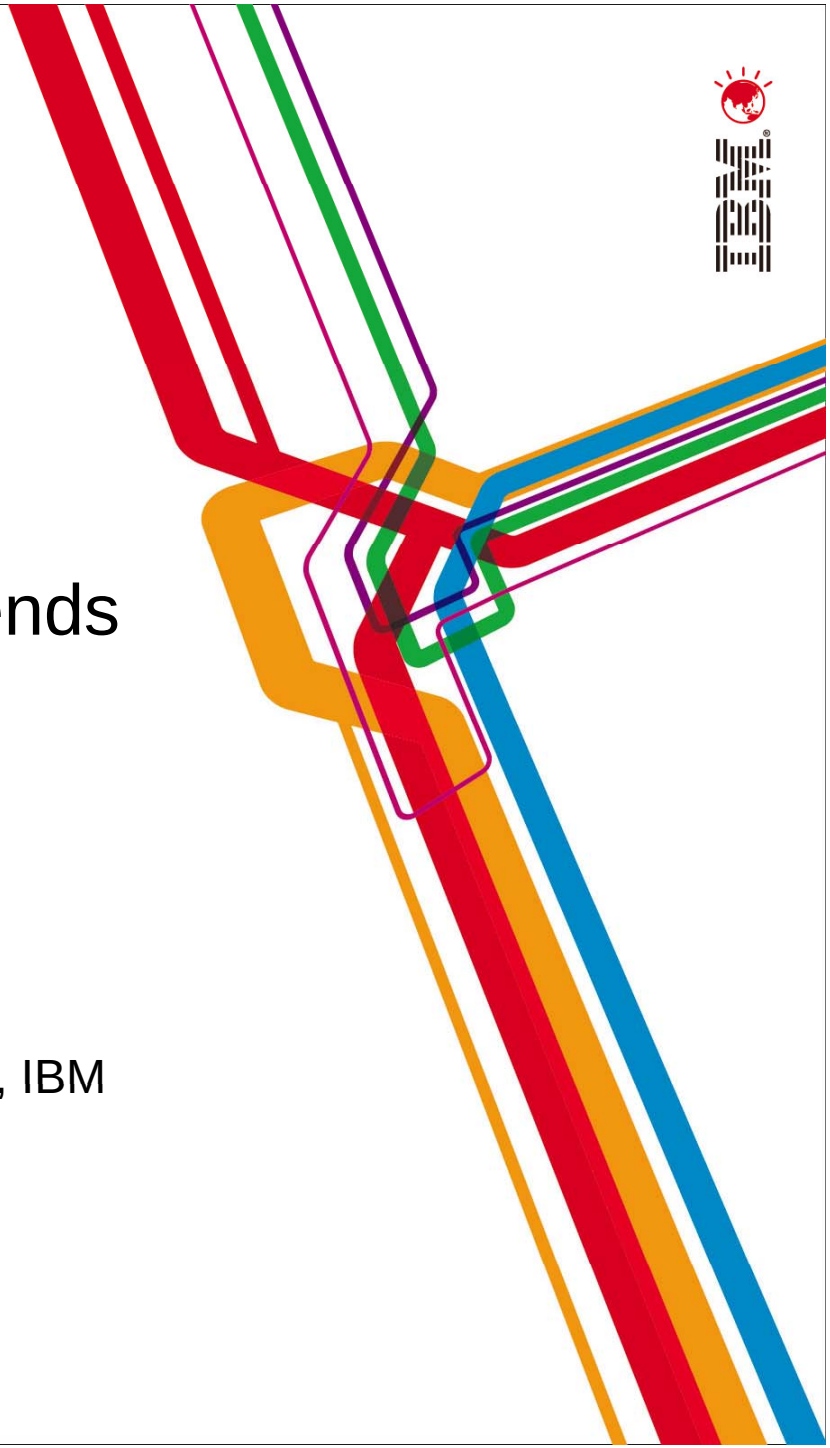
# Pulse Comes to You 2012

Business without **LIMITS**

21 Aug 2012 | Thailand

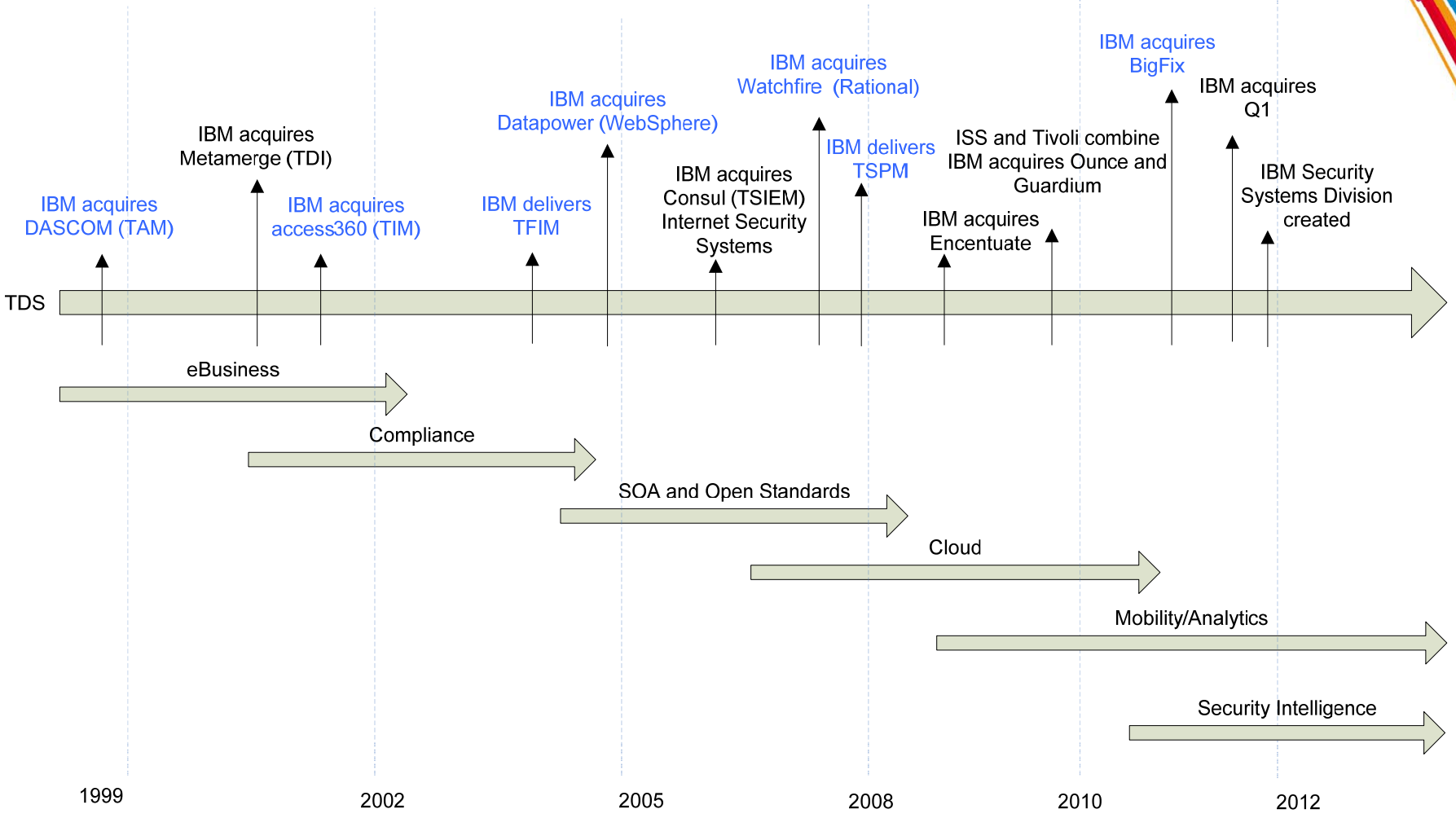


## Mobile Application Security Trends and Directions


**Chris Hockings**

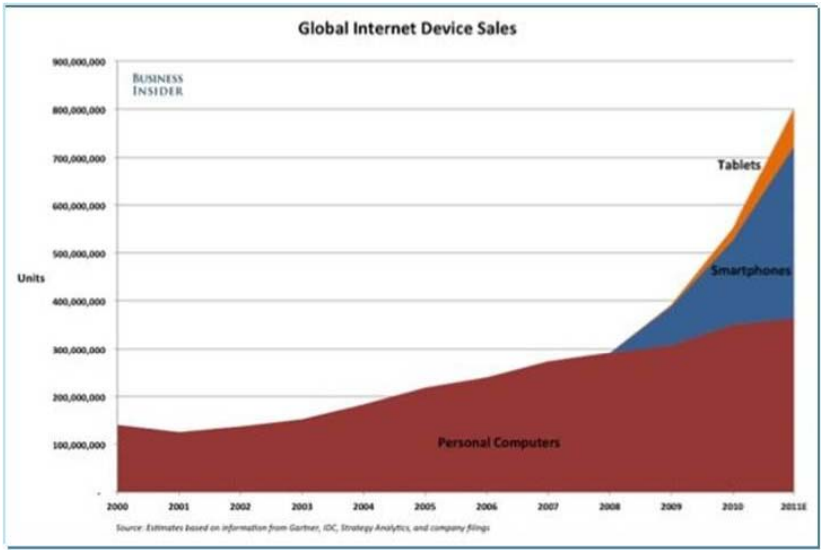
