US 20090232300A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2009/0232300 A1

(43) Pub. Date: Sep. 17, 2009

Zucker et al.

(54) SECURING DATA USING INTEGRATED HOST-BASED DATA LOSS AGENT WITH ENCRYPTION DETECTION

(75) Inventors: **Elad Zucker**, Netanya (IL); **Eran Werner**, Raanana (IL); **Mattias Weidhagen**, Stockholm (SE)

Correspondence Address:
Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120 (US)

(73) Assignee: **McAfee, Inc.**

(21) Appl. No.: **12/076,163**

(22) Filed: **Mar. 14, 2008**

Publication Classification

(51) **Int. Cl.**
H04K 1/00 (2006.01)

(52) **U.S. Cl.** **380/2**

(57) **ABSTRACT**

A method and system for securing data in a computer system provides the capability to secure information even when it leaves the boundaries of the organization using a data loss agent integrated with encryption software. A method for securing data in a computer system comprises detecting attempted connection or access to a data destination to which sensitive data may be written, determining an encryption status of the data destination, allowing the connection or access to the data destination when the data destination is encrypted, and taking action to secure the sensitive data when the data destination is not encrypted.

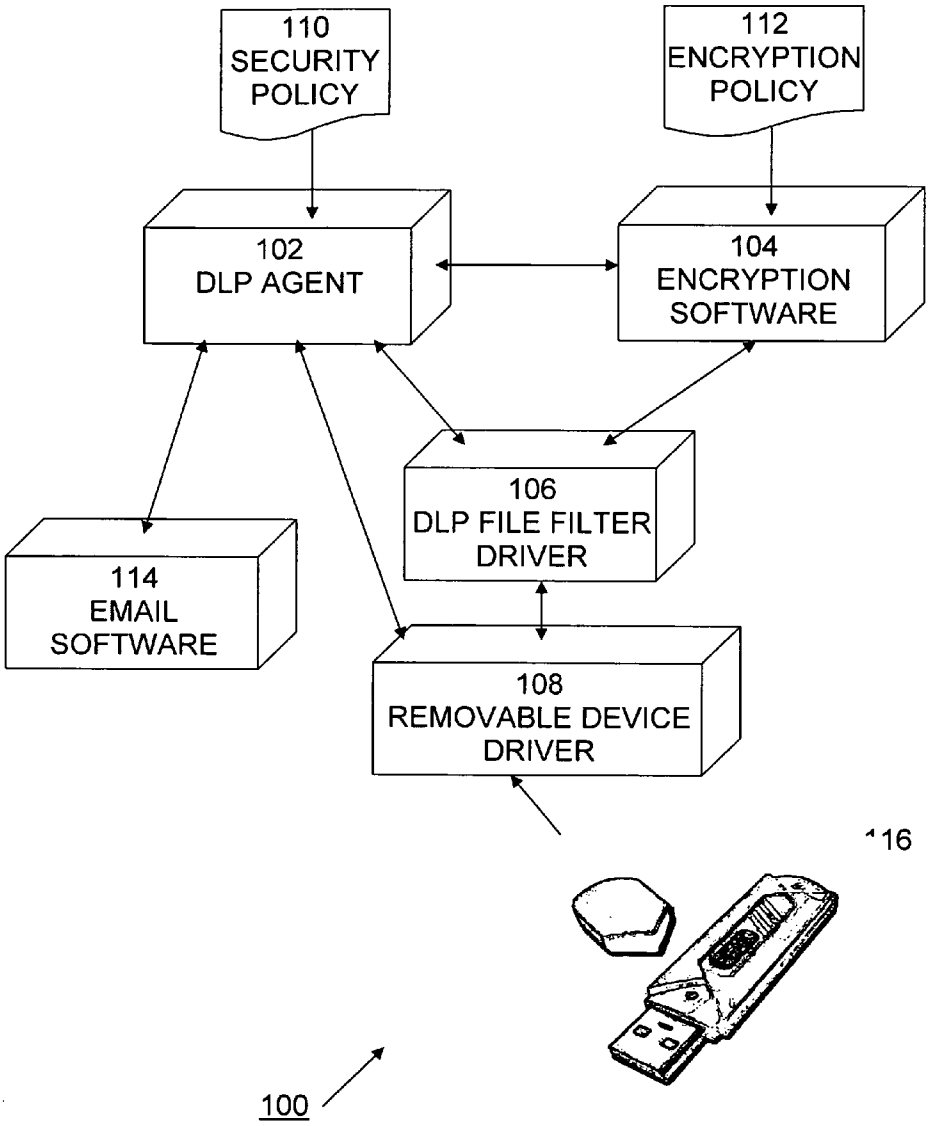


Fig. 1

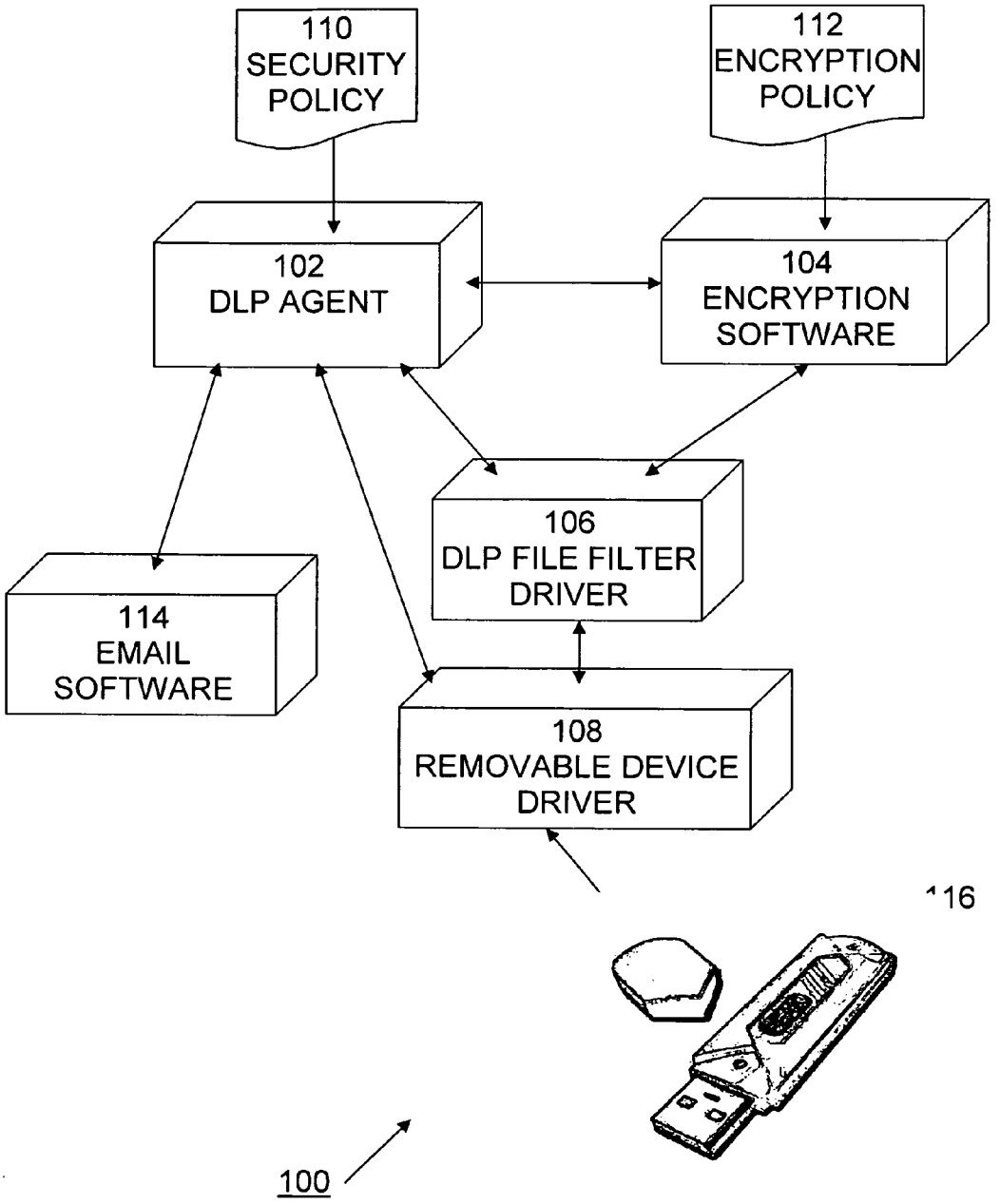

110
SECURITY
POLICY
112
ENCRYPTION
POLICY
102
DLP AGENT
104
ENCRYPTION
SOFTWARE
106
DLP FILE FILTER
DRIVER
114
EMAIL
SOFTWARE
108
REMOVABLE DEVICE
DRIVER
116
100

