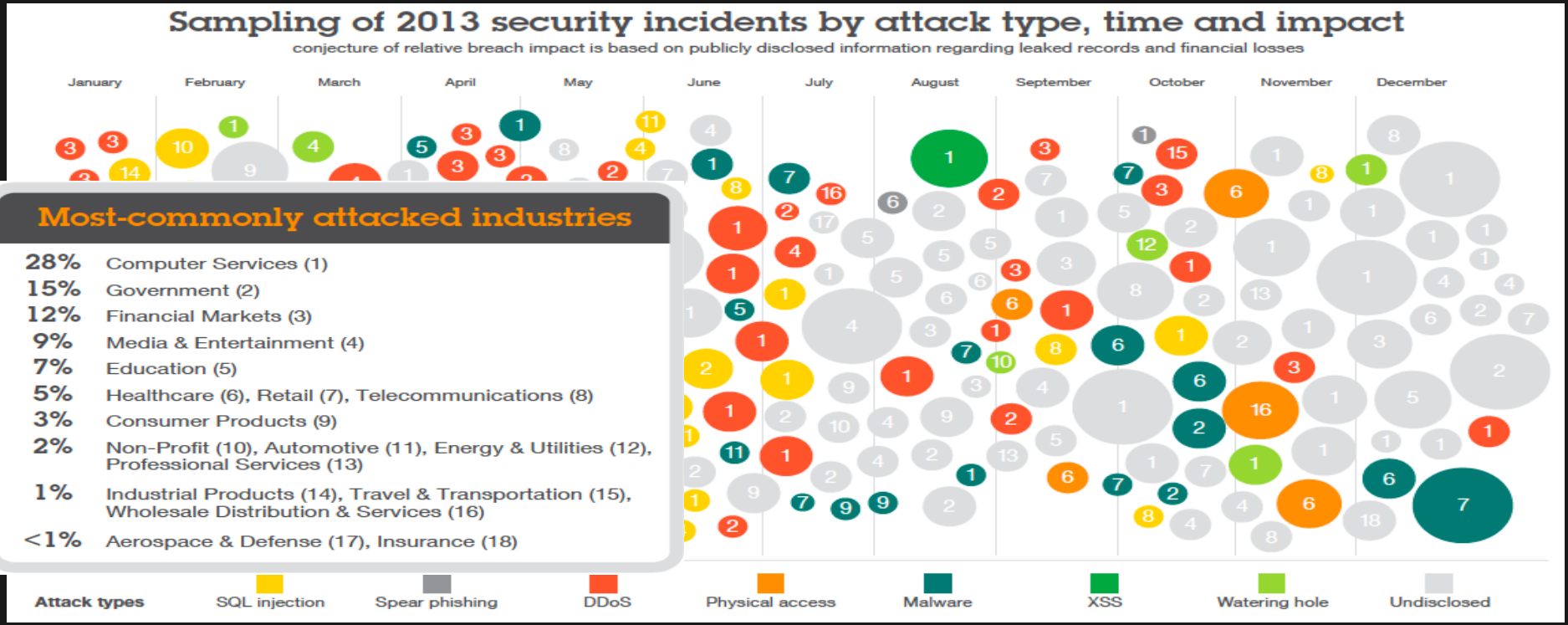
SolutionsConnect
A New Era of Smart

Threat-Aware Identity and Access Management

Glen Gooding
AP Security Business Leader, IBM Security Systems

