Balancing mobility & security of 'bring your own device' in the enterprise

Peter Cutler, BEng(Hons)
Security Systems Client Technical Professional

PCTY2012

Pulse Comes to You

Optimizing the World's Infrastructure
30th May, London

Agenda

1. Pirean Bring Your Own Device survey sample
2. Trends & Uniqueness
3. Security challenges
4. Observed mobile security requirements
5. Customer security scenarios
6. Mobile security intelligence

Pirean Bring Your Own Device Survey

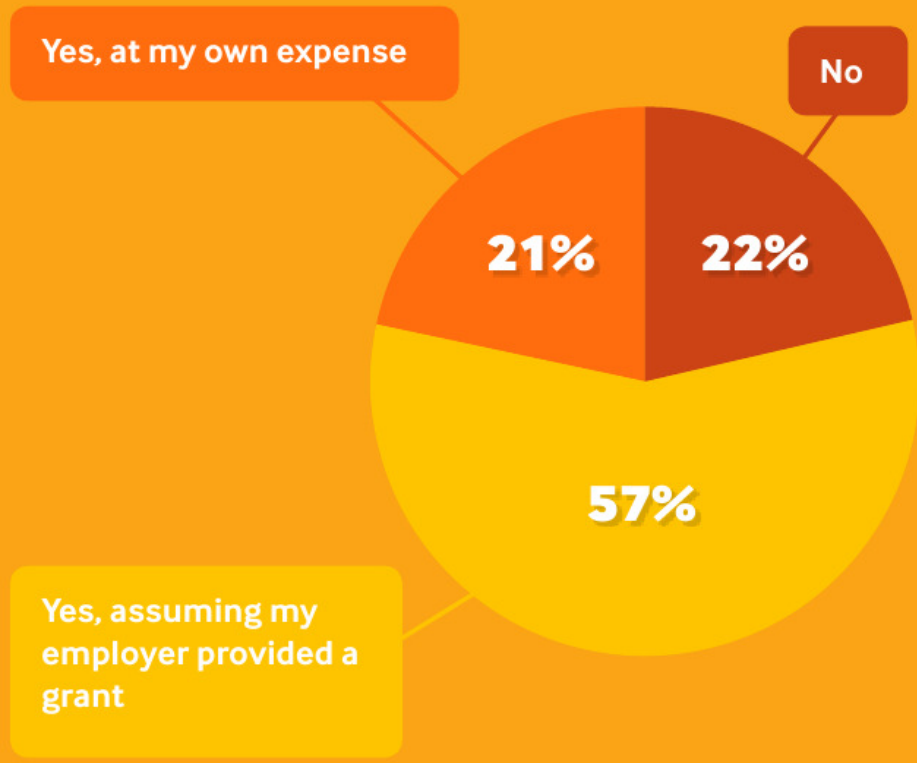
Pirean 'Bring Your Own Device' Survey Sample

"Would you be happy to support a BYOD program at your place of work?"

When rolling out a BYOD policy within an organization a number of considerations and mitigations must be made by the user, which traditionally would have been carried out by their employer, such as device insurance and the introduction of specific security measures such as mobile device firewalls, anti-virus and patching. This placement of responsibility onto the user could result in a lack of BYOD policy engagement on their part, thereby minimizing any efficiency gains. To understand more about this scenario, we asked more generically **"Would you be happy to support a BYOD program at your place of work?"**

Out of those users surveyed, **22%** stated that they would not be willing to do so, with **57%** stating that they would (but only with an employer backed stipend or expense limit to cover all associated costs), and finally only **21%** stated that they would support a BYOD policy at their own expense.

The results for both questions one and two show that the deployment of a 'Bring' you own device policy is much more challenging to realize than an optional 'Buy' your own device policy. This is predominantly due to user acceptance rather than technical reasons.



