GLOBAL SECURITY AND COMPLIANCE COMMUNITY CONFERENCE

08 FEBRUARY 2021

Notes from the field:

Securing Your Privileged Identity & Access in Microsoft Azure

Thomas Naunheim

Thomas Naunheim

Cloud Engineer | Koblenz, Germany

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net

Microsoft MVP Most Valuable Professional

Azure Meetup BONN

Most Valuable Mentor

Sponsor

Gesellschaft für Digitalisierung und digitalen Fortschritt e.V.

http://gdf-digital.de/

Securing privileged identity and access

Agenda and Overview

Privileged Identity

Privileged Access

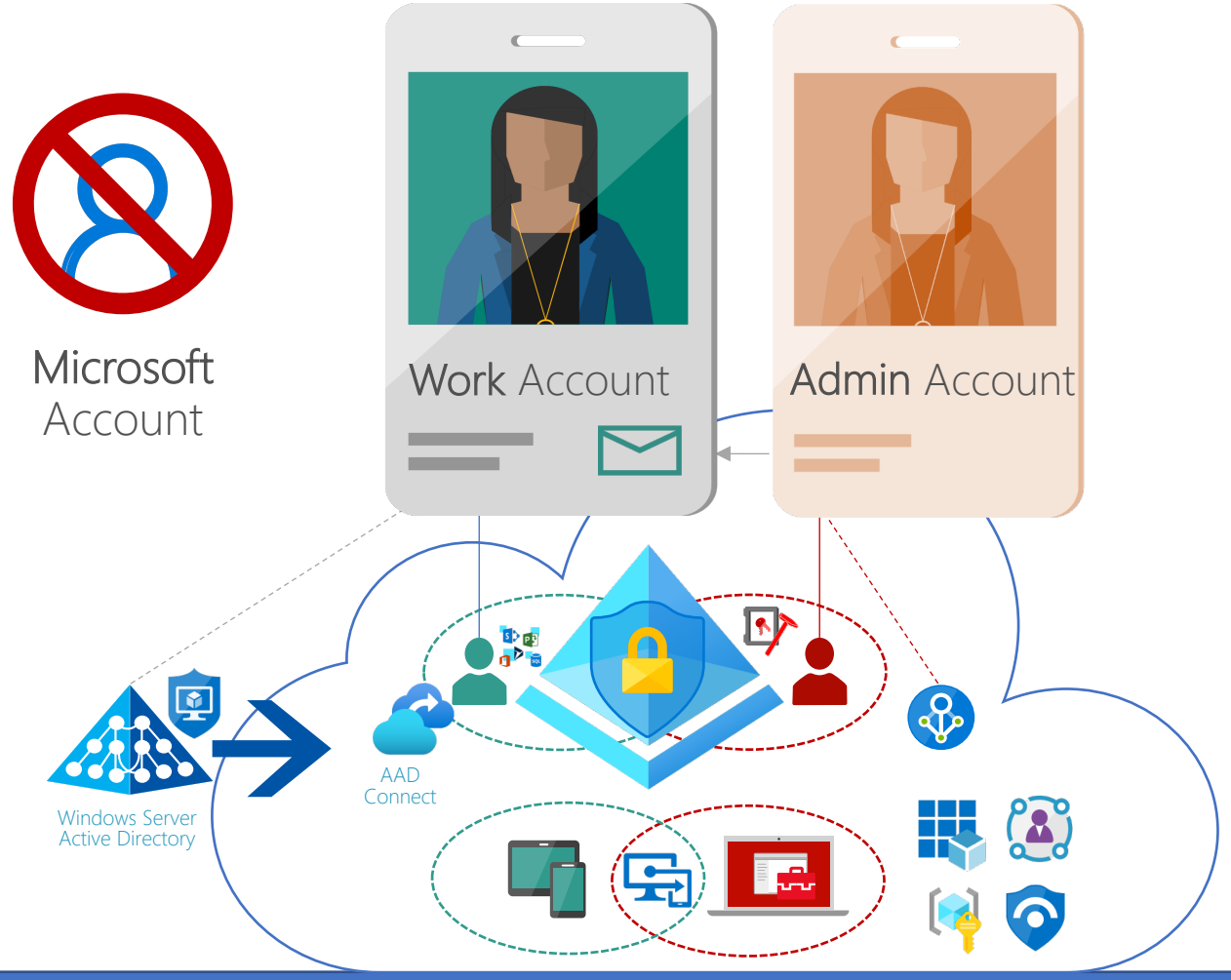
Secure Admin Workstation

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

Privileged Service Principals (Automation/DevOps Pipelines)

