Pulse

IBM SolutionsConnect 2013

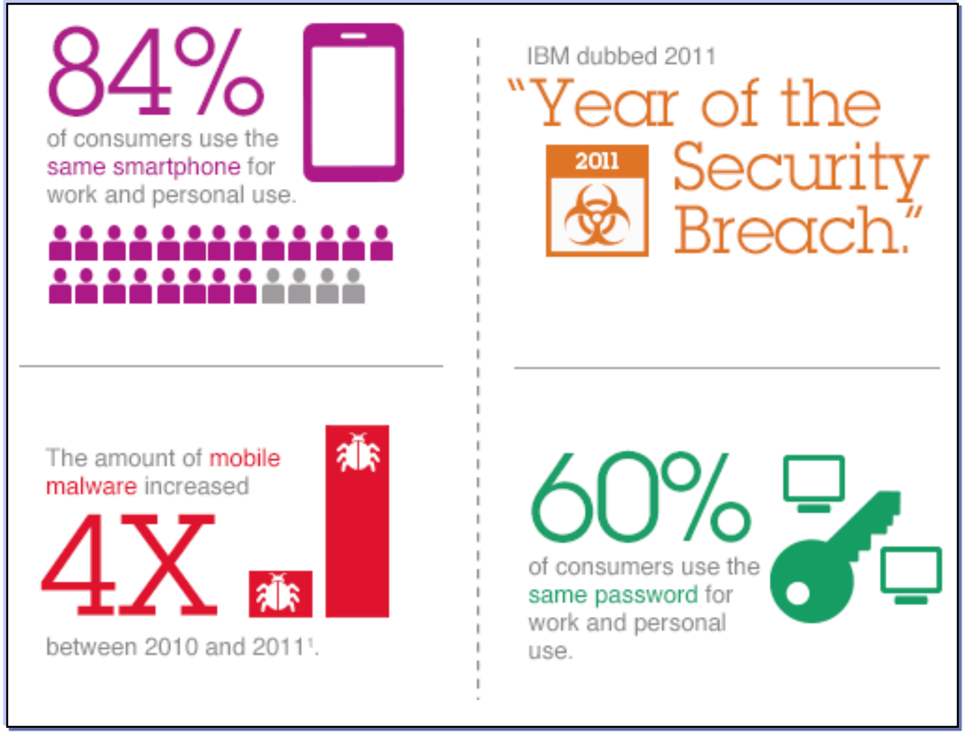
Crafting an Adaptive Mobile Security & Management Posture

Delivering Confidence

06/12/2013

IBM

Enterprises Need Confidence to Put Mobile First

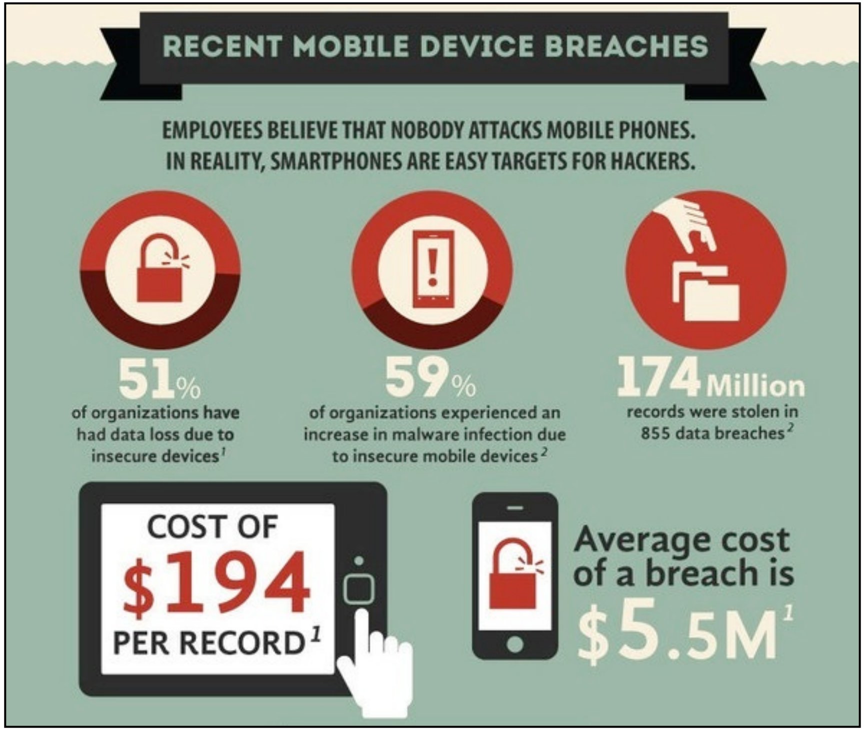


84% of consumers use the same smartphone for work and personal use.

IBM dubbed 2011 "Year of the Security Breach."

The amount of mobile malware increased 4X between 2010 and 2011[1].

60% of consumers use the same password for work and personal use.



RECENT MOBILE DEVICE BREACHES

EMPLOYEES BELIEVE THAT NOBODY ATTACKS MOBILE PHONES. IN REALITY, SMARTPHONES ARE EASY TARGETS FOR HACKERS.

