The Ten “Must Haves” for Secure Mobile Device Management

A Security Framework and Evaluators Checklist

WHITE PAPER

Contents

Implications of the Mobile Explosion on Enterprise Security

While the transition of mobile phones into computers has been a long time coming, the sea change in the past two years is dramatic: Consumer smartphones and tablets have become so compelling that enterprise executives are willing to upend the 'way we do things around here' to have them. But what has become a powerful medium for learning, transacting, sharing, presenting – even transforming business – also brings serious enterprise risk.

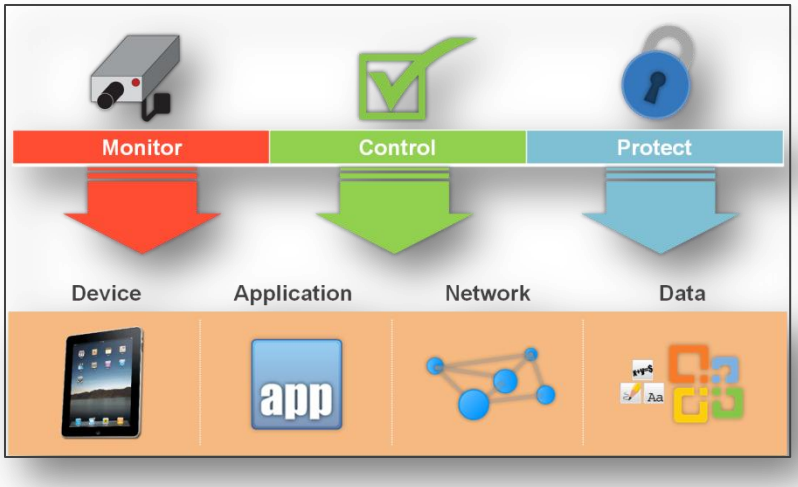
Employee Work Habits in the Age of the Pocket Enterprise

We call enterprise mobility 'the pocket enterprise' because we feel it aptly communicates what's at stake for organizations. Wherever they are, whatever time of day, employees can gain access to your entire enterprise – the corporate network, proprietary business applications, and sensitive data – from a device small enough to fit in their pocket.

As information technology (IT) and security professionals know all too well, the risks associated with the pocket enterprise are legion, with employee habits or behaviors that can lead to data loss, exposure of the corporate network, and compliance breaches. Have employees passcode-enabled their devices? Do they abide by the corporate mobile app policies? Have they tampered with the device's security features? Do they synch non-public data using Dropbox or forward it to their Gmail account? And the most pressing question of all: How can the enterprise even begin to answer these questions?

Urgently Needed: An End-to-End Mobile Security Framework

IT and security professionals are largely turning to mobile device management solutions to help them get mobile devices under control and secured in their workplaces. However, this range of mobile challenges requires a new, more comprehensive security framework; one that goes beyond the basic 'lock and block' capabilities of most mobile device management (MDM) solutions. For far too long MDM solutions have been reactive in nature, focusing almost exclusively on the device and, consequently, leaving wide gaps in mobile enterprise security. Today's enterprises need an MDM solution that arms them with tools to proactively monitor, control, and protect the enterprise end-to-end – across the device, application, network, and data layers.



We introduce the Zenprise Mobile Security Framework. Besides being a framework for what Zenprise has and will continue to deliver, we submit it should be an industry framework for both enterprises and their vendors to deliver secure mobility.

Besides providing end-to-end security, MDM solutions should integrate those layers so that each acts as a series of checks and balances. For instance, MDM solutions' device layer security should prevent users from downloading blacklisted applications. And if the MDM solution is unable to block a user from downloading a blacklisted app, the network layer – using a Mobile Security Gateway – should step-in to block that device from accessing the network.

Mobile security needs to be proactive, not reactive, that is to say, the MDM should stop threats before they happen rather than attempt to contain them once they occur. Proactive security is possible if the MDM solution has processes designed to monitor the mobile enterprise (e.g., Mobile Security Intelligence) as well as execute specific actions in response to both user behavior (e.g., 'context-aware') and the types of data that employees seek to access (e.g., 'content-aware').

