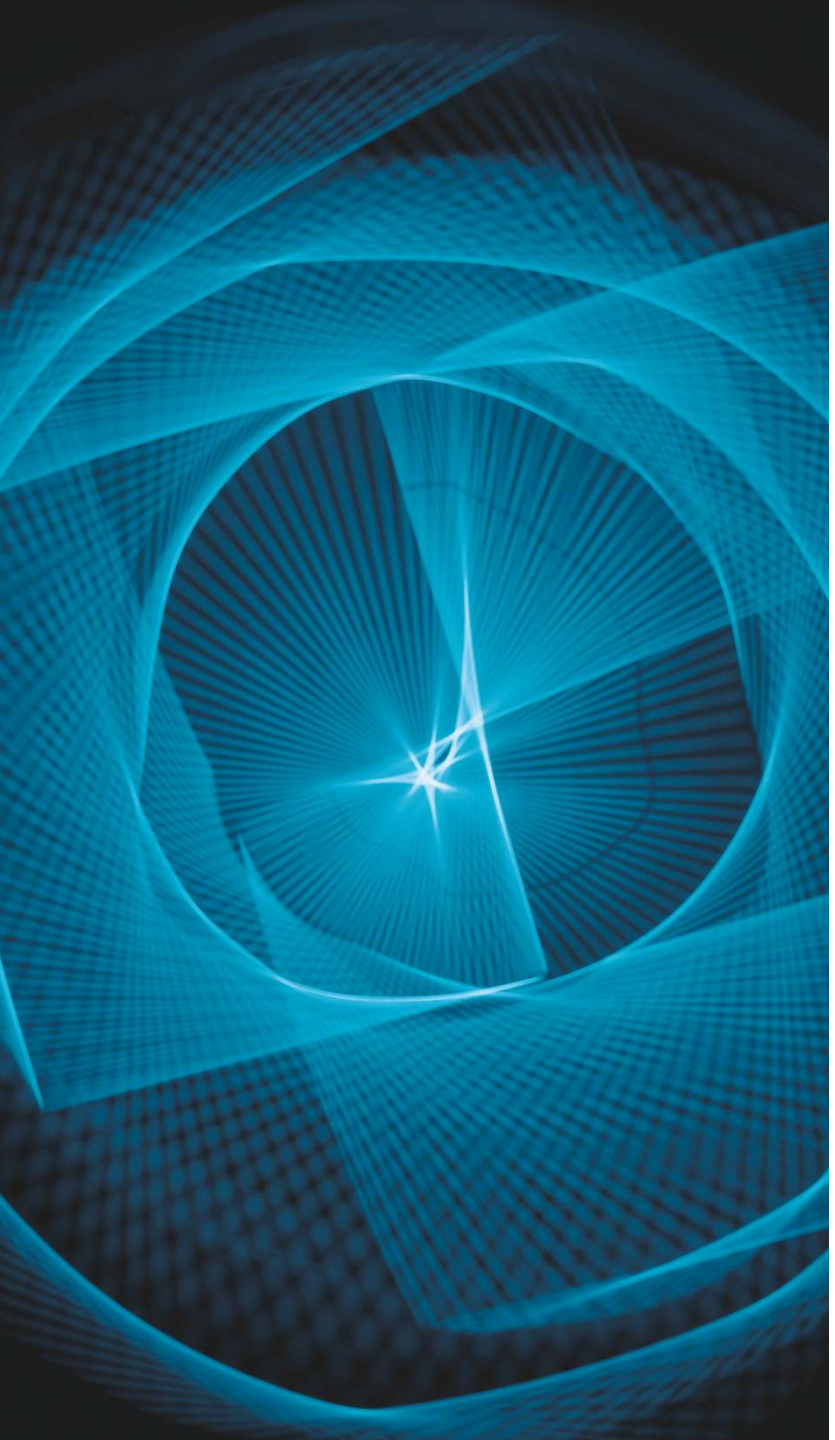


OXFORD COMPUTER GROUP

Saviynt & MIM: Adding Intelligence to your Identity Management Program

MIM Extension Webinar Series

Nabeel Nizar VP World-Wide Solutions Engineering, Saviynt

Hugh Simpson-Wells CEO, OCG

June 15, 2017

Identity-Driven Security from OCG

OXFORD COMPUTER GROUP

Delivering **long-term, value-added** services for Identity and Access Management, Identity Governance, Device Management, Security, and more.

Why OCG?

- 15+ year track record deploying identity and hybrid-identity solutions
- 700+ enterprise projects delivered around the world, and over 7 million Office 365 seats deployed
- Microsoft Identity Partner of the Year 2013-2014-2015, finalist 2016
- Deep connections with Microsoft Cloud engineering team

Planning & Assessment

- Envisioning workshops
- Readiness assessments
- Security reviews
- AD health-checks
- Training courses

Deployment Services

- Pilots for Azure AD, AD FS, Intune, RMS, and more
- Office 365 integration/migration
- FIM/MIM integration
- Azure Marketplace Application Integration
- SMS integration

Managed Services

- Help desk support
- System Center integration
- 24x7 monitoring, alerting & logging
- Maintenance
- 3rd party application management
- Training courses

Established
2010

Team of
170+

LA(HQ)

Strong heritage in IGA & Security

Vision

Be the foremost Cloud Identity Governance 2.0 provider

Enable organizations with access governance and intelligence 2.0 solutions
to adopt Compliance, Cloud First and Digitalization initiatives and
secure critical data, infrastructure and applications

SAVIYNT

What is Identity Governance & Administration?

User Account Provisioning

- Identity Lifecycle Management
- User Provisioning
- Password Management
- Centralized Identity Repository - 'One identity to rule them all'

Security - 1995

Access Governance

- Certifications
- Role Management
- Policy / Process
- Access Request
- Compliance reporting

Compliance - 2002

Compliance does not equal Security!

Whose has Access?
What do they have access to?
What does that Access secure?
Why was the Access granted?
Who approved the Access?
When was the Access granted?
Was the access re-certified?

Is the Access necessary?
What is the Business impact? Risk?
How is it being used?
Can it help improve Business process?

Digital, Cloud First and *Compliance* mandates are introducing a paradigm shift in IT

Massive Exposure

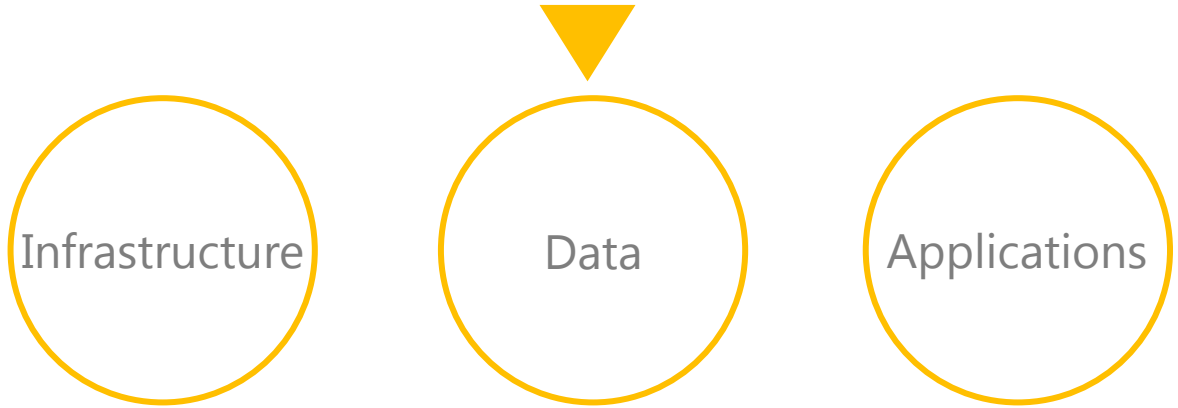
as assets are opened for external access

Excessive Privileges

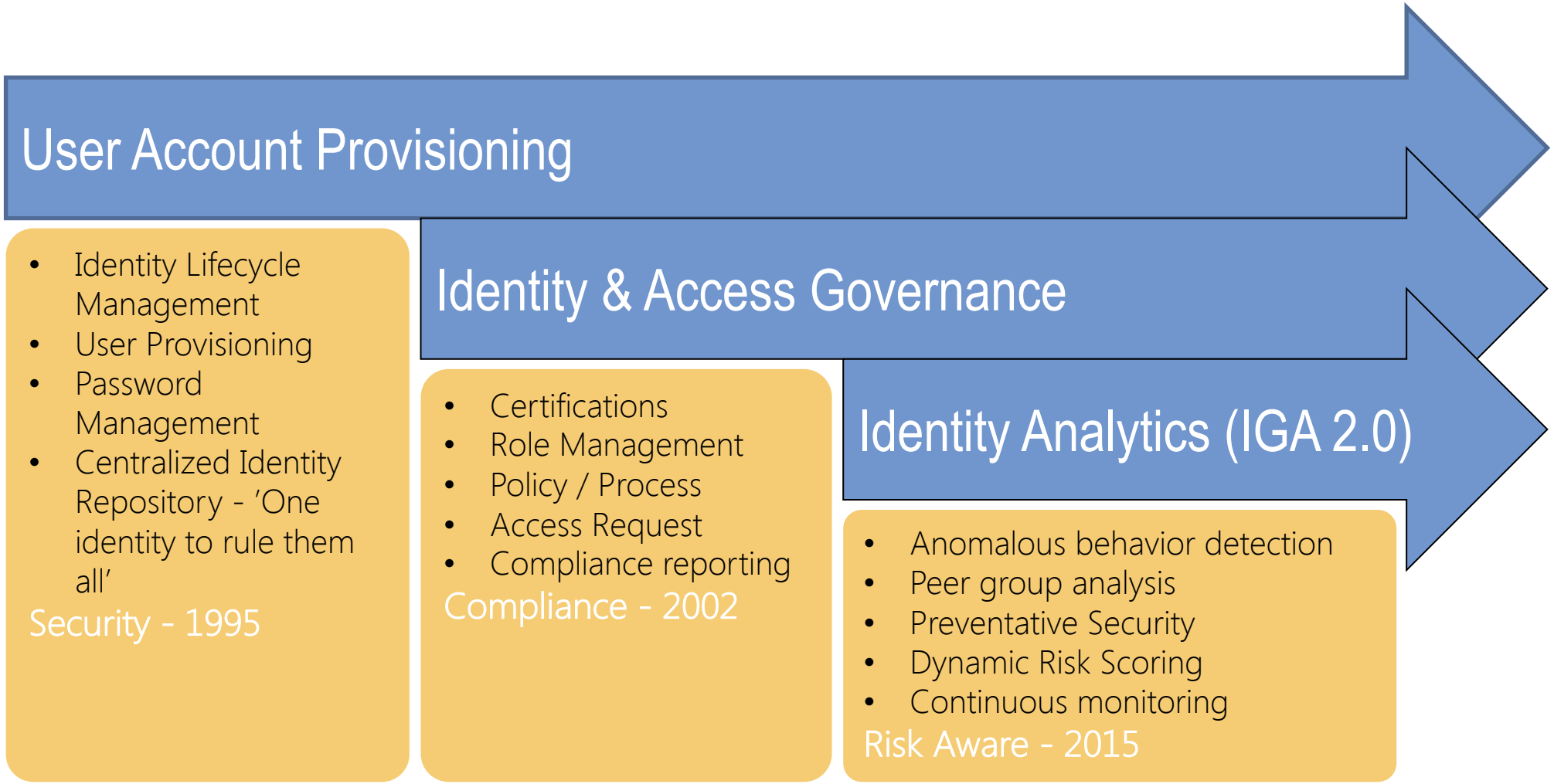
due to increased autonomy

High Overhead

in being up-to-date or incur risk penalties



IGA isn't enough….



IGA 2.0 → Identity Governance & Administration with Identity Analytics

Identity is the new Perimeter

Visibilty across Data, Infrastructure & Applications
on cloud and enterprise and across different user communities...

Governance is the new Imperative

Compliant identity across multiple regulations...

Intelligence in the new Prevention

Need to move from Compliance to Intelligent + Real-time Security in a transient environment...

IDM - IGA1.0 -> IGA 2.0

Legacy Identity Management Connectors

AD / Exchange | REST APIs | RACF ACF2 | LDAP | SPML / SCIM | UNIX | RDBMS DB Tables | Any App

Identity Governance and Intelligence

- Intelligent Access Request Management
- Risk-based Access Certification
- Provisioning & Connectors
- Usage / Risk Analytics
- Integrated Access Recommendations
- Continuous Controls Monitoring
- Password Management
- Privilege Access Governance
- Reporting & Dashboard
- Segregation of Duty (SOD) Management
- Role / Rule Engineering & Governance
- ABAC / Event-based Policy Management

Identity Analytics and Intelligence

- Usage / Outlier Analytics
- Integrated Access Recommendations
- Risk & Controls Library
- Fine-grained Segregation of Duty (SOD) Management
- Fine-grained Role & Rule Engineering & Governance
- Identity Governance Metrics & Reporting
- Application Onboarding Workbench
- Access Clean-up
- IGA Integration Interfaces

Secure data, applications and infrastructure with a single product

Infrastructure Access Governance

amazon web services™
GitHub
CHEF
Microsoft Azure
docker
puppet labs

Data Access Governance

Google Apps for Work
Office
SharePoint
box
hadoop
Dropbox

Application Access Governance

salesforce
SAP
workday
ORACLE E-BUSINESS SUITE
Epic
SAP HANA
Cerner
PeopleSoft

External / Customer Access Governance

RADIANT LOGIC
salesforce
Azure AD
Ping Identity
okta
FORGEROCK OpenDJ

Identity Governance and Intelligence

AD / Exchange | REST APIs | RACF ACF2 | LDAP v3 | SPML / SCIM | UNIX | RDBMS DB Tables | 120+ Apps

Identity addresses 3 primary needs to secure critical assets

Top governance problems solved by Saviynt

VISIBILITY

- Who has access to what?
- Who are my riskiest users / workloads?
- What are the privileged entitlements / sensitive data?
- What are they doing with that access?

GOVERNANCE

- How can I ensure appropriate access at all times, including emergency access?
- Can I enforce Segregation of Duty (SOD) rules, access policies?
- How do I revoke access in timely manner?

SECURITY

- How can I secure in 'real-time' access to sensitive data or critical workloads?
- Can I stay ahead of new threats? Identify suspicious users?
- How do I apply compliance mandates consistently?

Identity 2.0

IGA 2.0 success lies in understanding its

USER, UX and their imperatives

Requester, Approver

Catalog should be easy to find

If / when will I get access?

Understand risk exposure if approved

Compliance Owners

Identify non-compliant / risky users and their access

Revoke risky access in a timely manner

Are all crown jewels protected despite org changes?

Are controls effective, preventive?

Certifier

Manage exception access

Understand risk if access is extended

When / why was access granted?

Who else has reviewed the access?

App Owner

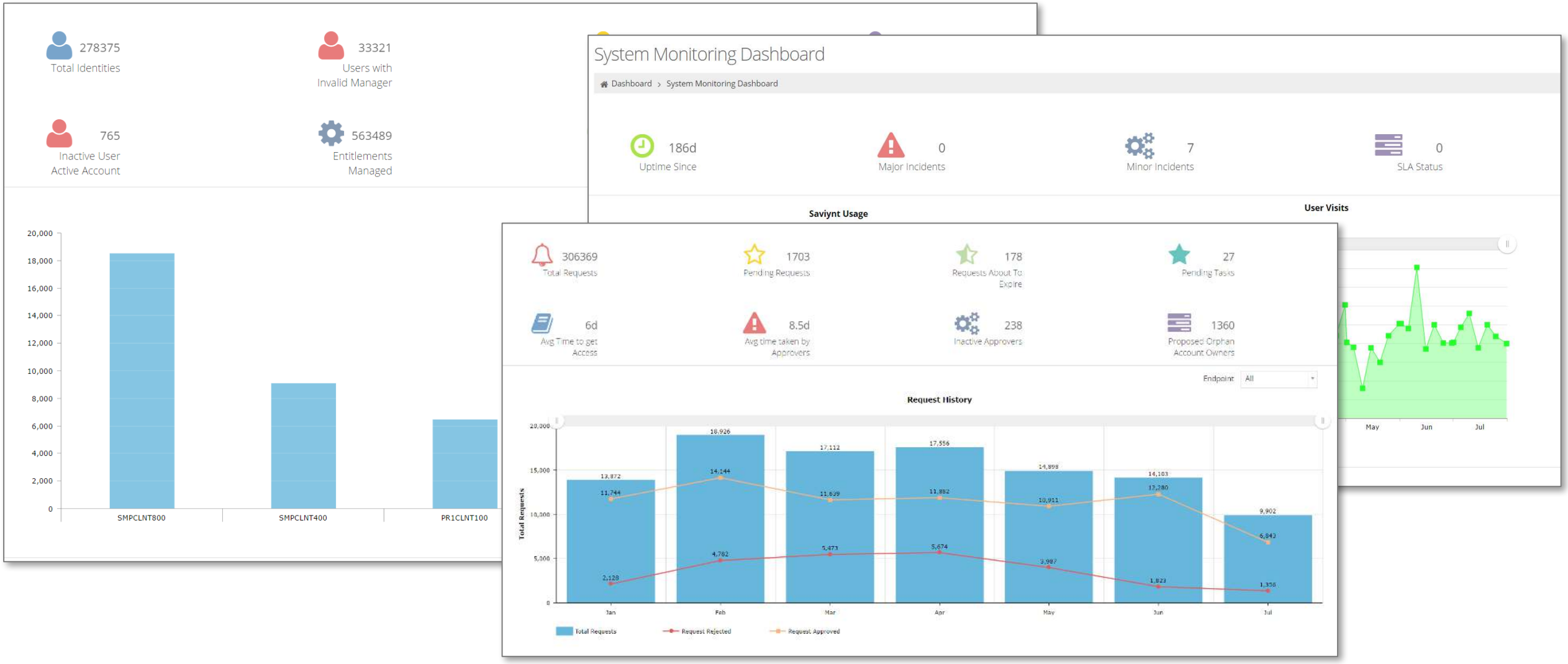
Can I see all the risky users / access / violations to my app?

How can I easily integrate my app?

