IBM Security
Thought Leadership White Paper

Mobilize your corporate content and apps

Enable simple and protected mobile collaboration for business

Mobile strategy for a new era

Q: Do you have a robust mobile strategy?

A: Mobile strategy? You mean, can our employees get access to email on their mobile device? Sure, we have that.

If this is your answer, you're not alone. Many companies still rely on email as the "app of choice" that enables employees to communicate outside of the office. And this was a huge win even just a couple of years ago. However, let's face it, checking email and responding outside of the office is not exactly "working" so much as removing a few obstacles, moving things along, and keeping up appearances. In today's world, mobile collaboration has so much more potential to unlock true productivity and facilitate real work in near real-time, but many companies have only scratched the surface and have yet to embrace, plan, and deploy a robust mobile strategy that harnesses the power of mobility with simple, protected access to business resources.

In this document we will discuss how continuous monitoring can be applied to laptops, desktop computers and other endpoint devices.

In this white paper, you will learn how to:

- Enable protected mobile access to corporate data without an on-device VPN
- Mobilize SharePoint, Windows File Share and all your intranet sites
- Protect sensitive corporate data with robust security policies and DLP controls
- Provide mobile access without requiring changes to your network or firewall security configuration
- Allow users to collaborate on-the-go from their personal devices

Read on to learn more about how you can give your employees access to resources behind the firewall while safeguarding your data with authorization, encryption and containerization policies.

Simple access with security

Here's a simple challenge: Build a perfectly safe house that can protect all of your priceless valuables. How do you approach it? You could build a house with no windows and no doors – no entry or exit points at all. This would probably be perfectly safe, but not very useful for actual living. Or, you could build it with windows and doors that have top-notch locks and security systems protecting them, and effectively have the same level of security, but still be able to enter, exit, welcome visitors, and get some fresh air without risking the loss of your precious belongings.

Your mobile strategy might be just like a house with no windows or doors. Or, it might be like a house with windows and doors that don't lock at all. You're charged with protecting your corporate content, but you also have to make it available to users so they can be productive. From customer contact lists to patient data, financial information to Human Resources files, from corporate apps to board minutes – the information your constituents want to access grows daily, and blocking access is no longer a feasible option. You need some windows and doors – and a security system that helps ensure only those who should be allowed through them can get in.

What happens if a user brings a personal smartphone or tablet to work and downloads sales contacts to the device? What if they email their proprietary financial reports to their home email address so they can work in the evening after their children are asleep? What about a vendor? You want to share your content and apps so you can collaborate more efficiently, but what happens when the project is over?

These scenarios happen daily. People find ways to get the information they need, putting corporate information at risk, unless you facilitate a more secure, reliable and simple way for them to get what they need.

Content considerations

Enterprise content is stored on corporate networks in places like Windows file shares, SharePoint, intranet sites and web apps. The information people need to collaborate with colleagues, partners, and customers to do their jobs is trapped in internal drives and data stores, knowledge bases, internal wikis, ERP, SCM, HRM, CRM, and other management systems or processes.

So the question becomes, how do you build on that for the modern mobile worker who needs on-the-go access – many times from devices that you do not own?

As you protect your data and the internal networks, file shares, and other systems that house it, you may want to think about the following considerations as part of your mobile strategy. Some may seem obvious, but they are worth noting.

1. Content must be accessible by users on demand through a push or pull approach
2. Each user must have access only to the content needed, based on context and identity
3. Data must be updateable and synchronized across devices over time
4. The process of accessing the data must not be onerous for the user
5. Maintaining security must not be costly, although it is a big investment
6. Maintaining security must not be time consuming for IT
7. Data in motion must be encrypted and protected
8. Data must not be permitted to leave the organization without authorization
9. Data created and stored in apps must be safeguarded
10. Because personal devices are not owned by the organization, there is a limit to what you can control

One of the most important goals of any federal cybersecurity legislation must be to enable the defenders to act as quickly to protect their systems as the attackers can act.

Current technologies

Let's take a look at the technologies being used today, and some of the issues inherent with enabling security and productivity.

Email

Email is the app of choice for collaboration, but it's just one tool among many.

It's not designed for collaboration. Email supports one-to-one or one-to-many communication instead of the many-to-many interactions your users need to be truly productive. This encourages silos to develop between groups that should be working together.

Emailed information can easily get stale – people get a spreadsheet and continue to work with it, not realizing it has been superseded by something more current.

The biggest problem is that data can be cut, pasted and forwarded to places you don't want it to go.

VPN

Logging on with a VPN is a common choice to provide access behind a firewall.

Unfortunately, forcing users to log in for access degrades the user experience. Given a choice between fresh content that's harder to access and easy-to-reach stale content that comes from old email attachments, people may choose the simpler route.

