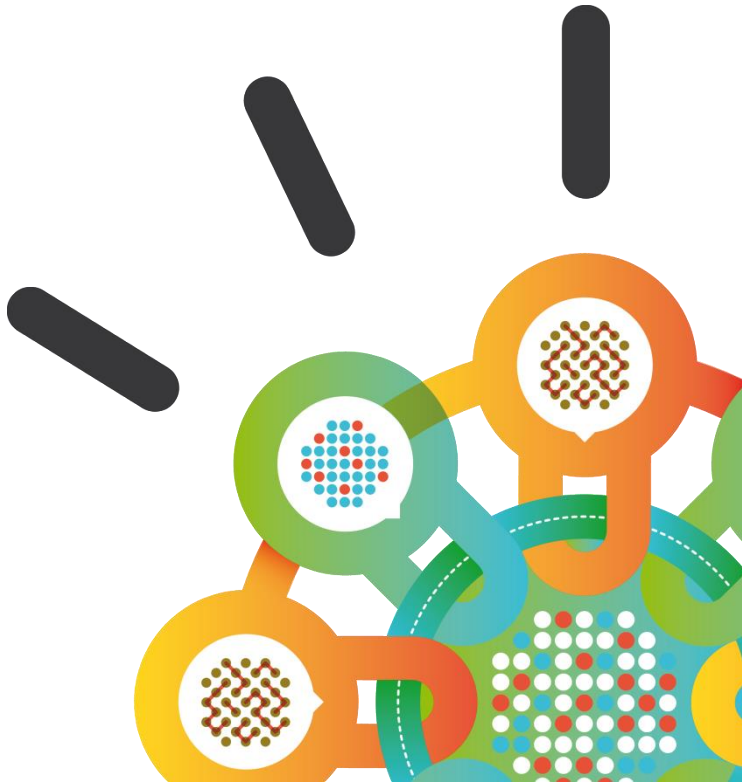
Security Intelligence.
Think Integrated.

Protect Your Organization from Your Biggest Threat – Insiders

Identity & Access Management

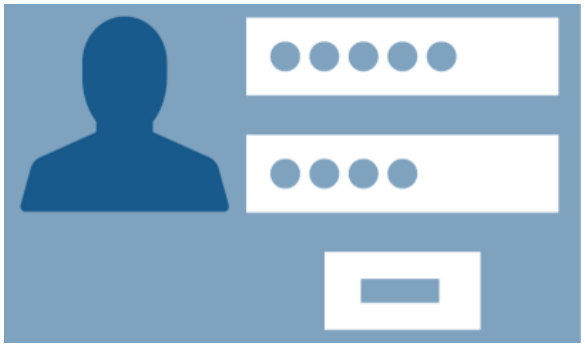
Brandon Whichard
Product Marketing
IBM Security

October 5, 2015



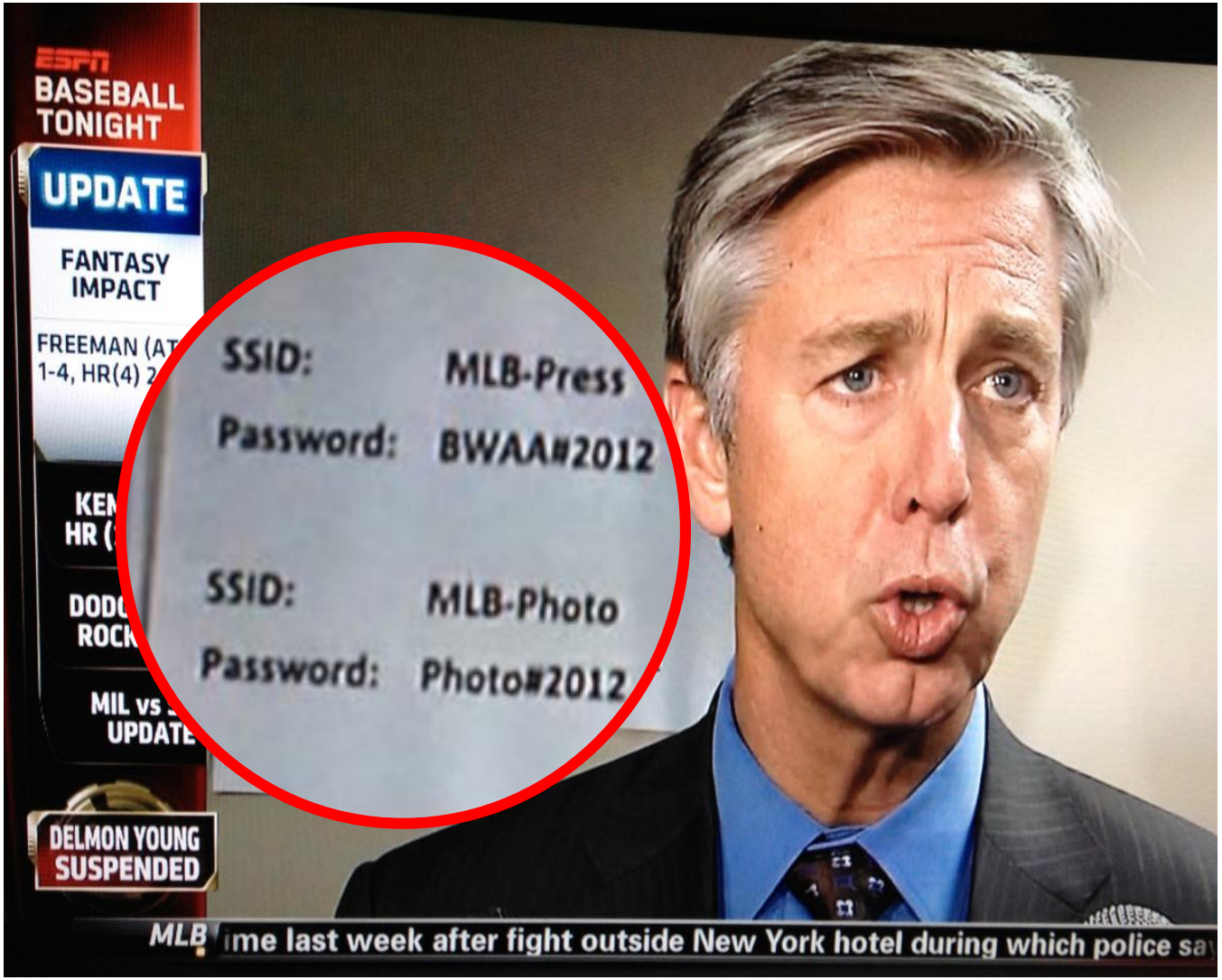
How are credentials compromised?

