UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
62/797,718	01/28/2019		140	ORCA P1414P		

CONFIRMATION NO. 6259

FILING RECEIPT

OC000000108010487

122066
M&B IP Analysts, LLC
500 Headquarters Plaza
Morristown, NJ 07960-7070

Date Mailed: 02/20/2019

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Avi SHAVA, Tel Aviv, ISRAEL;

Applicant(s)

Avi SHAVA, Tel Aviv, ISRAEL;

Power of Attorney:
Michael Ben-Shimon--69610

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

TECHNIQUES FOR SECURING VIRTUAL MACHINES

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

Wiz - EXHIBIT 1116
Wiz, Inc. v. Orca Security Ltd.
IPR2024-01191

06-12-25 - S.G.
Exhibit -1116
exhibitsticker.com

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Doc Code: **TR.PROV**
Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1 Remove

Given Name	Middle Name	Family Name	City	State	Country ¡
Avi		SHAVA	Tel Aviv		IL

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Title of Invention	TECHNIQUES FOR SECURING VIRTUAL MACHINES
Attorney Docket Number (if applicable)	ORCA P1414P

Correspondence Address

Direct all correspondence to (select one):

◉ The address corresponding to Customer Number	◯ Firm or Individual Name
Customer Number	122066

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

- ● No.
- Yes, the invention was made by an agency of the United States Government. The U.S. Government agency name is:
- Yes, the invention was under a contract with an agency of the United States Government. The name of the U.S. Government agency and Government contract number are:

PTO/SB/16 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Entity Status
Applicant asserts small entity status under 37 CFR 1.27 or applicant certifies micro entity status under 37 CFR 1.29

- (●) Applicant asserts small entity status under 37 CFR 1.27
- ( ) Applicant certifies micro entity status under 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
- ( ) No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Michael Ben-Shimon/			Date (YYYY-MM-DD)	2019-01-28
First Name	Michael	Last Name	Ben-Shimon	Registration Number (If appropriate)	69610

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or paten. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, t o a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

TECHNIQUES FOR SECURING VIRTUAL MACHINES

TECHNICAL FIELD

[001] This disclosure relates generally to cyber-security systems and, more specifically, to techniques for securing virtual machines.

BACKGROUND

[002] Organizations have increasingly adapted their applications to be run from multiple cloud computing platforms. Some leading public cloud service providers include Amazon®, Microsoft®, Google®, and the like.

[003] Virtualization is a key role in a cloud computing, allowing multiple applications and users to share the same cloud computing infrastructure. For example, a cloud storage service can maintain data of multiple different users.

[004] In one instance, virtualization can be achieved by means of virtual machines. A virtual machine emulates a number of "computers" or instances, all within a single physical device. In more detail, virtual machines provide the ability to emulate a separate operating system (OS), also referred to as a guest OS, and therefore a separate computer, from an existing OS (the host). This independent instance is typically isolated as a completely standalone environment.

[005] Modern virtualization technologies are also adapted by cloud computing platforms. Examples for such technologies include virtual machines, software container and serverless functions. With their computing advantages, applications and virtual machines running on top of virtualization technologies are also vulnerable to some cyber threats. For example, virtual machines can execute vulnerable software applications or infected operating systems.

[006] Protection of a cloud computing infrastructure, and particularly of virtual machines is can be achieved via inspection of traffic. Traditionally, traffic inspection is performed by a network device connected between a client and a server (deployed in a cloud computing platform or a data center) hosing virtual machines. Traffic inspection may not provide an accurate indication on the security status of the server due to inherent limitations, such as encryption and whether the necessary data is exposed in the communication. Furthermore, inspecting computing infrastructure may be performed by a network

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

[007] Traffic inspection may also be performed by a traffic monitor that listens to traffic flows between clients and the server. The traffic monitor can detect some cyber threats, e.g., based on the volume of traffic. However, the monitor can detect threats only based the monitored traffic. For example, misconfiguration of the server may not be detected by the traffic monitor. As such, traffic monitoring would not allow to detect vulnerabilities in software executed by the server.

[008] To overcome the limitations of traffic inspection solutions, some cyber-security solutions, such as vulnerability management and security assessment solutions are based on agents installed in each server in a cloud computing platform or data center. Using agents is cumbersome solution for a number of reasons, including IT resources management, governance, and performance. For example, installing agents in a large data center may take months.

