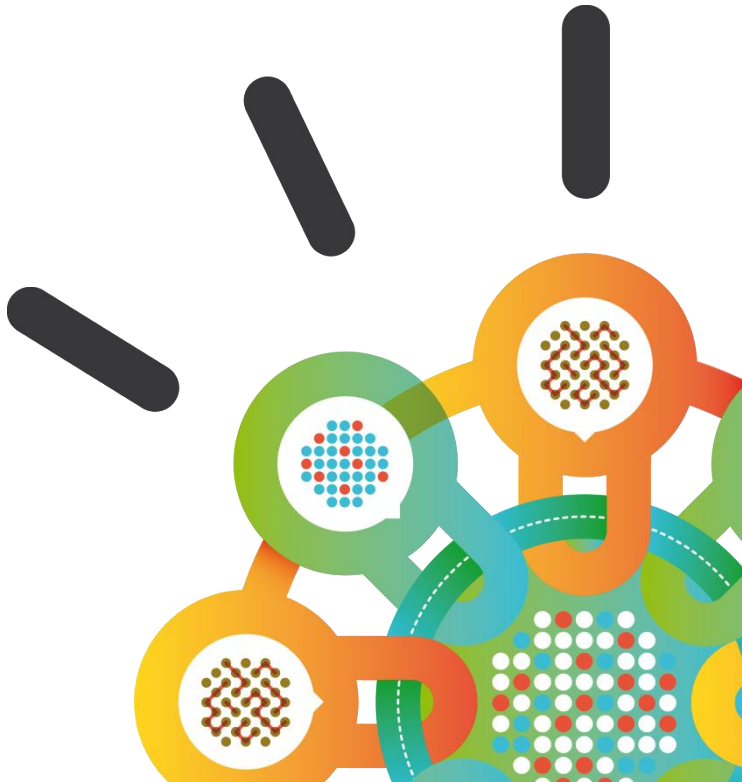
Security Intelligence.
Think Integrated.

Putting the Brakes on Mobile Insecurity

Tom Mulvehill
Mobile Security Strategy
IBM Security

May 19, 2015



Agenda

- Why Mobile Security Should be a Strategic Imperative
- IBM Mobile Security Framework
- IBM Mobile Security Solutions Address Real Problems
- Summary

Why Mobile Security Should be a Strategic Imperative

Enterprise Mobile Trends

The number of smartphone users worldwide will surpass 2 billion in 2016[1]

eMarketer

Mobile downloads will increase to 268 billion by 2017[2]

Gartner

"Enterprise mobility will continue to be one of the hottest topics in IT, and **high on the list of priorities** for all CIOs."

Ovum

OVUM

"IT organizations will dedicate at least **25% of their software budget to mobile application** development, deployment, and management by 2017."

IDC

IDC Analyze the Future

As Mobile Grows, So Do Security Threats

387 new malware threats every minute, or more than 6 every second -- half-billion samples by Q3 2015[3]

McAfee

Mobile devices & apps under attack 97% top Android, 87% top iOS mobile apps have been hacked[4]

