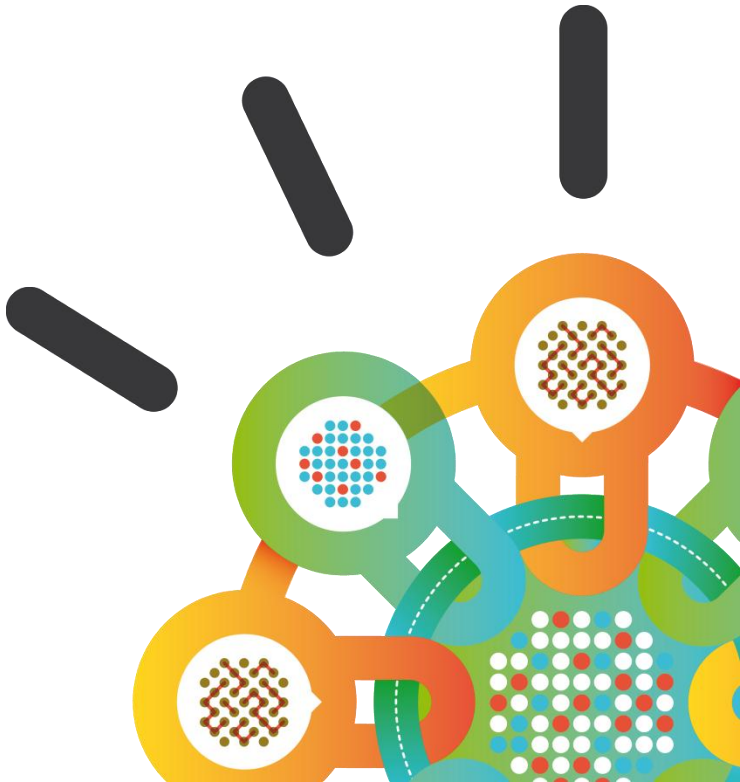
Security Intelligence.
Think Integrated.

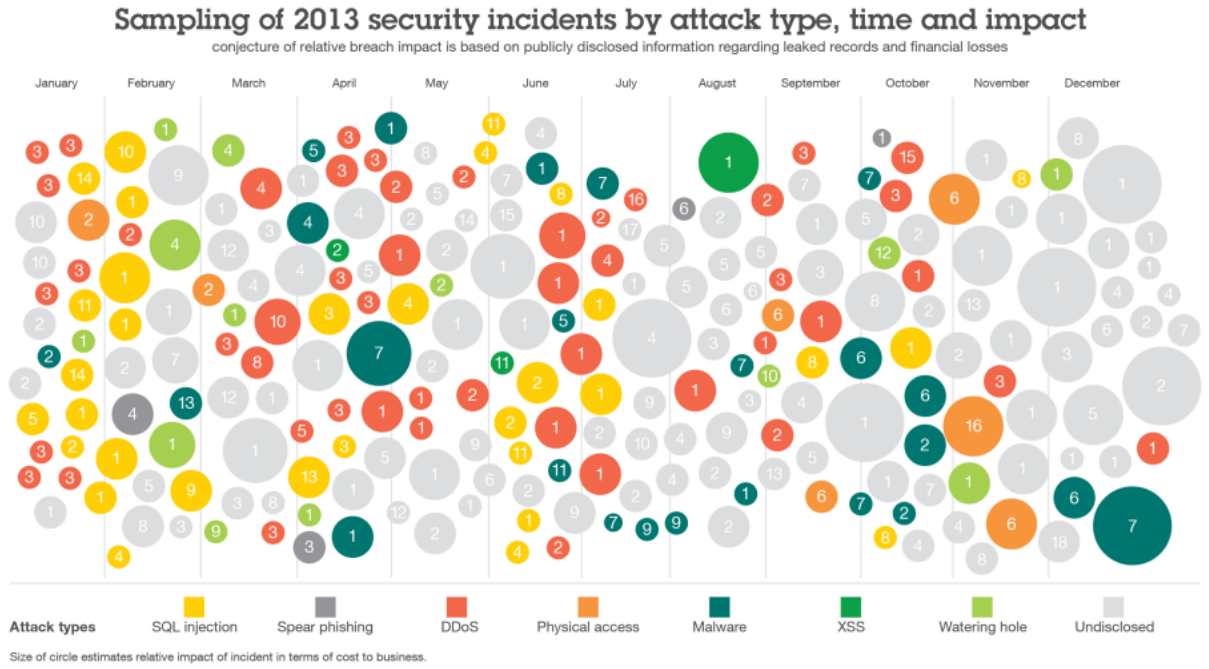
Threat-Aware Identity and Access Management

