complaint.

136. The '809 patent is entitled "Techniques for Securing Virtual Machines by Application Existence Analysis" and was duly and legally issued on August 15, 2023. A true and correct copy of the '809 patent is attached hereto as Exhibit 8.

137. Orca is the owner of all rights, title, and interest in the '809 patent.

138. The '809 patent is valid and enforceable.

139. The inventions claimed in the '809 patent improved on prior art cloud security systems and methods by, *inter alia*, determining 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 the snapshot, 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 a plurality of potential cyber vulnerabilities. *See, e.g.*, '809 patent at cls. 1-23. This analysis of instantiated virtual cloud assets using snapshots of a virtual disk to match installed applications with known vulnerable applications including was not well understood, routine, or conventional. It is an inventive concept that allows, for example, implementation of vulnerability management and security assessment across running virtual cloud assets without the burdensome installation of agents or interaction with particular virtual machines. This increases speed of detection for potential cyber vulnerabilities and reduces costs associated with such detection, including the cost of licensing, deployment, integration, training, and support. Furthermore, the claims of the '809 patent recite inventive concepts for correlating potential cyber vulnerabilities with a network location of virtual cloud assets to determine the risk of the virtual cloud assets. *See, e.g.*, *id.* Correlating cyber vulnerabilities with a network location of virtual cloud assets through agentless analysis was not well understood, routine, or conventional, and improves on prior art techniques by taking into consideration the criticality of a virtual cloud asset in the organization based on other accessible assets or an external network.

(a) *Direct Infringement of the '809 Patent*

140. Wiz, without authorization, directly infringes one or more claims of the '809 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 '809 patent.

141. Claim 1 of the '809 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 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 a plurality of potential cyber vulnerabilities;

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

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;

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

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

142. On information and belief, Wiz practices each and every limitation of claim 1 of the '809 patent by and through the use of Wiz's CSP and/or other similar products or services for Wiz's clients or customers.

143. 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").

144. 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" or services provided by AWS, GCP, and Azure, among other cloud computing environments.

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").

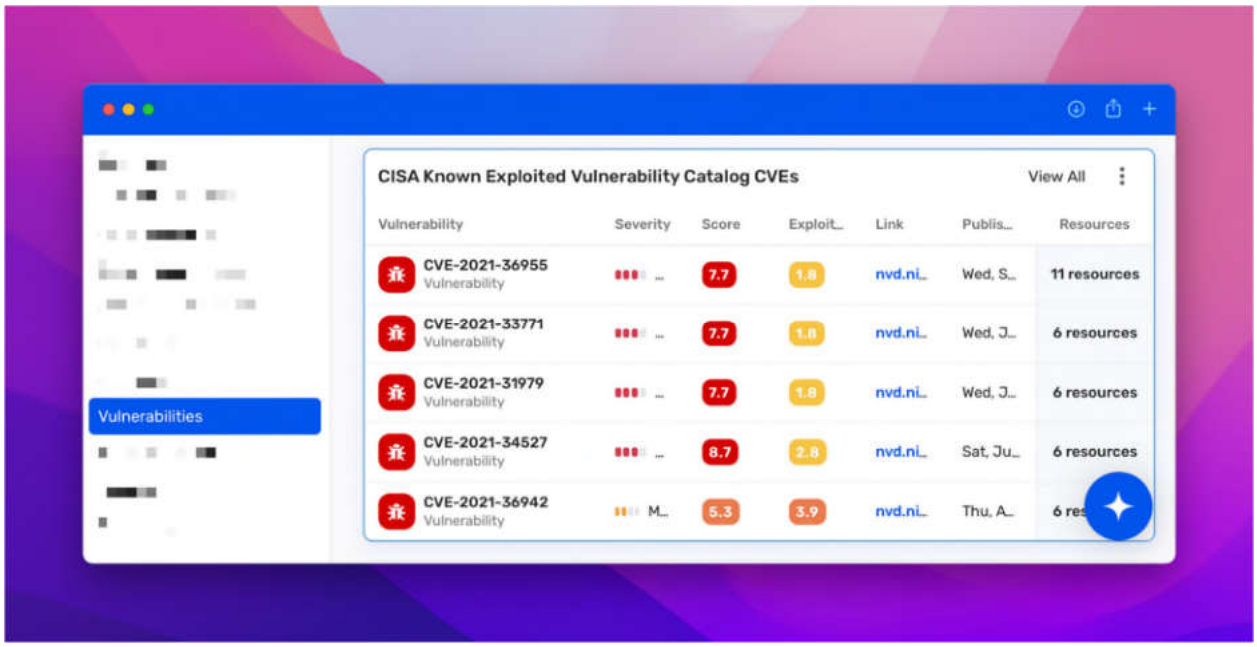
145. Claim 1 further recites "accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the virtual disk . . . ." Wiz performs this step by, for example, accessing the snapshot of a virtual disk in order to "analyze[] [the] operating 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).

146. 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.

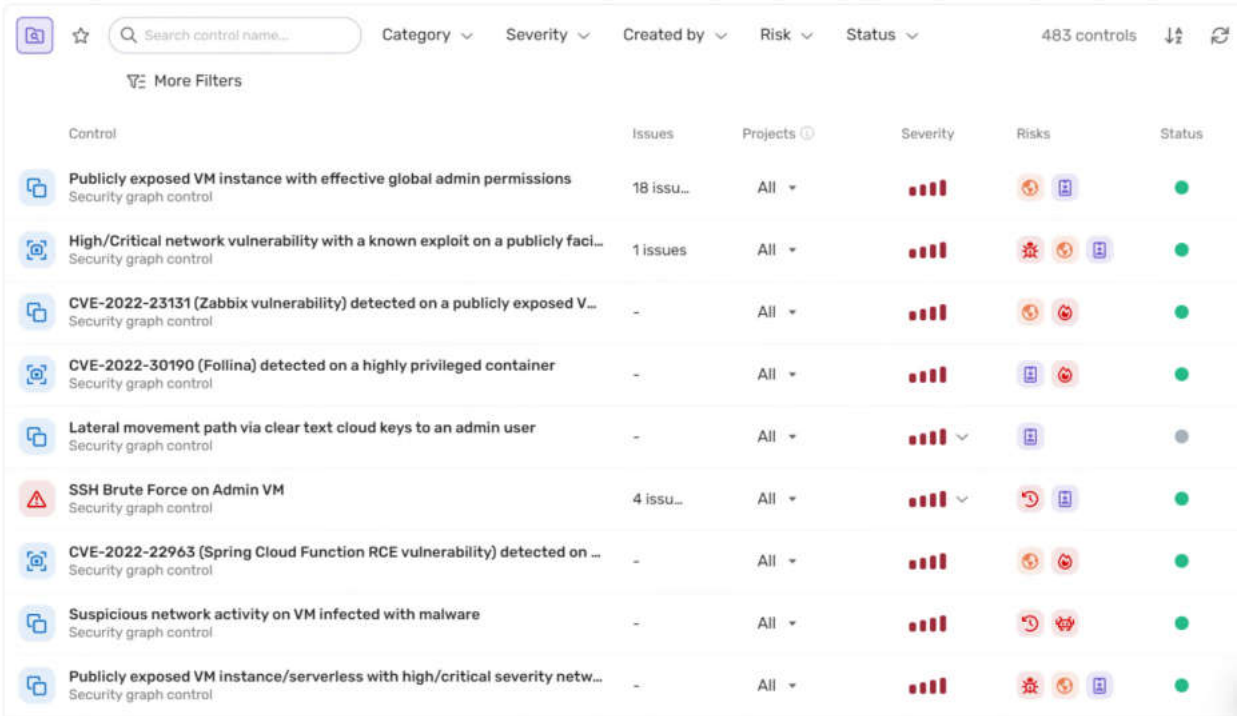
https://www.wiz.io/solutions/vulnerability-management.

147. Claim 1 further recites "determining, based on the matching, an existence of a plurality of potential cyber vulnerabilities . . . ." Wiz practices this step because, for example, it

uses results of matching installed applications 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.

