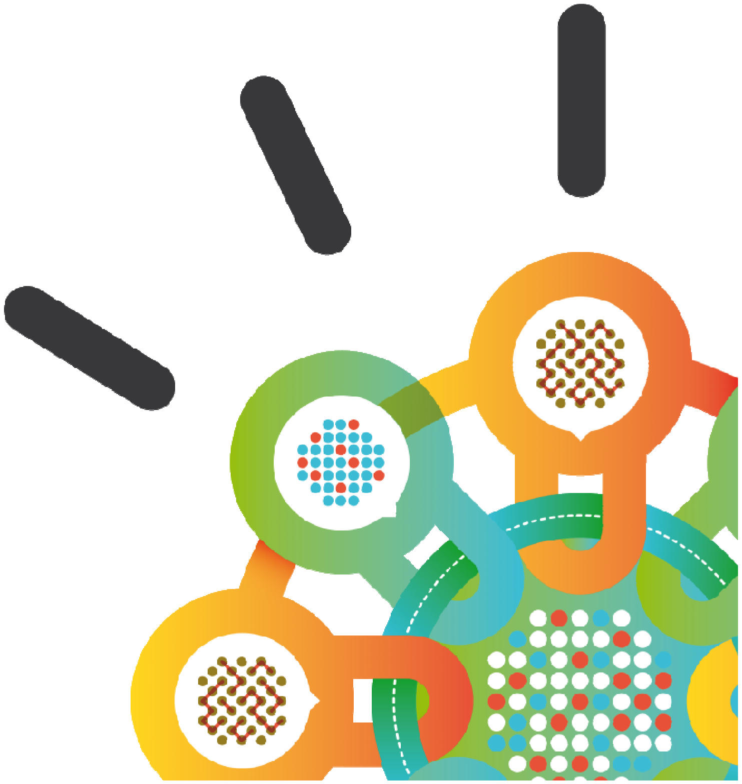
Security Intelligence.
Think Integrated.

Protect What's Yours –
Secure access in the era of mobile, cloud & social



Vaughan Harper
IBM Security Architect

vaughan_harper@uk.ibm.com

30 April, 2014

Business demands are leading to unprecedented security concerns

Business Transformations

mobile, cloud and social interactions

Strong business demands to access corporate resources anytime/anywhere through mobile devices, deploy cloud delivery models and interact via social media

Bring-your-own-device

Popularity of BYOD programs

With the increasing popularity of bring-your-own-device (BYOD) programs, employees, contractors and business partners also use their own devices within the workplace

Evolving Threats

Targeted attacks are the new norm

As IBM X-Force continues to see operationally sophisticated attacks, it is critical to check unauthorized access to sensitive data/applications and fraudulent execution of sensitive transactions

Compliance

Mandates are increasing

Insights into user and application behavior especially in mobile devices is required to enhance security controls. Also, need context-based policy enforcement across B2E and B2C use cases

Landscape of Identity & Access Management market is evolving

By 2020,

70%

of enterprises will use **attribute-based access control** as the dominant mechanism to protect critical assets ...

... and

80%

of user access will be shaped by **new mobile and non-PC architectures** that service all identity types regardless of origin.[1]

With the growing adoption of mobile, adaptive authentication & fine-grained authorization, traditional Web Access Management is being replaced by a broader "access management." [1]

A clear need exists in the market for a converged solution[2] that is able to provide or integrate with MDM, authentication, federation, and fraud detection solutions.[3]

[1] Gartner, *Predicts 2014: Identity and Access Management,* November 26, 2013
[2] Gartner, *MarketScope for Web Access Management,* November 15, 2013
[3] Forrester, *Predictions 2014: Identity and Access Management,* January 7, 2014

Security is only as strong as its weakest link – People

55% of scam and phishing incidents are campaigns enticing users to click on malicious links

Social media is fertile ground for pre-attack intelligence gathering

Criminals are selling stolen or fabricated accounts

Mobile and Cloud momentum continues to break down the traditional perimeter and forces us to look at security differently

→

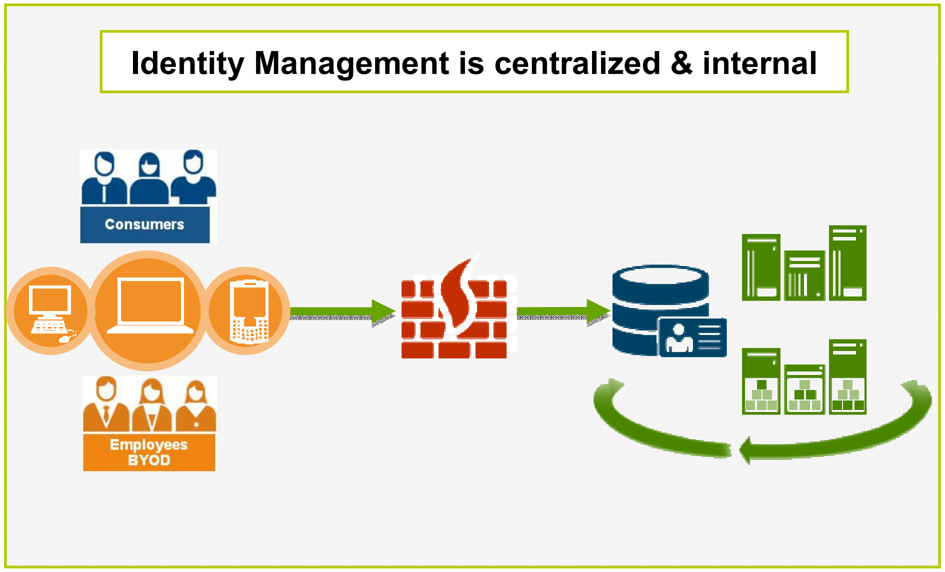
Threat-aware Identity and Access Management become the key line of defense of the multiple perimeters

