mobileiron

Unified Endpoint Management (UEM)

Challenge

Organizations need to securely access and easily manage their business data on any endpoint used by their employees, contractors, and frontline workers.

Today's modern digital workplace includes the use of diverse endpoints such as iOS, macOS, Android, Windows 10 based devices as well as other immersive and rugged devices such as HoloLens, Oculus, Zebra and more.

The need for managing privacy and compliance, and minimizing risk are necessitating the need to separate and protect corporate apps from the personal apps of their users' endpoint devices. There is a need for a secure unified endpoint management solution that also provides a superior user experience.

Secure your digital workplace with the industry's first mobile-centric security platform

MobileIron UEM is powered by the first mobile-centric security platform to securely access and protect data across your digital workplace. MobileIron's security approach validates the device, to ensure that only authorized users, devices, apps, and services can access business resources. You realize a delightful, native user experience across any endpoint.

MobileIron UEM puts enterprise mobile security at the center of your enterprise and allows you to build upon it with enabling technologies to eliminate passwords (zero sign-on (ZSO)), to ensure user authentication (multi-factor authentication (MFA)) and to detect and mitigate endpoint security threats (mobile threat defense (MTD)).

Key use cases

Ensure privacy and compliance in organizations primarily concerned about protecting sensitive data: Secure business data on any endpoint and separate business and personal data on various endpoints

Enable multi-device, multi-OS, multi-app management from a single console: The organization has a mixed device environment with iPhones, iPads, Macs, Android based devices, Win 10 laptops and PCs, Zebra, Oculus, etc. Unified management of these devices with different OSs and apps is top priority.

Empower frontline workers Support the field, fleet, and mobile workers in Healthcare, Transportation, Manufacturing, and other industries who use Rugged Devices or devices in Kiosk mode.

Provide a superior end user choice and delightful user experience: When user choice and end user experience matters, MobileIron UEM provides the simplest onboarding and superior on device experience which improves user productivity.

Security standards and certifications*

- Common Criteria Certification
- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield
- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- SOC 2 Type II
- CCN (Spain)

Additional information on MobileIron certifications can be found here:

www.mobileiron.com/en/certifications-and-uptime

About MobileIron

MobileIron UEM is powered by the first mobile-centric security platform to securely access data on any end point across your digital workplace while delivering a delightful user experience. For more information, please visit **www.mobileiron.com**

Comprehensive security

MobileIron's UEM provides the visibility and IT controls needed to secure, manage, and monitor any corporate or personal-owned mobile device or desktop that accesses business-critical data. It allows organizations to secure a vast range of BYO devices being used within the organization while managing the entire lifecycle of the endpoint including:

- Automated onboarding
- Policy configuration and enforcement
- Application distribution and management
- Management and security monitoring
- Decommissioning and retirement

MobileIron UEM is enabled on a proven, secure, scalable, enterprise-ready architecture with flexible deployment options that puts the user experience first while also maintaining the highest quality security standards.

MobileIron Sentry acts as an email and content in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems. MobileIron Tunnel is a multi-OS app VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction

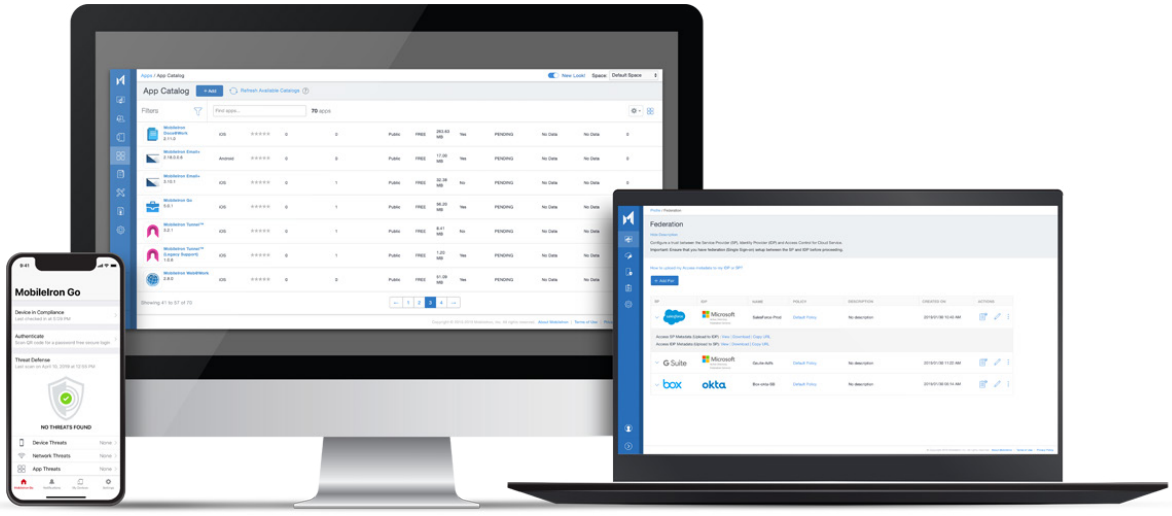
Manage and grow your business confidently and securely with mobile and cloud