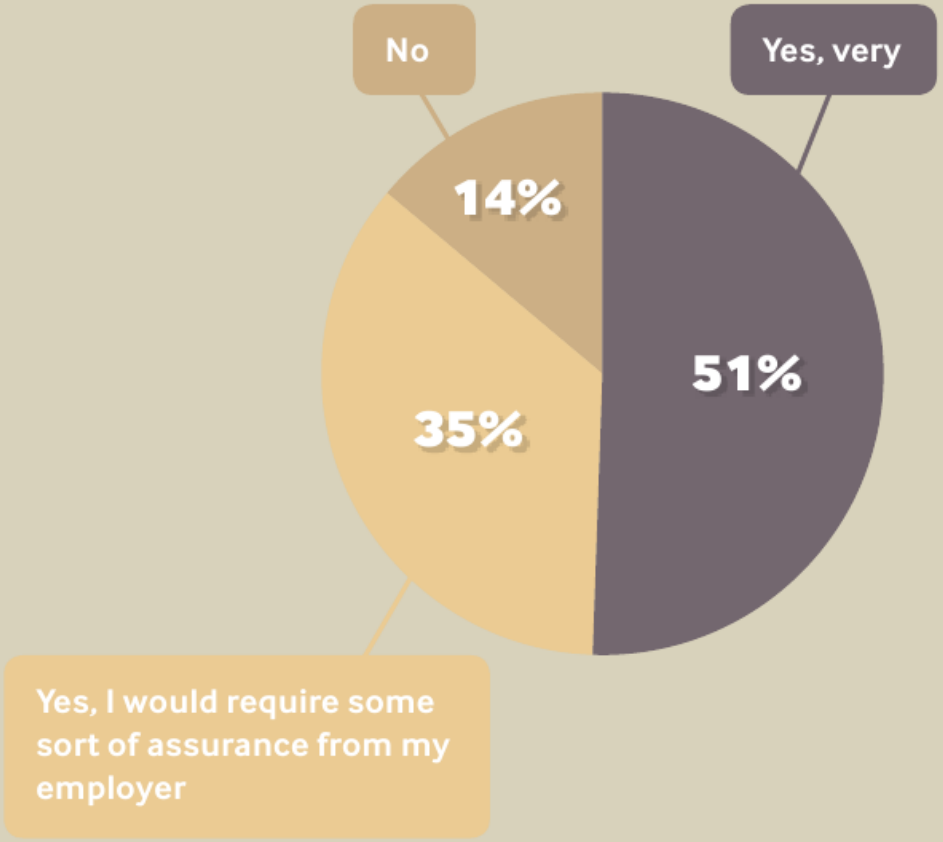
Pirean 'Bring Your Own Device' Survey Sample

"If using your own device for work purposes, would you be concerned about personal data privacy (e.g. online banking, personal email account)?"

To understand why there is some perceived resistance towards a BYOD policy, we asked **"If you were using your own device for work purposes, would you be concerned about personal data privacy (e.g. online banking, personal email account)?"**

51% of respondents stated that they would be very concerned about their employer's ability to respect and protect their own personal data, with an additional **35%** stating that would also require some level of assurance from their employer.

The UK Data Protection Act (DPA) 1998 states **"Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data."** Similar policies governing data protection are in place in the majority of countries worldwide, so if an organization were to transmit and store personally identifiable data about relevant persons (i.e. employees, customers, business partners) on a device that is not wholly governed by internal security policies, could it be in breach of the DPA and equivalent localized policies?



Trends in Enterprise Mobility...

The need for business agility along with changing employee behaviours 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

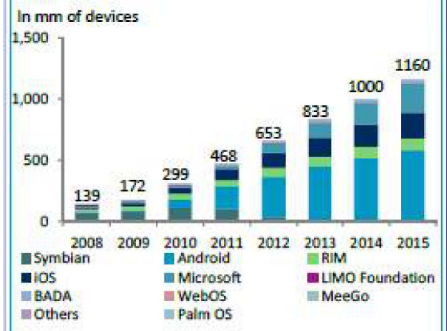
Increasing Demand for Enterprise Applications

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

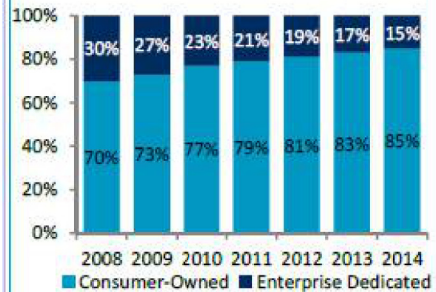
Security Requirements Becoming More Complex

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

Smartphone Proliferation

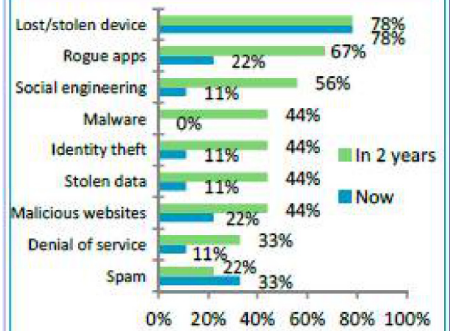


% of Consumer v. Enterprise Devices



Enterprise Application Market

Assessment of Security Threats



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.

