PROTECT YOUR PRIVILEGED IDENTITIES AND DEVOPS PIPELINES IN MICROSOFT AZURE!

Limerick DotNet-Azure User Group (LDNA)

Thomas Naunheim

April, 2022

THOMAS NAUNHEIM

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

AGENDA

PRIVILEGED
IDENTITIES

PRIVILEGED
ACCESS

PRIVILEGED
PIPELINES

Level of Isolation and Seperation
= Your Balance of Security, Complexitity and Usability

PROTECTION OF **PRIVILEGED IDENTITIES**

Foundation of Privileged Accounts

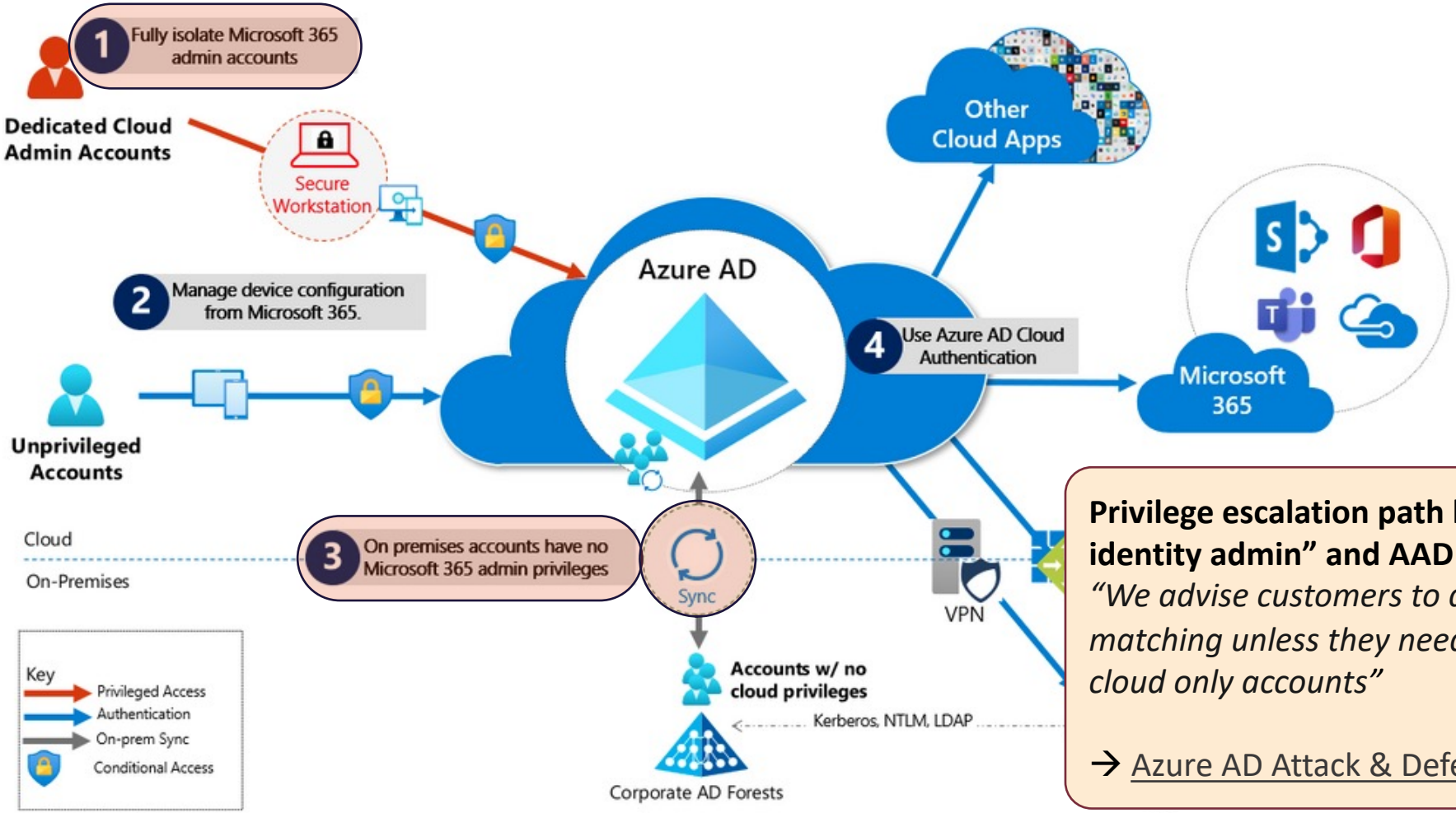
Separation of work and privileged accounts

- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Implement identity lifecycle and access review
- ✓ Remove licenses of productivity workloads

Secured and hardened Azure AD Tenant

- ✓ Strong tenant-level security baseline and active identity security posture management
- ✓ Consider external privileged access by Delegated Access Permissions (DAP) of CSP/MSP or consented (multi-tenant) apps
- ✓ Incident and Response for suspicious activities, Integrated Detections by MDA, IPC and MDC
- ✓ Isolation of work- and privileged resources

Protecting M365 and Azure from on-prem attacks

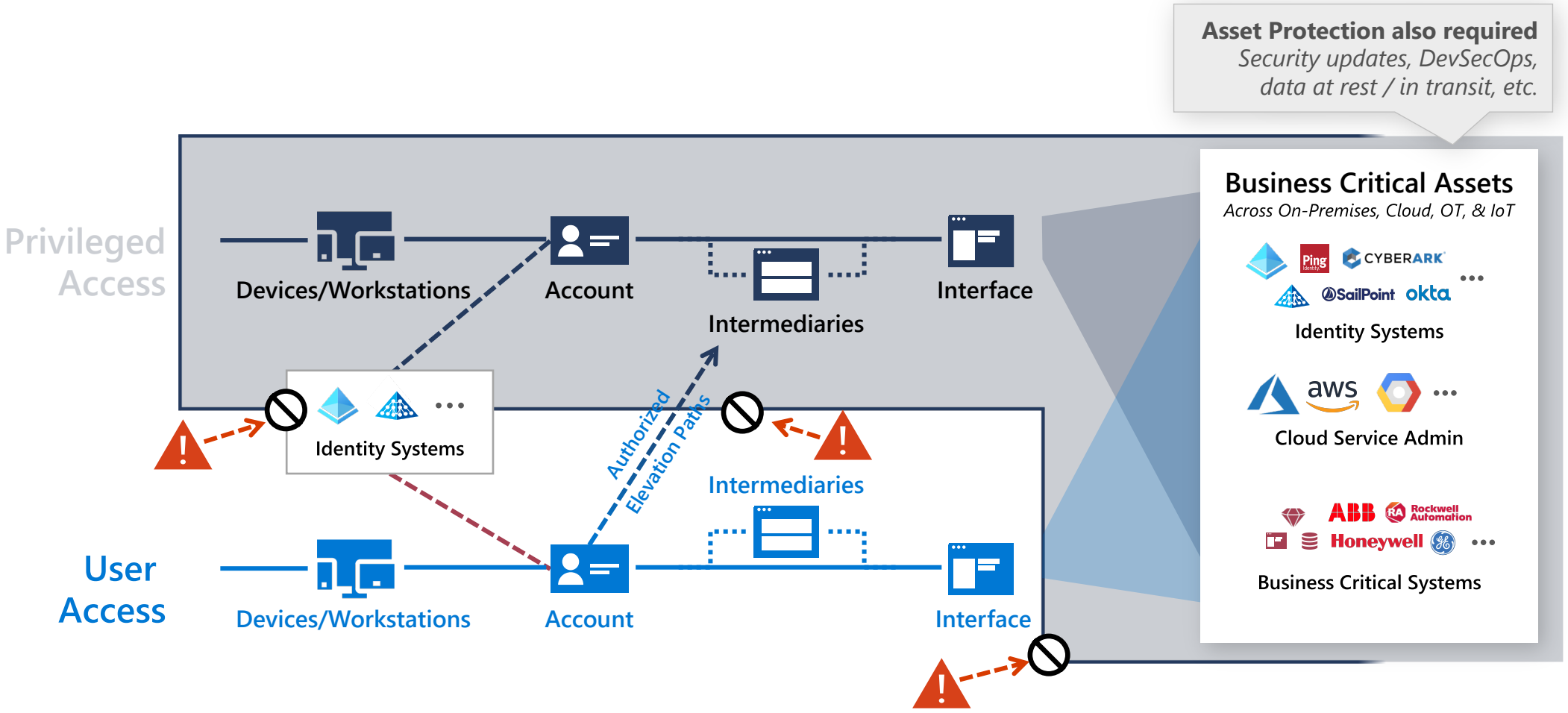


Privilege escalation path by "hybrid identity admin" and AAD Connect:
"We advise customers to disable soft matching unless they need it to take over cloud only accounts"

→ Azure AD Attack & Defense Playbook

Source: "Protecting Microsoft 365 from on-premises attacks" (Microsoft)

Privileged Access & Authorized Elevated Paths

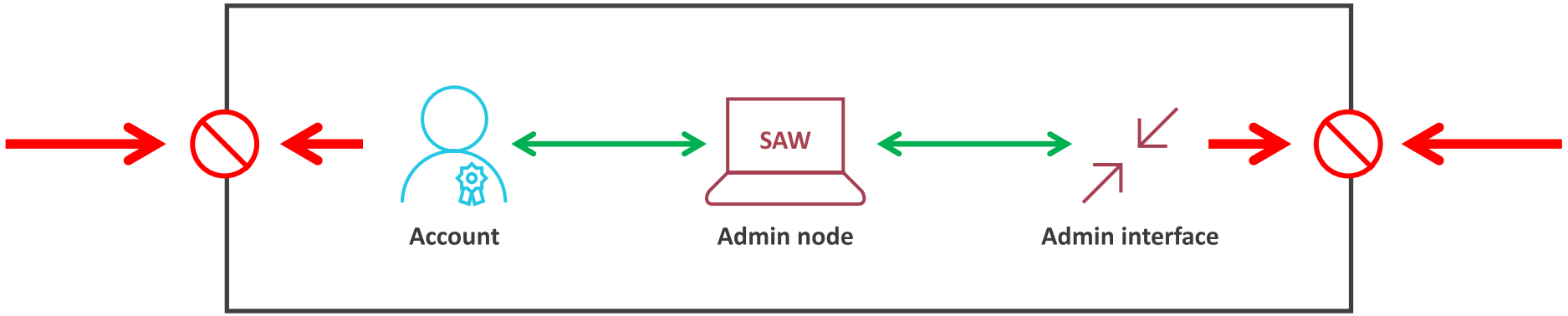


"End-to-end Session Security - Establish explicit Zero Trust validation for privileged sessions, user sessions, and authorized elevation paths."