ARXAN Protecting the App Economy

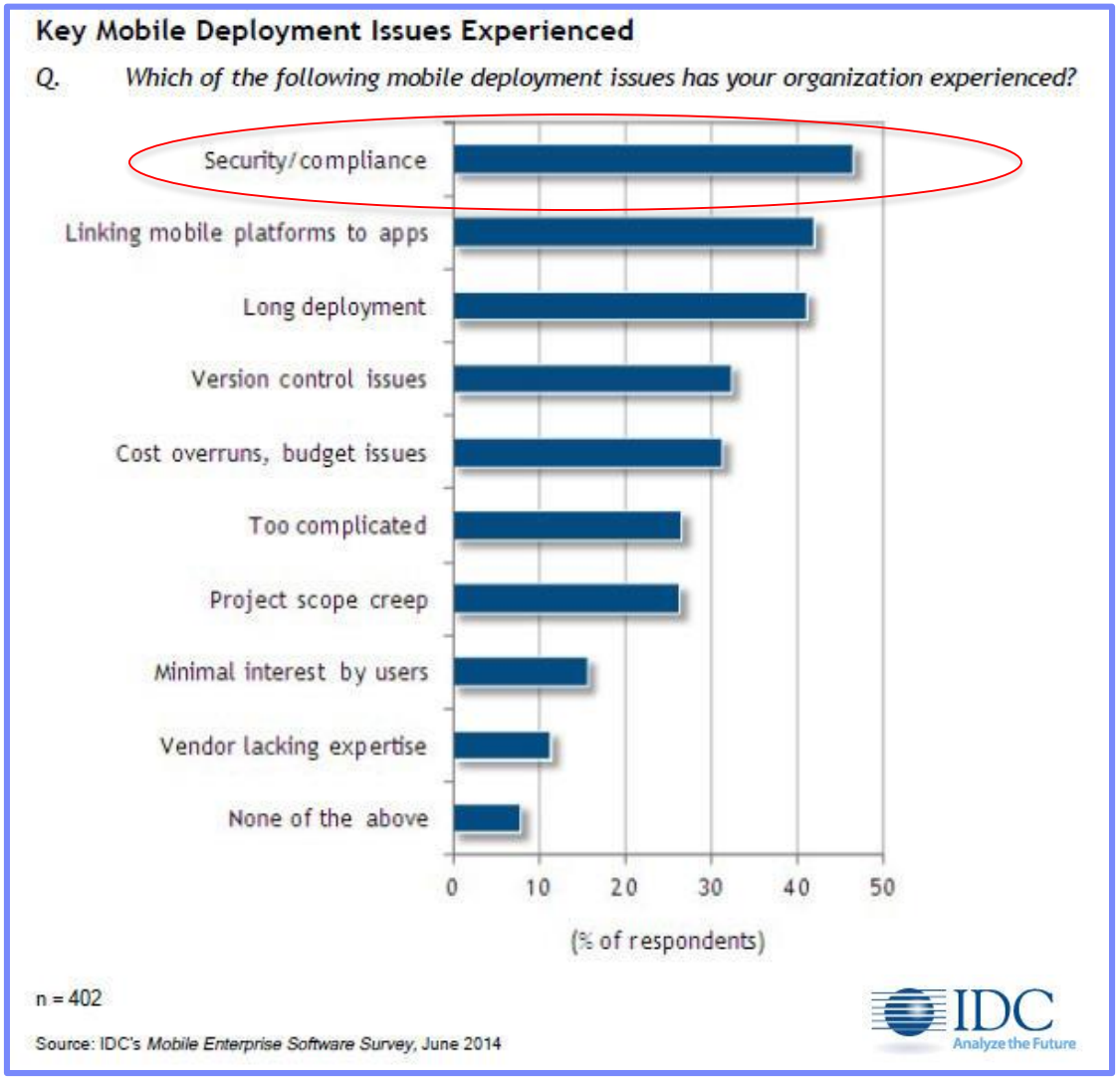
"With the growing penetration of mobile devices in the enterprise, security testing and **protection of mobile applications and data become mandatory**" *Gartner*