Protection of Privileged Identities

Foundation of Privileged Accounts



Separation of work and privileged accounts

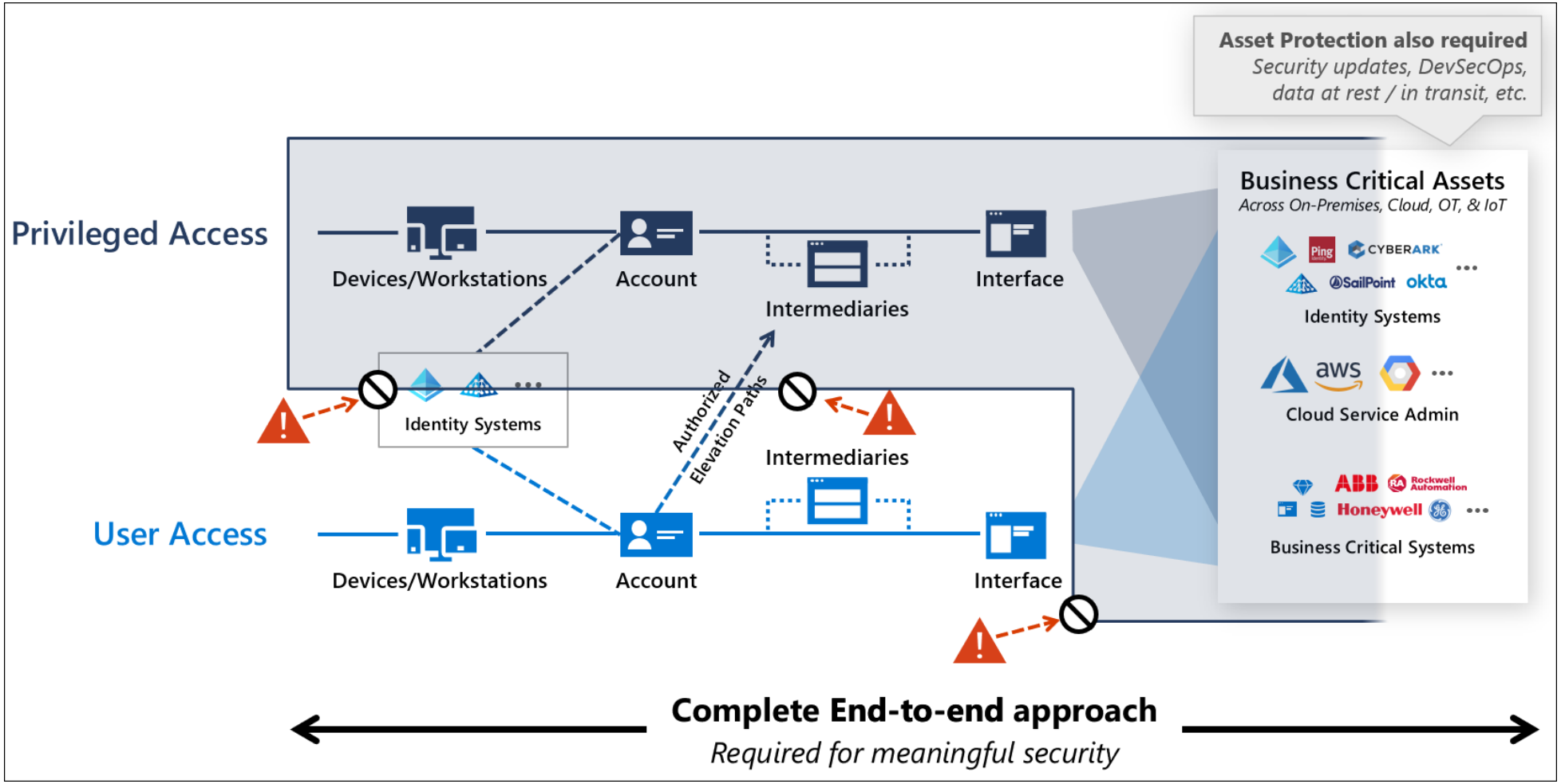
- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Implement identity lifecycle and access review
- ✓ Remove licenses of productivity workloads
- ✓ Forwarded mail address

Secured and hardened Azure AD Tenant

- ✓ Strong baseline and tenant-level security
- ✓ Monitor and response for suspicious activities
- ✓ Isolation of work- and privileged resources