Fig. 2

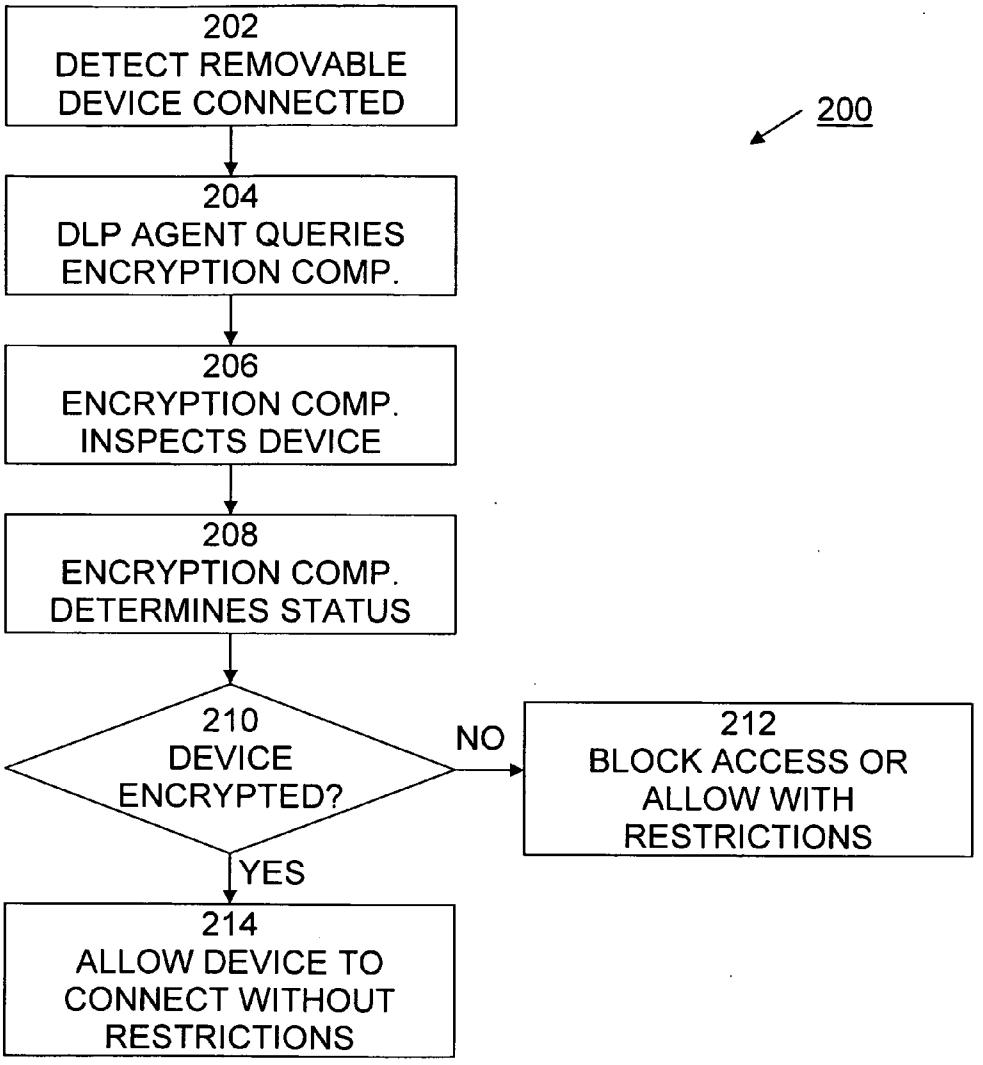

202
DETECT REMOVABLE DEVICE CONNECTED
200
204
DLP AGENT QUERIES ENCRYPTION COMP.
206
ENCRYPTION COMP. INSPECTS DEVICE
208
ENCRYPTION COMP. DETERMINES STATUS
210
DEVICE ENCRYPTED?
NO
212
BLOCK ACCESS OR ALLOW WITH RESTRICTIONS
YES
214
ALLOW DEVICE TO CONNECT WITHOUT RESTRICTIONS

Fig. 3

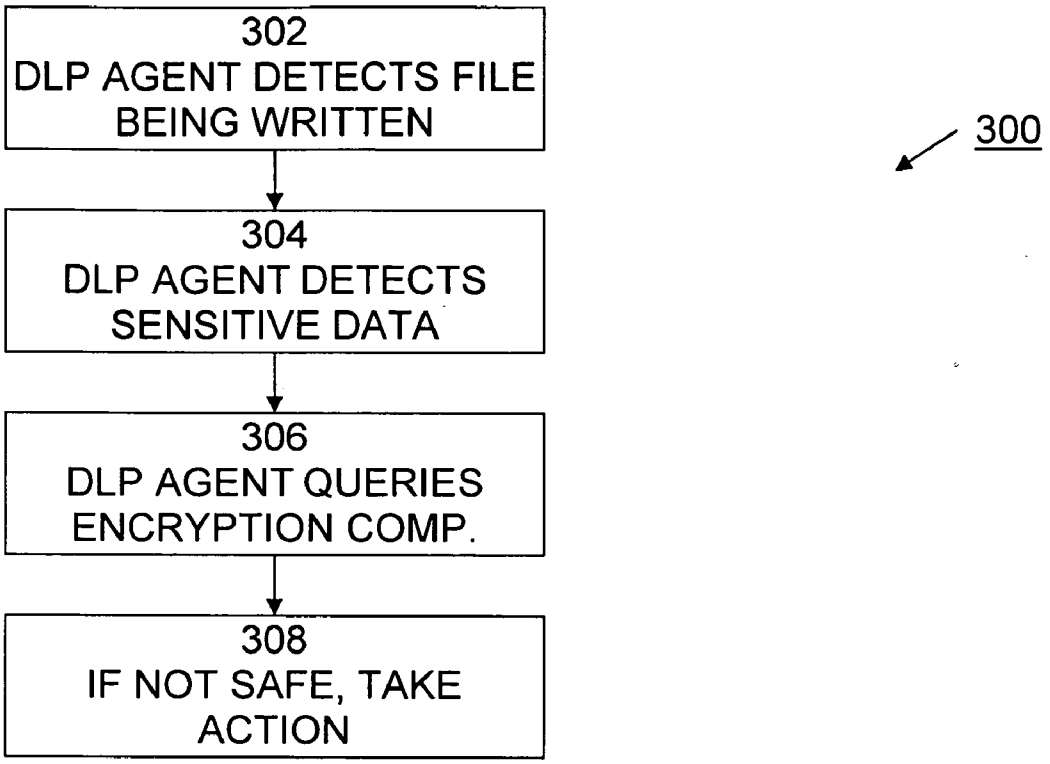

302
DLP AGENT DETECTS FILE BEING WRITTEN
304
DLP AGENT DETECTS SENSITIVE DATA
306
DLP AGENT QUERIES ENCRYPTION COMP.
308
IF NOT SAFE, TAKE ACTION
300

