



Invitación personal

Desayuno de trabajo IBM MaaS360

No lo decimos nosotros.
MaaS360, la mejor solución
de gestión de dispositivos

INVITACIÓN DESAYUNO

Miércoles, 21 de enero de 2015
IBM Client Center Madrid
C/ Corazón de María, 44



AGENDA

- **Introducción: IBM Security (Emmanuel Roeseler)**
- **Unified Device Management (Tito Irastorza)**
- **Novedades: MaaS360 Threat Management (Javier Jarava)**
- **Casos de éxito, licenciamiento y comercialización (Tito)**
- **Café**
- **Demostración MaaS360 (Javier Llorente)**
- **Resumen y Cierre**
- **Cóctel**

Gartner has recognized IBM as a leader in The Magic Quadrant ...

Client Management Tools



Magic Quadrant for Client Management Tools
Kevin Knox, Terrence Cosgrove, May 22, 2014

Enterprise Mobility Management Suites

Figure 1. Magic Quadrant for Enterprise Mobility Management Suites



Source: Gartner (June 2014)

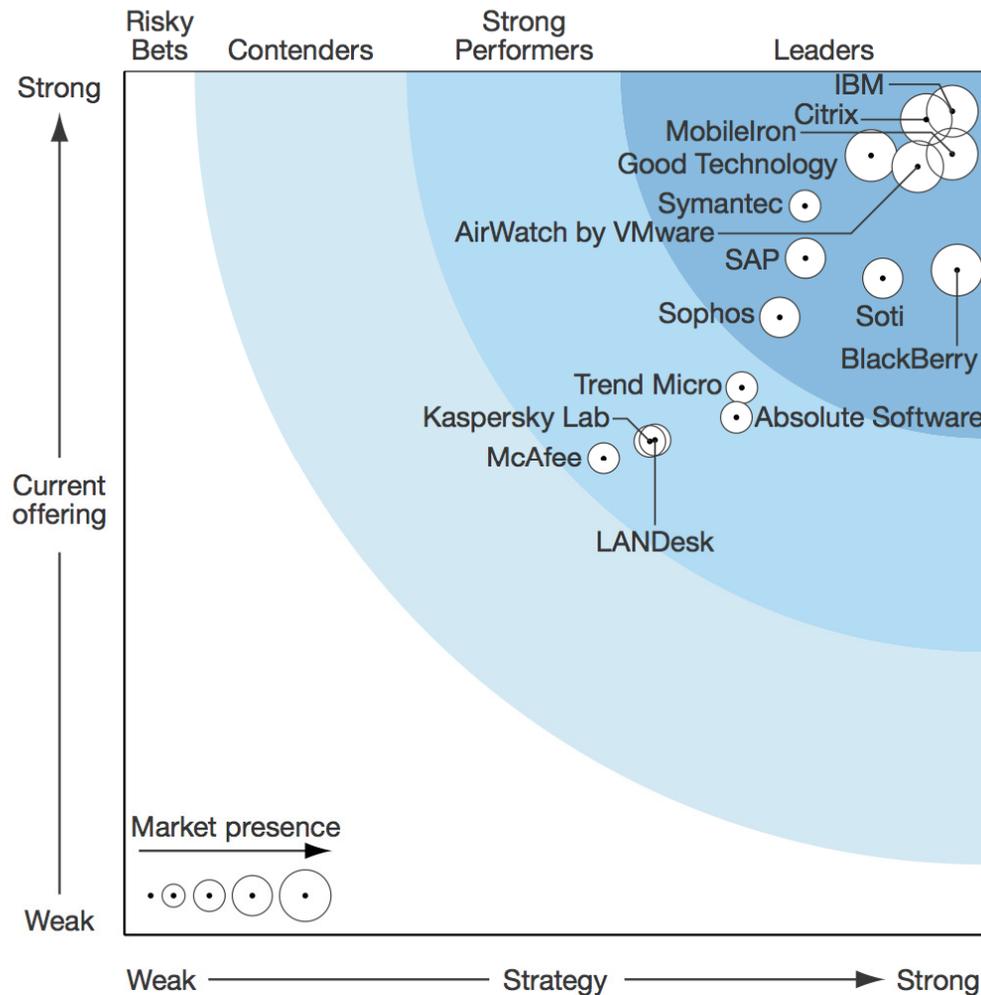
Gartner, Magic Quadrant for Enterprise Mobility Management Suites, Terrence Cosgrove et. al., 3 June 2014.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from IBM. G00260863

© 2014 Gartner, Inc. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Best-in-Class Devices and Management

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



IBM: A Leader in Enterprise Mobility Management

IBM is a Leader in the 2014 Forrester Wave for Enterprise Mobile Management, ranked Highest in Current Offering and received top scores in 20 out of 27 categories.



+

IBM



The IBM MobileFirst Platform for iOS provides enterprise-class software for building and deploying elegant iOS apps that integrate with enterprise systems. The platform also offers industry-leading mobile device management capabilities so your clients have flexible options for managing iPhone and iPad across their company.

IBM Unified Device and Persona based Management



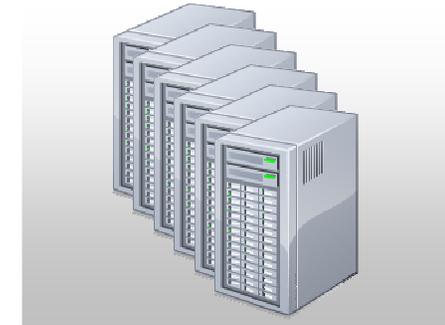
Smartphones & Tablets



Mobile Apps



PC's, Macs, POS, ATMs
On and off-network



Distributed Data Centers
Physical and Virtual



Patch Management



Lifecycle Management



Power Management



Core Protection



Security & Compliance



SW Usage & Analysis



Server Automation



Datacenters

Find and Fix problems in minutes across all enterprise computers and mobile devices



- **10 Años** en la gestión de la movilidad empresarial
- **5,000** Clientes
- **450** Empleados
- **97%** de renovación de contratos
- **LA MAYOR** base instalada de EMM en cloud
- **Millones** de dispositivos en la plataforma MaaS360

Diciembre 2013 →

Junio 2014 →

Noviembre 2014 →

Febrero 2015 →

IBM adquiere Fiberlink

MaaS360 on-premises en PPA

MaaS360 SaaS en PPA

Transfer of business

¿Qué es MaaS360?

Fácil de desplegar y escalar



Plataforma de gestión y seguridad de dispositivos móviles, aplicaciones, y contenidos

Para organizaciones ...

... desplegando dispositivos iOS, Android, Windows mobile, ...

... permitiendo a sus empleados usar sus propios dispositivos (BYOD)

... desarrollando y desplegando aplicaciones móviles

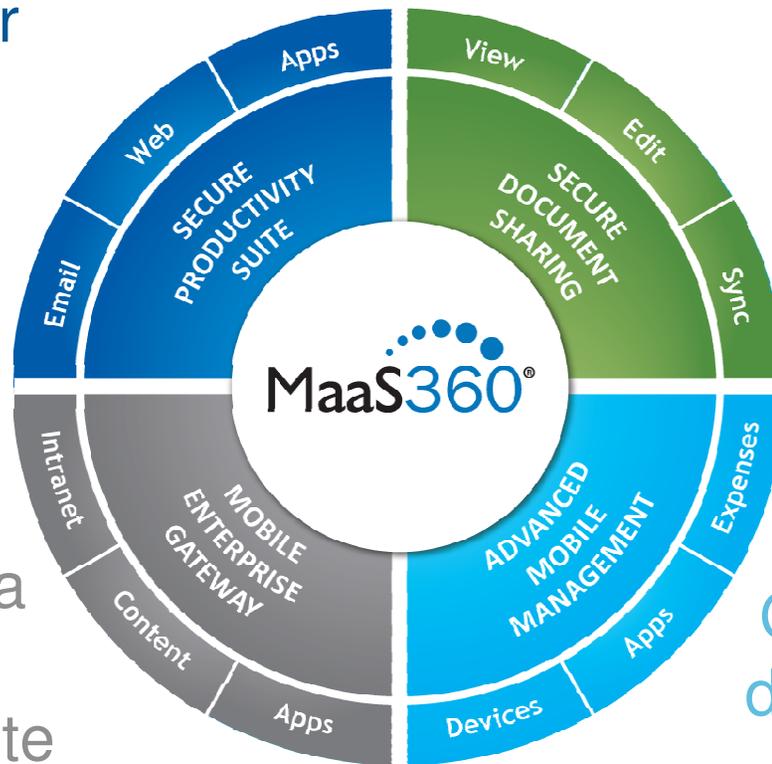
... que quieren permitir contenido corporativo en sus dispositivos de forma segura