[009] It would therefore be advantageous to provide a security solution that would overcome the deficiencies noted above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The foregoing and other objects, features, and advantages of the disclosed embodiments will be apparent from the following detailed description taken in conjunction with the accompanying drawings.

[0011] Figures 1 are network diagrams utilized to describe the various embodiments.

[0012] Figure 2 is a flowchart illustrating a method detecting cyber threats including potential vulnerabilities in virtual machines executed in a cloud computing platform according to some embodiments.

[0013] Figure 3 is an example block diagram of the security system according to an embodiment.

DETAILED DESCRIPTION

[0014] It is important to note that the embodiments disclosed herein are only examples of the many advantageous uses of the innovative teachings herein. In general, statements made in the specification of the present application do not necessarily limit any of the various claimed embodiments. Moreover, some statements may apply to some inventive features but not to others. In general, unless otherwise indicated, singular elements may be in plural and vice versa with no loss of generality. In the drawings, like numerals refer to like parts through several views.

[0015] Figs. 1A and 1B show an example network diagram 100 utilized to describe the various embodiments. A cloud computing platform 110 is communicably connected to a network 120. Examples of the cloud computing platform 110 may include, but are not limited to, AWS® by Amazon®, Azure® Microsoft Azure®, Google Cloud Google®, and the like. The network 120 may be the Internet, the world-wide-web (WWW), a local area network (LAN), a wide area network (WAN), and other networks.

[0016] The arrangement of the example cloud computing platform 110 is shown in Fig. 1B. As illustrated, the platform 110 includes a server 115 and a storage 117, serving as the storage space for the server 115. The server 115 is a physical device hosting at least one virtual machine (VM) 119. The storage 117 emulates virtual discs for the VMs executed in by the server 115. The storage 117 is typically connected to the server 115 through a high-speed connection, such as optic fiber allowing fast retrieval of data. In other configurations, the storage 117 may be part of the server 115. In this example illustrated in Fig. 1B, virtual disc 118-1 is allocated for the VM 119. The server 115, and hence the VM 119 may be executed in a client environment 130 within the platform 110.

[0017] The client environment 130 is an environment within the cloud computing platform 110 utilized to execute cloud-hosted applications of the client. A client may belong to a specific tenant. In some example embodiment, the client environment 130 may be part of a virtualized environment or on-premises virtualization solutions, such as VMware® based solution.

[0018] Also deployed in the cloud computing platform 110 is a security system 140 configured to perform the various disclosed embodiments. In some embodiments, the system 140 may be part of the client environment 130. In an embodiment, the security system 140 may be realized as a physical machine configured to execute a plurality of virtual instances, such as, but not limited to virtual machines. In yet another embodiment, the security system 140 may be realized as a virtual machine executed by a host server. Such a host server is a physical machine (device) and may be either the server 115, dedicated server, a different shared server, or other virtualization-based compute entity, such as serverless functions.

[0019] 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 environment 130 with the security system 140.

[0020] In the deployment, illustrated in Fig. 1, the configuration of resources of the cloud computing platform 110 is performed by means of the management console 150. As such, the management console 150 may be queried on the current deployment and settings of resources in the cloud computing platform 110. Specifically, the management console 150 may be queried, by the security system 140, about as the location (e.g., virtual address) of the virtual disc 118-1 in the storage 117. The system 140 is configured to interface with the management console 150 through, for example, an API.

[0021] In some example embodiments, the security system 140 may further interface with the cloud computing platform 110 and external systems 170. The external systems may include intelligence systems, security information and event management (SIEM) systems, and mitigations tools. The external intelligence systems may include common vulnerabilities and exposures (CVE®) databases, reputation services, security systems (providing feeds on discovered threats), and so on. The information provided by the intelligence systems may detect certain known vulnerabilities identified in, for example, a CVE database.

[0022] According to the disclosed embodiments, the security system 140 is configured to detect vulnerabilities and other cyber threats related to the execution VM 119. The detection is performed while the VM 119 is live, without using any agent installed in the

server 115 or the VM 119, and without relying on cooperation from VM 119 guest OS. Specifically, the security system 140 can scan and detect vulnerable software, non-secure configuration, exploitation attempts, compromised asserts, data leaks, data mining, and so on. The security system 140 may be further utilized to provide security services, such as incident response, anti-ransomware, and cyber insurance by accessing the security posture.

