**Wilhelm Mild**
**IBM Executive IT Architect**
**IBM Germany**

# Securing your mobile Mainframe

# As mobile grows, so do security threats

In 2014 the number of cell phones

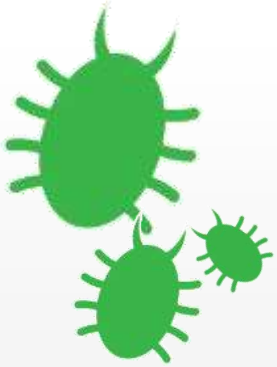
**(7.3 billion)**

will exceed the number of people on the planet (7 billion).[1]

Mobile downloads will increase to

**108 billion**

by 2017.[2]



Mobile malware is growing. Malicious code is infecting more than

**11.6 million**

mobile devices at any given time.[3]

Mobile devices and the apps we rely on are under attack.

**90%** of the top mobile apps have been hacked.[4]

# Top Drivers for Mobile App Protection

1. Prevent or detect **bypassing or disabling of security controls** (e.g., jailbreak/root detection, authentication, authorization, encryption, digital rights/licensing)

2. Prevent or detect **bypassing or modification of business logic** (e.g., transactions, restricted functionality, sensitive operations)

3. Prevent **information loss or exposure** (e.g., via compromised user credentials, keys, data storage)

4. Prevent creation of **rogue, cloned, pirated, or modified** versions

5. Prevent or detect **insertion of malicious code** in the app
(e.g., prevent remote control, information / identity stealing, financial charging)

6. Prevent **stealing of proprietary code/IP** from the app

7. Prevent **exposure of potential vulnerabilities** and sensitive source code

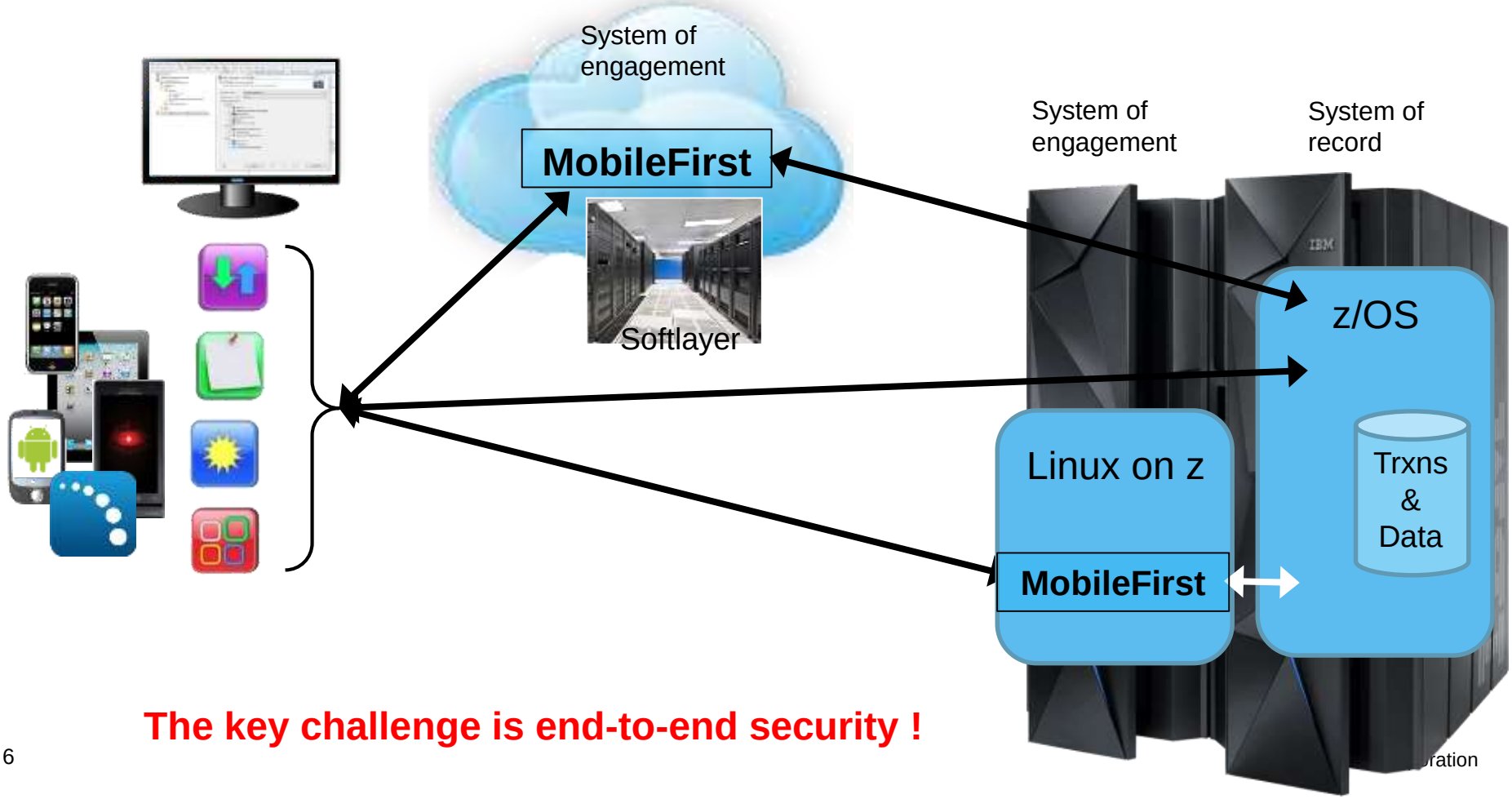
8. Ensure **compliance with industry guidelines**
(e.g., OWASP Mobile Top Ten)

# IBM positioning to solve the Mobilizing challenges

## MobileFirst Platform – An Enterprise Blueprint

# Key Mobile Solution scenarios

- on premise – with the System of engagement on System z
- off premise – with the System of engagement offsite – i.e. in IBM Softlayer




**The key challenge is end-to-end security !**

# Security features capabilities for the mobile enterprise


| Device Security | Content Security | Application Security | Transaction Security |
|---|---|---|---|
| • Enroll, provision and configure devices, settings and mobile policy<br>• Fingerprint devices with a unique and persistent mobile device ID<br>• Remotely Locate, Lock and Wipe lost or stolen devices<br>• Enforce device security compliance: passcode, encryption, jailbreak / root detection | • Restrict copy, paste and share<br>• Integration with Connections, SharePoint, Box, Google Drive, Windows File Share, Dropbox<br>• Secure access to corporate mail, calendar and contacts<br>• Secure access to corporate intranet sites and network | **Software Development Lifecycle**<br>•Integrated Development Environment<br>•iOS / Android Static Scanning<br>**Application Protection**<br>•App Wrapping or SDK *Container*<br>•Hardening & Tamper Resistance *IBM Business Partner (Arxan)*<br>•Run-time Risk Detection *Malware, Jailbreak / Root, Device ID, and Location*<br>•Whitelist / Blacklist Applications | **Access**<br>•Mobile Access Management<br>•Identity Federation<br>•API Connectivity<br>**Transactions**<br>•Mobile Fraud Risk Detection<br>•Cross-channel Fraud Detection<br>•Browser Security / URL Filtering<br>•IP Velocity |

**Security Intelligence**

Advanced threat detection with greater visibility

# Fast and easy security and management

## 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, webinars*

GARTNER'S MAGIC QUADRANT

**2014 Leader** Enterprise Mobility Management Suites

FORRESTER®

**"Innovator"** Cloud-hosted mobile device management


InfoTech Research Group

**"Champion"** Mobile Device Management

# Secure every transaction: Mobile to Mainframe


| Device Security | Content Security | Application Security | Transaction Security |
|---|---|---|---|

