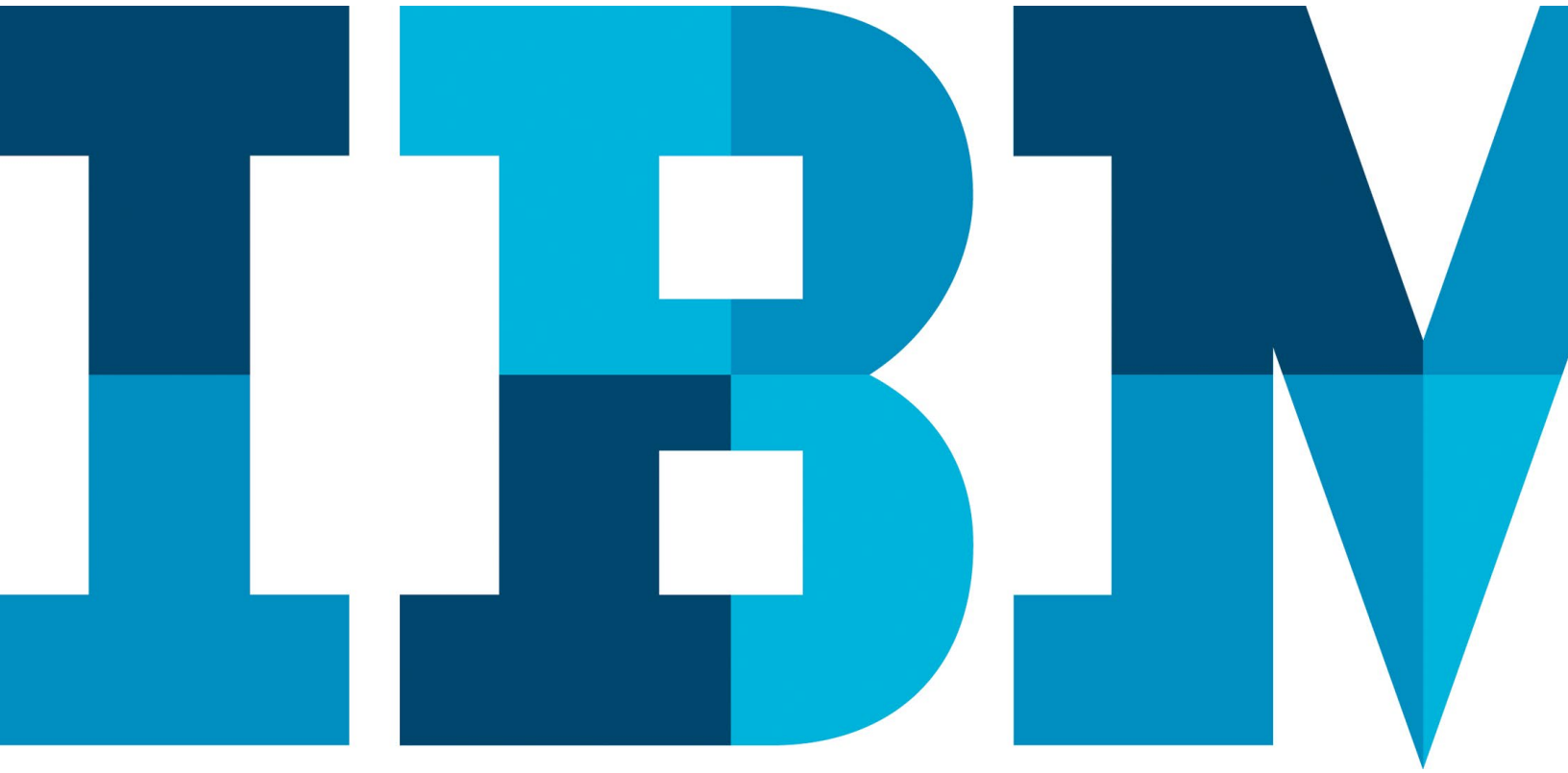
Security
Thought Leadership White Paper

January 2016

Securing mobile productivity for Microsoft Office 365

IBM MaaS360 enables you to deploy Microsoft tools with robust security across all mobile platforms



IBM

Introduction

From smartphones and tablets to laptops and wearable devices, today's enterprises are awash in mobile technology. Some of the technology is employee-owned—and may even be part of an official "bring-your-own-device" (BYOD) initiative—while the rest is company-issued equipment, but the distinction doesn't really matter when it comes to security. IT organizations must manage and secure all of the devices that access corporate data, applications (or "apps") and content.

