US 20170180318A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2017/0180318 A1

LUTAS et al. (43) Pub. Date: Jun. 22, 2017

(54) **DUAL MEMORY INTROSPECTION FOR SECURING MULTIPLE NETWORK ENDPOINTS**

(71) Applicant: **Bitdefender IPR Management Ltd.**, Nicosia (CY)

(72) Inventors: **Dan H. LUTAS**, Cluj-Napoca (RO); **Daniel I. TICLE**, Turda (RO); **Radu I. CIOCAS**, Cluj-Napoca (RO); **Sandor LUKACS**, Floresti (RO); **Ionel C. ANICHITEI**, Cluj-Napoca (RO)

(21) Appl. No.: **15/383,082**

(22) Filed: **Dec. 19, 2016**

Related U.S. Application Data

(60) Provisional application No. 62/269,952, filed on Dec. 19, 2015.

Publication Classification

(51) **Int. Cl.**

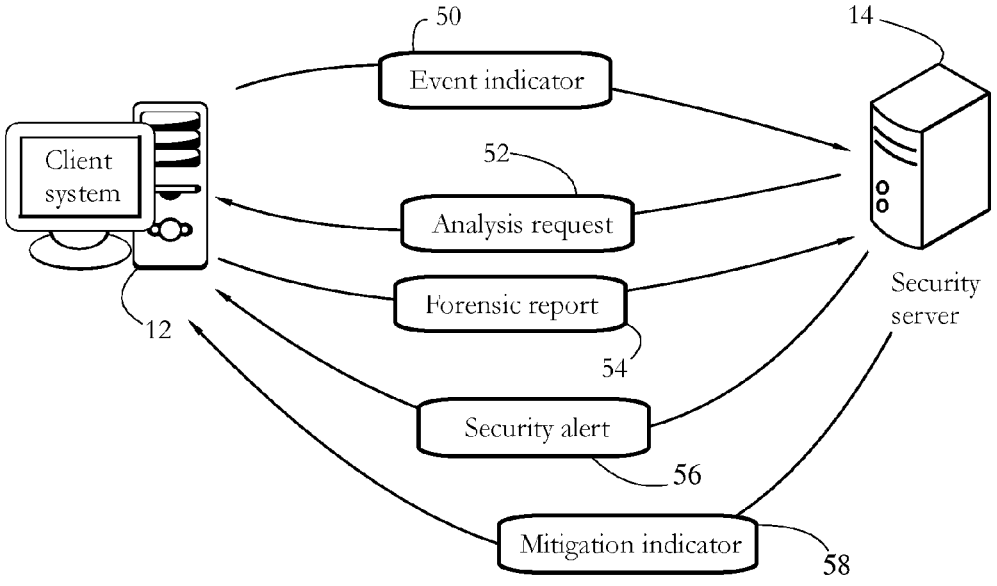
H04L 29/06	(2006.01)
G06F 9/54	(2006.01)
G06F 9/455	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/0254*** (2013.01); ***G06F 9/45558*** (2013.01); ***G06F 9/542*** (2013.01); ***H04L 63/0245*** (2013.01); ***H04L 63/0272*** (2013.01); ***H04L 63/14*** (2013.01); *G06F 2009/45587* (2013.01)

(57) **ABSTRACT**

Described systems and methods enable protecting multiple client systems (e.g., a corporate network) from computer security threats such as malicious software and intrusion. In some embodiments, each protected client operates a live introspection engine and an on-demand introspection engine. The live introspection engine detects the occurrence of certain events within a protected virtual machine exposed on the respective client system, and communicates the occurrence to a remote security server. In turn, the server may request a forensic analysis of the event from the client system, by indicating a forensic tool to be executed by the client. Forensic tools may be stored in a central repository accessible to the client. In response to receiving the analysis request, the on-demand introspection engine may retrieve and execute the forensic tool, and communicate a result of the forensic analysis to the security server. The server may use the information to determine whether the respective client is under attack by malicious software or an intruder.



