

29. The system of claim 21, wherein the data structure includes aggregated vulnerability data.

5 30. The system of claim 29, wherein the aggregated vulnerability data includes data from one or more third-party vendors.

31. The system of claim 28, wherein the aggregated vulnerability data includes data collected by a scanner.

10 32. The system of claim 28, wherein the aggregated vulnerability data includes at least one of an advisory, an exploit, a security announcement, or a known bug.

33. A method, comprising:

15 using a cloud provider API, accessing a block storage volume of a workload maintained in a cloud storage environment;
identifying an installed software application in the accessed block storage volume;
analyzing the identified installed software application to determine an associated software version;
20 accessing a data structure of known software vulnerabilities for a plurality of versions of software applications;
performing a lookup of the identified installed software version in the data structure to identify known vulnerabilities; and
perform at least one of the following:
25 query the cloud provider API to determine network accessibility information related to the workload;
identify at least one port on which the vulnerable application is accessible;
or
use network accessibility information and at least one port to identify one or more vulnerabilities susceptible to attack from outside the workload.

30 34. The method of claim 33, further comprising implementing a remedial action in response to the identified one or more vulnerabilities.

35 35. The method of claim 34, wherein the remedial measure includes transmitting an alert to a device associated with an administrator.

36. The method of claim 33, wherein querying the cloud provider API to determine the network accessibility information related to the workload further comprises:

examining data sources associated with the workload; and
determining the network accessibility information based on the examined data sources.

5 37. The method of claim 33, wherein querying the cloud provider API to determine network accessibility information related to the workload further comprises: wherein the network accessibility information includes at least one of: data from an external data source, cloud provider information, or at least one network capture log.

10 38. The method of claim 33, wherein identify the installed software application comprises:
extracting data from at least one of OS packages, libraries, or program language
libraries; and
identifying the installed software application based on the extracted data.

15 39. The method of claim 38, wherein the at least one processor is further configured to
identify a version of the installed software application.

40. A non-transitory computer-readable medium storing instructions that, when executed by
at least one processor, are configured to cause the at least one processor to perform
operations comprising:

20 using a cloud provider API, accessing a block storage volume of a workload
maintained in a cloud storage environment;
identifying an installed software application in the accessed block storage volume;
analyzing the identified installed software application to determine an associated
software version;
25 accessing a data structure of known software vulnerabilities for a plurality of versions
of software applications;
performing a lookup of the identified installed software version in the data structure
to identify known vulnerabilities;
perform at least one of the following:
30 query the cloud provider API to determine network accessibility information
related to the workload;
identify at least one port on which the vulnerable application is accessible;
and
use network accessibility information and at least one port to identify one or
35 more vulnerabilities susceptible to attack from outside the workload.

41. A cloud-based cybersecurity system for assessing internet exposure of a cloud-based
workload, the system comprising:
at least one processor configured to:

- 5 access at least one cloud provider API to determine a plurality of entities
 capable of routing traffic in a virtual cloud environment associated with a
 target account containing the workload;
 query the at least one cloud provider API to determine at least one
 networking configuration of the entities;
 build a graph connecting the plurality of entities based on the networking
 configuration;
 access a data structure identifying services publicly accessible via the
 Internet and capable of serving as an internet proxy;
10 integrate the identified services into the graph;
 traverse the graph to identify at least one source originating via the Internet
 and reaching the workload; and
 output a risk notification associated with the workload.
- 15 42. The system of claim 41, wherein the plurality of entities includes a virtual network
 appliance.
43. The system of claim 42, wherein the virtual network appliance is at least one of a load
 balancer, a firewall, a proxy, or a router.
- 20 44. The system of claim 41, wherein the networking configuration is at least one of a routing
 configuration, a proxy configuration, a load balancing configuration, a firewall configuration,
 or a VPN configuration.
- 25 45. The system of claim 41, wherein the graph includes a data structure sequentially
 connecting entities.
46. The system of claim 41, wherein the graph includes directional vectors indicating
 directions of dataflow.
- 30 47. The system of claim 41, to build the graph, the at least one processor is configured to:
 identify individual entities as nodes; and
 connect the nodes.
- 35 48. The system of claim 41, wherein the graph includes port numbers associated with the
 workload.
49. The system of claim 41, wherein the graph includes a path from the at least one source
 to the workload.

