US Patent & Trademark Office
Patent Public Search | Text View

Vulnerability remediation based on priority of policies

Abstract

A system for policy based vulnerability management of a network equipment of an enterprise is disclosed. A plurality of vulnerabilities associated with an end user device and a plurality of policies associated with the plurality of vulnerabilities is identified. Factors including a type of vulnerability, risks associated with the vulnerabilities and a time of action for a remediation of the vulnerabilities are identified. Based on the factors, each vulnerability is assigned a priority. Remediation for the plurality of vulnerabilities is determined based on the plurality of policies and the priority. A route based on a high compliance rate with the plurality of policies is selected. The cloud service is provided to the end user device via the route. Remediation of the plurality of vulnerabilities is executed based on the policies in accordance with the priority and the route with the high compliance rate.

Related U.S. Application Data

Publication Classification

Background/Summary

PRIORITY [0001] This application is a continuation of U.S. application Ser. No. 17/555,125, entitled "POLICY DRIVEN VULNERABILITY IDENTIFICATION AND REMEDIATION", filed on Dec. 17, 2021, which is a continuation of U.S. application Ser. No. 17/339,525, entitled "VULNERABILITY REMEDIATION BASED ON TENANT SPECIFIC POLICY," filed on Jun. 4, 2021, now issued as U.S. Pat. No. 11,233,815, which is a continuation of U.S. application Ser. No. 17/315,010 entitled "POLICY BASED VULNERABILITY IDENTIFICATION, CORRELATION, REMEDIATION, AND MITIGATION," filed on May 7, 2021, now issued as U.S. Pat. No. 11,997,127. The contents of the aforementioned applications are incorporated by reference in their entirety for all purposes.

BACKGROUND
[0002] This disclosure relates in general to vulnerability management in cloud-based multi-tenant systems and, but not by way of limitation, to policy-based vulnerability management and remediation.
[0003] Vulnerabilities in multi-tenant systems is often a complicated and convoluted area to manage across multiple vendor platforms and distinct software. Identification and tracking of vulnerabilities are difficult, especially when there are new Common Vulnerabilities and Exposures (CVEs) that are released daily. Remediation of a vulnerability involves patching or upgrading software, which is often intrusive and difficult to achieve, as there are large number of devices involved in an enterprise.
[0004] Remediating vulnerabilities in a timely manner becomes strenuous, especially in a multi-tenant system having a distributed work force, or employees working at home. When the employees connect to services and sites from outside a Local Area Network (LAN) of the enterprise, the risks associated with the security of the devices tend to increase.
[0005] Many enterprises have a bring your own device (BYOD) policy that allows different platforms, operating systems, and application versions to run with the workplace systems. Identifying threats in these circumstances is hard because of the number of unique systems and software.
SUMMARY
[0006] A system for policy based vulnerability management of a network equipment of an enterprise is disclosed. A plurality of vulnerabilities associated with an end user device and a plurality of policies associated with the plurality of vulnerabilities is identified. Security risks associated with the plurality of vulnerabilities based on a type of the plurality of vulnerabilities are identified. Remediation for the plurality of vulnerabilities is determined based on the plurality of policies and prioritized based on the vulnerabilities, the security risks, and the policies. The

plurality of policies is based on a cloud service selected from the end user device, a tenant, and a role associated with the end user device. A route corresponding to the plurality of policies and the cloud service is identified. The route specifies the end user device or a mid-link server. The cloud service is provided to the end user device via the route.

[0007] In an embodiment, a cloud-based multi-tenant system for policy based vulnerability management of a network equipment of an enterprise. The cloud-based multi-tenant system includes an application running on an end user device of a plurality of end user devices. The application selects a cloud service from a plurality of cloud services. A plurality of routes through the cloud-based multi-tenant system to deliver the plurality of cloud services to the plurality of end user devices. The plurality of routes is specified for a plurality of policies. A mid-link server of the cloud-based multi-tenant system is configured to identify a plurality of vulnerabilities associated with the end user device. Security risks associated with the plurality of vulnerabilities based on a type of the plurality of vulnerabilities The plurality of policies associated with the plurality of vulnerabilities is identified based on the type of the plurality of vulnerabilities and the end user device. The plurality of policies is specified for the plurality of end user devices. Remediation for the plurality of vulnerabilities is determined based on the plurality of policies. The plurality of policies is set based on the cloud service, a tenant, and/or a user role associated with the end user device. The remediation is executed at the end user device or the mid-link server based on a tenant specific policy from the plurality of policies. A route from the plurality of routes is identified corresponding to the plurality of policies and the cloud service. The route specifies the end user device or the mid-link server. The remediation of the plurality of firmware is prioritized based on the type of the plurality of vulnerabilities, the security risks, and the plurality of policies. The remediation of the plurality of firmware is executed by upgrading the plurality of firmware based on the plurality of policies according to the prioritization. Communication is established via the route between the application and the cloud service is based on the plurality of policies.

[0008] In another embodiment, a vulnerability identification and remediation method of identifying and remediating vulnerabilities for a network equipment in a cloud-based multi-tenant system of an enterprise is shown. In one step, a selection of a cloud service from a plurality of cloud services is received from an application running on an end user device of a plurality of end user devices. A plurality of vulnerabilities associated with a plurality of firmware of the end user device is identified by a mid-link server. A plurality of policies associated with the plurality of vulnerabilities is identified by the mid-link server based on the type of the plurality of vulnerabilities and the end user device. The plurality of policies is specified for the plurality of end user devices. Remediation for the plurality of vulnerabilities is determined by the mid-link server based on the plurality of policies. The plurality of policies is based on the cloud service, a tenant, and/or a user role associated with the end user device. A route from a plurality of routes is identified by the mid-link server corresponding to the plurality of policies and the cloud service. The route specifies the end user device or the mid-link server. The plurality of routes is specified for the plurality of policies. The plurality of routes through the cloud-based multi-tenant system delivers the plurality of cloud services to the plurality of end user devices. The remediation of the plurality of firmware is prioritized based on the type of the plurality of vulnerabilities, the security risks, and the plurality of policies. The remediation of the plurality of firmware is executed by upgrading the plurality of firmware based on the plurality of policies according to the priority. Communication is established via the route by the mid-link server between the application and the cloud service based on the plurality of policies.

