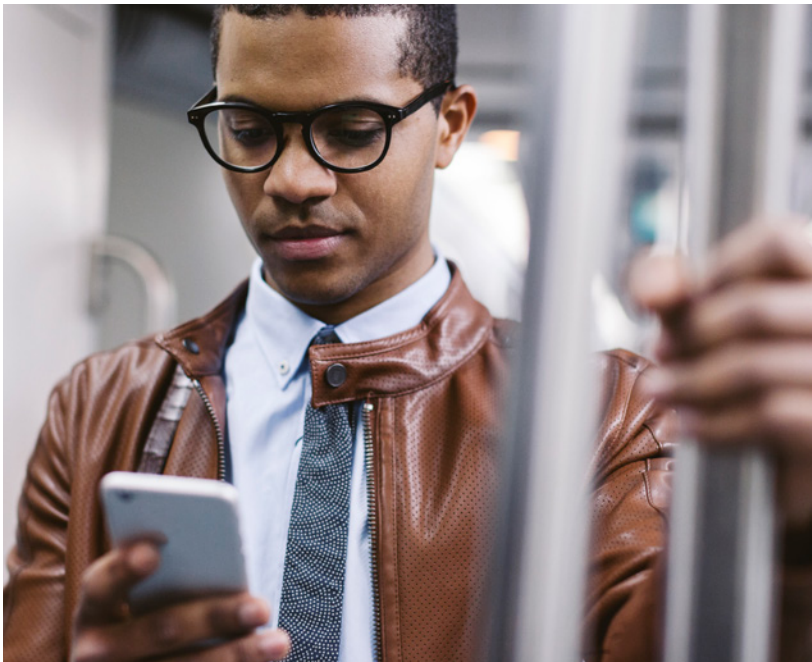


Increase the visibility of your mobile security for your workforce

IBM MaaS360 from AT&T



Business Challenges

Now, mobility is part of business strategy. It's viewed as a way to transform workflows and business processes in a very dramatic way. Companies realize the vulnerability of their data and may not have the framework to protect themselves in the following areas:

- The support of a range of usage models – corporate-owned, BYOD and shared devices
- Separating work and personal data from mobile devices
- Enforcing compliance with internal policy and industry regulations
- Providing protection for organizational data in apps and content
- Keeping pace with rapid OS and mobile platform updates

Ultimately, organizations are trying to find the right balance of maximizing productivity and amplifying data protection. IBM MaaS360 from AT&T (the “Solution”) can help to address these challenges with a comprehensive approach to Unified Endpoint Management (UEM).

Solution Overview

IBM MaaS360 from AT&T helps provide mobile enablement security for the way people work and collaborate with colleagues and agencies. The way we think of highly secure enterprise mobility is about supporting the user's expectations of being able to work while mobile and having the flexibility to use devices and apps of their choice. We do that by giving IT and security pros the capabilities they need to:

- Extend mobile to new areas of the organization and use cases
- Provide a high level of end-to-end mobile security across devices, apps, content and users
- Combine mobile management with IT tools to build and deploy mobile apps at scale
- Reduce the cost and complexity of managing mobile assets
- Help ensure compliance with policies and regulations

Features

- There are 4 different suite offerings: Essentials, Deluxe, Premier, and Enterprise

Capabilities

IBM MaaS360 from AT&T offers solutions to help manage your entire mobile device fleet, increase productivity with highly secure emails, apps and docs, reduce security and compliance risks and control your mobile IT environment. IBM MaaS360 from AT&T provides ease of use features like Over-The-Air configuration, compatibility with iOS, Android,

Windows PC and Mac OS-X, and integrates with Exchange, Office 365, AD/LDAP and Certificate Authorities. With mobile intelligence analytics, a reporting and action engine, along with near real time visibility with the MaaS360 Dashboard, you can now better control your entire mobile IT environment.