Source: IBM X-Force® Research 2013 Trend and Risk Report

Fundamental Shift around Identity & Access Management

Organizations are evolving the IAM controls for a Multi-Perimeter World

The Current Enterprise

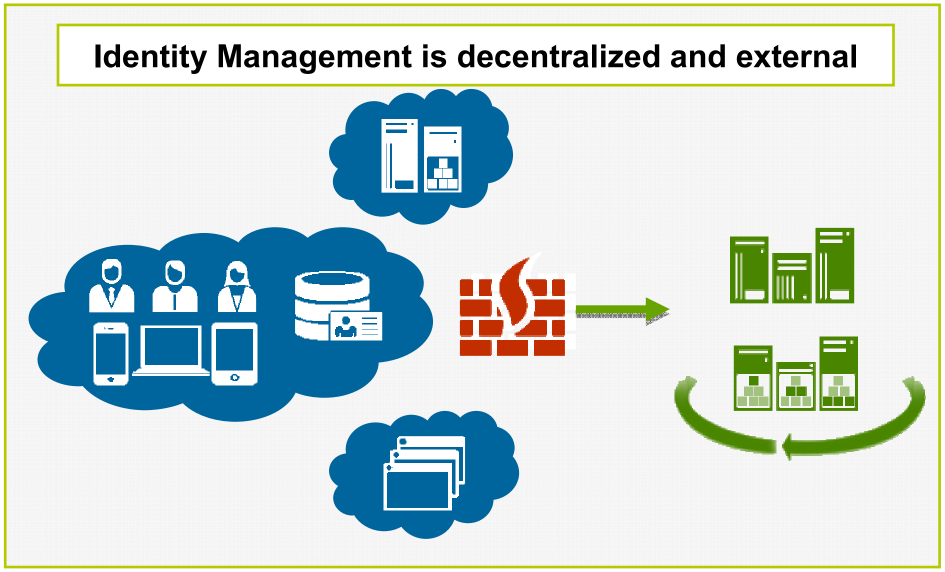


Identity Management is centralized & internal

Focus: *Administration*

- Operational management
- Compliance driven
- Static, trust-based

The New Hybrid Enterprise



Identity Management is decentralized and external

Focus: *Assurance*

- Security management
- Business driven
- Dynamic, context-based

Need for securing identities as a new perimeter with threat-aware Identity and Access Management

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

Prevent insider threat and identity fraud

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

Deliver intelligent identity and access assurance

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

Simplify identity silos and cloud integrations

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

IBM offers a comprehensive portfolio of security products

IBM Security Systems Portfolio

Security Intelligence and Analytics

QRadar Log Manager	QRadar SIEM	QRadar Risk Manager	QRadar Vulnerability Manager

Advanced Fraud Protection

Trusteer Rapport	Trusteer Pinpoint Malware Detection	Trusteer Pinpoint ATO Detection	Trusteer Mobile Risk Engine

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity Management	Guardium Data Security and Compliance	AppScan Source	Network Intrusion Prevention	Trusteer Apex
Access Management	Guardium DB Vulnerability Management	AppScan Dynamic	Next Generation Network Protection	Mobile and Endpoint Management
Privileged Identity Manager	Guardium / Optim Data Masking	DataPower Web Security Gateway	SiteProtector Threat Management	Virtualization and Server Security
Federated Access and SSO	Key Lifecycle Manager	Security Policy Manager	Network Anomaly Detection	Mainframe Security

IBM X-Force Research

Summary of IBM's Identity and Access Management capabilities

NEW	NEW	NEW	NEW
Safeguard mobile, cloud and social interactions	**Prevent insider threat and identity fraud**	**Simplify identity silos and cloud integrations**	**Deliver intelligent identity and access assurance**
Access Manager for Mobile	Access Manager for Web	Federated Identity Manager	Identity Manager
Access Manager for ESSO	Privileged Identity Manager	Directory Integrator & Server	Identity and Access Assurance
Worklight *	Trusteer *	Soft Layer *	QRadar *

* Offerings integrate with IBM IAM solutions for comprehensive end-to-end security

Details on key IBM Security Access Management products

Delivers core capabilities for People, Data, and Application areas

NEW

Safeguard mobile, cloud and social interactions

Access Manager for Mobile

Features:
- Context-based Access
- Strong Authentication
- Identity-aware Mobile Application / Device Registration

NEW

Prevent insider threat and identity fraud

Access Manager for Web

Features
- Centralized Authentication
- Centralized Session
- Management
- Centralized coarse-grained Authorization
- Web SSO
- Web App Firewall

Focus of this webinar

NEW

Simplify identity silos and cloud integrations

Federated Identity Manager

Features:
- Federated SSO
- Identity Mediation
- Secure Token Service
- User Self Care
- Delegated Authorization

Guiding Principles for Simplifying Access Management with IBM

1. Support key scenarios out-of-the-box

- Deploy standard use cases in days
- Minimize customization with business value accelerators

2. Easy to deploy

- Consolidate installs, configurations and multiple run-times
- Appliance form factor (virtual) with firmware update
- Easily scalable