*powered by…*

**IBM MobileFirst Platform**

IBM Security AppScan

IBM Security Access Manager

Trusteer an IBM Company

IBM Security zSecure

ARXAN Arxan Application Protection for IBM Solutions

IBM RACF
IBM Distributed Identity Data

IBM InfoSphere Guardium

**IBM MobileFirst Protect**

IBM DataPower

z/OS Connect

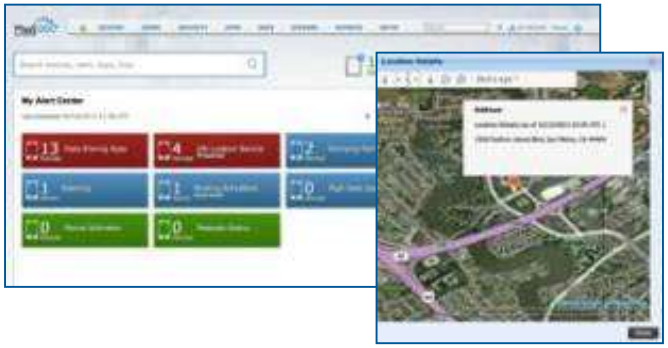
*Security Intelligence*

IBM QRadar Security Intelligence Platform

# 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



## 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

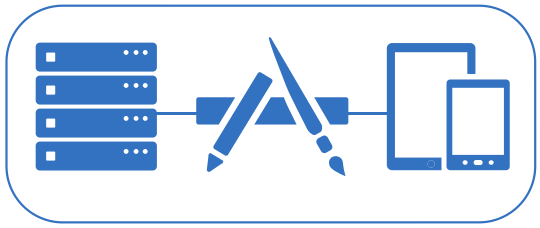
# IBM MobileFirst Protect Gateway Suite


## Mobile Enterprise Gateway for Browser

- Enable 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

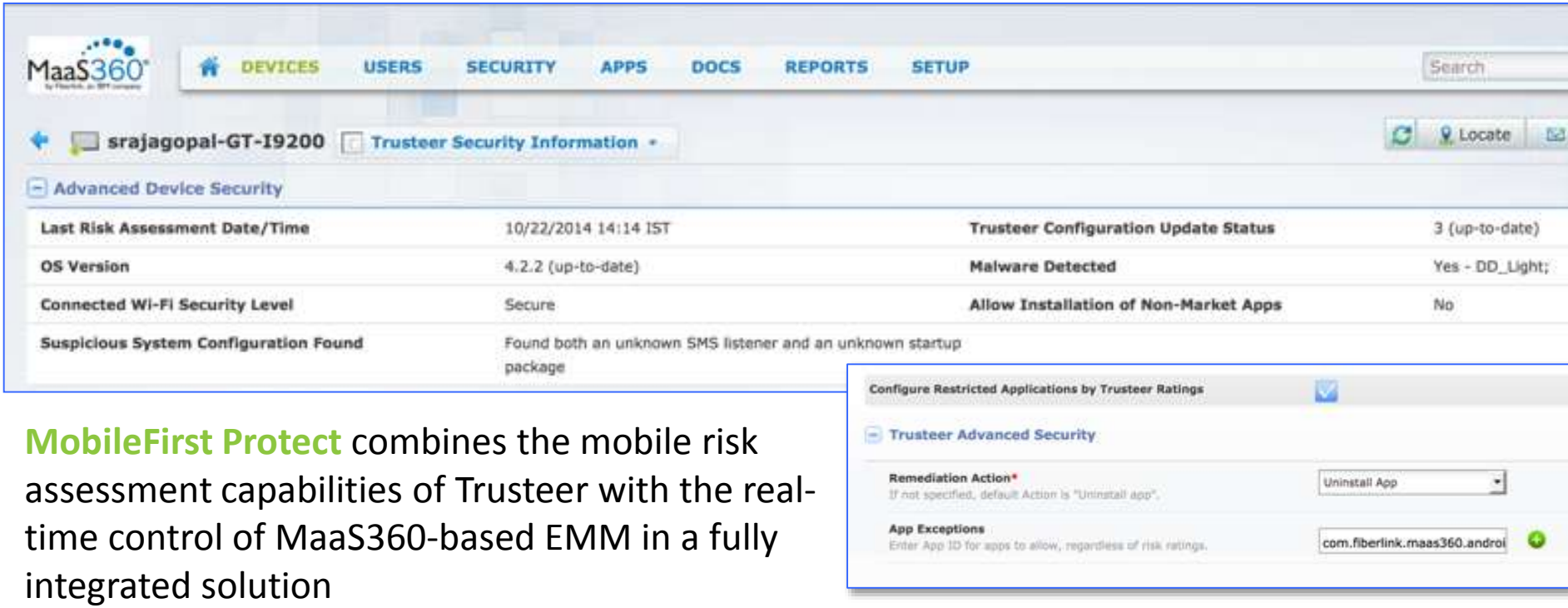



## Mobile Enterprise Gateway for Apps

- 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 Threat Management

Integrated Threat Management
powered by industry leading Trusteer technology

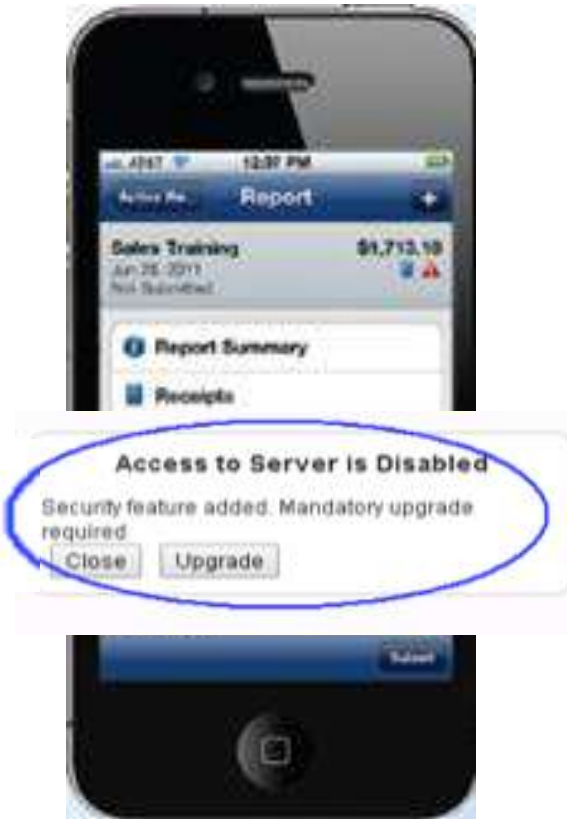



**MobileFirst Protect** combines the mobile risk assessment capabilities of Trusteer with the real-time control of MaaS360-based EMM in a fully integrated solution

- **Mobile malware detection** detects known malicious files based on their MD5s
- **Rogue app detection** identifies potentially malicious apps based on permission analysis
- **Cloud-based threat intelligence** to augment device context analysis with information such as last known location

# MobileFirst Platform V7 with additional Mobile apps security

- **User Authentication (Enhanced)**
  - Plugs into existing enterprise or 3rd party security systems with a variety of authentication methods
    - Certificate-based, Touch ID, LDAP server, Social
  - Multi-factor authentication
  - Disable app version, specific user or devices through the console
- **App Authenticity (Enhanced)**
  - Verify app identity; protect brand reputation, intellectual property and back-end data
  - Take more "fingerprints" from the app to better validate when the app was changed
    - Extend the number of shared secrets
    - New command line to extract the shared secrets
  - MobileFirst console can present app authenticity status
- **Encrypt local data**
  - Leverage user identity to encrypt and retrieve data stored locally on the device



# What part of the mobile environment does each product Secure?

## Mobile Device

- MaaS360 by Fiberlink, an IBM company
- Trusteer an IBM Company
- MobileFirst

## Mobile App

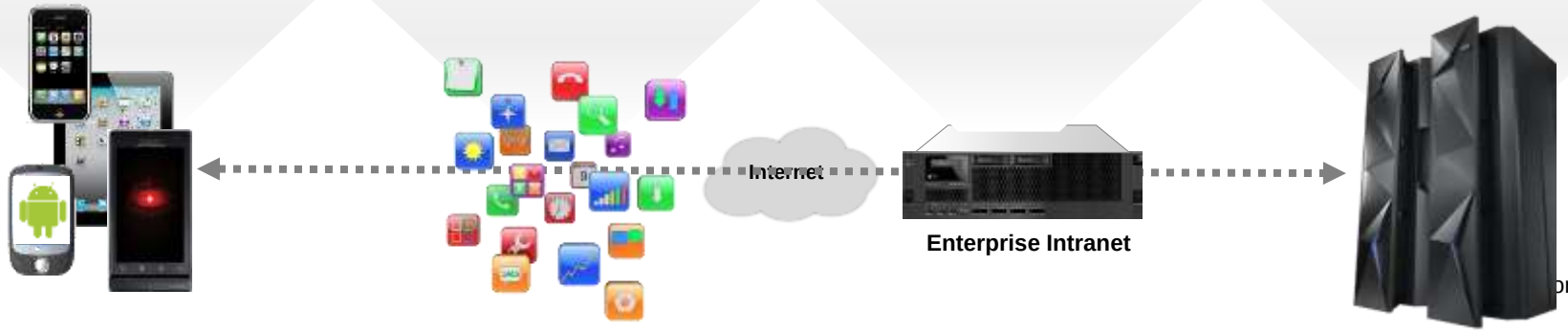
- IBM Security AppScan
- Trusteer an IBM Company
- MobileFirst
- Arxan Application Protection

