



Total Enterprise Mobility

Presented by Wlodek Dymaczewski, IBM

Wlodek Dymaczewski | dymaczewski@pl.ibm.com | www.maas360.com

Top Enterprise Mobility Initiatives



Embrace Bring Your Own Device (BYOD)



Migrate from BlackBerry to multi-OS



Deploy public and enterprise apps

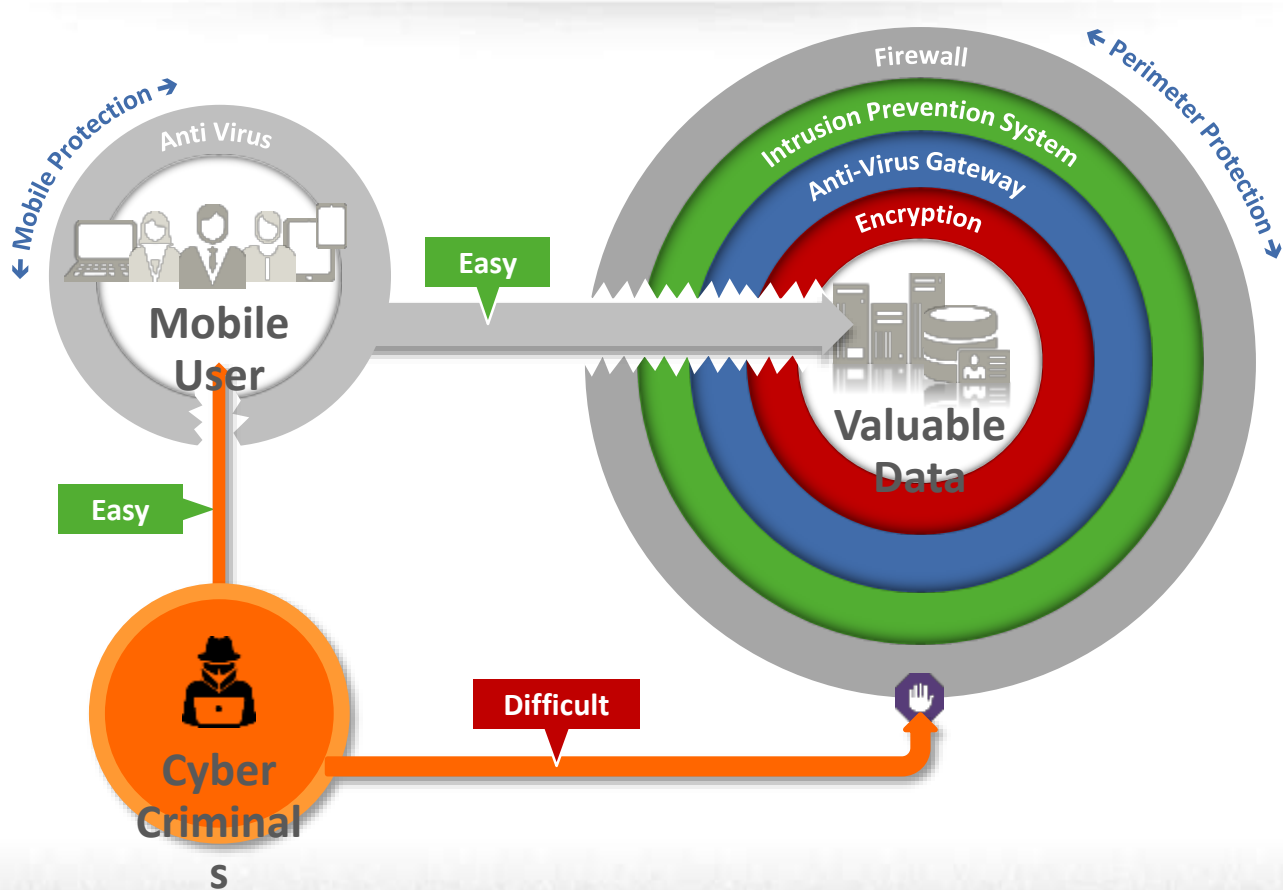


Provide access to work content



Protect sensitive corporate data

Why Mobile Security Is So Important



IBM Multi-layer Mobile Security Strategy



Device Security	Content Security	Application Security	Transaction Security
<ul style="list-style-type: none"> • Enroll, provision and configure devices, settings and mobile policy • Fingerprint devices with a unique and persistent mobile device ID • Remotely Locate, Lock and Wipe lost or stolen devices • Enforce device security compliance: passcode, encryption, jailbreak / root detection 	<ul style="list-style-type: none"> • Restrict copy, paste and share • Integration with Connections, SharePoint, Box, Google Drive, Windows File Share • Secure access to corporate mail, calendar and contacts • Secure access to corporate intranet sites and network 	<p>Software Development Lifecycle</p> <ul style="list-style-type: none"> • Integrated Development Environment • iOS / Android Static Scanning <p>Application Protection</p> <ul style="list-style-type: none"> • App Wrapping or SDK <i>Container</i> • Hardening & Tamper Resistance <i>IBM Business Partner (Arxan)</i> • Run-time Risk Detection <i>Malware, Jailbreak / Root, Device ID, and Location</i> • Whitelist / Blacklist Applications 	<p>Access</p> <ul style="list-style-type: none"> • Mobile Access Management • Identity Federation • API Connectivity <p>Transactions</p> <ul style="list-style-type: none"> • Mobile Fraud Risk Detection • Cross-channel Fraud Detection • Browser Security / URL Filtering • IP Velocity

