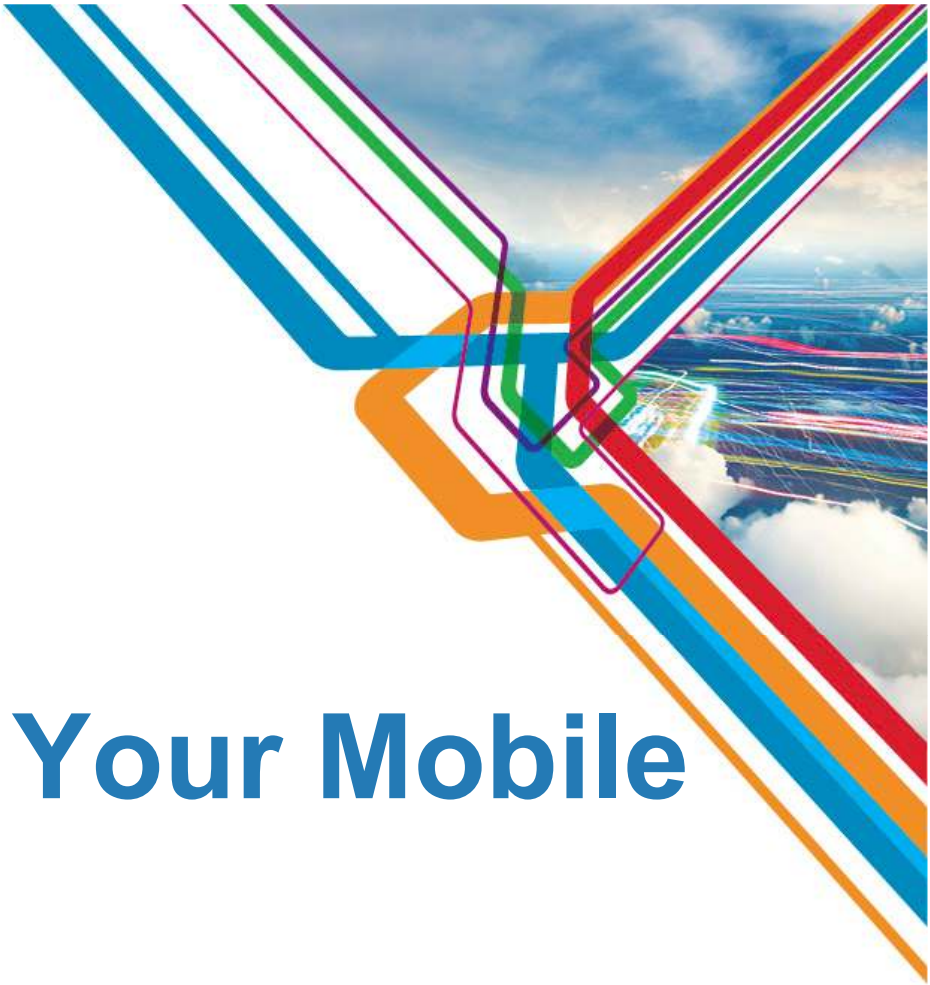
Pulse

IBM SolutionsConnect 2013



