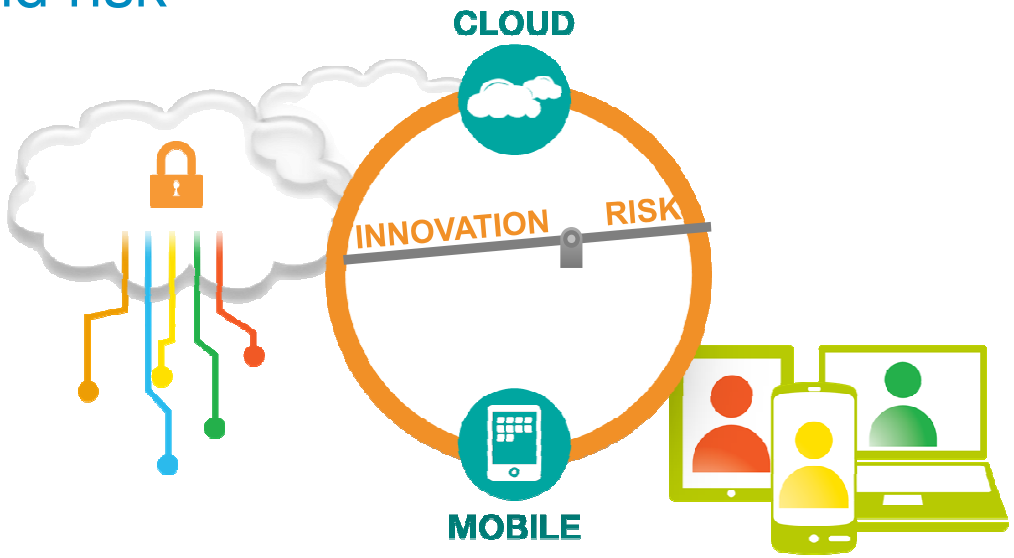
Secure mobile transactions: weakest link or safest bet?

Avi Dayan
R&D Engineer
Security Researcher @ AppScan Lab
Israel

IBM

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:

MaaS360 by Fiberlink

IBM Security Access Manager for Mobile

Trusteer an IBM Company

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 be part of process before apps are deployed into app store/catalog **(IBM AppScan)**

IBM Security capabilities for the mobile enterprise

Protect the Device	Protect the Application	Protect the Transaction
• Corporate devices • BYOD	• Developer solutions to secure applications. • Protect enterprise data in both the applications you build and the applications you buy.	• Customers • Business partners • Temporary workers

SECURITY INTELLIGENCE

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"
- Enforce proactive access policies

Prevent insider threat and identity fraud

- Manage shared access
- Defend applications and access

Deliver intelligent identity and access assurance

- Enable identity management
- Enhance user activity monitoring

Simplify identity silos and cloud integrations

- Provide visibility
- Unify "Universe of Identities"