Protecting Privileged Identities

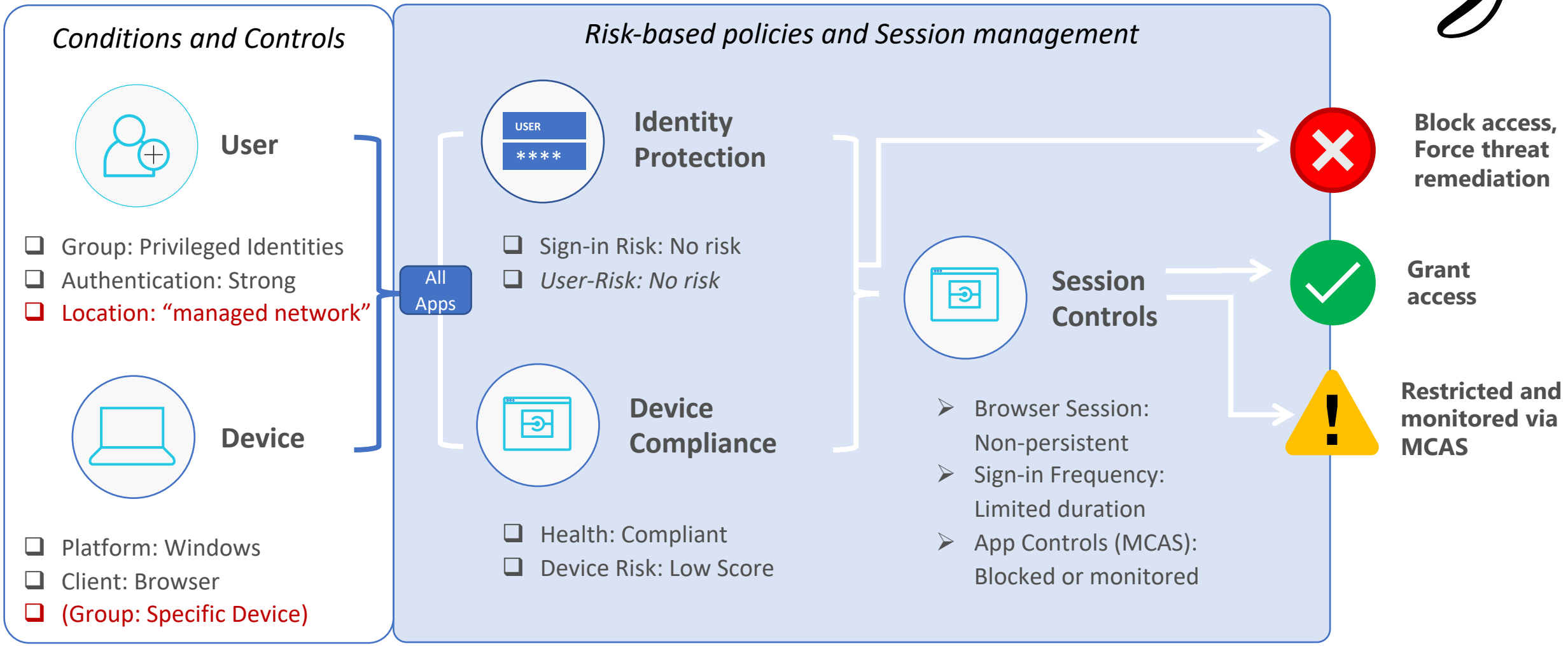
Actions from authorized pathways



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

Source: Privileged access Strategy (Microsoft Docs)

Conditional Access for Privileged Identities



Demo: Protecting Privileged Identities

- Conditional Access Design
- MCAS Integration, Activity Logs and Detections of Azure Platform
- Azure Sentinel Detections for suspicious privileged activities
- Privileged Identity Compliance in Azure Security, M365 Score and Compliance Center

Securing Privileged Access

Governance of Privileged Access

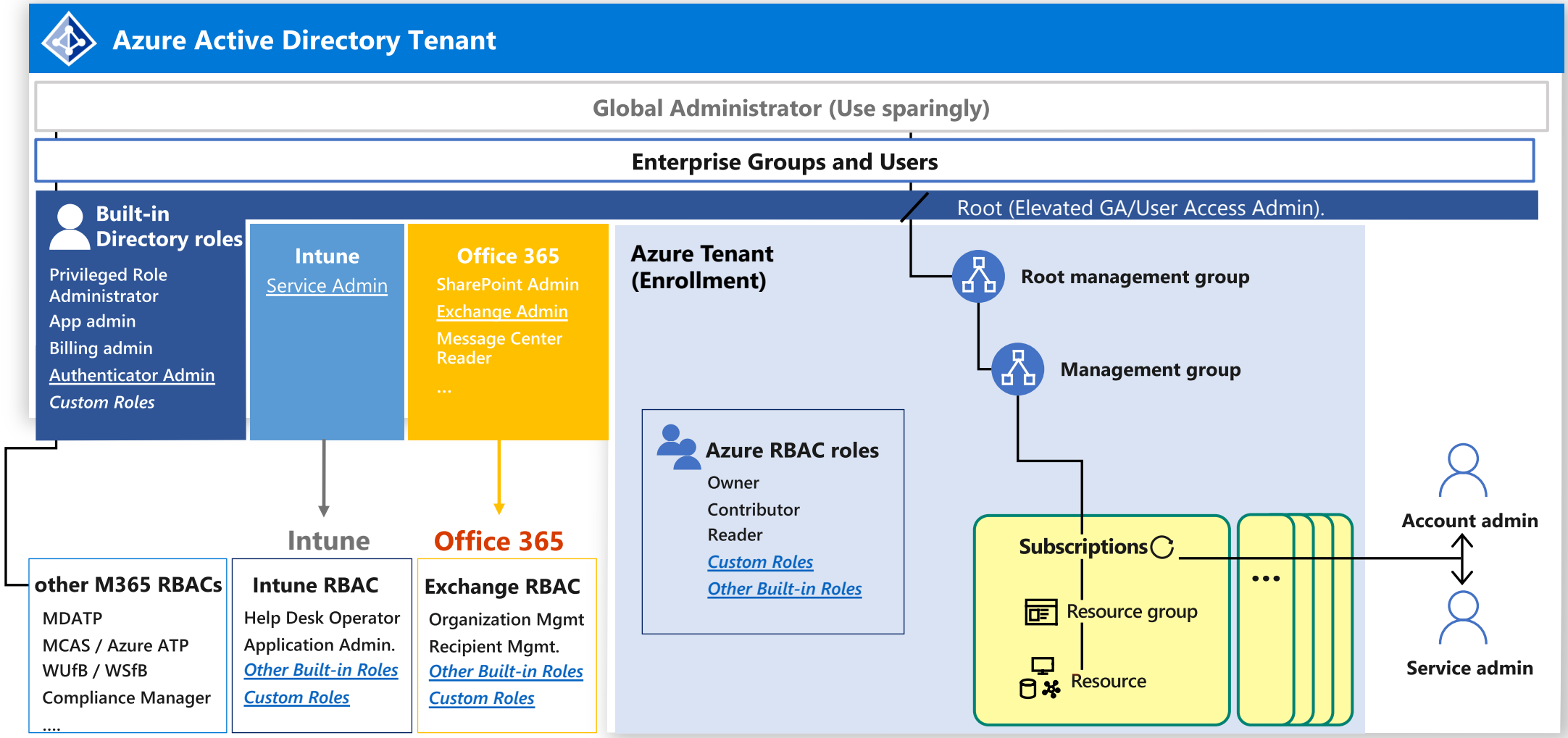
Granular Task Scoped Access (Just Enough)