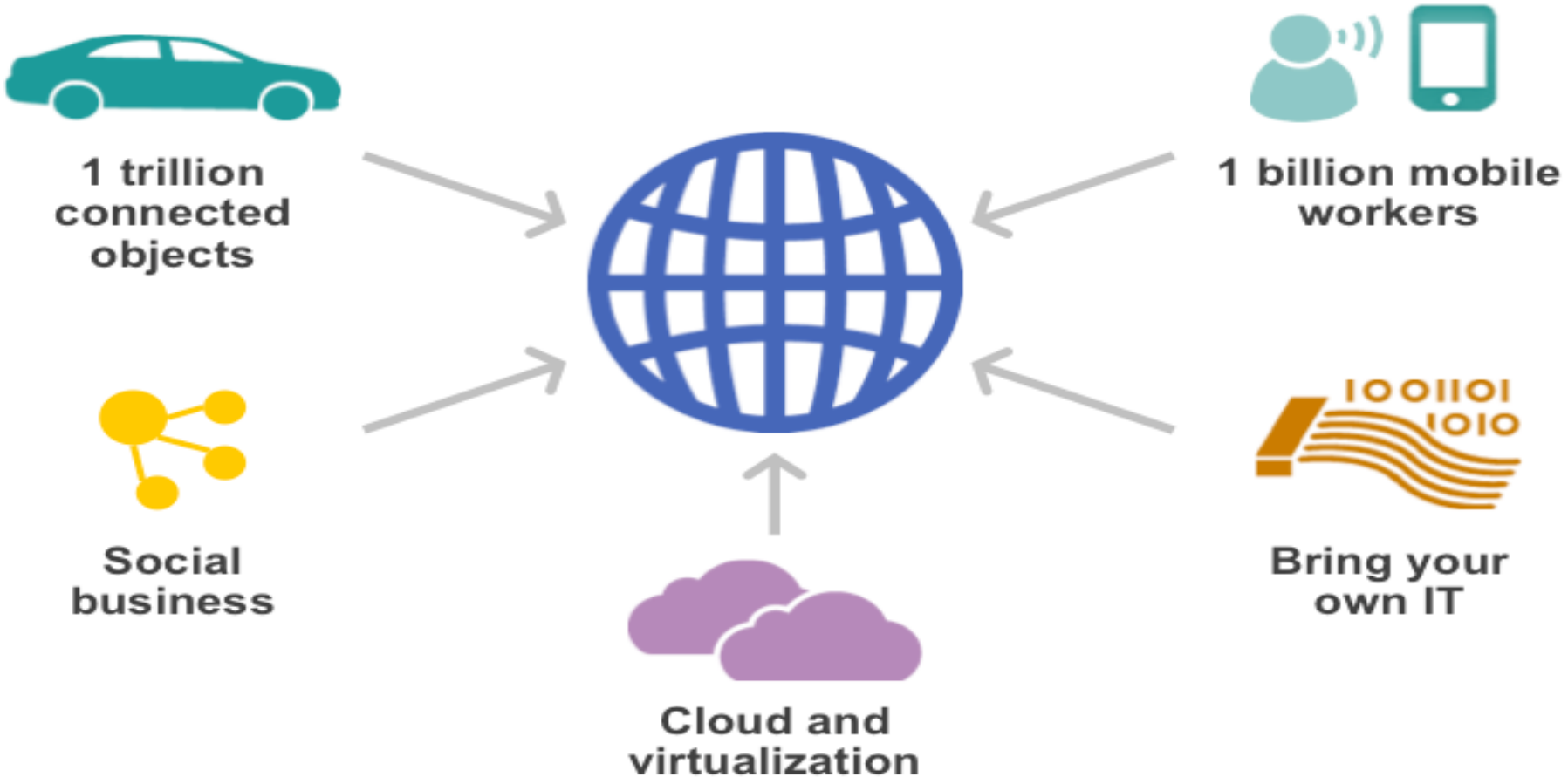
Securing & Managing Your Mobile Environment