Security Intelligence

Advanced threat detection with greater visibility

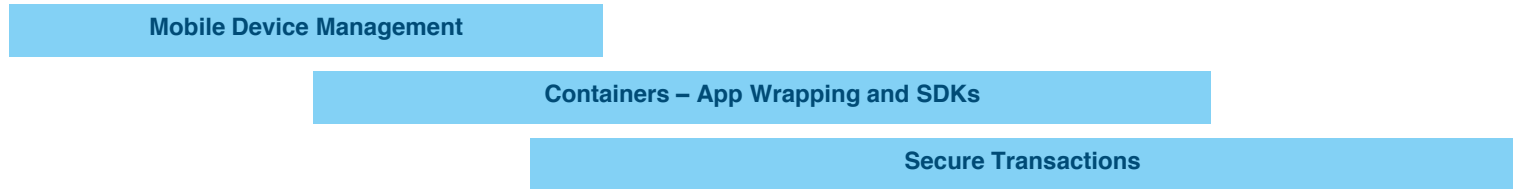


IBM Mobile Management and Security Solution

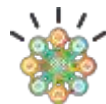
Requirements for Mobile Management and Security:



Solution Approaches:



IBM / Fiberlink Offerings:

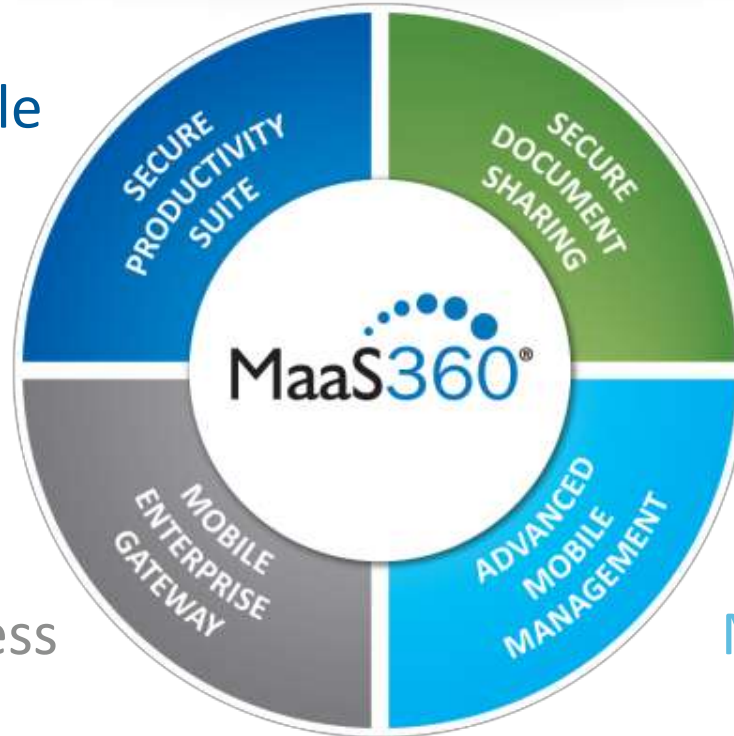


IBM Security Access Manager
for Mobile



MaaS360 Delivers an Integrated Approach

Secure Mobile
Containers



Secure Content
Collaboration

Seamless
Enterprise Access

Comprehensive
Mobile Management

One Platform for All Your Mobile Assets



MaaS360 Secure Productivity Suite



Secure Mail

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

Secure Browser

- Enable 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



Application Security

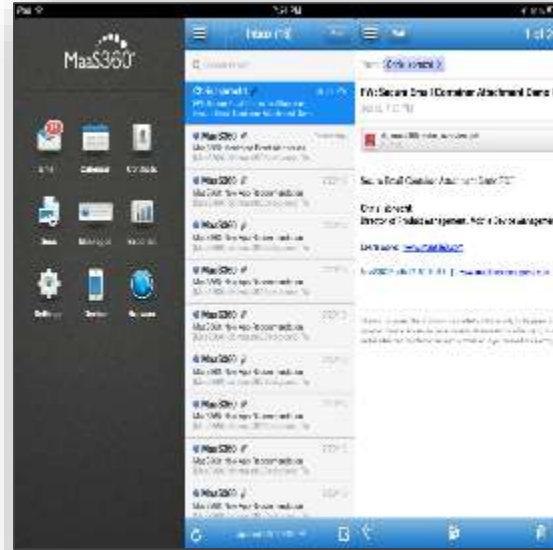
- Contain enterprise apps with a simple app wrapper or SDK
- Enforce authentication & copy/paste restrictions
- Prevent access from compromised devices



Secure Mail

An intuitive office productivity app with email, calendar, and contacts

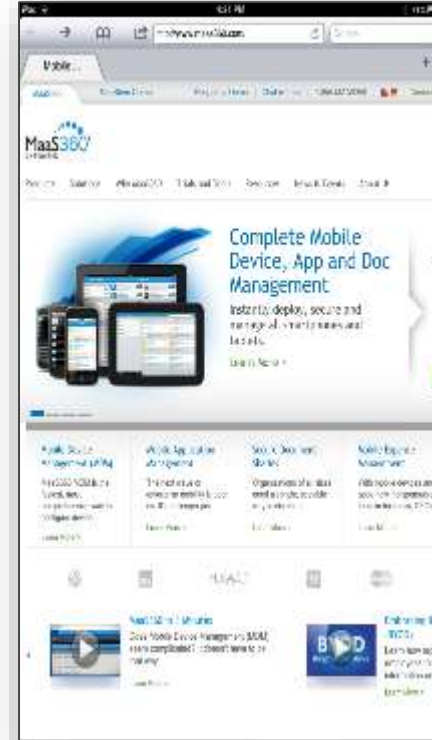
- Contains emails and attachments to prevent data leakage
- FIPS 140-2 compliant, AES-256 bit encryption for data at rest
- Restrict forwarding, moving, and screen captures
- Conduct on-line and off-line compliance checks prior accessing email
- Enforce authentication, cut and paste restrictions, and view-only mode



Secure Browser

A fully-functional web browser for iOS and Android devices to enforce compliance

- Define URL filters and security policies based on categories
- Block known malicious websites
- Enforce whitelists exceptions to specific websites
- Allow access to corporate intranet sites
- Restrict cookies, downloads, copy, paste, and print features to prevent data leaks
- Disable native and 3rd party web browsers
- Customizable event alerting and reporting



