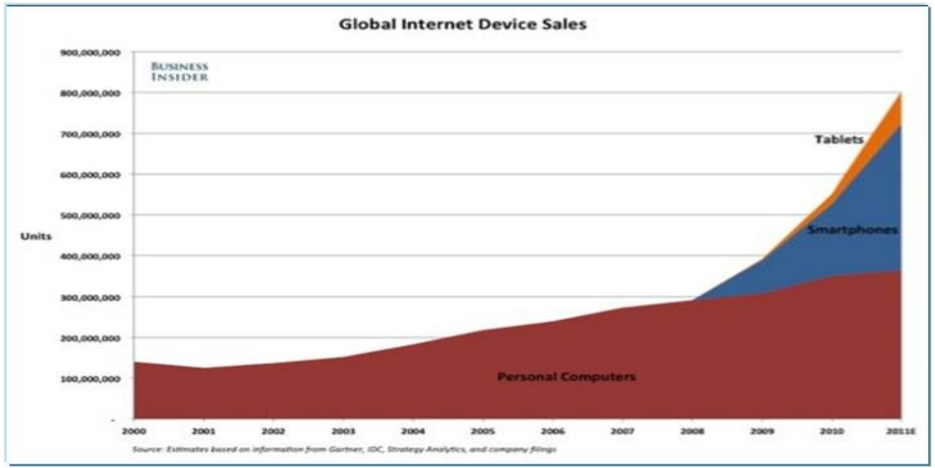
IBM MOBILE MANAGEMENT & SECURITY DELIVERING CONFIDENCE FOR THE MOBILE ENTERPRISE

Vijay Dheap
vdheap@us.ibm.com
Global Product Manager, Master Inventor
IBM Mobile Security Solutions

Pulse2012
Meet the Experts. Optimise your infrastructure.