... Y MAS

MaaS360 proporciona un acercamiento integrado

Contenedor Seguro

Contenido de colaboración seguro

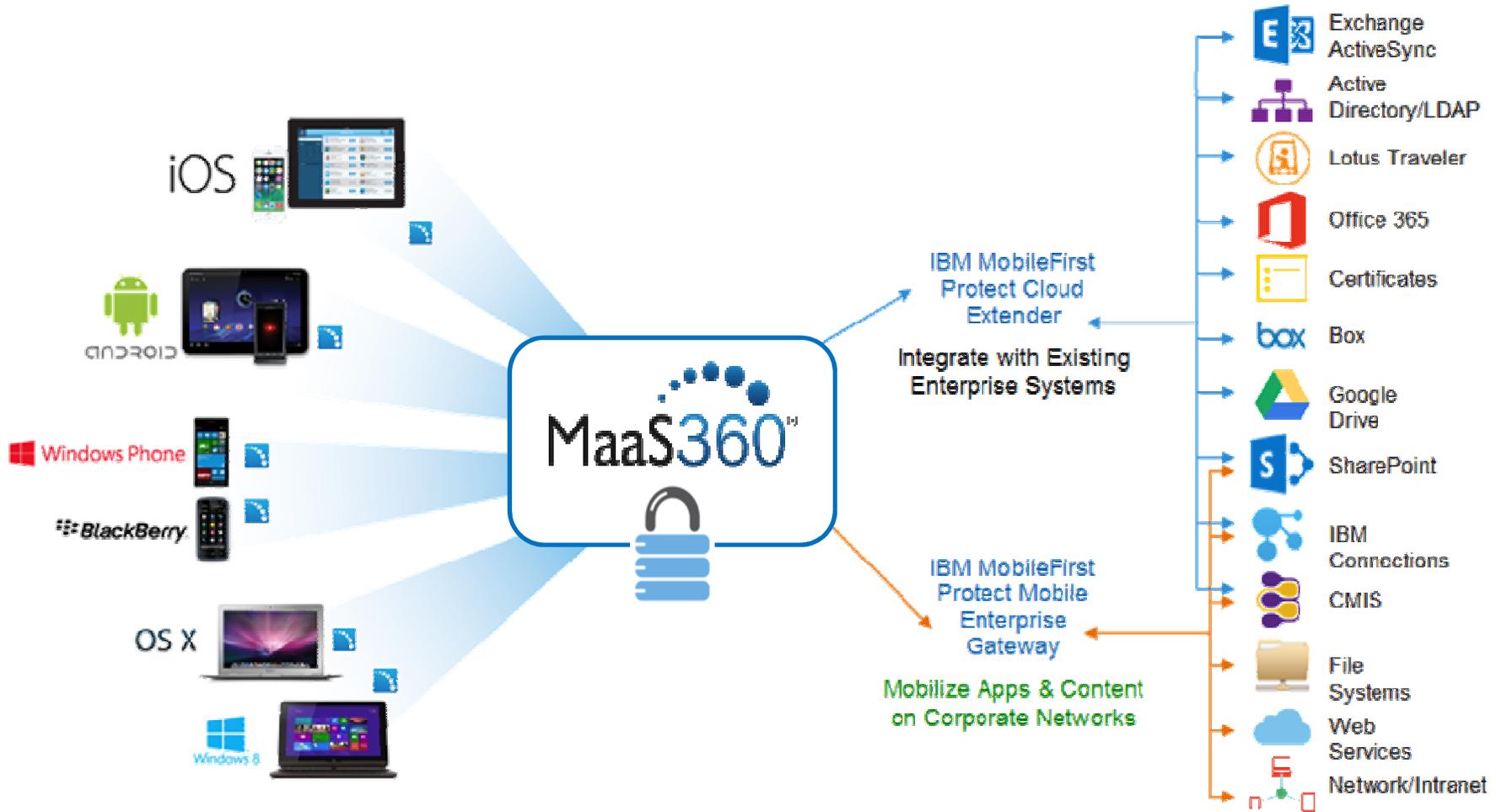


Acceso a la empresa transparente

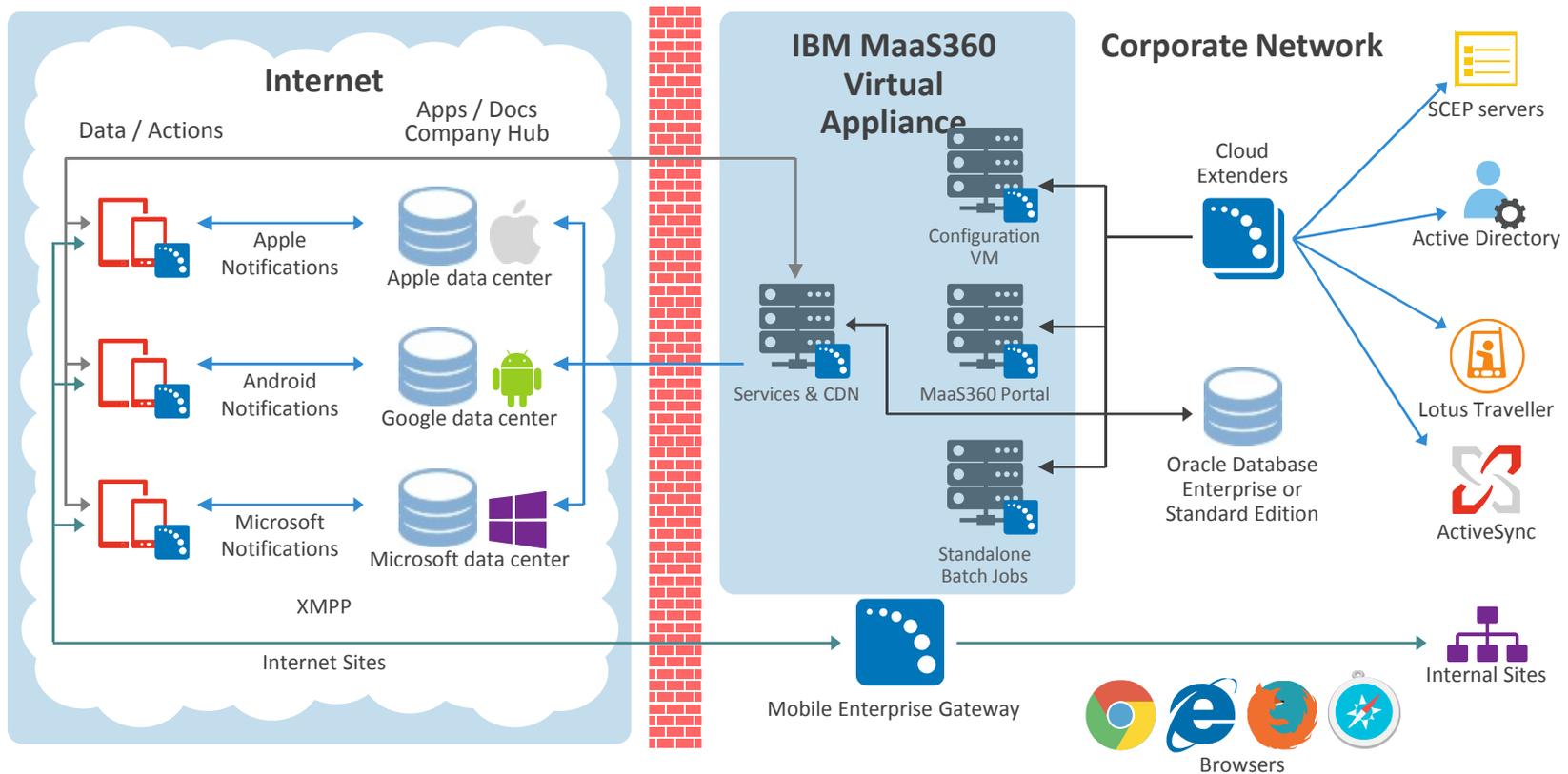
Gestión integral de dispositivos móviles