Development Lab Manager, Security Systems, IBM Software Group, Australia

# IBM Security Systems portfolio growth



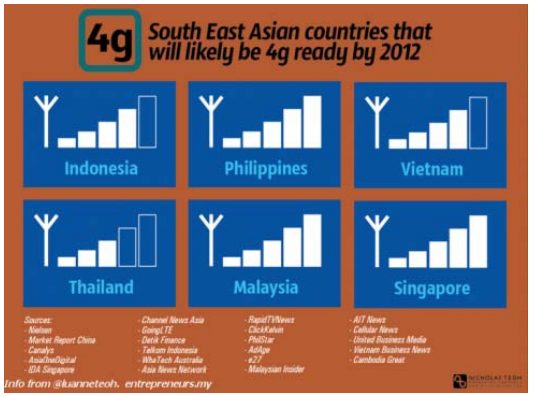

Blue text indicates products that have a direct functional impact on mobile use cases

# 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

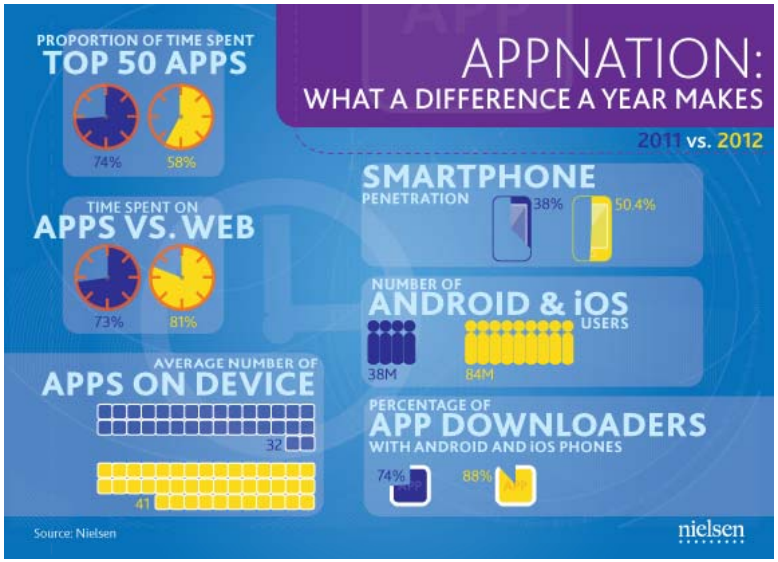

Singapore, Malaysia, Thailand, Vietnam, Indonesia, Philippines, and Cambodia registered spikes in demand for smartphones in the range of 40 to 400% more over the same period last year