Source: "Privileged access Strategy" (Microsoft)

Foundation of Secure Admin Workstations (SAW)

- **DISA STIG** requires Privilege Access Workstations (PAW) for Cloud Tenant Management
- **CIS (C4)**: Administrators shall use a dedicated, isolated machine for all administrative tasks
- **Azure Security Benchmark (PA-6)**: Use privileged access workstations (Secured, isolated workstations…)



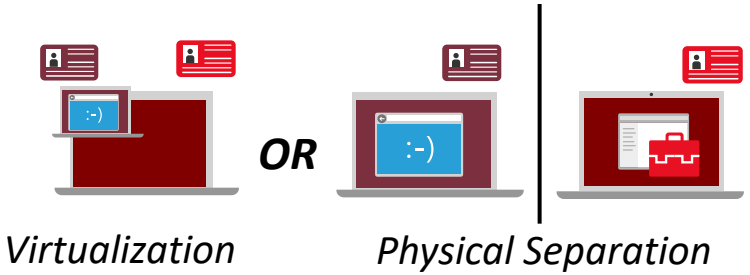


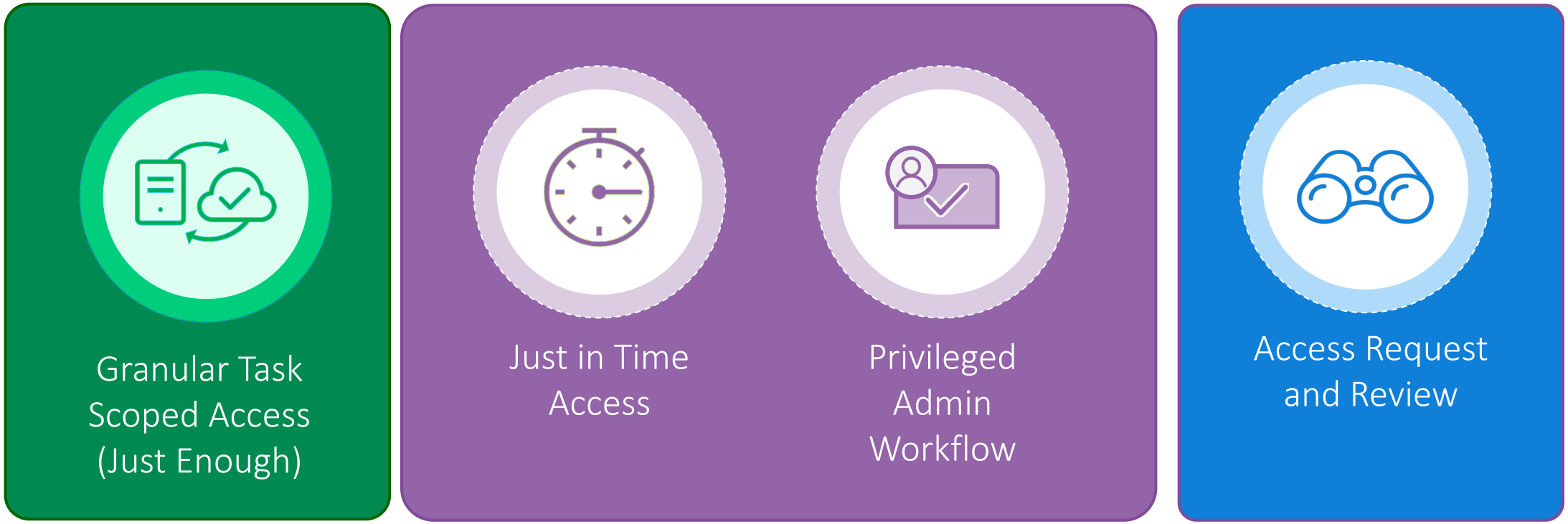
Image source: "Microsoft CISO Workshop 4a - Threat Protection Strategy"

Conditional Access + SAW for Admins and Monitoring of Privileged Identities

LIVE DEMO

SECURING
PRIVILEGED ACCESS

Foundation of Privileged Access



Cloud Infrastructure Entitlement Management (CIEM)

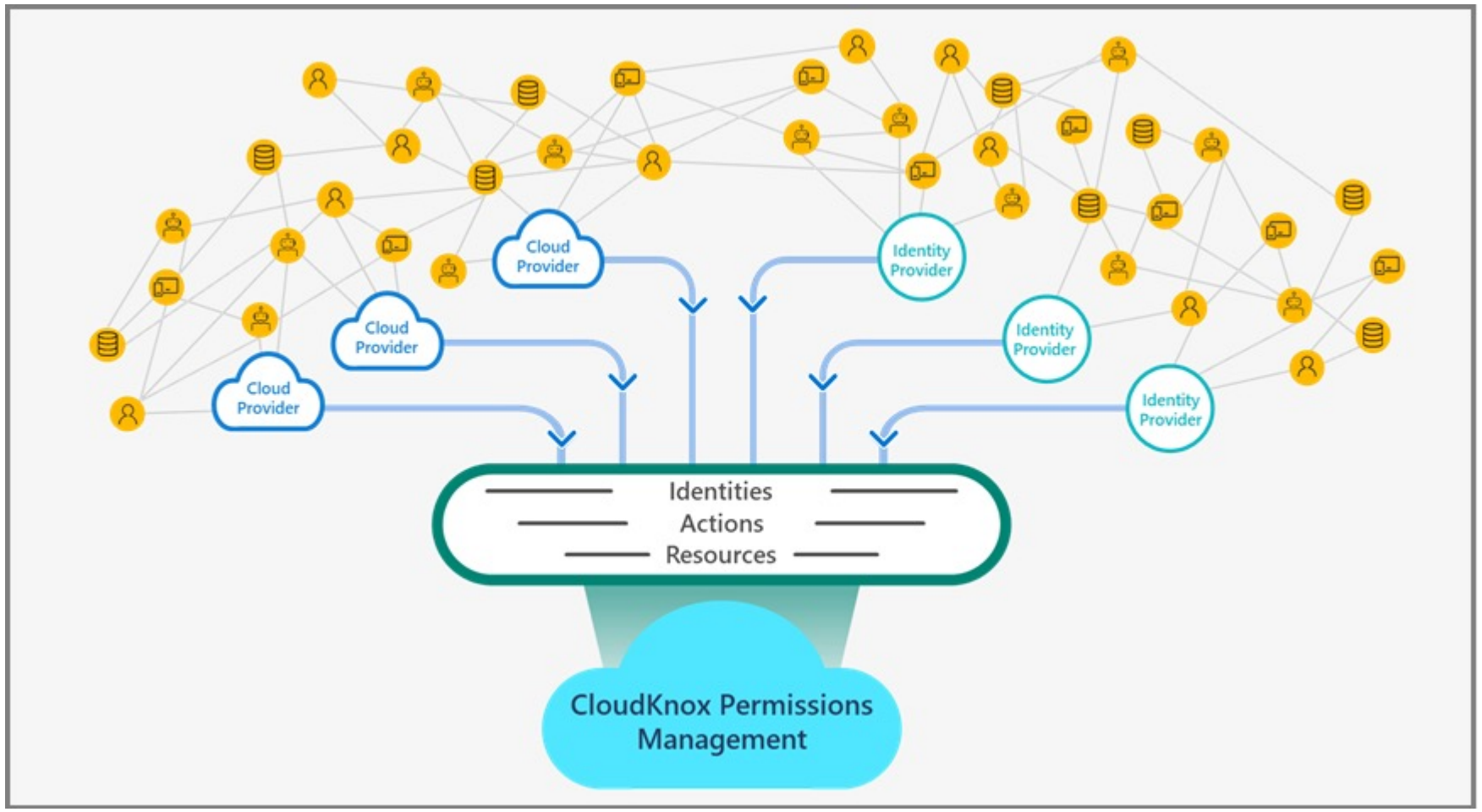


Image source: Microsoft (What's CloudKnox Permissions Management?)

Uncover and closing “Cloud Permissions Gap”

