



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/641,007	05/01/2012		125	0079152-000004		

CONFIRMATION NO. 9211

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

FILING RECEIPT



OC000000054177322

Date Mailed: 05/16/2012

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

Applicant(s)

Srinivas Kumar, Cupertino, CA;
Dennis Vance Pollutro, Clymer, NY;

Power of Attorney:

Charles Wieland III--33096

If Required, Foreign Filing License Granted: 05/09/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/641,007**

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

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

SYSTEM AND METHOD FOR OPERATIONAL INTEGRITY ATTESTATION

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

page 1 of 3

patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

page 2 of 3

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](https://www.selectusa.gov).

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 C.F.R. § 1.53(c).

Attorney Docket Number		0079152-000004			
Inventor(s)					
Given Name	Middle Name	Family Name	CITY	STATE	COUNTRY
Srinivas		KUMAR	Cupertino	California	USA
Dennis	Vance	POLLUTRO	Clymer	New York	USA
Title of Invention					
SYSTEM AND METHOD FOR OPERATIONAL INTEGRITY ATTESTATION					
Correspondence Address					
The address corresponding to Customer Number 2 1 8 3 9					
This invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.					
☒ No.					
☐ Yes, the name of the U.S. Government agency and the Government contract number are:					
Enclosed Application Parts					
☒	Specification/Claims/Abstract	# of Pages	46	☐	CD(s) Number
☒	Drawings	# Sheets	26	☐	Other (specify):
	Total Pages in Spec/Drawings		72		
☒ Application Data Sheet. See 37 CFR 1.76					
Method of Payment of Filing Fees				FILING FEE AMOUNT	
☒	Applicant claims small entity status. See 37 CFR 1.27				
☒	The Director is hereby authorized to charge any deficiency in filing fees or credit any overpayment to Deposit Account 02-4800.			Filing Fee (2005)	\$ 125.00
				Total Page Fee	
☒	Payment by credit card. Payment will be made electronically at time of filing.			(101+ pages) (2085) \$155	\$ _____
☐	Charge filing fee to Deposit Account 02-4800.			Total App. Filing Fee	\$ 125.00

SIGNATURE

TYPED or PRINTED NAME

Charles F. Wieland III

703.836.6620

DATE _____

May 1, 2012

Regis. No.

33,096

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

APPLICATION DATA SHEET

Application Information

Application Number::

Filing Date::

Application Type:: Provisional

Subject Matter:: Utility

CD-ROM or CD-R?: None

Computer Readable Form (CRF)?:: No

Title:: SYSTEM AND METHOD FOR OPERATIONAL
INTEGRITY ATTESTATION

Attorney Docket Number:: 0079152-000004

Request for Early Publication?: No

Request for Non-Publication?: No

Total Drawing Sheets:: 26

Small Entity?: Yes

Petition Included?: No

Secrecy Order in Parent Appl.?: No

Applicant Information

Applicant Authority Type:: Inventor

Primary Citizenship Country:: USA

Status:: Full Capacity

Given Name:: Srinivas

Family Name:: KUMAR

City of Residence:: Cupertino

State or Province of Residence:: California

Country of Residence::	USA
Street of Mailing Address::	10926 Northridge Square
City of Mailing Address::	Cupertino
State or Province of Mailing Address::	California
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	95014
Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Dennis
Middle Name::	Vance
Family Name::	POLLUTRO
City of Residence::	Clymer
State or Province of Residence::	New York
Country of Residence::	USA
Street of Mailing Address::	8613 Knowlton Road
City of Mailing Address::	Clymer
State or Province of Mailing Address::	New York
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	14724

Correspondence Information

Correspondence Customer Number:: 21839

Phone Number:: (703) 836-6620

Fax Number: (703) 836-2021

Representative Information

Representative Customer Number:: 21839

Assignee Information

Assignee Name:: TAASERA, INC.

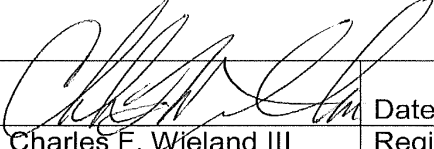
Street of Mailing Address:: 1030 State Street

City of Mailing Address:: Erie

State or Province of Mailing Address:: Pennsylvania

Country of Mailing Address:: USA

Postal or Zip Code of Mailing Address:: 16501

Signature		Date	May 1, 2012
Name	Charles F. Wieland III	Registration No.	33,096

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SYSTEM AND METHOD FOR OPERATIONAL INTEGRITY ATTESTATION		
First Named Inventor/Applicant Name:		Srinivas KUMAR		
Filer:		Charles F. Wieland III/Beverly Caraway		
Attorney Docket Number:		0079152-000004		
Filed as Small Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional Application filing fee	2005	1	125	125
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				125

Electronic Acknowledgement Receipt	
EFS ID:	12677224
Application Number:	61641007
International Application Number:	
Confirmation Number:	9211
Title of Invention:	SYSTEM AND METHOD FOR OPERATIONAL INTEGRITY ATTESTATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/Beverly Caraway
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000004
Receipt Date:	01-MAY-2012
Filing Date:	
Time Stamp:	16:39:36
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$125
RAM confirmation Number	3597
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Specification	SPEC.pdf	160047 fb2d948343462430c641852470a3009ad45ec752	no	45
Warnings:					
Information:					
2	Drawings-only black and white line drawings	DRAW.pdf	2568107 54dc6376c6f860e660901db5f10a6d387cd461d7	no	26
Warnings:					
Information:					
3	Transmittal of New Application	TL.pdf	55361 7697da91e0169a6bf7e682812461b4f45ea75077	no	1
Warnings:					
Information:					
4	Application Data Sheet	ADS.pdf	65424 6c3a752904064c0448720d82f839a6c06d48dc66	no	3
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
5	Fee Worksheet (SB06)	fee-info.pdf	29865 9621f11b2d2913ed462df63a2a43a340d6a20cfc	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2878804		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

**APPLICATION FOR
UNITED STATES LETTERS PATENT**

FOR

SYSTEM AND METHOD FOR OPERATIONAL INTEGRITY ATTESTATION

by

**SRINIVAS KUMAR
AND
DENNIS POLLUTRO**

**Attorney Docket No. 0079152-000004
BUCHANAN INGERSOLL & ROONEY PC
CUSTOMER No. 21839
P.O. Box 1404
Alexandria, VA 22313-1404**

SYSTEM AND METHOD FOR OPERATIONAL INTEGRITY ATTESTATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of U.S. Non-Provisional Patent Application No. 13/399,065 entitled "SYSTEM AND METHOD FOR APPLICATION ATTESTATION," filed February 16, 2012, and U.S. Provisional Patent Application No. 61/443,854 entitled "SYSTEM AND METHOD FOR APPLICATION ATTESTATION," filed February 17, 2011, both of which are incorporated herein by reference in their entireties.

BACKGROUND OF THE DISCLOSURE

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to the field of data center virtualization and, more particularly, to a system and method to provide operational integrity attestation of application security and user reputation at runtime.

DESCRIPTION OF THE RELATED ART

[0003] One recent trend in computing is the trend towards virtualization and cloud computing in which, for example, enterprise software is no longer owned by the customer, but instead the Information Technology infrastructure can be provided by a third party and the software applications may be sold as service offerings.

-3-

[0004] Traditional legacy and emerged security solutions such as next-generation anti-virus, network firewalls, intrusion detection/prevention systems operate based on signatures, protocol anomalies or virtual execution in a sandbox to monitor threats and attacks. However, once the target system becomes infected or compromised, these technologies have been proven ineffective in the protection of the systems and prevention of data breaches or service disruptions. Emerging attacks exhibit a low and slow mode of operation and are signature-less to evade traditional defensive methods. Further, these technologies are agnostic to the runtime operational integrity of compute workloads on the target (victim) systems and therefore do not offer any level of remediation to service the affected systems and merely provide coarse grained access controls limited to a simple allow or deny decision logic. The virtualized and cloud computing on-demand and elastic models require dynamic security orchestration both at the device and network level that is lacking in these approaches.

[0005] A significant metric that relates to the lack of remediation controls in current security controls is the high rate of false positives and negatives in the detection of threats. False positives are unproductive and reduce operating capacity in data centers. False negatives lead to the bypass of security controls and compromise of the target systems and services. Signature based approaches are vulnerable to improvised attacks staged at targeted systems.

[0006] The proliferation of applications (business, social networking and gaming software) in Enterprise and cloud computing ecosystems has significantly increased the attack surface and window of exposure. Application runtime operational integrity

-4-

is a critical factor in building end-to-end trust from device to service. The proliferation of unmanaged devices such as mobile smart phones and Bring Your Own Device (BYOD) policies in Enterprise network environments have increased the risk of advanced coordinated threats.

[0007] Current identity management (IdM) approaches are generally aimed at domain level authentication of users for the use of a security token in a transaction or business process wherein the issuance of the token is strictly based on proof of possession of credentials and not the reputation of the user. While the industry has adopted multi-factor authentication technologies for increased protection from malicious users, whose intent is to steal credentials for the purpose of impersonation or delegation, these security controls do not provide the means to incorporate attribution of an authenticated user's risk posture, independent of provisioned entitlements, as a component of access policy, based on correlation of location and device agnostic global threat intelligence about the user.

[0008] The emerging cloud based application hosting model requires a higher level of scrutiny of device and user security posture. Threats are posed by both external and internal users, and therefore it has become harder to determine whether an authenticated user is a trustworthy operative. Application and network layer entitlements are largely static in nature. While role based access control (RBAC) systems are positioned to offer dynamic policies, these are not based on any form of aggregation of external threat intelligence in the context of the user in the transaction.

-5-

[0009] Tokenization of identities by Security Token Services (STS) intended to facilitate in Identity Federation and Single Sign On (SSO) for web and Enterprise applications have only aggravated the threat vectors by expanding the scope of resources that an authenticated user may access implicitly without granular context. Along with the coarse access policies offered by traditional security controls, such as firewalls and intrusion prevention systems, this increases the attack surface for application exploits by malicious users leveraging the excessive privileges granted by default to most users (and groups) today, in the absence of strict Separation of Duties (SoD) and Principle of Least Privilege (PoLP) enforcement.

[0010] Several studies have uncovered conclusive evidence that the largest risk, associated with malicious activities resulting in theft of confidential data, intellectual property or financial losses for enterprises and consumers, arises from insider rather than outsider or man-in-the-middle attacks. Threat assessment systems have been predominantly focused on the means and methods rather than the adversary or operator. There was been no emphasis on the reputation score of a user in the transaction or business process as a real time integrity metric for integration with access policy decision logic. A user reputation score may serve either as a punitive or corrective method of intervention for the proactive prevention of exploits and data breaches.

SUMMARY OF THE DISCLOSURE

[0011] The presently disclosed technology may be embodied as a method, apparatus and/or system to continuously monitor one or more systems and/or to

-6-

correlate event and behavior of systems on an instrumented target platform at runtime using or based on a plurality of assertions (or statements).

[0012] The presently disclosed technology also may be embodied as a method, apparatus, and/or system for infection diagnosis based on reconnaissance based intelligence correlation and a threat life cycle model of advanced low-and-slow attacks wherein malware may operate through a series of benign actions at the endpoint device.

[0013] The presently disclosed technology also may be embodied as a method, apparatus, and/or system for a plurality of services that enable visibility, control, and/or compliance in a cloud computing environment with a runtime dashboard to display operational integrity metrics of systems based on a plurality of threat vectors.

[0014] The presently disclosed technology also may be embodied as a further method, apparatus and/or system to establish device-to-network flows based on dynamic attestation of device integrity, and/or security controls provisioned based on integrity and context aware business logic instead of, for example, topology based coordinates associated with encapsulation headers in network packets.

[0015] The presently disclosed technology also may be embodied as a yet further method, apparatus and/or system to authorize user-to-application transactions and/or data exchange in an established connection, during the authentication phase based on dynamic attestation of devices.

[0016] The presently disclosed technology also may be embodied as an additional method, apparatus and/or system for a calculus of risk based on a plurality

-7-

of sensory inputs from network and endpoint sensors to correlate network activity, system configuration, resource utilization and application integrity.

[0017] The network and endpoint sensors may be configured to measure runtime operational integrity and/or detect anomalous deviations from baseline based on rulesets to generate tiered alerts.

[0018] The presently disclosed technology also may be embodied as a method, apparatus and/or system that may include an event and behavior correlation engine to receive alerts, calculate risks and generate warnings.

[0019] The presently disclosed technology also may be embodied as another method, apparatus and/or system to remediate systems that are deviated, vulnerable, in duress or compromised based on the calculus of risk.

[0020] The presently disclosed technology also may be embodied as a method, apparatus and/or system for: (1) a correlation engine to receive scan reports form vulnerability, configuration, compliance, and patch scan services; (2) a correlation matrix to analyze elements of the scan reports; (3) generation of an integrity profile of systems.

[0021] The presently disclosed technology also may be embodied as a method, apparatus and/or system for: (1) an event correlation logic based on multiple predicate scores; (2) a deviation from a prescribed value constraint per attribute (or metric) to determine a predicate score; (3) a score that is inversely proportional to the deviation; (4) a sample rate that is the required measurement frequency; (5) a recurrence of successive deviations; (6) a weight for the attribute constraint; (7) an integrity confidence for the system or process (or application) entity that is

-8-

determined as a weighted average of predicate scores; (8) outliers identified as exceptions (across multiple systems or processes).

[0022] The presently disclosed technology also may be embodied with threat identification categories including: (1) static image (binary, intermediate code, or script) analysis; (2) dynamic image (binary, intermediate code, or script) analysis with process, platform and network monitors; (3) malware analysis for evasion techniques (multiple packing, obfuscated APIs, anti-debugging, anti-memory, anti-tracing, VMM/emulator detection); (4) dynamic system analysis of performance metrics harvested through native machine instrumentation, registry, and file system monitors; (5) temporal system analysis with consolidated integrity measurement and verification assessments and scan reports.

[0023] The presently disclosed technology also may be embodied as a method, apparatus and/or system for integrity confidence measurement including: (1) a weighted average of system (or platform) predicate scores; (2) system (or platform) outliers; (3) weighted average of process (or application package) predicate scores; (4) process outliers.

[0024] The presently disclosed technology also may be embodied as a method, apparatus and/or system for the generation of user reputation scores based on: (1) threat vectors modeled by user actions; (2) risk correlation with aggregation of intelligence related to accessed object (resource) attribution, subject roles, globally unique subject identifiers, security information and event management analytics, and geo-location services.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

-9-

[0025] The invention is best understood from the following detailed description when read in connection with the accompanying drawings. According to common practice, various features/elements of the drawings may not be drawn to scale. Common numerical references represent like features/elements. The following figures are included in the drawings:

FIG. 1 is a schematic diagram illustrating an exemplary system/architecture in accordance with various exemplary embodiments;

FIG. 2 is a schematic diagram illustrating a method of endpoint and network activity correlation in accordance with various exemplary embodiments;

FIG. 3A is a schematic diagram illustrating another method of early warning and response automation in accordance with various exemplary embodiments;

FIG. 3B is a schematic diagram illustrating another method of intersystem risk assessment and remediation in accordance with various exemplary embodiments;

FIG. 4 is a schematic diagram illustrating a further method to consolidate and normalize network endpoint assessments in accordance with various exemplary embodiments;

FIG. 5 is a schematic diagram illustrating a method to measure and evaluate executable image (binary, intermediate or script) risk with various exemplary embodiments;

FIG. 6 is a schematic diagram illustrating a method to instrument and measure the network endpoint risk with various exemplary embodiments;

FIG. 7A is a schematic diagram illustrating a method to monitor endpoint events with various exemplary embodiments;

-10-

FIG. 7B is a schematic diagram illustrating a method to generate endpoint alerts with various exemplary embodiments;

FIG. 7C is a schematic diagram illustrating a method to correlate endpoint alerts and generate endpoint warnings with various exemplary embodiments;

FIG. 8 is a schematic diagram illustrating a method to correlate a plurality of events for system operational integrity determination with various exemplary embodiments;

FIG. 9 is a schematic diagram illustrating a method to consolidate and correlate a plurality of identity, inventory and log management systems for user reputation determination with various exemplary embodiments;

FIG. 10 is a schematic diagram illustrating a method for the calculus of risk with various exemplary embodiments;

FIG. 11 is a schematic diagram illustrating a method for the generation of user reputation scores based on a calculus of risk with various exemplary embodiments;

FIG. 12 is a schematic diagram illustrating a method for network flow remediation based on a calculus of risk with various exemplary embodiments;

FIG. 13 is a schematic diagram illustrating a method to remediate mobile devices and wireless network flows based on a calculus of risk with various exemplary embodiments;

FIG. 14 is a schematic diagram illustrating an exemplary trust management console including an operational runtime integrity dashboard in accordance with various exemplary embodiments;

-11-

FIG. 15 is a schematic diagram illustrating an exemplary trust management console including a system configuration dashboard in accordance with various exemplary embodiments;

FIG. 16 is a schematic diagram illustrating an exemplary trust management console including a resource utilization dashboard in accordance with various exemplary embodiments;

FIG. 17 is a schematic diagram illustrating an exemplary trust management console including an application integrity dashboard in accordance with various exemplary embodiments;

FIG. 18 is a schematic diagram illustrating an exemplary security administration console including a network activity dashboard in accordance with various exemplary embodiments;

FIG. 19 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 20 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 21 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 22 is a flowchart illustrating a method in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 23 is a diagram of an example computer system in which embodiments can be implemented.