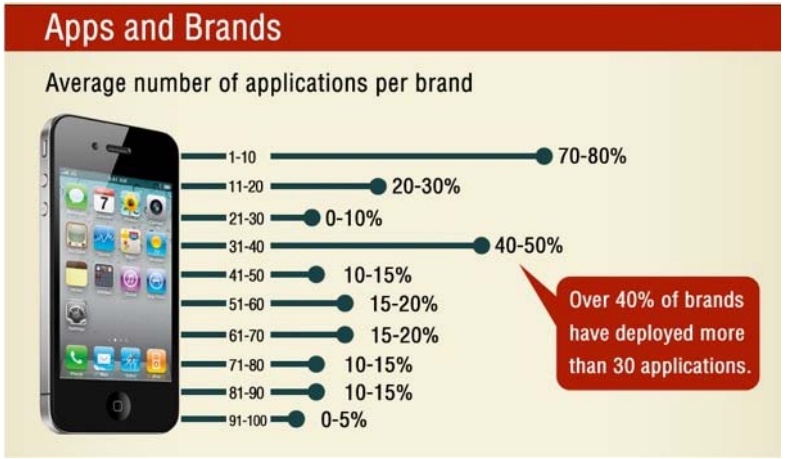
**Pulse Comes to You 2012**

Business without LIMITS

- GfK Asia

# Apps…In a Mobile World…Its all about Apps





**Pulse Comes to You 2012**

- Apps are stealing users face-time from browsers.
- Browsing is almost equating to browsing apps stores for apps
- Browsers still important but for business tasks like connecting, informing and managing people preferring the app user experience

# A Primer on Mobile Apps…

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





***Richness of Mobile Presentation / Services***

***Portability (cross-device reuse)***

***Maintenance Cost (TCO)***

# Understanding the Mobile App Development Process…

LoB demands mobile apps as a way to drive brand value

More direct involvements from users/stakeholders

Native programming models are not portable across devices

Fragmentation of mobile devices and platforms

**Marketing, Customer Service, Partners**

**Customers**

**Consumerization of IT**

***Analysis Phase***

**Line of Business**

**Analyze**

***Build Phase***

**Development Team**

**Design**

**Implement**

**Test**

**Optimize**

***Deploy Phase***

**Operations/ Manufacturing Team**

**Run**

**Manage**

**Monitor**

- Ensure quality on combinatorial number of configurations of devices, platforms, carriers, etc.
- May need access to large library of mobile devices for testing

