MobileIron

WHITE PAPER

Mobile Security:
Threats and Countermeasures

Introduction

Mobile devices are rapidly becoming the primary end-user computing platform in enterprises. The intuitive user-experience, robust computing capabilities, extensive catalog of apps, and always-on connectivity combined with portability make mobile devices very compelling PC replacements. However, the shift to mobile is a major transition from the PC era, requiring enterprise IT to consider a new approach to securing corporate data and minimizing risk. Securing enterprise content on mobile requires IT to adopt new management tools and security strategies given the differences in the way mobile operates compared to PCs. However, those organizations that take a mobile first approach and address new requirements will enjoy the benefits that result, which include marked competitive differentiation and heightened innovation.

This document summarizes the basic, supplemental, and compensating controls that can be implemented with MobileIron to mitigate the risk of data loss on corporate and personal mobile devices.

Top Considerations When Going Mobile First

There are two key reasons why IT needs to adopt new strategies for securing corporate data on mobile, as compared to PCs, when pursuing a strategy to heighten user productivity.

- **Reduced IT control over mobile devices:** The Mobile First era is all about the end user. They get to pick a mobile platform that best meets their personal preferences, with the expectation that the device should also work in a business context for the full range of apps and content needed to stay productive. This is in stark contrast from the PC era where IT offered end-users an approved PC with a set of pre-selected apps. End-users had very limited say on what the PC was able to access and IT had the ability to control every aspect of the corporate-owned device from physical ports, to software and application versions. For mobile, end-users make the decision for many of these variables and IT can only recommend devices and applications. IT has no way to enforce a standard OS, device or app across the organization. In fact, the more IT tries to lock down devices, the more end-users will try to by-pass policies, increasing risk to the organization.

- **Old security models are no longer relevant**: In the PC operating system scenario, the agent-based security method worked well. This involved a piece of software residing on the PC that controlled the process and data belonging to other applications. Unfortunately, this agent-based security model cannot be used to secure Mobile because of the differences in the way these operating systems are designed. Mobile operating systems are designed using a sandboxed architecture which enables for isolation of apps and associated data which can only interact and share data through very well-defined mechanisms. This allows for greater security than the

MAKING ENTERPRISE MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

open-file system used by PC OS, and needs new tools that leverage specific security capabilities made available by the device vendor itself.

With the rapid adoption of mobile into the enterprise comes great opportunity for growth and innovation, but also heightened risks. This document summarizes the key threats introduced by mobile devices and how IT organizations can leverage Enterprise Mobility Management tools to mitigate risk and protect business data without compromising end-user productivity.

Threat Vectors Introduced by Mobile

As trends such as BYOD accelerate the use of Mobile devices to enhance enterprise productivity, organizations are being exposed to a variety of information security risks and threats. Threats introduced by mobile can be grouped in to three categories:

1) **Device based threat vectors**
   Mobile devices enable end-users to perform a variety of business-related tasks such as receiving email and accessing, editing and sharing corporate content via a variety of productivity apps. As a result, mobile devices store a significant amount of sensitive data. This data can be compromised in a variety of ways due to:
   - Always-on connectivity which could allow unauthorized parties to access business data.
   - Software vulnerabilities that allow “jailbreak” or “rooting” of devices, compromising data security.
   - Portable form-factor making the devices susceptible to theft and misplacement.

2) **Network based threat vectors**
   The always-on model requires mobile devices to be constantly connected to the internet. As a result, end-users might often rely on untrusted public networks enabling malicious parties to access and intercept transmitted data using
   - Rogue access points
   - Wi-Fi sniffing tools
   - Sophisticated Man-in-the-Middle (MitM) attacks

3) **User based threat vectors**
   Mobile empowers end-users. While this is great for user-choice, well-meaning end-users often indulge in risky behaviors that could compromise business data. Examples of risky behaviors include:
   - Using un-approved cloud-based apps to share and sync data
   - Using un-approved productivity apps that maintain copies of corporate data
   - Jail breaking/ rooting devices to bypass security controls
   - Using malicious apps from un-approved app-stores
   - Exposing business data with malicious intent

While one may argue that the list of threat vectors introduced by Mobile devices are similar to those introduced by laptops and similar portable PC-based devices, the fundamental differences between Mobile and PC operating systems require IT to adopt purpose-built Enterprise Mobility Platforms to mitigate risks introduced by Mobile.

