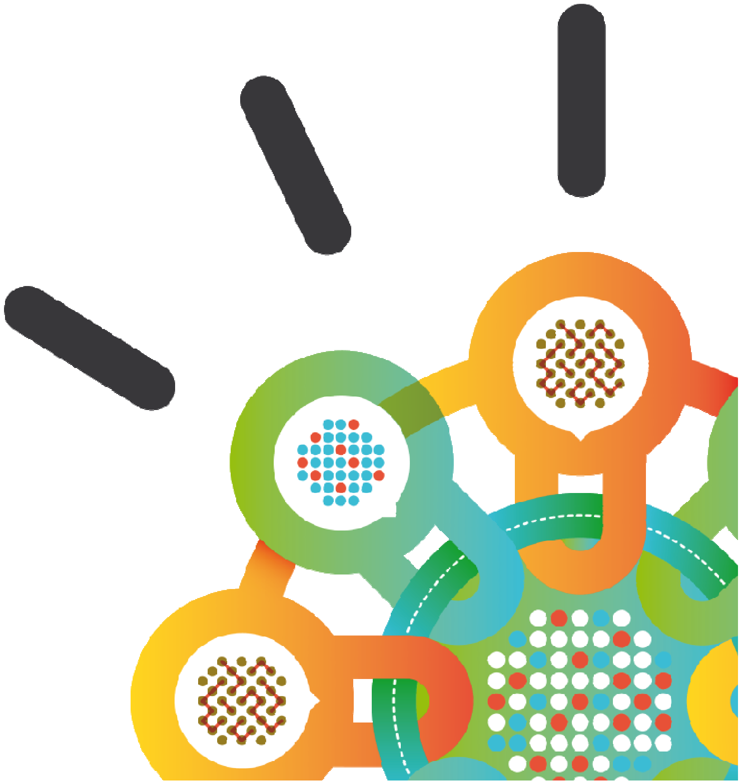
Security Intelligence.
Think Integrated.

IBM IAM Security Strategy

Threat-aware Identity and Access Management

IBM Security Systems

Gonzalo de la Hoz
IAM Segment Leader, Europe



July 2014

Information Security is only as strong as its weakest link – Identity

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

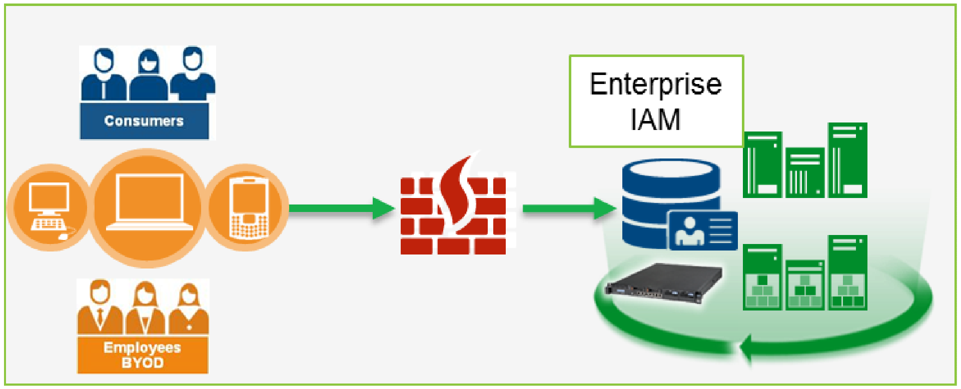
Criminals are selling stolen or fabricated accounts

***Mobile** and **Cloud** breaking down the traditional perimeter*

*IAM becomes fist line of defense with **Threat** and **Context** awareness*

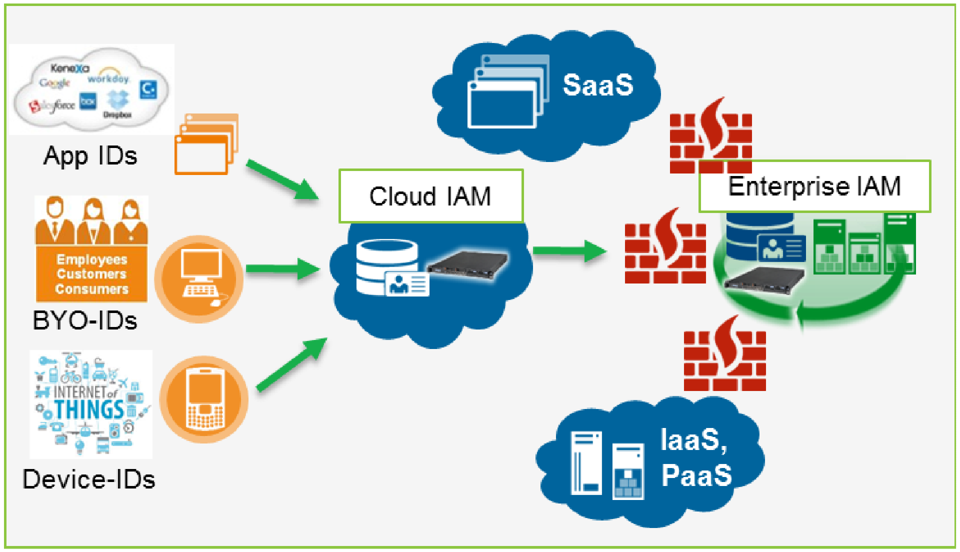
Source: IBM X-Force® Research 2013 Trend and Risk Report

Identity is a key security controls for a multi-perimeter world



Today: Administration

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



Tomorrow: Assurance

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

Threat-aware Identity and Access Management becomes the first line of defense for securing multi perimeter world

Safeguard mobile, cloud and social access

- **Validate "who is who"** especially when users connect from outside the enterprise
- **Proactively enforce access policies** on web, social and mobile collaboration channels

Prevent advanced insider threats

- **Manage and audit privileged access** across the enterprise
- **Defend applications and data** against unauthorized access

Deliver actionable identity intelligence

- **Streamline identity management** across all security domains
- **Manage and monitor user entitlements and activities** with security intelligence

Simplify cloud integrations and identity silos

- **Provide federated access** to enable secure online business collaboration
- **Unify "Universe of Identities"** for efficient directory management

Threat-aware Identity and Access Management becomes the first line of defense for securing multi perimeter world

Safeguard mobile, cloud and social access

- **Validate "who is who"** especially when users connect from outside the enterprise
- **Proactively enforce access policies** on web, social and mobile collaboration channels

Prevent advanced insider threats

- **Manage and audit privileged access** across the enterprise
- **Defend applications and data** against unauthorized access

Deliver actionable identity intelligence

- **Streamline identity management** across all security domains
- **Manage and monitor user entitlements and activities** with security intelligence

Simplify cloud integrations and identity silos

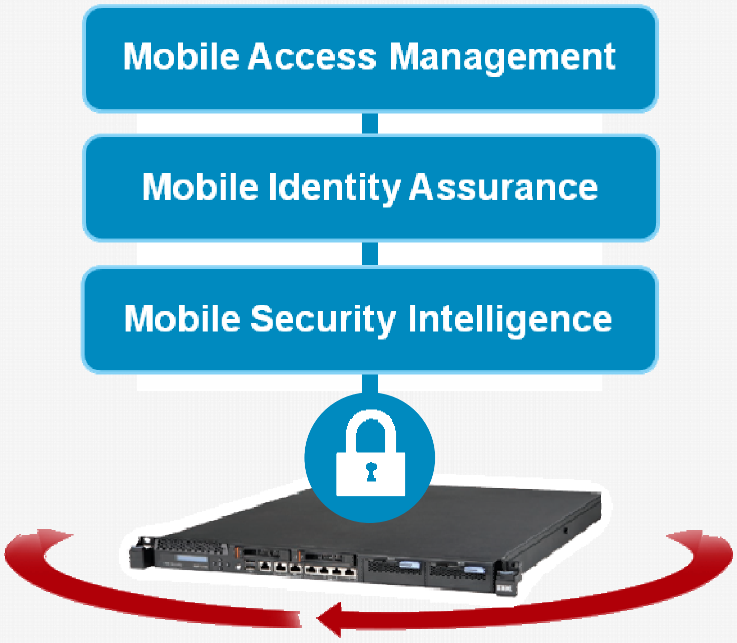
- **Provide federated access** to enable secure online business collaboration
- **Unify "Universe of Identities"** for efficient directory management

Introducing New Access Management Solution

NEW

Safeguard mobile, cloud and social access

IBM Security Access Manager for Mobile



Mobile Access Management

Mobile Identity Assurance

Mobile Security Intelligence

- **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

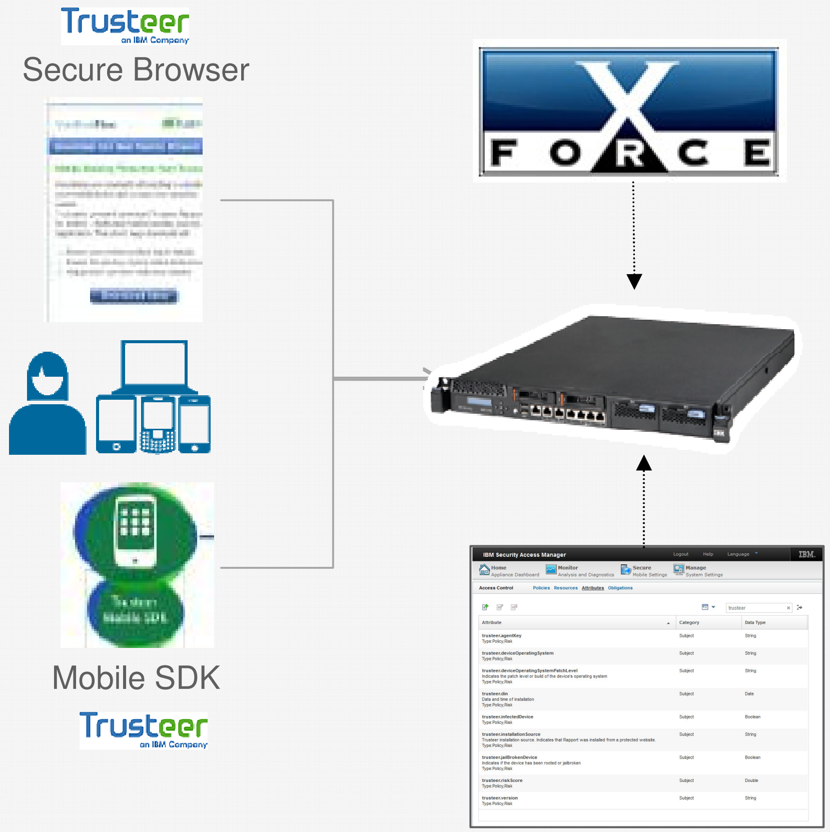
Protect against advanced threats and cyber-attacks

with Trusteer integration, Risk-scoring and real time IBM X-Force feeds

NEW

Safeguard mobile, cloud and social access

- Out-of-the-box recognition of Trusteer-specific attributes being included in request messages from Secure Browser and Mobile SDK
- Author reusable policies that can be attached to multiple applications
- Enforce consistent fraud & malware detection policies without updating the apps
- Built-in Risk scoring engine using user attributes and real-time X-Force data (e.g. **Geo-political location, IP reputation)**



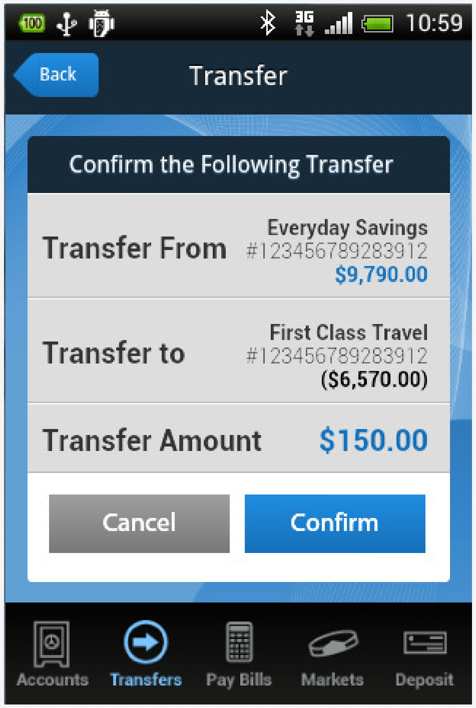
IBM Security Access Manager

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

Implement a context-aware access posture for mobile access and BYOD

Safeguard mobile, cloud and social access

User attempts high-value transaction



10:59

Back Transfer

Confirm the Following Transfer

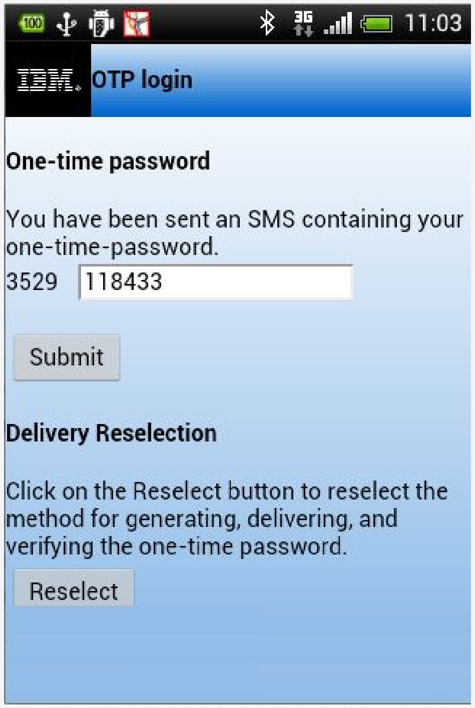
Transfer From — Everyday Savings #123456789283912 $9,790.00