Just in Time Access

Privileged Admin Workflow

Audit Ready

Understanding Azure AD, M365 and Azure RBAC



Source: Azure Security Compass (Microsoft)

Tiering of Privileged Access and Accounts

„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**.“

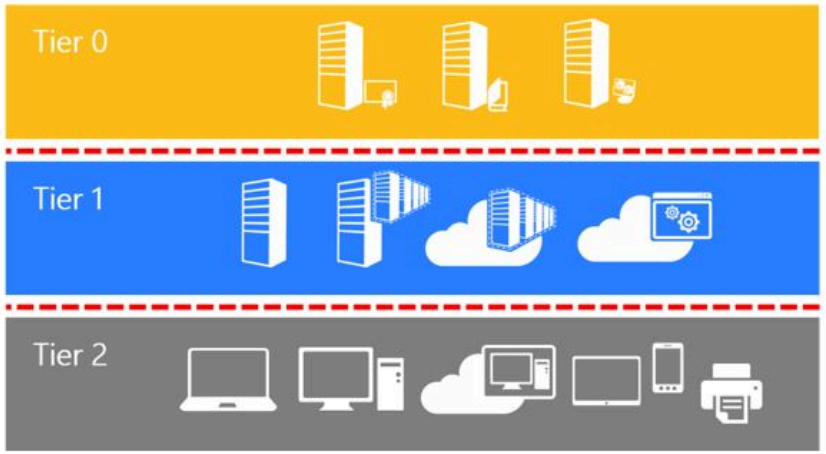
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

Active Directory administrative tier model

02/14/2019 • 33 minutes to read • +6

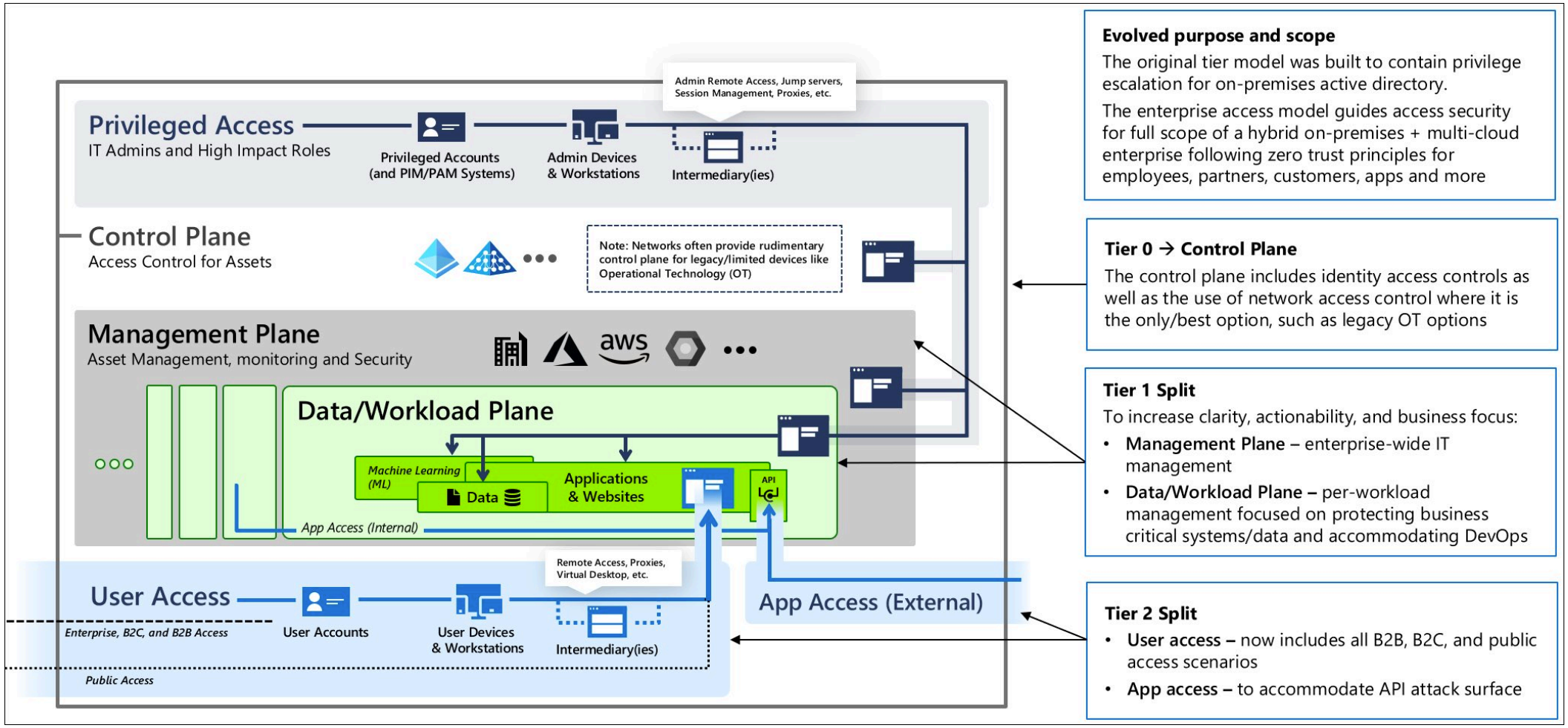
Applies To: Windows Server

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



Evolved purpose and scope

The original tier model was built to contain privilege escalation for on-premises active directory.

