

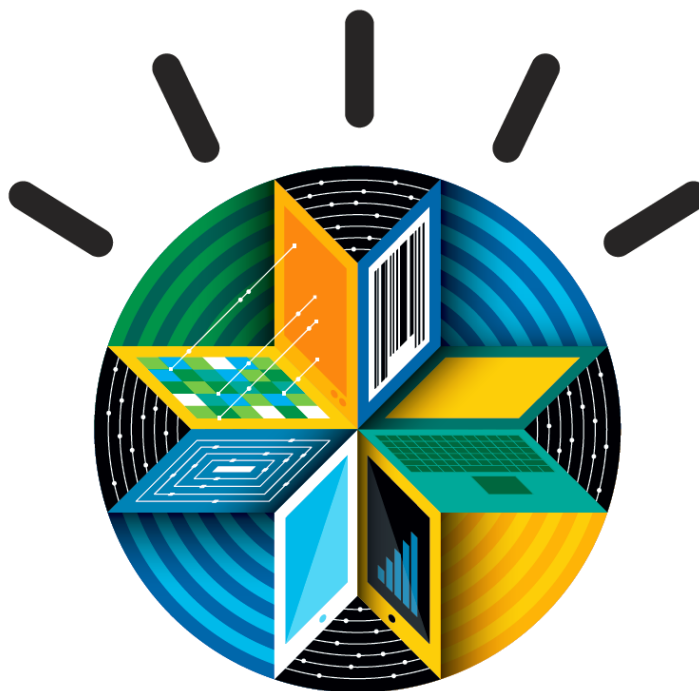


Neil Warburton

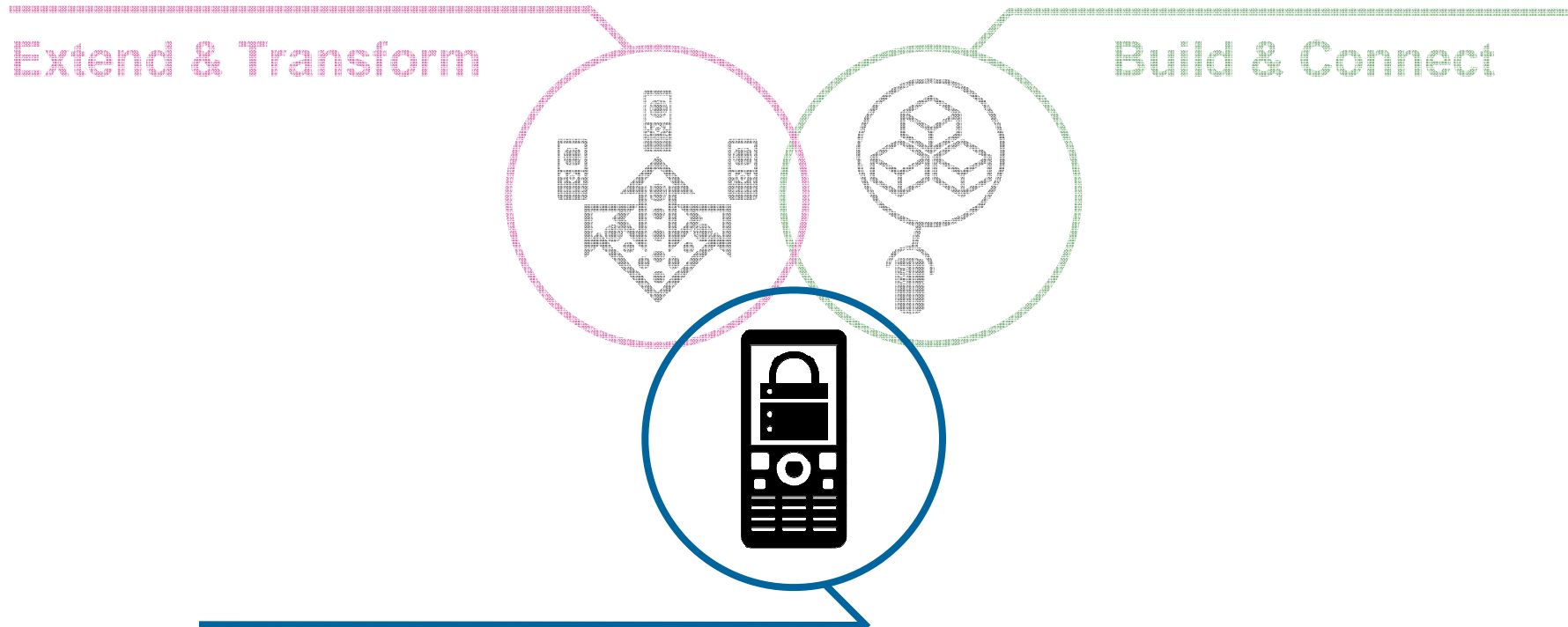
Security Architect, IBM Security Systems

Infosecurity Europe April 2013

Manage & Secure Your Mobile Enterprise: *Delivering Visibility & Confidence*



A deeper look at **Manage & Secure** capabilities



Manage & Secure

Manage mobile devices, services and applications

Secure my mobile business

Key Capabilities

- Mobile lifecycle management
- Device analytics and control
- Secure network communications & management

Mobile Devices: Unique Management & Security Challenges

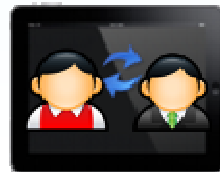
Mobile devices are shared more often

- 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 organization
- Security profile per persona?