Una plataforma para todos los activos móviles

MaaS360: Arquitectura SaaS



MaaS360: Arquitectura On-Premises



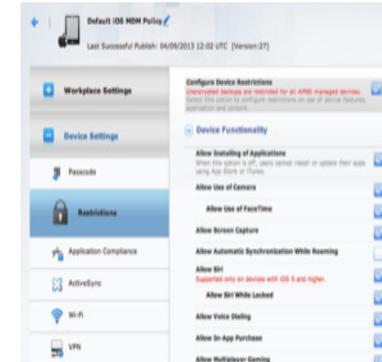
Potente gestión de dispositivos móviles

Gestión básica

- Registro por SMS, email, URL
- Perfiles de Email, calendario y contactos
- Configuraciones de VPN y Wi-Fi
- Configuración de características de dispositivos
- Actualizaciones y cambios de políticas
- Gestión de inventario
- Informes de cumplimiento



Registro de dispositivos,



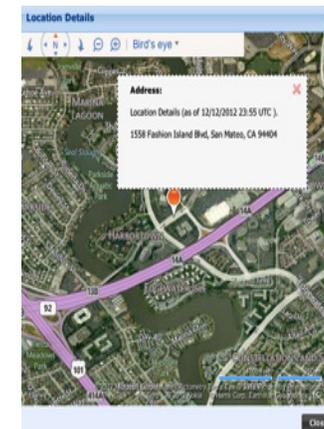
Configuración OTA

Gestión avanzada

- Gestión de aplicaciones móviles
- Compartición de documentos
- Políticas basadas en eventos
- Controles de gastos proactivos
- Configuración de privacidad para BYOD
- Soporte de dispositivos compartidos
- Portal auto-servicio



Enterprise App Catalog



Políticas basadas en localización

Robusta seguridad de entornos móviles



MaaS360 Secure Productivity Suite

Contenedor para separar datos de uso personal del profesional

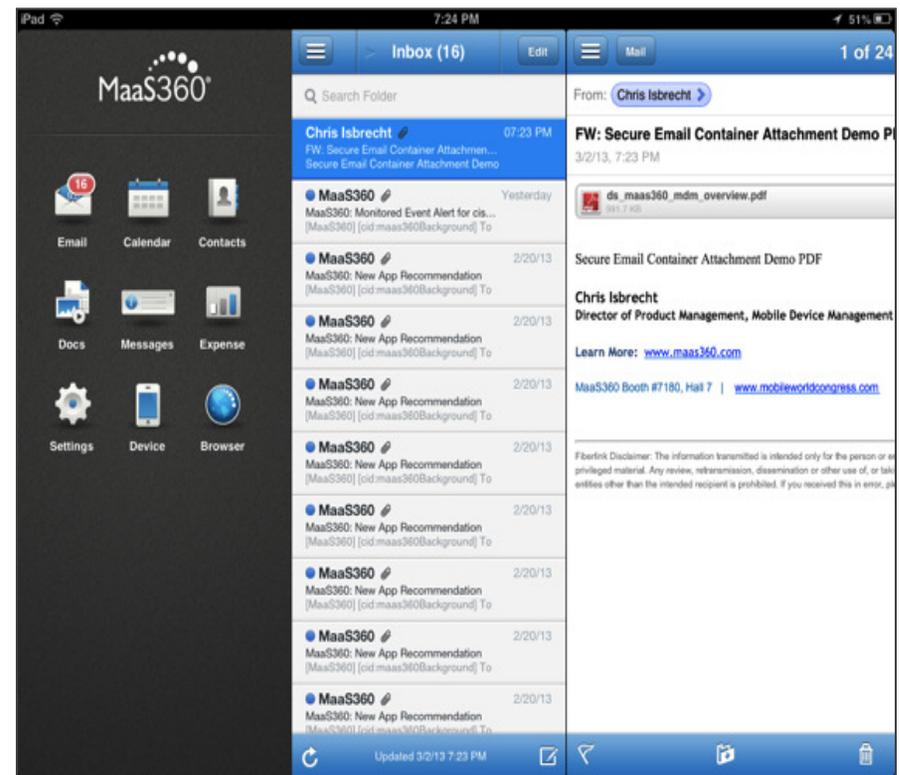
- Correo seguro
- Aplicaciones securizadas
- Compartición de Documentos segura
- Navegador seguro



Correo seguro

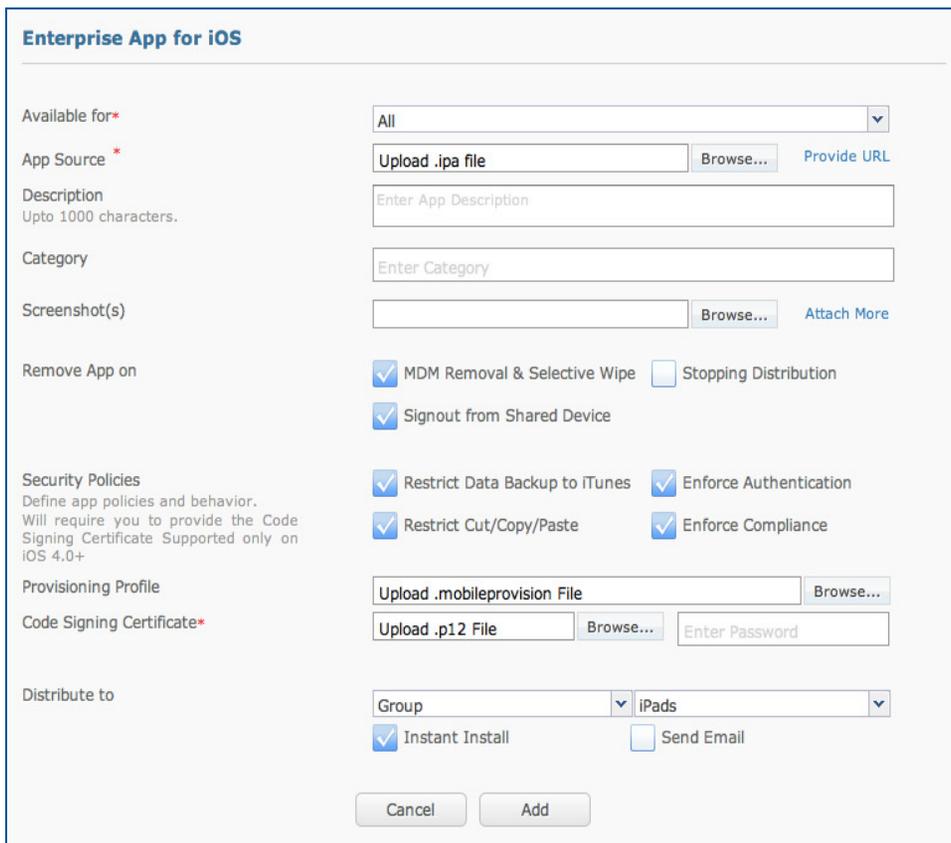
Aplicación con correo, calendarios y contactos

- Contiene la información de correos y ficheros adheridos para prevenir pérdidas de datos
- Cumple FIPS 140-2 y cifrado de 256 bits AES-256 para los datos
- Restricción de reenvíos, traspasos y capturas de pantalla
- Cheques de cumplimiento on-line y off-line antes de acceder al correo
- Refuerza la autenticación, restricciones de copiado/pegado y con el modo sólo visualización



Aplicaciones securizadas

Un contenedor de aplicaciones con gestión operacional y de seguridad para protegerse contra pérdidas de información no deseadas



Enterprise App for iOS

Available for*

App Source* [Provide URL](#)

Description
Upto 1000 characters.

