McAfee DLP Endpoint

Don't be the next data loss statistic

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 uploading to the cloud—potentially costing you millions.

Key Advantages

- *Unrivaled protection*—Prevent data loss at work, on the road, to the cloud, or at home.
- *Content-aware device management*—Filter, monitor, and block confidential data on any removable storage device.
- *Centralized management*—Leverage McAfee® ePolicy Orchestrator® (McAfee ePO™) software to streamline policy and incident management.
- *Complete visibility*—Stop data loss before it happens by monitoring and controlling user behavior.

Overview

Every day companies like yours fall victim to massive data loss through malicious and unintentional leakage of information. The costs of data breaches and remediation are extremely high. What if you could easily and effectively stop data loss? What if you could meet industry and government compliance and protect intellectual property at the same time? Now you can—with the comprehensive McAfee® DLP Endpoint solution.

Protect and Comply

With McAfee DLP Endpoint, you can quickly and easily monitor real-time events and apply centrally managed security policies to regulate and restrict how employees use and transfer sensitive data without impacting employee productivity. You'll protect data from threats originating from the inside, such as email, IM, web posting, USB copying, and printing. You can also stop confidential data loss initiated by Trojans, worms, and other file-sharing applications.

- Protection for all potential leaking channels including removable storage devices, email, web, printing, clipboard, screen capture, and network shares.
- Flexible classification including dictionaries, regular expressions and validation algorithms, registered documents, and support for third-party, end-user classification solutions, such as TITUS.
- Unique tagging technology for identifying documents according to their origin. Protect sensitive information being copied from web applications, network applications, and network shares.
- Endpoint discovery for local drives and email archives to protect sensitive files and emails. Furthermore, it allows employees to self-remediate any compliance violations, such as PCI, and reduces manual involvement of DLP administrators.
- Enhanced virtualization support to protect remote desktops and VDI solutions.
- Fully customized user notification and business justification dialogues help reinforce end-user behaviors.

Control and Manage

Comprehensive device management helps control and block confidential data copied to USBs, flash drives, CD/DVDs, Apple iPods, and other removable storage devices. Device parameters such as product ID, vendor ID, serial number, device class, and device name can be specified and categorized. Furthermore, different policies, such as block or encrypt, can be enforced based on the content loaded onto the devices.

- Support for plug-and-play devices and removable storage devices.
- Removable storage devices can be blocked or made read-only.
- Content-aware protection for removable storage devices.
- Integration with McAfee Endpoint Encryption for file folders and digital rights management (DRM) solutions.

System Requirements

McAfee ePO server OS

- Microsoft Server 2003 SP1, 2003 R2

Desktop and laptop endpoint OS

- Microsoft Windows XP
- Professional SP1 or higher
- Microsoft Windows 2000 SP4 or higher

Hardware requirements for endpoint

- CPU: Pentium III 1 GHz or better
- RAM: 1GB, 2GB (recommended)
- Disk space: 200 MB minimum

Supported Platforms

- Microsoft Windows XP Professional SP3 or later, 32-bit
- Windows Vista SP1 or later, Enterprise and Business editions, 32-bit
- Windows 7 SP1 or later Enterprise and Business editions, 32-bit and 64-bit
- Windows 8 Professional, 32-bit and 64-bit
- Windows 2003 Server R2 SP2 or later, 32-bit and 64-bit
- Windows 2008 Server SP2 or later, 32-bit and 64-bit
- Windows Server 2012 64-bit

Virtualization systems

- Citrix XenApp 6.0 and 6.5
- Citrix XenDesktop 5.5 and 5.6
- VMware View 4.6, 5.0, and 5.1
- MS Terminal Server (Windows 2003/2008/2012 server)

McAfee ePO software and agents

- McAfee ePO software 4.5, 4.6, and 5.0
- McAfee agent 4.5 Patch 3, 4.6 Patch 3, and 4.8

- File access protection for files that reside on removable storage devices.
- The Citrix device rule blocks access to the thin-client device mapping: local drives, removable storage, printers, CD/DVD, clipboard, and more.
- Non-system hard disks rule blocks and monitors read-only files and provides notifications of user actions on fixed disk drives.

Centralized Management Through McAfee ePO Software

Integration with McAfee ePolicy Orchestrator (McAfee ePO) software offers real-time event monitoring and centralized policy and incident management. It allows for easy collection of critical usage data, such as sender, recipient, time stamp, and data evidence. With a click of a button, McAfee ePO software offers detailed reports to prove to auditors, senior management, and other stakeholders that internal and regulatory compliance measures are in place.

- Deploy and update McAfee DLP Endpoint agents via McAfee ePO software.
- Manage McAfee DLP Endpoint policies and incidents via McAfee ePO software.
- Integrate with McAfee ePO software for event monitoring, centralized reporting, and auditing capabilities.
- Set role-based access control (also known as separation of duties) by McAfee ePO software for incident review.
- Notify violators and/or managers automatically.
- Access helpdesk interface.

McAfee
An Intel Company

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

60264ds_dlp-endpoint_0613_fnl_ETMG