

Learn to Talk to Your Clients about Security for zMobile

December, 2014

[Robert Kennedy](#)



You know? you can do this
with your mobile device now.



Mobile Adoption continues to march on...

In Context - 7 Billion people on the planet

- 3.5 billion people use toothbrushes
- 4.5 billion people with access to a working toilet
- **6 billion Mobile Devices**



Marc Andreessen: “Even the poorest people in the world will choose smartphone and internet access even over indoor plumbing & electricity, given the choice”

Mobile is becoming the “primary” platform for users

- 1/3 government web site visits come from mobile
- 20% of online financial transactions are from mobile
- 81% of adults use personally owned devices for business
- 91% of adults have their smartphone within reach



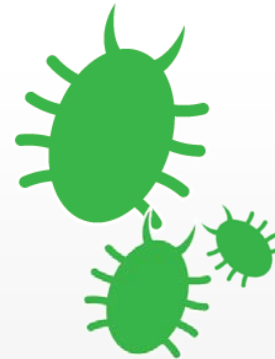
As mobile grows, so do security threats for our customers



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

Mobile malware grew

155%  in 2011

614%       

from March 2012 to March 2013



73% of all malware exploit holes in mobile payments by sending fraudulent premium SMS messages, each generating around **\$10** USD in immediate profit



Android is responsible for **92%** of all known mobile malware. An increase from **47%** in 2012...

...a significant threat given more than

1 BILLION

Android-based smart phones are estimated to be shipped in 2017

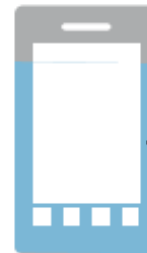
Source: Canals Smart Phone Report, June 2013



There are more than

500

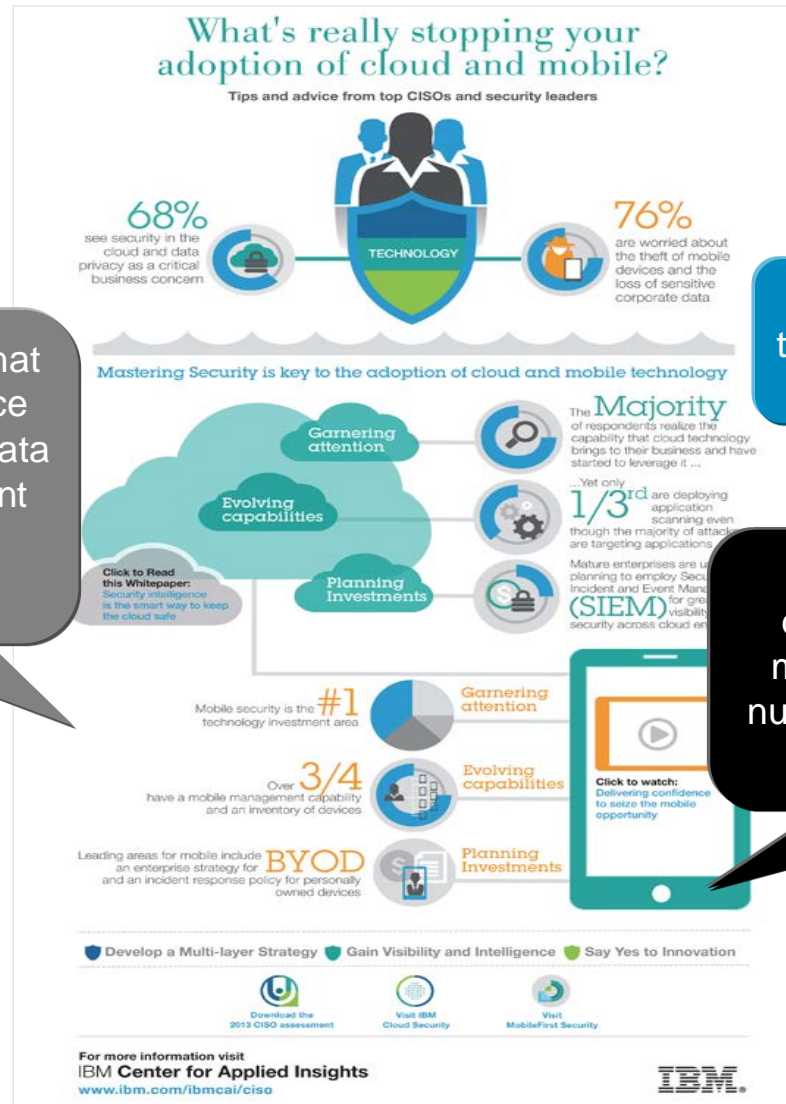
third-party app stores containing malicious apps



77% of Android threats could be largely eliminated today if all Android devices had the latest OS. Currently only **4%** do

Source: Juniper Mobile Threat Report, 2013

Business must adapt and redefine security for mobile



"76% of responders say that the loss of a mobile device with access to corporate data could result in a significant security event."

"Mobile security is the #1 technology investment area."

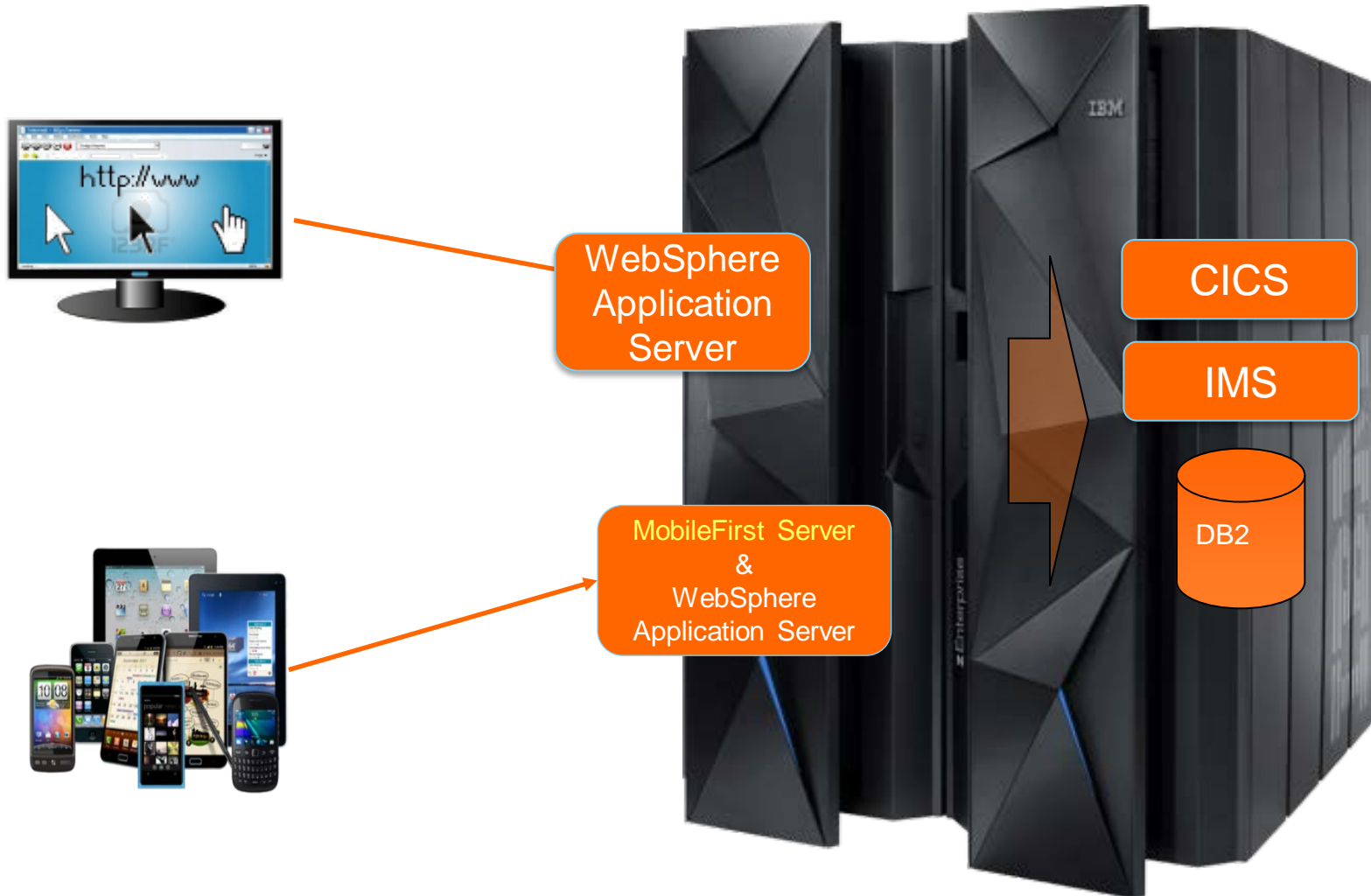
"Although many are planning to develop an enterprise strategy for mobile security (39%), a significant number have not done so yet (29%)."