[0023] In some embodiment, the security system 140 is configured to query the cloud management console 150 as the address of the virtual disc 118-1 serving the VM 119 and a location of the snapshot. Then, a snapshot of the VM 119 as saved of the virtual disk 118-1 is accessed by the system 140. In an embodiment, the VM's 119 snapshot may be copied to the system 140. If such a snapshot does not exist, the system 140 may take a new snapshot, or request for such an action. The snapshots may be taken at a predefined schedule or upon predefine events (e.g., a network event or abnormal event). Further, the snapshots may be access or copied predefined schedule or upon predefine events. It should be noted that when the snapshot is taken or copied, the VM 119 still runs. It should be noted that the snapshot of the virtual disk 118-1 may not be necessary stored in the storage 117, but for ease of the discussion it is assumed that the snapshot is saved in the storage 117. It should be further noted that the snapshot is being accessed without cooperation of the guest, virtual OS of the virtual machine.

[0024] 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.

[0025] Various techniques can be utilized to analyze the snapshots, and depends on the type of vulnerability and cyber threats to be detected. Following are some example embodiments for techniques that may be implemented by the security system 140.

[0026] In an embodiment, the security system 140 is configured to detect whether there is vulnerable code executed by the VM 119. To this end, the security system 140 is configured to match installed application list with their respective versions to a known list of vulnerable applications. 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, the security system 140 may read installation logs of package managers used to install the packages of the application.

[0027] In yet another embodiment, the security system 140 is configured to verify whether the vulnerability is relevant to the VM 119. For example, if there is a vulnerable version or module not being in used. The priority of that issue is reduced dramatically.

[0028] To this end, security system 140 may be configured to check the configuration files of the applications and operation system of the VM 119; verify access times to files by the operating system; analyzing the active application and/or system logs in order to deduce what applications and modules are running.

[0029] In yet another embodiment, the security system 140 may instantiate a copy of the VM 119 or a subset of applications of the VM 119 on the server 115 or a separate server and monitor all activity performed by the instance of the VM. The execution of the instance of the VM is an isolated sandbox, which can be a full VM or subset of it, such as docker.

[0030] In order to determine if the vulnerability is relevant to the VM 119, the security system 140 is configured to analyze the machine memory, as reflected in the page file. The page file is saved in the snapshot and extends how much system-committed memory (also known as “virtual memory”) a system can back. In an embodiment, analyzing the page file allows to deduce running applications and modules by the VM 119.

[0031] In an embodiment, the security system 140 is configured to read process identification number (PID) files and check their access or write times, which are matched against process descriptors. The PID can be used to deduce which processes are running, and hence the priority of vulnerabilities detected in processes existing on the disk. It should be noted the PID files are also maintained in the snapshot.

[0032] 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, and suspicious PATH, LD_LIBRARY_PATH, or LD_PRELOAD definitions, services running on startup, and the like.

[0033] In an embodiment, the security system 140 may further monitoring for changes in sensitive machine areas, and alert on unexpected changes (e.g., added or changed application file without installation). In an example embodiment, this can be achieved by computing a cryptographic hash of the sensitive areas in the virtual disk and checking for differences over time.

[0034] In some embodiment, the all detected cyber threats (including vulnerabilities) are reported to a user console 180 and/or a security information and event management (SIEM) system (not shown). The reported cyber threats may be filtered or prioritized based in part on their determined risk. Further, the reported cyber threats may be filtered or prioritized based in part on the risk level of the machine. This also to reduce the number of alerts reported to the user.

[0035] 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 data is determined by searching for the PII, analyzing the application logs to determine whether the machine accessed PII/PII containing servers, or whether the logs themselves contain PII, and searching the machine memory, as reflected in the page file, for PII.

[0036] In an embodiment, the security system 140 may determine the risk of the VM 119 based on communication with an untrusted network. This can be achieved by analyzing the VM's 119 logs as saved in the virtual disk and can be derived from the snapshot.

[0037] In an example embodiment, the security system 140 may cause an execution of one or more mitigation actions. Example for such actions may include blocking traffic from untrusted networks, halting the operation of the VM, quarantining an infected VM, and the like. The mitigation actions may be performed by a mitigation tool and not the system 140.

[0038] It should be noted that the example implementation shown in Fig. 1 is described with respect to a single cloud computing platform 110 hosting a single VM 119 in a single server 115, merely for simplicity purposes and without limitation on the disclosed embodiments. Typically, virtual machines are deployed and executed in a single cloud computing platform or data center and may be protected without departing from the scope

of the disclosure. It should be further noted that the disclosed embodiments can operate using multiple security systems 140, each of which may operate in a different client environment.