App Security

A mobile application container with full operational and security management to protect against data leaks

- Enable user authentication
- Prevent access from compromised devices
- Alert administrators of violations
- Take automated actions
- Restrict cut/copy/paste
- Limit data backup to iTunes

The screenshot shows a configuration window titled "Enterprise App for iOS". It includes the following sections:

- App Source:** Upload .ipa file (Browse...), Entitlements (.plist)
- Description:** App Name, Description (text area)
- Category:** Type of app (dropdown)
- Screenshots(s):** Upload screenshot (Browse...), Attach None
- Enterprise App:** MDM Remote Service
- Security Policies:** Define app policies and enforce them. Includes: Restrict Data Backup to iTunes, Enforce Authentication, Restrict Cut/Copy/Paste, Enforce Compliance.
- Provisioning Profile:** Upload .mobileprovision file (Browse...), Renew...
- Code Signing Certificate:** Upload .p12 file (Browse...), Select Password (text field)
- Distribute to:** All Devices (dropdown), Inherit Info, Send Time

Buttons: Cancel, Add





MaaS360 Application Security can secure apps

- Application security features:
 - Single Sign On (SSO) using container authentication
 - DLP controls
 - Cut/ Copy/ Paste restrictions
 - “Open-in” to Whitelisted container apps only (Ex: Open docs from MaaS container in whitelisted app for printing)
 - In-app VPN through Mobile Enterprise Gateway
 - Block usage of app on non-compliance
 - Data encryption (through SDK)



MaaS360 Application Security delivery methods

- App Security (MAAS360APPSEC) can be delivered in two ways:
 - App Wrapping – Requires no code change and is for apps the customer owns i.e. Enterprise apps
 - Software Development Kit (SDK) – Involves code changes to the app, but offers more granular controls. Needs to be implemented by owner of app

	App Wrapping	WorkPlace SDK
Public App		
Enterprise app		

App wrapping process for Enterprise apps

Application wrapping secures enterprise apps with a layer of corporate policies, with zero code change by developer



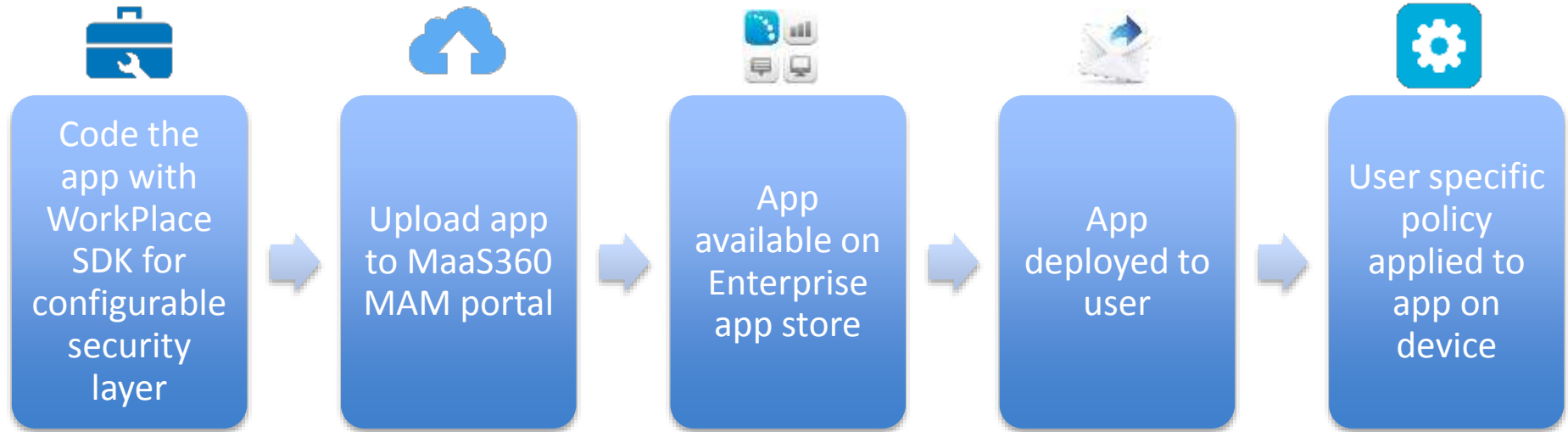
*In-app VPN requires Mobile Enterprise Gateway to be installed

App Wrapping workflow for Enterprise apps (Ex: Acme conference)

- Upload Acme conference app through “Add Enterprise app for iOS” workflow
- Check the “Enforce WorkPlace settings” box
- Upload the Mobile Provisioning and Code signing certificates
- Distribute app to end users
- To configure app for a particular user
 - Select the Persona policy (Security -> Policies) that is applied to the user and modify the WorkPlace Security settings for restricting cut/ copy/ paste or in-app VPN

SDK for Enterprise apps

Application wrapping secures enterprise apps with a layer of corporate policies, with zero code change by developer



