IBM Security
Intelligence. Integration. Expertise.

IBM

IBM Mobile Security

Putting the Brakes on Mobile Insecurity

Jason Hardy
Worldwide Market Segment Manager, Mobile Security
IBM Security

October 22, 2015

Enterprise mobile trends

by 2016

The number of smartphone users worldwide will surpass

2 billion

eMarketer

by 2017

Mobile downloads will increase to

268 billion

Gartner

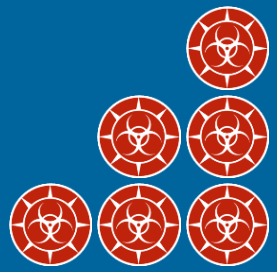
"Enterprise mobility will continue to be one of the hottest topics in IT, and high on the list of priorities for all CIOs."

Ovum

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

IDC

As mobile grows, so do security threats



387 new threats

every minute or more
than six every second

McAfee

Top mobile devices and apps hacked

97% Android

87% iOS

Arxan

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

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

What concerns does this create for the enterprise?

57% say a lost or stolen device is top concern

60% use passcodes for device security

50% are content and data leakage are their top security concern

60% use secure containers for data security

52% worry about application vulnerabilities

Only 23% have tamper-proofing capabilities

32% are concerned about fraudulent transactions

Only 18% can detect malware / jailbreaks

Source: 2014 Information Security Media Group Survey, “The State of Mobile Security Maturity”

IBM Mobile Security Framework

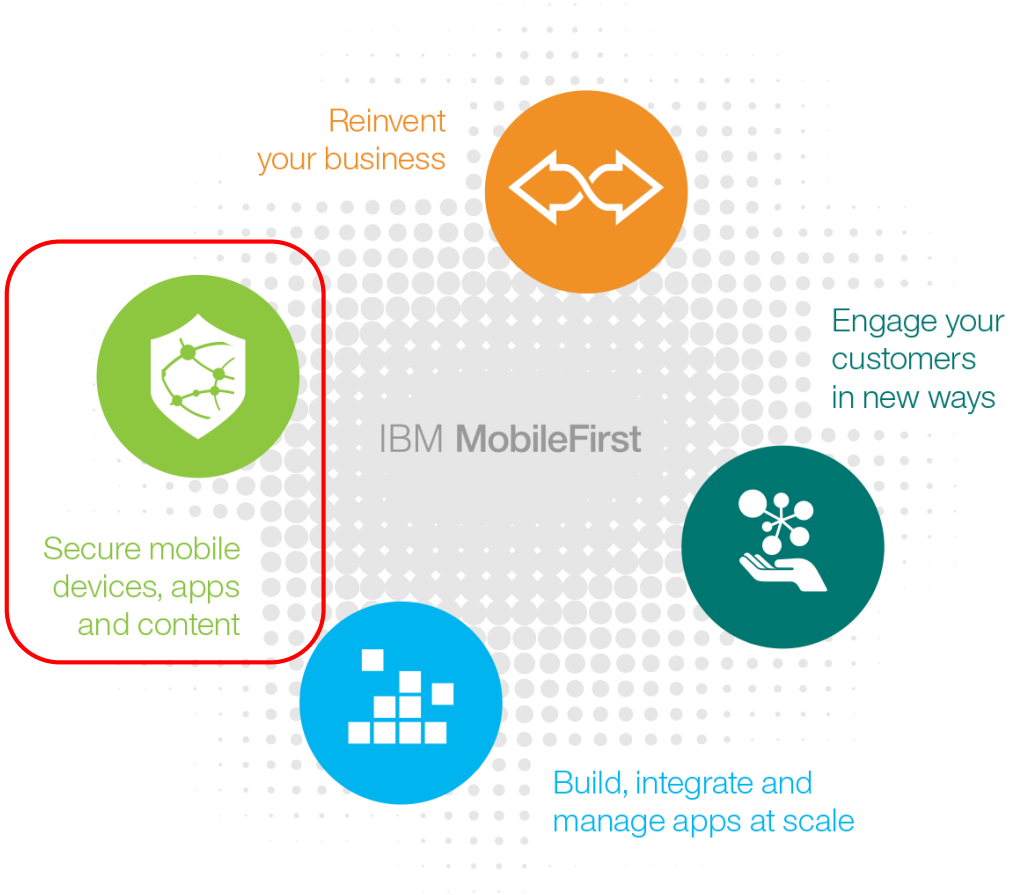
Protect Devices	Secure Content and Collaboration	Safeguard Applications and Data	Manage Access and Fraud
• Manage multi-OS BYOD environment • Mitigate risks of lost and compromised devices	• Separate enterprise and personal data • Enforce compliance with security policies	• Distribute and control enterprise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

