

McAfee Host Data Loss Prevention

Don't be the next big data loss media story

Are you losing data without even knowing it? Your customer information, intellectual property, financial data, and personnel files may be leaving your corporate borders right now. And the perpetrators are not only hackers—they are also your own employees. Accidental and malicious data loss can occur through common channels such as email, web posting, USB drives, and printing—potentially costing you millions.

Key Advantages

Unrivaled protection

- Prevent data loss anywhere your data goes: at work, at home, or on the road

Comprehensive device management

- Specify detailed content-based filtering, monitoring, and blocking of confidential data on any removable storage device

Multi-layered protection

- Ensure that data is protected on all endpoints, independent of the device type

ePO centralized management

- Leverage your McAfee security risk management architecture to prevent data loss

Complete visibility

- Prove internal and regulatory compliance measures to auditors, senior management, and other stakeholders

Stop Data Loss Before It Happens

Every day companies like yours fall victim to massive data loss through malicious and unintentional leakage of information. A recent study found that more than 75 percent of Fortune 1000 companies had fallen victim to accidental or malicious data leakage. In a recent study, over 55 percent of employees use portable devices to take confidential data out of the workplace every week.¹ The costs to companies resulting from data breaches and remediation are extremely high. In 2008, the average was \$6.65 million.²

What if you could easily and effectively stop data loss? What if you could help manage compliance with industry and government regulations at the same time? Now you can with a solution for monitoring, auditing, and controlling user behavior with your sensitive data.

Protect and Comply

Gain complete visibility and control the transfer of your most critical data with McAfee® Host Data Loss Prevention (Host DLP). Instantly monitor and prevent confidential data loss at work, at home, and on the road. Host DLP protects your organization from the risks of financial loss, brand damage, lost customers, competitive disadvantage, and non-compliance.

With Host DLP, you can quickly and easily monitor real-time events, apply centrally managed security policies to regulate and restrict how employees use and transfer sensitive data, and generate detailed forensics reports without affecting your daily business activities. Protect your enterprise from data loss threats originating from the inside,

such as email, IM, CD burns, web posting, USB copying, and printing. You also stop confidential data loss initiated by Trojans, worms, and file-sharing applications that hijack employee credentials without their knowledge.

Protect Without Disrupting

Prevent data loss and leakage without interrupting legitimate business activities, even when data is modified, copied, pasted, compressed, or encrypted. Protect content for more than 390 data file types. Data is classified using dictionaries and regular expressions (including validating algorithm). In addition, unique tagging technology allows for tagging of data according to its original location, or the application that generated the data. Classification can also be done by registering sensitive documents.

Compliance Management Simplified

Easy management through McAfee ePolicy Orchestrator® (ePO™) enables event monitoring and incident details to prove internal and regulatory compliance measures to auditors, board members, and other stakeholders. Host DLP integration with ePO allows you to easily collect critical usage data, such as sender, recipient, time stamp, and data evidence. With a click of a button, ePO enables event monitoring and detailed reports to prove to auditors, senior management, and other stakeholders that internal and regulatory compliance measures are in place.

The Payoff: Unrivaled Data Protection

Gain full visibility and control over the data leaving your endpoints, so you can stop the losses—and the negative headlines—before they happen.

¹ Illuminas 2007, Threats Within Volume II Data Loss Disaster
² Ponemon Institute's 2008 Cost of Data Breach Study

System Requirements

ePO Server

- Operating systems
- Microsoft® Server 2003 SP1, 2003 R2

Desktop and laptop endpoints

- Operating systems
- Microsoft Windows® Vista
- Microsoft Windows® XP
- Professional SP1 or higher
- Microsoft Windows 2000 SP4 or higher

Hardware requirements

- CPU: Pentium III 1 GHz or better
- RAM: 1 GB recommended
- Disk space: 200 MB minimum
- Network connection: TCP/IP for remote access

When Host DLP is combined with Endpoint Encryption and Network DLP, McAfee offers the most comprehensive data protection solution on the market.

