SECURING YOUR PRIVILEGED ACCESS IN MICROSOFT AZURE

OVERVIEW AND PRACTICES

Azure Ruhrgebiet

January 24th, 2023

THOMAS NAUNHEIM

Microsoft Security MVP,
Cyber Security Architect @glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

Microsoft® Most Valuable Professional

Azure Meetup BONN

CLOUD IDENTITY SUMMIT '22

AGENDA

PRIVILEGED
IDENTITIES

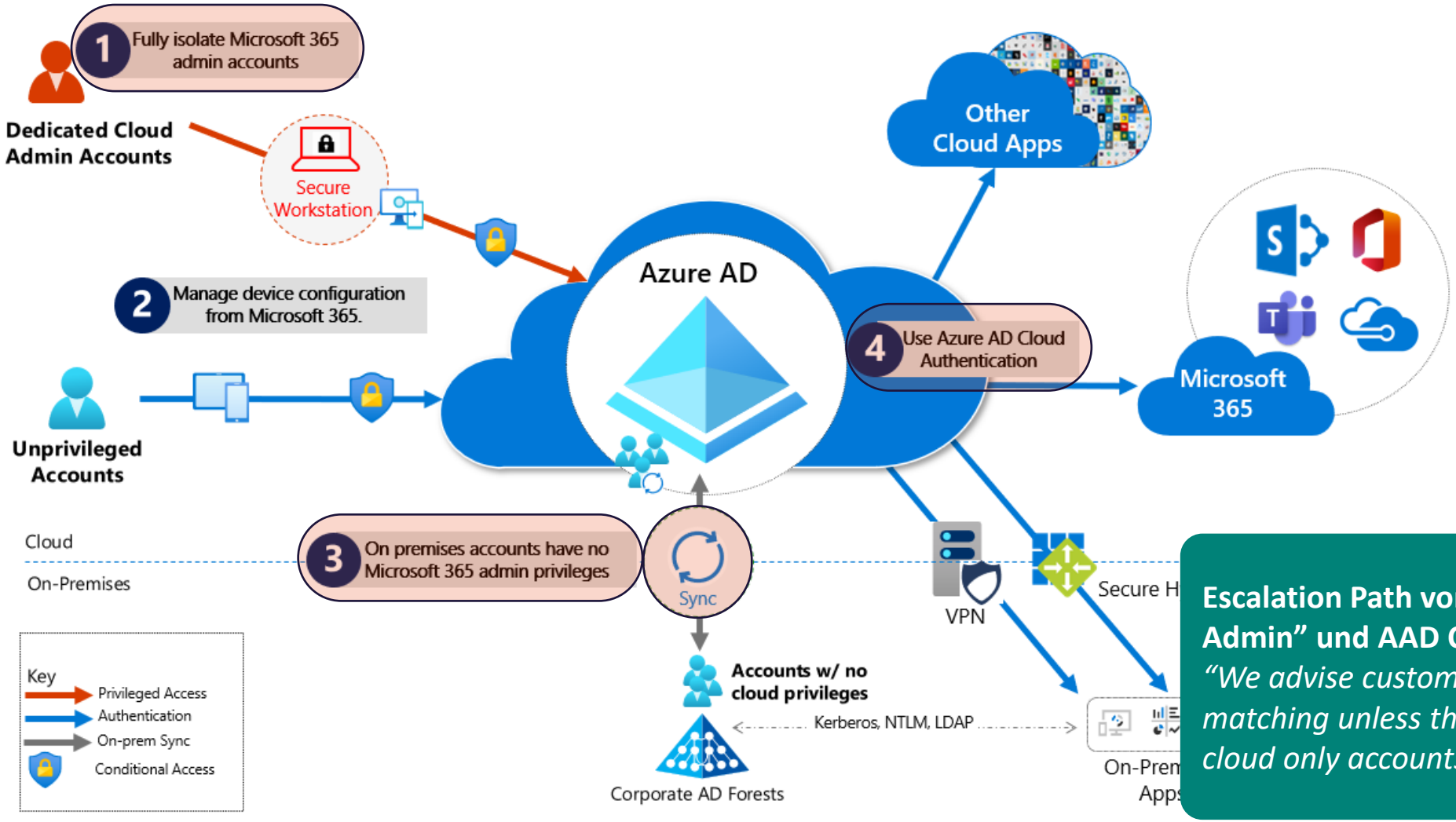
PRIVILEGED
ENDPOINTS

PRIVILEGED
ACCESS

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

PROTECTION OF **PRIVILEGED IDENTITIES**

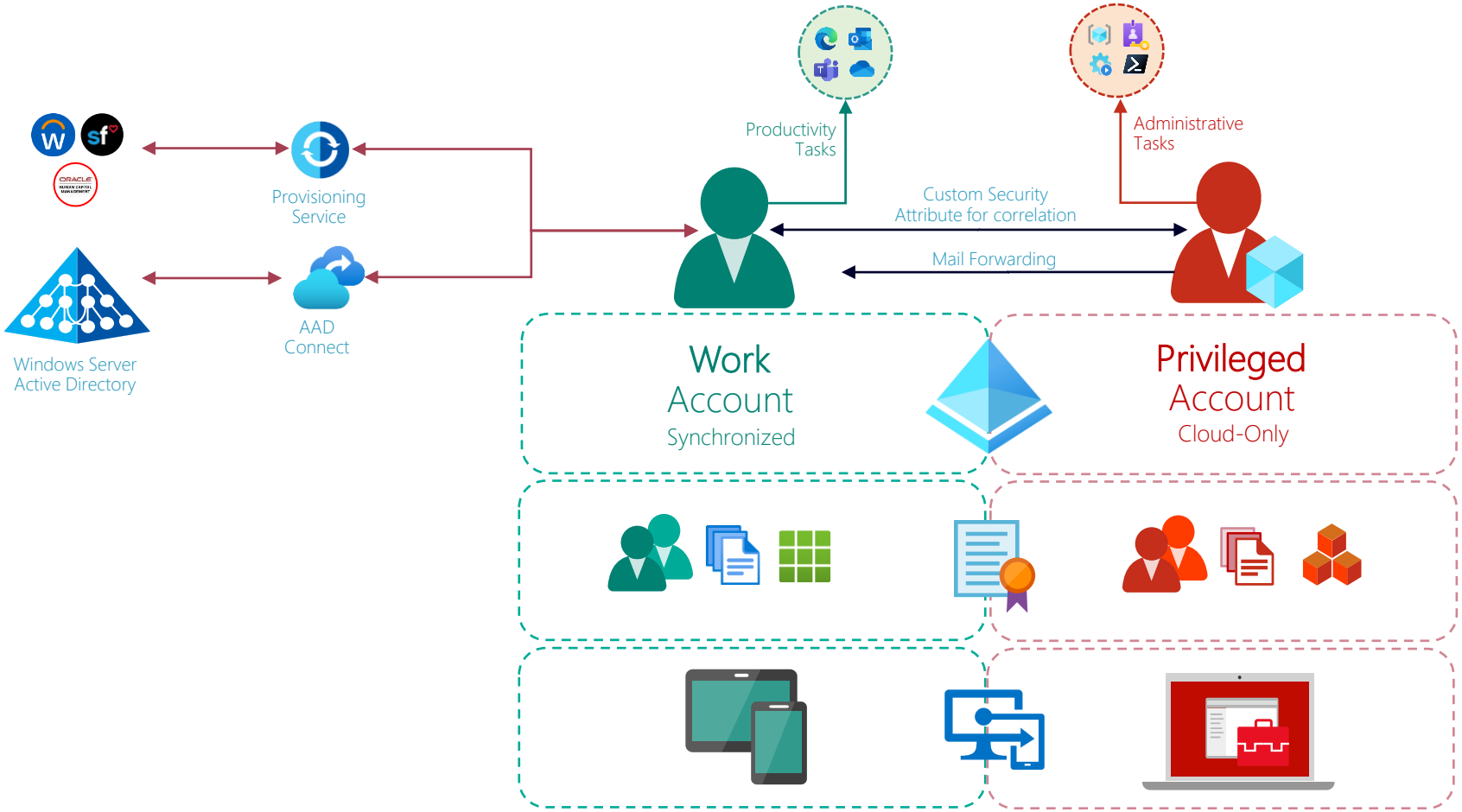
Protecting M365 and Azure from on-prem attacks



