

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

September 15, 2025

IPR2024-00863 (Patent 11,663,031 B2)

IPR2024-00864 (Patent 11,663,032 B2)

IPR2024-00865 (Patent 11,693,685 B2)

The '031 Patent

1. A system for inspecting data, the system comprising:

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

[1.1] establish an interface between a client environment and security components;

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

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

[1.4] receive an identification of the location of the virtual disks of the virtual machine;

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

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

[1.7] report the detected vulnerabilities as alerts.

Ex.1001 (Shua) '031 Patent, Claim 1

The '685 Patent

1. A system for inspecting data, the system comprising: at least one processor configured to:
 - [1.1] establish an interface between a client environment and security components;
 - [1.2] using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment;
 - [1.3] use the computing platform APIs to query a location of at least one of the identified virtual disks;
 - [1.4] receive an identification of the location of the virtual disks of the virtual machine;
 - [1.5] generate at least one snapshot of the virtual disks of the virtual machine;
 - [1.6] analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine;
 - [1.7] determine a risk level of the virtual machine; and
 - [1.8] report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.

Ex.1001 (Shua) '685 Patent, Claim 1

The '032 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 at least one 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 potential cyber vulnerabilities of the protected virtual cloud asset;

[1.5] determining whether the matching installed applications are used by the protected virtual cloud asset;

[1.6] prioritizing the potential cyber vulnerabilities based on the use determinations; and

[1.7] reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.

Ex.1001 (Shua) '032 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)

'031 Patent (Ground 1)

- No Motivation To Combine Veselov Embodiments
- Veselov/Price Would Not Be Combined
- Cloud APIs To Identify/Locate Disks
- Snapshot/Analysis Of Inactive VMs
- Reporting As Alerts
- Claims 4/12

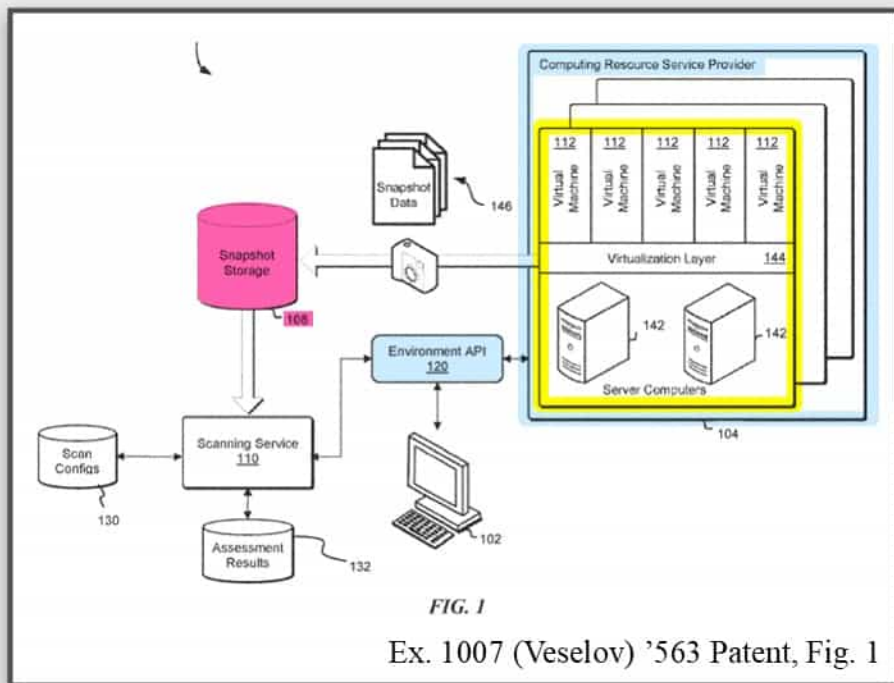
Combining Embodiments Requires Motivation



“Whether a rejection is based on combining disclosures from multiple references, combining multiple embodiments from a single reference, or selecting from large lists of elements in a single reference, there must be a motivation to make the combination and a reasonable expectation that such a combination would be successful, otherwise a skilled artisan would not arrive at the claimed combination.”

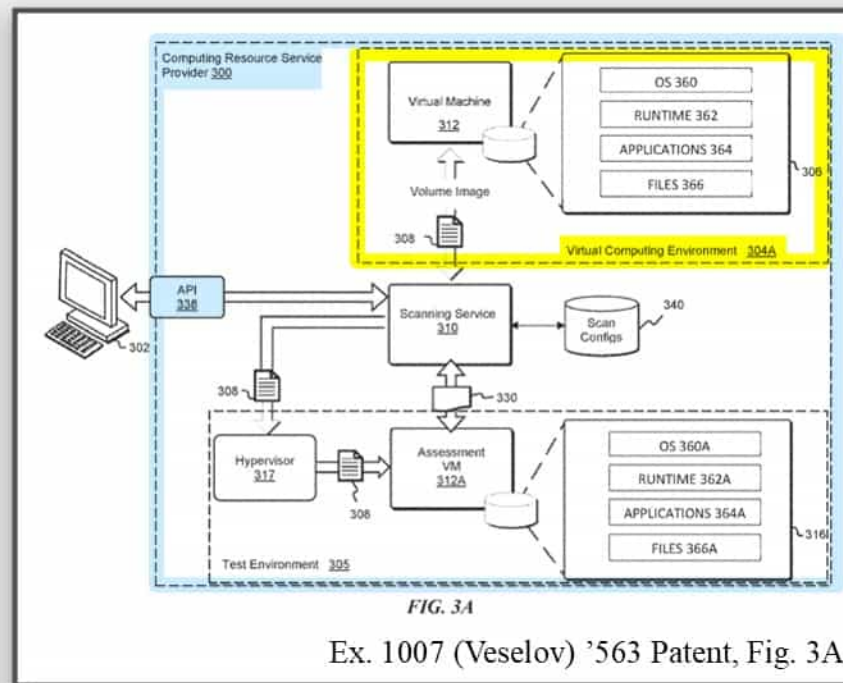
In re Stepan Co., 868 F.3d 1342, 1346 (Fed. Cir. 2017)

Veselov's Embodiments



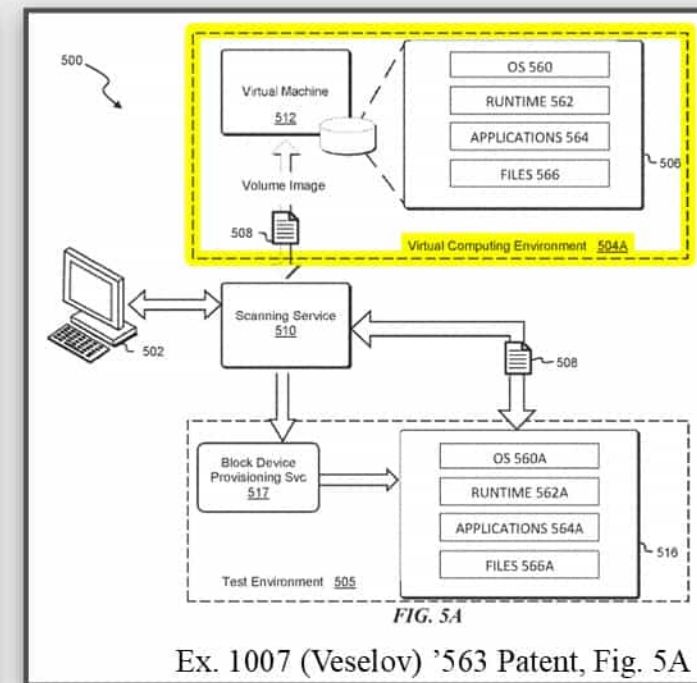
as virtual computing resources provided by a network-accessible services system 110 allocated within a virtual computing environment implemented by the computing resource service provider 104. In some embodiments, the

Ex. 1007 (Veselov) '563 Patent at 2:22-29



FIGS. 3A-B illustrate example computing environments implemented by a computing resource service provider 300, 350, in which computing environments a scanning service

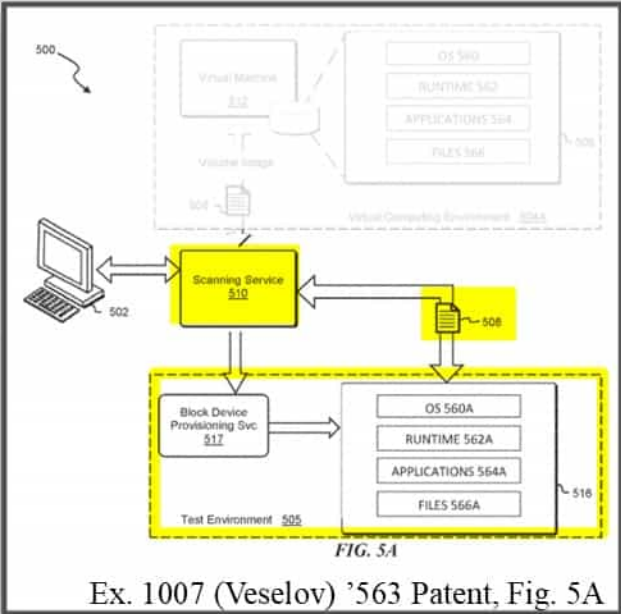
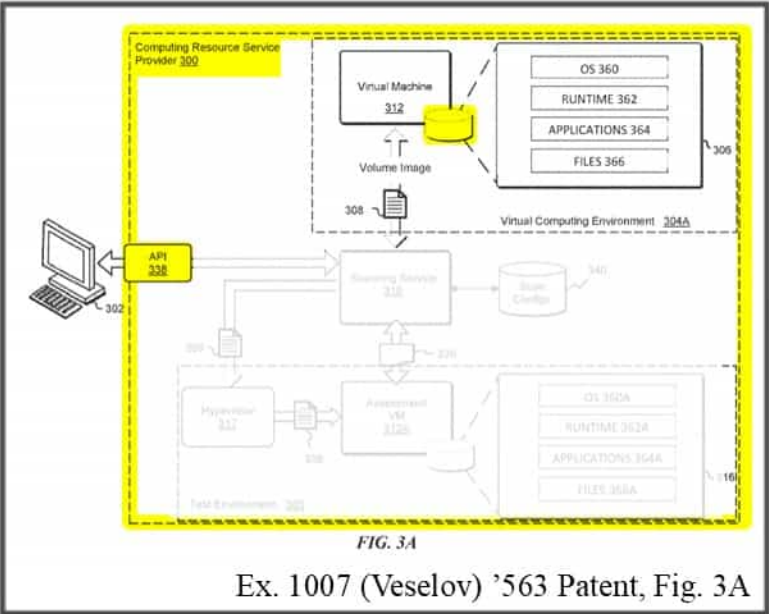
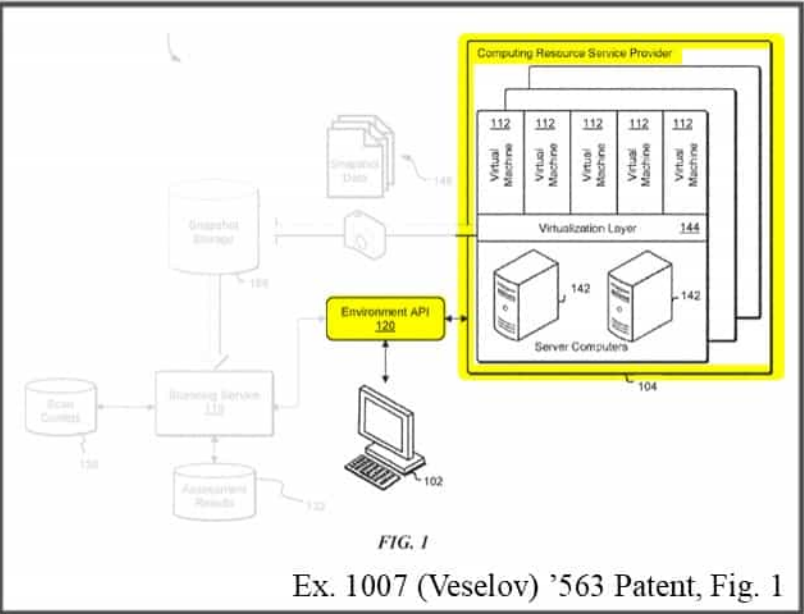
Ex. 1007 (Veselov) '563 Patent at 10:37-39



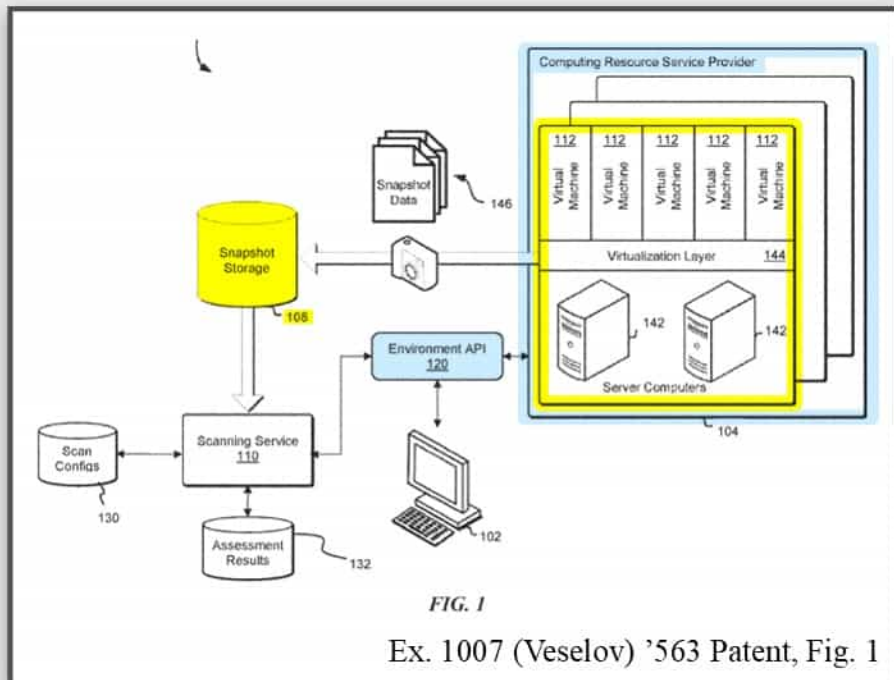
FIGS. 5A-B illustrate example computing environments 500, 550 providing additional embodiments of the present security assessment systems. The examples again use a

Ex. 1007 (Veselov) '563 Patent at 16:56-58

Wiz's Hindsight Reconstruction



Wiz Cannot Rely On Figure 1



1. A system for inspecting data, the system comprising:

* * *

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

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

[1.4] receive an identification of ~~the location of the virtual disks of the virtual machine;~~

Ex.1001 (Shua) '031 Patent, Claim 1 (excerpt)

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

* * *

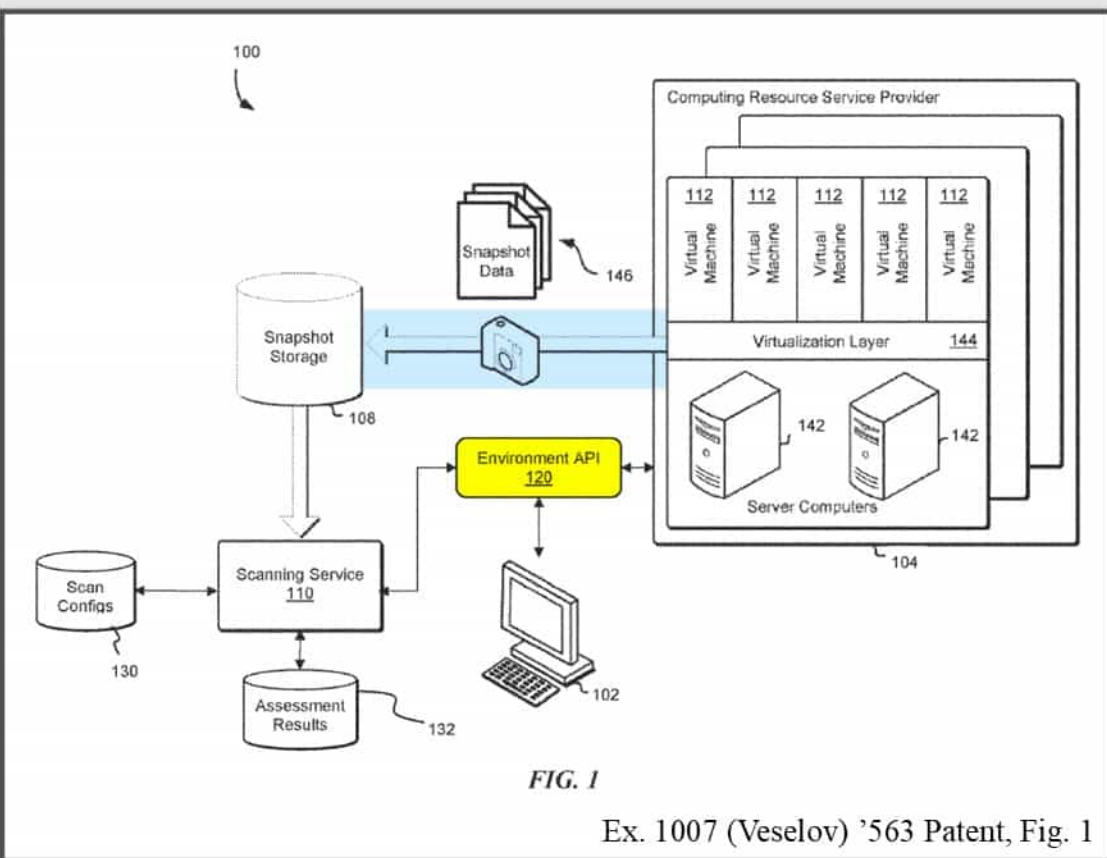
[1.2] using the interface, utilize cloud computing platform APIs ~~to identify virtual disks of a virtual machine in the client environment;~~

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

[1.4] receive an identification of the ~~location of the virtual disks of the virtual machine;~~

Ex.1001 (Shua) '685 Patent, Claim 1 (excerpt)

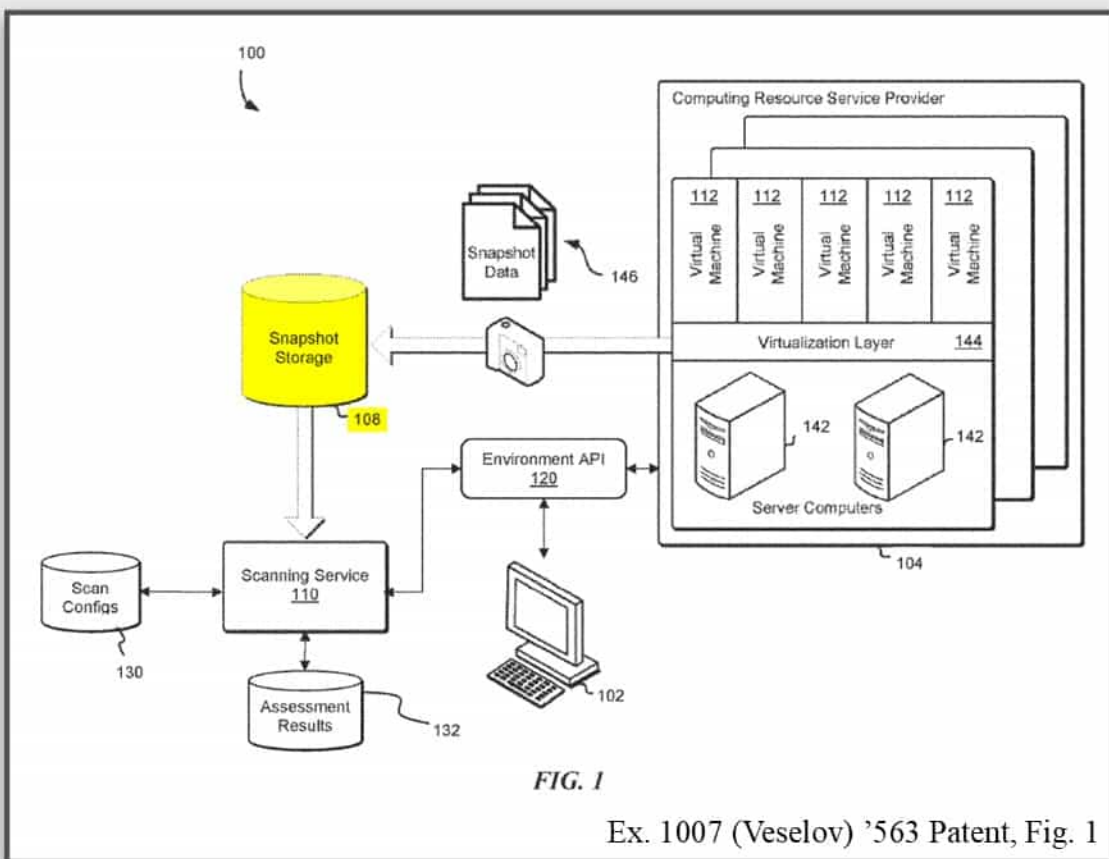
Figure 1: APIs Used To Identify VMs/Snapshots, Not Disks



For example, a user device **102** may transmit a request to the scanning service **110** for a particular security assessment of one or more instances of a virtual machine **112**. The request may be an API call including information corresponding to the requestor, the user associated with the virtual machine **112**, the on-demand storage service **108**, and/or the particular virtual machine **112**. The scanning service **110** may determine the corresponding virtualization layer **144** for the virtual machine **112** identified by the request and transmit a command to the virtualization layer **144** to provide snapshot data **146** (or to provide access to snapshot data **146**) corresponding to the virtual machine **112**. The virtualization layer

Ex. 1007 (Veselov) '563 Patent at 6:32-43

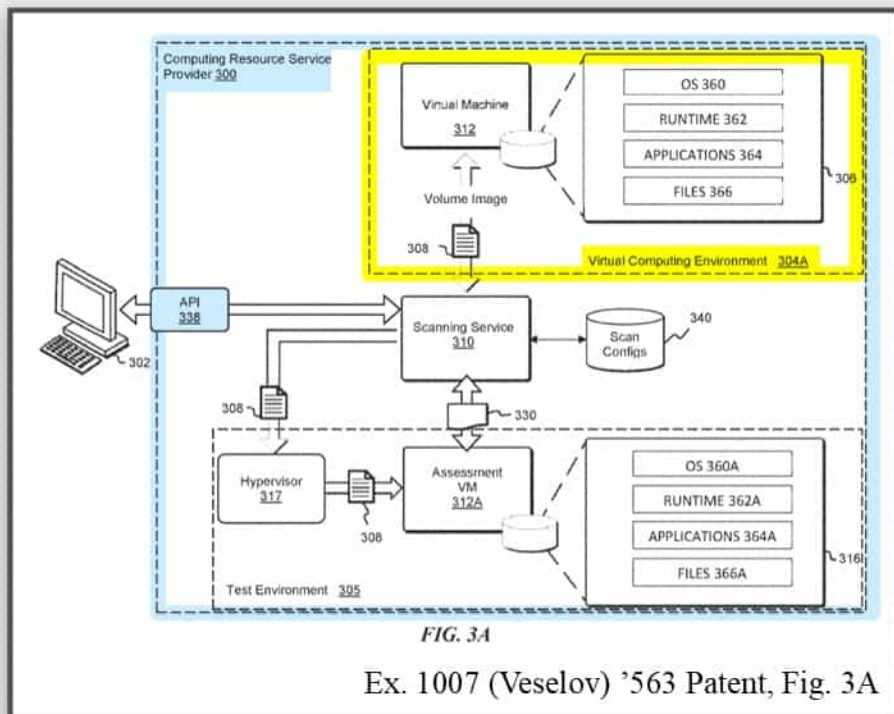
VMs And Snapshot IDs, Not Disks



stored by the snapshot storage service **108**. For example, the snapshot data **146** may be stored with its own unique identifier as well as the identifier of the virtual machine instance from which the snapshot data **146** was derived; the snapshot storage service **108** may be queryable by either or both identifiers. In another example, the snapshot storage service **108** may be non-queryable in so much as the snapshot storage service **108** stores snapshot data **146** (e.g., volume images) as data objects which are identifiable and retrievable by a data object identifier, such as a file name or key, but does not enable queries on information contained in the snapshot storage service **108**.

