



Ironclad Security for Lost Devices

Confidently protect valuable data while managing security

Ironclad Encryption with McAfee

Data breaches are widespread and costly

- 36 percent of data breaches involved lost or stolen laptop computers or other mobile data-bearing devices in the US³
- In the US, the average cost of a single data breach is \$6.75 million and \$204 for one lost data record⁴

Ingredients of ironclad encryption

- Comprehensive encryption solutions protect data on a wide range of endpoints, including laptops, smartphones, USB drives, and shared files and folders
- Robust, centralized management, shared policies, full reporting, and proof of protection—all from a single management architecture

Losing a laptop, smartphone, or USB flash drive can cost your organization more than you might think. The average cost of a *single* lost or stolen laptop is \$49,246.¹ Aside from hardware replacement, most of the financial impact results from factors associated with the loss of sensitive corporate data, including detection and escalation, intellectual property loss, lost productivity, and legal or regulatory costs. With data loss incidents and costs escalating, safeguarding valuable business and compliance-related information is one of most critical issues companies face.

McAfee data protection offers multiple layers of protection against data loss. McAfee® Endpoint Encryption encrypts data on desktop PCs, laptops, network files and folders, removable media, and USB storage devices. McAfee Enterprise Mobility Management provides security and mobile device management for a wide range of smartphones and mobile devices. And McAfee Data Loss Prevention and McAfee Device Control help companies understand, monitor, control, restrict, and protect data.

It seems that everywhere you turn, you hear about yet another data loss incident. A conservatively estimated 500 million sensitive records have been breached from 2005 to 2010.² With more and more data breaches grabbing attention in headlines, it's apparent that many organizations lack proper safeguards for their business-critical confidential data—especially when it comes to a mixed-device environment where information assets are stored, used, and transferred to desktops, laptops, smartphones, removable media, and portable storage devices.

Exactly what is the actual breakdown of the \$49,246 price tag for a lost or stolen laptop? According to the 2009 Ponemon Institute report *The Cost of a Lost Laptop*, which analyzed 138 different cases, the calculation is based on seven key cost components:

- Laptop replacement cost, including software and corporate overhead
- Detection and escalation based on the time spent by an employee trying to recover the laptop and reporting the loss
- Forensics and investigation cost, based on the number of hours IT staff spend on forensic analysis
- Data breach cost, estimated by Ponemon to be an average of \$204 per record
- Lost intellectual property costs, based on the probability that this intellectual property or other business confidential information would be discovered by a competitor or other opportunistic party
- Productivity losses of the employee whose laptop was lost
- Other legal, consulting, or regulatory cost

Piecemeal Encryption Solutions Leave Gaps

Mid-sized and large organizations are certainly aware of the problem, but many deployed encryption solutions are piecemeal at best and leave security gaps. Many businesses have full-disk encryption for just select laptops or protect all laptops and desktops but neglect the smartphones and USB drives.

Companies also need to address the security risks presented by employees who bring their own laptops with self-encrypting and solid-state hard drives to the office. While self-encrypting drives enhance data security, enterprise-wide encryption solutions aren't always compatible, making it difficult or impossible to track, audit, and report on these systems without forklift upgrades of existing laptops or re-architecture of the encryption environment when new laptops are added. Plus, the fact that software-based encryption and hardware-based encryption have separate management systems makes across-the-board policy enforcement impossible and leaves more gaps in data security.

Another issue is management. More often than not, encryption solutions and endpoint solutions are managed from different consoles, requiring additional training and consuming more of your IT staff's valuable time. Higher administrative overhead may make it cost prohibitive to add encryption to your security arsenal. Even if you do have the budget to deploy encryption, how good is the solution at making sure that all devices are encrypted, tracked, and secured? And is the reporting accurate and detailed enough so that IT can detect an incident and swiftly respond to it?

Overlooking just a single laptop or smartphone can spell disaster. According to the Ponemon Institute study, the cost of a lost laptop goes up dramatically the longer it takes to discover the loss and respond to it. If the loss is discovered on the same day, it costs a company \$8,950. If a week goes by before the loss is discovered, the cost jumps to \$115,849.⁵

Comprehensive Data Security with McAfee Encryption Technology

The best cure for data breaches is prevention—through comprehensive protection for sensitive information with McAfee Endpoint Encryption and McAfee Enterprise Mobility Management solutions.