Top 5 Security Challenges faced

Security and Privacy cited as the number one mobile adoption concern

– 2011 IBM Tech Trends Report

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

- Achieving Data Separation
  - Privacy
  - Corporate Data protection

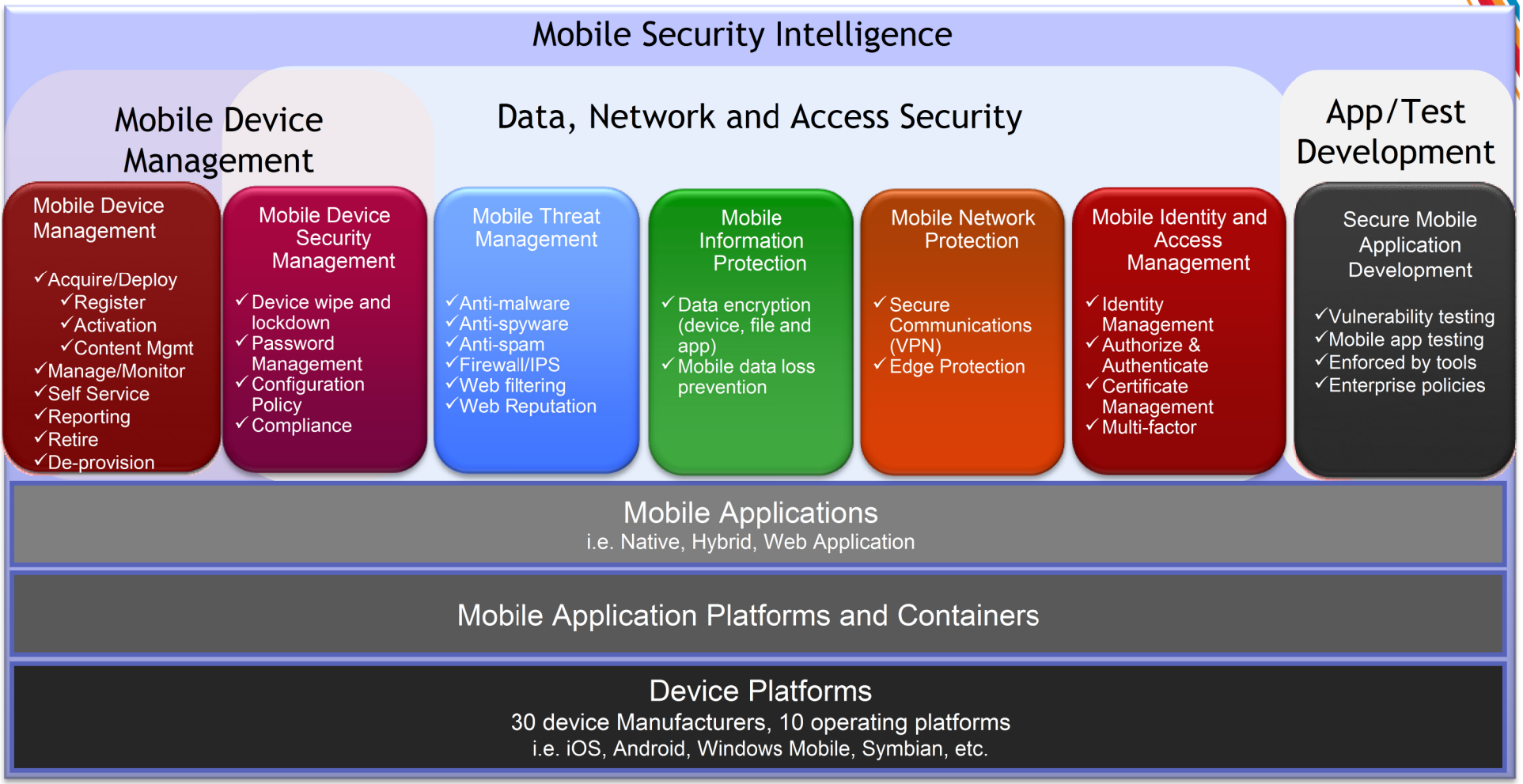
- Providing secure access to enterprise applications & data
  - Secure connectivity
  - Identity, Access and Authorization

- Developing Secure Mobile Apps
  - Vulnerability testing

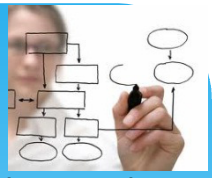
- Designing an Adaptive Security Posture
  - Policy Management
  - Security Intelligence