IAM 2020 Vision

September 2014



More than half a billion records of PII were leaked in 2013



Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

Most-common attack types

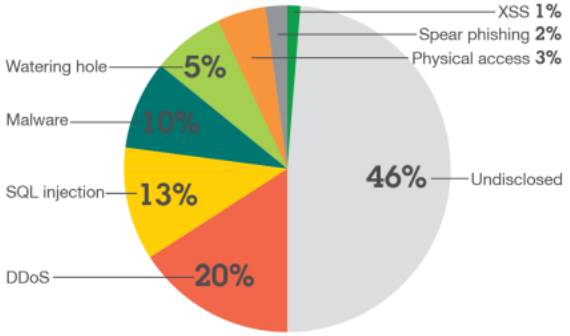


Figure 2a. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

Enterprise 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

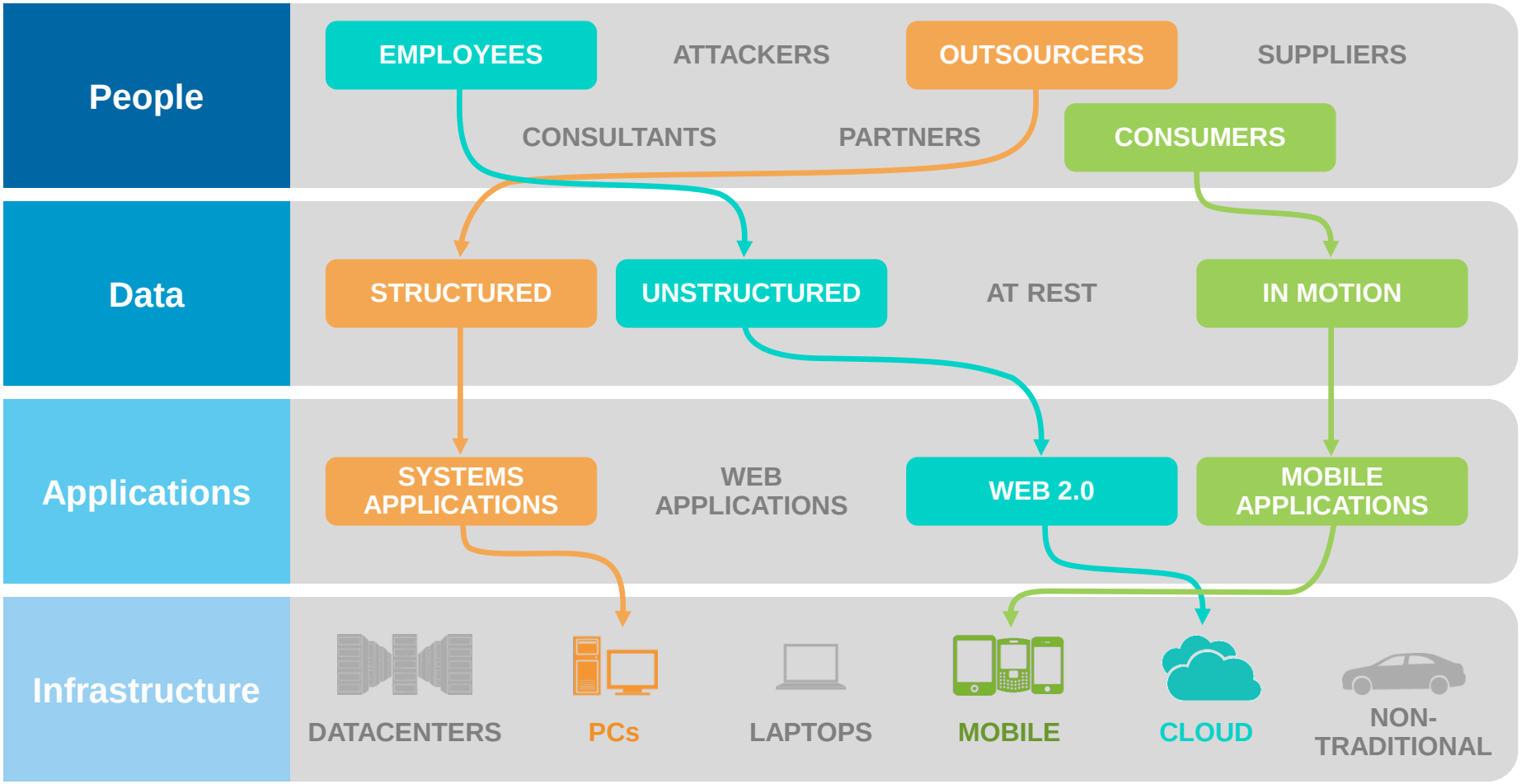
Criminals are selling stolen or fabricated accounts

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

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

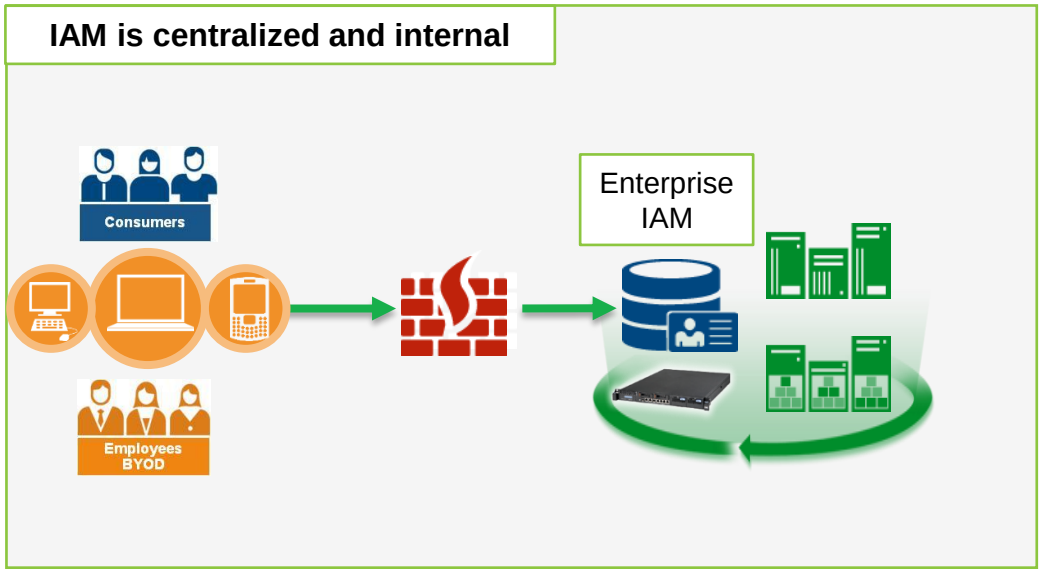
Source: IBM X-Force® Research 2013 Trend and Risk Report

