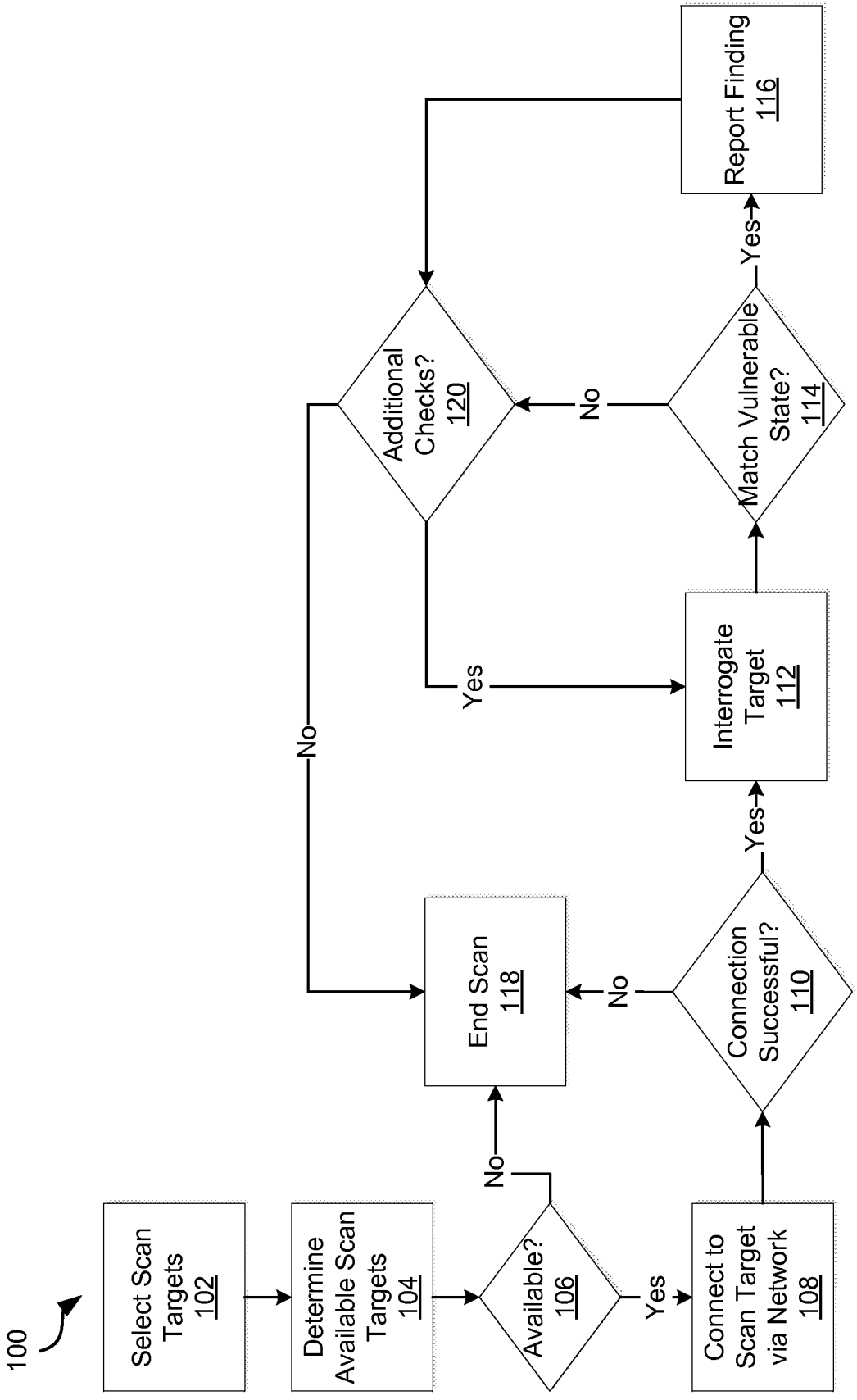


FIG. 1
Prior Art

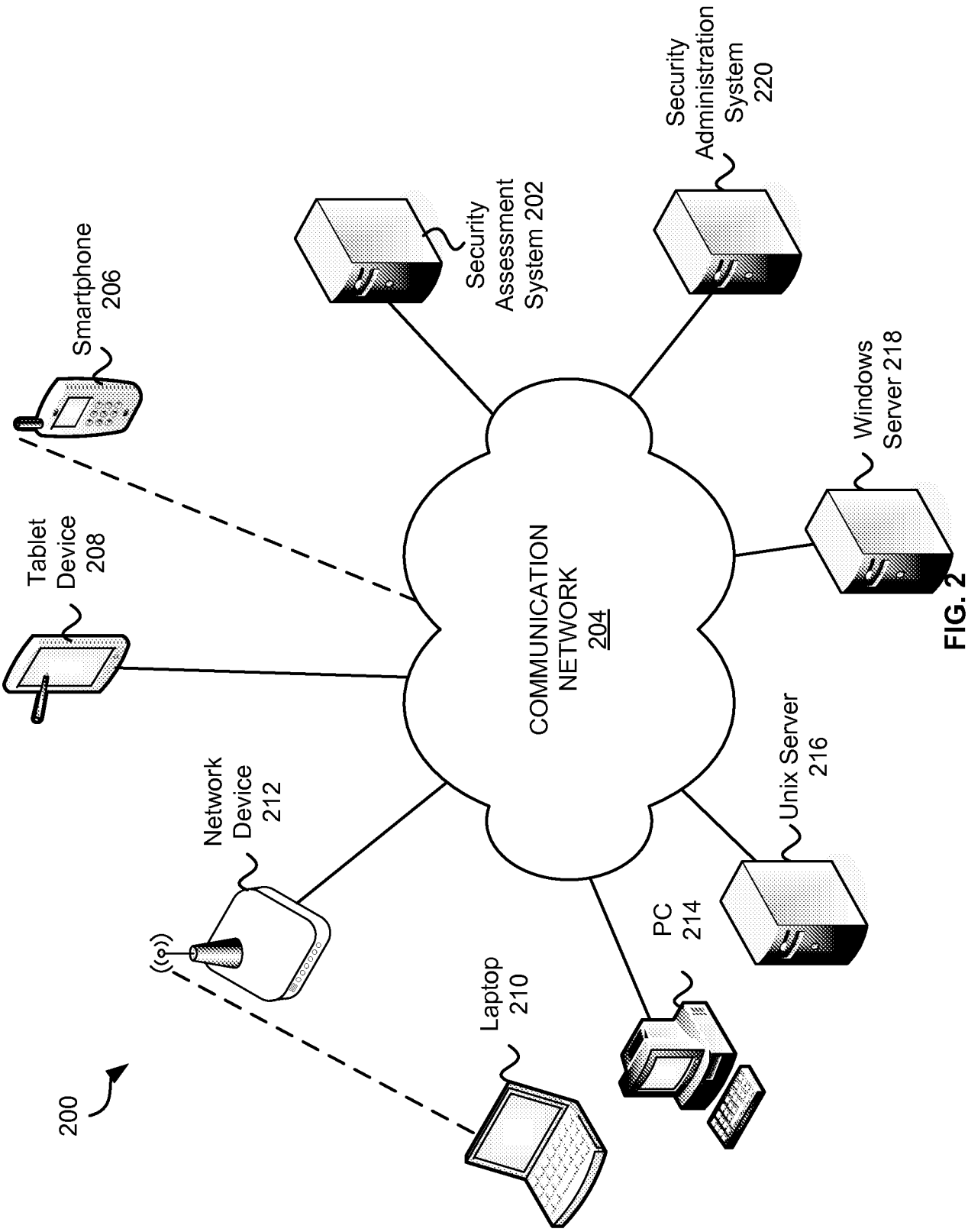

200
Smartphone 206
Tablet Device 208
Network Device 212
Laptop 210
PC 214
Unix Server 216
Windows Server 218
Security Assessment System 202
Security Administration System 220
COMMUNICATION NETWORK 204

