IBM MobileFirst Protect:

Secure & Manage your mobile enterprise

SolutionsConnect Philippines March 2015

Stephen Downie – Growth Markets, Unified Endpoint Management

Digital and mobile technologies are making your customers and employees more empowered than ever…

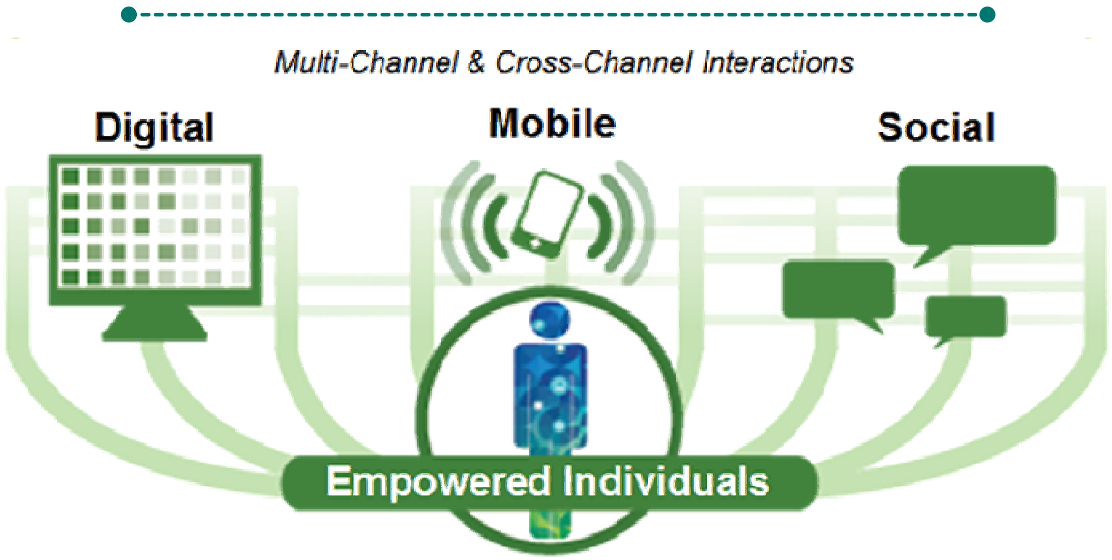
40% of smartphone users search for an item while in a store

38% yearly increase in revenue from people using mobile devices to purchase items.

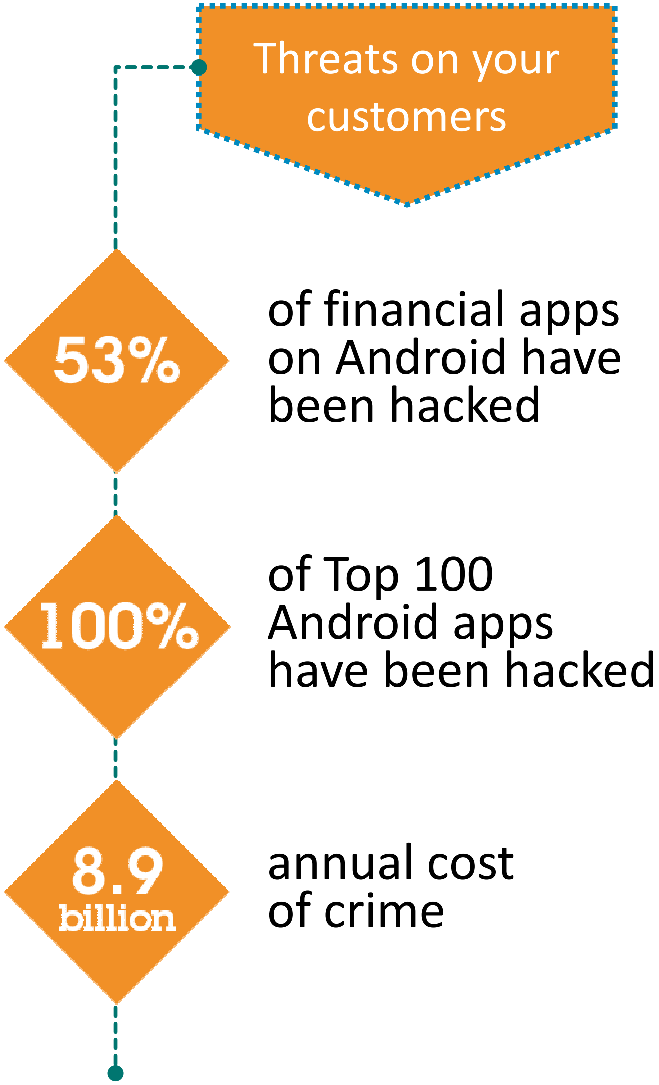
80% of individuals will exchange personal information for a personalized offering

200 million Mobile workers will use at least one business-focused app this year

81% of employed adults use at least one personally-owned mobile device for business



