MobileIron and iOS:

The Security Backbone for the Modern Enterprise

MobileIron

415 East Middlefield Road
Mountain View, CA 94043

info@mobileiron.com
www.mobileiron.com

Tel: +1.877.819.3451
Fax :+1.650.919.8006

Table of Contents

Executive Summary

The modern, mobile enterprise is expanding faster than ever, across every part of the world and in every industry. Increasingly, organizations are looking for comprehensive security blueprints to help them secure their mobile devices, apps, and data without compromising productivity or the user experience. For that reason, iOS has become the mobile OS of choice in a majority of enterprises because of its highly intuitive, user-friendly, and easy to manage design.

In recent releases, Apple has delivered multiple security and app management features to help IT teams ensure the integrity of mobile apps and data on any iOS device. While the features address many critical security concerns, no OS is completely immune to the risk of data loss and modern malware attacks. With MobileIron's enterprise mobility management (EMM) platform, IT organizations gain a comprehensive mobile solution that complements and augments the security features inherent in iOS.

Simply stated, iOS provides security from the inside out; that is, iOS security begins during chip fabrication and extends throughout the device and software lifecycle. MobileIron EMM delivers mobile protection from the outside in by enabling organizations to deploy a comprehensive mobile security strategy that protects devices, apps, and data whenever users access environments such as cloud resources or unsecured networks. MobileIron EMM provides a standardized platform to automatically distribute configurations and security settings to multiple devices across the enterprise.

This paper provides an in-depth overview of the security features of both iOS and MobileIron EMM. It also explains how, working together, they enable organizations to deploy a highly secure fleet of iOS devices that are easy to configure, secure, and maintain with the most current security policies and app updates.

Introduction: Securing the User-first, Modern Digital Enterprise

Thousands of companies around the world have started the journey toward building a real-time enterprise that puts the digital user experience at the core of their competitive strategies. Every key business process in every global industry including healthcare, manufacturing, retail, technology, transportation, and financial services now depends on enabling secure and seamless digital transactions. As a result, staying competitive requires more than just enabling email on mobile devices. It requires a blueprint for executing a mobile strategy that meets complex security requirements without hindering the digital user experience.

Building a user-first digital workspace is complicated by the growing number of security challenges every enterprise faces today. According to the Ponemon Institute, the biggest factor contributing to the complexity of IT security is the rapidly expanding use of cloud-based apps and mobile devices.[1] Although some amount of complexity is to be expected in any enterprise, too much complexity can diminish an organization's ability to respond to cyber threats. It can also create an environment that's fractured by disparate security technologies across different platforms, inconsistently applied security policies, and an overwhelmed security team that lacks the resources needed to securely manage a rapidly expanding mobile fleet. The explosion of unstructured data and ongoing changes that result from mergers and acquisitions, divestitures, reorganizations, and downsizing also increase complexity.[2] The challenge for IT is to keep all of this massive complexity hidden from end users so all they see and experience are secure, intuitive, and easy-to-access mobile apps and data.

Part of the reason iOS has become the dominant global platform for mobility is due to the user-friendly and highly productive experience it delivers. However, while iOS maintains a well-deserved reputation for security, no mobile OS is immune from threats. Going forward, enterprise IT will need a comprehensive iOS security strategy that includes an EMM platform that can anticipate and prevent mobile attacks. More importantly, organizations will need to unify fractured, highly complex IT infrastructures so they can adequately secure a global fleet of iOS business apps and devices — including desktops, wearables, and other devices that have not yet come on the market.

1 Ponemon Institute LLC, "The Cost and Consequences of Security Complexity," November 2016.

2 Ponemon Institute LLC

Anatomy of Modern Vulnerabilities and Attacks

Superficially, the threats affecting modern mobile devices appear very similar to those affecting legacy endpoints, but there are important differences in how vulnerabilities are exploited and attacks are executed.

Device and OS

Operating system vulnerabilities are nothing new, but mobile operating systems offer a better security foundation through their stricter enforcement of boundaries between kernel and user space as well as techniques like application sandboxing. However, these mechanisms are not infallible and the process of compromising the OS (commonly called "jailbreaking" or "rooting") removes the protection provided by the OS. These compromises, once primarily the domain of power users looking to modify the behavior of their devices, are now becoming components of various malware attacks.

