



TIER BREAKERS

BLIND SPOTS IN CLOUD-MANAGED PAWS



Thomas Naunheim
Cyber Security Architect
@glueckkanja AG



Martin Sohn Christensen
Security Researcher
@SpecterOps





TIER BREAKERS: BLIND SPOTS IN CLOUD-MANAGED PAWS

- **Introduction “Cloud-Managed PAW”**
- **Overview of Intune RBAC**
- **Intra-Tenant Isolation with Scope/Tags**
- **Example: Privilege Escalation Path**
- **EntraOps x BloodHound**
- **Inter-Tenant Isolation with Red Tenant**



MARTIN SOHN CHRISTENSEN

Security Researcher @ **SPECTER**  **PS**

Copenhagen, Denmark



martinsohn.dk



[martinsohn.dk](https://twitter.com/martinsohn.dk)



[martinsohn](https://www.linkedin.com/in/martinsohn)



[martinsohndk](https://twitter.com/martinsohndk)



THOMAS NAUNHEIM

Cyber Security Architect @glueck■kanja
Microsoft MVP (Identity & Access, Cloud Security)
Koblenz/Lahnstein, Germany



cloud-architekt.net



Naunheim.cloud



thomasnaunheim

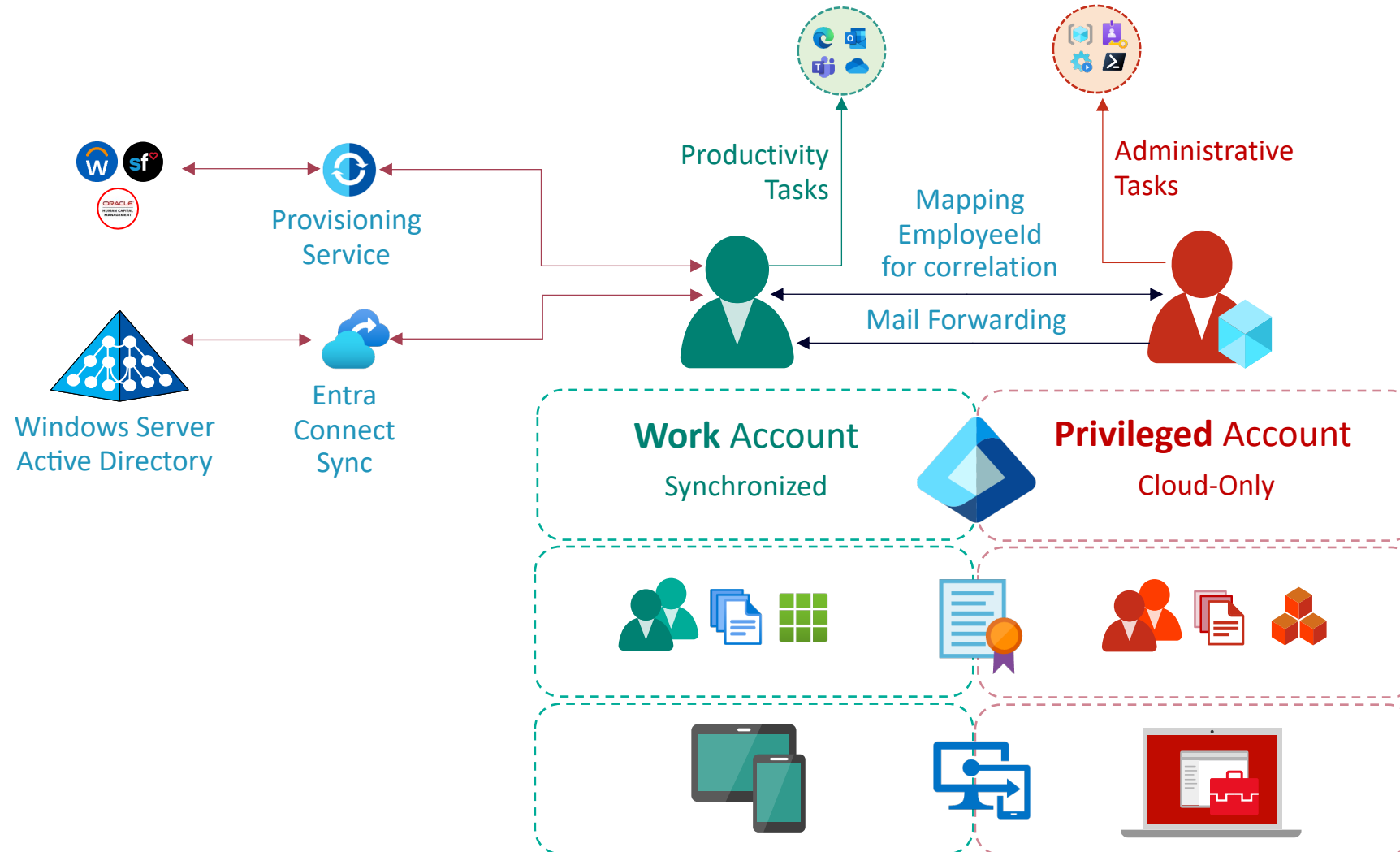


Thomas_Live

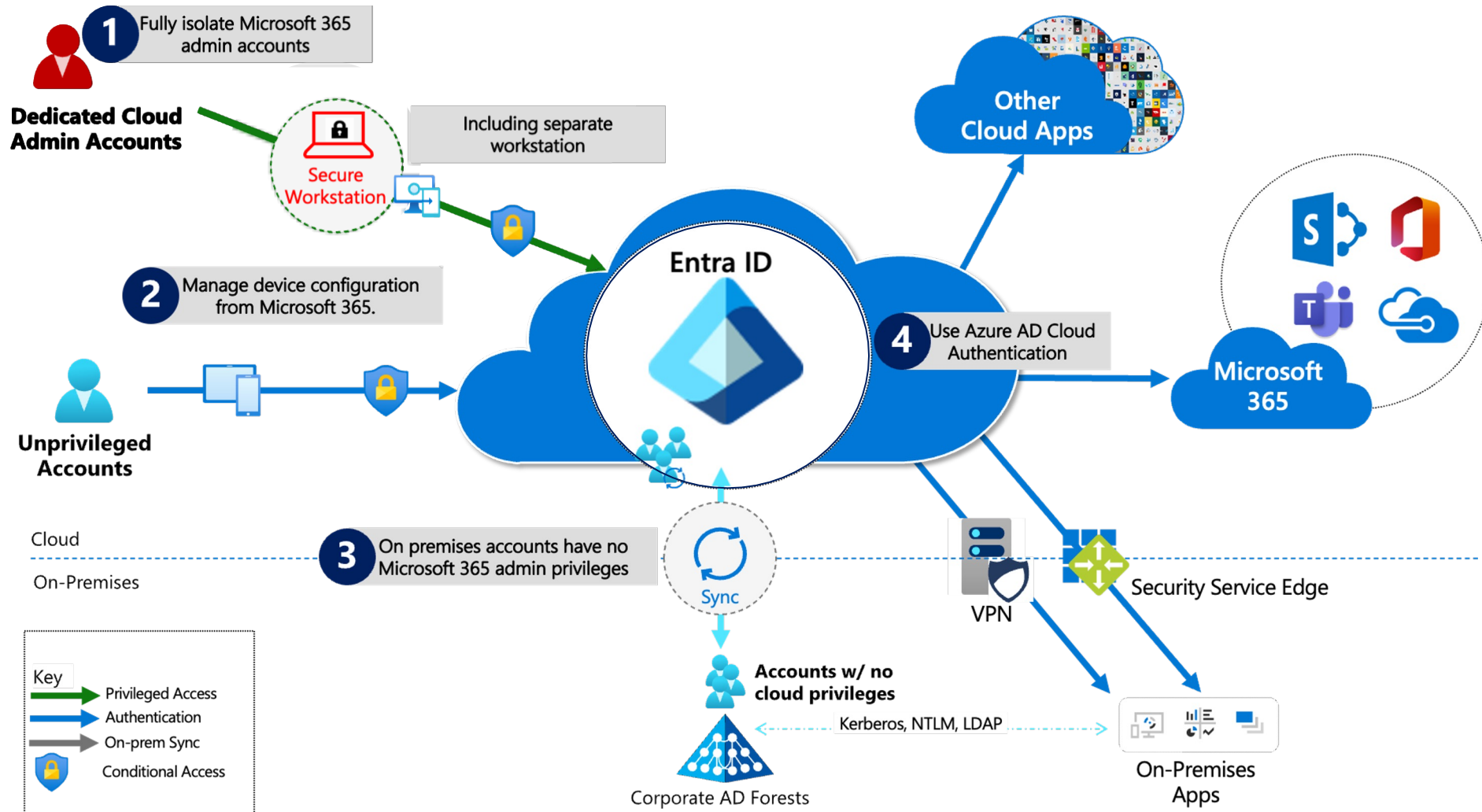
INTRODUCTION CLOUD-MANAGED PAW



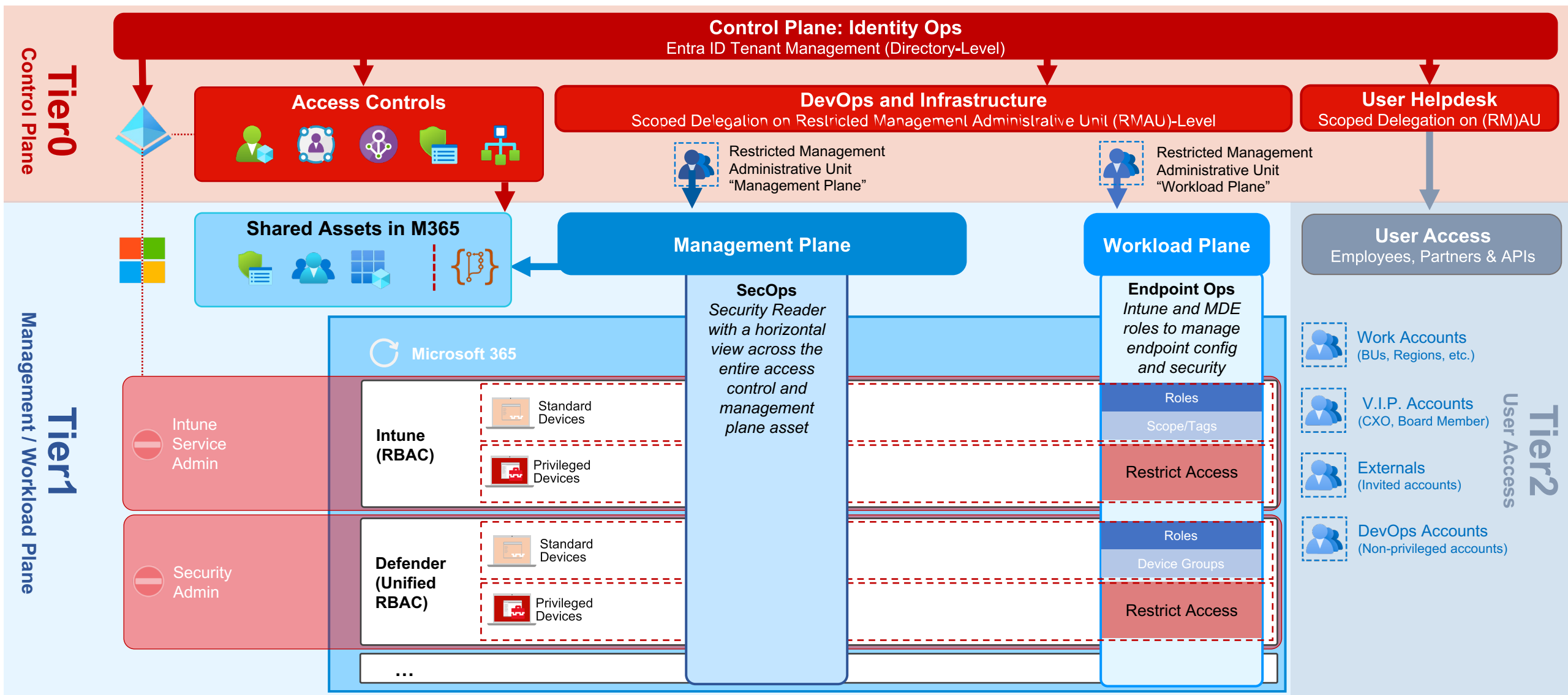
Separation of Privileged Device and User



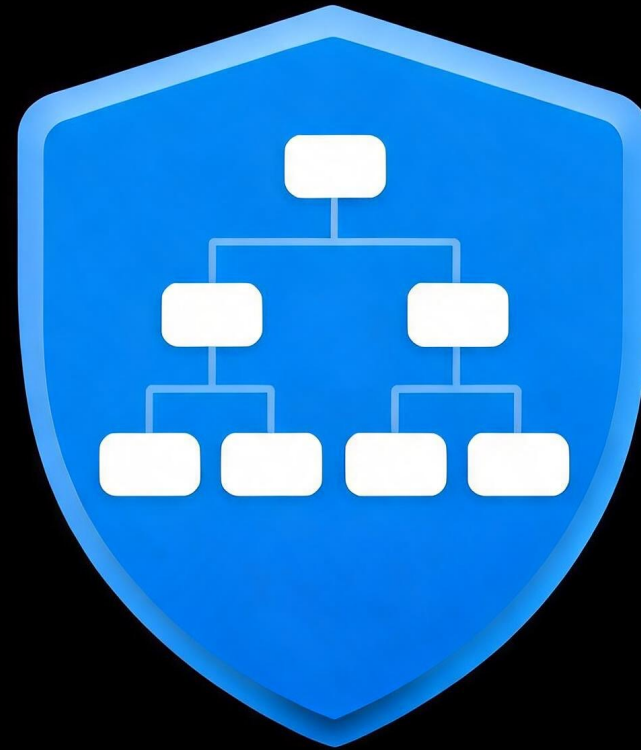
Protect Microsoft 365 from on-premises attacks



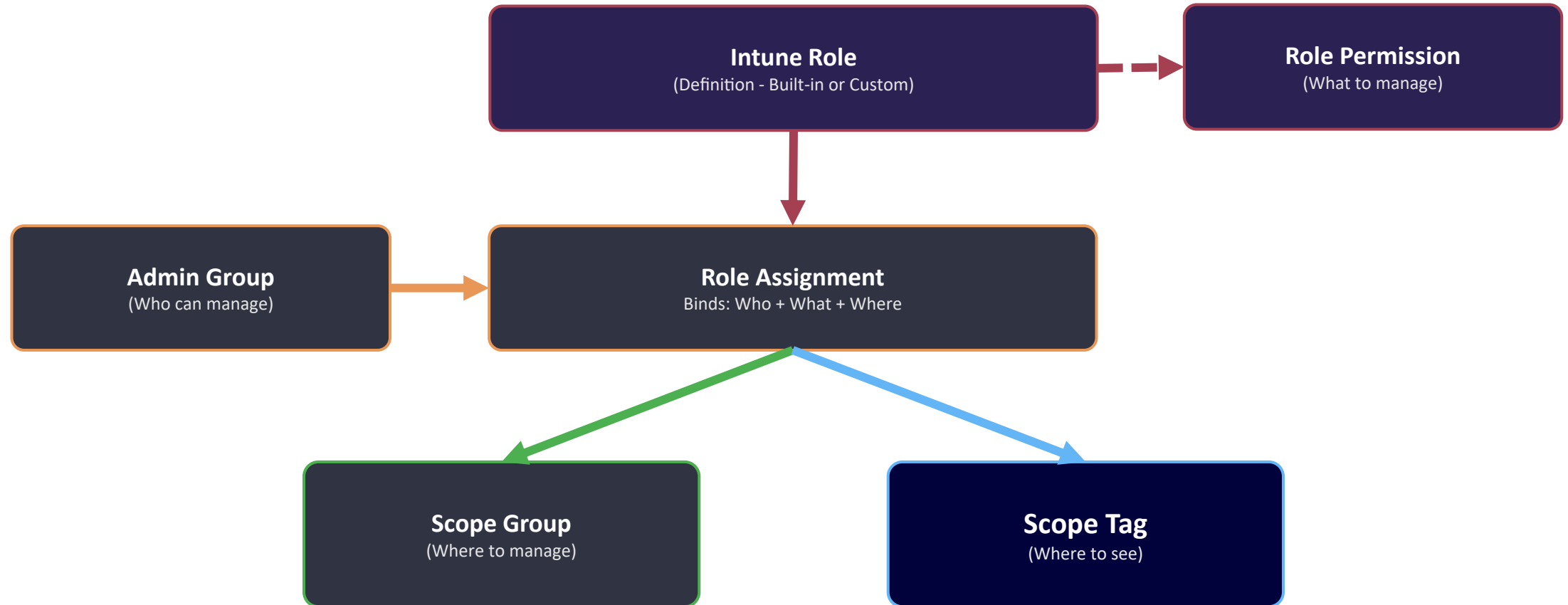
Practical implementation of Enterprise Access Model