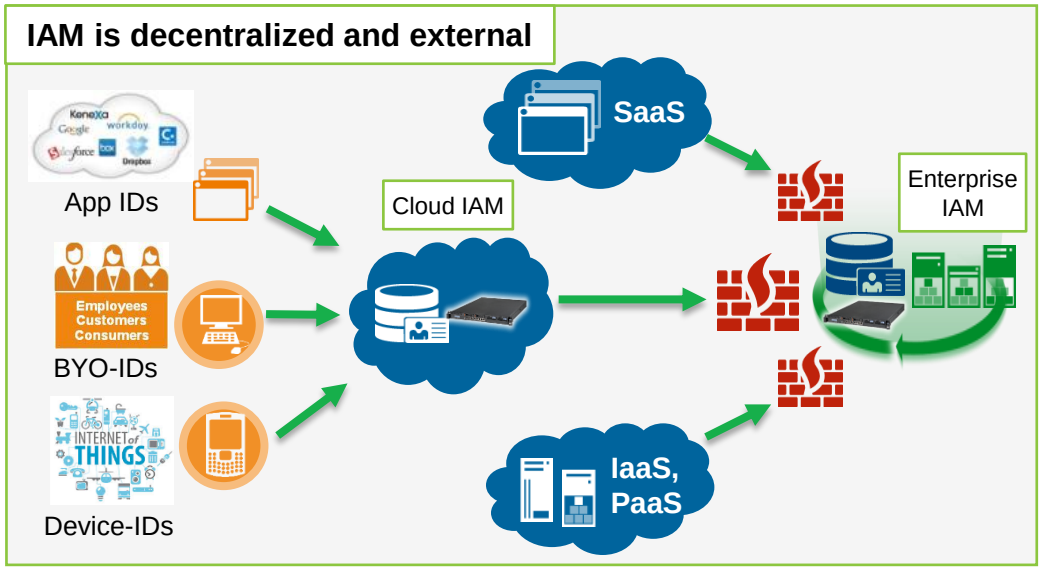
Enterprise Security will need to focus on Identity and Interactions



…and that is emerging role for IAM 2020

1. Identity is a key security control for a multi-perimeter world





Was: Administration

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

Is: Assurance

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

2. Cloud security focusing on Identity + Protection + Insights

SaaS: Secure usage of business applications

Enable employees to connect securely to SaaS

- Identity federation
- SaaS access governance

PaaS: Secure service composition and apps

Integrate identity into services and applications

- Authentication and authorization APIs
- DevOps access management

IaaS: Securing infrastructure and workloads

Manage cloud administration and workload access

- Privileged administrator management
- Access management of web workloads

3. Evolving business –driven Identity Governance and Analytics

Identity and Governance Evolution

Wave 1: Administration

- Cost savings
- Automation
- User lifecycle
- Key on premise applications and employees

Wave 2: Governance

- Role management
- Access certification
- Extended enterprise and business partners
- On and off-premise applications

Wave 3: Analytics

- Risk-based control
- Baseline normal behavior
- Application usage
- Privileged activity
- Employees, partners, consumers – anywhere

Identity Intelligence – 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

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

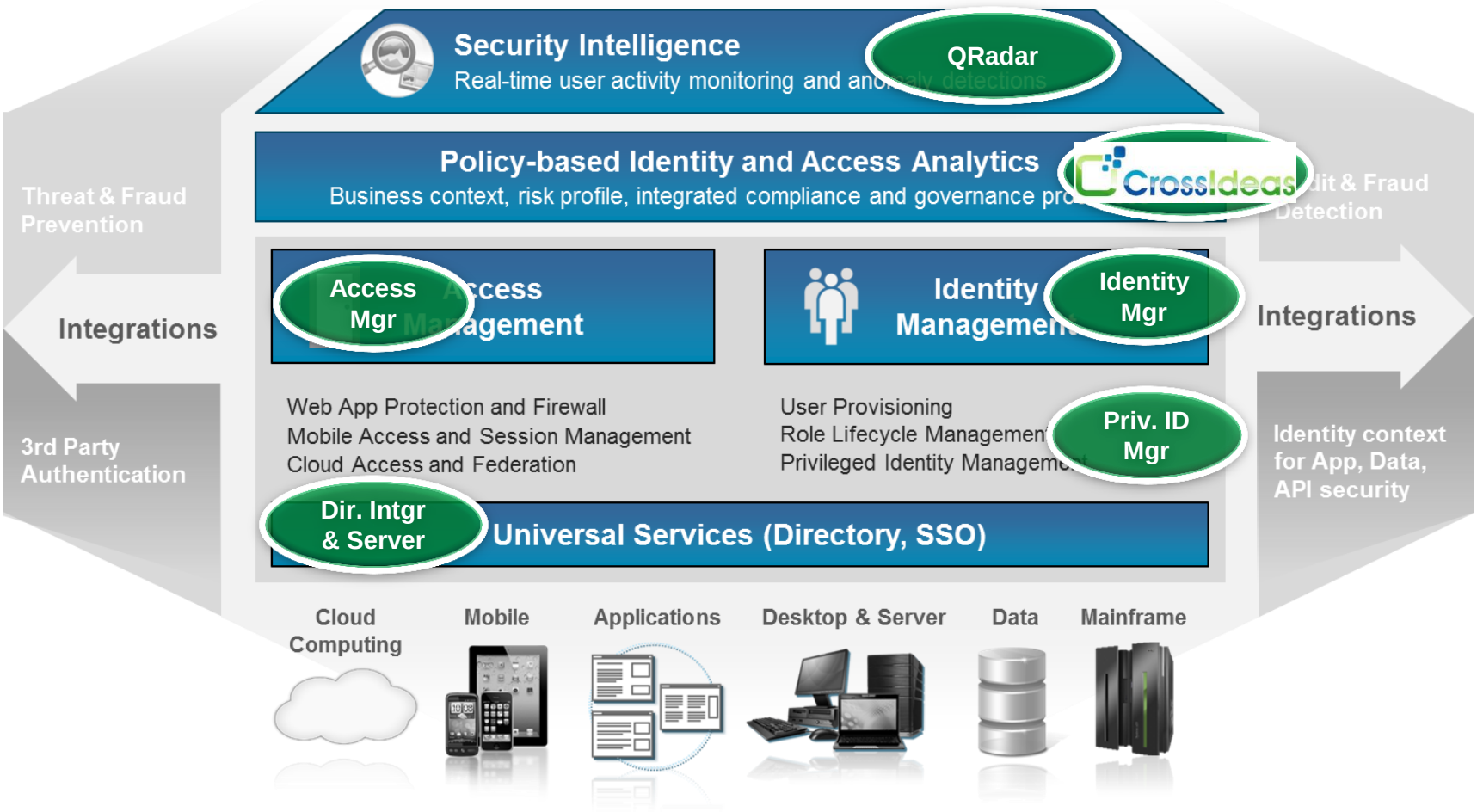
Deliver actionable identity intelligence