FIG. 2

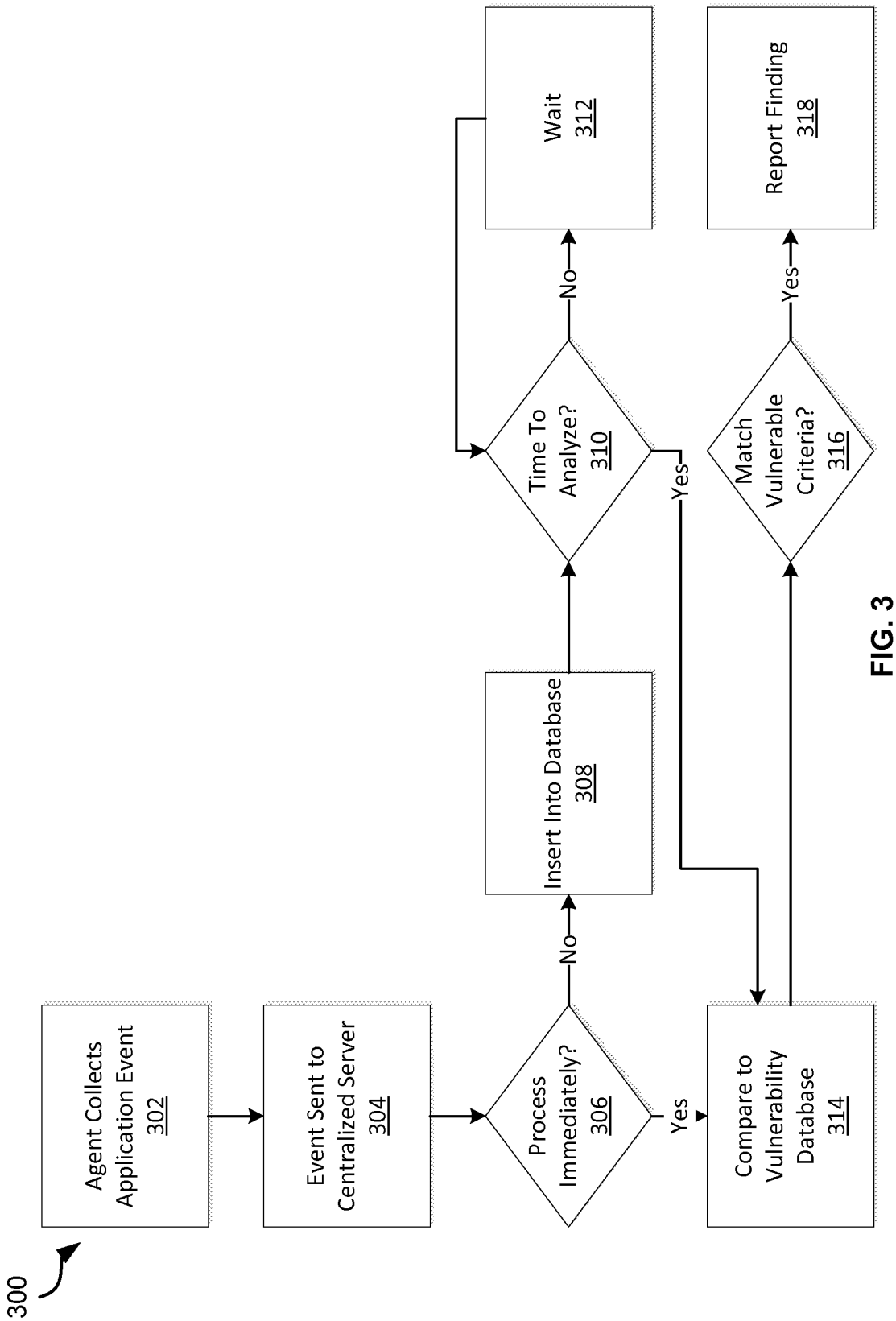

300
Agent Collects Application Event 302
Event Sent to Centralized Server 304
Process Immediately? 306
No
Yes
Insert Into Database 308
Time To Analyze? 310
No
Yes
Wait 312
Compare to Vulnerability Database 314
Match Vulnerable Criteria? 316
Yes
Report Finding 318

FIG. 3

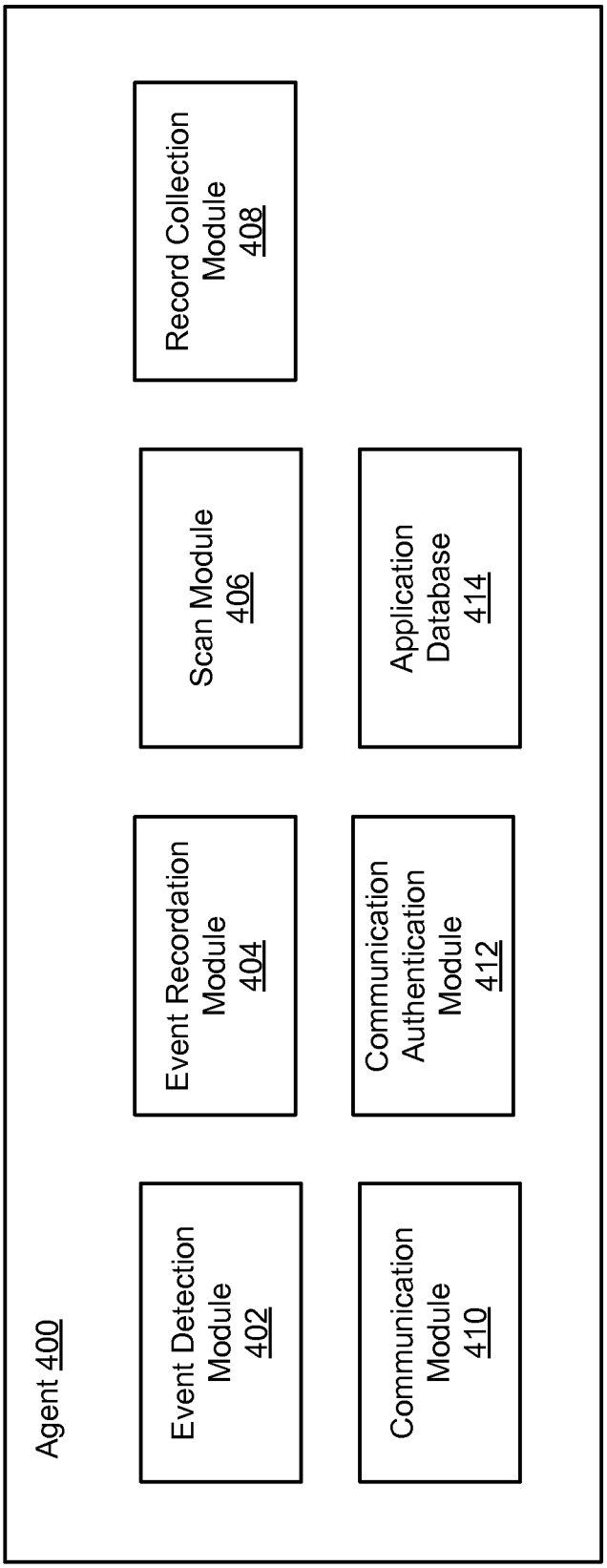

Agent 400
Event Detection Module 402
Event Recordation Module 404
Scan Module 406
Record Collection Module 408
Communication Module 410
Communication Authentication Module 412
Application Database 414