VPNs require per-device licenses so your costs can mount up over time. In addition, there's evidence that using a device VPN can drain the device's battery more quickly.

Because mobile devices use wireless technology to connect, you will want to require encryption. However, there's the question of access while roaming. Typically, solutions that rely on higher-level encryption have the potential to break when users roam between access points. Fortunately, there are some solutions that address that.

Desktop virtualization

Some applications allow you to display a desktop on mobile devices. All the items accessible from the desktop would be available on your smartphone or tablet, too. However, it's generally expensive and the user experience can be poor. With this approach, availability and performance is heavily dependent on network connectivity. Also, screen size and resolution issues pose another challenge, especially on smartphones which have small displays and workspaces. Applications optimized for a desktop environment may be accessible on a mobile device via desktop virtualization, but that doesn't mean they're necessarily usable.

Another consideration IT has to take into account is that server and network resources must be able to support numerous devices connecting into their network at the same time.

Third-party file shares

Third-party file shares allow you to keep collateral in the cloud. One of the big problems here is that you have no control. Content can be sent to anyone, can be accessed by anyone, and you can have version control issues.

There's a user experience issue here, too. Users don't like to be forced to learn new software just to get access to the content they need, and you have to factor in the time it will take them to learn it.

Third-party file shares can also be costly: as you add users you will need to add licenses, plus you may not be able to use your existing investments like apps and content stores.

Third-party and custom apps

If you go to a third-party developer for your apps, you are dependent on your vendor. Data leak prevention (DLP) may not be built into the app.

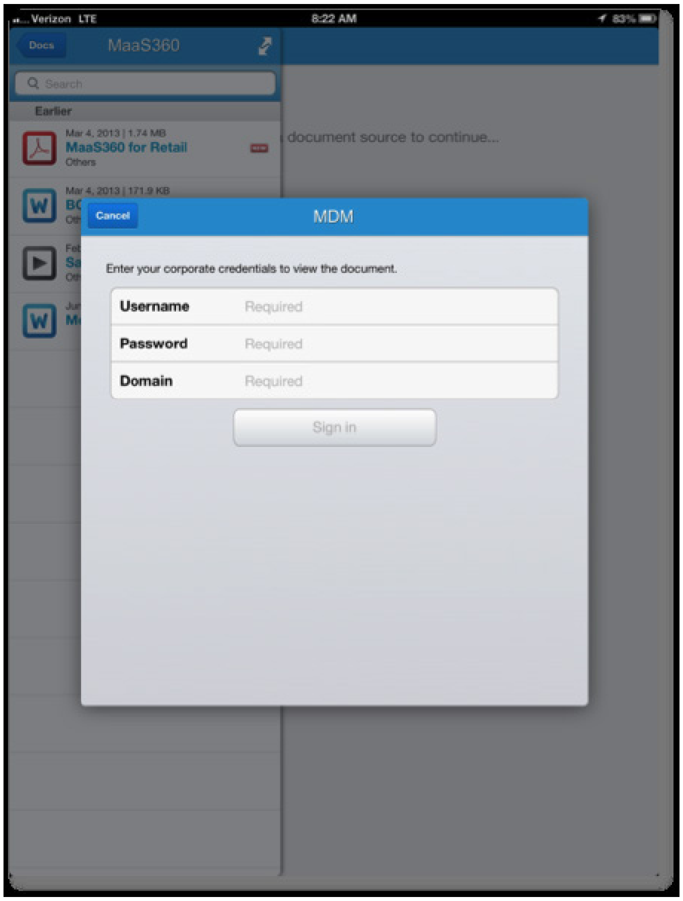
You can try to develop your own apps, but then you'll need staff to support it and any changes that are required for new devices types, operating system updates, etc.

Many security experts, top federal government cybersecurity officials, and Congressional leaders are pushing for an increased emphasis on continuous monitoring, automated monitoring tools, and rapid reaction to attacks on government information technology systems.

The importance of policies

If you intend to allow users to access corporate resources on their personal devices, you will need to create policies to regulate how your data is accessed and used.

You can require a user to enter a password before accessing important data.