Despite the security challenges, encouraging employee use of mobile devices is smart for the modern enterprise because it increases both productivity and overall satisfaction. In a survey of business and IT professionals, 67 percent of respondents said they were significantly more productive when using their own mobile device for work-related activities.[1] The key is for IT organizations to walk the middle ground of helping ensure that these employees can be productive, while also deploying the right technology to help reduce risk.

For years, Microsoft products have been widely used for business productivity, so the need to deploy and secure them on mobile devices is an urgent requirement. IBM® MaaS360® empowers IT organizations to manage and secure the ecosystem of Microsoft business products within heterogeneous mobile environments. The broad range of product support includes Microsoft Office 365, Microsoft Office for mobile devices, Microsoft Lync and Microsoft Skype for Business, among others.

This white paper explains why IBM MaaS360 is the right choice for deploying and securing the Microsoft ecosystem across all mobile platforms, including Microsoft Windows 10. The focus is on enabling IT to efficiently manage enterprise productivity, connectivity and security in the mobile world of today and tomorrow.

Work safely in Office 365

Today's organizations are deploying a broad range of mobile apps to help employees get their work done anytime, anywhere. And increasingly, Office 365 is their choice for productivity software, built around the Office platform. In fact, Microsoft says that the cloud-based productivity suite is used monthly by nearly 50 million business users.[2]

Office 365 offers baseline security settings for controlling mobile access to enterprise apps. But the reality is that Office 365 is typically not deployed in isolation; IT teams need to be able to secure and manage mobile devices, apps and content within a cross-platform environment. They need the flexibility to manage all types of mobile devices, both employee- and company-owned, from a single console. And they need to be able to enforce security standards without controlling the actual device.

What is Office 365?

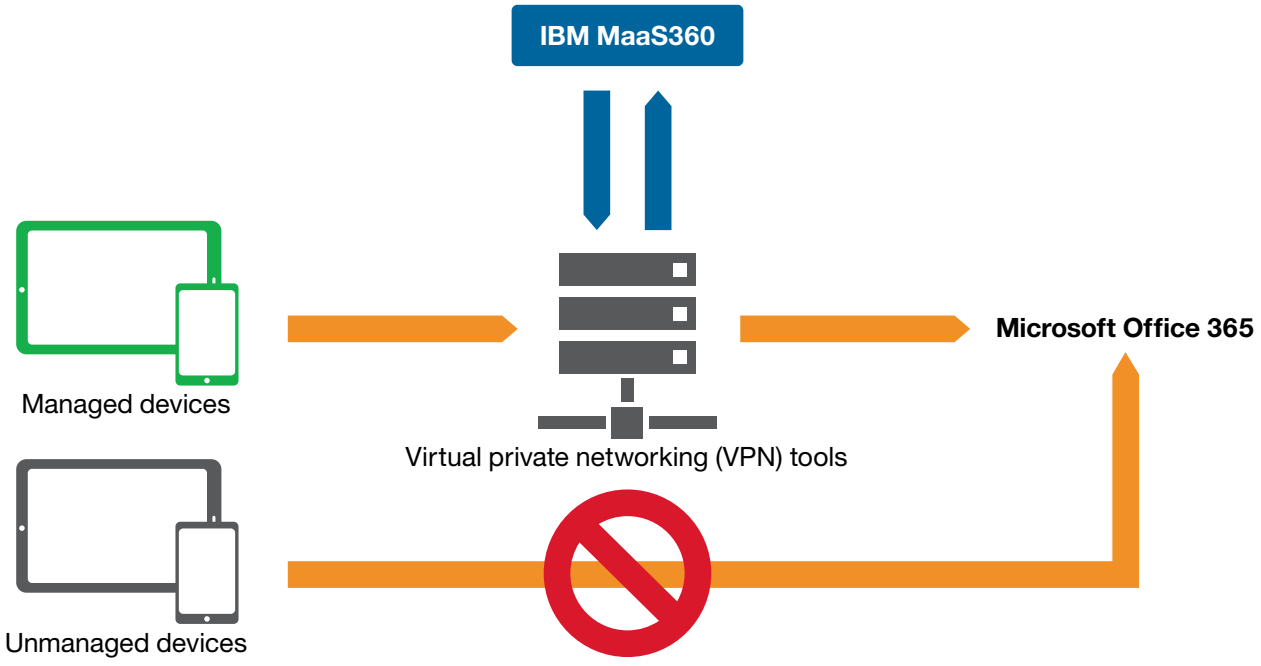
Office 365 is a Microsoft productivity solution that offers subscription-based access to Office apps, as well as other cloud services such as Skype for Business web conferencing, Microsoft SharePoint collaboration services, Microsoft OneDrive for storage and Microsoft Exchange Online hosted email.