Delivering Confidence

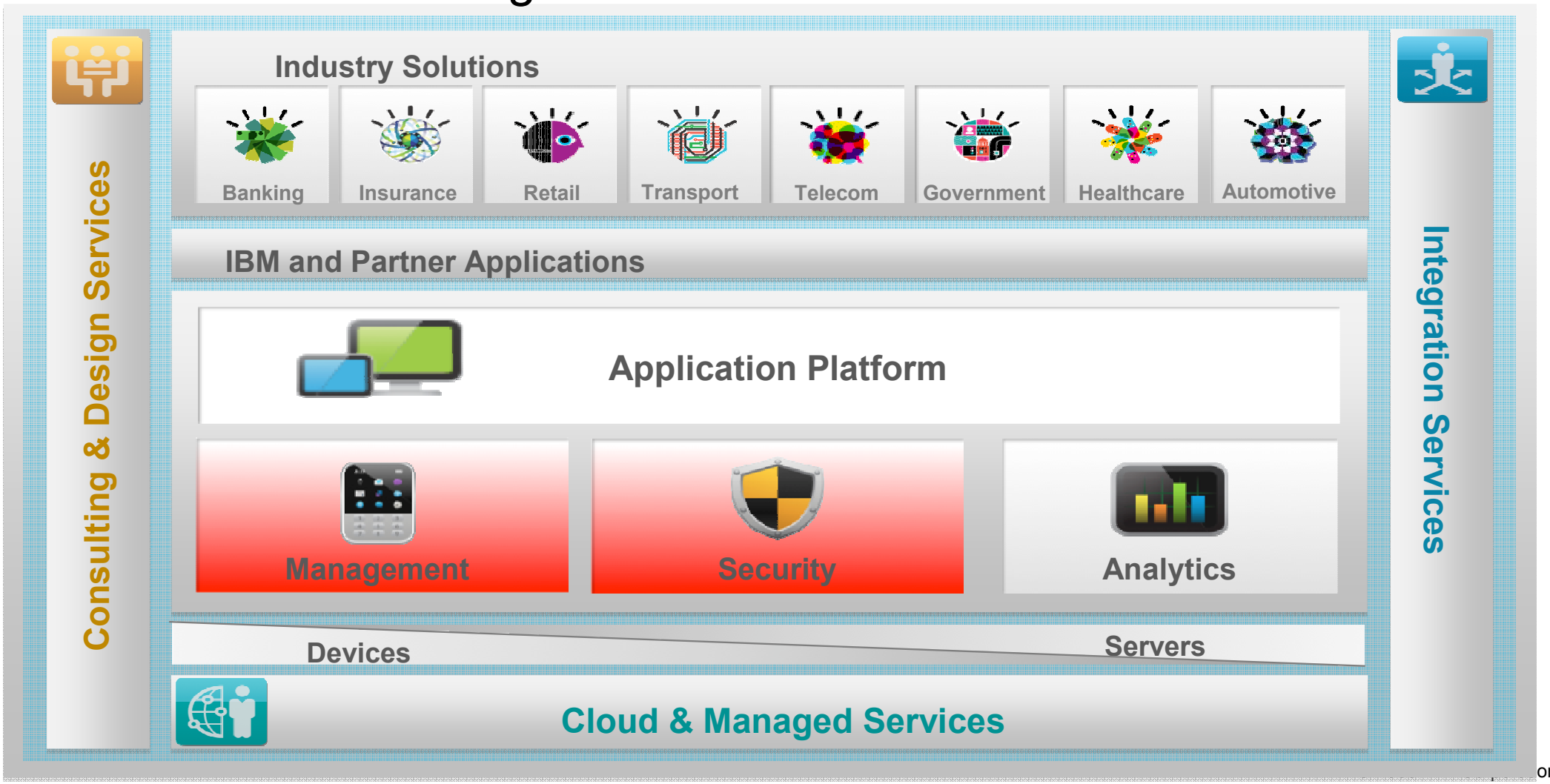
06/13/2013

IBM

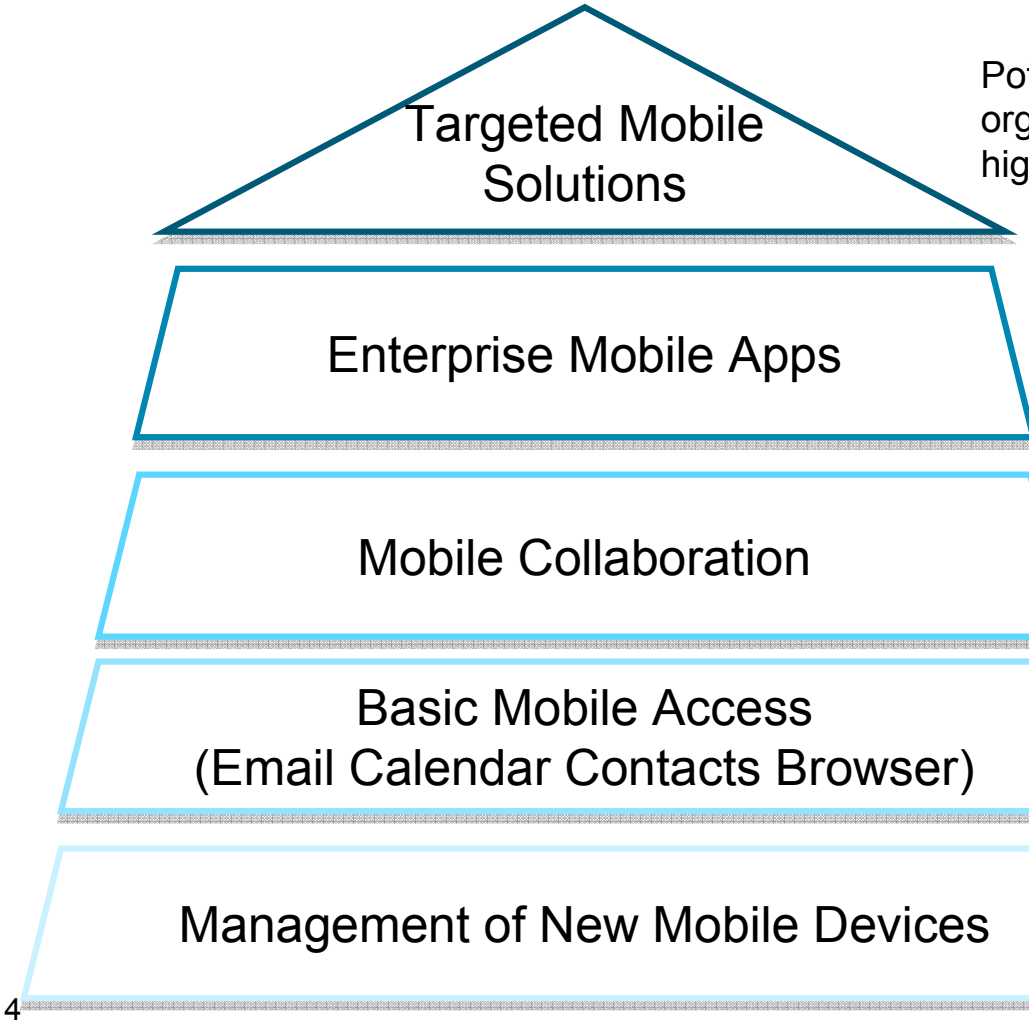
Innovative Technologies Changes Everything



IBM MobileFirst Offering Portfolio



Operational Priorities in Evolving to a Mobile Enterprise



Potential for productivity gains and enhancing employee and organization responsiveness motivating organizations to transform high value processes (i.e. Mobile Payments, Health Monitoring etc)

Mobile as the preferred channel to reach employees and partners encouraging proliferation of mobile business apps

Dynamic work tasks and context-specific interactions promote the use of mobile devices for content collaboration (i.e. messaging, file sharing, etc)

Employees demanding greater mobile access to core productivity tools