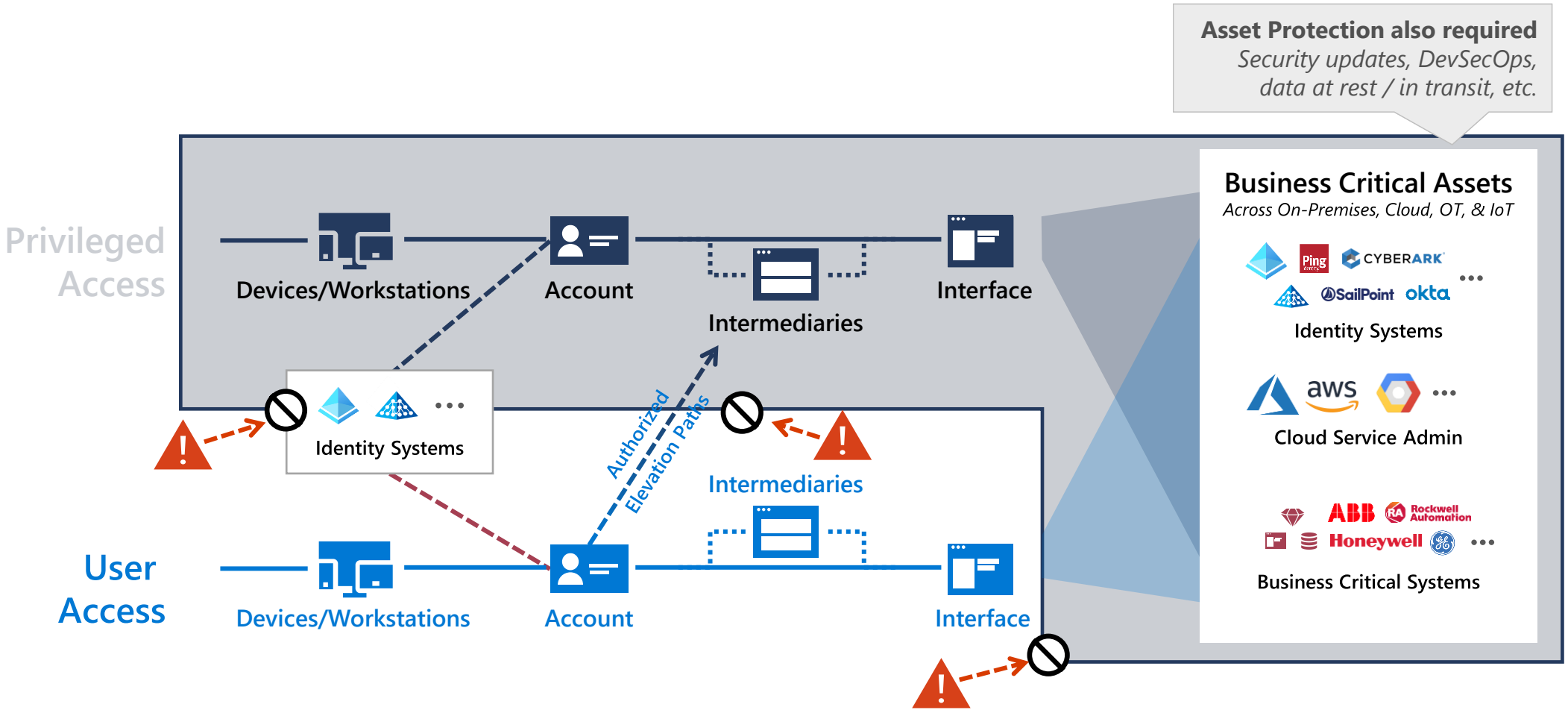
Escalation Path von "Hybrid Identity Admin" und AAD Connect:
"We advise customers to disable soft matching unless they need it to take over cloud only accounts"