***Governance and Best Practices***

Higher expectations of user experience

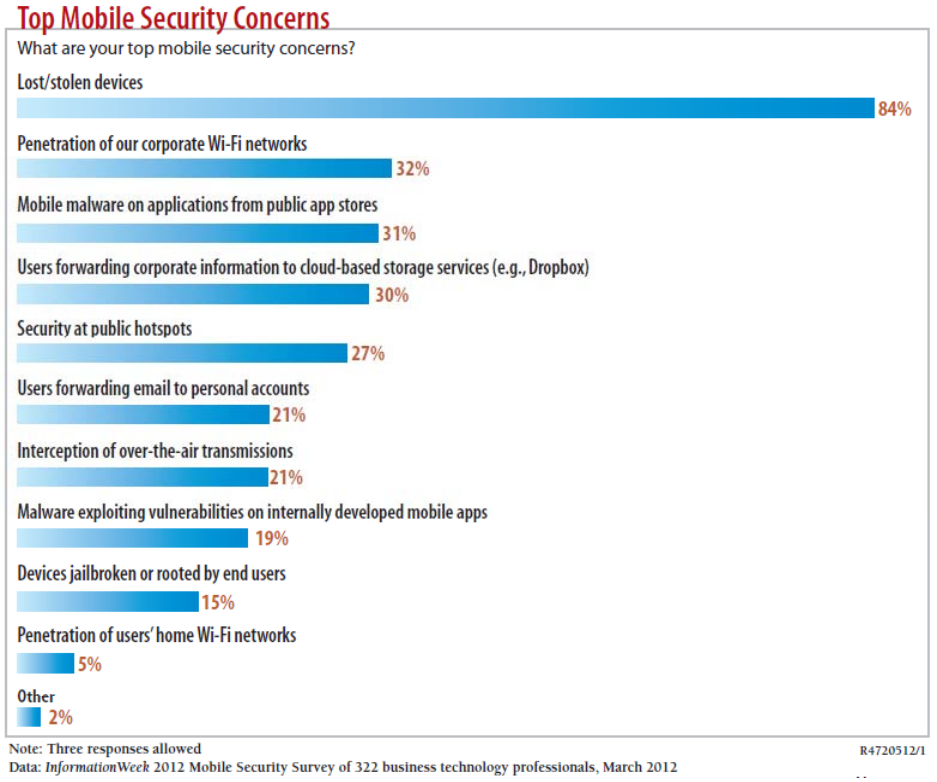
Lack of best practice guidance on how to deliver mobile applications

- Mobile landscape evolves at a much faster pace
- More frequent releases and updates with urgent time-to-market demands

# 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

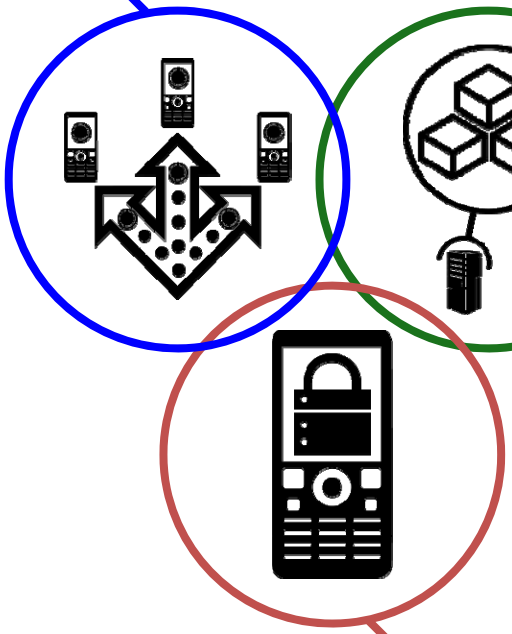
| | |
|---|---|
| Social Engineering | Mobile Borne DoS Attacks |
| Rogue Apps | Identity Theft |
| Malicious Websites | Man-in-the-Middle Attacks |