[0009] In one embodiment, a cloud-based multi-tenant system for policy-based vulnerability management, the cloud-based multi-tenant system comprising one or more processors and one or more memories with code for: [0010] extracting: configuration items associated with a plurality of firmware of a plurality of end user devices from a configuration database using Application Programming Interfaces (APIs), device configurations including vendor specific information from

a device configuration repository, and external vulnerability information including external websites, social media, and/or vendor websites from a plurality of data sources; [0011] correlating the configuration items, the device configurations, and the external vulnerability information; and [0012] identifying a plurality of vulnerabilities associated with the plurality of firmware based on the correlation; [0013] receiving from an application running on an end user device of the plurality of end user devices, a selection of a cloud service from a plurality of cloud services; [0014] identifying security risks associated with the plurality of vulnerabilities based on a type of the plurality of vulnerabilities; [0015] identifying a plurality of policies associated with the plurality of vulnerabilities based on the type of the plurality of vulnerabilities and the end user device, wherein the plurality of policies is specified for the plurality of end user devices; [0016] determining remediation for the plurality of vulnerabilities based on the plurality of policies, wherein the plurality of policies is based on the cloud service, a tenant, and/or a user role associated with the end user device; [0017] identifying a route from a plurality of routes corresponding to the plurality of policies and the cloud service, wherein: the route specifies the end user device or a mid-link server of the cloud-based multi-tenant system; the plurality of routes is specified for the plurality of policies; and the plurality of routes through the cloud-based multi-tenant system delivers the plurality of cloud services to the plurality of end user devices; [0018] executing the remediation of the plurality of firmware by upgrading the plurality of firmware based on the plurality of policies; and [0019] communicating via the route between the application and the cloud service based on the plurality of policies.

[0020] Further areas of applicability of the present disclosure will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating various embodiments, are intended for purposes of illustration only and are not intended to necessarily limit the scope of the disclosure.

Description

BRIEF DESCRIPTION OF THE DRAWINGS
[0021] The present disclosure is described in conjunction with the appended figures:
[0022] FIG. **1** illustrates a block diagram of an embodiment of a cloud network allowing multiple-tenants in different domains to communicate with various cloud providers over the public internet;
[0023] FIG. **2** illustrates a block diagram of an embodiment of a single-tenant cloud network where an end user device communicates with a cloud provider;
[0024] FIG. **3** illustrates a block diagram of an embodiment of an end user device that includes a client for enabling enhanced routing control;
[0025] FIG. **4** illustrates a block diagram of an embodiment of a client that can specify by policy routes to be used for cloud services under management of a client controller;
[0026] FIG. **5** illustrates an overview of a block diagram of an embodiment of a mid-link server;
[0027] FIG. **6** illustrates a detailed block diagram of an embodiment of a mid-link server;
[0028] FIG. **7** illustrates a block diagram of an embodiment of a vulnerability identifier;
[0029] FIG. **8** illustrates a block diagram of a priority assigner;
[0030] FIG. **9** illustrates a flowchart of an embodiment of a process for policy-driven vulnerability management of network devices in cloud-based multi-tenant systems;
[0031] FIG. **10** illustrates a flowchart of an embodiment of a process for policy-driven vulnerability management of network devices and execution of the remediations in cloud-based multi-tenant systems; and
[0032] FIG. **11** illustrates a flowchart of an embodiment of a process for policy-driven remediation of vulnerabilities in cloud-based multi-tenant systems.
[0033] In the appended figures, similar components and/or features may have the same reference

label. Further, various components of the same type may be distinguished by following the reference label by a dash and a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

DETAILED DESCRIPTION

[0034] The ensuing description provides preferred exemplary embodiment(s) only, and is not intended to limit the scope, applicability or configuration of the disclosure. Rather, the ensuing description of the preferred exemplary embodiment(s) will provide those skilled in the art with an enabling description for implementing a preferred exemplary embodiment. It is understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope as set forth in the appended claims.

[0035] Referring first to FIG. **1**, a block diagram of an embodiment of a cloud network **100** allowing multiple-tenants in different domains to communicate with various cloud providers over the public internet is shown. The cloud network **100** allows multiple tenants or enterprises to use the same network separated by domain or some other logical separation. Encryption, leased/encrypted tunnels, firewalls, and/or gateways can be used to keep the data from one enterprise **198** separate from other enterprises **198**. Each end user device **195** can communicate with cloud providers **140** of services and storage using a public internet **125**. A mid-link server **185** provides multi-tenancy control, policies and routing for each domain.

[0036] The cloud network **100** may include a first computing environment **150-1** having end user devices **195-1** for a first domain, a second computing environment **150-2** having end user devices **195-2** for a second domain, and a third computing environment **150-3** having end user devices **195-3** for a third domain. Each domain communicates with its respective enterprise **198** using a virtual private network (VPN) **190** over local area networks (LANs), wide area networks (WANs), and/or the public Internet **125**. Instead of a VPN **190** as an end-to-end path, tunneling (e.g., IP-in-IP, GRE), policy-based routing (PBR), BGP/IGP route injection, or proxies could be used. The first cloud provider **140-1**, the second cloud provider **140-2**, and the third cloud provider **140-3** may be public or private clouds. Some examples of the cloud providers **140** include Amazon Web Services (AWS)®, Google Cloud Platform (GCP)®, and Microsoft Azure®. Some or all of the cloud providers **140** may be different from each other, for example, the first cloud provider **140-1** may run Amazon Web Services (AWS)®, the second cloud provider **140-2** may run Google Cloud Platform (GCP)®, and the third cloud provider **140-3** may run Microsoft Azure®. Although three cloud providers **140** are shown, any suitable number of cloud providers **140** may be provided with some captive to a particular enterprise or otherwise not accessible to multiple domains.

[0037] Each of the cloud providers **140** may communicate with the public Internet **125** using a secure connection. For example, the first cloud provider **140-1** may communicate with the public Internet **125** via a virtual private network (VPN) **190**, the second cloud provider **140-2** may communicate with the public Internet **125** via a different VPN **190**, and the third cloud provider **140-3** may communicate with the public Internet **125** via yet another VPN **190**. Some embodiments could use leased connections or physically separated connections to segregate traffic. Although one VPN **190** is shown, it is to be understood that there are many VPNs to support different end user devices, tenants, domains, etc.