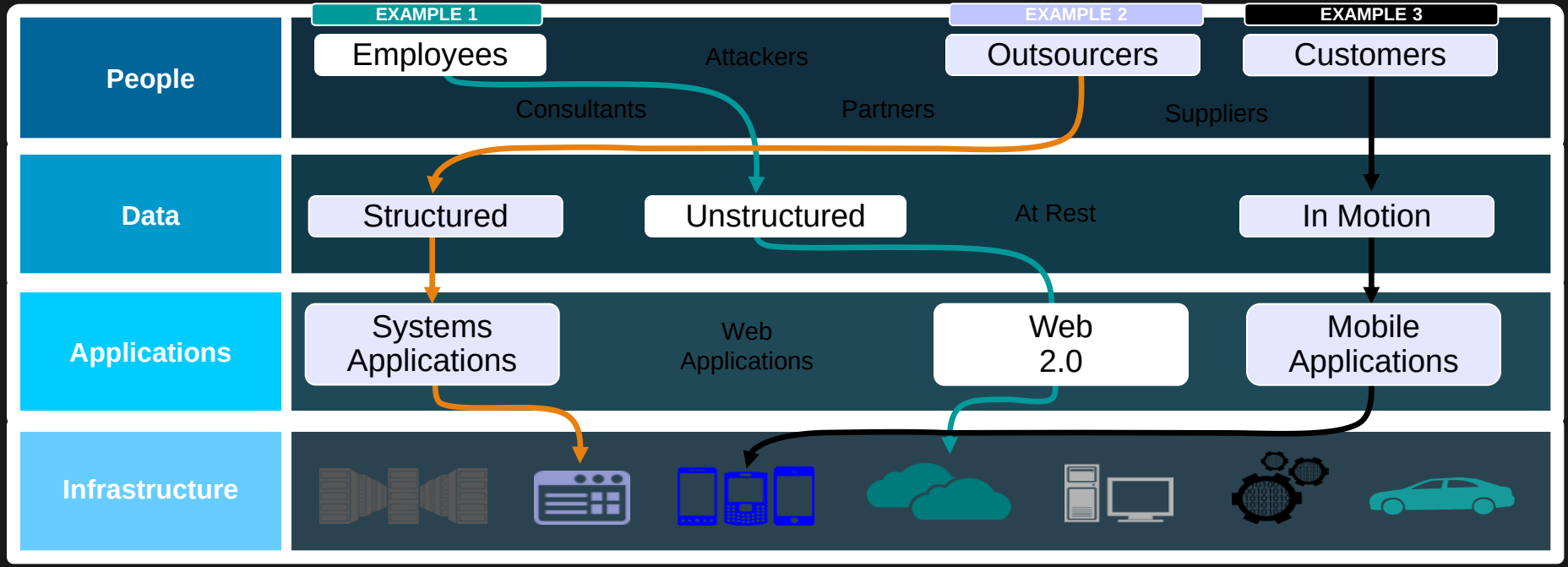
@gg00ding

X-Force Research: Attackers are taking advantage of the human factor



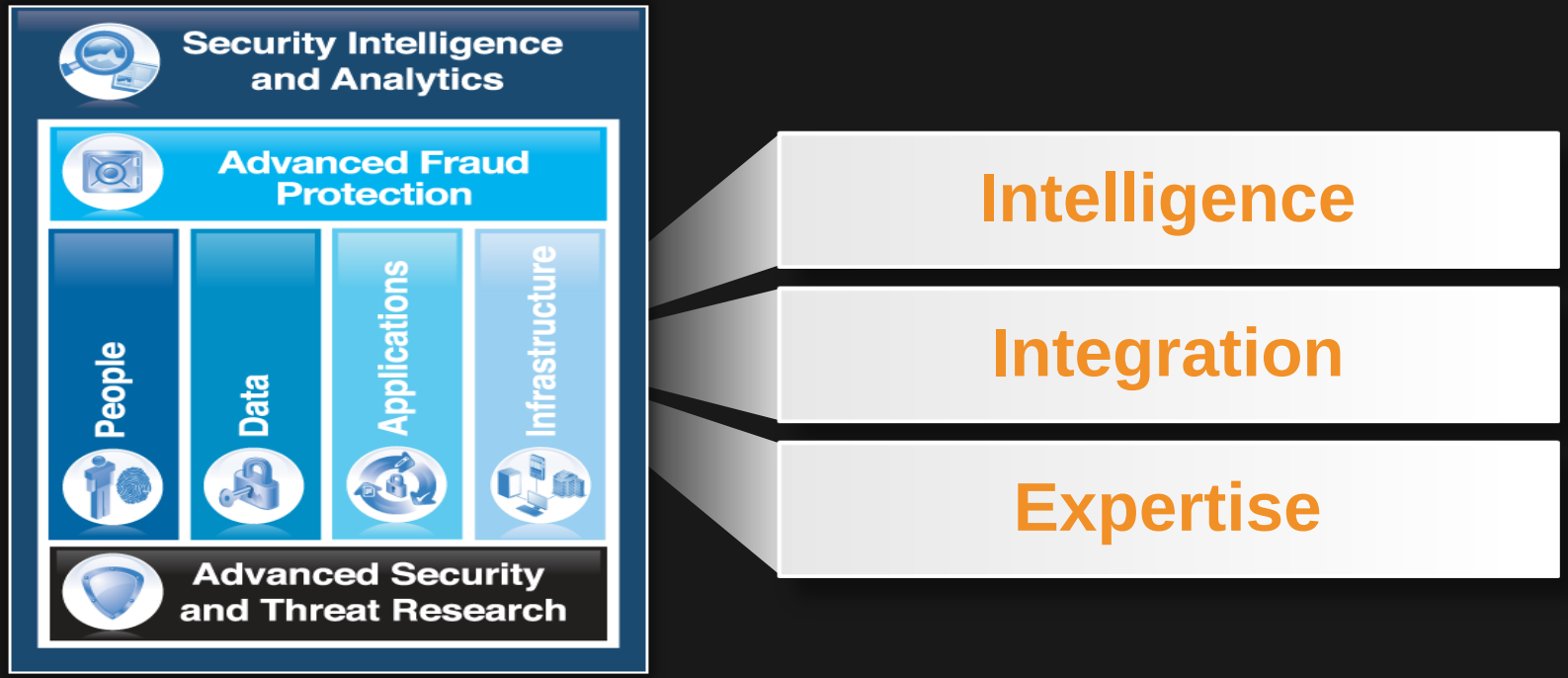
Source: IBM X-Force® Research 2013 Trend and Risk Report

