Petitioner's Demonstratives

Wiz, Inc. v. Orca Security Ltd.

IPR2024-01109, IPR2024-01190, IPR2024-01191

U.S. Patent Nos. 11,726,809; 11,740,926; & 11,775,326

Wiz - EXHIBIT 1417
Wiz, Inc. v. Orca Security Ltd.
IPR2024-01109, IPR2024-01190, IPR2024-01191

WILSON SONSINI

October 14, 2025

PROTECTIVE ORDER MATERIAL, CONFIDENTIAL – ATTORNEY'S EYES ONLY

The ’809 Patent

1. A method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising:

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

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

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

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

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

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

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

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

The ’926 Patent

1. A method for securing virtual cloud assets against cyber threats in a cloud computing environment, the method comprising:

[1.1] receiving a request to scan a protected virtual cloud asset in the cloud computing environment;

[1.2] 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;

[1.3] accessing, using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk;

[1.4] 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;

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

[1.6] 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

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

The ’326 Patent

1. A method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising:

[1.1] receiving a request to scan a protected virtual cloud asset in the cloud computing environment;

[1.2] for each of the requested plurality of protected virtual cloud assets in the cloud computing environment:

[1.2.a] 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 respective protected virtual cloud

asset,

[1.2.b] 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,

[1.2.c] analyzing the snapshot of the at least one virtual disk to determine an existence of potential cyber vulnerabilities, and

[1.2.d] determining a risk associated with each of the determined potential cyber vulnerabilities, and

[1.3] for each of the requested plurality of protected virtual cloud assets with the determined potential cyber vulnerabilities, determining a risk level to the cloud computing environment; and

[1.4] reporting, for each of the requested plurality of protected virtual cloud assets with the determined potential cyber vulnerabilities, the existence of the potential cyber vulnerabilities, such that the plurality of protected virtual cloud assets with the determined potential cyber vulnerabilities are prioritized based on associated risk levels.

Obviousness Grounds

Ground	Claims	35 U.S.C. §	Prior Art
'809 Patent			
1	1-10, 12-23	103	Veselov and Mohanty
2	1-10, 12-23	103	Veselov, Mohanty, and Czarny
3-4	11	103	Veselov, Mohanty, and Hutchins (with or without Czarny)
'926 Patent			
1	1, 5-10, 12-15	103	Veselov and Mohanty
2	1-2, 4-10, 12-15	103	Veselov, Mohanty, and Ranum
3-4	3	103	Veselov, Mohanty, and Seo (with or without Ranum)
5-6	11	103	Veselov, Mohanty, and Hutchins (with or without Ranum)
'326 Patent			
1	1-21 and 28	103	Veselov and Basavapatna
2	4-5 and 17	103	Veselov, Basavapatna, and Czarny
3	22-27	103	Veselov, Basavapatna, and Giakouminakis.

'809 Patent

Topic	Issues
Claim Construction	• "location" of a snapshot (not disputed) • "analyzing" the snapshot
Ground 1	• Veselov-Mohanty Combination • Elements 1.5-1.7 • Element 1.8 • Claims 15/22
Ground 2 (+ Czarny)	• Combination • Element 1.8
Grounds 3-4 (+ Hutchins)	• Combination

Claim Construction – "location" of a snapshot

'809 Pet., 9

A POSA would have understood that the ordinary and customary meaning of a "location" in this context broadly encompassed a virtual location and a non-virtual location. EX1002, ¶¶77-78; *see also id.*, ¶¶30 (data locations), 38 (snapshot locations).

Claim Construction –"analyzing the at least one snapshot"

'809 Pet., 10-11

> Accordingly, the discussion below applies a construction of "[analyze/analyzing] the snapshot" encompassing both direct analysis of the snapshot data and analysis of a VM instantiated from the snapshot. EX1002, ¶83. Veselov describes both of these approaches. *Infra*, §XI.B.5.

Claim Construction – "analyzing the snapshot"

'809 POR, 21

In contrast, Veselov's Figures 5A/5B embodiments include analyzing a snapshot as a data file, but Veselov does not disclose using, analyzing, or

Dr. Kaeli

Q. So it's your understanding that the embodiment starting at line 62 describing instantiating a copy of the VM is one of the various techniques that can be used to analyze the views and snapshots that is described in the paragraph starting at line 30.

Did I get that right?

A. The specification is describing various embodiments for techniques that can be used to analyze the views and snapshots.

EX1401, 36:2-11

'809 Patent

Various techniques can be utilized to analyze the snapshots, depending on the type of vulnerability and cyber threats to be detected. Following are some example embodiments for techniques that may be implemented by the security system **140**.

5:26-30

In yet another embodiment, the security system **140** may instantiate a copy of the VM **119** and/or a subset of applications of the VM **119** on the server **115** or a separate server and monitor all activity performed by the instance of the VM. The execution of the instance of the VM is an isolated

5:55:59

PO's District Court Brief

or data about the snapshot). But a snapshot can be analyzed indirectly, and nothing in the intrinsic evidence supports reading such indirect analysis out of the claims as Wiz asks the Court to do. *See,*

snapshots even if the VMs are instantiated from snapshots. Further, on its face, the language Wiz selectively quotes—"limitations reciting 'analyzing the at least one snapshot' ***encompass*** analyzing the snapshot itself"—is not limiting. *See Thorner v. Sony Comput. Ent. Am. LLC*, 669

EX1117, 64, 67-68

Veselov

machines. The present disclosure contemplates implementation of any suitable security assessment, including security assessments that are defined by rules packages, such as Common Vulnerabilities and Exposures (CVEs), Center for Internet Security (CIS) benchmarks, "best practices" packages, static or runtime behavior analysis, host configuration assessments, and the like.

is/are the target of the security assessment. In various embodiments, the scanning system obtains, or obtains access to, a state of the resource at a point in time (e.g., a "snapshot") prior to, or in conjunction with, initiating the security assessment. The snapshot may include all of the data needed to recreate the state of the computing resource within a duplicate, virtual computing resource. For example, the target computing resource may be an instance of a virtual machine implemented within block-level storage device resources allocated to a logical volume. The snapshot may be a copy of the state of memory, the state of any devices (virtual or physical) allocated to the resource, block-level image of the entire logical volume; or, the snapshot may be an image of only a portion of the logical volume containing

In any case, the snapshot is prepared so that the security assessment produces the results that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance.

2:35-41, 3:23-40, 4:1-4

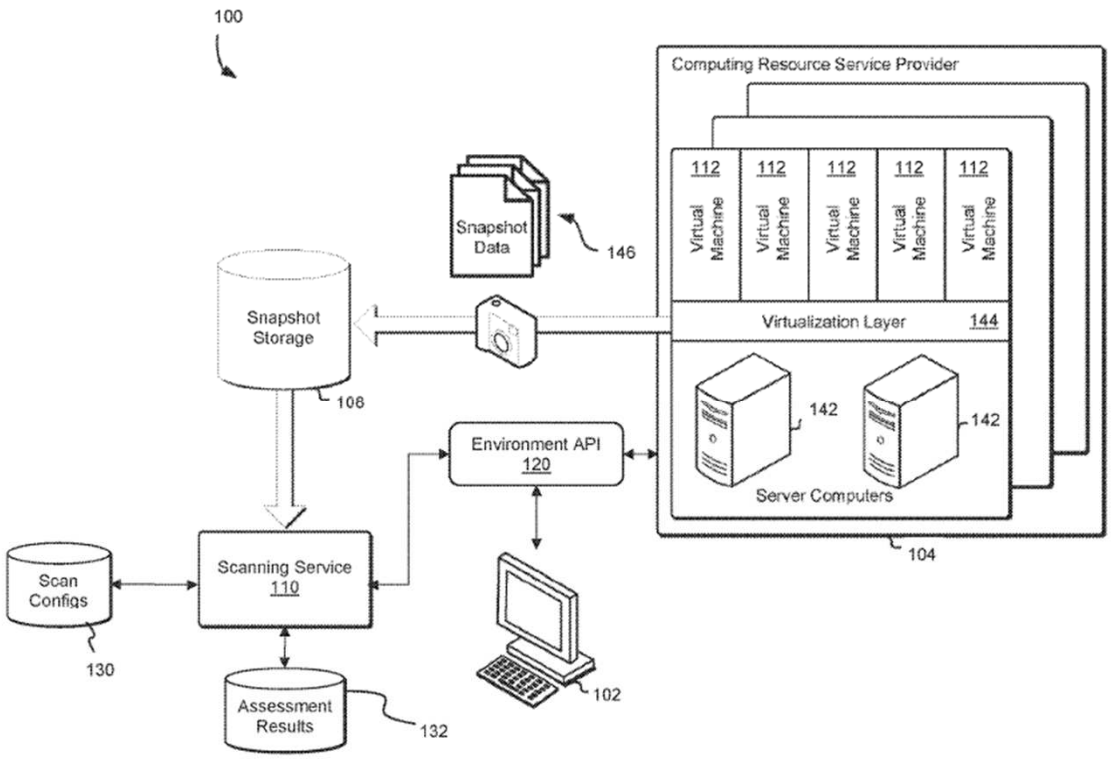
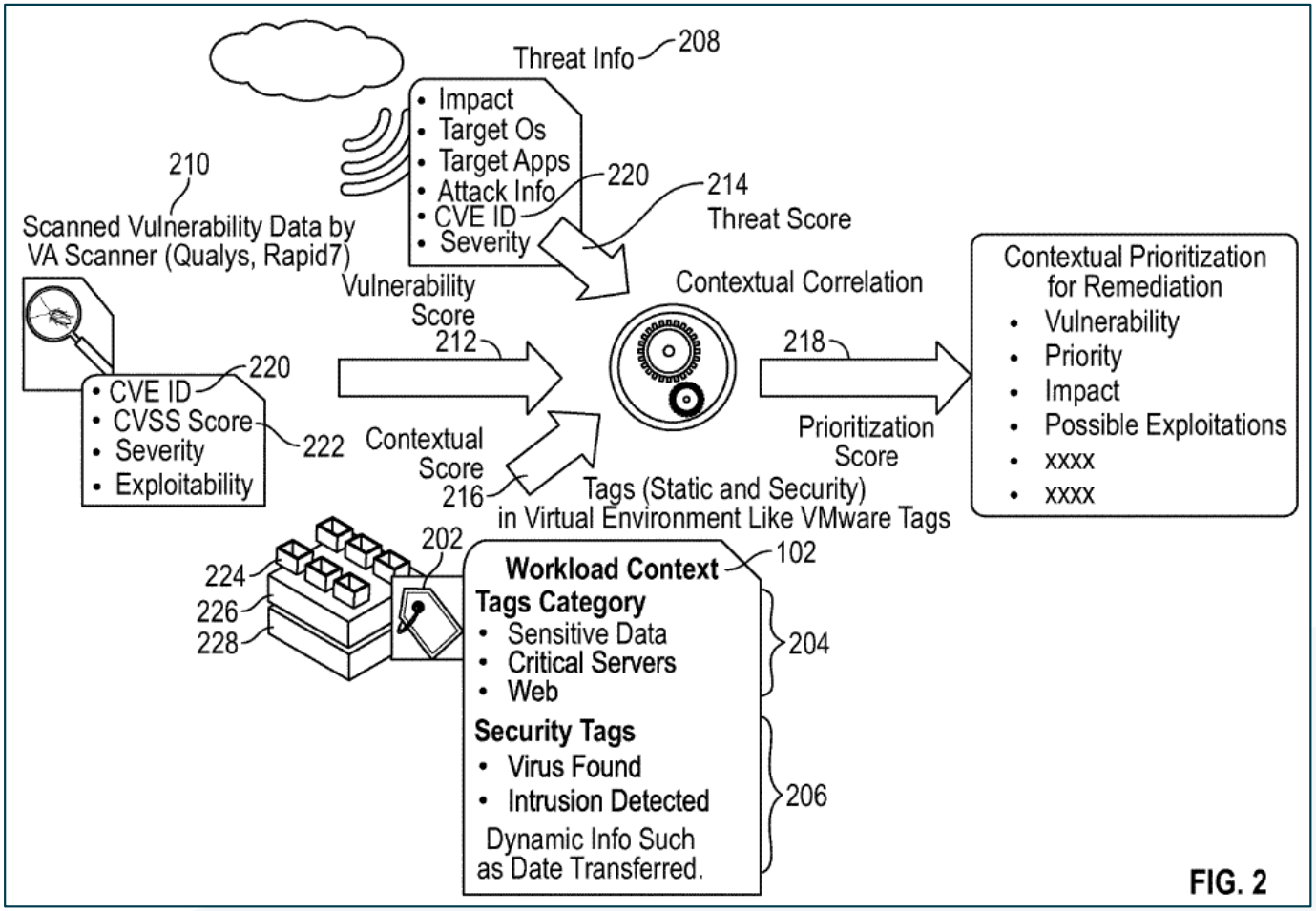


FIG. 1

computing resource service provider **104**. The scanning service **110** may access the computing resource service provider **104**, or any associated virtual computing environments and/or computing resources, via the API **120** or another API. In some embodiments, the scanning service **110** may use the API **120** to provide user interfaces to the user device **102**, enabling the user to configure settings of the scanning service **110** as described further below.

