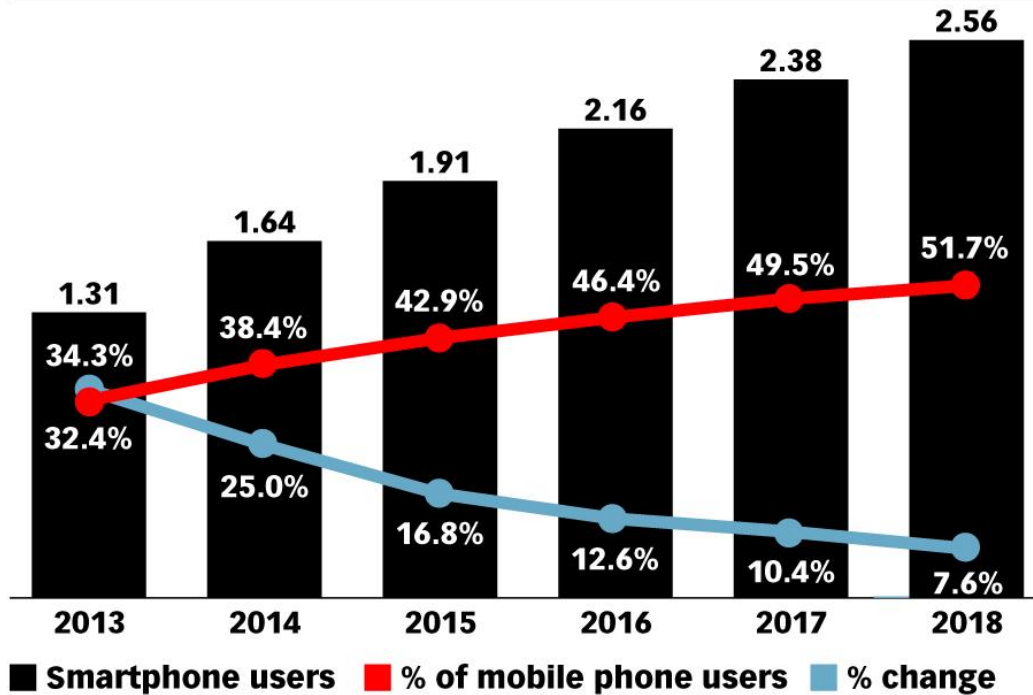


Smartphone Users and Penetration Worldwide, 2013-2018

billions, % of mobile phone users and % change



Note: individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month

Source: eMarketer, Dec 2014

182903

www.eMarketer.com

MORE TIME ON MOBILE DEVICES

There are 175 million Americans with at least one mobile device and they are devoting more time to them. Minutes spent on devices:

Q1 2013

158

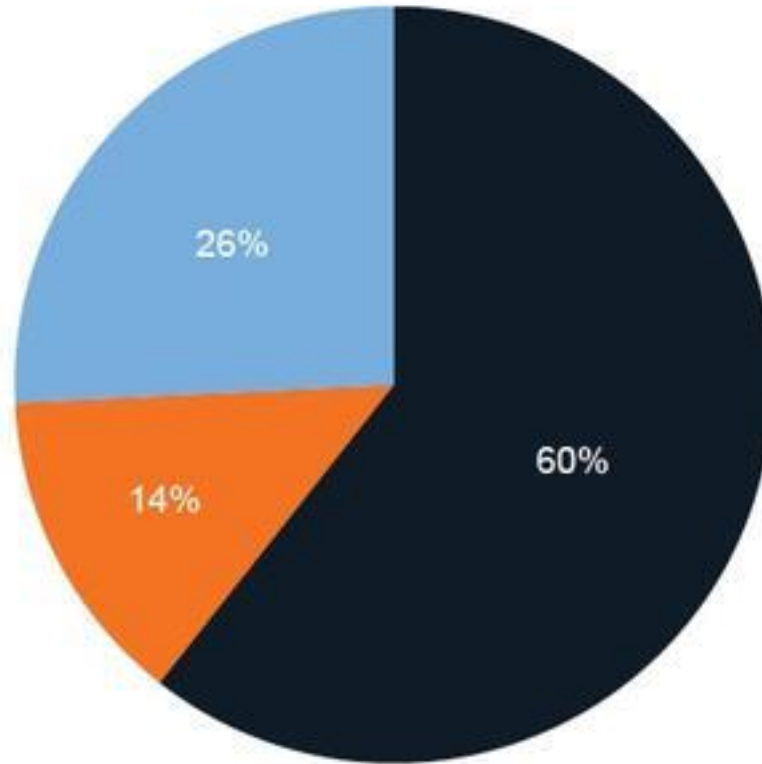
Q1 2014

162

Q1 2015

220

DOES YOUR ORGANIZATION CURRENTLY ALLOW BYOD?