May 31 – June1
Sheraton on the Park Hotel, Sydney

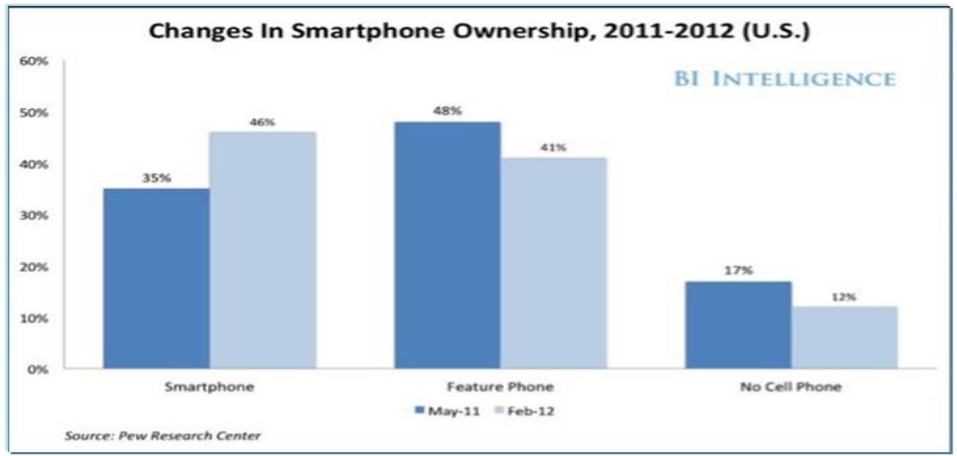
It's a (Smarter) Mobile World



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

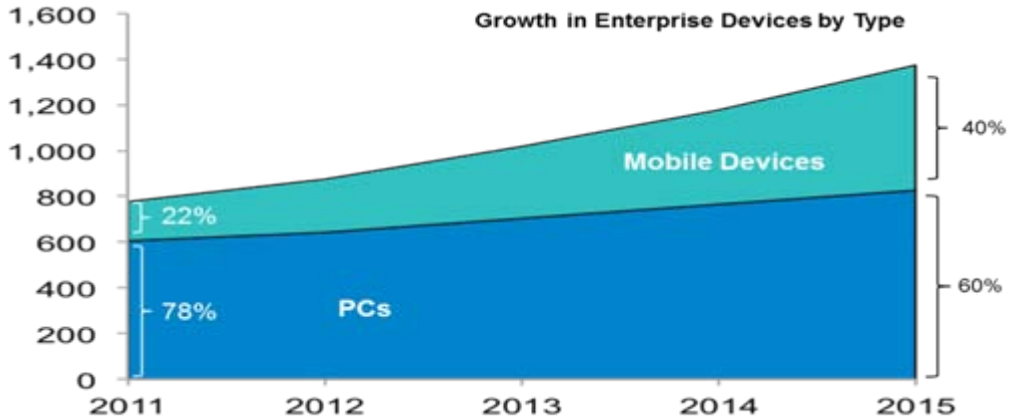
- Business Insider

Users are increasingly adopting smartphones over feature phones – as of this year there is a greater percentage of smartphone users in the US than feature phone users. This trend is accelerating worldwide



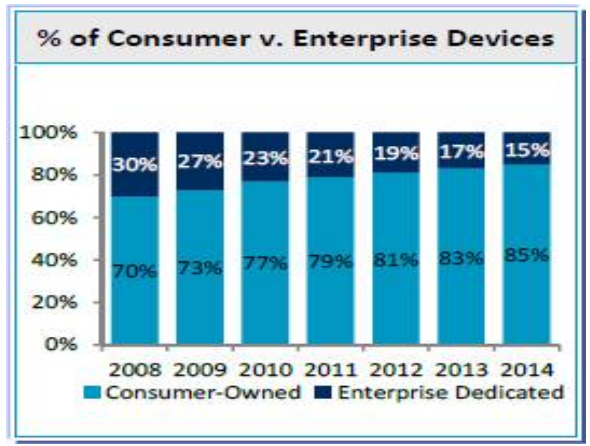
Your Mobile Device is Your…

Users Bringing Smart Mobile Devices to Work



By 2015 40% of Enterprise devices will be mobile devices

- IBM Projection



Bring Your Own Device (BYOD)

The trajectory of adoption is coming from the consumer space into the enterprise.

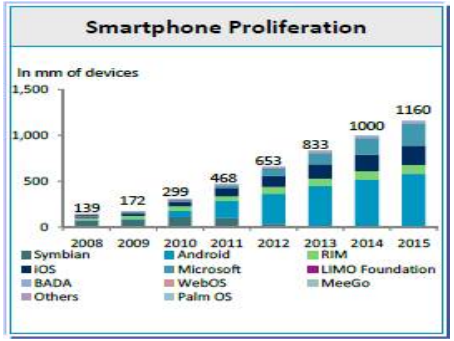
Organizations must enable or become uncompetitive because BYOD can potentially increase employee productivity, develop interactive relationships with customers and enhance collaboration with partners.

Trends in Enterprise Mobility

The need for business agility along with changing employee behaviors will require enterprises to mitigate operational risk associated with mobility

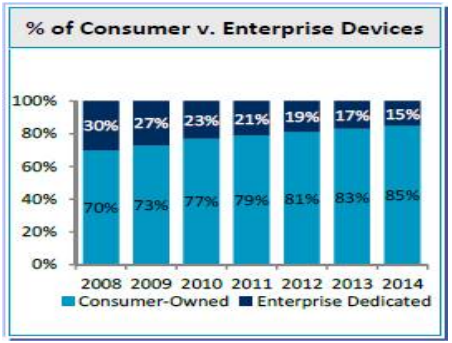
Number and Types of Devices are Evolving

- 1 Billion smart phones and 1.2 Billion Mobile workers by 2014
- Large enterprises expect to triple their smartphone user base by 2015



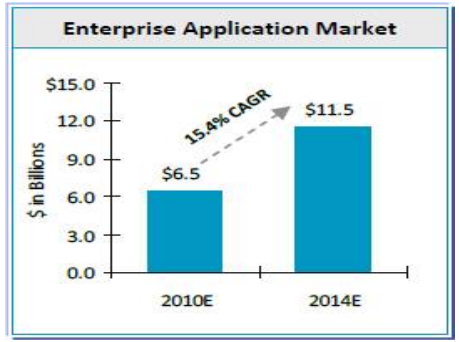
Mobility is Driving the "Consumerization" of IT