## Over the Network

- IBM Security Access Manager
- QRadar
- DataPower
- MessageSight

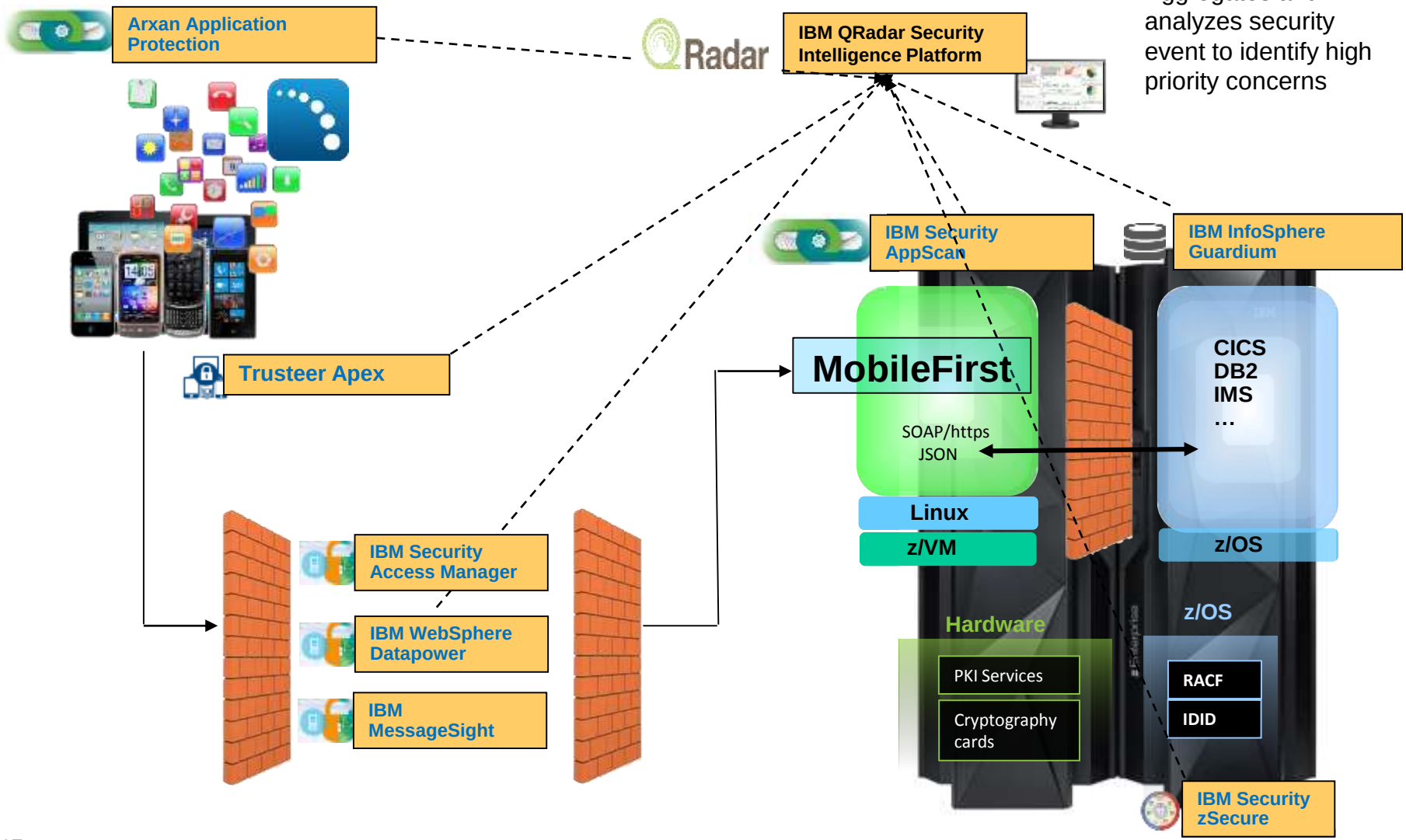
## Within the Enterprise

- IBM RACF
- IBM Security zSecure
- Hardware Crypto, PKI

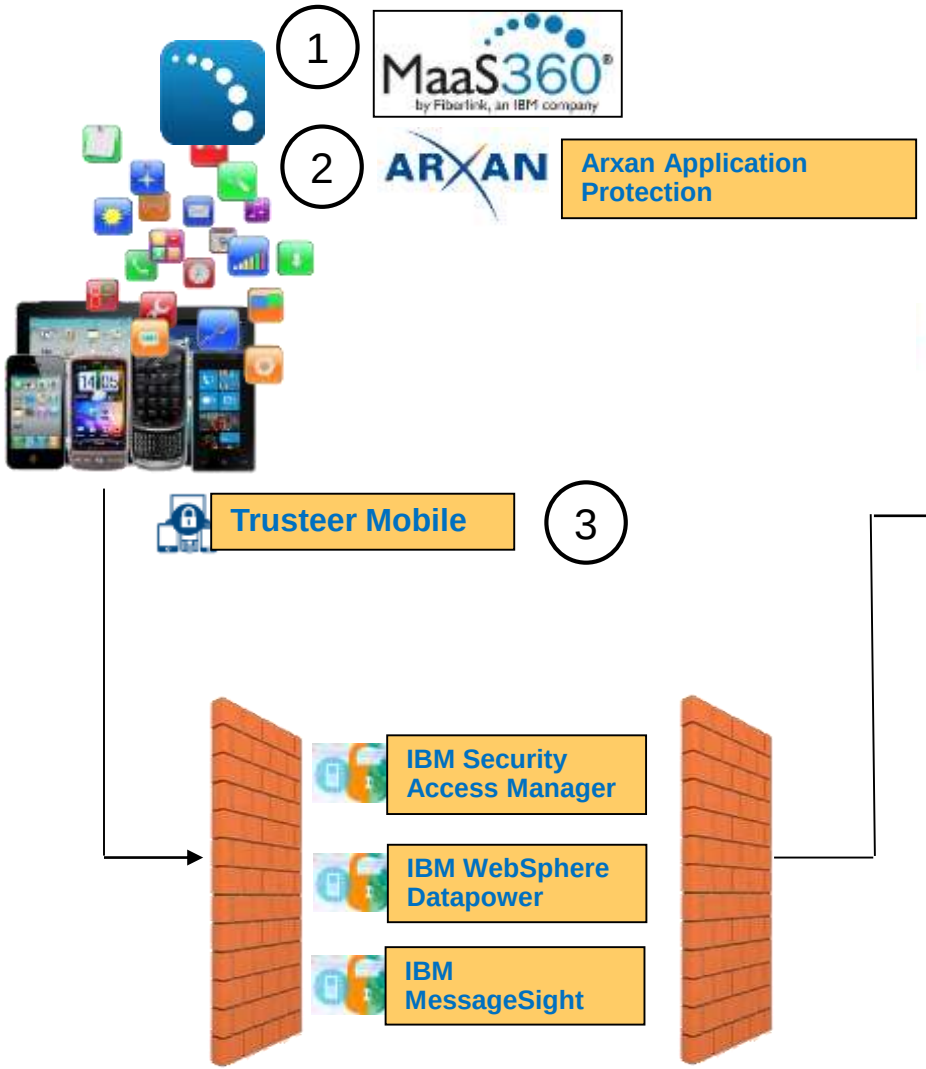


# Real-time security intelligence for the Mobile Enterprise

Aggregates and analyzes security event to identify high priority concerns



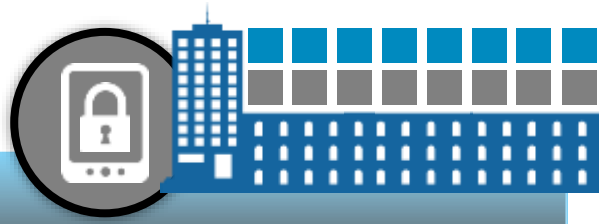
# Secure the Users & Devices for the Mobile Enterprise




1. Secure the device – run enterprise Apps in a secured container
2. Protect the applications against hacking attacks & malware
3. Authenticate and authorize the user

# (1) MobileFirst Protect - MaaS360 Enterprise Mobility Management

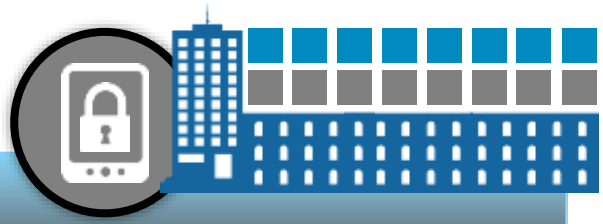
***Instantly deploy, manage and secure devices, apps and content in the enterprise***



- **Challenge:** Businesses need flexible and efficient ways to promote their mobile initiatives while protecting data and privacy.
- **Solution:** Deliver comprehensive mobile management and security capabilities for users, devices, apps, documents, email, web and networks.
- **Key benefits**
  - Support corporate and employee-owned devices
  - **Promote dual persona with full containerization and BYOD privacy**
  - Take automated action to ensure compliance with policies
  - Control emails and attachments to prevent data leakage
  - Distribute, secure and manage mobile applications
  - Allow corporate documents on mobile devices securely
  - Filter and control access to the web and corporate intranet sites

# (2) Arxan Application Protection for IBM Solutions

***Application hardening and run-time protection to secure applications against hacking attacks and malware exploits***



- **Challenge:** Protect applications to make them self-defending, hardened, and tamper-resistant "out in the wild" against hacking attacks and malware exploits.
- **Solution:** Instrument a risk-based custom Guard Network in the application binary that enables it to defend against compromise, detect attacks at run-time, and react to ward off attacks.
- **Key benefits**
  - "Gold Standard" protection strength vs. attacks and exploits
    - Multi-layer interconnected Guard Network for defense-in-depth and no single point of failure
    - Breadth of static & run-time Guard types vs. threats
    - Automated variability and randomization for each build
  - No source code involvement due to unique binary-based guard injection engine; no disruption to SDLC
  - Broadest multi-platform support to enable standardization
  - No impact to user experience, negligible performance impact
  - Battle-tested with protected apps on over 300 million devices
  - Validated with MobileFirst and AppScan, tested with Trusteer

**More Information**

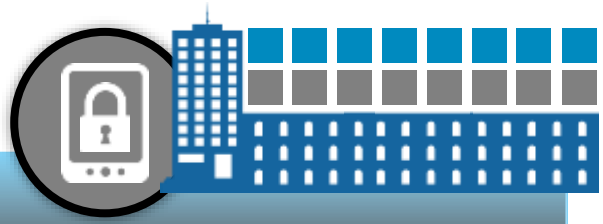
- Landing Page

# Arxan Case Example in Mobile Financial Services


- **CIO challenge: Drive mobile app innovation without compromising security and company assets**
  - External customer apps (B2C)
  - Internal employee apps (B2E)
- **Identified multiple hacking attack risks and targets for apps "out in the wild"**
  - Bypassing security controls, getting unauthorized access
  - Sensitive information exposure
  - Inserting exploits / malware, cloning applications
  - Exposing app internals and vulnerabilities
- **Used Arxan to protect mobile apps against attacks** (~15 apps protected to date)
- **CIO won CIO 100 Award for innovation**

# (3) Trusteer Mobile

***Risk-aware mobile application and risk-based mobile transaction assessment***

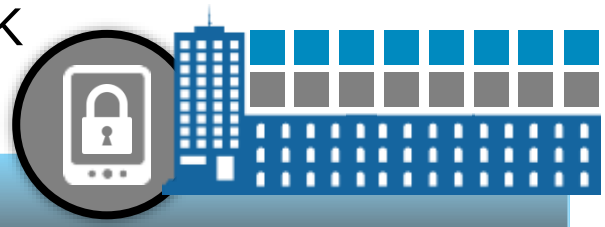


- **Challenge:** Compromised devices and applications create fraud risk and an insecure environment.
- **Solution:** Dynamically detect device risk factors and capture the underlying device.
- **Key benefits**
  - Accurately detects device risk factors
  - Allows or restricts sensitive mobile application functions based on risks
  - Mobile transaction risk can be correlated with cross-channel risk factors to detect complex fraud schemes.
  - Promotes comprehensive risk assessment and secure application development
  - Helps secure transactions from devices to the back office
  - Integrates with IBM MobileFirst projects

## More Information

- Website
- Whitepaper
- Trusteer Mobile SDK
- Trusteer Mobile App

# Large retail bank in Europe strengthens security for its mobile money transfers and banking applications with **Trusteer** SDK



**$1 million**

in fraud stopped in the **first week**

**$60 million**

in fraud stopped in the **first year**

**Business problem:** A retail bank in the EU sought a secure means to allow its users to perform the same functions they performed online with their mobile devices.

**Solution:** Trusteer Mobile SDK helped protect the organizations' existing mobile banking application by adding device risk analysis and providing a persistent mobile device ID.

**Benefits:**

- Detects high risk access from compromised or vulnerable devices
- Generates a persistent mobile device ID for unique device identification

**Featured Security Offering**: Trusteer Mobile SDK

# Secure the Users & Devices for the Mobile Enterprise

MaaS360 by Fiberlink, an IBM company

ARXAN

Trusteer Mobile

4. Authenticate and authorize the user
5. Authenticate massive number of requests simultaneously
6. Authenticate especially mass of MQTT requests