Category

Screenshot(s) [Attach More](#)

Remove App on
 MDM Removal & Selective Wipe Stopping Distribution
 Signout from Shared Device

Security Policies
Define app policies and behavior.
Will require you to provide the Code Signing Certificate Supported only on iOS 4.0+
 Restrict Data Backup to iTunes Enforce Authentication
 Restrict Cut/Copy/Paste Enforce Compliance

Provisioning Profile

Code Signing Certificate*

Distribute to
Group Instant Install Send Email

- Autenticación de usuarios
- Acceso no permitido en dispositivos comprometidos
- Alerta a los administradores acerca de violaciones
- Acciones automáticas
- Restricciones de cortado/copiado/pegado
- Limitación de backup de datos a iTunes

Compartición de Documentos segura

Un contenedor de documentos securizado con soporte de usuarios extendido

- Distribución segura de documentos directa al contenedor
- Autenticación de usuarios forzada
- Permite a los usuarios editar y compartir ficheros adheridos
- Añadir, sincronizar y borrar documentos
- Proteger documentos sensibles con controles de DLP
- Integración con SharePoint y otros repositorios de ficheros
- Trabaja con el correo seguro para facilitar la visualización y seguridad de los ficheros adheridos



Add Documents
All Docs

Available for:

Select Files *
Multiple file selection (up to 15) supported. Selected folders will be ignored.

Document Names *

Tags

Security Settings
Define security settings for selected documents. Supported only on iOS.

Download Policies
Configure download policies for documents. Supported on iOS only.

Distribute to

Restrict Share

Password Protected

Download Automatically Download only on Wi-Fi

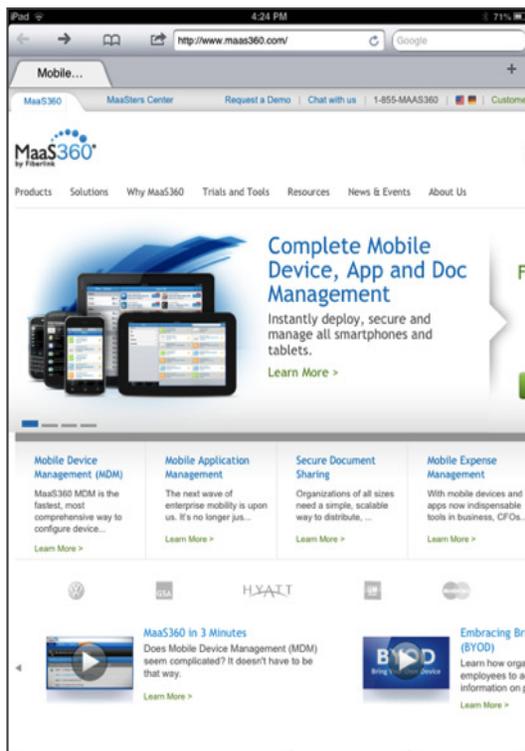
Hide Doc Preview in App Restrict Delete after Download

Group: Android Devices:

Enter expiration date:

Navegador seguro

Un navegador web completamente funcional para reforzar el cumplimiento de políticas y el control de acceso a contenidos



- Permite definir filtros de URLs y políticas de seguridad basadas en categorías de contenidos
- Bloquea sitios web conocidos como maliciosos
- Permite establecer excepciones a listas blancas de direcciones para sitios específicos
- Permite acceso a sitios de la intranet corporativa
- Permite restringir cookies, descargas, copiado, pegado e impresión para prevenir fugas de datos
- Permite deshabilitar navegadores web nativos o de terceros
- Alertas e informes personalizables

Página inicial – Centro de Alertas

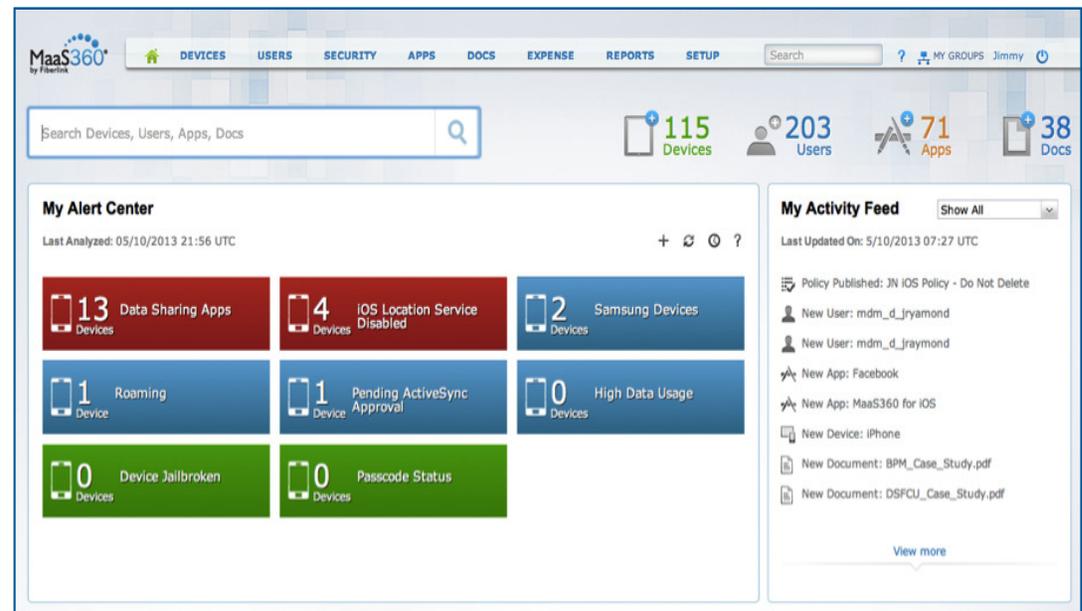
Portal para una experiencia elegante y eficiente

Centro de Alertas para disponer de un cuadro de mandos interactivo y personalizable

Centro de Actividades para disponer de las anotaciones de las acciones realizadas

