Mobile Security Management

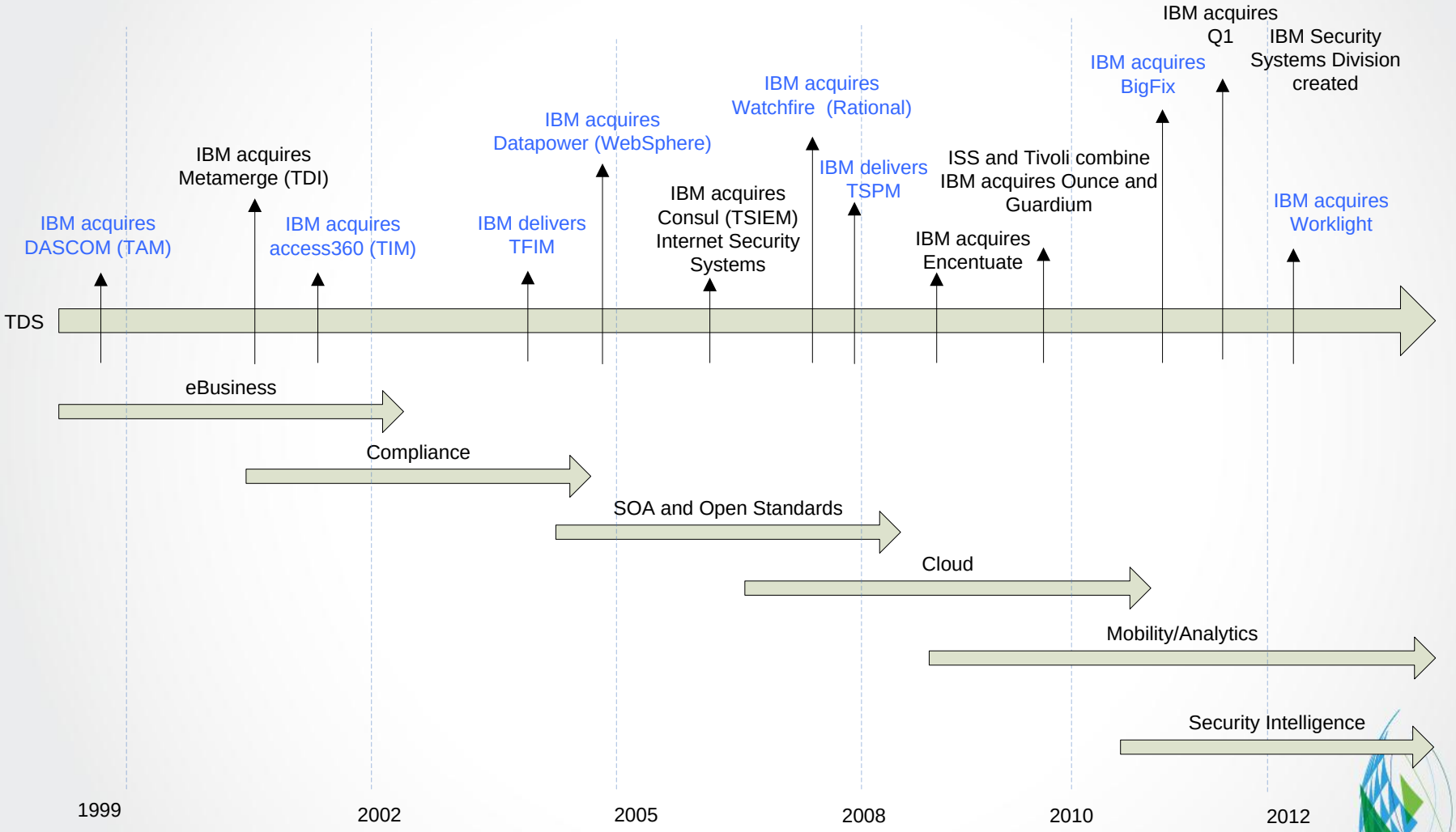
Chris Hockings
E: hockings@au1.ibm.com
T: @chockings

09/04/2102

Where am I from? (IBM Security Lab Gold Coast)

- **Background**
  - 1999 acquisition of DASCOM
  - Founded in 1996
  - Strong links to Queensland universities
- **Profile**
  - 90+ technical staff
  - Design, development, test, project management, documentation, support
  - World class security expertise
  - Close to Asia Pacific Customers
- **Excellent Talent in Region**
  - Good University Relationships
  - Universities have security focus
  - Ability to hire top graduates
  - Many security specialists in region