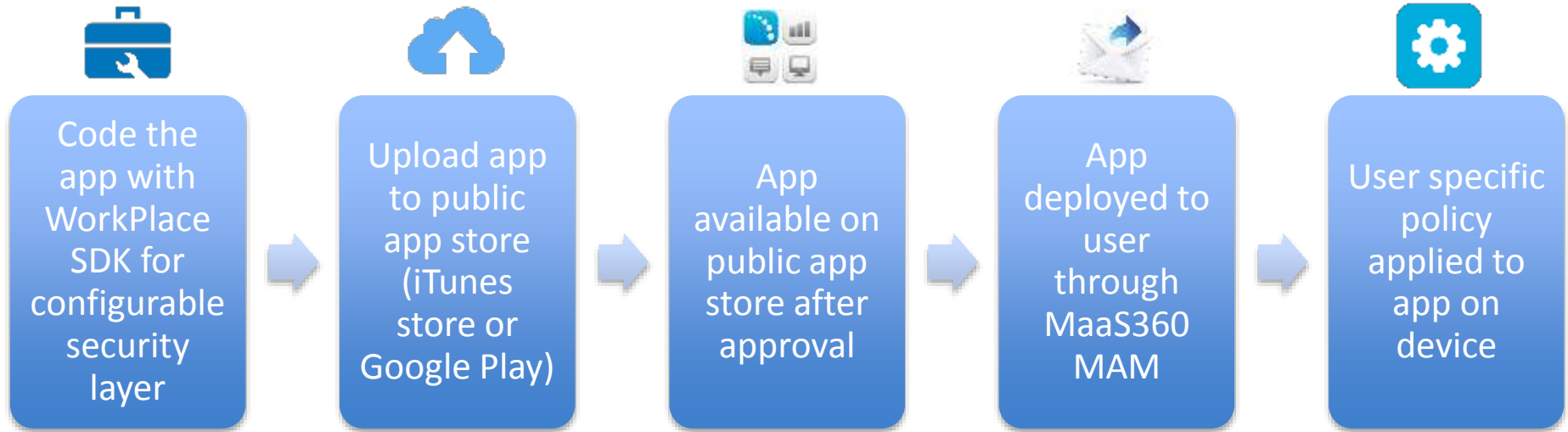
*In-app VPN requires Mobile Enterprise Gateway to be installed

SDK workflow for Enterprise apps (Ex: Acme conference)

- Download the WorkPlace SDK
- Include the SDK in the development project of the app (say, Acme conferencer) as per SDK documentation (XCode or Eclipse, for example)
- Upload the finished Acme app into the MaaS360 portal through the “Add Enterprise app” workflow
- Check the “Enforce WorkPlace settings” box
- Upload the Mobile Provisioning and Code signing certificates
- Distribute app to end users
- To configure app for a particular user
 - Select the Persona policy (Security -> Policies) that is applied to the user and modify the WorkPlace Security settings for restricting cut/ copy/ paste or in-app VPN

SDK for Public apps

Application wrapping secures enterprise apps with a layer of corporate policies, with zero code change by developer



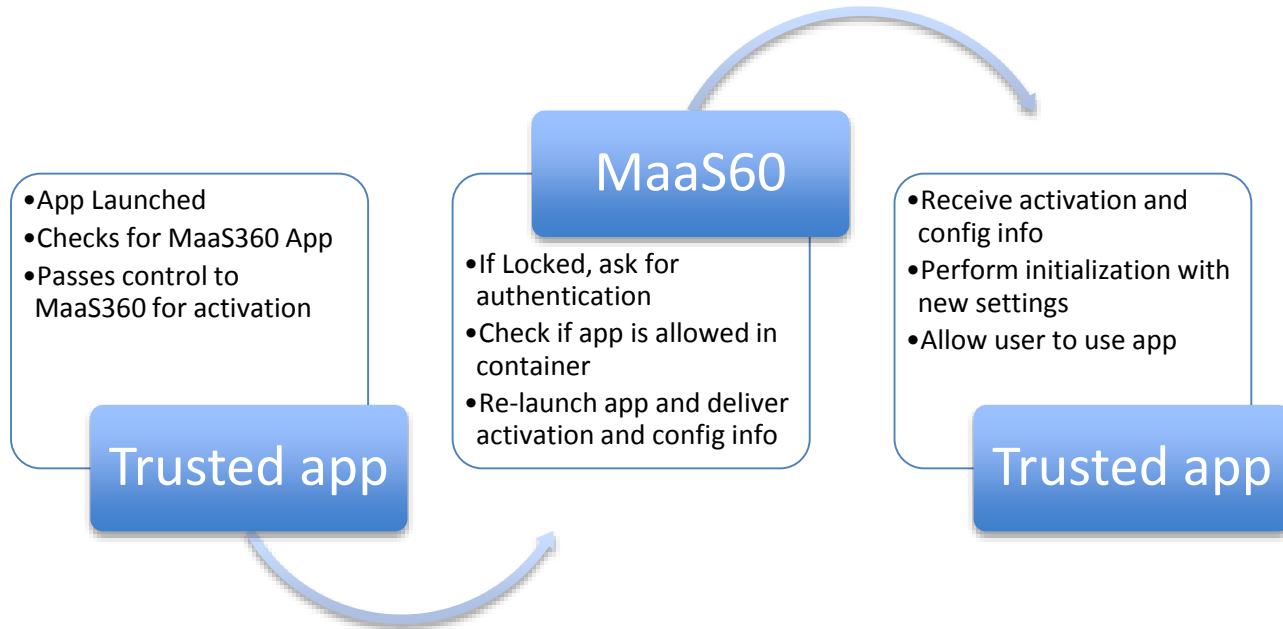
*In-app VPN requires Mobile Enterprise Gateway to be installed

SDK workflow for Public apps (Ex: Salesforce)

- Salesforce mobile developer downloads the WorkPlace SDK
- Includes the SDK in the development project of the Salesforce app as per SDK documentation (XCode or Eclipse, for example)
- Developer submits the finished Salesforce app to the public app store for approval
- Customer admin can then add the app to the app catalog through the “Add iTunes Store app” workflow
- Admin distributes app to end users. The SDK automatically initiates on a device enrolled on MaaS360
- To configure the Salesforce app for a particular user
 - Select the Persona policy (Security -> Policies) that is applied to the user and modify the WorkPlace Security settings for restricting cut/ copy/ paste or in-app VPN