- 46% of large enterprises supporting personally-owned devices
- Billions of downloads from App Stores; longer term trend for app deployment



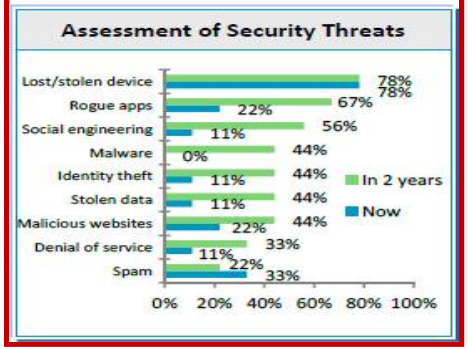
Increasing Demand for Enterprise Applications

- 20%of mobile workers are getting business apps from app stores today
- 50% of organizations plan to deploy mobile apps within 12 months



Security Requirements Becoming More Complex

- Threats from rogue applications and social engineering expected to double by 2013
- 50% of all apps send device info or personal details

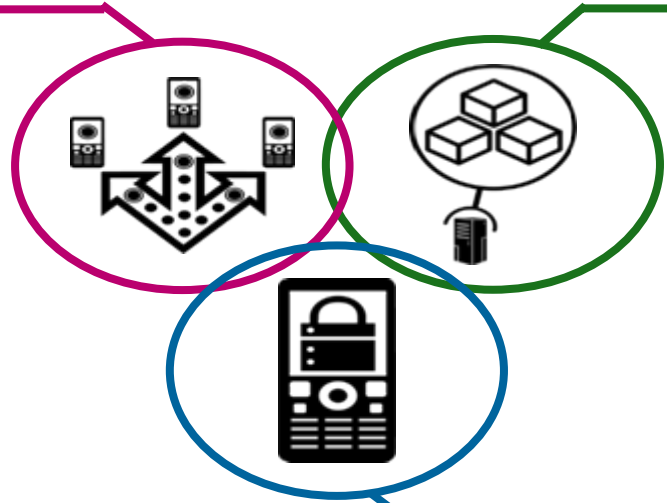


IBM Strategy Addresses Clients' Mobile Initiatives

Extend & Transform

Extend *existing business capabilities to mobile devices*

Transform *the business by creating new opportunities*



Build & Connect

Build *mobile apps*

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

Manage & Secure

Manage *mobile devices and apps*

Secure *my mobile business*

Enterprises Need Visibility & Confidence…

Security and Privacy cited as the number one mobile adoption concern

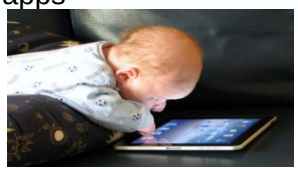
– 2011 IBM Tech Trends Report

The top security threat for 2012 indicated by respondents of the Deloitte 2011 TMT Global Security Survey was Mobile Devices

Uniqueness of Mobile…

Mobile Devices are Shared More Often

Smartphones and tablets are multi-purpose personal devices. Therefore, users share them with friends, and family more often than traditional computing devices – laptops and desktops. Social norms on privacy are different when accessing file-systems vs. mobile apps



Mobile Devices are Used in More Locations

Smartphones and tablets are frequently used in challenging wireless situations that contrast with laptop friendly remote access centers. Laptops are used in a limited number of trusted locations

Mobile Devices prioritize User Experience

Smartphones and tablets place a premium on user experience and any security protocol that diminishes the experiences will not be adopted or will be circumvented. Workstation level security cannot be assumed unless they are dedicated devices

Mobile Devices have multiple personas

Smartphones and tablets may have multiple personas – entertainment device, work tool, etc. Each persona is used in a different context. Users may want to employ a different security model for each persona without affecting another.

Mobile Devices are Diverse

Smartphones and tablets employ a variety of different platforms and have numerous applications aimed at pushing the boundaries of collaboration. The standard interaction paradigms used on laptops and desktops cannot be assumed.

