MBCOM TECHNOLOGIES | vmware by Broadcom

Adria Forum 2025

Identity Without Borders – How IGA + PAM Deliver Unified Control?

Maciej Machacz

Technical Presales Manager, CEE & Turkey

14 X 2025

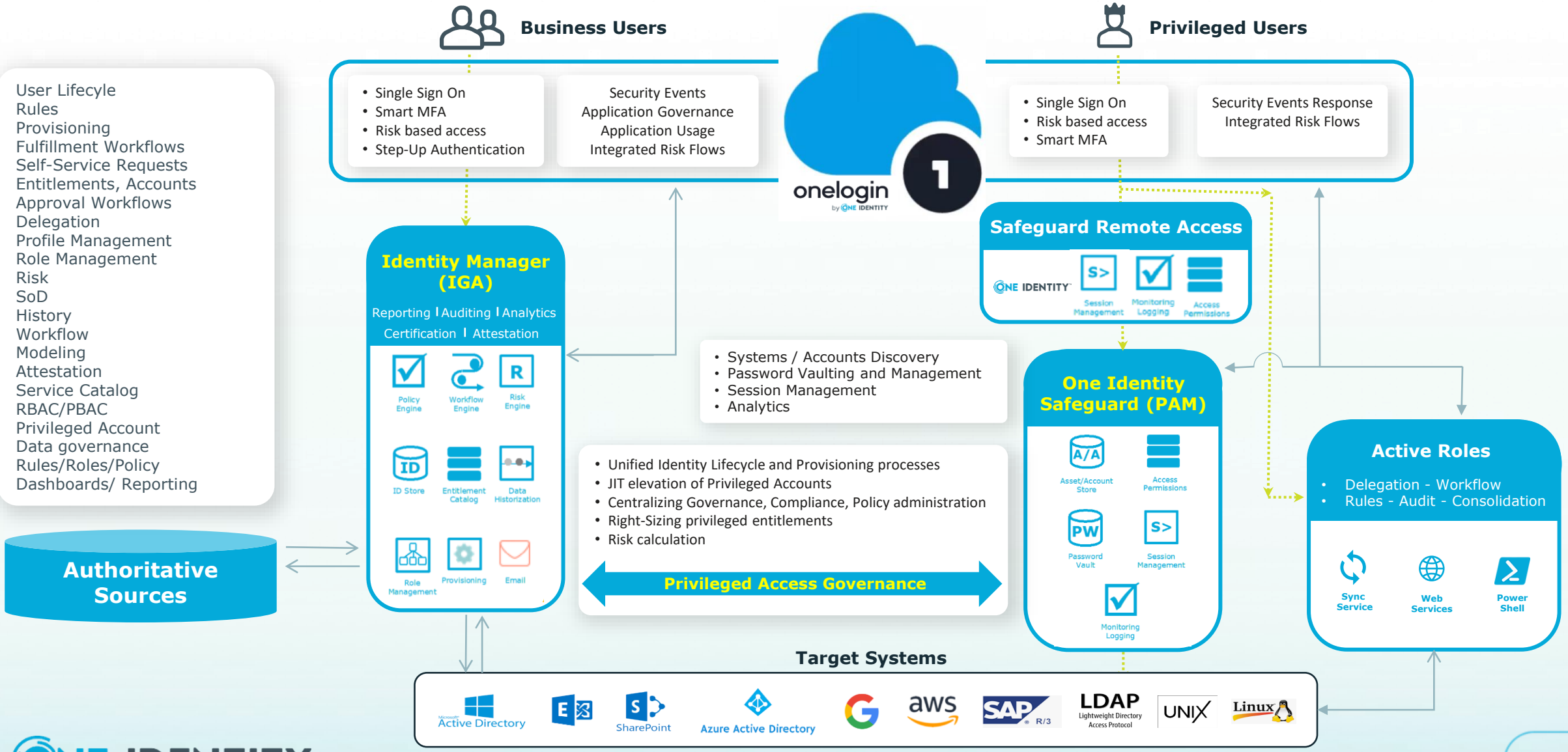
- One Identity Fabric
- What is Identity Manager?
- What is Safeguard PAM?
- Privileged Access Governance

One Identity Fabric Introduction

The **One Identity Fabric** integrates key **IAM/IGA Identity Manager** capabilities into one cohesive solution, including **Safeguard PAM**, AM and AD/Entra ID, providing both security and operational efficiency.

With seamless data synchronization and communication, administrators can consistently manage security controls across all systems, whether cloudbased or legacy.

One Identity Fabric in action



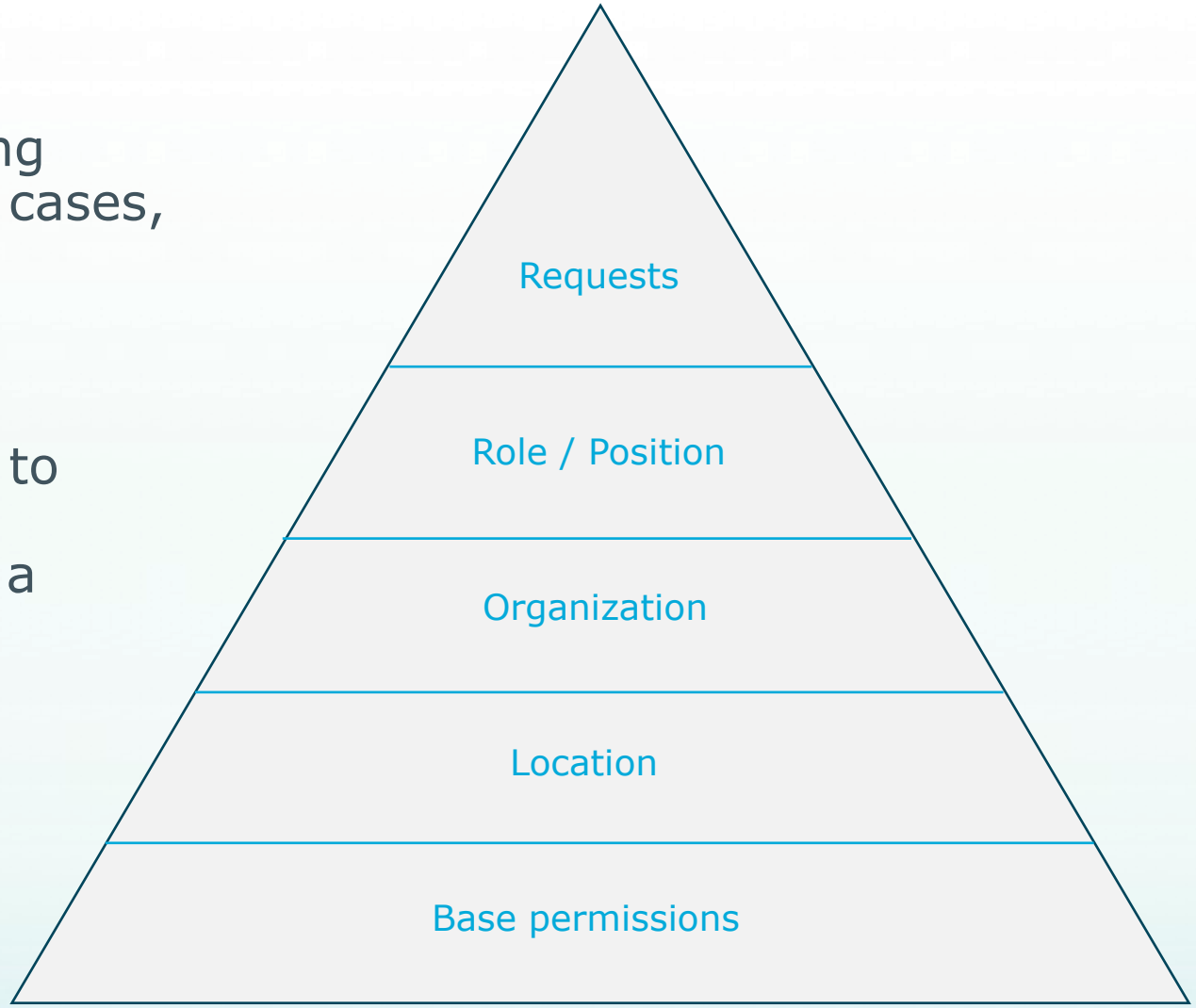
Identity Manager

ONE IDENTITY

The art of Identity Management

Automation is the fine art of providing access to persons based on – in most cases, data from authoritative source(s)

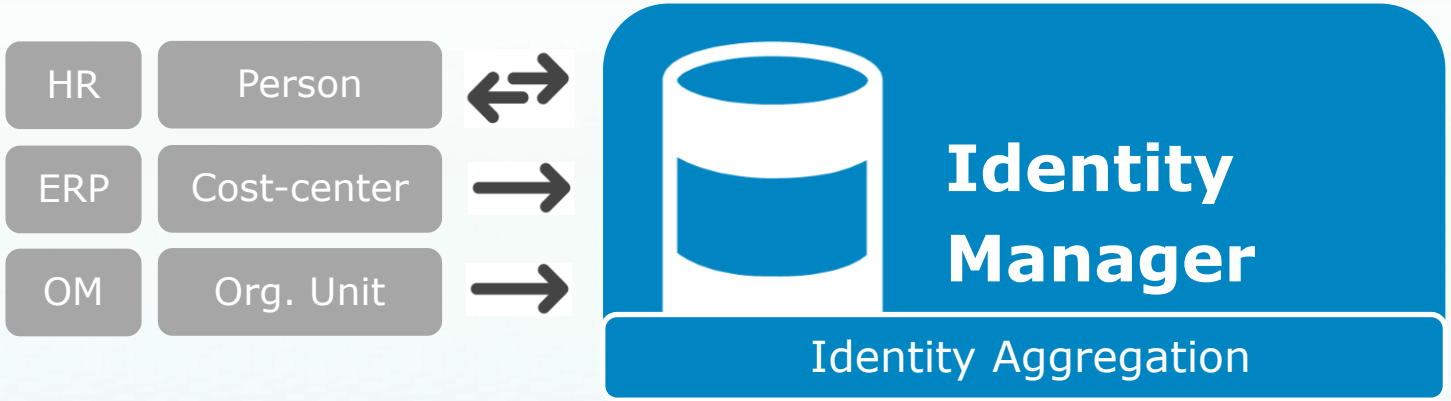
A common approach to automation is to provide access to applications and permissions based on this model – or a similar model



Identity Manager: Complete Identity Governance

A central database repository using one (1) data model and one (1) code base

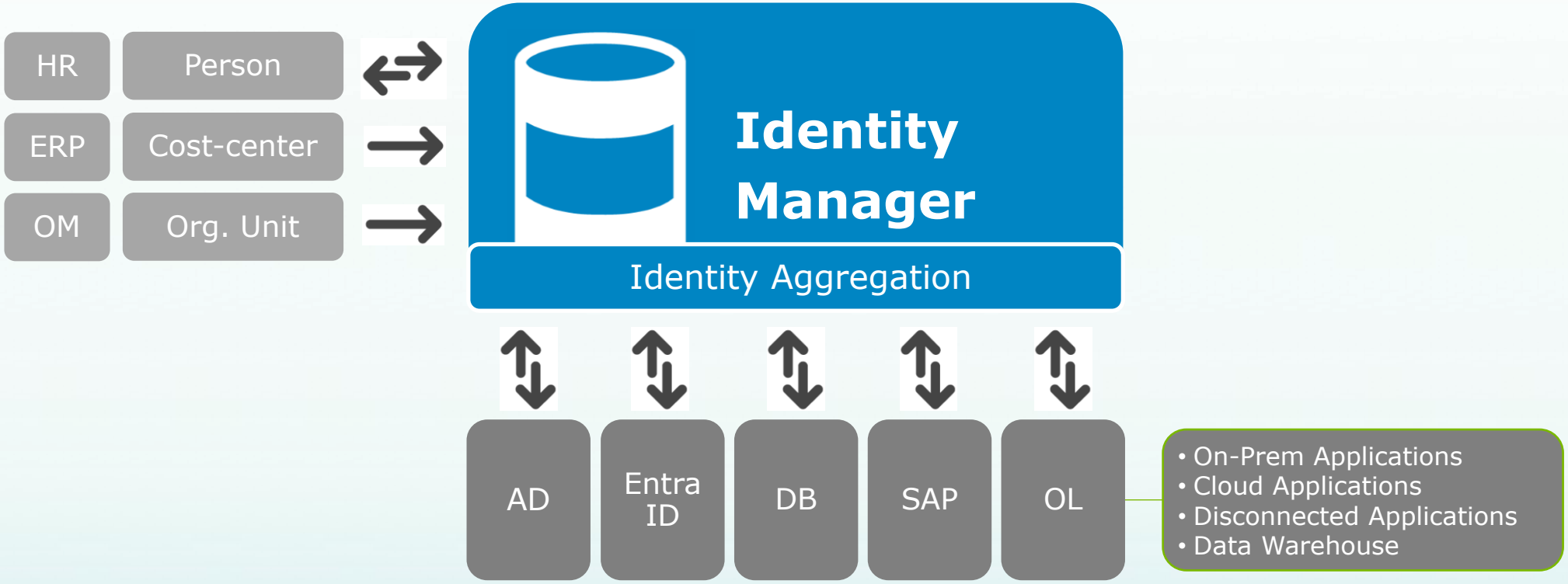
Identity Manager: Complete Identity Governance



