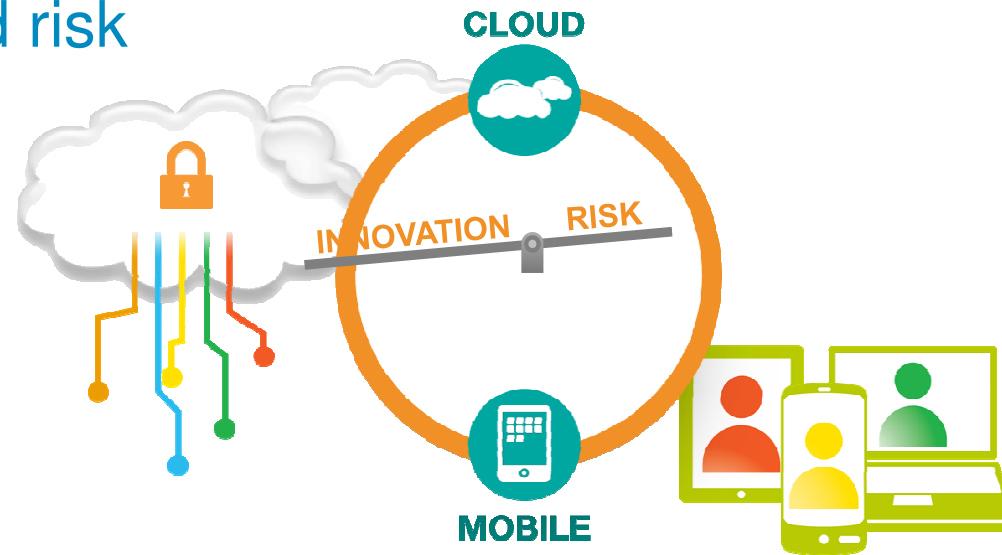


# Secure mobile transactions: weakest link or safest bet?

Martin Borrett  
Director of the IBM Institute for Advanced Security  
Europe



## Customers are faced with challenge of balancing innovation and risk



- 1 Cloud and mobile create opportunities for enhanced security
- 2 IBM security portfolio enables clients to innovate with confidence
- 3 IBM mobile security portfolio enables clients to manage mobile device, application and transactions

## Agenda

- Mobile Security – Landscape and Strategy
  
- IBM Mobile Security Solutions
  - Protect the
    - Device
    - Application
    - Transaction
  
- Summary



# Mobile Security and Management spans business control spectrum

## Requirements for Mobile Management and Security:



## Solution Approaches:



# Mobile Security and Management spans business control spectrum

## Requirements for Mobile Management and Security:



## Solution Approaches:



## IBM Offerings:



**IBM Security  
Access Manager  
for Mobile**



## Additional Integration Points:

- SDKs can be used in Worklight IDE so all apps can be secured (**IBM Worklight**)
- Security information and events will feed into QRadar for analysis and actions will return to mobile tools (**IBM QRadar**)
- Code scan can be part of process before apps are deployed into app store/catalog (**IBM AppScan**)



# IBM Security capabilities for the mobile enterprise



<i>Protect the Device</i>	<i>Protect the Application</i>	<i>Protect the Transaction</i>
Solutions to manage a diverse set of mobile devices from corporate owned assets to BYOD and do it all easily from the cloud.	Developer solutions to secure applications by design early in the development process. Protect enterprise data in both the applications you build and the applications you buy.	Solutions to protect mobile transactions with customers, business partners, and temporary workers that are not part of your enterprise mobile management framework.
<b>SECURITY INTELLIGENCE</b>		
A unified architecture for integrating mobile security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management.		





# Addressing Mobile Security challenges with IBM solutions



# Threat-Aware Identity and Access Management

*Capabilities to help organizations secure enterprise identity as a new perimeter*

## Safeguard mobile, cloud and social interactions

- **Validate “who is who”** when users connect from outside the enterprise
- **Enforce proactive access policies** on cloud, social and mobile collaboration channels

## Deliver intelligent identity and access assurance

- **Enable identity management** for the line of business
- **Enhance user activity monitoring** and security intelligence across security domains



## Prevent insider threat and identity fraud

- **Manage shared access** inside the enterprise
- **Defend applications and access** against targeted web attacks and vulnerabilities

## Simplify identity silos and cloud integrations

- **Provide visibility** into all available identities within the enterprise
- **Unify “Universe of Identities”** for security management





