
# Secure:
# Mobile Security Intelligence

**Rohit Umashankar Satayanarayana**

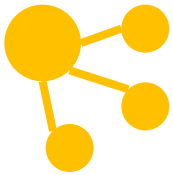
**Lead, Strategic Accounts, Security Growth Markets, IBM Asia Pacific**

CIOs in the era of big data, cloud, mobility and social

# Innovative technology changes everything

1 trillion connected objects

1 billion mobile workers



Social business

Bring your own IT

Cloud and virtualization

# Techniques, tools, and targets are also increasing


In 2011 there was an

**80%**

increase in phishing attacks, many of which impersonate social networking sites.

In 2011 there was a

**19%**

increase in the number of tools released publicly that can be used to attack mobile devices.

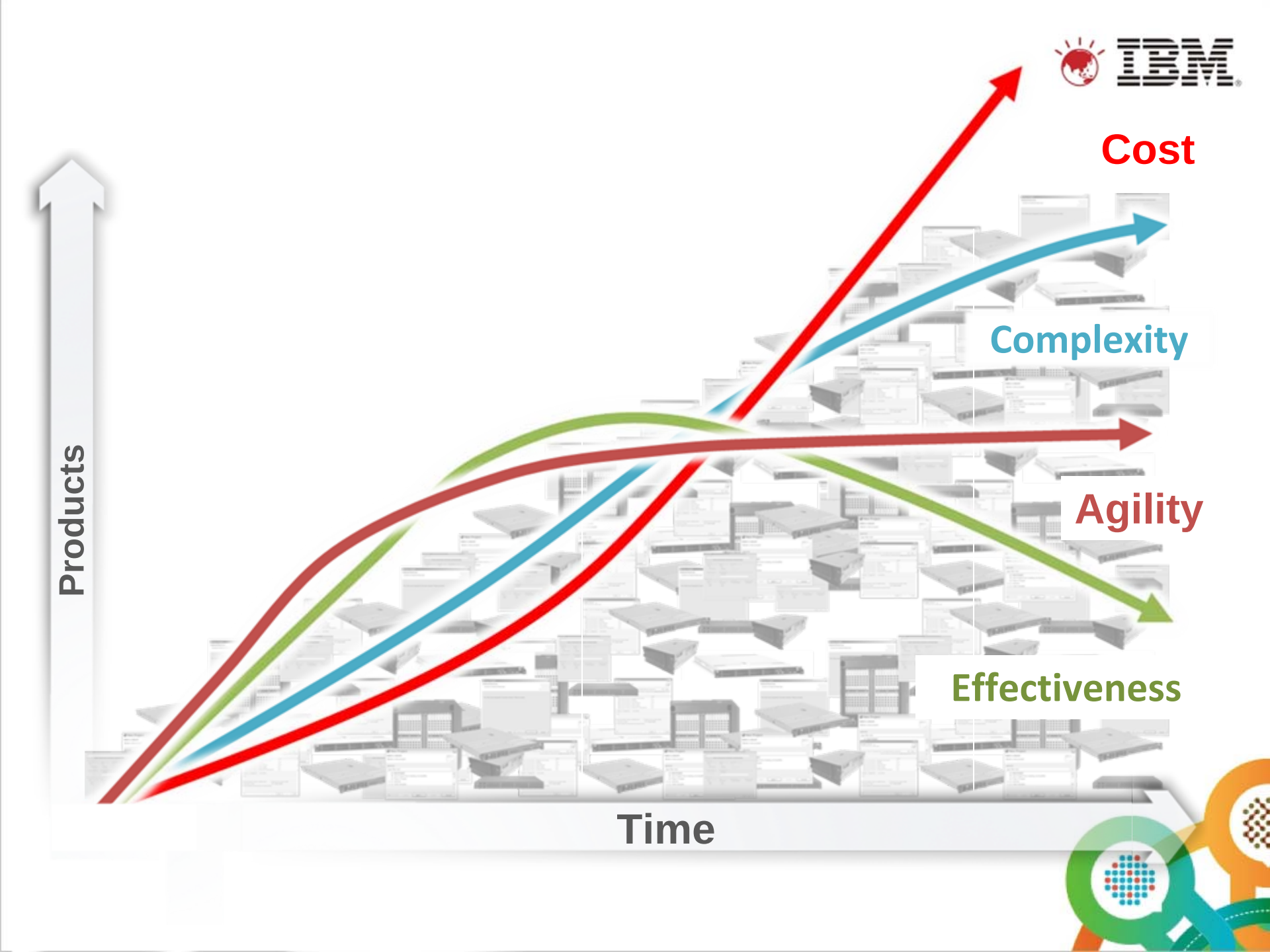
So far in 2012, IBM reports over

**4,400**

new security **vulnerabilities**.

Source: *IBM X-Force® 2011 Trend and Risk Report*


Products
Time


Cost
Complexity
Agility
Effectiveness
Products
Time

# Your security team sees noise

# Devices follow unique usage scenarios

## 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 organiser
- Security profile per persona?

## Mobile devices are diverse

.

