Securing Office 365 with MobileIron

Introduction

Office 365, Microsoft's cloud-based productivity suite, 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, and Skype for Business. Office 365 is central to Microsoft's strategy as the company evolves into a mobile-first, cloud-first software and solutions provider. Many MobileIron customers are increasingly using Office on mobile devices instead of on traditional PCs. Therefore the ability to secure and deploy Office 365 on mobile devices using MobileIron is a common requirement.

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

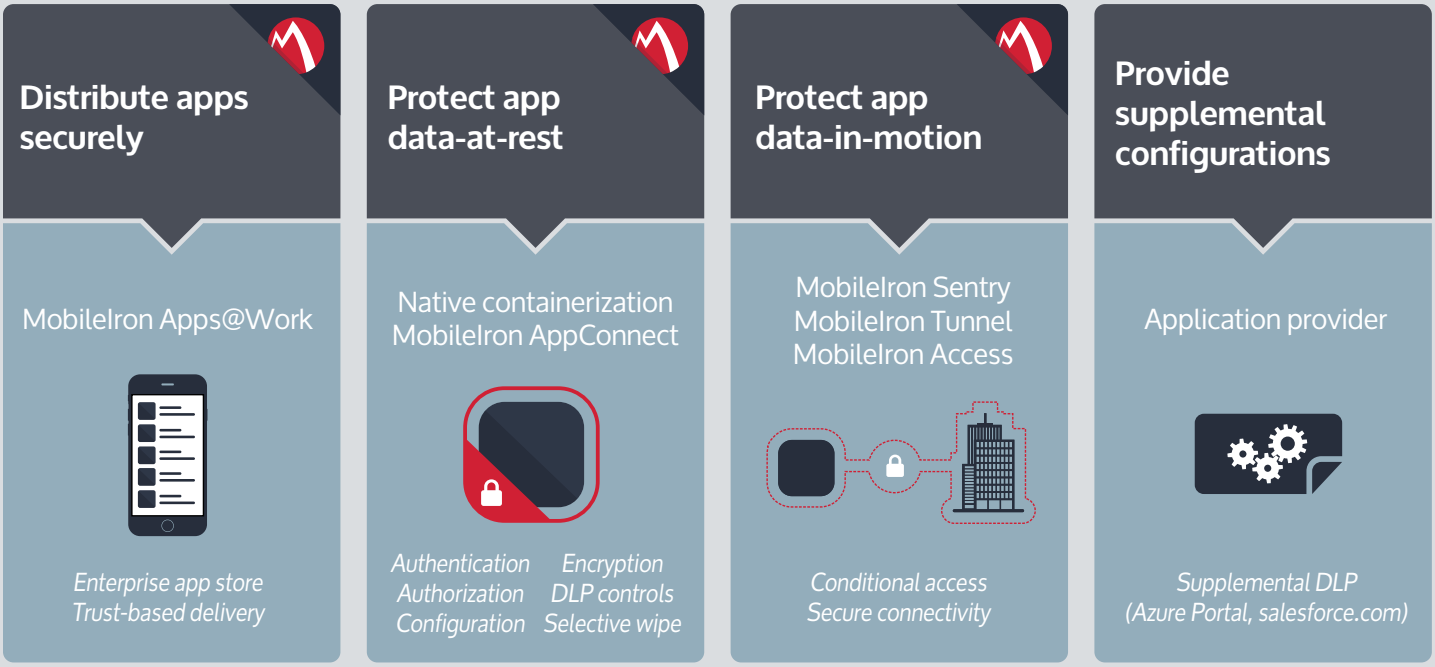
MobileIron

MKT-9926 v2.1

Most organizations have a multi-vendor application strategy that stretches far beyond Microsoft to workflow and line-of-business applications from Oracle, salesforce.com, SAP, and many other best-of-breed application providers. As a result, IT needs a central security model that is consistent across all the mobile apps, both Microsoft and non-Microsoft, that the organization will deploy today and tomorrow. This whitepaper describes the MobileIron app security model and how MobileIron secures Office 365. Some approaches in this document might vary depending on operating system and deployment characteristics, so please contact your MobileIron technical representative if you need more information. This document represents our best understanding, at the time of writing, of how the various technologies integrate, but it is subject to change.