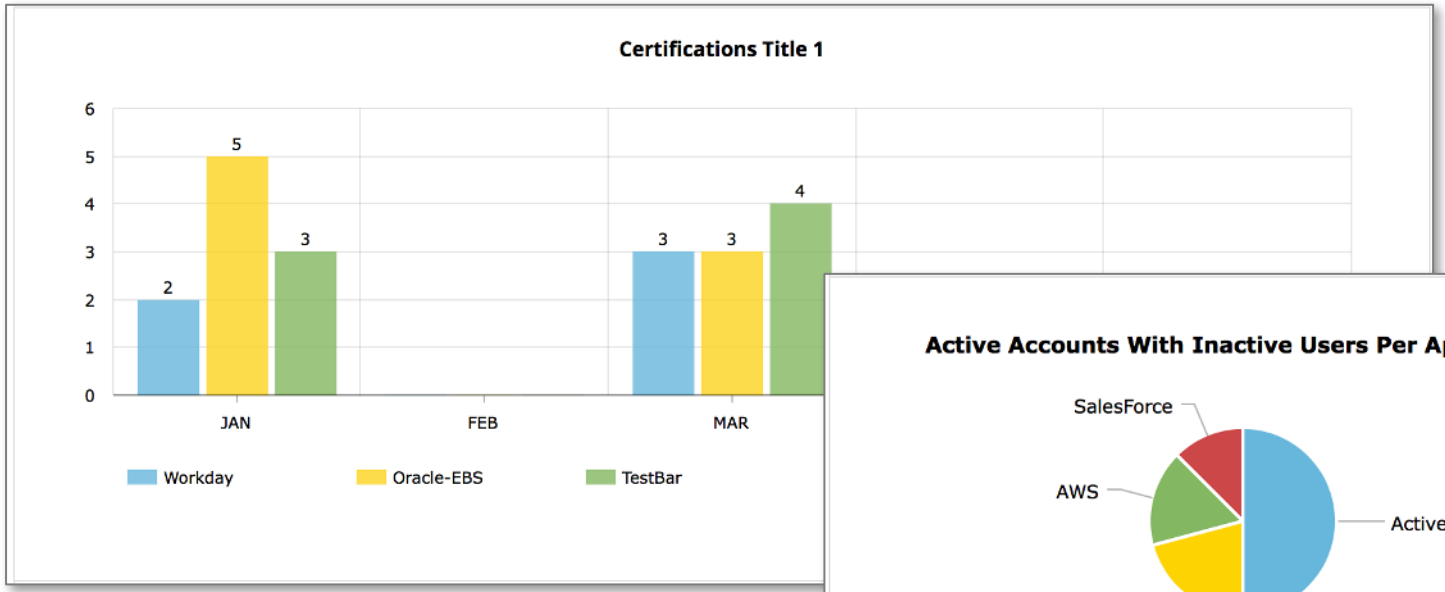
Easily make bulk changes

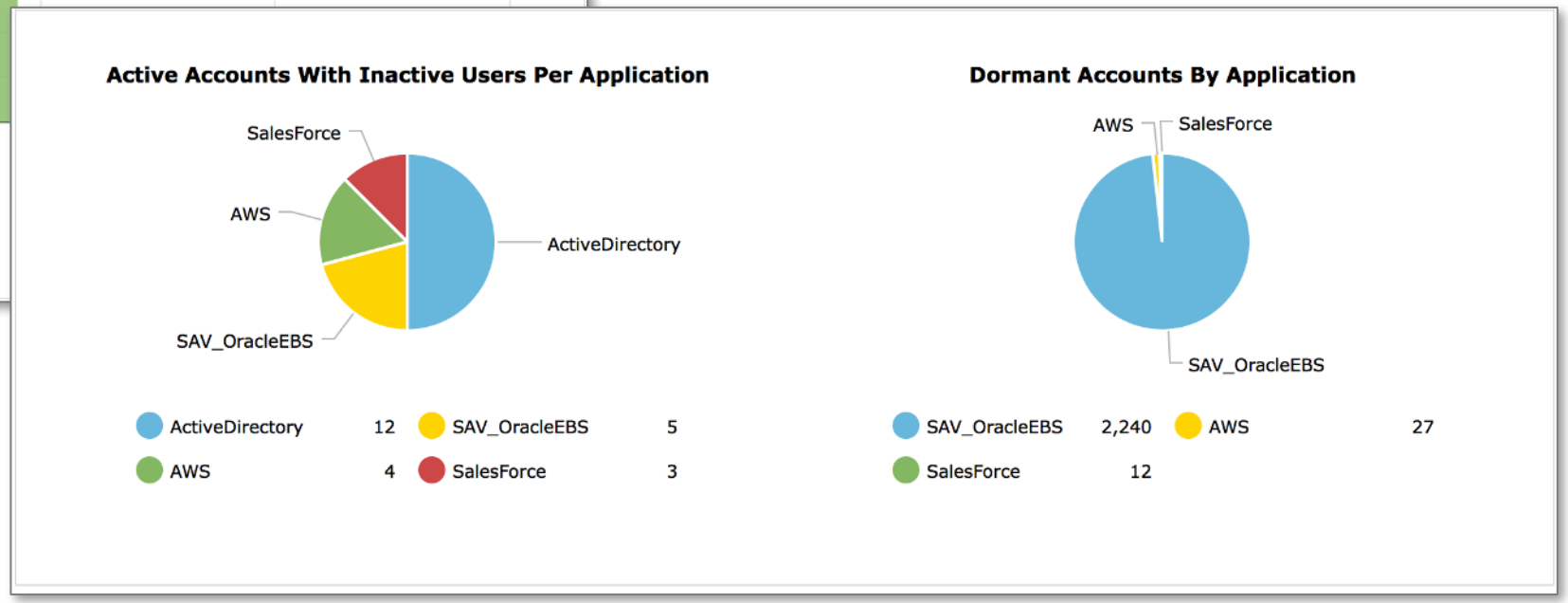
Manage licenses

Built to demonstrate continuous business value with out-of-box KPIs, drill down dashboards

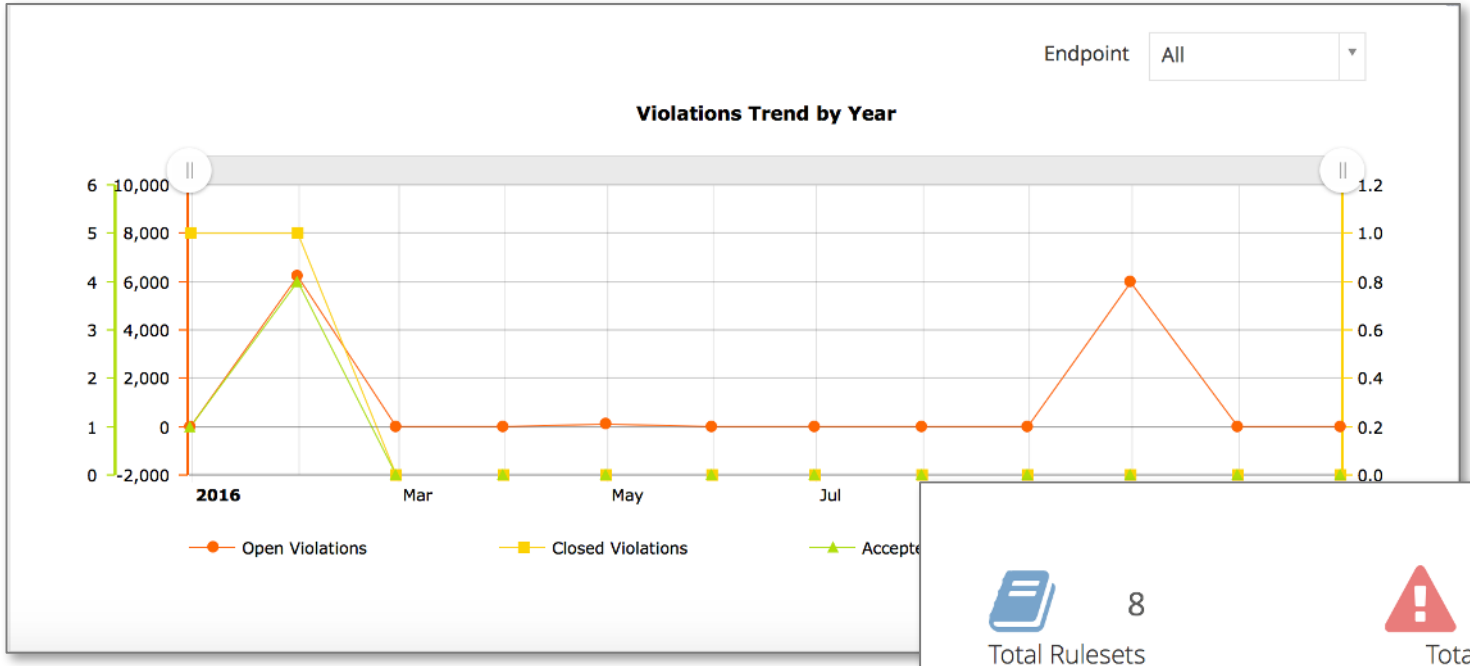


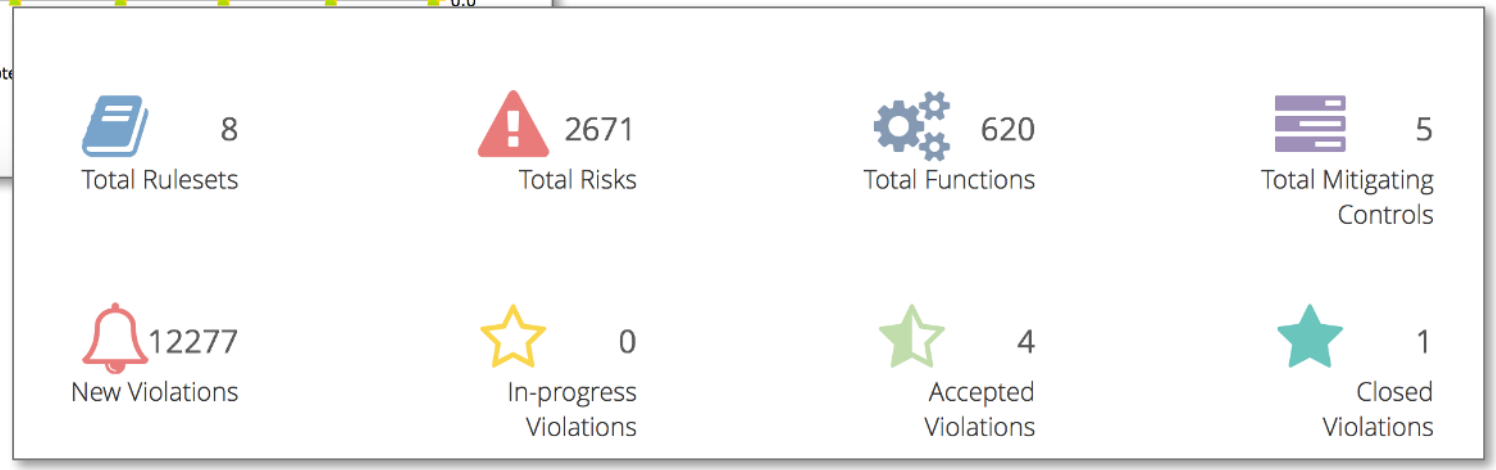
Built to demonstrate continuous business value with out-of-box KPIs, drill down dashboards





Built to demonstrate continuous business value with out-of-box KPIs, drill down dashboards





Manage and govern privilege access / just-in-time administration

1

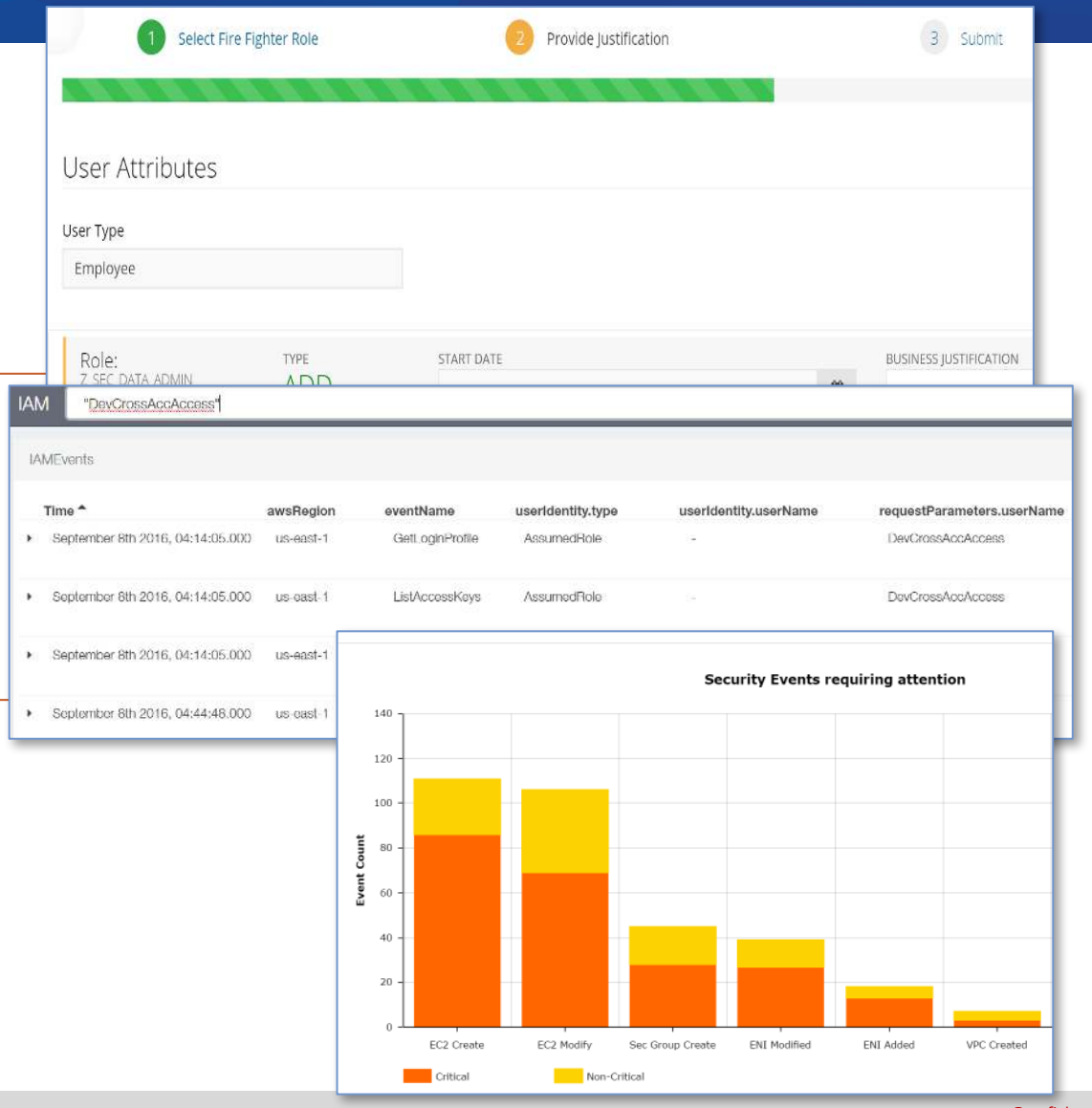
- Self-service, time-bound (checkout / check-in)
- Multi-level approval workflow for privileged access / role across multiple applications

2

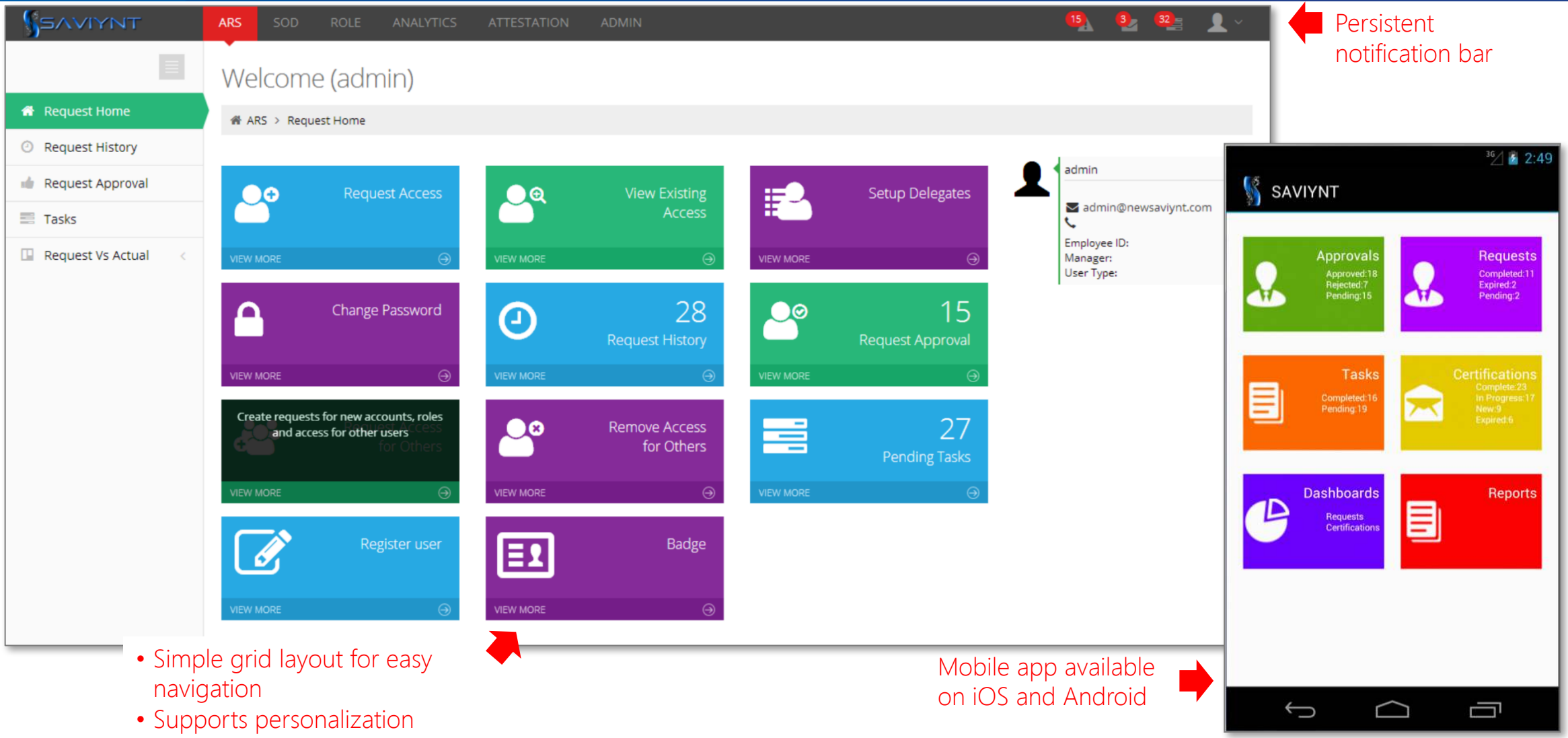
- Activity monitoring of privileged access and correlation of temporary access keys to actual identity

3

- Launch automatic certification of privileged activity
- Perform behavioral analytics to identify suspicious privileged activity



