

Keep Your Enemies Close: Three Steps to Bring Mobile Devices into Your Security Infrastructure

A call to action for IT and security professionals



“Keep your friends close, and your enemies closer.” Attributed to Machiavelli and Sun Tzu, this citation points to the importance of keeping a close eye on those who can hurt you the most.

Against a backdrop of unprecedented growth in smartphones and tablets in the enterprise, the consumerization of IT, software vendors creating mobile versions of their business applications, and the revelation that Web 2.0 technology is here to stay in the workplace, enterprise IT and security professionals are finding themselves under intense pressure to say “yes” to mobile devices on the corporate network.

This drive to support mobile devices and applications within the enterprise arrives on the heels of nearly a decade of collective investment in security and compliance numbering in the tens of billions of dollars. Following several high-profile data breaches—and in response to substantial regulatory and industry policy—corporations around the world have deployed security infrastructures to lock down, manage, monitor, and report on the security of their IT environments. The result is a reasonably effective security infrastructure that allows IT and security professionals to set access and security policies, enforce those policies, prove compliance, and certify to auditors that the policies have been followed.

Beyond becoming and staying compliant, organizations at the forefront of this curve have been able to optimize the technology and processes they established, driving down costs and using their security posture as a source of competitive advantage to facilitate business, resulting in noticeable growth.

Today's influx of mobile devices threatens that model. The countermeasures, processes, and policies that were implemented over the last several years rely on more traditional data center oriented client/server approaches, fixed-line infrastructure, and a defined network perimeter that, more often than not, rests at the physical perimeter of the organization. The existing model can't easily incorporate mobile devices accessing corporate resources and applications from anywhere, cloud services, virtualized desktops, and social networking. These newer computing models are pushing the security boundaries and creating even more pressure on IT organizations to manage and secure mobile devices faster than ever, across a greater number of platforms that host a multitude of mobile applications.

To deal with this, many organizations are creating a second security silo to manage and secure mobile devices and prevent them from creating new compliance gaps. Others are managing around the gaps with largely manual processes. And still others are just beginning to address mobility and are hoping that a major data breach does not occur. Creating a separate, parallel security silo around mobile devices is costly, inefficient, and out of alignment with security best practices. Organizations that are ahead of the curve recognize that these devices can cause harm, and are bringing those devices into the existing security infrastructure so they can manage them like they would any other endpoint.

Mobile Devices Pose Three Primary Risk Areas for Enterprises

Device loss

A lost device can wreak havoc if it's not properly locked down and equipped to have sensitive data wiped from it remotely, completely, and in an auditable way. A lost device with access to sensitive corporate, employee, or customer data can bring the same kinds of legal liabilities, media and regulatory scrutiny, customer notification requirements, and reputation loss that many businesses experienced over the last decade.

Data loss or breach

A device with access to corporate systems and business applications but without security measures commensurate with traditional computers is at a greater risk of losing data through theft or inadvertent data exposure because the user may be more careless due to the device's smaller form factor and lower perceived risk.

Exposure of the corporate network to malware

Mobile malware is a threat of growing significance, and many experts believe explosive device growth and diversity coupled with operating system insecurity are too irresistible for cybercriminals to ignore. Given the alignment of a cybercriminal's incentives with the potential rewards (such as access to lucrative personal financial data today, and, over time, the ability to intercept financial transactions as devices increasingly become the platform of choice for mobile transactions), mobile devices are poised to become the next malware frontier. Not only are enterprises at risk of having their users' devices infected with malware, but they are also at risk of having their corporate networks infected as those devices become easy entry points into systems housing mission-critical applications and sensitive data.

Most enterprises make significant investments in security that result in largely effective systems and process. But with mobile devices posing significant risks to the status quo, there is a strong argument to be made for bringing mobile devices into the existing security infrastructure and managing them (and especially managing their security) alongside other endpoints such as servers, desktops, and laptops. Rather than building a new system, organizations should seek to bring devices into their management frameworks and have them become part of the security infrastructure—aligning with the same policies and practices for access controls, anti-malware, data loss prevention, web protection, and network protection—as other endpoints in the enterprise.

What can organizations do to make this happen? There are three primary steps organizations should pursue in parallel:

1. Secure the mobile device.
2. Secure the mobile data.
3. Secure the mobile apps.

These steps involve, but are not limited to, integration with technologies such as anti-malware, data loss prevention, web protection, application security, comprehensive threat information, and of course, centralized security management.

For each of the three steps, we identify basic requirements and next steps, and highlight the most important security technologies needed to achieve the objective.

