Solution Brief

Endpoint Encryption Keeps Your Data Safe

Core data protection components available in Intel Security protection suites.

Intel Security endpoint encryption solutions protect valuable corporate data on user devices and shared servers with comprehensive encryption and integrated, centralized management; consistent policies; robust reporting; and proof-of-protection.

Support productivity while confidently protecting data stored on office desktop PCs and Macs, on-the-go laptops, and collaborative tools like shared network files, USB storage devices, and cloud storage. The McAfee® ePolicy Orchestrator® (McAfee ePO™) software management infrastructure masterfully enables centralized deployment, management, policy administration, password recovery, monitoring, reporting, and auditing for ease of management, consistent protection, and low TCO.

Intel Security encryption solutions are available as key components in the following protection suites:

- **McAfee Complete Data Protection—Advanced**
- **McAfee Complete Data Protection**
- **McAfee Complete Data Protection—Essential**
- **McAfee Complete Endpoint Protection—Business**

Comprehensive Data Protection

Intel Security data protection offers multiple layers of protection against data loss and unauthorized access. The cornerstone of data protection is encryption, which is used primarily to prevent unauthorized access from outsiders, especially when a device is lost or stolen.

The range of encryption solutions available in Intel Security protection suites include:

- **Drive encryption:** Encrypts data on desktop PCs, laptops, and Microsoft Windows tablets.
- **File and removable media protection:** Encrypts data on network files and folders, removable media, USB portable storage devices, and cloud storage.
- **Management of native encryption:** Manages the native encryption functionality offered by Apple FileVault on OS X and Microsoft BitLocker on Windows, directly from McAfee ePO software.

Key Advantages

- Secure data on office desktop PCs, Macs, mobile laptops, VDI workstations, and collaborative tools like shared folders, USB drives, and cloud storage.
- Confidently ensure consistent and persistent data protection across devices.
- Protect company intellectual property and meet compliance requirements.
- Simplify security management and enable broad yet granular visibility using McAfee ePO software for centralized deployment, management, policy administration, auditing, and reporting.
- Easily and consistently enforce company-wide security policies.
- Reduce total cost of ownership and complexity by using comprehensive data protection solutions integrated with centralized management.

intel Security

Endpoint Encryption Solutions

Industry-leading data protection solutions from Intel Security are available as key components in our endpoint and data protection suites for extensible, customized protection to fit your security needs today and in the future.

Encryption Solution	Key Features
Drive Encryption Full disk encryption for Microsoft Windows laptops and desktop PCs prevents the loss of sensitive data, especially from lost or stolen equipment.	• Enforces strong access control with pre-boot authentication. • Uses military-strength, certified encryption algorithms (FIPS, Common Criteria). • FIPS 140-2 and Common Criteria EAL2+ certified for the Intel® Advanced Encryption Standard–New Instructions (Intel AES-NI) implementation. • Enables automatic, transparent encryption without hindering performance. • Supports mixed device environments, including solid-state drives. • Supports Trusted Computing Group (TCG) Opal v1.0 self-encrypting drives. • Enhances performance through support for Intel AES-NI technology.
File and Removable Media Protection Policy-enforced encryption of files, folders, removable media, and cloud storage.	• Delivers policy-enforced, automatic, transparent encryption of files and folders stored or shared in PCs, file servers, VDI workstations, email attachments, removable media (USB drives, CD/DVDs, and ISO files), and cloud-storage services. • Prevents unauthorized access to information on network servers and removable media. • Provides key-sharing mechanisms that allow users to share files securely. • Reads and edits encrypted data on media without installing any software; data is saved with retained encryption. • Hardware independent—even the least expensive media can be protected.
Management of Native Encryption Protects data with Apple's native encryption, FileVault, for Macs and with Microsoft's native encryption, BitLocker, for Windows.	• Through McAfee ePO software, an IT administrator can secure and manage all OS X Mountain Lion, Mavericks, Yosemite, and El Capitan[2] Macs that support Apple FileVault. • Through McAfee ePO software, an IT administrator can secure and manage all Windows 7, 8, and 10[3] PCs that support Microsoft BitLocker. • Provides for zero-day compatibility with OS X patches, upgrades, and firmware updates from Apple. • Provides single sign-on from FileVault's pre-boot environment directly into OS X. • Upgrade from one major OS X version to next without having to decrypt and re-encrypt the drive. • Manage BitLocker on Windows 7, 8, and 10[4] systems directly from McAfee ePO software, without the need for a separate Microsoft BitLocker Management and Administration (MBAM) server.