Extend Security Intelligence

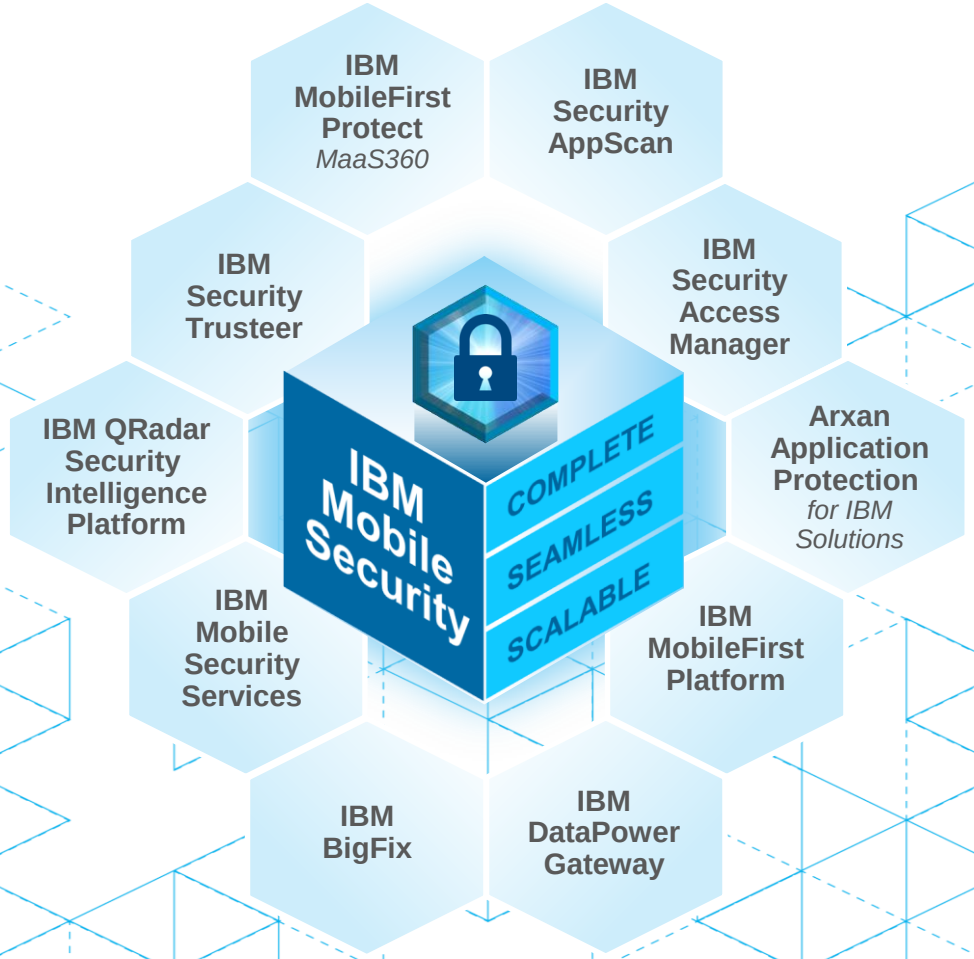
- Extend security information and event management (SIEM) to mobile platform
- Incorporate mobile log management, anomaly detection, configuration and vulnerability management

IBM MobileFirst

IBM **MobileFirst** delivers apps, infrastructure and ways to engage that are designed exclusively for mobile users, personalized with data, highly secure and convenient.



IBM Mobile Security Portfolio



Protecting devices

Every three minutes, a mobile device is wiped

Protect Devices | Secure Content and Collaboration | Safeguard Applications and Data | Manage Access and Fraud

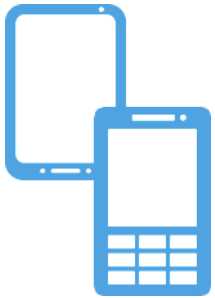
Extend Security Intelligence

Millennials and their smartphones…

87% have their smartphone at their side, day and night

78% spend over 2 hours a day using their smartphones

68% consider their smartphone to be a personal device



Source: "55 US Mobile Facts Every Marketer Needs For 2015" by Heidi Cohen, December 2014

By 2017, mobile devices will make up **87%** of Internet-enabled technology total sales

Source: Lander Blog, "Five Online Marketing Trends for 2014, April 2014

46% say their smartphone is something they couldn't live without

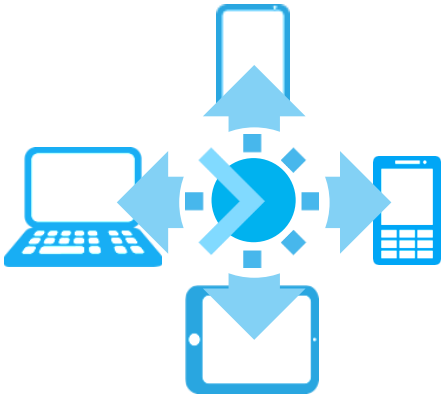
Source: "6 facts about Americans and their smartphones" by Pew Research Center, April 2015

How do you protect your devices?