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

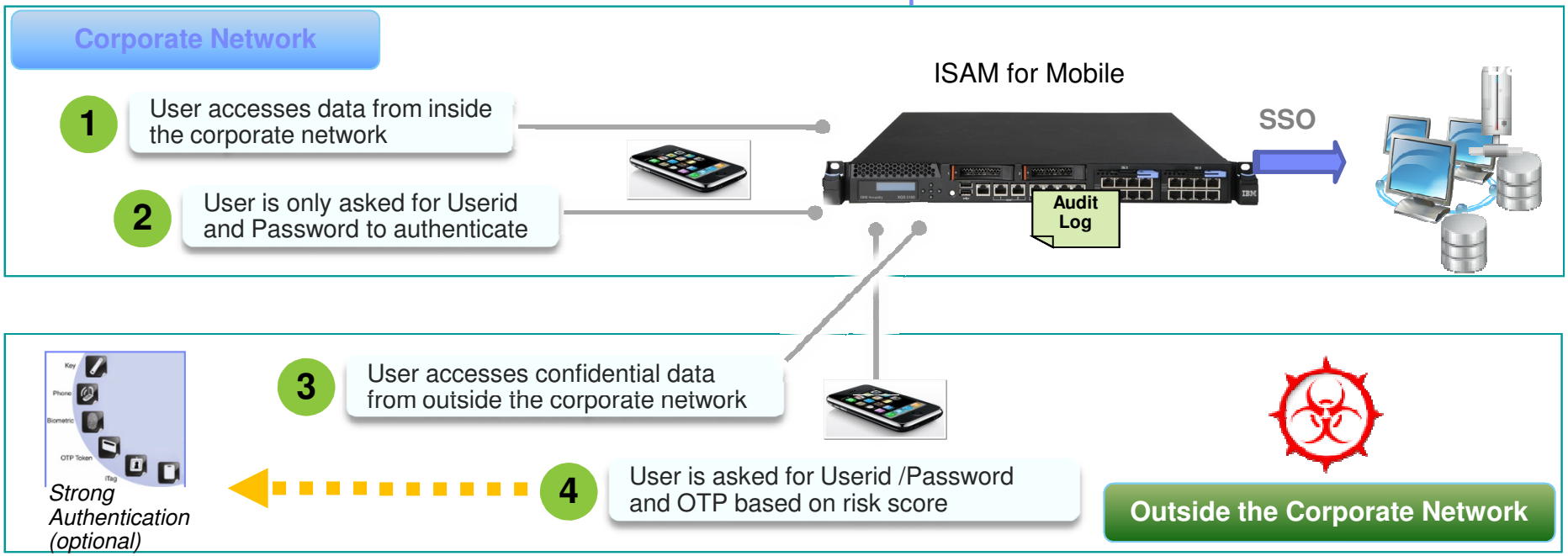
NEW

IBM Security Access Manager for Mobile

- **Mobile Access Management**
- **Mobile Identity Assurance**
- **Mobile Security Intelligence**

- **Deliver Mobile SSO and session management**
- **Enforce context-aware access**
- **Improve identity assurance**
- **Help secure mobile app deployment**
- **Reduce TCO and time to value**

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



How IBM SAM for Mobile Can Help

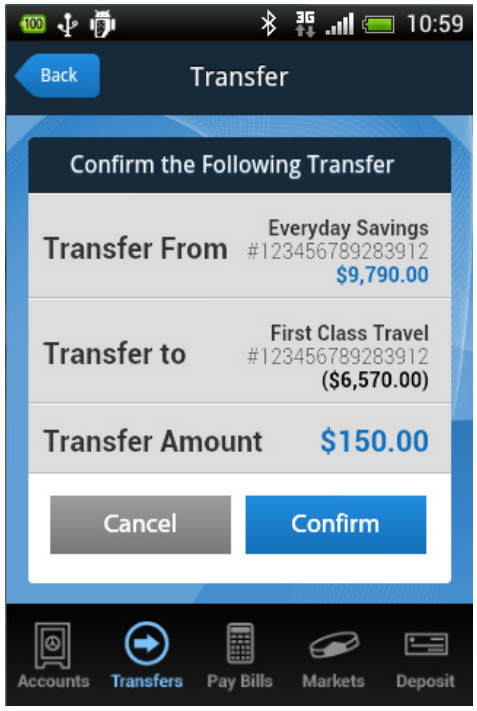
- ✓ Deploy mobile security gateway for user access based on risk-level (e.g. permit, deny, step-up authenticate)
- ✓ Built-in Risk scoring engine real-time context (e.g. location, device)
- ✓ Support mobile authentication with built-in One-Time Password (OTP)
- ✓ Offer Software Development Kit (SDK) to integrate with 3rd party authentication factors

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

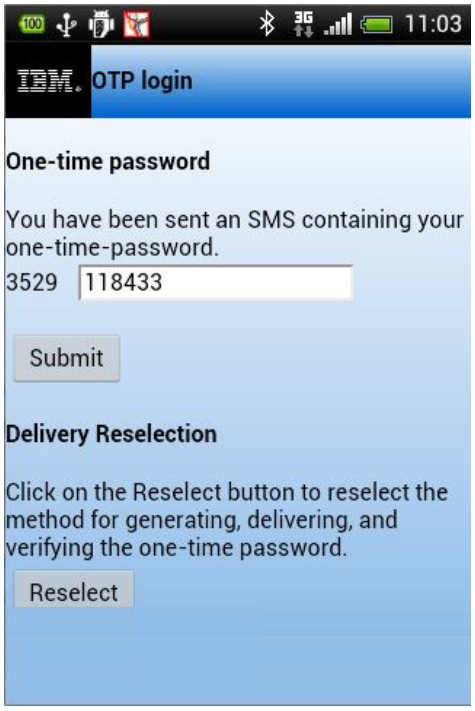
Reduce risk associated with mobile user and service transactions