IBM Security Systems portfolio growth

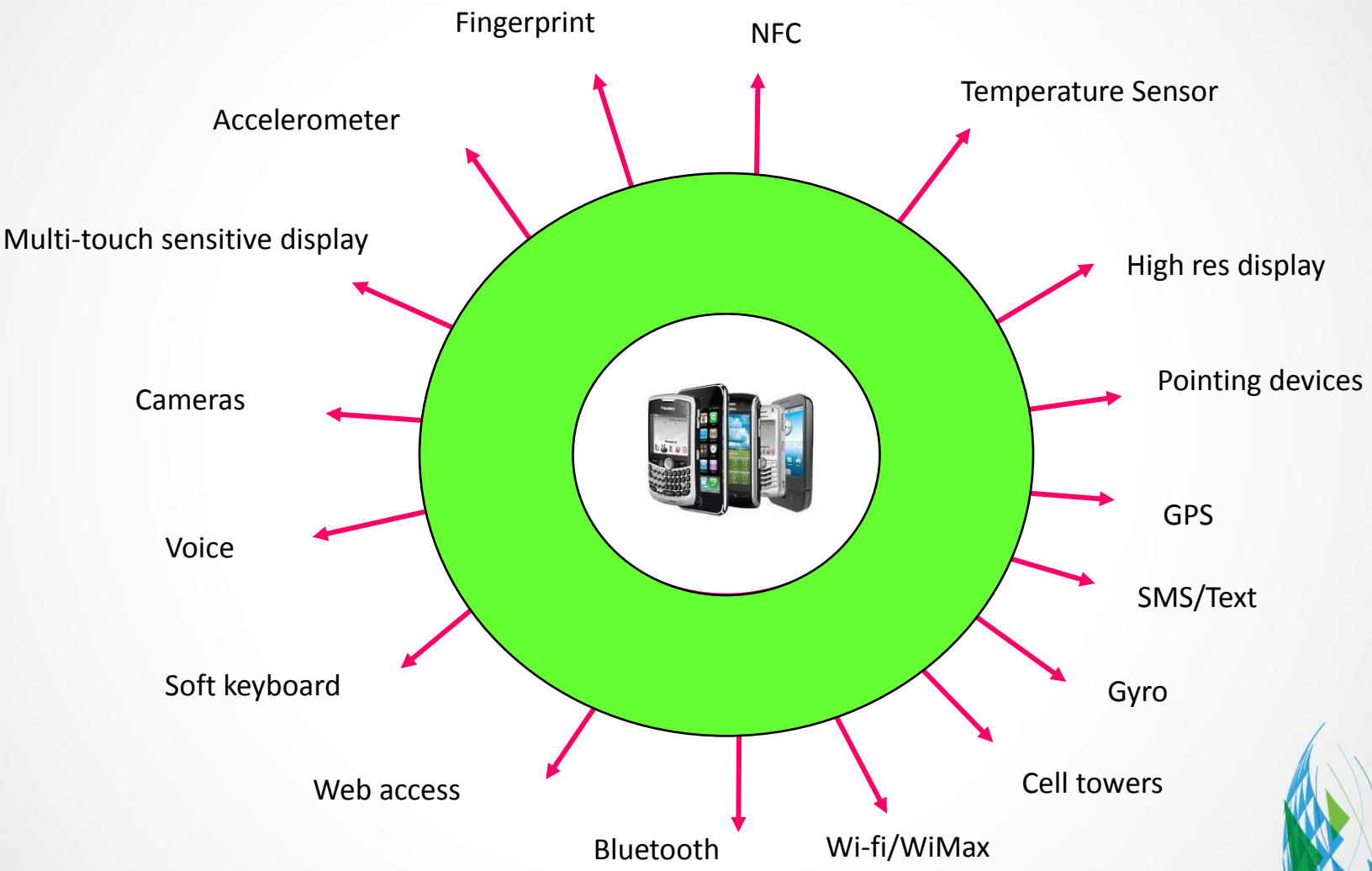


Blue text indicates products that have a direct functional impact on mobile use cases

Mobile devices provide opportunity for consolidation

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

Devices do present an opportunity for to reduce risk



People are bringing these Mobile Devices to Work

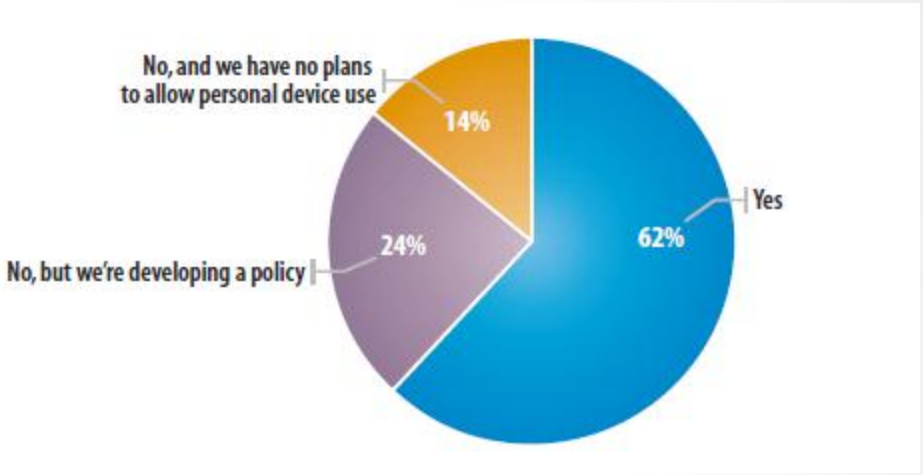
By 2015 40% of Enterprise devices will be mobile devices