Apps and Data

Traditional malware has limited efficacy on mobile devices due to their architecture as well as the steps that commercial app stores take to prevent its introduction and spread. Because personal and business apps can co-exist on end-user devices, unauthorized "user agents" may gain access to corporate data. Furthermore, apps may not adequately protect the data in transit or at rest. They may also leak sensitive information or attempt to harvest user credentials.

Networks

Mobile devices attach to many more networks than traditional endpoints and comparatively few of those are corporate managed. Because the security of these networks can vary greatly or is non-existent (in some cases), they present an opportunity for attackers to intercept data or perform other malicious acts. Organizations must ensure that their data is protected in transit between corporate repositories and the endpoints accessing them.

User Behavior

Because of their ubiquitous connectivity and the multitude of productivity tools available, mobile devices create scenarios in which end users can willfully or inadvertently exfiltrate enterprise data. Such actions may take the form of "hairpinning e-mail" (i.e., receiving a message from a business account and forwarding via a personal account) or transferring data to personal cloud storage services. In order to mitigate these risks, organizations must have a strategy for ensuring that users have access to the data they need but can control its flow to prevent unauthorized disclosure.

Rising Costs of Breaches

A mobile device that is compromised or out of compliance increases an enterprise's exposure and costs, because data breaches are becoming more expensive. In 2016, the Ponemon Institute conducted a survey of 383 companies in 12 countries. The results showed that the average total cost of a data breach is $4 million — an increase of 29% since 2013.[3]

3 https://www.mobileiron.com/en/quarterly-security-reports/q2-2016-mobile-security-and-risk-review

iOS Security:
Protection From the Inside Out

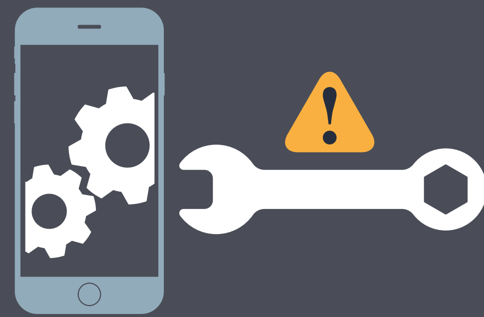
What began in 2007 with a revolutionary piece of hardware offering a great user experience through its remarkable mobile browser has now become the secure foundation of profound business transformation. When Apple launched the iPhone and the iOS operating system, the stage was set for an entirely new approach to endpoint computing and endpoint security. The successful combination of security with usability has helped iOS achieve and maintain dominance in the enterprise with over 80% of enterprise mobile device market share.[4]

The security of iOS devices is achieved through a unique marriage of hardware and software capabilities designed to protect the device, the data it handles (either at rest or in transit), and the ecosystem, including apps and Internet services used by the device. Security is a central goal for iOS, so much so that integration of security components and capabilities actually begins during chip fabrication. iOS security extends throughout the device and software lifecycle. Many of the security features covered below are enabled by default and, in some instances, not configurable by end users.

Secure Boot: Ensure a Secure Chain of Trust

Each of the processors in an iOS device (application processor, baseband chipset, and the Secure Enclave on devices with A7 or newer chips) utilizes a secure boot process in which each stage relies on cryptographically signed components and a chain of trust that ensures the boot process will only proceed after the chain of trust has been verified.

4 Source: MobileIron 2Q16 Security and Risk Review.



Unauthorized OS Modification

The process of modifying iOS outside of the standard update procedure, also known as "jailbreaking," refers to a set of techniques in which iOS is hacked to change its underlying functionality. Performing these types of modifications bypasses many of the security capabilities that are core to iOS and can expose devices to a variety of undesirable side effects[5] such as:

- Shortened battery life
- OS instability
- Disruption of services including voice, data, and Apple Push Notifications (APNs)
- Exposure to malware and other security vulnerabilities
- Inability to apply future updates or total device disablement

While the overall trend of unauthorized OS modification has been flat or slightly down, devices running compromised operating systems can present a significant risk to user and enterprise data, so measures should be taken to defend against their introduction.[6]