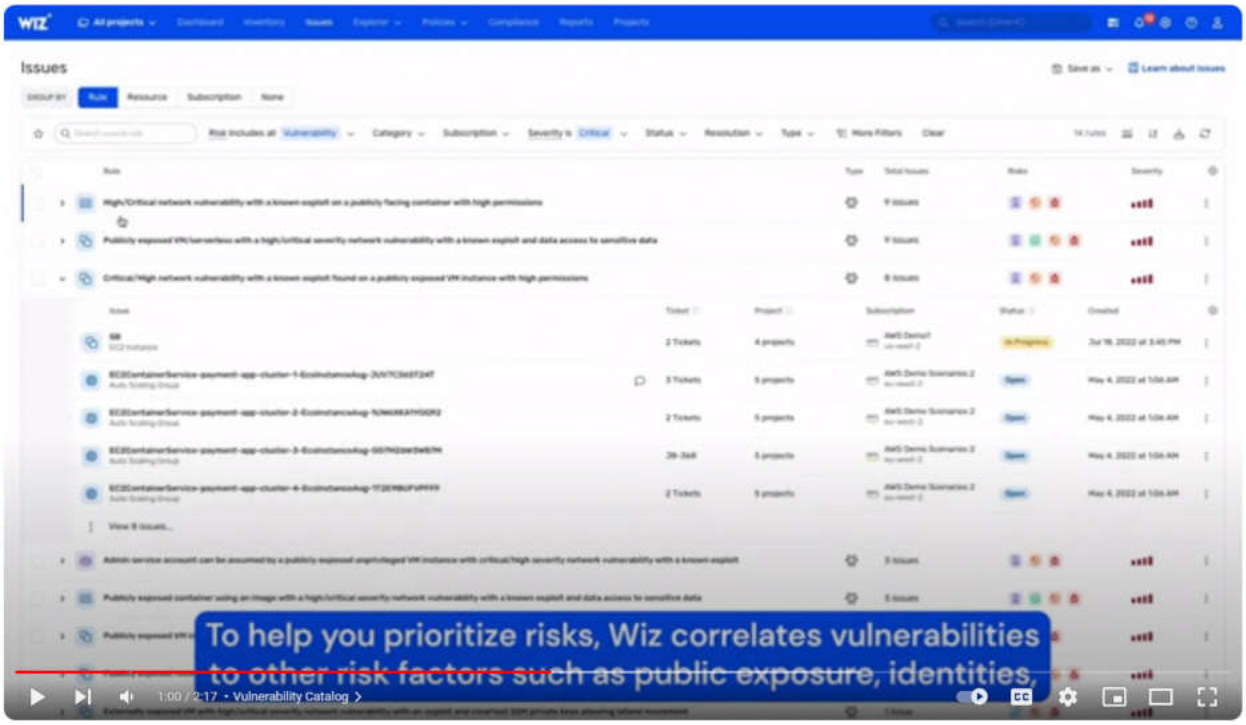


See id.

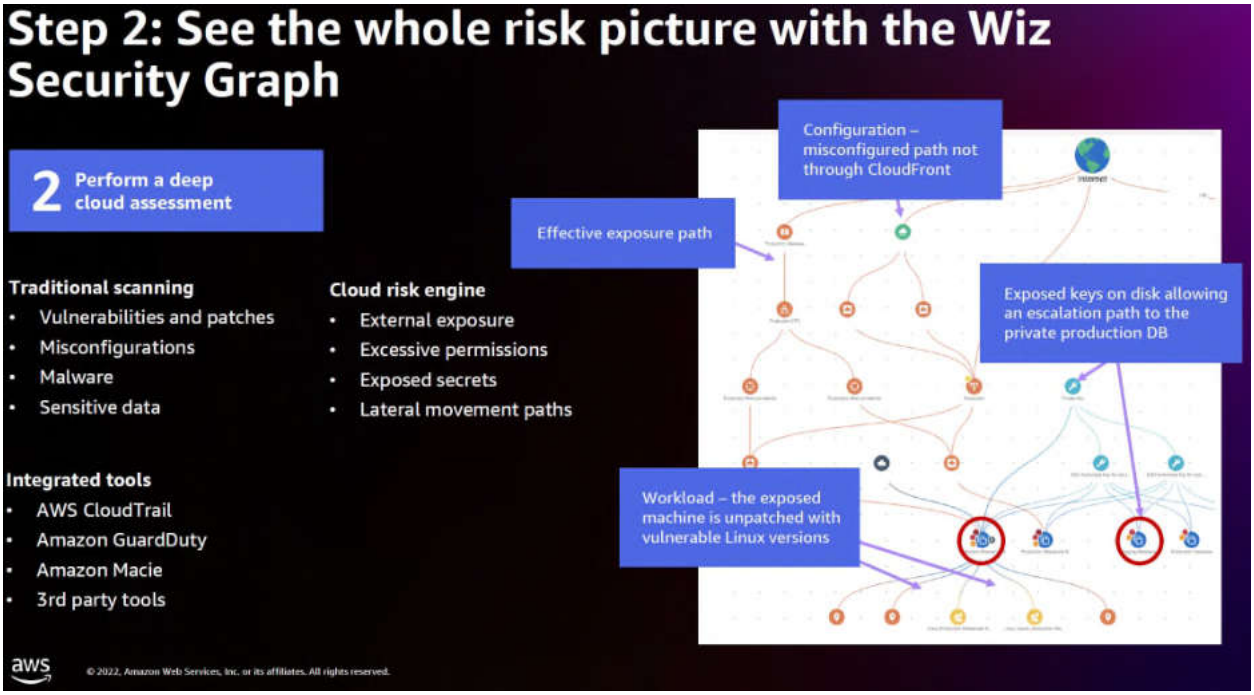


See also Exhibit 5 at 27.

148. Claim 1 further recites "correlating the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset . . . ." Wiz practices this step because, for example, Wiz "correlates vulnerabilities to other risk factors such as public exposure."



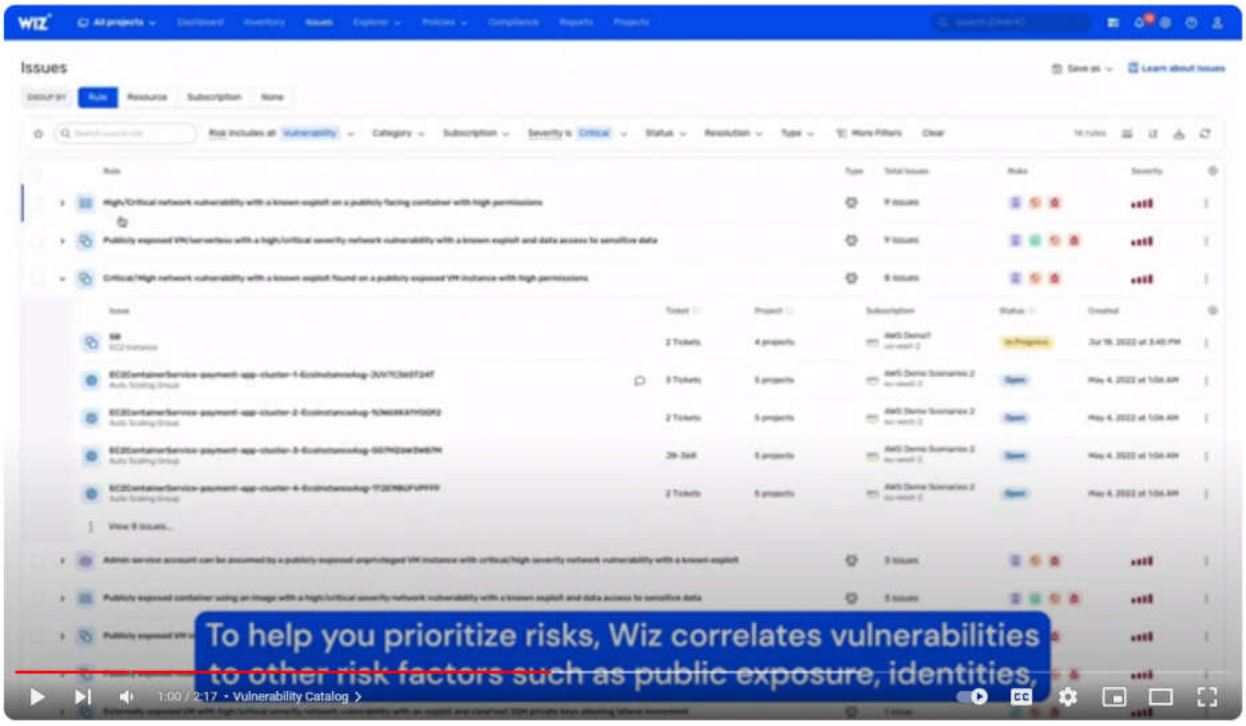
https://www.youtube.com/watch?v=GP0NWZa_7vk at 1:00.