Countermeasures for data loss prevention on Mobile

Implementing data loss prevention on mobile devices requires a layered security approach. This layered security approach can be implemented using the controls listed below:

1) Secure operating system architecture
2) Authentication
3) Remote wipe
4) Encryption
5) Data sharing
6) Network security
7) Application lifecycle management
8) Secure browsing

Below are descriptions of the data loss prevention requirements and specific controls supported by MobileIron. Each class of controls can include basic controls, which directly address the requirements, supplemental controls, which strengthen the basic controls, and compensating controls, which apply when no basic control is available. These layered security controls, together, establish the data loss prevention model for Mobile.

1. Secure operating system architecture

Requirements:

- Sandbox applications to prevent malware from accessing application data
- Provide a safe application ecosystem
- Protect operating system integrity
- Patch OS vulnerabilities quickly

Basic controls:

- *Sandbox*: A "sandbox" is the isolated set of data associated with an application ("app") on mobile. Unlike PC operating systems, Mobile operating systems do not allow apps to access data outside their specific sandboxes, except through well-defined sharing controls. This mitigates the risk of malware, because even if downloaded to the device, the malware cannot access the file system to damage or steal data.
- *App ecosystem*: Mobile App Stores such as Google Play and the Apple App Store are tightly curated to minimize the likelihood of malware in posted apps. Apple prohibits certain backdoors, like the download of new, executable code into an already approved app. Apps can also be immediately revoked from app stores if they are later found to break to violate policies.
- *OS integrity*: "Jailbreak" or "root" is the term used in the mobile community to represent a compromise of the underlying operating system that removes built-in security mechanisms. MobileIron does jailbreak and root detection on each registered mobile device on an ongoing basis to ensure that the operating system has not been compromised. If it is compromised, MobileIron triggers the appropriate security action based on the policy defined by the organization. This can be performed online and offline in the event that a device is lost or stolen and loses network connectivity.
- *OS patching*: Because Apple controls the global distribution of the iOS operating system, any vulnerability that Apple considers to be substantial has traditionally been patched quickly, and the resulting new version of iOS has been made available to the global user base for download. The delivery of OS patches for Android devices is dependent on device manufacturers and carriers.

Supplemental controls:

- *OS update enforcement*: MobileIron monitors the OS version of all devices under management. Therefore, if users neglect to update their devices after a patch is available, those devices can be quarantined and enterprise data can be removed until the issue is remediated.

Compensating controls:

- *OS version monitoring*: Unlike traditional Windows, IT does not control OS patch distribution for iOS or Android. This means that new patches are available to users when device manufacturers make them available, regardless of whether IT has approved them for distribution. While this reduces IT control, IT can still monitor OS versioning through MobileIron and take action if the user has upgraded too early or not at all.

The sandboxed operating system architecture isolates application data into separate containers to limit the ability of malware to damage or steal data.

MobileIron monitors the integrity and versioning of the operating system to ensure compliance and consistency across the organization.

2. Authentication

Requirements:

- Remotely configure password policy
- Auto-wipe device after a certain number of failed authentication attempts
- Enforce identity for enterprise services

Basic controls:

- *Device password:* MobileIron allows remote configuration and local enforcement of device password policy. IT can configure the following password policy variables through MobileIron:
  - Type
  - Minimum length
  - Maximum inactivity timeout
  - Minimum number of complex characters
  - Maximum password age
  - Maximum number of failed attempts
  - Password history
  - Grace period for device lock
- *App password*: MobileIron AppConnect is a containerization solution for securing internal and public apps. Authentication for access to the collection of secured apps on the device is one of its capabilities.
- *Auto-wipe*: Excessive failure attempts are an indicator of theft and will result in an automatic wipe of the device.
- *Certificate-based identity*: MobileIron uses digital certificates to secure access to enterprise services on the device, like email, Wi-Fi, and VPN. The user experience improves because users do not have to type their password each time. If a device or user falls out of compliance, purging the identity certificate also cuts access to the corresponding service.

New biometric methods supported by iOS can strengthen both authentication and encryption controls.

MobileIron provides the policy engine for device-level and app-level authentication to prevent unauthorized access to corporate data.