MobileIron app security model

Consistent approach across multi-app, multi-OS deployments



Only trusted users on trusted devices using trusted apps should be able to access enterprise data. The data should 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-premises (for example, traditional Exchange or SharePoint) and other times it will reside in the cloud (for example, Office 365 or salesforce.com).

MobileIron app security model 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
4. Set supplemental configurations through the application provider

For Office 365, MobileIron app security model 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 Ensure that only trusted apps and devices can access Office 365 data by using *MobileIron Access* to enforce conditional access.
    c. Block traffic to specific destinations (e.g., Dropbox) using *MobileIron Sentry* for advanced traffic control.
4. Set supplemental Office 365 configurations through the Azure Portal
    a Configure Office-specific data transfer controls such as "Save As" and "Copy/Paste."

The first three elements of the app security model above each have a section in this white paper that describes:

- Enterprise security requirements
- How MobileIron addresses those requirements for mobile apps in general
- How MobileIron addresses those requirements for Office 365 apps in specific

MobileIron's goal is to provide a **consistent security model** across all the mobile apps that an enterprise deploys to its employees. Some apps will be from Microsoft, but most will be from other vendors or will be developed internally.

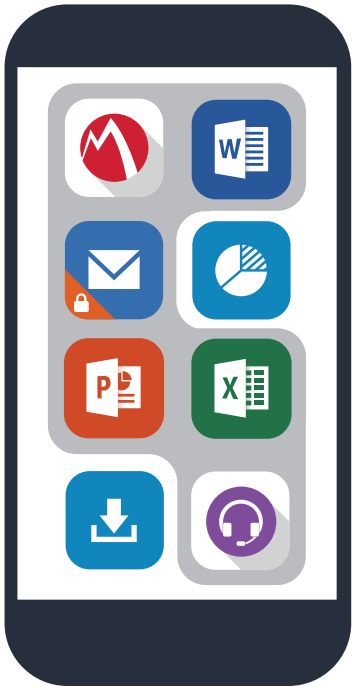
Distribute apps securely

An **enterprise app store** is the mechanism to securely distribute mobile apps to employees. MobileIron is an innovator in this area and has been granted several patents for the management of mobile applications.

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. This 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, if it is 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 and provides IT a streamlined way to distribute apps:

- IT publishes apps to *Apps@Work* through the MobileIron administration 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 a trusted employee on a trusted device.
- The employee can then download the app securely through *Apps@Work*.

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

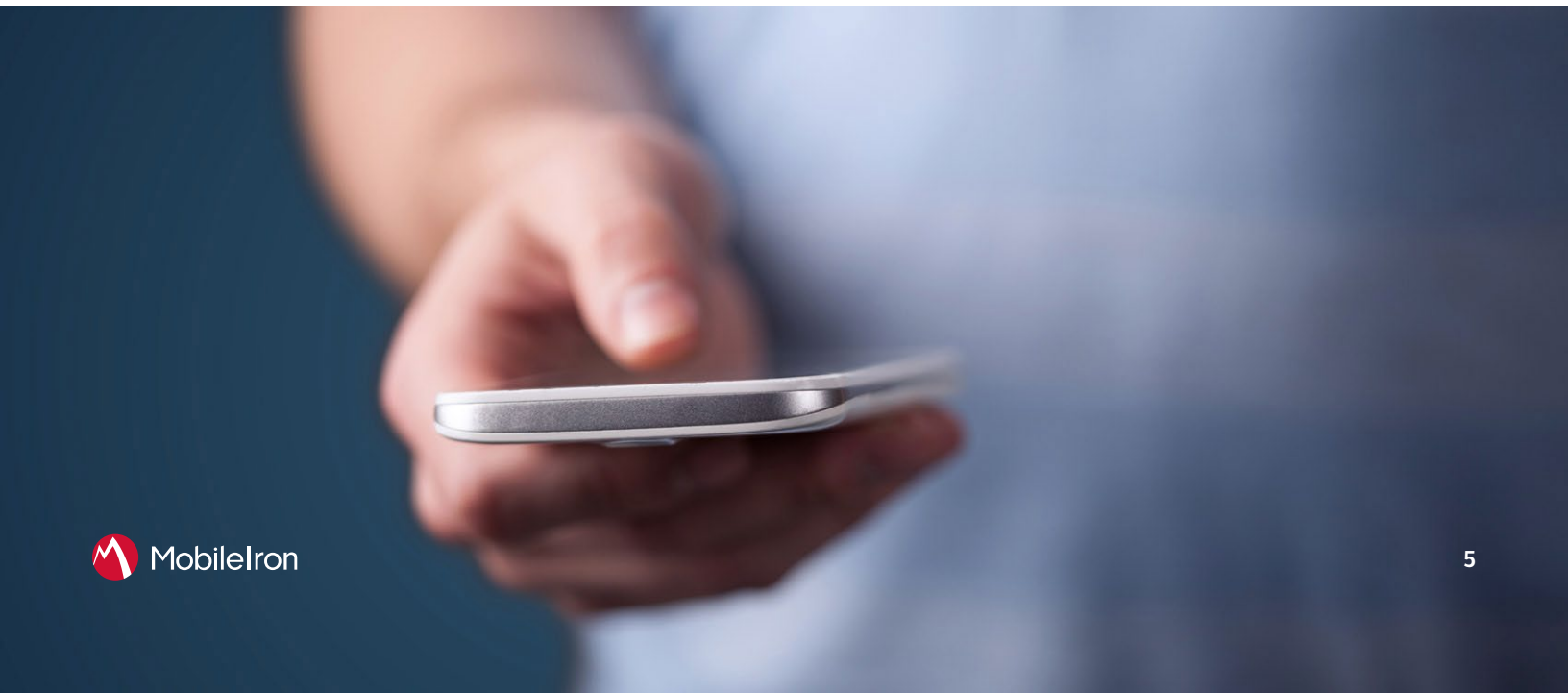
IT publishes the standalone Office apps through *Apps@Work* as described above. If the customer is using the native email and PIM apps on the mobile device, then MobileIron configures those services directly while distributing the other Office apps through *Apps@Work*.

