



Protect what you value.

# McAfee Endpoint Encryption

(Formerly SafeBoot® Encryption)

## Secure data on PCs, laptops, tablets and PDAs

Data protection is now ranked as the number-one priority for CISOs.<sup>1</sup> McAfee® Endpoint Encryption provides a scalable, enterprise-wide security solution that uses powerful encryption and strong access control to prevent unauthorized data access on desktops, laptops, and Tablet PCs as well as smartphones and PDAs.

### KEY ADVANTAGES

#### Strong encryption and access control

- Protect against unauthorized access and data exposure, with powerful device encryption and strong preboot authentication
- Transparently encrypt data “on-the-fly,” with no end-user interaction or training required
- Ensure files and folders remain encrypted wherever they are saved or transferred

#### Internal and external security compliance

- Enforce mandatory, company-wide security policies
- Demonstrate compliance with data privacy legislation
- Control which applications users may access

#### Easy centralized management and lower TCO

- Gain extensive centralized management capabilities
- Synchronize and integrate the solution with Active Directory, Novell, LDAP, and PKI
- Enjoy single sign-on and support for popular smart cards and tokens
- Take advantage of support for all common languages, keyboards, and Windows operating systems

#### Protect your assets and your brand

Loss of confidential data, including customer data, employee records, intellectual property, and business documents has become a pervasive problem for companies worldwide. According to a 2007 survey conducted by the Ponemon Institute, 85 percent of respondents said their businesses had experienced a data security breach.<sup>2</sup> Also reported by the Ponemon Institute, the average cost of a data breach was \$6.3 million.<sup>3</sup>

#### Attain maximum data security with full-disk encryption

The protection of data assets is a primary issue facing today's organizations. Protect your company's mission-critical data with McAfee Endpoint Encryption. The solution uses strong access control with preboot authentication and government certified algorithms to encrypt data on endpoint devices, including desktops, laptops, Tablet PCs, smartphones, and PDAs. Encryption and decryption are transparent to the user and performed “on-the-fly,” with virtually no performance degradation. McAfee Endpoint Encryption seamlessly integrates with existing enterprise systems and provides operational efficiency that ensures low total-cost-of-ownership.

#### Protect files and folders wherever they go

Control what files or folders are encrypted. McAfee Endpoint Encryption allows administrators to specify that the contents of certain folders, files created by particular applications, or files of a certain type be encrypted. Groups of users are granted access rights to particular files and folders, and securely share files across the network.

No matter where files are saved and transferred, data remains encrypted using Persistent Encryption Technology™. If an unauthorized user tries to save a file that is viewable on a company laptop to an unapproved storage device, that user will walk away with an encrypted and unreadable file.

#### Achieve compliance and lower TCO

Prevent loss of data wherever your data goes and achieve regulatory compliance with a full range of security and encryption solutions all managed from one central console. McAfee Endpoint Encryption provides central management capabilities including administration, central deployment, remote upgrades, auditing, mandatory security policy management, a scripting tool, hot revocation, recovery, synchronization, and more. Extensive auditing capabilities prove the device was encrypted at the time of loss or theft, demonstrating compliance. Mandatory security policies can be transparently enforced by administrators. McAfee Endpoint Encryption also supports single sign-on and secure offline user recovery.

<sup>1</sup> 2007 Merrill Lynch survey of CISOs.

<sup>2</sup> Ponemon Institute: The Business Impact of Data Breach, 2007.

<sup>3</sup> Ponemon Institute: 2007 Annual Study: Cost of a Data Breach.