51% of organizations have had data loss due to insecure devices[1]

59% of organizations experienced an increase in malware infection due to insecure mobile devices[2]

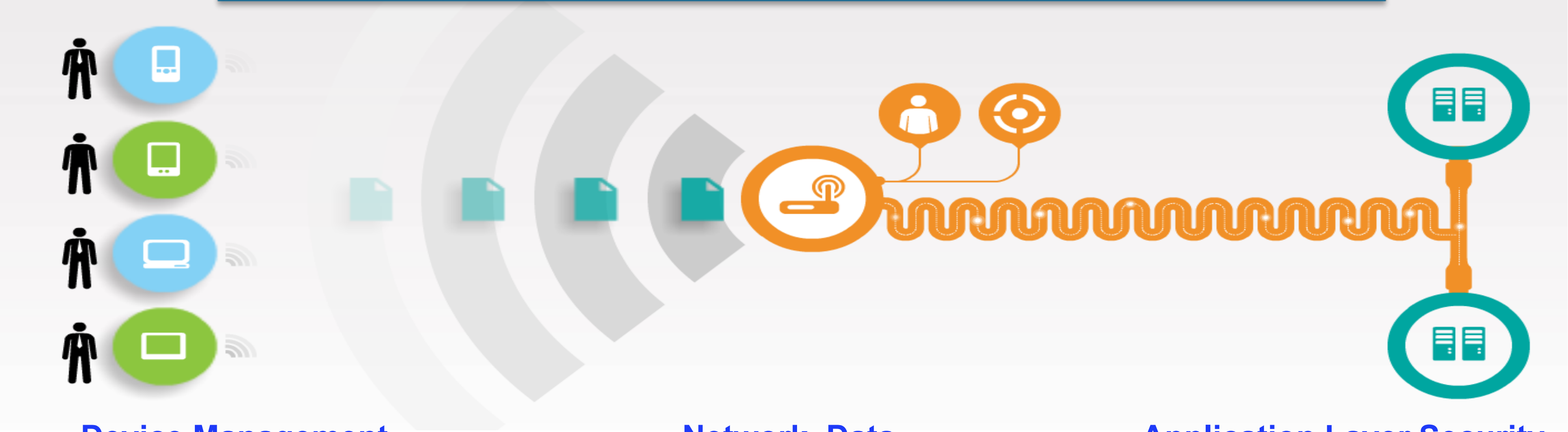
174 Million records were stolen in 855 data breaches[2]

COST OF $194 PER RECORD[1]

Average cost of a breach is $5.5M[1]

