

Wiz, Inc., Petitioner v. Orca Security LTD., Patent Owner

Patent Owner's Demonstratives

October 14, 2025

IPR2024-01109 (Patent 11,726,809)

IPR2024-01190 (Patent 11,740,926)

IPR2024-01191 (Patent 11,775,326)

Table of Contents

Introduction

2

Claim Construction (809/926/326 All Grounds)

9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds)

17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds)

30

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds)

52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds)

56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14)

72

Objective Indicia (809/926/326 All Grounds)

87

926 Ground 2

191

809 Ground 2

201

326 Ground 3

206

926 Grounds 3-4

209

809 Grounds 3-4

212

Motion to exclude

216

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

'809 Patent, Claim 1

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.

'326 Patent, Claim 1

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.

Ex. 1001 '926 Patent, Claim 1

New Combinations Of Known Components Are Patentable



“[I]nventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.”

KSR Intern. Co. v. Teleflex Inc., 550 U.S. 398, 418 (2007)



“A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art.”

KSR Intern. Co. v. Teleflex Inc., 550 U.S. 398, 401 (2007)

New Combinations Of Known Elements Are Patentable



“Only God works from nothing. Men must work with old elements.”

Fromson v. Advance Offset Plate, Inc., 755 F.2d 1549, 1556 n.3 (Fed. Cir. 1985)



“we cannot allow hindsight bias to be the thread that stitches together prior art patches into something that is the claimed invention”

Metalcraft of Mayville, Inc. v. The Toro Co., 848 F.3d 1358, 1367 (Fed. Cir. 2017)

Table of Contents

Introduction

2

Claim Construction (809/926/326 All Grounds)

9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds)

17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds)

30

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds)

52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds)

56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14)

72

Objective Indicia (809/926/326 All Grounds)

87

926 Ground 2

191

809 Ground 2

201

326 Ground 3

206

926 Grounds 3-4

209

809 Grounds 3-4

212

Motion to exclude

216

Analyzing The At Least One Snapshot

Orca's Construction

The claims mean what they say and require analyzing snapshots and snapshot data—not duplicate VMs instantiated from snapshots.

Wiz's Construction

“Analyzing the snapshot’ encompass[] both [1] direct analysis of the snapshot data and [2] analysis of a VM instantiated from the snapshot.”

Wiz Abandoned Its Incorrect Construction

809 Reply

Regardless, the petition does not depend on the assessment-VM approach, mooting PO's claim-construction argument. Pet., 34-37; EX1400, ¶¶10-15.

809 Pet. Reply 2

Wiz's Expert Performed No Analysis

Dr. Stavrou

Q. And you don't have an opinion as an expert, a technical expert, that it's correct to say that analyzing a virtual machine that's been instantiated from the snapshot would meet the analyzing the snapshot requirement of Orca's patent claims; is that true?

A. I do not have an opinion because I didn't look into that subject. I was instructed to perform that analysis under this assumption, and I did.

* * *

Q. ...There is nowhere in your declarations where you lay out evidence or analysis that would say, well, I've been asked to assume it, here is evidence, or analysis that says that assumption is a good one?

A. I don't believe so.

Ex. 2077 (Angelos Stavrou Dep.), at 268:4-13; 269:15-20

Analyzing A Duplicate VM Is *Not* Analyzing A Snapshot

Dr. Kaeli

“analysis of a VM instantiated from a snapshot.” As an initial matter, there appears to be no disagreement that an instantiated VM is not a snapshot—otherwise Dr. Stavrou would not have enumerated it as separate from “direct analysis of snapshot data” in his assumed construction. Rather, an instantiated VM is a VM, and analysis of a VM instantiated from a snapshot is an analysis of a VM—not a snapshot. Once a VM is instantiated from a snapshot, e.g., when a duplicate VM is instantiated from a snapshot for subsequent monitoring, the instantiated VM is no longer a “snapshot,” and monitoring, assessing, or evaluating it is not “analyze/analyzing” a “snapshot” as claimed. This would have been readily

Ex. 2073 (Kaeli '809 Decl.), ¶ 46

Analyzing A Duplicate VM Is *Not* Analyzing A Snapshot

Dr. Kaeli

patent), 4:60-61. The specification also distinguishes analyzing a snapshot by a “security system 140 to detect vulnerabilities” (Ex.1001 (’809 patent), 5:20-21), as claimed, from “another embodiment” where a system “instantiate[s] a copy of the VM” and performs “execution of the instance of the VM... [in] an isolated sandbox” (Ex.1001 (’809 patent), 5:55-60, 7:42-52).

Ex. 2073 (Kaeli ’809 Decl.), ¶ 46

Dr. Kaeli's Analysis Is Undisputed

Dr. Stavrou

10. I understand that Dr. Kaeli argues that this limitation does not encompass analyzing a duplicate VM created from the snapshot. Kaeli-Dec, ¶¶43-47. Even if his view were adopted, this would not impact my previous conclusion that the claims were obvious in view of the Veselov combinations since Veselov teaches analyzing duplicate VMs instantiated from snapshots and directly analyzing snapshots as data files as alternative ways of conducting the analysis step. EX1007 (Veselov), 3:20-4:4, 10:1-16. In other words, there does not appear to be any dispute that Veselov's snapshot-as-a-data-file analysis option satisfies this limitation.

Ex. 1400 (Stavrou '809 Reply Decl.), ¶ 10

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

No MTC: Mohanty Disparages Snapshots Of A Vulnerability Assessment Report

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

Ex.1007 (Veselov) at 3:23-27

At step 210, the scanning service may perform the security assessment on the scannable volume. Generally, performing the security assessment includes applying the rules of the assessment to the properties of the reproduced target resource to produce assessment results that describe “findings” relative to the assessed properties; examples depending on the method of generating the scannable volume and the rules of the assessment are described below. At step 212,

Ex.1007 (Veselov) at 10:18-24

Virtualization has redefined how IT ops (information technology operations) build and deliver assets in a virtualized environment, where virtual machines or virtual applications (apps) go online or offline, or change zones dynamically within minutes or hours. Traditional Vulnerability Assessment (VA) products which scan machines to report vulnerabilities have difficulties in a virtualized environment.

A snapshot of a vulnerability assessment report of a system provided in the past becomes obsolete within hours or minutes as virtual machines or workloads change positions within a virtualized environment. Consequently, in virtualized environments, any risks, threat exposures or known vulnerabilities are constantly changing. A security operations team needs a strong and continuous prioritization system to track critical vulnerabilities and take actions as changes occur.

Ex.1075 (Mohanty) at 1:7-22

No MTC: “Continuous” Snapshots Renders Veselov Inoperable For Intended Purpose

The snapshot data 146 may be point-in time consistent. This may require that all writes to the disk are queued until a complete copy of the virtual machine 112 may be generated. Queuing the writes may cause the writes to disk to be deferred or otherwise stalled until generation of the snapshot is completed. In some embodiments, the snapshot data 146

Ex.1007 (Veselov) at 6:50-55

The present systems and methods overcome drawbacks of existing security assessment systems, such as allocation and overuse of processing power, unavailability of resources services that are part of the assessment, and complexity of installation and monitoring of the assessment system. A

Ex.1007 (Veselov) at 2:42-47

No REOS: Snapshots Cannot Provide “Continuous” Assessment

Scenario 1: Real-Time, Continuous Vulnerability Management and Compliance

Agentless solutions are engineered to provide basic visibility into vulnerabilities and misconfigurations based on scanning from the outside-in. While this may provide some level of insight, they are not continuous, real-time solutions.

Ex. 2106 at 1

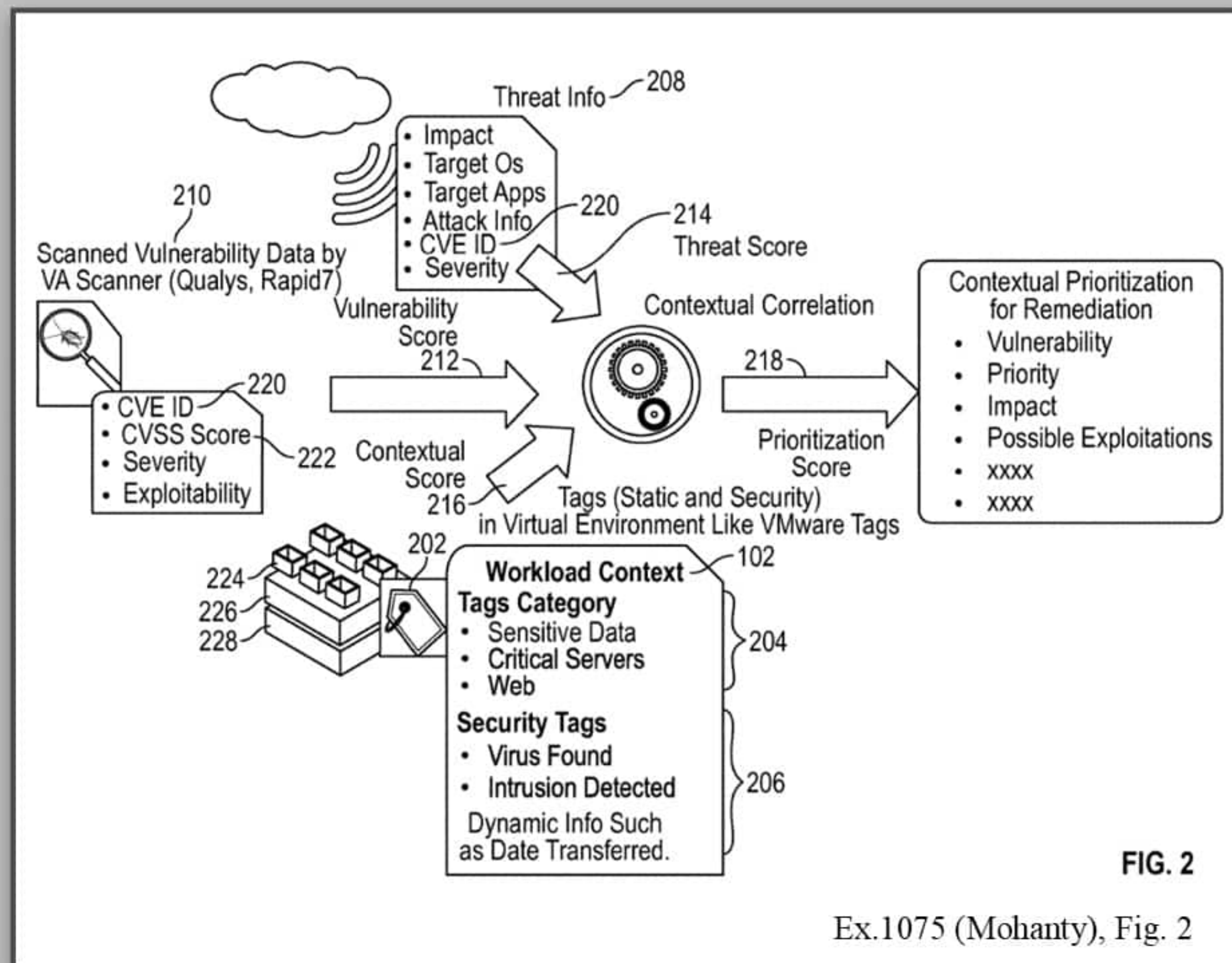
that delivers security for cloud native workloads. Unfortunately, this lightweight architecture only delivers rudimentary security capabilities, mostly useful for compliance. These solutions fail to take advantage of immutable infrastructure principles and only offer a “point-in-time” view, or “snapshot” of what’s running at any given time. They cannot capture the dynamic evolution of workloads or provide runtime attack prevention and policy enforcement. Here we present a few scenarios that demonstrate this shortcoming.

Ex. 2106 at 1

No MTC: Veselov Advises Against Complex Monitoring Systems

The present systems and methods overcome drawbacks of existing security assessment systems, such as allocation and overuse of processing power, unavailability of resources services that are part of the assessment, and complexity of installation and monitoring of the assessment system. A

Ex.1007 (Veselov) at 2:42-46



No MTC: Veselov's Snapshots Do Not Result In Hundreds Of Vulnerabilities

The scanning system may store the assessment results, or provide them to an owner or administrator of the virtual machine in order to evaluate the vulnerabilities of the target resources. The scanning system may then delete the snap-

Ex.1007 (Veselov) '563 Patent at 4:5-8

The scanning service 110 performs the desired security assessment using the snapshot data 146. For example, the scanning service 110 may obtain the snapshot data 146 from the snapshot storage service 146 and may process the snapshot data 146 to generate one or more assessment results. Processing the snapshot data 146 may require apply-

Ex.1007 (Veselov) '563 Patent at 8:16-21

as well. The challenges presented include how to interpret hundreds of vulnerabilities reported by these VA products and how to identify specific vulnerabilities that truly represent a clear and present risk to security. The CVSS score (as

Ex.1075 (Mohanty) at 1:28-31

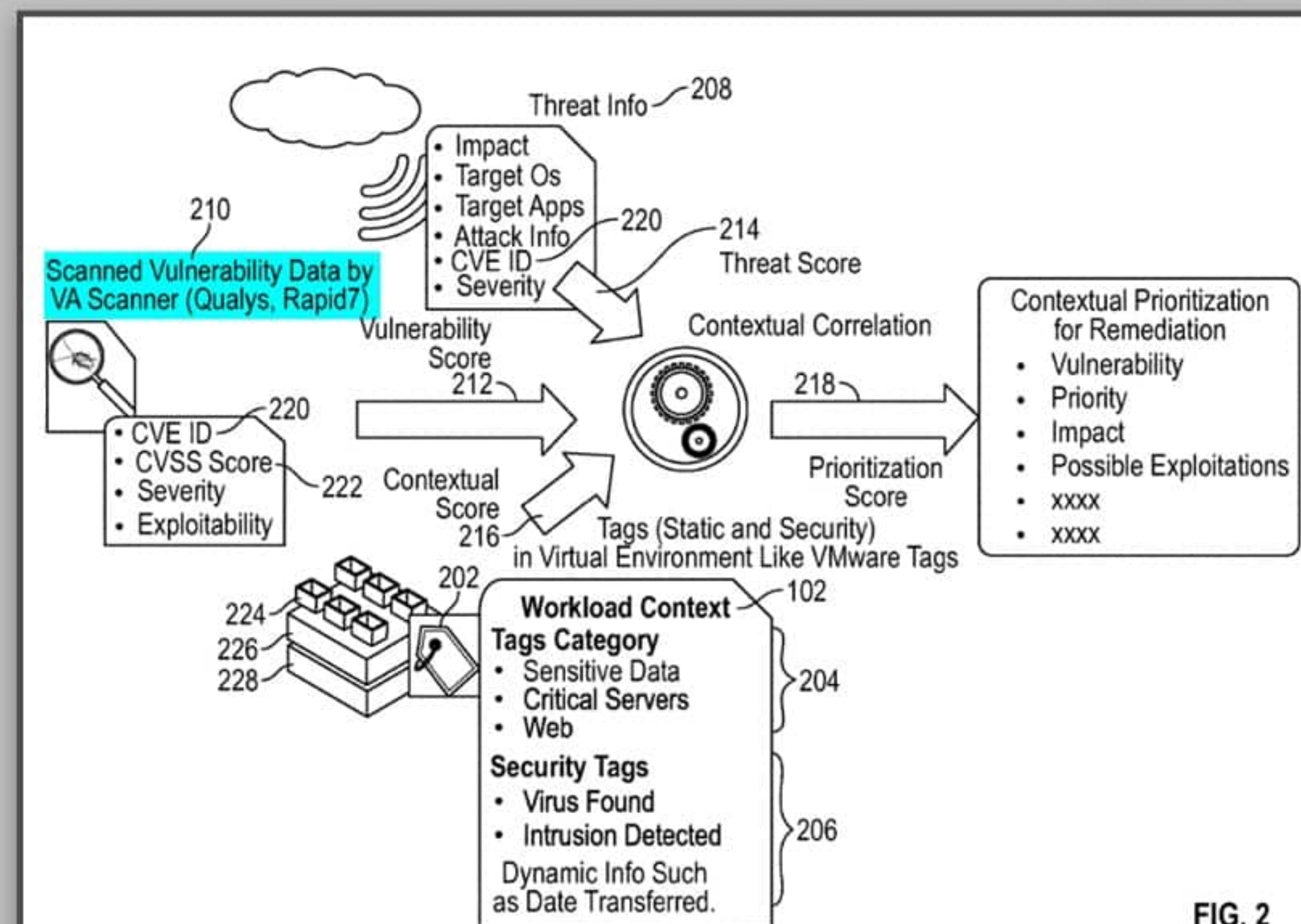


FIG. 2

Ex.1075 (Mohanty), Fig. 2

No REOS: Collecting Network Location Without Agents

original. In other embodiments, the assessment virtual machine 312A-B may be “non-viable,” in that it cannot perform material operations of the original virtual machine 312. A predominant cause of non-viability is that the virtual machine 312 performs requisite operations on dynamic data, the sources of which cannot be captured in the snapshot data (i.e., the volume image 308) without violating the data integrity. Security assessments may nonetheless be performed on a non-viable assessment virtual machine 312A-B if the assessments themselves evaluate only the static data associated with the original virtual machine 312.

Ex.1007 (Veselov) at 14:2-12

In some embodiments, the scanning service 310 can cause processing activity to occur within the assessment virtual machine 312A-B in order to apply tasks of the security assessment to real-time dynamic or static data, network connections, communications to computing resources, and other computational activities of the assessment virtual machine 312A-B. In order to stimulate activity that mirrors

Ex.1007 (Veselov) at 15:41-47

implementations of FIGS. 5A-B, rather than recreating and instantiating a duplicate VM, the scanning service 510 is configured to analyze the volume image 508 as a data file. The scanning service 510 may transform the volume image 508 into a format in which the scanning service 510 can read the copied files and other data; in the illustrated examples, the scanning service 510 does this by mounting the volume image as a virtual storage device.

Ex.1007 (Veselov) at 17:1-8

instance that was imaged. At step 614, the scanning service may perform the security assessment by reading the files of 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

Ex.1007 (Veselov) at 18:32-38

No REOS: Agents Collect Different Data

Agentless access also does not have the depth of visibility that agent-based solutions do. Agent-based software can see vulnerabilities hidden from remote solutions because it has privileged access to the OS.

Ex. 2104 at 3

REDACTED

REDACTED

REDACTED

REDACTED

Analyzing Snapshots Is Not The Same As Agents/Network Scanners



SideScanning™ Tech

SideScanning™ – Inside the Engine that Powers Orca Security

The cloud estate of an organization comprises its complete inventory of cloud assets including running and stopped workloads of all types including VMs, containers, storage objects, load balancers, IAM configurations, and more. Organizations are searching for effective ways to scan their cloud estate to look for risks stemming from vulnerabilities, misconfigurations, malware, lateral movement risk, weak and leaked passwords, and improperly secured PII.

Orca Security introduces a radically new approach that secures the entire cloud estate and helps meet compliance mandates, but without disrupting business operations in live environments.

Orca Security Ltd.
Exhibit 2067
Wiz v. Orca
IPR2024-00862, -00864, -00865,
-01109, -01190, -01191
Ex. 2067-001

Orca Security uses a novel patent-pending technology called SideScanning™. SideScanning is a radical approach because Orca doesn't go *inside* each workload to inspect data. Instead, it uses an out-of-band process to reach cloud workloads through the runtime storage layer, combining this with metadata gathered from cloud provider APIs. Orca is able to provide deep and contextualized visibility of cloud environments. It covers 100% of an organization's assets with absolutely no agent or network scanner.

An apt analogy is to think of a medical MRI. Instead of probing inside the body with needles and scalpels, such imaging is an out-of-band method of obtaining a detailed picture of the organs and tissue within. The person is never physically touched. SideScanning is similar in that it's able to build a full model of the cloud environment without affecting it in any way—and all assets and their associated risks are clearly visible. Orca can probe the read-only view it has obtained in an entirely touchless manner.

Ex. 2067 at 5

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds) 17

**Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds) 30**

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Limitation 1.4 Is Not Taught Or Suggested

[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;

Ex. 1001 '926 Patent, Claim 1

926 Petition Reply

Third, PO's argument addressing the recited data types fail. Wiz addressed

unencrypted sensitive data, weak encryption schemes, personally identifiable

information ("PII"), weak passwords, and startup services. Pet., 38-40. As to

926 Pet. Reply 6-7

926 Patent: Stored-Data Cyber Threats Are Not Vulnerabilities

[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:

- ① unencrypted sensitive data,
- ② weak passwords,
- ③ weak encryption schemes,
- ④ services to be run on startup,
- ⑤ personally identifiable information,

Ex. 1001 '926 Patent, Claim 1

In yet another embodiment, the security system 140 is configured to detect cyber threats that do not represent vulnerabilities. For example, the security system 140 may detect and alert on ① sensitive data not being encrypted on the logical disk, private keys found on the disks, system credentials stored clearly on the disk, risky application features (e.g. support of weak cipher suites or authentication methods), ② weak passwords, ③ weak encryption schemes, a disable address space layout randomization (ASLR) feature, suspicious manipulation to a boot record, suspicious PATH, LD_LIBRARY_PATH, or LD_PRELOAD definitions, ④ services running on startup, and the like.