Gartner Magic Quadrant for Mobile Data Protection

Endpoint encryption is a significant part of mobile data protection. Intel Security has been positioned as a Leader in the **Gartner Magic Quadrant for Mobile Data Protection Solutions** for eight consecutive years and is placed in the highest position for ability to execute and completeness of vision.[1]

Drive Encryption

Intel Security drive encryption solutions protect valuable data on PC laptops and desktop computers with full drive encryption and strong access control. When a PC or Mac with managed encryption is lost or stolen, it's generally not considered to be a breach event because the data is "unusable, unreadable, or indecipherable to unauthorized individuals."[5] Without encryption or proof-of-protection through managed encryption, the biggest security concern is around the possibility of a data breach. The breach of confidential corporate or customer data can result in loss of intellectual property, industry and legal noncompliance penalties, and more.

Key features

- Encrypts all data on PCs.
- Enforces strong access control with pre-boot authentication.
- Uses military-strength, certified encryption algorithms (FIPS, Common Criteria).[6]
- Enables automatic, transparent encryption in the background.
- Enhances performance through support for Intel AES-NI technology.[7]
- Supports environments with software- and hardware-based encryption, including solid-state and self-encrypting drives.[8]
- Optimizes policy enforcement automatically for each client, regardless of whether the PC uses software- or hardware-based encryption or if it's a new or existing device.
- Supports multifactor authentication via password or a wide variety of supported tokens and smartcards.[9]

- Simplifies operating system (OS) updates with the optional ability to temporarily suspend pre-boot authentication when deploying OS patches and the ability to do a major refresh on the OS without needing to decrypt and re-encrypt data on the PC.[10]
- Works with select third-party forensics tools.[11]

Benefits

- **Multiple storage and sharing options:** Encrypts data on local disks, file servers, removable media, and in email attachments (whether or not the recipient has Intel Security encryption software), providing storage and sharing options to meet a wide range of needs.
- **Policy-based, scalable encryption:** Encryption is automatically deployed in accordance with the organization's information security policy and can be set differently for separate individuals, groups, or entire companies. Encryption policies are created using McAfee ePO software and can be assigned to users based on information from Microsoft Active Directory. Encryption keys are generated and managed centrally using McAfee ePO software. Users can not override policies.
- **Automatic, always-on encryption:** Encryption follows the document when transferred between storage media to ensure that the data remains secure without user interaction. The encryption information travels with the file in a "file header." Files are encrypted when they are created, preventing hidden data loss through plain text temporary files or system page files (virtual memory from the hard disk), for example. Encryption is retained when copying, moving, and editing files on supported storage media.
- **Transparent end-user experience:** Encrypted documents keep original file extensions and still appear as "normal" to the authorized user with a minimum of user interaction. The user authentication is fully integrated with the Microsoft Windows logon, meaning that any authentication token used for the Windows logon is automatically supported by file and removable media protection, yielding a completely transparent and simplified user experience.
- **Granular flexibility:** Granular options to encrypt individual documents, entire folders, locations, and/or file types provide more effective selection of valuable data to encrypt based on policies, while also allowing the user to encrypt additional files on demand.
- **Encrypted document sharing:** Authorized users can easily share encrypted documents among individuals or within groups enabled by the centralized key management in McAfee ePO software. The encryption and decryption happens "on the fly" on the client side when accessing and saving protected documents. Self-extracting files can be used for email attachments, and, for user convenience, the recipient doesn't need to install any encryption software in order to read the encrypted attachment.
- **Removable media encryption:** All data (or portions of data) on standard off-the-shelf USB and other removable storage devices can be encrypted, modified, and saved on the device with separate authentication and retained encryption, without needing any software installation or local administrative rights on the device host. No files are left on the host PC because wiping is built in.
- **Multiple, configurable protection:** Authentication (password, CAC, or PIV smart cards) and recovery methods can be used. Separately, Intel Security also offers hardware-encrypted USB flash and hard drives.