Fig. 4

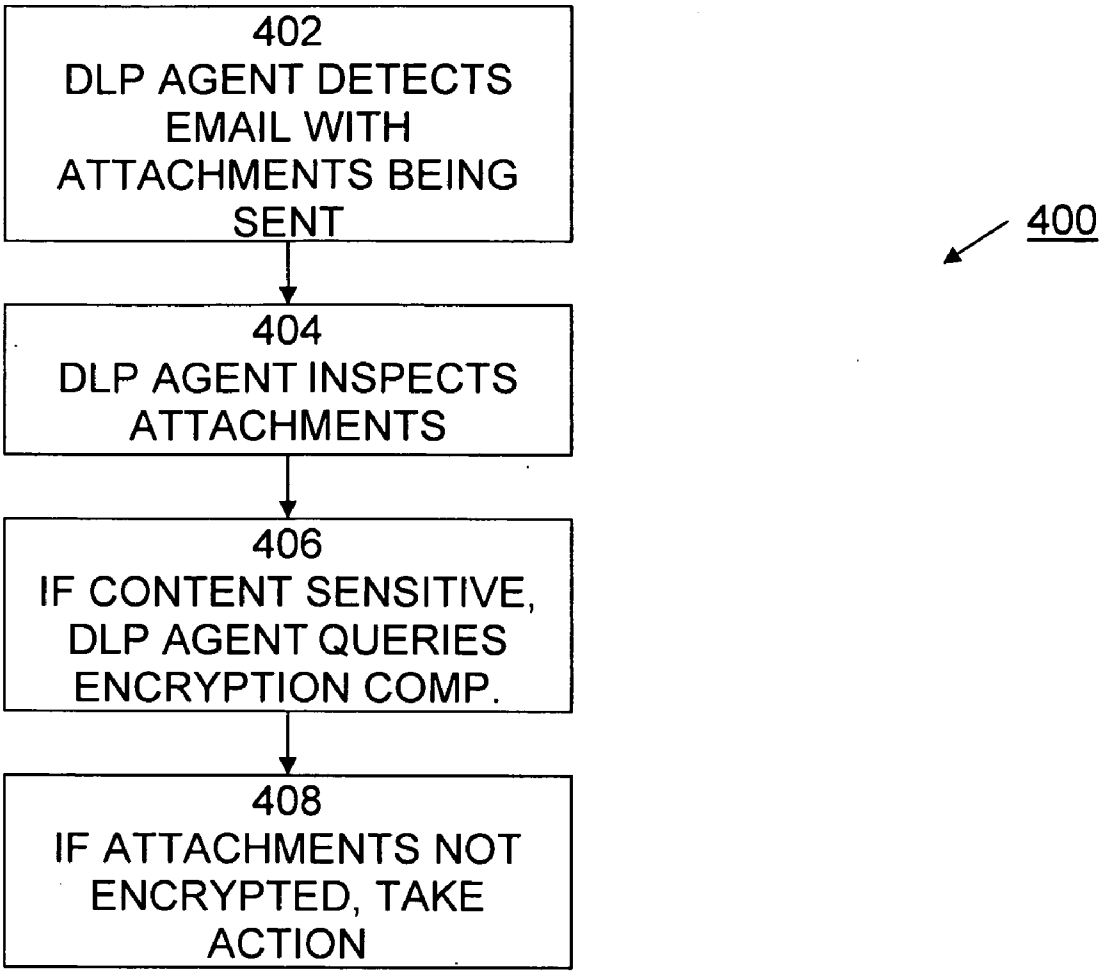
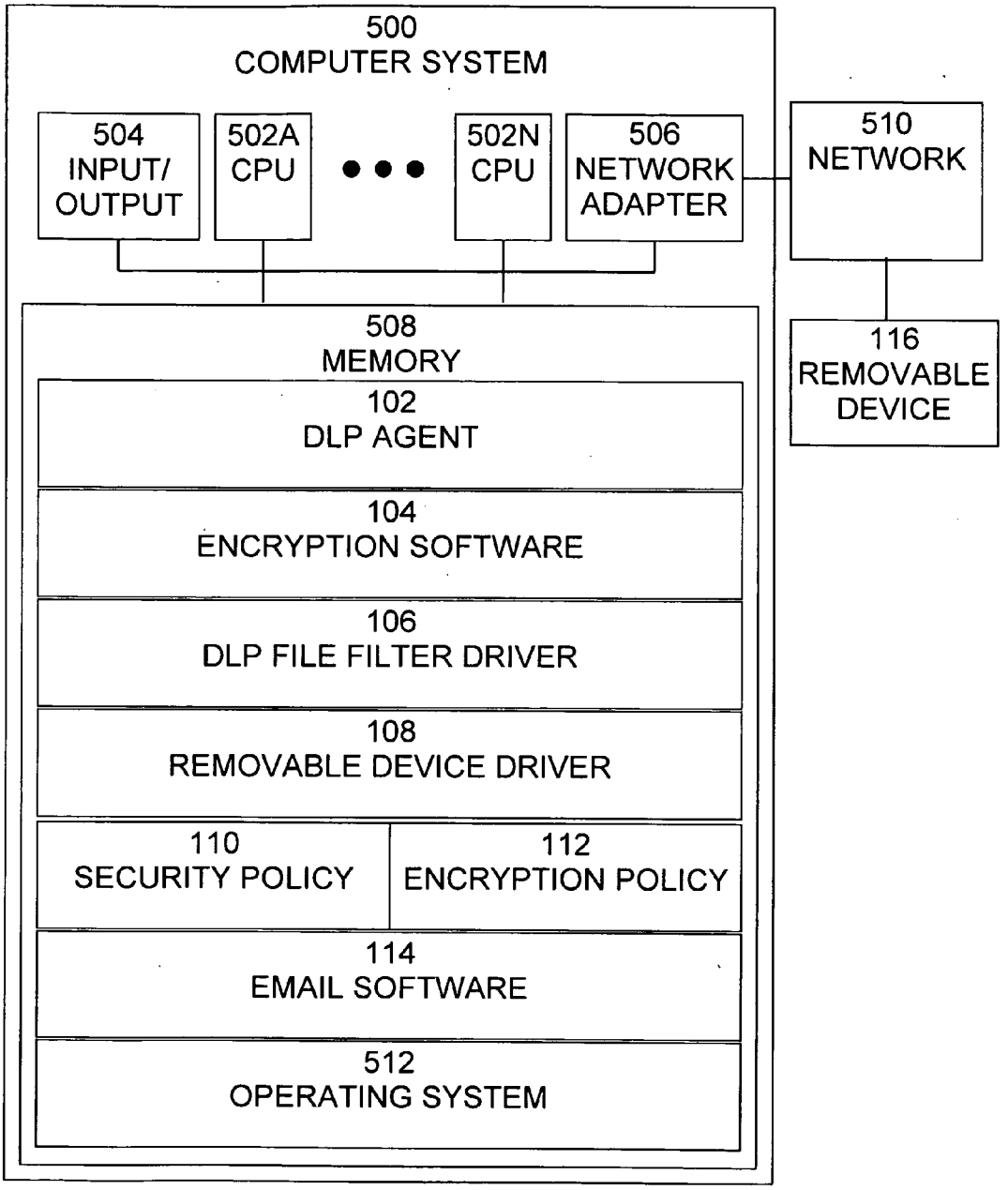

