IBM MaaS360 Mobile Application Management

Simply deploy, manage and secure mobile apps

Key benefits

- Protect enterprise apps with containerization
- Increase employee productivity and satisfaction
- Centrally manage mobile apps with web-based console
- Safely support BYOD
- Reduce risk of sensitive data leakage
- Enforce on-device access control and compliance with policies and regulations
- Perform selective wipe of app catalog and managed apps
- Use granular administrative controls and interactive, graphical reports
- Reduce network load and increase app performance and scalability

Provide protected access to apps

Smartphones and tablets are transforming businesses by increasing productivity, improving efficiencies and enhancing customer satisfaction. However, the proliferation of mobile devices can't be left unchecked without securing sensitive enterprise data, especially in this bring your own device (BYOD) era.

It's no longer just about controlling email and managing devices. Mobile apps are unleashing the true potential of mobile devices.

However, mobile apps are increasingly sources of corporate security vulnerabilities due to poor data storage practices, malware, unauthorized access, lack of encryption, and data leaks from synching.

There are over a million distinct mobile apps available for your employees to install and use on their smartphones and tablets.[1]

Enterprises need the power to distribute, manage and secure mobile apps critical to their business on both personal and corporate-owned devices.

IBM® MaaS360® Mobile Application Management simplifies mobile application management by delivering an intuitive enterprise app catalog with robust security and operational lifecycle management of apps.

"By 2017, 25 percent of enterprises will have an enterprise app store for managing corporate-sanctioned apps on PCs and mobile devices"[2] – Gartner

Enterprise application catalog

- Provide an intuitive, customizable enterprise app catalog for iOS, Android and Windows Phone devices
- Deliver an exceptional user experience
- Instantly help enable users to view available apps, install apps and be alerted to update apps
- Distribute a selection of public and enterprise apps
- Use a protected, web-based console for managing and distributing apps

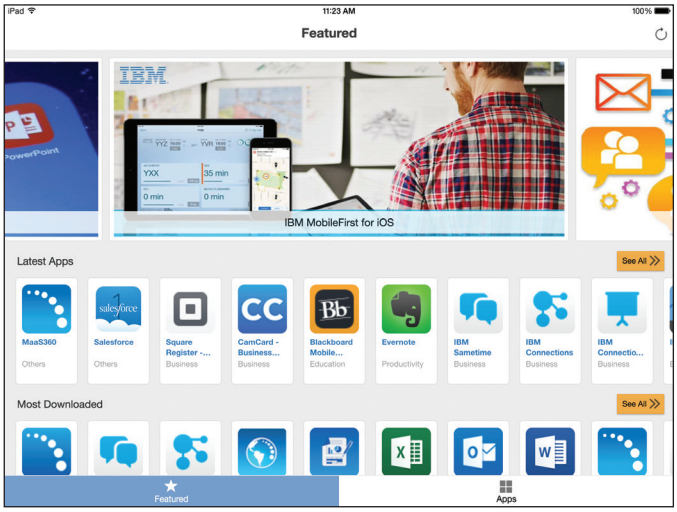

Figure 1: Example of an enterprise app catalog on a mobile device

Mobile application lifecycle management

- Use best practice mobile app management workflows
- Distribute apps and track their installation over-the-air (OTA) to all users, groups of users or individual devices
- Publish app updates
- Reference continuous app inventory reports
- Integration with public app stores such as the Apple App Store, Google Play and Windows Phone Store for seamless workflows.

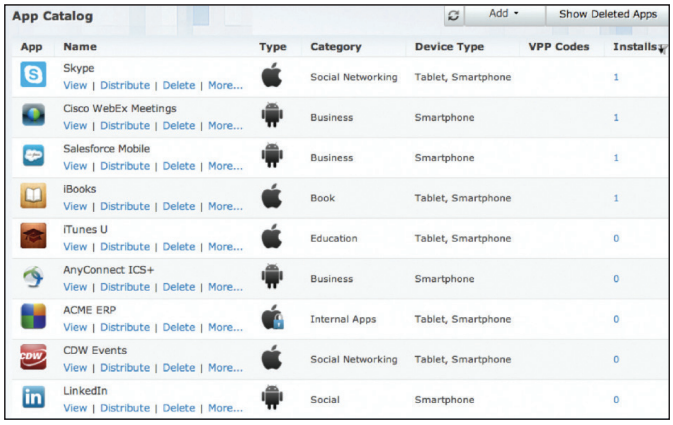

Figure 2: Example of an app catalog in the MaaS360 portal

IBM® MaaS360® Mobile Application Security

- Use a simple app wrapper or Software Development Kit (SDK) as a security add-on to MaaS360 Mobile Application Management
- Authenticate users before accessing apps
- Enforce device compliance checks
- Restrict copy and paste, as well as local and cloud data backups
- Receive near real-time alerts of compliance violations
- App-level tunneling for protected access to corporate data without needing a device VPN

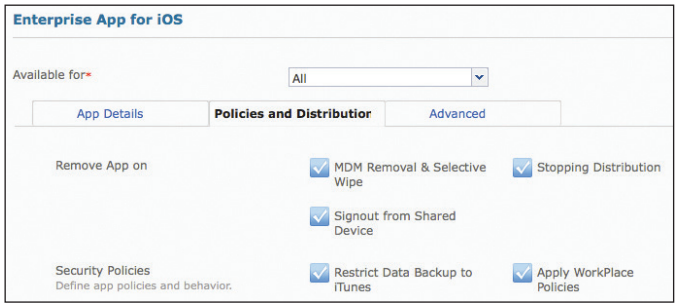

Figure 3: Example of security options that can be set for an app

Mobile app compliance and enforcement

- Blacklist, whitelist and set required apps
- Limit native apps on a device (e.g., YouTube)
- Restrict access for jailbroken or rooted devices
- Configure automated compliance enforcement actions
- Take instant action through automation or manual intervention to block email access, restrict network resources (e.g., no VPN) and perform a remote wipe
- View graphical reports of security and compliance history

Figure 4: Example showing how an app can be blacklisted so it cannot be installed on a device

Enterprise mobile app container

MaaS360 Mobile Application Management simplifies mobile application management by delivering an easy-to-use enterprise app catalog with robust security and operational lifecycle management of apps.

Enterprise application catalog

An intuitive, customizable enterprise app catalog for iOS, Android and Windows Phone.

Mobile application lifecycle management

A platform to distribute, update, manage and protect both public and enterprise mobile apps.

MaaS360 Mobile Application Security

A mobile application container for enterprise apps with built-in security management as an optional add-on to MaaS360 Mobile Application Management.

Mobile application compliance and enforcement

Security policies to blacklist, whitelist and require apps. Automated enforcement rules to alert administrators, block email, restrict network resources and perform remote wipes.

IBM® MaaS360® Content Service

An option to host and distribute your enterprise mobile apps on a globally optimized app distribution network.

Volume purchase program

Support for bulk app licenses for employees.

To learn more about IBM Security fraud-prevention solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on the specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM product and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle

1 Number of apps available in leading app stores as of July 2014, Statista, http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

2 "*Gartner Says That by 2017, 25 Percent of Enterprises Will Have an Enterprise App Store*," Gartner Group Press Release, February 12, 2013, http://www.gartner.com/newsroom/id/2334015

WGD03060-USEN-01