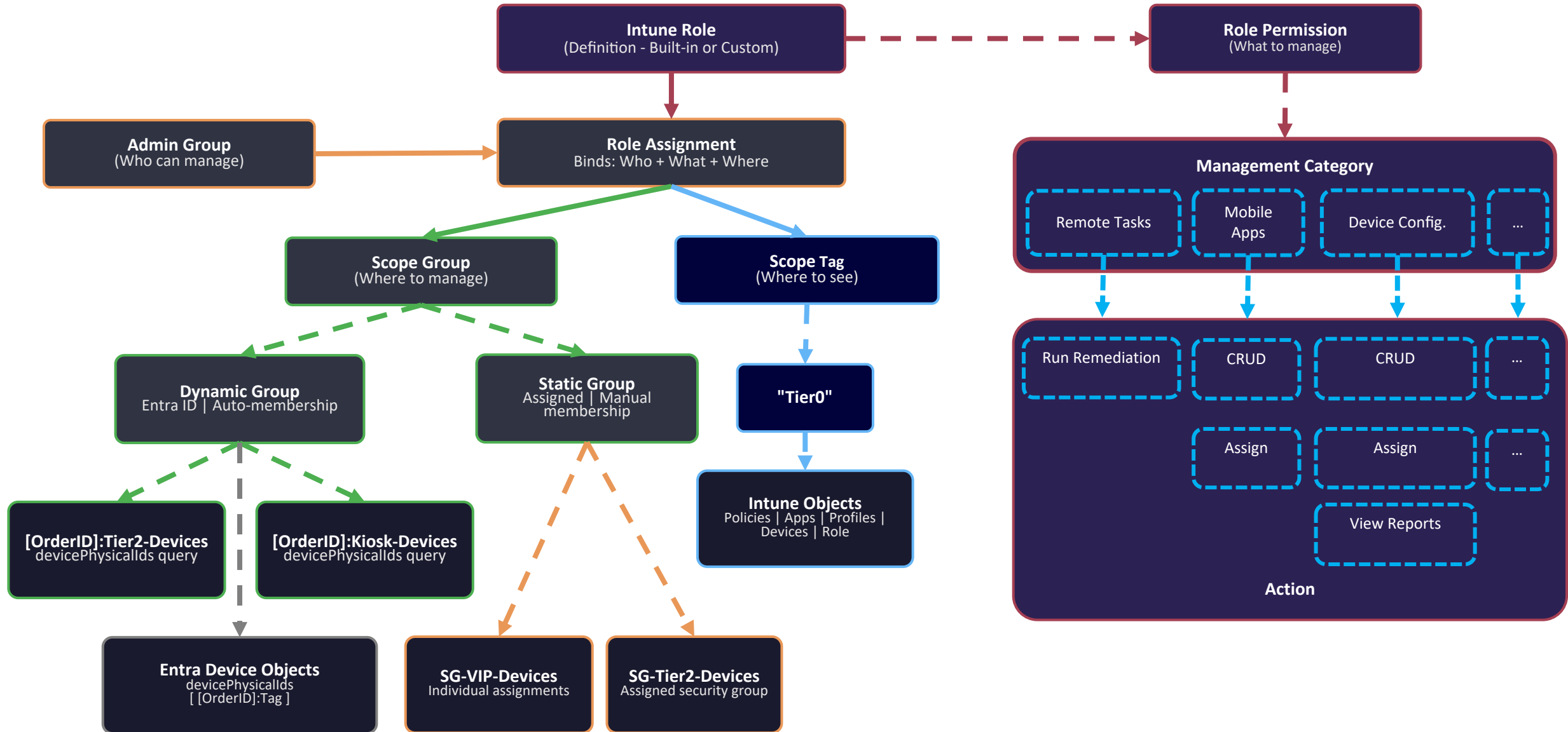
OVERVIEW OF INTUNE RBAC



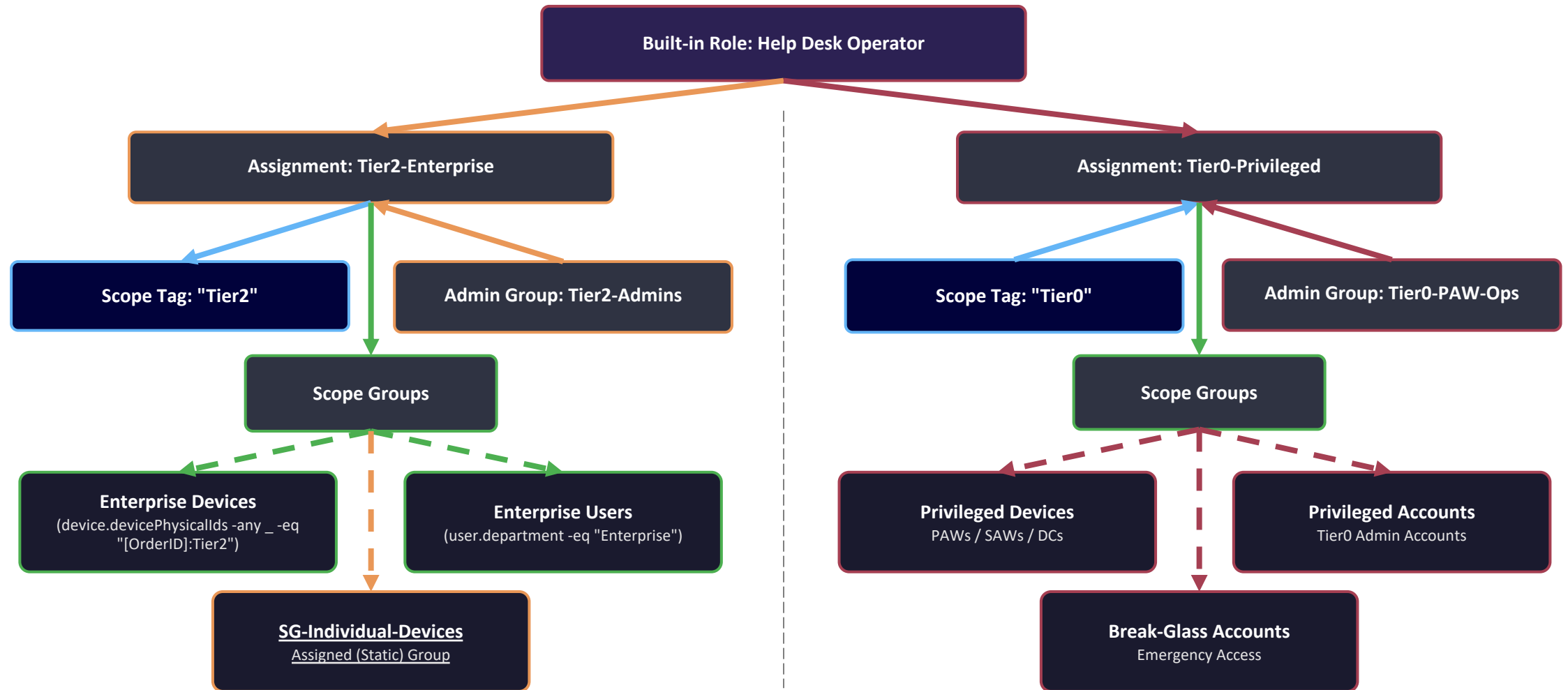
Role Assignment and Scopes



Role Assignment and Scopes



Role & Role Assignments in different scopes



Intune RBAC considerations

Role Assignment

- Can **only assign a scope tag** that are **in the role assignment**
- Can **only target groups** that are **in the Scope (Groups)**
- Nested **admin group** requires license

Scope Tags limitations

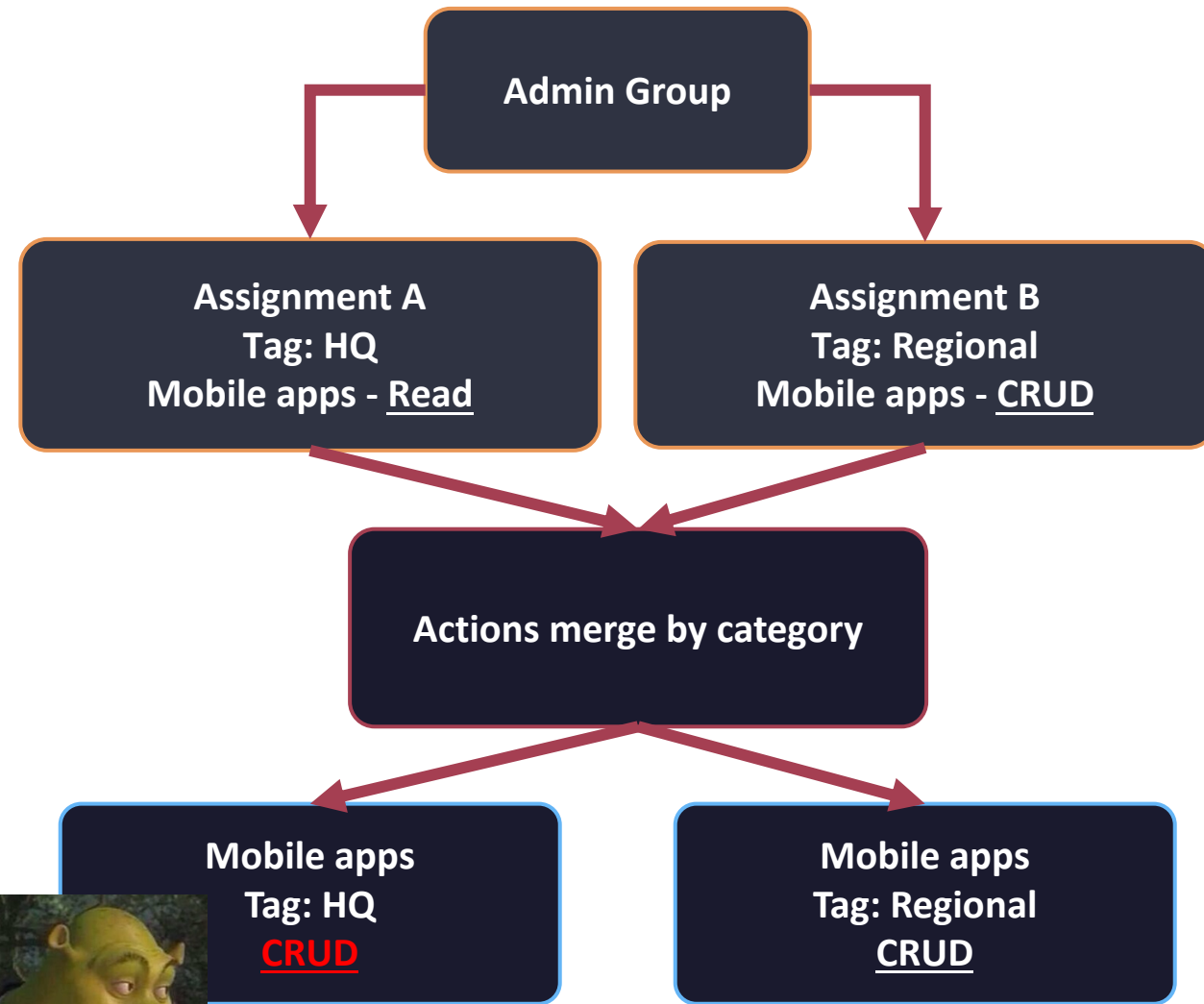
- Not available for **Windows Autopilot Devices** and more
- Support is improving, example **Endpoint Privilege Management** reports

Multi Admin Approval limitations

Scope Tag & Role Assignment scoped permission merge

- Multiple **role assignments** w/ same **permission category** & different **scope tags**
= **actions merged** – **potential unintended behavior**

