IBM

IBM Security Symposium

Intelligence | Integration | Expertise

# IBM Mobile Security

## DELIVERING CONFIDENCE

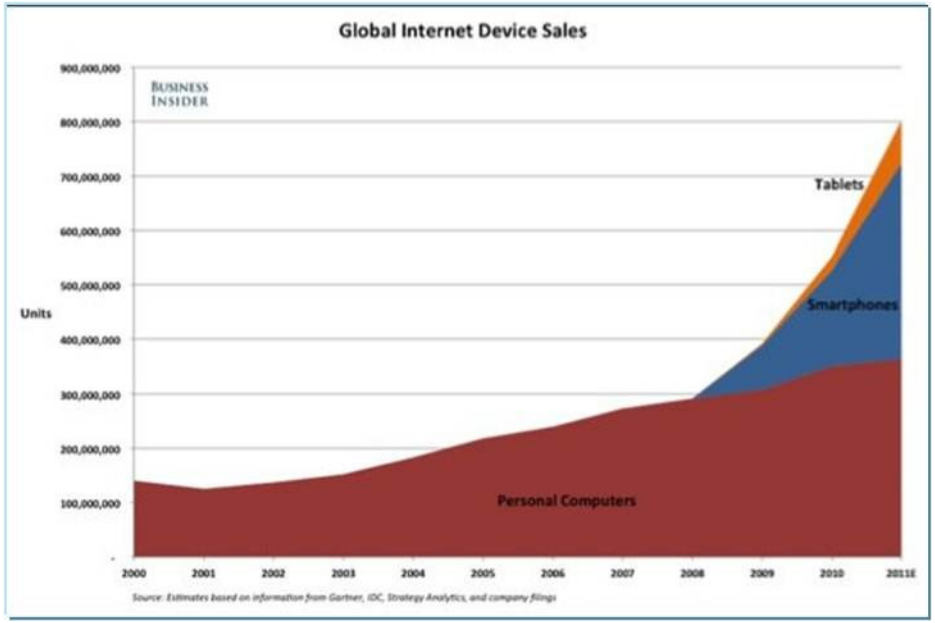

Vijay Dheap

Global Product Manager, IBM Mobile Security Solutions

IBM Master Inventor

Twitter: @dheap

# It's a (Smarter) Mobile World!

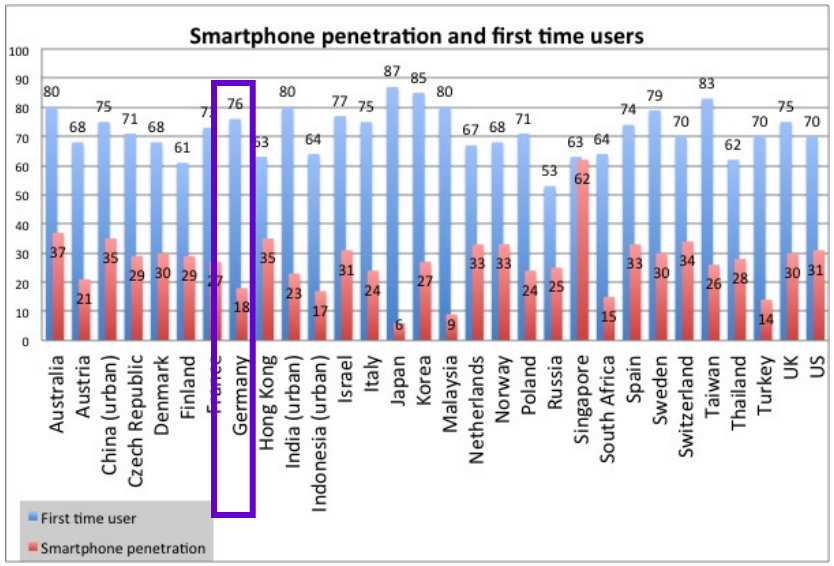


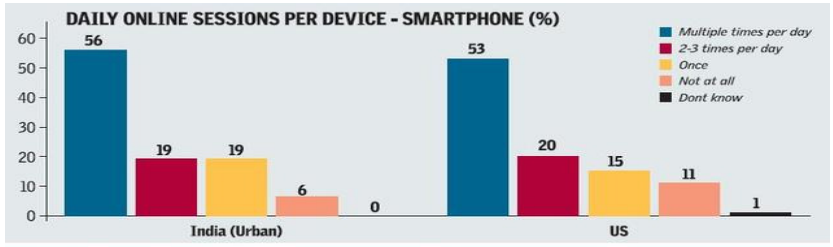


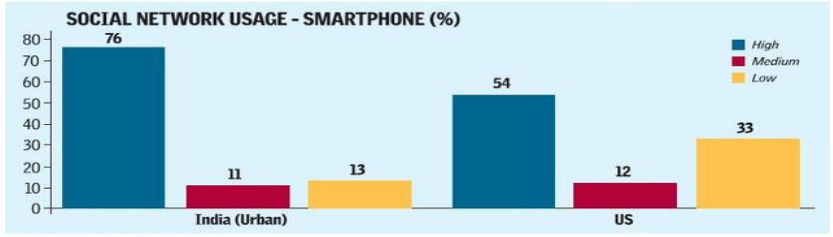
In 2011 sales of smartphones surpassed that of PCs, soon they will dwarf the sales of PCs

- Business Insider

# Mobile India…



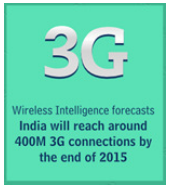




Source: www.ourmobileplanet.com

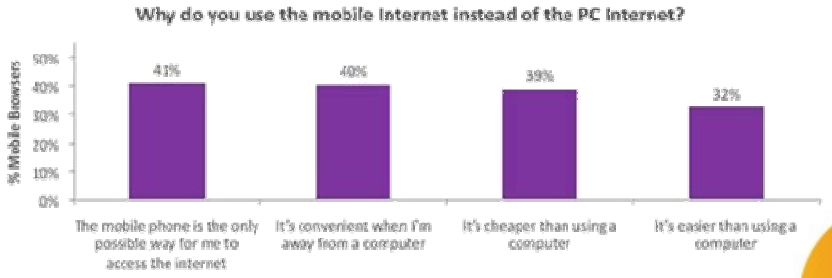
IBMSecuritySymposium
Intelligence | Integration | Expertise

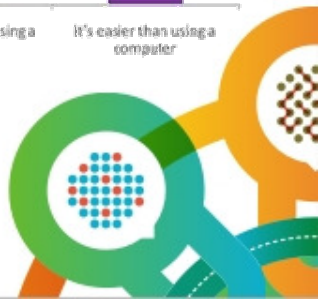
23% of Urban India population have smart phones, and 80% are first time users