IBM MaaS360 from AT&T Products by Suites				
Feature	Essentials Suite	Deluxe Suite	Premier Suite	Enterprise Suite
Unified Endpoint Management (Smartphones, Tablets and Laptops)	•	•	•	•
Mobile Application Management	•	•	•	•
Container App	•	•	•	•
Telecom Usage	•	•	•	•
API Mgt. for W10 & OSX	•	•	•	•
App. Catalog (Win & Mac)	•	•	•	•
Patch/Updates (Win & Mac)	•	•	•	•
SW Distribution	•	•	•	•
Secure Mobile Mail		•	•	•
Secure Mobile Browser	Optional Add On	Optional Add On	•	•
Gateway for Browser			•	•
Mobile Content Management			•	•
Gateway for Documents			•	•
Mobile Application Security			•	•
Gateway for Apps			•	•
Mobile Identity Management			•	•
Mobile Document Editor				•
Mobile Document Sync				•
Mobile Threat Management	Optional Add On	Optional Add On	Optional Add On	•

Essentials Suite

Unified Endpoint Management

- Manage smartphones, tablets and laptops featuring iOS, Android, Windows and OS X. (NOTE: Windows 10 and OS X work with APIs only).
- Help enforce compliance with near real-time and automated actions

Laptop Management with software updates, device management, and an optional add on for Location Based Service, (Laptop Location Based Service may not be used in the European Union)

Mobile Application Management

- Deploy custom enterprise app catalogs
- Blacklist, whitelist and require apps
- Administer app volume purchase programs

Container App

- A separated mobile workspace for iOS, Android, and Windows
- Send contained messages to users from the Solution's portal
- Monitor telecom usage
- Monitor mobile data usage with alerts
- Set policies to restrict or limit data and voice roaming
- Review integrated reporting and analytics

Deluxe Suite

Includes everything in the Essentials Suite plus:

Secure Mobile Mail

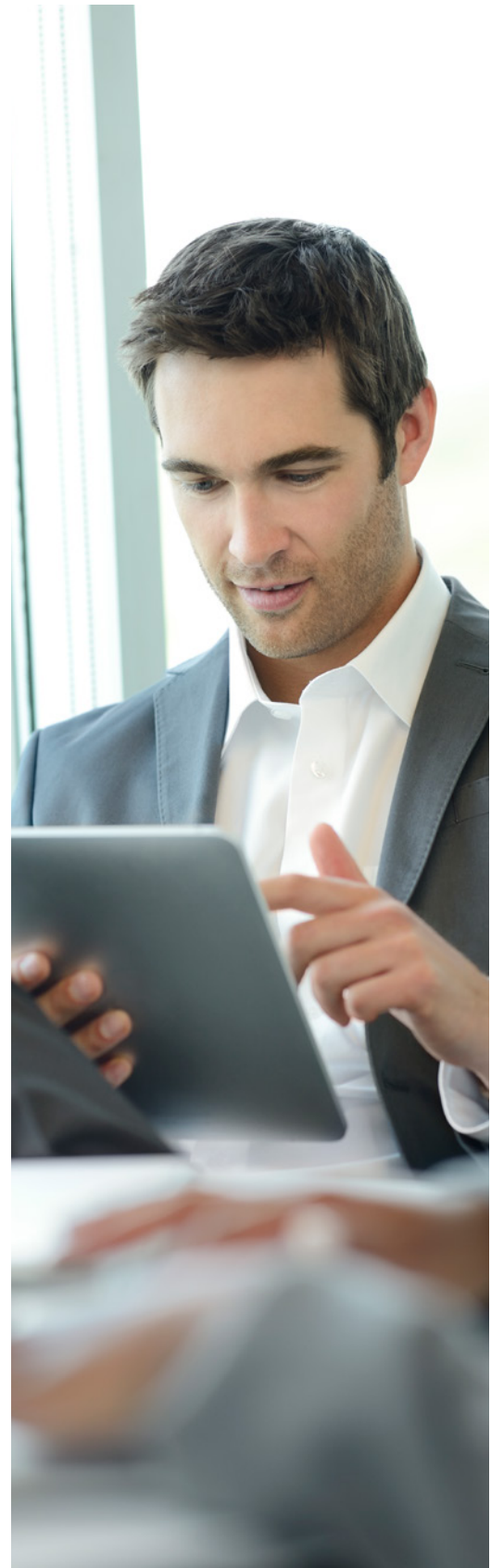
- Highly secure container for email, text and attachments to help prevent data leakage
- Enforce authentication, copy/paste and forwarding restrictions
- FIPS 140-2 compliant, AES-256 bit encryption for data at rest