Protect app data-at-rest

Many people refer to these requirements as app containerization. This means the ability to separate enterprise app data from personal data on the mobile device and to mitigate the risk of untrusted apps accessing that enterprise data.

IT security requirements for data-at-rest

1. **Authentication:** Enforce user authentication for the enterprise app or the collection of enterprise apps on the device so that an untrusted user cannot access them. Client-side certificates are often used to make the process transparent for the user after initial authentication.
2. **Authorization**: Ensure that the app will only function if the mobile device is in compliance.
3. **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 create security vulnerabilities.
4. **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 an additional layer.
5. **DLP controls:** Prevent data transfer from trusted apps to untrusted apps. Data loss prevention (DLP) is the top security concern with mobile apps. DLP controls can include restrictions such as the "Open In" controls embedded in iOS to prevent untrusted apps from opening enterprise documents or the "Copy/Paste" controls embedded in Android for Work to prevent employees from copying text from a trusted app into an untrusted app. These controls are intended to prevent inadvertent data loss from the actions of well-intentioned users. However, these controls are unlikely to block the malicious user, who will search out other mechanisms, such as screenshots, to capture data from the device.
6. **Selective wipe:** Delete the app binary on the device when the employee is no longer authorized to use the app (for example, when the employee leaves the company) or when the device is no longer authorized to run the app (for example, when the device is compromised or lost).



MobileIron app security model for data-at-rest

MobileIron supports the six-step security framework described above by enforcing policy for the native app containerization capabilities of the operating system and by providing supplemental controls through the ***MobileIron AppConnect*** SDK and wrapper.

Each operating system is at a different stage in its evolution, therefore each provides a different set of native app containerization controls. These controls are managed through 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 a trusted app to an untrusted app. The iOS Managed Apps framework allows IT to use MobileIron to set security controls for the enterprise apps on the device. These Managed Apps are distributed through the *MobileIron Apps@Work* enterprise app store. Apps such as Microsoft Outlook and Salesforce1 can use MobileIron and iOS Single Sign-On (SSO) to securely authenticate to the appropriate cloud service using Kerberos. This simplifies the user experience because the employee only has to login once to authenticate to multiple cloud services.
- **Android (Android for Work):** Launched by Google in 2015, Android for Work is the enterprise security stack for the Android operating system. Android for Work allows IT to use MobileIron to deploy a profile to devices running Android 5.0 and above. This profile separates personal and work data so that IT can deploy and manage enterprise apps securely using MobileIron.
- **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, which are managed by MobileIron.
- **Windows 10:** Microsoft has embedded app containerization into the operating system for modern apps. These apps are distributed through *MobileIron Apps@Work* and the security policies surrounding enterprise data are set through MobileIron as well. Later in 2016, Windows Enterprise Data Protection (EDP) will expand the native data loss prevention (DLP) controls of the operating system.