A key component of the McAfee data protection portfolio, McAfee encryption solutions secure your data anywhere, anytime, regardless of where it is used, stored, or transferred. With industry-leading encryption, strong access control, and centralized management, McAfee encryption solutions offer sweeping protection for mixed device environments, including desktops, laptops, mobile devices, smartphones, network files and folders, removable media, and portable storage—with virtually no degradation in system performance and no need for forklift upgrades. And, since the encryption process and policy enforcement are completely transparent to the user, you reduce risk of data loss by preventing user errors and unauthorized access to sensitive data that circulates around the company.

- *Comprehensive range of endpoint encryption solutions*—No matter what mix of devices you have in your environment, you can be assured that your desktop PCs, laptops, smartphones, and mobile storage devices are encrypted and secured at all times. McAfee Endpoint Encryption technology also supports the latest PC technology, including software-based encryption, self-encrypting drives, solid-state drives, and Intel Advanced Encryption Standard-New Instructions (AES-NI) hardware acceleration. McAfee Enterprise Mobility Management provides security and mobile device management for a wide range of smartphones and mobile devices.
- *Persistent encryption safeguards sensitive data*—The longer it takes to discover a lost device, the bigger and costlier the problem. Yet, encryption can make all the difference by reducing lost laptop costs by as much as \$20,000, a Ponemon Institute study states.⁶ If an encrypted device is lost or stolen, the encrypted data is rendered indecipherable and unreadable if it falls into the wrong hands. More importantly, if it's a managed device and it can be proven that the data it contains is encrypted, it is generally considered not to be a data breach event. Designed for all data formats, from files and folders to email attachments and files copied to removable media, McAfee Endpoint Encryption technology uses central key management, which allows encryption to follow your data wherever it is moved or copied—persistently, so that data is safe at all times.

This occurs transparently, on the fly, and encrypted files look just like normal files to authorized users. There's no need for your users to get involved in the actual encryption process. Transparent, persistent enforcement minimizes user error and the risk of abuse by unauthorized users. McAfee Enterprise Mobility Management blends mobile device management with policy-managed endpoint security, network access control, and compliance reporting features in a seamless system. Security features include controls for authentication, encryption, applications, and resources like Wi-Fi. Management features include over-the-air (OTA) software and policy distribution, data collection, logging, and more.

- **Centralized management architecture cuts administrative overhead**—The McAfee® ePolicy Orchestrator® (McAfee ePO™) platform ties it all together for simple and effective management. Your IT staff administers McAfee-based endpoint, management, and encryption solutions from a centralized platform. From this central hub, your IT staff assigns and manages encryption keys, policies, deployment, and end-user provisioning for devices. Built for the future with support for a broad range of popular platforms and operating systems, McAfee Endpoint Encryption technology automatically applies policies to devices, even as you introduce new endpoint systems or devices. In fact, only one agent needs to be deployed by McAfee ePO software on each client to manage both endpoint security and encryption. Detailed auditing, enforcement, and compliance reporting help you ensure that nothing slips through the cracks and that your organization abides by industry regulations and government mandates.



Figure 1. Magic Quadrant for Mobile Data Protection.⁷ (Source: Gartner)

The Power of McAfee Endpoint Encryption Technology

As a leading vendor of endpoint encryption worldwide, McAfee supports more than 6,000 customers in this area of security. Customers in all sectors are incorporating McAfee Endpoint Encryption technology into their overall security strategy.

Citrix reduces risk with McAfee Endpoint Encryption technology

As part of its initiative to reduce risk company-wide, Citrix standardized on McAfee integrated solutions, including McAfee Endpoint Encryption technology, complemented by the centralized management capabilities of the McAfee ePolicy Orchestrator platform. With a 99.5 percent installation success rate, Citrix protects its 2,200 laptops, and both management and users are pleased with the fact that the solution is transparent, so it doesn't interfere with their productivity.