In an embodiment, any ⑤ detected cyber threats related to sensitive data (including personally identifiable information, PII) is reported at a higher priority. In an embodiment, such data is determined by searching for the PII, *analyzing the*

Ex. 1001 '926 Patent at 6:21-32, 48-51

CVE Assessments Detect Vulnerabilities, Not Stored Data Cyber Threats

926 Petition

First, Veselov teaches applying rule packages such as CVEs, which were known to identify cyber threats. EX1007, 2:22-54, 7:16-22; EX1002, ¶156 (citing EX1077, 8:1-15); *supra*, §§IX.B, XI.B.1. For example, many CVEs were associated with application features posing a threat to system security and common startup services. EX1002, ¶156 (citing EX1090; EX1091; EX1100; EX1101; EX1102; EX1103). The '926 patent identifies these types of security problems as

926 Pet. 36-37



The Common Vulnerabilities and Exposures (CVE) Program's primary purpose is to uniquely identify vulnerabilities and to associate specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities. The use of CVEs ensures that two or more parties can confidently refer to a CVE identifier (ID) when discussing or sharing information about a unique vulnerability. For detailed information regarding CVE please refer to <https://cve.org/> or the CNA Rules at <https://www.cve.org/ResourcesSupport/AllResources/CNARules>.

Ex.2188 (NIST) at 2

In yet another embodiment, the security system 140 is configured to detect cyber threats that do not represent vulnerabilities. For example, the security system 140 may detect and alert on sensitive data not being encrypted on the logical disk, private keys found on the disks, system credentials stored clearly on the disk, risky application features (e.g., support of weak cipher suites or authentication methods), weak passwords, weak encryption schemes, a disable address space layout randomization (ASLR) feature, suspicious manipulation to a boot record, suspicious PATH, LD_LIBRARY_PATH, or LD_PRELOAD definitions, services running on startup, and the like.

Ex. 1001 '926 Patent at 6:21-32

CVE Assessments Detect Vulnerabilities, Not Stored Data Cyber Threats

926 Petition

First, Veselov teaches applying rule packages such as CVEs, which were known to identify cyber threats. EX1007, 2:22-54, 7:16-22; EX1002, ¶156 (citing EX1077, 8:1-15); *supra*, §§IX.B, XI.B.1. For example, many CVEs were associated with application features posing a threat to system security and common startup services. EX1002, ¶156 (citing EX1090; EX1091; EX1100; EX1101; EX1102; EX1103). The '926 patent identifies these types of security problems as

926 Pet. 36-37

Dr. Kaeli

(Stavrou Decl.) ¶156 (discussing Exs. 1090-1091, 1100-1103). I have reviewed Exs.1090-1091, and 1100-1103, and none of them reference “services to be run on startup,” provide any indication of what services are run on startup, and do not explain what types of security assessments will detect the particular vulnerabilities. For example, Ex.1090 is a vulnerability associated with “[T]he iax_net_read function in the iaxclient open source library,” which is listed as a “vulnerability type(s) execute code overflow.”

Vulnerability Details : [CVE-2006-2923](#)

The iax_net_read function in the iaxclient open source library, as used in multiple products including (a) LoudHush 1.3.6, (b) IDE FISK 1.35 and earlier, (c) Klax 0.8.5 and earlier, (d) DIAX, (e) Ziaxphone, (f) IAX Phone, (g) X-lite, (h) MediaX, (i) Extreme Networks ePhone, and (j) iaxComm before 1.2.0, allows remote attackers to execute

Ex. 2073 (Kaeli Decl.) ¶ 124

CVE Definitions Don't Describe Snapshot Analysis Detection

Dr. Stavrou

such assessments. EX1002, ¶¶166-67. Dr. Kaeli argues that the exemplary CVEs I discussed to illustrate that point do not “reference ‘services to be run at startup,’ provide any indication of what services are run on startup, and do not explain what types of security assessments will detect the particular vulnerabilities.” Kaeli-Dec, ¶124. But CVE definitions describe the security flaw, not the typical use case for a given piece of software or the assessments that will look for that CVE. Regardless,

926 Ex. 1400 (Stavrou) ¶ 44

“Configuration” Arguments Are Hindsight-Biased

926 Petition

EX1002, ¶157. A POSA would have understood detecting nonsecure configurations to include, or at least suggest, determining the existing of potential cyber “threats” since such configurations pose potential threats to system security.

EX1002, ¶157. This is confirmed by the '926 specification, which identifies several types of “cyber threats” based on nonsecure system configurations.

EX1001, 6:21-32 (listing, e.g., weak passwords and weak encryption schemes);

EX1002, ¶157.

926 Pet. 37



“Prior knowledge in the field of the invention must be supported by tangible teachings of reference materials, and the suggestion to combine references must not be derived by hindsight from knowledge of the invention itself.”

Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 381 F.3d 1371, 1376 (Fed. Cir. 2004)

926 Patent Refutes PO's "Configuration" Argument

926 Petition

EX1002, ¶157. A POSA would have understood detecting nonsecure configurations to include, or at least suggest, determining the existing of potential cyber "threats" since such configurations pose potential threats to system security.

EX1002, ¶157. This is confirmed by the '926 specification, which identifies several types of "cyber threats" based on nonsecure system configurations.

EX1001, 6:21-32 (listing, e.g., weak passwords and weak encryption schemes);

EX1002, ¶157.

926 Pet. 37

In yet another embodiment, the security system 140 is configured to detect cyber threats that do not represent vulnerabilities. For example, the security system 140 may detect and alert on sensitive data not being encrypted on the logical disk, private keys found on the disks, system credentials stored clearly on the disk, risky application features (e.g., support of weak cipher suites or authentication methods), weak passwords, weak encryption schemes, a disable address space layout randomization (ASLR) feature, suspicious manipulation to a boot record, suspicious PATH, LD_LIBRARY_PATH, or LD_PRELOAD definitions, services running on startup, and the like.

Ex. 1001 '926 Patent at 6:21-32

Configurations are different

relying on cooperation from VM 119 guest OS. Specifically, the security system 140 can scan and detect vulnerable software, non-secure configuration, exploitation attempts, compromised asserts, data leaks, data mining, and so on. The

Ex. 1001 '926 Patent at 4:50-53

Wiz's “Detecting Threats” Are External

926 Petition

like Veselov, Mohanty expressly teaches detecting “threats” that pose a potential risk to the assessed asset. EX1075, 3:42-67, 4:24-58, 6:64-7:13, 7:14-8:18, Figs. 2-4, claim 1; *supra*, §X.B; EX1002, ¶159. For example, Mohanty discusses a threat module that “tracks specific threats” via threat information 208, which may be provided by threat intelligence systems. EX1075, 3:55-59, 4:24-41, 6:64-7:9, 7:30-33, 9:45-49; EX1002, ¶159. The threat module determines the existence of

926 Pet. 38

ecosystem like VMware of the asset 224. Threat intelligence systems such as DEEPSIGHT provide threat information 208 about external threats. The embodiments of the system

* * *

14. The computer-readable media of claim 9, wherein: the specific asset includes a virtual machine or a virtual application, based on physical computing resources; the threat information is received from a source external to the specific asset; and

Ex.1075 (Mohanty) at 4:33-35, Claim 14

External Cyber Threats Do Not Teach Or Suggest Claimed Data Threats

[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:

- ① unencrypted sensitive data,
- ② weak passwords,
- ③ weak encryption schemes,
- ④ services to be run on startup,
- ⑤ personally identifiable information,

Ex. 1001 '926 Patent, Claim 1

Dr. Kaeli

132. Additionally, Dr. Stavrou's reliance on Mohanty's "threat information" and "threat module" fails. Ex.1002 (Stavrou Decl.) ¶¶159-160. Mohanty's threat module does not "determine" cyber threats "based on data stored on the virtual disk" as claimed. Instead, Mohanty explains that its "threat module" refers to an external "threat intelligence system" such as DEEPSIGHT that provides "information 208 *about external threats*" and "reports the latest lists" of such threats. Ex.1075 (Mohanty), 3:60-67, 4:33-36, 6:64-7:5. A POSA would have understood that references to things like an "external threat," would be in reference to risks that originate from outside of an organizations network like a known hacking group is currently targeting machines with a particular operating system (OS) using a specific exploitable vulnerability. See Ex.1075 (Mohanty), 6:64-7:5. In other words, Mohanty's threat information stems from risk external to the asset, rather than potential cyber threats present on a virtual disk, and Mohanty combines this external threat data with vulnerability data collected from its agent-based scanners in order to form its security assessment. Ex.1075 (Mohanty), 7:5-9.

Ex. 2073 (Kaeli Decl.) ¶ 132

Workloads Analyzed For Dynamic Tags, Not Sensitive Data

readily devised, consistent with the teachings herein. A first mechanism is to mark a virtual machine with a set of tags 202 such as CRITICAL DATA, WEB, INTERNET FACING, ADOBE_APP, INTERNET_EXPLORER_APP, etc. These are known as Static Tags, and have static tag information 204. A second mechanism is to mark a virtual machine with a set of dynamic tags 202 such as VIRUS FOUND, INTRUSION DETECTED, etc., by security technologies monitoring the same systems. These are known as dynamic tags or security tags, and have dynamic security related information 206. Thus, the above questions or characteristics of a virtual machine or virtual application can be defined by both static as well as dynamic tags. For example, static tag information 204 could include indication of whether there is sensitive data in or handled by the asset 224,

Ex.1075 (Mohanty) at 5:38-52

Workloads Analyzed For Dynamic Tags, Not Sensitive Data

defined by both static as well as dynamic tags. For example, static tag information 204 could include indication of whether there is sensitive data in or handled by the asset 224, whether the asset 224 includes one or more critical servers, and whether the asset is Web-connected. Dynamic tag infor-

Ex.1075 (Mohanty) at 5:50-54

situations occur. Static tags 104 have information about tag categories, i.e., each tag category could have one or more tags as information about the asset. These static tags 104 could also be referred to as operational tags, in that the static tag 104 specifies aspects of the operation of the asset. Static tag information affects the workload context 102 of the asset. Dynamic tags 106 have information that is subject to change during the lifespan of the asset. Dynamic tags 106 can also be referred to as security tags, since the changing information is of interest regarding security of the asset. Dynamic tag information affects the workload context 102 of the asset. Dynamic information and security events 108

Ex.1075 (Mohanty) at 4:9-20

Workload Context Tags Category

- Sensitive Data
- Critical Servers
- Web

Security Tags

- Virus Found
- Intrusion Detected

Dynamic Info Such
as Date Transferred.

Ex.1075 (Mohanty), Fig. 2

Sensitive Data Is Not Determined By Security Assessment

[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:

- ① unencrypted sensitive data,
- ② weak passwords,
- ③ weak encryption schemes,
- ④ services to be run on startup,
- ⑤ personally identifiable information,

Ex. 1001 '926 Patent, Claim 1

Dr. Kaeli

Although Mohanty discusses “sensitive data,” Mohanty does not suggest “analyzing” a virtual disk of a virtual cloud asset to *determine* sensitive data as required by claims 1.4, 14.4 and 15.4, and instead acknowledges that sensitive data may be tagged upon **creation** of an asset. More specifically, Mohanty’s data is a “static tag” that can be set by a virtual cloud environment (such as VMWare) when “an asset (e.g., a virtual machine or a virtual application) is created and deployed in a virtual environment.” Ex.1075 (Mohanty), 4:4-8, 4:13-15. The “static tag

Ex. 2073 (Kaeli Decl.) ¶ 133

No Combining Veselov/Mohanty To Analyze Snapshots For Tags

Dr. Stavrou

Q. You do not offer an opinion -- and if you do, please direct me to where it is in your declaration -- that Mohanty or Veselov disclose analyzing a snapshot to determine any tags; right?

A. I -- I -- a POSA would have understood that you can apply the teachings of Mohanty to Veselov and vice versa. I don't think that the goal -- so, again, while this is something that is not explicitly mentioned, a POSA would have understood that the teachings are not applied piecemeal, and you can apply teachings from one -- Mohanty, in this case -- to Veselov's scanning.

Ex. 2172 (Stavrou) 206:4-16 (objections omitted)

“Same Types Of Data” Not Enough

“Demonstrating that a reference is analogous art or relevant to the field of endeavor of the challenged patent is not sufficient to establish that one of ordinary skill would have had reason to combine its teachings with other prior art in the manner set forth in the claim....Mere compatibility of the references is likewise not sufficient.”

Johns Manville Corp. v. Knauf Insulation, Inc., IPR2018-00827, Paper 9 at 10 (P.T.A.B. Oct. 16, 2018) (informative)

Agentless Cloud Sensitive Data Detection Was Not Routine

Wiz, which has evolved from a field called CSPM (Cloud Security Posture Management). CSPM - in which another Israeli unicorn, Orca Security, operates - does not protect organizations from cyberattacks in real time, but attempts to identify and issue warnings ahead of potential infiltration into organizations' cloud systems. Such

Ex. 2154 at 2

DSPM attempts to perform a similar preventive activity, but focused on data, in a way that will add another layer of protection for what in most cases is the most vulnerable assets for organizations. The field aims at automating currently manual processes, primarily by identifying where critical information - such as customers' financial and personal information or commercial secrets - is stored in the cloud.

The field of identifying and protecting information in the cloud is relatively new, emerging only in recent years. According to a report by research firm Gartner, which identified the field as a category on the rise, less than 1% of companies around the world use a DSPM solution. Despite this, those in

Ex. 2154 at 3

22 Nov, 2022 13:29
Ofir Dor



Agentless Cloud Sensitive Data Detection Was Not Routine

Wiz VP product strategy Raaz Herzberg says the combination of CSPM and DSPM gives Wiz increased strength. "Our advantage is the ability to combine the analysis of sensitive information with the mapping we do of the entire environment. This intersection helps us give a complete picture of the risks in the cloud and to understand when the risk is immediate and requires action, as when sensitive data is involved and when the risk is secondary. This current development stems from the requests of many customers," she says.

Ex. 2154 at 1, 3

22 Nov, 2022 13:29
Ofir Dor



Limitations 1.5-1.6 Are Not Taught Or Suggested

[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,

weak passwords,

weak encryption schemes,

services to be run on startup,

personally identifiable information,

[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

Ex. 1001 '926 Patent, Claim 1

Dr. Stavrou

Q. Yeah. And so I just -- the -- in element 14.4, you analyze the snapshot to determine the potential cyber threats. And then elements like 1.5 and 1.6 are referring to the same cyber threats, like as an antecedent basis, each of the limitations is talking about the same potential cyber threats; right?

A. I don't know. I mean, I -- I do recognize that this is -- I -- I think that's probably correct, yes.

Ex. 2172 (Stavrou) at 217:4-14 (objections omitted)

Wiz Only Shows Risks For *Vulnerabilities*, Not Claimed Data Threats

926 Petition Reply

Third, PO's argument addressing the recited data types fail. Wiz addressed unencrypted sensitive data, weak encryption schemes, personally identifiable information ("PII"), weak passwords, and startup services. Pet., 38-40. As to

926 Pet. Reply 7

926 Petition

7. Elements 1.5, 14.5, and 15.5

Mohanty teaches "[determine/determining] a risk associated with each of the determined plurality of potential cyber threats," as recited, with its discussion of calculating threat scores. As explained above, the references teach identifying cyber threats via CVE assessments, and Mohanty further teaches identifying threats by correlating threat information with the asset's vulnerability data and contextual information describing data stored on the asset. EX1002, ¶¶169-70;

926 Pet. 41

926 POR 26-27; 926 POSR 11

926 Petition

8. Elements 1.6, 14.6, and 15.6

Mohanty teaches these elements, which recite "[prioritize/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." Mohanty prioritizes cyber threats with a prioritization score that indicates "the impact or severity of vulnerability, so that vulnerabilities can be prioritized as to which ones need attention or remediation." *Id.*, 6:1-6; *see also id.*, Abstract, 1:47-2:31, 3:28-42, 8:60-9:13, 10:9-11, claims 1, 9, 15, Figs. 2-4; EX1002, ¶¶173-74.

926 Pet. 41-42

Wiz Maps “Threat Scores” To Claimed Risk

Dr. Stavrou

Q. Okay. So in -- in the context of your opinions in your declaration, you're relying on the -- what Mohanty refers to as a threat score as corresponding to the claimed risk associated with each of the determined plurality of potential cyber threats; right?

A. I believe that this is a correct interpretation, and I would put the caveat that basically this is about, again, a risk of cyber threats. Yes.

Ex. 2172 (Stavrou) at 215:16-22

Threat Scores Are Relative To Vulnerabilities

926 Petition Reply

Third, PO's argument addressing the recited data types fail. Wiz addressed unencrypted sensitive data, weak encryption schemes, personally identifiable information ("PII"), weak passwords, and startup services. Pet., 38-40. As to

926 Pet. Reply 7

The threat module **308** of FIG. 3 tracks specific threats, for example by establishing a data structure in memory and populating the data structure with information about each threat reported in the threat information **208**. When the

* * *

202. Based on this correlation, the threat module **308** produces a threat score **214** for the asset **224**, relative to the vulnerability under consideration.

Ex. 1075 (Mohanty) at 7:30-33; 7:56-58

Wiz Does Not Show Alerts Based On Claimed Data Threats

[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,
weak passwords,
weak encryption schemes,
services to be run on startup,
personally identifiable information,

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

'926 Patent, Claim 1

Dimension#2—Threat (e.g., threats received from Threat Intelligence systems such as DeepSight). Related data could include threat impact, impacted CVE ID, type of threat, operating system impacted, applications impacted, etc.

Ex.1075 (Mohanty) at 3:55-59

926 Reply

Third, PO's argument addressing the recited data types fail. Wiz addressed unencrypted sensitive data, weak encryption schemes, personally identifiable information ("PII"), weak passwords, and startup services. Pet., 38-40. As to

926 Reply 7

926 Petition

First, Mohanty teaches or suggests including prioritization information in the alerts. Mohanty discusses sending "a message, a report, an alert or a file, etc." for higher-risk cyber threats. EX1075, 9:11-26; EX1002, ¶180. These alerts can have "various formats and include various types of information," including "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." EX1075, 9:16-26 (emphasis added); *see also id.* 3:55-59 (listing types of threat data) 4:33-

926 Pet. 43

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds) 30

**Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds) 52**

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Wiz's Two Theories

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

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

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

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

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

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

'809 Patent, Claim 1

809 Petition

5. Elements 1.3, 16.3, and 19.3

* * *

Veselov discloses two general ways to perform the analysis, each of which satisfies the previously discussed construction of “[analyzing/analyze] the snapshot.” EX1007, 8:30-45 (scanning service may “determine whether to reconstitute an active duplicate virtual machine instance or to analyze the snapshot as a data file”), 10:1-16 (describing types of analyses); *supra*, §VIII.B (construction). First, the scanning service can instantiate a duplicate/assessment VM from the snapshot and analyze this VM. EX1007, 3:54-61, 12:1-20 (same);

* * *

Second, the scanning service can mount the snapshot as a data file and directly analyze the snapshot data. *Id.*, 3:61-67 (scanning service may mount logical

809 Pet. 34-35

Wiz's Element 1.5-1.8 Require Analyzing VM, Not Snapshot

809 Petition

7. Elements 1.5, 16.5, and 19.5

The combination of Veselov and Mohanty teaches these elements, which recite “[correlating/correlate] the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset.” Veselov’s analysis considers the target VM’s network properties. EX1007, 9:55-67 (snapshot may include “configurations of network protocols and services” and “properties of connections to other computing resources”), 15:41-16:14 (snapshot may capture communications/connections), 21:3-23 (analyzing telemetry data), claims 2, 5; EX1002, ¶¶161-62. Consistent with Veselov’s general disclosures, Mohanty

809 Pet. 38

uniform. The “state” of the target resource represented by the snapshot data may include any properties of the target resource instantiated in the computing resource service provider 104 that are relevant to the security assessment. 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.

* * *

In some embodiments, the scanning service 310 can cause processing activity to occur within the assessment virtual machine 312A-B in order to apply tasks of the security assessment to real-time dynamic or static data, network connections, communications to computing resources, and other computational activities of the assessment virtual machine 312A-B. In order to stimulate activity that mirrors

* * *

with the first virtual machine instance. The computer-executable instructions upon execution may further cause the system to: install a security agent program within the second virtual machine instance, the security agent program configured to, upon execution, collect telemetry data of the second virtual machine instance, the telemetry data indicating network activity, file system activity, or processing activity, and send the telemetry data to the system; receive the telemetry data for a duration of the security assessment; and, analyze the telemetry data using assessment rules to produce the first assessment result.