Gartner

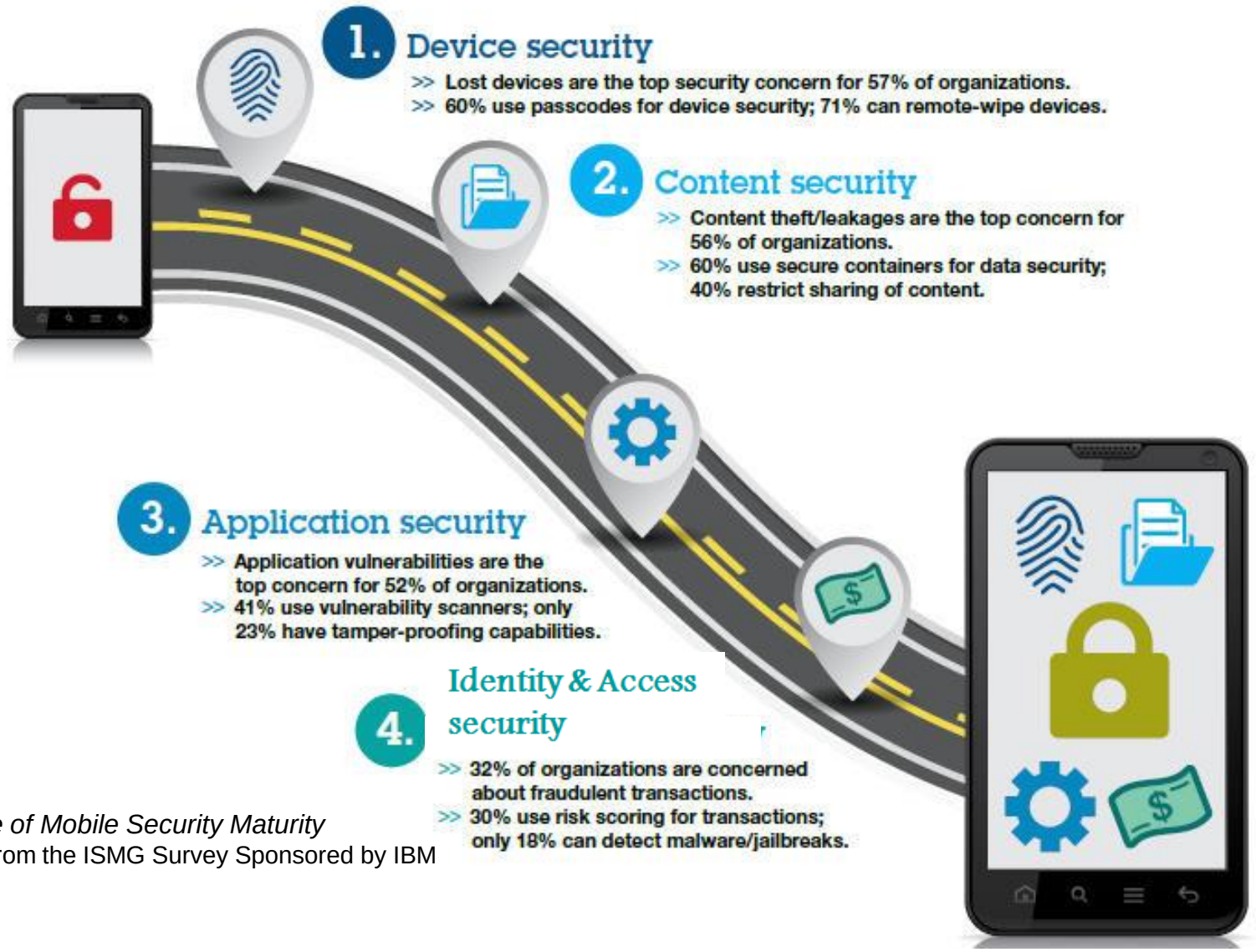
"Enterprise mobility … new systems of engagement. These new systems help firms empower their customers, partners, and employees with **context-aware apps** and smart products." *Forrester*

FORRESTER®

Top Issue Experienced in Mobile Deployments?



Roadmap to Effective Mobile Security



The State of Mobile Security Maturity
Findings from the ISMG Survey Sponsored by IBM

Link to report

Mobile Apps Continue to Explode in the Enterprise

In 2014, 60% of large companies used **3 or fewer mobile apps**[1]

The number of custom mobile apps **will double** compared to 2014[2]

The number of enterprise mobile apps is **expected to quadruple**[3]

85% of companies have a **mobile backlog of up to 20 apps**[4]