Key set of Mobile Security Requirements

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



Customer scenarios – security check list



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

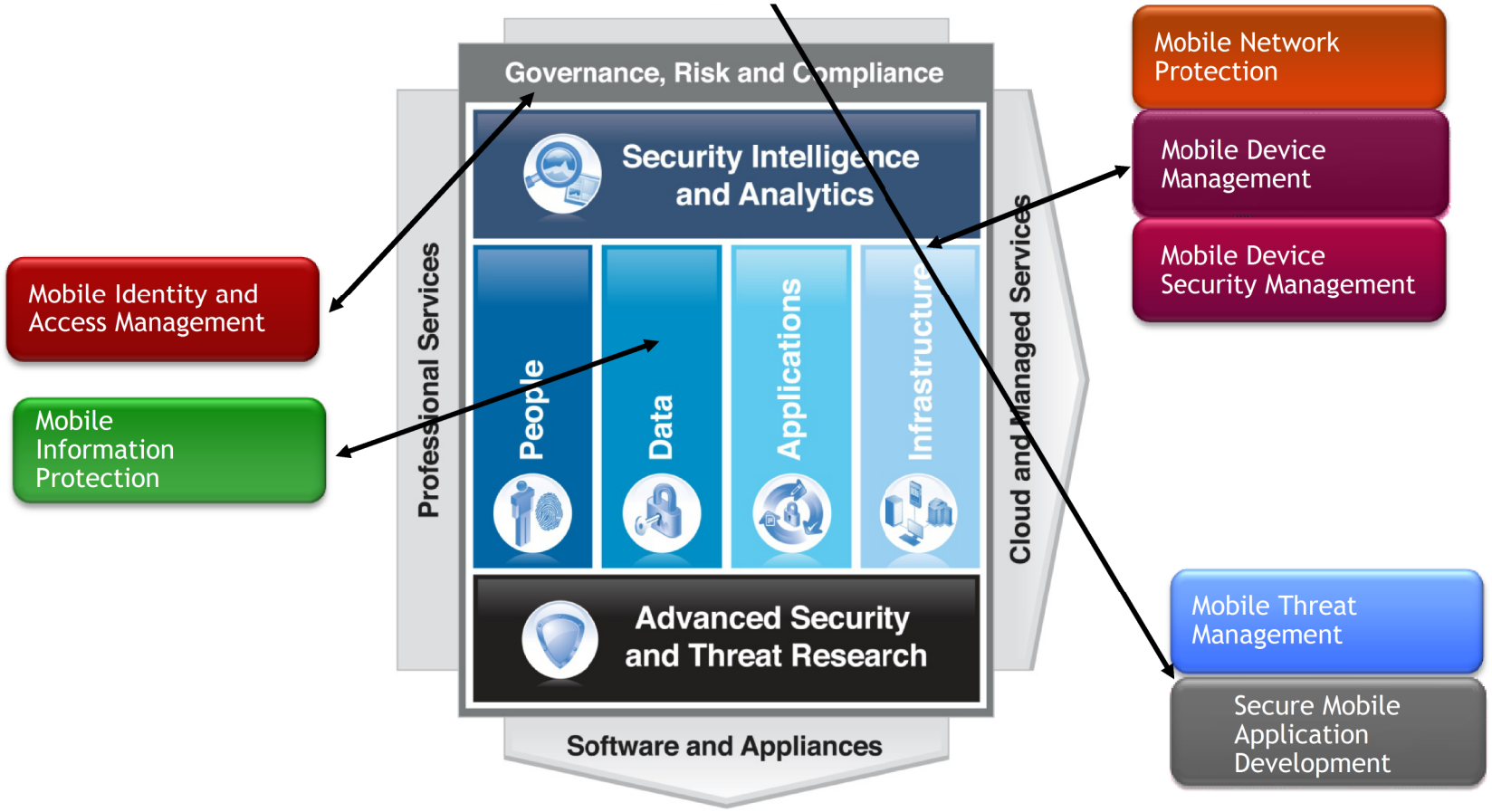
- ➢Provide secure access to enterprise systems
  - ❑ VPN
- ➢Prevent unauthorized access to enterprise systems
  - ❑ Identity
  - ❑ Certificate management
  - ❑ Authentication
  - ❑ Authorization
  - ❑ Audit
- ➢Protect users from Internet borne threats
  - ❑ Threat protection
- ➢Enforce Corporate Policies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

