IBMSoftwareNetwork2013

Fare partnership con il Software IBM

Roma, 24 - 25 gennaio 2013

Soluzioni per una Customer Experience efficace e appagante

Eugenio Barozzi Channel & ICS Technical Manager

AGENDA

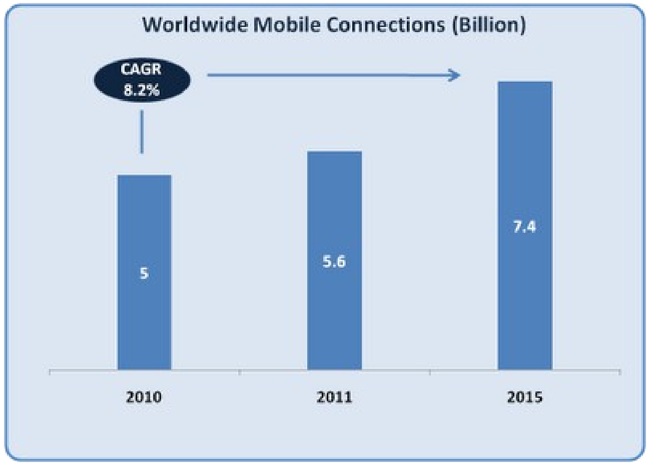
- Il portale: storia di una vision
- Cosa ha scritto chi e quando? La gestione dei contenuti
- Posso usare il mio tablet? La gestione dei dispositivi mobili
- 11:00 Break
- Freeze police - La sicurezza
- Scotty beam me up: trasformare un e-commerce in un $ocial commerce

Due Aspetti fondamentali

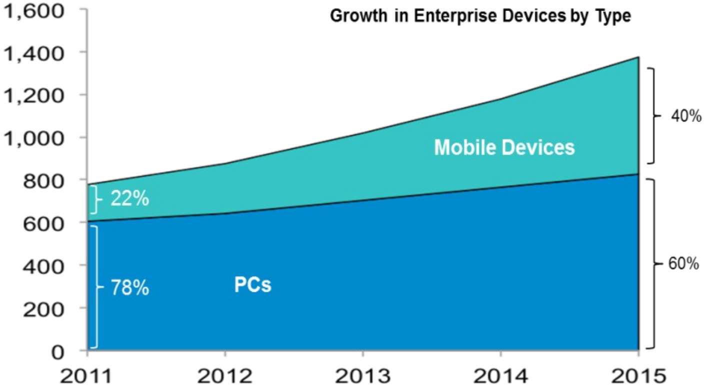
- La sicurezza in ambito mobile
  - BYOD
  - Apps
  - Network access
- La sicurezza in ambito applicativo
  - Web application
  - Mobile applications
  - Third party sw integration

Mobile facts

- Mobile devices are pervasive in our daily lives and increasingly coming to work
- Chief Information Security Officers (CISOs) turn to IBM to help them manage the risks associated with mobility
- Mobile Security market is large and growing rapidly (approx. $900M, CAGR >35%)
- IBM is committed to delivering on its secure mobile enterprise vision
- Compelling IBM Mobile Security Solutions that help customers address their challenges holistically
  - Mobile Device Management
  - Access Management of mobile users and their devices
  - Application Security achieved by employing vulnerability testing
  - Security Intelligence
- Mobile Security will drive demand for existing assets in our security portfolio



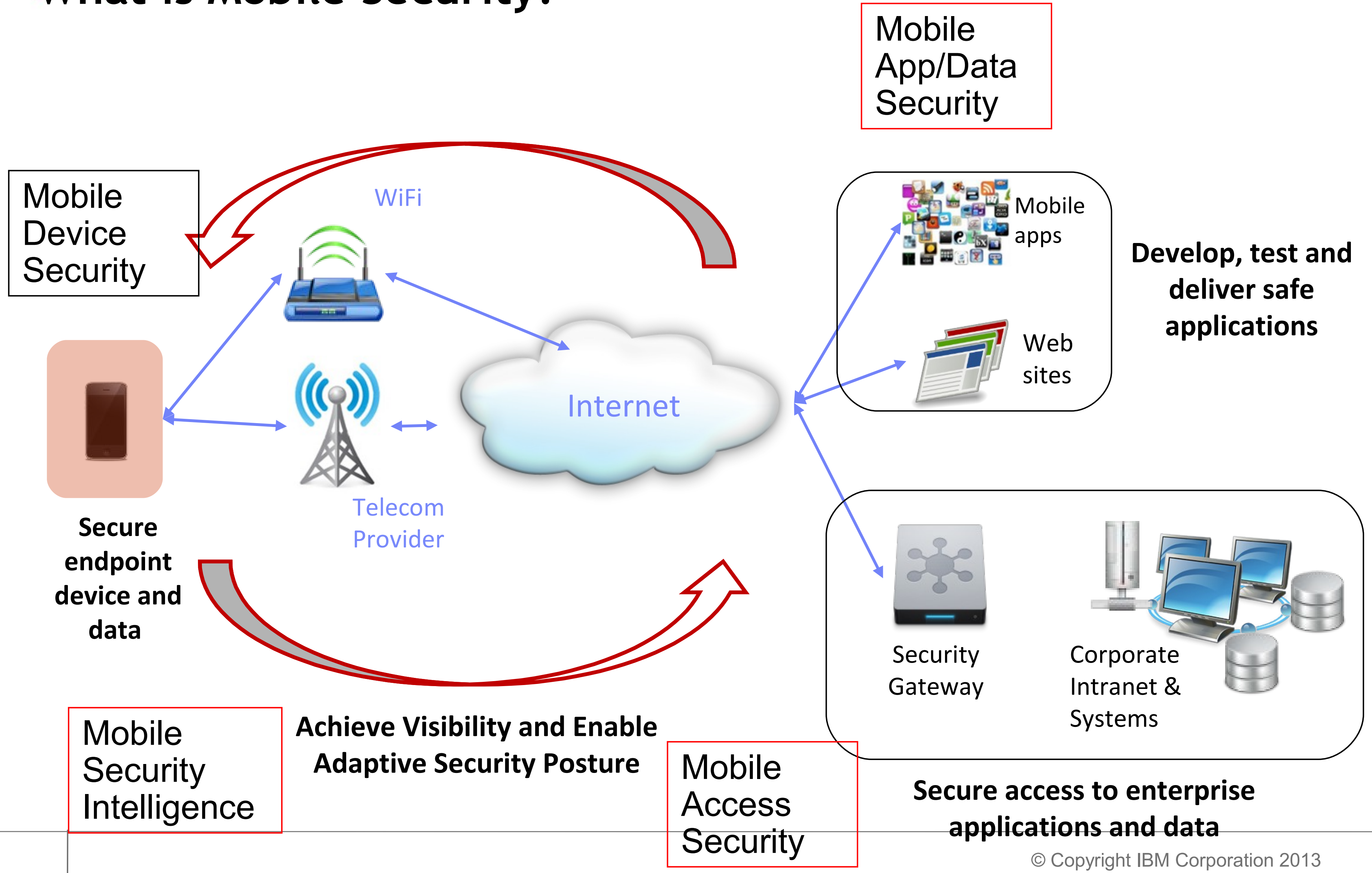
5.6 Billion connections growing to 7.4 by 2015
- Gartner



By 2015 40% of Enterprise devices will be mobile devices

- IBM Projection

What is Mobile Security?