But security threats are ever present



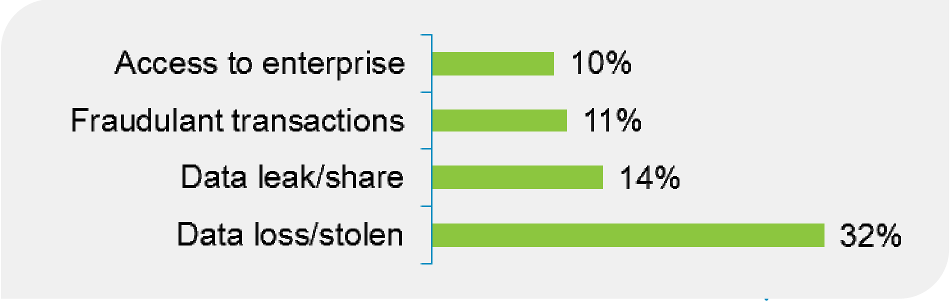
Threats on your customers

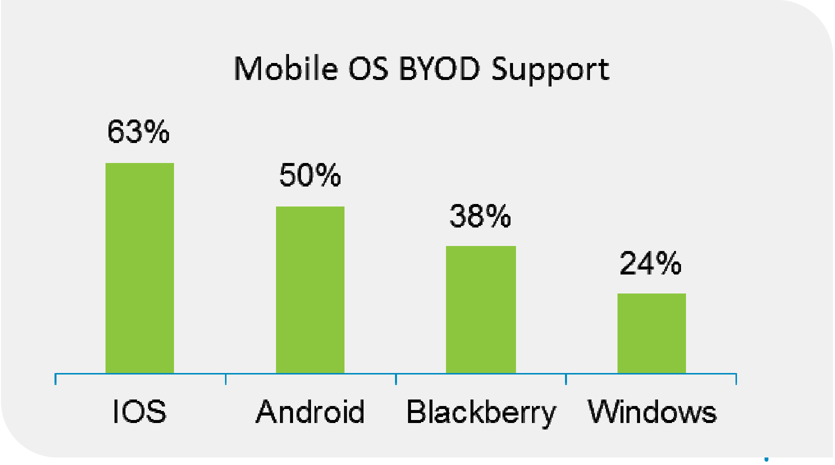
53% of financial apps on Android have been hacked

100% of Top 100 Android apps have been hacked

8.9 billion annual cost of crime

Threats on your employees

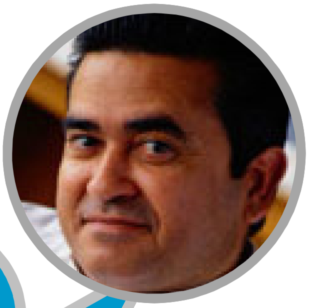




Mobile OS BYOD Support

CIOs and CISOs want to deliver a great user experience on leading devices but cannot compromise on best-of-breed security

Chief Information Officer



How do I manage rapid deployment of devices in a cost-effective way?

How do I enable my workforce with the right apps with the right user experience at the right time?

What do I do with all of our old devices? I need to protect my investment!

Chief Information Security Officer

How do I ensure all devices accessing our network are secured and encrypted?

How do I ensure proper authorized access to private customer data and protect against fraud?

CIOs and CISOs are looking for a modern mobile security solution

Legacy Mobile Security Experience	IBM's Mobile Security Experience
End-to-end proprietary architecture	Leverage best-of-breed systems and partners (Identity, Email, Network Security, EMM, Apps)
Email and messaging-oriented solutions	Apps and Content in addition to secure email
On-premises deployment only	Choice of simple cloud, on-premises or hybrid deployment options depending on customer needs
Complex deployment and integration project measured in months	Fast and easy deployment task measured in days
Dedicated IT headcount needed to support	Just a task for an IT administrator – set and forget

IBM MobileFirst Protect delivers exceptional end user experience with:

✓ **Best-in-Class**

✓ **Simplified Security**

✓ **Ease of Deployment**

IBM MobileFirst

IBM MobileFirst Protect safeguards my data and my company's data

When my work tablet – containing my credit card information and patients' data – was being attacked by malware without my knowledge, it could have been devastating for me and my practice. Luckily, my company discovered it immediately and was able to secure the data, protecting me and my patients.

IBM MobileFirst

Katy is a retail associate working to find the perfect gift for Jane’s son.

While accessing Jane’s customer information. Special care is taken to ensure her customer data is protected.

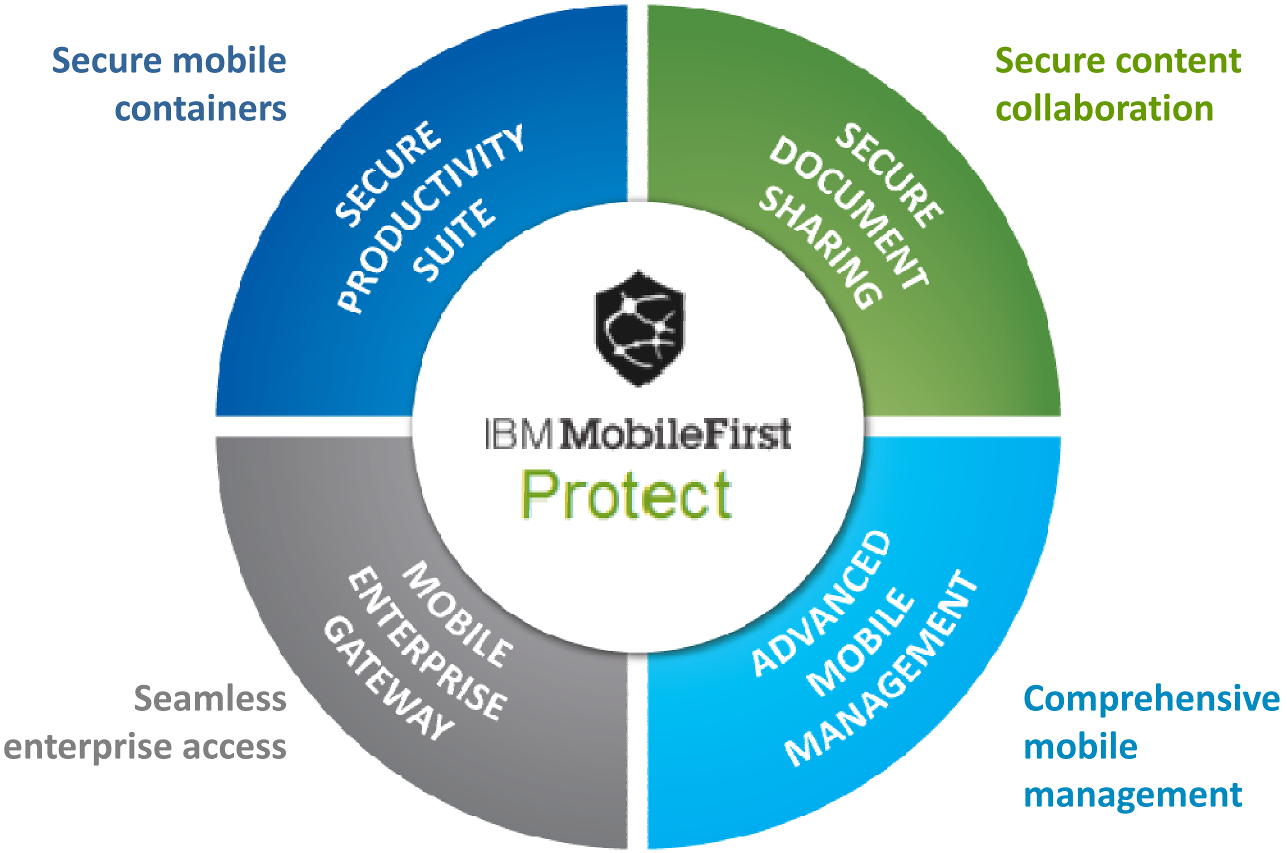
Customer data is protected on the device and through secured transmission.