Scoped Permission Merge

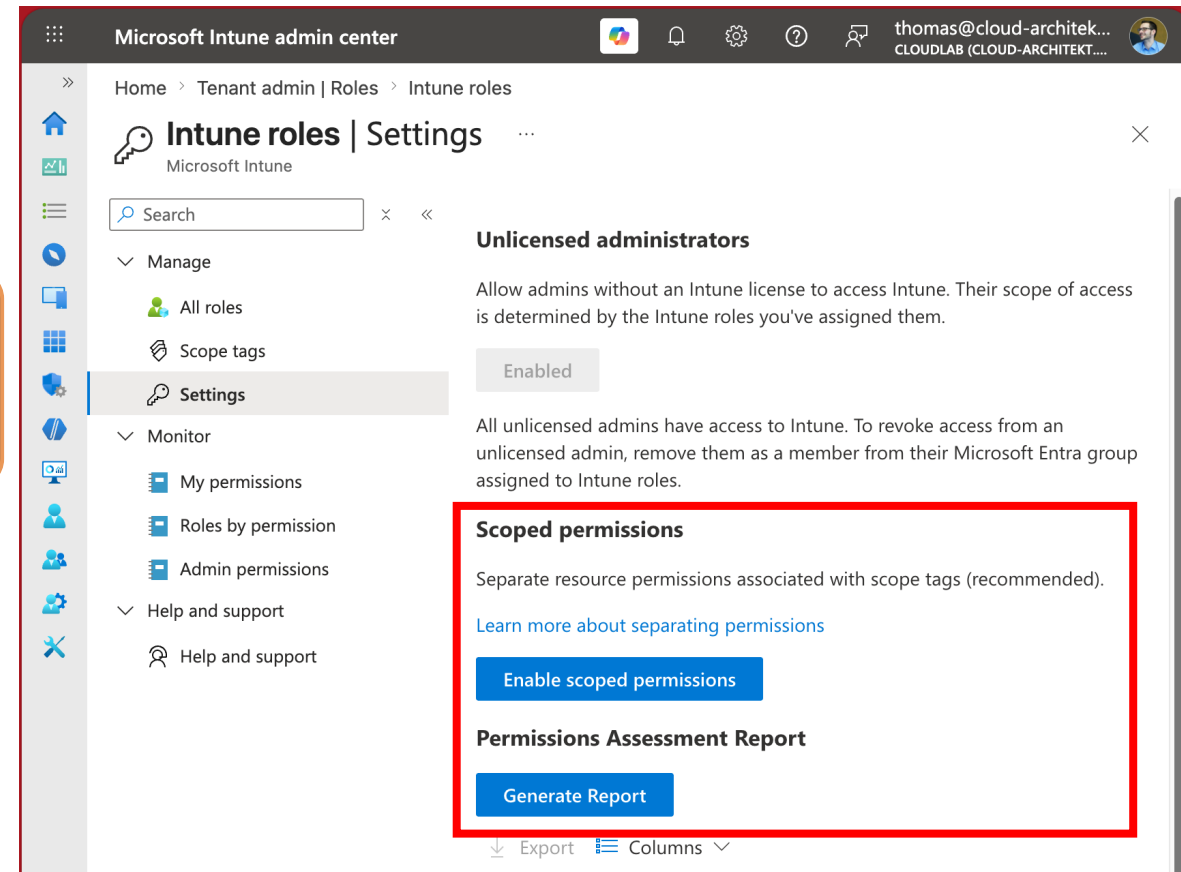
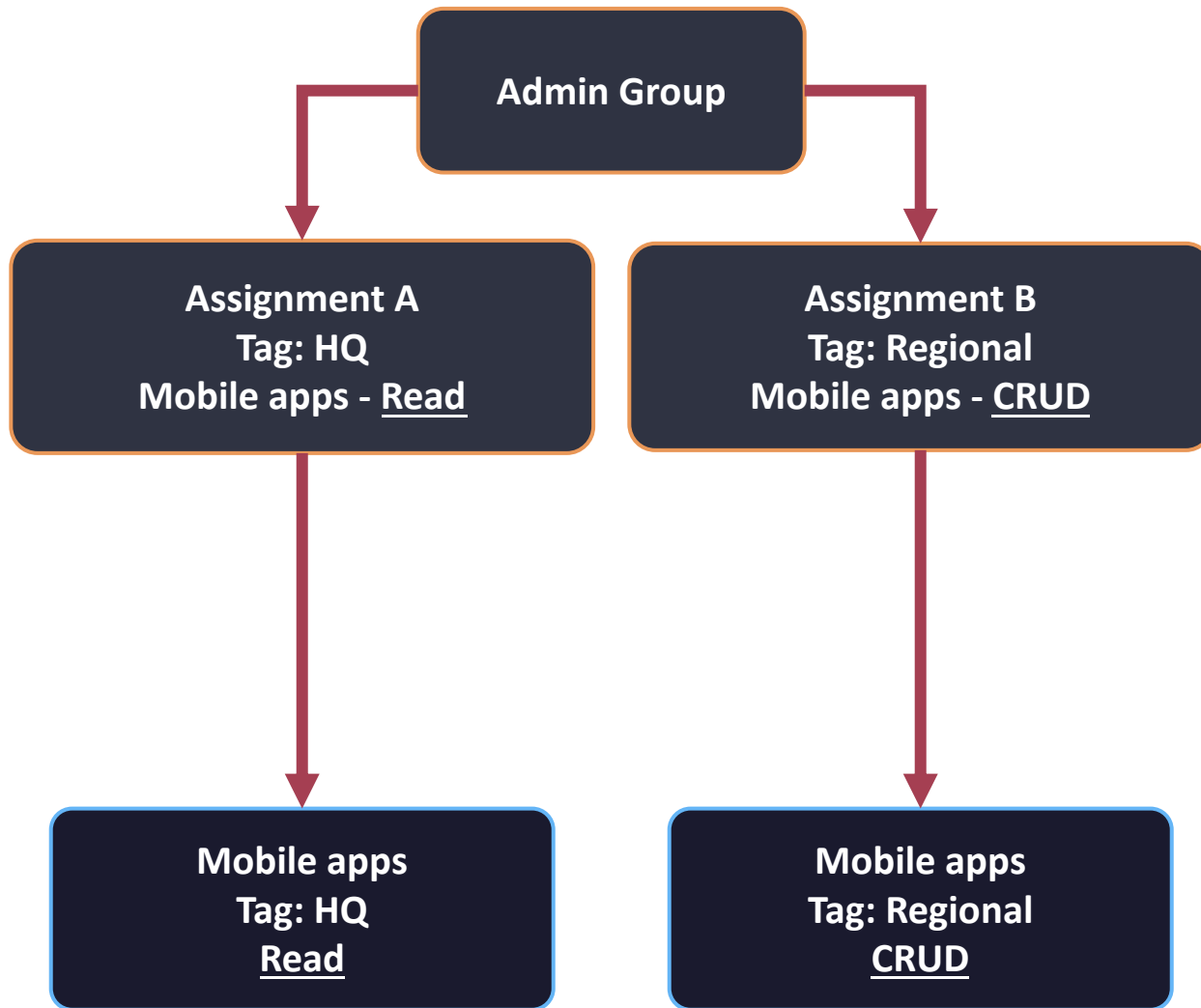


The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Tenant admin | Roles, and Intune roles. The main content area is titled 'Intune roles | Settings' and includes a search bar. The 'Settings' tab is selected, showing options for 'Unlicensed administrators' (Enabled) and 'Scoped permissions' (Learn more about separating permissions, Enable scoped permissions). A red box highlights the 'Scoped permissions' section, which includes a 'Generate Report' button. The bottom of the page shows 'Export' and 'Columns' options.

Microsoft Learn - Use role-based access control (RBAC) and scope tags for distributed IT: Permission behavior across role assignments

Medium - Janic Verboon: A deep dive into the new Intune RBAC Scoped permissions

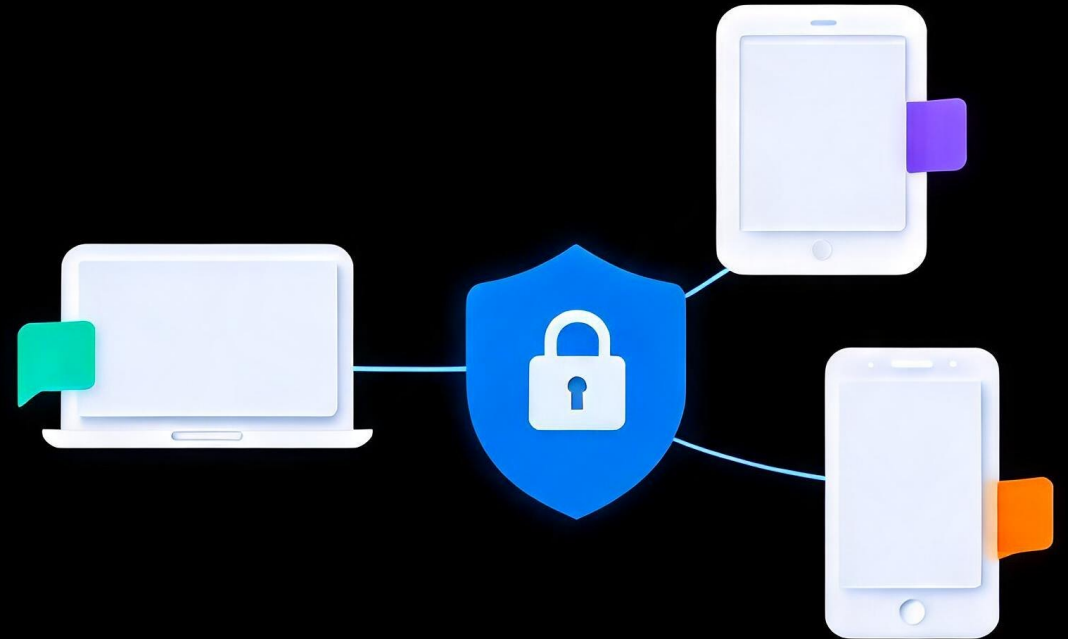
Scoped Permission Merge



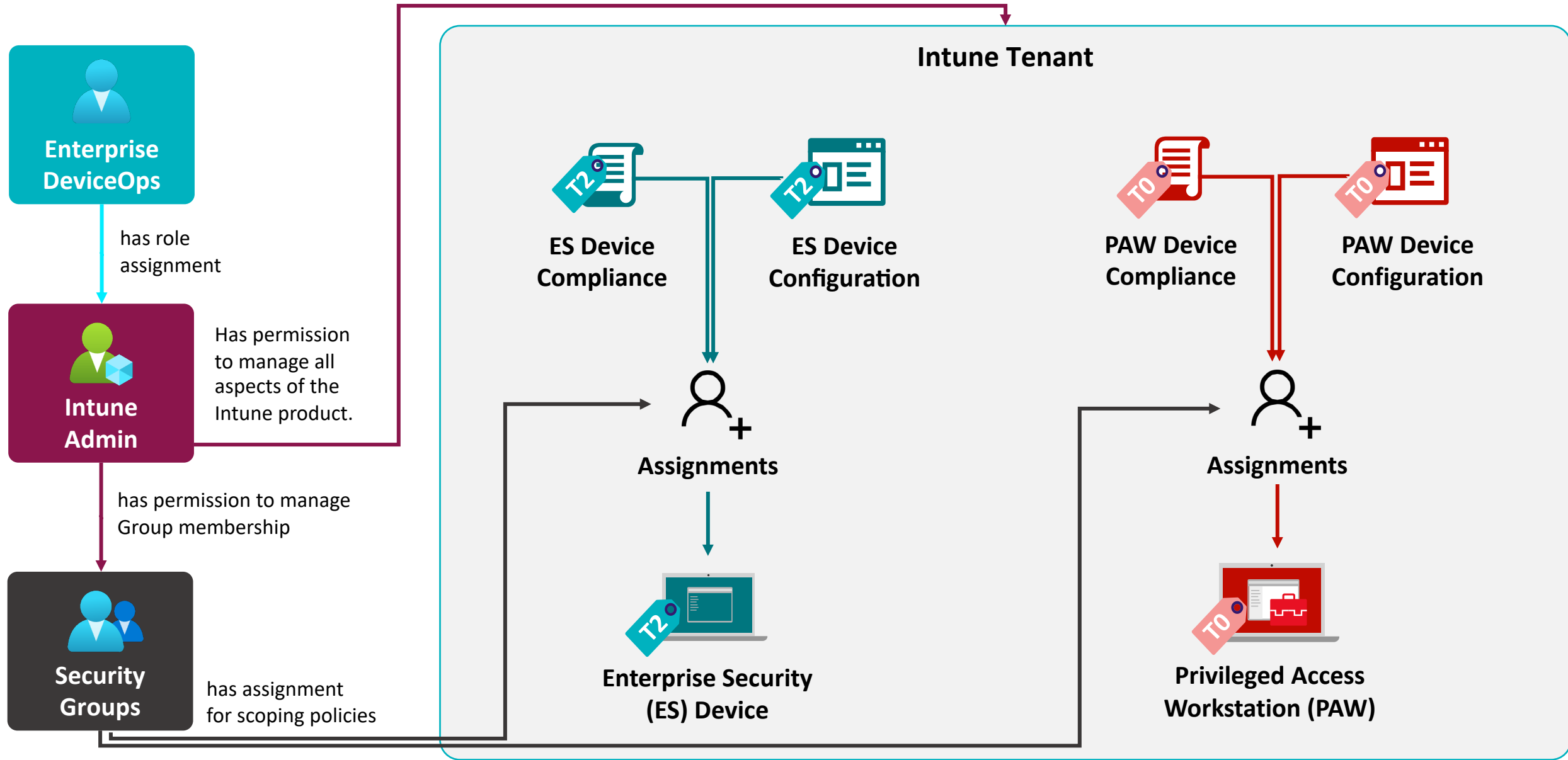
Microsoft Learn - Use role-based access control (RBAC) and scope tags for distributed IT: Permission behavior across role assignments

Medium - Janic Verboon: A deep dive into the new Intune RBAC Scoped permissions

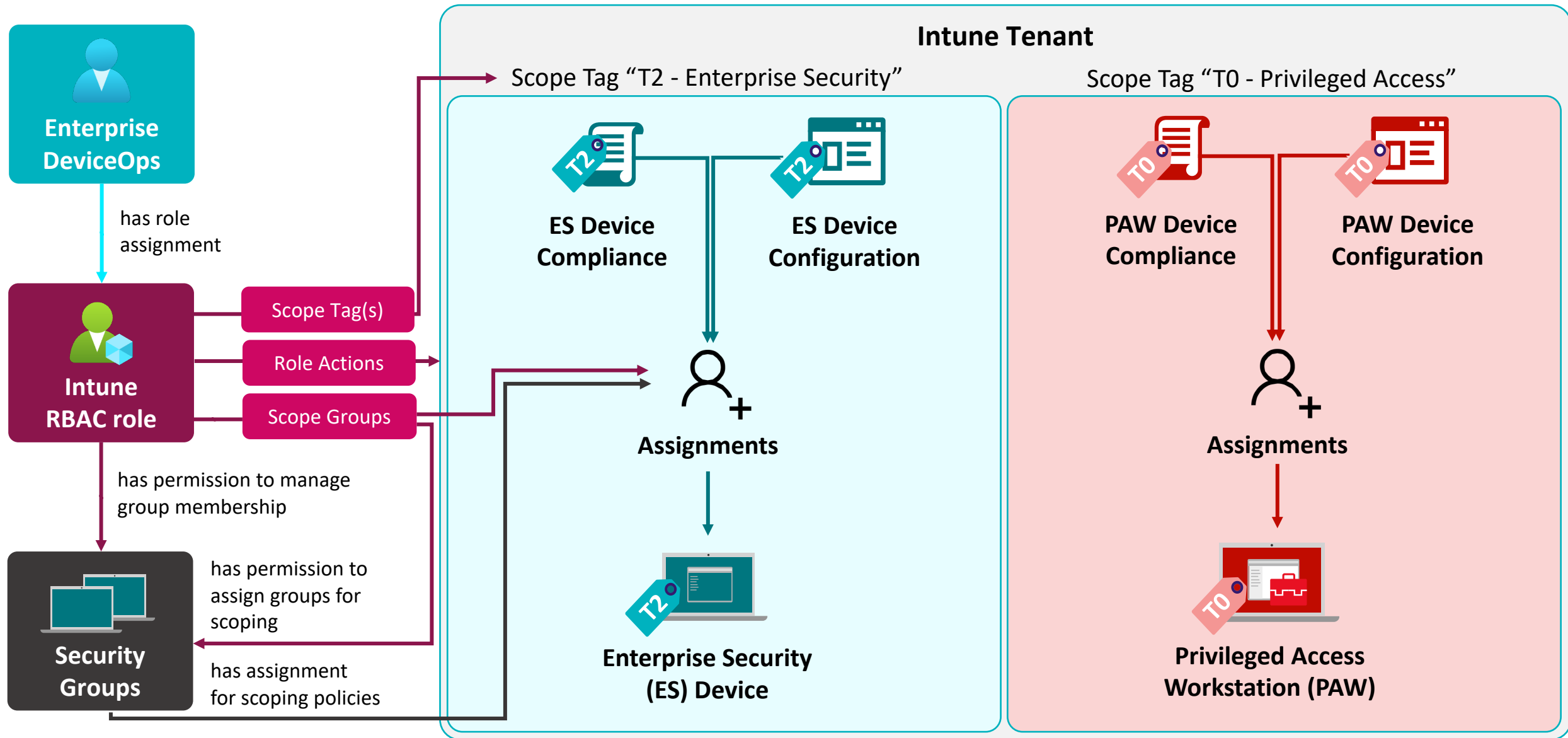
INTRA-TENANT ISOLATION WITH INTUNE SCOPE/TAGS