Usernames and Passwords will be stolen



Phishing

What's wrong with this picture?



Identity and Access Management

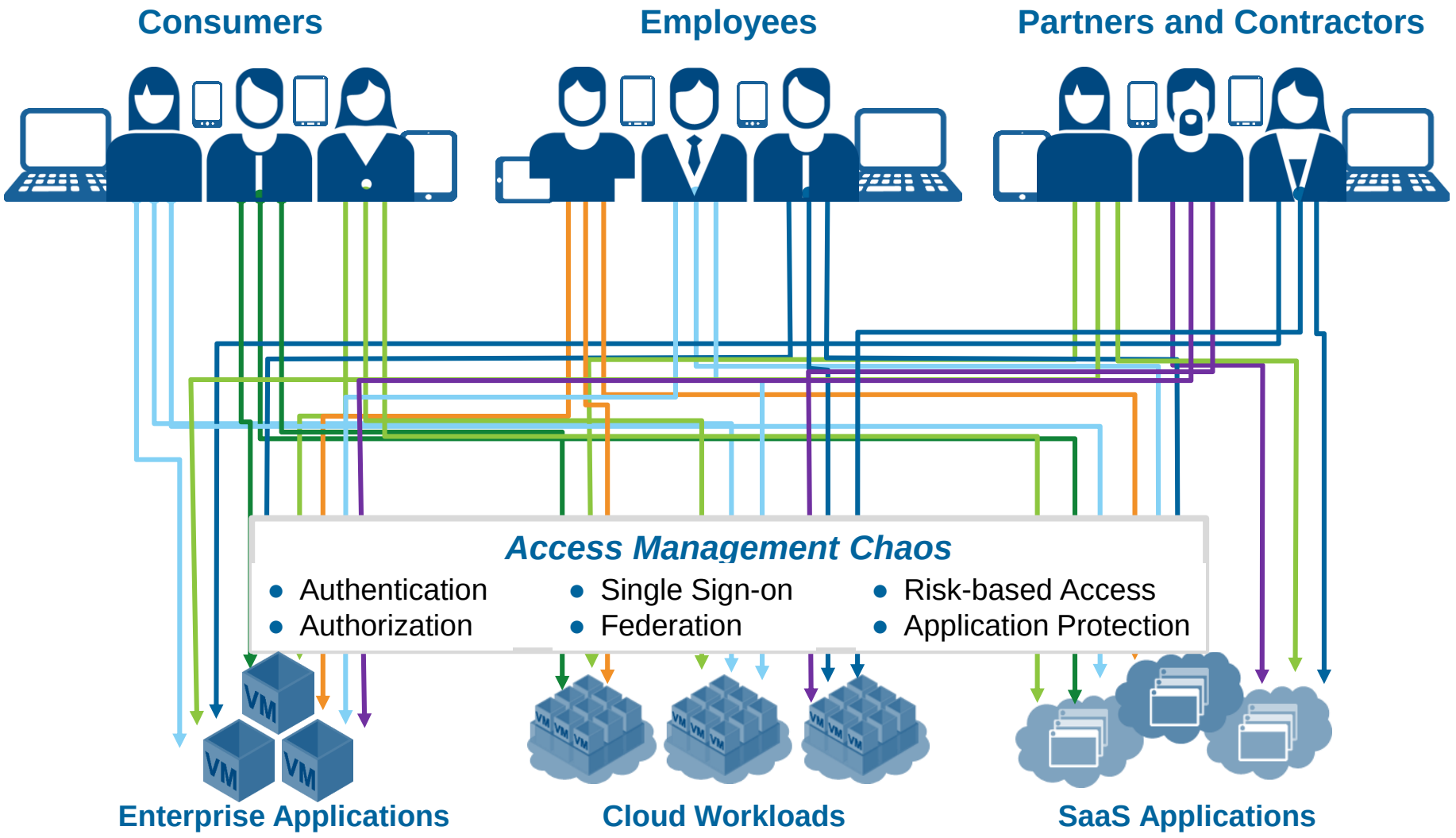
Govern and administer users and their access

<Identity Management>
Control unauthorized access and prevent "entitlement creep"