Additional controls are used to ensure the device has not been compromised

Context-aware security protects all customer data and transactions across devices, apps, and the enterprise, which improves usability. Separating customer data on the device ensures no other apps can access it, ensuring customer privacy.

IBM MobileFirst Protect:

One security and management platform for all your mobile assets


Secure mobile containers
SECURE PRODUCTIVITY SUITE
Secure content collaboration
SECURE DOCUMENT SHARING
IBM MobileFirst Protect
Seamless enterprise access
MOBILE ENTERPRISE GATEWAY
Comprehensive mobile management
ADVANCED MOBILE MANAGEMENT

New in Q4

- Threat Protection / Prevention
- Zero-day iOS 8 support
- Content Management Updates
- Content access from End User Portal
- Shared folders
- Gmail integration for device discovery & access controls
- Windows Phone
- Certificates for Email and Wi-Fi configuration
- Kiosk mode
- Secure Container / Secure Mail
- iOS Notifications for Exchange 2013

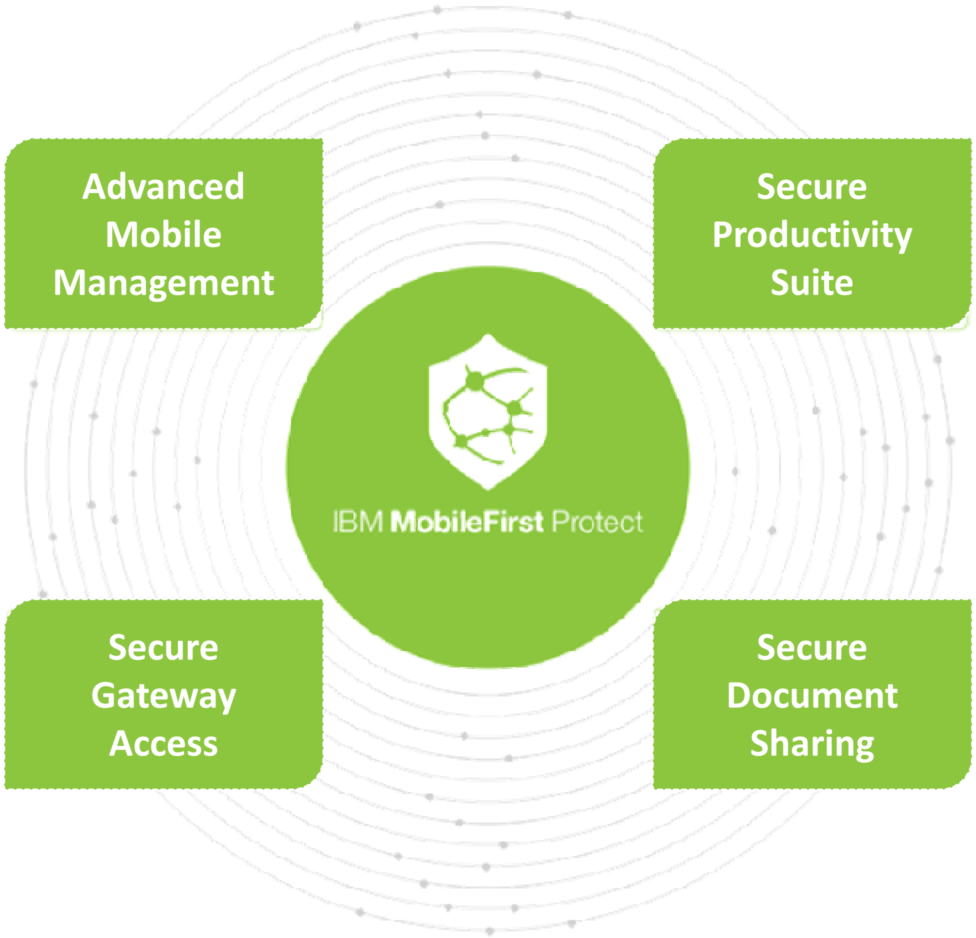
IBM MobileFirst Protect: Comprehensive security to enhance employee productivity and protect sensitive enterprise data

Manage and secure enterprise-owned and personal BYO devices

- Mobile device management
- Mobile application management
- Mobile expense management

Simple, secure access to behind-the-firewall resources

- Mobile enterprise gateway for browser
- Mobile enterprise gateway for docs
- Mobile enterprise gateway for apps



Isolate and contain work emails, Web access and app data to prevent data leaks:

- Secure mail
- Secure browser
- Application security

Securely view, distribute, create, edit and share documents via mobile device:

- Mobile content management
- Secure editor
- Secure document sync

IBM MobileFirst Protect: Easiest to Deploy and Scale

Mobile Device, App, and Content Management & Security platform

For organizations that are…

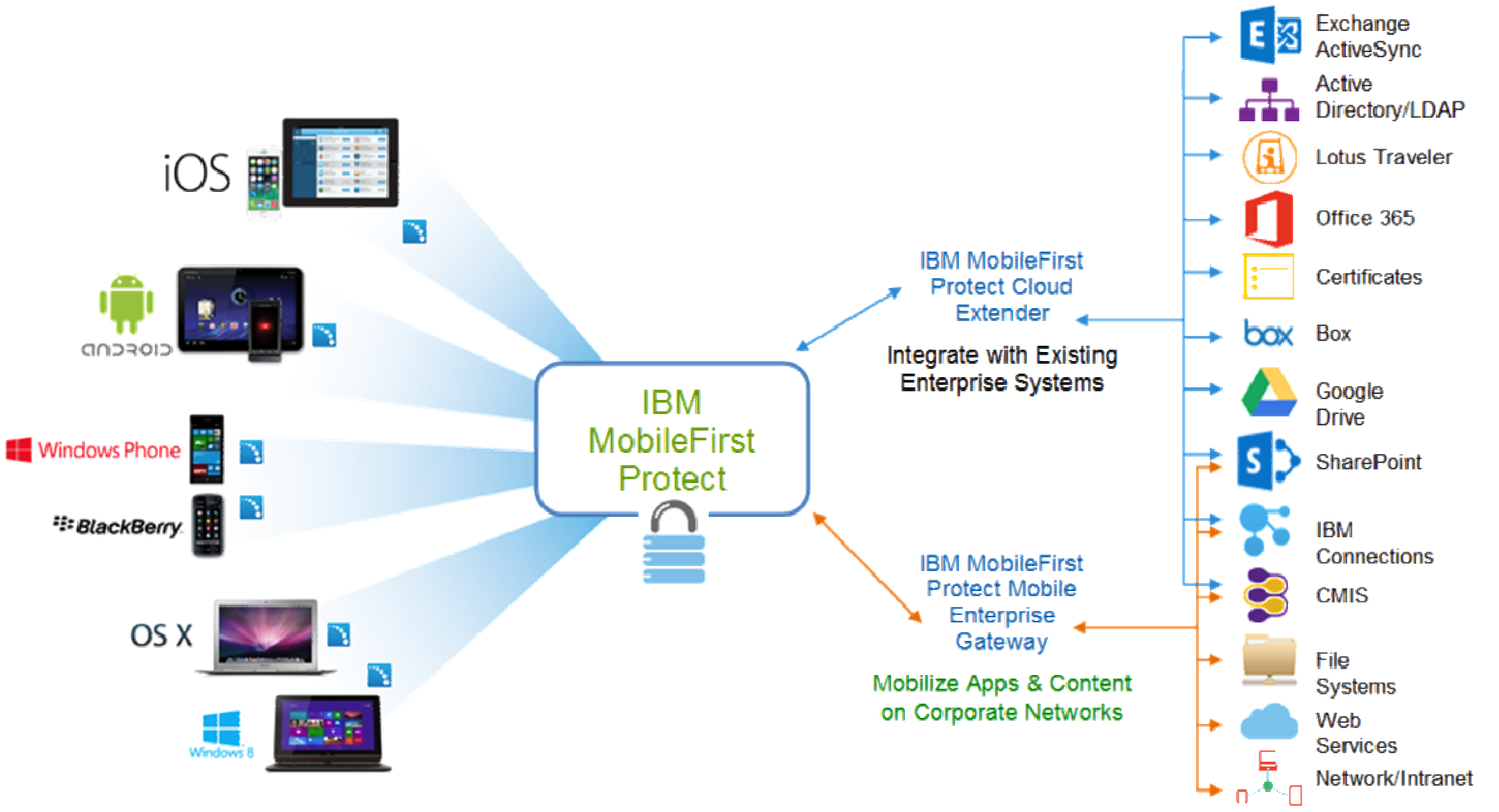
- Embracing multi-OS environments (iOS, Android, Windows Phone)
- Allowing Bring-Your-Own-Device (BYOD) programs
- Developing and deploying mobile apps (public and private)
- Enabling corporate content on mobile devices securely (push and pull)
- AND MORE….

IBM MobileFirst Protect: Dual Persona to Separate Work and Personal

- Secure Mail
- Application Security
- Secure Browser
- Secure Document Sharing

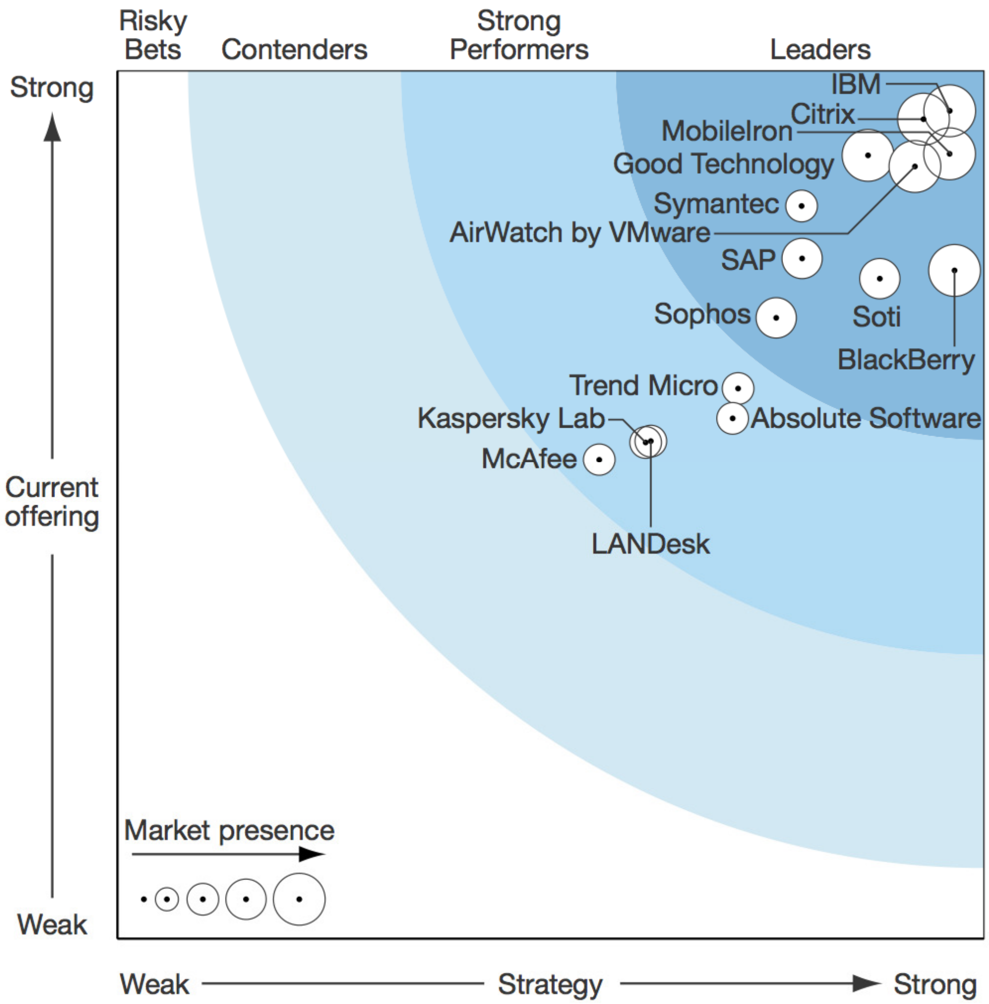
WorkPlace Container for Mobile Collaboration

Seamless Enterprise Integration



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.