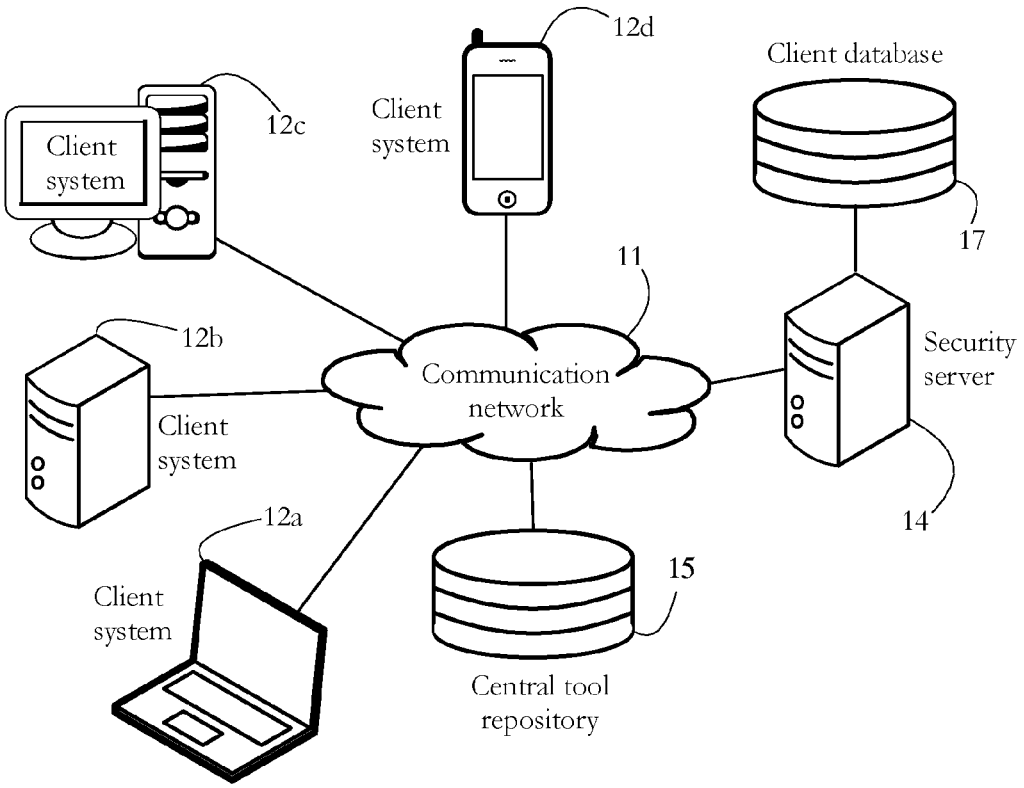


FIG. 1

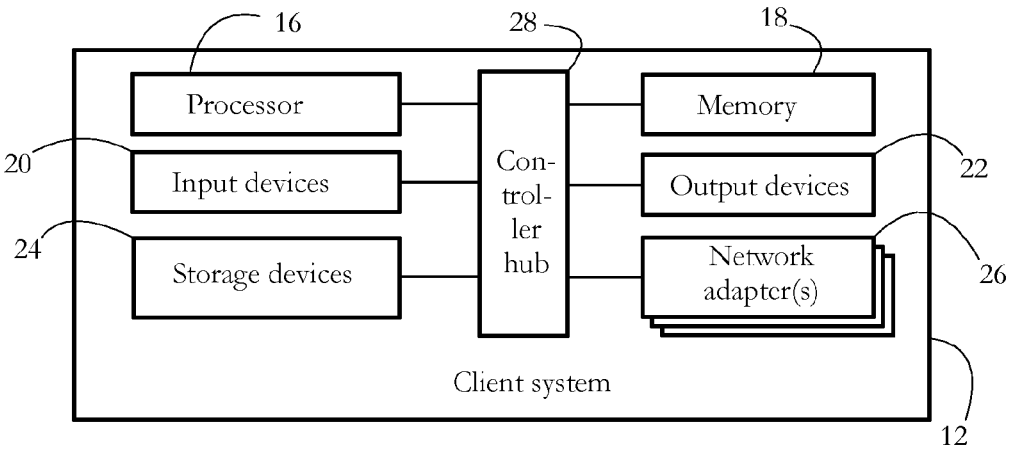


FIG. 2-A

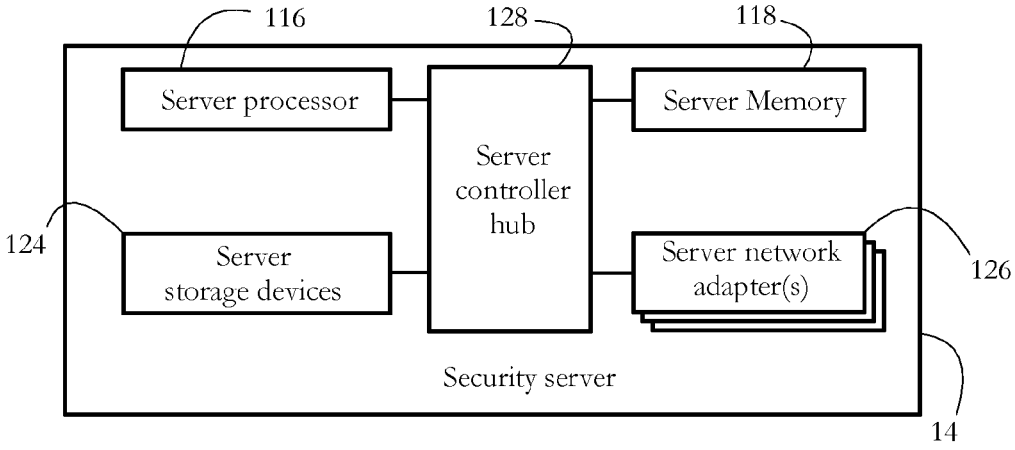


FIG. 2-B

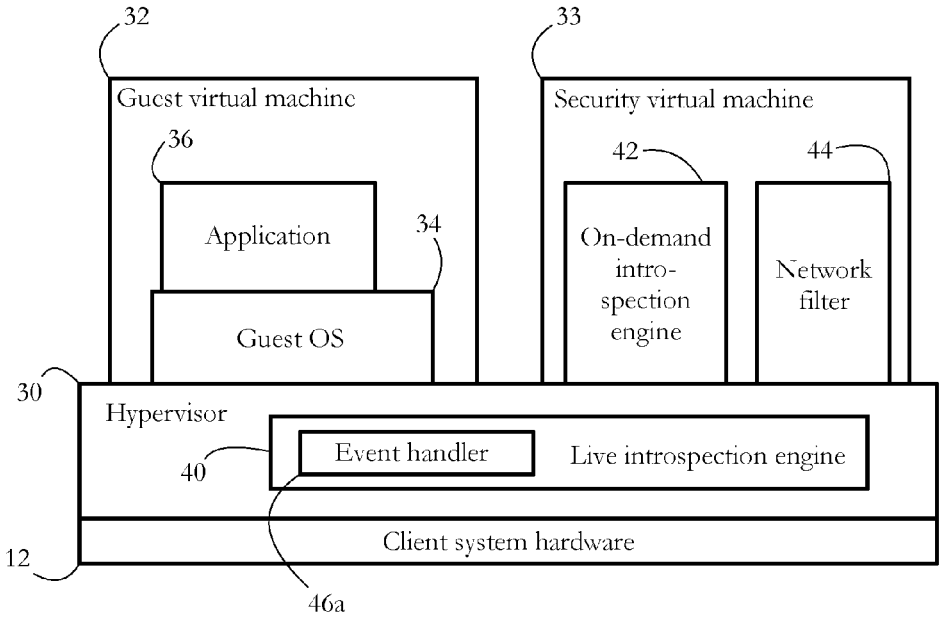


