

# McAfee®



Protect what you value.

## Enabling Your Mobile Workforce without Putting Your Data at Risk

# Introduction

**Mobility isn't the next big thing—it IS the big thing.** Laptop computers are ubiquitous in every company, allowing employees to produce work not only in the office, but also at home and on the road. BlackBerrys, PDAs, and other handheld devices and smartphones can be seen in nearly every traveler's hands. And if you take a look into these travelers' luggage, you're nearly certain to find pocket-sized USB drives, MP3 players, CDs and DVDs—removable media upon which multi-gigabytes of data can be stored.

Analyst data squarely supports the mobile computing trend. In its 2007 annual report, "The Future of Mobile Computing," BCC Research estimates that the global market for mobile computing will reach more than \$88.9 billion by 2011. Fueling this growth are both laptop computers, which are expected to account for \$69.2 billion by 2011, and smartphones, which BCC Research estimates will have a compound aggregate growth rate (CAGR) of nearly \$17.8 billion. IDC, the Framingham, Mass.-based industry research firm, also anticipates that the market for converged mobile devices (e.g., smartphones and PDAs) will grow from 124.6 million units in 2008 to 376.2 million in 2012.

And as mobile devices and accompanying wireless technologies become more powerful and robust, demand for mobile office - and business - related applications will only increase, fueling the mobility trend. But with the surge in mobile access comes a growing need for security of the data stored on all types of mobile devices—from laptops to handheld devices to so-called 'flash' or 'thumb' drives. The more employees take their laptops or other mobile devices filled with sensitive company and customer data outside the physical enterprise, the greater the threat of data loss or theft.

In fact, security breaches related to mobile devices have been grabbing headlines around the globe. From the first big breach of a major wireless service provider's network in 2005, in which a hacker was able to obtain the provider's customers' passwords and Social Security numbers as well as download photos taken and stored by the customers on their mobile devices to the theft of government laptops with citizens' email addresses and other personal information to a recent theft of backup information tapes from the backseat of a courier's vehicle, the statistics strike



fear into the heart of every CIO. Millions of dollars of data lost. Countless hours of employee time wasted to recreate information. And the unquantifiable loss of customer trust and revenue, a tarnished reputation—not to mention the financial and fines incurred due to a breach of government regulatory compliance requirements.

*According to IDC's 2007 Security Survey, 51 percent of organizations that experienced a data breach said that the source of the breach was a lost or stolen laptop. Another 33 percent said that the breach was the result of a lost or stolen smartphone or PDA. But while CIOs recognize the security problem posed by the mobility trend—nearly 66 percent of CIOs responding to a 2007 survey sponsored by mobile device management vendor Mformation Technologies Inc. said that they are very concerned about data loss from mobile devices—most have not implemented a mobile security strategy within their organization. Why not? Because protecting organizations from mobile security breaches is complicated and difficult and often, CIOs simply don't know how to approach the problem.*

It's clear that enterprises must protect their brand, reputation, competitive position, and regulatory compliance status from this 'moving liability'. So what can a forward-thinking company that wants to encourage employees to be productive anywhere—office, home, or on the road—do to ensure the security of its intellectual property and privacy of customer data?

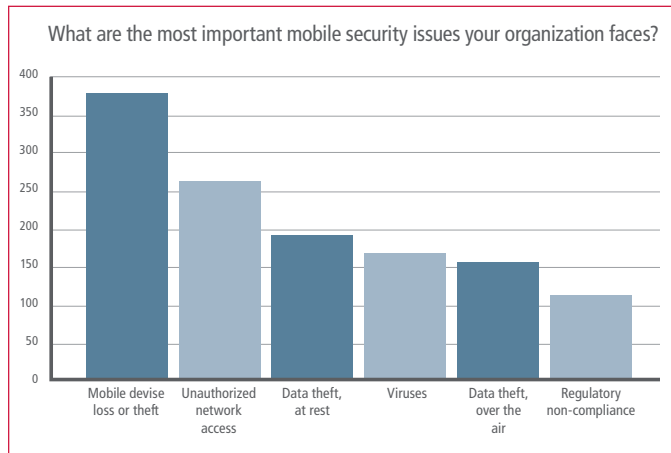


Figure1: SearchMobileComputing.com survey – Oct 2007.