The enterprise access model guides access security for full scope of a hybrid on-premises + multi-cloud enterprise following zero trust principles for employees, partners, customers, apps and more

Tier 0 → Control Plane

The control plane includes identity access controls as well as the use of network access control where it is the only/best option, such as legacy OT options

Tier 1 Split

To increase clarity, actionability, and business focus:

- **Management Plane –** enterprise-wide IT management
- **Data/Workload Plane –** per-workload management focused on protecting business critical systems/data and accommodating DevOps

Tier 2 Split

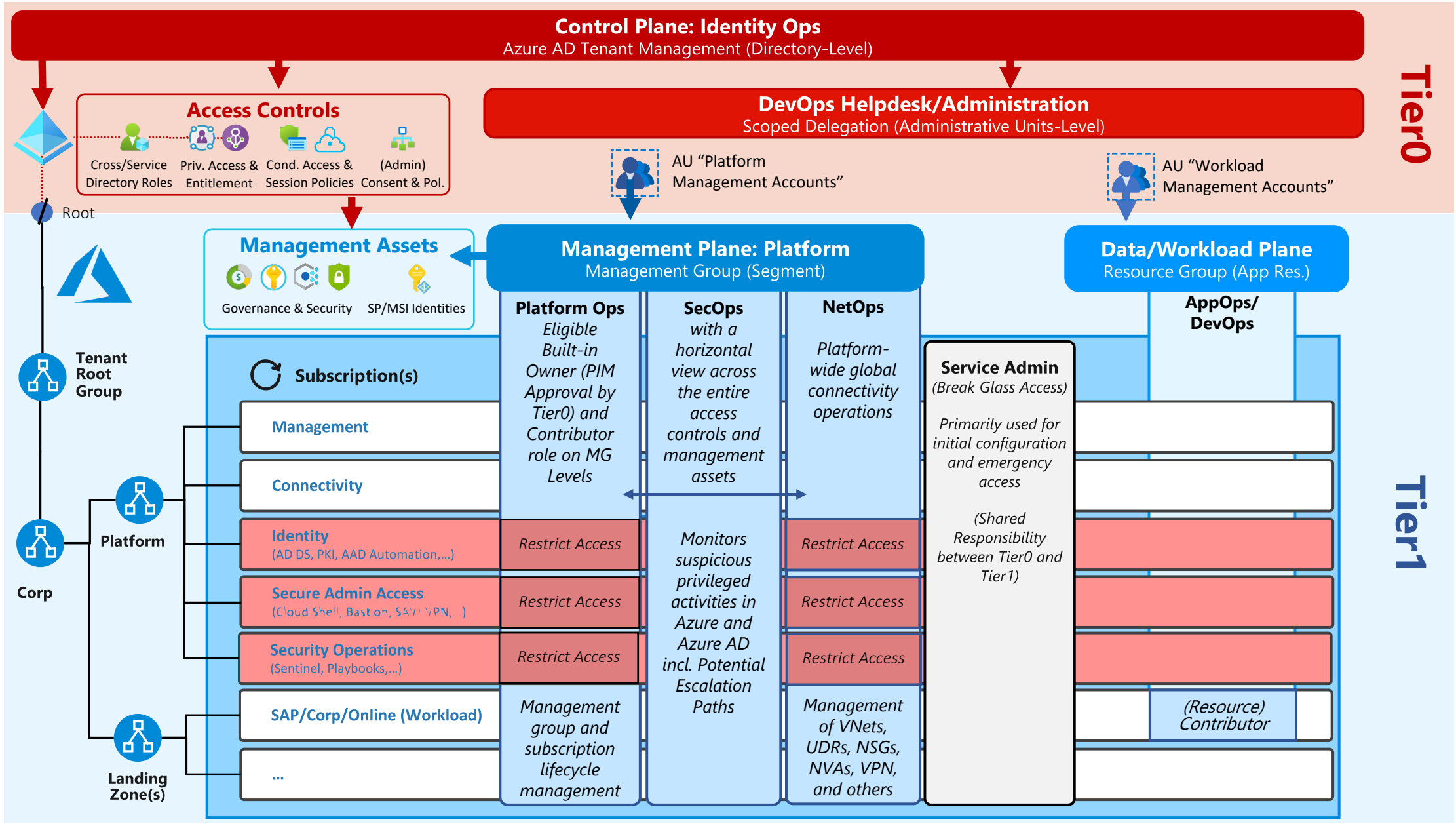
- **User access –** now includes all B2B, B2C, and public access scenarios
- **App access –** to accommodate API attack surface

Image source: Enterprise Access Model

Demo: Privileged Access Design by Azure AD Roles

- Considerations of “Service-Specific” Azure AD Directory Roles
- Protected Privileged (Access) Groups and Roles by Azure AD PIM PAG
- Introduction of Enterprise Access Model