Ex. 1007 (Veselov) '563 Patent at 7:50-61

Wiz Cannot Rely On Figures 3A/3B



1. A system for inspecting data, the system comprising:

* * *

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

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

[1.4] receive an identification of ~~the location of the virtual disks of the virtual machine;~~

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

Ex.1001 (Shua) '031 Patent, Claim 1 (excerpt)

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

* * *

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

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

[1.4] receive an identification ~~of the location of the virtual disks of the virtual machine;~~

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

Ex.1001 (Shua) '685 Patent, Claim 1 (excerpt)

Figs 3A/3B

In an example embodiment, the scanning service 310 may produce, or cause the production of, a duplicate of the virtual machine 312 (e.g., of an instance thereof) using the volume image; the duplicate is referred to herein as the assessment virtual machine 312A, 312B. In one example embodiment,

Ex. 1007 (Veselov) '563 Patent at 12:1-5

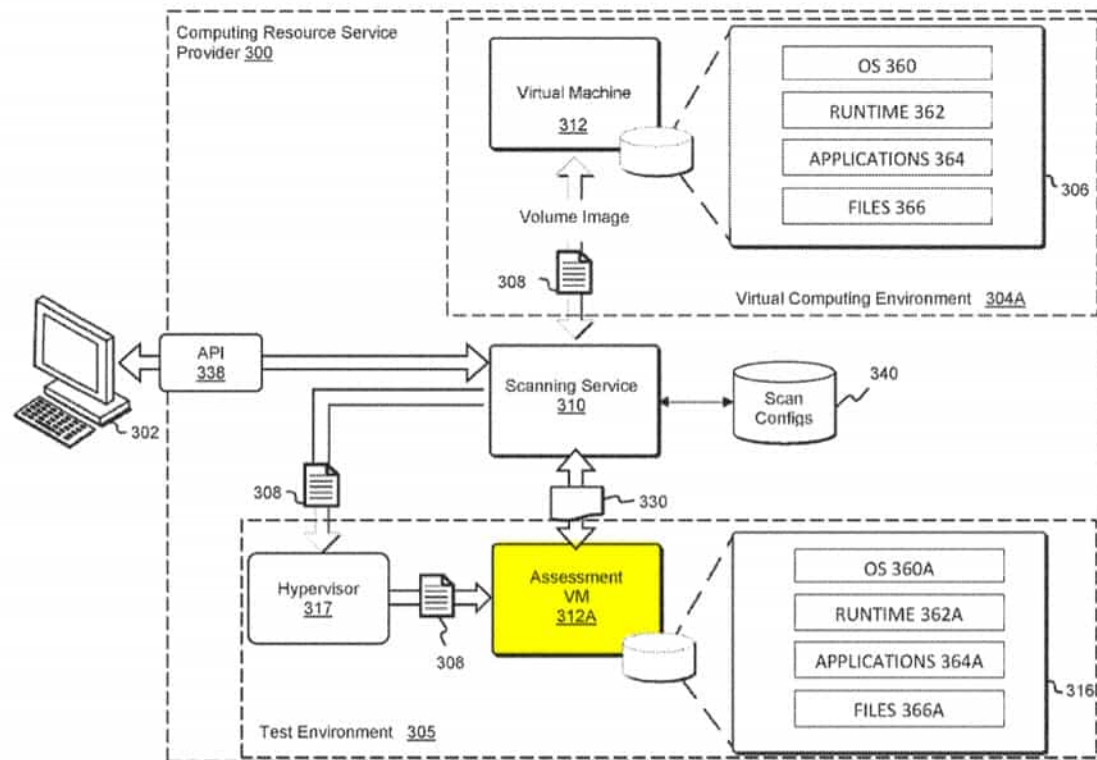


FIG. 3A

Ex. 1007 (Veselov) '563 Patent, Fig. 3A

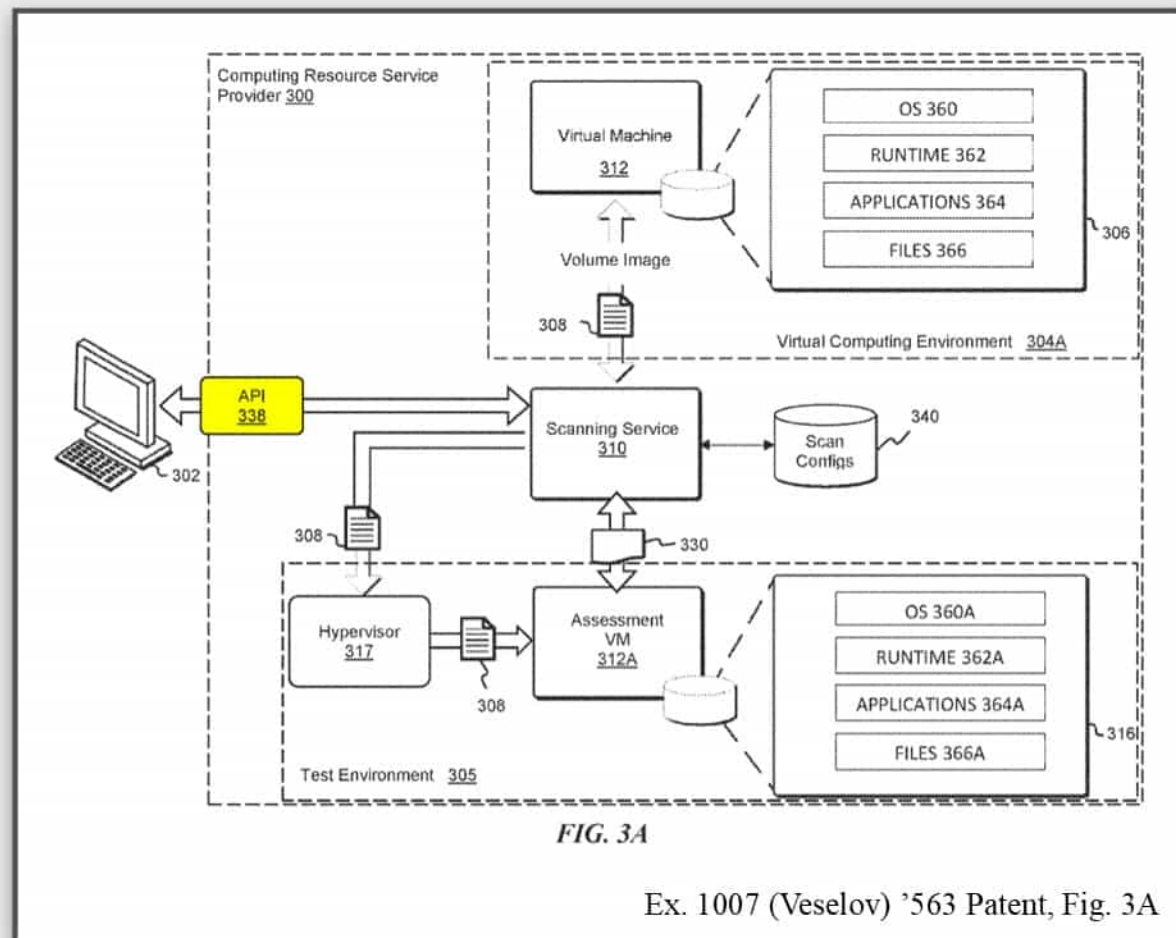
Figure 3A/3B: APIs Provide User Interface

In various embodiments, an owner or administrator of the target computing resources to be assessed may configure one or more security assessments, such as by using the user device 302 to access the scanning service 310 via one or more APIs 338, web interfaces, and the like. Various aspects

Ex. 1007 (Veselov) '563 Patent at 14:37-41

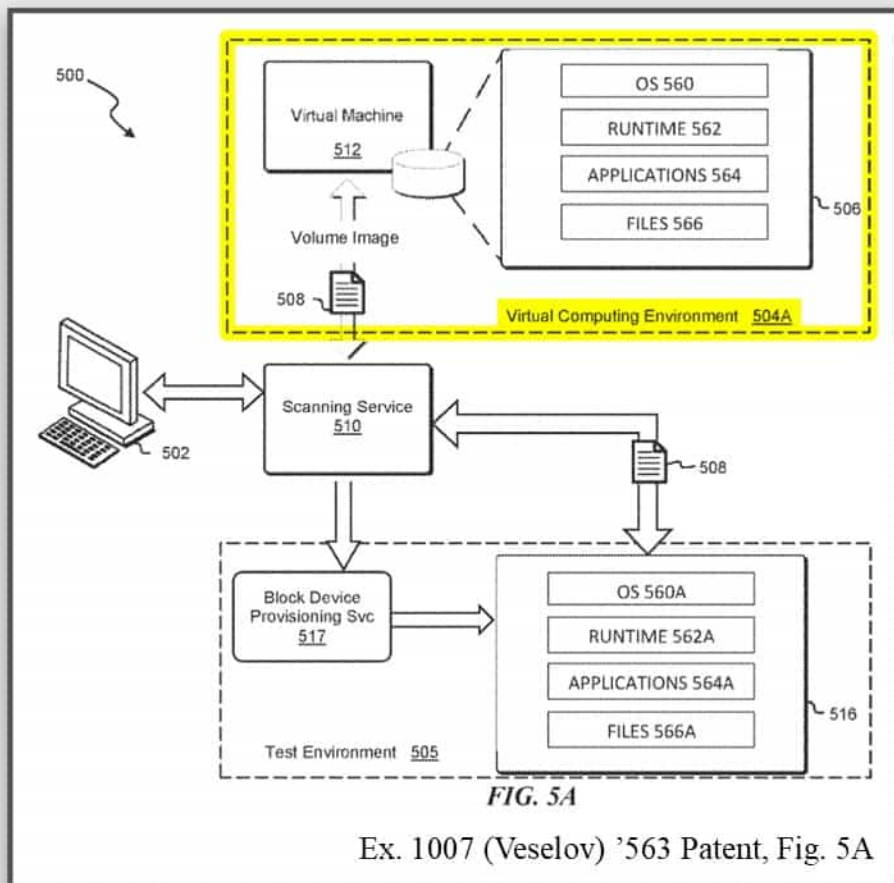
between security assessments. Alternatively, the API 338 may be configured to receive the request, determine its contents, and then control the scanning service 310 to implement the security assessment according to the user input. The scanning service 310 may obtain the identified

Ex. 1007 (Veselov) '563 Patent at 15:23-27



Ex. 1007 (Veselov) '563 Patent, Fig. 3A

Wiz Cannot Rely On Figures 5A/5B



1. A system for inspecting data, the system comprising:

* * *

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

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

[1.4] receive an ~~identification of the location of the virtual disks of the virtual machine;~~

Ex.1001 (Shua) '031 Patent, Claim 1 (excerpt)

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

* * *

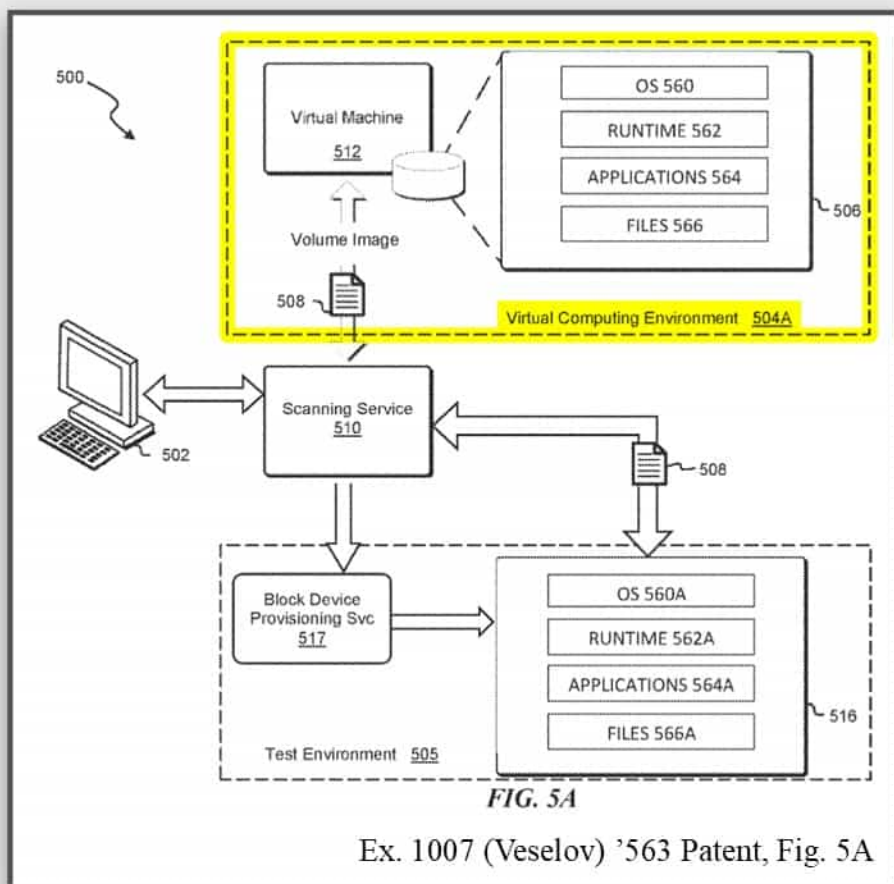
[1.2] using the interface, ~~utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment;~~

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

[1.4] receive an ~~identification of the location of the virtual disks of the virtual machine;~~

Ex.1001 (Shua) '685 Patent, Claim 1 (excerpt)

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 (Veselov) '563 Patent at 16:56-58

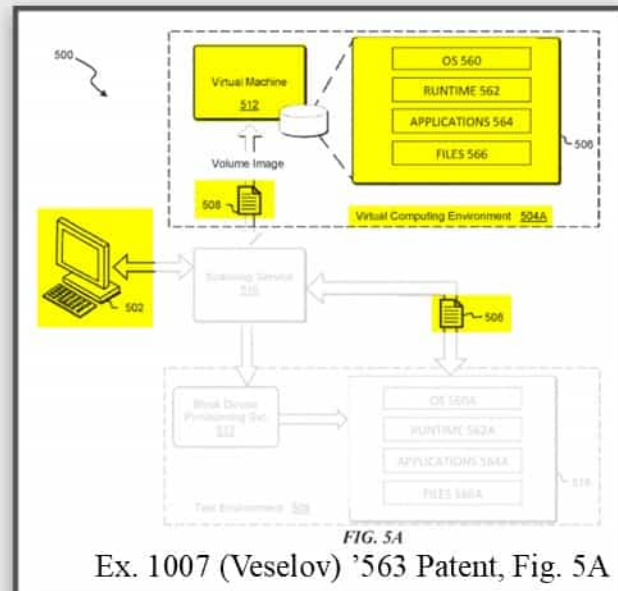
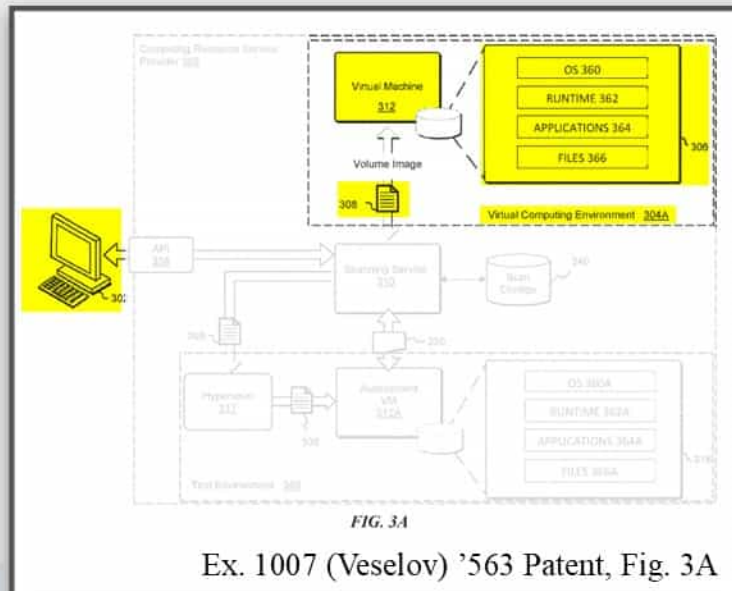
implementations of FIGS. 5A-B, rather than recreating and instantiating a duplicate VM, the scanning service 510 is configured to analyze the volume image 508 as a data file.

Ex. 1007 (Veselov) '563 Patent at 17:1-3

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) '563 Patent at 16:45-67

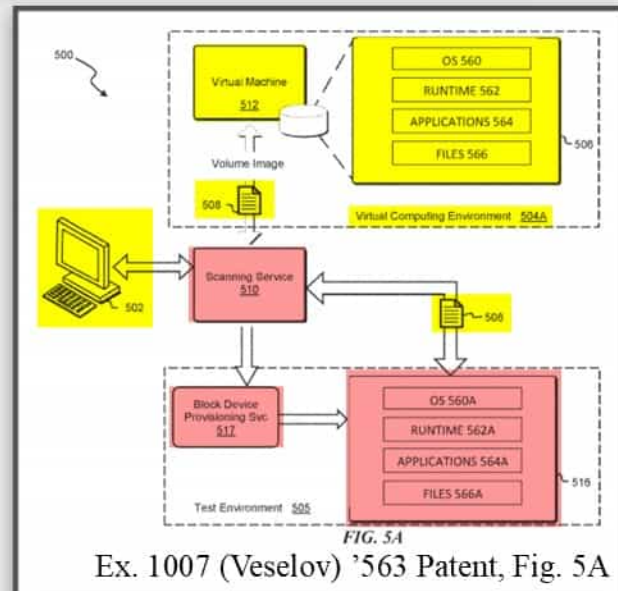
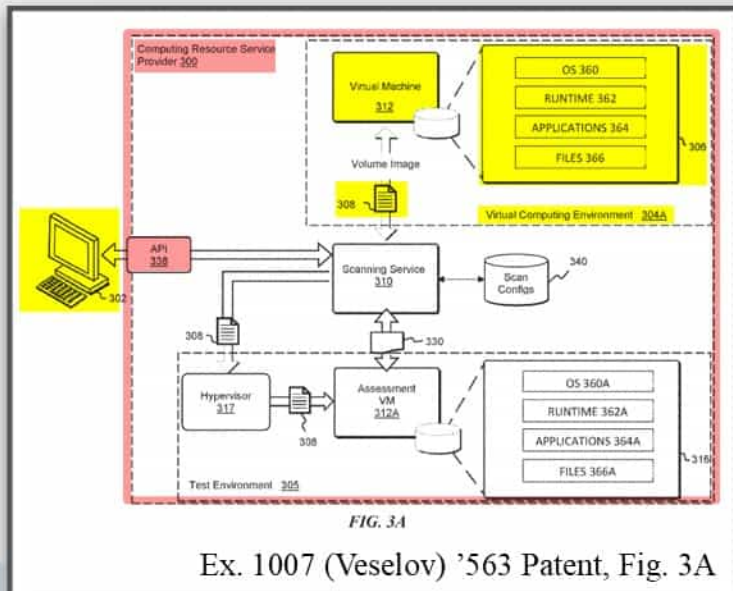


Wiz Does Not Rely On Common Features

'031 Reply

an undepicted aspect. EX1007, 18:1-15; EX1400, ¶¶16-17. Moreover, 5A/B has the same “implementation” as the 3A/3B environment PO admits is “implemented” by the service provider. POR, 15; EX1007, 16:56-67; EX1400, ¶17. The environments have the same “interactions” (EX1007, 16:56-67), which PO admits involves APIs. POR, 15-18; EX1400, ¶¶17-18.