Solution Brief Keep Your Enemies Close: Three Steps to Bring Mobile Devices into Your Security Infrastructure

Secure the Mobile Device

Basic Requirements Initial technologies that support the objective*	<ul style="list-style-type: none">• Remote lock• Device encryption• Password security• Automated compliance policy enforcement
Next Steps Security technology integration necessary to achieve the objective*	<ul style="list-style-type: none">• Anti-malware• Web protection• Global threat intelligence• Centralized security management

* The enterprise objective is to bring mobile devices into the existing security infrastructure and manage them (especially their security) alongside other endpoints.

Basic requirements

To secure users' mobile devices, organizations must be able to lock down the devices. Mobile device management solutions on the market today do this in different ways, but an emerging best practice is to leverage the native device security features such as encryption and remote device lock. Beyond harnessing native features, organizations must take a policy-based approach to enforcing compliance similar to other endpoints. This includes ensuring that operating system levels are up to date, encryption is enabled, enforcing strong password security, and verifying that the devices have not been compromised, not only upon initial provisioning but each and every time the device interacts with the corporate network. Using native device security features and policy-based compliance enforcement are basic requirements.

Next steps

In order to truly integrate devices into the security infrastructure to protect them, organizations need to find ways to apply the same level of protection to devices as they do for their other endpoints. This includes deploying anti-malware and web protection on each device, as well as leveraging cross-product security capabilities such as global threat intelligence and centralized security management.

Anti-malware

Mobile malware is growing at an alarming rate, reminiscent of how malware has compromised desktop computing environments. Because the malware threat landscape is far more sophisticated and onerous today than ever before, it is imperative for organizations to deploy mobile device-optimized anti-malware in the same "enterprise" way as they do for traditional endpoints—that is, policy-based and auditable, with quality assurance processes and deployment best practices.

Web protection

The primary vehicle for hosting and delivering malware is the web. This has begun to play out in the mobile web as well, as evidenced by high-profile incidents such as the more than 50 malware "apps" removed from the Android Market in March 2011. In addition to becoming a malware delivery mechanism, the mobile web is fast becoming a hunting ground for cybercriminals. With mobile devices poised to take over PCs in web access (and already doing so in some countries), the mobile web will soon become the venue of choice for sites that engage in phishing and other scams. Ideally, organizations will integrate with security technology at the host, as well as the network, levels. Having host web protection ensures ubiquitous safe browsing and search, while gateway protection allows organizations to stop threats at the perimeter and take a policy-based approach to content viewing across all endpoints—laptops, desktops, tablets, or smartphones.

Comprehensive threat information

As organizations protect against suspicious files or websites to safeguard mobile devices, integration with a cloud-based reputation system that sees global threats across all threat vectors is essential. Just

Solution Brief Keep Your Enemies Close: Three Steps to Bring Mobile Devices into Your Security Infrastructure

as many organizations are leveraging security intelligence at each of the network, message, web, or file threat vectors to update security technologies in the traditional computing world, so they must with mobile devices.

Centralized security management

In each protection vector, mobile device integration into security management frameworks is necessary. Once organizations administer, apply policy, take action, and report on mobile devices centrally and alongside the rest of their security technology, then they can more fully understand their risks, prioritize actions, and prove compliance.

Secure the Mobile Data

Basic Requirements

Initial technologies that support the objective*

- Remote lock
- Device encryption
- Remote wipe (total data deletion)
- Remote selective wipe (deletion of certain data)
- Identity and access management

Next Steps

Security technology integration necessary to achieve the objective*

- Data loss prevention
- Global threat intelligence
- Centralized security management

* The enterprise objective is to bring mobile devices into the existing security infrastructure and manage them (especially their security) alongside other endpoints.

Basic requirements

In its 2010 enterprise mobility survey, *CSO Magazine* reported that 64 percent of respondents in companies of 1,000 employees or above identified data loss prevention among their top mobile security challenges.¹ When we talk about securing data, especially as distinct from securing devices, we are referring to the prevention of data being lost, stolen, accessed by the wrong parties, or inadvertently leaked to the wrong parties. This is not only a significant security issue (consider corporate intellectual property), but also a huge compliance one (consider GLBA, PCI, and HIPAA). Basic requirements focus on protecting the data through remote lock and encryption in the event that the device becomes lost or stolen. Strategies also include data removal from a device in the event that the user keeps the device but is no longer allowed access to the data (such as in the event of employment termination), which would include a remote data wipe (data deletion from the device), as well as selective wipe (selective deletion of certain, but not all, data from the device, such as removal of email and personal information manager (PIM) data, but not of personal apps and data such as Flickr and photos).

Beyond technologies that focus on data loss or leakage, authentication and access control to the network and applications are also basic requirements for mobile devices because they ensure that only those with authorization, a compliant device status, and proper credentials are given access to data in the first place. Thus, mobile devices must be brought into the organization's access management fold. They must leverage existing user directories like LDAP, adhere to the same password policies enforced on the rest of the IT environment, have the same role-based authorizations applied to them, and must integrate with an organization's strong authentication systems such as PKI, one-time password technologies, or biometrics.