3. Easy to use

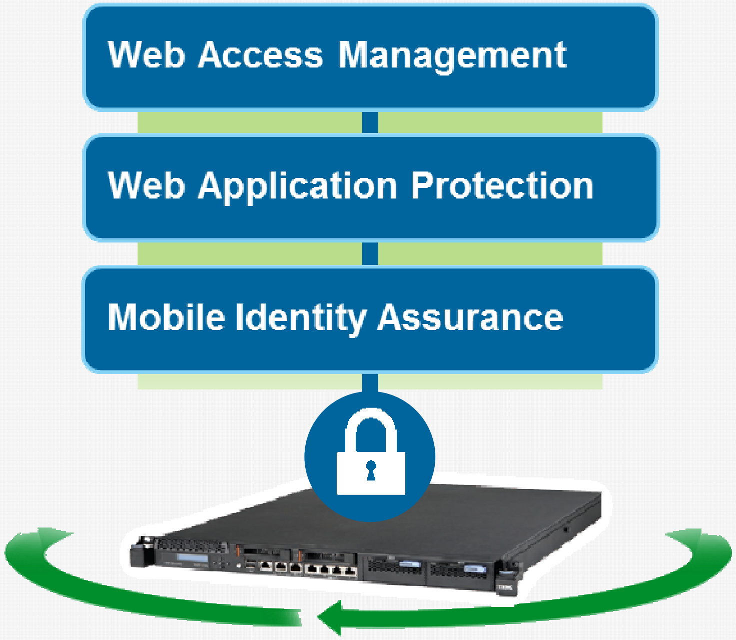
- Simpler interface for end user persona
- Enable IT operations skill transfer
- Common look and feel across IAM

IBM Security Access Manager 8.0

"All-in-one" access management powered by X-Force, Trusteer and QRadar

NEW

IBM Security Access Manager



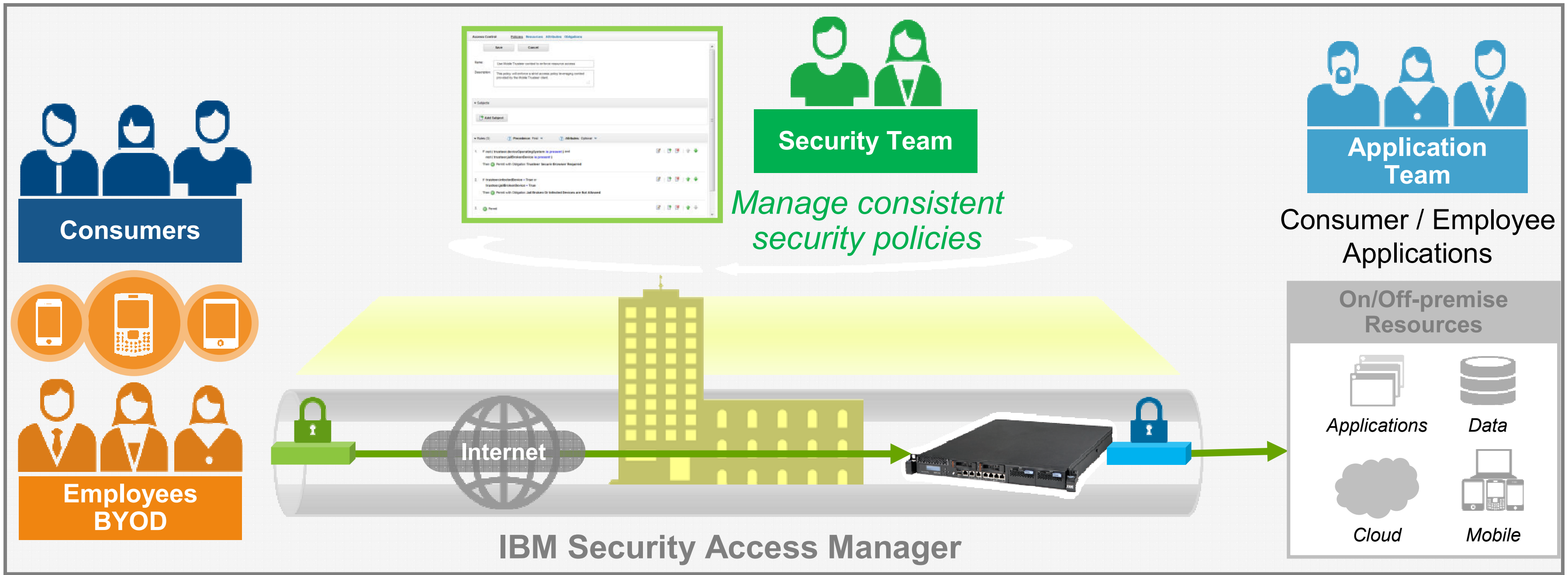
Web Access Management

Web Application Protection

Mobile Identity Assurance

- **Enable secure access to web and mobile applications** with SSO, session management and built-in support for IBM Worklight
- **Protect web and mobile applications** against common attack vectors including the OWASP Top 10 web application risks with integrated X-Force threat protection
- **Enforce context-aware access** with mobile device fingerprinting, geo-location awareness, IP Reputation and integration with Trusteer Mobile SDK
- **Enhance security intelligence and compliance** through integration with QRadar Security Intelligence
- **Reduce TCO and time to value** with an "all-in-one" access appliance that allows flexible deployment of web and mobile capabilities as needed

Modular Feature Design Offers Secure Access with Graded Trust



IBM Security Access Manager for Web	**IBM Security Access Manager for Mobile**
Web Single Sign-On and session management	Mobile Single Sign-On and session management
Web Application Protection (Firewall)	Authentication service with built-in OTP support
Highly-scalable Reverse Proxy	Context-, Risk-based Access (RBA)
Policy Server	Trusteer Mobile SDK / Secure Browser integration
Coarse-grained Authorization	Worklight integration for risk-based access enforcement

Physical appliances for hardware performance & security

Virtual appliances for deployment flexibility

vmware®

SOFTLAYER® an IBM Company

IBM Security Access Manager 8.0 - Innovative and Differentiating IAM Capabilities

Empowering clients to more easily deliver end-to-end security solutions to mitigate the risks associated with a diverse set of Web, Mobile and Cloud applications