- OS immaturity for enterprise mgmt
- BYOD dictates multiple OSs
- Vendor / carrier control dictates multiple OS versions
- Diverse app development/delivery model

## Mobile devices are used in more locations

- A single location could offer public, private, and cell connections
- Anywhere, anytime
- Increasing reliance on enterprise WiFi
- Devices more likely to be lost/stolen


## Mobile devices prioritise the user

- Conflicts with user experience not tolerated
- OS architecture puts the user in control
- Difficult to enforce policy, app lists
- Security policies have less of a chance of dictating experience

# App delivery means a shift in development paradigms

## Browser-based Mobile Applications

**Description:**
Web application resides on server and is accessed via the Internet using a browser.

**Advantages:**
- Relatively low development costs
- Version management
- Ubiquitous channel for application delivery

**Disadvantages:**
- Network latency
- Bandwidth consumption
- Limited access to device capabilities (i.e. accelerometer, GPS, camera, contacts etc.)

**Advancements:**
- Tools to provide native look-and-feel
- Standards (i.e. HTML5) offering greater access to device capabilities, some offline support, and client side execution
- Techniques to mimic user experience in launching applications

## Native Applications

**Description:**
An application that is mainly acquired through app stores and installed on the device. Platform specific SDKs required for development.

**Advantages:**
- Rich user experience
- Offline computing
- Access to device capabilities

**Disadvantages:**
- Development and maintenance costs required to support multiple platforms
- Version support
- Externally controlled delivery channels (app stores)

**Advancements:**
- Development frameworks with in-built business models for monetizing applications

## Hybrid Applications

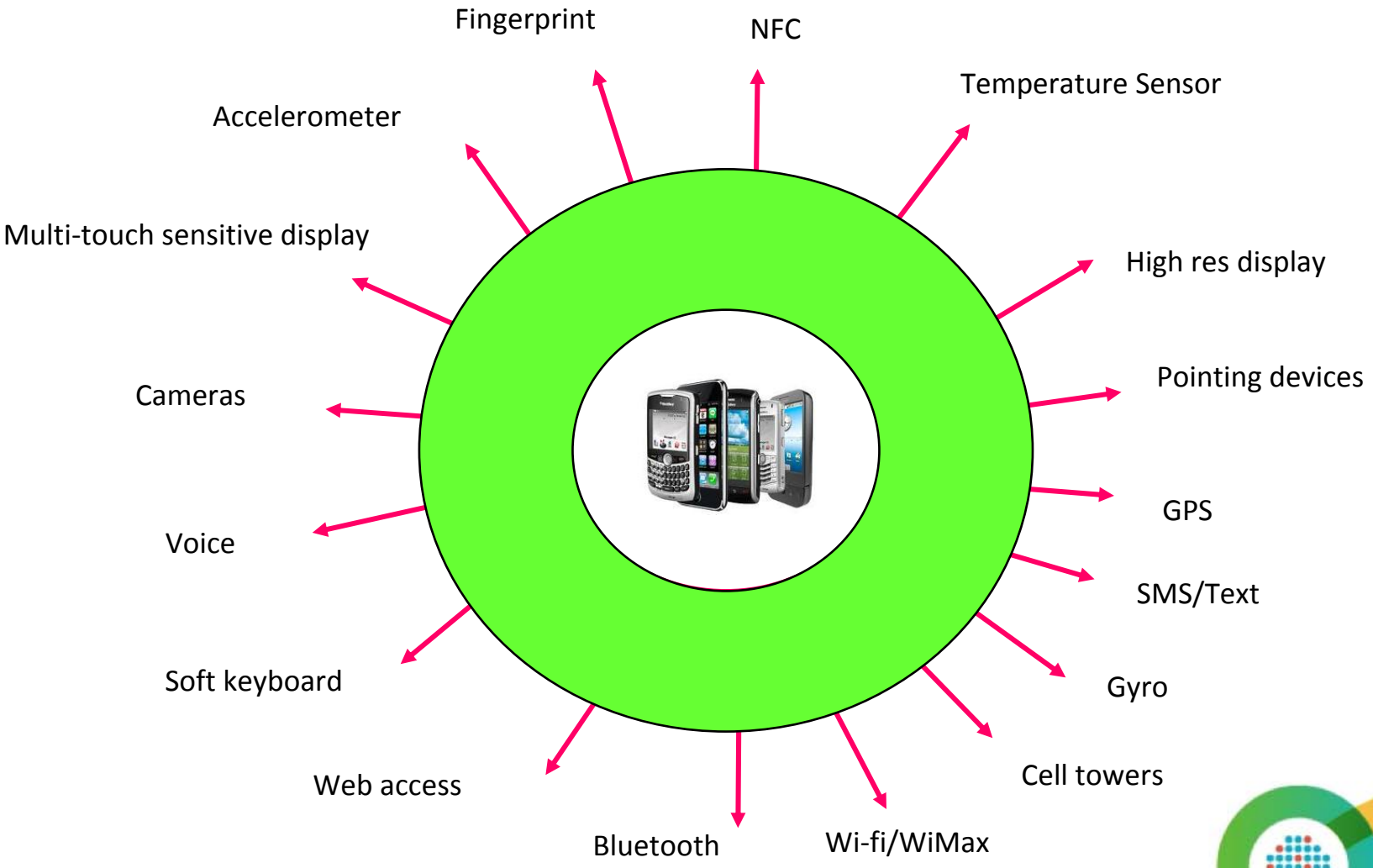
**Description:**
Installed application built using web technologies (i.e. JavaScript, CSS, HTML) that leverage platform specific wrappers to access to device capabilities.