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

Foundation of Privileged User Accounts



Privileged Access & Authorized Elevated Paths

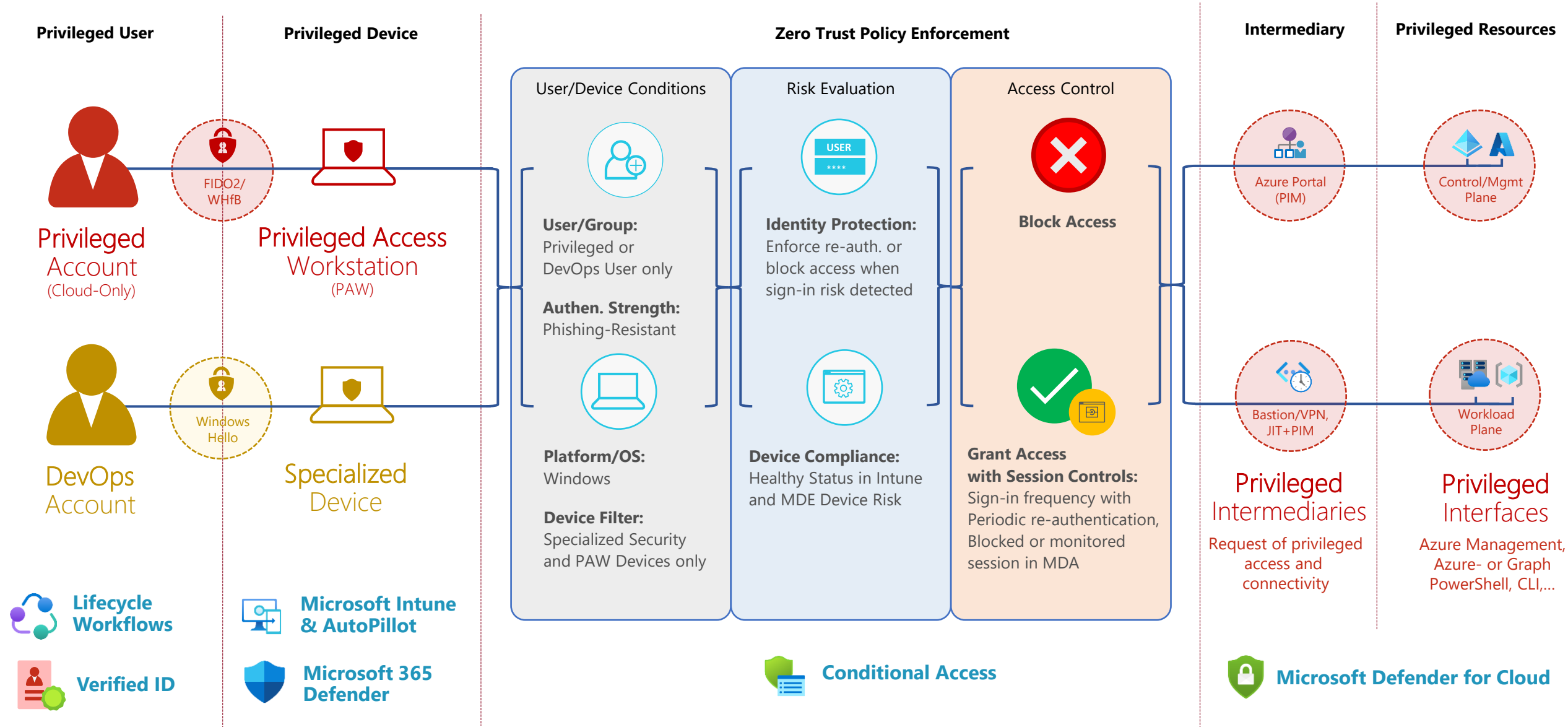


"End-to-end Session Security - Establish explicit Zero Trust validation for privileged sessions, user sessions, and authorized elevation paths."

Source: "Privileged access Strategy" (Microsoft)

PROTECTION OF PRIVILEGED IDENTITIES

Access Paths to Privileged Interfaces



Identity Lifeycle, Conditional Access and Monitoring of Privileged Identities

LIVE DEMO

SECURING
PRIVILEGED ENDPOINTS

Foundation of Admin Workstations (SAW/PAW)

- **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…)

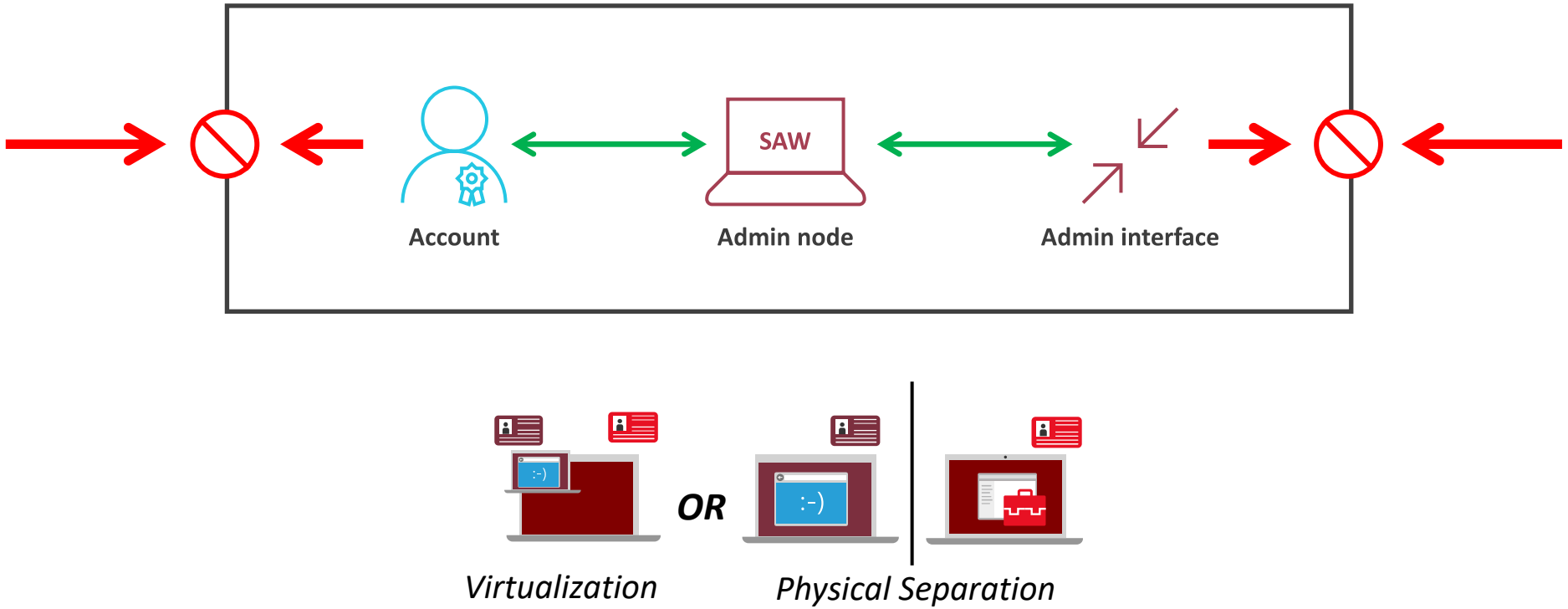


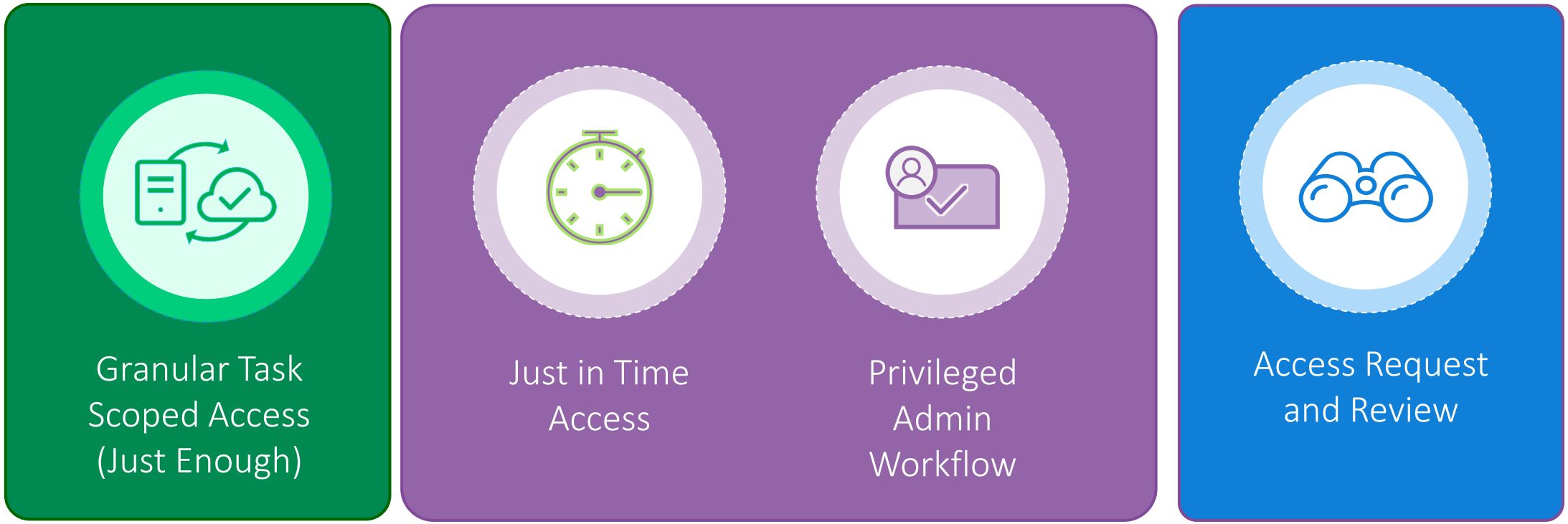
Image source: "Microsoft CISO Workshop 4a - Threat Protection Strategy"