Defining the security perimeter is increasingly difficult…



- **Complexity** stems from **interactions** that spread across People, Data, Application and Infrastructure security domains
- Defense approach is shifting from “Secure the perimeter” to ‘**Thinking like an attacker**’

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework



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	Infrastructure: 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

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

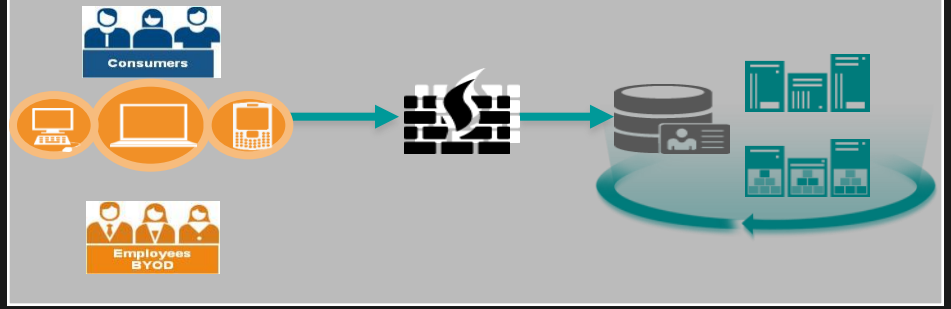
Source: IBM X-Force® Research 2013 Trend and Risk Report