- **Integrated access governance and lifecycle management** with identity analytics, risk-based governance and proactive provisioning policies
- **Provide real time, user activity profiling** 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

IBM Threat-aware Identity and Access Management Strategy



Manage Enterprise Identity Context Across All Security Domains

IAM maturity model to support Enterprise Security

	Security Intelligence: User activity monitoring, Anomaly detection, Identity Analytics & Reporting				
Optimized	IAM Integration with GRC Fine-grained entitlements	Integrated Web & Mobile Access Gateway Risk / Context based Access	Governance of SaaS applications IAM as a SaaS	IAM integration with GRC Risk/ Context-based IAM Governance	Risk / Context-based Privileged Identity Mgmt
Proficient	Closed-loop Identity & Access Mgmt Strong Authentication	Strong Authentication (e.g. device based) Web Application Protection	Bring your own ID Integrated IAM for IaaS, PaaS & SaaS (Enterprise)	Closed-loop Identity and Access Mgmt Access Certification & fulfillment (Enterprise)	Closed-loop Privileged Identity Mgmt
Basic	Request based Identity Mgmt Web Access Management	Federated SSO Mobile User Access Management	Federated access to SaaS (LoB) User Provisioning for Cloud/SaaS	Access Certification (LoB) Request based Identity Mgmt.	Shared Access and Password Management
	Compliance	**Mobile Security**	**Cloud Security**	**IAM Governance**	**Privileged IdM**

Recent Updates

IBM Security Access Manager 8.0

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

NEW

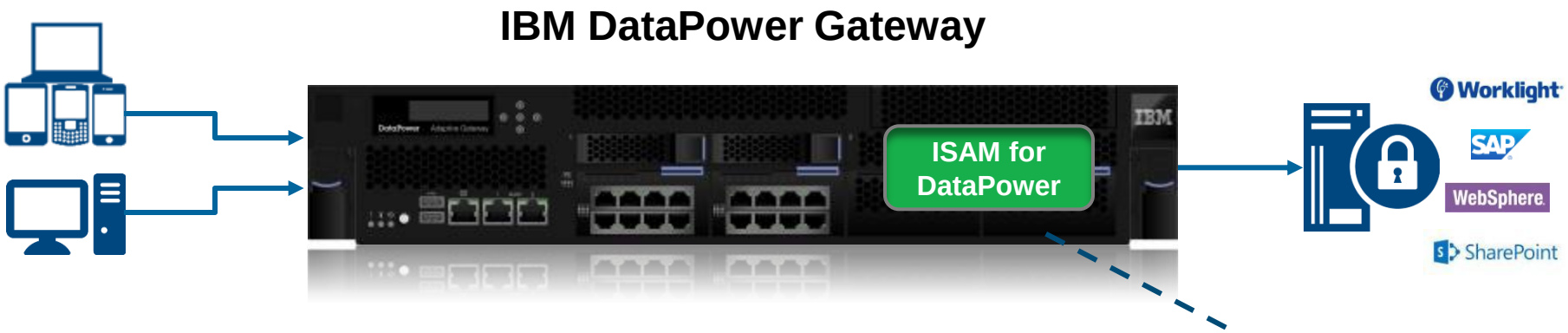
Safeguard mobile, cloud, and social access

IBM Security Access Manager

- **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, and IP reputation input via 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

Introducing IBM's multi-channel gateway solution

Leverage the combined capabilities of IBM DataPower Gateway and IBM Security Access Manager in a single, converged security and integration gateway solution



Message security

Traffic control & optimization

Message & transport bridging

User access security

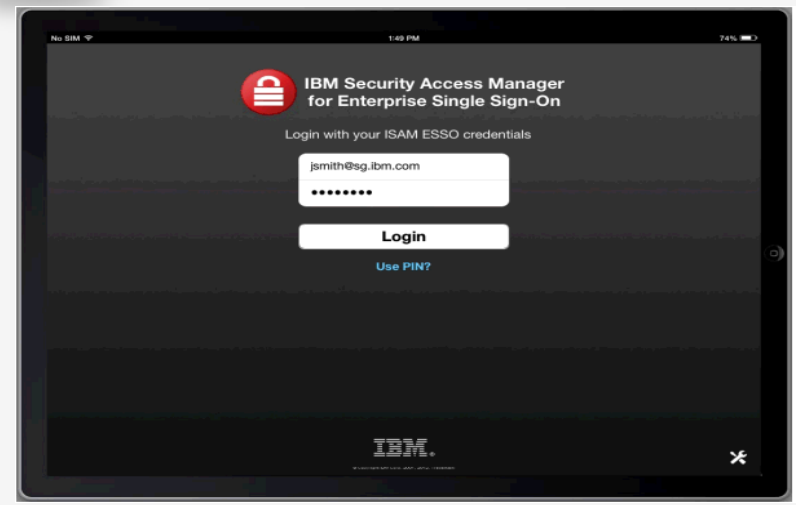
Key Benefits

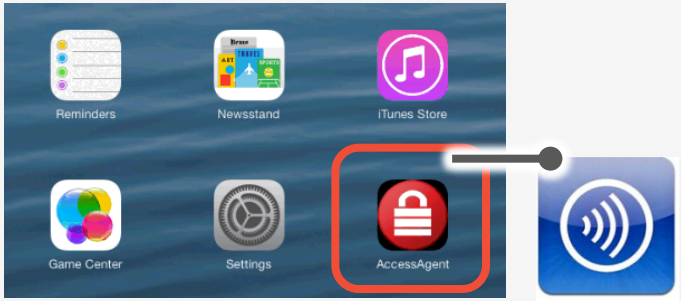
Reduce Operating Costs	Improve Business Agility	Improve Edge Security	Secure User Interactions	Secure App Interactions
Single gateway reduces hardware footprint and uses common set of management and operational skills	Common security policy framework that can be shared across business channels	Comprehensive security at the message-level, infrastructure-level, and user-level	Safeguard mobile, cloud, and social access	Protect applications at the message-level and provide optimized application delivery