But the mobile revolution will put huge demands on business and IT

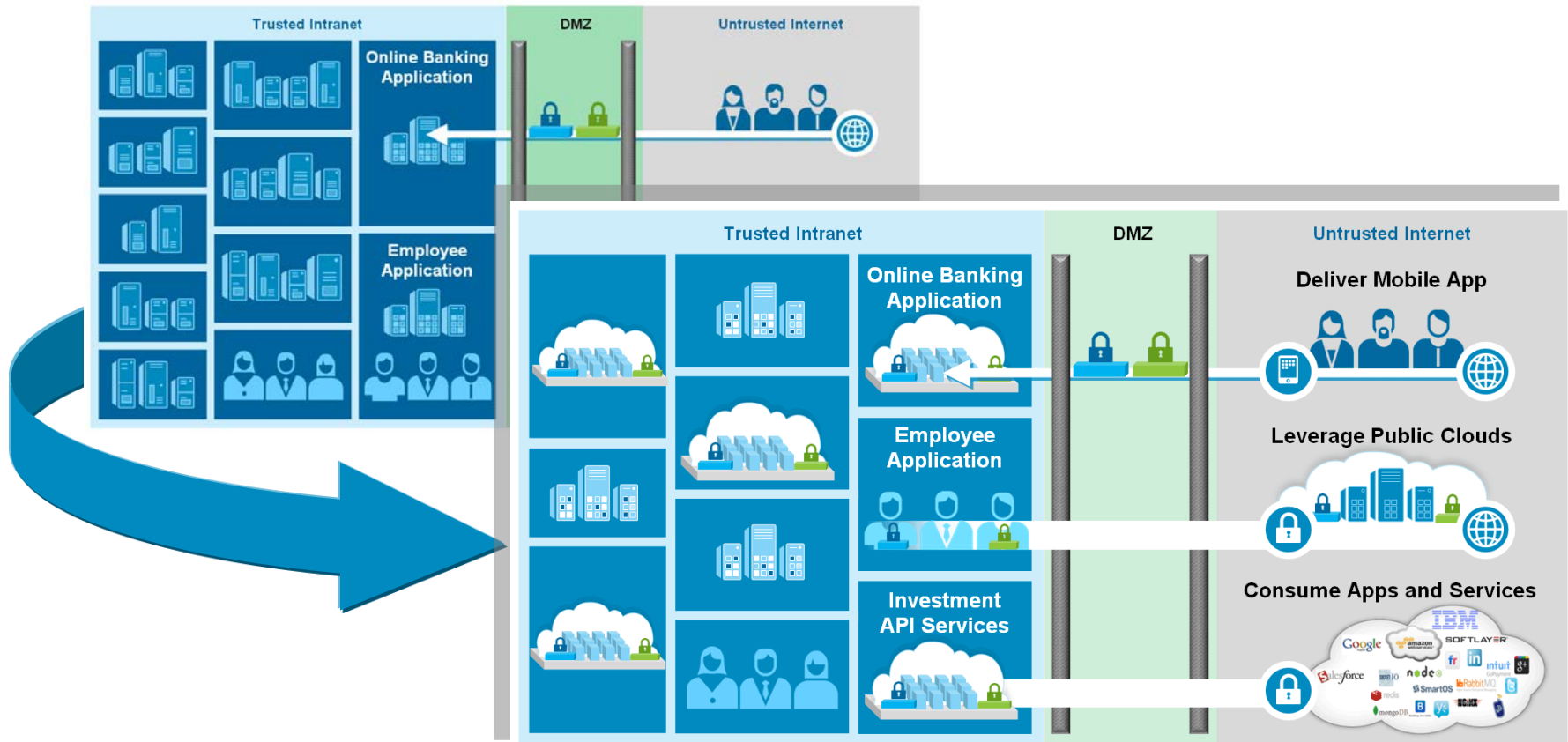
- Security and privacy are paramount, of course
- But additionally
- Inconsistent peaks 24/7 will be common
 - Increased system load
 - New versions of apps occurring weekly (or more frequently) vs. yearly
 - Development, control and support of apps and multiple devices will not be standard



Mobile is simply a new channel into the Enterprise



Mobile is changing the way we view the perimeter



Imperatives to securing the mobile enterprise

CISO / CIO
Chief Information Security Officer
Chief Information Officer



- Mitigate security risk across devices, applications, content and transactions
- Monitor enterprise security across all endpoints
- Manage mobility across the enterprise

IT Operations



Line-of-Business Application Developer



Security Specialist



Device Security

- Manage the mobile enterprise with BYOD, BYOA, secure e-mail and document sharing

Content Security

- Secure file and document sharing across devices and employees including integration with SharePoint

Application Security

- Instrument applications with security protection by design
- Identify vulnerabilities in new, existing or purchased applications

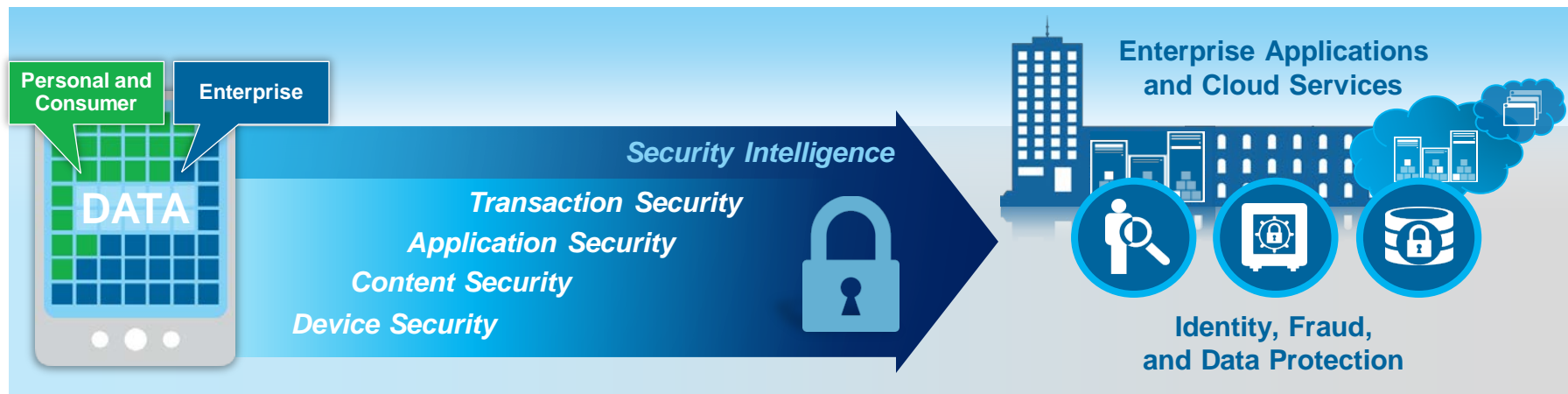
Transaction Security

- Secure mobile transactions from customers, partners and suppliers

Security Intelligence

Correlate mobile security events with broader infrastructure including log management, anomaly detection and vulnerability management for proactive threat avoidance

IBM Security capabilities for the mobile enterprise



<i>Device Security</i>	<i>Content Security</i>	<i>Application Security</i>	<i>Transaction Security</i>
<ul style="list-style-type: none"> Solutions to manage a diverse set of mobile devices from corporate owned assets to BYOD, all from the cloud 	<ul style="list-style-type: none"> Solutions to help secure file and document sharing across devices and SharePoint 	<ul style="list-style-type: none"> Solutions to develop applications with security by design Protect enterprise data in both the applications you build and the applications you buy 	<ul style="list-style-type: none"> Solutions to help protect mobile transactions with customers, business partners and temporary workers that are not part of your enterprise mobile management framework

Security Intelligence

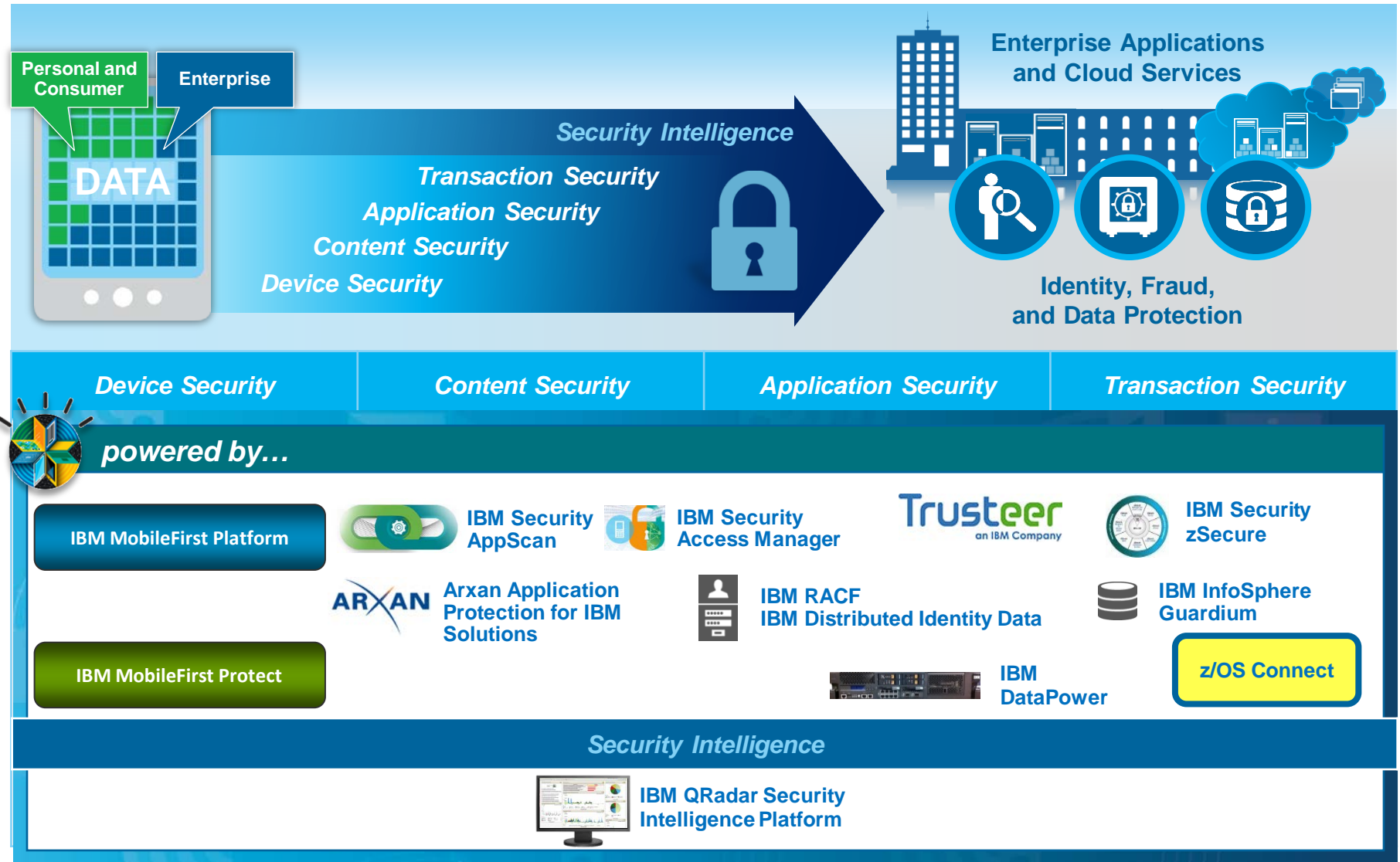
A unified architecture for integrating mobile security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management