FIG. 4

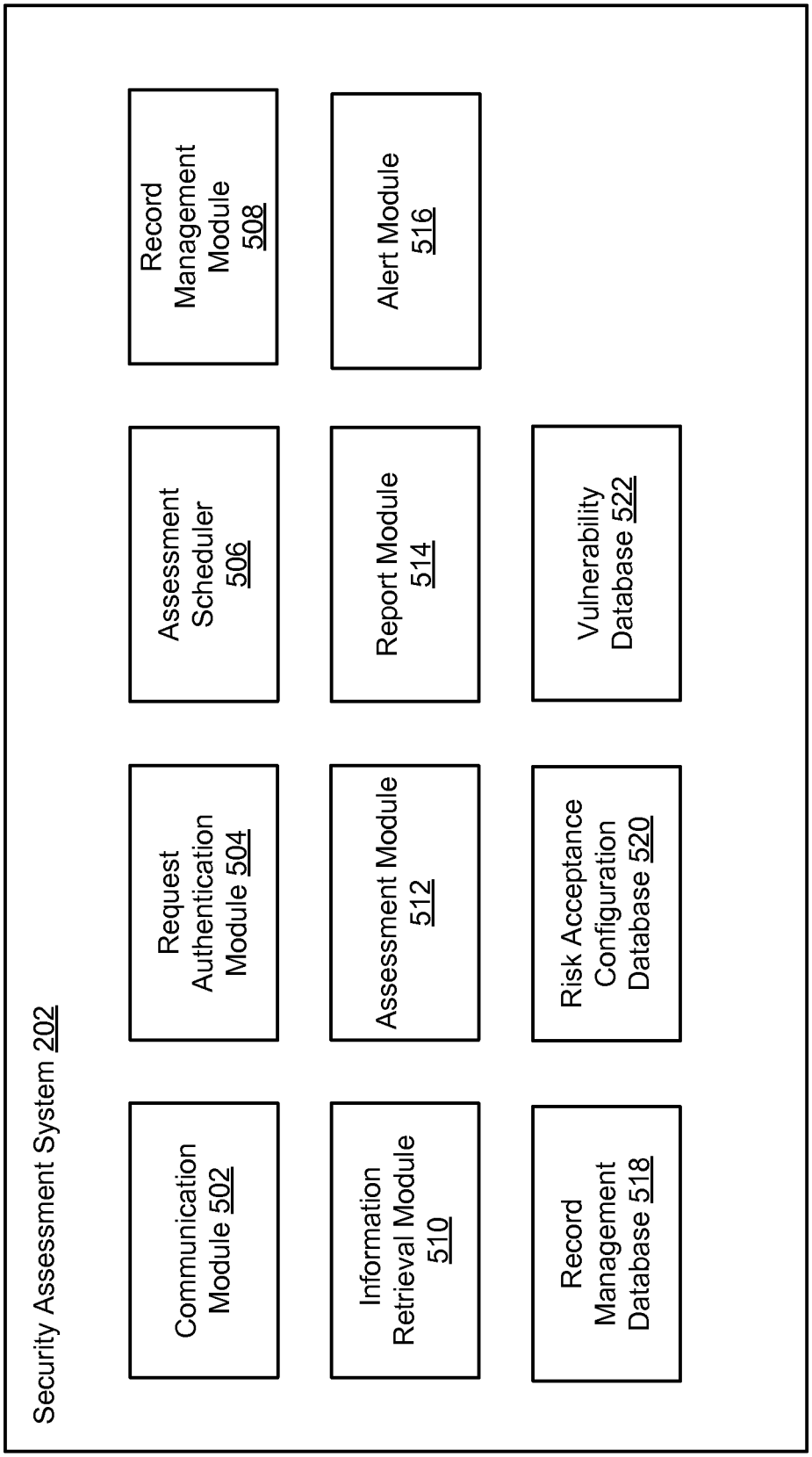

Security Assessment System 202
Communication Module 502
Request Authentication Module 504
Assessment Scheduler 506
Record Management Module 508
Information Retrieval Module 510
Assessment Module 512
Report Module 514
Alert Module 516
Record Management Database 518
Risk Acceptance Configuration Database 520
Vulnerability Database 522

