



Defending Tier 0: Taking Control of Your Cloud's Control Plane

Thomas Naunheim
Cyber Security Architect
[@glueckkanja](#)



Thomas Naunheim

Cyber Security Architect @glueckkanja AG

- From Koblenz/Lahnstein, Germany
- Microsoft MVP (Identity & Access, Cloud Security)
- X: @Thomas_Live
- Blog: www.cloud-architekt.net

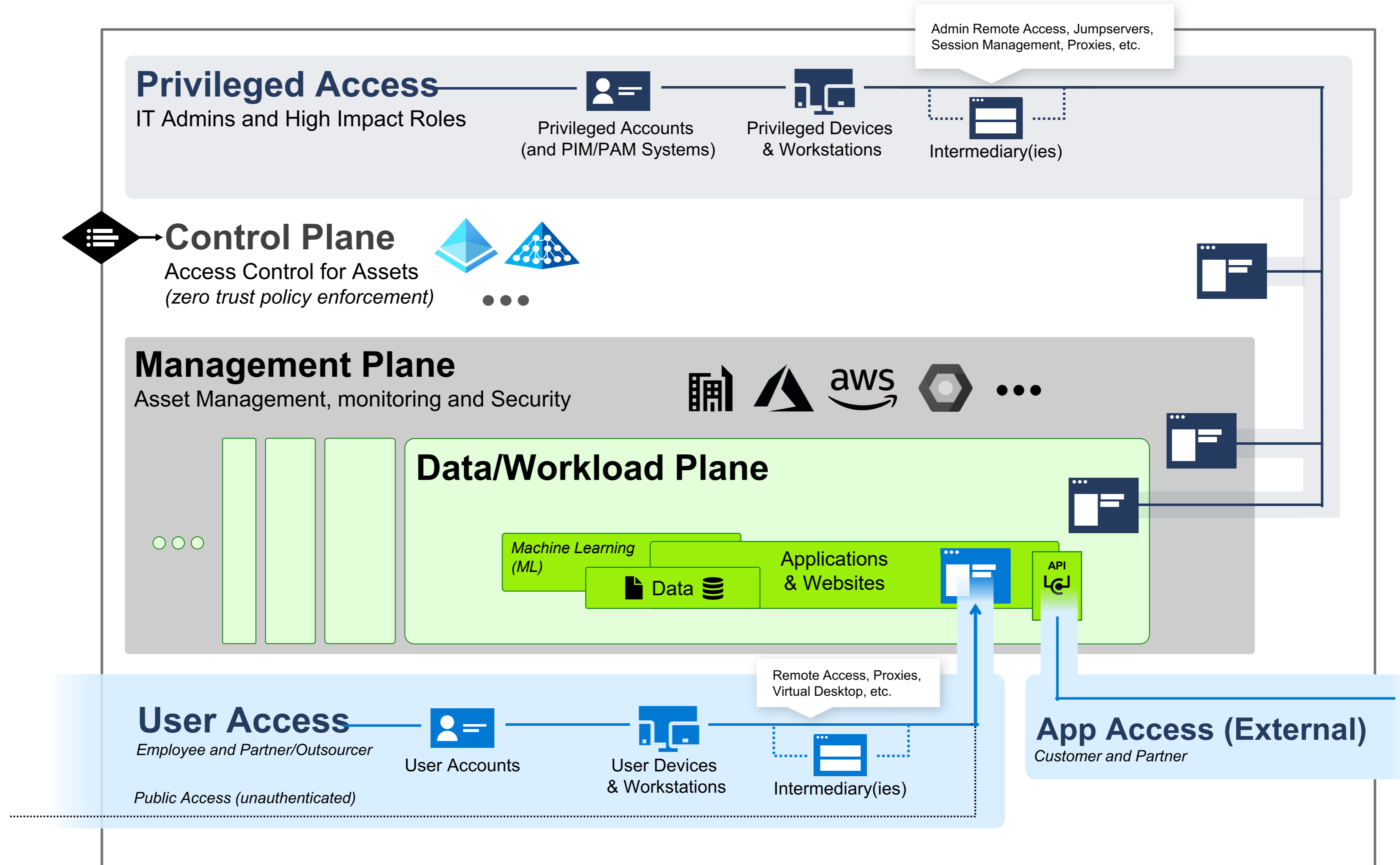


Agenda

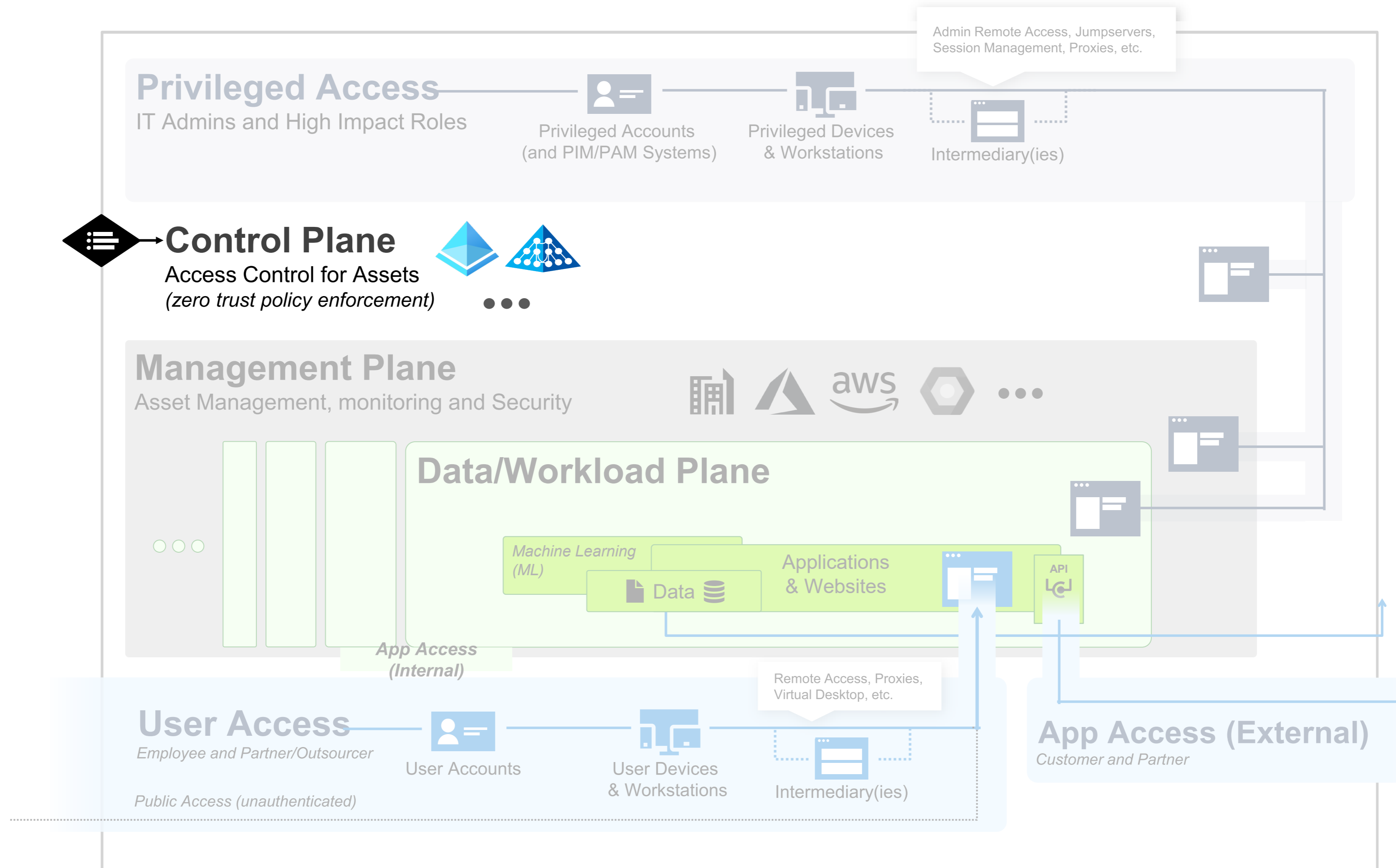
- Introduction to Microsoft Enterprise Access Model (EAM)
- Identify Control Plane (Tier 0) privileges
- Mitigation of “tier breach” and integration to ITDR
- Intra- vs. Inter-Tenant Isolation (“Red Tenant”)

