

Security Intelligence.
Think Integrated.

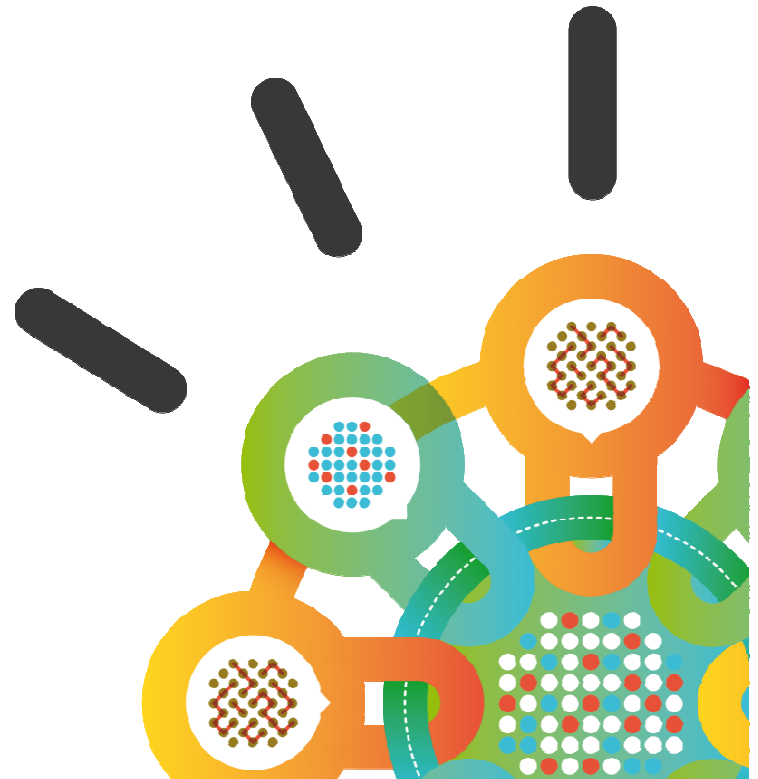
Identity and Access Management Intelligence

12th November, 2013

Chris Hockings

IBM Master Inventor

hockings@au1.ibm.com



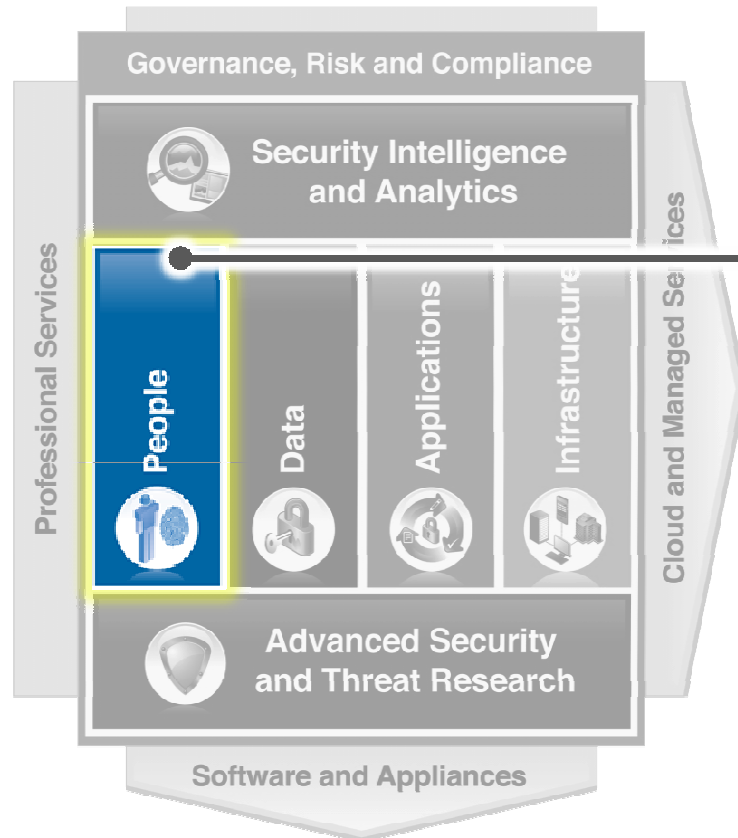
Worldwide IBM Security Systems Labs



IAM Strategy

- IBM Security Framework
- ISAM Overview and Strategy
- ISIM Overview and Strategy
- Demonstrations