Premier Suite

Includes everything in the Deluxe Suite plus:

Secure Mobile Browser

- A feature-rich web browser for highly secure access to intranet sites
- Define URL filters and security policies based on categories
- Block known malicious websites



Gateway for Browser

- Enables the Secure Mobile Browser to access enterprise intranet sites, web apps and network resources behind your firewall
- Access seamlessly and with higher security without needing a VPN session on mobile devices

Mobile Content Management

- Store documents and files in the container to help prevent data leakage
- Apply authentication, copy/paste and view-only restrictions
- Access distributed content/repositories: SharePoint, Box, Google Drive and OneDrive

Gateway for Documents

- Enhance protections for your content with highly secure access to internal files, e.g. SharePoint and Windows File Share
- Retrieve enterprise documents without a device VPN session

Mobile Application Security

- Apply authentication and copy/paste restrictions
- Limit or prevent access from compromised devices

Gateway for Apps

- Add per app VPN to Mobile Application Security to integrate behind-the-firewall data in private apps
- Incorporate enterprise data without a device VPN session

Mobile Identity Management

- Integration with Active Directory, LDAP and Azure AD for authentication, enrollment and reporting
- Single sign on to container apps, productivity tools and enterprise apps
- SAML federated authentication for the administrative portal

Enterprise Suite

Includes everything in the Premier Suite plus:

Mobile Document Editor

- Create, edit and save content in a highly secure, encrypted container
- Collaborate on Word, Excel, PowerPoint and text files
- Change fonts and insert images, tables, shapes, links and more

Mobile Document Sync

- Synchronize user content across managed devices
- Restrict copy/paste and opening of unmanaged apps
- Store content more securely, both in the cloud and on devices

Mobile Threat Management

- Detect and analyze mobile malware on compromised devices
- Automate remediation via near real-time compliance engine
- Take action on jailbroken/rooted devices over-the-air

Monthly Pricing		
Product	Price per device per month	Price per user per month
Essentials Suite	\$3.00	\$6.00
Deluxe Suite	\$5.00	\$10.00
Premier Suite	\$6.25	\$12.50
Enterprise Suite	\$9.00	\$18.00

Annual Pricing		
Product	Price per device per year	Price per user per year
Essentials Suite	\$36.00	\$72.00
Deluxe Suite	\$60.00	\$120.00
Premier Suite	\$75.00	\$150.00
Enterprise Suite	\$108.00	\$216.00

Mobility Professional Services Offers

Basic Configuration and Training (\$500) – Required with purchase of Essentials Suite. AT&T will remotely provide implementation services associated with the purchase of Solution subscriptions. Does not include implementation of Cloud Extender or any components on customer premises.

Basic Plus Configuration and Training (\$1,500) – Required with purchase the Essentials Suite with the Cloud Extender. The Cloud Enterprise Extender provides the ability to integrate with enterprise systems such as Microsoft Exchange, Microsoft Office 365, and Active Directory/ LDAP in a highly secure manner. Includes associated implementation services.

Premium Configuration and Training (\$2,000) – Required with purchase of Deluxe Suite. AT&T will provide implementation services conducted in a supplier hosted environment. The hosted instance will leverage a Cloud Extender server installed in the Customer’s environment to integrate with its enterprise directory and corporate email environment.