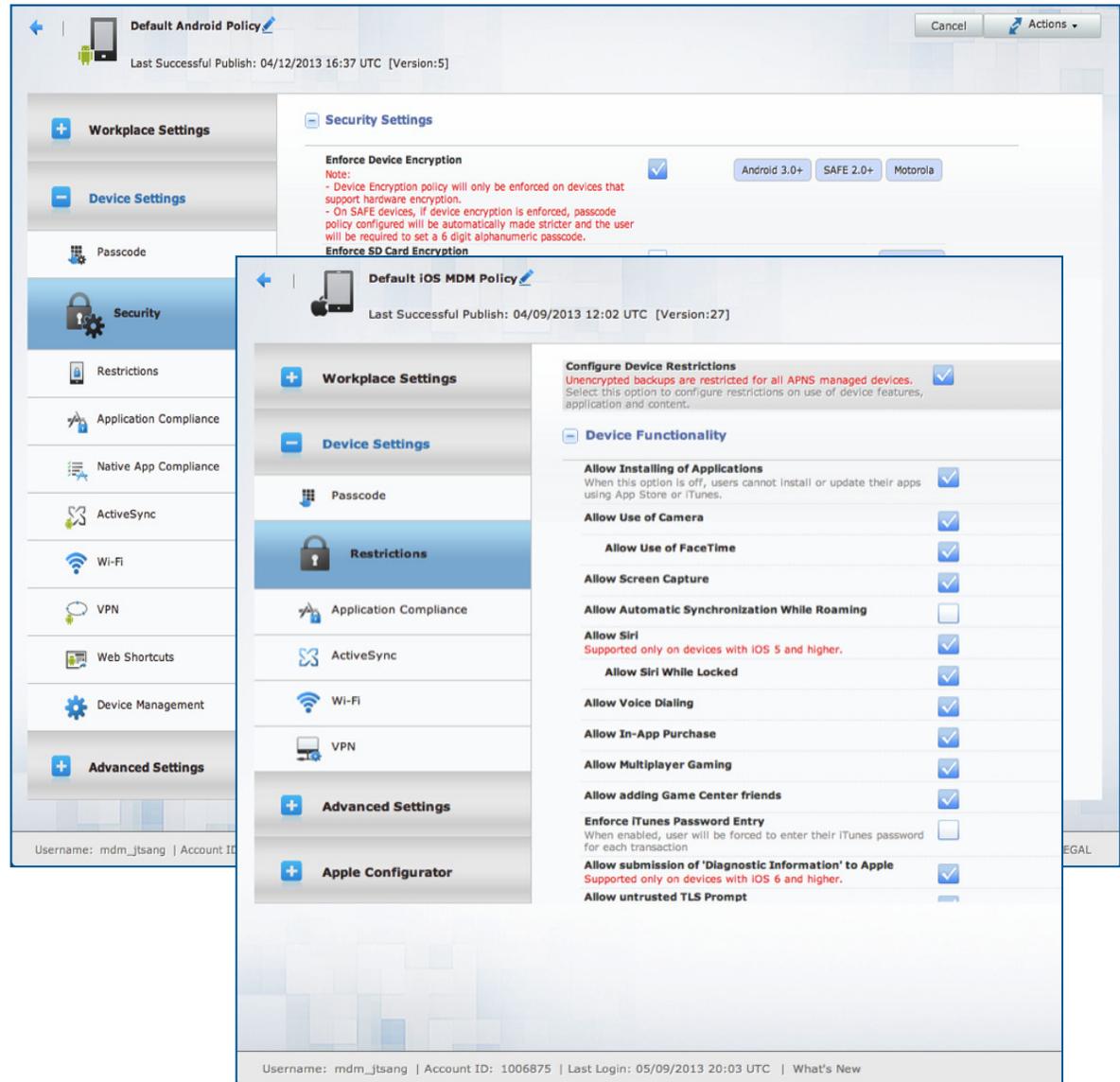
Perspectiva de dispositivos, usuarios, aplicaciones y documentos

Barra de búsqueda y acciones



Gestión de Configuración OTA

- Configuración de claves
- Correo corporativo, calendario y contactos
- Perfiles Wi-Fi y VPN
- Restricciones del dispositivo:
 - Cámara
 - FaceTime
 - Siri
 - iCloud
 - Capturas de pantalla
 - ...
- Cumplimiento de aplicaciones
- Configuración de Roaming
- Agrupación de dispositivos



Gestión de Eventos contextual

Perfiles basados en localización

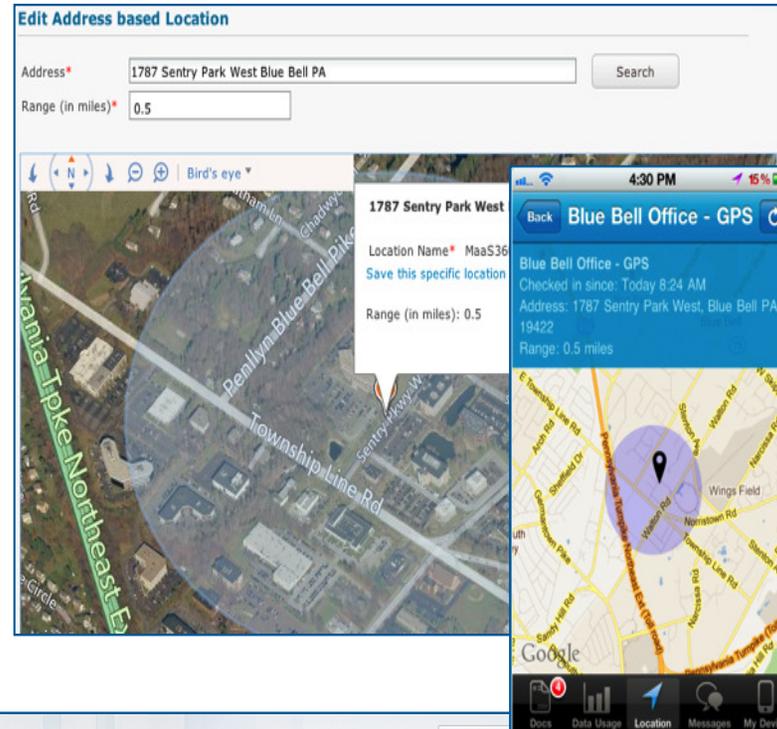
- Localización física
- Conexión de red (p.e. SSID)

Asignación dinámica de políticas

- Cambiar política mediante la entrada o salida de una localización específica

Reglas de perímetro geográfico

- Tomar acciones si:
 - El dispositivo deja una localización
 - El dispositivo entra en una localización



Locations

1. In order to use location based functionality, devices must be enrolled and have the respective agent or application installed.
 2. Add a location by specifying a physical address or by identifying Wi-Fi network details.

Location Name	Location Info	Policy Rules	Last Updated By	Last Updated On	Actions
London Airport	Address: heathrow Airport Range (in miles): 1.0	iOS : All Pilots : UK Demo iOS Policy - with Asavie VPN	mdm_jnielsen	01/23/2013 20:39 U...	-----Select Action-->
MaaS360 - Blue Bell	Address: 1787 Sentry Park West Blue Be... Range (in miles): 0.5	-	mdm_jnielsen	01/26/2013 23:19 U...	-----Select Action-->
MaaS360 - San Mateo	Address: 1510 Fashion Island Blvd., Suit... Range (in miles): 0.25	-	mdm_jnielsen	01/26/2013 23:20 U...	-----Select Action-->
MaaS360 - Philadelp...	Address: 1601 Cherry Street 20th Floor ... Range (in miles): 0.25	-	mdm_jnielsen	01/26/2013 23:20 U...	-----Select Action-->
Naval Air Station Oc...	Address: 1750 Tomcat Blvd. Virginia Bea... Range (in miles): 4.5	iOS : CB - devices : iOS Disable Camera	mdm_cbrown	04/30/2013 12:01 U...	-----Select Action-->
YH 158	Address: 158 s eagle rd, havertown, pa Range (in miles): 0.5	-	vhetrick	04/09/2013 15:32 U...	-----Select Action-->
Fiberlink Visitor Net...	Wi-Fi SSID: fVisitor MAC Address: -	iOS : jnielsen Devices : JN iOS Policy - Do Not Delete	mdm_jnielsen	05/09/2013 13:17 U...	-----Select Action-->

First Previous | Next Last Showing 1 to 7 of 7 entries

Opciones de privacidad para BYOD

Deshabilitan la recogida de información personal de un dispositivo, grupos o todos los dispositivos

- Información de inventario de aplicaciones
- Información de localización
- Dirección IP y SSID

Privacy Settings

View Change History
Save

➤ **Restrict Location Information**
 Restrict administrators from collecting location indicators such as Physical Address, Geographical Coordinates & History, IP Address and SSID.

Select Applicable Ownership Types

Corporate owned
 Unknown

Employee owned

Select Applicable Device Group: All Devices

➤ **Restrict App Inventory Information**
 Restrict administrators from collecting personal App information. Apps distributed via the enterprise app catalog or part of corporate security policy will continue to be tracked.