Intuitive web and mobile UI ensures acceptance by the most demanding business users

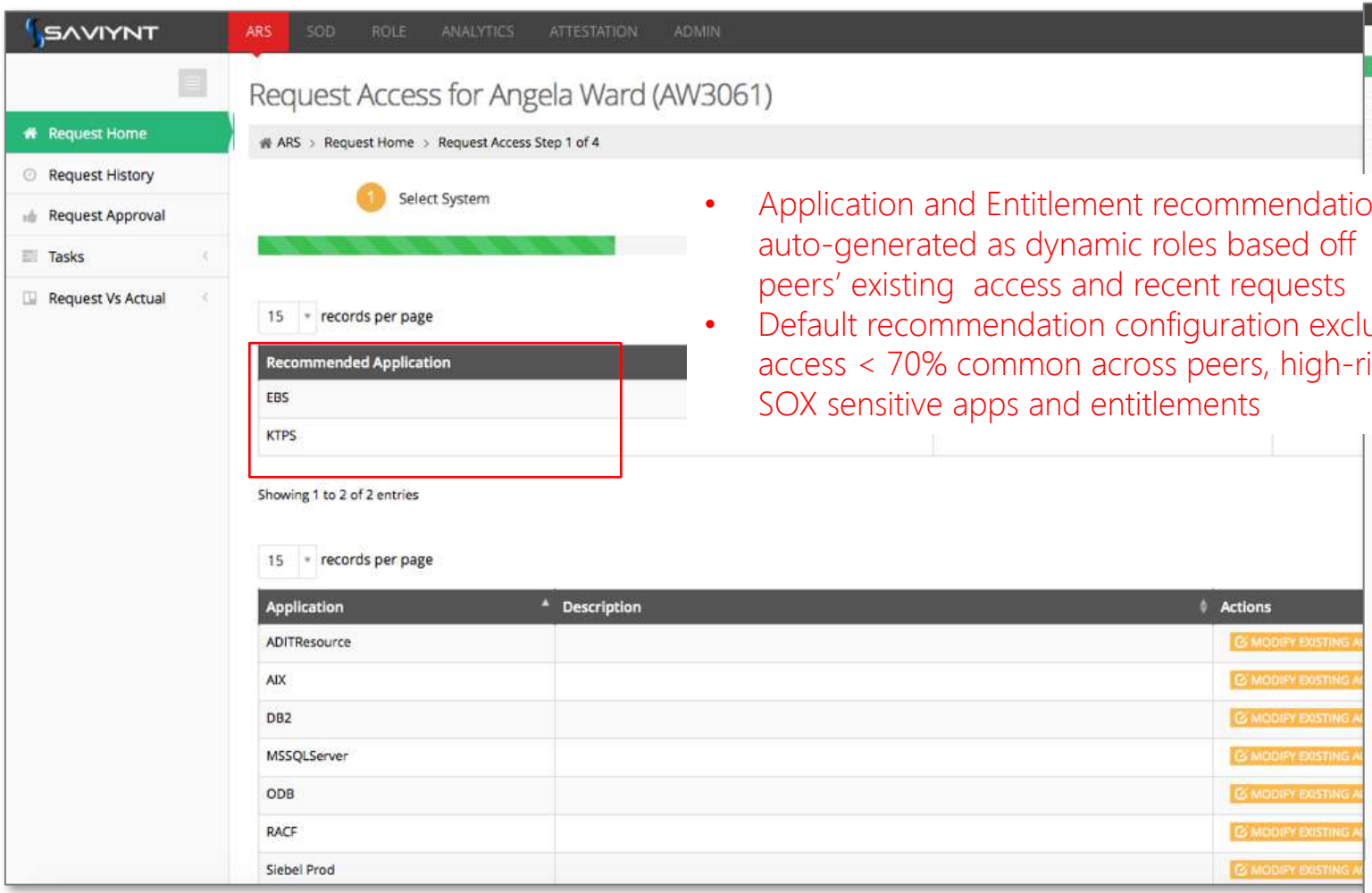


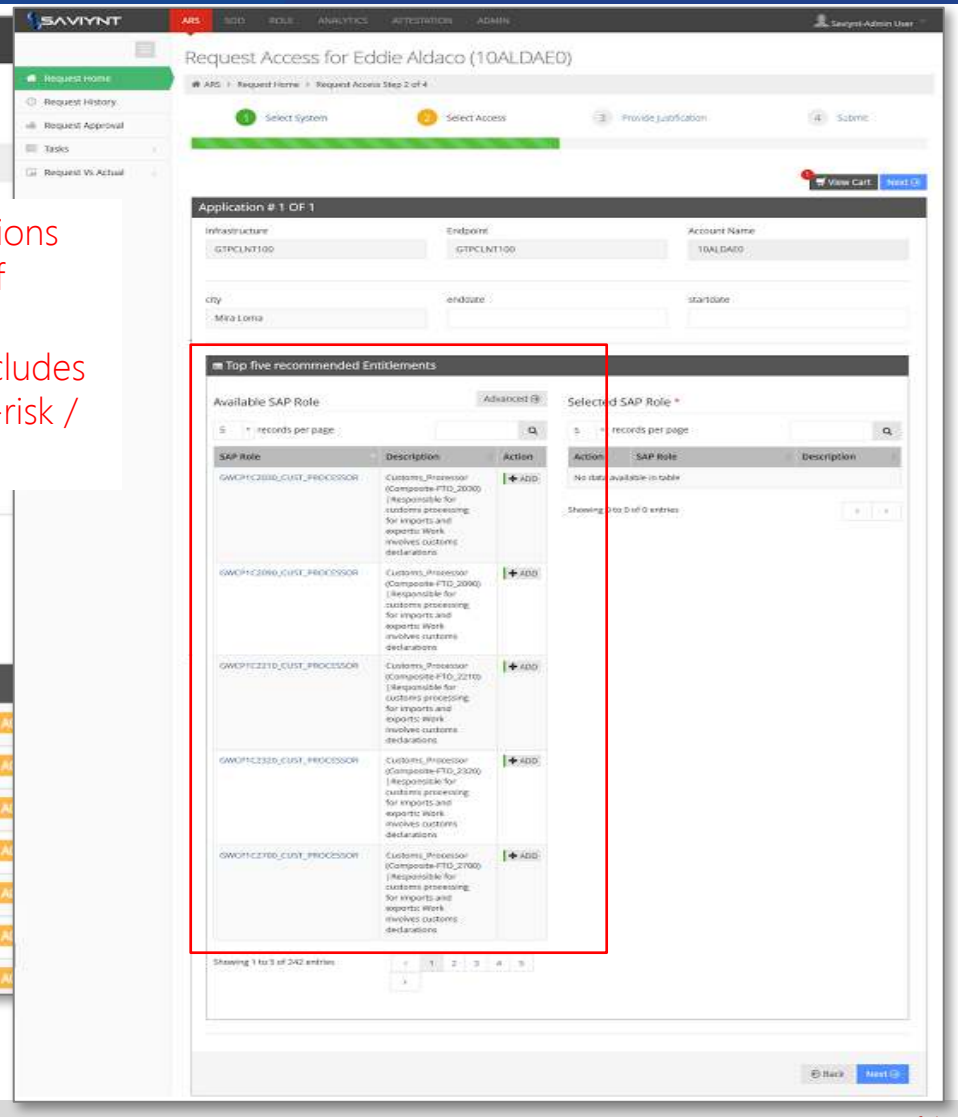
- Simple grid layout for easy navigation
- Supports personalization

Mobile app available on iOS and Android

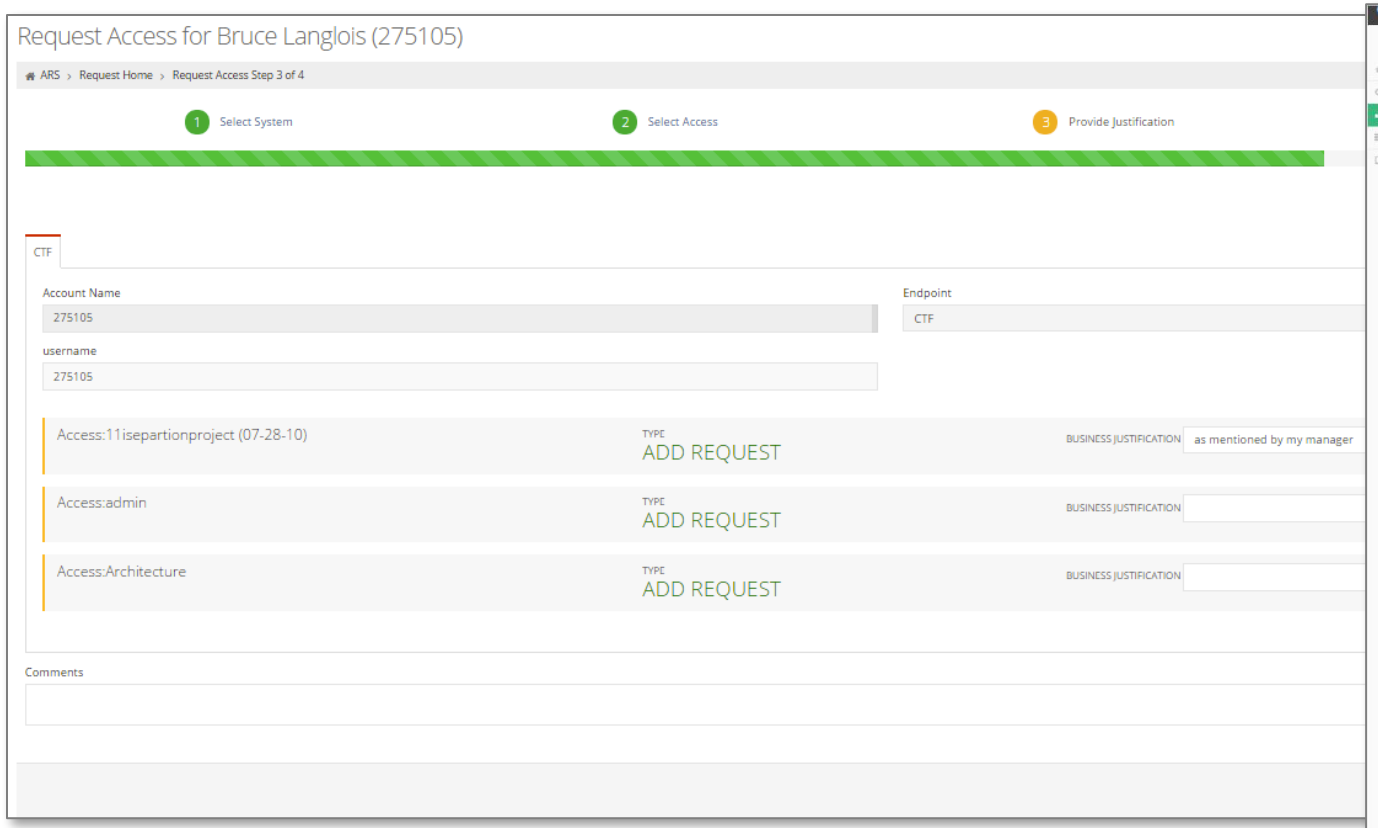
Access recommendations as decision tools for requesters, approvers and certifiers

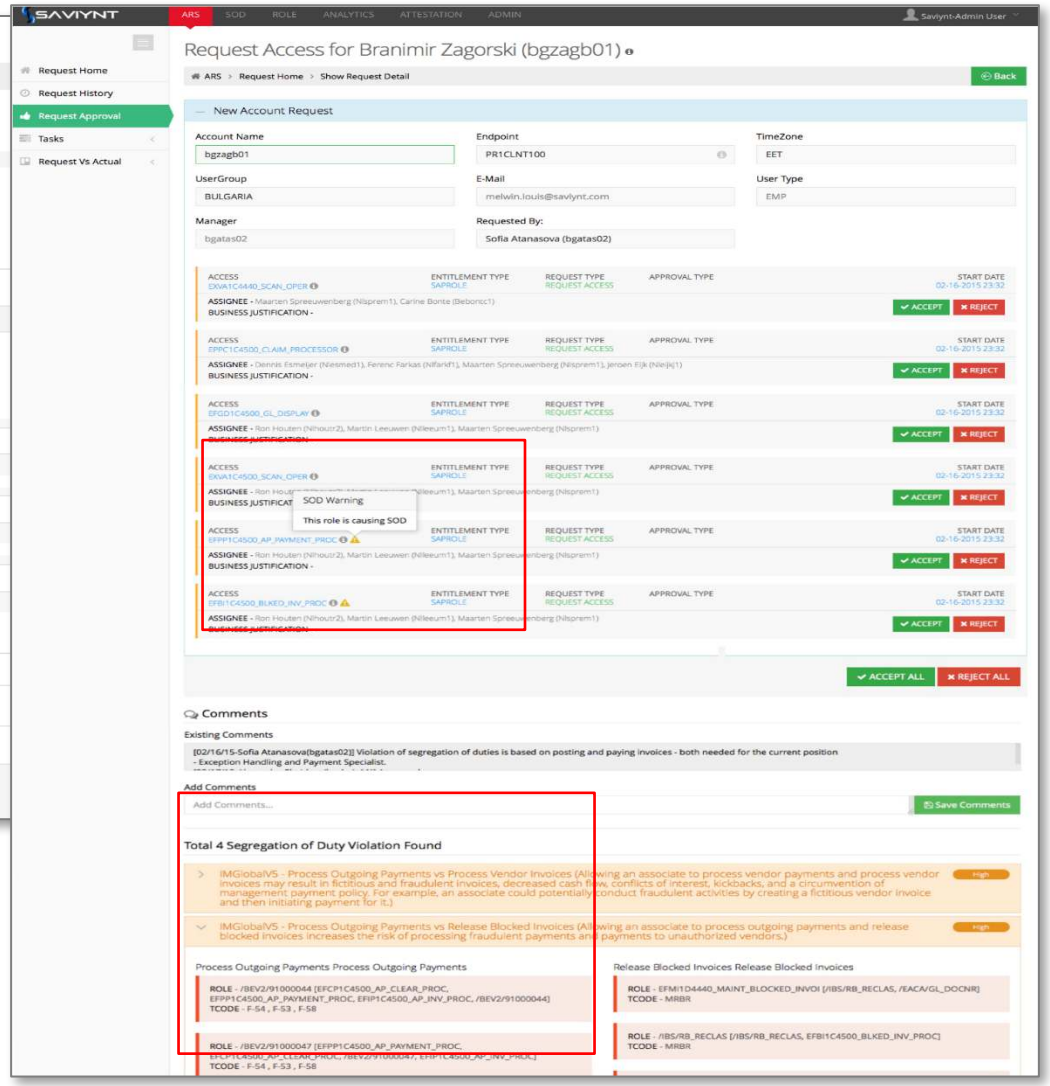
- Application and Entitlement recommendations auto-generated as dynamic roles based off peers' existing access and recent requests
- Default recommendation configuration excludes access < 70% common across peers, high-risk / SOX sensitive apps and entitlements





Inline preventive policy and SOD violation analysis





- Run-time preventive SOD and policy validation
- Risk-based enterprise workflow ensures dynamic routing of approvals based on request risk

Saviynt enables adoption of multi-dimensional RISK model and data driven analytics

RISK

Access + Usage

Static

Classification / glossary

Segregation of duty policies

Context-based access policies

Security & Compliance controls

Dynamic

Outlier / Peer analysis

Access outside role

Usage analysis

Behavior analysis

Inherent

Geolocation

User type

Threat intelligence / vulnerability

Request

- Netflix-style Recommendations
- Outlier-based Approval Confidence
- Preventive SOD Rules / Access Policies

Review

- Access Outliers
- SOD Violations
- Usage Analytics
- Critical Access

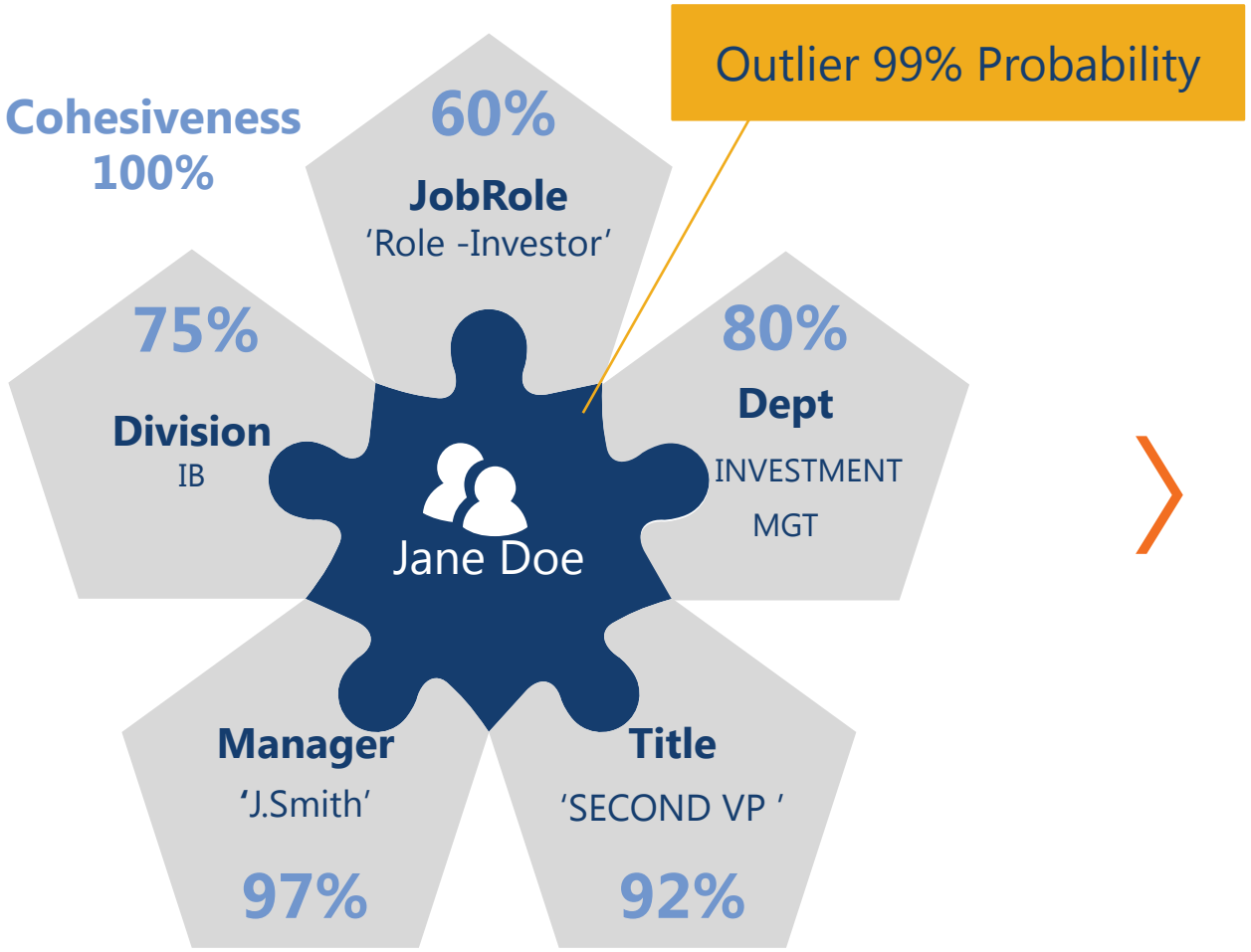
Reports / Analytics

- Out-of-band Provisioning
- Closed-loop Provisioning / Certification
- Entitlement Enrichment
- Ownership Discovery
- SLA Violations
- Risk Dashboards