# As part of our Mobile Security strategy, IBM has launched its **NEW** appliance-based solution - **IBM Security Access Manager for Mobile**

Safeguard mobile, cloud and social interactions



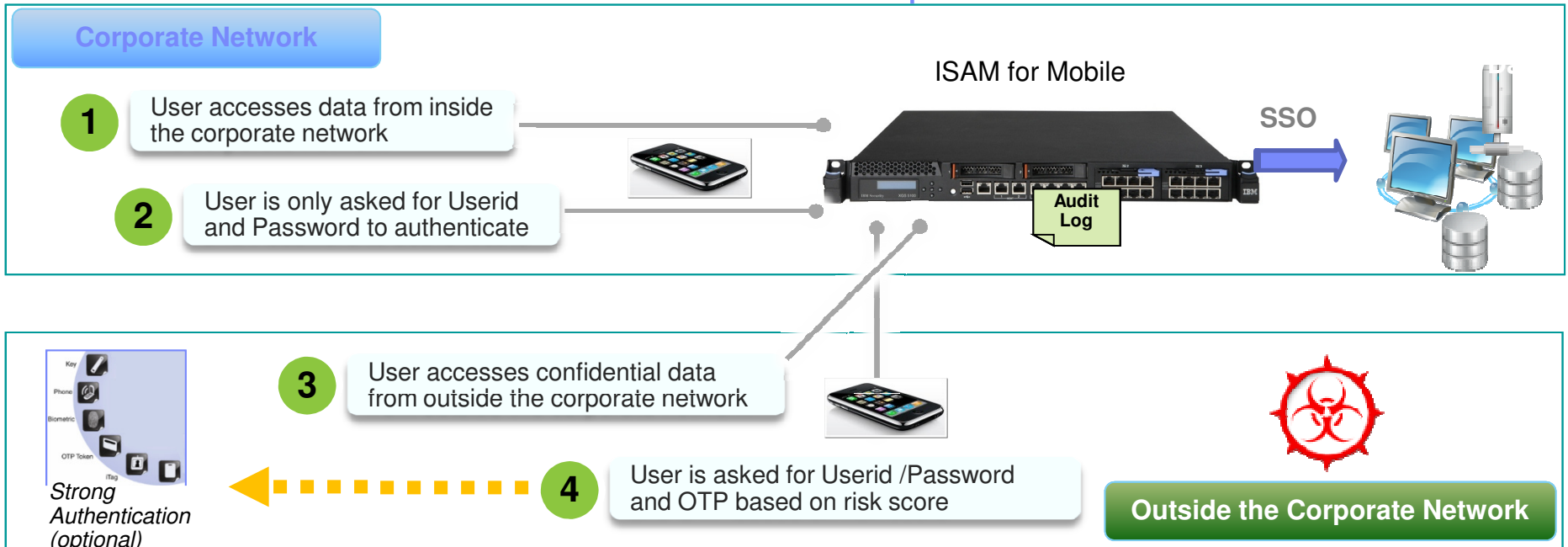
## IBM Security Access Manager for Mobile



- **Deliver Mobile SSO and session management** to help secure employee and consumer access to mobile and web apps
- **Enforce context-aware access** with mobile device fingerprinting, geo-location awareness and IP Reputation
- **Improve identity assurance** using built-in mobile authentication service and one-time-password use
- **Help secure mobile app deployment** with IBM WorkLight and QRadar security intelligence integration to support access control
- **Reduce TCO and time to value** with an “all-in-one” access appliance in virtual and hardware form factors



## Deliver mobile SSO and session management for employees, partners and consumer interactions across the enterprise



### How IBM SAM for Mobile Can Help

- ✓ Deploy mobile security gateway for user access based on risk-level (e.g. permit, deny, step-up authenticate)
- ✓ Built-in Risk scoring engine using user attributes and real-time context (e.g. location, device)
- ✓ Support mobile authentication with built-in One-Time Password (OTP) and ability to integrate with 3<sup>rd</sup> party strong authentication vendors, as needed
- ✓ Offer Software Development Kit (SDK) to integrate with 3rd party authentication factors and collect additional contextual attributes from the device and user session

