Introduction

Office 365 is Microsoft’s cloud-based productivity suite. It includes online versions of Microsoft’s most popular solutions, like Exchange and SharePoint, storage through OneDrive, and several mobile apps, including Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Skype for Business, and Yammer. Office 365 is central to Microsoft’s strategy as the company evolves into a mobile-first, cloud-first software and solutions provider. Office 365 is also central to the productivity strategy of many MobileIron customers since their employees will increasingly use Office on mobile devices instead of traditional PCs. Therefore the ability to secure and deploy Office 365 on mobile devices using MobileIron is a common requirement.

Most large organizations deploy or intend to deploy a broad range of mobile apps to their employees for productivity, collaboration, CRM, ERP, analytics, and industry-specific business processes. Office 365 might be the productivity solution, but the IT team needs a central platform that can provide a consistent security and policy framework across all the mobile apps the organization will deploy both today and tomorrow.

This whitepaper describes the MobileIron app security model and how it can be used to secure Office 365 for mobile devices. Some approaches in this document might vary depending on operating system and deployment model, so please contact your MobileIron technical representative if you need more information.
MobileIron App Security Model

Only authorized users on authorized devices should be able to access enterprise apps. The data in those apps must be protected when at-rest on the device and when in-motion from the device to the back-end application service. Sometimes that back-end service will reside on-premise (for example, traditional Exchange or SharePoint) and other times it will reside in the cloud (for example, Office 365 or Salesforce).

MobileIron allows IT to:
1. Distribute apps securely
2. Protect app data-at-rest on the device
3. Protect app data-in-motion to back-end services

For Office 365, MobileIron allows IT to:
1. Distribute Office 365 apps securely
   a. Configure the native email and PIM apps on mobile devices so they can connect to Office 365.
   b. Securely distribute Office 365 apps to mobile devices through the MobileIron Apps@Work enterprise app store.
2. Protect Office 365 data-at-rest on the device
   a. Enforce operating system containerization controls such as data separation, Open In restrictions, and selective wipe to protect Office 365 data on the mobile device.
3. Protect Office 365 data-in-motion to the Microsoft Cloud
   a. Securely tunnel data from the device to the cloud through MobileIron Tunnel per app VPN.
   b. Block rogue devices and browsers from accessing Office 365 by using Microsoft Active Directory Federation Services (ADFS) to limit authentication paths.
The following sections describe each of the three elements of the MobileIron app security model in more detail. Each section lays out enterprise security requirements, how MobileIron addresses those requirements for mobile apps in general, and then how MobileIron addresses them specifically for Office 365. Our goal is to provide a consistent security model across all the mobile apps that an enterprise deploys to its employees.

### Distribute Apps Securely

An enterprise app store is the mechanism to distribute mobile apps to employees. MobileIron was the originator of the enterprise app store, launched the first implementation over five years ago, and has been granted three patents covering this invention.

**IT security requirements for distributing apps:**

- Employees should be able to tap the enterprise app store on their mobile devices to see the catalog of apps authorized by the enterprise for their use.

- The catalog of apps should be both user- and device-aware:
  - **User-aware**: The catalog of apps should be different for different employees based on their identity. For example, a Marketing Manager should see different apps in the catalog than a Help Desk Engineer.
  - **Device-aware**: If the device is not compliant, for example jailbroken, the employee should not be able to download catalog apps.

**MobileIron security model for distributing apps:**

- **MobileIron Apps@Work** is our enterprise app store. Apps@Work can be implemented by IT as either a Web Clip on iOS or as a downloaded app on Android, iOS, or Windows Phone.

- IT publishes apps to Apps@Work through the MobileIron admin console.

- IT then assigns each app to groups of users or devices based on policy so that that app will only appear in the app catalog of an authorized employee on an authorized device.

- The employee can then download the app securely through Apps@Work.

- **Email/PIM**: If the MobileIron customer is using the native email and PIM apps on the mobile device, MobileIron remotely configures those native apps to be able to access the back-end email service. If the customer is using a third-party email app on the device, then MobileIron distributes that app through Apps@Work just like other enterprise apps.