State governments and agencies protect, comply, and save

Budget shortfalls in the multibillions of dollars combined with an increase in data breaches targeting state governments were two of the challenges facing the State of New York as they sought to consolidate endpoint protection, increase efficiency, and control costs. The decision to choose McAfee as New York State's primary security vendor resulted in a 75 percent savings over a three-year period compared with licensing point products for endpoint security from multiple vendors. Fully cognizant of the importance of a proactive approach to data breach prevention, the State of New York Office of Cybersecurity and Critical Infrastructure Coordination had issued a policy requiring encryption of all mobile devices used by New York State. Ironically, many New York State agencies were unable to comply with the mandate because they lacked budget. But because the McAfee solution was so affordable, all agencies were fully protected and in compliance. Today, McAfee Endpoint Encryption technology is deployed at all 106 New York State agencies.

"McAfee lets me sleep at night. My workforce could not be truly mobile without the security products we've put in place."

—David O'Berry
 Director of Information
 Systems and Services
 State of South Carolina
 Department of Probation
 Parole and Pardon Services

"McAfee's encryption solution has more management options; greater connectivity with Microsoft Active Directory, which is crucial for us, and greater interoperability."

—Paul Baltzell
 Distributed Services Manager
 State of Indiana



Other state governments and state government agencies that collect and store sensitive personal information have selected McAfee Endpoint Encryption technology as an ironclad defense against data breaches and a way to ensure compliance with both state and federal compliance regulations. The Indiana State government, with 8,000 laptops across its 82 agencies, was looking to replace its existing encryption system, which had weak management capabilities. The State of Indiana opted for McAfee Endpoint Encryption technology, particularly because of its integration with McAfee ePO software, which they were already using with McAfee Total Protection™ for Endpoint and other McAfee products.

The South Carolina Department of Probation, Parole, and Pardon Services maintains data on more than 32,000 offenders and highly sensitive victim services data. A data breach could have serious consequences, including threats to public safety and possible re-victimization of individuals. A McAfee customer since 1998, the department proactively adopted McAfee Endpoint Encryption technology to increase protection of sensitive data to be in compliance with South Carolina's Consumer Protection Act. Encrypting laptops for its mobile workforce was another motivation for the move to McAfee Endpoint Encryption technology. The state agency also appreciated simplified management through "a single pane of glass" with the McAfee ePO platform.

McAfee Total Protection™ for Data suite

- Consists of McAfee Endpoint Encryption for PCs, McAfee Endpoint Encryption for Files and Folders, and McAfee Host DLP (including McAfee Device Control)
- Protects your data in use, in transit, and at rest against loss or theft using powerful encryption, strong access control, user behavior monitoring, and policy-driven security enforcement

Add McAfee Encryption Technology to Your Data Protection Arsenal

Today, organizations are concerned about safeguarding data to protect competitive advantage and/or to meet compliance mandates. Mobile devices like laptops, USB drives, and smartphones by their very nature are especially vulnerable to loss or theft—which places the data they contain or access in jeopardy.

McAfee Endpoint Encryption and McAfee Enterprise Mobility Management solutions provide a comprehensive yet modular solution set that makes encrypted data unreadable to unauthorized parties. These encryption solutions come with integrated, centralized management, shared policy administration, robust reporting, and proof of protection using McAfee ePO software for ease of management and lower TCO. This customizable solution set from a single vendor is flexible and extensible to meet your organization's needs today and as they evolve in the future.

Named by Gartner as a leader in mobile data protection, McAfee encryption solutions offer proven, industry-leading encryption and management technologies.⁸ For additional information, please contact your McAfee sales representative or authorized McAfee reseller.

1 Ponemon Institute, *The Cost of a Lost Laptop*, April 22, 2009.

2 <http://www.privacyrights.org/500-million-records-breached>

3 Ponemon Institute, *2009 Annual Study: Cost of a Data Breach*, January 2010.

4 Ibid.

5 Ponemon Institute, *The Cost of a Lost Laptop*, April 22, 2009.

6 Ibid.

7 *Gartner Magic Quadrant for Mobile Data Protection*, September 2011. This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from McAfee.

8 Ibid.

The Magic Quadrant is copyrighted 2011 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

