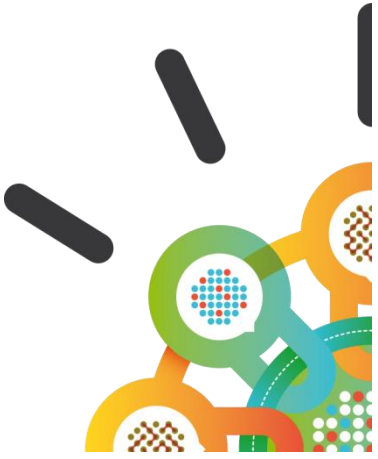
Bilgi Birikim Sistemleri

KİMLİK ve ERİŞİM YÖNETİMİ

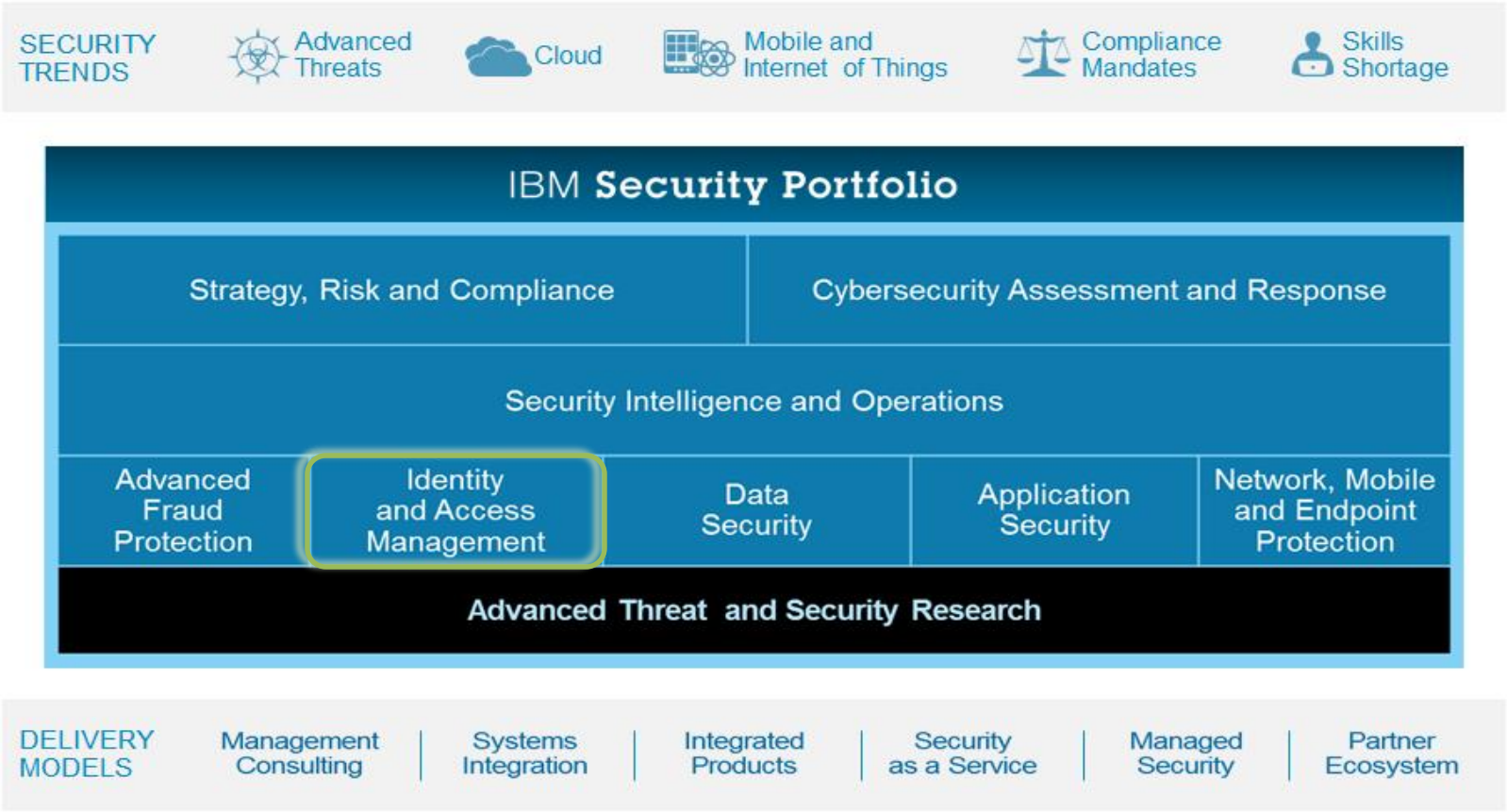
IBM İŞ UYGULAMALARI



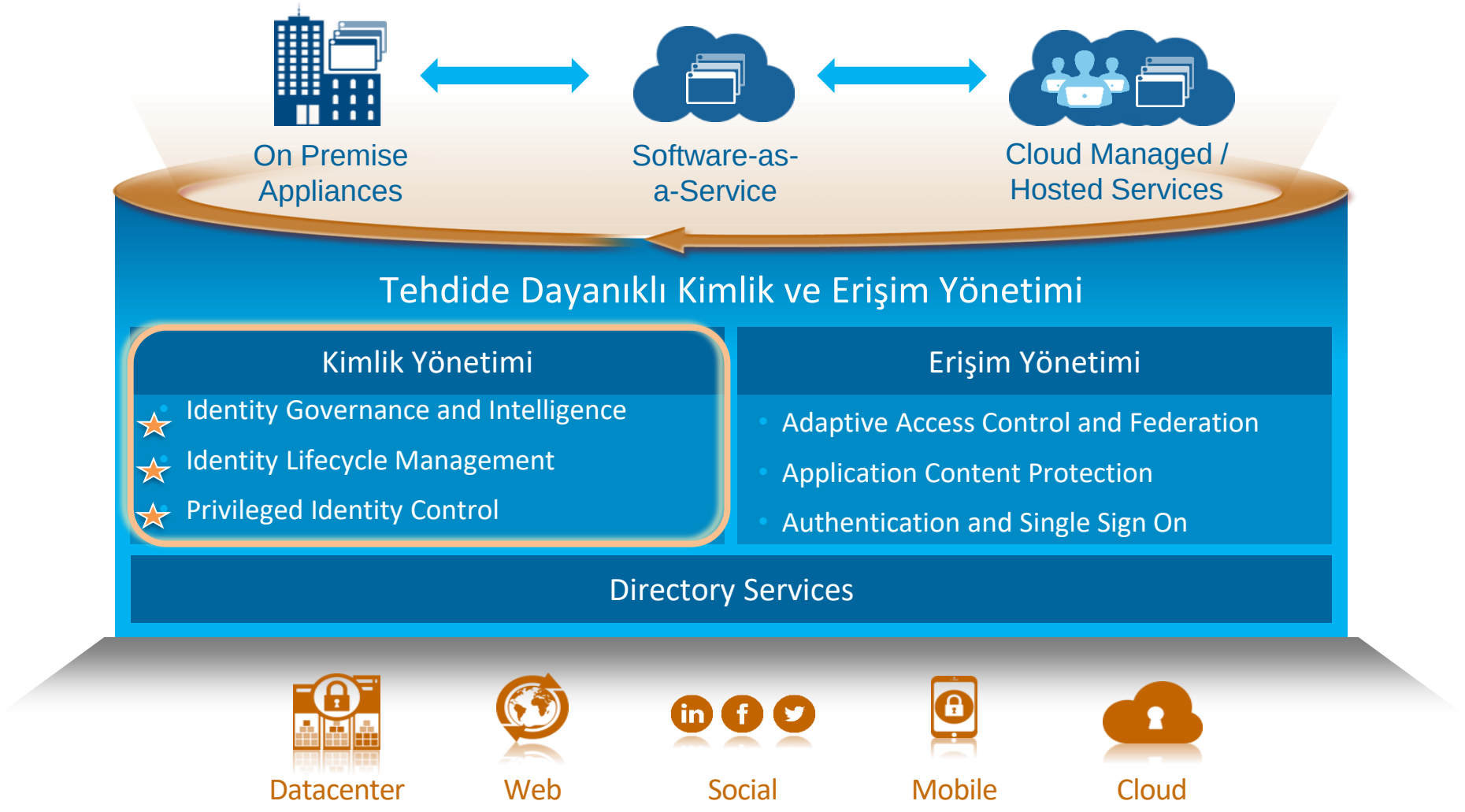
Identity and Access Management

IBM Security Identity and Access Management

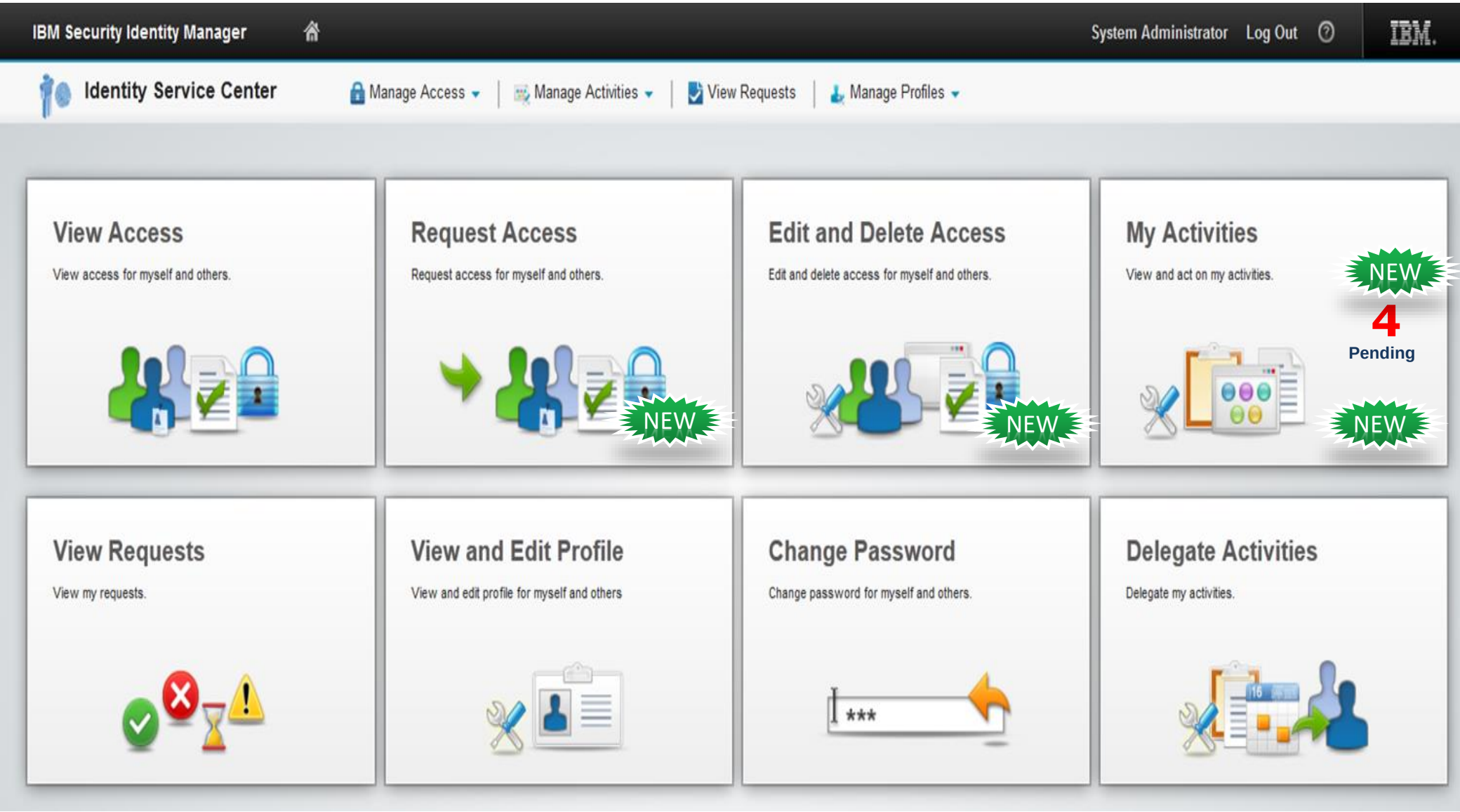
- Kimlik ve Erişim Yönetimi odak alanları
- Kimlik Yönetimi ve İdaresi
- IBM Security Identity Manager
- IBM Security Privileged Identity Manager



IBM Kimlik ve Erişim Yönetimi, açık bir kuruluş için dijital kimliklerin güvenliğini sağlamaya yardımcı olur



Kimlik Hizmetleri Merkezi



Adaptör portföyü: hızlı değer elde etmek için entegrasyon genişliği ve derinlik

Broad Support for Prepackaged Adapters

Applications and Messaging

Blackberry Ent. Server
Cognos
Command line-based applications
EMC Documentum
LDAP-based applications
Lotus Notes/Domino
Microsoft Lync
Microsoft Sharepoint
NetIQ (Novell) eDirectory
Novell Groupwise
Oracle E-Business Suite
Oracle PeopleTools
Rational Clearquest
Rational Jazz Server
Remedy
SAP GRC
SAP Netweaver
SAP AS Java
SAP HANA
Siebel
Windows AD/ Exchange

Partner Offered Integrations

Approva BizRights
Citrix Pwd Mgr
Cryptovision PKI
ActivIdentity
Lawson
SecurIT R-Man
JD Edwards
Epic
Meditech
Tandem
BMC Remedy
Zimbra Mail

Authentication and Security

CA Top Secret
CA ACF2
Cisco UCM
Desktop Password Reset Assistant
IBM Security Access Mgr.
IBM Security Access Manager for ESSO
RACF zOS
RSA Authentication Mgr.

Cloud

ServiceNow
Microsoft Office 365
Salesforce.com
Google Apps
Box
MS Azure

Operating Systems

HP-UX
IBM AIX
IBM i/OS
Red Hat Linux
Solaris
Suse Linux
Windows Local

Databases

DB2/UDB
Oracle
MS SQL Server
Sybase

Application adapter
Host adapter
Requires local adapter

Fast, adaptable tooling for custom Adapters