Organizations facing an ever increasing influx of consumer mobile devices on the corporate network require visibility over those devices

A Frame of Reference to Structure Your Strategy

Device Management

Security for endpoint device and data

Network, Data, and Access Security

Achieve visibility and adaptive security policies

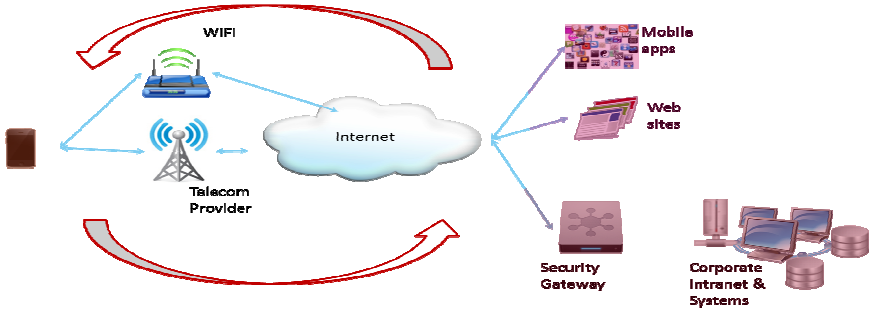
Application Layer Security

Develop and test applications

Mobile Security & Management Focus Areas

Risk based mobile access management

Secure mobile solutions



Mobile Security Intelligence

Tailoring BYOD for an Organization

Degree of Platform & Device Choice: Determine the degree of device choice employees are offered

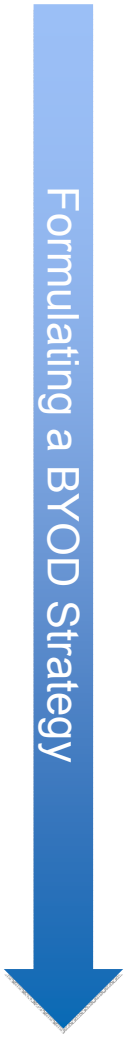
Workforce Demographics by Roles: Assess influence of employee's role on propensity to participate and benefit from a BYOD program.