[0038] A plurality of enterprises **198** may also communicate with the public Internet **125** and the end user devices **195** for their domain via VPNs **190**. Some examples of the enterprises **198** may include corporations, educational facilities, governmental entities, and private consumers. Each enterprise may support one or more domains to logically separate their networks. The end user devices **195** for each domain may include individual computers, tablets, servers, handhelds, and network infrastructure that are authorized to use computing resources of their respective enterprise **198**.

[0039] Further, the mid-link server **185** may communicate with the public Internet **125** via a VPN **190**. The mid-link server **185** also provides cloud access security broker (CASB) functionality for cloud security to enterprises **198** with data flows of the CASB being regulated with a global cloud traffic controller (GCTC). Communication between the mid-link server **185** and cloud providers **140** for a given enterprise **198** can be either a VPN connection or tunnel depending on preference of the enterprise **198**. The mid-link server **185** may configure, test, and enforce policies and routing across the cloud network **100**. For example, the mid-link server **185** may ensure that the policies are consistent across the cloud providers **140**, enterprises **198** and computing environments **150**. The mid-link server **185** provides proxies to cloud providers and may apply various policies. The connection between end user devices **195** and the mid-link server **185** is over an encrypted VPN or tunnel.

[0040] With reference to FIG. **2**, a block diagram of an embodiment of a single-tenant cloud network **200** where an end user device **195** communicates with a cloud provider **140** is shown. The end user device **195** is operated by an end user **204**. The cloud provider **140** is accessible directly or through the mid-link server **185** depending on the route chose, services, policies, etc. Included in the cloud provider **140** are services **216** such as storage **212** that enable applications and functionality on the end user devices **195**.

[0041] Service endpoints **214** are provided in the cloud provider **140** to enable communication with the mid-link server **185** and end user devices **195**. Service endpoints **214** may include VPN terminations and proxies that provide for a secure tunnel with the mid-link server **185** and/or end user devices **195**. The mid-link server **185** can optionally connect directly with services **216** and storage **212** of the cloud provider **140** without using the service endpoints **214**. In some cases, the end user device **195** communicates with the services **216** and storage **212** through the mid-link server **185** depending on route preference and policies.

[0042] Referring next to FIG. **3**, a block diagram of an embodiment of an end user device **195** that includes a client **304** for enabling enhanced routing control is shown. The end user device **195** includes applications **302** and a browser **308** that use the client **304** for communication over the LAN **306** and ultimately to cloud providers **140** (not shown). The browser **308** and the apps **302** can be redirected using domain name services (DNS) to use the client **304**. Alternatively, the browser **308** and the apps **302** may natively support the client **304** to utilize Application Programming Interfaces (APIs) or other communication to select policies and receive the corresponding routes.

[0043] Referring next to FIG. **4**, a block diagram of an embodiment of a client **304** is shown that can specify by policy routes to be used for cloud services under the management of a client controller **404**. The client controller **404** configures a DNS, fulfills API request, populates routes **410**, identifies threats in a threat identifier **416**, and a policy cache **412**. In operation, the client controller **404** configures data and service requests over the cloud network **100**.

[0044] The client **304** can be specified for use with a DNS **408** who redirects traffic from browsers **308** and the apps **302** to go through the client **304**. Without changing any apps **302** or the browser **308**, the client **304** can process traffic for the cloud network **100**. The client **304** can operate as a proxy using a service proxy **402** or a VPN using the client endpoint **406**. An API **414** is provided for the apps **302** to configure the client **304** if they have that capability. The mid-link server **185** may also configure the client **304**.

[0045] The mid-link server **185** sends relevant policies to the policy cache **412** to provide functionality to the client **304**. The policies allow specifying vulnerabilities, type of remediation and route for the client **304** to use. Table I gives examples of policies along with the target compliance rate before the remediation. For example, policy 1 specifies different routes such as **185-1**, **140-2** with 100% compliance, route **185-1**, **140-1**, **140-2** with 99% compliance, route **185-1**, **140-1**, **140-2**, with 90% compliance, and route **185-4**, **140-3** with 70% compliance.

TABLE-US-00001 TABLE I Policies Policy Route Compliance Policy 1 185-1, 140-2 100% 185-1,

140-1, 140-2   99% 185-1, 140-2, 140-2   90% 185-4, 140-3   70% Policy 2 185-4, 140-6, 195 60% Policy 3 185-6, 140-5 100% 185-7, 140-2   99% 185-1, 140-3-140-1   95%

Routes **410** are sent for the domain and enterprise **198** by the mid-link server **185**.

[0046] Where non-compliance with a policy is determined, routes **410**, policies and configuration from the mid-link server **185** remediates the problem. The threat identifier **416** receives identified threats, priority and suggested remediation from the mid-link server **185** and displays it to the end user **204** for review. The end user **204** may initiate remediation that is performed by the mid-link server **185**.

[0047] Referring next to FIG. **5**, an overview of a block diagram of an embodiment of a mid-link server **185** is shown. A security analyst and a network operator have access to analysis performed at the mid-link server **185**. Systems of the security analyst and the network operator are interconnected to the mid-link server **185** via the internet. In another embodiment, the security analyst and the network operator may be interconnected through a Local Area Network (LAN) of an enterprise. The security analyst and the network operators may perform remedial actions on the vulnerabilities based on the policies and the determination performed at a remedial and mitigation system of the mid-link server **185**.

[0048] The remedial and mitigation system of the mid-link server **185** determines remedies to the vulnerabilities based on the policies. The policies include different types of vulnerabilities, and an extent of risk posed by the vulnerabilities. The remedies identified are used to mitigate risks associated with the end user devices **195**. An API is used to receive the vulnerabilities from a vulnerability identification system.

[0049] The vulnerability identification system identifies the vulnerabilities in firmware, operating system, software, and/or other programs of the end user devices **195** using machine learning (ML) models. The vulnerability identification system correlates configuration items (CI) data including hostnames, IP addresses, models, make, roles, or software versions of the end user devices **195**, device configurations including vendor specific information, common vulnerabilities and exposure (CVE) data and external data such as using web or social media data. The correlation is used to determine the vulnerabilities of the end user devices **195**. The CI data, the device configurations, the CVE data and the external data are stored in respective repositories. The repository storing the CI data is a configuration item (CI) repository, the device configurations are stored in a device configuration repository, and the external data is stored in an external repository. The API is used for communications between the repositories and the other components of the vulnerability identification system. The vulnerability identification system includes memory that is a random access memory (RAM) and/or any other kind of

[0050] storage, a processor that is a central processing unit (CPU) and a graphical processing unit (GPU).