50. The system of claim 41, wherein the risk notification includes one or more resolution recommendations.

5 51. A method for assessing internet exposure of a cloud-based workload, comprising:
accessing at least one cloud provider API to determine a plurality of entities capable
of routing traffic in a virtual cloud environment associated with a target account
containing the workload;
10 querying the at least one cloud provider API to determine at least one networking
configuration of the entities;
building a graph connecting the plurality of entities based on the networking
configuration;
accessing a data structure identifying services publicly accessible via the internet
and capable of serving as an internet proxy;
15 integrating the identified services into the graph;
traversing the graph to identify at least one source originating via the internet and
reaching the workload; and
outputting a risk notification associated with the workload.

20 52. The method of claim 51, wherein the plurality of entities includes a virtual network
appliance.

25 53. The method of claim 52, wherein the virtual network appliance is at least one of a load
balancer, a firewall, a proxy, or a router.

30 54. The method of claim 51, wherein the networking configuration is at least one of a routing
configuration, a proxy configuration, a load balancing configuration, a firewall configuration,
or a VPN configuration.

55. The method of claim 51, wherein the graph includes a data structure sequentially
connecting entities.

35 56. The method of claim 51, wherein the graph includes directional vectors indicating
directions of dataflow.

57. The method of claim 51, wherein building the graph comprises:
identifying individual entities as nodes; and

connecting the nodes.

58. The method of claim 51, wherein the graph includes port numbers associated with the workload.

5

59. The method of claim 51, wherein the graph includes a path from the at least one source to the workload.

60. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations comprising:

10

accessing at least one cloud provider API to determine a plurality of entities capable of routing traffic in a virtual cloud environment associated with a target account containing a workload;

15

querying the at least one cloud provider API to determine at least one networking configuration of the entities;

building a graph connecting the plurality of entities based on the networking configuration;

20

accessing a data structure identifying services publicly accessible via the internet and capable of serving as an internet proxy;

integrating the identified services into the graph;

traversing the graph to identify at least one vector originating via the internet and reaching the workload; and

outputting a risk notification associated with the workload.

25

61. A cyber security system for a cloud environment, the system comprising:

at least one processor configured to:

utilize a cloud provider API to access a block storage volume of a workload maintained on a target account in a target system of a cloud storage environment;

30

utilize a scanner at a location of the block storage volume and on a secondary system other than the target system;

scan the block storage volume for malicious code, using the secondary system;

identify malicious code based on the scan; and

35

output from the secondary system, a notification of a presence of malicious code in the target system.

62. The system of claim 61, wherein the at least one processor is further configured to determine the location of the block storage volume based on at least one of: the target account, a secondary system account, a cloud provider account, or a third party account.

5 63. The system of claim 61, wherein, scanning the block storage volume comprises scanning disk-backed memory.

64. The system of claim 63, wherein the disk-backed memory includes at least one of a page file or a cache file.

10

65. The system of claim 61, wherein the secondary system includes at least one of a virtual machine, a container, or a serverless function.

15

66. The system of claim 61, wherein the secondary system has an operating system different from an operating system of the target account.

67. The system of claim 61, wherein the malicious code includes a rootkit.

20

68. The system of claim 61, wherein utilizing the scanner comprises suspending an operation of the scanner after the scan of the block storage volume.

69. The system of claim 61, wherein utilizing the scanner includes modifying a pre-utilized scanner at the location of the block storage volume based on information related to the target account to obtain a modified scanner, and utilizing the modified scanner.

25

70. The system of claim 61, wherein:

the at least one processor is further configured to identify a source of the malicious code; and

30

the notification includes information related to the identified source of the malicious code.

71. A method for a cloud environment, the method comprising:

utilizing a cloud provider API to access a block storage volume of a workload maintained on a target account in a target system of a cloud storage environment;

35

utilizing a scanner at a location of the block storage volume and on a secondary system other than the target system;

5 scanning the block storage volume for malicious code, using the secondary system;
identifying malicious code based on the scan; and
outputting from the secondary system, a notification of a presence of
malicious code in the target system.

10 72. The method of claim 71, wherein the location of the block storage volume includes at least one of: the target account, a secondary system account, a cloud provider account, or a third party account.

73. The method of claim 71, wherein scanning the block storage volume includes scanning disk-backed memory.

15 74. The method of claim 73, wherein the disk-backed memory includes at least one of a page file or a cache file.

75. The method of claim 71, wherein the secondary system includes at least one of a virtual machine, a container, or a serverless function.

20 76. The method of claim 71, wherein the secondary system has an operating system different from an operating system of the target account.

77. The method of claim 71, wherein the malicious code includes a rootkit.

25 78. The method of claim 71, wherein utilizing a scanner includes suspending an operation of the scanner after the scan of the block storage volume.