Documenting Usage Scenarios: Profile risk of a BYOD program, by documenting employees work behavior using personal devices. Will influence the degree of oversight necessary to mitigate the risk.

Identification of Sensitive Data/Content: Enumerate what data or content needs to be accessed and if that content will need to be stored on devices.

Building the Business Case – Cost/Benefit Analysis: Identify hidden costs of BYOD programs that erode the cost savings gained from not having to purchase the devices. An imperative to define metrics that help quantify the business value gained from the program.

Phased Deployment Plan: Formulate a transparent phased deployment of a BYOD program to enable steady buildup of competencies in managing the risk while meeting the demand from its employees.



Granular Risk Assessment for Access Control

Centralized User Management: Assembling singular view of all the mobile users across one or more mobile apps enables for consistent user governance and reduces redundancy and complexity of access control embedded in each app.

Segmenting Mobile Users: Segmenting mobile users based on access privileges allows for better management through tiered access. This practice assists in anomaly detection.

Enumerating Context Attributes: Selection of the contextual attributes that can influence risk when accessing applications and content will facilitate a granular risk assessment of each user interaction.

Defining Access Policies to Govern Risk: Codification of access policies for applications and content allows for greater consistency and logic testing. Externalizing these policies from applications improves the flexibility of the security posture.

Selection of Authentication and Authorization schemes: Organizations can select employing one or more authentication schemes that can builds trust between the organization and the user. Additionally, an organization can decide on multi-factor or step-up authorization schemes to mitigate risk.

Safe Apps as the Basis of Secure Solutions

Establishing a Security Standard: Mobile app development can be undertaken by different parts of the organization or even outsourced, therefore a security quality standard has to be defined which all development efforts can adhere to.

Segregating Security Logic from Business Logic: Security requirements will have less variation than business logic and requires different set of skills. Security features can be developed and leveraged across multiple apps.

Security Analysis of Applications: Mobile apps need to be assessed for their risk exposure – sensitivity of data, usage scenarios etc. This aids in prioritizing and investment of security rigor employed in safeguarding it.

Vulnerability Analysis: Organizations can incorporate vulnerability analysis into the software development cycle and employ it as a tool to educate developers on secure coding practices.

App Management Policies: Active management of applications is required to respond when mobile apps are compromised. This includes defining the update process, conditions when the app will be locked and situations when data stored locally by an app are wiped.

Developing Mobile Security Intelligence

Identifying Sources of Security Events: Organizations can choose to collect security events from a variety of sources to gain broader awareness of evolving threats – i.e. from mobile devices to access requests to mobile apps

Enumerating Reports: Defining templates of reports that will enable security professionals to quickly gain visibility of how well their security posture is performing and demonstrate compliance with corporate policies.

Detecting Anomalies & Risky Behavior: An organization needs to formulate rules that enable it to detect new threats and behaviors that increase its risk profile and may not be covered by existing policies or controls.

Integration to Remediation Process: Remediation makes intelligence actionable so organizations need to plan how detection of security events can be channeled appropriately to take corrective action.

Defense in Depth

IBM

Mobile Security Maturity Model

	Mobile Security Intelligence Risk Assessments, New Threat Detection, Active Monitoring			
Optimized	Integrated management of multiple devices Device Security policy management	Prevent loss or leakage of sensitive information Risk / Context based Access Threat Detection on inbound network traffic	Context / Risk based document collaboration / creating / viewing Enforce restrictions on copy/paste	Multi-factor context aware access and offline access Granular security policy definition and enforcement Enable data sharing based on policy
Proficient	Endpoint Protection with Anti-malware White/black list apps Detection of Jailbreak/rooted devices	Prevent copy and paste of email, calendar, contacts and intranet data Application level VPN	Secure document creation and viewing Document Collaboration with secure file sync / collaboration	App Management – provisioning/updates/disabling Separation of corporate apps from personal apps Application validation
Basic	Update management Device lock / Device wipe Device Registration	Segregated secure access corporate email, calendar, contacts and browser User /device authentication and single sign-on	Connectivity to social networks Secure instant messaging	Enforcing encryption of data within an app App Vulnerability Testing and Certification
	BYOD	**Data Separation**	**Mobile Collaboration**	**Mobile App. Security**