5:1-8

Mohanty



By correlating and combining threat information, vulnerability data and workload context, and rapidly updating the prioritization score that results from such analysis, the disclosed system and method provide information that is more context-based than the CVSS (common vulnerability scoring system) score.

EX1075, 3:3-8

’809 Ground 1 Combination - Motivation

More accurate measure of risk

Dr. Stavrou

(Mohanty), 1:5-22, 12:41-58. Mohanty further teaches that risk may be assessed more effectively by considering not just public information about known vulnerabilities, but also context-specific factors such as the asset’s network location, data stored on the asset, and the impact of an asset being compromised. EX1075

EX1002, ¶112

Mohanty

module **308**. The threat information **208** indicates a target operating system and/or one or more target applications. The threat module **308** can then determine whether that target operating system or that target application is indicated by one or more tags **202** as applicable to the asset **224**. If the asset **224** has that target operating system and/or that target application, the threat module **308** would then produce a higher threat score **214** associated with the asset **224**, the CVE ID **220**, and the threat under consideration. The threat

EX1075, 7:64-8:5

220 of vulnerabilities reported by VA products. Since the method and system use environment specific details with a threat feed (i.e., a supplier of threat information **208**), the derived prioritization is more accurate and meaningful than just the CVSS score **222** and the CVE ID **220**. A vulner-

EX1075, 5:64-6:1

Prioritization benefits

Dr. Stavrou

associated alerts. It was well known that prioritizing alerts was beneficial for security assessments in several ways, including rapid identification of which assets are most at risk and which threats and vulnerabilities are the most dangerous.

EX1002, ¶113

Mohanty

genuine risk to the organization may be unknown. Various embodiments of a system and method described below identify assets as to criticality of vulnerability, thereby lowering incidence of false positives and increasing awareness of assets that are critical, which may require immediate attention of a security operations team. This solves a critical problem in virtualization space, by identifying, correlating, calculating and determining the prioritization of vulnerabilities that pose serious risk to an organization that has operating assets in a virtualized environment.

EX1075, 3:33-42

’809 Ground 1 Combination – Prioritization Useful in Veselov

’809 POR, 14, 17

Kaeli¶¶90-91. Wiz also fails to address or explain why a POSA would have sought to prioritize or “alert” on Veselov’s assessment based on information gathered in the past, considering Mohanty taught that such information would be quickly rendered “obsolete.” Mohanty, 1:14-17, 1:17-22 (“in virtualized environments …

Second, Wiz ignores that Mohanty disparages vulnerability assessments that are based on reports of a system “provided in the past” because such systems “become[] obsolete within hours or minutes as virtual machines or workloads change positions within a virtualized environment.” Mohanty, 1:14-17, 2:13-35,

Dr. Stavrou

114. A POSA would have recognized that applying Mohanty’s prioritization techniques would similarly benefit snapshot-based assessments such as those described in Veselov. Snapshot-based analysis of virtual cloud assets, like other types of security analysis, would have been expected to identify multiple security problems of varying importance. *Supra*, §§VIII.D.2-3; *see also* EX1025 (NIST

EX1002, ¶114

captures that become obsolete. Kaeli-Dec, ¶98. As I explained above, however, a POSA would have understood that Veselov’s approach is reasonably current and continuous given its teaching of using fresh snapshots (EX1007, 8:62-9:25) and performing assessments on-demand, triggered, or periodically. *Id.*, 4:11-18, 6:25-31, 14:51-52. Regardless, it would have been clear to a POSA that measuring context-sensitive risk would be similarly useful to assessments of live VMs and snapshot-based assessments. Risk levels do not become irrelevant simply because assessments are based on snapshots (let alone the reasonably current snapshots taught by Veselov). Dr. Kaeli repeats his arguments that Mohanty relies on agents

EX1400, ¶27

Veselov

more virtual machines **112**. In some embodiments, a desired security assessment may be initiated by receipt of a request.

examples, the scanning service may obtain the snapshot data by executing the snapshot itself, by requesting another service to capture the snapshot and provide it to the scanning

snapshot. In some embodiments, the scanning system may enable the owner to authorize periodic assessments of the

identification of trigger events that cause the assessment to begin; which security agents **330** to install, and on which

EX1007, 6:30-31, 9:18-22, 4:11-14, 14:51-52

’809 Ground 1 Combination – Comparable Data

’809 POR, 11

But it is not true that Mohanty’s agent-based assessments and Veselov agentless snapshot-based assessments detect the same “types of data.” Kaeli¶¶88-

Mohanty

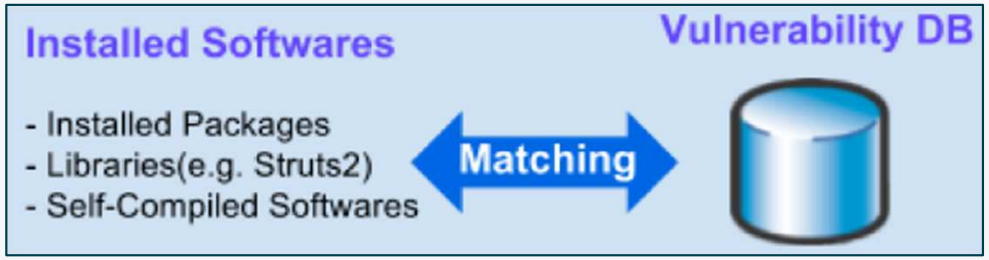
systems (see FIG. **3**). Vulnerability data **210** comes from one or more scanners (see FIG. **3**). Tag information **204**, **206**

combinations thereof. A scanner **314**, for example a VA scanner by QUALYS or RAPID7, performs vulnerability checks (i.e., scans) on the virtual machines **318** and the virtual applications **320**, and reports vulnerability data **210**, including a CVSS score **222**. This may be accompanied by a CVE ID **220**, which identifies a specific vulnerability or exposure, and which is now associated with the CVSS score **222** for a specific asset **224**. The scanner **314** can be coupled to the virtual machines **318** and the virtual applications **320** by a network **324** in some embodiments.

EX1075, 4:30-31 6:54-63

EX1140 (Vuls)

Agentless Vulnerability Scanner



Dr. Kaeli

A. So a person of ordinary skill in the art would have been aware of techniques that were available for protecting virtual assets that were either agent-based or non-agent-based.

EX1415, 11:8-11

809-Pet., 37, 47; 809-Reply, 4-5 (citing EX1400, ¶18)

’809 Ground 1 Combination – Comparable Data

’809 POR, 11

> But it is not true that Mohanty’s agent-based assessments and Veselov agentless snapshot-based assessments detect the same “types of data.” Kaeli¶¶88-

Mohanty

> scores. Whenever a CVE ID **220**, operating system, associated applications like ACROBAT, CHROME, etc. identifying a vulnerability or exposure of the asset **224**, is provided in the vulnerability data **210** from a scanner, the disclosed system and method can use this information to correlate with a CVE ID **220** provided in the threat information **208**, or operating system, impacted applications, etc. in production of a threat score **214**. Vulnerability data **210** can also include

EX1075, 5:5-12

Veselov

> machines. The present disclosure contemplates implementation of any suitable security assessment, including security assessments that are defined by rules packages, such as Common Vulnerabilities and Exposures (CVEs), Center for Internet Security (CIS) benchmarks, “best practices” packages, static or runtime behavior analysis, host configuration assessments, and the like.

> Non-limiting examples of such properties include: properties of logical volume(s) containing the target resource; properties of physical storage devices allocated to the logical volumes; file system and file information; operating system information; system and software patches applied; configurations of network protocols and services; properties of connections to other computing resources; permission settings; software packages installed, and configurations thereof; system log properties; and the like.

EX1007, 4:1-4, 2:35-41, 9:55-67

EX1139 (2008 NIST Guide)

> discovery and network port and service identification. Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization’s security policy. This is done by identifying the operating systems and major software applications running on the hosts and matching them with information on known vulnerabilities stored in the scanners’ vulnerability databases.

> Vulnerability scanners can be run against a host either locally or from the network.

4-4 to 4-5

809-Pet., 22-23, 40; 809-Reply, 2-5 (citing EX1400, ¶18)

’809 Ground 1 Combination – Location Readily Determined

’809 POR, 13, 19

target virtual machine 312.” Veselov, 18:34-38. Veselov does not teach that analyzing a snapshot itself would permit any analysis of “dynamic” data, “network connections” or “communications to computing resources,” or any of the other information available in Veselov’s agent-based VM analyses. *See id.*; Section III.A

Wiz has failed to do so here. Wiz does not show that determining the network location of a virtual cloud asset was routine or well known in security systems that analyze ***snapshots*** in a cloud computing environment-based system, as opposed to security systems that utilize agents to perform security assessments. Kaeli¶¶100-

Veselov

Non-limiting examples of such properties include: properties of logical volume(s) containing the target resource; properties of physical storage devices allocated to the logical volumes; file system and file information; operating system information; system and software patches applied; configurations of network protocols and services; properties of connections to other computing resources; permission settings; software packages installed, and configurations thereof; system log properties; and the like.

At step **208**, the scanning service may generate a scannable volume, or cause a scannable volume to be generated, based at least in part on the snapshot data. A scannable

. . .

service. Examples of generating the scannable volume described below include launching a duplicate virtual machine instance in an allocated logical volume, mounting the snapshot data in an allocated logical volume like a storage device and reading the target resource state like a data file, and incorporating data elements of the snapshot data into a partial framework of the target resource to produce the duplicate target resource.

EX1007, 9:59-10:16

312, storing in the snapshot data a real-time snapshot describing the activity and connections of the virtual machine **312**. Additionally or alternatively, the statically

system **566**), virtual machine **512**, and volume image **508**, as well as their implementation and interactions, are the same as described above for the associated components **302**, **304**A, **306**, **308**, **312**, **360-366** of FIGS. **3**A-B. In the

EX1007, 15:55-57, 16:64-67

809-Pet., 22-23, 38-39; 809-Reply, 3, 6

’809 Ground 1 Combination – Veselov’s Assessment Not Rudimentary

’809 POR, 13

In contrast, Veselov also teaches determining comparatively basic information when analyzing a snapshot as a data file, such as “to identify files, software packages, application versions, and the like, for software installed on the target virtual machine 312.” Veselov, 18:34-38. Veselov does not teach that

Veselov

assessment on the duplicate instance. In one embodiment, the scanning system may set up and launch an active virtual machine instance in the allocated computing resources, the active virtual machine instance having the same configuration as the original virtual machine instance had at the time the snapshot was captured; the system may then perform the security assessment on the active virtual machine instance in a static or runtime environment. In another embodiments, the scanning system may mount the logical volume (or transform the snapshot into a data file by identifying the file system of the original logical volume and then mount the snapshot in the duplicate logical volume) as a hard drive with data stored thereon; the system may then perform the security assessment on the data at the file system level.

In any case, the snapshot is prepared so that the security assessment produces the results that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance.