5 Additional information: https://support.apple.com/en-us/HT201954

6 Source: MobileIron 2Q16 Security and Risk Review

Mandatory Code Signing: Ensure the Integrity of all iOS Updates

The use of cryptographic verification goes beyond Secure Boot. It is used on an ongoing basis to ensure the integrity of all iOS updates. During an OS upgrade, Apple installation authorization servers receive a list of cryptographic "measurements" for each component of the installation package, the unique ID of the device, and a nonce value to prevent replay attacks. If the measurements match versions for which upgrades are permitted, the authorization server signs the result and returns it in the upgrade payload. This process makes OS updates highly tamper-resistant.

Code signing also comes into play for applications installed and running on iOS. All executable code on iOS must come from a known and approved source, which is verified through the use of an Apple-issued certificate. In addition to validating the source, mandatory code signing also prevents third-party apps from loading unsigned modules or using polymorphic code that could dynamically change the operation of the app.

App Store: Deploy and Update Applications

The role of the App Store is primarily to provide the infrastructure to deploy and update applications. However, the App Store also plays a central role in device security. All apps submitted to the App Store are subject to review by Apple and checked to ensure that they operate as described, are free of obvious bugs, and generally follow best practices for iOS app development. Moreover, in order for developers to distribute an app via the App Store, they must join the Apple Developer Program. This registration enables Apple to validate the identity of the developer and issue a certificate that allows the developer's app to be uploaded to the App Store and run on the device (see Mandatory Code Signing for more information). Requiring a valid identity deters developers from creating malicious apps. More importantly, if an app is found to be malicious, the developer's certificate can be revoked to prevent all their apps from running.

You should carefully manage access to the Apple-issued code signing identities, to prevent developers from creating malicious apps appearing to be originating from your organization. Such scenarios may not only pose a big reputation and liability risk, but can also cause an operational risk, if Apple revokes your certificates and all your in-house apps suddenly stop working. If you work with multiple vendors who create your apps, consider providing a self-service code-signing portal. MobileIron integrates with incapptic Connect, a software solution combining self-service for app owners and vendors with full automation of the release process, enabling new apps to be submitted, and existing ones updated at the click of a button. For more information visit: https://incapptic.com/

App Execution: Protect Against Unauthorized Code

App execution on iOS is a significant departure from traditional operating systems. Unlike legacy operating systems, most system processes and all third-party apps on iOS run as a non-privileged user. Apps are also sandboxed, which prevents them from modifying the device and OS, and also prevents them from accessing and modifying the data of other apps. Apps can expose frameworks or libraries that can be accessed by other apps from the same developer. However, built-in executables cannot link against any library that did not ship with the system, providing further protection against unauthorized code execution.

Default Encryption: Protect Data at Rest and in Motion

The data on the flash storage of an iOS device is protected by a technology called Data Protection. Data Protection builds on the cryptographic hardware capabilities to provide per-file encryption via the dedicated AES-256 crypto engine built into each device. Each new file is assigned a Data Protection class when it is created and the file encryption keys are encrypted based on the assigned class. Data Protection is enabled for all third-party apps on iOS 7 and higher. Perhaps more importantly, Data Protection provides mechanisms to eject encryption keys from memory, which controls when and how data is decrypted and made accessible.

In addition to protecting the data at rest on the device, iOS also supports protecting data in motion. Introduced in iOS 9, App Transport Security (ATS) is a mechanism for requiring the encryption of connections to Internet services using Transport Layer Security (TLS) v1.2. Apple's intent was to mandate the use of ATS or explicitly specified exceptions as of January 1, 2017 for all apps submitted to the App Store. Enforcement has been temporarily delayed, but Apple strongly recommends the use of HTTPS so that end users and organizations can be assured that the data they access is better protected from accidental disclosure or interception during transmission. The use of TLS v1.2 also ensures that backend services are less vulnerable to attacks that exploit weaknesses in older protocol versions.

iOS Device Configuration, Management, and Ownership

Beyond the integrity of the OS and application, iOS security considerations include the lifecycle process of managing and updating the device settings. These can be adjusted depending on whether the device is corporate-owned or owned by the employee and used for both personal and work tasks.