Based on the 2011 estimate by Census India, urban Indian population (37.7 Crore), there are more smartphone users in India than the population of Germany! (~86M > ~81M)




36% of all smartphone owners in India are in 18-29 age group – the demographic dividend

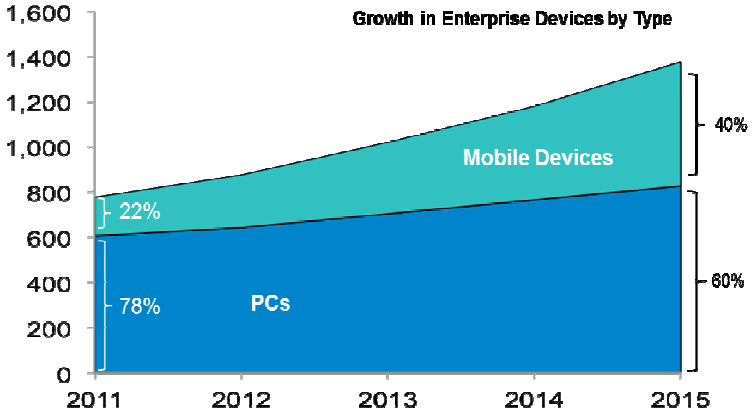


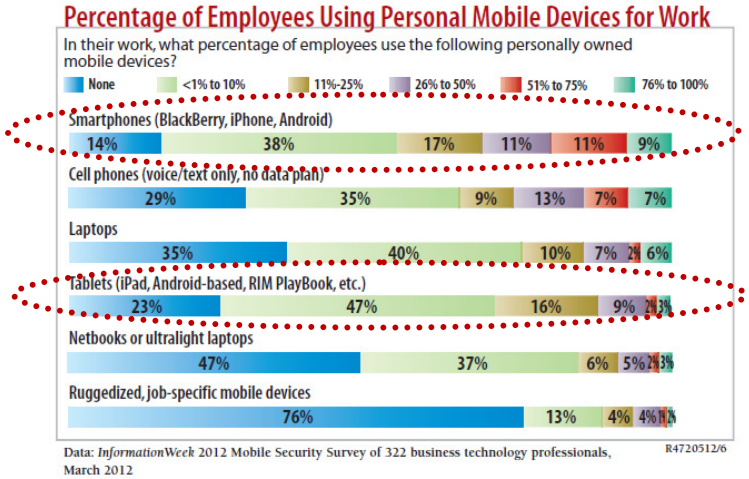



# Employees Bringing Smart Devices to Work…

By 2015 40% of Enterprise devices will be mobile devices

- IBM Projection




*80%of the employees from India claim that their companies permit them to connect to the corporate network with personally owned devices and use them for work.*

- BT Assure- Rethink the Risk Survey

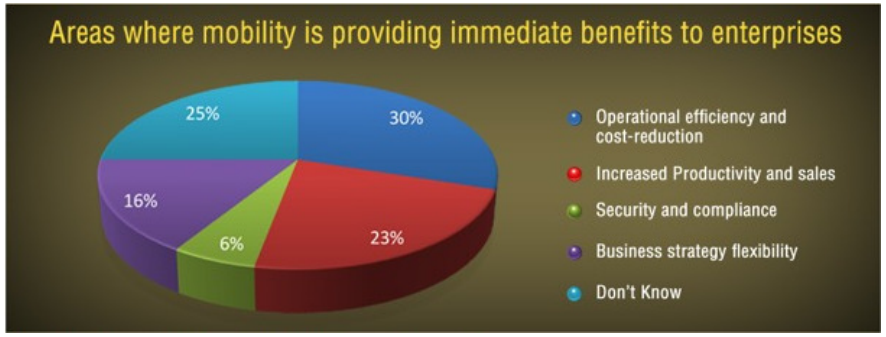
**Bring Your Own Device (BYOD)**

- The trajectory of adoption is coming from the consumer space into the enterprise.
- Greater propensity for users of smartphones and tablets to use their personal devices for work
- Organizations starting to view BYOD for its business value and organizations recognizing the competitive differentiation it can offer


IBMSecuritySymposium

Intelligence | Integration | Expertise

# Mobility as an Enabler for India Inc.


Business value driven by mobility applies across regions, but mobile is also opening up unique opportunities for the Indian market

**Increasing the Banking Population**

•A major Indian Bank wants to educate rural communities on the benefits of banking and grow its cash reserves

•Hired 250,000 agents to teach and market banking products

•Each agent used their own personal mobile phone and the bank's mobile solution facilitated transactions, captured information for risk determination and incentivized agents

**Achieving Operational Excellence**

•Inefficient workflows at a major Indian airport was raising operational costs for airlines

•Mobile solution to guide and monitor airport workers dramatically transformed operations leading to achieving unrealized efficiencies

•Exported solution to airports in other regions (i.e. China, Middle East, Europe)

# Uniqueness of Mobile…

## Mobile devices are shared more often

- Personal phones and tablets shared with family
- Enterprise tablet shared with co-workers
- Social norms of mobile apps vs. file systems

## Mobile devices have multiple personas

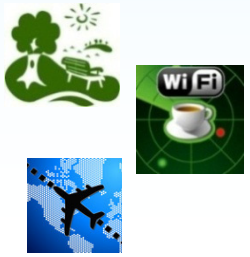
- Work tool
- Entertainment device
- Personal organiser
- Security profile per persona?

## Mobile devices are diverse

- OS immaturity for enterprise mgmt
- BYOD dictates multiple OSs
- Vendor / carrier control dictates multiple OS versions
- Diverse app development/delivery model

## Mobile devices are used in more locations

- A single location could offer public, private, and cell connections
- Anywhere, anytime
- Increasing reliance on enterprise WiFi
- Devices more likely to be lost/stolen