Fundamental Shift around Identity & Access Management

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

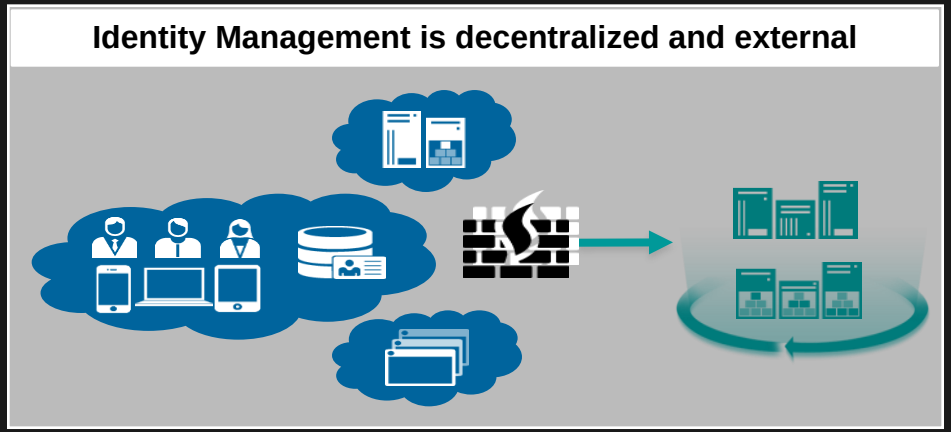
The Current Enterprise

Identity Management is centralized and internal



The New Hybrid Enterprise

Identity Management is decentralized and external



Administration

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

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

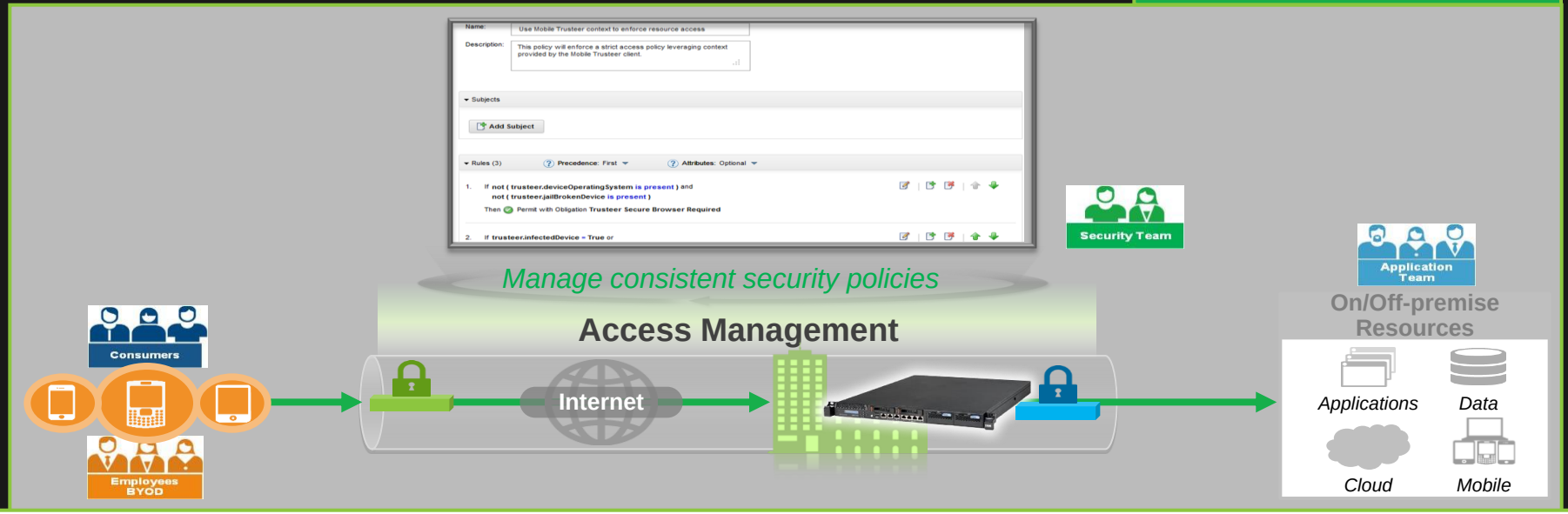
- **Enable identity management** for the line of business
- **Enhance user activity monitoring** and security intelligence across security domains

Simplify identity silos and cloud integrations

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

Leverage a Graded Trust Model to Achieve Secure Transaction

Safeguard mobile, cloud and social interactions



Identity-aware application access on the mobile device

Strong Authentication, m**obile SSO, session management** for secure user interactions

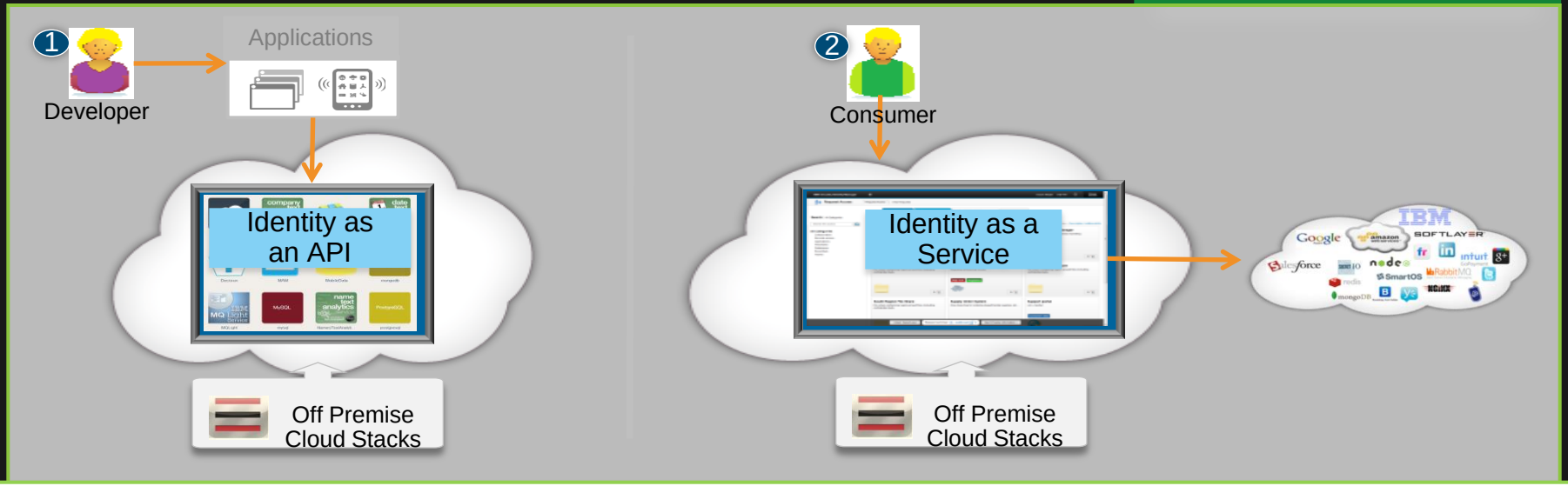
Context-based access and stronger assurance for transactions

Transparently enforce security policies for mobile applications

Enforce security polices **without modifying the applications**

Evaluate and prioritize scenarios for Identity as a Service (From the Cloud)

Safeguard mobile, cloud and social interactions



Offer open standards-based Login and SSO as an API for new application development

Enable policy-based multi-factor authentication (i.e. Password, OTP, certificate)

