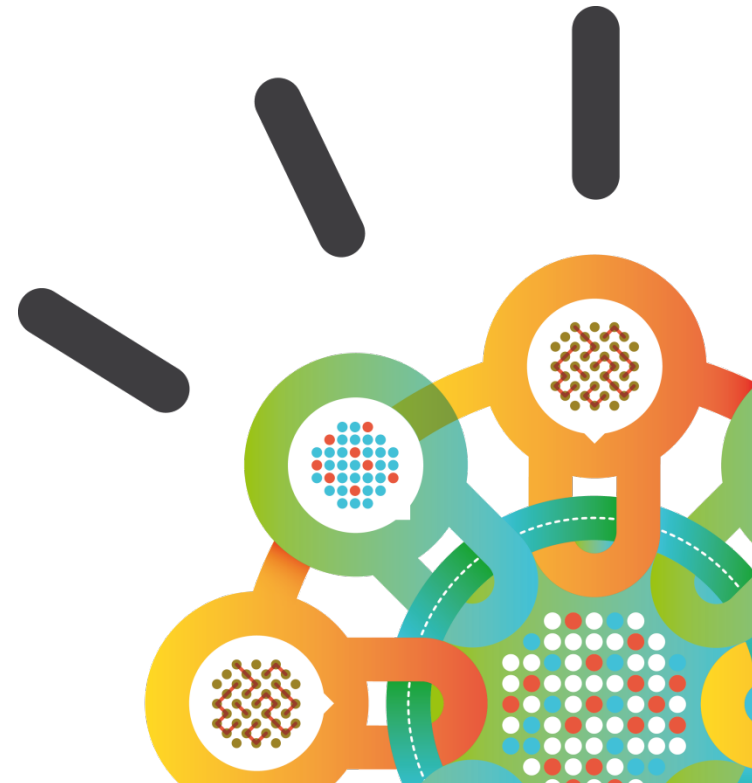


Security Intelligence.
Think Integrated.

Enabling Your Workforce - Securing the Mobile Enterprise

Darren Argyle *CISM CISSP*
WW Security Solutions Market Leader

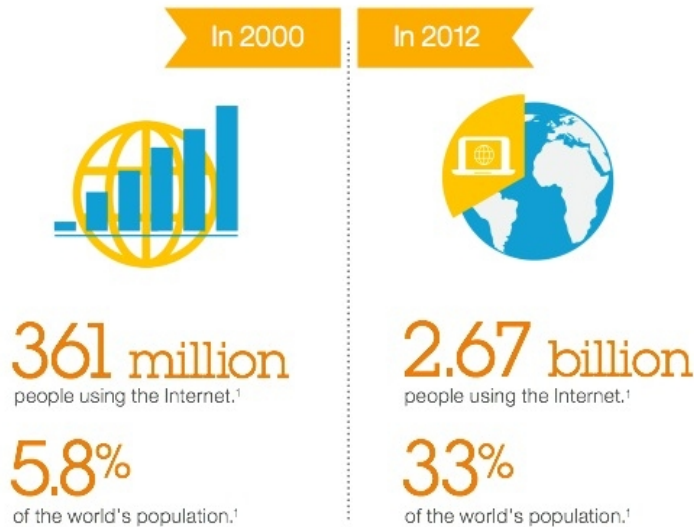




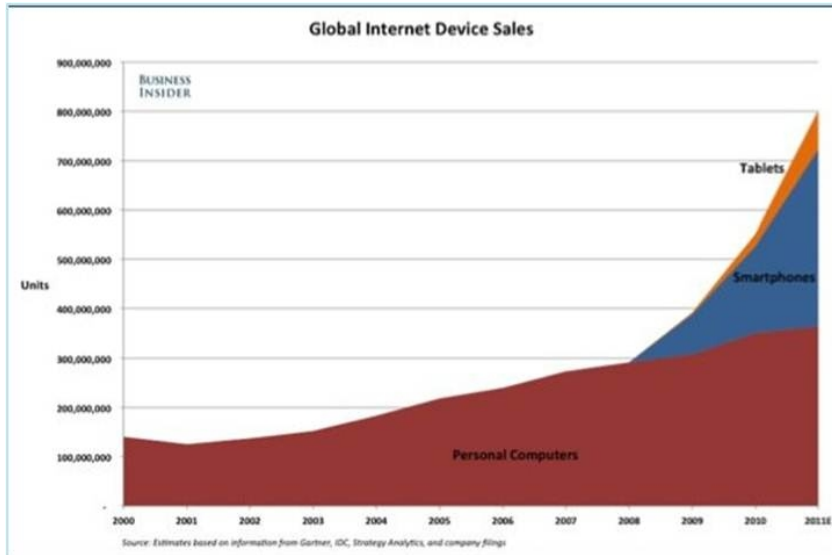
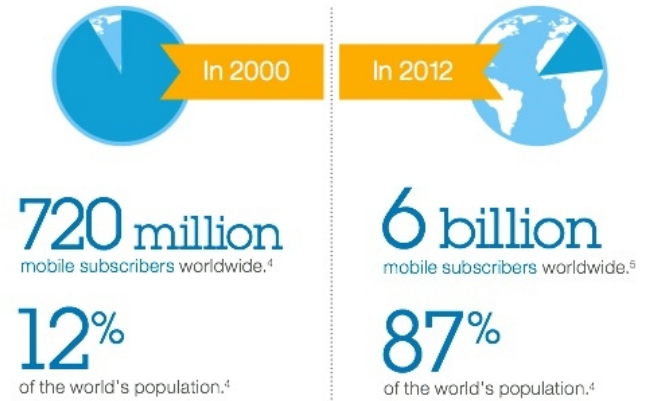
Introduction

- Rapidly changing landscape – it's a smarter world
- Business opportunities and challenges
- IBM case study – becoming a secure mobile enterprise
- Getting started on your own journey
- Accelerating mobile deployment with IBM Security solutions
- Summary and close

It's a (Smarter) Mobile World!