4 IBM Security Access Manager

5 IBM WebSphere Datapower

6 IBM MessageSight

IBM Security AppScan

MobileFirst

SOAP/https

Linux

z/VM

CICS
DB2
IMS
…

z/OS

Hardware

PKI Services

Cryptography cards

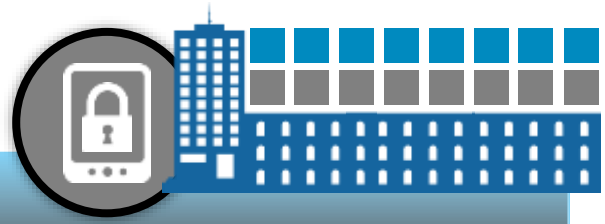
z/OS

RACF

IDID

# (4) IBM Security Access Manager for Mobile

***Safeguard mobile, cloud and social interactions***



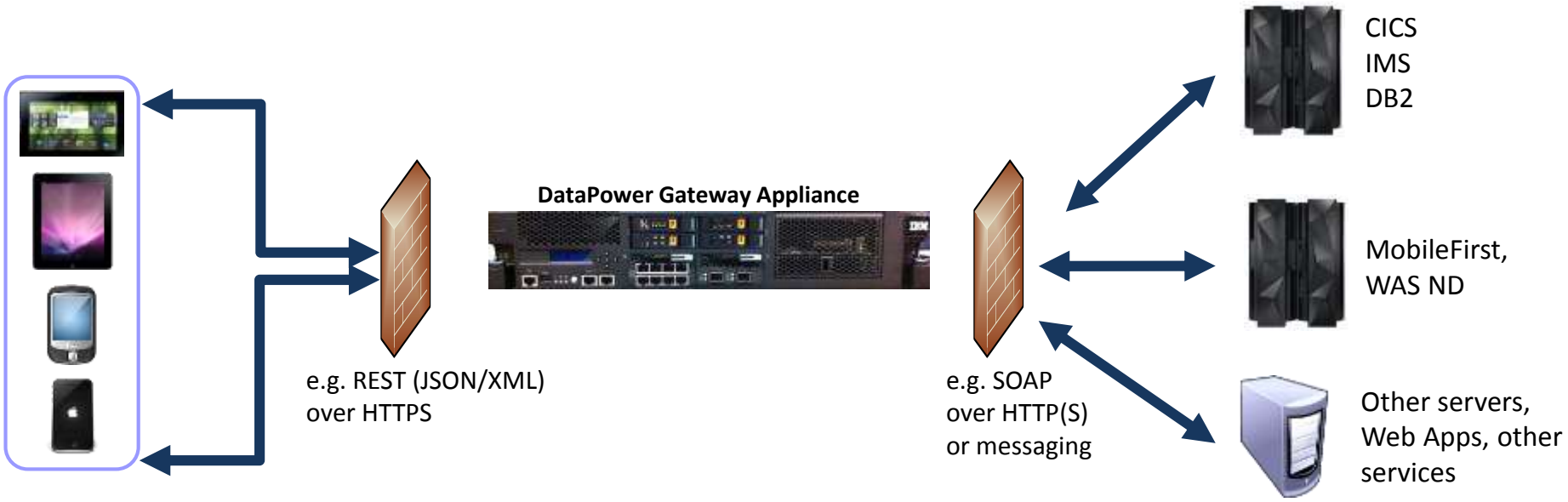
- **Challenge:** Provide secure access to mobile apps and reduce the risks of user access and transactions from the mobile devices.
- **Solution:** Deliver mobile single sign-on and session management, enforce context-aware access and improve identity assurance.
- **Key benefits**
  - Protects the enterprise from high risk mobile devices by integrating with **Trusteer** Mobile SDK
  - Built-in support to seamlessly authenticate and authorize users of **MobileFirst** developed mobile applications
  - Enhances security intelligence and compliance through integration with **QRadar** Security Intelligence
  - Protects web and mobile applications against OWASP Top 10 web vulnerabilities with integrated **XForce** threat protection (OWASP- Open Web Appl. Security Project)
  - Reduces TCO and time to value with an **"all-in-one"** access appliance that allows flexible deployment of web and mobile capabilities as needed

**More Information**

- Website
- Whitepaper
- Datasheet
- Demo Video
- Webinar

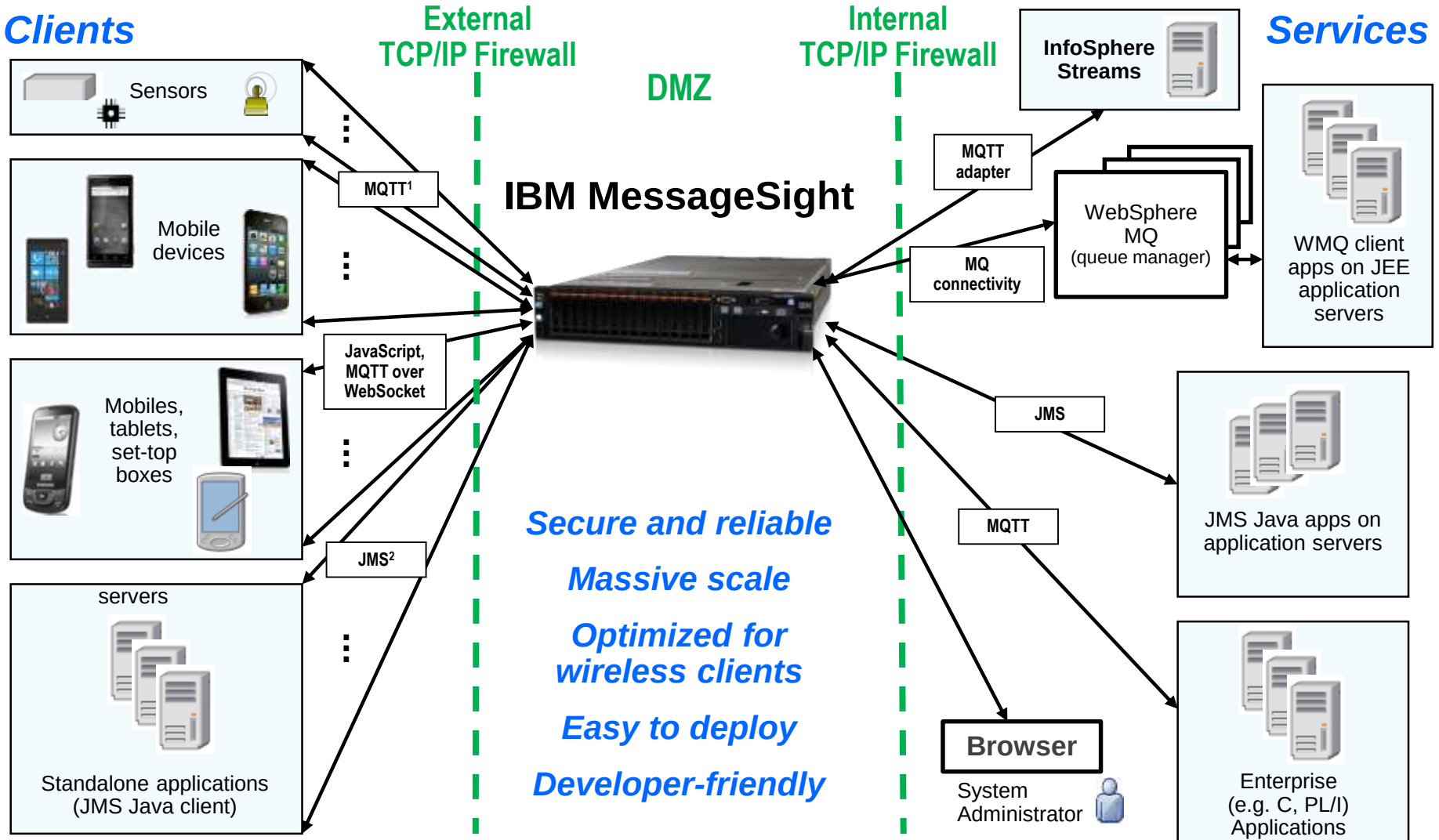
# (5) DataPower Mobile Security Features

*Available as a physical or virtual appliance*




- Security, Control, Integration & Optimization of mobile workload
- Enforcement point for centralized security policies
- Authentication, Authorization, **SAML**, OAuth 2.0, Audit
- Threat protection for XML and JSON
- Message validation and filtering
- Centralized management and monitoring point
- Traffic control / Rate limiting
- Integration with MobileFirst

# IBM MessageSight enables asynchronous mobile integration




[1] MQTT = Message Queuing Telemetry Transport connectivity protocol
[2] JMS support to include publish-subscribe and point-to-point domains; not Java EE JCA resource adapter

# Secure the Users & Devices for the Mobile Enterprise

MaaS360 by Fiberlink, an IBM company

ARXAN

Trusteer Mobile

IBM Security Access Manager

IBM WebSphere Datapower

IBM MessageSight

7. Protect during development
8. MobileFirst real time protection
9. Real-time DB security
10. Pro-active security actions
11. z/OS Connect security Auth

7

IBM Security AppScan

IBM InfoSphere Guardium

9

8

MobileFirst

JSON/https

SOAP/https

CICS
DB2
IMS

11

z/OS Connect

Linux

z/VM

z/OS

Hardware

z/OS

PKI Services

Cryptography cards

RACF

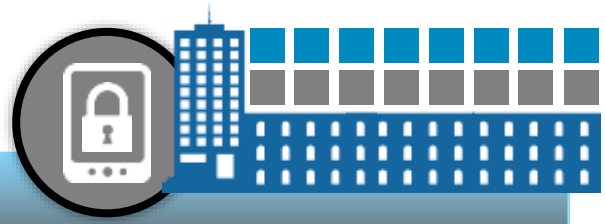
IDID

10

IBM Security zSecure

# (7) IBM Security AppScan

***Static, dynamic and interactive application security testing***



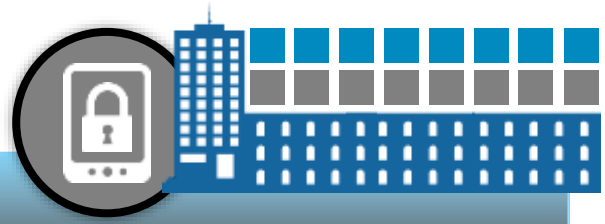
- **Challenge:** Build in security during development of mobile applications as well as assess the security of existing applications.
- **Solution:** Mitigate application security risk and establish policies, scale testing and prioritization and remediation of vulnerabilities.
- **Key benefits**
  - Promotes secure mobile application development
  - Provides enhanced mobile application scanning
  - Delivers comprehensive application security assessments to measure and communicate progress to stakeholders
  - Prioritizes application assets based on business impact and highest risk
  - Integrates with IBM MobileFirst projects

## More Information

- Free Trial
- Client Brochure
- Analyst Report
- Solution Brief

# (8) IBM MobileFirst platform

***Build and manage mobile applications with security***



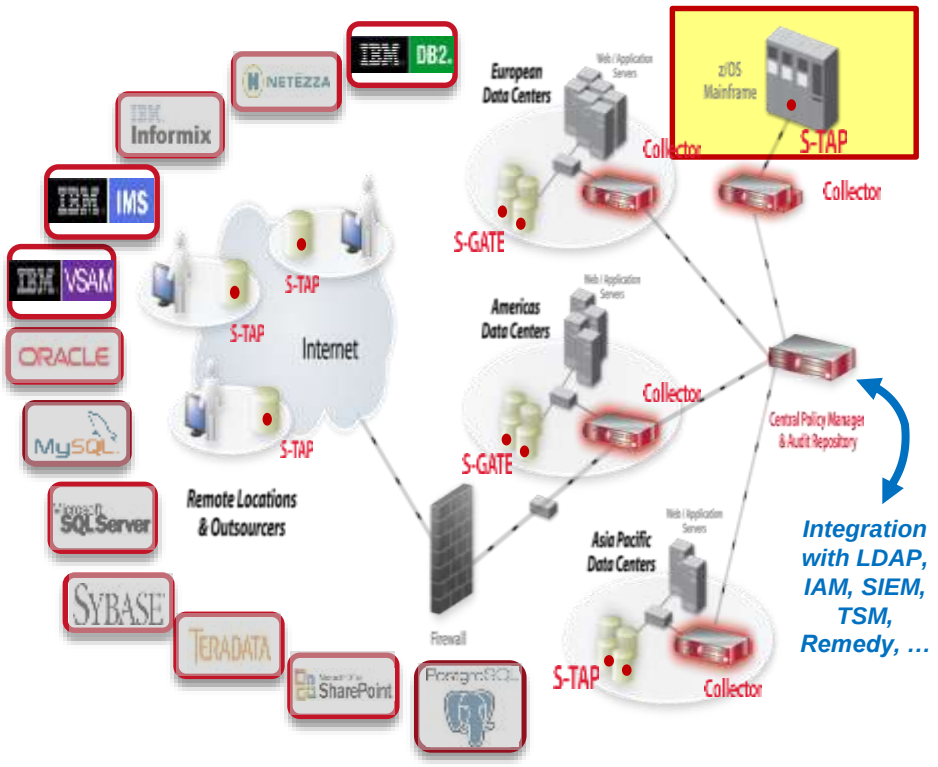
- **Challenge:** Create an open, comprehensive, but secure platform that manages HTML5, hybrid and native mobile apps.
- **Solution:** Secure the application, reduce both development and maintenance costs, improve time-to-market and enhance mobile app governance and security.
- **Key benefits**
  - **Support multiple mobile operating environments and devices** with the simplicity of a single, shared code base
  - **Connect and synchronize** with enterprise data, applications and cloud services
  - **Safeguard mobile security** at the device, application and network and adapter layer
  - **Govern your mobile app portfolio from a central interface**