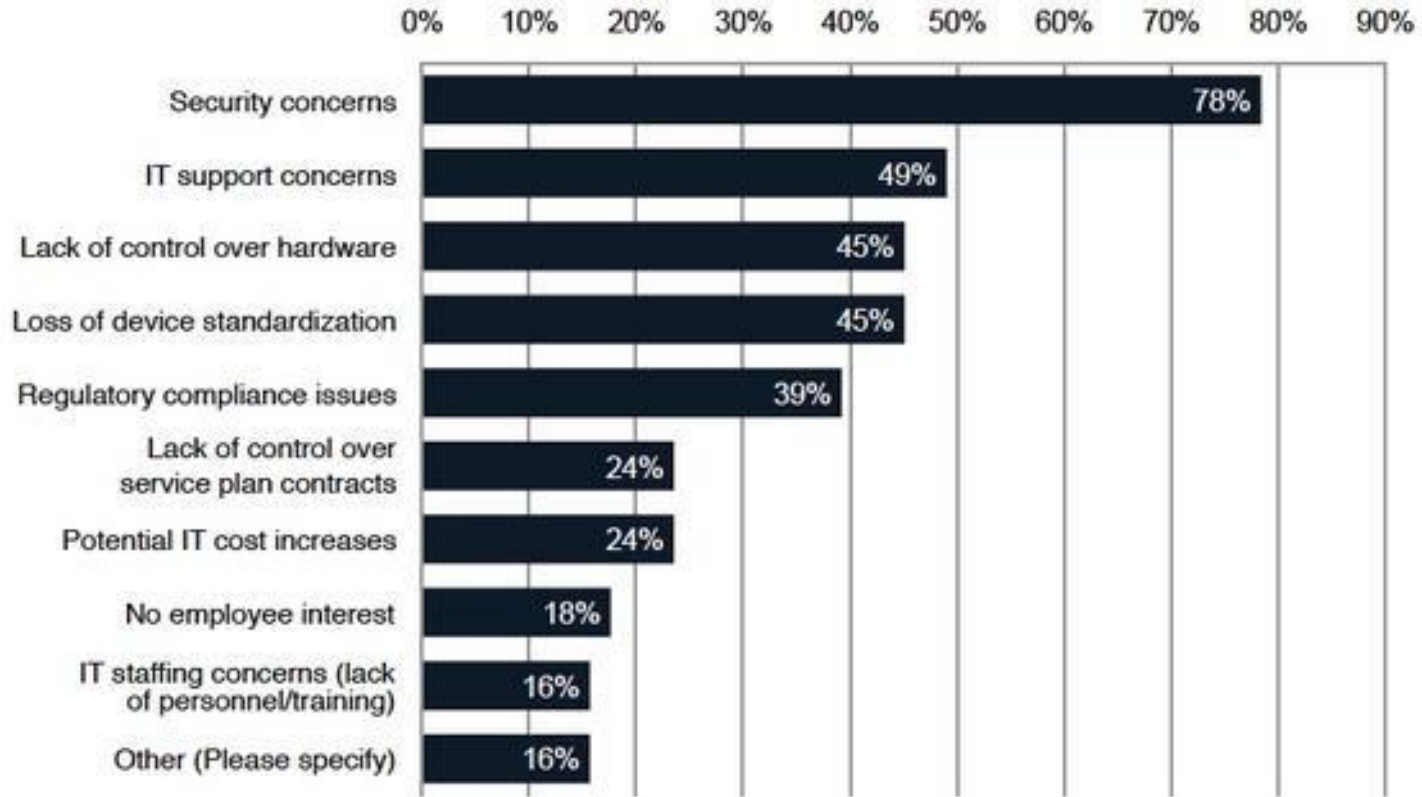


- Yes, we currently allow the use of personal devices for work purposes (i.e. to access company networks and data)
- We do not currently allow, but within the next 12 months we plan to begin allowing the use of personal devices for work purposes
- No, we have no plans to allow the use of personal devices for work purposes

Number of respondents, n=198

Fuente: Tech Pro Research Enero 2015

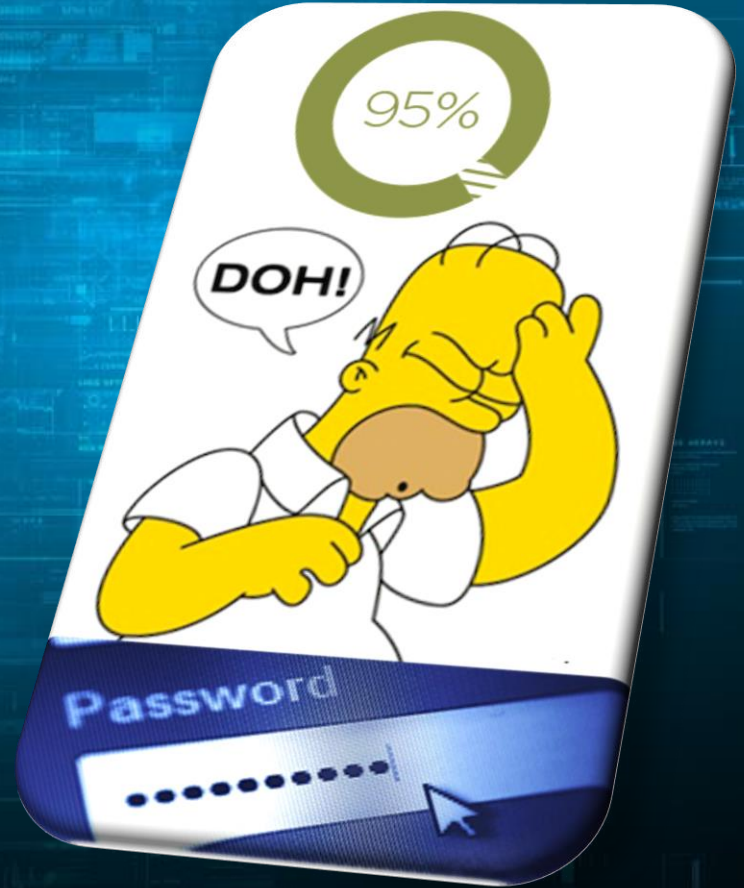
REASONS FOR RULING OUT THE BYOD CONCEPT



Number of respondents, n=51

Fuente: Tech Pro Research Enero 2015

Preocupaciones asociadas a la seguridad



Preocupaciones asociadas a la seguridad

Today's large companies* each spend an average of **\$34 million annually** to develop mobile apps we use to shop, bank and more.

However, only an average of **5.5% of this immense budget** is spent on securing these apps against hackers and security breaches.¹

*Including many in the Fortune 500



How does this stack up against other things on which money is spent?



Shouldn't we be doing more to protect our security when using mobile apps?

