

McAfee Device Control

Prevent unauthorized use of removable media devices on your network

USB drives, MP3 players, CDs, DVDs, and other removable media—however useful—pose a real threat to your organization. Their small size combined with enormous storage capacity makes it all too easy for confidential customer data and intellectual property to walk right out the front door and fall into the wrong hands through loss or theft.

In a survey conducted by McAfee, Inc. more than half of respondents (some 55 percent) said they use a portable device to take confidential documents out of their business every week.¹ How do you know who is storing what on which type of device? And even if they have permission to use the data, how can you be sure they are keeping it secure?

Key Advantages

Unrivaled protection

- Prevent data loss via unauthorized use of removable storage devices

Comprehensive device management

- Specify detailed hardware- and content-based filtering, monitoring, and blocking of confidential data on any removable storage device
- Enable safe use of removable media devices—no need to “block all” and hinder work productivity

ePO centralized management

- Leverage your McAfee security risk management platform to prevent data loss through removable storage devices
- Centrally deploy and manage security policy to prevent confidential data loss via removable media

Complete visibility

- Prove internal and regulatory compliance measures to auditors, board members, and other stakeholders

Stem the rising costs of exposure

Data loss is one of the most widespread, serious, and costly security problems facing companies today. In fact, more than 75 percent of Fortune 1000 companies have fallen victim to accidental or malicious data loss. And the costs are staggering. In 2008, the average cost to companies resulting from data breaches was \$6.65 million.²

Monitor and control data copied to portable devices and media

McAfee® Device Control protects critical data from leaving your company through removable media, such as USB drives, iPods, Bluetooth devices, recordable CDs and DVDs. It gives you the tools to monitor and control data transfers from all desktops and laptops—regardless of where users and confidential data go, even when they are not connected to the corporate network.

Device Control provides extremely granular control over your sensitive data. Specify which devices can and cannot be used. Define what data can and cannot be copied onto allowed devices. And restrict users from copying data from specific locations, such as a file server that stores propriety information, and from certain applications, such as an accounting program that generates confidential reports.

Automatically enforce detailed device and data policies

Gaining centralized control over your information assets is easy. Use McAfee ePolicy Orchestrator® (ePO™) to distribute the McAfee Device Control agent to your managed desktops and laptops. Then specify in detail which content can and cannot be copied to which removable storage devices. Device Control does the rest, automatically monitoring usage and blocking any attempts to use devices or transfer data in violation of the policies you have set, even when data is modified, copied, pasted, compressed, or encrypted. Likewise, Device Control allows legitimate business activities to proceed without disruption.

Demonstrate regulatory compliance at will

McAfee Device Control gives you complete visibility and control over the transfer of confidential information to removable storage devices and media. Integration with ePO allows you to easily collect critical usage data, such as device, time stamp, and data evidence. A click of the mouse enables real-time event monitoring and detailed forensics report generation to prove to auditors, board members, and other stakeholders that internal and regulatory compliance measures are in place.

¹ McAfee. The Threats Within Volume II: Data Loss Disaster. February 2007.

² Ponemon Institute's 2008 Cost of Data Breach Study.

System requirements

ePO Server

Operating systems
• Microsoft Server 2003 SP1, 2003 R2

Hardware requirements

- Disk space: 250 MB
- RAM: 512 MB
1 GB RAM (recommended)
- CPU—Intel Pentium II-class or higher - 450MHz minimum

Device Control Endpoint

Operating systems
• Microsoft Windows XP Professional SP1 or higher

• Microsoft Windows 2000 SP4 or higher

Hardware requirements

- CPU: Pentium III 1 GHz or better
- RAM: 512 MB recommended
- Disk space: 200 MB minimum
- Network connection: TCP/IP for remote access

Features

Unrivaled data protection

- Regulate how users copy data to USB drives, iPods, recordable CDs and DVDs, floppies, Bluetooth and IrDA devices, imaging devices, COM and LPT ports, and more
- Protect all data, formats, and derivatives even when data is modified, copied, pasted, compressed, or encrypted
- Prevent data loss wherever users go, without disrupting legitimate day-to-day activities

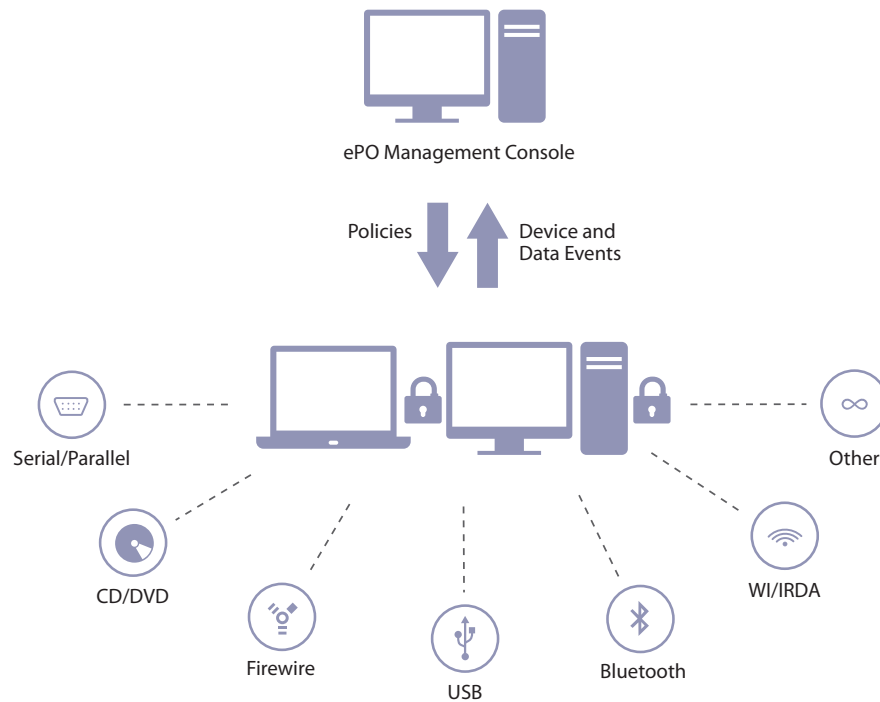
Centralized management through McAfee ePO

- Quickly and easily configure, deploy, and update policies and agents throughout your environment from a centralized management console

- Set device and data policies by user, group, or department
- Specify which devices can and cannot be used by any Windows device parameter, including product ID, vendor ID, serial numbers, device class, device name, and more
- Specify what content can or cannot be copied onto devices that are allowed access

Full visibility and control at your fingertips

- Support auditing and compliance needs with detailed user- and device-level logging
- Gather incident details such as device, time stamp, data evidence, and more for prompt and proper response, investigation, and audit



McAfee Device Control specifies which devices can be used and what data can be copied.

For more information about Data Protection, visit www.mcafee.com/data_protection.