Using PAW for Privileged Access and Replay of (Refresh) Tokens from Cloud Shell

LIVE DEMO

SECURING
PRIVILEGED ACCESS

Foundation of Privileged Access



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**.“

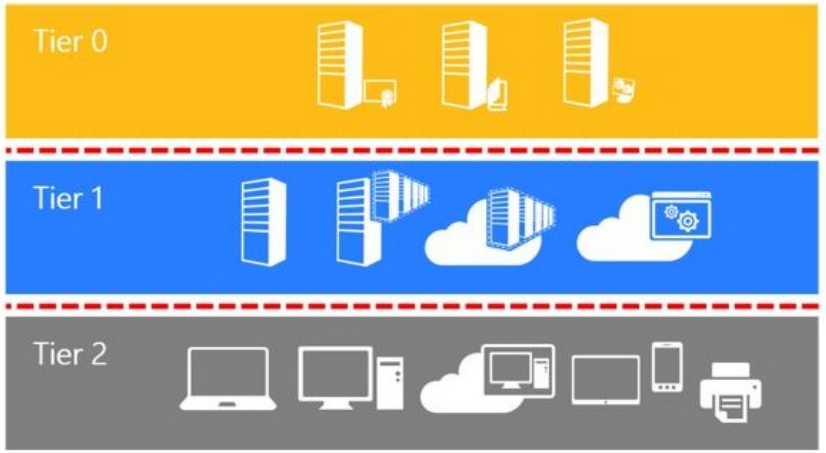
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