Challenges of Enterprise Mobility

- Adapting to the Bring Your Own Device (BYOD) to Work Trend
  - Device Management & Security
  - Application management

- Achieving Data Separation
  - Privacy
  - Corporate Data protection

- Providing secure access to enterprise applications & data
  - Secure connectivity
  - Identity, Access & Authorization

- Developing Secure Mobile Apps
  - Vulnerability testing

- Designing an Adaptive Security Posture
  - Policy Management
  - Security Intelligence

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

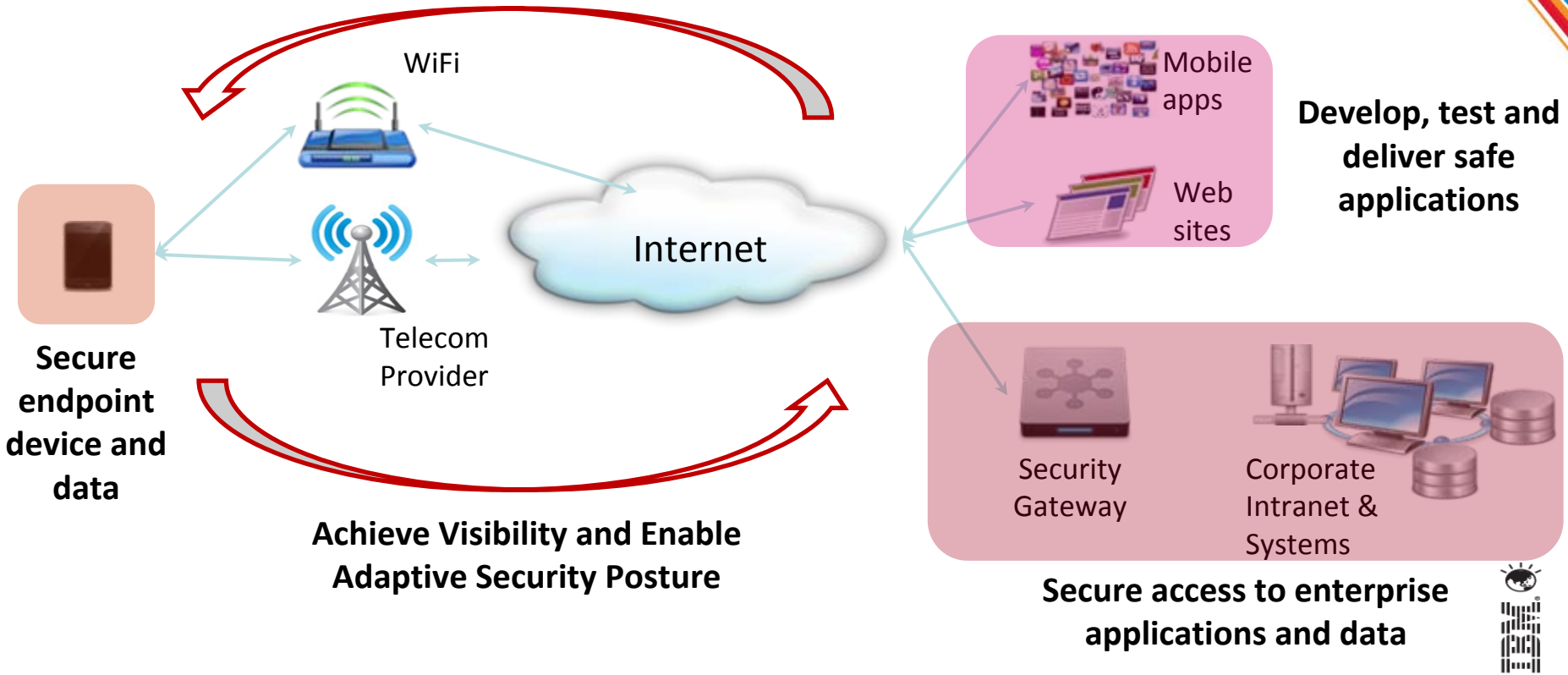
7.Security Decisions Via Untrusted Inputs