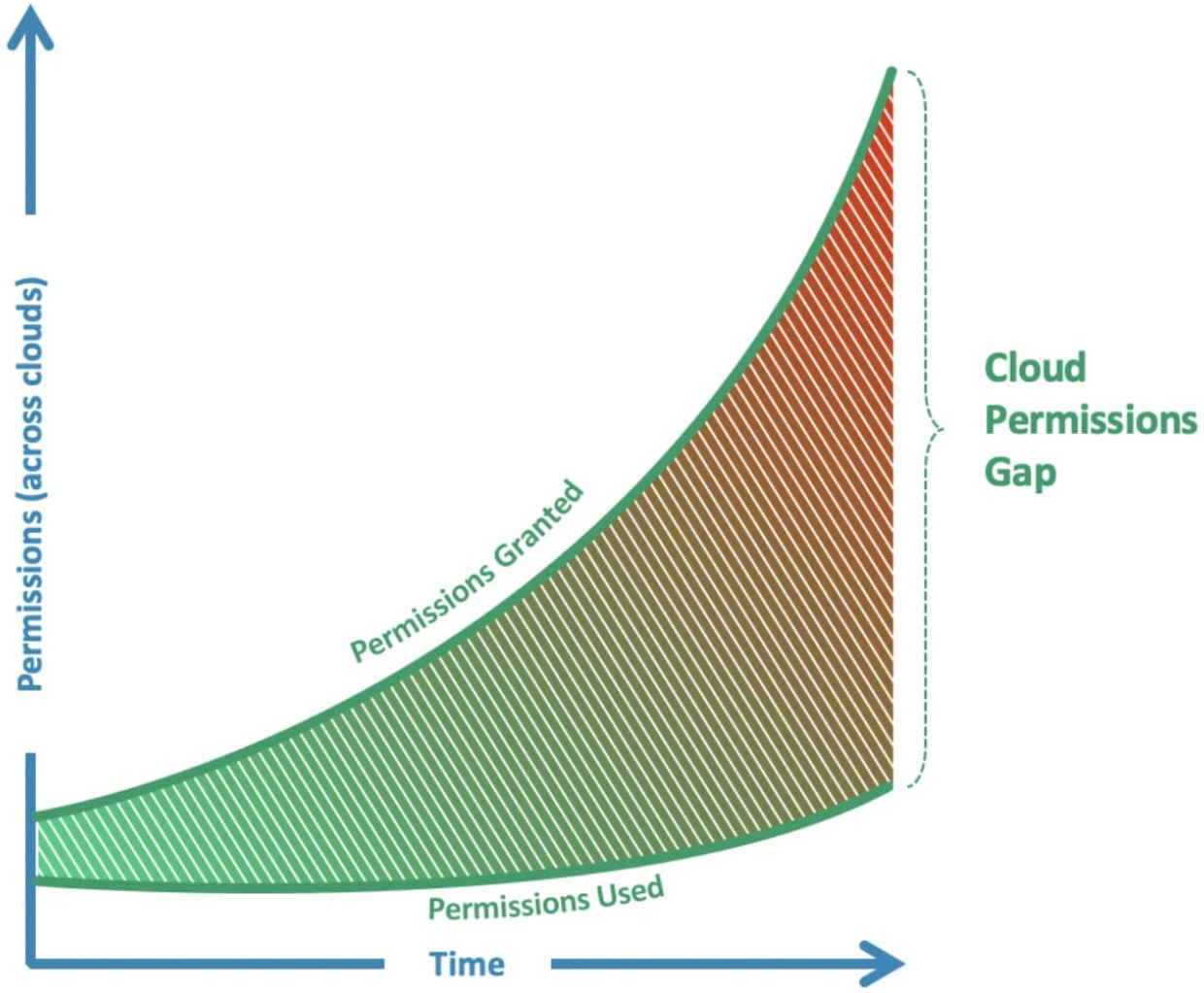
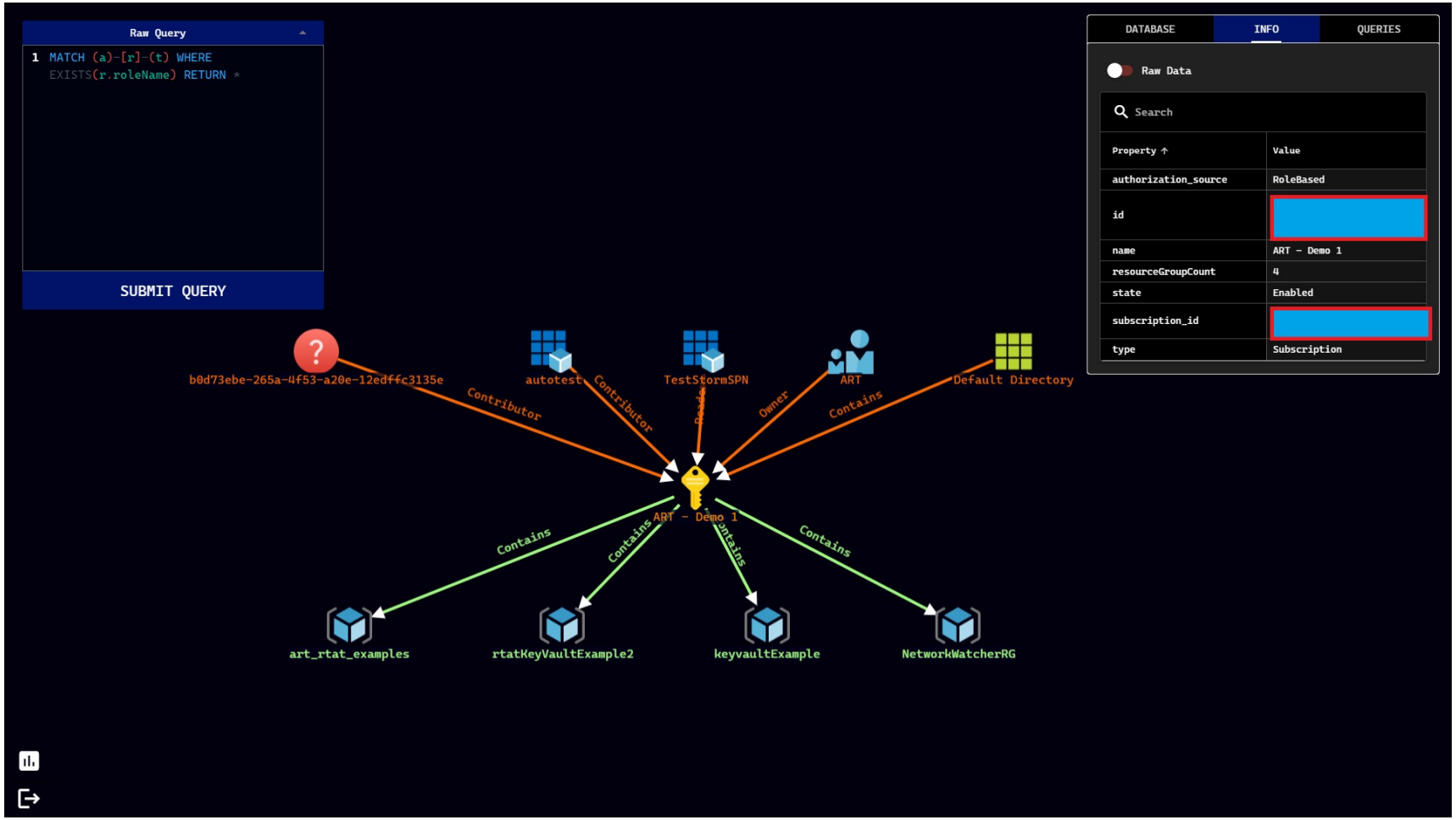


Image source: Microsoft (What's CloudKnox Permissions Management?)

Consideration of Privileged Access/Escalation Path

STORMSPOTTER



Administrative Tier Model

„To mitigate risk of identity compromise, or bad actors, implement **tiered administration** and ensure that you **follow principles of least privilege for Azure AD Administrator Roles**.“

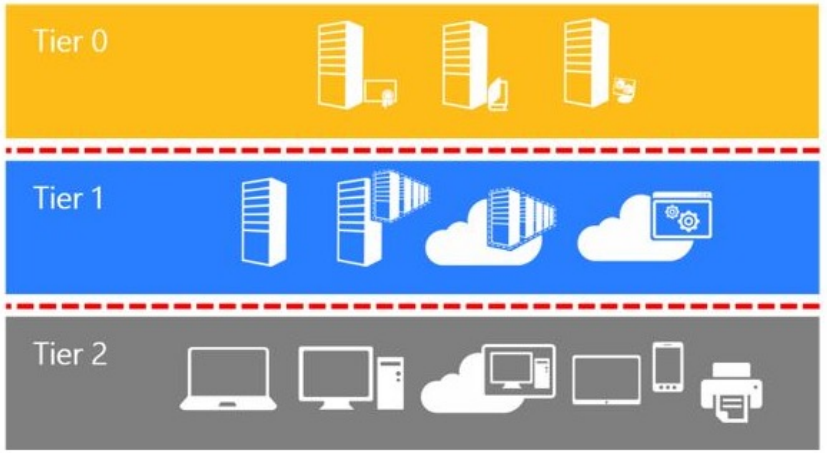
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

Active Directory administrative tier model

02/14/2019 • 33 minutes to read • +6

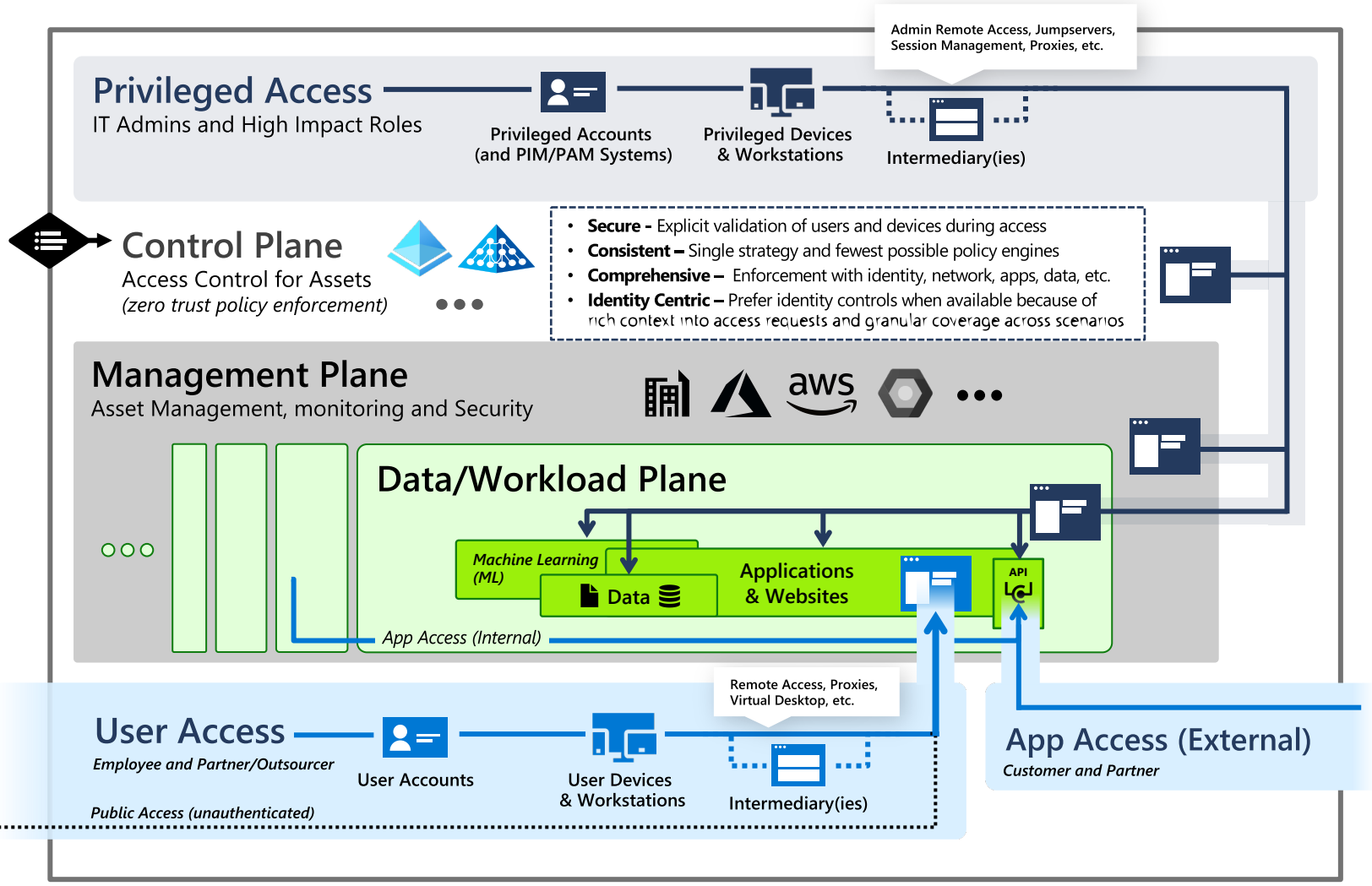
Applies To: Windows Server

The purpose of this tier model is to protect identity systems using a set of buffer zones between full control of the Environment (Tier 0) and the high risk workstation assets that attackers frequently compromise.