Introduction to Microsoft Enterprise Access Model

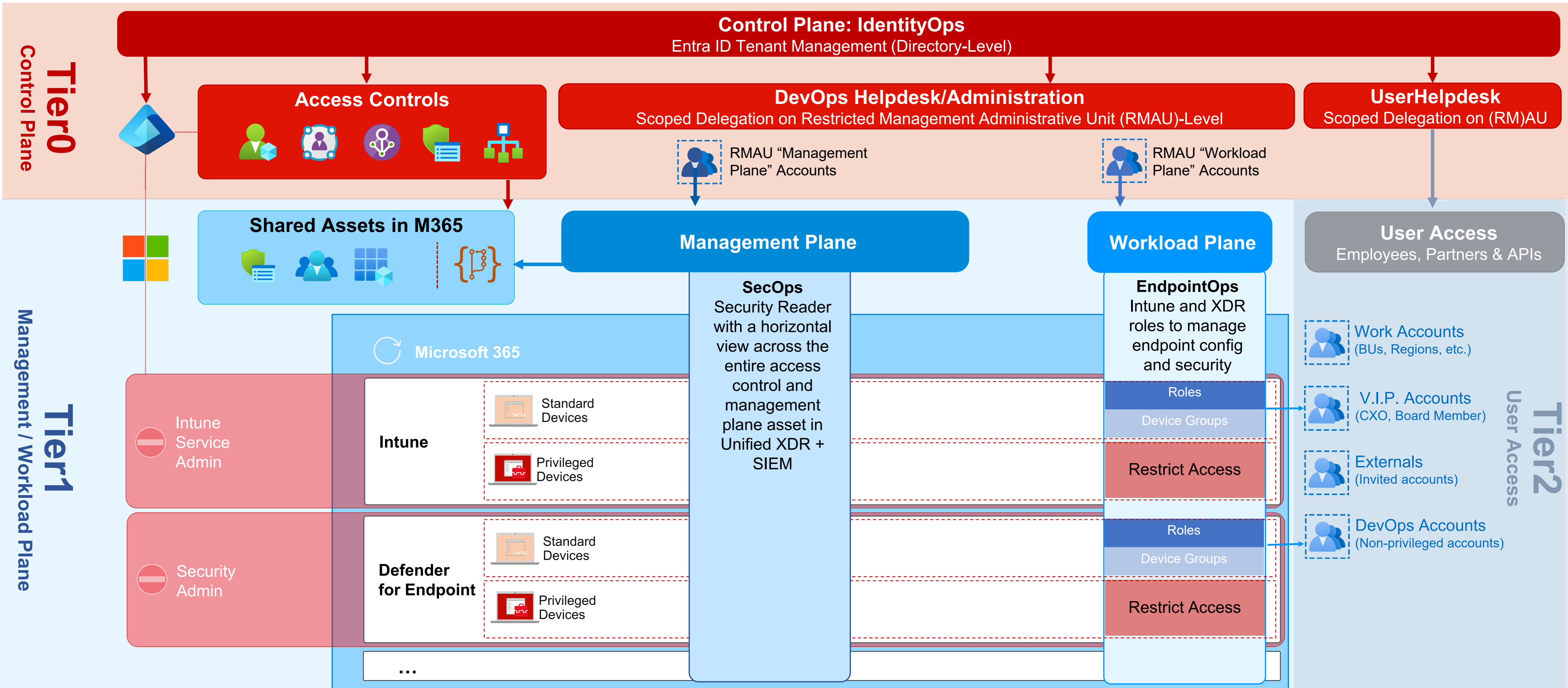
Microsoft Enterprise Access Model



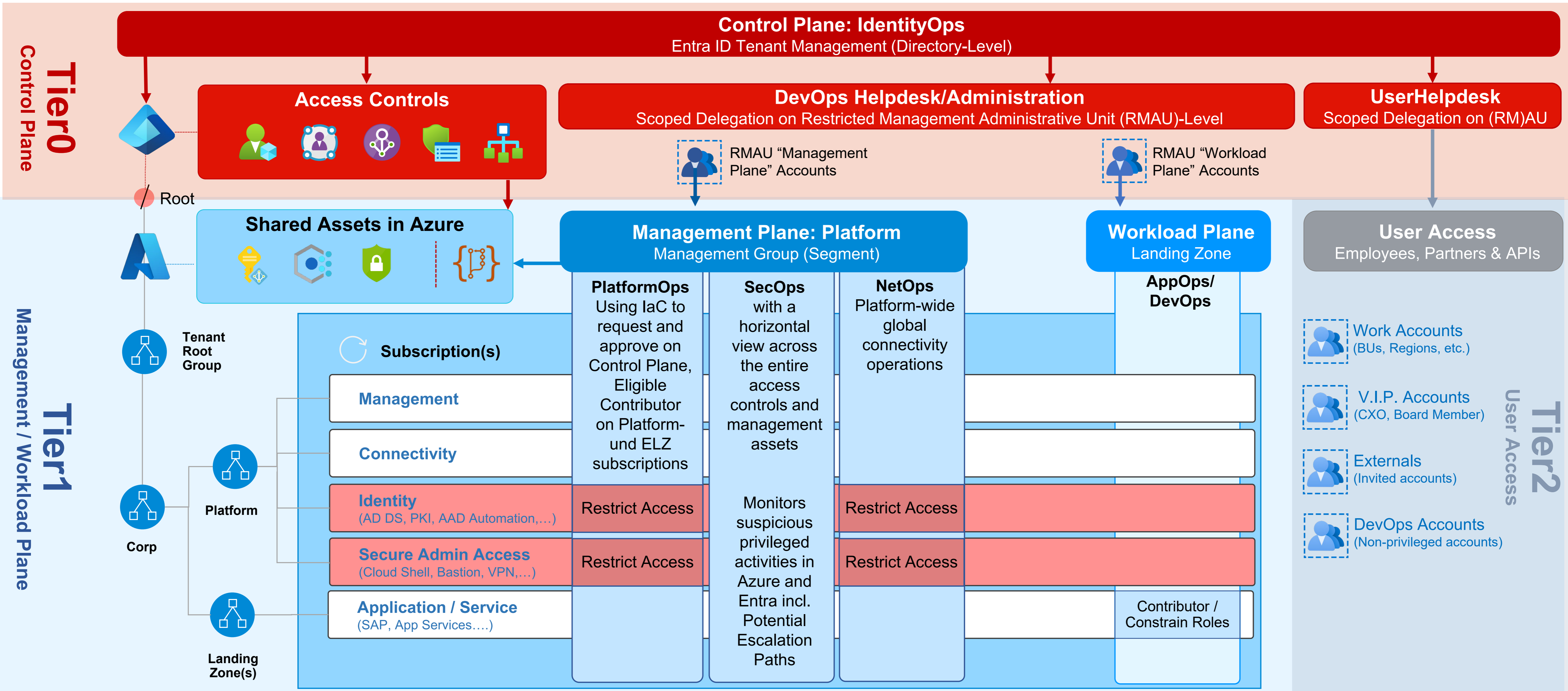
Microsoft Enterprise Access Model



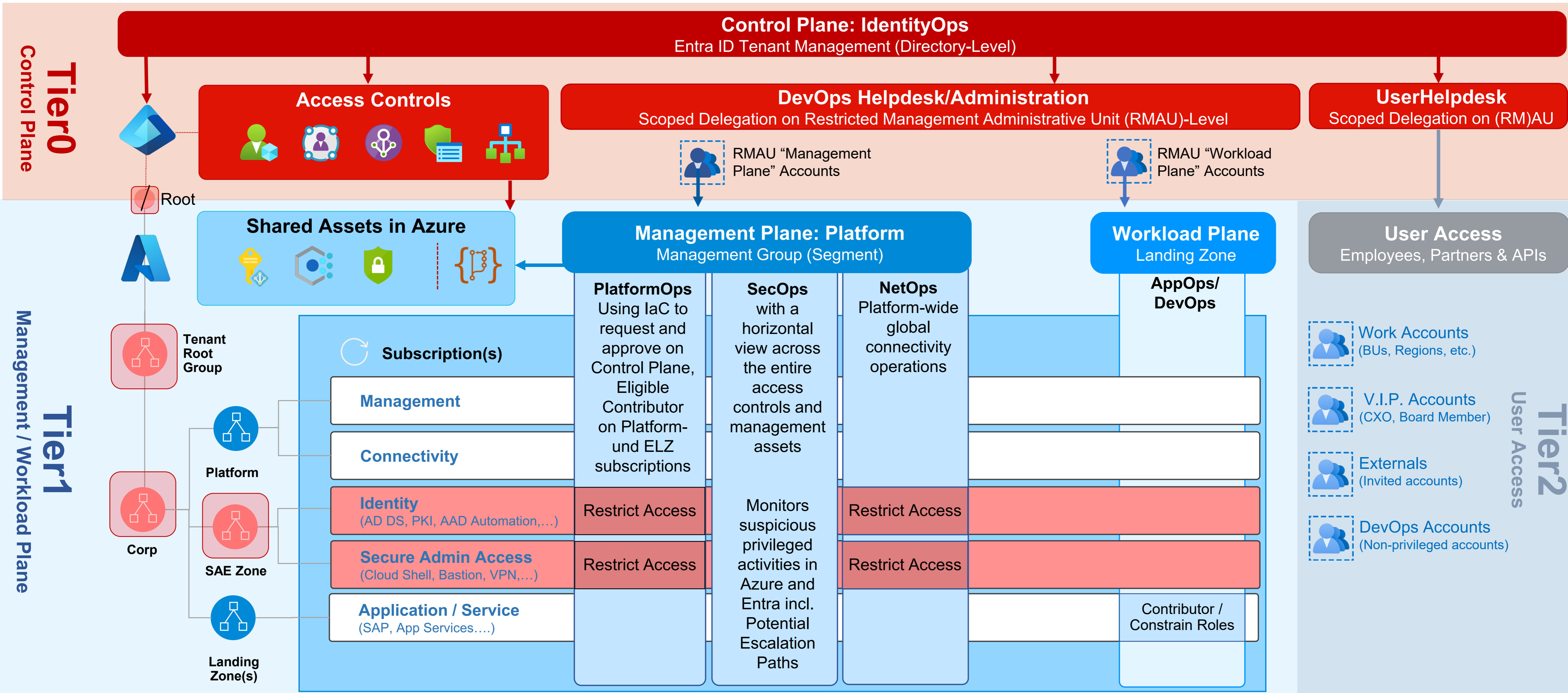
My adoption of EAM for M365 services



My adoption of EAM for Microsoft Azure



My adoption of EAM for Microsoft Azure



Owner with Role Assignment Conditions

Dashboard > Resource groups > businessapp-rg | Access control (IAM) >




Add role assignment condition - prg_Lab-Tier1.Azure.2.Business-AppOps

/subscriptions/53a56f38-edca-4db2-add6-8fbd44a0be0d/resourceGroups/businessapp-rg/providers/Microsoft.Authorization/roleAssignments/f6659d9a-1ca0-404b-a6ee-b354349d6

Select a condition template. [Learn more](#)


Constrain roles

- Allow user to only assign roles you select

 Configure

Constrain roles and principal types

- Allow user to only assign roles you select
- Allow user to only assign these roles to principal types you select (users, groups, or service principals)

 Configure

Constrain roles and principals

- Allow user to only assign roles you select
- Allow user to only assign these roles to principals you select

 Configure

Configured

Allow

Constrain roles and principals

Roles

+ Add role

Website Contributor

Storage Account Contributor

Storage Account Backup Contributor

Storage Account Key Operator Service Role

Storage Blob Data Contributor

Storage Blob Data Owner

Storage Blob Delegator

Storage Blob Data Reader

Storage Table Data Contributor

Storage Table Data Reader

Principals

+ Add principals

prg_Lab-Tier1.Azure.2.Business-AppOps

businessapp

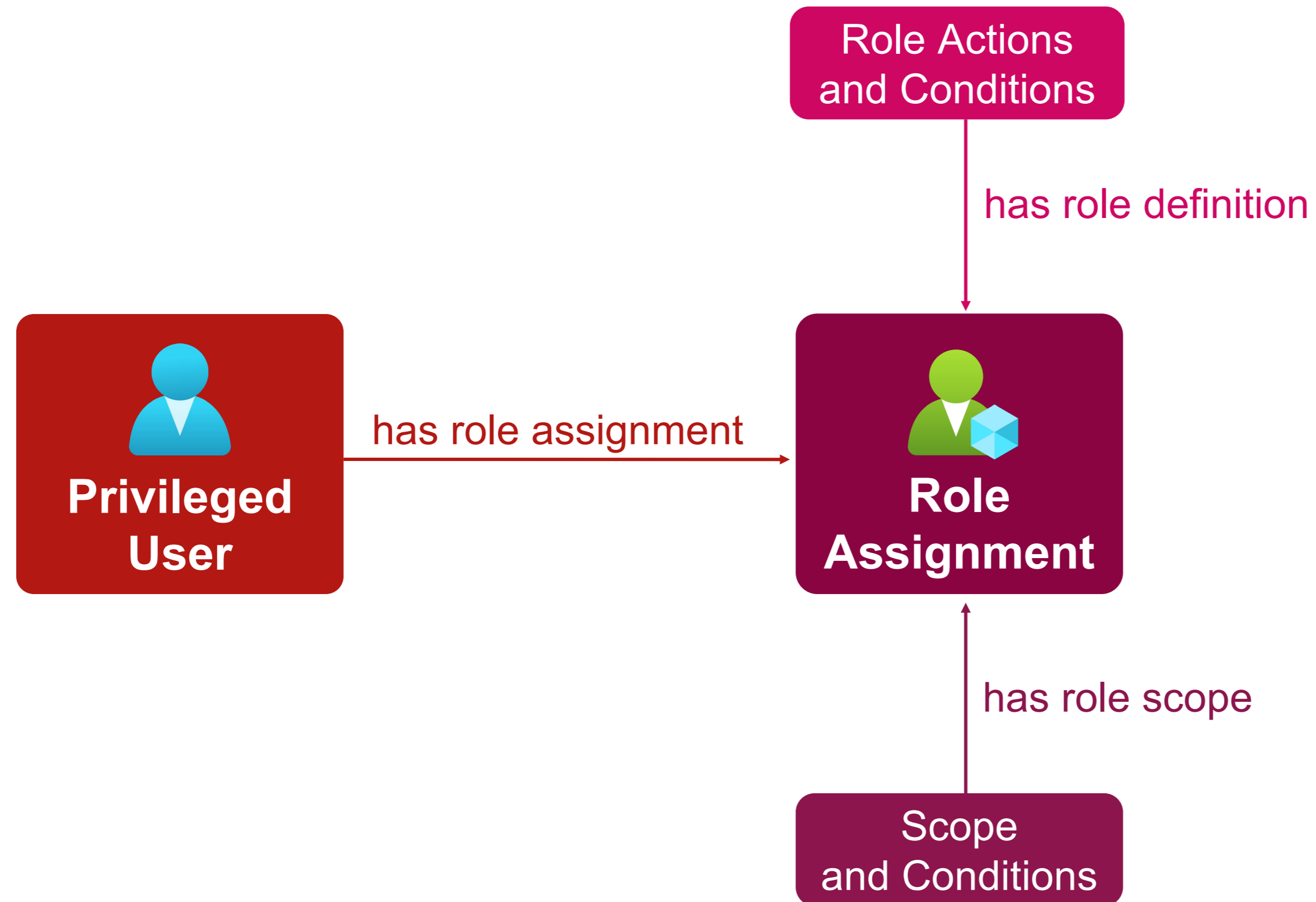
BusinessApp-Auth-WebAPI

[Reset condition templates](#)