## More Information

- Website
- Case Study
- Datasheet

# (9) IBM InfoSphere Guardium

*IBM Guardium Provides Real-Time Database Security & Compliance for Data at Rest, Data in Motion, and Configuration Data*




## Client Challenge

Companies must proactively prepare for data breaches and be made immediately aware when their data is at risk

## Solution

Protect data assets with activity monitoring, vulnerability analysis, data classification, data masking, entitlement reporting, actions blocking and data quarantine

## Key Benefits

- Continuous, policy-based, real-time monitoring of all database activities, including actions by privileged users
- Database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities
- Data protection compliance automation

# (10) IBM Security zSecure

*Automates routine RACF administration tasks and provides proactive compliance reporting for the mainframe operating system and sub-systems*

## Client Challenge

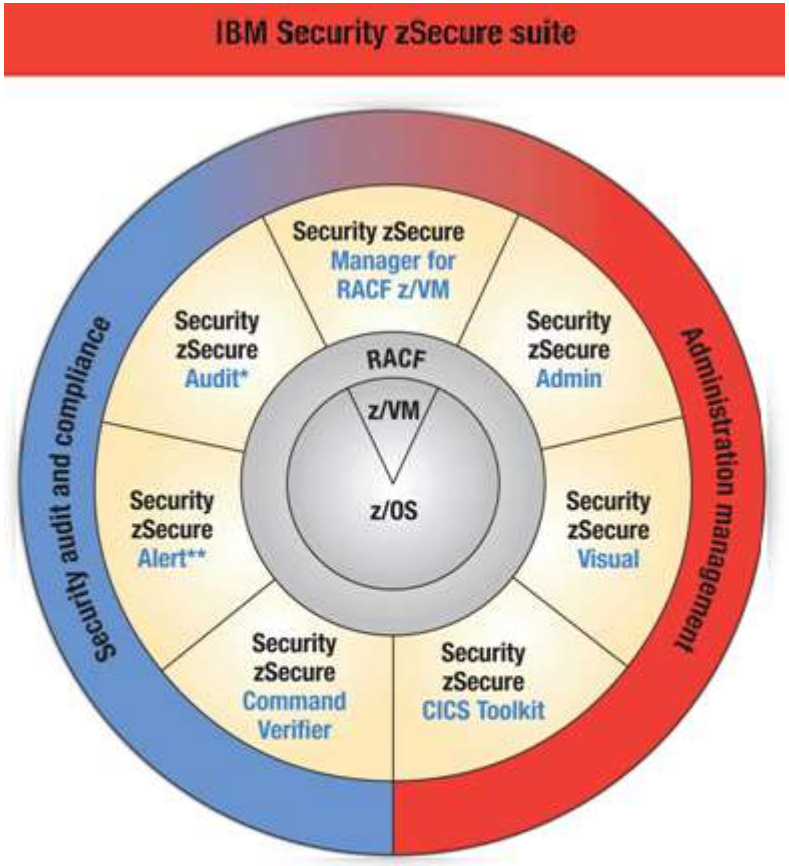
The mainframe is a complex platform; inattention to configuration management details can create vulnerabilities

## Solution

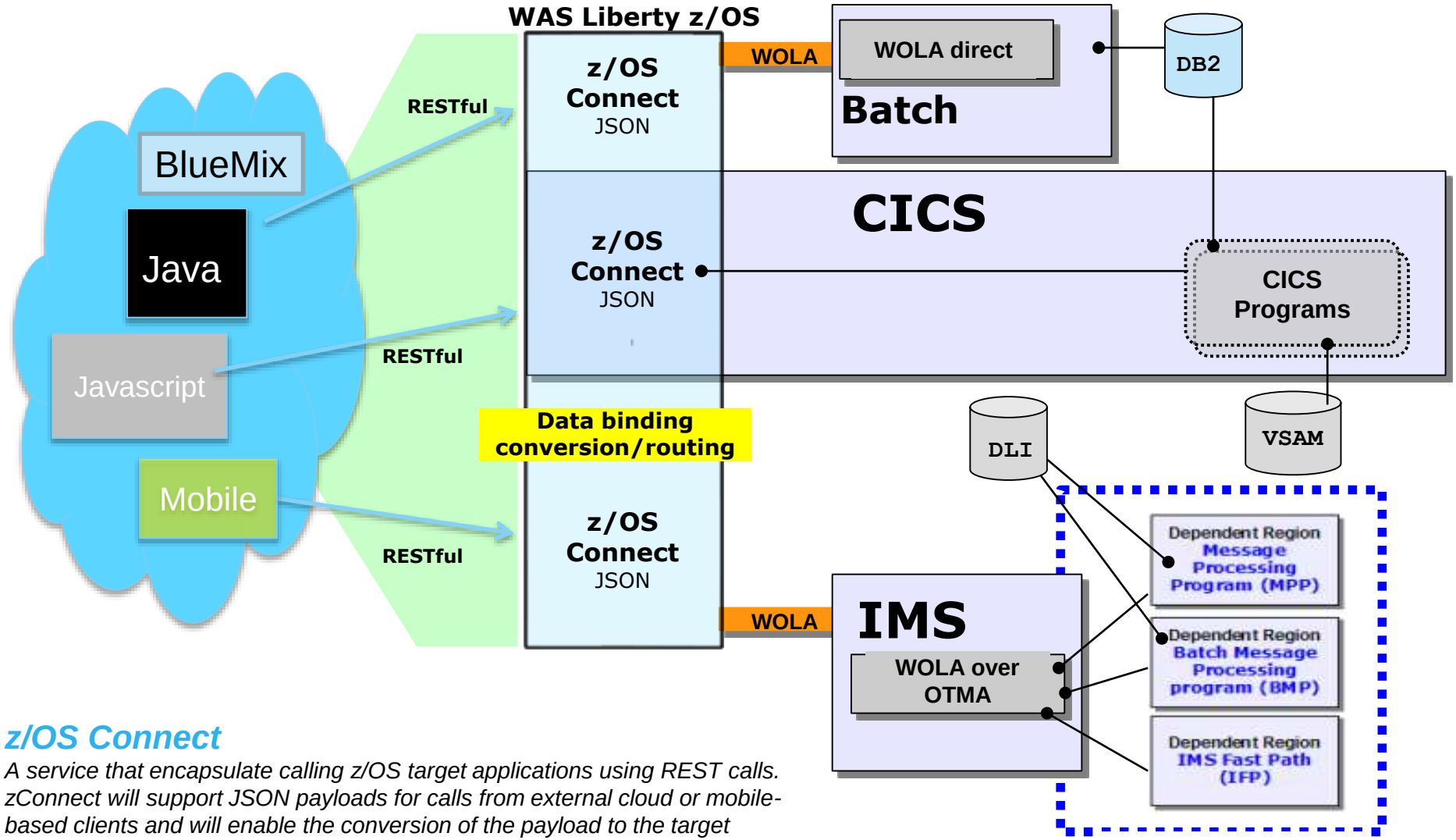
Automate proactive security scans and provide real-time alerts of suspicious activities

## Key Benefits

- Enables more efficient and effective RACF administration, using significantly less resources
- Automatically analyzes and reports on security events and detects security exposures
- Provide real-time mainframe threat monitoring allowing you to monitor intruders



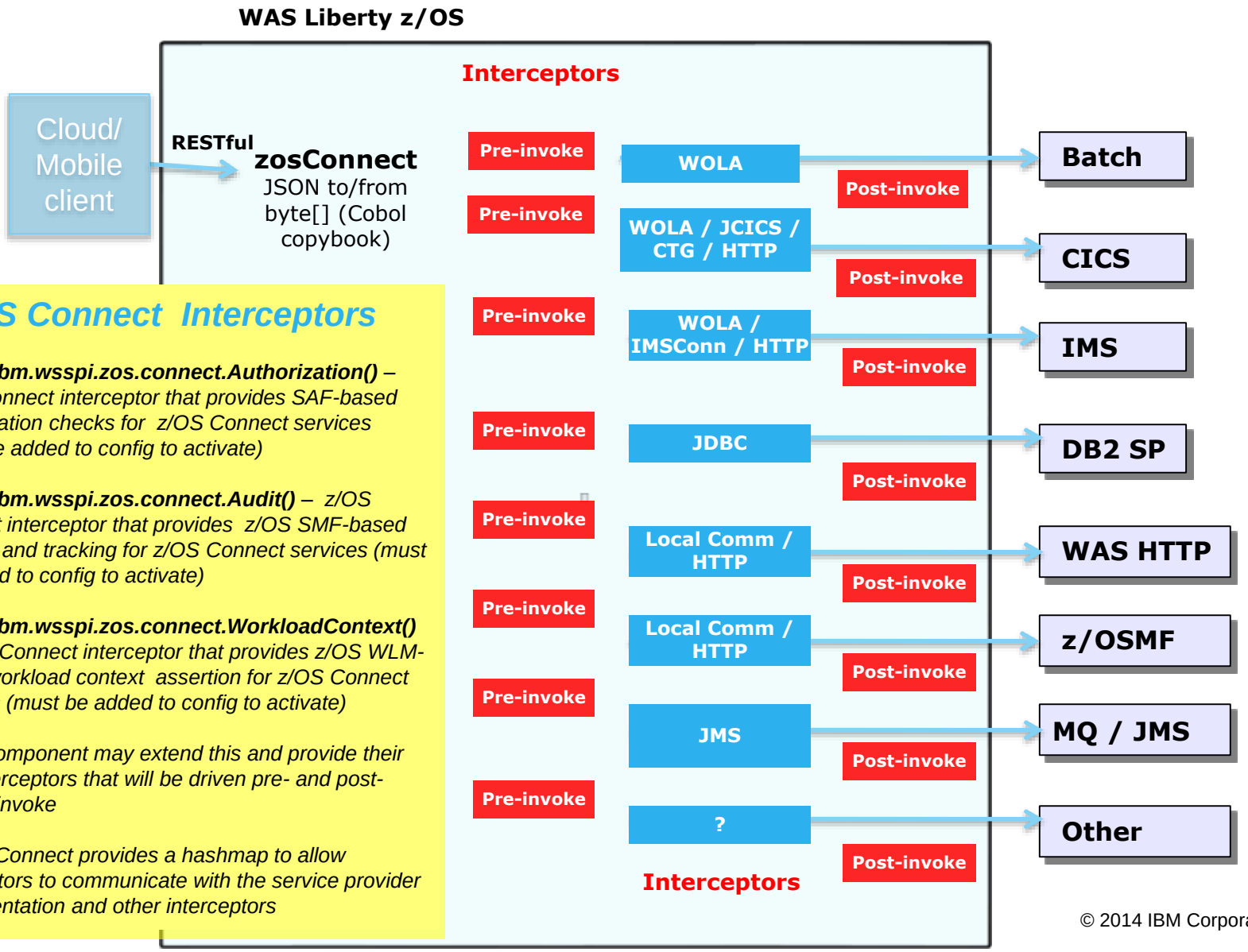
# (11) Access to z/OS via z/OS Connect with increased security