Configuration Profiles: Distribute Device Settings

iOS provides a mechanism to distribute custom device settings in the form of Configuration Profiles.[7] These XML files can contain a variety of settings, including digital certificates, email accounts (POP, IMAP, and Microsoft Exchange), LDAP directory services, web-clips, Wi-Fi, and VPN. Configuration Profiles can be created with a macOS app called Apple Configurator 2 and they may be installed by tethering devices to Macs running Apple Configurator 2 via USB or via several over-the-air (OTA) methods. Settings defined in Configuration Profiles cannot be modified by the user, providing enterprise IT admins with a convenient way to standardize the setup of iOS devices.

Mobile Device Management: Check-in and Execution of Remote Management Commands

Mobile device management (MDM) was introduced in iOS 4 and gives device administrators the ability to perform management tasks remotely. MDM works through a combination of HTTP, TLS, and APNs, and is composed of the MDM check-in protocol and the MDM protocol. The check-in protocol exists to verify device eligibility for MDM enrollment, as well as to ensure that the management server can communicate with the device. The MDM protocol defines the actual commands that admins can use to perform operations on devices. The commands

7 Additional information: https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

are divided into two categories: queries and actions. Queries allow admins to gather information about a device, while actions allow admins to perform functions such as removing an app or factory resetting a device.

Supervision: Advanced Security Capabilities for Enterprises

Employee-owned devices enrolled in MDM are managed by a baseline set of security and management controls, but corporate-owned iOS devices in supervised mode are managed by more restrictive IT controls via the MDM system. For example, supervision is commonly used for devices that need to be restricted to single-app mode in which a device runs a single application in a locked kiosk-like or dedicated-use configuration. IT can also prohibit access to consumer- and personal-use features such as the iCloud Photo Library and automatic app downloads by making them restrictions that the user can't modify.

On supervised devices, IT admins can prevent users from accessing restricted apps. While the user may download a blacklisted app, an EMM server can use MDM controls to block the app from being used or even being seen at all. For example, an organization may block the use of social media apps like Facebook on supervised work devices. Supervised devices can be locked down so that employees can only access company-approved apps and no others, not even the iOS out-of-the-box apps. IT admins can also control which apps, icons, and web-clips appear on the home screen and place applications persistently in the dock via MDM controls.

Device Enrollment Program: Mandatory MDM Enrollment and OTA Supervision

The Device Enrollment Program (DEP) ties the device to the corporate Apple purchasing account for a customer using the device's unique serial number. In doing so, the customer gains access to an online portal where serial numbers or entire purchasing orders can be configured to enforce OTA supervision and to optionally enforce MDM enrollment so the user can't remove the MDM profile.

DEP offers a mechanism for IT admins to create a more streamlined onboarding workflow for employees. With DEP, IT can modify the out-of-the-box experience and eliminate many unnecessary touches by customizing the steps in the iOS Setup Assistant, including the ability to skip certain screens. Fewer prompts and notifications mean less frustration for employees and helps to get them up, running, and productive more quickly.

"Managed" and "Supervised" Devices: Understanding the Difference

Managed device:
A managed device can be owned by either the employee or the company. With a managed device, IT can secure and manage corporate data and apps separately from the employee's personal data and apps by installing an MDM profile. Corporate content and apps can be wiped if the device is lost, stolen, or falls out of compliance, while personal information remains untouched. A managed device meets enterprise security requirements and can isolate personal from corporate accounts and apps with their data, but it cannot and should not stop the end user from enjoying most of the consumer-centric Apple iOS capabilities and ecosystem.

Supervised device:
Apple is sending a strong message that supervision is the only desirable mode by which an enterprise can fully control and restrict iOS device functions. Supervision is reserved for corporate-owned devices and provides IT with greater control than a managed device. In supervised mode, an iOS device can be secured with several management features, including single-app mode and always-on VPN. IT can also restrict features such as the iCloud Photo Library and automatic app downloads — restrictions that the user can't modify. Supervision is typically initiated during device setup via USB connection or OTA through DEP.