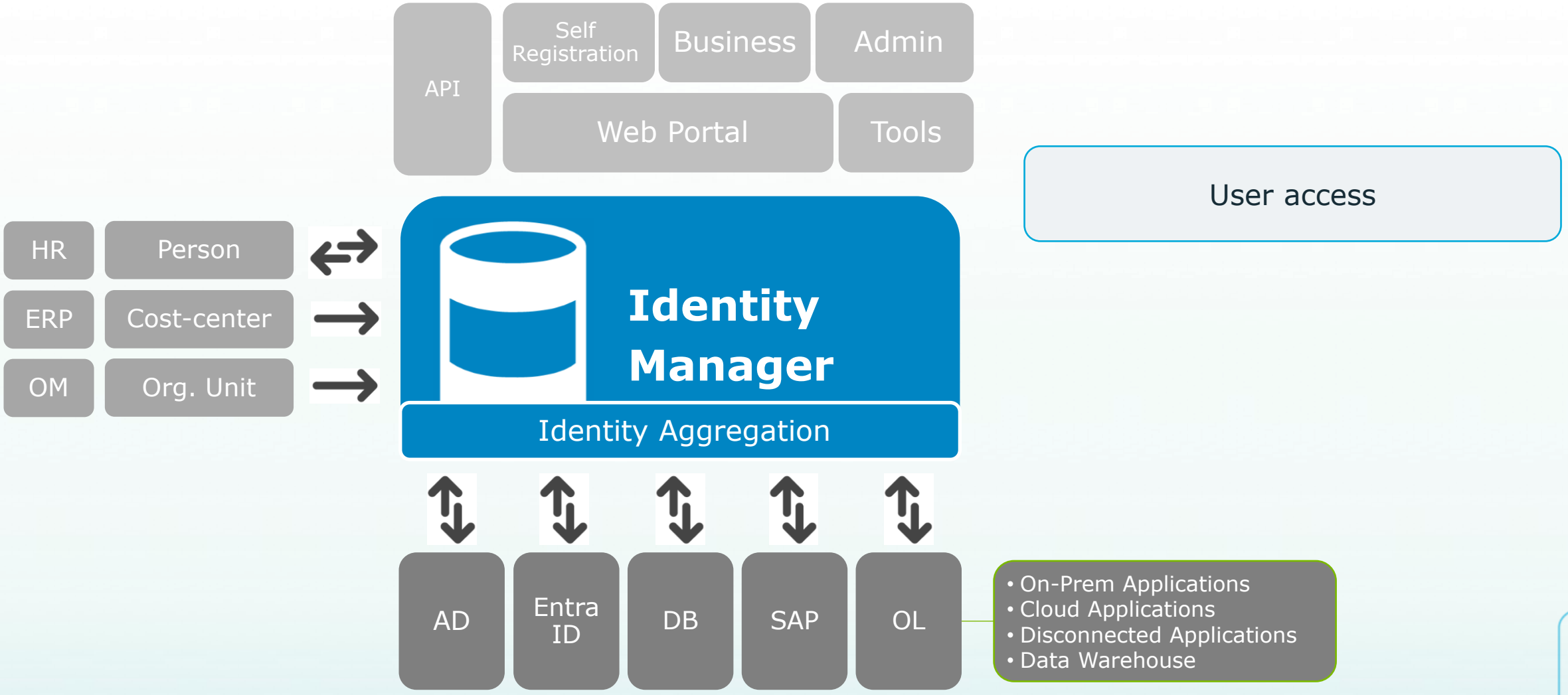
Authoritative sources for proper lifecycle management

Identity Manager: Complete Identity Governance

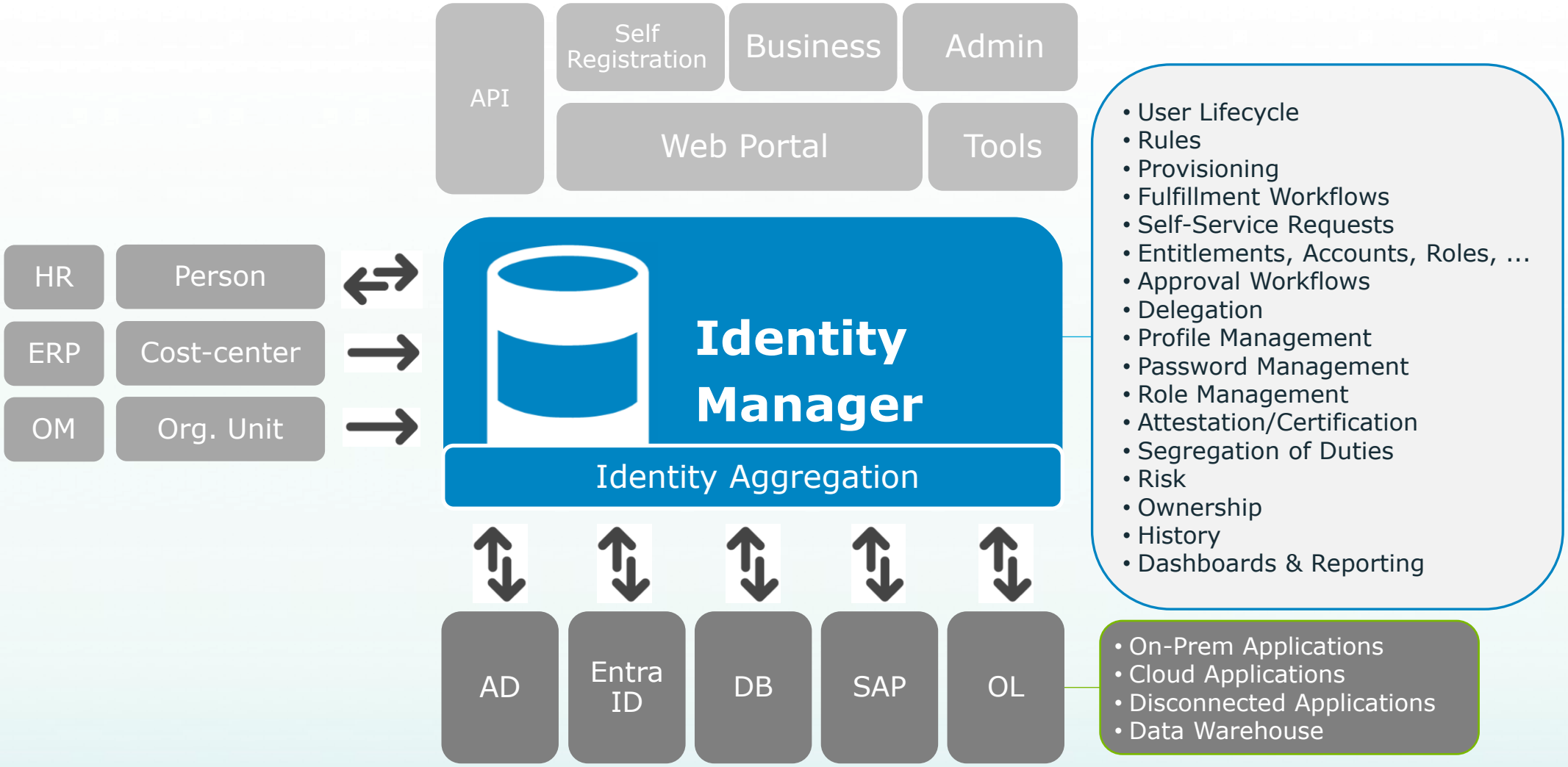
Connectivitiy based on framework



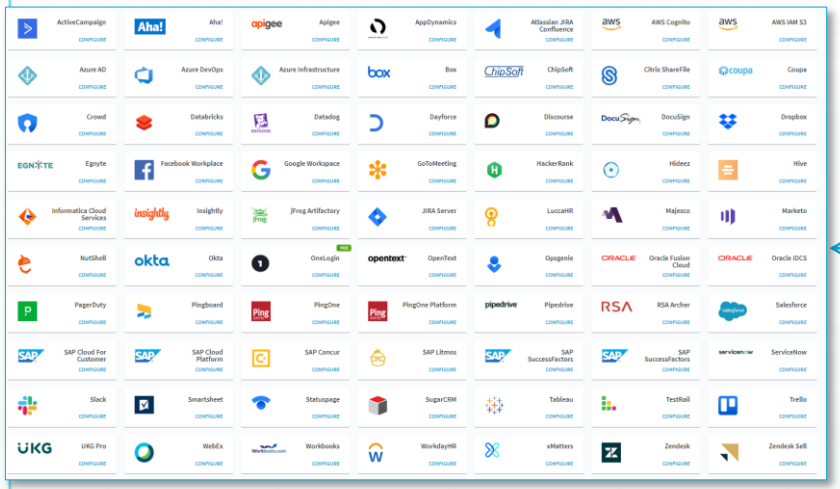
Identity Manager: Complete Identity Governance



Identity Manager: Complete Identity Governance



Identity Manager - Target system connectivity



Starling Connect

SCIM

Identity Manager

Microsoft Entra ID

SharePoint Online

onelogin

Exchange Online

Google Workspace

Connected system modules

CSV

SCIM

Web Services

Powershell

Microsoft ADO .Net

Generic connectors

Mainframe

Active Directory

SharePoint

SAP R/3

SAP S/4 HANA

IBM Notes

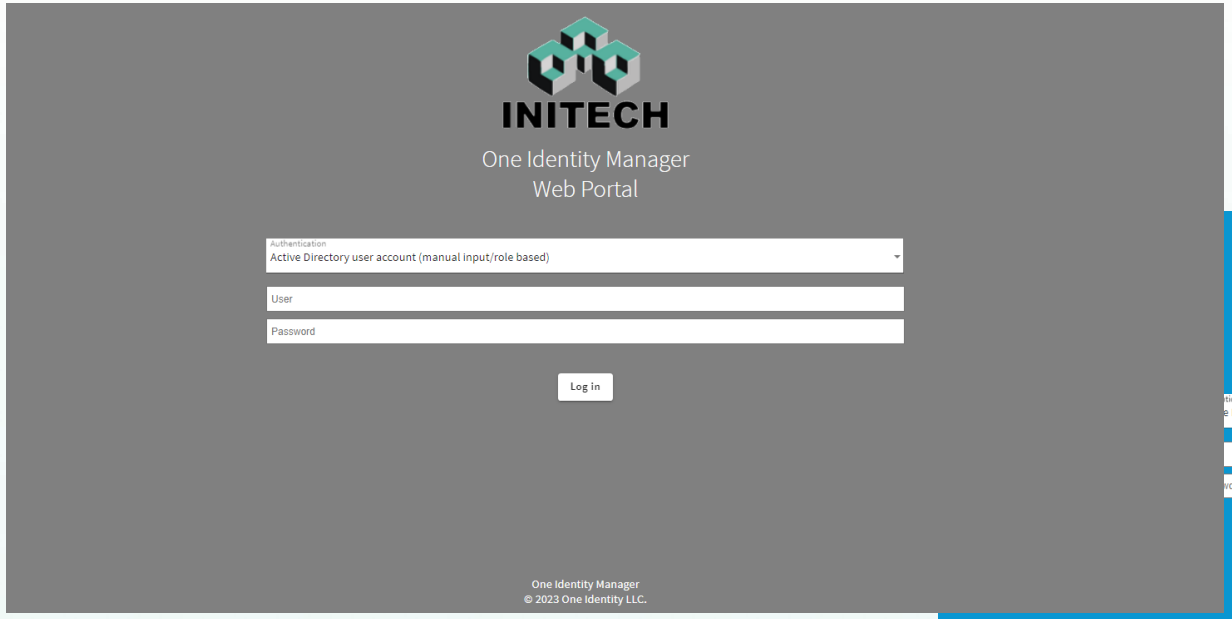
LDAP Lightweight Directory Access Protocol