Select Applicable Ownership Types

Corporate owned
 Unknown

Employee owned

Select Applicable Device Group: All Devices

Gestión de aplicaciones móviles

Catálogo de aplicaciones corporativas

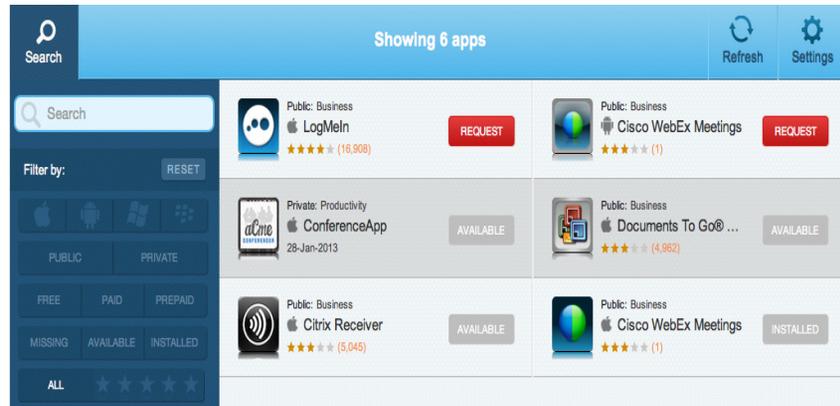
Gestión de seguridad y cumplimiento

Distribución y actualización de aplicaciones

Borrado selectivo de aplicaciones gestionadas

Gestión de programas de compras por volumen

Almacenamiento en la nube para hosting y distribución



App	Name	Type	Category	VPP Codes	Installs	Distributions	Last Updated
	ConferenceApp View Distribute Delete More...		Others		9	Yes	03/13/2013 21:05 UTC
	MaaS iOS App View Distribute Delete More...		Others		9	Yes	03/12/2013 18:34 UTC
	Corp Web Site View Distribute Delete More...		Business		5	Yes	01/09/2013 21:04 UTC
	MaaS360 Secure Browser View Distribute Delete More...		Business		4	Yes	02/06/2013 19:33 UTC
	MaaS360 Secure Browser View Distribute Delete More...		Business		3	Yes	01/28/2013 22:40 UTC
	Cisco WebEx Meetings View Distribute Delete More...		Business		3	Yes	01/27/2013 16:34 UTC
	Keynote View Distribute Delete More...		Productivity	0 Available	3	Yes	03/15/2012 18:39 UTC
	Cisco WebEx Meetings View Distribute Delete More...		Business		2	Yes	03/09/2013 05:37 UTC
	iCorpPassLite - Windows Domain Passwor... View Distribute Delete More...		Business		2	Yes	02/19/2013 15:03 UTC
	Skype View Distribute Delete More...		Social Networking		2	Yes	07/05/2012 18:43 UTC

Displaying 1 - 10 of 71 Records

Total Space Available: 25 GB | Free Space Remaining: 24.75 GB

Gestión de Documentos

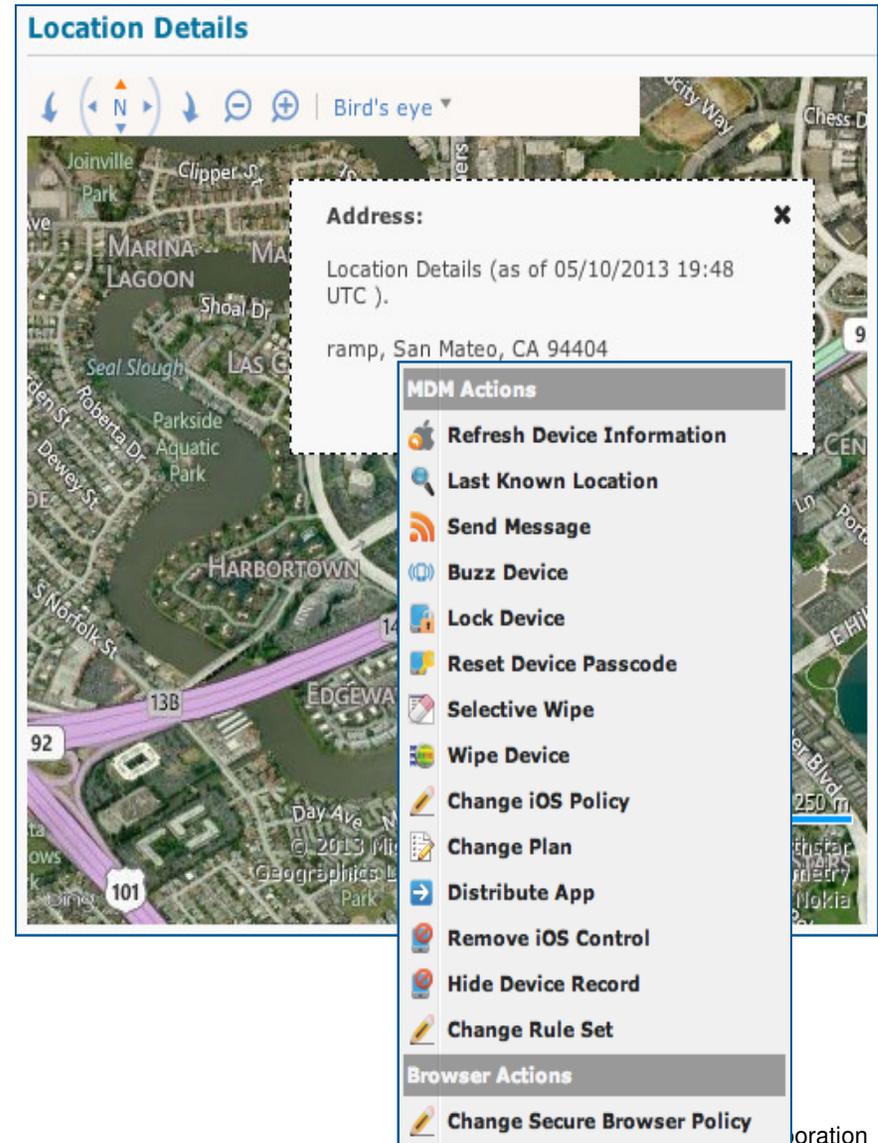


- Aplicación de catálogo de documentos para iOS y Android
- Gestión centralizada de la distribución
- Autenticación basada en usuarios para el acceso
- Notificación a los usuarios de contenido nuevo o actualizado
- Restricciones de cortado/copiado/pegado y modo de sólo visualización
- Versionados y expiraciones por tiempo
- Integración con SharePoint
- Almacenamiento en la nube para hosting y distribución

Search Results: Content Library: All Docs				
Document	Available for	Type	File Size	Tags
MaaS360 Datasheets Edit Distribute Delete	All		19.14 MB	maas360
Sample MOV File Edit Distribute Delete	All		3.13 MB	Others
Brokerage Accounts Edit Distribute Delete	All		22.7 KB	Others
iPAD Background Image Edit Distribute Delete	All		60.38 KB	Others
MaaS360_Mac_MDM_Data_Sheet Edit Distribute Delete	All		389.59 KB	maas360
Mobile Policies Edit Distribute Delete	All		66.52 KB	Others