8.Side Channel Data Leakage

9.Broken Cryptography

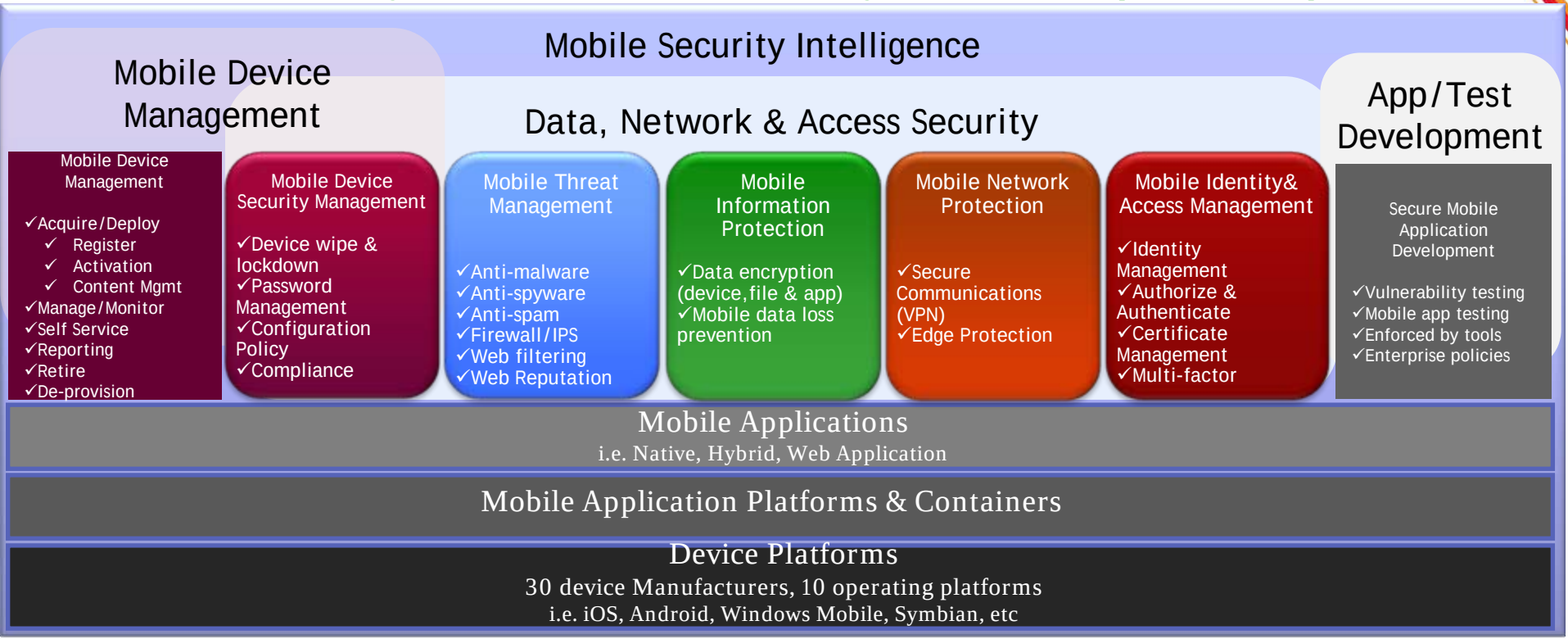
10.Sensitive Information Disclosure

Visualizing Mobile Security

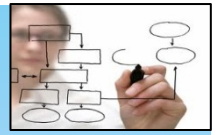


Spectrum of Mobile Security Solutions

Mobile devices are not only computing platforms but also communication devices, hence mobile security is multi-faceted, driven by customers' operational priorities



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

DELIVERING CONFIDENCE

Mobile Endpoint & Data Protection

IBM Hosted Mobile Device Security Management: *Turn-key security for employee-owned and corporate-liable mobile devices*

Client Challenge

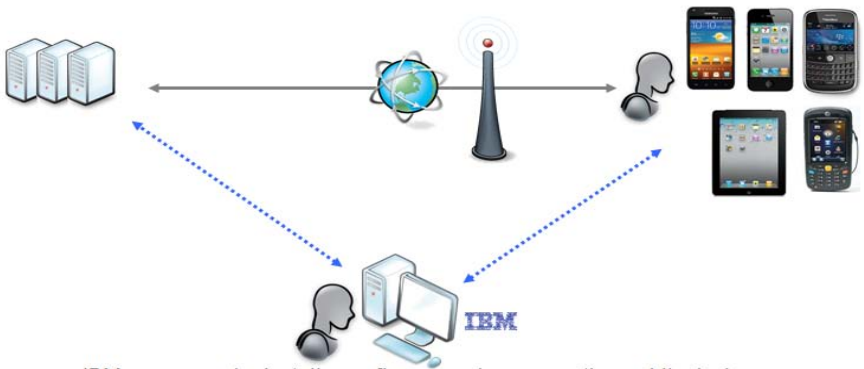
Mobile threat protection without in-house skills or technology to own or manage