MobileIron EMM: Protection From the Outside In

Apple is continually improving the security of iOS devices, which is partly why they have become such popular devices among both consumers and business users. For IT organizations, extending uniform iOS security across hundreds or thousands of devices is critical to ensuring that enterprise data protection is not limited to the device itself. Once devices connect to open networks, IT needs the ability to secure apps and data outside of the iOS platform.

Enterprise mobility management (EMM) is an all-encompassing set of processes and technologies aggregated as a unified lifecycle product to manage mobile devices, secure wireless networks access, and provide other mobile computing services in a business context. In addition to addressing security concerns, a strong EMM strategy also helps employees be more productive by providing them with the tools they need to perform work-related tasks on mobile devices. EMM solutions combine at least three or more mobility management lifecycle capabilities such as:

- **Mobile device management (MDM):** These capabilities provide the fundamental visibility and IT controls needed to securely configure, deploy, manage, and retire devices.
- **Mobile application management (MAM):** The tools and technologies used to deploy, manage, and extend security of applications.
- **Mobile content management (MCM):** A type of deeply integrated content management system (CMS) capable of securely storing and delivering content and file services to mobile devices.
- **Additional advanced integration capabilities:** These can include directory services and identity provider integration, public key infrastructure (PKI) certificate issuance and management, and much more.

EMM is the ideal solution for effectively utilizing the security tools within iOS to augment device security whenever users access environments such as cloud resources or unsecured networks in hotels, airports, and coffee shops. An EMM platform must be selected and deployed in order to take advantage of all the Apple iOS advanced MDM and MAM features outlined in the previous section. With an EMM platform like MobileIron, organizations fully benefit from the innate security of iOS and the MDM protocol it supports by providing a standardized platform to distribute configurations and security settings to multiple devices across the enterprise. Business productivity and process transformation through mobility can be facilitated by adding more advanced capabilities. A strong EMM platform like MobileIron provides the infrastructure to deploy a comprehensive corporate mobility strategy.

Getting Started: User Authorization and Authentication

Linking Devices, Users, and Policies via Enterprise Directories

Applying policies and granting entitlements requires a “source of truth” to scale in the enterprise. In the legacy model, policies and entitlements are typically linked to an enterprise directory and based on various attributes available in the directory, such as group membership. While this approach has served traditional endpoints very well, it is ill-suited to modern consumer devices because they are not directory-aware. MobileIron EMM helps organizations leverage their existing security models by creating a conduit between the device and the enterprise directory, giving them the ability to map policies and configurations to users and devices as they would with traditional endpoints. Using the Lightweight Directory Access Protocol (LDAP) as well as its internal database of 200+ unique device attributes, MobileIron is able to combine user and device information into flexible rules to ensure that rights are assigned appropriately.

Stronger, Simpler User Authentication with Digital Certificates, Kerberos, and Single Sign-on

MobileIron also offers robust support for PKI. Digital certificates offer an improved user experience for mobile devices because they can provide strong authentication without the need for users to enter cumbersome passwords. The MobileIron EMM platform has a built-in certificate authority and can enroll devices against third-party PKI from Entrust, OpenTrust, Symantec and other PKI providers via Simple Certificate Enrollment Protocol (SCEP).

Digital certificates can also be used in conjunction with Kerberos constrained delegation (KCD) which provides a high level of security and a smooth user experience by allowing users to authenticate to Kerberos-enabled services without requiring enterprises to expose Kerberos infrastructure externally.

MobileIron also supports the Kerberos single sign-on (SSO) capabilities in iOS by providing a Kerberos Key Distribution Center Proxy (KKDCP). This allows iOS devices to directly request and receive Kerberos tickets to access enterprise services while protecting the critical key distribution center (KDC) server.

Manage and Secure at Scale: The MDM Protocol as an Enterprise Control Plane

Once the directory policy and authentication rules have been established, device provisioning at scale can begin. An admin can place the MDM payload within a configuration profile and distribute it to managed devices through email or a web page. Once the enrollment process is complete, additional configuration profiles can be delivered OTA. Configuration profiles and provisioning profiles installed through the MDM service are called managed profiles and are automatically deleted when the MDM payload is removed. Although an MDM service may have the rights to inspect the device for the complete list of configuration profiles or provisioning profiles, it may only remove apps, configuration profiles, and provisioning profiles that it originally installed. A configuration profile installed through MDM cannot be removed or modified by the end user, making it an ideal option for corporate-owned, single-app devices that require tighter IT control and security.