**Advantages:**
- Reduced development costs over native applications
- Can support offline computing
- Access to some of the device capabilities

**Disadvantages:**
- Inclusion of third-party wrappers could impact performance
- Version support & management

**Advancements:**
- Frameworks for building hybrid applications maturing
- Tools to provide native look-and-feel
- Improvements in performance

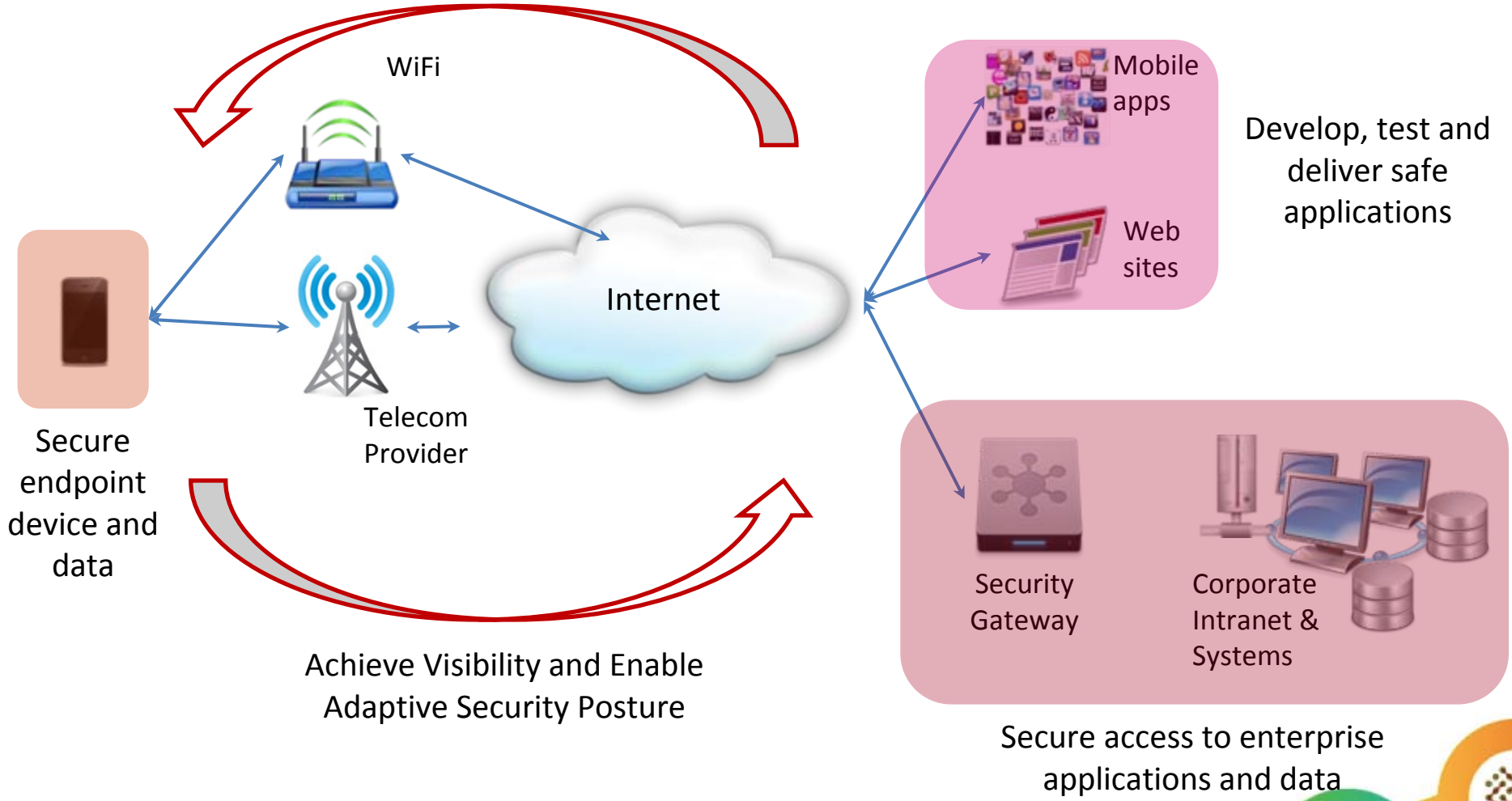
# Devices do present an opportunity for IT Security to reduce risk



# IBM Mobile Security

| Device Management | Network, Data, and Access Security | Application Layer Security |
| --- | --- | --- |
| Security for endpoint device and data | Achieve visibility and adaptive security policies | Develop and test applications |

# Visualizing Mobile Security



# Possible Mobile Security technology focus areas

- Provide device lifecycle management
  - Device Management & Security
  - Application management