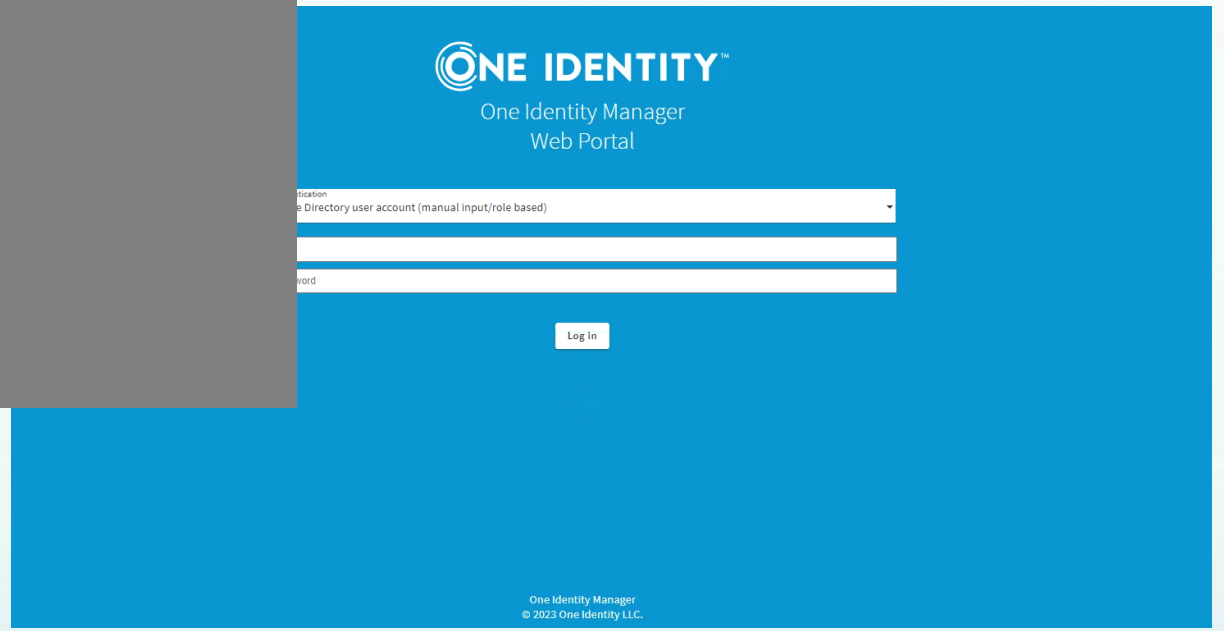
UNIX

Linux

Identity Manager - web portal

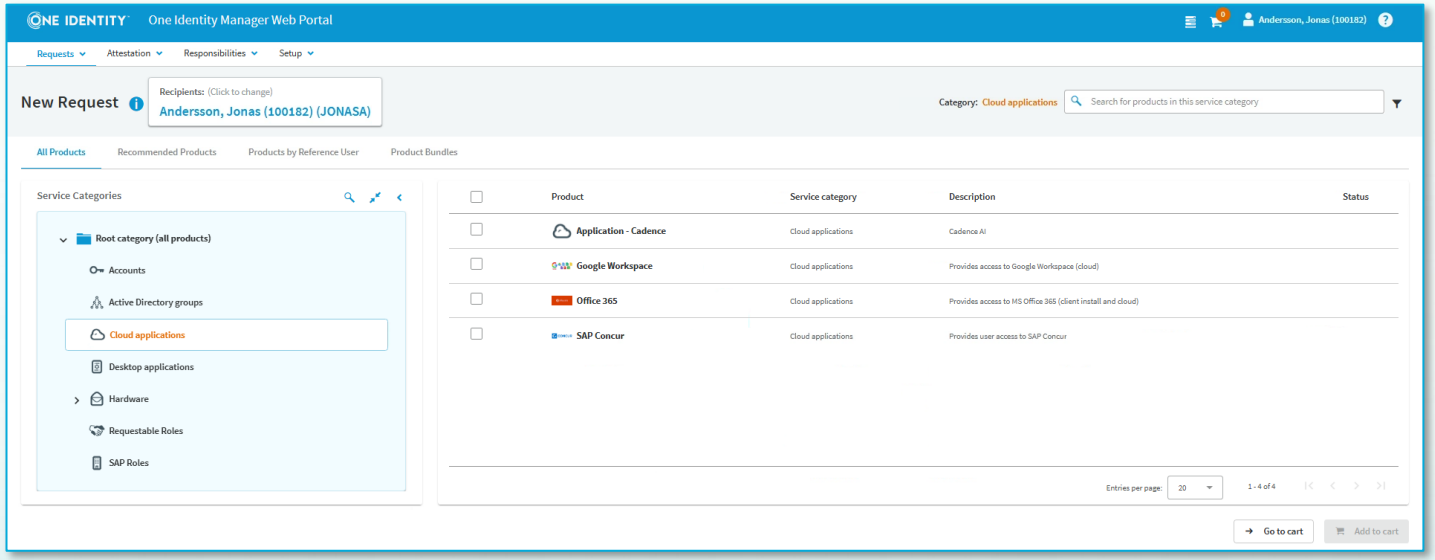
- Easily branded with logo
- Custom themes





Self Service Use Cases

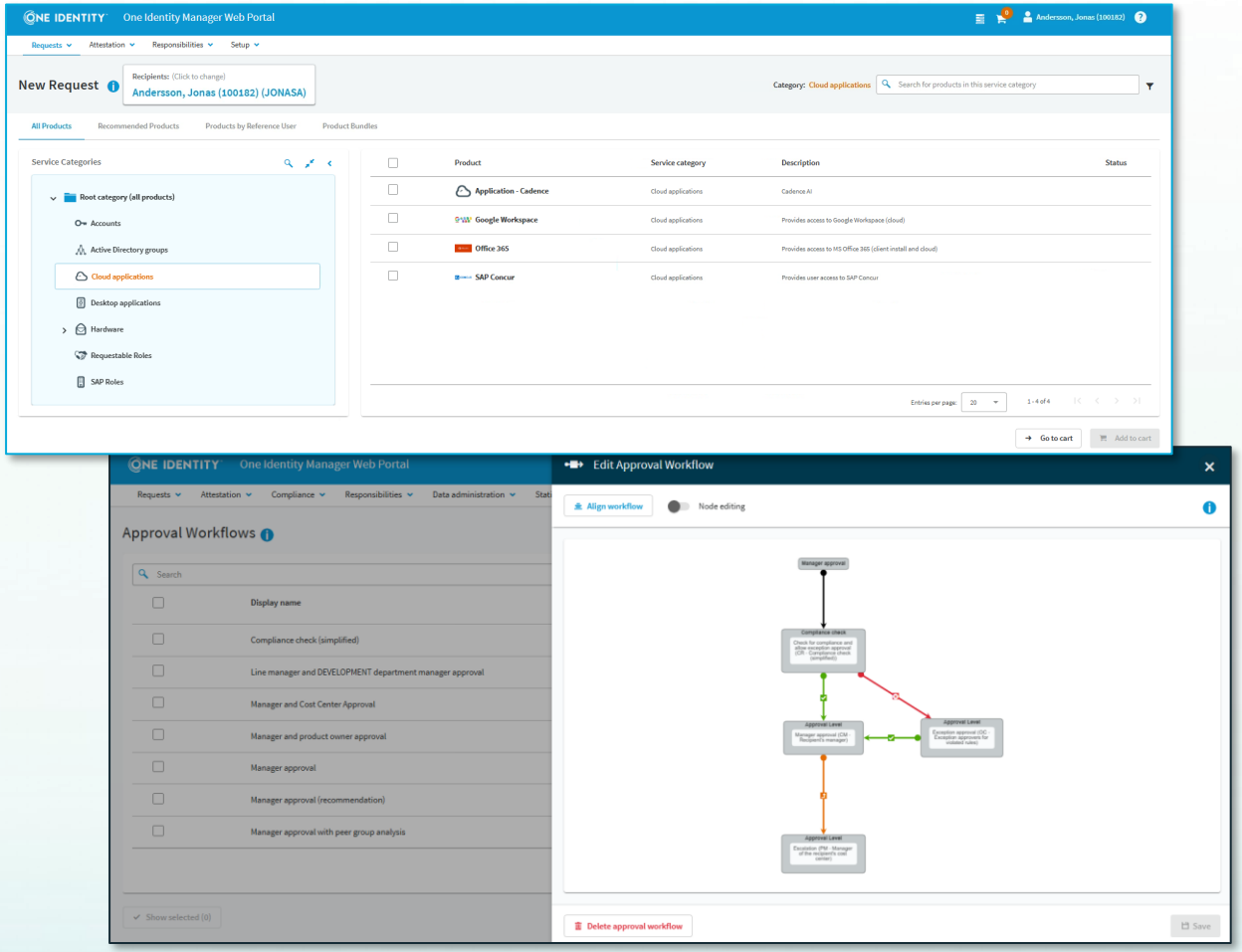
- Eliminates the need for IT to fulfill undocumented requests. Users can simply put their requests via an online portal. The online portal enables an automatic compliance check for requests including - separation of duties before directing the request through to the appropriate data owner.
- Removes IT involvement by automating the fulfillment of approved access requests for end users.
- Full support for delegation
- ServiceNow Ticketing Integration supported as standard



Identity Manager – IT Shop: Features

Web Self-Service Front

- Compliance check option for all requests during checkout
- Compliance check during approval
- User can only request items which are allowed based on his/her roles
- Request history and process monitoring
- Manager can make requests for his/her employees
- Requester can see peer's requests
- Peer-group analysis and recommendations



Identity Manager - summary

Key Benefits

- **Security:** Reduces risk by providing visibility and control over user accounts and access rights.
- **Compliance:** Satisfies audit and regulatory requirements through comprehensive governance and attestation processes.
- **Efficiency:** Automates provisioning, deprovisioning, and access management, reducing manual intervention and IT workload.
- **Unified Identity Security:** Integrates with dozens of applications, including Active Directory (AD), Azure AD, and cloud apps, to unify policies and reduce risk exposure.
- **Zero Trust Model:** Supports deployment of a Zero Trust identity security model.

Core Capabilities

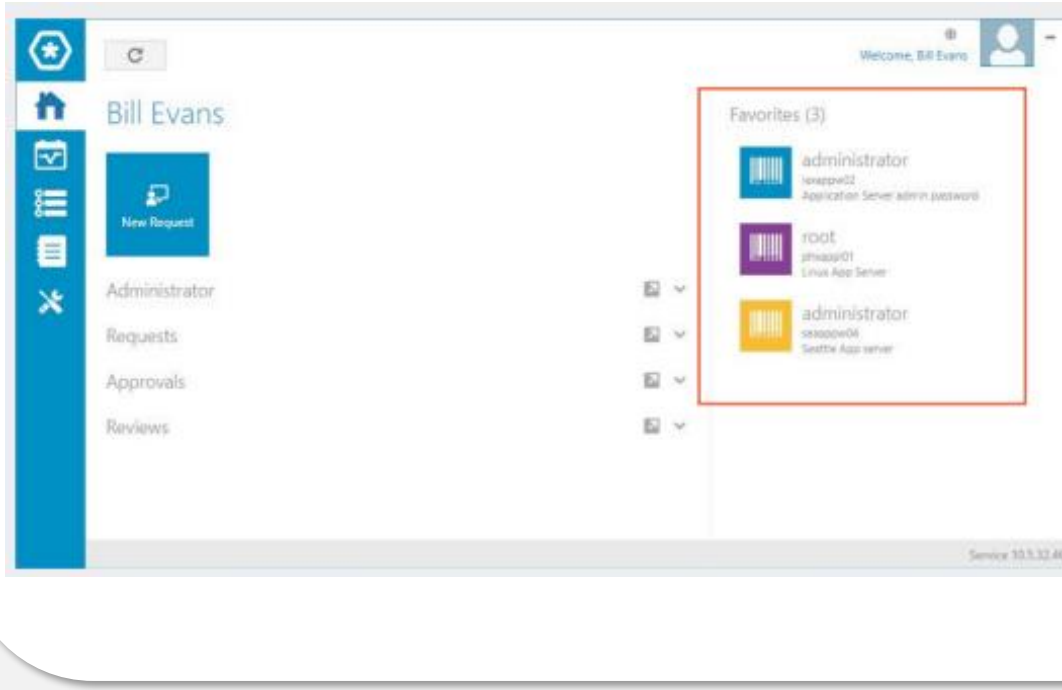
- **Enterprise-wide provisioning and governance** for all identity types.
- **Role management and RBAC:** Simplifies defining and managing roles, reducing complexity in access governance.
- **Integration:** Deep integration with AD, Azure AD, SAP, and other systems, supporting hybrid and complex environments.
- **Privileged Access Management (PAM):** Natively integrates with One Identity Safeguard for governance of privileged accounts.
- **Audit and Reporting:** Maintains a detailed audit trail of all operations for compliance and security.
- **Cost Efficiency:** Recognized for faster deployment and lower total cost of ownership, especially for mid-sized enterprises.

