US 20140245376A1

(54) **SYSTEMS AND METHODS OF RISK BASED RULES FOR APPLICATION CONTROL**

(71) Applicant: **BeyondTrust Software, Inc.**, Phoenix, AZ (US)

(72) Inventors: **Brad Hibbert**, Carp (CA); **Chris Silva**, Laguna Beach, CA (US)

(73) Assignee: **BeyondTrust Software, Inc.**, Phoenix, AZ (US)

(21) Appl. No.: **14/182,651**

(22) Filed: **Feb. 18, 2014**

Related U.S. Application Data

(63) Continuation-in-part of application No. 14/156,375, filed on Jan. 15, 2014.

(60) Provisional application No. 61/768,809, filed on Feb. 25, 2013.

Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC *H04L 63/1433* (2013.01); *H04L 63/20* (2013.01)
USPC **726/1**

(57) **ABSTRACT**

In various embodiments, an agent on a digital device may comprise a monitor module, an application identification module, a vulnerability module, a rules database, and a rule module. The monitor module may be configured to monitor a device for an instruction to execute a legitimate application. The application identification module may be configured to identify one or more attributes of the legitimate application. The vulnerability module may be configured to retrieve risk information based on the one or more attributes of the legitimate application. The risk information may be determined from known vulnerabilities of the legitimate application. The rules database may be for storing a rule associated with the risk information. The rule module may be configured to retrieve the rule from the rule database based on the risk information and to control the legitimate application based on the rule.
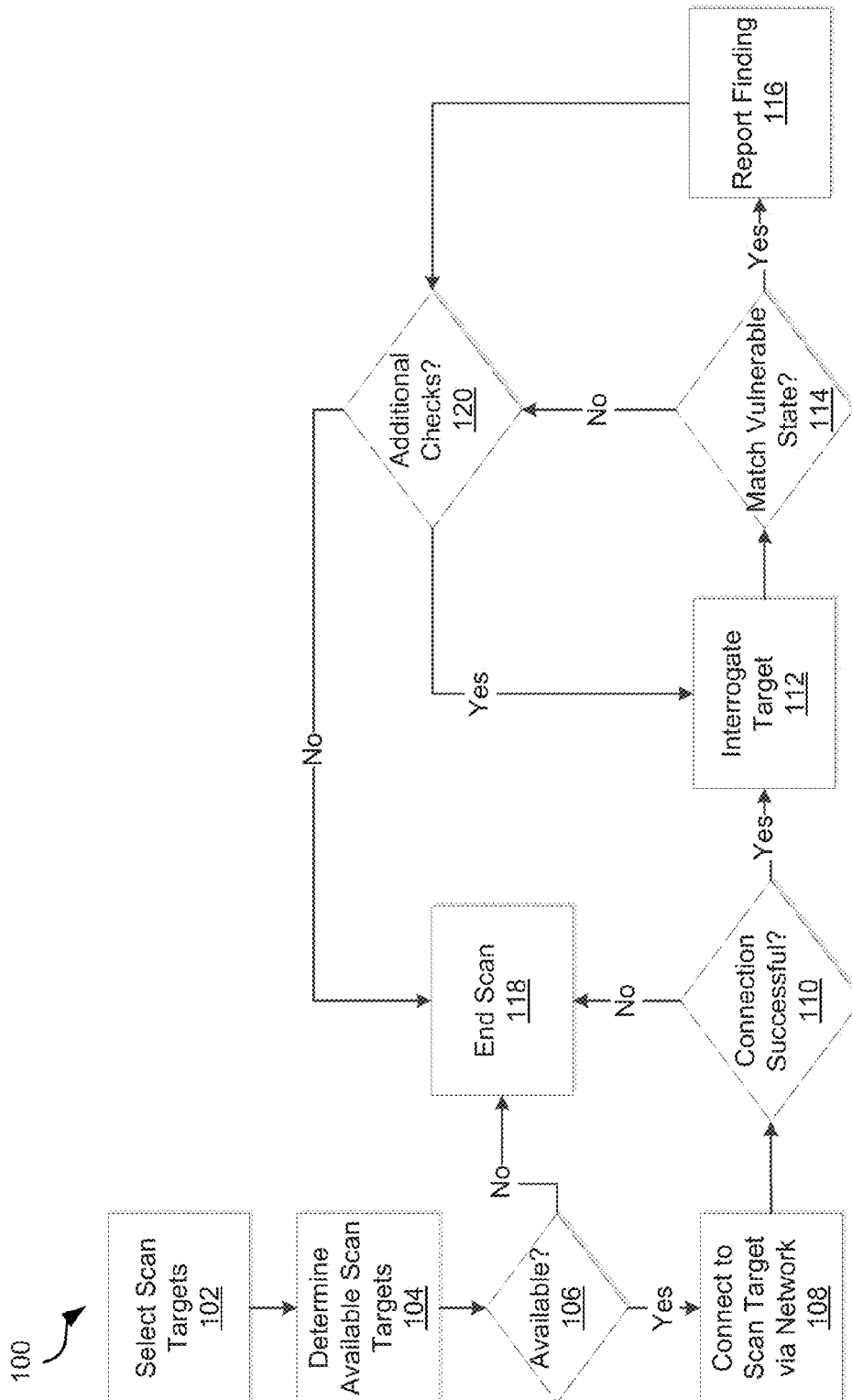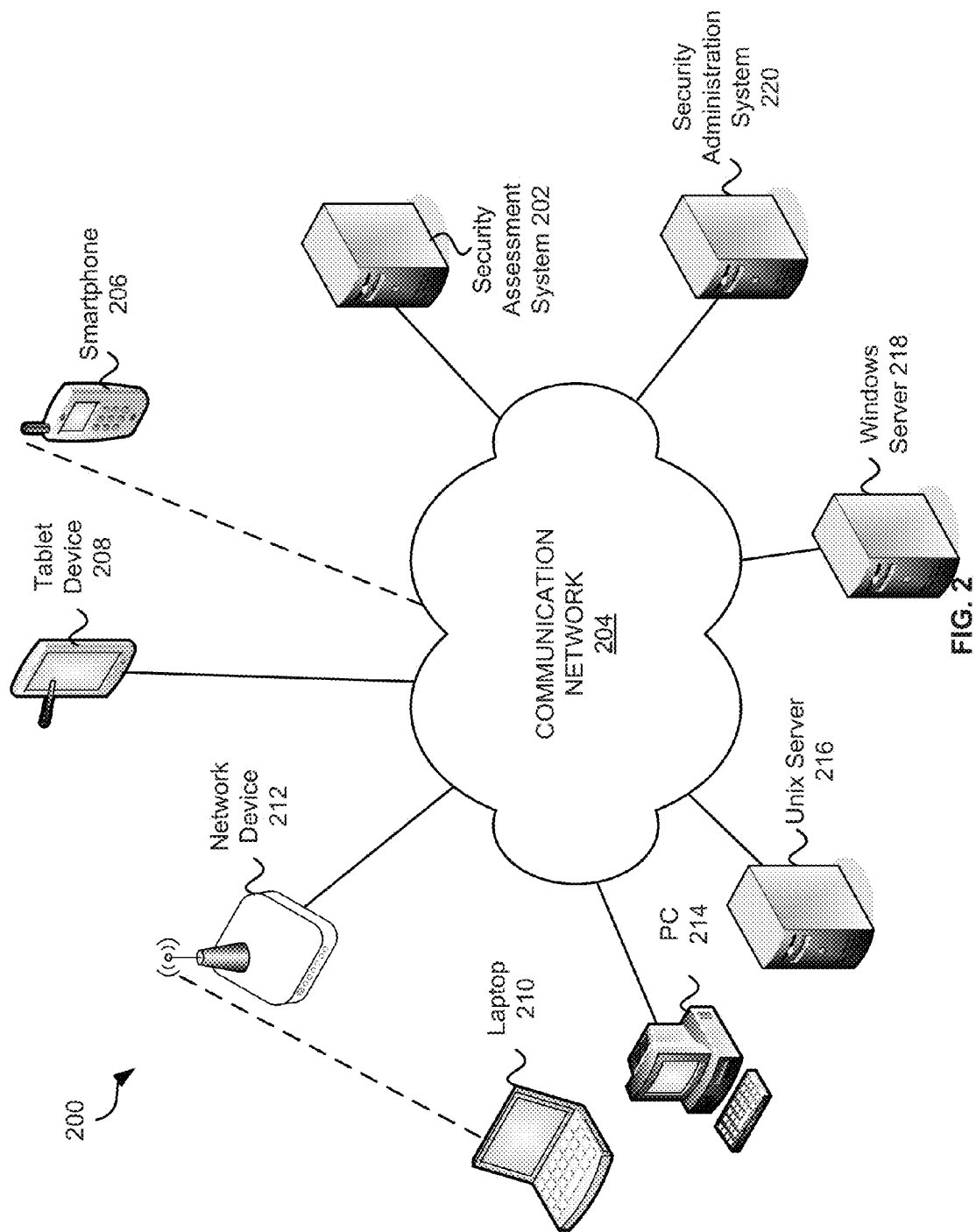
FIG. 1