DETAILED DESCRIPTION

[0026] Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range of equivalents of the claims and without departing from the invention.

[0027] Many enterprises are moving there IT infrastructures to cloud computing environments (e.g., in which third parties may provide shared computing resources and applications running on those resources are offered as services to a plurality of customers) for various reasons including: (1) increased computing power; (2) increased storage capacity, and/or (3) increased network bandwidth, among others. Enterprise applications and mission critical applications may be executed in the cloud. Without adequate device, system and application security, the cloud can compromise these applications causing large financial losses. Data confidentiality, data integrity and data availability can be maintained in the cloud computing environment even when such applications may be controlled by these third parties. For example, enterprises are moving from self-managed on-premise data centers to service-provider managed outsourced virtual data centers (e.g., the cloud computing environments). The cloud may enable traditional information technology devices, systems and applications to transparently execute from these service-providers managed outsourced virtual data centers. As newer technologies emerge, the cloud infrastructure may evolve transparent to and scalable with enterprise operations. Security in such environments may be an emerging challenge.

-13-

[0028] The current security paradigm is based on a hard edge and soft core architecture. Security appliances such as network firewalls and intrusion detection/prevention systems deploy at the edge (perimeter). Antivirus and network based integrity measurement and verification services scan and audit the soft-core that comprises of business critical systems, services and high value data silos. Once the edge is breached, defensive methods are ineffective in protecting vulnerable or compromised systems. The hard edge does not provide any level of assurance of the runtime operational integrity of the soft core.

[0029] The heavy reliance on extensive application whitelists/blacklists, IP reputation lists, signatures, protocol anomalies and virtual execution in a sandbox, provides targeted and coordinated attacks a large staging surface to maneuver around with meticulously engineered evasion methods exploiting the gaps. Irrespective of the method of break-in, the post-infection behaviors during the window of exposure on a victim machine or environment are difficult to conceal, but may be obscured from timely detection and diagnosis by security administrators and virtual execution (sandbox) environments through evasion techniques. Various exemplary embodiments include an early warning system for threat identification and diagnosis with high forensic confidence and infection summaries for manual and/or automated intervention.

[0030] In certain exemplary embodiments, deviations from a baseline healthy operational state to a vulnerable or compromised state may be detected, and the infection identified, before there is further propagation of the threat across interconnected systems, or information is exfiltrated resulting in data loss or theft.

-14-

[0031] The proliferation of unmanaged smart phones and Bring Your Own Device (BYOD) initiatives in the Enterprise ecosystem have increased the ability of advanced malware to evade traditional network and endpoint security controls and propagate to connected systems over standard protocols. Various exemplary embodiments include determination of the operational integrity of the device and/or the user in a transaction with an on-premise or off-premise service, based on the calculus of risk from a plurality of sensory inputs, for transaction and/or flow level remediation of infected devices.

[0032] FIG. 1 is a schematic diagram illustrating an exemplary network 100 in accordance with various exemplary embodiments.

[0033] Referring to FIG. 1, the exemplary network 100 may include an event and behavior correlation engine 130 that may perform risk correlation 120 based on continuous monitoring 110 using a plurality of sensory inputs of network activity 111, system configuration 113, resource utilization 115 and application integrity 117, a runtime dashboard 150 that may receive real time status indications 131 for visibility of operational integrity of systems, a remediation engine 170 that may receive real time directives 132 for control of infected systems.

[0034] The event and behavior correlation engine 130 may receive system events and infection profiles 112 from the network activity sensor 111, integrity measurement and verification reports 114 of scans performed as per a schedule (for example, daily, weekly, bi-weekly, monthly) from the system configuration sensor 113, system events 116 of compute, network and storage resource consumption

-15-

from the resource utilization sensor 115, and system events 118 of image profiles and local execution context 118 from the application integrity sensor 117.

[0035] The remediation engine 170 may perform actions 171 on a virtual machine 172, actions 173 on a network flow controller 174, or actions 175 on a transaction 176 based on configured trigger controls.

[0036] FIG. 2 is a schematic diagram illustrating an exemplary method 200 in accordance with various exemplary embodiments.

[0037] Referring to FIG. 2, the exemplary method 200 may include endpoint event correlation 240 that may receive system alerts 230 from an instrumented system 210 with a plurality of sensors for application integrity 211, resource utilization 212, and system configuration 213, a network activity correlation 260 that may receive system alerts 250 from a network activity sensor 220, an orchestrator 290 that may receive system warnings 270 from the network activity correlation 260, and system warnings 270 from the endpoint event correlation 240, to coordinate manual or automated actions on infected systems.

[0038] FIG. 3A is a schematic diagram illustrating an exemplary method 300 in accordance with various exemplary embodiments.

[0039] Referring to FIG. 3A, the exemplary method 300 may include a early warning system 301 for continuous monitoring of runtime integrity of systems, a automated and rapid response 303 for orchestration and remediation of infected systems, and a protocol 302 for data exchange between the monitoring and orchestration systems.

-16-

[0040] The early warning system 301 may monitor instrumented systems to measure and evaluate runtime operational integrity to determine whether a system has deviated, become vulnerable, is in duress or has been compromised.

[0041] FIG. 3B is a schematic diagram illustrating an exemplary method 310 in accordance with various exemplary embodiments.

[0042] Referring to FIG. 3B, the exemplary method 301 may include a calculus of risk 320 for the data center application and data silos, that may receive sensory inputs 314 from instrumentation 313 including integrity measurement and verification scan correlation 315, network activity correlation 316 and endpoint event correlation 317, and may generate integrity metrics for security orchestration 321, and may dispatch directives to an edge device 323 (for example, network firewall) for user access controls 322, to a load balancer 325 for session controls 324, or to a network fabric element 327 (for example, a switch or router) for flow controls 326.

[0043] The security orchestration 321 may include user access controls 322 to block the infected device or malicious user from accessing protected data center centers, session controls 324 to divert users from infected systems or infected devices from protected systems, flow controls 326 to quarantine infected systems, divert traffic away from protected systems, or redirect traffic from attackers to pure, high-interaction or low-interaction honeypots.

[0044] FIG. 4 is a schematic diagram illustrating an exemplary method 400 in accordance with various exemplary embodiments.

[0045] Referring to FIG. 4, the exemplary method 400 may include a trust orchestrator 430, a trust broker 407 that may receive integrity reports 406 published

-17-

by endpoint assessment services 401 generated by performing a vulnerability scan 402, configuration scan 403, compliance scan 404 or patch scan 405 of networked endpoints, a normalizer and collator 408, a system event correlator 410 that may receive temporal events 409 associated with an endpoint and use a risk correlation matrix 411 to correlate and generate an integrity profile 420 for an endpoint.

[0046] FIG. 5 is a schematic diagram illustrating an exemplary method 500 in accordance with various exemplary embodiments.

[0047] Referring to FIG. 5, the exemplary method 500 may include an endpoint trust agent 510 that may comprise of a process monitor 514 that may observe local execution context of applications and services, a socket monitor 513 that may observe network activities of applications and services, a system monitor 512 that may observe system and platform resources consumed by applications and services, an application integrity module 516 and a resource utilization module 515 that may assess operational integrity based on rulesets, a native machine instrumentation 511 on the device, a trust orchestrator 530 that may comprise of a system event correlator 531 and a trust broker 532, and a malware analyzer 540.

[0048] The system event correlator 531 may receive endpoint events 520 from the endpoint trust agent 510 as sensory inputs to a calculus of risk. The trust broker 532 may receive an image file and image attributes 518, send the received image file to a malware analyzer 540 for diagnosis, receive an asynchronous prognosis 533 and forward an asynchronous image profile 519 to the process monitor 514 to include in ruleset processing for diagnosis at the application integrity module 516.

-18-

[0049] FIG. 6 is a schematic diagram illustrating an exemplary method 600 in accordance with various exemplary embodiments.

[0050] Referring to FIG. 6, the exemplary method 600 may include a device 660 that may comprise of a runtime monitor 620 that may register for and receive raw events 611 from native machine instrumentation 610 and raise integrity events 621 to an integrity processor 630 that may apply rulesets 631 to generate integrity alerts 632 and an event correlation matrix 633 to map integrity warnings 634 to endpoint events 635 for dispatch to a trust orchestrator 670 that may comprise of a system event correlator 640 that may use a risk correlation matrix 641 to generate an integrity profile 650 for the system.

[0051] In certain exemplary embodiments, application integrity 516 and resource utilization 515 described in FIG. 5 may be included in the integrity processor 630.

[0052] In certain exemplary embodiments, the process monitor 514, system monitor 512 and socket monitor 513 as described in FIG. 5 may be included in the runtime monitor 620.

[0053] FIG. 7A is a schematic diagram illustrating an exemplary method 700 in accordance with various exemplary embodiments.

[0054] Referring to FIG. 7A, the exemplary method 700 may include per process events 701, per processor events 702, system events 703, and per image binary analysis 704. The events include, but are not limited to, all events available through native machine instrumentation and extensible on the platform with provider plug-ins.

[0055] FIG. 7B is a schematic diagram illustrating an exemplary method 710 in accordance with various exemplary embodiments.

-19-

[0056] Referring to FIG. 7B, the exemplary method 710 may include platform alerts 711, per image alerts 712, grayware alerts 713, and per application alerts 714. The alerts are configurable and extensible, and not limited to the enumerations illustrated in FIG. 7B.

[0057] FIG. 7C is a schematic diagram illustrating an exemplary method 720 in accordance with various exemplary embodiments.

[0058] Referring to FIG. 7C, the exemplary method 720 may include a risk correlation matrix 721, system warning classes 722, system warnings 723, integrity warnings 724, and alert expression 725 as a function of at least an attribute, a attribute value constraint, a sample rate, a recurrence, a score and a weight.

[0059] The risk correlation matrix 721 may comprise of at least a universally unique identifier (UUID) for the system, system warnings mapped to at least one system warning class, and at least a system warning class to diagnose system deviated, system duress, system vulnerable and system infected.

[0060] In certain exemplary embodiments, a plurality of timers may be associated in the evaluation of system warnings and system warning classes, the calculus of risk, and generation of an integrity profile for the system.

[0061] FIG. 8 is a schematic diagram illustrating an exemplary method 800 in accordance with various exemplary embodiments.

[0062] Referring to FIG. 8, the exemplary method 800 may include an endpoint trust agent 810 on a device 801, a network analyzer 830 that may include a network activity correlator 831, an endpoint assessment service 820, a service provider for orchestration and/or policy enforcement point services 860, and a trust orchestrator

-20-

840 that may include a trust broker 841, a system event correlator 843, a trust supervisor 846, and a remediation controller 848.

[0063] In certain exemplary embodiments, the system event correlator 843 may receive endpoint events 811 from the endpoint trust agent 810, temporal events 842 from the trust broker 841, correlate and send an integrity profile for a network endpoint 844 to the trust supervisor 846 and the network activity correlator 831.

[0064] In certain exemplary embodiments, the trust supervisor 848 may receive an infection profile 832 for a network endpoint from the network activity correlator 831, an integrity profile 844 for a network endpoint from the system event correlator 843, analyze and classify threats along with a forensic confidence score, send real time actions 847 to the remediation controller 848, and real time status indications 850 to a dashboard controller 870. The remediation controller 848 may send directives 849 to orchestration and policy enforcement point services 860 for machine, flow or transaction level remediation.

[0065] In certain exemplary embodiments, the infection profile 832 may comprise of at least the victim endpoint address, a forensic confidence of the declared infection, the attacker source, the command and control source, the full evidence chain, and the infection time range (onset, duration).

[0066] In certain exemplary embodiments, the integrity profile 844 may comprise of at least the endpoint address, system warning class, forensic confidence of the declared warning, and the full evidence chain.

-21-

[0067] In certain exemplary embodiments, the risk correlation matrix 411, 641 and 911 of FIGs. 4, 6 and 9 respectively may be included in the trust supervisor 846 to consolidate and correlate integrity profile 844 and infection profile 832 of FIG. 8.

[0068] FIG. 9 is a schematic diagram illustrating an exemplary method 900 in accordance with various exemplary embodiments.

[0069] Referring to FIG. 9, the exemplary method 900 may include a trust orchestrator 930, a trust broker 920 that may query and receive an associated response 905 from a plurality of management systems, an inventory management system 901 that may provide resource object attributes, a role management system 902 that may provide subject (or user) attributes (roles and entitlements), an identity management system 903 that may provide aggregated subject attributes, and log management system 904 that may provide information and events categorized by subject, a system event correlator 910 that may receive temporal events 921 categorized by subject, a risk correlation matrix to generate an integrity profile 920 for a subject that may comprise of at least a unique subject identifier and a reputation score.

[0070] FIG. 10 is a schematic diagram illustrating an exemplary method 1000 in accordance with various exemplary embodiments.

[0071] Referring to FIG. 10, the exemplary method 1000 may include a network endpoint assessment 1001 that may generate a network security scan report 1025, a endpoint collator 1002 to parse a plurality of received reports for categorization by address or geo-location, a normalizer 1003 for report consolidation, an object collator 1004 for categorization by package and component, an integrity processor 1011 on a

-22-

device 1017, for runtime system 1016, application 1015 and user 1014 context, a global object context generator 1005 for aggregation of context, an event processor 1006 for evaluation of context, a rules repository 1012 of object attributes that may include at least constraints 1023, a sample rate 1022, a recurrence 1021, a score 1020 and a weight 1019 for integrity assessments, an event correlator 1007, an event correlation matrix 1013, a threat classifier 1008, a dashboard controller 1009, and a remediation controller 1010.

[0072] In certain exemplary embodiments, a network endpoint assessment 1001 may perform a security scan of network endpoints for vulnerability, configuration, compliance and patch management and generate a security assessment report that may be received 1026 by the endpoint collator 1002 and sorted by endpoint address or geo-location. The categorized reports may be received 1028 by the object collator 1004 and sorted by object package and component.

[0073] In certain exemplary embodiments, the global object context generator 1005 may receive endpoint events 1018 that may include the local object execution context from the integrity processor 1011 on a device 1017, and temporal events 1029 that may include endpoint security context from the object collator 1004.

[0074] In certain exemplary embodiments, the event processor 1006 may receive endpoint integrity profiles 1030 from the global object context generator 1005, retrieve associated endpoint rules 1031 from the rules repository 1012, generate and send endpoint alerts 1033 to the event correlator 1007.

[0075] In certain exemplary embodiments, the event correlator 1007 may receive endpoint events 1033 from the event correlator 1007, map the alerts 1032 using the

-23-

event correlation matrix 1013, generate and send endpoint warnings 1034 to the threat classifier 1008.

[0076] In certain exemplary embodiments, the threat classifier 1008 may categorize threats, send status indications 1024 to the dashboard controller 1009 for real time visibility of endpoint integrity, and send action requests 1025 to the remediation controller 1010.

[0077] In certain exemplary embodiments, the endpoint collator 1002, normalizer 1003 and object collator 1004 may be included in the trust broker 841 as described in FIG. 8.

[0078] In certain exemplary embodiments, the global object context generator 1005 may be included in the system event correlator 843 described in FIG. 8.

[0079] In certain exemplary embodiments, the event processor 1006, event correlator 1007 and threat classifier 1008 may be included in the trust supervisor 846 as described in FIG. 8.

[0080] FIG. 11 is a schematic diagram illustrating an exemplary method 1100 in accordance with various exemplary embodiments.

[0081] Referring to FIG. 11, the exemplary method 1100 may include a user 1101 authenticated on a device 1102 through an authentication ceremony 1115 with an authentication service 1103, a service provider 1104 that may receive a service request, a managed application 1105 that may be the target service, a reputation broker 1106, a trust broker 1107, a log management system 1108, an identity (role) management system 1109, an inventory management system 1127, an reputation

-24-

processor 1110, a risk correlator 1111, a risk correlation matrix 1113 and a reputation score generator 1112.

[0082] In certain exemplary embodiments, a device 1102 may send a service request 1116 on behalf of a user 1101 to a service provider 1104 to access a managed application 1105. The service provider 1104 may send a reputation query 1117 to the reputation broker 1106, receive a reputation token 1118 that may include at least a reputation score for the user 1101 or device 1102, and enforce a reputation based access control 1119 to permit or deny the service request 1116 to access the managed application 1105.

[0083] In certain exemplary embodiments, the trust broker 1107 may receive a query 1120 for a reputation score for a subject (user or device), send a subject activity query 1121 to log management systems 1108, send a subject attribute query to identity (or role) management systems 1109, send a device attribute query to inventory management systems 1128, generate and send subject events 1123 to the event processor 1110.

[0084] In certain exemplary embodiments, the risk correlator 1111 may receive user alerts 1124 (or integrity profiles), use the risk correlation matrix 1113 to map user alerts to user warnings 1126, and use the reputation score generator 1112 to establish a user reputation score 1125 that may be included in the reputation token 1118 by the reputation broker 1106.

[0085] In certain exemplary embodiments, the reputation processor 1110 may be included in the system event correlator 843 described in FIG. 8.