30 79. The method of claim 71, wherein utilizing a scanner includes:
modifying a pre-utilized scanner at the location of the block storage volume based on information related to the target account to obtain a modified scanner; and
utilizing the modified scanner.

35 80. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, cause the at least one processor to execute operations comprising:
utilizing a cloud provider API to access a block storage volume of a workload maintained on a target account in a target system of a cloud storage environment;

utilizing a scanner at a location of the block storage volume and on a secondary system other than the target system;
scanning the block storage volume for malicious code, using the secondary system;
5 identifying malicious code based on the scan; and
outputting from the secondary system, a notification of a presence of malicious code in the target system.

81. A graphical user interface system for providing forward and backward facing attack vector visualizations, the system comprising:

10 at least one processor configured to:
identify assets in a cloud environment;
identify risks associated with each of the identified asset;
identify relationships between at least some of the identified assets,
the relationships including at least one of a trust, a network
15 connectivity, or a mechanism of network proxying;
receive an identification of a specific asset under investigation;
perform a forward analysis of the specific asset under investigation to identify at least one possible attack vector reaching the specific asset via a network outside the cloud environment;
20 perform a backward analysis of the specific asset to identify at least one exposure risk to one or more assets that is in a downstream of the specific asset, wherein the at least one exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset;
25 and
output a signal to cause on a display to present a presentation of forward and backward paths associated with the specific asset, thereby enabling visualization of a plurality of entry points and lateral movement risks associated with the plurality of entry points.

30 82. The system of claim 81, wherein the network outside the cloud environment includes the Internet.

35 83. The system of claim 81, wherein the assets in the cloud environment include at least one of: a virtual machine, a network appliance, a storage appliance, a compute instance, or an engine instance.

84. The system of claim 81, wherein identifying the assets in a cloud environment includes identifying the assets based on at least one of: an identity and access management policy, an organization policy, or an access policy.

5 85. The system of claim 81, wherein the presentation of the forward and backward paths indicates alternative paths connecting between the specific asset and an upstream asset or a downstream asset.

10 86. The system of claim 85, wherein the visualization includes a presentation of the alternative paths.

87. The system of claim 81, wherein the presentation of the forward and backward paths indicates port numbers for each pathway.

15 88. The system of claim 81, wherein the visualization of the entry points indicates at least one entry point at risk.

20 89. The system of claim 81, wherein the at least one processor is further configured to monitor network activities of the assets in a cloud environment.

90. The system of claim 85, wherein the at least one processor is further configured to detect a potential risk associated with the specific asset based on the monitored network activities.

25 91. The system of claim 81, the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of the specific asset.

30 92. The system of claim 81, the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of an upstream asset of the specific asset.

35 93. The system of claim 81, the at least one processor is further configured to detect a potential risk associated with the specific asset based on a network activity of a downstream asset of the specific asset.

94. A method for generating a graphical user interface for providing forward and backward facing attack vector visualizations, the method comprising:

- identifying assets in a cloud environment;
identifying risks associated with each of the identified asset;
identifying relationships between at least some of the identified assets, the
relationships including at least one of a trust, a network connectivity, or a mechanism
5 of network proxying;
receiving an identification of a specific asset under investigation;
performing a forward analysis of the specific asset under investigation to identify at
least one possible attack vector reaching the specific asset via a network outside the
cloud environment;
10 performing a backward analysis of the specific asset to identify at least one exposure
risk to one or more assets that is in a downstream of the specific asset, wherein the
at least one exposure risk includes an identification of an exposed asset, an entry
point to the exposed asset, and a lateral movement risk associated with the exposed
asset; and
15 outputting a signal to cause on a display to present a presentation of forward and
backward paths associated with the specific asset, thereby enabling visualization of
a plurality of entry points and lateral movement risks associated with the plurality of
entry points.
- 20 95. The method of claim 94, wherein the network outside the cloud environment includes the
Internet.
96. The method of claim 94, wherein the assets in the cloud environment include at least
one of: a virtual machine, a network appliance, a storage appliance, a compute instances, or
25 an engine instance.
97. The method of claim 94, wherein identifying the assets in a cloud environment includes
identifying the assets based on at least one of: an identity and access management policy,
an organization policy, or an access policy.
30
98. The method of claim 94, wherein the presentation of the forward and backward paths
indicates alternative paths connecting between the specific asset and an upstream asset or
a downstream asset.
- 35 99. The method of claim 98, wherein the visualization includes a presentation of the
alternative paths.

100. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations comprising:

- identifying assets in a cloud environment;
- 5 identifying risks associated with each of the identified asset;
- identifying relationships between at least some of the identified assets, the relationships including at least one of a trust, a network connectivity, or a mechanism of network proxying;
- receiving an identification of a specific asset under investigation;
- 10 performing a forward analysis of the specific asset under investigation to identify at least one possible attack vector reaching the specific asset via a network outside the cloud environment;
- performing a backward analysis of the specific asset to identify at least one exposure risk to one or more assets that is in a downstream of the specific asset, wherein the
- 15 at least one exposure risk includes an identification of an exposed asset, an entry point to the exposed asset, and a lateral movement risk associated with the exposed asset; and
- outputting a signal to cause on a display to present a presentation of forward and backward paths associated with the specific asset, thereby enabling visualization of
- 20 a plurality of entry points and lateral movement risks associated with the plurality of entry points.

101. A cybersecurity system for matching keys with compute resources, the system comprising:

- at least one processor configured to:
- 25 analyze a cloud environment to identify a plurality of keys to the compute resources in the cloud environment;
- perform a cryptographic analysis on the plurality of keys to identify a first set of fingerprints that uniquely identify each of the plurality of keys, the first set of fingerprints being non-functional;
- 30 analyze trust configurations of the compute resources to identify a second set of fingerprints for each of the compute resources; and
- compare the first set of fingerprints with the second set of fingerprints to identify matching relationships between the plurality of keys and the compute resources without using any of the plurality of keys to access the
- 35 compute resources.

102. The system of claim 101, wherein the plurality of keys are stored in at least one workload.

103. The system of claim 101, wherein at least one of the first set of fingerprints is not identical to any key of the plurality of keys.

5 104. The system of claim 101, wherein at least one of the plurality of keys includes at least one of a password, a script containing a password, a private component of a private-public key pair, a cloud key or an Secure Shell (SSH) key.

10 105. The system of claim 101, wherein the at least one processor is further configured to test validity of at least one of the plurality of keys.

15 106. The system of claim 101, wherein the at least one processor is further configured to analyze a multi-machine interaction in the cloud environment using the first set of fingerprints.

107. The system of claim 106, wherein analyzing the multi-machine interaction includes comparing the first set of fingerprints with the second set of fingerprints.

20 108. The system of claim 101, wherein the at least one processor is further configured to analyze a multi-machine interaction in the cloud environment using the plurality of keys.

109. The system of claim 108, wherein analyzing the multi-machine interaction includes comparing a first key for accessing a first one of the compute resources and a second key for accessing a second one of the compute resources.

25 110. A method for matching keys with compute resources, the method comprising:
analyzing a cloud environment to identify a plurality of keys to the compute
resources in the cloud environment;
performing a cryptographic analysis on the plurality of keys to identify a first set of
30 fingerprints that uniquely identify each of the plurality of keys, the first set of
fingerprints being non-functional;
analyzing trust configurations of the compute resources to identify a second set of
fingerprints for each of the compute resources; and
comparing the first set of fingerprints with the second set of fingerprints to match
35 keys with the compute resources without using the keys to access the compute
resources.

111. The method of claim 110, wherein the plurality of keys are stored in at least one

workload.

112. The method of claim 110, wherein at least one of the first set of fingerprints is not identical to any key of the plurality of keys.

5

113. The method of claim 110, wherein at least one of the plurality of keys includes at least one of a password, a script containing a password, a private component of a private-public key pair, a cloud key, or an Secure Shell (SSH) key.

10

114. The method of claim 110, further comprising testing validity of at least one of the plurality of keys.

115. The method of claim 110, further comprising analyzing a multi-machine interaction in the cloud environment using the first set of fingerprints.

15

116. The method of claim 115, wherein analyzing the multi-machine interaction includes comparing the first set of fingerprints with the second set of fingerprints.

20

117. The method of claim 110, further comprising analyzing a multi-machine interaction in the cloud environment using the plurality of keys.

118. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations for matching keys with compute resources, the operations comprising:

25

analyzing a cloud environment to identify a plurality of keys to the compute resources in the cloud environment;

performing a cryptographic analysis on the plurality of keys to identify a first set of fingerprints that uniquely identify each of the plurality of keys, the first set of fingerprints being non-functional;

30

analyzing trust configurations of the compute resources to identify a second set of fingerprints for each of the compute resources; and

comparing the first set of fingerprints with the second set of fingerprints to match keys with the compute resources without using the keys to access the compute resources.