- Provide consistent user management and access
  - Secure connectivity
  - Identity, Access & Authorisation

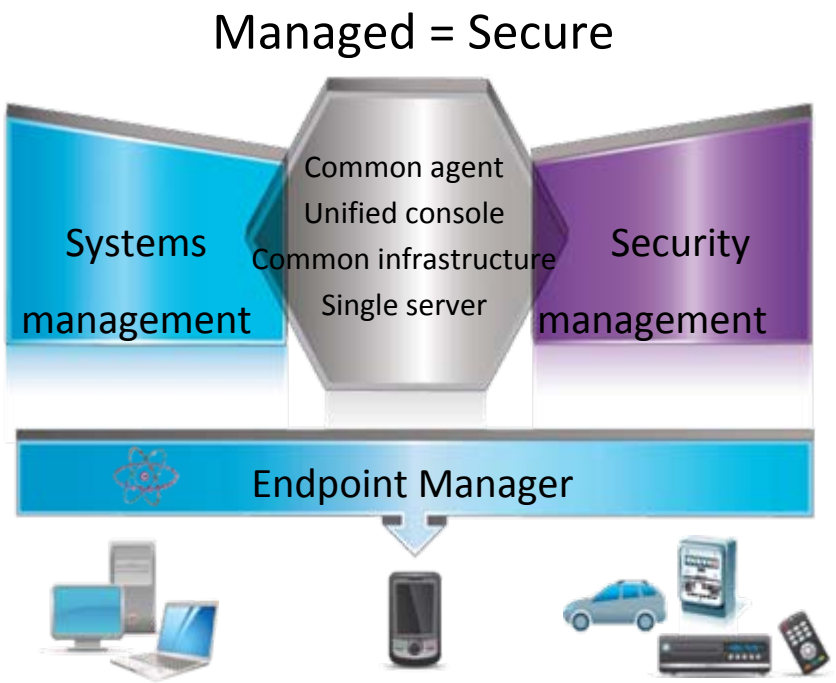
- Deliver and manage Safe and Security Rich Apps
  - Vulnerability testing
  - Development lifecycle consistency
  - Achieving data Separation

- Provide a flexible set of connectivity options
  - VPN or standard HTTP

- Design an Adaptive Security Intelligence framework
  - Policy Management
  - Security Intelligence

# Device Lifecycle Management

*A unified solution that offers device management and security across device types*




## Client Challenge

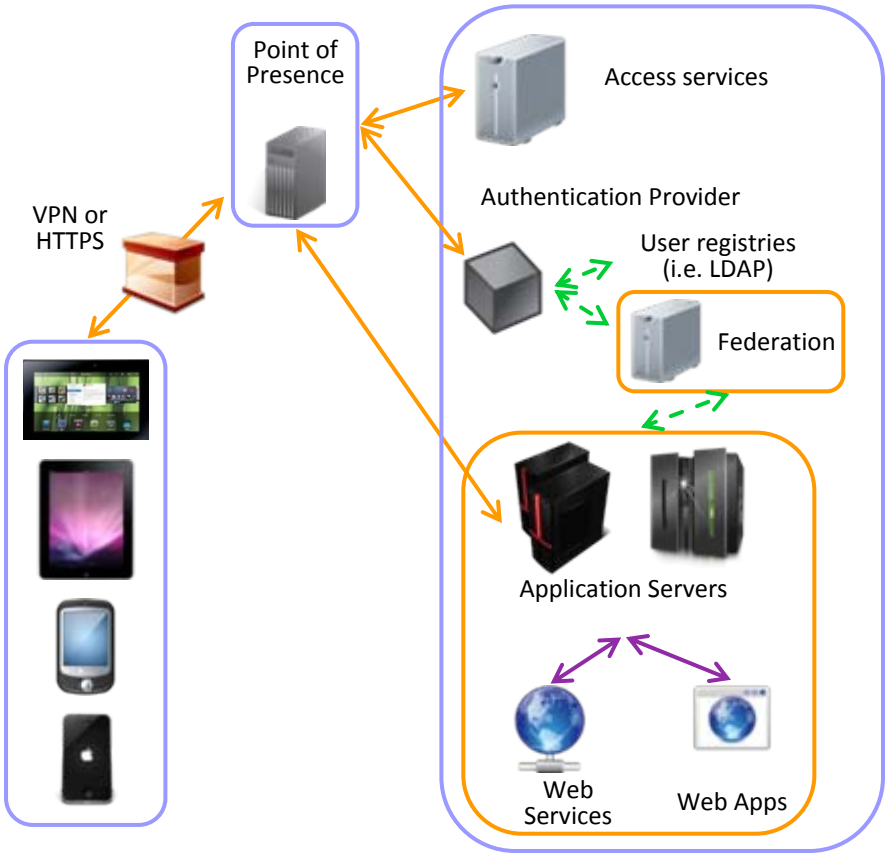
Managing and securing enterprise and BYOD mobile devices without additional resources

## Key functional requirements

- 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

# Provide consistent User & Access Management

*Extending Access Management strategy to support mobile use cases for apps*




## Client Challenge

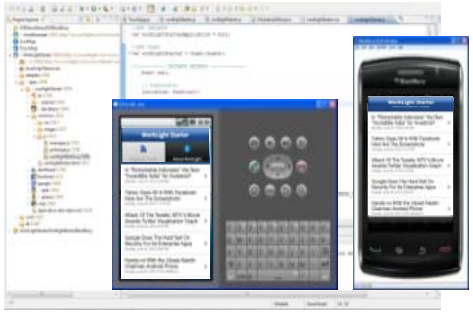
Ensuring users and devices are authorised to access enterprise resources from that specific device.