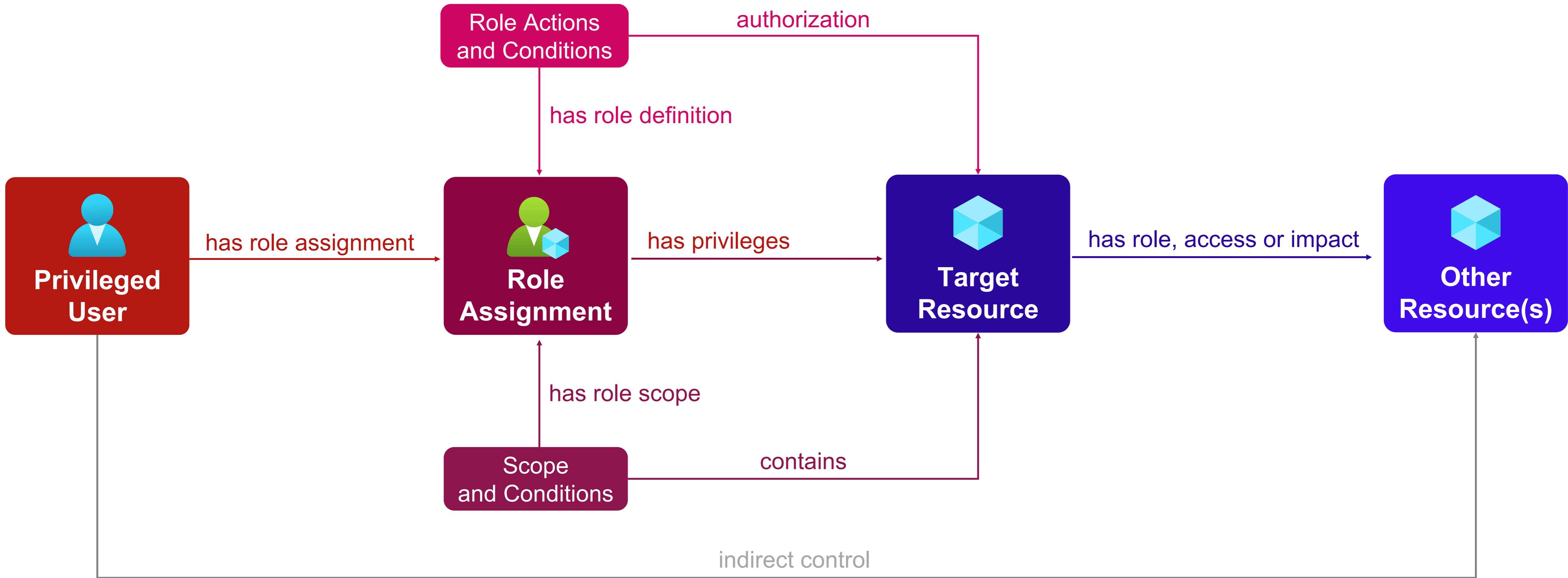
[Open advanced condition editor](#)

Identify Control Plane (Tier 0)

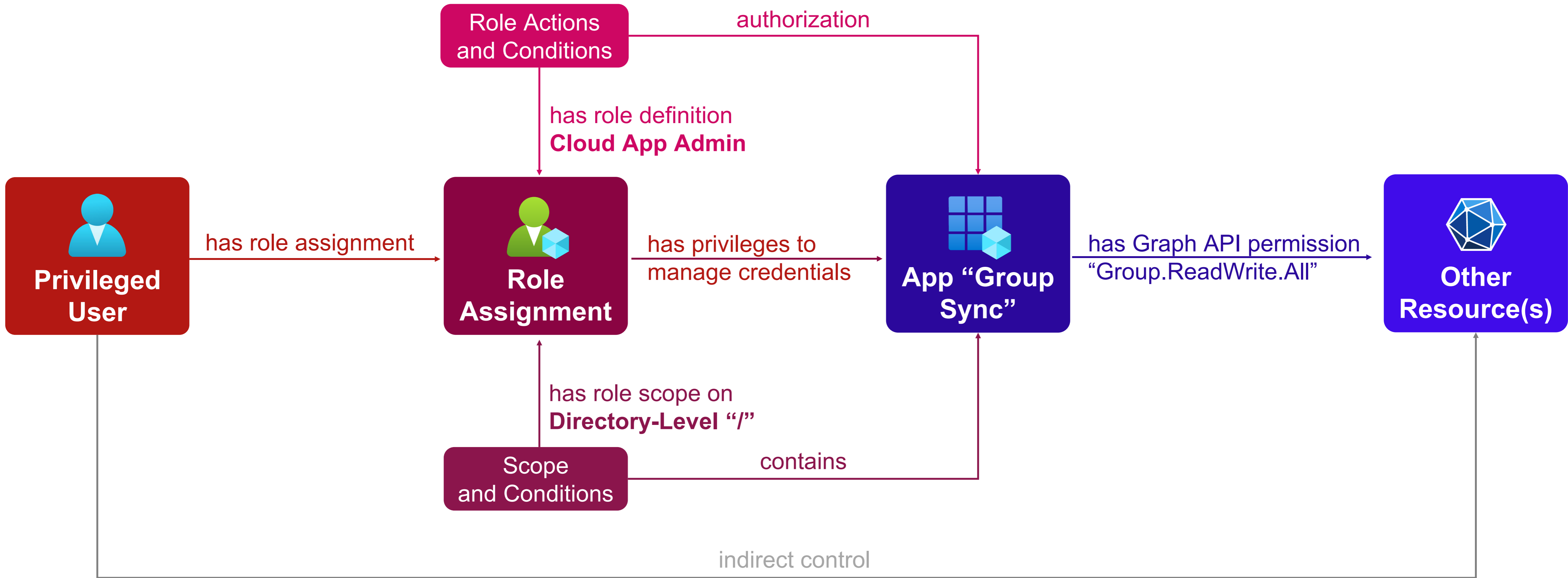
Delegation and Control Relationship



Transitive Control Relationship

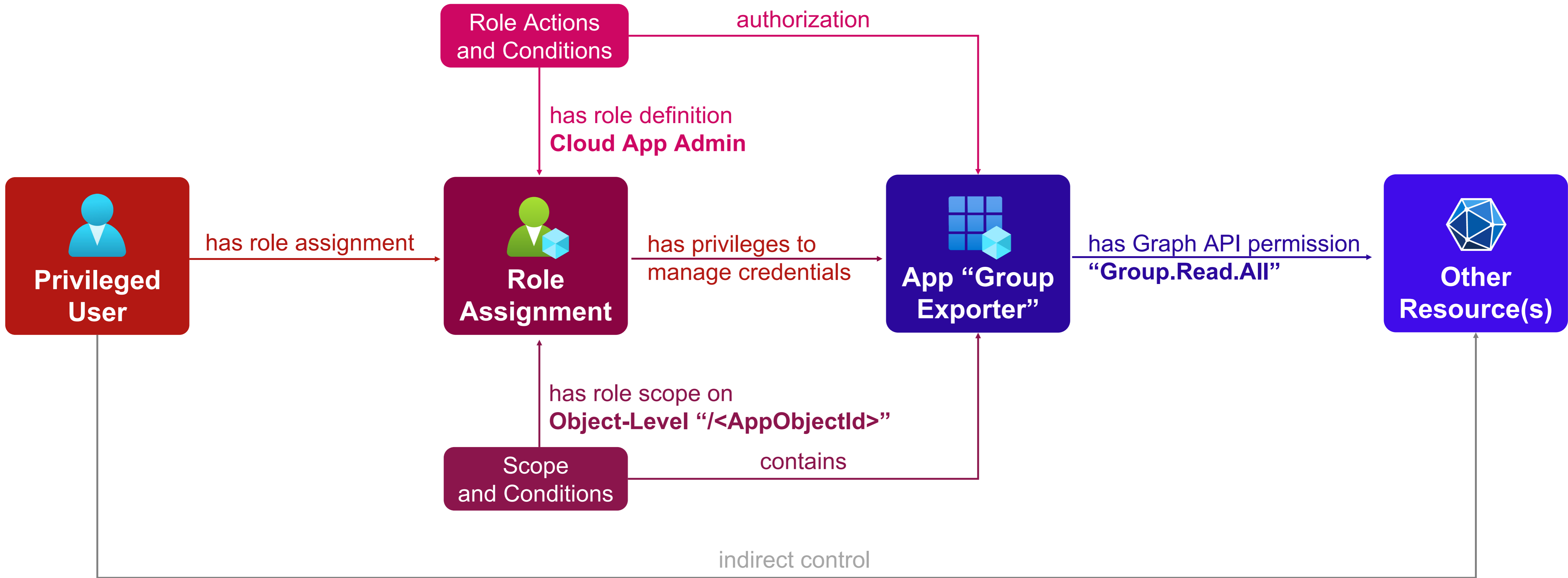


Transitive Control Relationship



Workload with Control Plane Access?