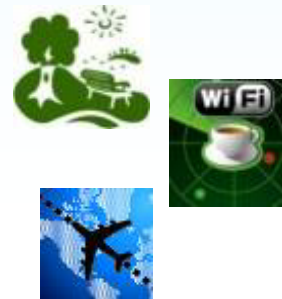
Mobile devices are diverse

- OS immaturity for enterprise mgmt
- BYOD dictates multiple OSs
- Vendor / carrier control dictates multiple OS versions



Mobile devices are used in more locations

- A single location could offer public, private, and cell connections
- Anywhere, anytime
- Increasing reliance on enterprise WiFi



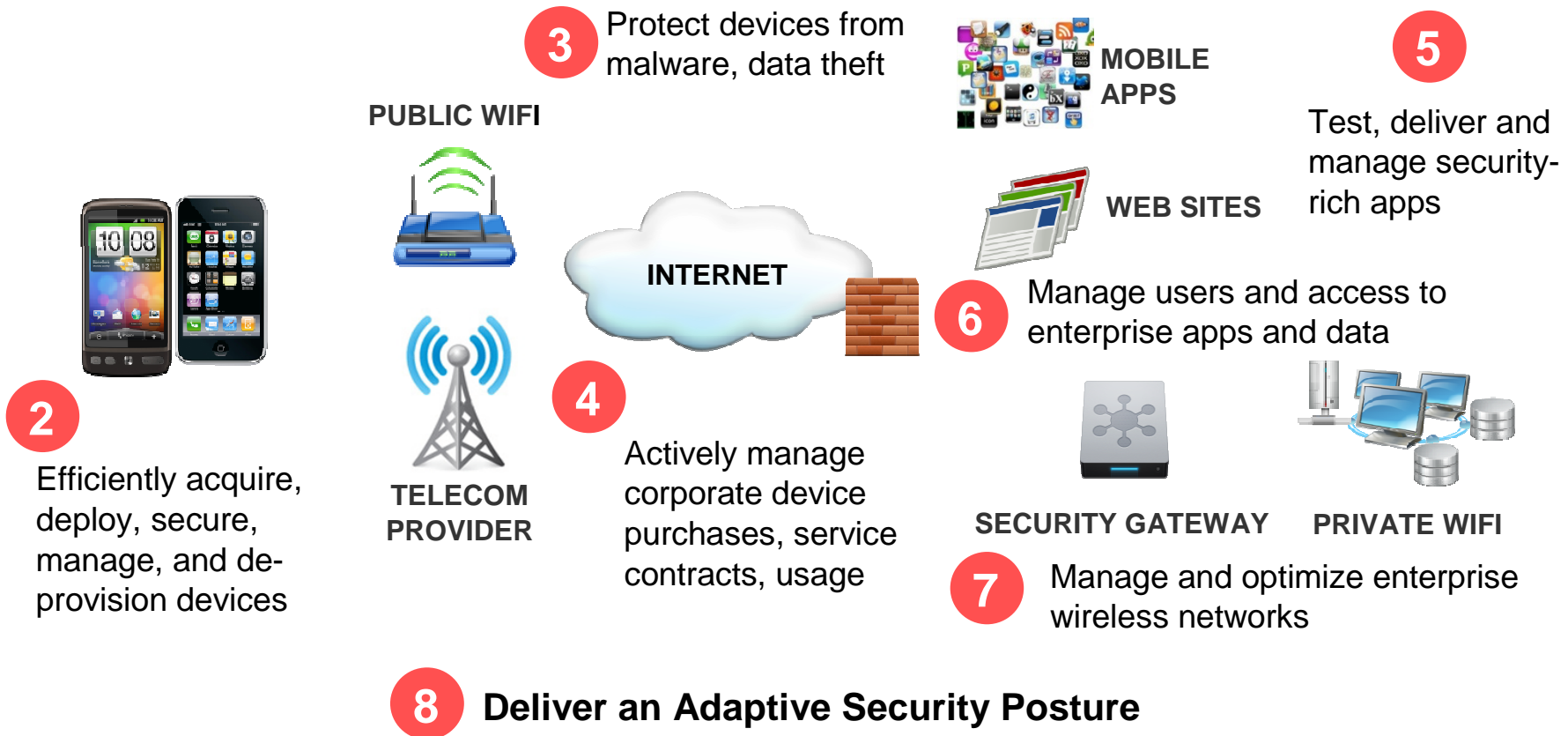
Mobile devices prioritize the user

- Conflicts with user experience not tolerated
- OS architecture puts the user in control
- Difficult to enforce policy, app lists



A Holistic Approach to Managing & Securing the Mobile Environment

1 Develop and Communicate Formal Mobile Strategy, Policies





Solutions for Managing & Securing the Mobile Environment

1 Develop and Communicate Formal Mobile Strategy, Policy *Global Business, Technology, & Security Services*

Issue: Mobile devices have been growing in their importance to employees and partners for over a decade, ahead of an enterprise-wide strategy, resulting in an inconsistent approach from department to department.

IBM: Brings together a unique combination of business advisory, technology, and security services with the right software solutions to help clients devise and implement the most appropriate strategy for their organization

2 Device Lifecycle *IT Operations*

Issue: Frequent turnover increases asset management, service desk, security costs

IBM: Reduce total cost of ownership (TCO) with integrated device management, self-service capabilities that automates the complete device lifecycle

3 Data Protection *IT Security*

Issue: Mobile malware up 155%¹, small device used everywhere, user-centric OS architecture all increase security risk

IBM: Prevent infections, data loss with hosted or on-premise mobile anti-malware + MDM

4 Cost Management *Finance*

Issue: Unmanaged device & service plan procurement, incorrect billing and inventories results in overpayment

IBM: Reduce mobile costs by up to 35% through integrated asset, procurement, and expense management solutions



Solutions for Managing & Securing the Mobile Environment

<p>5 Security-rich Apps <i>App Dev / R&D</i></p> <p>Issue: Lack of deep security knowledge in development and test teams results in application vulnerabilities</p> <p>IBM: Eliminate most app vulnerabilities during the dev cycle with automated, integrated development and testing tools</p>	<p>6 Authenticated Access <i>IT Security</i></p> <p>Issue: Devices that are easily lost or borrowed, insecure data connections increases unauthorized access risks</p> <p>IBM: Ensure only authorized users and devices are connected to enterprise resources and that data is encrypted in transit.</p>	<p>7 Network Optimization <i>Network Operations</i></p> <p>Issue: Increased load, dependency on corporate wireless networks</p> <p>IBM: Improve uptime, problem resolution time with the only solution that combines data from roaming endpoints with deep network mapping and access point monitoring</p>
<p>8 Deliver an Adaptive Security Posture <i>Security Intelligence and Analytics</i></p> <p>Issue: lack of Visibility of security events across the enterprise, to stay ahead of the threat and respond to real time threats</p> <p>IBM: provides fully integrated security intelligence from monitoring data and enterprise event collection</p>		