# 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*

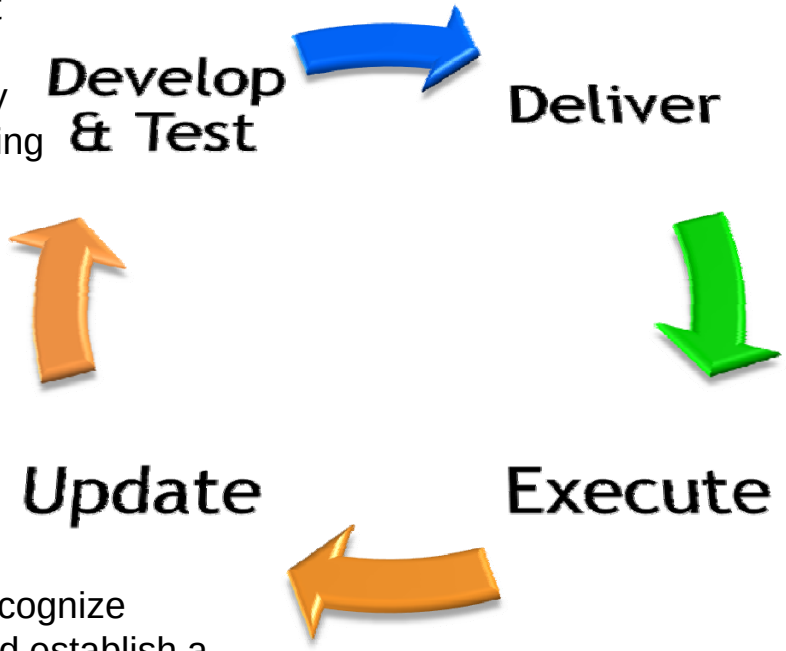
## Manage & Secure

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

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

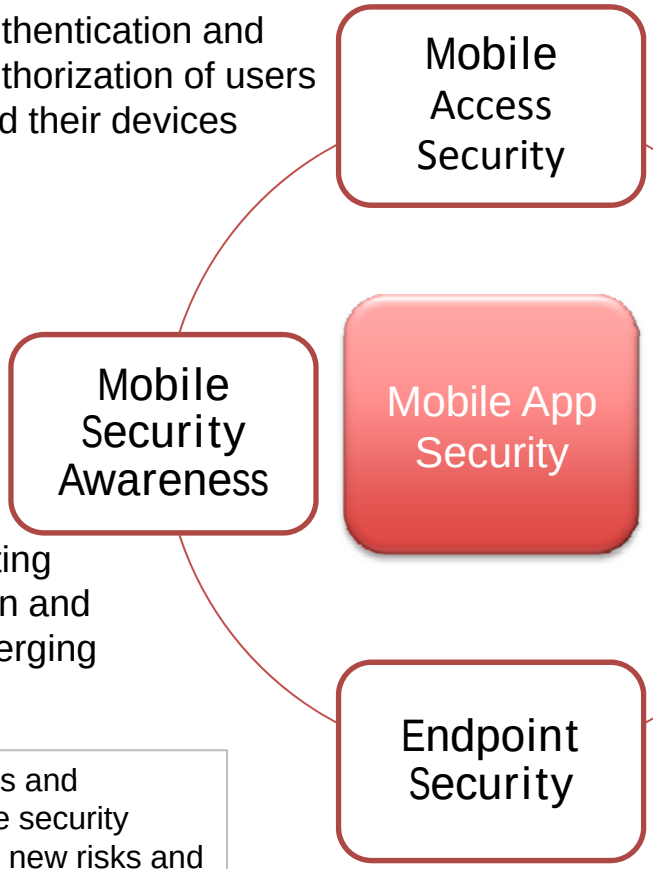
# Mobile App Security: Defending the Software

- Consistently apply and enforce best practices during Development
- Perform vulnerability analysis during Testing




- Provide or employ a secure channel for delivering apps
- Employ a secure runtime environment to safeguard app data
- Perform checks to validate the integrity of apps
- As threats evolve recognize required updates and establish a process for pushing them to users

# Adjacent Security Considerations




- Authentication and Authorization of users and their devices

A majority of mobile applications access back-end services and systems to either request content or perform operations on behalf of the user.