Safeguard PAM

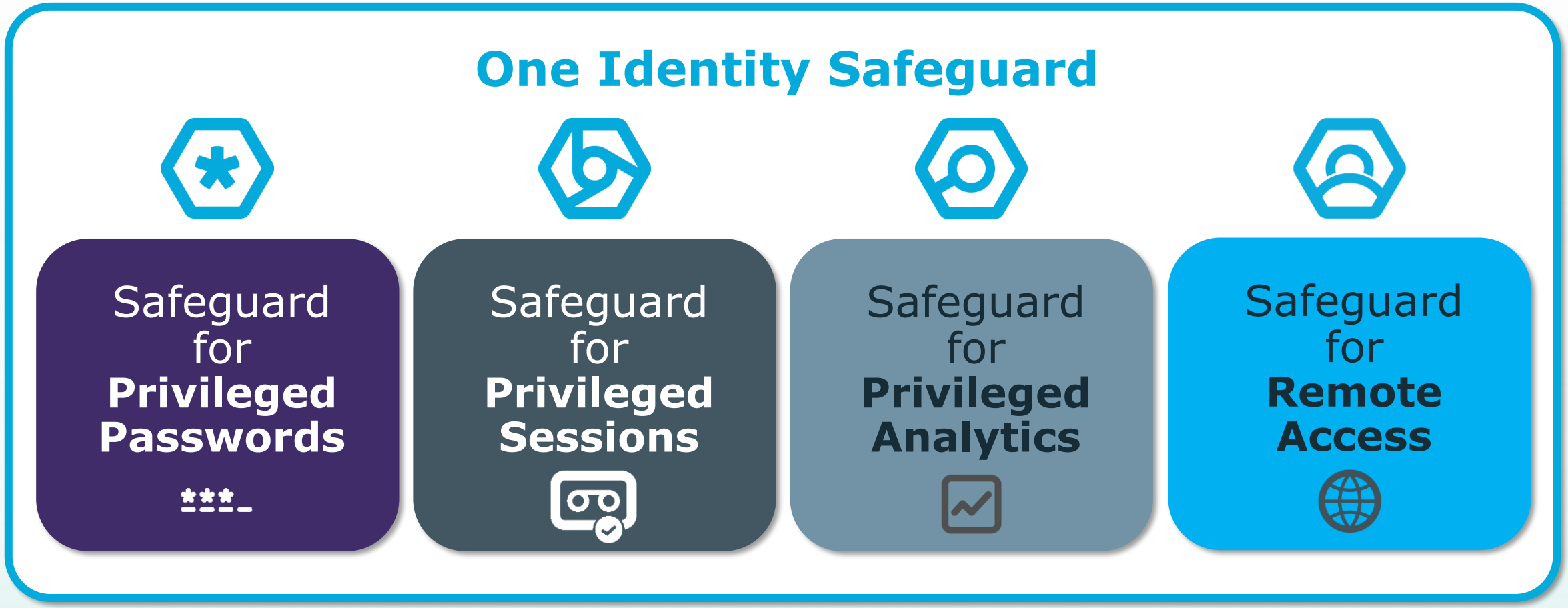
ONE IDENTITY

What Is Safeguard PAM?

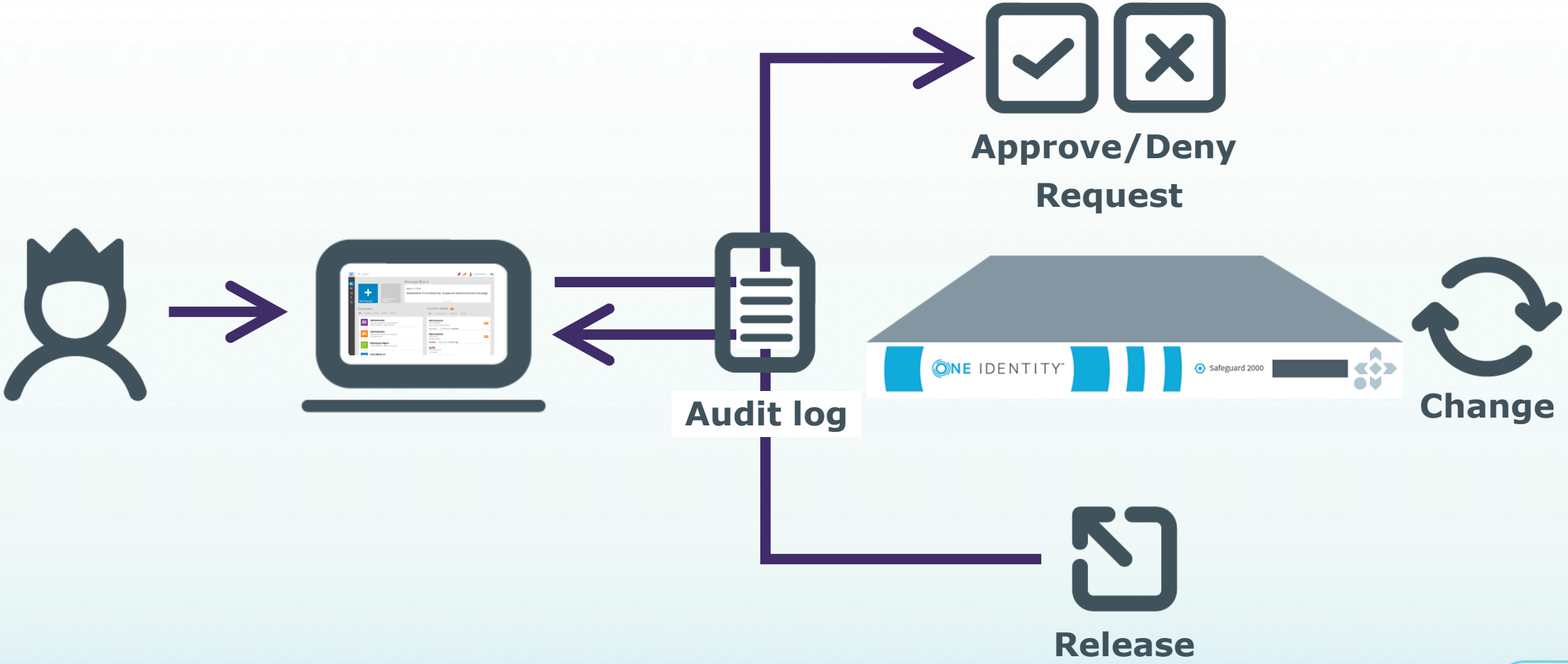
- One Identity Safeguard PAM is a **hybrid-ready, easy-to-use, and comprehensive Privileged Access Management solution.**
- Secure, control, monitor, **analyze** and govern **privileged access** across multiple environments and platforms
- Grants privileged credentials with role-based access management and automated workflows
- Enables ability to **manage passwords** from anywhere and using nearly any device.
- Controls, monitors and **records privileged sessions** of administrators, remote vendors and other high-risk users



The Safeguard PAM core platform



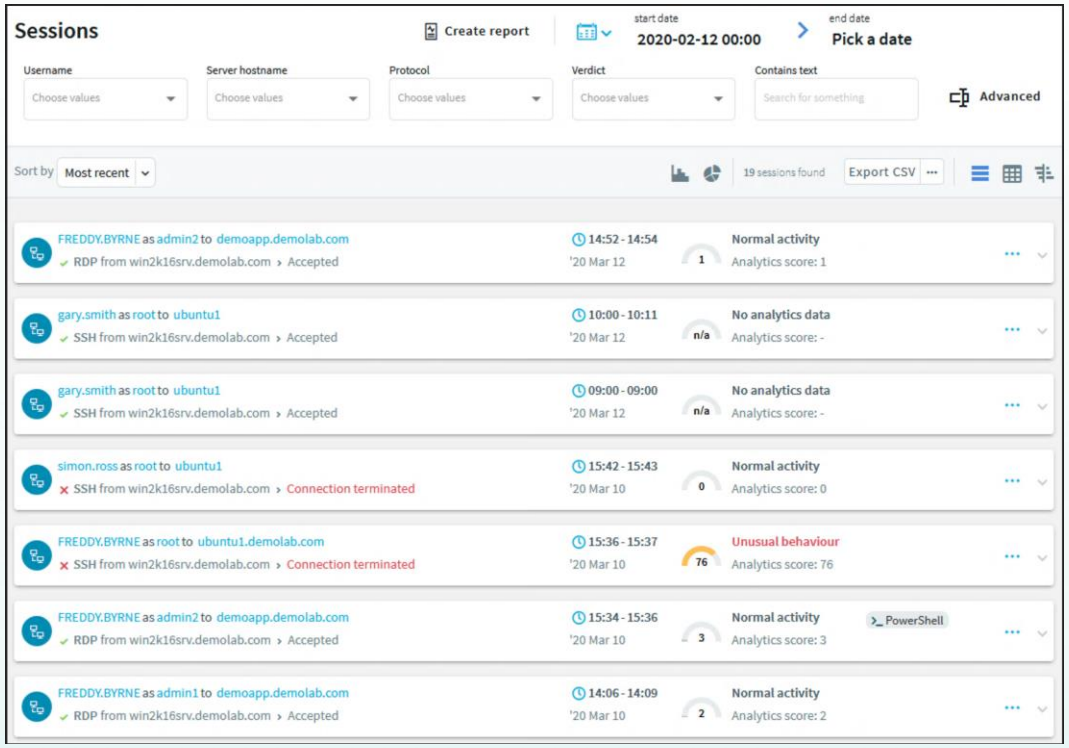
Safeguard Privileged Password - Password vaulting