Introduced IBM IAM capabilities



Portfolio Overview

IBM Security Identity Manager

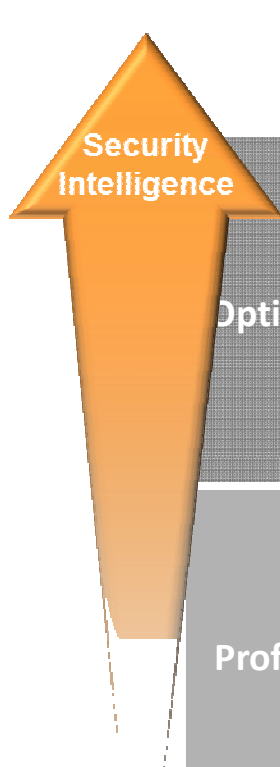
- Automate the creation, modification, and termination of users throughout the entire lifecycle
- Identity control including role management and auditing and Privileged Identity Management

IBM Security Access Manager

- Automates sign-on and authentication to enterprise web applications and services
- Entitlement management for fine-grained access enforcement

Manage Enterprise Identity Context Across All Security Domains

Focused on helping organizations' security to mature



	People	Data	Applications	Infrastructure	Security Intelligence
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Securing systems	Advanced threat detection Network anomaly detection Predictive risk management
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management	Real-time event correlation Network forensics
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus	Log management Compliance reporting

IAM Strategy

- IBM Security Framework
- ISAM Overview and Strategy
- ISIM Overview and Strategy
- Demonstrations