Security features capabilities for the mobile enterprise



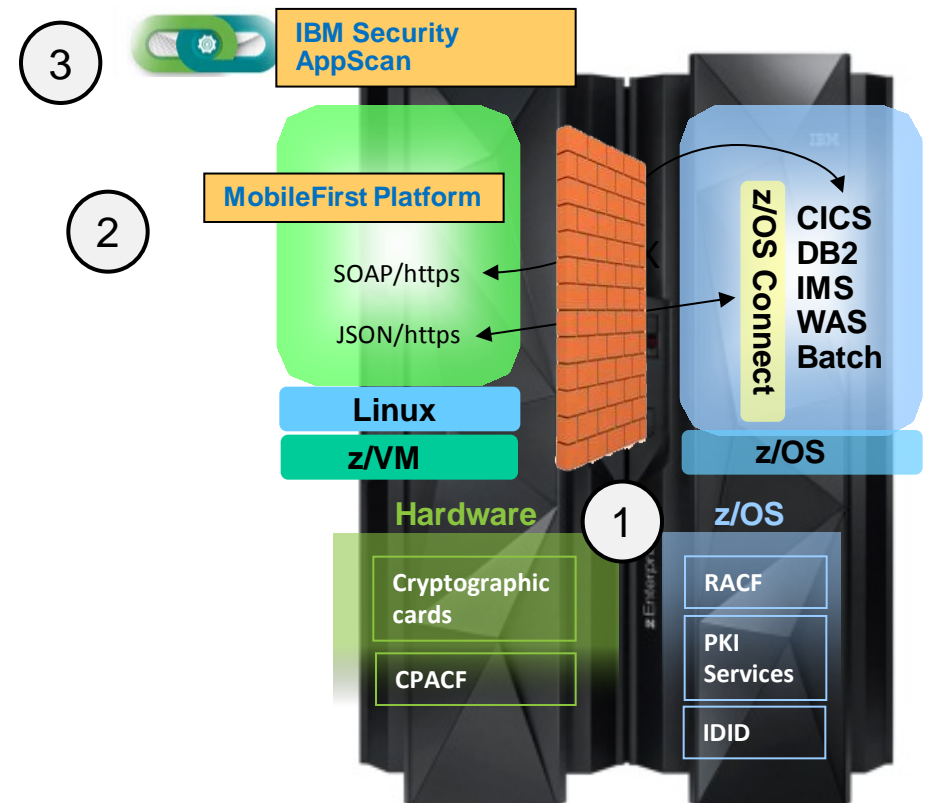
Device Security	Content Security	Application Security	Transaction Security
<ul style="list-style-type: none"> Enroll, provision and configure devices, settings and mobile policy Fingerprint devices with a unique and persistent mobile device ID Remotely Locate, Lock and Wipe lost or stolen devices Enforce device security compliance: passcode, encryption, jailbreak / root detection 	<ul style="list-style-type: none"> Restrict copy, paste and share Integration with Connections, SharePoint, Box, Google Drive, Windows File Share Secure access to corporate mail, calendar and contacts Secure access to corporate intranet sites and network 	<p>Software Development Lifecycle</p> <ul style="list-style-type: none"> Integrated Dev Environment iOS / Android Static Scanning <p>Application Protection</p> <ul style="list-style-type: none"> App Wrapping or SDK <i>Container</i> Hardening & Tamper Resistance <i>IBM Business Partner (Arxan)</i> Run-time Risk Detection <i>Malware, Jailbreak / Root, Device ID, and Location</i> Whitelist / Blacklist Applications 	<p>Access</p> <ul style="list-style-type: none"> Mobile Access Management Identity Federation API Connectivity <p>Transactions</p> <ul style="list-style-type: none"> Mobile Fraud Risk Detection Cross-channel Fraud Detection Browser Security / URL Filtering IP Velocity
<p>Security Intelligence</p> <p>Advanced threat detection with greater visibility</p>			

Security solutions for the mobile enterprise



Building and Maintaining Secure Enterprise Mobile Applications

1. Start with the most secure operating system, applications and database
2. Build, deliver, deploy & maintain secure mobile applications
3. Identify and correct security vulnerabilities as the application is developed and maintained



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

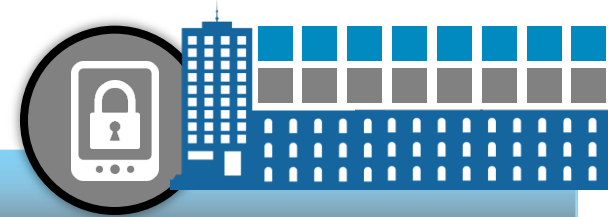
Key Benefits

- RACF and IDID provides discrete, end to end authentication, transaction auditing, and identity mapping
- Cryptography options supports advanced encryption processing
- PKI services centrally manage certificates
- High level security connection to backend applications via hipersockets



IBM MobileFirst Platform

*Build and manage mobile applications
with security*



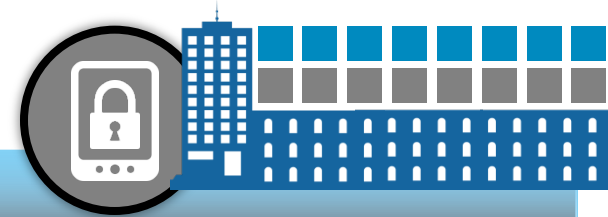
- **Challenge:** Create an open, comprehensive, secure platform that manages HTML5, hybrid and native mobile apps.
- **Solution:** Secure the application, reduce both development and maintenance costs, improve time-to-market and enhance mobile app governance and security.
- **Key benefits**
 - **Support 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 layer
 - **Govern your mobile app portfolio from a central interface**

More Information

- [Website](#)
- [Case Study](#)
- [Datasheet](#)

IBM Security AppScan

Static, dynamic and interactive application security testing



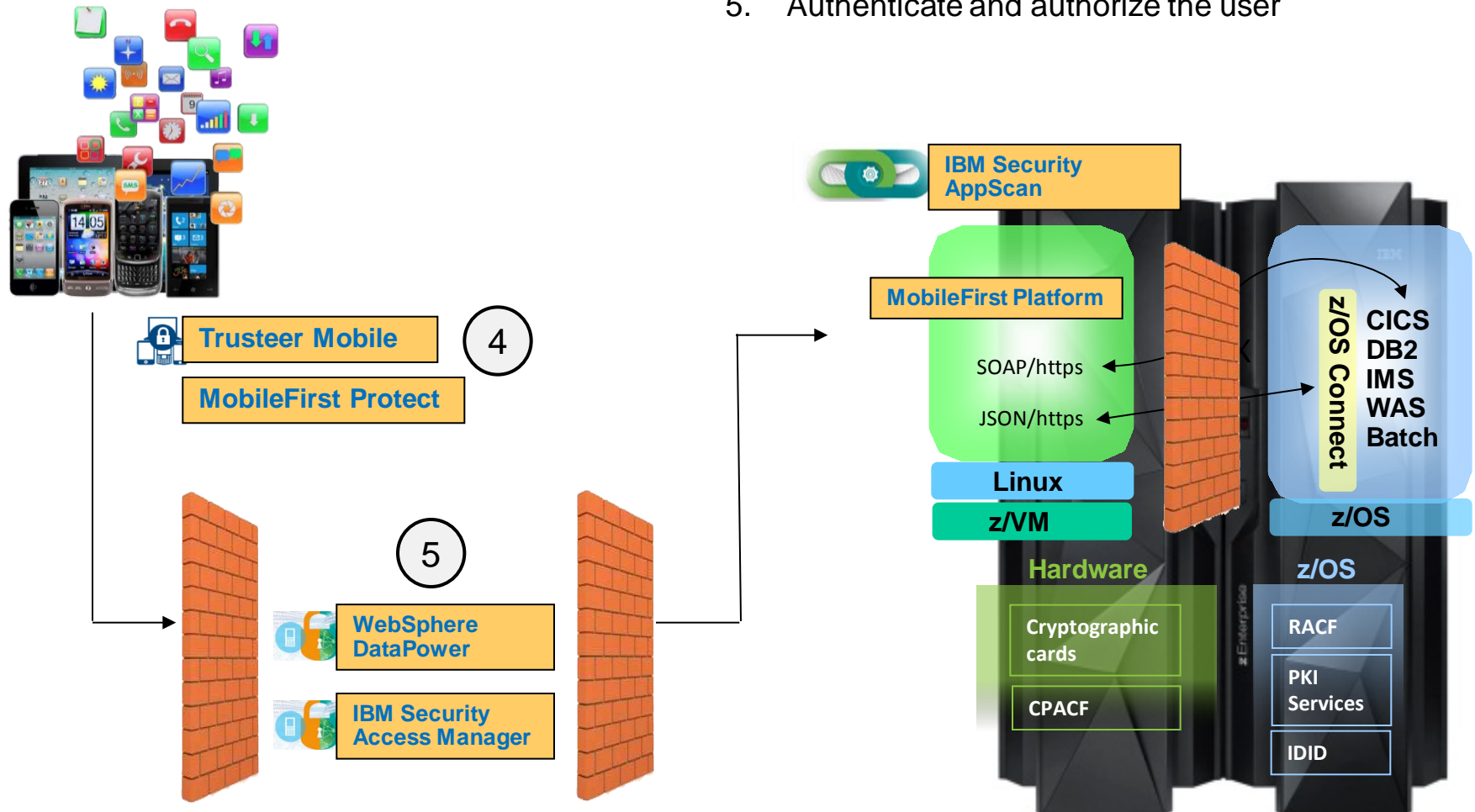
- **Challenge:** Build in security during development of mobile applications as well as assess the security of existing applications.
- **Solution:** Mitigate application security risk and establish policies, scale testing and prioritization and remediation of vulnerabilities.
- **Key benefits**
 - Promotes 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 Platform projects

More Information

- [Free Trial](#)
- [Client Brochure](#)
- [Analyst Report](#)
- [Solution Brief](#)

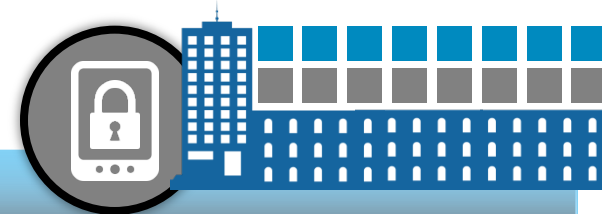
Secure the Users & Devices for the Mobile Enterprise

4. Secure the device
5. Authenticate and authorize the user



MobileFirst Protect 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

More Information

- [Data Sheets](#)
- [Videos](#)
- [Case Studies](#)
- [White Papers](#)
- [Free 30-day Trial](#)

Trusteer Mobile

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



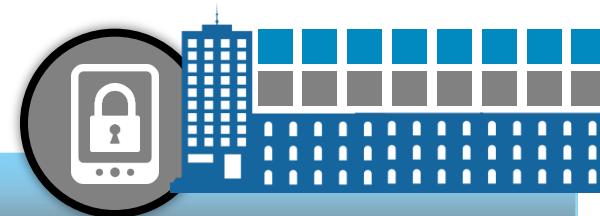
- **Challenge:** Compromised devices and applications create fraud risk and an insecure environment.
- **Solution:** Dynamically detect device risk factors and capture the underlying device.
- **Key benefits**
 - Accurately detects device risk factors
 - Allows or restricts sensitive mobile application 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 Platform projects

More Information

- [Website](#)
- [Whitepaper](#)
- [Trusteer Mobile SDK](#)
- [Trusteer Mobile App](#)

IBM Security Access Manager for Mobile

Safeguard mobile, cloud and social interactions



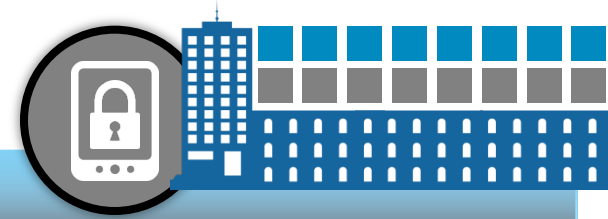
- **Challenge:** Provide secure access to mobile apps and reduce the risks of user access and transactions from the mobile devices.
- **Solution:** Deliver mobile single sign-on and session management, enforce context-aware access and improve identity assurance.
- **Key benefits**
 - Protects the enterprise from high risk mobile devices by integrating with **Trusteer** Mobile SDK
 - Built-in support to seamlessly authenticate and authorize users of **MobileFirst Platform** 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
 - 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](#)

IBM DataPower

A secure gateway protecting and optimizing mobile interactions



- **Challenge:** Provide secure access to mobile apps and reduce the risks of user access and transactions from the mobile devices.
- **Solution:** Use DataPower to connect Mobile Applications with Enterprise Apps & Services: IMS, CICS, DB2, etc.
- **Key benefits**
 - Highest level of protection for back-end service calls
 - Pre-processing of messages to reduce load on back end
 - Resiliency, scalability, and acceleration at the edge
 - Configuration, not coding
 - Hardened security for mobile access
 - Rapid deployment and change management

More Information

- [Website](#)
- [Redbook](#)
- [Datasheet](#)
- [Demo Video](#)

Secure the Mobile Enterprise Run Time Environment

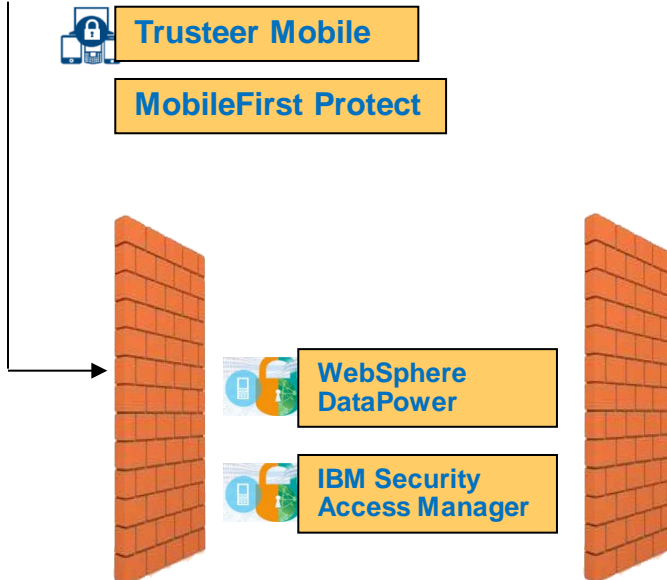


6



Trusteer Mobile

MobileFirst Protect



6. Protect the applications against hacking attacks & malware
7. Monitor databases in real time for vulnerabilities
8. Monitor operating system in real time for vulnerabilities