IBM Security Access Manager for ESSO now supports iPad SSO

NEW

Safeguard mobile, cloud, and social access





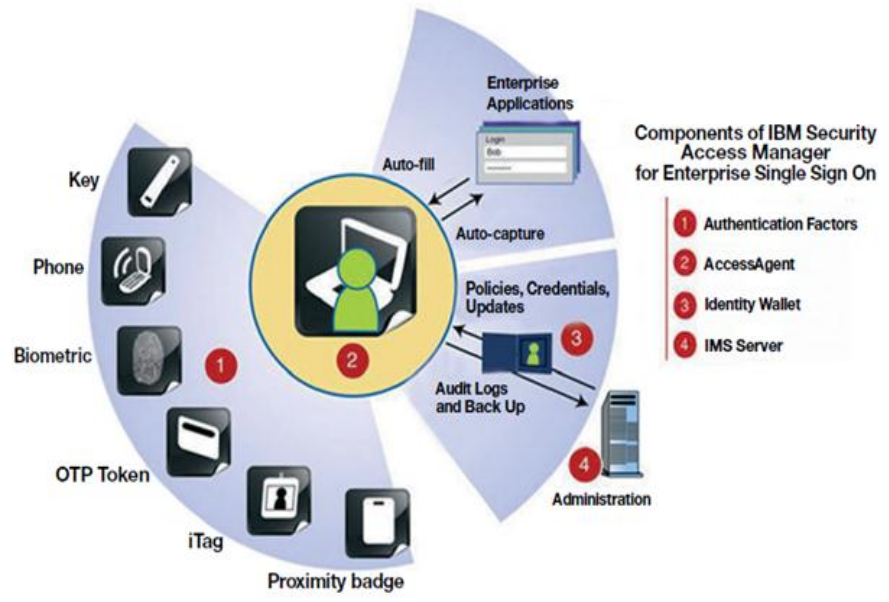
- **Single Sign-On into web applications** with Secure Browser for iPad
- **Local secure password store** for all users on the device with Wallet Manager for iPad
- **SSO from iPad to Application Virtualization platforms** such as Citrix XenApp
- **SSO from iPad to Virtual Desktop Infrastructure platforms** such as Citrix XenDesktop and VMWareView

IBM Security Access Manager for Enterprise Single Sign-On

Prevent advanced insider threats

Updated

IBM Security Access Manager For Enterprise Single Sign-On



- **Simplify password management** for reduced help desk costs and improved security
- **Provide visibility** into user activity, control over user access, and automation of sign-on process
- **Deliver policy-based authentication** with support for third party multi-factor devices
- **Track and report on user access activities** with Session Management and fine grained application audit logs

NEW - MAY 2014 Release

- **Broader Platform support** - Citrix XenDesktop 7.0/7.1 and Windows 8.1
- **Support for Host on Demand** - Introducing IBM Host on Demand support for providing mainframe coverage
- **Improved Performance and enhanced monitoring**
- **Advanced reporting based on Cognos** - Ensuring better insight and visibility of the system

IBM Security Privileged Identity Manager updates

Updated

Prevent advanced insider threats

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

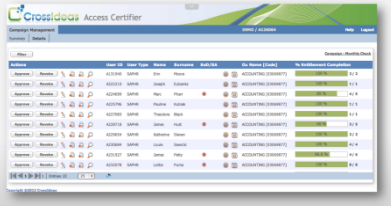
MAY 2014 Release

- **Session Recorder with enhanced search, image compression and archiving** to lower TCO and simplify management of stored recordings.
- **Additional checkout capabilities** to support both manual and automated credential checkout
- **Unified Cognos reporting** with state of the art dashboard.
- Virtual Appliance **high availability and failover functions.**

Driving business-focused compliance with Identity Management

Deliver actionable identity intelligence

Access Certification and Activity-based SOD
with Integrated Governance capabilities

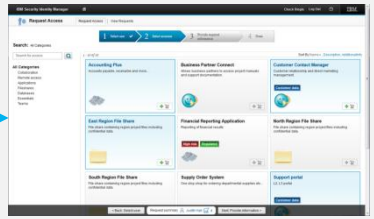


Identity Governance and Administration

Identity Change → *Access Policy* → *Access Certification* → *Accounts Updated*

Detect and Correct Local Privilege Settings

HR Systems/Identity Stores



Risk Based Access

On/Off-premise Resources

Applications *Data* *Cloud* *Mobile*

Empower Line of Business to manage and define the user access for governance, risk and compliance

Improve user assurance with strong authentication integration and closed-loop user activity monitoring