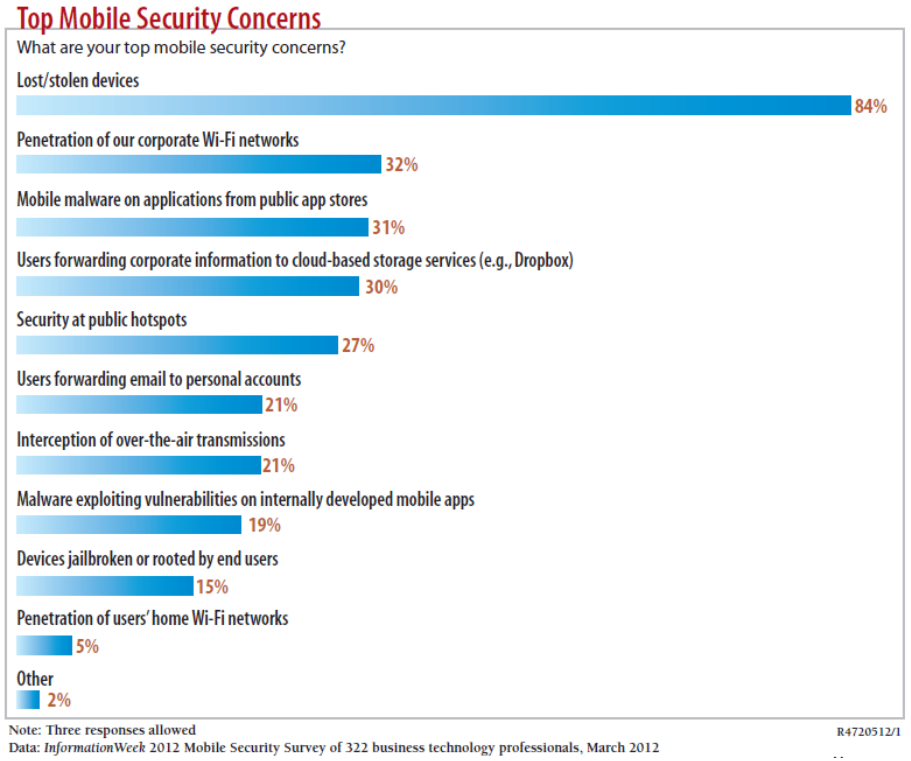

## Mobile devices prioritise the user

- Conflicts with user experience not tolerated
- OS architecture puts the user in control
- Difficult to enforce policy, app lists
- Security policies have less of a chance of dictating experience

# Mobile Security Risks, Concerns & Emerging Threats

**OWASP Mobile Security Project:**
*Top 10 Mobile Risks, (Release Candidate v1.0)*

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure




| Emerging Mobile Threats | |
|---|---|
| Social Engineering | Mobile Borne DoS Attacks |
| Rogue Apps | Identity Theft |
| Malicious Websites | Man-in-the-Middle Attacks |

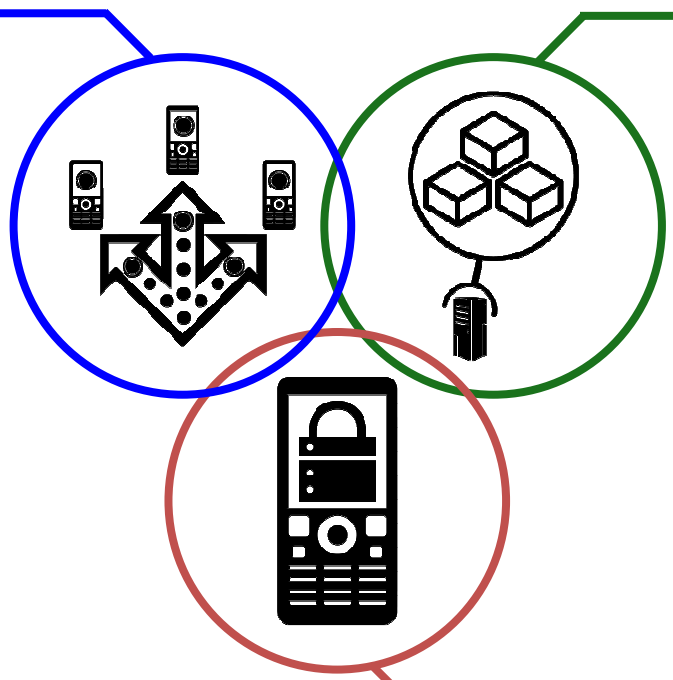
IBMSecuritySymposium
Intelligence | Integration | Expertise

# IBM Strategy Addresses Client Mobile Initiatives

## Extend & Transform

***Extend*** *existing business capabilities to mobile devices*

***Transform*** *the business by creating new opportunities*



## Build & Connect

***Build*** *mobile applications*

***Connect*** *to, and* ***run*** *backend systems in support of mobile*

## Manage & Secure

***Manage*** *mobile devices and applications*

***Secure*** *my mobile business*

IBMSecuritySymposium
Intelligence | Integration | Expertise

# IBM Case Study

- 95% of IBM employees are issued laptops
- Over 100,000 smartphones and tablets with access to the IBM corporate network and growing rapidly!
- Personally owned devices can be used for business purposes
- Strong dependency on collaboration and social media tools to conduct IBM business and stay connected

*IBM's BYOD program "really is about supporting employees in the way they want to work. They will find the most appropriate tool to get their job done. I want to make sure I can enable them to do that, but in a way that safeguards the integrity of our business."*

***– IBM CIO Jeanette Horan***

## How did IBM become a mobile enterprise?

- Established policies for mobile employees
- Established policies for personally-owned devices
- Sold expensive office space and created world-wide mobility centers
- Launched small, focused "opt-in" BYOD pilots. Resisted the urge to "boil the ocean"
- Embraced collaboration and social media tools to allow mobile devices to stay connected

**A highly diverse workforce:**

- 425,000 employees worldwide
- 50% workforce has less than 5 years of service
- 50% of employees work remotely – not from a traditional IBM office
- 71% of employees are outside the US

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Execute Based on Segmentation

## Approach

Determine key IT services necessary for employees to do their jobs

Determine the environment and attitude of employees

Cluster employees with similar IT requirements and work locations in groups

Validate IT requirements and employee segments through a survey or user interviews