Features

Unrivaled protection

- Control the way users send, access, and print sensitive data over the network, through applications, and onto storage devices. Protect email (Microsoft Outlook and Lotus Notes), webmail, peer-to-peer applications, IM, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, printers, fax, and removable storage
- Enforcement options include:
 - » Encrypt (requires McAfee Endpoint Encryption solution)
 - » Block (prevent data transfer)
 - » Business justification (bypass blocking with justification)
 - » Notify user
 - » Store evidence
- Discovery remediation options include:
 - » Encrypt (requires McAfee Endpoint Encryption solution)
 - » Quarantine (locally, AES encrypted)
 - » Monitor
 - » Store evidence
 - » Delete

Complete visibility at your fingertips

- Use comprehensive incident reporting and monitoring to gather all the data you need,

such as sender, recipient, time stamp, and data evidence for proper analysis, investigation and audit, damage control, and risk assessment

- Ability to crawl sensitive data-at-rest on local hard drives with granular performance and directory settings

Comprehensive device management

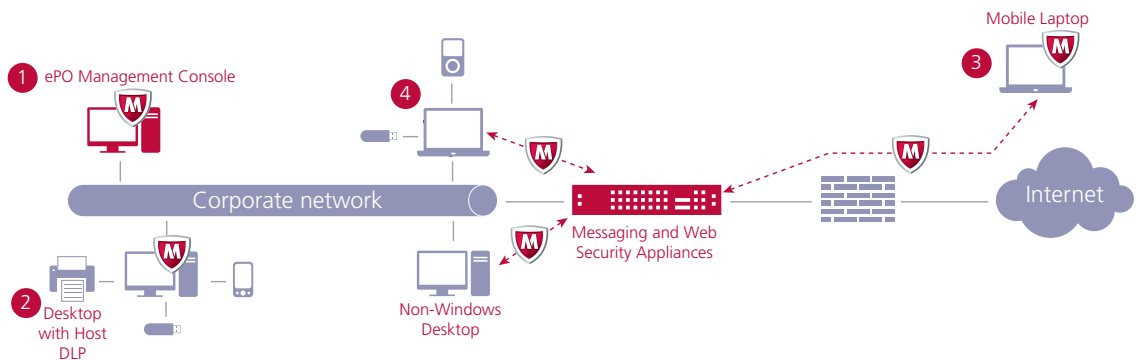
- Control and block confidential data copied to USB devices, flash drives, iPods, and other removable storage devices
- Specify and categorize which devices can be used by any Windows-based device parameter, including product ID, vendor ID, serial number, device class, device name, and more

Multi-layered protection

- Centralized policy deployment and enforcement from USB-to-Gateway
- Stops data loss company-wide when combined with McAfee Endpoint Encryption, Device control and Network DLP
- Seamless on-demand encryption when data is copied to removable media or network shares, and blocks an email or webpost unless encrypted

ePO centralized management

- Single endpoint agent for Host DLP, Network DLP, Endpoint encryption and McAfee Endpoint security
- Common management console with unified rules and policies
- Common event database
- Common reporting and notification mechanism



1 ePO Management Console—Centralized policy management, auditing, reporting, and software distribution. Ensures your security policies align closely with your business processes and operations.

2 Host DLP and Endpoint Encryption—Monitoring, reporting, control, and prevention of user behavior that could put your data at risk. Strong, FIPS-certified encryption for the whole disk or individual files and folders to protect the integrity of data in the event of loss or theft.

3 Endpoint Encryption—Strong, full-disk encryption as well as encrypted, protected space on laptops for sensitive data. Protects the integrity and confidentiality of that data in the event the laptop is lost or stolen.

4 Device Control and Endpoint Encryption—Controls user behavior with external media devices such as iPods and USB thumb drives to prevent sensitive data loss. Strong, full-disk encryption ensures the laptop is unusable in the event of loss or theft.

