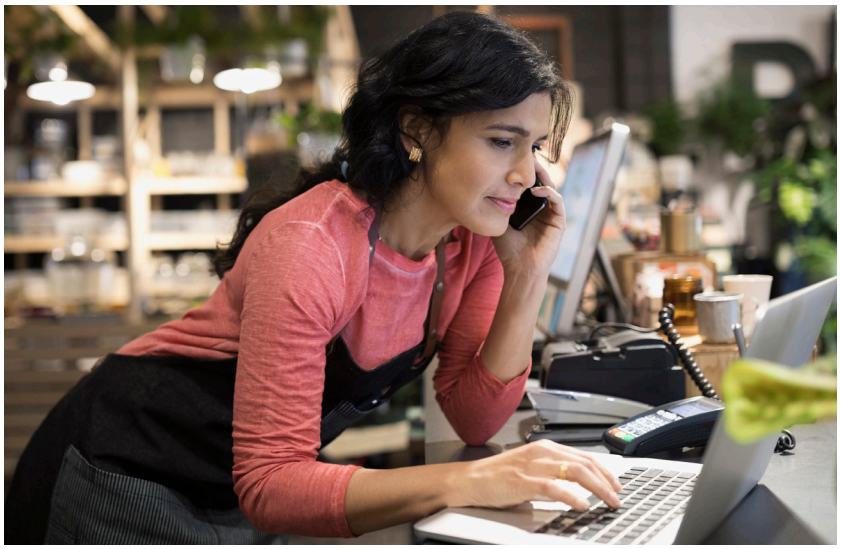
AT&T Business

Unlock the benefits of mobility to work faster, better, and smarter



MobileIron Core (the "Solution") is a highly secure mobile centric security platform which accesses and protects data across your digital workplace.

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.

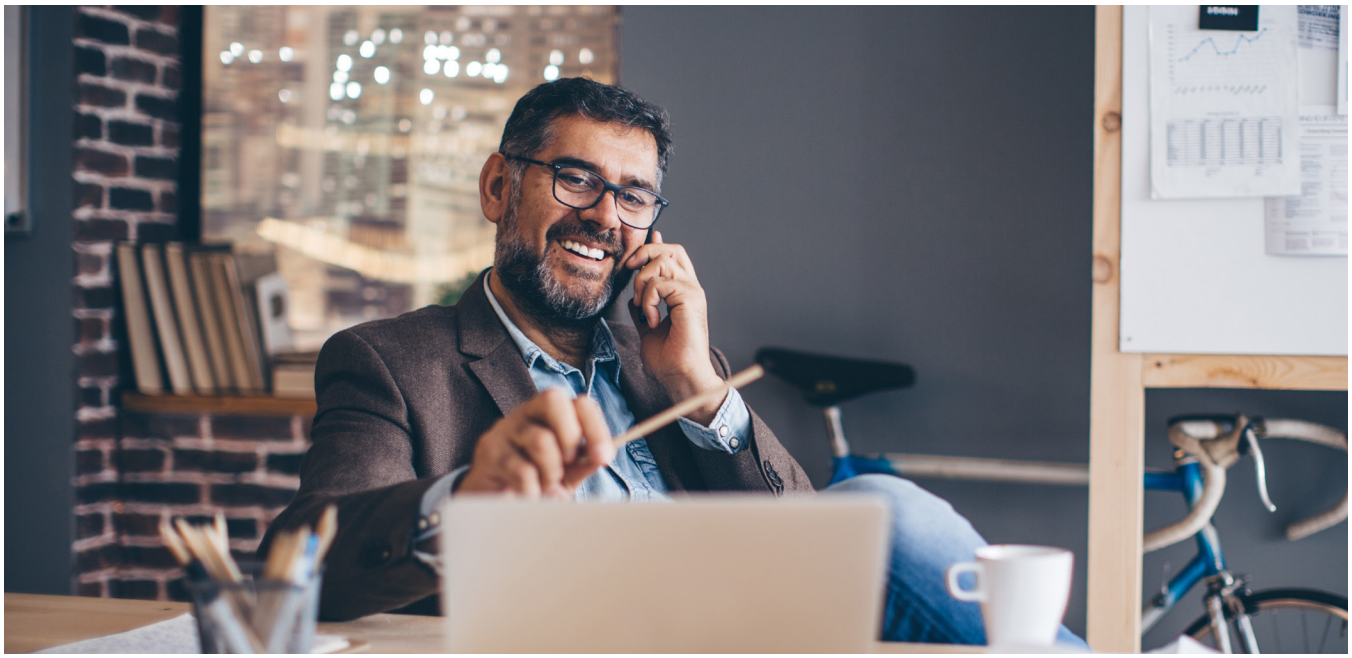
This Product Brief applies to purchases made on and after August 7, 2020. For purchases made before that date, see https://www.business.att.com/content/dam/businesscenter/pdf/mobileiron-core-product-brief.pdf.