Roles & Policies

- Usage Analytics
- Actual vs. potential SOD Violations
- Role vs. Actual
- Transaction Monitoring

Peer analysis to detect access Outliers or Inliers to form Access Recommendations



Request

- Netflix-style access recommendations
- Outlier-based approval confidence

Review

- Review 5-10% entitlements, get >70% revokes

Sample Risk Based Access Requests

Asset Risk / User Risk	Approve / Request	Outlier + SOD review Dynamic
Critical	Manager approval + Resource / Role Owner required	+ Security Team
High	Manager approval + Resource / Role Owner (for critical and high risk entitlement / role)	+ Security Team
Medium (Baseline)	Auto approved with manager override options	+ Security Team + Resource Owner
Low	Auto approved with manager override options	

Sample Risk Based Access Reviews

Asset Risk / User Risk	Full Access Review	Outlier Certification (Dynamic + Inherent) ~ 5% entitlements to be reviewed
Critical	Annual	Monthly risk based reviews
High	Annual	Quarterly
Medium (Baseline)	As needed	Semi annual
Low	As needed	Yearly

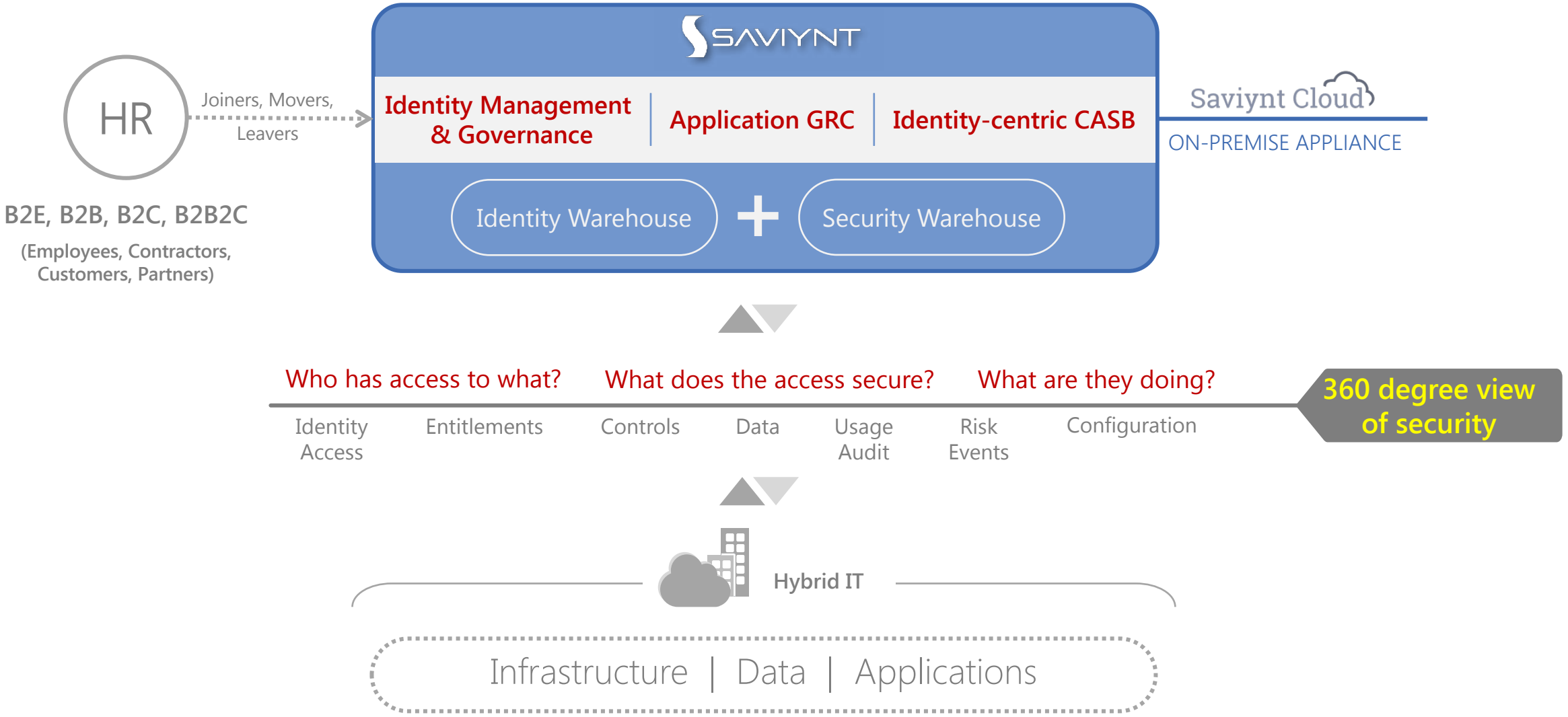
Sample risk-based role management process

Role Risk Category	Access Request (min. approval levels)	Access Certification (min. review levels)	Role Content Certification (min. review levels)
Critical	1. Manager 2. Resource owner / IT security / compliance office 3. ISO	1. Manager 2. Resource owner / IT security / compliance office	1. Role owner approval 2. Resource owner approval 3. Role governance committee approval 4. Performed semi-annually
High	1. Manager 2. Resource owner / IT security / compliance office	1. Manager 2. Resource owner / IT security / compliance office	1. Role owner approval 2. Resource owner approval 3. Role governance committee approval 4. Performed semi-annually
Medium	1. Manager	1. Manager / Resource Owner	1. Role owner approval 2. Resource owner approval 3. Role governance committee approval (optional) 4. Perform annually
Low	Auto approval if role constraints are met	Auto approval if role constraints are met	1. Role owner approval 2. Perform annually

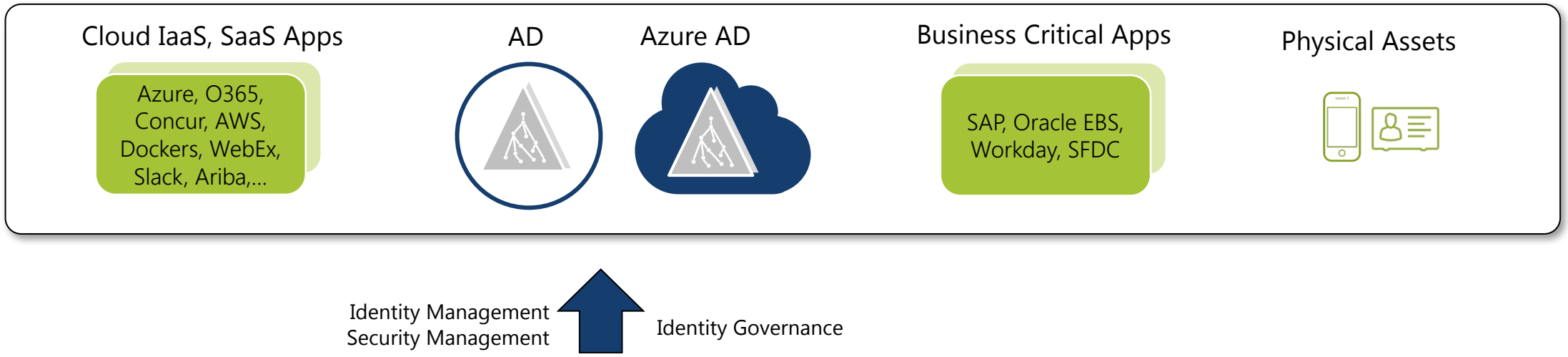
Outlying Entitlement Risk Category	Access Request	Access Certification
High	1. Manager 2. Resource owner / IT security / compliance office	1. Manager 2. Resource owner / IT security / compliance office
Medium	1. Manager	1. Manager

Note: any entitlement assigned outside of access role is default considered as medium risk or higher, although BUs could choose to have low risk

IGA 2.0 is a single pane for holistic security built from the ground-up on most comprehensive & actionable security controls and usage / risk analytics



(Saviynt + Microsoft) provides comprehensive enterprise IAM and cloud access governance for critical applications



Application

Saviynt + MIM for Critical Applications

Data

IaaS

SAVIYNT

Why Application Access Governance?

1 Most are mission critical…

Strict access control especially for privileged access is a must to secure mission critical data and transactions

Heavy compliance mandates dictate deployment and continuous monitoring of GRC and security controls

2 Authorization is complex, hierarchical & unique

Each application has potentially multiple modules with varied architecture, unique and complex access hierarchy implementation

Segregation of duty (SOD) enforcement / fraud management is complex, needs automation and deep integration with application's access hierarchy

3 Typically managed in a silo…

Enterprise applications have a standalone security solution, leading to inconsistencies and redundancy in policy enforcement

APPLICATION ACCESS GOVERNANCE

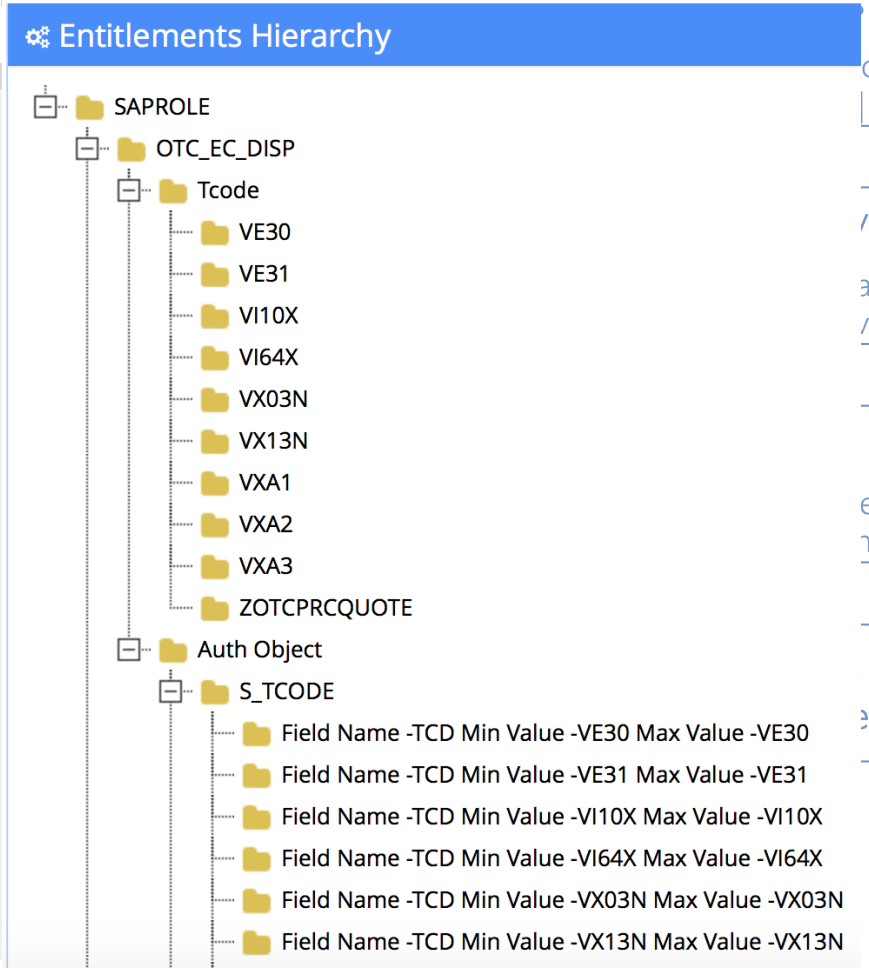
- Application SOD Management & Remediation
- Mitigating Controls Management
- Usage Analytics
- Role / Privilege Design & Governance
- Emergency Access Management
- Security Controls

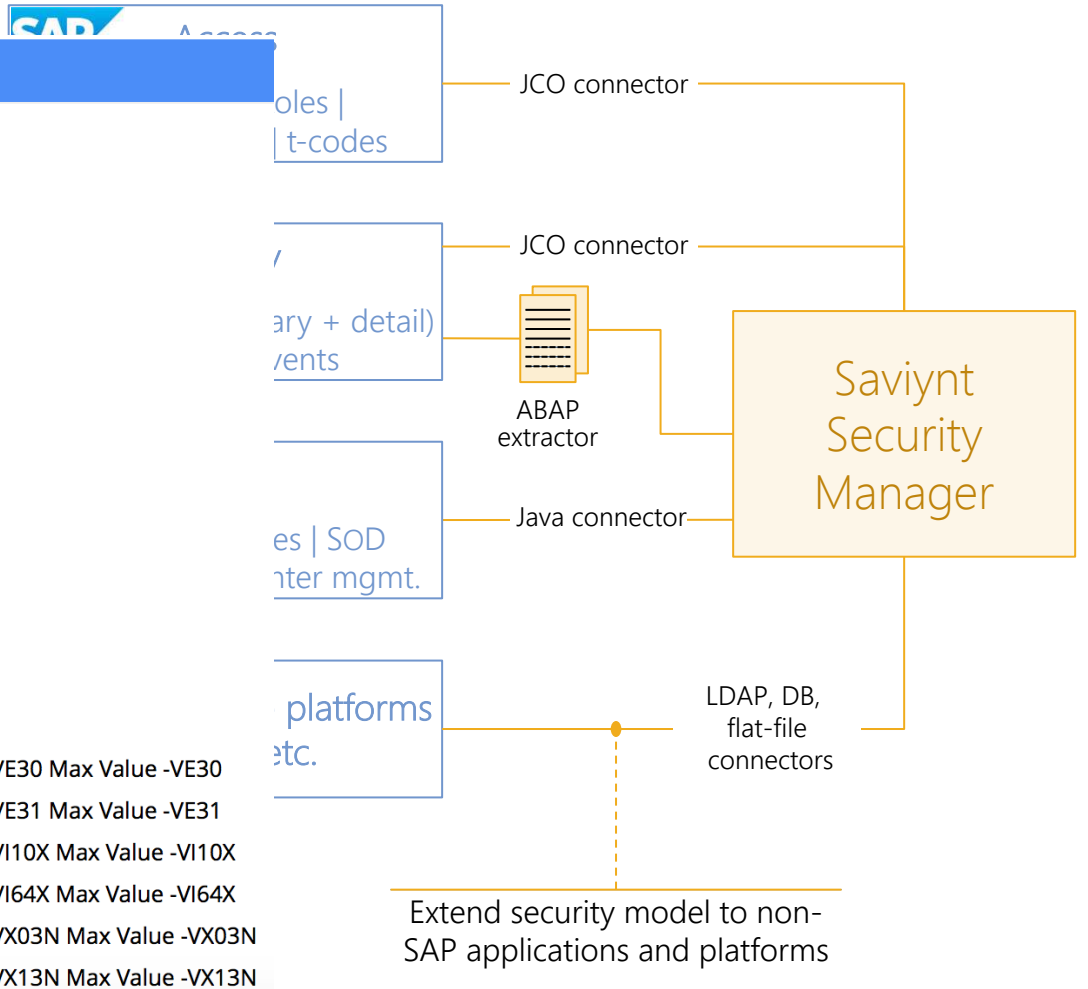
Saviynt for SAP

SAP Security

- **Continuous controls monitoring** with 100+ SAP controls
- SoD analysis, **remediation** and workbench for management
- Privilege access risk analysis / monitoring
- **Actionable usage** analysis and analytics
- Risk-based access certification based
- Firefighter / emergency access review
- **License management**
- Custom transactions and program review
- **Vulnerability & Security Configuration** Management
- Role engineering based on statistical algorithms, includes **simulation and version control**