[0039] Fig. 2 shows an example flowchart 200 illustrating a method for detecting cyber threats including potential vulnerabilities in virtual machines executed in a cloud computing platform according to some embodiments. The method may be performed by the security system 140.

[0040] At S210, a request, for example, to scan a VM for vulnerabilities is received. The request may be received, or otherwise triggered every predefined time interval or upon detection of an external event. The request may at least designate an identifier of the VM to be scanned.

[0041] At S220, a location of a snapshot of a virtual disk of the VM to be scanned is determined. In an embodiment, S220 may include determining the virtual disk allocated for the VM, prior to determining the location of the snapshot. As noted above, this can be achieved by querying a cloud management console.

[0042] At S230, a snapshot of the virtual disk is accessed, or otherwise copied.

[0043] At S240, the snapshot is analyzed to detect cyber threats and potential vulnerabilities. In an embodiment, S240 may include comparing the snapshot to some baseline (e.g., list of applications, pervious snapshots), analyzing logs of the VMs, instantiating a copy of the VM and executing the instance or applications executed by the VM in a sandbox, analyzing the machine memory, as reflected in the page file, or any combination of these techniques. Some example embodiments for analyzing the snapshots and the types of detected vulnerabilities and threats are provided above.

[0044] At S250, the detected threats and vulnerabilities are reported, for example, as alerts. In an embodiment, S250 may include filtering and prioritizing the reported alerts.

[0045] At optional S260, a mitigation action may be triggered to mitigate a detected threat or vulnerability. A mitigation action may be executed by a mitigation tool and triggered by the system 140. Such an action may include blocking traffic from untrusted networks, halting the operation of the VM, quarantining an infected VM, and the like.

[0046] Fig. 3 is an example block diagram of the security system 140 according to an embodiment. The security system 140 includes a processing circuitry 310 coupled to a

memory 320, a storage 330, and a network interface 340. In an embodiment, the components of the security system 140 may be communicatively connected via a bus 360.

[0047] The processing circuitry 310 may be realized as one or more hardware logic components and circuits. For example, and without limitation, illustrative types of hardware logic components that can be used include field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), application-specific standard products (ASSPs), system-on-a-chip systems (SOCs), general-purpose microprocessors, microcontrollers, digital signal processors (DSPs), and the like, or any other hardware logic components that can perform calculations or other manipulations of information.

[0048] The memory 310 may be volatile (e.g., RAM, etc.), non-volatile (e.g., ROM, flash memory, etc.), or a combination thereof. In one configuration, computer readable instructions to implement one or more embodiments disclosed herein may be stored in the storage 330.

[0049] In another embodiment, the memory 320 is configured to store software. Software shall be construed broadly to mean any type of instructions, whether referred to as software, firmware, middleware, microcode, hardware description language, or otherwise. Instructions may include code (e.g., in source code format, binary code format, executable code format, or any other suitable format of code). The instructions, when executed by the one or more processors, cause the processing circuitry 310 to perform the various processes described herein. Specifically, the instructions, when executed, cause the processing circuitry 310 to determine over-privileged roles vulnerabilities in serverless functions.

[0050] The storage 330 may be magnetic storage, optical storage, and the like, and may be realized, for example, as flash memory or other memory technology, CD-ROM, Digital Versatile Disks (DVDs), hard-drives, SSD, or any other medium which can be used to store the desired information. The storage 330 may store communication consumption patterns associated with one or more communications devices.

[0051] The network interface 340 allows the security system 140 to communicate with the external systems, such as intelligence systems, SIEM systems, mitigation systems, a cloud management console, a user console, and the like.

[0052] It should be understood that the embodiments described herein are not limited to the specific architecture illustrated in Fig. 3, and other architectures may be equally used without departing from the scope of the disclosed embodiments.

[0053] The various embodiments disclosed herein can be implemented as hardware, firmware, software, or any combination thereof. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage unit or computer readable medium consisting of parts, or of certain devices and/or a combination of devices. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units ("CPUs"), a memory, and input/output interfaces. The computer platform may also include an operating system and microinstruction code. The various processes and functions described herein may be either part of the microinstruction code or part of the application program, or any combination thereof, which may be executed by a CPU, whether or not such a computer or processor is explicitly shown. In addition, various other peripheral units may be connected to the computer platform such as an additional data storage unit and a printing unit. Furthermore, a non-transitory computer readable medium is any computer readable medium except for a transitory propagating signal.

[0054] As used herein, the phrase "at least one of" followed by a listing of items means that any of the listed items can be utilized individually, or any combination of two or more of the listed items can be utilized. For example, if a system is described as including "at least one of A, B, and C," the system can include A alone; B alone; C alone; A and B in combination; B and C in combination; A and C in combination; or A, B, and C in combination.

[0055] All examples and conditional language recited herein are intended for pedagogical purposes to aid the reader in understanding the principles of the disclosed embodiment and the concepts contributed by the inventor to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover,

all statements herein reciting principles, aspects, and embodiments of the disclosed embodiments, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

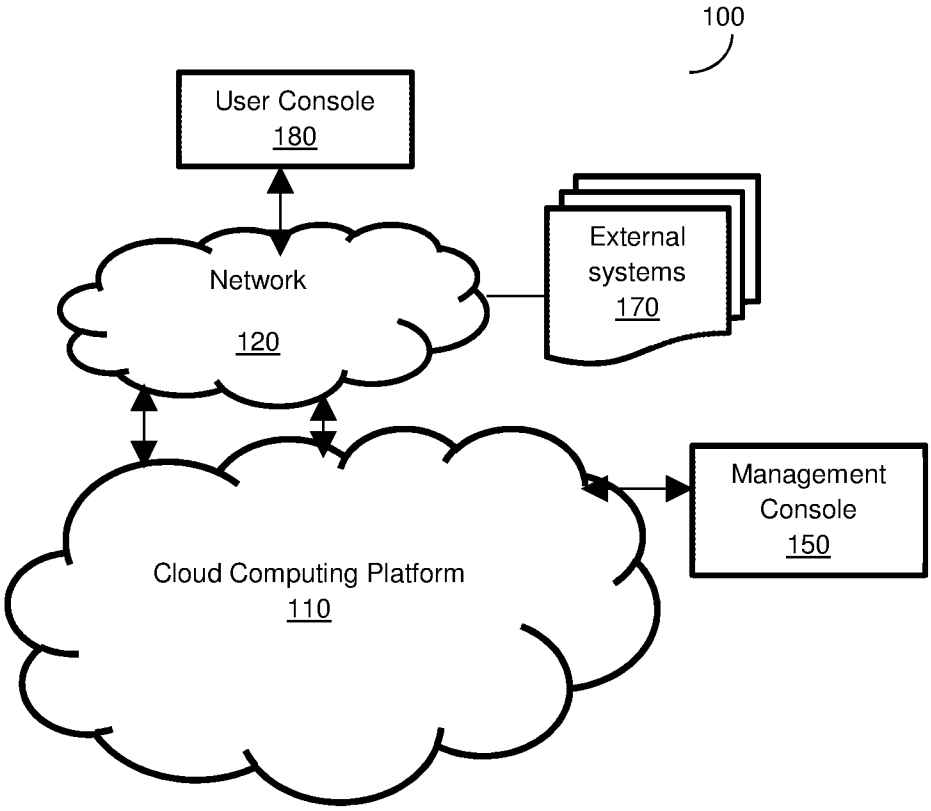
100
User Console
180
Network
120
External
systems
170
Management
Console
150
Cloud Computing Platform
110

FIG. 1A

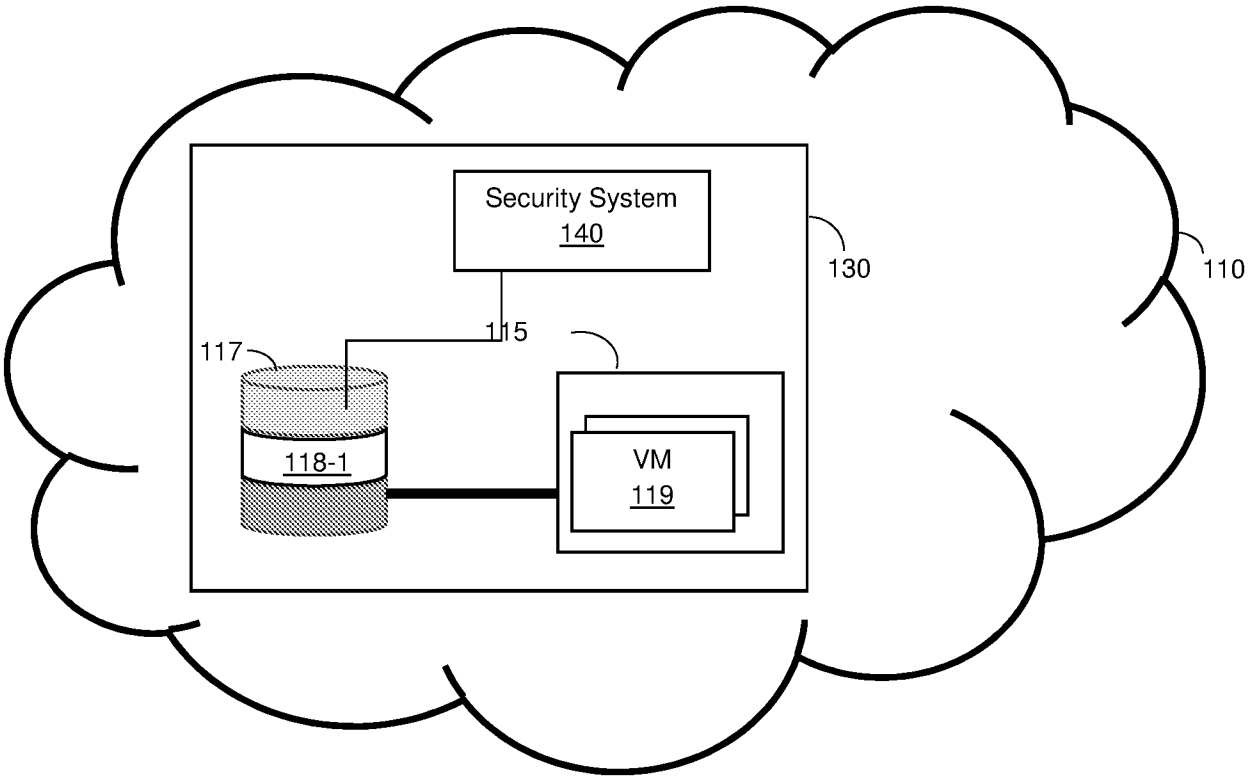

FIG. 1B

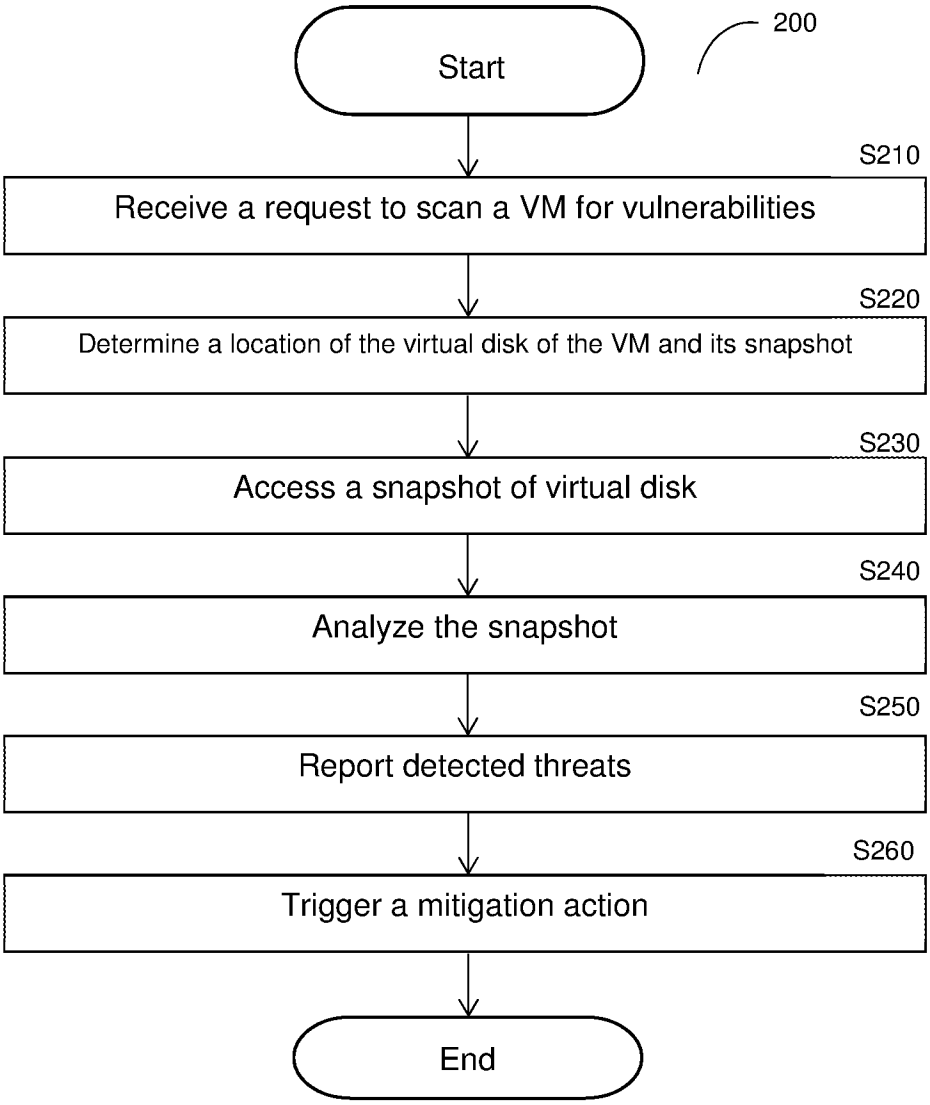
200
Start
S210
Receive a request to scan a VM for vulnerabilities
S220
Determine a location of the virtual disk of the VM and its snapshot
S230
Access a snapshot of virtual disk
S240
Analyze the snapshot
S250
Report detected threats
S260
Trigger a mitigation action
End