Premium Plus Configuration and Training Services (\$2,500) – Required with purchase of Premier and Enterprise Suites. AT&T will provide implementation services in a supplier hosted environment. The hosted instance will use a Cloud Extender server installed in the Customer’s environment to integrate with its enterprise directory and corporate email environment as well as a Mobile Enterprise Gateway for highly secure access.

General: IBM MaaS360 from AT&T 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 of the IBM Cloud Services Agreement (“CSA”) located at <https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/us-en/10>; the IBM MaaS360 Service Description located at <https://www-03.ibm.com/software/sla/slabnfs/sla/sd-6741-21>; and the End User License Agreement found at <https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/us-en/10> and <https://www-03.ibm.com/software/sla/slabnfs/sla/sd-6741-21> (collectively, the “Additional Product Terms”). 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. Except for government customers, Customer must accept the Additional Product Terms on behalf of its end users and be responsible for their use of the Solution. 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.

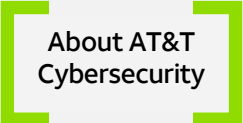
Technical Information: The Solution may only be purchased by Customers in the United States. A minimum of 20 licenses is required for initial purchase. The Solution is available for use with multiple network service providers and its functionality is limited to certain mobile devices and operating systems. A list of the compatible devices and operating systems is available by contacting an AT&T Account Executive. For users subscribed to AT&T wireless service, activation of an eligible AT&T data plan with short message service (“SMS”) capabilities is required. For 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. The Solution includes an application (App) that is downloaded to devices from a third party. A compatible device with SMS capabilities is required. The Solution’s administrative interface is accessed via a Web portal and requires a browser 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 may not use the Solution if failure of the Solution could lead to death, bodily injury, or property or environmental damage. Customer is responsible to assess the suitability of the Solution for its intended use and Content and to take necessary actions to order, enable, or use available data protection features appropriate for the Content being used with the Solution. By using the Solution, Customer accepts responsibility for use of the Solution, and acknowledges that it meets Customer’s requirements and processing instructions to enable compliance with applicable laws. The App may only be used in connection with the Solution.

Reservations: 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 perform work at a remote location or use, in AT&T’s sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution. 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 may not use the Solution if failure of the Solution could lead to death, bodily injury, or property or environmental damage. Customer is responsible to assess the suitability of the Solution for its intended use and Content and to take necessary actions to order, enable, or use available data protection features appropriate for the Content being used with the Solution. By using the Solution, Customer accepts responsibility for use of the Solution, and acknowledges that it meets Customer’s requirements and processing instructions to enable compliance with applicable laws. The App may only be used in connection with the Solution. To the extent not in conflict with the Qualified Agreement or applicable law Customer’s sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service.

Data Privacy: Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world; (ii) third parties who act on AT&T’s or AT&T’s 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. As used herein, 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's Privacy Policy at <https://about.att.com/csr/home/privacy.html>. 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 any content on them. Customer acknowledges that Laptop Location Service may not be used in the European Union.

Content: Content consists of all data, software, and information that Customer or its authorized users provides, authorizes access to, or inputs to the Solution. Customer is responsible for obtaining all necessary rights and permissions to enable, and grants such rights and permissions to, AT&T, its suppliers and their affiliates, and contractors to use, provide, store and otherwise process Content in the Solution. This includes Customer making necessary disclosures and obtaining consent, if required, before providing individuals' information, including personal or other regulated data in such Content. If any Content could be subject to governmental regulation or may require security measures beyond those specified by AT&T and its suppliers for the Solution, Customer will not input, provide, or allow such Content unless specifically permitted in writing by AT&T to implement additional security and other measures.



**About AT&T
Cybersecurity**

AT&T Cybersecurity's enterprise-grade technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning — helping to enable our customers around the globe to anticipate and act on threats to protect their business.