## *z/OS Connect*

*A service that encapsulate calling z/OS target applications using REST calls. zConnect will support JSON payloads for calls from external cloud or mobile-based clients and will enable the conversion of the payload to the target program's expected format (WOLA – WebSphere Optimized Local Adapters). It will also provide the response payload conversion from a byte array into JSON format before returning the response to the caller.*

# z/OS Connect - Security Interceptors




## *z/OS Connect Interceptors*

- ***com.ibm.wsspi.zos.connect.Authorization()*** – *z/OS Connect interceptor that provides SAF-based authorization checks for z/OS Connect services (must be added to config to activate)*

- ***com.ibm.wsspi.zos.connect.Audit()*** – *z/OS Connect interceptor that provides z/OS SMF-based auditing and tracking for z/OS Connect services (must be added to config to activate)*

- ***com.ibm.wsspi.zos.connect.WorkloadContext()*** – *z/OS Connect interceptor that provides z/OS WLM-based workload context assertion for z/OS Connect services (must be added to config to activate)*

- *Any component may extend this and provide their own interceptors that will be driven pre- and post-service invoke*

- *z/OS Connect provides a hashmap to allow interceptors to communicate with the service provider implementation and other interceptors*

# IBM System z Core Capabilities

*Resilience and security have long been hallmarks of mainframe computing, making System z the application computing platform of choice*

## Client Challenge

Customer's security challenges are compounded by starting with less secure computing platforms.

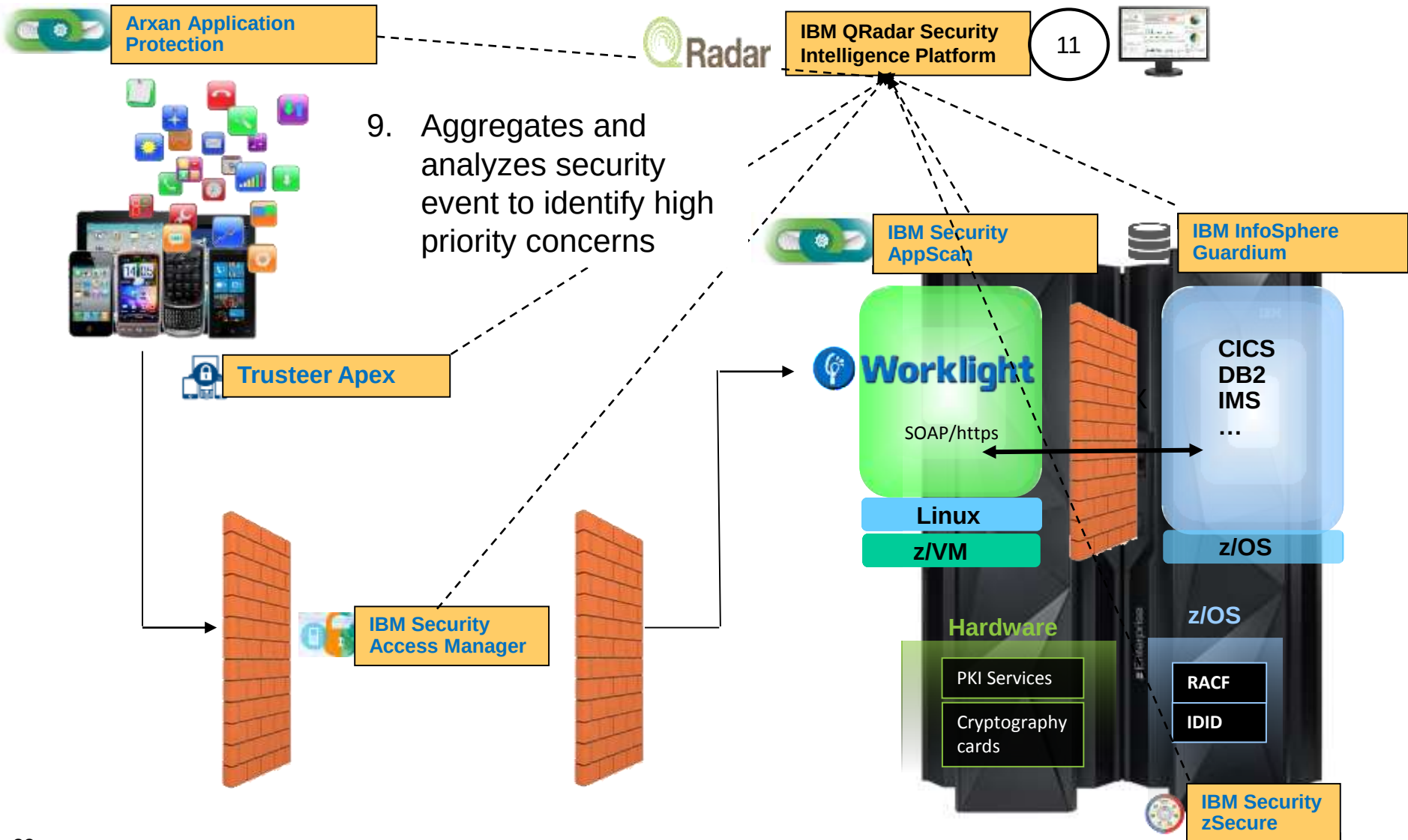
## Solution

z/OS has the highest security rating or classification of any commercially available system

## Key Benefits

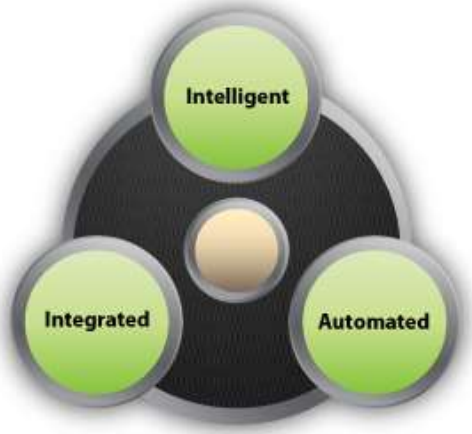
- **RACF** and **IBM Distributed Identity Data** (IDID) provides discrete, end to end authentication, transactions auditing, and identity mapping
- Cryptography options supports advanced encryption processing
- PKI services centrally manage certificates
- High level security connection to backend applications via hipersockets or IEDN

# (11) End-to End Real-time security intelligence for the Mobile



# (11) IBM QRadar Security Intelligence

*Deliver mobile security intelligence by monitoring data collected from other mobile security solutions – visibility, reporting and threat detection*




## Client Challenge

Visibility of security events across the enterprise, to stay ahead of the threat, show compliance and reduce risk

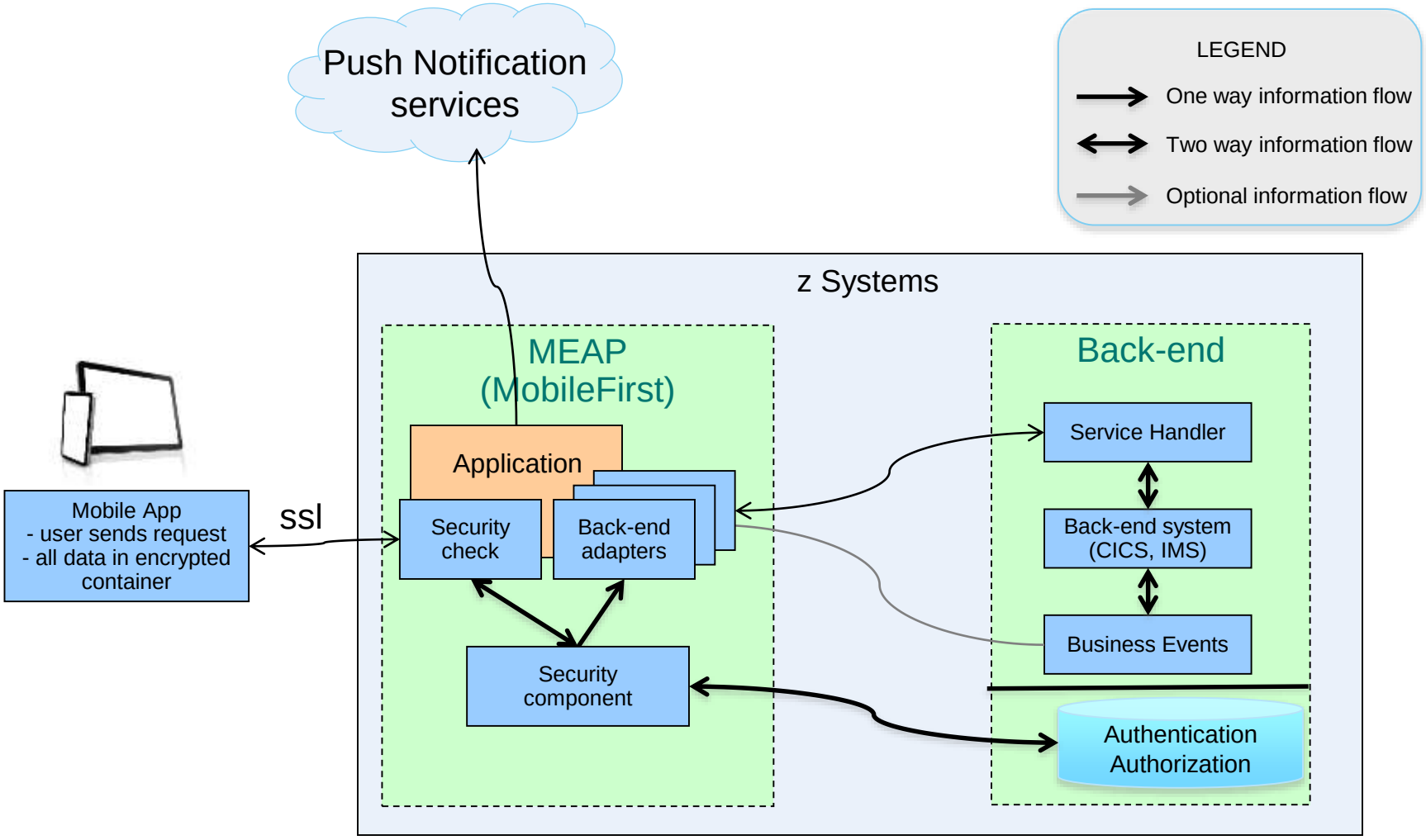
## Solution

Use event correlation to identify high probability incidents and eliminate false positive results