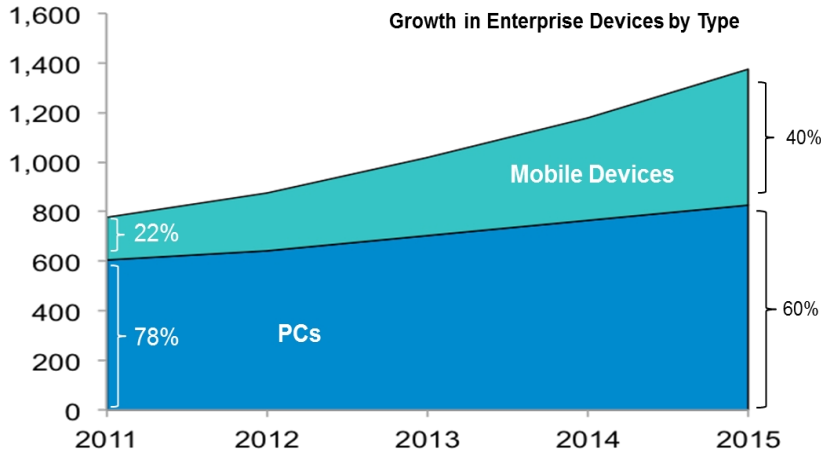


The rise of mobile



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

Employees Bringing Smart Devices To Work...



By 2015 40% of Enterprise devices will be mobile devices

- IBM Projection

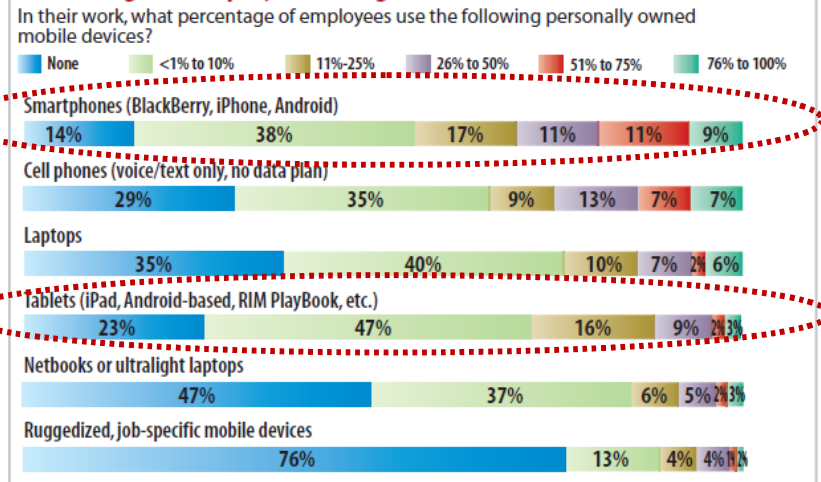
Bring Your Own Device (BYOD)

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

Greater propensity for users of smartphones and tablets to use their personal devices for work

Organizations starting to view BYOD for its business value and organizations recognizing the competitive differentiation it can offer

Percentage of Employees Using Personal Mobile Devices for Work



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

"34% of CIOs think employees are accessing their network with personal devices and 69% of users confirm they are indeed accessing corporate network with personal devices."

60% of companies now offer **BYOD**

NINETY PERCENT OF COMPANIES WILL OFFER BYOD BY 2014



Opportunities for the enterprise

Business to Enterprise



- Increase worker productivity
- Improved decision making for mobile workers
- Increase revenue through sales efficiency
- Extend existing applications to mobile workers and partners
- Deploy industry specific solutions to streamline business processes and reduce costs
- Increase employee satisfaction through flexible BYOD programs
- Reduce personnel cost (utilizing personal owned instead of corporate issued devices)

Business to Consumer



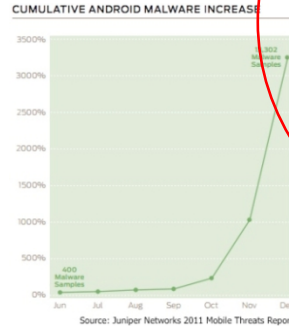
- Drive increased sales through personalised offers
- Handle retail sales transactions and opportunities more efficiently
- Offer accurate and usable data to customers in realtime and at anytime they choose
- Maintain contact with clients, on 24/7 basis for access to mobile online apps
- Deeper insight into customer buying behavior for up sell and cross sell
- Improve conversion rate for high value clients by providing enhanced choices



Mobile Security Threat Landscape

Malware

- Malware existed in various forms (viruses, worms, Trojans, spyware) has been constantly increasing.
- 25,000 mobile malware apps were identified as of the second quarter of 2012--a 417 percent rise from the first quarter. (Trend)
- No platform is immune. Malicious applications on increase in all app stores
- “Zeus for Mobile”
- First large scale mobile botnet in 1Q2012 – RootStrap (Symantec)



Top mobile security concern by over 84%

Loss and Theft

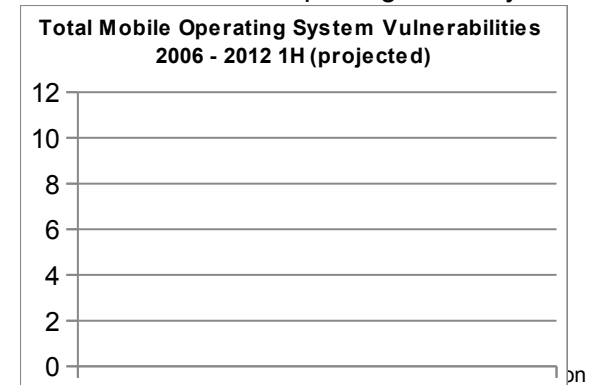
- The major benefits of mobile devices (size and portability) unfortunately come with the big risk of losing sensitive data that has to be accepted but can be mitigated.
- A survey of consumer users found that one out of every three users has ever lost a mobile device.
- 2011 study - 36 percent of consumers have either lost their mobile phone or had it stolen. (Symantec)
- Cell phone theft in New York City jumped from eight percent of robberies 10 years ago to more than 40 percent today (CBS News)

Communication

- SMS toll fraud continues as one of primary exploited areas
- Bluetooth is an exploited vector because a device in a discoverable mode can be easily discovered and lured to accept a malicious connection request.
- “Man in the middle” attacks have been demonstrated to be possible with several platforms using Wi-Fi links.
- Phishing or pharming attacks can leverage multiple channels: email, SMS, MSS, and voice

OS vulnerability based attacks

- Mobile OS vulnerabilities continue to be discovered at significant rates
- Always on and connected, mobile device is a prime target for hit-and-run network-based attacks and exploiting zero-day vulnerabilities.
- Published techniques to “jailbreak” or “root” mobile devices allow hackers to get administrative access, commonly within days of release



Mobile is fast becoming the target of choice – a use case

- Confidentiality leaks
 - Private conversations leaked to public
 - Private contact information leaked to public
 - Location leaked to public
- Integrity violations
 - Corruption of local databases
 - Fraudulent use of application
- Abuse of privileges
 - Sending text messages
 - Placing calls
 - Surveillance of device's user

Which QR code is evil?