FIG. 5

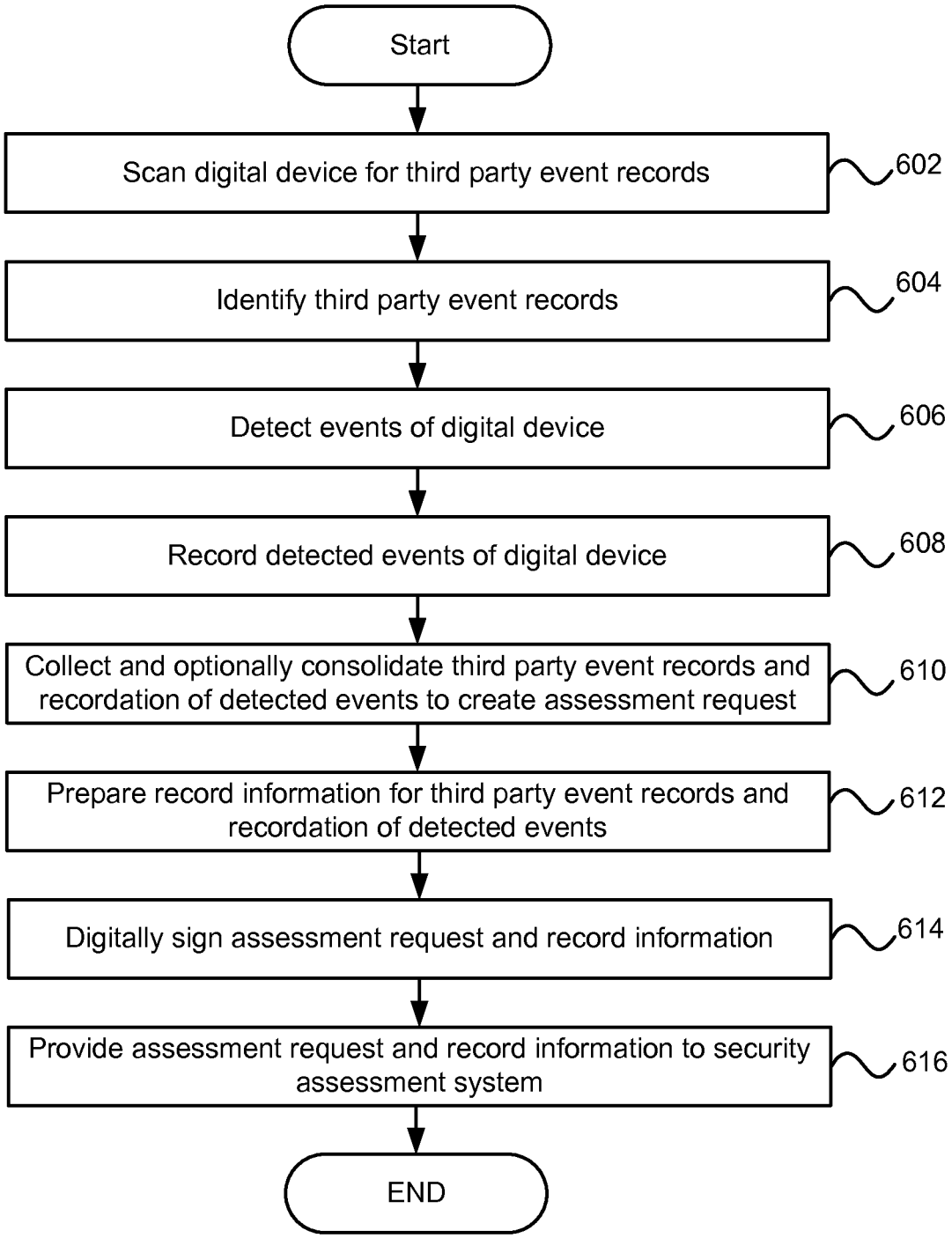

Start
Scan digital device for third party event records
602
Identify third party event records
604
Detect events of digital device
606
Record detected events of digital device
608
Collect and optionally consolidate third party event records and recordation of detected events to create assessment request
610
Prepare record information for third party event records and recordation of detected events
612
Digitally sign assessment request and record information
614
Provide assessment request and record information to security assessment system
616
END

FIG. 6

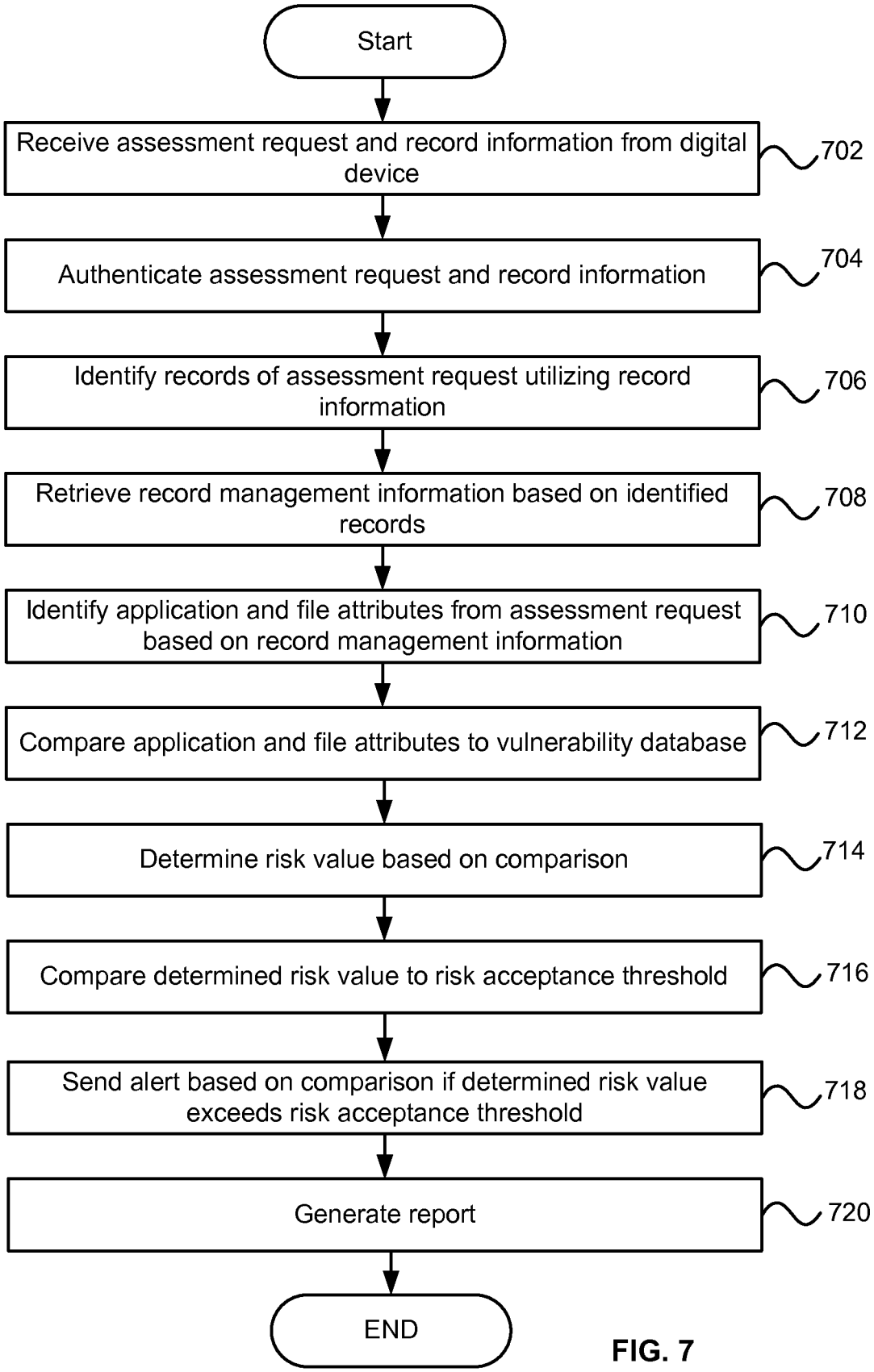

Start
Receive assessment request and record information from digital device
702
Authenticate assessment request and record information
704
Identify records of assessment request utilizing record information
706
Retrieve record management information based on identified records
708
Identify application and file attributes from assessment request based on record management information
710
Compare application and file attributes to vulnerability database
712
Determine risk value based on comparison
714
Compare determined risk value to risk acceptance threshold
716
Send alert based on comparison if determined risk value exceeds risk acceptance threshold
718
Generate report
720
END