-25-

[0086] In certain exemplary embodiments, the risk correlator 1111 may be included in the trust supervisor 846 described in FIG. 8.

[0087] FIG. 12 is a schematic diagram illustrating an exemplary method 1200 in accordance with various exemplary embodiments.

[0088] Referring to FIG. 12, the exemplary method 1200 may include an endpoint trust agent 1201 on a device 1202 that may execute an application 1203, a trust orchestrator 1205, a plurality of collaboration services 1207 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1230 that may include a network trust agent 1209 and an openflow security framework 1211, an openflow controller 1214, and an openflow enabled network element 1216 (for example, a switch or router).

[0089] In certain exemplary embodiments, the endpoint trust agent 1201 may send a dynamic context 1204 that may include the local execution context of an application 1203 to the trust orchestrator 1205 that may perform a calculus of risk on a global security context, that may include endpoint assessment reports 1206 received from collaboration services 1207, and send a system warning 1208 (endpoint threat intelligence) as a subscription based reputation service to a network trust agent 1209 for network flow remediation.

[0090] In certain exemplary embodiments, the network trust agent 1209 may send messages 1210 to the openflow security framework 1211 middleware to send directives 1213 to an openflow controller 1214, or send directives 1212 to an openflow controller 1214, to notify by means of a protocol 1215 an openflow enabled network element 1216 to apply access controls 1217 to block or divert traffic flows.

-26-

[0091] FIG. 13 is a schematic diagram illustrating an exemplary method 1300 in accordance with various exemplary embodiments.

[0092] Referring to FIG. 13, the exemplary method 1300 may include an endpoint trust agent 1301 on a mobile device 1202 that may execute a mobile application 1303, a trust orchestrator 1310, a plurality of collaboration services 1312 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1350 that may include a network trust agent 1315 and an network security framework 1318, a network element 1320 (for example, a switch or router), a wireless access point 1322, a mobile policy manager 1313 and a mobile device manager 1324.

[0093] In certain exemplary embodiments, the endpoint trust agent 1301 may send a dynamic context 1304 that may include the local execution context of a mobile application 1303 to the trust orchestrator 1310 that may perform a calculus of risk on a global security context, that may include endpoint assessment reports 1311 received from collaboration services 1312, and send threat intelligence as a subscription based reputation service 1314 to a network trust agent 1315 for network flow remediation.

[0094] In certain exemplary embodiments, the network trust agent 1315 may send messages 1316 to the network security framework 1318 middleware to send policies 1319 to a wireless access point 1320, or send policies 1317 to a wireless access point 1320, to apply access controls 1321 to block or divert traffic flows.

[0095] In certain exemplary embodiments, the trust orchestrator 1310 may send messages 1307 to the mobile policy manager 1313 to send directives 1308 to the

-27-

mobile device manager 1324 to set feature controls 1306 on the mobile device 1302 or send directives 1305 to the endpoint trust agent 1301 for the integrity processor 630 and runtime monitor 620 of FIG. 6.

[0096] FIG. 14 is a schematic diagram illustrating an exemplary data center administration console 1400 including an operational integrity dashboard 1450 in accordance with various exemplary embodiments of the invention.

[0097] Referring to FIG. 14, the exemplary data center administration console 1400 may visually display as a single pane of glass an operational integrity dashboard or display window 1450. The display window 1450 may include information fields including a global view of the data center inventory 1401 in a hierarchical tree view of resources, a component level view of a resource 1402, a resource name 1403, a resource platform type 1404, integrity metrics for a plurality of trust vectors that include at least the system configuration 1405, resource utilization 1406, application integrity 1407 and network activity 1408, a remediation action 1409, a remediation control 1410 that may include at least a restore, quarantine and divert users function, an action summary 1413, a details pane 1411, a status pane 1412, and color coded runtime integrity indicators 1440.

[0098] The information fields may be displayed and/or updated in real time or near real time. The color coded runtime integrity indicators 1440 for each displayed trust vector 1405, 1406, 1407 and 1408 may be animated with audio-visual effects (for example, blinking or beeping), and may be a hyperlinked graphic for a drill-down or detailed view.

-28-

[0099] Although the integrity dashboard 1450 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible. For example, additional trust vectors or a custom filter based perspective view may be displayed, or the dashboard may be embedded as a plug-in control and streamlined in a third party management console.

[00100] FIG. 15 is a schematic diagram illustrating an exemplary runtime operational integrity monitoring console 1500 including a system configuration dashboard 1550 in accordance with various exemplary embodiments of the invention.

[00101] Referring to FIG. 15, the exemplary runtime operational integrity monitoring console 1500 may visually display as a single pane of glass a system configuration dashboard or display window 1550. The display window 1550 may include information fields including a severity 1501, a warning or observed activity 1502, a timestamp 1503, an evaluation status 1504, a recommended action 1505, advanced details 1506 that may include a timestamp corresponding to the displayed threat details pane 1507, source location, threat identifier and victim identifier, threat details pane 1507, and machine history 1508 that may pertain to infection history.

[00102] The threat details pane 1507 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[00103] Although the system configuration dashboard 1550 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

-29-

[00104] FIG. 16 is a schematic diagram illustrating an exemplary runtime operational integrity monitoring console 1600 including a resource utilization dashboard 1650 in accordance with various exemplary embodiments of the invention.

[00105] Referring to FIG. 16, the exemplary runtime operational integrity monitoring console 1600 may visually display a resource utilization dashboard or display window 1650. The display window 1650 may include information fields including a severity 1601, a warning or observed activity 1602, a timestamp 1603, an evaluation status 1604, a recommended action 1605, advanced details 1606 that may include a timestamp corresponding to the displayed threat details pane 1607, source location, threat (or malware) identifier and victim identifier, threat details pane 1607, and machine history 1608 that may pertain to infection history.

[00106] The threat details pane 1607 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[00107] Although the resource utilization dashboard 1650 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[00108] FIG. 17 is a schematic diagram illustrating an exemplary runtime operational integrity monitoring console 1700 including an application integrity dashboard 1750 in accordance with various exemplary embodiments of the invention.

-30-

[00109] Referring to FIG. 17, the exemplary runtime operational integrity monitoring console 1700 may visually display an application integrity dashboard or display window 1750. The display window 1750 may include information fields including a severity 1701, a warning or observed activity 1702, a timestamp 1703, an evaluation status 1704, a recommended action 1705, advanced details 1706 that may include a timestamp corresponding to the displayed threat details pane 1707, source location, threat (or malware) identifier and victim identifier, threat details pane 1707, and machine history 1708 that may pertain to infection history.

[00110] The threat details pane 1707 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[00111] Although the application integrity dashboard 1750 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[00112] FIG. 18 is a schematic diagram illustrating an exemplary runtime operational integrity monitoring console 1800 including a network activity dashboard 1850 in accordance with various exemplary embodiments of the invention.

[00113] Referring to FIG. 18, the exemplary runtime operational integrity monitoring console 1800 may visually display a network activity dashboard or display window 1850. The display window 1850 may include information fields including a severity 1801, a warning or observed activity 1802, a timestamp 1803, an evaluation status 1804, a recommended action 1805, advanced details 1806 that may include a timestamp corresponding to the displayed threat details pane 1807, source location,

-31-

threat (or malware) identifier and victim identifier, threat details pane 1807, and machine history 1808 that may pertain to infection history.

[00114] The threat details pane 1807 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[00115] Although the network activity dashboard 1850 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[00116] FIG. 19 is a flowchart illustrating a method in accordance with various exemplary embodiments.

[00117] Referring to FIG. 19, the method 1900 may provide threat identification and remediation for an infected device 801 using a trust orchestrator 840, an endpoint trust agent 810, a network analyzer 830 and an endpoint assessment service 820.

[00118] At block 1901, the endpoint runtime monitor 620 may receive raw events 611 from the native device and/or platform instrumentation 610. At block 1902, the process monitor 514, included in the endpoint runtime monitor 620, may send image file and attributes 518 to the trust broker 532 at the trust orchestrator 840 for specialized image analysis. At block 1903, the trust broker 532 may validate the image file based on received image attributes. At block 1904, the trust broker 532 may send the received image file to the malware analyzer 540 for specialized static and dynamic image introspection. At block 1905, the trust broker 532 may generate and send, based on the received diagnosis, an image profile 519 to the endpoint

-32-

process monitor 514. At block 1906, the endpoint runtime monitor 620 may generate and send integrity events 621 to the integrity processor 630. At block 1907, the endpoint integrity processor 630 may process and map received events to alerts using rulesets 631. At block 1908, the endpoint integrity processor 630 may generate and send warnings 634 using an event correlation matrix 633 to the trust orchestrator 840 as endpoint events 635. At block 1909, the system event correlator 640 may receive endpoint events 635 from the endpoint integrity processor 630. At block 1910, the trust broker 841 may receive network endpoint integrity measurement and verification reports 821 from an endpoint assessment service 820. At block 1911, the system event correlator 640 may receive temporal events 842 from the trust broker 841. At block 1912, the system event correlator 640 may correlate the received endpoint and temporal events and generate an integrity profile 844 for the device 801. At block 1913, the system event correlator 640 may send an integrity profile 844 of the device 801 to the trust supervisor 846. At block 1914, the network activity correlator 831 may send infection profiles 831 to the trust supervisor 846. At block 1915, the trust supervisor 846 may process the received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification on the device 801. At block 1916, the trust supervisor 846 may send to the remediation controller 848 actions 847 to perform on the infected device 801. At block 1917, the remediation controller 848 may process the received action request on the infected device 801 and send directives 849 based on configured thresholds and triggers to system orchestration and policy enforcement point (or network security) services 860.

-33-

[00119] FIG. 20 is a flowchart illustrating a method in accordance with various exemplary embodiments.

[00120] Referring to FIG. 20, the method 2000 may provide a user reputation service for a service provider 1104 using a trust orchestrator 840, an endpoint trust agent 810, a network analyzer 830 and an endpoint assessment service 820.

[00121] At block 2001, the endpoint runtime monitor 620 may receive raw events 611 from the native device and/or platform instrumentation 610, detect and identify the user 1101 authenticated by the authentication service 1103 at the device 1102. At block 2002, the endpoint runtime monitor 620 may receive user activity events from the native device and/or platform instrumentation 610. At block 2003, the endpoint runtime monitor 620 may generate and send integrity events 621 to the endpoint integrity processor 630. At block 2004, the endpoint integrity processor 630 may process and map received events to alerts using rulesets 631. At block 2005, the endpoint integrity processor 630 may generate and send warnings 634 using an event correlation matrix 633 to the trust orchestrator 840 as endpoint events 635. At block 2006, the trust broker 1107 may query and receive user and resource attributes 1121, 1122, 1128 from a plurality of collaboration services 1108, 1109, 1127 and generate subject events 1123. At block 2007, the reputation processor 1110 may analyze received subject events 1123 and generate user alerts (or integrity profiles) 1124. At block 2008, the risk correlator 1111 may correlate received user alerts 1124 to generate user warnings 1126 using the risk correlation matrix 1113, and user reputation score 1125 using the reputation score generator 1112. At block 2009, the trust supervisor 846 may process the received integrity and

-34-

infection profiles for classification of warnings based on forensic confidence for threat identification of user 1101 on the device 1102.

[00122] At block 2010, the reputation broker 1106 may receive a reputation query 1117 for a user 1101 on a device 1102 from a service provider 1104. At block 2011, the reputation broker 1106 may send a reputation token 1118 for the user 1101 on the device 1102 that may include at least a user reputation score 1125. At block 2012, the service provider 1104 may apply a reputation based access control 1119 in processing a service request 1116 received from the device 1102 for the user 1101 to access a managed application 1105.

[00123] At block 2013, the trust supervisor 846 may send to the remediation controller 848 actions 847 to perform on the network fabric for sessions of user 1101 on device 1102. At block 2014, the remediation controller 848 may process received action request for sessions of user 1101 on device 1102 and send directives 849 based on configured thresholds and triggers to system orchestration and policy enforcement point (network security) services 860.

[00124] FIG. 21 is a flowchart illustrating a method in accordance with various exemplary embodiments.

[00125] Referring to FIG. 21, the method 2100 may provide network flow level remediation for an infected device 1202 at a network element 1216 using a trust orchestrator 1205, an endpoint trust agent 1201, a network trust agent 1209 and an collaboration services 1207.

[00126] At block 2101, the endpoint runtime monitor 620 at the endpoint trust agent 1201 on the device 1202 may send a dynamic context 1204 that may include

-35-

endpoint events 635 to the trust orchestrator 1205. At block 2102, the trust orchestrator 840 may analyze received endpoint events 635 from the endpoint trust agent 1201 on the device 1202. At block 2103, the trust broker 841 may receive and analyze network endpoint assessments (or integrity measurement and verification reports) 821 from an endpoint assessment service (or collaboration services) 820 and generate temporal events 842. At block 2104, the system event correlator 843 may correlate endpoint 811 and temporal 842 events and generate an integrity profile 844 for the device 1202. At block 2105, the trust supervisor 846 may generate and send to the remediation controller 848 flow remediation actions 847 to perform on the network fabric. At block 2106, the remediation controller 848 at the trust orchestrator 1205 may send to the network trust agent 1209 a system warning 1208 for the network device 1202. At block 2107, the network trust agent 1209 may generate and send to the openflow security framework 1211 directives 1210 to formulate commands 1213 for the openflow controller 1214. At block 2108, the openflow controller 1214 may send rules 1215 to the openflow enabled network element (switch) 1216 to divert or block traffic flows to/from the forewarned network device 1202. At block 2109, the openflow enabled network element (switch) 1216 may enforce received access restrictions (controls) 1217 for the forewarned network device 1202. At block 2110, the trust supervisor 846 may monitor and send reputation score updates 847 for the forewarned network device 1202 to the remediation controller 848. At block 2111, the remediation controller 848 at the trust orchestrator 1205 may send system security posture status updates 1208 for the forewarned network device 1202 to the network trust agent 1209. At block 2112, the

-36-

network trust agent 1209 may generate and send to the openflow security framework 1211 directives 1210 to formulate commands 1213 for the openflow controller 1214 to restore normal flows to/from the forewarned network device 1202.

[00127] FIG. 22 is a flowchart illustrating a method in accordance with various exemplary embodiments.

[00128] Referring to FIG. 22, the method 2200 may provide network flow level remediation for an infected mobile device 1302 at a wireless access point 1320 using a trust orchestrator 1310, an endpoint trust agent 1301, a network trust agent 1315 and an endpoint assessment service 1312.

[00129] At block 2201, the endpoint runtime monitor 620 at the endpoint trust agent 1301 on the mobile device 1302 may send a dynamic context 1304 that may include endpoint events 635 to the trust orchestrator 1310. At block 2202, the trust orchestrator 840 may analyze received endpoint events 635 from the endpoint trust agent 1301 on the mobile device 1302. At block 2203, the trust broker 841 may receive and analyze network endpoint assessments (or integrity measurement and verification reports) 821 from an endpoint assessment service (or collaboration services) 820 and generate temporal events 842. At block 2204, the system event correlator 843 may correlate endpoint 811 and temporal 842 events and generate an integrity profile 844 for the mobile device 1302. At block 2205, the trust supervisor 846 may generate and send to the remediation controller 848 flow remediation actions 847 to perform on the network fabric.

[00130] At block 2206, the remediation controller 848 at the trust orchestrator 1310 may send to the network trust agent 1209 a system warning 1208 for the mobile

-37-

device 1302. At block 2207, the network trust agent 1209 may generate and send to the wireless access point 1320 policies 1317 to apply access controls 1321 for the mobile device 1302.

[00131] At block 2208, the remediation controller 848 at the trust orchestrator 1310 may send to the mobile policy manager 1313 a system warning 1307 for the mobile device 1302. At block 2209, the mobile policy manager 1313 may generate and send to the mobile device manager 1324 directives 1309 to formulate advisories and security settings for the registered user (service subscriber) and the mobile device 1302.

[00132] At block 2210, the reputation broker 1106 may receive a reputation query 1117 for a mobile device 1302 from a service provider 1104. At block 2211, the reputation broker 1106 may send a reputation token 1118 for the device 1302 that may include at least a security posture established by the trust supervisor 846 based on the received infection 832 and integrity 844 profiles for the device 1302. At block 2212, the service provider 1104 may apply a reputation based access control 1119 in processing a service request 1116 received from the device 1302 to access a managed application 1105.

[00133] Although exemplary embodiments have been described in terms of a computing device or instrumented platform, it is contemplated that it may be implemented in software on microprocessors/general purpose computers such as the computer system 2300 illustrated in FIG. 23. In various embodiments, one or more of the functions of the various components may be implemented in software

-38-

that controls a computing device, such as computer system 2300, which is described below with reference to FIG. 23.

[00134] Aspects of the present invention shown in FIGS. 1-22, or any part(s) or function(s) thereof, may be implemented using hardware, software modules, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems.

[00135] FIG. 23 illustrates an example computer system 2300 in which embodiments of the present invention, or portions thereof, may be implemented as computer-readable code. For example, network systems ? of FIGS. ?-?, can be implemented in computer system 2300 using hardware, software, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Hardware, software, or any combination of such may embody any of the modules and components used to implement the network systems 100, 400, 500, 600, 800, 900, 1000, 1100, 1200, 1300 of FIGS. 1, 4-6, 8-13.