A Frame of Reference to Structure Your Strategy

IBM Mobile Security and Management Framework



Device Management

Security for endpoint device and data

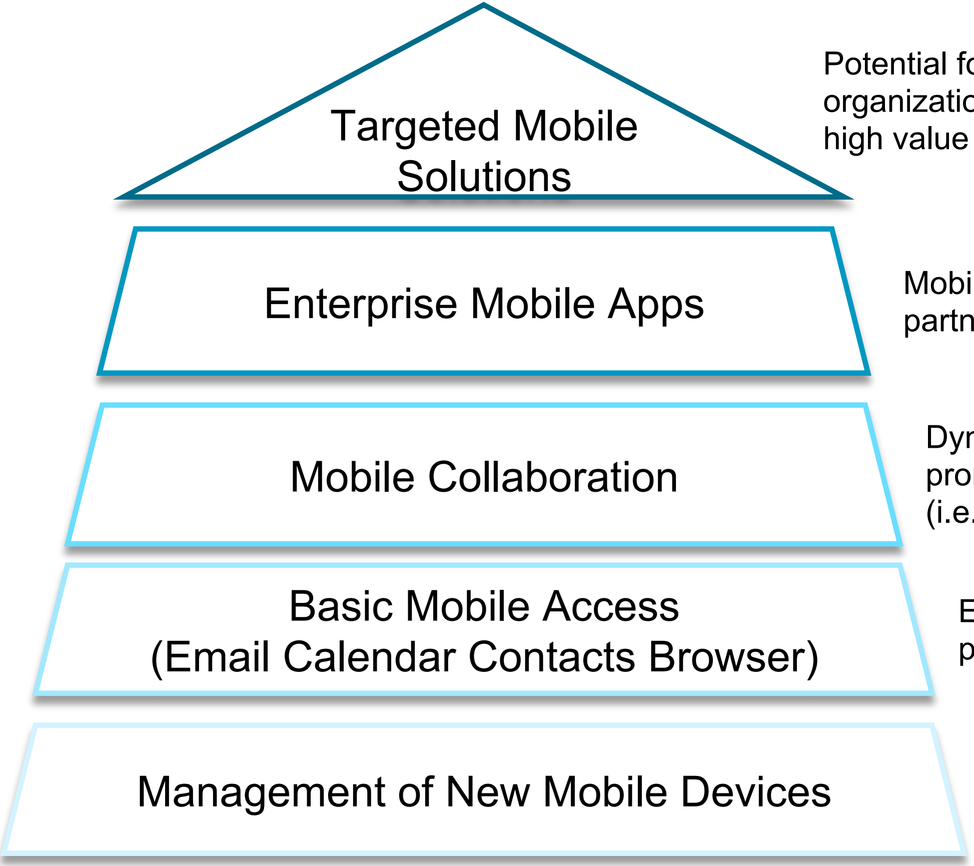
Network, Data, and Access Security

Achieve visibility and adaptive security policies

Application Layer Security

Develop and test applications

Operational Priorities in Evolving to a Mobile Enterprise



Targeted Mobile Solutions

Potential for productivity gains and enhancing employee and organization responsiveness motivating organizations to transform high value processes (i.e. Mobile Payments, Health Monitoring etc)

Enterprise Mobile Apps

Mobile as the preferred channel to reach employees and partners encouraging proliferation of mobile business apps

Mobile Collaboration

Dynamic work tasks and context-specific interactions promote the use of mobile devices for content collaboration (i.e. messaging, file sharing, etc)

Basic Mobile Access
(Email Calendar Contacts Browser)

Employees demanding greater mobile access to core productivity tools

Management of New Mobile Devices

Organizations facing an ever increasing influx of consumer mobile devices on the corporate network require visibility over those devices

Mobile Security Maturity Model

Optimized	**Mobile Security Intelligence** Risk Assessments, New Threat Detection, Active Monitoring			
	Integrated management of multiple devices Device Security policy management	Prevent loss or leakage of sensitive information Risk / Context based Access Threat Detection on inbound network traffic	Context / Risk based document collaboration / creating / viewing Enforce restrictions on copy/ paste	Multi-factor context aware access and offline access Granular security policy definition and enforcement Enable data sharing based on policy
Proficient	Endpoint Protection with Anti-malware White/black list apps Detection of Jailbreak/ rooted devices	Prevent copy and paste of email, calendar, contacts and intranet data Application level VPN	Secure document creation and viewing Document Collaboration with secure file sync / collaboration	App Management – provisioning/ updates/disabling Separation of corporate apps from personal apps Application validation
Basic	Update management Device lock / Device wipe Device Registration	Segregated secure access corporate email, calendar, contacts and browser User /device authentication and single sign-on	Connectivity to social networks Secure instant messaging	Enforcing encryption of data within an app App Vulnerability Testing and Certification
	BYOD	**Data Separation**	**Mobile Collaboration**	**Mobile App. Security**

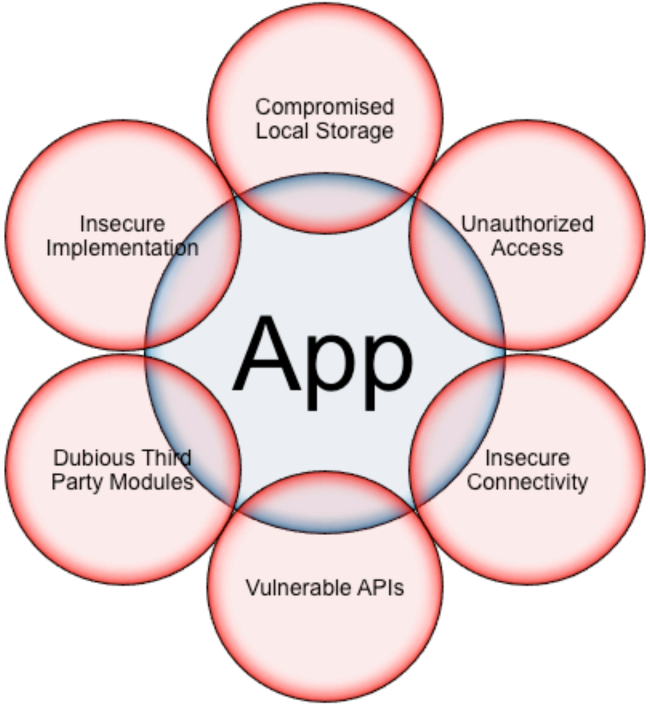
What if context determined capabilities automatically & securely?

