White Paper

Docs@Work: Data Loss Prevention and Secure Access for Mobile Content

Secure Content

Email and SharePoint are the two largest repositories of corporate documents in many organizations. Mobile users require access to these documents, but mobile presents several security challenges that increase the risk of data loss:

- Mixed personal and professional use
- Extensive local storage
- Cloud connectivity
- Hyper connectivity

Mobile IT organizations must secure both email attachments and SharePoint documents in this environment while preserving the native user experience of the mobile device and operating system.

Introduction

Enterprises are increasingly turning toward mobile devices, specifically smartphones and tablets, as their primary computing endpoints. Mobile users now expect access to a wide array of content from behind the firewall, from email to corporate repositories like Microsoft SharePoint. This move to mobile, however, brings new challenges that increase the risk of data loss:

- Mobile devices are designed for the consumer. From the technical side, they are impossible to lock down as tightly as laptops. Lockdown also damages the user experience. For user satisfaction, most companies allow a mix of personal and corporate apps on mobile devices and impose far fewer usage restrictions.
- Mobile devices have lots of storage. A large amount of corporate data can be potentially stored locally on the device.
- Mobile devices are cloud-connected. Data services, such as Dropbox, have made it very easy to move data from the device to clouds outside enterprise control.
- Mobile devices are hyper-connected. Mobile connections are persistent. Devices try to connect constantly to any available network – corporate Wi-Fi, public Wi-Fi, or cellular – whether or not it is trusted by the enterprise.

MobileIron was purpose-built to address these issues. The MobileIron platform provides security and management for mobile apps, content, and devices in the enterprise. MobileIron is available as either an on-premise or cloud solution. This paper focuses on content security and provides an overview of the MobileIron Docs@Work product on iOS. Docs@Work gives end users an intuitive way to access, store, and view documents from email and SharePoint. It lets Mobile IT administrators establish data loss prevention controls to protect these documents from unauthorized distribution.

The Legacy: Heavy Containerization of Email

Email is the primary source of enterprise documents flowing to the mobile device. Enterprises often ask “How can I containerize email?” Their goal is to separate professional from personal email so that the former can be secured and the latter can remain untouched, particularly in BYOD environments. iOS already provides data loss prevention controls for the email text itself, but not for attachments.

Mobile IT’s challenge is to give the user full corporate email access on their mobile device while ensuring that users cannot save corporate email attachments to apps or cloud-based storage services outside IT control. The power, as well as the challenge, of mobility for the enterprise is that this one-click sharing of information

Contact

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

from the device to external cloud services is simple and frequent. An enterprise email attachment can quickly end up in Dropbox without any malicious intent or even effort on behalf of the user.

As a result, some regulated companies in industries such as financial services have felt that they have no choice but to deploy an entirely separate email experience on the device, with a local email container to protect attachments. Unfortunately, this approach has forced users into an email experience they do not like.

Users have voted with their App Store ratings. In almost every organization, users prefer the native iOS email experience to the third-party email container. Users want the integrated experience, real-time push email, high performance, and great usability that only native iOS email can give them. However, their organizations have historically only offered them a third-party, heavily-containerized email app.

The Future: Targeted Containerization

MobileIron Docs@Work allows Mobile IT to protect email attachments in the native iOS email experience with containerization targeted specifically to the storage of documents. Users get to use the email experience they love, and IT does not have to manage separate infrastructure for the sake of security. Docs@Work applies the same controls to documents from SharePoint. Other content repositories are planned for future releases.

The Docs@Work secure content hub is a document container on the mobile device with strong controls that enable Mobile IT to provide access and protect data-at-rest:

- View documents
- Store documents securely on the device
- Protect data with application-level encryption, e.g., iOS Data Protection on iPhones and iPads
- Selectively wipe documents on the device if the device is compromised or “jailbroken,” even if the device is offline
- Selectively wipe documents on the device if the MobileIron server places the device in a quarantine state for non-compliance
- Block clipboard functions to cut/copy/paste information from secure documents to other apps
- Control whether third-party programs can access secure documents
- Prevent email distribution of secure documents
- Utilize policies, users, roles, groups, and permissions already set in MobileIron

Administrators can rest easy knowing that their enterprise documents reside in a secure container and not in an application or cloud service outside of their control.