IBM Solutions

IBM MobileFirst offerings to secure the enterprise

IBM Security Framework domains

- Security Intelligence, Analytics & GRC
- People
- Data
- Applications
- Infrastructure

Mobile Security Strategy and Lifecycle Management

At the Device

Manage Device & Data
IBM Endpoint Manager for Mobile

Malware Protection
IBM Mobile Device Security (hosted)

Application Security
IBM Worklight

Over the Network & Enterprise

Secure Access
IBM Security Access Manager
IBM WebSphere Datapower

Monitor & Protect
IBM QRadar

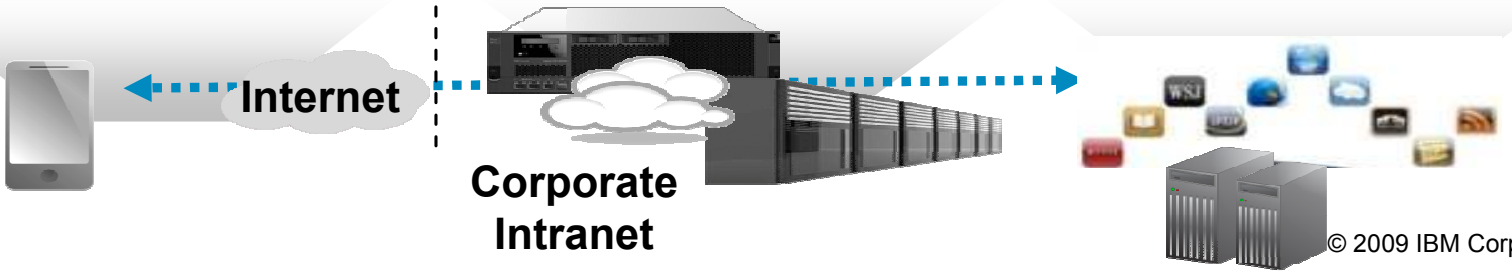
Secure Connectivity
IBM Mobile Lotus Connect

For the Mobile App

Secure Applications
IBM Security AppScan

Integrate Securely
IBM WebSphere DataPower

Manage Applications
IBM Worklight



*A **Mobile First** organization needs…*

Prioritized security and privacy throughout the mobile app lifecycle to protect sensitive business systems

IBM Security AppScan 8.7

What's New

- **Accelerates the use of iOS** in an Enterprise setting
- **Native security scanning of iOS applications** built in Objective C, Java or JavaScript
- **Facilitates a "secure by design" process** in the software development lifecycle for mobile applications
- Addresses requirements for **usage in the US Federal Government**

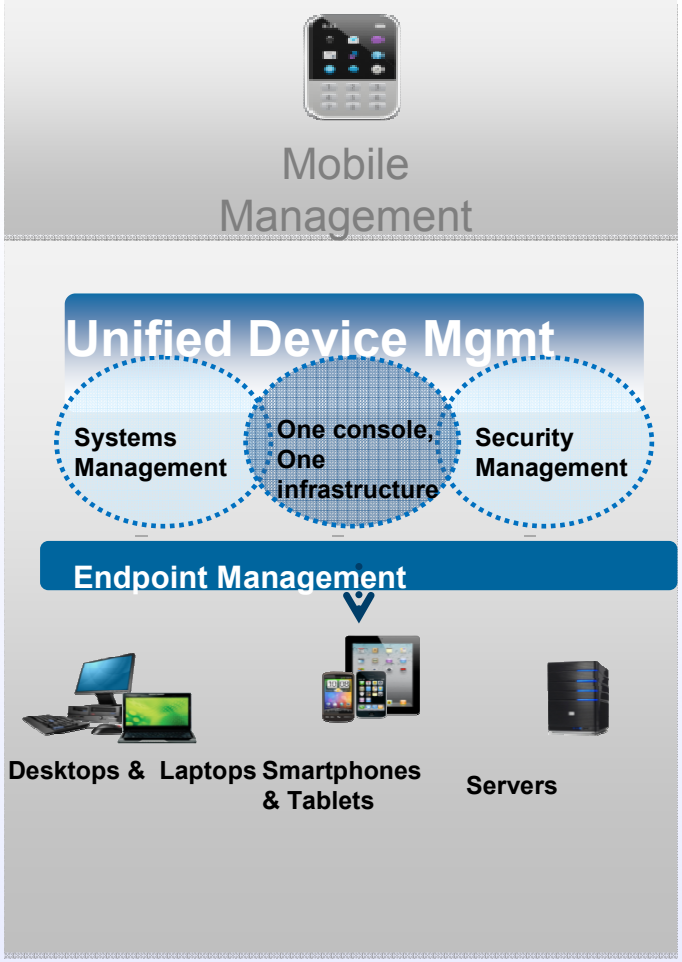
*A **Mobile First** organization needs…*

