

McAfee DLP Prevent

Enforce policies to protect your sensitive information

Key Advantages

Leverage existing infrastructure

- Protect corporate email through integration with MTA gateways using SMTP with X-Headers for blocking, bouncing, encrypting, quarantining, and redirecting
- Deliver traffic enforcement through integration with ICAP-compliant web proxies to block content violations over HTTP, HTTPS, IM, FTP, and webmail

Proactively enforce policies for all types of information

- Protect more than 300 unique content types
- Enforce policies for the information you know is sensitive as well as the non-obvious information you may not know about
- Scale to support hundreds of thousands of concurrent connections

Classify, analyze, and address data leaks

- Filter and control sensitive information to protect against known and unknown risks
- Index and enforce fine-grained security policies for all types of content
- Apply policies regarding internal file share access to prevent users from accessing information or repositories in an unauthorized manner

The more people share information electronically, the greater the likelihood that someone will inadvertently or intentionally send sensitive data to an unauthorized individual—and put confidential corporate data at risk. Whether through email, web, instant messaging (IM), or FTP, information can leave the company across many different electronic channels. This creates a tremendous challenge for corporate security and compliance officers. Some messages or transactions are allowable but should be encrypted to ensure data privacy. Other types of messages, or their recipients, are simply unacceptable at any time, and these transmissions must be blocked. Enforcing the right policies at the right time is essential to ensuring data security, regulatory compliance, and intellectual property protection.

Enforce Security Policies for Data in Motion

Across each division of every company, individuals share data using multiple applications and a variety of protocols. To prevent against inadvertent or intentional data leakage, companies must be able to proactively protect sensitive information from leaving the network and enforce correct business processes.

McAfee Data Loss Prevention (DLP) Prevent enforces policies for information leaving the network through email, webmail, Instant Messaging, wikis, blogs, portals, HTTP/HTTPS, and FTP transfers by integrating with Message Transfer Agent (MTA) gateways using Simple Mail Transfer Protocol (SMTP) or ICAP-compliant web proxies. Upon encountering a policy violation, McAfee DLP Prevent allows you to take a variety of actions, including applying encryption, blocking, redirecting, quarantining, and more—so you can ensure compliance with regulations governing the privacy of sensitive information and reduce the risk of security threats.

Integrate with Web Proxies and MTAs for Greater Protection

McAfee DLP Prevent integrates with web proxies (using ICAP) and with MTAs (using X-Headers) for the required action. Because it terminates unauthorized transactions at the application layer rather than simply dropping the TCP session, which does nothing to modify application behavior, McAfee DLP Prevent alerts the initiating

application that the transmission was denied due to a policy breach. This ensures greater data protection for your organization because McAfee DLP Prevent learns what must be protected and stops the application from reattempting the same behavior.

Protect Known and Unknown Sensitive Information

With the ability to classify more than 300 different content types, McAfee DLP Prevent helps you ensure that the security of the information you know remains confidential—Social Security numbers, credit card numbers, and financial data—and learn what non-obvious information or documents require protection, such as highly complex intellectual property. McAfee DLP Prevent includes a wide range of built-in policies, ranging from compliance to acceptable use to intellectual property, enabling you to match entire and partial documents to a comprehensive set of rules, so you can protect all your sensitive information, both known and unknown.

Customize Views and Incident Reports

Using the McAfee ePolicy Orchestrator® (McAfee ePO™) management console, you can customize summary views of security incidents and subsequent actions based on any two contextual pivot points. List and detail views, as well as summary views with trending, are available at your fingertips. McAfee DLP Prevent also includes a

Specifications

Capture and index capacity

- Index up to 80 TB of information and up to 50 million documents on the McAfee DLP 4400 appliance

System throughput

- Up to 150 Mbps of full content analysis, indexing, and storage throughput

Network integration

- Integrates into the network as an off-path appliance that is active within the data path using MTAs and ICAP-compliant web proxies

Content types

Supports file classification of more than 300 content types, including:

- Microsoft Office documents
- Multimedia files
- P2P
- Source code
- Design files
- Archives
- Encrypted files

Protocols supported

Supports HTTP, HTTPS, FTP, and Instant Messaging protocols via the ICAP protocol to an ICAP-compliant proxy. Please refer to your proxy vendor for protocols supported by your proxy. Supports SMTP via integration with MTAs.

Built-in policies

Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use. Enables complete customization of rules to meet business-specific needs by leveraging the McAfee capture database.

large number of pre-built reports, each of which can be viewed, saved for later use, or scheduled for periodic delivery.

Complex Data Classification

McAfee DLP Prevent empowers your organization to protect all kinds of sensitive data—from common, fixed-format data to complex, highly variable intellectual property. By combining these object-classification mechanisms, McAfee DLP Prevent leverages a highly accurate, detailed classification engine that blocks sensitive information and identifies hidden or unknown risks. Object classification mechanisms include:

- *Multilayer classification*—Covers both contextual information and content in a hierarchical format

- *Document registration*—Includes biometric signatures of information as it changes
- *Grammar analysis*—Detects grammar or syntax of anything from text documents to spreadsheets to source code
- *Statistical analysis*—Tracks how many times a signature, grammar, or biometric match occurred in a particular document or file
- *File classification*—Identifies content types regardless of the extension applied to the file or compression

Specifications: McAfee DLP 4400 Appliance

Component	Description
Mother Board	Intel TimberCreek System (S5520URR)
CPU	2 x Intel X5660 12 M Cache, 2.8 GHz (6 cores)
Memory	24 GB P1333 DDR3 memory
Raid Controller	Intel RS2MB044 raid controller
Power Supply	2 x 760 W hot-swap power supply modules
Hard Drives	12 x Seagate Constellation ES 1T 7200 rpm 3 1/2" SATA drives
NIC Card	Intel Dual Copper 1 Gbps Ethernet I/O module
DVD Drive	SATA DVD-ROM
IPMI	Intel Remote Management Modules 3 (AXRMM3)
Product Size	2 rack units (2U)

Specifications: Virtual Machine

McAfee DLP Prevent is available as a virtual appliance that can run on VMware ESX or VMware ESXi 4.1 servers. Below are the minimum hardware requirements for running the virtual appliance.

Component	Requirement
CPU	Intel Quad Core
Memory	8 GB RAM
Hard disk drive(s)	Drive 1: Minimum size, 128 GB for VM software Drive 2: Minimum size, 640 GB for DLP virtual image
Network ports	1 port for McAfee DLP Prevent application
BIOS	Enable VT thread