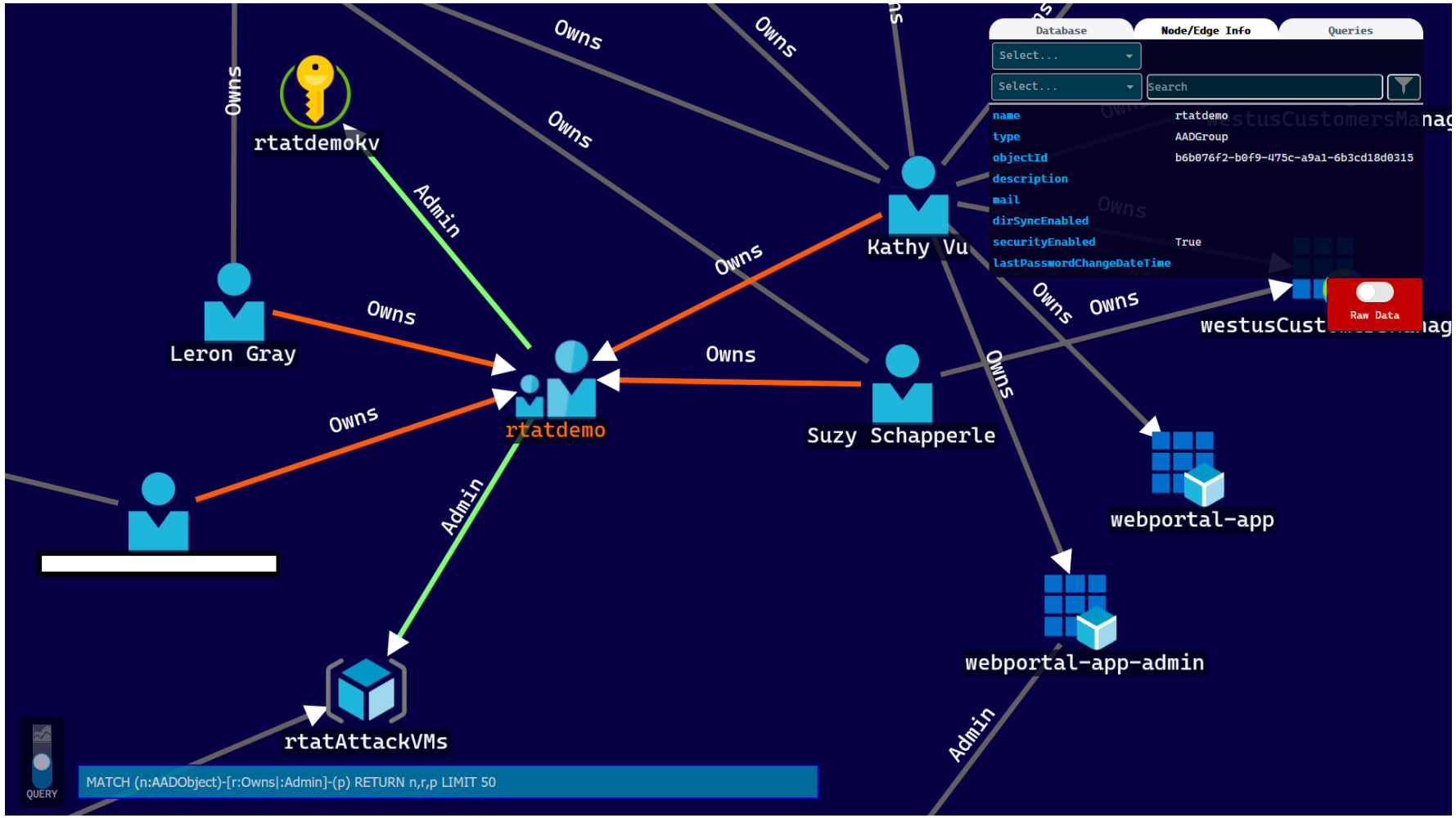
Sample of “Enterprise Access Model” implementation



Demo: Privileged Access Model for Azure

- Role-Assignable Groups and PAGs
- Entitlement Management and Access Package
- Custom RBAC Roles
- Operationalization with ”RBAC-as-Code”