Next steps

Beyond performing rudimentary data loss prevention tasks such as remote lock, wipe, and selective wipe, organizations need to be able to provide true data loss prevention, many via an interim secure container approach.

1. Source: *CSO's Enterprise Mobility Survey*, IDG Research, October 2010

Secure containers

For mobile devices to be integrated into the security infrastructure, they must be integrated into data loss prevention (DLP) frameworks on hosts and ultimately on the network. Some organizations have addressed this by deploying a secure container or sandbox, a proprietary wrapper for email, and, in some cases, contacts and calendars, that sequesters the apps from the rest of the device. While this can be effective, so far it has been at the expense of the user experience, and is not scalable or appropriate for the long term. Asymco recently noted that more than 60 apps were installed per iOS device.² Building a secure sandbox for each app just doesn't scale to address the hundreds of thousands of apps that are making their way to mobile devices. Most organizations believe that what's needed is a secure device on which all apps can sit, and then, in some cases, a belt-and-suspenders approach with added security for email.

Data loss prevention

Many organizations believe that the more practical approach is to secure the data themselves by doing true data loss prevention at the host (and ultimately at the network) rather than to sequester an app from the rest of the device by building a proprietary sandbox around it. This "secure container 2.0" approach enables organizations to extend their DLP strategy to mobile devices and gives them the ability to discover, classify, monitor, manage, and prevent loss of critical business data.

As in the prior section, comprehensive threat information and centralized security management are not only key ingredients but serve as integration machinery across the security infrastructure, letting one countermeasure "learn" from a threat seen in another threat area or in a completely different part of the world, and, of course, enabling centralized visibility and control of IT security and compliance in the organization.

Secure the Mobile App

Basic Requirements

Initial technologies that support the objective*

- Enterprise app store

Next Steps

Security technology integration necessary to achieve the objective*

- App scanning and certification
- App monitoring
- Global threat intelligence
- Centralized security management

* The enterprise objective is to bring mobile devices into the existing security infrastructure and manage them (especially their security) alongside other endpoints.

Basic requirements

Now more than ever, with the explosion of mobile apps and the app store delivery model, mobile apps are a front-and-center security concern for consumers and businesses alike. For organizations to deliver and maintain mobile application security, basic requirements include rolling out an enterprise app store to ensure that users have access to and download the recommended corporate apps, securely receive them over the air, and are alerted to and download updates when available. Secondly, organizations need to leverage this feature to keep an accurate inventory of the mobile apps that are installed at any given time, and be able to report on them by device, user, and group, as well as take action such as blocking certain apps or making other policy-based decisions based on what apps are installed in the organization.

Next steps

In a recent investigative piece on 101 popular smartphone apps published in *The Wall Street Journal*, more than half were found to exhibit inappropriate behavior with personal data stored on the phone.³ Moreover, Apple, Google, and others have recently come under scrutiny about location tracking and user privacy. Besides app *behavior*, there is also significant concern about app vulnerability and integrity, harkening back to the example of malware in the Android Market.

2. Asymco, January 16, 2011, <http://www.asymco.com/2011/01/16/>

3. "Your Apps Are Watching You," *The Wall Street Journal*, December 17, 2010

Solution Brief Keep Your Enemies Close: Three Steps to Bring Mobile Devices into Your Security Infrastructure

Beyond organizations using the enterprise app store model to ensure a level of app consistency, secure delivery, and reporting, the next step for both organizations as well as the whole mobile security market includes establishing a mobile app security model that has three primary features or functions:

1. *App scanning and certification*—The first step of the model for mobile application security involves having mobile apps scanned for vulnerabilities or malware and certified that they are free from both. This scanning and certification should be an ongoing process, similar to the process of scanning and certifying e-commerce websites that they are who they claim to be, aren't a copycat phishing site, or haven't been otherwise compromised.
2. *App monitoring*—Even if the app has no vulnerabilities, isn't infected with malware, and hasn't been altered, it can still exhibit unusual behavior. The second step of the model is to scan mobile apps for what permissions they have on the device, as well as monitor those behaviors on the device for malicious or inappropriate behavior, such as the sending of an individual's private information to a third party.
3. *App reputation and comprehensive threat information*—The third step of the model is to share and learn from mobile app behavior in the aggregate. The knowledge gained from the monitoring of app activity on any one device should be aggregated and analyzed against that learned from other devices. It should also be correlated with threat data from other vectors (file, web, message, network connection) for a comprehensive threat picture and to capture insight into threats' temporal nature. For example, a mobile application may be interacting with an IP address that is temporarily compromised; the app's reputation should reflect this only for the duration of the threat and improve after threat remediation. These elements—both app-specific and from other threat vectors—would become part of a dynamic mobile application reputation for each app that would help individuals and organizations make decisions about which apps to download, keep app vendors honest, and provide an understanding about the risks to users and the organization. Ideally this would happen in the cloud for scale, efficiency, and pervasiveness.

