IBM MaaS360
Enterprise Mobility Management

Frank Gentile / Chris Mangano
IBM Security / Mercadien Technologies
March 2, 2016
Built on a Trusted and Secure Cloud

On-demand and Multi-tenant

- Redundant Architecture
- Geographically Load Balanced
- Logical/Physical Security
- Disaster Recovery
- Data Encryption
- Standard Certifications

IBM MaaS360

AICPA, FISMA, FedRAMP, CSA Security Alliance

IBM Security
Instant Enterprise Mobility Management

Agility of the cloud for the pace of change in mobility

- Fast deployment
  - Simple provisioning processes
- Effortless scalability
  - Instantly turn up devices, users, apps
- Automatic upgrades
  - Continuous updates available instantly
- Unmatched affordability
  - Zero infrastructure, pay as you grow
Powerful Mobility Management

The Essentials

• SMS, email, URL enrollment
• Email, calendar, contact profiles
• VPN & Wi-Fi settings
• Device feature configuration
• Policy updates & changes
• Inventory management
• Compliance reporting

Advanced Management

• Mobile app management
• Event-based policies
• Real-time, automated compliance
• Proactive expense controls
• BYOD privacy settings
• Shared device support
• Self service portal
Robust Mobile Security

**Device**
- Encryption & passcodes
- Jailbreak/Root detection
- Locate, lock, wipe

**Email**
- Auto-quarantine/access approval
- Contain emails & attachments
- Remote wipe of work email

**Applications**
- Blacklist/Whitelist mobile apps
- Wrapping & compliance rules
- Remote wipe of managed apps

**Documents**
- Password authentication
- Restrict copy, paste, share
- Remote wipe of work files

**Web**
- Define URL filters & categories
- Allow access to intranet sites
- Disable native/3rd party browsers

**Network**
- Configure Wi-Fi & VPN profiles
- Cert delivery & authentication
- Dynamic policy based on SSID
Complete Mobility Management
Seamless Enterprise Integration

IBM MaaS360 Cloud Extender for plug & play hybrid cloud

- Advanced control of email access for mobile users
- Leverage existing directories & groups to manage users
- Use corporate credentials for enrollment & authentication
- Integrate certificates for advanced user authentication
- Install easily on any Windows machine

Not in-line & no points of failure
Complete Mobility Management and Security

IBM MaaS360

Management Suite
Visibility & Control

Productivity Suite
Trusted Workplace

Mobile Threat Management
Malware Protection

Content Suite
Content Collaboration

Gateway Suite
Enterprise Access
IBM MaaS360 Secure Mobile Mail

An intuitive personal information management (PIM) app with email, calendar & contacts for iOS, Android & Windows Phone

- Contains emails & attachments to prevent data leakage
- FIPS 140-2 compliant, AES-256 bit encryption for data at rest
- Enforce authentication, cut & paste restrictions & view-only mode
- Restrict forwarding, moving & screen captures
- Conduct on-line & off-line compliance checks prior accessing email
IBM MaaS360 Secure Mobile Browser

A feature-rich web browser for secure access to intranet sites & compliance of content policies for iOS, Android & Windows Phone

- Allow access to corporate intranet sites & network without VPN (e.g. JIRA)
- Define URL filters & security policies based on categories
- Block known malicious websites
- Enforce whitelist exceptions
- Restrict cookies, downloads, copy/paste, & print features to prevent data leaks
- Disable native & 3rd party web browsers
IBM MaaS360 Mobile Application Security

A mobile application container with full operational & security management to protect against data leaks for iOS & Android

- Enable user authentication
- Stop access from compromised devices
- Restrict cut/copy/paste
- Enforce file protection
- Limit data backup to iTunes
- Alert administrators of violations
- Take automated actions
- MaaS360 Market for best-in-class apps from developers leveraging SDK