EX1007, 3:54-4:8

the mounted volume image. In some embodiments, the scanning service may use string or other pattern comparisons to identify files, software packages, application versions, and the like, for software installed on the target virtual machine **312**. For example, once the file system of the

. . .

particular software applications and versions thereof. In this manner, the scanning service may identify which assessment tasks to run based on the installed software packages. The scanning service may then, in some embodiments, run the assessment tasks on the raw file data of the mounted volume image to obtain the assessment results. At step **616**, the

EX1007, 18:34-53

’809 Ground 1 Combination – PO Ignores Veselov’s Benefits

Medichem, S.A. v. Rolabo, S.L.

finding of nonobviousness. Likewise, a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine. *See id.* at 1349 n. 8 (“The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another. Instead, the benefits, both lost and gained, should be weighed against one another.”). Where

437 F.3d 1157, 1165 (Fed. Cir. 2006)

Dr. Stavrou

meaning such assessments would be reasonably current and continuous. In any event, Dr. Kaeli’s point does not address the net benefit provided by applying Mohanty’s techniques to snapshot-based assessments. EX1002, ¶¶111-15. In other words, Veselov explains several benefits of snapshot-based assessments and explains that they yield results comparable to assessments performed on the target itself (i.e., agent-based assessments). EX1007, 2:42-4:4. Applying the teachings of Mohanty that I previously discussed then provides further benefits to that snapshot-based assessment without compromising Veselov’s existing benefits.

EX1400, ¶17

’809 Ground 1 Combination – Strawmen

’809 POR, 15, 17-18

6:54-58; Kaeli¶¶81-87, 97-105. A POSA would not be motivated to modify Veselov to nevertheless interact with the VM as taught in Mohanty because that would require processing time and power from the target VM, which is contrary to Veselov’s objective to “avoid[] consuming processing time, processing power, and storage space of the target computing resource.” Veselov, Abstract, 12:21-43, 2:54-

Veselov’s snapshot-based scanning. Kaeli¶¶88-105. Indeed, such a combination would not have a reasonable expectation of success because, as Dr. Stavrou admitted, “an agent can only be installed on a virtual machine” and “I don’t think that an agent can be installed on a snapshot.” 2nd Stavrou Tr.53:14-20. The Board should not

Dr. Kaeli

Veselov’s Figures 3A-3B), and it is not possible to install an agent on a snapshot (e.g., as in Veselov’s Figures 5A-5B) (Ex.2172 (2nd Stavrou Tr.) 53:14-20). Thus, the only implementation in Veselov that could be combined with Mohanty’s teachings is the implementation in Veselov that does not analyze a snapshot.

104. So, in Veselov’s Figures 5A-5B, the only implementations of Veselov that analyze a snapshot, installation of an agent is not possible, which means that Mohanty’s techniques (all of which rely on agents) could not be combined with Veselov’s analysis of a snapshot. Given these differences between the teachings

EX2073, ¶¶87, 104

’809 Petition, 22-23

Mohanty’s techniques would also have their known function and produce predictable results in snapshot-based analysis since snapshot analysis typically considers the same types of data (e.g., applications, configurations, etc.) and security issues as assessments performed directly on target VMs. *See* EX1007, 4:1-4, 9:55-67; EX1002, ¶110.

In re Mouttet, 686 F.3d 1322, 1332 (Fed. Cir. 2012)

crossbar arrays. It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements.

’809 Ground 1 – Elements 1.5-1.7

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

’809 POR, 21-22

resources. Kaeli¶¶107-108; *see* Veselov, 16:56-18:56, Figs. 5A, 5B, 6. Indeed, Wiz does not cite to or rely on Veselov’s snapshot analysis embodiments as disclosing limitations 1.5-1.7 or the corresponding limitations of claims 16 and 19. *See* Pet.38-

resources.” *Id.* Wiz fails to note, however, that Veselov indicates these “properties” are only included where “relevant to the security assessment.” Veselov, 9:55-58. And the only security assessments Veselov teaches where network protocols or connections to other computing resources are relevant are in the context of agent-based duplicate-VM assessments in its Figures 3A/3B embodiments. Veselov,

Veselov

Non-limiting examples of such properties include: properties of logical volume(s) containing the target resource; properties of physical storage devices allocated to the logical volumes; file system and file information; operating system information; system and software patches applied; configurations of network protocols and services; properties of connections to other computing resources; permission settings; software packages installed, and configurations thereof; system log properties; and the like.

At step **208**, the scanning service may generate a scannable volume, or cause a scannable volume to be generated, based at least in part on the snapshot data. A scannable

. . .

service. Examples of generating the scannable volume described below include launching a duplicate virtual machine instance in an allocated logical volume, mounting the snapshot data in an allocated logical volume like a storage device and reading the target resource state like a data file, and incorporating data elements of the snapshot

EX1007, 9:59-10:16

Dr. Stavrou

information in the 3A/B example. Kaeli-Dec, ¶108. As an initial matter, as I explained above, Dr. Kaeli overlooks Veselov’s teachings that the snapshot is the same in both approaches (i.e., using assessment VMs or analyzing the snapshot as a datafile). *Supra*, §VI.B; EX1007, 3:20-4:4, 9:42-10:16, 16:56-67. Even if that were not the case, the applied teachings of Mohanty provide an express reason to use the network information, making the information “relevant to the security assessment” in the combination regardless. EX1002, ¶¶108-15; EX1007, 9:42-

EX1400, ¶33

’809 Ground 1 – Element 1.8

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

Veselov

in a results data store; providing the assessment results in a user-readable format to a user interface to be displayed on the user device; if vulnerabilities are identified in the assessment results, comparing the assessment results to a remediation framework to identify one or more actions the user can take to address the vulnerabilities, and providing the identified actions to the user; and the like.

10:17-36

image; perform a security assessment on the second virtual machine instance to produce a first assessment result describing a security vulnerability of the first virtual machine instance; and, associate the first assessment result with the first virtual machine instance. The computer-ex-

20:57-21:13

Dr. Stavrou

Dr. Kaeli’s argument also fails to consider the perspective of the POSA in reading these descriptions in Veselov. As I previously explained, reporting vulnerabilities as alerts was commonplace in security platforms (EX1002, ¶¶64-68), and a POSA would have recognized that Veselov’s descriptions that I noted above are consistent with this well-known, commonplace technique.

EX1400, ¶39

Dr. Kaeli

requires an additional step beyond simply reporting the information. For example, as stated above, it is my opinion that alerts are notifications triggered to inform stakeholders of a situation that needs attention. *See* Ex.2011 [U.S. Pat. No.

EX2073, ¶124

’809 Ground 1 – Element 1.8

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

’809 POR, 25

But Wiz’s assertions merely refer to what Mohanty discloses alone, without providing any explanation how a POSA would have applied Mohanty’s teachings to Veselov in the combination. That is not enough: obviousness “cannot be predicated

Dr. Stavrou

vulnerabilities that pose serious risk”); *see also id.*, 2:9-15, 4:1-4; *supra*, §XI.B. A POSA would have recognized that Mohanty’s more detailed teachings regarding alert prioritization were a natural fit with Veselov’s more high-level description of providing assessment results to users. Mohanty simply provides a more detailed discussion than Veselov with respect to the alerting aspect of the security assessment, including a more robust description of the common, well-understood technique of prioritizing certain threats and alerts. *See supra*, §VIII.D.3; *see also* EX1046 (Crabtree), 11:52-12:14 (need for dynamic threat ranking “obvious and immediate”). That technique was likewise appropriate and useful in the types of security assessments described in Veselov.

EX1002, ¶115

809-Pet., 23-24; 809-Reply, 9

’809 Ground 1 – Claims 15/22

[Claim 15] …wherein determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the **cloud computing environment** for the location of the snapshot and the location of the virtual disk

’809 POR, 27

Wiz concedes that Veselov only discloses computing environments that are implemented by a computing resource service provider (what Wiz contends is a “cloud computing environment”) in Figures 1 and 3A-B, but not in Figures 5A-B. Pet.60-61. In the admittedly non-cloud context of Figures 5A-B, however, Veselov

Dr. Kaeli

Ex.1002 (Stavrou Decl.) ¶246. I first note that “computing resource service provider” is not typically used in the art to refer to a cloud computing environment.

EX2073, ¶133

’809 Pet., 60-61

Discussing Fig. 1—teachings that apply to all embodiments (EX1002, ¶91)—Veselov discloses a user interface (“UI”) for accessing snapshots via an application programming interface (“API”) of the protected cloud environment. EX1007, 5:1-

EX1007, Fig. 1; *see also id.*, Figs. 3A-B (depicting API 338). While Figs. 5A-B do not depict such APIs, Veselov indicates that the depicted components have the same “implementation and interactions … as described above for the associated components … of FIGS. 3A-B.” *Id.*, 16:56-17:8. Further, a POSA would have

Dr. Kaeli

Q. Is it your understanding that the Veselov inventors coined the term "computing resource service provider" specifically for their patent?

A. I don't believe I have an opinion on that. I'd have to do more research to have an opinion.

Q. When you saw that term used in Veselov, did you do any research to understand its meaning or typical usage?

MR. BAJAJ: Objection to form.

A. So I looked online to see if that was a common term, and I -- again, given the description around computing resource provider, I came to an understanding that they were referring to a cloud computing environment.

EX1401, 38:17-39:13

809-Reply, 9-10 (citing EX1400 ¶43)

’809 Ground 1 – Claims 15/22

[Claim 15] …wherein determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the **location of the virtual disk**

Veselov

lar virtual machine **112**. The scanning service **110** may determine the corresponding virtualization layer **144** for the virtual machine **112** identified by the request and transmit a command to the virtualization layer **144** to provide snapshot data **146** (or to provide access to snapshot data **146**) corresponding to the virtual machine **112**. The virtualization layer

6:38-43

Dr. Stavrou

query would also determine the virtual disk’s location. For example, a POSA would have understood that the snapshot of a virtual disk and the underlying virtual disk itself would sometimes have the same general location (e.g., being located in the same computing environment). This is further supported by Figs. 3A-B and 5A-B

EX1002, ¶250

EX1133, 1

You can attach multiple EBS volumes to a single instance. The volume and instance must be in the same Availability Zone. Depending on the

Veselov

104. For example, the API **120** may be a web-based interface implemented on a web server of the computing resource service provider **104** as described further below; one or more user interfaces may be transmitted to the user device **102** and displayed thereon, enabling the user of the user device **102** to provide settings, commands, software packages, and other user input, to the computing resource service provider **104**.

4:35-41

more APIs **338**, web interfaces, and the like. Various aspects of the security assessment(s) may be configured by user input, non-limiting examples of such aspects including: selection of the assessment target(s); parameters of the security assessment(s), such as tests or tasks to perform,

14:37-63

Veselov

scanning service may cause the snapshot data to include metadata, such as a tag, that identifies the target resource embodied in the snapshot data. In some embodiments, the

the user device; if vulnerabilities are identified in the assessment results, comparing the assessment results to a remediation framework to identify one or more actions the user can take to address the vulnerabilities, and providing the identified actions to the user; and the like.

9:9-41, 10:32-36

Dr. Stavrou

253. Querying a cloud management console to determine the virtual disk’s location also would have been obvious as part of the mitigation process that I discussed earlier in relation to claim 10, since these assessments may identify vulnerabilities associated with the virtual disk, and a POSA would have expected the console discussed above to provide query-based determination of the virtual disk’s location so that those vulnerabilities can be resolved. *Supra*, §XII.C.9 (claim

EX1002

809-Pet., 62-64; 809-Reply, 11 (citing EX1400, ¶49)

’809 Ground 2 – Claims 1-10 and 12-23 Obvious over Veselov, Mohanty, and Czarny

Benefits of reporting asset’s risk level

Dr. Stavrou

scans taught by Veselov and Mohanty. That is, a POSA would have understood that reporting the risk level would allow system administrators to make more informed decision such as whether to connect a vulnerable asset to other, more secure assets, in response to the assessment results. *Id.* (discussing a system administrator

EX1002, ¶267

Czarny

the target device **103** to the secure environment **104**. In some embodiments, the security vulnerability level may be provided as a score value indicating a level of vulnerability of the target device **103**. For example, the security vulnerability

EX1084, 7:50-53

Benefits of binary/hash matching

Dr. Stavrou

software). Furthermore, binary comparison and hash-based matching were also known to provide fast and accurate matching against lists of known applications.

EX1002, ¶266

Czarny

The binary data (for the product binary data or the target binary data) generally contains 1) binary hashes of binary level files of the software products, 2) binary hashes of

comparing type of function. The scanning and matching searches for a match between two files or two strings within two files at the low level of binary data, rather than matching a file name or other higher level meta data of two files.

data. The computer security vulnerability assessment system **100**, thus, can be used in place of a conventional security vulnerability assessment system, or in combination therewith, to enable a more thorough, robust and flexible level of functionality that is not available in conventional security vulnerability assessment systems.