- QR Code contained a URL to download malware
- The malware sent SMS messages to a premium rate number (US \$6 per message)

<http://siliconangle.com/blog/2011/10/21/infected-qr-malware-surfaces-on-smartphones-apps/>

So how does this translate to the enterprise mobility challenge ?



Achieving Data Separation & Providing Data Protection

- ★ Personal vs corporate
- ★ 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



IBM's internal approach as an enterprise and service provider

Focused on security essentials, informed by the IBM Security Framework



1. Build a risk-aware culture and management system



6. Control network access and help assure resilience



2. Manage security incidents with greater intelligence

IBM Security Framework



7. Address new complexity of cloud and virtualization



3. Defend the mobile and social workplace





8. Manage third-party security compliance




4. Security-rich services, by design

9. Better secure data and protect privacy



5. Automate security "hygiene"

10. Manage the identity lifecycle



Case study with IBM

- 95% of IBM employees are issued laptops
- Over 100,000 smartphones and tablets with access to the IBM corporate network and growing rapidly!
- Personally owned devices can be used for business purposes
- Strong dependency on collaboration and social media tools to conduct IBM business and stay connected

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."
– **IBM CIO Jeanette Horan**



How did IBM become a mobile business?

- Established policies for mobile employees
- Established policies for personally-owned devices
- Sold expensive office space and created world-wide mobility centers
- Launched small, focused “opt-in” BYOD pilots. Resisted the urge to “boil the ocean”
- Embraced collaboration and social media tools to allow mobile devices to stay connected

A highly diverse workforce:

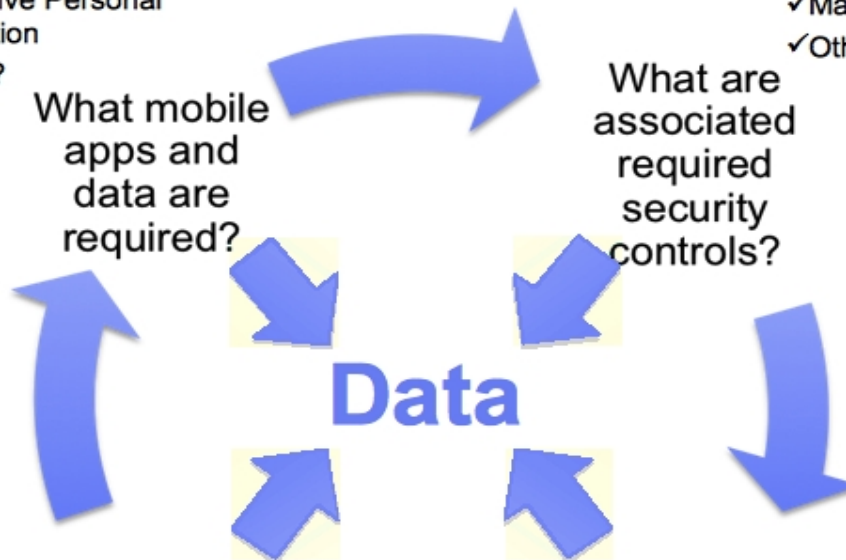
- 425,000 employees worldwide
- 50% workforce has less than 5 years of service
- 50% of employees work remotely – not from a traditional IBM office
- 71% of employees are outside the US

IBM started by asking four questions....



- ✓ eMail
- ✓ Contacts
- ✓ Calendar
- ✓ Intranet Access
- ✓ Sensitive Personal Information
- ✓ Other?

- ✓ Security Policy
- ✓ Password
- ✓ Device Timeout
- ✓ Disk Encryption
- ✓ Malware Protection
- ✓ Other?



- Blackberry
- Windows Mobile
- Symbian
- iOS
- Android

What platforms are desired?

What additional mobile controls?

- ✓ Data Wipe
- ✓ Device Kill
- ✓ Other?



Then executed based on segmentation

Approach

h

Identified Personas



Determine key IT services necessary for employees to do their jobs

13 Personas based on the IT requirements of IBMers



Determine the environment and attitude of employees

Customer facing IBMer

IBM office based employee



Cluster employees with similar IT requirements and work locations in groups

Growth market employee in a global support role

Work at home employee (non-traveller)



Validate IT requirements and employee segments through a survey or user interviews

Manufacturing and other non-traditional office employees

Employee with a basic software and application need



Map segments to traditional HR demographics such as Job Role and Business Unit

Researcher, SW and HW development engineer with a high end workstation requirement

Employee with accessibility requirements



Use employee segments to identify targets for new technology deployments

Employee with low technology adoption attitude score

Employee in a leadership or executive role

Employee with a high technology adoption attitude score

Frequent traveller – non customer facing (e.g. Education, internal auditor etc)

Employee joining through an acquisition (Before systems integration)



Endpoint Management Convergence Matters....

- Why does this matter?
 - Cost
 - Compliance and reporting
 - Enablement of role-based security management

- Proliferation of tactical mobile security tools and point products
 - Served purpose
 - Ultimately inefficient and complex

- Consistency across all endpoints
 - Tablets and smartphones are really just computers
 - Same data at risk
 - Extend security standards → Roles → Configuration policies



Our own IBM Endpoint Manager technology now delivers a unified systems and security management solution for all enterprise devices



Unix / Linux Servers

Android / iOS / Symbian /
Windows Phone devices

Windows & Mac
Desktops/Laptops

Windows Mobile / Kiosks /
POS devices

Supporting more devices...