Transitive Control Relationship



Workload with User Access

Definition by Actions and Scopes

```
"EAMTierLevelName": "ControlPlane",  
"EAMTierLevelTagValue": "0",  
"TierLevelDefinition": [  
  {  
    "Category": "Microsoft.AzureAD",  
    "Service": "Privileged User Management",  
    "RoleAssignmentScopeName": [  
      "/",  
      "/administrativeUnits/<AzureAdmin>",  
      "/administrativeUnits/<M365Admin>"  
    ],  
    "RoleDefinitionActions": [  
      "microsoft.directory/users/authenticationMethods/create",  
      "microsoft.directory/users/authenticationMethods/delete",  
      "microsoft.directory/users/authenticationMethods/basic/update",  
      "microsoft.directory/users/create",  
      "microsoft.directory/users/disable",  
      "microsoft.directory/users/delete",  
      "microsoft.directory/users/enable",  
      "microsoft.directory/users/basic/update",  
      "microsoft.directory/users/manager/update",  
      "microsoft.directory/users/userPrincipalName/update",  
      "microsoft.directory/users/invalidateAllRefreshTokens",  
      "microsoft.directory/users/restore",  
      "microsoft.directory/users/password/update"  
    ]  
  }  
]
```

Applied Classification by EAM Definition

Definition of Actions and Scope

Classified Privileged Access of User

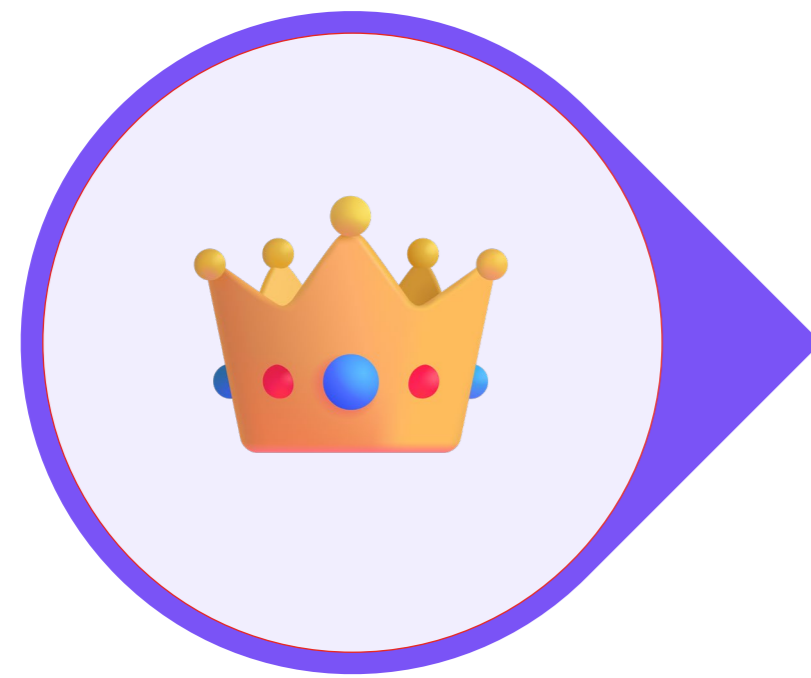
```

"EAMTierLevelName": "ControlPlane",
"EAMTierLevelTagValue": "0",
"TierLevelDefinition": [
  {
    "Category": "Microsoft.AzureAD",
    "Service": "Privileged User Management",
    "RoleAssignmentScopeName": [
      "/",
      "/administrativeUnits/<AzureAdmin>",
      "/administrativeUnits/<M365Admin>"
    ],
    "RoleDefinitionActions": [
      "microsoft.directory/users/authenticationMethods/create",
      "microsoft.directory/users/authenticationMethods/delete",
      "microsoft.directory/users/authenticationMethods/basic/update",
      "microsoft.directory/users/create",
      "microsoft.directory/users/disable",
      "microsoft.directory/users/delete",
      "microsoft.directory/users/enable",
      "microsoft.directory/users/basic/update",
      "microsoft.directory/users/manager/update",
      "microsoft.directory/users/userPrincipalName/update",
      "microsoft.directory/users/invalidateAllRefreshTokens",
      "microsoft.directory/users/restore",
      "microsoft.directory/users/password/update"
    ]
  }
]
  
```

```

"ObjectId": "ControlPlane",
"ObjectType": "0",
"ObjectDisplayName": "0",
"Classification": [
  {
    "AdminTierLevel": "Microsoft.AzureAD",
    "AdminTierLevelName": "User Management",
    "Service": "Privileged User Management",
  },
],
"RoleAssignments": [
  "RoleAssignmentId": "18160c44-b052-45b3-9874-0f289d1d6cb4",
  "RoleAssignmentScopeId": "/administrativeUnits/<AzureAdmin>",
  "RoleAssignmentScopeName": "Tier0-ControlPlane.1.DevOps",
  "RoleAssignmentType": "Direct",
  "PIMAssignmentType": "Eligible",
  "RoleDefinitionName": "User Administrator",
  "RoleDefinitionId": "fe930be7-5e62-47db-91af-98c3a49a38b1",
  "RoleType": "BuiltinRole",
  "Classification": [
    {
      "AdminTierLevel": "0",
      "AdminTierLevelName": "ControlPlane",
      "Service": "Privileged User Management",
      "TaggedBy": "JSONwithAction"
    }
  ]
]
  
```


Steps to adopt Enterprise Access Model



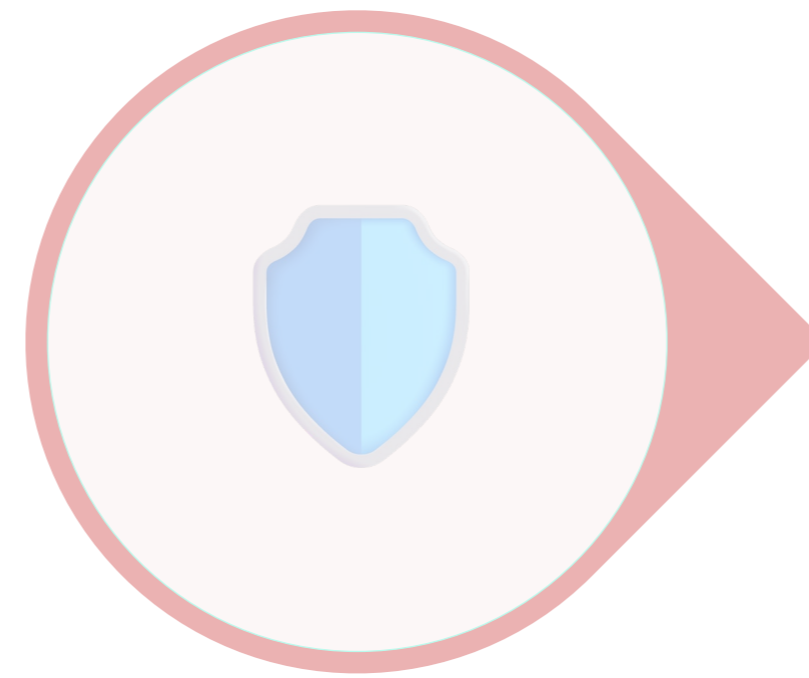
Classify

Adjusted classification template including critical scopes for your environment

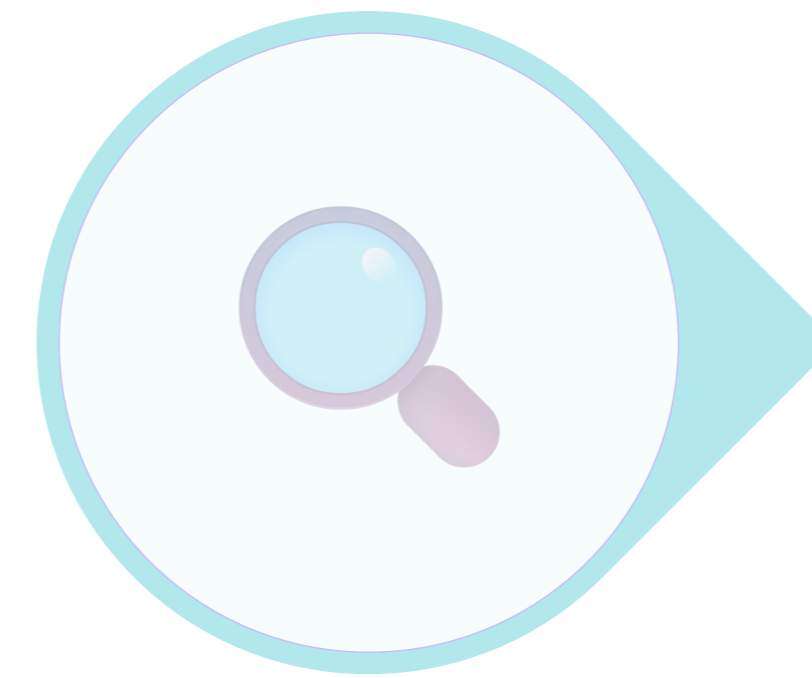


Identify

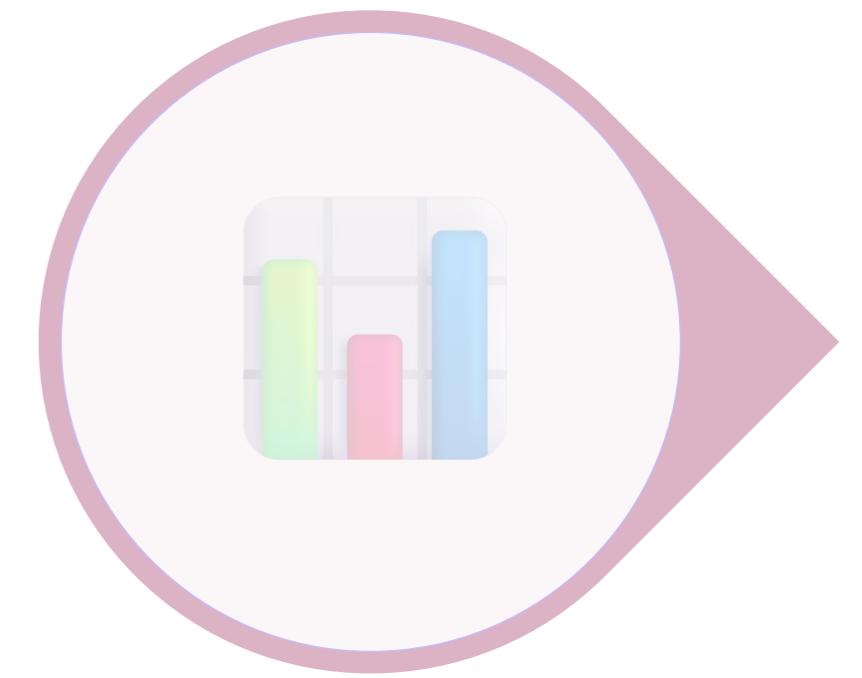
Analyze role assignments and apply classification on roles and principals