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

Transfer Amount — $150.00

Cancel Confirm

Strong authentication challenge



11:03

IBM. OTP login

One-time password

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

3529 118433

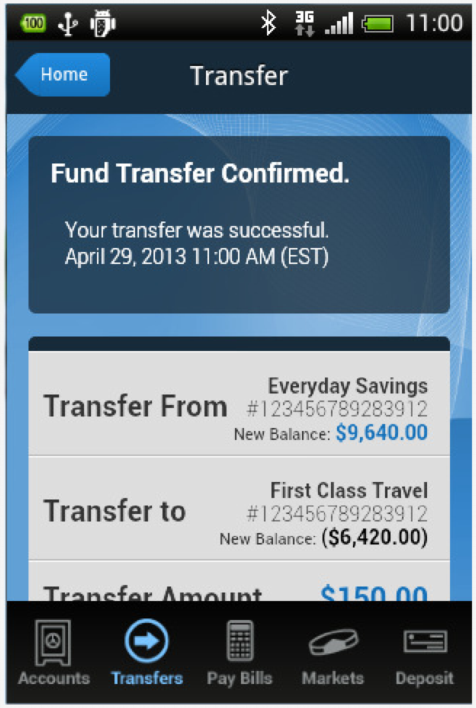
Submit

Delivery Reselection

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

Reselect

Transaction completes



11:00

Home Transfer

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

✓ 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

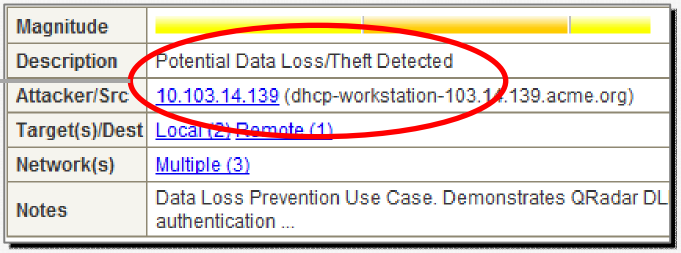
Protect against advanced threats and cyber-attacks

with QRadar Integration

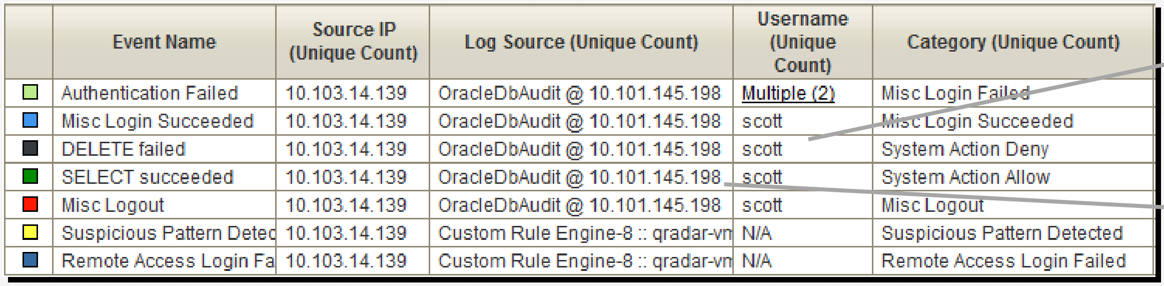
Safeguard mobile, cloud and social access

Potential Data Loss

Who? What? Where?



Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (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 ...



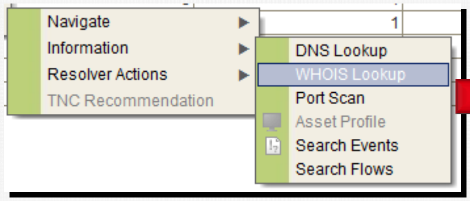
	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
🟩	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
🟦	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
⬛	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

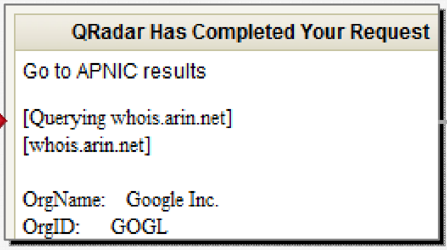
Who?

An internal user

What?

Oracle data





QRadar Has Completed Your Request

Go to APNIC results

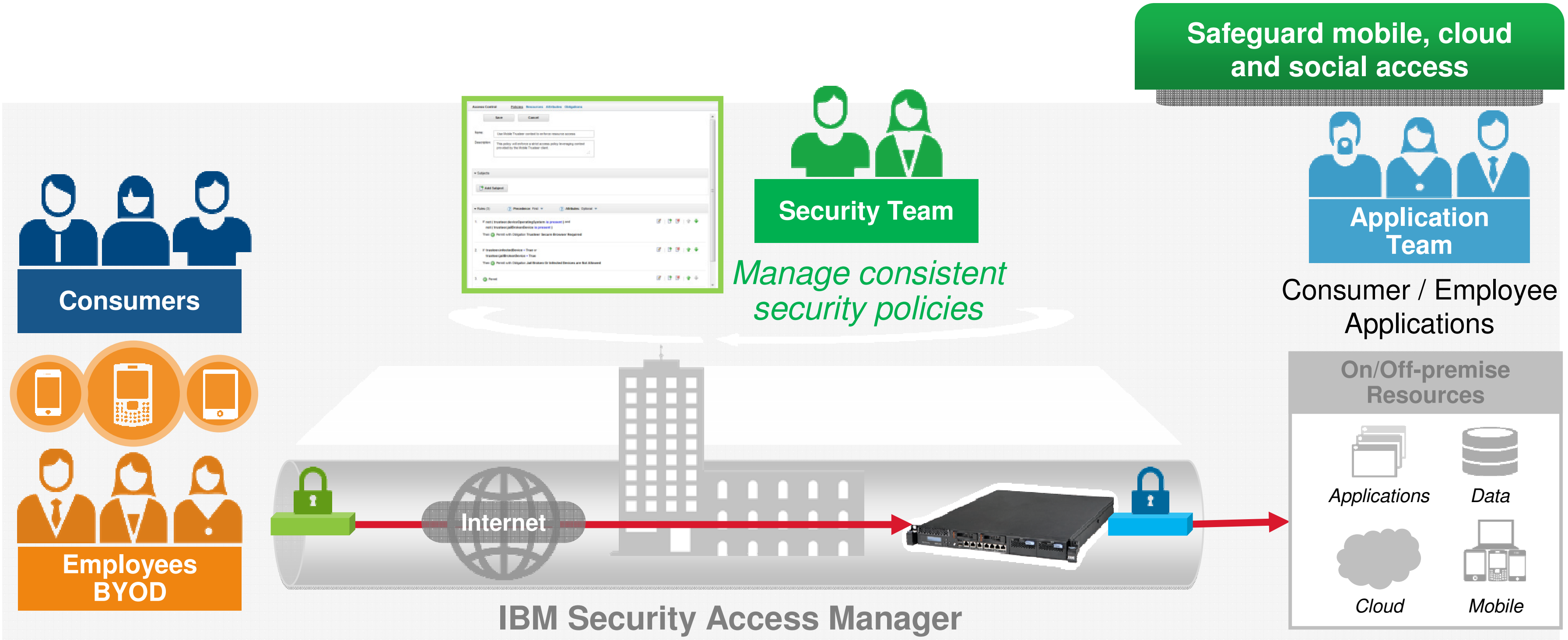
[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

Where?

Gmail

Unified Access Gateway to deliver modular support for access requirements


Safeguard mobile, cloud and social access
Consumers
Employees BYOD
Security Team
Manage consistent security policies
Application Team
Consumer / Employee Applications
Internet
On/Off-premise Resources
Applications
Data
Cloud
Mobile
IBM Security Access Manager

Access Control Policies Resources Attributes Obligations

Save Cancel

Name: Use Mobile Trusteer context to enforce resource access

Description: This policy will enforce a strict access policy leveraging context provided by the Mobile Trusteer client.

▾ Subjects

Add Subject

▾ Rules (3) Precedence: First ▾ Attributes: Optional ▾

1. If not (trusteer.deviceOperatingSystem is present) and not (trusteer.jailBrokenDevice is present)
   Then Permit with Obligation Trusteer Secure Browser Required

2. If trusteer.infectedDevice = True or trusteer.jailBrokenDevice = True
   Then Permit with Obligation Jail Broken Or Infected Devices are Not Allowed

3. Permit

Access Manger for Web

Web Single Sign-On and session management

Web Application Protection (Firewall)

Highly-scalable Reverse Proxy

Policy Server

Coarse-grained Authorization

Access Manager for Mobile

Mobile Single Sign-On and session management

Authentication service with built-in OTP support

Context-, Risk-based Access (RBA)

Trusteer Mobile SDK / Secure Browser integration

Worklight integration for risk-based access enforcement

Physical appliances for hardware performance & security

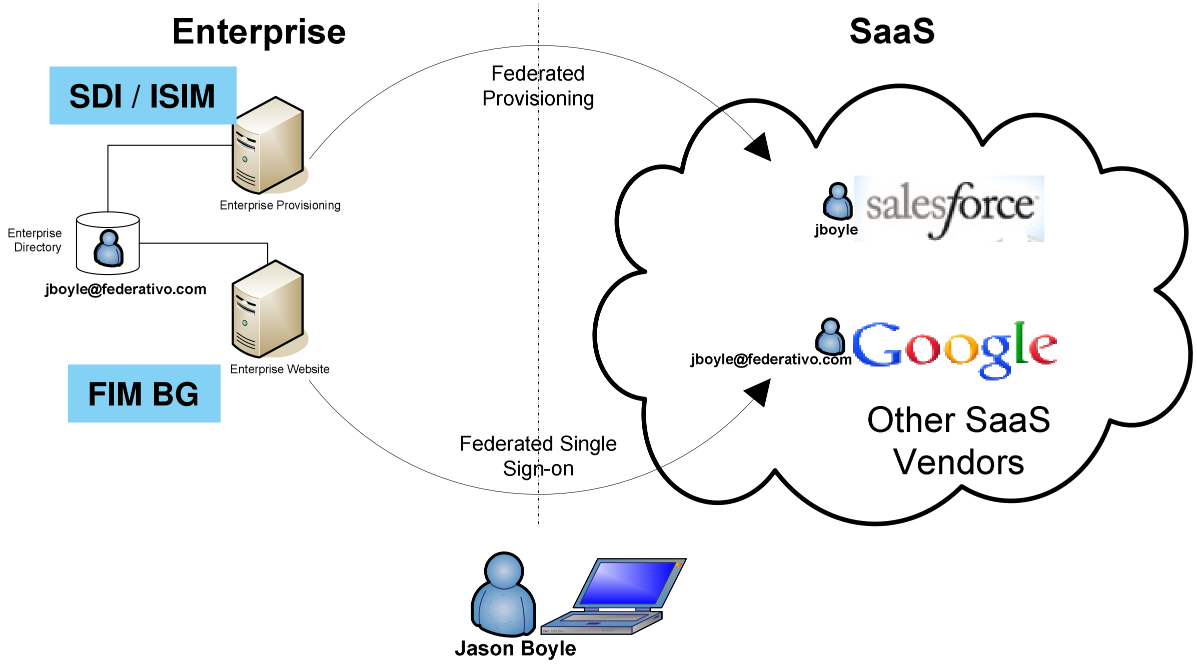
Virtual appliances for deployment flexibility

vmware

SOFTLAYER an IBM Company

Cloud Use Case 1: Enabling Access to SaaS with Identity Federation

- Scenario: Identity and access to the cloud
  - Examples: Salesforce, GoogleApps, Workday, Office365, IBM SmartCloud
- Target: B2E
- Capabilities: Federated provisioning and single sign-on