Governed Policy

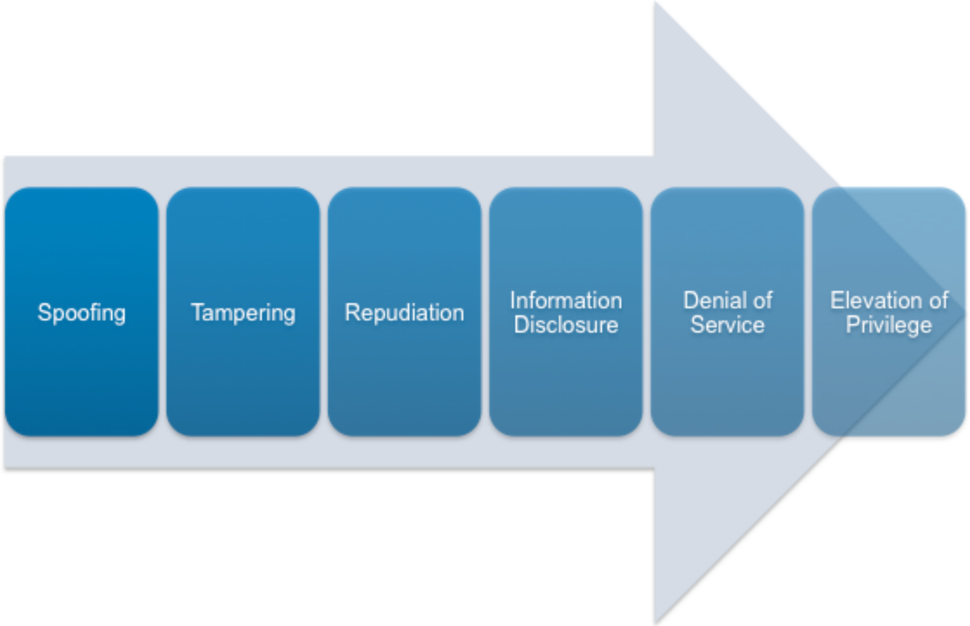
- Context
  - On-site inside emergency room
  - On the hospital network
  - Authorized doctor on shift
- Function: All app features
- Data: Full data access and storage
- Security: Single-factor authentication

- Context
  - At coffee shop
  - On an unsecured network
  - Authorized doctor on call
- Function: Designated features only
- Data: Specific encrypted data
- Security: Multi-factor authentication