Many Office 365 plans include the latest Office applications, such as: Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneNote, and Microsoft Outlook, all of which can be installed across multiple devices, including PCs, Macs, Google Android tablets and phones, and Apple iPads and iPhones. The suite also includes Microsoft Publisher and Microsoft Access, which are available for PCs only.

IBM MaaS360 enables organizations to keep devices and content safe with advanced mobile device management. IT teams can block access to corporate data from jailbroken and rooted devices, locate lost or stolen devices, disallow unsafe apps, and provide advanced capabilities to manage mobile devices accessing corporate data on Office 365. With cloud-based support for Office 365, IBM MaaS360 delivers the essential security features needed to protect sensitive corporate data on mobile devices, including:

- Over-the-air configuration of Office 365 profiles
- Support for multiple mobile operating systems and devices for BYOD
- Email access control of devices trying to access Office 365
- Automatic quarantine of new or unknown devices, until they are approved by IT
- Conditional access to Office 365 only from managed devices
- The ability to blacklist unsafe apps
- Restrictions on using "Open In" controls on Apple iOS devices, helping to prevent unauthorized apps from opening Office 365 documents and "leaking" data
- Location-based services for tracking lost or stolen devices
- Automated compliance and policy enforcement
- Selective wipes for removing only work-related content, including Office 365 apps and data, without compromising employee privacy or personal data
- Secure access to Microsoft OneDrive for Business folders

Conditional access to Microsoft Office 365 with IBM MaaS360



IBM MaaS360 helps ensure that only authorized devices are able to access Office 365. The devices must be managed by the IT department—and in compliance.

IBM MaaS360 is especially well suited for organizations that need stringent security policy and compliance controls, such as those in the highly regulated healthcare and financial services industries. Its *containerization* features help separate corporate data (in this case, Office 365 data) from other data on the mobile device, while also helping mitigate the risk of unauthorized apps on the device accessing that sensitive data.

Mobile email requires a different approach

Employees love to use email on their mobile devices, but its use can open the door to security threats and corporate data leaks. To help secure mobile access to corporate email from Microsoft Exchange or Office 365, IBM MaaS360 delivers a trusted workplace app designed to keep an employee's work emails, calendar, contacts and app data separate from personal data and apps. This IBM secure container app:

- **Protects email text and attachments on iOS, Android and Microsoft Windows Phone devices**
- **Provides Federal Information Processing Standard (FIPS) 140-2 compliant, Advanced Encryption Standard (AES) 256-bit encryption for data at rest**
- **Enforces authentication, cut-and-paste restrictions and view-only mode**
- **Restricts forwarding, moving and screen captures**
- **Conducts online and offline compliance checks before email access is granted**

Secure mobile content in Office

Many organizations opt to have layers of Microsoft deployment, which help reduce licensing fees and simplify operations. For example, they may deploy Office 365 for power users who need a full suite of productivity tools, while providing mobile-friendly Office apps to the rest of the user population for occasional work with documents.