Mobile App/Data Security

Mobile Device Security

Develop, test and deliver safe applications

Secure endpoint device and data

Mobile Security Intelligence

Achieve Visibility and Enable Adaptive Security Posture

Mobile Access Security

Secure access to enterprise applications and data

Mobile Security Solutions IBM Has to Offer

Achieve Visibility and Enable Adaptive Security Posture

IBM QRadar
System-wide Mobile Security Awareness
Risk Assessment
Threat Detection

Secure Data and the Device

IBM WorkLight
Runtime for safe mobile apps
Encrypted data cache
App validation

IBM Endpoint Manager for Mobile
Configure, Provision, Monitor
Set appropriate security policies
Enable endpoint access
Ensure compliance

Protect Access to Enterprise Apps and Data

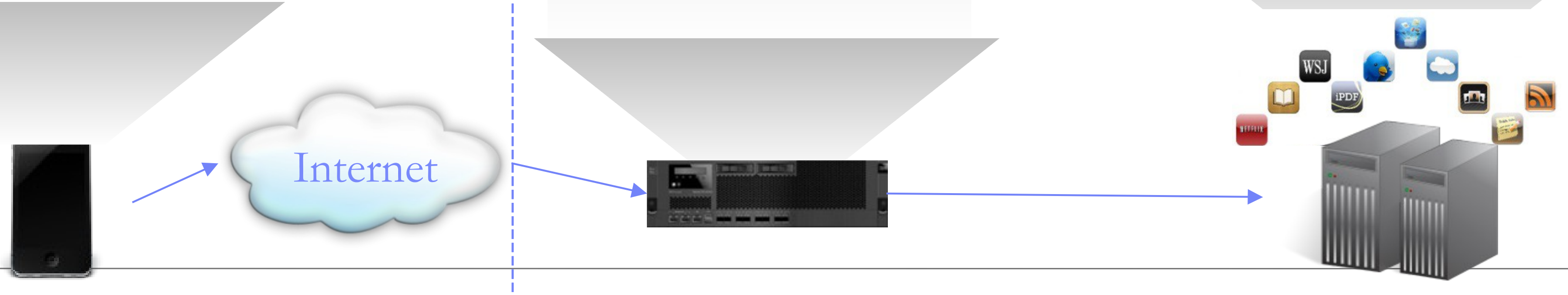
IBM Security Access Manager for Mobile (TAMeb)
Authenticate & authorize users and devices
Standards Support: OAuth, SAML, OpenID
Single Sign-On & Identity Mediation

IBM Mobile Connect
Secure Connectivity
App level VPN

Develop and Test Mobile Apps

IBM WorkLight
Develop safe mobile apps
Direct Updates

IBM AppScan for Mobile
Vulnerability testing
Dynamic & Static analysis of Hybrid and Mobile web apps



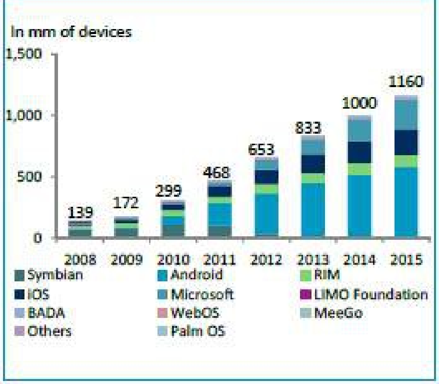
Trends in Enterprise Mobility …

The need for business agility along with changing employee behaviors 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

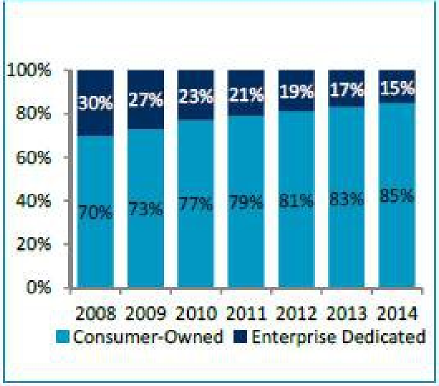
Smartphone Proliferation



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

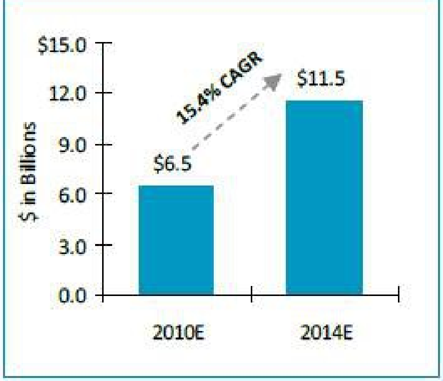
% of Consumer v. Enterprise Devices



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

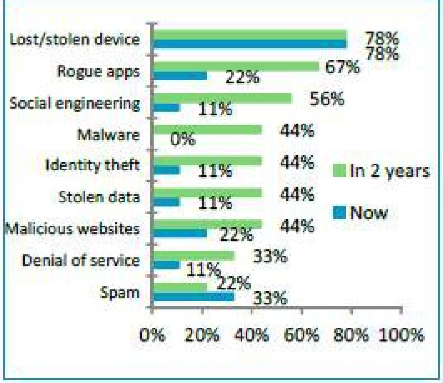
Enterprise Application Market



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

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.

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.

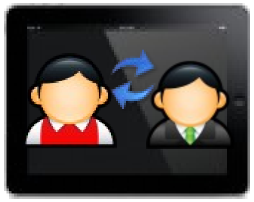
Mobile Devices are Diverse

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.