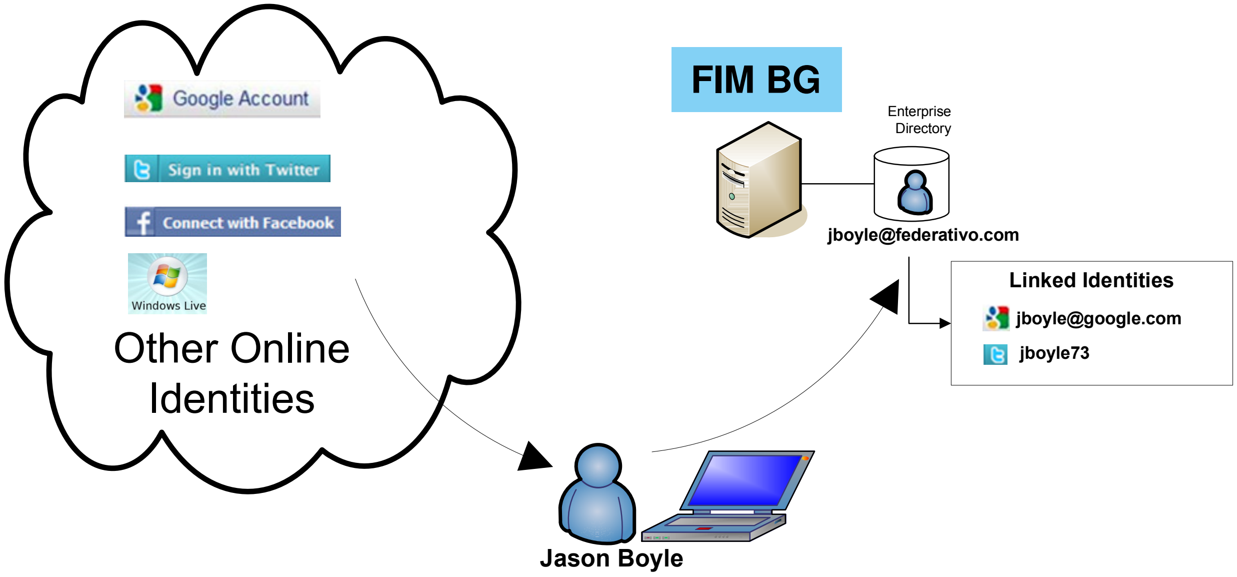


SDI = Security Director Integrator
ISIM = IBM Security Identity Manager
FIM BG = Federated Identity Manager Business Gateway

Cloud Use Case 2: Implementing BYO-ID with Identity Federation

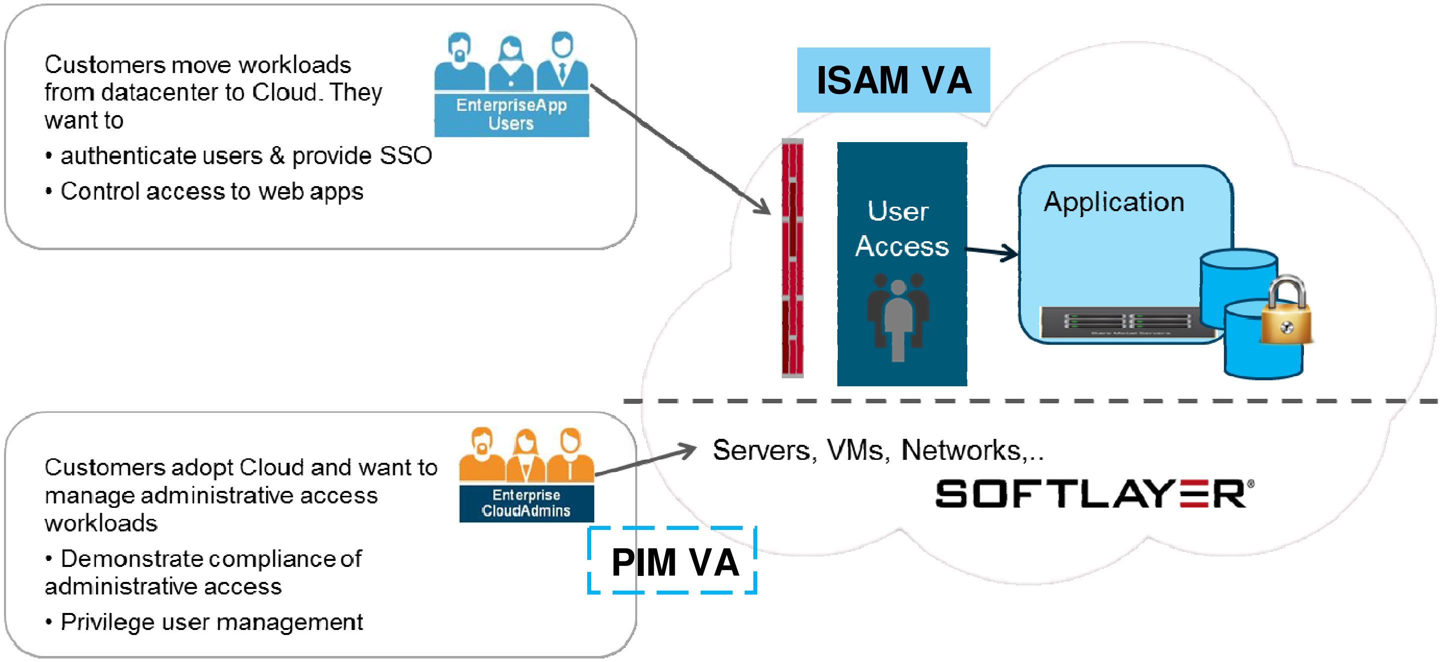
- Scenario: Bring your own identity
  - Examples: LinkedIn, Facebook, Twitter, Google, Yahoo IDs
- Target: B2C
- Capabilities: Self-registration, single sign-on, user self-care

"Making access easy, with a familiar, fast, fun and secure user experience is key to attaining and retaining new customers."



Cloud Use Case 3: Implementing IAM in IaaS to secure workloads

- Scenario: Deploying IAM capabilities in a cloud infrastructure
  - Examples: SoftLayer, Amazon EC2
- Target: Enterprise
- Capabilities: Access Management, Privileged Identity Management
- Example:



Customers move workloads from datacenter to Cloud. They want to

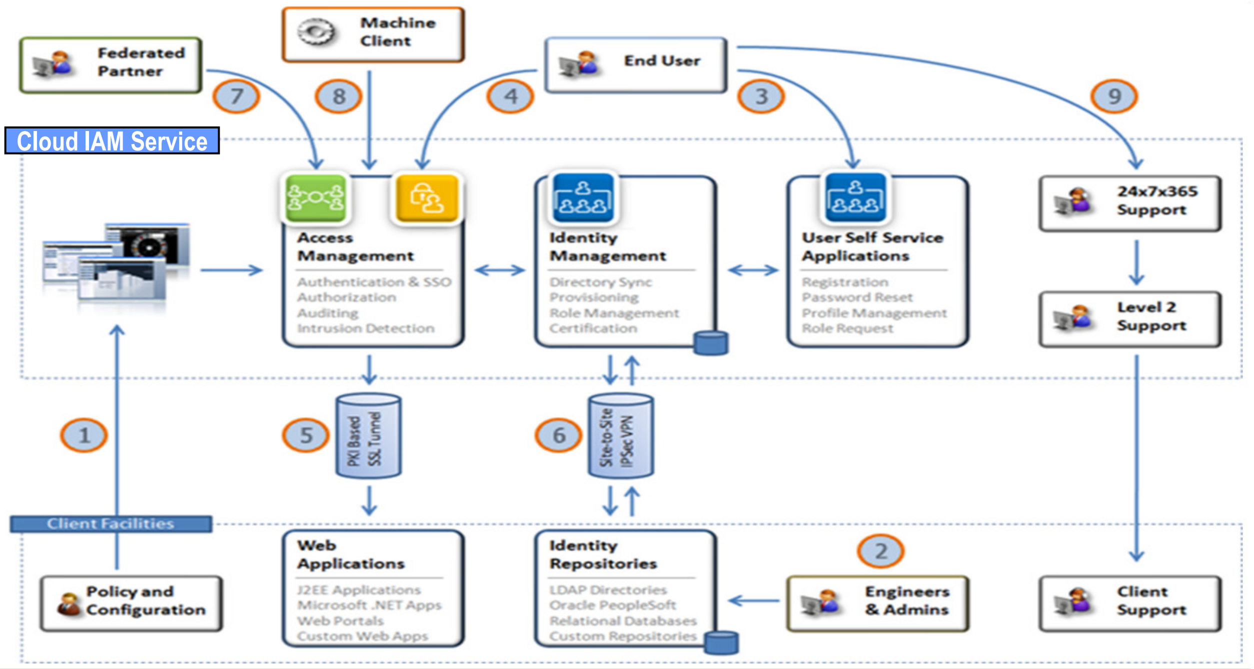
- authenticate users & provide SSO
- Control access to web apps

Customers adopt Cloud and want to manage administrative access workloads

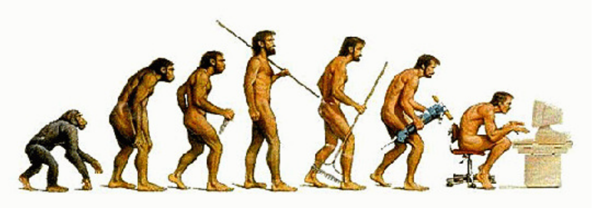
- Demonstrate compliance of administrative access
- Privilege user management

Cloud Use Case 4: Adopting IAM as a managed service from the cloud

- Scenario: IAM as a managed service from the cloud
  - Examples: Customize IAM infrastructure and deploy in a hosted manner
- Target: Enterprise
- Capabilities: Access Management, Identity Management and Federation
- Example:

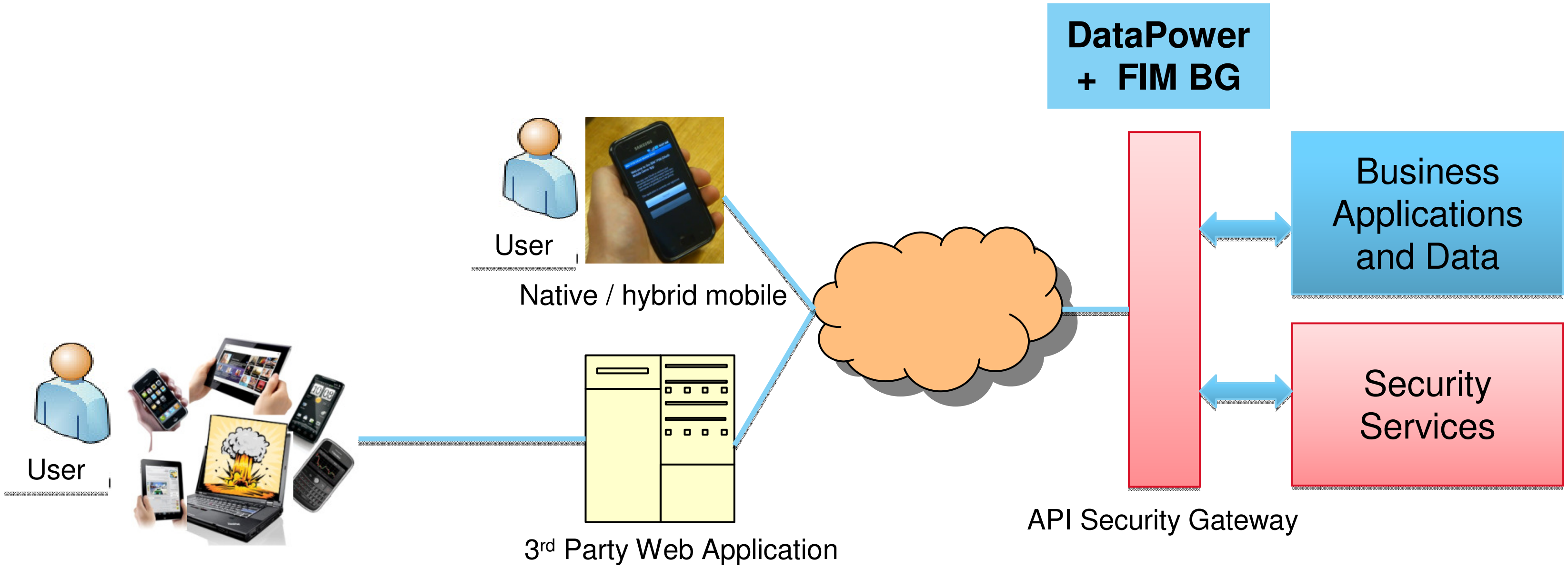


Cloud Use Case 5: Integrated Services via API



No IT ⇨ Internal IT ⇨ Web 1.0 ⇨ Business via API

- Scenario: Exposing services via API
  - Examples: Google API's, Twilio, Facebook, CloudFoundry
  - See www.programmableweb.com
- Target: Mobile, B2B
- Capabilities: OAuth, Basic-Auth, Mutual SSL, WS-*