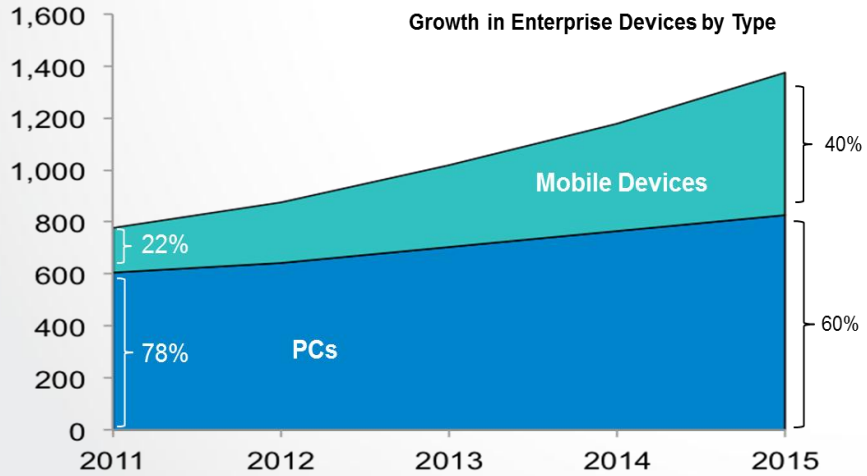
Within a few years, over 50% of all employees will be generation Y

IBM Projection

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

ZDNet





Many organizations don't have a plan to allow mobile devices into the workplace

- Information Week

Devices follow unique usage scenarios

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

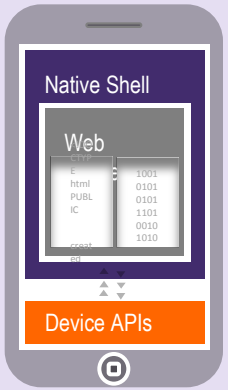
- A single location could offer public, private, and cell connections
- Anywhere, anytime
- Increasing reliance on enterprise WiFi
- Devices more likely to be lost/stolen

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

App delivery means a shift in development paradigms

Web	Mobile Web	Hybrid Mobile	Native
▪ HTML, JavaScript, CSS ▪ Accessed from a mobile web browser ▪ No device-specific capabilities	▪ HTML, JavaScript, CSS ▪ Accessed from a mobile web browser; mobile-optimized UI ▪ Limited access to lower-level device capabilities	▪ HTML, JavaScript, CSS, with optional native code ▪ Installed and run like a native mobile app; mobile-optimized UI ▪ Access to lower-level device capabilities	▪ Native code ▪ Access to full set of lower-level device capabilities



Richness of Mobile Presentation / Services

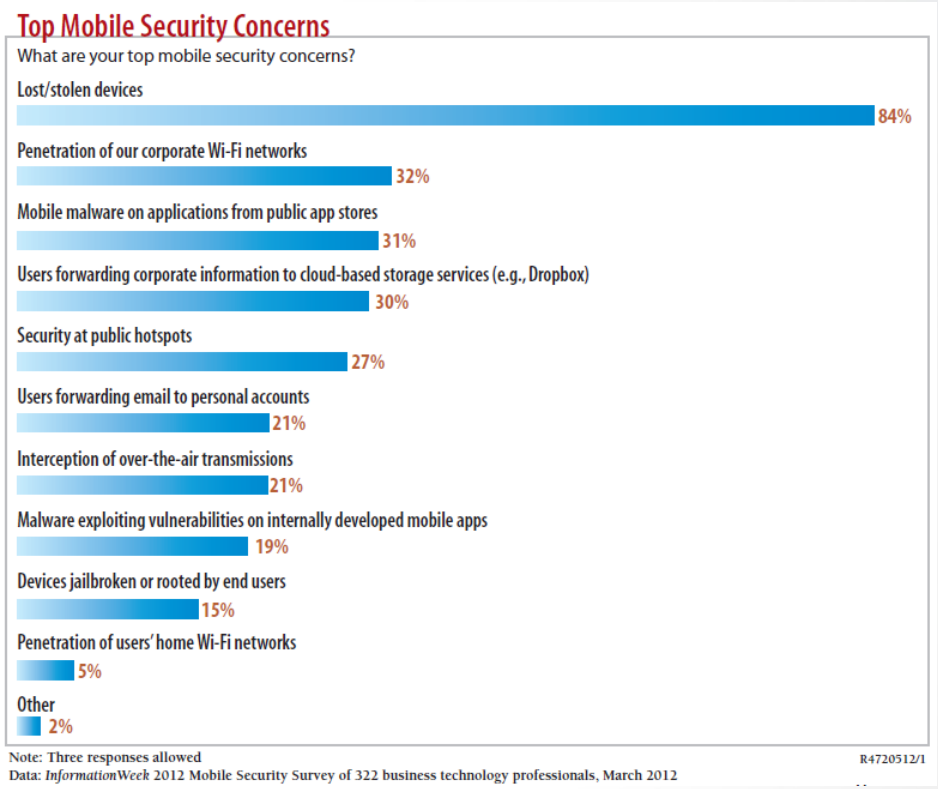
Portability (cross-device reuse)