Protect



Monitor



Reporting

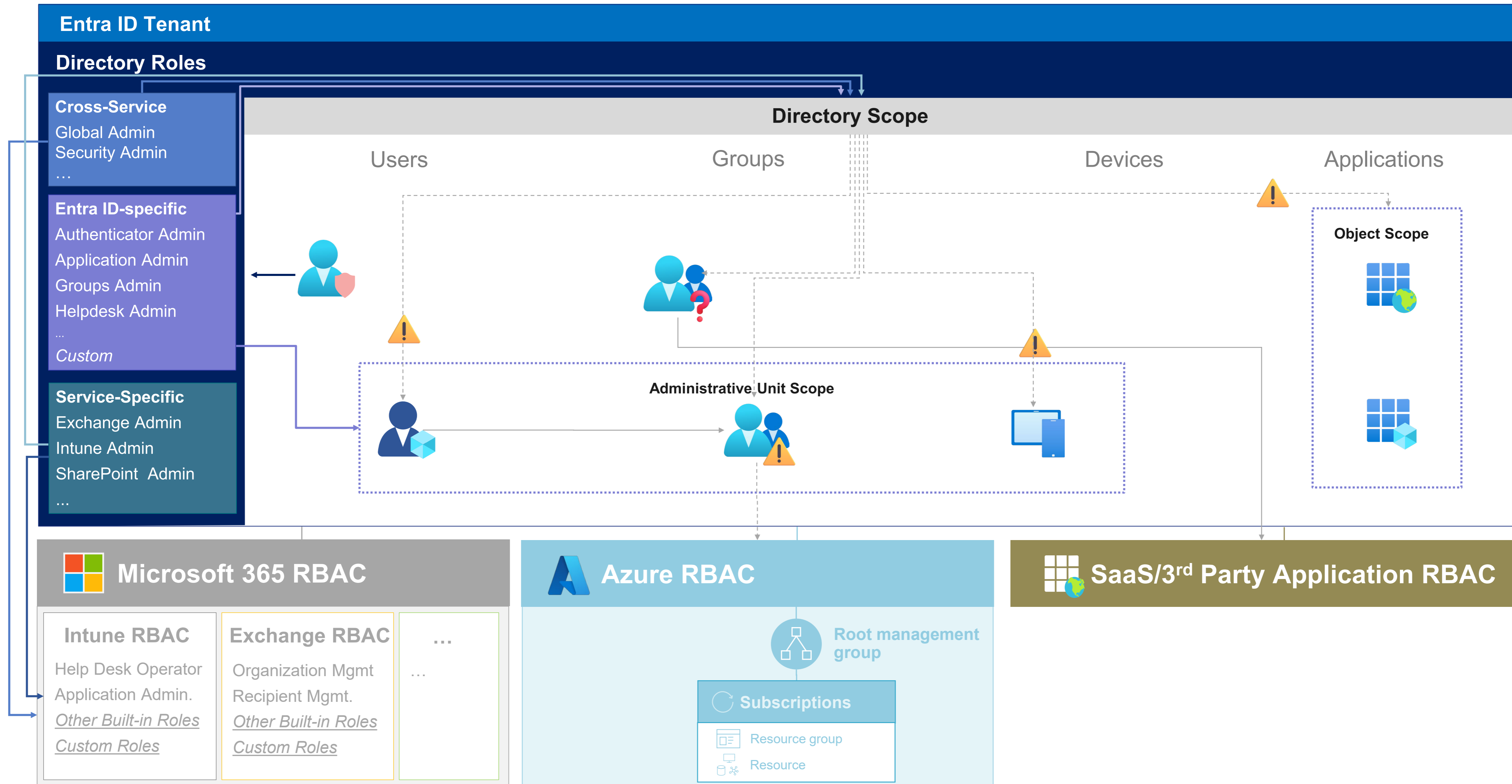


EntraOps Classification Demo

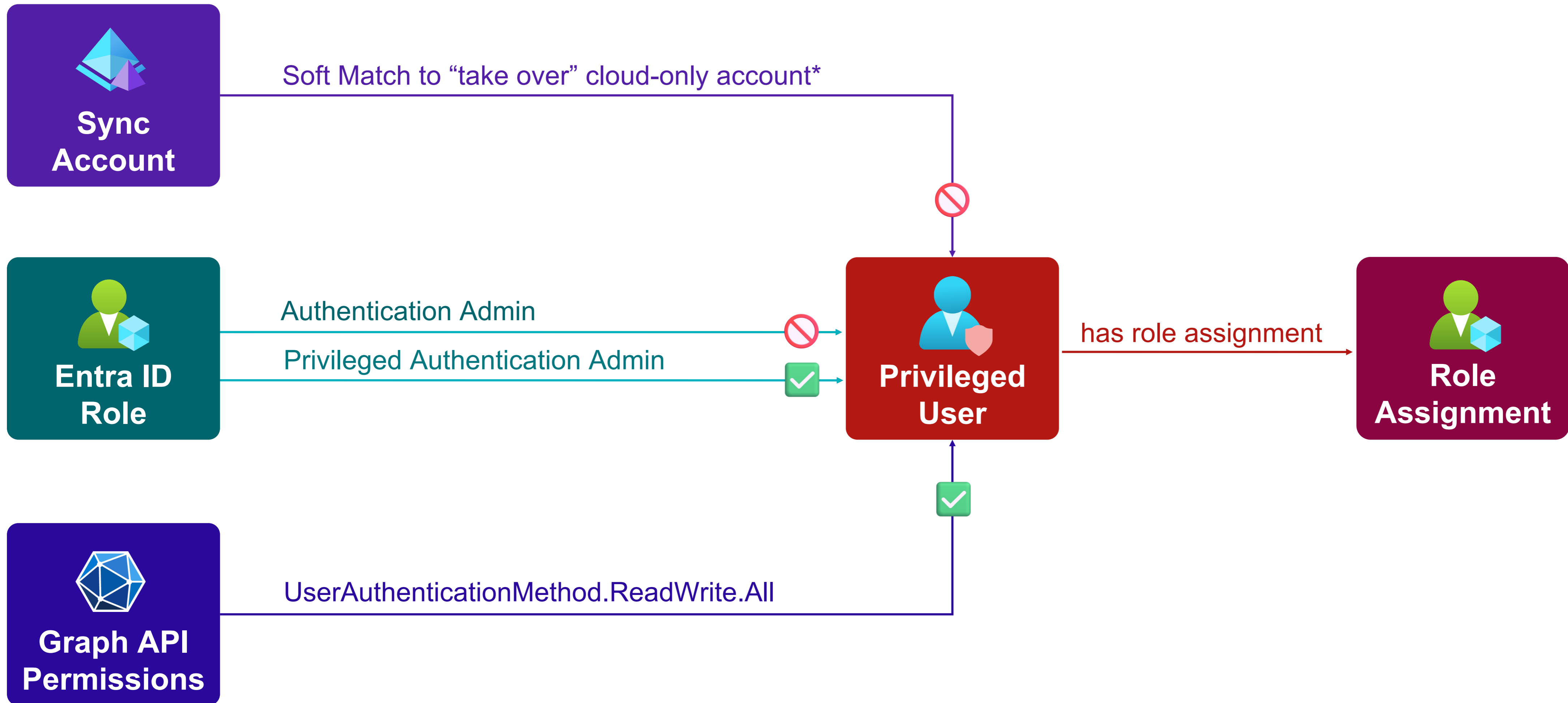
- Customizing classification templates manually or enriched by external data sources
- Identify Control Plane assets by applied classification

Mitigation of “tier breach” and integration to ITDR

Service-specific and scoped roles

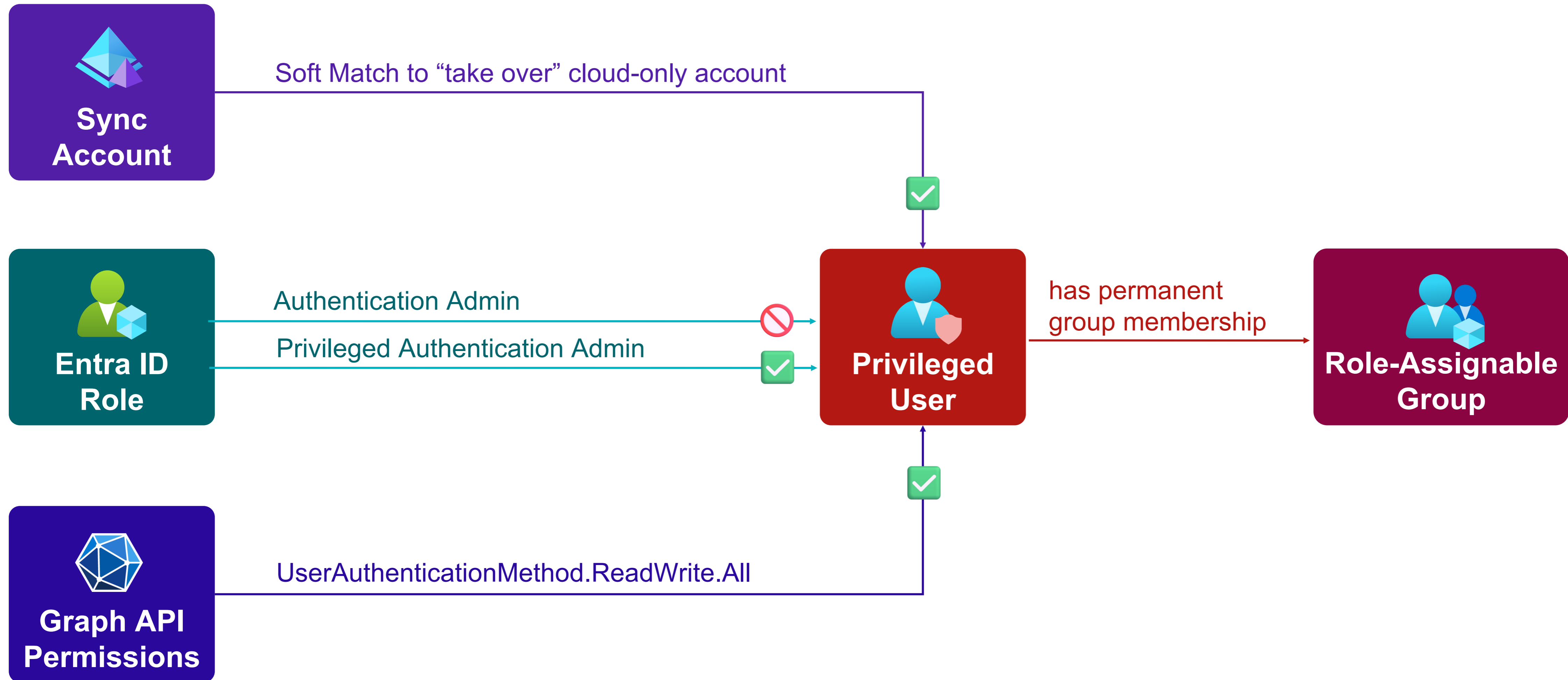


Protection of high-privileged users by eligible/permanent Entra ID role assignment