Need to Defend the Mobile App

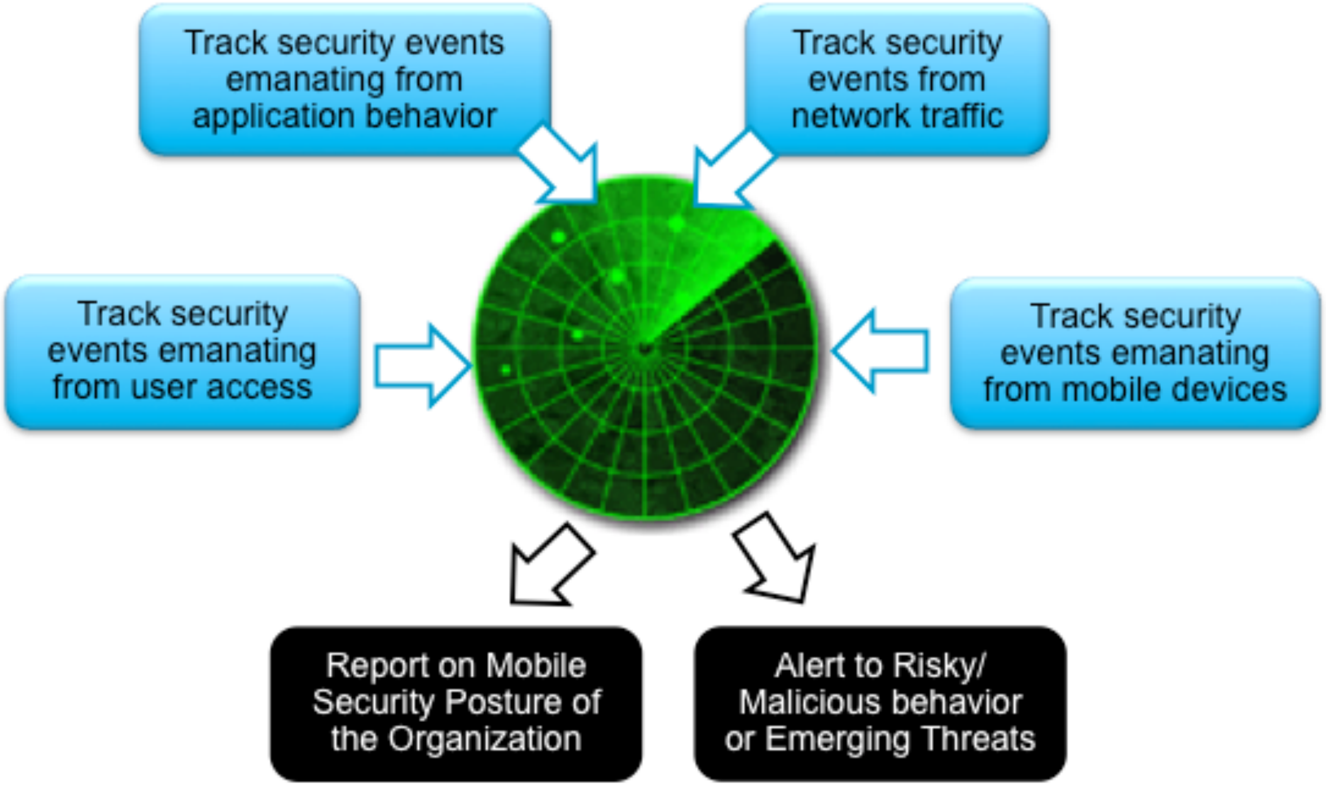


App Threat Surface Area



App Attack Approaches

Mobile Security Intelligence



Track security events emanating from application behavior

Track security events from network traffic

Track security events emanating from user access

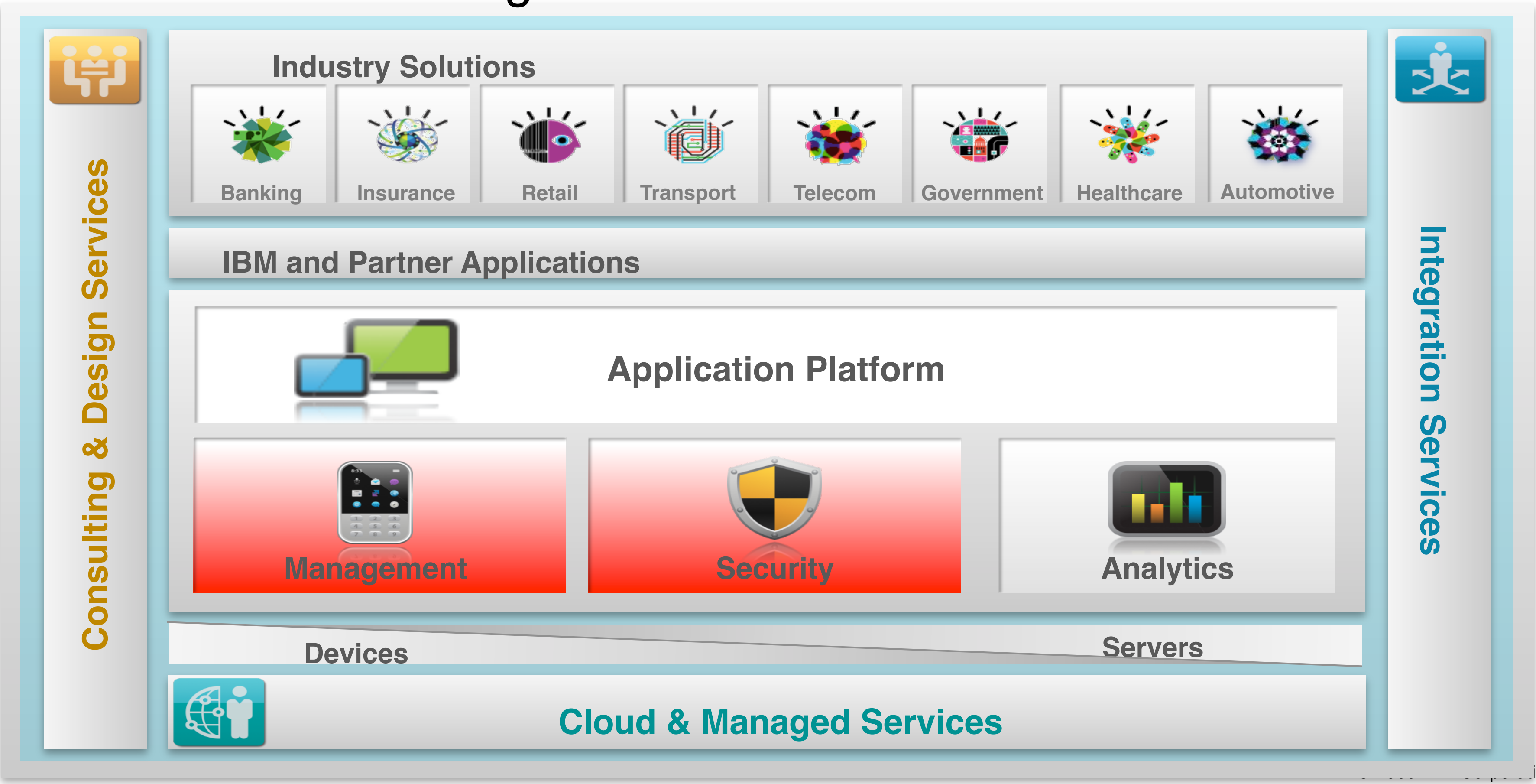
Track security events emanating from mobile devices