- Identify and respond to any device accessing your corporate data?
- Deploy and manage a multi-OS environment with BYOD?
- Remotely provision policies and restrictions?

- Identify devices at risk pre/post deployment?
- Ensure devices accessing the network are encrypted?
- Mitigate risks of lost and compromised devices?

Deploy, manage and secure devices while mitigating the risks of lost and compromised devices



Rapidly deploy devices

Streamline the device provisioning, configuration and enrollment process for enterprise use over the air

Centrally manage devices

Embrace BYOD, corporate, and shared device with centralized policy and control from a single console

Proactively secure devices

Implement dynamic policies and compliance rules to continuously monitor devices and take automated action

Large manufacturer deploys successful BYOD program with IBM MobileFirst Protect

Client securely enabled mobility from the corporate office worker to the field service representative to better serve customers while keeping sensitive data secure.

Securing content and collaboration

Protect Devices | **Secure Content and Collaboration** | Safeguard Applications and Data | Manage Access and Fraud

Extend Security Intelligence

60% of employees access content from outside the office

"Productivity Anywhere, Anytime: Mobilize Your Business", Box

64% of decision-makers read their e-mail via mobile devices

"73 Astonishing E-Mail Marketing Statistics You Need to Know", Mark the Marketer, February 2014

59% allow employees to share or collaborate on documents if the company provides the mobile device

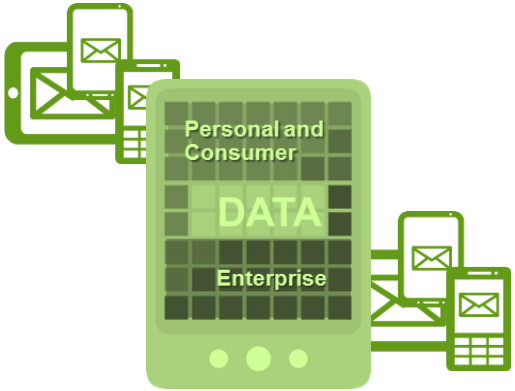
"Breaking Bad: The Risk of Unsecure File Sharing", Ponemon Institute, October 2014

How do you secure content and collaboration?

- Separate enterprise and personal data?
- Prevent data leakage?

- Provide secure access to sensitive data
- Enforce compliance with security policies?

Separate enterprise and personal data enforcing compliance with security policies



Separate work email

Contain email text and attachments to prevent data leakage, enforce authentication, copy / paste and forwarding restrictions

Enable the secure web

Provide access to intranet sites and web apps, URL filtering, and restrict cookies, downloads, copy / paste and print features

Collaborate on content

Ensure the availability of files from repositories with authentication, DLP controls, secure edit and sync, and selective wipe

A retail store chain uses IBM MobileFirst Protect for faster service to its customers

Client empowered in-store customer service representatives with shared smart devices to securely view inventory and merchandise information while on the store floor.

Safeguarding applications and data

Protect Devices | Secure Content and Collaboration | **Safeguard Applications and Data** | Manage Access and Fraud

Extend Security Intelligence

76% overall mobile app usage grew in 2014

Shopping, Productivity and Messaging Give Mobile Another Stunning Growth Year", Flurry Insights, January 2015

75% of all mobile security breaches are through apps

Gartner Press Release, May 2014

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

33% never test apps to ensure they are secure

Ponemon The State of Mobile Application Insecurity, February 2015

2.2 billion malicious attacks on computers and mobile devices were blocked during Q1 2015

Kaspersky Lab "IT Threat Evolution Report for Q1 of 2015"

How can you safeguard applications and data?

- Prevent deployment of risky mobile apps
- Protect app data at rest and in motion
- Distribute and control public and enterprise apps

- Develop secure mobile apps and assess the security of existing apps
- Secure apps against reverse engineering and runtime attacks

Build, test and secure mobile apps before distributing to end users

Test app security

Identify vulnerabilities in development and pre-deployment; isolate data leakage risks; ensure proper use of cryptography

Protect apps

Harden mobile apps to defend against reverse engineering; prevent repacking of apps; protect apps from mobile malware

Secure app data

Protect enterprise apps with authentication, tunneling, copy / paste restrictions and prevent access from compromised devices

Safely distribute apps

Deploy custom enterprise app catalogs; blacklist, whitelist and require apps; administer app volume purchase programs

A hospital uses IBM Mobile Security to build a secure and protected patient care app