- Quickly integrate with home-grown applications
- Easy wizard-driven templates reduces development time
- Requires fewer specialized skills

Deep support, beyond a ‘check box’, for critical infrastructure and business applications

salesforce
ORACLE
SAP
Microsoft
IBM
ca
CISCO

IBM Security Identity Manager
BBS Referansları

- 20.000 kullanıcılı Kamu Bankası ve İştirakleri

ANADOLU SİGORTA

TAI TUSAŞ-Türk Havacılık ve Uzay Sanayii A.Ş.

ÇALIK HOLDİNG

ZORLU

TC İSTANBUL KÜLTÜR ÜNİVERSİTESİ

Kamu Bankası

- ~20.000 kullanıcı
- Kişi başına 16 hesap, toplamda yaklaşık 300.000 hesap
- Humanist (SQL view)
- RACF, AD, Exchange, Lync, IBM LDAP, DB tablolarıyla yönetilen sistemler, Cisco CM, BMC Remedy
- İştiraklerin yönetimi
- Günde 300 yetki değişikliği
- Tüm sistemlerde şifre senkronizasyonu
- Pazartesi sabahları 1500'den fazla şifre değişiklik talebi, 500'den fazla bloke kaldırma (DPRA ve self servis)
- Yıllık toplantılarda yetki değişimi (vekalet) (1 gecede 5000'den fazla değişiklik)
- Çağrı merkezi ile şifre değişim taleplerinde gizliliğin sağlanması

TAI

- 4000 kullanıcı
- IK değişiklikleri anında sisteme yansıyor
- Kullanıcıların yetki talep mekanizması (self servis)
- SMS ile şifre bilgilendirme
- Kişisel ve paylaşılan ortak klasörlerin yetkilerinin yönetilmesi

Çalık Holding

- 2000 kullanıcı
- 2 farklı IK kaynağı
- SAP hesaplarının yönetimi (20 kadar SAP servisi)
- AD, Exhange, SAP
- Şifre değişiminde DPRA ve self servis
- İşe giriş çıkış süreçlerinin yönetilebilir hale gelmesi
- Danışman hesaplarının yönetilmesi
- PIM: Sistem yönetici hesaplarının yönetilmesi, danışmanların yönetilmesi

Anadolu Sigorta

- ~20.000 kullanıcı
- AS400, Host OnDemand, AD, LDAP, Exchange, IBM Access Manager, özel uygulamalar
- 5 farklı IK kaynağı