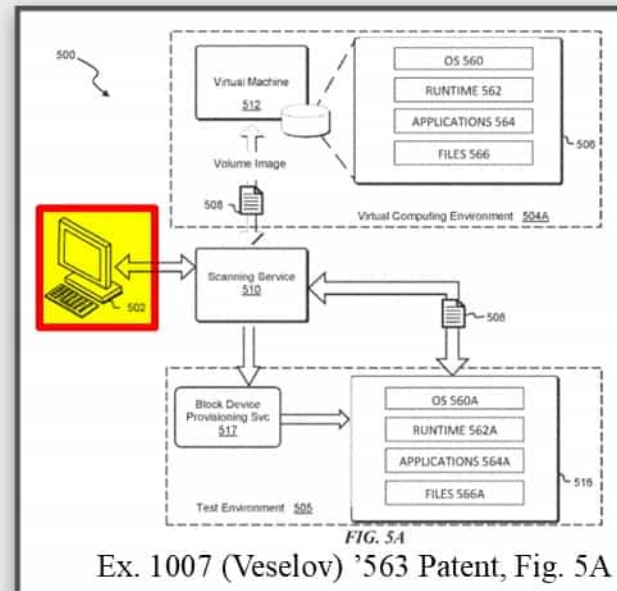
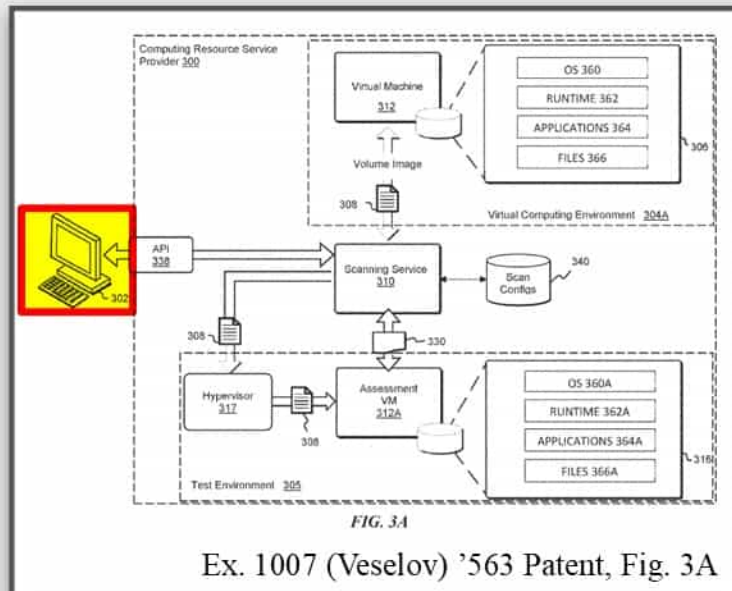
Wiz 031 Reply at 5



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

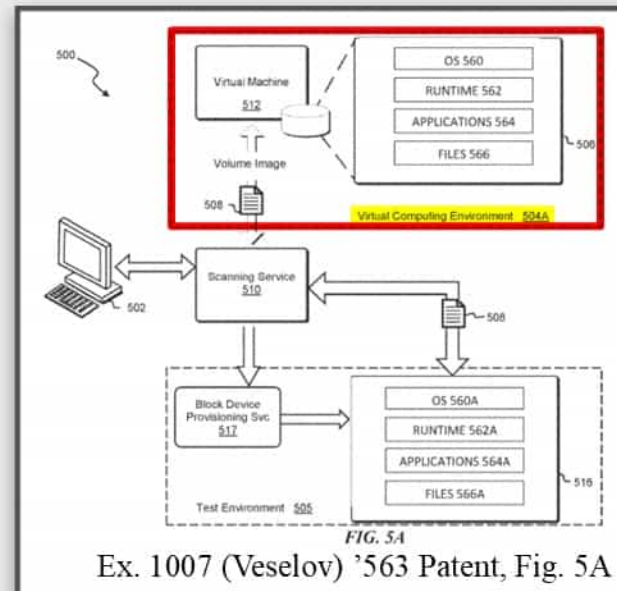
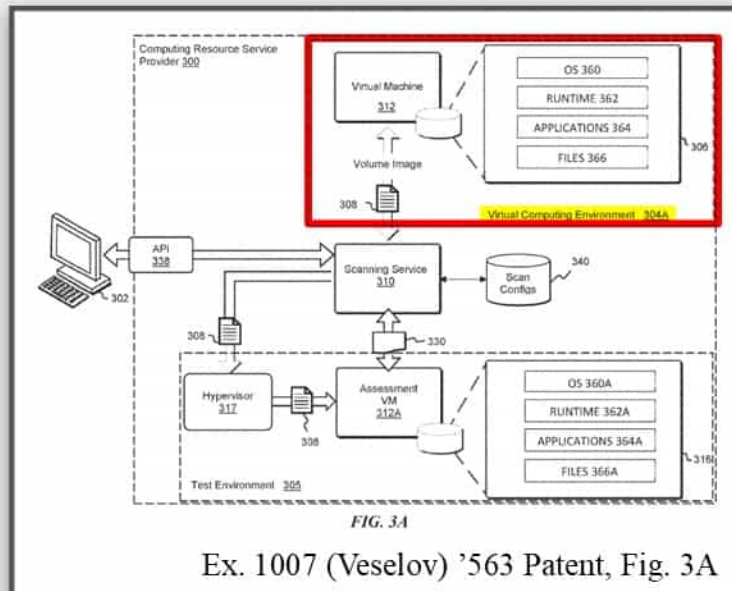
Ex. 1007 (Veselov) '563 Patent at 16:56-67



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

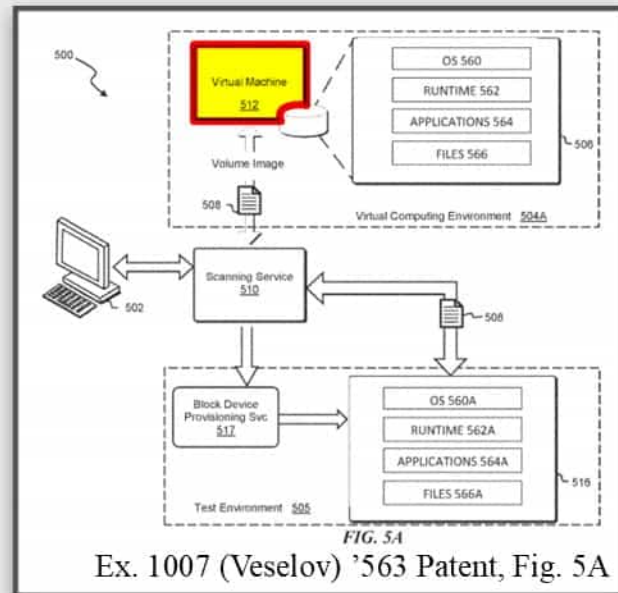
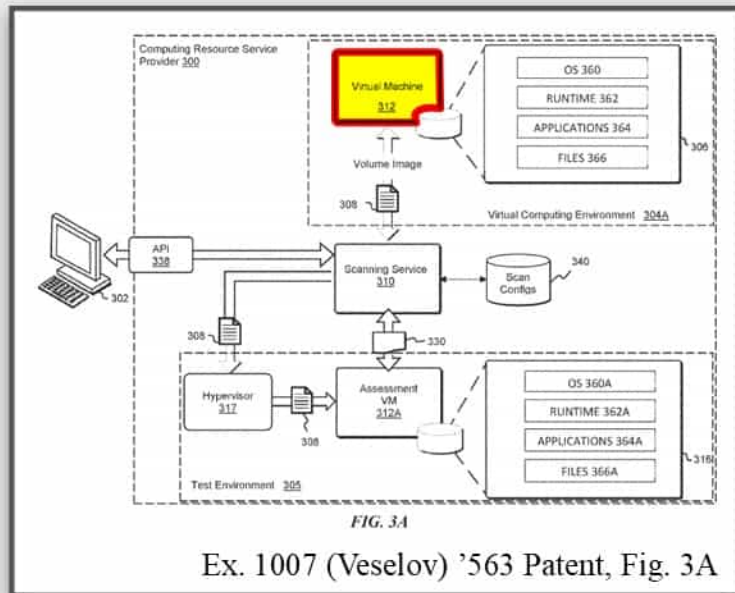
Ex. 1007 (Veslov) '563 Patent at 16:56-67



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

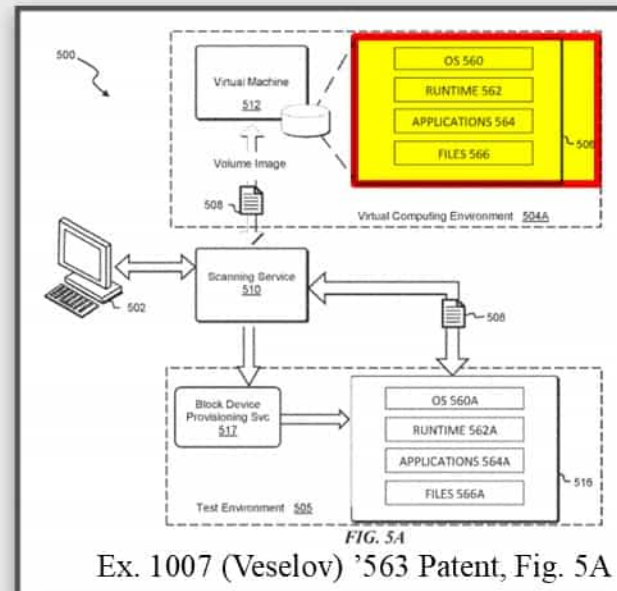
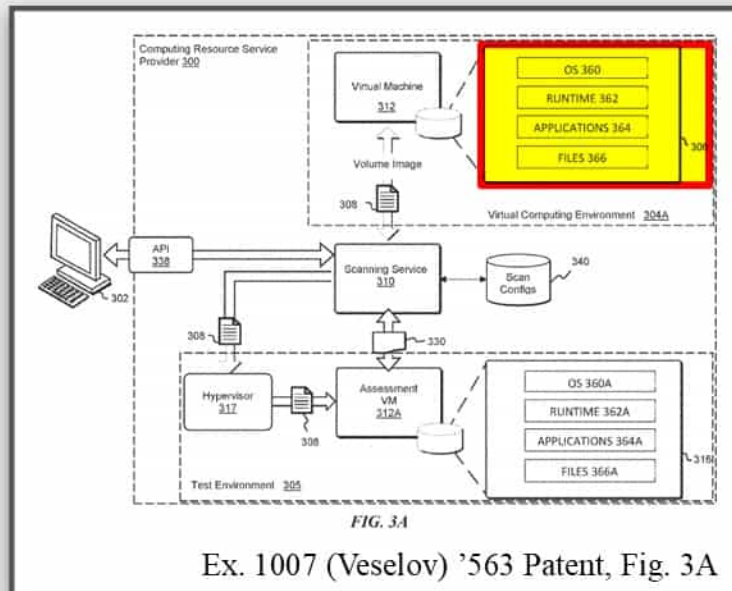
Ex. 1007 (Veselov) '563 Patent at 16:56-67



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

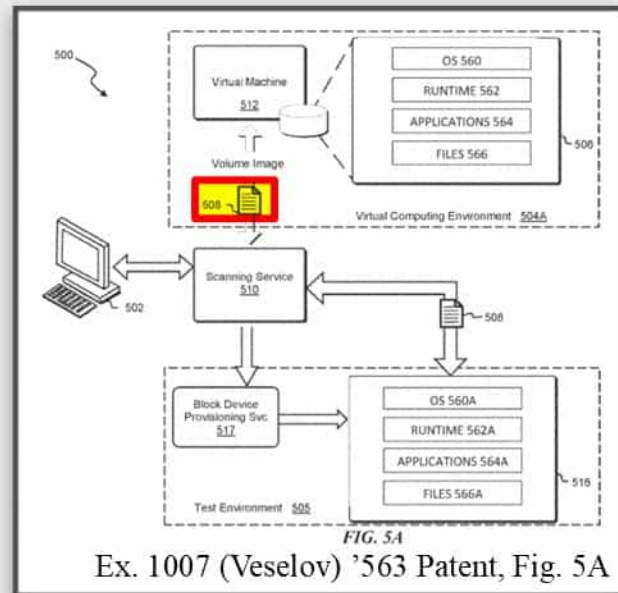
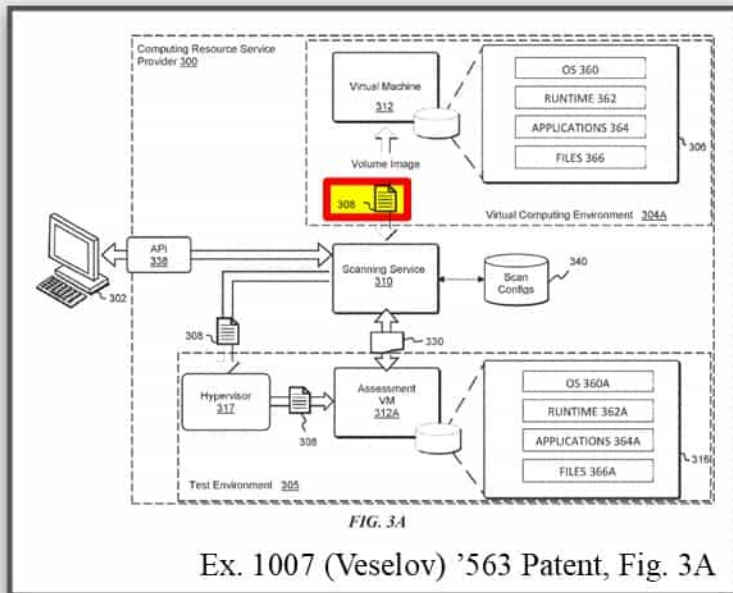
Ex. 1007 (Veselov) '563 Patent at 16:56-67



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) '563 Patent at 16:56-67



Wiz's "Undepicted" Hosting Unrelated To Computing Environment

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) '563 Patent at 18:1-15

'031 Patent (Ground 1)

- No Motivation To Combine Veselov Embodiments
- Veselov/Price Would Not Be Combined
- Cloud APIs To Identify/Locate Disks
- Analyzing Snapshot Of Inactive VMs
- Reporting As Alerts
- Claims 4/12

Veselov Collects Online Snapshots

Dr. Angelos Stavrou, Wiz's Expert

Q. It's true that the only embodiment that's actually described that lays out the state of the virtual machine in Veselov is this one where it's describing it as actively running when the snapshot is taken. In other words, just talking what you said there?

A. Yes, I believe that's correct.

Ex. 2077 Angelos Stavrou, Ph.D. Deposition at 204:11-17

Veselov Collects Online Snapshots

Dr. Angelos Stavrou, Wiz's Expert

Q. There is no reference in Veselov Exhibit 1007 to a virtual machine being offline when the snapshot is taken, true?

A. I believe that is correct.

Ex. 2077 Angelos Stavrou, Ph.D. Deposition at 204:18-21

Offline VMs Contrary To Veselov Objectives

target computing device's capabilities. For example, a server that is the target of a security assessment may not be capable of responding to a client as quickly as normal, or may not be capable of providing content as quickly as possible because processor time and memory of the target is used to perform the assessment instead of running its normal workload.

Ex. 1007 (Veselov) '563 Patent at 2:58-63

Referring to FIG. 3A, in some embodiments it may be suitable or advantageous to perform the security assessment on a different but similar virtual machine than the customer's virtual machine because the assessment can be performed without impacting the customer's virtual machine, which may be servicing requests from its customers or performing other useful work. For example, the virtual computing

Ex. 1007 (Veselov) '563 Patent at 12:21-27

Deposition of Angelos Stavrou, Ph.D.

Q. The virtual machine of Price, whether it's offline or at rest, as you put it, wouldn't be running its normal workload; is that true?

A. If it is at rest, it wouldn't be able to run its normal workload, that's true.

Q. And the virtual machine in Price, if it's offline or at rest, wouldn't be free or able to continue servicing requests; is that true as well?

A. That is true.

Ex. 2077 Angelos Stavrou, Ph.D. Deposition at 263:16-264:2

Objective Evidence: Inspecting Data “At Rest” Unconventional

panorama

SolutionsPartnersSuccess StoriesBlogContact

orca security

Unprecedented Holistic View of Cloud Security

At Panorama Technologies, we understand the importance of having a holistic view of your cloud environment. As an Orca Security partner, we employ their innovative "SideScanning"™ technology to give you complete visibility into your cloud assets, without the need for intrusive agents. This non-intrusive approach facilitates a smooth transition to Orca, focusing you on the essentials: a robust and reliable cloud security solution.

Securing Everything You Have in the Cloud

Identify and Inventory Assets

Assess and Prioritize Risks

Investigate and Remediate

Monitor and Report

Intelligent Prioritization for Decisive Action

It is not enough to detect risks; the key is to identify those that require immediate attention. Orca Security, a leader in the field of cloud security, excels in contextual risk prioritization, allowing you to optimize your resources and ensure effective protection with the least amount of effort.

Deep Protection with Data-at-Rest Analysis

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.

Orca Security Ltd.
Exhibit 2117
Wiz v. Orca
IPR2024-00863
Ex. 2117-001

Document title: Solution Orca Security - Panorama IT
Capture URL: <https://panoramait.com/en/solution-orca-security/>
Capture timestamp (UTC): Wed, 19 Mar 2025 16:14:20 GMT

Page 1 of 3



Orca Security transcends traditional solutions by inspecting data at rest, providing an additional layer of security. This unique capability reveals

Ex. 2117 at 1

REDACTED

'031 Patent (Ground 1)

- No Motivation To Combine Veselov Embodiments
- Veselov/Price Would Not Be Combined
- Cloud APIs To Identify/Locate Disks
- Analyzing Snapshot Of Inactive VMs
- Reporting As Alerts
- Claims 4/12

VMs And Virtual Disks Have Different Locations

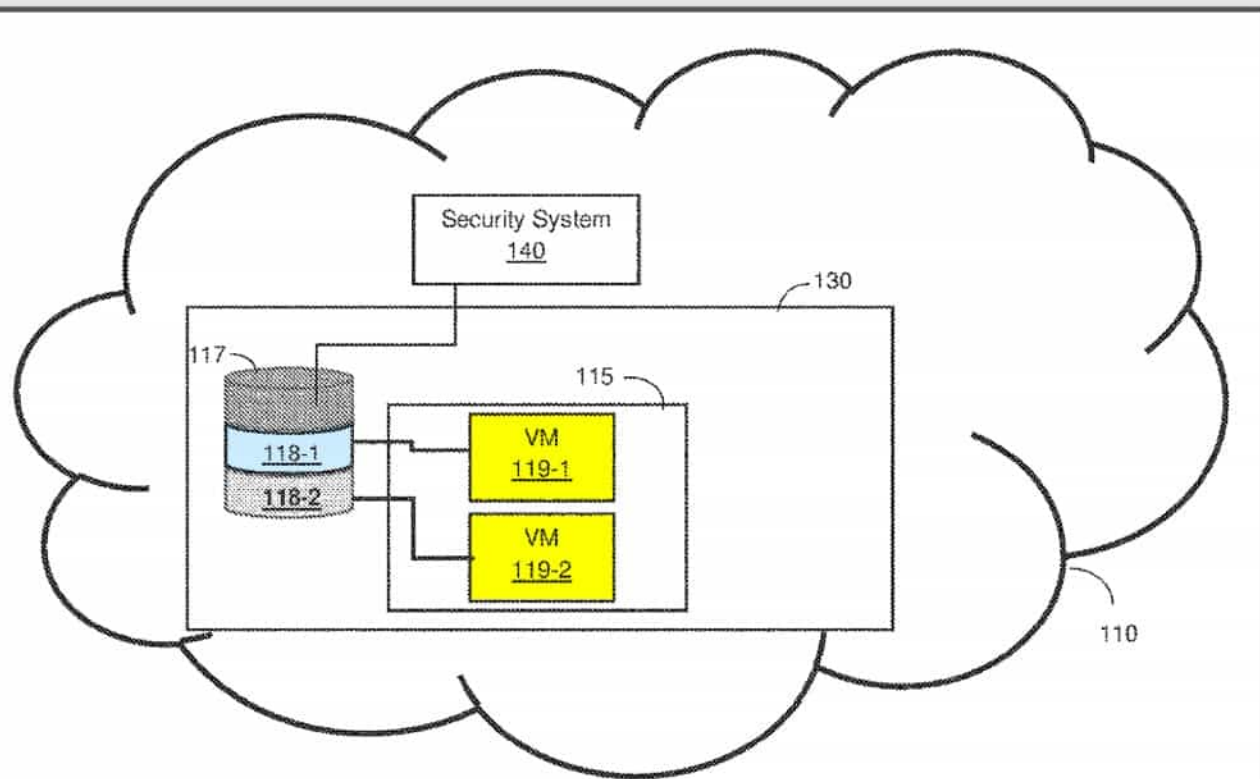


FIG. 1B

Ex.1001 (Shua) '031 Patent, Fig. 1B

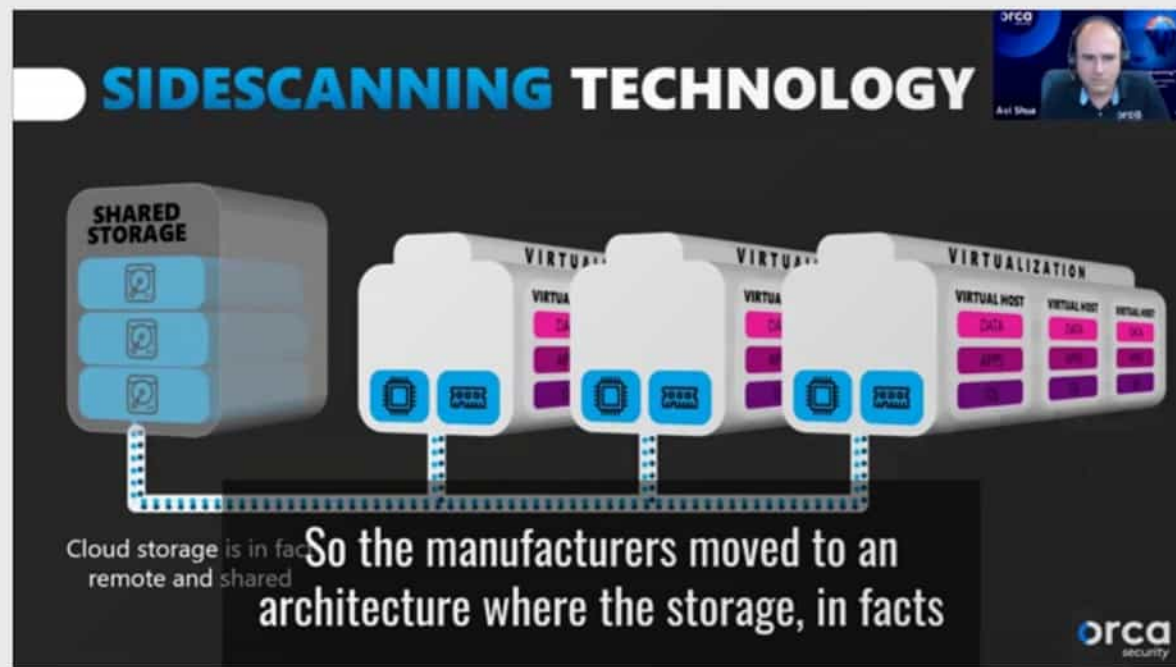
The storage **117** emulates virtual discs for the **VMs 119-1** and **119-2** executed in by the server **115**. The storage **117** is typically connected to the server **115** through a high-speed connection, such as optical fiber, allowing fast retrieval of data. In other configurations, the storage **117** may be part of the server **115**. In this example, illustrated in FIG. 1B, a virtual disk **118-1** is allocated for the VM **119-1** and the virtual disk **118-2** is allocated for the VM **119-2**. The server **115**, and, hence, the VMs **119-1** and **119-2**, may be executed in a client environment **130** within the platform **110**.