Maintenance Cost (TCO)

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

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

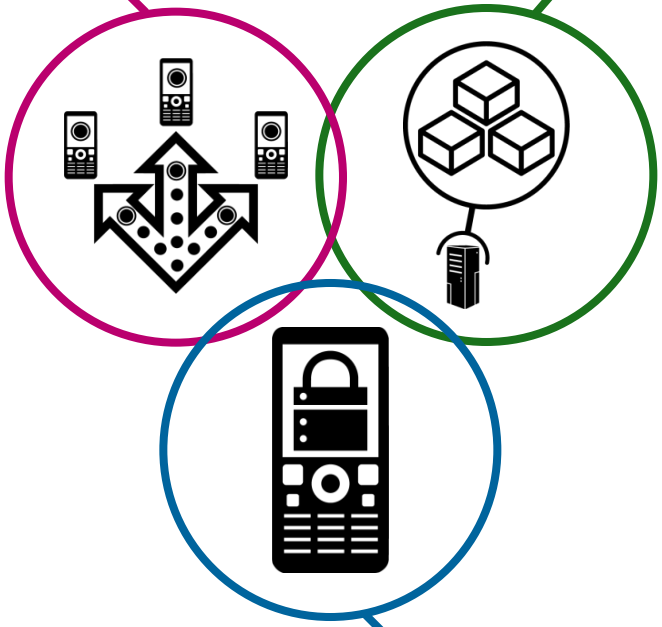
IBM Strategy point of view on Mobile Security

Aspects to consider in any Mobile Security Strategy

Extend & Transform

Extend *existing business capabilities to mobile devices*

Transform *the business by creating new opportunities*



Build & Connect

Build *mobile apps*

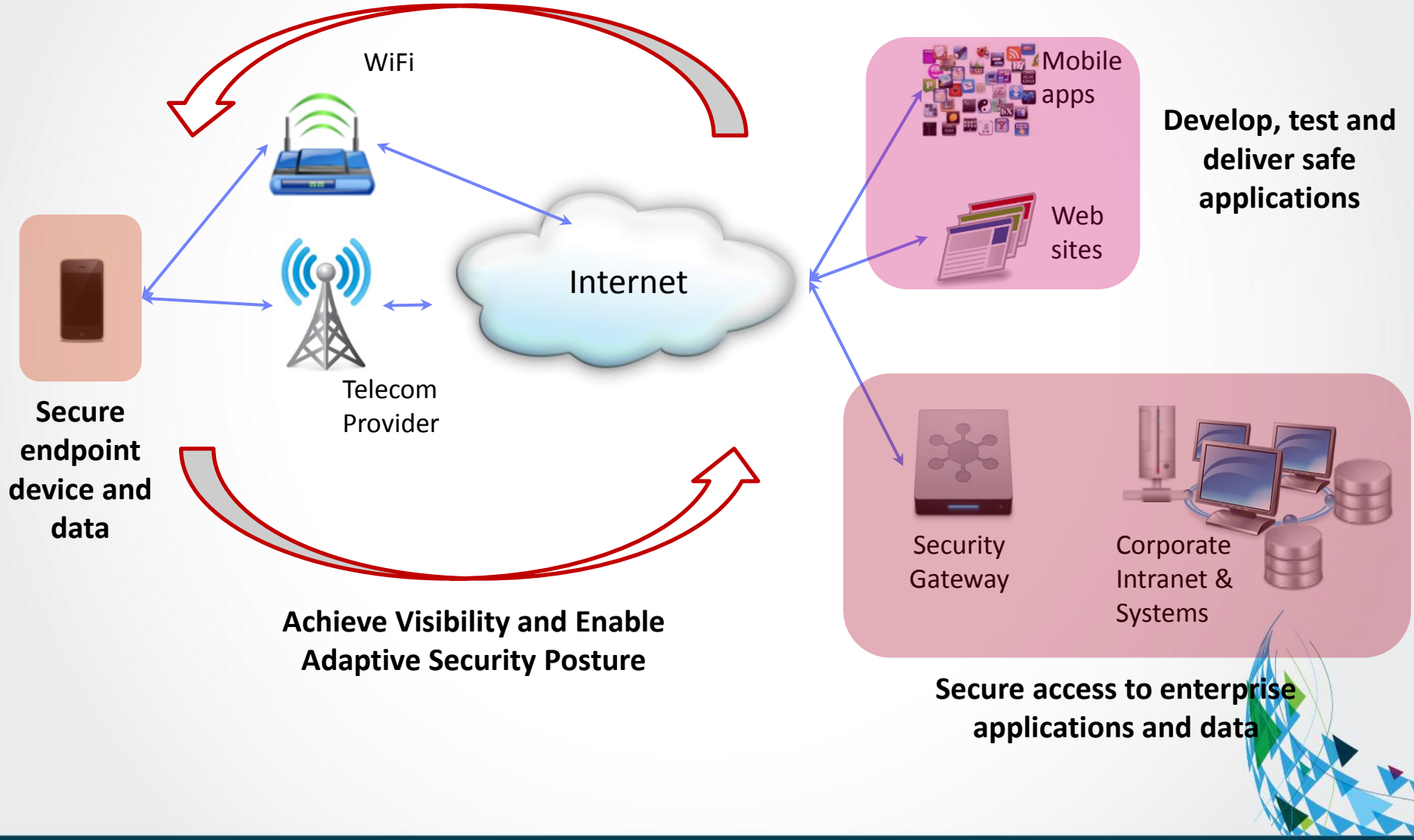
Connect *to, and* ***run*** *backend systems in support of mobile*