Real-time visibility and control over all mobile devices

IBM Endpoint Manager for Mobile Devices

What's New

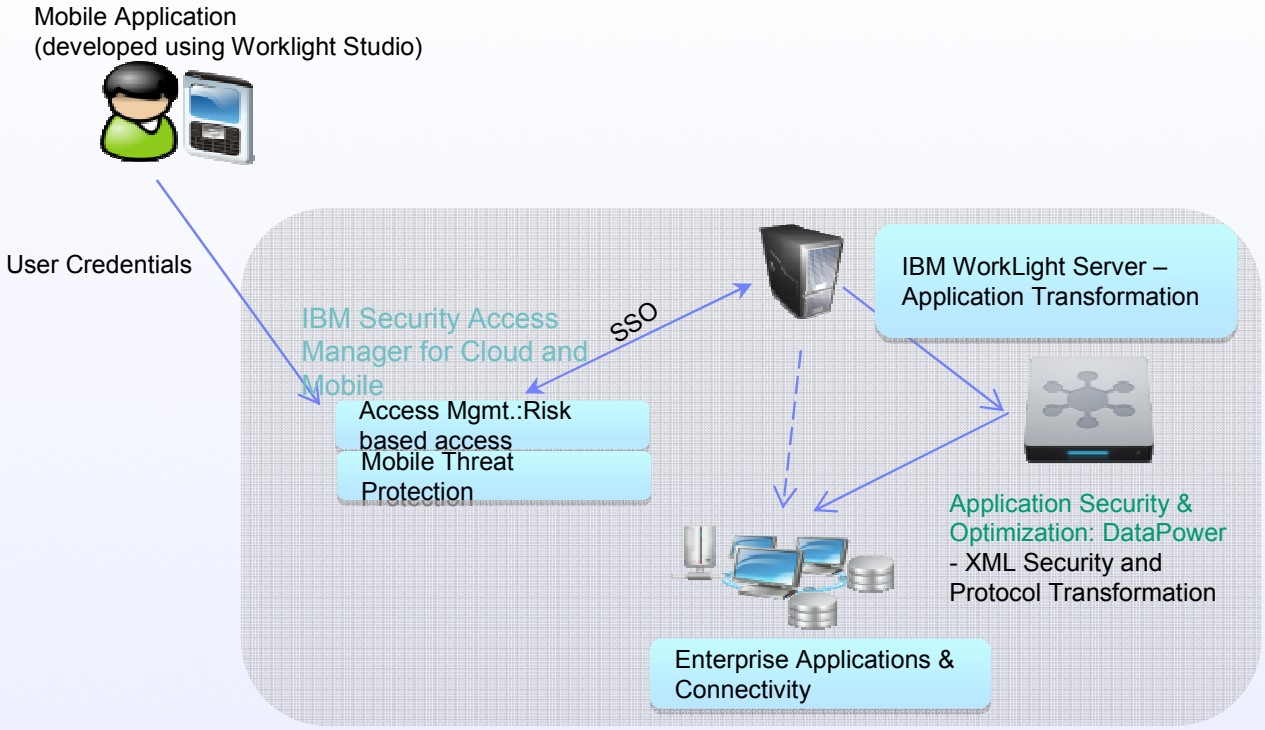
- **FIPS 140-2 Certified Encryption Module**
  - – Meet US Government standards for data protection
- **Automated Compliance-based Email Access**
  - – Automatically grant or deny email access based on device compliance.
- **IBM Lotus Notes Traveler Security Policy Integration**
  - – Ease security administration by setting and reporting Lotus Traveler security policies through the Endpoint Manager console
- **Expanded BYOD Platform Support**
  - – BlackBerry 10, Microsoft Windows Phone 8, Windows RT, Apple iOS 6.1