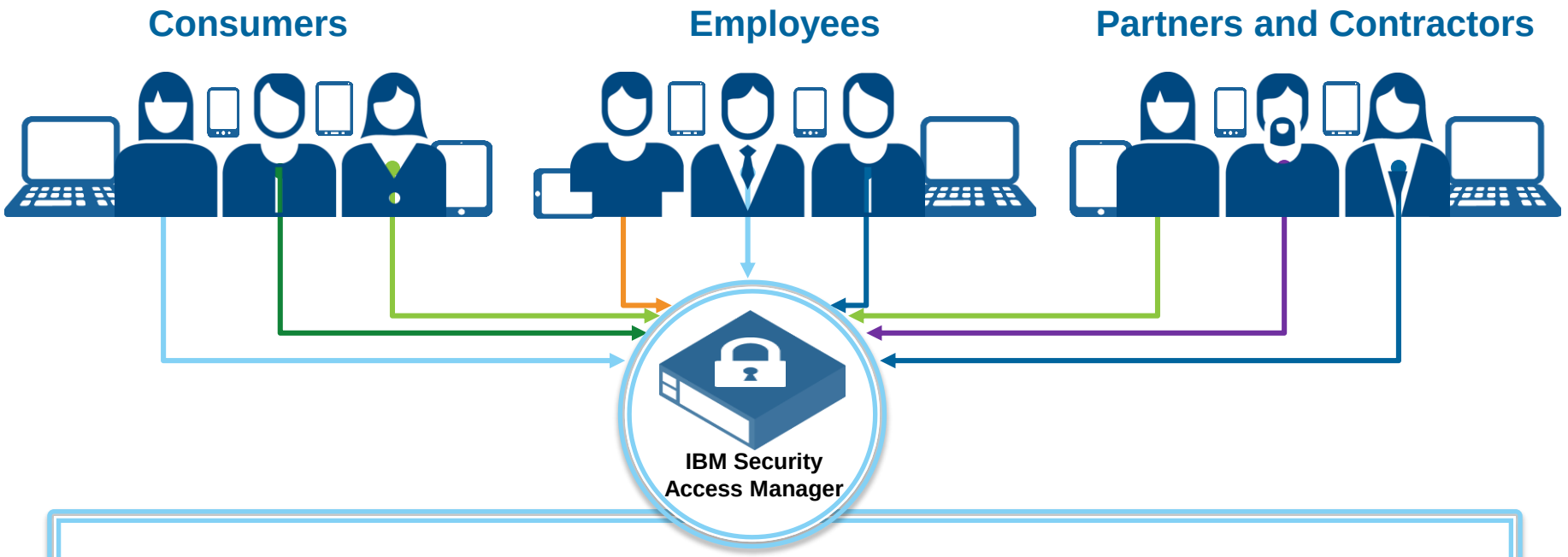
<Access Management>
Validate "who is who" across the enterprise and the cloud

1. ***Is this really a valid user?***
2. ***What does the user want to do?***
3. ***What access does that user need to do their job?***

Access Management environments are becoming highly fragmented and complex, making enterprises less secure

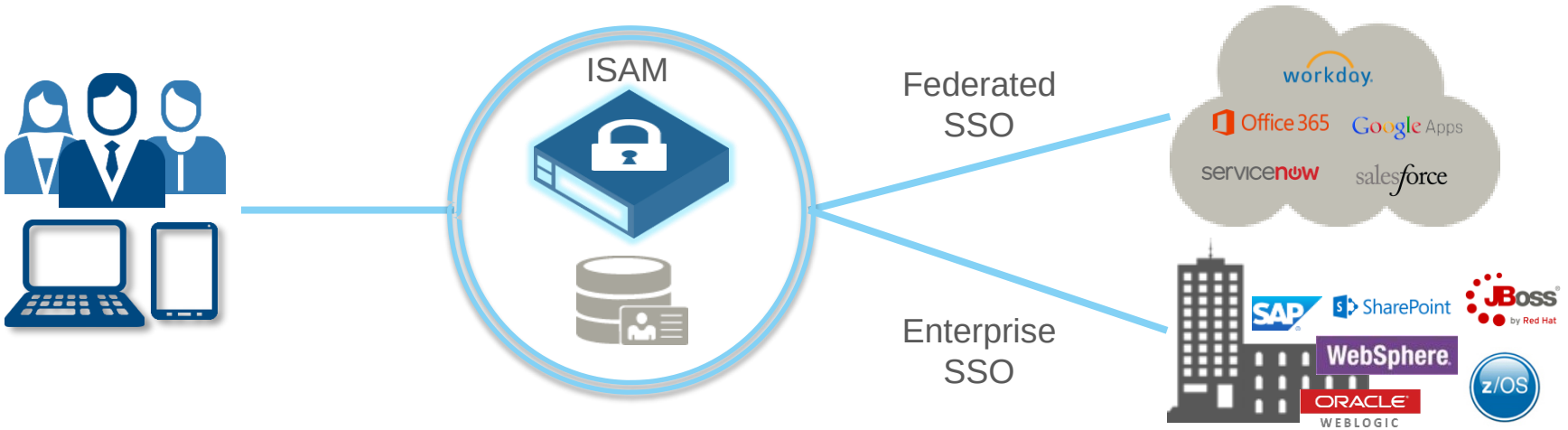


Take back control of Access Management



1. Manage access in the world of hybrid cloud

Enable SSO and identity federation to apps running inside & outside of the enterprise



- Quickly establish single sign-on connections to popular SaaS applications
- More easily create custom application connectors with Do-It-Yourself federations based on SAML 2.0 standard
- Deliver single sign-on to enterprise applications and support user identity propagation in hybrid cloud application interactions

2. Risk-aware access security for mobile apps and APIs

Transparently register mobile devices and enforce user-centric authentication policies

- Dynamically assess risk associated with mobile app access using contextual information about the device, user, environment, resource, and past user behavior
- Adaptive authentication improves mobile security posture while providing the least obtrusive end user experience
- Audit or block fraudulent and high-risk transactions from infected devices without modifying backend applications

CLIENT EXAMPLES

Risk-Based Access

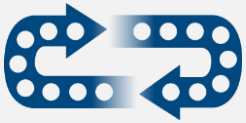
Large bank protects user access to apps from mobile and web channels for