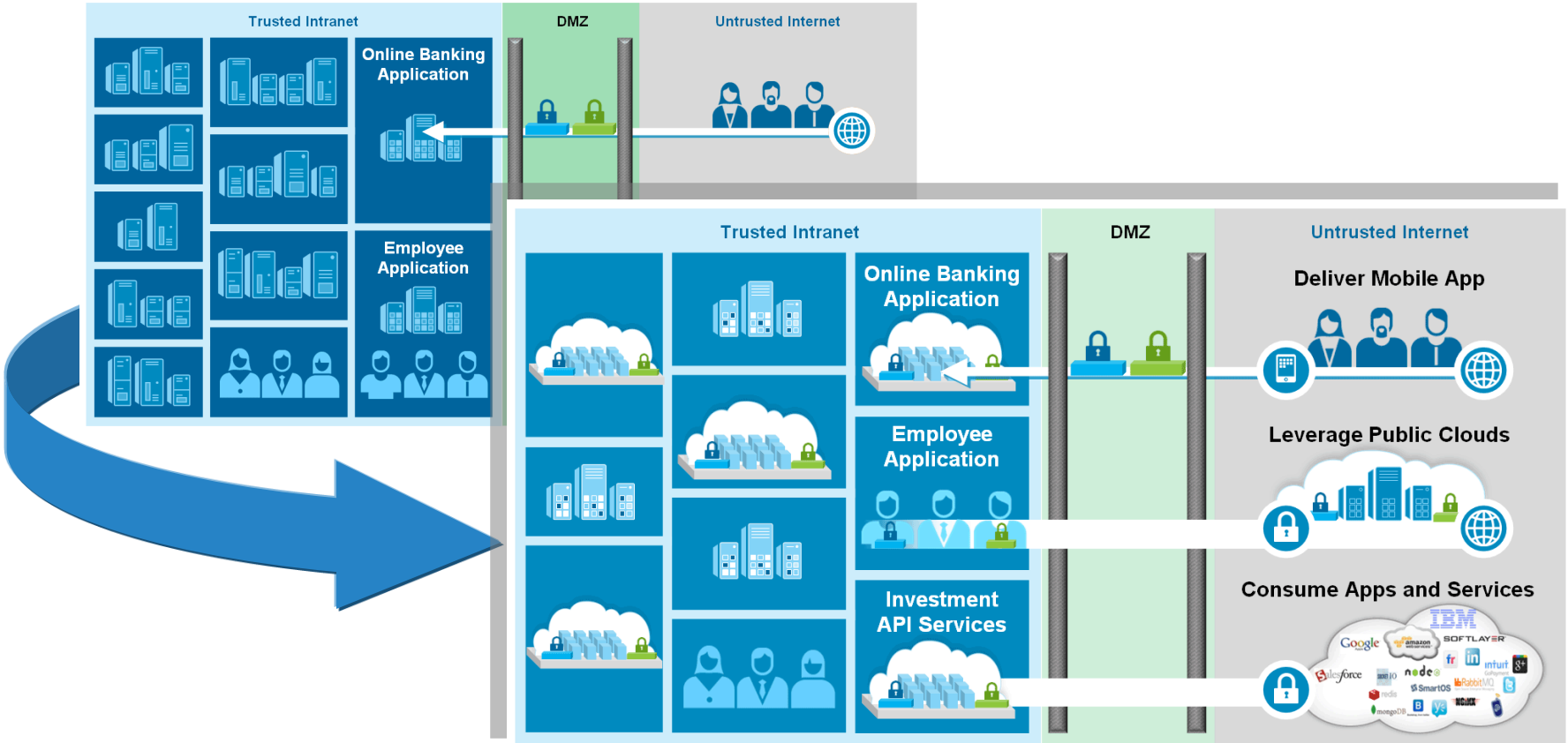
Mobile app development will out number PC **projects 4:1**[5]

More than half of b2e apps will be **created by the enterprise**[6]