EX1084, 4:7-38

’809 Ground 2 – PO’s Arguments Fail

’809 POR, 69

IV.A. Czarny concerns assessments of electronic devices – *not* virtualized resources, and does not involve either snapshot analyses, instantiated VM analyses, or agent-based analyses of VMs, as in Veselov and Mohanty. Czarny (Ex.1084), Abstract,

Instead, Czarny relies on receiving “product binary data” and using that “binary data” for a security assessment. Neither Mohanty nor Veselov discuss any similar “binary data,” and Wiz does not explain how or why a technique relying on such binary data was “supposed to work” in the combination. *Personal Web*, 848 F.3d at

’809 POR, 69-70

before the asset becomes part of a distributed environment). Accordingly, Czarny is not related to determining a risk of a protected virtual cloud asset that is “instantiated ***in***” a cloud computing environment, as in the challenged claims. *See*

’809 Petition, 69

also id., 12:11-18, Figs. 6, 10; EX1002, ¶¶269-70. As discussed in §XII.A, it would have been obvious to apply these teachings with the combination of Ground 1 such that the scanning system would report the detected vulnerabilities along with prioritization information, including asset-level risk (i.e., reporting the vulnerabilities as alerts prioritized according to the determined risk). EX1002,

Dr. Stavrou

known function for the same or similar purpose as described in Czarny. The use of these techniques would not be meaningfully impacted in the context of snapshot-based analysis since, as I previously explained, the type of snapshot-based analysis taught by Veselov involves comparable data (e.g., applications) and detection techniques (e.g., matching against lists of vulnerable applications) as non-snapshot-based analysis. *Supra*, §XII.A. Indeed, Czarny teaches analyzing disk data of offline systems, which is similar to analyzing snapshot data as in Veselov.

information stored as binary data). EX1002, ¶¶24-29. Veselov’s snapshot captures disk state (which is binary data). *Id.*, ¶¶32-36; EX1007, 3:20-40, 9:42-67.

EX1002, ¶264; EX1400, ¶55

Veselov

Referring to FIG. **1**, embodiments of the present disclosure may operate within or upon a computing environment **100** in which users, e.g., developers, customers, administrators, and other “users” that may hold a “user account” with a computing resource service provider **104**, may use user

EX1007, 4:19-29

Dr. Kaeli

around computing resource provider, I came to an understanding that they were referring to a cloud computing environment.

EX1401, 39:5-13

809-Pet., 60, 66; 809-Reply, 9-10, 12-13

'809 Grounds 3-4 – Claim 11 Obvious over Veselov, Mohanty, and Hutchins (with or without Czarny)

[Claim 11] … wherein mitigating a potential cyber vulnerability includes at least one of:
… **quarantining the protected virtual cloud asset**.

Veselov

the user device; if vulnerabilities are identified in the assessment results, comparing the assessment results to a remediation framework to identify one or more actions the user can take to address the vulnerabilities, and providing the identified actions to the user; and the like.

10:32-36

Hutchins

machine to address the detection of the malicious code. Thus, the action in response to detecting the malicious code may include placing the first virtual machine in quarantine.

Abstract

Dr. Stavrou

function, with predictable results. I discussed the well-known, predictable nature of the Veselov-Mohanty combination in Ground 1 (*supra*, §XII.A), and the further combination with Hutchins would simply add the well-known, predictable mitigation technique of quarantining a VM without significantly impacting the rest of the security assessment. Indeed, Veselov already contemplates taking mitigating actions in general. EX1007 (Veselov), 10:24-36.

285. A POSA would have also been motivated to obtain the well-known benefits of quarantining a vulnerable/infected virtual cloud asset. It was widely recognized that quarantining a compromised asset, as taught by Hutchins, has several benefits. For example, it was well known that quarantining such an asset (1) would minimize its exposure to attacks that might exploit an identified vulnerability and (2) prevent a potentially compromised asset from contaminating other resources in the system (e.g., an infected asset might spread malware to other systems on the network). *See supra*, §VIII.D.3; EX1048 (Price), ¶14 ("The security assessment of

EX1002, ¶¶283, 285

'926 Patent

Topic	Issues
Claim Construction	• "location" (not disputed) • "analyzing the snapshot" (previously discussed)
Ground 1	• Veselov-Mohanty Combination • Element 1.4 • Elements 1.5-1.6 • Element 1.7 • Claim 13 (previously discussed)
Ground 2 (+ Ranum)	• Combination • Claim 2 • Claim 4
Grounds 3-4 (+ Seo)	• Combination
Grounds 5-6 (+ Hutchins)	• Combination (previously discussed)

’926 Ground 1 Combination - Motivation

More accurate risk characterization

Dr. Stavrou

exposure of confidential information and encryption-key information). Thus, a POSA would have recognized that applying Mohanty's teachings of detecting applicable threats based on various types of data stored on the asset, determining associated risks, and prioritizing/reporting accordingly would allow security scans such as Veselov's to provide more useful results by determining and reporting more precise indications of potential harms associated with particular cyber threats.

EX1002, ¶113

Mohanty

module **308**. The threat information **208** indicates a target operating system and/or one or more target applications. The threat module **308** can then determine whether that target operating system or that target application is indicated by one or more tags **202** as applicable to the asset **224**. If the asset **224** has that target operating system and/or that target application, the threat module **308** would then produce a higher threat score **214** associated with the asset **224**, the CVE ID **220**, and the threat under consideration. The threat

EX1075, 7:64-8:5

220 of vulnerabilities reported by VA products. Since the method and system use environment specific details with a threat feed (i.e., a supplier of threat information **208**), the derived prioritization is more accurate and meaningful than just the CVSS score **222** and the CVE ID **220**. A vulner-

EX1075, 5:64-6:1

Prioritization benefits

Dr. Stavrou

associated alerts. It was well known that prioritizing threats/alerts based on associated risk levels was beneficial for security assessments in several ways, including rapid identification of which cyber threats are the most dangerous.

EX1002, ¶114

Mohanty

diation. Vulnerability data **210** and/or threat information **208** can be consulted to guide the remediation effort. In some embodiments, a remediation module **326** performs such analysis, and generates a remediation recommendation. For example, a remediation module **326** could respond to a prioritization score **218** reaching a predetermined threshold, and produce a message, a report, an alert or a file, etc. This could be in various formats and include various types of information, such as indicating the correlation of the asset **224**, the vulnerability (e.g., as identified by a CVE ID **220**), one or more applicable threats, and relevant information from tags **202**. Information technology personnel could then perform an appropriate remediation, based on this information.

lation performed in the action **406**. The threat score correlates threat information with vulnerabilities and asset characteristics to get magnitude of impact of threat in terms of threat score. Vulnerability data and tag information are

EX1075, 9:13-26, 9:62-65

’926 Ground 1 – The Combination Teaches Element 1.4

[1.4] 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, … services to be run on startup….

’926 POR, 22, 26

> 40. As an initial matter, the Board should reject Wiz’s Mohanty arguments because none of the “cyber threats” Wiz identifies are determined by analyzing “snapshots” as required by limitations 1.4, 14.4 and 15.4. Kaeli¶130. If Wiz is alleging a POSA

Palo Alto Networks, Inc. v. Centripetal Networks, LLC

> *Ltd.*, 942 F.3d 1343, 1352 (Fed. Cir. 2019). Where, as here, the grounds for obviousness are based on a specific combination of references, arguments that “attack the disclosures of the two references individually” lack merit. *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1050 (Fed. Cir. 2019). Here, Paxton

122 F.4th 1378, 1386 (Fed. Cir. 2024)

’926 Ground 1 – The Combination Teaches Element 1.4

[1.4] 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, … services to be run on startup….

’926 POR, 23

Mohanty’s “threats” are ***external*** to an asset and categorically different than the claimed “threats based on data ***stored on*** the virtual disk.” Kaeli¶132. Mohanty

exploitable vulnerability. *See* Mohanty, 6:64-7:5; Kaeli¶132. Mohanty never analyzes the virtual cloud asset to determine threats “in data stored on the virtual disk” as in the challenged claims. Kaeli¶132.

Mohanty

the CVE ID **220**, and the threat or threats. Now that the threat module **308** has determined which specific threat or threats should be associated with the asset **224** and the vulnerability or vulnerabilities thereof, the threat module **308** can correlate associated threat information **208**, concerning this threat or threats, and characteristics of the asset **224**. These characteristics can be determined from the tags

EX1075, 7:49-55

CVE ID **220**, and the threat under consideration. The threat module **308** could determine whether the threat has an impact on the asset **224**, whether the asset **224** has an operating system targeted by the threat, whether the asset **224** has an application targeted by the threat, whether the asset has a vulnerability associated with a common vulnerabilities and exposures identifier (i.e., CVE ID **220**) that is associated with the threat, or severity of impact the threat poses to the asset **224**. This information is applied to the generation of the threat score **214**. The threat score **214**

EX1075, 8:5-14

926-Pet., 38-39; 926-Reply, 6

’926 Ground 1 – The Combination Teaches Element 1.4

[1.4] 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**, … services to be run on startup….

’926 POR, 23

Third, although Mohanty discusses “sensitive data” (Pet.38), Mohanty does not “determine” sensitive data by “analyzing” a virtual cloud asset, let alone by analyzing a snapshot of its virtual disk. Kaeli¶133. Mohanty refers to “sensitive data” only as an example of a “static tag” set by a virtual cloud environment when “an asset (e.g., a virtual machine or a virtual application) is created and deployed in a virtual environment.” Mohanty, 4:4-8, 4:13-15, 5:50-54 (“*static tag information*

1376 (Fed. Cir. 2004). Here, Wiz has not identified anything in Veselov teaching “configuration” assessments include weak passwords or weak encryption schemes as claimed. Kaeli¶¶126-127. Nor can Wiz rely on inherency, because nothing about “configuration assessments” *necessarily* requires a detection of weak passwords, weak encryption schemes, or any of the other expressly identified types of data in elements 1.4, 14.4 and 15.4. Kaeli¶¶126-127; *see, e.g., PAR Pharm.*, 773 F.3d at

Mohanty

information, severity of the threat, etc. This threat information **208** can be used to correlate with vulnerability data **210** and workload context as tags information **204**, **206** from tags **202** to derive the magnitude of the threat and attack surface.

asset, in an action **420**. For example, remediation could include updating or patching an operating system, applying a stronger encryption to sensitive data, investigating a data transfer, updating or upgrading equipment, etc.

EX1075, 4:55-58, 10:31-34

sented in and derived from various tags **202**. In some embodiments, the workload context **102** represents answers to some of the following questions:

…

Do the virtual machines/workloads contain sensitive data?

…

Answers to the above questions can be defined as characteristics and written to tags **202** of assets **224**. Generally,

EX1075, 5:17-35

926-Pet., 38-39; 926-Reply, 7-9

REDACTED

’926 Ground 1 – The Combination Teaches Element 1.4

[1.4] 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, … **services to be run on startup**….

’926 POR, 18

services," Wiz's argument fails factually and legally. Factually, none of the six "CVE" exhibits Wiz cites states the vulnerabilities are associated with "common startup services," and neither the Petition nor Wiz's expert provides any explanation supporting that assertion. Kaeli¶¶124-125; Exs.1090-1091, 1100-1103. Even if any

supporting that assertion. Kaeli¶¶124-125; Exs.1090-1091, 1100-1103. Even if any of the identified CVEs actually relate to "common startup services," that still is not enough because Veselov does not teach determining any of the particular CVEs Wiz identified. *See* Pet.36-37. At best, Wiz's argument puts the cart before the horse. A

Mohanty

ments. The operating system on the computing device may be MS-WINDOWS™, UNIX™, LINUX™, iOS™ or other known operating systems. It should be appreciated that the

EX1075, 11:9-11

Dr. Stavrou

cyber threats routinely included services that run when a system starts up. For example, "systemd" was a common service the runs on startup in certain Linux systems, and there were numerous threats associated with various versions of this startup service. *See, e.g.*, EX1100 (CVE-2018-6954); EX1101 (CVE-2018-15687).

Veselov

ing virtual machine and/or containing the instance. For example, the logical volume may be a boot volume utilized by a customer to launch an instance of a web server and execute applications of the web server.