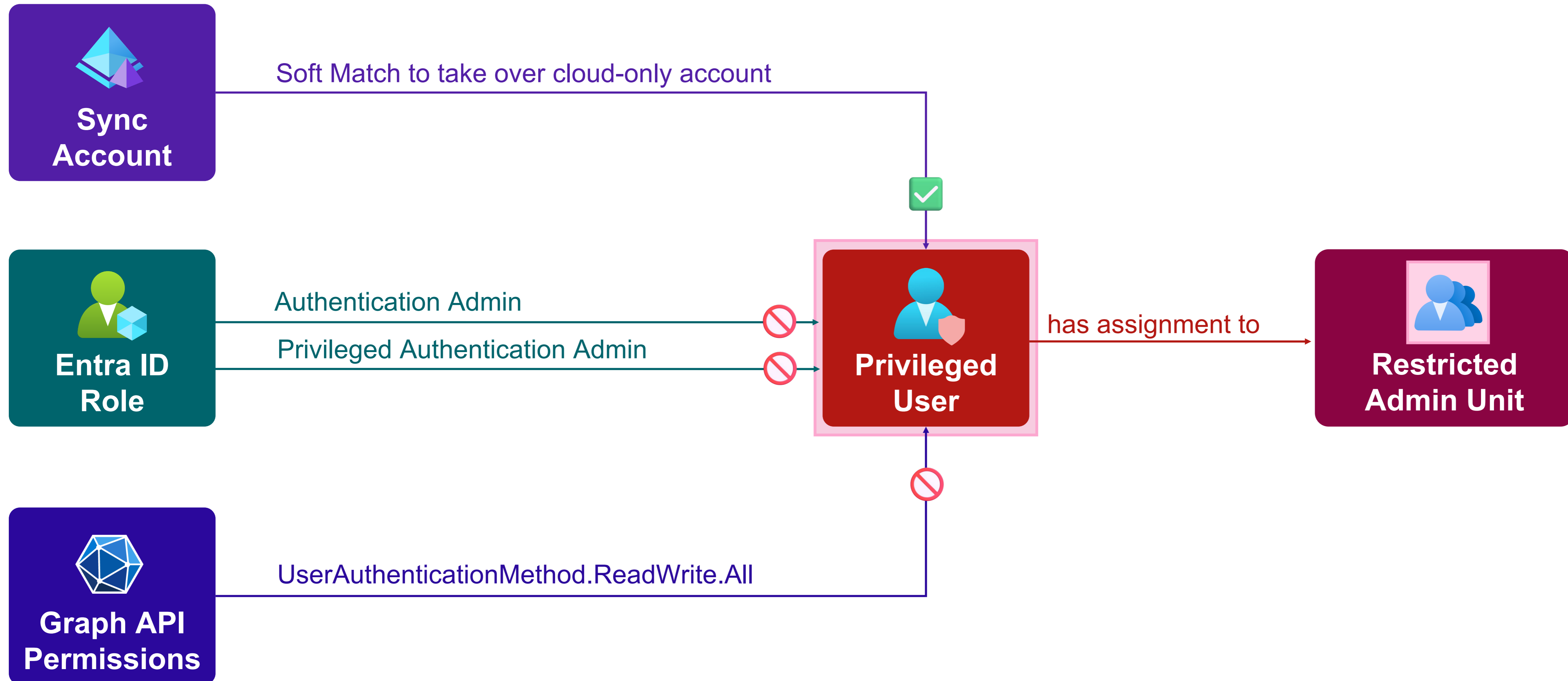


* only by permanent role assignments

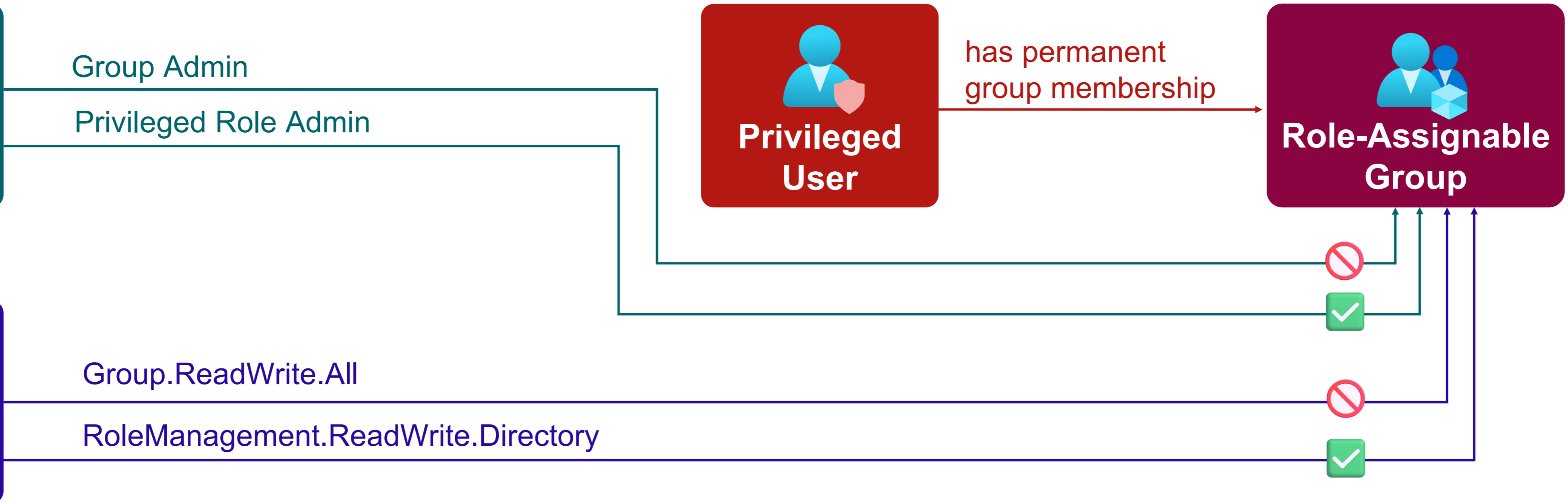
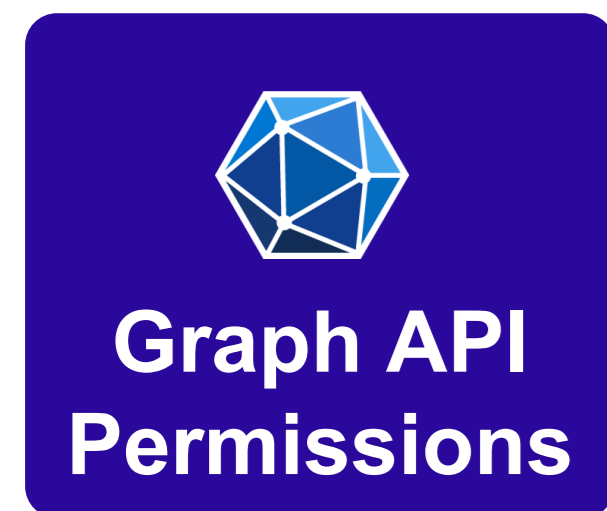
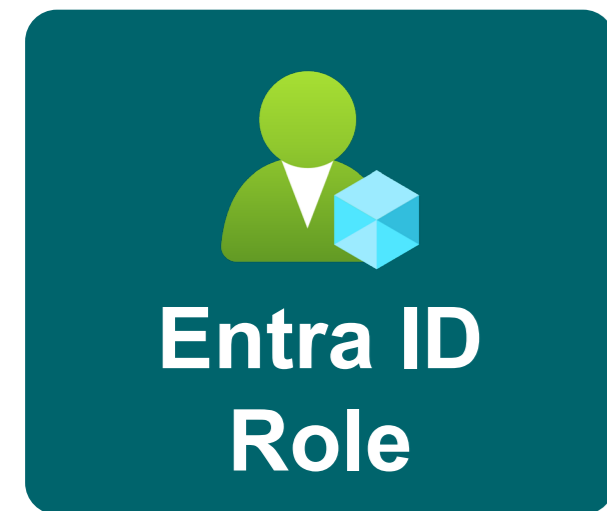
Role-assignable groups (RAG) to implement persona-based “role groups”



Protect sensitive users from directory-scoped roles by RMAUs



Role-assignable groups (RAG) to implement persona-based “role groups”



Protect sensitive groups from directory-scoped roles by RMAUs

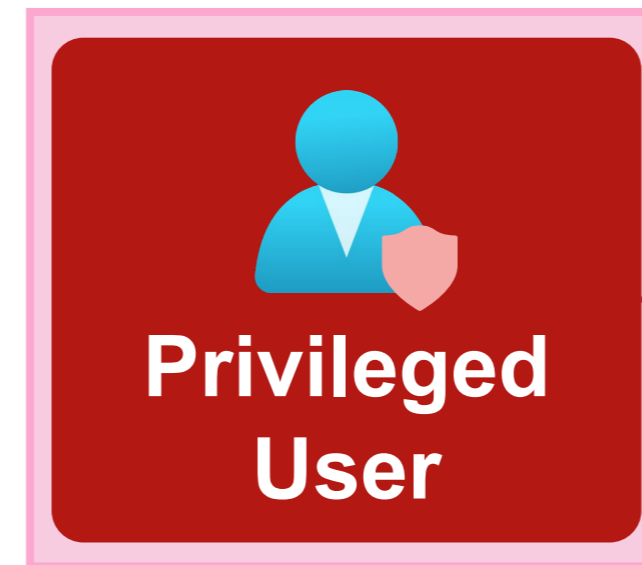


Group Admin

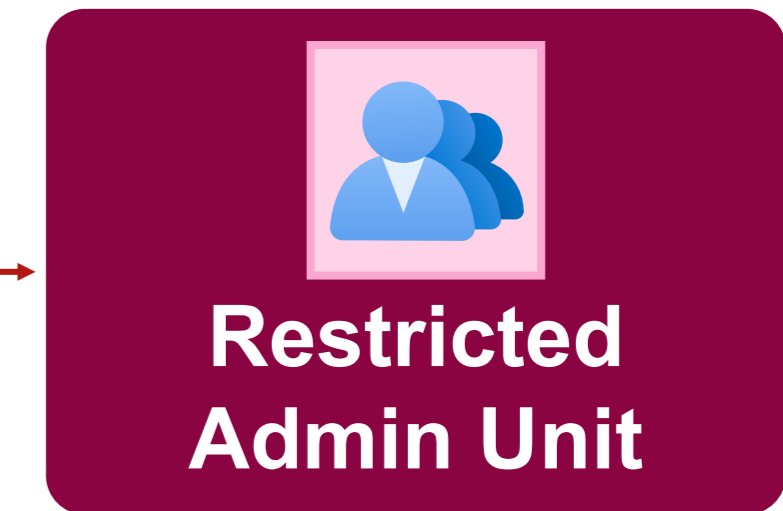
Privileged Role Admin

Group.ReadWrite.All

RoleManagement.ReadWrite.Directory



has membership to





(Known) limitations on RMAU

First Party Apps will be also blocked

Identity Governance, PIM for Groups (MS-PIM)

Limited availability on scoped (RM) AU directory roles

e.g., Privileged Role Admin not available for managing RAGs

No support for Application and Service Principals objects

Directory-scoped (Cloud) App Admins and Owner cannot be restricted

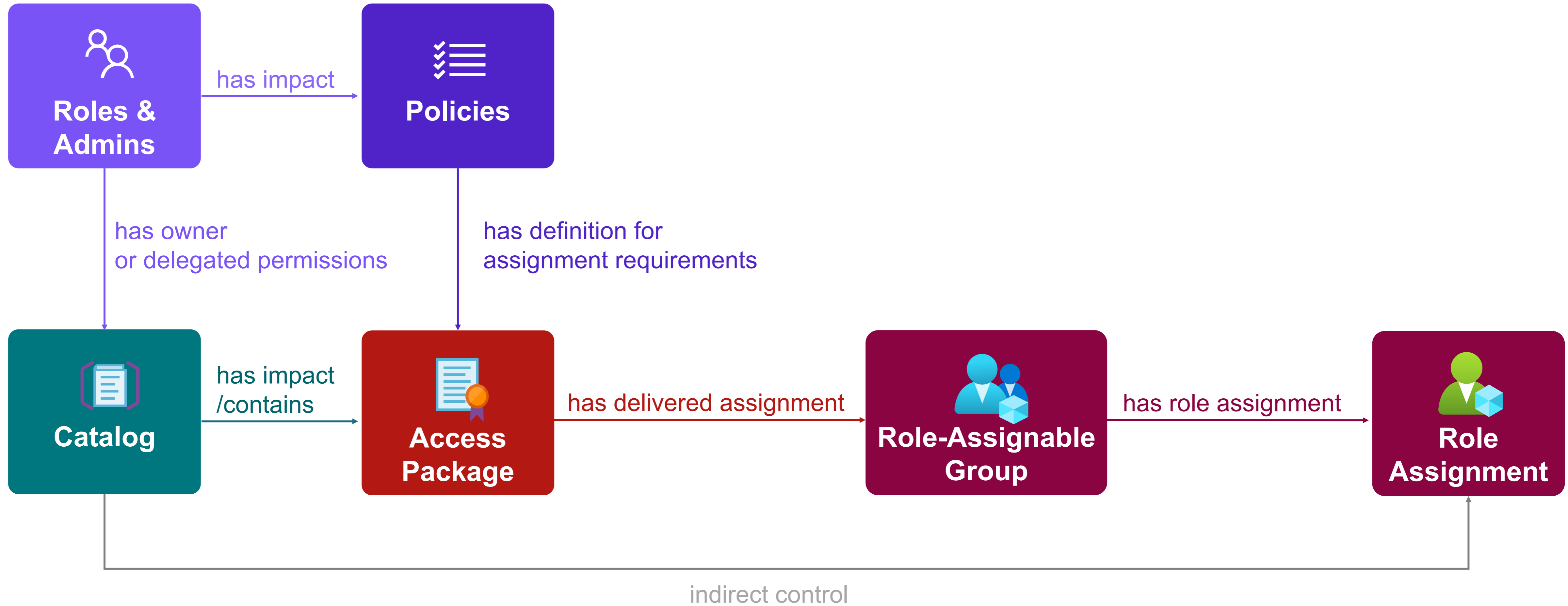
Remove RMAU assignments with Graph API App roles