How does proactive security work? Let's take the example of a financial services company that, as a safeguard against insider trading, keeps an audit log of all messages sent by its traders during business hours or when they're on premise. Traders, using their Facebook mobile app, can send Facebook messages that are outside of the institution's audit log. In such cases, a context-aware MDM solution will disable the traders' Facebook mobile app during trading hours or while they're on premise. Once business hours end or the trader has left the office, the MDM solution re-enables the app.

Finally, due to Consumerization of IT and 'bring your own device' trends, enterprises need an MDM solution that supports a hybrid security model that accommodates both company-issued and personally-owned devices. In addition to disabling and re-enabling apps such as Facebook, the MDM solution should enable IT to lock and wipe company-issued devices if they're lost or stolen, and selectively wipe personally-owned devices of enterprise data once the employee leaves the company.

What follows is a 10-question checklist as well as an in-depth discussion of the range of mobile threats and concerns, and the requirements for addressing them via a holistic mobile security framework encompassing mobile devices, applications, the network, and data.

The Ten "Must Haves" for Securing the Mobile Enterprise

Below are the ten questions enterprises must ask any mobile device management (MDM) solution vendor they're considering to ensure they get the level of security they need.

Question	Rationale
Does your solution feature **end-to-end security** across mobile devices, apps, the network, and data?	Mobile device management solutions must proactively monitor, control, and protect all layers of the mobile enterprise, providing both multi-layer coverage and checks and balances.
Beyond setting security policies, you're your solution give me the option to set **dynamic, context-aware policies**?	Many employees use personally-owned devices for and at work. IT departments can't reasonably expect them to eliminate popular apps and functions (e.g., Facebook or cameras). The MDM solution should offer Dynamic Defense (context-aware security) to block or lock access to specified resources or apps during work hours or while the employee is on premise. Once the employee leaves the office or business hours have ended, the apps should be re-enabled.
Beyond application security and access policies, does your MDM solution let me grant **granular access to mobile apps** on an app-by-app basis, and can I segregate my critical business apps from non-compliant or potentially malicious apps?	For many enterprises, giving VPN access to mobile users means that access is an all-or-nothing proposition. Once the employee has mobile access, many corporate apps are open to that device. Thus, the MDM solution must provide Mobile App Tunnels, additional app-specific layers of security that specifically address corporate apps. Mobile App Tunnels are VPN-like in that they automatically establish a dedicated, fully-encrypted, fully-auditable network connection between the app client on the device and the enterprise app, but they are app-specific. This puts granular app access into the hands of the enterprise and protects critical business apps from non-compliant or potentially malicious apps that may be on employees' devices.
Can your solution **monitor and profile mobile network traffic and user behavior**, and can we integrate it with our Security Information and Event Management (SIEM) solution?	IT must have clear visibility into the devices and apps that access the corporate network (IT cannot secure that which it doesn't know about). Thus, the MDM solution must provide real-time visibility into mobile network traffic and user behavior, audit employee devices, and block any that are unauthorized from accessing the network. To enhance real-time, proactive security even further, the MDM solution should integrate with SIEM solutions.
If we use your MDM solution, can our IT department **support employee devices remotely**?	The myriad employee devices presents unique security challenges from an IT standpoint, including how to monitor, provision, and secure multiple applications across different platforms. IT has no way of ensuring that employees install the security patches and updates released by major vendors. Therefore, remote management is a critical requirement. IT needs the ability to service devices, push compliance policies, and perform diagnostics remotely.
Is your solution **architected for security**, and will my data reside behind my firewall?	The manner in which the MDM solution is architected will have a critical impact on security. Many MDM solutions are architected so that the database housing the employee contact details resides in the DMZ, and not behind the firewall, potentially exposing user and device details. All components of the MDM solution should be fully secured to the highest degree possible.
Can your solution **scale to support multiple locations and all of my employees**? Tell me about your largest deployment (size, hardware required to support), and how many large production deployments do you have, and how long have you had them?	Mobility is on the rise, and all enterprises should plan for long-term scalability. Your MDM solution provider should be able to support all of your employees – and multiple devices per employee – with little or no increase in management complexity. Further, it should do so in a way that doesn't require multiple consoles, break the bank on hardware purchases, and create a siloed mobile environment.