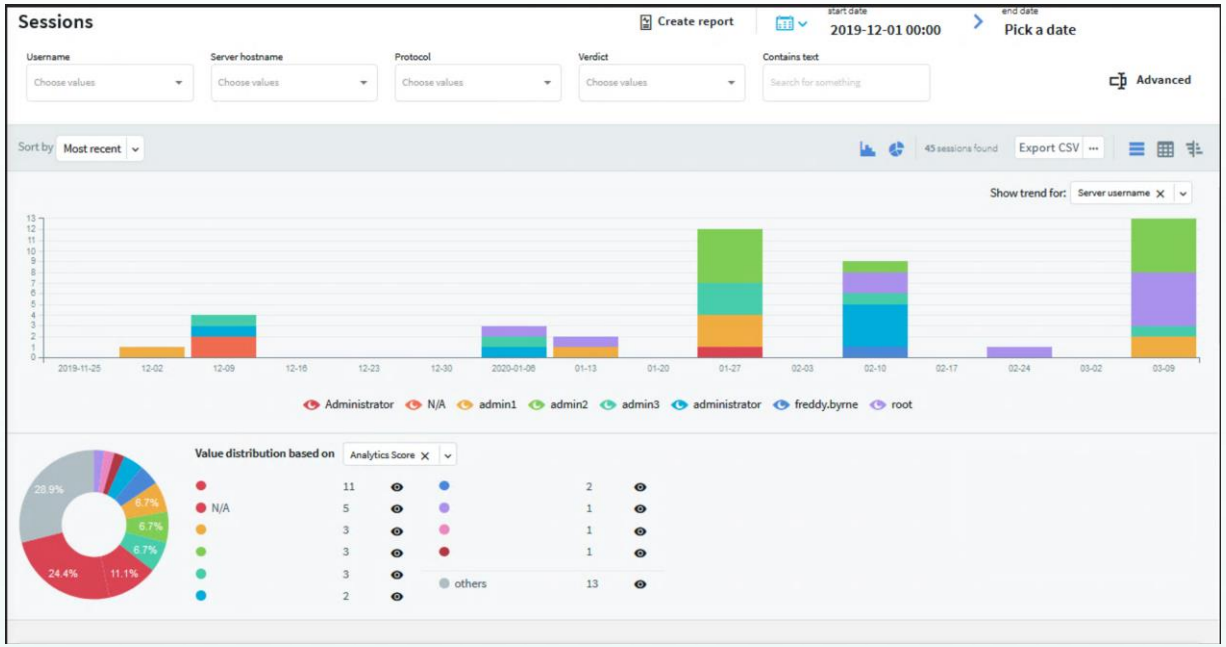


Safeguard for Privileged Sessions - recording

Safeguard for Privileged Analytics

- Baseline, Compare, Report





SPA - determining digital behavior

Behavioral information based on log data

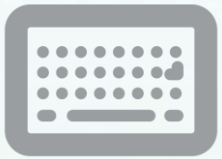
Typical time of logging in

Range of accessed servers and applications

Behavioral information based on granular session data

Activities performed

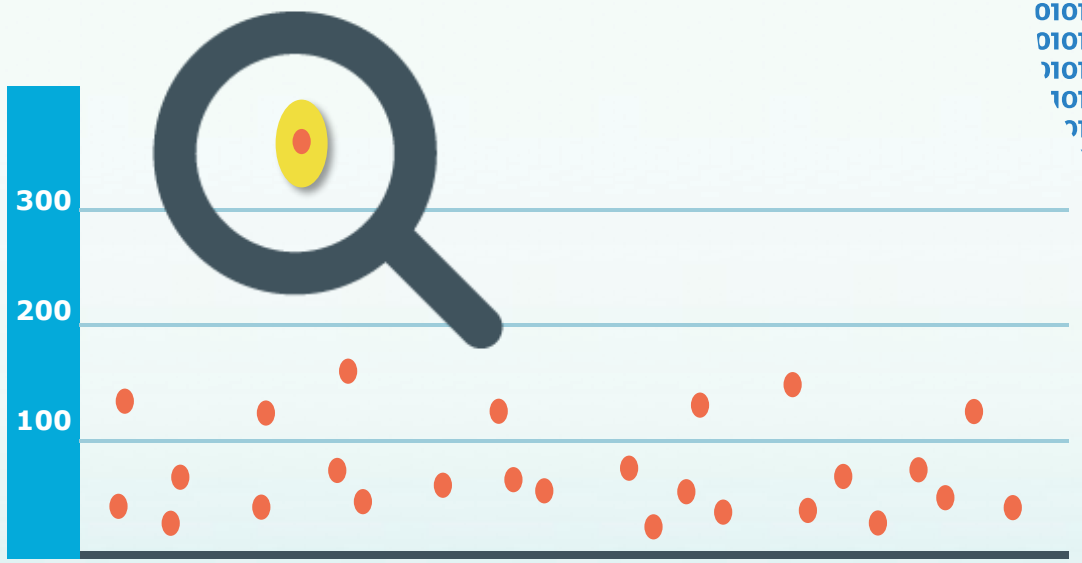
Mouse movement characteristics



Keystroke dynamics analysis

User behavior analytics (UEBA)

- Gather digital footprints
- Define what is normal, build user baselines
- Identify unusual & risky events in real-time



Safeguard PAM - summary

Business Value

- **Stronger Security:** Reduces the enterprise attack surface by automating and simplifying privileged credential management, resulting in a more secure environment.
- **Compliance:** Simplifies compliance and audit reporting with recorded sessions and detailed access controls, helping organizations meet regulatory requirements.
- **Operational Efficiency:** Quick deployment, user-friendly interfaces, and automation help reduce administrative overhead and speed up adoption.
- **Visibility and Control:** Provides granular visibility into who has access to what, when, and why, supporting both security and operational needs.

Core Capabilities

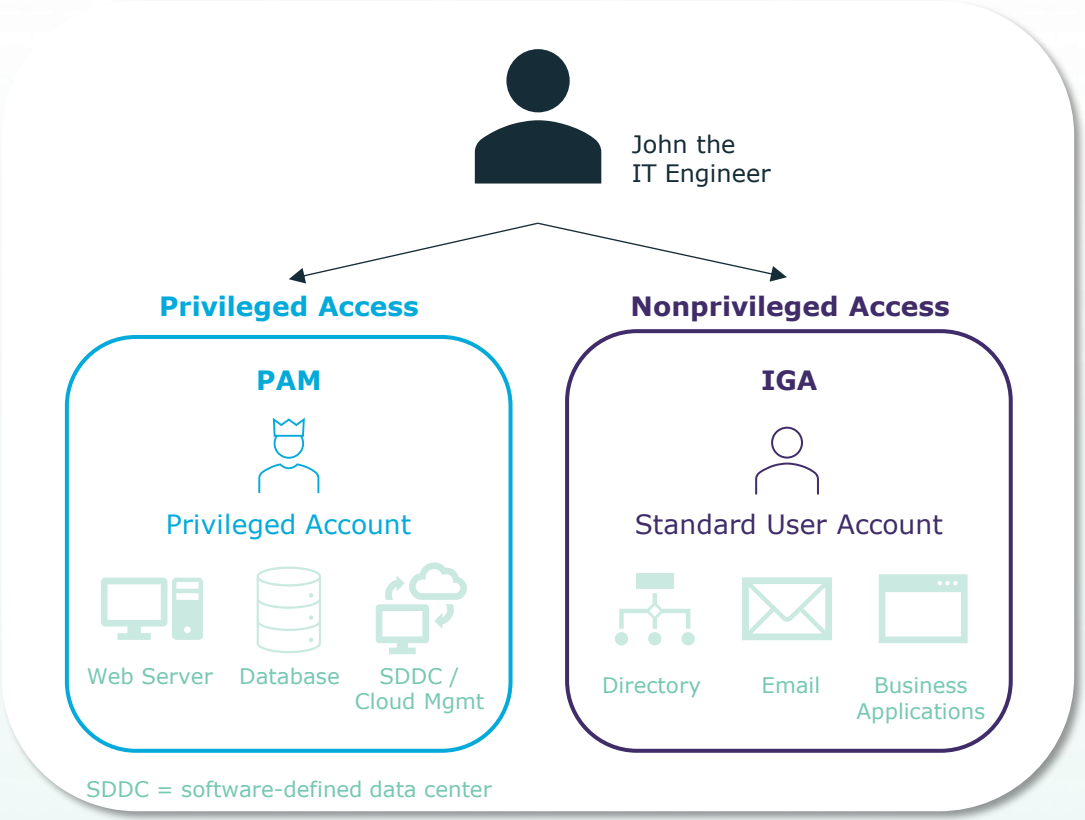
- **Privileged Credential Management:** Automates and secures credential management with role-based access and automated workflows. Passwords can be managed from anywhere, on nearly any device.
- **Session Management:** Controls, monitors, and records privileged sessions of administrators, remote vendors, and other high-risk users. Sessions are indexed for easy event search and compliance reporting.
- **Privileged Analytics:** Uses behavioral analytics to detect and rank anomalies, helping organizations identify and respond to risky behaviors in real time.
- **Zero Trust Model:** Enforces just-in-time access, ensuring users only have the privileges they need, when they need them, reducing the attack surface.

Privileged Access Governance

ONE IDENTITY

The Unfortunate Truth

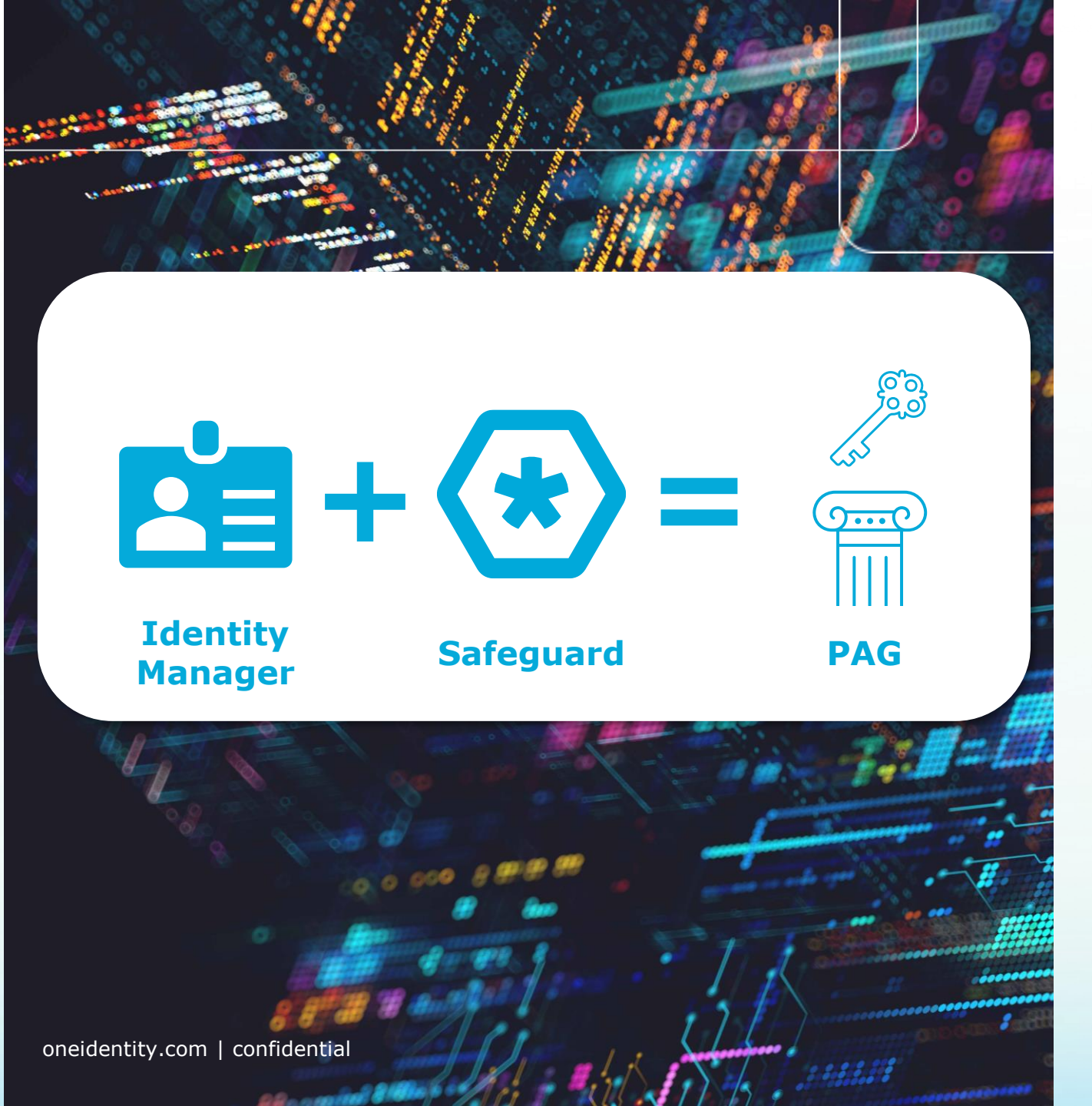
- Organizations that still operate privileged access management and identity governance in a siloed manner **are locked out from performing critical functions that impact security**:
  - Applying identity provisioning process to privilege accounts
  - Enforcing cohesive access policies across target systems and platforms
  - Benefiting from modern governance practices
- When these systems are run independently, you are unable to get a **360-degree view of all identities, and their associated user accounts, entitlements and activity**



What Is It?

Privileged access governance (PAG) protects and manages privileged access and grants a 360-degree view of users, accounts and activities. The PAG integration module connects **Identity Manager** with **Safeguard PAM** and provides:

- **Provisioning** and deprovisioning
- **Access request** and approvals
- **Delegation of roles** and responsibilities
- **Policy/SoD detection** and enforcement
- **Attestation**/Certification of access



ONE IDENTITY

How Does PAG Help?

