WHITE PAPER: SECURITY AND MANAGEMENT

Mobile Security and Management

Meeting the enterprise mobility challenge

Confidence in a connected world. Symantec.

White Paper: Security and Management

Mobile Security and Management

Meeting the enterprise mobility challenge

Contents

The enterprise mobility challenge

Enterprise executives are among the earliest adopters of every new mobile technology, and no wonder: phones, messaging devices, and wireless-enabled non-telephones like Apple's iPad concentrate productivity, utility, social engagement, and entertainment into a tiny handful. Mobile devices also embody and illustrate all four of the fastest-growing challenges to enterprise IT security that Symantec has identified:

- *Consumerization of IT*—Mobile devices are designed, sold and used as consumer devices, and enterprise-grade security and manageability are secondary concerns
- *Mobility*—This most fundamental attribute of mobile devices allows applications and data to reach easily across multiple networks, both trusted and untrusted, and exposes the devices themselves to high risks
- *Social networks*—Highly engaging real-time networks of nominal friends are exploited for social-engineering attacks on enterprise infrastructure and data, and phones make them available instantly, anywhere
- *Virtualization and cloud computing*—Mobile, cloud, and virtualization technologies are connecting enterprises to the world, and transmitting their information far beyond their corporate firewalls

Mobile devices are highly portable, carry enormous volumes of data, and connect across devices and networks using Wi-Fi, Bluetooth, infrared, and multiple mobile telephony standards. They are a gateway to countless productivity tools, entertainment resources, and opportunities for social interaction.

Mobile devices are a consumer's dream—and an IT security and management nightmare, *for exactly the same reasons*. Portability makes mobile devices easy to lose and steal, capacity puts business information at risk, and connectivity exposes enterprise networks to a dangerous world.

The purpose of this paper is to help IT professionals manage the transition of mobile devices from "consumer device on an enterprise network" to "just another endpoint." We will show how to get ahead of the mobile-device adoption curve, understand how these devices work in enterprise environments, and show what needs to be done now to incorporate mobile devices without excessive cost and risk.

Mobile security requirements

Mobile devices are powerful but vulnerable computing devices that penetrate and interconnect between networks quickly, and for which widespread adoption of security and management solutions remains on the horizon. Ultimately, they will join servers, desktops, and laptops standard elements of extended enterprise networks, both in the ways employees use them and the ways IT will inventory, secure, and manage them. To bring that day closer, consider these requirements for mobile security and management:

1: Visibility of devices and vulnerabilities

Simply scoping out the dimensions of the challenge is a major advance: you can't protect or manage what you can't see. Asset management—beginning with device inventory—is the essential first step to defining, securing, and managing mobile infrastructure. Visibility requires protecting devices across multiple networks, and includes scanning for current

security software and operating-system patch level in addition to model and serial number, and other information about the hardware device.

2: Effective protection on the device

Since they are essentially portable computers, mobile devices need the same multilayer protection we apply to other business endpoints, including:

- *Firewall* protecting the device and its contents by port and by protocol, regardless to which network the device connects
- *Antivirus protection*, again spanning multiple attack vectors, which might include MMS (multimedia messaging service), infrared, Bluetooth, and e-mail
- *Real-time protection*, including intrusion prevention with heuristics to block "zero-day" attacks for which a signature has not yet been published, and user and administrator alerts that an attack is in progress
- *Antispam* for the growing problem of short messaging service spam

3: Unified protection across hardware platforms and operating systems

Mobile devices are endpoints like any other, and their security and management should be integrated within your overall enterprise security and management framework, and administered in the same way—ideally using compatible solutions. This creates operational efficiencies, but more important, it ensures consistent protection across your infrastructure.

Defenses should be unified across Symbian, Windows Mobile, BlackBerry, Android, iPad, and iPhone operating systems, and their successors. And noncompliant mobile phones should be denied network access until they have been scanned, and if necessary patched, upgraded, or remediated—just as modern endpoint security software requires for laptops, for example.

4: Encryption

With mobile devices, loss and theft are major risks. Business Week reports that of 285 million mobile phones used in the U.S. alone, 30 million “go missing” every year. Passwords are inadequate security when a thief or hacker will maintain physical possession of the device over a long period. Protection should cover phone data such as contact names and numbers as well as e-mail, email attachments, and the data both may contain. Email encryption should happen automatically right on the mobile device for instant, protection of sensitive information over all the networks it may cross.

5: Secure confidential information

Loss of confidential data held on or accessed through mobile devices can result in direct revenue losses and remediation costs, plus long-term losses of customer and brand loyalty. Breaches occur—and thieves attack—at a network’s most vulnerable point. While content-aware data-loss prevention (DLP) technologies for phones are in the development stage, rapid adoption of these technologies on corporate networks will inevitably include mobile devices. Inventory, security, and management of mobile devices offer the best degree of protection today, and the best preparation for tomorrow.

6: Unified security and management

We've already discussed one management essential—discovering phones across multiple networks, determining their patch status, and scanning them for vulnerabilities. But disciplined management raises standards across the security spectrum, with capabilities that include:

- *Automatic updates* to the operating system, security application, and antivirus signatures and antispam data
- *Configuration and policy enforcement* remotely, over any network—including security and network access policies today, but extending to data loss prevention in the near future
- *Remote lock and wipe* to deny thieves and their customers use of the devices, and remove data before it can be decrypted and exposed
- *Event logging* to deliver "closed loop" security over the extended enterprise network, and monitor threats that emerge using mobile vectors

7: Scalability

Threats that target mobile devices or are introduced through them are the same for consumers, small businesses, and enterprises. Device-by-device security management is acceptable for individuals, but beyond the scale of a small family organizations need automated, policy-based security and management. And from the smallest business to the largest communications service provider, a mobile security and management vendor with the capability to scale with you as your business grows.

Mobile infrastructure grows with your business, when more employees use mobile devices, and as new mobile platforms and services are introduced. To keep networks secure and manageable at this pace requires a solution provider with an intelligence network capable of identifying threats on a global scale, and the best practices for securing mobile devices together with other endpoints in your organization.

Guarding the new perimeter

Your employees—and even their family members—are the new perimeter of your corporate network. They're constantly in motion, and they treat their devices—your network endpoints—as consumer devices: downloading music and applications, "sharing" contact information and files, browsing websites, receiving and responding to instant messages, and interacting with an expanding array of social-networking communications.

While the challenges of consumerization, mobility, social networking and virtualization are new, the security principles needed to meet them are already well established on corporate networks.

Mobile security needs to be centrally managed and seamlessly automated to protect information in place or in motion, personal identity and authentication data along with the integrity and efficiency of networks and infrastructure. It also requires backing from a global intelligence network so IT can respond instantly to changes in the external threat environment. Mobile security and management also needs to integrate with solutions used to manage laptops, desktops, and servers, creating a continuous protected environment as mobile devices take their place as just another network endpoint.

When security and management become pervasive across multiple networks and devices, everyone benefits:

- *Enterprises* gain visibility and control of all their mobile platforms, and their users can choose their devices without compromising governance and security
- *Carriers* gain an improved experience for their enterprise customers and stronger network security, and lower operational costs by eliminating malware, viruses and mobile spam
- *Consumers* gain security for their phones and personal data—including remote device lock or wipe in case of loss or theft, and anti-malware functionality to keep devices clean

Getting Started

Meet with Symantec to learn more about our Mobile Security and Management solutions, or visit go.symantec.com/mobile.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security** and **application security** solutions.

10/2010 21155057