McAfee

Together is power.

McAfee DLP Prevent

Enforce policies to protect your sensitive information

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. Information can leave the company across many different channels—email, web, instant messaging (IM), or FTP. Some messages or transactions are allowable but need to be encrypted to ensure data privacy. Other types of communications are simply unacceptable at any time and must be blocked. Enforcing the right policies at the right time is essential to ensuring data security, regulatory compliance, and intellectual property protection.

Enforcement of Security Policies for Data in Motion

Across each department of every company, individuals share data using multiple applications and a variety of protocols. Guard against inadvertent or intentional data loss by proactively protecting sensitive information from leaving the network and enforce correct business processes.

McAfee® DLP Prevent helps you enforce policies for information leaving the network through email, webmail, IM, wikis, blogs, portals, HTTP/HTTPS, and FTP transfers by integrating with message transfer agent 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.

Fully Unified with McAfee ePolicy Orchestrator Software

McAfee DLP Prevent is fully unified with McAfee® ePolicy Orchestrator® (McAfee ePO™) software and McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) with common policy, incident and case management. Administrators can create a single email and web protection policy in McAfee ePO software and

Key Advantages

Leverage existing infrastructure

- Protect corporate email through integration with message transfer agent (MTA) gateways using SMTP with X headers for blocking, bouncing, encrypting, quarantining, and redirecting.

- Deliver traffic enforcement through integration with internet content adaptation protocol (ICAP)-compliant web proxies to block content violations over HTTP, HTTPS, IM, FTP, and webmail.

Connect With Us

deploy it to endpoints and the network. In addition, McAfee DLP Endpoint and McAfee DLP Prevent share a common classification engine that allows for a single email and web policy. Common dictionaries and regular expression (regex) syntax provide continuity for creating common web and email protection rules. With centralized management, McAfee DLP solutions provide single-pane-of-glass visibility and help increase business efficiency and reduce administrative overhead.

Monitor Mobile Email

McAfee® DLP Prevent for Mobile Email provides content-aware protection to mobile email by intercepting emails downloaded to mobile device via ActiveSync proxy with DLP capability. In addition, it is capable of intercepting ActiveSync on both on-premises Microsoft Exchange and on Microsoft Office 365 Hosted Exchange. It is fully managed from McAfee ePO software and is included as part of the McAfee DLP Prevent license. It does not require any agent installation on mobile devices. With McAfee DLP Prevent for Mobile Email, enterprises can monitor email for compliance and evidence collection and can protect both managed and unmanaged mobile devices.

Integration 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 attempting the same behavior again.

Protection for 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 are aware of remains confidential—Social Security numbers, credit card numbers, and financial data. It also helps you learn what 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.

Customizable Views and Incident Reports

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

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 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.

Specifications

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.

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 signatures of information as it changes

- **Grammar analysis:** Detects grammar or syntax of everything from text documents to spreadsheets to source code

- **Statistical analysis:** Tracks the number of 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

Forensic and Rule Tuning Capability

Unique capture technology enables you to leverage your own historical data to implement a much faster, efficient deployment--no more guessing, months of trial and error, or business disruption. This makes it easy to fine-tune DLP rules (including classification tuning) for accuracy based on your ever-changing business needs. Capture technology can also aid in forensic investigation by acting as a digital recorder and by replaying after-the-fact DLP incidents for thorough investigation. Capture technology is available either as a virtual environment, or as a 2U 16TB storage array connected to a NDLP 6600 appliance via a SAS cable.

Form Factor and Appliance Options

McAfee DLP Prevent is available as a hardware appliance or a virtual appliance. See the **McAfee DLP 6600 hardware appliance data sheet** for additional details.

Content types

Supports file classification of more than 300 content types:

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

Protocols supported

Supports HTTP, HTTPS, FTP, and IM 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.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com