Ex.1001 (Shua) '031 Patent at 4:20-29

VMs And Virtual Disks Have Different Locations

that came the concept of virtualization clusters. Why should they care on which physical machine my workloads run? Let's just take a bunch of physical machines and treat them as my shared pool of resources. But it didn't scale very well because of many cases you needed to move data. So, the manufacturers moved to an architecture where the storage in fact sits physically on a different box. There is the shared storage box connected via high-speed fiber optics and shared

Ex.2083 at 3



Ex.2082 at 8:53

VMs And Virtual Disks Have Different Locations

Dr. Angelos Stavrou, Wiz's Expert

Q. In doing your work, in looking at prior art to see if you could map it to the claims, did you understand you had to show something showing the virtual machine and also something showing a virtual disk? Or do you think they are synonymous, and you can just find one and then you have both?

A. Again, I don't believe that the two of them are synonymous, just to be clear. But there are cases where they might be as part of the same system. I don't know if that holds here. Figure 1 points to two different elements, but in the claim here, as I have it in front of me, that is not something that I can -- I will be able to tell based on reading the claims. **They are definitely not synonymous. Virtual disks are different from virtual machines.**

3/5/2025 Stavrou Tr. at 97:13-98:10 (objections omitted)

Veselov Does Not Identify Or Locate Virtual Disks

Dr. Angelos Stavrou, Wiz's Expert

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?

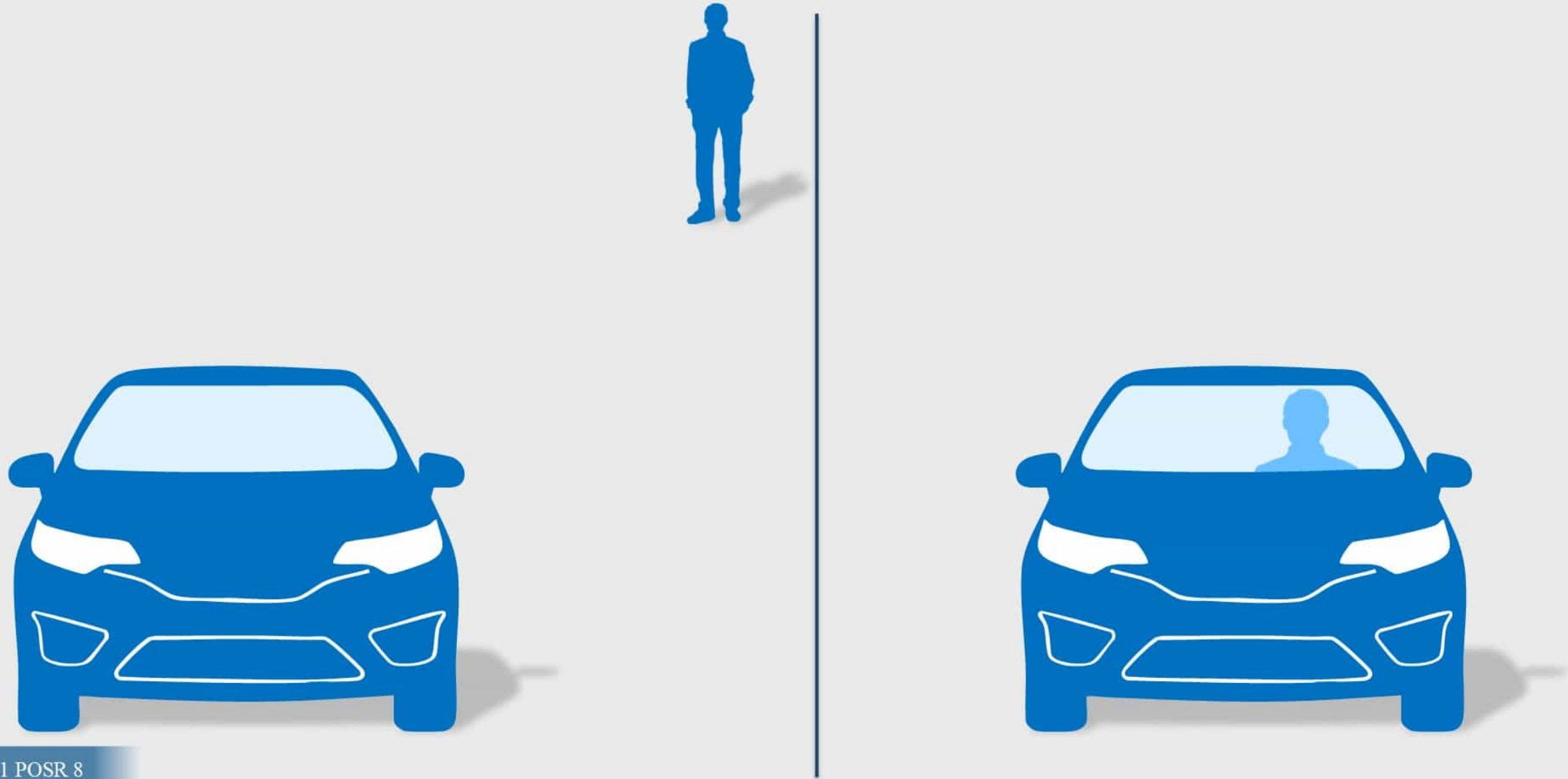
A. I'd have to look at it more carefully. I'm not -- I haven't searched the entire patent about the virtual disk identifier keyword.

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

VM Identifier Is Not Disk Location



031 POSR 8

Wiz's "Routine" Snapshot Generation "Described In Veselov"

teachings, since APIs for identifying a VM's virtual disks were a well-known feature of virtualization platforms used in cloud systems, and using such APIs to identify virtual disks of cloud-hosted VMs was a routine part of generating snapshots as described in Veselov. EX1002, ¶¶45-46, 127 (citing EX1051, 47 (disks included in snapshot), 125 (snapshot-configuration tools include drive selection); EX1052, 445-46 (UI identifies and displays disks associated with discovered VM); EX1053, ¶¶77-79 (API-based snapshot generation), 81-82 (system generating snapshot "determines the volumes of the virtual machine 110 (e.g., by calling an API function of the integration component 157 or by calling a function of the API component 210)"), 87-88 (similar), 92 (similar), Fig. 7 (steps 724, 748); EX1020, 21:9-41 (management component "discovers and identifies the virtual disks" via API), Fig. 4 (block 410)).

'031 Petition at 31

**No citations to
Veselov Ex.1007**

“Disk Identification Tools” Not In Veselov Or Combination

changed, etc.” (*id.*, 14:37-57). For the scanning service to manage the snapshot-generation process at this level of granularity, a POSA would have understood Veselov as teaching, or least suggesting, the use of commonplace disk-identification tools. EX1002, ¶128 (citing EX1051, 125 (disk identification tool used to exclude particular disks from snapshot); EX1053, ¶¶81-85 (volumes and directories/files thereon identified “to enable the administrator to select which files and/or directories are to be copied”)).

’031 Petition at 32

**No citations to
Veselov Ex.1007**

Hindsight Reconstruction: “Tailoring Snapshots”

scan data store 130. The scanning service 110 may, in some embodiments, use the scan data to determine the parameters of the security assessment, and further to identify the data elements of the virtual machine 112 that are needed to perform the security assessment. The scanning service 110

Ex. 1007 (Veselov) '563 Patent at 8:30-34

“data elements” + hindsight =

API to identify virtual disk +
query virtual disk location

REDACTED

Objective Evidence: Orca Introduced Using Cloud APIs For SideScanning

1/8/25, 9:35 AM

Redefining CNAPP: A Complete Guide To The Future of Cloud Security

Exhibit #

Stavrou 2076:

00000005_13

Redefining CNAPP: A Complete Guide To the Future of Cloud Security

This report provides a holistic view of cloud security's evolution and provides a framework for redefining the future of cloud security.

FRANCIS (SOFTWARE ANALYST) AND JAMES BERTHOTY

SEP 12, 2024

64

13

5

Share

Readers, today I'm incredibly excited to publish one of the biggest reports I've ever done within any cybersecurity industry. This report provides a holistic view of cloud security's evolution, tracing its major milestones, a detailed breakdown of the key vendors today, and evolving market shifts. It presents a new framework for redefining Cloud Native Application Protection Platforms (CNAPP), addressing its limitations and contradictions while offering a comprehensive roadmap to navigate the future of cloud security. James Berthoty and I have been working for months to make this report happen today. We hope you enjoy every part of it.

Authors of the report

- Francis is the founder of the software analyst research platform that helps security leaders understand emerging themes and industries in cybersecurity.

<https://softwareanalyst.substack.com/p/redefining-cnapp-a-complete-guide>

1/85

Orca Security Ltd.
Exhibit 2076
Wiz v. Orca
IPR2024-00863, -00864, -00865
Ex. 2076-001

- **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

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.

* * *

- **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.

Ex. 2076 at 11-12

Objective Evidence: Orca's Cloud API Use Was “Big Leap In Cybersecurity”

18/05, 9:35 AM

Redefining CNAPP: A Complete Guide To the Future of Cloud Security

Exhibit #

Stavrou 2076

Exhibit 1.5

Redefining CNAPP: A Complete Guide To the Future of Cloud Security

This report provides a holistic view of cloud security's evolution and provides a framework for redefining the future of cloud security.



FRANCIS (SOFTWARE ANALYST) AND JAMES BERTHOTY
SEP 12, 2024

64

13

5

Share

Readers, today I'm incredibly excited to publish one of the biggest reports I've ever done within any cybersecurity industry. This report provides a holistic view of cloud security's evolution, tracing its major milestones, a detailed breakdown of the key vendors today, and evolving market shifts. It presents a new framework for redefining Cloud Native Application Protection Platforms (CNAPP), addressing its limitations and contradictions while offering a comprehensive roadmap to navigate the future of cloud security. [James Berthoty](#) and I have been working for months to make this report happen today. We hope you enjoy every part of it.



Authors of the report

- Francis is the founder of the software analyst research platform that helps security leaders understand emerging themes and industries in cybersecurity.

<https://softwareanalyst.substack.com/p/redefining-cnapp-a-complete-guide>

145

Orca Security Ltd.

Exhibit 2076

Wiz v. Orca

IPR2024-00863, -00864, -00865

Ex. 2076-001

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.

Ex. 2076 at 31

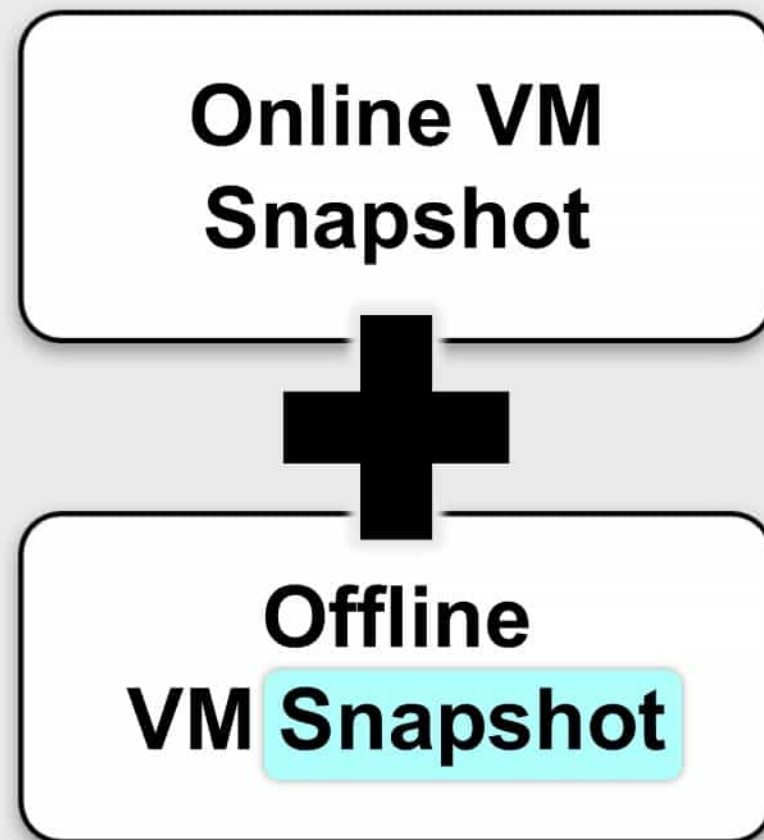
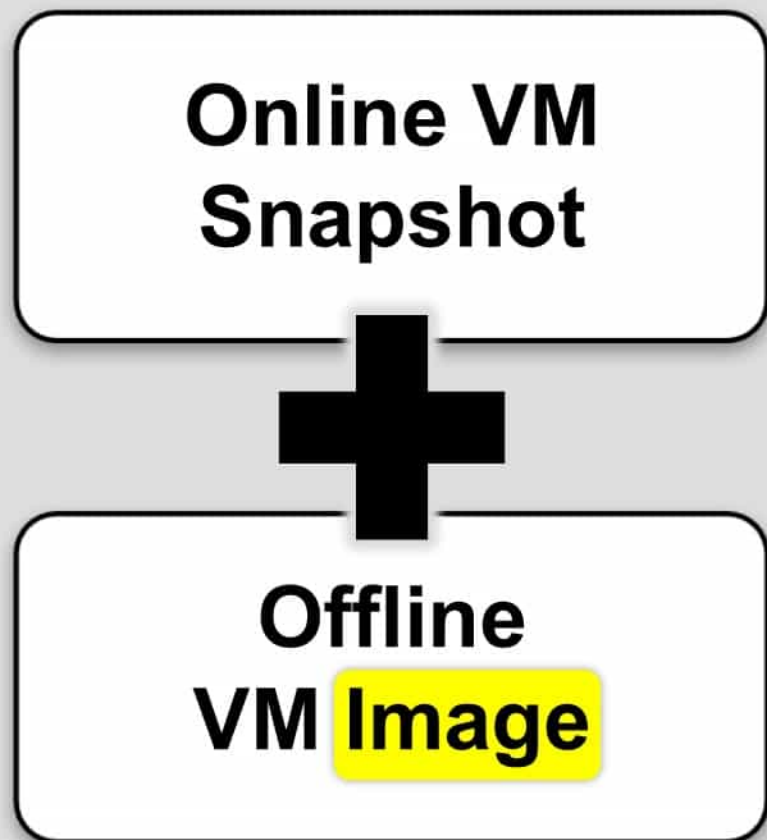
REDACTED

REDACTED

'031 Patent (Ground 1)

- No Motivation To Combine Veselov Embodiments
- Veselov/Price Would Not Be Combined
- Cloud APIs To Identify/Locate Disks
- Analyzing Snapshot Of Inactive VMs
- Reporting As Alerts
- Claims 4/12

Wiz's Hindsight Reconstruction



VM Images Are Not Snapshots

Dr. Angelos Stavrou, Wiz's Expert

Q. Do you agree with those distinctions that we just talked through here, from Paragraph 37 of your declaration?

A. Can you be more precise? What do you mean if I agree? I agree that snapshots and images are different, but they contain a lot of overlapping information, as actually is recited here.

Ex. 2077 Angelos Stavrou, Ph.D. Deposition at 272:7-13

Dr. Angelos Stavrou Reply Declaration

Before turning to the specific machine image resources that are used in cloud platforms like AWS, it is worth noting that the term “image” was often used to broadly refer to system/disk state. While this is not literally synonymous with “snapshot,” this broader sense of “image” was often used in a way that

Ex. 1400 (Stavrou Reply Decl.) at ¶ 26

“Equivalent Data” Not Enough



“[T]he combination of Woodhill and Stefik would have allowed for the selective access features of Stefik to be used with Woodhill's content-dependent identifiers feature. But that reasoning seems to say no more than that a skilled artisan, once presented with the two references, would have understood that they could be combined. And that is not enough: it does not imply a motivation to pick out those two references and combine them to arrive at the claimed invention.

Pers. Web Techs., LLC v. Apple, Inc., 848 F.3d 987, 993-994 (Fed. Cir. 2017) (internal citation/quotation omitted)

52



(10) Patent No.: US 8,011,010 B2
(45) Date of Patent: Aug. 30, 2011

2006-0155735	A1*	7/2006	Trant et al.	707/101
2006-0155931	A1	7/2006	Birrell et al.	711/115
2006-0218544	A1	9/2006	Chakraborty et al.	717/168
2006-0225065	A1	10/2006	Chandhok et al.	717/168
2006-0253706	A1	11/2006	Roberts et al.	715/106
2007-0009199	A1	1/2007	Van Riel	714/183
2007-0234337	A1*	10/2007	Suzuki et al.	717/168
2007-0256075	A1	11/2007	Dennis	718/102
2008-0104091	A1*	5/2008	McCreary et al.	719/101

OTHER PUBLICATIONS

Garfinkel, T. et al., "When Virtual is Harder than Real: Security challenges in Virtual Machine Based Computing Environments," *USENIX XFS Paper*, 2005, <http://www.usenix.org/events/hotsec05/program/program/GarfinkelGarfinkel.html>.

Markelak, T. et al., "Terra: A Virtual Machine-Based Platform for Trusted Computing," *SCISP*, 2003, 193-206.

cited by examiner

Defendants' Examinations — Issues K. G. Lee

74) *Attorney, Agent, or Firm* — Woodcock Washburn LLP

ABSTRACT

The virtual machine image may be stored as a collection of one or more virtual hard disk files. The virtual machine image

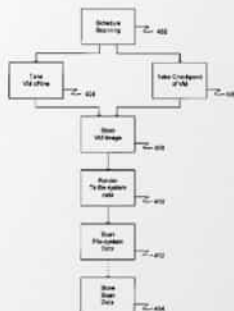
may be stored by taking the virtual machine off-line or may be stored by taking a checkpoint of the virtual machine while the virtual machine is on-line. The virtual machine image is non-

er to file-system data. Rendering the virtual machine image to file-system data may comprise mounting the virtual

engine is invoked to scan the exposed file-system data, and any indication of the corruption must be stored.

19 Claims, 8 Drawing Sheets

19 Claims, 8 Drawing Sheets



Wiz - EXHIBIT 1129
Wiz, Inc. v. Orca Security Ltd.
IPR2024-00863

Ex. 1129 (Michael) at 2:29-33

Price's Offline *Images* Important

(57)

ABSTRACT

Each virtual machine in a set of virtual machines managed by the virtual machine manager is identified. For each virtual machine in the set, it is determined whether the respective virtual machine is online. For at least the virtual machines determined to be offline, a machine image is collected for each offline virtual machine. Security of the offline virtual machines is assessed from the collected images. For virtual machines identified as online, an agent is loaded on each online virtual machine in the set via the virtual machine manager. The loaded agents are used to assess security of the online virtual machines in the set.

Ex. 1048 (Price) Pub No. 20130247133 at Abstract

virtual machine in the offline virtual machines. Assessing security of the offline virtual machines from the collected images can include simulating operation of each offline virtual machine based on data in the corresponding image of the respective virtual machine. The plurality of virtual machines

Ex. 1048 (Price) Pub No. 20130247133 at ¶ 14

Wiz's New Reply Evidence

7/13/25, 8:55 AM Amazon EC2 backup and recovery with snapshots and AMIs - AWS Prescriptive Guidance

Documentation > AWS Prescriptive Guidance > Backup and re...

<https://docs.aws.amazon.com/index.html> > <https://aws.amazon.com/prescriptive-guidance/>

Amazon EC2 backup and recovery with snapshots and AMIs

PDF (/pdfs/prescriptive-guidance/latest/backup-recovery/backup-recovery.pdf#ec2-backup) RSS (backup-recovery.rss) Focus mode

Consider whether you need to create a full backup of an EC2 instance with an Amazon Machine Image (AMI) or take a snapshot of an individual volume.

Using AMIs or Amazon EBS snapshots for backups

An AMI includes the following:

- One or more snapshots. Instance-store-backed AMIs include a template for the root volume of the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it's launched.

Note
In most cases, AMIs for Windows, Red Hat, SUSE, and SQL Server require correct licensing information to be present on the AMI. For more

<https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/ec2-backup.html>

Wiz - EXHIBIT 1131
Wiz, Inc. v. Orca Security Ltd.
IPR2024-00863

7/13/25, 8:55 AM

You can use AMIs to launch new instances with preconfigured software and data. You can create AMIs when you want to establish a baseline, which is a reusable configuration for launching more instances. When you create an AMI of an existing EC2 instance, a snapshot is taken for all the volumes that are attached to the instance. The snapshot includes the device mappings.

You can't use snapshots to launch a new instance, but you can use them to replace volumes on an existing instance. If you experience data corruption or a volume failure, you can create a volume from a snapshot that you have taken and replace the old volume. You can also use snapshots to provision new volumes and attach them during a new instance launch.

ces, it checks whether these changes violate any of the
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.
If a resource violates a rule, AWS Config flags the resour

Ex. 1131 at 1, 2, 6

New AWS Evidence Copied From Orca

6/18/25, 4:06 PM

6/18/25, 4:06 PM

CreateSnapshot - Amazon Elastic Compute Cloud

The Wayback Machine - https://web.archive.org/web/20141226192222/http://docs.aws.amazon.com:80/AWSEC2/latest/APIReference/API_CreateSnapsh...

Did this page help you? [Yes](#) | [No](#) | [Tell us about it...](#)



documentation

Amazon Elastic Compute Cloud

English ▼

[View PDF](#)

[Go to the forums](#)

CreateSnapshot

Creates a snapshot of an Amazon EBS volume and stores it in Amazon S3. You can use snapshots for backups, to make copies of Amazon EBS volumes, and to save data before shutting down an instance.