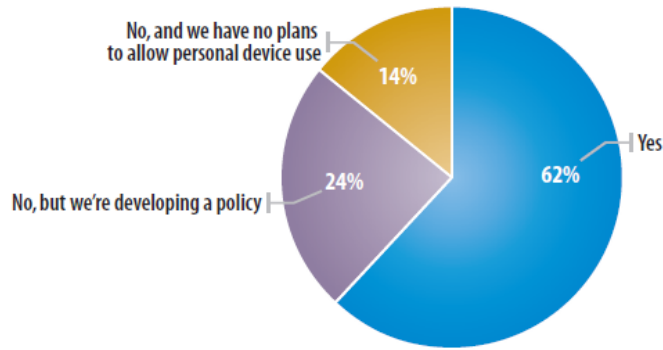
...and more capabilities.

| | | | |
|--------------------|---------------------|----------------------|--------------------|
| Device Inventory | Endpoint Protection | S/W Use Analysis | |
| Patch Mgmt | Power Mgmt | Security Config Mgmt | Mobile Device Mgmt |
| Configuration Mgmt | Remote Control | OS Deployment | |

Final point on BYOD: It's a Spectrum....

Policy on Personal Mobile Device Use?

Does your mobility policy allow employees to use personal mobile devices for work?

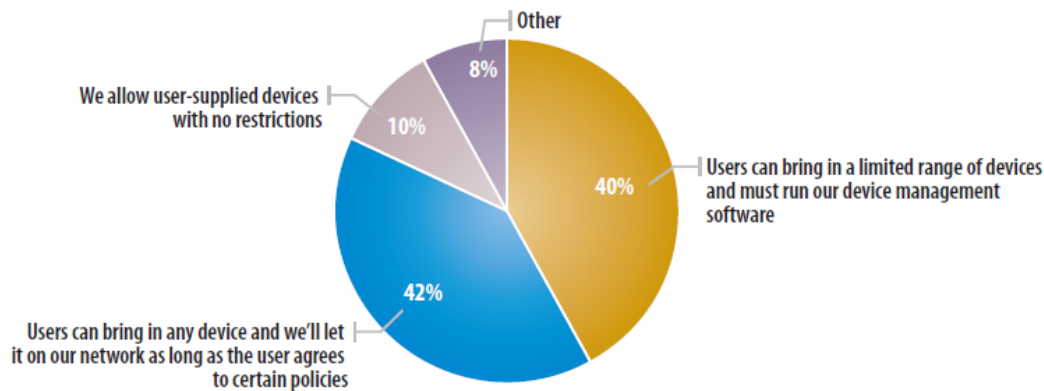


Data: InformationWeek 2012 Mobile Security Survey of 322 business technology professionals, March 2012

R4720512/3

Personal Mobile Device Policy

Which of the following best describes what is or will be your policy on acceptable user-supplied devices?



Base: 278 respondents at organizations with, or developing, a policy for personal mobile device use.

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

R4720512/4

Employees will use their own devices in the workplace anyway

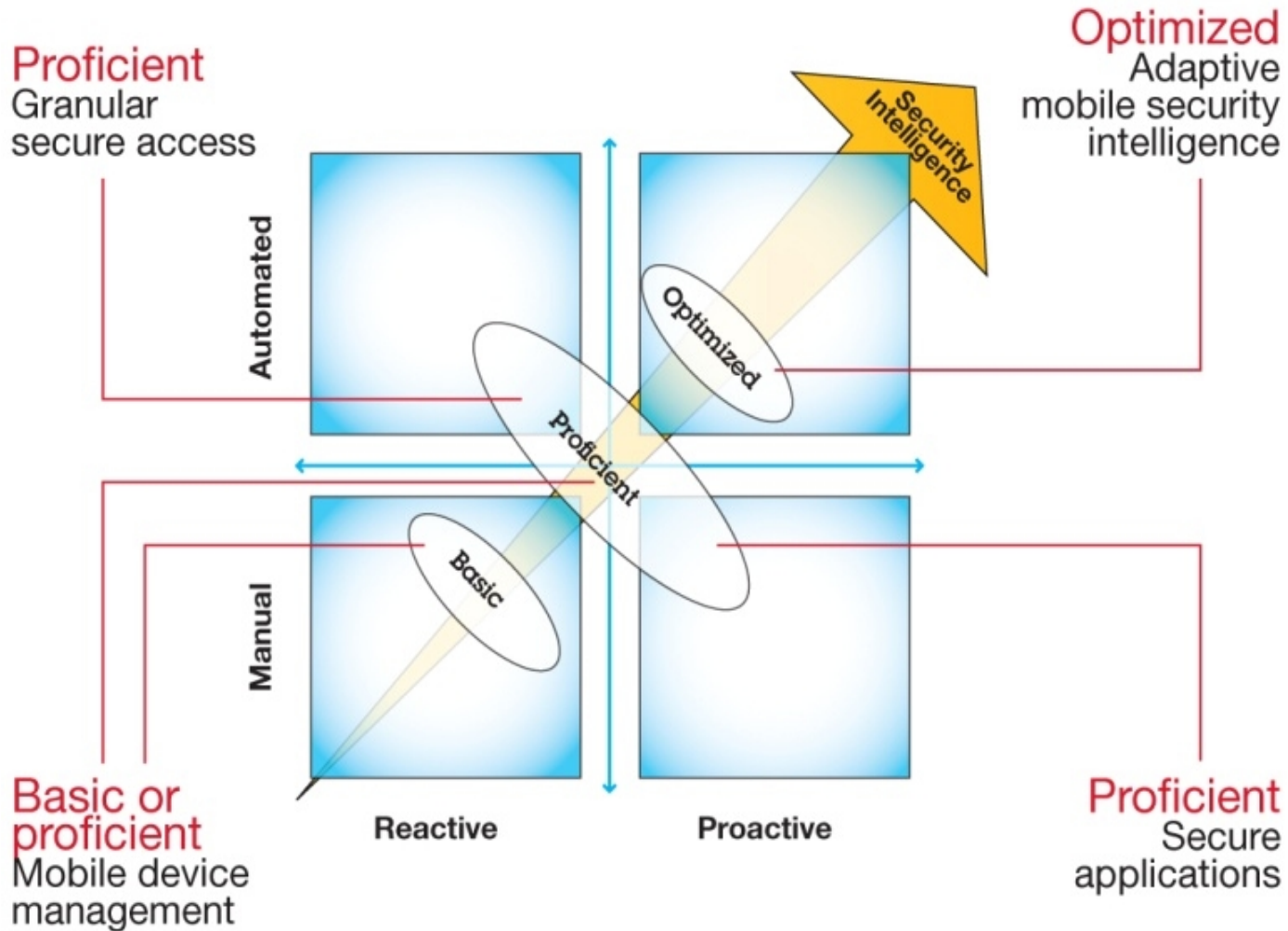
So, organizations have to start on the BYOD journey by establishing policies that meet their current operational objectives

Policies can evolve as an organization and its employees better understand the risks as well as the benefits.