Even for native applications only approx. 15% of app launches happen offline

- A trusted connection to back-end systems

- Visibility & Reporting
- Risk determination and awareness of emerging threats

Introduction of new features and capabilities always precede security methods which can lead to new risks and emerging threats

- Detect the integrity of the device and gain awareness of known threats present on the device

# 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
    - 2/3$^{rds}$ BYOD, 1/3$^{rd}$ IBM-supplied
  - Best practices from pilot now available as a client service via managed services

# DELIVERING CONFIDENCE

# 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

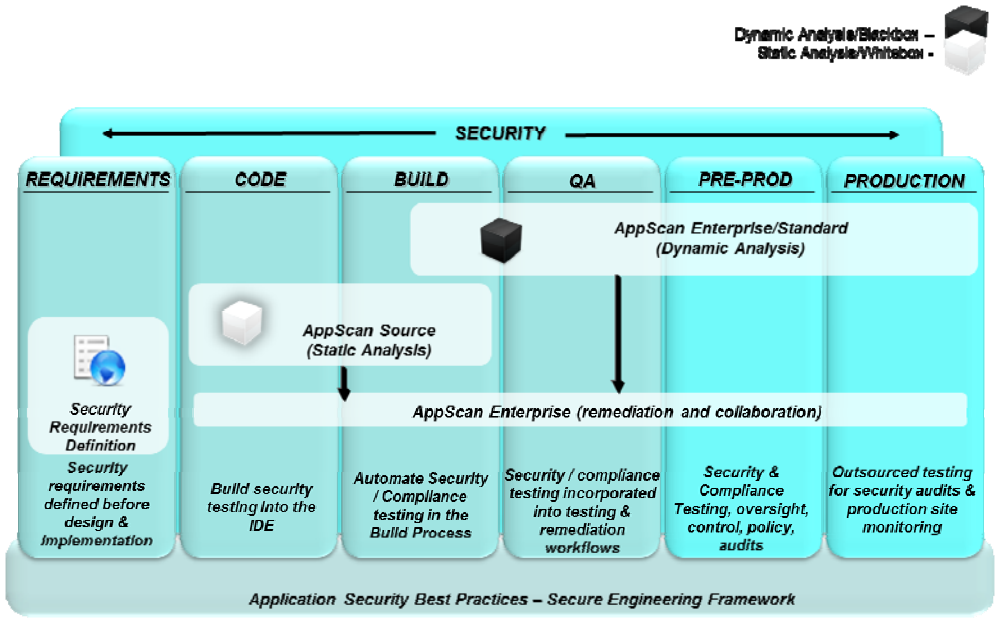
Efficiently and securely, create and run HTML5, hybrid and native mobile apps for a broad set of mobile devices

## 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

# Mobile App Security

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




## Client Challenge

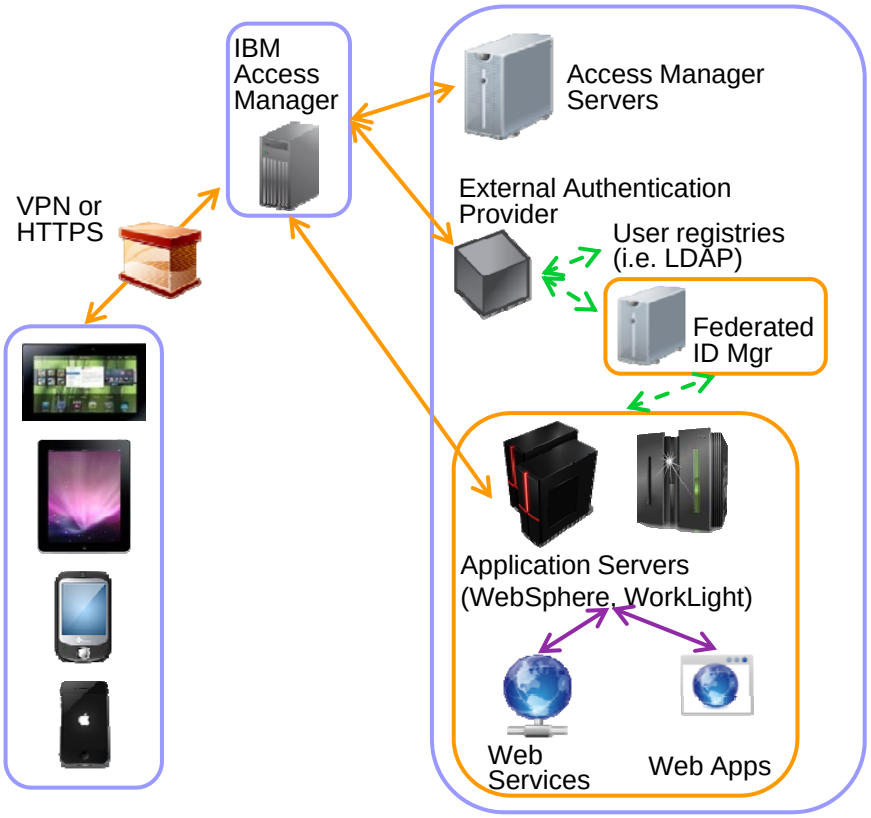
Applying patches and resolving application vulnerabilities after apps are Delivered and Deployed is a very costly and time consuming exercise