## A Four-Pronged Mobile Security Strategy

Leading-edge companies hoping to encourage mobile access to improve employee productivity should put into place a comprehensive mobile security strategy that encompasses the following four areas:

- Ensuring that information stored at-rest on desktops, laptops, and other mobile devices remains safe and secure;
- Restricting and monitoring what data can be transferred or copied onto removable storage devices and media;
- Preventing the unauthorized viewing of data stored on all types of removable media; and
- Controlling what actions users can take with specific data (e.g., edit, change, update, and print) on any laptop, mobile device, or removable media.

The following section describes each prong of a comprehensive mobile security strategy in greater detail.

### 1. Securing data at-rest on laptops and other mobile devices

Because the number-one cause of data loss or theft is a stolen or misplaced laptop, organizations must protect themselves—and their confidential data stored on those mobile systems—from access should the laptop or mobile device fall into unauthorized hands. Encryption is the key technology that helps secure the data at-rest on (e.g., saved or stored) or in-transit between corporate laptops and other mobile devices, including Tablet PCs, smartphones, and PDAs.

To protect themselves, organizations should implement full-disk encryption to protect all the information stored on all corporate systems and removable devices. In addition, organizations should consider implementing file and folder encryption, ensuring that files and folders remain encrypted and unreadable by anyone other than authorized individuals, no matter where the file or folder is saved or transferred.

*"We are using McAfee to prevent instead of react. I don't want to spend millions responding to a breach. I'd rather spend our resources preventing one."*

—Craig Williams / Information Security Officer / The Doe Run Company

### 2. Restricting and monitoring what data can be copied onto which types of removable storage devices and media

The proliferation of various types of removable storage devices—USB flash drives, MP3 players, recordable CDs and DVDs, Bluetooth and infrared equipment, and more—is enough to give any CIO an Excedrin headache. More than half of the respondents to a recent McAfee-sponsored survey admitted to using portable devices to take confidential data out of their company every week. How can organizations protect themselves from this new security risk?

By restricting and monitoring what data can be copied or transferred to removable storage devices and media, organizations can ensure confidential data and other intellectual property does not leave the company's control. Part of any comprehensive mobile security strategy, controlling data transfer should be done in a granular manner. That is, organizations should be able to specify what data or content can be copied and which cannot, as well as to which types of removable media—even down to a specific device based on serial number.

*"Data protection is ranked as the number-one priority for CISOs."*

—2007 Merrill Lynch CISO Survey

### 3. Preventing the unauthorized viewing of data stored on removable media

Pocket-sized USB flash drives are one of the fastest-growing means of removable storage: they are small, portable, and provide incredible amounts of storage. But while they are a dream for users, they are a security nightmare for CIOs. It's just too easy for confidential information and corporate intellectual property to literally walk out the front door—and into the hands of unauthorized individuals, whether by design or by accident. In a recent study, over 55 percent of respondents claimed that they regularly brought documents out of the workplace on a USB drive. Of those, 17 percent admitted they accidentally left their USB drive in a public place.

Leading-edge organizations must protect the information on these USB drives as part of a comprehensive mobile security strategy. By encrypting the data stored on these drives and ensuring only authorized individuals can view it through strong access control and authentication, organizations can ensure that their confidential data remains safe and secure from accidental or intentional unauthorized access.