BYOD programs vary across organizations, industries and regions

*95% of organizations have policies in place for mobile devices. However, less than one in three employees are aware of their company's mobile security policy**

How Can You Get Started with Enabling Your Workforce...



Gaining Visibility Over Mobile Devices



Mobile platforms and the apps they support are diverse. The state of the devices users employ are highly dynamic



Mobile devices evolving into the primary interaction channel for many users

Without visibility over these new devices employed for business use organizations might not fully understand the threat surface area or be able to advise employees

Increased malicious targeting of mobile devices via apps, and web content may lead to attacks on the corporate network or infection of corporate systems



Users have on average more than 1 mobile device. Corporate data may reside on these devices.



Dramatic increase in the number of devices an organization needs to manage

Data loss as a result of lost or stolen devices as well as employee turnover can carry tremendous business costs

Savings from not purchasing the devices and cost of managing each device may be eroded by the scale of devices that need to be managed

Unique Requirements for Secure Mobile Access



Mobile users prioritize user experience and make device decisions based on their preferences

Imposing access security controls and methods that are unsuited for mobile can either lead to non-compliance or non-participation



Mobile devices are most often used outside the corporate network and consumers may employ a wide variety of networks to access their accounts

The integrity of the user's transactions or communication can be compromised while they are interacting with mobile apps



Mobile devices are shared and can have multiple personas

Authenticating and authorizing just the user OR just the device might not provide necessary levels of controls on data and apps



The context in which mobile devices can change dramatically from one session to the next

The context can significantly influence the risk of the interaction and without proper consideration can lead to data loss or leakage

Mobile Apps: New Security Challenges



In addition to IT, Line of Business teams (i.e. Marketing) are building mobile apps ad hoc to seize market opportunities or serve growing demand



An enterprise cannot reproduce all the apps demanded by employees so will need to support third-party apps

Lack of security understanding and structured development processes may introduce significant risks

App creators may have different security standards or have not performed security testing



New technologies for building native, hybrid and web apps for mobile



Mobile apps often employ multiple collaborative techniques and channels

New vulnerabilities, different types of exploits and susceptibility to old attacks being discovered

Multiple interaction points are exposed to threat vectors

Need for Intelligence...



Targeted attacks at individuals, organizations or specific regions are growing in sophistication and frequency



Emerging threats are evolving, and new sets of vulnerabilities being uncovered

The development of counter measures is inhibited by a lack of awareness of the attack since it may require monitoring across various security solutions