EX1007, 2:35-41, 9:5-8

Similarly, web-server services such as Apache HTTP Server were commonly run as startup services—e.g., Apache version 2 or "apache2" was a service that was commonly run when VMs operating Apache web servers started up— and there were numerous threats associated with this startup service. *See, e.g.*, EX1102 (CVE-

EX1002, ¶166

’926 Ground 1 – The Mapping of Elements 1.4-1.6 Is Consistent

[1.5] **determining a risk** associated with each of the determined plurality of potential cyber threats
[1.6] 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

’926 POR, 26-27

threats according to the risk. Pet.41. Wiz’s mapping of Mohanty to these limitations, however, is inconsistent with its analysis of limitations 1.4, 14.4, and 15.4. Ex.2172, 217:4-14 (agreeing elements 1.5 and 1.6 are “referring to the same cyber threats” as element 1.4). What Wiz maps to the “threat” in limitation 1.5-1.6 is a “threat score” that quantifies the magnitude of impact of an ***external*** threat, i.e., a threat that is ***not*** “based on data stored on the virtual disk. Pet.41; *see* Mohanty, 4:38-58, cl. 14; *see*

’926 Petition, 41-42

Type, etc.”), 7:56-8:14, claim 1; EX1002, ¶¶170-72. Mohanty teaches or at least suggests determining a threat score associated with each threat (i.e., determining “a risk associated with each threat of the determined plurality of potential cyber threats”). *See* EX1075, 7:30-33, 8:14-18, claim 3; EX1002, ¶170.

The prioritization score is based in part on the threat score (i.e., the “risk associated with each of the determined plurality of potential cyber threats”), so Mohanty prioritizes the cyber threats “based on the determined risk.” EX1075, 6:1-6, 10:9-

’926 Ground 1 – The Combination Teaches Element 1.7

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

’926 POR, 29

> prioritization scores.” Pet.44. The “prioritization score[s]” do not relate to “cyber threats based on data stored on a virtual disk” as claimed, instead being associated with “a specific **vulnerability** of a specific asset.” Mohanty, 9:6-19; Kaeli¶¶154-

Mohanty

> just the CVSS score **222** and the CVE ID **220**. A vulnerability score **212**, a threat score **214**, and a contextual score **216** are combined to form a prioritization score **218**. The

EX1075, 6:1-3

> analysis, and generates a remediation recommendation. For example, a remediation module **326** could respond to a prioritization score **218** reaching a predetermined threshold, and produce a message, a report, an alert or a file, etc. This could be in various formats and include various types of information, such as indicating the correlation of the asset **224**, the vulnerability (e.g., as identified by a CVE ID **220**), one or more applicable threats, and relevant information from tags **202**. Information technology personnel could then

EX1075, 9:19-24

’926 Ground 2 – Ranum

above, the active scanners **210** may perform the credentialed and/or uncredentialed scans in the network in a scheduled or distributed manner to perform patch audits, web application tests, operating system configuration audits, database configuration audits, sensitive file or content searches, or other active probes to obtain information describing the network.

. . .

hosts **230**, etc.), wherein the snapshot may further include any exposures that the actively running assets to vulnerabilities identified in the network (e.g., sensitive data that the assets contain, intrusion events, anomalies, or access control violations associated with the assets, etc.), configurations for the actively running assets (e.g., operating systems that the assets run, whether passwords for users associated with the assets comply with certain policies, whether assets that contain sensitive data such as credit card information comply with the policies and/or industry best practices, etc.), or any other information suitably describing vulnerabilities and assets actively detected in the network. In one implementation, in

EX1093, 13:48-14:3

ated processes. Further, in one implementation, the active scanners may compare current file systems associated with the scanned hosts to identify differences relative to the trusted file systems indexed in operation **310** (which may include previous file systems associated with the scanned hosts at an earlier time when the scanned hosts were baselined or otherwise profiled). Accordingly, in response to the active scanners

In particular, the suspicious files identified in operation **410** may include any files that have the same name but different cryptographic hashes in the file systems associated with the scanning targets and the trusted file systems, files that only appear in the scanning target file systems, files that were not present or have different cryptographic hashes relative to earlier file system versions associated with the scanning targets, and/or files having cryptographic hashes that match known malware signatures described in the malware information data feeds. For example, operation **410** may identify

EX1093, 17:62-18:1, 22:41-50

Risk Factor:	High

EX1093, Table 1

’926 Ground 2 Combination – PO Attacks a Strawman

’926 POR, 63, 65

A POSA also would have understood Ranum’s “active scanner” teachings are *incompatible* with analyzing snapshots as claimed in the ’926 Patent, and with the embodiments analyzing snapshots in Veselov. Kaeli¶¶173-178; Shua¶¶159-161; *see*

Further, Wiz and Dr. Stavrou’s assertion that Veselov, Mohanty and Ranum detect the “same types of data” is not true. Pet.58; Kaeli¶177. POSAs would have understood Mohanty’s agent-based “vulnerability assessment tools,” Ranum’s “network scanners,” and Veselov’s agentless “snapshot” based analyses inspect virtual cloud assets in fundamentally different ways. Kaeli¶177; *see* Ex.2172,

was a “different approach” Ex.2182. And both Ranum and Mohanty’s techniques require interactions with the running asset being analyzed, which is contrary to Veselov’s objective to “avoid[] consuming processing time, processing power, and

’926 Petition, 58

The combination merely involves using Ranum’s teachings according to their known function (e.g., hash-based analysis and reporting risk information) to achieve predictable results (e.g., effectively detecting changes and informing users of risk levels) since snapshot-based VM assessments typically analyzed the same types of data as in Ranum’s network scan (e.g., files), and Veselov and Mohanty teach similar comparison techniques. EX1007, 2:35-41 (may use any suitable

Veselov

Non-limiting examples of such properties include: properties of logical volume(s) containing the target resource; properties of physical storage devices allocated to the logical volumes; file system and file information; operating system

EX1007, 9:59-67

Ranum

In particular, the suspicious files identified in operation **410** may include any files that have the same name but different cryptographic hashes in the file systems associated with the scanning targets and the trusted file systems, files that only appear in the scanning target file systems, files that were not present or have different cryptographic hashes relative to earlier file system versions associated with the scanning targets, and/or files having cryptographic hashes that match known malware signatures described in the malware information data feeds. For example, operation **410** may identify

EX1093, 22:41-50

926-Pet., 58; 926-Reply, 13

’926 Ground 2 – Claim 2 Obvious

[Element 1.4] wherein the data includes at least one of: …
at least one change in at least one area of the virtual disk, as compared to an earlier point in time

[Claim 2] The method of claim 1, further comprising detecting the data stored on the virtual disk by **determining an unexpected change in the data stored on the virtual disk**

’926 POR, 66

> change in the data stored on the virtual disk.” Pet.63. But Ranum performs that comparison to identify “malware signatures,” which is not “**the** data stored on the virtual disk” that takes its antecedent basis from limitations 1.4, 14.4, 15.4. *Compare*

’926 Petition, 62

> Moreover, as discussed for claims 2 and 4 (*infra*, §§XII.C-D), Ranum teaches detecting threats based on data that includes “at least one change in at least one area of the virtual disk, as compared to an earlier point in time” as recited.

Ranum

> ated processes. Further, in one implementation, the active scanners may compare current file systems associated with the scanned hosts to identify differences relative to the trusted file systems indexed in operation **310** (which may include previous file systems associated with the scanned hosts at an earlier time when the scanned hosts were baselined or otherwise profiled). Accordingly, in response to the active scanners

EX1075, 17:62-18:1

926-Pet., 62; 926-Reply, 13-14

’926 Ground 2 – Claim 4 Obvious

’926 POR, 66-67

Claim 4 recites “detecting ***the*** data stored on ***the*** virtual disk by computing a cryptographic hash …,” which takes it antecedent from the virtual disk in claim 1 undergoing a snapshot analysis. Kaeli¶¶180-182. That differs from Wiz’s cited portions of Ranum, which use “cryptographic hashes” to “index[] one or more ***trusted file systems*** … known to have no malware infections.” Ranum, 17:1-9; *see also id.* 17:9-20[9], 17:21-23, 17:49-54. Dr. Stavrou admitted those trusted file systems “aren’t the running systems in the network.” Ex.2172, 261:18-22. Thus, they are not relevant to claim 4, because they are not cryptographic hashes of a virtual cloud asset undergoing a security assessment. Kaeli¶¶180-182.

Ranum

network. Furthermore, in response to scanning a certain host in the network and determining that the scanned host does not have any viruses or other malware infections, the file system associated with the scanned host may be indexed at that time to preserve a validated data set that can be referenced to subsequently audit or otherwise scan the host (e.g., identifying files on the host or processes running on the host that were not present or running at the time when the host was determined to have no infections, identifying files on the host or processes running on the host that have different signatures from the time when the host was determined to have no infections, etc.).

EX1093, 17:37-48

926-Pet., 64-65; 926-Reply, 14-15

’926 Grounds 3-4 – Claim 3 Obvious over Veselov, Mohanty, and Seo (with or without Ranum)

[Claim 3] …detecting the data stored on the virtual disk by **determining added or changed files on the virtual disk without a corresponding installation process**

Seo

history regarding an application is. An application that is not legitimately installed on an electronic device may be regarded as being more highly likely to be a malicious program compared to a legitimately installed application. Thus, memory loading of the executable code may be hooked only when there is no installation history of an application of the executable code, and when there is an

EX1094, ¶125

Dr. Stavrou

potentially malicious. *Id.*, ¶¶125, 134, 172. Moreover, while Seo’s process is particularly focused on applications that run encryption algorithms (in order to identify potential ransomware), a POSA would have recognized that its teachings were broadly applicable to other types of files stored on a computer system since it was well known that problematic additions/changes were not limited to executable application files. *See, e.g.*, EX1076 (Milner), 1:29-45 (security problems may be

library)”). In other words, a POSA would have understood that detecting files without corresponding installation records—be they encryption-related applications/services, other types of applications/services, or files that are not applications/services—would help identify changes to a computer system that are more likely to be illegitimate and therefore pose a security risk.

EX1002, ¶272

Dr. Stavrou

applications vs. illegitimately installed applications), Figs. 2A-B. Using installation records to distinguish between legitimate and illegitimate files was well known and routinely implemented. *E.g.*, EX1098 (Mao), Abstract, 1:64-66, 6:6-8 (identifying

EX1002, ¶269

EX1098 (Mao)

In some embodiments, determining that the system file has changed may include determining that the system file has changed without a legitimate system update to the system file.

1:64-66

’926 Grounds 3-4 – Claim 3 Obvious over Veselov, Mohanty, and Seo (with or without Ranum)

[Claim 3] …detecting the data stored on the virtual disk by **determining added or changed files on the virtual disk without a corresponding installation process**

Dr. Kaeli

artificial intelligence technology is enabled. Ex.1094 (Seo), Abstract. Dr. Stavrou does not provide any indication why a POSA would have looked solely to Seo’s alleged teaching of identifying illegitimate files based on “installation records” (Ex.1002 (Stavrou Decl.) ¶269) in a combination with Veselov and Mohanty, where these processes of Seo are based on Seo’s artificial intelligence network,

EX2073, ¶187

Dr. Stavrou

¶191 (similar arguments for Ground 4). But Dr. Kaeli’s premise is incorrect since Seo does not use AI to check for installation records. The AI aspect is part of an earlier step, and the subsequent installation-record check is just a straightforward check of “whether there is an installation history of an application.” EX1094, ¶27;

EX1400, ¶272

Seo

[0027] The method may further comprise determining whether to perform the hooking based on at least one of whether the executable code is included in a white list, a frequency of execution of the executable code, or a period of time that has elapsed since an installation or an update of an application that includes the executable code, *and determining whether to perform* the hooking based on whether there is an installation history of an application including the executable code.

926-Pet., 67; 926-Reply, 15-16

'326 Patent

Topic	Issues
Claim Construction	• "location" (not disputed) • "analyzing the snapshot" (previously discussed)
Ground 1	• Veselov-Basavapatna Combination • Claims 6 and 8 • Claim 14 (previously discussed)
Ground 2 (+ Ranum)	• No additional dispute
Ground 3	• Veselov-Basavapatna-Giakouminakis Combination

Basavapatna

[0001] This disclosure relates in general to the field of computer security assessment and, more particularly, to calculating risk metrics for assets in a system of computing assets.