402
DLP AGENT DETECTS EMAIL WITH ATTACHMENTS BEING SENT
404
DLP AGENT INSPECTS ATTACHMENTS
406
IF CONTENT SENSITIVE, DLP AGENT QUERIES ENCRYPTION COMP.
408
IF ATTACHMENTS NOT ENCRYPTED, TAKE ACTION
400

Fig. 5


500
COMPUTER SYSTEM
504
INPUT/
OUTPUT
502A
CPU
502N
CPU
506
NETWORK
ADAPTER
510
NETWORK
508
MEMORY
102
DLP AGENT
104
ENCRYPTION SOFTWARE
106
DLP FILE FILTER DRIVER
108
REMOVABLE DEVICE DRIVER
110
SECURITY POLICY
112
ENCRYPTION POLICY
114
EMAIL SOFTWARE
512
OPERATING SYSTEM
116
REMOVABLE
DEVICE

SECURING DATA USING INTEGRATED HOST-BASED DATA LOSS AGENT WITH ENCRYPTION DETECTION

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a method and system for data loss prevention, securing data by integrating a host based data loss agent with file and full disk encryption software, as to facilitate the data loss agent with encryption detection abilities.

[0003] 2. Description of the Related Art

[0004] Host-based data loss prevention (DLP) agents are used to prevent unauthorized user activities that result in data leaving the organization in a manner that compromises a set security policy. User activity is monitored within each host by an application software agent. The agent intercepts user activities via software probes that gather information about application requests and provide that information to the agent to determine if the user request should be allowed or blocked. Data loss incidents can be of many forms, such as file copy, email, web posting and printing of sensitive content.

[0005] Host-based DLP agents are used to manage devices by blocking removable media devices or setting them as read only according to device parameters and a security policy. A DLP agent may also allow a device to work, but detect and prevent data loss by analyzing the contents of files written to the removable device, and prevent only files containing sensitive data from being written. The same applies to other channels of data loss such as email, network connectivity, web, etc.

[0006] Often, it is required that sensitive data should leave the organization by one of the above methods. Information must be collaborated or shared with suppliers, buyers, or other parts of the organization which are not controlled by the same DLP system. A need exists to secure information even when it leaves the boundaries of the organization.

SUMMARY OF THE INVENTION

[0007] The present invention provides the capability to secure information even when it leaves the boundaries of the organization using a data loss agent integrated with a file and full disk encryption software.

[0008] The data loss agent will query the encryption software for encryption detection. The data loss agent may check if a connected device is currently encrypted, or if the encryption software policy forces encryption of any data written to the device. The data loss agent may also check if files that are about to be written to removable storage are encrypted. It may allow only such files to be written and block plain text files. The same mechanism may be provided for other data loss channels such as emails, instant messaging, etc.

[0009] A method for securing data in a computer system comprises detecting attempted connection or access to a data destination to which sensitive data may be written, determining an encryption status of the data destination, allowing the connection or access to the data destination when the data destination is encrypted, and taking action to secure the sensitive data when the data destination is not encrypted. The data destination may comprise a removable device and the encryption status is determined based on attributes of the removable device or data on the removable device. The encryption status may further be determined by examining blocks and/or sectors written on the device and comparing them by reading the data with the operating system's file reading interface to determine whether or not they are encrypted. The data destination may comprise a removable device and the encryption status is determined based on an encryption policy for the removable device. The data destination may comprise a removable device and the action taken comprises blocking access to the removable device or allowing restricted access to the removable device. Blocking access to the removable device may comprise indicating that connection of the device failed and allowing restricted access to the removable device comprises allowing read-only access to the device. The data destination may comprise a removable device, the attempted access may comprise attempting to write data to the removable device and the determination of the encryption status may comprise detecting that the data being written includes sensitive data and determining if the data being written is encrypted or if it will be encrypted during or after being written to the removable device. The action taken may comprise blocking writing of the data to the removable device. The attempted access may comprise attempting to send an email message having at least one attachment and the determination of the encryption status comprises determining if the at least one attachment is encrypted. The action taken may comprise blocking sending of the email message or encrypting at least one attachment before the email message is sent.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The details of the present invention, both as to its structure and operation, can best be understood by referring to the accompanying drawings, in which like reference numbers and designations refer to like elements.

[0011] FIG. **1** is an exemplary block diagram of a software environment, such as in a host computer system, in which the present invention may be implemented.

[0012] FIG. **2** is an exemplary flow diagram of a process of securing data on a removable device when such a device is connected to a host computer system.

[0013] FIG. **3** is an exemplary flow diagram of a process of securing data on a removable device when data is to be written to the device.

[0014] FIG. **4** is an exemplary flow diagram of process of securing data attached to email messages.

[0015] FIG. **5** is an exemplary block diagram of a computer system, in which the present invention may be implemented.