Potential benefits

- Windows 10, iOS, and Android management available
- Multi-OS Security
- Effective data security and compliance
- Help Desk and IT reporting and efficiency

Features

- Highly secure enterprise gateway
- Highly secure applications and app-specific VPNs
- Single sign on
- Enterprise app store
- Workflow integration
- Visibility and reporting
- End-user and self-service via BYOD portal
- Zero Sign On provides conditional access to services from mobile apps and browsers
- MobileIron Threat Defense provides a view into malicious threats using one app on iOS and Android devices



Core Secure UEM bundle

The Secure UEM bundle provides all the essential capabilities required to build the foundation of a mobile-first enterprise. The Secure UEM bundle includes capabilities that allow for near-seamless device onboarding, configuration of security settings, app distribution, policy enforcement, and remediation.

Core Secure UEM Premium bundle

The Secure UEM Premium bundle is designed for organizations that have a solid mobile foundation and are ready to enter the advanced stages of the mobile-first journey. The Secure UEM Premium bundle provides additional capabilities, including a highly secure per-app VPN, Help Desk tools for remote viewing and control over end-user devices, and integrations with specific third-party products and services.

MobileIron optional add-on features

Zero Sign On (ZSO)

Zero Sign On is a cloud security Solution that provides conditional access to cloud services. It helps you keep business data within IT bounds so it can't be stored on unsecured devices, connect to unmanaged apps, or share information with unsanctioned cloud services. Installation at additional cost.

ZSO is only available for per user licenses. Secure UEM Premium is required and includes use with a single cloud application. Use with multiple applications may be purchased as an optional feature. Additional installation and configuration services may be required.

MobileIron Threat Defense

MobileIron Threat Defense protects and remediates against known and unknown threats on compatible Android and iOS mobile devices. With one app, you can detect and remediate known and zero-day attacks on the subscribed devices without disruption to users' productivity. MobileIron Threat Defense Premium includes additional reporting capability. Installation at an additional cost.

		Secure UEM	Secure UEM Premium
Core Portal	A central administrative console	•	•
Sentry	An in-line intelligent gateway that manages, encrypts, and helps secure the traffic between mobile devices and back-end enterprise systems	•	•
Apps@Work	A data-at-rest app store that can be used to house all of the Customer's public and in-house applications	•	•
AppConnect	Containerizes apps to help protect enterprise data-at-rest without touching users' personal data	•	•
Email+	A highly secure email/personal information manager (PIM) app for iOS and Android	•	•
Kiosk Mode/Apple Business Manager	In the US, Apple allows accredited businesses with a Data Universal Numbering System (DUNS) number to automatically enroll new devices purchased directly from Apple	•	•
Help@Work	Help desk tools that allow users to request help with a tap and enable IT staff to remotely view a user's screen	•	•
Bridge and Derived Credentials	Bridge unifies mobile and desktop operations for Windows using a single console. Derived Credentials is used by federal agencies so that mobile devices can access agency information without needing additional hardware		•
Docs@Work	Enables users to annotate, share and view enterprise documentation from email, file repositories and cloud file repositories		•
Web@Work	A highly secure browser that lets users access web content within the enterprise's intranet without requiring them to use a device-wide VPN		•
Tunnel	A per-app VPN for enterprise apps and data that enables mobile apps to access corporate data and content that is behind a firewall		•
ServiceConnect integrations*	ServiceNow integration to streamline IT workflows		•
Zero Sign On	A cloud security Solution that provides conditional access to cloud services for one Cloud service (included with Secure UEM Premium) or multiple mobile apps and browsers	Add on SKU. Secure UEM Premium required	
MobileIron Threat Defense Premium **	Help guard against data loss from mobile threat events		

* ServiceConnect integrations available with the Secure UEM bundle include MobileIron developed software to integrate with specific third-party products and services. API-based integrations do not require the purchase of the Secure UEM bundle.