[00136] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. One of ordinary skill in the art may appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device.

-39-

[00137] For instance, at least one processor device and a memory may be used to implement the above described embodiments. A processor device may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor “cores.”

[00138] Various embodiments of the invention are described in terms of this example computer system 2300. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[00139] Processor device 2304 may be a special purpose or a general purpose processor device. As will be appreciated by persons skilled in the relevant art, processor device 2304 may also be a single processor in a multi-core/multiprocessor system, such system operating alone, or in a cluster of computing devices operating in a cluster or server farm. Processor device 2304 is connected to a communication infrastructure 2306, for example, a bus, message queue, network, or multi-core message-passing scheme.

[00140] Computer system 2300 also includes a main memory 2308, for example, random access memory (RAM), and may also include a secondary memory 2310. Secondary memory 2310 may include, for example, a hard disk drive 2312,

-40-

removable storage drive 2314. Removable storage drive 2314 may comprise a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, or the like.

[00141] The removable storage drive 2314 reads from and/or writes to a removable storage unit 2318 in a well known manner. Removable storage unit 2318 may comprise a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 2314. As will be appreciated by persons skilled in the relevant art, removable storage unit 2318 includes a non-transitory computer usable storage medium having stored therein computer software and/or data.

[00142] In alternative implementations, secondary memory 2310 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 2300. Such means may include, for example, a removable storage unit 2322 and an interface 2320. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 2322 and interfaces 2320 which allow software and data to be transferred from the removable storage unit 2322 to computer system 2300.

[00143] Computer system 2300 may also include a communications interface 2324. Communications interface 2324 allows software and data to be transferred between computer system 2300 and external devices. Communications interface 2324 may include a modem, a network interface (such as an Ethernet card), a

-41-

communications port, a PCMCIA slot and card, or the like. Software and data transferred via communications interface 2324 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals capable of being received by communications interface 2324. These signals may be provided to communications interface 2324 via a communications path 2326. Communications path 2326 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link or other communications channels.

[00144] In this document, the terms “computer program medium,” “non-transitory computer readable medium,” and “computer usable medium” are used to generally refer to media such as removable storage unit 2318, removable storage unit 2322, and a hard disk installed in hard disk drive 2312. Signals carried over communications path 2326 can also embody the logic described herein. Computer program medium and computer usable medium can also refer to memories, such as main memory 2308 and secondary memory 2310, which can be memory semiconductors (e.g. DRAMs, etc.). These computer program products are means for providing software to computer system 2300.

[00145] Computer programs (also called computer control logic) are stored in main memory 2308 and/or secondary memory 2310. Computer programs may also be received via communications interface 2324. Such computer programs, when executed, enable computer system 2300 to implement the present invention as discussed herein. In particular, the computer programs, when executed, enable processor device 2304 to implement the processes of the present invention, such as the stages in the methods illustrated by the flowcharts 1900, 2000, 2100, 2200 of

-42-

FIGS. 19-22, discussed above. Accordingly, such computer programs represent controllers of the computer system 2300. Where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 2300 using removable storage drive 2314, interface 2320, and hard disk drive 2312, or communications interface 2324.

[00146] Embodiments of the invention also may be directed to computer program products comprising software stored on any computer useable medium. Such software, when executed in one or more data processing device, causes a data processing device(s) to operate as described herein. Embodiments of the invention employ any computer useable or readable medium. Examples of computer useable mediums include, but are not limited to, primary storage devices (e.g., any type of random access memory), secondary storage devices (e.g., hard drives, floppy disks, CD ROMS, ZIP disks, tapes, magnetic storage devices, and optical storage devices, MEMS, nanotechnological storage device, etc.), and communication mediums (e.g., wired and wireless communications networks, local area networks, wide area networks, intranets, etc.).

[00147] It is to be appreciated that the Detailed Description section, and not the Summary and Abstract sections, is intended to be used to interpret the claims. The Summary and Abstract sections may set forth one or more but not all exemplary embodiments of the present invention as contemplated by the inventor(s), and thus, are not intended to limit the present invention and the appended claims in any way.

[00148] Embodiments of the present invention have been described above with the aid of functional building blocks illustrating the implementation of specified functions

-43-

and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

[00149] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

[00150] Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range equivalents of the claims and without departing from the invention.

-44-

What is claimed is:

1. A method of providing an attestation service for runtime operational integrity of systems executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server, comprising:
2. A method of providing an attestation service for the reputation of a user executing on a computing platform using an endpoint trust agent and trust orchestration server, comprising:
3. A method of providing network flow remediation to isolate infected systems executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server, comprising:
4. A method of providing service providers with runtime operational integrity of mobile devices executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server, comprising:
5. A method of providing a data center level runtime operational integrity dashboard and remediation controls for systems executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server, comprising:

ABSTRACT OF THE DISCLOSURE

An instrumented network, machine and platform having a target application or user thereon is disclosed. A security orchestration service may generate runtime operational integrity profiles having associated therewith forensic evidence statements having at least one of a plurality of risk assertions describing the examined runtime local execution and introspection based derived security context. The forensic statements may represent a level threat identification or contextual trustworthiness, at near real time, of a subject (device, application or user), on the instrumented target platform. A runtime device (platform) and network monitor may examine the local execution context of the target subject, and a plurality of security services may be queried for external intelligence of the subject. A physical or logical network flow controller may regulate access of the target subject to a protected resource (device or application), or initiate preventive intervention (remediation actions) on the target subject, based on a dynamic forensic statement issued by the security orchestration service.