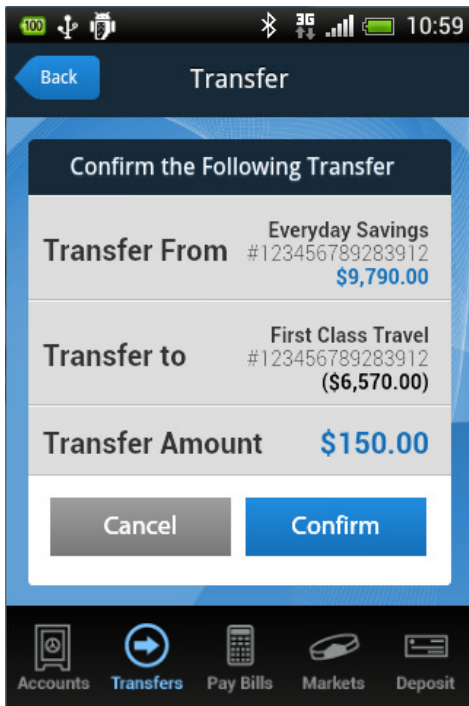


## Enforce risk-based access and strong authentication for transactions

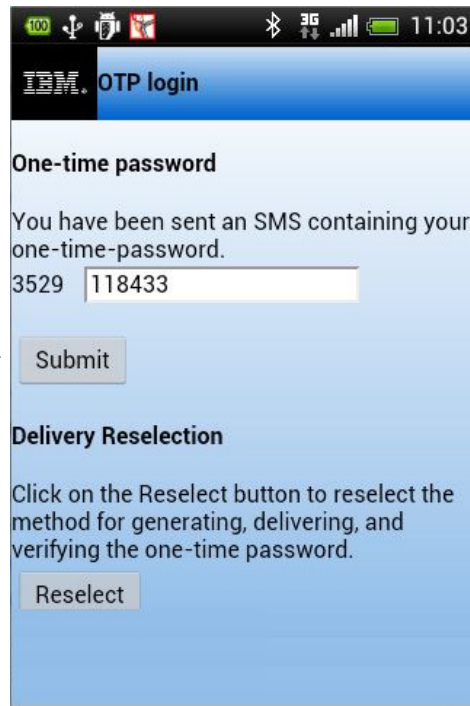
### Reduce risk associated with mobile user and service transactions

- ✓ Example: transactions less than \$100 are allowed with no additional authentication
- ✓ User attempts transfer of amount greater than \$100 – requires an OTP for strong authentication

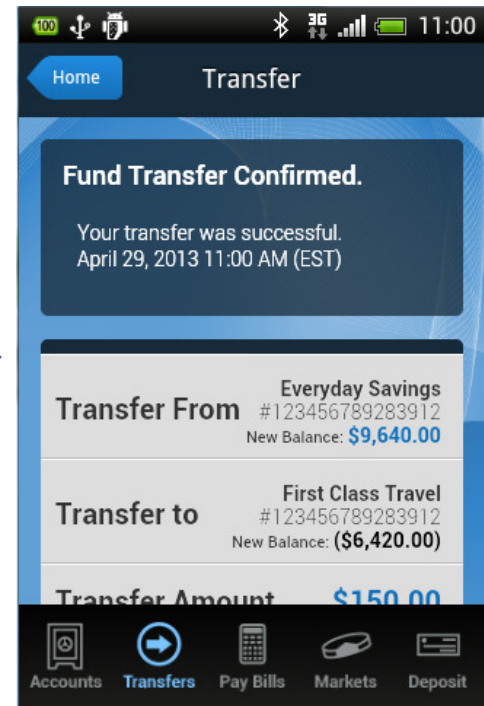
User attempts high-value transaction



Strong authentication challenge



Transaction completes



# Get "Mobile Security Intelligent" with OOTB QRadar integration

Potential Data Loss  
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	<u>10.103.14.139</u> (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

Who?  
An internal user

What?  
Oracle data

- Navigate
- Information
- Resolver Actions
- TNC Recommendation

- DNS Lookup
- WHOIS Lookup
- Port Scan
- Asset Profile
- Search Events
- Search Flows

**QRadar Has Completed Your Request**

Go to APNIC results

[Querying whois.arin.net]  
[whois.arin.net]