Challenges of Enterprise Mobility

> ***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



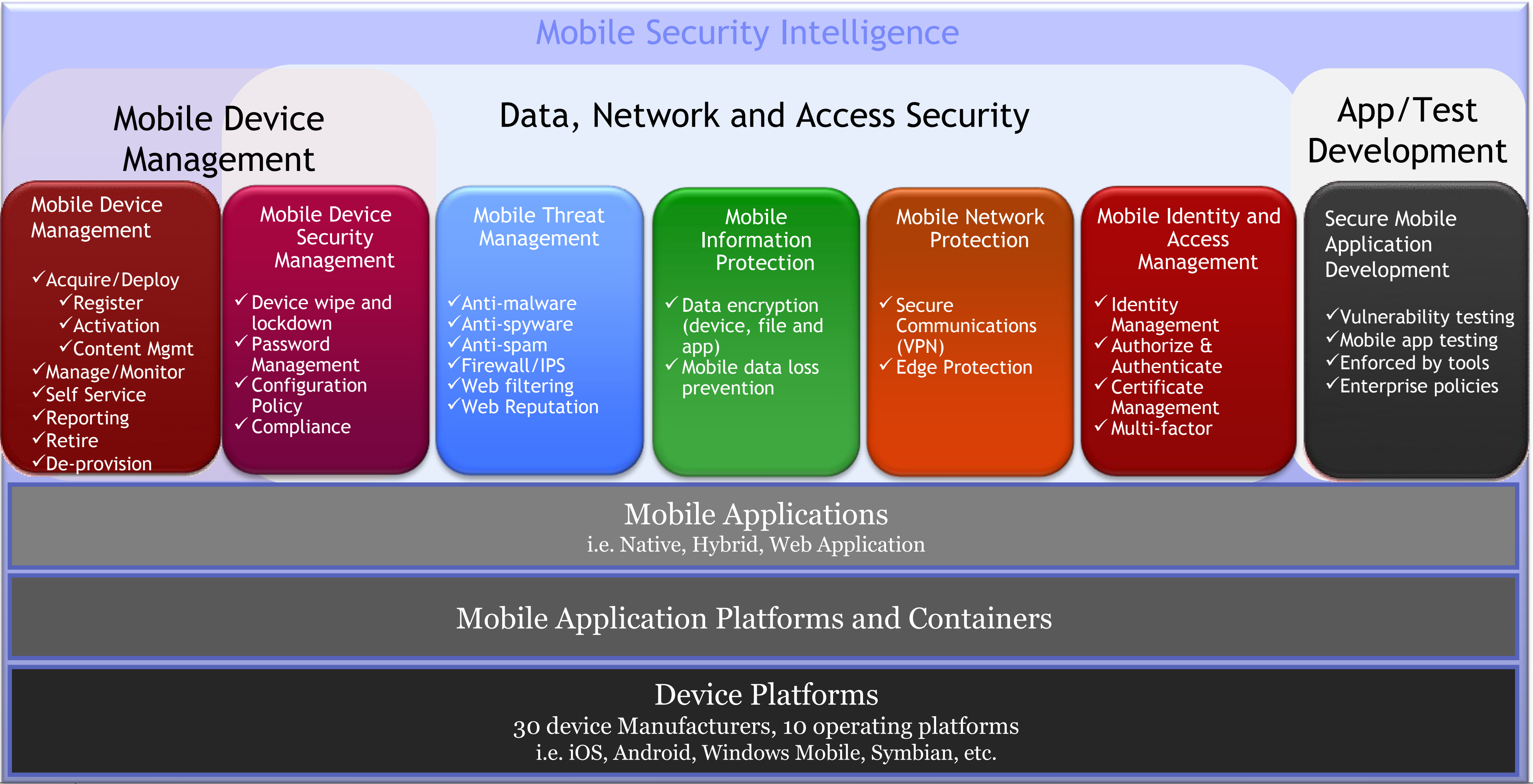
- Achieving Data Separation
  - Privacy
  - Corporate Data protection

- 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

… Driving Key Set of Mobile Security Requirements

Mobile devices are not only computing platforms but also communication devices, hence mobile security is multi-faceted, driven by customers' operational priorities



Mobile Security Intelligence

Mobile Device Management

Data, Network and Access Security

App/Test Development

Mobile Device Management
- ✓Acquire/Deploy
  - ✓Register
  - ✓Activation
  - ✓Content Mgmt
- ✓Manage/Monitor
- ✓Self Service
- ✓Reporting
- ✓Retire
- ✓De-provision

Mobile Device Security Management
- ✓ Device wipe and lockdown
- ✓ Password Management
- ✓ Configuration Policy
- ✓ Compliance

Mobile Threat Management
- ✓Anti-malware
- ✓Anti-spyware
- ✓Anti-spam
- ✓Firewall/IPS
- ✓Web filtering
- ✓Web Reputation

Mobile Information Protection
- ✓ Data encryption (device, file and app)
- ✓ Mobile data loss prevention

Mobile Network Protection
- ✓ Secure Communications (VPN)
- ✓ Edge Protection

Mobile Identity and Access Management
- ✓ Identity Management
- ✓ Authorize & Authenticate
- ✓ Certificate Management
- ✓ Multi-factor

Secure Mobile Application Development
- ✓Vulnerability testing
- ✓Mobile app testing
- ✓Enforced by tools
- ✓Enterprise policies

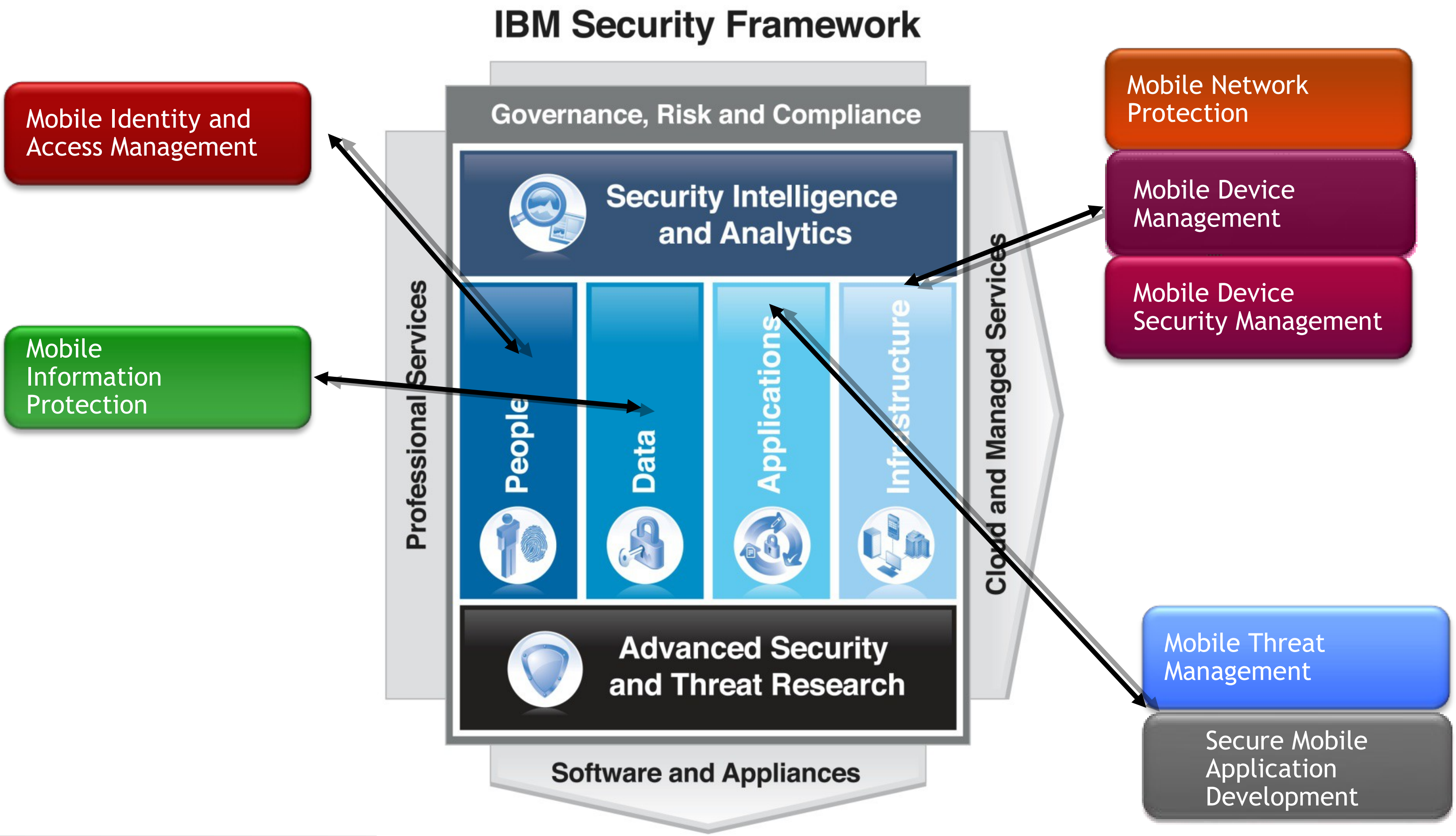
Mobile Applications
i.e. Native, Hybrid, Web Application

Mobile Application Platforms and Containers

Device Platforms
30 device Manufacturers, 10 operating platforms
i.e. iOS, Android, Windows Mobile, Symbian, etc.