In such an environment, IBM MaaS360 enables IT organizations to manage and secure Office apps for mobile users—across iOS, Android and Windows Phone devices. From a single console, administrators can manage everything from device enrollment to security policies, monitoring, app and document distribution, and help desk support. They can create robust policies to help ensure BYOD security and privacy. And it all can happen without compromising the end-user experience.

To be productive anytime, anywhere, users want to be able to view, create, edit and print Word, Excel and PowerPoint documents using their mobile device. Many times, these documents are sent as attachments from within their work email. However, working with attachments on mobile devices has traditionally been cumbersome and fraught with security risks.

IBM MaaS360 makes it easy to deploy apps to all users, a group of users or a specific device—all from a central app catalog.

IBM MaaS360 helps remove barriers to secure mobile productivity, empowering IT organizations to:

- Help prevent data leaks by managing "Open In" controls on iOS devices
- Extend storage access (beyond OneDrive or Microsoft SharePoint Online) to other file repositories, such as IBM Connections, Microsoft SharePoint On-Premises, Microsoft Windows File Shares, Box, Google Drive and Content Management Interoperability Services (CMIS) systems
- Provide access to internal repositories without needing a device-level virtual private network (VPN)
- Support secure emailing of documents with IBM MaaS360 Secure Mail
- Deliver a high-fidelity editing experience with IBM MaaS360 Document Editor, including:
  - Support for all platforms and form factors, including iOS, Android and Windows Phone
  - Support for multiple file types beyond Office formats, such as PDF documents
  - Comprehensive data leak prevention with restrictions on copying or pasting content and moving files
- Deploy automated compliance and policy enforcement
- Enable selective wipes for removing only work-related content, including Office documents, without compromising employee privacy or personal data

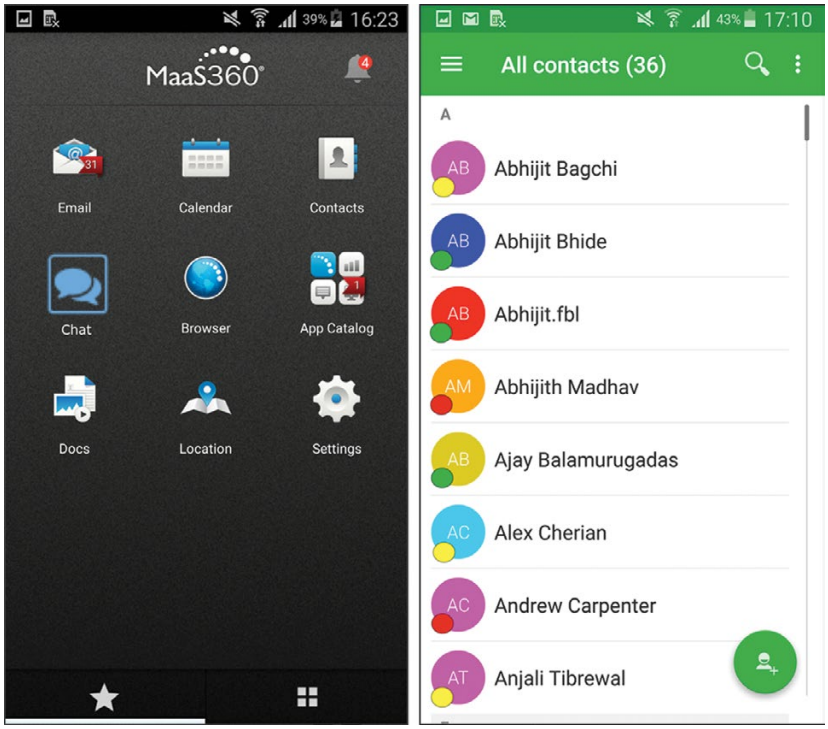
Connect teams with Skype for Business and Microsoft Lync

Real-time collaboration is an essential part of getting work done. That's why many organizations are deploying Skype for Business (formerly known as Microsoft Lync) to provide a unified communications experience. From within their Office apps, employees can collaborate using instant messaging (IM), screen shares, phone calls or video chat. They can schedule meetings and see IM history in Outlook, and start meetings from apps such as Word or PowerPoint for faster results.