DETAILED DESCRIPTION OF THE INVENTION

[0016] The present invention provides a method and system for data loss prevention, and more particularly to a method of protecting sensitive data once the data is required to leave the boundaries of the organization by means of encryption. The system includes software agents on host machines that enforce a security policy and determine when files are copied to removable storage. The agents examine various criteria to determine if the file copy is allowed and if the contents of the copied files contains sensitive data

[0017] FIG. **1** illustrates a software environment **100**, such as in a host computer system, in which the present invention may be implemented. Software environment **100** includes Data Loss Prevention (DLP) agent **102**, encryption software **104**, file filter driver **106**, removable device driver **108**, security policy **110**, encryption policy **112**, and email software

114. Additional typical software components, such as application programs, are not shown, for simplicity. Removable device **116** is accessed by software environment **100**, typically via removable device driver **108**. Removable device **116** may be any device that can be connected to a host computer system and receive data from the host computer system. This received data may be stored on removable device **116** and/or it may be transmitted by removable device **116** to one or more other devices or systems. Examples of removable devices include, without limitation, flash drives, floppy disks, CDs, DVDs, hard disks, or wired adapters, such as USB adapters, IEEE1394, etc.

[0018] DLP agent **102** is software that is typically installed on all computers in an organization. DLP agent **102**, in conjunction with DLP file filter driver **106**, intercepts all requests to access removable device **116** and allows them to proceed only if they comply with security policy **110**.

[0019] Security policy **110** is the definition of security for software environment **100**, and may also define security for one or more systems, organizations or other entities associated with software environment **100**. For an organization, security policy **110** addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, security policy **110** addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

[0020] File filter driver **106** is a driver that adds value to or modifies the behavior of another driver—specifically, the file system (not shown) of software environment **100**. File filter driver **106** can filter I/O operations for one or more file systems or file system volumes. Depending on the nature of the driver, file filter driver **106** can log, observe, or modify file system events, or the filter can even prevent file system events from occurring.

[0021] Encryption software **104** controls, determines, and performs encryption of data in software environment **100**, as specified by encryption policy **112**. Encryption policy **112** specifies what data and/or types of data are to be encrypted based on a number of conditions, such as the location of the data, the locations and/or devices to which the data is to be written, etc. Encryption software **104** includes an encryption detection application program interface (API), which provides the capability for other software, such as DLP agent **102**, to request and control encryption software **104** to perform inspection of data for encryption or lack of encryption.

[0022] By providing the encryption detection API from encryption software **104** to DLP agent **102**, and using the file write blocking and email blocking capabilities of the DLP agent, DLP agent **102** has the ability to secure data with encryption detection in a number of situations. For example, DLP agent **102** provides the capability to detect the connection of a removable device **116** and to block access to the device, unless the device or the data on the device is encrypted in accordance with encryption policy **112**. Likewise, DLP agent **102** provides the capability to block sensitive content from being written to removable device **116** unless the content is encrypted in accordance with encryption policy **112**. Further, DLP agent **102** provides the capability to block email attachments to email messages being processed by email software **114**, which include sensitive data that are not encrypted in accordance with encryption policy **112**.

[0023] A flow diagram of a process **200** of securing data on a removable device when such a device is connected to a host computer system is shown in FIG. **2**. It is best viewed in conjunction with FIG. **1**. Process **200** begins with step **202**, in which DLP agent **102** detects that a removable device **116** has been connected to the host computer. In step **204**, DLP agent **102** queries the encryption software component **104** to determine if the removable device **116** is safe. This includes passing device information relating to the removable device **116** to the encryption software. In step **206**, the encryption software **104** inspects the removable device **116** and in step **208** determines whether or not the device is safe, i.e. properly encrypted. Encryption software **104** can determine that the device is encrypted based on attributes of the device or data on the device, such as attributes indicating encryption, or by examining blocks and/or sectors written on the device and comparing them with data read by the operating system file interface to determine whether or not they are encrypted. Alternatively, or in addition, encryption software **104** can determine that the device is encrypted by checking the encryption policy repository **112** to determine if the policy will force files written to the device to undergo encryption. If one of these is positive the encryption software will reply that the device is safe.

[0024] In step **210**, DLP agent **102** determines how to proceed based on the encryption status returned by encryption software **104** in step **208**. If removable device **116** is not safe, then process **200** proceeds to step **212**, in which DLP agent **102** prevents sensitive data from being written to the removable device **116**. Such prevention may be accomplished, for example, by blocking access to the removable device **116**, such as by indicating to the host computer system that connection of the device failed, or by allowing restricted access in accordance with the DLP security policy **110**, such as read-only access, to the device. If removable device **116** is safe, then process **200** proceeds to step **214**, in which DLP agent **102** allows sensitive data to be written to removable device **116**. In this case, the sensitive data written to removable device **116** will be encrypted by encryption software **104** in accordance with encryption policy **112**.

[0025] A flow diagram of a process **300** of securing data on a removable device when data is to be written to the device is shown in FIG. **3**. It is best viewed in conjunction with FIG. **1**. Process **300** begins with step **302**, in which DLP agent **102** identifies that a file is being written to a removable device **116**. Typically, this is done by the DLP agent's file filter driver **106** detecting an attempt to write data to removable device **116**. In step **304**, DLP agent **102** further detects that the data being written includes sensitive data according to the DLP security **110** policy and the DLP agent's content detecting and tracking mechanism. In step **306**, DLP agent **102** queries the encryption software **104** to determine if the file being written is encrypted or alternatively if it will be encrypted by the encryption software **104** during or after being written to removable device **116**. The information provided by DLP agent **102** to encryption software **104** relating to the query may include information such as the logged in user, the files that are being written, and the destination (device and location) that the files are being written to. This information can be used by encryption software **104** to determine if the files are or will be encrypted. In step **308**, if the encryption software **104** cannot guarantee that written data are or will be encrypted, the DLP agent **102** takes action to secure the data, such as blocking the file write request. A flow diagram of a

process **400** of securing data attached to email messages is shown in FIG. **4**. It is best viewed in conjunction with FIG. **1**. Process **400** begins with step **402**, in which DLP agent **102** detects that an email containing attachments is being sent by email software. In step **404**, DLP agent **102** inspects the contents or other attributes of the attachments as to determine if they contain sensitive data. In step **406**, if the attachments are sensitive, DLP agent **102** queries encryption software **104** to determine if the attachments are encrypted. In step **408**, if the attachments are not identified as encrypted, DLP agent **102** takes action to secure the sensitive data, such as by blocking the email software from sending the email.