Increased governmental regulation and competitive pressures

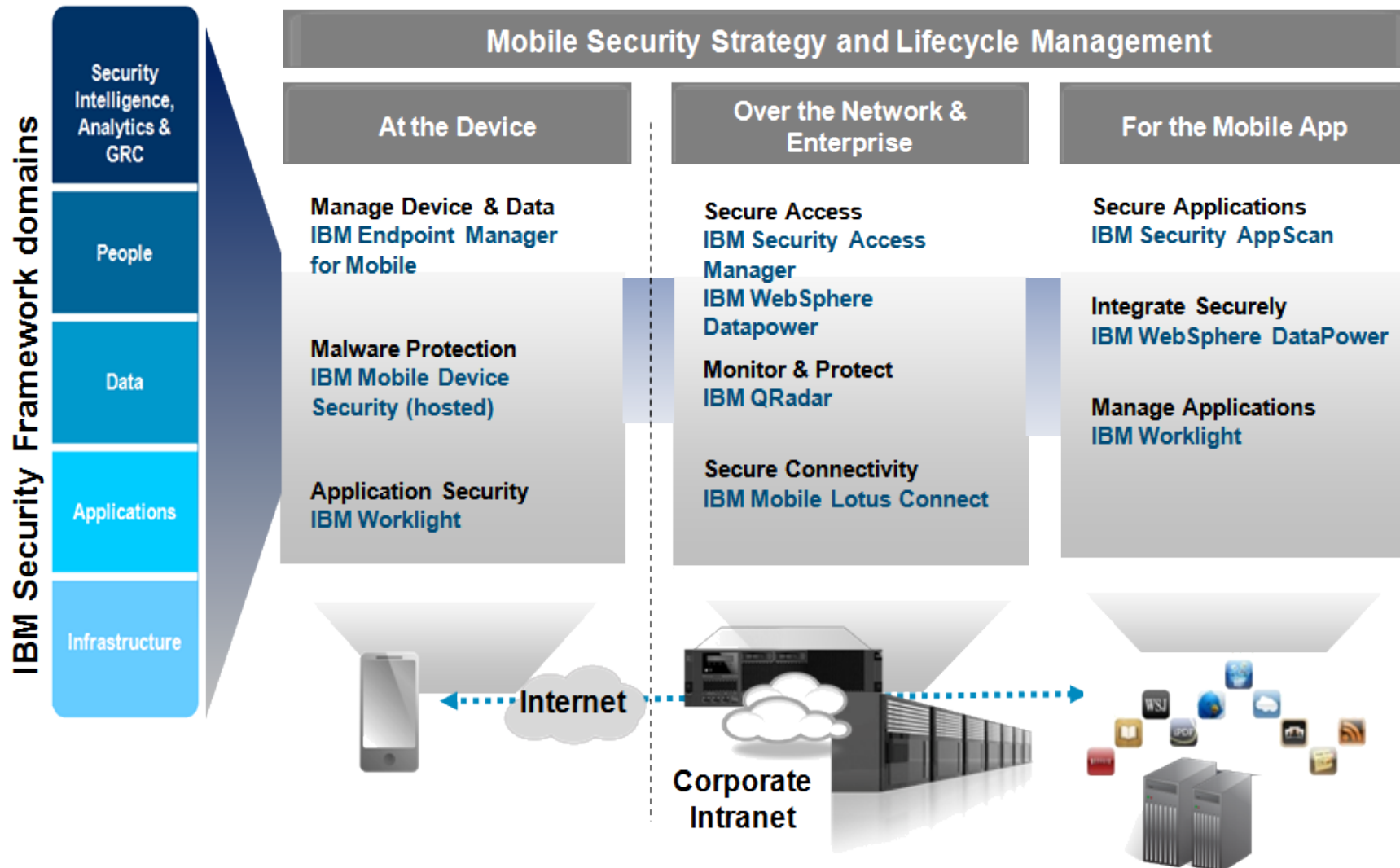


The dynamic mobile ecosystem is inherently social and consumer oriented with each new capability introducing new interaction mechanisms

The penalties for security breaches are not only monetarily expensive but it could result in the loss of trust relationships with customers, partners and employees

User behavior deemed risky from an enterprise security perspective might be practiced without awareness

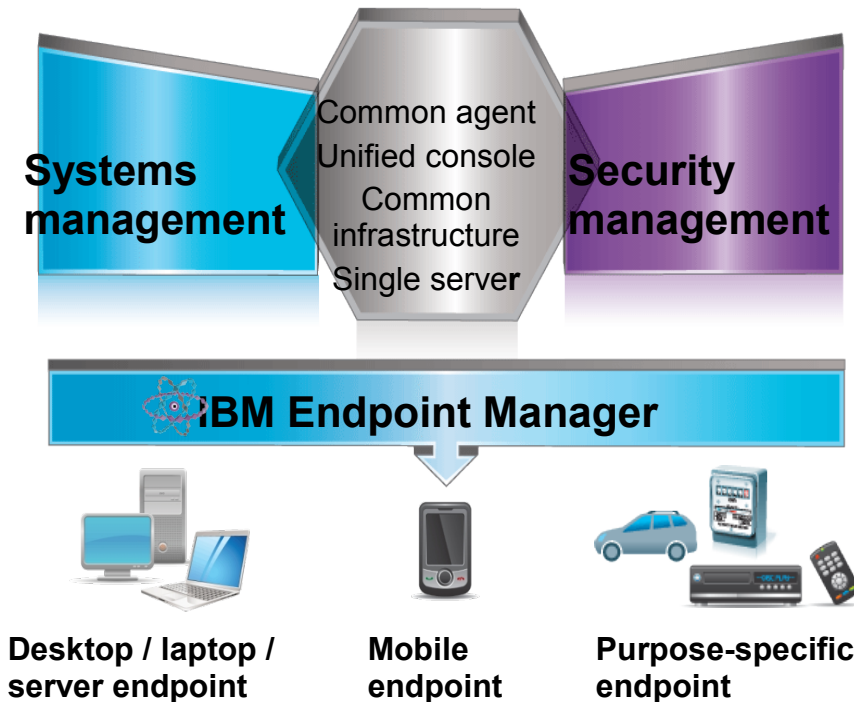
Securing the Mobile Enterprise with IBM Solutions



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

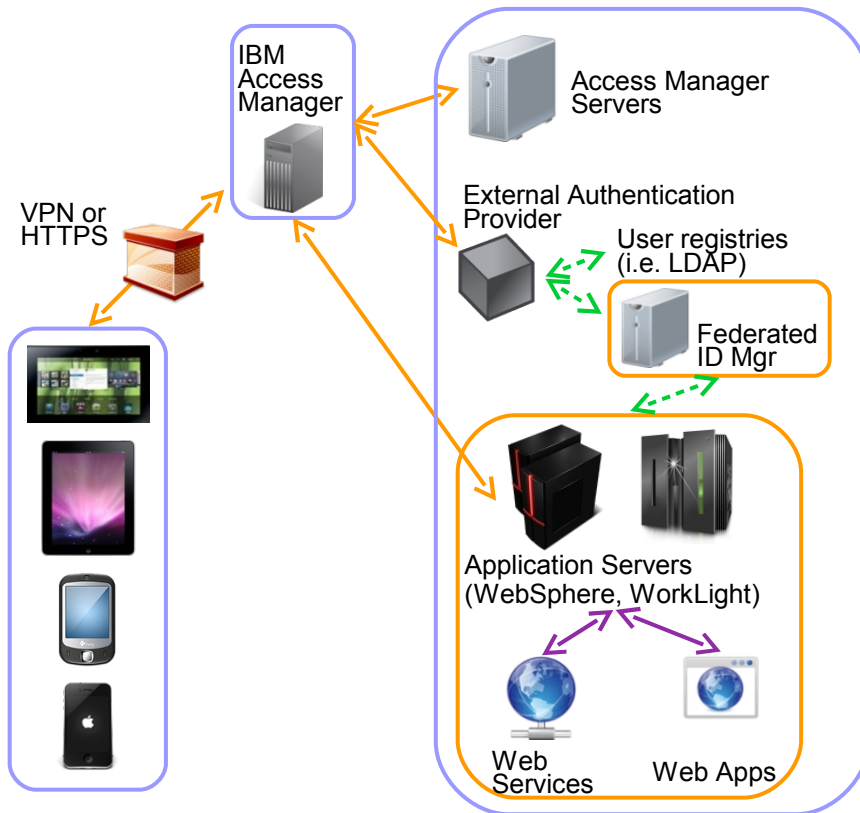
Managing and securing enterprise and BYOD mobile devices without additional resources