1	**Embedded Threat Protection for Web & Mobile**	Tolly Group evaluation validates that ISAM for Web is able to effectively protect against 100% of OWASP Top 10 web application risks while maintaining high performance and scalability
2	**Integrated Security Intelligence**	As the centralized policy enforcement point for all Web-based access, ISAM generates actionable events for QRadar SIEM that enable clients to stay ahead of threats and demonstrate regulatory compliance
3	**Protection from High Risk Mobile Devices**	Out-of-the-box consumption of Trusteer Mobile SDK and Secure Browser context data enables users to create comprehensive access policies that include fraud and malware detection without modifying applications
4	**Built-in Identity Assurance for IBM Worklight**	Built-in support to seamlessly authenticate and authorize users of Worklight developed mobile applications and provide additional value-add with context based access enforcement
5	**Modular Access Management Platform**	Consolidated platform allows both Web and Mobile capabilities to be licensed as needed, including flexible deployment options with both physical and virtual appliance form factors

IBM Security Access Manager for Web

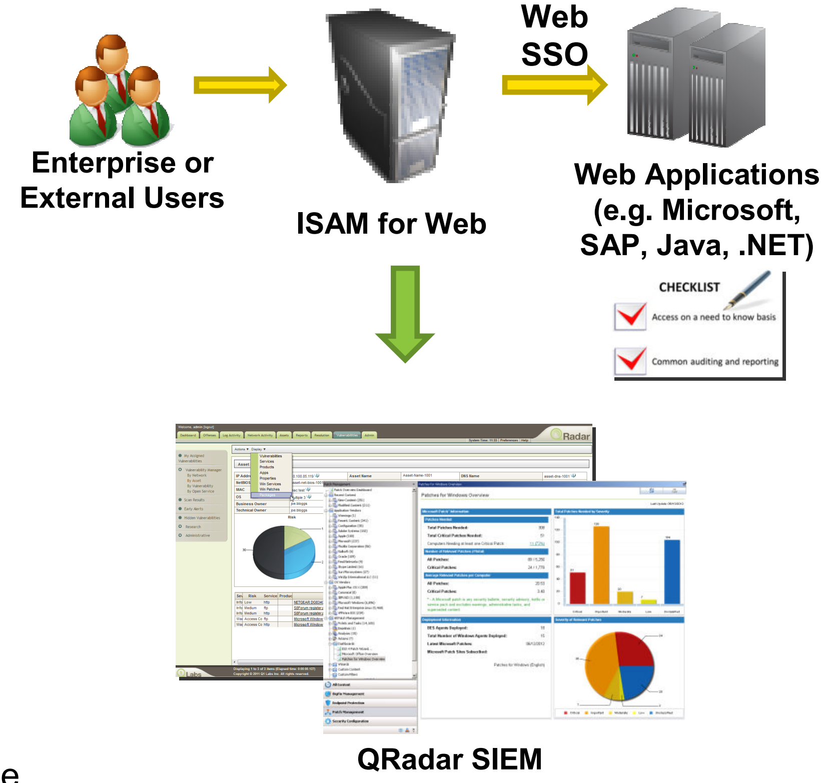
Simplifies managing and enforcing user access to corporate applications and help demonstrate compliance

Key Highlights

- Native 64 bit support for improved scalability
- Web Reverse-proxy Appliance/Virtual Appliance for fast time to value
- Integrated front end load balancer and web threat protection provided with appliance/virtual appliance
- Multiple authorization server support and high availability for policy servers
- Integration with QRadar Security Intelligence platform
- Improved policy-driven security to enforce compliance
- NIST compliant

Benefits

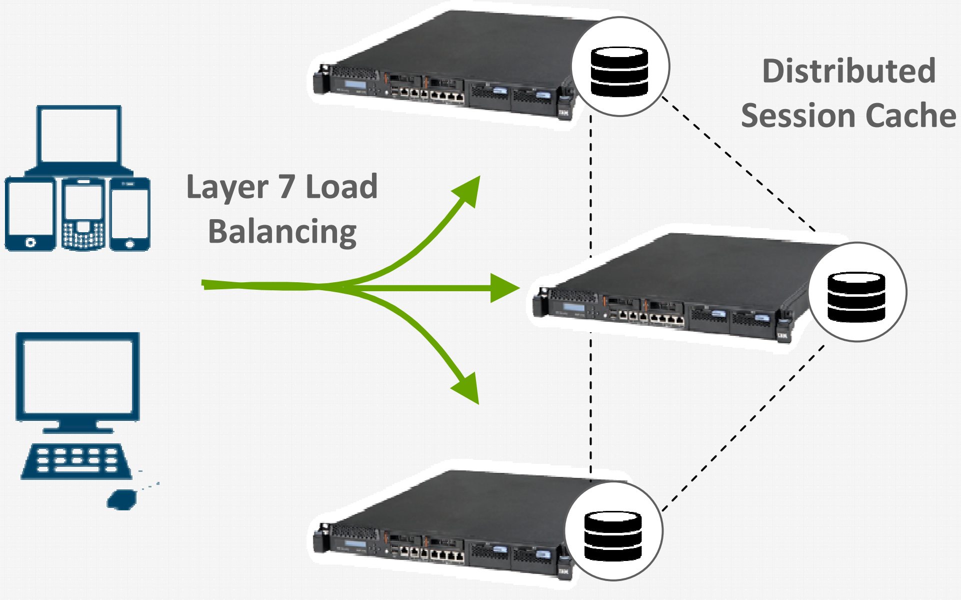
- Reduce operational cost and strengthen access control
- Highly scalable to support external user access and demonstrate compliance across heterogeneous IT environment
- Flexible, rich integration with 3rd party applications and strong authentication vendors


Enterprise or External Users
ISAM for Web
Web SSO
Web Applications (e.g. Microsoft, SAP, Java, .NET)
CHECKLIST
Access on a need to know basis
Common auditing and reporting
QRadar SIEM