35

119. A cybersecurity scanner deployment system, comprising:
at least one processor configured to:

access a primary account maintained in a cloud environment;

5 receive information defining a structure of the primary account, wherein the structure includes a plurality of assets, and wherein the information excludes raw data of the primary account;
deploy, inside the primary account or inside a secondary account for which trust has been established with the primary account, at least one ephemeral scanner configured to scan at least one block storage volume and to output metadata defining the at least one block storage volume, the output excluding raw data of the primary account;
10 receive a transmission of the metadata from the at least one ephemeral scanner, wherein the transmission excludes raw data of the primary account;
analyze the received metadata to identify a plurality of cybersecurity vulnerabilities; correlate each of the identified plurality of cybersecurity vulnerabilities with one of the plurality of assets; and
15 generate a report correlating the plurality of cybersecurity vulnerabilities with the plurality of assets.

20 120. The system of claim 119, wherein defining the at least one block storage volume includes presenting risk data without sharing consumer data or data that was used to identify the risk data.

25 121. The system of claim 119, wherein the metadata defining the at least one block storage volume includes at least one of: an indication of an installed application, a version of an installed application, an operating system configuration, an application configuration, or a profile configuration.

30 122. The system of claim 119, wherein the at least one processor is further configured to receive a transmission of updated metadata defining the at least one block storage volume in response to at least one change to the at least one block storage volumes.

35 123. The system of claim 119, wherein the ephemeral scanner is configured to perform vulnerability scanning of the at least one block storage volume.

124. The system of claim 119, wherein the ephemeral scanner is configured to perform configuration scanning of the at least one block storage volume.

125. The system of claim 119, wherein the ephemeral scanner is configured to perform malware scanning of the at least one block storage volume.

126. The system of claim 119, wherein the ephemeral scanner is configured to perform lateral-movement risk analysis of the at least one block storage volume.

5 127. The system of claim 119, wherein the ephemeral scanner is configured to perform sensitive information scanning of the at least one block storage volume.

128. The system of claim 119, wherein the ephemeral scanner is configured to perform container scanning of the at least one block storage volume.

10 129. The system of claim 119, wherein the ephemeral scanner is configured to perform keys and password scanning of the at least one block storage volume.

130. A method for cybersecurity scanner deployment, comprising:

15 accessing a primary account maintained in a cloud environment;
 receiving information defining a structure of the primary account, wherein the
 structure includes a plurality of assets, and wherein the information excludes raw
 data of the primary account;
 deploying, inside the primary account or inside a secondary account for which trust
20 has been established with the primary account, at least one ephemeral scanner
 configured to scan at least one block storage volume and to output metadata
 defining the at least one block storage volume, the output excluding raw data of the
 primary account;
 receiving a transmission of the metadata from the at least one ephemeral scanner,
 wherein the transmission excludes raw data of the primary account;
25 analyzing the received metadata to identify a plurality of cybersecurity vulnerabilities;
 correlating each of the identified plurality of cybersecurity vulnerabilities with one of
 the plurality of assets; and
 generating a report correlating the plurality of cybersecurity vulnerabilities with the
 plurality of assets.

30 131. The method of claim 130, wherein defining the at least one block storage volume includes presenting risk data without sharing consumer data or data that was used to identify the risk data.

35 132. The method of claim 130, wherein the metadata defining the at least one block storage volume includes at least one of: an indication of an installed application, a version of an installed application, an operating system configuration, an application configuration, or a profile configuration.

133. The method of claim 130, further comprising receiving a transmission of updated metadata defining the at least one block storage volume in response to at least one change to the at least one block storage volumes.

5

134. The method of claim 130, wherein the ephemeral scanner is configured to perform vulnerability scanning of the at least one block storage volume.

10

135. The method of claim 130, wherein the ephemeral scanner is configured to perform configuration scanning of the at least one block storage volume.

136. The method of claim 130, wherein the ephemeral scanner is configured to perform malware scanning of the at least one block storage volume.

15

137. The method of claim 130, wherein the ephemeral scanner is configured to perform lateral-movement risk analysis of the at least one block storage volume.

20

138. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations comprising:

accessing a primary account maintained in a cloud environment;

receiving information defining a structure of the primary account, wherein the structure includes a plurality of assets, and wherein the information excludes raw data of the primary account;

25

deploying, inside the primary account or inside a secondary account for which trust has been established with the primary account, at least one ephemeral scanner configured to scan at least one block storage volume and to output metadata defining the at least one block storage volume, the output excluding raw data of the primary account;

30

receiving a transmission of the metadata from the at least one ephemeral scanner, wherein the transmission excludes raw data of the primary account;

analyzing the received metadata to identify a plurality of cybersecurity vulnerabilities;

correlating each of the identified plurality of cybersecurity vulnerabilities with one of the plurality of assets; and

35

generating a report correlating the plurality of cybersecurity vulnerabilities with the plurality of assets.