Report on Mobile Security Posture of the Organization

Alert to Risky/ Malicious behavior or Emerging Threats

IBM Solutions

IBM MobileFirst Offering Portfolio



Consulting & Design Services

Industry Solutions

Banking

Insurance

Retail

Transport

Telecom

Government

Healthcare

Automotive

IBM and Partner Applications

Application Platform

Management

Security

Analytics

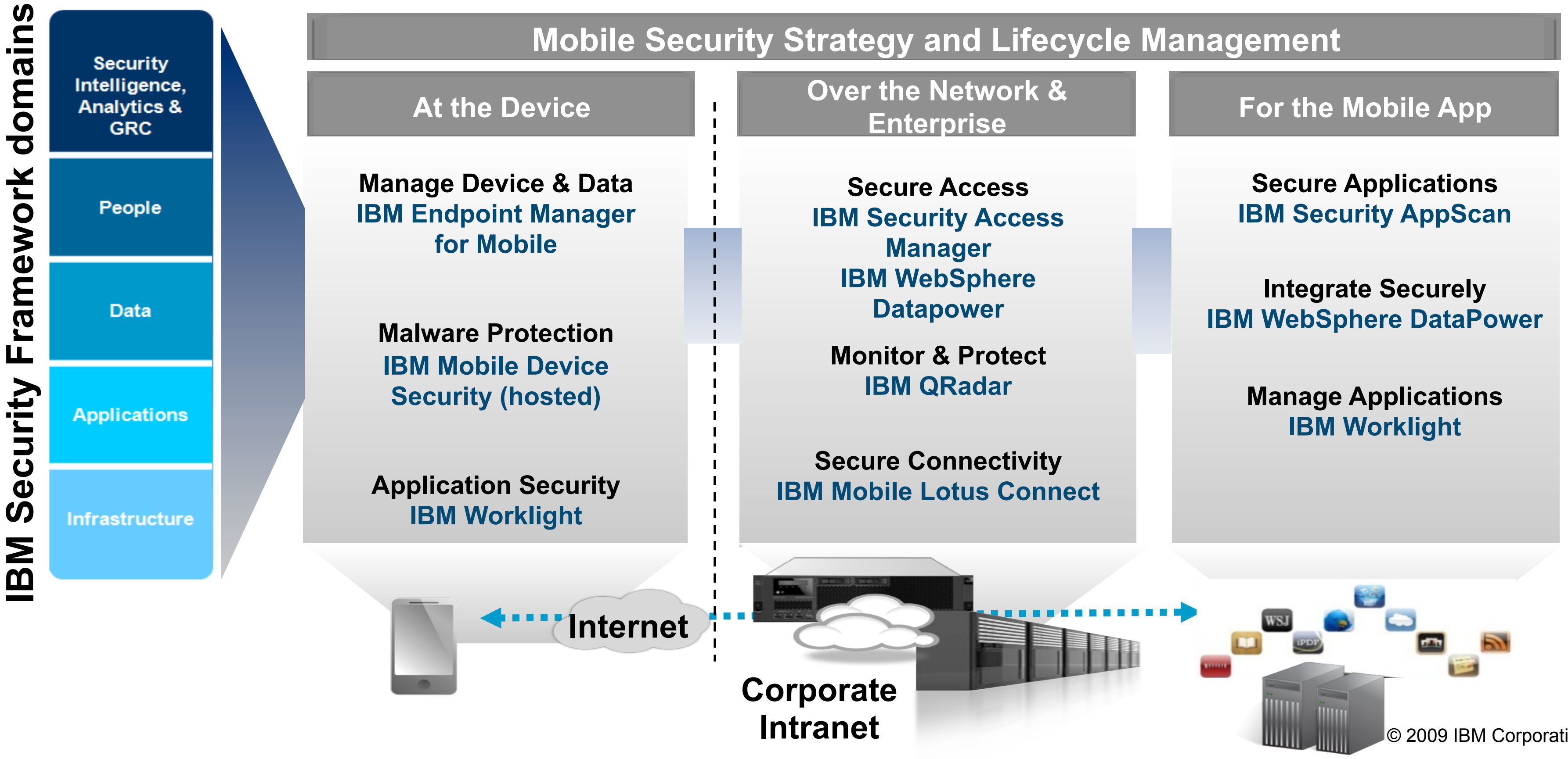
Devices

Servers

Cloud & Managed Services

Integration Services

IBM MobileFirst offerings to secure the enterprise



IBM Security Framework domains

- Security Intelligence, Analytics & GRC
- People
- Data
- Applications
- Infrastructure

Mobile Security Strategy and Lifecycle Management

At the Device

Manage Device & Data
IBM Endpoint Manager for Mobile

Malware Protection
IBM Mobile Device Security (hosted)

Application Security
IBM Worklight

Over the Network & Enterprise

Secure Access
IBM Security Access Manager
IBM WebSphere Datapower

Monitor & Protect
IBM QRadar

Secure Connectivity
IBM Mobile Lotus Connect

For the Mobile App

Secure Applications
IBM Security AppScan

Integrate Securely
IBM WebSphere DataPower

Manage Applications
IBM Worklight

*A **Mobile First** organization needs…*

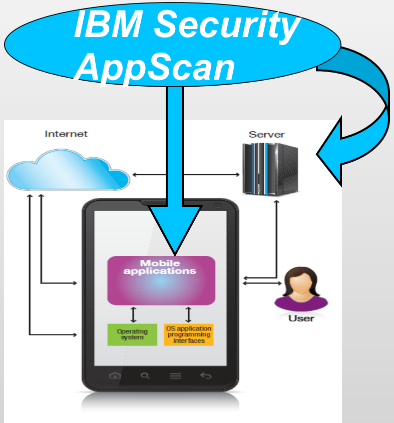
Prioritized security and privacy throughout the mobile app lifecycle to protect sensitive business systems

IBM Security AppScan 8.7

What’s New

- **Accelerates the use of iOS** in an Enterprise setting
- **Native security scanning of iOS applications** built in Objective C, Java or JavaScript
- **Facilitates a "secure by design" process** in the software development lifecycle for mobile applications
- Addresses requirements for **usage in the US Federal Government**