Comprehensive threat information and centralized security management are key ingredients in identifying and reporting on insecure, infected, or badly-behaving mobile apps.

Summary

In summary, many organizations recognize that building a second security infrastructure around mobile devices doesn't make sense. They are already requiring a set of "table stakes" or basic security features—capabilities such as native device encryption, data loss prevention, and an enterprise application store—and, in many cases, securely connecting mobile devices to core data center services, directories, authentication solutions, and security management frameworks. The next step is to bring those devices into the security infrastructure through integration with key security technologies—from anti-malware to data loss prevention to application security—to protect the mobile device, the mobile data on it, the mobile apps, and, ultimately, the organization.

What You're Securing	Description	Anti-malware	Data loss prevention	Web protection	App scanning and certification	Application monitoring	Global threat intelligence	Centralized security management
Device	Lock down the device, especially if lost or stolen	•		•			•	•
Data	Protect corporate or sensitive data from loss, theft, or inadvertent leakage		•			•	•	•
Application	Ensure that mobile apps are free from vulnerabilities or malware and aren't behaving inappropriately on the device				•	•	•	•

Solution Brief Keep Your Enemies Close: Three Steps to Bring Mobile Devices into Your Security Infrastructure

McAfee, the world's largest dedicated security company, has a long history of protecting organizations by securing their IT infrastructure. We are a long-time believer that security and compliance are achieved through integration, and we have prioritized investment in integration of our own technologies through our security management software, McAfee ePolicy Orchestrator® (McAfee ePO™) software, cloud-based McAfee Global Threat Intelligence™ multithreat vector reputation capability, and security technology point integrations. Moreover, we have helped our customers get the most out of their security investments by integrating with the technologies of more than 100 third-party security vendors, members of the McAfee Security Innovation Alliance and a core component of Security Connected, our open framework for delivering security that offers ubiquitous and continuous protection for our customers' IT infrastructure.

We have applied Security Connected to mobile devices, with a robust security integration roadmap. Starting with the integration of McAfee Enterprise Mobility Management (McAfee EMM™) software, our enterprise mobility solution, with our security management software, McAfee® ePO software, for centralized security visibility and control of mobile devices, we are dedicated to enabling our customers to manage mobile devices alongside the rest of the security infrastructure.

Anti-malware is next. Leveraging more than 20 years of fighting global cyberthreats, including a 10-year history offering mobile anti-malware to more than 150 million mobile devices via some of the world's largest service providers, we are integrating our award-winning mobile anti-malware technology into our enterprise management framework.

Following that is data loss prevention (DLP). McAfee has been a leader in DLP for the last several years following its acquisitions of DLP companies Reconnex and Onigma. Our objective is to integrate mobile devices with these technologies where appropriate, as well as develop and license new technology to achieve mobile device DLP at each of the secure container, host, and, ultimately, network levels.

Next on the integration agenda is web protection, with our host-based McAfee SiteAdvisor® software to mobile devices in enterprises, as well as the integration of our McAfee EMM server-side software with McAfee Web Gateway to enable web enterprise policies, content filtering, and web-based malware protection that occur at the gateway to apply to mobile devices in the same way they do to other endpoints.

In parallel to these activities, we are extending the expertise we gained in our award-winning McAfee SECURE™ website certification program to apply the same framework to mobile apps and are using that foundation to create a complete mobile app security model consisting of app vulnerability scanning and certification, app monitoring, and app reputation leveraging McAfee Global Threat Intelligence, the most comprehensive cloud threat intelligence in the industry.

Longer-term, we are extending McAfee EMM's already-robust mobile identity and access management capabilities—spanning strong authentication, directory integration, and role-based access control—to integrate mobile devices with network access control (NAC). This will allow us to extend the same fine-grained NAC policies to mobile devices as we have to other endpoints.

Similarly, we plan to bring mobile devices into our perimeter security technologies, such as our next-generation firewall, so that they are governed by the same network traffic and web application policies as other endpoints.

Finally, we are targeting our Software-as-a-Service (SaaS) expertise—acquired and developed from our acquisition of MX Logic and used for email, web, and other security offerings—to mobile devices. Our goal is to offer our customers flexible delivery options to support both their infrastructure and business models.

All of this is, of course, within the context of our Security Connected open framework and reflected in McAfee ePO software, our security management software.

McAfee, the world's largest dedicated security company, is unique in its ability to bring mobile devices into the existing infrastructure for a truly secure and productive mobile workforce.

Solution Brief Keep Your Enemies Close: Three Steps to Bring Mobile Devices into Your Security Infrastructure

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

<http://www.mcafee.com>