FIG. 7

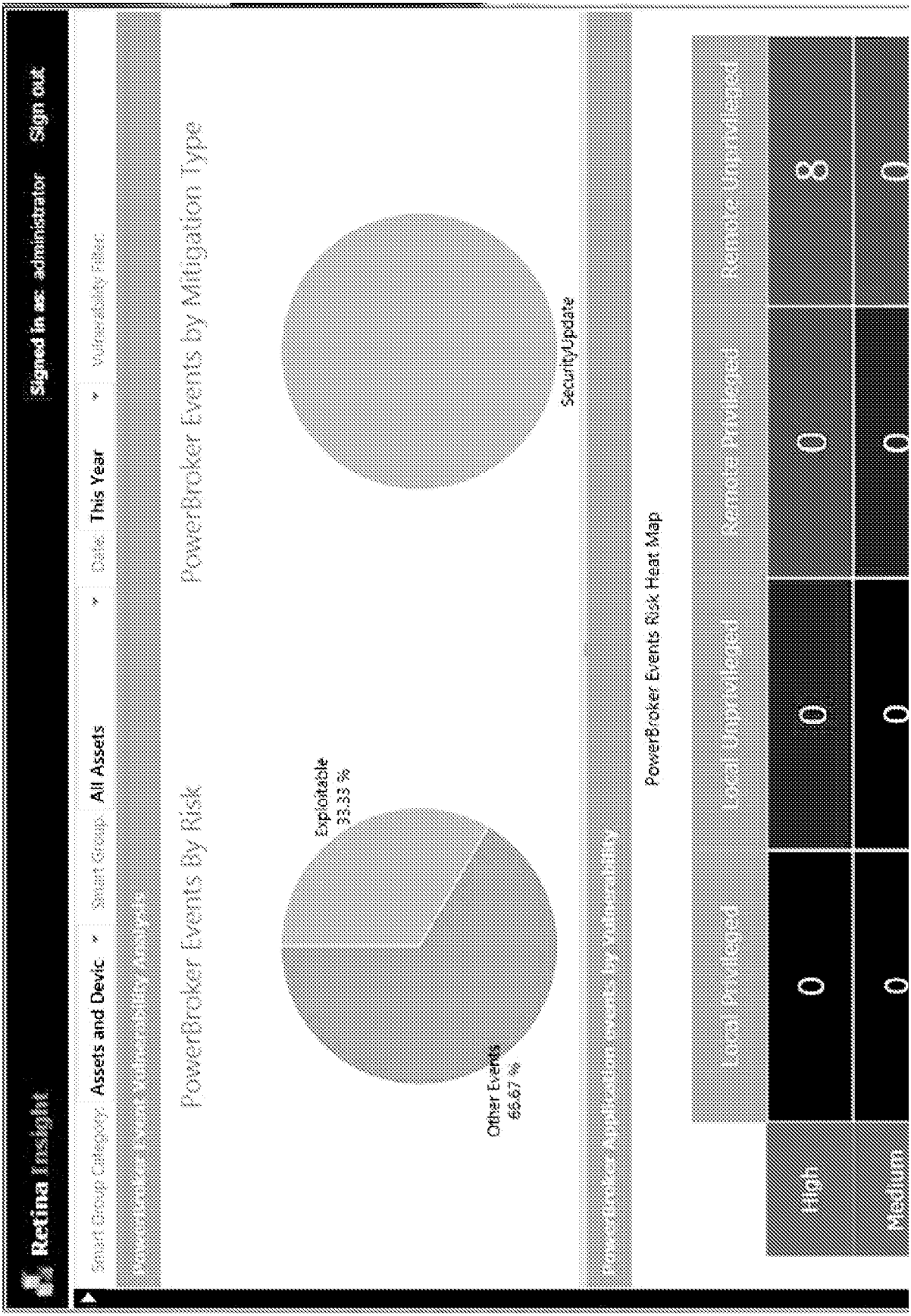

Retina Insight
Signed in as: administrator
Sign out
Smart Group Category: Assets and Devic
Smart Group: All Assets
Date: This Year
Vulnerability Filter
PowerBroker Events By Risk
Exploitable
33.33 %
Other Events
66.67 %
PowerBroker Events by Mitigation Type
SecurityUpdate
PowerBroker Events Risk Heat Map
Unauthorized
Unauthorized
Unauthorized
Unauthorized
High
Medium
0
0
0
0
8
0

FIG. 8

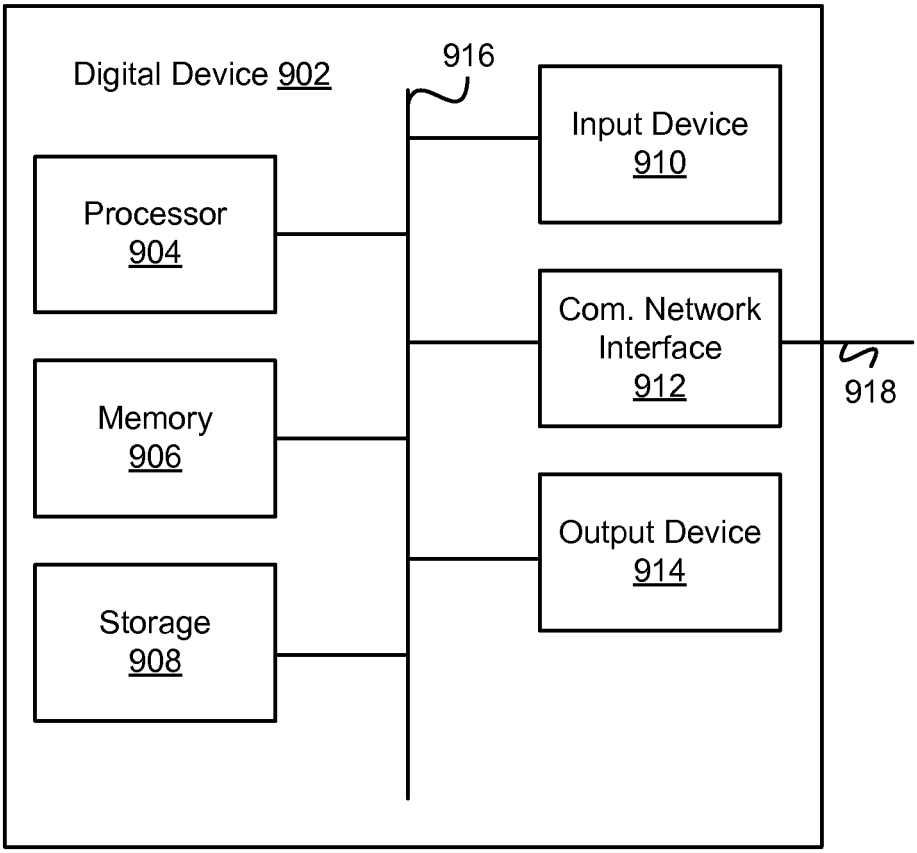

Digital Device 902
916
Input Device
910
Processor
904
Com. Network
Interface
912
918
Memory
906
Output Device
914
Storage
908

