Trust in Tech Cologne

Securing your privileged identity and access in Azure (Active Directory)

Thomas Naunheim

(July 28th, 2020)

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net

Securing your privileged identity and access

More than just vaulting and protecting admin passwords

Privileged Identity

Privileged Access

Secure Access Worktation

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

Privileged Service Principals (Automation/DevOps Pipelines)

Protection of Privileged Identities

Protecting Privileged Identities

Foundation of Administrative Accounts

Separation of work and privileged accounts

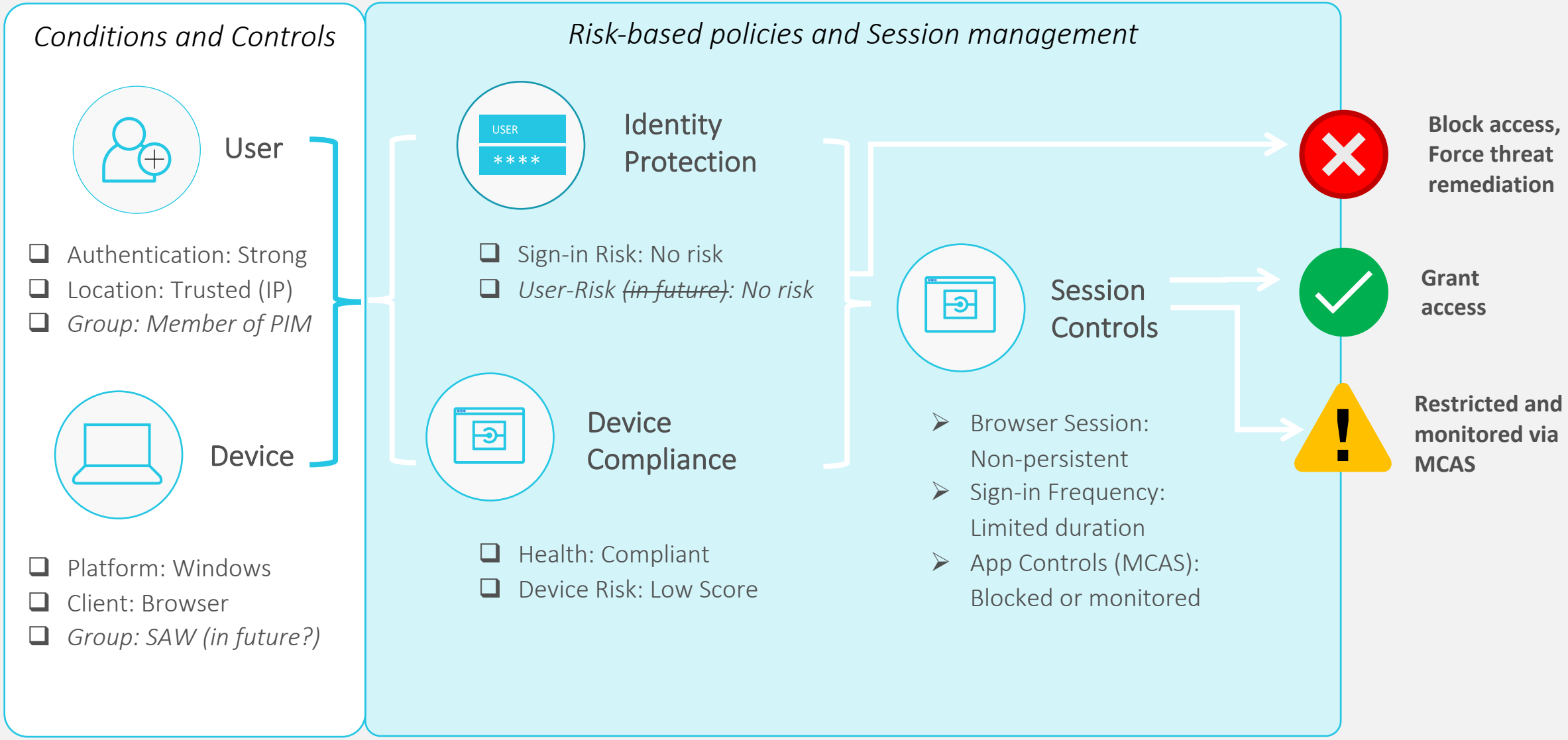
- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Separated custom domain name space
- ✓ Implement identity lifecycle and access review
- ✓ Remove licenses of productivity workloads
- ✓ Forwarded mail address

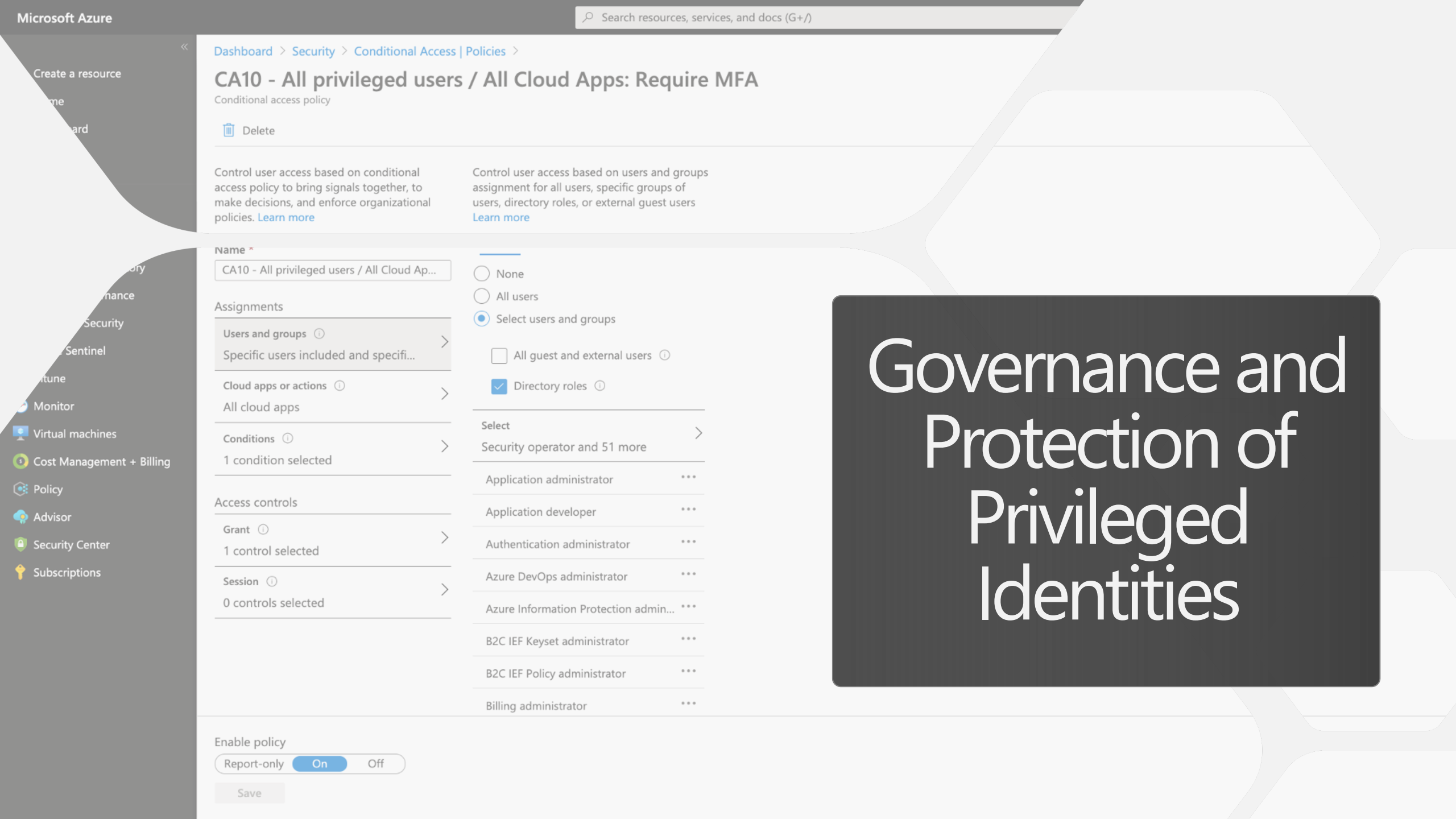
Secured and hardened Azure AD Tenant

- ✓ Synchronizing from secured Active Directory
- ✓ Monitor and response for suspicious activities
- ✓ Isolation of work- and privileged resources
- ✓ Strong baseline and tenant-level security

Protecting Privileged Identities

Design of Conditional Access for Privileged Identities




Microsoft Azure
Search resources, services, and docs (G+/)
Create a resource
Monitor
Virtual machines
Cost Management + Billing
Policy
Advisor
Security Center
Subscriptions
Dashboard > Security > Conditional Access | Policies >
CA10 - All privileged users / All Cloud Apps: Require MFA
Conditional access policy
Delete
Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users Learn more
Name *
CA10 - All privileged users / All Cloud Ap...
Assignments
Users and groups
Specific users included and specifi...
Cloud apps or actions
All cloud apps
Conditions
1 condition selected
Access controls
Grant
1 control selected
Session
0 controls selected
None
All users
Select users and groups
All guest and external users
Directory roles
Select
Security operator and 51 more
Application administrator
Application developer
Authentication administrator
Azure DevOps administrator
Azure Information Protection admin...
B2C IEF Keyset administrator
B2C IEF Policy administrator
Billing administrator
Enable policy
Report-only
On
Off
Save
Governance and Protection of Privileged Identities

Securing Privileged Access

Securing Privileged Access

Zero Standing Privileged Access for your organiztion

Granular Task
Scoped Access
(Just Enough)