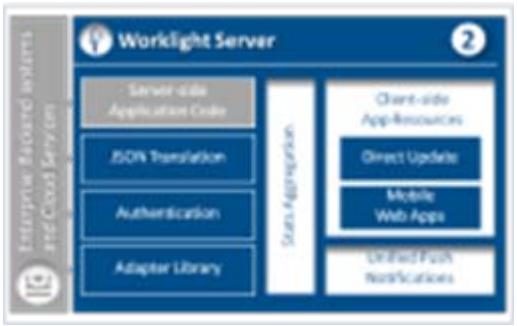
## Key functional requirements

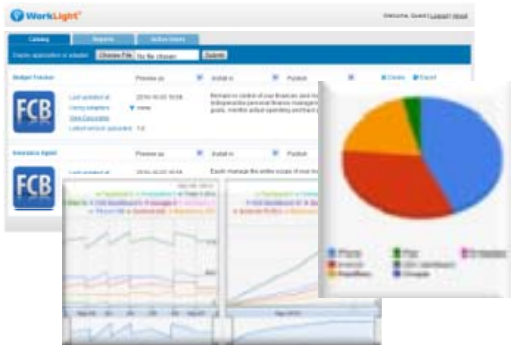
- Satisfy complex context-aware authentication requirements
- Reverse proxy, authentication, authorisation, and federated identity
- Mobile native, hybrid, and web apps
- Flexibility in authentication: user id/password, basic auth, certificate, or custom
- Supports open standards applicable to mobile such as OAuth
- Advanced Session Management

# Deliver and Manage Safe Mobile Applications (Apps)

*Application development processes need a consistent platform for implementation*





## Client Challenge

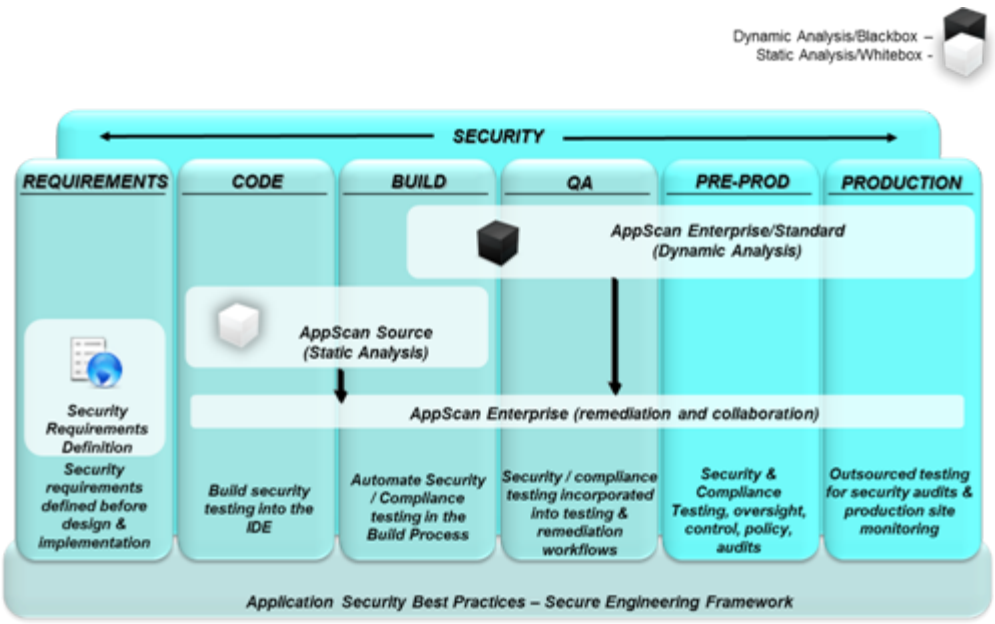
Efficiently and securely, create and run HTML5, hybrid and native mobile apps for a broad set of mobile devices

## Key functional requirements

- Integrated secure access to backend application resources
- Secured by design - develop secure mobile apps using corporate best practices, e.g. code obfuscation
- Protect mobile app data with encrypted local storage for data, offline user access, app authenticity validation, and enforcement of organisational security policies

# Deliver Security-Rich Applications (Apps)

*Application security testing for 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 functional requirements

- Leverage application scanning 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 into development