2014 → 2016 → 2018

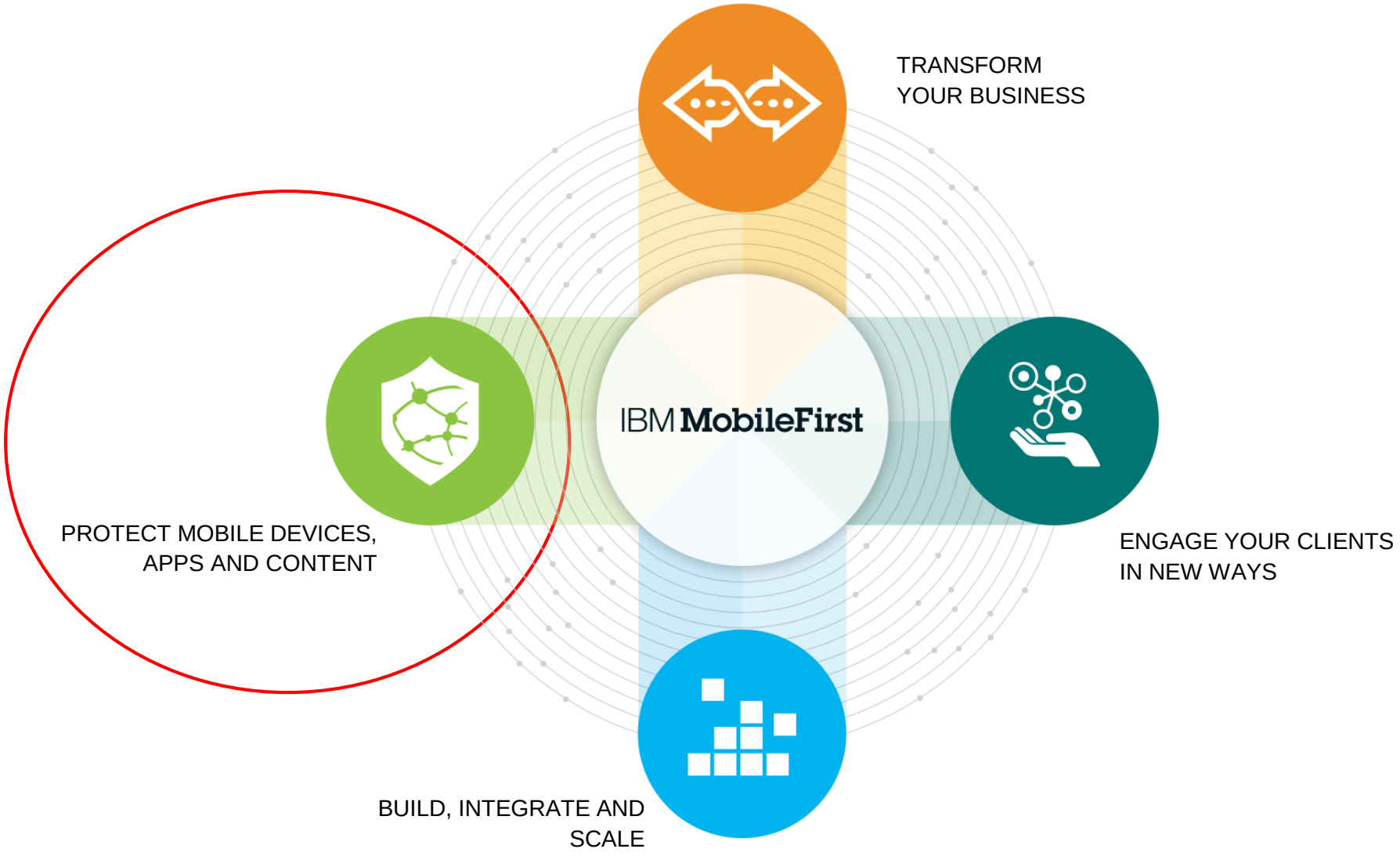
Mobile Changes the Way We View Perimeter

Security is no longer controlled and enforced through the network perimeter



IBM Mobile Security Framework

IBM MobileFirst



IBM Mobile Security Framework

Protect Devices	Secure Content & Collaboration	Safeguard Applications & Data	Manage Access & Fraud
• Manage multi-OS BYOD environment • Mitigate risks of lost & compromised devices	• Separate enterprise and personal data • Enforce compliance with security policies	• Distribute & control enterprise apps • Build and secure apps & protect them "in the wild"	• Provide secure web, mobile, API access control • Meet ease-of-use expectation

Extend Security Intelligence

- Extend security information & event management (SIEM) to mobile platform
- Incorporate mobile log management, anomaly detection, configuration & vulnerability mgmt

Executing a Strategy with IBM Mobile Security

Comprehensive Approach ***Integrated Solutions*** ***Scalable Security***

IBM MobileFirst Protect (MaaS360)

IBM MobileFirst Platform

Arxan Application Protection for IBM Solutions

IBM Security Trusteer

IBM Security AppScan

IBM Security Access Manager

IBM DataPower Gateway

IBM Mobile Security Services

IBM QRadar Security Intelligence Platform

IBM is the ONLY Leader in **8** Gartner Mobile Magic Quadrants

Enterprise Mobility Management Suites
June 2014

Client Management Tools
May 2014

Managed Mobility Services
July 2014

Enterprise Content Management
September 2014

Identity, Governance, Access
August 2014

Mobile Application Development Platforms
August 2014

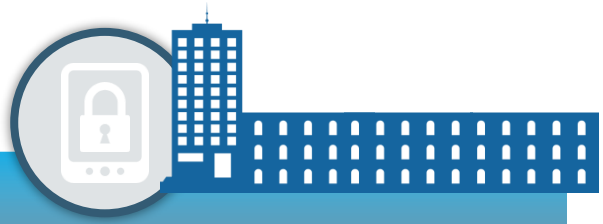
Application Security Testing
July 2014

Security Information and Event Management
June 2014

IBM Mobile Security Solutions Address Real Problems

MobileFirst Protect (formerly MaaS360) EMM

Deploy, manage and secure devices, apps and content in the enterprise

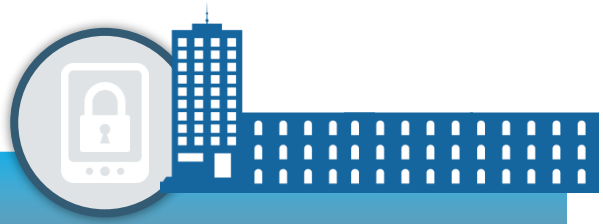


- **Challenge:** Businesses need flexible and efficient ways to promote their mobile initiatives while protecting data and privacy

- **Key Questions To Consider:**
  - What happens if an employees mobile device is lost or stolen?
  - How do you prevent your employees from using unauthorized mobile applications?
  - How do you define and enforce mobile security polices?