[0051] Referring next to FIG. **6**, a detailed block diagram of an embodiment of a mid-link server **185** is shown. The mid-link server **185** is configured to determine vulnerabilities in programs associated with the end user devices **195**, and remediate the vulnerabilities based on policies and facilitate communication through routes. The programs may be software applications, firmware, applets or other software codes. The mid-link server **185** includes a configuration repository **602**, a device repository **604**, an external data repository **606**, a correlator **608**, a policy store **610**, a vulnerability identifier **612**, a priority assigner **614**, a remediator **616**, an Information Technology (IT) module **618**, and routes **620**.

[0052] The configuration repository **602** stores configuration items including hostnames, Internet Protocol (IP) addresses, models, make, roles, or software versions of the end user devices **195**. The configuration repository **602** is a database that stores the configuration items. The configuration items are acquired through web crawlers or other data extraction methods. The configuration items are acquired from various sources such as an Information Technology Asset Management (ITAM) and a Configuration Management Data Base (CMDB). These sources track data from IT

infrastructure of enterprises among other sources.

[0053] The device repository **604** stores device configurations including vendor specific information. A variety of tools exist that can extract network device configurations, store them for reference, restoral, and historical purposes. Different vendors use different ways to format and implement the configurations, which provides a need for a common configuration or data model that may be parsed, analyzed and/or stored. The device configurations provide useful insights on vulnerabilities associated with the end user devices **195**.

[0054] The external data repository **606** stores common vulnerability and exposures (CVE) information from external websites, social media, vendor websites, and/or National Vulnerability Database (NVD). Vendor websites typically have publicly accessible documentation for security advisories. Some vendors are including "solutions" and "work-around" sections within the CVE. Vendor web pages on vulnerabilities have crucial information. Machine learning capabilities provide an intelligent way to filter out the unnecessary information and extract the relevant information.

[0055] The correlator **608** retrieves the configuration items from the configuration repository **602**, the device configurations from the device repository **604**, and the CVE information from the external data repository **606** using Application Programming Interfaces (APIs). A correlation is performed by the correlator **608** using machine learning techniques. The configuration items, the device configurations and the CVE information are correlated, and a correlation result so obtained is provided to the vulnerability identifier **612** for further processing.

[0056] The vulnerability identifier **612** receives the correlation result to determine

[0057] vulnerabilities associated with the end user devices **195**. The vulnerability identifier **612** includes machine learning models that identify the vulnerabilities. The policy store **610** includes the policies as retrieved from the policy cache **412**. The policy store **610** includes policies for the end user devices **195**. The policies are determined based on a type of vulnerability. The policies specify remediation and a route for remediation. The policies may specify whether the remediation is to be performed at the end user device **195**, at the mid-link server **185** or by an administrator (via the IT module **618**). The routes corresponding to the policies are determined from the routes **620**. The routes are stored and dynamically updated in the routes **620**. The routes **620** include paths through the cloud providers **140**, the mid-link server **185** and the end user devices **195** to remediate the vulnerabilities. For example, a policy may specify that remediation of a vulnerability related to software updates of an end user device **195** working remotely may be performed at a user device by its user. The route in this case will be through the user device. Another policy for threats in program code attacked by a virus may be performed at the mid-link server **185** or by an administrator. The route in this case will be though the mid-link server **185** or the enterprise software. The vulnerabilities identified by the vulnerability identifier **612** are provided to the priority assigner **614** for further processing.

[0058] The priority assigner **614** includes machine learning models to assign priority to the vulnerabilities. The priority assigner **614** identifies a number of factors including the type of vulnerability, risks associated with the vulnerabilities and a time of action for the remediation based on the type of vulnerability and a level of the risks. For example, the priority assigner **614** may also use Common Vulnerability Scoring System (CVSS) or any other threat management system to capture main characteristics of the vulnerability and generate a numerical score reflecting its severity. The numerical score is translated into a qualitative representation such as low, medium, high, and critical to prioritize their remediation and/or vulnerability management processes. Based on the identified factors, each vulnerability is assigned a priority rank. By way of an example, among a set of vulnerabilities, a vulnerability related to a software update of a router may be assigned a lower priority rank as compared to another vulnerability associated with a software on public internet. By way of another example, firmware lacking firewall is assigned a higher priority for the remediation, and firmware that is within a private network or the firmware that do not have

public Internet Protocol (IP) addresses are assigned a lower priority of the remediation. The vulnerabilities along with the assigned priorities are provided to the remediator **616** for analysis.

[0059] The remediator **616** identifies remediations based on the type of vulnerabilities, the policies, and the level of the risks associated with the vulnerabilities. The remediator **616** initiates remediation of the vulnerabilities in accordance with the assigned priorities. The vulnerabilities with higher priority ranks are remediated first at the end user device **195**, the mid-link server **185** or by the enterprise administrator. For example, misconfigured firewalls call for firewall configuration reviewed by the administrator through the mid-link server **185**. The remediations are approved at the IT Module **618** before implementation in order to avoid any work-related disruption at the end user device **195**.

[0060] The IT module **618** provides approvals of the administrators or network operators of the enterprise to the remediator **616** to perform the remediations based on the approvals. The remediations should be performed in a non-intrusive manner. The user of the end user device **195** may be working on an urgent task and/or may need to save the work done before the upgradations or updates start at the end user device **195**. In order to perform the updates in non-intrusively it is important to take approvals from the IT module **618**. The IT module **618** may also review the priority ranks assigned by the priority assigner **614** and may modify the priority ranks. In this case, the remediations are performed according to the modified priority ranks.

[0061] Referring next to FIG. **7**, a block diagram of an embodiment of a vulnerability identifier **612** is shown. The vulnerability identifier **612** receives correlated results from the correlator **608** to identify vulnerabilities associated with the end user devices **195**. The vulnerabilities may be in application software, system software or other programs of the end user devices **195**. The vulnerability identifier **612** includes a policy database **702**, a machine learning repository **704**, a processor **706** and a router **708**.