## 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 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.

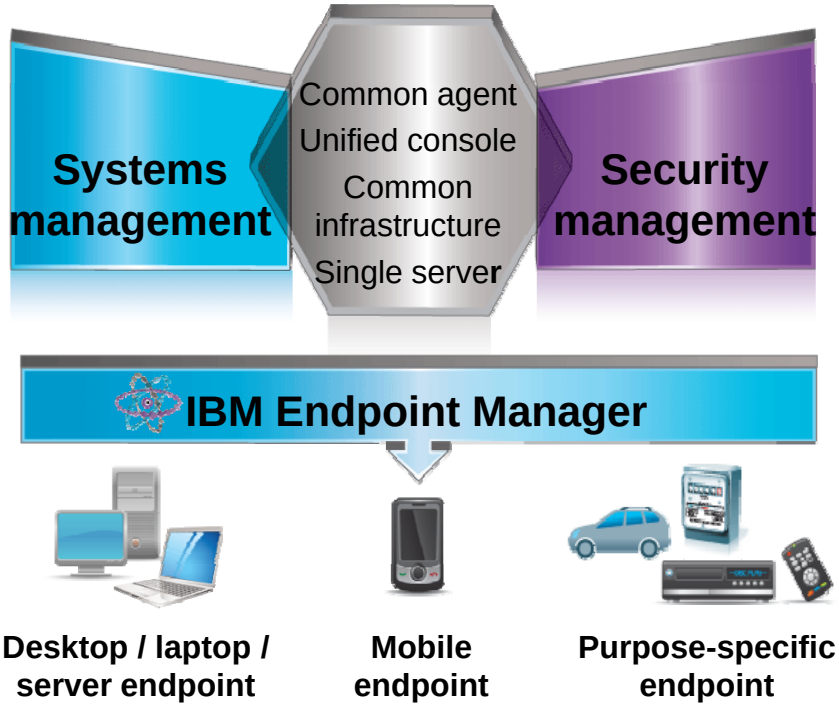
## Key Capabilities

- 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 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

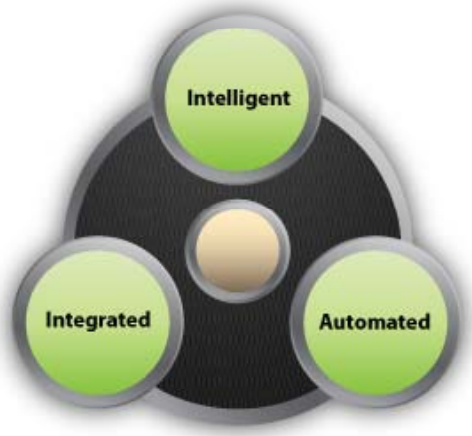
Managing and securing enterprise and BYOD mobile devices without additional resources

## 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
- Distribution of Enterprise apps

# 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

# 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