Why IBM

1

Best in Class Security Solution:

- We are leaders in MDM
- Best in class – Apple Devices & MDM
- Offered on-prem/cloud
- Ease and speed of migration

2

Security is more than encryption:

- Risk-aware applications
- Anti-malware
- Fraud protection

3

Enterprises need complete **Security and Management solutions for** both employee- and customer-facing app opportunities

IBM’s Industry-leading MobileFirst Portfolio

200+ IBM SOFTWARE APPS are available today in App Stores, with almost 1,000,000 downloads

IBM named A LEADER among Global Digital Marketing Agencies

IBM named A LEADER for application security testing

100% OF THE TOP 100 communication service providers use IBM software

IBM named A LEADER in Mobile Application Development Platforms

IBM named the <u>only</u> LEADER for managed mobility services

IBM is cited as A LEADER in app design and managed services

IBM LEADS in
Worldwide Mobile Application Development, Testing, Management & Infrastructure Services

Software & Information Industry Association (SIIA) honored IBM

for Best Mobile Development Solution (May 2013)

Thank You!

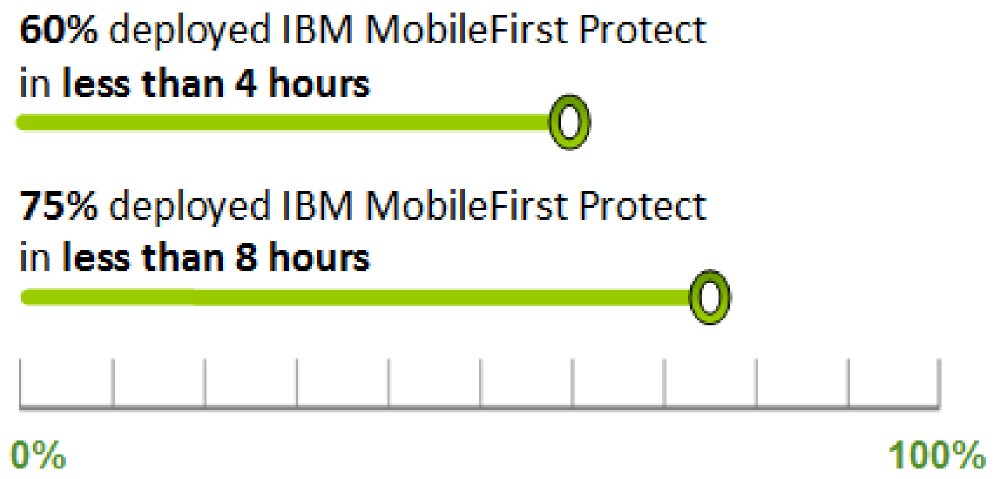
Learn: ibm.com/mobilefirst

Try: ibm.com/bluemix

Watch: youtube.com/IBMMobileEnterprise

Why IBM MobileFirst Protect?

Fastest Time to Trust



60% deployed IBM MobileFirst Protect in **less than 4 hours**

75% deployed IBM MobileFirst Protect in **less than 8 hours**

Sales & customer support at no additional charge

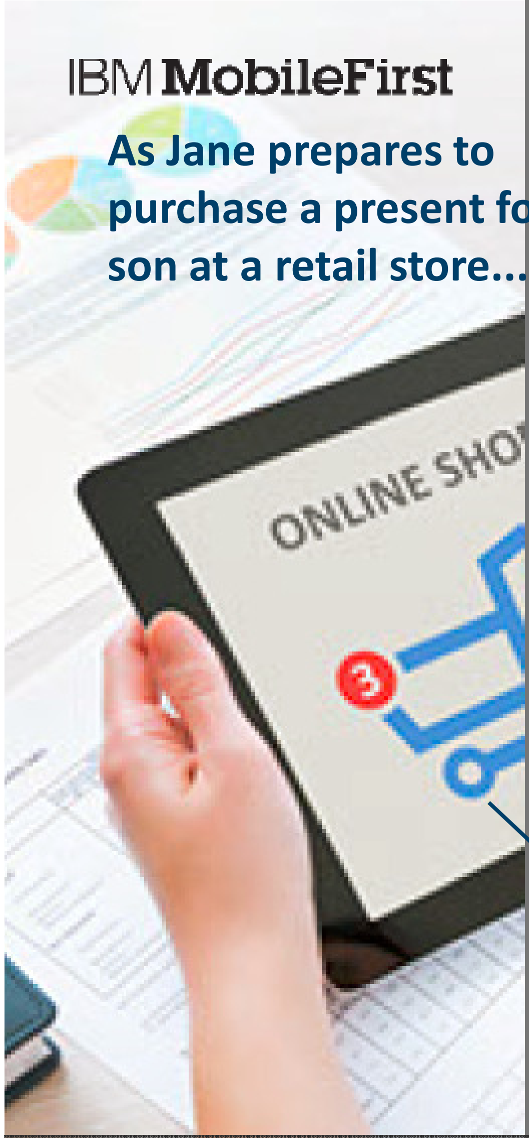
24x7 customer support by phone, chat or email

Community, forums, blogs, on-demand webinars

A LEADER
2014
Mobile Enterprise
Mobility Management
Gartner Magic Quadrant

A LEADER
2014
Enterprise
Mobile Management
The Forrester Wave™

A CHAMPION
2014
Mobile Device
Management
Info-Tech Research
Vender Landscape Award



As Jane prepares to purchase a present for her son at a retail store...