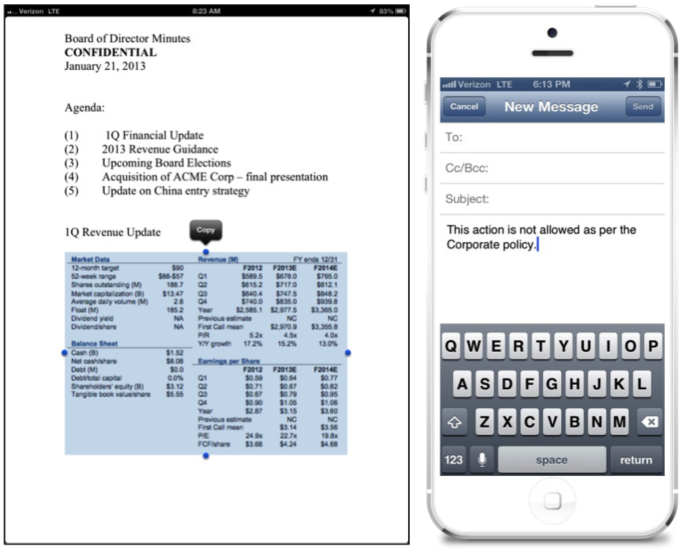
Enter your corporate credentials to view the document.

Username	Required
Password	Required
Domain	Required

Sign in

Figure 1: An authentication request

You can also restrict cutting and pasting text from a document.



Board of Director Minutes
CONFIDENTIAL
January 21, 2013

Agenda:

(1) 1Q Financial Update
(2) 2013 Revenue Guidance
(3) Upcoming Board Elections
(4) Acquisition of ACME Corp – final presentation
(5) Update on China entry strategy

1Q Revenue Update

Market Data	
12-month target	$90
52-week range	$88-$57
Shares outstanding (M)	188.7
Market capitalization (B)	$13.47
Average daily volume (M)	2.8
Float (M)	185.2
Dividend yield	NA
Dividend/share	NA

Balance Sheet	
Cash (B)	$1.52
Net cash/share	$8.08
Debt (M)	$0.0
Debt/total capital	0.0%
Shareholders' equity (B)	$3.12
Tangible book value/share	$5.55

Revenue (M)			FY ends 12/31
	F2012	F2013E	F2014E
Q1	$589.5	$678.0	$765.0
Q2	$615.2	$717.0	$812.1
Q3	$640.4	$747.5	$848.2
Q4	$740.0	$835.0	$939.8
Year	$2,585.1	$2,977.5	$3,365.0
Previous estimate		NC	NC
First Call mean		$2,970.9	$3,355.8
P/R	5.2x	4.5x	4.0x
Y/Y growth	17.2%	15.2%	13.0%

Earnings per Share			
	F2012	F2013E	F2014E
Q1	$0.59	$0.64	$0.77
Q2	$0.71	$0.67	$0.82
Q3	$0.67	$0.79	$0.95
Q4	$0.90	$1.05	$1.06
Year	$2.87	$3.15	$3.60
Previous estimate		NC	NC
First Call mean		$3.14	$3.56
P/E	24.9x	22.7x	19.8x
FCF/share	$3.68	$4.24	$4.68

To:
Cc/Bcc:
Subject:

This action is not allowed as per the Corporate policy.

Figure 2: Data leak prevention controls such as copy and paste restrictions

IBM® MaaS360® Productivity Suite

MaaS360 Productivity Suite helps you overcome challenges posed by the current technologies and is designed with multiple ways of allowing secure access and protecting your data at rest:

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360 uses a container for a dual persona approach – data, apps and content that are company-specific stay in a protected area on the device. You determine the controls placed on that protected area so mail, contacts, calendars, apps (and app data), documents and web page access can be safeguarded.

Figure 3: MaaS360 Productivity Suite and MaaS360 Content Suite

MaaS360 Productivity Suite uses persona policies to specify security on all a user's devices. These policies are created in the MaaS360 portal and deployed to enrolled devices over the air, so IT doesn't have to physically touch the devices.

When the device falls out of compliance, or the project is over and the vendor leaves, you just remove the container remotely and the data and apps are gone.

The container has security built in. It includes FIPS 140-2 compliant, AES-256 encryption. You can require users to enter a passcode when accessing it. You can also use these policy settings to remove the container completely if devices are jailbroken or rooted, or if the devices haven't checked in within a specified period of time.

You can also prevent files from being moved, copied or printed from the container, and you can prevent files from being imported into it.

IBM® MaaS360® Content Suite

MaaS360 Content Suite provides an encrypted container and productivity tools to distribute, view, create, edit and share documents on mobile devices, giving organizations the control they need and employees the access they demand:

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

MaaS360 Mobile Content Management delivers a mobile document container for content collaboration with a robust set of lifecycle management capabilities to distribute, update, manage and safeguard documents. IT administrators can enforce authentication, copy/paste and view-only restrictions. Users can access corporate-distributed content and file repositories such as SharePoint, Box and Google Drive.

MaaS360 Mobile Document Editor is designed to prevent corporate data leaks while allowing users to create, edit and save. Users can collaborate on Word, Excel, PowerPoint and text files on mobile devices while on-the-go.