MobileFirst Protect (formerly MaaS360) EMM

Deploy, manage and secure devices, apps and content in the enterprise



- **Challenge:** Businesses need flexible and efficient ways to promote their mobile initiatives while prote

- **Key Question**
  - What happer ce is lost or stolen?
  - How do you using unauthorized
  - How do you define and enforce mobile security polices?

In a BYOD environment why are you concerned if an employee's mobile device is lost or stolen?

You Can't Manage What You Don't Measure

MobileFirst Protect

1,175+

different security policy settings and controls

IBM Deploys MobileFirst Protect

Solutions must scale…

… must be ease to deploy

70,000+ Users migrated in one month

16,000+ Users registered within 24 hours

48,000+ Users registered in 15 days

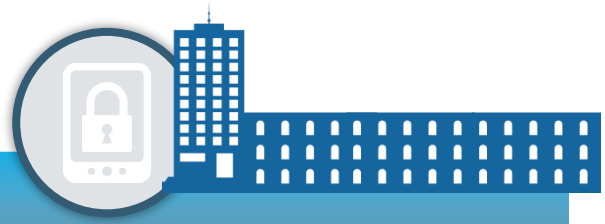
200+ Devices enrolled per minute*

*at high point

<500 Help Desk calls – less than ½ of 1%

IBM Security Trusteer Mobile Solutions

Detect & Action Device Risk

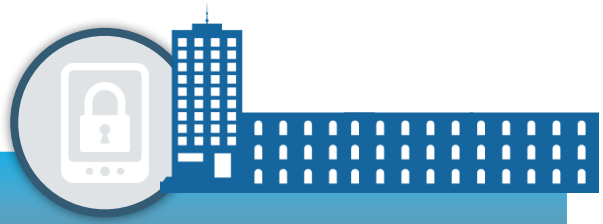


- **Challenge:** Compromised or vulnerable devices (jailbroken/rooted) AND malicious mobile applications create security risk for users and enterprises

- **Key Questions To Consider:**
  - How do you determine the risk posed by employee owned devices to enterprise data and systems?
  - How do you determine if a device has been compromised (jailbroken/rooted/malware)?
  - If a device has been compromised how do you mitigate the risk to enterprise apps, content and backend systems?

IBM Security Trusteer Mobile Solutions

Detect & Action Device Risk



- **Challenge:** Compro ed) AND malicious mobile applications c

- **Key Question**
  - How do you nployee owned devices to er
  - How do you compromised (jailbroken/ro
  - If a device has been compromised how do you mitigate the risk to enterprise apps, content and backend systems?

Do you understand the risk to your apps & data on jailbroken devices?

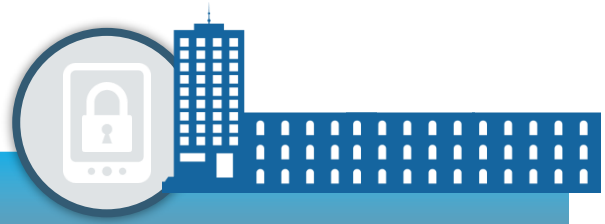
Do you know if the employee device has been compromised?

MobileFirst Protect Mobile Threat Management

- Jailbreak / Root detection, malware detection
- Provides device risk awareness within Mobile Apps, Mobile Device Management, Mobile Identity & Access
- Enables enforcement of app functionality, content wipe/delivery and enterprise access based on device risk
- Prevents deployment of containers into jailbroken or rooted device

IBM Security AppScan & Arxan Application Protection

Secure and Protect mobile applications

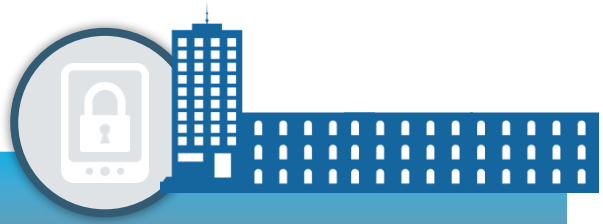


- **Challenge:** Mobile app development fast paced; need automated tools to identify security risk and protect “applications in the wild”

- **Key Questions To Consider:**
  - How do develop secure mobile applications to ensure they do not leak enterprise or sensitive user data?
  - How do you keep pace with the constant mobile updates?
  - How do you protect your mobile apps from reverse engineering and repackaging with malware?