Manage & Secure

Manage *mobile devices and apps*

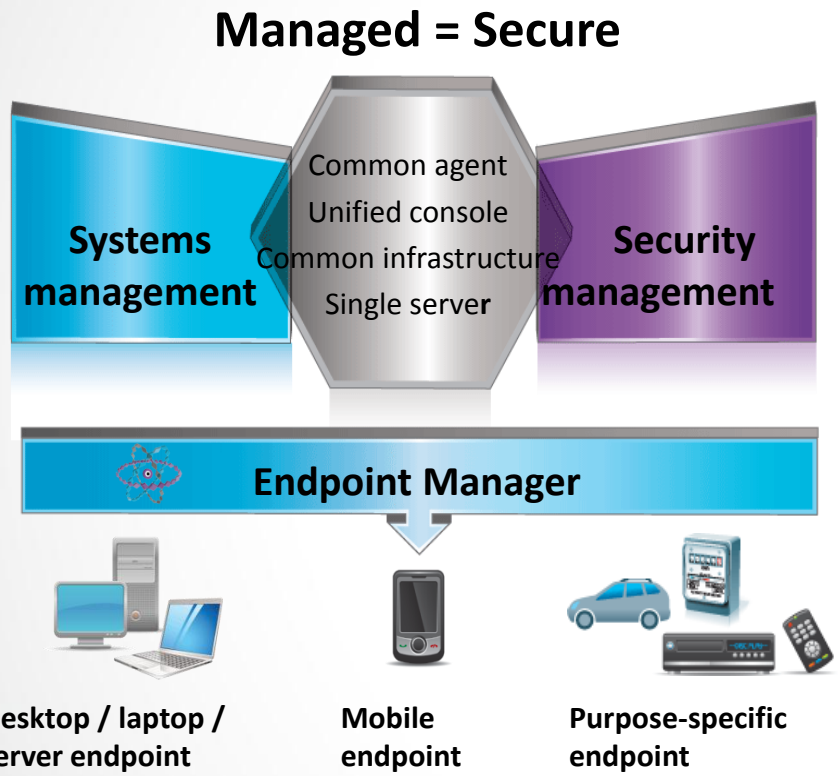
Secure *my mobile business*

Visualizing Mobile Security



Device Lifecycle Management

A unified solution that offers device management and security



Client Challenge

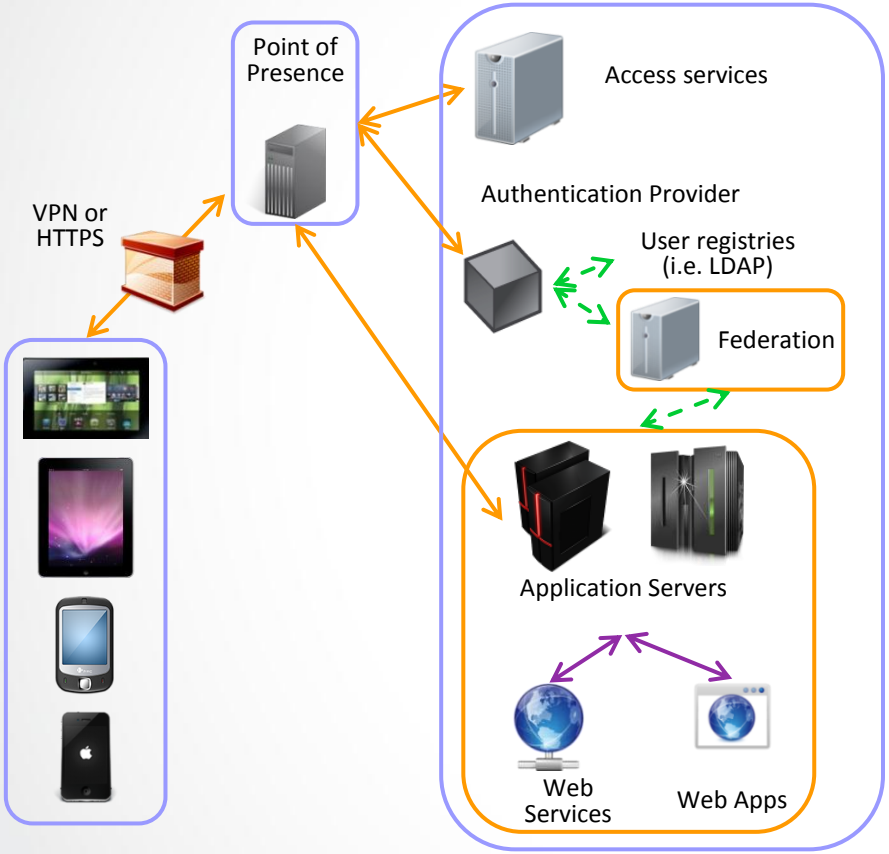
Managing and securing enterprise and BYOD mobile devices without additional resources