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 VP CIO

Customer Needs

- Support BYOD for a variety of mobile platforms securely for a highly mobile population
- Scale to hundreds of thousands of devices

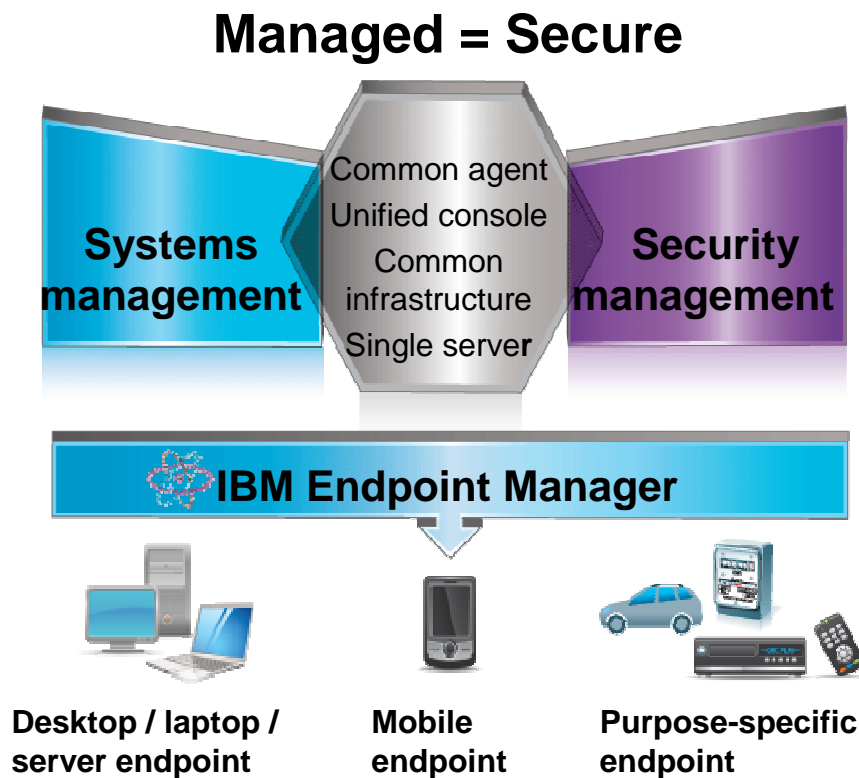
Key Features & Outcomes

- 120,000 mobile devices, 80,000 personally owned, supported in months
- Integrated Lotus Traveler, IBM Connections, IBM Sametime, and IBM Endpoint Manager

Device Lifecycle, Data Protection 2 3

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 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



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

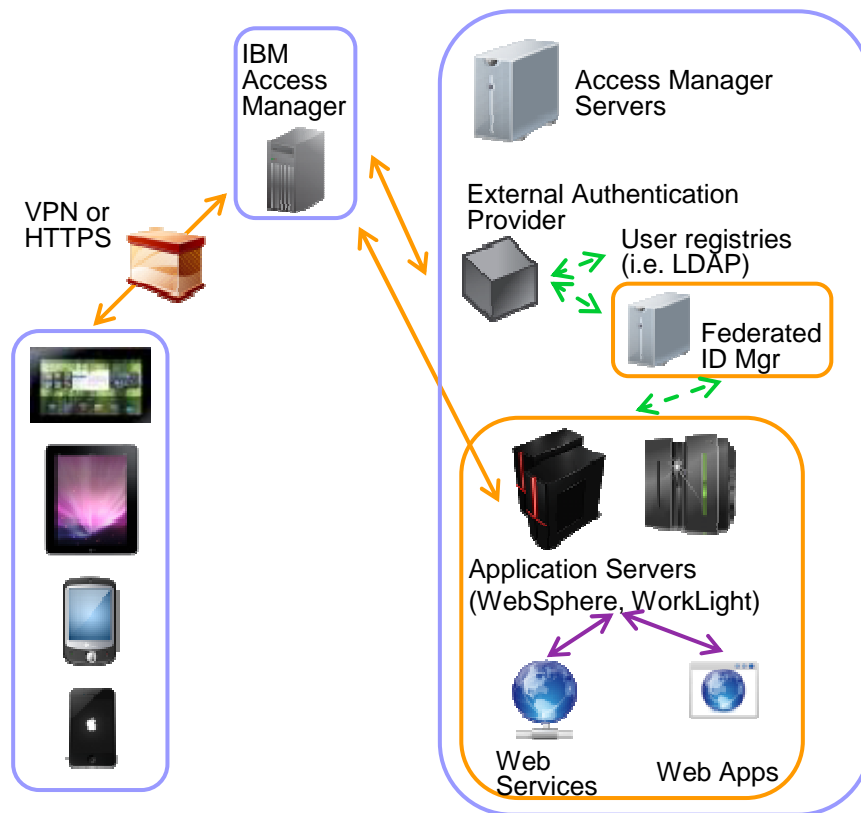
Key Features & Outcomes

- Scalability to 250,000 endpoints provides room to grow
- Added mobile devices to existing IEM deployment in days
- Ability to integrate with Maximo, Remedy
- Responsiveness and agility of product and product team

User Management & Access 6

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 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

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 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