Map segments to traditional HR demographics such as Job Role and Business Unit

Use employee segments to identify targets for new technology deployments

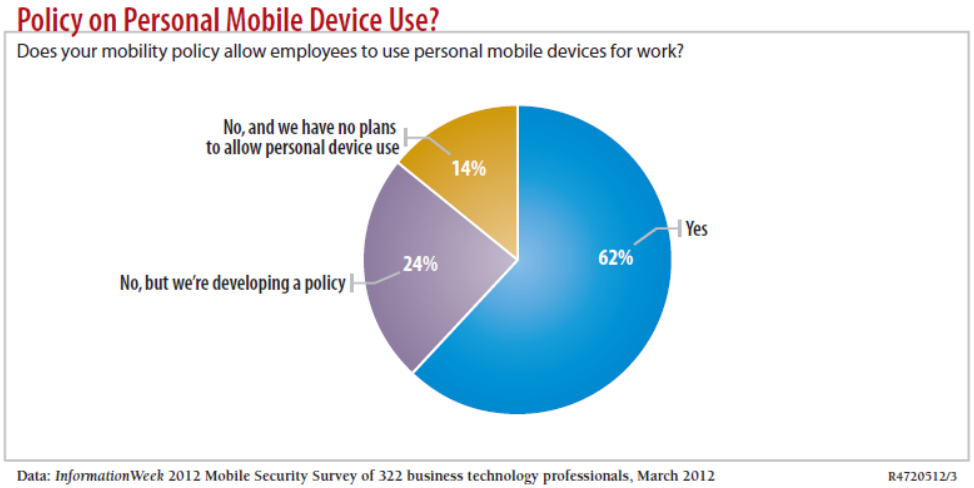
## Identified Personas

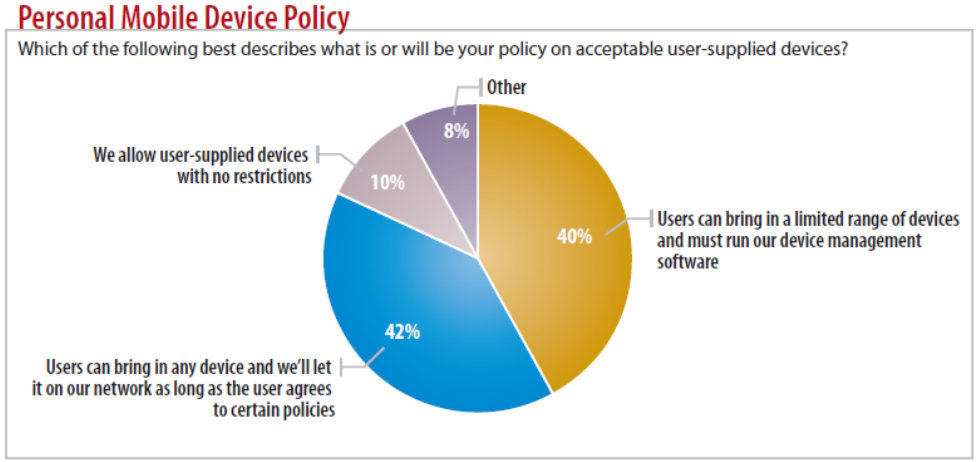
| ***13 Personas based on the IT requirements of IBMers*** | |
|---|---|
| Customer facing IBMer | IBM office based employee |
| Growth market employee in a global support role | Work at home employee (non-traveller) |
| Manufacturing and other non-traditional office employees | Employee with a basic software and application need |
| Researcher, SW and HW development engineer with a high end workstation requirement | Employee with accessibility requirements |
| Employee with low technology adoption attitude score | Employee in a leadership or executive role |
| Employee with a high technology adoption attitude score | Frequent traveller – non customer facing (e.g. Education, internal auditor etc) |
| Employee joining through an acquisition (Before systems integration) | |

# Cost Considerations of BYOD

- Roadmap for BT/IT Shared Service includes yty expense reduction while workforce grows
- Corporate managed program by role/segments
  - Mobility tool for guidance and options
  - Compliance Process & Validation (A&E)
- Cost management
  - Employees can leverage IBM contracts
  - Negotiate local geo/country contracts with global mobile carriers including ongoing service cost reduction
  - Strict Reimbursement policy
- A consistent mobile rendering of IBM web applications will require some investment and re-engineering (target apps based on relevance)
- IBM is investing in Mobile Device Management to improve security and systems management of these mobile devices

# BYOD: It's a Spectrum




Organizations have to start on the BYOD journey by establishing policies that meet their current operational objectives.

Policies can evolve as an organization and its employees better understand the risks as well as the benefits.

BYOD programs vary across organizations, industries and regions.

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Mobile Security Challenges Faced By Enterprises

**Achieving Data Separation & Providing Data Protection**

- Personal vs corporate data
- Data leakage into and out of the enterprise
- Partial wipe vs. device wipe vs legally defensible wipe
- Data policies

**Adapting to the BYOD/ Consumerization of IT Trend**

- Multiple device platforms and variants
- Multiple providers
- Managed devices (B2E)
- Unmanaged devices (B2B,B2E, B2C)
- Endpoint policies
- Threat protection

**Providing secure access to enterprise applications & data**

- Identity of user and devices
- Authentication, Authorization and Federation
- User policies
- Secure Connectivity

**Developing Secure Applications**

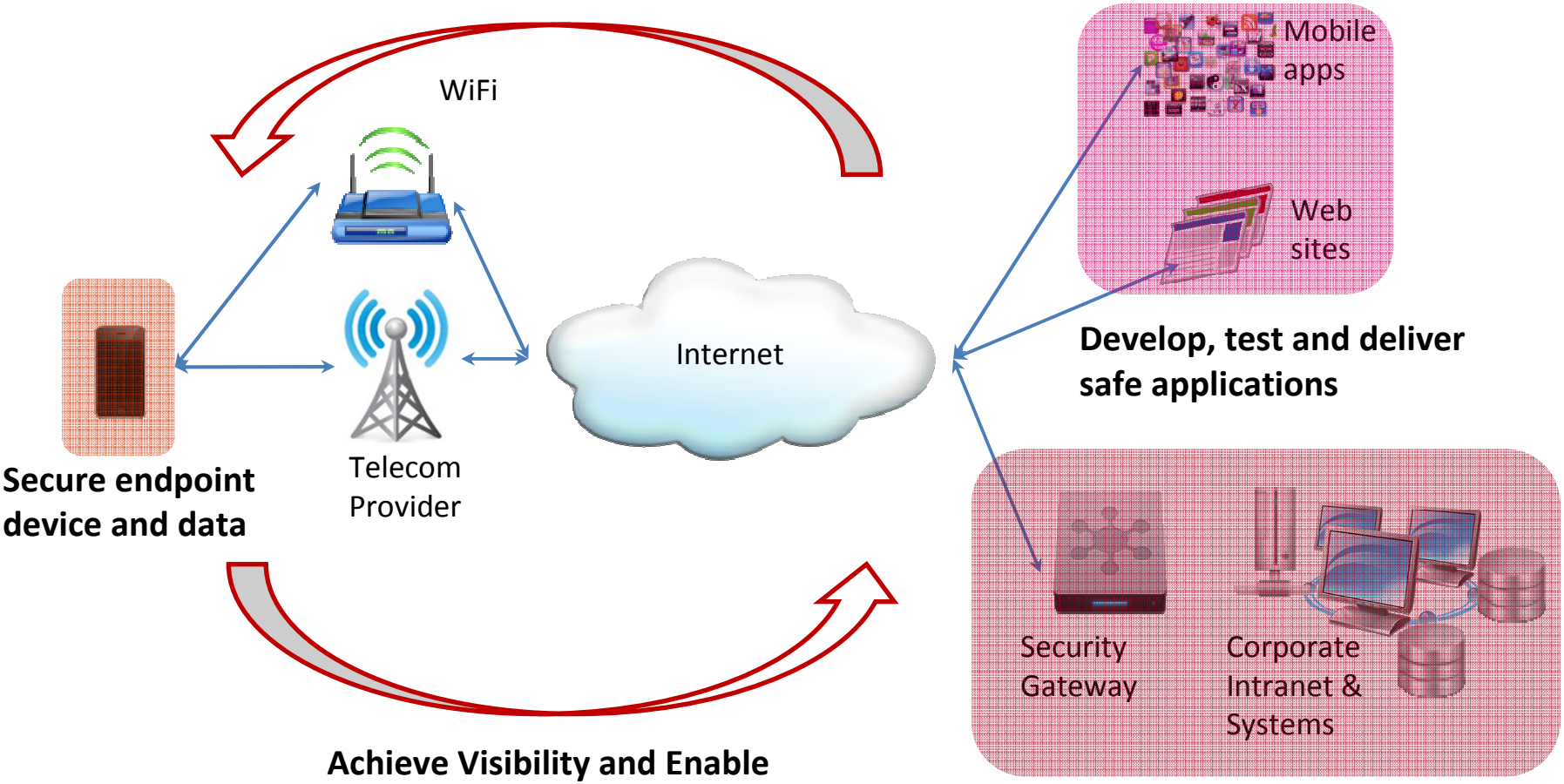
- Application life-cycle
- Vulnerability & Penetration testing
- Application Management
- Application policies