40% of companies do not scan the code in their mobile apps for security vulnerabilities.¹



1 billion personal data records were compromised by cyber-attacks in 2014,⁵ and at any given time mobile malware is affecting **11.6 million** mobile devices.⁶

On average, a company tests less than half of the mobile apps they build, and

33% never test apps to ensure they're secure.¹



Fuente: IBM Security

Preocupaciones asociadas a la seguridad

TOP IDENTITY GOVERNANCE SUSPECTS

FAILED AUDITS



Managers may not understand the access they are certifying and can accidentally provide non-compliant access.

Without an audit focused solution, organizations may face a never ending audit cycle.

37% OF MASSIVE DATA BREACHES WERE CAUSED BY UNAUTHORIZED ACCESS, accounting as the primary mode of attack.

SEGREGATION OF DUTIES VIOLATIONS



Lack of visibility into "toxic combinations" while security and compliance needs are increasing.

Shortage of skilled personnel to monitor, analyze, prioritize and respond to threats.

Multinational manufacturer manages **OVER 430 MILLION POTENTIAL ENTITLEMENT CONFLICTS WITH ONLY A FEW HUNDRED SoD RULES.**

ENTITLEMENT CREEP



As users change jobs they amass more entitlements while old entitlements are never taken away.

Accounts with unnecessary entitlements are key in insider attacks.

A large European designer found that **ALMOST 80% OF THEIR USERS HAD UNNECESSARY ACCESS.**

Unauthorized access was nearly twice as prevalent in 2014 as in 2013 among the top 5 industries

37%

Unauthorized access was the primary mode of attack...

Usually denotes suspicious activity on a system or failed attempts to access a system by a user or users who do not have access

20%

...followed by sustained probes/scans...

Reconnaissance activity usually designed to gather information about the targeted systems

20%

...and malicious code

Software designed to disrupt systems, gain unauthorized access, or gather information about the system or user being attacked

Who are the "bad guys"? More than half are insiders*

* Anyone who has physical or remote access to a company's assets



45%

Outsiders



31.5%

Malicious Insiders

23.5%

Inadvertent actor



Whether they're **malicious insiders** or **inadvertent actors**, they pose a big security risk

Fuente: IBM Security

Preocupaciones asociadas a la seguridad



Preocupaciones asociadas a la gestión de los dispositivos

- En Mobile se fusionan los datos personales con los del trabajo
- En Mobile los dispositivos se mueven fuera del perímetro corporativo
- Mobile es multiplataforma
- Las Apps se actualizan automáticamente de los Apps Stores
- En Mobile las conexiones son por 3G/4G, WIFI.



Caso ficticio





Les presento a parte del equipo de la empresa!

Cuando hago los partos del martes, almuerzo con la patrona y nadie se da cuenta..

Siempre chequeo las paginas de futbol durante el día y me cuelgo con algún partido en rojadirect

Que buenos que están los nuevos videos de maquillaje en youtube... suerte que no se enteran de la selfies que me saco con con el ipad para mandárselas a mis amigas por el whats...

A veces le envío a mi sobrino los balances anuales (que vienen adjuntos al mail) así los toma de ejemplo para la facultad

Hace dos días estaba en un café en ciudad vieja y cuando salía me robaron el iPad con todos los datos de la empresa y todavía no le dije a nadie..

Mi novio le hizo jailbroken a mi iPhone así puedo bajar las apps sin pagar... el Candy Crush versión Uruguay me encanta...

“Somos una compañía de distribución de productos, hago foco en el personal y en garantizar la seguridad tanto de ellos como de los recursos corporativos. Hemos comprado varios iPads para algunos funcionarios de la empresa para aumentar la productividad. Pero me preocupa porque varios utilizan sus smartphones personales y no se cuanta cosa mas...”