IBM Security AppScan & Arxan Application Protection

Secure and Protect mobile applications



- **Challenge:** Mobile app development fast paced; need automated tools to identify security risk and protect "applications in the wild"

- **Key Questions**
  - How do devel… to ensure they do not leak er…?
  - How do you k…obile updates?
  - How do you p…reverse engineering a…are?

How do you develop secure mobile applications?

How do you protect your mobile app IP and safeguard apps from malware?

Mobile Application Security Risk

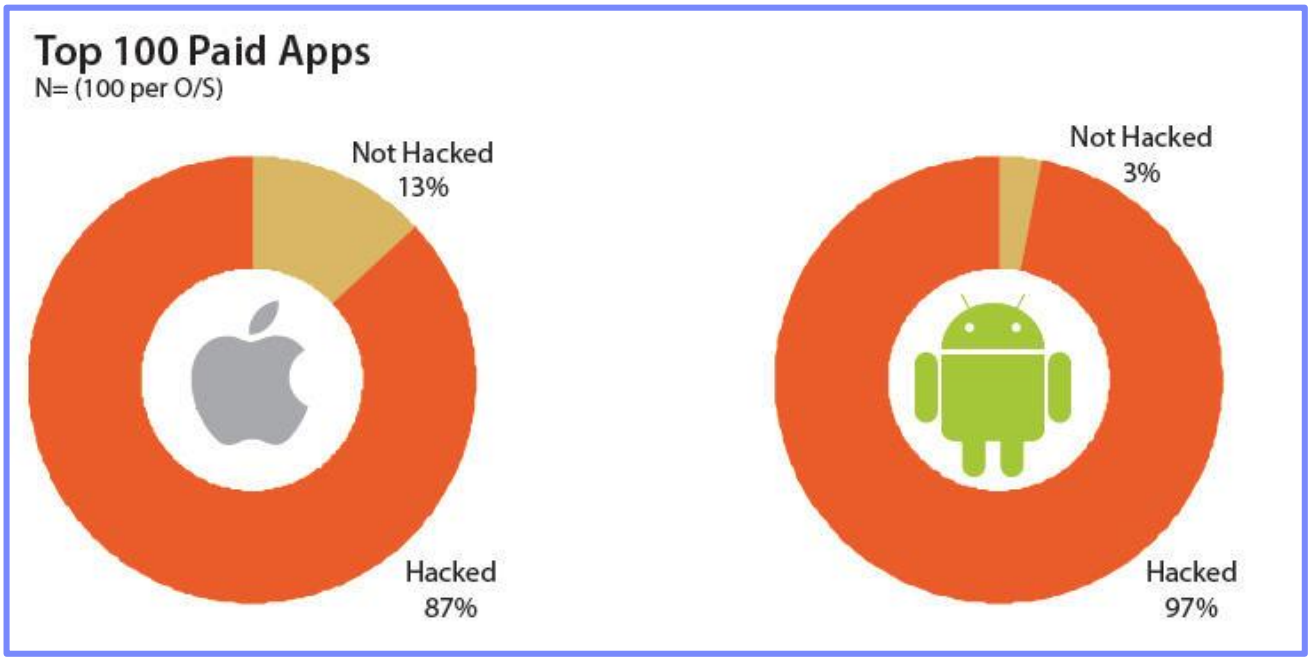
User

- Threat from Malware
  - Trojans and Spyware
- Phishing
- Fake Marketplace
  - Malware added to app
- Unauthorized Use of:
  - Contact DB
  - Email
  - SMS (text messages)
  - Phone (placing calls)
  - GPS (public location)
  - Data on device

Enterprise

- Data leakage
  - Attack from malware
  - Account info. on mobile device
- Cracking mobile apps
  - Easy access to applications
  - Reverse engineering
- Little to no App control
  - BYOD
  - Consumer devices

Reverse Engineering & IP Theft Risk



Source: State of Security in the App Economy
- "Apps Under Attack" (Dec 2014)