SAP





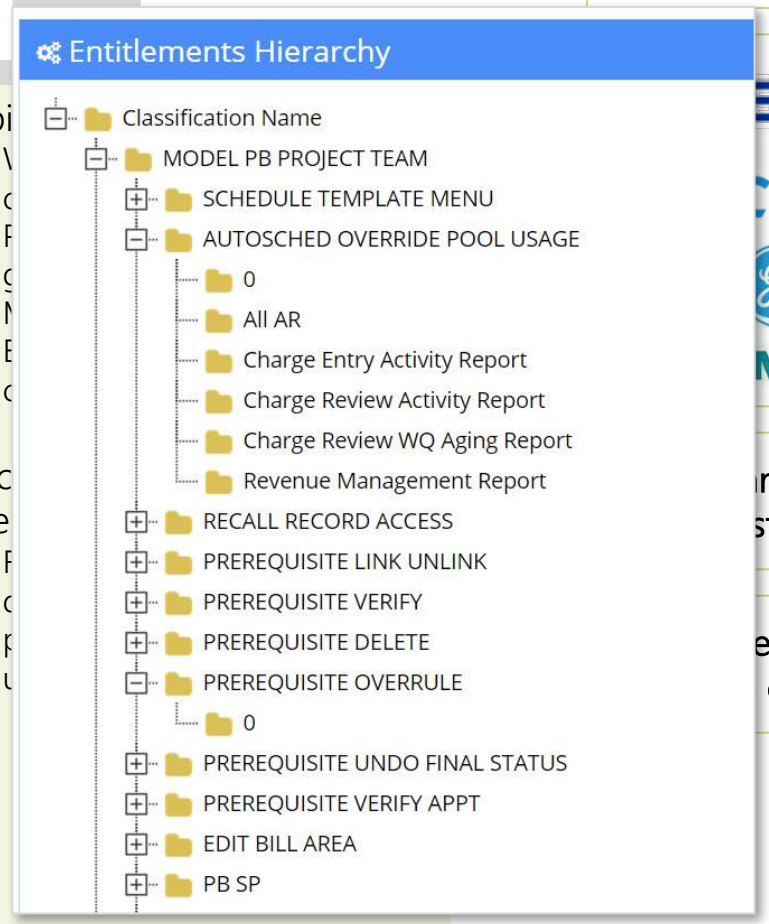
Saviynt for Healthcare applications

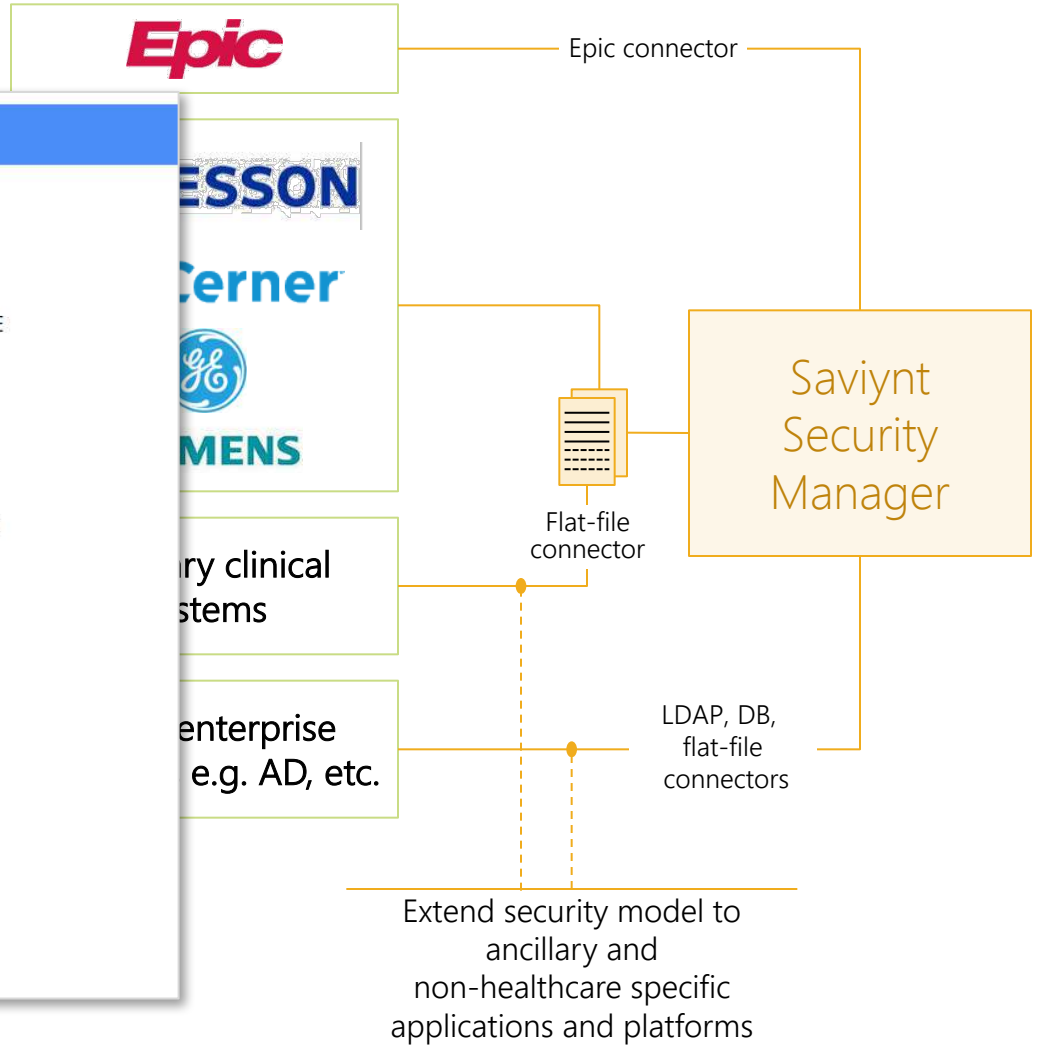
Healthcare Security

- Security **controls testing**
- (Sub-) **Template analysis** for overlapping access & SoD
- Template / class management including **version control**
- Periodic template / class **owner review**
- **170+ out of box rules for SoD analysis and remediation** across all clinical and financial modules
- 50+ out of box security controls
- Role engineering
- Role life-cycle management
- **Advanced simulation** before applying role and SoD changes
- **Access and usage** reporting
- Intuitive **web and mobile** access request system

Epic

- Epi
  - V
  - F
  - M
  - E
- Mc
  Sie
  - F

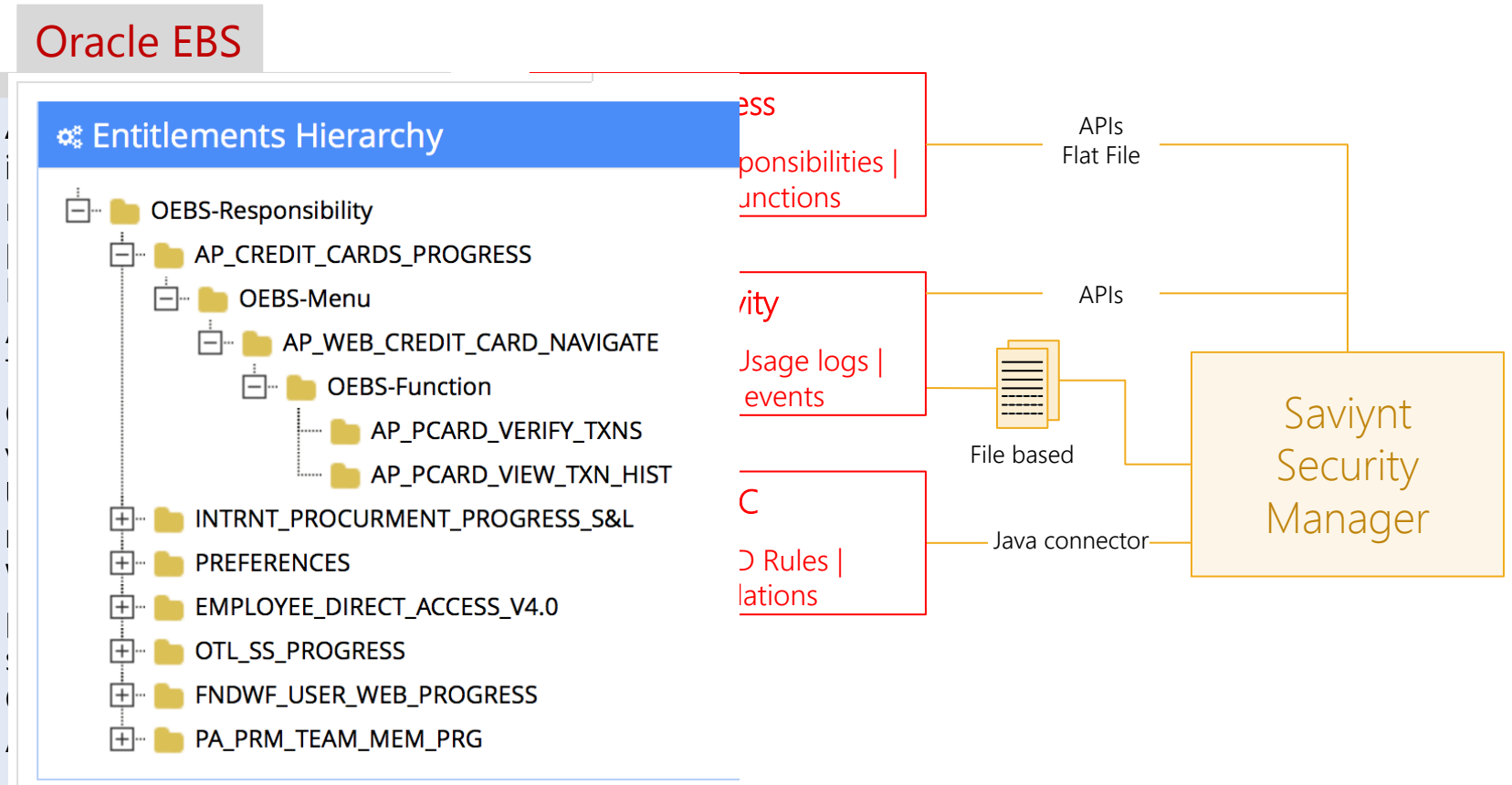




Saviynt for Oracle E-Business Suite

Oracle EBS Security

- Fine grained access control with the ability to import the entire stack of access
- 150+ out of the box security controls and remediation workbench
- **Functional Application Role Engineering** based on advanced statistical algorithms
- Saviynt engineered roles are **SoD free** and have **no entitlement redundancy**
- **Responsibility consolidation** checking the underlying functions
- Custom responsibility / functions review
- Role life-cycle management with version control and ability to roll back



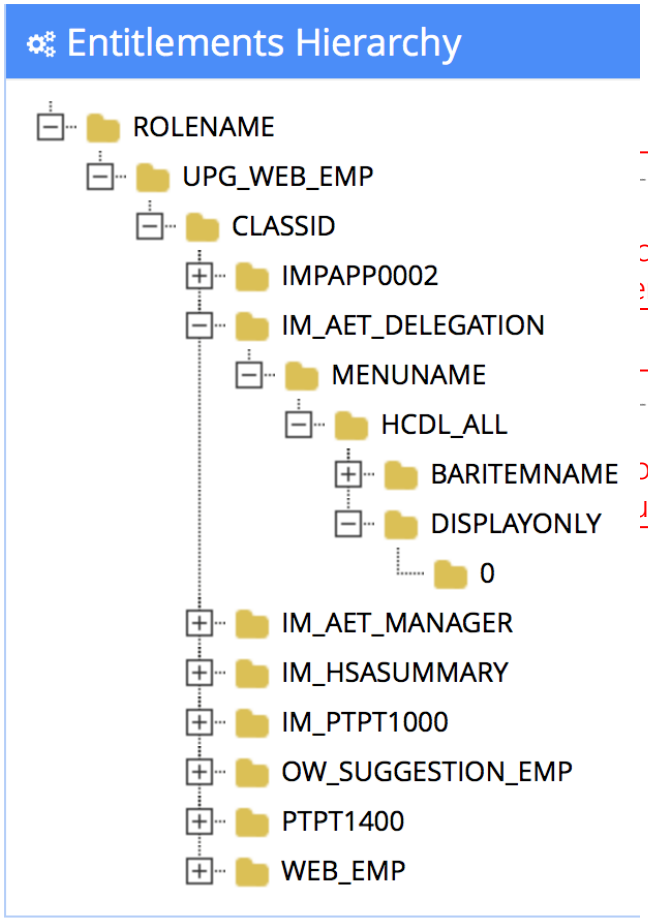
Saviynt for PeopleSoft

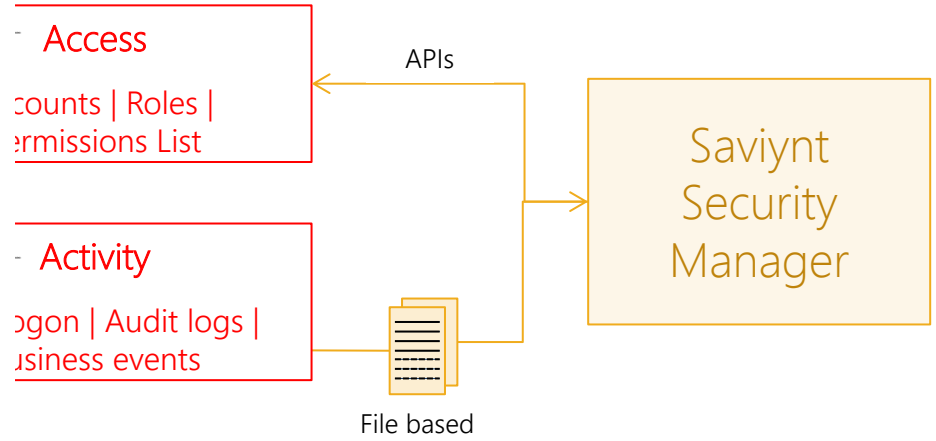
PeopleSoft Security

- Fine grained access control with the ability to import the entire stack of access
- **50+ out of the box security controls** and remediation workbench
- **Functional / Application Role Engineering** based on advanced statistical algorithms
- Saviynt engineered roles are **SoD free** and have **no entitlement redundancy**
- **Role consolidation** checking the underlying permissions
- Role life-cycle management with version control and ability to roll back

- A
- M
- A
- W

Peoplesoft



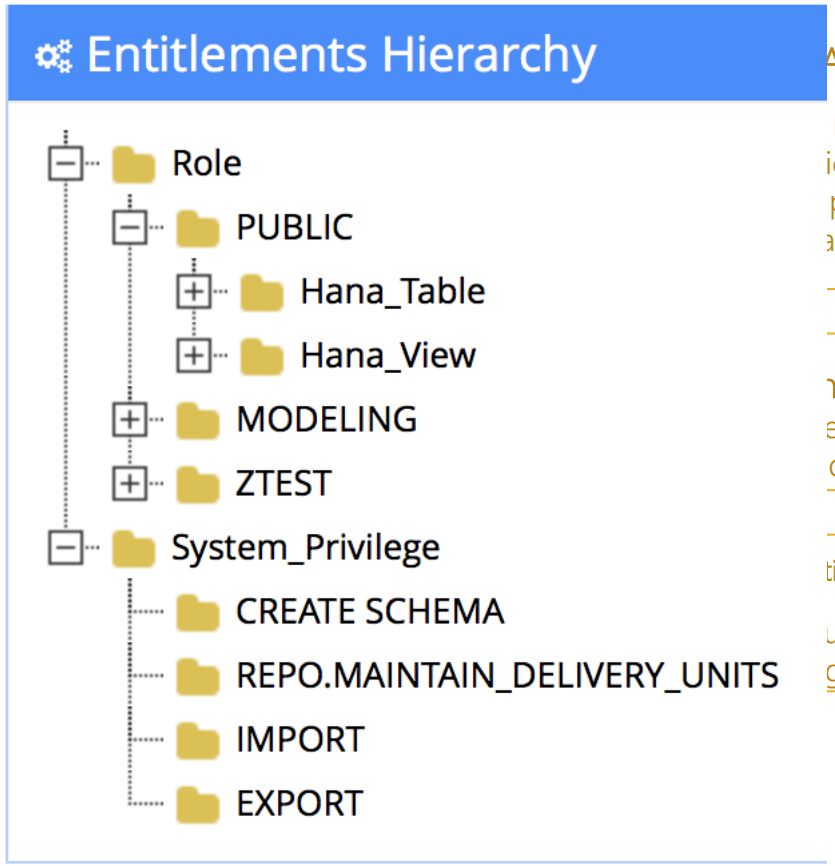


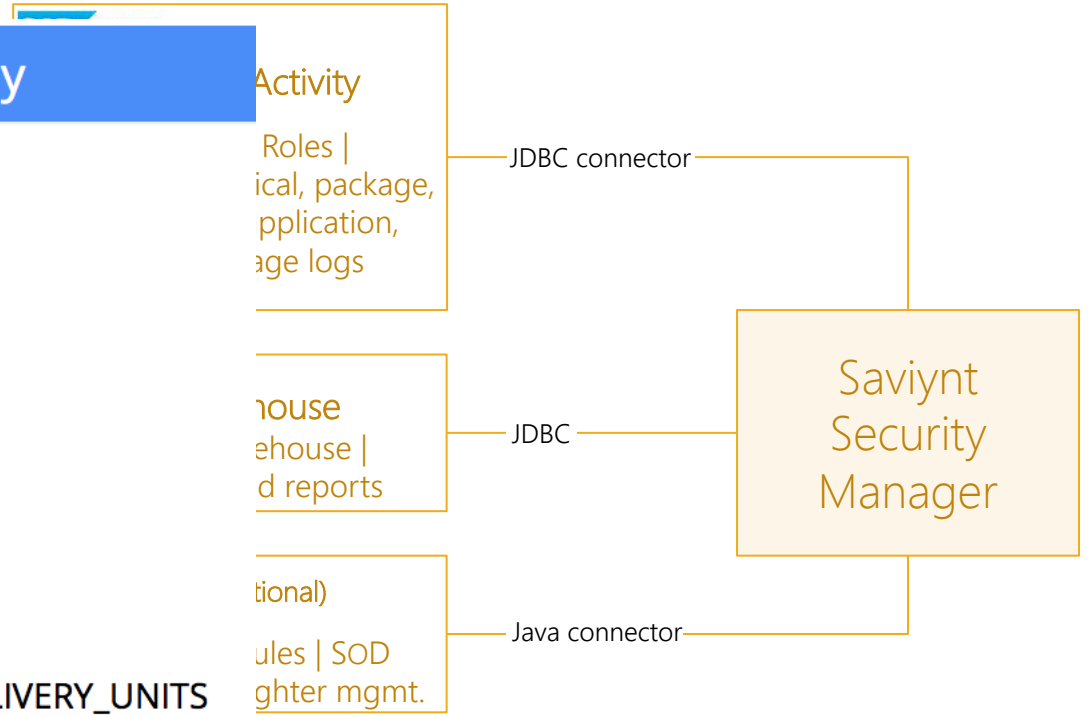
Saviynt for Big Data platforms

SAP HANA Security

- **Access Abstraction layer** to translate business rules in to complex database object models
- Automatic creation of optimal **roles and privileges** based on business rules
- Automated **provisioning** of controls for HANA
- **User management** with built-in security and compliance control checks
- **Real-time audit / alert** of access and any violations including out-of-band provisioning, SoD conflict, etc.

HANA



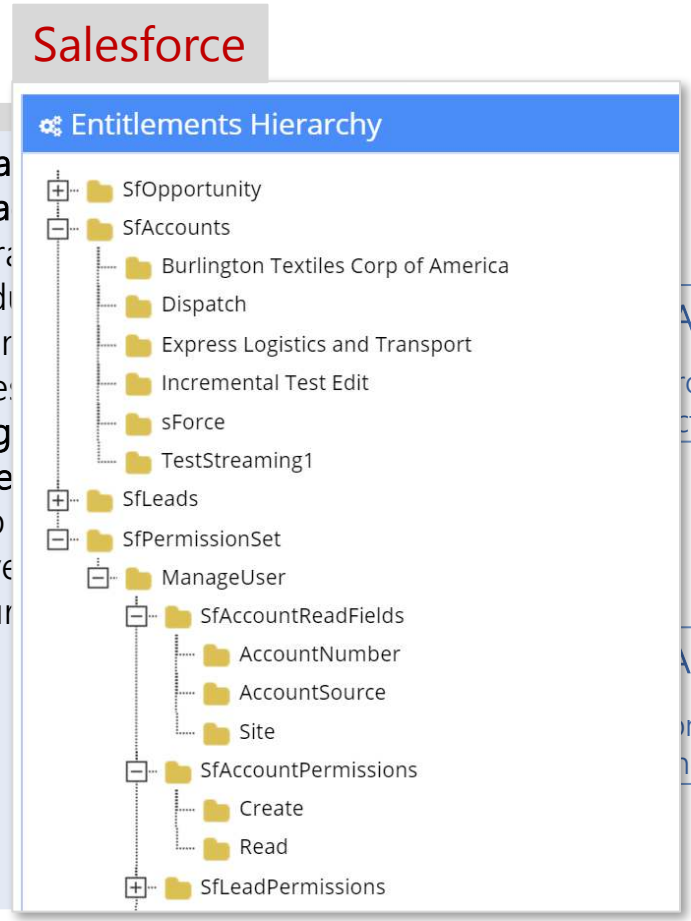


Saviynt for Salesforce.com

Salesforce Security

- Fine grained access control with the ability to import the entire stack of access – profiles, permission sets, objects, object fields, etc.
- Out of the box security controls and remediation workbench
- **Application Role Engineering** based on advanced statistical algorithms
- Saviynt engineered roles are **SoD free** and have **no entitlement redundancy**
- **Profile / Role consolidation** checking the underlying functions
- Custom profile review
- Role life-cycle management with version control and ability to roll back

- **Adva**
  impa
  migra
  produ
- Minir
  Acce
- **Usag**
  reme
- Web
  preve
  secur



Access

ofiles | Permission
t Fields | Records

Activity

n | Usage logs |
ness events

APIs

File based

Saviynt Security Manager

Application

Saviynt + MIM for Cloud Applications

Data

IaaS

SAVIYNT

Why IaaS Access Governance?