Improved Availability, Scalability and Appliance Utilization

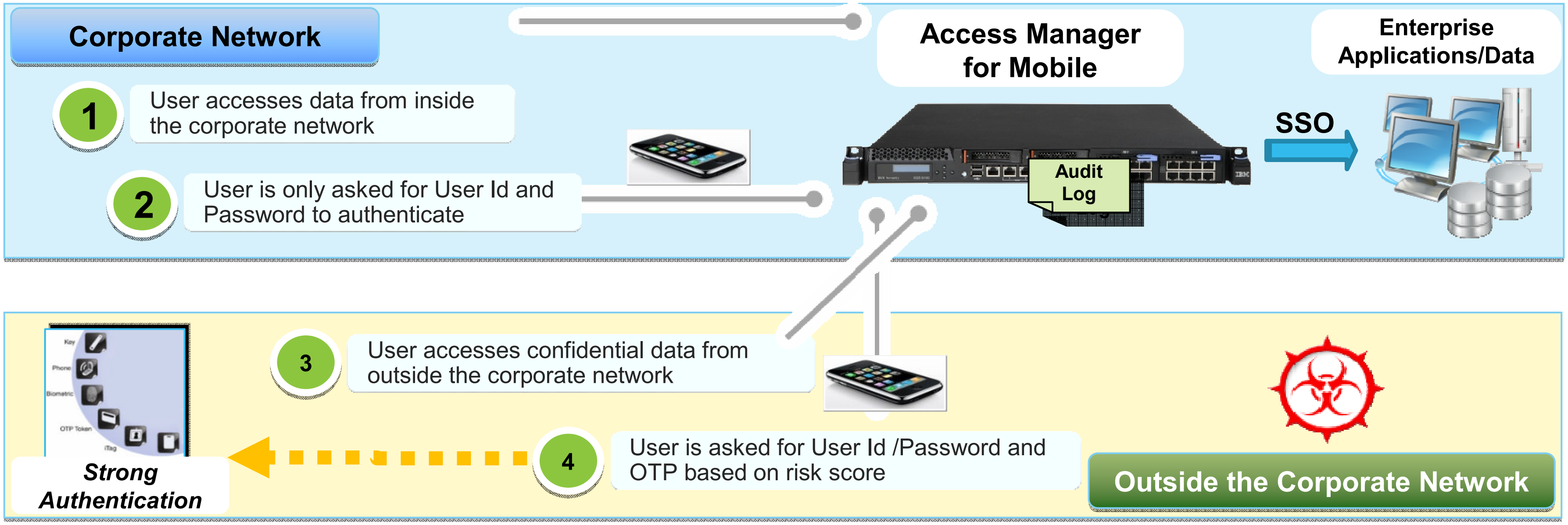
Embedded load balancing & session caching reduces overall infrastructure needs

- New application layer load balancing option (Layer 7) removes the need to have dedicated ISAM appliance to distribute load across the cluster
- Reduce cost and more rapidly deploy clustered solution with embedded session cache, no longer requiring a separate session management server
- Improved testing and validation of web protection policies in simulation mode with X-Force Protocol Analysis Module (PAM)



IBM Security Access Manager for Mobile

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



Corporate Network
1 User accesses data from inside the corporate network
2 User is only asked for User Id and Password to authenticate
Access Manager for Mobile
Audit Log
SSO
Enterprise Applications/Data
3 User accesses confidential data from outside the corporate network
4 User is asked for User Id /Password and OTP based on risk score
Key
Phone
Biometric
OTP Token
iTag
Strong Authentication
Outside the Corporate Network

How ISAM 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 3rd 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

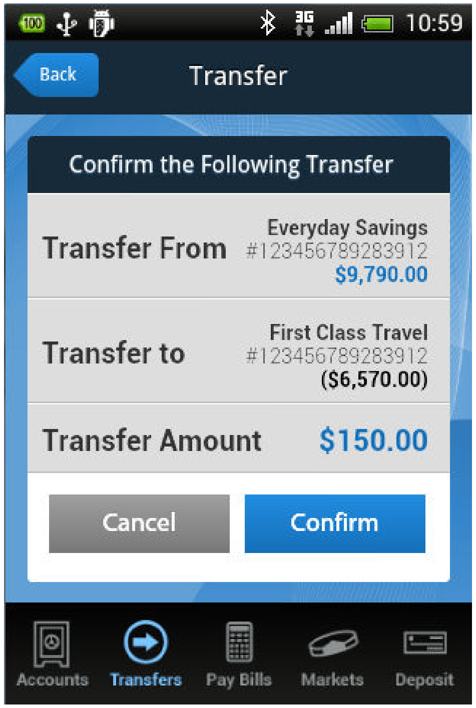
Enforce risk-based access and strong authentication for transactions

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



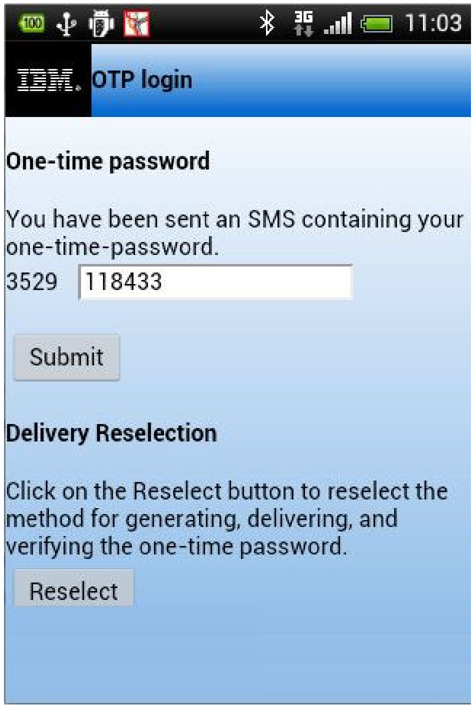
Confirm the Following Transfer

Transfer From — Everyday Savings #123456789283912 $9,790.00

Transfer to — First Class Travel #123456789283912 ($6,570.00)