[0062] The policy database **702** retrieves the correlated results from the correlator **608** and the policies from the policy store **610**. The policy database **702** stores the retrieved vulnerabilities and the associated policies. The correlated results are obtained by correlation of configuration items including hostnames, IP addresses, models, make, roles, or software versions, device configurations including vendor specific information related to vulnerabilities and threats, and external data from websites, social media and other public databases.

[0063] The machine learning repository **704** includes various machine learning models used to identify the vulnerabilities of the software, operating system, or firmware of the end user devices **195**. The machine learning repository **704** uses the correlated results and policies from the policy database **702** to identify specific machine learning model for identification of the vulnerabilities. The machine learning models are trained based on real time vulnerability datasets.

[0064] Based on the identification of the machine learning model, the vulnerability is determined by the processor **706**. The processor **706** uses the identified machine learning model to process the correlated results to determine the vulnerabilities. The information of the vulnerabilities is provided to the router **708** for further analysis.

[0065] The router **708** receives the vulnerabilities determined by the processor **706** and uses the vulnerabilities to identify the respective policies from the policy database **702**. Based on the identified policies, routes are further identified for remediation. The routes are identified from the routes **620**. For example, vulnerability A has policy B that has routes C, D, F. One of the routes C is identified based on highest compliance with the policies. The remediations are performed through the identified route based on the policy.

[0066] Referring next to FIG. **8**, a block diagram of a priority assigner **614** is shown. The priority assigner **614** is configured to assign priority levels to vulnerabilities identified by the vulnerability identifier **612**. The priority assigner **614** includes a machine learning cache **802**, a risk aggregator **804**, and a ranker **806**.

[0067] The machine learning cache **802** is a repository of machine learning models for identifying

the priority levels for the vulnerabilities. A machine learning model for a specific vulnerability may be identified based on a type of each of the vulnerabilities received from the vulnerability identifier **612** and the respective policies received from the policy store **610**. The policies specify a method of addressing the specific type of vulnerabilities. Weights are assigned to the policies based on the end user device **195**, role of the end user **204**, location of work, connections or other parameters associated with the policies. For example, a policy specifying addressing a malware related vulnerability using a specific firewall or anti-malware software update have a higher weight. Another policy may specify addressing obsolete router software by installing updates at the end user device **195** may have comparatively lower weight. The type of vulnerability, a risk level, and the associated policy weight determines a priority level of remediation of the vulnerability.

[0068] The risk aggregator **804** determines risk levels associated with the vulnerabilities received from the vulnerability identifier **612**. The risk level is determined based on the type of vulnerability. The risk level identifies a level of a severity of the vulnerability on an end user device **195**. The machine learning models determine severity of the vulnerabilities from the data gathered through social media, NVD database, configuration item repositories and vendor supplied information. The severity is used to determine the risk level of the vulnerabilities. The risk level of the vulnerabilities is used by the machine learning models to determine the priority levels of each of the vulnerabilities.

[0069] The priority levels of the vulnerabilities are provided to the ranker **806** for assigning ranks or scores to the vulnerabilities. The ranker **806** assigns priority scores or priority ranks and may order the vulnerabilities based on the priority levels. For example, a priority may be scored on a scale of 10-100 with 100 being the highest or the highest priority level may be ranked as '1'. The priority ranks are used for remediation. The remediation is performed in the order of the priority ranks such that the vulnerabilities with higher priority ranks are remediated before the vulnerabilities with lower priority ranks.

[0070] Referring next to FIG. **9**, a flowchart of an embodiment of a process for policy-driven vulnerability management of network devices in cloud-based multi-tenant systems is shown. In one embodiment, the network devices may be associated with an enterprise. The network devices may be laptops, computers, mobile phones, routers, servers, databases or any other network equipment associated with an end user **204**. The network devices are associated with an end user device **195** of the end user **204**. The depicted part of the process begins in block **902** where a cloud service is selected using a local application of the end user device **195** by the end user **204**.

[0071] At block **904**, vulnerabilities associated with software of the network devices are identified using a machine learning algorithm. The vulnerabilities may also be associated with operating system, firmware, freeware, groupware, sharewares, bundled software, programs, application software, system software, or spreadsheet of the end user device **195**. Vulnerabilities may be due to weaknesses or threats in the network device's operating system, software or hardware of the network device. Vulnerabilities may arise from poor protocol implementation or specification flaws, misconfiguration of the network device, obsolete software applications installed or stored on the network device, and/or the cloud services associated with the network device. Vulnerabilities may arise from the network connection being used on the network device such as a home WiFi router, a VPN network of a hotel. Further, device features, capabilities, or other communication interfaces and protocols available on the network device influence the vulnerabilities in the network devices.

[0072] At block **906**, policies associated with the vulnerabilities are identified. Each of the vulnerabilities have an associated policy. For example, a vulnerability of a downgrade software on a WiFi router at home has a policy that entails update of the software at the end user device **195** by the end user **204**. A vulnerability associated with a protocol implementation requires latest version of the software to be installed by an administrator at the end user device **195**. The policies are based on a tenant including the end user device **195** of the cloud-based multi-tenant system. The

policies are based on the cloud service, the tenant, and a role associated with the end user device **195**.

[0073] At block **908**, remediation is determined for the vulnerabilities based on the policies. Remediation includes patching, disabling the vulnerable process or program, removing a vulnerable component, updating or upgrading system configuration, platform and service being used. By way of an example, in case of a malicious software at the end user device **195**, a policy specifies remediation by installing an anti-virus software at the end user device **195**. The software may be installed by the end user **204**, by an administrator, and/or through a link provided by the mid-link server **185**. In another embodiment, the policy may specify remediation of a malicious software through the mid-link server **185**, where an Intrusion Detection System (IDS) and/or an Intrusion Prevention System (IPS) detects and scrubs known malware signatures as a remediation service.

[0074] At block **910**, a route is identified corresponding to the policies in order to provide the cloud service at the end user device **195**. A number of routes specify the policies through the cloud-based multi-tenant system. The routes terminate with the cloud services across the internet to deliver the cloud services to a number of end user devices **195**. The routes are distributed to the end user devices **195** in a number of domains. The domains separate subsets of the end user devices **195** for tenants.