DataPower + FIM BG

User

Native / hybrid mobile

User

3rd Party Web Application

Business Applications and Data

Security Services

API Security Gateway

Identity as an API: Simplified Security for App Developers

Easily add user authentication and single sign on to on-premise & cloud applications

BETA

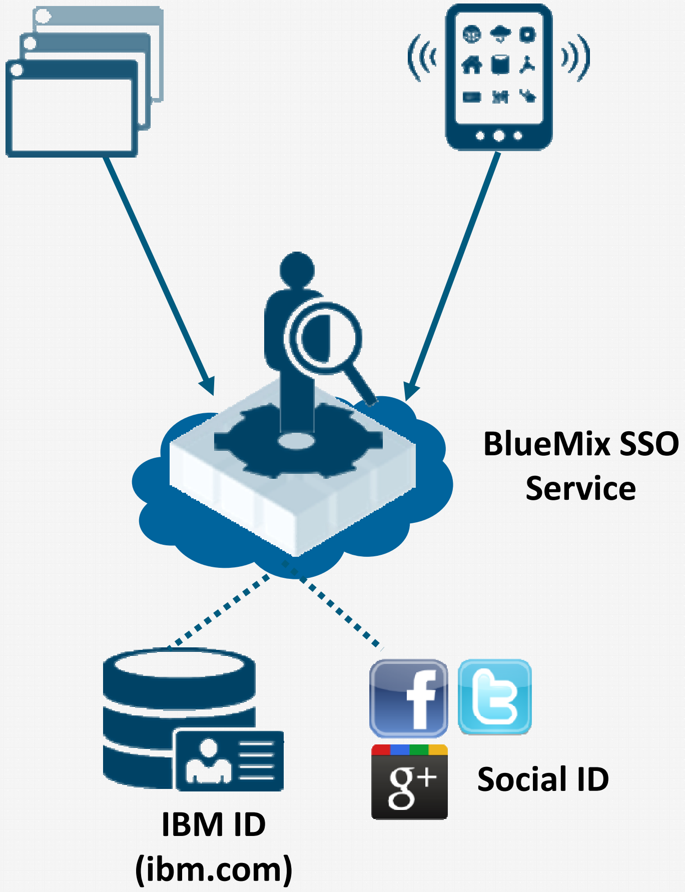
Safeguarding mobile, cloud, and social access

Easy to use service allows developers to add access security for web and mobile applications using "SSO with IBM ID"

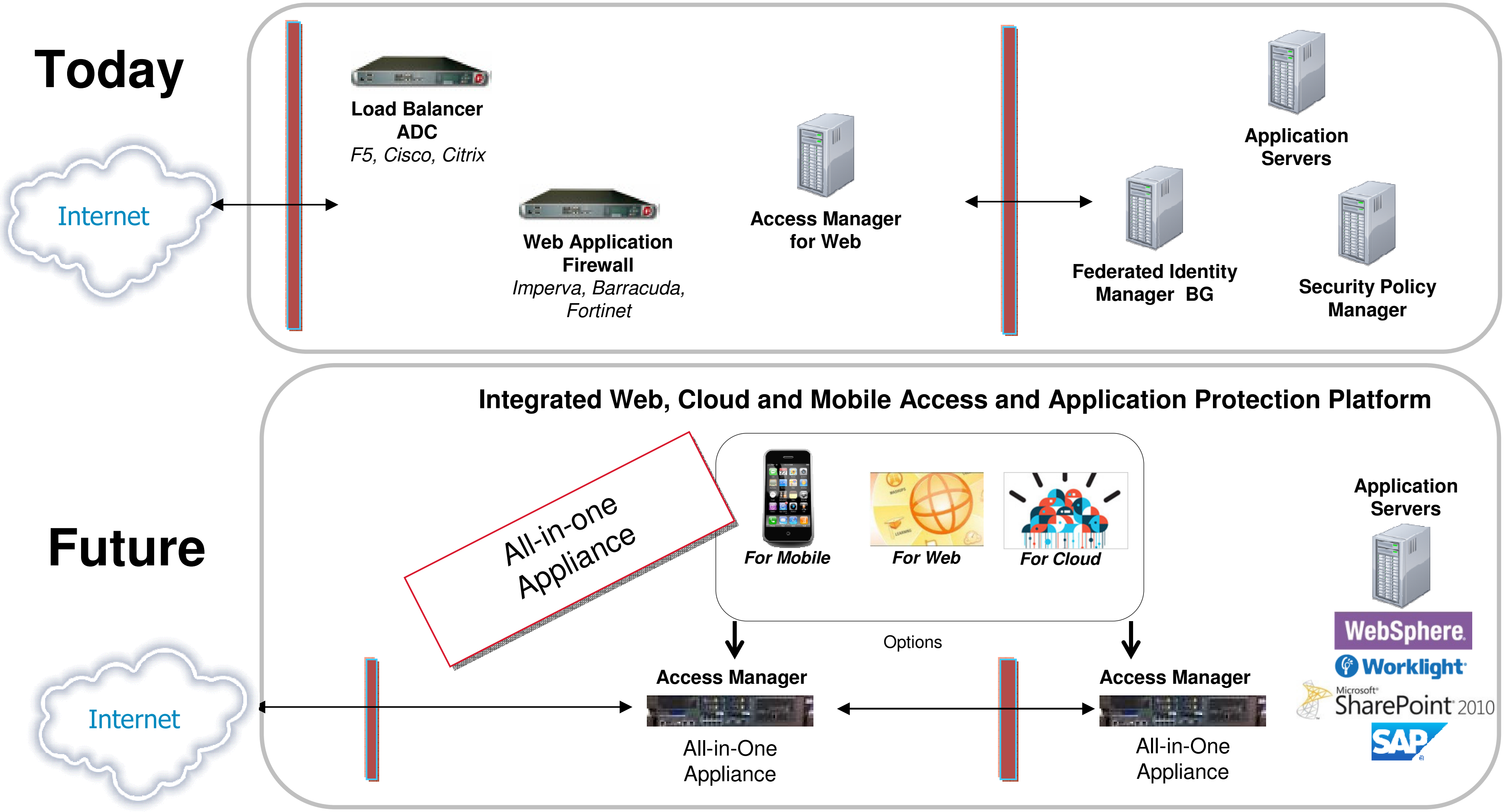
Policy-based authentication service provides easy-to-use SSO capability

Lightweight identity proofing adds identity assurance for IBM ID

Flexible SSO options based on industry standards such as OpenID and OAuth



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



Today

Internet

Load Balancer ADC
F5, Cisco, Citrix

Web Application Firewall
Imperva, Barracuda, Fortinet

Access Manager for Web

Application Servers

Federated Identity Manager BG

Security Policy Manager

Future

Integrated Web, Cloud and Mobile Access and Application Protection Platform

All-in-one Appliance

For Mobile

For Web

For Cloud

Options

Internet

Access Manager
All-in-One Appliance

Access Manager
All-in-One Appliance

Application Servers

WebSphere

Worklight

Microsoft SharePoint 2010

SAP

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

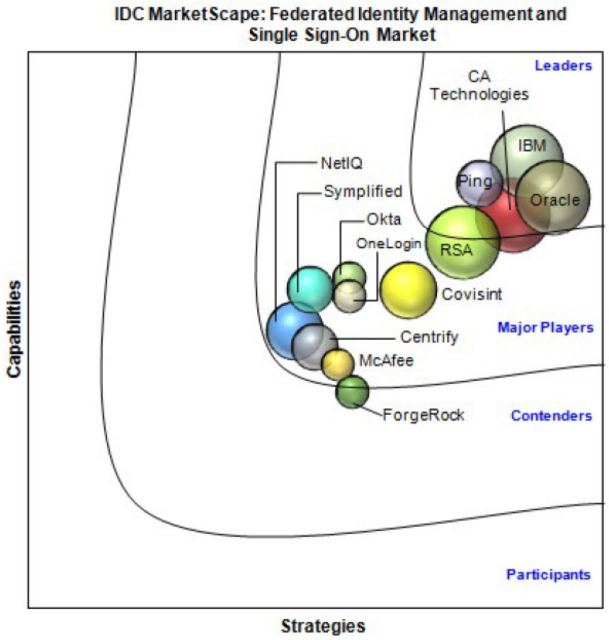
IBM has always been recognized as leader in Access Management

FROST & SULLIVAN

2014

IBM®

2014 Global Mobile Identity and Access Management
Customer Value Leadership Award



Source: IDC, 2014

IBM Access Management Customers

EXA CORPORATION

WESTJET

kotak
Kotak Mahindra Bank

ADP

me Bank
BANK FAIRER.

Boston Children's Hospital
OPENPediatrics™

PREMIER

metro

BlueCross BlueShield
of North Carolina

Threat-aware Identity and Access Management becomes the first line of defense for securing multi perimeter world

Safeguard mobile, cloud and social access

- **Validate "who is who"** especially when users connect from outside the enterprise
- **Proactively enforce access policies** on web, social and mobile collaboration channels

Prevent advanced insider threats

- **Manage and audit privileged access** across the enterprise
- **Defend applications and data** against unauthorized access

Deliver actionable identity intelligence

- **Streamline identity management** across all security domains
- **Manage and monitor user entitlements and activities** with security intelligence

Simplify cloud integrations and identity silos

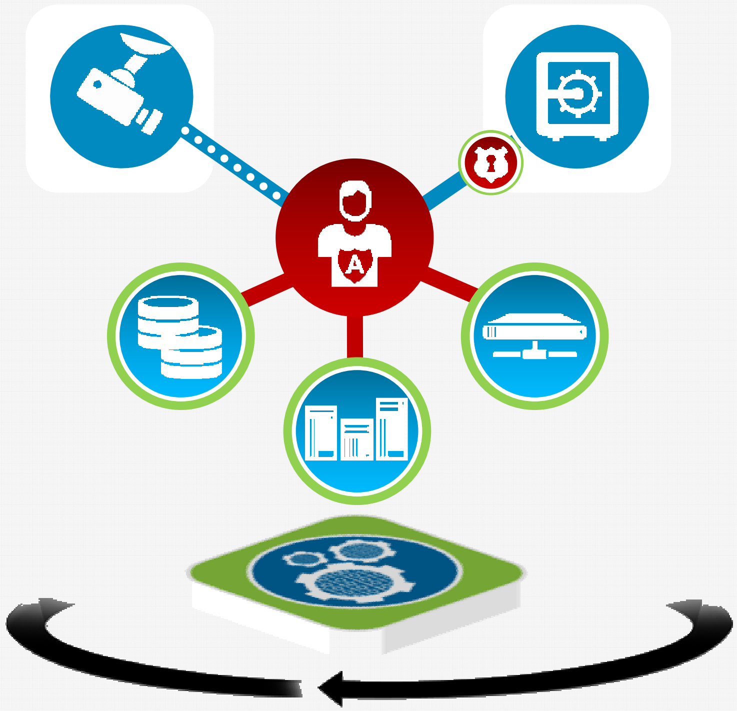
- **Provide federated access** to enable secure online business collaboration
- **Unify "Universe of Identities"** for efficient directory management

Introducing New Privileged Identity Management Solution

Prevent advanced insider threats

NEW

IBM Security Privileged Identity Manager

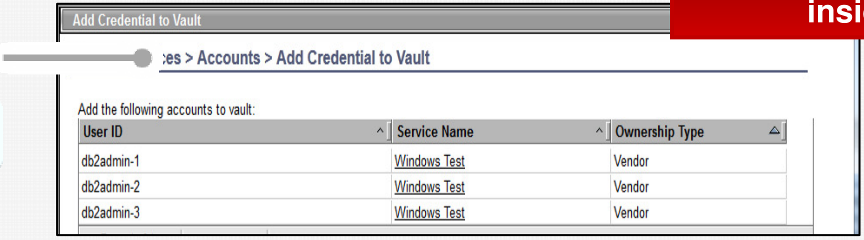


- **Eliminate the need to share passwords** for privileged users and shared accounts with an automated privileged identity management
- **Ensure compliance and audit support** with session recording and replay support
- **Improve ROI** using common Identity management and support for applications and resources
- **Strong authentication controls and SSO** for high-risk account access
- **Reduce TCO and time to value** with a scalable virtual appliance deployment