Eczacıbaşı Holding

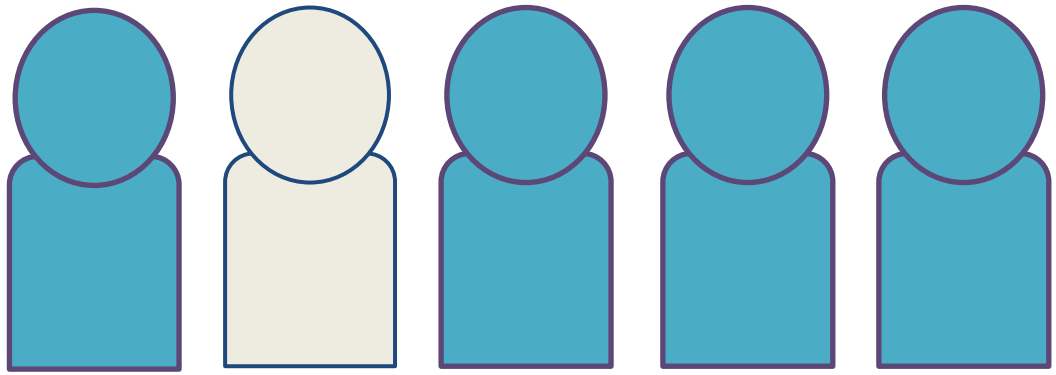
- ~20.000 kullanıcı
- Yaklaşık 100 adet şirket
- 100 adet SAP servisi
- Her organizasyon kendi yetkilisi tarafından yönetiliyor (Sistem yönetici arayüzünün etkin kullanımı)
- AD, Exchange, Skype, SAP, CA Help Desk

Zorlu Holding

- 7000 Çalışan
- SMS ile başlayan şifre sıfırlama süreci

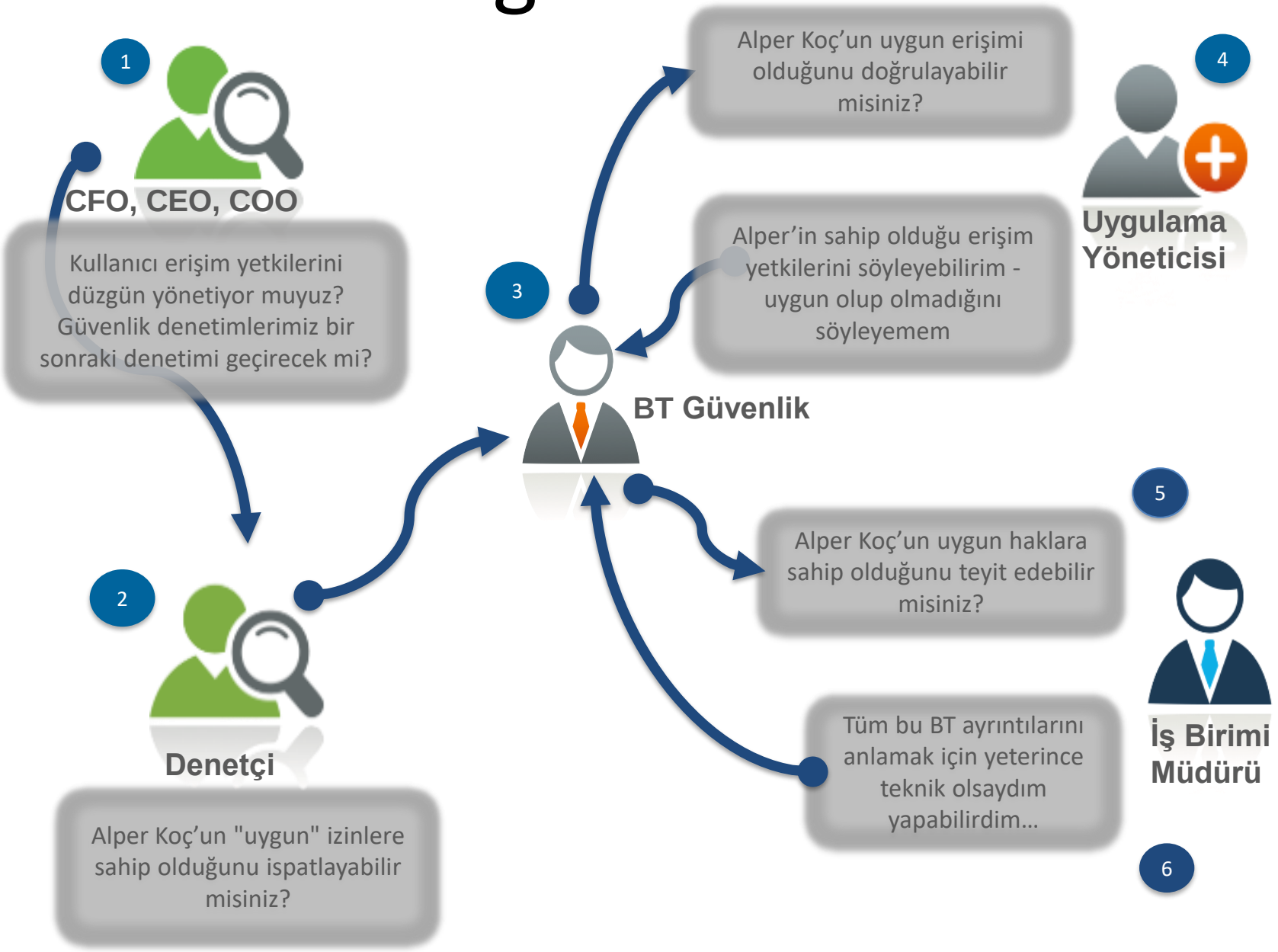
Identity Governance and Intelligence

~%80 kullanıcının gereksiz erişimi oldu



Source: Large European designer

Ağrı zinciri



Kuruluşlar, kimlik yönetimi ve istihbarata iş odaklı bir yaklaşım arıyor

Kimlik ve Yönetim Gelişimi

1 İdare/Yönetim

- Tasarruf
- Otomasyon
- Kullanıcı yaşam döngüsü
- Öncül uygulamalar ve Çalışanlar Anahtarı

2 Yönetişim

- Rol yönetimi
- Erişim belgesi
- Genişletilmiş işletme ve iş ortakları
- Açık ve kapalı uygulamalar

3 Mantıksal Analiz

- Uygulama kullanımı
- İmtiyazlı etkinlik
- Risk esaslı kontrol
- Temel normal davranış
- Çalışanlar, ortaklar, tüketiciler - her yerde

Kimlik Zekası: Kimlik Verilerini Toplama ve Analiz Etme

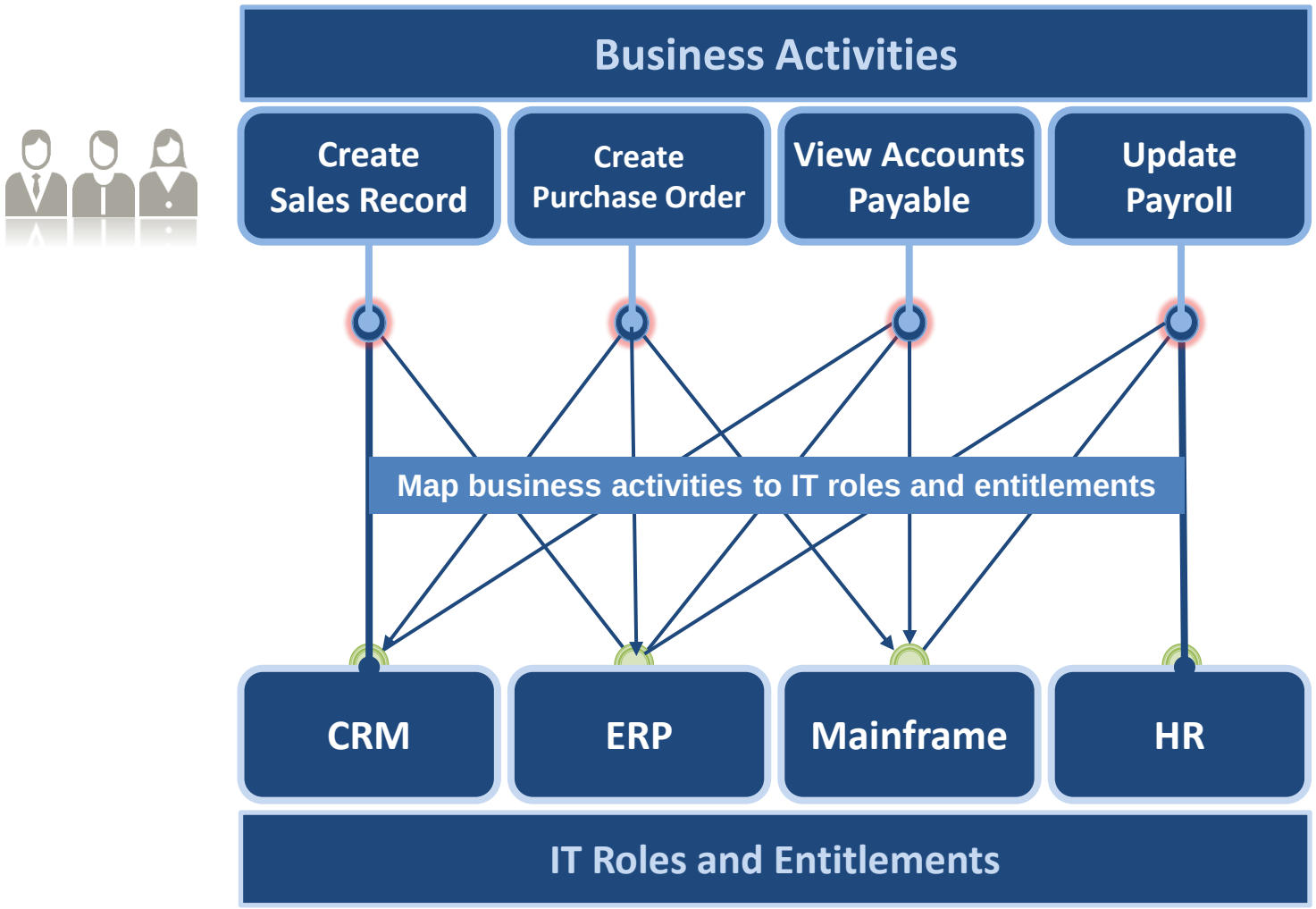
Kullanıcı erişimine görünürlük nasıl kazanılır?

