A 3-STEP PLAN FOR MOBILE SECURITY

websense®

A complex problem that requires a holistic approach

Mobility is here. Mobility is now. Mobility (along with cloud and social media) is one of the three new technologies that brings new productivity opportunities—and associated security risks. Add in the consumerization of IT, an explosion of corporate and personal mobile devices, and the fact that there are no simple mobile security solutions, and you have one of the major IT security strategy challenges of 2012.

The challenge is how to enable productivity and mitigate the threats, vulnerabilities, and risks in a way that strikes the best balance and lowest total costs.

This paper identifies specific countermeasures and management controls that you can use to establish a mobile security strategy that encompasses both corporate and personal devices. It also covers the threat scenarios, risks, complications, and solutions that IT security professionals should use to guide their decisions in this critical area of enterprise vulnerability.

Organizations that narrowly focus on one aspect of the problem and fail to holistically address the security challenges posed by mobility, as well as consumerization and device proliferation, run the risk of much lower user satisfaction, productivity, and business gains, along with higher costs and even exposure of sensitive data.

Start with your goals

Regardless of the devices involved and who owns them, what are you trying to accomplish? Is the goal to provide mobile access to useful corporate resources such as email, file services, and intranet apps? If so, having highly limited, isolated mobile devices provides little value. In order to provide secure mobile access to these valuable resources (which is the goal of most organizations), you must:

1. Protect accessed ***data*** that is now local to the client device, and
2. Protect the client ***device*** itself, which serves as a conduit to both local and remotely accessible resources.

As you clarify your objectives you begin to reveal the security tools and technologies that you will need. Some examples:

- Communication over unsecure networks requires an authenticated and encrypted tunnel.
- Protecting data that is both stored and in use on mobile devices requires encryption and data loss prevention (DLP).
- Device protection requires configuration management and anti-malware software.

Identify and understand the threats

It is easy to see why data loss is such a high priority for mobile security. Regulatory requirements and the low cost of mobile devices contribute to the problem. As this table illustrates, most organizations should start with a focus on tools and techniques that help protect mobile data.

Threat	Risk
Lost or stolen device	Unauthorized access to local or network-based data; data loss
Lost or stolen media card	Local data loss
Misuse of local comms (e.g., Bluetooth, IR)	Compromised/infected device, and data loss and potentially degraded operation
Compromised apps	Data loss and potentially degraded operation
Malware	Data loss and potentially degraded operation
Web/network-based attacks	Data loss and potentially degraded operation

Countermeasures and other related controls

Given the objectives, threats, and risks discussed above, we present below three tiers of countermeasures and controls to help you establish and maintain a mobile security strategy.

Because of the scope of the problem, we recommend that you start with the first set. Then adopt items from the other two, with your schedule based on such things as your organization's tolerance for risk, the nature of the business you are in, regulatory requirements, and the level of mobile maturity in your organization. Some of the security controls listed below—such as mobile DLP, enterprise sandboxing, and self-defending apps—are newly emerging solutions. Unless your need is critical, delay adoption of these. More mature solutions are on the horizon that will be easier to implement and manage.

Tier 1: Mobile Device Management (MDM)

The term mobile device management is an artifact of convenience in this context. It's the capabilities that matter most, not the specific product category they come from. Some organizations get everything they need from Exchange ActiveSync® or BlackBerry® Enterprise Server, while others require a fully blown enterprise-class MDM solution. No matter which MDM solution makes sense, most organizations will eventually find it necessary to also implement some of the supplemental security measures described below.

Because current MDM offerings are light on security, we can expect the industry to evolve. Specifically:

1. MDM vendors may add more security capabilities to their solutions.
2. Mobile security vendors will add MDM capabilities to their solutions (this is more likely because it is easier to add simple to complex (that is, MDM to security), than vice-versa.

Most organizations identify data loss as the top concern in the mobile scenario. That's why the primary emphasis should be on tools and techniques that help protect mobile data.

3. MDM and advanced mobile security could remain independent solutions.

All of these scenarios can deliver good solutions to the market, but the best integration and lowest overall costs are most likely if mobile security vendors add MDM.

While the primary objective of MDM is centralized life cycle management of mobile devices such as smart phones and tablets, many of the so-called device management features are also relevant from a security perspective. For example, if you can configure Wi-Fi settings and update applications, you can use these same features to reduce a device's surface area for attack. And other features such as remote wipe and encryption control provide added layers of data protection.

Robust MDM solutions should include the following:

- **Application management** - Includes the ability to inventory a device's applications, distribute/update software, and restrict the use (if not installation) of individual applications. It also often includes support for a self-service portal and/or enterprise app store.
- **Configuration management and resource control** - This entails having control over a wide range of device-level capabilities and parameters including password requirements, camera functionality, SD card usage, and VPN, Wi-Fi, Bluetooth, and encryption settings.
- **Device integrity** - All of your defenses are effectively undermined when a mobile device is jailbroken or rooted. Being able to detect this condition is, therefore, a critical capability.