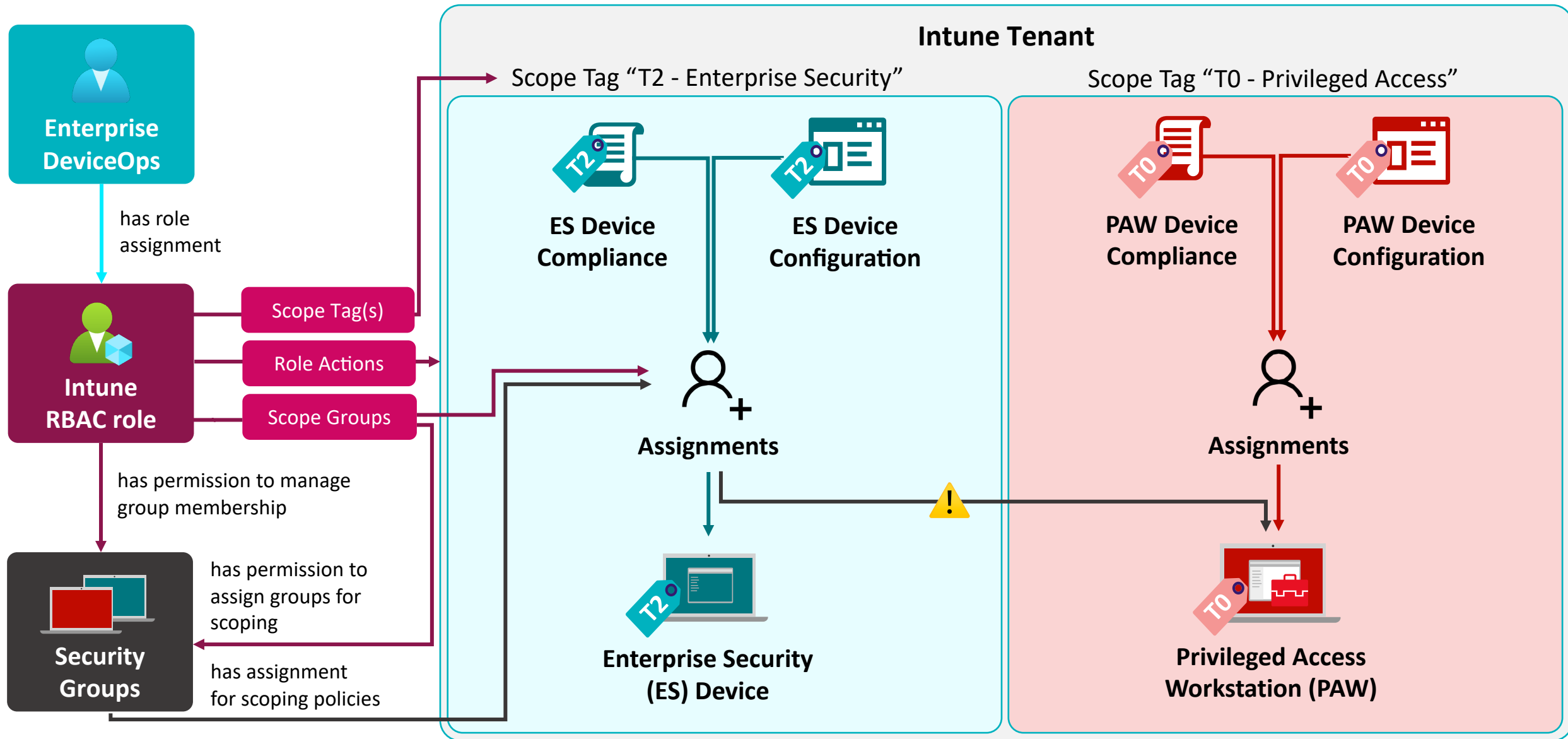
Avoid Intune Admin Role Assignments



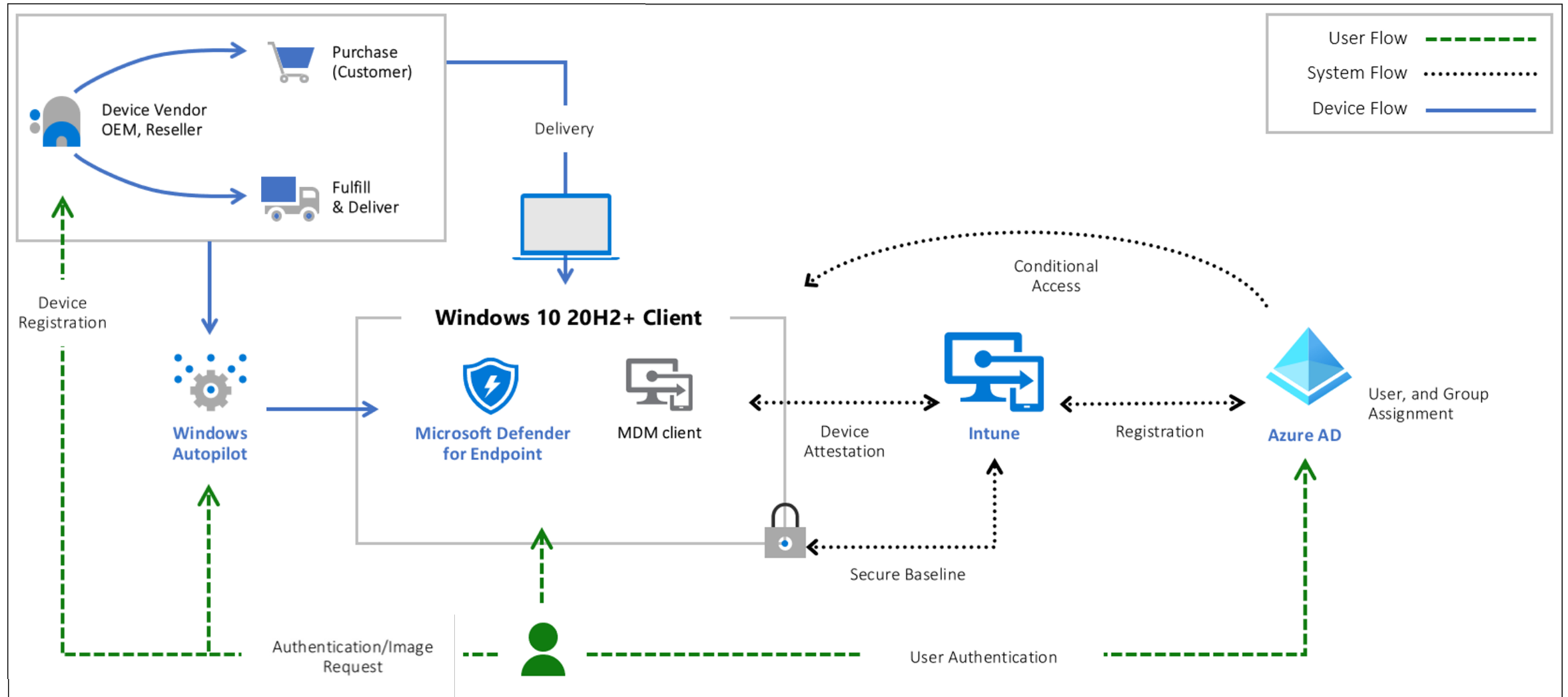
Scoped role with Intune RBAC



Limited isolation with Intune RBAC



Privileged access deployment



Attribute for assigning PAW scope

- **Group type** - Security
- **Group name** - Secure Workstation Devices
- **Membership type** - Dynamic Device
- **Dynamic Membership rules** - `(device.devicePhysicalIds -any _ -contains "[OrderID]:PAW")`

ⓘ Note

The Group Tag is used by the Secure Workstation dynamic group to make the device a member of its group,

Attribute for assigning PAW scope

Home > Devices | Windows > Windows | Enrollment

Windows Autopilot devices

Windows enrollment

[Refresh](#) [Export](#) [Columns](#) [Sync](#) [Import](#) [Assign user](#)

Device name ⓘ

SAW2

Group tag ⓘ

Tier0.SAW

Profile status ⓘ

Assigned

Assigned profile ⓘ

Tier0.SAW Deployment Profile

Date assigned ⓘ

08.04.26, 8:08

Enrollment state ⓘ

Enrolled

Associated Intune device ⓘ

[SAW2](#)

Home > Groups | All groups > ddg_Lab-Tier0.SAW.Devices

ddg_Lab-Tier0.SAW.Devices | Dynamic membershi...

[Save](#) [Discard](#) | [Got feedback?](#)

[Configure Rules](#) [Validate Rules](#)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ [Learn more](#)

And/Or	Property	Operator	Value
	devicePhysicalIds	Any	_ -contains "[Orderl... Edit

[+ Add expression](#)

Rule syntax

[Edit](#)

(device.devicePhysicalIds -any _ contains "[OrderID]:Tier0.SAW")

Mitigation Option: Granular CA Filter

Devices matching the rule:

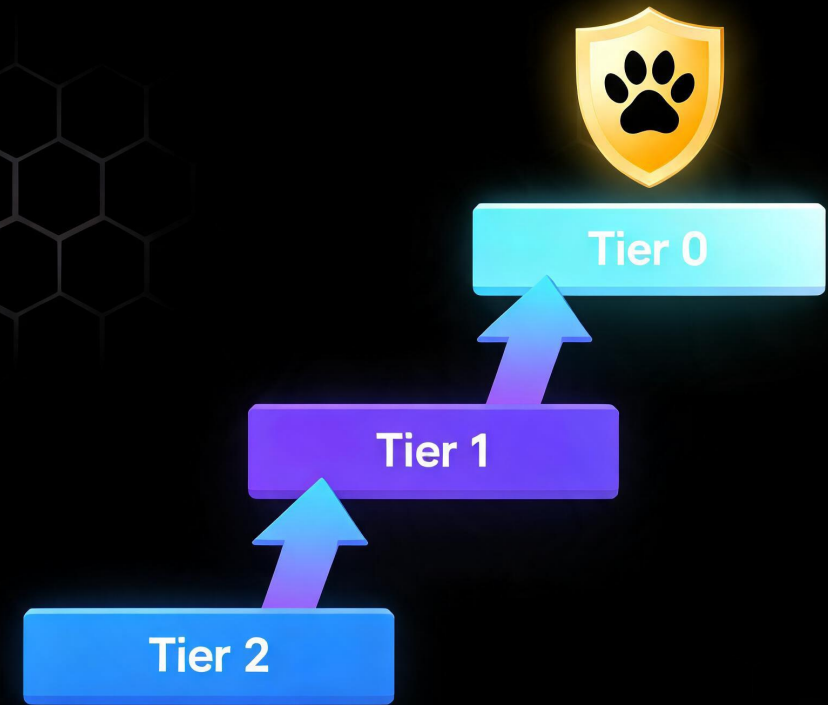
- ☒ Include filtered devices in policy
☐ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	PhysicalIds	Contains	Add a value

+ Add expression

EXAMPLE: PRIVILEGE ESCALATION PATH



Attack Path Scenario from Tier2 > Tier0

1. Intune Scoped Permission

Has enrollment program
permissions and delegation
on scope of Tier2 Devices

>>

Home > Enrollment Program Manager

Enrollment Program Manager | Properties

Microsoft Intune

Search

×

<<

Overview

Favorites

Assignments

Manage

Properties

Assignments

Basics

Edit

Name

Enrollment Program Manager

Description

No Description

Permissions

Edit

Enrollment programs

Sync device

Read device

Create device

Organization

Read

Scope tags

Edit

Default

Add or remove favorites by pressing Cmd+Shift+F

>>

Home > Enrollment Program Manager | Assignments

 pag_Lab-Tier1.Intune.2.EnrollmentProgramManager | Properties

...

Search

×

<<

Manage

Properties

Basics [Edit](#)

Name

pag_Lab-Tier1.Intune.2.EnrollmentProgramManager

Description

No Description

Members [Edit](#)

Included groups

Group	Status
pag_Lab-Tier1.Intune.2.EnrollmentProgramManager	Active

Scope (Groups) [Edit](#)

Included groups

Group	Status
dug_AAD.EnterpriseAccounts	Active
ddg_Lab-Tier2.User.Devices	Active

Scope tags [Edit](#)

Tier2.User

Add or remove favorites by pressing **Cmd+Shift+F**

☐	Name ↑	Type	Email	User type	Object Id
☐	 admScott1	User	admScott1@lab.cloud-architekt.net	Member	6e68479a-153b-4088-bcaf-661d2d327b

Home > Tenant admin | Roles > Intune roles

Intune roles | My permissions

Microsoft Intune

Search

×

«

Manage

All roles

Scope tags

Settings

Monitor

My permissions

Help and support

Help and support

You have the resource permissions shown in the table below.

Refresh

Export

Columns

5 items

Search

i

Resource ↓	Permission
Organization	Read
DefaultScopeTagEnabled	Read
AppleDeviceSerialNumbers	Update
AppleDeviceSerialNumbers	Read
AppleDeviceSerialNumbers	Create

Add or remove favorites by pressing Cmd+Shift+F

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

thomas@cloud-architek...
CLOUDLAB (CLOUD-ARCHITEKT...

Home > Administrative units > Tier0-ControlPlane.0.Intune.SAW [Restricted management] | Devices > SAW3 | Properties > Roles and administrators | All roles > Devices | All devices

SAW3 | Properties
CloudLab - Microsoft Entra ID

Enable Disable Delete Manage Got feedback?

Manage

Properties

Roles and administrators

Administrative Units

BitLocker keys

Local administrator password recovery

This device is a Windows Autopilot device. Devices deployed with Windows Autopilot cannot be deleted in the Microsoft Entra admin center. Learn more about managing Windows Autopilot devices.

Name	SAW3
Device ID	350c15b0-a02c-431c-9438-04f7d3487522
Object ID	ae4855e-d083-4ca7-b5df-4c1717567536
Enabled	Yes
OS	Windows
Version	10.0.28000.1719
Join type	Microsoft Entra joined
Owner	admThom0
User principal name	admThom0@lab.cloud-architekt.net
MDM	Microsoft Intune
Security settings management	Microsoft Intune
Compliant	Yes
Registered	4/23/2026, 6:32:19 PM
Activity	4/19/2026, 6:03:30 PM

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

2

thomas@cloud-architek...
CLOUDLAB (CLOUD-ARCHITEKT....)

Home > Administrative units > Tier0-ControlPlane.0.Intune.SAW [Restricted management] | Devices > SAW3 | Properties > Roles and administrators | All roles > Devices | All devices

SAW3 | Properties
CloudLab - Microsoft Entra ID

✕

Manage

Properties

Roles and administrators

Administrative Units

BitLocker keys

Local administrator password recovery

«

✓ Enable

⊘ Disable

🗑 Delete

⚙ Manage

|

🗣 Got feedback?

Copy to clipboard

📘 This device is a Windows Autopilot device. Devices deployed with Windows Autopilot cannot be deleted in the Microsoft Entra admin center. Learn more about managing Windows Autopilot devices. →

Enabled	Yes
OS	Windows
Version	10.0.28000.1719
Join type	Microsoft Entra joined
Owner	admThom0
User principal name	admThom0@lab.cloud-architekt.net
MDM	Microsoft Intune
Security settings management	Microsoft Intune
Compliant	Yes
Registered	4/23/2026, 6:32:19 PM
Activity	4/19/2026, 6:03:30 PM
Groups	ddg_Lab-Tier0.SAW.Devices
Extension attributes	extensionAttribute1 : SAW

ddg_Lab-Tier0.SAW.Devices | Members ...

« + Add members Bulk operations Refresh Refresh Manage view Remove Got feedback?