## Key Capabilities

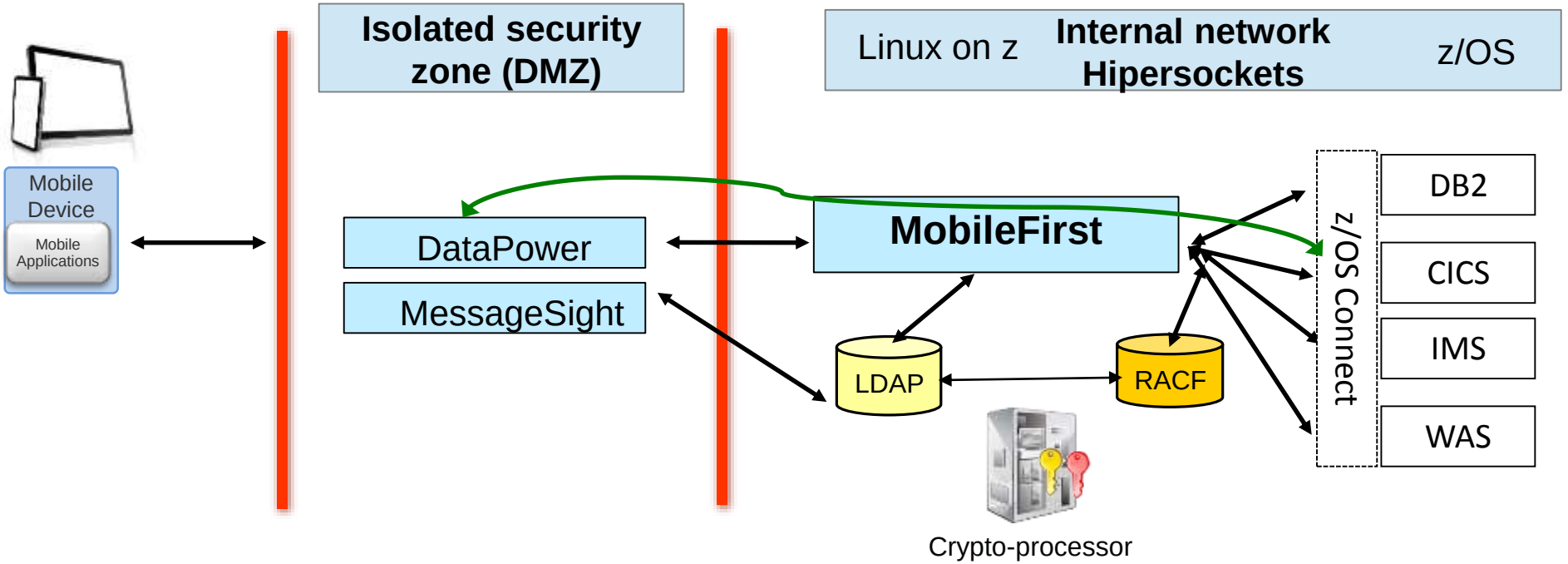
- Document user, application and data activity to satisfy compliance reporting requirements
- Protect private data and intellectual property by detecting advanced persistent threats
- Inspect network device configurations, visualize connections and perform attack path simulations to understand assets at risk
- zSecure Audit enriches the event data with information from the security database and system snapshot (CKFREEZE) information

# Summary: Operational setup



# Topology – DataPower as a reverse proxy for MobileFirst Platform

| Capabilities | Deployment scenario | System z benefits |
|---|---|---|
| • Combined capabilities of MobileFirst and DataPower (DP) or MessageSight (MS)<br>• DP or MS in an isolated secured network zone DMZ – DeMilitarized Zone | • When hybrid mobile apps use a combination of web and Restful interactions<br>• Secured high volume of internet and mobile access<br>• Shared crypto on z capabilities | • Additional benefits of DataPower as a mobile security gateway for MobileFirst on Linux on z<br>• LDAP user registry shared between DataPower and MobileFirst<br>• Integration of LDAP and RACF |



# 2. How do you **expose** and **secure** your capabilities?


verizon

Secures and manages traffic across its mobile network – safeguarding and processing over **20 million** mobile transactions per day

# 1. How do you **Open** existing systems to reinvent the secure way you engage?

BlueCross BlueShield of North Carolina

Enhanced connectivity between internal and external systems to help drive nearly **1,500-fold growth** over three years—while cutting the time and cost to deliver new projects by up to **80%**.

# Mobile security benefits on IBM z Systems

## Business challenges

Mobile is about re-imagining your business around constantly connected customers, partners and employees. to sell products or retain customers.

## Business solution & Benefits

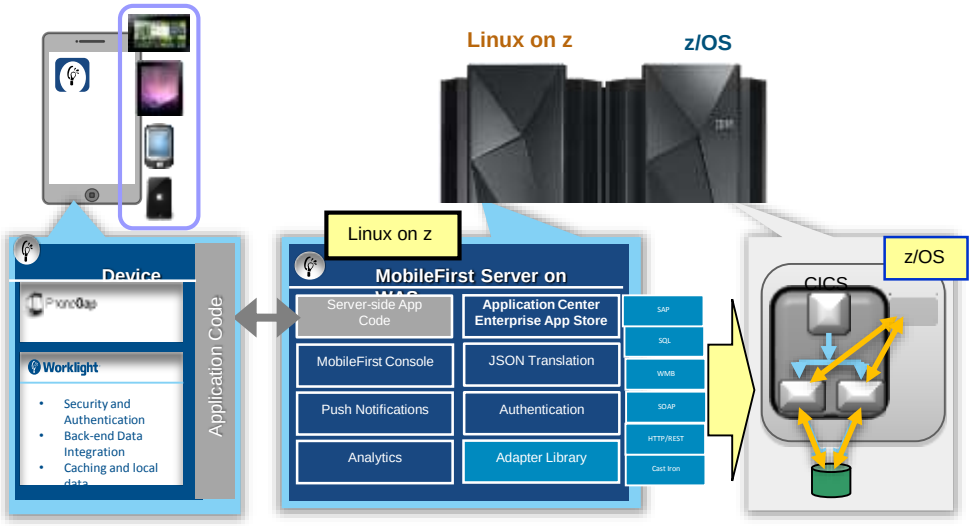
Mobile solutions are pushing companies to rethink the user experience, from the presentation of data to the interaction.

The mobile engagement allows you to build new insight into your customer's behavior so that you can anticipate their needs and gain a competitive advantage by offering new services.

## IT Challenges

Mobile has characteristics that causes to rethink or redefine IT architectures and implementations.

- Unpredictable workloads that can vary any minute of the day.
- Very high demanding customers that expects 24/7/365 to be serviced. With fast response times.
- The security of Mobile ranges from mobile Endpoint security to prevent malicious attacks on back end systems. And everything in between.
- Integrating mobile apps into existing application landscape.




## Infrastructure benefits

- Massive scalability in a single footprint, to handle the workload of millions of devices and sensors
- Workload Management to provide a quick reaction to sharp spikes in demand
- Hardware encryption speeds SSL applications
- System z may also have other roles in the overall security architecture e.g security policy management, certificate and key management
- Business Resiliency for critical mobile apps
- Integration of co-located existing Applications, Services and Systems of Record

# Gartner has recognized IBM as a leader in the Magic Quadrant for Mobile Application Development Platforms

Magic Quadrant for Mobile Application Development Platforms
Ian Finley, Van L. Baker, Ken Parmelee, David Mitchell Smith, Ray Valdes, Gordon Van Huizen
Aug 7, 2013

*"As unprecedented numbers of enterprises build mobile applications, the mobile application development platform market continues to grow and evolve rapidly."*

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 full report is available at http://ibm.co/13TU2Dm

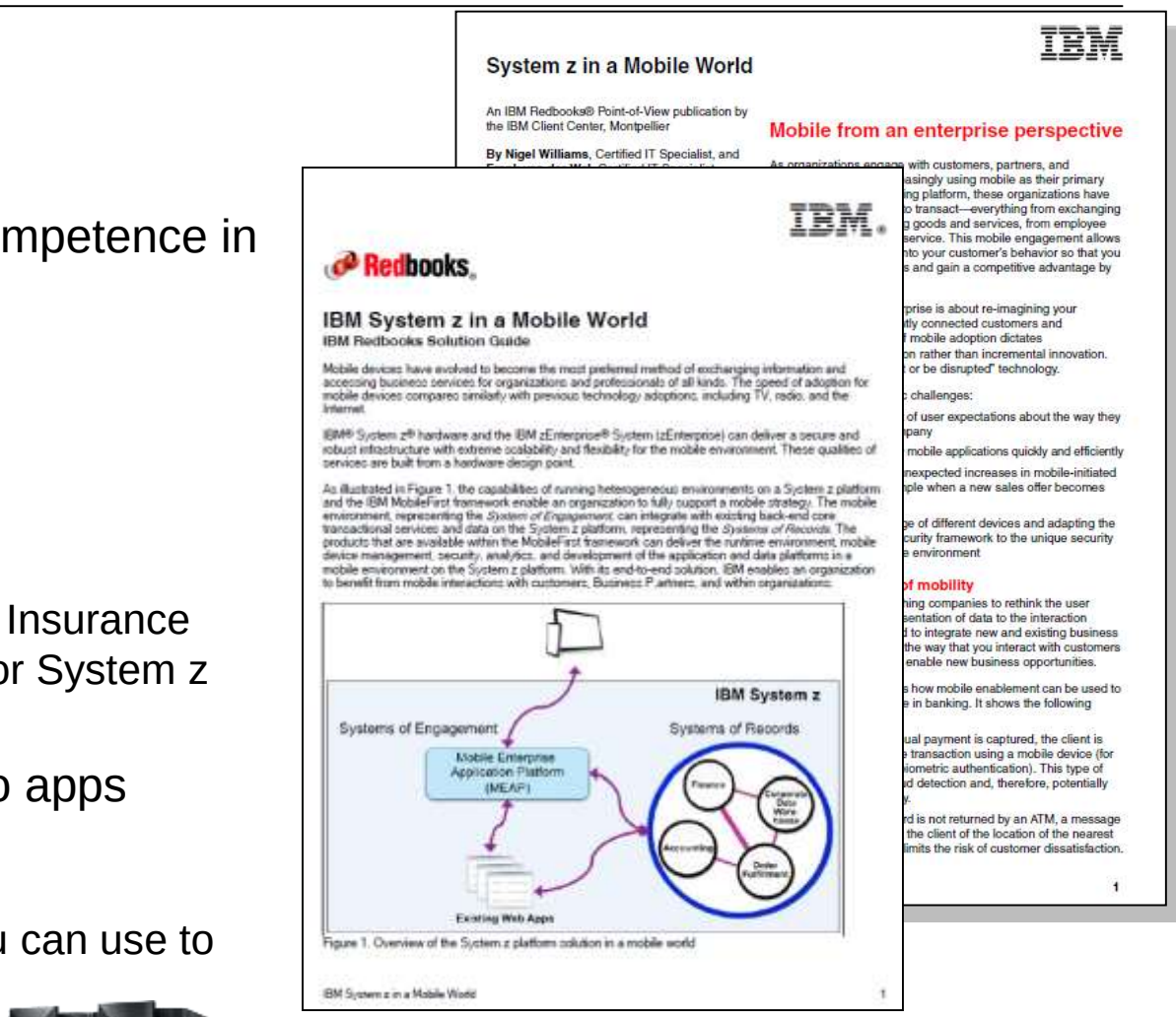
Figure 1. Magic Quadrant for Mobile Application Development Platforms