Key functional requirements

- 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
- IBM Endpoint Manager

Provide consistent User & Access Management

Extending Access Management to support mobile use cases for apps



Client Challenge

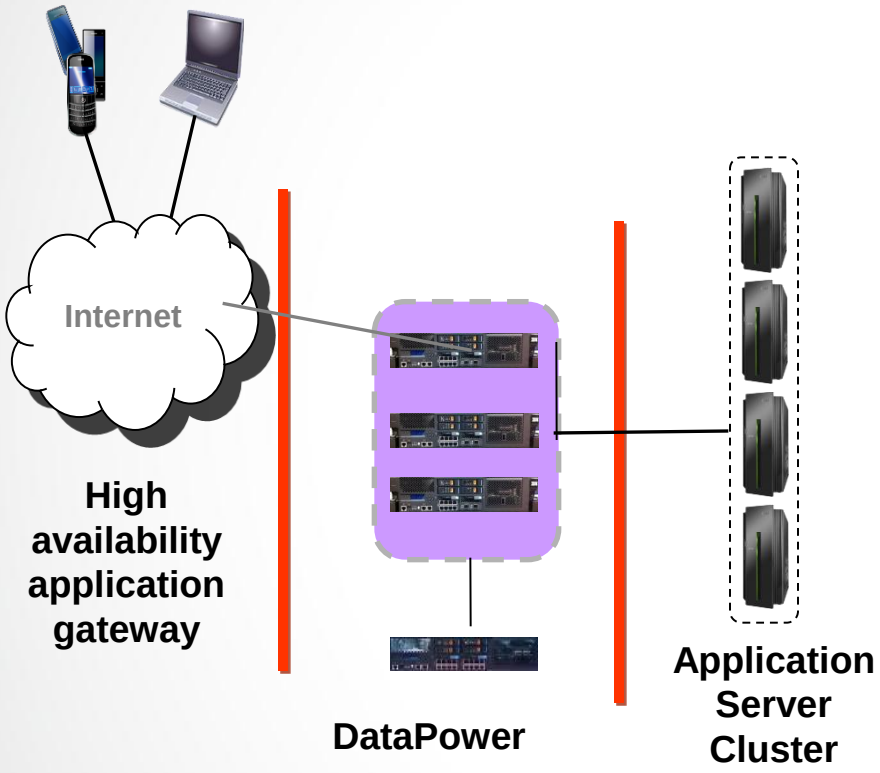
Ensuring users and devices are authorised to access enterprise resources from that specific device.