Simple **App Wrapper** when deploying enterprise apps with MAM

**or**

Robust **Software Development Kit (SDK)** to integrate right in app code

- Restrict Data Backup to iTunes
- Enforce Authentication
- Restrict Cut/Copy/Paste
- Enforce Compliance
- Enforce File Protection
IBM MaaS360 Mobile Content Management

A mobile document container for secure content collaboration

- Contain content files to prevent data leakage
- Doc Catalog App for iOS & Android
- Centralized distributed content & repositories such as SharePoint, Windows File Shares, Box, Google Drive, OneDrive, IBM Connections & other CMIS systems
- User-based authentication for access
- Alert users on new or updated content
- Cut/paste restrictions & view only mode
- Versioning & time-based expirations
- Content Cloud for hosting & distribution
IBM MaaS360 enables mobile access and security of content with Box

- **Box App for EMM**
  - Pre-integrated with Box APIs
  - Preserves the native Box app experience
  - Controls access to content based on a user’s role or device security posture
  - Includes user authentication, open-in restrictions, selective wipe and blocking user access

- **Direct integration with IBM MaaS360 Productivity Suite**
  - Consolidates view of content repositories needed for work
  - Enforces policies to ensure data is secure
  - Includes user authentication, copy/paste restrictions and open-in to only authorized apps
IBM MaaS360 Mobile Document Editor

An office productivity app to create, edit & save documents on mobile devices

- Work on documents anywhere in an encrypted container for iOS & Android
- Collaborate on Word, Excel, PowerPoint & text files
- Change fonts, font size & color
- Insert images, camera photos, links, shapes, tables & more
- Perform searches within documents
- Share seamlessly with IBM MaaS360 Secure Mobile Mail & to corporate file folders
IBM MaaS360 Mobile Document Sync

Automatically synchronize files across managed devices to enhance user productivity & efficiency

- Synchronize user content across managed devices
- Restrict copy/paste & opening in unmanaged apps
- Store content securely, both in the cloud & on devices
- Access documents only through My Docs on devices
IBM MaaS360 Gateway for Browser

Simple & secure access to enterprise intranet sites & legacy web apps on a mobile device

- Browse right from the IBM MaaS360 Secure Mobile Browser
- No need for user to initiate a device-level VPN connection
- Protect data with robust security policies & DLP controls
- No changes to your network or firewall security settings
IBM MaaS360 Gateway for Documents

Seamless & secure access to internal SharePoint sites, Windows File Shares & other enterprise file stores on a mobile device

- Access documents & folders using IBM MaaS360 Mobile Content Management
- Create, edit, save & share documents securely
- No need for user to initiate a device-level VPN connection
- Protect data with robust security policies & DLP controls
IBM MaaS360 Gateway for Apps

Secure per app VPN tunnel to internal data resources to enhance enterprise apps on a mobile device

- Enable & distribute private apps with enterprise data, secured using IBM MaaS360 Mobile Application Management & IBM MaaS360 Mobile Application Security
- No need for user to initiate a device-level VPN connection
- No changes to your network or firewall security settings
Auto Quarantine

With ActiveSync enabled, you can still require approval

End user receives an alert (from Exchange or Notes)

Admin receives an alert (from IBM MaaS360)

Admin can view details, set policy & approve the device
Simple Enrollment

SMS text message

and/or

Email with one-time passcode + custom URL + QR code
New portal redesign for an elegant & efficient experience
My Alert Center for a customizable & interactive dashboard
My Activity Feed for a real-time timeline of every activity
At-a-glance overview of devices, users, apps & docs
Global search & action bar
OTA Configuration Management

- Passcode settings
- Corporate email, calendar & contacts
- Wi-Fi & VPN profiles
- Device features restrictions
  - Camera
  - FaceTime
  - Siri
  - iCloud
  - Screen Captures
  - …and many more
- App compliance
- Roaming settings
- Device groupings
Policy Enforcement

Automated action on non-compliant events

- Enforce MDM management
- Minimum OS version
- Remote wipe support
- SIM change

- Encryption support
- Application compliance
- Jailbreak / Root detection
- Roaming state change
Policy Enforcement