Over 750K

users

Uses risk-based access, device registration and strong authentication

Performance & Scale



Large state agency needed to authenticate

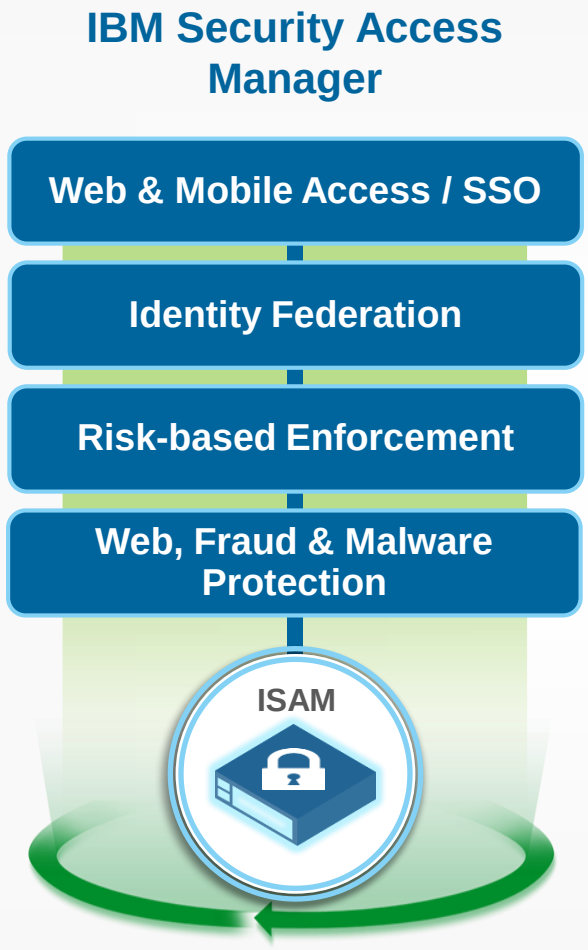
Over 10M

users

Major concern was to scale as user base grows and registrations increase

IBM Security Access Manager

Take back control of access management



- **Reduce TCO and time to value** with an modular “all-in-one” access appliance in virtual and hardware form factors
- **Deliver a multi-channel access gateway** to help secure employee and consumer access to mobile, web, APIs, and SaaS applications
- **Enforce identity- and risk-aware application access** for web and mobile devices
- **Secure identity assurance** with built-in mobile authentication service, one-time-password use
- **Deploy identity federation rapidly** using pre-integrated connectors to popular SaaS applications
- **Centrally manage policies** to protect enterprise from fraud and malware via Trusteer without modifying apps and risks associated with OWASP top 10 vulnerabilities
- **Deliver built-in integrations** with, MobileFirst Platform, MobileFirst Protect, Microsoft Office 365, SAP, Websphere and more

Identity and Access Management

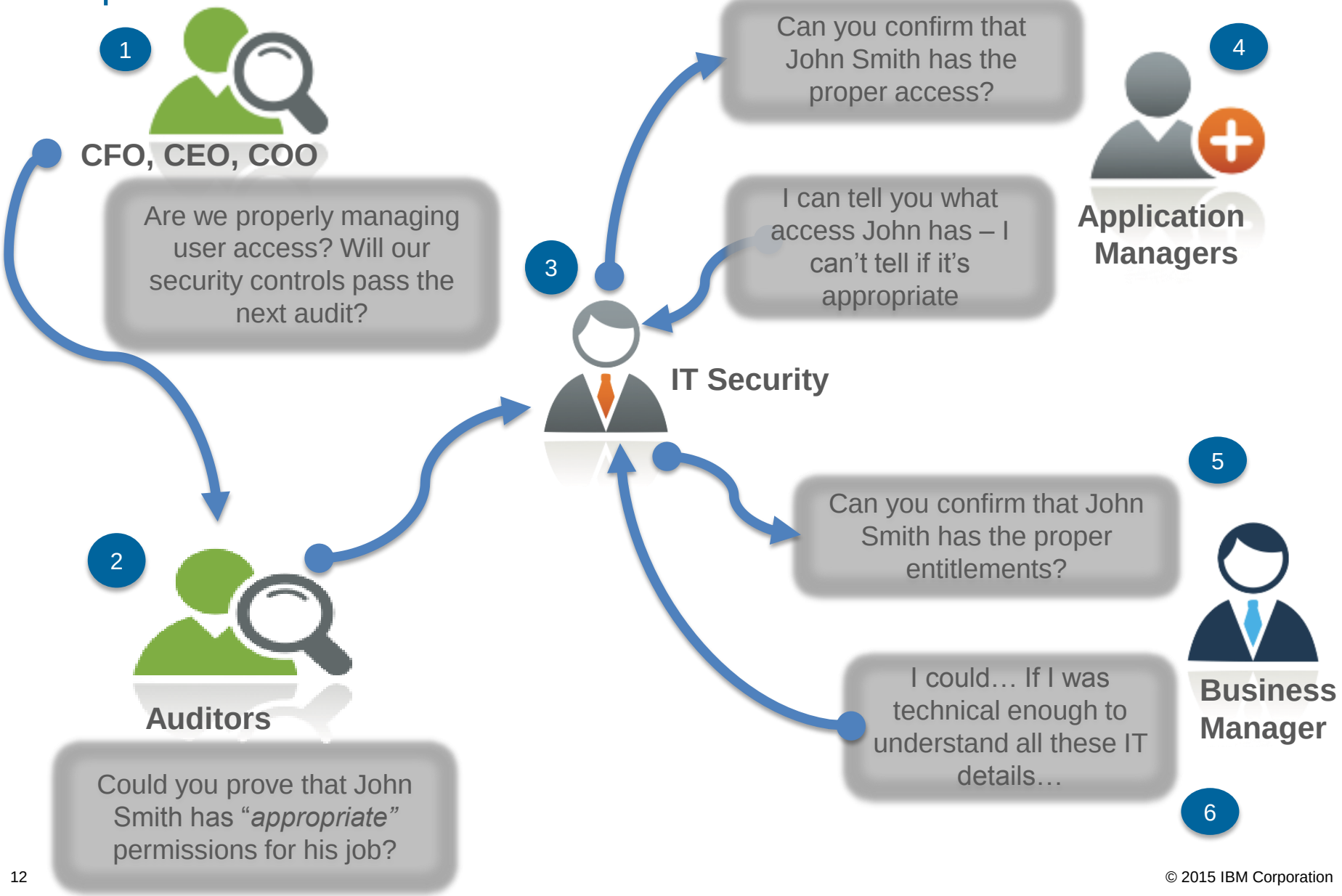
Govern and administer users and their access