**MobileIron security model for distributing Office 365 apps:**

- IT publishes the standalone Office apps through Apps@Work as described above.

- If the customer is using the native email and PIM apps on the mobile device, then MobileIron configures those services directly while distributing the other Office apps through Apps@Work.
Protect app data-at-rest

Many people refer to the requirements below as *app containerization*. This means the ability to separate enterprise app data from other data on the mobile device and to mitigate the risk of unauthorized apps on the device accessing that enterprise data.

**IT security requirements for data-at-rest:**

- **Authentication**: Enforce user authentication for the enterprise app or the collection of enterprise apps on the device so that an unauthorized user cannot access them. Client-side certificates are often used to make the process transparent for the user after initial authentication.

- **Authorization**: Ensure that the app will only function if the mobile device is in compliance.

- **Configuration**: Automatically push configuration variables (e.g., server name, language, or policies) to the app. This is a better alternative than employees manually entering configuration information because it reduces errors and Help Desk calls. Misconfigured apps also often result in security holes.

- **Encryption**: Provide secondary encryption for app data stored on the device. Modern mobile operating systems and devices have encryption built in, but some organizations may require more protection.

- **DLP protections**: Prevent data loss from authorized apps to unauthorized apps. Data loss prevention (DLP) is the top security concern with mobile apps. DLP protections can include restrictions such as *Open In* controls embedded in iOS to prevent unauthorized apps from opening enterprise documents or *Copy/Paste* controls to prevent employees from copying text from an authorized app into an unauthorized app. These controls are intended to prevent inadvertent data loss from the actions of well intentioned users. These controls will not necessarily block the malicious user, who will search out other mechanisms, such as screenshots, to capture data from the device.

- **Selective wipe**: Delete the app binary on the device when the employee is no longer authorized to use the app (e.g., leaves the company) or when the device is no longer authorized to run the app (e.g., is compromised or lost).

**MobileIron app security model for data-at-rest:**

- MobileIron supports all six of the security requirements above through a combination of enforcing central policy for the native app containerization capabilities of the operating system and providing supplemental controls through the MobileIron AppConnect SDK and wrapper.

- Because each operating system is at a different stage in its evolution, each provides a different set of native app containerization controls. These controls are managed through MobileIron:
  - **Android (Android for Work)**: Android for Work is the new security stack for the Android operating system. It was launched by Google in 2015. It includes a container, managed by MobileIron, into which IT deploys enterprise apps. The policies for this app container are managed through MobileIron. Google intends Android for Work to be available across the major Android hardware manufacturers.
  - **Android (Samsung KNOX)**: Samsung has made substantial investments in Android security under the Samsung KNOX program. Samsung KNOX has many components, including an app container that is also managed by MobileIron.
• **iOS (Managed Apps):** Apple has embedded app containerization into the operating system itself. Every app has isolated memory and storage to prevent the leak of data from an authorized app to an unauthorized app. The iOS Managed Apps framework allows IT to use MobileIron to set additional security controls around the enterprise apps on the device. These Managed Apps are distributed through the MobileIron Apps@Work interface.

• **Windows:** Microsoft has also embedded app containerization into the operating system for modern apps. In the future, Windows 10 Enterprise Data Protection (EDP) will allow “open in”-style and copy/paste controls to be applied automatically based on the resource list.

• The security requirements of some customers extend beyond the native app containerization controls described above. *MobileIron AppConnect* provides supplemental controls through an SDK (iOS and Android) and wrapper (Android). Some examples of supplemental AppConnect controls:
  - **Authentication:** Enforce passcode for AppConnect apps.
  - **Authorization:** Prevent AppConnect apps from launching on a compromised device.
  - **Encryption:** Provide secondary encryption for data written to disk.
  - **DLP protections:** Prevent copy/paste.