Yo hace 1 mes que me fui de la empresa xq conseguí otra laburo en otro lado... todavía guardo con “cariño” algunos documentos y la app corporativa



Ing. Gerardo Pereira - Interamericana de Computos -

Solucionándole la vida al Capitán Con Mobile First Protect



IBM MobileFirst Protect

Mobile Modjo (MaaS360)

Mobile First Protect (MaaS360)



IBM MobileFirst Protect



IBM MobileFirst Protect

- o Automated Policy Compliance
- o Encryption & Data Protection
- o Authentication & Restrictions
- o Containerization & App VPN
- o Device Quarantine & Wipe



Trusteer
Mobile Threat
Management



QRadar
Risk & Event
Detection



ISAM
Mobile Identity
Access Control



BigFix
Unified Endpoint
Management



Worklight
Integrated
App Security

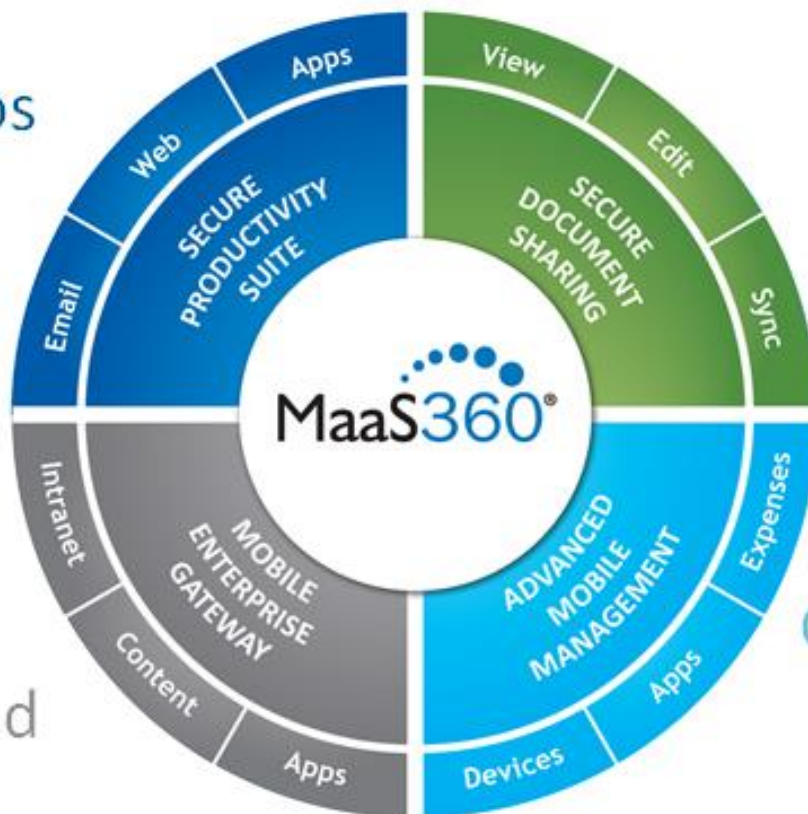


Guardium
Integrated
Data Security

MaaS360 Ofrece una integración completa

Contenidos seguros para Movilidad

Colaboración de contenidos segura



Acceso seguro y sin discontinuidad

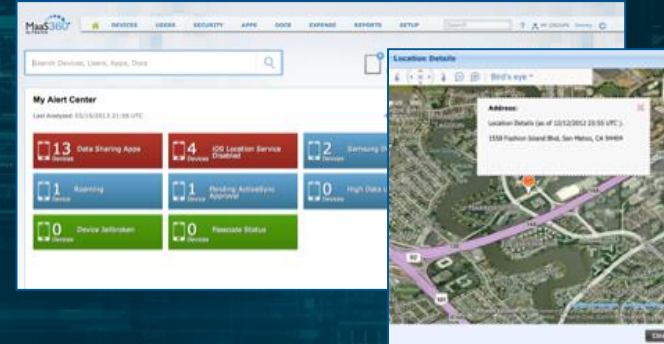
Gestión completa de la Movilidad



IBM MobileFirst Protect Management Suite

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

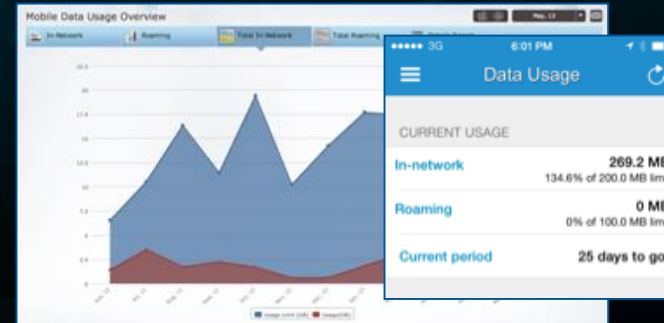


Mobile Application Management

- Deploy custom enterprise app catalogs
- Blacklist, whitelist & require apps
- Administer app volume purchase programs