Mobile Security Enabled with IBM Solutions

IBM can bring together a broad portfolio of technologies and services to meet the mobile security needs of customers across multiple industries


IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances
Mobile Identity and Access Management
Mobile Information Protection
Mobile Network Protection
Mobile Device Management
Mobile Device Security Management
Mobile Threat Management
Secure Mobile Application Development

Customer Scenarios

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

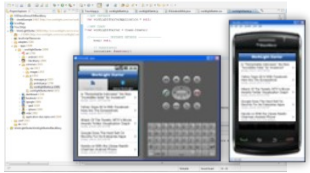
Business Need:
Protect Enterprise Systems & Deliver Secure Access

- ➢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

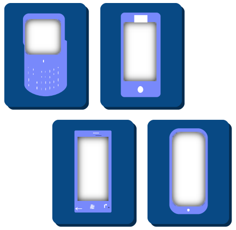
- ➢Enforce Corporate Development Best Practices
  - ❑ Development tools enforcing security policies
- ➢Testing mobile apps for exposure to threats
  - ❑ Penetration Testing
  - ❑ Vulnerability Testing
- ➢Provide Offline Access
  - ❑ Encrypted Local Storage of Credentials
- ➢Deliver mobile apps securely
  - ❑ Enterprise App Store
- ➢Prevent usage of compromised apps
  - ❑ Detect and disable compromised apps

Application Security Solution: WorkLight



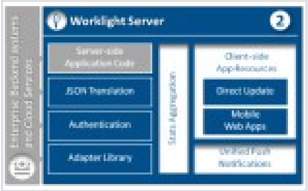
Security by Design

✓Develop secure mobile apps using corporate best practices
✓Code Obfuscation



Protecting Mobile App Data

✓Encrypted local storage for data,
✓Offline user access
✓Challenge response on startup
✓App Authenticity Validation
✓Enforcement of organizational security policies


Worklight Server
Enterprise Backend Systems and Cloud Services
Server-side Application Code
JSON Translation
Authentication
Adapter Library
Stats Aggregation
Client-side App Resources
Direct Update
Mobile Web Apps
Unified Push Notifications

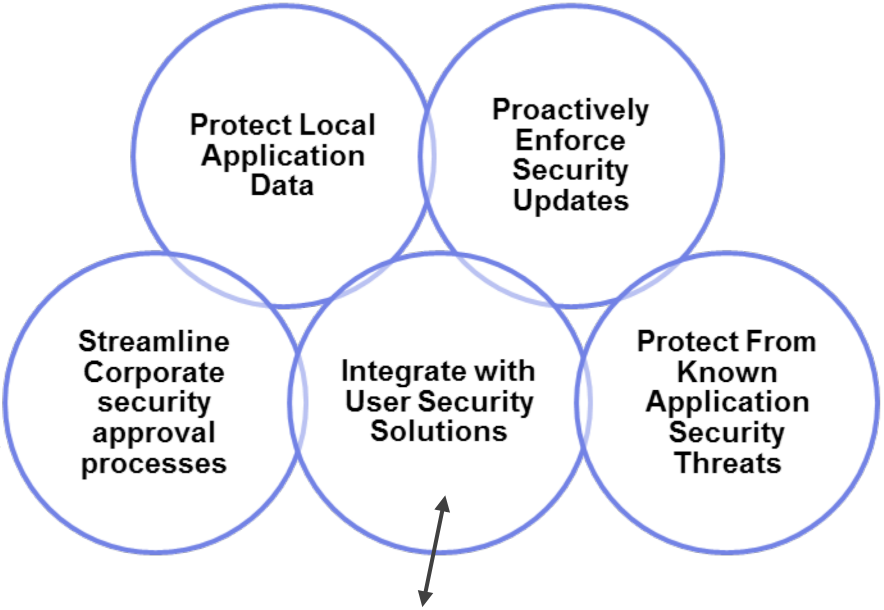
Enforcing Security Compliance

✓Direct Updates
✓Integration with User Security Solutions

App Management

✓Analytics
✓Remote Disabling of apps

Application Security Objectives


Protect Local Application Data
Proactively Enforce Security Updates
Streamline Corporate security approval processes
Integrate with User Security Solutions
Protect From Known Application Security Threats

Integration point with IBM Security Access Management (TAMeb)

Application Security Solution: AppScan

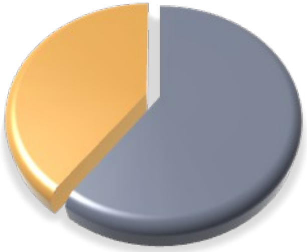
Detection of Vulnerabilities before Apps are Delivered and Deployed

- Known vulnerabilities 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

Leverage AppScan for vulnerability testing of mobile web apps and web elements (JavaScript, HTML5) of hybrid mobile apps

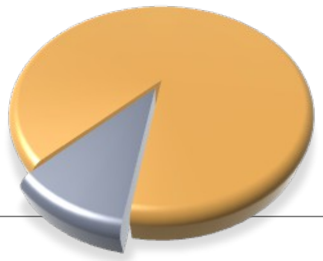
Apps vulnerable To Client-side JavaScript vulnerabilities