Is your solution **highly available at all tiers**: web, app, data, and, in the case of cloud, at the data center? Do you back that up with a 100% uptime service level agreement for cloud?	If the very server you rely on to protect your enterprise goes down, all of your company data and apps are exposed to risk. To prevent this risk, the MDM solution should protect against every source of potential failure. The MDM solution should offer high availability with load balancing and redundancy featuring active-active clustering at the web, app, and data tiers, as well as global data center redundancy in the case of cloud deployments. The MDM vendor should be so confident in its HA support and in its alignment with your uptime goals that it offers a 100% uptime SLA.
Does your solution feature **flexible deployment** options?	Due to mobile explosion, enterprises will need a variety of deployment options, including on-premise, public cloud, or hybrid cloud. The MDM solution you choose should have the flexibility to grow with your enterprise.
Does your solution feature **Mobile Data Leakage Prevention**, or prevent leakage of my sensitive business data via mobile devices?	Mobile DLP is a serious issue for virtually every enterprise mobilizing its business. Once an employee downloads sensitive data to his or her device, the organization loses control and cannot get it back. The MDM solution should enable IT to set content- and context-aware security policies for employee access to sensitive business data on their mobile devices, protect the data from being leaked, and claw the data back when employees leave the organization.

End-to-End Mobile Security

Mobile Device Layer Challenges and Security Requirements

Most MDM solutions focus on device layer security, and offer table-stakes, or minimum, features such as setting and re-setting device passcodes, locking and wiping lost or stolen devices, and enabling encryption capabilities. But given Consumerization of IT and 'bring your own device' trends, along with the evolving mobile work habits of employees, those capabilities no longer sufficient to secure the mobile enterprise.

Personally-Owned Vs. Company-Issued Devices

How do you issue devices to some employees and let others bring-their-own? Employees demand freedom of device choice, and for many organizations, it's an attractive, cost-saving strategy. But unlike standard-issue, locked-down PCs or tightly controlled BlackBerrys, mobile devices in today's enterprise are diverse, have varying levels of vulnerability, and offer no consistent way for IT to manage even the most basic security policies.

Nor is IT able to protect enterprise data in the event that an employee's device is lost or stolen, or when an employee leaves the company. Further, as privacy battles and legal actions play out around the world, it is becoming increasingly clear that wiping all of the content from a departing employee's device personally-owned is simply unacceptable for many organizations.

Fragmentation of Mobile Device Platforms

How do you support all the devices employees want to bring to work? According to Aberdeen Research, the average best-in-class company supports 3.3 mobile platforms,1 including iOS, Android, BlackBerry, Symbian, Windows Mobile and others. Fragmentation presents unique security challenges from an IT standpoint, including how to monitor, provision, support and secure multiple applications across the different platforms, or ensure that employees have installed the security patches and updates released by major vendors.

Device Mystery

How do you enforce device policy when you have no visibility into the devices employees use to access the network? Because mobile access is provided to the employee, not the device, IT has limited ability to enforce company device policies. The IT

1 "The Need for Mobility Management", Aberdeen blog, February 2010

department may have an approved list of mobile devices based on their security considerations, but if a username and password are all that are required to access the network, IT has no way of enforcing that policy.

No Dynamic Defense over Device Resources or Apps

How do you ensure that employees don't access forbidden applications during work hours or while on premise? With no visibility into the resources or apps employees have installed on their devices, organizations have no way of ensuring that employees adhere to company and regulatory policy (e.g., no Angry Birds during work hours; no sending Facebook messages from the trading floor).

In a hybrid environment (where some employees carry personally-owned devices and while others use company-issued devices) the enterprise can't reasonably expect them to eliminate popular apps and functions, leaving the organization exposed.

Mobile Device Layer Security Requirements

In addition to all of the reactive capabilities (set/re-set passcode, encryption, device lock, etc.) currently considered table-stakes, the MDM solution should provide a robust set of proactive functionalities that allow IT to monitor, control and protect the enterprise on the device layer. Referring to the Zenprise mobile security framework, the solution should enable IT to:

Monitor	Control	Protect
• Audit devices (IT should be able to generate a list of individual devices that actually access the enterprise) • See device details (type, OS, version, device integrity, etc.) • Ascertain device usage patterns	• Push corporate security and regulatory-compliance policies to every device • Audit devices at pre-configured intervals to ensure that no IT-mandated policies have been disabled. • Quarantine any device that is out of compliance from the network • Set dynamic defense (or context-aware) security policies to prevent employees from accessing device resources and apps during certain times or in certain locations. This includes mobile app locking.	• Locate, lock and wipe devices upon loss or theft; enable a limited set of self-service capabilities (e.g., locate and lock). • Selectively wipe personally-owned devices once employees leave the company • Provide comprehensive support to all device types (iOS, Android, BlackBerry, Symbian, Windows Mobile, and others)

Beyond the baseline capabilities outlined above this table, device layer security gives rise to a new concept in MDM known as Dynamic Defense. Dynamic Defense enables the enterprise to put in place context-aware security that blocks access to resources or applications based on the context (time, location, or combination of the two) of the user for the purposes of ensuring compliance, reducing business risk, maintaining business productivity, keeping mobile employees safe, or keeping mobile employees compliant with company or regulatory policy. With Dynamic Defense, off-limit resources or applications can be blocked or locked based on situational context such as location, time of day, and other factors. This is essential for organizations that allow their employees to use their own devices in the business environment.

Mobile Application Layer Challenges and Security Requirements

Many MDM solutions offer minimal security at the mobile app layer. Protection at this layer is increasing in urgency as mobile apps are growing in number and increasingly becoming an entrance point to the enterprise.

No Control Over Mobile Apps or Device Resources

How do you get a handle on the mobile apps in your environment? The proliferation of mobile apps has complicated mobile security. With an average of 60 mobile apps per device2, organizations have no control over – or even visibility into – the apps that are on their employees' devices. This has tremendous security and compliance implications, and can be a showstopper to

2 Asymco, January 2011 http://www.asymco.com/2011/01/16/more-than-60-apps-have-been-downloaded-for-every-ios-device-sold/

mobility for many types of organizations. For instance, government organizations have a keen interest in protecting sensitive documents, and forbid personally cameras and video-recorders on premise – standard features on today's mobile devices.

Exposure to All Mobile Apps on an Employee Device

How do you grant mobile access without exposing the enterprise to any app installed on the device? Once IT grants an employee mobile access – usually so the employee can access corporate email – the entire enterprise is opened up to any mobile app the employee has installed on the device. This is true even in cases where the MDM solution offers VPN connectivity and protection (since that connectivity is applied to the device, not specific mobile apps).

If the device is personally-owned employees are free to download any application they wish. If they unknowingly download malware, that malware can expose the corporate network, infect other resources, and create a point of entry for data breaches or systems or code modification, as high-profile attacks like Operation Aurora and Shady Rat revealed. This too can be a showstopper to mobility for organizations that must comply with regulatory and industry policies requiring them to properly patch vulnerable software, protect critical systems from improper access, and safeguard networks from malware.

Mobile App Layer Security Requirements

Securing the mobile app is table-stakes, or a basic requirement, for securing the mobile enterprise. The MDM solution should provide IT visibility into the range of mobile apps installed on employee devices, create an easy way for enterprises to provision apps to users in a role-based way, set policies for app usage in the enterprise, and proactively secure the enterprise against mobile threats. Again referring to the Zenprise mobile security framework, the solution should enable IT to:

Monitor	Control	Protect
• See an inventory of apps running in your enterprise • Provide an enterprise app store where IT can make available or push packages of apps to devices, roles, and groups in a secure and organized way	• Blacklist/whitelist apps that negatively affect employee productivity or break with company or regulatory compliance	• Provide Mobile App Tunnels to secure access to – and all communication between – employees and enterprise applications • Prevent users from opening apps that are unapproved or out-of-compliance

Like device layer security, mobile app layer security gives rise to a new concept in MDM solutions that is worth further discussion: Mobile App Tunnels. Mobile App Tunnels provide an additional layer of protection against all-or-nothing mobile access. Mobile App Tunnels protect the enterprise by providing app-specific VPN security, and can be used with or without VPNs. When configured in the MDM solution, the Mobile App Tunnel automatically establishes a dedicated, fully-encrypted, fully-auditable network connection between the mobile device and enterprise application. In other words, it secures the connection between user and app, and segregates the connection from all other apps on the employee's mobile device.