Key functional requirements

- Satisfy complex context-aware authentication requirements
- Reverse proxy, authentication, authorisation, 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
- IBM Security Access and Identity Management

Secured Mobile Applications

Deliver optimized and secure mobile app experience



Client Challenge

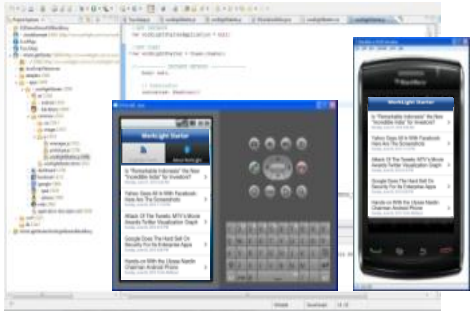
- Mobile Applications place new demands on application resources
- Some mitigations for vulnerabilities can be enforced at the gateway

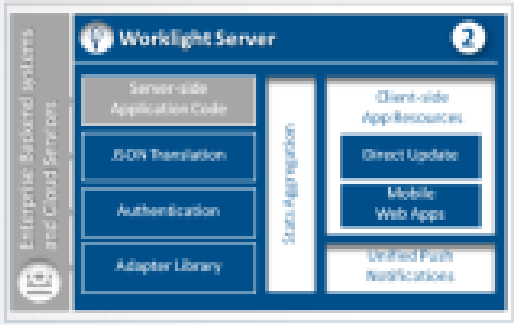
Key Capabilities

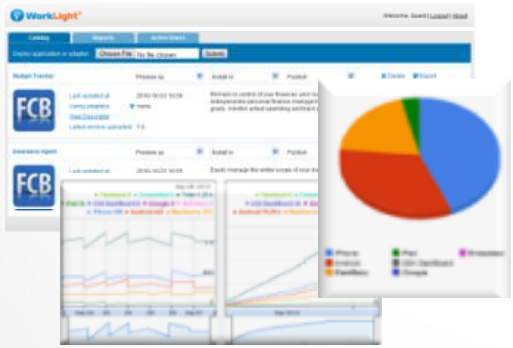
- Satisfy complex routing & scaling requirements
- Message protection/validation and XML firewall
- Mobile native, hybrid, and web apps
- Supports open standards applicable to mobile such as OAuth
- App authentication and authorization
- Synergy with IBM Security Access Manager to deliver context aware user access security
- IBM Datapower

Deliver and Manage Safe Mobile Applications (Apps)

Application development processes need a consistent platform







Client Challenge

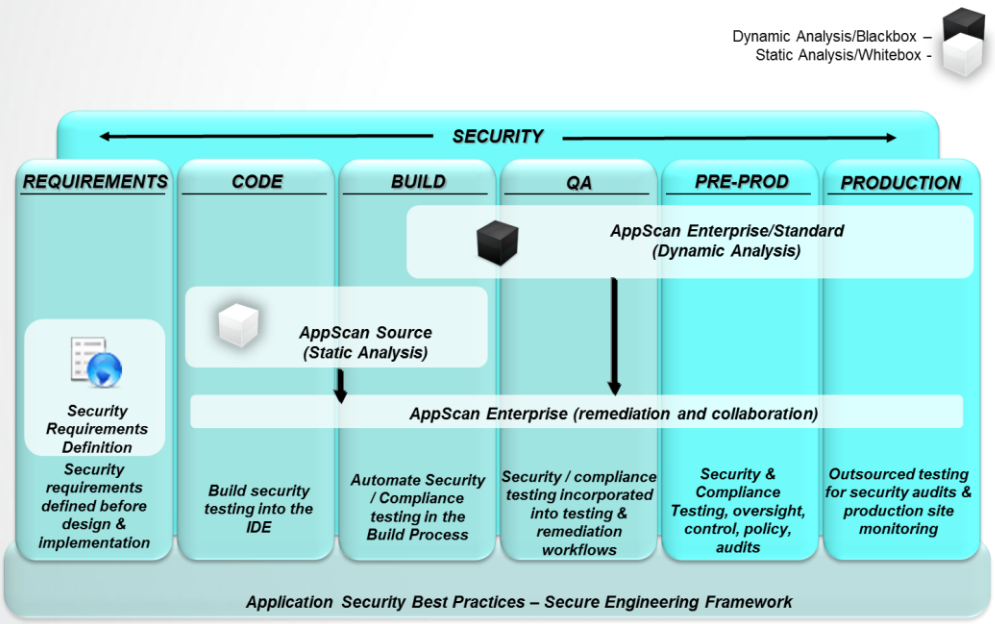
Efficiently and securely, create and run HTML5, hybrid and native mobile apps for a broad set of mobile devices

Key functional requirements

- Integrated secure access to backend application resources
- Secured by design - develop secure mobile apps using corporate best practices, e.g. code obfuscation
- Protect mobile app data with encrypted local storage for data, offline user access, app authenticity validation, and enforcement of organisational security policies
- IBM Worklight

