Data Sheet

McAfee Complete Data Protection—Advanced

Comprehensive Data Protection Anywhere, Anytime

Sensitive data is constantly at risk of loss, theft, and exposure. Many times, the data simply walks right out the front door on a laptop or USB device. Companies that suffer such a data loss risk serious consequences, including regulatory penalties, public disclosure, brand damage, customer distrust, and financial losses. According to a Ponemon Institute report, 7% of all corporate laptops will be lost or stolen sometime during their useful life.[1] The rapid proliferation of mobile devices with large storage capacities and often Internet access is opening up even more channels for data loss or theft, so protecting sensitive, proprietary, and personally identifiable information must be a top priority. McAfee® Complete Data Protection Suites address all of these concerns and many more.

Key Features

- McAfee Data Loss Prevention Endpoint
- McAfee Device Control
- Drive encryption
- File and removable media protection
- Management of native encryption
- McAfee ePO Deep Command

Key Advantages

- Gain control over your data by monitoring and regulating how employees use and transfer data via common channels, such as email, IM, printing, and USB drives—both in and away from the office.
- Stop data loss initiated by sophisticated malware that hijacks sensitive and personal information.
- Secure data when it's stored on desktops, laptops, tablets, and other mobile devices.
- Manage Apple FileVault and Microsoft BitLocker native encryption on endpoints directly from McAfee ePO.

Data Loss Prevention for Greater Control

Preventing data loss at the endpoint begins with improving visibility and control over your data, even when it is disguised. McAfee Complete Data Protection—Advanced enables you to implement and enforce company-wide security policies that regulate and restrict how your employees use and transfer sensitive data via common channels, such as email, IM, printing, and USB drives. It does not matter if they are in the office, at home, or on the move—you stay in control.

Enterprise-Grade Drive Encryption

Secure your confidential data with an enterprise-grade security solution that is FIPS 140-2 and Common Criteria EAL2+ certified, and accelerated with the Intel Advanced Encryption Standard—New Instructions (AES-NI) set. McAfee Complete Data Protection Suites use drive encryption combined with strong access control via two-factor pre-boot authentication to prevent unauthorized access to confidential data on endpoints, including desktops, VDI workstations, laptops, USB drives, CD/DVDs, and more.

Persistent, Transparent Removable Media and File and Folder Encryption

Ensure that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved. McAfee Complete Data Protection Suites feature content encryption that automatically and transparently encrypts the files and folders you choose on the fly—before they move through your organization. You create and enforce central policies based on users and user groups for specific files and folders without user interaction.

Management of Native Encryption

Management of native encryption allows customers to manage the native encryption functionality offered by Apple FileVault on OS X and Microsoft BitLocker on Windows platforms directly from McAfee® ePolicy Orchestrator®

Key Advantages (continued)

- Communicate with and take control of your endpoints at the hardware level whether they are powered off, disabled, or encrypted to halt desk-side visits and endless help desk calls due to security incidents, outbreaks, or forgotten encryption passwords.
- Prove compliance with advanced reporting and auditing capabilities; monitor events and generate detailed reports that show auditors and other stakeholders your compliance with internal and regulatory privacy requirements.

Features Specific to McAfee ePO Deep Command

- Reduce remediation times.
- Manage remote remediation to any PC anywhere in the world with access from the hardware.
- Improve user productivity.
- Conduct resource-intensive tasks during off hours to limit impact to users.
- Lower IT costs by reducing frequent desk-side visits and lengthy service calls.
- Decrease PC power costs by adopting a power savings program, but still maintain access for security or patching.
- Quickly discover and provision Intel AMT by easily identifying Intel vPro-equipped PCs and then enabling Intel AMT for streamlined activation.

(McAfee ePO™) software. Management of native encryption thus provides zero-day compatibility with OS X and Windows patches, upgrades, firmware updates from Apple, as well as zero-day support for new hardware from Apple. Management of native encryption allows administrators to manually import recovery keys where users have already enabled FileVault and BitLocker.

Remote, Out-of-Band Management Reduces Operational Costs

McAfee ePO Deep Command software uses Intel vPro Active Management Technology (AMT) that helps reduce operational costs, enhances security and compliance, and accelerates remote PC remediation. McAfee ePO Deep Command software can wake up PCs, update policies, and securely return them to their power state.[2]

Centralized Security Management and Advanced Reporting

Use the centralized McAfee ePO software console to implement and enforce mandatory, company-wide security policies that control how data is encrypted, monitored, and protected from loss. Centrally define, deploy, manage, and update security policies that encrypt, filter, monitor, and block unauthorized access to sensitive data.

McAfee Complete Data Protection—Advanced Suite Features

Device control

- Monitor and regulate how employees transfer data to removable media—even when they are not connected to the corporate network.

Data loss prevention

- Control how users send, access, and print sensitive data at the endpoint—physical or virtual, through applications, and onto storage devices.
- Stop confidential data loss initiated by Trojans, worms, and file-sharing applications that hijack employee credentials.
- Protect all data, formats, and derivatives, even when data is modified, copied, pasted, compressed, or encrypted.