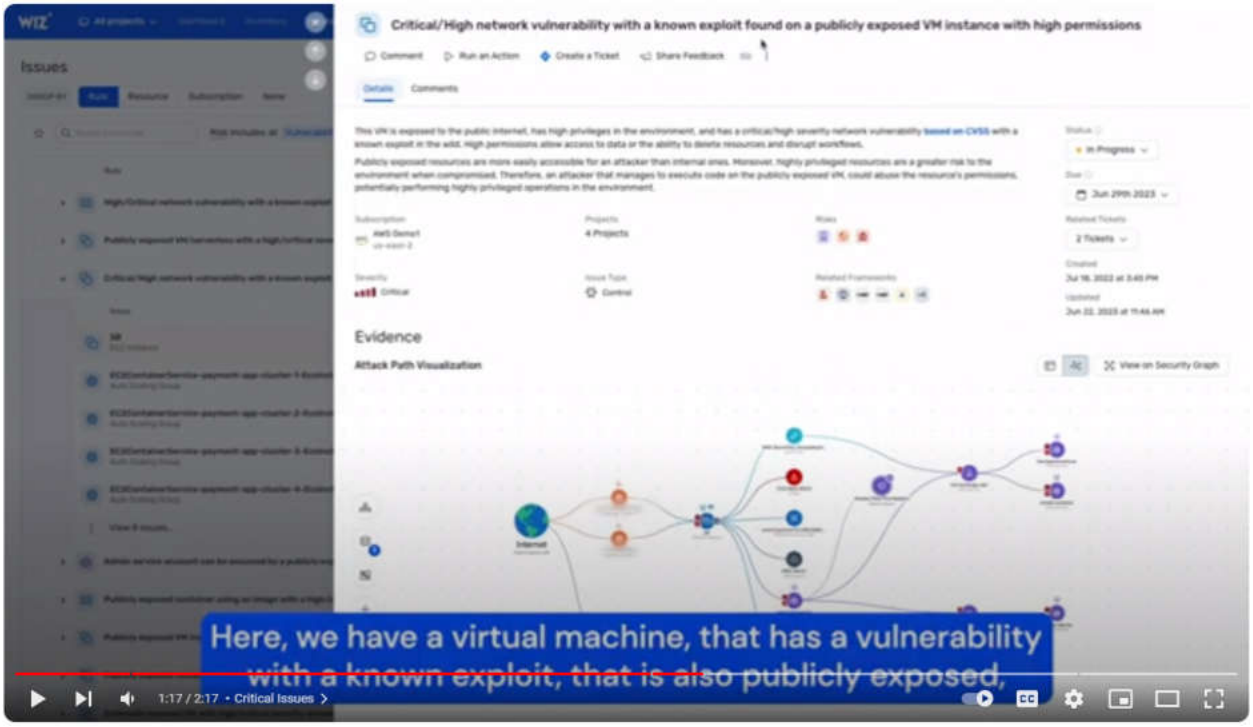
See Exhibit 5 at 14, 11 (showing vulnerabilities corresponding to network locations of virtual cloud assets).

See also Exhibit 6 at 3 (showing vulnerability correlated with a Jenkins container in the network).

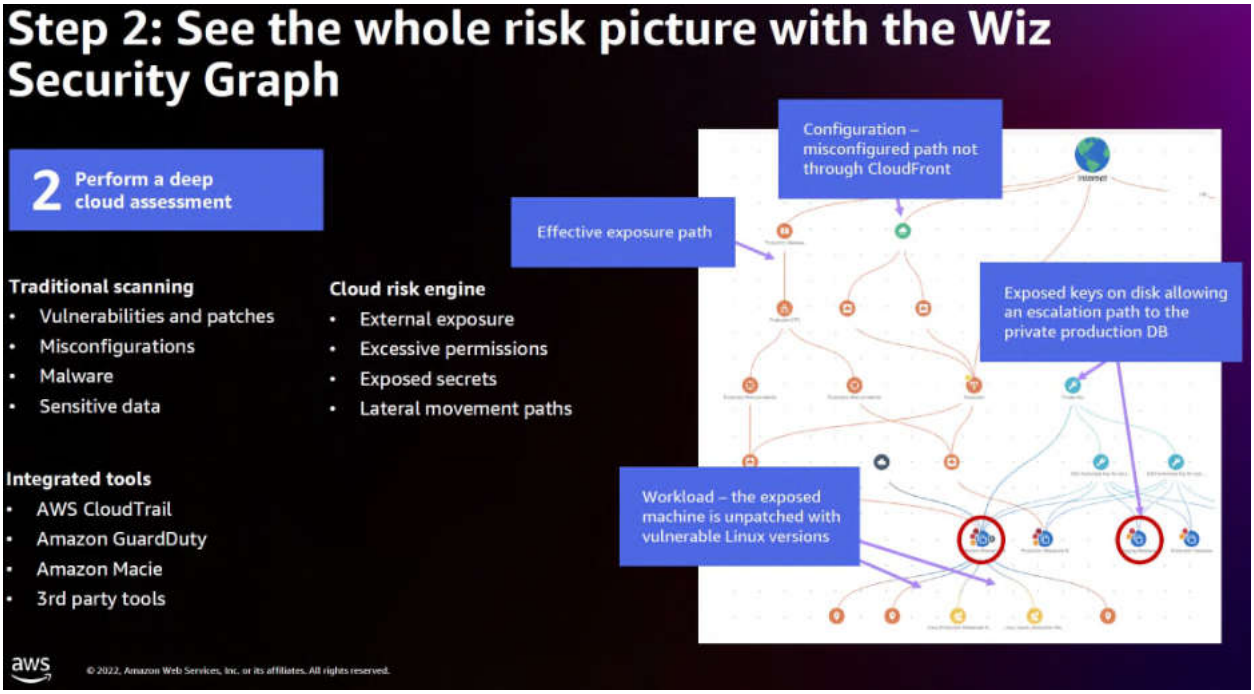
149. Claim 1 further recites "using the determined plurality of potential cyber vulnerabilities and the network location of the protected virtual cloud asset to determine a risk of the protected virtual cloud asset to the cloud computing environment . . . ." Wiz practices this step because, for example, Wiz determines the risk of virtual cloud assets to the cloud computing environment based on the determined cyber vulnerabilities and network locations of the virtual cloud asset.



https://www.youtube.com/watch?v=GP0NWZa_7vk at 1:00.

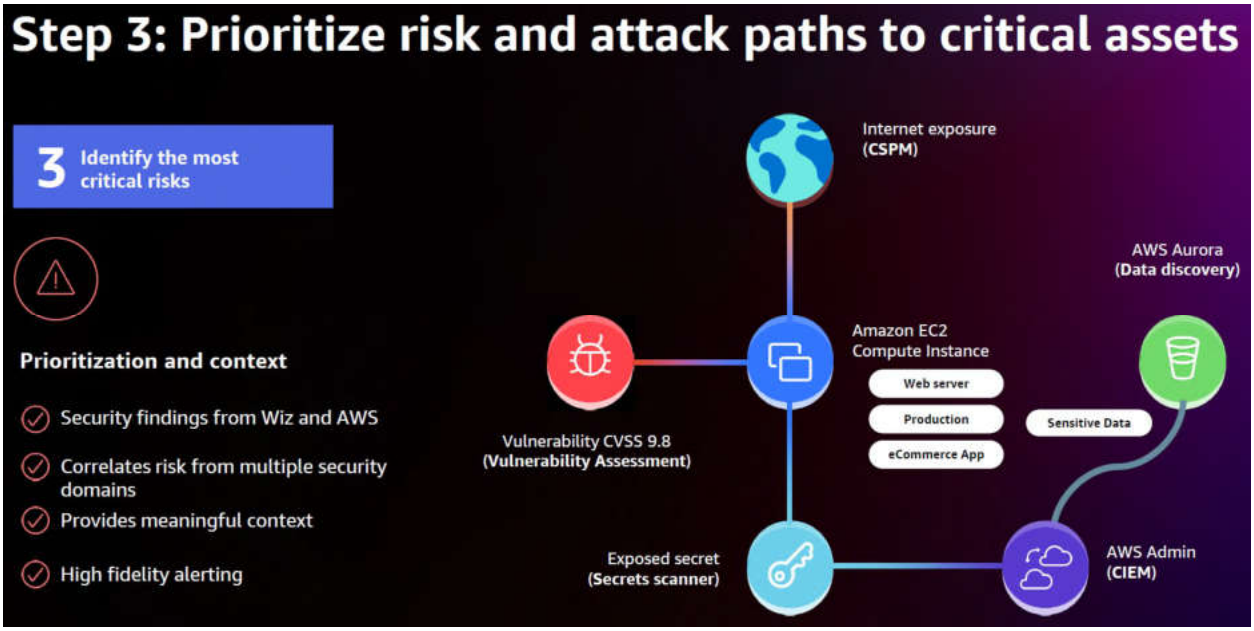


*Id.*at 1:17.