Active Directory administrative tier model

02/14/2019 • 33 minutes to read • +6

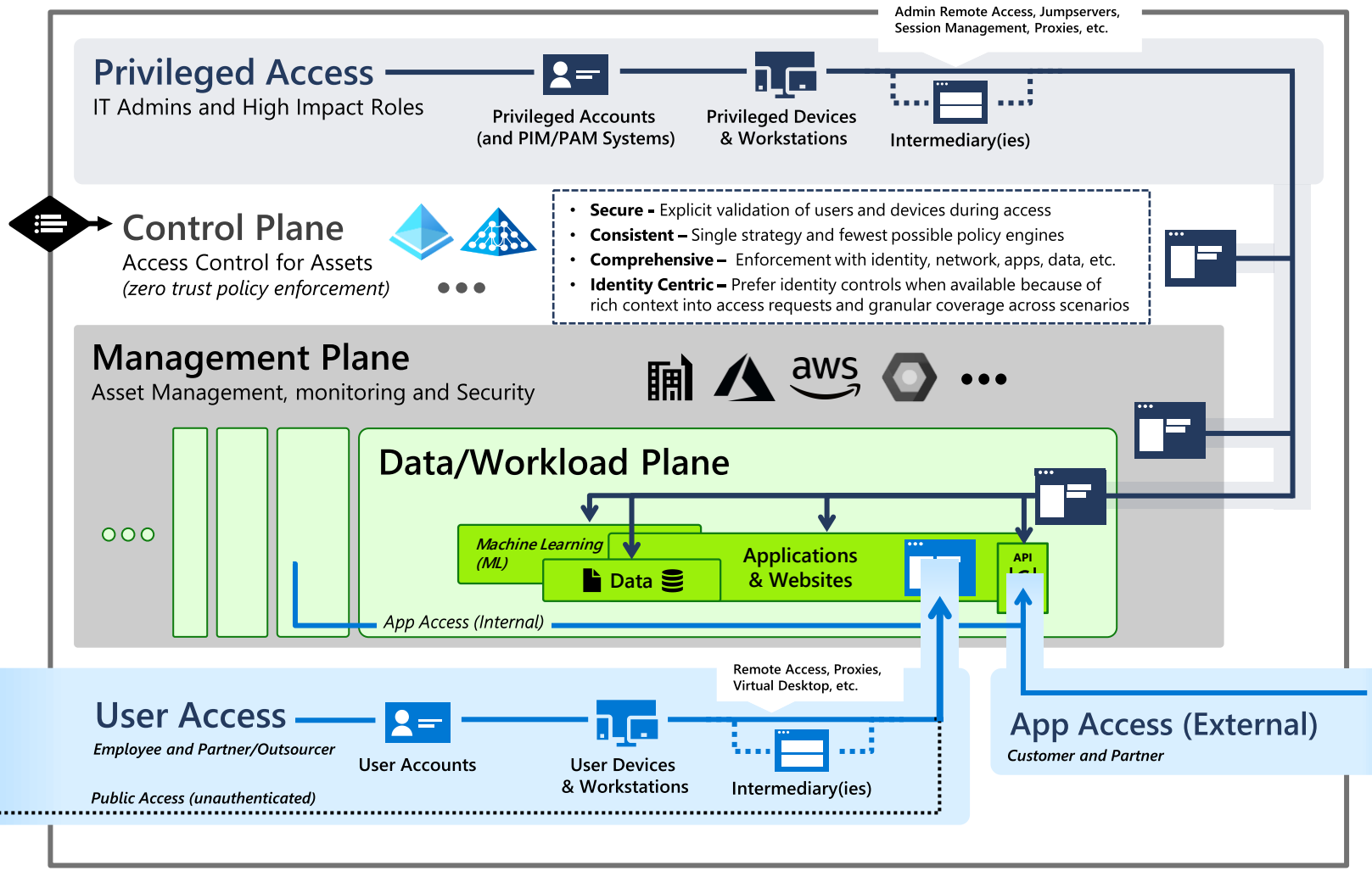
Applies To: Windows Server

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

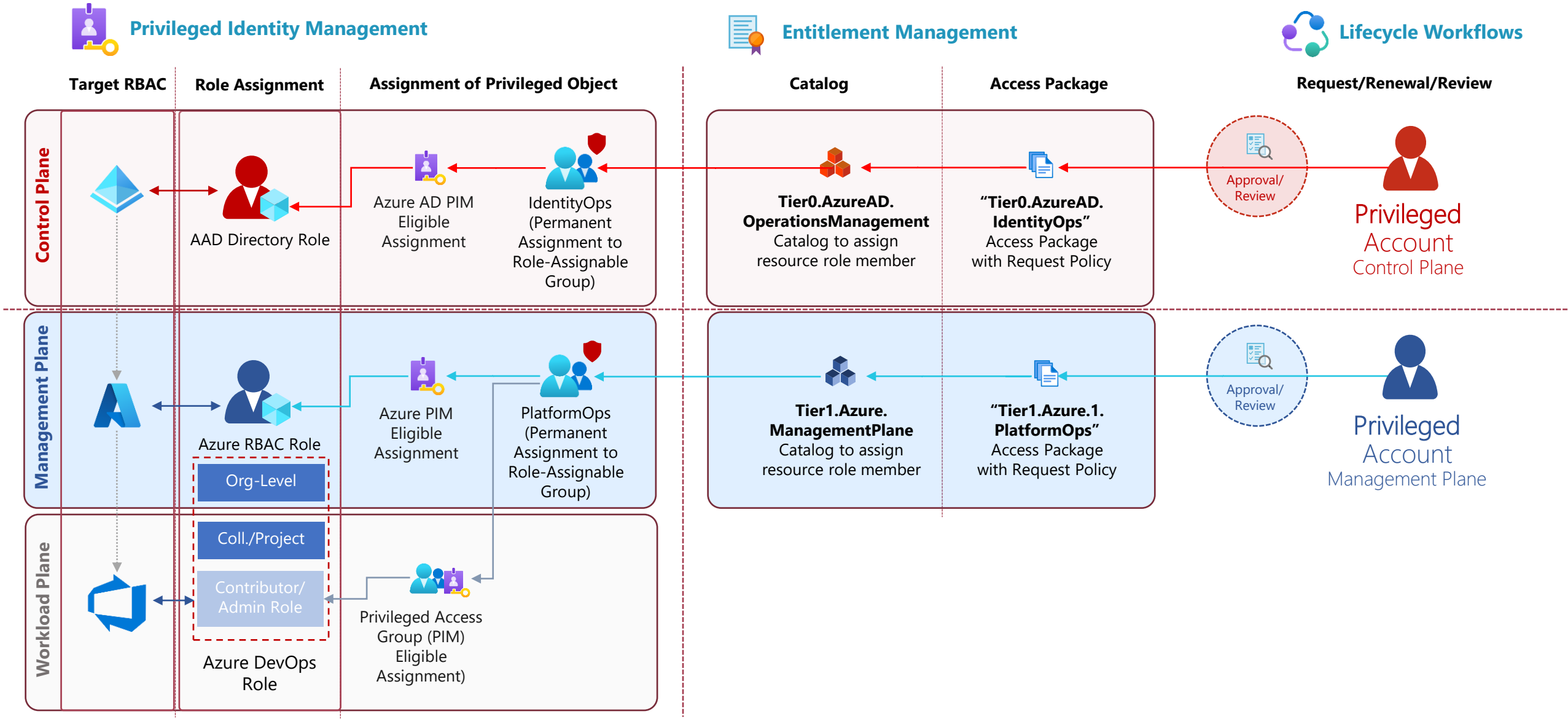
- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access

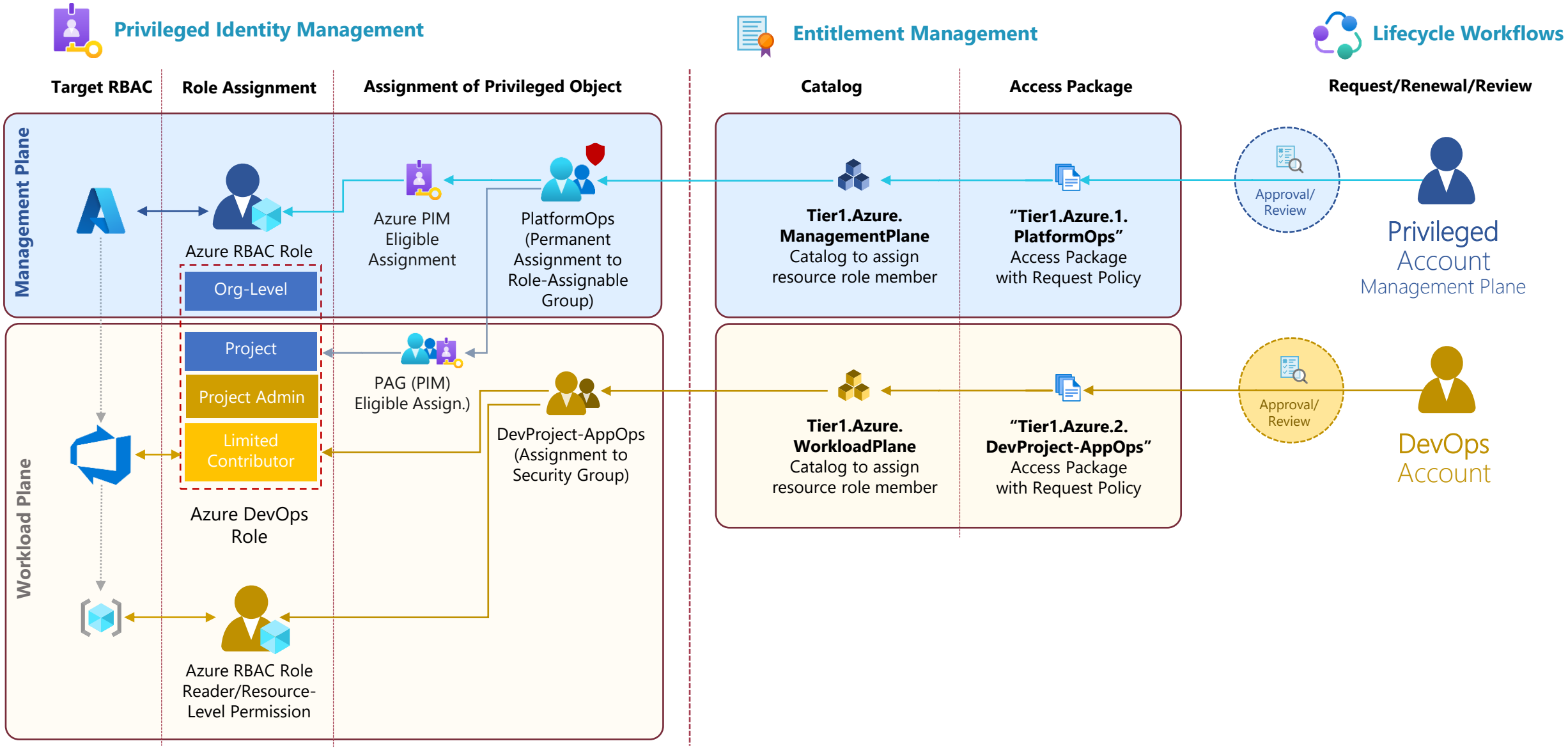
How employees, partners, and customers access these resources