FIG. 9

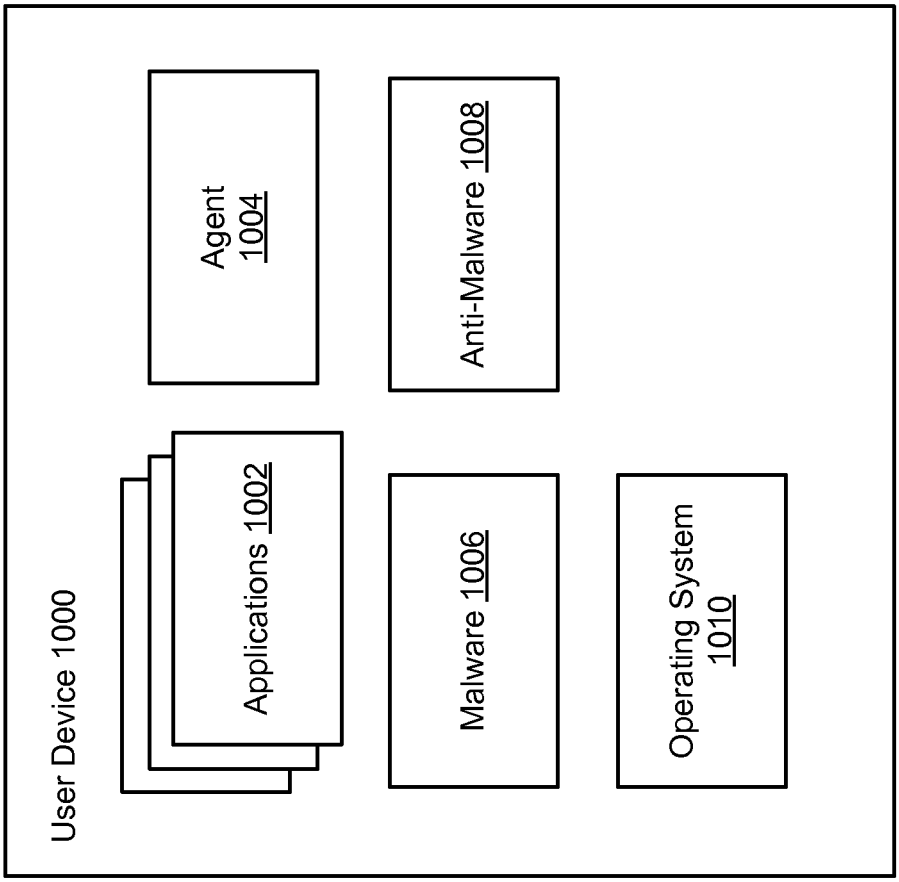

User Device 1000
Agent 1004
Anti-Malware 1008
Applications 1002
Malware 1006
Operating System 1010

FIG. 10

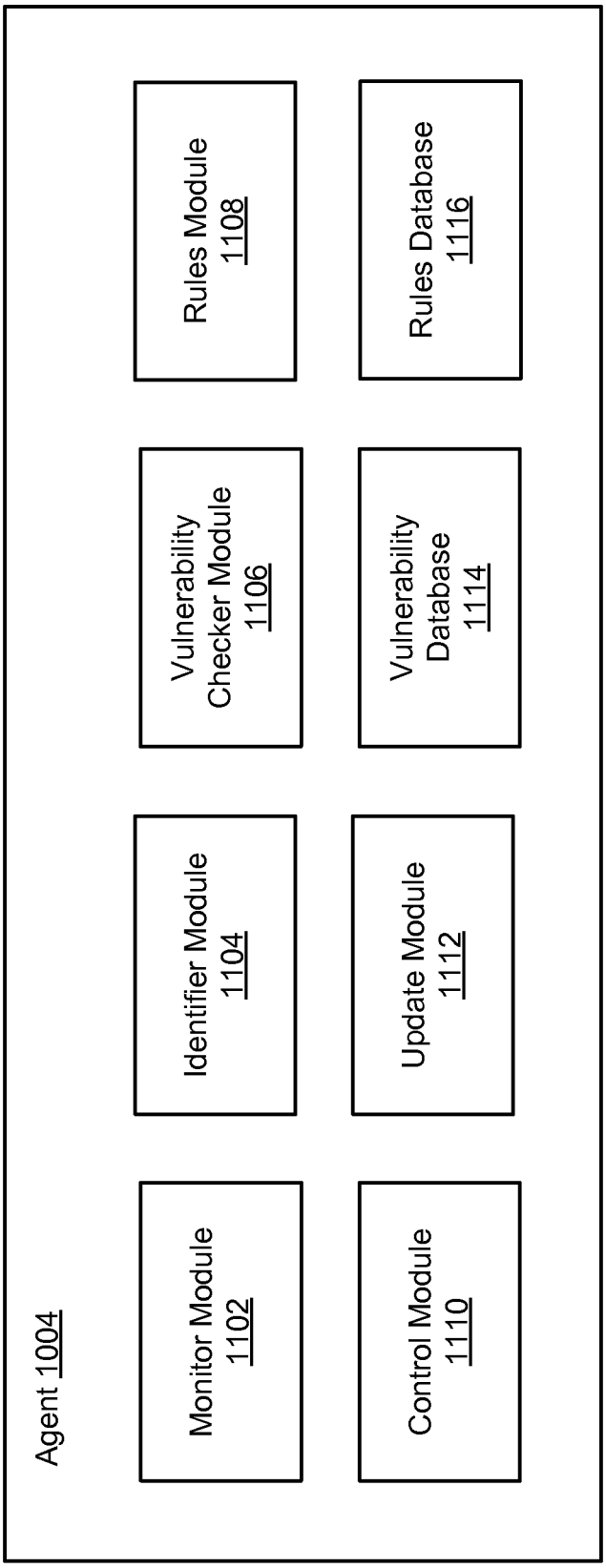

Agent 1004
Monitor Module 1102
Identifier Module 1104
Vulnerability Checker Module 1106
Rules Module 1108
Control Module 1110
Update Module 1112
Vulnerability Database 1114
Rules Database 1116

