Everywhere Enterprise

MobileIron is a highly secure mobile-centric security platform that accesses and protects data from anywhere.

MobileIron (the Solution) provides the platform to help secure the Everywhere Enterprise. Using the MobileIron platform, Everywhere Enterprises can enable employees to work from virtually anywhere, while helping to ensure that corporate data is secure on any device, application, or network. Organizations need to keep access to their enterprise data highly secure and easily manage all endpoints used by their employees, contractors, and frontline workers. The platform is available both as a cloud app (MobileIron Cloud) and on-premises solution (MobileIron Core).

The need to manage privacy and compliance makes it essential to separate and protect corporate apps from the personal apps on the users' endpoint devices. This requires a unified endpoint management solution that is highly secure while also providing a superior user experience.

Potential benefits

- Enhances productivity with app management and content integration
- Provides data security and compliance that meets many federal guidelines and privacy certifications
- Integrates easily and cost-effectively
- Delivers a scalable solution (Cloud or on-premises)

Features

- MacOS, Windows 10, Android, and iOS management available
- TRUSTe Privacy Seal and FedRAMP Authority to Operate (ATO)
- Choices to maximize your budget; select from either device or user subscriptions
- Email+ provides an email/Product Information Management
- Web@Work offers a highly secure native web browser
- Tunnel provides a highly secure tunnel-per-app virtual private network (VPN)

This Product Brief applies to purchases made on and after 06/30/2020. For purchases made before that date, see https://www.business.att.com/content/dam/businesscenter/pdf/mobileIron-cloud-product-brief.pdf .

Product offerings:

Secure Unified Endpoint Management (UEM) – Streamline security and management capabilities for bring-your-own-device or corporate devices running iOS, macOS, Android, and Windows 10 with a highly secure productivity suite and connectivity.

Secure UEM Premium – Extend security and device management capabilities with a highly secure productivity suite, highly secure connectivity, and advanced conditional access capabilities for cloud apps and on-premises services.

Optional add on features:

MobileIron Threat Defense – Protect and remediate against known and zero-day threats and phishing attacks on mobile devices, while also leveraging basic app analytics.

Zero Sign-on – For organizations that want to eliminate passwords to reduce the risk of data breaches.

Bundle Features	Secure UEM	Secure UEM Premium
Device management and security		
Security and management – Help secure and manage endpoints running Apple iOS, macOS, iPadOS, Google Android, and Microsoft Windows 10 operating systems.	•	•
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 helps secure 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.	•	•
Scale IT Operations		
Help desk 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.	•	•
Improve productivity		
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.		•
Secure web browsing – Web@Work enables highly secure web browsing by protecting both data-in-motion and data-at-rest. Custom bookmarks and highly 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 more 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).		•
ServiceConnect integrations* – Integrate MobileIron Cloud with ServiceNow Solutions or services to help streamline IT workflows.		•

Optional add on features		
MobileIron Threat Defense	**MTD**	**MTD Premium**
Threat detection – Protect against known and zero-day threats and active attacks with sophisticated machine learning and behavior-based detection on the mobile endpoint.	•	
Threat remediation – Limit time of exposure for possible exploitation and help stop zero-day attacks with policy-based compliance actions that provide alerts of risky behaviors and proactively shuts down attacks on the mobile endpoint with or without network connectivity.	•	
Advanced app analytics – Continually evaluate mobile app risks to identify privacy and security risks.		•
Zero Sign-on (requires Secure UEM Premium)	**ZSO**	
Passwordless user authentication – Passwordless, multi-factor authentication using device-as-identity to protect against credential theft.	•	
Stronger authentication factors – Replace passwords with stronger authentication factors including biometrics, authenticator apps, push notifications, one-time PINs (OTP), and QR codes.	•	
Conditional access – Integration with Secure UEM Premium allows for conditional access based on signals such as user, device, app, network, and location.	•	
Intuitive user experience – Customizable access and remediation workflows to enable users to self-remediate without requiring assistance from the IT helpdesk.	•	

* Availability of certain features and functionality is dependent on the deployment type – on-premises vs cloud aka Software-as-as-Service (SaaS). Availability might vary based on operating system and device type.

Professional Services

Purchase of a professional configuration and training package is required for the initial purchase of both Secure UEM and Secure UEM Premium offerings. Professional Services may be provided by AT&T or MobileIron (only one may be chosen). Customers who select MobileIron will be provided a service summary and statement of work by MobileIron.

AT&T Professional Services

AT&T Professional Services include configuration and training as well as the AT&T Business customer support desk (CSD). Customers may select from one of the following AT&T Professional Services packages for implementation and training:

- **Basic**, Standard, or Standard Plus installation and training services for Cloud Secure UEM
- **Premium** installation and training services for Cloud Secure UEM Premium
- **Premium** or Premium Plus installation and training for Core Secure UEM and Secure UEM Premium.

Customer Support Desk (CSD)*

Monthly recurring charge (MRC) subscriptions include a subscription plus CSD Support.

All subscriptions include the following CSD Support:

- Technical support
- MACD (moves, adds, changes, disconnects) administration
- Service optimization

Monthly recurring charge (MRC) subscriptions to all MobileIron editions include CSD Support.

* AT&T will not provide technical support to end users and will not provide technical support for applications and/or content that Customer chooses to distribute and are not included in the Solution's feature list.

Remote Administration Support Plan (optional)

The Remote Administration Support Plan provides a higher level of CSD managed technical support from certified technicians from AT&T Business.