Key Capabilities

- Mobile malware prevention (spyware, viruses, etc.)
- Simple, cloud-based delivery
- Policy compliance monitoring
- Device management and security for Apple, Android, BlackBerry, Windows Mobile, and Symbian devices
- End-user portal to locate/lock/wipe a lost or stolen device

Device Lifecycle

IBM Mobile Enterprise Services for Managed Mobility: *Managed service for iOS, Blackberry, Android, and Windows Mobile smartphones, tablets, and ruggedized devices*



IBM recommends, installs, configures and manages the mobile devices and mobile infrastructure on an ongoing basis

Client Challenge

Delivering enterprise mobile services to increasing numbers of mobile workers, including BYOD, at less cost than delivering in house

Key Capabilities

- Procurement, staging and kitting
- Mobile device management
- Mobile application management
- Mobile messaging (e.g. Lotus Domino, Microsoft Exchange)
- Help desk services
- Negotiated discounts with leading mobile hardware and software vendors
- Over 15 years world-wide experience

IBM Integrated Mobile Software Security Solutions

Achieve Visibility & Enable Adaptive Security Posture

IBM QRadar
System-wide Mobile Security Awareness
- Risk Assessment
- Threat Detection

Secure Data & the Device

IBM WorkLight
Runtime for safe mobile apps
- Encrypted data cache
- App validation

IBM Endpoint Manager for Mobile
Configure, Provision, Monitor
- Set appropriate security policies
- Enable endpoint access
- Ensure compliance

Protect Access to Enterprise Apps & Data

IBM Security Access Manager for Mobile
Authenticate & Authorize users and devices
- Standards Support: OAuth, SAML, OpenID
- Single Sign-On & Identity Mediation

IBM Mobile Connect
Secure Connectivity
- App level VPN

Build & Run Safe Mobile Apps

IBM WorkLight
Develop safe mobile apps
- Direct Updates

IBM AppScan for Mobile
Vulnerability testing
- Dynamic & Static analysis of Hybrid and Mobile web apps

IBM DataPower
Protect enterprise applications
- XML security & message protection
- Protocol Transformation & Mediation

Internet

Deliver and Manage Safe Mobile Apps

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

Client Challenge

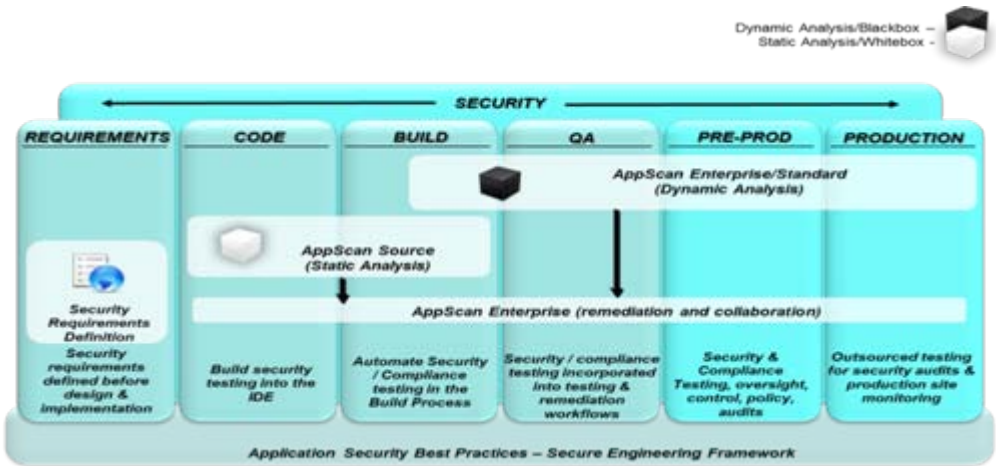
Efficiently and securely, create and run HTML5, hybrid and native mobile apps for a broad set of mobile devices