<Identity Management>
Control unauthorized access and prevent "entitlement creep"

<Access Management>
Validate "who is who" across the enterprise and the cloud

1. ***Is this really a valid user?***
2. ***What does the user want to do?***
3. ***What access does that user need to do their job?***

The pain chain



The dependencies of traditional identity management

Business activities vs. Entitlements

Business Manager

Understands what **business activities** employees need

Requests employee IT entitlements from IT Security Manager

Which entitlements grant access to which business activities?

IT Security Manager

Provides information regarding who has which **entitlements**

Who SHOULD have which entitlements?

CRM	ERP
Mainframe	HR
Application Entitlements	

Auditor

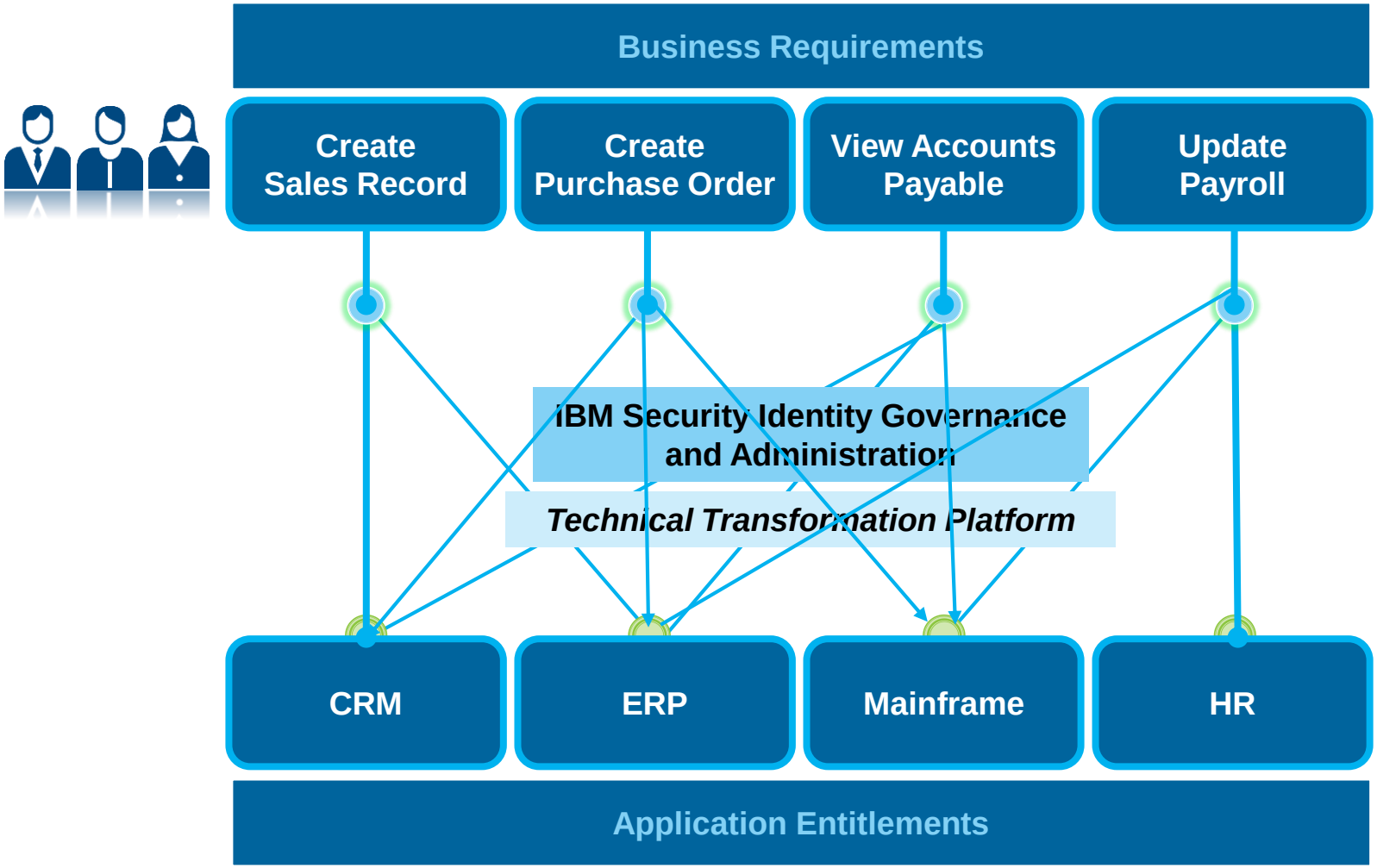
Identifies what **business activities** cause SoD violations *(toxic combinations)*

Receives list of entitlements based on IT Security Manager's request

Which entitlements cause toxic combinations?