ISAM: Ability to secure user access and protect from web attacks

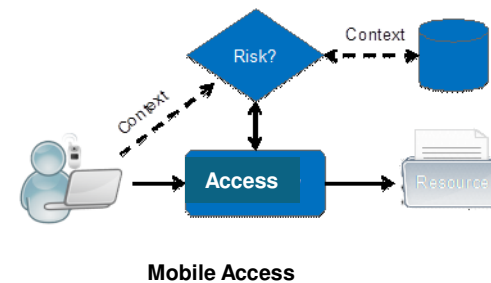
1 Secure Access and Content Protection



2 Cloud Access and Collaboration

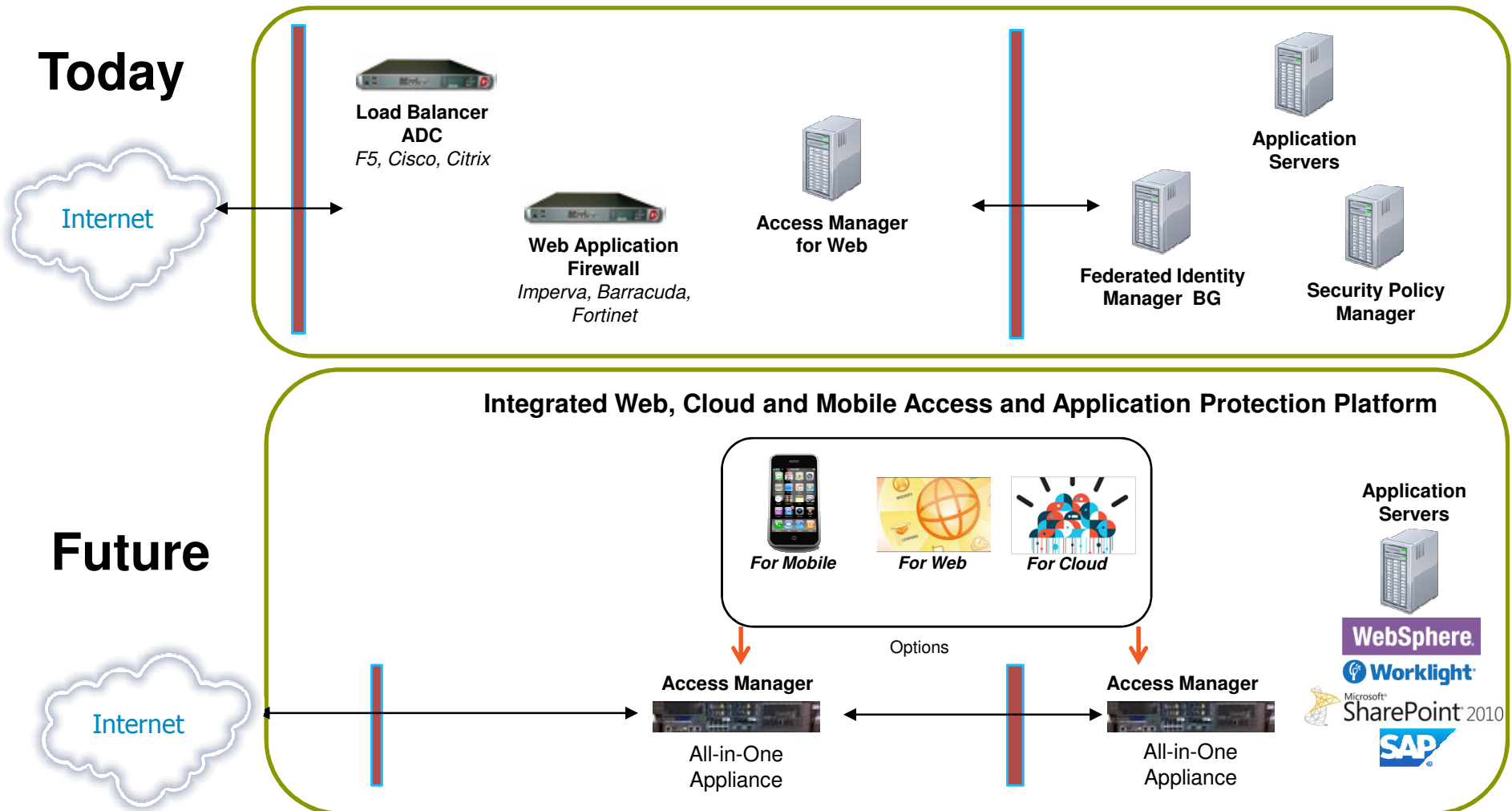


3 Mobile and Risk-based Access



Access Management in a multi-perimeter world
 Integrated Web Access and Content Protection in a Single Appliance

ISAM : Consolidated, Consumable, Comprehensive platform for Web, Cloud and Mobile Security



ISAM: Delivering software (virtual) and physical appliances for fast time to value and lower TCO



ISAM FOR WEB

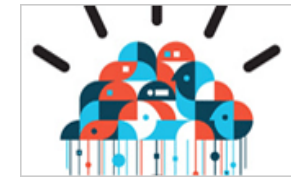
- Web Reverse Proxy
- Web Application/Content Protection
- Built-in Policy Server
- Layer 4 and 7 load balancing for HA



ISAM FOR MOBILE

- Context-based Authorization
- Strong Authentication Services
- *OAuth for Mobile Apps
- Built-in OTP with support for 3rd party providers
- *Worklight integration for OTP and RBA

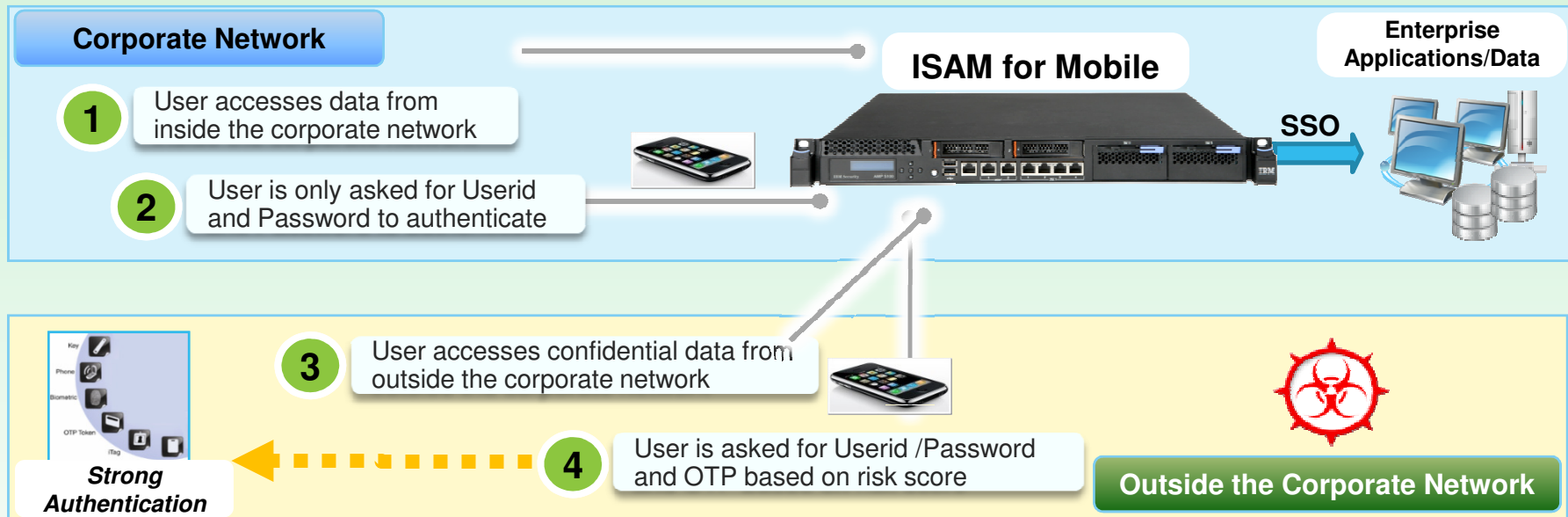
*Note: planned to be delivered in the December update