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

Deliver Security-Rich Apps

AppScan: *application security testing and risk management*



Client Challenge

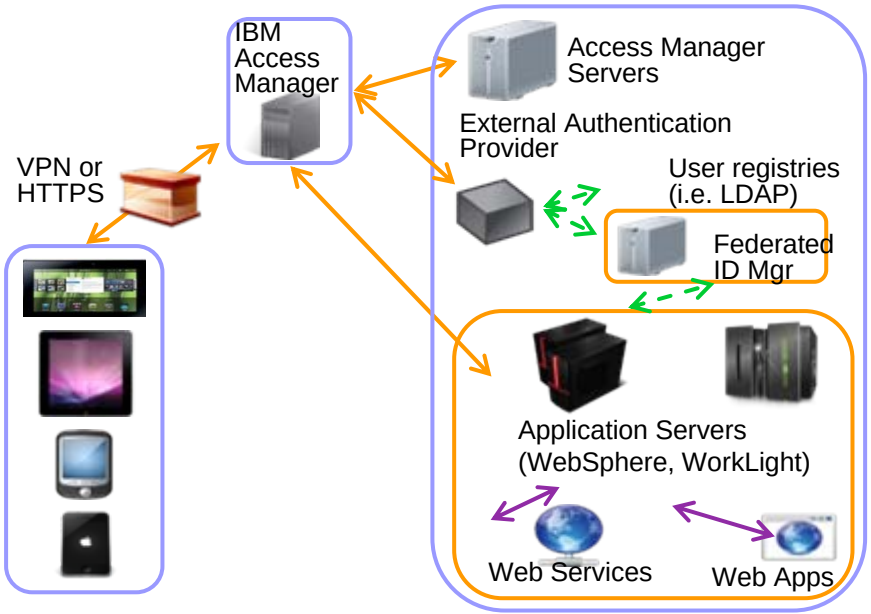
Applying patches and resolving application vulnerabilities after apps are Delivered and Deployed is a very costly and time consuming exercise

Key Capabilities

- Leverage AppScan for vulnerability testing of mobile web apps and web elements (JavaScript, HTML5) of hybrid mobile 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

User Management & Access

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

Security-rich Mobile Connectivity

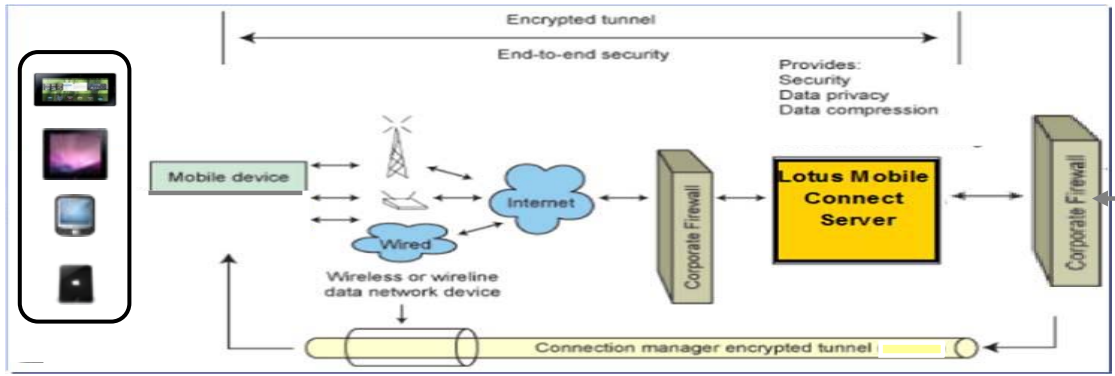
IBM Lotus® Mobile Connect: *Provides features that help deliver a security-rich connection to enterprise resources from mobile devices.*