However, just as with Office 365 and Office for mobile devices, IT teams need to be able to manage and secure the use of Skype for Business. They need to help ensure that employee devices are compliant with corporate security policies, manage chat notifications and prevent data leakage.

IBM MaaS360 provides granular control of Skype for Business chat features, so IT and security personnel can:

- Enforce policies for authentication, group chats, conversation history and file sharing
- Support secure chat features, such as the ability to see user presence, manage notifications and start a chat, from within IBM MaaS360 Secure Mail
- Integrate with existing infrastructure using IBM MaaS360 Cloud Extender, including:
  - Support for advanced authentication via Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), certificate authorities and Security Assertion Markup Language (SAML)
  - Comprehensive data leak prevention with restrictions on copying or pasting content and moving files
- Deploy automated compliance and policy enforcement
- Selectively wipe devices to remove only work-related content, including Skype for Business configurations, without compromising employee privacy



IBM MaaS360 enables secure, real-time collaboration and displays the presence of users.

Integrated security across the Microsoft ecosystem

Over the years, IBM MaaS360 has evolved to support the Microsoft ecosystem of business products, enabling organizations to manage and secure content and apps on mobile devices. Other key Microsoft integrations include:

- Exchange ActiveSync—Securing email access from mobile devices, including automatic quarantines of unknown devices, policy enforcement and remote wipe support
- SharePoint On-Premises—Enabling collaboration via public and private SharePoint sites, while securing content with authorization, encryption and containerization policies
- Windows File Shares—Helping protect access to network folders from within a secure, encrypted container
- OneDrive for Business—Providing a secure container to access, store, synchronize and share work files from a managed device
- Windows laptops, desktops and tablets—Supporting Windows PC lifecycle management from within the same interface used for other mobile devices, including Windows XP, Windows Vista, Windows 7, Windows 8+ and Windows 10
- Windows Phone and Windows Mobile—Delivering visibility and control of Windows Phone 7, Windows Phone 8+ and Windows 10 Mobile devices, including policy enforcement, application management and compliance reporting
- Active Directory—Integrating Active Directory information to be used for mobile device management, streamlining device authentication and group management

Conclusion

Organizations of all sizes are using BYOD programs to boost productivity and employee satisfaction, while IT teams are left with the challenge of how to ensure data security, compliance and governance. IBM MaaS360 takes the complexity out of managing the mobile workforce—from supporting a large number of smartphones and tablets across multiple mobile OS platforms, to high-volume app and document distribution.

What's more, IBM MaaS360 provides a comprehensive platform for managing and securing the Microsoft ecosystem of business products. With real-time visibility, continuous monitoring and automated policy enforcement, IBM MaaS360 is the fast way to enable mobile security for Office 365, Office for mobile devices, Microsoft Lync and Skype for Business. To manage mobility demands into the next generation of BYOD, IBM MaaS360 is an excellent choice.

For more information

To learn more about IBM MaaS360, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/security/mobile/maas360.html

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

© Copyright IBM Corporation 2016

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
January 2016

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Cloud Extender and MaaS360 are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

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 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.

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle

[1] "Making BYOD work: Balancing productivity and security," *Harvard Business Review Analytic Services Report*, *sponsored by Verizon Wireless*, October 2014. https://hbr.org/resources/pdfs/comm/verizon/18918_HBR_Verizon_BYOD_OCT_2014.pdf

[2] Julie Bort, "Here's more proof that companies are jumping on Microsoft Office 365 like crazy," *Business Insider*, April 24, 2015. http://www.businessinsider.com/chart-shows-the-rise-of-office-365-2015-4

WGW03197-USEN-00