OrgName: Google Inc.  
OrgID: GOGL

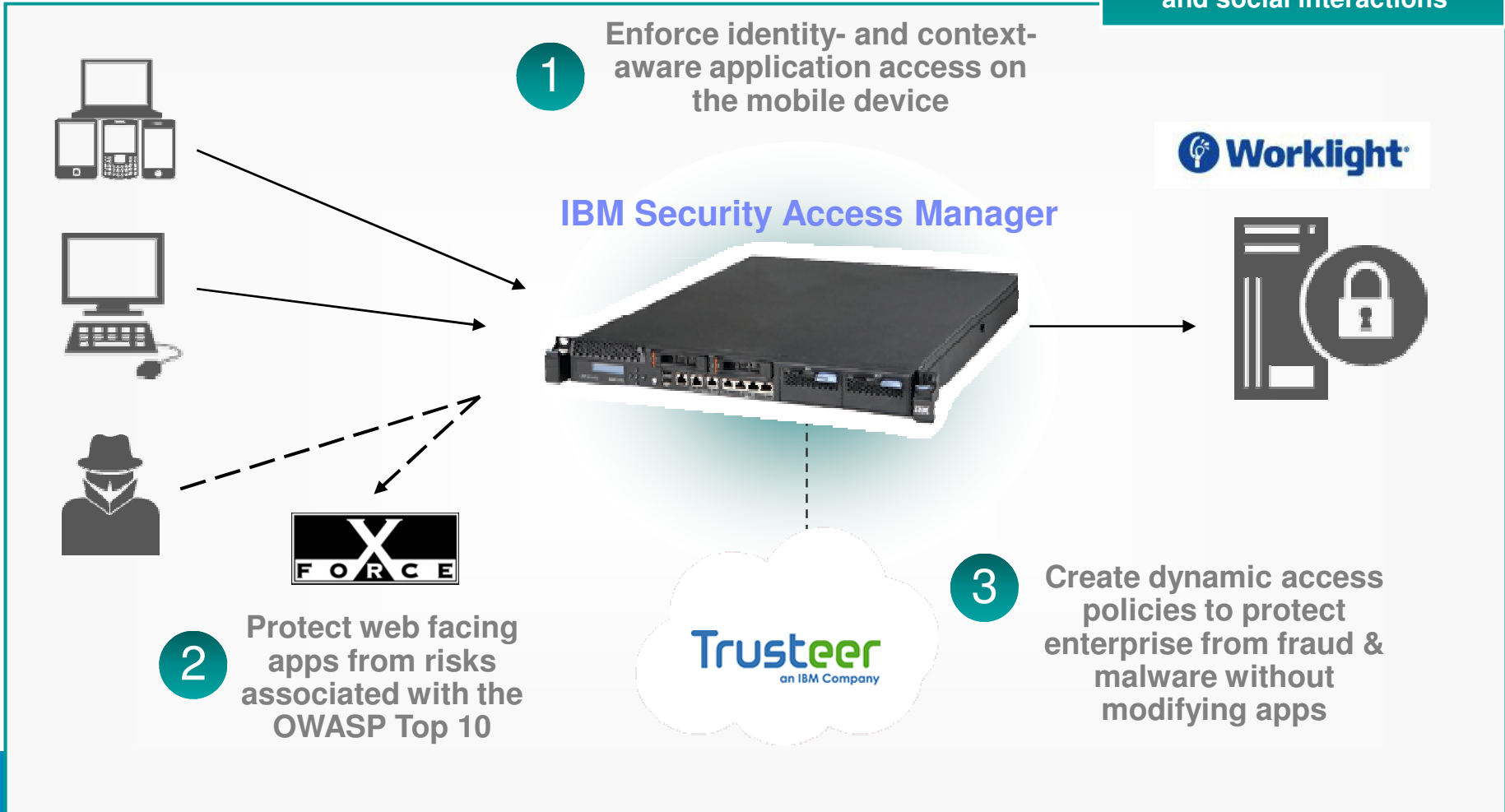
Where?  
Gmail



# Mobile Security: Centralized and Consistent Policy Enforcement for Context-Aware Access, Threat Protection, Fraud & Malware Detection