FIG. 11

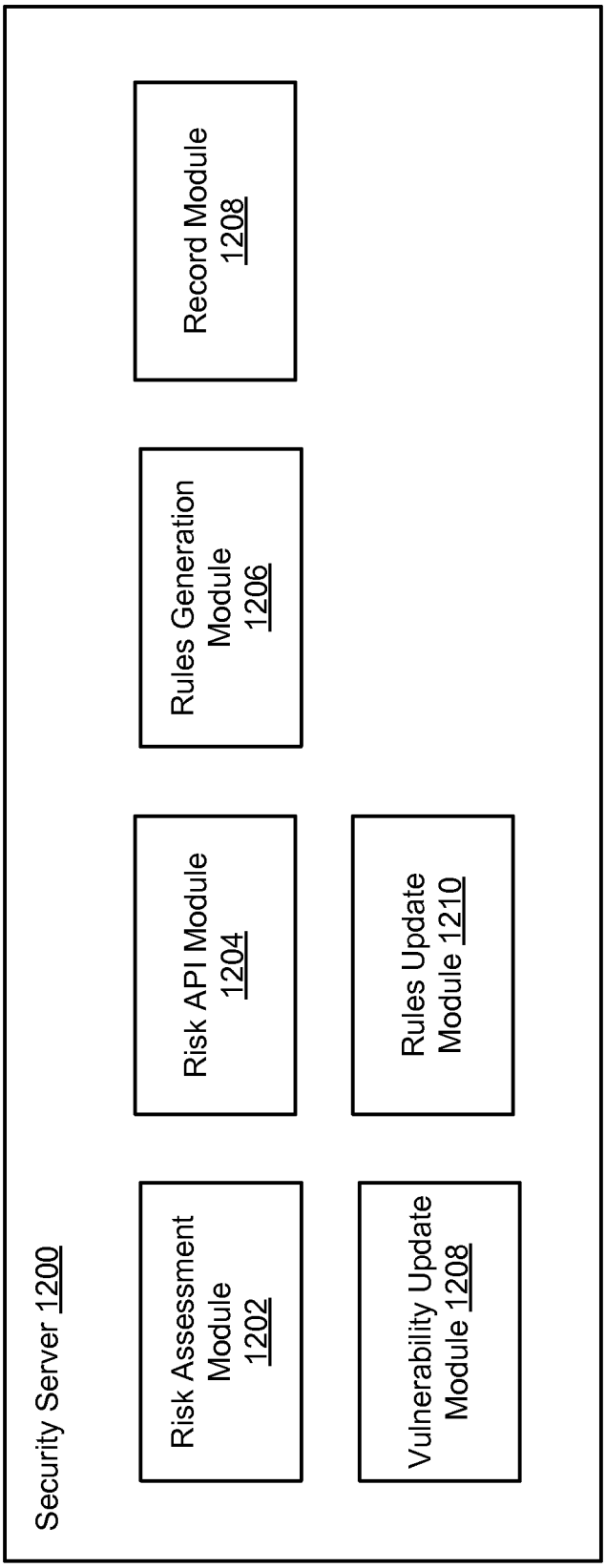

Security Server 1200
Risk Assessment Module 1202
Risk API Module 1204
Rules Generation Module 1206
Record Module 1208
Vulnerability Update Module 1208
Rules Update Module 1210

FIG. 12

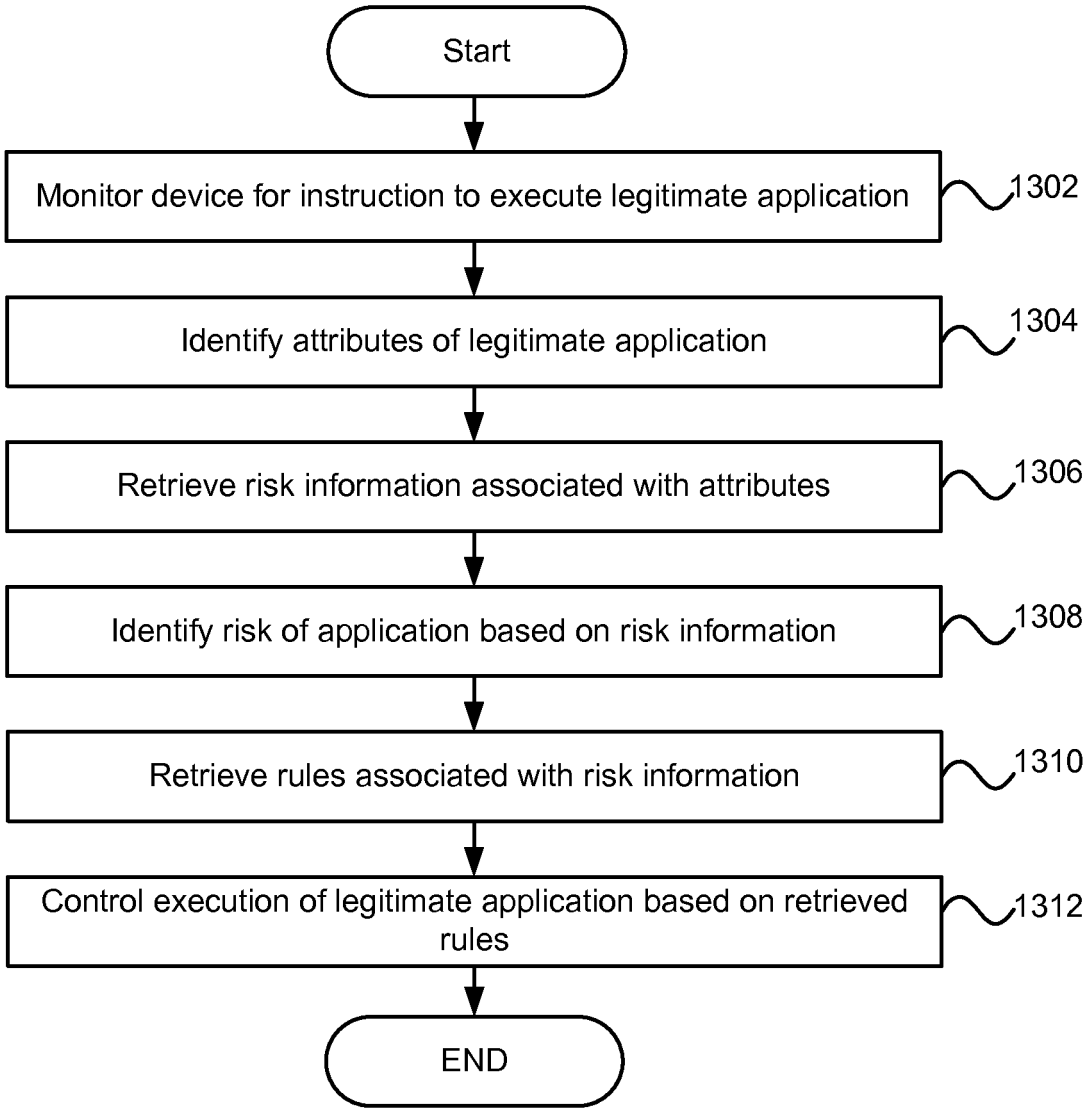

Start
Monitor device for instruction to execute legitimate application
1302
Identify attributes of legitimate application
1304
Retrieve risk information associated with attributes
1306
Identify risk of application based on risk information
1308
Retrieve rules associated with risk information
1310
Control execution of legitimate application based on retrieved rules
1312
END

