

# McAfee Endpoint Encryption for PCs and Mac

Managed full disk encryption for confident data protection

McAfee® Endpoint Encryption for PCs and McAfee Endpoint Encryption for Mac protect valuable data on laptop and desktop<sup>1</sup> computers with full disk encryption and strong access control. The McAfee ePolicy Orchestrator® (McAfee ePO™) platform provides robust, centralized management and proof of protection.

From a single console, the McAfee ePO platform delivers centralized deployment, management, shared policies, policy administration, password recovery, monitoring, auditing, reporting, and proof of protection. This provides customers with ease of management, consistent protection, and lower TCO.

Intellectual capital (like patented technology, trade secrets, and proprietary data) makes up a majority of a company's value,<sup>2</sup> so it makes sense to protect access to it, especially on mobile endpoints.

Due to their mobility, large storage capacity, and database access capabilities, laptop computers have historically been a major source of confidential data loss and leakage. To help keep the vast amounts of digital data on these endpoints protected, companies deploy managed full disk encryption to automatically secure all data on the laptop from unauthorized access.

When a PC 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."<sup>3</sup> 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 Encryption Features

- All data stored on the PC is encrypted
- Enforces strong access control with pre-boot authentication

- Military-strength, certified encryption algorithms (FIPS, Common Criteria)<sup>4</sup>
- Enables automatic, transparent encryption in the background
- Enhanced performance through support for Intel AES-NI technology<sup>5</sup>
- Supports environments with software- and hardware-based encryption, including solid-state and self-encrypting drives<sup>6</sup>
- Automatically optimizes policy enforcement for each client, no matter whether the PC uses software- or hardware-based encryption, or if it's a new or existing device
- Supports multifactor authentication via password or wide variety of supported tokens and smartcards<sup>7</sup>
- Simplified operating system (OS) updates with 1) the optional ability to temporarily suspend preboot authentication when deploying OS patches and 2) the ability to do a major refresh on the OS without needing to decrypt and re-encrypt data on the PC<sup>8</sup>
- Works with select third-party forensics tools<sup>9</sup>

## Specifications

### Microsoft Windows

#### Operating systems

- Microsoft Windows 7 (all 32- and 64-bit versions)
- Microsoft Vista (all 32- and 64-bit versions)
- Microsoft Windows XP (32-bit versions 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: 256 MB minimum (1 GB recommended)
- Hard disk: 200 MB minimum free disk space
- Network connection: TCP/IP for remote management

### Apple Mac

#### Operating systems

- Mac OS X Leopard (10.5.8 and above)
- Mac OS X Snow Leopard (10.6.x)
- Mac OS X Lion

#### Hardware requirements

- CPU: Intel-based Mac laptop with 64-bit EFI
- RAM: 1 GB minimum
- Hard disk: 200 MB minimum free disk space
- Network connection: TCP/IP for remote management

### Centralized management

See McAfee ePolicy Orchestrator platform data sheet for technical specifications

### McAfee ePO platform support

- 4.5 P1 and beyond: for McAfee Endpoint Encryption for PCs 6.0
- 4.5 P4 HF1 and beyond: for McAfee Endpoint Encryption for PCs 6.1 scalability
- 4.6: for McAfee Endpoint Encryption for PCs 6.1

## Key McAfee ePO Platform Features

### Enterprise-class scalability

- Efficient server utilization for larger installations

### Simplified deployment

- Single console and common management agent for data protection and endpoint security products enable lower administrative overhead
- Identifies PCs that aren't protected; then deploys the McAfee ePO agent to protect the PC according to policies
- Checks for non-compatible products before activating the McAfee client and provides status reporting via the McAfee ePO platform
- Enable 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

- Support for 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

- Customize by user (individual, shared by groups, or the entire company), PC, or server
- Alternatively, specify a new encryption policy at any level of the organization to handle specific use cases

- Use scripting to customize a wide range of management tasks like user and password management<sup>10</sup>
- Optional policy-based lockout of PC to network resources if there is no recent check in to the network and McAfee ePO software

### Status dashboards and full reporting

- All audit and logging information is stored inside the McAfee ePO console
- Get standard or custom reports on the entire McAfee ePO-managed network

### Actionable reporting with the McAfee ePO 4.5 console and above

- Superior recovery tools, including end-user self-recovery
- Take immediate action directly from a report to perform tasks on targeted systems or resolve issues
- Use the McAfee ePO console Rogue System Detection option to determine what machines are unsecured, even if there is no McAfee agent running on the machine

A March 2010 Forrester Research report found that proprietary knowledge and company secrets are twice as valuable as custodial data (for example, payment card and medical data).<sup>11</sup> McAfee delivers strong access control and encryption combined with robust management and proof of protection so companies can be confident that their data remains secure.

1. Supported for McAfee Endpoint Encryption for PCs only.

2. *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest in Cybercrime Currency*, McAfee 2011

3. *Federal Register Notice*, August 24, 2009. Hhs.gov

4. Supported for McAfee Endpoint Encryption for PCs only.

5. Ibid

6. Ibid

7. Ibid

8. Ibid

9. Supported for McAfee Endpoint Encryption for PCs only. Third-party forensic solutions are required at additional cost.

10. Supported for McAfee Endpoint Encryption for PCs only.

11. *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest in Cybercrime Currency*, McAfee 2011