Prior Art

FIG. 2

300

Agent Collects
Application Event
302

→

Event Sent to
Centralized Server
304

→

Process
Immediately?
306

No →

Insert Into Database
308

→

Time To
Analyze?
310

No →

Wait
312

Yes
↓

Compare to
Vulnerability
Database
314

→

Match
Vulnerable
Criteria?
316

Yes →

Report Finding
318

Yes

FIG. 3

Agent 400

Event Detection
Module
402

Event Recordation
Module
404

Scan Module
406

Record Collection
Module
408

Communication
Module
410

Communication
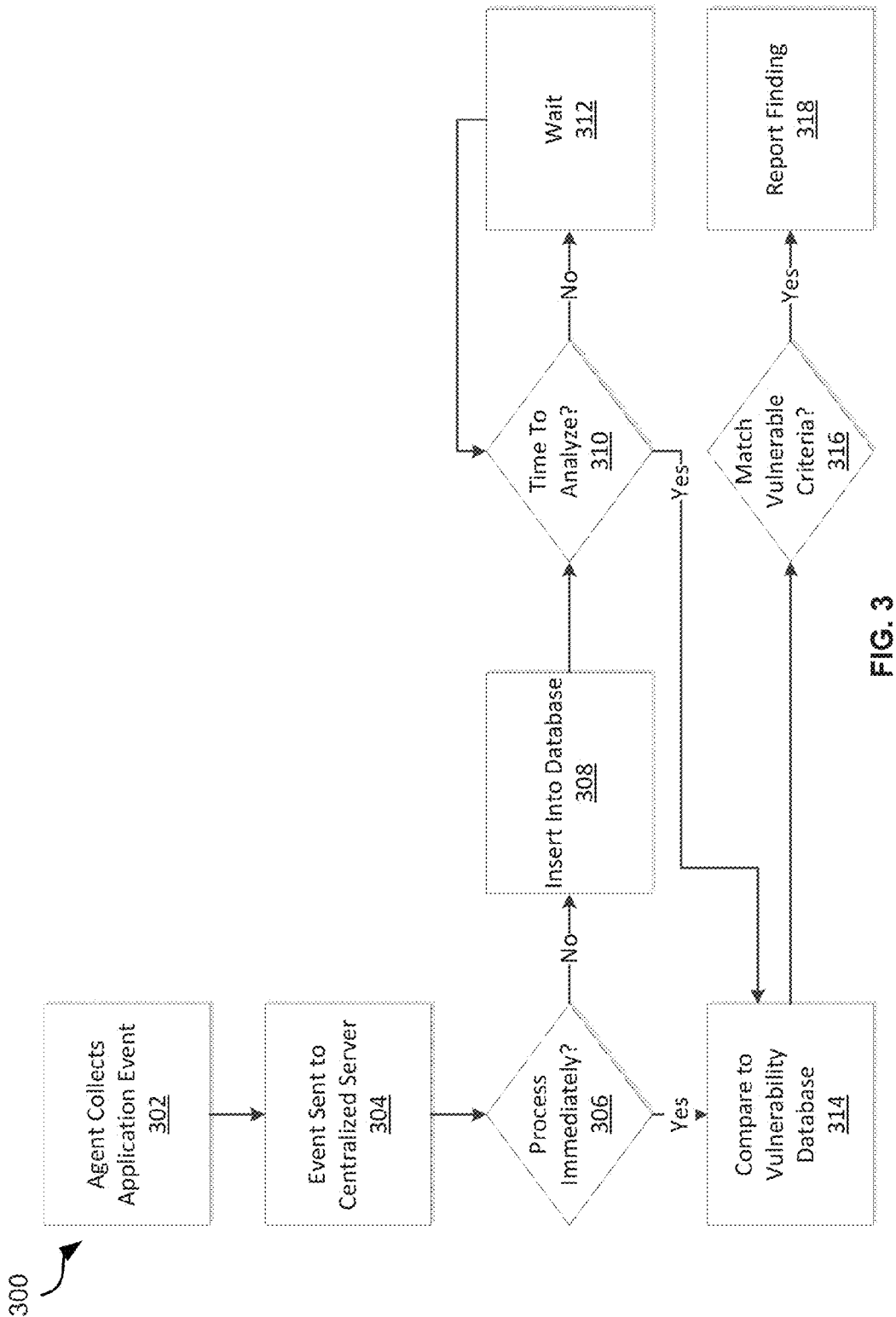Authentication
Module
412

Application
Database
414

FIG. 4

DOCKET ALARM
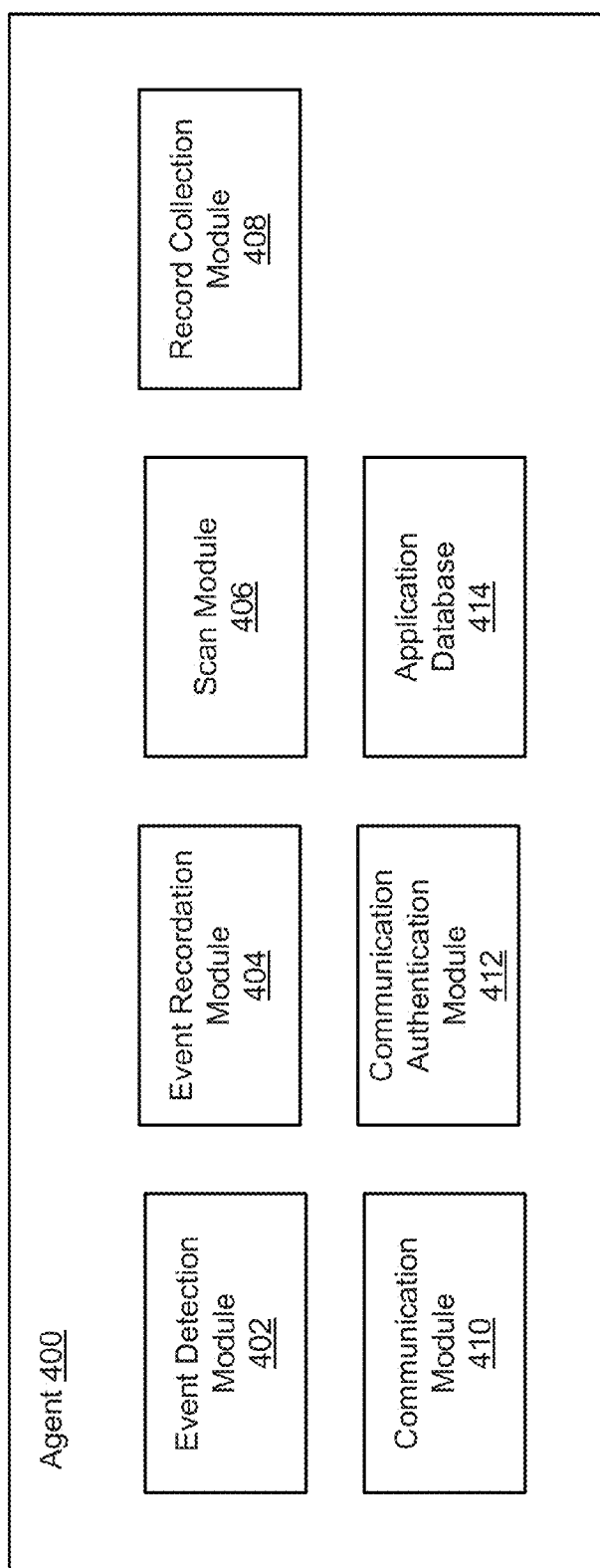
Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase®
Smarter legal research.