FIG. 1

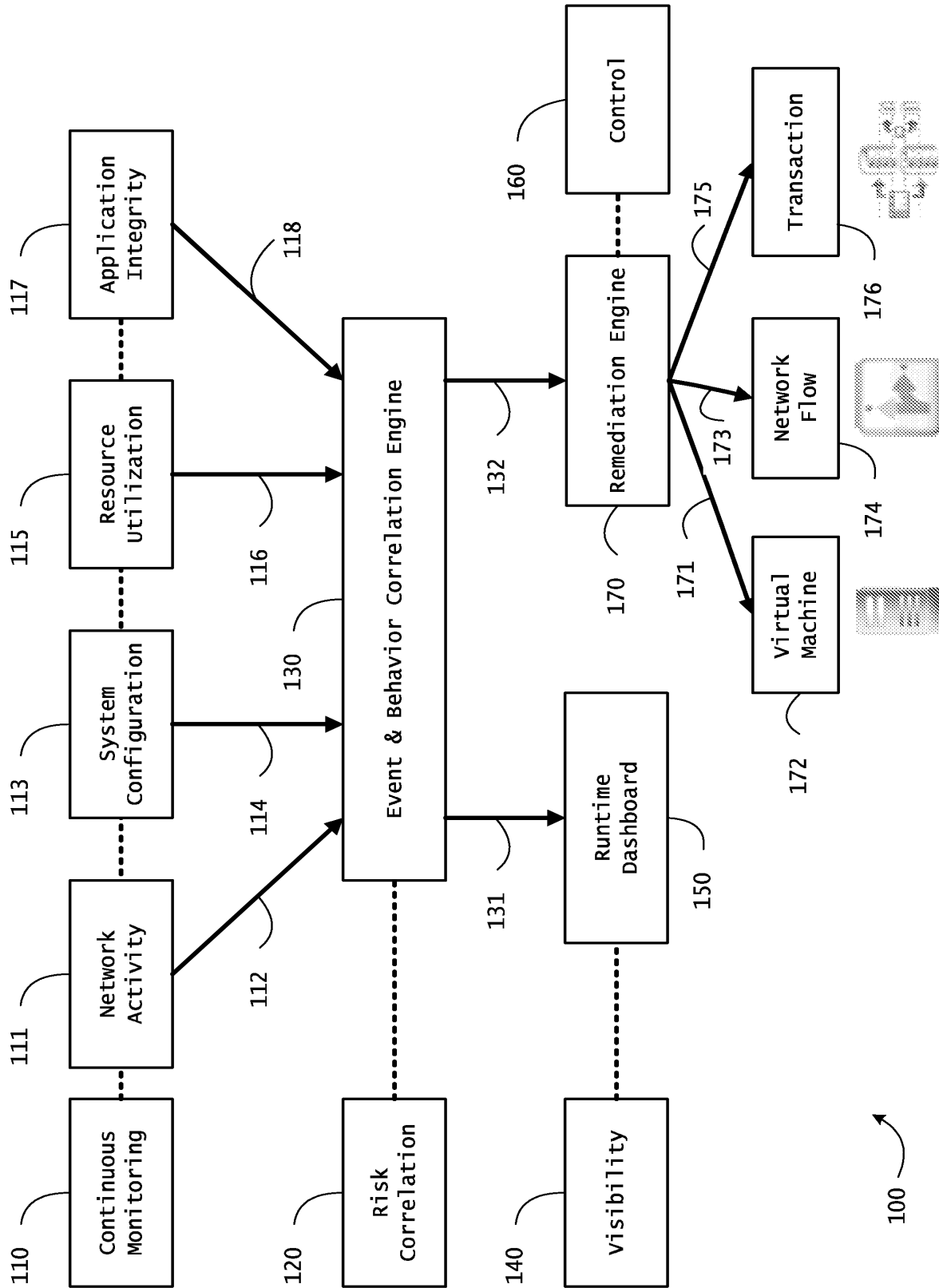


FIG. 2

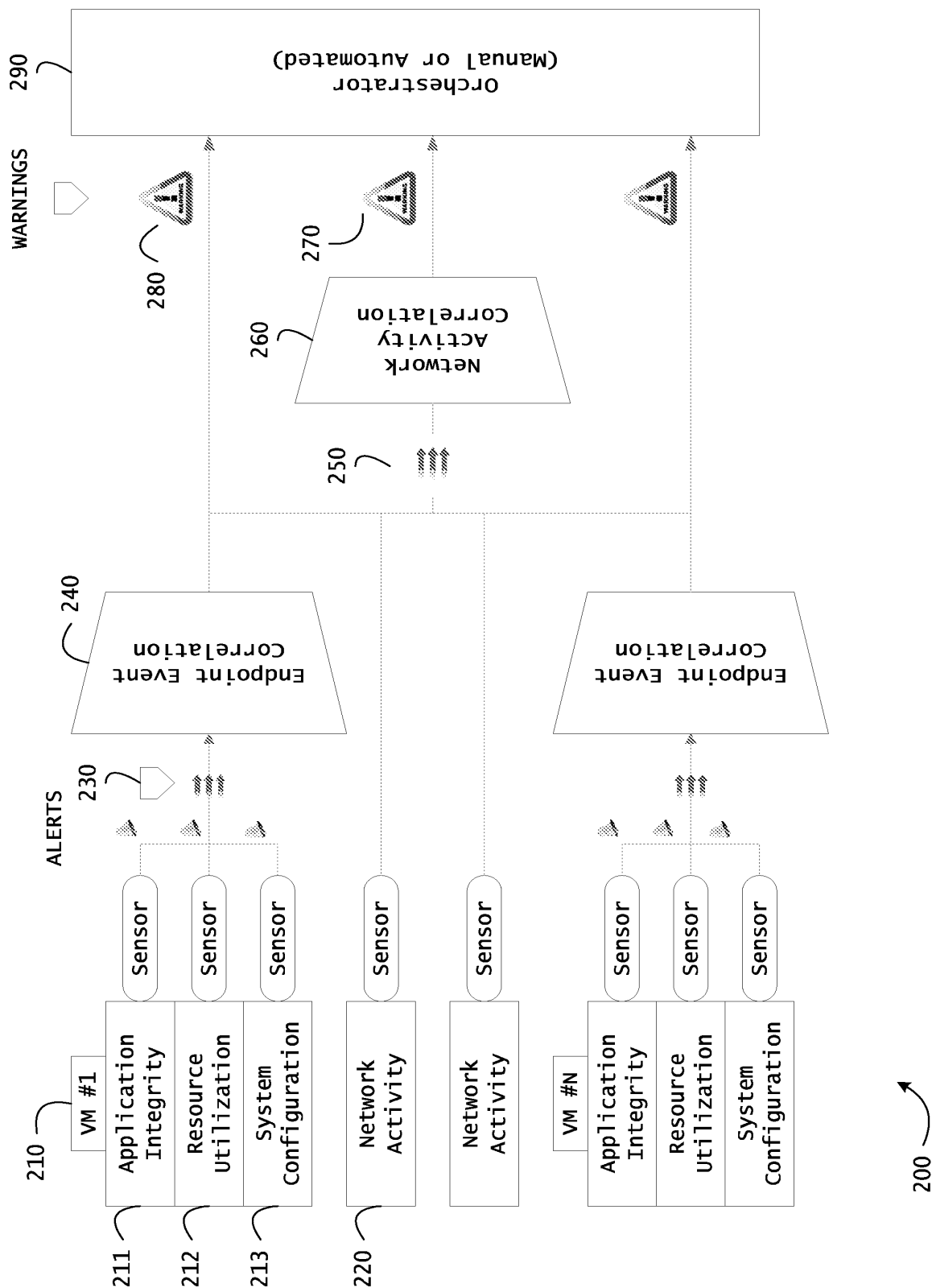


FIG. 3A

300

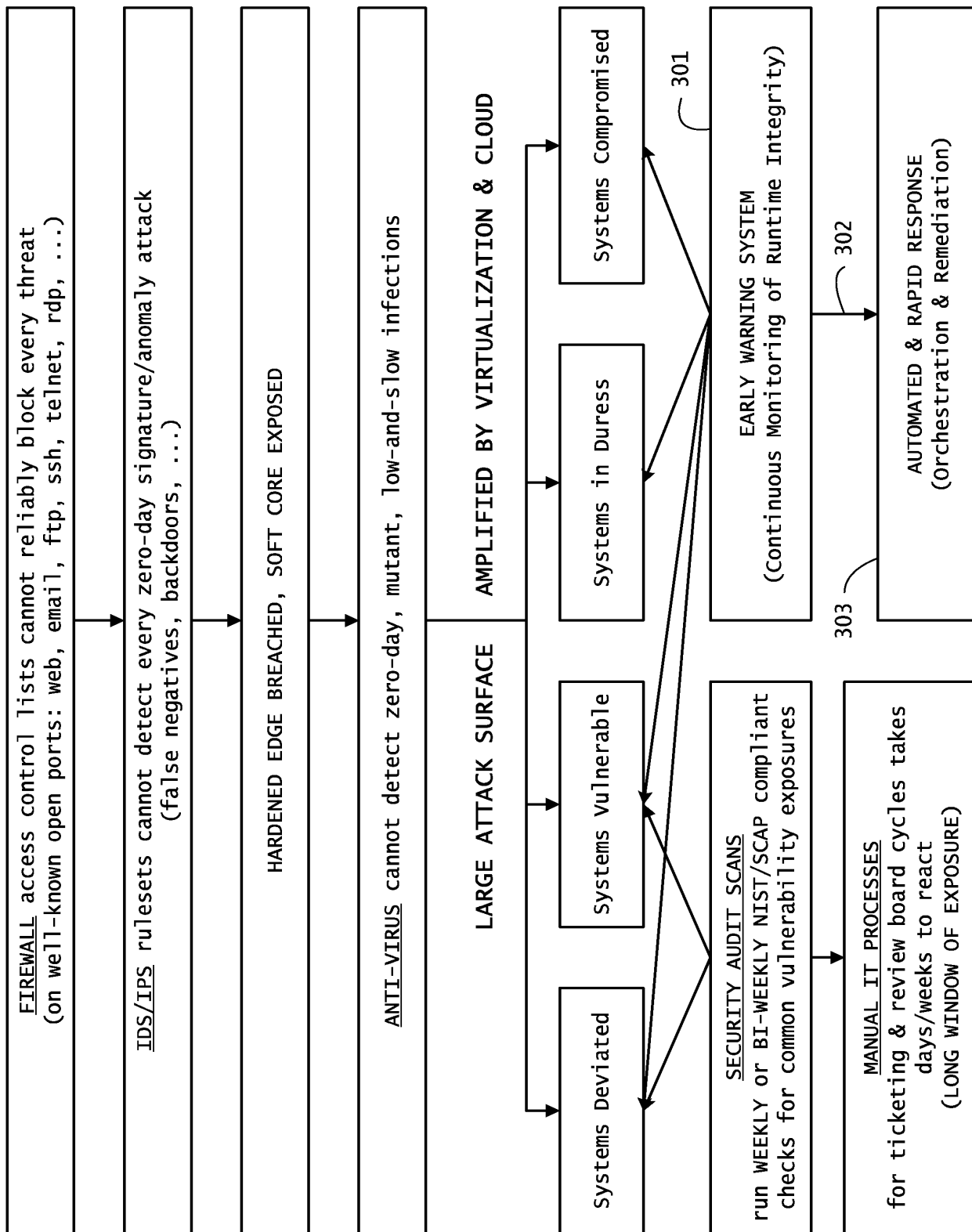


FIG. 3B

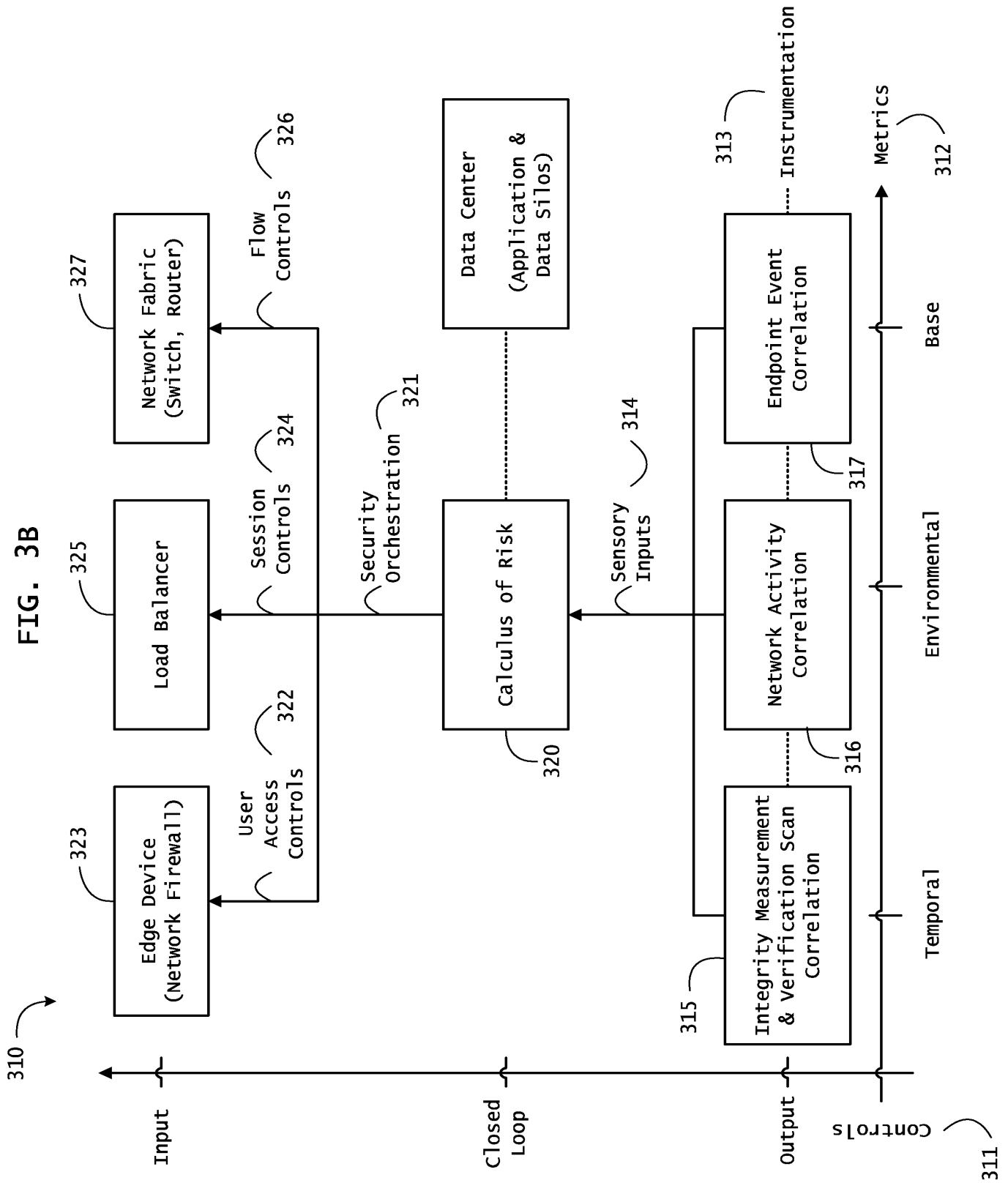


FIG. 4

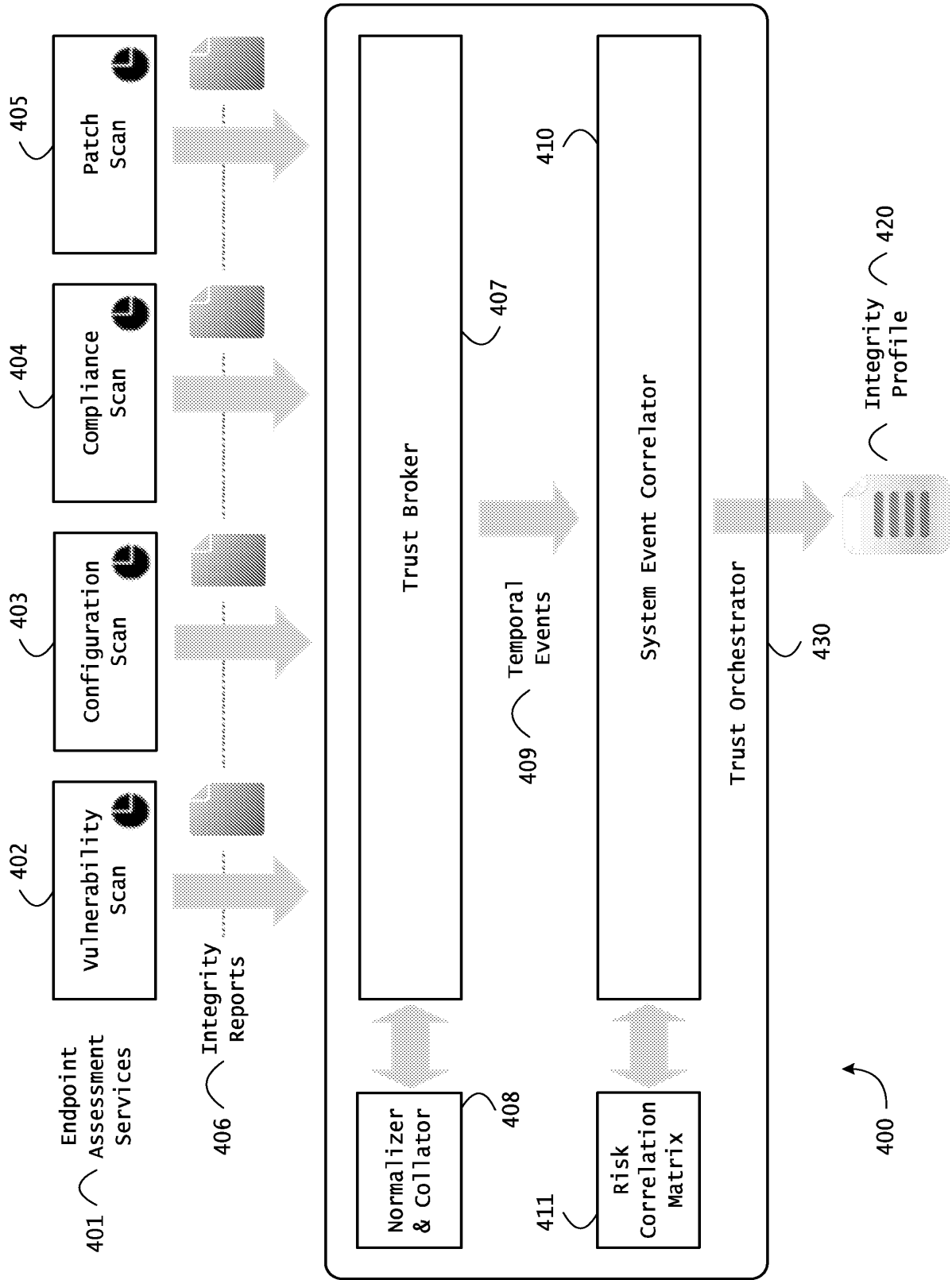


FIG. 5

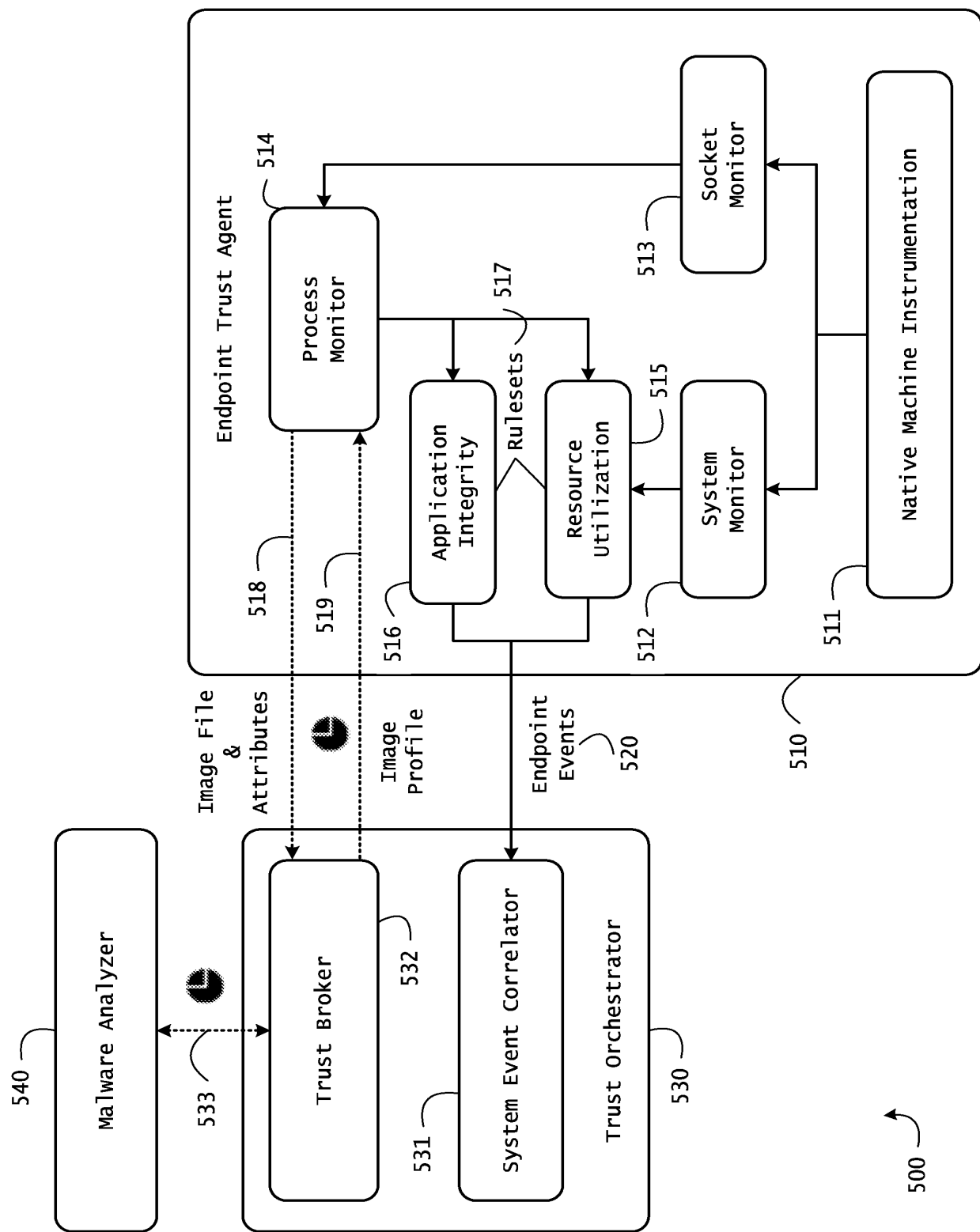