Ex. 1121 at 1

Nexpose

User's Guide

You can create the policy in JSON format using the editor in the AWS Management Console. The following code sample indicates how the policy should be defined:

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

Ex. 1122 at 1, 166

REDACTED

REDACTED

'031 Patent (Ground 1)

- No Motivation To Combine Veselov Embodiments
- Veselov/Price Would Not Be Combined
- Cloud APIs To Identify/Locate Disks
- Analyzing Snapshot Of Inactive VMs
- Reporting As Alerts
- Claims 4/12

Veselov Does Not Disclose Alerts

claims require, e.g., “report the detected vulnerabilities as alerts.” Ex. 1 at claim 1. A report and

an alert must mean different things to give meaning to all the claim language. *Merck & Co. v.*

Teva Pharms. USA, 395 F. 3d 1364, 1372 (Fed. Cir. 2005) (“A claim construction that gives

* * *

claims presuppose that one would be able to report results without using alerts. Otherwise the “as

alerts” language in the relevant claims would be superfluous. *Intel Corp. v. Qualcomm Inc.*, 21

F.4th 801, 810 (Fed. Cir. 2021) (“It is highly disfavored to construe terms in a way that renders

Ex. 2048 (Wiz’s Claim Construction Br.) at 12

Dr. Angelos Stavrou, Wiz’s Expert

“ I mean, a report is a little bit more generic term. An alert is something that potentially makes it stand out.”

Ex. 2077 Angelos Stavrou, Ph.D. Deposition at 287:4-12

Veselov's Assessment Results Are Not Alerts

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, the scanning service may associate the assessment results with the target resource, such as by identifying the target resource from a metadata tag included in the snapshot data, and then may take various actions on the assessment results including without limitation: storing the assessment results in a results data store; providing the assessment results in a user-readable format to a user interface to be displayed on the user device; if vulnerabilities are identified in the assessment results, comparing the assessment results to a remediation framework to identify one or more actions the user can take to address the vulnerabilities, and providing the identified actions to the user; and the like.

Ex. 1007 (Veselov) '563 Patent at 10:18-36

'031 Patent (Ground 1)

- No Motivation To Combine Veselov Embodiments
- Veselov/Price Would Not Be Combined
- Cloud APIs To Identify/Locate Disks
- Analyzing Snapshot Of Inactive VMs
- Reporting As Alerts
- Claims 4/12

'031 Patent Claims 4 And 12

4. The system of claim 1, wherein the identification of the location of the virtual disks of the virtual machine includes a virtual address of at least one of the virtual disks.

Ex.1001 (Shua) '031 Patent, Claim 4

12. The method of claim 9, wherein the identification of the location of the virtual disks of the virtual machine includes a virtual address of at least one of the virtual disks.

Ex.1001 (Shua) '031 Patent, Claim 12

Veselov Does Not Teach VM Identifier

Dr. Angelos Stavrou, Wiz's Expert

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.

Ex. 2077 Angelos Stavrou, Ph.D. Deposition at 142:15-143:3

'031 Patent (Ground 2)

- Veselov/Price/Hufsmith Would Not Be Combined To Arrive At Claims 2 and 10

031 Patent Claims 2 and 10

2. The system of claim 1, wherein reporting the detected vulnerabilities as alerts includes indicating **priority levels associated with the detected vulnerabilities.**

Ex. 1001 (Shua) '031 Patent, Claim 2

10. The method of claim 9, wherein reporting the detected vulnerabilities as alerts includes providing indications of the detected vulnerabilities based on **priority levels associated with the detected vulnerabilities.**

Ex. 1001 (Shua) '031 Patent, Claim 10

Hufsmith's Scores Are Associated With Container, Not Detected Vulnerabilities

2. The system of claim 1, wherein reporting the detected vulnerabilities as alerts includes indicating priority levels associated with the detected vulnerabilities.

Ex. 1001 (Shua) '031 Patent, Claim 2

severity of the risk associated with a given security issue. Hufsmith's weights are applied to evaluate "context properties" "identified within a container score record associated with a container image." Ex.1078 (Hufsmith), ¶135; *see also* Ex.1078 (Hufsmith), ¶¶135-143. The weights are used to calculate a weighted sum of vulnerabilities and therefore are used to calculate a type of "count of the number of potential vulnerabilities detected." Ex.1078 (Hufsmith) ¶90. Further, the weights are not reported as alerts, nor are they "prioritized...according to the use determinations" as claimed. In paragraph 120, cited by Dr. Stavrou, the weights

Ex. 2073 Kaeli 031 Decl. ¶ 111

Hindsight Reconstruction



“It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one skilled in the art.”

Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 448 (Fed. Cir. 1986)

Wiz's "IDE" Theories Are Hindsight Reconstruction

[0153] Independent Development Environment Configured to Annotate Source Code of Container Images with Notifications of Security Vulnerabilities

Ignore image/container

[0158] In a typical devops environment, development teams are constantly updating/creating microservices in containers and deploying them to production multiple times a day. They need to have deep insight into vulnerabilities that will be introduced by them into the container that is going to be created and deployed with their services. During that

Ignore pre-deployment context

[0180] In some embodiments, a single annotation may display information about a single security vulnerability (also referred to as a potential security vulnerability). Examples include when a scan was performed that revealed the security vulnerability, a type of scanning application that revealed the security vulnerability (or multiple instances thereof), an identifier of the body of code or other resource to which the security vulnerability pertains, and one or more classifications of the security vulnerability according to various criteria. In some cases, security vulnerabilities may be classified as high, medium, or low; scored on a scale of 1 to 10; assigned some other ordinal or cardinal classification based on attributes of vulnerabilities; labeled in a taxonomy or ontology of security vulnerabilities; or otherwise associated with classifications that make the security vulnerability faster for a developer to assess than if only provided its identifier.

Ignore annotation

Use this

Use this

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶¶ 153, 158, 180

Undisputed: Code Analysis/Annotation Inapplicable In Combination

177. Third, Dr. Stavrou cites to “annotations in a development environment”, i.e., displaying information about a vulnerability in order to show a developer particular lines of source code in a pre-deployment container image that should be addressed. Ex.1002 (Stavrou Decl.) ¶211 (citing Ex.1078 (Hufsmith) ¶¶154, 156, 180-183). This is inapplicable to Veselov, which only analyzes deployed VMs or snapshots where such source code would be unavailable for such annotating. Dr. Stavrou does not explain how or why persons of ordinary skill in the art could have or would have implemented this feature in Veselov’s systems or the proposed Veselov-Price combination. Although he asserts that this disclosure is “broadly applicable to other types of reporting,” Dr. Stavrou explicitly relies on “annotations” of the source code that persons of ordinary skill in the art would understand *not* to apply to situations, such as in the proposed Veselov-Price combination, where *source code is not available to be annotated*. Ex.1002 (Stavrou Decl.) ¶¶211-212. Even so, Dr. Stavrou does not explain how such Ex. 2073 (Kaeli Decl. ’031 Patent) at ¶ 177

'031 Patent (Ground 3)

- Veselov, Price, Hufsmith and Huseinovic would not be combined

Huseinović Counsels Against Offline Analysis

Physical memory can contain some important data such as encryption keys, open network sessions, etc. If the computer is set to off, the data are lost and cannot be retrieved for later analysis. With growth of virtual machine market, it became popular to use virtual machines for different tasks. As a consequence, virtual machine forensic recently took more place in collecting forensic data.

Ex. 1049 (Huseinović) at 940

'032 Patent (Ground 1)

- Veselov/Hufsmith Would Not Be Combined
- Determining Whether Installed Applications Are Used
- Alerts Prioritized By Use
- Dependent Claims

Hufsmith: Pre-Deployment Container/Image Scanning For Devops

images or build upon existing container images. In turn, the combined threat scores may be considered during application or container development and deployment. For example, an IDE 60 of the developer computer 58 may include a plugin 62 to request one or more combined threat scores for container images or distributed applications.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶108

results engine 54. An example policy may indicate the applications and container images must be scanned and that their scores must meet a specific threshold or benchmark to be deployed in a given environment. The score evaluator 135B may reject distributed applications or containers that do not meet the policy. As described above, combined threat

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶147

[0158] In a typical devops environment, development teams are constantly updating/creating microservices in containers and deploying them to production multiple times a day. They need to have deep insight into vulnerabilities that will be introduced by them into the container that is going to be created and deployed with their services. During that development cycle, there is often no easy way for a developer or team of developers to determine if the images and files they are using, e.g., in a given base image, for a container are safe. They have often no insight into the vulnerabilities of the image and files prior to deployment from within the IDE.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶158

Hufsmith: Monitor Highly Complex Development Environments

[0005] In many cases, the bodies of code and other resources by which the services are implemented can be challenging to secure. Often, the range of services is relatively diverse and arises from diverse sets of bodies of code and other resources, thereby increasing the number of potential vulnerabilities. Further, such bodies of code and other resources can undergo relatively frequent version changes, and in many cases the bodies of code and other resources, are downloaded from third parties that create the bodies of code and other resources, such as public repositories that may be un-trusted or accorded less trust than code built in-house. Consequently, detecting and managing potential vulnerabilities in distributed application code and other resources can be particularly complex.

* * *

[0155] In some cases, container images can be relatively complex, with more than five, and in many cases more than a dozen or two dozen constituent layers, and each of those layers can be subject to potential security vulnerabilities of varying types or varying risk. Developers often struggle with managing security vulnerabilities when faced with this complexity. The cognitive load of developing container images standing alone is relatively high, and layering on complexity from managing security vulnerabilities can

Ex. 1078 (Hufsmith) ¶¶ 05, 155

Veselov: Post-Deployment Snapshot Assessments For Owners/Administrators

in accordance with various embodiments. In some embodiments, the target resource is one or more executing instances of a virtual machine 312 or of a plurality of virtual machines. Instances of the virtual machine 312 may execute within a virtual computing environment 304A, 304B that may enable certain operations and interactions of instances of the virtual machine 312 as well as impose limits on operations and interactions. For example, the virtual computing environ-

Ex. 1007 (Veselov) '563 Patent at 10:41-48

In any case, the snapshot is prepared so that the security assessment produces the results that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance. 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 4:1-8

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) '563 Patent at 2:42-54

POSA Would Not Add Pre-Deployment Complexity Contrary To Veselov's Objectives

EX1078, ¶¶109, 113-28. Hufsmith uses a “context evaluator” to adjust weights for vulnerabilities identified by other evaluators based on various context properties.

'032 Pet. 38

user interface, like a dashboard a report.” *Id.*, ¶96. Such reports can be “comprehensive” and convey an overall score for the resource and information about individual vulnerabilities. *Id.*, ¶¶31-33 (“comprehensive” report of image’s exposure), 36 (results engine may provide “scoring information”); *see also id.*, ¶¶120 (CVE evaluator reports weights), 128 (malware evaluator reports weights); EX1002, ¶162. Hufsmith teaches, or at least suggests, that this reported

'032 Pet. 42

Hufsmith's Multitude Of Scanners Important

(57)

ABSTRACT

Provided is a process for determining threat scores for container images or distributed applications that consider the results of a multitude of different scanners and other factors such as context information which may include information about a given execution environment for the container image. Scanner results, or scanner properties, are determined for a container image or container images in a multi-container distributed application by various vulnerability scanners. The scanner properties determined by each

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at Abstract

[0002] The present disclosure relates generally to tooling for software development related to distributed applications and, more specifically, to techniques that combine metrics of heterogeneous vulnerability scans of container images.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶ 2

Wiz's Alert Fatigue Problem Doesn't Apply To Veselov

[0155] In some cases, container images can be relatively complex, with more than five, and in many cases more than a dozen or two dozen constituent layers, and each of those layers can be subject to potential security vulnerabilities of varying types or varying risk. Developers often struggle with managing security vulnerabilities when faced with this complexity. The cognitive load of developing container images standing alone is relatively high, and layering on complexity from managing security vulnerabilities can potentially lead to missed vulnerabilities and less secure code. Further, even when developers are aware of such security vulnerabilities, accessing relevant information to assess the risk and potentially mitigate those risks is difficult and cumbersome, particularly when the developer needs to keep in mind both aspects of the container image and larger distributed application as well as aspects of the security vulnerabilities.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶155

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

Wiz's Alert Fatigue Problem Doesn't Apply To Veselov

Containers vs. VMs: What's the difference?

In a nutshell, containers and virtual machines (VMs) are two inherently different approaches to packaging and deploying applications/services in isolated environments.

Ex. 2075 (Stavrou) at 1

Containers and VMs both provide isolation and hence security, but on different levels.

* * *

With containers, the processes, file system, and resources (CPU, RAM, disk) also have flexible isolation, making containers more prone to vulnerabilities. With good security measures and scanning tools like Wiz and Kubescape, you can, however,

Ex. 2075 (Stavrou) at 6

'032 Patent (Ground 1)

- Veselov/Hufsmith Would Not Be Combined
- Determining Whether Installed Applications Are Used
- Alerts Prioritized By Use
- Dependent Claims

Hufsmith Discloses Active/Dormant Application Modules

Execution environment records may further indicate which portions of a container image are dormant and which are active in a given use case. For instance, a container image may include a subroutine that registered with a network socket, but a composition file or other code may indicate that the subroutine is never invoked. Or a container image may include a library with module having a sys.exec command based on a passed value, but a call graph of the larger distributed application may indicate that the sys.exec command module is never called. Environmental context may be hand-coded by a developer or inferred from the composition file or other configuration data of the distributed application. Vulnerabilities associated with dormant code may be down-weighted in some cases.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶140

'032: Application Modules Are Not Installed Applications

tions. Further, the security system 140 may be configured to match the application files, either directly (using binary comparison) or by computing a cryptographic hash against database of files in vulnerable applications. The matching may be also on sub-modules of an application. Alternatively,

Ex.1001 (Shua) '032 Patent at 5:37-41

determining, based on the matching, an existence of potential cyber vulnerabilities of the protected virtual cloud asset;
determining whether the matching installed applications are used by the protected virtual cloud asset;

Ex.1001 (Shua) '032 Patent, Claim 1

10. The method of claim 9, wherein scanning the parsed snapshot further includes at least one of:
checking configuration files of applications and an operating system installed in the protected virtual cloud asset;
verifying access times to files by the operating system installed in the in the protected virtual cloud asset; or
analyzing system logs to deduce applications and modules executed in the protected virtual cloud asset.

Ex.1001 (Shua) '032 Patent, Claim 10

Whether A “File Or Code Is Executed,” Not Whether Installed Applications Are Used

[0121] The malware evaluator 115 may evaluate malware properties 116 identified within a container score record associated with a container image. The malware properties 116 may list known potential malicious files, i.e., malicious or infected files, detected within the container image. Potential malicious files may be listed by an identifier of each file (e.g., file name/location) and may include information about the file. The information about the file may include image-specific information determined about the file such as a file name, file type, file location, file size, hash of the file, hash of a malicious portion of the file, one or more virus/malware signatures, whether the file or code is executed, etc. determined during a scan of the container image. The information

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶121

(Stavrou Decl.) ¶153. Dr. Stavrou further asserts that “[d]iscussing the calculation of individual weights for malware—which includes installed applications that are infected with malware—the malware evaluator considers ‘whether the file or code is executed (i.e., whether the matching installed application is used by the protected virtual cloud asset).’ Ex.1002 (Stavrou Decl.) ¶153. But again, this calculation involves evaluating whether a “file or code” is executed, and such “file or code” is simply a portion of a larger “application package in a container image” even if it has malware. Ex.1078 (Hufsmith) ¶¶121, 123. Thus, in both passages Dr. Stavrou cites for disclosure of this limitation, Hufsmith only determines whether a particular component of an application (file, subroutine, etc.) is executed, but does not teach or suggest determining whether an installed application is used.

Ex. 2073 (Kaeli Decl. 032 Patent) at ¶ 99

'032 Patent (Ground 1)

- Veselov/Hufsmith Would Not Be Combined
- Determining Whether Installed Applications Are Used
- Alerts Prioritized By Use
- Dependent Claims

Wiz's "Report" Argument Prioritizes Resources, Not Vulnerabilities

- [1.5] determining whether the matching installed applications are used by the protected virtual cloud asset;
- [1.6] prioritizing the potential cyber vulnerabilities based on the use determinations; and
- [1.7] reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.

Ex.1001 (Shua) '032 Patent, Claim 1

Although Veselov does not expressly describe reporting the vulnerabilities as “prioritized alerts according to the use determinations,” Hufsmith teaches this feature. Hufsmith describes reporting vulnerabilities to “a user, for instance, in a user interface, like a dashboard a report.” *Id.*, ¶96. Such reports can be “comprehensive” and convey an overall score for the resource and information about individual vulnerabilities. *Id.*, ¶¶31-33 (“comprehensive” report of image’s

'032 Petition at 42

Wiz's "IDE" Theory Inapplicable To Combination

Hufsmith further teaches this limitation with its discussion of presenting annotations in a development environment. In these embodiments—teachings that apply to other embodiments (EX1078, ¶¶154, 156; EX1002, ¶163)—the system presents annotations that “display information about a single security vulnerability” such as a classification or score. *Id.*, ¶¶180-82. The vulnerabilities

’032 Petition at 42-43

Undisputed: Hufsmith's IDE Annotations Inapplicable To Veselov

implemented this feature in Veselov's systems. Although he asserts that this disclosure "also appl[ies] to the other embodiments," Dr. Stavrou explicitly relies on "annotations" of the source code that persons of ordinary skill in the art would understand *not* to apply to situations, such as in Veselov, where *source code is not available to be annotated*. Ex.1002 (Stavrou Decl.) ¶¶163-164. And without the

Ex. 2073 (Kaeli Decl. 032 Patent) at ¶ 111

Dr. Angelos Stavrou Reply Declaration

discussed in the IDE embodiments. He states that these teachings are "inapplicable to Veselov, which only analyzes deployed VMs or snapshots where *such source code would be* unavailable for such annotating." Kaeli-Dec, ¶177. As I explained above, however, the *combination does not involve a wholesale incorporation of the embodiment into Veselov (i.e., literally performing source-code annotations)*, nor is that how a POSA would have approached the combination. *Supra*, §VII.A;

Ex. 1400 (Stavrou 032 Reply Decl.) ¶ 59

Hindsight Reconstruction

[0153] Independent Development Environment Configured to Annotate Source Code of Container Images with Notifications of Security Vulnerabilities

Ignore image/container

[0158] In a typical devops environment, development teams are constantly updating/creating microservices in containers and deploying them to production multiple times a day. They need to have deep insight into vulnerabilities that will be introduced by them into the container that is going to be created and deployed with their services. During that

Ignore pre-deployment context

[0180] In some embodiments, a single annotation may display information about a single security vulnerability (also referred to as a potential security vulnerability). Examples include when a scan was performed that revealed the security vulnerability, a type of scanning application that revealed the security vulnerability (or multiple instances thereof), an identifier of the body of code or other resource to which the security vulnerability pertains, and one or more classifications of the security vulnerability according to various criteria. In some cases, security vulnerabilities may be classified as high, medium, or low; scored on a scale of 1 to 10; assigned some other ordinal or cardinal classification based on attributes of vulnerabilities; labeled in a taxonomy or ontology of security vulnerabilities; or otherwise associated with classifications that make the security vulnerability faster for a developer to assess than if only provided its identifier.

Ignore

Use this

Use this

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶¶ 153, 158, 180

'032 Patent (Ground 1)

- Veselov/Hufsmith Would Not Be Combined
- Determining Whether Installed Applications Are Used
- Alerts Prioritized By Use
- Dependent Claims 4-5
- Dependent Claims 16 and 20

Claim 4 – “Known” Is Not Enough

4. The method of claim 1, wherein determining whether the matching installed applications are used by the protected virtual cloud asset includes **verifying access times to files** by an operating system of the protected virtual cloud asset to determine whether at least one of the matching installed applications is not in use by the protected virtual cloud asset, and wherein prioritizing reduces priority of potential cyber vulnerabilities for a matching installed application not in use.

Ex.1001 (Shua) '032 Patent, Claim 4

cloud asset. Hufsmith describes a variety of ways to determine whether the matching installed applications are used, including “[e]xecution environment records.” EX1078, ¶140. While **Hufsmith does not expressly state** that these records include access times to files by an operating system, this would have been obvious to a POSA because such **access times were a common part of such records and because use determinations such as those described in Hufsmith were routinely and predictably performed by verifying such access times.** EX1007, 9:55-67

'032 Petition at 46



“The Board reasonably identified a **gap between the concept of a look-up table being well-known and the beneficial application of that concept to Carter’s gaming system ... And it reasonably found that simply calling the addition of a look-up table ‘an obvious design choice’ did not fill that gap.**”

Fanduel, Inc. v. Interactive Games LLC, 966 F.3d 1334, 1344 (Fed. Cir. 2020)

Claim 5 – “Known” Is Not Enough

5. The method of claim 2, wherein determining whether the matching installed applications are used by the protected virtual cloud asset includes analyzing application logs or system logs to determine matching installed applications not in use by the protected virtual cloud asset, and wherein prioritizing reduces priority of potential cyber vulnerabilities for at least one of the matching installed applications not in use.

Ex.1001 (Shua) '032 Patent, Claim 5

installed applications is not in use by the protected virtual cloud asset. Records such as application logs and system logs were routinely kept in cloud systems such as those described in Veselov and Hufsmith, and they were also routinely analyzed during these types of security assessments. EX1007, 9:55-67 (snapshot includes

* * *

includes analyzing application logs or system logs. EX1002, ¶178. At a minimum, this would have been obvious since use determinations such as those described in Hufsmith were routinely made by analyzing such logs. EX1002, ¶¶178-80 (citing EX1079, 33-36; EX1063, ¶¶126, 184).

'032 Petition at 47-48

'032 Patent (Ground 1)

- Veselov/Hufsmith Would Not Be Combined
- Determining Whether Installed Applications Are Used
- Alerts Prioritized By Use
- Dependent Claims 4-5
- Dependent Claims 16 and 20

Claims 16 and 20

16. 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.