Source: “Securing Azure environments with Azure Active Directory”

Enterprise Access Model (EAM)



Privileged Access

Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes

Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

Data/Workloads

Create and store business value in

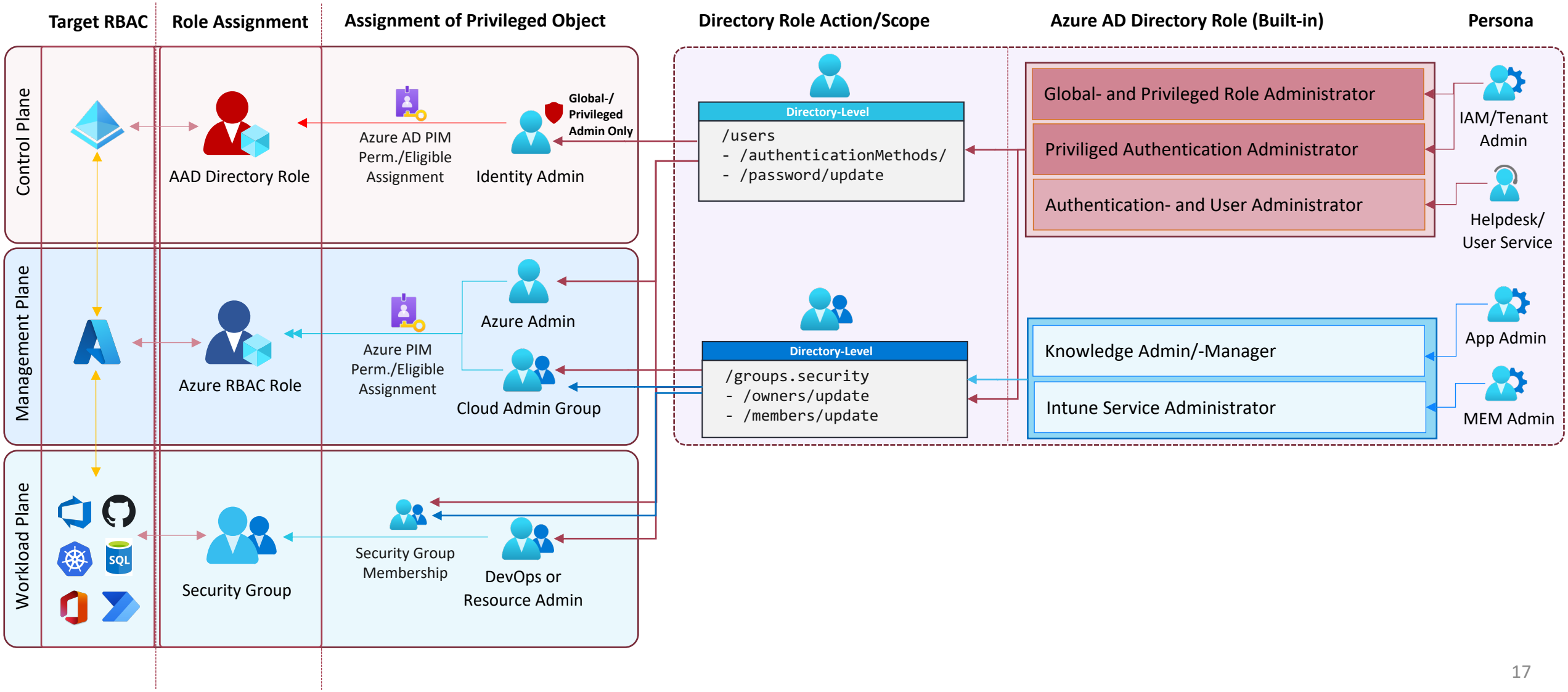
- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access

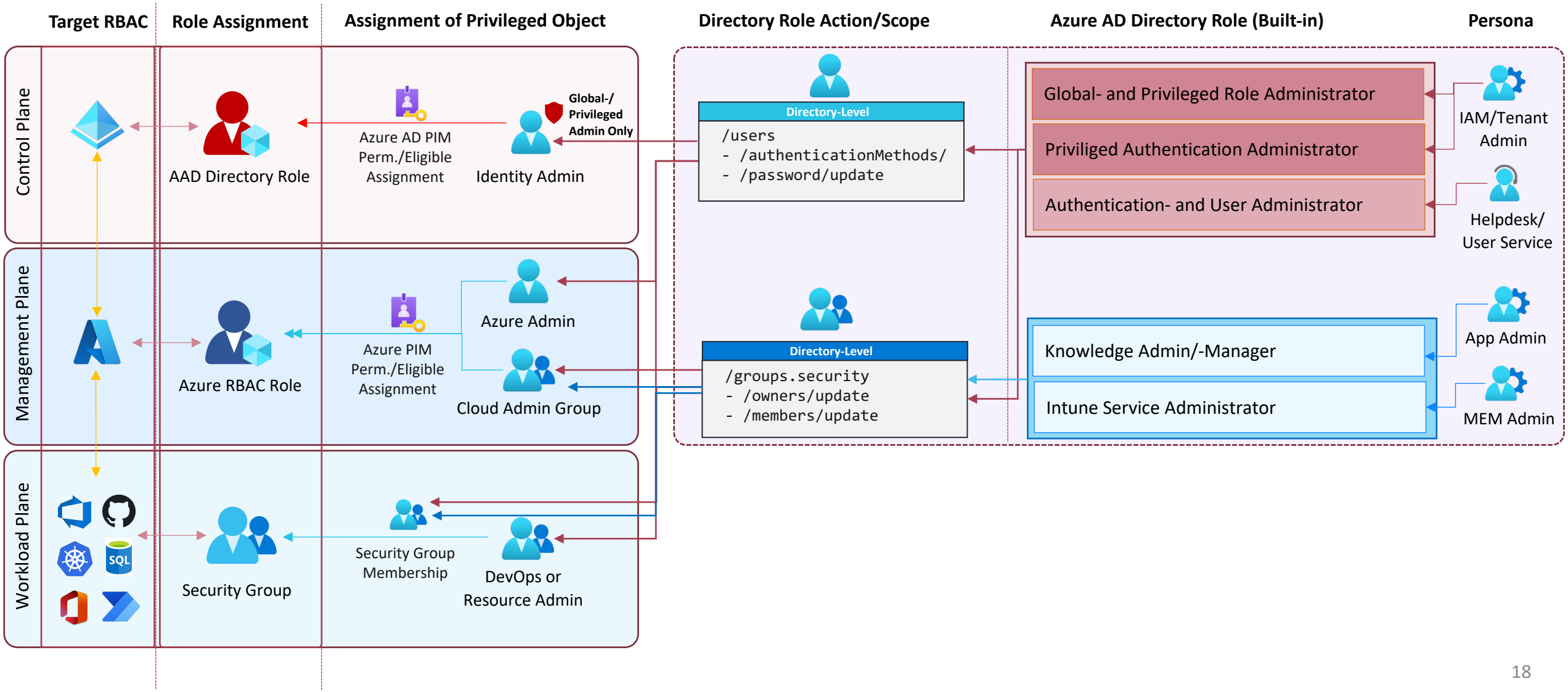
How employees, partners, and customers access these resources

Source: "Securing Azure environments with Azure Active Directory"

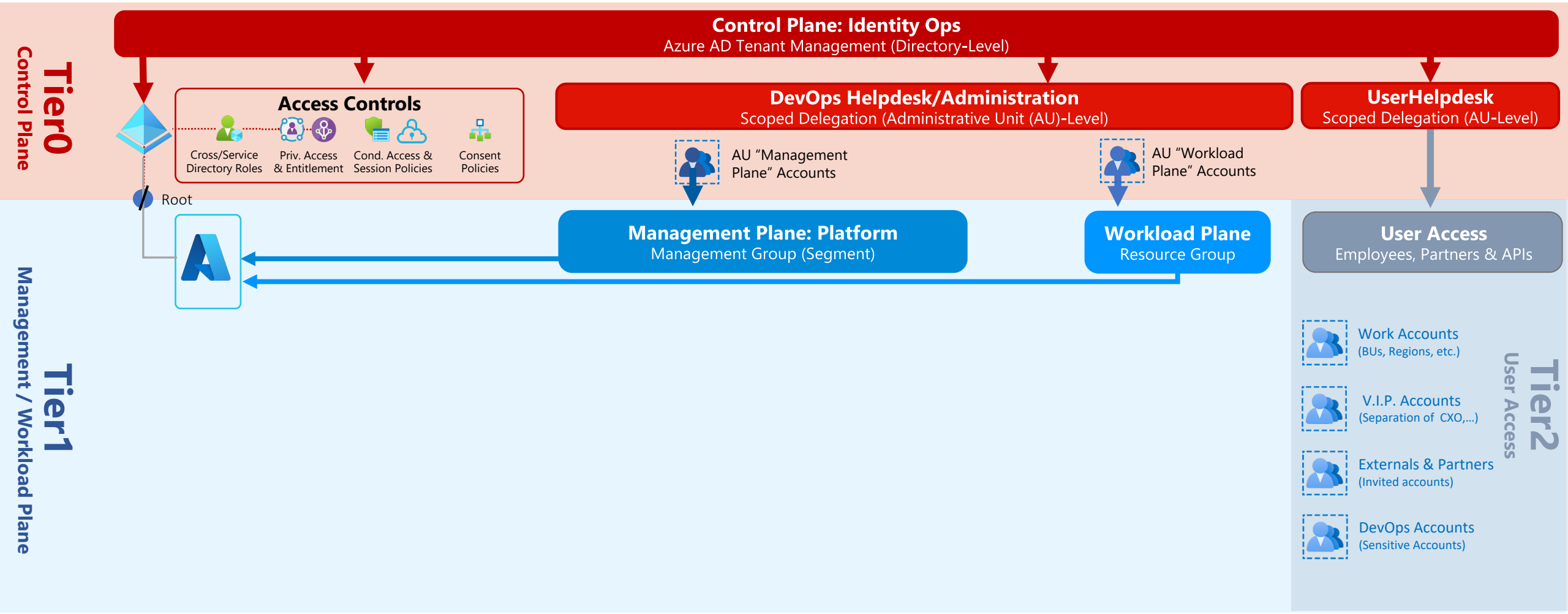
Privileged Access in Microsoft Cloud Services