1 High risk due to privileged access…

Compromise of a single AWS / Azure Account can lead to breach of entire datacenter on Cloud

DevOps users can have privileged access to IaaS services / workloads / policies and CI/CD tools in their VPCs

2 Complex services and entities to manage…

Access control extends beyond users to entities such as VPCs, subnets, instances, DBs, data objects, etc. Policies are usually defined as JSON objects

Multiple points of failure such as incorrect workload tags, misconfigured instances, open ports / open access, non-rotated certificates, etc.

Need to keep pace with IaaS innovation e.g. Amazon released 200+ capabilities and services for AWS in 2015 alone

3 Scale and intelligence is a must…

Visibility of a single AWS account needs integration with at least 5 log sources including CloudWatch, CloudTrail, VPC flow logs, AWS Config, several DevOps tools, etc.

Large volumes of user access, configuration and activity data need smarter tools such as intelligence and analytics to identify riskiest users and access

amazon web services™

GitHub

Windows Azure

CHEF

docker

puppet labs

INFRASTRUCTURE ACCESS GOVERNANCE

- 200+ Risk Controls Library
- Near Real-time Preventive Workload Security
- DevSecOps & Secure CI/CD
- Entity Life-cycle Management
- Privilege Access Governance
- User Behavior Analytics

Saviynt IaaS Access Governance

Secure IaaS platforms such as AWS, Azure and DevOps

EC2 | RDS | ELB | EBS | S3 | AWS IAM | Chef Puppet (DevOps) | amazon web services™ Ecosystem

CloudTrail, CloudWatch, AWS Config / SNS, AWS APIs, DevOps logs, VPC flow logs

Discover

- API-based Connectors for IaaS & DevOps Tools
- IAM Users, Access Policies, Configuration Objects
- Unstructured Data
- Audit & Usage Logs

Analyze

- 200+ Risk Signatures
- Risk Intelligence
- Peer Group Analytics
- Access Policy / Configuration Analysis
- Data Classification

Protect

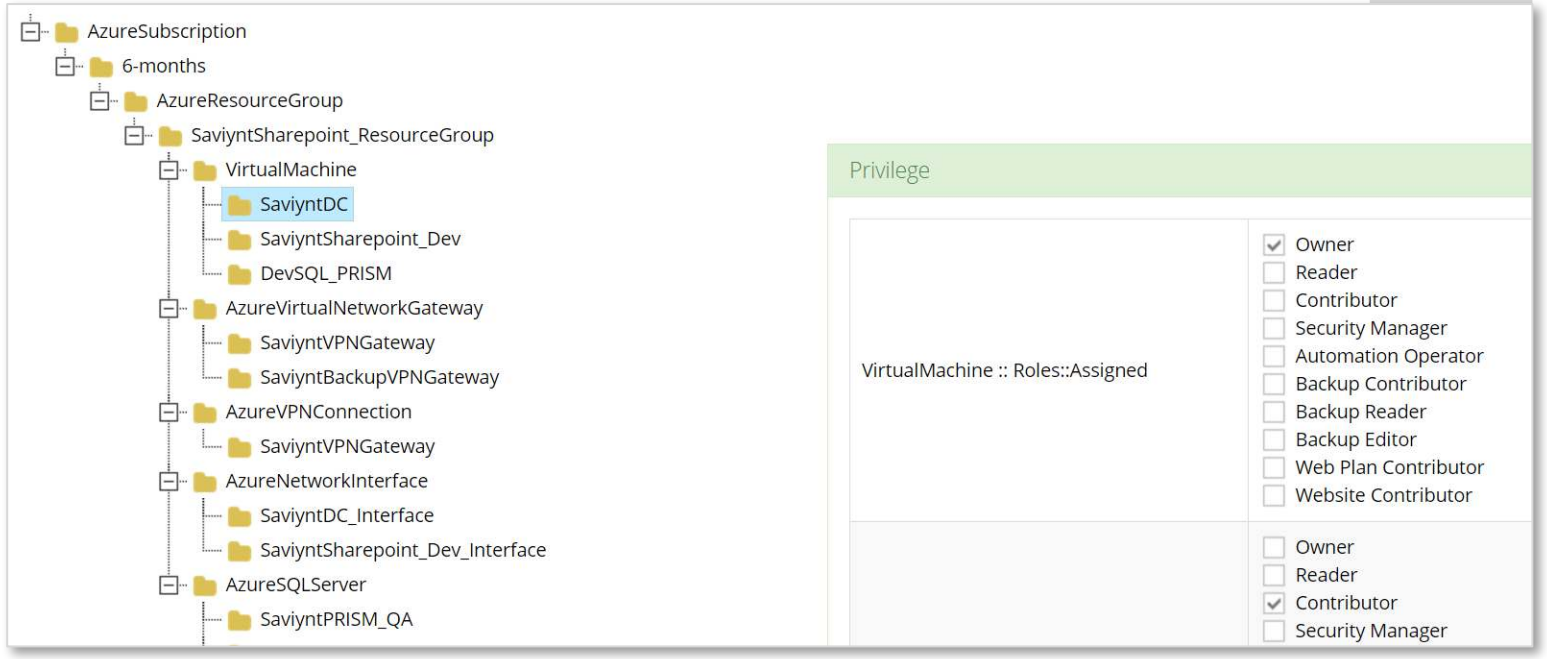
- Near Real-time Preventive Security
- Review / Approve Access
- Infrastructure Access Policies (RBAC / ABAC)
- Privilege Access Management / Governance
- Segregation of Duty rules

Manage

- Access Request / Review
- Access Provisioning
- Continuous Controls Monitoring
- Reporting Dashboards
- User Behavior Analytics

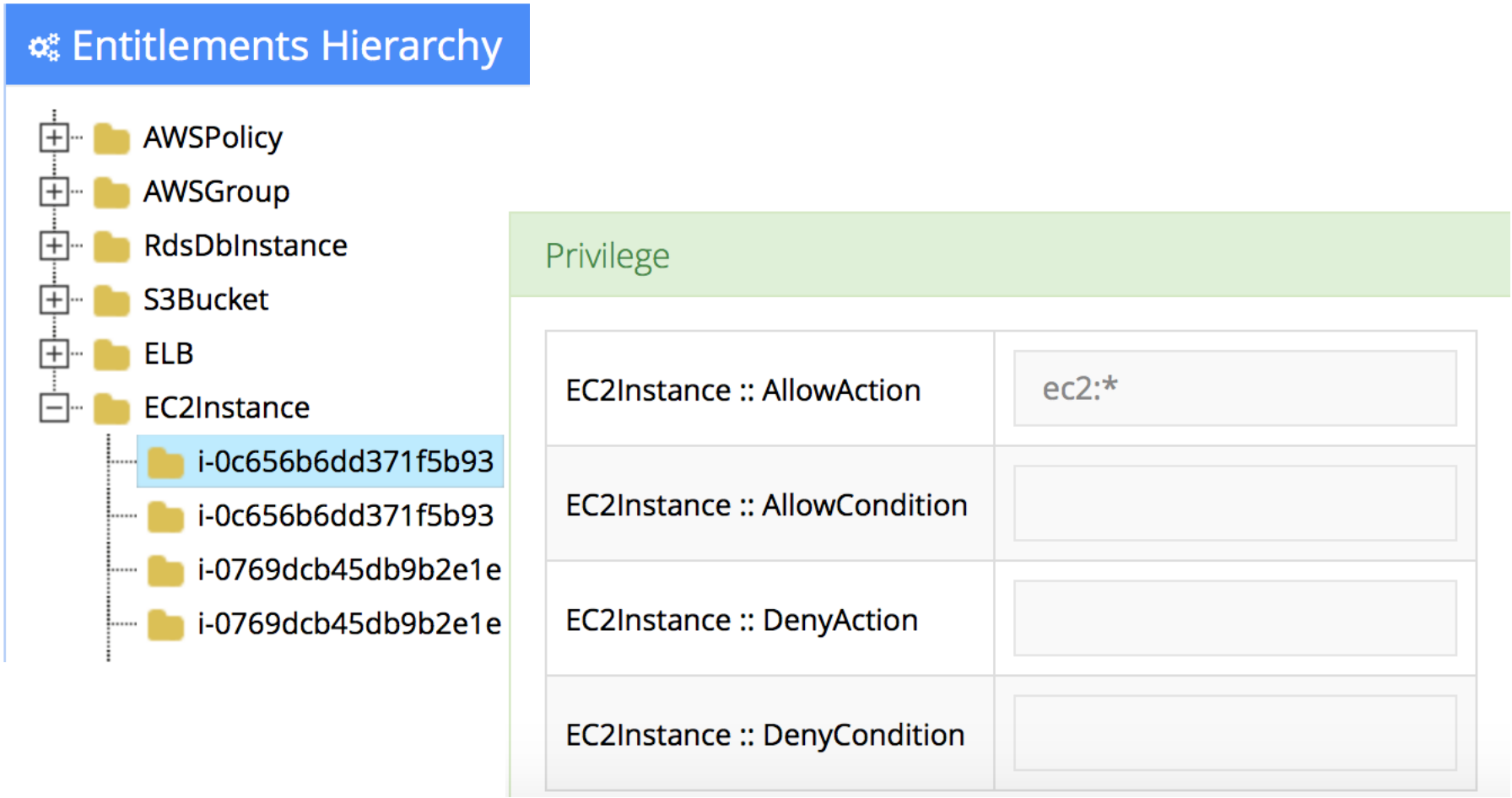
...with flexibility of data sparse vs. data full connector integration

Azure



...with flexibility of data sparse vs. data full connector integration

AWS



Integrated with security warehouse to store audit and usage logs

AWS


```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJHYEU2RSSDRXOELEM:admin@saviyntcloud.net",
    "arn": "arn:aws:sts::661222050851:assumed-role/SaviyntCiti-SaviyntSuperAdministrator-6UNP1H2JPILG/admin@saviyntcloud.net",
    "accountId": "661222050851",
    "accessKeyId": "ASIAIQT6JFCE7T3UXIZA",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2016-06-13T18:54:18Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJHYEU2RSSDRXOELEM",
        "arn": "arn:aws:iam::661222050851:role/SaviyntCiti-SaviyntSuperAdministrator-6UNP1H2JPILG",
        "accountId": "661222050851",
        "userName": "SaviyntCiti-SaviyntSuperAdministrator-6UNP1H2JPILG"
      }
    }
  },
  "eventTime": "2016-06-13T18:55:52Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "DeleteUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "107.21.87.59",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "userName": "dev-admin-fed"
  },
  "responseElements": null,
  "requestID": "737caf5e-3198-11e6-a86a-21f93c79d401",
  "eventID": "fa1c1e2d-8185-498d-b2cc-2a1e804087a0",
  "eventType": "AwsApiCall",
  "recipientAccountId": "661222050851"
}
```

Why Data Access Governance?

1 Access model is discretionary…

A user with read-only access can share a sensitive document with any internal or external user

Access escalation or privilege modification performed by Privileged User can go unnoticed

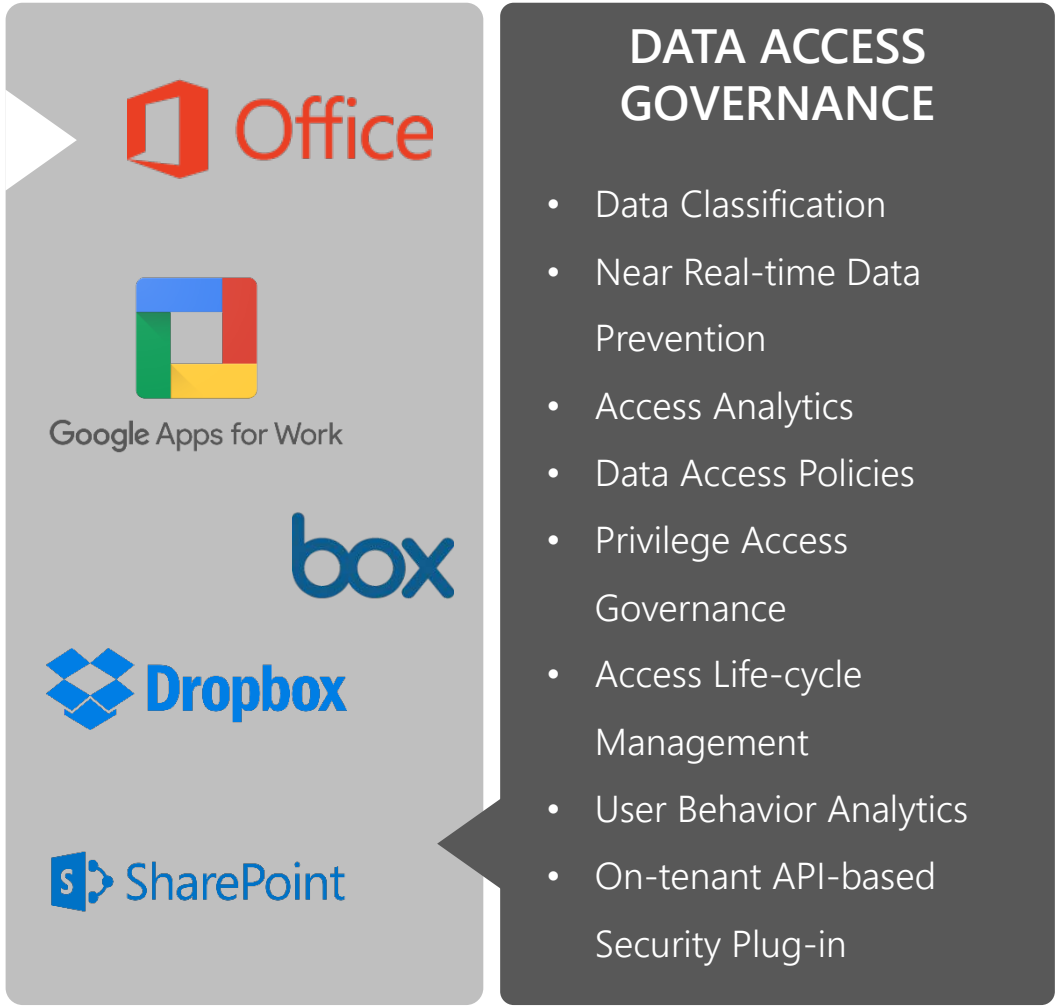
2 Files can be exchanged without 'sharing'…

A user can create 'share link' for a document and distribute it out-of-band leaving no trace and open to anonymous access

3 Data encryption is not enough…

It protects only against external rogue access or if service provider is compromised. Authorized users with appropriate access still get access to encrypted data

Gateway-based encryption strategies might not work well with mobile access

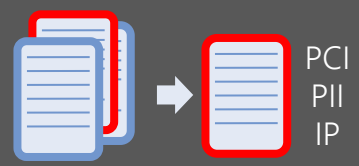


Saviynt Data Access Governance

Secure unstructured data in Cloud, Big Data and Enterprise platforms

Office 365
Box
Google Apps
MS SharePoint 2013
Dropbox
Hadoop

Discover



- API-based Connectors on Cloud Tenant
- Access Hierarchy
- Unstructured Data
- Audit & Usage Logs

Analyze

- Data Classification
- 50+ Risk Signatures
- Risk Intelligence
- Peer Group Analytics
- Access Hierarchy Analysis

Protect

- Near Real-time Quarantine
- Review / Approve Access
- Data Access Policies (RBAC / ABAC)
- Encrypt / IRM
- Multi-factor Authentication*
- Privilege Access Governance

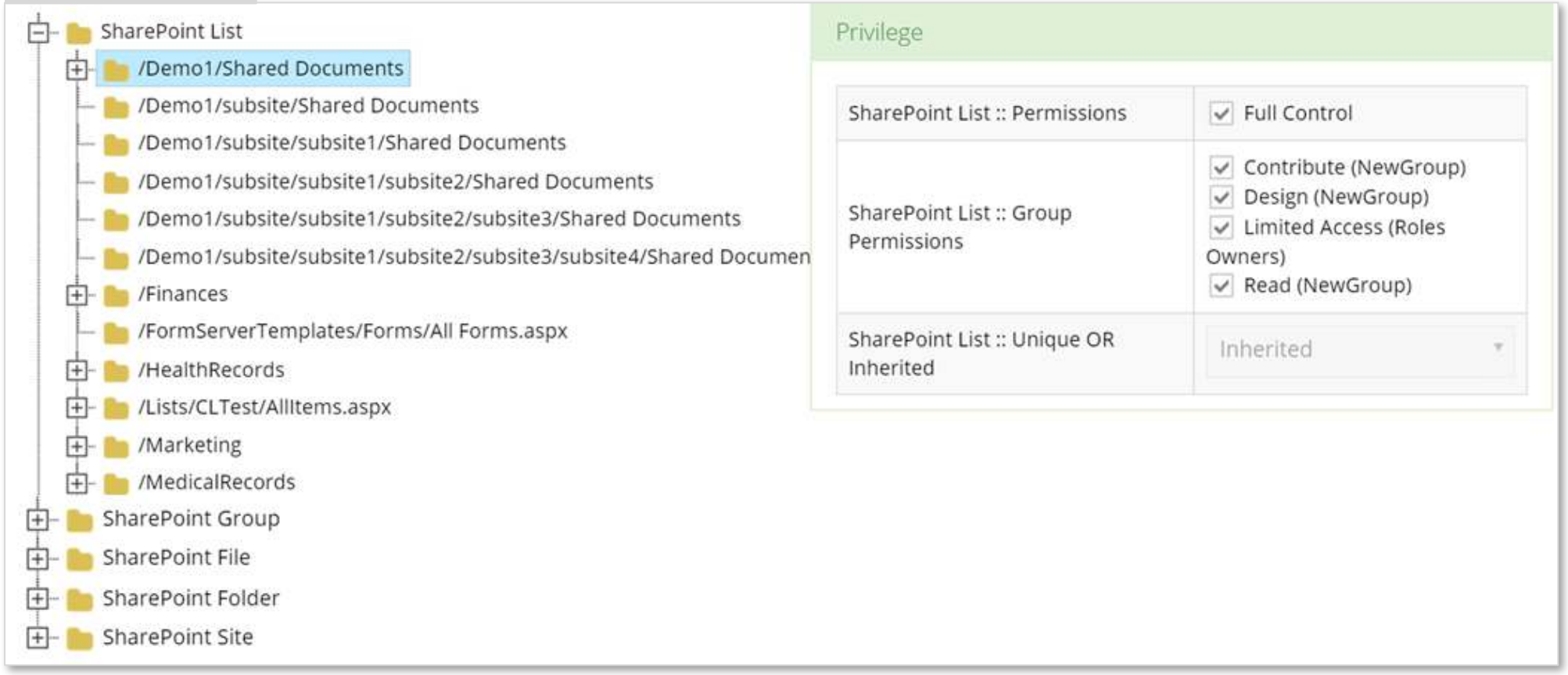
Manage

- Access Request / Review
- Access Provisioning
- Continuous Controls Monitoring
- Reporting Dashboards
- User Behavior Analytics

* Via partners e.g. okta, Oracle, Ping, RSA,...