Supplemental controls:

- *Biometric authentication*: Apple released its first biometric authentication mechanism, Touch ID, with the iPhone 5S in late 2013. Touch ID allows the user to use a fingerprint for device-level authentication, mitigating the risk of over-the-shoulder password theft:
  - If the thumbprint fails a certain number of times, the user is presented with a password screen set by MobileIron password policy.
  - Prior to the availability of Touch ID, the key tradeoff for authentication was that stronger passwords resulted in user dissatisfaction because they were hard to remember and type. As a result, most financial services organizations allowed a weaker password than they would have liked in order to drive adoption. The weaker password also decreased encryption strength and potentially made it easier to brute-force the device.
  - With Touch ID as the main gate, however, IT can go back to strong passwords if desired, because the only time a user will need to enter the password is when the fingerprint fails multiple times, which is a strong indicator of device theft.

3. Remote wipe

Requirements:

- For company-owned devices, remotely wipe all the data on the device
- For employee-owned devices, remotely wipe ONLY the enterprise data on the device

Basic controls:

- *Full wipe*: MobileIron allows the administrator or user to send a remote wipe command to the device, which wipes the entire device and resets it to factory default settings.
- *Selective wipe*: MobileIron also allows the administrator to remove just the enterprise data on the device, which includes:
    - Removing the enterprise email account on the device without touching the personal email account.
    - Removing apps on the device that were installed through the MobileIron enterprise app store without touching the personal apps.
    - Removing the digital certificates on the device that provide authentication to enterprise services like email, Wi-Fi, and VPN.
    - Removing enterprise content such as documents, presentations, spreadsheets, etc.
    - Stopping the enforcement of enterprise policies.

Logical separation of personal and business data on the device allows IT to take actions to protect enterprise security without compromising individual privacy.

Supplemental controls:

- *Privacy*: Enterprises worry that, on a BYOD device, the user's personal data might be deleted by IT through human error, wiping a lost device, or extenuating circumstances, such as a legal action, where the organization has no choice. In such situations, users can lose important personal data, such as family photos or text messages.
    - MobileIron allows IT to set a privacy policy by device or by group so that only security-impacting information is accessible to IT.
    - Every BYOD program must have a clear and well-communicated policy around data access and data removal that is credibly practiced in daily operations. Otherwise, BYOD adoption will suffer due to mistaken privacy assumptions on the part of the user.
    - Every BYOD program must also have an end-user agreement to provide the organization with legal protection in case personal data is deleted, even if this is not expected to happen in the normal course of operations.
    - Because there will always be edge cases, every BYOD program must also educate users about how to backup personal data to, for example, Apple's iCloud service. Then, even if the device is wiped, personal data is not lost. This is a good practice for the end user, just as enterprise data backups are good practice for IT.

MobileIron manages the lifecycle of enterprise services on the device, including distribution, configuration, data protection, and deletion, with separate policies for corporate and personal devices.

4. Encryption

Requirements:

- Encrypt all enterprise data-at-rest on the device
- Encrypt all enterprise data-in-motion to and from the device
- Encrypt all enterprise data in secure apps

Basic controls:

- *Data-at-rest encryption – embedded:* MobileIron can enforce the presence and strength of the device password to enable device level encryption and ensure that it is available to all apps. The stronger the device password, the stronger the secondary layer of encryption. Apple's biometric authentication method, Touch ID, can allow IT to enforce a strong password through MobileIron without damaging the user's sign-in experience.
- *Data-at-rest encryption – additional*: MobileIron's AppConnect containerization solution for apps provides several additional security controls, including encryption. Even though iOS and Android have embedded encryption, many organizations want this additional level of encryption for unlocked devices.
- *Data-in-motion*: Enterprise mobile data, which includes email, apps, documents, and web pages, flows through MobileIron's intelligent gateway, called MobileIron Sentry. This data is protected against man-in-the-middle (MitM) attacks and interception through the use of digital certificates and transport layer encryption.
- *FIPS 140-2 validation*: MobileIron's use of FIPS 140-2 cryptographic libraries has been validated by an accredited Cryptographic and Security (CST) laboratory in full compliance with the Cryptographic Module Validation Program (CMVP). The validation letters can be found here.