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

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 Access Security

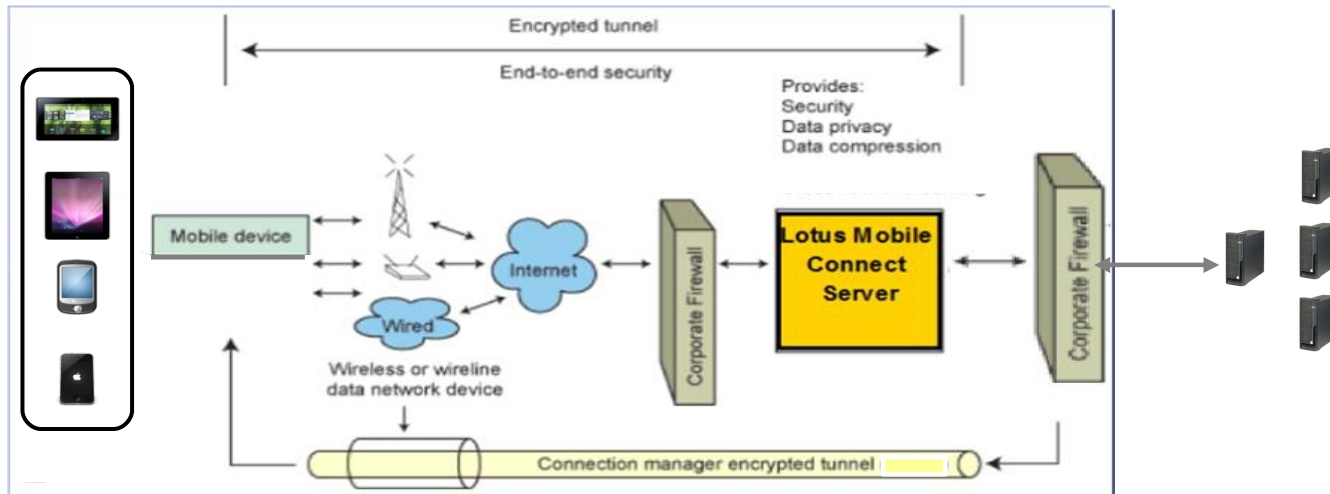
IBM Lotus[®] Mobile Connect: Provides features that help deliver a security-rich connection to enterprise resources from mobile devices.

Client Challenge

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

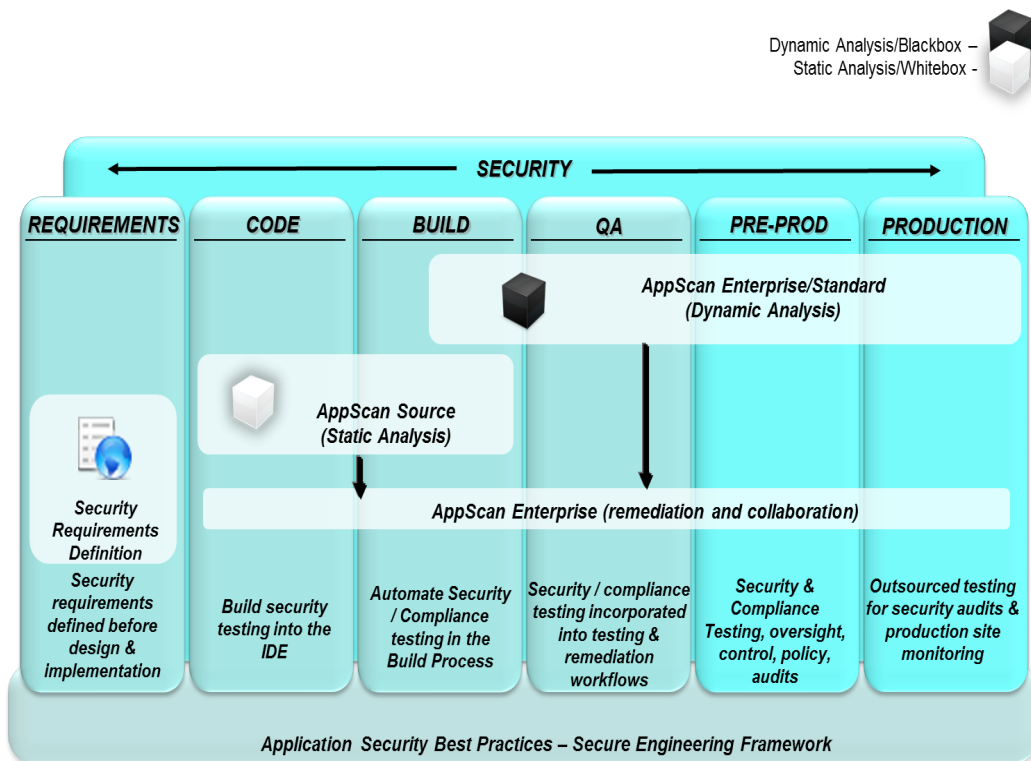
Key Capabilities

- 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



Mobile App Security

AppScan: app security testing and risk management



Client Challenge

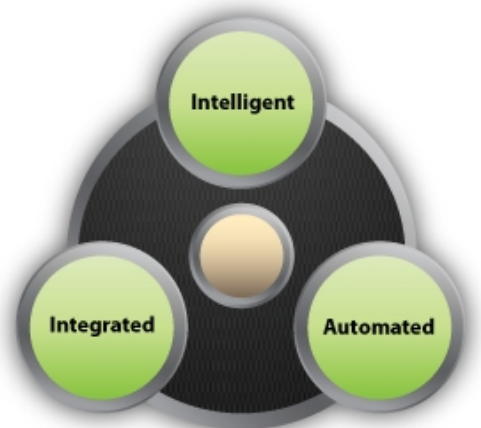
Applying patches and resolving application vulnerabilities after apps are Delivered and Deployed is a very costly and time consuming exercise

Key Capabilities

- Leverage AppScan for vulnerability testing of mobile web apps 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

Mobile Security Intelligence

QRadar: Deliver mobile security intelligence by monitoring data collected from other mobile security solutions – visibility, reporting and threat detection