[0075] At block **912**, the remediations of the vulnerabilities are prioritized using a machine learning algorithm based on a type of the vulnerability, a risk level, and the policies. The risk level is determined based on the type of vulnerability. The risk level identifies a level of an impact of the vulnerability on the network device. The policies determine a manner in which the vulnerabilities are to be remediated. Priority ranks may be assigned to each of the vulnerabilities based on the prioritization. The vulnerabilities may be ordered based on the rank. The vulnerabilities are remediated based on their priority ranks. The vulnerabilities with highest priority ranks are remediated before the vulnerabilities with lower priority ranks.

[0076] At block **914**, the remediation of the vulnerabilities is performed based on the policies in the order of the priority levels. The remediations may be performed at the end user device **195**, at the mid-link server **185** or by the administrator. The end user **204** may perform remediations if specified by the policies. For example, updating firmware of a home router may be performed using a web link at the end user device **195** by the end user **204**.

[0077] At block **916**, the application of the end user device **195** and the cloud service communicate via the route in order to provide the cloud service at the end user device **195**. The route corresponds to the policy of the end user device **195**. It is further determined whether there are other network devices associated with the end user device **195** for identification of the vulnerabilities. If yes, the process moves to block **904**, and the next network device is inspected for vulnerabilities, else the process ends.

[0078] Referring next to FIG. **10**, a flowchart of an embodiment of a process for policy-driven vulnerability management of network devices and execution of the remediations in cloud-based multi-tenant systems is shown. The depicted portion of the process begins in block **1002** where the mid-link server **185** extracts the configuration items from a configuration repository, device configurations from a device repository, and external vulnerability information from external sources such as social websites, vendor websites, etc. The extracted information is updated in real time. Information relevant to an end user device **195** is filtered from the extracted information. The repositories extract data using web crawlers, publicly accessible APIs, or machine learning models from various vendor databases, NVD database, and other publicly available data sources.

[0079] At block **1004**, the configuration items, the device configurations, and the external vulnerability information specific to the end user device **195** are correlated by the mid-link server **185**.

[0080] At block **1006**, vulnerabilities of the end user device **195** are identified based on the

correlation. The vulnerabilities are associated with a software or operating system of the end user device **195**.

[0081] At block **1008**, security risks associated with the vulnerabilities are identified based on a type of the vulnerability. The security risks signify an impact of the vulnerability on the end user device **195**. The security risks identify a threat or damage posed by the vulnerabilities on the end user device **195** if unattended for a period of time.

[0082] At block **1010**, policies are identified for the vulnerabilities based on the type of vulnerability and the end user device **195**. The policies specify a manner in which the vulnerabilities are to be remediated. Each vulnerability has a policy associated with it. The policies are based on a cloud service for the end user device **195**, a tenant of the end user device **195**, and a role associated with the end user device **195**. The policies are stored in the policy store **610**. Weights are assigned to the policies based on the end user device **195**, a role of the end user **204**, a location of work, connections or other protocols associated with the policies.

[0083] At block **1012**, remediations are determined for the vulnerabilities in accordance with the policies. A priority of remediation is assigned to each of the vulnerabilities based on the type of the vulnerability, the security risk, Common Vulnerability Scoring System (CVSS) scores, and the policies associated with the vulnerability. A policy weight is used in the determination of the priority. Priority ranks or scores may be assigned as the priority for the vulnerabilities. The remediation of the vulnerabilities is performed based on the priority of remediation. The remediations of the vulnerabilities may be performed at the end user device **195** by the end user **204**, an administrator, or the mid-link server **185** based on the policies of the vulnerabilities.

[0084] At block **1014**, based on the policies of the vulnerabilities of the end user device **195**, the remediations are performed at the end user device **195** or the mid-link server **185**. The cloud service is provided to the end user device **195** after remediation of the vulnerabilities through a route that is determined based on the policies. The route specifies the end user device **195** or the mid-link server **185**.

[0085] At block **1016**, in case the policies specify that the vulnerabilities cannot be remediated at the end user device **195** and requires the administrator to remediate the vulnerability, an alert is notified to the end user device **195**. The administrator performs the remediation through the mid-link server **185**.

[0086] At block **1018**, in case the policies specify malicious programs or content to be disabled, the end user device **195** may disable the programs and/or block the malicious content. A notification may be provided to the end user **204** through the end user device **195** regarding the remediation to be performed.

[0087] At block **1020**, end user devices **195** are identified for vulnerability identification, in case there are other end user devices **195**, the process moves to block **1002** else the process ends.

[0088] Referring next to FIG. **11**, a flowchart of an embodiment of a process for policy-driven remediation of vulnerabilities in cloud-based multi-tenant systems is shown. The depicted portion of the process begins in block **1102** where the vulnerabilities in a software or an operating system of the end user device **195** are identified.

[0089] At block **1104**, policies corresponding to the vulnerabilities are identified. The policies are based on a cloud service for the end user device **195**, a tenant of the end user device **195**, and a role associated with the end user device **195**. The policies are determined from the policy store **610**. Policies are associated with each of the vulnerabilities.

[0090] At block **1106**, remediation for the vulnerabilities are determined based on the policies. The remediations include parsing, updating and/or upgrading software prone to vulnerabilities.

[0091] At block **1108**, a priority of the remediation for each of the vulnerabilities is determined. The priority is determined based on a type of the vulnerability, a risk level of the vulnerability and a policy of the vulnerability. The vulnerabilities are remediated in order of the priority of remediation.

[0092] At block **1110**, based on the policy associated with the vulnerability, it is determined whether the remediation is performed at the end user device **195** or at the mid-link server **185**. If the remediation is determined to be performed at the end user device **195**, then at block **1114**, the remediation is executed at the end user device **195** by the end user **204**. The remediation may be performed using a web browser link or instructions from an administrator. If the remediation is determined to be performed at the mid-link server **185**, then at block **1112**, the administrator may perform the remediation through the mid-link server **185**. The remediation may also be performed automatically using automatic updates or installs through the mid-link server **185**.