Source: Gartner (August 2013)

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

# Interested in mobile and System z Next steps…

- Contact a Mobile Center of competence in Boeblingen or Montpellier
- Point-of-View paper.
- Mobile Solution Guide
- Point of Value Mobile security
- Request a Demo.
  - Banking, Retail, Government, Insurance
  - Deploy MobileFirst on Linux for System z
  - Reuse z/OS transactions
- Try the System z Mobile demo apps
  - CICS GENAPP
  - CICS EGUI
  - IBM Remote. Sample App you can use to manage z HMC
- System z Mobile home page
  - Customer case studies
  - Analyst reports
  - Customer Videos

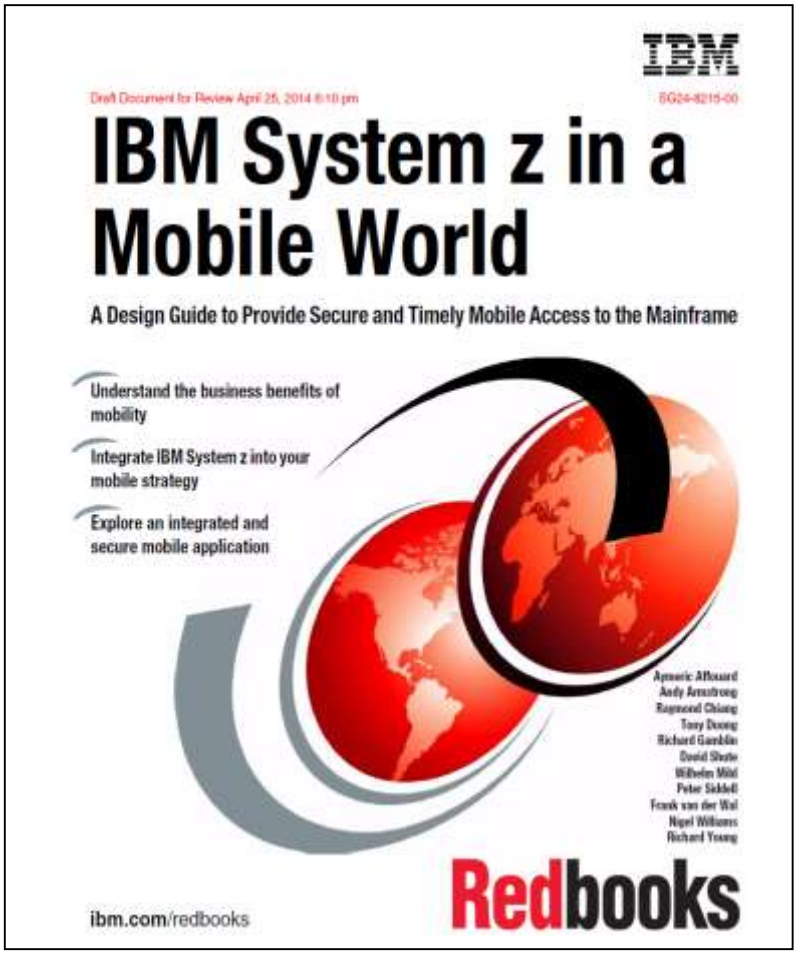



# Redbook – draft available

- **Understanding the business context in a mobile world**
  1. Business drivers
  2. IBM MobileFirst
  3. SoE and SoR
  4. IBM Worklight
  5. Industry use cases

- **Architecting and planning the solution**
  6. Deployment models
  7. Enterprise architecture
  8. Designing for resilience
  9. Designing for security

- **Customer scenario**
  10. Overview of scenario
  11. Agile approach to deliver applications
  12. Deploying to a HA infrastructure
  13. Enabling E2E security
  14. Mobile analytics




http://www.redbooks.ibm.com/redpieces/abstracts/sg248215.html?Open





48

http://www-03.ibm.com/security/mobile/



# IBM Security



## Finally, security is in your hands

### Confidently protecting the mobile enterprise


The line between work and personal technology use is blurring. As smartphones, tablets and other handheld devices proliferate, they increasingly blend organizational, personal and sensitive data. This introduces substantial security risks at the data, application and network levels. Especially when a single click or a rogue application can expose your entire enterprise to threats.

As a mobile security leader, IBM Security has created a New Mobile Security Framework (Youtube, 00:07:09). This comprehensive approach to Mobile security enables trusted, higher-quality interactions at the device, content, application and transaction level. We have

### Contact IBM

Considering a purchase?

Email IBM

Request a quote

Or call us at: +1(506)449-7901
Priority code: 102PW03W

### Securing the mobile enterprise with IBM security solutions


→ Read this solutions brief to find out how IBM's New Mobile Security framework can help protect your enterprise (PDF, 802KB)

### IBM Threat Protection System

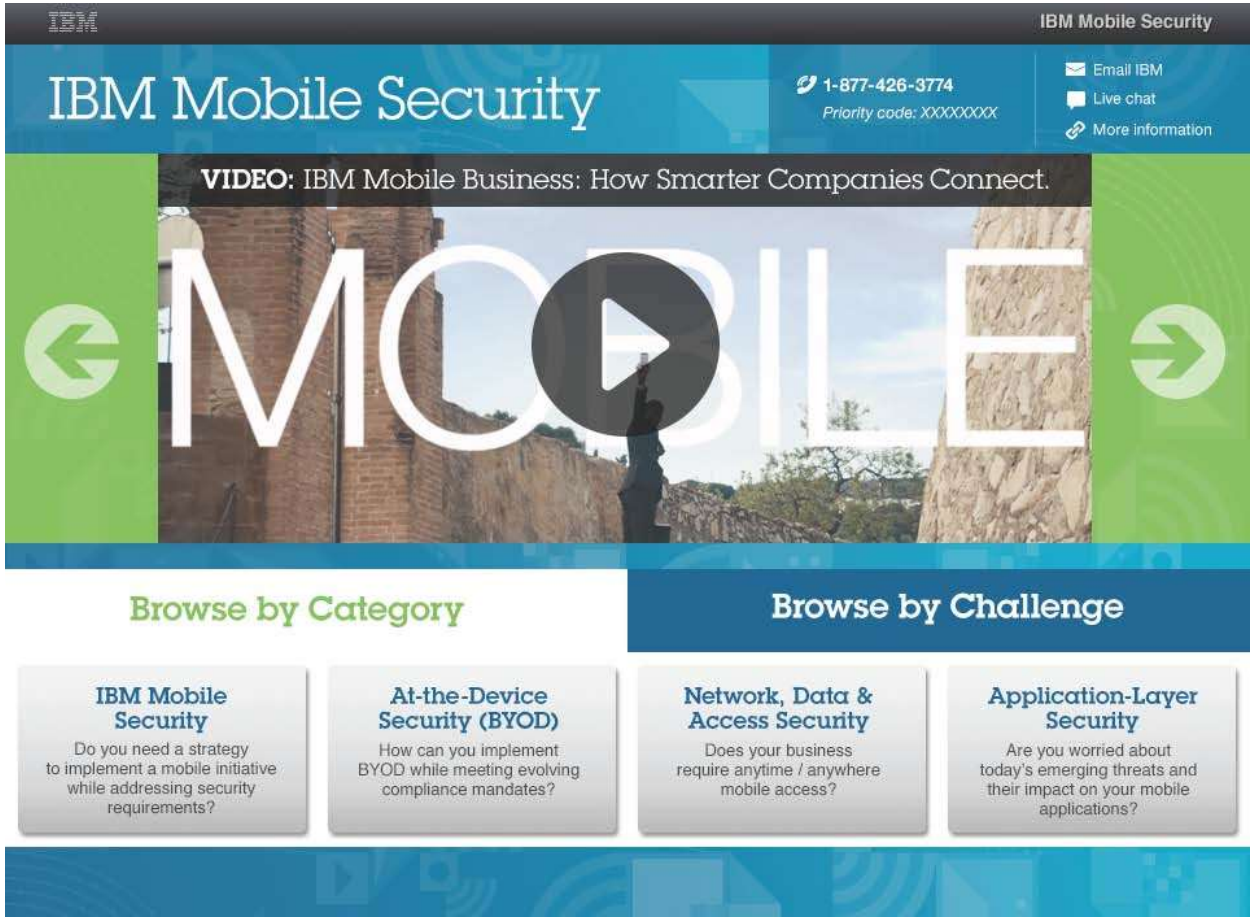
Prevention is possible. Discover how the latest advances in Threat Protection can keep your

# Looking for more information to Secure your Mobile Enterprise? Use the IBM Mobile Security Solution Finder

.

**Two ways to find the information you need to select the best mobile security solution for your business :**

- By category: Identifies component area for enforcing security within the mobile enterprise.
- By challenge: Identifies common requirements and connects to assets that best address these concerns.



# Additional information in Mobile Redbooks

- ***Transform Your Organization into a Mobile Enterprise with IBM Worklight***, *Solution Guide,* published 9 October 2013
- ***Extending Your Business to Mobile Devices with IBM Worklight***, SG24-8117-00 ***Red****books,* published 12 August 2013
- ***IBM MobileFirst Strategy Software Approach***, SG24-8191-00 *Draft* ***Red****books, 5* December 2013
- ***IBM System z in a Mobile World***, *Solution Guide,* published 21 February 2014
- ***System z in a Mobile World***, REDP-5088-00, *Point-of-View,* 24 January 2014
- ***Implementing IBM CICS JSON Web Services for Mobile Applications***, TIPS1066 *Solution Guide,* 9 September 2013
- ***Securing Your Mobile Business with IBM Worklight***, SG24-8179-00, 7 October 2013
- ***Enabling Mobile Apps with IBM Worklight Application Center***, REDP-5005-00 ***Red****papers,* 1 June 2013
- ***Responsive Mobile User Experience Using MQTT and IBM MessageSight***, SG24-8183-00 *Draft* ***Red****books,* last update 18 December 2013
- ***Mobilizing Employees with IBM Notes Traveler***, *Solution Guide,* published 19 February 2013

# Questions?

***Wilhelm Mild***

*IBM Executive IT Architect*
*for Mobile and z Systems*

The Open Group Open Certified Distinguished Architect

*IBM Deutschland Research & Development GmbH*
*Schönaicher Strasse 220*
*71032 Böblingen, Germany*

*Office: +49 (0)7031-16-3796*
*wilhelm.mild@de.ibm.com*





52

# THE END

# Trademarks

- This presentation contains trade-marked IBM products and technologies. Refer to the following Web site:

  http://www.ibm.com/legal/copytrade.shtml