Simplified, Low-touch Device Provisioning

In this OTA management model, iOS can enroll through SCEP into an MDM configuration, which then manages all subsequent profiles. This makes it easy for large enterprise organizations to simultaneously configure a large number of devices and distribute MDM payloads from a server with custom email settings, network settings, or certificates.
Using the MDM protocol, an admin can distribute an MDM enrollment payload by embedding it into a configuration profile and making it accessible to targeted devices through email or a web page. The MDM protocol enables system administrators to send device management commands to managed iOS devices running iOS 4 and later. IT administrators can inspect, install, or remove profiles, delete

passcodes, and selectively wipe a managed device. MDM servers can use the MDM protocol to ensure that only authorized users can access corporate apps and data on their devices.

Because configuration profiles can be both encrypted and locked by MDM, they become managed profiles and users can't arbitrarily remove, alter, or share the settings with others. Configuration profiles and application provisioning profiles installed through the MDM service as managed profiles are automatically deleted when the MDM payload itself is removed. By default, the MDM payload can be removed at any time from an end user's personal device.

That authority over the ownership model is how the Apple MDM protocol empowers the enterprise IT administrator to bridge the security gaps between fully enterprise-owned devices and completely disconnected user-owned devices. That is also why, on a user-owned device, MDM is and must always be removable. The enterprise saves money by not having to pay for the equipment. In exchange, IT has only limited control over the device and data but the end user must allow IT to wipe enterprise data and settings if a device is compromised or stolen. To that effect, Apple ensures that personal user settings and data can be backed up and restored by the end user; the enterprise cannot prevent that process for devices that are not supervised.

Getting Down to Work: App Security and Lifecycle Management

Distributing mobile apps through an enterprise app store

Of course, no single security measure is enough on its own. Hackers will always find ways to break into their intended targets, so additional security is always recommended — especially in enterprise environments with large volumes of sensitive corporate data. By curating and deploying a list of IT-approved apps through an enterprise app store, IT can prevent unauthorized apps from being downloaded through the App Store onto corporate-owned devices.

The release of iOS 9 allowed IT to disable the App Store globally while maintaining the ability of the IT admin to install, manage, update, and remove App Store apps via MDM. IT can now silently push apps through the EMM server on supervised devices or assign apps to the device for the end user to install. This allows mobile administrators to more easily maintain a standard deployment blueprint and not worry about end users installing personal apps on supervised devices. IT can easily manage curated apps, whitelists, and blacklists in an EMM app catalog and reduce the risk of data loss by preventing users from installing unauthorized and potentially compromised apps. These app security capabilities are especially advantageous for managing kiosk devices and fleet deployments.

Mobile Application Management: Augment the App Sandbox

When application installs are initiated via an enterprise app storefront using the MDM protocol, the applications become known as managed apps. By installing managed apps, IT gains more control over how apps and their data are used on the device. Managed apps build on the protections provided by application sandboxing by giving organizations the ability to remove the application and selectively wipe application data. Managed apps also enable security features like "Open In" and can enable or disable data backup to iCloud or iTunes.

Managed Open In restricts the organizational information that gets sent to employee devices by allowing it to be processed only in specified managed apps. For example, if EMM delivered the Microsoft Word app, users would only be able to open .docx attachments in the Word app or another EMM-installed app that can handle that same data type.

When a device is removed or quarantined from EMM by either the user or an administrator, all payloads installed by EMM are removed. This also includes the managed apps and any data they delivered to the device. If the action taken is not a complete wipe, this removes all corporate apps, data, and settings, which effectively removes the corporate sandbox contents and enhancements and leaves behind only the user's personal content.

As more enterprise data moves outside of traditional repositories and into the local storage of mobile devices, the use of these capabilities is integral to a comprehensive data loss prevention (DLP) strategy. In extreme cases, IT may also initiate a full wipe or factory reset of the device.