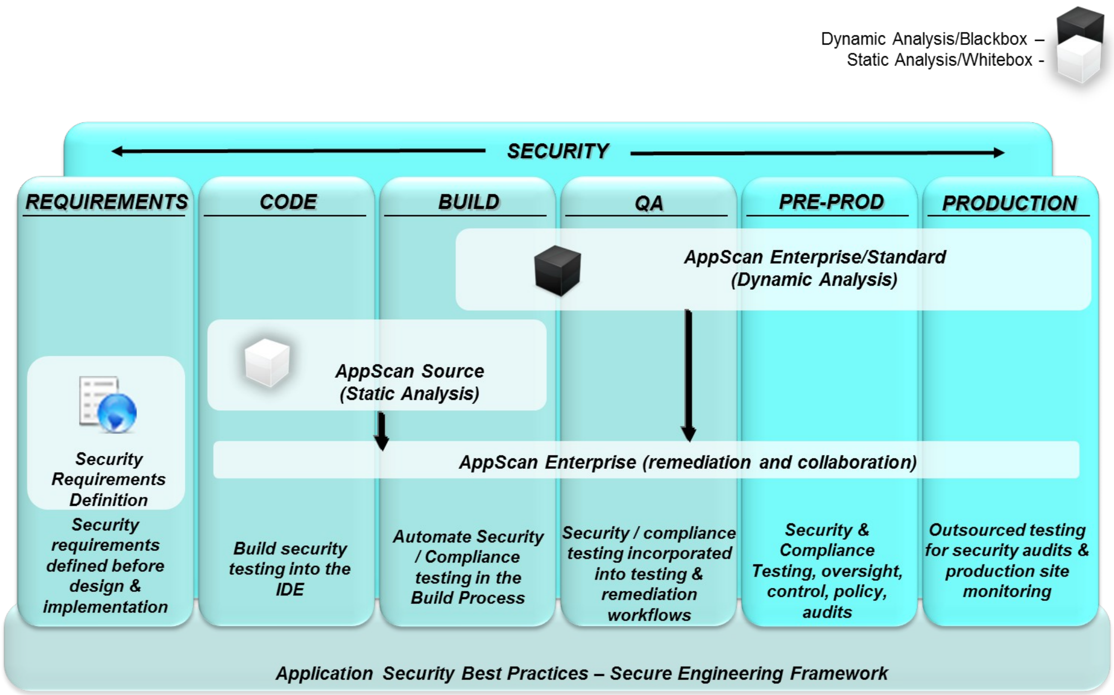
40%



Applications with issues in 3rd Party JavaScript code

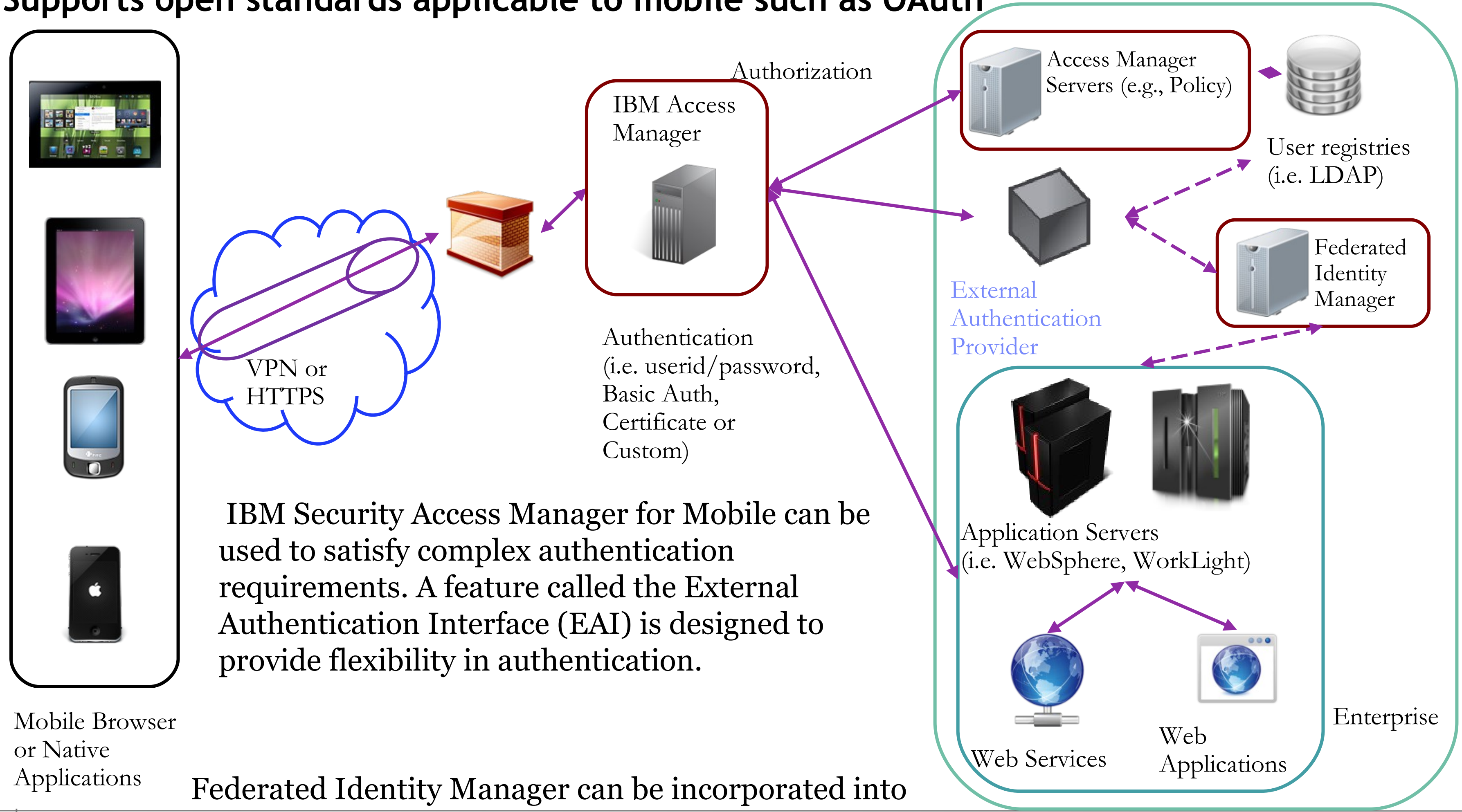
90%




Dynamic Analysis/Blackbox –
Static Analysis/Whitebox -
SECURITY
REQUIREMENTS
CODE
BUILD
QA
PRE-PROD
PRODUCTION
AppScan Enterprise/Standard (Dynamic Analysis)
Security Requirements Definition
AppScan Source (Static Analysis)
AppScan Enterprise (remediation and collaboration)
Security requirements defined before design & implementation
Build security testing into the IDE
Automate Security / Compliance testing in the Build Process
Security / compliance testing incorporated into testing & remediation workflows
Security & Compliance Testing, oversight, control, policy, audits
Outsourced testing for security audits & production site monitoring
Application Security Best Practices – Secure Engineering Framework

User Security Solution: IBM Security Access Manager for Mobile (current product name: Tivoli Access Manager for e-business -TAMeb)

Delivers user security by authenticating & authorizing the user along with their device. Supports open standards applicable to mobile such as OAuth

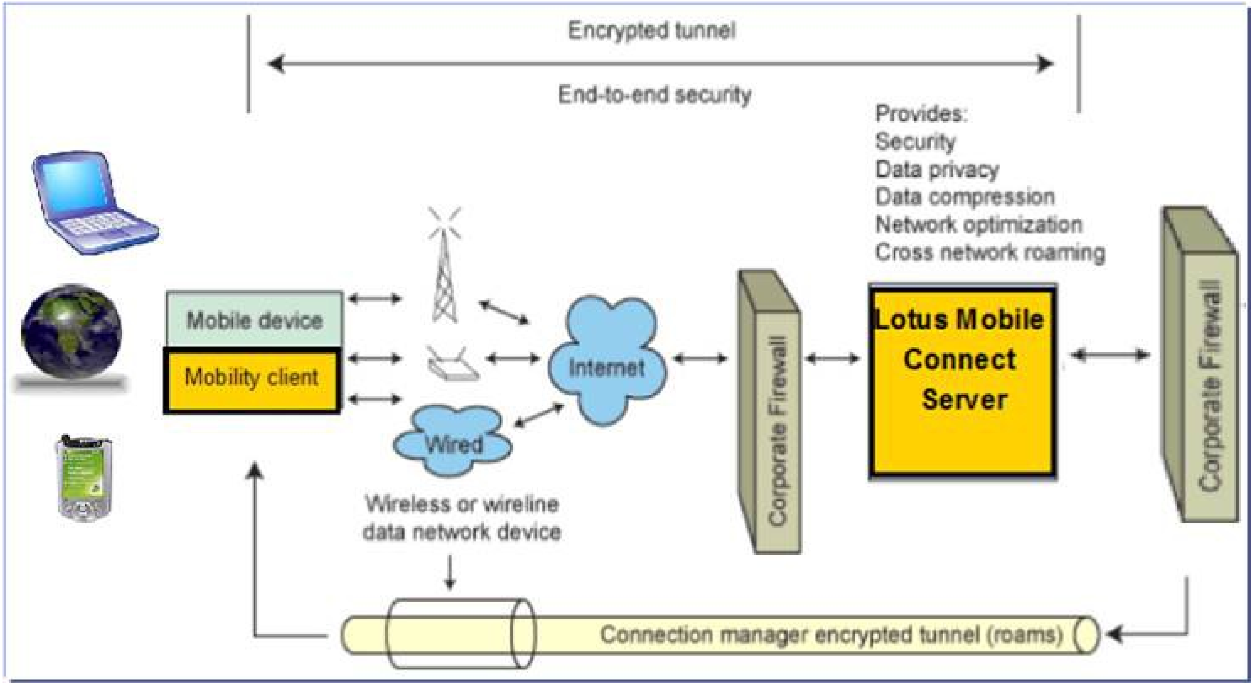

Mobile Browser or Native Applications
VPN or HTTPS
IBM Access Manager
Authorization
Authentication (i.e. userid/password, Basic Auth, Certificate or Custom)
Access Manager Servers (e.g., Policy)
User registries (i.e. LDAP)
External Authentication Provider
Federated Identity Manager
Application Servers (i.e. WebSphere, WorkLight)
Web Services
Web Applications
Enterprise