MaaS360 Mobile Document Sync enables users to easily synchronize content across managed mobile devices to continue creating or editing their files without interruption. IT can apply policies to content such as restricting copy/paste and blocking opening or sharing in unmanaged apps. These controls can be applied to all documents, a group of documents or individual documents, giving you the flexibility you need to safeguard precious corporate data.

The use cases for protected content sharing are numerous in virtually every organization, whether in Sales, Marketing, Operations or Finance:

- View and share last minute changes to a sales presentation on-the-go, right before a customer meeting
- Collaborate on the latest financials in a spreadsheet before boarding a plane

- Brainstorm marketing messages and share with colleagues while in a cafe
- Distribute quarterly financial documents to the Board of Directors, and set the document to expire after the meeting
- Share product materials in near real-time to sales teams so they don't need to scramble to find the latest data sheet or competitive information
- Make sure tablets in retail stores have the most up-to-date product and inventory information

IBM® MaaS360® Gateway Suite

MaaS360 Gateway Suite is a key component to help make all of this possible. It protects data in motion by providing seamless and protected access to your corporate content and intranet from mobile devices:

- Deliver simple, protected mobile access to data without an on-device VPN; you don't need to sign on to the VPN each time you want information
- Mobilize SharePoint, Windows File Shares, intranet sites and web apps
- Protect data with robust security policies and DLP controls
- No changes to your network or firewall security settings are required

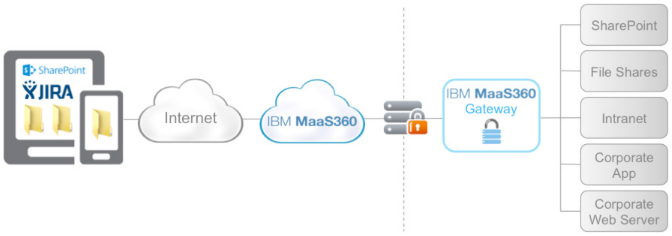


Figure 4: Data flows with MaaS360 Gateway

You can configure policy options to manage how MaaS360 Productivity Suite interacts with your users' devices. For example, you can specify URLs to corporate wikis, bug tracking systems, etc., or corporate folders accessible via MaaS360 Gateway, and they will appear as bookmarks in MaaS360 Secure Mobile Browser. You can also specify if authentication is required to access these locations.

MaaS360 Gateway determines what corporate resources users will see when they access the data container on their devices.

Try before you buy

MaaS360 is easy and fast to try – plus the time you invest in configuring MaaS360 for your needs is time well spent. Once you decide that MaaS360 is the right solution for your organization, your trial environment becomes your live environment!

For a no cost trial of MaaS360, please click here. You can start right away – there's no complicated set up process or infrastructure to change. Try MaaS360 today!

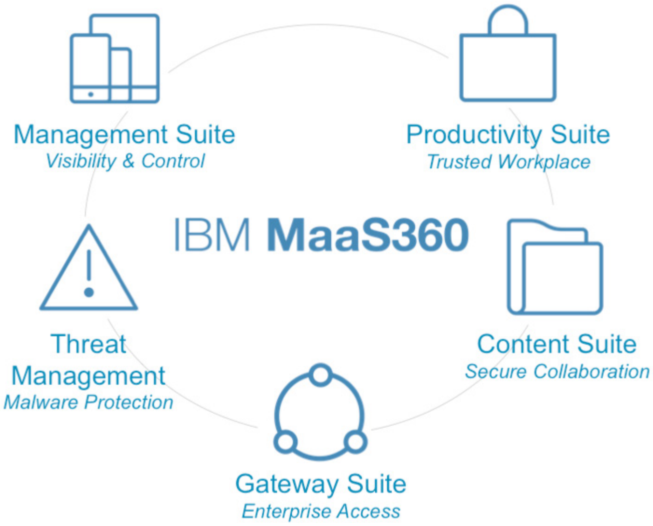


Figure 5: MaaS360 products

About IBM MaaS360

IBM MaaS360 is the enterprise mobility management platform to enable productivity and data protection for the way people work. Thousands of organizations trust MaaS360 as the foundation for their mobility initiatives. MaaS360 delivers comprehensive management with strong security controls across users, devices, apps and content to support any mobile deployment. For more information on IBM MaaS360, and to start a no cost 30-day trial, visit www.ibm.com/maas360

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, MaaS360 Productivity Suite™, MaaS360® Secure Mobile Mail, MaaS360® Mobile Document Sync, MaaS360® Mobile Document Editor, and MaaS360® Content Suite, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company. 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

Microsoft, Windows, Windows NT, and the Windows logo 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 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