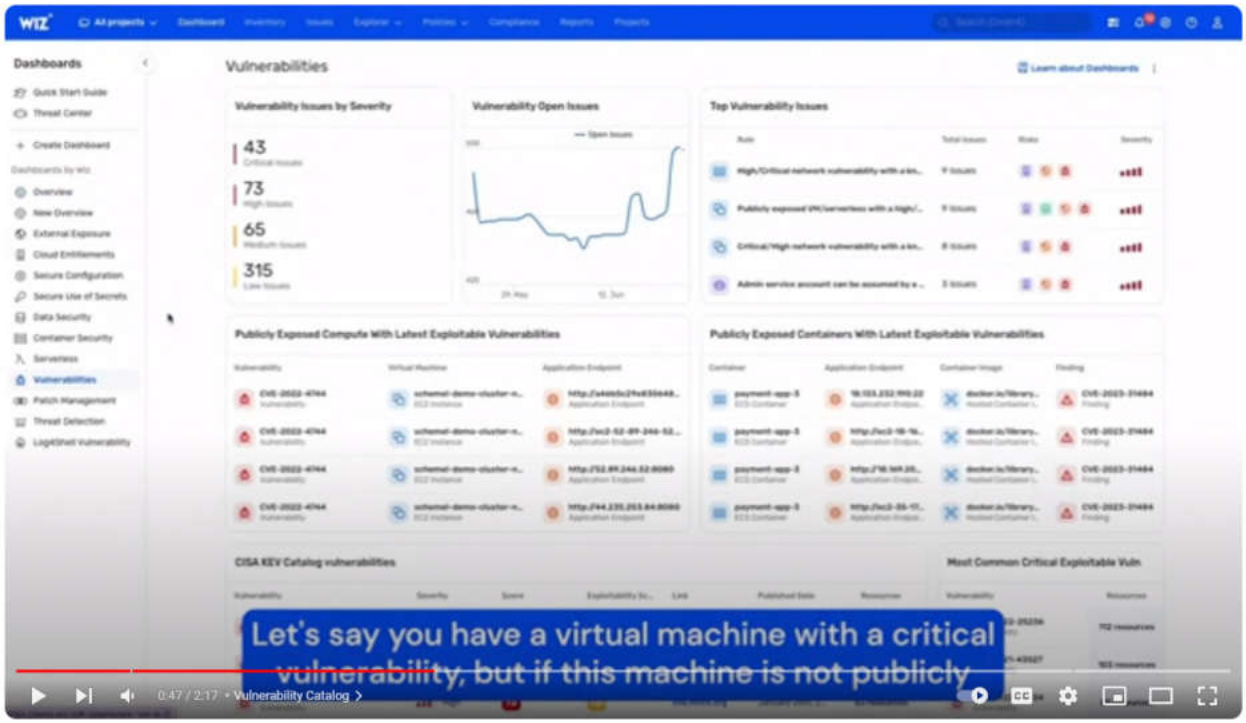
See Exhibit 5 at 14, 11 (showing vulnerabilities corresponding to network locations of virtual cloud assets). Wiz "[p]riotize[s] risk and attack paths to critical assets" within the cloud computing

environment based on detected vulnerabilities and the network locations, including "external exposure."

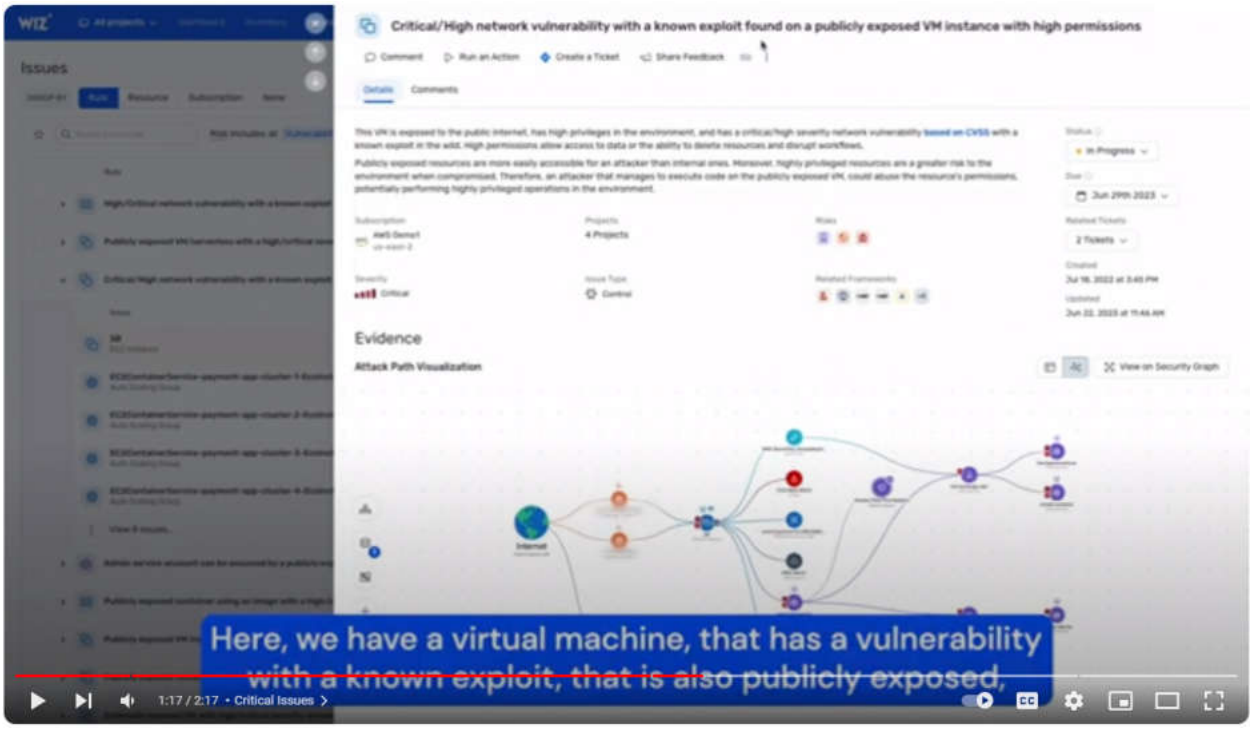


See, e.g., *id.* at 17; Exhibit 6 at 3 ("Scan for vulnerable and unpatched operating systems, installed software, and code libraries in your workloads prioritized by risk."); https://www.wiz.io/solutions/cnapp ("The Wiz Security Graph immediately uncovers the toxic combinations that create attack paths in your cloud and eliminates the need for manual work of sifting through and analyzing siloed alerts."); https://www.wiz.io/solutions/vulnerability-management ("Contextual Risk-Based Prioritization Reduce alert fatigue by correlating vulnerabilities with multiple risk factors, including external exposure, cloud entitlements, secrets, misconfigurations, malware, and more, to surface the vulnerabilities that should be prioritized.").

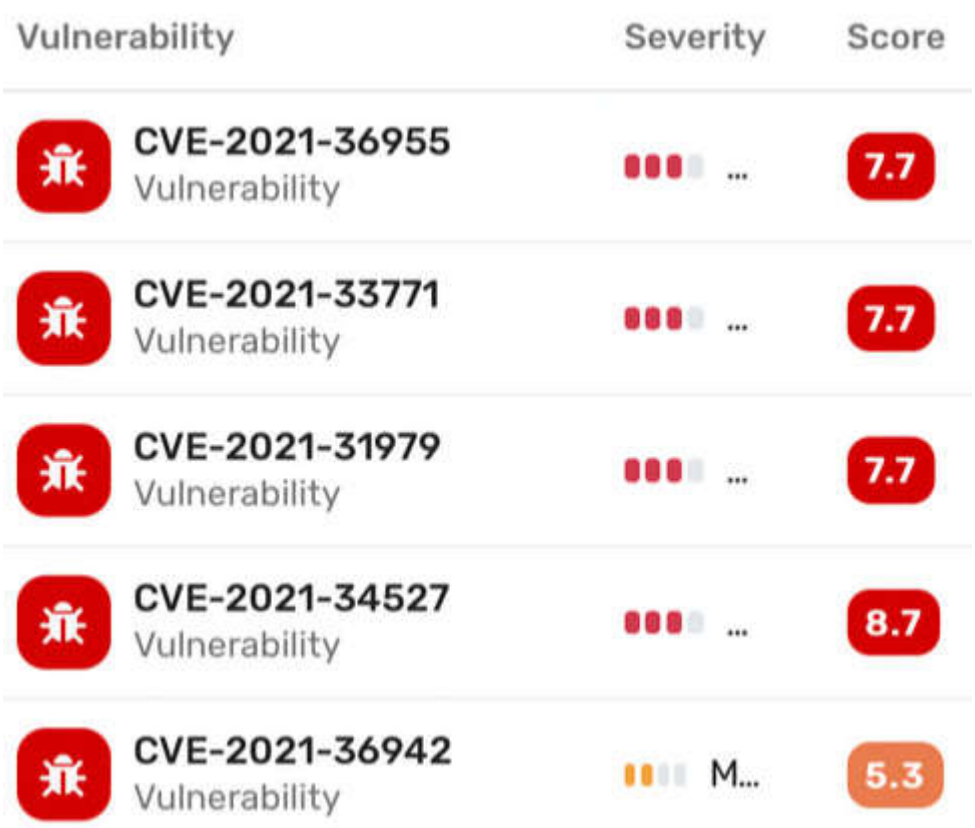
150. Claim 1 further recites "prioritizing, by the determined risk, the plurality of potential cyber vulnerabilities . . . ." Wiz performs this step by, for example, "prioritiz[ing] and mitigat[ing] the critical risks." *See* https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz. Wiz also prioritizes cyber vulnerabilities based on determined risk as shown below.



https://www.youtube.com/watch?v=GP0NWZa_7vk at 0:47.