139. A graphical user interface system for providing comprehensive cloud environment risk inventory visualization, the system comprising:

at least one processor configured to:

cause a display to present a plurality of asset categories;

receive, via an input device, a selection of one or more particular
asset category;

5 cause the display to present a list of assets in the selected category
that have cyber security risks; and

for each listed asset:

retrieve workload component cybersecurity risk information,
and

10 retrieve cloud component cybersecurity risk information;
cause the display to present a common interface providing
access to the workload component cybersecurity risk
information and cloud component cybersecurity risk
information; and

15 cause the display to present, in the common interface, an
interconnection between the workload component
cybersecurity risk information and the cloud component
cybersecurity risk information.

20 140. The system of claim 139, wherein the plurality of asset categories include at least one
of an account category, an authentication category, a container category, a database
category, an image category, a container category, a managed service category, a
messaging service category, a monitoring category, a network category, a storage category,
a user category, a access category, a virtual machine category, or a serverless category.

25 141. The system of claim 139, wherein the common interface is configured to display
information relating to at least one of an asset type, a risk, a region, or an account.

30 142. The system of claim 139, wherein the common interface is configured to display
description for each listed asset.

35 143. The system of claim 139, wherein the common interface is configured to display at
least one of a vulnerability, an insecure configuration, an indication of a presence of
malware, a neglected asset, a data at risk, a lateral movement, or an authentication.

144. The system of claim 139, wherein the common interface is configured to display one or
more possible attack vectors reaching the each listed asset.

145. The system of claim 139, wherein the common interface is configured to display potential lateral movement risk from the asset to other assets in the organization, and the potential organization.

5 146. The system of claim 139, wherein the common interface is configured to display a recommended mitigation tactic for the each listed asset.

147. The system of claim 139, wherein the common interface is configured to display one or more workload metrics associated with the each listed asset.

10

148. The system of claim 139, wherein the at least one processor is further configured to provide a cybersecurity report for the each listed asset.

15

149. The system of claim 139, wherein the at least one processor is configured to identify a risk level distribution among the listed assets.

150. The system of claim 139, wherein the at least one processor is configured to:
 receive a search query for a specific risk; and
 identify one or more assets vulnerable to the specific risk.

20

151. A method for providing comprehensive cloud environment risk inventory visualization in a graphical user interface, the method comprising:

 causing a display to present a plurality of asset categories;

 receiving, via an input device, a selection of a particular asset category;

25

 causing the display to present a list of assets in the selected category that have cyber security risks; and

 for each listed asset:

 retrieving workload component cybersecurity risk information, and

 retrieving cloud component cybersecurity risk information;

30

 causing the display to present a common interface providing access to the workload component cybersecurity risk information and cloud component cybersecurity risk information; and

 causing the display to present, in the common interface, an interconnection between the workload component cybersecurity risk information and the cloud component cybersecurity risk information.

35

5 152. The method of claim 151, wherein the plurality of asset categories include at least one of an account category, an authentication category, a container category, a database category, an image category, a container category, a managed service category, a messaging service category, a monitoring category, a network category, a storage category, a user category, a access category, a virtual machine category, or a serverless category.

153. The method of claim 151, wherein the common interface is configured to display information relating to at least one of an asset type, a risk, a region, or an account.

10 154. The method of claim 151, wherein the common interface is configured to display description for each listed asset.

15 155. The method of claim 151, wherein the common interface is configured to display at least one of a vulnerability, an insecure configuration, an indication of a presence of malware, a neglected asset, a data at risk, a lateral movement, or an authentication.

156. The method of claim 151, wherein the common interface is configured to display one or more possible attack vectors reaching the each listed asset.

20 157. The method of claim 151, wherein the common interface is configured to display a recommended mitigation tactic for the each listed asset.

25 158. The method of claim 151, wherein the common interface is configured to display one or more workload metrics associated with the each listed asset.