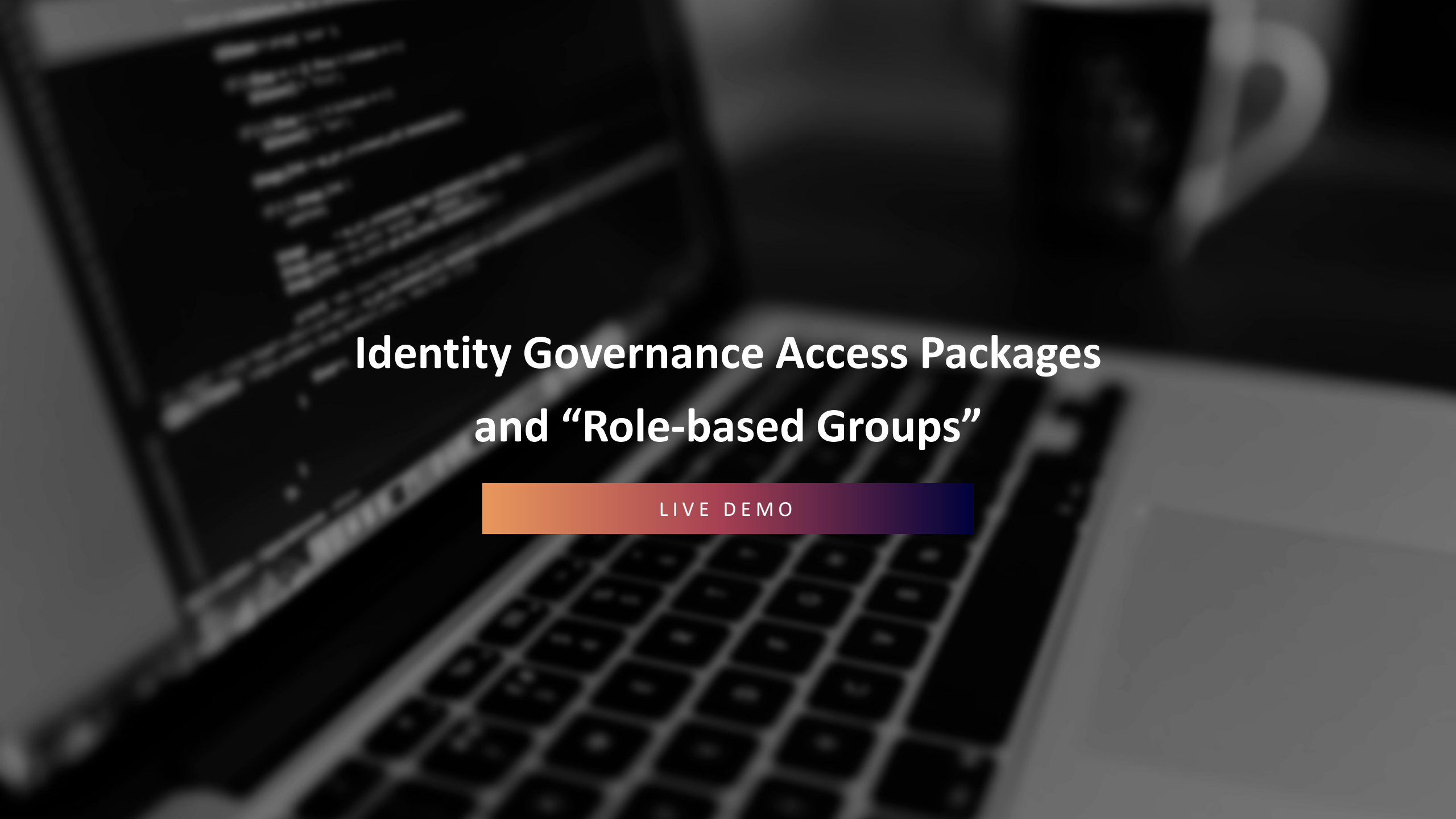
Source: "Securing Azure environments with Azure Active Directory"