Uyumluluk eylemlerine nasıl öncelik verilir?

Daha iyi iş kararları nasıl elde edilir?

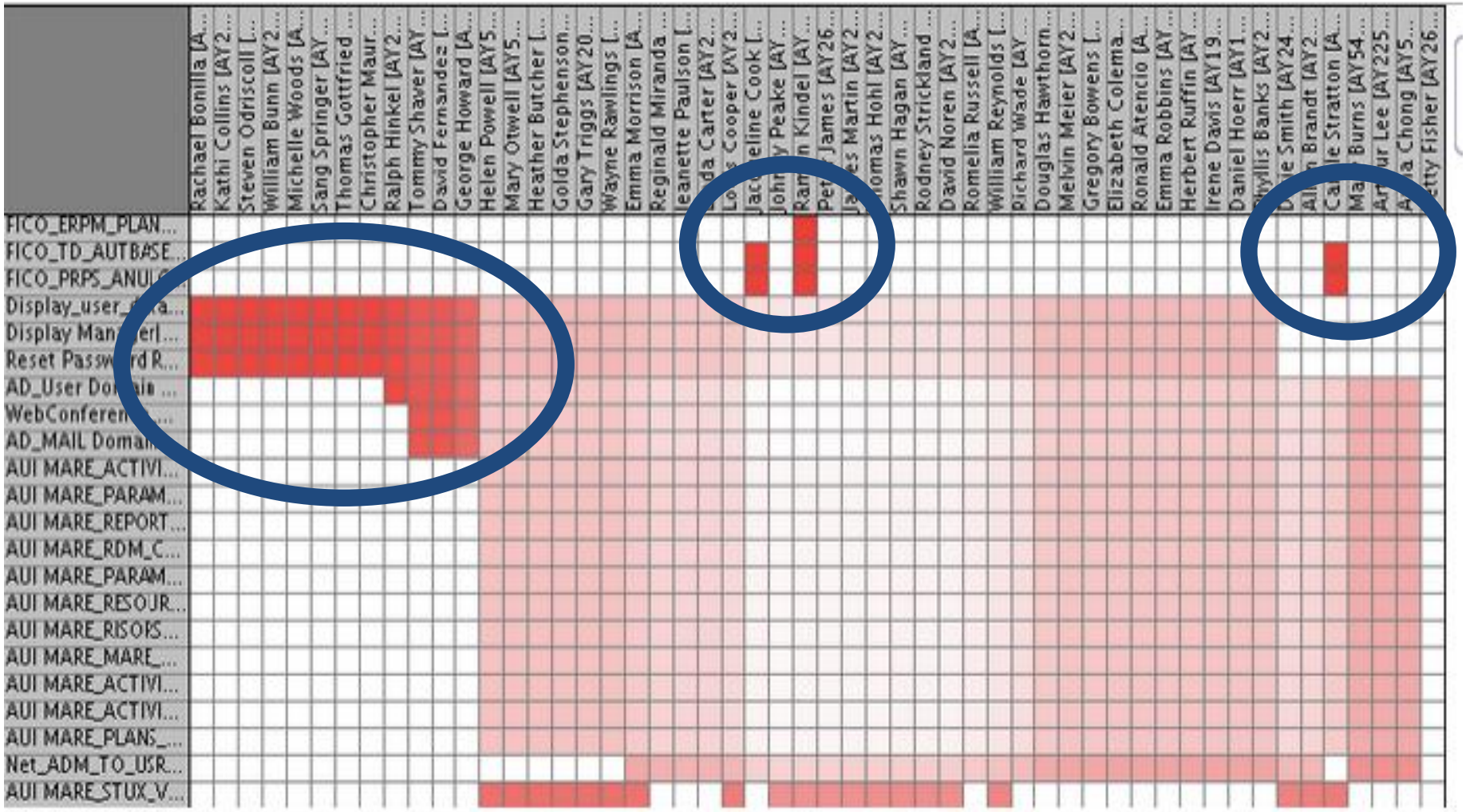
Bridging Business, Denetçi ve BT Bakış Açıları

Erişim isteğini ve sertifikasyonunu basitleştirmek için İş Merkezli SoD haritalama



Kimlik ve Erişim İstihbaratı - Aykırı değerlerin belirlenmesi

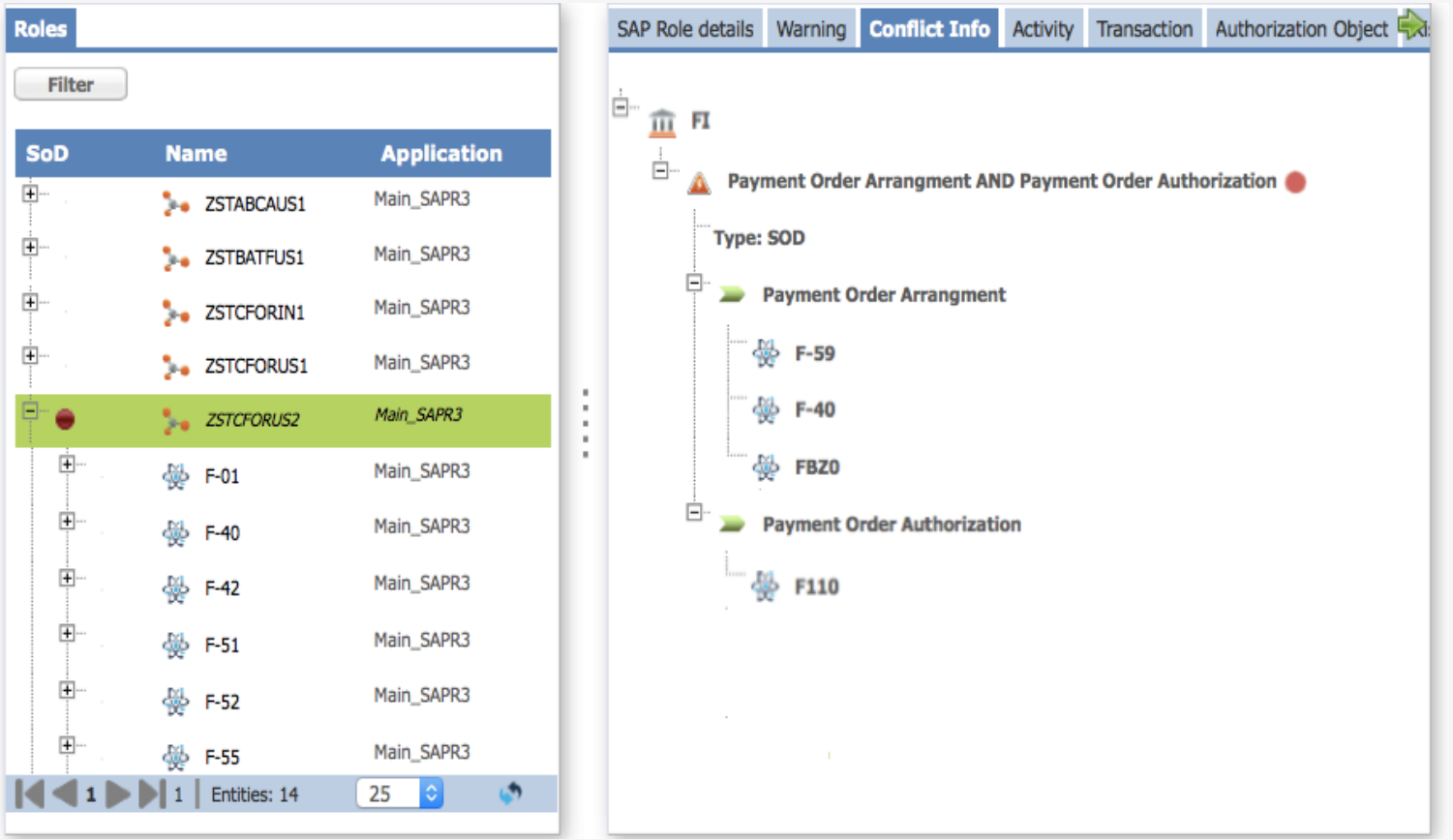
'Isı haritaları' kullanarak risk odaklı erişim sertifikası