Secure and authenticate access with SSO and credentials vault

Prevent advanced insider threats

1 **Configure** Privileged Account



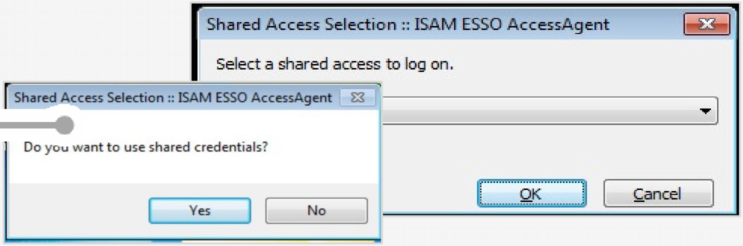
Add Credential to Vault

:es > Accounts > Add Credential to Vault

Add the following accounts to vault:

User ID	Service Name	Ownership Type
db2admin-1	Windows Test	Vendor
db2admin-2	Windows Test	Vendor
db2admin-3	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



Shared Access Selection :: ISAM ESSO AccessAgent

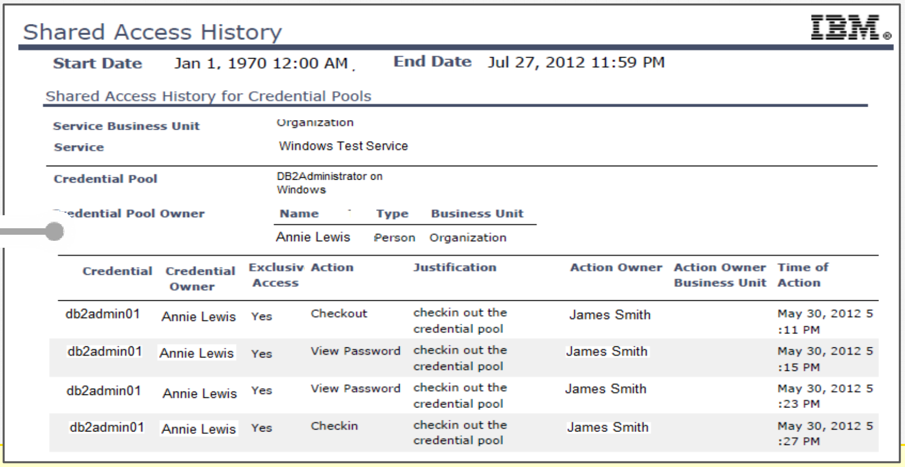
Select a shared access to log on.

Shared Access Selection :: ISAM ESSO AccessAgent

Do you want to use shared credentials?

Admin ID

3 User activity is logged



Shared Access History

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

~edential Pool Owner

Name	Type	Business Unit
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

✓ Privileged User Activity Monitoring:

- Recording and logging of user activity in sessions accessed through a shared ID
- Discourage users with privilege from abusing their rights

Threat-aware Identity and Access Management becomes the first line of defense for securing multi perimeter world

Safeguard mobile, cloud and social access

- **Validate "who is who"** especially when users connect from outside the enterprise
- **Proactively enforce access policies** on web, social and mobile collaboration channels

Prevent advanced insider threats

- **Manage and audit privileged access** across the enterprise
- **Defend applications and data** against unauthorized access

Deliver actionable identity intelligence

- **Streamline identity management** across all security domains
- **Manage and monitor user entitlements and activities** with security intelligence

Simplify cloud integrations and identity silos

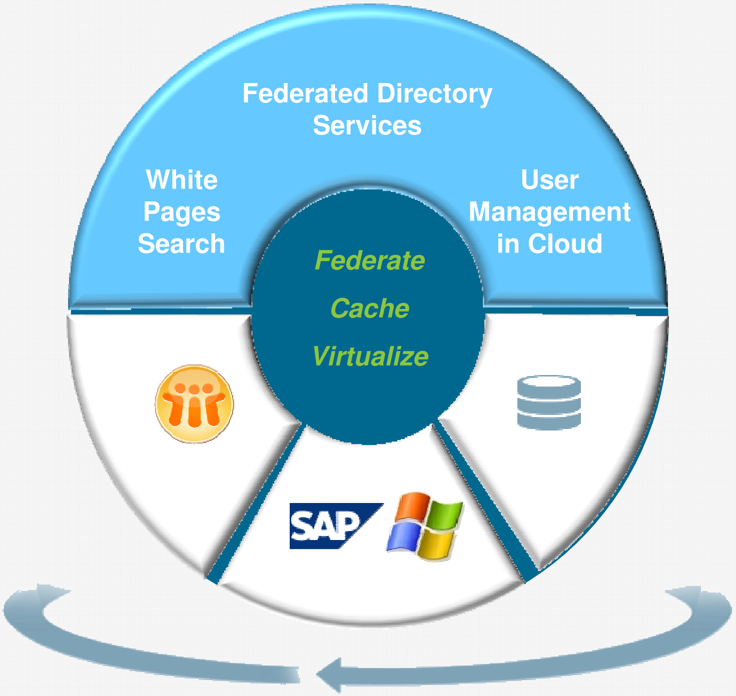
- **Provide federated access** to enable secure online business collaboration
- **Unify "Universe of Identities"** for efficient directory management

Introducing New Directory Services

Simplify identity silos and cloud integrations

NEW

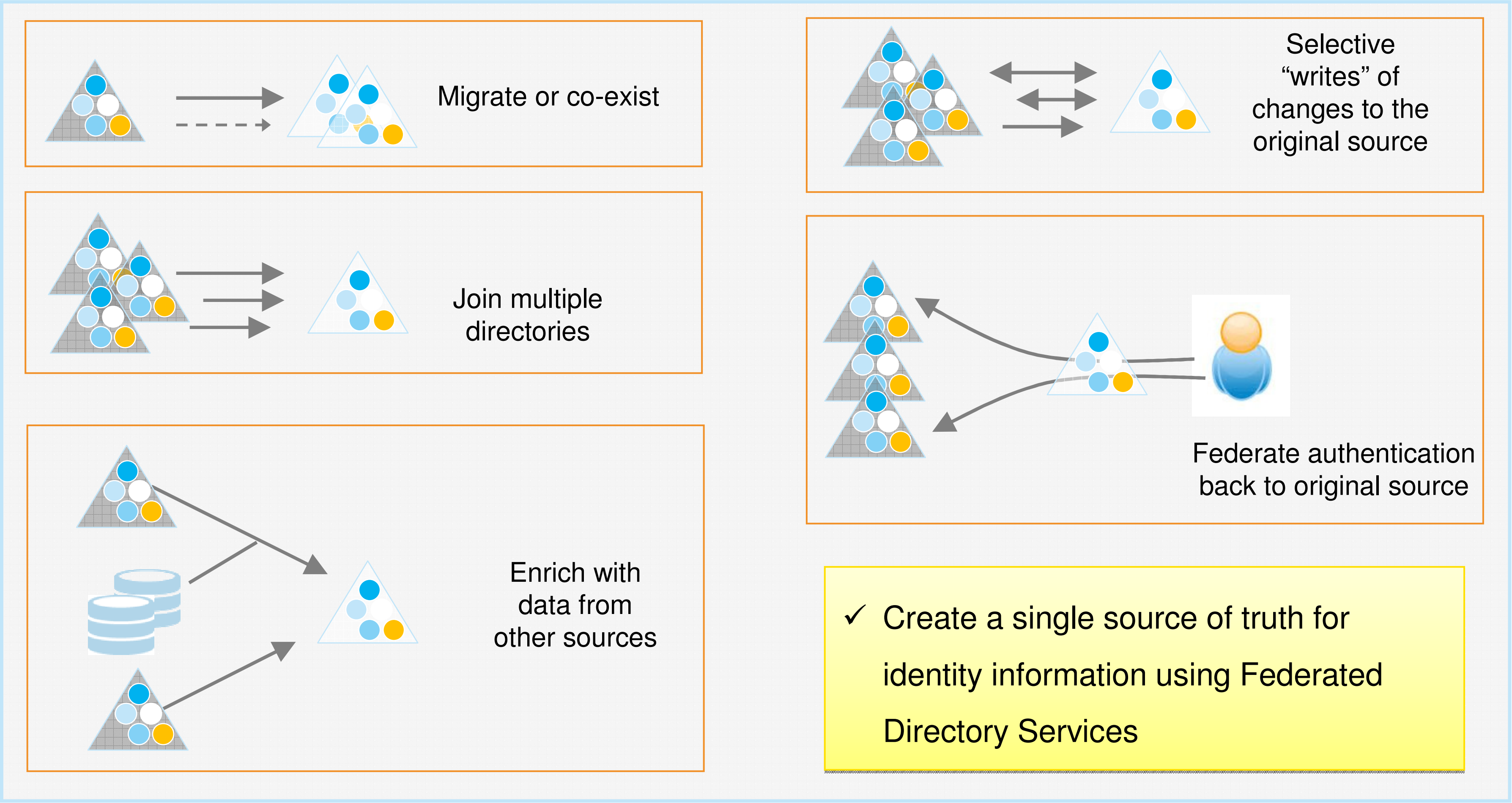
IBM Security Directory Server and Integrator



- **Universal directory** to transform identity silos and to support “virtual directory”-like deployments
- **Scalable directory backbone** leveraging existing infrastructure for enterprise-wide Identity and Access Management
- **Simplified sourcing of identities and attributes** for enterprise applications, Cloud/SaaS integrations
- **Intelligent White Pages search with social networking feature** to enable intuitive identity store browsing
- **In-depth user insight** with out of the box reports and IBM SIEM QRadar integration

“Untangle” identity silos to support business growth and increase efficiency

Simplify identity silos and cloud integrations



Migrate or co-exist

Join multiple directories

Enrich with data from other sources

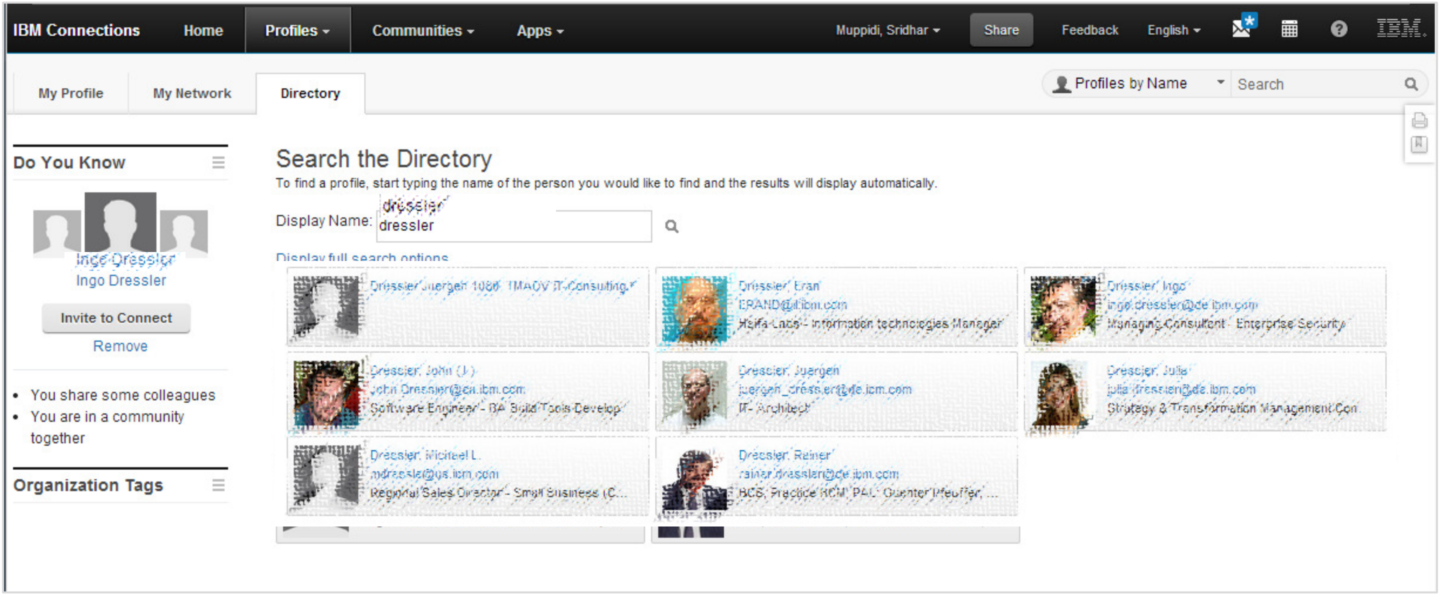
Selective “writes” of changes to the original source

Federate authentication back to original source

✓ Create a single source of truth for identity information using Federated Directory Services

Simplify integrating and maintaining multiple identity stores

Simplify identity silos and cloud integrations



- You share some colleagues
- You are in a community together

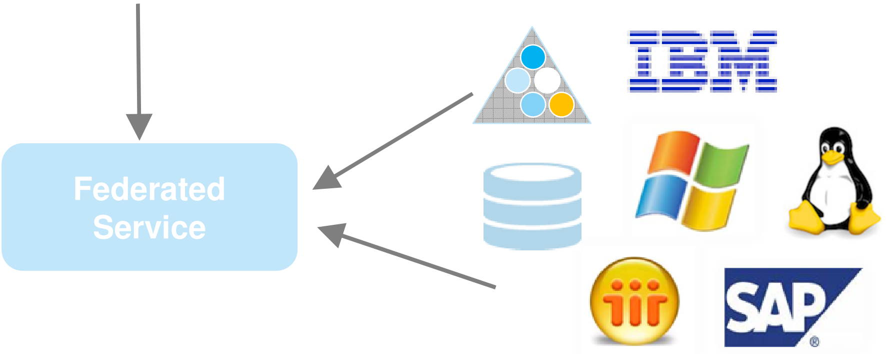
Search the Directory

To find a profile, start typing the name of the person you would like to find and the results will display automatically.