ISAM FOR CLOUD

- Federated SSO with support for SAML, OAuth, OpenID, WS-Federation, WS-Trust, etc.
- Security Token Service and identity mediation
- Fine grain authorization policy management

Strong Authentication, SSO, Session Mgmt. for secure user interactions



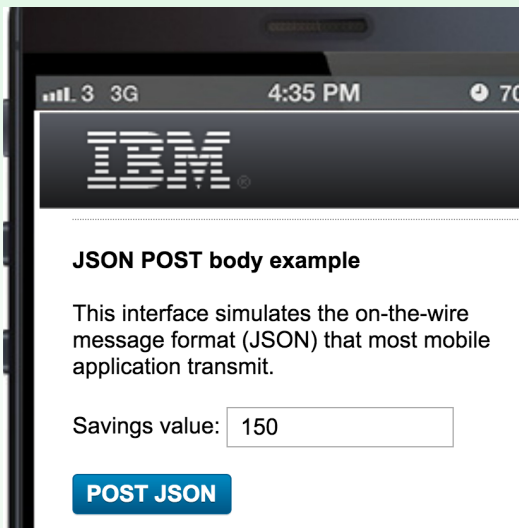
- ✓ Built-in Risk scoring engine using user attributes and real-time context (e.g. Risk Scoring and Access policy based on **Device registration, Geo-political location, IP reputation**, etc.)
- ✓ Support mobile authentication with built-in **One-Time Password (OTP)** and ability to integrate with 3rd party strong authentication vendors, as needed. Example of supported OTPs are MAC OTP (email & SMS), HMAC OTP (TOTP & HOTP using client generators like Google Authenticator), RSA SecurID Soft and Hard tokens
- ✓ Offer Software Development Kit (SDK) to integrate with 3rd party authentication factors and collect additional contextual attributes from the device and user session

Implement Risk Based access posture for BYOD

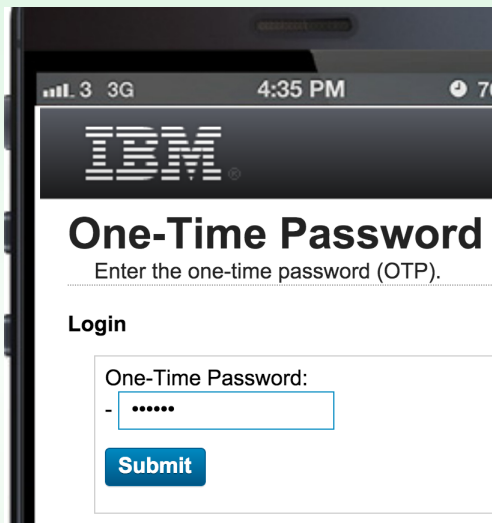
Context based access and stronger assurance for transactions

- ✓ 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
- ✓ Context based on HTTP POST Data and JSON content