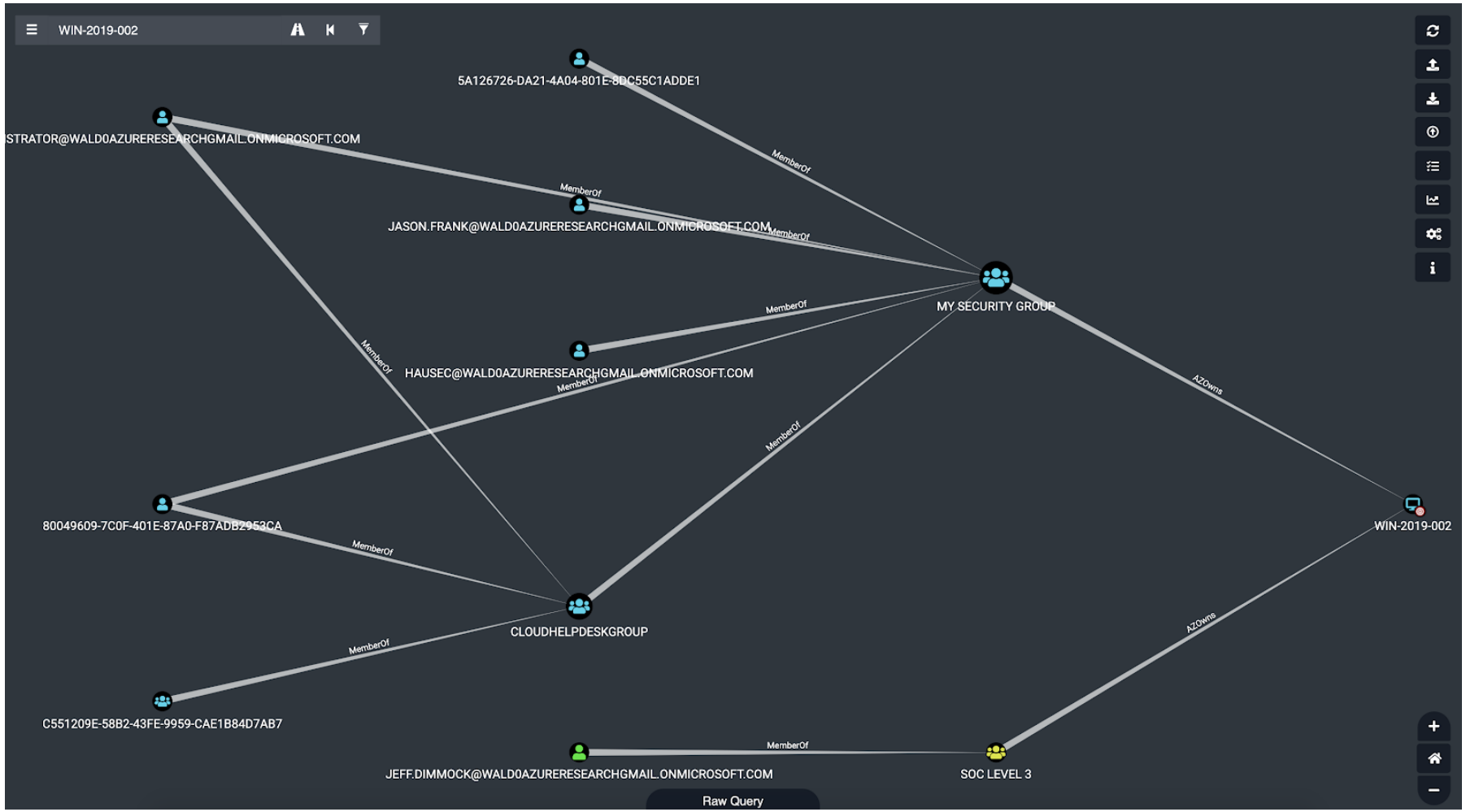
Stormspotter (Released in May 2020)



STORMSPOTTER

Source: GitHub Project "Stromspotter"

BloodHound 4.0 („The Azure Update“)

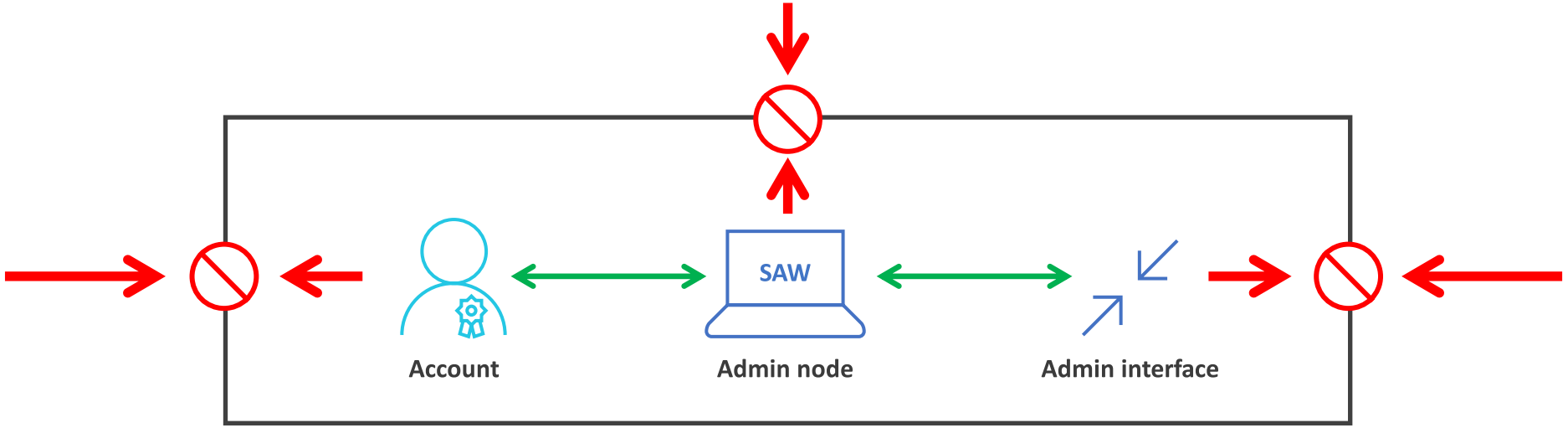


BLOODHOUND

Source: Introducing BloodHound 4.0: The Azure Update

Securing your Access Workstation

Overview of Secure Admin Workstation



- DISA STIG requires Privilege Access Workstations (PAW) for Cloud Tenant Management
- **CIS (C4)**: Administrators shall use a dedicated, isolated machine for all administrative tasks