 This group is a member of restricted management administrative unit. Management rights are limited to administrators scoped on that administrative unit

Direct members All members

Search

 Add filter

3 group members found

☐	Name ↑	Type	Email	User type
☐	 SAW0	Device		
☐	 SAW2	Device		
☐	 SAW3	Device		

Activity

 Access reviews

-  Audit logs

Bulk operation results

Troubleshooting + Support

 New support request

 Got feedback?

 New support request

```
(device.devicePhysicalIds -any _ -contains "[OrderID]:Tier0.SAW")
```

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

2

thomas@cloud-architek...
CLOUDLAB (CLOUD-ARCHITEKT....

Home > Administrative units > Tier0-ControlPlane.0.Intune.SAW [Restricted management] | Devices > SAW3 | Properties > Roles and administrators | All roles > Devices | All devices > SAW3

SAW3 | Administrative Units

CloudLab - Microsoft Entra ID

<<

+ Assign to administrative unit

X Remove from administrative unit

Manage

Properties

Roles and administrators

Administrative Units

BitLocker keys

Local administrator password recovery

☐	Name	Description	Restricted management	Membership type
☐	Tier0-ControlPlane.0.Intune.SAW	Control assets on scope of Tier0 "Control Pla...	Yes	Dynamic

 SAW3 | Group membership ...

× × «

 Refresh  Export  Columns ▼

▼ Monitor

 Group membership



 Add filters

Group Name	Object ID 	Membership type	Direct or Transitive 
ddg_Lab-Tier0.SAW.Devices	eb2e4591-19d1-4b3b-8751-d70...	Dynamic	Direct

SAW3 | Properties ...

>>

Save Discard

Device name ⓘ

SAW3

Rename

Management name *

admThom0_Windows_4/23/2026_4:32 PM

Device category

Tier0.SAW

Device ownership

Corporate

Primary user ⓘ

admThom0

Change primary user

Remove primary user

Scope tags ⓘ

1 scope tag selected

Open

Notes

Select tags

×

Search by name ⓘ

- Name
- Default
- Tier0.SAW
- Tier1.SAW
- Tier2.User

Selected scope tags

Tier0.SAW

Remove

Select

 Add filters

>>

Attack Path Scenario from Tier2 > Tier0

1. Intune Scoped Permission

Has enrollment program permissions and delegation on scope of Tier2 Devices



2. Update Group Tag

Change Group Tag on a Tier0 PAW device in Windows Autopilot enrollment

Manage devices by platform



Configuration policy assignment failures



Unauthorized

You don't have authorization to retrieve any device. Please contact your Global or Intune administrator.

Noncompliant devices



Unauthorized

You don't have authorization to retrieve any device. Please contact your Global or Intune administrator.

Attack Path Scenario from Tier2 > Tier0

1. Intune Scoped Permission

Has enrollment program permissions and delegation on scope of Tier2 Devices

2. Update Group Tag

Change Group Tag on a Tier0 PAW device in Windows Autopilot enrollment

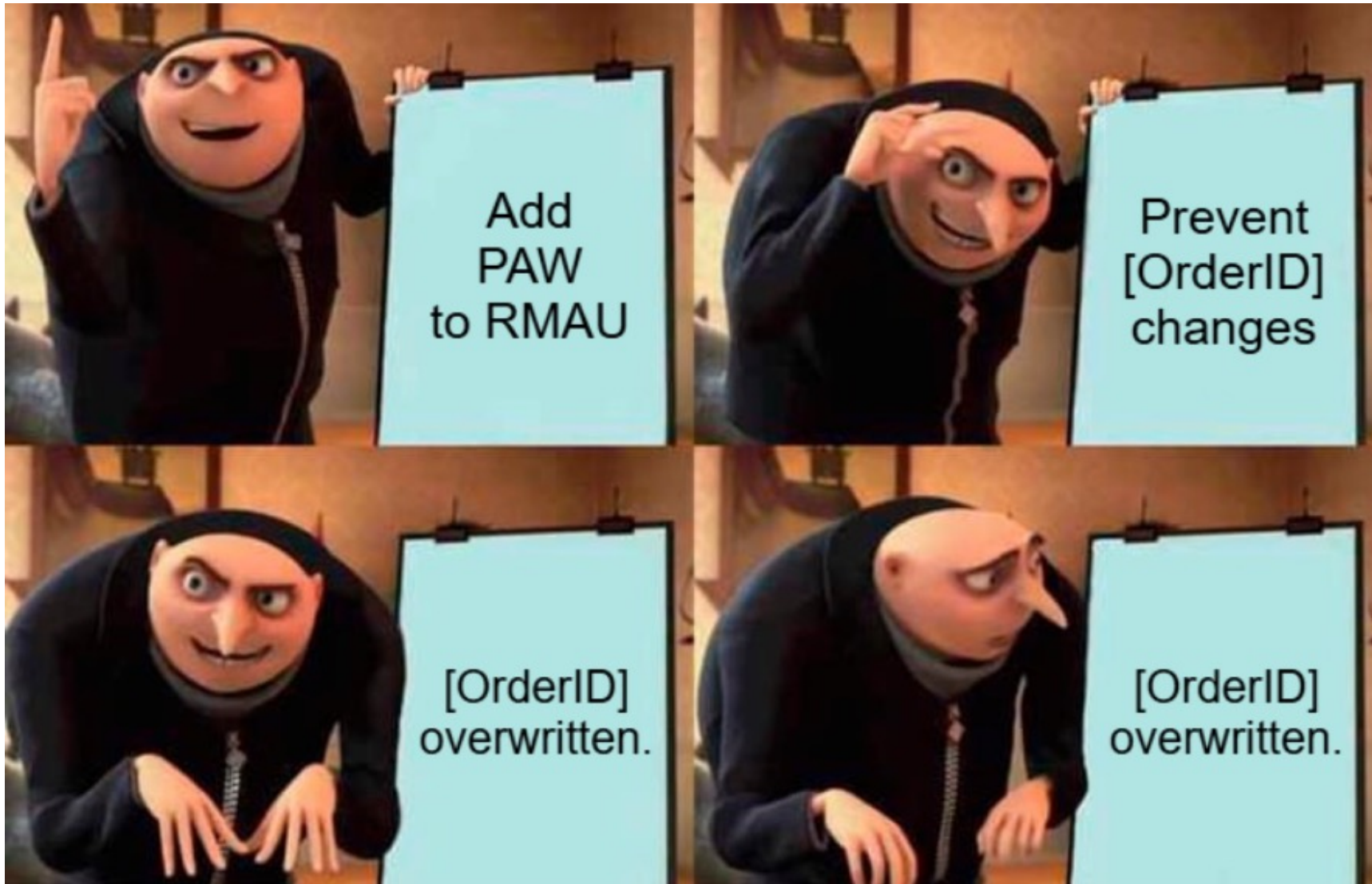
3. OrderID Changes

Group Tag maps to [OrderID] on the Entra device object - attribute is overwritten

4. Dynamic Group Shift

PAW moves from Tier0 to Tier2 scope group via [OrderID] filter

Changed Group Tag affects the device attribute?



Home > Devices

Devices | Audit logs

CloudLab - Microsoft Entra ID

>> Download Refresh Columns Got feedback?

This view will soon be replaced with a view that includes custom security attributes

Date : Last 1 month

Show dates as : Local

Service : All

Date	Service	Category
4/25/2026, 11:41:56 AM	Core Directory	Device
4/25/2026, 11:39:17 AM	Core Directory	Device
4/25/2026, 11:38:55 AM	Core Directory	Device
4/25/2026, 11:35:22 AM	Core Directory	Device
4/25/2026, 11:34:12 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:33:49 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:33:43 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:33:32 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:33:24 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:33:17 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:33:06 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:32:58 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:32:53 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:32:35 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:30:16 AM	Self-service Group Mana...	GroupManagement
4/25/2026, 11:29:58 AM	Self-service Group Mana...	GroupManagement

Audit Log Details

Activity Target(s) Modified Properties

Activity

Date4/25/2026, 11:41 AM

Activity TypeUpdate device

Correlation ID11774926-a5f5-4b70-a636-bcda35f9a42b

CategoryDevice

Statussuccess

Status reason

User Agent

Initiated by (actor)

TypeApplication

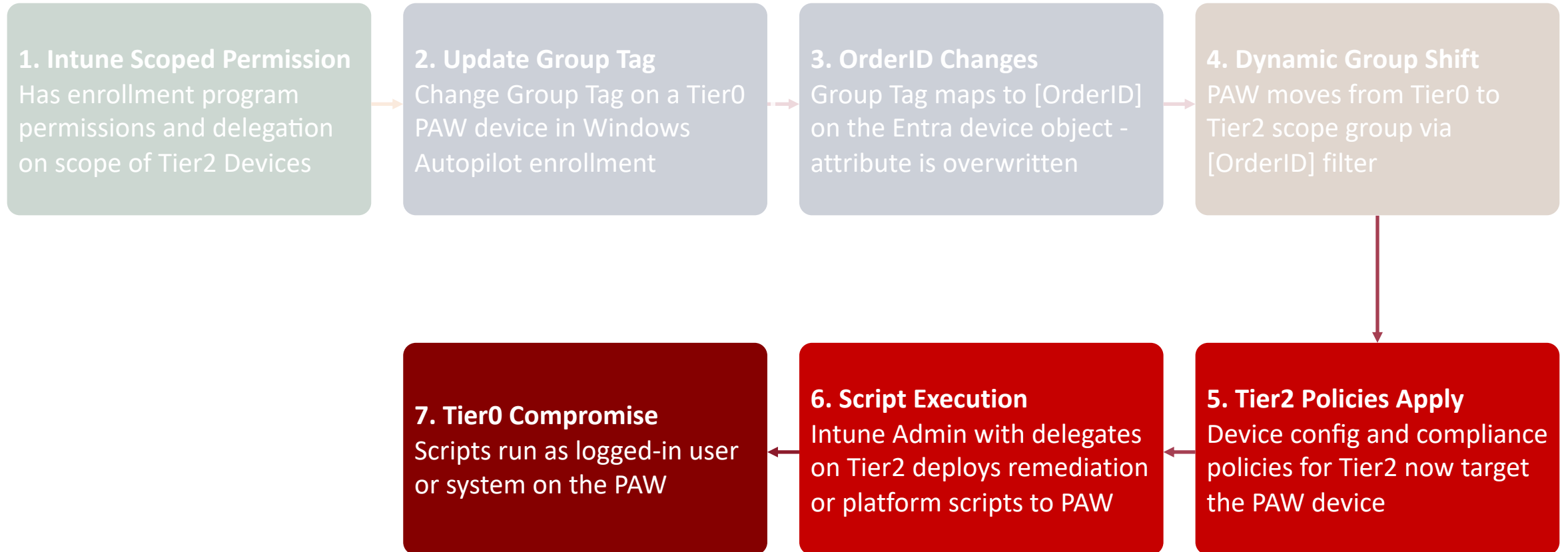
Display NameDevice Registration Service

App ID

Service principal ID9349ebff-7874-4f23-a2ed-2a5317510b46

Service principal name

Attack Path Scenario from Tier2 > Tier0



 Home

 Dashboard

 All services

 Explorer

 Devices

 Apps

 Endpoint security

 Agents

 Reports

 Users

 Groups

 Tenant administration

 Troubleshooting + support

<<

Home > Tenant admin | Roles > Intune roles | All roles > CloudLab-DeviceOps

 **CloudLab-DeviceOps | Properties** ...

Microsoft Intune

×

<<

 Overview

 Favorites

 Assignments

 Manage

 **Properties**

 Assignments

Filters

Intune data warehouse

Managed apps

Managed devices

Microsoft Store For Business

Mobile apps

Organization

Policy Sets

Remote tasks

Security tasks

Create

Update

Delete

Read

Read

Wipe

Read

Assign

Delete

Update

Create

Update

View reports

Read

Set primary user

Delete

Read

Modify

Read

Delete

Relate

View reports

Create

Assign

Update

Read

Delete

Create

Assign

Update

Read

Run Remediation

Update

Read

Add or remove favorites by pressing Cmd+Shift+F

Home

Dashboard

All services

Explorer

Devices

Apps

Endpoint security

Agents

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Tenant admin | Roles > Intune roles | All roles > CloudLab-DeviceOps | Assignments

Tier2-UserDeviceOps | Properties

Search

Manage

Properties

Basics Edit

NameTier2-UserDeviceOps

DescriptionNo Description

Members Edit

Included groups

Group	Status
pag_Lab-Tier1.Intune.2.UserDeviceOps	Active

Scope (Groups) Edit

Included groups

Group	Status
dug_AAD.EnterpriseAccounts	Active
sug_AAD.Tier2.CustomScopeUser	Active
ddg_Lab-Tier2.User.Devices	Active
sug_AAD.Tier2.CustomScopeDevice	Active

Scope tags Edit

Tier2.User

Add or remove favorites by pressing Cmd+Shift+F

 [New support request](#)

Role	↑↓	Group	↑↓	Group type	↑↓	Membership	↑↓	State	End time	Action
Member		pag_Lab-Tier1.Intune.2.UserDeviceOps		Security		Direct		Activated	4/25/2026, 8:13:40 PM	Deactivate
Member		pag_Lab-Tier1.Intune.2.EnrollmentProgramM		Security		Direct		Assigned	Permanent	Deactivate



Recycle Bin



Microsoft
Edge



Hunting in Microsoft Defender XDR

Query

Run query

Create summary rule

Create detection rule

Custom time range

```
1 union DeviceEvents, DeviceFileEvents, DeviceProcessEvents
2 | where DeviceName == "saw3"
3 | where InitiatingProcessParentFileName contains "AgentExecutor.exe" or InitiatingProcessFileName contains "powershell" or FolderPath contains "AccessTokens" or InitiatingProcessVersionInfoFileDescription contains "Mic
4 | project Timestamp, DeviceName, ActionType, FolderPath, InitiatingProcessFileName, InitiatingProcessAccountUpn, InitiatingProcessParentFileName
```