Advanced Security for In-house Applications: MobileIron AppConnect

MobileIron AppConnect allows organizations to embed additional security and management controls into their applications using a special SDK. AppConnect containerizes apps to protect corporate data-at-rest without touching personal data and provides more granular policy controls than those available via standard iOS management capabilities. As a result, each app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable.

Each app container is also connected to other secure app containers. This allows security policies and corporate data to be shared between secure applications. Policies for the behavior of application containers are controlled by the MobileIron EMM console. AppConnect-enabled applications can also leverage MobileIron Sentry to exchange information with enterprise backend systems using per-app VPN solutions or MobileIron AppTunnel. Additionally, MobileIron Access delivers a cloud security solution that provides conditional access to cloud services from mobile apps and browsers. It correlates user identity with unique information feeds such as device posture and app state to ensure business data can't be accessed by unverified users, stored on unsecured devices, or shared with unauthorized cloud services.

Secure Dynamic Access Control

Devices regularly fall in and out of compliance, especially in BYOD programs, so IT needs an automated approach to monitor the security posture of devices and prevent non-compliant devices from accessing corporate resources. MobileIron AppTunnel provides dynamic access control by combining the secure transport of traditional VPN with certificate-based identity and posture-based policy. This simplifies enterprise access for the user while ensuring only authorized devices can access corporate resources.

Protect Data-in-Motion with Tunneling

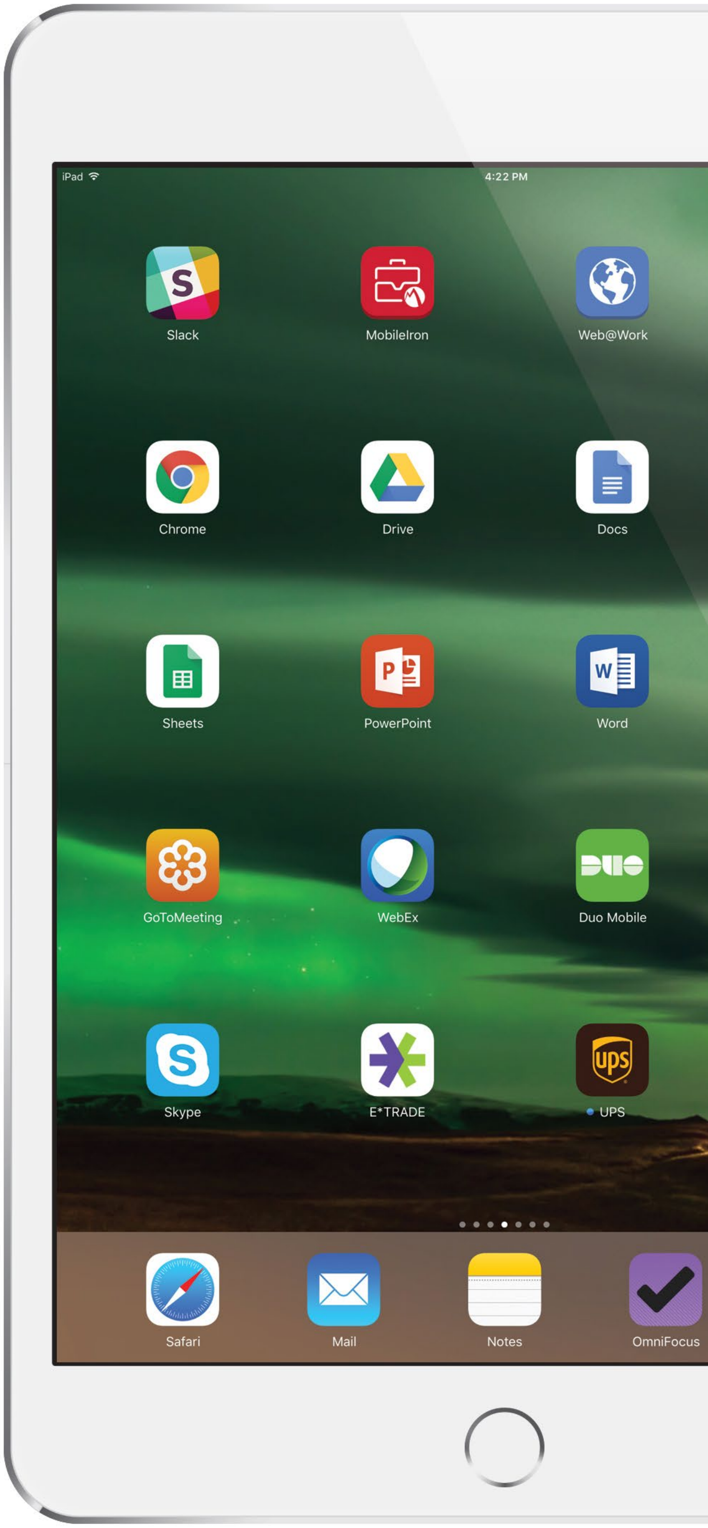
MobileIron's ability to proxy Kerberos allows iOS devices that are not on the corporate network to use iOS SSO without exposing the Kerberos KDC. This protects both data-in-motion and the organization's Kerberos infrastructure. For example, MobileIron Tunnel enables Apple's Safari browser to securely access intranet sites behind the firewall with transparent authentication so users do not have to re-enter their usernames and passwords as they go from site to site.