FIG. 6

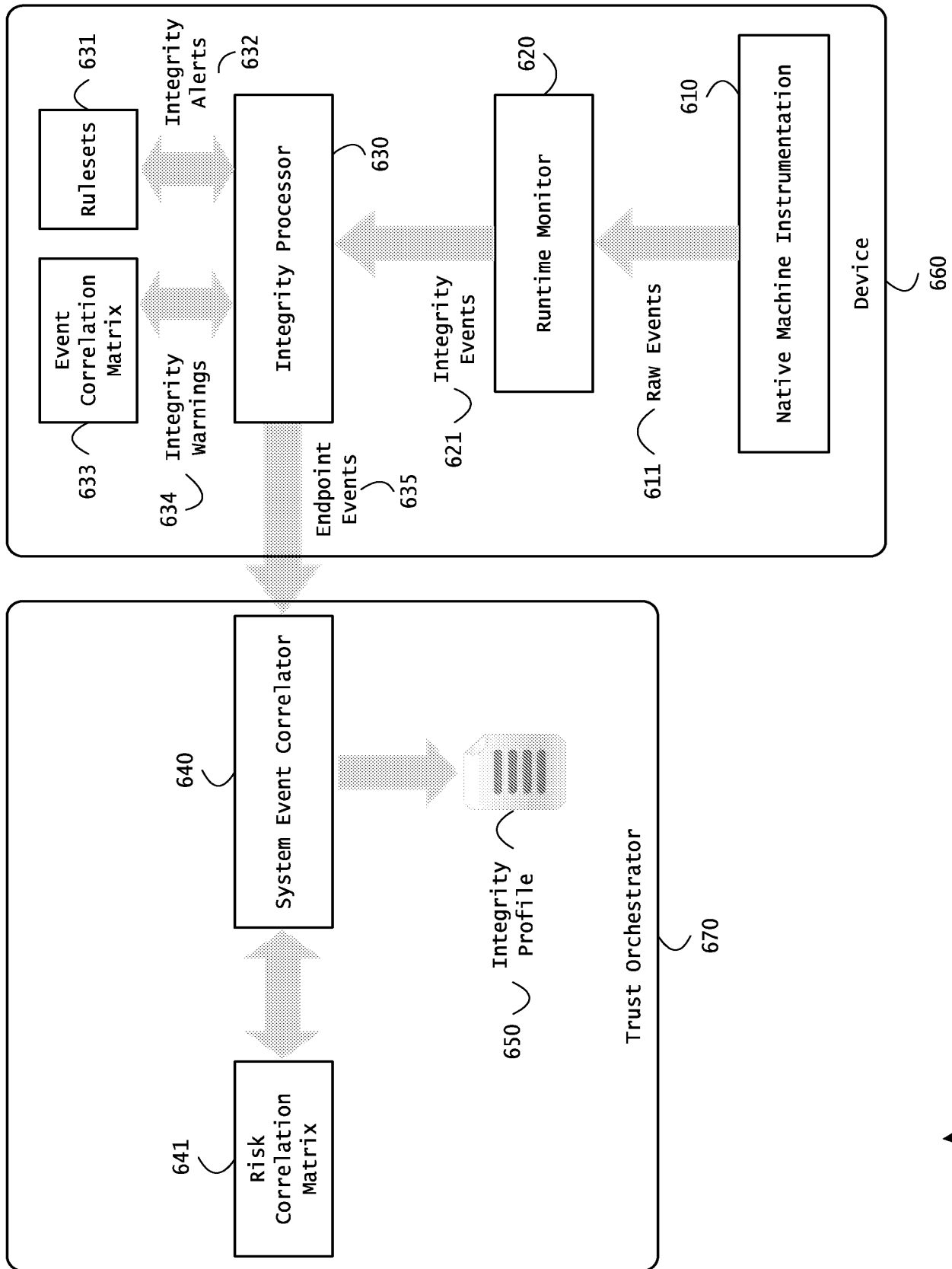


FIG. 7A

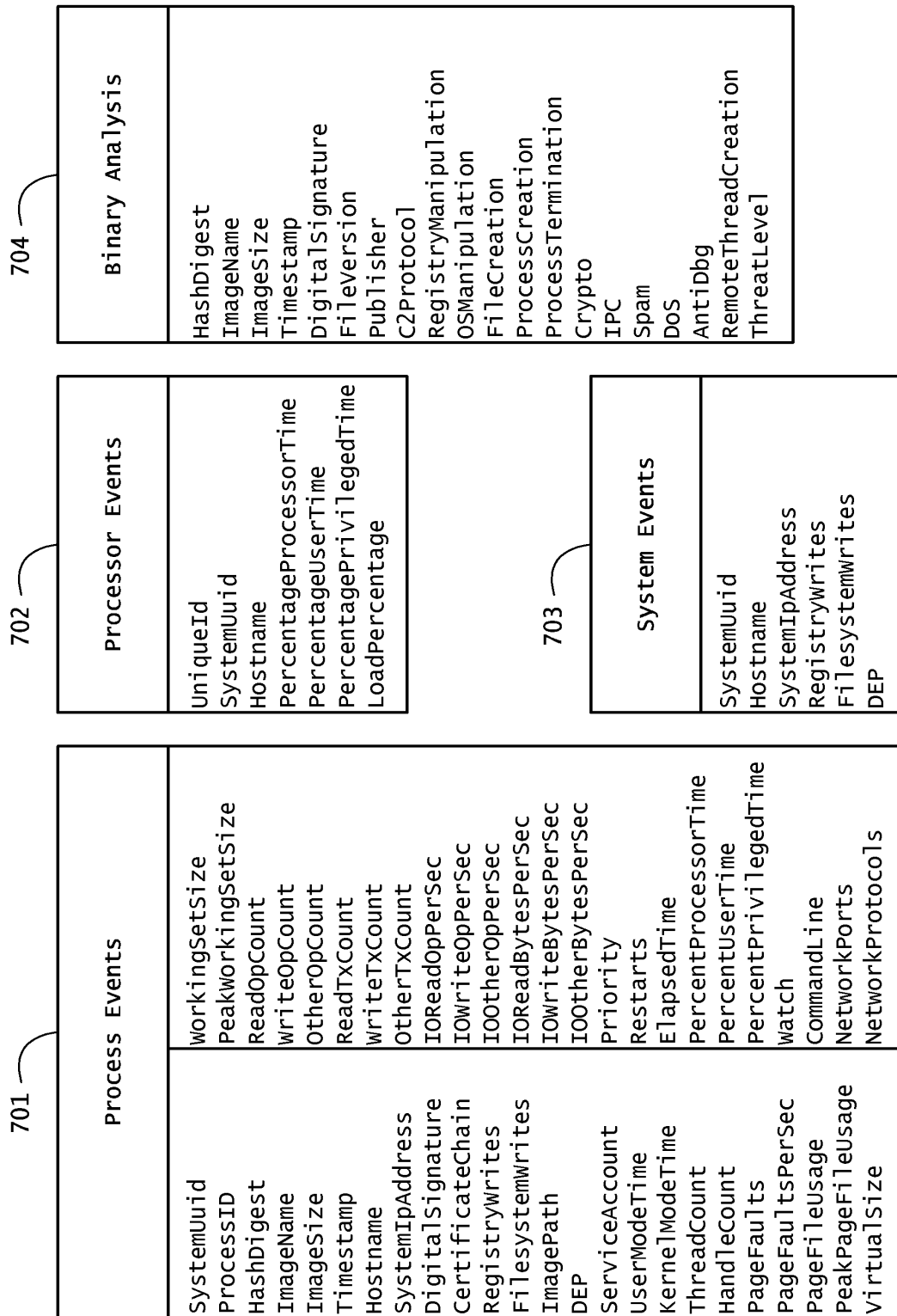


FIG. 7B

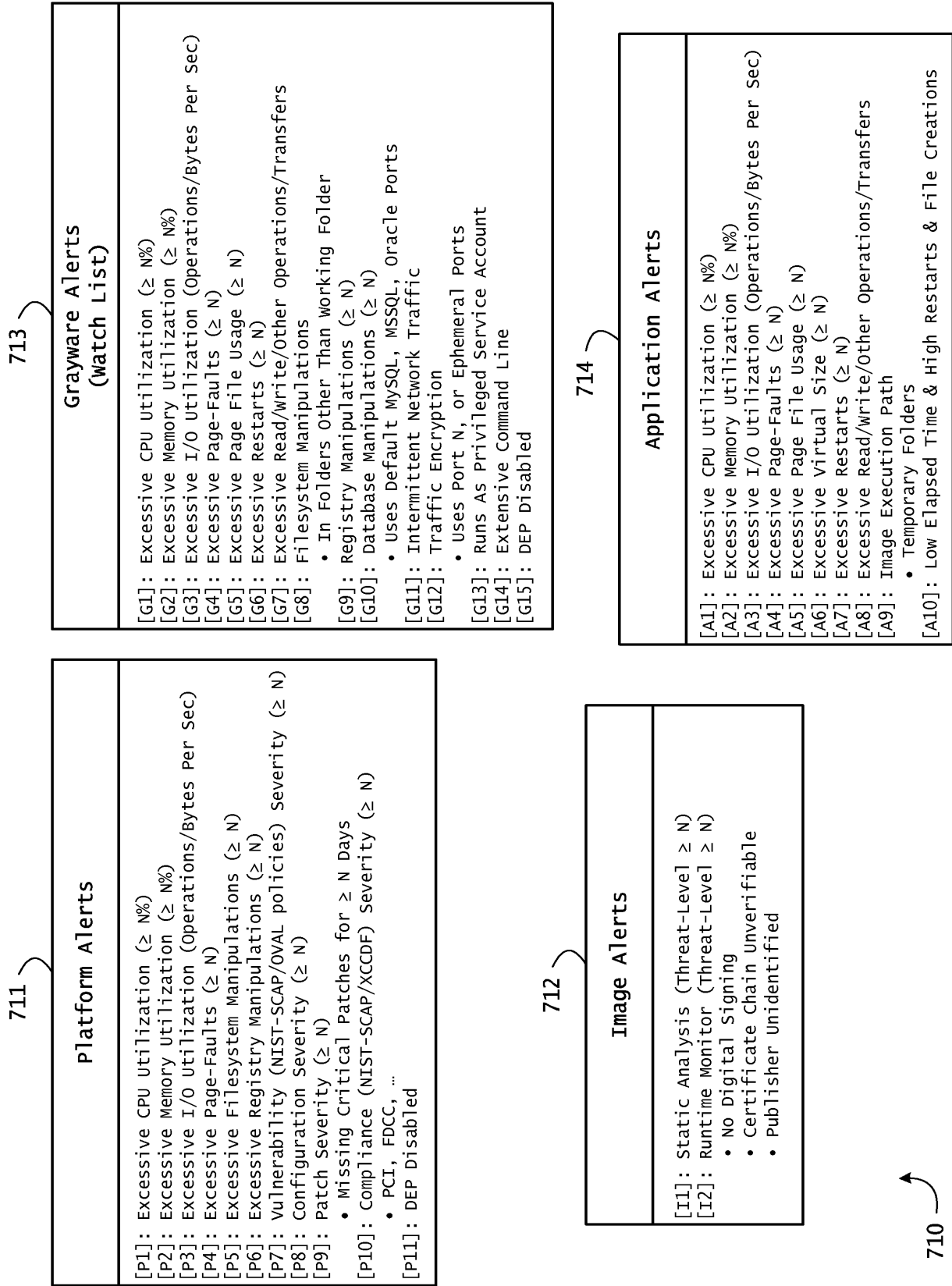
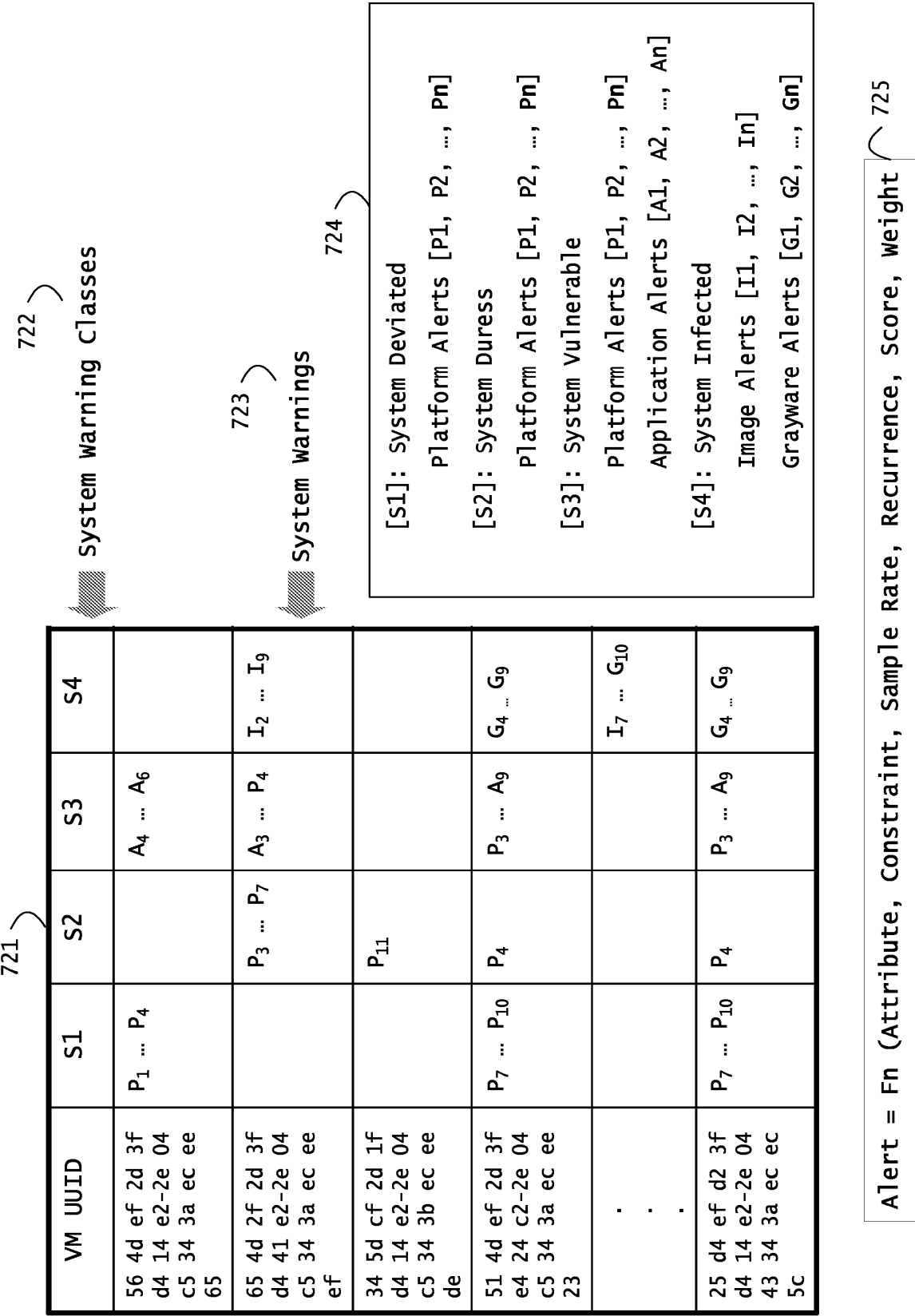


FIG. 7C



720

FIG. 8

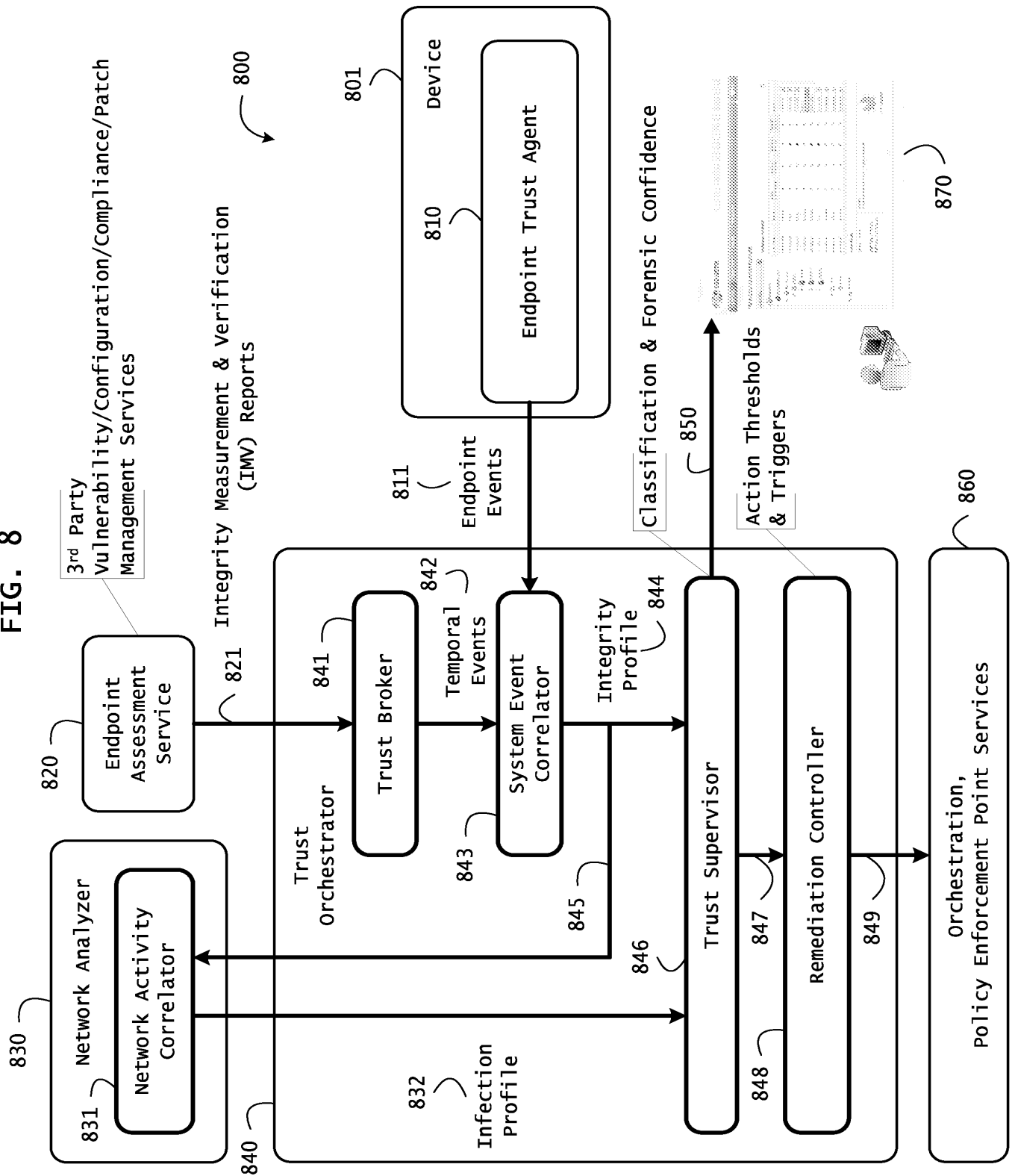
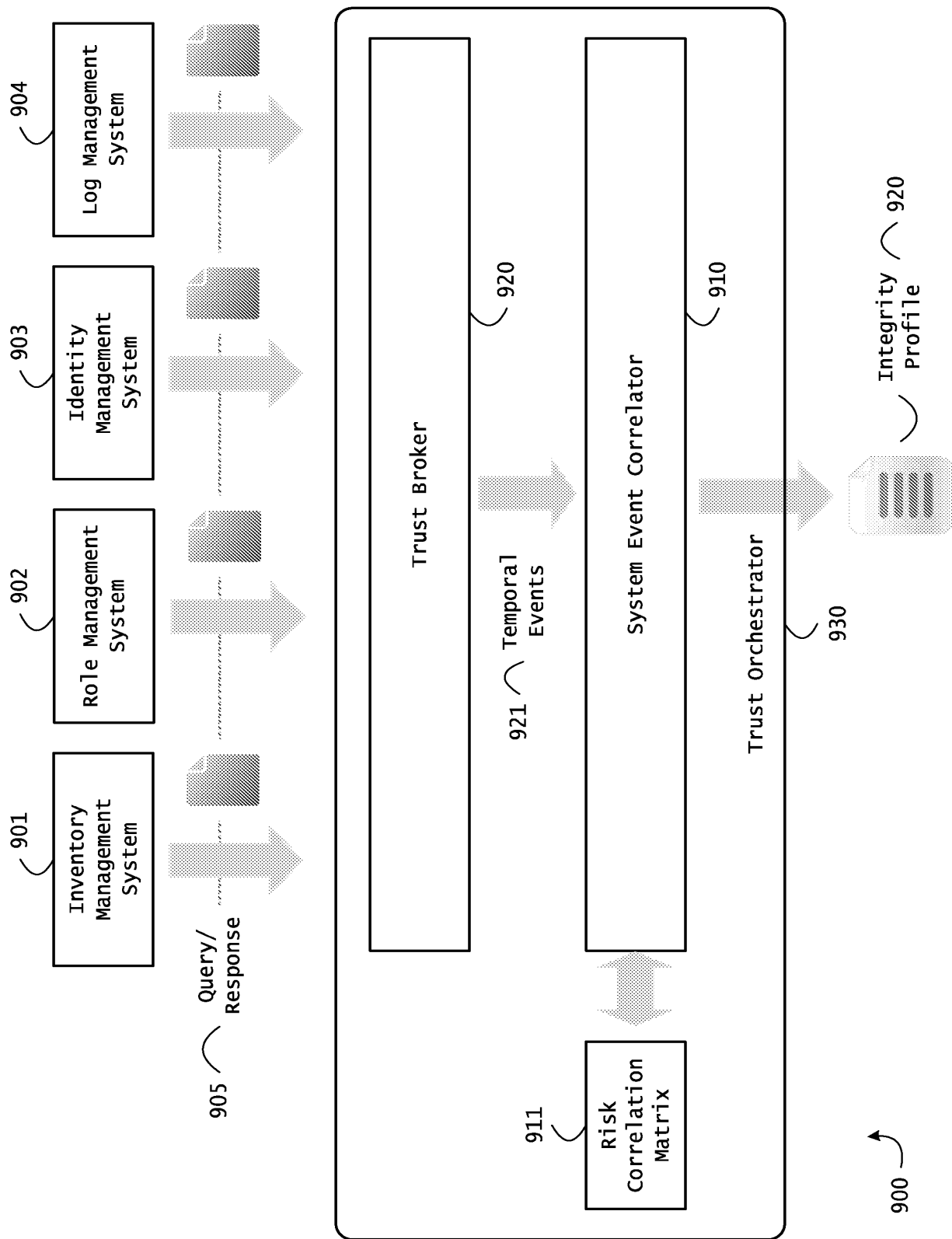