AdministrativeUnit.ReadWrite.All grant permissions to manage RMAU

Capability matrix for restricted management

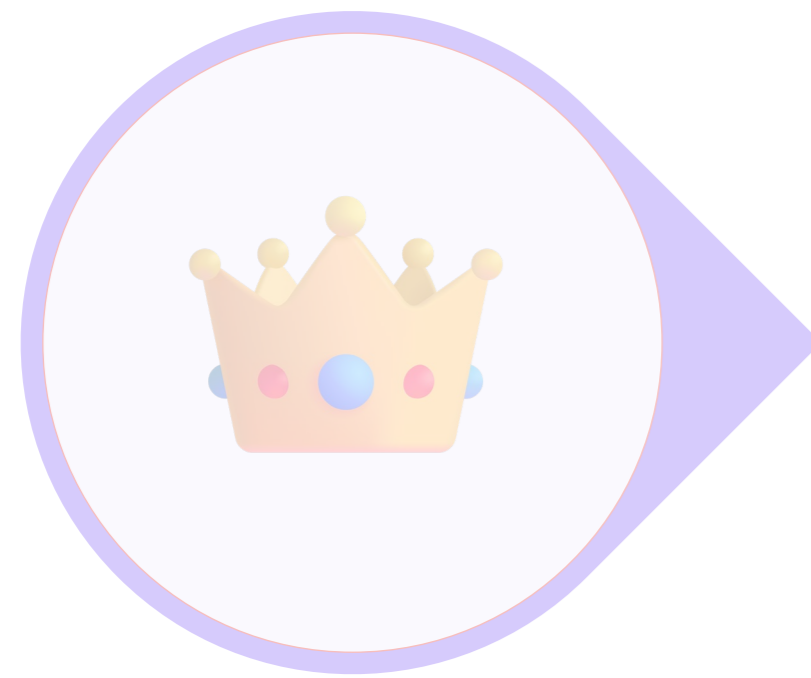
	Restricted Management by High-Privileged Roles	Restriction applies to group members	Support for Identity Governance	Preferred use case/scenario
Security Group without PIM	✗ No restriction on directory-scoped roles or object owners	✗ No restriction	✓ Assignment by Access Packages	Assignments to “User Access” when avoiding directory-level delegations
Security Group in Restricted AU	✓ RMAU-scoped Admins, Blocks modification by Owner and Graph API Permissions	✗ No restriction	⚠ No RMAU support for Access Packages	Assignment to sensitive groups (e.g., Conditional Access Exclusion)
Security Group with PIM for Groups	✗ No restriction on directory-scoped roles or object owners	✗ No restriction	✓ Support for eligible assignments by Access Packages	Just-In-Time Access outside of Azure and Entra ID RBAC when avoiding directory-level delegations
Security Group with PIM for Groups in RMAU	✓ RMAU-scoped Admins, Blocks modification by Owner and Graph API Permissions	✗ No restriction	⚠ No RMAU support for PIM and Access Packages	No valid use case because of missing support for PIM/Identity Governance
Role-Assignable Security Group	✓ GA, Privileged Role Admin, Owners, RoleManagement.-ReadWrite.Directory	✓ Restricted to GA and Privileged Auth. Admin when active/permanent member	✓ Assignments by PIM for Groups and Access Packages	Assigning Entra ID roles (or other Control Plane/high-privileges), limit of 500 role-assignable group objects
Role Assignable Security Group in RMAU	✓ RMAU-scoped Admins, Blocks modification by Owner and Graph API Permissions	✓ Restricted to Privileged Auth. Admin on RMAU-level	⚠ No RMAU support for PIM and Access Packages	No valid use case because of missing RMAU-scope role for delegation

Avoid delegations on Access Packages



Control Plane Access

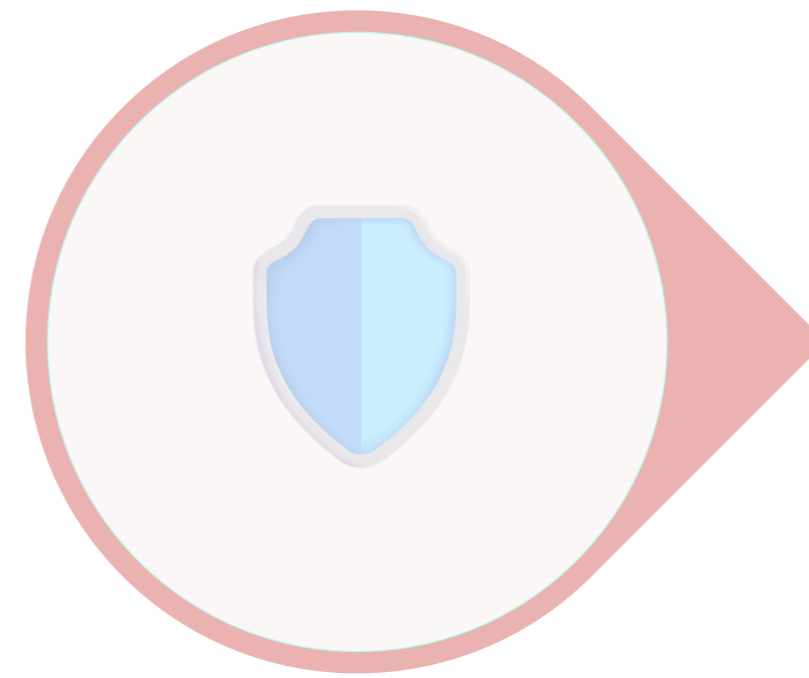
Steps to adopt Enterprise Access Model



Classify

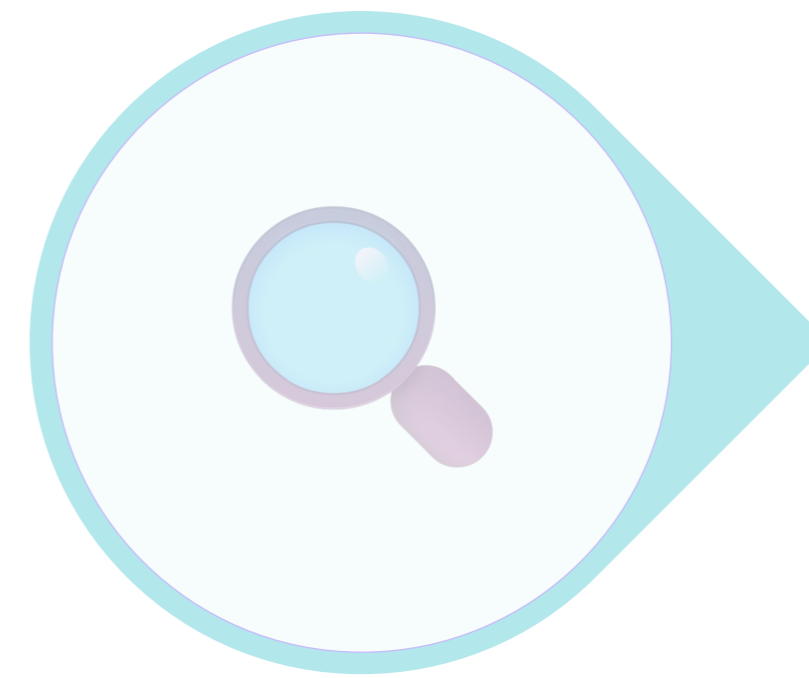


Identify



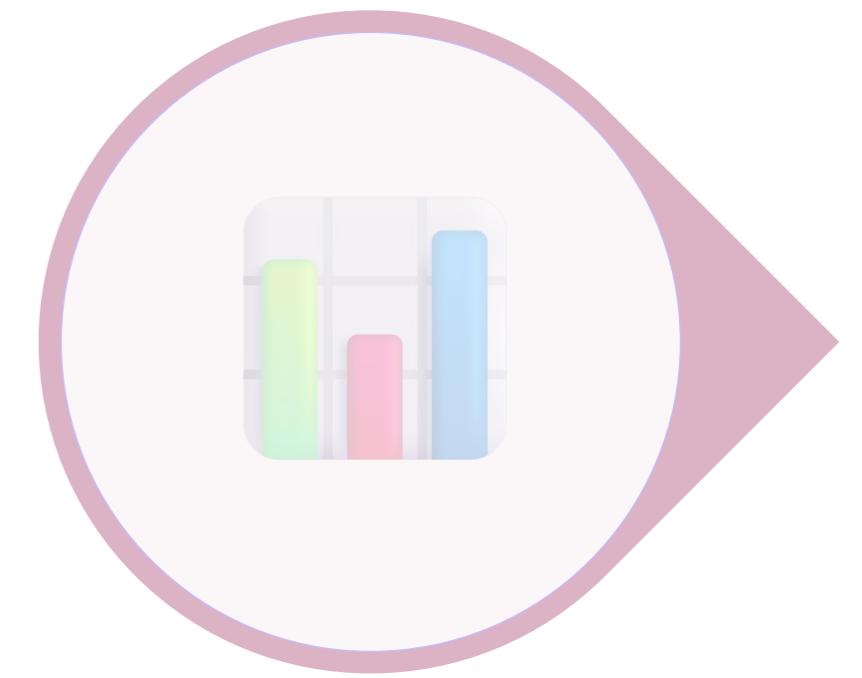
Protect

Apply protection on privileged assets to apply restricted management and advanced Conditional Access coverage



Monitor

Ingest classification data to XDR/SIEM for monitoring on privileged assets & entity enrichment



Reporting

Tracking security posture and attack paths correlation with other signals and data sources