**Designing & Instituting an Adaptive Security Posture**

- Policy Management: Location, Geo, Roles, Response, Time policies
- Security Intelligence
- Reporting

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Visualizing Mobile Security



# Getting Started with Mobile Security Solutions…

## Business Need:
Protect Data & Applications on the Device

- ➢Prevent Loss or Leakage of Enterprise Data
  - ❑ Wipe
  - ❑ Local Data Encryption
- ➢Protect Access to the Device
  - ❑ Device lock
- ➢Mitigate exposure to vulnerabilities
  - ❑ Anti-malware
  - ❑ Push updates
  - ❑ Detect jailbreak
  - ❑ Detect non-compliance
- ➢Protect Access to Apps
  - ❑ App disable
  - ❑ User authentication
- ➢Enforce Corporate Policies

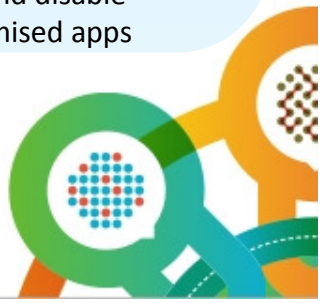
## Business Need:
Protect Enterprise Systems & Deliver Secure Access

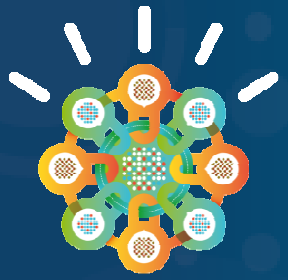
- ➢Provide secure access to enterprise systems
  - ❑ VPN
- ➢Prevent unauthorized access to enterprise systems
  - ❑ Identity
  - ❑ Certificate management
  - ❑ Authentication
  - ❑ Authorization
  - ❑ Audit
- ➢Protect users from Internet borne threats
  - ❑ Threat protection
- ➢Enforce Corporate Policies
  - ❑ Anomaly Detection
  - ❑ Security challenges for access to sensitive data

## Business Need:
Build, Test and Run Secure Mobile Apps

- ➢Enforce Corporate Development Best Practices
  - ❑ Development tools enforcing security policies
- ➢Testing mobile apps for exposure to threats
  - ❑ Penetration Testing
  - ❑ Vulnerability Testing
- ➢Provide Offline Access
  - ❑ Encrypted Local Storage of Credentials
- ➢Deliver mobile apps securely
  - ❑ Enterprise App Store
- ➢Prevent usage of compromised apps
  - ❑ Detect and disable compromised apps

IBMSecuritySymposium
Intelligence | Integration | Expertise



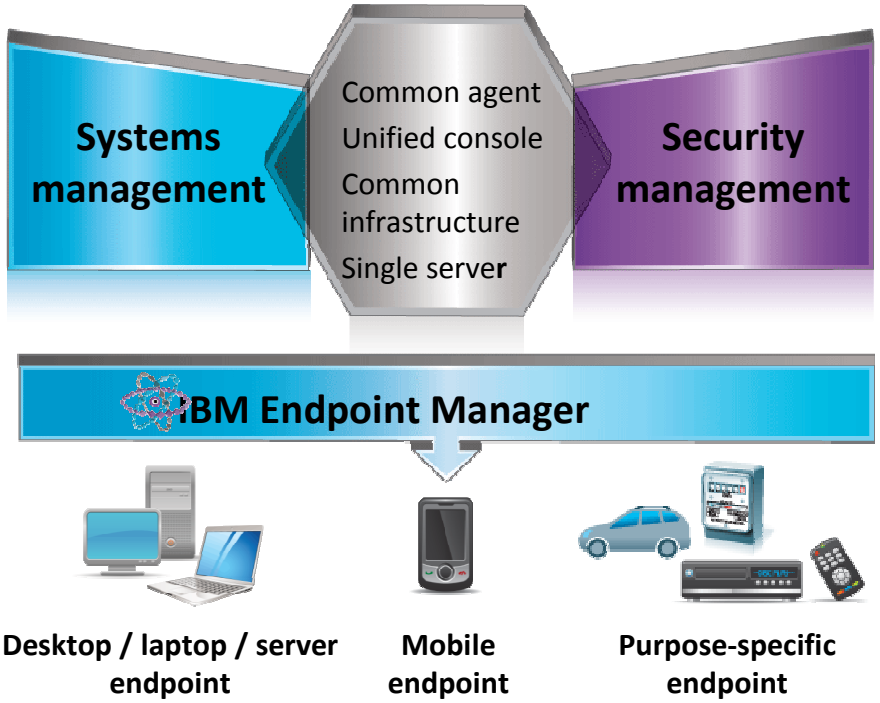


# DELIVERING CONFIDENCE

# Mobile Device Security

***IBM Endpoint Manager for Mobile Devices:*** *A highly-scalable, unified solution that delivers device management and security across device types and operating systems for superior visibility and control*