Results

Query history

Getting started

Export

Show empty columns

101 items

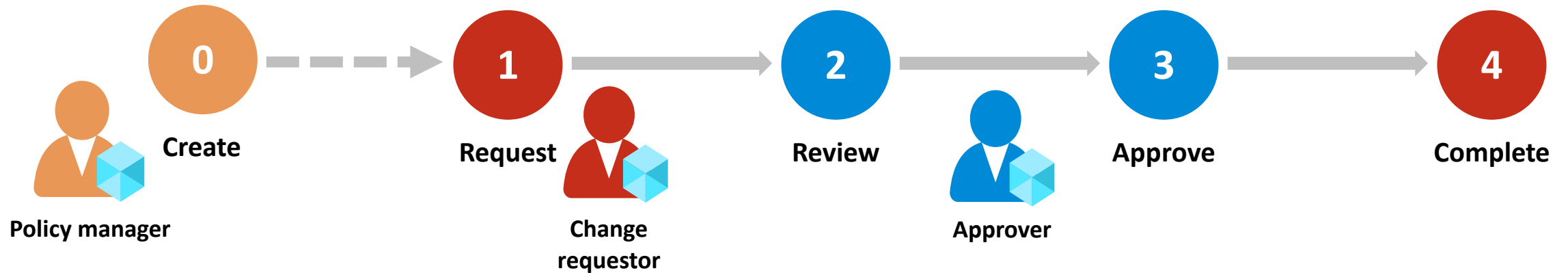
Search

00:00.434

Low

	Timestamp	ActionType	FolderPath	InitiatingProcessFileName	InitiatingProcessPa...
☐	> Apr 25, 2026 11:02:14 AM	ProcessCreated	C:\Program Files (x86)\Microsoft Intune Management Extension\AgentExecutor.exe	microsoft.management.services.	services.exe
☐	> Apr 25, 2026 11:02:14 AM	ProcessCreated	C:\Windows\System32\conhost.exe	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:02:15 AM	FileCreated	C:\Windows\SystemTemp_PSScriptPolicyTest_tnw3na3c.xdm.ps1	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:02:15 AM	FileCreated	C:\Windows\SystemTemp_PSScriptPolicyTest_sygs1l31.gbv.psm1	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:02:18 AM	FileCreated	C:\Program Files\PowerShell\Modules\Az.Resources\9.0.3\PostImportScripts2\ValidationModule.ps1	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:02:18 AM	FileCreated	C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupPr	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:02:29 AM	FileCreated	C:\Program Files\PowerShell\Modules\Az.Resources\9.0.3\PostImportScripts2	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:04:18 AM	ProcessCreated	C:\Program Files (x86)\Microsoft Intune Management Extension\AgentExecutor.exe	microsoft.management.services.	services.exe
☐	> Apr 25, 2026 11:04:18 AM	ProcessCreated	C:\Windows\System32\conhost.exe	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:04:19 AM	FileCreated	C:\Windows\SystemTemp_PSScriptPolicyTest_kryga41a.5ou.ps1	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:04:19 AM	FileCreated	C:\Windows\SystemTemp_PSScriptPolicyTest_tktjtvel.pn4.psm1	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:04:22 AM	FileCreated	C:\Program Files\PowerShell\Modules\Az.Resources\9.0.3\PostImportScripts\ValidationModule.ps1	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:04:39 AM	FileCreated	C:\Program Files\PowerShell\Modules\Az.Resources\9.0.3\PostImportScripts	powershell.exe	AgentExecutor.exe
☐	> Apr 25, 2026 11:07:18 AM	ProcessCreated	C:\Program Files (x86)\Microsoft Intune Management Extension\AgentExecutor.exe	microsoft.management.services.	services.exe
☐	> Apr 25, 2026 11:21:02 AM	ProcessCreated	C:\Program Files (x86)\Microsoft Intune Management Extension\AgentExecutor.exe	microsoft.management.services.	services.exe

Mitigation Option: Multi Admin Approval



Breaks Automation

Break automation process using service principals

No Notifications

New requests & approvals require manual contact

No Target Scoping

No target options for specific scope or tags

All Scripts Covered

Covers all Remediation and Platform Scripts at once



Ready for large and real-world organizations?

Mitigation Option: Multi Admin Approval

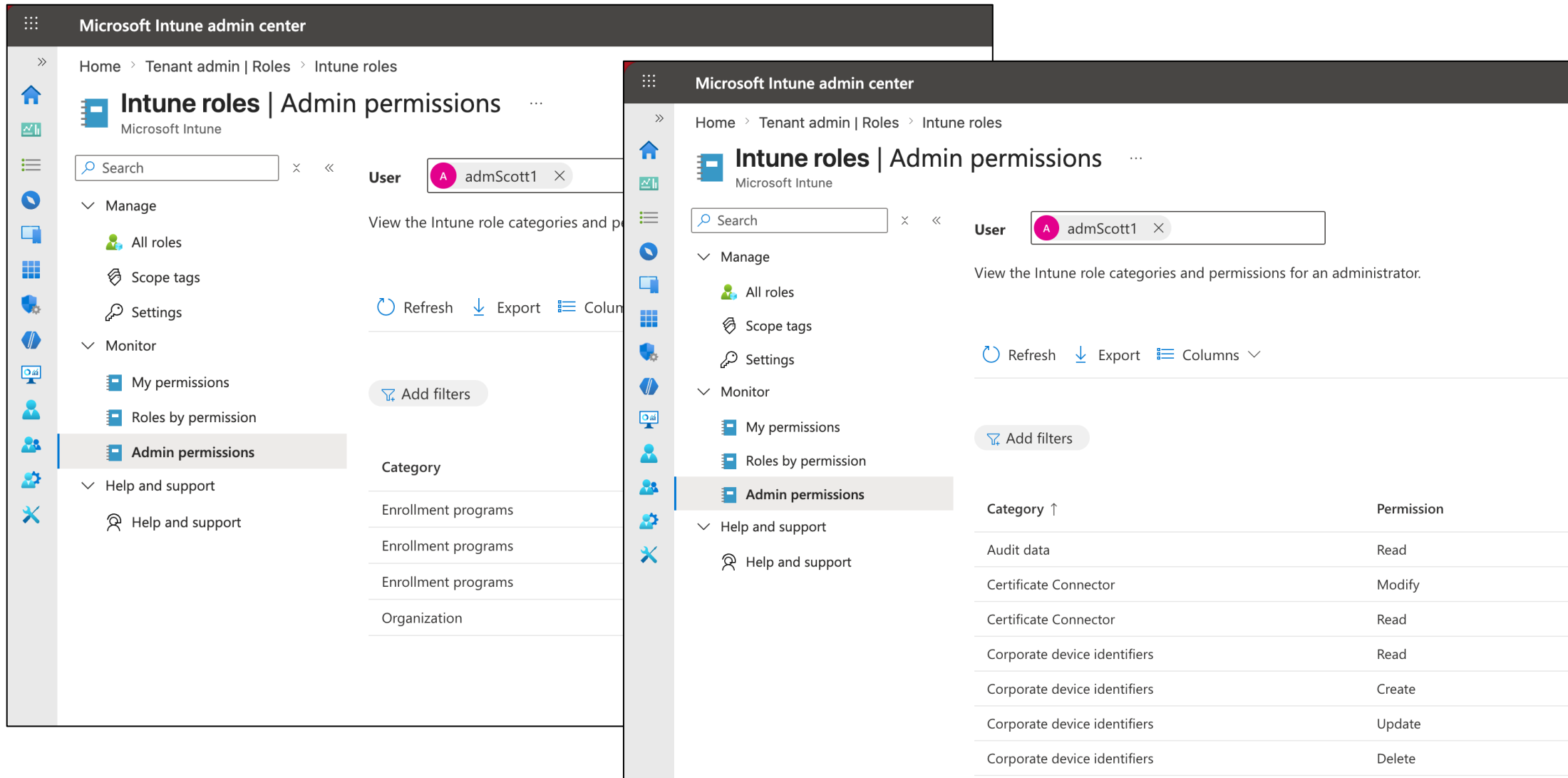
The screenshot displays the Microsoft Intune admin center interface. The left sidebar shows the navigation menu with categories like Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Tenant admin | Multi Admin Approval' and shows a list of requests. The 'Test Script - Assign' request is highlighted, showing details such as Resource type (PowerShell script), Operation (Assign), Requested by (AdeleV@c4a8ando.com), Requested on (4/9/2026, 8:10:12 AM), Request expires on (4/12/2026, 8:10:12 AM), Business justification (Test), and Status (Needs approval).

The 'Script assignments changes' section shows a JSON payload for a device management script assignment:

```
1+ [
2+ {
3+   "@odata.type": "microsoft.graph.DeviceManagementScriptAssignment",
4+   "target": {
5+     "@odata.type": "microsoft.graph.GroupAssignmentTarget",
6+     "deviceAndAppManagementAssignmentFilterType": "None",
7+     "groupId": "8057dfea-0dd6-4c40-87d8-1d11336beb95",
8+     "groupName": "ddg_Lab-Tier2.User.Devices"
9+   }
10+ }
11+ ]
```

The 'Approver notes' section is empty, and the bottom of the modal shows the text 'You may approve or reject this request if you have approver permission.' with buttons for 'Approve request' and 'Reject request'.

Detection/Mitigation: Visibility on Intune RBAC



The image displays two screenshots of the Microsoft Intune admin center, specifically the 'Intune roles | Admin permissions' page. The left screenshot shows the page with a search bar and a user filter set to 'admScott1'. The right screenshot shows the same page with a table of permissions for the user 'admScott1'.

Microsoft Intune admin center

Home > Tenant admin | Roles > Intune roles

Intune roles | Admin permissions

Microsoft Intune

Search

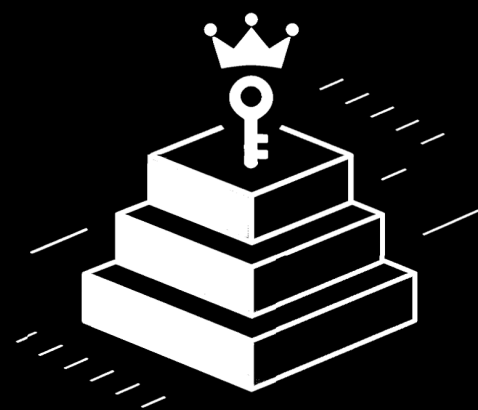
User: admScott1

View the Intune role categories and permissions for an administrator.

Refresh Export Columns

Add filters

Category	Permission
Audit data	Read
Certificate Connector	Modify
Certificate Connector	Read
Corporate device identifiers	Read
Corporate device identifiers	Create
Corporate device identifiers	Update
Corporate device identifiers	Delete



EntraOps

What is EntraOps?



Classify

Classification template incl. dynamic updates on critical scopes of your privileged assets

Identify

Analyze role assignments by role actions and scope and apply classification on privileged objects

Protect

Apply Administrative Unit membership for restricted management of unprotected objects

Monitor

Export data as JSON and ingest to Microsoft Sentinel for monitoring and entity enrichment

Reporting

Reporting of classified privileged objects and their role assignments in Azure Workbooks

Open Source, PowerShell Module with GitHub Template
runs **locally** in an interactive session, inside **CI/CD pipelines**, in **serverless** environments,
or on any other platform where PowerShell Core is supported

What is Control Plane (Tier0)?

```
[
{
  "EAMTierLevelName": "ControlPlane",
  "EAMTierLevelTagValue": "0",
  "TierLevelDefinition": [
    {
      "Category": "Microsoft.DeviceManagement",
      "Service": "Privileged IAM",
      "RoleAssignmentScopeName": [
        "/"
      ],
      "ExcludedRoleAssignmentScopeName": [],
      "RoleDefinitionActions": [
        "Microsoft.Intune/Roles/Assign",
        "Microsoft.Intune/Roles/Create",
        "Microsoft.Intune/Roles/Delete",
        "Microsoft.Intune/Roles/Update"
      ]
    }
  ]
}
]
```

full access to modify Intune RBAC

assignment (only) on Intune Tenant Level

What is Control Plane (Tier0)?

```
[
{
  "EAMTierLevelName": "ControlPlane",
  "EAMTierLevelTagValue": "0",
  "TierLevelDefinition": [
    {
      "Category": "Microsoft.DeviceManagement",
      "Service": "Global Device Enrollment Management",
      "RoleAssignmentScopeName": [
        "/*"
      ],
      "ExcludedRoleAssignmentScopeName": [],
      "RoleDefinitionActions": [
        "Microsoft.Intune/AppleDeviceSerialNumbers/Create",
        "Microsoft.Intune/AppleDeviceSerialNumbers/Delete",
        "Microsoft.Intune/AppleDeviceSerialNumbers/Update",
        "Microsoft.Intune/CorporateDeviceIdentifiers/Create",
        "Microsoft.Intune/CorporateDeviceIdentifiers/Delete",
        "Microsoft.Intune/CorporateDeviceIdentifiers/Update",
        "Microsoft.Intune/DeviceEnrollmentManagers/Update",
        "Microsoft.Intune/EnrollmentProfiles/EnrollmentTimeMembershipAssign",
        "Microsoft.Intune/EnrollmentProgramToken/Create",
        "Microsoft.Intune/EnrollmentProgramToken/Delete",
        "Microsoft.Intune/EnrollmentProgramToken/Update"
      ]
    }
  ]
}
]
```

access to modify Autopilot Device Objects

all assignment scopes (non-scopeable)

What is Control Plane (Tier0)?

```
[
{
  "EAMTierLevelName": "ControlPlane",
  "EAMTierLevelTagValue": "0",
  "TierLevelDefinition": [
    {
      "Category": "Microsoft.DeviceManagement",
      "Service": "Global Endpoint Policy Management",
      "RoleAssignmentScopeName": [
        "/"
      ],
      "ExcludedRoleAssignmentScopeName": [],
      "RoleDefinitionActions": [
        "Microsoft.Intune/DeviceCompliancePolicies/Assign",
        "Microsoft.Intune/DeviceCompliancePolicies/Create",
        "Microsoft.Intune/DeviceCompliancePolicies/Delete",
        "Microsoft.Intune/DeviceCompliancePolicies/Update",
        "Microsoft.Intune/DeviceConfigurations/Assign",
        "Microsoft.Intune/DeviceConfigurations/Create",
        "Microsoft.Intune/DeviceConfigurations/Delete",
        "Microsoft.Intune/DeviceConfigurations/Update"
      ]
    }
  ]
}
]
```

modify Device Configuration and Policies on every device

assignment on Intune Tenant Level without scopes

What is Control Plane (Tier0)?

```
[
{
  "EAMTierLevelName": "ControlPlane",
  "EAMTierLevelTagValue": "0",
  "TierLevelDefinition": [
    {
      "Category": "Microsoft.DeviceManagement",
      "Service": "Privileged Endpoint Policy Management",
      "RoleAssignmentScopeName": [
        <Tier0IncludedGroupIds>,
        <Tier1IncludedGroupIds>
      ],
      "ExcludedRoleAssignmentScopeName": [],
      "RoleDefinitionActions": [
        "Microsoft.Intune/DeviceCompliancePolicies/Assign",
        "Microsoft.Intune/DeviceCompliancePolicies/Create",
        "Microsoft.Intune/DeviceCompliancePolicies/Delete",
        "Microsoft.Intune/DeviceCompliancePolicies/Update",
        "Microsoft.Intune/DeviceConfigurations/Assign",
        "Microsoft.Intune/DeviceConfigurations/Create",
        "Microsoft.Intune/DeviceConfigurations/Delete",
        "Microsoft.Intune/DeviceConfigurations/Update"
      ]
    }
  ]
}
]
```

modify Device Configuration and Policies on PAW devices

assignment on scope groups which includes device objects of Control Plane and Management Plane users
→ Who is owner of devices? Who is privileged user?