159. A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations for matching keys with compute resources, the operations comprising:

30 causing a display to present a plurality of asset categories;
receiving, via an input device, a selection of a particular asset category;
causing the display to present a list of assets in the selected category that have cyber security risks; and
for each listed asset:
35 retrieving workload component cybersecurity risk information, and
retrieving cloud component cybersecurity risk information;
causing the display to present a common interface providing access to the workload component cybersecurity risk information and cloud component cybersecurity risk information; and

Docket Number: 15635.0004-00304

causing the display to present, in the common interface, an interconnection between the workload component cybersecurity risk information and the cloud component cybersecurity risk information.

ABSTRACT

5 Systems, methods, and computer-readable media are provided for securing cloud infrastructure, including a method comprising: establishing a trusted relationship between a source account in a cloud environment and a scanner account, using the established trust relationship, utilizing at least one cloud provider API to identify workloads in the source account, using the at least one cloud provider API to query a geographical location of at least one of the identified workloads, receiving an identification of the geographic location, using the cloud provider APIs to access block storage volumes of the at least one workload, determining a file-
10 system of the at least one workload, mounting the block storage volumes on a scanner based on the determined file-system, activating a scanner at the geographic location, reconstructing from the block storage volumes a state of the workload, and assessing the reconstructed state of the workload to extract insights.

Sheet No.

Box No. VIII (iv) DECLARATION: INVENTORSHIP (only for the purposes of the designation of the United States of America)

The declaration must conform to the following standardized wording provided for in Section 214; see Notes to Boxes Nos. VIII, VIII (i) to (v) (in general) and the specific Notes to Box No. VIII (iv). If this Box is not used, this sheet should not be included in the request.

**Declaration of inventorship (Rules 4.17(iv) and 51bis.1(a)(iv))
for the purposes of the designation of the United States of America:**

I hereby declare that I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

This declaration is directed to the international application of which it forms a part (if filing declaration with application).

This declaration is directed to international application No. PCT/..... (if furnishing declaration pursuant to Rule 26ter).

I hereby declare that the above-identified international application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Name: Avi Shua

Residence: 6630 Moore Dr, Los Angeles
(city and either US state, if applicable, or country)

Mailing Address: 6630 Moore Dr, Los Angeles,
CA, 90048

DocuSigned by:

Avi Shua3/21/2022

Inventor's Signature:
(The signature must be that of the inventor, not that of the agent)

Date:

Name:

Residence:
(city and either US state, if applicable, or country)

Mailing Address:

Inventor's Signature:
(The signature must be that of the inventor, not that of the agent)

Date:

Name:

Residence:
(city and either US state, if applicable, or country)

Mailing Address:

Inventor's Signature:
(The signature must be that of the inventor, not that of the agent)

Date:

☐ This declaration is continued on the following sheet, "Continuation of Box No. VIII (iv)".

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Avi SHUA	)	Group Art Unit: Not Yet Assigned
	)	
Application No.: Not Yet Assigned	)	Examiner: Not Yet Assigned
	)	
Filed: Herewith	)	Confirmation No.: Not Yet Assigned
	)	
For: SYSTEMS AND METHODS FOR	)	
MANAGING CYBER VULNERABILITIES	)	<u>VIA EFS-WEB</u>
(AS AMENDED)	)	
	)	
	)	
	)	
	)	
	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

PRELIMINARY AMENDMENT

Prior to the examination of the above application, please amend this application
as follows:

Amendments to the Title are included on page 2 of this paper

Amendments to the Specification begin on page 3 of this paper.

Amendments to the Claims are reflected in the listing of claims in this paper.

Remarks follow the amendment sections of this paper.

AMENDMENTS TO THE TITLE:

Please amend the title of this application as follows:

~~Systems and Methods for Side Scanning~~

Systems and Methods for Managing Cyber Vulnerabilities

AMENDMENTS TO THE SPECIFICATION:

Please amend paragraph [0001] as follows:

Cross References to Related Applications

This application is a continuation of PCT International Application No. PCT/IB2022/052670, filed March 23, 2022, which claims the benefit of U.S. Provisional Application No. 63/180,048 filed April 26, 2021, the contents of each of which are hereby incorporated by reference in their entireties.

AMENDMENTS TO CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1-20 (Cancelled)

21. (Original) A cyber security system for a cloud environment, the system comprising:

at least one processor configured to:

using a cloud provider API, access a block storage volume of a workload maintained in a cloud storage environment;

identify an installed software application in the accessed block storage volume;

analyze the identified installed software application to determine an associated software version;

access a data structure of known software vulnerabilities for a plurality of versions of software applications;

perform a lookup of the identified installed software version in the data structure to identify known vulnerabilities; and

perform at least one of:

query the cloud provider API to determine network accessibility information related to the workload;

identify at least one port on which the vulnerable application is accessible; and

use network accessibility information and at least one port to identify one or more vulnerabilities susceptible to attack from outside the workload.