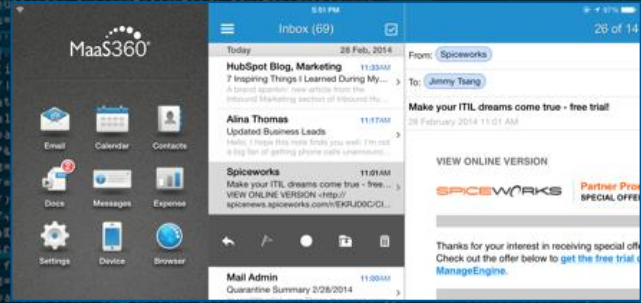
Mobile Expense Management

- Monitor mobile data usage with real-time alerts
- Set policies to restrict or limit data & voice roaming
- Review integrated reporting and analytics





IBM MobileFirst Protect Productivity Suite

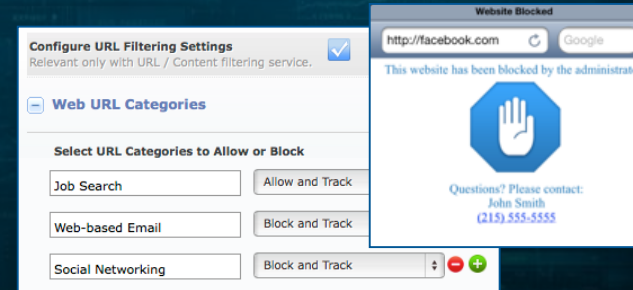


Secure Mail

- 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



- ✓ Restrict Data Backup to iTunes
- ✓ Enforce Authentication
- ✓ Enforce Compliance
- ✓ Restrict Cut/Copy/Paste
- ✓ Enforce File Protection

Application Security

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



IBM MobileFirst Protect Content Suite

Mobile Content Management

Contain documents & files to prevent data leakage

Enforce authentication, copy/paste & view-only restrictions

Access IBM MobileFirst Protect 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

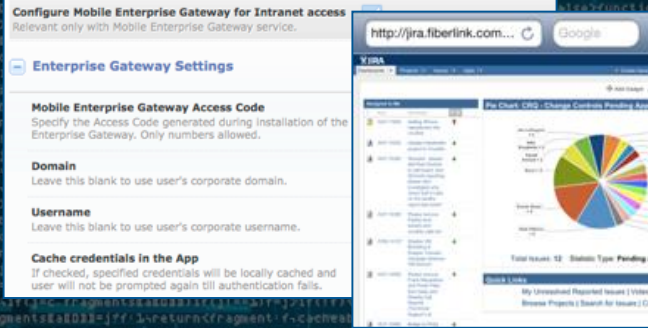
Synchronize user content across managed devices

Restrict copy/paste & opening in unmanaged apps

Store content securely, both in the cloud & on devices



IBM MobileFirst Protect Gateway Suite



Mobile Enterprise Gateway for Browser

Enable MobileFirst Protect 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 Documents

- Enhance MobileFirst Protect Content 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 per app VPN to MobileFirst Protect Application Security to integrate behind-the-firewall data in private apps
- Incorporate enterprise data without a device VPN session

IBM MobileFirst Protect Threat Management

Combina las capacidades de monitoreo de amenazas de IBM Trusteer con controles en tiempo real de MobileFirst Protect EMM dentro de una solución integrada