Ability to support Reporting and Analytics for audit and compliance

Launch Self-service and Single Sign-On to enterprise, SaaS & personal applications

User on/off boarding - Enterprise directory integration, Integration with social identity providers (BYO-Id)

Ability to support Access certification to enterprise and Cloud/SaaS applications

Securing mobile identities

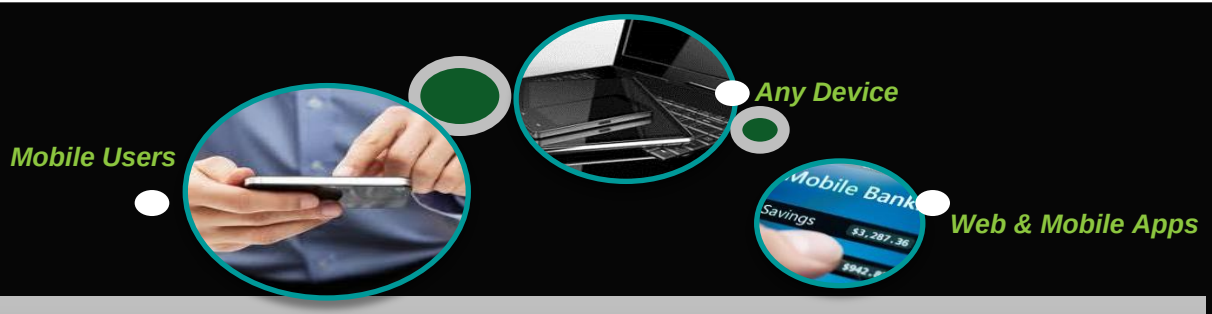
An international banking organization targeting mobile user access for employees and end users

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

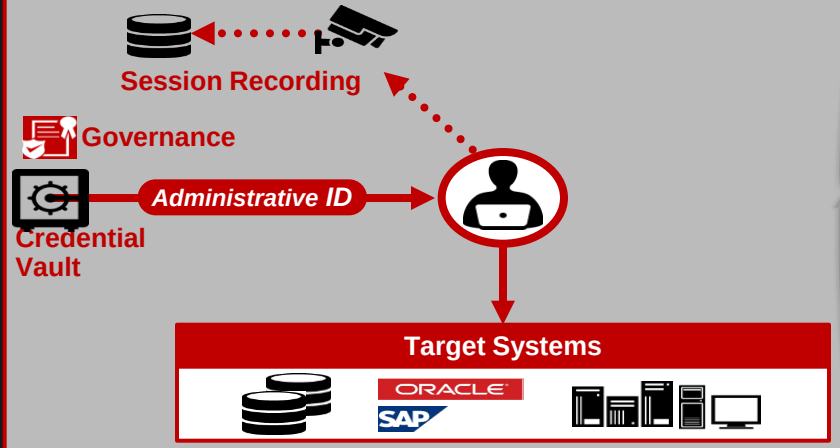
- Secure employees and contractors access to web and mobile apps
- Rollout new mobile apps; ensure end user access from mobile devices
- Eliminate passwords as a weak link to enforce access to web and mobile

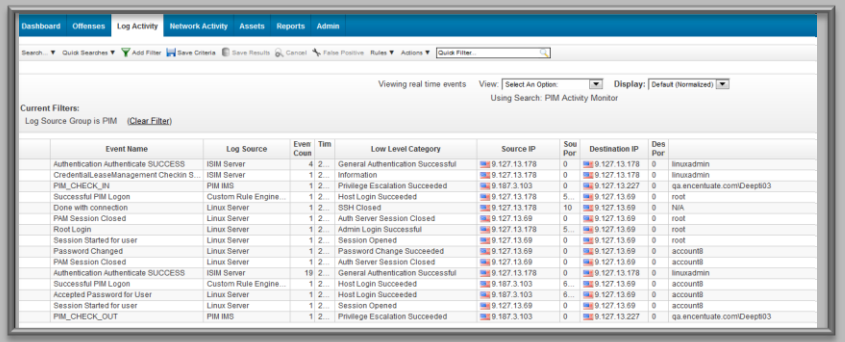
Solution benefits

- 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

Address Insider Threat with Privileged Identity Management

Prevent insider threat and identity fraud





Eliminate the need to share passwords for privileged users and shared accounts with automated privileged identity management

Ensure compliance and audit support with session recording and replay support

Leverage common Identity management and support for applications and resources

Strong authentication controls and SSO for high-risk account access

Audit privileged user activity and sensitive data access

Address **compliance, regulatory and privacy** requirements

Secure user access and content against targeted attacks

Leading provider of information technology, consulting, and business process outsourcing services

Integrated solution to safeguard privileged ID's:

Prevent insider threat and identity fraud

500
privileged administrator users

Business challenge

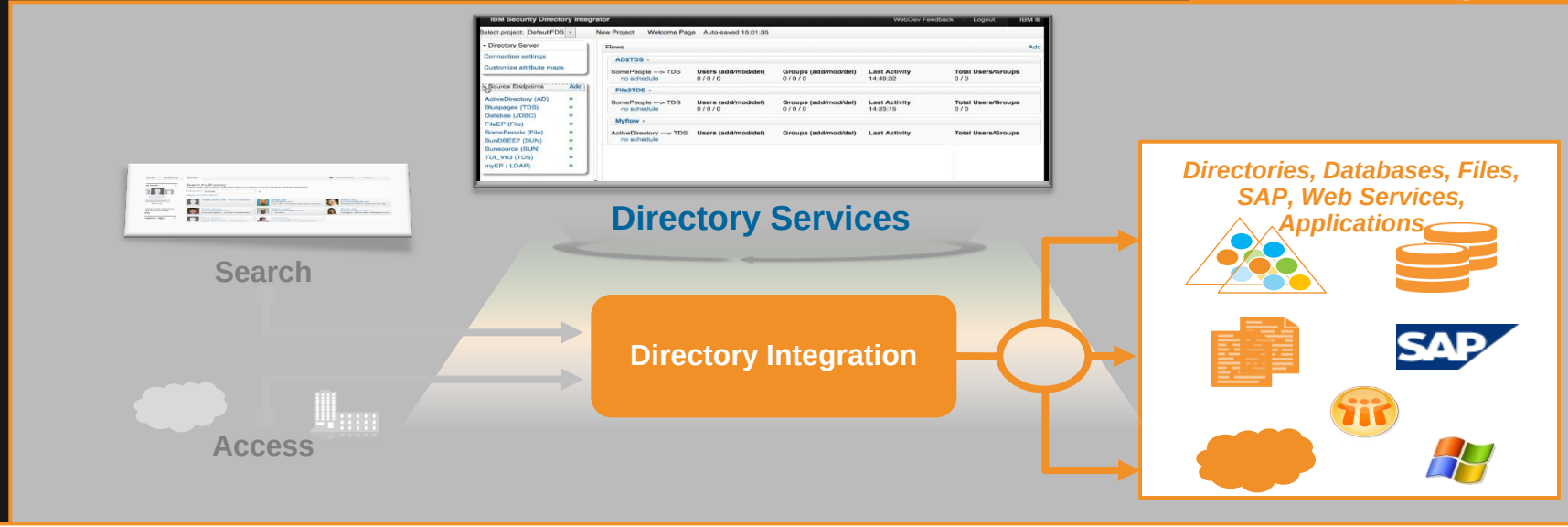
- Increased security risks as a result of limited privileged activity monitoring
- Exposure to the insider threat due to enterprise-wide use of shared privileged IDs
- Audit and Compliance issues: Poor privileged user management and lack of audit trail for privileged user access

Solution benefits

- Streamlined and automated privileged user management
- Audit trail and monitoring of privileged access to all critical systems
- Secure management of shared privileged IDs and their passwords
- Full support of periodic privileged access recertification for audit and compliance purposes

“Untangle” Identity Silos to Support Business Expansion

Simplify identity silos and cloud integrations



Universal directory to transform identity silos to support disparate identity sources

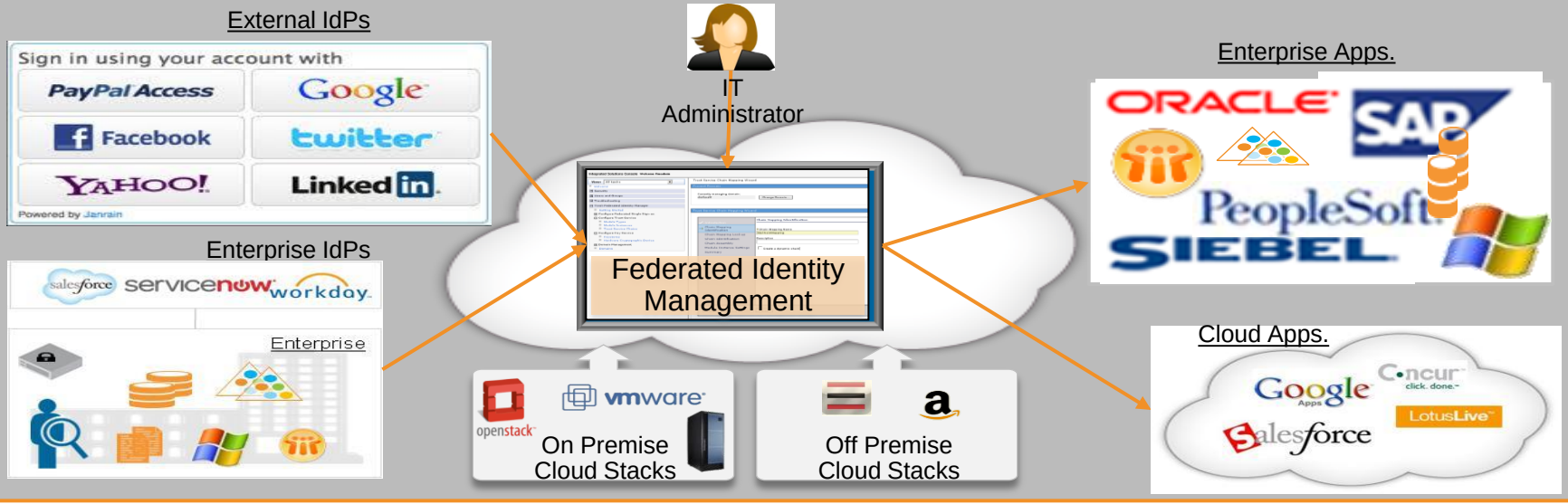
Scalable directory backbone leveraging existing infrastructure for enterprise-wide Identity and Access Management