Display Name: dressler

Dressler, Juergen 1080 IMADV IT-Consulting
Dressler, Eran
ERAND@il.ibm.com
Haifa Labs - Information technologies Manager
Dressler, Ingo
ingo.dressler@de.ibm.com
Managing Consultant - Enterprise Security
Dressler, John (J.)
John.Dressler@ca.ibm.com
Software Engineer - BA Build Tools Develop
Dressler, Juergen
juergen_dressler@de.ibm.com
IT- Architect
Dressler, Julia
julia.dressler@de.ibm.com
Strategy & Transformation Management Con
Dressler, Michael L.
mdressle@us.ibm.com
Regional Sales Director - Small Business (C...
Dressler, Rainer
rainer.dressler@de.ibm.com
BCS, Practice RCM, PAL: Guenter Pfeuffer, ...

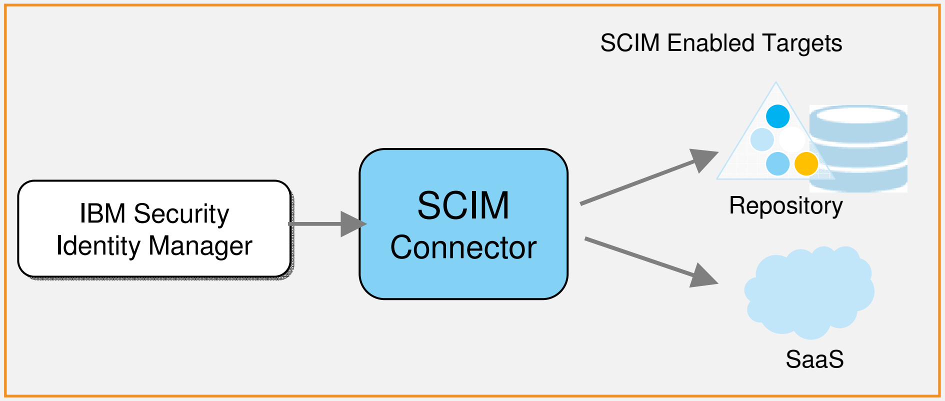
- ✓ White Pages application ready for social business
- ✓ Based on IBM Profiles
- ✓ Configured as Federated Directory Services instance to pull information from multiple repositories

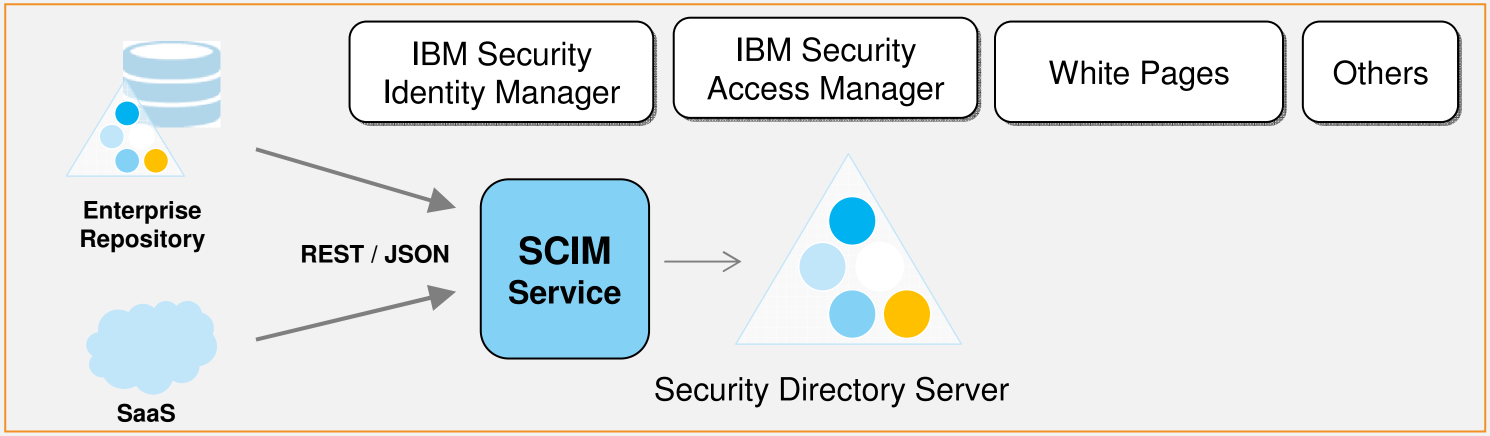


Directory Services: Authenticate and secure user access to Cloud and online environments

Simplify identity silos and cloud integrations

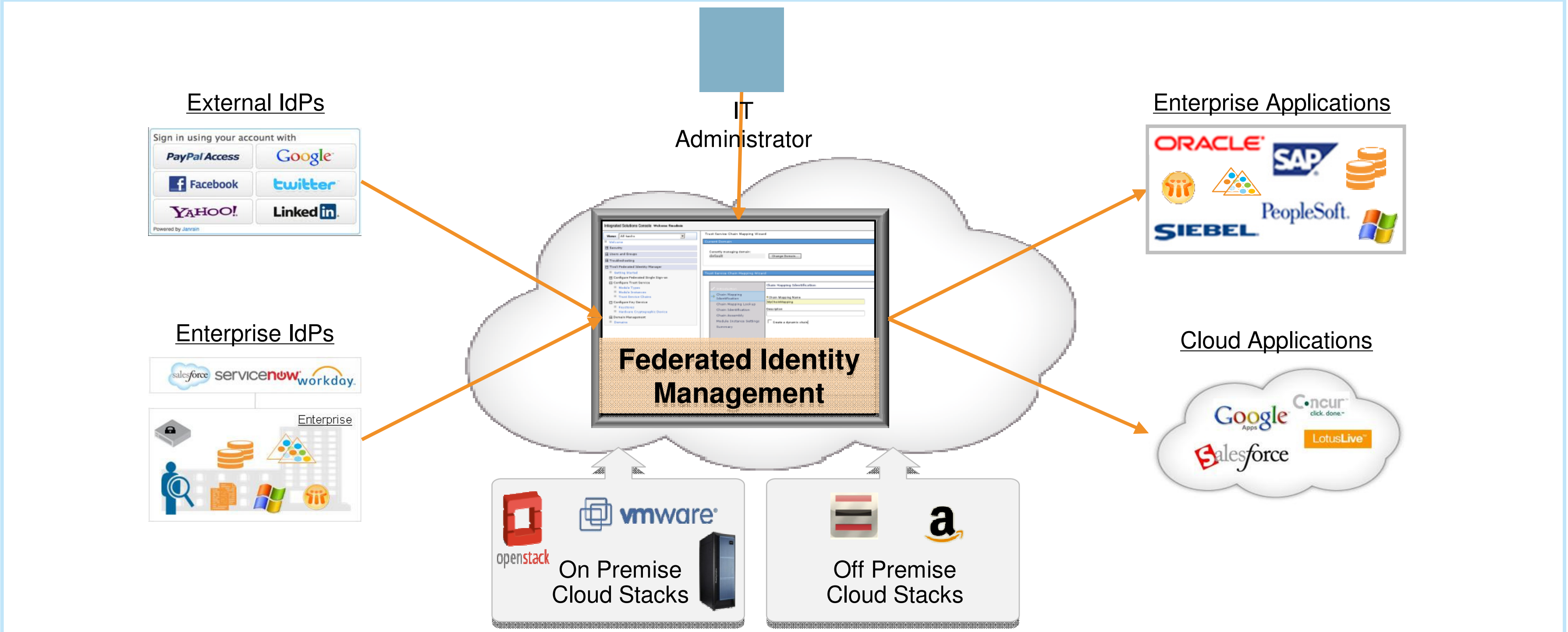
- ✓ Using SCIM for User On/Off-boarding with Cloud Environments
- ✓ REST/JSON interface for user & group management
- ✓ Security Directory Integrator provided as a service as well as through a connector




IBM Security Identity Manager
IBM Security Access Manager
White Pages
Others
Enterprise Repository
SaaS
REST / JSON
SCIM Service
Security Directory Server

Federated Identity Manager: Enabling user access to wide variety of apps including cloud, SaaS and web services

Simplify identity silos and cloud integrations



- **Consumer Federation and SSO with** support for standard protocols like SAML, OAuth, OpenID, WS-Trust
- **Built-in B2C self service and authentication for** scalability & flexible integration to improve identity assurance
- **Ease of deployment and integration to** support rapid Cloud, SaaS and application-level federation
- **Cross platform SSO** with built-in Security Token Service (STS) transforms between inbound and outbound security tokens like SAML, Kerberos, LTPA

Threat-aware Identity and Access Management becomes the first line of defense for securing multi perimeter world

Safeguard mobile, cloud and social access

- **Validate "who is who"** especially when users connect from outside the enterprise
- **Proactively enforce access policies** on web, social and mobile collaboration channels

Deliver actionable identity intelligence

- **Streamline identity management** across all security domains
- **Manage and monitor user entitlements and activities** with security intelligence

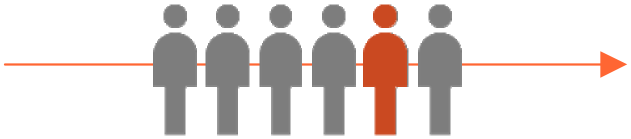
Prevent advanced insider threats

- **Manage and audit privileged access** across the enterprise
- **Defend applications and data** against unauthorized access

Simplify cloud integrations and identity silos

- **Provide federated access** to enable secure online business collaboration
- **Unify "Universe of Identities"** for efficient directory management

IAM Analytics will help control the risks across all security domains



Wave 1

Administration

- Cost savings
- Automation
- User lifecycle
- Key on premise apps & employees

Wave 2

Governance

- Role management & mining
- Access certification & attestation
- SOD
- Fine-grain entitlement reports

Wave 3

Analytics

•Application usage

•Privileged activity

•Risk-based control

•Baseline normal behavior

•Employees, partners, consumers – anywhere

IAM Analytics – Collect and Analyze Identity Data

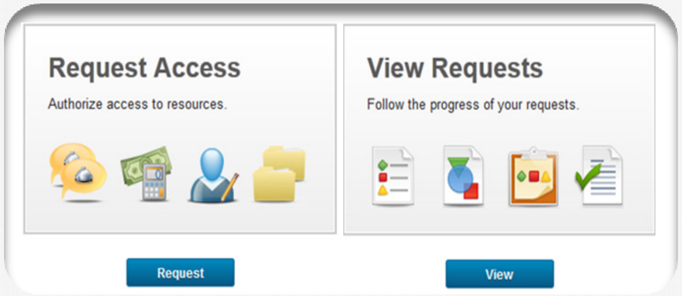
- Improved visibility into how access being utilized
- Risk-based insights for prioritized compliance actions
- Clear actionable dashboards for better business decision making

Introducing New Identity Management Solution

Deliver actionable identity intelligence

NEW

IBM Security Identity Manager



Request Access

Authorize access to resources.

View Requests

Follow the progress of your requests.