*"In 2007, the average cost to companies resulting from data breaches was \$6.3 million"*

*—Ponemon Institute's 2007 Cost of Data Breach Study*

### 4. Controlling what actions users can take with specific data (e.g., editing, updating, copying, and printing) on any laptop, mobile device, or removable media

It's not just the transfer or copying of data onto specific systems, mobile devices, and removable media that CIOs must worry about: it's what users do with the data once it's on that system. That means more than simply viewing the information. Can they email the information to an outsider? Copy it to another drive? Change it in any way? Print it onto paper and send it out to hundreds of others?

As part of a comprehensive mobile security strategy, organizations must implement strict controls over what actions users can take with specific data—and implement these controls on every system within their network, from desktops to laptops to smartphones and PDAs to every type of removable media and storage device. In this way, organizations can prevent data loss anywhere the data goes—at work, at home, or on the road.

*"We deployed McAfee Total Protection in about a week and we haven't had to deal with viruses or spyware since."*

*—Brian Young, Senior Network / Security and System Administrator, Adena / Health System*

## McAfee's Mobile Security Solution

McAfee Total Protection (ToPS) for Data includes the products you need to implement a comprehensive mobile security strategy that encompasses the four key areas described above. Comprised of McAfee Endpoint Encryption, McAfee Device Control, McAfee Encrypted USB, and McAfee Host Data Loss Prevention—all centrally managed by McAfee ePolicy Orchestrator® (ePO™)—the McAfee ToPS for Data suite brings together network and system threat protection, physical and behavioral controls for sensitive data, and compliance management in a single, integrated solution. So only authorized users can access your confidential and sensitive information.

### McAfee Endpoint Encryption

Offering two forms of encryption to protect data from unauthorized access when stored or in transit, McAfee Endpoint Encryption provides robust, certified, standards-based physical protection for data on every system in your organization. Full-disk encryption helps ensure that information remains secure when stored at-rest on desktops, laptops, tablets, and mobile devices.

### McAfee Device Control

To control how users copy data onto removable media, such as USB drives, MP3 players, CDs, and DVDs, McAfee Device Control lets you monitor and restrict what data can be copied onto these devices. First, deploy the software onto your managed endpoints. Then, define the policies that control which content can and cannot be copied onto which removable storage devices. McAfee Device Control automatically enforces these policies, monitors usage, and blocks any unauthorized attempts to use these devices or transfer data in violation of defined policies.

### McAfee Encrypted USB

With McAfee Encrypted USB, you can prevent data on USB drives from being viewed by unauthorized individuals, either accidentally or maliciously. McAfee's powerful encryption technology and strong access controls ensures that information copied and stored on USB storage devices is protected and can only be read by authorized users.

### McAfee Host Data Loss Prevention (Host DLP)

McAfee Host DLP lets you protect data from internal and external data loss threats with comprehensive monitoring, auditing, and control over user behavior across all endpoints. Host-based protection secures data regardless of where users or information go, or whether or not client machines are connected to the corporate network. A key component of McAfee ToPS for Data, McAfee Host DLP lets you monitor and control your critical information—even when the data has been modified from its original form.

## Conclusion

As the global workforce becomes increasingly mobile, it is more important than ever to prevent that workforce from becoming a liability to your organization. If just one employee loses a laptop, USB drive or handheld device or uses sensitive data in unintended ways, your entire company could risk a highly public breach incident.

In this environment you need new breeds of security applications to help shield your organization and employees from the latest mobile threats. With McAfee's comprehensive and integrated mobile security solutions, you have complete confidence and control of your confidential data and mobile workforce.

For more information on McAfee Total Protection (ToPS) for Data or McAfee ePolicy Orchestrator (ePO), visit: [www.mcafee.com](http://www.mcafee.com) or call us at 888.847.8766 - 24 hours a day, seven days a week.

## About McAfee, Inc.

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world.

With its unmatched security expertise and commitment to innovation, McAfee empowers businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security. [www.mcafee.com](http://www.mcafee.com)

---

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

McAfee and/or additional marks 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. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved. 1-cor-mobile-dp-002-0808