MobileIron Access: Extending Security and Trust to SaaS Apps

As more organizations transition their mobile apps and data to the cloud, they have to rethink their security requirements. Traditional cloud security solutions that rely primarily on a user ID and password can't sufficiently protect cloud data from falling into the wrong hands through unsecured mobile apps and devices. Extending security and trust to software-as-a-service (SaaS) apps such as Office 365, Salesforce, G Suite, and Box requires a solution that enforces conditional access policies based on user identity, the security posture of the mobile device, and the state of the mobile app. MobileIron Access is a cloud security solution that allows IT admins to define granular cloud access control policies based on application, IP address, identity, device posture, and other criteria. As a result, IT can bridge the gap between mobile and cloud security and get better control over how users access enterprise cloud services.

MobileIron ServiceConnect: Integration with Third-party Enterprise Security Systems

The exclusive 1:1 relationship between a managed device and an EMM platform puts MobileIron in a unique position to fill roles previously held by multiple software agents. MobileIron ServiceConnect extends the visibility of the MobileIron EMM platform to other enterprise IT and security systems, enabling them to support iOS devices as they would a legacy endpoint. Whether it's an IT service management (ITSM) console, mobile app release automation system, or a security information and event management (SIEM) system, organizations can seamlessly leverage their existing policies and procedures across iOS devices using MobileIron EMM as a "source of truth" as well as a policy instrument.



EMM + iOS: A Blueprint for Securing the Modern Mobile Enterprise

A mobile security strategy that combines EMM with iOS can give organizations the confidence to meet the biggest security challenges they face today. Together, iOS and EMM provide a comprehensive, secure management platform and operating system that give IT security teams the scalable, proactive control they need to manage a rapidly expanding mobile footprint. An EMM solution like MobileIron provides a comprehensive platform that protects enterprise information wherever it lives: in the datacenter, in the cloud, in mobile apps, on mobile devices, and in motion between them.

By using EMM to manage their entire mobile fleet, organizations can ensure all their iOS devices are secured with the latest policy configurations, run the most current apps and OS versions, and can only be accessed by authorized users. Unified endpoint management with EMM also reduces total cost of ownership (TCO) because organizations can eliminate many labor-intensive configuration processes, remotely install apps and policy updates, troubleshoot remotely, and empower IT to manage a range of corporate-owned and BYOD device types.

With MobileIron's advanced mobile security platform and Apple's expanding iOS security capabilities, IT can deliver the full value of iOS enterprise mobility without putting data at risk. Our EMM platform is designed to both augment and simplify the existing security capabilities provided in iOS so enterprise organizations can ensure the security and ease-of-use of every iOS device and app in their environment.

MobileIron

415 East Middlefield Road
Mountain View, CA 94043
info@mobileiron.com
www.mobileiron.com
Tel: +1.877.819.3451
Fax :+1.650.919.8006