# Provide a Flexible set of Connectivity options

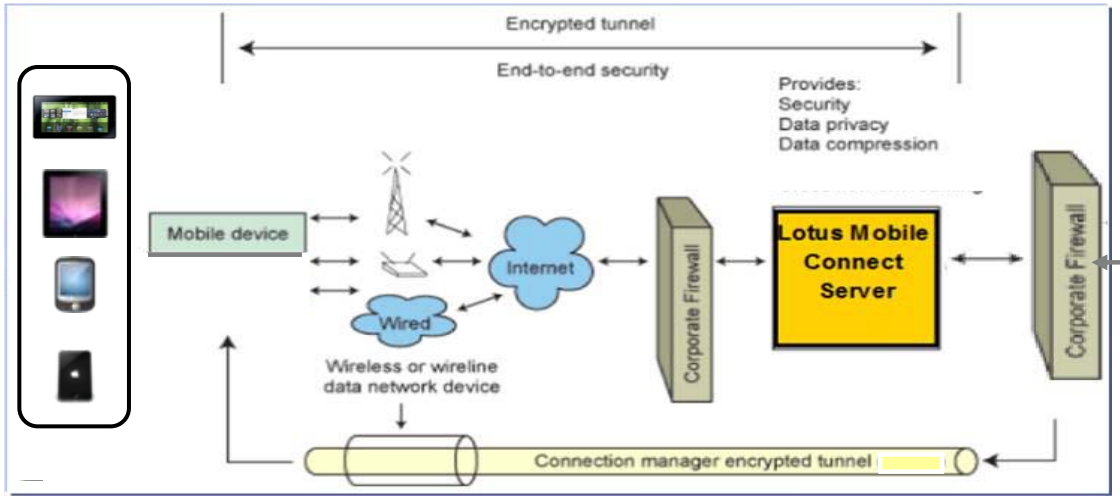
*Deliver a security-rich connection to enterprise resources from mobile devices*

## Client Challenge

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

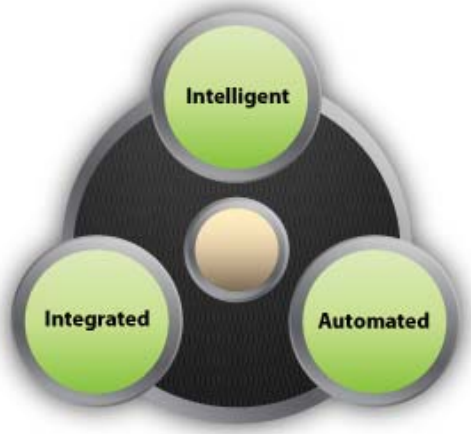
## Key functional requirements

- Minimum app level Virtual Public Network (VPN) with a SSL-secured tunnel to specific HTTP application servers
- Strong authentication and encryption of data in transit



# Deliver An Adaptive Security Posture

*Deliver mobile security intelligence by monitoring data collected – visibility, reporting and threat detection*





## Client Challenge

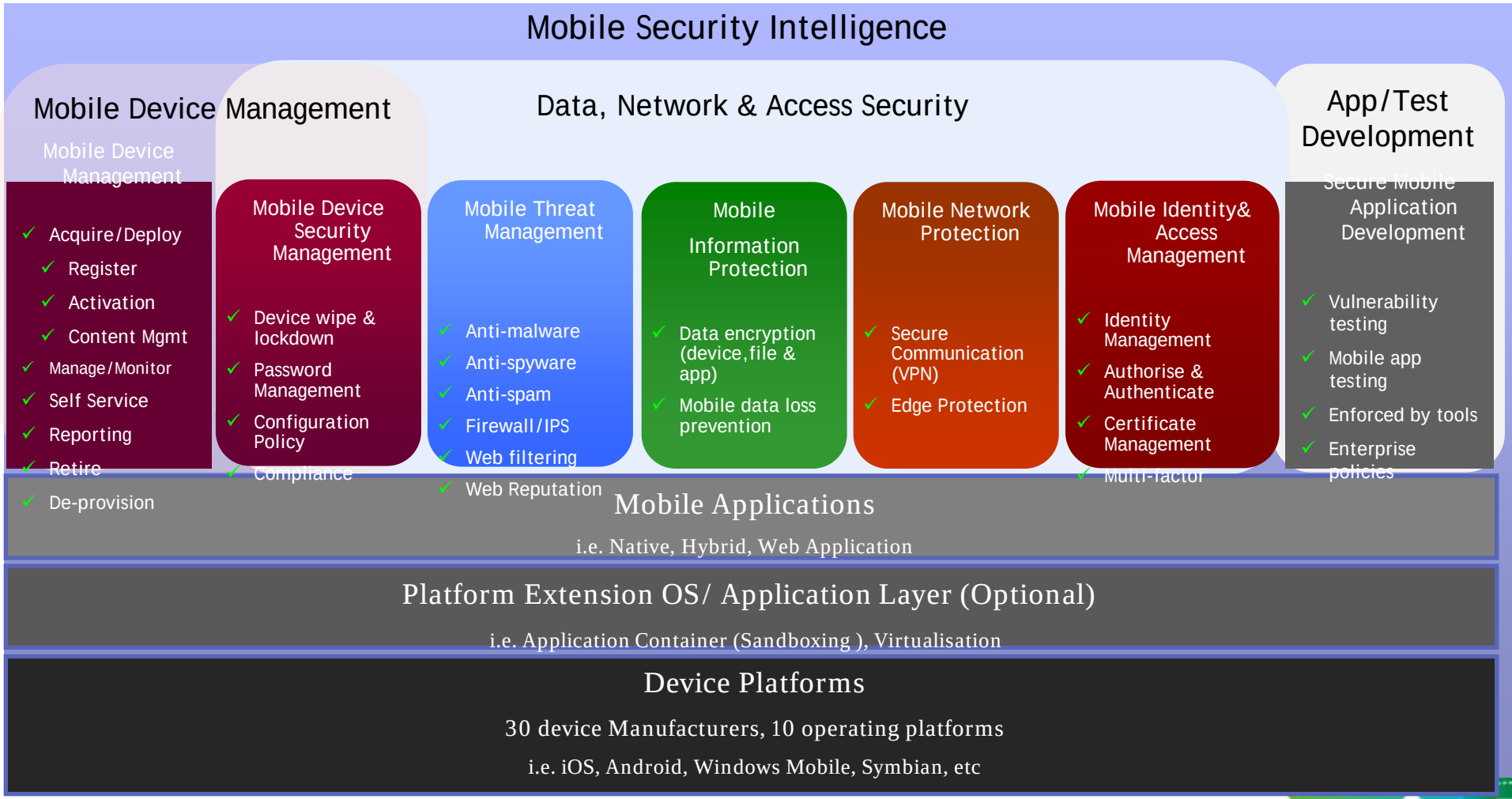
Visibility of security events across the enterprise, to stay ahead of the threat, show compliance and reduce enterprise risk