Mobile Security



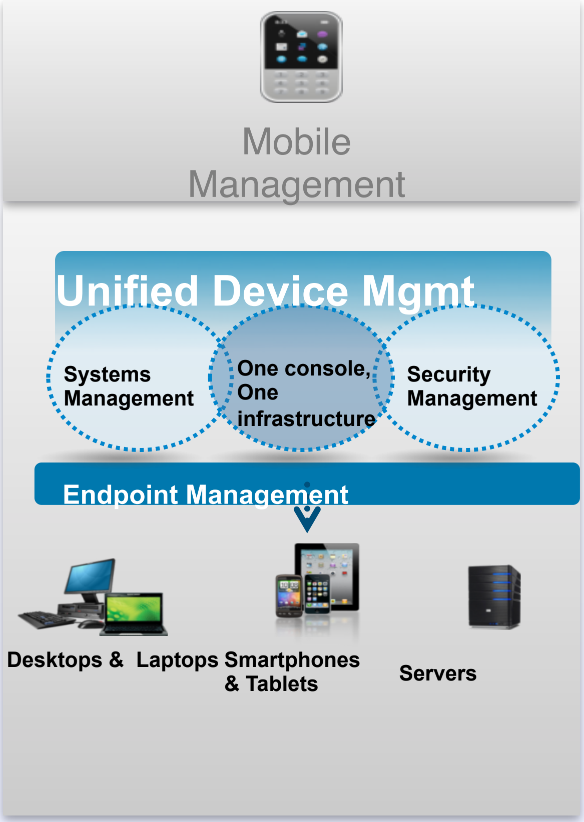
*A **Mobile First** organization needs…*

Real-time visibility and control over all mobile devices

IBM Endpoint Manager for Mobile Devices

What' s New

- **FIPS 140-2 Certified Encryption Module**
  – Meet US Government standards for data protection
- **Automated Compliance-based Email Access**
  – Automatically grant or deny email access based on device compliance.
- **IBM Lotus Notes Traveler Security Policy Integration**
  – Ease security administration by setting and reporting Lotus Traveler security policies through the Endpoint Manager console
- **Expanded BYOD Platform Support**
  – BlackBerry 10, Microsoft Windows Phone 8, Windows RT, Apple iOS 6.1



Mobile Management

Unified Device Mgmt

Systems Management

One console, One infrastructure

Security Management

Endpoint Management

Desktops & Laptops

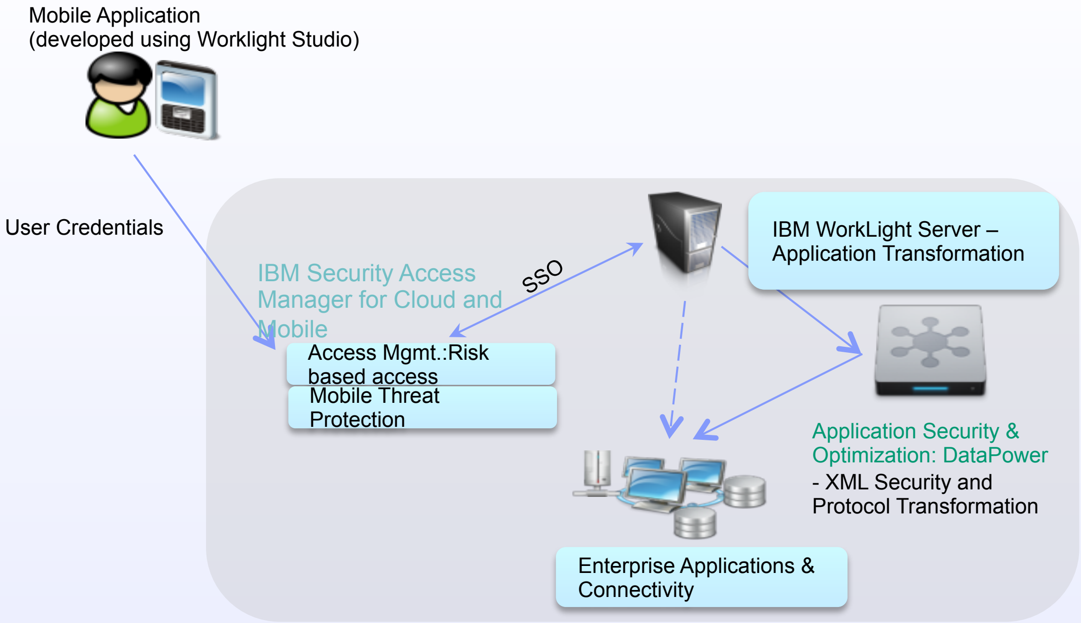
Smartphones & Tablets

Servers

*A **Mobile First** organization needs…*

Increase accuracy of identifying mobile access security risks

IBM Security Access Manager for Cloud and Mobile



Mobile Application
(developed using Worklight Studio)