FIG. 2

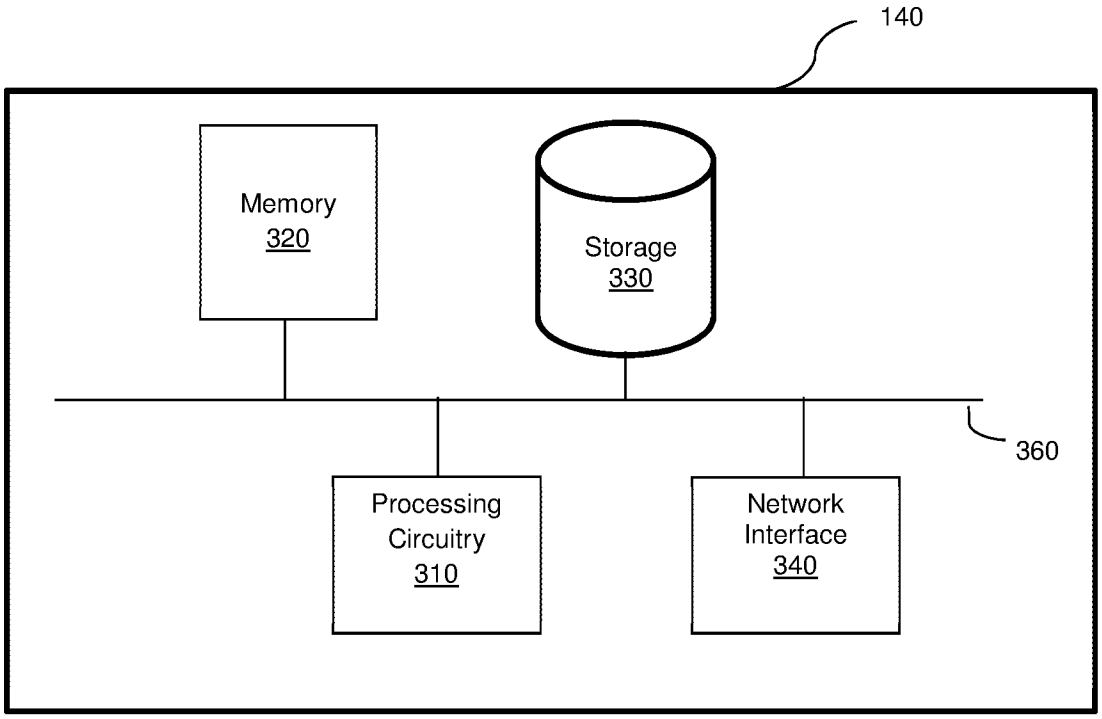
140
Memory
320
Storage
330
360
Processing
Circuitry
310
Network
Interface
340

FIG. 3