Ex. 1007 (Veselov) at 9:55-67; 15:41-48; 21:3-13

Wiz's Element 1.5-1.8 Require Analyzing VM, Not Snapshot

809 Petition

7. Elements 1.5, 16.5, and 19.5

The combination of Veselov and Mohanty teaches these elements, which recite “[correlating/correlate] the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset.” Veselov’s analysis

considers the target VM’s network properties. EX1007, 9:55-67 (snapshot may include “configurations of network protocols and services” and “properties of connections to other computing resources”), 15:41-16:14 (snapshot may capture communications/connections), 21:3-23 (analyzing telemetry data), claims 2, 5;

EX1002, ¶¶161-62. Consistent with Veselov’s general disclosures, Mohanty

809 Pet. 38

2. The system of claim 1, wherein the computer-executable instructions upon execution by the processor further cause the system to:

install a security agent program within the second virtual machine instance, the security agent program configured to, upon execution:

collect telemetry data of the second virtual machine instance, the telemetry data indicating network activity, file system activity, or processing activity; and send the telemetry data to the system; receive the telemetry data for a duration of the security assessment; and analyze the telemetry data using assessment rules to produce the first assessment result.

* * *

5. The system of claim 1 wherein said performing the security assessment on the second virtual machine instance includes:

intercepting network traffic directed to the first virtual machine instance and routing the intercepted network traffic to the first virtual machine instance; analyzing the intercepted network traffic and generating a traffic profile describing characteristics of the intercepted network traffic; generating simulated network traffic including characteristics described by the traffic profile; directing the simulated network traffic to the second virtual machine instance; generating a partial assessment result for the first virtual machine instance by analyzing behavior of the second virtual machine instance in response to the simulated network traffic; and including the partial assessment result in the first assessment result.

Ex. 1007 (Veselov), Claims 2, 5

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable Expectation Of Success (REOS) Combining Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud Management Console" For "The Location Of A Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Wiz's Theory Applied Basavapatna Directly To Veselov

326 Petition

XI. GROUND 1: CLAIMS 1-21 AND 28 WERE OBVIOUS OVER VESELOV AND BASAVAPATNA

The combination of Veselov and Basavapatna teaches or suggests all limitations of claims 1-21 and 28 as a whole. Veselov describes locating a

* * *

Basavapatna further discusses determining a risk of the vulnerabilities, determining a risk level to the cloud computing environment of each asset, and reporting the assets prioritized by their associated risk level. *Supra*, §X.B. A POSA had reason to combine Veselov and Basavapatna to, for example, perform snapshot-based security assessments, as taught by Veselov, while further applying Basavapatna's teachings involving identification of vulnerabilities, determining risk levels, and prioritizing/reporting vulnerabilities and assets accordingly. EX1002, ¶104; *infra*, §XI.A.

326 Pet. at 20-21

Wiz's Theory Applied Basavapatna Directly To Veselov

326 Petition

¶¶121, 140). The combination uses these techniques to predictably perform their known functions since the references describe analogous security assessments, and applying Basavapatna's techniques in snapshot-based VM assessments would not meaningfully change their function or result. EX1007, 4:1-4, 9:55-67; EX1002, ¶108.

326 Pet. 22

Wiz's Risk Determination Is Basavapatna Alone

326 Petition

1. Preambles

To the extent the preambles are limiting, Veselov teaches them. Claim 1

* * *

2. Element 18.i

Veselov teaches this element, which recites “at least one processor

* * *

3. Elements 1.1, 15.1, and 18.1

Veselov, alone or in combination with Basavapatna, teaches these elements,

* * *

a. Elements 1.2.a, 15.2.a, and 18.2.a

These elements recite “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.” Veselov teaches these elements.

* * *

b. Elements 1.2.b, 15.2.b, and 18.2.b

Veselov teaches these elements, which recite “accessing, based on the

* * *

c. Elements 1.2.c, 15.2.c, and 18.2

Veselov, alone or in combination with Basavapatna, teaches “analyzing the

* * *

d. Elements 1.2.d, 15.2.d, and 18.2.d

Basavapatna teaches “determining a risk associated with each of the

* * *

5. Elements 1.3, 15.3, and 18.3

The combination teaches these elements, which recite “for each of the

* * *

6. Elements 1.4, 15.4, and 18.4

The combination of Veselov and Basavapatna teaches these elements, which

326 Pet. at 24-36

Wiz Relies On Basavapatna's Vulnerability And Threat Metrics

**No reference
to combination**

326 Petition

d. Elements 1.2.d, 15.2.d, and 18.2.d

Basavapatna teaches “determining a risk associated with each of the determined potential cyber vulnerabilities,” as recited, in its vulnerability-centric and threat-centric assessments.

Basavapatna teaches determining a vulnerability-centric risk metric for each vulnerability on a given asset. EX1008, ¶¶99-113, Fig. 3B. This risk metric is based on a “standard vulnerability score” and a “composite vulnerability score.” *Id.*, ¶¶100, 101-02, 106, 112, Fig. 3B; *see also id.*, ¶¶103, 113. The vulnerability-

* * *

Basavapatna similarly teaches determining a threat-centric risk metric for each threat that exploits one or more vulnerabilities detected on the asset. EX1008, ¶¶73-98, Fig. 3A. The threat-centric risk metrics are “associated” with the detected vulnerabilities since they are based on vulnerability scores that estimate “whether the asset possesses a particular vulnerability.” *Id.*, ¶¶83-85; EX1002, ¶¶164-65.

326 Pet. at 33

Vulnerability/Threat Metrics Require Host/Network Sensors

Dr. Kaeli

97. Two things are therefore clear from Basavapatna's disclosure: to determine risks associated with vulnerabilities and assets and provide those teachings, Basavapatna: (1) installs agents on target assets (i.e., computing devices); and (2) relies upon execution and activity of its target assets (e.g., sending or receiving information over a network).

Ex. 2073 (Kaeli Decl.) at ¶ 97

Vulnerability-Centric Risk Metric Requires Countermeasure Score C

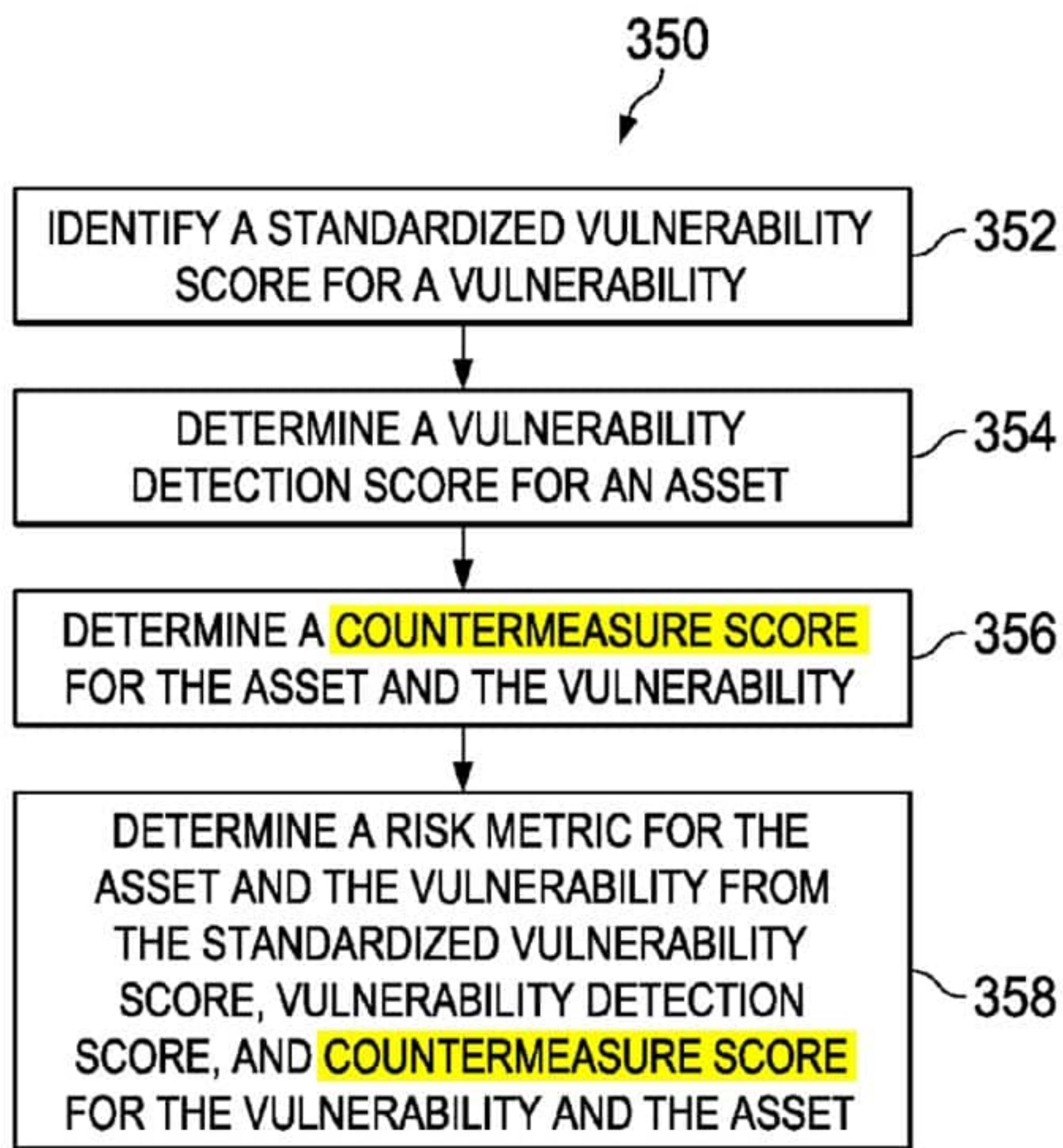


FIG. 3B

Ex. 1008 (Basavapatna), Fig. 3B

[0112] The process 350 determines a risk metric for the asset and the vulnerability from the composite vulnerability score V_C and the countermeasure score C (358). In some implementations, the system determines the risk metric by dividing the composite vulnerability score V_C by the countermeasure score C, such that the vulnerability-centric risk metric can be calculated as follows:

$$\frac{V_C}{C}$$

in instances where a CVSS standardized vulnerability score is used, the vulnerability-centric risk metric can be calculated as:

$$\frac{BX_T(X_{CDP}X_{TD}X_{CIA})V_D}{C}$$

Ex. 1008 (Basavapatna) at ¶¶ 112, 99-100

Threat-Centric Risk Metric Requires Countermeasure Score C

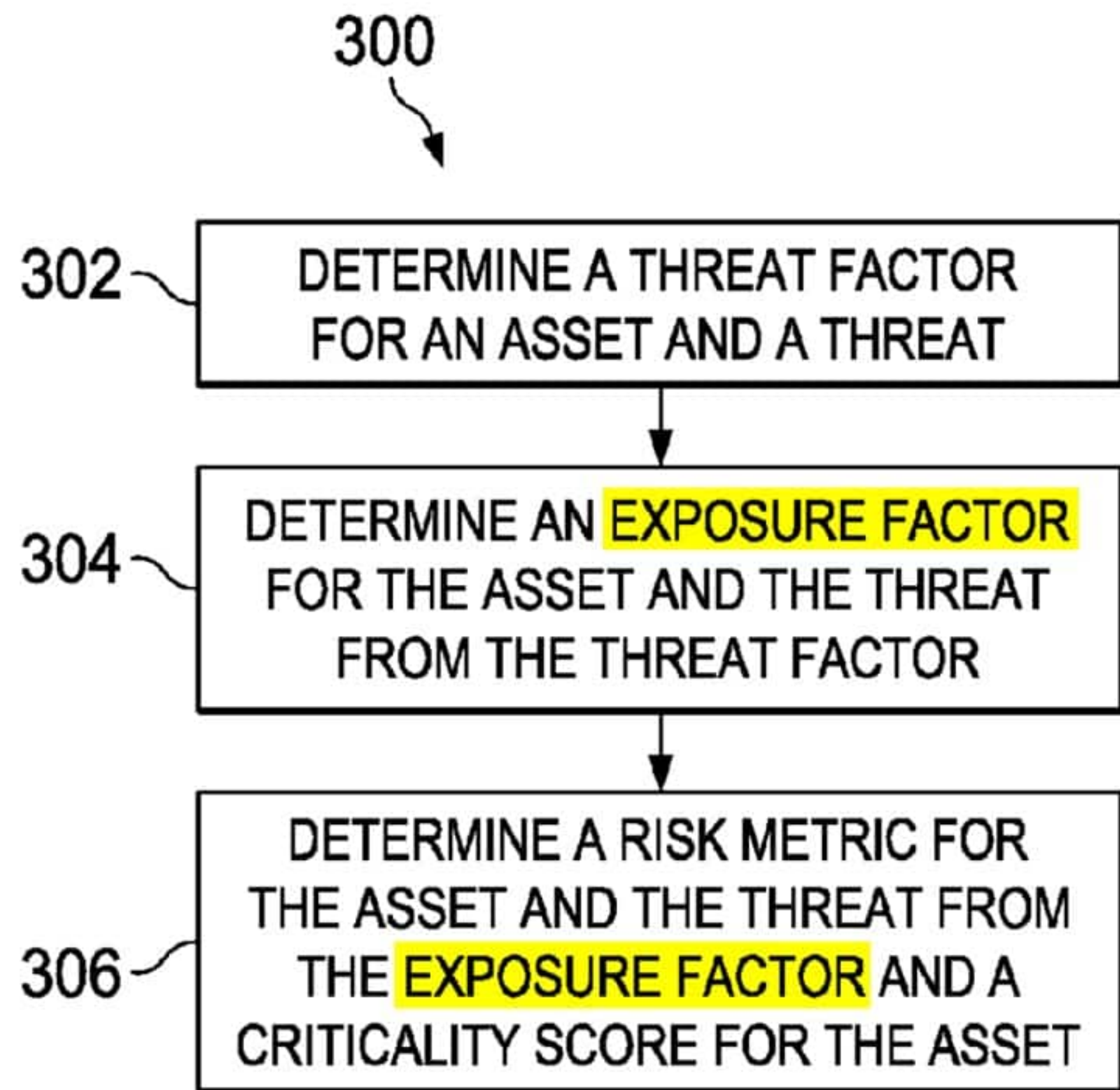


FIG. 3A

Ex. 1008 (Basavapatna), Fig. 3a

the asset and the threat (304). The exposure factor E estimates the risk that an asset will be affected by the threat, and is derived from the threat factor T, a vulnerability score V, and a countermeasure score C. In some implementations, the expo-

$$E = \frac{TV}{C}$$

Ex. 1008 (Basavapatna) at ¶ 82

Countermeasure Score C Requires Host And Network Sensors

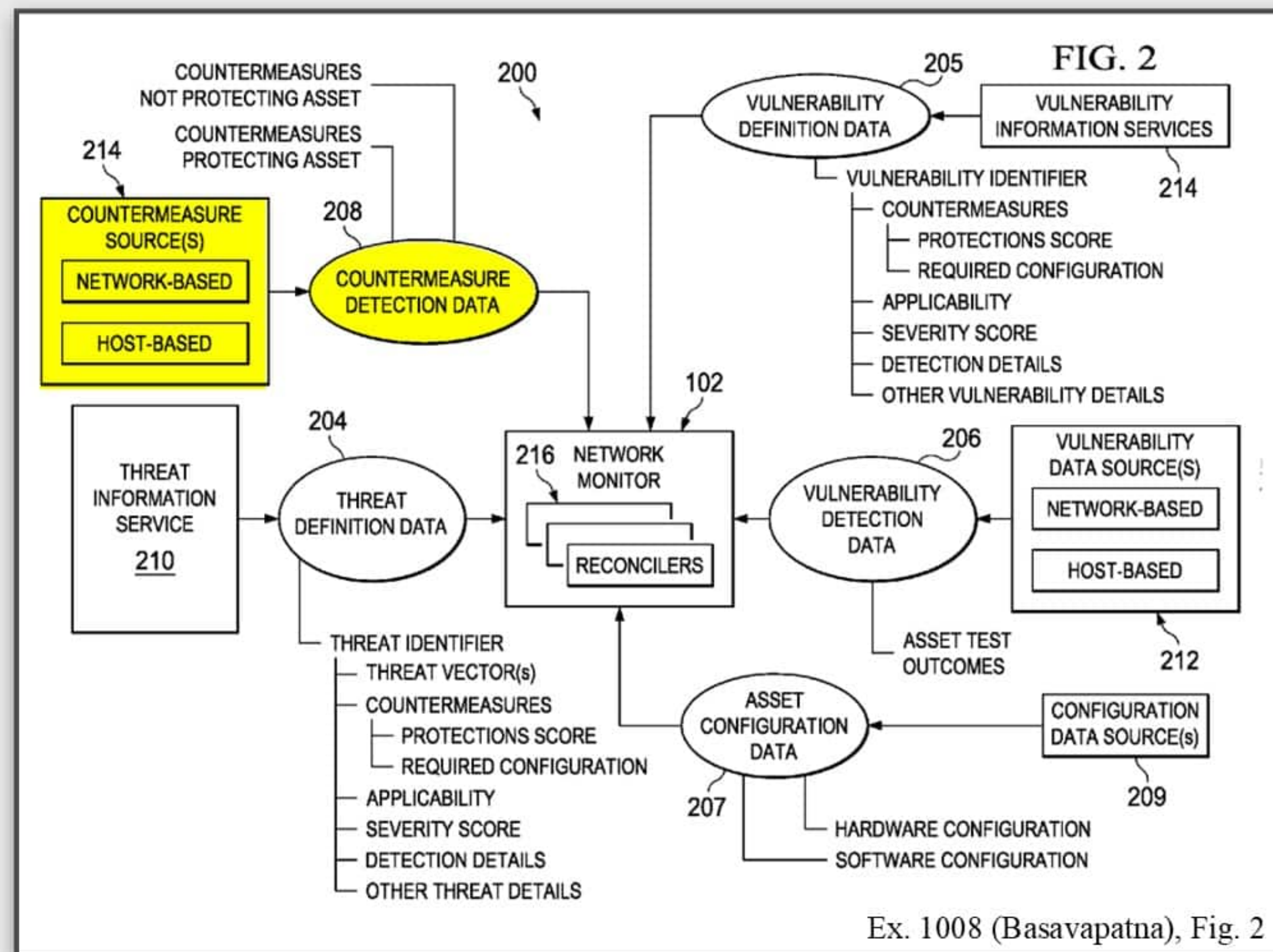
[0063] §2.1.5 Countermeasure Detection Data

[0064] The countermeasure detection data 208 is received from countermeasure source(s) 214. In general, the countermeasure detection data 208 specifies, for a given asset, what countermeasures are in place to protect the asset. In some

Ex. 1008 (Basavapatna) at ¶¶ 63-64, 66

[0023] Passive countermeasures can be provided by two kinds of sensors: host-based sensors 108 and network-based sensors 110. The host-based sensors 108 and the network based sensors 110 monitor the assets themselves and/or network traffic to and from the assets. For illustrative purposes, the sensors are described below as both monitoring the assets and protecting the assets by providing one or more countermeasures. However, the monitoring and countermeasure

Ex. 1008 (Basavapatna) at ¶ 23



Ex. 1008 (Basavapatna), Fig. 2

No REOS: Host Sensors Cannot Be Used With Analyzing Snapshots

Dr. Stavrou

Q. When Veselov discusses analyzing the snapshot itself as a data file, Veselov does not disclose installing an agent on the snapshot; correct?

A. **I don't think that an agent can be installed on a snapshot. I think an agent can only be installed on a virtual machine.**

Ex. 2172 (Stavrou Dep.) at 53:14-20

No REOS: Network Sensors Cannot Be Used With Analyzing Snapshots

Dr. Stavrou

Q. It would not be possible to send or communicate packets or other messages to a snapshot as a data file; right?

A. It's not through the data file. It doesn't have active processing.

Ex. 2172 (Stavrou Dep.) at 256-257

“How The Combination” Works Is Required – And Missing From The Petition



“Indeed, the Board nowhere clearly explained, or cited evidence showing, how the combination of the two references was supposed to work. At least in this case, such a clear, evidence-supported account of the contemplated workings of the combination is a prerequisite to adequately explaining and supporting a conclusion that a relevant skilled artisan would have been motivated to make the combination and reasonably expect success in doing so.”

Pers. Web Techs., LLC v. Apple, Inc., 848 F.3d 987, 994 (Fed. Cir. 2017) (internal citation/quotation omitted)

Wiz's Rehabilitation Attempts Fail

326 Reply

PO claims Basavapatna's data is "inextricably tied" to host/network-based sensors POR, 17-18; EX1400, ¶¶17, 20. But the record confirms that equivalent data—files, applications, configurations, etc.—is included and readily analyzed in Veselov's snapshot. Pet., 20-23, 46-47; EX1007, 3:20-4:4, 7:16-22, 9:55-10:16;

image 508 same as 308); EX1400, ¶22. Previous descriptions similarly describe the same robust content of the snapshot used in both approaches. EX1007, 3:20-4:4, 9:14-10:16; EX1400, ¶22. Veselov describes an additional way to use stored activity/connection data in the 3A/B analysis, but the underlying data is still stored in the snapshot. EX1007, 15:50-59 (snapshot taken during "capture period")

326 Reply 4-5

Veselov Confirms Different Inspection Techniques Have Different Data

original. In other embodiments, the assessment virtual machine 312A-B may be “non-viable,” in that it cannot perform material operations of the original virtual machine 312. A predominant cause of non-viability is that the virtual machine 312 performs requisite operations on dynamic data, the sources of which cannot be captured in the snapshot data (i.e., the volume image 308) without violating the data integrity. Security assessments may nonetheless be performed on a non-viable assessment virtual machine 312A-B if the assessments themselves evaluate only the static data associated with the original virtual machine 312.