Transfer Amount — $150.00

Strong authentication challenge



One-time password

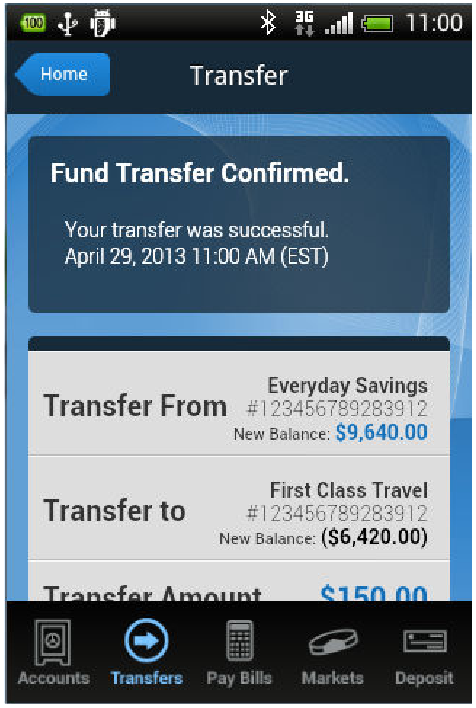
You have been sent an SMS containing your one-time-password.

3529 118433

Delivery Reselection

Click on the Reselect button to reselect the method for generating, delivering, and verifying the one-time password.

Transaction completes



Fund Transfer Confirmed.

Your transfer was successful.
April 29, 2013 11:00 AM (EST)

Transfer From — Everyday Savings #123456789283912 New Balance: $9,640.00

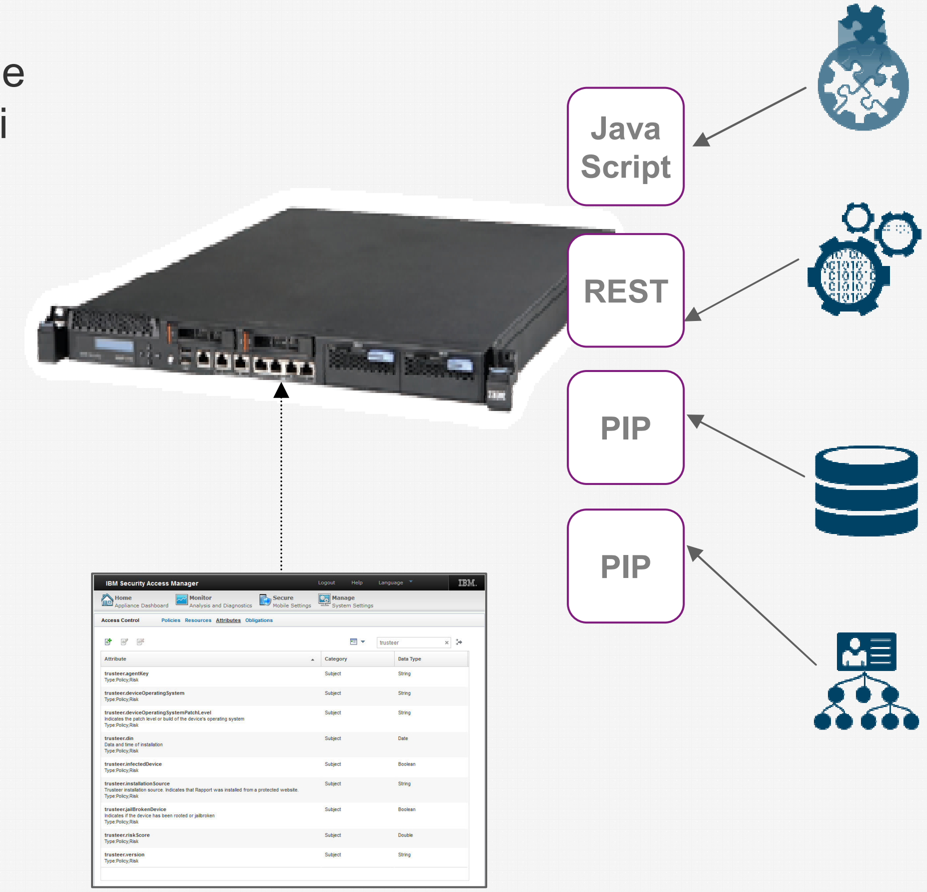
Transfer to — First Class Travel #123456789283912 New Balance: ($6,420.00)

Transfer Amount — $150.00

Simplify the Creation of Mobile-Centric Security Policies

Streamlined user experience enables rapid deployment of complex access policies

- ISAM for Mobile offers new easy-to-use visual editor for creating reusable multi factor authentication policies
  - Out of the box MFA policies including TOTP, HOTP, etc.
  - Create custom auth policies
- Extensible policy information points (PIPs) make it easier to include external data as part of context based access (CBA) decisions
  - REST (XML/JSON)
  - JavaScript