Security for Email Attachments

Email attachments are the primary source of mobile documents. Security for email attachments starts with the intelligent transfer of those attachments from the ActiveSync server to the mobile device.

Docs@Work utilizes MobileIron Sentry to continually scan email messages for attachments. Sentry is MobileIron’s intelligent gateway and acts as an inline proxy for ActiveSync email access control. When an attachment is found, Sentry will protect the attachment so only Docs@Work can open it. In addition, Sentry can use AES encryption to add another protection layer or remove all attachments before they get to the device.

Sentry is intelligent, so when users forward attachments from their corporate email account on the mobile device, document protections are removed as the attachment passes through Sentry on its way back to the corporate email server. The corporate server then forwards the properly formatted attachment to the appropriate user, passing through whatever data loss prevention (DLP) policies and controls the organizations may be utilizing. Sentry protects mobile attachments, but does not interfere with email DLP controls already in place in the enterprise.

When Docs@Work opens an email attachment on the mobile device, it can now also store that document in the secure content hub with all the protections described in the section above.

Mobile IT can now provide strong protection of corporate data in email attachments without compromising the native iOS email experience. Most importantly, users are satisfied because they can now use the native iOS email experience, which they prefer strongly over third-party email apps, for their corporate communications.

Access to Enterprise Content

While mobile enterprise communication primarily happens over email today, much enterprise content resides in repositories like SharePoint. To this end, Docs@Work allows users to access content repositories using the WebDAV protocol.

Administrators can configure Docs@Work centrally. Usernames and server information can be automatically pre-populated based on Active Directory or LDAP groups. Because Docs@Work is part of the MobileIron client already on the device, there is no additional software for the user to install. As a result, Docs@Work can quickly be deployed at scale without any action required by the user.

With Docs@Work, users can navigate remote file shares to view content. Users can also store content locally on their device for offline viewing. Docs@Work will keep this offline content up-to-date if the device has connectivity when the file is opened for viewing.

All the content protection mechanisms available for email attachments, including quarantining of enterprise data and blocking access to remote information, are also available when accessing remote file shares for SharePoint.

Security for Data-in-Motion through MobileIron Sentry

Mobile devices are hyper-connected and will use a variety of networks to get access to corporate data. Unfortunately, not all of these networks can be trusted. As a result, session security is critical.

To mitigate the risk of untrusted networks, MobileIron Sentry employs a two-phased authentication model for accessing corporate email. With this model, device identity is established using a certificate. This certificate can be issued from either a corporate Certificate Authority (CA) or from the MobileIron server itself, which includes an integrated CA. The latter approach requires no additional infrastructure. Once the certificate has been installed on the device, it must be presented to the Sentry server. Without the proper certificate, all attempts to access mail will be denied.

The second phase of authentication requires the user's username and password. Once device identity has been established, user identity is passed back to the corporate ActiveSync email server. This allows email administrators to validate user identity without having to implement changes to the email infrastructure, like configuring Kerberos. Sentry does also support pure certificate-based authentication with Kerberos.

With certificate-based identity, enterprises can be confident that communications are trusted from the device all the way back to the Sentry server. If a mobile device does join an untrusted network that tries to listen in on end-user communications, the certificate presented to the Sentry will be inherently invalid, and no communication will flow through that network. Because MobileIron can issue certificates as a CA, and Sentry can process them, organizations get the benefits of end-to-end session security with zero additional infrastructure, even if they do not have access to a CA themselves.

Conclusion

MobileIron Docs@Work addresses the entire lifecycle of mobile content security:

- Protects data-at-rest with a secure content hub, or container, on the device
- Prevents data loss by ensuring that email attachments and other documents in the secure content hub cannot be opened by untrusted apps
- Preserves the native email experience by securing attachments without the need for a third-party email app
- Provides secure access to SharePoint
- (With MobileIron Sentry) Secures email sessions end-to-end using certificate-based identity to prevent enterprise data from flowing through untrusted networks

Docs@Work solves the core content challenge for Mobile IT: Provide a great mobile user experience without sacrificing document security. **MobileIron is the only Mobile IT platform to provide secure access and data loss prevention controls across content from both enterprise email and SharePoint.**

For more information about Mobile IT solutions from MobileIron for the security and management of mobile apps, docs, and devices, visit http://www.mobileiron.com/.