Ex.1007 (Veselov) at 14:2-12

In some embodiments, the scanning service 310 can cause processing activity to occur within the assessment virtual machine 312A-B in order to apply tasks of the security assessment to real-time dynamic or static data, network connections, communications to computing resources, and other computational activities of the assessment virtual machine 312A-B. In order to stimulate activity that mirrors

Ex.1007 (Veselov) at 15:41-47

implementations of FIGS. 5A-B, rather than recreating and instantiating a duplicate VM, the scanning service 510 is configured to analyze the volume image 508 as a data file. The scanning service 510 may transform the volume image 508 into a format in which the scanning service 510 can read the copied files and other data; in the illustrated examples, the scanning service 510 does this by mounting the volume image as a virtual storage device.

Ex.1007 (Veselov) at 17:1-8

instance that was imaged. At step 614, the scanning service may perform the security assessment by reading the files of 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

Ex.1007 (Veselov) at 18:32-38

Wiz's Rehabilitation Attempts Fail

326 Reply

PO claims Basavapatna's data is "inextricably tied" to host/network-based sensors. POR, 17-18; EX1400, ¶¶17, 20. But the record confirms that equivalent data—files, applications, configurations, etc.—is included and readily analyzed in Veselov's snapshot. Pet., 20-23, 46-47; EX1007, 3:20-4:4, 7:16-22, 9:55-10:16;

Seventh, PO fails to rebut Wiz's expectation-of-success showing. PO's also Kaeli-Transcript, 75:19-81:25. Moreover, Wiz's dependent-claim analysis identifies specific risk information available and readily used in Veselov's assessment. Pet., 38-40 (external intelligence), 44-48 (application-use determinations that include checking application configuration files); EX1400, ¶¶28, 30-33.

326 Reply at 4, 7

326 Petition

7. Claim 8
* * *
-46- -47- -48-
326 Pet.

326 Petition

5. Claim 6
* * *
-44- -45-
326 Pet.

Wiz, Inc.
Argenti (margenti@wsgr.com)
Rosato (mrosato@wsgr.com)
Werryberry (werryberry@wsgr.com)
Thomas (tthomas@wsgr.com)
Willargeon (jbaillargeon@wsgr.com)
SINI GOODRICH & ROSATI
11 Road
A 94304

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

Case IPR2024-01191
Patent No. 11,775,326

PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 11,775,326

Board Not Obligated To Cobble Wiz's Arguments Together



While the Board should review a petition holistically, it is not obligated to cobble together assertions from different sections of a petition or citations of various exhibits in order to infer every possible permutation of a petitioner's argument.

Netflix, Inc. v. DIVX, LLC, 84 F. 4th 1371 (Fed. Cir. 2023) (internal citation/quotation omitted)

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting “Querying A Cloud
Management Console” For “The Location Of A
Virtual Disk” (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Challenged Claims

13. The method of claim 1,

[1.1] wherein locating 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 of the respective protected virtual cloud asset.

Ex. 1001 '926 Patent, Claim 13

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

* * *

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

'809 Patent, Claims 15, 22

14. The method of claim 1, wherein determining the location of the snapshot of at least one virtual disk further includes querying a cloud management console of the cloud computing environment for the location of the snapshot and the location of a specific virtual disk of the respective protected virtual cloud asset.

'326 Patent, Claims 14

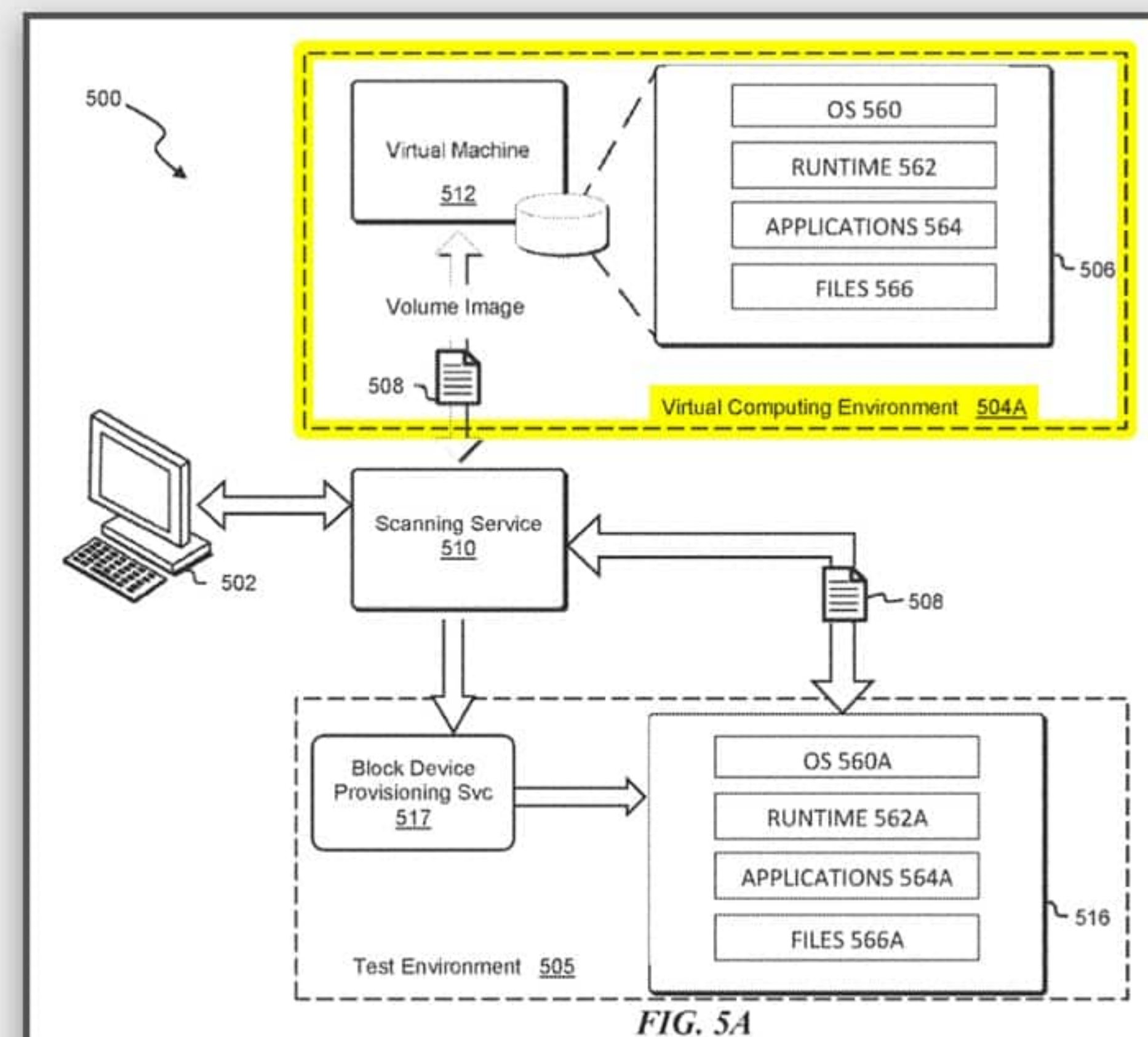
Figures 5A/5B: Computing Environment Not Implemented By Computing Resource Service Provider

FIGS. 5A-B illustrate example computing environments 500, 550 providing additional embodiments of the present security assessment systems. The examples again use a

Ex.1007 (Veslov) at 16:56-58

implementations of FIGS. 5A-B, rather than recreating and instantiating a duplicate VM, the scanning service 510 is configured to analyze the volume image 508 as a data file.

Ex.1007 (Veslov) at 17:1-3



Ex.1007 (Veslov), Fig. 5A

Combining Embodiments Requires Motivation



“all of the limitations are found in two separate embodiments pictured side by side in the patent, not in one embodiment ... We agree with Cordis that one of ordinary skill in the art **would have been motivated to combine the embodiment** in figure 3B of Wolff with the embodiment in figure 4 of Wolff to arrive at a metal stent with two coating layers.”

Bos. Sci. Scimed, Inc. v. Cordis Corp., 554 F.3d 982, 991 (Fed. Cir. 2009)

Petitioner further argues that: Given the interchangeable nature taught for various features of Wang’s embodiments, it would have been a routine and obvious matter for a POSA to combine aspects from Wang’s various embodiments. ... We determine that these reasons are inadequate and too generic to satisfy Petitioner’s burden as they lack a clear explanation of what and how “aspects from Wang’s various embodiments” are proposed to be combined along with reasoning specific to that proposal. ... It is not enough for Petitioner to allege that all of the elements of the challenged claims can be found somewhere in the various embodiments of Wang.

Tesla, Inc. v. Graphite Charging Co., IPR2024-00388, Paper 49 at 34-40 (Aug. 19, 2025)

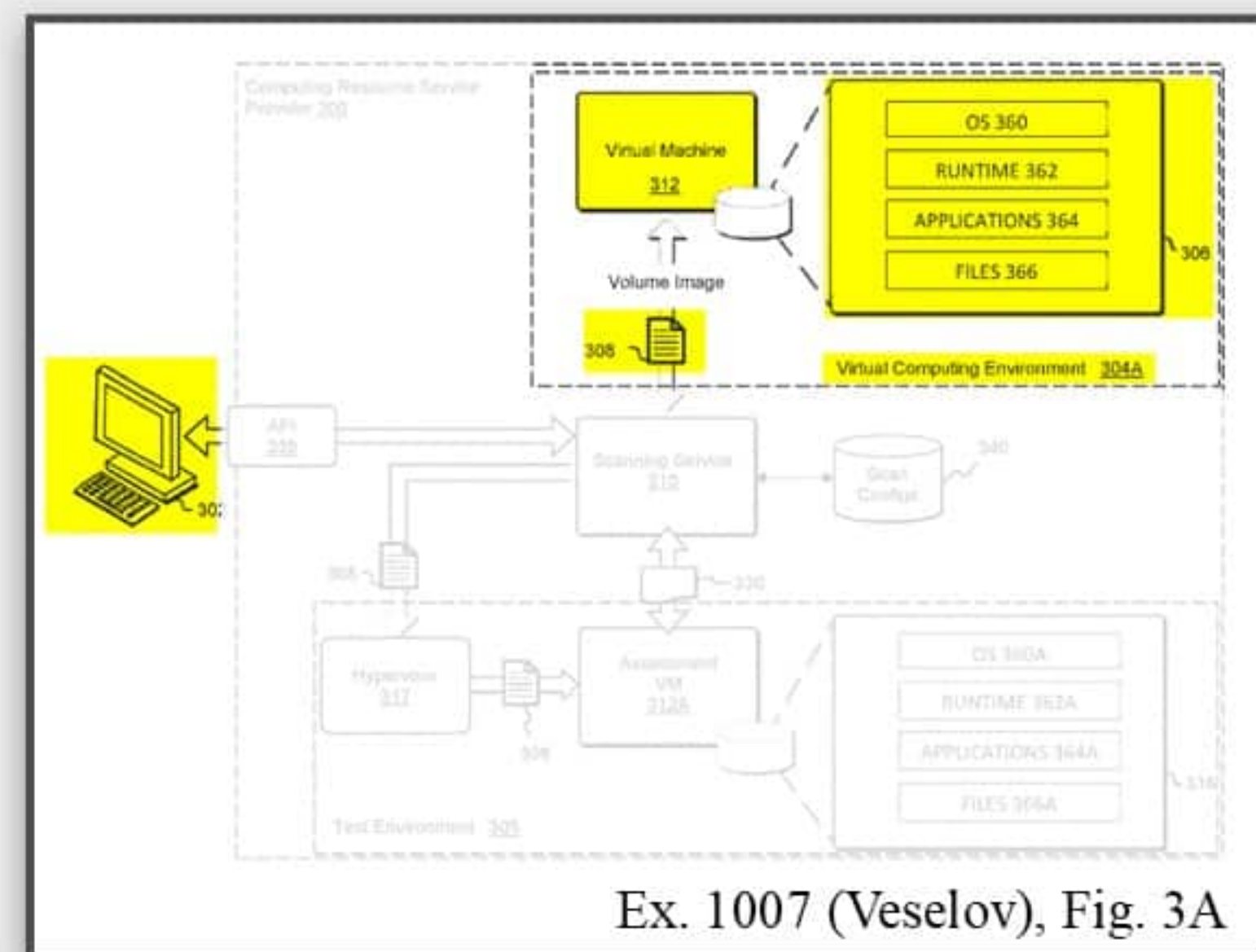
The **court’s analysis in *Boston Scientific* indicates that adjacent placement alone is not sufficient.** Accordingly, the fact that Yano describes the fifth embodiment shown in Figure 5 immediately after discussing the fourth embodiment shown in Figure 4 is not by itself sufficient to show a reason or motivation to combine the features of those embodiments in the manner set forth by Petitioner. ... In particular, we are not persuaded that Petitioner’s reliance on *Boston Scientific* overcomes its lack of explanation as to why a POSITA would have combined the different embodiments depicted in Figure 4 and Figure 5. **It is not sufficient to demonstrate that each of the components in a challenged claim is known in the prior art; Petitioner must also explain why a POSITA would have combined the elements disclosed in the separate embodiments described in Yano.**

Intel Corp. v. Tela Innovations, Inc., IPR2019-01520, Paper 64 at 23-26 (Mar. 9, 2021)

Wiz Does Not Rely On Common Features

security assessment systems. The examples again use a virtual machine **512** as the example target computing resource of the security assessment; the user device **502**, virtual computing environment **504A**, logical volume **506** (with virtual machine **512** operating system **560**, runtime environment **562**, software applications **564**, and files/file 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**, **304A**, **306**, **308**, **312**, **360-366** of FIGS. 3A-B. In the