*Out-of-the-box and seamless integration delivers unmatched end-to-end security*

Safeguard mobile, cloud and social interactions



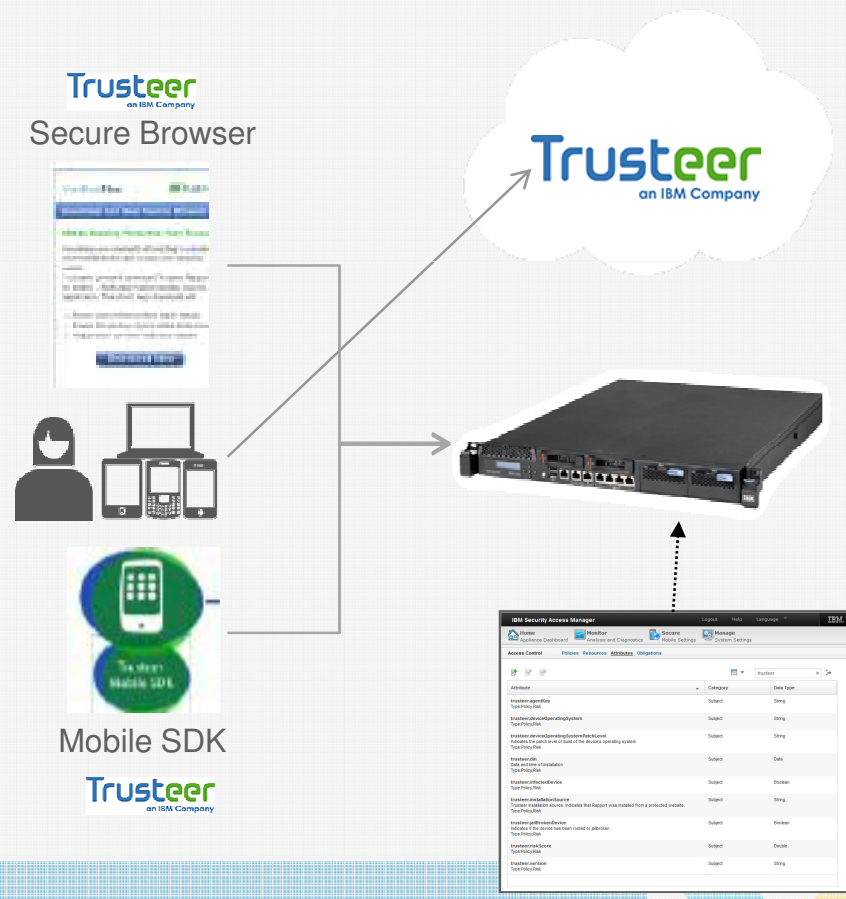
# Easier Fraud & Malware Detection with IBM SAM for Mobile and Trusteer

*Attach Trusteer context-based policy to any app resources with no code updates*

**NEW**

**Safeguard mobile, cloud and social interactions**

- Out-of-the-box recognition of Trusteer-specific attributes being included in request messages from Secure Browser and Mobile SDK
  - Device attributes
  - Malware
  - Jailbroken / rooted
- Author reusable policies that can be attached to multiple applications
- Enforce consistent fraud & malware detection policies without updating the apps





## Securing mobile identities

*An international banking organization targeting mobile user access for employees and end users*