Re-designed, business friendly user interface

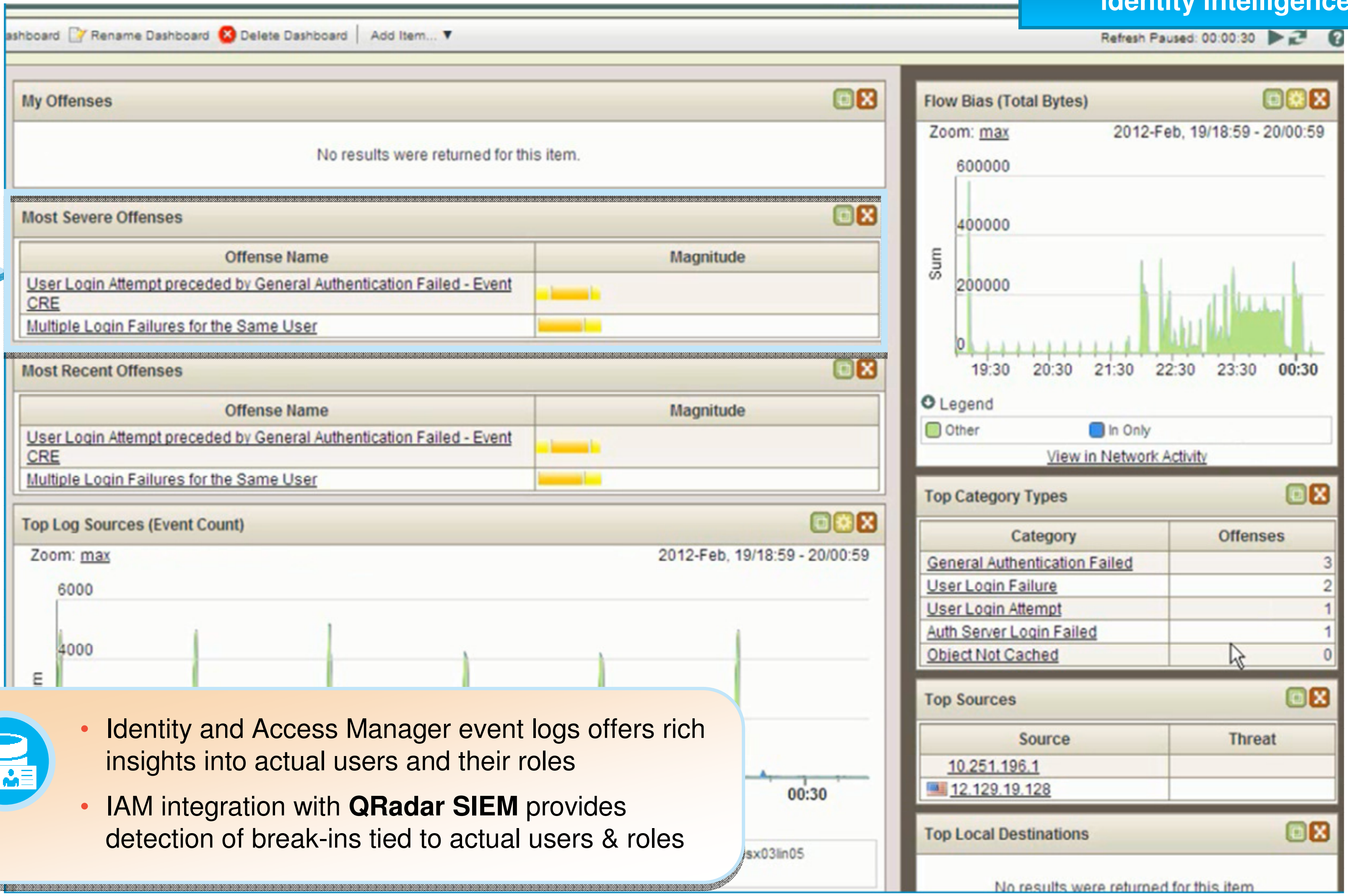
Identity analytics

IAM integration with Security Intelligence

- **Empower Line of Business** to manage and define the user access for governance, risk and compliance
- **Reduce cost of enterprise identity management** with centralized policy, integrated role and identity lifecycle management
- **Improve user assurance** with strong authentication integration and closed-loop user activity monitoring
- **Effective and actionable compliance** with centralized identity and access management across the enterprise
- **Real-time insider fraud detection** with integrated IAM and Security Intelligence

Integrated products provide user activity and detect anomalies

Deliver actionable identity intelligence



My Offenses

No results were returned for this item.

Most Severe Offenses

Offense Name	Magnitude
User Login Attempt preceded by General Authentication Failed - Event CRE	
Multiple Login Failures for the Same User	

Most Recent Offenses

Offense Name	Magnitude
User Login Attempt preceded by General Authentication Failed - Event CRE	
Multiple Login Failures for the Same User	

Top Log Sources (Event Count)

Flow Bias (Total Bytes)

Top Category Types

Category	Offenses
General Authentication Failed	3
User Login Failure	2
User Login Attempt	1
Auth Server Login Failed	1
Object Not Cached	0

Top Sources

Source	Threat
10.251.196.1	
12.129.19.128	

Top Local Destinations

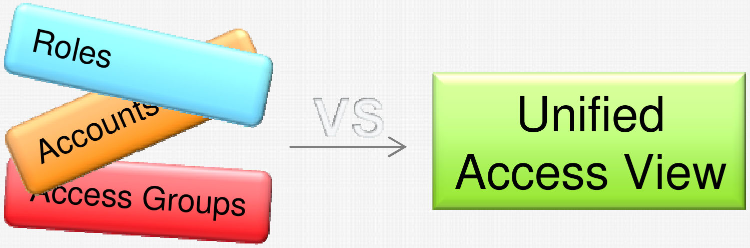
No results were returned for this item.

- Identity and Access Manager event logs offers rich insights into actual users and their roles
- IAM integration with **QRadar SIEM** provides detection of break-ins tied to actual users & roles

Empower business users to manage and govern access

Relevant to Business Users:

What access does Judith have?



Intuitive resource names

IT name
LDAP server
a2164.raleigh…

VS

Business name
East region
corporate directory

Functional tasks:
Judith is transferring departments I need to…

Remember to…
1. Delete access
2. Modify her user record
3. Notify her new manager

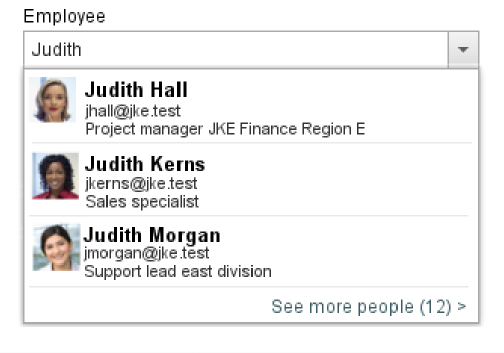
VS

Simply launch…

Transfer my employee

Modern, Intuitive, Efficient

Modern features - take cues from social media and e-commerce


Employee

Judith

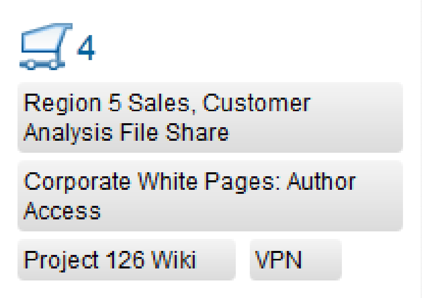
Judith Hall
jhall@jke.test
Project manager JKE Finance Region E

Judith Kerns
jkerns@jke.test
Sales specialist

Judith Morgan
jmorgan@jke.test
Support lead east division

See more people (12) >

Batch requests - shopping cart


4

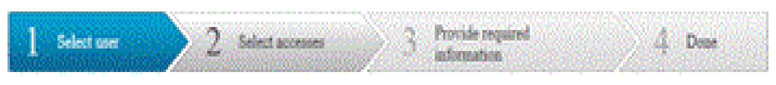
Region 5 Sales, Customer Analysis File Share

Corporate White Pages: Author Access

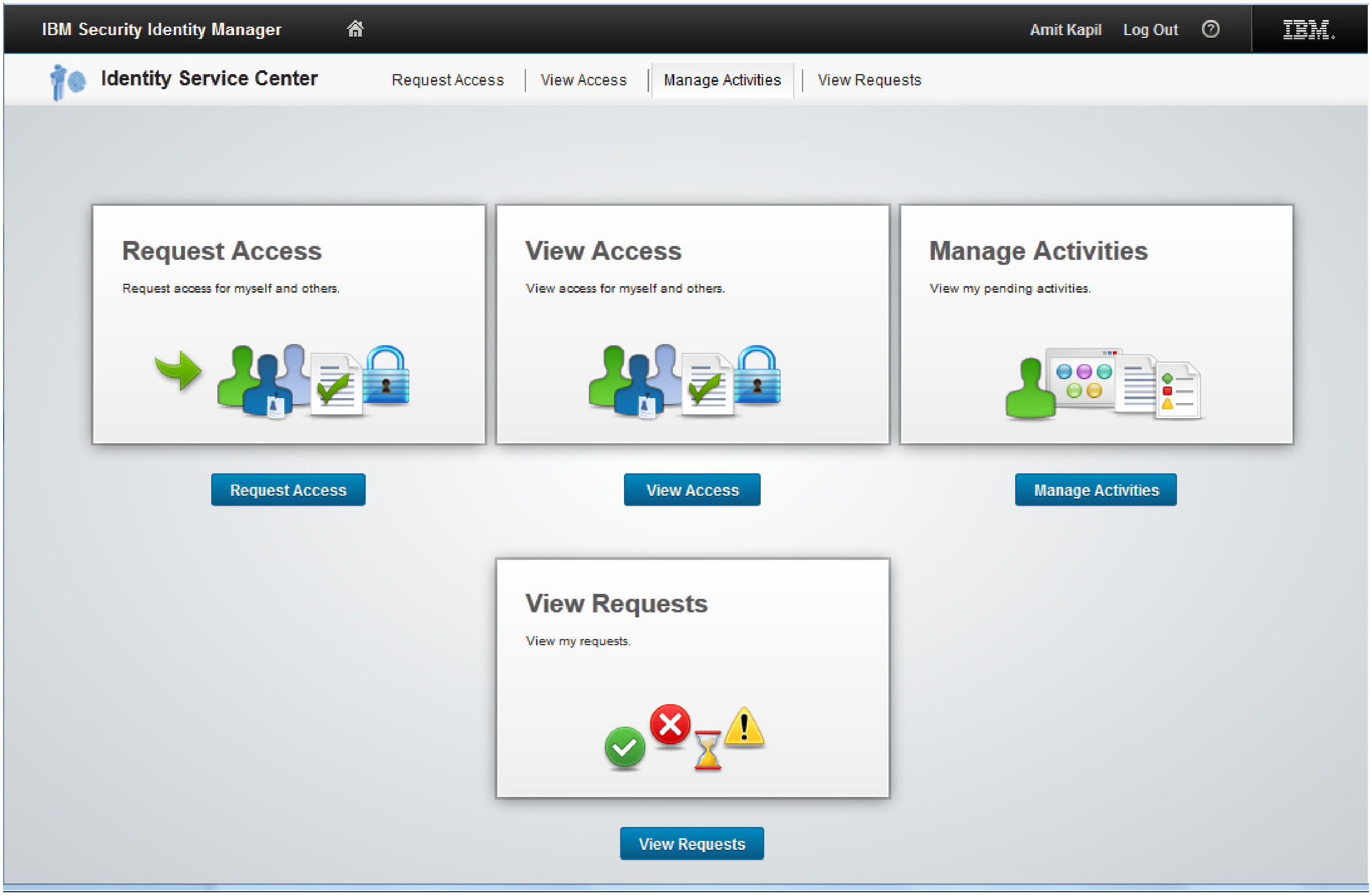
Project 126 Wiki

VPN

Guided



Identity Service Center – Home screen



Request Access

Request access for myself and others.

View Access

View access for myself and others.