[0093] Specific details are given in the above description to provide a thorough understanding of the embodiments. However, it is understood that the embodiments may be practiced without these specific details. For example, circuits may be shown in block diagrams in order not to obscure the embodiments in unnecessary detail. In other instances, well-known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

[0094] Also, it is noted that the embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a swim diagram, a data flow diagram, a structure diagram, or a block diagram. Although a depiction may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in the figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0095] For a firmware and/or software implementation, the methodologies may be implemented with modules (e.g., procedures, functions, and so on) that perform the functions described herein. Any machine-readable medium tangibly embodying instructions may be used in implementing the methodologies described herein. For example, software codes may be stored in a memory. Memory may be implemented within the processor or external to the processor. As used herein the term "memory" refers to any type of long term, short term, volatile, nonvolatile, or other storage medium and is not to be limited to any particular type of memory or number of memories, or type of media upon which memory is stored.

[0096] In the embodiments described above, for the purposes of illustration, processes may have been described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. It should also be appreciated that the methods and/or system components described above may be performed by hardware and/or software components (including integrated circuits, processing units, and the like), or may be embodied in sequences of machine-readable, or computer-readable, instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. Moreover, as disclosed herein, the term "storage medium" may represent one or more memories for storing data, including read only memory (ROM), random access memory (RAM), magnetic RAM, core memory, magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine readable mediums for storing information. The term "machine-readable medium" includes, but is not limited to portable or fixed storage devices, optical storage devices, and/or various other storage mediums capable of storing that contain or carry instruction(s) and/or data. These machine-readable instructions may be stored on one or more machine-readable mediums, such as CD-ROMs or other type of optical disks, solid-state drives, tape cartridges, ROMs, RAMs, EPROMS, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

[0097] Implementation of the techniques, blocks, steps and means described above may be done in

various ways. For example, these techniques, blocks, steps and means may be implemented in hardware, software, or a combination thereof. For a hardware implementation, the processing units may be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, other electronic units designed to perform the functions described above, and/or a combination thereof.

[0098] Furthermore, embodiments may be implemented by hardware, software, scripting languages, firmware, middleware, microcode, hardware description languages, and/or any combination thereof. When implemented in software, firmware, middleware, scripting language, and/or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium such as a storage medium. A code segment or machine-executable instruction may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a script, a class, or any combination of instructions, data structures, and/or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, and/or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0099] The methods, systems, devices, graphs, and tables discussed herein are examples. Various configurations may omit, substitute, or add various procedures or components as appropriate. For instance, in alternative configurations, the methods may be performed in an order different from that described, and/or various stages may be added, omitted, and/or combined. Also, features described with respect to certain configurations may be combined in various other configurations. Different aspects and elements of the configurations may be combined in a similar manner. Also, technology evolves and, thus, many of the elements are examples and do not limit the scope of the disclosure or claims. Additionally, the techniques discussed herein may provide differing results with different types of context awareness classifiers.

[0100] Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly or conventionally understood. As used herein, the articles "a" and "an" refer to one or to more than one (i.e., to at least one) of the grammatical object of the article. By way of example, "an element" means one element or more than one element. "About" and/or "approximately" as used herein when referring to a measurable value such as an amount, a temporal duration, and the like, encompasses variations of ±20% or ±10%, ±5%, or ±0.1% from the specified value, as such variations are appropriate to in the context of the systems, devices, circuits, methods, and other implementations described herein. "Substantially" as used herein when referring to a measurable value such as an amount, a temporal duration, a physical attribute (such as frequency), and the like, also encompasses variations of ±20% or ±10%, ±5%, or ±0.1% from the specified value, as such variations are appropriate to in the context of the systems, devices, circuits, methods, and other implementations described herein.

[0101] As used herein, including in the claims, "and" as used in a list of items prefaced by "at least one of" or "one or more of" indicates that any combination of the listed items may be used. For example, a list of "at least one of A, B, and C" includes any of the combinations A or B or C or AB or AC or BC and/or ABC (i.e., A and B and C). Furthermore, to the extent more than one occurrence or use of the items A, B, or C is possible, multiple uses of A, B, and/or C may form part of the contemplated combinations. For example, a list of "at least one of A, B, and C" may also include AA, AAB, AAA, BB, etc.

[0102] While illustrative and presently preferred embodiments of the disclosed systems, methods, and machine-readable media have been described in detail herein, it is to be understood that the inventive concepts may be otherwise variously embodied and employed, and that the appended

claims are intended to be construed to include such variations, except as limited by the prior art. While the principles of the disclosure have been described above in connection with specific apparatuses and methods, it is to be clearly understood that this description is made only by way of example and not as limitation on the scope of the disclosure.

Claims

1. (canceled)

2. A cloud-based multi-tenant system for policy driven vulnerability management of a network equipment of an enterprise, the cloud-based multi-tenant system comprising: an application running on an end user device of a plurality of end user devices that selects a cloud service from a plurality of cloud services; a plurality of routes through the cloud-based multi-tenant system to deliver the plurality of cloud services to the plurality of end user devices, wherein the plurality of routes is specified for a plurality of policies; and a mid-link server configured to: identify a plurality of vulnerabilities associated with a plurality of firmware of the end user device, identify a plurality of factors including a type of vulnerability, risks associated with the plurality of vulnerabilities and a time of action for a remediation of the plurality of vulnerabilities, wherein based on the identified plurality of factors, each vulnerability is assigned a priority for remediation, identify the plurality of policies associated with the plurality of vulnerabilities, wherein the plurality of policies is specified for the plurality of end user devices, identify the plurality of routes corresponding to the plurality of policies for the remediation, wherein the plurality of routes are associated with the plurality of policies and a corresponding compliance rate with the plurality of policies, determine the compliance rate with the plurality of policies, select a route from the plurality of routes for the remediation based on the route with a high compliance rate with the plurality of policies, execute the remediation of the plurality of vulnerabilities based on the plurality of policies in accordance with the priority and the route with the high compliance rate, and establish communication via the route between the application and the cloud service based on the plurality of policies.

3. The cloud-based multi-tenant system for the policy driven vulnerability management of the network equipment of the enterprise as recited in claim 2, wherein the plurality of vulnerabilities is identified based on a machine learning algorithm.

4. The cloud-based multi-tenant system for the policy driven vulnerability management of the network equipment of the enterprise as recited in claim 2, wherein the priority associated with plurality of vulnerabilities is based on a numerical score indicating a severity of the plurality of vulnerabilities translated into a qualitative representation including low, medium, high, and critical.