The native app security and configuration frameworks built into modern operating systems are very powerful. MobileIron is a founding member of the **AppConfig Community**, an EMM-neutral and app-neutral organization that provides developer education, best practices, and tools for using iOS and Android for Work frameworks effectively. For more information, please go to www.appconfig.org.

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 wrapper (iOS and 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 controls:** Prevent copy/paste.

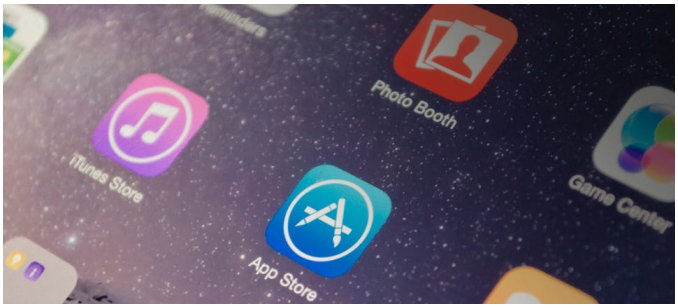
We recommend that customers use the six-step security model described above to prioritize their security requirements and implementation options:

- Start with native OS containerization because MobileIron can apply these native controls to almost any enterprise app on the device without requiring 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://marketplace.mobileiron.com/).

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

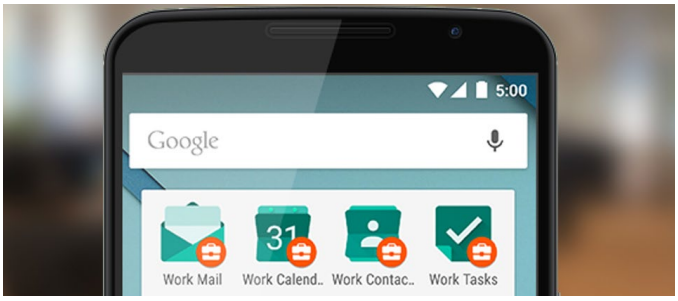
MobileIron uses native OS containerization controls to secure data-at-rest for Office 365:

- IT sets these controls in the MobileIron administration console, and they are then automatically applied to Office apps based on device and user groups.
- MobileIron selectively wipes Office data and apps from the device when the device or user are out of compliance. This capability allows MobileIron to protect Office data on personally owned (BYOD) devices without compromising the privacy of the employee.



Securing Office 365 on iOS:

- MobileIron configures native email/PIM on the iOS device to connect to Office 365.
- MobileIron designates native email/PIM as a Managed Account and all Office apps as Managed Apps.
- MobileIron enforces the "Open In" DLP control for email/PIM and Office apps, including the Outlook app, to prevent Office documents from being opened in untrusted apps.
- MobileIron selectively wipes all email/PIM work data and Office apps from the mobile device if the employee leaves the company or if the device is lost, stolen, or falls out of compliance. This wipes work data without wiping personal data.



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 apps, if the employee leaves the company or if the device is lost, stolen, or falls out of compliance. This wipes work data without wiping personal data on the device.
- MobileIron disables the Android for Work container as a temporary quarantine action if the device falls out of compliance.

Securing Office 365 on Windows 10:

- MobileIron configures the native email profile to connect to Office 365 on mobile devices and desktops.
- MobileIron silently installs Win32 and Universal Windows Platform (UWP) apps on the device. Since the user is already enrolled in Azure Active Directory (AAD), the device can authenticate securely to Office apps without the need for a second authentication.
- Enterprise Data Protection (EDP) is an upcoming Windows 10 capability from Microsoft that will provide a broad range of native DLP controls.

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

However, several supplemental controls, as described below, are available for Office 365 apps through the Microsoft Azure Portal, which co-exists with MobileIron.

Supplemental Office-specific controls for securing data-at-rest

Most enterprise application vendors, like Box, Oracle, Salesforce, and SAP, plan to use the native frameworks of iOS (Managed App Config) and Android for Work (App Restrictions) for configuration of their mobile apps. Using native frameworks allows a company's IT department to configure apps in a consistent way across application vendors and across EMM solutions like MobileIron. See www.appconfig.org for best practices on how the app development community is using native frameworks.