SAP için Görevler Ayrılığı Yönetimi (SoD)

Segregation of Duties for SAP

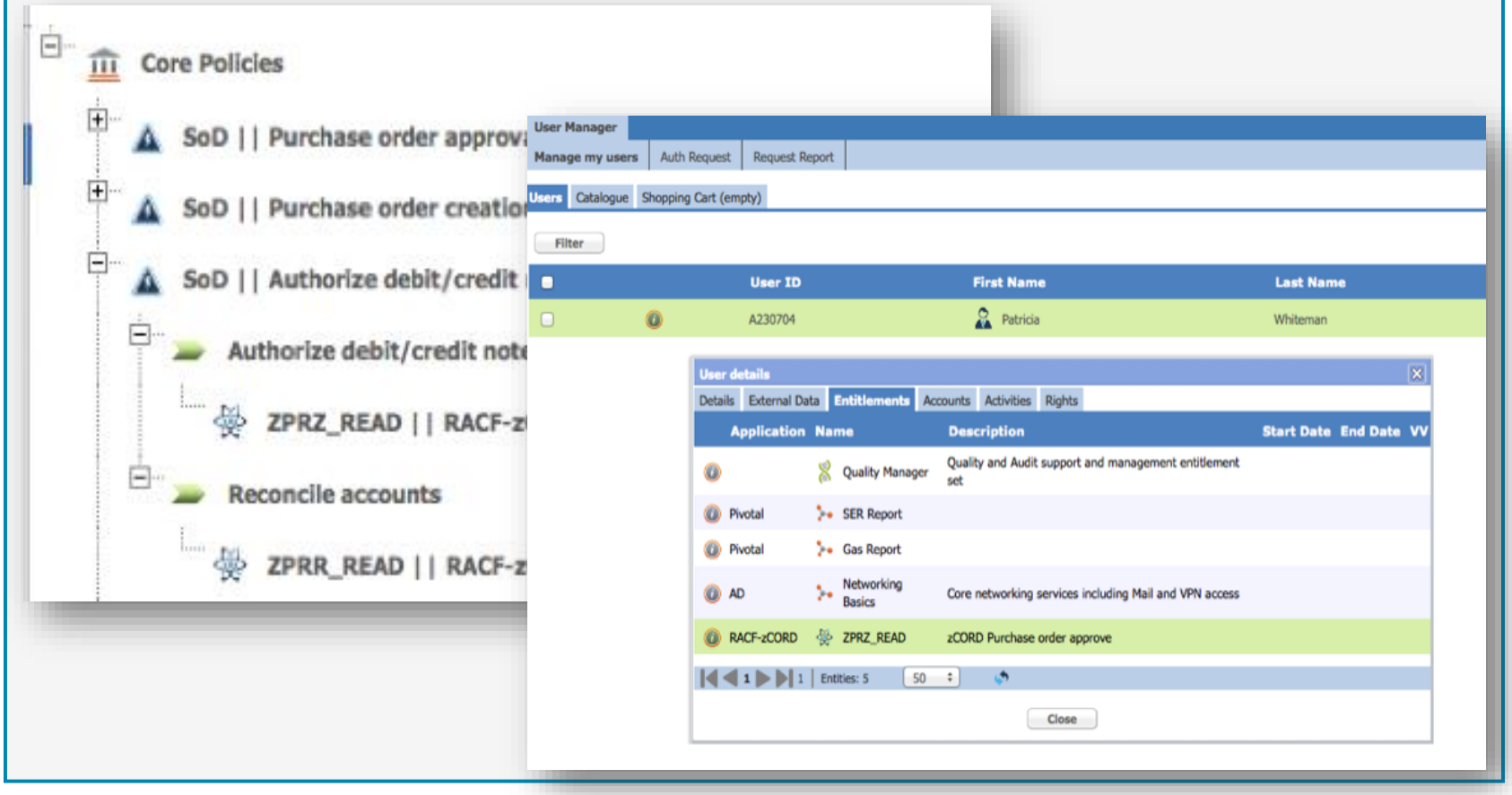
- Extends fine-grained SoD controls to SAP (users and roles).
- One governance platform for SAP and non-SAP applications



Mainframe’de Kimlik Yönetişimi

Governance on the Mainframe

- Extends fine-grained SoD controls to the mainframe-specific data model
- Provides Access Review and Request Management capabilities



Kimlik Yönetimi ve İstihbarat Sonuçları

CLIENT EXAMPLES

Denetim Erişimi

Large European designer found almost

80%

of users had unnecessary access

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

Yönetişim

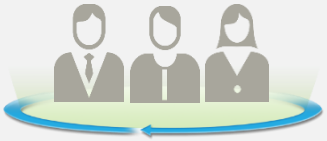
Large European insurance and financial services firm governs access to