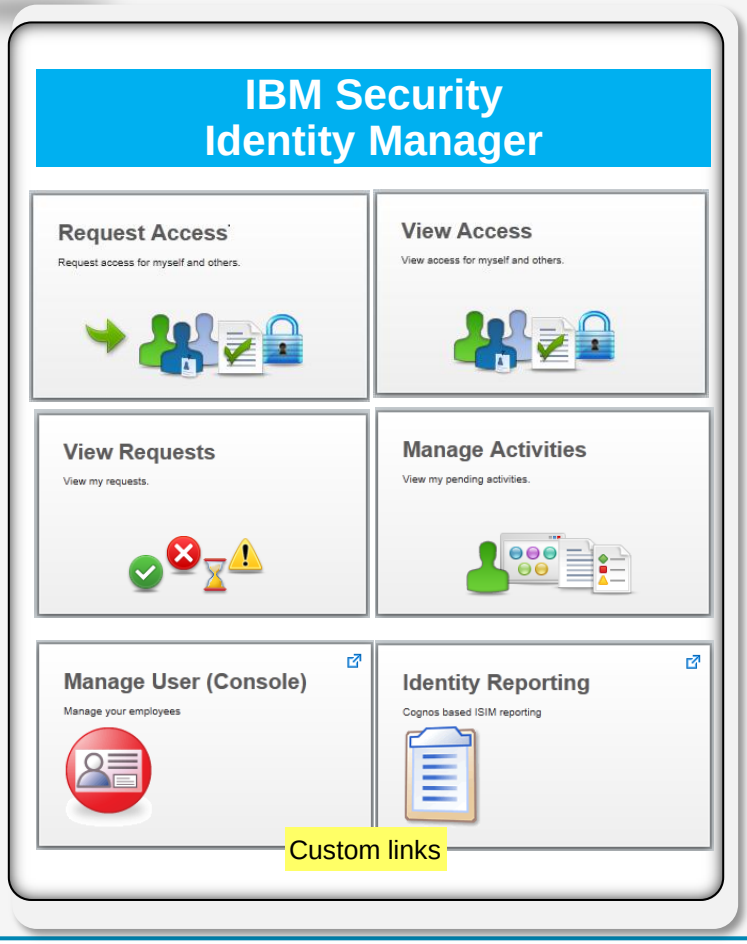
Reduce cost of enterprise identity management with centralized policy, integrated role and identity lifecycle management

Effective and actionable compliance with centralized identity and access management across the enterprise

IBM Security Identity Manager

Updated

Deliver actionable Identity 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

MAY 2014 Release

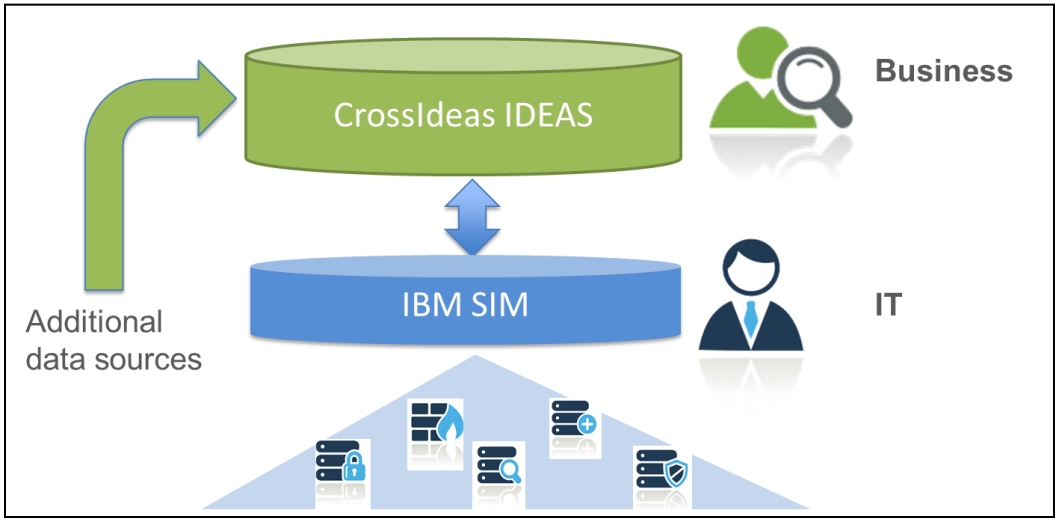
- Improved Identity Service Center user interface for business managers and end users
- Customer sponsored enhancement requests for improved consumability and compliance:
- Enhanced compliance and operational reporting with Cognos reporting additions and improvements

Extending ISIM for Broader Access Governance: CrossIdeas

NEW

CrossIdeas An IBM Company

- "IDEAS" product
  - Strong attestation/ recertification and SoD capabilities, SAP specific controls, role modelling
  - Helps ISIM customers rapidly introduce Access Governance capabilities with no changes in their existing ISIM environment
- Enables Access Governance on top of ISIM infrastructure and data;
- Deployed and configured as an ordinary ISIM Adapter
  - Provides bidirectional synchronization between ISIM and IDEAS



IDEAS - modular solution built on a single governance platform

NEW

Auditors, CRO

Business Managers

IT Security

- **Access review: Business friendly certification campaign**
  - Business User access review perspective
  - User conflict (SOD) violations perspective
- **Advanced segregation of duties Management**
  - Both general/Enterprise and SAP-specific
  - SoD Rules with out of the box templates
- **Role management - discovery and cleansing**
  - Visual maps and cost driven analysis