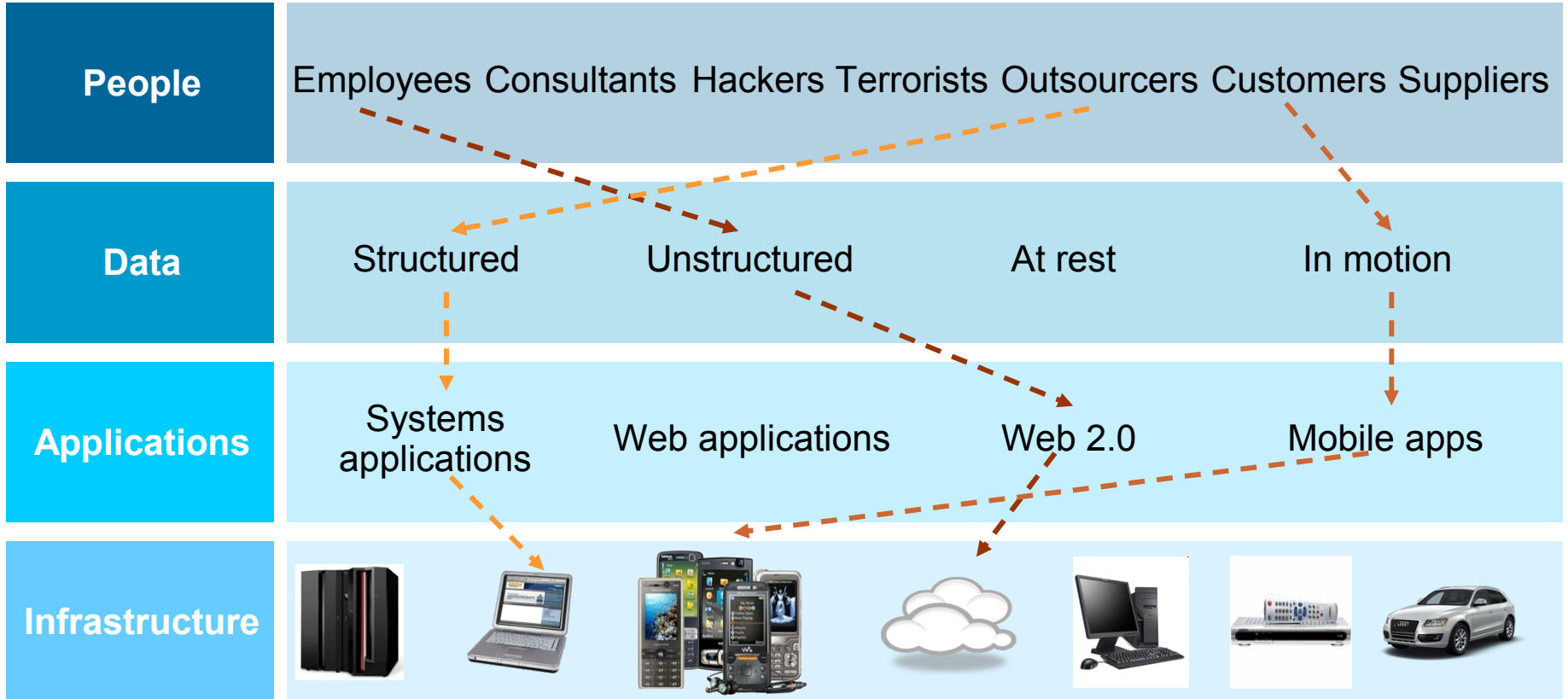
Client Challenge

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

Key Capabilities

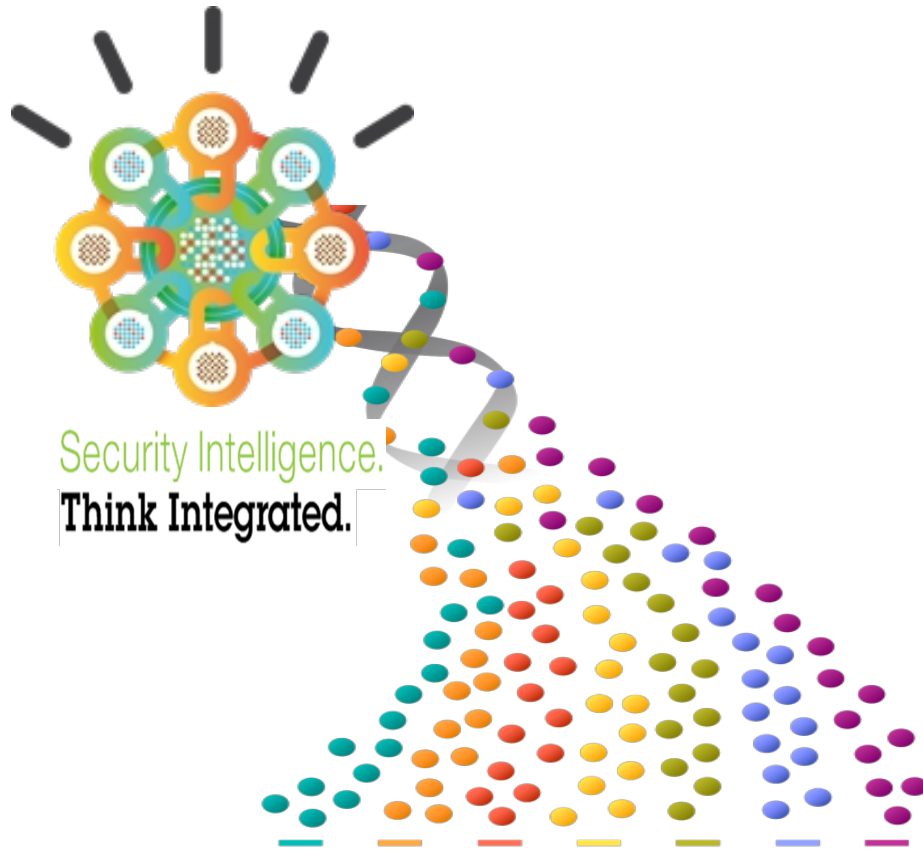
- Integrated intelligent actionable platform for
 - Searching
 - Filtering
 - Rule writing
 - Reporting functions
- A single user interface for
 - Log management
 - Risk modeling
 - Vulnerability prioritization
 - Incident detection
 - Impact analysis tasks

Mobile endpoints are part of Enterprise Threat management



While tactically we may treat them as unique, its all about the data, so strategically they should be put into enterprise context

IBM's Intelligent solutions provide the DNA to Secure a Smarter Planet



Security Intelligence.
Think Integrated.

Darren Argyle *CISM CISSP*
WW Security Solutions Market Leader



darren.argyle@uk.ibm.com



0774 0830210



twitter

[@D_Argyle](#)
[@ibmsecurity](#)
[@instituteAdvSec](#)

Thank You !



ibm.com/security