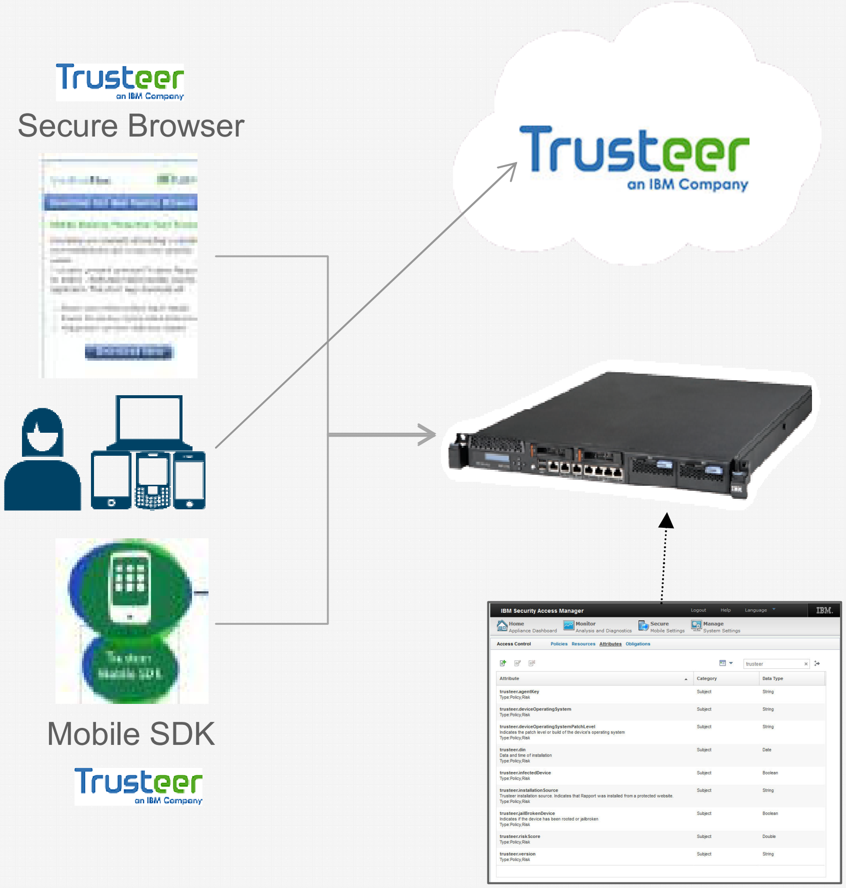


Attribute	Category	Data Type
trusteer.agentKey Type:Policy,Risk	Subject	String
trusteer.deviceOperatingSystem Type:Policy,Risk	Subject	String
trusteer.deviceOperatingSystemPatchLevel Indicates the patch level or build of the device's operating system Type:Policy,Risk	Subject	String
trusteer.din Data and time of installation Type:Policy,Risk	Subject	Date
trusteer.infectedDevice Type:Policy,Risk	Subject	Boolean
trusteer.installationSource Trusteer installation source. Indicates that Rapport was installed from a protected website. Type:Policy,Risk	Subject	String
trusteer.jailBrokenDevice Indicates if the device has been rooted or jailbroken Type:Policy,Risk	Subject	Boolean
trusteer.riskScore Type:Policy,Risk	Subject	Double
trusteer.version Type:Policy,Risk	Subject	String

Easier Fraud & Malware Detection with ISAM for Mobile and Trusteer

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

- 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



IBM Security Access Manager

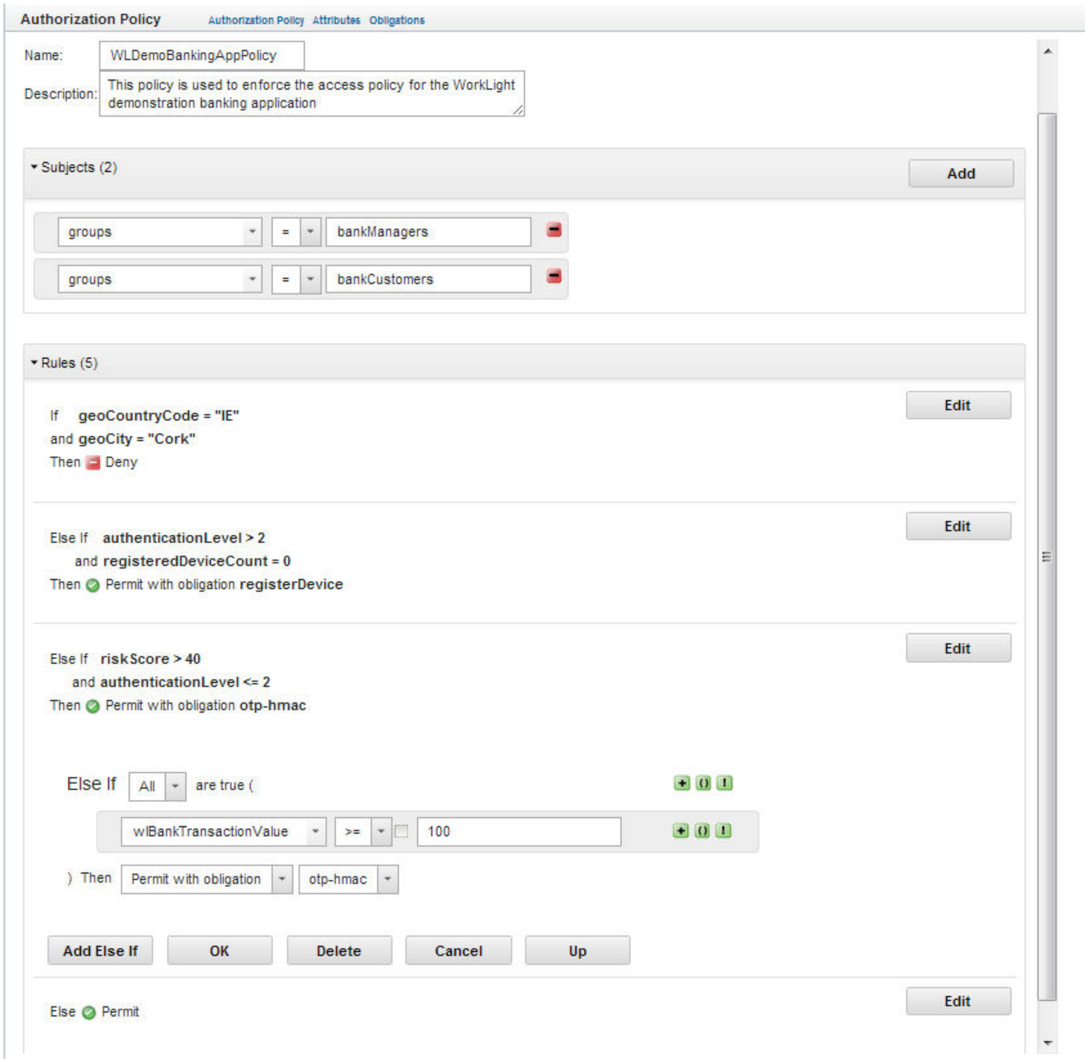
Attribute	Category	Data Type
trusteer.agentKey Type:Policy,Risk	Subject	String
trusteer.deviceOperatingSystem Type:Policy,Risk	Subject	String
trusteer.deviceOperatingSystemPatchLevel Indicates the patch level or build of the device's operating system Type:Policy,Risk	Subject	String
trusteer.din Data and time of installation Type:Policy,Risk	Subject	Date
trusteer.infectedDevice Type:Policy,Risk	Subject	Boolean
trusteer.installationSource Trusteer installation source. Indicates that Rapport was installed from a protected website. Type:Policy,Risk	Subject	String
trusteer.jailBrokenDevice Indicates if the device has been rooted or jailbroken Type:Policy,Risk	Subject	Boolean
trusteer.riskScore Type:Policy,Risk	Subject	Double
trusteer.version Type:Policy,Risk	Subject	String