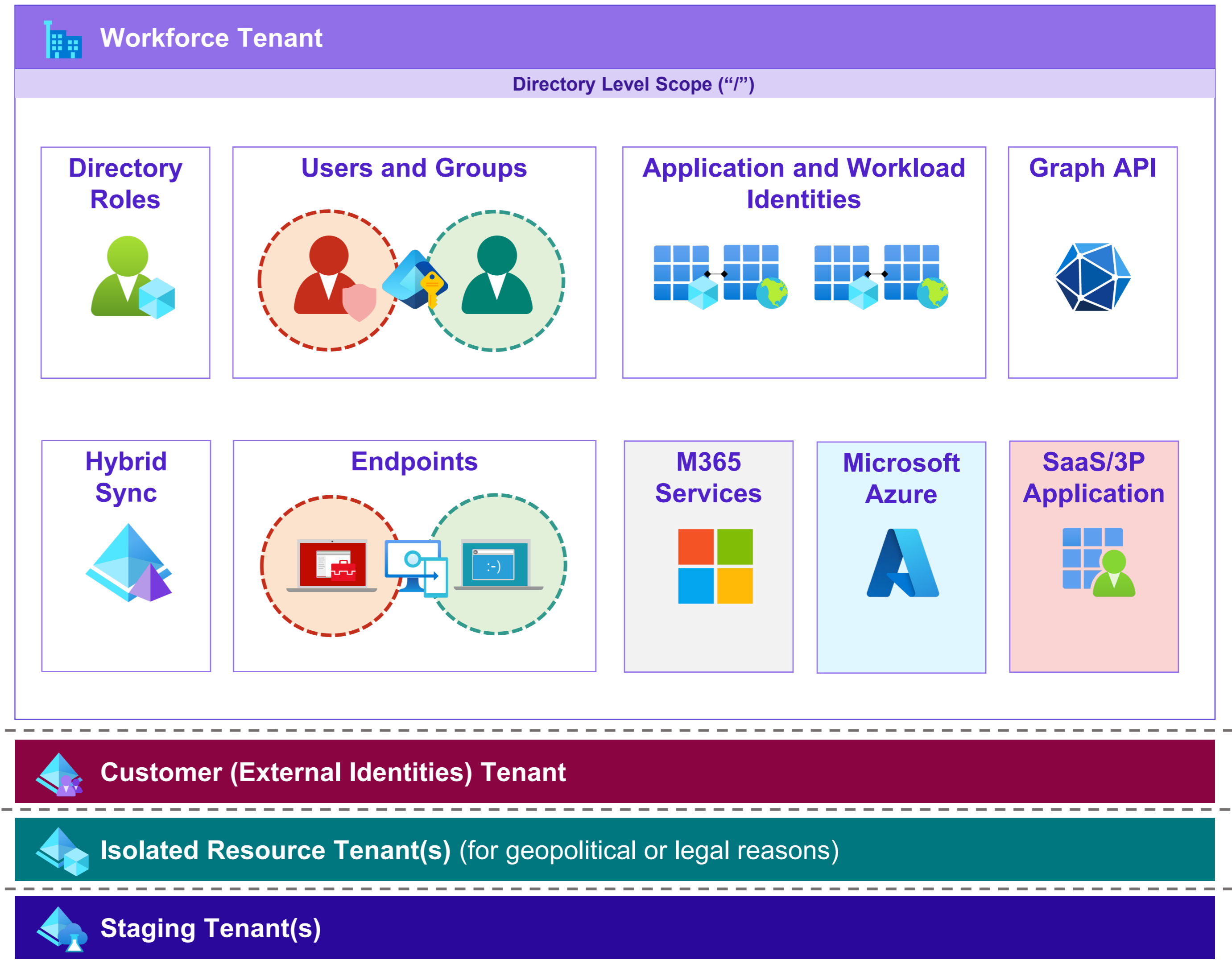


SOC Enrichment and Integration to ITDR

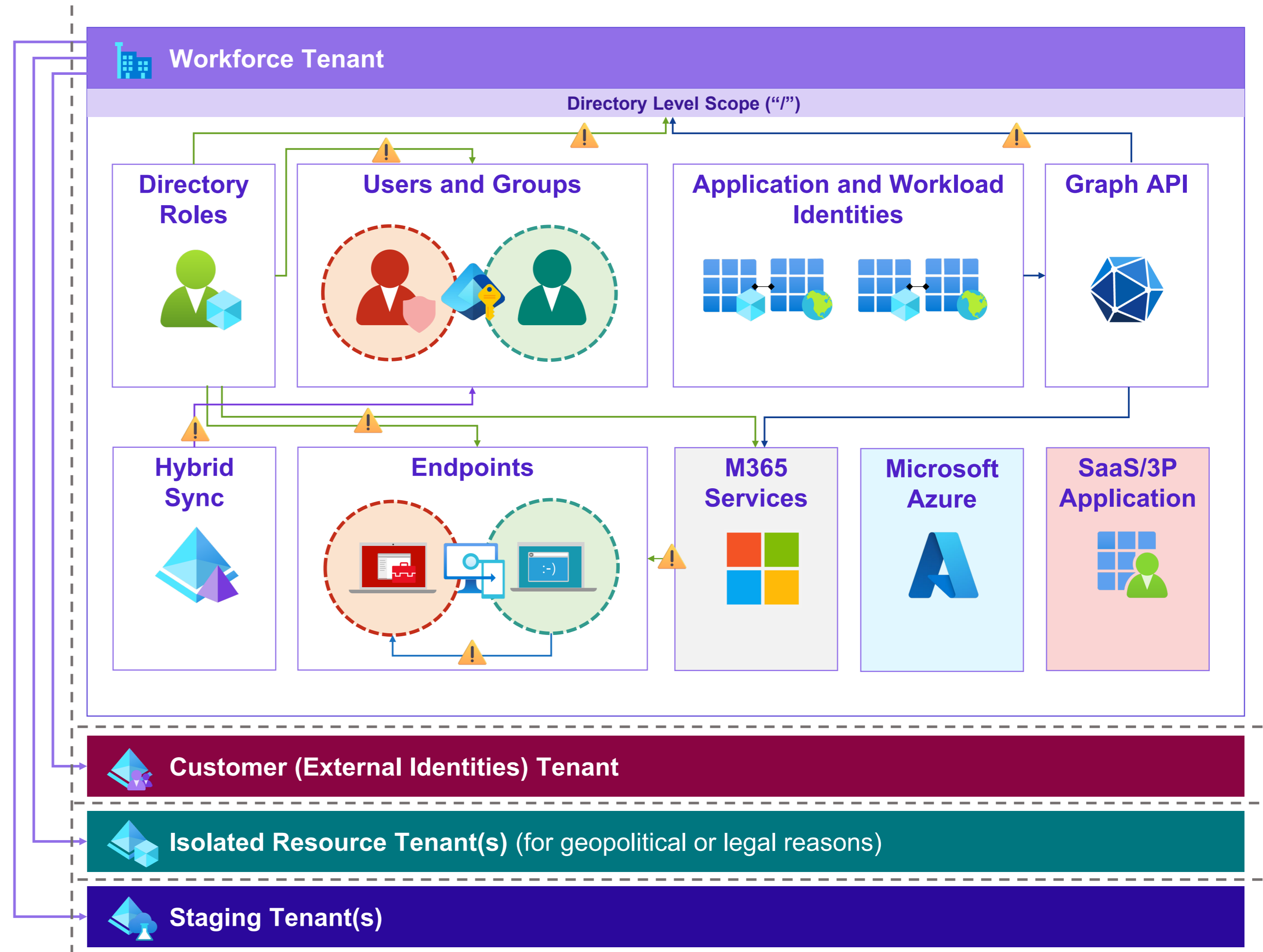
- Apply protection on Control Plane users and coverage in Conditional Access
- Identify “tier breach” by using analytics rules and workbooks

Intra- vs. Inter-Tenant Isolation (“Red Tenant”)

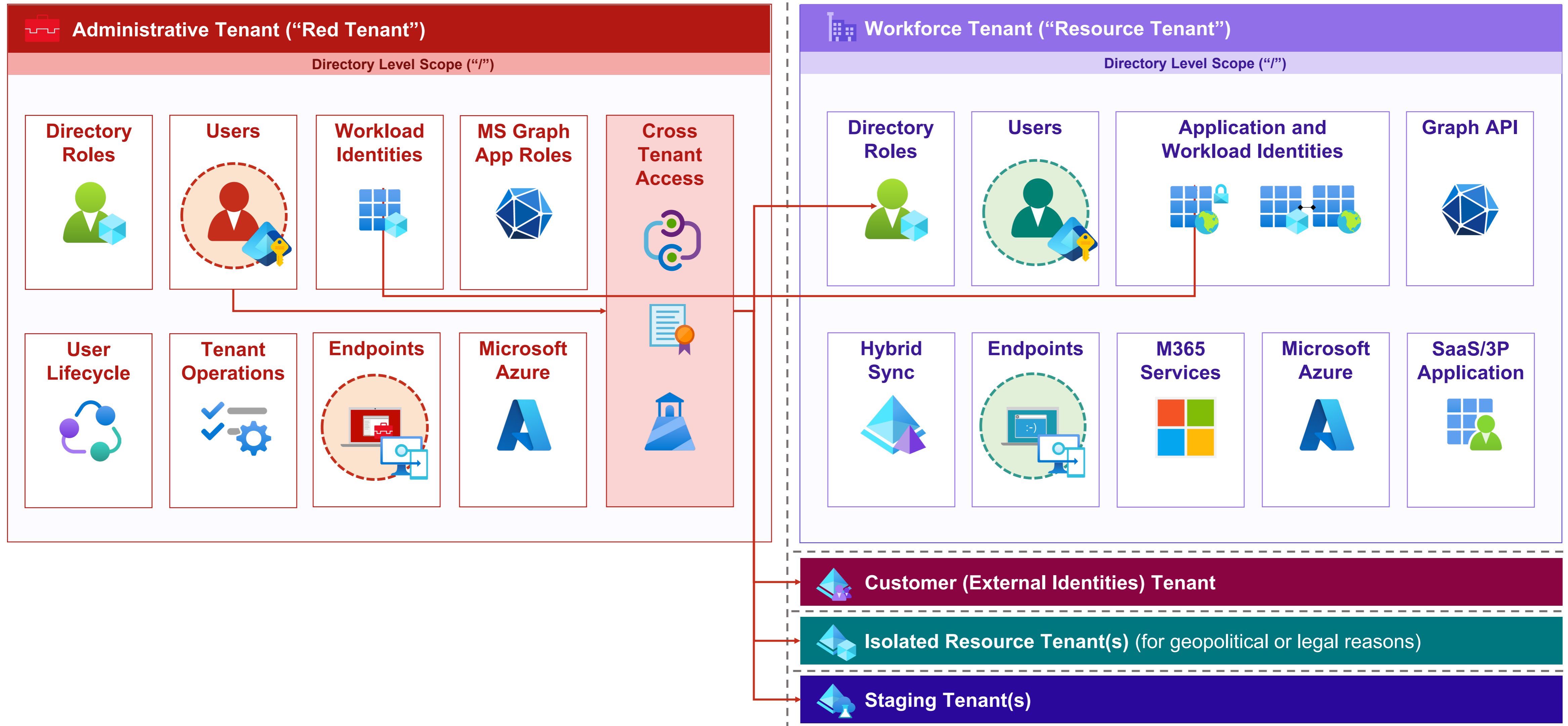
Intra-Tenant Isolation



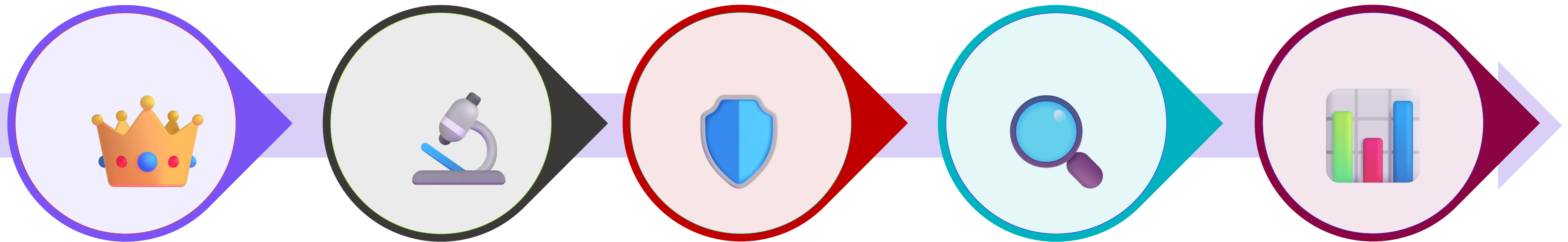
Intra-Tenant Isolation



Inter-Tenant Isolation by “Red Tenant”



Steps to adopt Enterprise Access Model



Classify

Adjusted classification template incl. critical scopes for your environment

Identify

Analyze role assignments and apply classification on roles and principals

Protect

Apply protection on privileged assets to apply restricted management and Conditional Access coverage

Monitor

Ingest classification data to XDR/SIEM for monitoring on privileged assets & entity enrichment

Reporting

Tracking security posture and attack paths correlation with other signals and data sources

Questions?