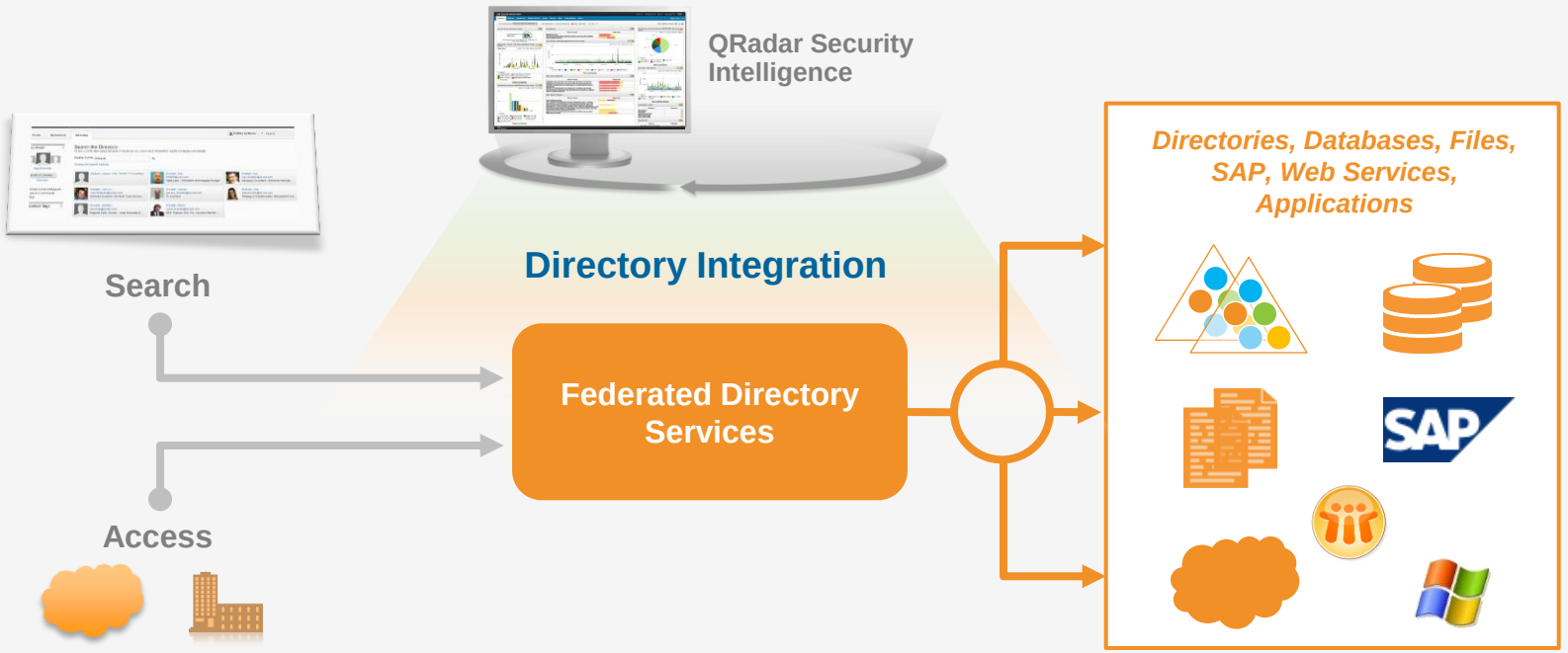
Customer Value

- Business-driven approach to Identity and Access Governance
- Integral part of an organization's compliance and risk strategy
- Extends ISIM via out-of-box standard adapter integration

Unite Identity Silos with Federated Directory Services

Support secure business expansion

Simplify cloud integrations and identity silos



Universal directory to transform identity silos to support disparate identity sources

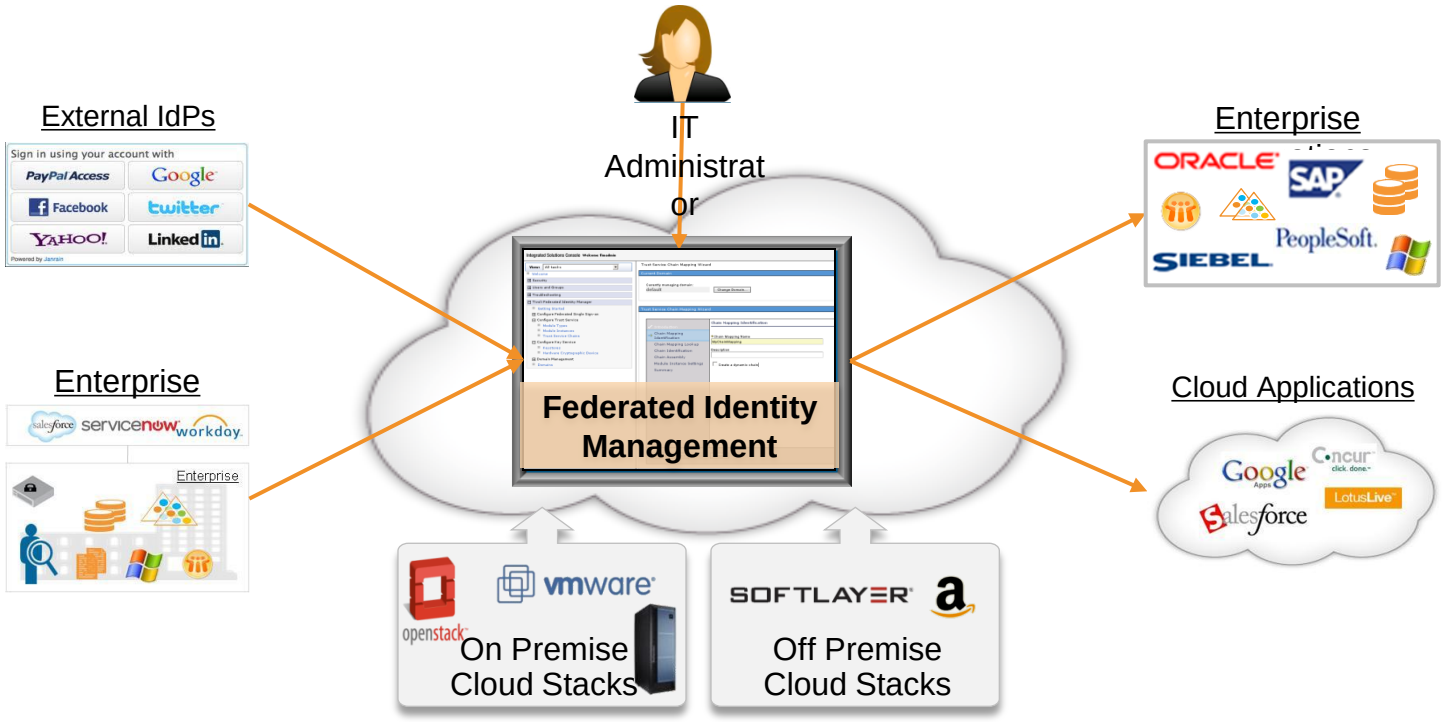
Scalable directory backbone leveraging existing infrastructure for enterprise-wide Identity and Access Management

Sourcing of identities and attributes for enterprise applications, Cloud/SaaS integrations leveraging open standards.