** Add on SKU

Pricing Options

Note: MRC = monthly recurring charge; ARC = annual recurring charge. User subscriptions may be downloaded on up to 5 devices.

Subscription and pricing options	Secure UEM	Secure UEM Premium
Device subscription license	$48	$90
User subscription license	$72	$138
Device MRC license	$4	$7.50
User MRC license	$6	$11.50

Configuration and training*		
Enterprise Support configuration and training	$3,500	AT&T will provide implementation services connected with the purchase of Secure UEM MobileIron Software Licenses. The deployment will be conducted remotely in a hosted environment with the integration supported by on-premises MobileIron Connector to Active Directory in the client's data center and one Sentry.
Enterprise Support configuration and training	$7,500	AT&T will provide implementation services connected with the purchase of Secure UEM Premium MobileIron Software Licenses. The deployment will be conducted remotely in a hosted environment with the integration supported by on-premises MobileIron Connector to Active Directory in the client's data center and two Sentries.

Training topics include:

- Overview of Core architecture and features
- Device registration and retirement
- Device configuration management
- Device troubleshooting
- User management
- Policy management and security
- Application management
- Reports and logs

*Configuration and training may alternatively be purchased from MobileIron.

Feature add-on options		
Zero Sign On user – subscription	$36 ARC	$3 MRC
MobileIron Threat Defense device – subscription	$48 ARC	$4 MRC
MobileIron Threat Defense user – subscription	$72 ARC	$6 MRC
MobileIron Threat Defense Premium device – subscription	$72 ARC	$6 MRC
MobileIron Threat Defense Premium user – subscription	$108 ARC	$9 MRC

Optional professional services		
Installation of one additional MobileIron Sentry	**$500**	If you require the installation of an additional MobileIron Sentry, AT&T will install it on a server that you provide and integrate it with MobileIron Core. Customer will provision, set up, and configure any load-balancing equipment or software required to front-end the MobileIron Sentry software
MobileIron administrator training	**$1,500**	For additional training for system administrators, AT&T will coordinate a web conference for up to 10 people. This half-day training will be a mixture of slide presentation, lecture, and demonstration regarding the MobileIron virtual smartphone platform.
High availability	**$6,000**	Customers who want greater uptime can utilize the High Availability Professional Service: • Review of the Customer's existing traffic management and monitoring system required to redirect network traffic to the redundant server • Installation of a redundant server on the Customer-provided platform and one optional sentry (an existing in-service Core is required) • Installation and testing of the synchronization script between Core and the failover. Note: Customer is responsible for providing a server/appliance for the installation of the redundant server and to provide a traffic management and monitoring system to redirect network traffic to the failover. Optional hardware appliances (servers) are available only to U.S. customers as purchased equipment at an additional charge of $7,500 (lower capacity) or $25,000 (higher capacity) each.
Advanced Authentication using Certificates and Kerberos Delegation	**$1,750**	To use Certificate Authentication, the Customer's UEM server will need to be configured to issue certificates. Certificate authentication provides enterprises the ability to establish identity while eliminating the need for end users to enter usernames and passwords on their mobile devices to access enterprise resources, such as Exchange ActiveSync, VPN, and Corporate Wi-Fi. Service scope AT&T will implement and configure the integration settings to enable the MobileIron Core appliance to issue certificates to mobile devices from a supported interface to the Customer's Certificate Authority. AT&T will complete the Certificate Authority integration configuration and settings: • Create one certificate template representing the Customer's desired type of identity certificate • Define one-device policy profile for Exchange ActiveSync auto-configuration using an UEM-issued identity certificate • Define one-device policy profile for VPN client auto-configuration using anidentity certificate • Define one-device policy profile for preferred WiFi network auto-configuration using an identity certificate • Configure the service accounts in ActiveDirectory (User or Computer object) for Kerberos authentication delegation and create service principal names (SPNs) if necessary Configure the email proxy service to request Kerberos delegated credentials on behalf of device users for mailbox access AT&T will assist with the testing of each device profile on a single supported device.*

*Diagnosis and remediation of failed test cases to verify that a certificate of the correct type is issued by the Certificate Authority and installed within the device certificate store. The Customer is responsible for any diagnosis or remediation of authentication or authorization failures within the authentication, authorization and accounting (AAA) infrastructure.

