Increase the Visibility of Your Mobile Security

IBM MaaS360 (formerly IBM MobileFirst Protect)

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. Businesses realize the vulnerability of corporate 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
- Complying with internal policy and industry regulations
- Protecting corporate 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 can help to address these challenges with a comprehensive approach to Enterprise Mobility Management (EMM).

Solution Overview

IBM MaaS360 delivers mobile enablement security for the way people work and collaborate with colleagues and customers. The way we think of security for 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

IBM Maas360 Products by Suite

Feature	Management Suite	Productivity Suite	Content Suite	Gateway Suite	Laptop Management
Mobile Device Management	Included				
Mobile Expense Management	Included				
Mobile Application Management	Included	Included			
Content Service	Included	Included	Included		
Secure Mobile Mail		Included			
Secure Mobile Browser		Included			
Mobile Application Security (container)		Included			
Mobile Content Management			Included		
Mobile Document Editor			Included		
Mobile Document Sync			Included		
Gateway for Documents				Included	
Gateway for Browser				Included	
Gateway for Apps (tunnel apps)				Included	
Laptop Lifecycle					Included
Laptop Location					Included
Mobile Threat Management	Optional				

The Management Suite OR Productivity Suite must be purchased as base suites before any other suite can be added.

To learn more about AT&T Mobile Device Management solutions, visit www.att.com/mdm or have us contact you.

Share this with your peers

- Provide highly secure end-to-end mobile access 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

Capabilities

IBM MaaS360 offers solutions to manage your entire mobile device fleet, increase productivity with highly secure emails, app & docs, reduce security & compliance risks and control your entire mobile IT environment. IBM MaaS360 provides ease of use like Over-The-Air configuration, is compatible with iOS, Android, Windows Phone, Windows PC and Mac OS-X and integrates with Exchange, Lotus Notes, Office 365, AD/LDAP and Certificate Authorities. With Mobility Intelligence™ analytics, a reporting & action engine, along with complete, real time visibility with MaaS360 Dashboard, you can now control your entire mobile IT environment.

Features

There are 5 different suite offerings; Management Suite, Productivity Suite, Content Suite, Gateway Suite, and Laptop Management. *The Management Suite or the Productivity Suite must be purchased before any other suite or feature can be added.*

Management Suite

Mobile Device Management

- Manage smartphones and tablets using iOS, Android, Windows Phone and BlackBerry
- Gain complete visibility of devices, security & network
- Enforce compliance with real-time & automated actions

Mobile Application Management

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

Mobile Expense Management

- Monitor mobile data usage with real-time alerts
- Set policies to restrict or limit data & voice roaming
- Review integrated reporting and analytics

Content Service

- Host and distribute corporate documents and apps with a globally optimized distribution network

Mobile Threat Management (optional)

- Proactively manage mobile threats in real time
- Reduce risk of sensitive data leakage of corporate and personal information
- Take automated actions to reduce and mitigate risk

Productivity Suite

Mobile Application Management

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

Secure Mobile Mail

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

Secure Mobile Browser

- Enable highly secure access to intranet sites & web apps w/o VPN
- Define URL filters based on categories & whitelisted sites
- Restrict cookies, downloads, copy/paste & print features

Mobile Application Security

- Containerize enterprise apps with a simple app wrapper or SDK
- Enforce authentication & copy/paste restrictions
- Prevent access from compromised devices

Content Service

- Host and distribute corporate documents and apps with a globally optimized distribution network

Content Suite

Mobile Content Management

- Containerize documents & files to help prevent data leakage
- Enforce authentication, copy/paste & view-only restrictions
- Access IBM MaaS360 distributed content & repositories such as SharePoint, Box & Google Drive

Mobile Document Editor

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

Mobile Document Sync

- Synchronize user content across managed devices
- Restrict copy/paste & opening in unmanaged apps
- Highly secure storage for content, both in the cloud & on devices

Content Service

- Host and distribute corporate documents and apps with a globally optimized distribution network

To learn more about AT&T Mobile Device Management solutions, visit www.att.com/mdm or have us contact you.

Share this with your peers

Gateway Suite

Gateway for Browser

- Enable MaaS360 Secure Browser to access enterprise intranet sites, web apps & network resources
- Access seamlessly with high security without needing a VPN session on mobile devices

Gateway for Documents

- Enhance MaaS360 Content with highly secure access to internal files, e.g. SharePoint & Windows File Share
- Retrieve enterprise documents without a device VPN session

Gateway for Apps

- Add per app VPN to MaaS360 Application Security to integrate behind-the-firewall data in private apps
- Incorporate enterprise data without a device VPN session

Laptop Management

Laptop Lifecycle

- Take control of devices over the air: lock, shut down, restart, distribute software
- Provide real-time security alerts and reports
- Supports Microsoft Windows PC and Mac OSX devices

Laptop Location

- Locate devices in real-time
- View location history

Mobility Professional Services Offers

Basic Configuration and Training

(Required with purchase of either IBM MaaS360 Management Suite or IBM MaaS360 Productivity Suite without the Cloud Extender configured – IBM MaaS360 (MaaS360) Cloud Extender provides the ability to integrate with enterprise systems such as Microsoft Exchange, Microsoft Office 365, Active Directory/LDAP, Lotus Traveler, and Certificate Authorities) in a highly secure manner. AT&T will provide implementation services associated with the purchase of IBM MaaS360 Software Licenses and Hosting. The deployment will be conducted in an IBM MaaS360 hosted environment. This project is conducted in one meeting conducted remotely.