- **Location-Based Policies**
  - Physical location (e.g. Address)
  - Network connection (e.g. SSID)

- **Dynamic Policy Assignment**
  - Change policy on:
    - Automated location **Check in**
    - Automated location **Check out**

- **Geo-Fencing Rules**
  - Take action on:
    - Device leaving specified location
    - Device entering specified location

- **Time-Based Policies**
  - Assign group persona policies based on:
    - Time of day
    - Days of the week
BYOD Privacy Settings

Disable collection of personal information on a single device, all devices, or a device group

- App inventory information
- Location information
- IP address & SSID
IBM MaaS360 Mobile Application Management

- Enterprise App Catalog
- App security & compliance management
- Distribute & update apps
- Selectively remove managed apps
- Volume Purchase Program management
- App Cloud for hosting & distribution
New App Catalog for iOS

- New look and feel for iPhones & iPads
  - Similar to native App Store user experience
  - In collaboration with Apple designers
  - Keeps app info up-to-date with public app store

- Simplify discovery of relevant apps
  - Intuitive search, sort, filter, multiple tabs
  - Highlights recent and most popular apps
  - Easy navigation between categories

- Promote key apps for users
  - App Bundles to logically group apps
  - Featured Apps & Bundles to draw users’ attention
  - Similar Apps to help users find the right app

- Install/Update All apps with one touch

Unmatched App UX in EMM industry
New App Catalog for iOS – Advanced Mode

- **Ideal for medium to large enterprises**
  - IT teams that deploy more than 20 apps to users
- **Adds many new and advanced features**
  - App Bundles
  - Featured Apps & Bundles
  - Similar Apps
  - Multiple Tabs
  - …and all of the upgraded features to aid in the discovery of relevant apps
New App Catalog for iOS – Simple Mode

- **Ideal for small & medium companies**
  - IT teams that deploy less than 20 apps to users
- **Simple, clean app experience with upgraded features**
  - Single app list
  - Intuitive search, sort, filter
  - Highlights recent and most popular apps
  - Easy navigation between categories
As Mobile Grows, Threats Grow

In 2014 the number of mobile phones (7.3 billion) will exceed the number of people on the planet (7 billion). 138 billion apps were downloaded in 2014. By 2017 50% of employers will require BYOD. Mobile malware is growing. Malicious code is infecting >11.6 million mobile devices at any given time. Mobile devices and the apps we rely on are under attack. 97% and 87% of top paid Android and iOS apps have been hacked.
Criminals Attack the Weakest Link
IBM MaaS360 Mobile Threat Management

Detects, analyzes and remediates mobile risks delivering a new layer of security for Enterprise Mobility Management (EMM) with the integration of IBM Security Trusteer® to protect against:

- Mobile malware
- Suspicious system configurations
- Compromised devices
Mobile Malware Detection and Remediation

IBM MaaS360 helps stop mobile apps with malware signatures on iOS & Android devices from a continually updated database

- Set granular policy controls & app exceptions
- Automate remediation with compliance engine
- Alert user & admins when malware is found
- Uninstall apps with malware automatically*
- Block access, selectively or fully wipe
- Restrict use of container solutions
- View device threat attributes in portal

*select Samsung SAFE Android devices
Enhanced Jailbreak and Root Device Detection

IBM MaaS360 discovers & remediates compromised or vulnerable iOS & Android devices with detection logic that’s updated over-the-air

- Protect against jailbroken iOS & rooted Android devices that can provide attackers with additional privileges on the operating system, enabling various attack vectors
- Seek out hiders & active hiding techniques that try to mask detection of jailbroken & rooted devices
- Leverage detection logic updated over-the-air without any app updates to be more responsive to fast-moving hackers
- Set security policies & compliance rules to automate remediation
- Block access, selectively or fully wipe devices or remove device control
IBM MaaS360 Mobile Expense Management