In-depth user insight with reporting and SIEM integration

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

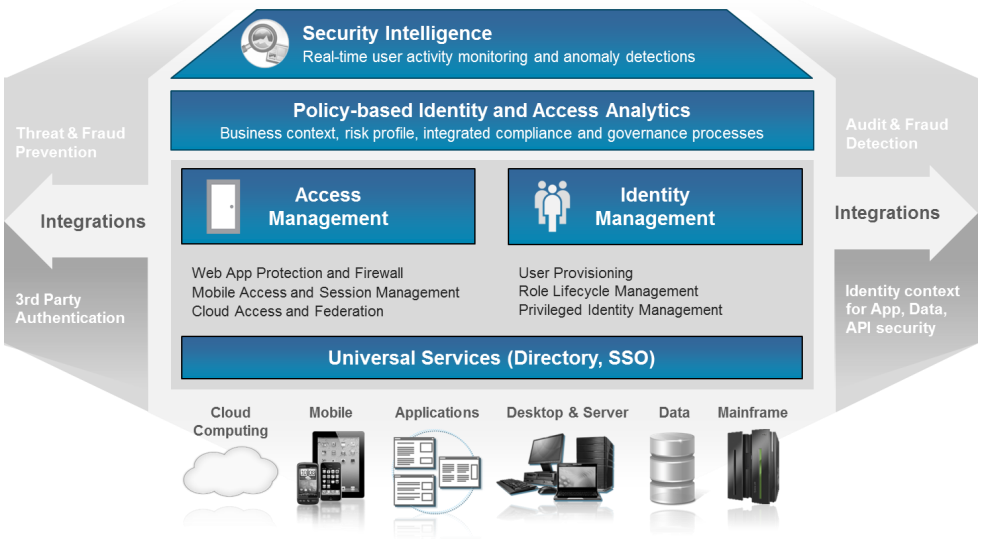
Simplify cloud integrations and identity silos



- **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 and RACF PassTickets

Customers seeking flexible delivery models to deploy and manage IBM Identity and Access Management

IBM Security Identity and Access Management



Lighthouse cloud-hosted IAM combines the power of enterprise IAM with the ease, lower cost, and agility of cloud

Lower the Total Cost of Ownership

Dramatically **lower ownership costs** by eliminating CapEx and OpEx costs (e.g., HW / SW deployment, upgrades, maintenance) associated with traditional IAM deployments

Expedite Deployment

Significantly quicker start-up and **faster-time to value** through use of innovative automation technologies and elimination of traditional infrastructure deployment

Improve Agility and Flexibility

Scalable cloud IAM platform with the agility to "turn-on" and utilize additional services as they become necessary, without the need to source new solutions

Reduce Skills Requirements

Simple administration that reduces the need for clients to acquire, train, and retain specialized security skills

Lighthouse Security Group Key Client References and Benefits

Automotive	Finance	Healthcare	Education	Retail
▪ Business enabler for driving revenue ▪ 8+ million users ▪ Enterprise, B2B, and B2C	▪ Enable secure business collaboration ▪ Simple consumer registration and self-service	▪ Improve user experience and efficiency ▪ Secure access to SaaS applications	▪ Secure access to internal and SaaS apps ▪ Rapid on-boarding / off-boarding for dynamic user base	▪ Migration of on-prem IAM to cloud ▪ Lower TCO and reduced need for specialized security skills

New Cloud SSO Service on IBM BlueMix Cloud Platform

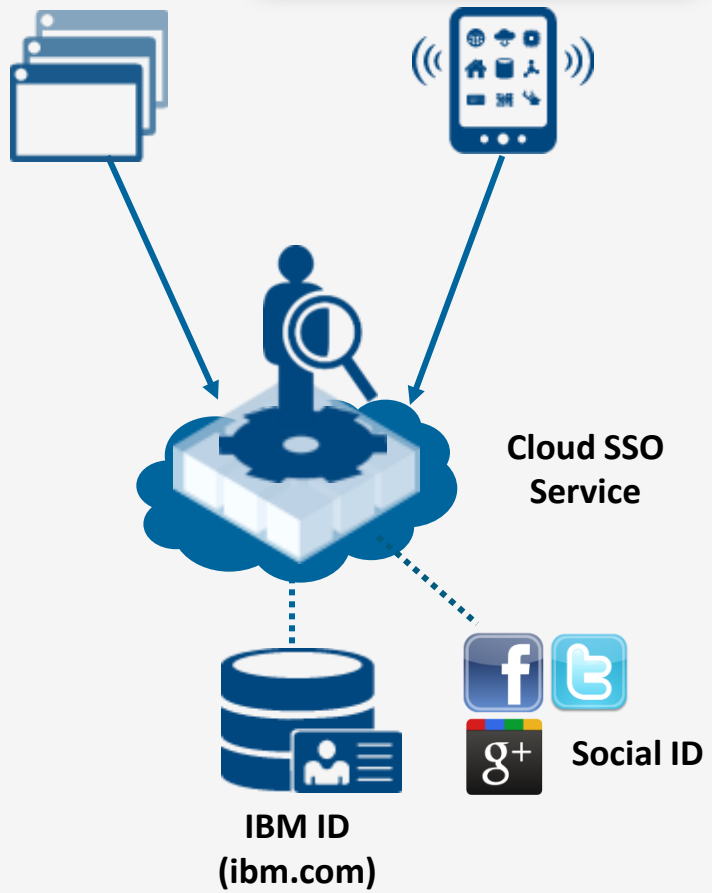
Easily add user authentication and single sign into applications

BETA

Safeguard mobile, cloud, and social access

Allows developers to add access security for web and mobile apps 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**



Summary: IBM Threat-aware Identity and Access Management

Safeguard mobile, cloud and social access	Prevent advanced insider threats	Simplify cloud integrations and identity silos	Deliver actionable identity intelligence
			
Access Manager for Mobile	Privileged Identity Manager	Federated Identity Manager	Identity Manager
Access Manager for Web	Access Manager for ESSO	Directory Integrator & Server	CrossIdeas

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