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 use of diverse endpoints such as iOS, Android, Chrome OS, macOS, 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 delightful user experience.

Secure your digital workplace with the industry’s first mobile-centric, zero trust security platform

MobileIron UEM is the foundation of the first mobile-centric, zero trust security platform to securely access and protect data across your digital workplace. MobileIron’s zero trust 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 device and OS.

MobileIron UEM puts enterpise 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, network, or application, and separate business and personal data on various devices.

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

Provide a superior end user choice and delightful user experience: When user choice and end user experience matters, MobileIron 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 the foundation of the first mobile-centric, zero trust 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 employee-owned mobile device or desktop that accesses business-critical data. It allows organizations to secure a vast range of employee devices being used within the organization while managing the entire lifecycle of the device including:

- Policy configuration and enforcement
- Enterprise application distribution and management
- Conditional access and multi factor authentication (MFA) with MobileIron Access
- Mobile threat detection and remediation with MobileIron Threat Defense

MobileIron UEM is based on a proven, secure, scalable, and enterprise-ready architecture that puts the user experience first while also maintaining the highest quality security standards.

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 devices 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 zero trust foundational platform prevents business interruption without being intrusive to the user. Invisible and automated security ensures compliance while allowing your business to forge ahead.
<table>
<thead>
<tr>
<th>MobileIron unified endpoint management (UEM)</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile device management and security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mobile device management (MDM)</strong> - Secure and manage endpoints running Apple iOS and Google Android operating systems. Available on-premise and as a cloud service.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Easy onboarding</strong> - Leverage services such as Apple Device Enrollment Program (DEP), Apple Business Manager, Android zero-touch, or Samsung KNOX mobile enrollment to provide users with the simplest user onboarding process.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Mobile app distribution and configuration</strong> - Apps@Work, a customizable 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.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Secure email gateway</strong> - MobileIron Sentry is an email and content in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Desktop management and security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Windows 10 management</strong> – Unified platform to manage modern Windows endpoints using a combination of Windows MDM APIs and traditional group policy objects.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Mac management</strong> – Manage macOS endpoints using state-of-the-art MDM APIs that allows for seamless enrollment, app distribution, and lifecycle management for Macs.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Secure productivity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secure email and personal information management (PIM) app</strong> – 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 complex passcode enforcement.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Secure web browsing</strong> - Web@Work enables secure web browsing by protecting both data in motion and data at rest on the endpoint. Custom bookmarks and secure tunneling ensure that users have quick and safe access to business information.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Secure content collaboration</strong> - Docs@Work allows users to access, create, edit, mark up, and share content securely from repositories such as SharePoint, Box, Google Drive, and more.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Mobile app containerization</strong> – 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.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Derived Credentials</strong> – Support multi-factor authentication (MFA) using common access cards (CAC) and personal identity verification (PIV) cards.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
### Secure connectivity

**Per-app VPN** – 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. Tunnel is available for iOS, Android, macOS, and Windows 10.

### Scale IT operations

- **IT systems integrations** – ServiceConnect lets you share data from the MobileIron UEM platform with other IT systems, such as Splunk or ServiceNow, to streamline IT operations.

- **Server monitoring and management** – MobileIron Monitor is a single dashboard view of system performance and historical trends for MobileIron Core and Sentry servers.

- **Help desk tools** – Help@Work is an app that lets IT remotely view and control a user’s screen, with the user’s permission, to help solve issues in an efficient manner.

### Note:

- Availability of certain features and functionality depends on the deployment: cloud versus on-premises
- Availability might vary based on operating system and device type.
- ServiceConnect integrations available with the Platinum bundle include MobileIron-developed software to integrate with specific third-party products and services. API-based integrations do not require the purchase of the Platinum bundle.