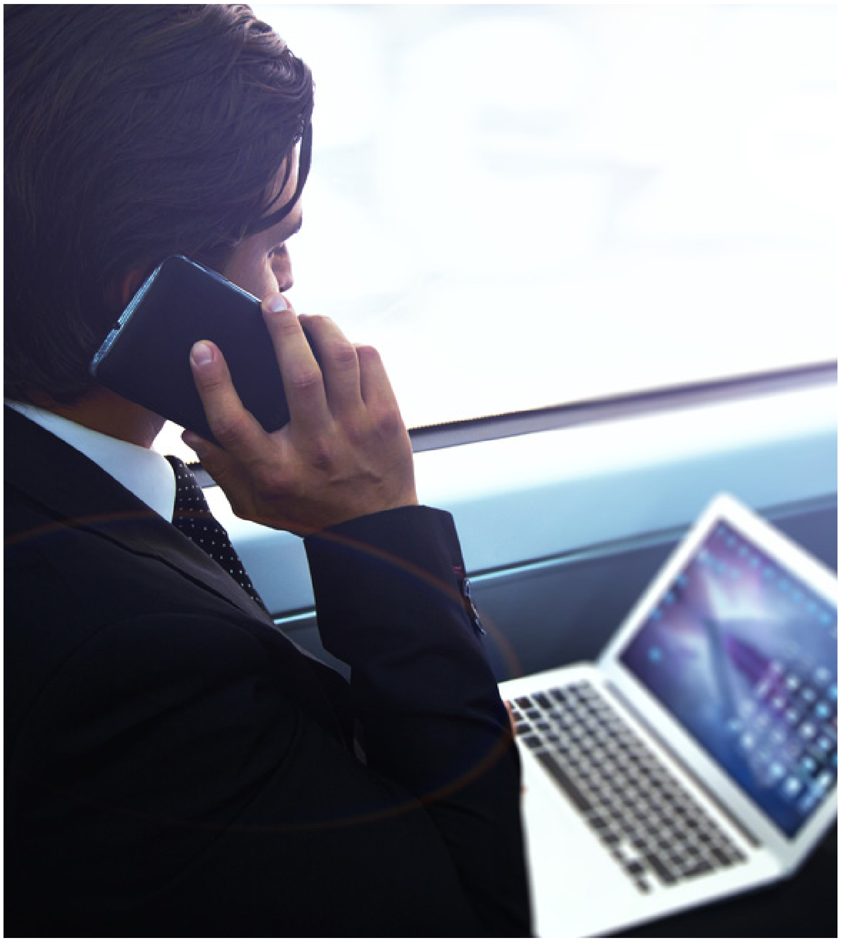
Manage your mobile device with built-in threat detection



Benefits

- Defend against phishing, network, app, and device attacks
- Add device and security policies based on each user's role
- Administer business apps based on the role and responsibilities of each user
- Install and update through a single app on the device
- Configure email, Wi-Fi, network access, passcodes, and other security policies remotely
- Wipe apps and data from the device instantly if lost or time to retire
- Detect threats even when the device is offline
- Update without user interruption

With MobileIron Blue, you don't have to choose between mobile security and mobile productivity. Now you can get world-class, enterprise-grade mobile management and security for businesses of all sizes—all in one affordable package.

We all know that cybercriminals and hackers have set their sights on mobile devices, which hold the keys to all kinds of valuable data such as credit card information, bank accounts, customer data, and more. With phishing attacks and other mobile threats on the rise, it's time for a mobile security solution that virtually anyone can use—and at a price that's friendly to the bottom line.

With MobileIron Blue, you also get cloud-based mobile threat protection that's always on and continuously updated without interrupting users. Best of all, it's fully deployed and supported by world-class support from AT&T Business, so you don't have to worry about updating complicated software on all your devices. Just activate it and go—it's really that easy.