Container Logic Flow Example



Process is repeated for SSO if container is Locked

MaaS360 Secure Document Sharing



Mobile Content Management

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



Secure Editor

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

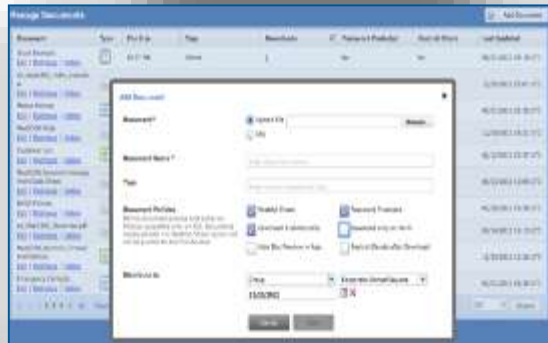
Secure Document Sync

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



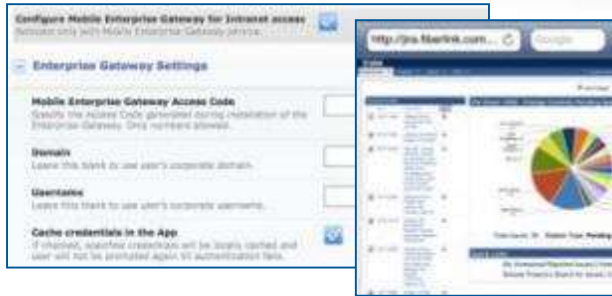
Secure Document Sharing

An extension of the MaaS360 Doc Catalog into a fully secure document container with expanded user support



- Integrated with Secure Mail for easy attachment viewing and security
- Allow users to edit and share attachments
- Securely distribute documents directly to the container
- Enforce user authentication
- Add, sync, and remove documents
- Protect sensitive documents with DLP controls

MaaS360 Mobile Enterprise Gateway

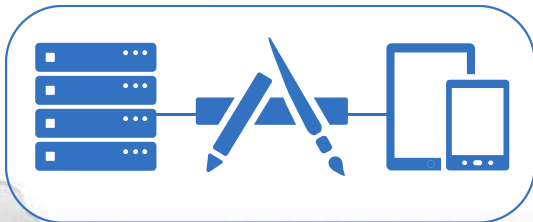


Mobile Enterprise Gateway for Browser

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

Mobile Enterprise Gateway for Docs

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



Mobile Enterprise Gateway for Apps

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

Architecture – Using Relay service

3. Device enrolls into MaaS360. Gets the gateway identifier from policies / enrollment



11. Device decrypts and renders content

4. Device talks to provisioning server to get the gateway address

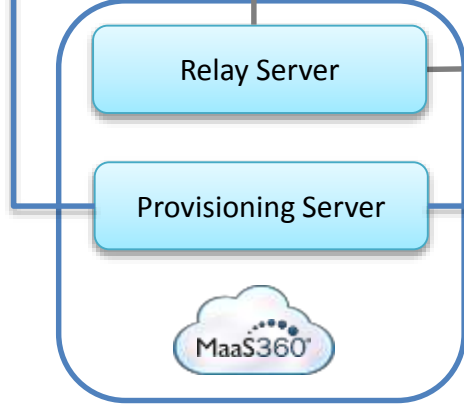
5. Device talks to the relay and requests internal resources from a gateway (using the gateway address)

10. Sends the encrypted payload back to the relay service

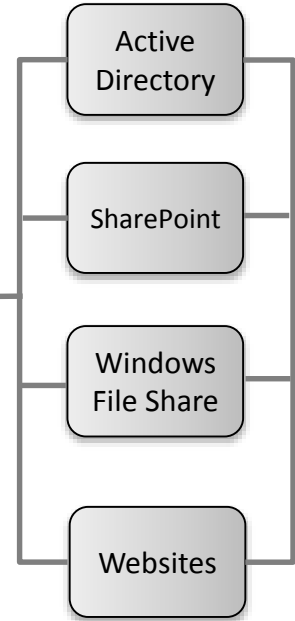
2. Activation request hits the provisioning service. The provisioning service returns a unique identifier to the gateway

6. Gateway gets the request from the relay.
7. Authenticates the user / device
8. Fetches the internal resource
9. Encrypts the resource using a secret key shared with the device (AES-256 bit encryption)