Detección, análisis y remediación de mobile malware y dispositivos comprometidos

Remediación automática con reglas de cumplimiento en tiempo real

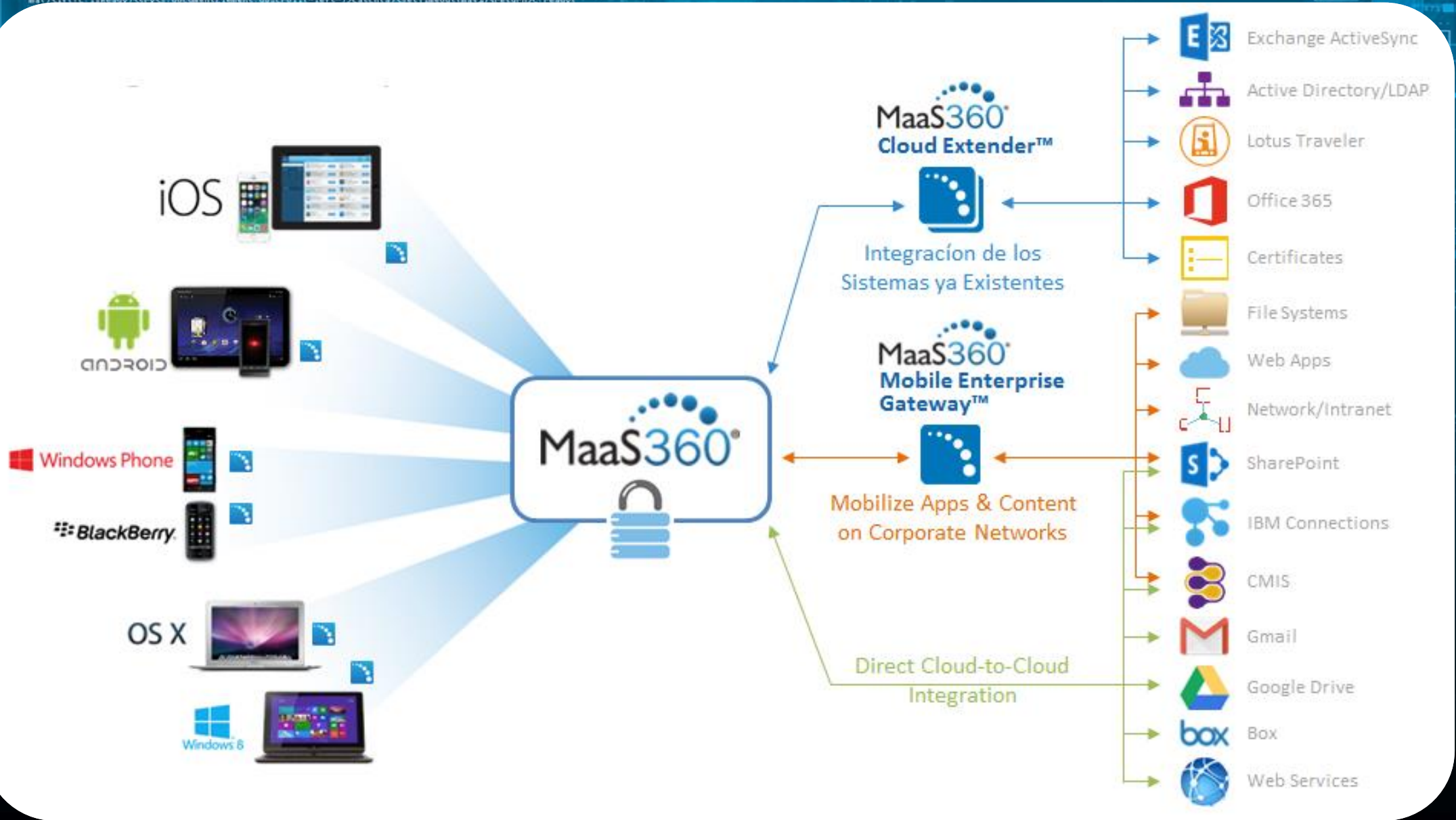
Detección de actualizaciones “over-the-air” para tomar acciones sobre dispositivos rooteados o con jailbroken