File and Removable Media Protection

Typical use cases

File and folder encryption

- I want to automatically encrypt all Microsoft Excel files on my laptop.
- I want to encrypt all files in a specific folder on my laptop.

Network sharing

- I want to transparently encrypt and limit access to a particular network folder to the human resources team.

Removable media encryption

- I want to block copying of files to a removable media device unless the drive is encrypted.
- I want to read the encrypted device on a home computer that does not have any Intel Security software installed.
- I want to allow access to the encrypted devices only within my organization.

Self-extracting files

- I want to send an encrypted email attachment to my partner and allow them to access the attachment witho ut requiring them to install any software.

File and Removable Media Protection

File and removable media protection delivers policy-enforced, automatic, transparent encryption of files and folders stored or shared on PCs, Macs, file servers, email attachments, removable media (for example, USB drives and CD/DVDs), and on cloud storage.

Benefits

- **Protect removable media:** Off-the-shelf USB devices are small and inexpensive, so they're easy to misplace or lose. With policy-based encryption and McAfee ePO software, it's quick and easy to enforce organization-wide encryption policies for removable media to mitigate the risk of data loss. Encrypting removable media still permits the media to be used by the authorized owner outside the organization for retained portability.
- **Protect local data:** File and removable media protection offers PCs and Macs an extra level of protection for sensitive data stored on a hard drive, whether the computer is on or off.
- **Protect data on network shares:** If a cybercriminal somehow gets into your network, having files and folders separately encrypted provides an extra layer of protection, as the data it contains is unreadable and unusable to unauthorized parties. It is also possible to stack separately encrypted files in separately encrypted folders for even more security.
- **Protect data on cloud storage:** Securely store encrypted data on cloud storage services such as Box, Dropbox, Google Drive, and Microsoft OneDrive.

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 ePO software.

Key features for Mac

- Manage FileVault on any Mac hardware that can run OS X Mountain Lion, Mavericks, Yosemite, or El Capitan[12] directly from McAfee ePO software.
- Enforce a standard password complexity policy on local OS X users.
- Report compliance in various reports and dashboards in McAfee ePO software.
- Provide the FileVault Recovery Key, as required, when you need to use Apple-provided recovery tools and workflows.
- Allow administrators to manually import FileVault Recovery Keys where users have already manually enabled FileVault.
- Proof-of-compliance report in the event of a lost or stolen laptop.

Benefits for Mac

- Ability to upgrade from one major OS X version to next without having to decrypt and re-encrypt the drive.
- Ability to SSO from FileVault's pre-boot environment directly into OS X.
- Zero-day compatibility with OS X patches, upgrades, and firmware updates from Apple.
- Zero-day support for new hardware from Apple.
- IT can enforce password policies for OS X.
- Full compatibility in pre-boot for all languages supported by Apple.
- Support for a new bring-your-own-device (BYOD) mode where the device is not managed—only the state of compliance is reported in McAfee ePO software (suitable for contractors).
- Simple to administer and manage.

Key features for Windows

- Manage Microsoft BitLocker on Windows 7, 8, or 10[13] hardware directly from McAfee ePO software.
- Utilizes the Trusted Platform Module (TPM) 1.2 and 2.0 hardware to provide a transparent user experience.
- Supports FIPS 140-2 requirements.
- Supports Microsoft eDrive.
- Consistent user interface for both FileVault and BitLocker management.
- Provides the BitLocker Recovery Key, when required, in recovery use cases.
- Report compliance in various reports and dashboards in McAfee ePO software.