Just in Time
Access

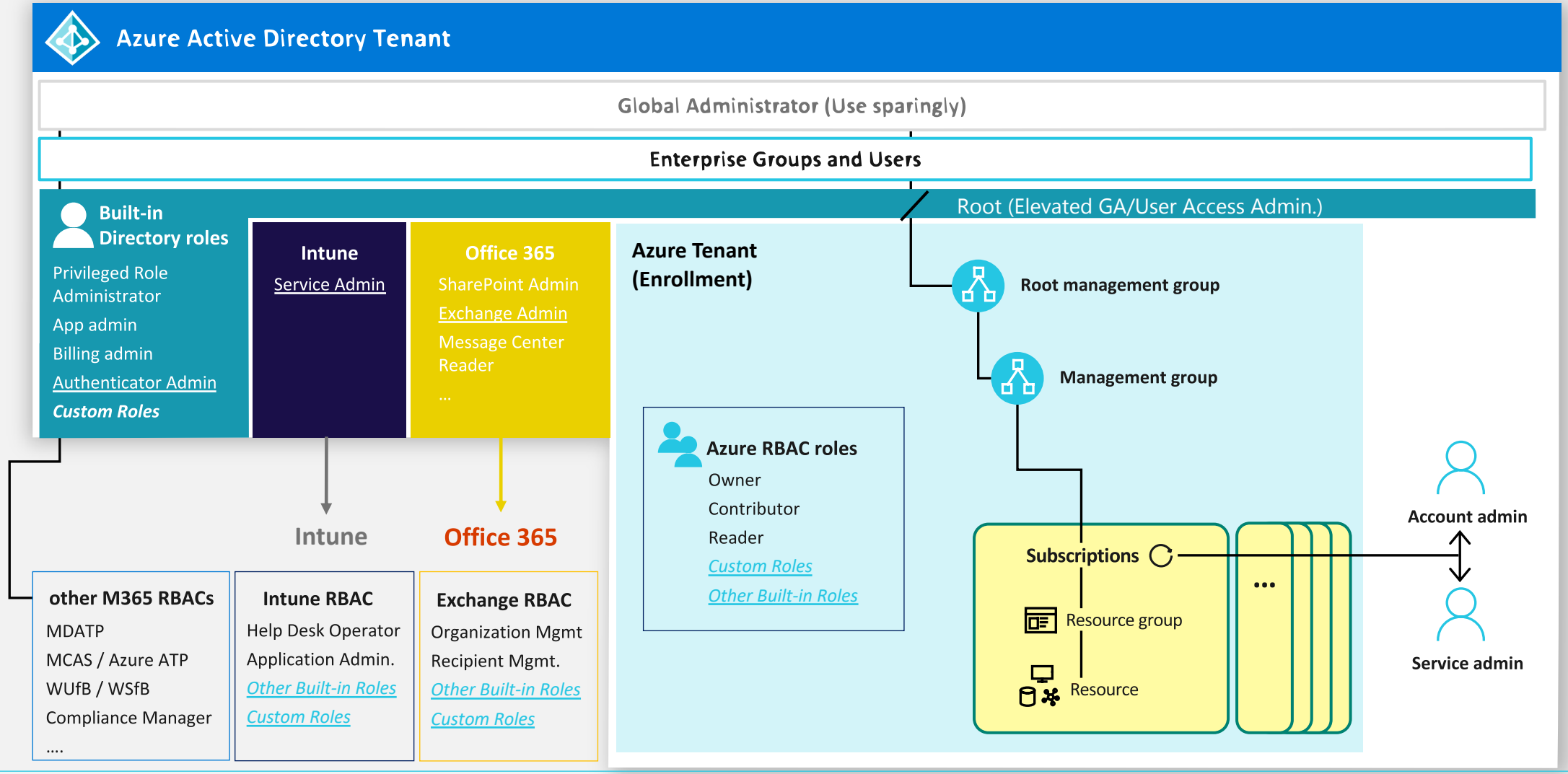
Privileged
Admin
Workflow

Audit
Ready

Source: Microsoft Ignite 2019 („Reduce risk with Microsoft 365 access control technologies“)

Securing Privileged Access

Understanding Azure and Azure AD RBAC



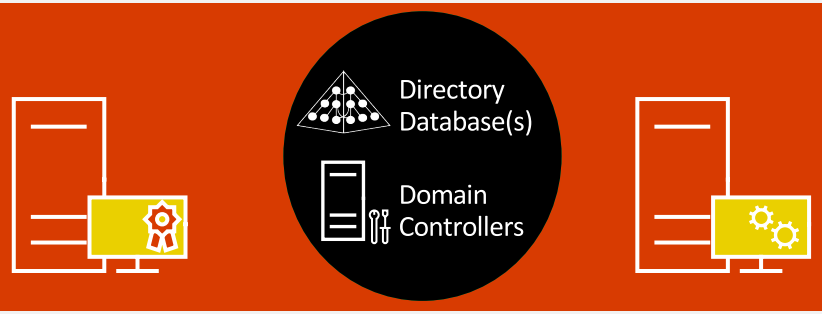
Original source: Azure Security Compass

Securing Privileged Access

Tiering of Administrative Accounts and Permissions

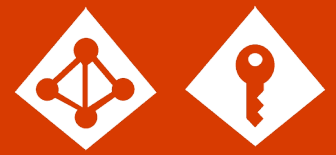
Tier 0 (Identity)

Domain &
Enterprise Admins



Tier 0 (Identity)

Global Admins
Authenticator Admin

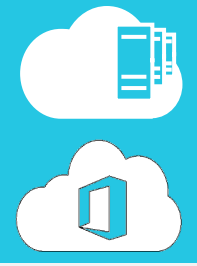


Tier 1 (Server)

Server Admins

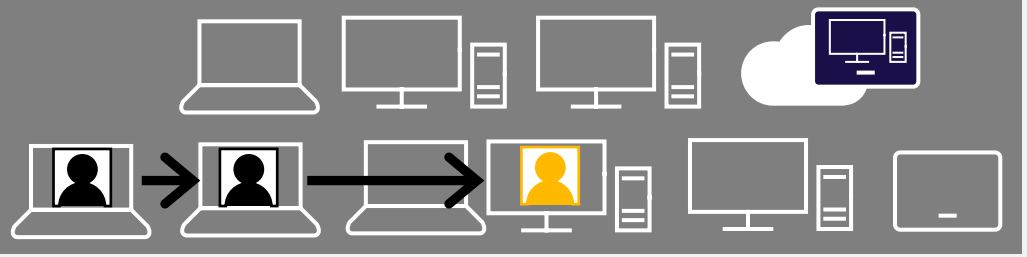
Tier 1 (Resources)

VM Contributor (IaaS)
Exchange Admin (SaaS)



Tier 2 (Clients)

Workstation &
Device Admins



Tier 2 (Endpoints)

Intune Service Admin
MDATP “Admin”?

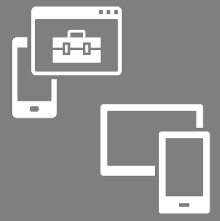
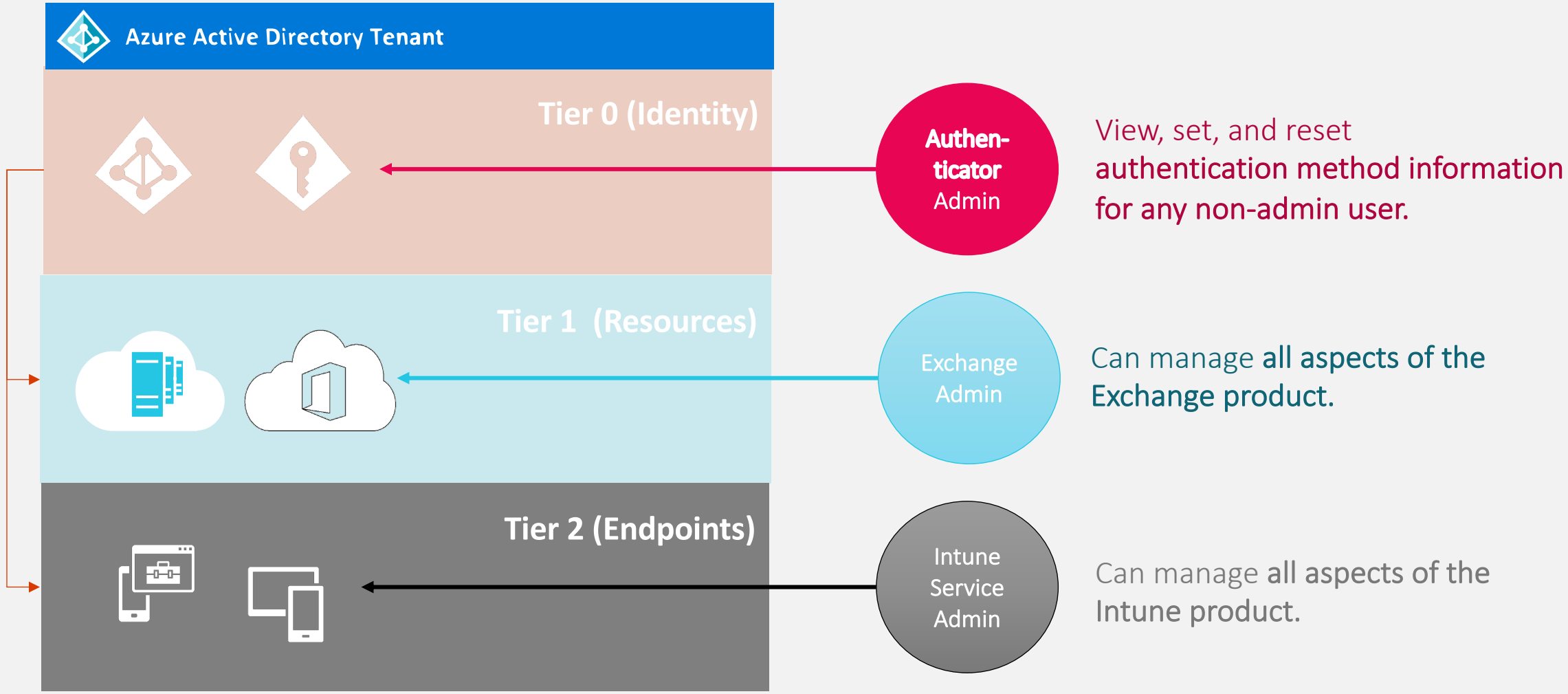
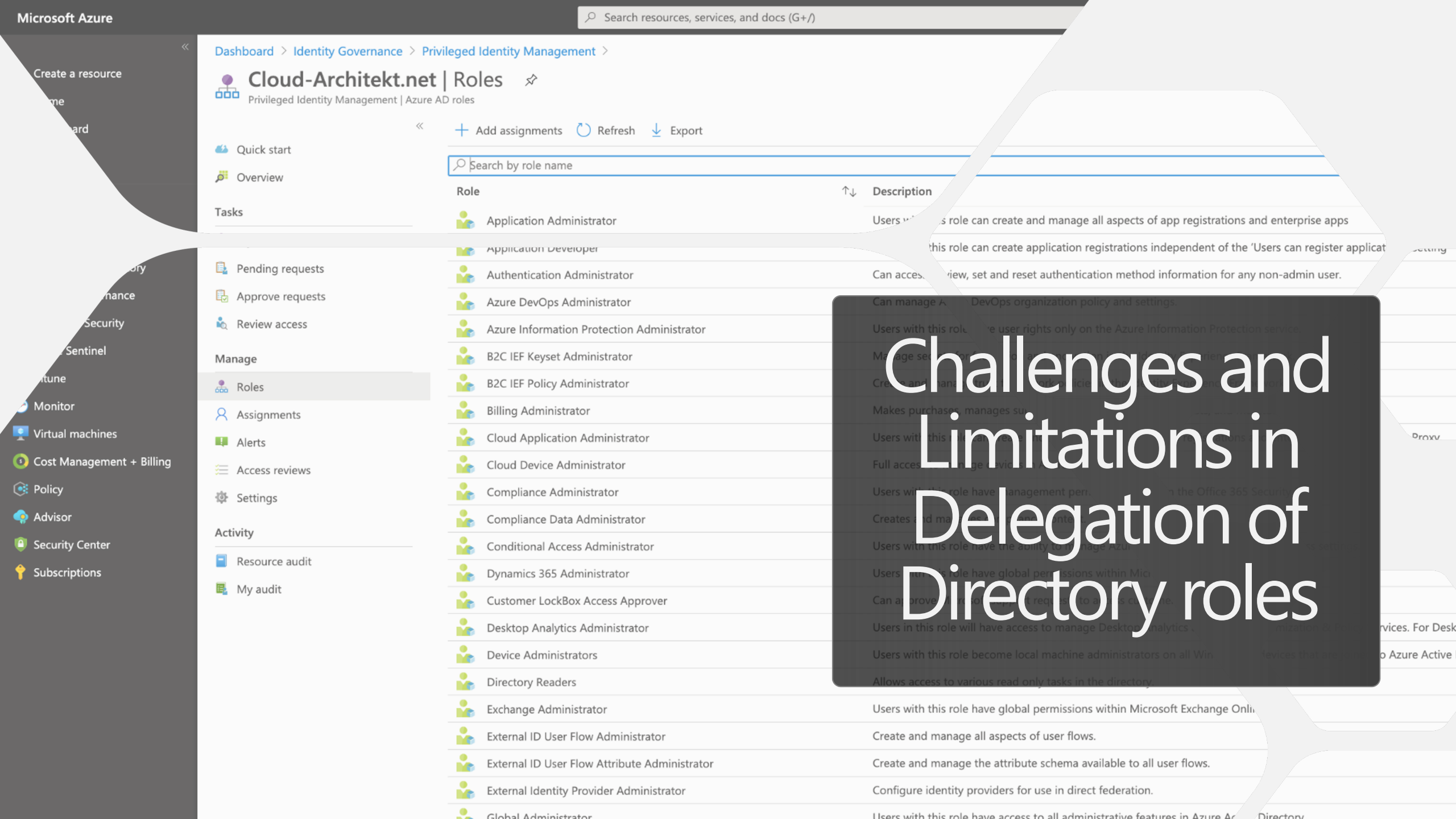