Deliver Security-Rich Applications (Apps)

Application security testing for risk management



Client Challenge

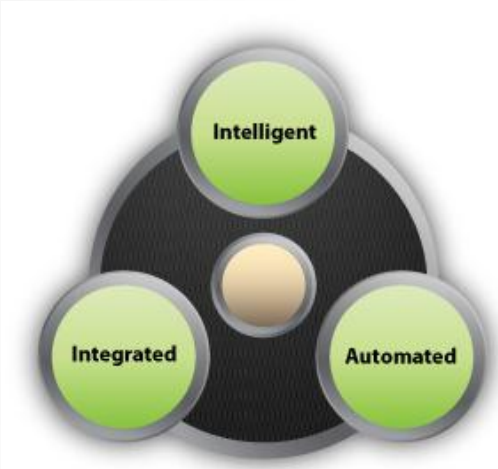
Applying patches and resolving application vulnerabilities after apps are Delivered and Deployed is a very costly and time consuming exercise

Key functional requirements

- Leverage application scanning 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 into development

Deliver An Adaptive Security Posture

Deliver mobile security intelligence by monitoring data collected



Client Challenge

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

Key functional requirements

- 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 Use Cases

IBM Office of the CIO

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

South Korean Credit Card Company

Rolls out a rich, 100-screen mobile app to customer base

The Need:

- Develop a rich application for credit card and benefit management for their client base
- Support for over 100 screens, some of them require sophisticated functionality such as augmented reality and barcode reader
- App required natively implemented screens, as augmented reality that cannot be implemented using web technologies

---

The Solution:

- Korean system integrator developed IBM Worklight app with a team of 10+.
- Natively implemented screens + encryption module mandated by the Korean government (instead of standard HTTPS), made possible with Hybrid coding.
- New frequent functionality uploaded to the app store or market.

The Benefit:

- Android app was ported to iOS in less than 4 weeks, re-implementing native code
- When a new version of the app is uploaded to the app store, older versions are disabled using Worklight's Remote Disable feature.

Solution Components:
IBM Worklight - Enterprise license

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
- Ability to integrate with other systems, Remedy
- Responsiveness and agility of product and product team

AimArs 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 customised 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

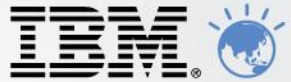
- Extend secure access to banking apps to mobile customers
- Enhance productivity of employees to perform secure banking transactions via mobile devices
- Support for iOS, Android, and Windows Mobile

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

IBM's Mobile Security Strategy

Mobile security is multi-faceted, driven by customers' operational priorities



Mobile Security Intelligence

Mobile Device Management

Mobile Device Management
- ✓ Acquire/Deploy
- ✓ Register
- ✓ Activation
- ✓ Content Mgmt
- ✓ Manage/Monitor
- ✓ Self Service
- ✓ Reporting
- ✓ Retire
- ✓ De-provision

Mobile Device Security Management
- ✓ Device wipe & lockdown
- ✓ Password Management
- ✓ Configuration Policy
- ✓ Compliance

Data, Network & Access Security

Mobile Threat Management
- ✓ Anti-malware
- ✓ Anti-spyware
- ✓ Anti-spam
- ✓ Firewall/IPS
- ✓ Web filtering
- ✓ Web Reputation

Mobile Information Protection
- ✓ Data encryption (device,file & app)
- ✓ Mobile data loss prevention

Mobile Network Protection
- ✓ Secure Communication (VPN)
- ✓ Edge Protection

Mobile Identity& Access Management
- ✓ Identity Management
- ✓ Authorise & Authenticate
- ✓ Certificate Management
- ✓ Multi-factor

App/Test Development

Secure Mobile Application Development
- ✓ Vulnerability testing
- ✓ Mobile app testing
- ✓ Enforced by tools
- ✓ Enterprise policies

Mobile Applications
i.e. Native, Hybrid, Web Application

Platform Extension OS/ Application Layer (Optional)
i.e. Application Container (Sandboxing), Virtualisation

Device Platforms
30 device Manufacturers, 10 operating platforms
i.e. iOS, Android, Windows Mobile, Symbian, etc

Complimentary Offer

Get hands on experience of the capabilities of IBM Mobile Enterprise by joining us for a complimentary Proof of Technology workshop.

These workshops will benefit anyone interested in evaluating IBM's latest Mobile Enterprise solution for use in their organisation.

Melbourne
9 October 2012
Cliftons, 1/440 Collins Street

Sydney
11 October 2012
Cliftons, 200 George Street

Canberra
18 October 2012
Cliftons, 10 Moore Street

To attend an upcoming workshop or for more information, call our WebSphere customer representative, Biju George on 1800 557 343 or email rlm@au1.ibm.com.

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.