[0072] Risk metrics can be generated to illustrate or assess the risk evident in particular assets by virtue of the asset's exposure to a particular vulnerability and thereby also, in some instances, an associated threat known to exploit the particular vulnerability. Generally, in modern systems, the

tor **102**. The data aggregators can receive configuration data from the assets themselves or from the sensors monitoring the assets. Example data aggregators include McAfee ePolicy

asset. In general, the configuration of the asset can include one or more of the physical configuration of the asset, the software running on the asset, and the configuration of the software running on the asset. Examples of configurations include particular families of operating systems (e.g., Windows™, Linux™, Apple OS™), specific versions of operating systems (e.g., Windows Vista™), particular network port settings (e.g., network port **8** is open), and particular software products executing on the system (e.g., a particular word processor or a particular web server). In some implementa-

[0115] As noted above, a threat-centric and vulnerability-centric risk metric can both be generated for a particular asset.

[0138] Once the network monitor **102** calculates the risk metrics, and aggregated risk metrics, as described above, the risk metrics and aggregated risk metrics can be used in various ways. In some implementations, the network monitor **102** allows users to view assets, vulnerabilities, or threats, sorted by the aggregate risk metric for the asset, vulnerability, or threat. For example, the network monitor **102** can list all assets, vulnerabilities, or threats, sorted by aggregate risk metric, or can list a top number, e.g., top ten, of the assets, vulnerabilities, or threats. Ranking assets, vulnerabilities,

EX1008, ¶¶36-37

326-Pet., 18-19, 34; 326-Reply, 4 (citing EX1400, ¶20)

’326 Ground 1 Combination - Motivation

Risk quantification benefits

Dr. Stavrou

considerations as non-virtual assets. *Supra*, §VIII.D.1. A POSA therefore would have recognized that applying Basavapatna’s teachings—e.g., determining risk levels of particular vulnerabilities/assets and communicating that information to users via filtered and prioritized alerts—would allow snapshot-based security assessments of VMs, such as those taught by Veselov, to provide more useful results that identify and quantify potential harms to the computing environment.

EX1002, ¶110

Basavapatna

[0072] Risk metrics can be generated to illustrate or assess the risk evident in particular assets by virtue of the asset’s exposure to a particular vulnerability and thereby also, in some instances, an associated threat known to exploit the particular vulnerability. Generally, in modern systems, the

Prioritization benefits

Dr. Stavrou

112. Given these teachings, a POSA would have reasonably expected the combination of Veselov with Basavapatna to improve the identification and remediation of the more significant security issues. Basavapatna’s teachings are a

(Giakouminakis), 6:9-18; EX1046 (Crabtree), 11:52-12:14. Likewise, a POSA would have understood that determining risk levels associated with vulnerabilities and alerts would provide useful bases for prioritizing and remediating higher risk vulnerabilities and assets (e.g., prioritizing assets presenting greater risks to the computing environment and prioritizing vulnerabilities associated with used applications). *See, e.g.*, *supra*, §§VIII.D.1-3; EX1025 (NIST Incident Handling), 3

EX1002, ¶112

Basavapatna

vulnerabilities, or threats. Ranking assets, vulnerabilities, and/or threats according to aggregate risk scores allows a user to quickly identify which assets are most at risk, or which vulnerabilities and threats are most dangerous for a system. The user can then remediate the most at-risk assets before remediating other less-at-risk assets, or can apply remediations across the system for the riskiest vulnerabilities and threats before applying remediations for other, less-risky ones.

EX1008, ¶138

’326 Ground 1 Combination – Bodily-Incorporation Strawmen

***In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012)**

crossbar arrays. It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements.

’326 POR, 14-15, 24

installed on a snapshot." 2nd Stavrou Tr.53:14-20. So Basavapatna's security assessments using host-based sensors, which Dr. Stavrou conceded are security agents that are "actually installed on the machine being analyzed" (*Id.* 224:20-225:2), could not operate in the proposed combination. Kaeli¶¶86-98; Shua¶161.

1025, 1034, 1036, 1040, 1044, 1045, 1046, 1048, 1063, 1076, 1077, 1078). As Dr. Kaeli explains, none of these background references support Wiz's fundamental assertions that a POSA could have or would have applied Basavapatna's agent and network sensor-based risk assessments to Veselov's agentless snapshot-based assessments. And Wiz's retreat to a laundry list of background references simply

Dr. Kaeli

could not be modified to have an agent installed. Thus, as Veselov's snapshot analysis **cannot** install an agent, it would not have been obvious to incorporate Basavapatna's teachings of determining risk, and there would not have been a reasonable expectation of success in incorporating Basavapatna's teachings of determining risk, because those teachings require installation of Basavapatna's host-based sensors 108.

EX2073, ¶99

Stavrou, so they have -- if we look at -- if we try to apply Basavapatna to the -- the snapshot embodiment described in Figures 5a and 5b of Veselov, it makes no sense to try to install those sensors and do the analysis, so -- but Dr.

EX1415, 70:13-16

326-Reply, 3, 4 (citing EX1400, ¶17)

’326 Ground 1 Combination – Snapshot-Based Risk Determination Routine

’326 POR, 17

In re Kahn, 441 F.3d 977, 986 (Fed. Cir. 2006). Nor is it plain how such a combination would work, as Wiz’s reliance on Basavapatna’s “risk assessments” are inextricably tied to the outputs of host and network based sensors that could not be applied to a security system for analyzing snapshots as proposed in Wiz’s combination. *See, e.g.*, Basavapatna, Fig. 2, ¶¶34-36, 58, 65-66; Kaeli¶¶99-101.

’326 POR, 25

levels.” ’326 Patent, cls. 1, 15, 18. In particular, as explained above, Wiz has not shown that a POSA would have reasonably expected to garner sufficient information from a snapshot to facilitate any type of cyber vulnerability risk determination, and Wiz has not shown that a POSA would have and could have modified Veselov’s snapshot-assessment embodiments to collect the data needed to apply Basavapatna’s teachings. Kaeli¶123.

Dr. Stavrou

EX1008 (Basavapatna), ¶¶99-113. This process determines a risk metric for a given vulnerability on a given asset (or in some cases a set of related vulnerabilities on the asset) based on several underlying scores, including a “standard vulnerability score” and a “composite vulnerability score.” *Id.*, ¶¶100 (vulnerability-centric risk metric

EX1002, ¶163

These standardized scores do not require agents or network-traffic inspection, and they are equally accessible to Veselov’s scanning service. For example, a POSA would have known that CVSS scores for detected CVEs were routinely included in the types of CVE results discussed in Veselov. EX1007, 2:35-41, 7:16-22

EX1400, ¶19

Basavapatna

vulnerability to particular assets or systems. In some implementations, standardized vulnerability score V_S can be derived according to a standardized, third-party vulnerability scoring system, such as the Common Vulnerability Scoring System (CVSS). Indeed, in some instances, V_S can be iden-

EX1008, ¶101

Veselov

machines. The present disclosure contemplates implementation of any suitable security assessment, including security assessments that are defined by rules packages, such as Common Vulnerabilities and Exposures (CVEs), Center for Internet Security (CIS) benchmarks, “best practices” packages, static or runtime behavior analysis, host configuration assessments, and the like.

EX1007, 2:35-41

326-Pet., 32-33, 38-39; 326-Reply, 6-7

’326 Ground 1 Combination – Snapshot-Based Risk Determination Routine

’326 POR, 17

In re Kahn, 441 F.3d 977, 986 (Fed. Cir. 2006). Nor is it plain how such a combination would work, as Wiz’s reliance on Basavapatna’s “risk assessments” are inextricably tied to the outputs of host and network based sensors that could not be applied to a security system for analyzing snapshots as proposed in Wiz’s combination. *See, e.g.*, Basavapatna, Fig. 2, ¶¶34-36, 58, 65-66; Kaeli¶¶99-101.

’326 POR, 25

levels.” ’326 Patent, cls. 1, 15, 18. In particular, as explained above, Wiz has not shown that a POSA would have reasonably expected to garner sufficient information from a snapshot to facilitate any type of cyber vulnerability risk determination, and Wiz has not shown that a POSA would have and could have modified Veselov’s snapshot-assessment embodiments to collect the data needed to apply Basavapatna’s teachings. Kaeli¶123.

Dr. Stavrou

EX1008 (Basavapatna), ¶¶99-113. This process determines a risk metric for a given vulnerability on a given asset (or in some cases a set of related vulnerabilities on the asset) based on several underlying scores, including a “standard vulnerability score” and a “composite vulnerability score.” *Id.*, ¶¶100 (vulnerability-centric risk metric

EX1002, ¶163

Basavapatna

ity score V_C for the asset and the vulnerability (**356**). The composite vulnerability score V_C estimates the potential risk a particular vulnerability poses to an asset and is derived from the standardized vulnerability score V_S and the vulnerability detection score V_D. In some implementations, the composite

[0105] The process **350** determines whether the asset possesses a particular known vulnerability (and thereby the vulnerability detection score V) by analyzing the vulnerability detection data **206** and/or asset configuration data **207** to

EX1008, ¶¶105-06

Dr. Kaeli

Q. (BY ATTORNEY ARGENTI) Would the data collected from Basavapatna's host-based sensors that you refer to also include identification of installed software?

A. I hadn't considered that in my analysis.

Q. (BY ATTORNEY ARGENTI) In the system that Basavapatna describes, would that configuration data be stored as a file?

A. I hadn't considered how it would be stored.

Q. Did you consider whether it would be stored?

A. So configuration data could be stored in flash memory, it could be stored in physical -- in a file, so there is -- there is different implementations of that.

Q. It could be stored on a disk of the asset, right?

A. It could be.

EX1415, 75:19-22, 77:16-25

326-Pet., 21-22, 32-33; 326-Reply, 6-7

’326 Ground 1 – Claims 6 and 8 Obvious

[Claim 6] …wherein determining the risk associated with one of the plurality of potential cyber vulnerabilities further comprises **determining whether the one of the potential cyber vulnerabilities corresponds to an application that is in use** by the respective protected virtual cloud asset

[Claim 8] …**checking configuration files** of the matching installed applications to determine whether at least one of the matching installed applications is not in use

’326 POR, 26, 28

asset **is running** software’ exploited by the threat.” *Id.* 44. But Wiz ignores that a determination that an asset is “running” or “executing” software in Basavapatna is based on analyzing agent-based data of an executing physical machine. Basavapatna

configuration of the software running on the asset” (Basavapatna ¶37), Wiz points to nothing in Basavapatna that mentions “configuration files of … installed applications,” nothing that teaches examining “configuration files” of applications, and nothing in Basavapatna that teaches examining “configuration files” to determine application usage. Kaeli¶139.

Basavapatna

[0104] The process can further derive a vulnerability detection score V identifying whether a particular vulnerability is possessed by, or applicable to, a particular asset (**354**). The

generation. A vulnerability is applicable to or possessed by an asset when the asset is running software or utilizing hardware that is of a type that is associated with or otherwise evidences the vulnerability. For example, if a particular operating sys-

[0105] The process **350** determines whether the asset possesses a particular known vulnerability (and thereby the vulnerability detection score V) by analyzing the vulnerability detection data **206** and/or asset configuration data **207** to

EX1008, ¶¶104-05

asset. *In general, the configuration of the asset can include* one or more of the physical configuration of the asset, the software running on the asset, and the configuration of the software running on the asset. Examples of configurations

versions, patches, service packs, etc.). *In another example,* identifying that a particular asset has an installed or running version of a particular software product can be interpreted to mean that the asset is vulnerable to particular vulnerabilities known to exist on or that are attributable to the particular version of the product.

EX1008, ¶¶37, 60

326-Pet., 44, 46-47

’326 Ground 1 – Claims 6 and 8 Obvious

[Claim 6] …wherein determining the risk associated with one of the plurality of potential cyber vulnerabilities further comprises **determining whether the one of the potential cyber vulnerabilities corresponds to an application that is in use** by the respective protected virtual cloud asset

[Claim 8] …**checking configuration files** of the matching installed applications to determine whether at least one of the matching installed applications is not in use

’326 POR, 26, 28

asset **is running** software’ exploited by the threat.” *Id.* 44. But Wiz ignores that a determination that an asset is “running” or “executing” software in Basavapatna is based on analyzing agent-based data of an executing physical machine. Basavapatna

configuration of the software running on the asset” (Basavapatna ¶37), Wiz points to nothing in Basavapatna that mentions “configuration files of … installed applications,” nothing that teaches examining “configuration files” of applications, and nothing in Basavapatna that teaches examining “configuration files” to determine application usage. Kaeli¶139.