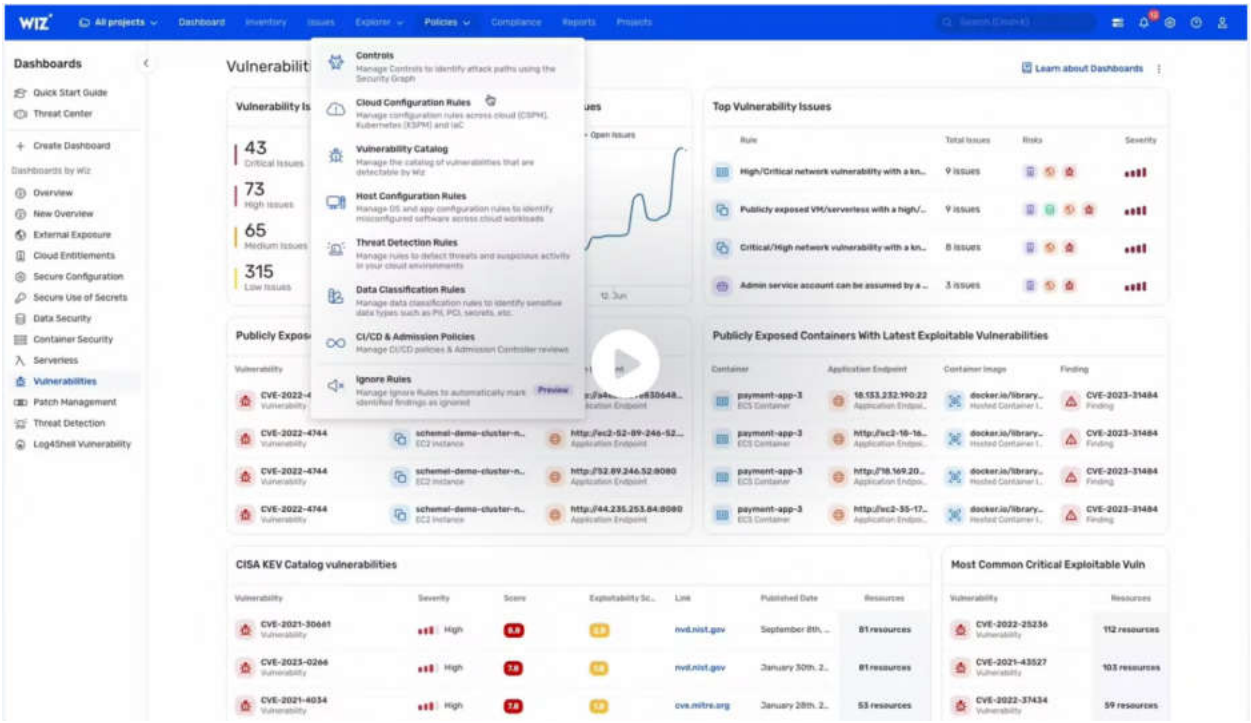


Id. at 1:17.



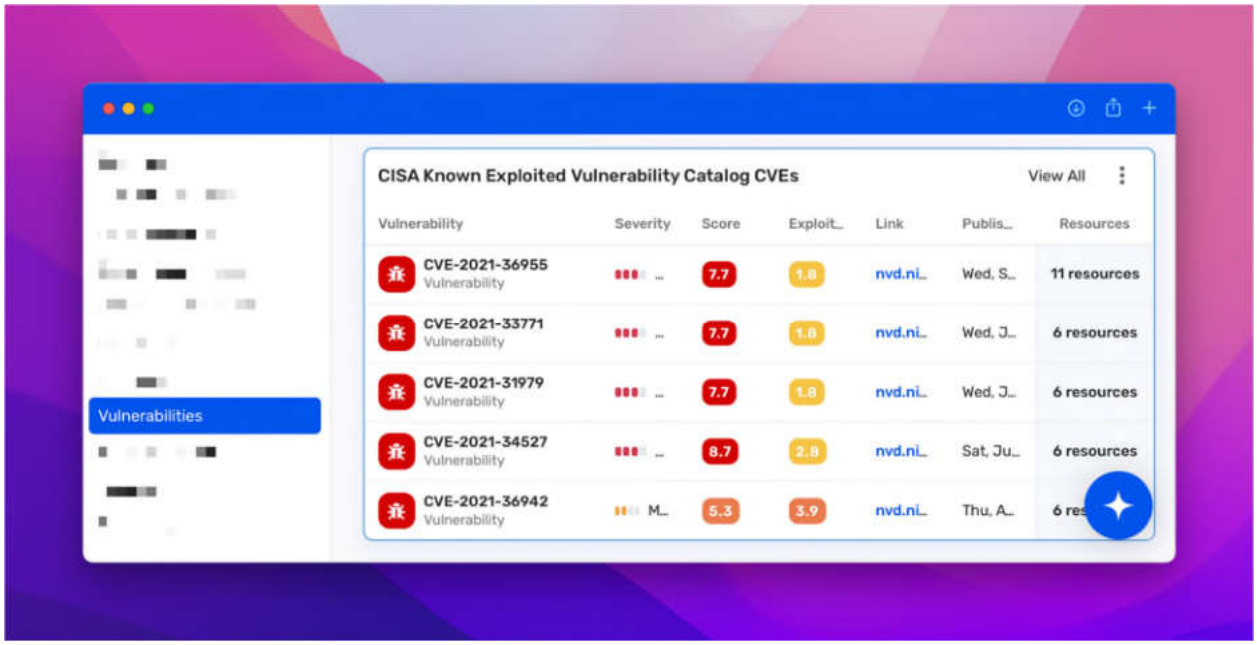
https://www.wiz.io/solutions/vulnerability-management; *see also* Exhibit 5 at 27 (same).

https://www.wiz.io/solutions/cnapp; *see also* Exhibit 5 at 17, 27.

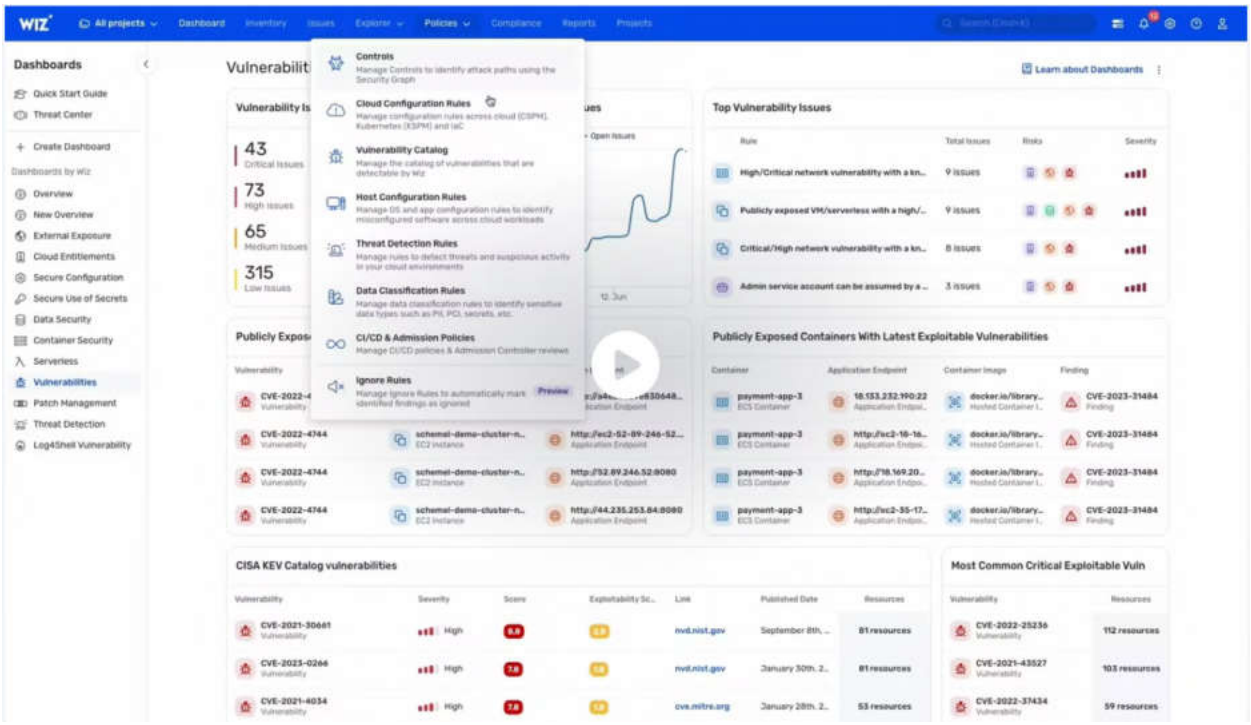


https://www.wiz.io/solutions/vulnerability-management.