Mobile Network Layer Challenges and Security Requirements

Enterprises need proactive mobile security at the network layer to do the heavy lifting of monitoring the mobile enterprise and enforcing policies. Without network layer security, IT and security professionals will always be one step behind security threats. Reactive approaches to security issues on the network layer are inefficient, time-consuming, and put the enterprise at risk.

Inability to Enforce Mobile Policies

How can you ensure that non-compliant or malicious apps are blocked from the network? The notion of multi-layered defense is about checks and balances. For example, if an employee downloads a blacklisted malicious app to his or her device, the network layer needs to offer a second layer of defense that to blocks the device via a network access policy.

Lack of Visibility into Device Usage and User Behavior

How can you secure devices that you don't know about and prevent unwanted user behavior you can't see? MDM solutions provide no visibility into mobile network traffic and behavior by device, user, system, or application. This lack of visibility prevents the enterprise from knowing if or when employees access sensitive information from their devices, and how employees use that data once it's on their devices.

No Integration with Security Information and Event Management Solutions

How can you extend the security systems you have in place for the enterprise when MDMs solutions don't integrate with SIEM? The Security Information and Event Management (SIEM) segment has played a critical role in identifying and thwarting internal and external threats and helping enterprises stay compliant, but they have no mobile device component.

Architecture Isn't Highly-Available

How do you ensure corporate security if the system meant to protect it goes down? High Availability (HA) is a necessary feature IT professionals expect, though few MDM solutions provide it fully or at all. This lack of meaningful HA means that a technology failure could mean downtime either for mobile users or for mobile security, which leads to unacceptable risk. Downtime can occur if redundancy isn't built into the system and MDM server goes down. In such cases, failover is delayed, preventing employees from accessing mission-critical applications during that time. Risk stems from the fact that the very system designed to protect the enterprise for mobile threats isn't available, and sensitive data and business apps are consequently exposed.

Mobile Network Layer Security Requirements

Network layer security solutions should be built around Mobile Security Intelligence – that is to say, provide for proactive monitoring of the mobile enterprise, and take automated actions to prevent threat. Yet again referring to the Zenprise mobile security framework, the solution should enable IT to:

Monitor	Control	Protect
• Provide Mobile Security Intelligence that enables IT to see device usage and user behavior • Provide alerts and reporting into mobile events such as unauthorized access, leakage of sensitive corporate data, and mobile compliance violations • Enable MDM integration with SIEM for correlated intelligence; alerting; compliance reporting; and forensic analysis	• Control network access based on device configurations or apps installed • Block any device that is unknown or unauthorized	• Proactively take action on user behavior (block users from certain resources such as sharing files) • Ensure high-availability at all tiers without compromising security

As is the case with mobile security at the app layer, mobile security at the network layer helps to proactively secure the enterprise. Proactive security safeguards enterprises from both insider threats such as data leakage and external threats, by proactively thwarting a security breach before it happens. If, for example, users download a non-compliant or malicious app, the MDM solution should shut down the application and prevent the user from ever opening or using it, or block the device from accessing the corporate network, thus isolating the app and protecting the enterprise.

Mobile Data Layer Challenges and Security Requirements

Mobile data leakage has been a concern among IT and security professionals for years. The mobile industry's response has largely been to solve the problem by 'containerizing' the app, which is neither effective nor user-friendly. In general, the mobile industry lacks a solution to secure sensitive data at the data layer.

Mobile Blind Spots

How do you ensure that files in confidential SharePoint folders aren't forwarded to an employee's personal email account? Sensitive data is more than customer payment records and employee data. It's also the Microsoft Word documents and PowerPoint presentations that detail next quarter's customer acquisition strategy, lay out the enterprise's product development roadmaps, and summarize risk assessments for the Board of Directors.

Many enterprises have standardized on Microsoft SharePoint as their repository for document organizing and sharing. From SharePoint, employees can download documents to their devices (usually tablets) and are free to use that file however they see fit.

Application Containers Aren't User Friendly

If the security mechanisms are difficult to use, how can you ensure that employees won't circumvent them? Application containers – the industry's response to data leakage to date – pose daunting challenges to the user. Employees can't access documents in their native format, making reviewing and editing cumbersome or impossible. The lack of version controls also means employees are never sure if they're working with the latest draft. With such obstacles, the temptation is great to simply circulate sensitive documents via email. And once an employee or contractor leaves the company, IT has no way of wiping sensitive data from their home computers.