[0026] An exemplary block diagram of a computer system **500**, in which the present invention may be implemented, is shown in FIG. **5**. Computer system **500** is typically a programmed general-purpose computer system, such as a personal computer, workstation, server system, and minicomputer or mainframe computer. Computer system **500** includes one or more processors (CPUs) **502**A-**502**N, input/output circuitry **540**, network adapter **506**, and memory **508**. CPUs **502**A-**502**N execute program instructions in order to carry out the functions of the present invention. Typically, CPUs **502**A-**502**N are one or more microprocessors, such as an INTEL PENTIUM® processor. FIG. **5** illustrates an embodiment in which computer system **500** is implemented as a single multi-processor computer system, in which multiple processors **502**A-**502**N share system resources, such as memory **508**, input/output circuitry **504**, and network adapter **506**. However, the present invention also contemplates embodiments in which computer system **500** is implemented as a plurality of networked computer systems, which may be single-processor computer systems, multi-processor computer systems, or a mix thereof.

[0027] Input/output circuitry **504** provides the capability to input data to, or output data from, computer system **500**. For example, input/output circuitry may include input devices, such as keyboards, mice, touchpads, trackballs, scanners, etc., output devices, such as video adapters, monitors, printers, etc., and input/output devices, such as, modems, etc. Network adapter **506** interfaces computer system **500** with network **510**. Network **510** may include one or more standard local area networks (LAN) or wide area networks (WAN), such as Ethernet, Token Ring, the Internet, or a private or proprietary LAN/WAN. Network **510** may further include networks that allow connection of removable devices **116**. Such networks may include standard device connection interfaces, such as Universal Serial Bus (USB), IEEE 1394, External Serial Advanced Technology Attachment (eSATA), Compact Flash, Secure Digital, etc.

[0028] Memory **508** stores program instructions that are executed by, and data that are used and processed by, CPUs **502**A-N to perform the functions of computer system **500**. Memory **504** may include electronic memory devices, such as random-access memory (RAM), read-only memory (ROM), programmable read-only memory (PROM), electrically erasable programmable read-only memory (EEPROM), flash memory, etc., and electro-mechanical memory, such as magnetic disk drives, tape drives, optical disk drives, etc., which may use an integrated drive electronics (IDE) interface, or a variation or enhancement thereof, such as enhanced IDE (EIDE) or ultra direct memory access (UDMA), or a small computer system interface (SCSI) based interface, or a variation or enhancement thereof, such as fast-SCSI, wide-SCSI, fast and wide-SCSI, etc, or a fiber channel-arbitrated loop (FC-AL) interface.

[0029] The contents of memory **508** varies depending upon the function that computer system **500** is programmed to perform. In the example shown in FIG. **5**, memory **508** includes Data Loss Prevention (DLP) agent **102**, encryption software **104**, file filter driver **106**, removable device driver **108**, security policy **110**, encryption policy **112**, and email software **114**. Additional typical software components, such as application programs, are not shown, for simplicity. DLP agent **102**, in conjunction with DLP file filter driver **106**, intercepts all requests to access removable device **116** and allows them to proceed only if they comply with security policy **110**. Security policy **110** is the definition of security for computer system **500**, and may also define security for one or more systems, organizations or other entities associated with computer system **500**. File filter driver **106** is a driver that adds value to or modifies the behavior of another driver—specifically, the file system (included in operating system **512**) of computer system **500**. Encryption software **104** controls, determines, and performs encryption of data in software environment **100**, as specified by encryption policy **112**. Encryption policy **112** specifies what data and/or types of data are to be encrypted based on a number of conditions, such as the location of the data, the locations and/or devices to which the data is to be written, etc. Removable device driver **108** provides the capability to connect and access removable device **116**. Operating system **512** provides overall system functionality.

[0030] As shown in FIG. **5**, the present invention contemplates implementation on a system or systems that provide multi-processor, multi-tasking, multi-process, and/or multi-thread computing, as well as implementation on systems that provide only single processor, single thread computing. Multi-processor computing involves performing computing using more than one processor. Multi-tasking computing involves performing computing using more than one operating system task. A task is an operating system concept that refers to the combination of a program being executed and bookkeeping information used by the operating system. Whenever a program is executed, the operating system creates a new task for it. The task is like an envelope for the program in that it identifies the program with a task number and attaches other bookkeeping information to it. Many operating systems, including UNIX®, OS/2®, and Windows®, are capable of running many tasks at the same time and are called multitasking operating systems. Multi-tasking is the ability of an operating system to execute more than one executable at the same time. Each executable is running in its own address space, meaning that the executables have no way to share any of their memory. This has advantages, because it is impossible for any program to damage the execution of any of the other programs running on the system. However, the programs have no way to exchange any information except through the operating system (or by reading files stored on the file system). Multi-process computing is similar to multi-tasking computing, as the terms task and process are often used interchangeably, although some operating systems make a distinction between the two.

[0031] It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are

capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include storage media, examples of which include, but are not limited to, floppy disks, hard disk drives, CD-ROMs, DVD-ROMs, RAM, and, flash memory, as well as transmission media, examples of which include, but are not limited to, digital and analog communications links.