IBM Security Access Manager for Mobile can be used to satisfy complex authentication requirements. A feature called the External Authentication Interface (EAI) is designed to provide flexibility in authentication.

Federated Identity Manager can be incorporated into the solution to provide federated identity management

Solution: IBM Mobile Connect

Delivers secure connectivity from mobile devices to back-end systems and adapts to a mobile user's unique requirements such as roaming support and cost-based routing



A high availability intelligent solution providing:

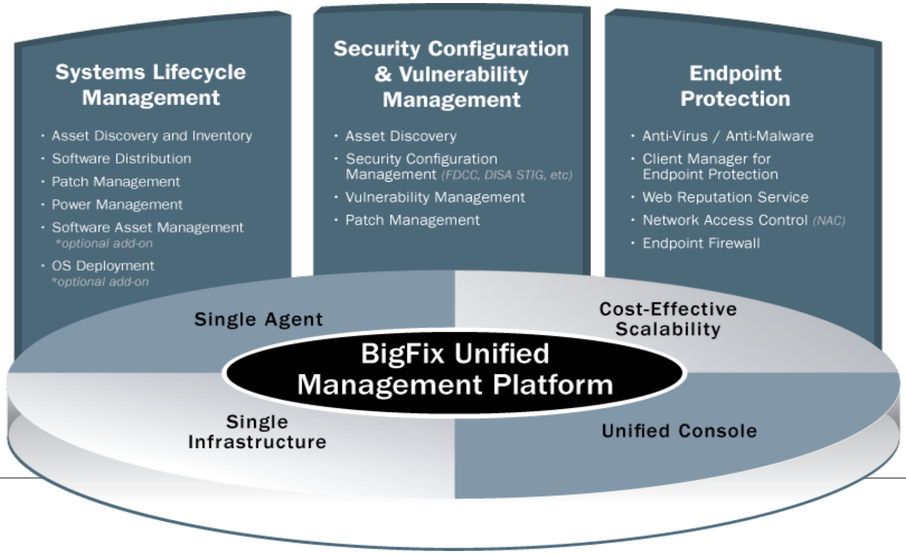
- ✓ Mobile VPN
  - ✓ SSL VPN
- ✓ Least cost routing & data optimization
- ✓ End-to-end encryption

Device Security Solution: IBM Endpoint Manager For Mobile

Delivers device security by providing visibility of the devices connected to the enterprise, and supports core capabilities such as device lock, selective wipe and jailbreak detection.

A highly-scalable, unified solution across platforms, device types, and IT functions providing:

- Near-instant deployment of new features and analytics reports in to customer's environments
- A unified systems and security management solution for all enterprise devices
- Platform to extend integrations with Service Desk, CMDB, SIEM, and other information-gathering systems to mobile devices


Systems Lifecycle Management
Asset Discovery and Inventory
Software Distribution
Patch Management
Power Management
Software Asset Management
*optional add-on
OS Deployment
*optional add-on
Security Configuration & Vulnerability Management
Asset Discovery
Security Configuration Management (FDCC, DISA STIG, etc)
Vulnerability Management
Patch Management
Endpoint Protection
Anti-Virus / Anti-Malware
Client Manager for Endpoint Protection
Web Reputation Service
Network Access Control (NAC)
Endpoint Firewall
Single Agent
Cost-Effective Scalability
BigFix Unified Management Platform
Single Infrastructure
Unified Console

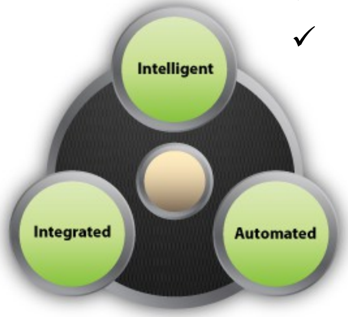
- Advanced mobile device management capabilities for iOS, Android, Symbian, and Windows Phone
- Unified management approach capable of automatically enabling VPN access based on security compliance
- Security threat detection and automated remediation
- Will be used internally, extending IBM's existing 500,000 device endpoint management deployment

Mobile Security Intelligence: QRadar

Delivers Mobile Security Intelligence by monitoring data collected from other mobile security solutions – visibility, reporting and threat detection

- Unified collection, aggregation and analysis architecture for:
  - Application logs
  - Security events
  - Vulnerability data
  - Identity and Access Management data
  - Configuration files
  - Network flow telemetry
- A common platform for
  - Searching
  - Filtering
  - Rule writing
  - Reporting functions
- A single user interface for
  - Log management
  - Risk modeling
  - Vulnerability prioritization
  - Incident detection
  - Impact analysis tasks

- Ingest log data and events from:
  - ✓ Endpoint Manager for Mobile Devices
  - ✓ Access Manager for Mobile
  - ✓ Mobile Connect
  - ✓ WorkLight



Mobile Security Solutions IBM Has to Offer

Achieve Visibility and Enable Adaptive Security Posture

IBM QRadar

System-wide Mobile Security Awareness
Risk Assessment
Threat Detection

Secure Data and the Device

IBM WorkLight

Runtime for safe mobile apps
Encrypted data cache
App validation

IBM Endpoint Manager for Mobile

Configure, Provision, Monitor
Set appropriate security policies
Enable endpoint access
Ensure compliance

Protect Access to Enterprise Apps and Data

IBM Security Access Manager for Mobile (TAMeb)

Authenticate & authorize users and devices
Standards Support: OAuth, SAML, OpenID
Single Sign-On & Identity Mediation