The optional Remote Administration Support Plan (available at an additional cost) is designed for organizations with minimal internal support and mobile expertise. An expert Unified Endpoint Management consultant will be assigned to you to provide additional benefits beyond basic CSD support. The Remote Administration Support Plan includes:

- Daily, ongoing configuration and lifecycle administration of the managed service on your behalf
- An expert Unified Endpoint Management Consultant will be assigned to you to provide proactive recommendations and ongoing consultation on UEM design, implementation, and administration
- Advanced security and policy
- Access to trained and experienced support staff with cross-solution expertise with UEM, OEM, OS, and application platforms (CCNA, CCNP, MCSA, CISSP)
- Ability to update security policies and authorize device configurations
- Annual performance health checks

MobileIron Monthly Pricing*		
	Price per device	**Price per user**
Secure UEM	$4	$6
Secure UEM Premium	$7.50	$11.50
Optional Features		
MobileIron Threat Defense	$4	$6
MobileIron Threat Defense Premium	$6	$9
Zero Sign On	N/A	$3

User subscriptions may be deployed on up to 5 devices. Additional pricing options available. Contact us here or contact your Account Manager for details.

AT&T Professional Services for configuration and training

Secure UEM Non-recurring Charge	
Basic (no Connector or Sentry)	$750
Standard (Connector Only)	$1,250
Standard Plus	$2,500
Premium	$5,000
Secure UEM Premium Non-recurring Charge	
Secure UEM Installation	$3,500
Premium Plus	$7,500

*All prices exclude applicable taxes, fees, and surcharges as well as charges for required professional services for configuration and training.

Important information

General: Each MobileIron solution as described in this product brief (the "Solution") is available only to eligible Business or government Customers with a qualified AT&T agreement ("Qualified Agreement") and a Foundation Account Number (FAN). The Solution is subject to (a) the terms and conditions found https://www.mobileiron.com/en/legal/customer_agreement (Additional Product Terms); (b) the Qualified Agreement; and (c) applicable Sales Information. Please see the service guides for additional information on service descriptions and pricing at http://serviceguidenew.att.com/sg_flashPlayerPage/MIVSP (Core) and http://serviceguidenew.att.com/sg_flashPlayerPage/MICLD (Cloud). For government Customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms.

A minimum of 20 Solution subscriptions are required for an initial MobileIron Cloud purchase. A minimum of 50 Solution subscriptions are required for initial MobileIron Core purchase. The Solution's functionality is limited to certain mobile devices and operating systems. A list of supported operating systems can be obtained by contacting an AT&T Business Account Executive. Not all features are available on all devices. All amounts paid for the Solution are non-refundable. Billing begins as of Effective Date of applicable order. User subscriptions may download licensed Software onto a maximum of 5 devices. If any user exceeds the 5-device limit per license, an additional monthly license fee will be charged.

The Solution may also be used with multiple different network service providers. The use of the Solution with AT&T wireless services requires activation of an eligible AT&T data plan on a compatible device with short message service ("SMS") capabilities. The use of the Solution with non-AT&T wireless providers requires compatible devices and SMS capabilities, and Customer is responsible for ensuring that its applicable end users and the Solution comply with all applicable terms of service of such other wireless carrier(s). All associated voice, messaging, and data usage will be subject to the applicable rates and terms of such other wireless carrier(s). Refer to applicable wireless carrier(s) for such rates, terms, and conditions.

The Solution administrative interface is accessed via a Web portal and requires a PC or laptop with internet connection. The Solution may be used as a tool to configure and customize certain settings and features and perform software updates only for compatible devices. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures.

Customer must accept the Additional Product Terms as the party liable for each authorized user (End User) and agrees in such case that the End User will comply with the obligations under the Additional Product Terms, including but not limited to the limitations of use in certain countries. Customer is responsible for providing each End User of an enabled mobile device with a copy of the Additional Product Terms. With the use of the Solution by residents of and in countries other than the U.S., Customer agrees to comply with the additional terms and conditions of use located in the Country Specific Provisions portion of the MobileIron Service Guides located at http://serviceguidenew.att.com. Not all optional features are available in every country.

Data privacy: Customer Personal Data: Customer Personal Data may be transferred to or be accessible by (i) AT&T personnel around the world; (ii) third parties who act on behalf of AT&T or AT&T supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement, or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data and End User personal data accessible when Customer has the legal authority to do so and for which it has obtained any necessary consents from its end users and will camouflage or securely encrypt such data as needed in a manner compatible with the Solution. The term, Customer Personal Data, includes, without limitation, name, phone number, email address, location information, or any other information that identifies or could reasonably be used to identify or link to Customer or its end users. Customer is responsible for providing its end users with clear notice of AT&T and the Customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising its end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the Product Brief or other sales information that describes the Solution and to AT&T Privacy Policy at http://www.att.com/gen/privacy-policy?pid=2506. Customer is responsible for notifying end users that the Solution provides unified endpoint management (UEM) capabilities and allows Customer to have full visibility and control of end users' devices, as well as content on them.

Miscellaneous. Solution software warranty and liability rights are contained in the Additional Product Terms between MobileIron and Customer. As between AT&T and the Customer, the Solution is provided "AS IS" with all faults and without warranty of any kind. AT&T HAS NO DEFENSE, SETTLEMENT, INDEMNIFICATION, OR OTHER OBLIGATION OR LIABILITY ARISING FROM THE ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY BASED ON THE SOLUTION.

AT&T reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause AT&T reserves the right to conduct work at a remote location or use, in AT&T sole discretion, employees, Contractors, or suppliers located outside the United States to perform work in connection with or in support of the Solution. **Exclusive Remedy:** Customer's sole and exclusive remedy for any damages, losses, claims, costs, and expenses arising out of or relating to use of the Solution will be termination of service.

For more information on AT&T Mobile Security Solutions, visit att.com/mobileIron.