* * *

20. The non-transitory computer readable medium of claim 18, 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.

Ex. 1001 '032 Patent, Claim 16, 20

Wiz's Laundry List Of Alternative Theories Fail

the snapshot's location. *Supra*, §XI.B.3. Querying consoles to determine resource locations was also a **common step** when managing and securing computer resources. *Id.*; EX1009, 221, 257-60; EX1015, 56, 124, 164-66, EX1031, 1

'032 Pet. at 66



“The Board reasonably identified a **gap between the concept of a look-up table being well-known and the beneficial application of that concept to Carter's gaming system ... And it reasonably found that simply calling the addition of a look-up table ‘an obvious design choice’ did not fill that gap.**”

Fanduel, Inc. v. Interactive Games LLC, 966 F.3d 1334, 1344 (Fed. Cir. 2020)

Wiz's Laundry List Of Alternative Theories Fail

computing environment); EX1002, ¶232; *supra*, §XI.C.9. 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 (scanning service may provide logical volume's parameters to hypervisor). This teaches or at a minimum suggests querying the console to

'032 Pet. at 67

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

Wiz's Laundry List Of Alternative Theories Fail

nevertheless obvious. For example, 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 determine the snapshot's general location (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, ¶232; *supra*, §XI.C.9. Veselov also teaches

'032 Pet. at 67

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)

'032 Patent (Ground 2)

- Veselov/Hufsmith/Hutchins Would Not Be Combined

Claim 12

12. The method of claim 11, 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.

Ex. 1001 '032 Patent, Claim 12

Wiz Abandoned Reliance On Assessment-VM

combination discussed in Ground 1 for multiple reasons. First, Veselov describes remediation generally but does not provide a detailed discussion of specific remediation steps, while Hutchins describes a similar snapshot-based security assessment that uses the well-known remediation step of quarantining a VM, making the combination a straightforward, routine implementation of Veselov's

'032 Pet. at 70

Regardless, the petition does not depend on the assessment-VM approach. Pet., 40-45; EX1400, ¶10. Thus, mooted PO's claim-construction argument.

'032 Reply. at 2

Hutchins Analyzes Running VMs

combined with, Veselov's approach. Veselov discloses scanning operations that are focused on a "scannable volume" from a snapshot captured at a specific point in time. *E.g.* Ex.1007 (Veselov) 10:1-2. In contrast, as discussed above, Hutchins is directed towards offloading resource-intensive (i.e., virus scanning) applications to replicated VMs. Ex.1070 (Hutchins) ¶53; *see also* Section VII.C. Application of Hutchins to Veselov would require additional resources beyond those provided for in Veselov. At best, Hutchins's approach has similarities to Veselov's Figs.

Ex. 2073 (Kaeli Decl.'032 Patent) at ¶ 135

[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 scanning operation can be fairly resource-intensive; the resource usage spike might be prohibitive in a virtual machine environment unless it is offloaded. By offloading this task onto the replicated virtual machine, the virus scan can run on the replicated disk image. This enables the segregation of the resource requirements of the scanning process from the original virtual machine and enables the enforcement of resource utilization policies for the scanning process without affecting the original virtual machine. For example, the resources granted to the replicated virtual machine could be bounded such that the overall impact of performance for other virtual machines is negligible, or the replicated virtual machine could be moved off to a different physical host computer that might be optimized for handling virtual machines performing certain specific tasks.

Ex. 1070 (Hutchins) at ¶ 53

'685 Patent (Ground 1)

- POSA Would Not Combine Veselov/Hufsmith
- No Cloud APIs To Identify/Locate Disks
- Improper Veselov Embodiment Mixing
- Analyzing Snapshots To Detect Vulnerabilities And Sensitive Data
- Reporting Vulnerabilities And Sensitive Data As Filtered and Prioritized Alerts
- Dependent Claims

Hufsmith: Pre-Deployment Container/Image Scanning For Devops

images or build upon existing container images. In turn, the combined threat scores may be considered during application or container development and deployment. For example, an IDE 60 of the developer computer 58 may include a plugin 62 to request one or more combined threat scores for container images or distributed applications.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶108

results engine 54. An example policy may indicate the applications and container images must be scanned and that their scores must meet a specific threshold or benchmark to be deployed in a given environment. The score evaluator 135B may reject distributed applications or containers that do not meet the policy. As described above, combined threat

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶147

[0158] In a typical devops environment, development teams are constantly updating/creating microservices in containers and deploying them to production multiple times a day. They need to have deep insight into vulnerabilities that will be introduced by them into the container that is going to be created and deployed with their services. During that development cycle, there is often no easy way for a developer or team of developers to determine if the images and files they are using, e.g., in a given base image, for a container are safe. They have often no insight into the vulnerabilities of the image and files prior to deployment from within the IDE.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶158

Hufsmith: Monitor Highly Complex Development Environments

[0005] In many cases, the bodies of code and other resources by which the services are implemented can be challenging to secure. Often, the range of services is relatively diverse and arises from diverse sets of bodies of code and other resources, thereby increasing the number of potential vulnerabilities. Further, such bodies of code and other resources can undergo relatively frequent version changes, and in many cases the bodies of code and other resources, are downloaded from third parties that create the bodies of code and other resources, such as public repositories that may be un-trusted or accorded less trust than code built in-house. Consequently, detecting and managing potential vulnerabilities in distributed application code and other resources can be particularly complex.

* * *

[0155] In some cases, container images can be relatively complex, with more than five, and in many cases more than a dozen or two dozen constituent layers, and each of those layers can be subject to potential security vulnerabilities of varying types or varying risk. Developers often struggle with managing security vulnerabilities when faced with this complexity. The cognitive load of developing container images standing alone is relatively high, and layering on complexity from managing security vulnerabilities can

Ex. 1078 (Hufsmith) ¶¶ 41, 50, 155

Veselov: Post-Deployment Snapshot Assessments For Owners/Administrators

in accordance with various embodiments. In some embodiments, the target resource is one or more executing instances of a virtual machine 312 or of a plurality of virtual machines. Instances of the virtual machine 312 may execute within a virtual computing environment 304A, 304B that may enable certain operations and interactions of instances of the virtual machine 312 as well as impose limits on operations and interactions. For example, the virtual computing environ-

Ex. 1007 (Veselov) '563 Patent at 10:41-48

In any case, the snapshot is prepared so that the security assessment produces the results that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance. 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 4:1-8

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) '563 Patent at 2:42-54

POSA Would Not Add Pre-Deployment Complexity Contrary To Veselov's Objectives

The detected security issues are prioritized. EX1002, ¶94. First, a set of evaluators—e.g., ¹a configuration evaluator, ²CVE evaluator, ³malware evaluator, ⁴CWE evaluator—assign weights (i.e., priorities) to each detected security risk. EX1078, ¶¶111-34. ⁵A context evaluator then determines global weights (or risk levels) that adjust the individual weights. *Id.*, ¶¶135-43; *see also id.*, ¶140 (down-weighting vulnerabilities associated with dormant code).

'685 Pet. at 18

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) '563 Patent at 2:42-54

Hufsmith And Veselov Inspect Different Data For Different Purposes

[0158] In a typical devops environment, development teams are constantly updating/creating microservices in containers and deploying them to production multiple times a day. They need to have deep insight into vulnerabilities that will be introduced by them into the container that is going to be created and deployed with their services. During that development cycle, there is often no easy way for a developer or team of developers to determine if the images and files they are using, e.g., in a given base image, for a container are safe. They have often no insight into the vulnerabilities of the image and files prior to deployment from within the IDE.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶158

images or build upon existing container images. In turn, the combined threat scores may be considered during application or container development and deployment. For example, an IDE 60 of the developer computer 58 may include a plugin 62 to request one or more combined threat scores for container images or distributed applications.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶108

In any case, the snapshot is prepared so that the security assessment produces the results that the scanning system otherwise would have obtained if the security assessment were performed on the original virtual machine instance. 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 4:1-8

Wiz's Tertiary References Discuss Unrelated Contexts

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

* * *

ous ways. In some implementations, the network monitor 102 allows users to view assets, vulnerabilities, or threats, sorted by the aggregate risk metric for the asset, vulnerability, or threat. For example, the network monitor 102 can list all

Ex. 1008 at ¶¶ 1, 138

[0135] The context evaluator 125 may evaluate context properties 126 identified within a container score record associated with a container image. The context properties 126 may include version history 127, score history 128, environments 129, or other contextual information for a container image to which the container score record corresponds. The context evaluator 125 may determine base

Ex. 1008 at ¶¶ 1, 138

[0129] Agent 400 is an exemplary agent configured to record events associated with application instances, identify records generated by other applications, provide copies of records (e.g., both the agent-generated records as well as the records generated by other applications) to the security assessment system 202.

Ex. 1063 at ¶ 129

Wiz's Alert Fatigue Problem Doesn't Apply

[0155] In some cases, container images can be relatively complex, with more than five, and in many cases more than a dozen or two dozen constituent layers, and each of those layers can be subject to potential security vulnerabilities of varying types or varying risk. Developers often struggle with managing security vulnerabilities when faced with this complexity. The cognitive load of developing container images standing alone is relatively high, and layering on complexity from managing security vulnerabilities can potentially lead to missed vulnerabilities and less secure code. Further, even when developers are aware of such security vulnerabilities, accessing relevant information to assess the risk and potentially mitigate those risks is difficult and cumbersome, particularly when the developer needs to keep in mind both aspects of the container image and larger distributed application as well as aspects of the security vulnerabilities.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶155

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

Wiz's Alert Fatigue Problem Doesn't Apply

Containers vs. VMs: What's the difference?

In a nutshell, containers and virtual machines (VMs) are two inherently different approaches to packaging and deploying applications/services in isolated environments.

Ex. 2075 (Stavrou) at 1

Containers and VMs both provide isolation and hence security, but on different levels.

* * *

With containers, the processes, file system, and resources (CPU, RAM, disk) also have flexible isolation, making containers more prone to vulnerabilities. With good security measures and scanning tools like Wiz and Kubescape, you can, however,

Ex. 2075 (Stavrou) at 6

Detecting Vulnerabilities And Sensitive Data Was Not Traditional

WIZ Platform - Solutions - Pricing - Resources - Customers - Company - Sign in - Get a demo

Blog

Wiz becomes the first CNAPP to deliver integrated Data Security Posture Management

Wiz expands its platform to proactively eliminate attack paths to discovered critical data.

George Pisha November 21, 2022 4 minute read

“Wiz alerts us with laser precision and all the context needed to take fast proactive action to prevent issues from becoming data breaches.”

Asonye Onwudebe
Cloud Security Architect, Chevron Phillips

When it comes to mission-critical data in the cloud era, exposure can become an incident in hours. Research has shown that an unsecured database can be breached in 8 hours flat. That's why we're excited to launch our new Data Security Posture Management (DSPM) capabilities to continuously monitor for critical data exposure so organizations can respond before a breach occurs. Our new features include visibility into PII, PHI, and PCI data; any exposure paths to that critical data that can be exploited; and how those exposure paths came to be. DSPM enables customers to proactively protect their cloud data, dramatically reducing the time it takes to discover and fix data exposure.

Orca Security Ltd.
Exhibit 2155
Wiz v. Orca
IPR2024-00865
Ex. 2155-001

Document title: Wiz becomes the first CNAPP to deliver integrated Data Security Posture Management | Wiz Blog
Capture URL: https://www.wiz.io/blog/wiz-becomes-first-cnapp-to-deliver-integrated-data-security-posture-management
Capture timestamp (UTC): Tue, 25 Mar 2025 10:00:43 GMT

Page 1 of 7

- [1.6] analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine;
- [1.7] determine a risk level of the virtual machine; and
- [1.8] report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.

Ex.1001 (Shua) '685 Patent, Claim 1



George Pisha
November 21, 2022



3+ Years Later

However, securing cloud data is a difficult problem. An organization with hundreds of data assets and tens of thousands of data items could have millions of individual configurations, permissions, and lifecycle policies to manage—this is far from a human-scale problem. Protecting a database from just simple network exposure is a complex problem that shows the limitations of taking siloed approaches to understanding cloud data risks. Traditional siloed tools don't capture the full picture when it comes to exposure and they completely miss complex risks that involve vulnerabilities and lateral movement. You would need many siloed tools that lack context and manual correlation across data and cloud to detect attack paths to critical data as they form. Wiz DSPM enables customers to get ahead of the data exposure problem with a comprehensive platform that understands data risks at cloud scale.

Ex. 2155 at 2

'685 Patent (Ground 1)

- POSA Would Not Combine Veselov/Hufsmith
- No Cloud APIs To Identify/Locate Disks
- Improper Veselov Embodiment Mixing
- Analyzing Snapshots To Detect Vulnerabilities And Sensitive Data
- Reporting Vulnerabilities And Sensitive Data As Filtered and Prioritized Alerts
- Dependent Claims

Wiz's 685 Patent Theories Are Wrong For Same Reason As 031 Patent

'031 Patent Petition

4. Elements 1.2, 9.2, and 16.2

Veselov teaches these elements, which recite “using the interface, utilize cloud computing platform APIs” (or “using the interface to utilize cloud computing

5. Elements 1.3, 9.3, and 16.3

Veselov teaches these elements, which recite “[use/using] the computing platform APIs to query a location of at least one of the identified virtual disks.”

6. Elements 1.4, 9.4, and 16.4

Veselov teaches element 1.4, which recites “[receive/receiving] an identification of the location of the virtual disks of the virtual machine,” in several ways.

'031 Pet. at 28, 33, 35

'685 Patent Petition

4. Element 1.2, 13.2, and 22.2

Veselov teaches these elements, which recite “using the interface, utilize cloud computing platform APIs” (or “using the interface to utilize cloud computing platform APIs”) “to identify virtual disks of a virtual machine in the client

5. Element 1.3, 13.3, and 22.3

Veselov teaches these elements, which recite “[use/using] the computing platform APIs to query a location of at least one of the identified virtual disks.”

6. Element 1.4, 13.4, and 22.4

Veselov teaches element 1.4, which recites “[receive/receiving] an identification of the location of the virtual disks of the virtual machine,” in several ways.

'685 Pet. at 29, 33, 34

'685 Patent (Ground 1)

- POSA Would Not Combine Veselov/Hufsmith
- No Cloud APIs To Identify/Locate Disks
- Improper Veselov Embodiment Mixing
- Analyzing Snapshots To Detect Vulnerabilities And Sensitive Data
- Reporting Vulnerabilities And Sensitive Data As Filtered and Prioritized Alerts
- Dependent Claims

Hufsmith Detects Weaknesses/Vulnerabilities, Not Sensitive Data

The assessment also identifies potential exposure of various types of sensitive data such as “confidential information” and “information about an encryption key.”

EX1078, ¶181; EX1002, ¶160; *see also* EX1078, ¶118 (scan may assess “confidentiality impact” by quantifying exposure of “restricted information”). At a
’685 Pet. at 39

[0181] In some cases, the annotation may include an indication of a type of harm associated with the security vulnerability, like indicating that the security vulnerability potentially allows for execution of remotely supplied code from an attacker, indicating that the security vulnerability potentially allows for the exfiltration of confidential information, indicating that the vulnerability leaks information about an encryption key, or indicating the security vulnerability potentially allows an attacker to direct network traffic elsewhere in a denial of service attack.

* * *

the value from the current line of text. In some embodiments, the annotation may include links to bug reports and issue tracker entries addressing the security vulnerability.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶ 181

'685: Detect Vulnerabilities And Sensitive Data

The snapshot is parsed and analyzed by the security system 140 to detect vulnerabilities. This analysis of the snapshot does not require any interaction and/or information from the VM 119. As further demonstrated herein, the analysis of the snapshot by the system 140 does not require any agent installed on the server 115 or VM 119.

Ex.1001 (Shua) '685 Patent at 5:19-24

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 (Shua) '685 Patent at 6:19-30

Veselov/Hufsmith Does Not Detect Vulnerabilities And Sensitive Data

Wiz's Veselov/Hufsmith Combination

■ - Vulnerabilities



'685 Patent

■ - Vulnerabilities

■ - Vulnerabilities *and* sensitive data



'685: Prioritize Sensitive Data

In an embodiment, any detected cyber threats related to sensitive data (including personally identifiable information, PII) is reported at a higher priority. In an embodiment, such

Ex.1001 (Shua) '685 Patent at 6:46-48

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

22 Nov, 2022 13:29

Ofir Dor



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

Agentless Cloud Sensitive Data Detection Was Not Routine

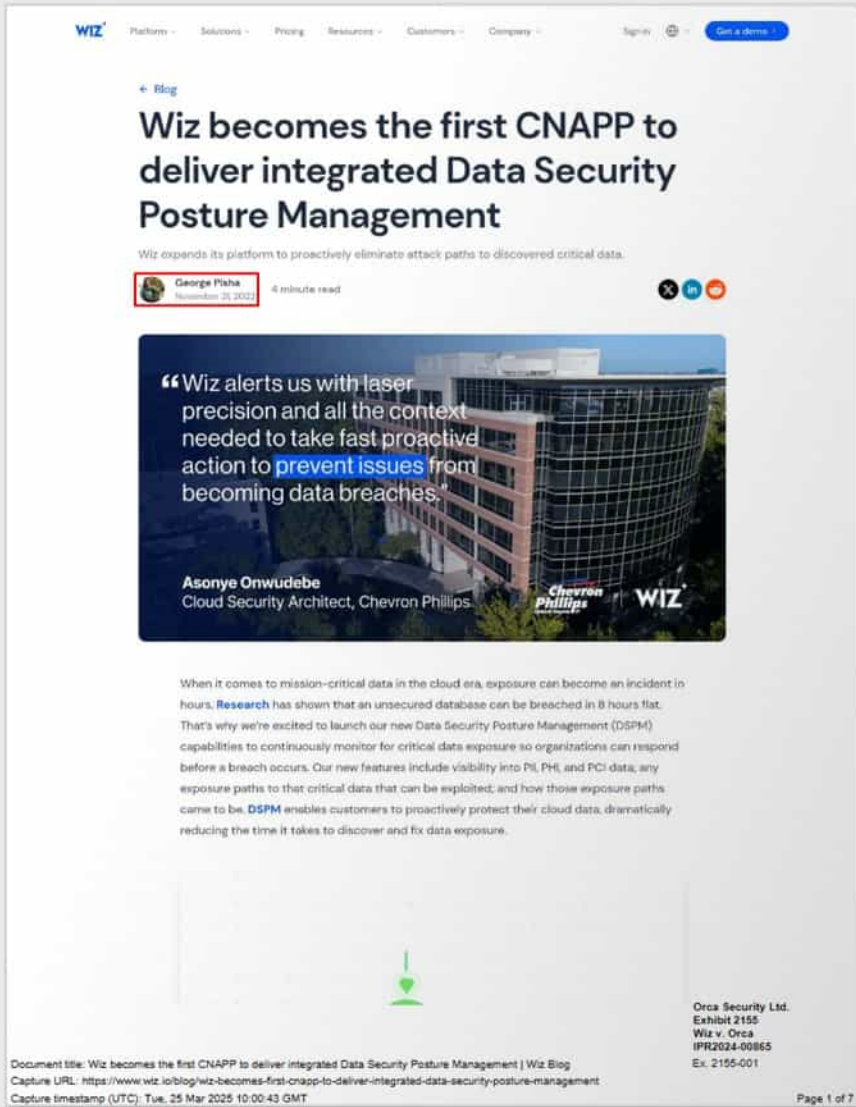
Wiz VP product strategy Raaz Herzberg says the combination of CSPM and DSPM gives Wiz increased strength. "Our advantage is the ability to combine the analysis of sensitive information with the mapping we do of the entire environment. This intersection helps us give a complete picture of the risks in 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



Detecting Vulnerabilities And Sensitive Data Was Not Traditional



- [1.6] analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine;
- [1.7] determine a risk level of the virtual machine; and
- [1.8] report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.

Ex.1001 (Shua) '685 Patent, Claim 1



George Pisha
November 21, 2022



3+ Years Later

However, securing cloud data is a difficult problem. An organization with hundreds of data assets and tens of thousands of data items could have millions of individual configurations, permissions, and lifecycle policies to manage—this is far from a human-scale problem. Protecting a database from just simple network exposure is a complex problem that shows the limitations of taking siloed approaches to understanding cloud data risks. Traditional siloed tools don't capture the full picture when it comes to exposure and they completely miss complex risks that involve vulnerabilities and lateral movement. You would need many siloed tools that lack context and manual correlation across data and cloud to detect attack paths to critical data as they form. Wiz DSPM enables customers to get ahead of the data exposure problem with a comprehensive platform that understands data risks at cloud scale.

Ex. 2155 at 2

'685 Patent (Ground 1)

- POSA Would Not Combine Veselov/Hufsmith
- No Cloud APIs To Identify/Locate Disks
- Improper Veselov Embodiment Mixing
- Analyzing Snapshots To Detect Vulnerabilities And Sensitive Data
- Reporting Vulnerabilities And Sensitive Data As Filtered and Prioritized Alerts
- Dependent Claims

Wiz Relies On Development Environment Annotations

This limitation is further suggested by Hufsmith's express discussion of reporting alerts associated with both vulnerabilities and sensitive data. Hufsmith describes reporting granular alerts via annotations in a development environment, a reporting technique that Hufsmith suggests applying to other reporting approaches. EX1078, ¶¶153-54 (annotation techniques may be used "in conjunction with the approaches above"), 156 (same), 180 (annotation "may display information about a single security vulnerability"); EX1002, ¶170. These notifications include specific alerts for identified vulnerabilities and sensitive data exposures. EX1078, ¶¶181 (annotation may indicate potential "exfiltration of confidential information" or leak of "information about an encryption key"), 182 (annotation may include "discrete entries for each of the security vulnerabilities"); EX1002, ¶170.

