McAfee®

Protect what you value.

McAfee Total Protection for Data

Comprehensive protection for your mission-critical data

The compromise of sensitive customer information has repeatedly made headline news over the past few years. Many times, the data has simply walked right out the front door on a laptop or other mobile device. Companies that suffer such a data loss risk serious consequences, including regulatory penalties, public disclosure, brand damage, customer distrust, and financial losses. In 2007, the average cost to companies resulting from data breaches was $6.3 million.[1]

In today's environment with the ubiquitous Internet and the rapidly growing number of mobile devices, protecting confidential customer information and intellectual property must be a top priority.

KEY ADVANTAGES

Data Loss Prevention

- Apply centrally managed security policies to regulate how employees access, use, and transfer confidential data

Enterprise-grade device encryption

- Gain full-disk encryption combined with strong access control to protect confidential data on all endpoints

Persistent file and folder encryption

- Enjoy automatic, transparent encryption of files and folders "on the fly," before they move through your organization

Centralized management console

- Define corporate security policies that control how sensitive data is encrypted, monitored, and protected from loss
- Reduce management effort, time, and training to increase ROI and lower TCO

Advanced reporting and auditing

- Monitor real-time events and generate detailed reports
- Prove internal and regulatory compliance measures to auditors, board members, and other stakeholders

McAfee Total Protection for Data

To secure your confidential data, McAfee® Total Protection for Data is the industry's most complete solution available. It uses strong encryption, authentication, data loss prevention, and policy-driven security controls to prevent unauthorized access and transfer of your sensitive information—anywhere, anytime.

Data Loss Prevention

Preventing data loss begins with improving visibility and control over your data, even when it is disguised. McAfee Total Protection for Data enables you to implement and enforce company-wide security policies that regulate and restrict how your employees use and transfer sensitive data via common channels, such as email, IM, printing, and USB drives. It does not matter if they are in the office, at home, or on the move. You remain in control.

Enterprise-grade device encryption

Secure your confidential data with an enterprise-grade security solution. Total Protection for Data uses full-disk encryption combined with strong access control via two-factor preboot authentication to prevent unauthorized access to confidential data on all endpoints, including desktops, laptops, handhelds, smartphones, and more.

Persistent, transparent file and folder encryption

Ensure specific files and folders are always encrypted regardless of where data is edited, copied, or saved—including desktops, laptops, handhelds, smartphones, and more. Total Protection for Data features content encryption that automatically, 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 to enforce encryption for specific files and folders without user interaction.

Centralized Security Management and Advanced Reporting

Total Protection for Data integration with ePolicy Orchestrator® (ePO™) is planned for 2008[2]. In addition to enabling centralized, policy-driven security management. This integration also provides advanced reporting capabilities to help meet tough privacy mandates from government and industry, ensure "Safe Harbor" protection, and demonstrate compliance to both internal and external auditors, board members, and other key stakeholders.

[1] Ponemon Institute's 2007 Cost of Data Breach Study.

[2] The information in this datasheet as it relates to future product plans should not be relied on in making a purchasing decision

SYSTEM REQUIREMENTS

ePO Server

Operating systems

- Microsoft Server 2003 SP1, 2003 R2

Hardware requirements

- Disk space: 250 MB
- RAM: 512 MB
  1 GB RAM (recommended)
- CPU - Intel Pentium II-class or higher - 450MHz minimum

Desktop and laptop endpoints

Operating systems

- Microsoft Vista* (all 32- and 64-bit versions)
- Microsoft Windows XP Professional SP1 or higher
- Microsoft Windows 2000 SP4 or higher

** Available for DLP in 2008*[2]

Hardware requirements

- CPU: Pentium III 1 GHz or better
- RAM: 512 MB recommended
- Disk space: 200 MB minimum
- Network connection: TCP/IP for remote access

Windows 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
- Network connection: TCP/IP for remote administration and Activesync 4.5 or higher for wired policy installation/ updates

Features

Data Loss Prevention

- Control how users send, access, and print sensitive data over the network, through applications, and onto storage devices: email, webmail, peer-to-peer applications, IM, Skype, HTTP, HTTPS, FTP, Wi-FI, USB, CD, DVD, printers, fax, and removable storage
- Stop confidential data loss initiated by Trojans, worms, and file-sharing applications that hijack employee credentials
- Protect all data, formats, and derivatives even when data is modified, copied, pasted, compressed, or encrypted—without disrupting legitimate day-to-day activities

Enterprise-grade device encryption

- Automatically encrypt entire devices without requiring end-user action or training, or impacting system resources
- Enjoy full-disk encryption support for multiple standard algorithms, including AES-256 and RC5-1024
- Identify and verify authorized users using strong multi-factor authentication

Persistent file and folder encryption

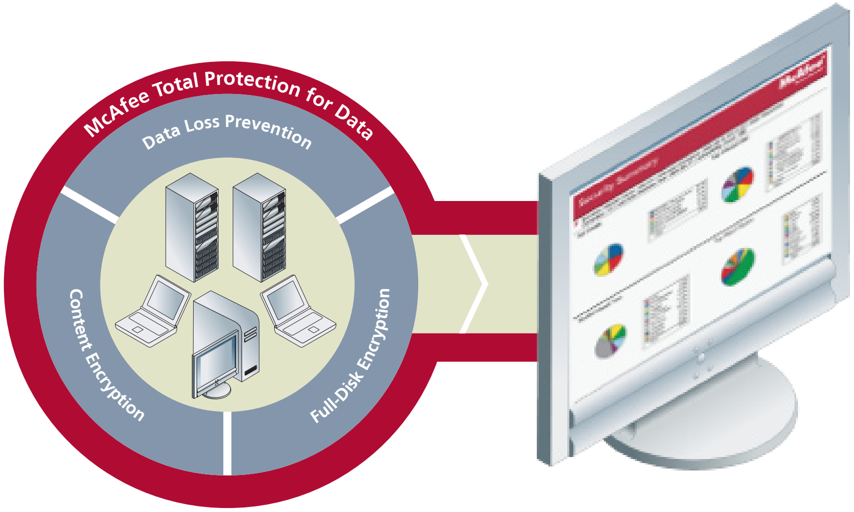
- Ensure files always remain encrypted when not in use by automatically adding a file header that travels with protected files
- Keep files and folders secure wherever they are saved, including on local hard disks, file servers, removable media—and even as email attachments

Centralized management console

- Use ePO to specify detailed content-based filtering, monitoring, and blocking of unauthorized access to confidential data
- Manage full-disk, file, and folder encryption; control policy and patch management; recover lost keys; and demonstrate regulatory compliance
- Synchronize security policies with Active Directory, Novell NDS, PKI, and others

Advanced reporting and auditing capabilities

- 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



McAfee Total Protection for Data

For more information about Data Protection, visit *www.mcafee.com/data_protection*.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com