- ✓ 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

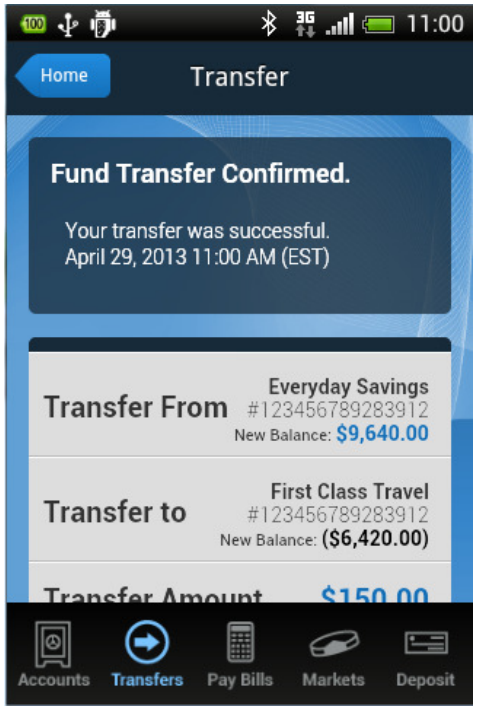
User attempts high-value transaction



Strong authentication challenge



Transaction completes



Get "Mobile Security Intelligent" with OOTB QRadar integration

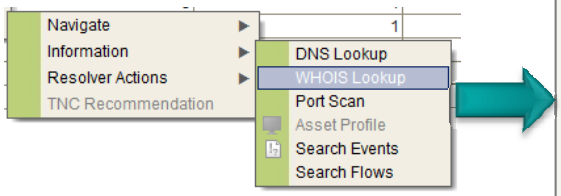
Potential Data Loss
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.1[illegible].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