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

In-depth user insight with reporting and SIEM integration

Leverage open standards from Enterprise to Cloud integrations

Simplify identity silos and cloud integrations



Support multiple deployment patterns (private, hybrid); Managed services

Ability to integrate with Enterprise Identity repositories and external IDs (e.g. Social)

Federated SSO to Enterprise and Cloud /SaaS Applications

Custom integrations by levering business meta-data in an enterprise (e.g. SCIM, STS)

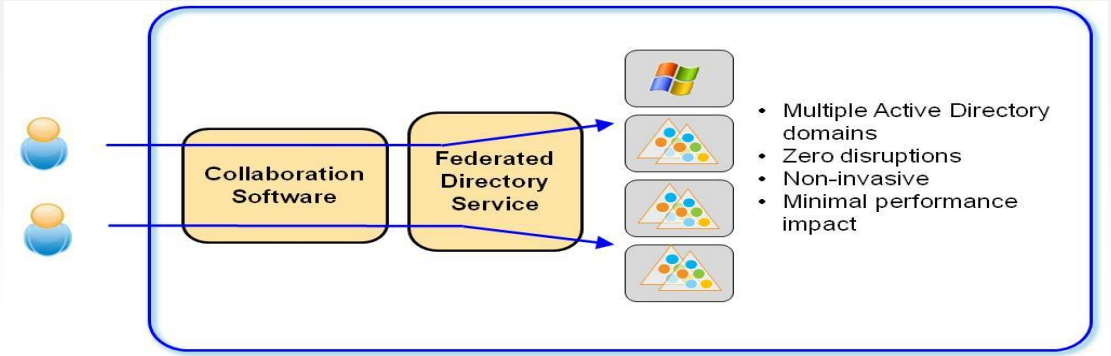
Directory Services to help Distributed Collaboration

Government entity to grow quickly to 800K application users

Simplify identity silos and cloud integrations

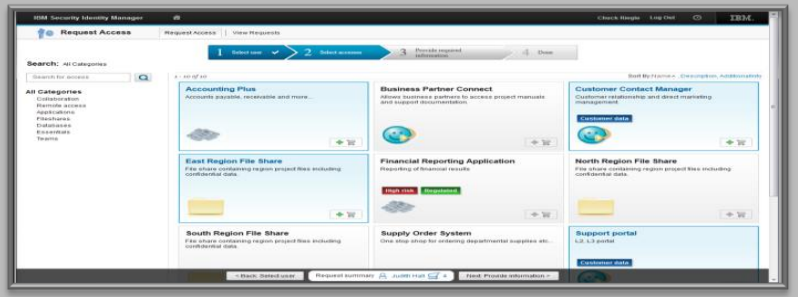
Improved solution design and integration allowed the environment to grow from 40,000 users to

800,000+users



Deliver Business Driven Compliance with Identity Management

Deliver intelligent identity and access assurance



Identity Management

HR Systems/Identity Stores

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

Detect and Correct Local Privilege Settings

Risk Based Access

On/Off-premise Resources

Applications *Data* *Cloud* *Mobile* *Devices*

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

Driving an intelligent Identity and Access Assurance program

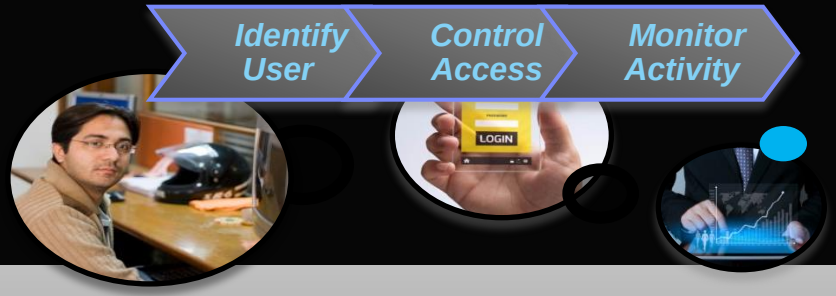
Large paint company servicing customers in over 65 countries.