## Managed = Secure




## Client Challenge

Managing and securing enterprise and BYOD mobile devices without additional resources

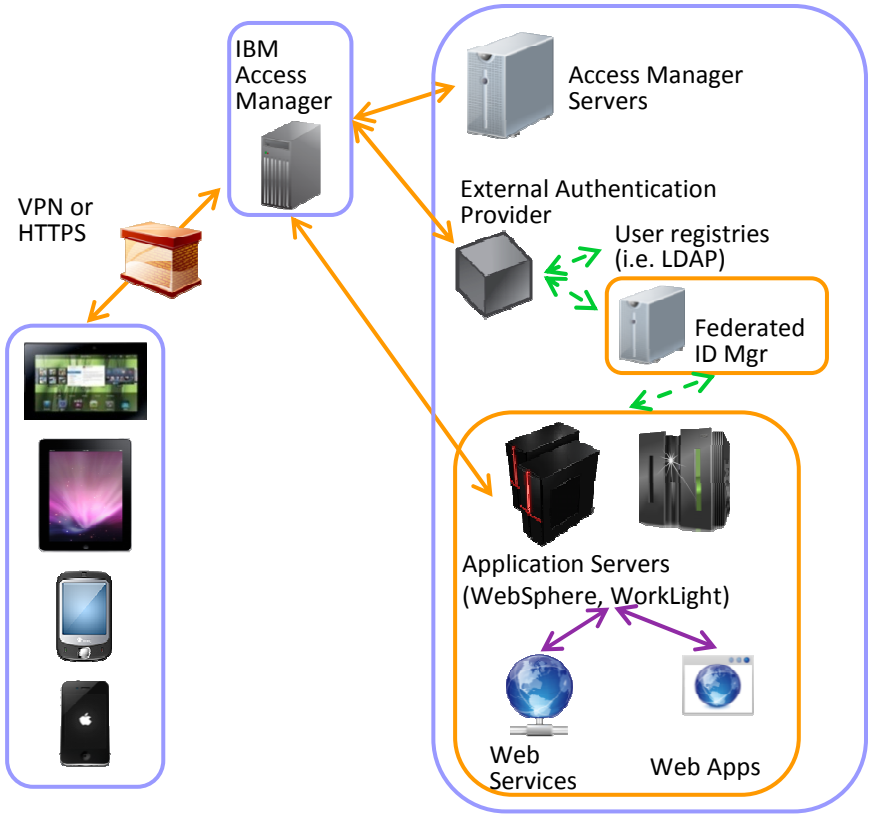
## Key Capabilities

- A unified systems and security management solution for all enterprise devices
- Near-instant deployment of new features and reports in to customer's environments
- Platform to extend integrations with Service Desk, CMDB, SIEM, and other information-gathering systems to mobile devices
- Advanced mobile device management capabilities for iOS, Android, Symbian, and Windows Mobile, Windows Phone
- Security threat detection and automated remediation

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Mobile Access Security

***IBM Security Access Manager for Mobile:*** *Delivers user security by authenticating and authorizing the user and their device*




## Client Challenge

Ensuring users and devices are authorized to access enterprise resources from that specific device.

## Key Capabilities

- Satisfy complex context-aware authentication requirements
- Reverse proxy, authentication, authorization, and federated identity
- Mobile native, hybrid, and web apps
- Flexibility in authentication: user id/password, basic auth, certificate, or custom
- Supports open standards applicable to mobile such as OAuth
- Advanced Session Management

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Mobile Access Security

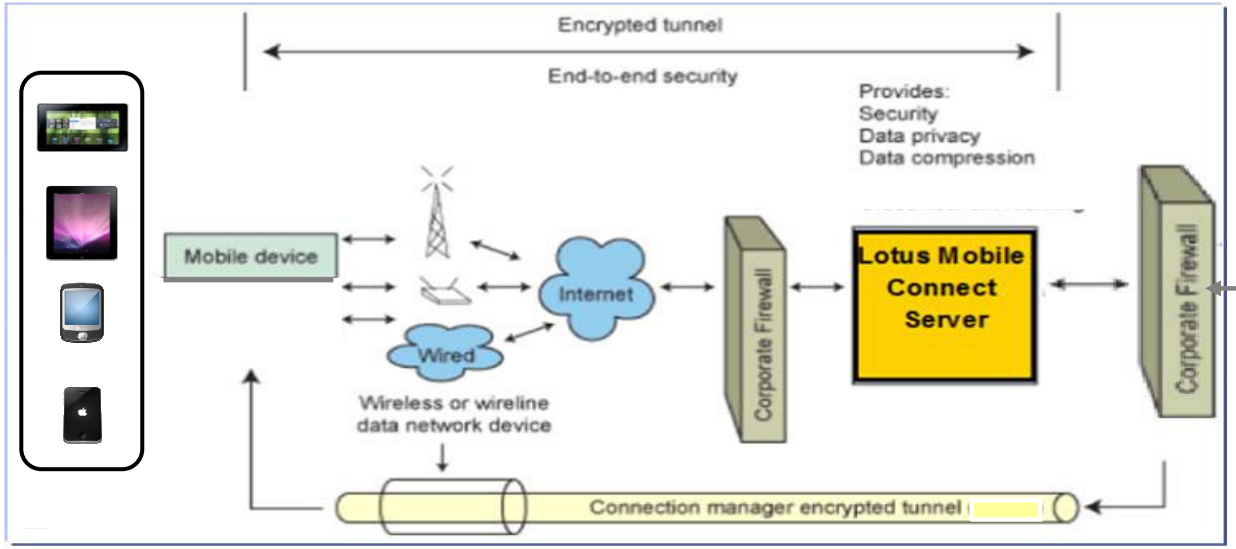
***IBM Lotus® Mobile Connect:*** *Provides features that help deliver a security-rich connection to enterprise resources from mobile devices.*

## Client Challenge

- Need to protect enterprise data in transit from mobile devices to back-end systems