Dr. Kaeli

Q. (BY ATTORNEY ARGENTI) Are you aware of operating systems where package managers do perform that -- provide that information?

ATTORNEY BRUNER: Objection to scope.

THE WITNESS: So there are files associated with an OS package manager that say whether files have been accessed, whether they have been run, I am familiar with that.

EX1415, 81:18-25

Veselov

relatively minimal. In one example of reproducing a virtual machine for a software application-level CVEs assessment, the snapshot may only need to contain a template, such as a *virtual machine image, from which the virtual machine is* instantiated, and a copy of the virtual machine package manager database, which lists all software packages installed on the virtual machine and their configurations.

EX1007, 7:16-21

326-Pet., 46; 326-Reply, 9-10

’326 Ground 3 – Claims 22-27 Obvious over Veselov, Basavapatna, and Giakouminakis

’326 POR, 26, 28

(Ex.1044), Abstract. But like Basavapatna (and unlike the challenged claims or the proposed combination), Giakouminakis’s security tool is “implemented and executed on … computing systems … in order to test and analyze the security of a computing system,” i.e., Giakouminakis utilizes agents on executing computing devices to identify vulnerabilities. Giakouminakis, 12:31-36; Kaeli¶¶154-155;

Additionally, Wiz’s generic rationale supporting the combination is insufficient to demonstrate obviousness. For example, Wiz asserts a motivation to combine the three references “to improve security by more accurately measuring risk” or to provide “more useful information” (Pet.65), yet this is virtually the same motivation asserted for combining Veselov and Basavapatna (*id.* 22: “more robust and accurate risk assessments”). *See ActiveVideo*, 694 F.3d at 1328. Wiz does not

Dr. Stavrou

same thing (quantify the asset’s risk to help improve security). The use of these techniques would not be meaningfully impacted in the context of snapshot-based analysis since the type of analysis taught by Veselov involves comparable data (e.g., configuration and network data) and comparable security risks (e.g., risk that would be reasonably informed by the scanned VM’s connection to other assets) as non-snapshot-based analysis. *Supra*, §§XI.A (Veselov summary); XII.A (reasons to

EX1002, ¶291

Ground 1 to improve security by more accurately measuring risk. Giakouminakis discusses the advantages of considering additional risk factors. For example, Giakouminakis explains that its multi-factorial risk assessment provides “a global view of an asset's risk” and “can, in real time, identify and analyze security threats to a computing system and provide details of vulnerabilities that accurately represent the threats to a user.” EX1044 (Giakouminakis), 2:35-50, Fig. 2; *see also id.*, Title (“Methods and systems for improved risk scoring of vulnerabilities”), 1:18-62 (discussing older approaches). These factors help capture different facets of the asset’s overall risk by taking into consideration things such as the asset’s stored data, the asset’s network location, and the asset’s connection to other assets. *Id.*, 7:45-

EX1002, ¶292

Secondary Considerations

Topics
PO Fails to Prove SideScanning Evidence Has Nexus
PO Fails to Prove Evidence Results from What is Both Claimed and Novel
PO Fails to Prove Long-Felt Need
PO Fails to Prove Skepticism
PO Fails to Prove Praise
PO Fails to Prove Copying
PO Fails to Prove Commercial Success

Nexus

***Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373-74 (Fed. Cir. 2019)**

In order to accord substantial weight to secondary considerations in an obviousness analysis, "the evidence of secondary considerations must have a 'nexus' to the claims, *i.e.*, there must be 'a legally and factually sufficient connection' between the evidence and the patented invention." *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019) (quoting *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). "The patentee bears the burden of showing that a nexus exists." *WMS Gaming Inc. v. Int'l Game Tech.*, 184

***Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33, 33**

Patent Owner does not provide an analysis demonstrating that its products are coextensive (or nearly coextensive) with the challenged claims. We, therefore, find that a presumption of nexus is inappropriate. *See* Pet.

***SightSound Techs., LLC v. Apple Inc.*, 809 F.3d 1307, 1319 (Fed. Cir. 2015)**

F.3d 135, 140 (Fed.Cir.1996). If a product both "embodies the claimed features" and is "coextensive" with the claims at issue, "a nexus is presumed." *Brown & Williamson*, 229 F.3d at 1130. In other words, a nexus exists if the commercial success of a product is limited to the features of the claimed invention. But "if the commercial success is due to an unclaimed feature of the device" or "if the feature that creates the commercial success was known in the prior art, the success is not pertinent." *Ormco Corp. v. Align Technology*,

809-Reply, 14-15, 28

Nexus

***Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373-74 (Fed. Cir. 2019)**

> *re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996). To the contrary, the patent owner is still afforded an opportunity to prove nexus ***1374** by showing that the evidence of secondary considerations is the "direct result of the unique characteristics of the claimed invention." *Id.*

***Janssen Pharms., Inc. v. Teva Pharms. USA, Inc.*, 97 F.4th 915, 933 (Fed. Cir. 2024)**

> obviousness analysis. And a proper nexus analysis must "consider the correspondence between the objective evidence and the claim scope." *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019); *see also Merck & Cie v. Gnosis S.P.A.*, 808 F.3d 829, 837 (Fed. Cir. 2015) ("Where objective indicia result from something other than what is both *claimed* and *novel* in the claim, there is no nexus to the merits of the claimed invention." (cleaned up) (first emphasis added)).

***Yita LLC v. MacNeil IP LLC*, 69 F.4th 1356, 1364 (Fed. Cir. 2023)**

> Where prior art teaches a feature and a relevant artisan would have been motivated to use it in combination with other prior-art teachings with a reasonable expectation of success to arrive at the claimed invention—as the Board here found—a secondary consideration related exclusively to that feature does not logically undermine the inference from those premises that the claimed invention would have been obvious from the full body of prior art just because the feature was not *well* known.

PO Fails to Prove SideScanning Evidence Has Nexus

Challenged patents have distinct claim features

Patent	Claims
’031 Patent	Cloud-API-based disk identification/locating
’032 Patent	Application matching and use determinations
’685 Patent	Sensitive-data detection/filtering/prioritization
’809 Patent	Network-location correlation/prioritization
’926 Patent	Data-based threat detection/prioritization
’326 Patent	Asset risk determination/prioritization

326-Reply 16-17; 326-Pet., 21

PO Fails to Prove SideScanning Evidence Has Nexus

Janssen Pharms., Inc. v. Teva Pharms. USA, Inc.

> To the extent the court's nexus analysis consists of the mere observation that Invega Sustenna is a product that embodies the claims and the praise related to Invega Sustenna, that was insufficient. For example, Janssen clearly asserts that the '906 patent covers an invention different from the '544 patent; however, both read on the Invega Sustenna product. *Cf. Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1377 (Fed. Cir. 2019) ("Where a product embodies claims from two patents, a presumption of nexus can be appropriate only if the claims of both patents generally cover the same invention.").

97 F.4th 915, 935 n.11 (Fed. Cir. 2024)

Fox Factory, Inc. v. SRAM, LLC

> The same evidence of secondary considerations cannot be presumed to be attributable to two different combinations of features. *See Therasense*, 593 F.3d at 1299. In such situations, the patentee retains the burden of proving the degree to which evidence of secondary considerations tied to a product is attributable to a particular claimed invention. *See, e.g.*, *WMS Gaming*, 184 F.3d at 1359.

944 F.3d 1366, 1378 (Fed. Cir. 2019)

REDACTED

PO Fails to Prove SideScanning Evidence Has Nexus

- ’809 claim 1: …determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one **virtual disk of a protected virtual cloud asset**….
- ’926 claim 1: …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**….
- ’326 claim 1: …determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one **virtual disk of a respective protected virtual cloud asset**….

Mr. Shua

A. No, we didn't limit ourselves to the virtual disks of the virtual machine. We are protecting cloud computing environment that include virtual machines and virtual disk, but they go beyond that.

EX1402, 37:10-14

Q. Does claim 2 of the '031 patent require automatically discovering and performing full stack scanning of an organization's cloud infrastructure to deliver comprehensive and seamless visibility into the organization's cloud inventory?

A. Let me try to answer it as clear as I can. The system of claim 1 and the system of claim 2 can be part of what you described. They can also be used to do a subset of that. So they're not -- it's not equal to one another, if that's the question? The claim describes a certain system and a certain process in the system. The other quote that you gave is a much more complete description of the system and what it does.

EX1402, 48:18-49:9

PO Fails to Prove SideScanning Evidence Has Nexus

- ’809 claim 1: …determining, based on the matching, an existence of a plurality of potential cyber **vulnerabilities**…
- ’326 claim 1: …analyzing the snapshot of the at least one virtual disk to determine an existence of potential cyber **vulnerabilities**….

PO’s Product Technical Brief

The Data Plane Path

For each region in your cloud account, Orca enumerates all the possible compute assets, taking snapshots of their data volumes to share with the Orca production account[1]. A collector—an ephemeral EC2 instance—is created within the Orca Security Cloud account (usually in the form of a spot instance). The collector successively mounts each snapshot, then immediately deletes it so customer billing isn’t affected. Next, the collector starts reorganizing the volumes. It mounts them in the same way as the scanned OS would’ve done and runs several data collection steps:

- Vulnerability Scanning
- Configuration Scanning
- Malware Scanning
- Lateral Movement Risk
- Exploitable Keys and Weak Password Detection
- Sensitive Information Scanning
- Container Scanning

EX2067, 10

Mr. Shua

Q. Are each of these seven data collection steps an important feature of SideScanning?

A. All of them are features of the Orca cloud security platform.

Q. Would you identify any one of those features as more important than the others?

A. All of these are features of the platform, which means that we deemed them to be important for our customers. I'm not ready to provide judgment on

EX1402, 77:1-9

REDACTED

REDACTED

PO Fails to Prove SideScanning Evidence Has Nexus

'326 claim 1:

- analyzing the snapshot … to determine an existence of potential cyber vulnerabilities
- reporting … the existence of the potential cyber vulnerabilities

Mr. Shua

Q. Again, looking at line 60 where it says 'analyze via at least one snapshot to detect vulnerabilities' -- do you see that?

A. Yes, I do see that.

Q. Is that the vulnerability scanning step that's listed in the first bullet point on page 10 of the technical brief?

A. Yes, it is.

EX1402, 76:11-18

PO's Product Technical Brief

During this phase, Orca provides definitive alerts regarding:

- S3 buckets exposed to the world
- snapshots that have been published to the entire world
- other misconfigurations at the cloud control plane level

EX2067, 9

Mr. Shua

Q. On page 9 Orca lists three types of definitive alerts that result from the control plane path process, right?

A. Yes.

Q. When Orca says on the same page that those alerts are provided without having to drill down, what does that mean?

A. That these alerts are generated without the need to run the data plane process. They are done solely from the control plane path.

EX1402, 70:18-71:5

REDACTED

PO Fails to Prove Evidence Results from What is Both Claimed and Novel

PO Cites:

question is today. There is no doubt, the pivotal moment was the introduction of **agentless** scanning by companies like Orca and Wiz. Agentless scanning was a turning point - but anyone who tells you they knew it at the time is lying. We're old enough to

EX2076, 8

"After years of dealing with agents, then seeing how easy it is to install and use Orca, I knew that its agentless approach was both a major innovation and a game changer, said Jeremy Turner, senior cloud security engineer at Paidy.

EX2123, 2

Known Approaches

PASSIVE MONITORING OF VIRTUAL SYSTEMS USING AGENT-LESS, OFFLINE INDEXING

EX1040 (Ammons)

file-system data. Scanning the exposed physical hard disks is similar to, and more effective than, scanning the file-system data from within the virtual machine if an anti-malware agent were to be deployed inside the operating system. Data indica-

EX1129 (Michael), 2:28-48

ically used in IaaS clouds. In addition to classic functions like image browsing, access control and deployment, Mirage provides offline image content introspection, and manipulation capabilities. This is enabled by indexing the

EX1073 (Mirage), 1

virtual machine (i.e., its offline and not operating). Security tasks may nonetheless be able to be performed on the offline virtual machine by accessing one or more machine images

IaaS). Virtual machine manager **130** interfaces can include interfaces and application programming interfaces (APIs) that can provide operations and accessing including guest management, offline registry access, virtual disk access, and other features of virtual machines that maybe running or accessible through a particular virtualization host environment. As an example, a virtual machine manager associated

. . .

faces as the VIX API and VDDK API, among others. Further, virtual machine manager-provided interfaces can be leveraged, in some instances, in connection with the performance of computer security tasks on virtual machines and guest operating services hosted on computing devices in a corresponding virtualization environment (e.g., **125**), to allow outside security tools (e.g., **105**) access to firewalled and other protected virtualized appliances and resources.