## Key functional requirements

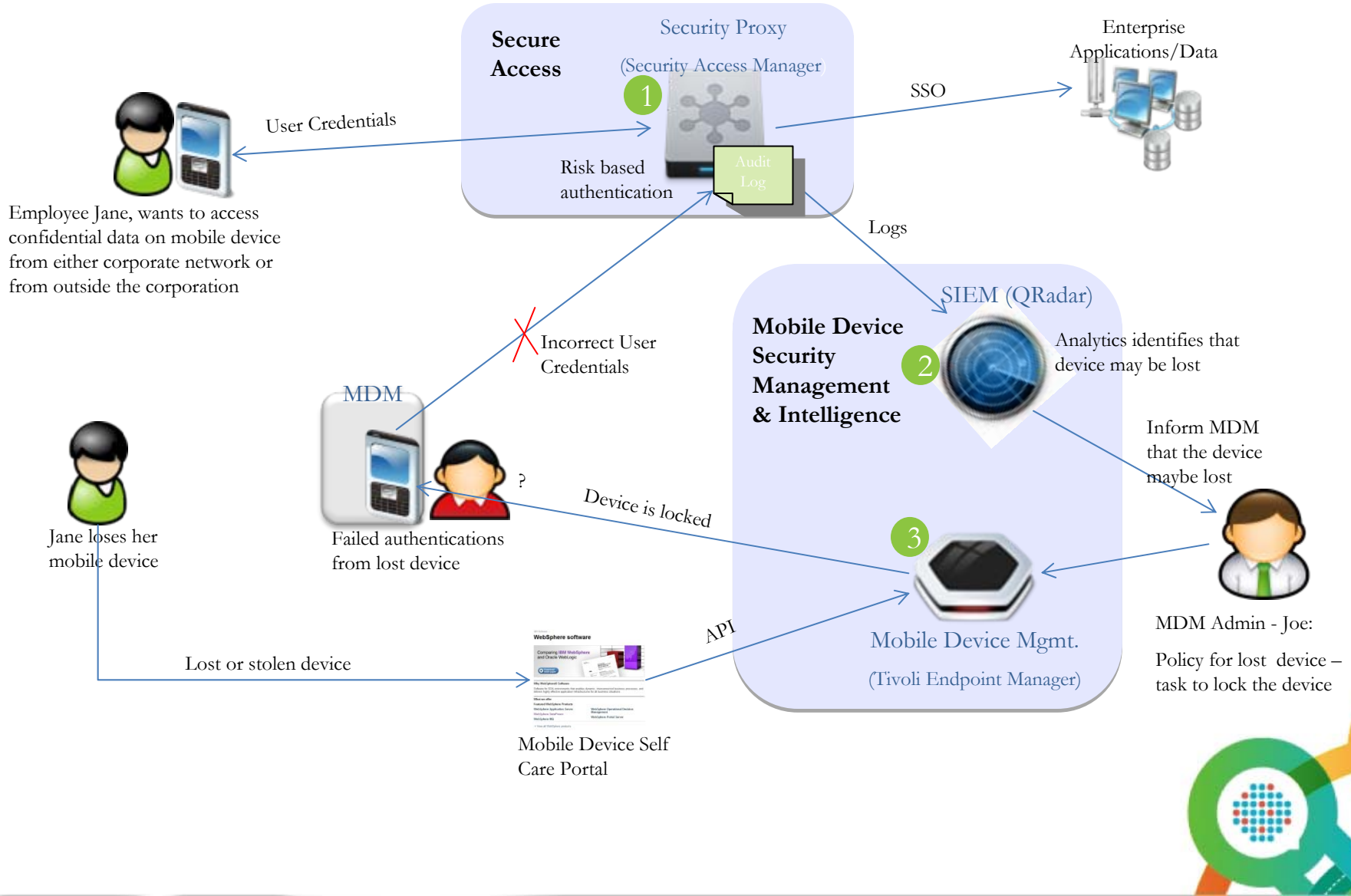
- Integrated intelligent actionable platform for
  - Searching
  - Filtering
  - Rule writing
  - Reporting functions
- A single user interface for
  - Log management
  - Risk modeling
  - Vulnerability prioritization
  - Incident detection
  - Impact analysis tasks