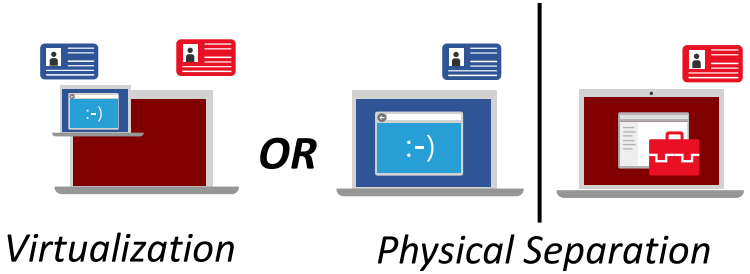
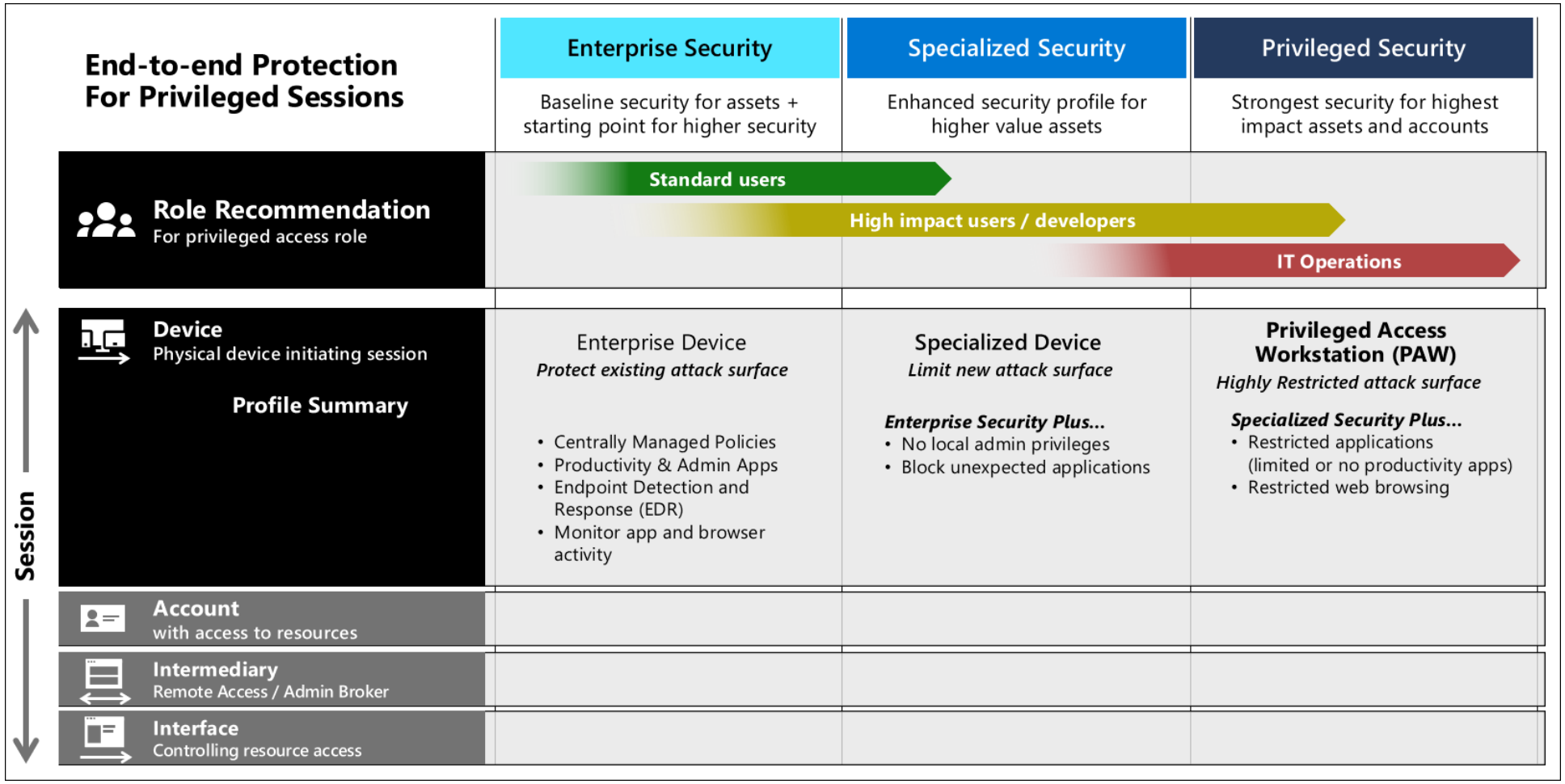


Image source: Microsoft CISO Workshop 4a - Threat Protection Strategy

Device roles and profiles



Source: [Why are privileged access devices important | Microsoft Docs]

Securing Your Privileged Identity & Access in Microsoft Azure

Privileged Identity

- Separated/isolated accounts from productive tasks
- Located in secured and monitored identity directory
- Strong and passwordless authentication options

Privileged Access

- “Least privileged” by defined and tiered RBAC design
- Zero Rights by default / Non-perisistent access
- Regular review of priviliged accounts and access

Secure Admin Worktation

- Privileged access from hardened device only
- Secured admin interface and restricted user sessions
- Balance between usability and security of administrators

Priviliged Service Principals

Auditing and protecting of secrets and priviliged access in Automation tasks or DevOps Pipelines (CI/CD)

Thank you!

Please share Feedback with us:

Feedback.complianceinsider.de