Doctors, nurses, and non-hospital employees share timely patient information and test results on multiple devices to manage care while protecting sensitive information

Manage access and fraud

Protect Devices | Secure Content and Collaboration | Safeguard Applications and Data | **Manage Access and Fraud**

Extend Security Intelligence

"The CyberVor gang amassed over **4.5 billion** *records, mostly consisting of stolen credentials. To get such an impressive number of credentials, the CyberVors robbed over 420,000 web and FTP sites."*
Hold Security

$6.53 million
average cost of a U.S. data breach
2015 Cost of Data Breach Study, Ponemon Institute

95% of financial services incidents involve harvesting credentials stolen from customer devices
2015 Verizon Data Breech Report

How can you manage access and fraud?

- How do you deliver mobile security capabilities in a consistent manner to address:
  - Web services / APIs
  - Traditional web access
- How do you maintain mobility authentication ease-of-use expectations?
- Can you ensure that security features are not being sacrificed as the pace of mobile development and deployment accelerates?
- Can you prevent access from high risk or compromised mobile devices?

Prevent unauthorized access and transactions by mobile users

Consolidated enforcement point

A single point of secure access control and authentication for APIs and mobile apps enabling mobile single-sign-on

Adaptive access polices

Dynamic and adaptive access policies provide risk and context aware policy enforcement while maintaining ease-of-use expectations

Integrated device risk management

Manage risk from rooted / jailbroken devices and from mobile malware integrated into access control polices and BYOD content management

An insurance company uses IBM Security Access Manager and Mobile Threat Management to keep customer data safe

Company and independent agents access policy information in corporate offices or field, access policies dynamically change based on risk factors to ensure confidentiality and compliance

Extend security intelligence

Protect Devices | Secure Content and Collaboration | Safeguard Applications and Data | Manage Access and Fraud

Extend Security Intelligence

Attackers spend an estimated

243 days on a victim's network

before being discovered

Annual Threat Report on Advanced Targeted Attacks, Mandiant

Annual U.S. cost of a cyber-crime is

$11.56 million

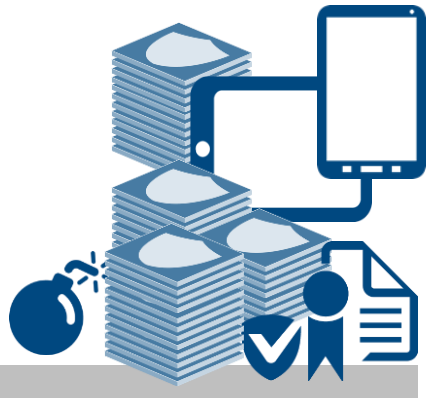
per organization

Cyber-Crime Costs Continue to Rise: Study, eWeek

63% of victims were made aware of breaches by an external organization

Annual Threat Report on Advanced Targeted Attacks, Mandiant

How can you extend security intelligence?

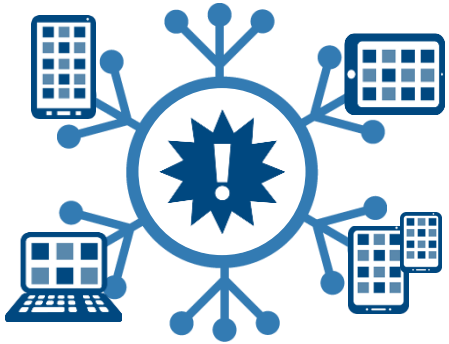


- Increasingly sophisticated mobile attack methods
- BYOD resulting in disappearing perimeters
- Accelerating mobile security breaches

- Infrastructure changing to support mobile
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

- Struggling security teams
- Mobile providing additional data sources with limited manpower and skills to manage it all
- Managing and monitoring increasing compliance demands

Gaining insights across the entire security event timeline



Identify Threats

Detect configuration errors and other deviations from the norm in order to gain awareness of vulnerabilities and assess exposures

Prioritize Events

Quickly analyze very large volumes of collected data (events and logs) to get to a manageably small number of true incidents to be further analyzed

Take Corrective Action

Dramatically reduce the time to remediation and increase the thoroughness of that remediation

A large international energy company parses billions of events per day to find those that should be investigated

An international energy firm analyzes 2 billion events per day, now extending analysis to the mobile platform and focusing on anomalies associated with key individuals

Summary

- Enterprise mobility management is needed and necessary
- MDM is a good place to start but additional security required
- Need to account for device risk
- Must build secure mobile apps and must secure apps “in the wild”
- Identity and access security must be adaptive – contextually aware

Think of mobile security more holistically

- Broader than MDM
- Think… device, content, application, and access
- More than a collection of point or partner 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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.

Legal notices and disclaimers

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml