

Pulse Comes to You 2012

Business without **LIMITS**

21 Aug 2012 | Thailand

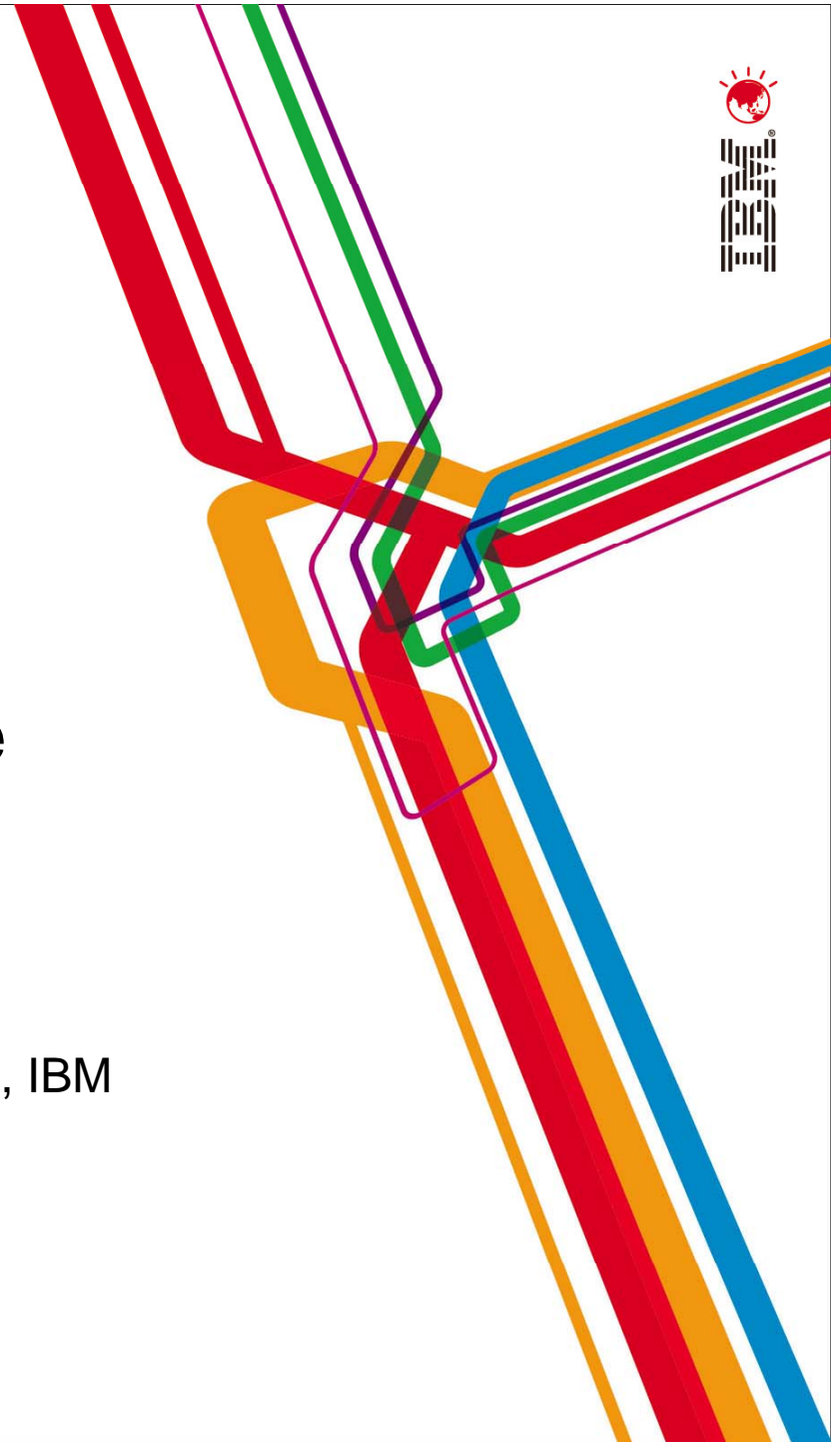


Mobile Security:

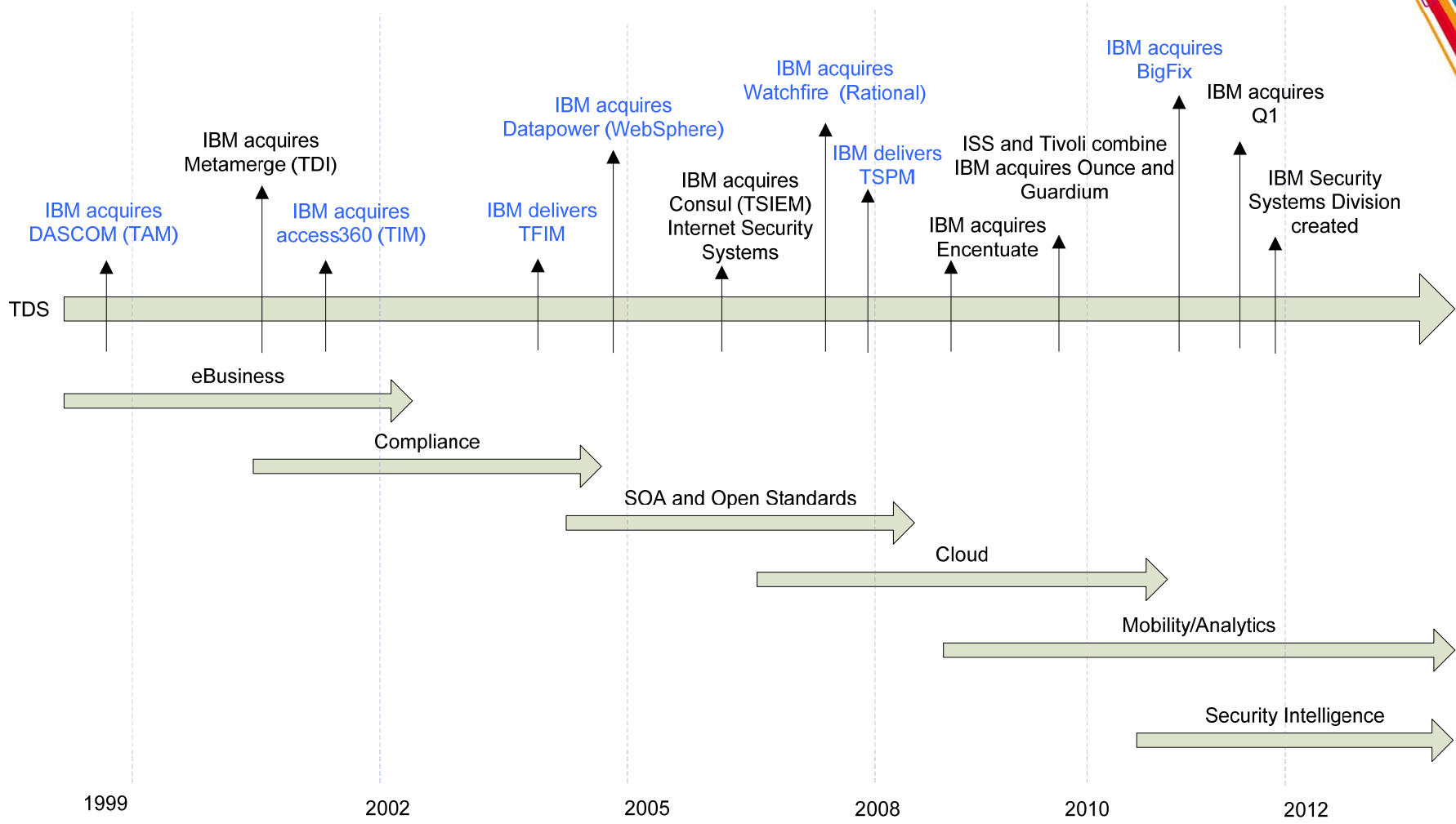
Security Implications from the
Consumerization of IT

Chris Hockings

Development Lab Manager, Security Systems, IBM
Software Group, Australia



IBM Security Systems portfolio growth

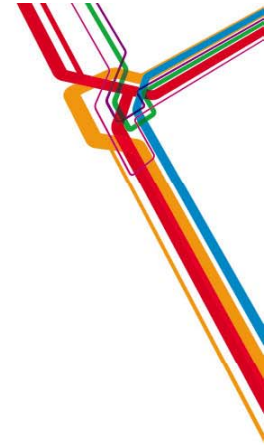


Blue text indicates products that have a direct functional impact on mobile use cases

Pulse Comes to You 2012

Business without **LIMITS**

Mobile devices provide opportunities for consolidation



By nature, devices bring many functional benefits that can be exploited in mobile use cases

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



Pulse Comes to You 2012

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



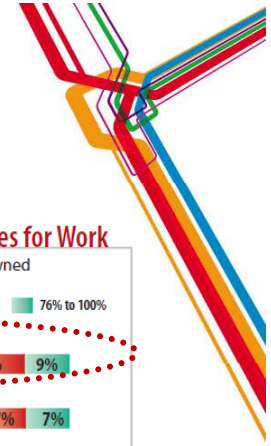
Mobile devices prioritise the user

- 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

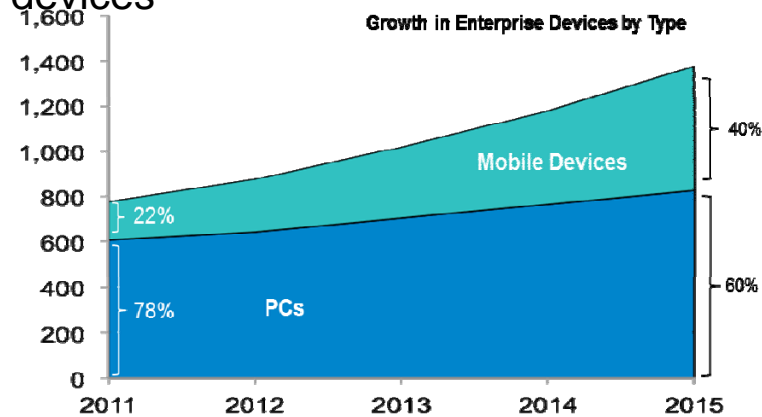


Business without **LIMITS**

Employees Bringing Smart Devices to Work...

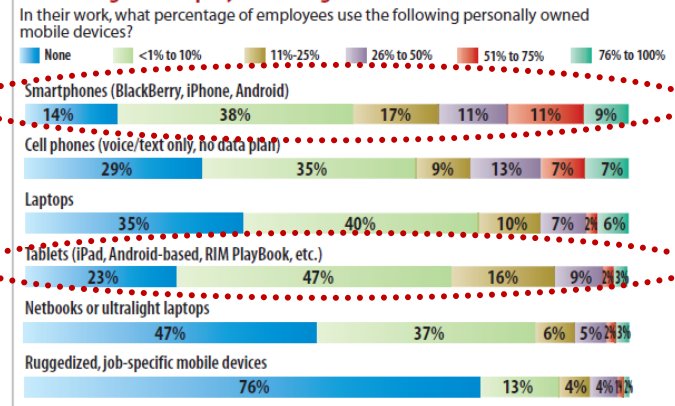


By 2015 40% of Enterprise devices will be mobile devices



- IBM Projection

Percentage of Employees Using Personal Mobile Devices for Work



Data: InformationWeek 2012 Mobile Security Survey of 322 business technology professionals, March 2012 R4720512/6

Bring Your Own Device (BYOD)

By 2015 40% of Enterprise devices will be mobile devices

Within a few years, over 50% of all employees will be generation Y -- IBM Projection

Research from Toyota USA shows gen-Y prefer new devices and gaming consoles purchase over new vehicle purchase -- ZDNet

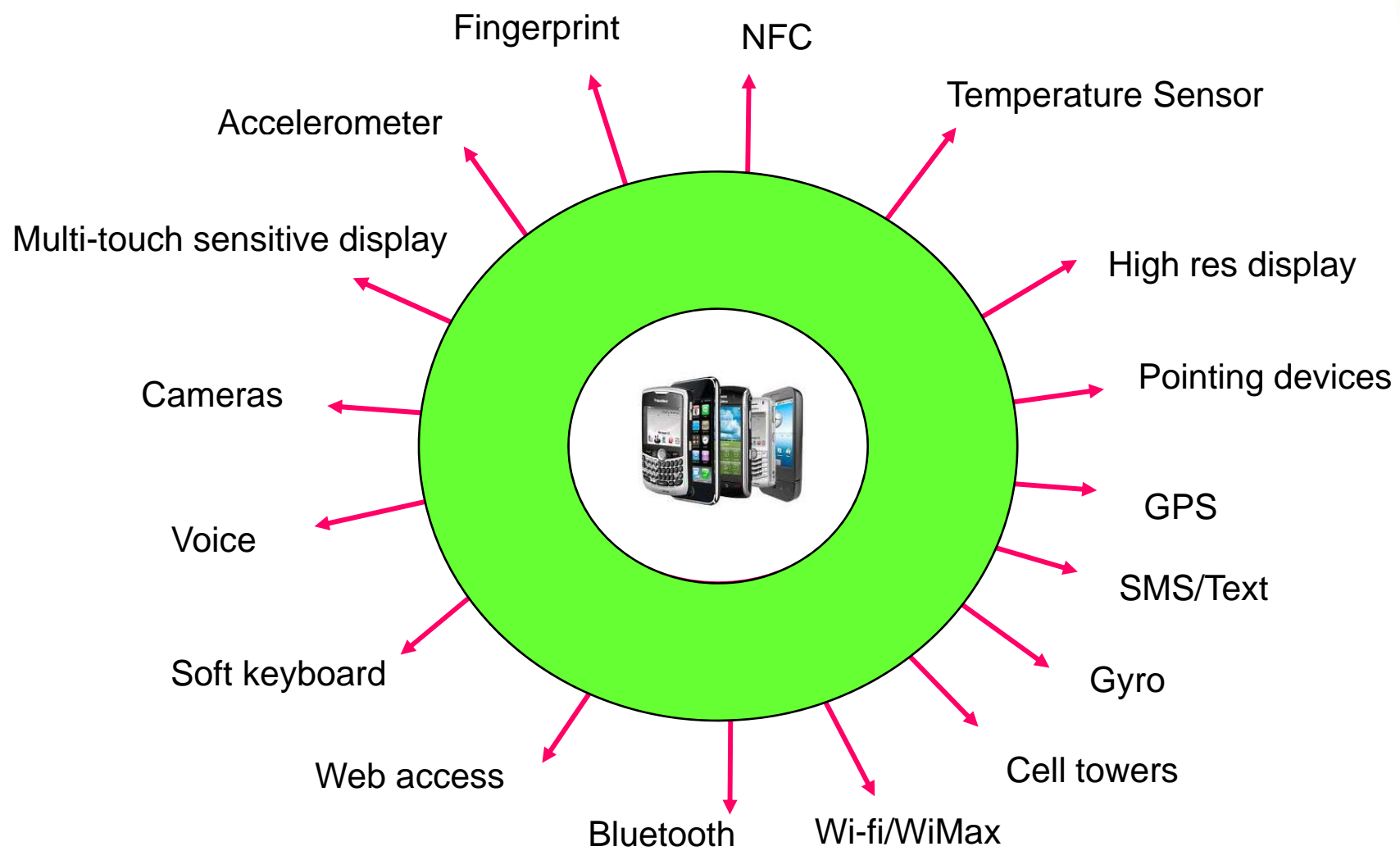
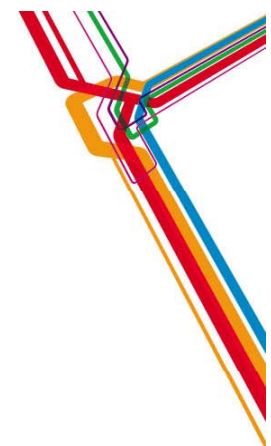
Pulse Comes to You 2012

More than 85% of Asia Pacific respondents already engage in the practice of BYOD, higher than the global figure of 74%.

47% of Asia Pacific were willing to contravene a corporate policy banning the use of personally-owned devices for work purposes, compared to the global figure of 42%.

Business without LIMITS
Forrester Survey

Mobility also brings many opportunities



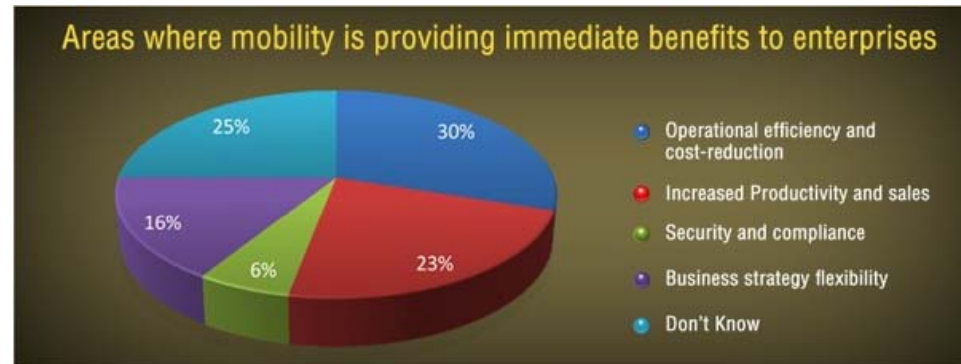
Pulse Comes to You 2012

Business without **LIMITS**

Enterprise Mobility Brings Business Value



Enterprise Mobility brings tangible business benefit and can offer organizations a competitive advantage.



Achieving Operational Excellence

- A manufacturing company wanted to have greater visibility across its workflows
- Using a mobile solution deployed to devices in the hands of employees, factory could track flow of thousands of parts in real-time

Extending the Reach of Knowledge

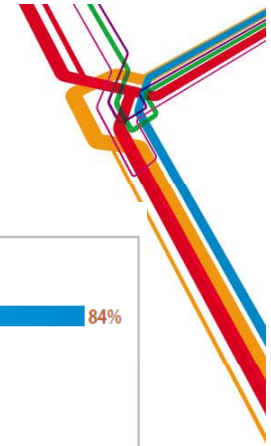
- Leverage the mobile platform to extend the access of knowledge to employees, constituents and other stakeholders
- A mobile solution was deployed that provided farmers fertilizer guidelines for their crops and other actionable data such as market prices



Pulse Comes to You 2012

Business without **LIMITS**

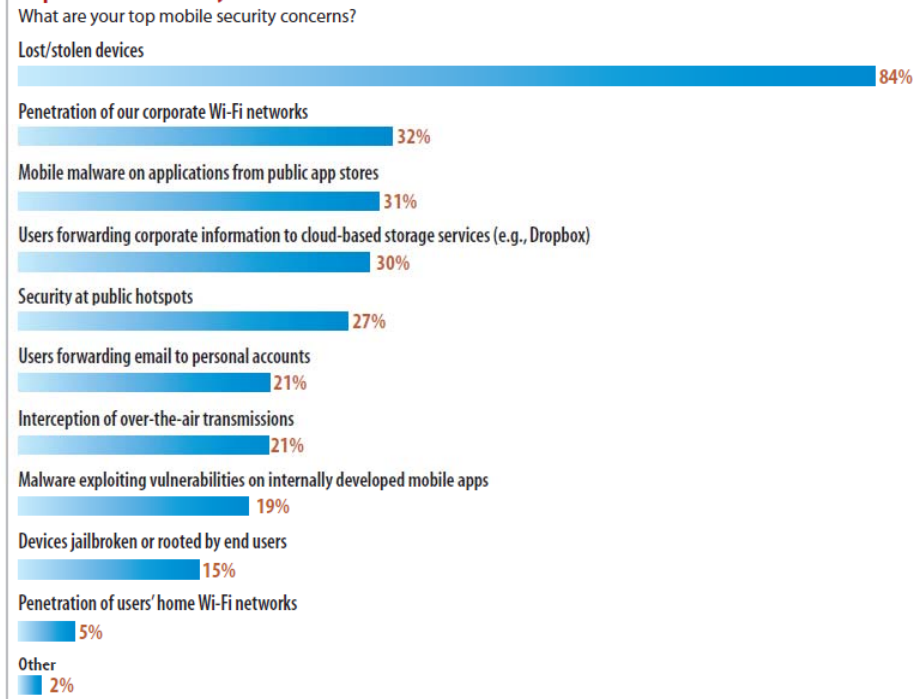
Mobile Security Risks, Concerns & Emerging Threats



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

Top Mobile Security Concerns



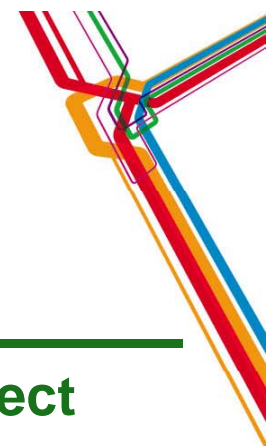
Note: Three responses allowed
Data: InformationWeek 2012 Mobile Security Survey of 322 business technology professionals, March 2012

R4720512/1

Emerging Mobile Threats

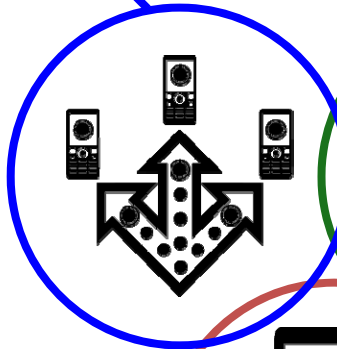
Social Engineering	Mobile Borne DoS Attacks
Rogue Apps	Identity Theft
Malicious Websites	Man-in-the-Middle Attacks

IBM Strategy Addresses Client Mobile Initiatives



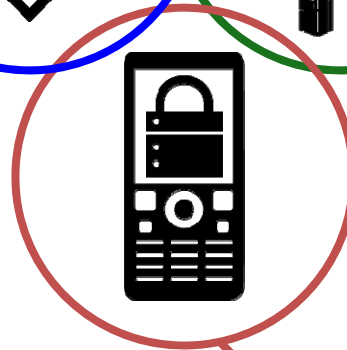
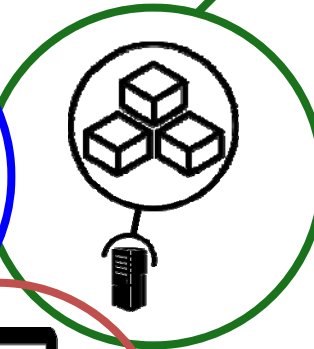
Extend & Transform

Extend existing business capabilities to mobile devices
Transform the business by creating new opportunities



Build & Connect

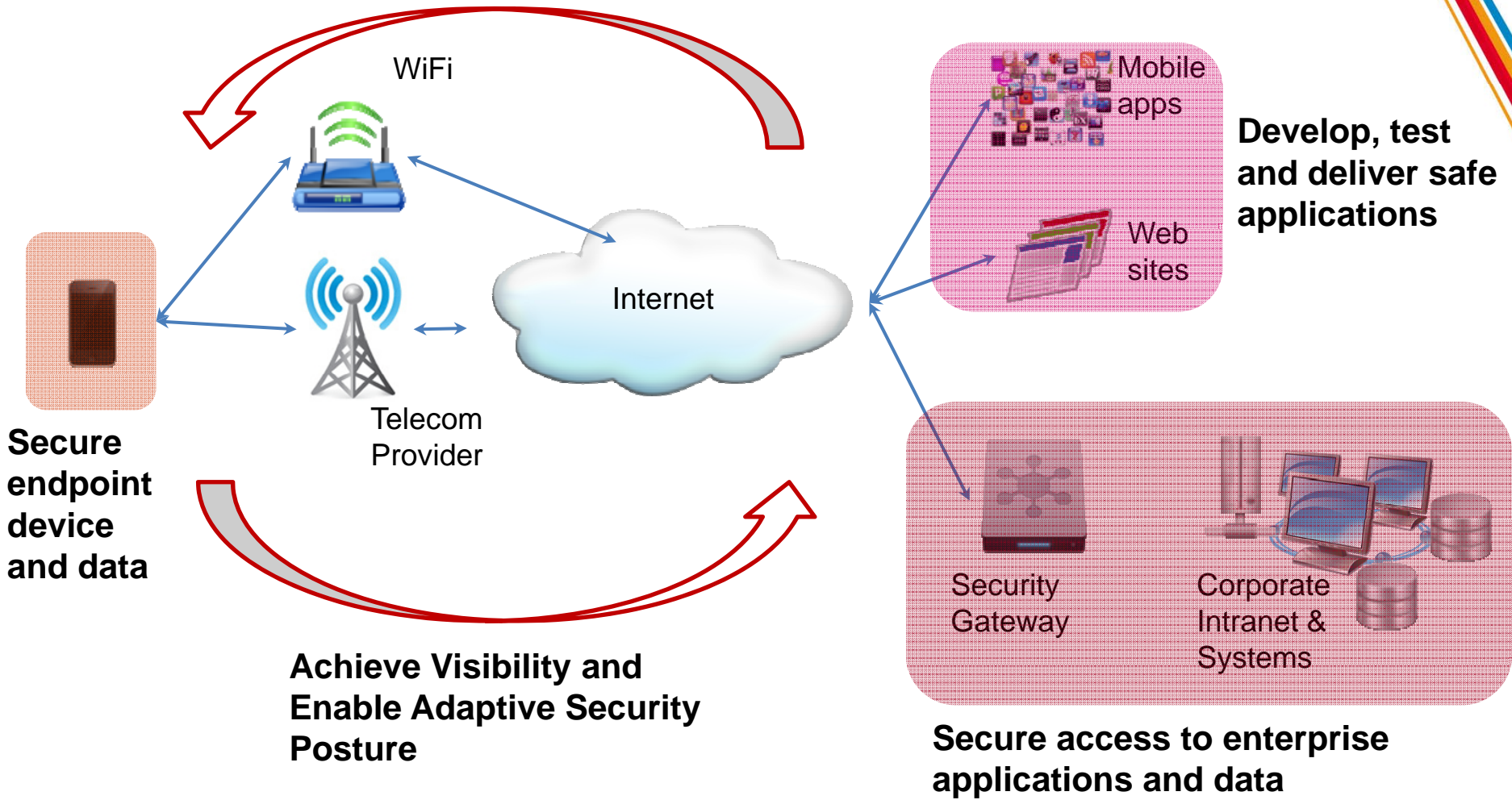
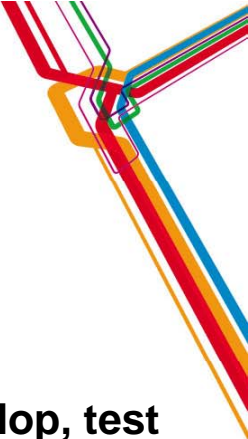
Build mobile applications
Connect to, and *run* backend systems in support of mobile



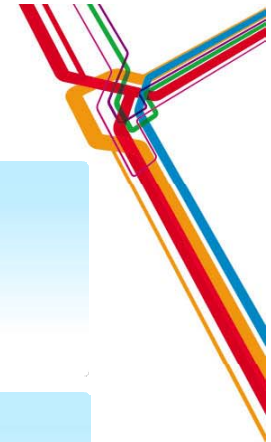
Manage & Secure

Manage mobile devices and applications
Secure my mobile business

Visualizing Mobile Security



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

Mobility @IBM today

- Security and safeguarding IBM data is paramount
 - Very conservative approach
 - Constantly evaluating devices, operating systems and applications for suitability
- IBM supports BYOD for employees
 - Work is no longer a “place you go to”
 - Potential to drive productivity
- Internal Appstore called WhirlWind
 - > 500 apps
 - More than 40k downloads
 - E.g. MyMobileHub delivers file sharing
- Lotus Traveller
 - Application allowing mobile access to email, calendar, contacts
 - 30% of employees currently enabled, 20% active
 - 120,000 mobile devices, 80,000 personally owned, supported in months
 - 2/3rds BYOD, 1/3rd IBM-supplied
 - Best practices from pilot now available as a client service via managed services



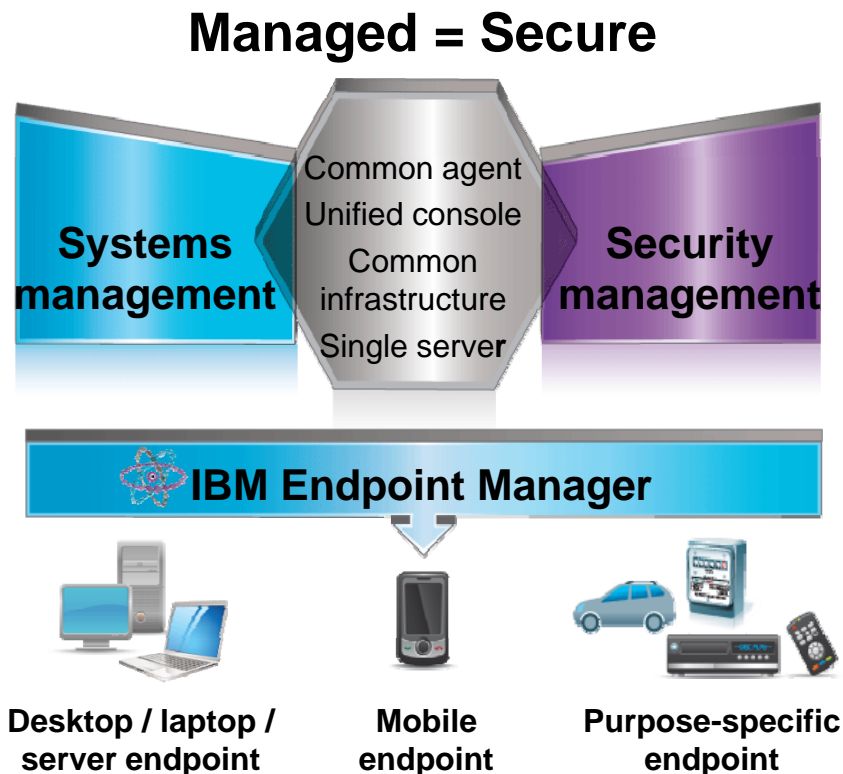


DELIVERING CONFIDENCE

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



Client Challenge

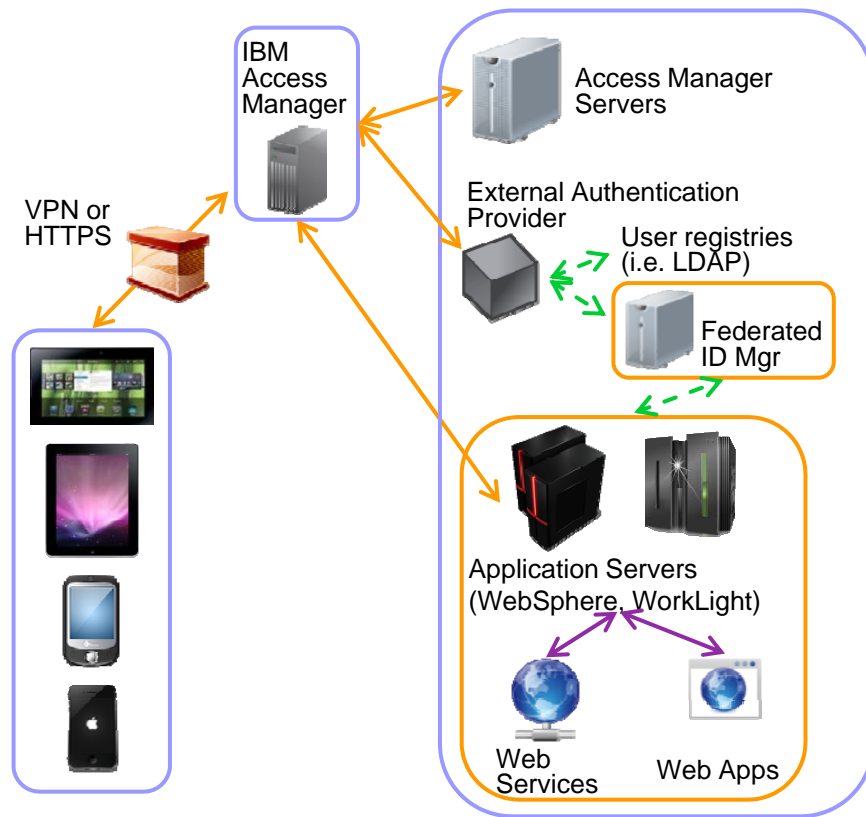
Managing and securing enterprise and BYOD mobile devices without additional resources

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

Mobile Access Security

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



Client Challenge

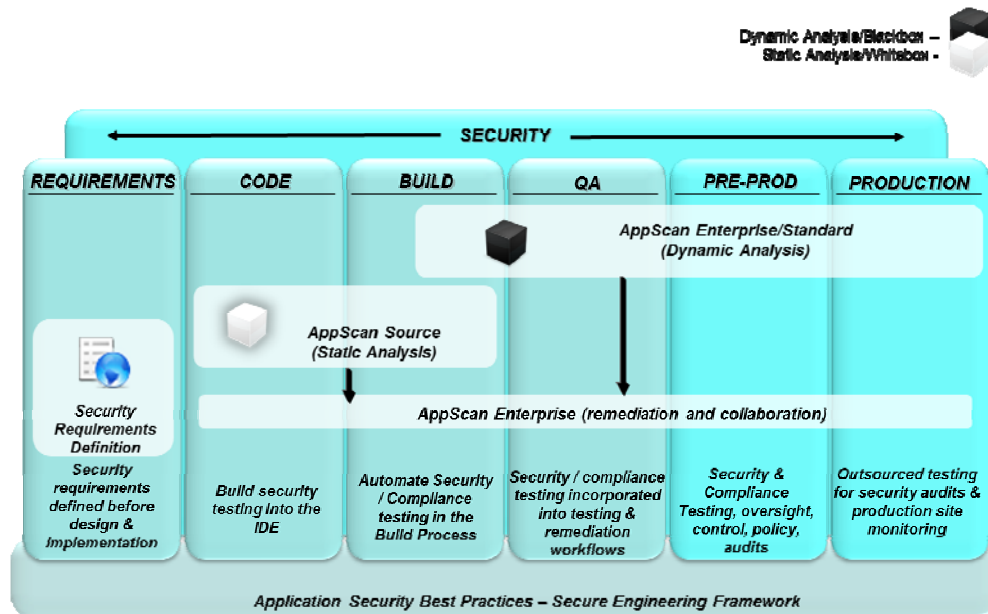
Ensuring users and devices are authorized to access enterprise resources from that specific device.

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

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

Pulse Comes to You 2012

Business without **LIMITS**

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

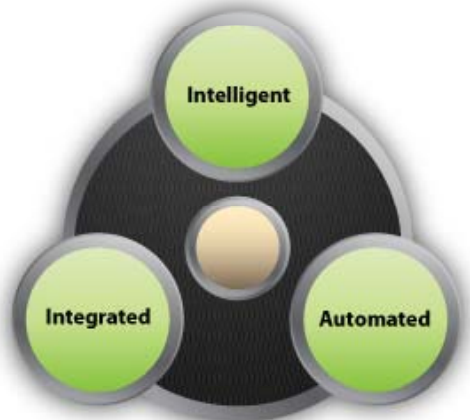
- Integrated secure access to backend application resources
- Secured by design - develop secure mobile apps using corporate best practices, code obfuscation
- Protect mobile app data with encrypted local storage for data, offline user access, app authenticity validation, and enforcement of organizational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

Pulse Comes to You 2012

Business without **LIMITS**

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



Pulse Comes to You 2012

Business without **LIMITS**



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

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

Pulse Comes to You 2012

Business without **LIMITS**



Thank You