IBM Mobile Connect

Secure Connectivity
App level VPN

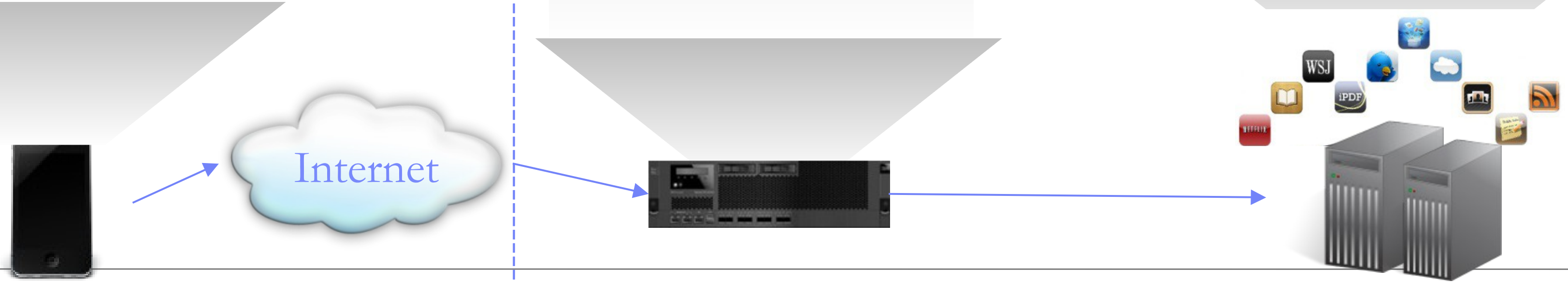
Develop and Test Mobile Apps

IBM WorkLight

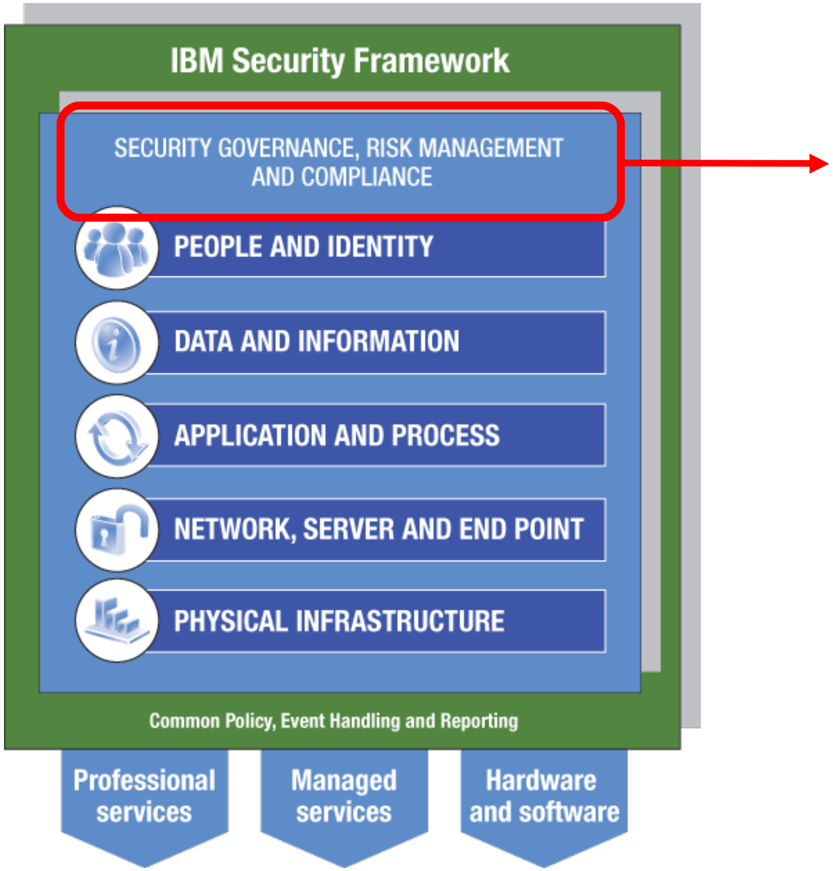
Develop safe mobile apps
Direct Updates

IBM AppScan for Mobile

Vulnerability testing
Dynamic & Static analysis of Hybrid and Mobile web apps



IBM Security Framework helps you address key challenges of cost, complexity and compliance



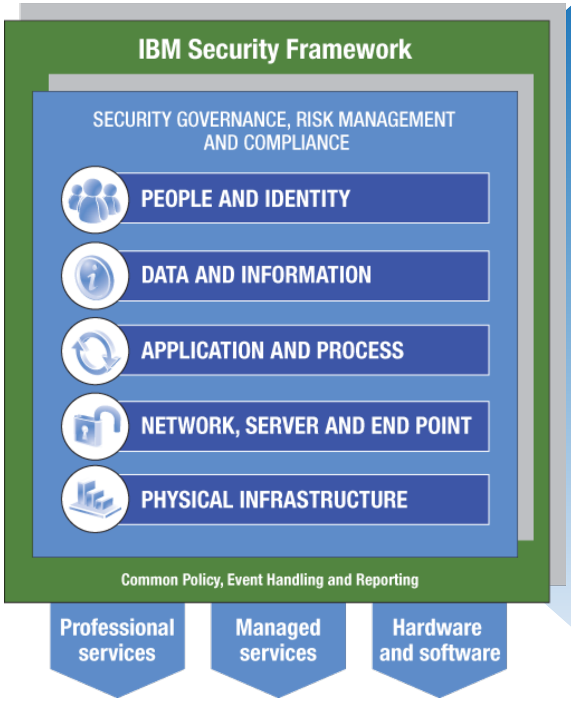
Build a strong foundation for IT security

Create and sustain security governance

Manage risk

Ensure compliance

The Framework identifies five security focus areas as starting points



PEOPLE AND IDENTITY
Mitigate the risks associated with user access to corporate resources

DATA AND INFORMATION
Understand, deploy, and properly test controls for access to and usage of sensitive data

APPLICATION AND PROCESS
Keep applications secure, protected from malicious or fraudulent use, and hardened against failure

NETWORK, SERVER AND END POINT
Optimize service availability by mitigating risks to network components

PHYSICAL INFRASTRUCTURE
Provide actionable intelligence on the desired state of physical infrastructure security and make improvements