IBM Security AppScan



IBM InfoSphere Guardium

7

MobileFirst Platform

SOAP/https

JSON/https

Linux

z/VM

Hardware

Cryptographic cards

CPACF

z/OS Connect

CICS
DB2
IMS
WAS
Batch

z/OS

z/OS

RACF

PKI Services

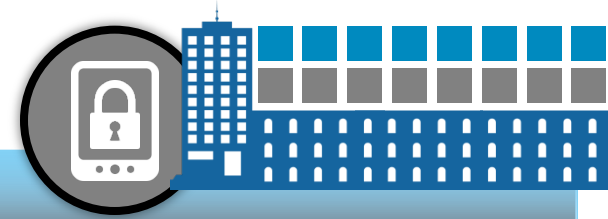
IDID

8



IBM Security zSecure

Arxan Application Protection for IBM Solutions



- **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**

- “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 changes with binary-based guard injection engine
- Broadest multi-platform support to enable standardization
- No impact to user experience, negligible performance impact
- Validated with MobileFirst Platform and AppScan, tested with Trusteer

More Information

- [Website](#)
- [Whitepaper](#)
- [Datasheet](#)
- [Webinar](#)

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

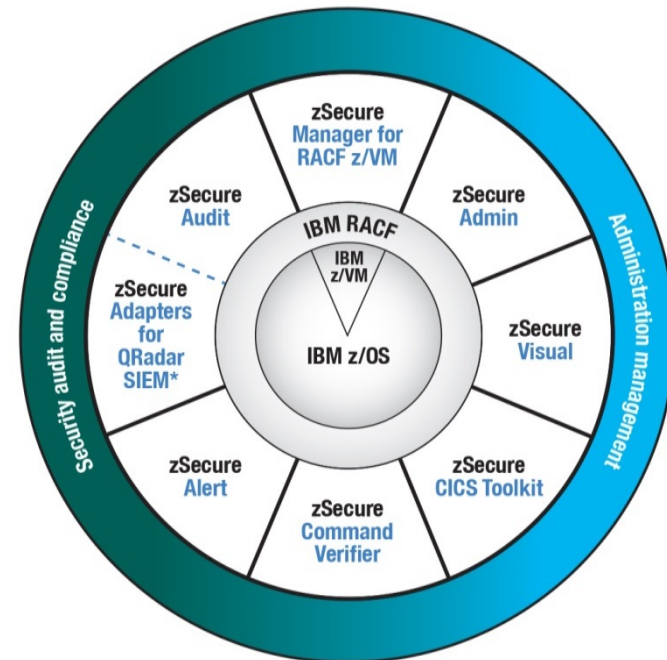
Solution

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

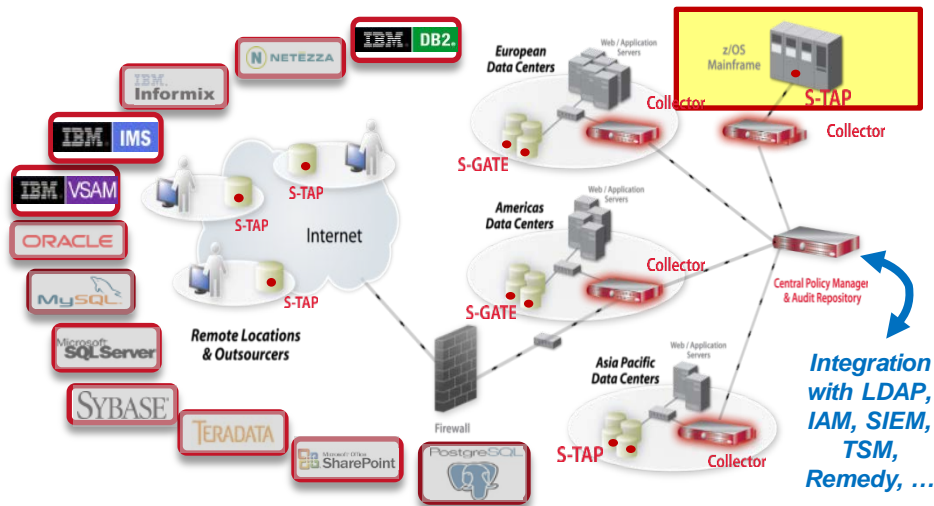
IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

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.