22. (Original) The system of claim 21, wherein the at least one processor is further configured to implement a remedial action in response to the identified one or more vulnerabilities.

23. (Original) The system of claim 22, wherein the remedial measure includes transmitting an alert to a device associated with an administrator.

24. (Original) The system of claim 21, wherein querying the cloud provider API to determine network accessibility information related to the workload further comprises examining data sources associated with the workload; and determining the network accessibility information based on the examined data sources.

25. (Original) The system of claim 21, wherein querying the cloud provider API to determine network accessibility information related to the workload further comprises: wherein the network accessibility information includes at least one of: data from an external data source, cloud provider information, or at least one network capture log.

26. (Original) The system of claim 21, wherein to identify the installed software application, the at least one processor is configured to:
extract data from at least one of operating system packages, libraries, or program language libraries; and
identify the installed software application based on the extracted data.

27. (Original) The system of claim 21, wherein the at least one processor is further configured to identify a version of the installed software application.

28. (Original) The system of claim 21, wherein the identified installed software application includes one or more scripts.

29. (Original) The system of claim 21, wherein the data structure includes aggregated vulnerability data.

30. (Original) The system of claim 29, wherein the aggregated vulnerability data includes data from one or more third-party vendors.

31. (Original) The system of claim 28, wherein the aggregated vulnerability data includes data collected by a scanner.

32. (Original) The system of claim 28, wherein the aggregated vulnerability data includes at least one of an advisory, an exploit, a security announcement, or a known bug.

33. (Original) A method, comprising:

- using a cloud provider API, accessing a block storage volume of a workload maintained in a cloud storage environment;

- identifying an installed software application in the accessed block storage volume;

- analyzing the identified installed software application to determine an associated software version;

- accessing a data structure of known software vulnerabilities for a plurality of versions of software applications;

- performing a lookup of the identified installed software version in the data structure to identify known vulnerabilities; and

- perform at least one of the following:

 - query the cloud provider API to determine network accessibility information related to the workload;

 - identify at least one port on which the vulnerable application is accessible; or

 - use network accessibility information and at least one port to identify one or more vulnerabilities susceptible to attack from outside the workload.

34. (Original) The method of claim 33, further comprising implementing a remedial action in response to the identified one or more vulnerabilities.

35. (Original) The method of claim 34, wherein the remedial measure includes transmitting an alert to a device associated with an administrator.

36. (Original) The method of claim 33, wherein querying the cloud provider API to determine the network accessibility information related to the workload further comprises:

- examining data sources associated with the workload; and
- determining the network accessibility information based on the examined data sources.

37. (Original) The method of claim 33, wherein querying the cloud provider API to determine network accessibility information related to the workload further comprises: wherein the network accessibility information includes at least one of: data from an external data source, cloud provider information, or at least one network capture log.

38. (Original) The method of claim 33, wherein identify the installed software application comprises:

- extracting data from at least one of OS packages, libraries, or program language libraries; and
- identifying the installed software application based on the extracted data.

39. (Original) The method of claim 38, wherein the at least one processor is further configured to identify a version of the installed software application.

40. (Original) A non-transitory computer-readable medium storing instructions that, when executed by at least one processor, are configured to cause the at least one processor to perform operations comprising:

using a cloud provider API, accessing a block storage volume of a workload maintained in a cloud storage environment;

identifying an installed software application in the accessed block storage volume;

analyzing the identified installed software application to determine an associated software version;

accessing a data structure of known software vulnerabilities for a plurality of versions of software applications;

performing a lookup of the identified installed software version in the data structure to identify known vulnerabilities;

perform at least one of the following:

- query the cloud provider API to determine network accessibility information related to the workload;

- identify at least one port on which the vulnerable application is accessible; and

- use network accessibility information and at least one port to identify one or more vulnerabilities susceptible to attack from outside the workload.

41-159 (Cancelled)

REMARKS

Applicant amends the application to insert a reference to the parent applications, for which benefit is claimed, of this new continuing application, and to incorporate by reference the parent applications. Further, Applicant cancels claims 1-20 and 41-159 without prejudice or disclaimer of their subject matter. Claims 21-40 remain pending. No new matter has been introduced.

Applicant respectfully requests the timely examination and allowance of pending claims 21-40.

Please grant any extensions of time required to enter this paper and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: 5 April 2022

By: /Christopher C. Johns/
Christopher C. Johns
Reg. No. 68,664
(202) 408-4000