Ex. 1007 (Veselov) at 16:45-67



Ex. 1007 (Veselov), Fig. 3A

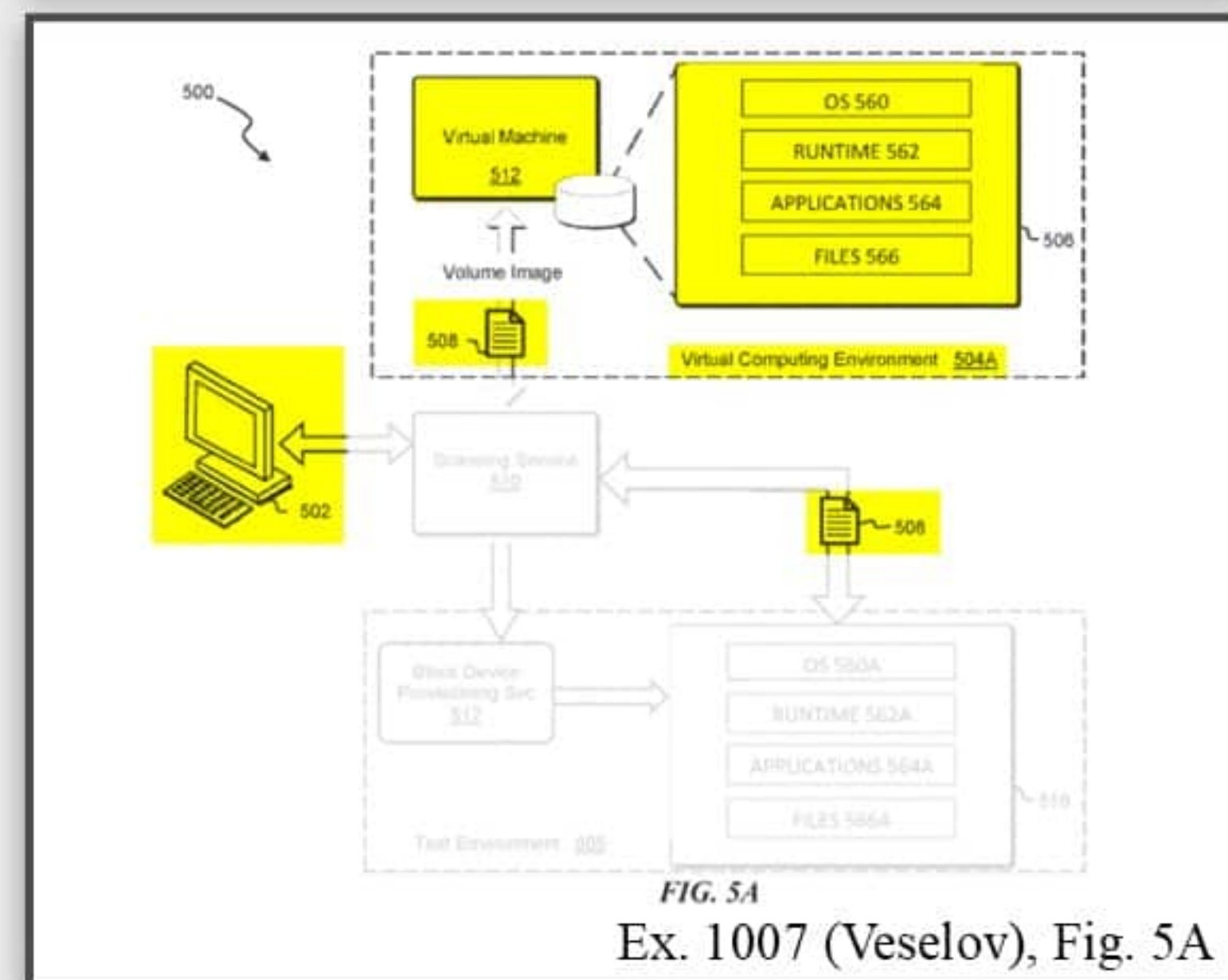


FIG. 5A

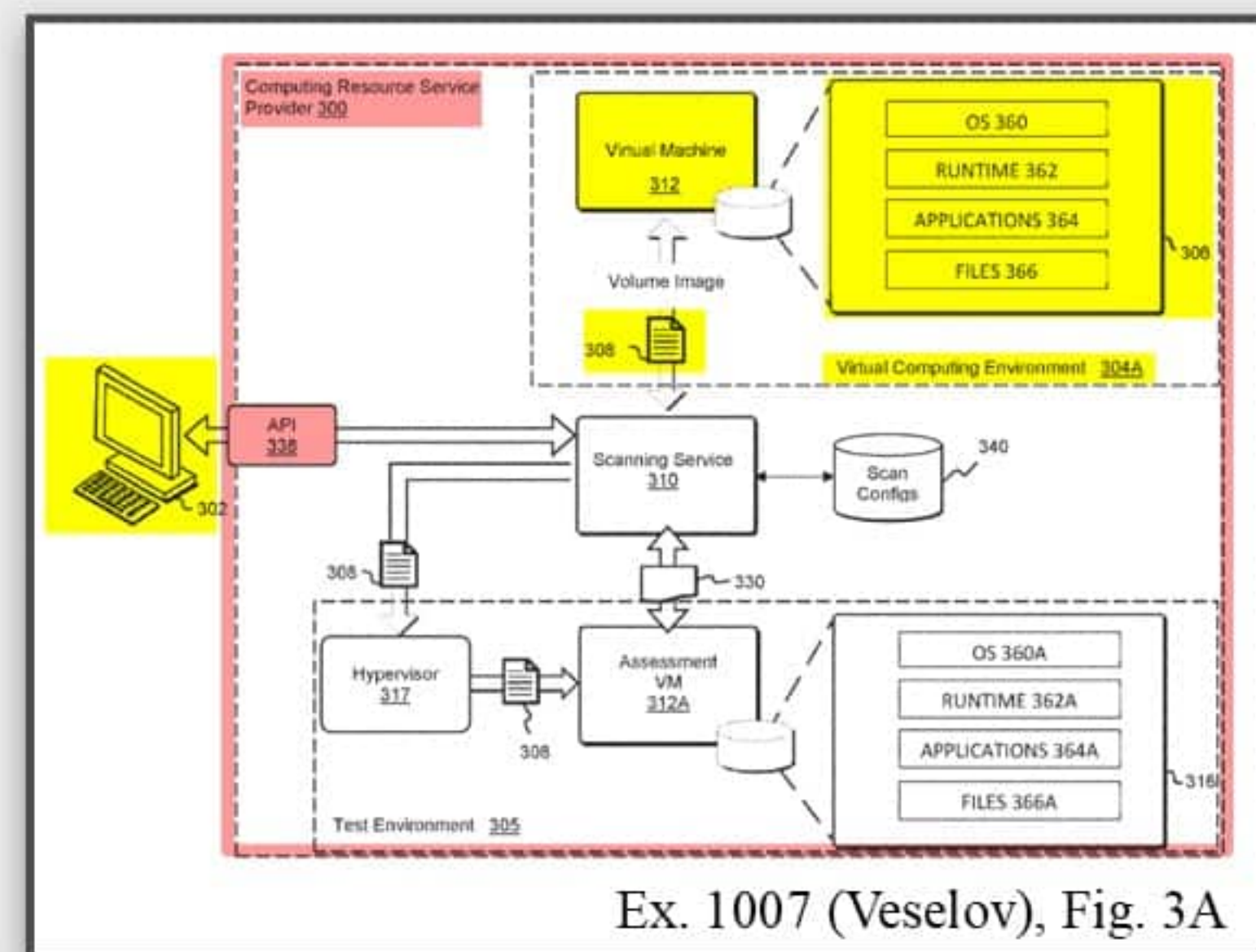
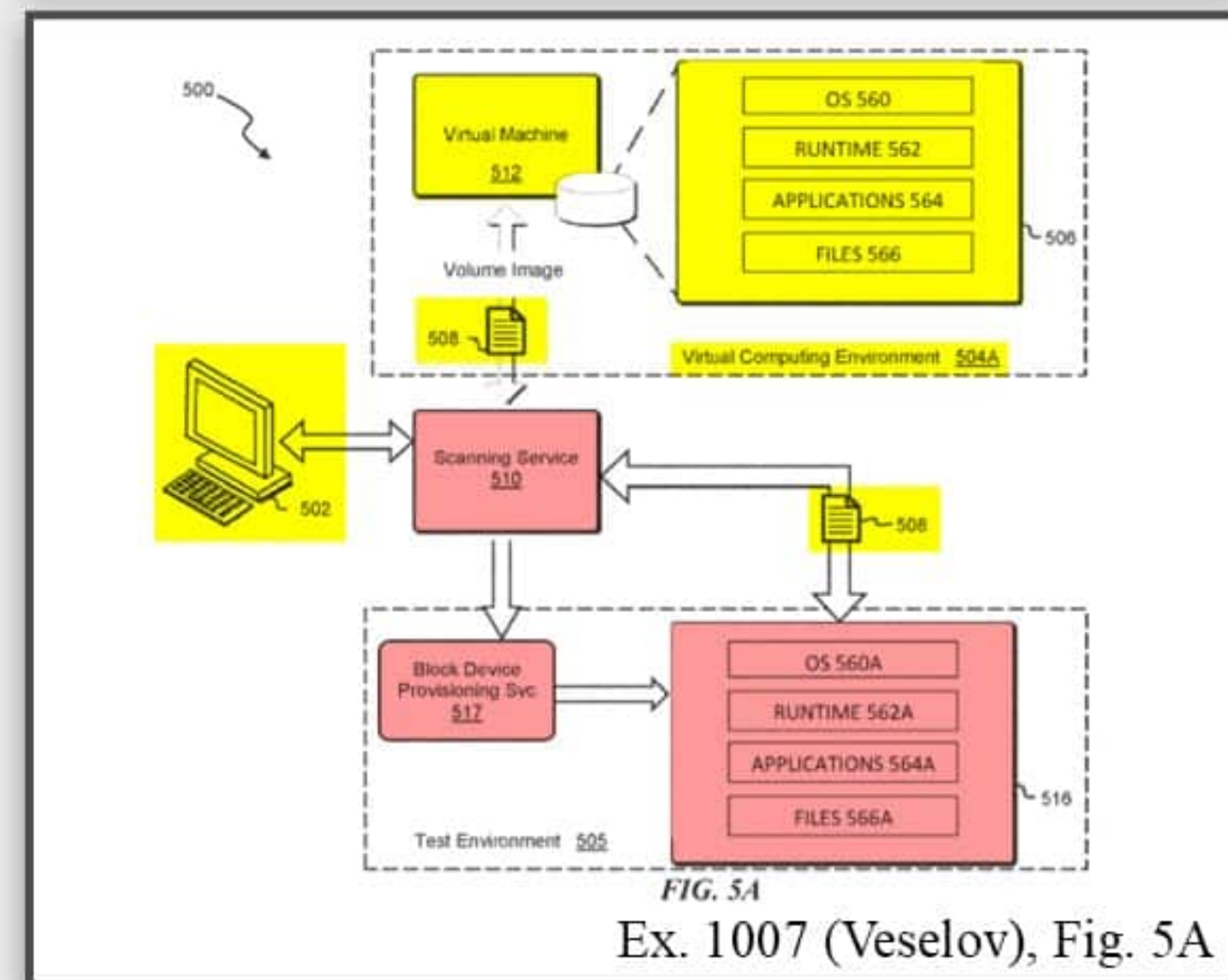
Ex. 1007 (Veselov), Fig. 5A

Wiz Does Not Rely On Common Features

926 Petition

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 recognized that API-mediated interactions between the scanning service and the virtualization layer of the target VMs were equally applicable to those embodiments. EX1002, ¶¶226-27 (citing EX1015, 164-66; EX1020, Abstract, 21:42-22:58).

926 Pet. 54



Undepicted Encryption Key Storage Unrelated

The scanning service **510** may mount volume images as read only to avoid inadvertently modifying the volume corresponding to a volume image. A public key or other cryptographically verified information may be applied to the volume image **508** to verify the identity and authenticity of the data. In addition, the volume image **508** may be encrypted and the scanning service **510** may require access to the encryption key to perform the analysis. The encryption key may be maintained in a security module or security service (not shown) of the computing resource service provider. In these embodiments, the scanning service **510** gains access to the key by obtaining credential information from the user and may also obtain key identification information if necessary. Alternatively, the user may maintain the key and provide the scanning service **510** with the key.

Ex. 1007 (Veselov) at 18:1-15

Veselov Does Not Identify Or Locate Virtual Disks

Dr. Stavrou

Q. Are you aware of any other place anywhere else in Veselov Exhibit 1007, where it identifies or describes an identifier for a virtual disk?

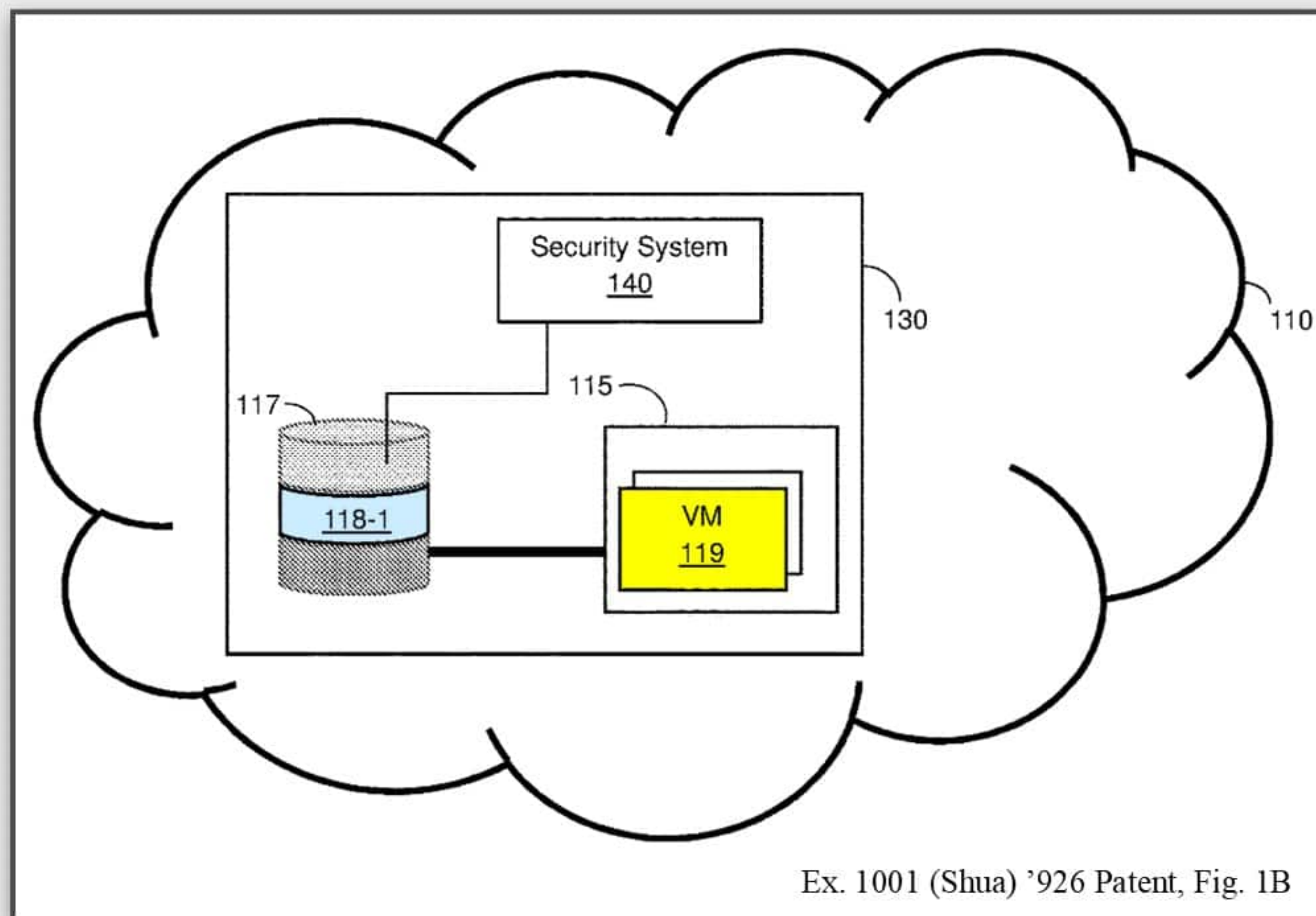
A. I'd have to look at it more carefully. I'm not -- I haven't searched the entire patent about the virtual disk identifier keyword.

Q. Okay. Without reading the whole patent, you're not aware of one as you sit here now that you can point me to. You're just saying you're not sure there isn't one; is that fair?

A. That's fair.

3/5/2025 Stavrou Tr. at 142:15-143:3

VMs And Virtual Disks Have Different Locations

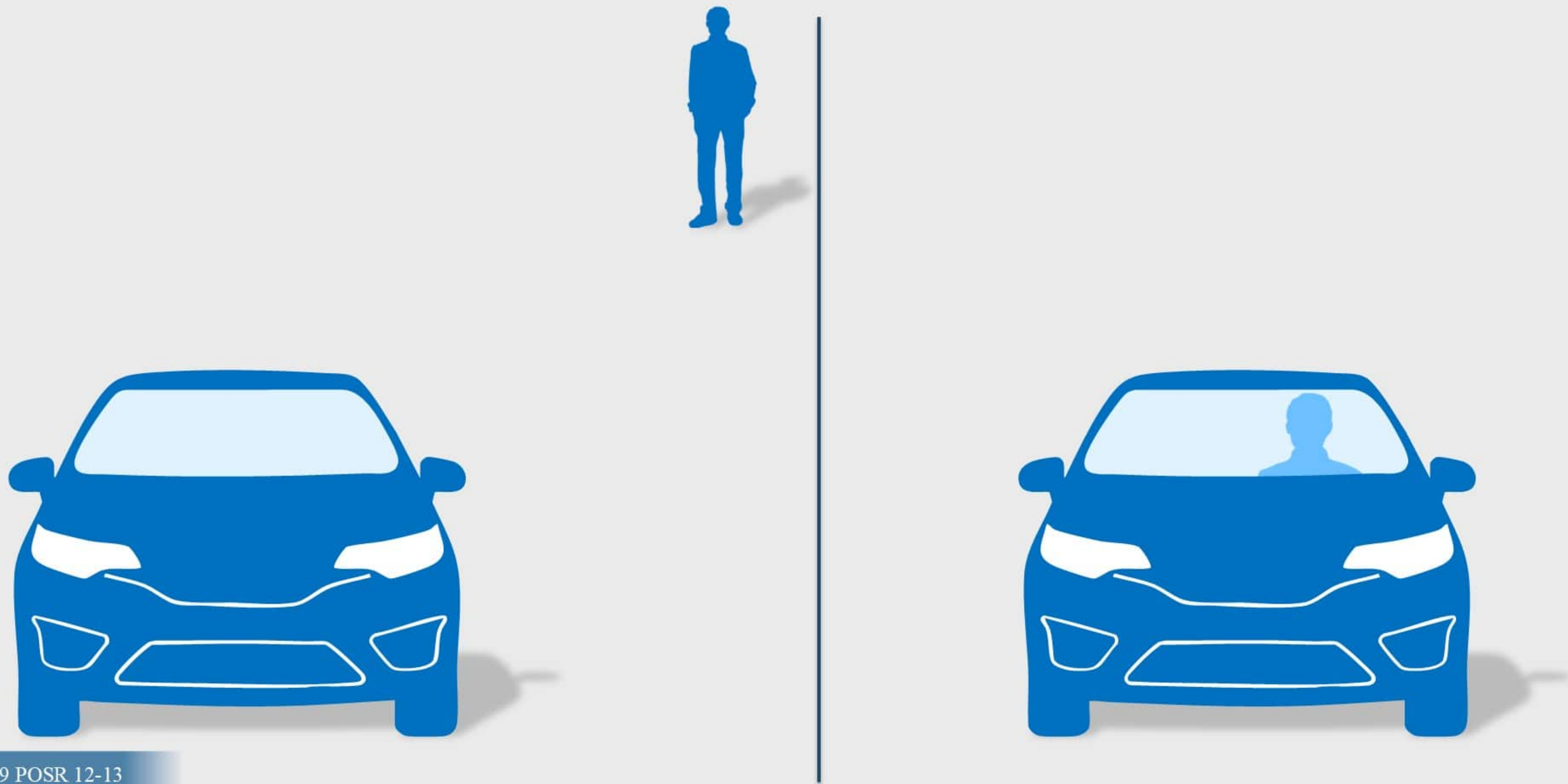


Ex. 1001 (Shua) '926 Patent, Fig. 1B

The storage 117 emulates virtual discs for the VMs executed in by the server 115. The storage 117 is typically connected to the server 115 through a high-speed connection, such as optic fiber allowing fast retrieval of data. In other configurations, the storage 117 may be part of the server 115. In this example illustrated in FIG. 1B, virtual disk 118-1 is allocated for the VM 119. The server 115, and hence the VM 119, may be executed in a client environment 130 within the platform 110.

Ex. 1001 (Shua) 926 Patent at 3:55-63

VM Identifier Is Not Disk Location



809 POSR 12-13

Wiz's Laundry List Of Alternative Theories Fail

926 Petition

see also id., 5:1-5, 5:59-60. Managing security computer resources, as taught by Veselov, also **routinely involved** querying consoles to determine resource locations. EX1002, ¶230 (citing EX1009, 221, 257-60; EX1015, 56, 124, 164-66, EX1031, 1 (Executive Summary), ii, 1-4; EX1074, 10, 12).

926 Pet. 56



“Although the Board twice stated that ‘board 5 could have been used to prevent twisting of core 1 by one with ordinary skill in the art exercising ordinary creativity,’...it did not stop there—and properly so, because **obviousness concerns whether a skilled artisan not only could have made but would have been motivated to make** the combinations or modifications of prior art to arrive at the claimed invention.”

Belden Inc. v. Berk-Tek LLC, 805 F.3d 1064, 1073 (Fed. Cir. 2015)

809 POR 31; 926 Pet.
56; 926 POR 30-33;
326 POR 30-31

Wiz's Laundry List Of Alternative Theories Fail

926 Petition

environment); EX1002, ¶231; *supra*, §XI.C.7. Veselov also teaches using the UI/API to display and configure aspects of the assessment, including selection of the assessment target (e.g., the virtual disk). EX1007, 4:19-48, 8:52-62 (target resource may be logical volume), 11:28-33 (logical volume known as virtual disk drive), 11:34-67 (snapshot may be volume image of logical volume containing VM), 14:37-63 (configuration/display of assessment information); *see also id.*, 16:27-44; EX1002, ¶232. At a minimum, querying the console to determine the

926 Pet. 56

Mixing embodiments; no need to “query” location of disk if already known

Wiz's Laundry List Of Alternative Theories Fail

926 Petition

nevertheless obvious. Veselov shows the snapshot and its associated virtual disk initially located in the same computing environment, which at least suggests that querying the console to generally locate the snapshot (e.g., virtualization layer) would also determine the virtual disk's general location. EX1007, Figs. 3A-B, 5AB (image 308/508 and logical volume 306/506 in same computing environment); EX1002, ¶231; *supra*, §XI.C.7. Veselov also teaches using the

926 Pet. 56

**Relying solely on figures
and conflating
snapshot/disk location**



“Qualcomm failed to put forth any argument or evidence in its petitions as to whether Nozawa’s device, even if capable of doing so, actually would output a periodic signal with a plurality of integer-multiple harmonics, or why a person of ordinary skill in the art would have been motivated to use the particular inputs that would result in such an output”

ParkerVision, Inc. v. Qualcomm Inc., 903 F.3d 1354, 1363 (Fed. Cir. 2018)

Table of Contents

Introduction

2

Objective Indicia (809/926/326 All Grounds)

87

Claim Construction (809/926/326 All Grounds)

9

926 Ground 2

191

No Motivation To Combine (MTC) Or Reasonable Expectation Of Success (REOS) Combining Veselov And Mohanty (809/926 All Grounds)

17

809 Ground 2

201

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.4-1.7 (926 All Grounds)

30

326 Ground 3

206

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.5-1.8 (809 All Grounds)

52

926 Grounds 3-4

209

No MTC Or REOS Combining Veselov And Basavapatna (326 All Grounds)

56

809 Grounds 3-4

212

No Teaching/Suggesting "Querying A Cloud Management Console" For "The Location Of A Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14)

72

Motion to exclude

216

Wiz's Combination References

Veselov et al.

- (54) SECURITY ASSESSMENT OF VIRTUAL COMPUTING ENVIRONMENT USING LOGICAL VOLUME IMAGE
- (71) Applicant: Amazon Technologies, Inc., Seattle, WA (US)

Czarny et al.

- (54) COMPUTER SECURITY VULNERABILITY ASSESSMENT
- (71) Applicant: OPSWAT, Inc., San Francisco, CA (US)

Basavapatna et al.

- (54) CALCULATING QUANTITATIVE ASSET RISK
 - * * *
- (73) Assignee: McAfee, Inc.

Mohanty

- (54) METHOD AND SYSTEM TO PRIORITIZE VULNERABILITIES BASED ON CONTEXTUAL CORRELATION
- (71) Applicant: Symantec Corporation, Mountain View, CA (US)

HUTCHINS et al.

- (54) OFFLOADING OPERATIONS TO A REPLICATE VIRTUAL MACHINE
- (71) Applicant: VMWARE, INC., Palo Alto, CA (US)

Ranum et al.

- (54) SYSTEM AND METHOD FOR STRATEGIC ANTI-MALWARE MONITORING
- (71) Applicant: Tenable Network Security, Inc., Columbia, MD (US)

SEO

- (54) SECURITY ENHANCEMENT METHOD AND ELECTRONIC DEVICE THEREFOR
- (71) Applicant: Samsung Electronics Co., Ltd., Suwon-si (KR)

Giakouminakis et al.

- (54) METHODS AND SYSTEMS FOR IMPROVED RISK SCORING OF VULNERABILITIES
 - * * *
- (73) Assignee: RAPID7 LLC, Newton, MA (US)

Wiz's "Background" Art

Rosendahl et al.

(54) VERTICALLY INTEGRATED AUTOMATIC THREAT LEVEL DETERMINATION FOR CONTAINERS AND HOSTS IN A CONTAINERIZATION ENVIRONMENT

(71) Applicant: NeuVector, Inc., Milpitas, CA (US)

Crabtree et al.

(54) SYSTEM AND METHODS FOR SANDBOXED MALWARE ANALYSIS AND AUTOMATED PATCH DEVELOPMENT, DEPLOYMENT AND VALIDATION

(71) Applicant: QOMPLX, Inc., Reston, VA (US)

LUTAS et al.

(54) DUAL MEMORY INTROSPECTION FOR SECURING MULTIPLE NETWORK ENDPOINTS

(71) Applicant: Bitdefender IPR Management Ltd., Nicosia (CY)

(54) METHOD AND SYSTEM FOR IDENTIFICATION OF SECURITY VULNERABILITIES

(72) Inventor: LI, David
Reston, Virginia 20190 (US)

Ammons et al.

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

(73) Assignee: INTERNATIONAL BUSINESS MACHINES CORPORATION, Armonk, NY (US)

Burdett et al.

(54) CLOUD STORAGE SCANNER

(71) Applicant: Sophos Limited, Abingdon (GB)

Sancheti et al.

(54) INFORMATION MANAGEMENT OF VIRTUAL MACHINES HAVING MAPPED STORAGE DEVICES

(71) Applicant: CommVault Systems, Inc., Oceanport, NJ (US)

Ackley

(54) TRANSLATING MEDIA ACCESS CONTROL (MAC) ADDRESSES IN A NETWORK HIERARCHY

(71) Applicant: Rackspace US, Inc., San Antonio, TX (US)

Milner et al.

(54) DETECTION OF MALICIOUS SOFTWARE PACKAGES

(71) Applicant: Red Hat, Inc., Raleigh, NC (US)

(54) SYSTEM AND METHOD FOR DETECTING VULNERABILITY STATE DELTAS

(71) Applicant: Qualys, Inc., Redwood Shores, CA (US)

Kirti et al.

(54) TECHNIQUES FOR DISCOVERING AND MANAGING SECURITY OF APPLICATIONS

(71) Applicant: Oracle International Corporation, Redwood Shores, CA (US)

Loureiro et al.