QRadar Has Completed Your Request

Go to APNIC results

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

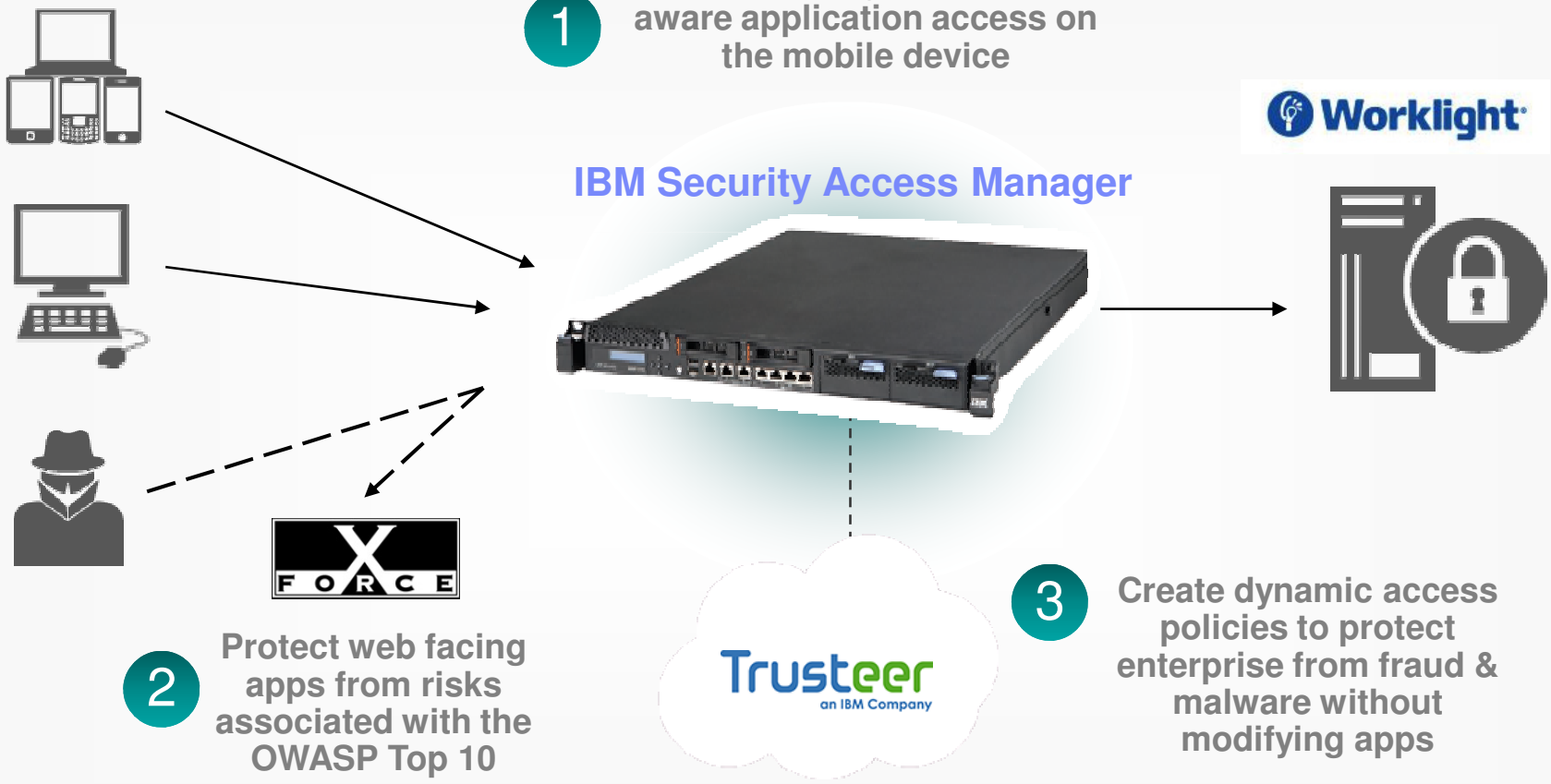
OrgName: Google Inc.
OrgID: GOGL

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



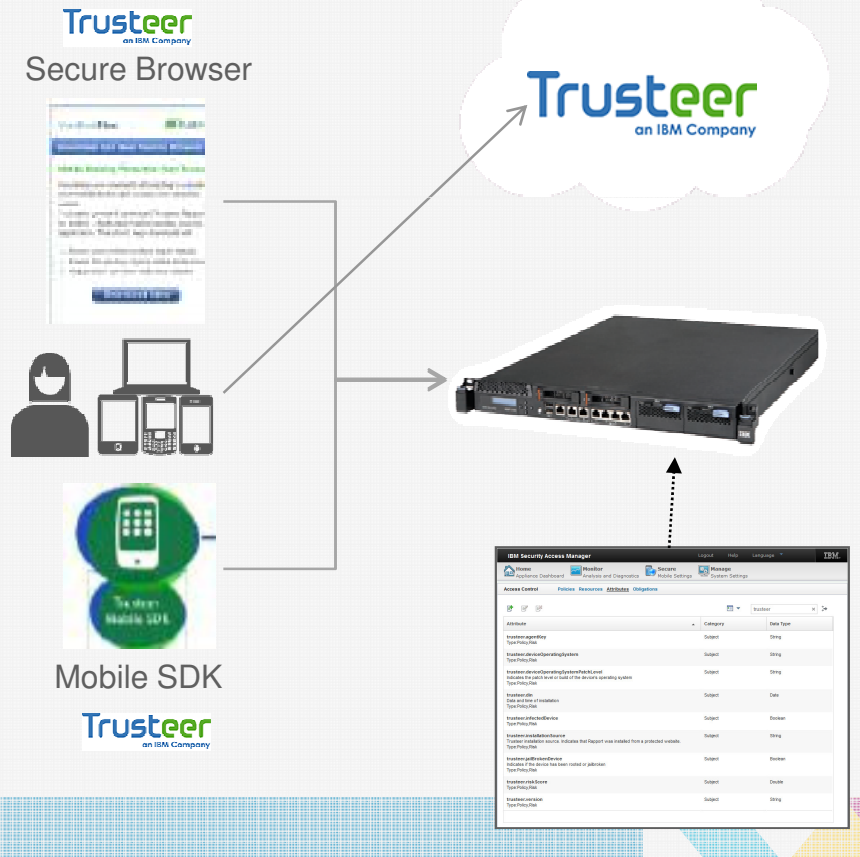
Easier Fraud & Malware Detection with IBM SAM for Mobile and Trusteer