Her bank notices potential fraudulent activity happening overseas.

Jane is sent a “one time password via text” to add extra security without alarming her.

The threat goes unnoticed to Jane, improving her mobile experience while simplifying her shopping experience.

Security and Protection extends beyond employees to customers. Ensuring personal information is secured and accessed by only the people who are allowed to access it helps enterprises manage threats on customers.

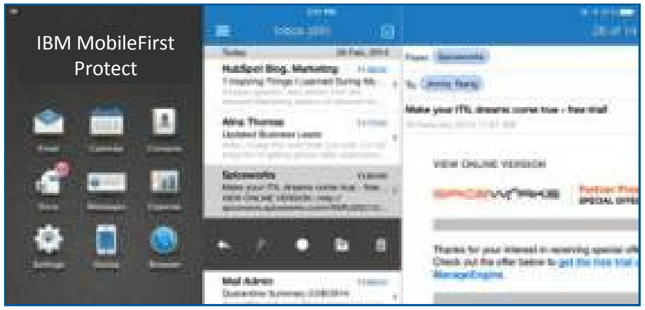
Protect User, Device, Data and Transactions with IBM Security Access Manager

1 **Context Aware** security means you authenticate when you need to, which provides a better user experience

2 **Protect** against targeted attacks and web vulnerabilities

3 **Detect Insider Fraud**

IBM MobileFirst Protect: Secure Productivity Suite

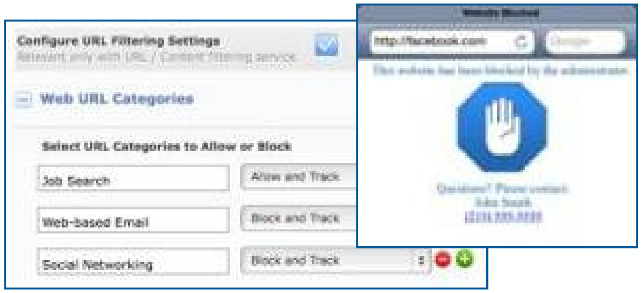


Secure Mail

- 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



Configure URL Filtering Settings ☑
Relevant only with URL / Content filtering service

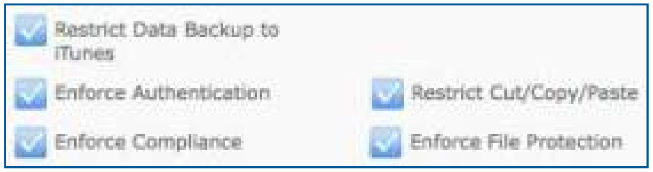
Web URL Categories

Select URL Categories to Allow or Block

Job Search	Allow and Track
Web-based Email	Block and Track
Social Networking	Block and Track

http://facebook.com

This website has been blocked by the administrator



☑ Restrict Data Backup to iTunes

☑ Enforce Authentication

☑ Restrict Cut/Copy/Paste

☑ Enforce Compliance

☑ Enforce File Protection

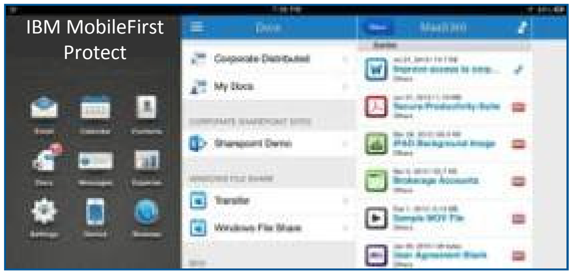
Application Security

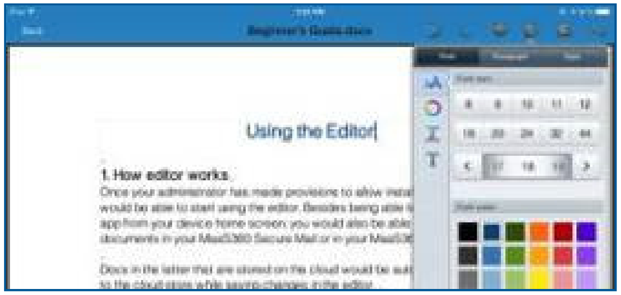
- Contain enterprise apps with a simple app wrapper or SDK
- Enforce authentication & copy/paste restrictions
- Prevent access from compromised devices

IBM MobileFirst Protect: Secure Document Sharing

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





Using the Editor

1. How editor works

Once your administrator has made provisions to allow insta
would be able to start using the editor. Besides being able t
app from your device home screen, you would also be able
documents in your MaaS360 Secure Mail or in your MaaS36

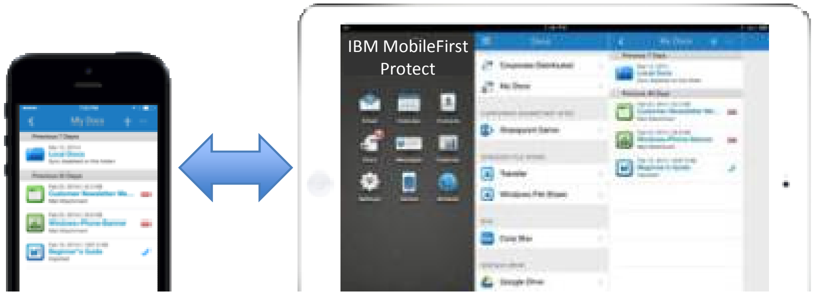
Docs in the latter that are stored on the cloud would be aut
to the cloud store while saving changes in the editor.

Secure Editor

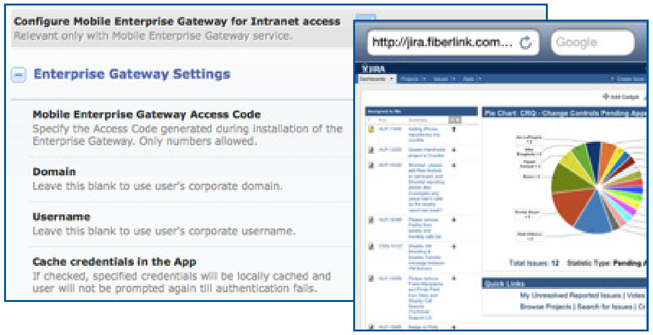
- Create, edit & save content in a secure, encrypted container
- Collaborate on Word, Excel, PowerPoint & text files
- Change fonts & insert images, tables, shapes, links & more

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: Mobile Enterprise Gateway



Configure Mobile Enterprise Gateway for Intranet access
Relevant only with Mobile Enterprise Gateway service.