Increased Security

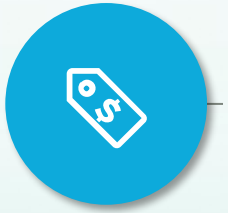
Manage all identity types from a **centralized platform** and enforce SoD policies

Stronger Compliance

Correct **improper or redundant access** to privileged accounts

Better Governance

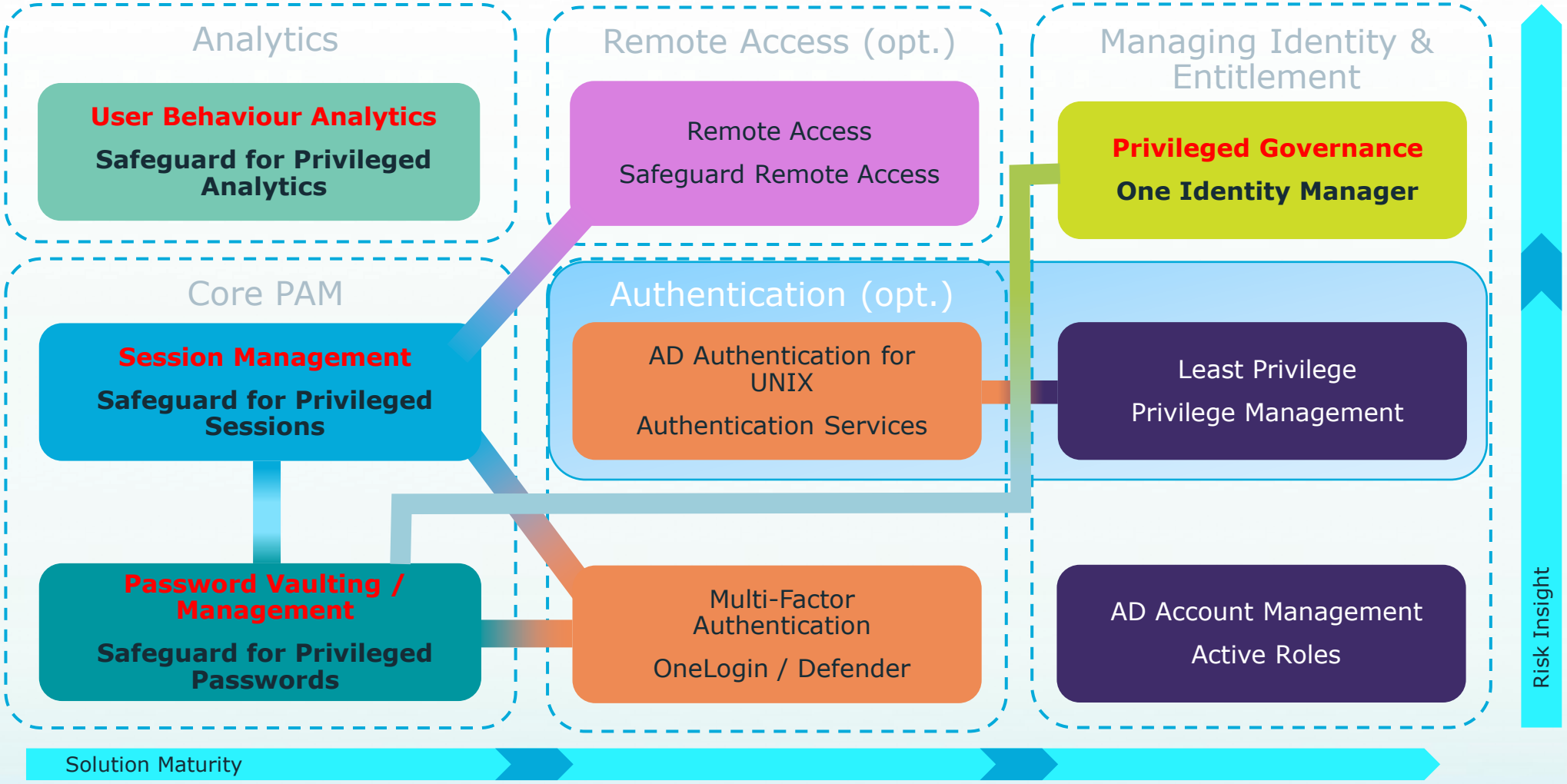
Provides **ongoing certification/attestation** of PAM access



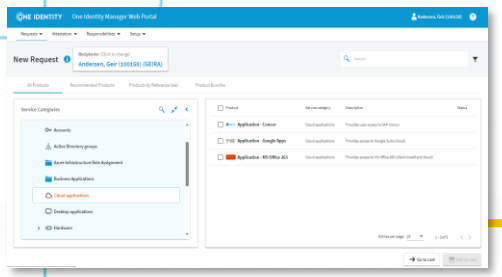
Lower Costs

Unified identity lifecycle management and provisioning processes that eliminate administration silos and redundant tasks

How does it work together?



PAG Module in Identity Manager



Business User
- Business Administration
- Request & approval
- Resource management
- Compliance/Attestation
- Risk Management

Authoritative Sources

Target System, Application Business Permissions

Identity Manager (IGA)

Policy Engine

Workflow Engine

Risk Engine

ID Store

Entitlement Catalog

Data Historization

Role Management

Provisioning

Email

PAG

One Identity Safeguard (PAM)

Asset/Account Store

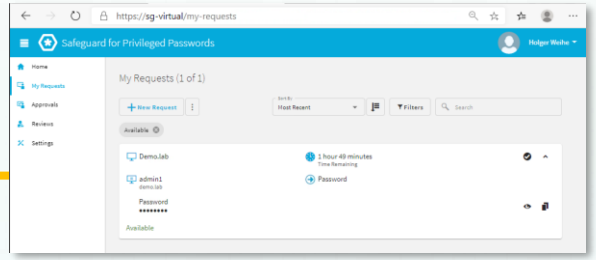
Access Permissions

Password Vault

Session Management

Monitoring Logging

Privileged Secrets and Sessions



Administrators / privileged users
- Request privileged sessions & secrets
- Configuration

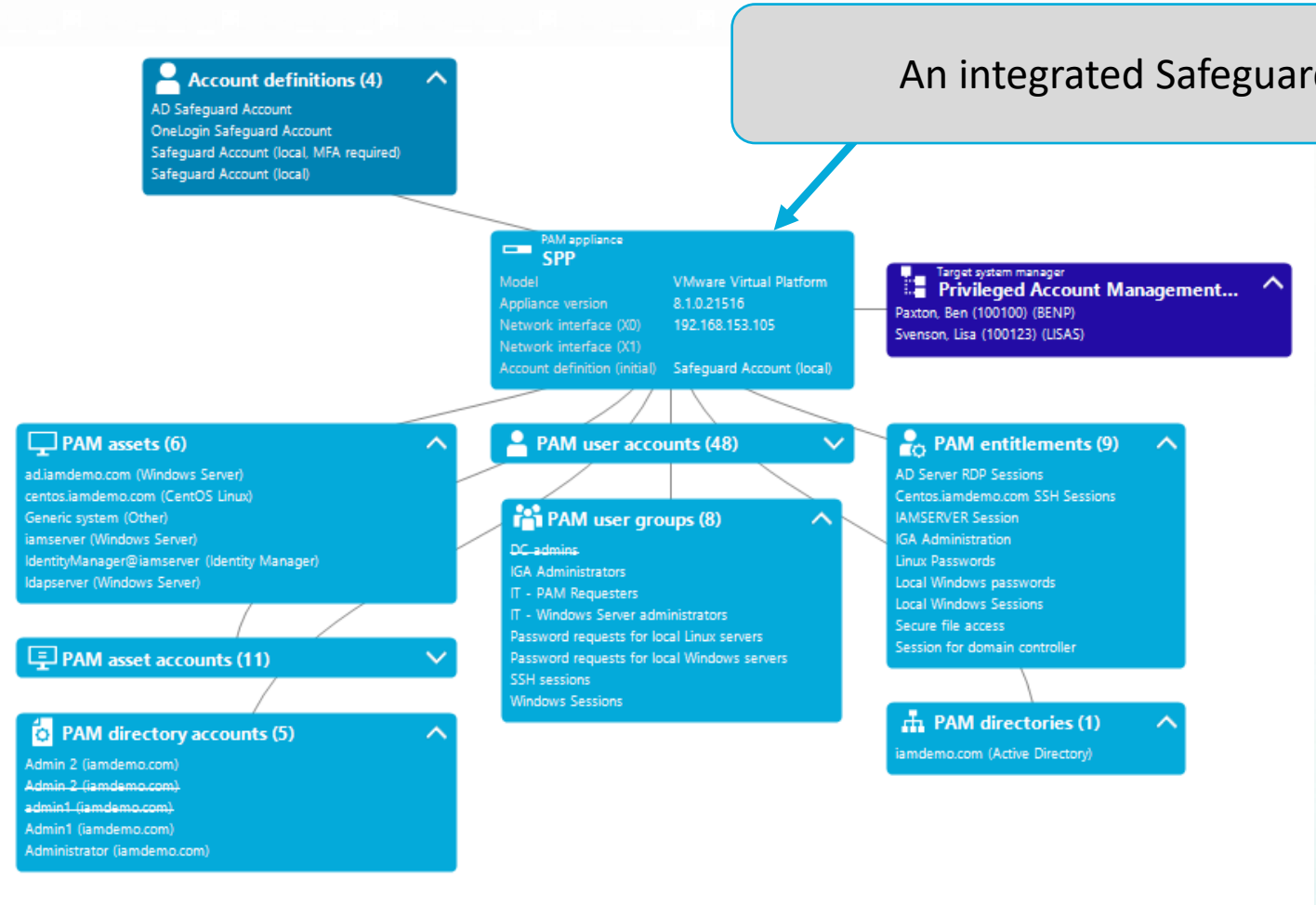
PAG module in Identity Manager

- **Unified identity lifecycle and provisioning processes**
  - Correlation of users to identities
  - Correlation of privileged accounts to user accounts in synchronized target systems
  - Provisioning users and user group memberships in Safeguard

- **Centralized governance, compliance and policy administration**
  - Attestation/Recertification of Access to Safeguard objects
  - Compliance rules and policies
  - Workflows, Reports and Dashboards
  - Behavior Driven Governance