Benefits for Windows

- Manage BitLocker from McAfee ePO software, without the need for a separate Microsoft BitLocker Management and Administration (MBAM) server.
- Self-service portal allows users to recover their own machines.
- Zero-day compatibility with Windows OS patches and updates from Microsoft.
- Zero-day support for tablet hardware from Microsoft.
- Support for certified Windows To Go devices.
- Support for a BYOD mode where the device is not managed—only the state of compliance is reported in McAfee ePO software (suitable for contractors).
- Simple to administer and manage.

Integrated, Centralized Management with McAfee ePO Software

The award-winning McAfee ePO software management infrastructure provides centralized deployment, management, shared policy administration, password recovery, monitoring, reporting, auditing, and proof-of-protection. McAfee ePO software works for encryption, data loss prevention (DLP), and other Intel Security products for ease of management, consistent protection, holistic visibility, and low TCO. It's security management you can rely on.

Key features

Enterprise-class scalability

- Enables efficient server utilization for larger installations.

Simplified deployment

- Enables lower administrative overhead with single-console and common management agent for data protection and endpoint security products.
- Identifies PCs and Macs that are not protected and then deploys the McAfee ePO software agent to protect PCs and Macs according to policies.
- Checks for incompatible products before activating the Intel Security client and provides status reporting via the McAfee ePO platform.
- Enables remote, no-touch Microsoft Windows XP to Microsoft Windows 7 migration, including keeping the user's data and machine encrypted during the entire process.

Shared infrastructure

- Supports mixed encryption environments, enabling organizations to maintain a single policy and management infrastructure for the entire environment, regardless of whether it is software- or hardware-based encryption.
- Share tasks, policies, and management infrastructure regardless of the encryption mix.

Customizable, granular policies

- Offers customization by user (individual, shared by groups, or the entire company), PC/Mac, or server.
- Enables you to specify a new encryption policy at any level of the organization to handle specific use cases.
- Allows you to use scripting to customize a wide range of management tasks, like user and password management.[14]
- Provides optional policy-based lockout of PC-to-network resources if there is no recent check-in by the endpoint to the network.

Status dashboards and full reporting

- Stores all audit and logging information on the McAfee ePO software console.
- Generates standard or custom reports on the entire McAfee ePO software-managed network.

Actionable reporting with the McAfee ePO software console and above

- Includes superior recovery tools, including user self-recovery.
- Empowers you to take immediate action directly from a report to perform tasks on targeted systems or resolve issues.
- Allows you to use the McAfee ePO software console rogue system detection option to determine which machines are unsecured, even if there is no agent running on the machine.
- Intel Security delivers strong access control and encryption combined with robust management and proof-of-protection so companies can be confident that their data remains secure.

Intel Security data protection solutions deliver comprehensive protection with integrated, centralized management. These customizable solutions help organizations protect vast amounts of confidential business and compliance-related data today and are easily extensible to meet evolving future security needs as well. Trust Intel Security to provide data protection solutions that will let you stay focused on what you do best: running a successful business.

For more information about Intel Security endpoint encryption and management solutions, please visit **www.mcafee.com/dataprotection**, or call us at 888 847 8766, 24 hours a day, seven days a week.

1. *Gartner Magic Quadrant for Mobile Data Protection Solutions*, October 2015 http://www.mcafee.com/us/independent-reports/gartner-mq-mobile-data-protection.aspx
2. Second half of 2015.
3. Ibid.
4. Ibid.
5. Federal Register Notice, August 24, 2009. Hhs.gov.
6. Supported on McAfee Drive Encryption for PCs only.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Supported on McAfee Drive Encryption for PCs only. Third-party forensic solutions are required at additional cost.
12. Second half of 2015.
13. Ibid.
14. Supported on McAfee Drive Encryption for PCs only.

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