Image source: [Microsoft CISO Workshop 4a - Threat Protection Strategy]

Securing Privileged Access

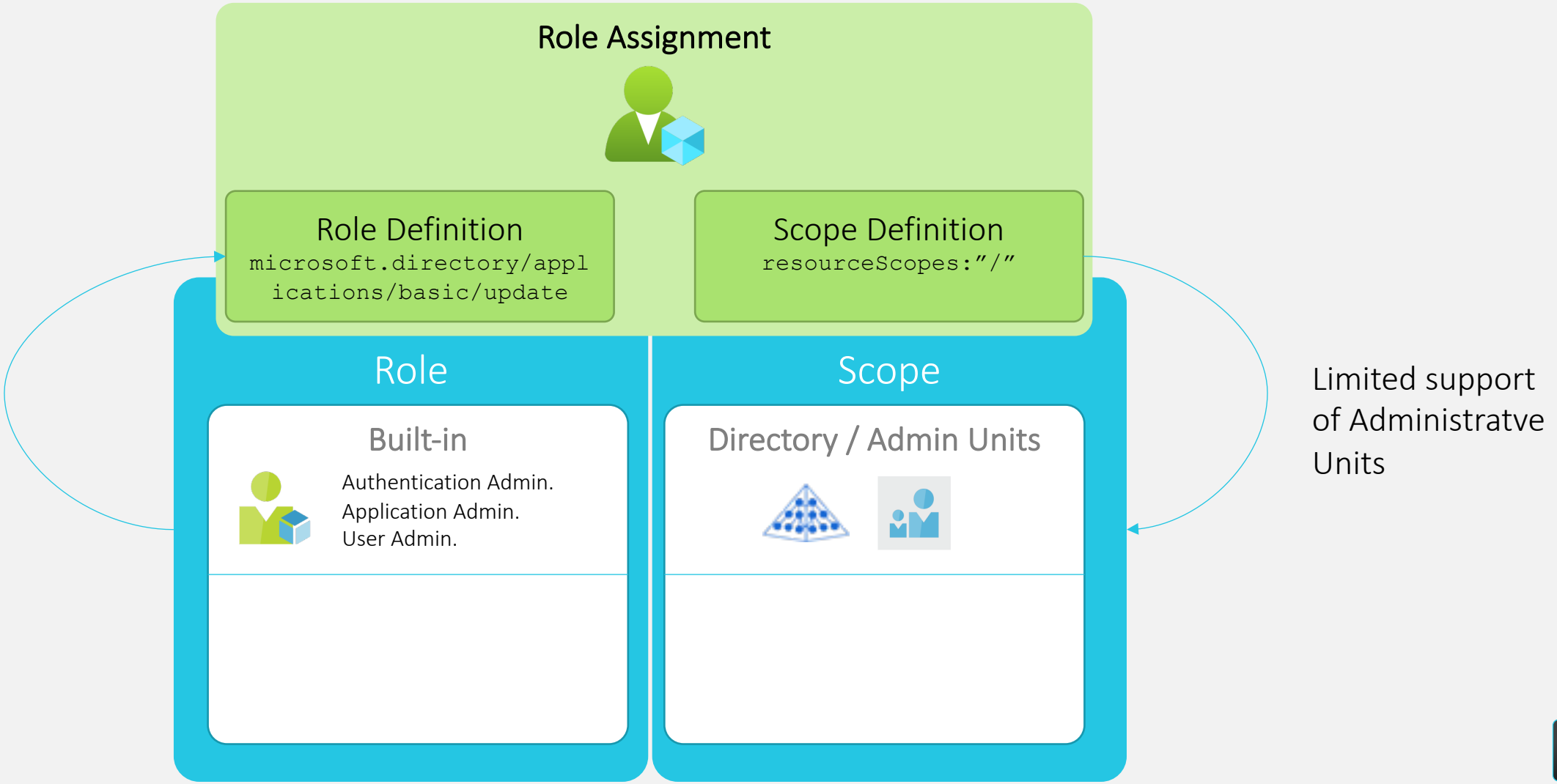
Azure AD: Tiering of Administrative Accounts and Permissions




Microsoft Azure
Search resources, services, and docs (G+/)
Create a resource
Monitor
Virtual machines
Cost Management + Billing
Policy
Advisor
Security Center
Subscriptions
Dashboard > Identity Governance > Privileged Identity Management >
Cloud-Architekt.net | Roles
Privileged Identity Management | Azure AD roles
Quick start
Overview
Tasks
Pending requests
Approve requests
Review access
Manage
Roles
Assignments
Alerts
Access reviews
Settings
Activity
Resource audit
My audit
Add assignments
Refresh
Export
Search by role name
Role
Description
Application Administrator
Authentication Administrator
Azure DevOps Administrator
Azure Information Protection Administrator
B2C IEF Keyset Administrator
B2C IEF Policy Administrator
Billing Administrator
Cloud Application Administrator
Cloud Device Administrator
Compliance Administrator
Compliance Data Administrator
Conditional Access Administrator
Dynamics 365 Administrator
Customer LockBox Access Approver
Desktop Analytics Administrator
Device Administrators
Directory Readers
Exchange Administrator
External ID User Flow Administrator
External ID User Flow Attribute Administrator
External Identity Provider Administrator
Create and manage all aspects of user flows.
Create and manage the attribute schema available to all user flows.
Configure identity providers for use in direct federation.
Challenges and Limitations in Delegation of Directory roles