'685 Pet. at 42-43

No Dispute Pre-Deployment Code Annotations Inapplicable In Combination

Although he asserts that this disclosure “also appl[ies] to the other embodiments,”

Dr. Stavrou explicitly relies on “annotations” of the source code that persons of

ordinary skill in the art would understand *not* to apply to situations, such as in

Veselov, where *source code is not available to be annotated*. Ex.1002 (Stavrou

Decl.) ¶¶169-170. And without the source code available, Hufsmith’s stated

objectives of annotating the source code—e.g., to increase awareness “earlier in

the workflow of container development” and identify vulnerabilities “in a more

real time manner” (Hufsmith ¶160)—do not apply. A person of ordinary skill in

the art would not have had a reasonable expectation of success in combining these

cited portions of Hufsmith with Veselov as a result. In addition, a person of

Ex. 2073 (Kaeli) ’685 Decl. ¶ 152

Dr. Angelos Stavrou Reply Declaration

52. I also disagree with Dr. Kaeli’s arguments involving Hufsmith’s

discussion of annotations in the IDE embodiments. He states that these teachings

are “inapplicable to Veselov, which only analyzes deployed VMs or snapshots

where such source code would be unavailable for such annotating.” Kaeli-Dec,

¶152 (arguing no reasonable expectation of success for the same reason). As I

explained above, however, the combination does not involve a wholesale

incorporation of that embodiment into Veselov. *Supra*, §VI.B. Dr. Kaeli’s focus

Ex. 1400 (Stavrou) ’685 Reply Decl. ¶ 52

Hindsight Reconstruction

[0153] Independent Development Environment Configured to Annotate Source Code of Container Images with Notifications of Security Vulnerabilities

Ignore image/container

[0158] In a typical devops environment, development teams are constantly updating/creating microservices in containers and deploying them to production multiple times a day. They need to have deep insight into vulnerabilities that will be introduced by them into the container that is going to be created and deployed with their services. During that

Ignore pre-deployment context

[0180] In some embodiments, a single annotation may display information about a single security vulnerability (also referred to as a potential security vulnerability). Examples include when a scan was performed that revealed the security vulnerability, a type of scanning application that revealed the security vulnerability (or multiple instances thereof), an identifier of the body of code or other resource to which the security vulnerability pertains, and one or more classifications of the security vulnerability according to various criteria. In some cases, security vulnerabilities may be classified as high, medium, or low; scored on a scale of 1 to 10; assigned some other ordinal or cardinal classification based on attributes of vulnerabilities; labeled in a taxonomy or ontology of security vulnerabilities; or otherwise associated with classifications that make the security vulnerability faster for a developer to assess than if only provided its identifier.

Ignore annotation

Use this

Use this

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶¶ 153, 158, 180

Wiz's Annotations Are Vulnerabilities, Not Sensitive Data

[0181] In some cases, the annotation may include an indication of a type of harm associated with the security vulnerability, like indicating that the security vulnerability potentially allows for execution of remotely supplied code from an attacker, indicating that the security vulnerability potentially allows for the exfiltration of confidential information, indicating that the vulnerability leaks information about an encryption key, or indicating the security vulnerability potentially allows an attacker to direct network traffic elsewhere in a denial of service attack. In some embodi-

* * *

the value from the current line of text. In some embodiments, the annotation may include links to bug reports and issue tracker entries addressing the security vulnerability.

Ex. 1078 (Hufsmith) Pub. No. 20200097662 at ¶ 181

Annotations Inapplicable To Veselov's Read-Only Snapshots

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

Ex. 1007 (Veselov) U.S. Patent No. 11,216,563 B1 at 18:1-3

copied to produce the volume image. At step 610, the scanning service may format the new logical volume into the corresponding file system and then mount the volume image in the logical volume as a read-only virtual hard disk.

Ex. 1007 (Veselov) U.S. Patent No. 11,216,563 B1 at 18:26-29

'685 Patent (Ground 1)

- POSA Would Not Combine Veselov/Hufsmith
- No Cloud APIs To Identify/Locate Disks
- Improper Veselov Embodiment Mixing
- Analyzing Snapshots To Detect Vulnerabilities And Sensitive Data
- Reporting Vulnerabilities And Sensitive Data As Filtered and Prioritized Alerts
- **Dependent Claims**

Wiz's Claim 2 and 14 Arguments Are Admittedly Wrong

1. Dependent Claims 2 and 14

Claims 2 and 14 depend from claims 1 and 13, respectively, and further recite “wherein during the analysis of the at least one snapshot, the virtual machine is inactive wherein the snapshot includes a page file of memory associated with the virtual machine.” Veselov teaches these limitations.

Veselov teaches “wherein during the analysis of the at least one snapshot, the virtual machine is inactive,” as recited. As discussed below with respect to '685 Pet. at 45

known, as demonstrated by the combination of Veselov and Price. Veselov teaches every aspect of the independent claims, except that it does not expressly describe requesting taking a snapshot of the VM at rest (one of two recited alternatives, the other simply being “taking a snapshot”) or analyzing the snapshot while the VM is inactive. However, these were common techniques, as shown by '031 Pet. at 1

'685 Patent (Ground 2)

- POSA Would Not Combine Veselov/Hufsmith/Chari

Chari's Incompatibility With Veselov

[0037] Virtual machine image manager 218 inserts labeler 222 and sanitizer 224 in each virtual machine image that virtual machine image manager 218 generates. In other words,

Ex. 1056 (Chari) Pub. No. 20150033221 at ¶ 37

[0039] Labeler 222 includes labeling scripts 228, labeling policies 230, and labeling script execution policies 232. Labeling scripts 228 are programming language scripts, such as Perl scripts, Python scripts, or shell scripts, that labeler 222 uses to identify and label sensitive data contained within a virtual machine based on labeling policies 230. Labeling

Ex. 1056 (Chari) Pub. No. 20150033221 at ¶ 39

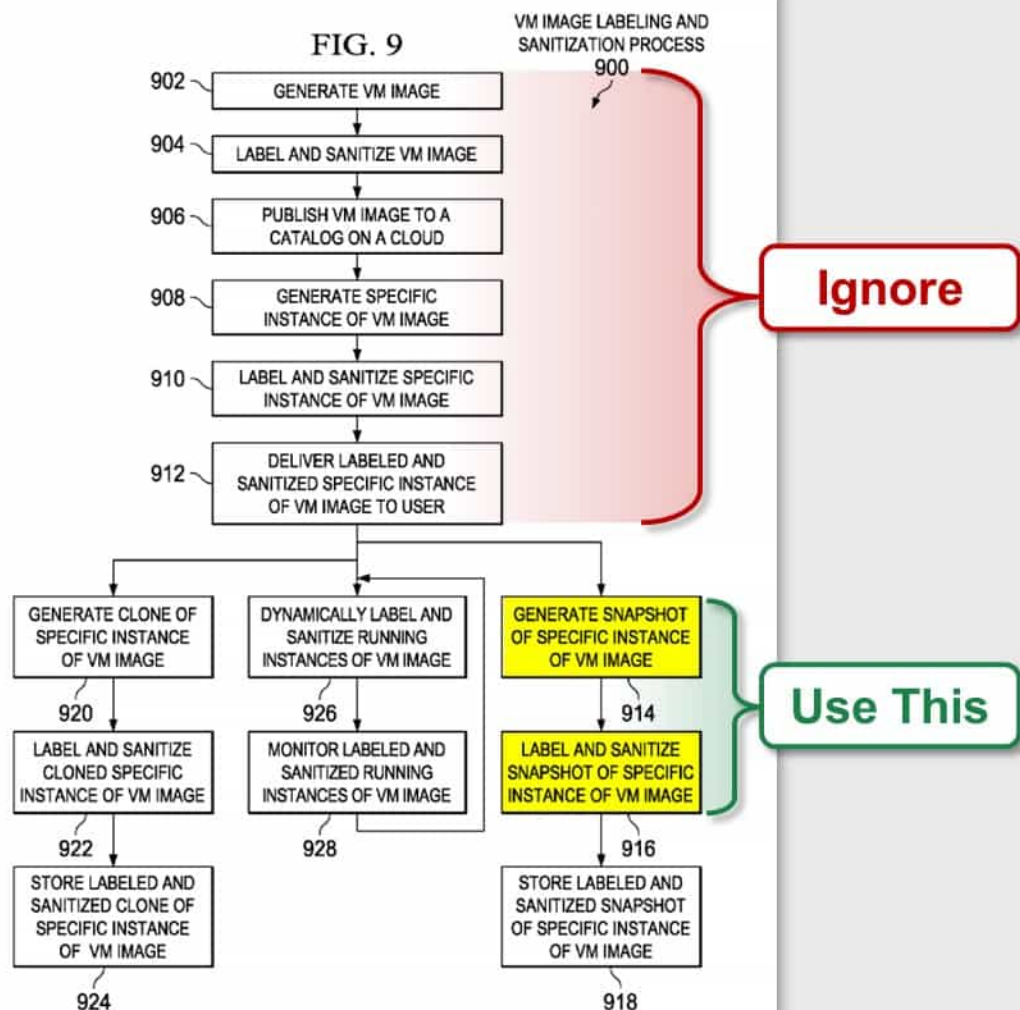
The scanning service 510 may mount volume images as read only to avoid inadvertently modifying the volume corresponding to a volume image. A public key or other

Ex. 1007 (Veselov) U.S. Patent No. 11,216,563 B1 at 18:1-3

copied to produce the volume image. At step 610, the scanning service may format the new logical volume into the corresponding file system and then mount the volume image in the logical volume as a read-only virtual hard disk.

Ex. 1007 (Veselov) U.S. Patent No. 11,216,563 B1 at 18:26-29

Wiz's Hindsight Reconstruction



[0094] Further, the virtual machine image manager generates a snapshot of the specific instance of the virtual machine image at 914. The virtual machine image manager may generate the snapshot of the specific instance of the virtual machine image for rollback purposes in case the specific instance of the virtual machine image fails or becomes corrupted. In addition, the virtual machine image manager labels and sanitizes the snapshot of the specific instance of the virtual machine image at 916 and stores the labeled and sanitized snapshot of the specific instance of the virtual machine image at 918.

Ex. 1056 (Chari) Pub. No. 20150033221, Fig. 9

Ex. 1056 (Chari) Pub. No. 20150033221 at ¶ 37

Wiz's Hindsight Reconstruction

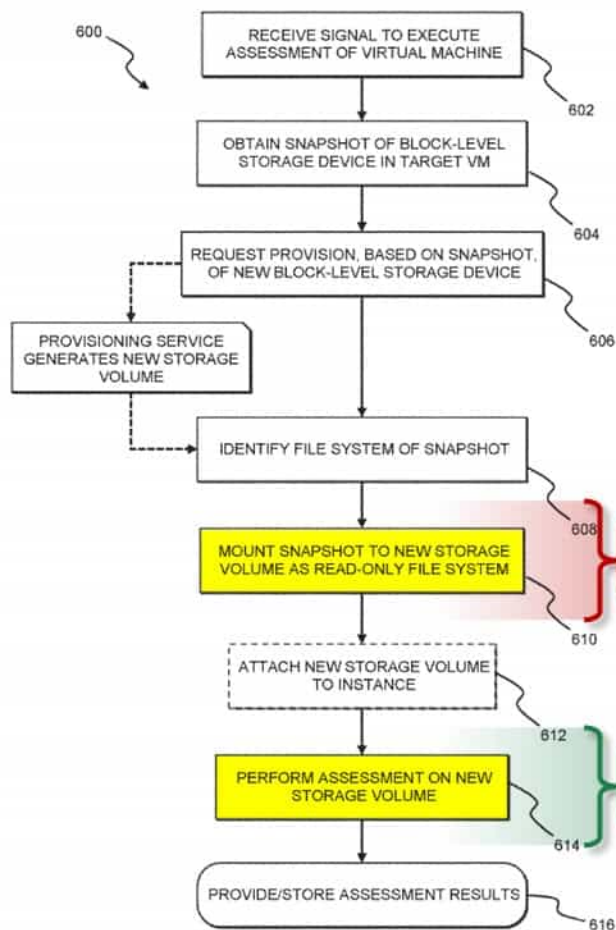


FIG. 6

Ex. 1007 (Veslov) U.S. Patent No. 11,216,563 B1, Fig. 6

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) U.S. Patent No. 11,216,563 B1 at 17:1-3

Use This

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

Ex. 1007 (Veslov) U.S. Patent No. 11,216,563 B1 at 18:1-3

Ignore

copied to produce the volume image. At step 610, the scanning service may format the new logical volume into the corresponding file system and then mount the volume image in the logical volume as a read-only virtual hard disk.

Ex. 1007 (Veslov) U.S. Patent No. 11,216,563 B1 at 18:26-29

Ignore

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)

'685 Patent Ground 3

- POSA Would Not Combine
Veselov/Hufsmith/Chari/Price/Huseinović

'685 Patent, Claims 2-3 and 14-15

2. The system of claim 1, wherein during the analysis of the at least one snapshot, the virtual machine is inactive wherein the snapshot includes a page file of memory associated with the virtual machine.

Ex. 1001 (Shua) '685 Patent, Claim 2

14. The method of claim 13, wherein during the analysis of the at least one snapshot, the virtual machine is inactive wherein the snapshot includes a page file of memory associated with the virtual machine.

Ex. 1001 (Shua) '685 Patent, Claim 14

3. The system of claim 2, wherein the page file is configured to allow deduction of one or more applications running on the virtual machine.

Ex. 1001 (Shua) '685 Patent, Claim 3

15. The method of claim 14, wherein the page file is configured to allow deduction of one or more applications running on the virtual machine.

Ex. 1001 (Shua) '685 Patent, Claim 15

Huseinović Counsels Against Offline Analysis

Physical memory can contain some important data such as encryption keys, open network sessions, etc. If the computer is set to off, the data are lost and cannot be retrieved for later analysis. With growth of virtual machine market, it became popular to use virtual machines for different tasks. As a consequence, virtual machine forensic recently took more place in collecting forensic data.

Ex. 1049 (Huseinović) at 940

By using VMware workstation it is possible to choose two natively supported options to save a physical memory State and data. The first one is preserving appropriate *vmem* file (by using suspend option) and the second option is to take a virtual machine snapshot. File *vmem* is virtual machine paging file. The snapshot consists of multiple files: *vmdk* (the redo log), *vmssd* (snapshot metadata) and *vmssn* (snapshot state). [2]

Ex. 1049 (Huseinović) at 940

Claim Construction

**(i) Taking at Least One Snapshot,
and (ii) Requesting Taking at Least
One Snapshot of the
Virtual Machine at Rest**

Orca's Construction

“of the Virtual Machine at Rest” modifies both “(i) taking at least one snapshot” and “(ii) requesting taking at least one snapshot....”

Wiz's Construction

“of the Virtual Machine at Rest” modifies only “(i) taking at least one snapshot”

Claim Language

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

- establish an interface between a client environment and security components;
- using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment;
- use the computing platform APIs to query a location of at least one of the identified virtual disks;
- receive an identification of the location of the virtual disks of the virtual machine;
- perform at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time;
- analyze the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive; and
- report the detected vulnerabilities as alerts.

Actions

Subject

Ex.1001 (Shua) '031 Patent, Claim 1

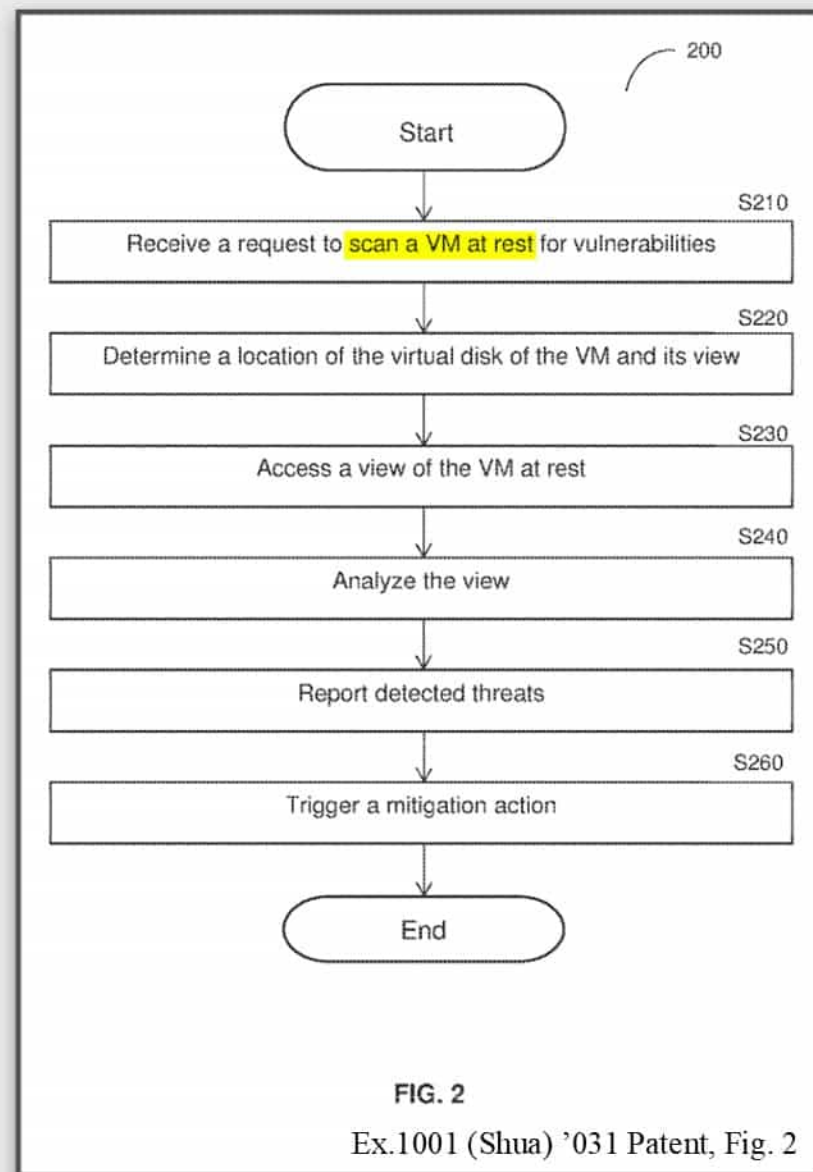
Written Description

(57)

ABSTRACT

A method and system for securing virtual cloud assets at rest against cyber threats. The method comprises determining a location of a view of at least one virtual disk of a protected virtual cloud asset, wherein the virtual cloud asset is at rest and, when activated, instantiated in the cloud computing environment; accessing the view of the virtual disk based on the determined location; analyzing the view of the protected virtual cloud asset to detect potential cyber threats risking the protected virtual cloud asset, wherein the virtual cloud asset is inactive during the analysis; and alerting detected potential cyber threats based on a determined priority.

Ex.1001 (Shua) '031 Patent, Abstract



Various techniques disclosed herein include techniques for securing data at rest or machines at rest (collectively referred to as “machines at rest”). Data at rest may include

Ex.1001 (Shua) '031 Patent at 3:45-47

Written Description

The disclosed techniques are utilized to scan for embedded vulnerabilities in machines at rest, when the machine is powered off. For example, a machine at rest may be utilized

Ex.1001 (Shua) '031 Patent at 3:53-55

The '031 Patent's Title

TECHNIQUES FOR SECURING VIRTUAL CLOUD ASSETS AT REST AGAINST CYBER THREATS

Ex.1001 (Shua) '031 Patent



“The patent’s title—’Universal Folding Boom Trailer’—also indicates that a relevant artisan would understand that the claims require a universal folding boom trailer ... The title thus reinforces what the written description makes clear.”

Wastow Enters., LLC v. Truckmovers.com, Inc., 855 F. App’x 748, 750-51 (Fed. Cir. 2021)

Prosecution History

20. (Currently Amended) A system for inspecting data, the system comprising:

at least one processor configured to:

establish an interface between a client environment and security components;

using the interface, utilize cloud computing platform APIs to identify virtual disks

of a virtual machine in the client environment;

use the computing platform APIs to query a location of at least one of the

identified virtual disks;

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

generate perform at least one of taking a snapshot of the virtual machine at

rest, or requesting the snapshot of the virtual disks of the virtual machine at

rest, wherein the snapshot represents a copy of the virtual disks of the

virtual machine at a point in time;

analyze the ~~at least one~~ snapshot to detect vulnerabilities; and

report the detected vulnerabilities as alerts.

Ex.1004 at 123 (Claim Amendments Filed June 30, 2022)

Claim 20, as amended, recites, inter alia:

"...perform at least one of: (i) taking at least one snapshot, and (ii)

requesting taking at least one snapshot of the virtual machine at rest,

wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time; and

analyze the at least one snapshot to detect vulnerabilities; and report the detected vulnerabilities as alerts."

Ex.1004 at 130 (Claim Amendments Filed June 30, 2022)

Prosecution History

Claim 20, as amended, recites, *inter alia*:

“...perform at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time; and
analyze the at least one snapshot to detect vulnerabilities; and report the detected vulnerabilities as alerts.”

Ex.1004 at 130 (Claim Amendments Filed June 30, 2022)

Regarding Derbeko

The Examiner asserted that in Col. 4:35-54 Derbeko describes ‘*analyzing the snapshot in isolation when VM is not running*’. Applicant respectfully disagrees. A direct quotation of Derbeko from Col. 4:35-54 is provided below:

“analyzing snapshots of VMs, instead of the VMs **while running**, may enable isolation of a detecting module from the malware itself.” (emphasis added).

Thus, while analyzing Derbeko's snapshot, the VM is not at rest, as required by claim 20, **but is running** (e.g., active). Nor does Derbeko describe taking and analyzing a snapshot while the VM is at rest elsewhere.

Ex.1004, 131 (Applicant Arguments for Claim Amendments Filed June 30, 2022)

Prosecution History

Claim 20, as amended, recites, *inter alia*:

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

analyze the at least one snapshot to detect vulnerabilities; and report the detected vulnerabilities as alerts.”*

Ex.1004 at 130 (Claim Amendments Filed June 30, 2022)

Regarding Bansal

The Examiner asserted that Bansal describes taking snapshots of VMs including the virtual disks of the VMs when the VM is powered off. However, nowhere does Bansal describe analyzing snapshots to detect vulnerabilities. Rather, Bansal uses snapshots to backup a virtual machine. In fact, Bansal's technique would perpetuate an existing vulnerability in a powered-off machine, and thus also does solve or attempt to solve the problem addressed by the pending claims, e.g., to analyze a snapshot taken while the VM is at rest to detect vulnerabilities.

Ex.1004, 131 (Applicant Arguments for Claim Amendments Filed June 30, 2022)



“Edwards points out that, during prosecution, the inventors amended claim 12 (which ultimately issued as claim 1 of the '073 patent) and its dependent claims to delete the word “intraluminal,” modifying ‘graft.’...Thus, Edwards argues, the inventors specifically intended for ‘graft’ to have a meaning broader than ‘intraluminal graft.’ However, the accompanying remarks stated that ‘[i]ndependent claim 12 defines an *intraluminal* graft.’....Thus, the inventors’ statements urged a change in claim language that did not affect the breadth of the claim, and we cannot allow the claim to now be broadened.”