Organizational and user control: MobileIron UEM allows organizations to implement individualized mobility and security strategies to meet their business needs at their own pace. We also ensure the privacy of users' personal data while protecting corporate data – giving users and administrators alike control over their information.

Freedom of choice: MobileIron UEM is OS- and device-agnostic. Administrators can choose cloud or on-premises deployment based on their budget and employees can use their favorite endpoints for work.

Experience-driven adoption: MobileIron UEM helps IT drive adoption by supporting a native user experience across productivity apps at work. This simplifies compliance while mitigating security threats and shadow IT. With higher user adoption rates, IT can accelerate productivity and growth across the organization.

Enable business resiliency: Our mobile-centric security platform prevents business interruption without being intrusive to the user. Invisible and automated security ensures compliance while allowing your business to forge ahead.



MobileIron unified endpoint management (UEM)

	Secure UEM	Secure UEM Premium
Device management and security		
Security and management - Secure and manage endpoints running Apple's iOS, macOS, iPadOS, Google's Android, and Microsoft's Windows 10 operating systems. Available on-premises and as a cloud service.	✓	✓
Mobile application management (MAM) - Secure business apps with MobileIron AppStation on contractor and employee devices without requiring device management.	✓	✓
Easy on-boarding - Leverage services such as Apple Business Manager (ABM), Google Zero-Touch Enrollment and Windows AutoPilot to provide users with automated device enrollment.	✓	✓
Secure email gateway - MobileIron Sentry, an in-line gateway that manages, encrypts, and secures traffic between the mobile endpoint and back-end enterprise systems.	✓	✓
App distribution and configuration - Apps@Work, an enterprise app storefront, combined with Apple Volume Purchase Program (VPP) facilitates the secure distribution of mobile apps. In addition, capabilities such as iOS Managed Apps and Android Enterprise allow for easy configuration of app-level settings and security policies.	✓	✓
Scale IT operations		
Helpdesk tools - Help@Work lets IT remotely view and control a users' screen, with the user's permission, to help troubleshoot and solve issues efficiently.	✓	✓
Reporting - Gain in-depth visibility and control across all managed devices via custom reports and automated remediation actions.	✓	✓

Continued on next page...

Secure productivity		
Secure email and personal information management (PIM) app - MobileIron Email+ is a cross-platform, secure PIM application for iOS and Android. Security controls include government-grade encryption, certificate based authentication, S/MIME, application-level encryption, and passcode enforcement.		✓
Secure web browsing - Web@Work enables secure web browsing by protecting both data-in-motion and data-at-rest. Custom bookmarks and secure tunneling ensure that users have quick and safe access to business information.		✓
Secure content collaboration - Docs@Work allows users to access, create, edit, markup, and share content securely from repositories such as SharePoint, Box, Google Drive and more.		✓
Mobile app containerization – Deploy the AppConnect SDK or app wrapper to provide an additional layer of security for your in-house mobile apps or choose from our ecosystem of AppConnect integrated apps.		✓
Derived Credentials – Support two-factor authentication using common access cards (CAC) and personal identity verification (PIV).		✓
Secure connectivity		
Per app VPN – MobileIron Tunnel is a multi-OS VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.		✓
Conditional access		
Trust Engine – Combine various signals such as user, device, app, network, geographic region, and more to provide adaptive access control.		✓
Passwordless user authentication – Passwordless multi-factor authentication using device-as-identity for a single cloud or on-premises application.		✓

Note:

- Availability of certain features and functionality is dependent on the deployment type – on-premises vs SaaS.
- Availability might vary based on operating system and device type