5. The cloud-based multi-tenant system for the policy driven vulnerability management of the network equipment of the enterprise as recited in claim 2, wherein an Information Technology (IT) module is configured to review and modify the priority in accordance with the plurality of end user devices to provide approval of the enterprise for the remediation.

6. The cloud-based multi-tenant system for the policy driven vulnerability management of the network equipment of the enterprise as recited in claim 2, wherein the plurality of policies associated with the plurality of vulnerabilities are assigned weights based on based on the end user device, role of an end user, location of work, connections or other parameters associated with the plurality of policies.

7. The cloud-based multi-tenant system for the policy driven vulnerability management of the network equipment of the enterprise as recited in claim 2, wherein when the plurality of vulnerabilities associated with the plurality of policies cannot be remediated at the end user device, an alert is notified to the end user device for an administrator to perform the remediation through the mid-link server.

8. A vulnerability identification and remediation method for a network equipment in a cloud-based multi-tenant system of an enterprise, the method comprising: receiving from an application running

on an end user device of a plurality of end user devices, a selection of a cloud service from a plurality of cloud services; identifying at a mid-link server, a plurality of policies associated with a plurality of vulnerabilities, wherein the plurality of policies is specified for the plurality of end user devices; identifying at the mid-link server, a plurality of factors including a type of vulnerability, risks associated with the plurality of vulnerabilities and a time of action for a remediation of the plurality of vulnerabilities, wherein based on the identified plurality of factors, each vulnerability is assigned a priority for remediation; determining at the mid-link server, remediation for the plurality of vulnerabilities based on the plurality of policies, wherein the plurality of policies is based on the cloud service, a tenant of the end user device, and/or a user role associated with the end user device; identifying at the mid-link server, the plurality of routes corresponding to the plurality of policies for the remediation, wherein the plurality of routes are associated with the plurality of policies and a corresponding compliance rate with the plurality of policies; determining at the mid-link server, the compliance rate with the plurality of policies and selecting a route from the plurality of routes for remediation based on the route with a high compliance rate; executing at the mid-link server, remediation of the plurality of vulnerabilities in accordance with the priority and the route with the high compliance rate; and establishing via the mid-link server, communication via the route between the application and the cloud service based on the plurality of policies.

9. The vulnerability identification and remediation method for the network equipment in the cloud-based multi-tenant system of the enterprise as recited in claim 8, wherein the plurality of vulnerabilities is identified based on a first machine learning algorithm.

10. The vulnerability identification and remediation method for the network equipment in the cloud-based multi-tenant system of the enterprise as recited in claim 8, wherein the priority associated with plurality of vulnerabilities is based on a numerical score indicating a severity of the plurality of vulnerabilities translated into a qualitative representation including low, medium, high, and critical.

11. The vulnerability identification and remediation method for the network equipment in the cloud-based multi-tenant system of the enterprise as recited in claim 8, further comprising reviewing and modifying by an Information Technology (IT) module, the priority in accordance with the plurality of end user devices to provide approval of the enterprise for the remediation.

12. The vulnerability identification and remediation method for the network equipment in the cloud-based multi-tenant system of the enterprise as recited in claim 8, wherein the plurality of policies associated with the plurality of vulnerabilities are assigned weights based on the end user device, role of an end user, location of work, connections or other parameters associated with the plurality of policies.

13. The vulnerability identification and remediation method for the network equipment in the cloud-based multi-tenant system of the enterprise as recited in claim 8, wherein when the plurality of vulnerabilities associated with the plurality of policies cannot be remediated at the end user device, notifying an alert to the end user device for an administrator to perform the remediation through the mid-link server.

14. A cloud-based multi-tenant system for policy-based vulnerability management, the cloud-based multi-tenant system comprising one or more processors and one or more memories with code for: correlating at a mid-link server, configuration items associated with a plurality of firmware of a plurality of end user devices, device configurations including vendor specific information, and external vulnerability information including external websites, social media, and/or vendor websites from a plurality of data sources; identifying at the mid-link server, a plurality of vulnerabilities associated with the plurality of firmware based on the correlation; receiving at the mid-link server, from an application running on an end user device of the plurality of end user devices, a selection of a cloud service from a plurality of cloud services; identifying at the mid-link server, a plurality of factors including a type of vulnerability, risks associated with the plurality of vulnerabilities and a time of action for a remediation of the plurality of vulnerabilities, wherein

based on the identified plurality of factors, each vulnerability is assigned a priority for remediation; determining at the mid-link server, remediation for the plurality of vulnerabilities based on a plurality of policies, wherein the plurality of policies is based on the cloud service, a tenant of the end user device, and/or a user role associated with the end user device; identifying at the mid-link server, the plurality of routes corresponding to the plurality of policies for the remediation, wherein the plurality of routes are associated with the plurality of policies and a corresponding compliance rate with the plurality of policies; determining at the mid-link server, the compliance rate with the plurality of policies and selecting a route from the plurality of routes for remediation based on the route with a high compliance rate; executing at the mid-link server, remediation of the plurality of vulnerabilities in accordance with the priority and the route with the high compliance rate; and communicating via the route between the application and the cloud service based on the plurality of policies.

15. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, further comprising prioritizing the remediation of the plurality of firmware based on the type of the plurality of vulnerabilities, security risks, and the plurality of policies.

16. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, wherein the priority associated with plurality of vulnerabilities is based on a numerical score indicating a severity of the plurality of vulnerabilities translated into a qualitative representation including low, medium, high, and critical.

17. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, wherein the plurality of policies varies with each tenant of a plurality of tenants of the cloud-based multi-tenant system.

18. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, further comprising reviewing and modifying by an Information Technology (IT) module, the priority in accordance with the plurality of end user devices to provide approval of an enterprise for the remediation.

19. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, wherein the plurality of policies associated with the plurality of vulnerabilities are assigned weights based on the end user device, role of an end user, location of work, connections or other parameters associated with the plurality of policies.

20. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, wherein when the plurality of vulnerabilities associated with the plurality of policies cannot be remediated at an end user device, notifying an alert to an end user device for an administrator to perform the remediation through the mid-link server.

21. The cloud-based multi-tenant system for the policy-based vulnerability management as recited in claim 14, wherein the configuration items include hostnames, IP addresses, models, make, roles, or software versions of the plurality of firmware.