- Real-time usage monitoring and alerting
- Policies based on specific groups
- Policies restricting or limiting roaming
- Integrated reporting & analytics
- On-device app to monitor usage
Remote Help Desk Support

- Reset forgotten device passcode
- Locate lost device
- Buzz lost device
- Selective wipe
- Full device wipe
- Send message
- Change policy
- Remove control
End-User Self Service Portal

A self service portal for end-users to manage their content, apps, devices

- Accessible from any web browser
- Authenticated via Active Directory or locally via IBM MaaS360

- Sync content across devices and PCs
- Add content, files, and folders
- Share files, folders, and links with colleagues and external users
- Take action on devices
  - Locate, Lock, Wipe, Passcode Reset
- View personal & corporate devices
  - Action History, Hardware/Network Info, Security/Compliance State
Mobility Intelligence™

Dashboards deliver a real-time, interactive, graphical summary of your mobile IT environment & security overviews
Mobile Metrics

- Benchmark key metrics
- Compare against other IBM MaaS360 customers
- Learn what others are doing with mobility
- Gain valuable insights & opportunities
- Make a stronger business case
IBM MaaS360 for iOS

- **Gain Mobile Insight**
  - Hardware & network information
  - Security, compliance & location details
  - Enable Apple’s Device Enrollment Program (DEP)

- **Set Security Policies**
  - Enforce passcode requirements
  - Enforce encrypted backups, restrict camera, allow Touch ID
  - Distribute Wi-Fi, VPN & email profiles; enable always-on VPN
  - Customize Lock Screen, Lost Mode, AirPrint, AirPlay
  - Restrict app installation, camera, FaceTime, Shared Photo Stream, Siri, YouTube, Safari, Touch ID & much more
  - Manage iCloud controls for documents, apps, backups & photo synching
  - Supervised Device features with Apple Configurator & DEP

- **Manage Mobile Apps**
  - Blacklist, whitelist or require apps
  - Distribute private enterprise apps
  - Leverage Managed Open In to prevent data leaks
  - Encrypt third-party app data automatically
  - Utilize Per App VPN, Single Sign On, App configuration
  - Delete an app & its data on-demand
  - Auto-remove corp apps if user deletes MDM profile
  - Restrict app backups to iTunes or iCloud
  - Manage new Apple Volume Purchase Program licensing for apps & books
Device-based App Assignment deploys apps directly to devices using the Volume Purchase Program & IBM MaaS360

- Distribute apps easily and with full control
- Assign apps directly to a device, without requiring an Apple ID / iTunes account
- Migrate to device-based from user-based app assignment

Makes life easier for IT and users

- All industries will benefit from this innovation, especially Education, Retail and Healthcare
- Streamlines user experience
- Makes DEP enrollment experience “magic”
- Reduces management overhead for IT
- No more provisioning iTunes accounts for corporate-owned, single use (COSU) devices

Requirements

- Volume Purchase Program & App Licenses (paid/free)
- App must be enabled for device assignment by developer (opt-in)
- iOS 9 Devices
New iOS 9 Enterprise Features

With IBM MaaS360 and iOS 9, you can deploy iOS devices faster, distribute apps easier, secure data better, save money, and provide a seamless mobile user experience.

New Enterprise Security features:
- Restrict AirDrop for managed apps & iCloud Photo Library
- Set a host of new Supervised restrictions:
  - Usage of App Store, keyboard shortcuts, Apple Watch, passcode modification, device name modification, wallpaper modification & automatic app downloads
- Turn off Trust of Enterprise Apps on Supervised devices
- Mail Drop disabled on MDM-created email accounts
- iOS 9 now requires at least a six-digit numeric passcode

New App Distribution features:
- Device-based app assignment deploys apps directly to devices using the Volume Purchase Program & MaaS360
  - Assign apps directly to a device with the serial number, without requiring an Apple ID
  - Migrate to device-based from user-based app assignment
  - Requires VPP licenses (paid/free) & app developers to opt-in
  - Silently install apps on Supervised devices
- Push or pull public apps w/o user having access to App Store
- Enterprise apps installed via MaaS360 are trusted
- Apps purchased & distributed through VPP can be assigned to devices or users in any country where the app is available
- VPP has expanded to include 26 countries
- Enforce apps distributed to device are managed
  - Silently manage apps on Supervised devices after users install them w/o reinstalling apps or any loss of user data