(54) METHOD FOR DETECTING VULNERABILITIES IN A VIRTUAL PRODUCTION SERVER OF A VIRTUAL OR CLOUD COMPUTER SYSTEM

(71) Applicant: SecludIT, Valbonne (FR)

Vorbach

(54) ADVANCED PROCESSOR ARCHITECTURE

(71) Applicants: Martin Vorbach, Lingenfeld (DE); Hyperion Core, Inc., Los Gatos, CA (US)

Epstein

(54) REORGANIZATION OF VIRTUALIZED COMPUTER PROGRAMS

(73) Assignee: Cisco Technology, Inc., San Jose, CA (US)

Rubin et al.

(54) METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS

(73) Assignee: Finjan, Inc., San Jose, CA (US)

Adams et al.

(54) OUT-OF-BAND CONTENT ANALYSIS

(71) Applicant: HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP, Houston, TX (US)

Canzanese, JR. et al.

(54) SYSTEMS AND METHODS FOR ALERT PRIORITIZATION USING SECURITY EVENTS GRAPH

(71) Applicant: Netskope, Inc., Santa Clara, CA (US)

Chari et al.

(54) SANITIZATION OF VIRTUAL MACHINE IMAGES

(71) Applicant: International Business Machines Corporation, Armonk, NY (US)

Wysopal et al.

(54) ASSESSMENT AND ANALYSIS OF SOFTWARE SECURITY FLAWS IN VIRTUAL MACHINES

(73) Assignee: Veracode, Inc., Burlington, MA (US)

Bezbaruah et al.

(54) EFFICIENTLY PROVIDING VIRTUAL MACHINE REFERENCE POINTS

(71) Applicant: MICROSOFT TECHNOLOGY LICENSING, LLC, Redmond, WA (US)

Michael et al.

(54) USING ANTIMALWARE TECHNOLOGIES TO PERFORM OFFLINE SCANNING OF VIRTUAL MACHINE IMAGES

(73) Assignee: Microsoft Corporation, Redmond, WA (US)

Hibbert et al.

(54) SYSTEMS AND METHODS OF RISK BASED RULES FOR APPLICATION CONTROL

(71) Applicant: BeyondTrust Software, Inc., Phoenix, AZ (US)

Khalid et al.

(54) SUSCEPTIBLE ENVIRONMENT DETECTION SYSTEM

(71) Applicant: FireEye, Inc., Milpitas, CA (US)

Budko et al.

(54) INTELLIGENT SECURITY CONTROL SYSTEM FOR VIRTUALIZED ECOSYSTEMS

(73) Assignee: HyTrust, Inc., Mountain View, CA (US)

+80 more

Continental Can Co. USA v. Monsanto



The district court concluded that the structure in suit is simply a variation on known themes. It is in such circumstance that the objective indicia—the so-called secondary considerations—are most useful to the decision-maker. The significance of a new structure is often better measured in the marketplace than in the courtroom.

Cont'l Can Co. USA v. Monsanto Co., 948 F.2d 1264, 1273 (Fed. Cir. 1991)

Ex. 2120: Forbes

Subscribe To Newsletters

Forbes

Subscribe: Less than \$150/yr

Sign In

More From Forbes

Mar 16, 2025, 12:40pm EDT

AI Agents Need To Be Managed As If They are Human

Mar 16, 2025, 10:00am EDT

The AI Graveyard: 7 Deadly Mistakes That Kill Most Enterprise AI Projects

Mar 16, 2025, 10:50am EDT

From Strategy To Success: How Process Drives 828 Growth

Mar 11, 2025, 10:40am EDT

AI Digital Twins: Your City's Edge In A World Of Unprecedented Change

us bank

ignite growth.

We can help prepare you for the next opportunity with expert advice.

INNOVATION > ENTERPRISE TECH

The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

By Louisa Columbus, Former Contributor

Nov 28, 2020, 05:00am EST

Share

Save

This article is more than 4 years old.



Orca Security - Orca Security is noteworthy for its innovative approach to providing instant-on, workload-deep security for AWS, Azure and GCP without the gaps in agents' coverage and operational costs. Orca integrates cloud platforms as an interconnected web of assets, prioritizing risk based on environmental context. Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords and unsecured PII.

Cybersecurity, privacy and security startups have raised \$10.7 billion so far this year, five times more than was raised throughout 2010 (\$1.7 billion), according to a Crunchbase Pro query today.

22,156 startups who either compete in or rely on cybersecurity, security and privacy technologies and solutions as a core part of their business models today, 1,450 of which have received pre-seed or seed funding in the last twelve months based on a Crunchbase Pro query

From network and data security to I.T. governance, risk measurement and policy

Document title: The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

Capture URL: https://www.forbes.com/sites/louisacolumbus/2020/11/29/the-top-20-cybersecurity-startups-to-watch-in-2021-based-on-crunchbase

Capture timestamp (UTC): Wed, 19 Mar 2025 18:16:37 GMT

The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

Orca Security - Orca Security is noteworthy for its innovative approach to providing instant-on, workload-deep security for AWS, Azure and GCP without the gaps in agents' coverage and operational costs. Orca integrates cloud platforms as an interconnected web of assets, prioritizing risk based on environmental context. Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords and unsecured PII.

Ex. 2120 at 7

809 POSR 32; 926 POSR 33; 326 POR 44-45

91

PROTECTIVE ORDER MATERIAL - DEMONSTRATIVE EXHIBIT - NOT EVIDENCE

Ex. 2120: Forbes

Subscribe To Newsletters

Forbes

Subscribe: Less than \$150/yr

Sign In

More From Forbes

Mar 16, 2025, 12:40pm EDT

AI Agents Need To Be Managed As If They are Human

Mar 16, 2025, 10:00am EDT

The AI Graveyard: 7 Deadly Mistakes That Kill Most Enterprise AI Projects

Mar 16, 2025, 10:50am EDT

From Strategy To Success: How Process Drives B2B Growth

Mar 11, 2025, 10:40am EDT

AI Digital Twins: Your City's Edge In A World Of Unprecedented Change

us bank

ignite growth.

We can help prepare you for the next opportunity with expert advice.

INNOVATION > ENTERPRISE TECH

The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

By Louisa Columbus, Former Contributor

Nov 28, 2020, 05:00am EST

Share

Save

This article is more than 4 years old.



Orca Security

Cybersecurity, privacy and security startups have raised \$10.7 billion so far this year, five times more than was raised throughout 2010 (\$1.7 billion), according to a Crunchbase Pro query today.

22,156 startups who either compete in or rely on cybersecurity, security and privacy technologies and solutions as a core part of their business models today, 1,450 of which have received pre-seed or seed funding in the last twelve months based on a Crunchbase Pro query

From network and data security to I.T. governance, risk measurement and policy

Document title: The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

Capture URL: https://www.forbes.com/sites/louiscolumbus/2020/11/29/the-top-20-cybersecurity-startups-to-watch-in-2021-based-on-crunchbase

Capture timestamp (UTC): Wed, 19 Mar 2025 18:16:37 GMT

Page 1 of 11



The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

Orca Security - Orca Security is noteworthy for its innovative approach to providing instant-on, workload-deep security for AWS, Azure and GCP without the gaps in agents' coverage and operational costs. Orca integrates cloud platforms as an interconnected web of assets, prioritizing risk based on environmental context. Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords and unsecured PII.

809+326

809+326

809

926

Ex. 2120 at 7

Pivotal Moments in Cloud

* * *

809+326+926

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

Ex. 2076 at 7

Ex. 2076: The Redefining CNAPP Guide

How Agentless Scanning Emerged

809+326+926

As discussed earlier, Orca launched the first version of agentless side scanning, which allowed deep visibility into cloud workloads without the need to install agents.

Subsequently, Wiz was able to make the experience more intuitive with the graph and more fully bring the approach to market. There's a lot you can do without an agent, and with most security teams already overwhelmed by that work, it's hard to argue they're looking for even more to do.

Ex. 2076 at 11

Ex. 2076: The Redefining CNAPP Guide

Pros

- **Quick deployment and rapid-time to value:** Agentless solutions are easier to deploy since they do not require installing software on each workload. They leverage cloud APIs to snapshot underlying instance hard disks, copy them into the security vendors account, where they're hooked up on the vendor's side and scanned. This creates an elegant "like magic" approach - where you get full visibility into the workload, without any instrumentation.

809+326+926

Ex. 2076 at 11-12

Ex. 2076: The Redefining CNAPP Guide

Orca Security made a big leap in cloud security with the introduction of its patented agentless SideScanning technique in 2019. This innovation introduced workload visibility without needing security teams to install an agent on endpoints or installing software on workloads for assessments.

They operate out-of-band by accessing cloud workloads at the runtime storage level, gathering crucial data through the cloud provider's APIs, while scanning disk snapshots. Their technology evaluates block storage bytes and reconstructs file systems, scans operating systems, and applications in a read-only mode, ensuring that virtual assets remain unaffected. This unique method allows companies to deploy Orca across their entire cloud environment without worrying about performance impacts or operational disruptions. For security teams, this means getting visibility into engineering workloads, without needing to bother them at all along the way.

809+326+926

Ex. 2076 at 31

“Patented” And “Patent-Pending” Refers To 809, 926, 326 Patents

Mr. Shua

16. As an initial matter, I note that in virtually all of Orca’s early marketing materials and presentations about its technology, Orca emphasized that its SideScanning™ used “patent-pending” techniques. And, until April 26, 2021, Orca did not have any pending patent applications other than those claiming priority to the ’718 Provisional Application discussed above. So “patent-pending” references in Orca’s marketing materials, presentations, and other documents from before April 2021 necessarily referred to the inventions described and claimed in the ’718 Provisional Application’s patent family, including the ’926 Patent. I discuss

926 Ex. 2074 (Shua Decl.) ¶16; *see also* 809 Ex.2074 ¶16; 326 Ex.2074 ¶16

Orca Has Received Numerous Awards For SideScanning

THE **CHANNEL** CO.
CRN

Forbes



Gartner
**COOL
VENDOR
2022**

 security current

aws

SC
Media

 **Redpoint.**

REDACTED

REDACTED

REDACTED

REDACTED

Nexus



“a nexus analysis need not be limited to a discussion of only novel features. It is instead important to consider ‘the invention as a whole,’ rather than on a ‘limitation-by-limitation’ basis.”

Volvo Penta of the Americas, LLC v. Brunswick Corp., 81 F.4th 1202, 1212 (Fed. Cir. 2023) (internal citations omitted)

Direct Nexus



We may also consider whether the patent owner proved a nexus independently of a presumption. ... As the Board found, these documents “clearly reference[] the Forward Drive that Patent Owner argues—and Petitioner does not dispute—practices the claims of the ’692 patent” and “discuss[] the objective of delivering a ‘comparable forward facing stern drive’ with ‘capabilities that match the Volvo Penta Forward Drive.’ ” ... The documents cited in its Response further demonstrate the connection between these claim elements and the objective evidence of nonobviousness.

Volvo Penta of the Americas, LLC v. Brunswick Corp., 81 F.4th 1202, 1211 (Fed. Cir. 2023)

Direct Nexus: Evidence Generally Referring To Claim Limitations



Patent Owner submits the testimony of Mr. Wexler, who explains: “I have been in many situations where for a variety of reasons there have been *RF dropouts and in some cases the wireless on the talent has moved way out of range [P]rior to Zaxcom’s invention, the audio would be lost forever in these situations.*” PO Resp. 54 (citing Ex. 2104 ¶ 6) (emphasis added). That is, Mr. Wexler refers generally to the prevention of dropouts and lost audio, i.e., the “replacing” limitation. See Section III.C. Mr. Wexler’s testimony has probative value in establishing that the asserted objective evidence is tied to the proposed substitute claims.

Lectrosonics, Inc. v. Zaxcom, Inc., IPR2018-01129, Paper 33 at 62 (Jan. 24, 2020) (precedential)

“Strong” Direct Nexus: Evidence Specifically Referring To Limitations



PO Resp. 54–56 (citing Ex. 2103 ¶¶ 3, 4–7; Ex. 2104 ¶¶ 6–7). Mr. Sarokin and Mr. Wexler refer specifically to the “replacing” limitation of the ’902 patent recited by the proposed substitute claims. For instance, Mr. Wexler states that each “transmitter can digitally record the output of the microphone along with transmitting the signal to the receiver. If there is a drop out of the RF signal, the identical recording in the transmitter can be used by post production.” Ex. 2104 ¶ 6. In other words, a dropout causing an issue with remotely recorded audio can be fixed by “replacing” the remotely recorded audio with local audio data from a recording transmitter. We determine that this evidence is strongly probative in establishing that the asserted objective evidence is tied to the invention recited in the proposed substitute claims.

Lectrosonics, Inc. v. Zaxcom, Inc., IPR2018-01129, Paper 33 at 63 (Jan. 24, 2020) (precedential)

Unclaimed Features Not Relevant To Direct Nexus



Although we agree with Petitioner that Patent Owner provides some evidence of industry praise directed to features not explicitly recited by proposed substitute claims 21–26, we are persuaded that Patent Owner provides evidence of industry praise related to the “replacing” limitation that specifically addresses dropouts. *See* PO Resp. 54–59. The evidence of features that are not recited by proposed substitute claims 21–26 weighs neither for nor against nonobviousness. However, the testimonial evidence

Lectrosonics, Inc. v. Zaxcom, Inc., IPR2018-01129, Paper 33 at 69-70 (Jan. 24, 2020) (precedential)

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Orca Showed Nexus Patent-By-Patent

809 POR

billion. Ex.2112, 1-2; Ex.2139, 1; Shua^{¶¶}109-111. These funding announcements again demonstrated how Orca's commercial success was attributable to the inventions claimed in the '809 Patent. Ex.2113, 1 ("Orca Security's patent-pending SideScanning™ technology collects data directly from cloud provider APIs and the workload's runtime block storage out-of-band" and detects "vulnerabilities"), 4 (Orca "[p]rioritize[s] risk based on the severity of the underlying security issue, its accessibility, and business impact" and reports issues as "alerts"), 3 ("Orca Security's rapid emergence as a cloud security leader is driven by customer love for its product.").

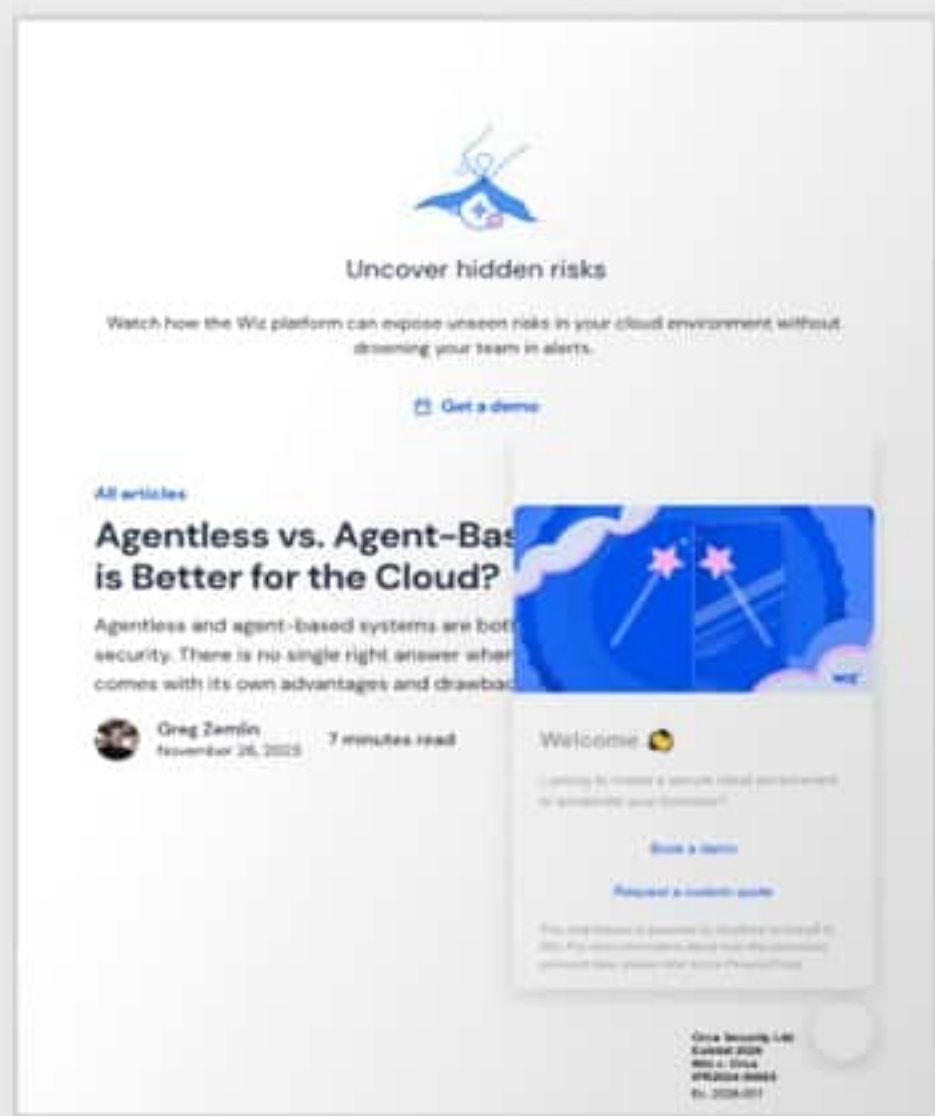
809 POR 65-66

926 POR

These funding announcements highlight Orca's commercial success is attributable to the cloud computing provider API-based techniques for analyzing snapshots for cyber threats stored on virtual disks, such as sensitive data, in the '926 Patent. Ex.2113, 1 ("Orca Security's patent-pending SideScanning™ technology collects data directly from cloud provider APIs and the workload's runtime block storage out-of-band" and detects "misplaced PII"), 3 (praise from industry), 4 (Orca "[p]rioritize[s] risk" and reports issues as "alerts.").

926 POR 59-60

Agentless Scanning Has Nexus To 809, 926 And 326 Claims



Agentless analysis approaches are based on two fundamental principles:

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

Ex. 2026 at 3

[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 ...

'926 Patent, Claim 1

[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;

'809 Patent, Claim 1

[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

'326 Patent, Claim 1

Wiz's IPRs Assert Agentless Scanning Well-Known Before Orca

926 Reply

evidence relates exclusively to unrecited and/or known features. Most evidence merely addresses “agentless” scanning, yet PO does not show this is recited, and it was known. *E.g.*, EX1002, ¶¶57, 88-89; EX1040, Abstract, ¶¶8-12, 23, 43-48, 52;

* * *

But the alleged solution—agentless scanning—was known. *Newell Companies*,

* * *

PO’s skepticism arguments fail. Most evidence relates exclusively to “agentless” scanning, but this unrecited aspect was known. *POR*, 39-40; EX2076,

* * *

connection is insufficient. *POR*, 42-43; EX1400, ¶109. Quoted statements relate exclusively to known/unrecited features such as the “agentless approach”

* * *

agentless scanning involves cloud APIs and sensitive-data detection is irrelevant since that was known. EX2076, 11-12; EX1400, ¶¶85-88, 92-94. *Additional*

926 Reply at 19, 20, 22, 23, 24

REDACTED

Wiz's Contradictory/Shifting Positions

**Petitions
acknowledged
claims required
agentless analysis:**

**Replies
unsuccessfully
disavow earlier
explicit statements:**

326 Petition

c. Elements 1.2.c, 15.2.c, and 18.2

* * *

data. EX1007, 3:61-67, 8:30-45, 17:10-29; EX1002, ¶156. Consistent with well-known security-assessment techniques, neither of these analysis techniques in Veselov uses an agent installed on the target VM, nor do they require an agent installed on the assessment VM. *Supra*, §X.A; EX1002, ¶157 (citing EX1040,

326 Pet. 31-32

326 Reply

patent” lacked nexus to claims); *supra*, §VI.A. Regardless, the evidence relates exclusively to unrecited and/or known features. Most evidence merely addresses “agentless” scanning, yet PO does not show this is recited, and it was known. *E.g.*,

326 Reply 18

Dr. Stavrou's Stonewalling

Dr. Stavrou

Q. Is there any aspect of the claims of the '809 patent that relate or correspond to cloud APIs?

A. I don't understand the -- your -- the meaning of the word "correspond." Can you please explain to me? I see the language of the claims in front of me, but I don't understand your use of the word "correspond."

Ex. 2195 (Stavrou 9.24.25) 101:10-19 (objection omitted)

Dr. Stavrou's Contradictory Testimony

Dr. Stavrou

Q. And then for the '032 patent, the cloud API limitations are 1.1 and 1.2?

A. Let me just confirm.

A. Again, to the extent that -- it depends on I use them for at least those locations that you mentioned, yes.

Ex. 2197 (Stavrou 8.19.2025) 113:22-113:7 (objections omitted)

[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 at least one virtual disk;

'032 Patent, Claim 1

Dr. Stavrou

Q. For the '926 patent, the cloud API limitations are limitations 1.2 and 1.3; right?

A. I disagree. The way that you pose the question is incorrect.

Ex. 2195 (Stavrou 9.24.25) 102:16-24 (objections omitted)

[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;

Ex. 1001 '926 Patent, Claim 1

Long-Felt Need

Pivotal Moments in Cloud

* * *

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

Ex. 2076 at 7

Ex. 2076: The Redefining CNAPP Guide

Deployment options for cloud security (Agent vs Agentless)

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

Ex. 2076 at 8



We also determine that the Board failed to properly evaluate long-felt but unresolved need. ... Volvo Penta cites an article in a 2015 issue of Boating World magazine, which describes Volvo Penta's Forward Drive as "radical," "game-changing," and as starting a "revolution." ... It further explains that although "inboard V-drive manufacturers—their props tucked safely under the hull—enjoyed serving [the wakesurfing] market[,] sterndrive manufacturers couldn't." That indisputably identifies a long-felt need: safe wakesurfing on stern-drive boats.