Edwards Lifesciences LLC v. Cook Inc., 582 F.3d 1322, 1330–31 (Fed. Cir. 2009)

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

Regardless, the petition does not depend on the assessment-VM approach.

Pet., 40-45; POR, 11-12. PO's embodiment-mixing argument is wrong (*infra*, §III.A), mooted PO's claim-construction argument.

031 Pet. Reply at 4

Wiz's Expert Performed No Analysis

Dr. Angelos Stavrou, Wiz's Expert

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

encompass “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

Ex.2073 (Kaeli '031 Decl), ¶55

Objective Indicia

Objective Indicia



“The objective indicia of non-obviousness play an important role as a guard against the statutorily proscribed hindsight reasoning in the obviousness analysis. Indeed, we have held that evidence of secondary considerations may often be the most probative and cogent evidence in the record.”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1328 (Fed. Cir. 2016)

Nexus



“Where the allegedly obvious patent claim is a combination of prior art elements, we have explained that the patent owner can show that it is the claimed combination as a whole that serves as a nexus for the objective evidence; proof of nexus is not limited to only when objective evidence is tied to the supposedly ‘new’ feature(s).”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1330-31 (Fed. Cir. 2016)

The Problems Solved By The Inventions

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) '031 Patent at 1:49-52; Ex. 1001 (Shua) ('032 Patent) at 1:52-55; Ex. 1001 (Shua) ('685 Patent) at 1:49-52

The Problems Solved By The Inventions

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

Ex. 1001 (Shua) '031 Patent at 1:57-64 ; Ex. 1001 (Shua) ('032 Patent) at 1:60-67; Ex. 1001 (Shua) ('685 Patent) at 1:57-64

The Problems Solved By The Inventions

e.g., based on the volume of traffic. However, the monitor can detect threats only based on the monitored traffic. For example, misconfiguration of the server may not be detected by the traffic monitor. As such, traffic monitoring would not allow for detection of vulnerabilities in software executed by the server.

Ex. 1001 (Shua) '031 Patent at 2:1-6; Ex. 1001 (Shua) ('032 Patent) at 2:4-9; Ex. 1001 (Shua) ('685 Patent) at 2:1-6

The Problems Solved By The Inventions

e.g., based on the volume of traffic. However, the monitor can detect threats only based on the monitored traffic. For example, misconfiguration of the server may not be detected by the traffic monitor. As such, traffic monitoring would not allow for detection of vulnerabilities in software executed by the server.

Ex. 1001 (Shua) '031 Patent at 2:1-6; Ex. 1001 (Shua) ('032 Patent) at 2:4-9; Ex. 1001 (Shua) ('685 Patent) at 2:1-6

The Problems Solved By The Inventions

or data center. Using agents is a cumbersome solution for a number of reasons, including IT resource management, governance, and performance. For example, installing agents in a large data center may take months.

Ex. 1001 (Shua) '031 Patent at 2:11-15; Ex. 1001 (Shua) ('032 Patent) at 2:14-17; Ex. 1001 (Shua) ('685 Patent) at 2:11-15

The Problems Solved By The Inventions ('031 Patent)

for the rest in the year. While at rest, the machines are powered off, and are not inspected for vulnerabilities, simply because scanners and/or installed monitoring agents cannot operate on a powered-off machine.

Another attempt would be to scan a machine at rest when the machine is powered on and preserving a log of its latest status. However, this would require keeping an updated log of the machine's configurations and all its applications. Further, as threats constantly evolve, scanning based on past information may not be relevant. As such, when data or a machine at rest becomes active, undetected vulnerabilities can pose cyber threats.

Ex. 1001 (Shua) '031 Patent at 2:25-36

The Solution

In an embodiment, the interface between the client environment 130 and the security system 140 can be realized using APIs or services provided by the cloud computing platform 110. For example, in AWS, a cross account policy service can be utilized to allow interfacing the client envi-

Ex. 1001 (Shua) '031 Patent at 4:51-54; Ex. 1001 (Shua) '032 Patent at 4:18-23; Ex. 1001 (Shua) '685 Patent at 4:16-21

The Solution

In an embodiment, the security system **140** is configured to detect vulnerabilities and other cyber threats related to the execution VM **119-1**. The detection is performed while the VM **119-1** is live, without using any agent installed in the server **115** or the VM **119-1**, and without relying on cooperation from the guest OS of the VM **119-1**.

According to another embodiment, the security system **140** is configured to detect vulnerabilities and other cyber threats related to the execution VM **119-2**. i.e., the machine at rest. The detection is performed while the VM **119-2** is powered off.

Ex. 1001 (Shua) '031 Patent at 5:13-23; Ex. 1001 (Shua) '032 Patent at 5:31-43; Ex. 1001 (Shua) '685 Patent at 5:30-42;

The Solution

The snapshot is parsed and analyzed by the security system 140 to detect vulnerabilities. This analysis of the snapshot does not require any interaction and/or information from the VM 119-1. As further demonstrated herein, the analysis of the snapshot by the system 140 does not require any agent installed on the server 115 or VM 119-1.

Ex. 1001 (Shua) '031 Patent at 6:17-22; Ex. 1001 (Shua) '032 Patent at 5:14-19; Ex. 1001 (Shua) '685 Patent at 5:19-24

The Solution

At S250, the detected cyber threats and/or vulnerabilities are reported, for example, as alerts. In an embodiment, S250

Ex. 1001 (Shua) '031 Patent at 8:60-61; Ex. 1001 (Shua) '032 Patent at 7:53-54; Ex. 1001 (Shua) '685 Patent at 7:50-51

'031 Claim 1

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

- establish an interface between a client environment and security components;
- using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment;
- use the computing platform APIs to query a location of at least one of the identified virtual disks;
- receive an identification of the location of the virtual disks of the virtual machine;
- perform at least one of: (i) taking at least one snapshot, and (ii) requesting taking at least one snapshot of the virtual machine at rest, wherein the at least one snapshot represents a copy of the virtual disks of the virtual machine at a point in time;
- analyze the at least one snapshot to detect vulnerabilities, wherein during the detection of the vulnerabilities by analyzing the at least one snapshot, the virtual machine is inactive; and
- report the detected vulnerabilities as alerts.

Ex.1001 (Shua) '031 Patent, Claim 1

'032 Claim 1

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

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

accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk; analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;

determining, based on the matching, an existence of potential cyber vulnerabilities of the protected virtual cloud asset;

determining whether the matching installed applications are used by the protected virtual cloud asset;

prioritizing the potential cyber vulnerabilities based on the use determinations; and

reporting the determined potential cyber vulnerabilities, as prioritized alerts according to the use determinations.

Ex.1001 (Shua) '032 Patent, Claim 1

'685 Claim 1

1. A system for inspecting data, the system comprising: at least one processor configured to:
establish an interface between a client environment and security components;
using the interface, utilize cloud computing platform APIs to identify virtual disks of a virtual machine in the client environment;
use the computing platform APIs to query a location of at least one of the identified virtual disks;
receive an identification of the location of the virtual disks of the virtual machine;
generate at least one snapshot of the virtual disks of the virtual machine;
analyze the at least one snapshot to detect vulnerabilities and sensitive data, wherein analyzing the at least one snapshot requires no interaction with the virtual machine;
determine a risk level of the virtual machine; and
report the detected vulnerabilities and sensitive data as alerts, wherein the alerts are filtered and prioritized based on the determined risk level of the virtual machine.

Ex.1001 (Shua) '685 Patent, Claim 1

No Dispute The Patents Claim Are Practiced By Orca's SideScanning

Dr. Angelos Stavrou, Wiz's Expert

Q. For the '031 reply declaration, the same question, which is you don't offer an opinion that Orca's SideScanning does not practice any --

A. I don't --

Q. -- claim of the challenged claims?

* * *

A. It doesn't appear that in that one either, the '031 I offer an opinion either way.

Angelos Stavrou, Ph.D. Deposition (8/19/25) at 95:5-13 (objection omitted)

No Dispute The Patents Claim Are Practiced By Orca's SideScanning

Dr. Angelos Stavrou, Wiz's Expert

So Dr. Stavrou, you do not offer in your -- an opinion in your reply declaration that Orca's SideScanning does not practice the challenged claims of the '032 patent; is that right?

* * *

A. Based on a very quick look of my declaration, it doesn't appear that I opine either way.

Angelos Stavrou, Ph.D. Deposition (8/19/25) at 93:12-96:2 (objections omitted)

No Dispute The Patents Claim Are Practiced By Orca's SideScanning

Dr. Angelos Stavrou, Wiz's Expert

Q. And then for the '685 patent, the same question, you don't offer an opinion that Orca's SideScanning does not practice any challenged claim of the '685 patent, right?

* * *

A. It doesn't appear so.

Angelos Stavrou, Ph.D. Deposition (8/19/25) at 96:14-20 (objections omitted)

No Dispute The Patents Claim Agentless Workload Scanning

Dr. Angelos Stavrou, Wiz's Expert

Q. Agentless workload scanning corresponds to each of the '031, the '032 and the '685 patent claims?

A. That's correct.

Angelos Stavrou, Ph.D. Deposition (8/19/25) at 112:1-7

No Dispute The Patents Claim Using Cloud APIs

Dr. Angelos Stavrou, Wiz's Expert

Q. Okay. The -- the requirements of the claims of the '031, '032 and '685 patent used cloud APIs to view workload data, right?

A. I think that section is needed for my reply declaration for all three of them, yes.

Angelos Stavrou, Ph.D. Deposition (8/19/25) at 112:20-113:4 (objection omitted)

No Dispute The Patents Claim Read Only Access & Block-level Analysis

Dr. Angelos Stavrou, Wiz's Expert

Q. Okay. So the - the **read-only access and block-level analysis** corresponds to the requirements in the '031, '032 and '685 patent claims discussing analyzing snapshots of virtual disks?

* * *

A. I think they apply to that too, but they can apply to other - I mean, again, this is a response to Dr. Kaeli's citation of documents.

Angelos Stavrou, Ph.D. Deposition (8/19/25) at 114:20-115:9 (objection omitted)

Long-Felt Need

Long-Felt Need



“Evidence of a long felt but unresolved need tends to show non-obviousness because it is reasonable to infer that the need would have not persisted had the solution been obvious.”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1332 (Fed. Cir. 2016)

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

REDACTED

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

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

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

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)

Orca Has Received Numerous Awards for SideScanning



Forbes



Gartner
COOL
VENDOR
2022



aws

SC
Media



Shua ¶¶ 124-141, Kaeli ¶ 198, Ex. 2119 at 6-7, Ex. 2120 at 7, Ex. 2143 at 3, Ex. 2122 at 1-2, Ex. 2124 at 1, Ex. 2123 at 1-2, Ex. 2125 at 1-2, Exs. 2127-2132, Shua ¶¶ 141, 93.

Exh. 2120: Forbes Article

Subscribe To Newsletters

Forbes

Subscribe: Less than \$1.50/wk

Sign In

AI Agents Need To Be Managed As If They Are Human

The AI Graveyard: 7 Deadly Mistakes That Kill Must-Enterprise AI Projects

From Strategy To Success: How Process Drives \$2B Growth

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 Louis Columbus - Former Contributor

Nov 29, 2020, 10:08am EST

< Share Save

This article is more than 4 years old.



- 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 IT 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/louiscolombus/2020/11/29/the-top-20-cybersecurity-startups-to-watch-in-2021-based-on-crunchbase/>

Capture timestamp (UTC): Wed, 19 Mar 2025 15:16:37 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. 2021 at 7

Orca Sec
Exhibit 2
Wiz v. Orca
IPR2024
Ex. 2120

Page 1 of 11

031 POR 45; 032 POR 42; 685 POR 44

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

How Agentless Scanning Emerged

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

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

Ex. 2076 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.

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.

Ex. 2076 at 31

REDACTED

REDACTED

Exh. 2138: Wiz Blog Article

← Blog

Agents are not enough: Why cloud security needs agentless deep scanning

In this post, we're going to dive into the role and limitations of security agents in the cloud, and put forth a different approach for cloud infrastructure security: agentless deep scanning.



Josh Dreyfuss

September 28, 2021

6 minute read



Cloud environments are characterized by their dynamic nature. It's easier than ever before to spin up new resources and add new technologies, which leads to an ever-increasing number of people and teams deploying in the cloud. Ephemeral resources like serverless functions and containers mean that workloads are being added and removed at blistering speeds.

From the security perspective however, these changes have made keeping up with the cloud all the more challenging. The dynamic nature of the cloud has strained some traditional security approaches to the breaking point. The latest one is agents.

In this post, we're going to dive into the role and limitations of security agents in the cloud, and put forth a different approach for cloud infrastructure security: agentless deep scanning.

The role of agents in a cloud world

It is time to rethink the role of agents in the cloud. While they still play an important role in

Agents are not enough: Why cloud security needs agentless deep scanning

The volume snapshot approach of agentless deep scanning ensures that there's no impact to performance in an environment, as the connectors are only reading data via APIs and scanning out of band, not relying on the cloud environment's compute resources to run. This allows agentless deep scanning approaches to achieve a level of comprehensiveness in terms of coverage and features that is not possible with agent-based approaches due to the tradeoff between performance and impact to the environment.

Ex. 2138 at 4

Orca
Exhibit 2138
Wiz v. Orca
IPR2024-00863, -00864, -00865
Ex. 2138-001

Page 1 of 7

Document title: Agents are not enough: Why cloud security needs agentless deep scanning | Wiz Blog
Capture URL: <https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning>
Capture timestamp (UTC): Wed, 19 Mar 2025 12:37:05 GMT

031 POR 39-40; 032 POR 35-36; 685 POR 37-38

REDACTED

REDACTED

Security Agents Don't Belong In Your Cloud!

Published 08/18/2021

* * *

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

Exh. 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

Copying



“Copying may indeed be another form of flattering praise for inventive features,” ... and thus evidence of copying tends to show nonobviousness. ... The fact that a competitor copied technology suggests it would not have been obvious.”

WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1336 (Fed. Cir. 2016)



“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

REDACTED

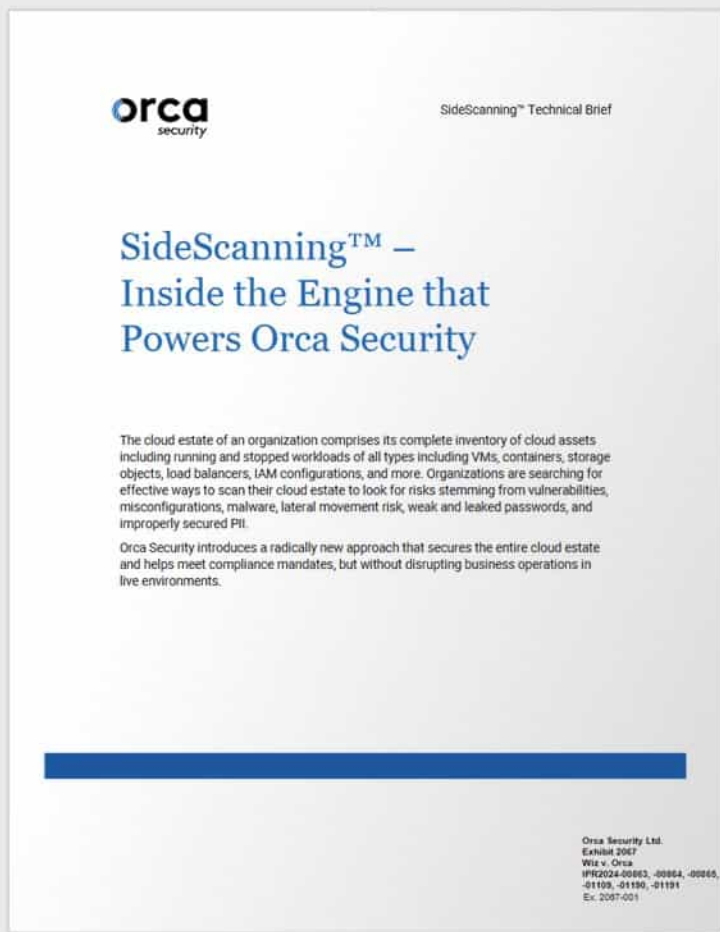
REDACTED

REDACTED

REDACTED

REDACTED

Orca's Technical Brief (Exh. 2067)



[Background](#)

[Traditional Scanning Methods](#)

[Agent-based scanning](#)

[Authenticated scanning](#)

[Unauthenticated scanning](#)

[Cloud Security Posture Manager \(CSPM\)](#)

[Introduction to SideScanning™ - A Radical New Approach](#)

[How SideScanning™ Works](#)

[Onboarding](#)

[The SideScanning Process](#)

[The Control Plane Path](#)

[The Data Plane Path](#)

[Vulnerability Scanning](#)

[Configuration Scanning](#)

[Malware Scanning](#)

[Detecting Lateral Movement Risk, Exploitable Keys, and Weak Passwords](#)

[Sensitive Information Scanning](#)

[Container Scanning](#)

[Collector Teardown](#)

[Combining Information, Analysis, and Reporting](#)

[Showing Alerts in Context](#)

[Extending the map into containerized environments](#)

[Combining Low Severity Issues into Larger Alerts](#)

[In Summary](#)

[About Orca Security](#)

Ex. 2067 at 2

031 POR 61; 032 POR 60; 685 POR 60



“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

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Commercial Success

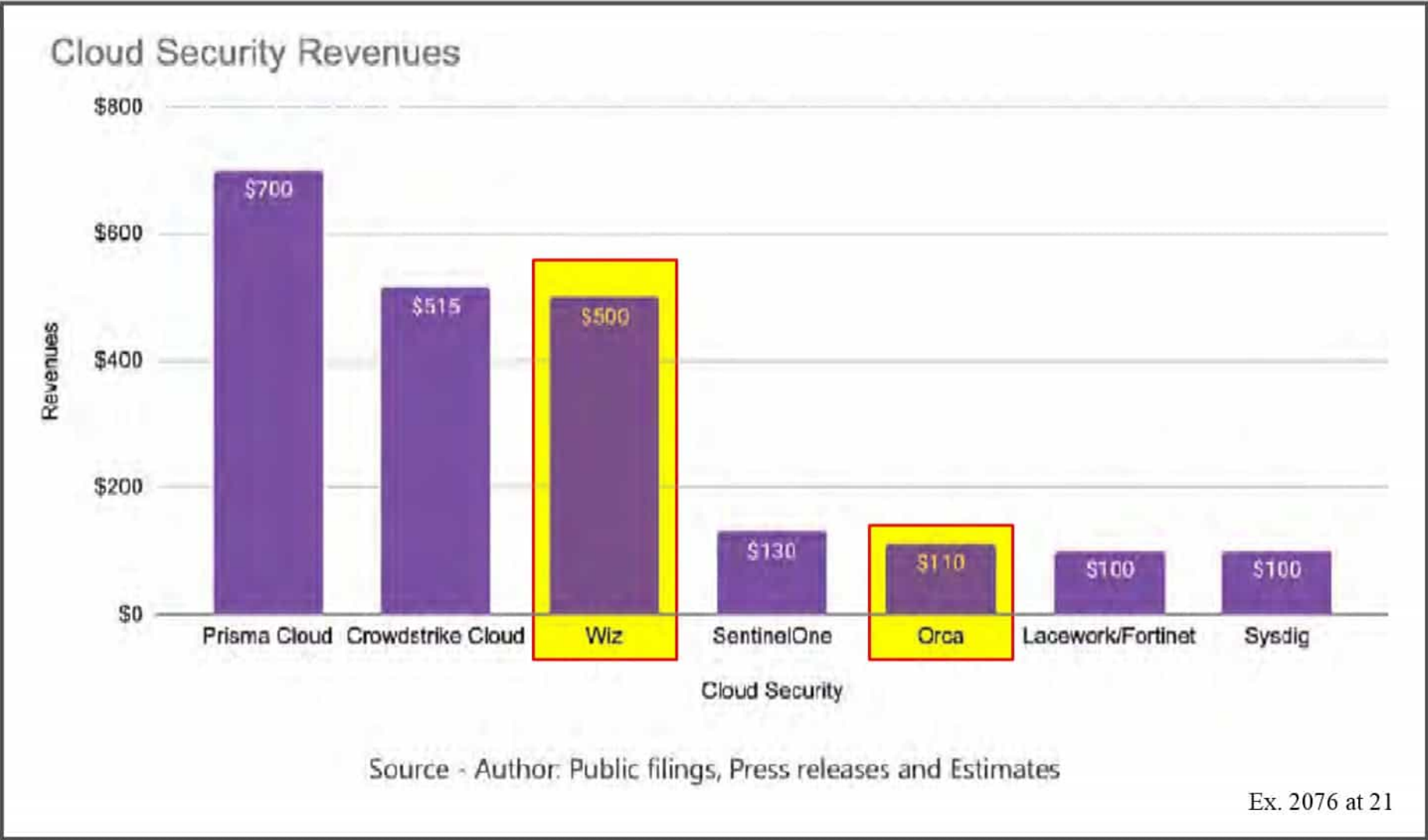
Commercial Success



“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)

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

Wiz's Motion to Exclude Evidence

None Of The Exhibits Are Hearsay



“Hearsay” means a statement that:

* * *

a part 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.’”

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

Orca Cites Statements Only For The Fact They Were Made

Accordingly, there was a long-felt, unmet need for a cloud security solution that could adequately address “constantly evolv[ing]” threats and “undetected vulnerabilities [that] can pose cyber threats,” including for “data or a machine at rest.” ’031 Patent, 2:33-36; Ex.2136, 2 (“traditional security tools are often not suited for the challenges of dynamic, virtual and distributed cloud environments.”), 14 (“traditional security solutions either don’t work at all in cloud environments or have only limited functionality.”); Ex.2137, 1 (“the journey to obtain the right level of visibility and control over the cloud workloads is still a challenge.”).

’031 POR at 39

Ex.2412, 10. As Wiz’s own documents confirm, skilled artisans were “in total awe” of Orca’s inventions. *Id.* 9 (“We were literally blown away when [Avi] showed us”; “It was mind boggling. We were in total awe.”) (alteration in original); Kaeli ¶¶193-

’031 POR at 5-6

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.

2/27/2025 Paper 19 ('031 Order re Conduct of the Proceeding) 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.

3/28/2025 Paper 29 ('031 Order Granting PO's Motion for Additional Discovery) 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. 2171 (2025.03.28 M. Argenti Email) at 1