FIG. 13

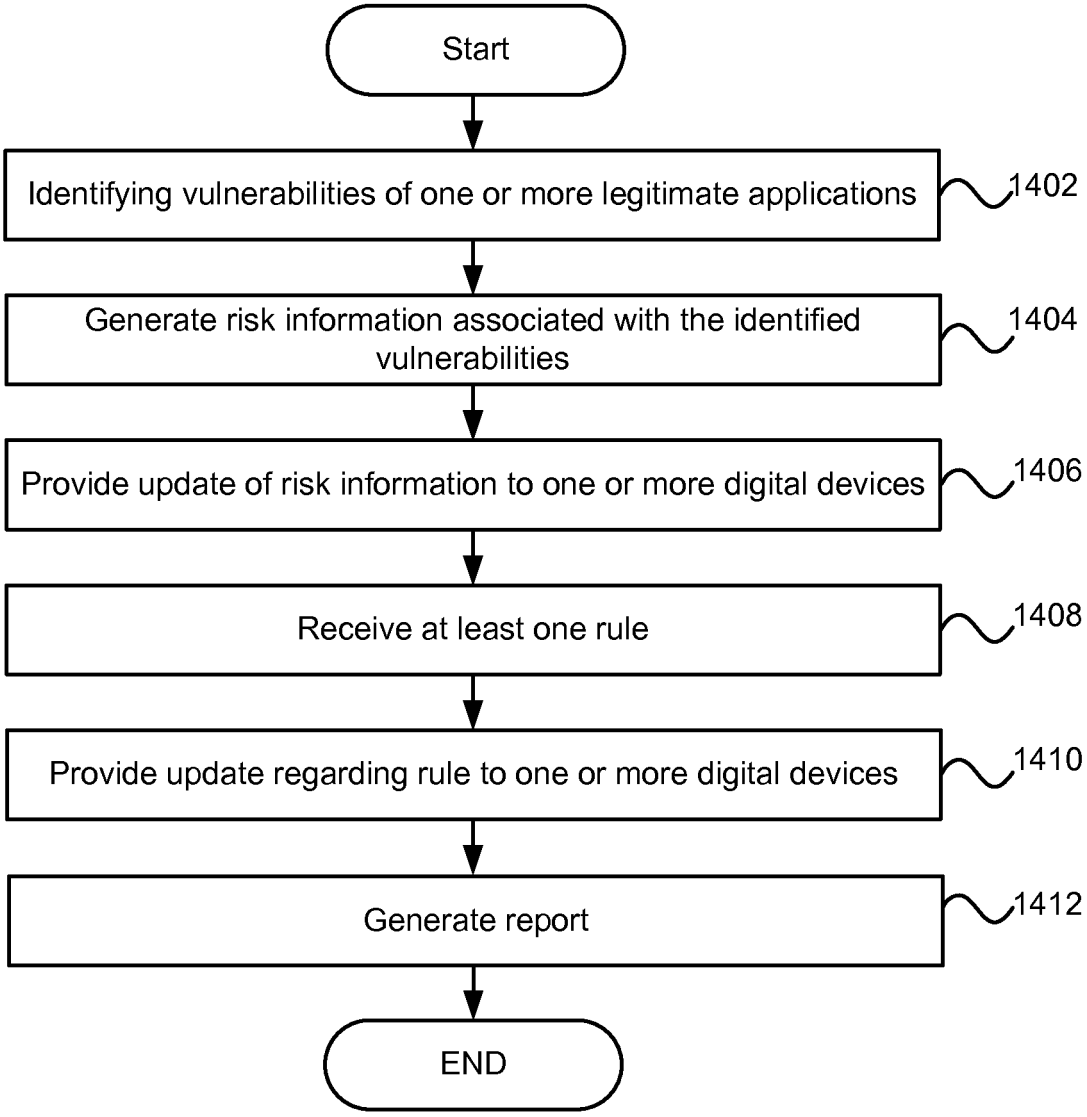

Start
Identifying vulnerabilities of one or more legitimate applications
1402
Generate risk information associated with the identified vulnerabilities
1404
Provide update of risk information to one or more digital devices
1406
Receive at least one rule
1408
Provide update regarding rule to one or more digital devices
1410
Generate report
1412
END

FIG. 14

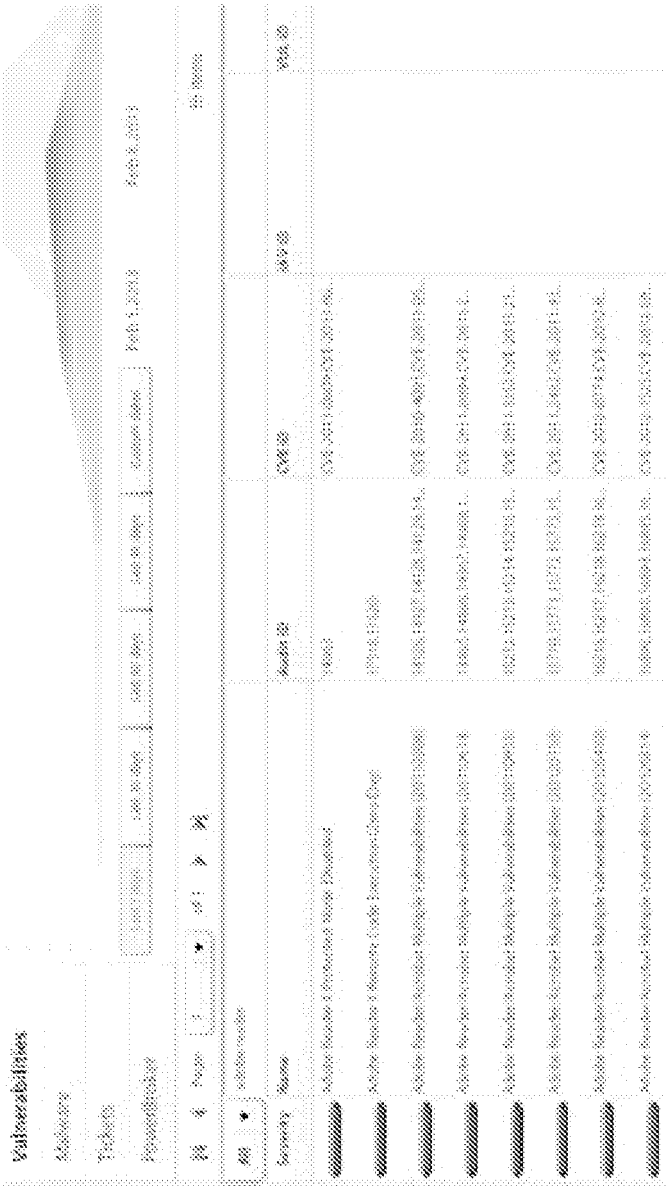


FIG. 15

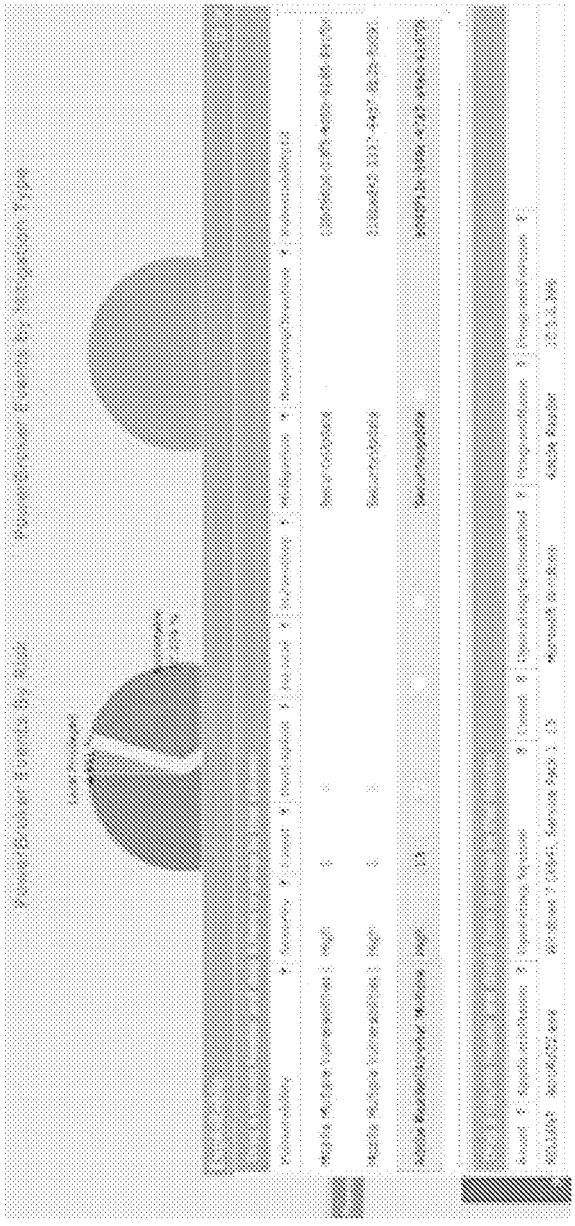


FIG. 16