Volvo Penta of the Americas, LLC v. Brunswick Corp., 81 F.4th 1202, 1214 (Fed. Cir. 2023)

Skepticism

Skepticism



“Evidence of industry skepticism weighs in favor of non-obviousness. If industry participants or skilled artisans are skeptical about whether or how a problem could be solved or the workability of the claimed solution, it favors non-obviousness. Doubt or disbelief by skilled artisans regarding the likely success of a combination or solution weighs against the notion that one would combine elements in references to achieve the claimed invention.”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1335 (Fed. Cir. 2016)

Ex. 2076: The Redefining CNAPP Guide

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

Ex. 2076 at 7-8

Ex. 2076: The Redefining CNAPP Guide

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

Ex. 2076 at 7-8

REDACTED

Praise



“Evidence that the industry praised a claimed invention or a product which embodies the patent claims weighs against an assertion that the same claim would have been obvious. Industry participants, especially competitors, are not likely to praise an obvious advance over the known art. Thus, if there is evidence of industry praise in the record, it weighs in favor of the nonobviousness of the claimed invention.”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1334 (Fed. Cir. 2016)

Ex. 2120: Forbes Article

Subscribe To Newsletters

Forbes

Subscribe: Less than \$150/yr

Sign In

More From Forbes

May 16, 2025, 12:40pm EDT

AI Agents Need To Be Managed As If They are Human

May 16, 2025, 10:00am EDT

The AI Graveyard: 7 Deadly Mistakes That Kill Most Enterprise AI Projects

May 16, 2025, 10:50am EDT

From Strategy To Success: How Process Drives 828 Growth

May 11, 2025, 10:40am EDT

AI Digital Twins: Your City's Edge In A World Of Unprecedented Change

us bank

ignite growth.

We can help prepare you for the next opportunity with expert advice.

INNOVATION > ENTERPRISE TECH

The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

By Louisa Columbus, Former Contributor

Nov 28, 2020, 05:00am EST

Share

Save

This article is more than 4 years old.



ORCA

- Cybersecurity, privacy and security startups have raised \$10.7 billion so far this year, five times more than was raised throughout 2010 (\$1.7 billion), according to a Crunchbase Pro query today.
- 22,156 startups who either compete in or rely on cybersecurity, security and privacy technologies and solutions as a core part of their business models today, 1,450 of which have received pre-seed or seed funding in the last twelve months based on a Crunchbase Pro query
- From network and data security to I.T. governance, risk measurement and policy

Document title: The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

Capture URL: https://www.forbes.com/sites/louisacolumbus/2020/11/28/the-top-20-cybersecurity-startups-to-watch-in-2021-based-on-crunchbase

Capture timestamp (UTC): Wed, 19 Mar 2025 18:16:37 GMT

Page 1 of 11



The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase

Orca Security - Orca Security is noteworthy for its innovative approach to providing instant-on, workload-deep security for AWS, Azure and GCP without the gaps in agents' coverage and operational costs. Orca integrates cloud platforms as an interconnected web of assets, prioritizing risk based on environmental context. Delivered as SaaS, Orca Security's patent-pending SideScanning™ technology reads cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords and unsecured PII.

809+326

809+326

809

926

Ex. 2120 at 7

809 POR 41; 926 POR 41; 326 POR 44

REDACTED

REDACTED

Security Agents Don't Belong In Your Cloud!

Published 08/18/2021

* * *

809+326+926

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

Ex. 2103 at 1

REDACTED

Ex. 2117: Panorama IT Brochure

Orca Security transcends traditional solutions by inspecting data at rest, providing an additional layer of security. This unique capability reveals hidden vulnerabilities and critical data exposures that other tools may ignore, strengthening your security from the ground up.

Ex. 2117 at 1-2

809+326+926

926

Copying



“Although copying is not alone dispositive of nonobviousness, we have usually considered a determination of copying to be “strong evidence of nonobviousness.” ... copying may often be the most probative and cogent evidence of nonobviousness.” In light of the Board's own findings that copying occurred, its assignment of only “some weight” was not supported by substantial evidence.”

Volvo Penta of the Americas, LLC v. Brunswick Corp., 81 F.4th 1202, 1213 (Fed. Cir. 2023)



“Evidence of access and substantial similarity is evidence of copying.”

Medtronic, Inc. v. Teleflex Innovations S.a.r.l., 70 F.4th 1331, 1340 (Fed. Cir. 2023)



“Evidence of access and substantial similarity is evidence of copying.”

Medtronic, Inc. v. Teleflex Innovations S.a.r.l., 70 F.4th 1331, 1340 (Fed. Cir. 2023)

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

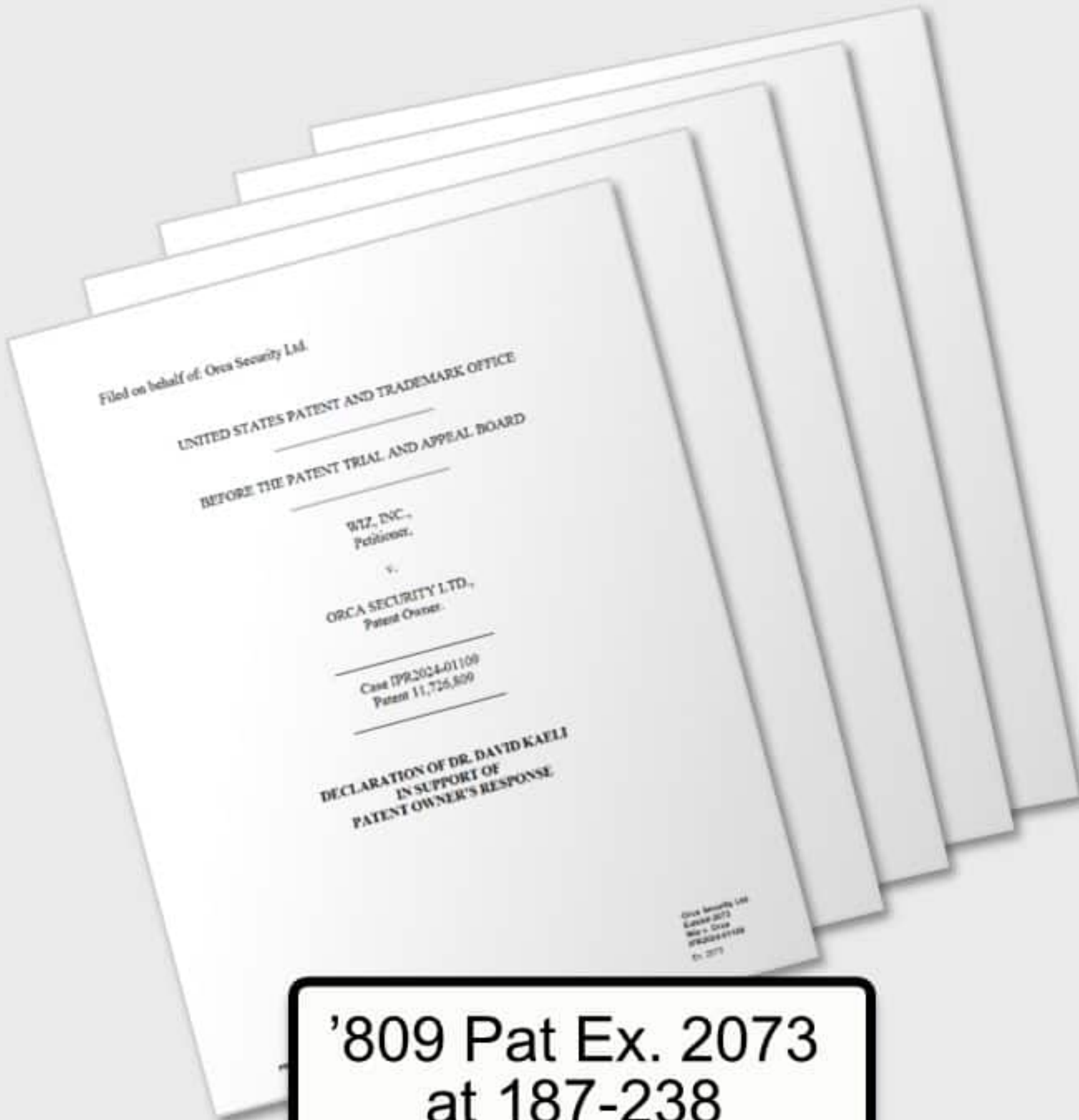
REDACTED



“Evidence of access and **substantial similarity** is evidence of copying.”

Medtronic, Inc. v. Teleflex Innovations S.a.r.l., 70 F.4th 1331, 1340 (Fed. Cir. 2023)

Dr. Kaeli: Wiz's Technology Is Nearly Identical To Orca's



Filed on behalf of: Orca Security Ltd.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner.

v.

ORCA SECURITY LTD.,
Patent Owner.

Case IPR2024-01109
Patent 11,735,809

DECLARATION OF DR. DAVID KAEI
IN SUPPORT OF
PATENT OWNER'S RESPONSE

Orca Security Ltd
London 2073
Wiz v. Orca
IPR2024-01109
Ex. 2073

'809 Pat Ex. 2073
at 187-238



Filed on behalf of: Orca Security Ltd.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Wiz.

v.

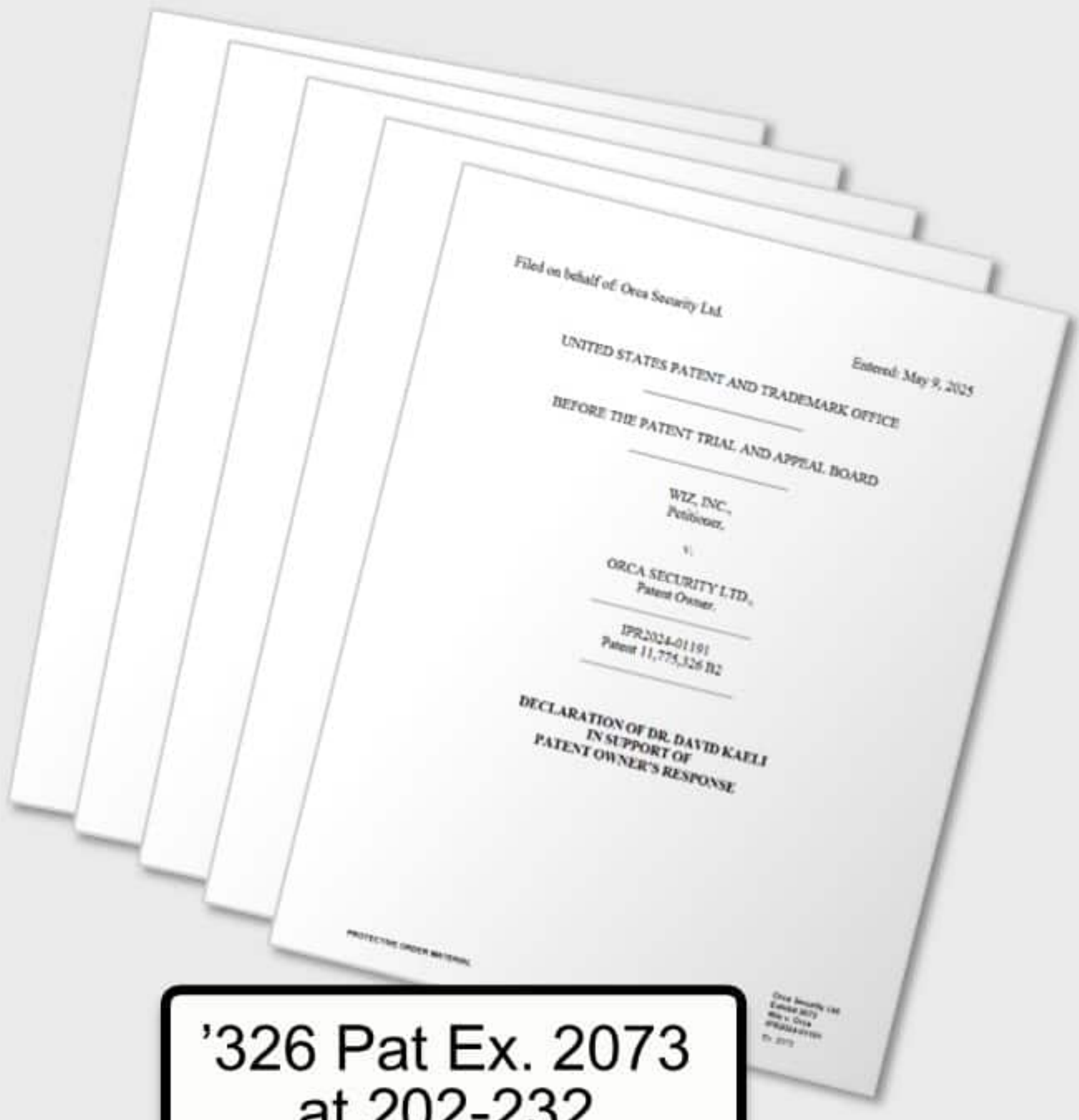
ORCA SECURITY LTD.,
Patent Owner.

IPR2024-01190
Patent 11,740,926

DECLARATION OF DR. DAVID KAEI
IN SUPPORT OF
PATENT OWNER'S RESPONSE

Orca Security Ltd
London 2073
Wiz v. Orca
IPR2024-01190
Ex. 2073

'926 Pat Ex. 2073
at 260-283



Filed on behalf of: Orca Security Ltd.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner.

v.

ORCA SECURITY LTD.,
Patent Owner.

IPR2024-01191
Patent 11,775,326 B2

DECLARATION OF DR. DAVID KAEI
IN SUPPORT OF
PATENT OWNER'S RESPONSE

Orca Security Ltd
London 2073
Wiz v. Orca
IPR2024-01191
Ex. 2073

'326 Pat Ex. 2073
at 202-232

809 POR 60; 926 POR 55; 326 POR 57

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Wiz's Response: Ami Luttwak

DocuSign Envelope ID: F66F494D-DB72-4125-8FA4-6AB1DA883371

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD,
Patent Owner.

DECLARATION OF AMI LUTTWAK

Wiz - EXHIBIT 1414
Wiz, Inc. v. Orca Security Ltd.
IPR2024-00864

PROTECTIVE ORDER MATERIAL
CONFIDENTIAL – ATTORNEY’S EYES ONLY



REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Wiz's Reply Evidence Shows Similarity

Agentless Scanning



The Original And Still The Champ

Full stack support for hosts, containers, and functions. Automated malware and PII detection. Automated and manual crown jewel identification.



Fast Follower

Followed Orca's patented SideScanning technology.

Ex. 1126 at 2

of long-felt but unmet need, industry praise, and commercial success. With respect to copying, we find a nexus exists for this evidence because (1) competitors had access to the GuideLiner products and produced substantially similar designs, and (2) there is direct evidence of copying of at least a portion of the GuideLiner device by Petitioner. *See Liqwd*, 941 F.3d at 1138 (“But where there is evidence of actual copying efforts, that evidence is always relevant.”).

Medtronic, Inc. v. Teleflex Life Sciences Ltd., IPR2020-01344, Paper 69 at 52-53

Commercial Success

Commercial Success



“When a product attains a high degree of commercial success, there is a basis for inferring that [attempts to a solution] have been made and have failed. ... Demonstrating that an invention has commercial value, that it is commercially successful, weighs in favor of its non-obviousness.”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1337 (Fed. Cir. 2016)

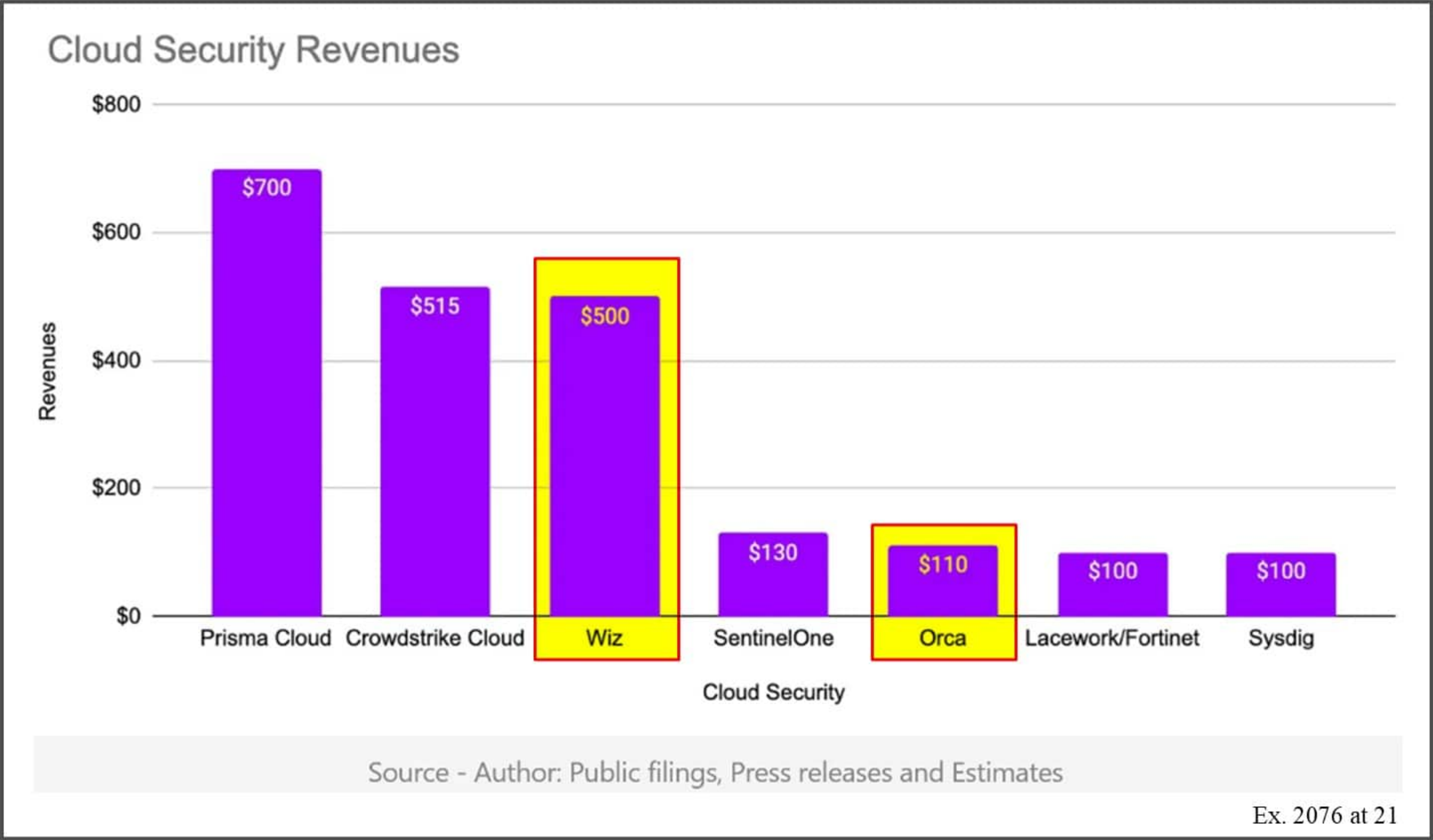
REDACTED



Brunswick's only arguments against commercial success of the Forward Drive were related to nexus. As the Board found, Brunswick either admitted or did not contest that "the Forward Drive essentially created a new market for stern drives," "sales of the 'Forward Drive have increased significantly since its launch in 2015,' " and "more and more boat builders are offering the Volvo Penta Forward Drive as original equipment, including boats specifically designed to incorporate the Forward Drive." *Id.* The Board further found that the record supported, and Brunswick did not contest, that boat manufacturers strongly desired Volvo Penta's Forward Drive and were urging Brunswick to bring a forward drive to market. Conf. J.A. 1300; ECF 46. Despite these findings and Brunswick's lack of arguments to the contrary (at least for the Forward Drive), the Board only afforded this factor "some weight." This finding was not supported by substantial evidence.