- **Device recovery and loss mitigation** – This include device tracking, manual and automatic lock-out, manual/automatic wiping of all or selected data, and support for device-level backup and restore.
- **Support and service management** - Remote control is useful for technical support, while expense control is intended to moderate usage, particularly when costs are high (e.g., roaming abroad).

What about policies, agreements, and user awareness? Policies are a key tool for any mobile security strategy, and the policies you choose determine the specific technical controls you need. Getting users to sign mobile-use agreements that document their rights, their responsibilities, and the company's rights is also crucial (e.g., this is where you would include a clause that allows the enterprise to wipe the device in exchange for providing the user with access to corporate resources). Signed agreements are especially important when bring-your-own-device (BYOD) and subsidized-usage models are supported, primarily due to legal uncertainties around liability and rights to data. And even though ongoing user awareness training on mobile security is probably a good idea, history proves that such efforts are not often very effective.

Tier 2: Supplemental Security

MDM-oriented security capabilities are an excellent starting point for a mobile security strategy. However, as mobile access scenarios continue to expand and the development of mobile malware continues to accelerate (in other words, as vulnerabilities, threats, and risks continue to grow), the effectiveness of MDM for security drops lower and lower. IT needs to implement measures that pick up where MDM leaves off in order to bolster secure access, threat protection, and data protection.

Secure access - ActiveSync and/or MDM-based security may be sufficient when mobile users are only using email. Once you provide access beyond email, three additional, access-oriented countermeasures become increasingly relevant: (1) strong authentication to the network—e.g., with tokens (2) an encrypted tunneling capability that supports access to all types of apps—e.g., an SSL VPN, and (3) a host-integrity-checking capability that supports access to all types of apps, and a host-integrity-checking capability that restricts access based on the security state of the user's device (available standalone or as an integral component of leading SSL VPNs).

Threat protection - Mobile malware has not historically been a major concern, but that started changing in 2011 and is expected to grow even faster in 2012. As a result, anti-malware for mobile platforms is becoming increasingly important—especially because the highly dynamic nature of today's web and the threats it harbors means that conventional technologies and mechanisms in this area (e.g., signatures) are glaringly insufficient. **What organizations need instead is a robust web security "cocktail" that examines content from every possible angle to detect new threats.** This requires real-time threat intelligence using multiple, complementary inspection engines capable of delivering real-time threat analysis and content classification. Equally valuable will be the ability to filter mobile applications based on reputation. Still emerging, this capability is analogous to reputation filtering for email, URLs, and downloaded files, but focuses instead on preventing users from downloading malware-infected mobile apps – a growing problem, particularly for non-curated app stores.

Data protection - Additional coverage in this area comes primarily in the form of DLP technology. The starting point for a complete solution is back at headquarters, where email and web security gateways with embedded DLP functionality should be used to control what data can make its way onto mobile devices in the first place (e.g., via email, or web-based file sharing services such as Dropbox). For data that does make it onto mobile platforms, the next layer of protection should be a mobile

DLP capability that helps keep the data from being either unwittingly or maliciously exposed. Notably, the need for mobile DLP is also being driven by increasing reliance on SaaS applications, where both data and users are outside the corporate perimeter and the protection it typically provides.

Agent vs. Cloud

What's the best way to deploy supplemental threat and data protection capabilities: local software agents, or cloud-based services? For some of the most popular platforms – such as Apple iOS – there's no option. The architecture limits the functionality or entirely precludes the use of security agents. Android supports agents, but the footprint on the device should be as lightweight as possible to reduce its performance impact. **Further tilting the scales in favor of cloud-based services are advantages such as: quicker, easier, and less costly implementation; universal platform compatibility; and greater adaptability.** Local agents can provide incrementally better functionality and effectiveness, but it seems unlikely that this will be enough of an advantage to offset the strengths of a cloud-based approach.

Tier 3: Emerging security measures

This third tier of countermeasures are fairly new to the market, and are often classified as advanced or emerging. Early adopters of such technologies tend to have a very low tolerance for risk, extremely sensitive data, or face very strict regulatory requirements.

App/desktop virtualization - Never allowing sensitive data to leave the data center in the first place clearly provides a superior degree of protection. One way to do this while still enabling view-only access to essential resources is to deploy server-hosted app and desktop virtualization solutions (e.g., from Citrix or VMware).

Self-defending apps - In some instances organizations will have the option to select mobile apps that have been designed from the outset to be inherently more secure – for example, by incorporating their own encryption and key management functionality, and relying less on native platform features and data storage locations for protection.

Enterprise sandbox - The intent with sandbox technology is to create an isolated zone on the mobile device where users can work with enterprise resources. Access to the zone depends on authentication and authorization, while all data transmitted to, from, and within the zone is encrypted. For mobile devices that support this technology, the result is another powerful layer of data protection. Tradeoffs include relatively limited app support and a hit to user experience, as native email and calendaring apps cannot be used to access enterprise resources.