# IBM's Mobile Security Strategy

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



# Mobile Security Intelligence Sample Use Case



## Major Australian Bank

***Better protection for mobile banking transactions***

- Over 1,500,000 mobile customer devices
- Centralized user security and policy management
- Single security infrastructure for multiple user touchpoints

## IBM Corporation

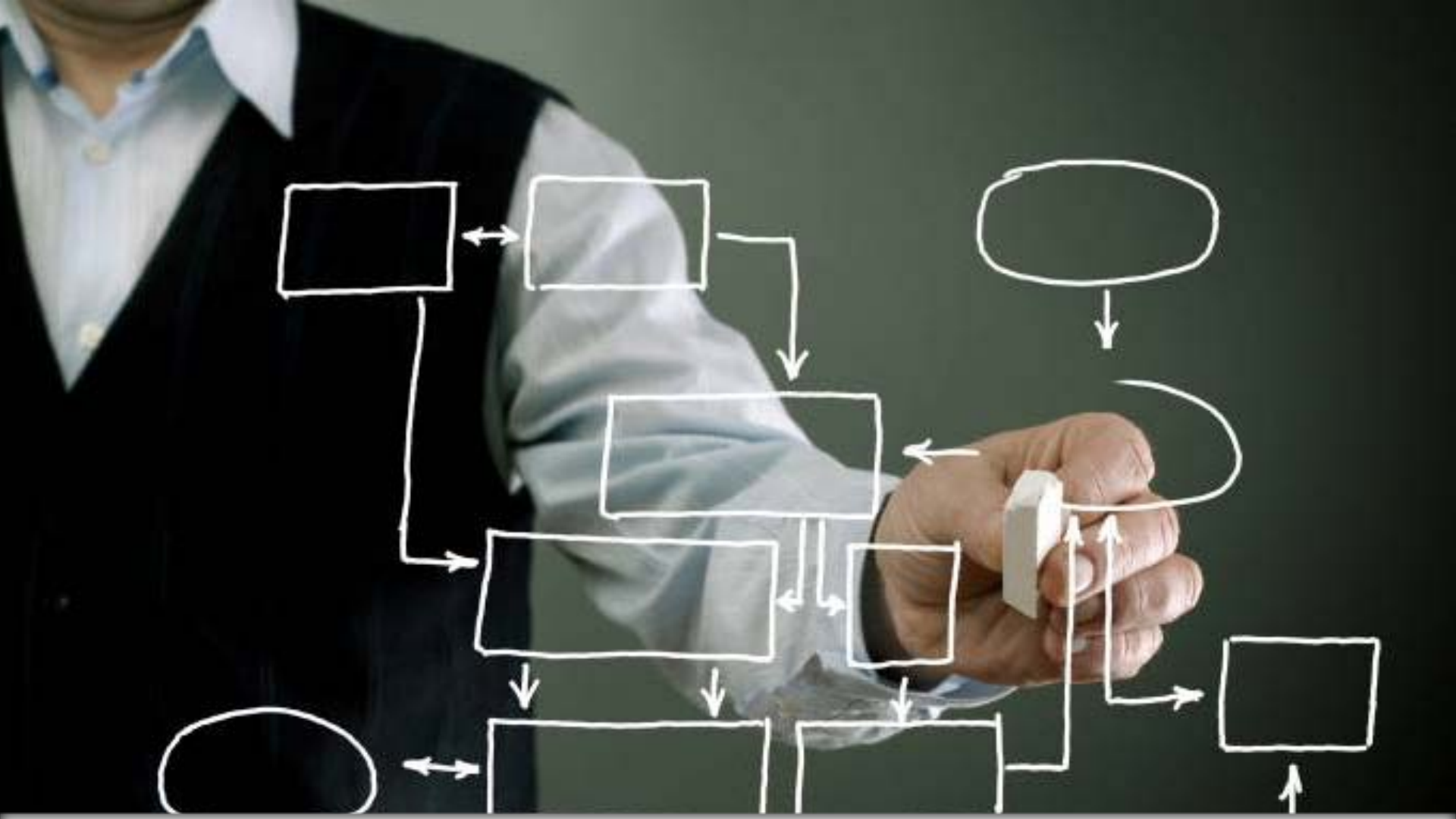
***Security for BYOD for a variety of platforms***


- 120,000 mobile devices deployed in months
- Reduced infections by 80-90%
- Achieve 98% patch compliance within 24 hours

# Your security team sees…

# Clarity…

# Insights…



# Everything…

# Security Intelligence