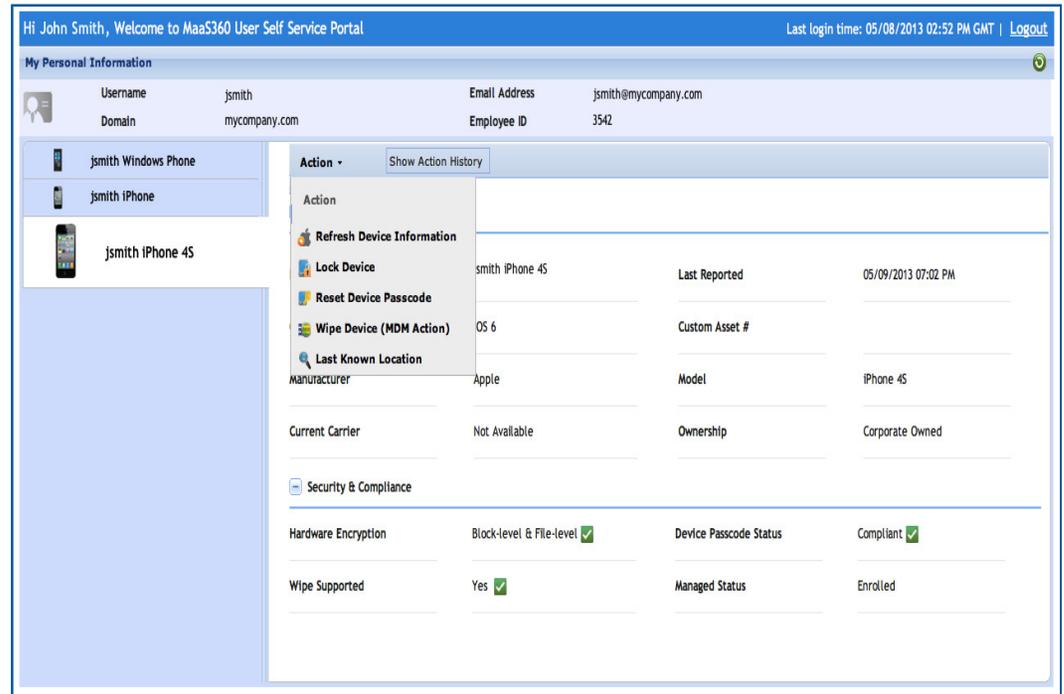
Ayudas a soporte remoto

- Inicialización de claves por olvido
- Localización de dispositivos perdidos
- Alarma en dispositivo perdido
- Borrado selectivo
- Borrado completo
- Envío de mensajes message
- Cambio de políticas
- Quitar el control del dispositivo



Portal de autoservicio de usuarios

- URL específica para portal de auto-servicio
- Autenticación via AD o usuarios locales
- Toma de acciones sobre los dispositivos:
 - Bloquear dispositivo
 - Inicialización de clave
 - Localización
 - Borrado
 - Histórico de acciones
- Vista de dispositivos personales y corporativos
 - Vista de información de hardware y redes
 - Vista de estado de seguridad y cumplimiento



Hi John Smith, Welcome to MaaS360 User Self Service Portal Last login time: 05/08/2013 02:52 PM GMT | [Logout](#)

My Personal Information

Username	jsmith	Email Address	jsmith@mycompany.com
Domain	mycompany.com	Employee ID	3542

Devices

- jsmith Windows Phone
- jsmith iPhone
- jsmith iPhone 4S

jsmith iPhone 4S

Action - Show Action History

Refresh Device Information

Lock Device

Reset Device Passcode

Wipe Device (MDM Action)

Last Known Location

Device	smith iPhone 4S	Last Reported	05/09/2013 07:02 PM
OS	OS 6	Custom Asset #	
Manufacturer	Apple	Model	iPhone 4S
Current Carrier	Not Available	Ownership	Corporate Owned

Security & Compliance

Hardware Encryption	Block-level & File-level <input checked="" type="checkbox"/>	Device Passcode Status	Compliant <input checked="" type="checkbox"/>
Wipe Supported	Yes <input checked="" type="checkbox"/>	Managed Status	Enrolled

Informes y cuadros de mando

Cuadros de mando en tiempo real e interactivos para mostrar vistas gráficas del entorno móvil y sus estados de seguridad y cumplimiento



Sobre Trusteer

 Global	Cientos de Clientes 140,000,000 Endpoints
 Solutions	Prevención Cybercrime para Clientes y Empleados
 Leader	Inteligencia Tecnología Experiencia

Organizaciones Global Punteras CONFIAN en Nosotros

7/10 Top US Banks 	9/10 Top UK Banks
4/5 Top Canadian Banks 	Grandes European Banks

Trusteer hace foco en los vectores de ataque prevalentes en el CyberCrimen actual – fraude online, robo de credenciales y datos

Fraude Web

The diagram illustrates a web fraud attack. At the top, a red silhouette of a criminal with a mask and a red hat is shown. Three arrows point down from this criminal to three circular icons: a red circle with a white envelope and a red circle with a white bug, and another red circle with a white bug. These icons are positioned around a central illustration of a customer's devices: a laptop, a smartphone, and a green silhouette of a person. Labels include 'Credential Theft', 'Account Takeover', 'Automated Malware-driven Fraud', and 'Mobile Malware'. Below the customer's devices, a red arrow points down to a server rack icon labeled 'Banking and E-Commerce Applications'. A red arrow also points from the criminal to the server rack, labeled 'Fraud from Customer or Criminal Device'.

Customer

Banking and E-Commerce Applications

El primer objetivo es el cliente. Malware instalado en su PC y dispositivo móvil puede generar transacciones fraudulentas. Además, malware y phishing ayudan a los atacantes a robar credenciales y otros datos personales

Seguridad Enterprise

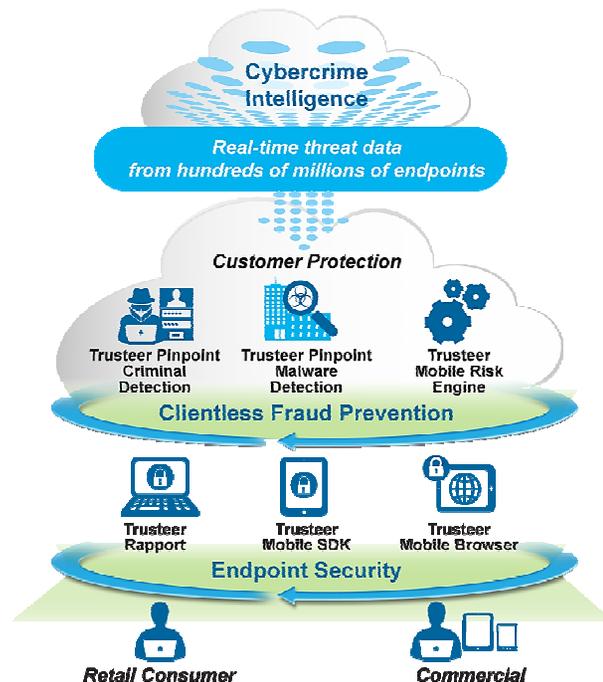
The diagram illustrates an enterprise security attack. At the top, a red silhouette of a criminal with a mask and a red hat is shown. Three arrows point down from this criminal to three circular icons: a red circle with a white envelope, a red circle with a white bug, and another red circle with a white bug. These icons are positioned around a central illustration of an employee's workstation: a laptop and a blue silhouette of a person in a suit. Labels include 'Spear-Phishing: Credential Theft', 'Malware Infection:', and 'Endpoint Remote Control'. Below the employee's workstation, an orange arrow points down to a server rack icon labeled 'Enterprise Applications & Data'. An orange arrow also points from the criminal to the server rack, labeled 'Targeted attacks and Advanced Persistent Threats'.

Employee

Enterprise Applications & Data

Un nuevo objetivo en alza son los empleados. Los criminales usan spear-phishing email para atacar a empleados y desplegar malware en sus endpoints. Los atacantes usan este malware para acceder a los sistemas y extraer datos de la empresa

MaaS360 Mobile Threat Management Incorpora tecnología Trusteer



Clientless Fraud Prevention

- **Trusteer Pinpoint Criminal Detection**
Conclusive detection of criminals and account takeover attempts
- **Trusteer Pinpoint Malware Detection**
Accurate, real-time malware detection
- **Trusteer Mobile Risk Engine**
Conclusive detection of mobile-fraud risks from compromised end user and criminal-owned devices

Endpoint Security

- **Trusteer Rapport**
Prevents and removes financial malware and detects phishing attacks
- **Trusteer Mobile SDK**
Embedded security library for native apps that detects compromised / vulnerable devices
- **Trusteer Mobile Browser**
Secure, risk-based mobile web access
- **Trusteer Apex**
Advanced threat detection and mitigation / Corporate credential protection

MaaS360 utiliza el Cloud Service de Trusteer para proporcionar Detección de Malware, Jailbreak & Root



- Incorporado en el MaaS360 Mobile App / Container
- Aprovecha detección de malware para configuración de cumplimiento y remediación