## Key Capabilities

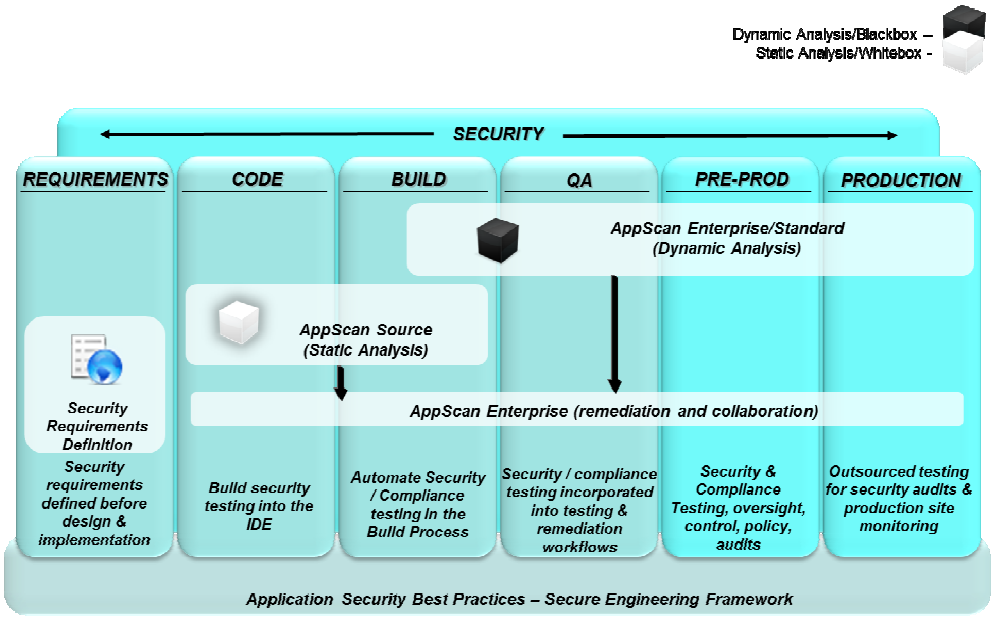
- Clientless app-level Virtual Public Network (VPN) with a SSL-secured tunnel to specific HTTP application servers
- Strong authentication and encryption of data in transit




IBMSecuritySymposium
Intelligence | Integration | Expertise

# Mobile App Security

***AppScan:*** *app security testing and risk management*




## Client Challenge

- Applying patches and resolving application vulnerabilities after apps are Delivered and Deployed is a very costly and time consuming exercise

## Key Capabilities

- Leverage AppScan for vulnerability testing of mobile web apps, web elements (JavaScript, HTML5) of hybrid mobile apps and Android apps
- Vulnerabilities and coding errors can be addressed in software development and testing
- Code vulnerable to known threat models can be identified in testing
- Security designed in vs. bolted on

# Mobile App Security

***WorkLight:*** *Develop, deliver and deploy security-rich mobile apps to streamline business activities while also delivering a rich user experience*


## Client Challenge

- Efficiently and securely, create and run HTML5, hybrid and native mobile apps for a broad set of mobile devices

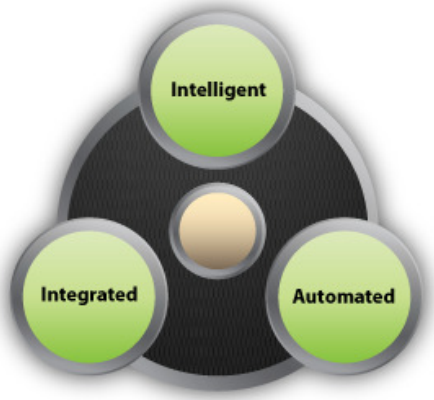
## Key Capabilities

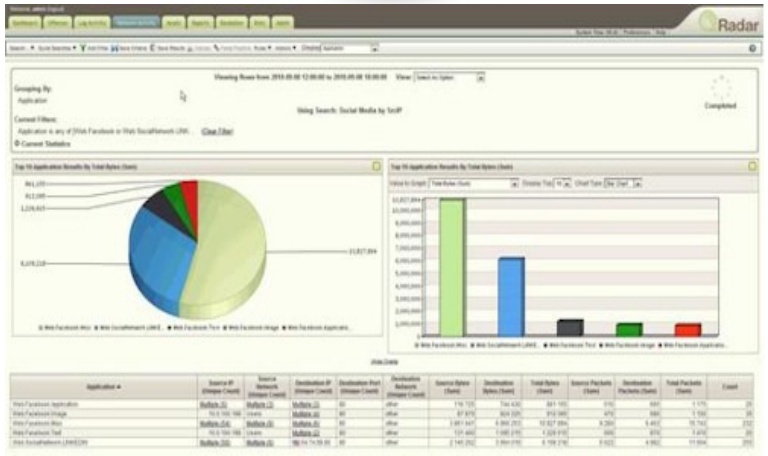
- Integrated secure access to backend application resources
- Secured by design - develop secure mobile apps using corporate best practices, code obfuscation
- Protect mobile app data with encrypted local storage for data, offline user access, app authenticity validation, and enforcement of organizational security policies
- Maximize mobile app performance with analytics, remote disabling of apps

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Mobile Security Intelligence

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




## Client Challenge

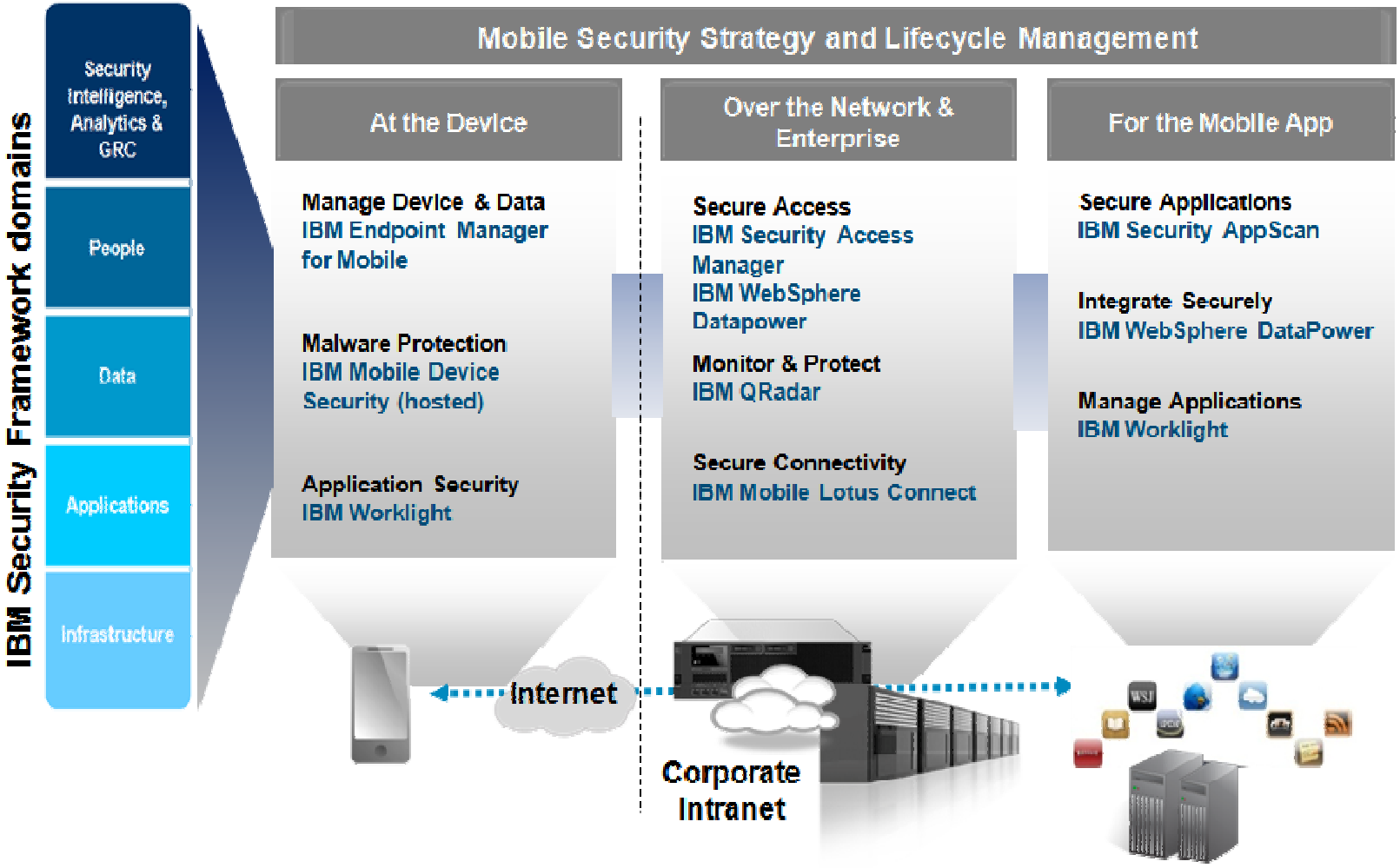
- Visibility of security events across the enterprise, to stay ahead of the threat, show compliance and reduce enterprise risk