151. Claim 1 further recites "reporting the determined plurality of potential cyber vulnerabilities as alerts prioritized according to the determined risk." Wiz performs this step by, for example, reporting "Vulnerabilit[ies]," prioritized according to risk.



See https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-kev-with-wiz; *see also* Exhibit 5 at 27 (prioritizing vulnerabilities).



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

152. As described in the preceding paragraphs, Wiz practices each limitation of claim 1 of the ’809 patent, either literally or under the doctrine of equivalents.

153. The above examples of how Wiz directly infringes claim 1 of the ’809 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 ’809 patent, additional claims of the ’809 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 '809 Patent

154. 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 '809 patent, including at least claim 1, literally and/or under the doctrine of equivalents pursuant to 35 U.S.C. § 271(b).

155. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '809 patent and its infringement thereof when the '809 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '809 patent's parent application, U.S. Patent Application No. 16/585,967 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '809 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '809 patent through a cease-and-desist letter, attached hereto as Exhibit 10. Accordingly, Wiz has had knowledge of the '809 patent since at least September 12, 2023. In any event, Wiz has had knowledge of the '809 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

156. 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 '809 patent, including at least claim 1 of the '809 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 '809 patent, including at least claim 1, and took deliberate steps to avoid learning of that infringement.

157. Wiz's specific intent to induce is demonstrated by its public instructions and other documentation. For example, in a video titled "Wiz for Vulnerability Management," posted by Wiz on August 11, 2023, Wiz specifically instructs users on how to use Wiz's platform to perform "agentless vulnerability scanning across every layer of your cloud environment," identify "the threats you need to pay attention to right now . . . and what resources are at risk," and "generate a vulnerability report" in a manner specifically intended to infringe at least claim 1 of the '809 patent. *See, e.g.*, https://www.youtube.com/watch?v=GP0NWZa_7vk at 0:05, 1:50, 2:00 ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023); *see also* https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

(c) *Contributory Infringement of the '809 Patent*

158. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '809 patent and its infringement thereof when the '809 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '809 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '809 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '809 patent through a cease-and-desist letter, attached hereto as

Exhibit 10. In any event, Wiz has had knowledge of the '809 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

159. 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 '809 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 '809 patent. Wiz has contributorily infringed and continues to contribute to the infringement of one or more claims of the '809 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.

160. Wiz's CSP, or any further component parts thereof, is not a staple article of commerce and has no substantial non-infringing use. On information and belief, Wiz's CSP cannot operate without incorporating technology claimed by the claims of the '809 patent. Specifically, as described above, Wiz's user guides, instructions, sales-related material, and/or other supporting documentation state that Wiz's CSP is intended to be used to perform agentless scanning of virtual assets in a client environment through snapshot scanning using an API provided by the cloud environment, determine a location of a snapshot of a virtual disk of a virtual asset and access the snapshot, analyze the snapshot by matching installed applications to a known list of vulnerabilities (such as vulnerabilities in the CISA KEV Catalog), determine potential vulnerabilities based on the matching and correlate those vulnerabilities with a network location of the virtual asset, and to prioritize and report potential vulnerabilities based on their determined risk, as claimed in the claims of the '809 patent. *See, e.g.*, Exhibit 4 at 1-2; Exhibit 5 at 11-23; Exhibit 6; https://www.wiz.io/blog/detect-and-prioritize-cisa-known-exploited-vulnerabilities-

kev-with-wiz. Its documentation do not advertise or otherwise suggest that Wiz's CSP is a staple article of commerce or has a substantial non-infringing use. *See generally* Exhibit 5; Exhibit 6. Furthermore, when used as shown in Wiz's documentation, Wiz's CSP directly infringes claims of the '809 patent as described above in Paragraphs 140-153.

(d) Willful Infringement of the '809 Patent

161. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '809 patent and its infringement thereof when the '809 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '809 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '809 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '809 patent through a cease-and-desist letter, attached hereto as Exhibit 10. In any event, Wiz has had knowledge of the '809 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

162. 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.

163. 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.

164. 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 V
(INFRINGEMENT OF THE '926 PATENT)

165. Orca incorporates all other allegations in this Amended Complaint.

166. The '926 patent is entitled "Techniques for Securing Virtual Machines by Analyzing Data for Cyber Threats" and was duly and legally issued on August 29, 2023. A true and correct copy of the '926 patent is attached hereto as Exhibit 9.

167. Orca is the owner of all rights, title, and interest in the '926 patent.

168. The '926 patent is valid and enforceable.

169. The inventions claimed in the '926 patent improved on prior art cloud security systems and methods by, *inter alia*, accessing the snapshot of at least one virtual disk, analyzing the snapshot to determine the existence of potential cyber threats based on data stored on the virtual disk, determining a risk associated with each of the determined potential cyber threats, and prioritizing the potential cyber threats based on the determined risk. *See, e.g.*, '926 patent at cls. 1-15. This snapshot-based analysis for potential cyber threats was not well understood, routine, or conventional. It is an inventive concept that allows, for example, practical implementations of agentless inspection, analysis, and protection of virtual cloud assets in cloud computing environments because, among other things, sensitive data stored on virtual disks can be analyzed without requiring any interaction and/or information from an online virtual asset, unlike agent-based or network scanner solutions. This improves ease of implementation and reduces costs,

including cost of licensing, deployment, integration, training, and support. Furthermore, the snapshot analysis provided in the claims of the '926 patent achieved more comprehensive detection and prioritization of potential cyber threats because it allowed for myriad kinds of data stored on virtual assets in a cloud computing environment to be analyzed for related potential cyber threats without requiring an agent or interaction with running virtual assets.

(a) *Direct Infringement of the '926 Patent*

170. Wiz, without authorization, directly infringes one or more claims of the '926 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 '926 patent.

171. Claim 1 of the '926 patent recites:

> 1. A method for securing virtual cloud assets against cyber threats in a cloud computing environment, the method comprising:
>
> receiving a request to scan a protected virtual cloud asset in the cloud computing environment;
>
> locating, using an API or service provided by the cloud computing environment, a snapshot of at least one virtual disk of the protected virtual cloud asset;
>
> accessing, 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 to determine the existence of a plurality of potential cyber threats, each cyber threat based on data stored on the virtual disk, wherein the data includes at least one of:

unencrypted sensitive data,

unencrypted system credentials,

weak passwords,

weak encryption schemes,

disabled Address Space Layout Randomization,

boot record manipulation,

suspicious definitions,

services to be run on startup,

personally identifiable information,

data in application logs indicating that the protected virtual cloud asset accessed personally identifiable information,

data in application logs indicating that the protected virtual cloud asset accessed a computer containing personally identifiable information, or

at least one change in at least one area of the virtual disk, as compared to an earlier point in time;

determining a risk associated with each of the determined plurality of potential cyber threats;

prioritizing the potential cyber threats associated with the protected virtual cloud asset based on the determined risk associated with each of the plurality of potential cyber threats; and

reporting at least some of the determined plurality of potential cyber threats as alerts prioritized according to their associated risks.

172. On information and belief, Wiz practices each and every limitation of claim 1 of the '926 patent by and through the use of Wiz's CSP and/or other similar products or services for Wiz's clients or customers.

173. The preamble of claim 1 recites "[a] method for securing virtual cloud assets against cyber threats 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 threats in cloud computing environments and secure virtual cloud assets within those environments against said threats. *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").

174. Claim 1 further recites "receiving a request to scan a protected virtual cloud asset in the cloud computing environment . . . ." Wiz's public presentations and technical documentation confirm that Wiz practices this step by, for example, receiving requests to perform an "agentless scan" of "workloads" in an organization's cloud computing environment.

See Exhibit 5 at 13; Exhibit 6 (supported cloud computing platforms include AWS, Azure, and GCP). Wiz states that in response to the requests, Wiz "connects within minutes with zero impact on resource or workload performance" and "builds an inventory of every technology running in your cloud and delivers complete visibility into every layer of your cloud stack." *See* https://www.datocms-assets.com/75231/1682034689-wiz-solution-brief-march-2023.pdf.