1. Gateway Activation: gateway talks to the MaaS360 during the install process

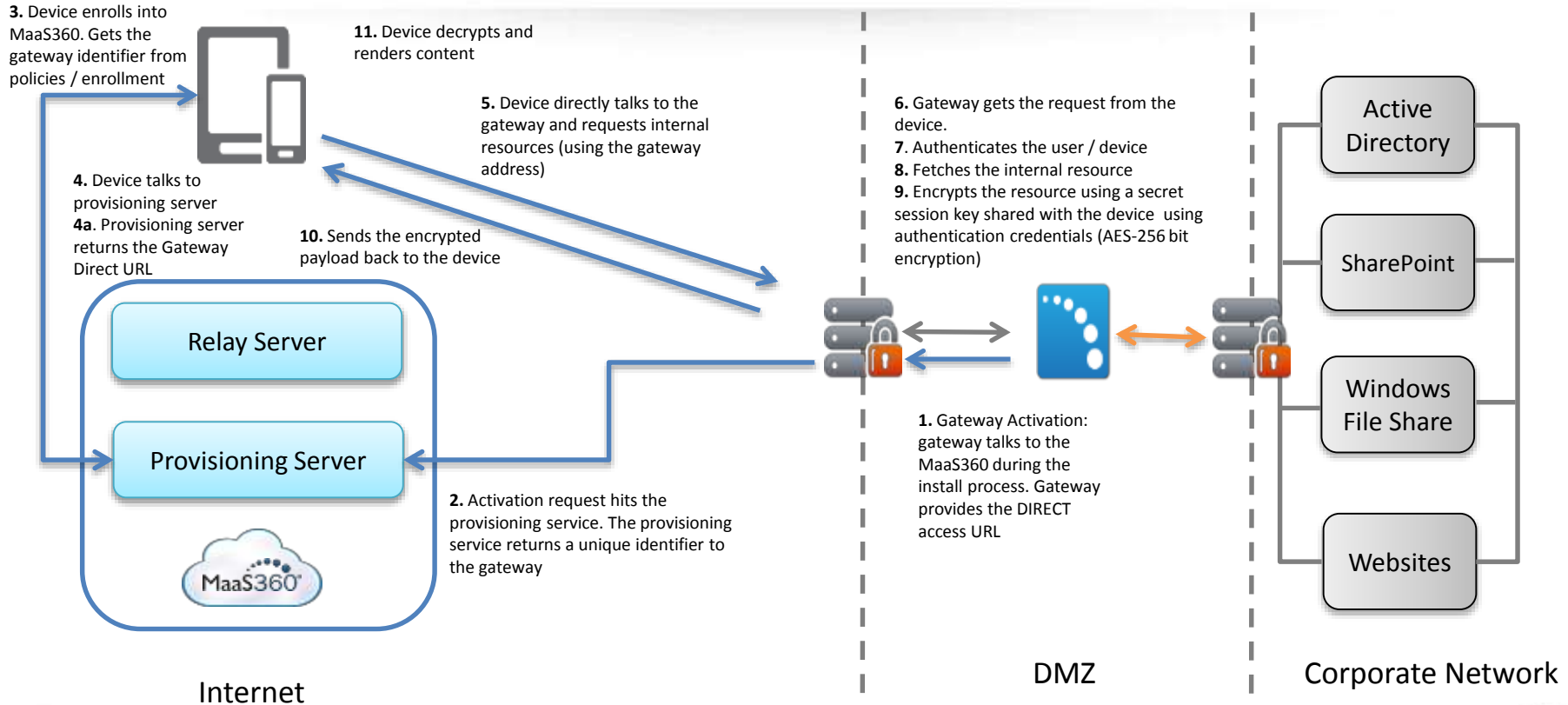


Internet



Corporate Network

Architecture – DMZ Gateway + Direct Access

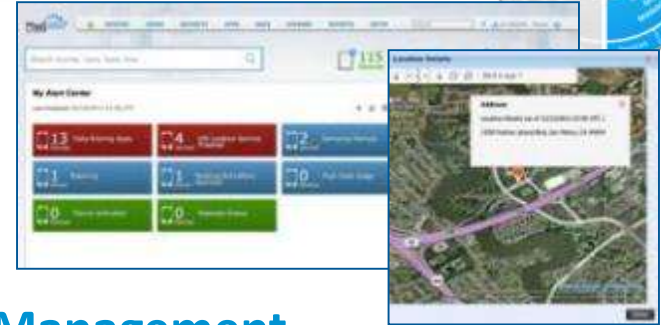


MaaS360 Advanced Mobile Management



Mobile Device Management

- Manage smartphones, tablets & laptops featuring iOS, Android, Windows Phone, BlackBerry, Windows PC & OS X
- 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



MaaS360: Most common use cases



Customer Use Cases

MDM Suite (MDM, Mobile App Mgmt, Mobile Expense Mgmt, Content Cloud)
Secure Productivity Suite ("Container") (Secure Mail, Secure Browser, App Security, MAM, Content Cloud)
Mobile Enterprise Gateway (For Internal Browser, Docs, and Apps Access/VPN)
Secure Content Collaboration (Doc Mgmt, Mobile Edit, Sync/Share, Content Cloud)



1. Best practice for iOS & Android adoption
2. BYOD and/or Apps
3. Compliance



Top 2014 Trend

4. Containerization of corporate content
5. User privacy from IT
6. BYOD for sensitive organizations / cultures



7. Access to internal resources from mobile
8. Content repositories
9. Intranet apps



10. Sales enablement (price sheets, etc.)
11. Line of business initiatives (board books)
12. Complete mobile content solution



MaaS360 powers user productivity



MaaS360: Meets comprehensive customer use cases



MDM Suite	→	✓	✓	✓	✓
SPS Suite	→		✓	✓	✓
Mobile Gateway	→			✓	✓
Secure Content	→				✓

Pfizer is using MaaS360 to manage and secure over 300 in-house mobile applications for over 50,000 corporate and BYOD users

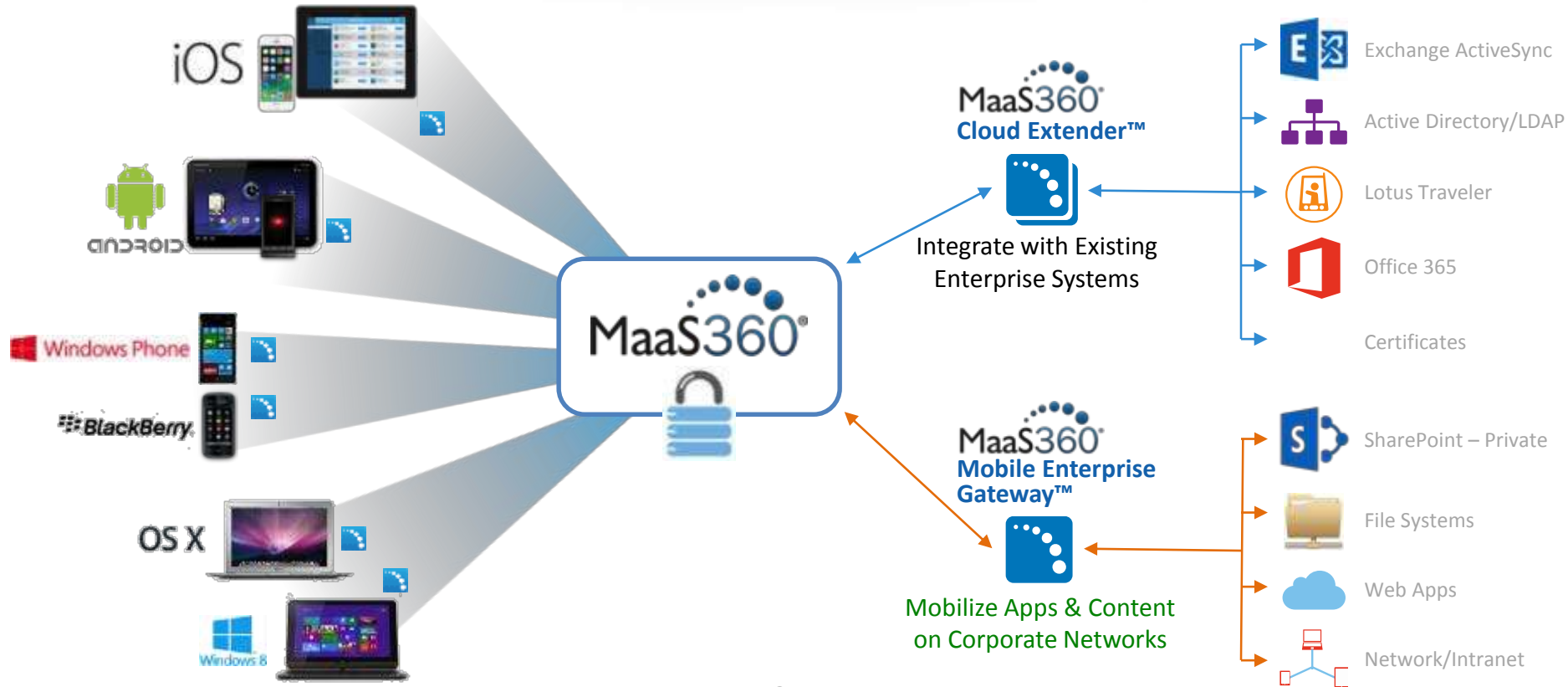
MaaS360 powered **London tube concierges** helping speed over 4.5M riders ⁽¹⁾ on their ways to the games on Aug 7th alone