• We recommend that customers use the framework of authentication / authorization / configuration / encryption / DLP protections / selective wipe to prioritize their security requirements and then decide which implementation method is the best match.
  - Start with native OS containerization because MobileIron can apply these native controls to almost all enterprise apps on the device without any modification to the app itself.
  - Add AppConnect for those apps that need supplemental controls. For in-house apps, IT will need to either integrate the AppConnect SDK into the app code or wrap the app with the AppConnect wrapper. IT can also deploy the broad ecosystem of third-party apps that are already AppConnect-enabled ([https://www.mobileiron.com/en/partners/appconnect-partners/available-now](https://www.mobileiron.com/en/partners/appconnect-partners/available-now)).

**MobileIron app security model for Office 365 data-at-rest:**

• MobileIron uses native OS containerization controls to secure data-at-rest for Office 365.

• Using MobileIron, IT can apply the appropriate security policies to Office data on the device and selectively wipe Office data and apps from the device when required.

• This selective wipe ability allows MobileIron to protect Office data on personally owned (BYOD) devices without compromising the privacy of the employee.

• The supplemental MobileIron AppConnect controls are not available for Office 365.

• Securing Office 365 on Android with Android for Work:
  - MobileIron configures native email and PIM in the Android for Work container to connect to Office 365.
  - MobileIron configures the Android for Work container, which also holds the Office apps, with the appropriate DLP controls, such as screen capture and copy/paste.
  - MobileIron selectively wipes the Android for Work container, removing Office email, PIM, and business apps if the employee leaves the company or if the device is lost, stolen, or falls out of compliance.
  - MobileIron can also disable the Android for Work container as a temporary quarantine action if the device falls out of compliance.
• Securing Office 365 on iOS:
  • MobileIron configures the native email and PIM apps on the iOS device to connect to Office 365.
  • MobileIron configures email/PIM as a Managed Account and all Office apps as Managed Apps.
  • MobileIron enforces the Open In DLP control for business apps and email.
  • MobileIron selectively wipes all Office apps plus Office email and PIM data from the mobile device if the employee leaves the company or if the device is lost, stolen, or falls out of compliance.

• Securing Office 365 on Windows:
  • In the future, with Windows 10, MobileIron should be able to report device posture into Azure Active Directory (AAD) attributes.
  • Customers would then define access rules inside AAD based on whether the device is managed or compliant.
  • This could be extended past Office 365 and other cloud apps to on-premise instances if customers are using ADFS.

Additional Office-specific controls for securing data-at-rest:

• Office 365 does have a few additional, proprietary security controls such as prevention of copy/paste and disablement of Save As to other storage repositories (for example, Dropbox). These controls are not exposed to third-parties today.

• Copy/paste control:
  • Some regulated organizations see copy/paste as a vector of email data loss.
  • The Office-specific copy/paste control does not satisfy this use case because it does not apply to the native email app or any third-party email app on the mobile device. This control only applies to Office apps, so the primary main use case is not satisfied.
  • However, copy/paste controls for both native email and Office apps can be implemented on Android by MobileIron without needing to use an Office-specific policy. With Android for Work, copy/paste restrictions can be applied to the entire Android for Work container. The restrictions then apply to all apps within that container, including native Android email and PIM as well as Office and third-party apps.

• Storage control:
  • Office 365 allows employees to store information in personal accounts, like Personal OneDrive or Dropbox, and provides a control to turn off this Save As feature.
  • An alternative approach is to leverage the routing controls of MobileIron Sentry using MobileIron Tunnel so that traffic from Office apps heading to unauthorized destinations can either be blocked or passed through network DLP services.

• IT does not want an Office-specific security console:
  • These additional Office controls are useful but our customers would prefer that Office apps use standardized configuration approaches, such as iOS Managed App Config or Android for Work AppRestrictions instead of introducing a new set of Office-specific interfaces. Other major cloud services, like Box and Salesforce, take this standardized approach.
Companies deploy many mobile apps to their employees and using standardized configuration approaches for Office apps would reduce the complexity for IT of securing the broader apps portfolio.

It is unclear whether Office 365 will adopt a more standardized approach for these controls in the future. We are willing to support either method through MobileIron, but, like our customers, we would prefer the more standardized approach.