175. Claim 1 further recites "locating, using an API or service provided by the cloud computing environment, a snapshot of at least one virtual disk of the protected virtual cloud asset . . . ." Wiz's public presentations and technical documentation confirm that Wiz practices this step by, for example, using Wiz's CSP to perform "agentless scanning via API" provided by AWS, GCP, and Azure, among other cloud computing environments.

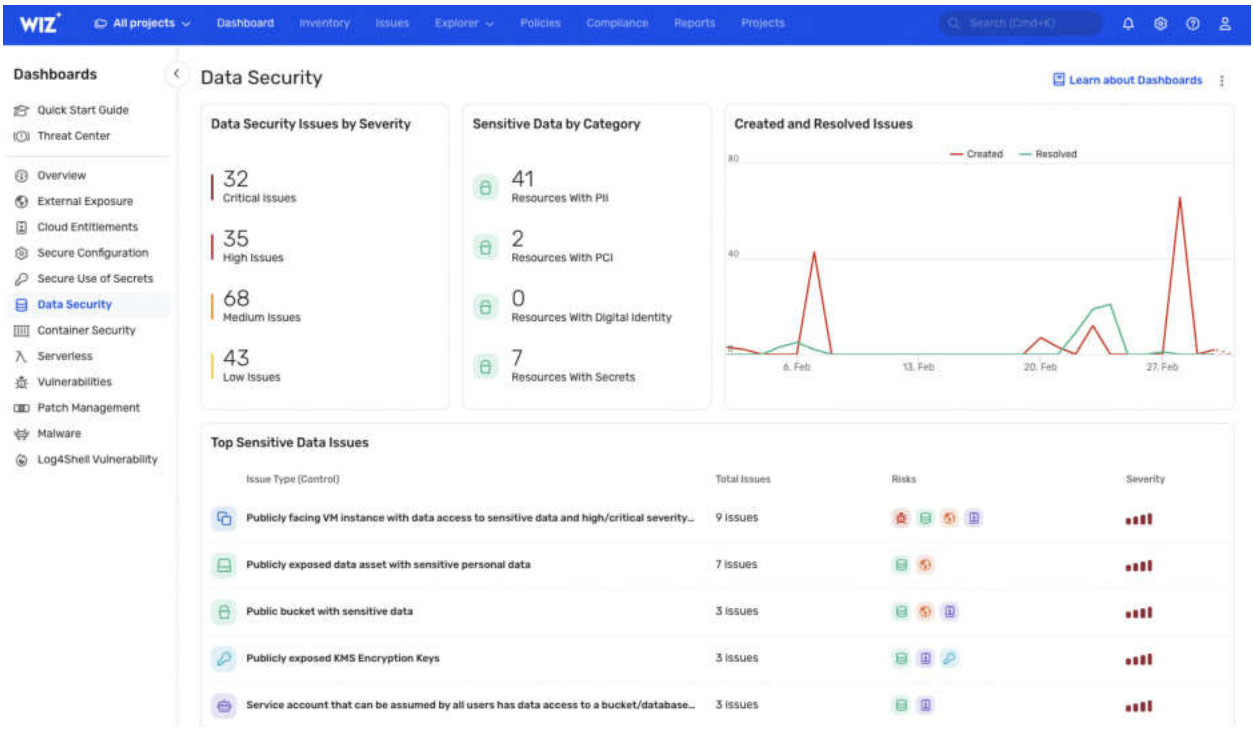
See Exhibit 5 at 13 ("Full visibility in minutes . . . without agents"); Exhibit 6 (supported cloud computing platforms include AWS, Azure, and GCP). Wiz's technical documentation confirms that its agentless scanning includes "snapshot scanning" of virtual cloud assets, wherein Wiz's CSP "takes a snapshot of each VM system volume and analyzes its operating system, application layer, and data layer statistically 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").

176. Claim 1 further recites "accessing, 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. 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).

177. Claim 1 further recites "analyzing the snapshot of the at least one virtual disk to determine the existence of a plurality of potential cyber threats, each cyber threat based on data stored on the virtual disk, wherein the data includes at least one of: unencrypted sensitive data, unencrypted system credentials, weak passwords, weak encryption schemes, disabled Address Space Layout Randomization, boot record manipulation, suspicious definitions, services to be run on startup, personally identifiable information, data in application logs indicating that the protected virtual cloud asset accessed personally identifiable information, data in application logs indicating that the protected virtual cloud asset accessed a computer containing personally identifiable information, or at least one change in at least one area of the virtual disk, as compared to an earlier point in time . . . ." Wiz practices this step by, for example, analyzing the snapshot for threats embodied in data stored on the virtual disk like "personally identifiable information" and "weak passwords." *See, e.g.*, https://www.wiz.io/solutions/ciem ("[I]dentify potential risks associated with exposed secrets, access keys, credentials, or weak passwords."); https://www.wiz.io/solutions/dspm ("Discover your sensitive data");

https://www.wiz.io/blog/hardening-your-cloud-environment-against-lapsus-like-threat-actor ("With Wiz, you can easily locate . . . particularly weak or empty passwords").

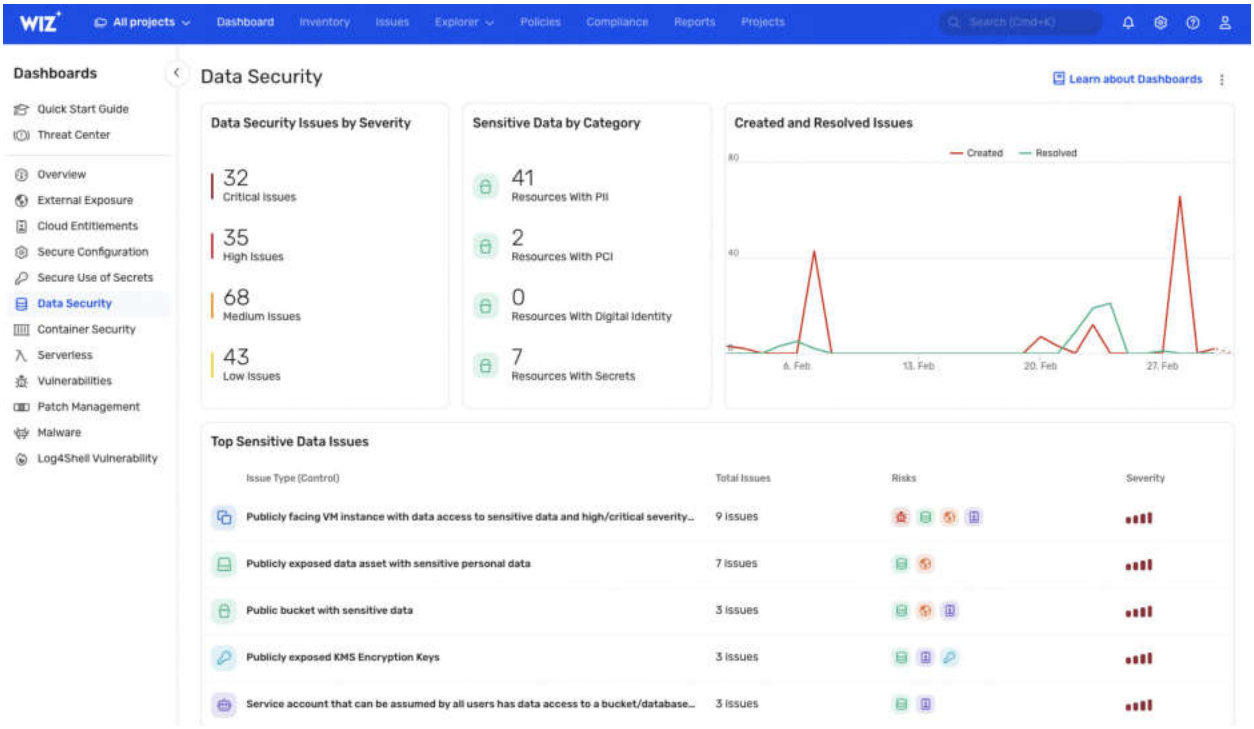
178. Claim 1 further recites "determining a risk associated with each of the determined plurality of potential cyber threats . . . ." Wiz practices this step by, for example, determining risks associated with data security and "sensitive data issues."



https://www.wiz.io/solutions/dspm ("Data risk prioritization Focus your teams on what is critical with a single prioritized queue of data issues ranked by severity and type"); *see also id.* ("With fully integrated DSPM, the Wiz Security Graph automatically alerts you when toxic combinations of risks create attack paths to your sensitive data so your teams can focus on the highest priority issues before they become breaches.").