FIG. 9



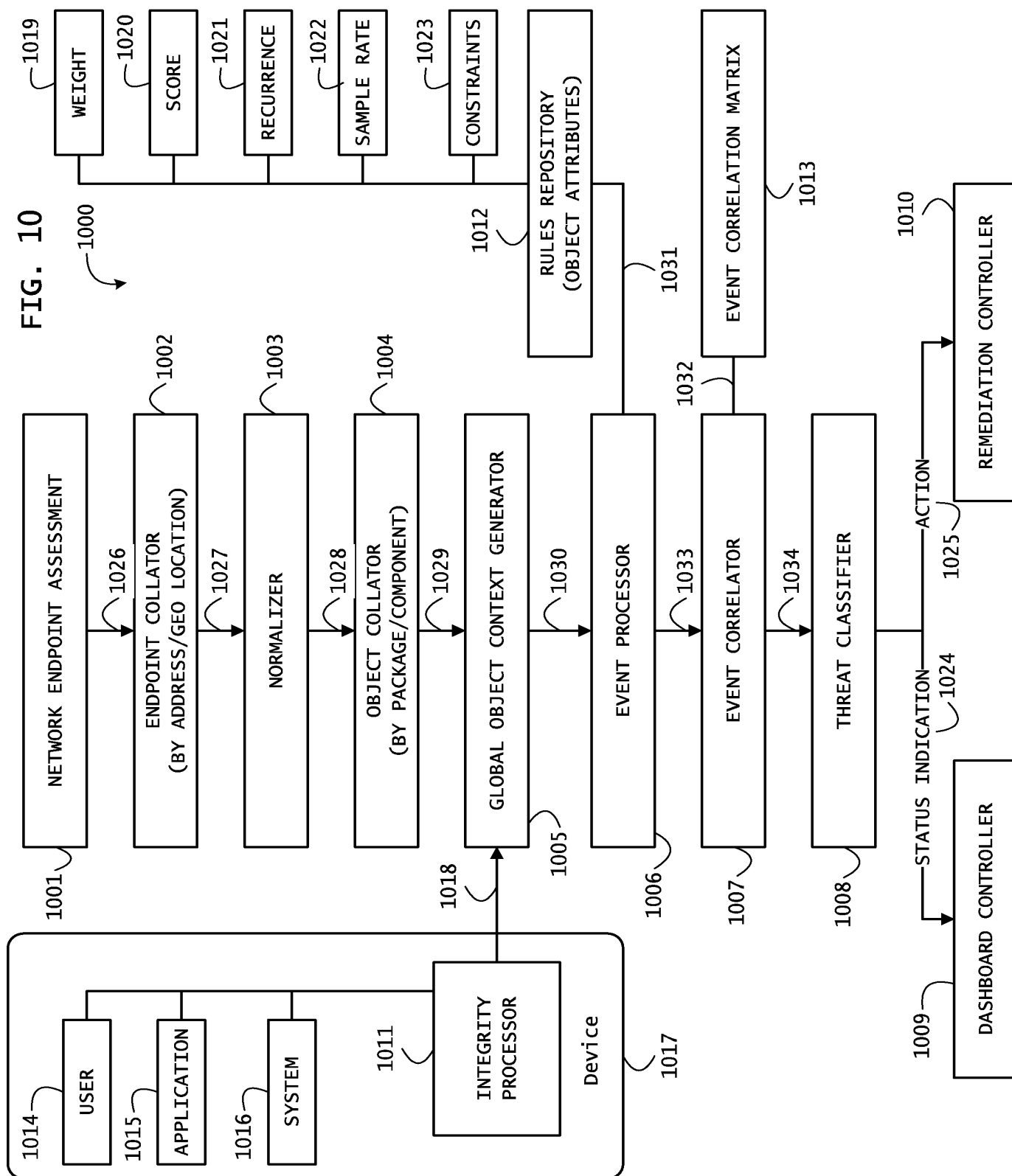


FIG. 11

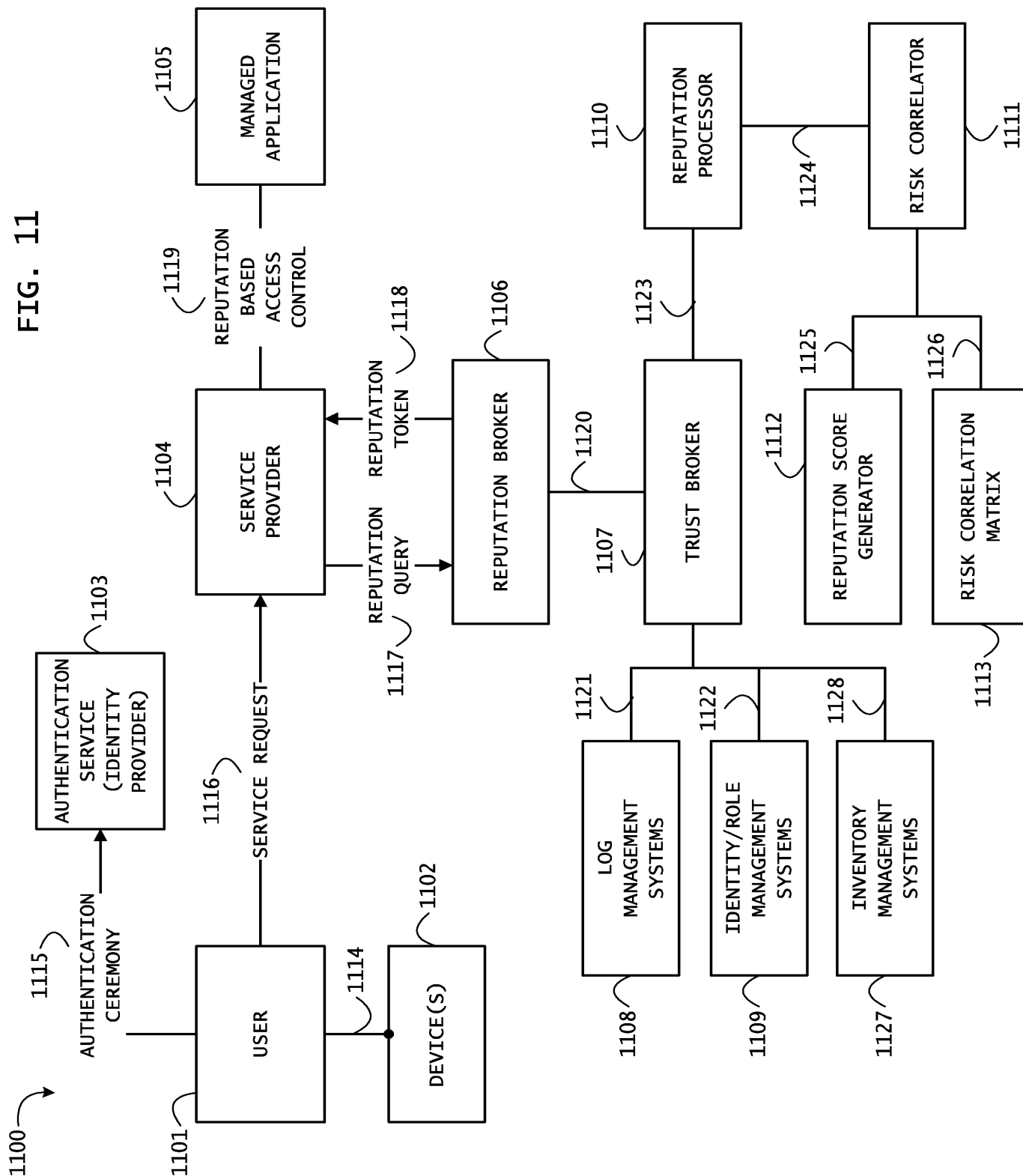
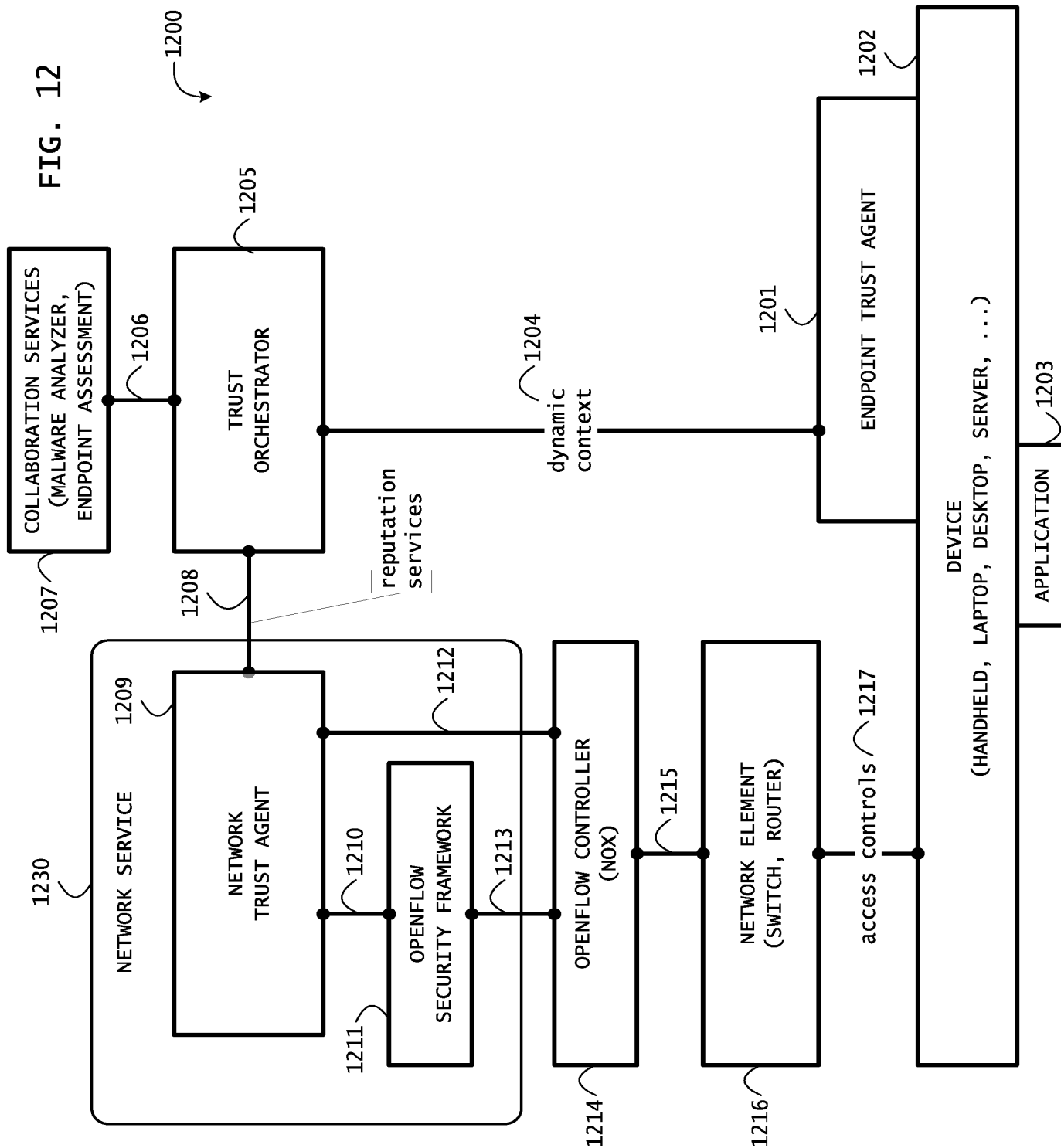