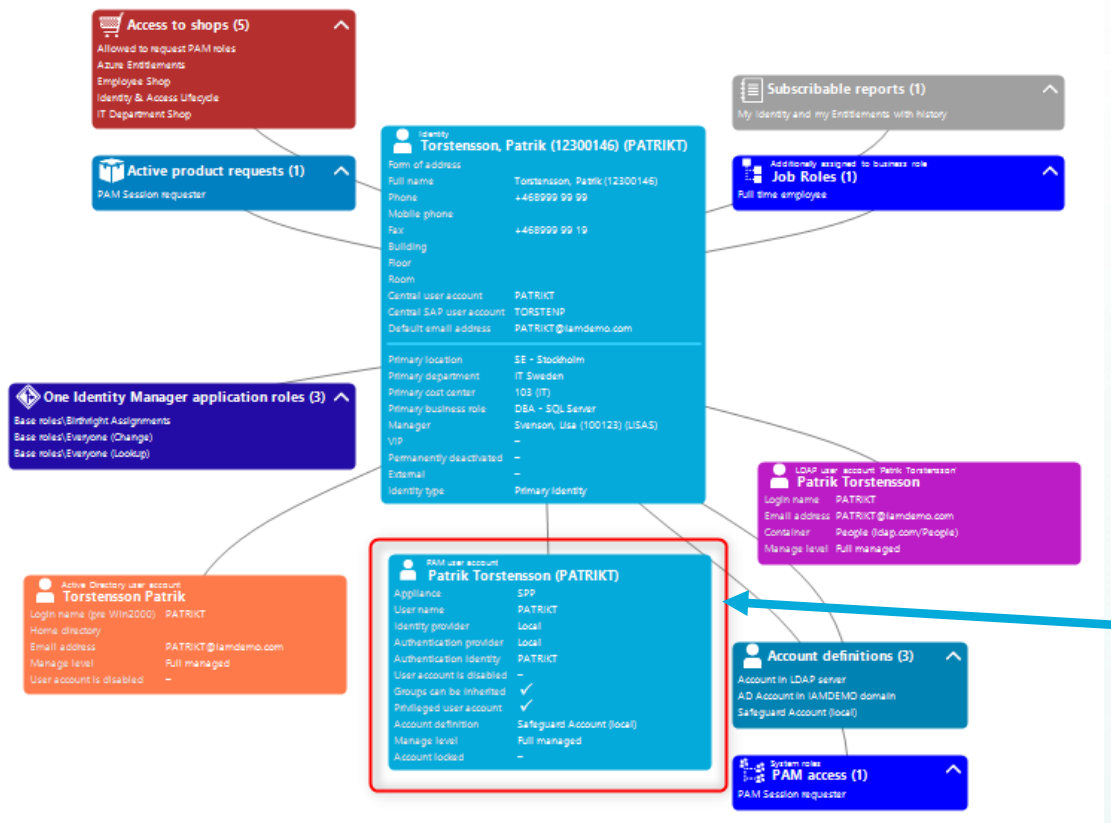
Privileged Access Governance

Integration to PAM platforms



Privileged Access Governance

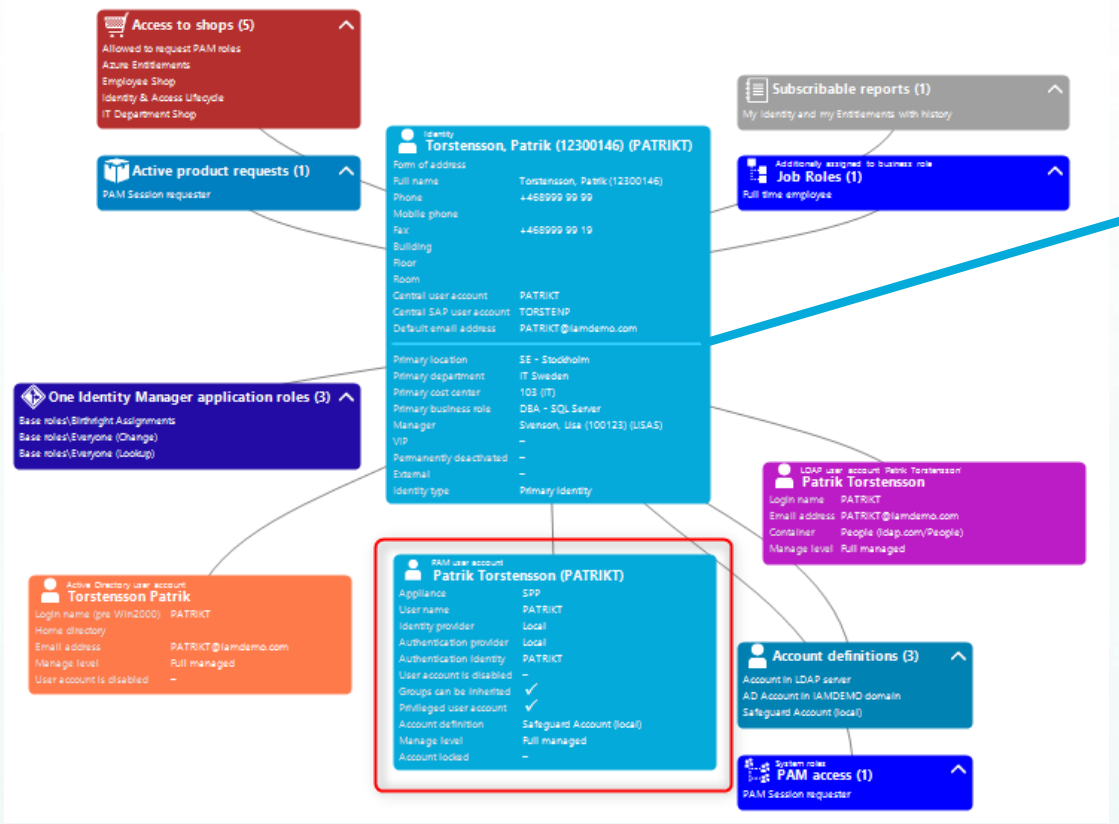
360° view of managed persons

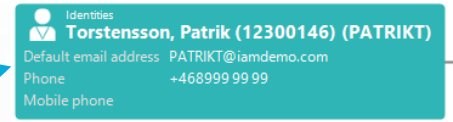


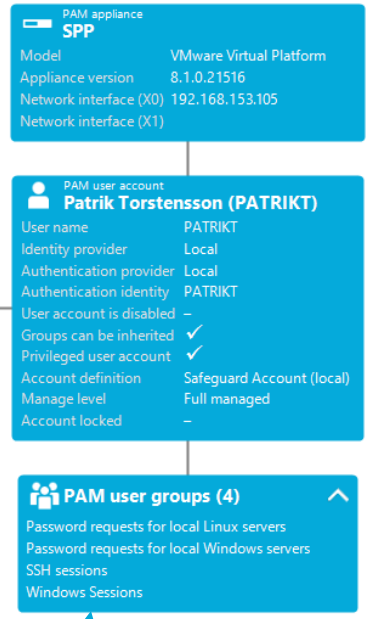
A person with a PAM user account

Privileged Access Governance

360° view of managed persons



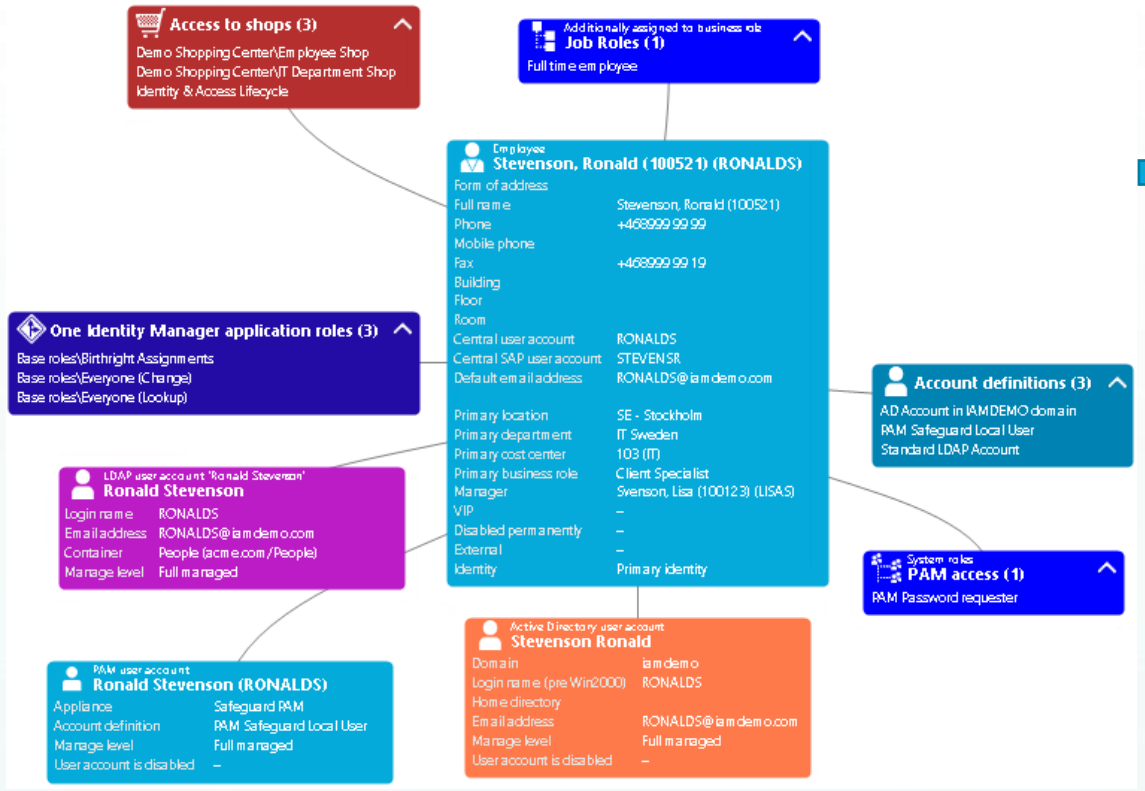


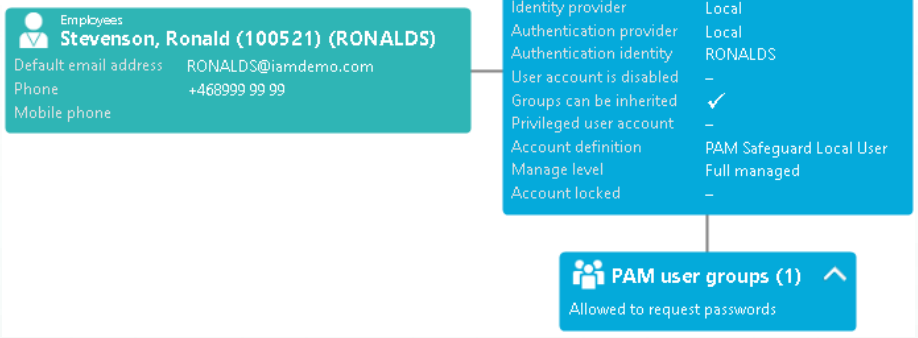


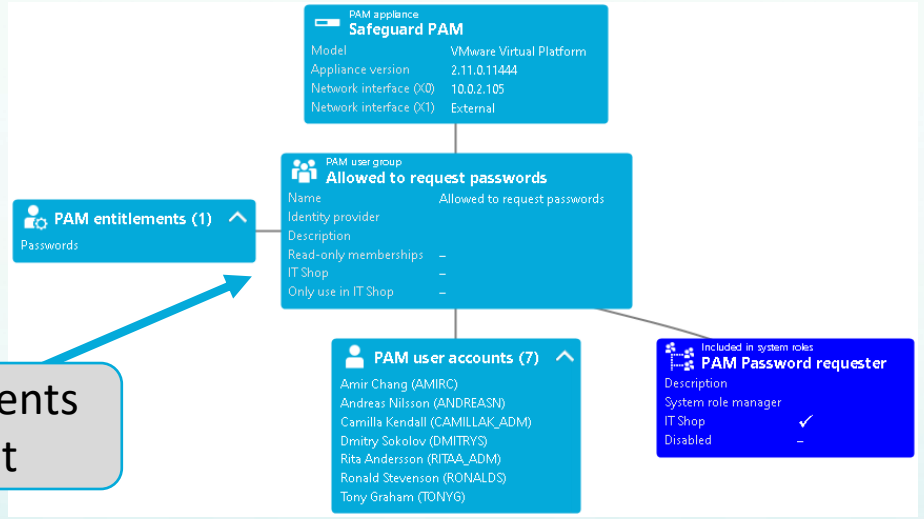
More information on the PAM user account…