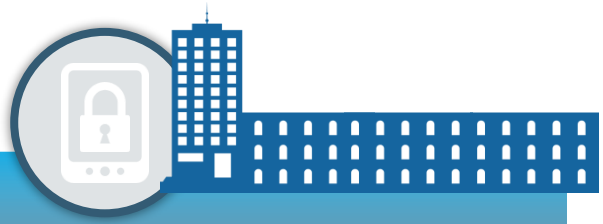
- 97% of top paid Android apps have been hacked
- 87% of top paid iOS apps have been hacked
- 80% of the most popular free Android apps have been hacked
- 75% of the most popular free iOS apps have been hacked

OWASP Mobile Top 10 Risks (RC 2014 V1)

https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

IBM Security Access Manager

Improve security & user experience with context-aware mobile access control

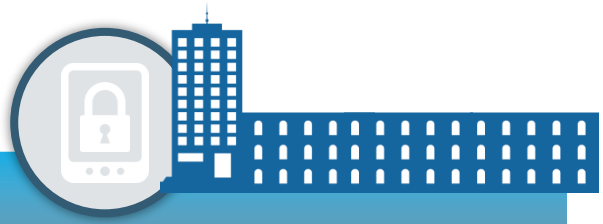


- **Challenge:** Providing secure access to mobile apps and APIs in order to prevent malicious, fraudulent, or unauthorized activities in both B2E and B2C scenarios

- **Key Questions To Consider:**
  - How do you determine if access to applications from a mobile device is high risk?
  - If you determine there is risk, how do you adapt your authentication and access policies to strengthen security?
  - What do you say to users who complain about entering multiple passwords to access enterprise systems & data?

IBM Security Access Manager

Improve security & user experience with context-aware mobile access control



- **Challenge:** Providing secure access to mobile apps and APIs in order to prevent malicious, fraudulent, c… …l B2C scenarios

How are you adapting your authentication & access policies to strengthen security on Mobile?

- **Key Questions**
  - How do you d… …ations from a mobile device…
  - If you determi… …adapt your authentication… …trengthen security?
  - What do you say to users who complain about entering multiple passwords to access enterprise systems & data?

What is Context?

Endpoints:

There are various unique attributes (device fingerprint).

Screen depth/resolution, Fonts, OS, Browser, Browser plug-in, device model & UUID

Identity:

Groups, roles, credential attributes, organization

Environment:

Geographic location, network, local time . . . etc

Resource / Action:

The application being requested and what is being done.

Behavior:

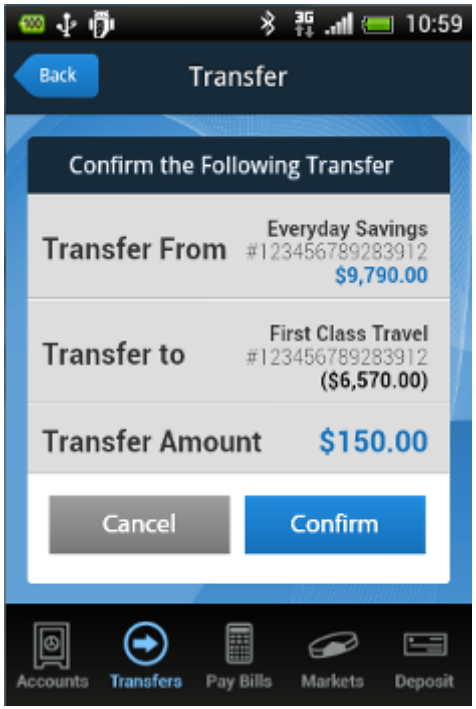
Analytics of user historical and current resource usage.

User activity monitoring, specific business activity monitoring

Authentication Changes Based on Context

- Transactions performed near users home – normal
- Try to transfer funds in another state or another country – requires an OTP for strong authentication

User attempts transaction from unexpected location



Strong authentication challenge

Transaction completes

Summary

Summary

- **Enterprise Mobility Management is needed & necessary**
- **MDM is a good place to start but additional security required**
- **Need to account for device risk**
- **Must build secure mobile apps & must secure apps "in the wild"**
- **Identity & Access security must be adaptive – contextually aware**
- **Think of mobile security more holistically**

Comprehensive ***Integrated*** ***Scalable***

  - Broader than MDM
  - Think… Device, Content, Application, & Access
  - More than a collection of point products
  - Must scale to address enterprise requirements

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security