New Device & Data Management features:
- Allow MaaS360 to trigger device updates to new versions of iOS to any device enrolled in the DEP program
  - Initiate both the download & installation of iOS updates separately
  - Only for iOS updates once device has installed iOS 9
- Apple Configurator is redesigned with a new user interface & delivers powerful new management capabilities
  - Pre-deploy apps & stream device enrollment with DEP
  - Works with device-based app assignment through VPP
- Activation step for Android Migration skipped with DEP
- Per App VPN now supports UDP to stream audio or video
- Specify how managed apps use cellular data networks by restricting an app when roaming on Supervised devices

New User Productivity features:
- Multitask on iPad by interacting with a second app with:
  - Slide Over to work with a second app w/o leaving current app
  - Split View to have two apps open & active at the same time
  - Picture in Picture to watch a video while on an app
- Annotate & mark up image files & PDFs
- Use the new Notes & News apps to keep track of daily events
Apple Device Enrollment Program (DEP)

An Apple program to help organizations manage their corporate-owned devices

- One touch device activation and MDM Enrollment
- Mandatory and lockable MDM
- Supervise devices over the air for enhanced security
- Customize user activation process for easy activation

Requires an MDM service and supported reseller

- Full IBM MaaS360 management
- IBM procurement support

Actions for MaaS360 DEP devices (iOS 9)

- Initiate OS version updates
- Push/track iOS updates to individual devices/groups
- Define template for automated naming of new DEP devices
  - Customizations include: model, username, device type, static strings and sequences
Shared Device Support for iOS

- Share a single device with multiple users
- Reduce device purchasing costs
- Maximize device utilization
- Log in to apply user specific settings
  - Authentication with Active Directory or IBM MaaS360 local
  - Email, Wi-Fi, VPN, Apps, Docs
- Log out to remove settings
- Maintain an audit trail of users
- Ideal for a number of use cases such as:
  - An iPad shared amongst doctors on rotating shifts
  - An iPhone shared for retail demonstrations
  - An iPad shared by shift workers on the manufacturing floor
IBM MaaS360 for Android

- **Enterprise-Grade Mobile Security**
  - Support for Android 2.2+, Android for Work, Samsung SAFE and Samsung KNOX
  - Flexible data and app separation with full OS encryption and granular security policies
  - Isolated workspace to access and manage enterprise emails, contacts, calendars, apps and the web, while reducing the risk of data leaks

- **Marshmallow in the Enterprise**
  - Same day support for Android’s latest mobile OS
  - Enrolled users running 6.0 prompted to accept or reject device permissions
  - Certain policies may require a user to accept permissions to remain in compliance
IBM MaaS360 for Android

Gain Mobile Insight
- Model, serial number, operating system
- Home network/current network
- Roaming status, MAC address
- Amount of free storage
- Apps, versions and size
- Device ID (phone number, IMEI, email address)
- Encryption level, root detection, passcode status, device restrictions, installed profiles and security policies
- In-depth reports for documents, users, devices, and apps

Set and Distribute Android Policies
- Enforce password requirements
- Prevent non-compliant device access to corporate data
- Disable Copy & Paste within external applications
- Enforce device encryption
- Allow or restrict installation of non-Google Play apps
- Restrict use of the device’s camera
- Prohibit use of Wi-Fi and/or Bluetooth
- Blacklist and Whitelist apps
- Set native app compliance rules
- Block devices when out of compliance