More Rapidly Respond to Emerging Threats & Security Requirements

Appliance form factor enables faster time to value with intuitive user experience and consistent policy enforcement across multiple applications & channels

IBM Security Access Manager

- ✓ User-centric GUI for authoring comprehensive risk based policies that can be attached to multiple applications
- ✓ SDK to integrate with 3rd party authentication vendors to leverage your existing investment
- ✓ Highly Scalable Virtual and HW appliances reduce TCO of solution



Name: WLDemoBankingAppPolicy

Description: This policy is used to enforce the access policy for the WorkLight demonstration banking application

Subjects (2)

groups = bankManagers

groups = bankCustomers

Rules (5)

If geoCountryCode = "IE"
and geoCity = "Cork"
Then Deny

Else If authenticationLevel > 2
and registeredDeviceCount = 0
Then Permit with obligation registerDevice

Else If riskScore > 40
and authenticationLevel <= 2
Then Permit with obligation otp-hmac

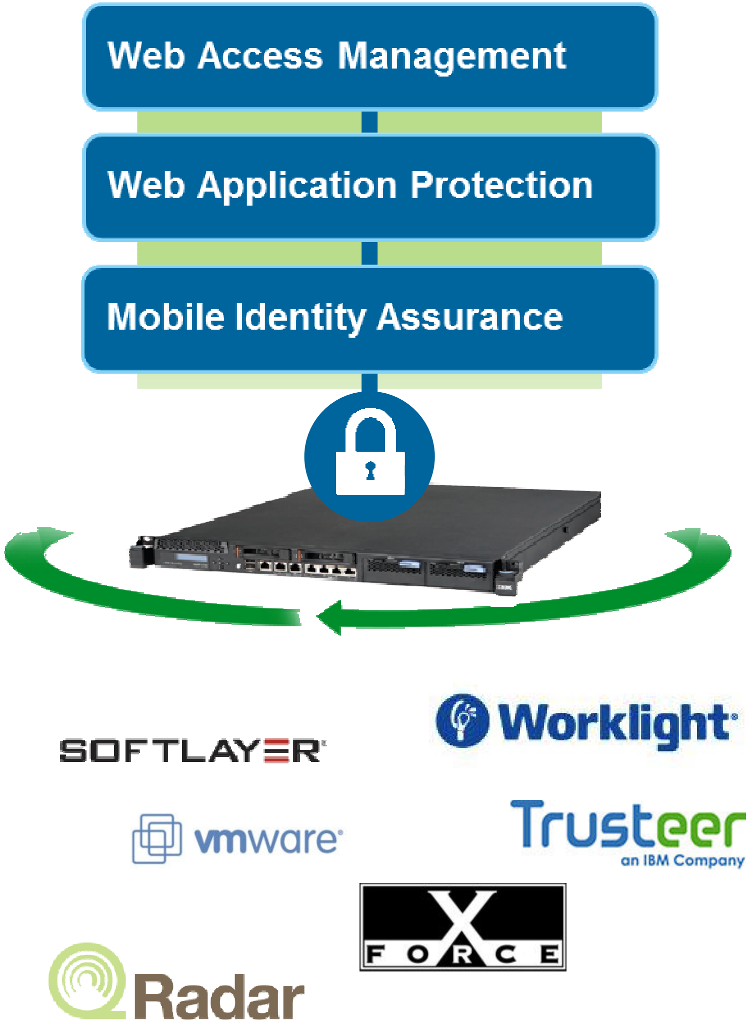
Else If All are true (
wlBankTransactionValue >= 100
) Then Permit with obligation otp-hmac

Else Permit

Summary

- IBM Security Access Manager "all-in-one" appliance delivers threat-aware access management for Web, Mobile and Cloud
  - Modular platform delivery across physical and virtual appliances provides ultimate flexibility
  - Start with one security use case and grow to meet evolving business demands, and leverage existing technology investment
- Out-of-the-box integrations with a broad range of IBM Security and other IBM software products
  - Provides unmatched end-to-end security for Web, Mobile and Cloud
  - Proven and certified integrations reduce cost, risk and time to value

IBM Security Access Manager 8.0



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

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

Connect with IBM Security

Follow us at @ibmsecurity

IBM Identity & Access Management Web Experience
http://www-03.ibm.com/software/products/en/category/identity-access-management

IBM Security Insights blog at www.SecurityIntelligence.com

Questions?

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security