Securing Privileged Access

Reduce scope and permission of Azure AD Roles



Pre-defined and managed roles by Microsoft only

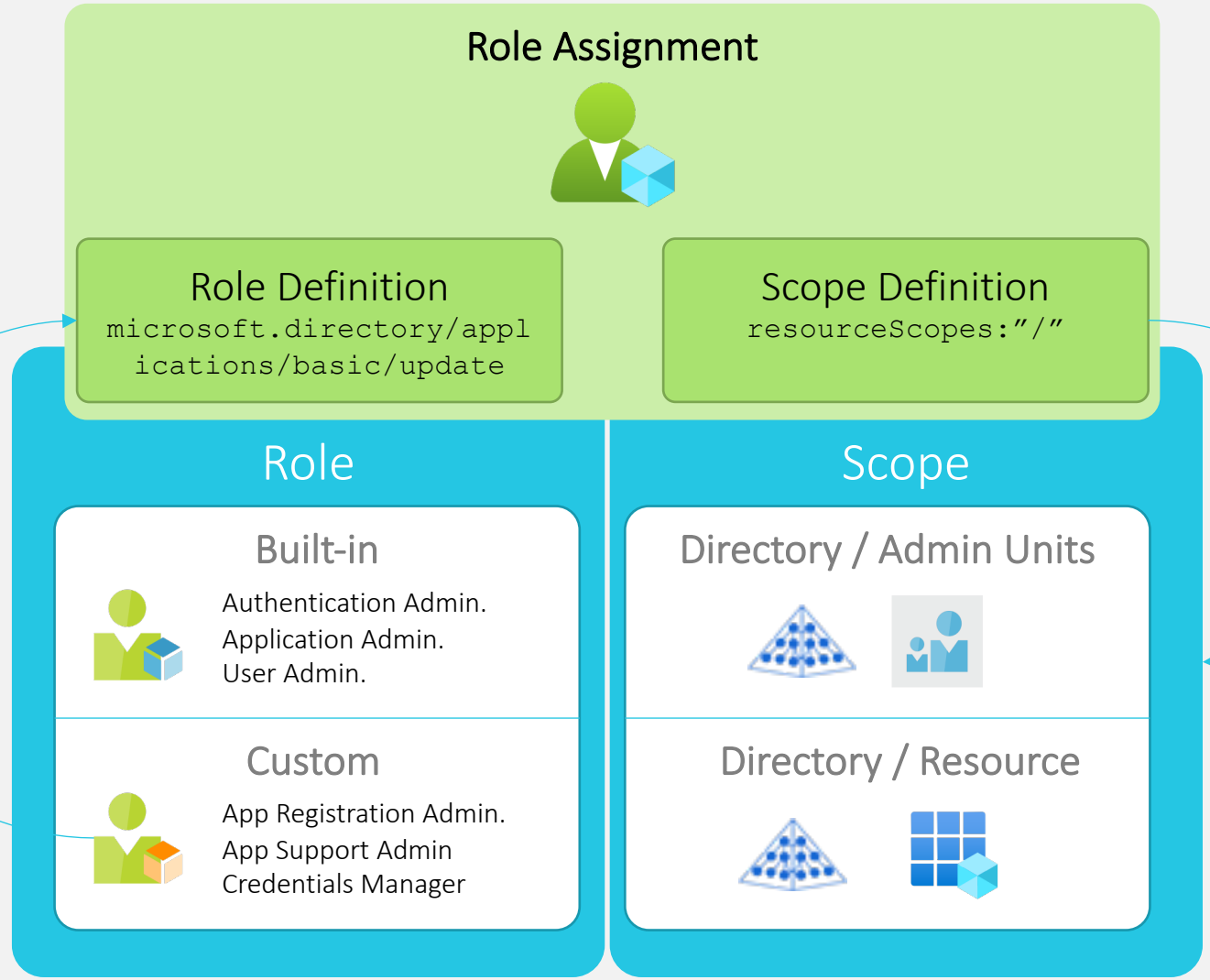
Limited support of Administratve Units

Securing Privileged Access

Reduce scope and permission of Azure AD Roles

Custom roles created and managed by your organization

Only few role permissions supported



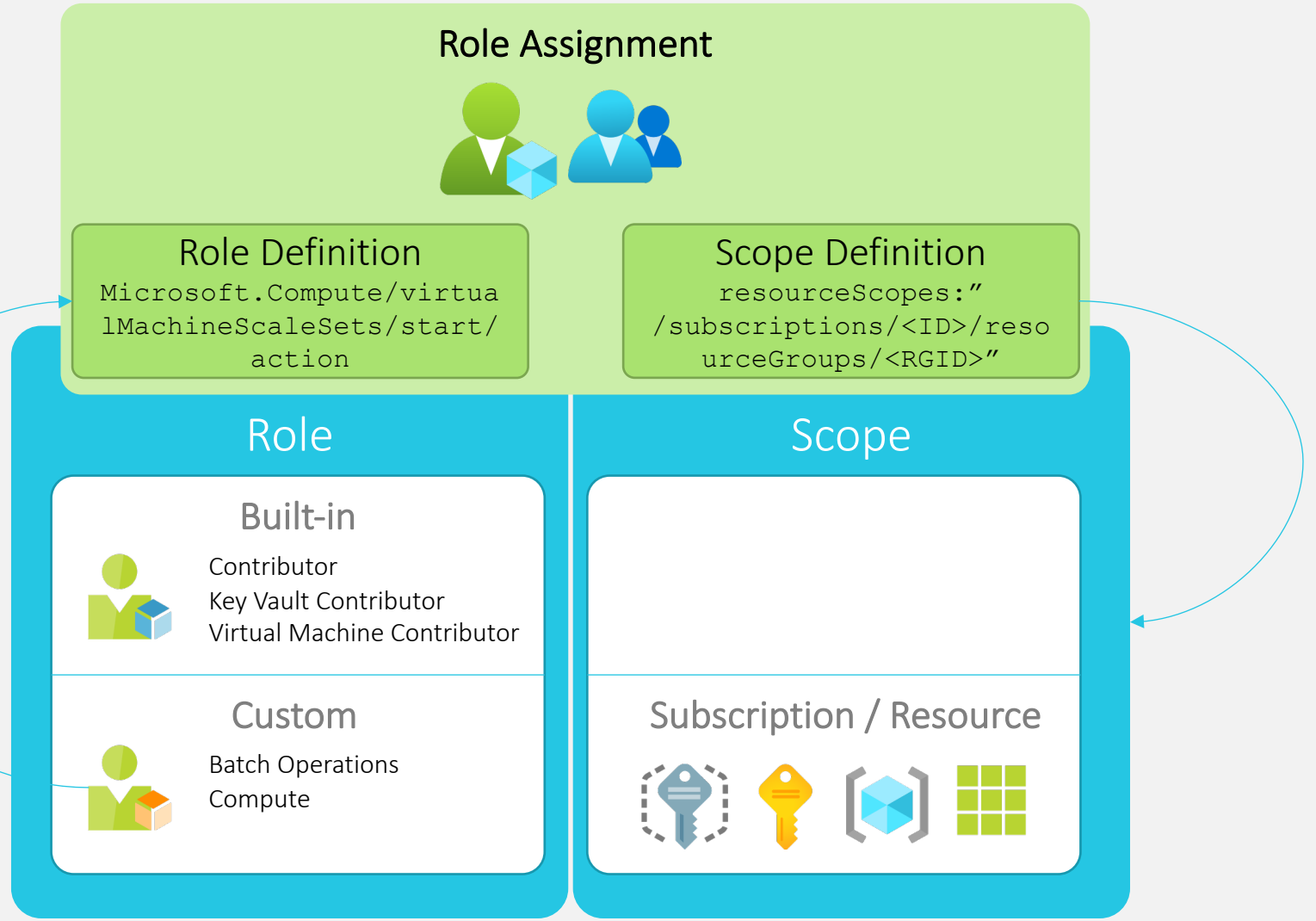
Directory- and resource-scope supported only (no Admin Unit support yet)

Securing Privileged Access

Reduce scope and permission of Azure RBAC

Custom roles created and managed by your organization

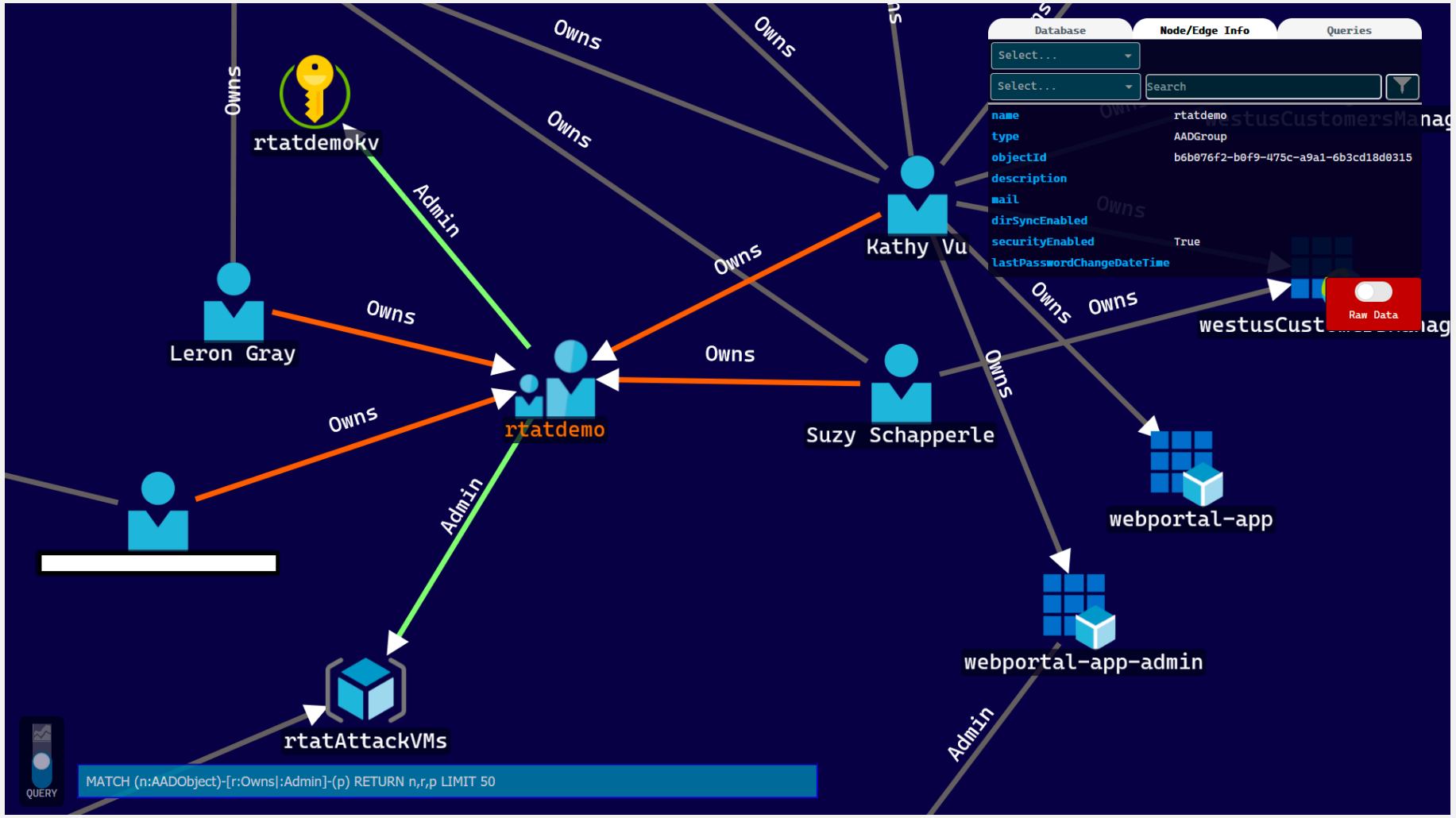
Delegate permissions on ARM operations



Management/ Resource Group, Subscription and resource-scope supported

Securing Privileged Access

Stormspotter (Released in May 2020)

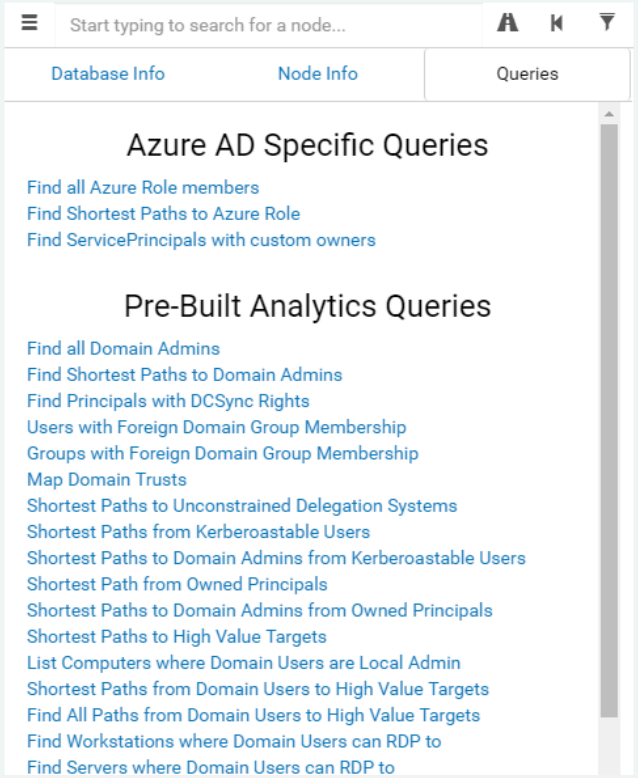


STORMSPOTTER

Source: GitHub Project "Stromspotter"

Securing Privileged Access

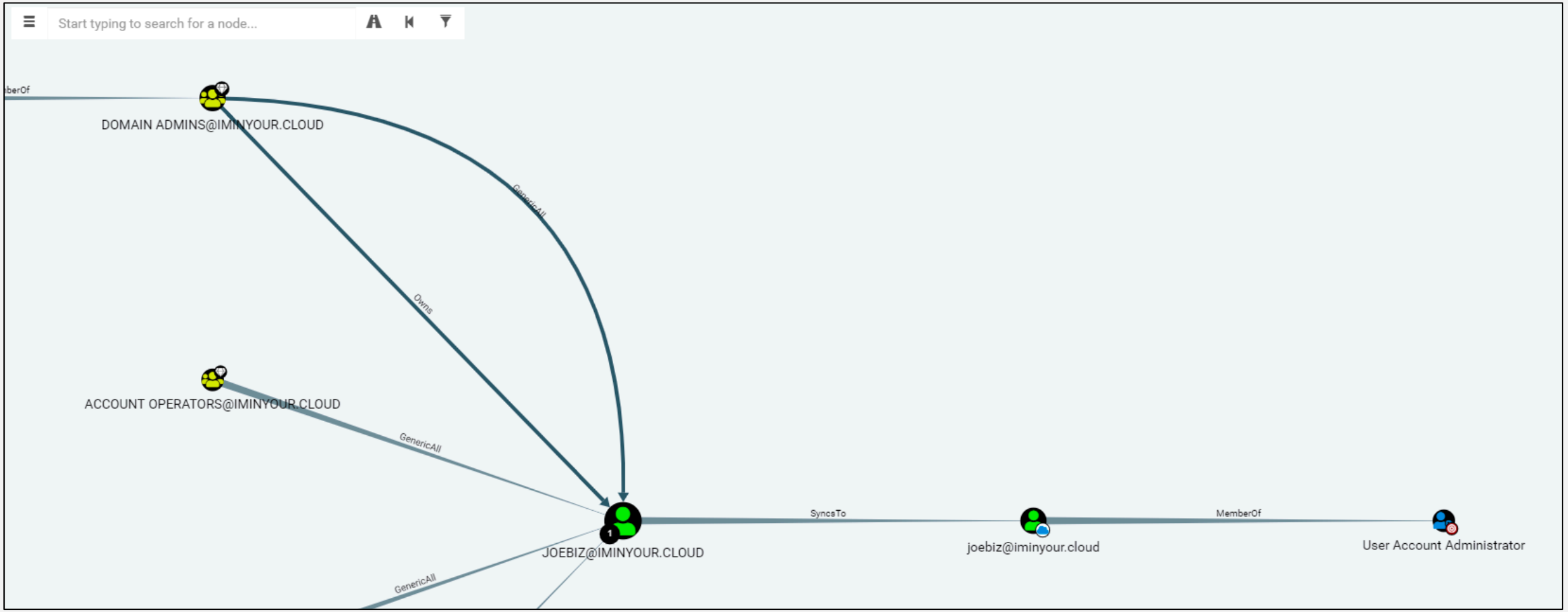
ROADtools (released in April 2020)



Source: GitHub Project "ROADtools"