MaaS360 provides **Telus** technicians with instant and secure mobile access to over 1,000 internal applications

Caesars has used MaaS360 to improve customer beverage delivery times over 80% to <4 minutes



Seamless Enterprise Integration



Potential white-label capability with MaaS360

- Vodafone Secure Remote Access – [link](#)
- O2/Telefonica Managed Mobility - [link](#)
- Cisco Mobile Collaboration Management Service
 - [Link](#) for more information
 - [YouTube](#) video
- Spiceworks – [link](#)



Example: Cisco MCMS Admin Portal

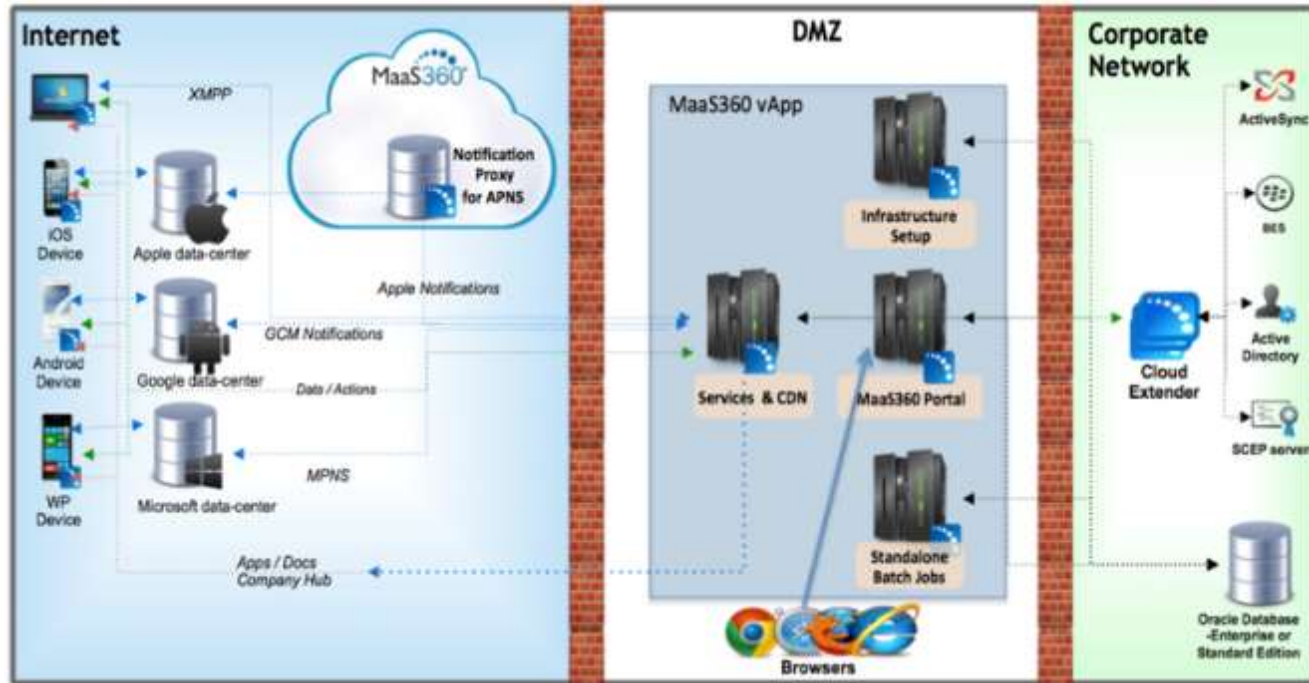
The screenshot displays the Cisco Mobile Collaboration Management Service (MCMS) Admin Portal. The interface includes a navigation menu with options: DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. A search bar is located at the top, and a notification indicates 29 Devices. The 'My Alert Center' section shows a last update time of 12/11/2013 10:05:33 and several alert cards: Active Devices (0), Inactivate Devices (29), Recently Added (0), No Policies (0), and Pending Approval (0). The 'App Catalog' section lists various applications with columns for App Name, Type, Category, VPP Codes, Last Updated, Install, and Distribute. The table contains 10 rows of application data.

