McAfee Complete Data Protection

Comprehensive endpoint encryption solution

Key Features

- Drive encryption.
- File and removable media protection.
- Management of native encryption.

Key Advantages

- Stop data loss initiated by sophisticated malware that hijacks sensitive and personal information.
- Secure data when it's stored on desktops, laptops, tablets, and cloud storage.
- Manage Apple FileVault and Microsoft BitLocker native encryption on endpoints directly from McAfee ePO software.
- 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 helpdesk 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.

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.

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 (Intel AES-NI) set. McAfee Complete Data Protection uses drive encryption combined with strong access control via two-factor pre-boot authentication to prevent unauthorized access to confidential data on endpoints, including desktops, virtual desktop infrastructure (VDI) workstations, laptops, Microsoft Windows tablets, USB drives, and more.

Removable Media, File and Folder, and Cloud Storage Encryption

Ensure that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved. McAfee Complete Data Protection features 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® (McAfee ePO™) software. Management of native encryption thus provides zero-day compatibility with OS X and Windows patches, upgrades, firmware updates from Apple and Microsoft, and 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.

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 Features

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.
- Supports Intel® Software Guard Extensions (Intel® SGX).
- Compatible with third-party credential providers.
- In-place upgrade support for Windows 10 Anniversary Update.

Removable media encryption

- Automatic, on-the-fly encryption for virtually any mobile storage device, company issued or not.
- Encrypt or block writes to removable media at VDI workstations.
- Access encrypted data anywhere, without the need for any additional software installation or local administrative rights on the device host.

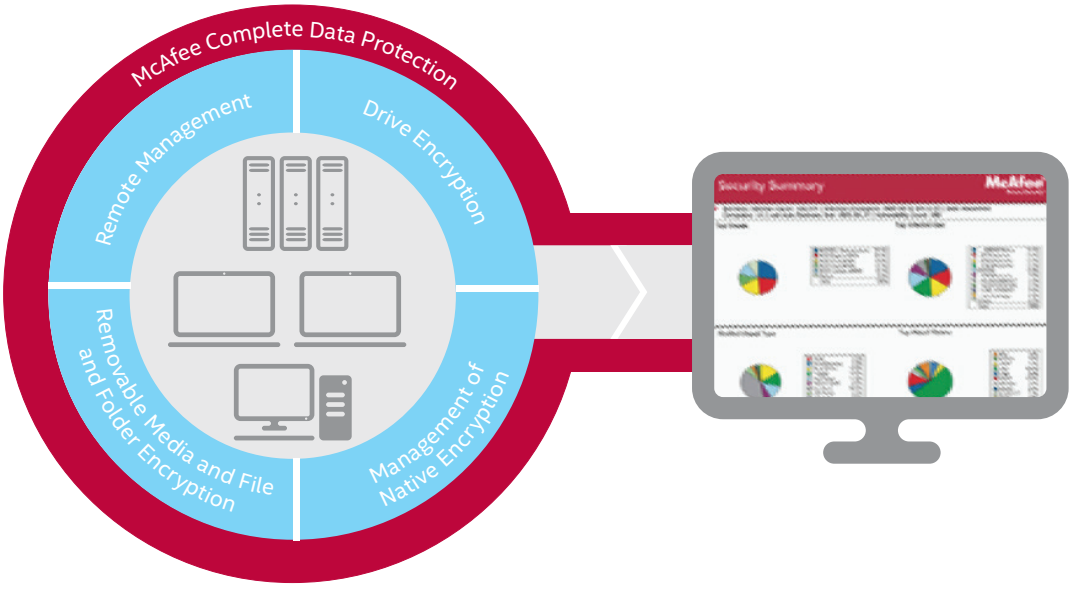

Figure 1. McAfee Complete Data Protection.

McAfee Complete Data Protection Specifications

Microsoft Windows operating systems

- Microsoft Windows 7, 8, and 10 (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 1 GHz 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 El Capitan, Yosemite, Mountain Lion, and 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

File, folder, and cloud storage encryption

- Keep files and folders secure wherever they are saved, including local hard disks, file servers, removable media, and cloud storage such as Box, Dropbox, Google Drive, and Microsoft OneDrive.

Manage native encryption on Macs and Windows

- Manage FileVault on any Mac hardware that can run OS X Mountain Lion, Mavericks, Yosemite, and El Capitan directly from McAfee ePO software.
- Manage BitLocker on Windows 7, 8, and 10 systems directly from McAfee ePO software, without the need for a separate Microsoft BitLocker Management and Administration (MBAM) server.
- Report compliance in various reports and dashboards in McAfee ePO software.

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 record such information as sender, recipient, timestamp, data evidence, date and time of last successful login, date and time last update received, and whether the encryption was successful.

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

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