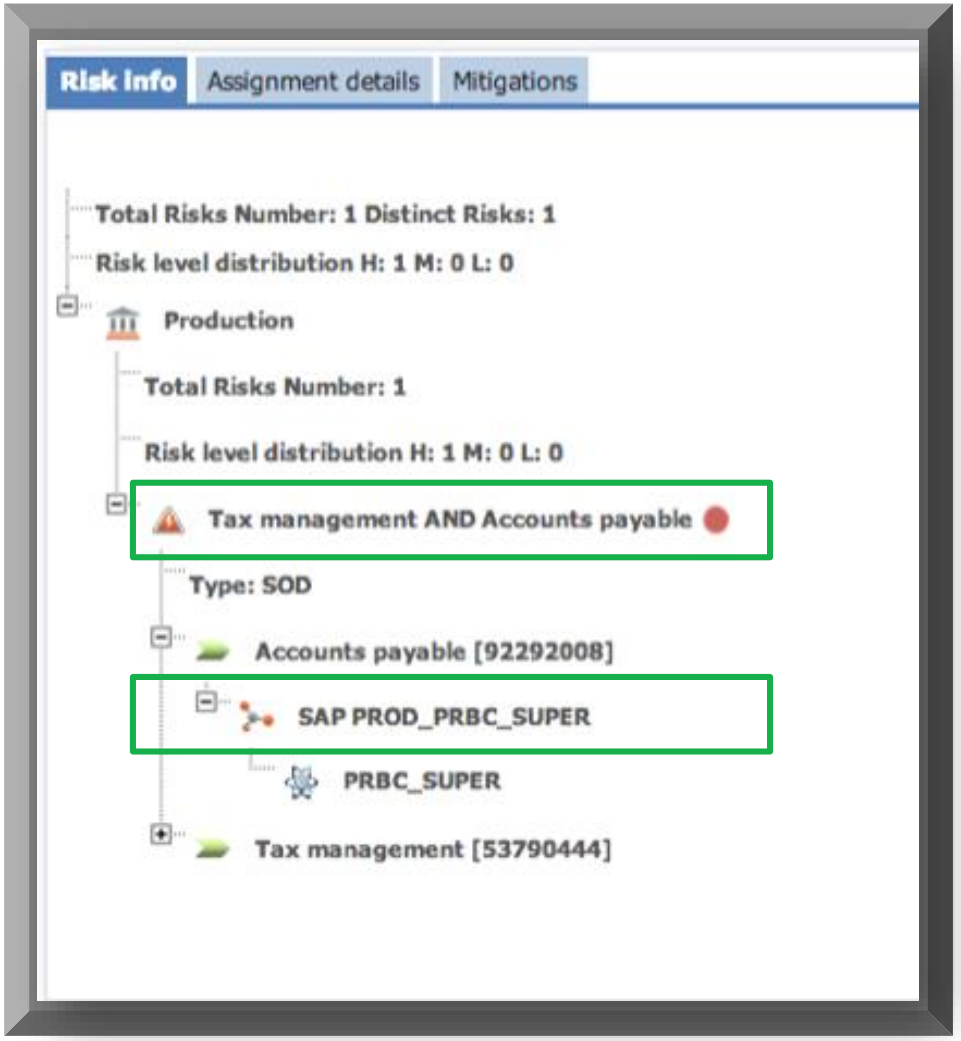
The IBM Security Identity Management Approach

Automatically map entitlements to Business activities



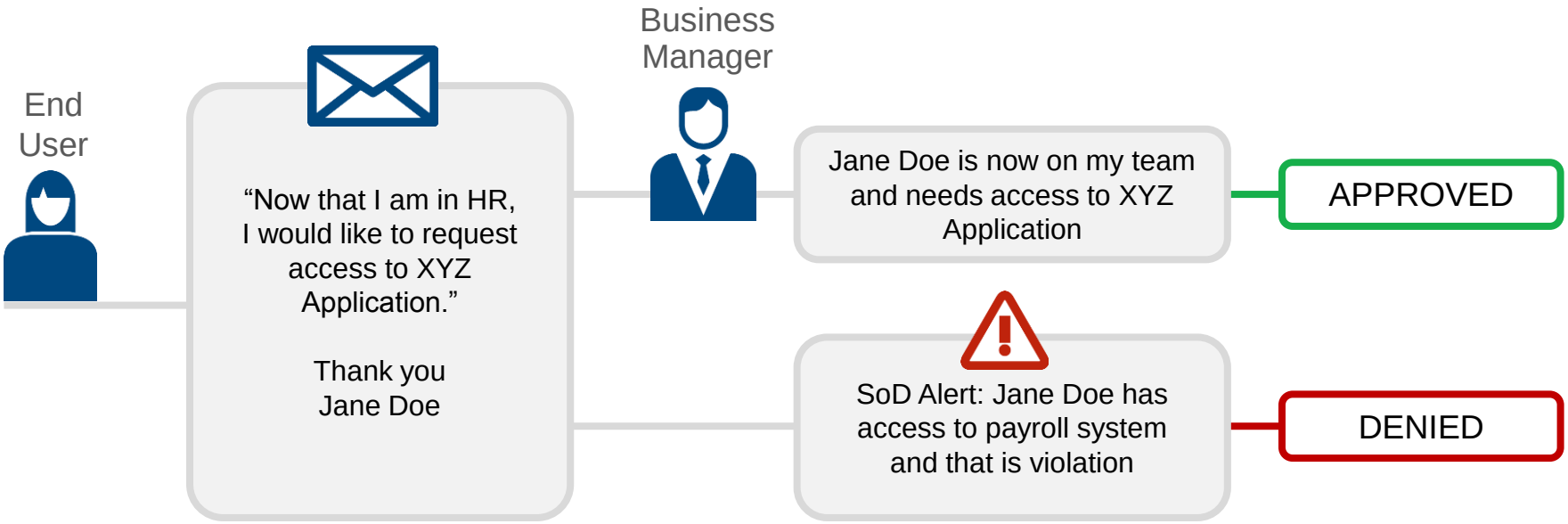
Simplified separation of duty modeling

- Auditors build rules from the top down starting with “Business Activity”
- IT maps the actual entitlements related to business activity
- Auditors may create, update and delete SoD rules without IT intervention
- IT can map new entitlements to business activities *one time*