Enterprise Gateway Settings

Mobile Enterprise Gateway Access Code
Specify the Access Code generated during installation of the Enterprise Gateway. Only numbers allowed.

Domain
Leave this blank to use user's corporate domain.

Username
Leave this blank to use user's corporate username.

Cache credentials in the App
If checked, specified credentials will be locally cached and user will not be prompted again till authentication fails.

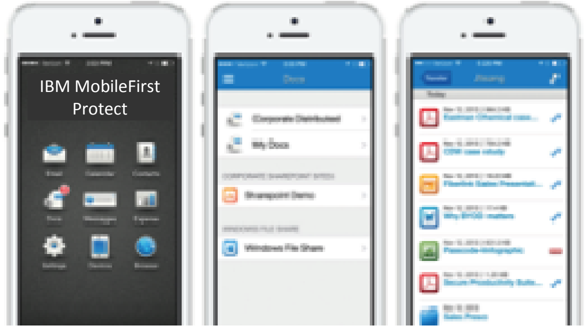
http://jira.fiberlink.com...
Google
JIRA
Pie Chart: CRQ - Change Controls Pending App
Total Issues: 12 Statistic Type: Pending
Quick Links
My Unresolved Reported Issues | Votes
Browse Projects | Search for Issues | Cr

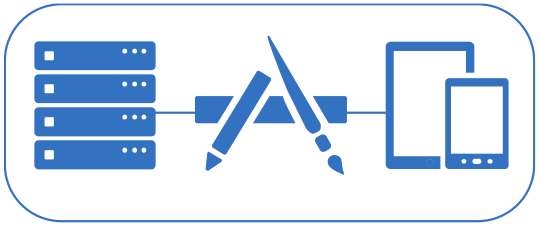
Mobile Enterprise Gateway for Browser

- Enable IBM 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 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





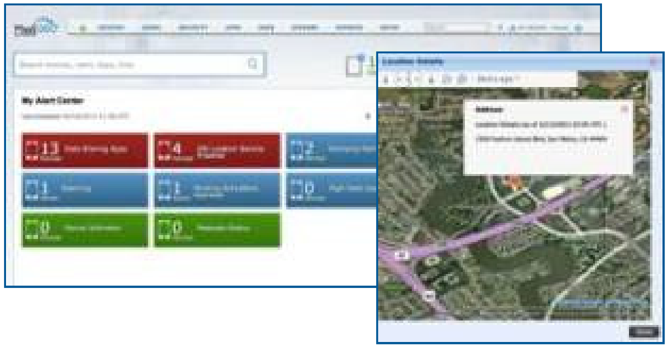
Mobile Enterprise Gateway for Apps

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

IBM MobileFirst Protect: Mobile Enterprise Gateway

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

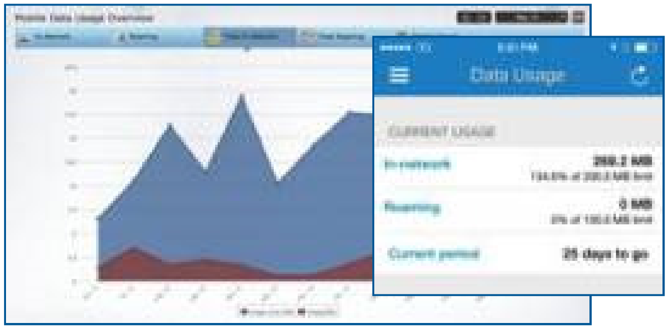


Mobile Application Management

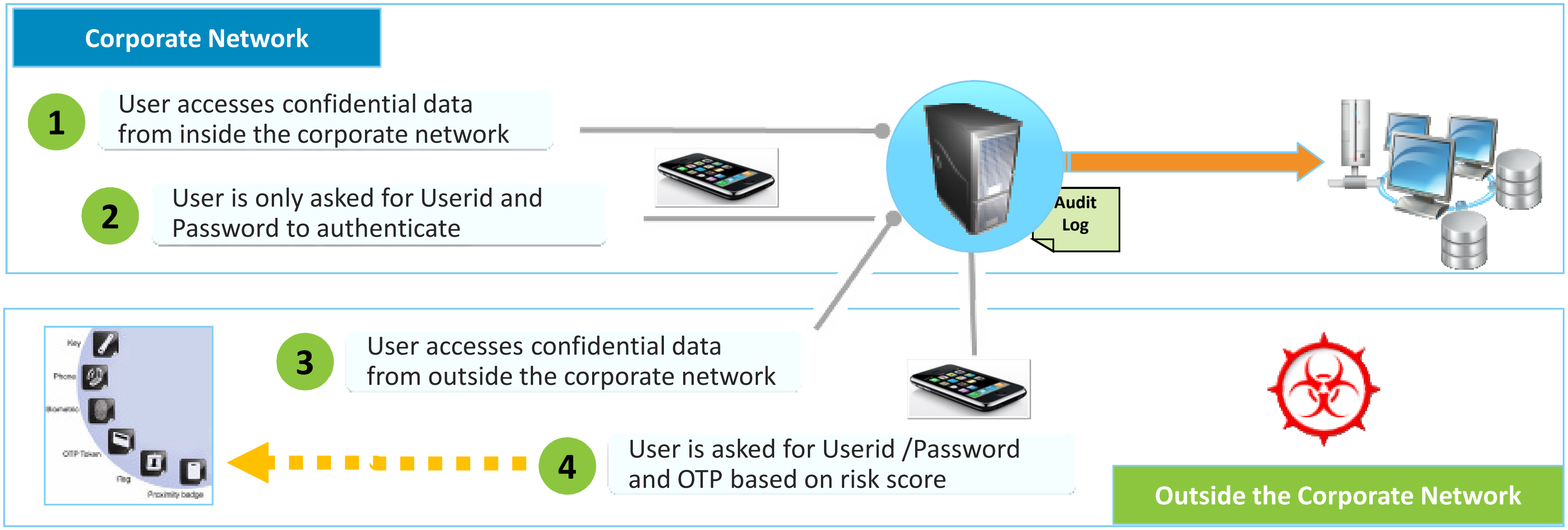
- Deploy custom enterprise app catalogs
- Blacklist, whitelist & require apps
- Administer app volume purchase programs