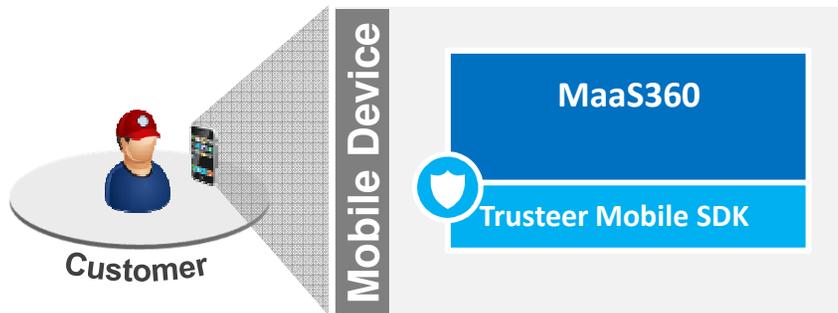
Caso de Uso #1 – Protección Integrada

Valor:

- Impedir el despliegue de contenedores en un dispositivo jailbroken or rooteado
- Restringir la compartición de contenido entre apps enterprise en dispositivos infectados por malware



1. Integrate Libraries within app code
2. Code the ability to collect data
3. Analyze risk Data
4. Send Data to Server
5. Enforce Policy

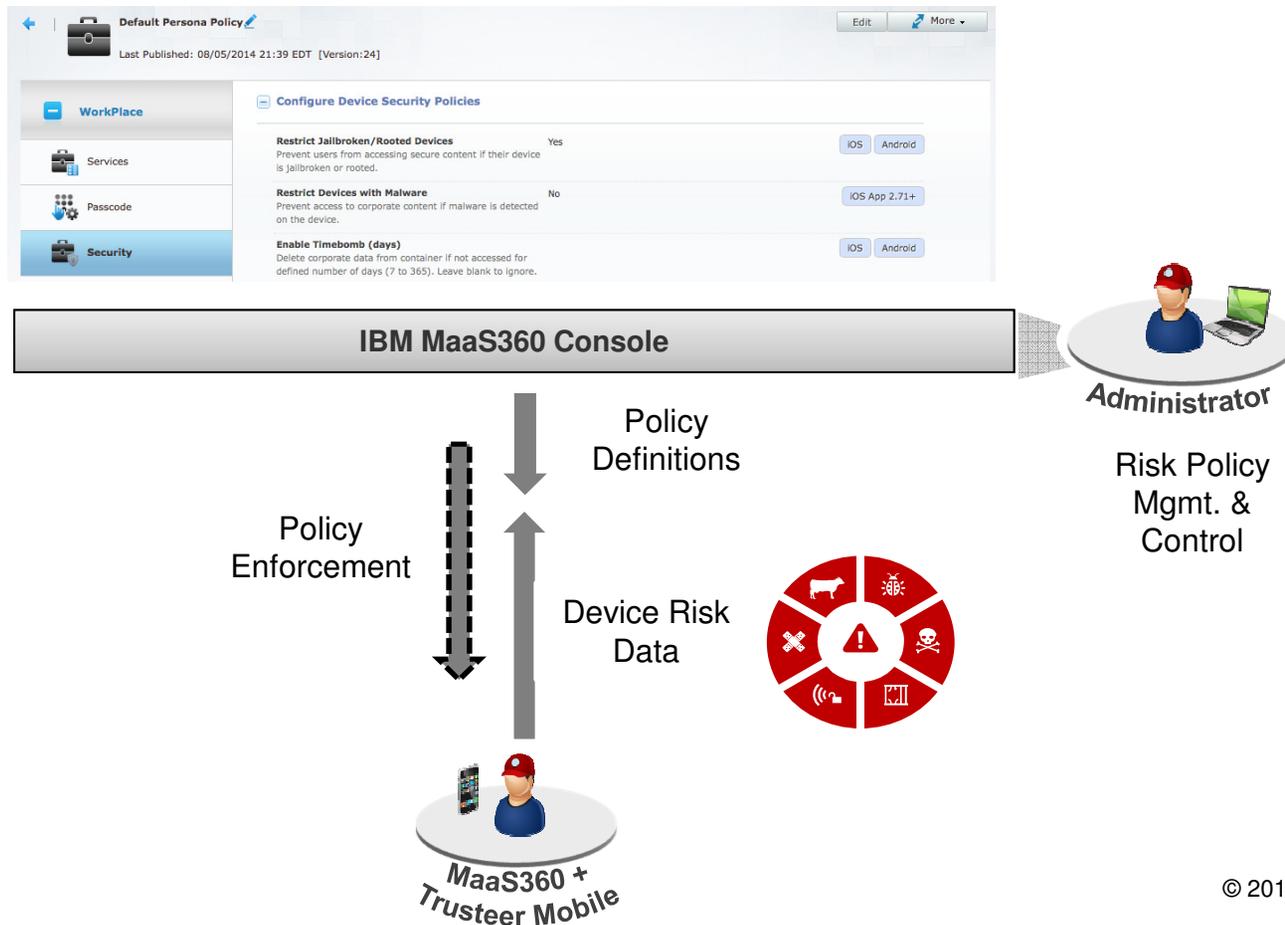


- Jailbroken/Rooted
- Jailbreak Hiders
- Malware Infection
- Suspicious Apps
- Persistent Device ID
- Geo-location
- Unpatched OS
- Unsecure Wi-Fi

Caso de Uso #2 – Implementar Políticas Granulares

Valor:

- Reduce el riesgo de que malware capture datos sensibles
- Restringir acceso a (algunos) recursos enterprise vía Maas360 browser
- Automáticamente eliminar malware en dispositivos Android específicos



IBM Deploys 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+ Devices enrolled per minute*

<500 Help Desk calls – less than 1/2 of 1%

*at high point

About Infrastructure in SPGI

Together with the IGA organisation we do manage :



Workstation provisioning and support

Voice services (fixed, mobile, BYOD)

Legacy applications maintenance and support

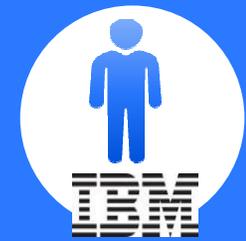
End user support **1.200** monthly tickets per country
5.000 weekly chats in Europe



More than **50** Mobile Applications (increasing number) are available at the **IBM MaaS360 App Catalog**



7.800
Employees supported



10.300 Workstations



200 Local legacy applications



5.400 Corporate mobile phones



11.700 fixed phone lines



Diverse Customer Base

Manufacturing

Healthcare

Consumer

Financial

Public

Others



BNY MELLON



Licenciamiento y comercialización

IBM MAAS360 ADVANCED MOBILE MANAGEMENT SUITE

- IBM MAAS360 MOBILE DEVICE MANAGEMENT
- IBM MAAS360 MOBILE APPLICATION MANAGEMENT
- IBM MAAS360 MOBILE EXPENSE MANAGEMENT

IBM MAAS360 SECURE PRODUCTIVITY SUITE

- IBM MAAS360 MOBILE APPLICATION SECURITY
- IBM MAAS360 SECURE MAIL
- IBM MAAS360 SECURE BROWSER

IBM MAAS360 SECURE DOCUMENT SHARING SUITE

- IBM MAAS360 MOBILE CONTENT MANAGEMENT
- IBM MAAS360 SECURE DOCUMENT SYNC
- IBM MAAS360 SECURE EDITOR

IBM MAAS360 MOBILE ENTERPRISE GATEWAY SUITE

- IBM MAAS360 MOBILE ENTERPRISE GATEWAY FOR APPS
- IBM MAAS360 MOBILE ENTERPRISE GATEWAY FOR SECURE BROWSER
- IBM MAAS360 MOBILE ENTERPRISE GATEWAY FOR DOCUMENTS

IBM MAAS360 ENTERPRISE SERVER MANAGEMENT FOR BLACKBERRY

IBM MAAS360 MOBILE THREAT MANAGEMENT

¿Cómo empezar?

1

Al instante

Acceso a una licencia de prueba de 30 días gratis y plenamente funcional

2

Fácil

Configuración del servicio en minutos



3

Móviles

Gestión y securización de los dispositivos, correos, aplicaciones y documentos



maas360.com