User Credentials

IBM Security Access Manager for Cloud and Mobile

SSO

Access Mgmt.:Risk based access

Mobile Threat Protection

IBM WorkLight Server – Application Transformation

Application Security & Optimization: DataPower

- XML Security and Protocol Transformation

Enterprise Applications & Connectivity

Mobile Security

Key Capabilities

Increase accuracy of identifying mobile access security risks

- Dynamically assess the security risk of an access request
- Quickly enforce Risk-Based Access
- Ensuring users and devices are authenticated and authorized
- Flexibility and strength in authentication: user id/password, OTP, biometrics, certificate, custom
- Protect applications from known security threats by analyzing HTTP traffic

Customer Case Studies

European Bank delivers secure mobile Internet banking

Background

Major European Bank needed to reduce operational complexity and cost with a single, scalable infrastructure to secure access to various back-end services from multiple mobile apps. A customized authentication mechanism empowered the bank to guarantee the security of its customers while safeguarding the trust relationship with a safe app platform that encrypts local data and delivers app updates immediately.

Customer Needs

- Extend secure access to banking apps to mobile customers
- Enhance productivity of employees to perform secure banking transactions via mobile devices
- Support for iOS, Android, and Windows Mobile

Benefits

- Authenticates requests made via HTTPS from hybrid mobile apps running on WorkLight platform to back-end services
- A custom certificates-based authentication mechanism implemented to secure back-end banking application

A health insurance provider offers secure mobile access

Challenges

Differentiate from competitors by offering customers greater access by supporting mobility

Reduce overhead of paper-based claims processing and call-center volume

Solution

Requests made via HTTPS to multiple back-end services from native device applications protected by IBM Security Access Manager

Authentication enforced with both Basic Authentication and a custom implementation through Access Manager's External Authentication Interface

Benefits

- Simultaneously build trust and improve user experience with secure membership management and claims processing
- Improve customer satisfaction and responsiveness through secure mobile solutions

Public utility adds mobile devices without adding infrastructure

Company Overview

Serving 4.5 million customers in the southwestern region of the United States, this electric company of 25,000 employees is a leader in clean energy while exceeding reliability standards and keeping consumer costs below average. They are experiencing a migration from traditional endpoints to mobile devices.

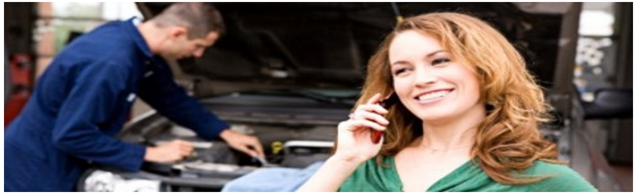
Customer Needs

- Support 20,000+ mobile devices
- Corporate and employee-owned, many platforms and OS versions
- High availability for certain devices used in the field
- Adherence to internal security policies, external regulations

Benefits

- Scalability to 250,000 endpoints provides room to grow without adding infrastructure
- Added mobile devices to existing IEM deployment in days
- Ability to integrate with Maximo, Remedy
- Responsiveness and agility of product and product team

Global automotive company secures mobile access



Challenges

- Automobile customers require secure, personalized access to vehicle information services on their mobile devices
- Required secure access to radio, internet and social network services from the automobile

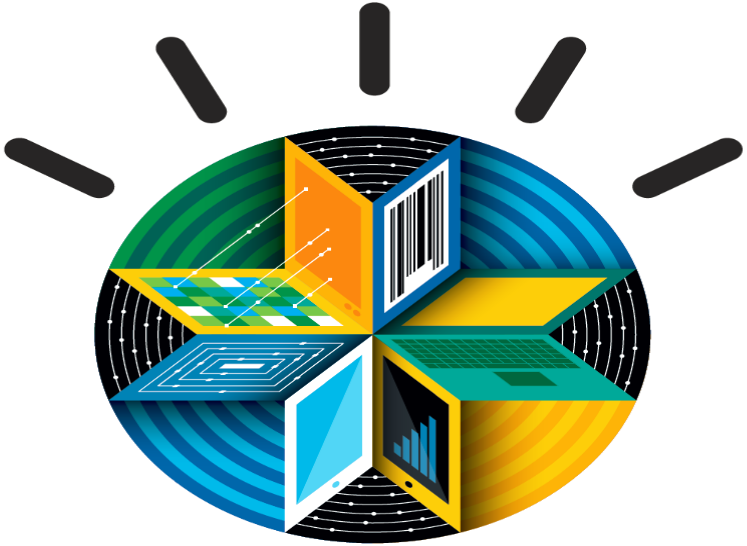
Solution

- IBM Security Access Manager and IBM Federated Identity Manager along with IBM DataPower
- Seamless authentication and authorization to back-end automotive business services

Benefits

- Simplified single sign-on for trusted third party service providers
- Scale to hundreds of thousands of devices and users
- Improved customer satisfaction

Get started with IBM



- Learn more at:

  www.ibm.com/mobilefirst

  - Access white papers and webcasts
  - Get product and services information

- Talk with your IBM representative or IBM Business Partner to find the right next step for you