Deliver intelligent identity and access assurance

Governing user access and compliance in 17 operating countries

8,500 Employees, interns, contractors, and privileged administrators

25,000 Business partners and services providers



Business challenge

- Manage the rising IT risks and cost from manual provisioning and changing access to 40+ applications, 50+ databases, 300+ servers, 200+ network and security devices
- Demonstrate compliance in different countries with central auditing and reporting
- Govern privileged administrator shared access and audit

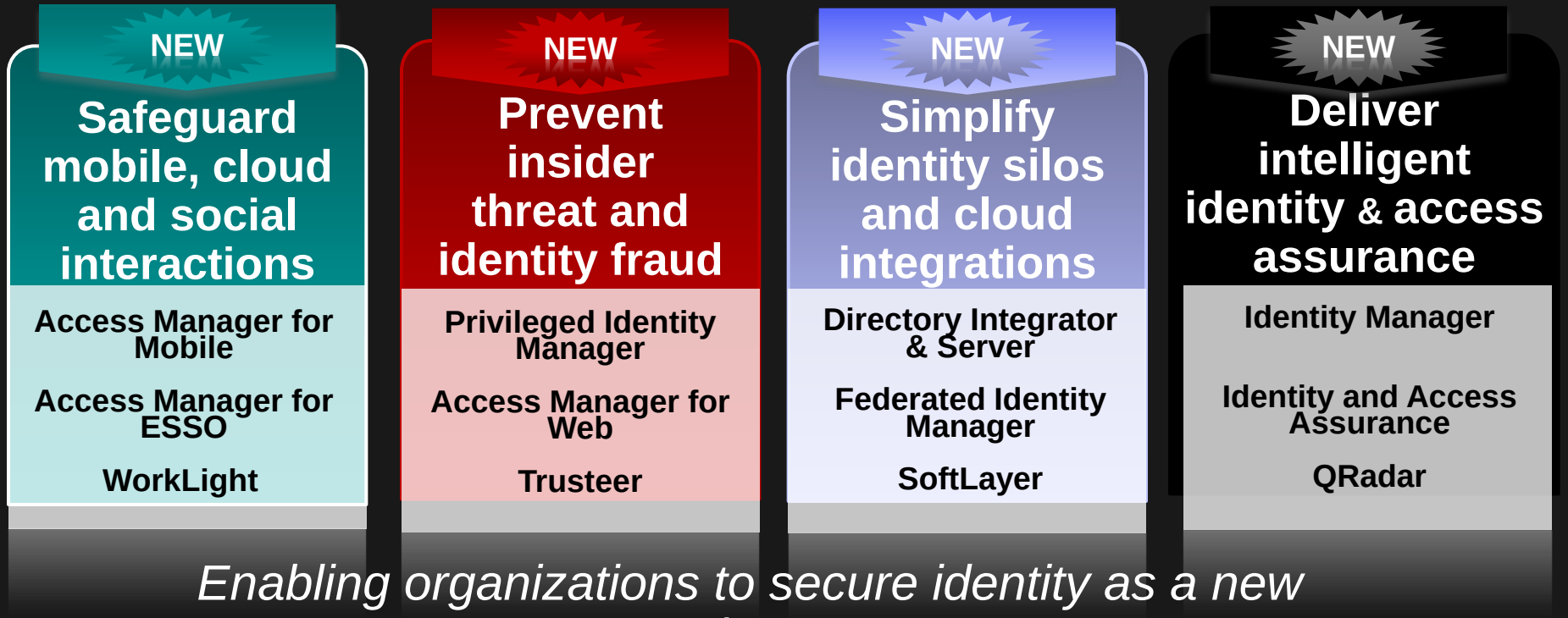
Solution benefits

- Reduced help-desk costs while enhancing governance and visibility of all internal and external user access consistently
- Provided zero-day and zero-based provisioning with federated access to resources
- Robust technology with integration capabilities across diverse applications and IT services (SAP, Portal, Informatica, Microsoft, WebMethods, WebSphere, and Oracle)

Adopt a maturity model to transform IAM program

Optimized	**Security Intelligence:** User activity monitoring, Anomaly detection, Identity Analytics & Reporting				
	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**

Introducing IBM Threat-Aware Identity and Access Management



Enabling organizations to secure identity as a new perimeter
with Threat-aware Identity and Access Management