## Key Capabilities

- Integrated intelligent actionable platform for
  - Searching
  - Filtering
  - Rule writing
  - Reporting functions
- A single user interface for
  - Log management
  - Risk modeling
  - Vulnerability prioritization
  - Incident detection
  - Impact analysis tasks

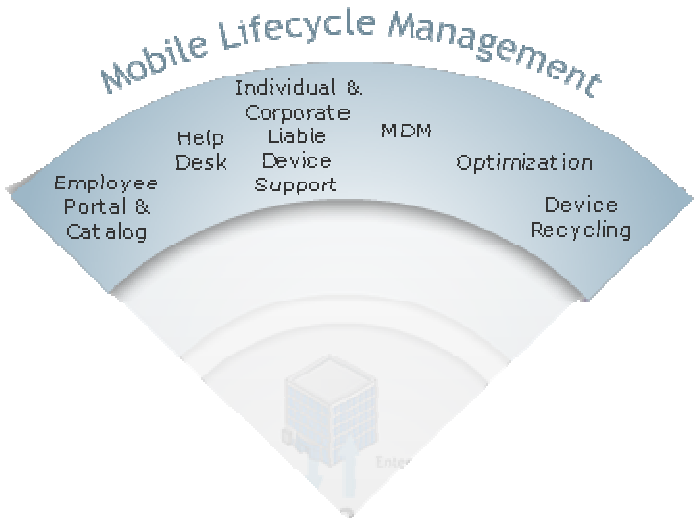
IBMSecuritySymposium
Intelligence | Integration | Expertise

# Securing the Mobile Enterprise with IBM Solutions



# Managing BYOD Costs

***Emptoris Rivermine Telecom Expense Management:*** *Manage, track and optimize mobile spend while ensuring policies are enforced*

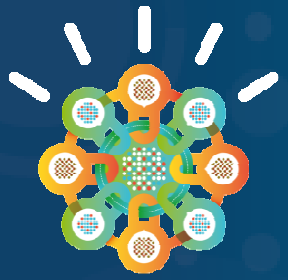



## Client Challenge

- Managing rapid proliferation of corporate and BYOD mobile devices to rein in costs and enforce policy compliance

## Key Capabilities

- Streamline mobile usage management with end-user portal
- Identify most cost effective rate plan for users with rate plan optimization and auditing
- Accelerate device issue resolution and corporate mobile policy enforcement
- Ensure bill accuracy and prevent overpayments with invoice processing
- Optimize contract costs, terms and conditions
- Personal vs. Business Call Tagging for tax legislation compliance
- Mobile Device Recycling for environmental compliance and possible rebates



# CUSTOMER CASE STUDIES

# IBM Case Study

## Extending Corporate Access

*"IBM's BYOD program "really is about supporting employees in the way they want to work. They will find the most appropriate tool to get their job done. I want to make sure I can enable them to do that, but in a way that safeguards the integrity of our business."*

**Jeanette Horan, IBM CIO**

## Customer Needs

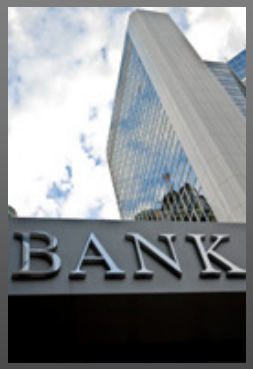
- Support BYOD for a variety of mobile platforms securely for a highly mobile population
- Scale to hundreds of thousands of devices

## Key Features & Outcomes

- 120,000 mobile devices, 80,000 personally owned, supported in months
- Integrated Lotus Traveler, IBM Connections, IBM Sametime, and IBM Endpoint Manager

IBMSecuritySymposium
Intelligence | Integration | Expertise

# Leading European Bank




**European Bank to Deliver Secure Mobile Internet Banking**

*AimArs 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.*

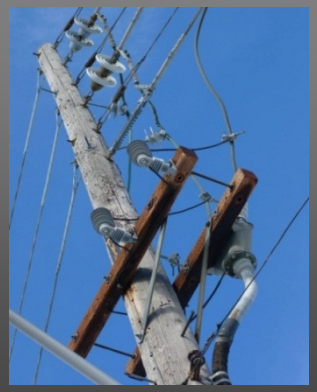
## Customer Needs

- 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

## Key Features & Outcomes

- 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

# Major Utility Company



**Adding Mobile Devices Without Adding Infrastructure**

*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

## Key Features & Outcomes

- Scalability to 250,000 endpoints provides room to grow
- Added mobile devices to existing IEM deployment in days
- Ability to integrate with Maximo, Remedy
- Responsiveness and agility of product and product team





IBMSecuritySymposium

Intelligence | Integration | Expertise