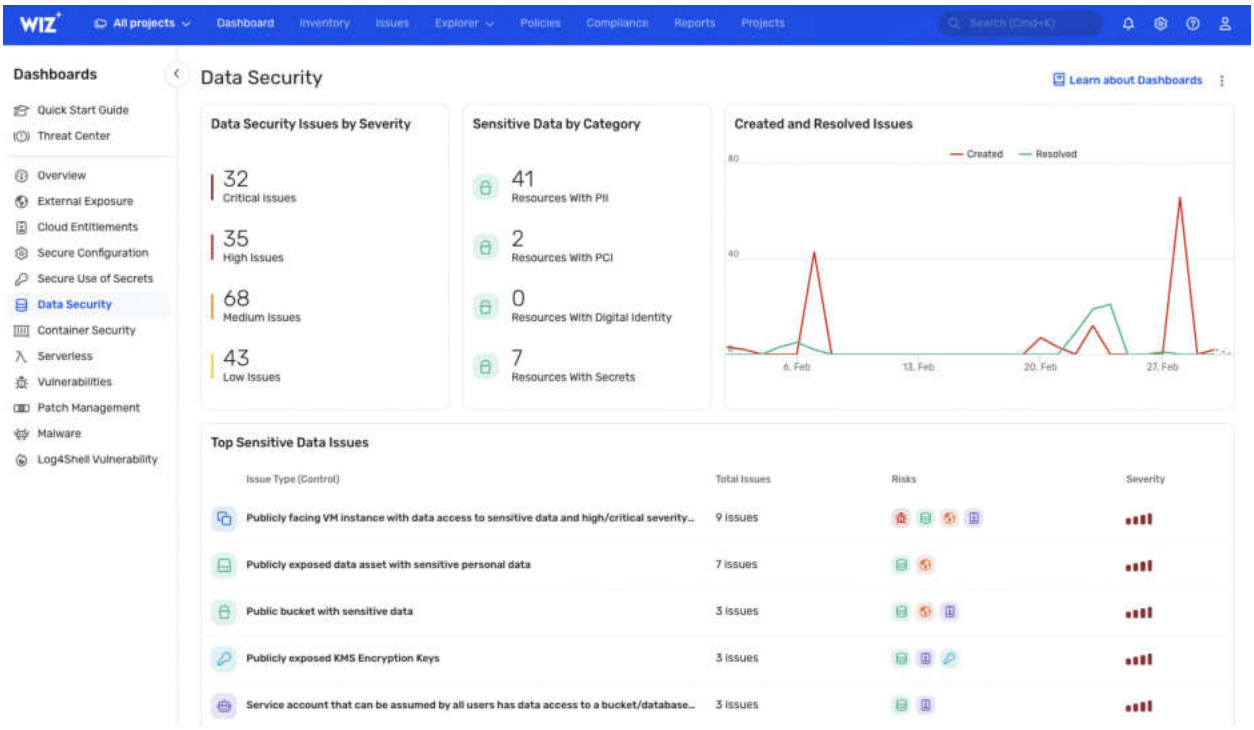
179. Claim 1 further recites "prioritizing the potential cyber threats associated with the protected virtual cloud asset based on the determined risk associated with each of the plurality of

potential cyber threats . . . ." Wiz practices this step by, for example, prioritizing data security issues associated with virtual cloud assets based on risk shown in its "Data Security" dashboard:



https://www.wiz.io/solutions/dspm ("Data risk prioritization Focus your teams on what is critical with a single prioritized queue of data issues ranked by severity and type").

180. Claim 1 further recites "reporting at least some of the determined plurality of potential cyber threats as alerts prioritized according to their associated risks." Wiz practices this step by, for example, reporting at least some of the determined plurality of potential cyber threats as alerts as shown in its "Data Security" dashboard that displays a "prioritized queue of data issues ranked by severity and type."



https://www.wiz.io/solutions/dspm ("Data risk prioritization Focus your teams on what is critical with a single prioritized queue of data issues ranked by severity and type").

181. As described in the preceding paragraphs, Wiz practices each limitation of claim 1 of the '926 patent, either literally or under the doctrine of equivalents.

182. The above examples of how Wiz directly infringes claim 1 of the '926 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 '926 patent, additional claims of the '926 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 '926 Patent

183. 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 '926 patent,

including at least claim 1, literally and/or under the doctrine of equivalents pursuant to 35 U.S.C. § 271(b).

184. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '926 patent and its infringement thereof when the '926 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '926 patent's parent application, U.S. Patent Application No. 16/585,967 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '926 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '926 patent through a cease-and-desist letter, attached hereto as Exhibit 10. Accordingly, Wiz has had knowledge of the '926 patent since at least September 12, 2023. In any event, Wiz has had knowledge of the '926 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

185. 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 '926 patent, including at least claim 1 of the '926 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 '926 patent, including at least claim 1, and took deliberate steps to avoid learning of that infringement.

186. Wiz's specific intent to induce is demonstrated by its public instructions and other documentation. For example, in a video titled "Wiz for Vulnerability Management," posted by Wiz on August 11, 2023, Wiz specifically instructs users on how to use Wiz's platform to perform "agentless vulnerability scanning across every layer of your cloud environment," identify "the threats you need to pay attention to right now . . . and what resources are at risk," and "generate a vulnerability report" in a manner specifically intended to infringe at least claim 1 of the '926 patent. *See, e.g.*, https://www.youtube.com/watch?v=GP0NWZa_7vk at 0:05, 1:50, 2:00 ("Wiz for Vulnerability Management Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023); *see also* https://www.youtube.com/watch?v=a8l9zIQUoVI ("Wiz for CSPM Demo" (Aug. 11, 2023)) (last accessed Sept. 15, 2023).

(c) *Contributory Infringement of the '926 Patent*

187. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '926 patent and its infringement thereof when the '926 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '926 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '926 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '926 patent through a cease-and-desist letter, attached hereto as Exhibit 10. In any event, Wiz has had knowledge of the '926 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

188. 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 '926 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 '926 patent. Wiz has contributorily infringed and continues to contribute to the infringement of one or more claims of the '926 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.

189. Wiz's CSP, or any further component parts thereof, is not a staple article of commerce and has no substantial non-infringing use. On information and belief, Wiz's CSP cannot operate without incorporating technology claimed by the claims of the '926 patent. Specifically, as described above, Wiz's user guides, instructions, sales-related material, and/or other supporting documentation state that Wiz's CSP is intended to be used to receive requests to scan a virtual cloud asset in a cloud computing environment through agentless scanning using an API provided by the cloud environment, locate and access a snapshot of a virtual disk to analyze the snapshot for potential threats based on data stored on the virtual disk, and to prioritize and report potential threats based on their determined risk, as claimed in the claims of the '926 patent. *See, e.g.*, Exhibit 4 at 1-2; Exhibit 5 at 11-23; Exhibit 6. Its documentation do not advertise or otherwise suggest that Wiz's CSP is a staple article of commerce or has a substantial non-infringing use. *See generally* Exhibit 5; Exhibit 6. Furthermore, when used as shown in Wiz's documentation, Wiz's CSP directly infringes claims of the '926 patent as described above in Paragraphs 170-182.

(d) Willful Infringement of the '926 Patent

190. On information and belief, Wiz monitors Orca's patent portfolio and was aware of the '926 patent and its infringement thereof when the '926 patent issued or soon thereafter at least as a result of its collective pattern of efforts to copy Orca's technology and its patents as discussed above in Paragraphs 13-29. Additionally, Wiz by and through its patent prosecution counsel had knowledge of the '926 patent's parent application, U.S. Patent Application No. 16/585,967, 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 23, Wiz's patents also include nearly identical figures and descriptions as those found in the '926 patent. Furthermore, on September 12, 2023, Orca notified Wiz of its infringement of the '926 patent through a cease-and-desist letter, attached hereto as Exhibit 10. In any event, Wiz has had knowledge of the '926 patent and its infringement thereof since at least as early as the filing of this Amended Complaint.

191. 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.

192. 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.

193. 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:

194. 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);

195. 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);

196. 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);

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

198. 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;

199. 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 Wiz derived from its infringement of the Asserted Patents;

200. 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;

201. 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;

202. 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;

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

204. 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/ Rodger D. Smith II

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@morrisnichols.com
rsmith@morrisnichols.com

Attorneys for Plaintiff Orca Security Ltd.

OF COUNSEL:

Douglas E. Lumish
Lucas A. 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

September 15, 2023

CERTIFICATE OF SERVICE

I hereby certify that on September 15, 2023, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on September 15, 2023, upon the following in the manner indicated:

Frederick L. Cottrell, III, Esquire — *VIA ELECTRONIC MAIL*
Kelly E. Farnan, Esquire
Christine D. Haynes, Esquire
RICHARD, LAYTON & FINGER, P.A.
One Rodney Square
920 North King Street
Wilmington, DE 19801
Attorneys for Defendant

/s/ Rodger D. Smith II

Rodger D. Smith II (#3778)