75,000

employees, agents, privileged users

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

SoD Basitleştirme



Multinational manufacturer manages over

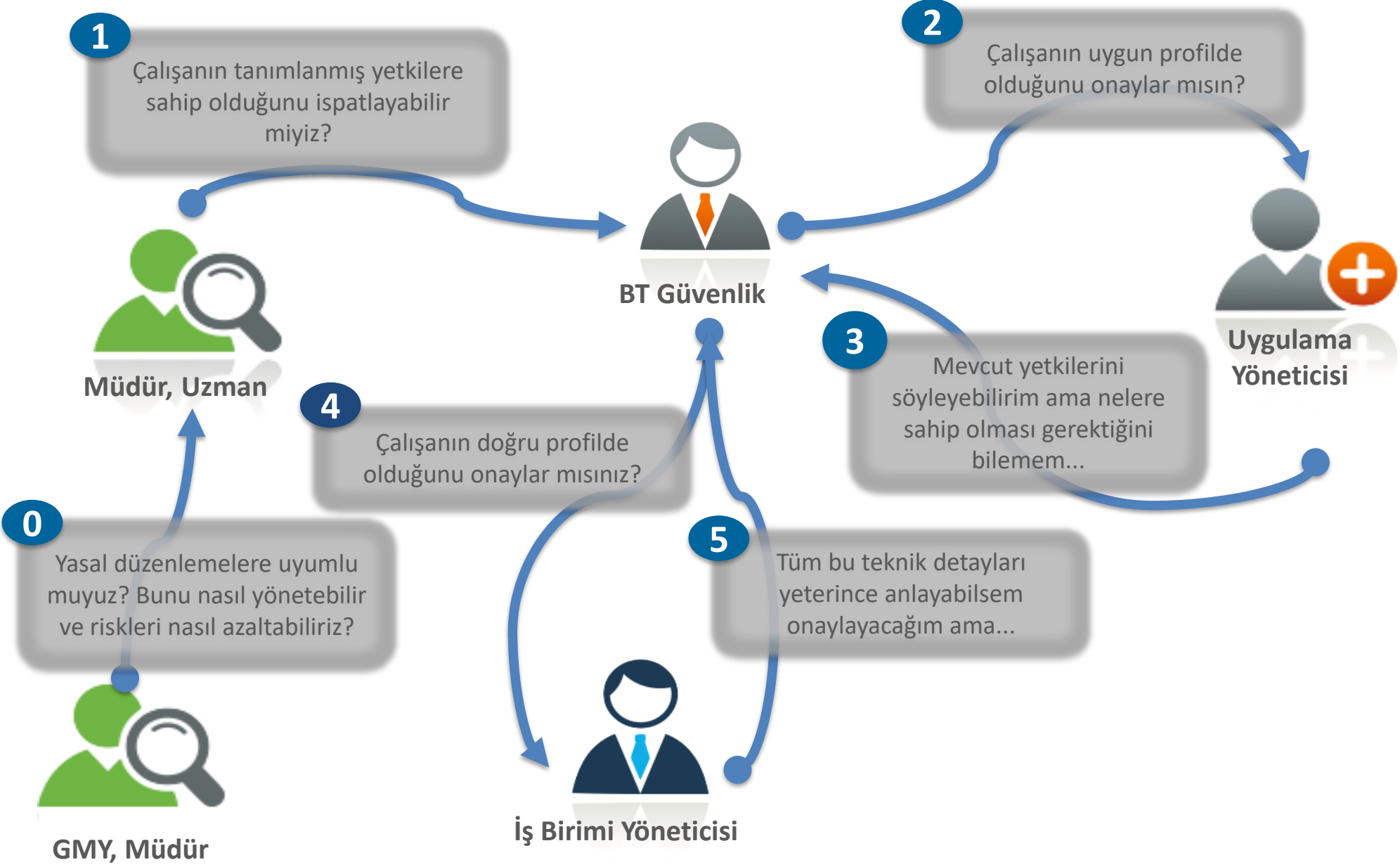
430M

potential entitlement conflicts

with only a few hundred segregation of duty rules

Identity Governance and Administration

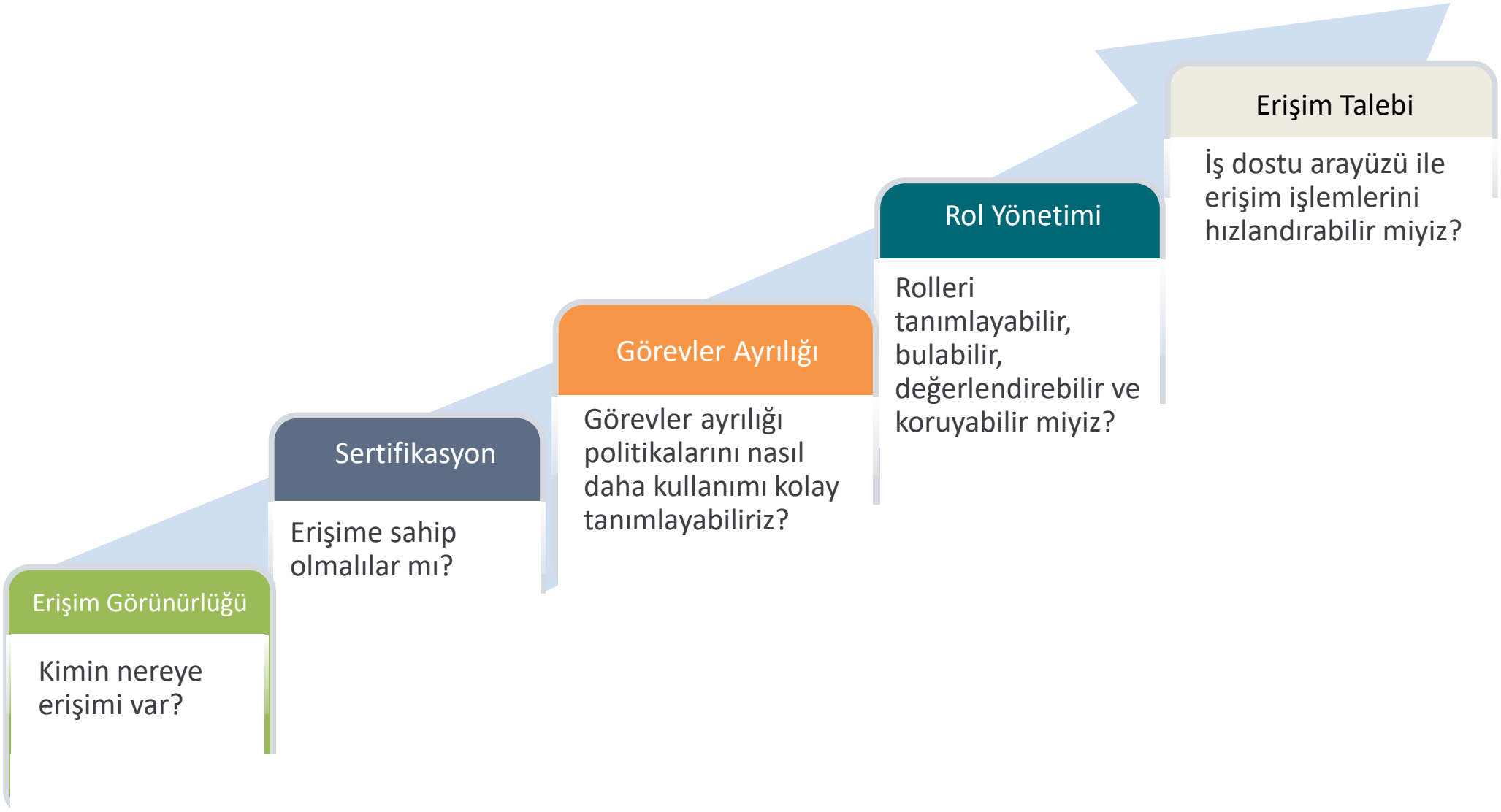
Bu görüşme NİYE yapılır? - Zahmet silsilesi...



Tipik Denetim Bulguları

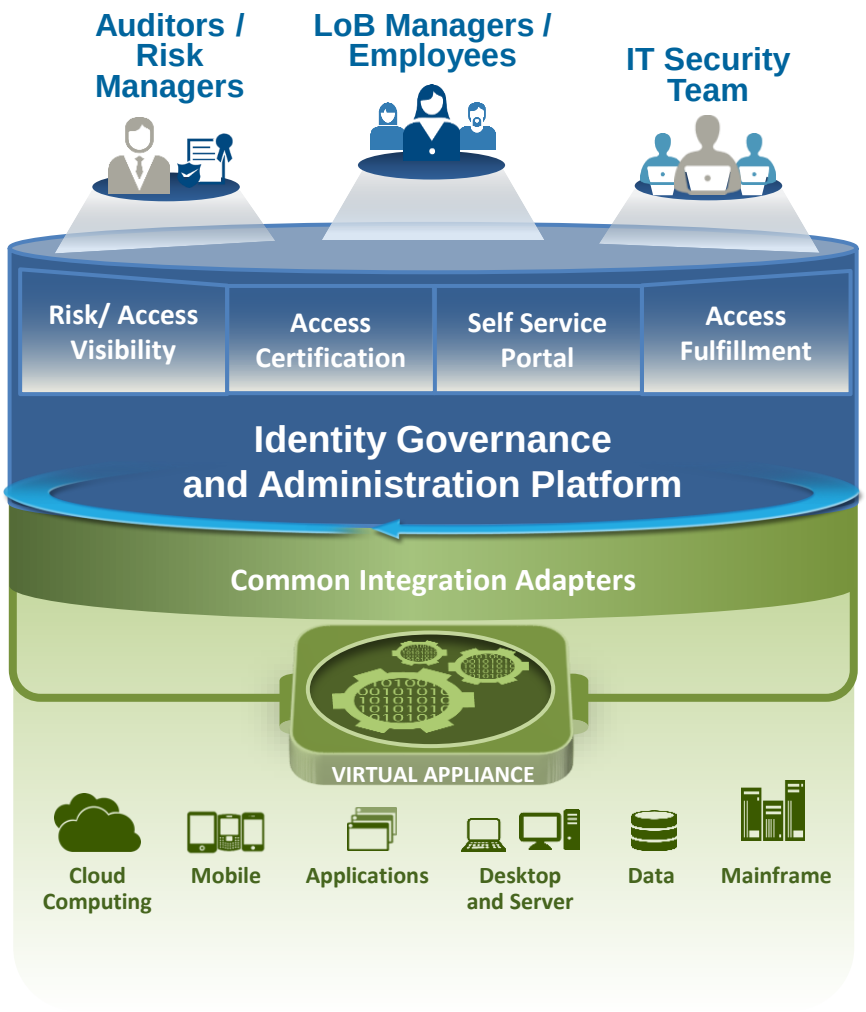
- ✗ Kötü görüş: Neden erişim hakkı verildi.
  - Kim talep etti ve kim onayladı?
  - Bu erişim hala gerekli mi?
- ✗ İhlal Tespiti Eksikliği
  - Sıradan çalışana hassas erişim tahsisi
  - Görevler Ayrılığı (Segregation of duties) ihlalleri oluşturan çakışan izinler
- ✗ Veri ve rapor almak için manuel çabalar
  - Zaman tüketimi
  - 3. parti danışmanlık ücretleri

Kimlik ve Erişim Denetlemesi Modelleri



IBM Güvenlik Kimliği Yönetişimi ve Yönetimi

Eylemlenebilir kimlik istihbaratı sağlama



NEW!

- **Full support for IBM Middleware and Database stack**
- **Enhanced integration with SIM to support Access Management Requests**
- **SAP Role Governance Enhancements**

- **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 Governance** with Separation of Duties (SoD), access risk and fine-grained entitlements reviews
- **Easy to deploy virtual appliances for multiple customer adoption scenarios**

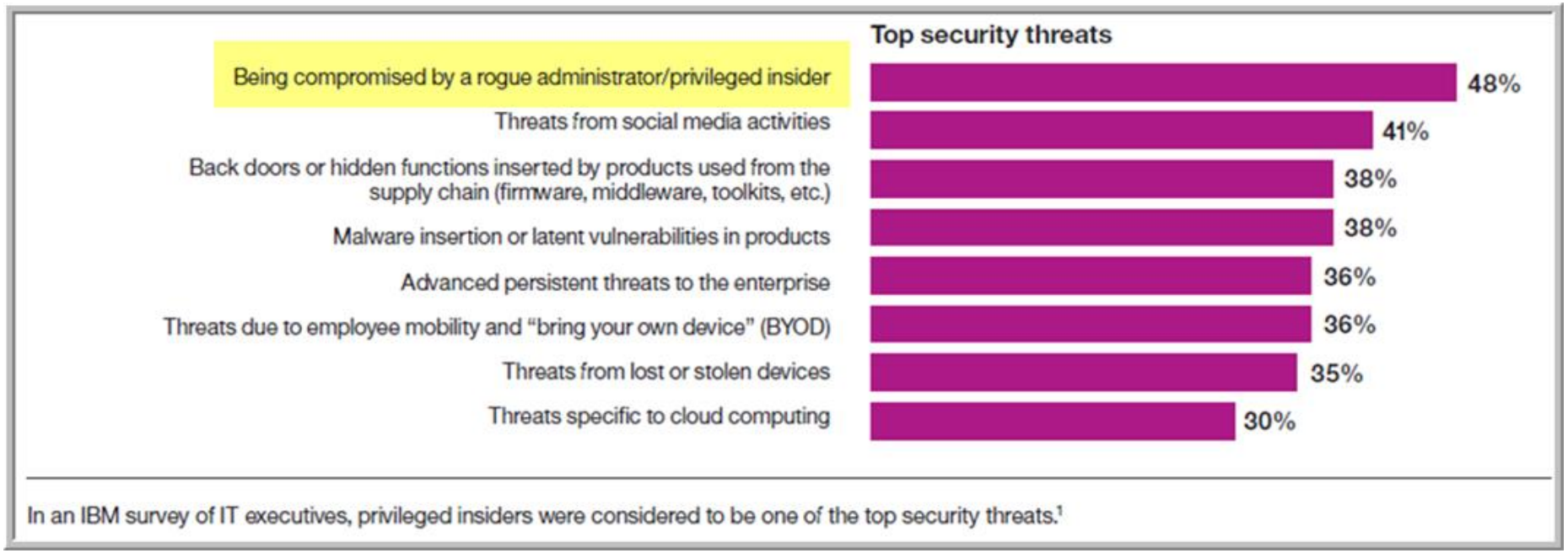
SAP için IBM Security Identity Governance

SAP Access Control için neden IBM'i düşünmelisiniz?

- SAP ve SAP dışı uygulamalar için birleştirilmiş model
- Yaklaşımı aşamalaştırmak için esneklik: ör. Başlangıçta kurumsal düzeyde tutun, ardından SAP'ye özel analizleri daha sonra gerçekleştirin .. ya da tam tersi
- Sadece SoD değil: Erişim Sertifikasyonları, Hazırlama ve Risk Skorlaması gibi diğer SAP kontrollerine başvurma becerisi

Ayrıcalıklı Kimlik Yönetimi / Privileged Identity Manager

Meydan okuma: İçeriden tehditlere karşı verilerinizi koruyun, Dolandırıcılık ve endüstri düzenlemelerine uyum sağlayın



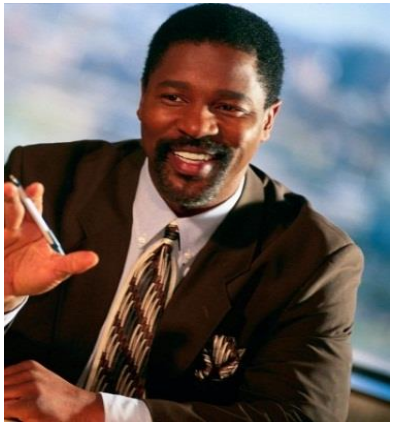
- Kuruluşlar, hassas sistemlere ve aygıtlara ayrıcalıklı kullanıcı erişimini denetlemeli ve izlemelidir.
- Son zamanlarda güvenlik ihlalleri, hassas verilere ayrıcalıklı erişim ve imtiyazlı kullanıcıların yapabileceği zarara vurgu yapar.

- Ankete katılan BT yöneticilerin %48'i en üst düzey güvenlik tehdidini ayrıcalıklı kişilerin oluşturduğunu belirtti [IBM Institute for Business Value study, July 2014]
- Hükümet ve güvenlik uyum kurallarının (PCI DSS, TRAI, IBTRM) artırılması ayrıcalıklı kullanıcıların dikkatli gözetimini gerektirir

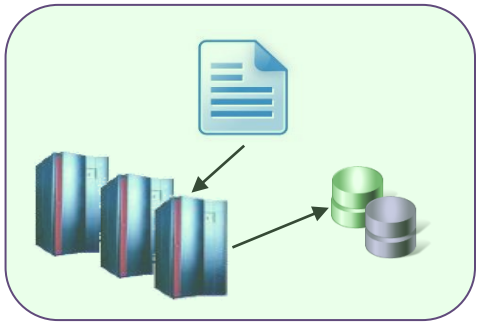
Ayrıcalıklı Kimlikler - Sadece Sistem Yöneticileri Değildir…

- Yüksek erişimli ayrıcalıklara sahip hassas kaynaklara erişen kullanıcılar
- Komut dizileri, uygulamalardaki kodlanmış kimlik bilgileri
  - Harici bileşenlere erişmek için uygulamalara gömülü yüksek erişim ayrıcalıkları ve komut dosyaları ile kimlik bilgileri
- Şirketi riske maruz bırakanlar;
  - Yanlışlıkla yapılan hatalar
  - Kasıtlı kötü muamele
- Örnek (Sadece Sistem Yöneticileri değil)
  - Root
  - UNIX File Shares Admin
  - DB2, SQL Server Admin
  - AD Domain Admins
  - SAP Admin
  - Security Infrastructure Admin
  - Firewall account access

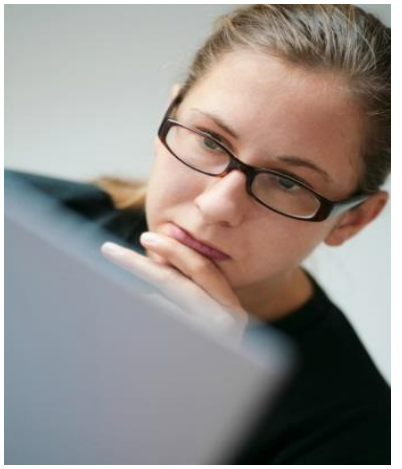
IT Sistem Yöneticileri



Uygulama Sahipleri



Uygulama Kimlik Bilgileri



Veritabanı Yöneticileri

Değişen BT eğilimleri, etkin Ayrıcalıklı Kimlik Yönetimi ihtiyacını beraberinde getiriyor