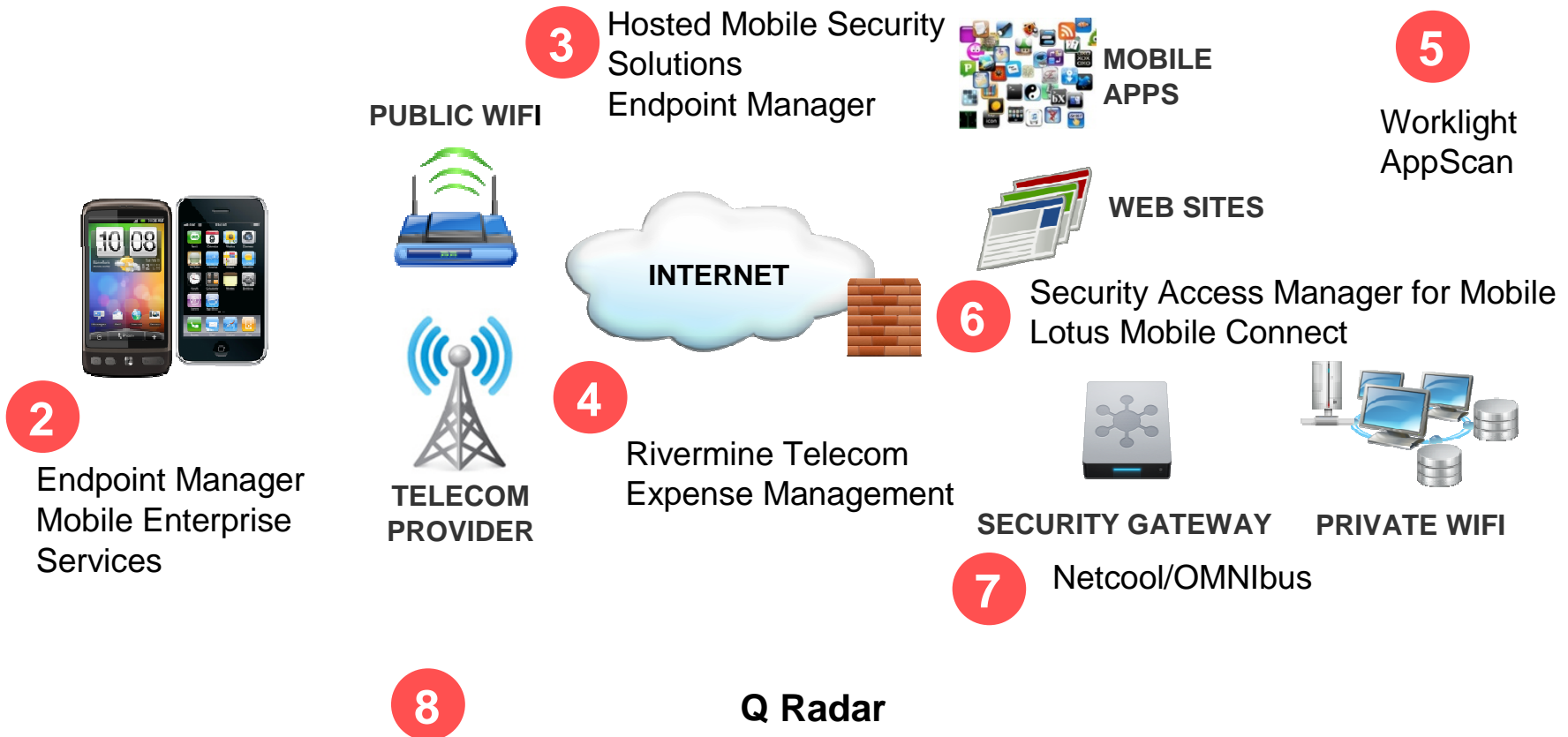
- Extend secure access to banking apps to mobile customers
- Enhance productivity of employees to perform secure banking transactions via mobile devices
- Support for iOS, Android, and Windows Mobile

Key Features & Outcomes

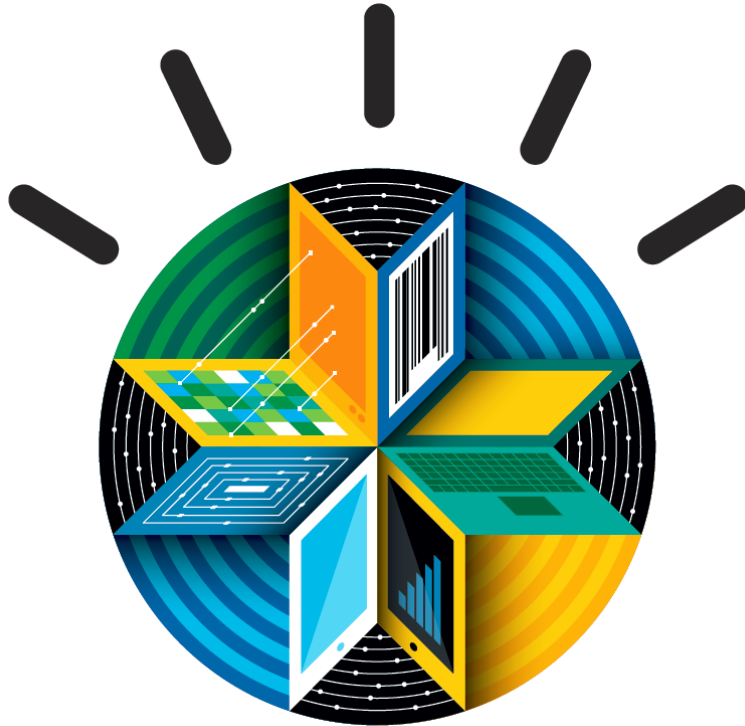
- Authenticates requests made via HTTPS from hybrid mobile apps running on WorkLight platform to back-end services
- A custom certificates-based authentication mechanism implemented to secure back-end banking application

A Holistic Approach to Managing & Securing the Mobile Environment

1 IBM Global Business, Technology, & Security Services



Next Steps



- Learn more at:
www.ibm.com/mobile-enterprise
 - Access white papers and webcasts
 - Get product and services information
 - Download and begin using IBM Endpoint Manager
- Talk with your IBM representative or IBM Business Partner to find the right next step for you



Learn more at: www.ibm.com/mobile-enterprise

© Copyright IBM Corporation 2012. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials 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 these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials 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. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

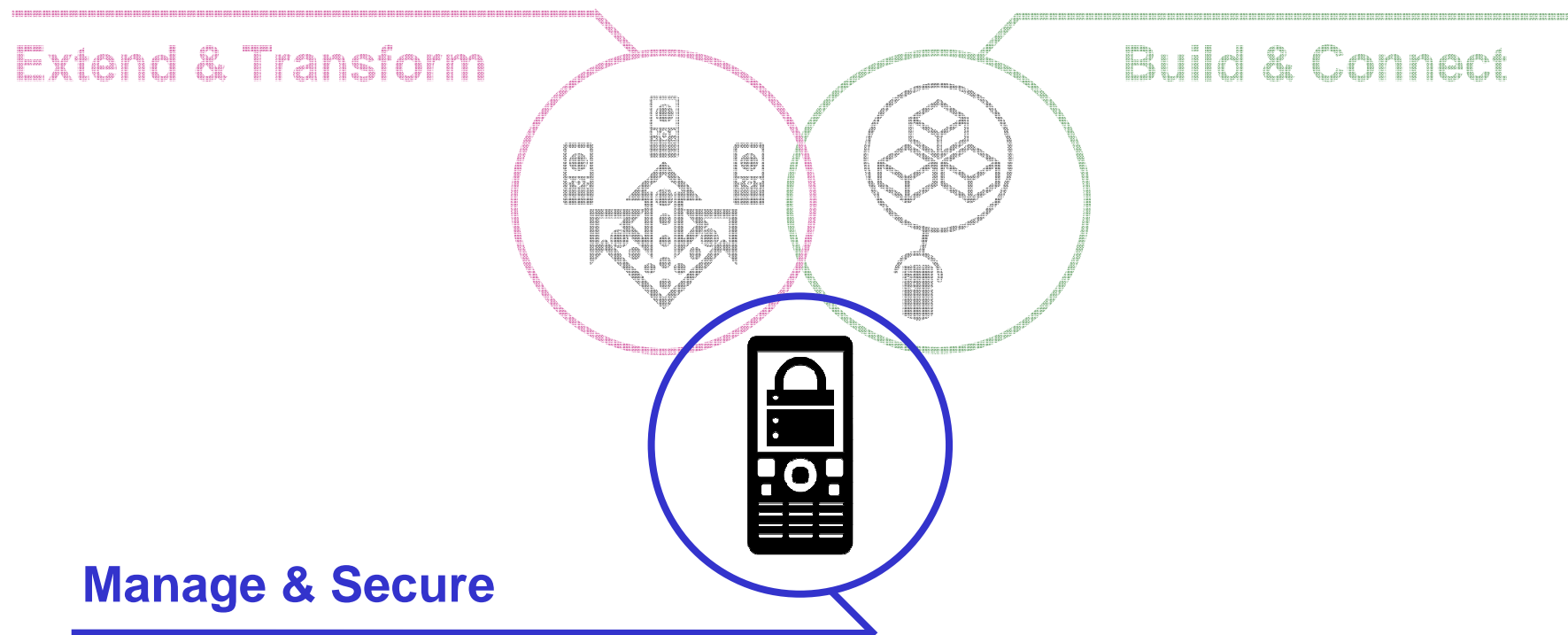


BACKUP

Device Lifecycle, Security, Data Protection Services

IBM Services

From strategy to application platform and development, to device and application management and security, and secure connectivity to the network.



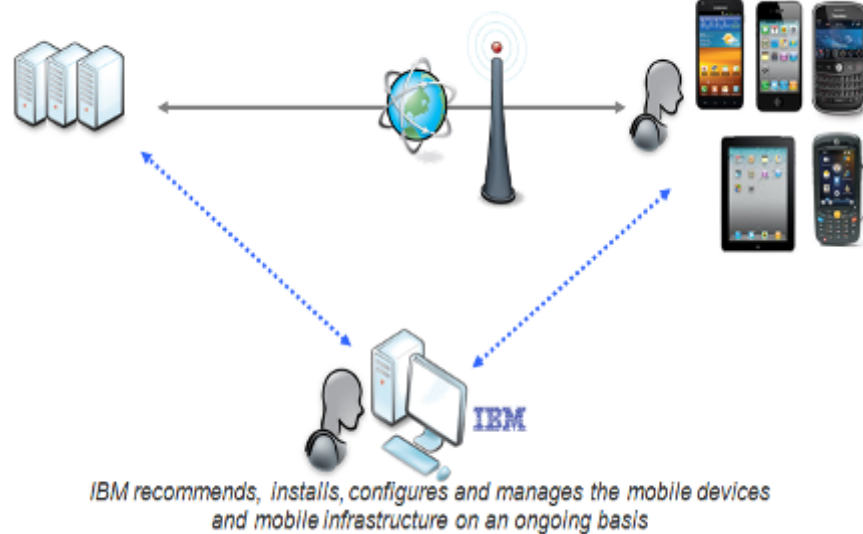
Key Services Capabilities

- Mobile device lifecycle, expense management and help desk
- Cloud-based mobile device security management
- Data and wireless network security
- Mobile application management including native, web, hybrid and virtual applications

Device Lifecycle **2**

IBM Mobile Enterprise Services for Managed Mobility

Managed service for iOS, Blackberry, Android, and Windows Mobile smartphones, tablets, and ruggedized devices.



Client Challenge

Delivering enterprise mobile services to increasing numbers of mobile workers, including BYOD, at less cost than delivering in house

Key Capabilities

- Procurement, staging and kitting
- Mobile device management
- Mobile application management
- Mobile messaging (e.g. Lotus Domino, Microsoft Exchange)
- Help desk services
- Negotiated discounts with leading mobile hardware and software vendors
- Over 15 years world-wide experience

Mobile Endpoint and Data Protection **3**

IBM Hosted Mobile Device Security Management

Turn-key security for employee-owned and corporate-liable mobile devices



Client Challenge

Mobile threat protection without in-house skills or technology to own or manage

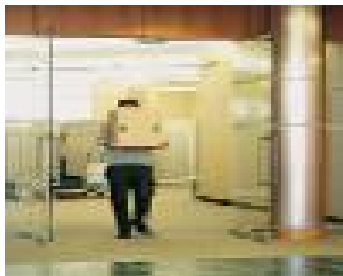
Key Capabilities

- Mobile malware prevention (spyware, viruses, etc.)
- Simple, cloud-based delivery
- Policy compliance monitoring
- Device management and security for Apple, Android, BlackBerry, Windows Mobile, and Symbian devices
- End-user portal to locate/lock/wipe a lost or stolen device

Enterprise Wireless Networks **4** **7**

IBM Mobility & Wireless Network Services

A full lifecycle of project deployment services for enterprise networks: strategy, assess, design, integrate, deploy, maintain, and run



Client Challenge

Secure, robust and high-bandwidth enterprise wireless network to support wireless network services such as voice, video, BYOD and real-time tracking

Key Capabilities

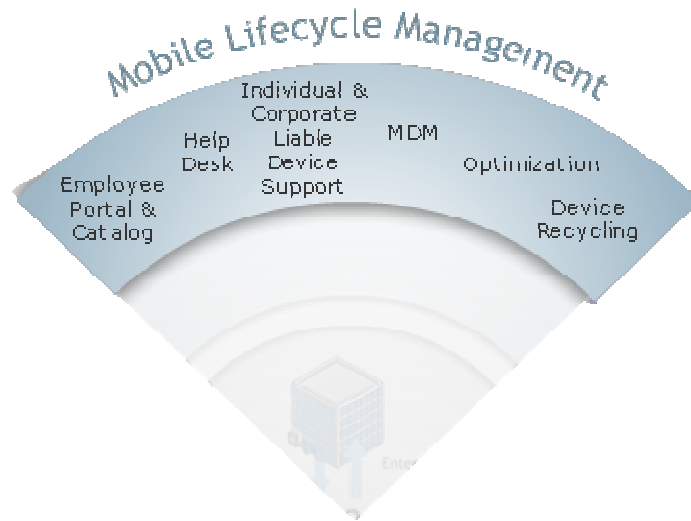
- Wireless Campus Infrastructure and Mobile Connectivity
- Wireless Remote Network Management
- Wireless Network Security
- Wireless Communications and Collaboration
- Real-time Location
- Event-driven Notification



Effectively Manage Mobile Costs **4**

Emptoris Rivermine Telecom Expense Management

Manage, track and optimize mobile spend while ensuring policies are enforced



Client Challenge

Managing rapid proliferation of corporate and BYOD mobile devices to rein in costs and enforce policy compliance

Key Capabilities

- Streamline mobile usage management with end-user portal
- Identify most cost effective rate plan for users with rate plan optimization and auditing
- Accelerate device issue resolution and corporate mobile policy enforcement
- Ensure bill accuracy and prevent overpayments with invoice processing
- Optimize contract costs, terms and conditions
- Personal vs. Business Call Tagging for tax legislation compliance
- Mobile Device Recycling for environmental compliance and possible rebates



Fortune 500 financial services company

Company Overview

- 200,000+ employees
- \$100 billion+ revenue
- Clients in 100+ countries

Business Challenges

- \$300 million in annual telecom spend
- Inability to view various telecom spend categories across business units, carriers and service types, including voice, data, conferencing, and international
- Reconciling contracts with services
- Optimizing telecom infrastructure
- Identifying disconnected services

Results Achieved Using Emptoris

- Cumulative savings of \$125 million over 5 years
- One unified view of the entire telecom spend spectrum
- TEM program viewed as a profit center





Fortune 500 medical supply company

Company Overview

- Leader in healthcare for over 75 years
- 45,000 employees worldwide
- 65 facilities in the US; global presence in over 100 countries

Business Challenges

- Mobile and wireline telecom spend over \$15 million and increasing
- Limited visibility into thousands of mobile devices
- Majority of invoices in paper format allowing for limited visibility and inefficient processes
- Exploding international costs

Results Achieved Using Emptoris

- \$15 million in wireless and wireline spend under management
- Overall savings to date of close to \$4 million
- 5X ROI within 1 year
- Well-defined process for managing the entire telecom lifecycle





Deliver and Manage Safe Mobile Apps 5

IBM 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

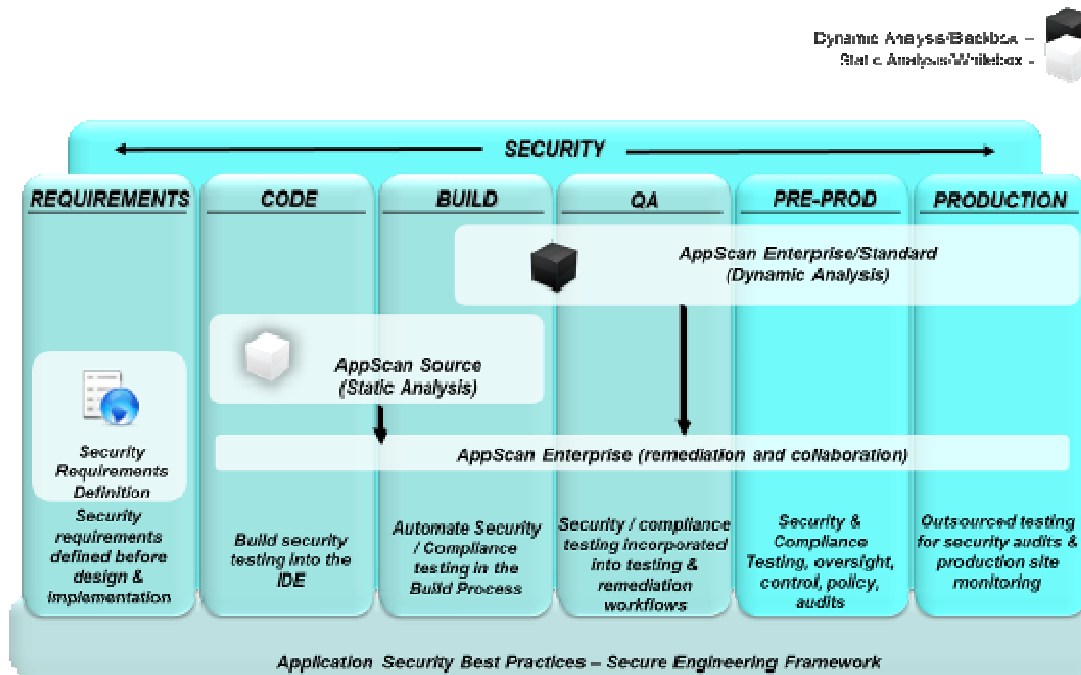
- Integrated secure access to backend application resources
- Secured by design - develop secure mobile apps using corporate best practices, code obfuscation
- Protect mobile app data with encrypted local storage for data, offline user access, app authenticity validation, and enforcement of organizational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



Deliver Security-Rich Apps 5

Appscan

Application security testing and risk management.

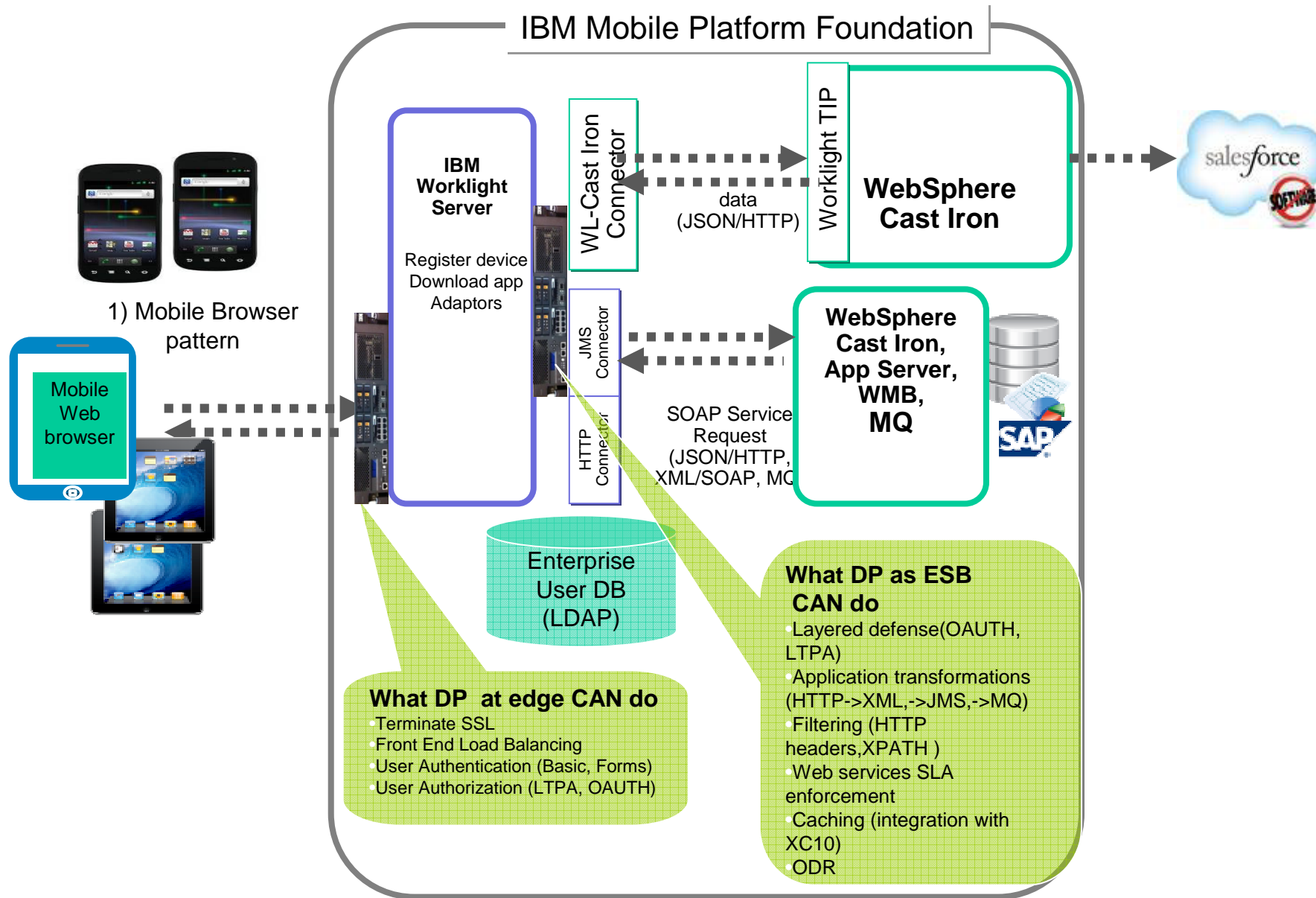


Client Challenge

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



Security-rich Mobile Connectivity 6

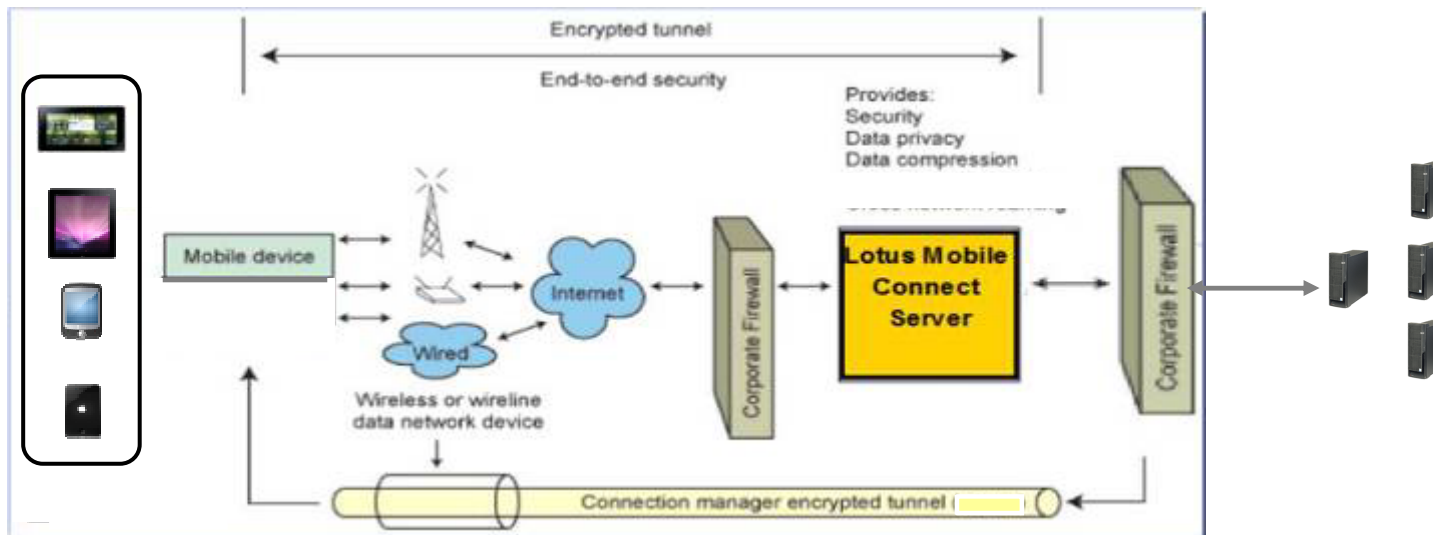
IBM Lotus® Mobile Connect: Provides features that help deliver a security-rich connection to enterprise resources from mobile devices.