MobileIron encryption for data-at-rest and data-in-motion has FIPS 140-2 validation and complements the embedded operating system encryption capabilities.

5. Data sharing

Requirements:

- For corporate email in the native email app:
  - Do not allow attachments to be opened in an unauthorized app
  - Do not allow forwarding through a personal email account
  - Do not allow copy/paste, printing, or screenshots of email text
  - Do not allow backup of email outside IT control
- For corporate apps:
  - Do not allow app data to be accessed by unauthorized apps
  - Do not allow copy/paste, printing, or screenshots of app data
  - Do not allow backup of app data outside IT control

The major vector of data loss on mobile is the well-intentioned user opening enterprise data in an unsecured app.

Basic controls:

- For corporate email in the native email app:
  - *Attachments*: MobileIron's intelligent gateway, MobileIron Sentry, encrypts all email attachments. Only the MobileIron Docs@Work viewer can decrypt those attachments. The attachments are stored in the Docs@Work secure container on the device. Unauthorized apps cannot access or decrypt these attachments. On Android, all corporate email is stored within a secure workspace and attachments can only be accessed by authorized apps.
  - *Forwarding*: MobileIron allows IT to disable the forwarding of email from one account through another account on the device.
  - *Copy*: MobileIron can disable the device screenshot function. However, the native iOS email client does not support disabling the copy/paste or printing functions for text. The "*Compensating controls*" section below describes a method to address this.
  - *Backup*: The corporate email account managed by MobileIron on the device is never backed up to services such as iCloud.
- For corporate apps:
  - *Sharing*: Mobile operating systems allow apps to share data with each other through the "Open In" function. MobileIron allows IT to control which apps can use this function to access app data.
  - *Copy*: MobileIron AppConnect is a containerization solution that provides an extra layer of security around enterprise apps, including the ability to restrict copy/paste and printing of app data. MobileIron can also disable the screenshot function across the entire device.
  - *Backup*: MobileIron can disable iCloud backup globally for all apps, but users might want to still use iCloud for personal data. MobileIron can also disable iCloud backup on a per-app basis for managed apps, but IT will need to ensure that those apps are not also coded to use iCloud for document or key/value pair persistence.

MobileIron AppConnect enforces several controls over data sharing to ensure that enterprise data can only be accessed by authorized apps.

Compensating controls:

- *Email client*: The native iOS email client cannot restrict copy/paste or printing actions. Many organizations have concluded that these functions pose low risk of data loss because the data sets are small, the user must take an intentional action, and there are several other ways for the malicious insider to copy the data mechanically (pen) or electronically (photo). However, if the risk is still considered too high, IT can deploy MobileIron Divide, a native email client that supports all the controls described.

6. Network security

Requirements:

- Prevent data loss as enterprise data traffic travels through public cellular and Wi-Fi networks outside IT control.

Basic controls:

- *App tunneling*: MobileIron Sentry provides secure app-level tunneling for all enterprise data, including email, app, document, and web traffic. This allows IT to separate the flow of enterprise data (which flows through Sentry on a secure channel) from personal data (which flows outside Sentry through the unsecured network).
- *VPN*: For companies that have standardized on device-wide VPN technology from vendors like Cisco and Juniper, MobileIron configures the VPN service to provide a secure channel for data.
- *NOC-free architecture*: A Network Operations Center (NOC) is a central location for the monitoring and management of a network. In the traditional BlackBerry architecture, the NOC was the external control point for the secure network, controlled by BlackBerry, through which email traffic travelled from the enterprise to the device. The challenge with NOC-based architectures is that they create a potential point of failure and data loss outside IT control. Luckily, neither the app tunneling nor VPN models described above require an external NOC. BlackBerry needed the NOC because the legacy model of push email required the solution to collect email from the enterprise email server, store it in an external location (NOC), and then forward it to the device. However, this model is not necessary because the ActiveSync protocol is used for push email. This eliminates the need for a store/forward, NOC-based architecture and is one of the main reasons ActiveSync has now become the standard protocol used for push email by most embedded and third-party email clients.

The mobile security model must assume that all enterprise data will flow through public networks.

MobileIron Sentry is the intelligent gateway that provides secure tunneling for enterprise data at the app level across any network.