Safeguard mobile, cloud and social interactions

North American entity secures user access from mobile and web channels

**10,000**

internal users by end of 2013

Mobile Users



Any Device



Web & Mobile Apps

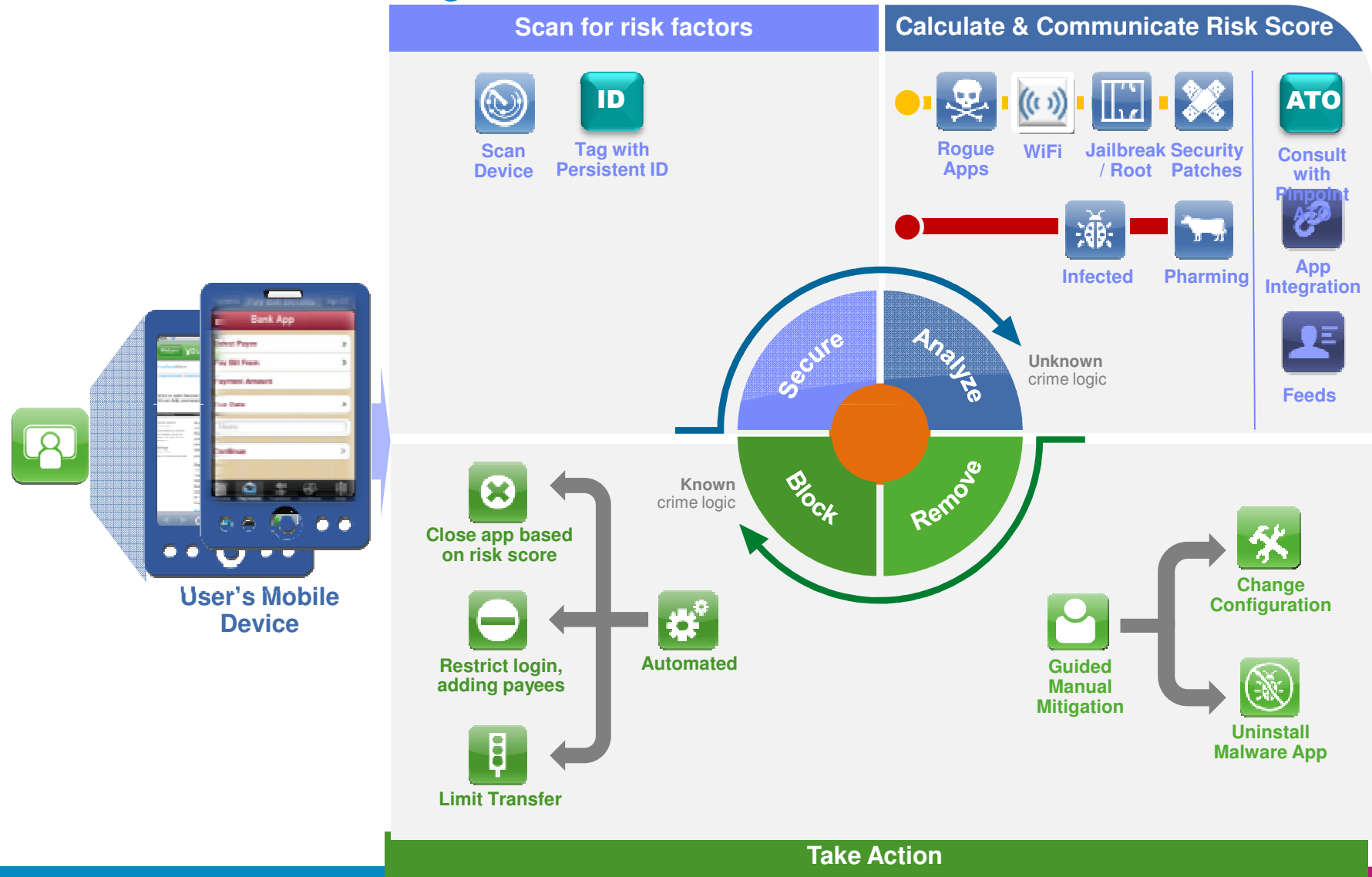
### **Business challenge**

- Secure employees and contractors access to web and mobile apps
- Rollout new mobile apps; ensure end user access from mobile devices
- Eliminate passwords as a weak link to enforce access to web and mobile

### **Solution benefits**

- Centralized user access control across web and mobile channels consistently
- Reduced IT cost with self-care, single sign-on and session management
- Introduced risk-based access and multi-factor authentication for 10M+ users