Take Action
- Silently install or uninstall mobile applications
- App blacklisting and whitelisting
- Automatically install Whitelisted/uninstall Blacklisted apps
- Prevent users from uninstalling apps
- Activate Kiosk Mode
- Block Hardware Keys
- Disable passcode reuse
- Enable VPN for specific applications via Android for Work
- Enforce location-specific policies via geofencing
- Disable native applications from being used or accessed
A **SAFE** device delivers security & management capabilities above and beyond standard Android features:

- **Security Policies**
  - Firmware Upgrades
  - Granular Bluetooth controls
  - Browser controls
  - Restrict device features
    - Microphone
    - Near Field Communications (NFC)
    - Use sensor aiding for location detection
    - Fingerprint authentication (SAFE 5.1+)

- **Restrict Security Features**
  - USB debugging
  - SD Card
  - SD card write
  - Clipboard
  - Screen capture
  - Data backups
  - Automatic restore
  - Google crash report
  - Factory reset
  - OTA upgrade

- **Restrict Network Settings**
  - Emergency calls only
  - Wi-Fi
  - User to add Wi-Fi networks
  - SMS & MMS
  - Sync during roaming
  - Voice roaming

- **Additional Settings**
  - Wi-Fi Network Configuration
  - Whitelist and Blacklist SSID's
  - Configuration of VPN and Native Email Client
  - Certificate Authentication
  - Internal & External Encryption
  - Silently Install & Delete Apps
  - Remote Control for Troubleshooting
  - Control App Store Access
Android for Work-enabled devices access pertinent work content without sacrificing end-user experience:

- Easy management & enhanced security
- Prepackaged with work applications and collaboration tools
- Geared towards getting employees to work smarter and faster (the way they prefer to)

**Android for Work Settings**
- Enforce Passcode by Quality, Length, and Age
- Restrict Clipboard, Screen Capture, Notifications
- Specify Work Apps to be displayed on Home Screen
- Prohibit USB Debugging
- Specify Required & Whitelisted Apps for Work Profile
- Configure ActiveSync Account, VPN and CA Certs
- Enable Chrome Browser:
  - URL Blacklist/Whitelist
  - Bookmarks
  - Browser Settings

**Supported Android Devices**
- Android L+* in standard “Work Native” mode
  - PO (Profile Owner) with Separate Work Profile
  - DO (Device Owner) Enterprise Owned; no separation between personal and work spaces
- Older devices running Work App 1.2.1+

* Not all Android L devices support Android for Work
IBM MaaS360 for Samsung KNOX™

MaaS360 supports Samsung KNOX, a comprehensive mobile solution for work and play, utilizing a separate container to manage & secure business data:

- Comprehensive management of apps, content, and devices for the KNOX platform
- Complete containerization of personal & work data on devices
- Over-the-air (OTA) configuration and management of KNOX container-level security policies
- Enhanced email & browser configuration
- Remote lock, unlock, and selective wipe of KNOX container data
IBM MaaS360 for Motorola EDM

- Motorola EDM (Enterprise Device Management) is a set of APIs used with specific Motorola devices that allows for additional security controls that are suited for the enterprise

- Additional Security Policies
  - Automatic configuration of email profiles
  - Enforcement of device & SD Card encryption
  - Automatic VPN profile configuration

- Supported Devices (partial list)
  - RAZR series
  - Atrix HD
  - Droid 4
  - Bionic
  - Many newer devices
IBM MaaS360 for Windows Phone

- **Agent integration with Microsoft Push Notification Services (MPNS)**
  - Supports Windows Phone 7.5, 8.0 and 8.1

- **Gain Mobile Insight**
  - Hardware information
  - Network information
  - Security & compliance
  - Location details

- **Set Security Policies & Take Action**
  - Integrate with Exchange ActiveSync
  - Configure email settings
  - Set passcode policy
  - Send message
  - Locate device
  - Wipe device
  - Change policy
  - Refresh data

- **Manage Mobile Apps**
  - Install & update internal apps
  - View installed internal apps & versions
  - Recommend public apps
IBM MaaS360 for Windows 10