[0032] Although specific embodiments of the present invention have been described, it will be understood by those of skill in the art that there are other embodiments that are equivalent to the described embodiments. Accordingly, it is to be understood that the invention is not to be limited by the specific illustrated embodiments, but only by the scope of the appended claims.

What is claimed is:

1. A method for securing data in a computer system comprising:
- detecting attempted connection or access to a data destination to which sensitive data may be written;
- determining an encryption status of the data destination;
- allowing the connection or access to the data destination when the data destination is encrypted; and
- taking action to secure the sensitive data when the data destination is not encrypted.

2. The method of claim **1**, wherein the data destination comprises a removable device and the encryption status is determined based on attributes of the removable device or data on the removable device.

3. The method of claim **2**, wherein the encryption status is determined by examining blocks and/or sectors written on the device to determine whether or not they are encrypted.

4. The method of claim **1**, wherein the data destination comprises a removable device and the encryption status is determined based on an encryption policy for the removable device.

5. The method of claim **1**, wherein the data destination comprises a removable device and the action taken comprises blocking access to the removable device or allowing restricted access to the removable device.

6. The method of claim **5**, wherein blocking access to the removable device comprises indicating that connection of the device failed and allowing restricted access to the removable device comprises allowing read-only access to the device.

7. The method of claim **1**, wherein the data destination comprises a removable device, the attempted access comprises attempting to write data to the removable device and the determination of the encryption status comprises:
- detecting that the data being written includes sensitive data; and
- determining if the data being written is encrypted or if it will be encrypted during or after being written to the removable device.

8. The method of claim **7**, wherein the action taken comprises blocking writing of the data to the removable device.

9. The method of claim **1**, wherein the attempted access comprises attempting to send an email message having at least one attachment and the determination of the encryption status comprises determining if the at least one attachment is encrypted.

10. The method of claim **9**, wherein the action taken comprises blocking sending of the email message before the email message is sent.

11. A computer system having secure handling of data comprising:
- a processor operable to execute computer program instructions;
- a memory operable to store computer program instructions executable by the processor; and
- computer program instructions stored in the memory and executable to implement:
- a data loss prevention agent to detect attempted connection or access to a data destination to which sensitive data may be written and to query encryption software for an encryption status of the data destination, allow the connection or access to the data destination when the data destination is encrypted, and take action to secure the sensitive data when the data destination is not encrypted; and
- encryption software to determine an encryption status of the data destination.

12. The system of claim **11**, wherein the data destination comprises a removable device and the encryption software determines the encryption status based on attributes of the removable device or data on the removable device.

13. The system of claim **12**, wherein the encryption software determines the encryption status by examining blocks and/or sectors written on the device and comparing the content by reading the files using the file system interface to determine whether or not they are encrypted.

14. The system of claim **11**, wherein the data destination comprises a removable device and the encryption software determines the encryption status based on an encryption policy for the removable device.

15. The system of claim **11**, wherein the data destination comprises a removable device and the action taken by the data loss prevention agent comprises blocking access to the removable device or allowing restricted access to the removable device.

16. The system of claim **15**, wherein the data loss prevention agent blocking access to the removable device comprises indicating that connection of the device failed and allowing restricted access to the removable device comprises allowing read-only access to the device.

17. The system of claim **11**, wherein the data destination comprises a removable device, the attempted access comprises attempting to write data to the removable device and the encryption software determines the encryption status by:
- detecting that the data being written includes sensitive data; and
- determining if the data being written is encrypted or if it will be encrypted during or after being written to the removable device.

18. The system of claim **17**, wherein the action taken by the data loss prevention agent comprises blocking writing of the data to the removable device.

19. The system of claim **11**, wherein the attempted access comprises attempting to send an email message having at least one attachment and the encryption software determines the encryption status by determining if the at least one attachment is encrypted.

20. The system of claim **19**, wherein the action taken by the data loss prevention agent comprises blocking sending of the

email message or encrypting the at least one attachment before the email message is sent.

21. A computer program product for securing data in a computer system comprising:

a computer readable storage medium;

computer program instructions, recorded on the computer readable storage medium, executable by a processor, for detecting attempted connection or access to a data destination to which sensitive data may be written;

determining an encryption status of the data destination;

allowing the connection or access to the data destination when the data destination is encrypted; and

taking action to secure the sensitive data when the data destination is not encrypted.

22. The computer program product of claim **21**, wherein the data destination comprises a removable device and the encryption status is determined based on attributes of the removable device or data on the removable device.

23. The computer program product of claim **22**, wherein the encryption status is determined by examining blocks and/or sectors written on the device and comparing the content by reading the files using the file system interface to determine whether or not they are encrypted.

24. The computer program product of claim **21**, wherein the data destination comprises a removable device and the encryption status is determined based on an encryption policy for the removable device.

25. The computer program product of claim **21**, wherein the data destination comprises a removable device and the action taken comprises blocking access to the removable device or allowing restricted access to the removable device.

26. The computer program product of claim **25**, wherein blocking access to the removable device comprises indicating that connection of the device failed and allowing restricted access to the removable device comprises allowing read-only access to the device.

27. The computer program product of claim **21**, wherein the data destination comprises a removable device, the attempted access comprises attempting to write data to the removable device and the determination of the encryption status comprises:

detecting that the data being written includes sensitive data; and

determining if the data being written is encrypted or if it will be encrypted during or after being written to the removable device.

28. The computer program product of claim **27**, wherein the action taken comprises blocking writing of the data to the removable device.

29. The computer program product of claim **21**, wherein the attempted access comprises attempting to send an email message having at least one attachment and the determination of the encryption status comprises determining if the at least one attachment is encrypted.

30. The computer program product of claim **29**, wherein the action taken comprises blocking sending of the email message or encrypting the at least one attachment before the email message is sent.

* * * * *