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

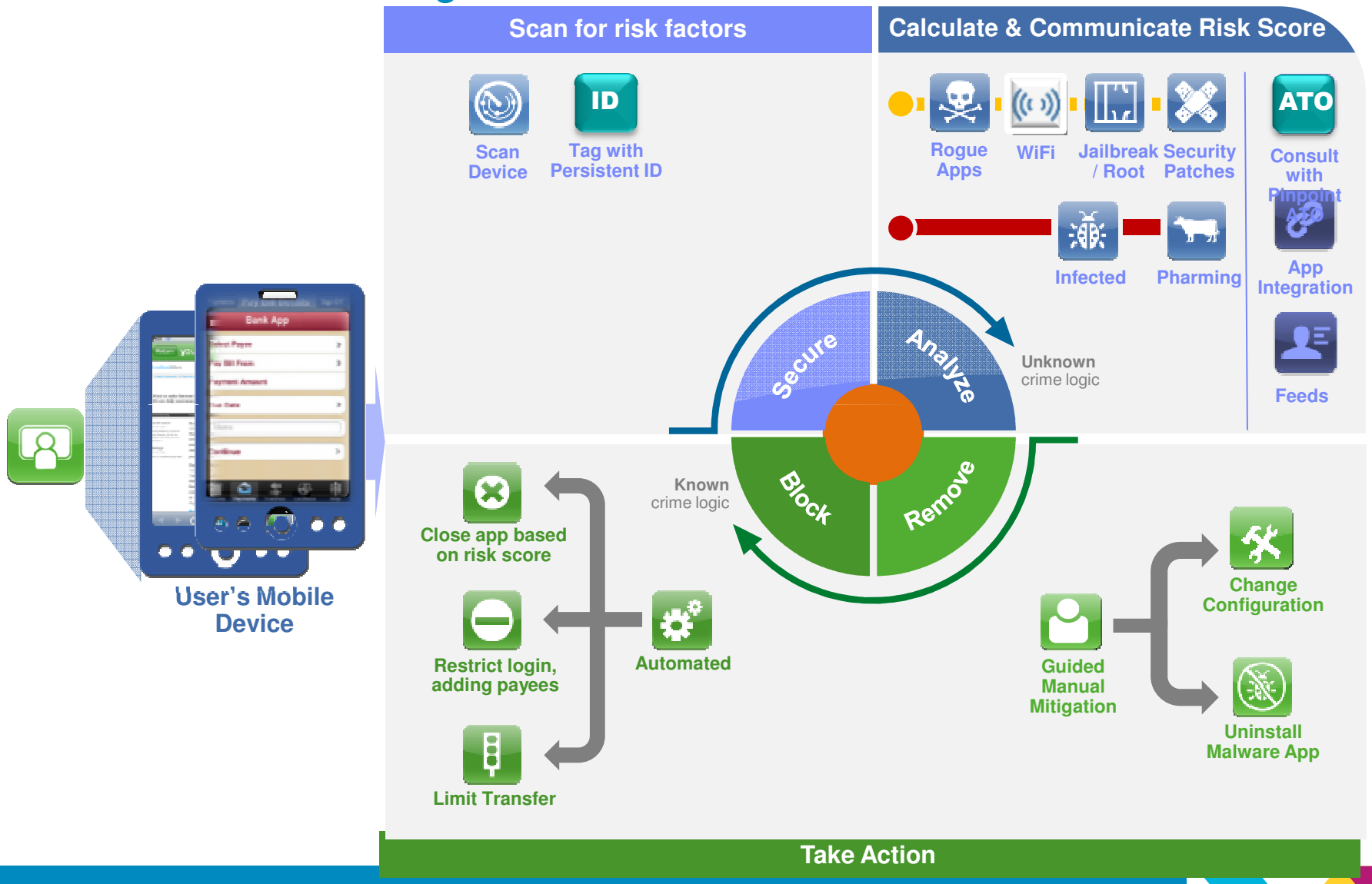
NEW

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



Fraud Protection using Trusteer Secure Mobile



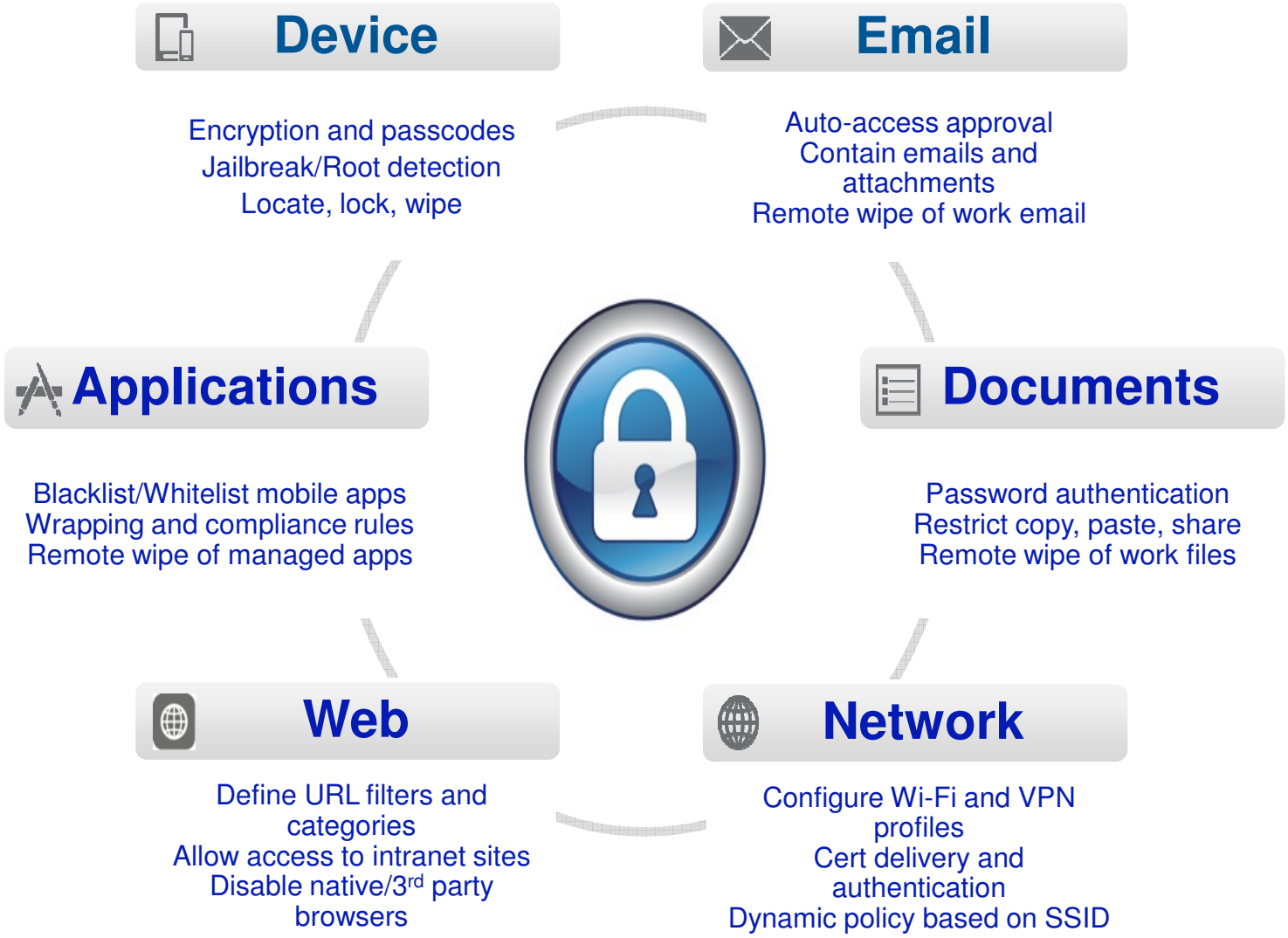
MaaS360 Delivers an Integrated Approach

Comprehensive Mobile Security