...with flexibility of data sparse vs. data full connector integration

Office 365



Integrated with security warehouse to store audit and usage logs

Cross platform Data Governance

Edit Scan Rule | Entitlements

Entitlement

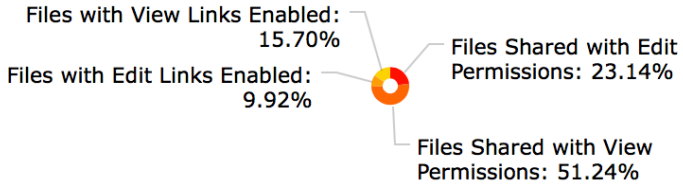
15 Records Per Page

Scan Rule	Entitlement Value	Endpoint	Match Count	Violation Probability
US SSN	PatientRecords.txt	Salesforce	9	HIGH
US SSN	AetnaRecords.txt	Salesforce	9	
US SSN	PatientRecords.txt	Salesforce	9	
US SSN	AetnaRecords.txt	Salesforce	9	
US SSN	PatientRecords11.txt	Salesforce	9	
US SSN	PatientRecords.txt	Salesforce	9	
US SSN	PatientRecords11.txt	Salesforce	9	HIGH
US SSN	AetnaRecords.txt	Salesforce	9	HIGH
US SSN	AetnaRecords.txt	Salesforce	9	HIGH

Box 647 Files Count RELOAD

Box 0 Shared Links without Expiry Count RELOAD

Office 365 External Sharing of Sensitive Files



Box 117 Folders Count RELOAD

Box 84 Shared Links Count RELOAD

Box 25 Shared Links without Password Count RELOAD

Box 316 PII Sensitive Files Count RELOAD

Box 84 PCI Sensitive Files Count RELOAD

Box 26 Collaborators Count RELOAD

Application

Customer Access Governance & Intelligence

Data

IaaS

SAVIYNT

Why IDM for External Entities?

1 Need to support Digitalization…

Involves empowering customers and partners with self-service tools and opening up traditionally closed IT processes

Plug-n-play micro services such as ID proofing, subscription management, granular delegated administration, ID linking, case management, etc.

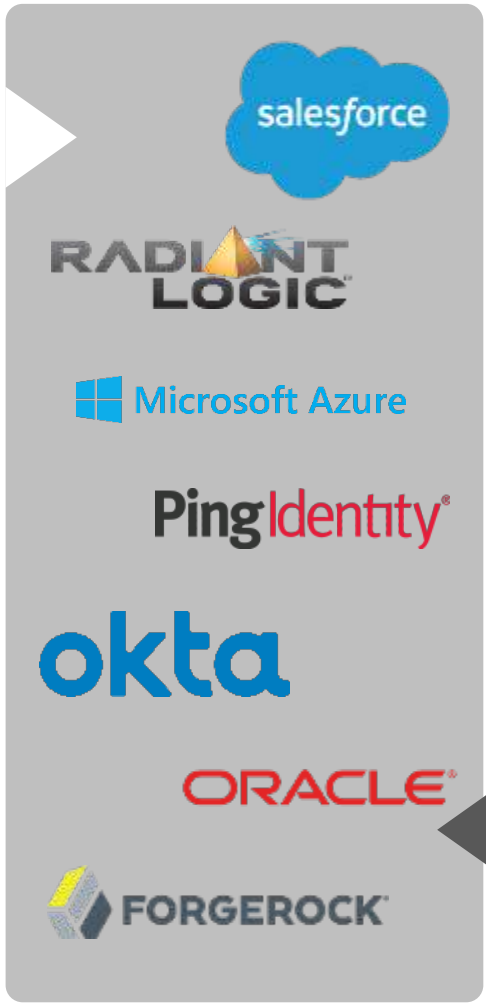
2 Security must scale to millions of entities…

Solution needs to provide / govern granular access control over portal services, attributes and fields

Such scale requires IDM solution to be data sparse and support fine-grained delegated administration and profile management

3 IDM integration needs to run deep…

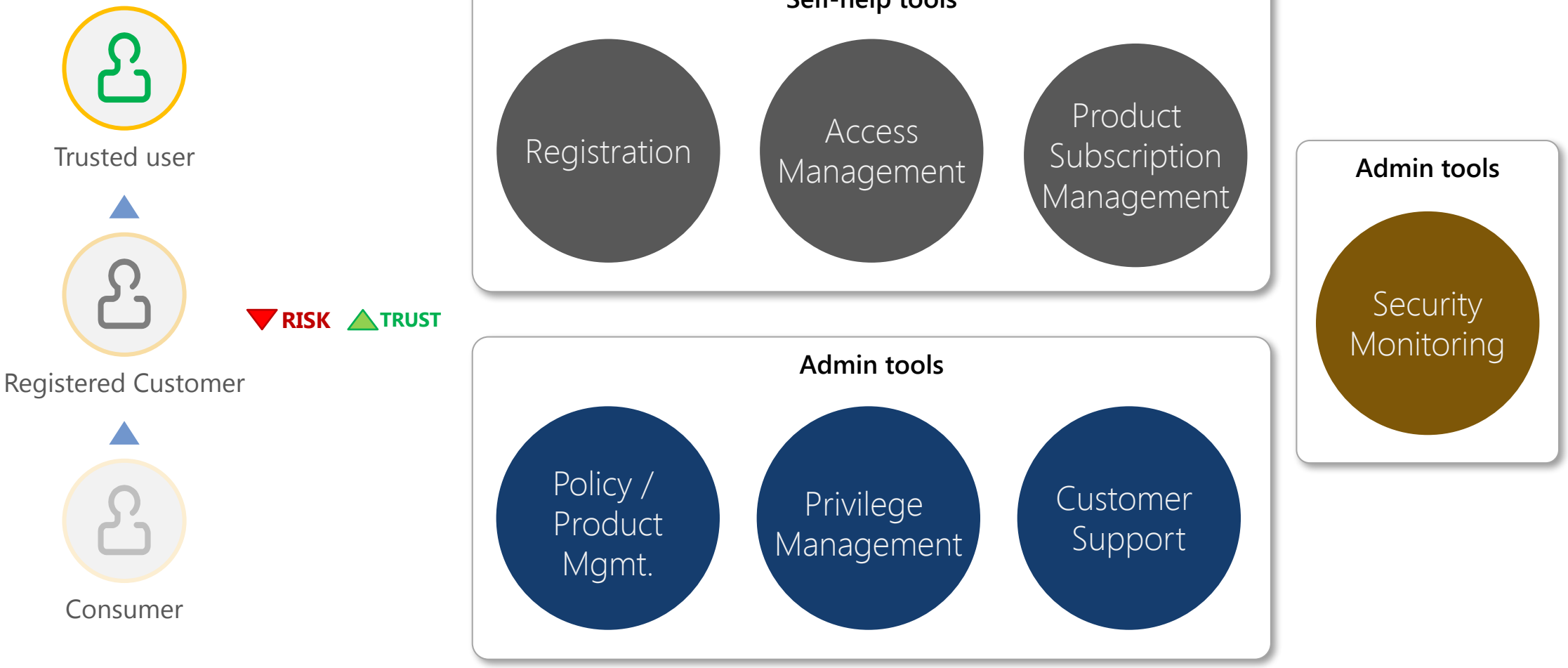
Needs to support extensive APIs and flexible configuration to seamlessly integrate with rest of customer experience – Portal, CSRs, legacy identity stores, fine-grained authorization stores,…



SAVIYNT FOR EXTERNAL ENTITIES

- Scale to Millions of Entities with Data Sparse
- ID Proofing Support
- Granular Attribute-based Access Control
- Self-service / Delegated Administration
- Profile Management (MFA, federation preferences, etc.)
- LDAP Group Provisioning
- Privileged Access Management

Path to creating a trusted customer by lowering / managing risk seamlessly

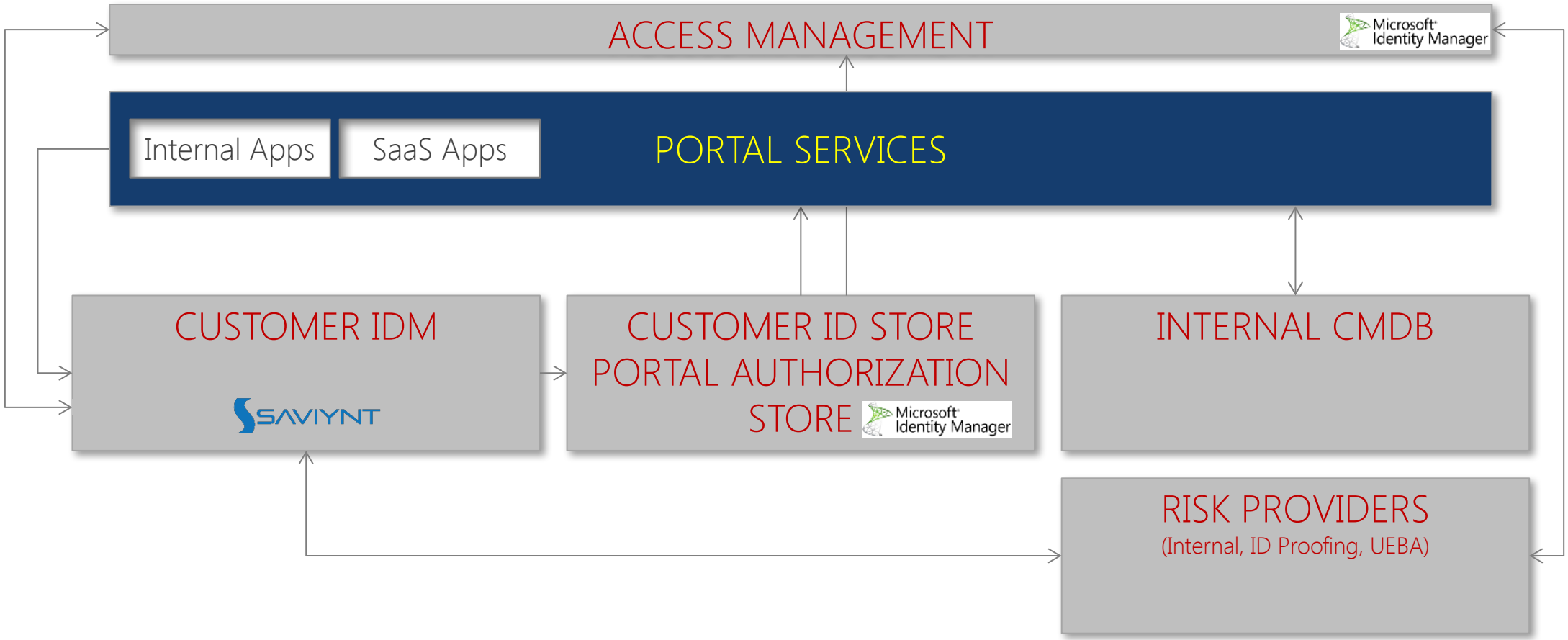


Key tenets of customer identity management and governance

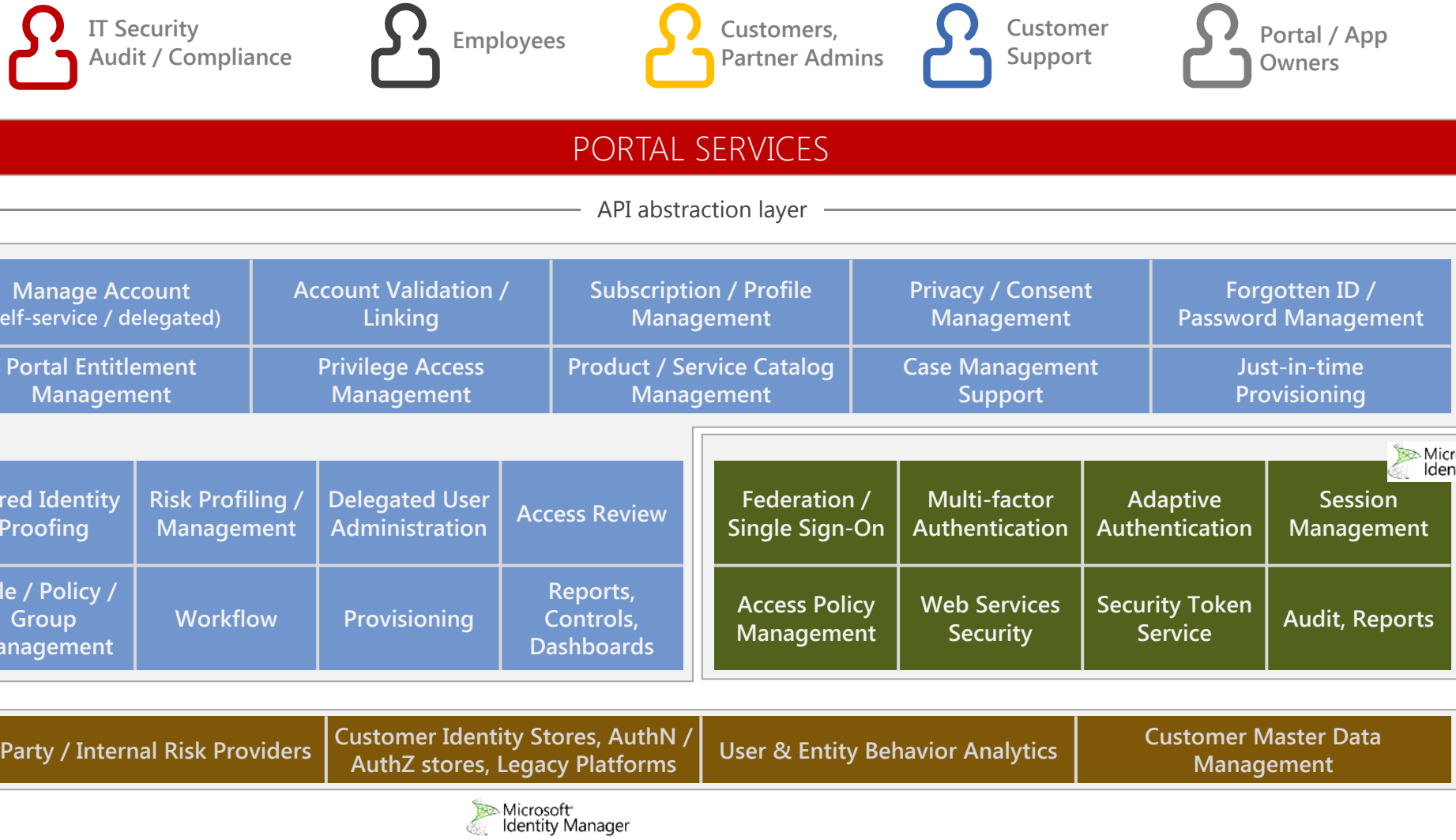
Registration	**Trust model for customer onboarding** Ability to perform tiered ID proofing based on type of resource being accessed
Product subscription	**Access control over portal resources** Trigger step-up authorization while accessing portal products
Access management	**Single sign-on across portals** Support for social / multi-factor authentication Support for adaptive / risk-based authentication Self-help tools including forgotten user name and password
Scalability	**Need to scale to millions of identities** Delivered as a (micro-) service Traditional reconciliation based methods fail with millions of transactions, support instant provisioning and on-the-fly administration
Privilege management	**Support for federated authorization** Externalize portal authorization model, typically based on LDAP, support SOA / services Provision across multiple legacy / SaaS identity stores Support for granular delegated administration (B2B / B2B2C)
Customer support	**Single sign-on across portals** Manage registration failures User password reset, OTP registration
Product policy management	**Manage access to portal resources** Manage privileged access for portal authorization store, authentication / authorization policies Bulk changes to users' access
Security Monitoring	**Identify threats and risks in real-time** Monitor user activity and behavior to detect malicious intent Force step-up or adaptive authentication