Volvo Penta of the Americas, LLC v. Brunswick Corp., 81 F.4th 1202, 1213–14 (Fed. Cir. 2023)

Wiz's & Orca's Revenues



Wiz's Revenue Growth

\$100M ARR in 18 months: Wiz becomes the fastest-growing software company ever

Just two years since its launch, Wiz protects hundreds of the world's leading organizations by enabling them to build faster and more securely in the cloud



Assaf Rappaport
August 10, 2022

5 minute read



Ex. 2116 at 1

REDACTED

Petitioner also argues that the touted benefits of on-demand classes, such as synchronizing live and archived user data and using group exercise to enhance competitiveness and interaction were all well-known and show that Patent Owner's evidence fails to link to the merits of the invention beyond the prior art. Reply 34. Petitioner's argument misses the mark because it focuses on isolated claim limitations allegedly known in the art rather than the claim as a whole. "While objective evidence of nonobviousness lacks a nexus if it exclusively relates to a feature that was 'known in the prior art,' the obviousness inquiry centers on whether 'the claimed invention as a whole' would have been obvious." *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013); *see also WBIP*, 829 F.3d at 1330–31 ("[T]he fact that an isolated feature may be present in the prior art may not render irrelevant objective evidence of non-obviousness of that feature in the claimed combination."). Petitioner does not persuasively argue that the commercial success "exclusively relates" to a known feature in the art. As noted above, the "claim as a whole" here includes not only the

Echelon Fitness Multimedia, LLC v. Peloton Interactive, Inc.,
IPR2020-01541, Paper 54 at 60 (Mar. 2, 2022)

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable Expectation Of Success (REOS) Combining Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud Management Console" For "The Location Of A Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Hindsight Reconstruction



“Care must be taken to avoid hindsight reconstruction by using ‘the patent in suit as a guide through the maze of prior art references, combining the right references in the right way so as to achieve the result of the claims in suit.’ ”

In re NTP, Inc., 654 F.3d 1279, 1299 (Fed. Cir. 2011)

Ranum Describes Network Scanners

As such, in one implementation, the **active scanners 210** may generally scan the respective portions of the network to obtain information describing vulnerabilities and assets in the respective network portions. In particular, as described in

* * *

For example, in one implementation, the **active scanners 210** may perform the various active probes to obtain a snapshot that describes assets actively running in the network at a particular point in time (e.g., actively running routers 240,

* * *

response to obtaining the snapshot of the network, the **active scanners 210** may then report the information describing the snapshot to the management console 250, which may use the

Ranum (Ex. 1093) at 13:41-44, 13:48-51, 14:4-6

tify potential vulnerabilities in the network. More particularly, in one implementation, the credentialed audits may include the **active scanners** using any suitable authentication technology to **log into and obtain local access to the hosts**, servers, or other devices in the network and perform any suitable operation that local users could perform thereon without necessarily requiring a local agent (although those skilled in the art will appreciate that a local agent may be used in certain implementations). Accordingly, the credentialed audits performed with the active scanners may be used to obtain highly accurate host-based data that includes various client-side issues (e.g., missing patches, operating system settings, locally running services, etc.), while the uncredentialed audits performed therewith may generally include network-based scans that involve **communicating packets or messages to the hosts, servers, or other devices in the network** and observing responses thereto in order to identify certain network vulnerabilities.

Ranum (Ex. 1093) at 4:40-47

926 Patent Overcame Problems With Network Scanners

hosting virtual machines. Traffic inspection may not provide an accurate indication of the security status of the server due to inherent limitations, such as encryption and whether the necessary data is exposed in the communication.

Ex. 1001 (Shua) '926 Patent at 1:52-55

926 Patent Overcame Problems With Network Scanners

vulnerability in the application. The disadvantage of such a scanner is that the server may not respond to all queries by the scanner, or not expose the necessary data in the response. Further, the network scanner usually communicates with the server, and the network configuration may prevent it. In addition, some types of queries may require credentials to access the server. Such credentials may not be available to the scanner.

Ex. 1001 (Shua) '926 Patent at 1:60-67

Ranum Does Not Analyze Snapshots Of Cloud Assets

Dr. Stavrou

Q. And you do not offer any opinion in your declaration that Ranum is analyzing snapshots of a virtual cloud asset; right?

A. I don't believe so.

Q. And Ranum does not teach or suggest that active scanners can be used to analyze snapshots of virtual cloud assets; right?

A. I don't think that this is here.

Ex. 2172 (Stavrou) at 276:17-277:2

Ranum's Scanning Is Fundamentally Different From Veselov's Snapshots

Dr. Stavrou

Q. Yeah. And my question is a different one -- I think maybe a simpler one, which -- I just want to make sure that I'm right that because a snapshot is a data file, does not have any active processing, it would not be possible to communicate messages or packets to it as described in Ranum?

A. That is correct.

Ex. 2172 (Stavrou) 251:18-252:18

Ranum's Scanning Is Fundamentally Different From Veselov's Snapshots

Dr. Stavrou

Q. Active network scanning and passive network monitoring are different security assessment techniques than what is disclosed in Veselov; right?

A. While they are -- on the face of it, it looks different, they rely on similar information.

* * *

So these things are present in a host. And the data here, the important part is that the data that Veselov analyzes and what Ranum is talking about are similar. Some of them might not be. So they're not identical. And then Ranum might have more information about the network. But there are -- there's an overlap. That's what I'm trying to say.

Ex. 2172 (Stavrou) 251:18-252:18

Failing To Reconcile Fundamental Differences Shows Lack Of Motivation



“Fundamental differences between the references are central to this motivation to combine inquiry. Thus, while the Board construed the Base Claims as encompassing pre-seamed and unseamed garments and garment sections, the Board properly considered the fundamental differences in the seaming techniques of Reed and Nishida ... the Board properly considered these fundamental differences in seaming techniques as part of its motivation to combine inquiry. Because Adidas failed to reconcile these differences, we conclude that the Board’s motivation to combine findings are supported by substantial evidence.”

Adidas AG V. Nike, Inc., 963 F.3d 1355, 1359 (Fed. Cir. 2020)

Wiz's Non-IPR Statements Distinguish Network Scanners From Agentless

 Platform Solutions Pricing Resources Customers Company Sign in Get a demo

[← Blog](#)

Automatically discover and secure your APIs with Wiz Dynamic Scanner

Wiz enhances its Dynamic Scanner to detect publicly exposed, unauthenticated APIs



Matika Lidgi, Nicolas Ehrman
December 21, 2022

5 minute read



Ex. 2182-001

The challenges of securing shadow APIs

API security is essential for organizations looking to protect their valuable assets and maintain the integrity and confidentiality of their data and systems. However, existing solutions fall short in catching shadow APIs, as they are mostly based on

- Agents
- Network scanners (in band or out of band)

These technologies are often based on two approaches such as the Web Application Firewall or API Gateway. In both cases, it is very complicated to get complete visibility because either an agent must be deployed or the flows must go through the API Gateway. This leaves security teams with blind spots on what APIs actually exist and prevents the application of good security practices.

Wiz brings an agentless, contextual approach

Wiz brings a different approach to API security with its agentless scanning for all major cloud providers and deep cloud risk assessment. This approach gives customers complete visibility of its cloud environments in minutes. Wiz then analyzes all the layers of the cloud

Ex. 2182-002

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable Expectation Of Success (REOS) Combining Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud Management Console" For "The Location Of A Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Czarny Taught Techniques For Physical Devices, Not Virtual Assets

Dr. Stavrou

Q. And I'm -- and I'm just asking that Czarny, it just -- it doesn't talk about virtual assets or virtual cloud assets. That's just not what it's directed to; right?

A. Yes

Ex. 2172 (Stavrou 4.02.25) at 246:22-247:4

No REOS: POSA Would Not Expect Physical Device Techniques Applicable To Cloud

Dr. Stavrou

Q. Dr. Stavrou, what information would you need in order to determine whether a CISO has experience in cybersecurity?

A. I believe your question is very generic. There are very different attributions that can be leveraged and used for someone to show a capability in understanding cybersecurity.

But also, I want to point out that cybersecurity is a very large field. So cloud security is very specific within that field, and it requires a different skill set or background. It's not that someone who knows about cybersecurity in general automatically is aware of, you know, technologies, techniques for cloud security.

Ex. 2195 (Stavrou 9.24.25) 28:10-29:9 (objections omitted)

Czarny's Risk Assessment Is Not Applicable

[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;

* * *

[1.6] 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;

* * *

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

'809 Patent, Claim 1

Dr. Stavrou

Q. And the risk that is -- that Czarny is looking at is to determine whether or not a target device should be granted or denied access to a secure environment; right?

A. Where do you read that? Give me one second to orient myself too because I maximized my screen.

Q. Yeah. It's the beginning of this, like 7, 46 through 50.

A. 46 through 50. It says -- yes.

Ex. 2172 (Stavrou 4.02.25) at 244:11-19

No REOS: Binary Data Not Available In Snapshot

The binary data is distinguished from data that simply identifies the software products or applications, e.g., the name and version of the software products or the file names or meta data of application files associated with, or mapped to, the software products. Conventional security vulnerability assessment systems use such file identification data (to determine which software products are on the target device **103** and then to assess the security vulnerability of the target device **103** in accordance therewith). However, this conventional technique is less thorough, robust or flexible than the present system, because it could potentially miss some known vulnerabilities, since the actual binary level data in the files of the software product could be different from the official version of the software product. For example, some

Ex.1084 (Czarny) at 4:25-38

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable Expectation Of Success (REOS) Combining Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud Management Console" For "The Location Of A Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Giakouminakis Requires Agents

326 Petition

Giakouminakis identifies vulnerabilities and determines associated risk levels as well as overall risk levels for assets based on numerous factors. EX1044, Abstract. For example, risk factors underlying an asset's overall risk include the asset's stored contents and connected assets. *Id.*, 6:36-58, 8:3-15, 8:47-9:29, 11:3-10; EX1002, ¶103.

326 Pet. at 20

Giakouminakis further teaches determining an asset's risk level by analyzing configurations "for each" of the requested assets. In addition to considering the particular asset's configuration (EX1044, 3:34-4:35, 7:32-62), Giakouminakis considers "vulnerabilities in connected assets" when determining an asset's overall risk, which a POSA would have understood to involve analyzing those assets' configurations since that is how Giakouminakis generally describes detecting vulnerabilities. *Id.*, 8:46-9:3; *see also id.*, 3:34-4:35, 6:35-58, 7:33-37, 13:59-14:7; EX1002, ¶298. At a minimum, this would have been obvious since, as discussed

326 Pet. at 67

Giakouminakis Requires Agents

In embodiments, as described herein, the security tool **102** can be implemented and executed on any of the computing systems of environment **100** in order to test and analyze the security of a computing system **104**. For example, the security tool **102** can be implemented and executed on a computing system **104** that is being tested. Likewise, **the security tool 102 can be implemented and executed** on a remote computing system **112**. In this example, the security tool **102** can remotely test and analyze the computing systems **104** via the network **106**. When configured as an application program, the security tool **102** can be stored on any type of computer readable storage medium, such as hard drives, optical storage, system memory, and the like, of the computing systems of the environment **100**.

Ex. 1044 (Giakouminakis) at 12:31-44

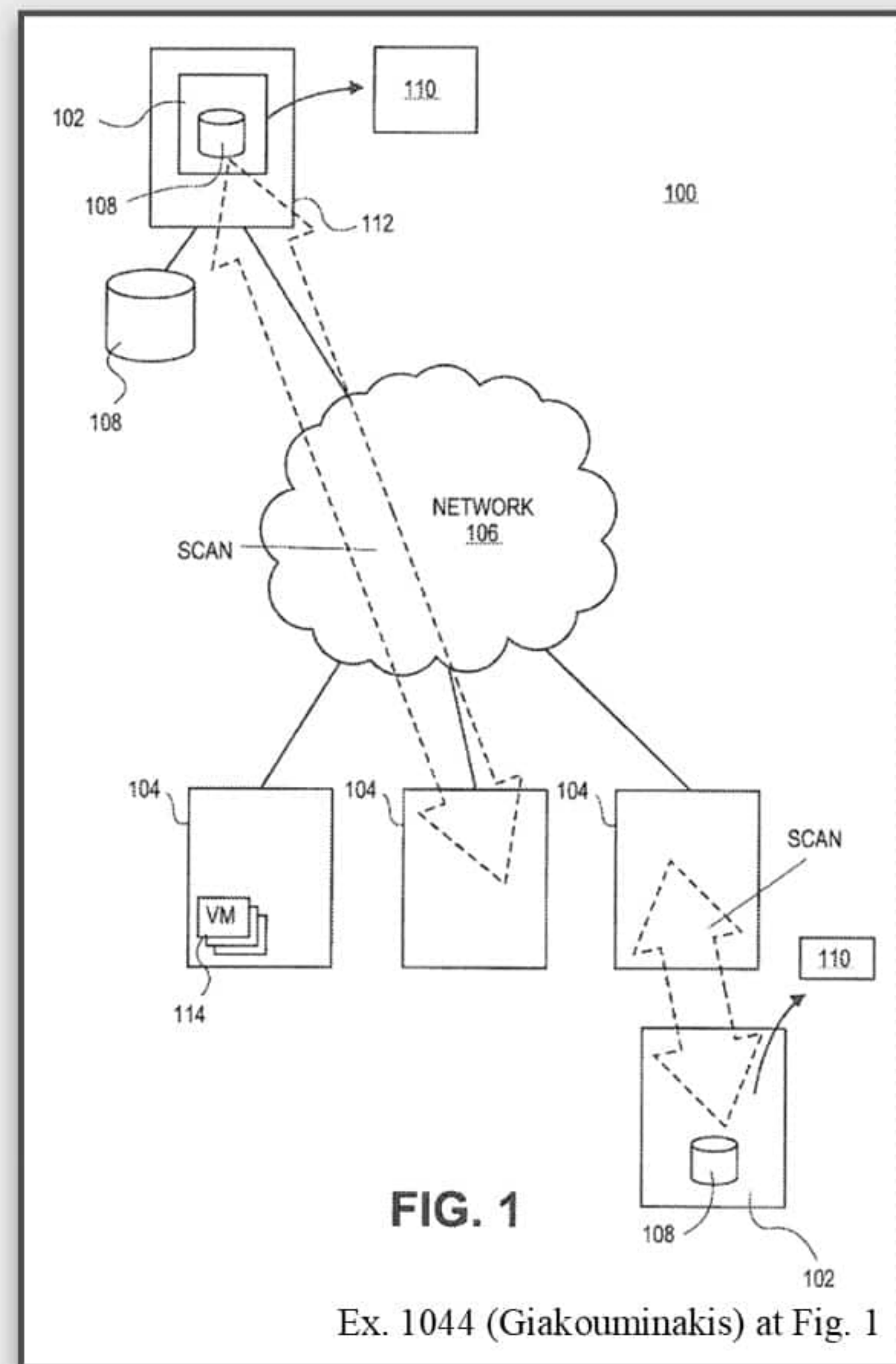


Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

3. The method of claim 1, further comprising detecting the data stored on the virtual disk by determining added or changed files on the virtual disk without a corresponding installation process.

Ex. 1001 '926 Patent, Claim 3

926 Petition

history. EX1094, ¶¶125, 134, 172; EX1002, ¶272. While Seo focuses on applications that run encryption algorithms, a POSA would have recognized its teachings were broadly applicable to other types of files stored on a VM. EX1002, 926 Pet. 68

[0002] The disclosure relates to an artificial intelligence (AI) system which mimics recognition and judgment of the human brain by using a machine-learning algorithm such as deep learning, and application thereof. More particularly, the

Ex. 1094 (Seo) ¶ 2

[0007] When data is encrypted by a malicious program such as ransomware or malware without permission, it is very difficult to restore the encrypted data. Therefore, it is preferable to block encryption before the malicious program encrypts data.

Ex. 1094 (Seo) ¶ 7

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable Expectation Of Success (REOS) Combining Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud Management Console" For "The Location Of A Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

Czarny Teaches Malware Is A Different Field Than Vulnerabilities

Vulnerability assessment and malware detection are two fields or industries that deal with issues of computer security. A positive malware detection generally requires an immediate response to eliminate a threat to the computer device of a potentially imminent malicious event. Typically, the response is to quarantine, remove, or replace the software file of the malware. With a positive vulnerability assessment, on the other hand, the computer device can usually continue to operate without concern for a threat to the computer device, since a malicious event is not necessarily imminent.

Ex.1084 (Czarny) at 1:6-15

Czarny Teaches Quarantining Malware, Not Vulnerabilities

11. The method of claim 10, wherein mitigating a potential cyber vulnerability includes at least one of:
blocking traffic from untrusted networks to the protected virtual cloud asset,
halting operation of the protected virtual cloud asset, or
quarantining the protected virtual cloud asset.

'809 Patent, Claim 11

Vulnerability assessment and malware detection are two fields or industries that deal with issues of computer security. A positive malware detection generally requires an immediate response to eliminate a threat to the computer device of a potentially imminent malicious event. Typically, the response is to quarantine, remove, or replace the software file of the malware. With a positive vulnerability assessment, on the other hand, the computer device can usually continue to operate without concern for a threat to the computer device, since a malicious event is not necessarily imminent.

Ex.1084 (Czarny) at 1:6-15

Hutchins Teaches Quarantining Viruses, Not Vulnerabilities

11. The method of claim 10, wherein mitigating a potential cyber vulnerability includes at least one of:
blocking traffic from untrusted networks to the protected virtual cloud asset,
halting operation of the protected virtual cloud asset, or
quarantining the protected virtual cloud asset.

'809 Patent, Claim 11

[0053] Yet another application suited for offloading onto a replicated virtual machine relates to virus scanning. Virus scanning is periodically done in order to check for potentially malicious code. If the virus scan finds one or more viruses, the original virtual machine can be quarantined. Again, this scan-

Hutchins ¶ 53

Table of Contents

Introduction 2

Claim Construction (809/926/326 All Grounds) 9

No Motivation To Combine (MTC) Or Reasonable
Expectation Of Success (REOS) Combining
Veselov And Mohanty (809/926 All Grounds) 17

Veselov And Mohanty Do Not Teach Or
Suggest Limitations 1.4-1.7 (926 All Grounds) 30

Veselov And Mohanty Do Not Teach Or Suggest
Limitations 1.5-1.8 (809 All Grounds) 52

No MTC Or REOS Combining Veselov
And Basavapatna (326 All Grounds) 56

No Teaching/Suggesting "Querying A Cloud
Management Console" For "The Location Of A
Virtual Disk" (809 Cls. 15, 22; 926 Cl. 13; 326 Cl. 14) 72

Objective Indicia (809/926/326 All Grounds) 87

926 Ground 2 191

809 Ground 2 201

326 Ground 3 206

926 Grounds 3-4 209

809 Grounds 3-4 212

Motion to exclude 216

None Of The Exhibits Are Hearsay



“Hearsay” means a statement that:

* * *

a party offers in evidence to prove the truth of the matter asserted in the statement.

Fed. R. Evid. 801(c)(2)



“[W]e do not find that the statement in the journal article is offered for the truth of the matter asserted therein. ... Rather, we find that Patent Owner offers the statement in an effort to show that third parties have praised ‘the patented features of the ’958 Patent.’”

MOM Enters., LLC v. Vieth, IPR2023-00726, Paper 112 at 89 (PTAB Sept. 10, 2024)

REDACTED

Hearsay Exceptions Apply



“The Court agrees with Plaintiffs that customers’ statements to Plaintiffs’ customer representatives are not hearsay or are subject to the state of mind exception to hearsay.”

Lincare Holdings Inc. v. Doxo, Inc., No. 8:22-cv-02349, 2024 WL 865881, at *2 (M.D. Fla. Feb. 29, 2024)



“Though the ... transcript ... may be lengthy, the Court nevertheless finds that [it] in [its] entirety qualif[ies] as [a] present sense impression[.]...”

Flythe v. District of Columbia, 4 F. Supp. 3d 222, 234 n.2 (D.D.C. 2014)

The Residual Exception Renders Wiz's Documents Admissible



In General. Under the following conditions, a hearsay statement is not excluded by the rule against hearsay even if the statement is not admissible under a hearsay exception in Rule 803 or 804:

(1) the statement is supported by sufficient guarantees of trustworthiness—after considering the totality of circumstances under which it was made and evidence, if any, corroborating the statement; and

(2) it is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts.

Fed. R. Evid. 807(a)

Wiz's Prejudice Argument Is Without Merit And Waived

The parties are reminded that any requests to enforce or modify the District Court Protective Order should be directed to the District Court and not the Board.

926 Paper 17 at 3

Conclusion

Because we are persuaded by the arguments and evidence presented by Orca that the additional discovery is in the interests of justice, we grant Orca's request.

926 Paper 26 at 7



“A party dissatisfied with a decision may file a single request for rehearing without prior authorization from the Board ... [w]ithin 14 days of the entry of a non-final decision...”

37 CFR § 42.71)

Wiz's Prejudice Argument Is Without Merit And Waived

Raghav,

Without waiving any evidentiary objections or rights under the district court protective order, we confirm production of the requested documents in the IPRs pursuant to the Board's order. The documents should be treated with the same level of confidentiality designation as in the district court case.

We also agree to your requested additional extension provided it will not preclude a further extension for our petitioner replies should one become necessary.

Regards,
Matt

Matthew A. Argenti
Wilson Sonsini Goodrich & Rosati
650 Page Mill Rd., Palo Alto, CA 94304
Direct: (650) 354-4154
Fax: (650) 493-6811

Ex. 2173 (2025.03.28 M. Argenti Email) at 1