Privileged Access Governance

360° view of managed persons



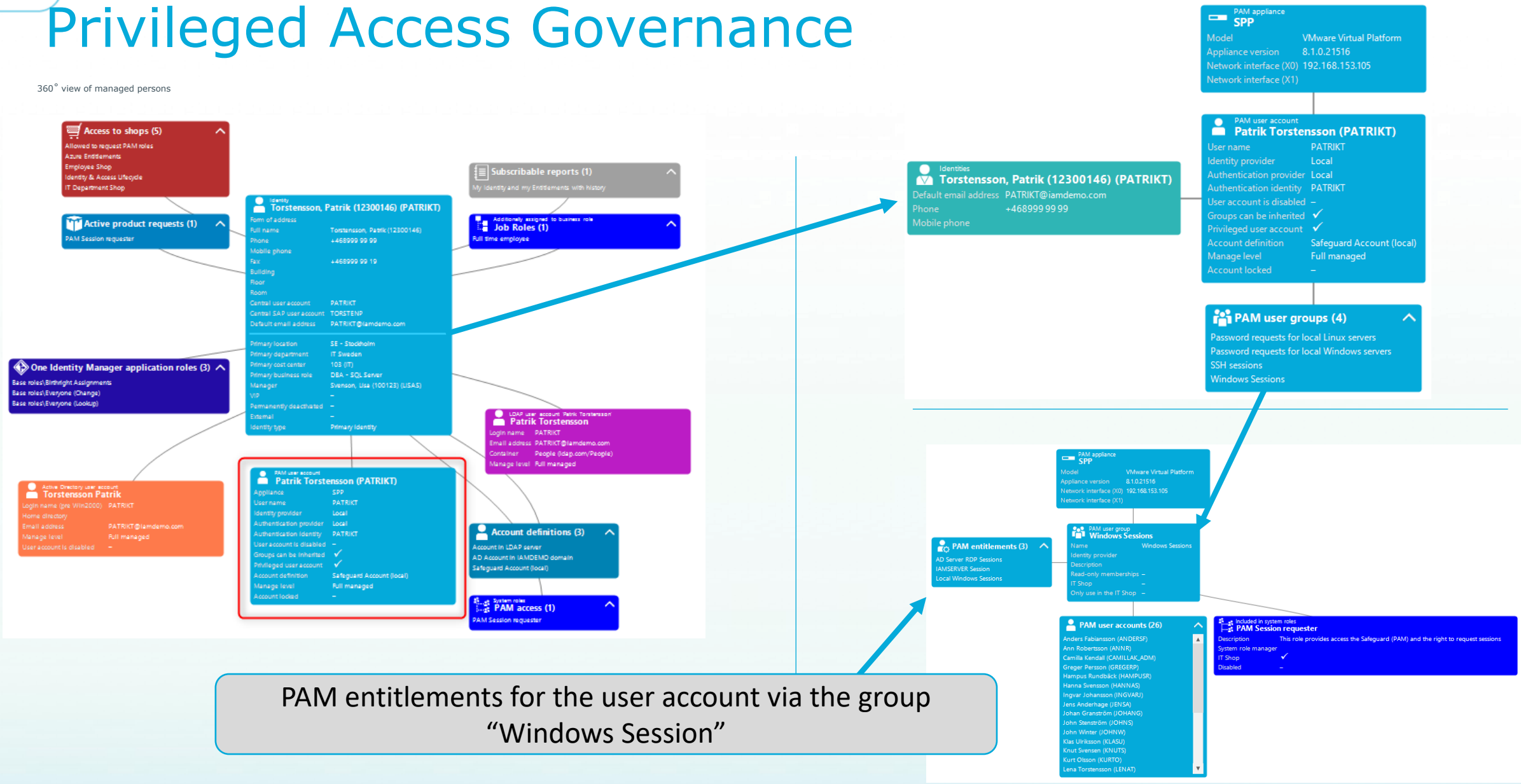




And the PAM entitlements for the user account

Privileged Access Governance

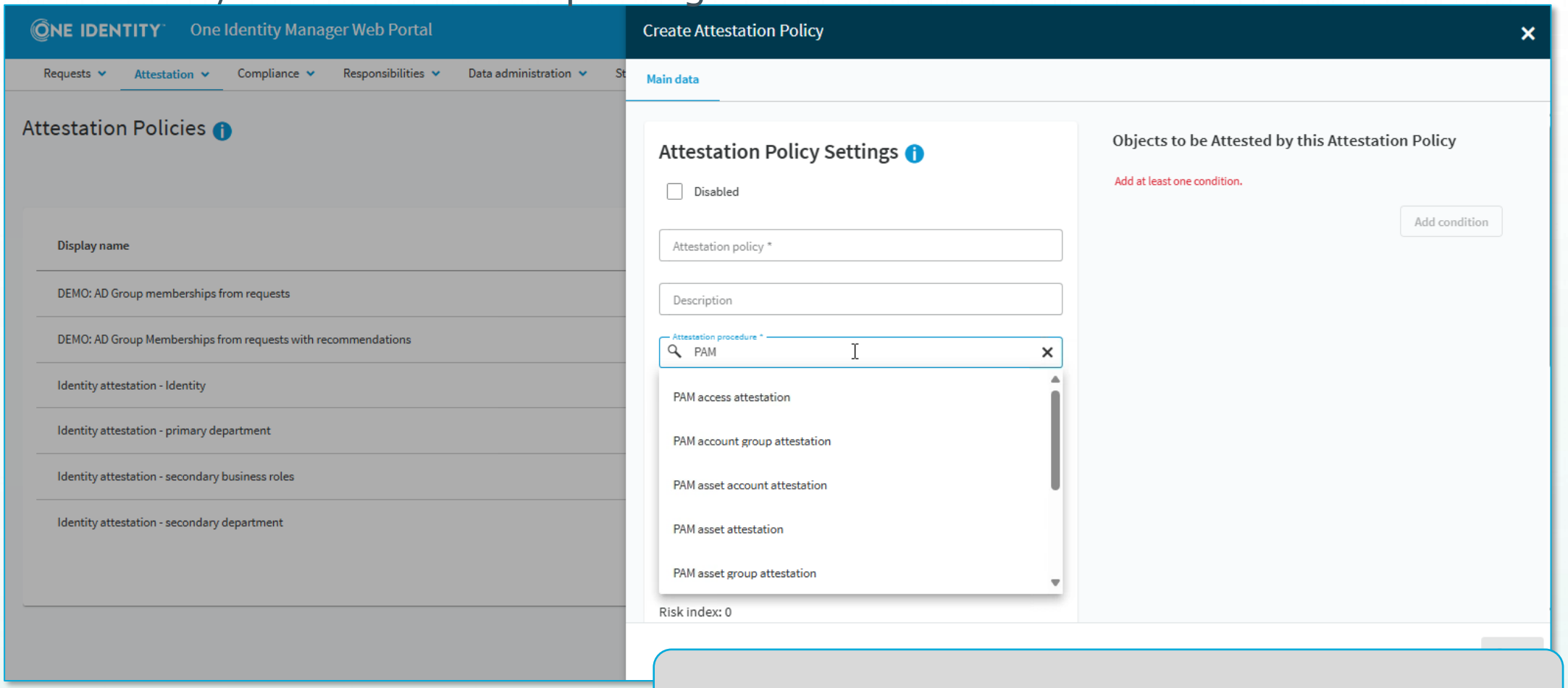
360° view of managed persons



PAM entitlements for the user account via the group “Windows Session”

Privileged Access Governance

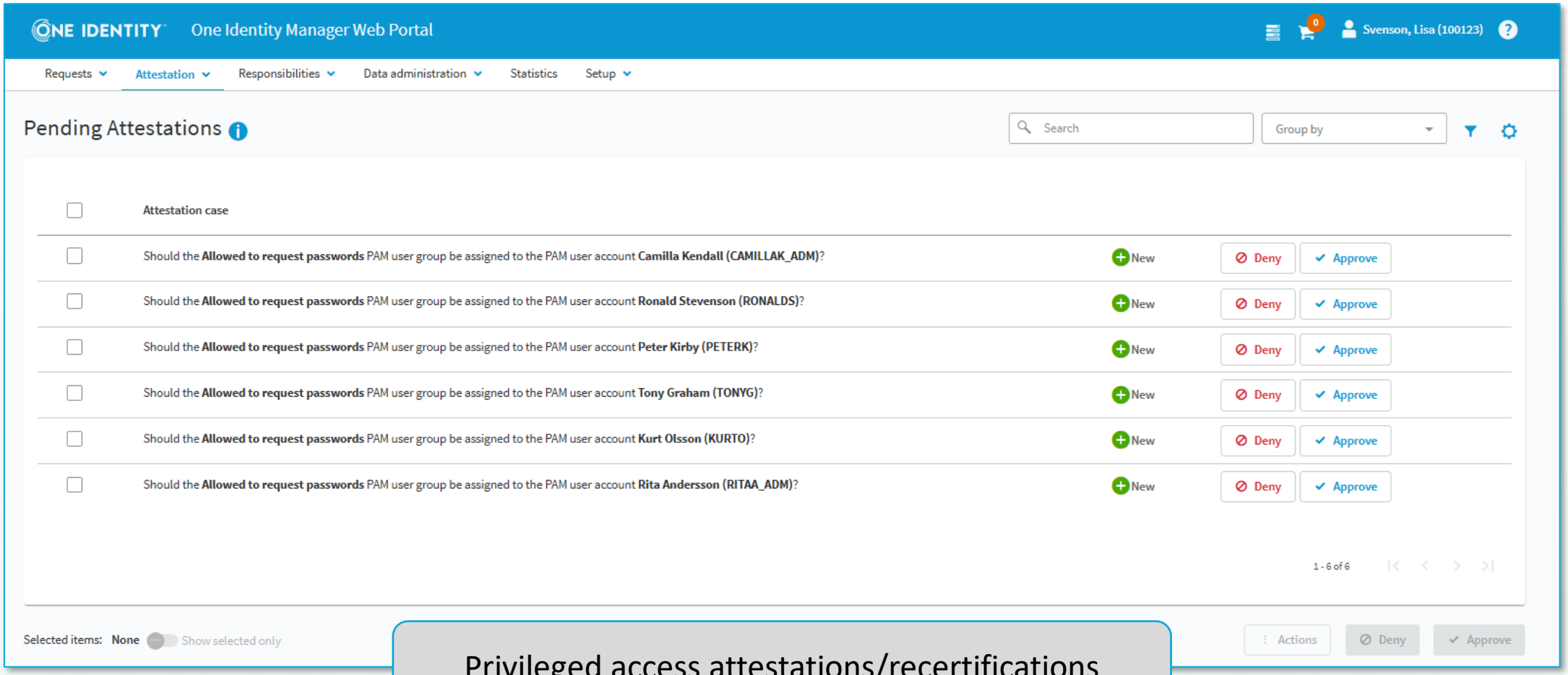
Attestation/recertification of privileged access



Comprehensive Privileged Account Governance options…

Privileged Access Governance

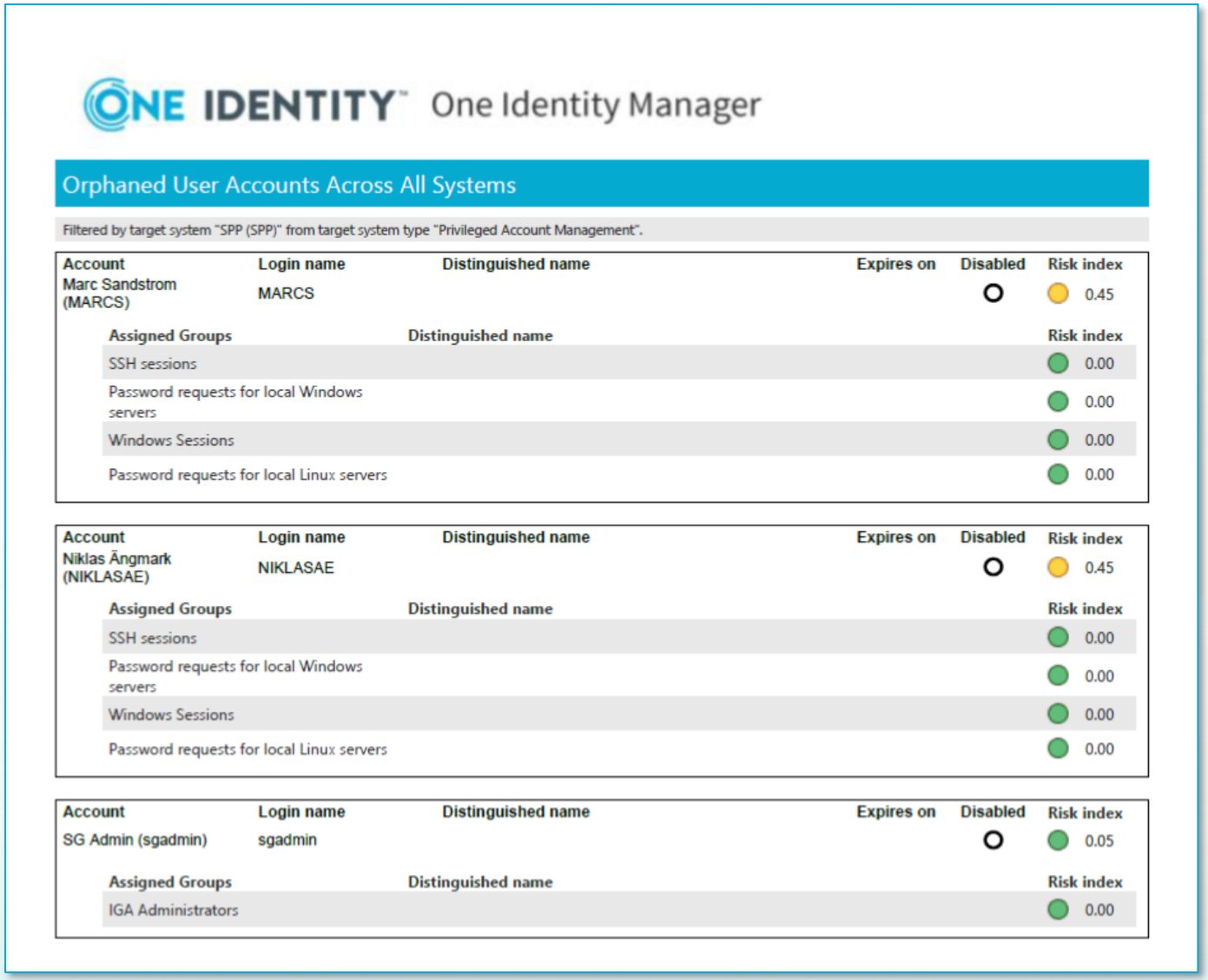
Attestation/recertification example:



Privileged access attestations/recertifications

Privileged Access Governance

Report example that shows orphaned PAM user accounts



ONE IDENTITY One Identity Manager

Orphaned User Accounts Across All Systems

Filtered by target system "SPP (SPP)" from target system type "Privileged Account Management".

Account	Login name	Distinguished name	Expires on	Disabled	Risk index
Marc Sandstrom (MARCS)	MARCS			○	0.45

Assigned Groups	Distinguished name	Risk index
SSH sessions		0.00
Password requests for local Windows servers		0.00
Windows Sessions		0.00
Password requests for local Linux servers		0.00

Account	Login name	Distinguished name	Expires on	Disabled	Risk index
Niklas Ängmark (NIKLASAE)	NIKLASAE			○	0.45

Assigned Groups	Distinguished name	Risk index
SSH sessions		0.00
Password requests for local Windows servers		0.00
Windows Sessions		0.00
Password requests for local Linux servers		0.00

Account	Login name	Distinguished name	Expires on	Disabled	Risk index
SG Admin (sgadmin)	sgadmin			○	0.05

Assigned Groups	Distinguished name	Risk index
IGA Administrators		0.00

Privileged Access Governance - summary

Technical Capabilities

- **360-Degree View:** Provides a complete, centralized view of all users, accounts (privileged and non-privileged), entitlements, and activities across the enterprise.
- **Provisioning & Deprovisioning:** Automates the lifecycle management of privileged accounts, ensuring timely and secure access changes.
- **Access Requests & Approvals:** Integrates privileged account access into enterprise-wide access request and approval workflows.
- **Delegation & Policy Enforcement:** Enables delegation of roles and responsibilities and enforces separation of duties (SoD) policies across all account types.
- **Attestation/Certification:** Supports ongoing certification and attestation of privileged access as part of regular governance processes.

Business Value

- **Increased Security:** Reduces risk by eliminating silos, ensuring proper provisioning, and providing visibility into all access rights.
- **Stronger Compliance:** Simplifies audit and compliance by centralizing reporting and enforcing consistent policies.
- **Better Governance:** Detects and corrects improper or redundant privileged access and unifies governance processes.
- **Lower Costs:** Streamlines administration by consolidating vendors and eliminating redundant processes.

MBCOM TECHNOLOGIES | vmware by Broadcom

Adria Forum 2025

Thank You !

Questions ?