FIG. 12



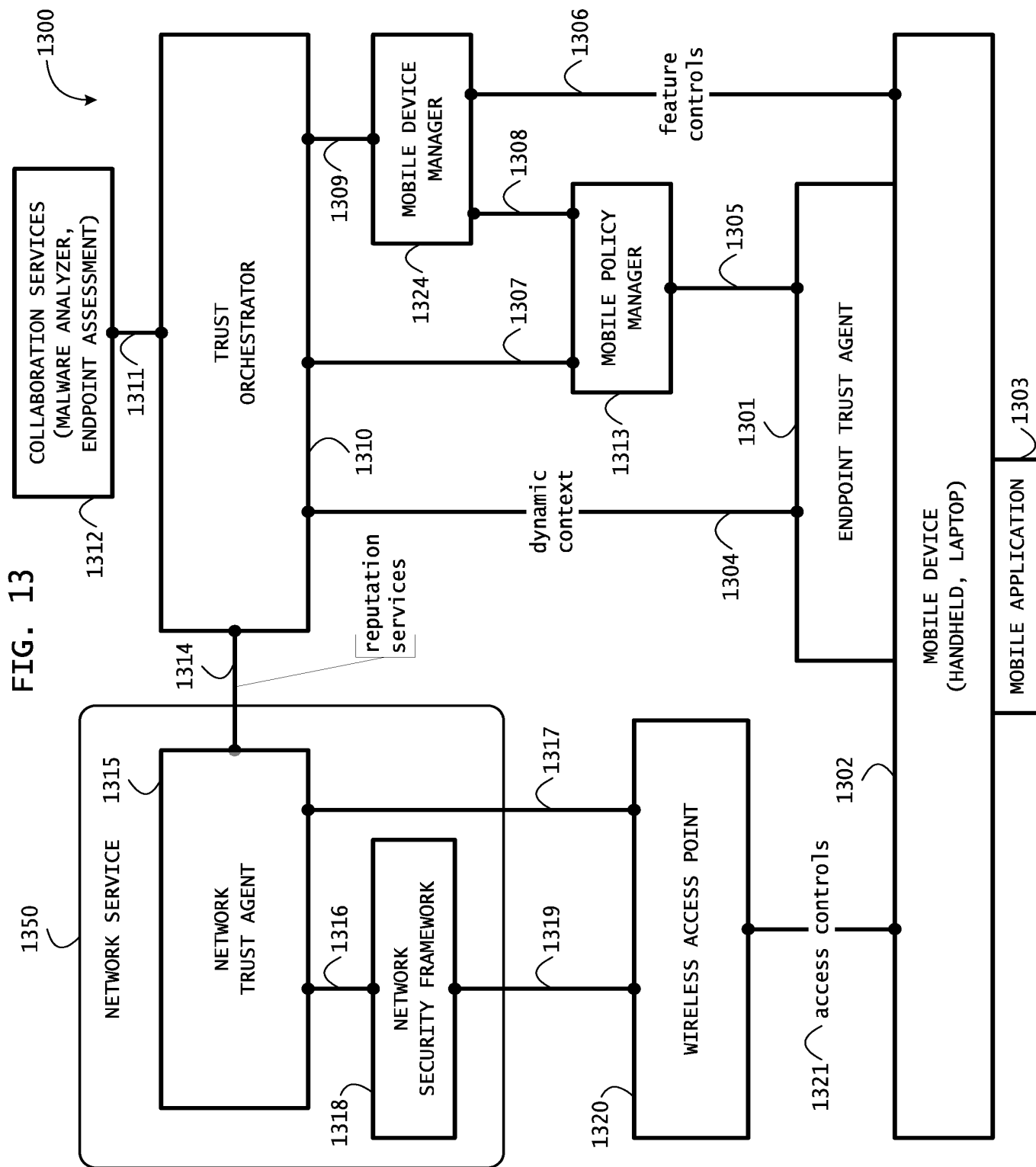


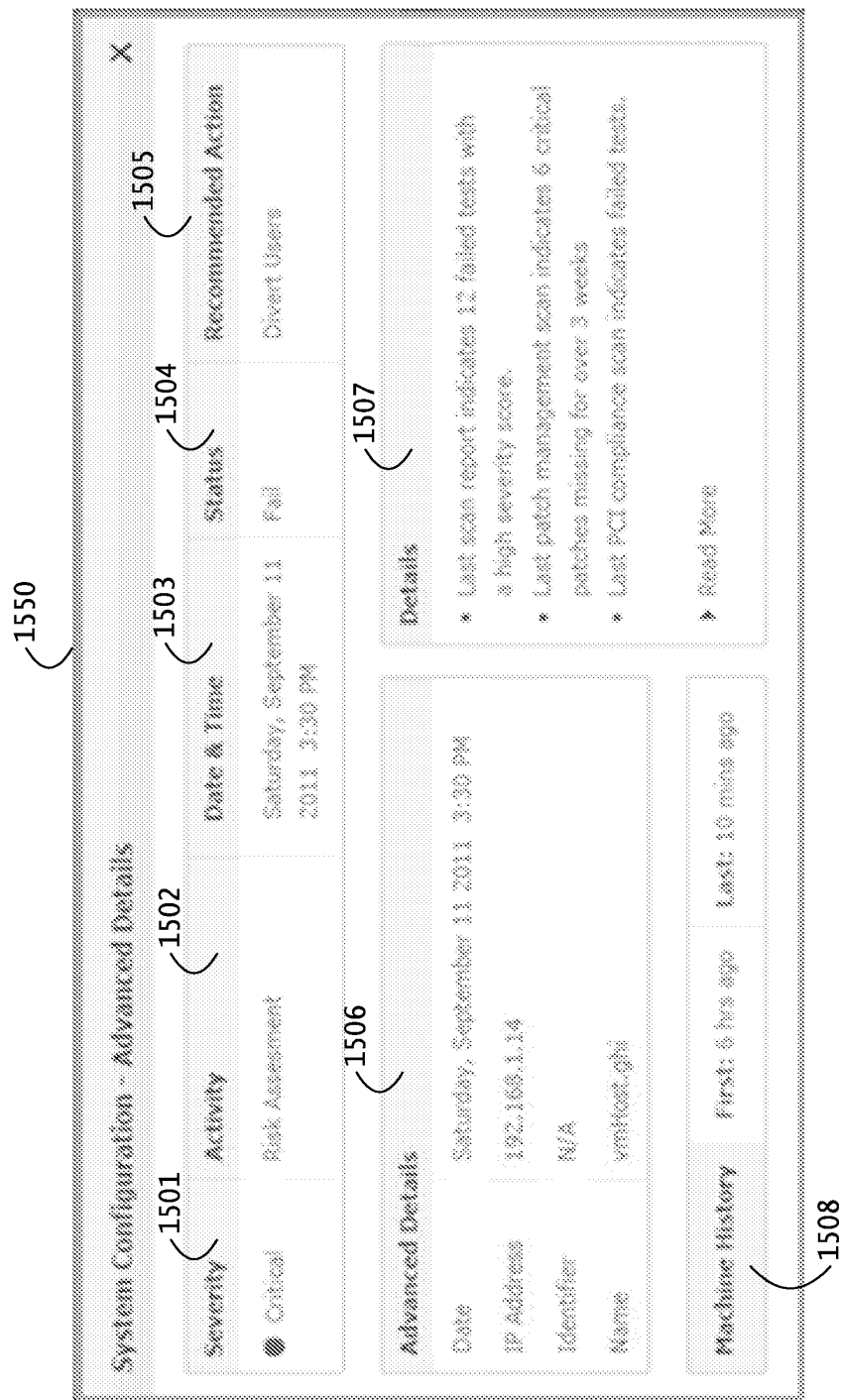
FIG. 14

1400



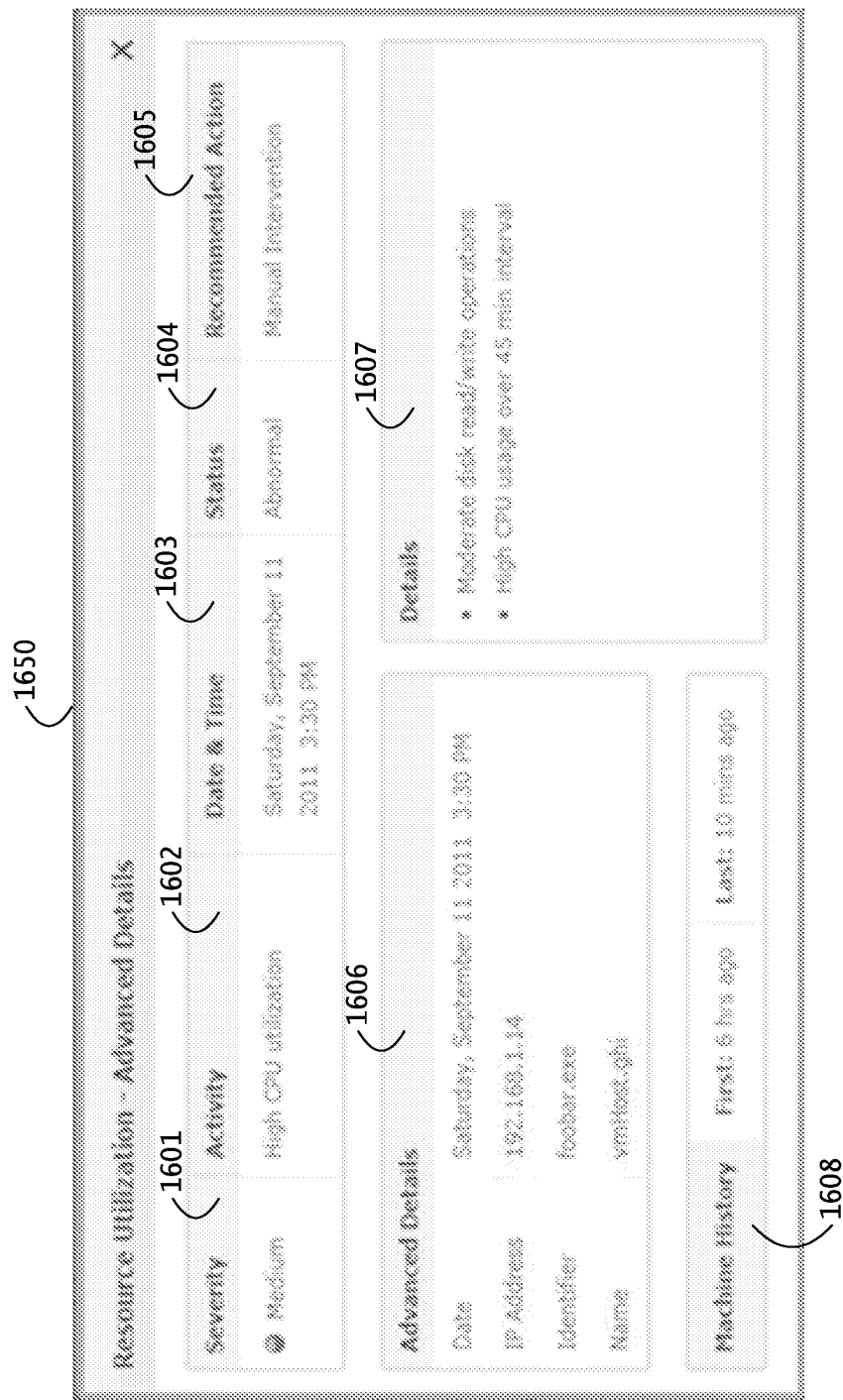
1500

FIG. 15



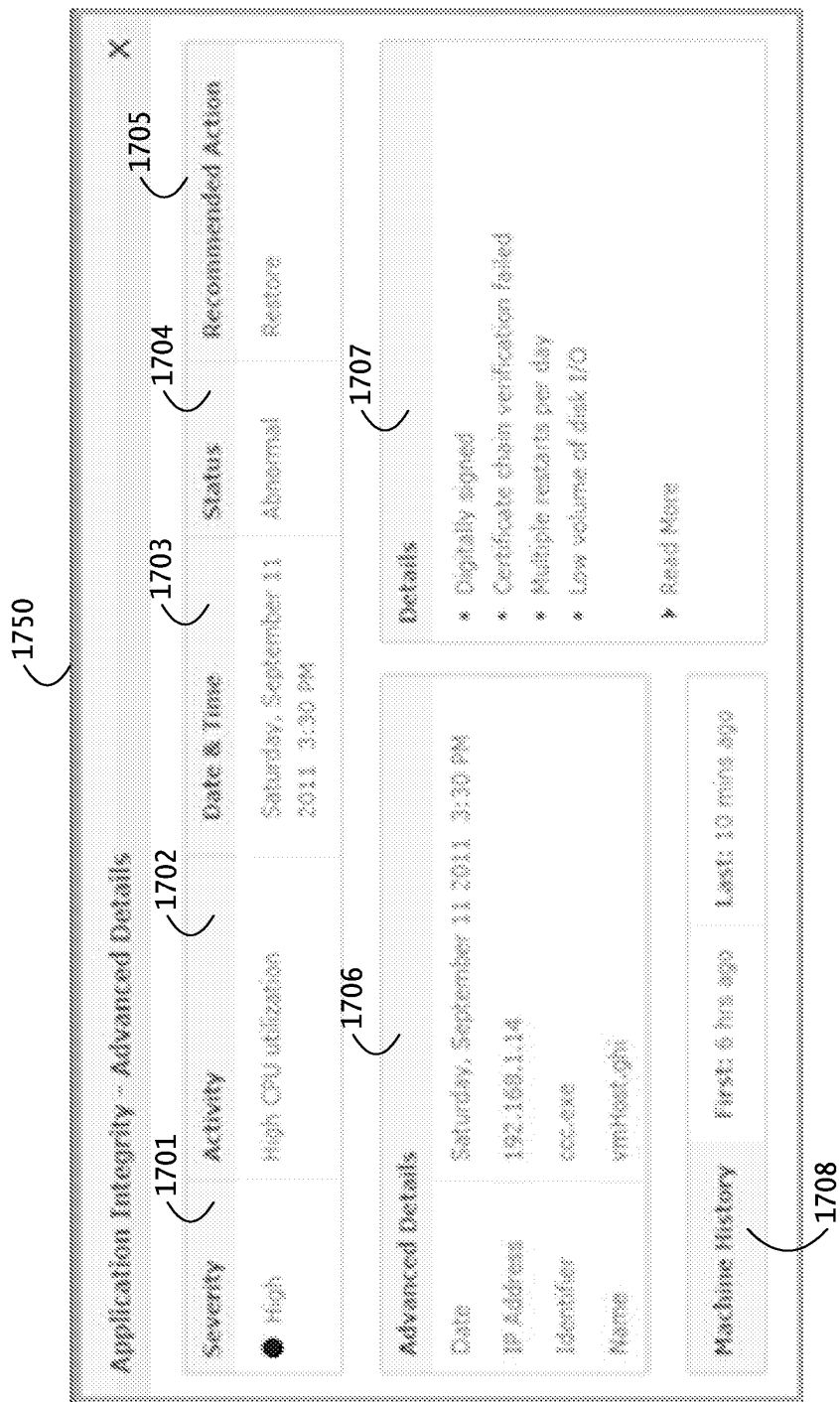
1600 →

FIG. 16



1700 →

FIG. 17



1800 →

FIG. 18

1850

Network Activity - Advanced Details

X

1801	1802	1803	1804	1805
Severity	Activity	Date & Time	Status	Recommended Action
● High	Connected BotClient, and its propagating	Saturday, September 11 2011 3:30 PM	Infected	Quarantine

1806

Advanced Details

Date	Saturday, September 11 2011 3:30 PM
IP Address	192.168.1.14
Identifier	00AC0000710
Name	vmHost.ghi

Machine history

First: 6 hrs ago	Last: 10 mins ago
------------------	-------------------

1807

Details

- * Suspicious Internet Binary Download
- * Confirmed BotNet C&C Checkin: Korgo command checking in
- * Outbound Malicious Scanning
- * Connection to known C&C Server
- Read More

1808

FIG. 19

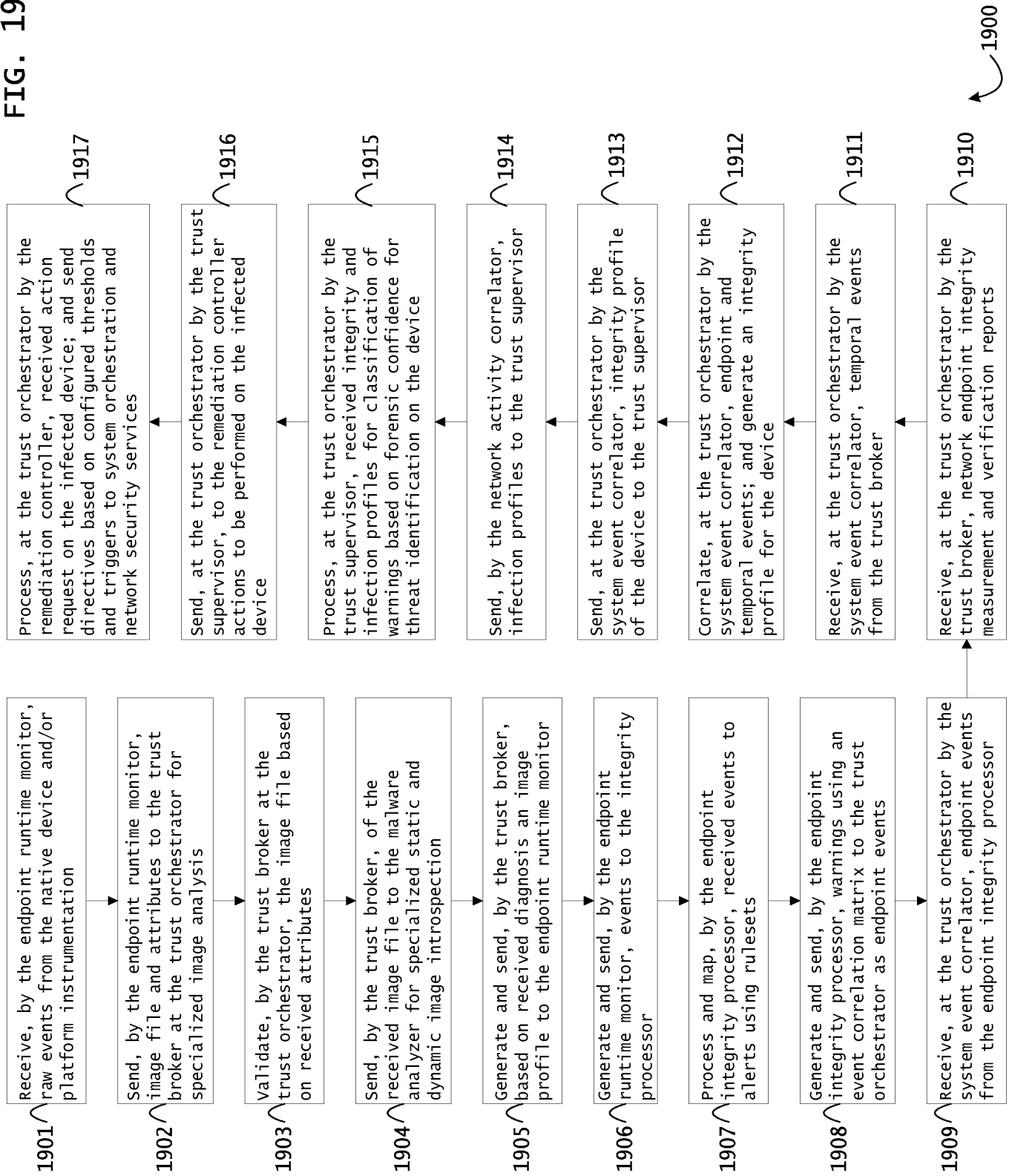


FIG. 20



FIG. 21

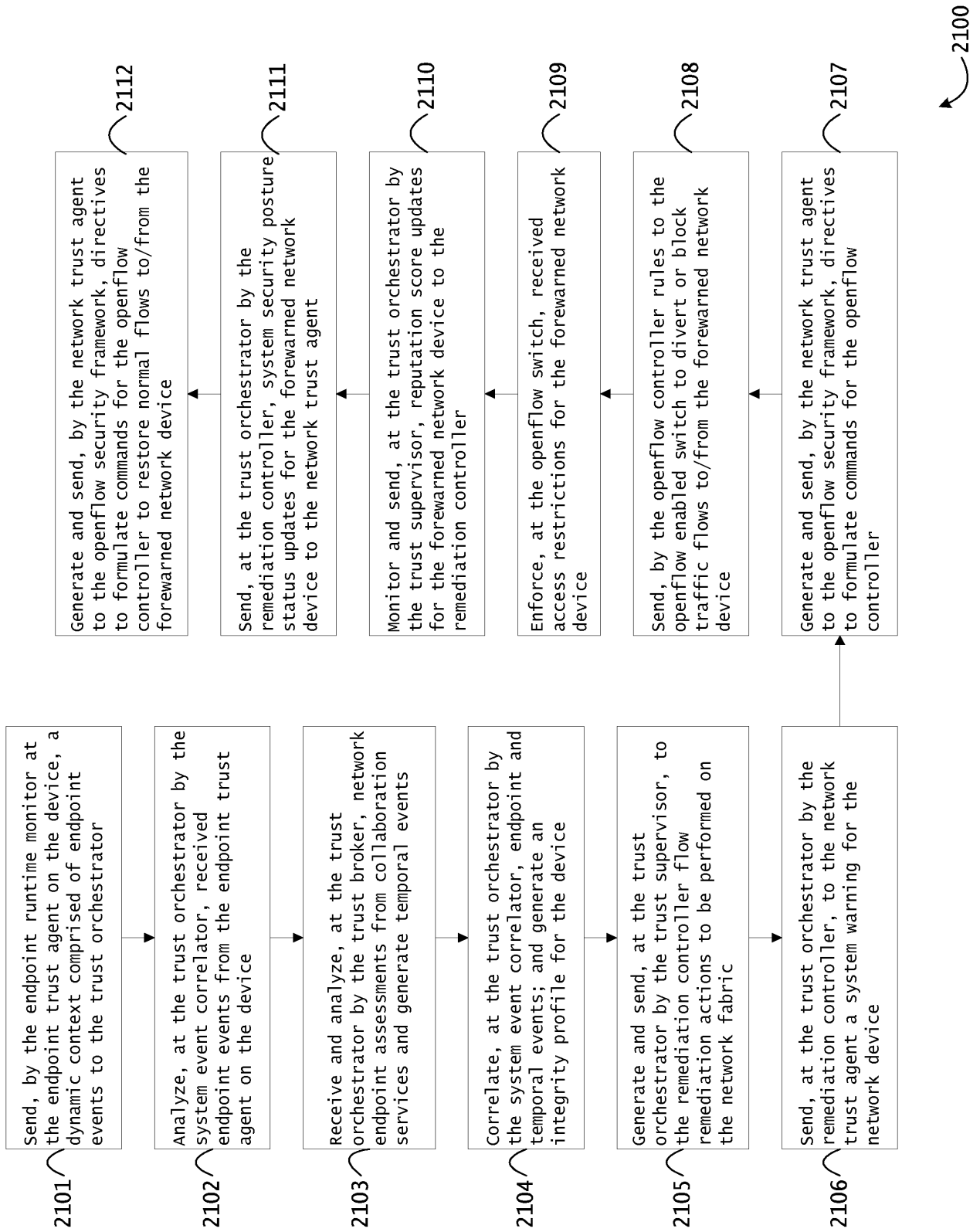


FIG. 22