App	Name	Type	Category	VPP Codes	Last Updated	Install	Distrib...
DocuView Social 2.0	View Distribute Delete Man...	Apple	Social		12/20/2012 12:26 EDT	E	No
Docu	View Distribute Delete Man...	Apple	Social		12/20/2012 12:21 EDT	E	No
DocuShare	View Distribute Delete Man...	Apple	Office		12/20/2012 12:57 EDT	I	No
DocuWeb Meetings	View Distribute Delete Man...	Apple	Web		12/19/2012 11:41 EDT	E	No
DocuWeb Meetings	View Distribute Delete Man...	Apple	Web		12/19/2012 11:30 EDT	E	No
DocuWeb	View Distribute Delete Man...	Apple	Web		12/20/2012 11:34 EDT	E	No
DocuShare for iPad	View Distribute Delete Man...	Apple	Social		12/20/2012 11:31 EDT	E	No
AnyConnect FCS	View Distribute Delete Man...	Apple	Business		12/20/2012 11:31 EDT	E	No
Docu AnyConnect	View Distribute Delete Man...	Apple	Business		12/20/2012 11:31 EDT	E	No

Example: Cisco MCMS Apps



MaaS360 On-Premise Solution



The MaaS360 Customer Experience

Fastest Time to Trust

60% deployed MaaS360 in **less than 4 hours**



75% deployed MaaS360 in **less than 8 hours**



Included sales and customer support at no additional charge



Customer support available 24 x 7 by phone, chat or email



Community, forums, blogs, on-demand webinars

“ Reference customers consistently praise MaaS360 for ease of use at the end-user and administrator levels. ”

– Gartner®



MaaS360 on the market



10 Yrs in Enterprise Mobility Management
5,000 Customers Across All Verticals
97% Customer Renewal Rate
Largest Cloud EMM Revenue Base
Millions of devices on MaaS360 platform

Industry Recognition

The Gartner logo, consisting of the word "Gartner" in a bold, blue, sans-serif font.

The Forrester logo, featuring the word "FORRESTER" in white, uppercase letters inside a dark green oval.

The Info-Tech Research Group logo, with "INFO~TECH" in white on a dark blue background and "research group" in smaller white text below.

The //CODiE// logo, featuring the text "//CODiE//" in a stylized, bold font, with "2013 SIIA CODiE WINNER" in smaller text below.

The IDC logo, with "IDC" in a large, blue, serif font and "Analyze the Future" in a smaller, italicized font below.

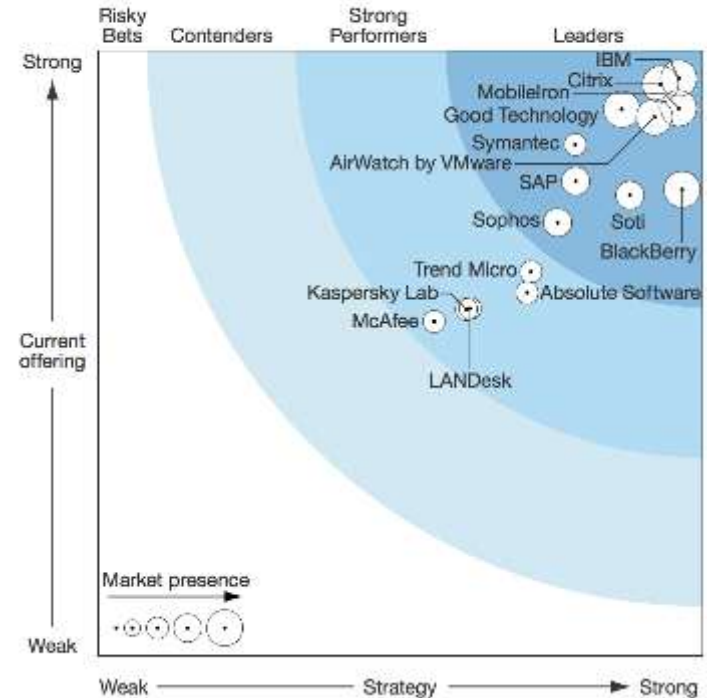
The NetworkWorld Clear Choice Test logo, with "NETWORKWORLD" in blue, "CLEAR CHOICE TEST" in bold black, and a magnifying glass icon over the word "TEST".



IBM recognized a leader in the 2014 Forrester Wave

- ✓ Ranked highest in current offering (product)
- ✓ Received more top scores (20/27) than any other vendor
 - Architecture & Scale
 - Containerization
 - App Security
- ✓ Achieved strong market strategy score

Figure 2 Forrester Wave™: Enterprise Mobile Management, Q3 '14



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Diverse Enterprise Customer Base

Manufacturing



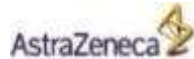
ArcelorMittal

EASTMAN

SIEMENS



Healthcare



Consumer



Financial



BNY MELLON



Public



Others



Case Study:

IBM migrates to MaaS360

IBM enabled MaaS360 for internal use **5 days** after acquisition close



70,000+

users migrated
in one month

16,000+

users registered within
24 hours

48,000+

users registered
in 15 days

200

Users enrolling **per
minute** at peak

< 500

help desk calls – less
than ½ of 1%



Why Customers Love MaaS360



Proven
approach to
mobile
management



Powerful
features to
address the full
mobility lifecycle



Secure
containers to
separate work
from play



Seamless
integration with
all of your existing
infrastructure



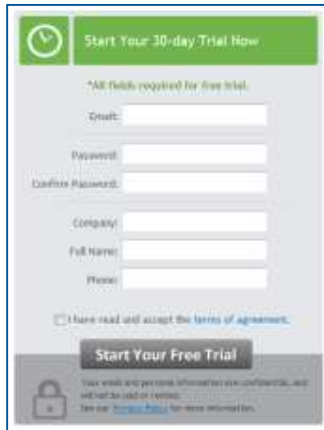
Simple
and fast with
an exceptional
experience

Get Started Now

1

Instant

Access a free, fully functional trial for 30 days



A screenshot of the MaaS360 registration form. The form is titled "Start Your 30-day Trial Now" and includes fields for Email, Password, Confirm Password, Company, Full Name, and Phone. There is a checkbox for "I have read and accept the terms of agreement." and a "Start Your Free Trial" button. A small lock icon and a disclaimer are visible at the bottom left.

2

Easy

Set up and configure your service in minutes



3

Mobile

Manage and secure your devices, emails, apps and docs



maas360.com



Questions ?

Thank you !

dymaczewski@pl.ibm.com