Securing Privileged Access

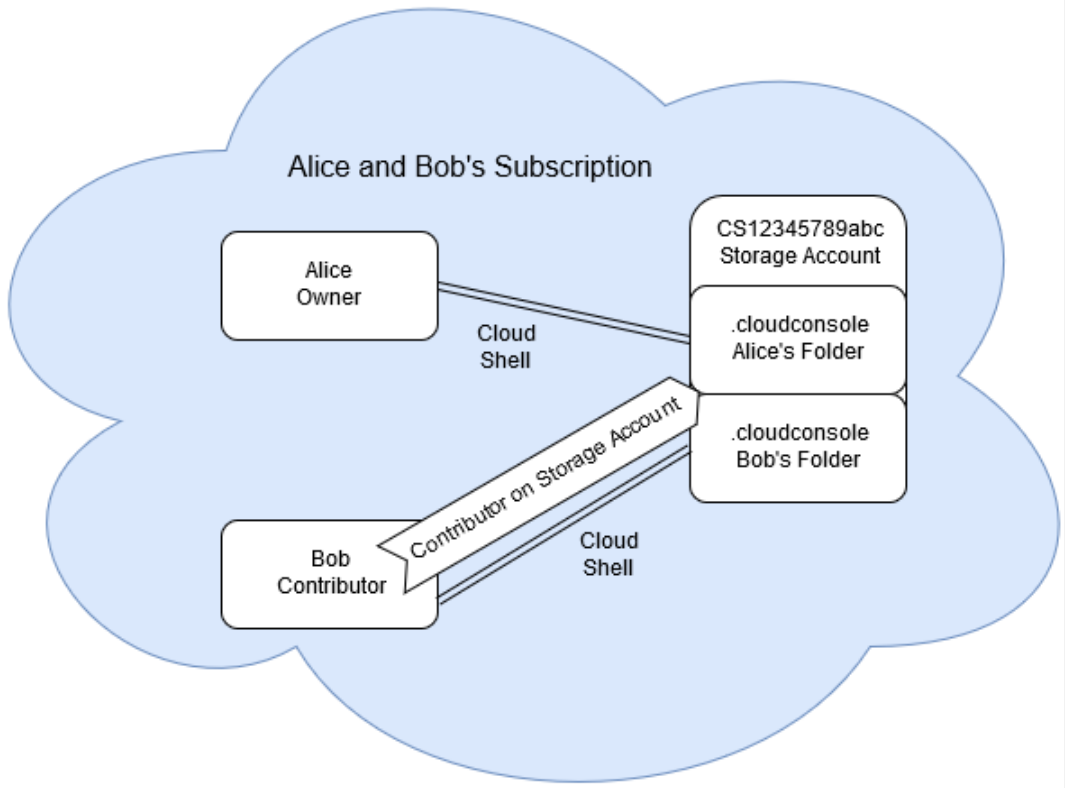
ROADtools (released in April 2020)

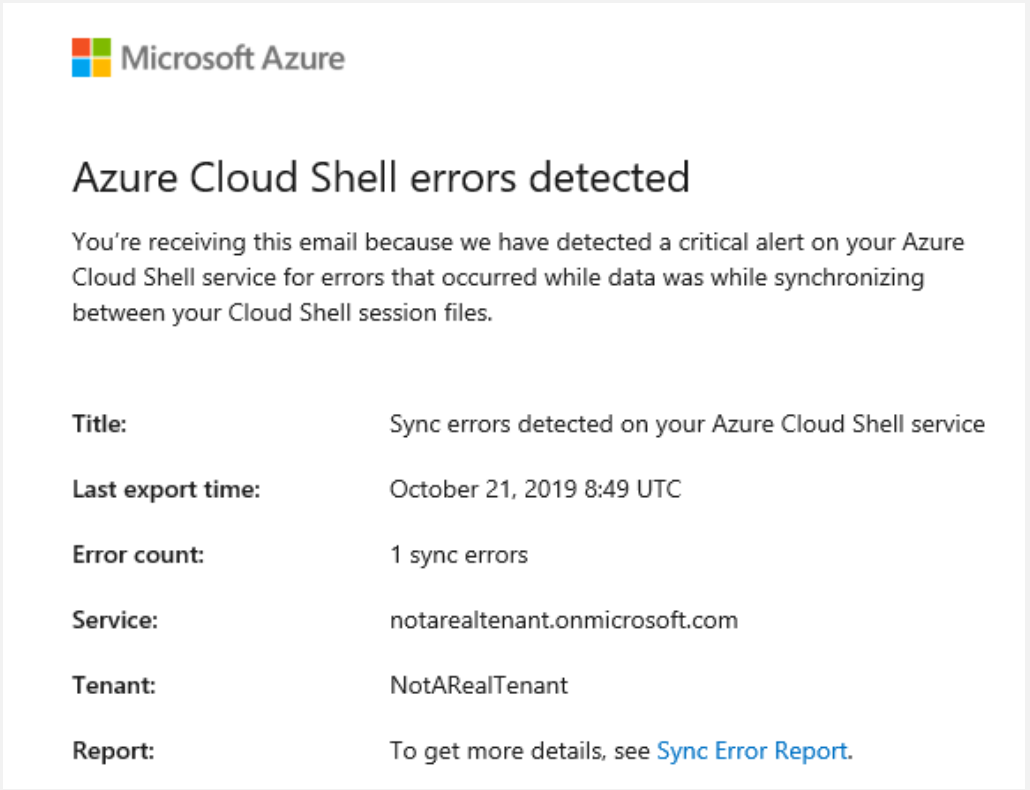


Source: GitHub Project "ROADtools"

Securing Privileged Access
Privilege Escalation from Storage Contributor

- Azure Privilege Escalation via Azure Cloud Shell:
  [Blog post by Karl Fosaaen (NetSPI)]





Microsoft Azure

Azure Cloud Shell errors detected

You're receiving this email because we have detected a critical alert on your Azure Cloud Shell service for errors that occurred while data was while synchronizing between your Cloud Shell session files.

Title:	Sync errors detected on your Azure Cloud Shell service
Last export time:	October 21, 2019 8:49 UTC
Error count:	1 sync errors
Service:	notarealtenant.onmicrosoft.com
Tenant:	NotARealTenant
Report:	To get more details, see Sync Error Report.

Source: Azure Privilege Escalation via Cloud Shell (NetSPI Blog)

Securing Privileged Access

Privilege Escalation from Storage Contributor

- Azure Privilege Escalation via Cloud Shell:

```
$token = (curl http://localhost:50342/oauth2/token --data
"resource=https://management.azure.com/" -H Metadata:true -s)
```

- Microsoft Security Response Center (MSRC) response:

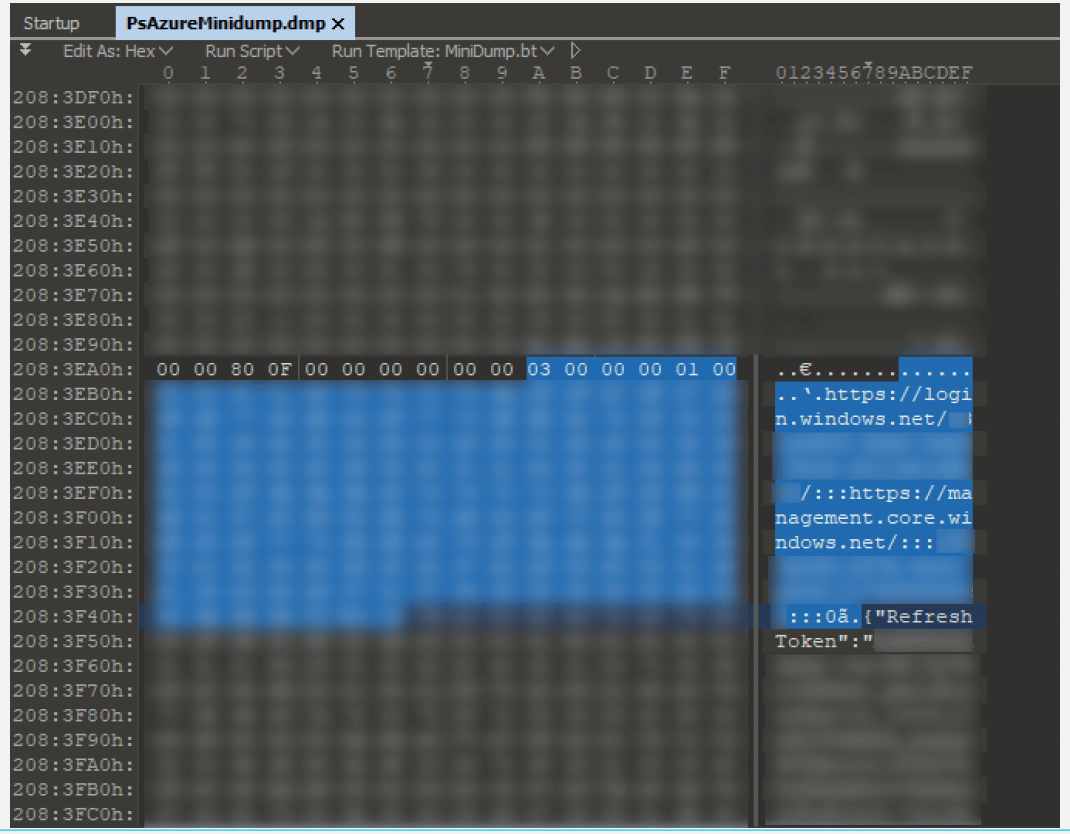
  *"…**confirming** that this is the **currently designed behavior**. We have expanded **our guidance** on this issue here – https://docs.microsoft.com/en-us/azure/cloud-shell/persisting-shell-storage#securing-storage-access and the team will look into **possible design changes** related to storage accounts."*

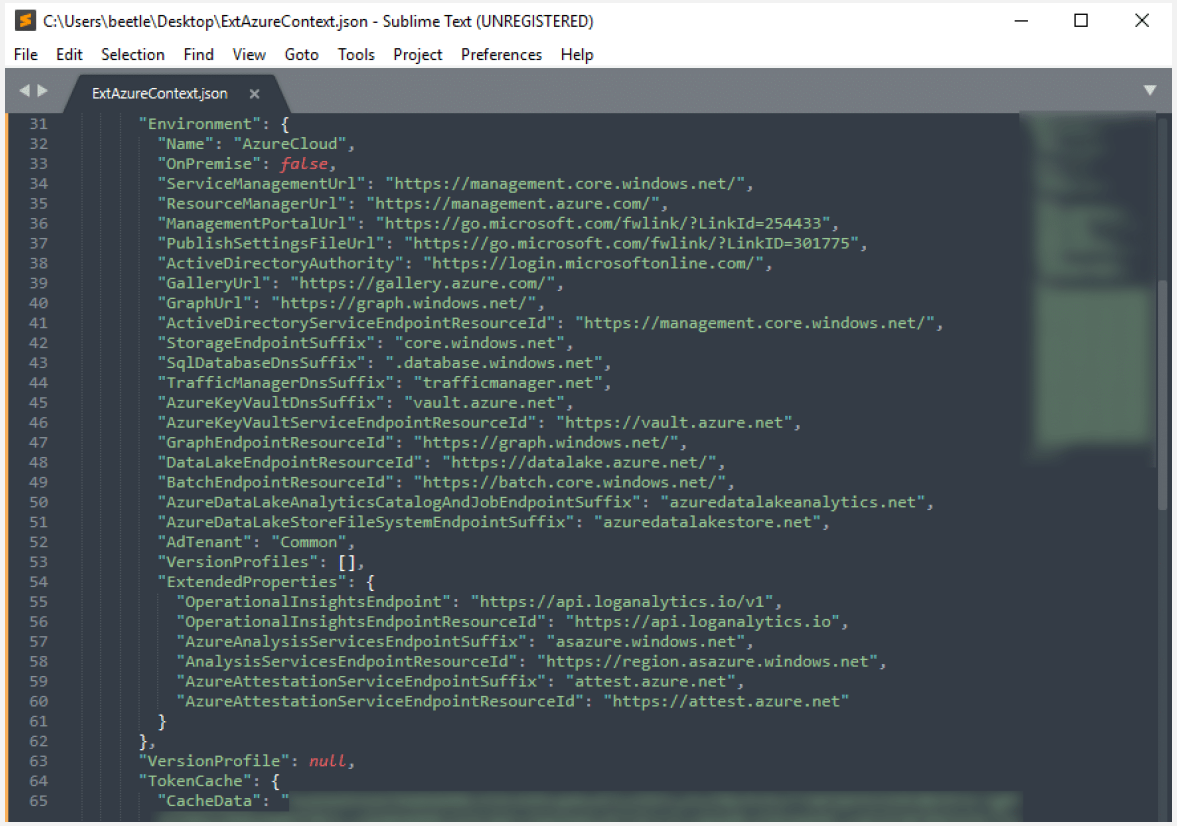
Source: Azure Privilege Escalation via Cloud Shell (NetSPI Blog)