## SYSTEM REQUIREMENTS

### Desktop, laptop, and tablet endpoints

#### Operating Systems

- Microsoft Vista (all 32- and 64-bit versions)
- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows Server 2003

#### Hardware requirements

- CPU: Pentium-compatible
- RAM: 128 MB minimum
- Disk space: 5–35 MB available, depending on localization and number of devices
- Network connection: TCP/IP for remote access

### Mobile endpoints

#### Operating systems

- Microsoft Windows Mobile 6.0 for Smartphone
- Microsoft Windows Mobile 6.0 for PDA
- Microsoft Windows Mobile 5.0 for Smartphone
- Microsoft Windows Mobile 5.0 for Pocket PC

#### Hardware requirements

- CPU: 195 MHz minimum
- RAM: 64 MB minimum
- Network connection: TCP/IP for remote administration and Activesync 4.5 or higher for wired policy installation/updates

### Centralized management

#### Operating systems

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

#### Hardware requirements

- RAM: 128 MB: 512MB recommended
- Disk space: 200 MB
- CPU: Pentium-compatible

### Strong encryption and access control

Prevent unauthorized access or use of desktops, laptops, tablets, smartphones, and PDAs as well as data on their hard disks with full-disk encryption.

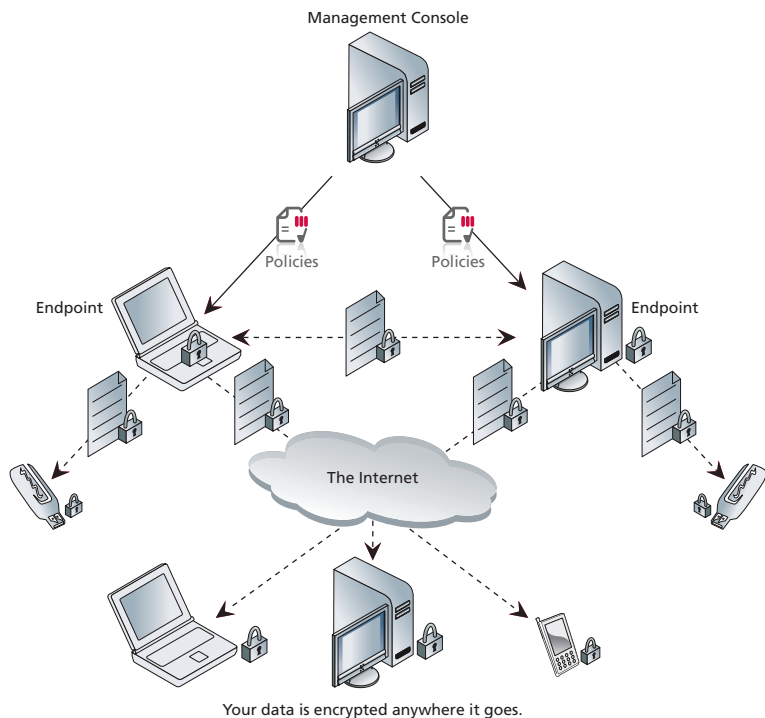
- Validate both user and machine prior to the PC starting using two-factor preboot authentication in addition to password authentication
- Achieve unsurpassed protection with industry-leading, award-winning encryption with algorithms including AES-256 and RC5-1024
- Encrypt devices transparently with no impact on daily operations and no end-user training
- Ensure files and folders remain encrypted regardless of where they are saved using Persistent Encryption Technology

### Meet internal and external security requirements

- Demonstrate a 360-degree audit trail, providing you with Safe Harbor protection so that a lost laptop or USB device presents no breach and requires no disclosure
- Set and enforce extensive mandatory security policies
- Control what specific file types or folders are encrypted without requiring end-user action
- Leverage FIPS 140-2 and Common Criteria EAL4 certification

### Easy centralized management and lower TCO

- Easy centralized management and lower TCO prevent loss of data everywhere with a full range of security and encryption solutions all managed from one central console
- Prove compliance with data privacy legislation and protect your assets and brand, retain customer loyalty and gain a competitive advantage
- Easily deploy and administer policies across the enterprise, saving time and money
- Recover passwords and tokens remotely and securely. A user's password can be reset after passing a verbal challenge/response verification and authentication, saving the helpdesk time and effort



### McAfee Endpoint Encryption

For more information about Data Protection, visit [www.mcafee.com/data\\_protection](http://www.mcafee.com/data_protection).

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://www.mcafee.com)

McAfee and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved. 1-dp-ee-001-0108