Privileged Access in Microsoft Cloud Services



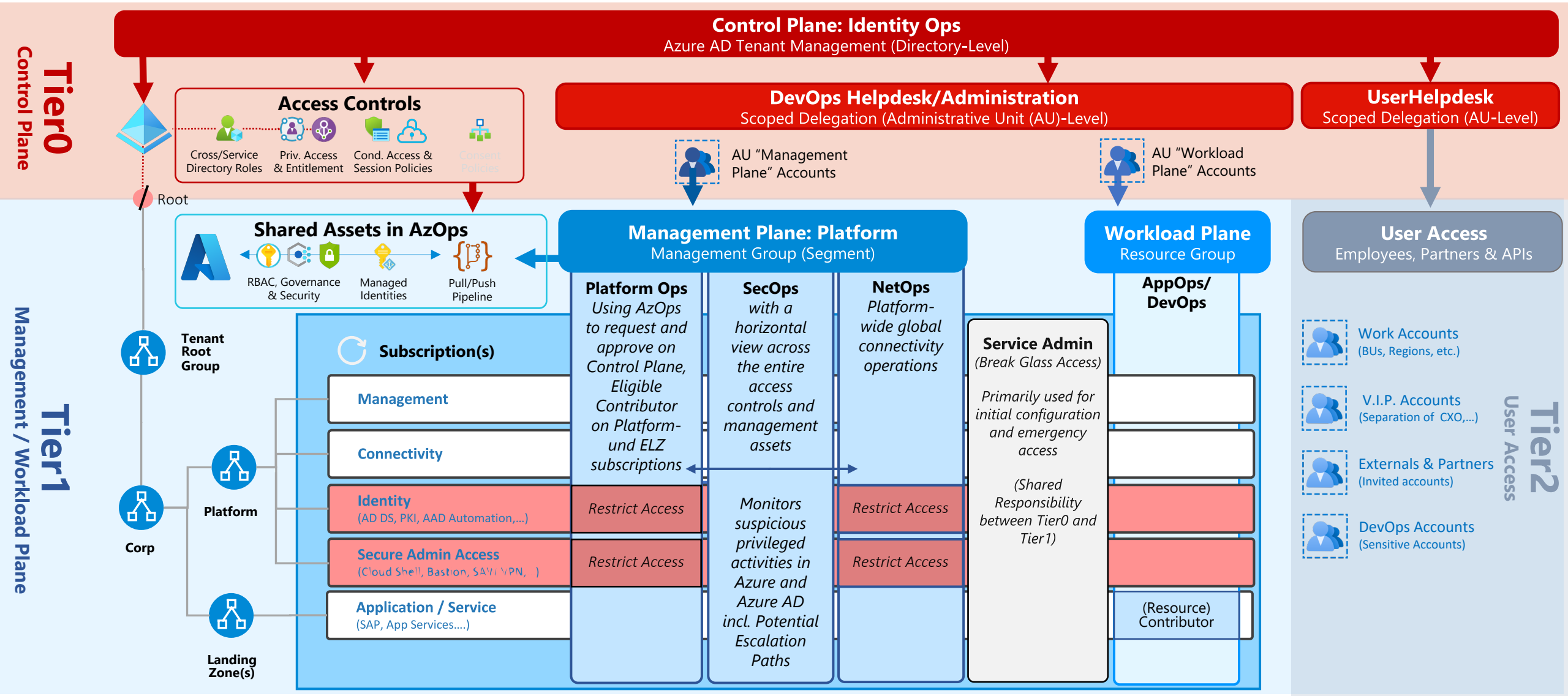
Privileged Access and Service-Specific Roles



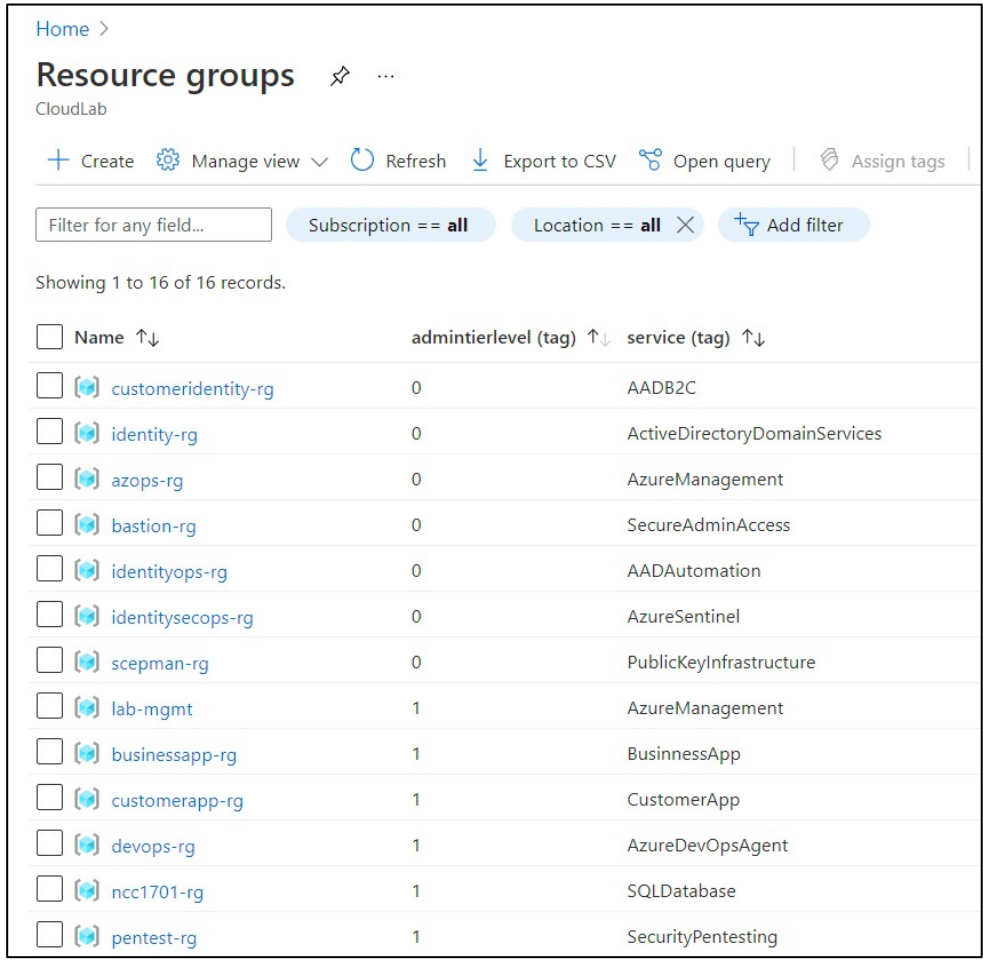
Isolation of IAM assets
on Control and Management Plane