Securing Privileged Access

Privilege Escalation from Device Administrator

- Disconnected Azure PowerShell Sessions: Dumping from PowerShell Memory: [Blog post by R.J. McDown (Lares)]



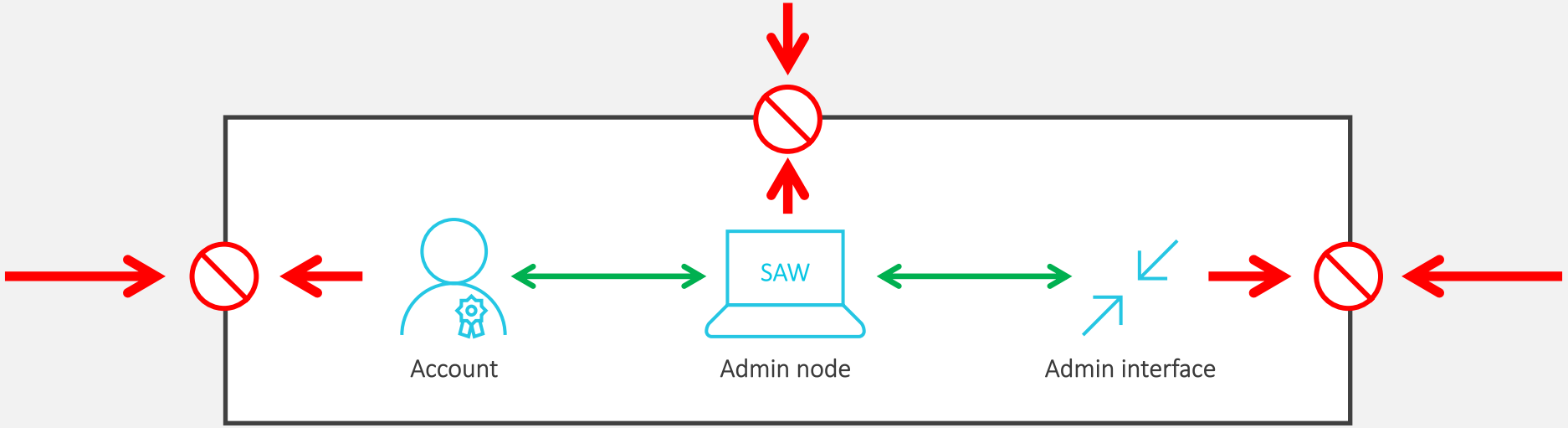


Source: [Disconnected Azure PowerShell Sessions (Lares Blog)]

Securing your Access Workstation

Securing your access workstations (SAW)

Overview of Secure Admin Workstation



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

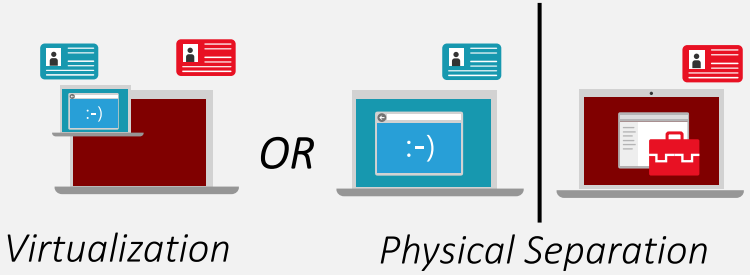
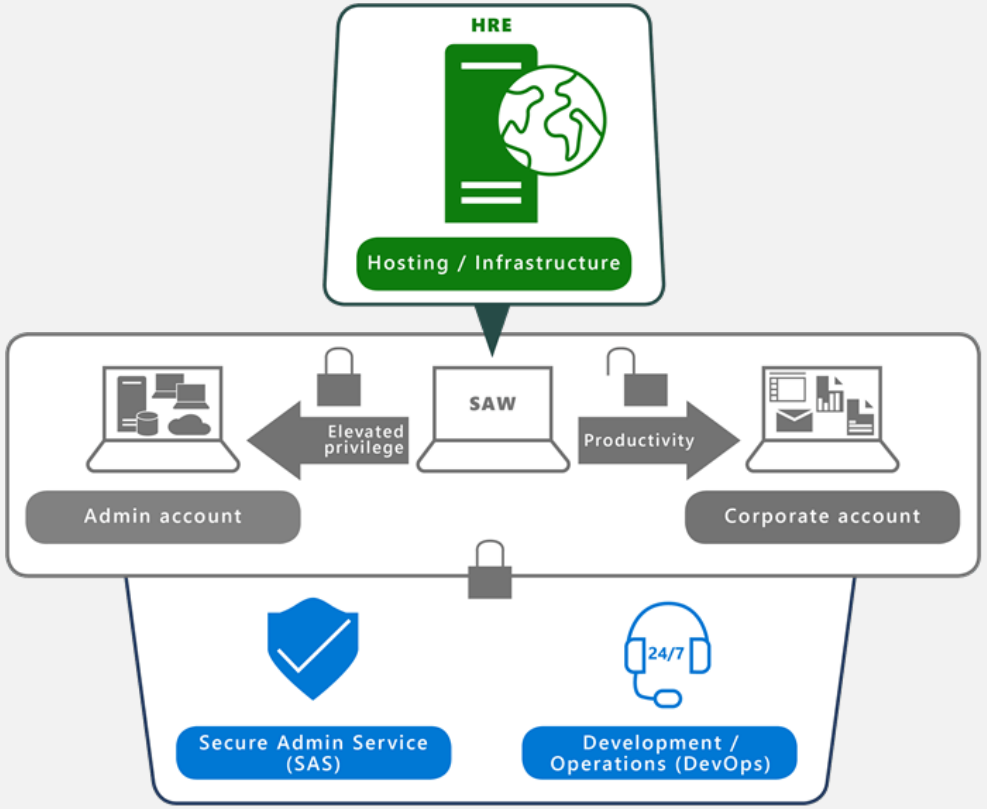


Image source: Microsoft CISO Workshop 4a - Threat Protection Strategy

Securing your access workstations (SAW)

Secure access to Azure by Microsoft IT

Secure Admin Workstation used for High Risk Environment at Microsoft

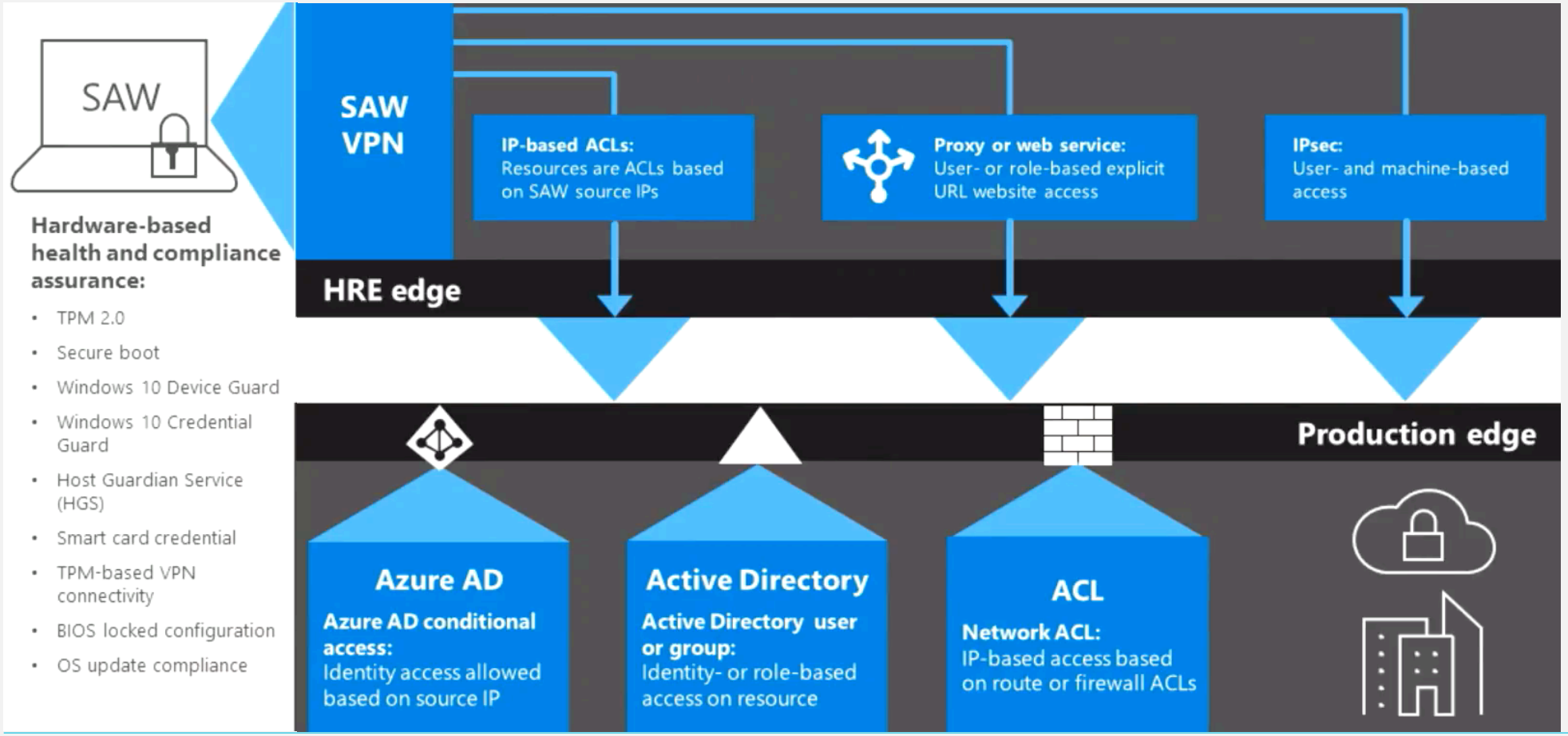


Source: Microsoft.com ("Improving security by protecting elevated-privilege accounts at Microsoft")

Securing your access workstations (SAW)