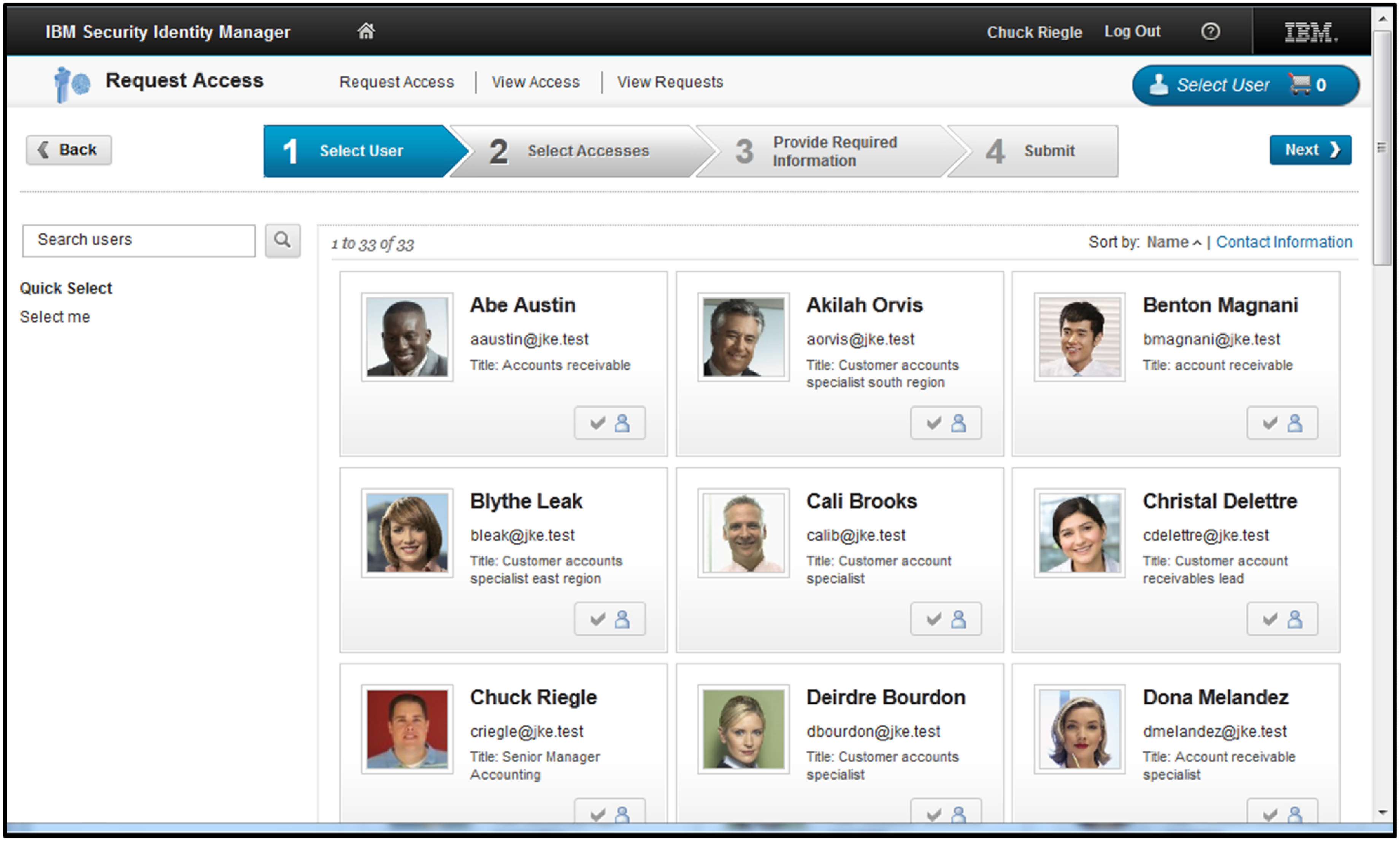
Manage Activities

View my pending activities.

View Requests

View my requests.

Identity Service Center - User search and selection


IBM Security Identity Manager
Chuck Riegle
Log Out
IBM.
Request Access
Request Access | View Access | View Requests
Select User 0
Back
1 Select User
2 Select Accesses
3 Provide Required Information
4 Submit
Next
Search users
Quick Select
Select me
Sort by: Name | Contact Information

1 to 33 of 33

Abe Austin
aaustin@jke.test
Title: Accounts receivable

Akilah Orvis
aorvis@jke.test
Title: Customer accounts specialist south region

Benton Magnani
bmagnani@jke.test
Title: account receivable

Blythe Leak
bleak@jke.test
Title: Customer accounts specialist east region

Cali Brooks
calib@jke.test
Title: Customer account specialist

Christal Delettre
cdelettre@jke.test
Title: Customer account receivables lead

Chuck Riegle
criegle@jke.test
Title: Senior Manager Accounting

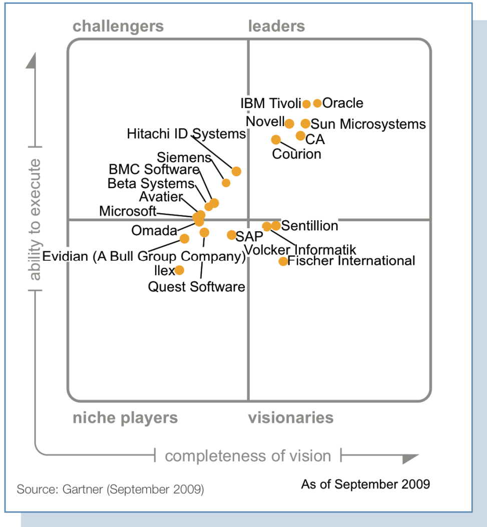
Deirdre Bourdon
dbourdon@jke.test
Title: Customer accounts specialist

Dona Melandez
dmelandez@jke.test
Title: Account receivable specialist

Gartner User Provisioning MQ

- Consistent Market Leadership
- 2013 Gartner changed MQ criteria
- Changes and IBM placement not consistent with past assessments

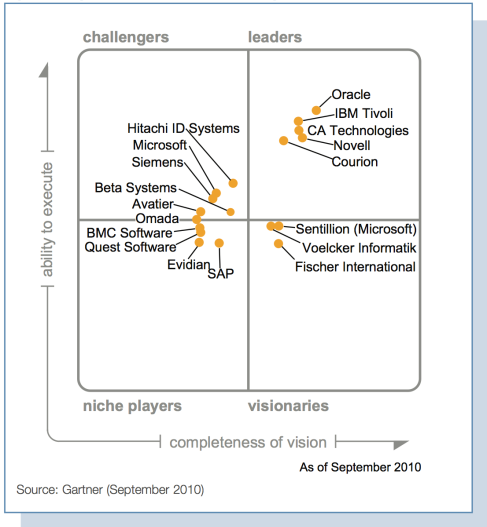
Figure 1. Magic Quadrant for User Provisioning



Source: Gartner (September 2009)

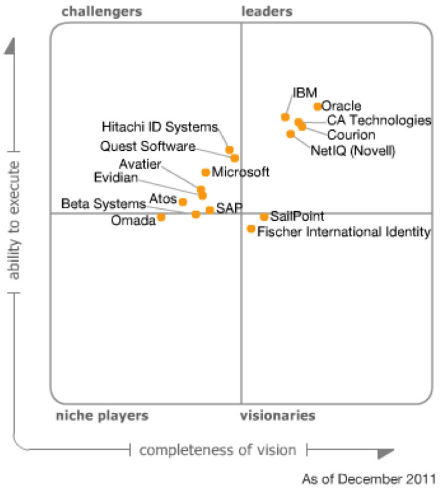
As of September 2009

Figure 1. Magic Quadrant for User Provisioning

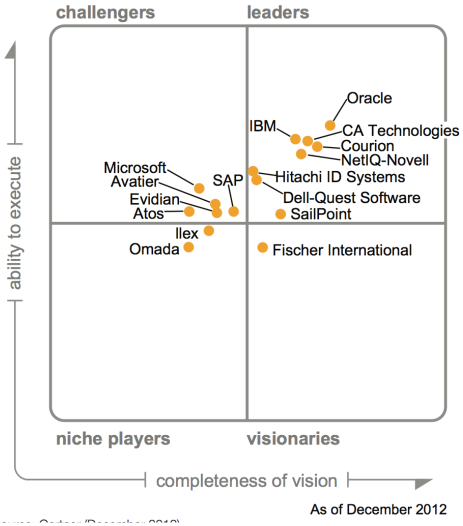


As of September 2010

Source: Gartner (September 2010)



As of December 2011



As of December 2012

Source: Gartner (December 2012)

Leading industry analysts recognized IBM IAM vision and strategy

FROST & SULLIVAN

- Recognizes IBM as a Leader in Mobile Identity and Access Management Solutions in 2014

IDC Analyze the Future

- Recognizes IBM as **market share leader** in 2013
  - WW Identity and Access Management
  - Federation Identity Management and SSO MarketScape leader in 2014

Gartner

- Recognizes IBM as a **visionary** in the new 2013 IAG MQ
  - New ISIM 6.0 service center UI
  - 2014 Roadmap focus on IAM Analytics, beyond today's Governance solutions

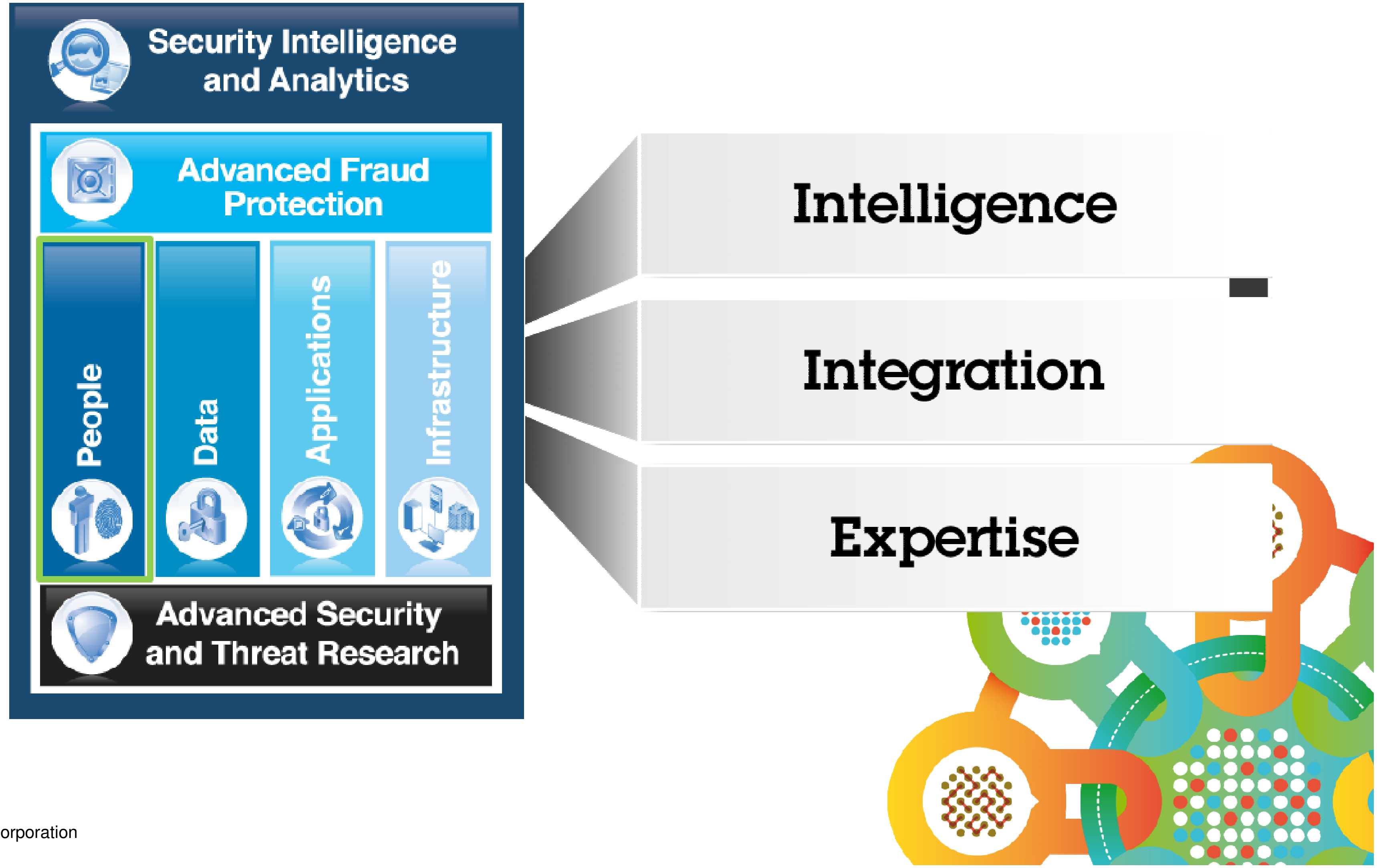
kuppingercole ANALYSTS

- Recognizes IBM as **leaders** in key leadership compass reports
  - Identity Provisioning, Privileged Identity Management
  - Access Management & Federation, Enterprise SSO

FORRESTER

- Recognizes IBM as **strong performer** in their 2013 Wave report
  - WW Identity and Access Management

Security Intelligence.
Think Integrated.


Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

Intelligence

Integration

Expertise

Thank you!

"The identity I stole was a fake!
Boy, you just can't trust people these days!"

ibm.com/security