FIG. 3-A

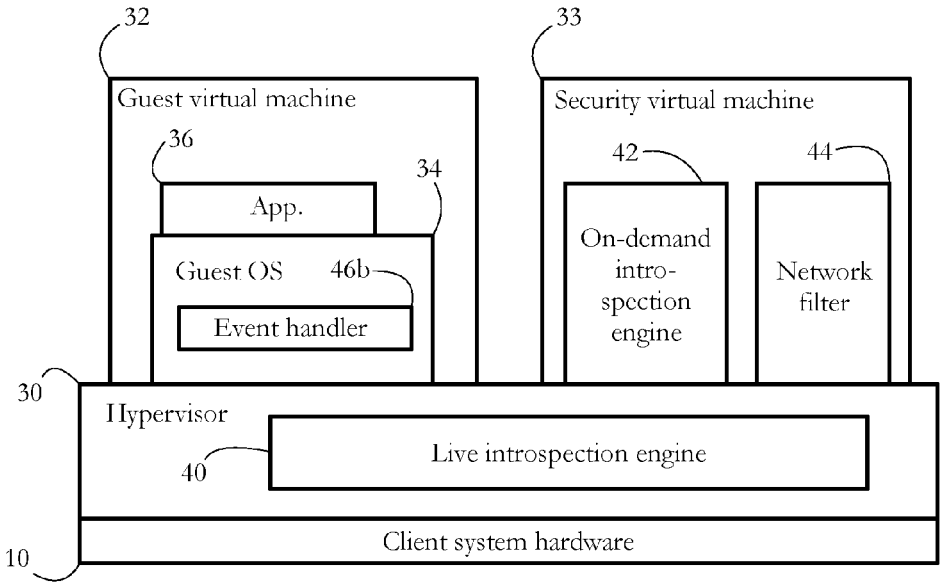


FIG. 3-B

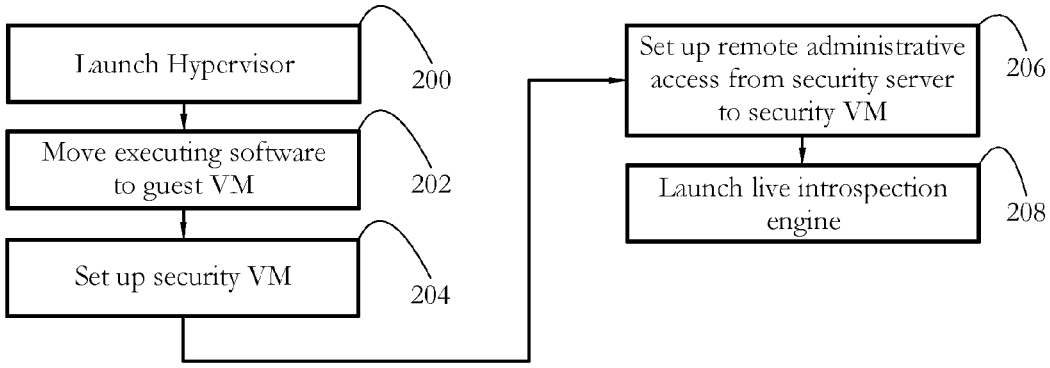


FIG. 4

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.