My implementation of “EAM” in Azure



My implementation of “EAM” in Azure

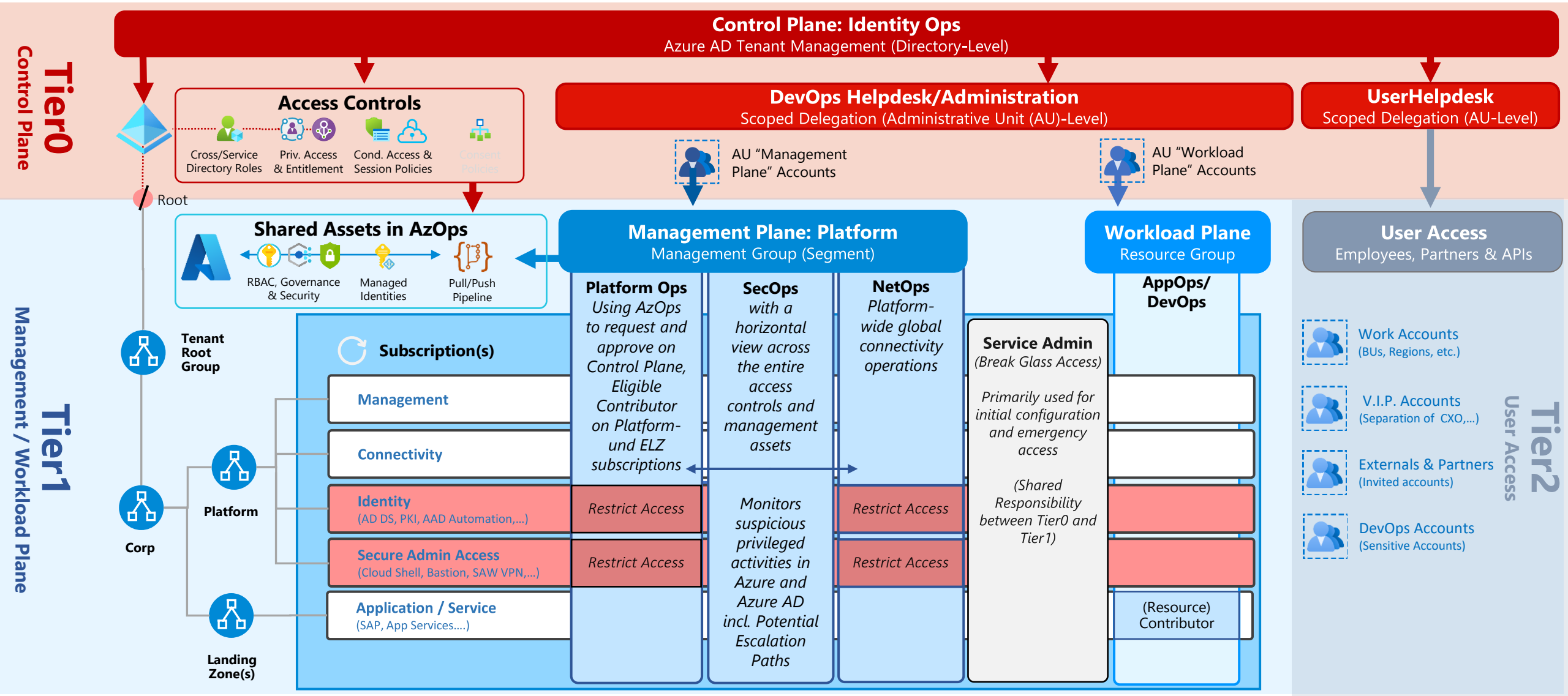




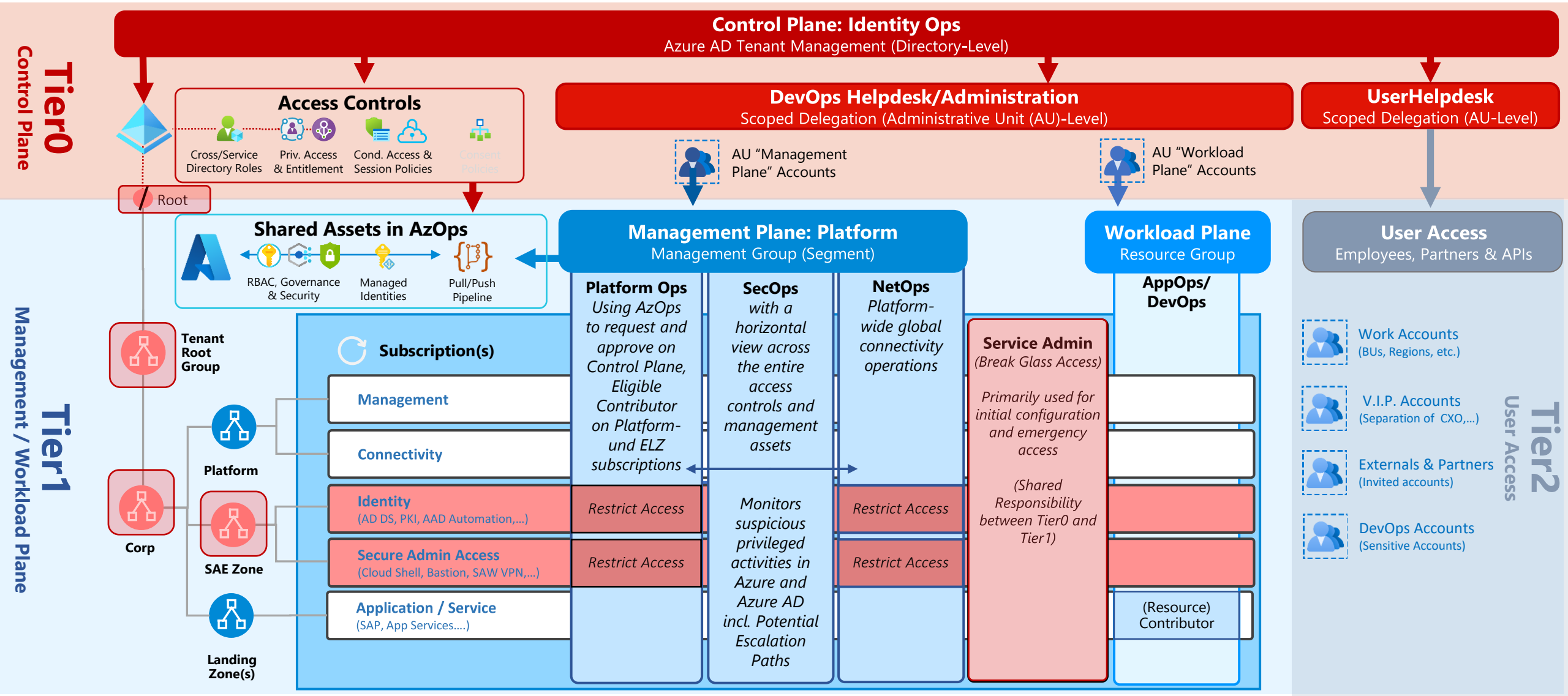
Identity Governance Access Packages and “Role-based Groups”

LIVE DEMO

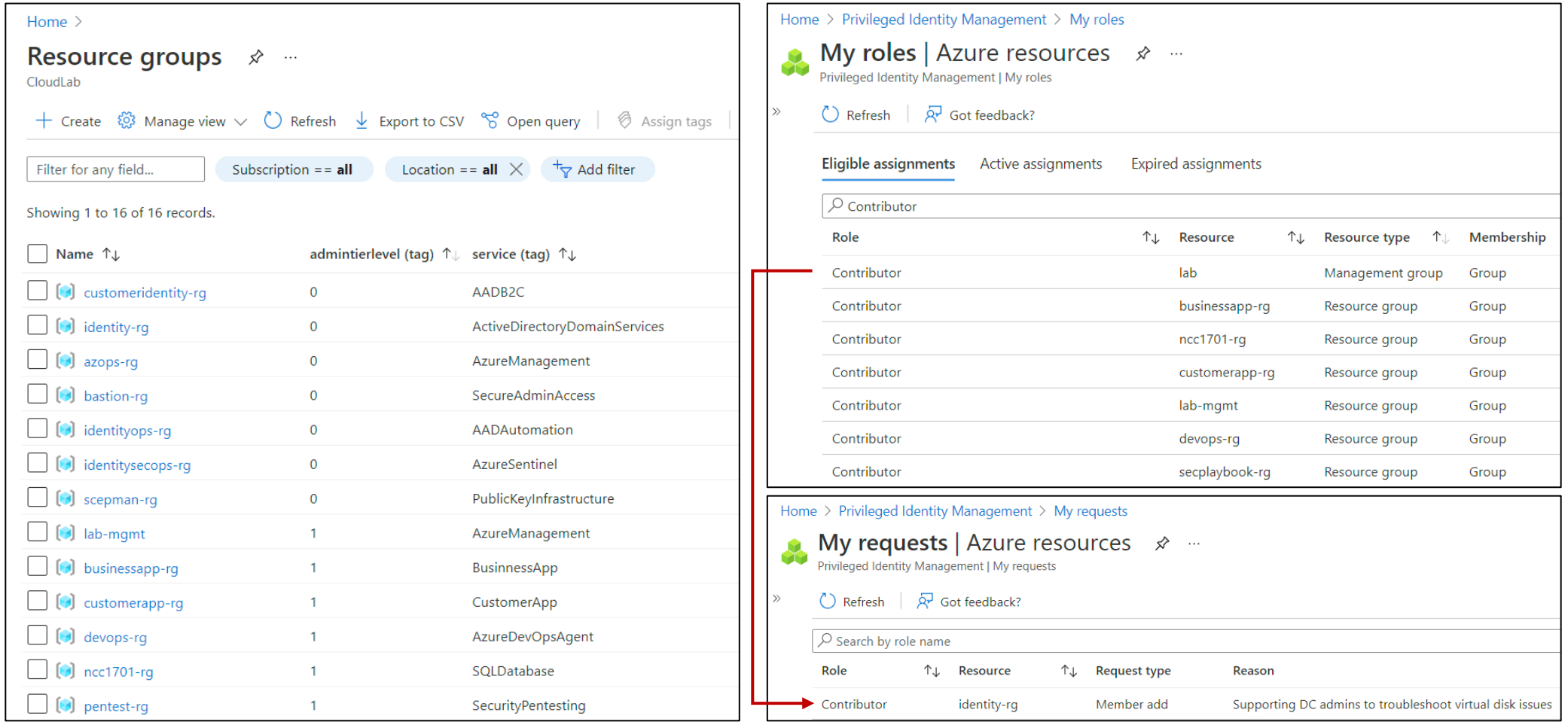
My implementation of “EAM” in Azure



My implementation of “EAM” in Azure



Tagged Control Plane Assets with Azure PIM Approval



Home >

Resource groups

CloudLab

Create | Manage view | Refresh | Export to CSV | Open query | Assign tags

Filter for any field... | Subscription == all | Location == all | Add filter

Showing 1 to 16 of 16 records.