However, because the native OS containerization policies managed through MobileIron are extensive and expand with every new release of each operating system, IT can secure Office data-at-rest even without the proprietary Office controls.

Protect app data-in-motion

Office 365 data resides in the secure Microsoft Cloud. However, networks are a major threat vector for mobile and mobile devices regularly slide in and out of compliance, so the final element of the MobileIron app security model is to protect data-in-motion.

IT security requirements for data-in-motion:

- IT should have full visibility over which devices are connecting to ActiveSync for email access.
- IT should be able to define policies so that unauthorized or non-compliant mobile devices cannot access the back-end email or apps service.
- IT should be able to protect the connection between mobile devices and back-end services from man-in-the-middle attacks.

MobileIron app security model for data-in-motion:

- **Email:** *MobileIron Sentry* is the intelligent gateway through which all ActiveSync traffic passes.
  - Sentry provides IT full visibility into which devices are connecting to ActiveSync.
  - Sentry also allows IT to define rules as to what devices can connect to ActiveSync and the posture they must meet in order to connect, for example:
    - Only devices actively managed by MobileIron can receive enterprise email.
    - Compromised devices cannot receive enterprise email.
  - Sentry secures the email connection through two-phased authentication, using a combination of client-side certificates and user identity to safeguard against devices connecting to email on untrusted networks.

- **Apps:** *MobileIron Tunnel* is the per app VPN solution that uses Sentry as its infrastructure and provides per app VPN for almost any app from the App Store.
  - MobileIron customers use Tunnel because it secures app traffic on iOS without any app modification required.
  - Android for Work will provide similar support, although VPN will be at the level of the container instead of the app.
MobileIron app security model for Office 365 data-in-motion:

- **Email:** If the customer is using Office 365 just for email, then MobileIron Sentry, as described above, provides visibility, secure tunneling, and access control for email traffic.

- **Apps:** If the customer is also using Office 365 apps, then MobileIron Tunnel provides secure tunneling and access control for app traffic as well as email.
  - IT publishes the Office apps through MobileIron Apps@Work so they are secured as iOS Managed Apps, which allows the Office apps to use Tunnel for per app VPN.
  - One exception is voice and video through Skype for Business (aka Lync), because UDP traffic is not currently supported by Apple’s per app VPN implementation on iOS.

- **Authentication flow:** All Office traffic from the device is forwarded through the Sentry gateway.
  - Authentication with ID/password redirects to ADFS. This ensures that, using the IP address claim restriction for ADFS, the authentication request is coming via the Sentry gateway.
  - Login succeeds and employee is redirected to Office 365 with the appropriate Access Token.
  - Office 365 grants access to the device. Unauthorized devices are not able to access the Office 365 cloud as the Sentry would deny authentication access to ADFS.
  - If the employee is trying to use an Office app that was downloaded from the public app store instead of from Apps@Work, it is not able to get the Tunnel configuration to login as long as ADFS is locked down to internal only. So the employee is able to login to a personal Office 365 account but not to the corporate Office 365 account.

- **Office 365 has an additional, proprietary mechanism for conditional access:**
  - Office 365 uses Azure Active Directory (AAD) not only for user credentials but also to store posture and correlation data for the device.
  - Based on the data in AAD, Office 365 decides whether or not to grant a user and device access to the service.
  - This is a new method of access control from Microsoft that accomplishes the same goal as described in the Sentry/Tunnel example above, but with a different architecture. MobileIron does not support this today but we may offer it as an option if it becomes available to third-parties in the future.

**Conclusion**

Office 365 is a powerful productivity solution that we expect to become a core part of the mobile app strategies of many of our customers.

Our goal at MobileIron is to provide the best security solution for Office 365 and for the entire ecosystem of mobile apps our customers deploy to their employees.

This white paper outlined the MobileIron app security model and how to specifically apply it to Office 365. As new capabilities and deployment models emerge, we will update this document to reflect the most up-to-date approach to securing Office 365 with MobileIron.