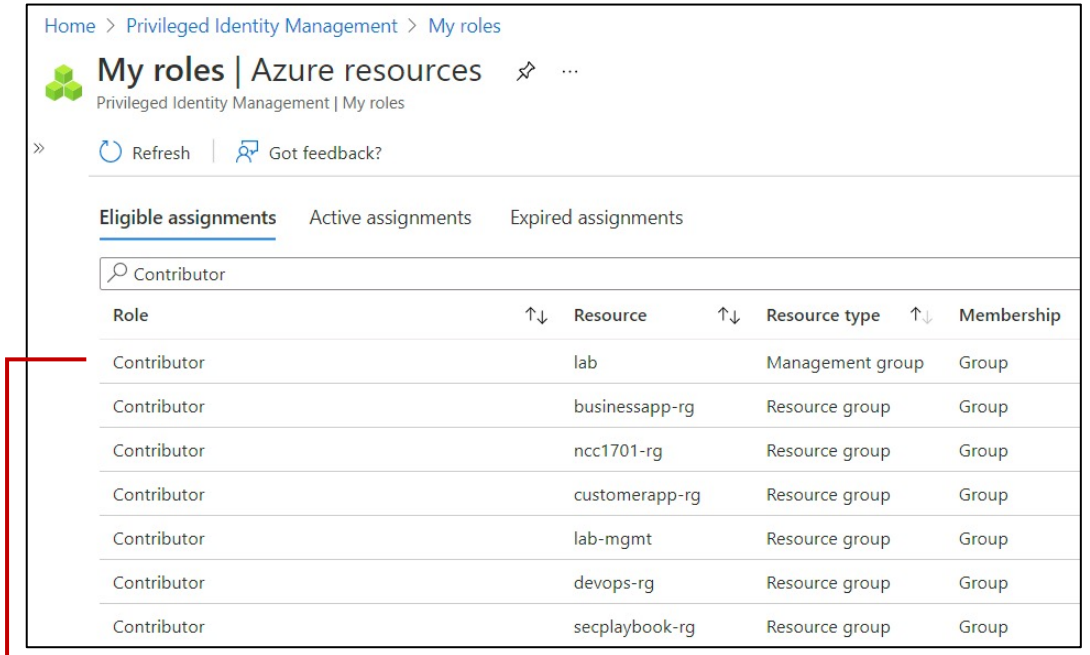
LIVE DEMO

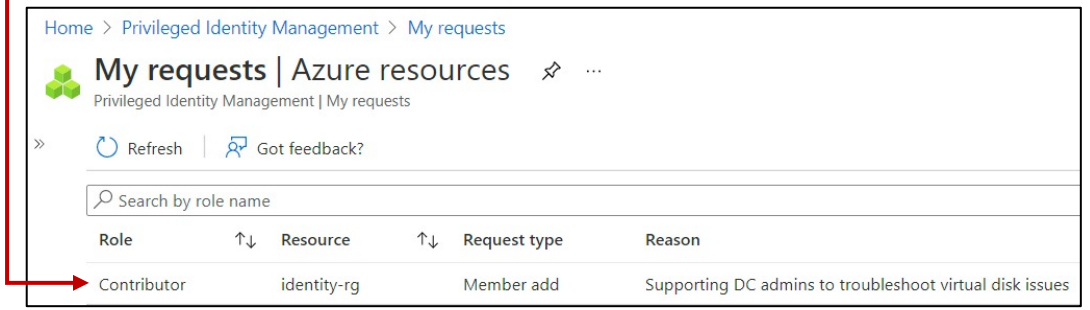
My implementation of “EAM” in Azure



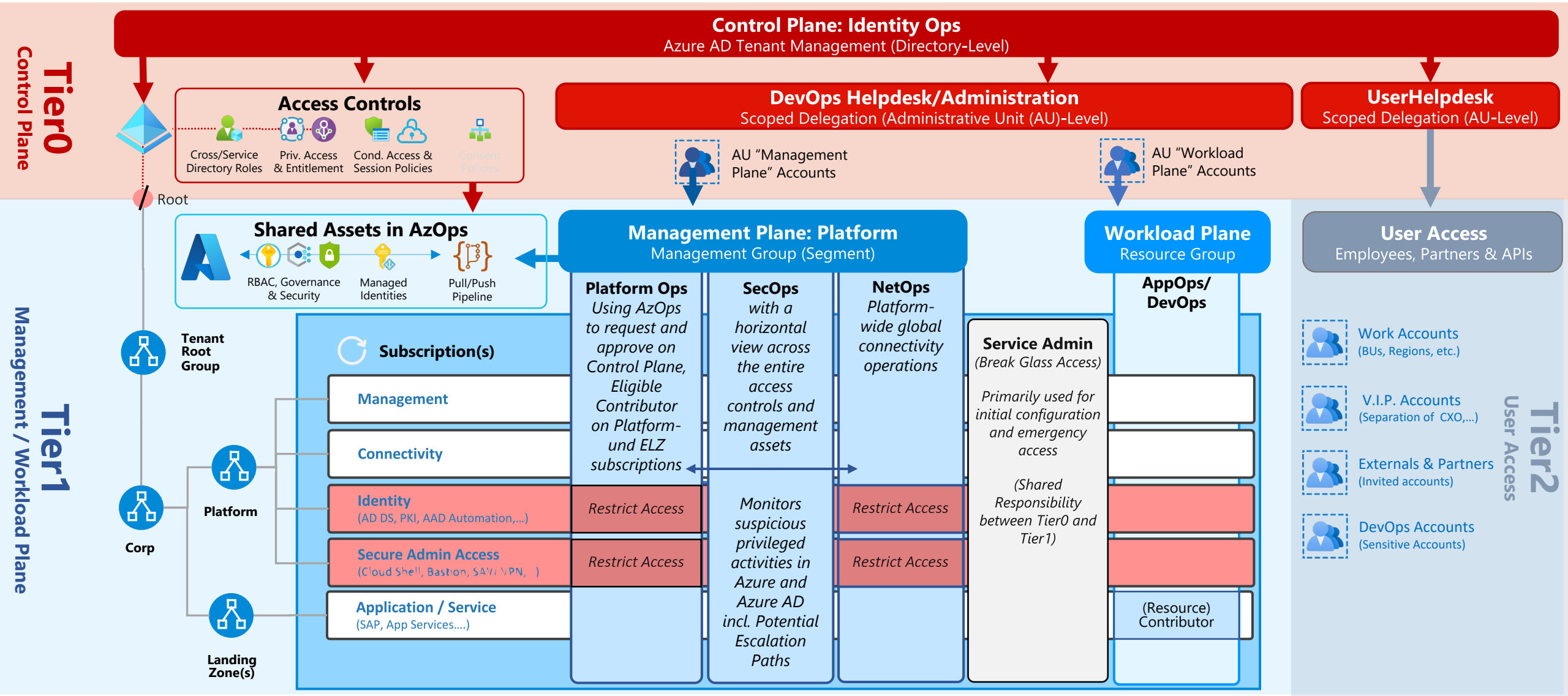
Tagged Control Plane Assets with Azure PIM Approval



