

McAfee Complete Data Protection—Essential

Essential endpoint encryption solution

Sensitive data is constantly at risk of loss, theft, and exposure. Often, 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 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—Essential addresses all of these concerns and many more.

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 provides zero-day compatibility with Apple OS X and Microsoft 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.

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—Essential 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.

Key Features

- Management of native encryption
- File and removable media protection

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.
- 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.

DATA SHEET

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 Suites Features

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.

Specifications

Microsoft Windows operating systems

- Microsoft Windows 10
- 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 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

- See McAfee ePO platform data sheet for technical specifications

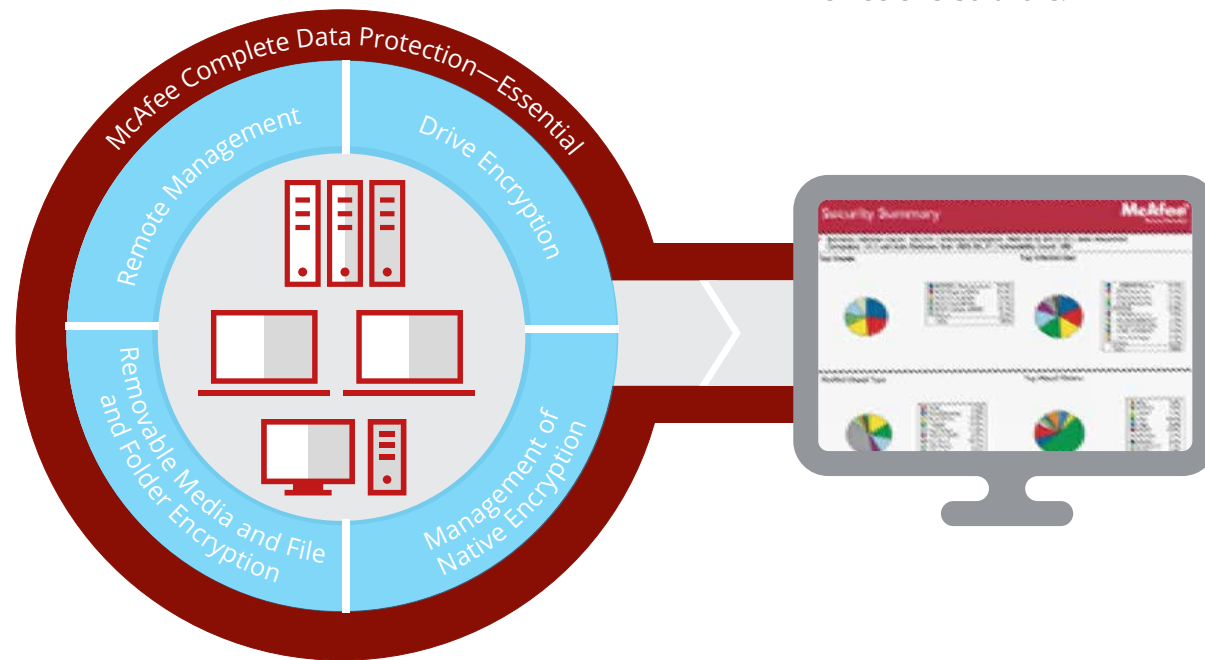


Figure 1. McAfee Complete Data Protection—Essential.

DATA SHEET

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

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.

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, date and time of last successful login, date and time last update received, and whether the encryption was successful or not.

Learn More

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

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



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

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.
62239ds_complete-data-ess_0116
JANUARY 2016