Secure access to Azure by Microsoft IT

Secure Admin Workstation used for High Risk Environment at Microsoft

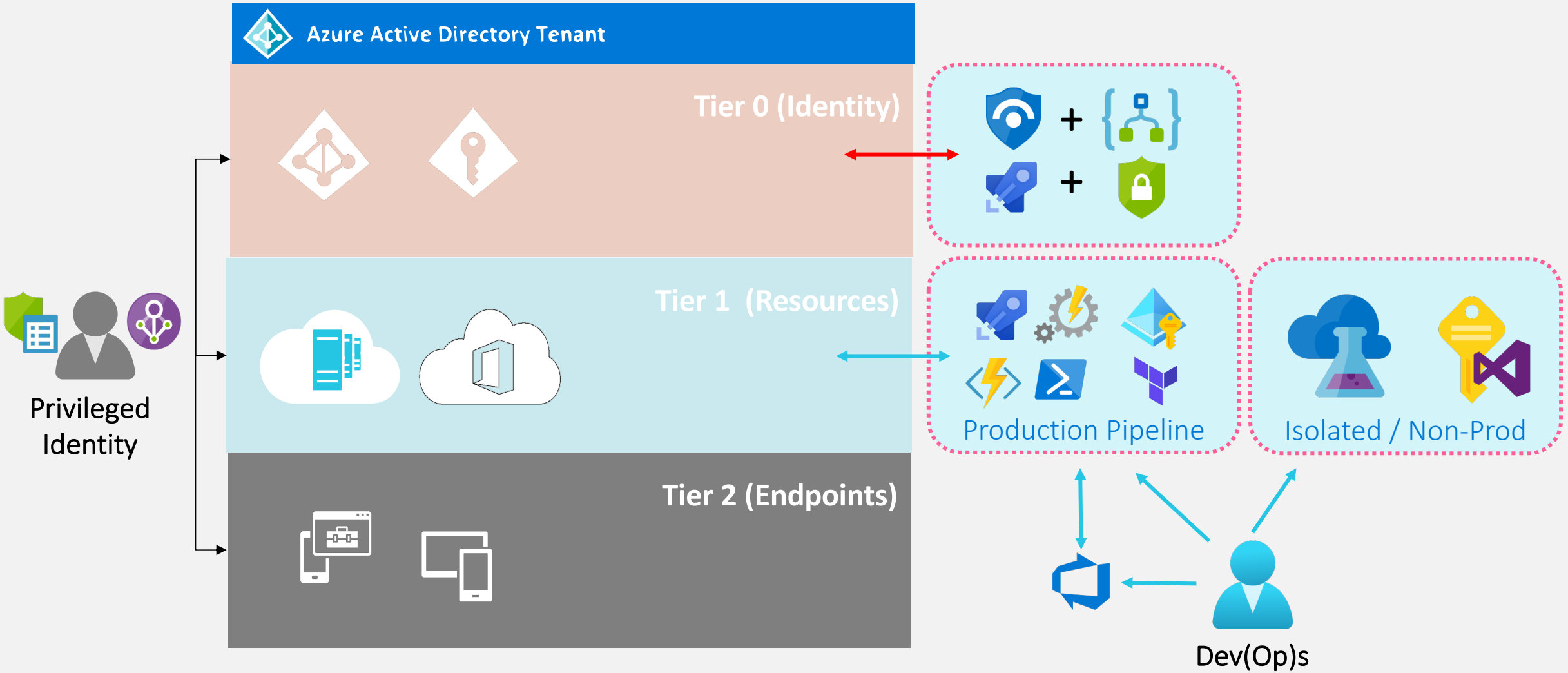


Source: Microsoft Docs („Protecting high-risk environments with secure admin workstations“)

Cloud-managed Secure Admin Workstation (SAW)

Securing Privileged Access

Tiering of Administrative Accounts and Permissions



Audit and Protection of Service Principals

Audit and Protection of Service Principals

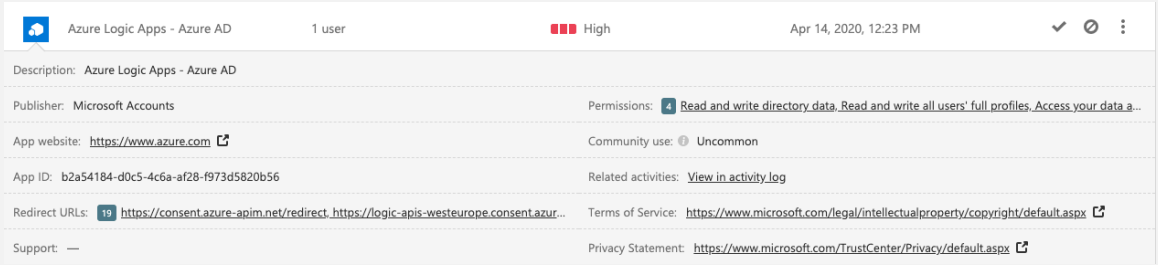
Risks of Service Principals

- Attack scenarios:
  - Delegated (OAuth2) vs. Application Permissions (without a signed-in user)
  - No security options (Conditional Access, MFA or IPC “Sign-in” risk policy)
  - No sign-in events

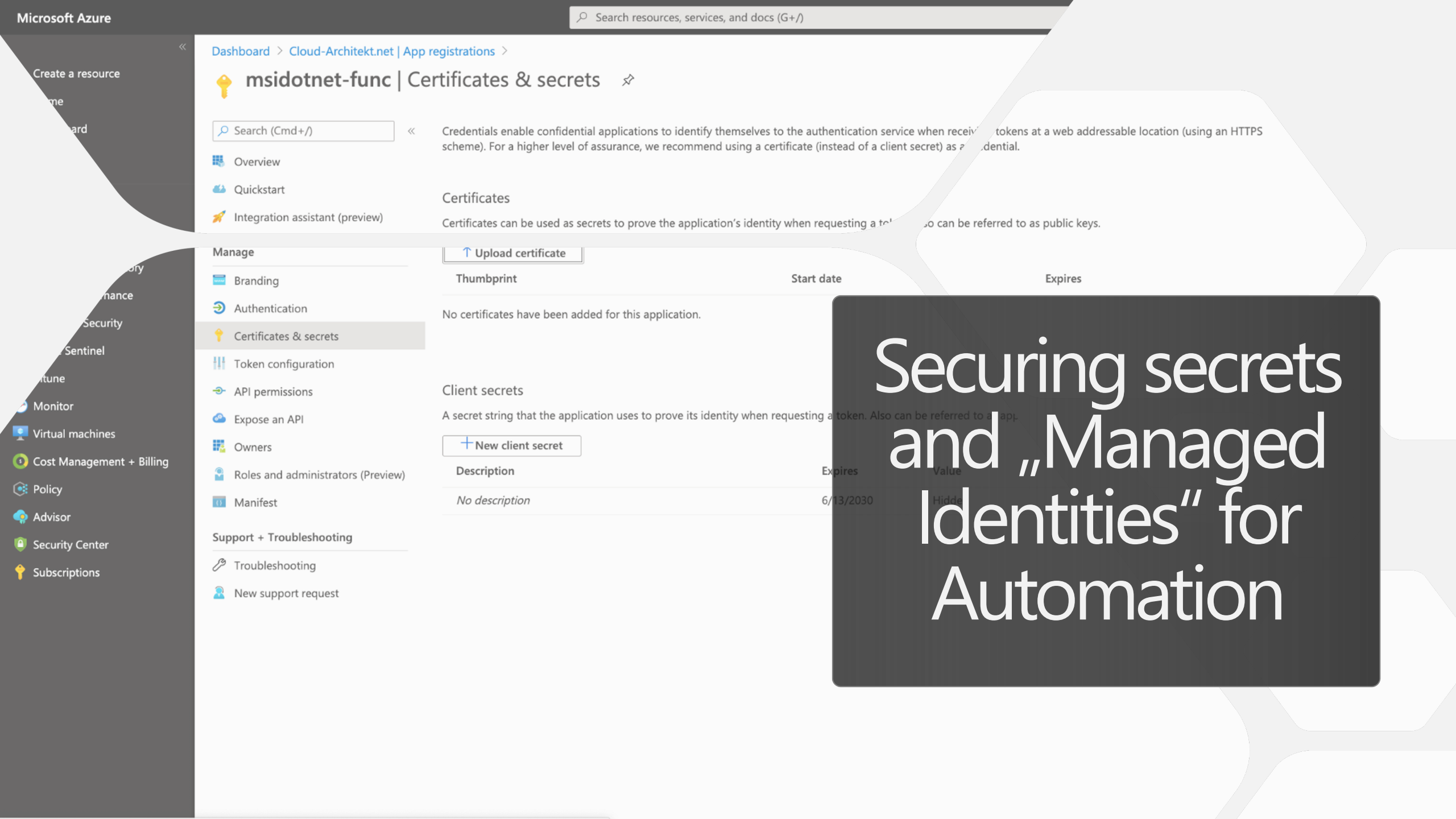
  = Application Administrators (Tier1) or Owner can impersonate an “application identity”

  = Backdooring Azure AD with service principals

- Defense and mitigations:
  - Inventory and monitoring
    - Assignments to Directory Roles
    - API permissions assignment
    - Owner of App Registration



  - “Application Administrator” as Custom Role / Scope
  - Configure expiration of ClientSecret and secure storing (Audited Key Vaults)

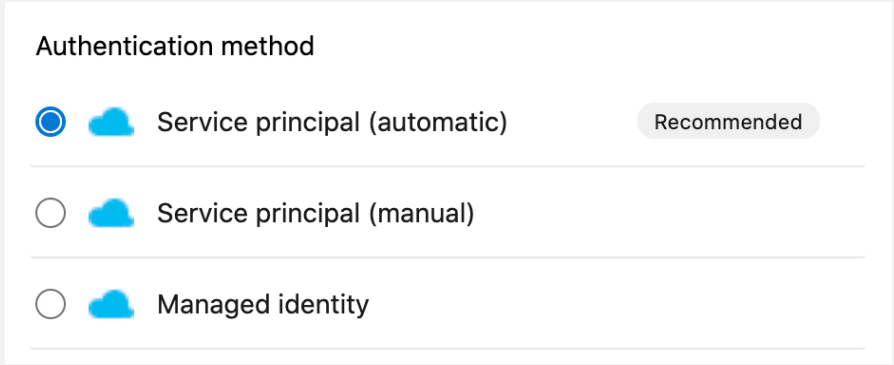


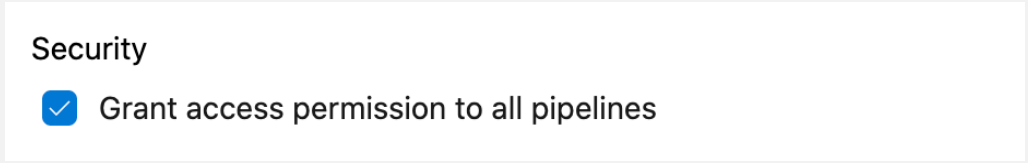
Securing secrets and „Managed Identities“ for Automation