Enterprise-grade drive encryption

- Automatically encrypt entire devices without requiring user action or training or impacting system resources.
- Identify and verify authorized users using strong multifactor authentication.

Removable media encryption

- Automatic, on-the-fly encryption for virtually any mobile storage device, company-issued or not.
- Access encrypted data anywhere without the need for any additional software.

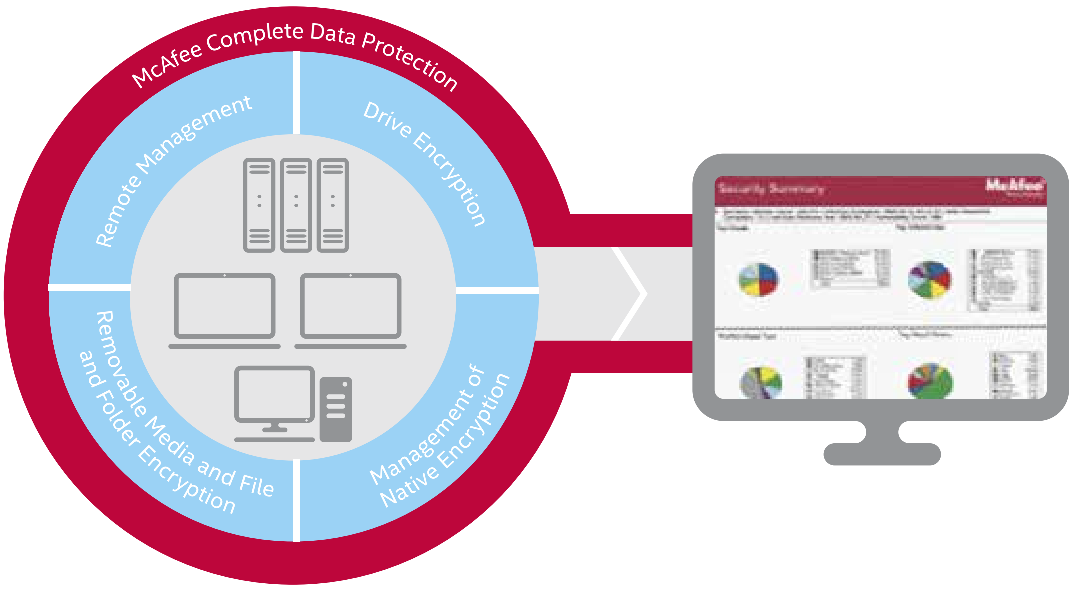
McAfee Complete Data Protection
Remote Management
Drive Encryption
Removable Media and File and Folder Encryption
Management of Native Encryption
Security Summary
McAfee

Figure 1. McAfee Complete Data Protection Suite.

McAfee Complete Data Protection Specifications

Microsoft Windows operating systems

- Microsoft Windows 7, 8, 8.1 (32/64-bit versions)
- Microsoft Vista (32/64-bit versions)
- Microsoft Windows XP (32-bit version only)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (32-bit version only)

Hardware requirements

- CPU: Pentium III 1GHz or higher laptop and desktop computers
- RAM: 512 MB minimum (1 GB recommended)
- Hard disk: 200 MB minimum free disk space

Apple Mac operating systems

- Mac OS X Mountain Lion
- Mac OS X Mavericks

Hardware requirements

- CPU: Intel-based Mac laptop with 64-bit EFI
- RAM: 1 GB minimum
- Hard disk: 200 MB minimum free disk space

Centralized management

- See McAfee ePO platform data sheet for technical specifications

McAfee ePO Deep Command Specifications

- Supports Intel vPro AMT versions 6.1.2, 7.0, 7.1.4, and 8.0 Intel Setup and Configuration Software (SCS) 8.2

Persistent file and folder encryption

- Keep files and folders secure wherever they are saved, including on local hard disks, file servers, removable media—and even as email attachments without requiring the email recipient to have encryption software.

Manage native encryption on Macs and Windows

- Manage FileVault on any Mac hardware that can run OS X Mountain Lion, Mavericks, and Yosemite directly from McAfee ePO software.
- Manage BitLocker on Windows 7 and 8 systems directly from McAfee ePO software, without the need for a separate Microsoft BitLocker Management and Administration (MBAM) server.

Remote, out-of-band management

- Remotely manage PCs beyond the operating system at the hardware level.
- Power on and wake up a PC, even if encrypted to execute security tasks.

Centralized management console

- Use the McAfee ePO software infrastructure management to manage full-disk, file and folder, and removable media encryption; control policy and patch management; recover lost passwords; and demonstrate regulatory compliance.
- Synchronize security policies with Microsoft Active Directory, Novell NDS, PKI, and others.
- Prove devices are encrypted with extensive auditing capabilities.
- Log data transactions to record such information as sender, recipient, timestamp, data evidence, and date and time of last successful login.

For more information about McAfee data protection, visit **www.mcafee.com/dataprotection**.

[1] *The Billion Dollar Lost Laptop Problem Study*, Ponemon Institute, September 2010.

[2] *Keep Your Client PCs Safer, Wherever They Go*: **http://www.mcafee.com/us/resources/solution-briefs/sb-keep-your-client-pcs-safer.pdf**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com