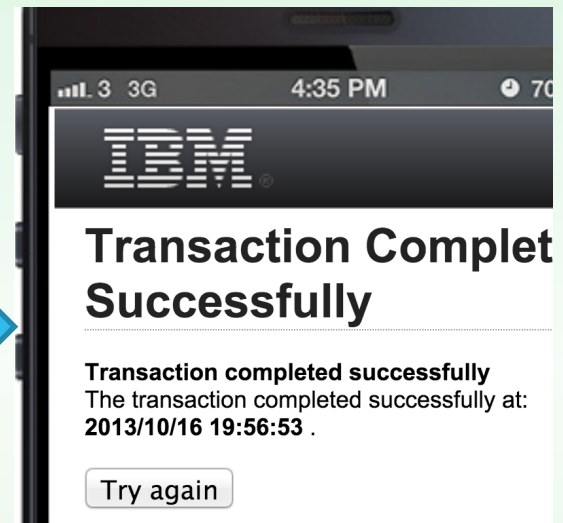
User attempts high-value transaction



Strong authentication challenge



Transaction completes



Ability to secure user access and content against targeted attacks



Access Operations	Grant/Deny
An authorized user requests access to the portal and SSO	Grant
Password is stolen, session is hijacked and HTTP content is compromised	Deny
HTTP content contains common vulnerabilities such as SQL Injection, Cross site scripting, Cross-site request forgery	Deny
IP Address has a low IP Reputation score and Geo Location allowed	Deny
Enforce step-up authentication or context-based access to restore authorized user access	Grant

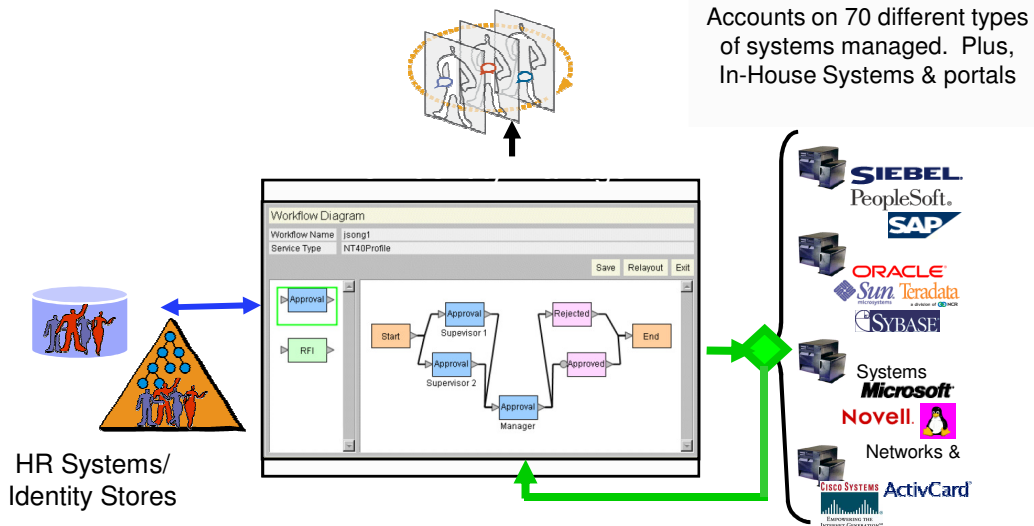
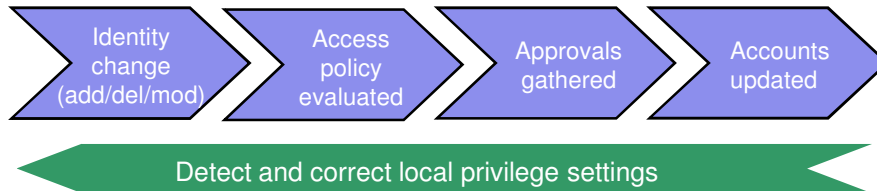
✓ Extend threat protection to support X-Force based IP Reputation and Geo Location

Secure access and protect content against targeted attacks

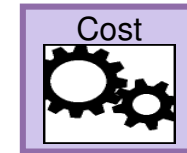
IAM Strategy

- IBM Security Framework
- ISAM Overview and Strategy
- ISIM Overview and Strategy
- Demonstrations

ISIM: Identity Manager automates, audits, and corrects user access rights across your IT infrastructure

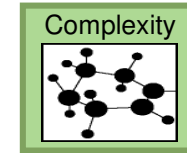


- Know the *people* behind the accounts and *why* they have the access they do
- Automate user privileges lifecycle across entire IT infrastructure
- Fix non-compliant accounts
- Match your workflow processes