Client Challenge

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

Key Capabilities

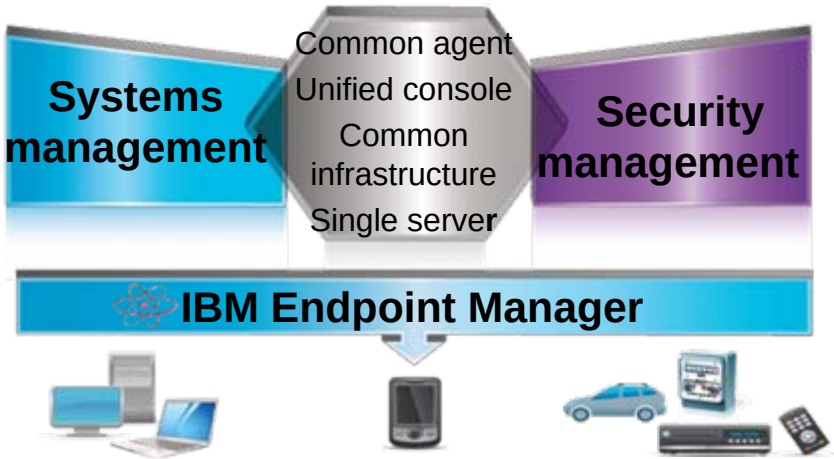
- Clientless app-level Virtual Public Network (VPN) with a SSL-secured tunnel to specific HTTP application servers
- Strong authentication and encryption of data in transit



Device Lifecycle, Data Protection

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



Desktop / laptop / server endpoint

Mobile endpoint

Purpose-specific endpoint

Client Challenge

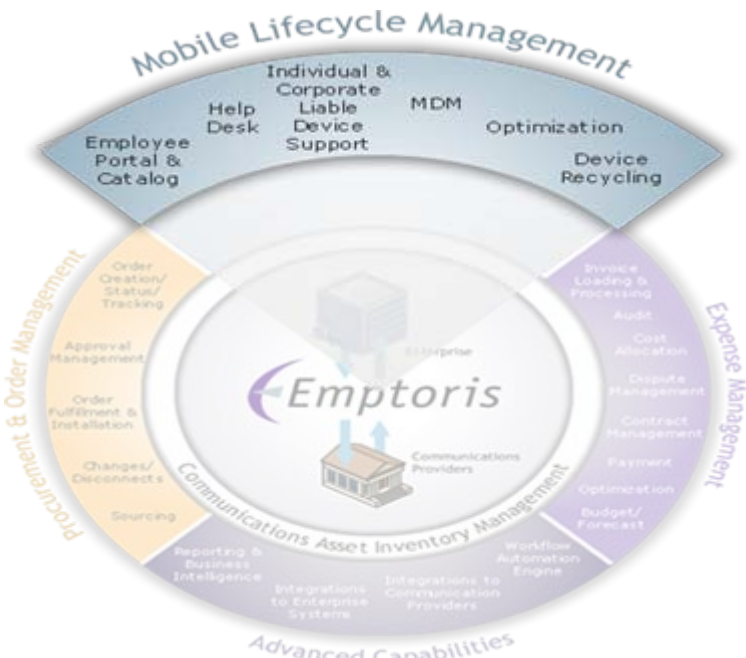
Managing and securing enterprise and BYOD mobile devices without additional resources

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

Effectively Manage Mobile Costs

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



Client Challenge

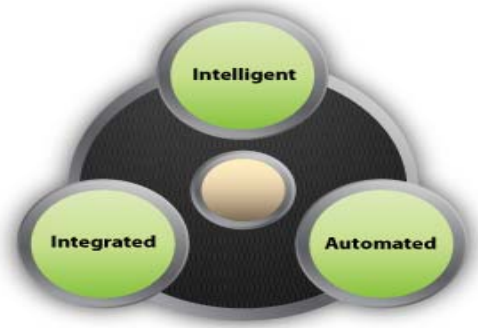
Managing rapid proliferation of corporate and BYOD mobile devices to rein in costs and enforce policy compliance

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

Deliver Visibility & an Adaptive Security Posture

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

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

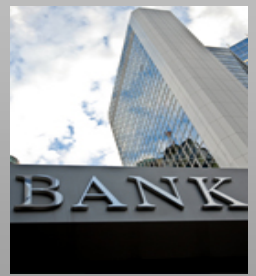
Customer Needs

- 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

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

Electricity Provider

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

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.