Basic Plus Configuration and Training

(Required with purchase of either IBM MaaS360 Management Suite or IBM MaaS360 Productivity Suite with the Cloud Extender configured) IBM MaaS360 Cloud Extender enables highly secure integration with enterprise systems such as Microsoft Exchange, Microsoft Office 365, Active Directory/LDAP, Lotus Traveler, and Certificate Authorities.

AT&T will provide implementation services associated with the purchase of IBM MaaS360 Software Licenses and Hosting. The deployment will be conducted in an IBM MaaS360 hosted environment. This hosted instance will leverage an IBM MaaS360 "Cloud Extender" Server installed in the Customer's environment to integrate with the Customer's Enterprise Directory. This project includes a total of three meetings, all conducted remotely unless agreed upon by all parties.

Premium Configuration and Training

(Required with purchase of IBM MaaS360 Management Suite and IBM MaaS360 Productivity Suite. You do not need to also purchase Basic or Basic Plus). AT&T will provide implementation services associated with the purchase of IBM MaaS360 Software Licenses and Hosting. The deployment will be conducted in an IBM MaaS360 hosted environment. This hosted instance will leverage an IBM MaaS360 "Cloud Extender" Server installed in the Customer's environment to integrate with the Customer's Enterprise directory and corporate E-mail environment. This project includes a total of four meetings, all conducted remotely unless agreed upon by all parties.

Premium Plus Configuration and Training Services

(Note: Order with IBM MaaS360 Content Suite and/or Gateway Suite. Premium Plus Configuration also includes the configuration of IBM MaaS360 Management Suite and the IBM MaaS360 Productivity Suite. You do not need to also purchase Basic, Basic Plus, or Premium, as they are included with Premium Plus). AT&T will provide implementation services associated with the purchase of IBM MaaS360 Software Licenses and Hosting. The deployment will be conducted in an IBM MaaS360 hosted environment. This hosted instance will leverage an IBM MaaS360 "Cloud Extender" Server installed in the Customer's environment to integrate with the Customer's Enterprise directory and corporate E-mail environment as well a Mobile Enterprise Gateway for highly secure access to internal corporate file shares and intranet sites. This project includes a total of four meetings, all conducted remotely unless agreed upon by all parties.

IBM's commitment to mobile is unmatched in the industry. IBM has 6,000 mobile experts and has secured more than 4,300 patents in mobile, social and security, which have been incorporated into IBM MobileFirst solutions, that enable enterprise clients to radically streamline and accelerate mobile adoption and help organizations engage more people and capture new markets.

Proof Points

- IBM named a Gartner Magic Quadrant Leader in Enterprise Mobility Management for past 4 years
- According to Gartner, IBM's "mature shared-processing multitenant architecture is the best-in-class cloud among ranked EMM vendors. It can support thousands of installations per day for large accounts."
- In Gartner's Critical Capabilities report, IBM is ranked #1 in key customer use cases such as SaaS Deployments and Unified Endpoint Management
- Only EMM vendor to have earned FISMA certification, FEDRamp controls and SOC 2 Type II certification

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/mdm.

To learn more about AT&T Mobile Device Management solutions, visit www.att.com/mdm or have us contact you.

Important Information and Additional Terms

A minimum of 20 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 fees paid for the Solution are non-refundable. Users may download licensed Software onto a maximum of 3 devices. If any user exceeds the 3 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. Both Corporate Responsibility Users ("CRUs") and Individual Responsibility Users ("IRUs") 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 With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, Customer is responsible for ensuring that Customer, its applicable end users and the Solution complies 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.

The Solution is subject to the terms and conditions of the applicable Enterprise Agreement between AT&T and Customer and the Cloud Services Agreement (CSA) located at https://portal.fiberlink.com/eula?channelName=fbl-dpte&serviceKey=SK_DPTE_MDM_C. Customer must agree to the terms of the CSA before its first use of the Solution. If Customer does not accept the terms of the CSA, Customer must not use the Solution. Customer's end users must accept the IBM End User License Agreement ("EULA") located at bit.ly/Fiberlink-EULA-2014. Customer must accept the EULA as the party liable for each CRU, and agrees in such case that the CRU will comply with the obligations under the EULA, 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 US. Customer and the CRU are individually and jointly liable under the EULA. Customer shall not permit any IRU or BYOD user to register as a user of the Solution unless it uses the procedures provided by AT&T to obtain and preserve proof that the IRU or BYOD user has accepted the EULA. Upon reasonable request from AT&T, Customer shall permit AT&T to review Customer's records of users' acceptances. Customer shall indemnify and hold harmless AT&T against all claims by any IRU or BYOD user relating to or arising from such IRU's or BYOD user's use of the Solution if the IRU or BYOD user has not accepted the EULA. With regard to use of the Solution by residents of countries other than the US, Customer agrees to comply with the additional terms and conditions of use located in the Country Specific Provisions portion of the IBM Maas360 Service Guide located at http://serviceguidenew.att.com/. Not all optional features are available in every country. The Solution is provided "AS IS" with all faults and without warranty of any kind. AT&T DISCLAIMS ALL REMEDIES FOR CLAIMS OF INFRINGEMENT BY A THIRD PARTY BASED UPON OR ARISING OUT OF CUSTOMER'S OR END USERS' USE OF THE SOLUTION.

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 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. 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 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.

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's 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. AT&T will not provide technical support to end users and will not provide technical support for the applications and/or content that Customer chooses to distribute and which are not included in the Solution's feature list. Customer shall not instruct end users to call AT&T Customer Care at 611 or any other carrier's customer care center in connection with end users' use of the Solution.

To learn more about AT&T Mobile Device Management solutions, visit www.att.com/mdm or have us contact you.

02/29/16 AB-3109-02