1. Access request management

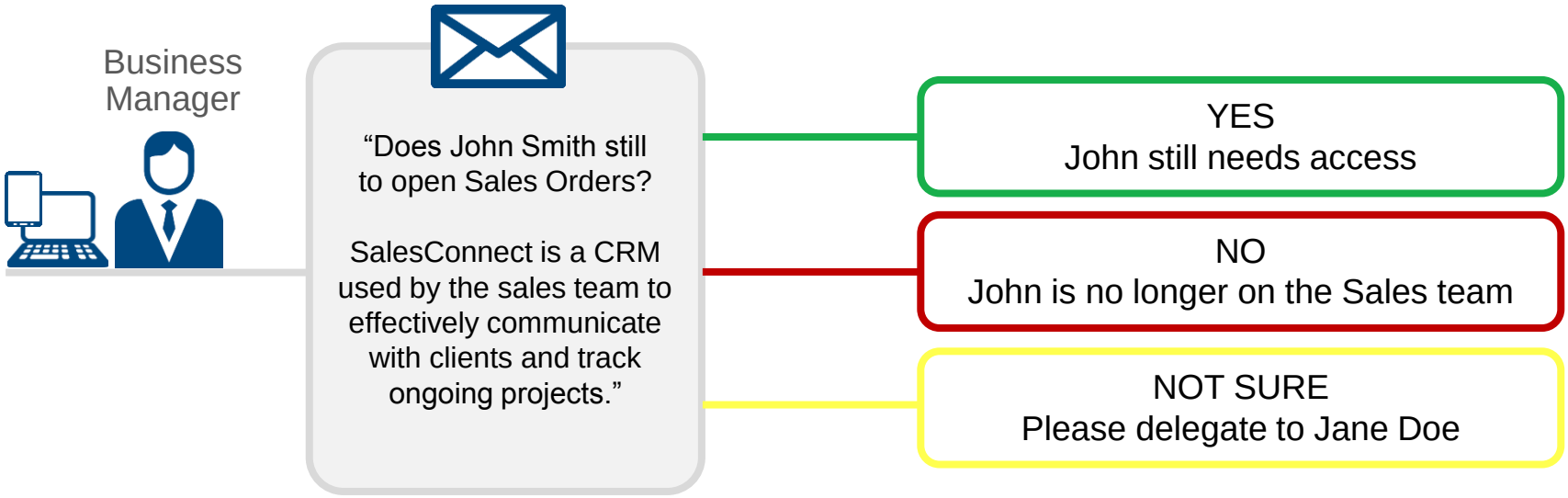
Allow users to quickly and effectively request their own access



- Self-service, shopping cart model
- Features multiple paradigms: business role, IT / application role, "Like Mike"
- Automatically alerts users when there is a separations of duties (SoD) conflict
- Saves time and money, while keeping the organization secure and compliant