Key differences from enterprise IGA

Conceptual customer IAM architecture

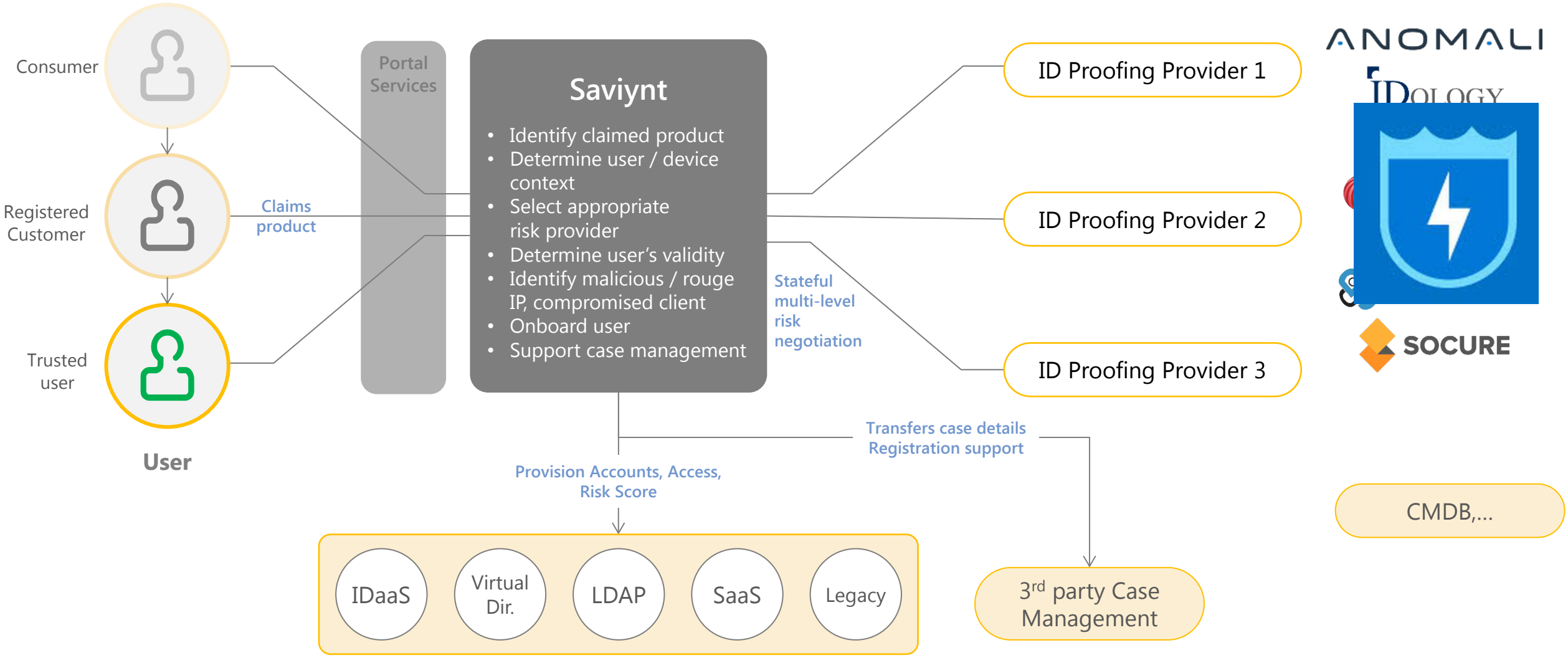


Detailed CIDM Services Architecture



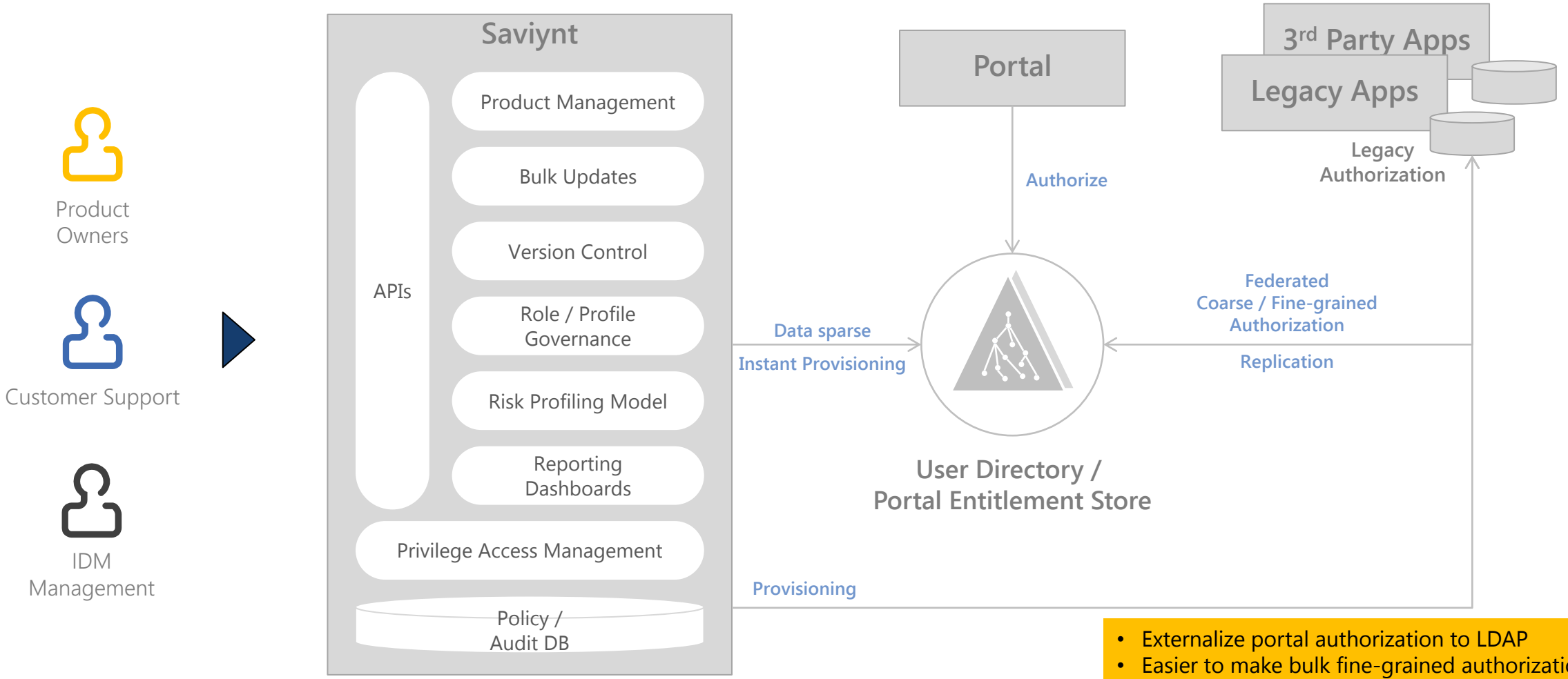
Customer identity lifecycle management

Registration with tiered ID proofing



Customer identity lifecycle management

Authorization and Privilege Management, Governance for Portal



- Externalize portal authorization to LDAP
- Easier to make bulk fine-grained authorization changes
- Implement privilege access management for portal authorization changes

Application

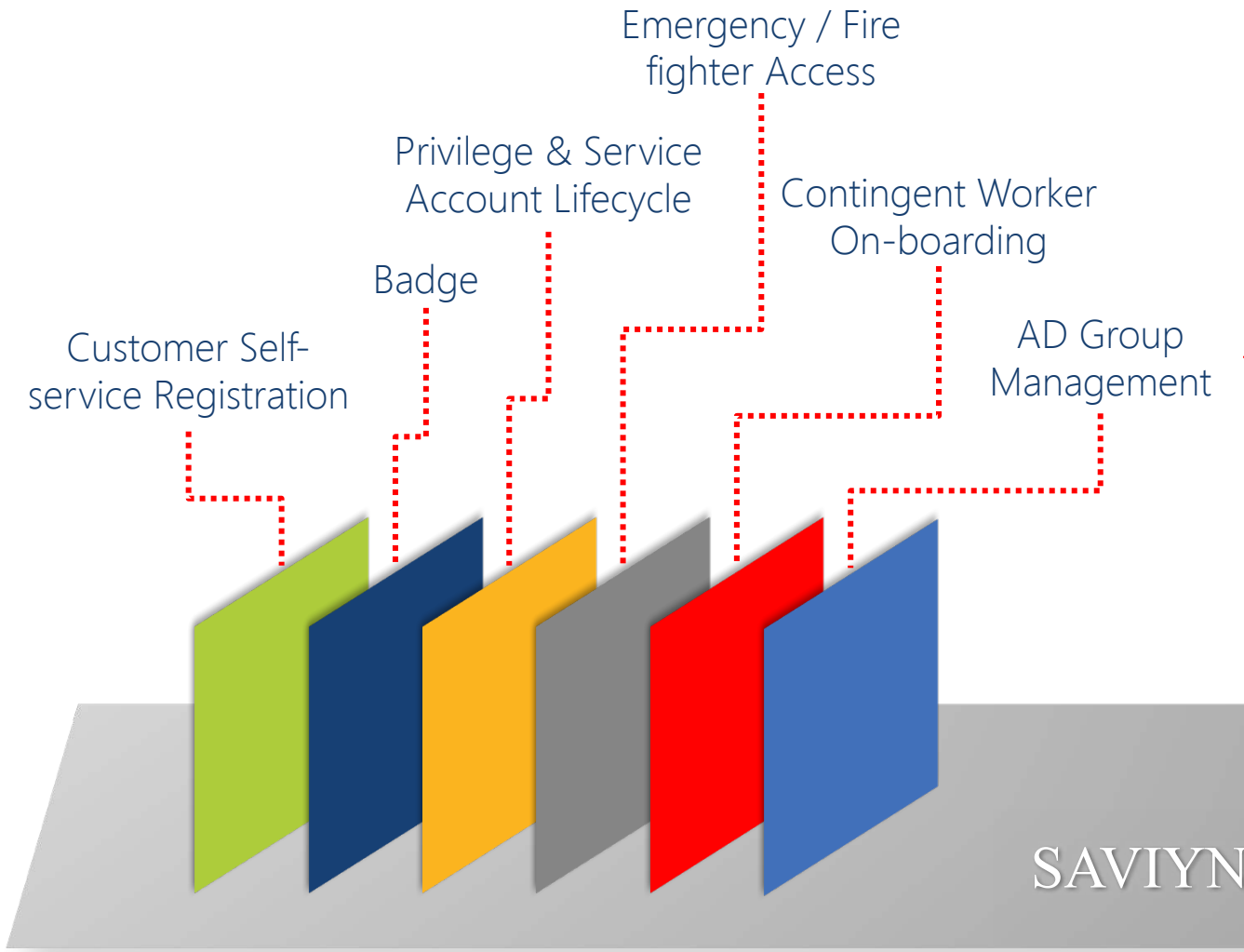
Active Directory Group Management

Data

IaaS

SAVIYNT

Saviynt provides several pre-built Access Life-Cycle Management modules to automate IAG processes and accelerate deployment by over 80%



- Self-service request for AD security group / DL provisioning
- Delegated administration for AD security group / DL management
- Support for nested AD groups
- Rules for AD group naming convention, OUs, etc.
- Bulk assignment of users to AD groups
- Integrated with risk-level for determining workflow behavior, certification review frequency
- Enhanced catalog integration with AD group description, risk level, etc.
- Dynamic group ownership management with primary and secondary owners
- Automatic group membership based on roles / rules

Application

What do the Analysts say?

Cloud

IaaS

SAVIYNT

Gartner IGA MQ 2017 and Report on Critical Capabilities for IGA 2017

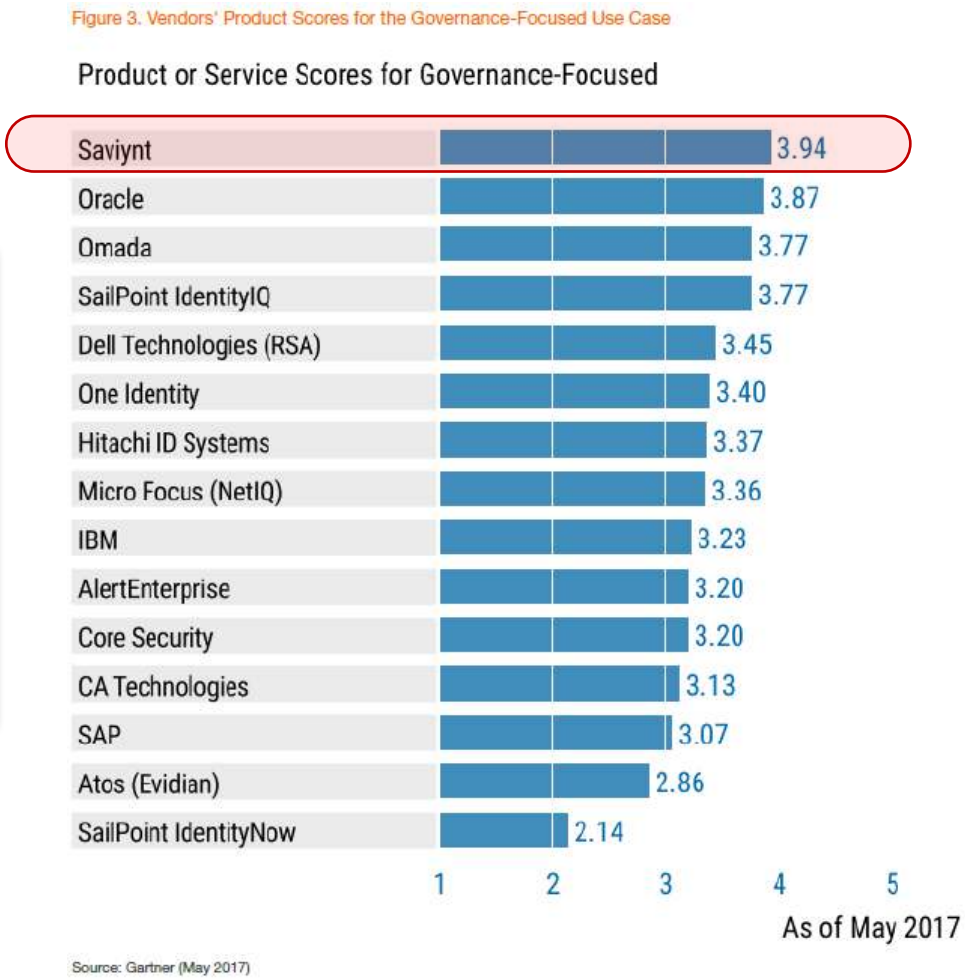
Identity Governance & Administration (IGA) MQ 2017

Source: Gartner (February 2017)

"Saviynt has the most fully featured IGA solution delivered as a service of any vendor reviewed in this Magic Quadrant."

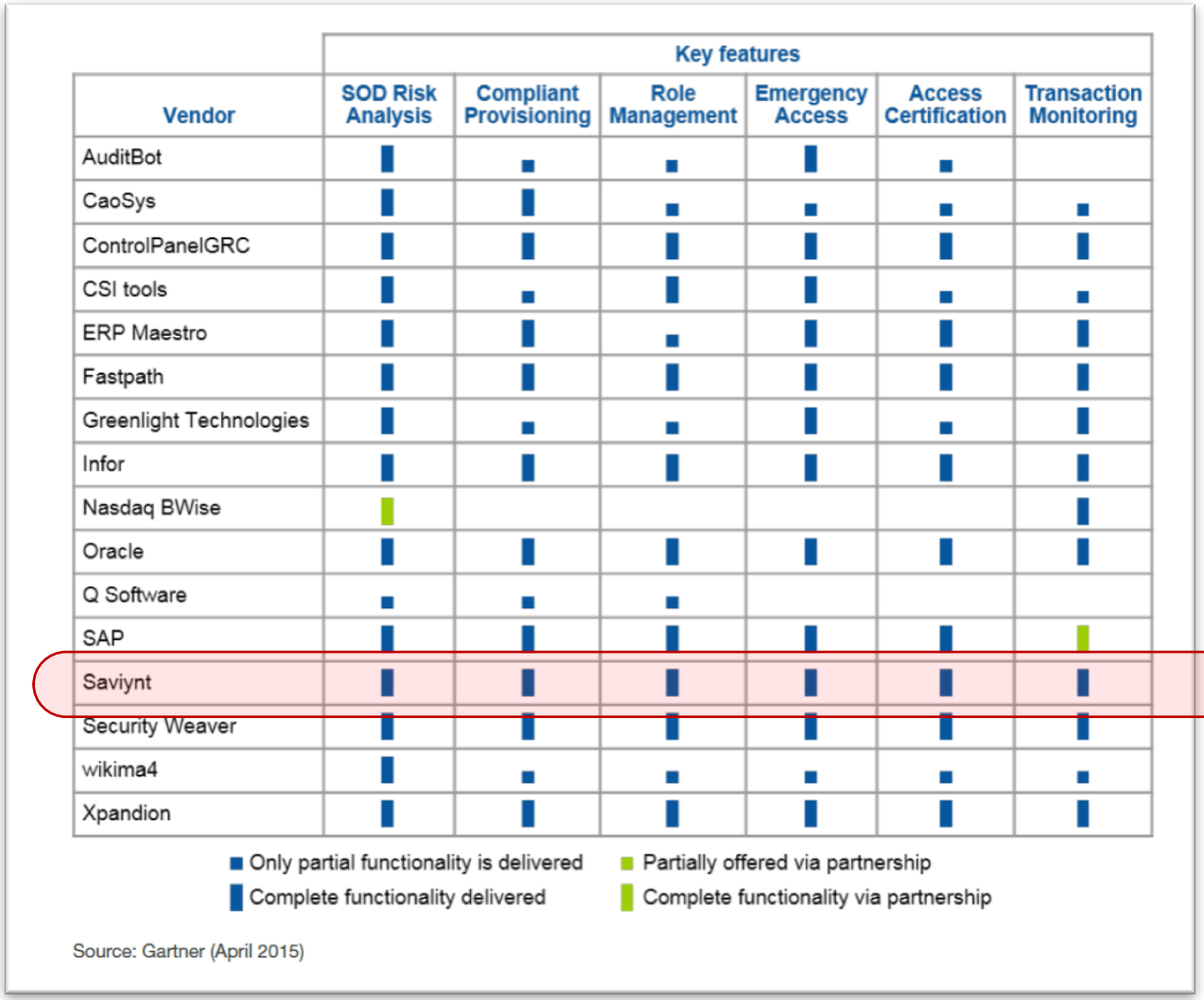
Gartner IGA Magic Quadrant 2017

Critical Capabilities for IGA 2017



Source: Gartner (May 2017)

Gartner Market Guide for SOD Controls Monitoring 2015



Vendor	Key features: SOD Risk Analysis	Compliant Provisioning	Role Management	Emergency Access	Access Certification	Transaction Monitoring
AuditBot	■	▪	▪	■	▪	
CaoSys	■	■	▪	▪	▪	▪
ControlPanelGRC	■	■	■	■	■	■
CSI tools	■	▪	■	■	▪	▪
ERP Maestro	■	■	▪	■	■	■
Fastpath	■	■	■	■	■	■
Greenlight Technologies	■	▪	▪	■	▪	■
Infor	■	■	■	■	■	■
Nasdaq BWise	▪					■
Oracle	■	■	■	■	■	■
Q Software	▪	▪	▪			
SAP	■	■	■	■	■	▪
Saviynt	■	■	■	■	■	■
Security Weaver	■	■	■	■	■	■
wikima4	■	▪	▪	▪	▪	▪
Xpandion	■	■	■	■	■	■

■ Only partial functionality is delivered
▪ Partially offered via partnership
■ Complete functionality delivered
▪ Complete functionality via partnership

Source: Gartner (April 2015)

"One of the **rare vendors that approaches IGA and Segregation of Duties controls monitoring** with a common suite of products. Whereas most SOD controls monitoring vendors tend to focus exclusively on financial applications, Saviynt has extended its coverage to include healthcare applications …"

Healthcare update to Gartner IGA Magic Quadrant 2015

"Organizations looking for a centralized SOD controls monitoring approach with advanced role mining and user provisioning requirements across multiple ERP platforms and complex authorization systems including SaaS applications, should consider Saviynt."

Market Guide for SOD Controls Monitoring 2015

Thank You

SAVIYNT