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



Context-aware access to secure mobile user access



Corporate Network

1 User accesses confidential data from inside the corporate network

2 User is only asked for Userid and Password to authenticate

3 User accesses confidential data from outside the corporate network

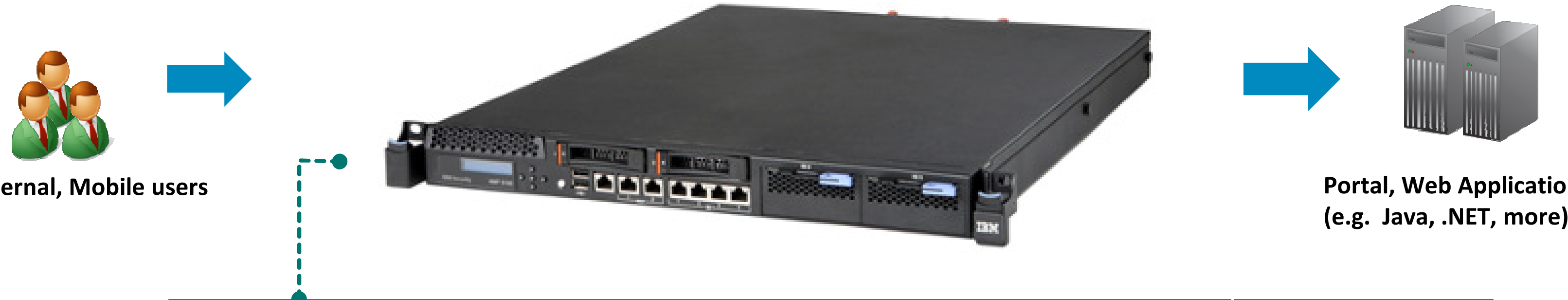
4 User is asked for Userid /Password and OTP based on risk score

Outside the Corporate Network

- Risk-based Access feature to determine and score risk levels using user attributes and real-time context (e.g. location, device)
- Enforce mobile user access based on risk-level (e.g. permit, deny, step-up authenticate)
- Support mobile authentication with built-in One-Time Password (OTP) and provide ability to integrate with 3rd party strong authentication vendors, as needed

Secure access and protect the content against targeted attacks and web vulnerabilities

IBM Security Access Manager Proxy Appliance (AMP 5100)



External, Mobile users

Portal, Web Applications
(e.g. Java, .NET, more)

Access Operations	Grant/Deny
An authorized user requests access to the portal and SSO	Grant
Password is stolen, session is hijacked and HTTP content is compromised	Deny
HTTP content contains common vulnerabilities such as SQL Injection, Cross site scripting, Cross-site request forgery	Deny
Enforce step-up authentication or risk-based access to restore authorized user access	Grant

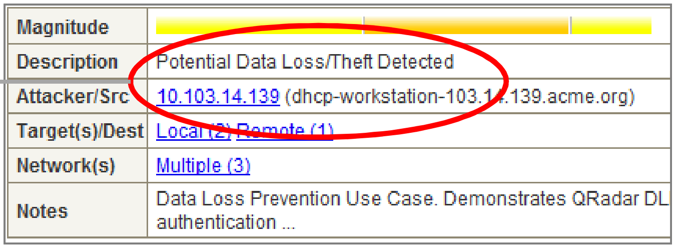
Access Management in a multi-perimeter world

Integrated Web Access and Web Content Protection in a Single Appliance (Powered by X-Force)

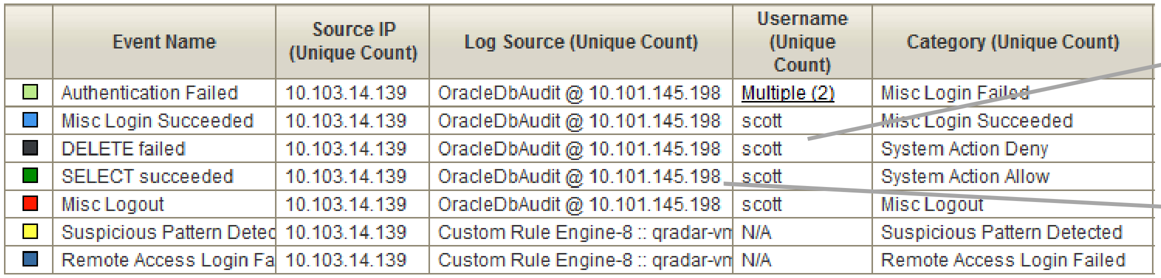
Detect insider fraud

Potential Data Loss

Who? What? Where?



Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...



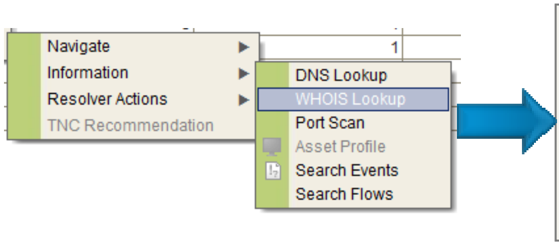
	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
🟩	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
🟦	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
⬛	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
🟩	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
🟥	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
🟨	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
🟦	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

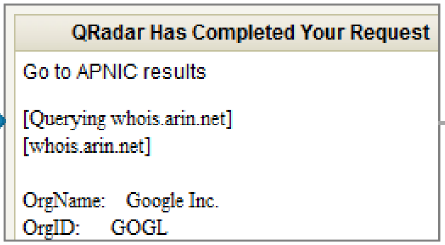
Who?

An internal user

What?

Oracle data





QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

Where?

Gmail

Threat detection in the post-perimeter world

User anomaly detection and application level visibility are critical to identify inside threats