# Fraud Protection using Trusteer to Secure Mobile





## MaaS360 Delivers an Integrated Approach



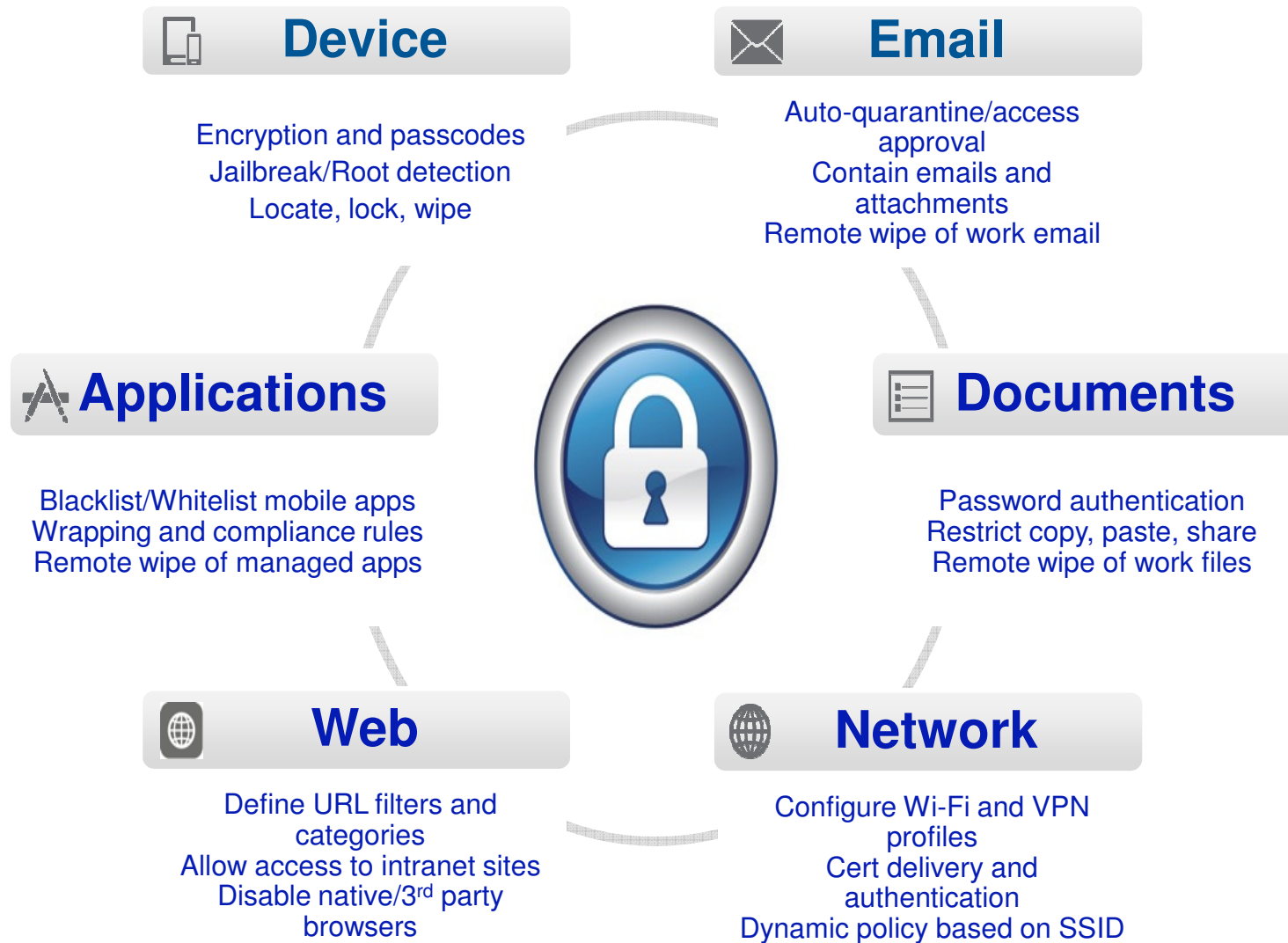
**Comprehensive Mobile Security**

**Complete Mobility Management**

### One Platform for All Your Mobile Assets



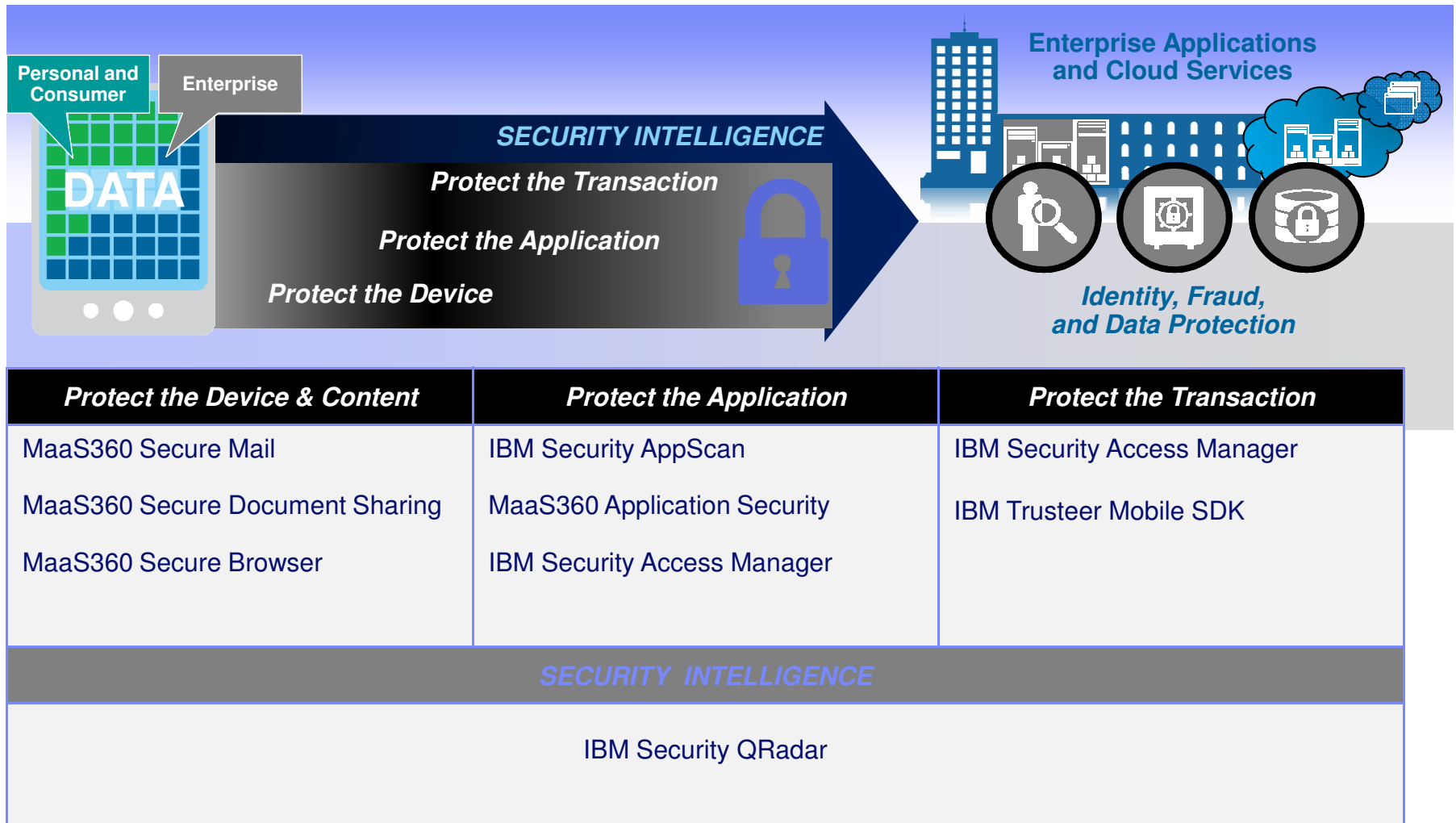
# MaaS360: Robust Mobile Security addressing BYOD