Audit and Protection of Service Principals

Considerations of CD Pipelines in Azure DevOps

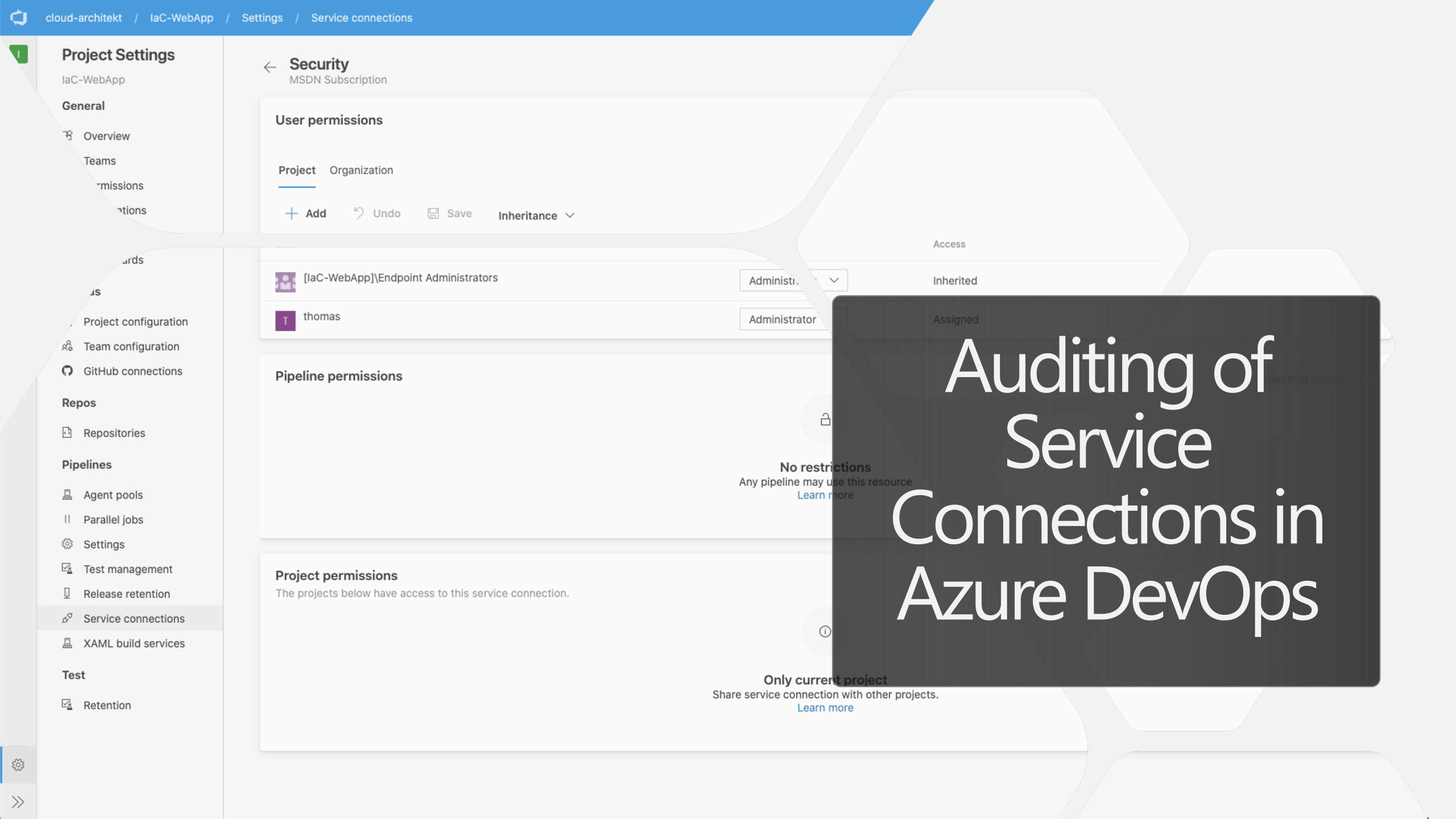
- Secrets and Service Principals in Pipeline
  - Accessing Azure Key Vault Secrets from your pipelines
  - Service Principal or Managed Identities in Service Connections

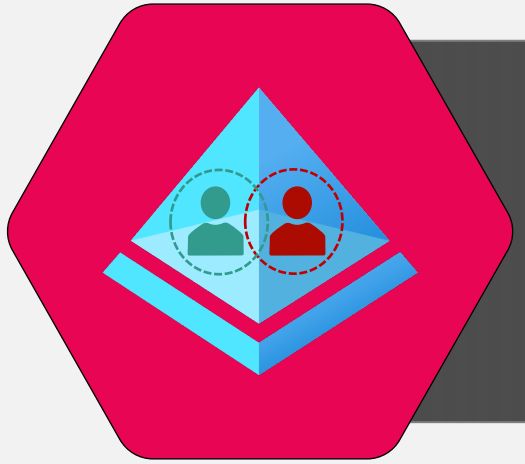




- Audit in Azure DevOps in Public Preview
  - Rest-API: **https://auditservice.dev.azure.com/<OrgName>/_apis/audit/actions**

  - **Streaming of "Auditing Logs"** → *EventHub, Log Analytics*
    - No correlation between Azure Activity and Pipeline Events → *My feature request*


cloud-architekt / IaC-WebApp / Settings / Service connections
Project Settings
IaC-WebApp
General
Overview
Teams
Project configuration
Team configuration
GitHub connections
Repos
Repositories
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Test
Retention
Security
MSDN Subscription
User permissions
Project
Organization
Add
Undo
Save
Inheritance
Access
[IaC-WebApp]\Endpoint Administrators
Inherited
thomas
Administrator
Assigned
Pipeline permissions
No restrictions
Any pipeline may use this resource
Learn more
Project permissions
The projects below have access to this service connection.
Only current project
Share service connection with other projects.
Learn more
Auditing of Service Connections in Azure DevOps



Isolation & Protection on Inter-Tenant-Level

Protecting Privileged Identities
Considerations and Limitations

Privileged Accounts and Resources

- Consider limitations of Administrative Units
- Tenant-wide delegation by AAD / Azure RBAC
  - Separation of all privileged resources (Cloud Shell)

Secure Admin Workstations (SAW)

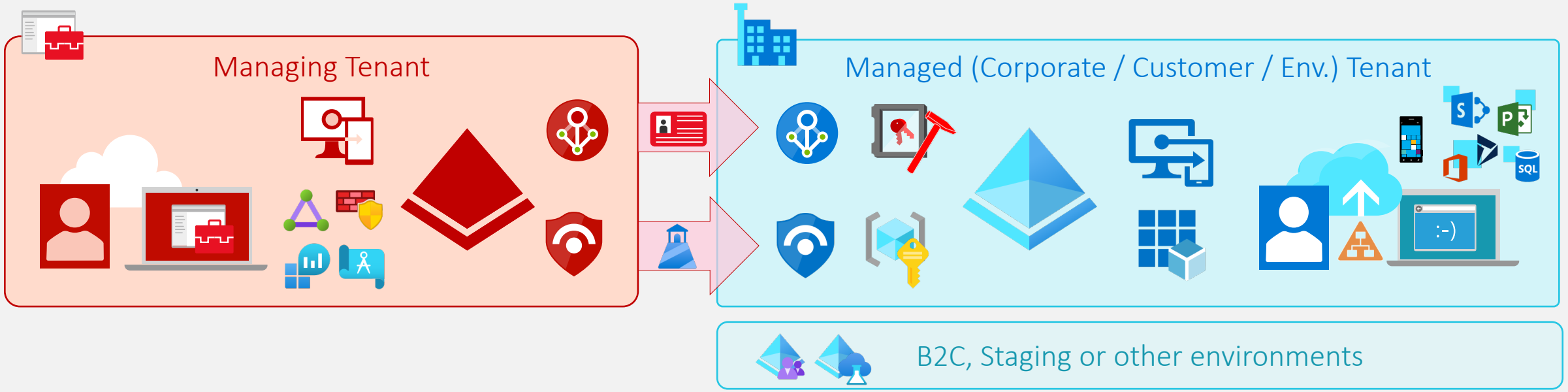
- Scoped and Intune RBAC roles separation between SAW and Standard Workplaces
- Client Certificate (via MCAS) or Trusted IP (VPN) to verify SAW device
- Deployment & Usability of Virtualization

Service Principals and DevOps

- Protection of secrets and automation tasks
- Audit and security concept of DevOps tools
- Using “Managed Identity” where possible

Protecting Privileged Identities

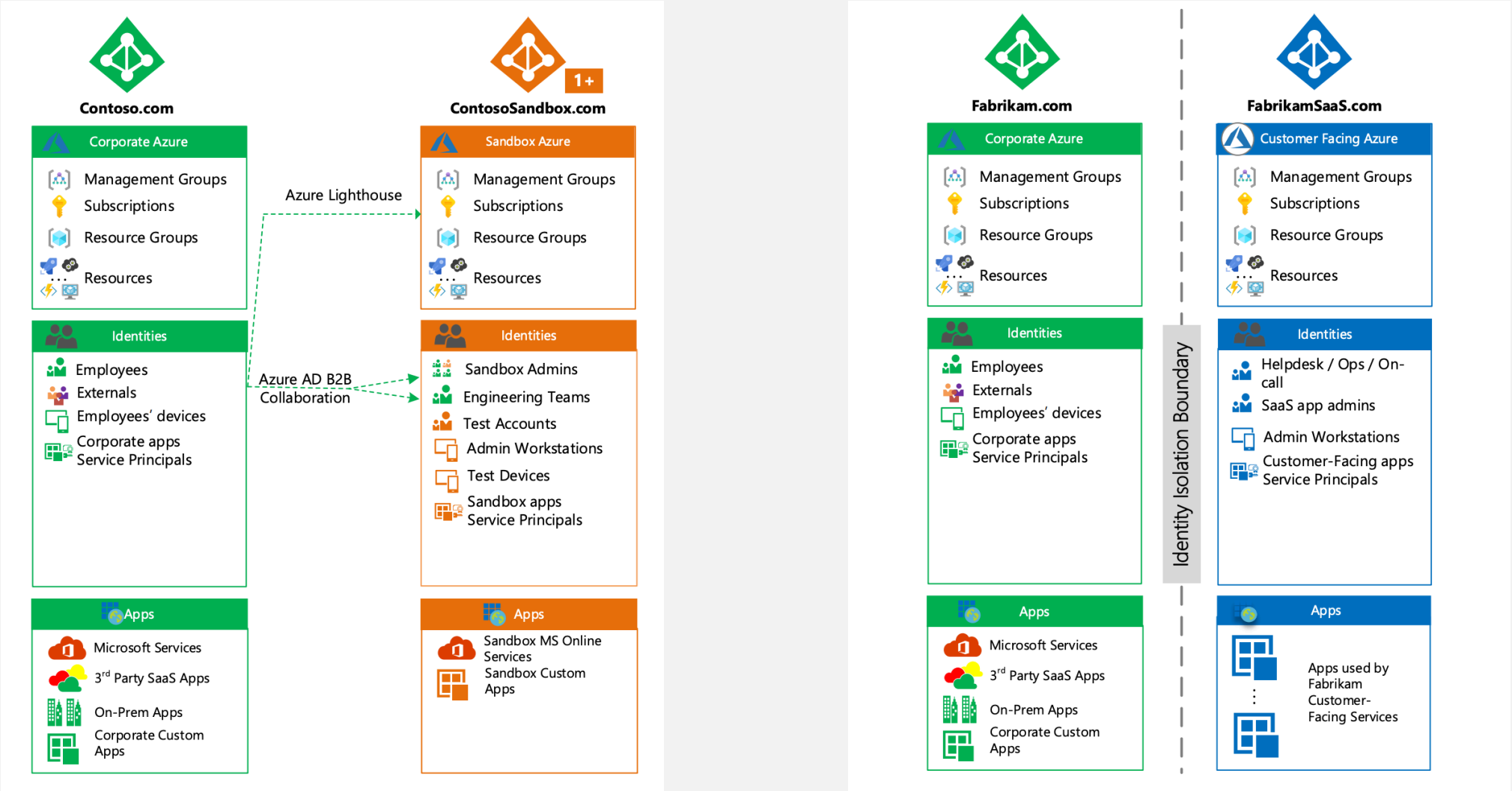
“Red Tenant“ – Azure AD Tenant as security boundary



- **No hybrid identity** integration (no security risks by Azure AD Connect)
- **Privileged resources only** (security groups, apps, network, devices,..)
- Reduced attack surface, **shared resources from secured environment**
- Dependance on **„Azure AD B2B“ feature**, Doubled Identity Protection, FIDO2 & Security Policies
- **Costs and Complexitiy** (Licenses, Administrative Costs, Additional VNet Peering)
- **Limited support by Microsoft** (no PAM trust, „single tenant“ approach, avoid complexiity)

Protecting Privileged Identities

“Sandbox/Staging Tenants“ – Identity Isolation Boundary



Source: [Microsoft Whitepaper ("Securing Azure environments with Azure Active Directory")]

Securing your privileged identity and access

More than just vaulting and protecting admin passwords

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 Access Worktation

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

Privileged Service Principals

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

Thank You

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net