What is Control Plane (Tier0)?

```
[
{
  "EAMTierLevelName": "ManagementPlane",
  "EAMTierLevelTagValue": "1",
  "TierLevelDefinition": [
    {
      "Category": "Microsoft.DeviceManagement",
      "Service": "User Endpoint Policy Management",
      "RoleAssignmentScopeName": [
        "/*"
      ],
      "ExcludedRoleAssignmentScopeName": [
        "/",
        <Tier0IncludedGroupIds>,
        <Tier1IncludedGroupIds>
      ],
      "RoleDefinitionActions": [
        "Microsoft.Intune/DeviceCompliancePolicies/Assign",
        "Microsoft.Intune/DeviceCompliancePolicies/Create",
        "Microsoft.Intune/DeviceCompliancePolicies/Delete",
        "Microsoft.Intune/DeviceCompliancePolicies/Update",
        "Microsoft.Intune/DeviceConfigurations/Assign",
        "Microsoft.Intune/DeviceConfigurations/Create",
        "Microsoft.Intune/DeviceConfigurations/Delete",
        "Microsoft.Intune/DeviceConfigurations/Update"
      ]
    }
  ]
}
]
```

modify Device Configuration and Policies on Non-PAW devices

assignment on every scope

except assignments without scope or scope groups which includes device objects of Control Plane and Management Plane users

EntraOps Automated Classification

✓ Get updated scope for definition of Control Plane in Entra ID

57s

```

415 -----
416 Filtering Groups by Intune Scope Tag Assignments
417 -----
418
419 Tier 0 (ControlPlane) groups with scope tag assignments:
420   ddg_Lab-Tier0.SAW.Devices (eb2e4591-19d1-4b3b-8751-d701c2d7c8e5) [EAMTierLevelName: ControlPlane (device)] -> ScopeTag(s): Tier0.SAW, Tier1.SAW
421   ddg_Lab-Tier2.User.Devices (f068c58c-f5d6-4171-be34-29cfae49d516) [EAMTierLevelName: ControlPlane (device)] -> ScopeTag(s): Tier2.User
422   dug_AAD.PrivilegedAccounts (76d5d44b-022e-4656-b698-b3f57be7c2ae) [EAMTierLevelName: ControlPlane (user)] -> ScopeTag(s): Tier0.SAW, Tier1.SAW
423   dug_AAD.Tier0.PrivilegedAccounts (0912a409-a233-4477-9a0f-1d9ac3d6f74c) [EAMTierLevelName: ControlPlane (user)] -> ScopeTag(s): Tier0.SAW
424 Tier 1 (ManagementPlane) groups with scope tag assignments:
425   ddg_Lab-Tier0.SAW.Devices (eb2e4591-19d1-4b3b-8751-d701c2d7c8e5) [EAMTierLevelName: ManagementPlane (device)] -> ScopeTag(s): Tier0.SAW, Tier1.SAW
426   ddg_Lab-Tier1.SAW.Devices (f70a2e17-1d96-4c01-987e-c4762d02d6ba) [EAMTierLevelName: ManagementPlane (device)] -> ScopeTag(s): Tier1.SAW, Tier0.SAW
427   dug_AAD.PrivilegedAccounts (76d5d44b-022e-4656-b698-b3f57be7c2ae) [EAMTierLevelName: ManagementPlane (user)] -> ScopeTag(s): Tier0.SAW, Tier1.SAW
428   dug_AAD.Tier1.PrivilegedAccounts (205de7a7-c20c-4f7d-bad0-6f5f97d90594) [EAMTierLevelName: ManagementPlane (user)] -> ScopeTag(s): Tier1.SAW
429
430 -----
431 Replacing DeviceManagement Scope Placeholders (GroupIds)
432 -----
433   <Tier0IncludedGroupIds> -> "0912a409-a233-4477-9a0f-1d9ac3d6f74c", "76d5d44b-022e-4656-b698-b3f57be7c2ae", "eb2e4591-19d1-4b3b-8751-d701c2d7c8e5",
" f068c58c-f5d6-4171-be34-29cfae49d516 "
434   <Tier1IncludedGroupIds> -> "205de7a7-c20c-4f7d-bad0-6f5f97d90594", "76d5d44b-022e-4656-b698-b3f57be7c2ae", "eb2e4591-19d1-4b3b-8751-d701c2d7c8e5",
" f70a2e17-1d96-4c01-987e-c4762d02d6ba "
435   Output file: /home/runner/work/EntraOps/EntraOps/Classification/cloudlab.onmicrosoft.com/Classification_DeviceManagement.json
436
437 -----
438 DeviceManagement Classification Summary
439 -----
440
441 Groups in scope (reason = EAMTierLevelName of members):
442   CloudLab (9ac13ba2-c878-4771-8819-26baf0006c15) [EAMTierLevelName: ControlPlane (user), ManagementPlane (user)]
443   ddg_Lab-Tier0.SAW.Devices (eb2e4591-19d1-4b3b-8751-d701c2d7c8e5) [EAMTierLevelName: ControlPlane (device), ManagementPlane (device)]
444   ddg_Lab-Tier2.User.Devices (f068c58c-f5d6-4171-be34-29cfae49d516) [EAMTierLevelName: ControlPlane (device)]

```

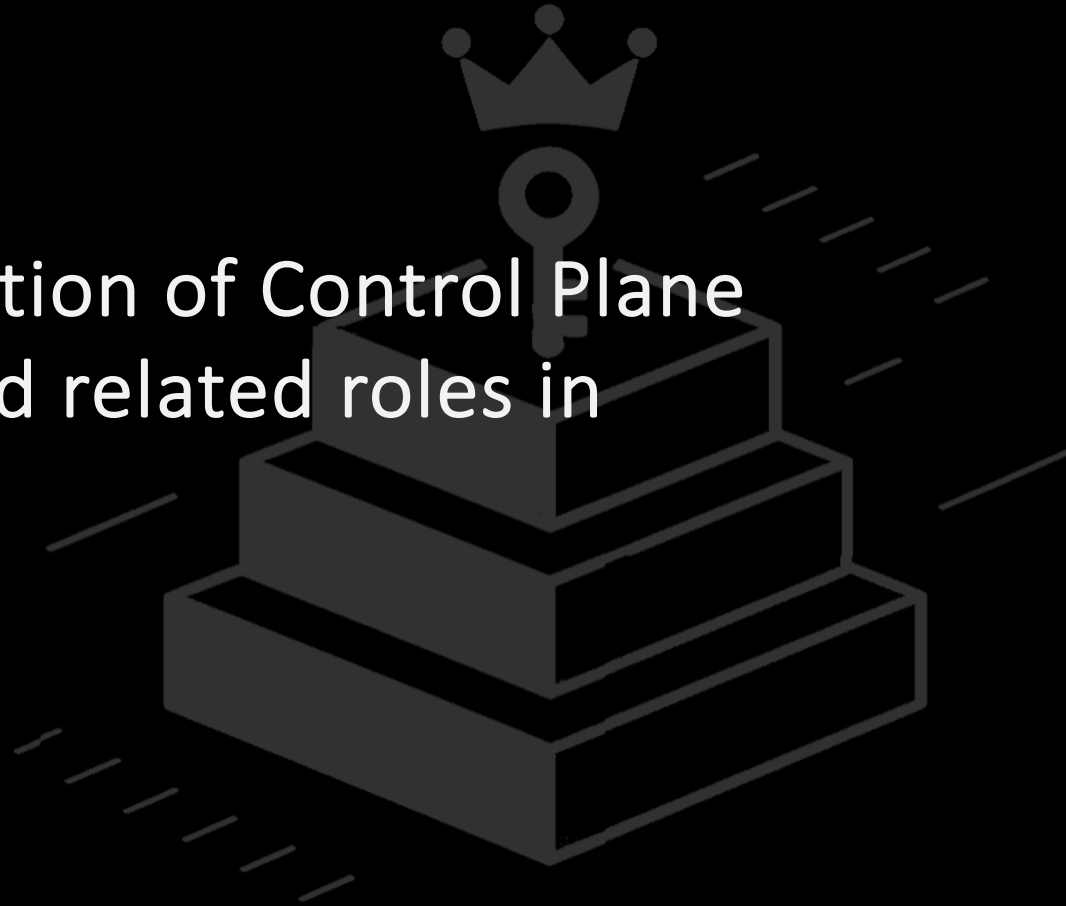
Applied Automated Classification to Roles

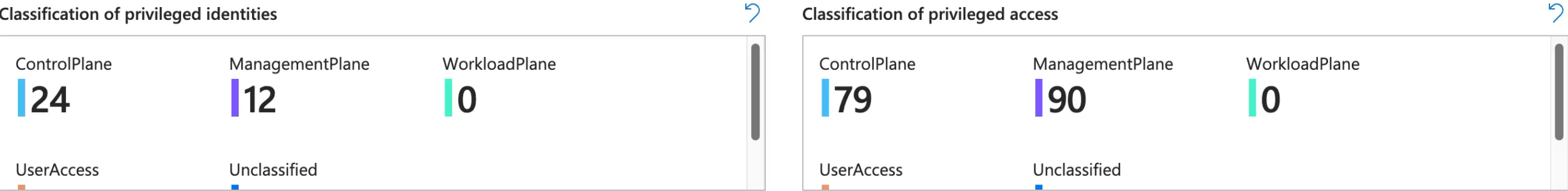
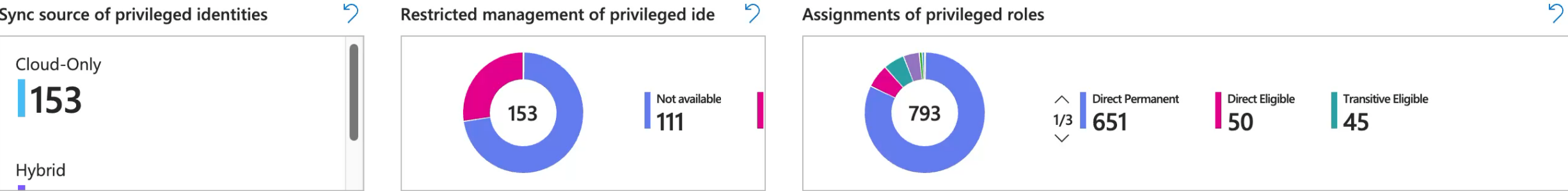
```
Classification/cloudlab.onmicrosoft.com/Classification_DeviceManagement.json
... @@ -1,1001 +1,1002 @@
"EAMTierLevelTagValue": "0",
"TierLevelDefinition": [
  {
    "Category": "Microsoft.DeviceManagement",
    "Service": "Privileged Endpoint Policy Management",
    "RoleAssignmentScopeName": [
      "0912a409-a233-4477-9a0f-1d9ac3d6f74c",
      "76d5d44b-022e-4656-b698-b3f57be7c2ae",
      "eb2e4591-19d1-4b3b-8751-d701c2d7c8e5",
      "f068c58c-f5d6-4171-be34-29cfae49d516",
      "205de7a7-c20c-4f7d-bad0-6f5f97d90594",
      "76d5d44b-022e-4656-b698-b3f57be7c2ae",
      "eb2e4591-19d1-4b3b-8751-d701c2d7c8e5",
      "f70a2e17-1d96-4c01-987e-c4762d02d6ba"
    ],
    "ExcludedRoleAssignmentScopeName": [],
    "RoleDefinitionActions": [
      "Microsoft.Intune/DeviceCompliancePolicies/Assign",
      "Microsoft.Intune/DeviceCompliancePolicies/Create",
      "Microsoft.Intune/DeviceCompliancePolicies/Delete",
      "Microsoft.Intune/DeviceCompliancePolicies/Update",
      "Microsoft.Intune/DeviceConfigurations/Assign",
      "Microsoft.Intune/DeviceConfigurations/Create",
      "Microsoft.Intune/DeviceConfigurations/Delete",
      "Microsoft.Intune/DeviceConfigurations/Update"
    ]
  }
],
},
```

```
PrivilegedEAM/DeviceManagement/user/6e68479a-153b-4088-bcaf-661d2d327b7d.json
... @@ -54,6 +54,11 @@
54 54 "AdminTierLevelName": "ControlPlane",
55 55 "Service": "Privileged Endpoint Management"
56 56 },
57 + {
58 + "AdminTierLevel": "0",
59 + "AdminTierLevelName": "ControlPlane",
60 + "Service": "Privileged Endpoint Policy Management"
61 + },
57 62 {
58 63 "AdminTierLevel": "0",
59 64 "AdminTierLevelName": "ControlPlane",
... @@ -155,6 +160,19 @@
155 160 },
156 161 "TaggedByRoleSystem": "ScopeTagAssignedGroup"
157 162 },
163 + {
164 + "AdminTierLevel": "0",
165 + "AdminTierLevelName": "ControlPlane",
166 + "Service": "Privileged Endpoint Policy Management",
167 + "TaggedBy": "JSONwithAction",
168 + "TaggedByObjectIds": [
169 + "f068c58c-f5d6-4171-be34-29cfae49d516"
170 + ],
171 + "TaggedByObjectDisplayNames": [
172 + "ddg_Lab-Tier2.User.Devices"
173 + ],
174 + "TaggedByRoleSystem": "ScopeTagAssignedGroup"
175 + },
```

DEMO

Classification of Control Plane
Scope and related roles in
EntraOps





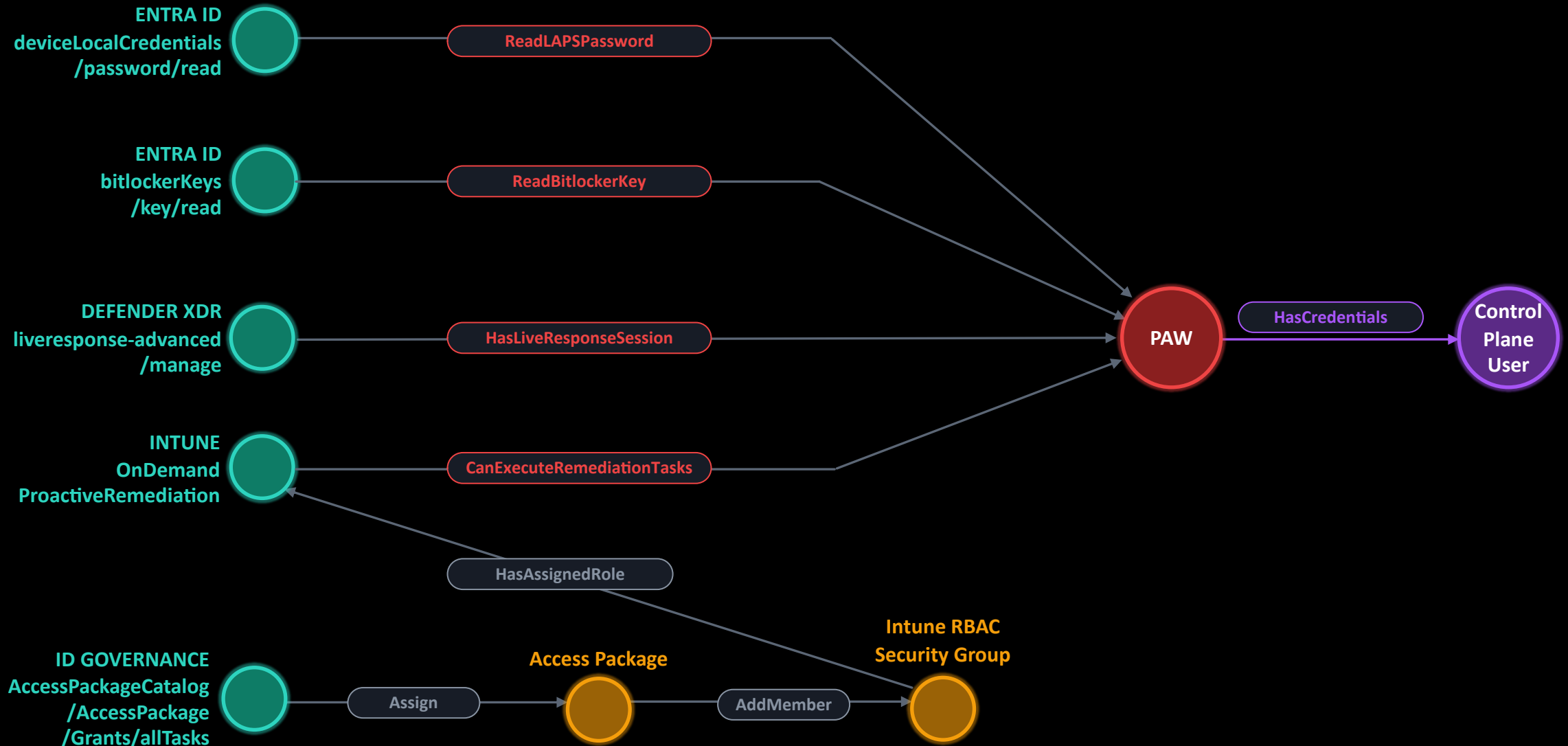
List of Privileged Assets

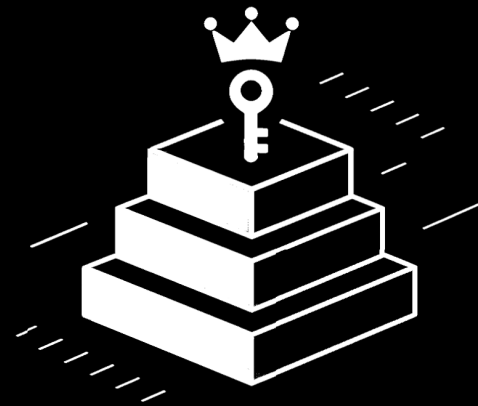
ObjectType	ObjectSubType	ObjectDisplayName	ObjectAdminTierLevelName	RestrictedManagement	ObjectId
Service Principal	Application	AAD Lifecycle Management	Unclassified	Not available	f0c73789-c...
Service Principal	Application	ASPADev	Unclassified	Not available	5892a25b-b...
Service Principal	AgentIdentityBlueprintPrincipal	App Lifecycle Management Agent Blueprint - Prod	Unclassified	Not available	0d06dba3-b...
Service Principal	Application	AzADServicePrincipalInsights	Unclassified	Not available	df91eeca-9...
Service Principal	Application	AzGovViz	Management Plane	Not available	4434a136-b...
Service Principal	Application	AzSentinel-Playbook-LAQuery	Management Plane	Not available	1c334d68-b...
Service Principal	Application	Azure AD Assessment	Unclassified	Not available	183200a2-b...