The screenshot shows the MaaS360 web interface. At the top, there are navigation tabs: DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. Below this, the user 'srajagopal-GT-19200' is selected, and the 'Trusteer Security Information' section is active. A table under 'Advanced Device Security' shows the following data:

Field	Value	Field	Value
Last Risk Assessment Date/Time	10/22/2014 14:14 IST	Trusteer Configuration Update Status	3 (u)
OS Version	4.2.2 (up-to-date)	Malware Detected	Yes
Connected Wi-Fi Security Level	Secure		
Suspicious System Configuration Found	Found both an u package		

A configuration window for 'Trusteer Advanced Security' is overlaid on the bottom right of the screenshot. It includes a checkbox for 'Configure Restricted Applications by Trusteer Ratings' which is checked. Below this, there is a 'Remediation Action' dropdown menu set to 'Uninstall App' and an 'App Exceptions' text input field containing 'com.fiberlink.maas360.androi'.

The screenshot shows an Android smartphone's notification shade pulled down. At the top, the status bar shows the time as 1:19 AM on Thursday, December 4. Below the status bar are icons for Wi-Fi, GPS, Vibrate, Screen rotation, and Bluetooth. A notification titled 'Device Out-of-Compliance' with a timestamp of 1:18 AM is visible, stating 'Device is out-of-compliance per Corporate policies for this device.' Below this is a 'Fix' button. Another notification titled 'Connected as a media device' is also visible. At the bottom of the notification shade, there is a 'Notifications' section with a 'Clear' button and a notification for 'Malware Detected' with a timestamp of 1:18 AM. The Verizon Wireless logo is visible at the very bottom of the screen.



¿Por qué MaaS360?



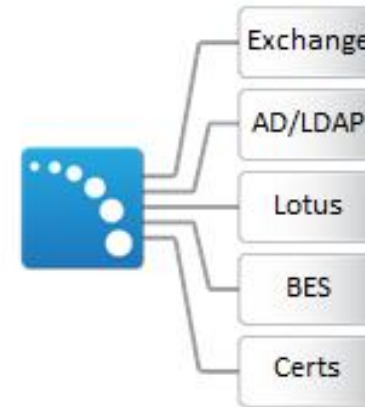
Demostrado
Centrado en la gestión de movilidad para cloud



Potentes
características para administrar el ciclo de vida completo de la movilidad



Seguros
contenedores para separar el trabajo de la vida privada



Sin sobresaltos
integración con toda la infraestructura de su empresa



Fácil
y rápido con una experiencia excepcional

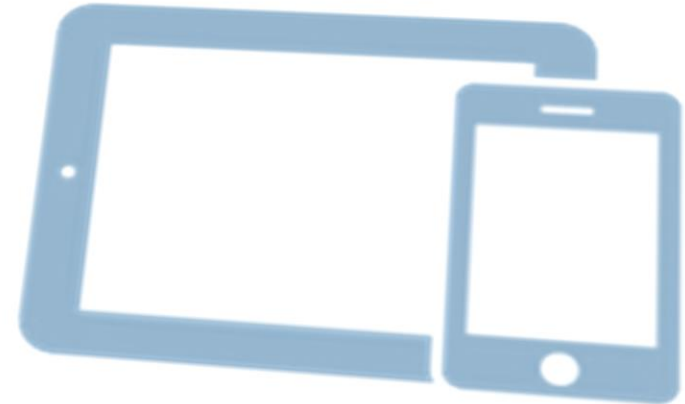
1 *Instant*
Access a free,
fully functional
trial for 30 days



2 *Easy*
Set up and
configure your
service in minutes



3 *Mobile*
Manage and secure
your devices, apps
and content



Y... el capitán?



IBM MobileFirst Protect



Ing. Gerardo Herrera - Interamericana de Computos

BYOD is coming, are you ready for this?