EX1048 (Price), ¶¶32, 21

809-Pet., 13; 809-Reply, 17, 20-21 (citing EX1400, ¶77)

PO Fails to Prove Evidence Results from What is Both Claimed and Novel

```
{
"Version": "2012-10-17",
"Statement": [
{ "Sid": "Stmt1402346553000", "Effect": "Allow", "Action":
[ "ec2:DescribeInstances", "ec2:DescribeImages",
"ec2:DescribeAddresses" ], "Resource": [ "*" ] }
]
}
```

EX1122 (Nexpose), 166

AWS EC2 connector inventory the instances under an account. It also collects metadata for every instance like ImageId, Instance State, Size, VPC, Subnet, EC2 Tags,..
The connector does DESCRIBE (read as "read-only") API calls to AWS API endpoint for Instances, Images, and Interfaces under the account, to build a complete EC2 inventory of your account.

EX1124 (Qualys Guide), 1

10. Enter the "**Policy Name**", then paste the following text into the "**Policy Document**" window:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1402678666000",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

EX1123 (Nessus), 11

virtual machines. At block **410**, the management component **254** discovers and identifies the virtual disks and the PRDM-mapped LUNs associated with the virtual machine, for example by using APIs to query the virtual machine host **105** on which the virtual machine resides or a virtual machine manager **150**.

EX1020 (Sancheti), 21:36-41

809-Reply, 18 (citing EX1400, ¶¶78-79)

REDACTED

PO Fails to Prove Evidence Results from What is Both Claimed and Novel

PO cites:

including on-premise devices, and now increasingly, cloud environments. The task of locating and classifying the entirety of an organization's data across all of the possible locales is no small endeavor and is generally proving unmanageable for legacy solutions such as data loss prevention (DLP) tools.

EX2152, 5

Discover More Data with Content-Aware Detection

Symantec DLP starts with a combination of advanced technologies that can accurately detect all of the confidential data in your organization—whether it's at rest, in motion, or in use. The detection technologies in Symantec DLP include:

EX1134, 1

Forcepoint Data Discovery can be used to learn the location of sensitive data both on-premises an in supported cloud-based applications. It can be used to scan data on file servers, email servers, and databases, as well as in content collaboration

EX1135, 5

[0038] Labeler **222** is a software module that labels sensitive data contained within virtual machines. Sensitive data is

rupted. In addition, the virtual machine image manager labels and sanitizes the snapshot of the specific instance of the virtual machine image at **916** and stores the labeled and sanitized snapshot of the specific instance of the virtual machine image at **918**.

EX1056 (Chari), ¶¶38, 94

Detect

Content Analytics

Leverages keywords, pre-defined alphanumeric patterns, regular expressions, file metadata, document fingerprints, and database fingerprints to identify sensitive data.

EX1136, 1

Applies unified policies to all cloud services across data at rest and in transit. Leverage policy templates, import

EX1136, 2

926-Reply, 20 (citing EX1400, ¶¶92-94)

PO Fails to Prove Nexus – No Connection to Recited/Novel Features

Dr. Stavrou

87. In sum, the features described in the secondary-considerations evidence cited by Dr. Kaeli were known, both individually and as a combination. In other words, the techniques that I describe above are not merely isolated features known in the limited context of agent-based scanning. Rather, as Veselov and the other agentless examples I discuss above make clear, these were known aspects of agentless workload scanning. *See, e.g.*, EX1007, 2:35-41, 4:1-4; EX1040 (Ammons), ¶¶28 (API), 35 (cloud), 45 (sensitive components); EX1078 (Hufsmith), ¶¶42 (API), 44-46 (cloud), 67 (cloud), 140 (cloud), 148 (API).

’809 EX1400

PO Fails to Prove It Solved Long-Felt Need

***Newell Companies, Inc. v. Kenney Mfg. Co.*, 864 F.2d 757, 768 (Fed. Cir. 1988)**

Like the inventor in *Calmar, Inc. v. Cook Chemical Co.*, part of the *Graham* trilogy, once another supplied the key element, there was no long-felt need or, indeed, a problem to be solved by Ferguson. The following statement in *Calmar* would apply

Qualys Unveils Cloud Agent Platform for Continuous Asset Inventory, Security and Compliance

April 22, 2015

Conventional host-based scanning methods combined with network scanning have been the de facto way for organizations to identify vulnerabilities as well as update and verify patches to mitigate threats. However, the challenges of establishing scanning windows and authenticated scans, managing and updating heavyweight agents, and the rise of the cloud and mobile environments, have proven difficult and cost prohibitive for most companies. The Qualys Cloud Agent Platform resolves this conundrum by combining the power of its Cloud Platform with lightweight agents that are extensible, centrally managed and self-updating.

EX2102, 1

Mr. Shua

Q. Does Orca offer an agent based solution?

MR. DAVIS: Objection. Relevance.

A. Orca recently added a sensor based capabilities to the platform.

Q. Is the sensor you're referring to in your answer an agent?

A. You can consider this sensor as an agent.

EX1402, 128:16-19 129:17-19

Containers are ephemeral. Agentless scanning doesn't fit the containerized world well, because many containers run for only seconds at a time. No matter how "real

Overall, the story of CNAPP is the story of security teams looking for agentless visibility solutions, before maturing into agent based ones as they learn that their cloud is mostly containers. Security teams start wanting visibility, and quickly realize that they

EX2076, 12-13

Agentless vs. agents: Companies that once championed agentless solutions are now all building agents.

EX1125 (unobscured version of 2076), 2

809-Reply, 19-20

REDACTED

PO Fails to Prove Praise – PO's "Objective" Evidence

EX2117

EX2118

EX2145

CISO Choice Awards Winners 2020

EX2129-2130

Orca Security Named to Inaugural Redpoint InfraRed 100 List

EX2132

Orca Security Named to Notable Capital's Rising in Cyber 2024

EX2117

At Panorama Technologies, we understand the importance of having a holistic view of your cloud environment. As an Orca Security partner, we employ

Mr. Shua

Q. Did Orca commission the TAG Cyber report submitted as Exhibit 2118?

A. Let me open that. Yes, I believe we worked with TAG Cyber on this report, which includes

Q. This TAG Cyber report is part of Orca's marketing materials available on Orca's website, right?

A. I believe that this TAG Cyber report is available on Orca website.

EX1402, 173:9-12, 174:1-5

Q. So, the company that sponsored the awards you cite in Exhibit 2145 had a significant financial interest in Orca at that time, right?

A. Yes. YL Ventures had significant interest in Orca. Having said that, to the best of my

EX1402, 178:9-13

A. Redpoint is indeed an investor and it's

EX1402, 180:8

Q. Notable Capital is another Orca investor, correct?

A. That is correct. They invested in Orca

EX1402, 182:20-22

PO Fails to Prove Praise

***Ingenico Inc. v. IOENGINE, LLC*, IPR2019-00929, Paper 53, 100-01**

We find Judge Bryson's well-reasoned decision in *Sonos* instructive. *Sonos* draws a distinction between two types of industry praise. On one

. . .

On the other hand, "that principle does not justify the admission of the full text of every document that contains a favorable comment about Sonos or its products from any source. In order to be admissible, *the evidence must reflect praise in the industry, not just an individual's favorable view of the product.*" *Sonos*, slip op. at 5 (emphasis added). As a result, "[d]ocuments that reflect simply favorable comments about a company and its products are more problematical" as they are "simply hearsay comments about . . . products." *Id.* at 5, 7.

In this case, Exhibit 2114 reflects personal opinions of the author, Dan Harkabi. *See* PO Resp. 66. Even if Mr. Harkabi was an industry leader, nothing in Exhibit 2114 indicates that he is speaking on behalf of an industry group or presenting an industry award. *See* Ex. 2114. Rather, the

REDACTED

PO Fails to Prove Copying

Mr. Shua

116. At this May 2019 meeting, we explained to Mr. Costica how cloud security would forever be changed by Orca's SideScanning™ technology, which enabled agentless cloud security, avoiding the need for installation of agents, and was key to consolidating cloud security capabilities, especially across multi-cloud environments.

'809 EX2074

Mr. Shua

Q. Did you use any presentation materials at the meeting, like Powerpoint slides?

A. I believe I did. I believe we did use slides.

Q. Those presentation materials are not among the exhibits that you cite in your declaration, right?

A. If you state so.

EX1402, 186:9-16

Mr. Shua

119. In early 2020, I began hearing rumors that there was a new company in "stealth mode" that was developing an agentless cloud computing platform that was very similar to Orca's. That company turned out to be Wiz, which emerged from stealth on December 9, 2020, but was competing for the same customers as Orca even earlier. Based on our direct competition with Wiz and the feedback we received

'809 EX2074

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

PO Fails to Prove Commercial Success

***In re Applied Materials, Inc.*, 692 F.3d 1289, 1300 (Fed. Cir. 2012)**

pad. However, the more probative evidence of commercial success relates to whether the sales represent "a substantial quantity in th[e] market." *Id.* at 140 ("This court has noted in the past that evidence related solely to the number of units sold provides a very weak showing of commercial success, if any."). The Board observed that "customers may have had a

. . .

the evidence presented by Applied. An important component of the commercial success inquiry in the present case is determining whether Applied had a significant market share relative to *all* competing pads based on the merits of the claimed invention, which Applied did not show.

Mr. Shua

Q. What is Orca's share of the CSPM market?

A. I don't think that I offered opinion on that and I'm not ready to provide numbers.

Q. I appreciate that. If we can just focus on the September 2024 timeframe when this document was generated that you cite in your declaration. As of that time, did SideScanning compete with Prisma Cloud?

A. Yes. Orca cloud security platform competed with Prisma Cloud.

Q. Do you know whether at the time that this article was generated Prisma Cloud was using agents?

A. Prisma Cloud at the time of this time included both agent and agentless capabilities.

Q. Does Orca also compete with CrowdStrike Cloud?

A. To a certain extent Orca compete with CrowdStrike.

EX1402, 122:3-5, 111:17-112:9

PO Fails to Prove Commercial Success

***Novartis AG v. Torrent Pharmaceuticals Ltd.*, 853 F.3d 1316, 1330-31 (Fed. Cir. 2017)**

> the '283 patent's priority date. The fact that Gilenya was the first to receive FDA approval for commercial marketing does not overcome the fact that solid multiple sclerosis compositions were already known. Thus, we agree with the Board that Novartis' proffered evidence is not probative of the nonobviousness inquiry.[5]

How Agentless Scanning Emerged

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

EX2076, 11

809-Reply, 22-23

PO Baselessly Takes Credit for Wiz's Success

Wiz: Wiz pushed agentless scanning to new limits, most importantly by introducing the intuitive graphing of asset relationships to security teams, and building their entire UX around that capability. They also showed publicly

revenue within four years of its founding. Wiz differentiated itself by taking a graph-based approach to visibility, detection, high-fidelity risk prioritization alerts and an obsessive customer-driven approach, setting it apart from the competition. While the

A core factor in Wiz's success is its graph-based architecture, from the actual database to the user experience. Cloud environments are composed of many interconnected

It is widely known and should be emphasized Wiz launched a much more effective agentless scanner that helped teams identify vulnerabilities with incredible quick time-to-value and deployment for the largest enterprises. The underlying premise comes

Wiz's true strength is in their ability to come to market at exactly the right time to meet customers where they're at. Rather than sit on their agentless success, they introduced an agent when people started asking for it. They improved their DSPM capabilities as teams cared about it. Most recently, they announced Wiz Code just as security teams are catching onto the power of ASPM capabilities. Wiz is frightening to the market precisely because they're not just a history lesson stuck in what they invented, but continue to release just the right features at just the right time to appease the majority of the market.

EX2076, 7, 8, 21, 22, 23

809-Reply, 27-28(EX1400, ¶125)