However, Microsoft is not using native frameworks and has instead built a set of proprietary configuration controls that are specific to Office apps. We believe this is because Microsoft wants to minimize its technical dependency on Apple and Google, who are Microsoft's competitors in the operating system, device, productivity, and identity markets. These proprietary Microsoft-specific controls co-exist with MobileIron:

- The customer uses MobileIron as the EMM platform for securing and managing its full portfolio of devices and apps, including Office 365 apps.
- The customer uses the Microsoft Azure Portal to set supplemental configurations specific to the Office apps. These include enforcement of data transfer restrictions like "Save As" and "Copy/Paste." This functionality requires an additional license for either Microsoft Intune or Microsoft's Enterprise Mobility Suite (EMS).
- These supplemental configurations will not be relevant to all organizations but may help those with specific security requirements.

Protect app data-in-motion

Office 365 data resides in the secure Microsoft Cloud, but the path from device to cloud is usually over untrusted networks. The third 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 and control over which devices are connecting to ActiveSync for email access.
- IT should be able to prevent man-in-the-middle attacks on the connection between mobile devices and back-end services.
- IT should be able to define conditional access policies that prevent untrusted mobile devices and apps from accessing back-end email or application services.

MobileIron app security model for data-in-motion

MobileIron Sentry is the intelligent gateway through which all ActiveSync traffic passes.

- *Sentry* gives IT full visibility into which devices are connecting to ActiveSync.
- *Sentry* lets IT define rules to enforce which devices can connect to ActiveSync and the posture they must meet in order to connect. Two sample rules:
  - Only devices actively managed by MobileIron should receive enterprise email.
  - Compromised devices, even if managed, should never 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.

MobileIron Tunnel is a device-side app that provides per app VPN secure tunneling for almost any business app on iOS, Android for Work, and Windows 10. No app modification is required.

MobileIron Access provides conditional access that prevents untrusted devices and untrusted apps from accessing enterprise cloud services. No app modification is required.

All three solutions leverage the *Sentry* gateway infrastructure.

MobileIron app security model for Office 365 data-in-motion

Email: If the customer is using Office 365 just for email, 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 per app VPN secure tunneling for app traffic as well as email.

- IT publishes the Office apps through *MobileIron Apps@Work* so that they are secured as iOS Managed Apps or as part of the Android for Work container. This allows the Office apps to use *MobileIron Tunnel* for per app VPN.
- One exception is voice and video through Skype for Business because UDP traffic is not yet supported by *Tunnel* on iOS.

Conditional Access: All Office traffic from the device is forwarded to *MobileIron Access*.

- *Access* is set up to intercept traffic to ADFS or other identity providers.
- When the employee attempts to log in, the authentication request is redirected to the *Access* gateway.
- *Access* ensures that the device is compliant and that the app is managed before passing on the authentication to ADFS.
- At ADFS, the employee provides his or her credentials and, if authentication succeeds, the employee is redirected to Office 365 with the appropriate access token.
- Office 365 then grants access to the device. Untrusted devices and untrusted apps are not able to access the Office 365 cloud as *Access* would block the authentication path 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*, the authentication request is not able to get to ADFS since *Access* will block it. As a result, the employee would be able to log in to a personal Office 365 account but not to a corporate Office 365 account.

Supplemental Office-specific configurations for securing data-in-motion

Office 365 has an additional, proprietary mechanism for conditional access:

- Starting with Windows 10, Office 365 uses Azure Active Directory (AAD) not only for user credentials but also to store posture and correlation data for the device.
- This posture data can come from the MobileIron server.
- The IT administrator could configure policies to grant or deny the device access to the service or to the app based on this posture data.
- This is a new method of conditional access that accomplishes a similar goal to that described in the *Access* example above, but with a different architecture that is specific to Microsoft services. We expect Microsoft to make this conditional access capability publically available later this year on Windows 10.
- We do not know if Microsoft will also make this capability available for integration on iOS and Android. So far, Microsoft has taken a closed approach and not opened the APIs for conditional access on iOS and Android to other software vendors.

Conclusion

Office 365 is a compelling suite that we expect to become a core part of our customers' productivity strategies.

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. Some of these apps will be from Microsoft, but most will be from other vendors or will be developed internally.

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 current methods for securing Office 365 with MobileIron.