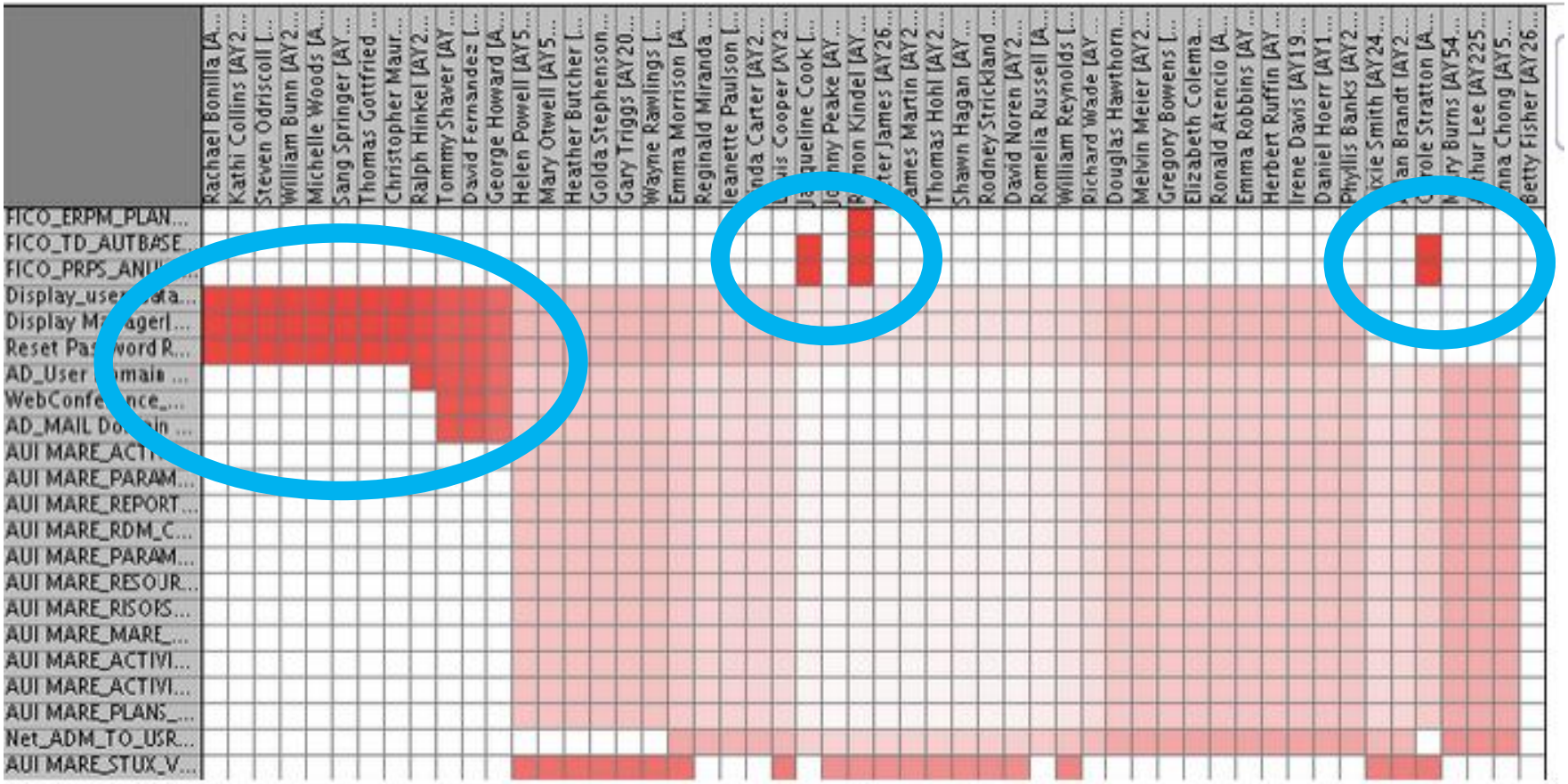
2. Access certification

Use business language to take quick and effective action regarding user access



- Focused, risk-driven campaigns
- Business language is used so the business manager can understand exactly what entitlements he is certifying and take the appropriate action
- Support business manager's decision making to certify user access

Identifying Outliers and Assessing Risk



Identity Governance and Administration Results

CLIENT EXAMPLES

Audit Access

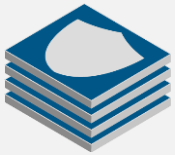
Large European designer found almost

80%

of users had unnecessary access

after leveraging the "last usage" information in their automated controls set

Governance



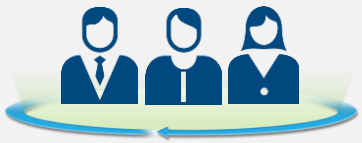
Large European insurance and financial services firm governs access to

75,000

employees, agents, privileged users

by identifying access risks, separation of duty and certify access for SAP, AD, mainframe, and custom-built apps

SoD Simplification



Multinational manufacturer manages over

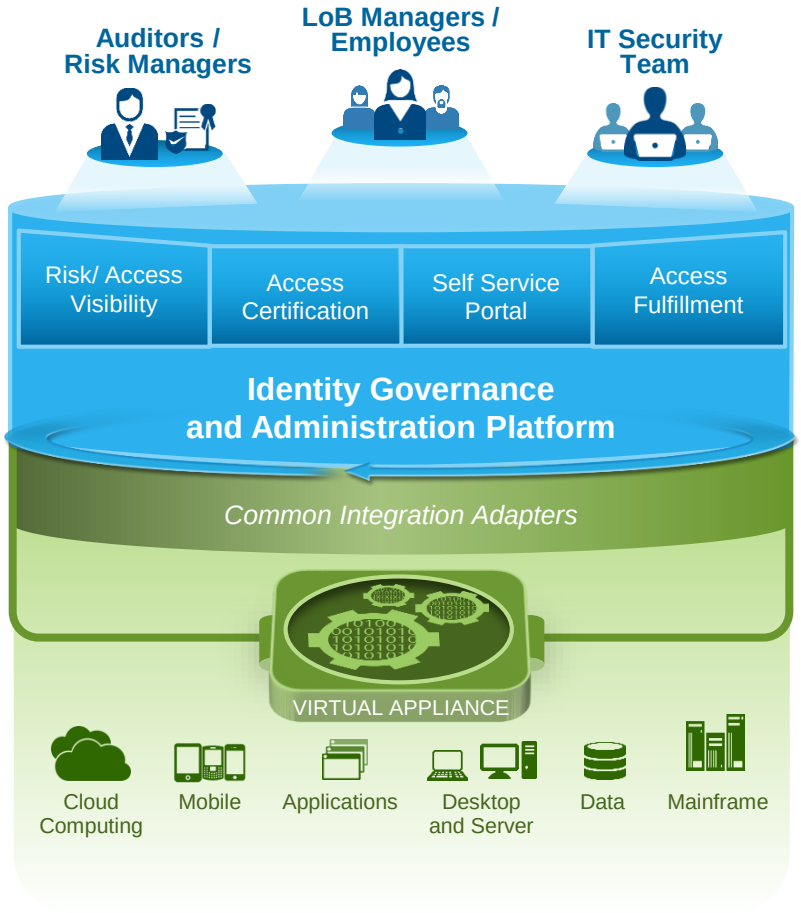
430M

entitlements

with only a few hundred separation of duty rules

Introducing IBM Security Identity Governance and Administration

Delivering actionable identity intelligence



- Align Auditors, LoB and IT perspectives in one consolidated Governance and Administration offering
- Easy to launch Access Certification and Access Request to meet compliance goals with minimal IT involvement
- Enhanced Role Mining and Separation of Duties Reviews using visualization dashboard and business-activity mapping
- In-depth SAP and RACF Governance with Segregation of Duties (SoD), access risk and fine-grained entitlements reviews
- Easy to deploy virtual appliances for multiple customer adoptions
  - Standalone Identity Governance
  - Integrate and modernize legacy Identity management with integrated governance and administration

Identity and Access Management

Capabilities to help organizations secure the enterprise identity as a new perimeter

Identity Management

- Identity Governance and Intelligence
- User Lifecycle Management
- Privileged Identity Control

Access Management

- Adaptive Access Control and Federation
- Application Content Protection
- Authentication and Single Sign On

Directory Services

IBM Identity and Access Management Solutions and IBM Security Services

A new way to think about security

IBM **Security**

Intelligence is the new defense

It helps prevent threats faster and make more informed decisions

Integration is the new foundation

It puts security in context and automates protection

Expertise is the new focus

It is essential to leverage global knowledge and experience to stay ahead