No Integration with Leading Content Repositories and Collaboration Tools

How do you extend enterprises' data-protection capabilities and version controls to the mobile enterprise? Microsoft SharePoint and other collaboration and sharing tools do a good job in enabling employees to label documents as sensitive, and ensuring that, if necessary, other employees can't access, remove, copy, forward and print them. In other words, they offer security on a fine-grain level. However, those controls are lost once a document is downloaded to an employee's tablet.

Mobile Data Layer Security Requirements

MDM solutions should offer a DLP strategy that addresses sensitive data – in all its formats. Moreover, it should provide secure document synchronization in the document container, provide content- and context-aware mobile DPL, and leverage enterprises' collaboration tools. Referring a final time to the Zenprise mobile security framework, the solution should enable IT to:

Monitor	Control	Protect
• Monitor the mobile employee's access to sensitive data	• Ensure synchronization of sensitive data and SharePoint • Set security policies based context and content classification (remove, email, copy, paste) • Control document versions • Control proliferation of old data through document expiration dates	• Prevent leakage of sensitive data through context and content-aware security policies and secure data containers • Prevent leakage of sensitive data from departing employees or contractors by wiping the container and all the data in it • Protect employees from using the wrong version of important files through version control • Protect employees by giving them instant access to the right document at the right time

The ability to monitor mobile employees' access to sensitive data, ensure synchronization of sensitive data and content repositories and collaboration tools, set security polices bases on context and content classification, and the ability to wipe the data container from a personally-owned device once the employee or contract leaves the company are now table-stakes for the enterprise.

Additional Security Considerations

Inability to Scale

Will scaling to all of the devices you'll need to support incur significant hardware costs and create management complexity? Even though scalability may seem like a distant concern for some enterprises, the explosion of mobile device sales and proliferation of mobile apps will make that concern a reality sooner than later. Enterprises will do well to incorporate long-term scalability requirements into their plans early on. The majority of leading MDM solutions support one to two thousand users per server, which means that scaling can become costly and unwieldy. For global enterprises, or ones with 10,000 employees or more, scale becomes a serious challenge. Some MDM solutions require that organizations run multiple servers or appliances, yet require that administrators sign in to multiple consoles, have separate integrations with corporate resources such as Active Directory, and tie high availability to each server. Scaling in this manner can be a time-consuming, error-prone, manual process that creates risky security silos.

Insecure MDM Architecture

Could you tolerate an MDM architecture that exposed your CEO's personal data? Many MDM solutions are not architected with security in mind by keeping sensitive data behind the firewall and brokering access to it via technology residing in the DMZ. Some MDM solutions are architected so that they must make tradeoffs between data availability and security measures, so they err on the side of data availability at the expense of security, rather than thoughtfully optimizing for both. As a result, MDM architectures can end up with choices such as data repositories residing in the DMZ, thus potentially exposing users' data, or behind-the-firewall data repositories being accessed insecurely from servers in the DMZ.

Conclusion

With the massive growth in smartphones and tablets in the enterprise and the security risks they bring, a comprehensive framework for implementing end-to-end secure mobility is critical. Zenprise satisfies and exceeds the requirements laid out in that framework, offering the industry's leading solution for *secure* mobile device management.

About Zenprise

Headquartered in Silicon Valley, Zenprise is the leader in secure mobile device management. Only Zenprise protects the mobile enterprise end-to-end, keeping organizations secure and compliant. Zenprise MobileManger™ and Zencloud™ let IT say "yes" to mobile device choice while safeguarding sensitive corporate data, shielding the network from mobile threats, and maintaining compliance with regulatory and corporate policies. This gives IT peace of mind, lets executives take their businesses mobile, and makes employees productive while on the go. Zenprise's extensive list of global customers and partners spans a cross-section of countries and vertical industries including: aerospace and defense, financial services, healthcare, oil and gas, legal, telecommunications, retail, entertainment, and federal, state and local governments. For more information about Zenprise, please visit www.zenprise.com or follow us on the Zenprise blog (http://www.zenprise.com/blog), Facebook (http://www.facebook.com/zenprise), and Twitter (@Zenprise_Inc).