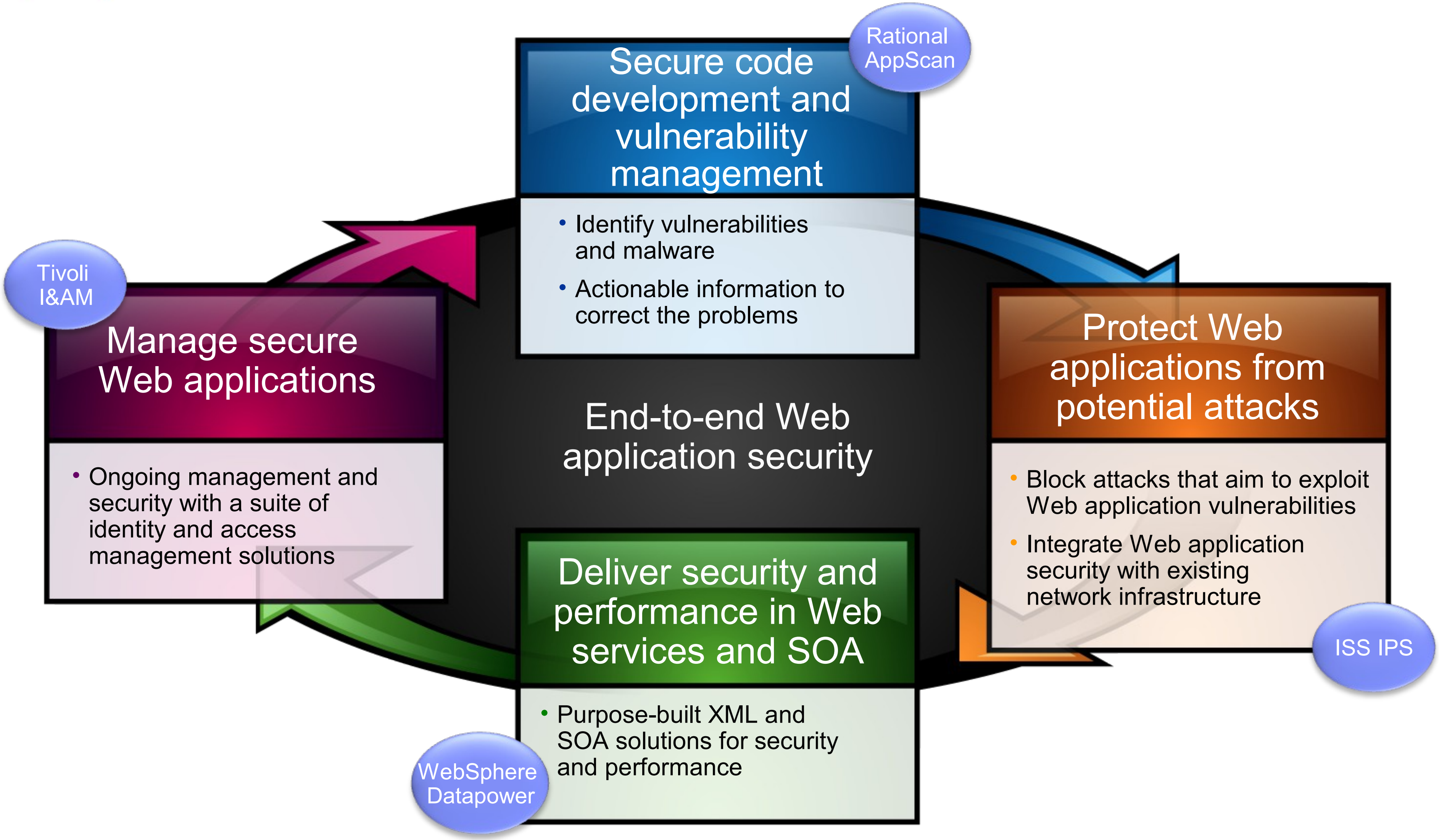
Click ⓘ for more information

IBM Security portfolio can help you meet challenges in each security focus area

Framework	Challenges	
PEOPLE AND IDENTITY	▪ Manage identities ▪ Control access to applications	▪ Audit, report and manage access to resources
DATA AND INFORMATION	▪ Protect Critical Databases ▪ Messaging Security and Content Filtering	▪ Monitor & manage data access ▪ Prevent Data Loss ▪ Encryption
APPLICATION AND PROCESS	▪ Ensure Security in App Development ▪ Discover App Vulnerabilities	▪ Embed App Access Controls ▪ Provide SOA Security
NETWORK, SERVERS & ENDPOINTS	▪ Protect Servers, Endpoints, Networks, Mainframes	
PHYSICAL INFRASTRUCTURE	▪ Video Surveillance ▪ Command and Control	▪ Video Analytics

Click i for more information

IBM Web application security for a smarter planet



Rational AppScan

Secure code development and vulnerability management

- Identify vulnerabilities and malware
- Actionable information to correct the problems

Tivoli I&AM

Manage secure Web applications

- Ongoing management and security with a suite of identity and access management solutions

End-to-end Web application security

Protect Web applications from potential attacks

- Block attacks that aim to exploit Web application vulnerabilities
- Integrate Web application security with existing network infrastructure

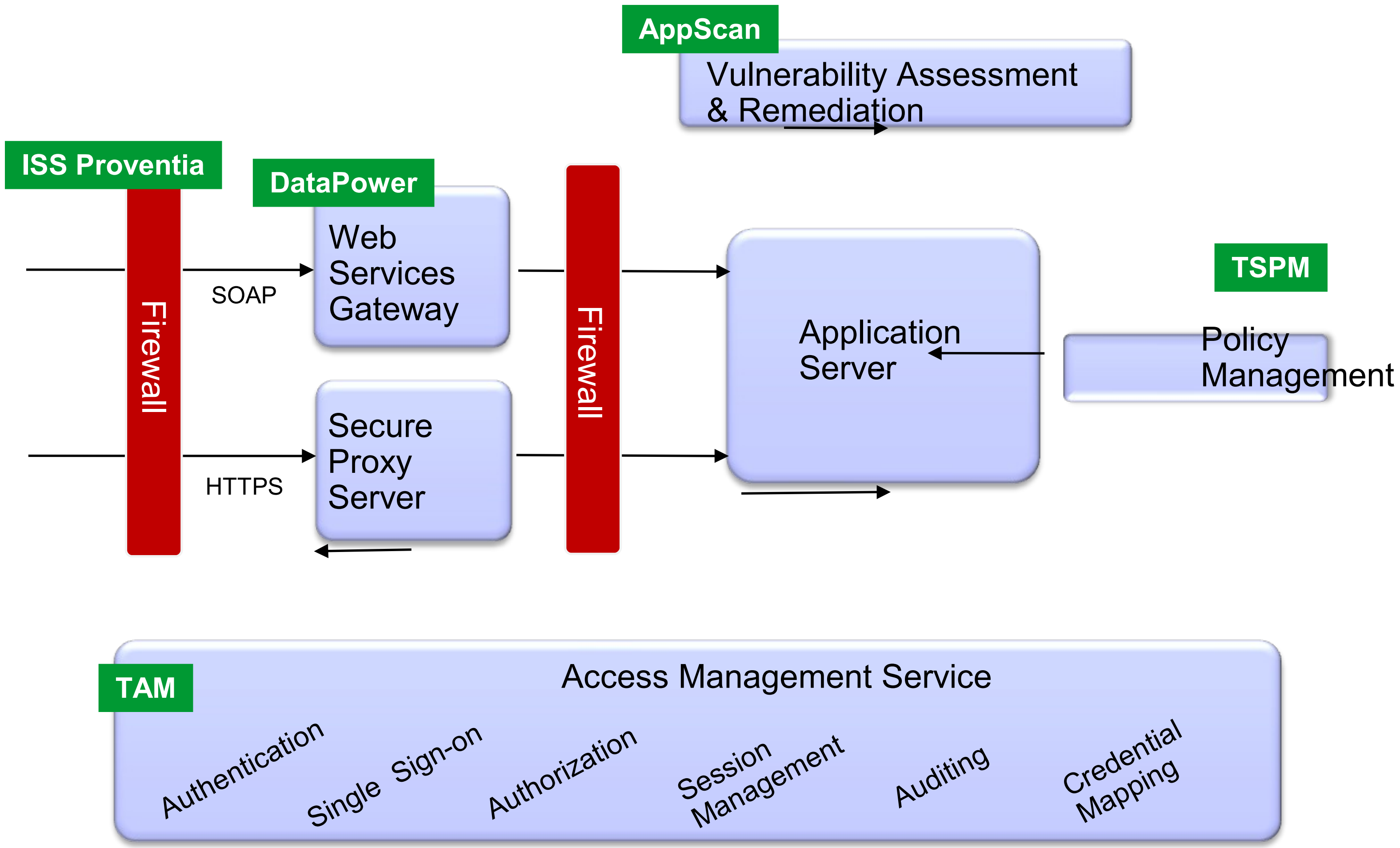
ISS IPS

Deliver security and performance in Web services and SOA

- Purpose-built XML and SOA solutions for security and performance

WebSphere Datapower

IBM Security Solutions End-to-End Application Coverage



TAM = Tivoli Access Manager
TSPM = Tivoli Security Policy Manager
DataPower = Secure XML Gateway