7. Application lifecycle management

Requirements:

- Prevent rogue apps from being downloaded to device
- Blacklist unauthorized apps
- Whitelist authorized apps
- Publish and distribute enterprise apps
- Update enterprise apps

Basic controls:

- *Rogue apps*: Much of the risk of rogue apps is mitigated on mobile because:
  - Mobile architecture isolates apps from each other in independent sandboxes so a rogue app cannot access data from an enterprise app except through data-sharing methods controlled by MobileIron.
  - Public App Stores are curated, so malware is uncommon.
  - Apple does not allow apps to download executable code. This prevents malicious code from being introduced into an existing app.
  - While Android allows users to side-load, or install apps from un-approved app stores, IT administrators can enforce policy to disable side-loading apps.
- *Blacklist / whitelist*: MobileIron also allows blacklisting and whitelisting of apps through policies that trigger appropriate notification or access control actions if a device is non-compliant. MobileIron can disable the App Store completely, but we don't recommend this because apps are so central to the mobile experience. MobileIron also integrates with third-party app reputation services to identify when risky apps are present.
- *Enterprise app store*: MobileIron invented and holds the patent for the enterprise app store, which allows IT to publish and securely distribute in-house and public apps to the user community.
- *App updates*: MobileIron monitors the versions of the enterprise apps installed on the device so that IT can prompt the user to update to the latest version when available. This ensures compliance across the enterprise and allows the quick patching of any security vulnerabilities found in the app.

Apps are central to the mobile experience and one of the biggest enablers of business productivity.

MobileIron invented the enterprise app store to securely distribute and manage enterprise apps.

Supplemental controls:

- *Filtered app inventory*: In BYOD deployments, privacy is critical. Users will not want IT to see the full application inventory on their devices, because it could provide a view into aspects of their personal lives, such as health or religion. MobileIron also gives IT the ability to monitor enterprise and blacklisted apps without exposing personal app inventory.

Compensating controls:

- *Rogue app blocking*: In standard deployments, IT cannot actually stop a user from downloading an app, because the user controls what software is installed on the device. Most users, especially with BYOD, will demand the ability to download personal apps to their devices, and restrictions on their ability to do so will limit their mobile adoption. However, the security architecture of mobile devices, combined with MobileIron's blacklist/whitelist policy, mitigates the risk of a rogue app on the device.

8. Secure browsing

Many enterprise resources exist as web apps behind the firewall but require data-at-rest and data-in-motion security controls similar to those of native apps.

Requirements:

- Allow secure access to enterprise web apps located behind the firewall
- Prevent data loss of downloaded documents and cached web content
- Protect against “drive by” malware browser attacks

Basic controls

- *Access*: MobileIron Web@Work is a secure browser that allows users to gain access to enterprise web resources. Web@Work uses native web views so the rendering experience is the same as native browsers like Safari. Preserving the user experience drives adoption, because the user does not have to learn two different browsing interfaces.
- *Documents and web cache*: MobileIron allows IT to set appropriate data-sharing rules for downloaded content and to secure and remove cached data based on policy triggers. For example, data cannot be siphoned from the cache, and the cache can be purged as the result of a trigger, such as jailbreak.
- *Whitelist to block “drive-by” attacks*: MobileIron Web@Work can be configured to whitelist specific internal sites. This means that if the user accesses a site that attempts to open a hidden frame (i.e., another site), that new site will be blocked unless it is also whitelisted. This control can be used to constrain secure browser access to only approved websites in order to mitigate the risk of drive-by attacks.

MobileIron Web@Work provides secure browsing with a native rendering experience and policy-based containerization to protect local data.

Conclusion

The pressure to support new mobile operating systems will be a constant challenge for IT departments because operating system and device choice are now determined by the consumer, not by the enterprise, and can change frequently. Mobile is one of the purest examples of the consumerization of IT, in which consumer behavior dictates which technologies get adopted for business use.

Mobile operating systems such as Android and iOS, and MobileIron, as an enterprise mobility management (EMM) platform, have matured to provide the layered security controls enterprise requires to mitigate the risk of data loss on both corporate-owned and personally-owned devices.

As a result of these controls, organizations can now support the new generation of mobile operating systems and devices that their user communities demand.

For more information about MobileIron, please visit www.mobileiron.com.