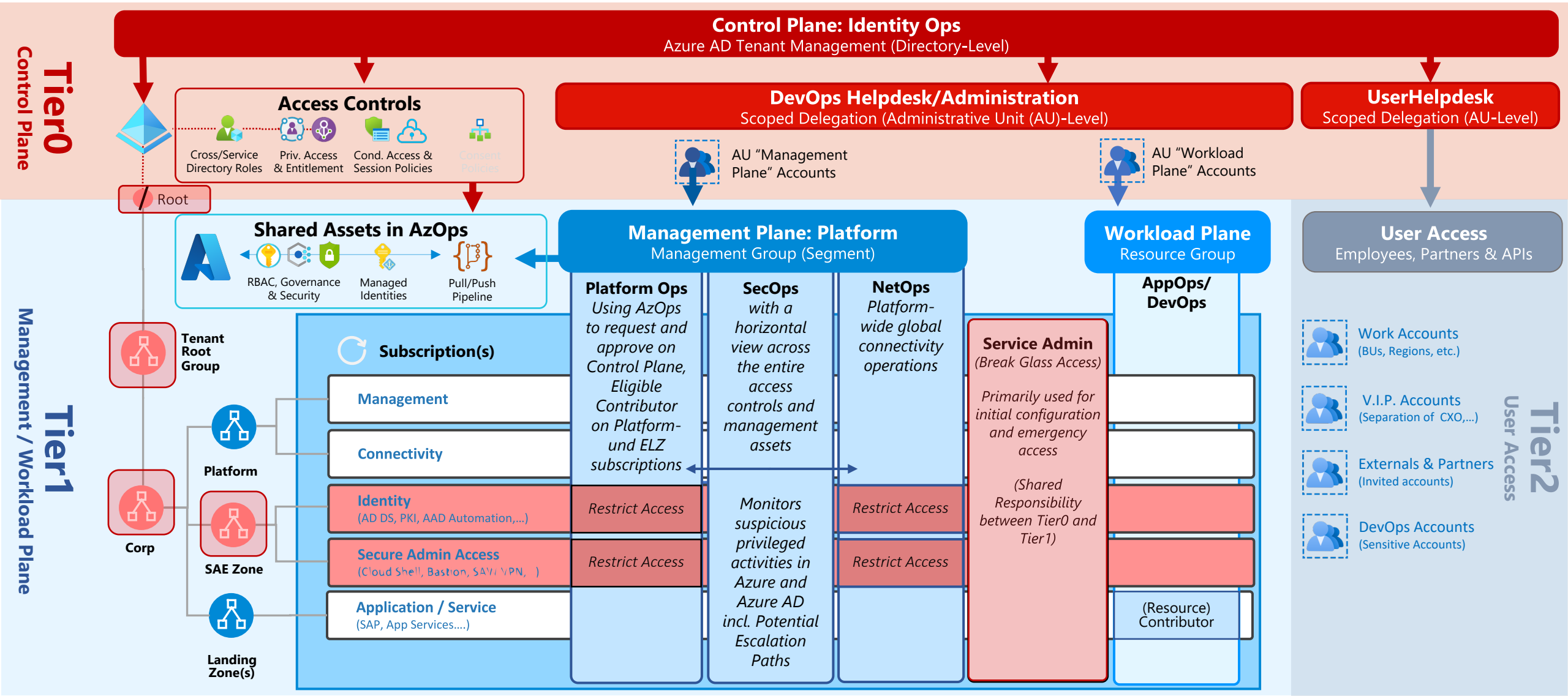




My implementation of “EAM” in Azure



My implementation of “EAM” in Azure

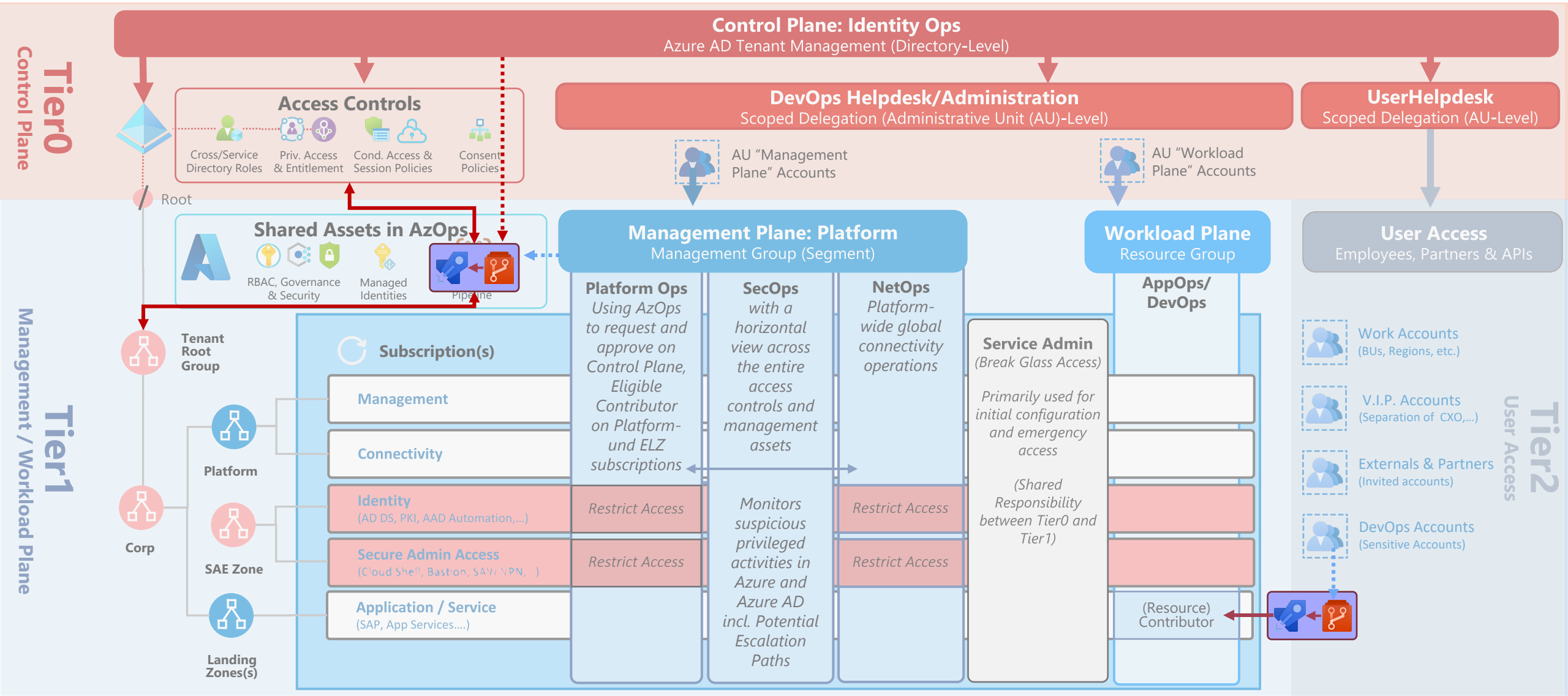


AzOps and AADOps

Management of Privileged Assets in Azure

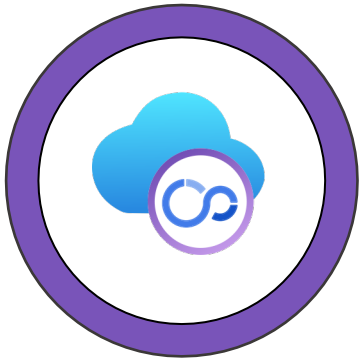
LIVE DEMO

Privileged CD/Release Pipelines in Azure

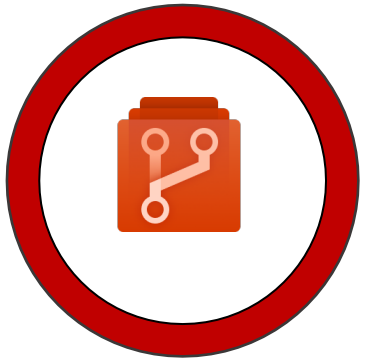


PRIVILEGED
DEVOPS PIPELINES

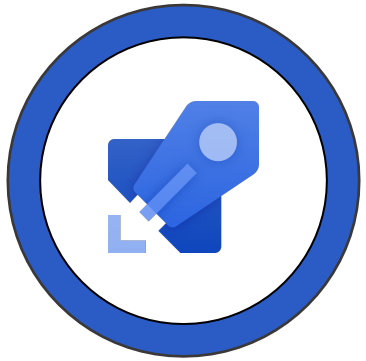
Foundation of Pipelines in Dev(Sec)Ops



Security Posture and RBAC Management of DevOps Platform



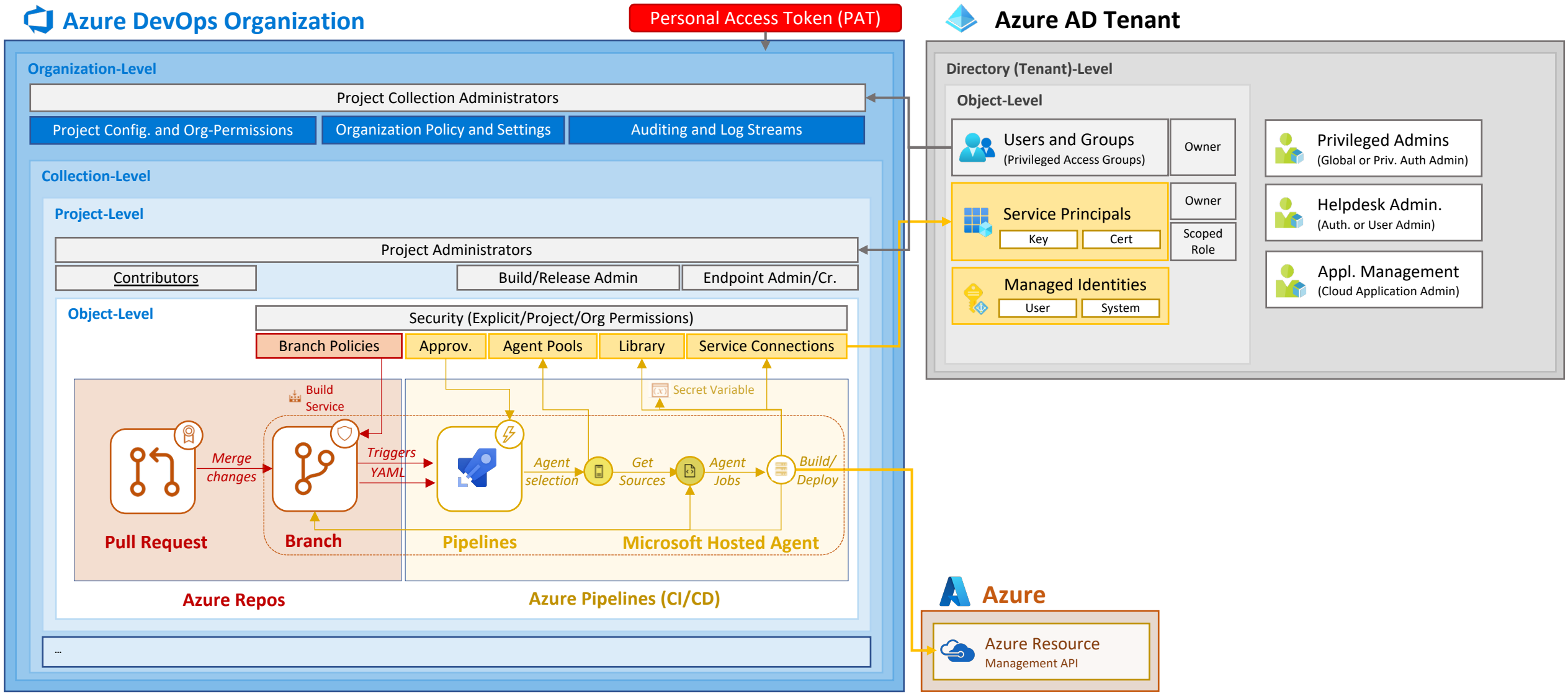
Repository Protection and Compliance Policies



Restricted and audited pipelines on secured agents

Protection and Monitoring of Workload Identity

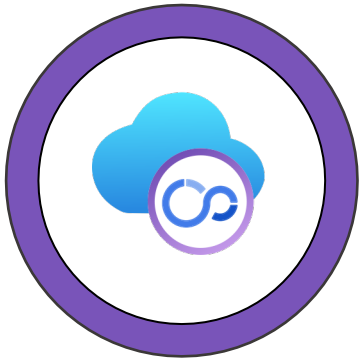
Overview of Azure DevOps and Security



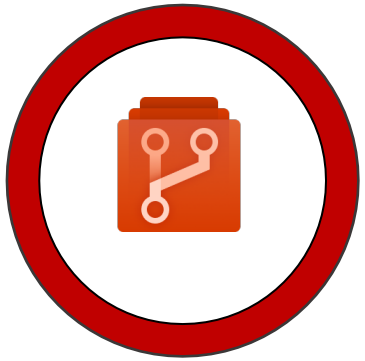
Securing Azure DevOps Configuration
Service Connections and Monitoring of usage