Always-on-VPN - This approach involves routing all data traffic back to headquarters via an encrypted tunnel. In this way it can be protected by all of an organization's centrally implemented countermeasures, including full enterprise-class DLP. Drawbacks include slower performance, increased traffic load on corporate security and networking infrastructure, and the complexity of having to create policies that also accommodate personal-use objectives.

Caveats and complications

Nothing related to information security is as easy as it first looks, and this is doubly true for mobile security. Here are two topics that are worth mentioning:

Device and platform diversity - The greatest complication to an organization's mobile security strategy is by far the diversity of mobile platforms and devices. This manifests itself in a couple of ways. First, differences in platform architecture impact both the need for and availability of many add-on security capabilities. For example, the isolation model employed by Apple iOS not only diminishes the effectiveness of most malware, but at the same time precludes use of fully functional security agents. Other platforms have

varying resistance to malware and other types of threats, along with varying degrees of support for local security agents. A related issue is that platform, device, and service provider diversity also impacts the availability and effectiveness of native security capabilities. The bottom line is that there is considerable variation from device to device in terms of both (a) what is necessary from a security perspective, and (b) how it can best be accomplished.

Different ownership and usage scenarios - Additional complications arise from new and varied ownership and usage models. No longer are all client devices owned by the organization and used strictly for business purposes. Employees expect to be able to use their mobile devices for personal tasks. And different ownership and reimbursement arrangements often lead to different policies and capabilities. For example, with BYOD and no reimbursement to users, wiping data needs to be a last resort and should be selective (i.e., wipe all business but no personal data). Adding service reimbursement into the mix, however, changes the situation. Wiping all data now becomes a more acceptable and therefore prominent part of the security plan, while other functionality also becomes more relevant, such as expense control.

Characteristics of an ideal enterprise solution

No one turns in their laptop or desktop when they get a smartphone, so mobility just adds to the challenges of enterprise security. This—and budget pressures—drive the need for administrative efficiency and low cost of ownership when selecting mobile security solutions. For today's businesses, ideal solutions will be those that are enterprise-class in nature and that keep costs down by minimizing the number of products and vendors.

Enterprise-class - Key features that should be a part of all mobile security solutions to further reduce cost and improve effectiveness include: centralized management, role-based administration, directory integration, group policies, flexible reporting, and configuration audit trails.

Consolidation - Meeting the organization's needs with a smaller set of products and vendors invariably reduces cost and complexity while improving integration and effectiveness. This is why IT/security managers typically favor solution providers that offer the greatest portfolio of capabilities for the greatest number of devices they intend to support (particularly across tiers 1 and 2). Even further gains can be realized if the advanced threat and data protection capabilities needed to support mobile devices are available as integral extensions of the solutions already being used to provide similar capabilities for the organization's fixed users/devices.

Conclusion

The need to support and secure a growing population of mobile devices is here now. The challenge of doing so, however, is complicated by a number of factors, especially: (a) the diversity of platforms and devices and how this impacts both the need for certain controls and the available solutions, and (b) the diversity of potential ownership, reimbursement, and usage scenarios, and how to maintain a balance between user and corporate expectations.

Because of these complexities, there is no straightforward, one-size-fits-all recipe for success when it comes to solving the security-for-mobility problem. Nonetheless, organizations should:

- Remain focused on the most important objective – ensuring adequate protection of mobile data – while balancing this with need for a positive user experience and reasonable cost of ownership;
- Pursue a layered approach where MDM-oriented security capabilities are supplemented by the advanced controls described herein for secure access, threat protection, and, above all else, data protection; and,

- Favor solutions that deliver a high degree of administrative efficiency and low overall TCO based on their capacity for consolidation and incorporation of enterprise-class features, such as centralized management, directory integration, and robust reporting.

"Even further gains can be realized if the advanced threat and data protection capabilities needed to support mobile devices are available as integral extensions of the solutions already being used to provide similar capabilities for the organization's fixed users/devices."

Contributing Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and analysis company specializing in information security, compliance management, application delivery, and infrastructure optimization. A former META Group analyst, Mark has analyzed business and technology trends pertaining to a wide range of information security and networking topics for more than 15 years. A veteran of the U.S. Navy, he is passionate about helping enterprises address their IT challenges and has assisted hundreds of organizations worldwide meet both tactical and strategic objectives.

About Websense

Today's productivity tools are increasingly mobile, social, and in the cloud. But so are advanced data-stealing attacks, which antivirus and firewall alone can't prevent. You can stay a step ahead with Websense® TRITON™ security, which combines best-of-breed web security, email security, and DLP modules (available together or separately) into one powerful solution. With shared analytics, flexible deployment options, and a unified management console, it's the effective and economical solution for today's security challenges.

websense®