Mobile Security enabled with IBM solutions



IBM Mobile Enterprise

Banking | Insurance | Healthcare | Telecom | Retail | Government | Others

IBM Enterprise Mobile Platform

Business Results

- Extending business to mobile customers and workforce
- Improve operational efficiencies and reduce costs
- Differentiate the customer experience
- Enable new services and business models

- Workforce Optimization
- Product and Service Innovation
- Customer Care and Insights
- 3rd Party Mobility Services
- Social Collaboration
- User Notification
- Location Services
- Mobile Payments
- Social Mobile Commerce

Build *mobile applications*

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

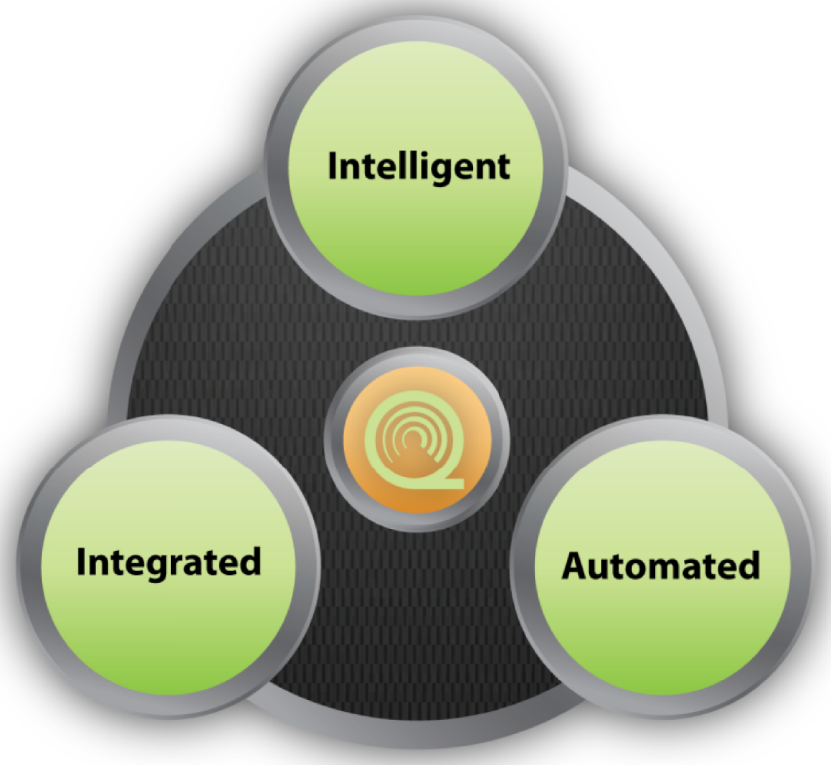
Manage *mobile devices and applications*

Secure *my mobile business*

Extend *existing business capabilities to mobile devices*

Transform *the business by creating new opportunities*

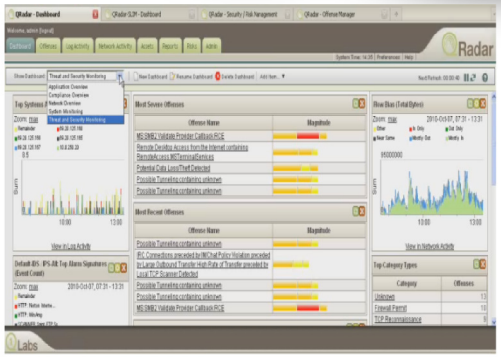
Mobile Security Intelligence

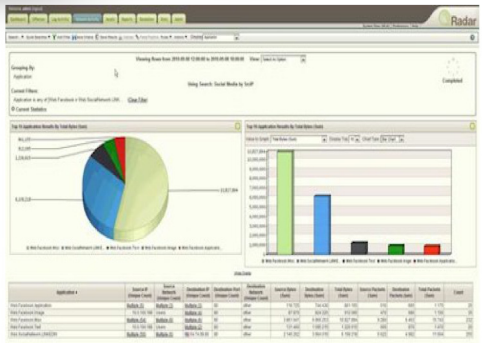


- Proactive threat management
- Identifies most critical anomalies
- Rapid, complete impact analysis

- Eliminates silos
- Highly scalable
- Flexible, future-proof

- Easy deployment
- Rapid time to value
- Operational efficiency





Please note:

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- 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 many factors, including 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 results similar to those stated here.

Acknowledgements, disclaimers and trademarks

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

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.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

PCTY2012

Pulse Comes to You