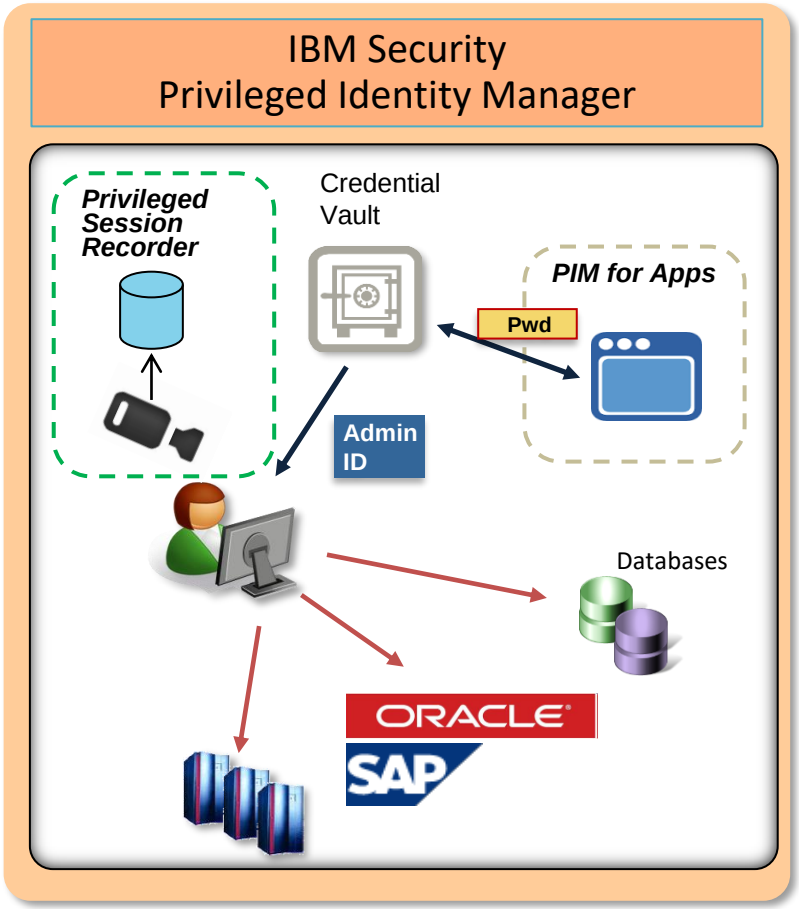
Denetim Hataları ve Düzenlemelere Uygunluk 	Whether there is an actual audit failure or a need to pre-empt one for regulatory compliance, auditors need to see proof that access controls are in place, and privileged access is a key concern, due to the inherent risk of these identities
İleri Kalıcı Tehdit 	Without strong privileged identity controls, once breached, hackers can gain unfettered access to sensitive resources
Public Cloud 	With public clouds, your data is only as secure as its access - it is important that strong controls be put on the sensitive administrative accesses to ensure only authorized individuals can access this data
Veri Merkezi Konsolidasyonu/ Private Clouds 	Data center consolidation and private cloud projects result in a high concentration of virtual and physical servers, accessible ubiquitously to a large number of system administrators and identities with elevated access rights. It is critical to control access of those privileged users in a consistent policy-based manner

IBM Security Privileged Identity Manager

Şirket genelinde paylaşılan kimlikleri merkezi olarak yönetin, denetleyin ve kontrol edin…

Başlıca ürün özellikleri

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



IBM Security Çözümü

- ***Privileged Identity Management (PIM) çözümü ayrıcalıklı kullanıcılar ve uygulamalar için eksiksiz kimlik yönetimi ve kurumsal tek oturum açma özellikleri sağlar.***

En yeni IBM Security Privileged Identity Manager (PIM) geliştirilmiş güvenlik ve esneklik sunar

YENİ!

- **Improved enterprise integration: external authentication support**
  Now supports use of Microsoft Active Directory (single domain) for user authentication
- **Improved ease of use with expanded Privileged Identity Service Center support of entitlement management**
- **Improved flexibility: application credential password management**
  The optional PIM for Applications now supports scheduled password updates of managed credentials
- **Enhanced customization support**
  New published REST APIs better support customer application integration initiatives.
- **Enhanced security: RFID authentication**
  Supports RFIDeas' RFID authentication solution
- **Quicker time to value with additional SSO profiles**
  New SSO profiles for
  - SQL Server Management Studio 2008
  - Secure CRT
  - DB2 Admin Tool *(July)*

Privileged Session Recorder option

Session Recording (Oturum Kaydı) ve Günlüğü Nedir?

- Session Recording, daha sonra arama ve görüntüleme için sistemdeki bir kullanıcı oturumu sırasında ekrandaki her şeyi görsel olarak yakalayan sanal bir gözetim kamerasıdır
  - Bir kullanıcının yaptığı şeyin en eksiksiz kaydı
  - Saygın olmayan (Non-reputable)
- Session Recording, oturum sırasında tanınan kullanıcı olaylarının bir metin günlüğüdür
  - Oturum kaydındaki zaman damgaları ile ilişkilendirildiğinden video aramalarında harcanan saatlerin kaybını önler
  - SIEM sistemleri ile entegre olup, veriler toplanabilir
- Yakaladığı şey
  - GUI veya web konsolu oturumları için meta veri içeren kullanıcı etkinliklerinin ekran görüntüleri
  - Metin konsolu oturumları için komut günlükleri
- Amaç
  - İmtiyazlı oturumların kaydedildiği ve izlendiği denetçiler için kanıt (yönetmeliklere uygunluk)
  - Ayrıcalıklı kullanıcıları eylemlerinin kaydedildiğinin farkında olun
  - Kök neden analizi ve adli tıp için kayıtlı oturumları arama yeteneği sağlayın

Temel İş Senaryoları

- **Ayrıcalıklı Kullanıcı Aktivitesi İzleme:**
  - Paylaşılan bir Kimlik No aracılığıyla erişilen oturumlarda kullanıcı etkinliğini kaydetme ve günlüğe yazma
  - Kullanıcıları haklarını kötüye kullanma ayrıcalığından vazgeçirin
- **Yasal Uyum**
  - Dünya çapında birçok düzenleyici makamlar, kuruluşların ayrıcalıklı kullanıcı etkinliğini izlemelerini ve bu kullanıcıların sistemlerinde neler yaptıklarını göstermelerini istemektedir.
    - Örnek: PCI DSS 10.2 Bu olayları yeniden yapılandırmak için tüm sistem bileşenleri için otomatik denetim izlerini uygulayın. Herhangi bir kişi tarafından kök veya idari ayrıcalıklara sahip olunan tüm eylemler.
    - Örn: Singapur IBTRM (bankalar için) "Ayrıcalıklı kullanıcılar tarafından gerçekleştirilen sistem faaliyetlerinin denetim günlüğü tutulur"; "Ayrıcalıklı kullanıcıların faaliyetlerinin ele geçirildiği sistem günlüklerine erişimi yoktur"; "Satıcılar ve müteahhitlerin, yakın denetim ve izleme olmadan sistemlere ayrıcalıklı erişim kazanmasına izin verilmemektedir."
    - Ör. Hindistan Telekom Düzenleme Kurumu
- **Kök Nedeni Analizi / Adli Tıp**
  - Ayrıntılı etkinlik kayıtlarını kullanma - hizmet kesintilerinde sorun gidermeye yardımcı olabilir

IBM Security Privileged Identity Manager - Privileged Session Recorder

Ayrıcalıklı etkinlik için artan görünürlük vasıtasıyla iyileştirilmiş yönetişim ve uyumluluk

Yönetme veya sorun giderme amacıyla kullanmayın.

Anahtar modül özeti

- *Kullanıcı bitiş noktası etkinliğinin kaydedilmesi*
  - *Triggered by credential checkout*
  - *Command line and GUI (e.g. Windows) activity recording*
- *Kayıtların daha sonra tekrar çalınması için saklanması*
  - *Supports audit and troubleshooting*
  - *Compression and archiving supported for storage management*
- *Kayıtlar için esnek arama*
  - *By user, date, application, command or endpoint system*

IBM Security Çözümü

- *Privileged Session Recorder provides visual recording of privileged user activities with on demand search and playback of stored recordings*
- *Improved IAM governance and compliance*
  - *Meet government compliance requirements*
  - *Provide oversight of privileged user activity*