Client Challenge

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

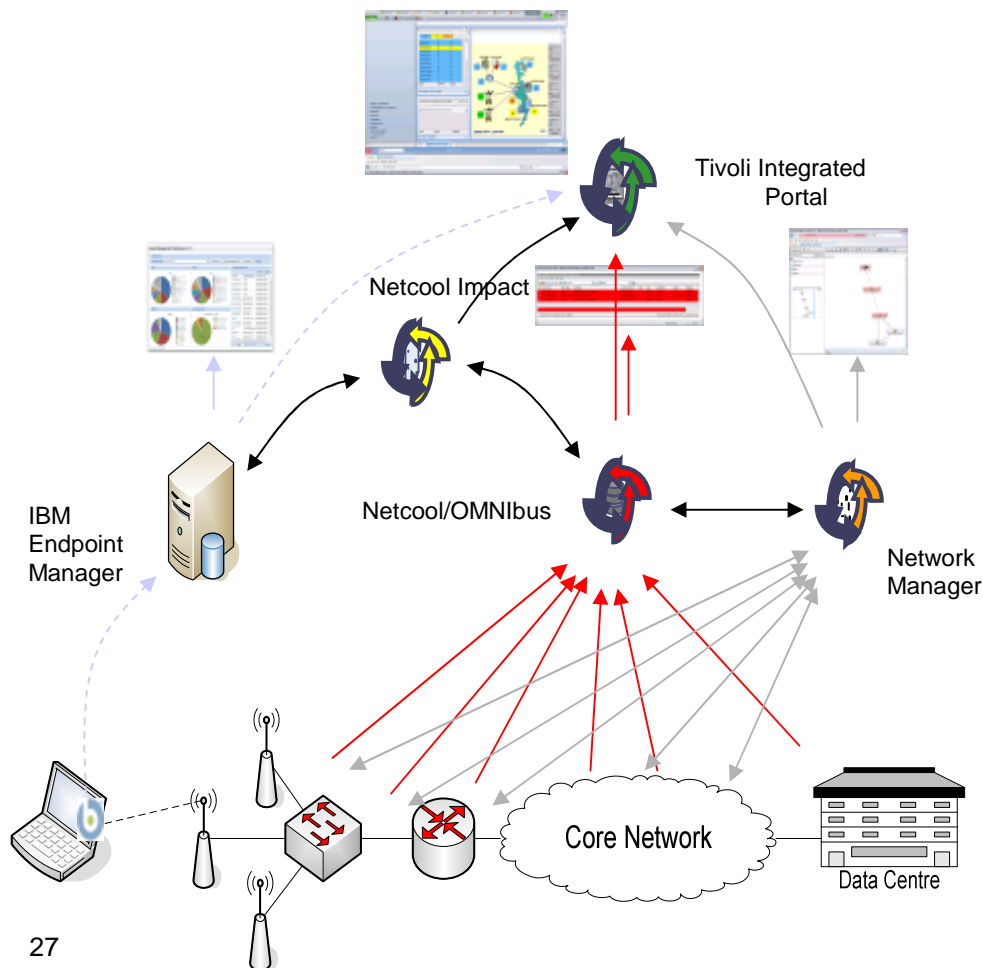
Key Capabilities

- 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



Manage & Optimize Enterprise Wireless Networks 7

Netcool / OMNibus: Operations management software that enables around-the-clock administration and automation of network management tasks for optimal performance and issue remediation



Client Challenge

Show in **REAL TIME** an enterprise wide view of the mobile workforce connecting through public and private networks.

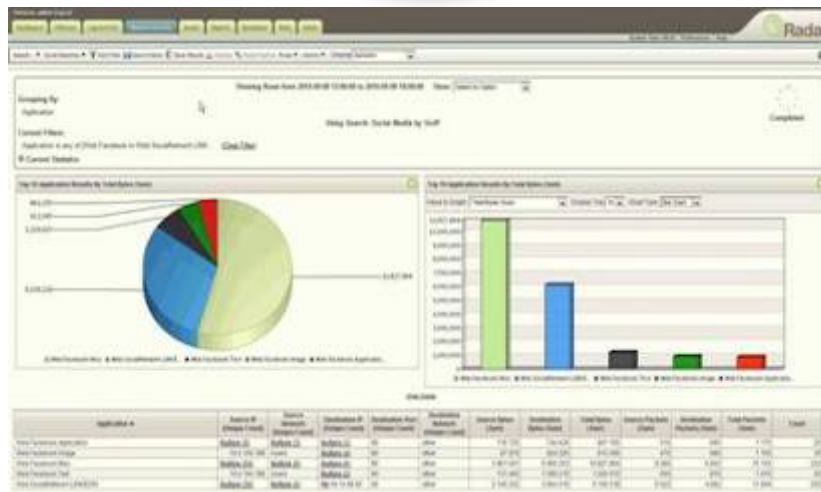
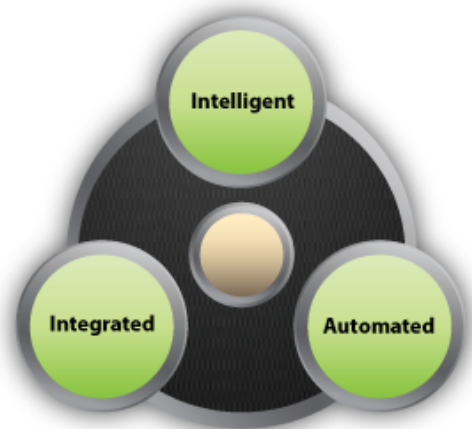
Key Capabilities

- Easily identify the impact of any outages and highlight ongoing issues resulting from a lack of capacity or poor radio signals:
- View current locations and connection point of mobile devices
- Gain visibility of the network and service quality experienced by mobile users
- Management of exceptions reported by IBM Endpoint Manager

Deliver An Adaptive Security Posture 8

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



ibm.com/mobile-security