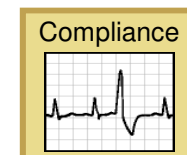
Lower Costs

- Self-service password reset
- Automated user provisioning



Reduce Complexity

- Consistent security policy
- Quickly integrate new users & apps



Address Compliance

- Closed-loop provisioning
- Access rights audit & reports

IBM Security Privileged Identity Manager

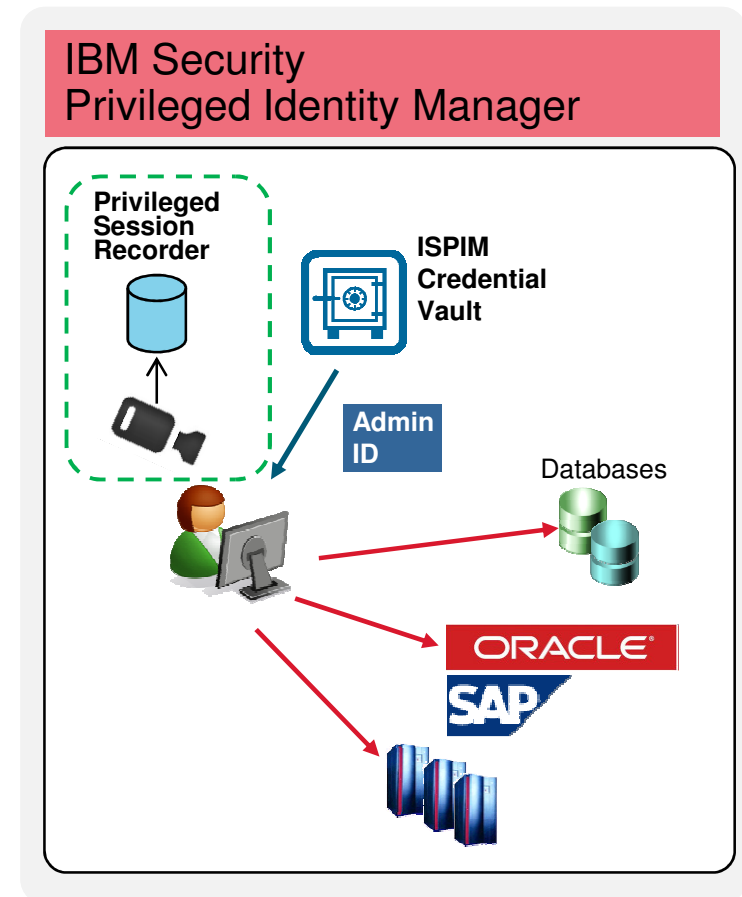
Centrally manage, audit and control shared identities across the enterprise

Key product highlights

- **Control shared access to sensitive userids**
 - Check-in / check-out using secure credential vault
- **Request, approve and re-validate privileged access**
 - Reduce risk, enhance compliance
- **Automated password management**
 - Automated checkout of IDs, hide password from requesting employee, automate password reset to eliminate password theft
- **Track and record usage of shared identities**
 - Provide accountability
- **Optional visual recording of user endpoint activity with on demand search and playback of stored recordings**
 - Heightened oversight to meet governance requirements

IBM security solution

- **Privileged Identity Management (PIM) solution providing complete identity management and enterprise single sign-on capabilities for privileged users**



Ability to deliver effective privileged identity control

1 Configure Privileged Account

Service Name	Ownership Type
Windows Test	Vendor
Windows Test	Vendor
Windows Test	Vendor

2 User's credential is automatically **checked out** of the vault and used to **log user into** privileged account. Credential is automatically checked in to vault upon logout

3 User activity is logged

Shared Access History IBM®

Start Date: Jan 1, 1970 12:00 AM, End Date: Jul 27, 2012 11:59 PM

Shared Access History for Credential Pools

Service Business Unit: Organization
 Service: Windows Test Service
 Credential Pool: DB2Administrator on Windows
 Credential Pool Owner: Annie Lewis (Person, Organization)

Credential	Credential Owner	Exclusiv Access	Action	Justification	Action Owner	Action Owner Business Unit	Time of Action
db2admin01	Annie Lewis	Yes	Checkout	checkin out the credential pool	James Smith		May 30, 2012 5:11 PM
db2admin01	Annie Lewis	Yes	View Password	checkin out the credential pool	James Smith		May 30, 2012 5:15 PM
db2admin01	Annie Lewis	Yes	View Password	checkin out the credential pool	James Smith		May 30, 2012 5:23 PM
db2admin01	Annie Lewis	Yes	Checkin	checkin out the credential pool	James Smith		May 30, 2012 5:27 PM

Identity Management in a multi-perimeter world
Controlling privileged user access across multiple domains

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.



ibm.com/security

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.