For more information on AT&T Cybersecurity Mobile Endpoint Security Solutions, contact your sales representative or visit our MobileIron webpage.

Important Information:

General: MobileIron Core as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement"). The Solution is subject to (a) the terms and conditions found at https://www.mobileiron.com/en/legal/customer_agreement ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. 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. Any service discounts, equipment discounts, and/or other discounts set forth in the Qualified Agreement do not apply to the Solution. The Solution may not be available for purchase in all sales channels or in all areas. Additional hardware, software, service and/or network connection may be required to access the Solution. Availability, security, speed, timeliness, accuracy and reliability of service are not guaranteed by AT&T. Additional fees, charges, taxes and restrictions may apply.

A minimum of 50 Solution licenses is required for initial 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 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 subscription 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 is available only to Customers with a qualified AT&T business or government agreement ("Enterprise Agreement") and a Foundation Account Number ("FAN"). The Solution is available for use with multiple network service providers. Qualified Responsibility Users ("QRUs"), Individual Responsibility Users ("IRUs") and Bring Your Own Device ("BYOD") users are eligible to participate in the Solution. With respect to users subscribed to an AT&T wireless service, activation of an eligible AT&T data plan on a compatible device with short message service ("SMS") capabilities is required. With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, 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. A compatible device with SMS capabilities is required. The Solution software requires a MobileIron operating environment server or, where available, the purchase of a MobileIron appliance from AT&T. Customer is responsible for the configuration of the appropriate Domain Name System (DNS) prior to AT&T installation activities. Core integration with enterprise public key infrastructure is not included. The Solution's administrative interface is accessed via a Web portal and requires a PC 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. AT&T does not guarantee compliance with such customized settings and/or updates. Customer must accept the Additional Product Terms as the party liable for each Customer Responsibility User (CRU), and agrees in such case that the CRU will comply with the obligations under the Additional Product Terms, including but not limited to the limitations of use in certain countries. See your account representative for additional information regarding use of the Solution outside the U.S. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the Additional Product Terms. The Customer and the CRU are individually and jointly liable under the Additional Product Terms. With regard to use of the Solution by residents of 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 Core Cloud Service Guide located at https://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 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 accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt Customer Personal Data in a manner compatible with the Solution. The term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify Customer or its end users. Customer is responsible for providing end users with clear notice of AT&T and 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 end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the Product Brief or other sales information that describes the Solution and to AT&T Privacy Policy at https://www.att.com/gen/privacy-policy?pid=2506. Customer is responsible for notifying end users that the Solution provides unified endpoint (UEM) capabilities and allows Customer to have full visibility and control of end users' devices, as well as any content on them.

Professional Services: Upon completion of AT&T Professional Services, Customer must either sign the acceptance document AT&T presents or provide within five business days of the service completion date written notice to AT&T identifying any nonconforming Professional Services. If Customer fails to provide such notice, Customer is deemed to have accepted the AT&T Professional Services. Customer acknowledges that AT&T and Customer are independent contractors. Customer will in a timely manner allow AT&T access as reasonably required for the Professional Services to property and equipment that Customer controls. The Professional Services provided shall be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., Eastern time. The mandatory software installation and configuration is estimated to take two days and must be completed within 45 days of order placement. If Customer's acts or omissions cause delay of installation and user configuration beyond 45 days of order placement, AT&T will invoice Customer for the installation and configuration charges after the 45th day. If the Professional Services provided in connection with the Solution are more complex than those described in this Product Brief, then a separate statement of work describing the activity and related terms and pricing will be executed. If impediments, complications or Customer-requested changes in scope arise (Changes), the schedule, Solution and fees could be impacted. In the event any Change(s) affect the Solution or fees, the parties will modify Customer's order (or statement of work, if applicable) accordingly by executing a change order.

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.

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.