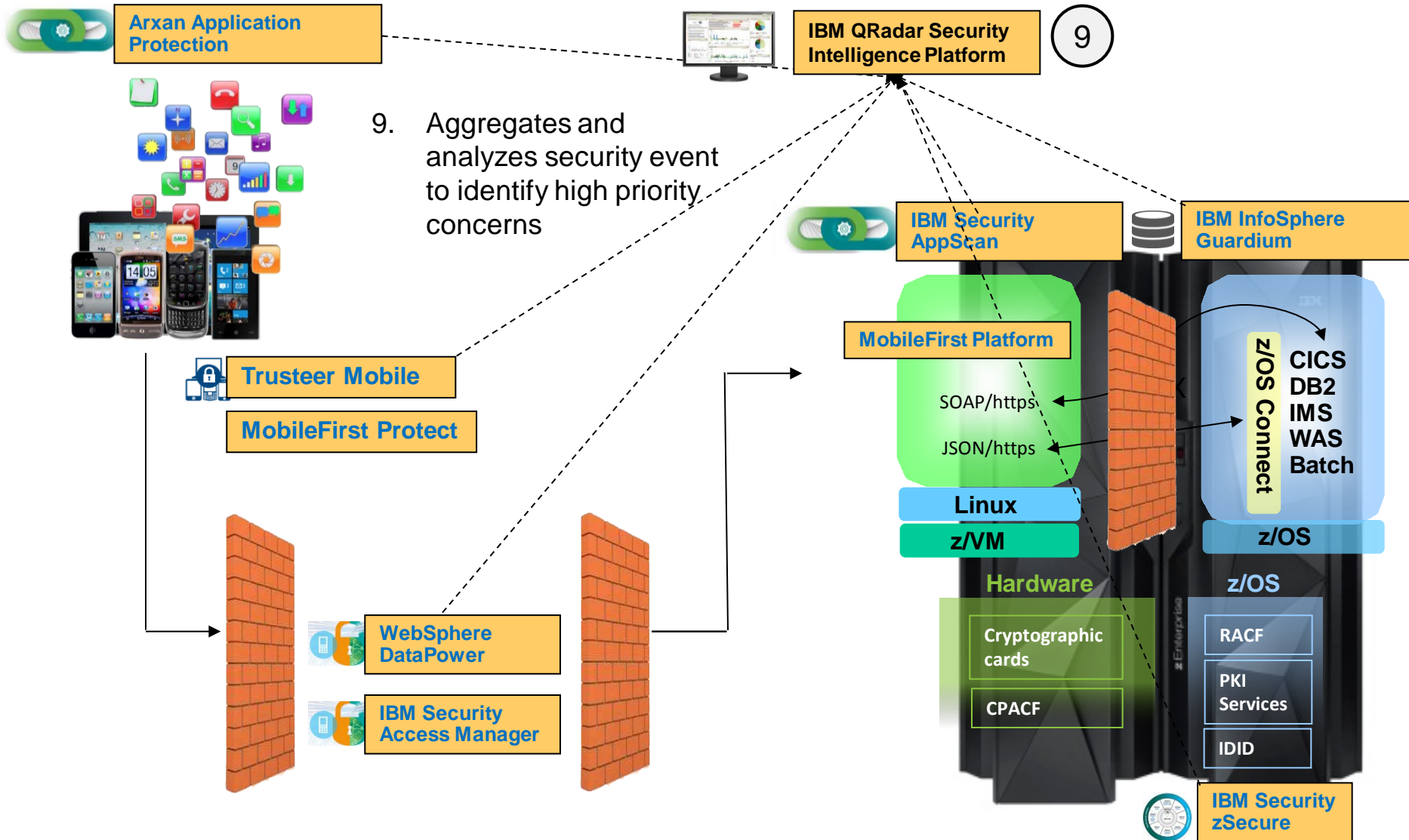
Solution

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

Key Benefits

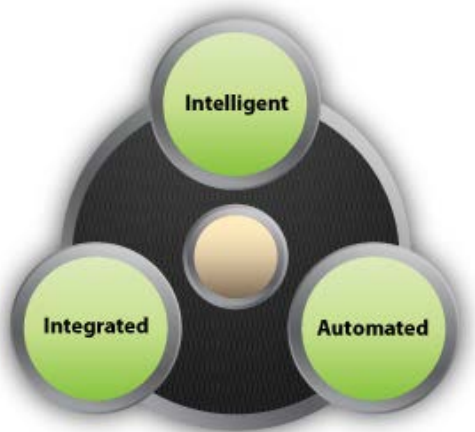
- Continuous, policy-based, real-time monitoring of all database activities, including actions by privileged users
- Database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities
- Data protection compliance automation

Real-time security intelligence for the Mobile Enterprise



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

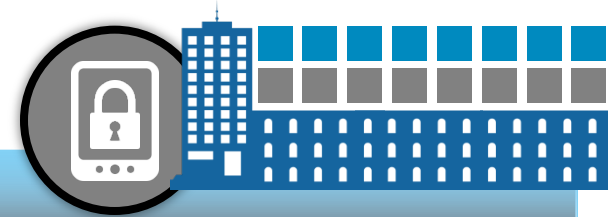
Solution

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
- Perform scheduled and real time asset vulnerability scanning and prioritization to stay ahead of possible attacks

Large retail bank in Europe strengthens security 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.

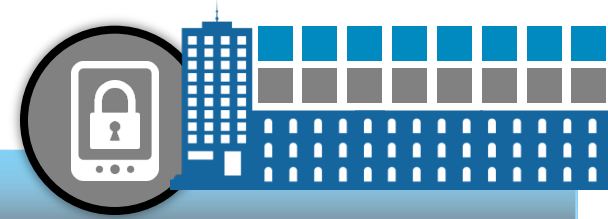
Solution: Trusteer Mobile SDK helped protect the organizations' existing mobile banking application by adding device risk analysis and providing a persistent mobile device ID.

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

Large retail company in UK builds secure access with MobileFirst Platform



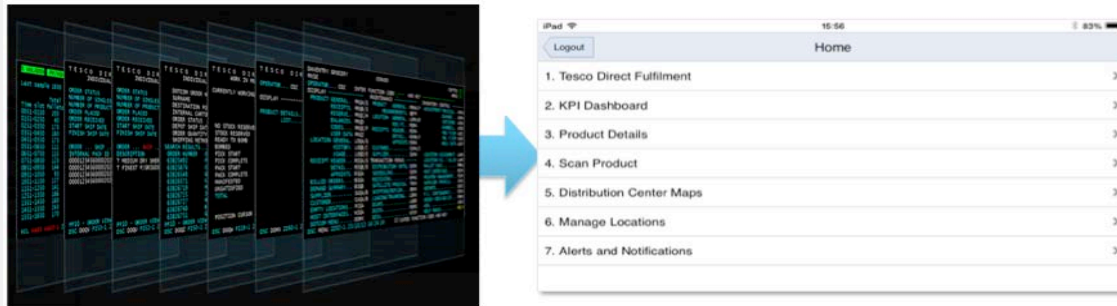
Business problem: A retail company in the UK sought to implement a easy to use and secure user interface to their existing warehouse fulfillment system.

Solution: MobileFirst Platform and zLinux provided a proven infrastructure to implement a secure & usable interface to their existing CICS based fulfillment system.

Benefits:

- Simplifies access to mission critical application, thus allowing greater productivity from a wider range of staff
- Retains secure access of existing CICS application

Featured Security Offering: MobileFirst Platform & Linux on System z



Travel expense management uses AppScan to scan their mobile applications



Business problem: A travel expense management company in the US needed to assure their customers that their mobile applications were secure and were protecting their data.

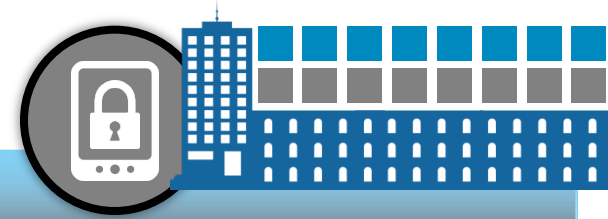
Solution: IBM Security AppScan provided a proven solution for analyzing their applications during development, identify security vulnerabilities, and remediating those vulnerabilities.

Benefits:

- Higher quality applications for their customers
- Reduced costs to identify & remediate vulnerabilities
- Overall lower costs for application development

Featured Security Offering: AppScan Source

IBM security experts help protect the mobile enterprise



Customer Results:

- Uncovered vulnerabilities
- Reduced development cost
- Improved brand image
- Protected intellectual property

Business problem: An industry leader is providing a wide range of smart devices to the world. The solution team was looking for a trusted partner to assist them with securing their line of products.

Solution: IBM used both source code analysis and a hacker's approach to assess the security of the smart device and its modules. IBM experts developed customized tools, a test methodology adapted to suit the client's needs and defined a threat model, re-usable on all their smart devices.