*A **Mobile First** organization needs…*

Increase accuracy of identifying mobile access security risks

IBM Security Access Manager for Cloud and Mobile



Mobile Security

Key Capabilities

Increase accuracy of identifying mobile access security risks

- Dynamically assess the security risk of an access request
- Quickly enforce Risk-Based Access
- Ensuring users and devices are authenticated and authorized
- Flexibility and strength in authentication: user id/password, OTP, biometrics, certificate, custom
- Protect applications from known security threats by analyzing HTTP traffic

Customer Case Studies

European Bank delivers secure mobile Internet banking

Background

Major European Bank 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

Benefits

- 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 health insurance provider offers secure mobile access

Challenges

Differentiate from competitors by offering customers greater access by supporting mobility

Reduce overhead of paper-based claims processing and call-center volume

Solution

Requests made via HTTPS to multiple back-end services from native device applications protected by IBM Security Access Manager

Authentication enforced with both Basic Authentication and a custom implementation through Access Manager's External Authentication Interface

Benefits

- Simultaneously build trust and improve user experience with secure membership management and claims processing
- Improve customer satisfaction and responsiveness through secure mobile solutions

Public utility adds mobile devices without adding infrastructure

Company Overview

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

Benefits

- Scalability to 250,000 endpoints provides room to grow without adding infrastructure
- Added mobile devices to existing IEM deployment in days
- Ability to integrate with Maximo, Remedy
- Responsiveness and agility of product and product team

Global automotive company secures mobile access

Challenges

- Automobile customers require secure, personalized access to vehicle information services on their mobile devices
- Required secure access to radio, internet and social network services from the automobile

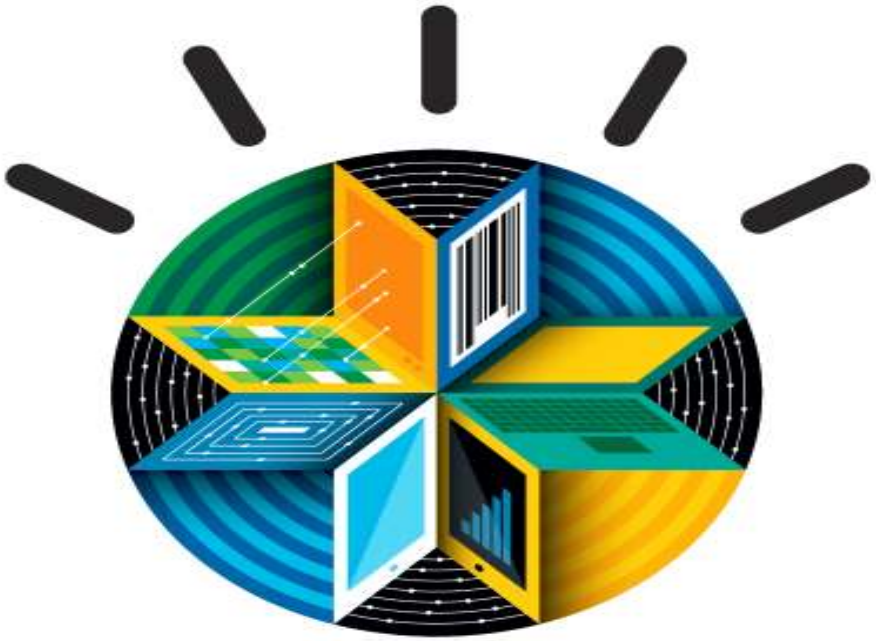
Solution

- IBM Security Access Manager and IBM Federated Identity Manager along with IBM DataPower
- Seamless authentication and authorization to back-end automotive business services

Benefits

- Simplified single sign-on for trusted third party service providers
- Scale to hundreds of thousands of devices and users
- Improved customer satisfaction

Get started with IBM



- Learn more at:

  www.ibm.com/mobilefirst

  - Access white papers and webcasts
  - Get product and services information

- Talk with your IBM representative or IBM Business Partner to find the right next step for you