Name	admintierlevel (tag)	service (tag)
customeridentity-rg	0	AADB2C
identity-rg	0	ActiveDirectoryDomainServices
azops-rg	0	AzureManagement
bastion-rg	0	SecureAdminAccess
identityops-rg	0	AADAutomation
identitysecops-rg	0	AzureSentinel
scepman-rg	0	PublicKeyInfrastructure
lab-mgmt	1	AzureManagement
businessapp-rg	1	BusinnessApp
customerapp-rg	1	CustomerApp
devops-rg	1	AzureDevOpsAgent
ncc1701-rg	1	SQLDatabase
pentest-rg	1	SecurityPentesting

Home > Privileged Identity Management > My roles

My roles | Azure resources

Privileged Identity Management | My roles

Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Contributor

Role	Resource	Resource type	Membership
Contributor	lab	Management group	Group
Contributor	businessapp-rg	Resource group	Group
Contributor	ncc1701-rg	Resource group	Group
Contributor	customerapp-rg	Resource group	Group
Contributor	lab-mgmt	Resource group	Group
Contributor	devops-rg	Resource group	Group
Contributor	secplaybook-rg	Resource group	Group

Home > Privileged Identity Management > My requests

My requests | Azure resources

Privileged Identity Management | My requests

Refresh | Got feedback?

Search by role name

Role	Resource	Request type	Reason
Contributor	identity-rg	Member add	Supporting DC admins to troubleshoot virtual disk issues

Automated Classification of Privileged Access

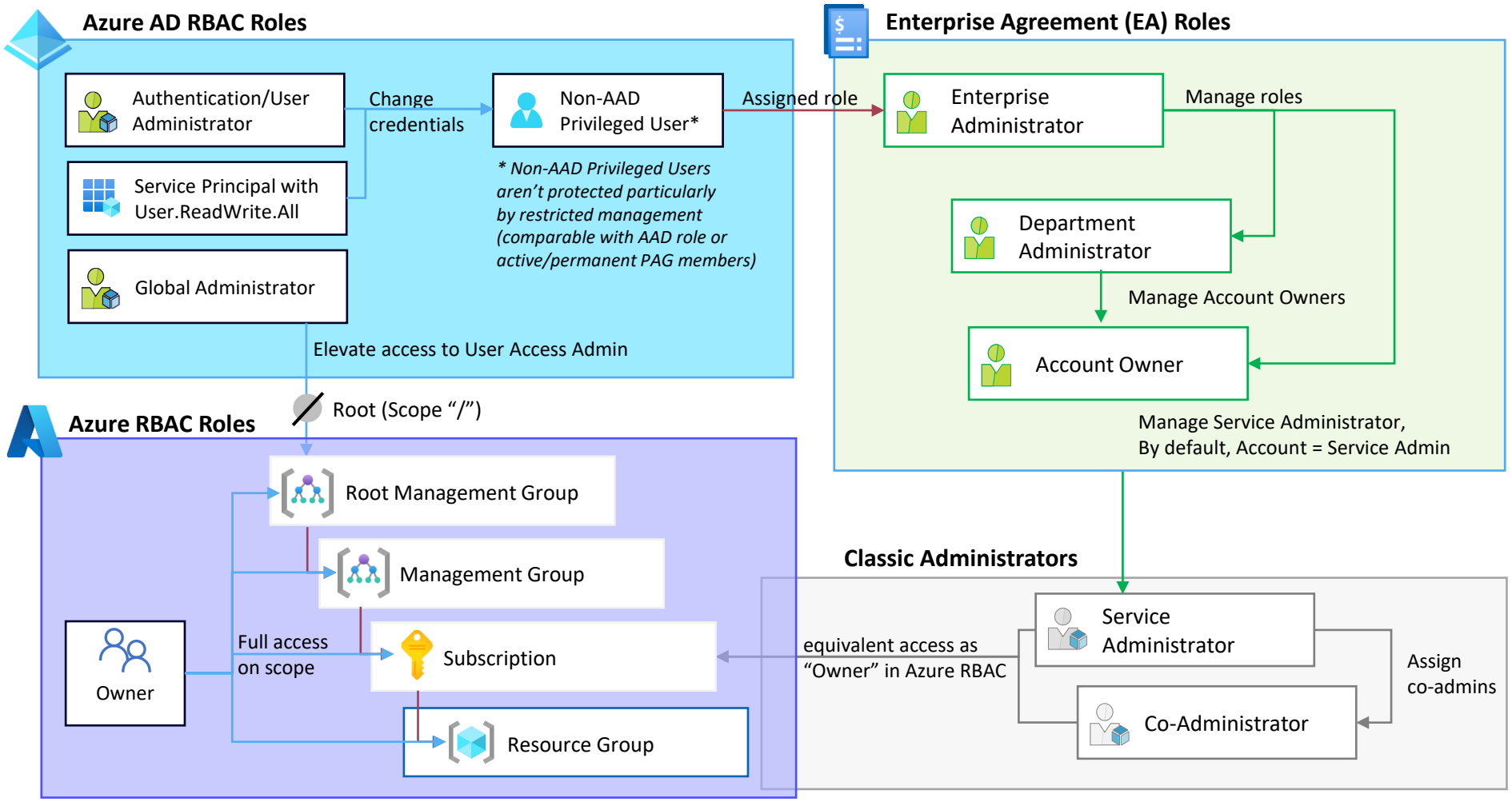
Classification of Action and Scope

```
[
    {
        "EAMTierLevelName": "ControlPlane",
        "EAMTierLevelTagValue": "0",
        "TierLevelDefinition": [
            {
                "Category": "Microsoft.Azure",
                "Service": "Management",
                "RoleAssignmentScopeName": [
                    "/",
                    "/providers/Microsoft.Management/managementGroups/36955ea9-c98e-
                    "/providers/Microsoft.Management/managementGroups/lab",
                    "/providers/Microsoft.Management/managementGroups/lab-platform",
                    "/providers/Microsoft.Management/managementGroups/lab-saezone"
                ],
                "RoleDefinitionActions": [
                    "Microsoft.Authorization/*",
                    "*"
                ]
            }
        ]
    }
]
```

Classification of Privileged Security Principal on Tier Level

```
{
  "ObjectId": "4fbcb88a-18b5-42cf-82ac-30ca6d4f6919",
  "ObjectType": "ServicePrincipal",
  "ObjectDisplayName": "azops-msi",
  "Classification": [
    {
      "AdminTierLevel": "0",
      "AdminTierLevelName": "ControlPlane",
      "Service": "Management"
    }
  ],
  "RoleAssignments": [
    {
      "RoleAssignmentId": "/providers/Microsoft.Authorization/roleAssignments/a308c801
      "RoleAssignmentScope": "/",
      "RoleAssignmentType": "Direct",
      "PIMManagedRole": "False",
      "PIMAssignmentType": "Permanent",
      "RoleDefinitionName": "Owner",
      "RoleDefinitionId": "8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
      "ObjectId": "4fbcb88a-18b5-42cf-82ac-30ca6d4f6919",
      "ObjectDisplayName": "azops-msi",
      "ObjectType": "ServicePrincipal",
      "Classification": [
        {
          "AdminTierLevel": "0",
          "AdminTierLevelName": "ControlPlane",
          "Service": "Management",
          "TaggedBy": "JSONwithAction"
        }
      ]
    }
  ]
}
```

Privileged Escalation/Access Path



Isolation of Control- and Management Plane Assets in Microsoft Azure

LIVE DEMO

THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net