- **Gain Mobile Insight**
  - Hardware Inventory
  - Device Name
  - Username
  - Email Address
  - Enrolled Device ID
  - Ownership Designation
  - ActiveSync Device ID
  - Windows Store apps
  - OS & Version
  - Manufacturer
  - Model
  - Wi-Fi Mac Address
  - Basic Input/Output System
  - Processor Type
  - Screen Resolution
  - OS Language
  - Enrolled Device ID
  - Ownership Designation
  - ActiveSync Device ID
  - Windows Store apps

- **Take Action**
  - Integrate with ActiveSync
  - Configure email settings
  - Set passcode policy
  - Send message
  - Locate device
  - Wipe device
  - Change policy
  - Refresh data
  - Root, CA and Publisher certificate configurations

- **Secure Devices and Network Access**
  - Enforce internal storage encryption
  - Enable or disable SD card use
  - Disable developer unlock
  - Allow VPN over mobile data or data roaming
  - Permit use of WiFi and WiFi Sense hotspot auto-connect

- **Place Restrictions**
  - Restrict Camera, Cortana, location data, Telemetry, Bluetooth, Internet Sharing, or adding non-MS accounts
  - Prohibit use of location information in Search
  - Deny use of MS account for non-email related connection authentication and services
  - Disallow Sync My Settings across multiple devices
  - Reject Non-Windows Store app installs

- **Enforce Compliance**
  - Perform policy changes
  - Locate devices and review breadcrumb history
  - Selectively or fully wipe lost, stolen or uncompliant devices
  - Restrict manual device decommissioning
IBM MaaS360 for Windows

Just as simple as managing mobile devices, all from a single portal.

- Supports XP SP3, Vista, Windows 7, 8+ (including Pro) & 32-bit & 64-bit where applicable
- Gain Instant Insight
  - Hardware inventory
  - Software inventory
  - Security & compliance
  - Custom attributes
  - Operating system details, patch levels
  - Location history
- Take Immediate Action
  - Enroll over-the-air
  - Locate, lock, restart or shutdown device
  - Deploy OS patches for latest security updates
  - Distribute software & documents via self-service
  - Send message
  - Wipe the hard drive
IBM MaaS360 for OS X

- Easy enrollment process as simple as MDM
- Gain Instant Insight
  - Hardware, software inventory
  - Network information, operating system
  - Missing OS patches
  - Security & compliance
    - Anti-Virus
    - Personal Firewall
  - Data Protection
- Set Security Policies
  - Enforce passcode, encrypted backups, Gatekeeper for apps
  - Add Certificate credentials
  - Configure Email accounts remotely – Exchange ActiveSync, IMAP, POP
  - Restrict users from moving emails between accounts
  - Push Wi-Fi & VPN profiles, proxy settings, SSID auto-join, printer config
  - User & Group Mgmt - e.g. restrict guest users
  - Disable changing preferences for mail, sharing, Bluetooth settings
  - Restrict media usage - External media, AirPlay
- Take Immediate Action
  - Lock device
  - Wipe device
  - Change OS X policy
  - Remove MDM control
IBM MaaS360 for BlackBerry

- **BES Server Integration & Device Merge**
  - Support for both BES & non-BES customers
  - For devices being managed by both BES & native MaaS360 MDM agent, actions & device records are automatically merged
  - BlackBerry 10 devices are supported with Exchange ActiveSync via MaaS360 Cloud Extender

- **Gain Mobile Insight**
  - Hardware & software information
  - Network information (BES server & policy)
  - Security & compliance
  - Location details

- **Set Security Policies**
  - Enforce passcode requirements
  - Enforce device & SD card encryption
  - Blacklist, whitelist or require apps
  - Take automated enforcement action such as wipe device if out of compliance
  - Configure data collection & heartbeat frequencies

- **Take Immediate Action**
  - Send message
  - Reset forgotten passcode
  - Locate device
  - Lock device
  - Wipe device
  - Selective wipe device (email)
  - Remove a device record from BES
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.

THANK YOU

www.ibm.com/security

IBM Security
Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.