Benefits:

- increase integrity and availability of their devices,
- address stability issues, and most importantly,
- prevent hackers from gaining root access to the devices

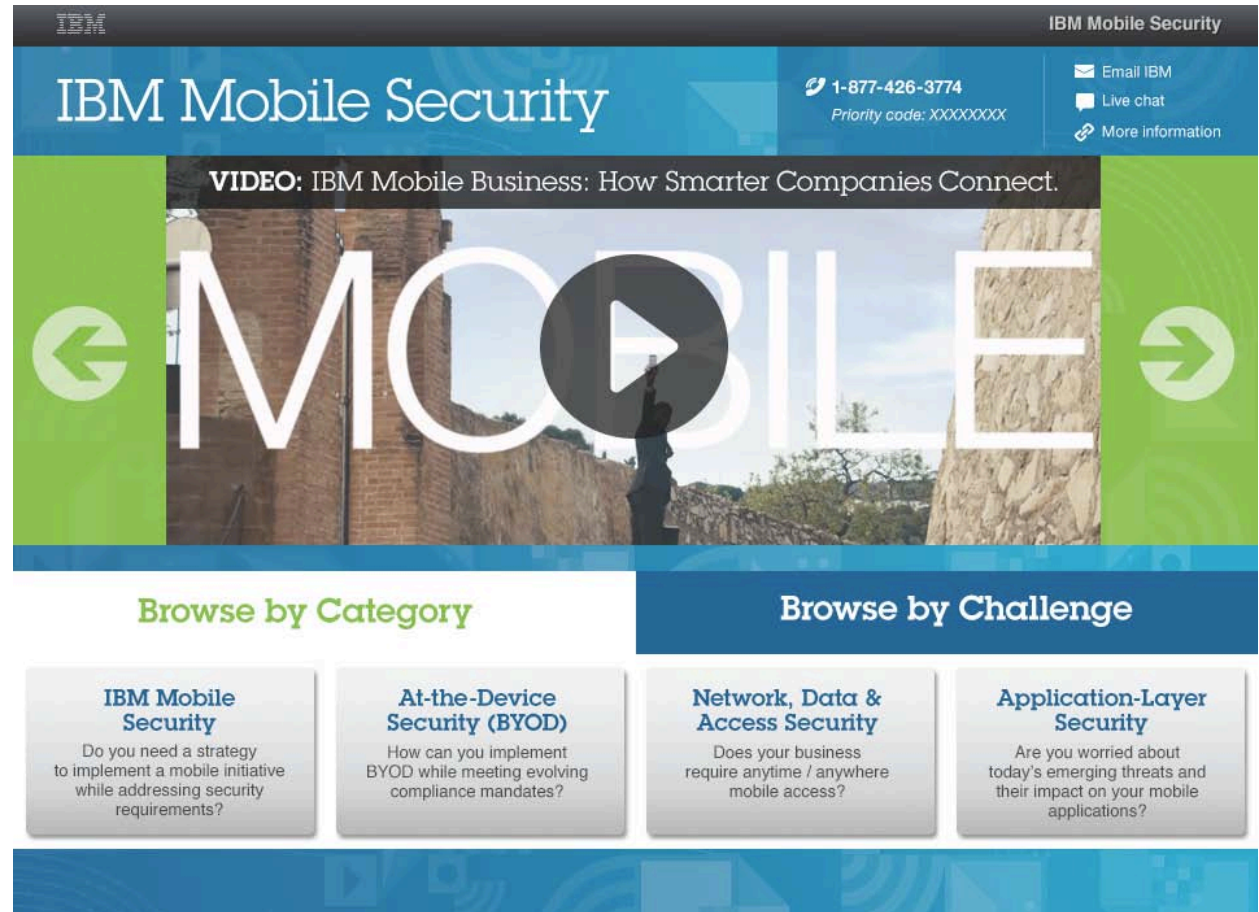
Featured Security Offering: IBM Security Services – Smart and Embedded Device Security

Looking for more information to Secure your Mobile Enterprise?

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.



IBM Mobile Security

1-877-426-3774
Priority code: XXXXXXXX

Email IBM
Live chat
More information

VIDEO: IBM Mobile Business: How Smarter Companies Connect.

MOBILE

Browse by Category

Browse by Challenge

IBM Mobile Security
Do you need a strategy to implement a mobile initiative while addressing security requirements?

At-the-Device Security (BYOD)
How can you implement BYOD while meeting evolving compliance mandates?

Network, Data & Access Security
Does your business require anytime / anywhere mobile access?

Application-Layer Security
Are you worried about today's emerging threats and their impact on your mobile applications?

Buyers Journey Assets – Mobile Security Solutions

Learn

- Video: [Delivering confidence to seize the mobile opportunity](#)
- Video: [Mobile Security - Confidently enable productivity, business agility and a rich experience](#)
- Whitepaper: [Getting a better grip on mobile devices](#)
- Video: [Enabling the Mobile Enterprise](#)
- Whitepaper: [When millions need access: Identity management in an interconnected world](#)
- Whitepaper: [Ensuring application security in mobile device environments](#)

Compare

- Datasheet: [IBM Endpoint Manager for Mobile Devices](#)
- Solution Brief: [Extend user-access protection to cloud and mobile environments](#)
- Demo: [Securing Mobile Applications using IBM Security AppScan Source](#)
- Datasheet: [IBM Security AppScan Source](#)
- Datasheet: [IBM Security Access Manager for Mobile](#)

Solve

- Solution Brief: [Securing the mobile enterprise with IBM security solutions](#)
- Whitepaper: [Accelerating the deployment of a secure mobile enterprise](#)
- Gated Whitepaper: [Manage user identities and access in the cloud](#)
- Video: IBM [Application Security Solutions: Build Security into Your Web and Mobile Applications](#)
- Whitepaper : [Beyond Password: Protect the Mobile Enterprise with Smarter Security Solutions](#)

Purchase

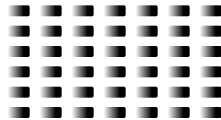
- Redbook: [Securely Adopting Mobile Technology Innovations for Your Enterprise Using IBM Security Solutions](#)

Starting a mobile conversation

- **How are you responding to mobile security challenges, such as employees who want to use their personal mobile devices for work applications?**
(Overview on IBM Mobile Security Framework)
- **Are you worried about the increasing volume and complexity of today's emerging security threats and its impact on your mobile applications?**
(IBM Security AppScan, Arxan Application Protection, Trusteer SDK, MobileFirst Platform)
- **Does your business require anytime/anywhere mobile access?** Organizations that require centralized web access management and SSO for mobile users often will need to demonstrate compliance.
(IBM can help by delivering user security that adapts to the requirements *IBM Security Access Manager (ISAM) for Mobile*)
- **Are you concerned about allowing Bring-your-own-device into your enterprise and still maintain control over enrolling and configuring devices to comply with your mobile policy? Do you have the ability to remotely locate, lock and wipe lost or stolen devices**
(MobileFirst Protect)

Call to Action

- Engage your Security Sellers
 - WW System z Security Sales Leader: [Andy Nietupski](#)
 - NA IOT System z Security Sales Leader: [Bob LaCapria](#)
 - Europe IOT System z Security Sales Leader : [Roberto Tomassi](#)
 - Former GMU System z Security Sales Leader: [Francesca Ferretti](#)
- *Exploit the Securing the Mobilized Mainframe sales play ([SSW](#)) ([PartnerWorld](#))*
- *Exploit the AppScan for System z sales play ([SSW](#)) ([PartnerWorld](#))*
- *Get the MobileFirst Platform for System z pipeline and cross-sell Security into existing opportunities*
 - WW Application Security Security Sales Leader: [Tim Bedard](#)
 - NA IOT Application Security Sales Leader: [Jason Bellomy](#)
 - Europe IOT Application Security Sales Leader : [Charles Tostain](#)
 - Former GMU Application Security Sales Leader: [Kat Ang](#)
- *Share the [System z in Mobile World](#) Redbook with your customers*



THE END