LIVE DEMO

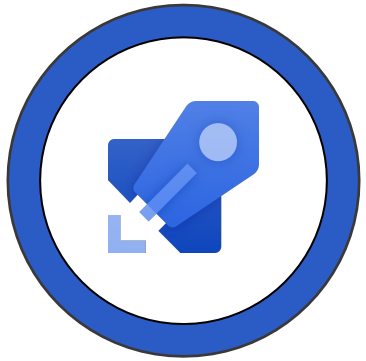
Foundation of Pipelines in Dev(Sec)Ops



Security Posture and RBAC Management of DevOps Platform



Repository Protection and Compliance Policies

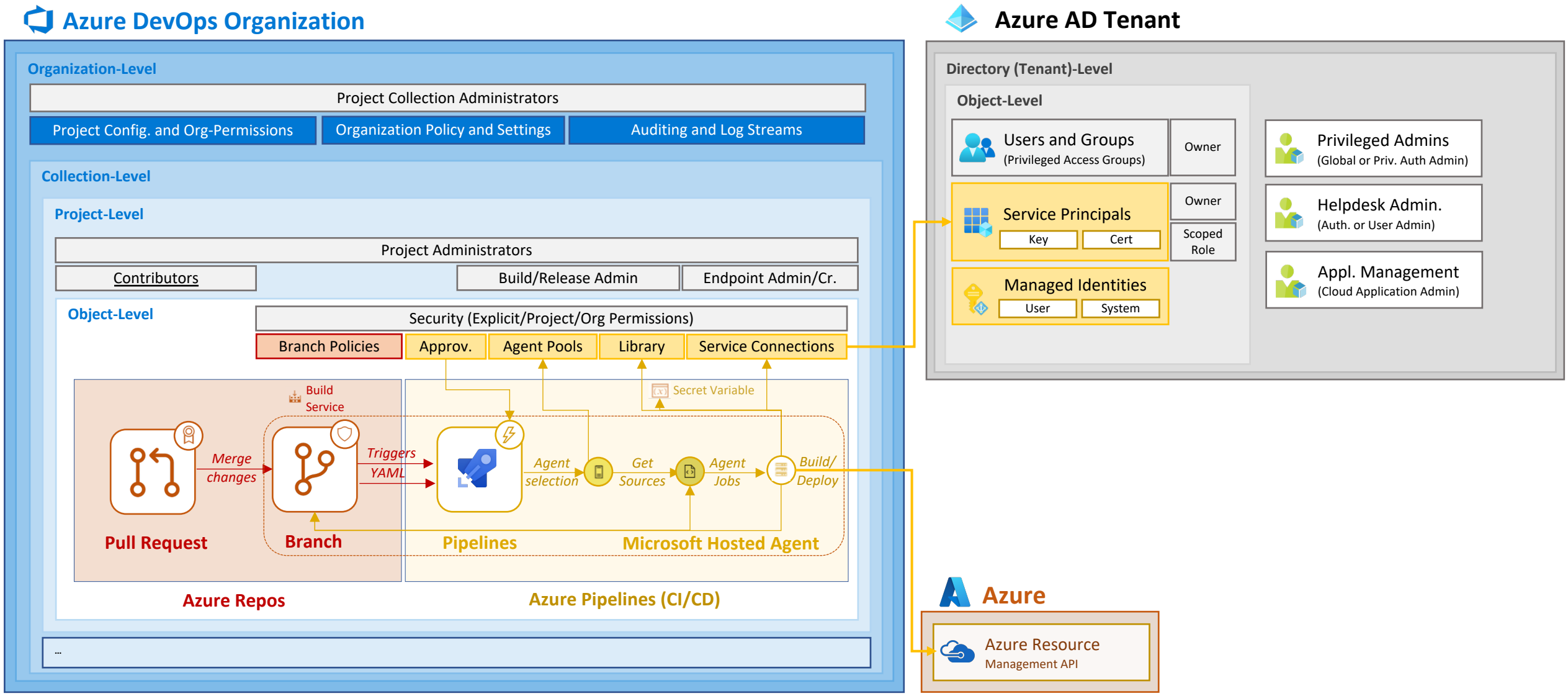


Restricted and audited pipelines on secured agents

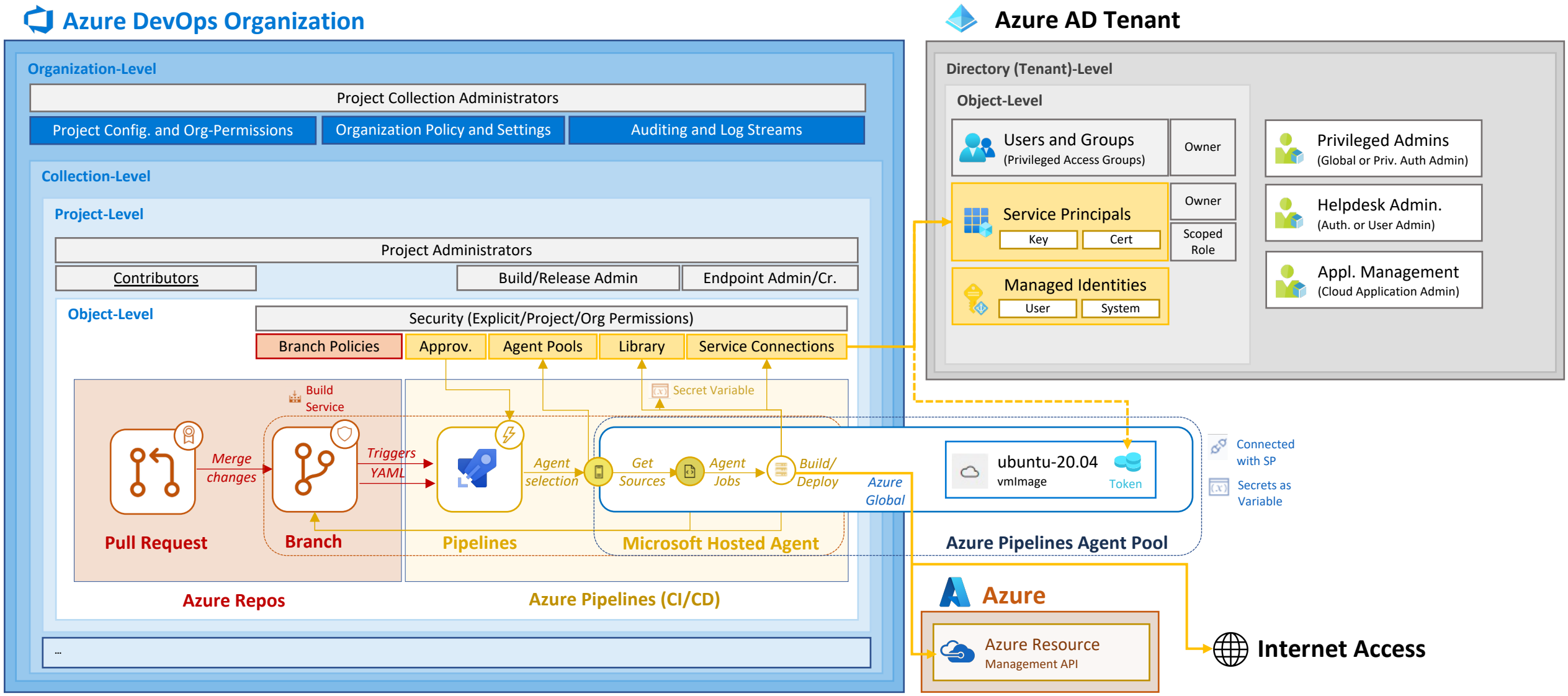
Protection and Monitoring of Workload Identity

→ Azure Security Benchmark v3 (DevOps Security)

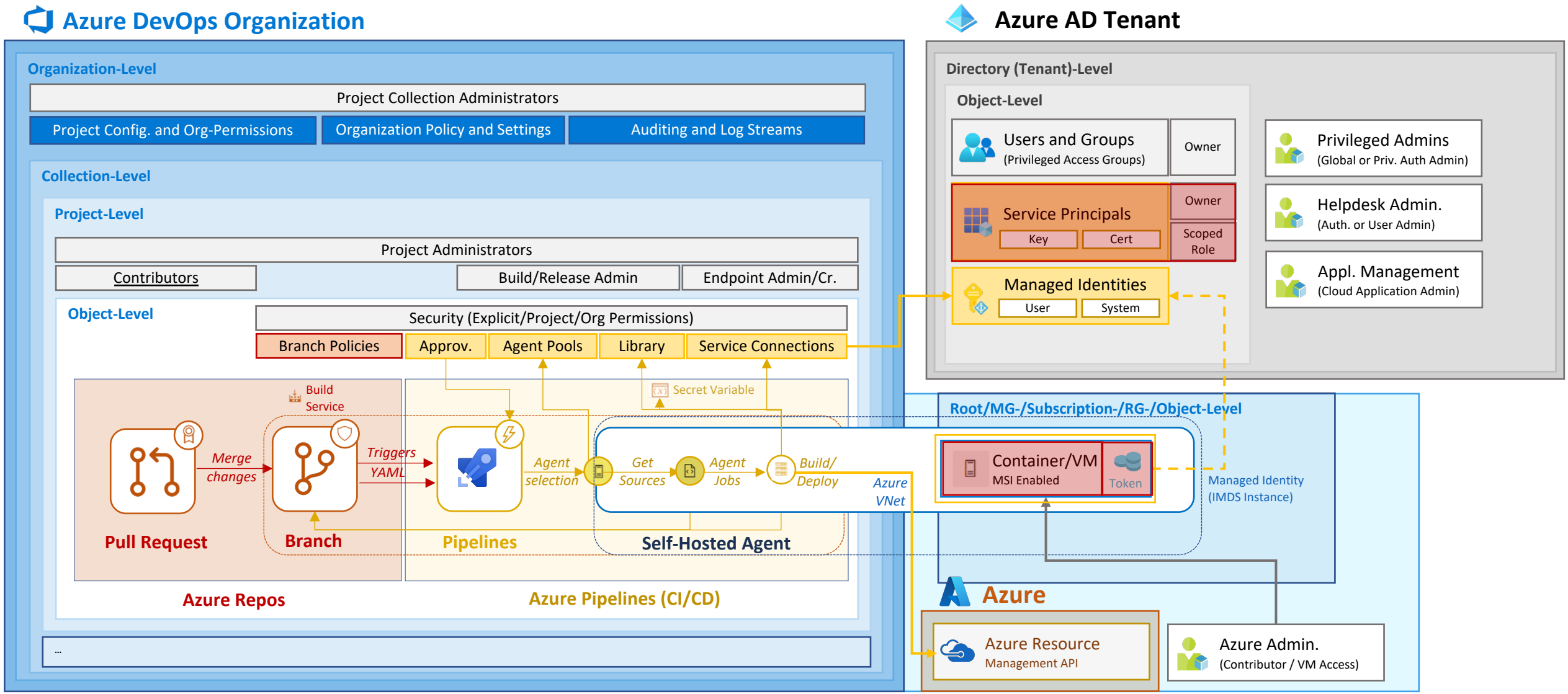
Overview of Azure DevOps and Pipelines



Overview of Azure DevOps and Pipelines



Overview of Azure DevOps and Self Hosted Agents



Protection of Azure Pipelines, Abuse of service connection and exfiltration of token on agents

LIVE DEMO

	Foundation (Small-Midsize Organization)	Large enterprise or regulatory environment
 **Privileged Identities**	• Separation of work and privileged accounts • Password-less authentication • CA Policies to limit access from specific devices, protect and restrict priv. authorization paths • Microsoft Sentinel+MDCA to detect suspicious events, monitor and audit privileged IAM	• Additional separation of Privileged Identities and Access on Control- and Management Plane • Privileged access on Control (Identity) and Management (Platform) Plane from Secure Admin Workstation (SAW) or secured Pipelines only
 **Privileged Access**	• Design of least privileged RBAC • Just-in-Time Access by Azure PIM • Approval, assignment and review privileged roles by Identity Governance • Protection of critical privileged objects by role-assignable/privileged access groups • Configuration in Portal UI • Export as Code for Documentation & Track Changes	• Tiered Admin model on scope of AU- and Service RBAC (avoid Directory-Level Roles) • Reduce numbers of direct assignment of privileged roles (part of privileged pipelines) • RBAC-/Policy-As-Code • Pre-Staged & Adv. QA (Tenant/Test Subscription)
 **Service Principals**	• Inventory and monitoring of Workload Identities • Lifecycle Process (Cred. Rotation, Access Review) • Auditing, restricted RBAC secure configuration of DevOps Platform and pipelines • Secured certificate-based auth. Service Principals	• Isolated DevOps management between pipelines of Control-, Management and Workload Plane • Active Monitoring of Token Exfiltration • Self-Hosted/Runner Agents on secured container instances with audited “Managed Identities”

Resources to learn more…

Privileged Identities

- CA Policies for Privileged Interfaces and Azure-managed Secure Admin Workstation (SAW)
- Workbook of "Azure Security Benchmark" and "M365 Secure Score" in Microsoft Sentinel
- User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel
- Security Operations (Guide) for Privileged Accounts

Privileged Access

- Management capabilities for Privileged Access groups
- Privileged Access Groups: Manage privileged access outside of Aad admin roles with Azure PIM
- Azure AD Administrative Units - Use cases, considerations and limitations
- Security considerations of Azure EA management and potential privilege escalation
- How to operationalize Enterprise-Scale with Infrastructure-as-Code via AzOps

Privileged Pipelines

- ADO Security Scanner and ADOPipelinesSecInfo
- Securing Azure Pipelines
- Azure AD Attack & Defense Playbook: Service Principals in Azure DevOps

THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net