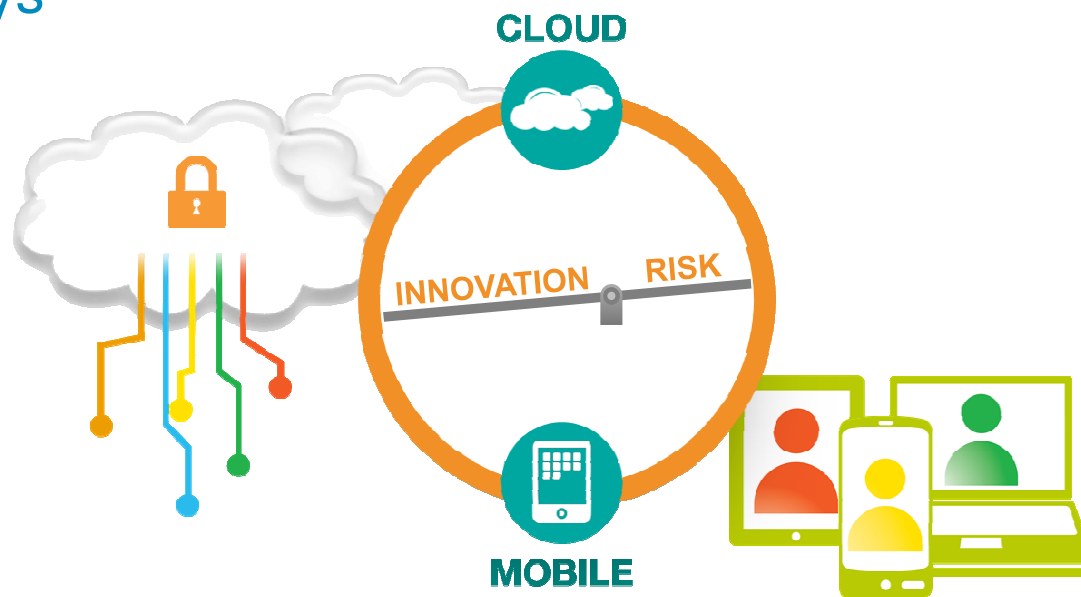
# Summary



# IBM Security capabilities for the mobile enterprise



## Key takeaways



- 1 Cloud and mobile create opportunities for enhanced security
- 2 IBM security portfolio enables clients to innovate with confidence
- 3 IBM mobile security portfolio enables clients to manage mobile device, application and transactions