MobileIron Blue: Features and capabilities

MobileIron Blue is an integrated bundle of MobileIron Cloud and MobileIron Threat Defense with 24X7 support from AT&T, all at one low monthly rate. MobileIron Threat Defense gives you continuous protection against phishing, malicious apps, device and network threats. MobileIron Cloud provides device management features for Android and iOS devices. That means you can quickly set up and enroll new devices with company email, passcode requirements, Wi-Fi settings, and other configurations right out of the box.

Threat defense

MobileIron Threat Defense provides continuous, on-device threat protection. It's easy to install and update through a single app, and it provides ongoing protection against threats such as phishing and malicious apps. You can rest easy knowing that Mobile Threat Defense continuously scans subscribed devices for threats and provides immediate notification and threat remediation when it detects a high level of risk.

Device management

Managing mobile devices is a challenge for companies of all sizes. The MobileIron Cloud bundle allows you to easily configure native email, apps, and device and security policies based on each user's role. The MobileIron solution supports Apple Business Manager (ABM) and Android zero-touch enrollment to help simplify device setup and policy configurations. Whichever option you choose, MobileIron Cloud enables you to deploy company devices through a central console without having to manually access each device. This not only saves you time, it gets employees up and running faster.

MobileIron Blue features

Threat defense

- Always on and integrated into one app
- Automated deployment
- Protect against known and zero-day threats
- Detect phishing, device, network, and application vulnerabilities
- Scan devices for threats
- On-device threat notification and remediation

Management

- Apple iOS and Google Android support
- Audit trails
- Enrollment program integration (ABM and Zero Touch)
- Native email configuration

Device security

- Lock, wipe, message, locate
- Passcode and restrictions
- Data loss prevention controls
- Policy compliance and automation
- Wi-Fi and VPN configuration

Apps

- Public, web and internal apps
- Encryption of applications
- Blacklisting apps (to restrict access on devices)
- App distribution and configuration

Device security

MobileIron Blue makes it easy to set up device configurations that help prevent your apps and data from falling into the wrong hands. You can remotely configure passcode requirements and other security policies. It's also easy to set up VPN and Wi-Fi configurations to provide protection for data traveling to and from company apps on subscribed devices. And if an employee leaves your company or retires a device, you can instantly wipe all business apps and company data. **App management**

MobileIron Blue also makes it easy to administer a company app store. You can deploy in-house, public, and web apps to users based on their roles and responsibilities and instantly update those apps on devices without any manual intervention. And if users changes roles, you can instantly wipe those apps from their devices.

Professional installation services – $250*

MobileIron Blue installation is simple and virtually seamless. The world class service support team from AT&T will help you set up tenant configuration policies and help provision 2 Android or iOS devices only. Basic installation includes configuring threat and remediation policies that will apply when a threat is identified.

Finally, enterprise-grade mobile management for companies of all sizes

With MobileIron Blue, companies large and small can access the same enterprise-grade mobile security and device management features thousands of global customers use. You can easily administer your internal apps as well as apps from public app stores. And, when employees leave the company or upgrade their devices, you can safely retire those devices and wipe all of your company apps and data. That makes life easier and more secure for everyone—you, your employees, and your customers.

*Additional professional services hours may be purchased for the following: Sentry, Connector, Tunneling, App Connect, LDAP, Custom policies, per App VPN, Kiosk mode, Mac or Windows devices, and Help@Work.

Important information

General: MobileIron Cloud 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 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.

A minimum of 20 Solution subscriptions are 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 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 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 a Qualified Agreement and multiple network service providers. Customer Responsibility Users ("CRUs"), 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'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 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 Cloud Service Guide 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 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's 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 http://www.att.com/gen/privacy-policy?pid=2506. Customer is responsible for notifying end users that the Solution provides mobile device management (MDM) 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 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 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., local 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 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.

Why AT&T

AT&T Business can help identify and implement the technologies you need —from one edge of your network to the other—to enhance your business.

To learn more about MobileIron Blue from AT&T, please contact your sales representative.

© 2021 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV and registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. | 294901-052521