Complete Mobility Management

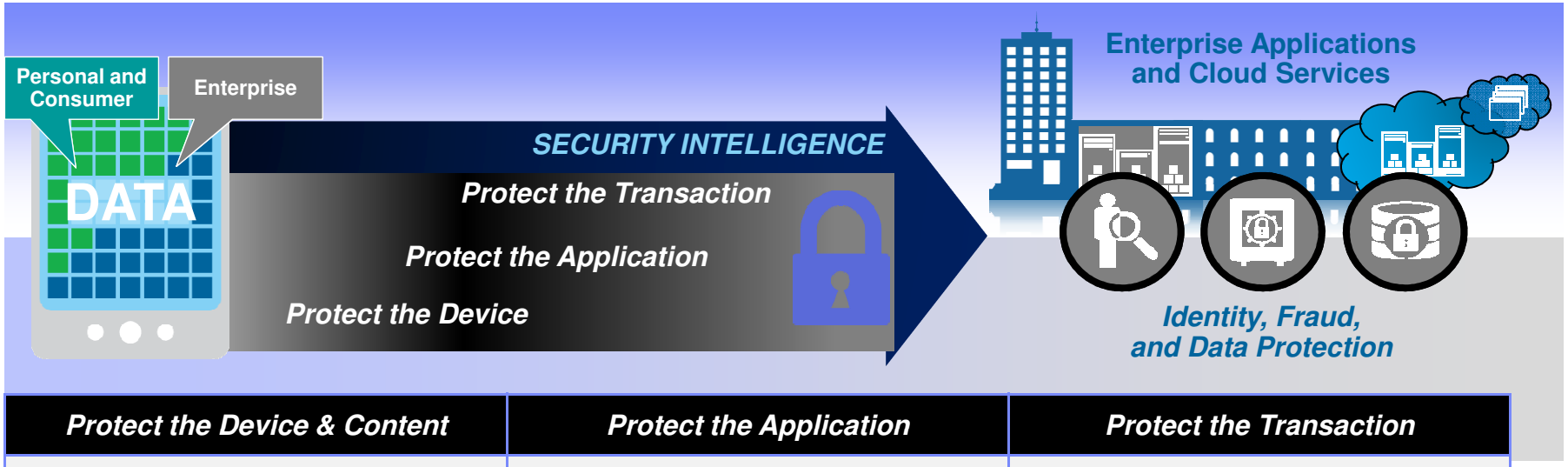
One Platform for All Your Mobile Assets

MaaS360: Robust Mobile Security addressing BYOD



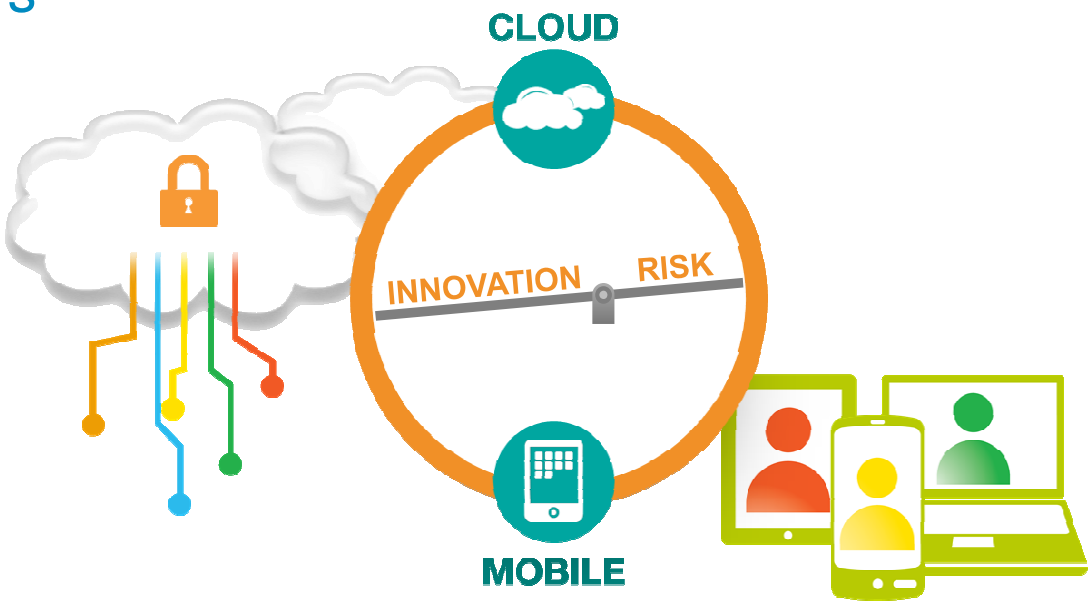
Summary

IBM Security capabilities for the mobile enterprise



Protect the Device & Content	Protect the Application	Protect the Transaction
MaaS360 Secure Mail	IBM Security AppScan	IBM Security Access Manager
MaaS360 Secure Document Sharing	MaaS360 Application Security	IBM Trusteer Mobile SDK
MaaS360 Secure Browser	IBM Security Access Manager	
SECURITY INTELLIGENCE		
IBM Security QRadar		

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