EntraOps and Sentinel Integration

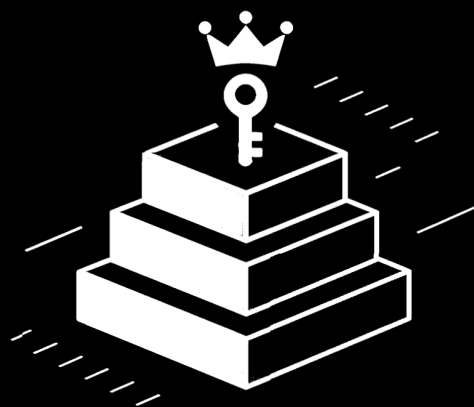
TimeGenerated [UTC]	2026-04-25T09:41:55.4377Z
ActorUpn	admsscott1@lab.cloud-architekt.net
ActorAdminTierLevel	1
OperationName	UpdateDeviceProperties WindowsAutopilotDeviceIdentity
NewScopeTag	Tier2.User
AadDeviceId	350c15b0-a02c-431c-9438-04f7d3487522
AadObjectDeviceId	aee4855e-d083-4ca7-b5df-4c1717567536
ZtdDeviceId	8fbbb7f5-194c-4e95-9e8c-2fb22db56717
AadCorrelationId	ec3bb27c-b5aa-44c1-b35f-aa40ddec1931
▼ ActorPermissions	["Microsoft.Intune/AppleDeviceSerialNumbers/Update","Microsoft.Intune/AppleDeviceSerialNumbers/Read"]
0	Microsoft.Intune/AppleDeviceSerialNumbers/Update
1	Microsoft.Intune/AppleDeviceSerialNumbers/Read
2	Microsoft.Intune/AppleDeviceSerialNumbers/Create
3	Microsoft.Intune/Organization/Read
4	Microsoft.Intune/DefaultScopeTagEnabled/Read

Examples of (In)Direct Attack Paths

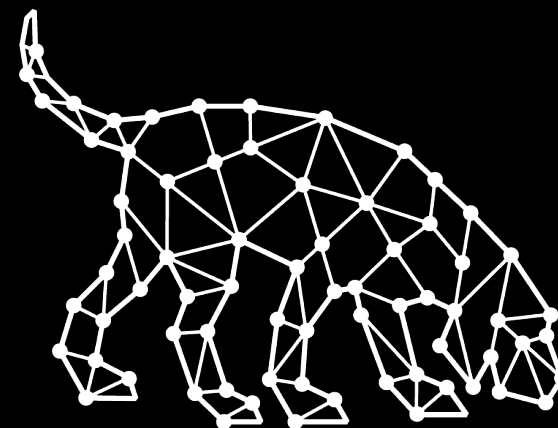




EntraOps

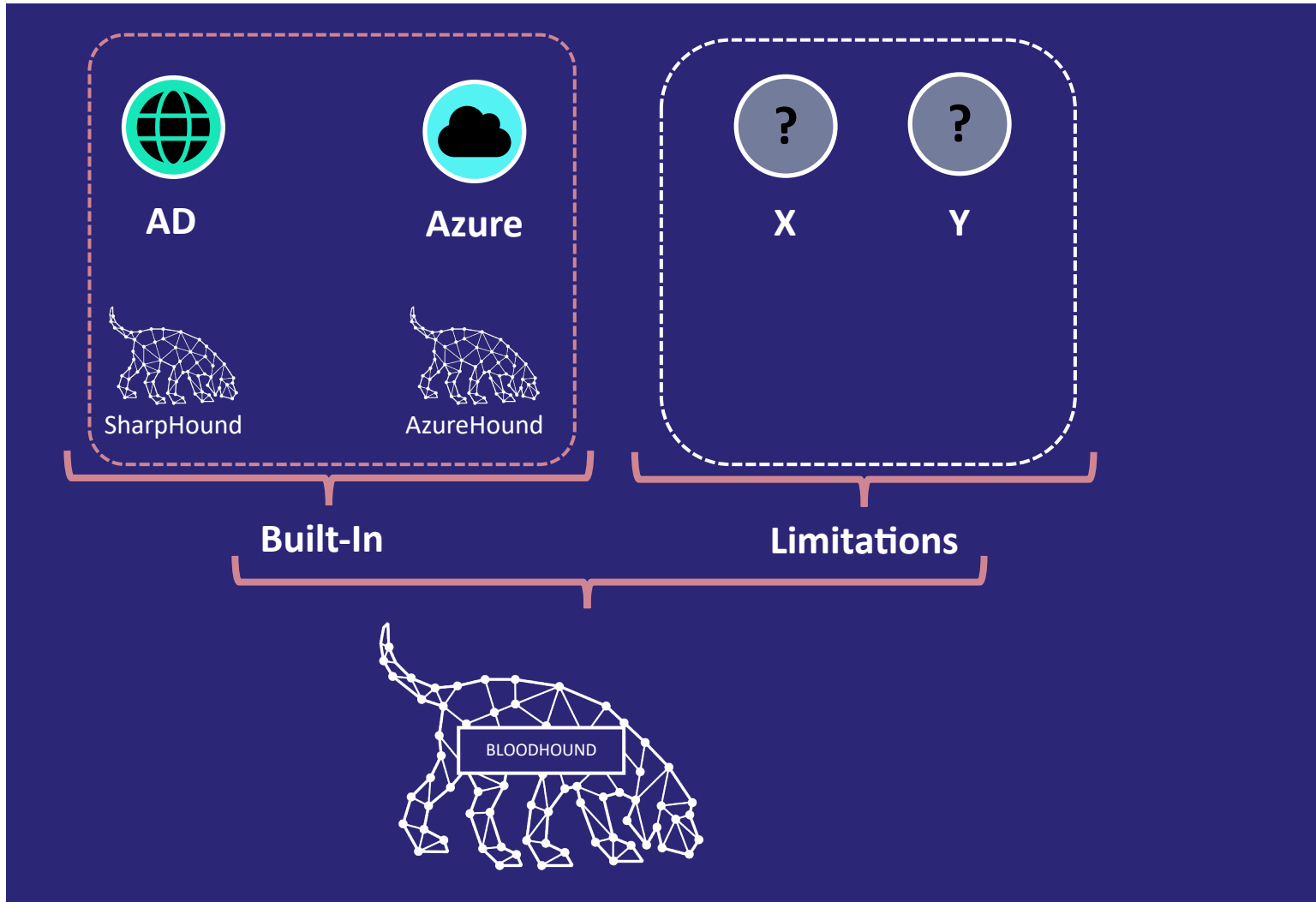


EntraOps

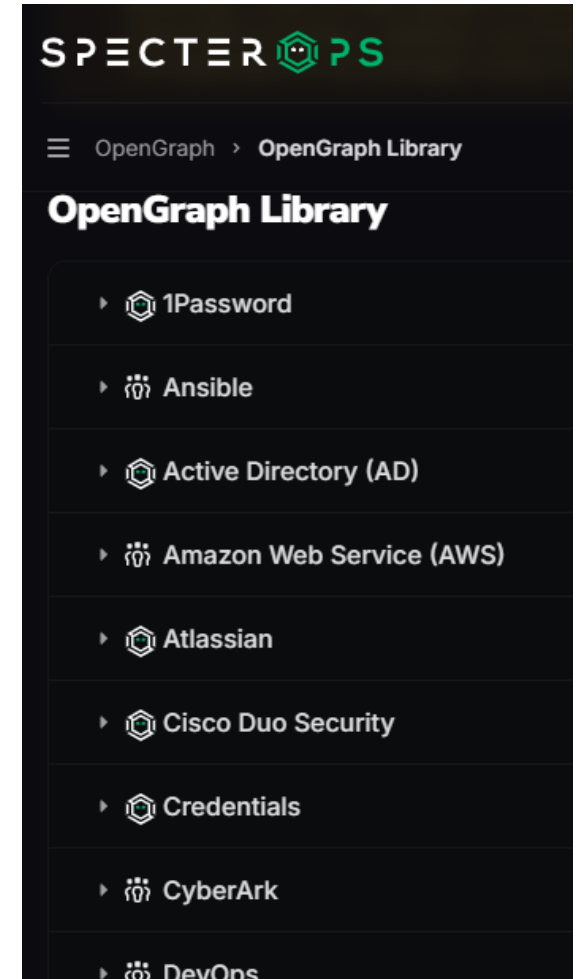
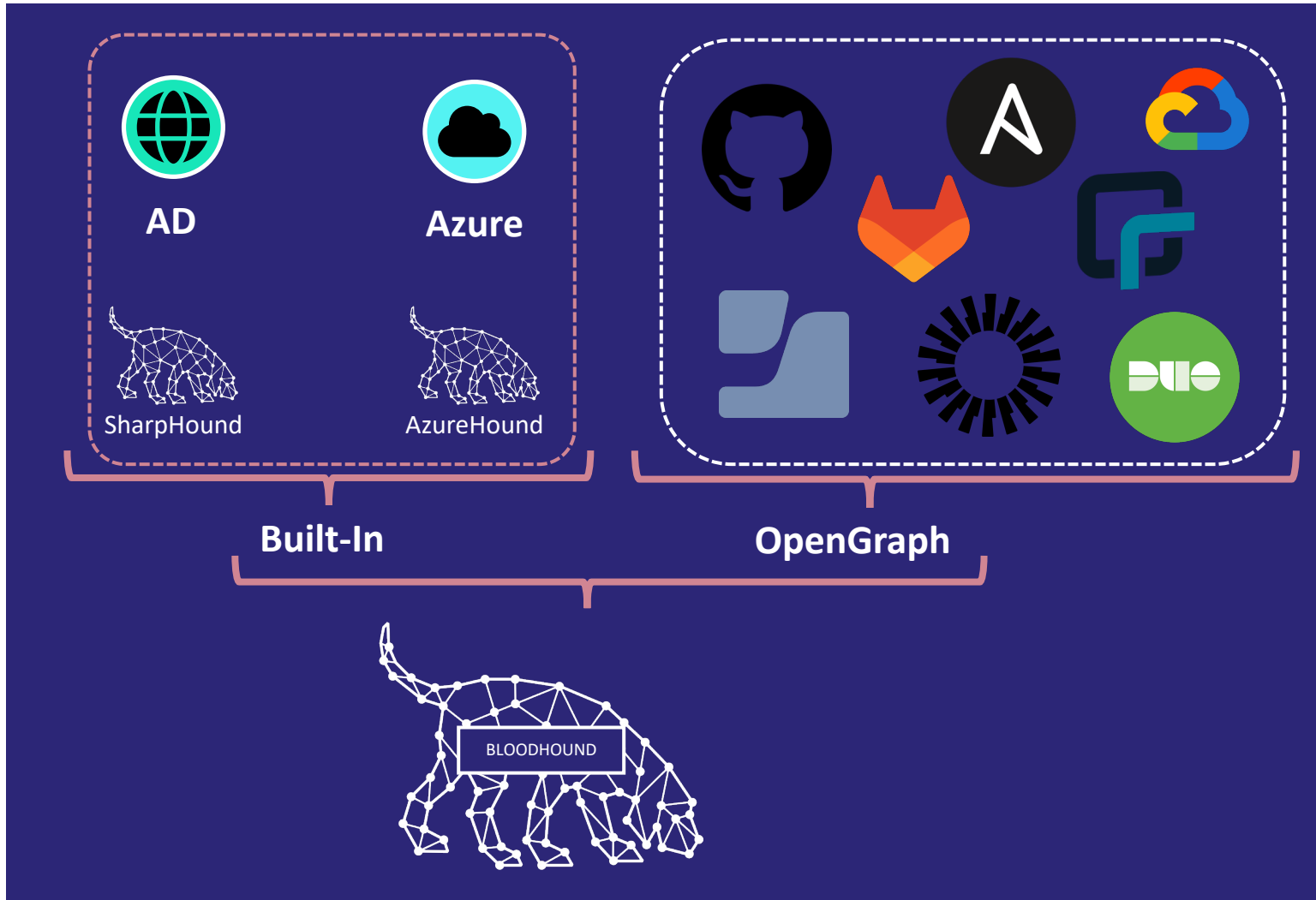


BLOODHOUND

BloodHound OpenGraph

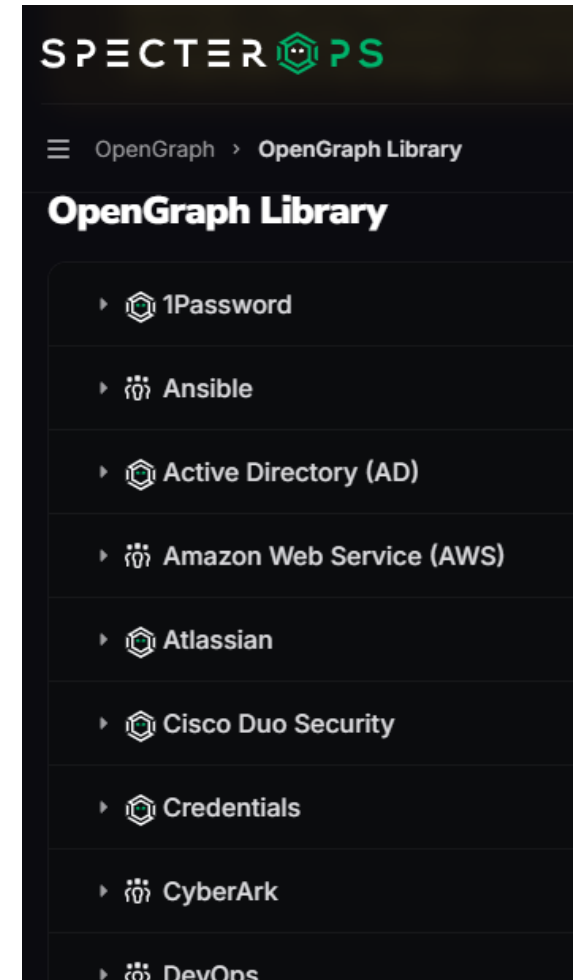
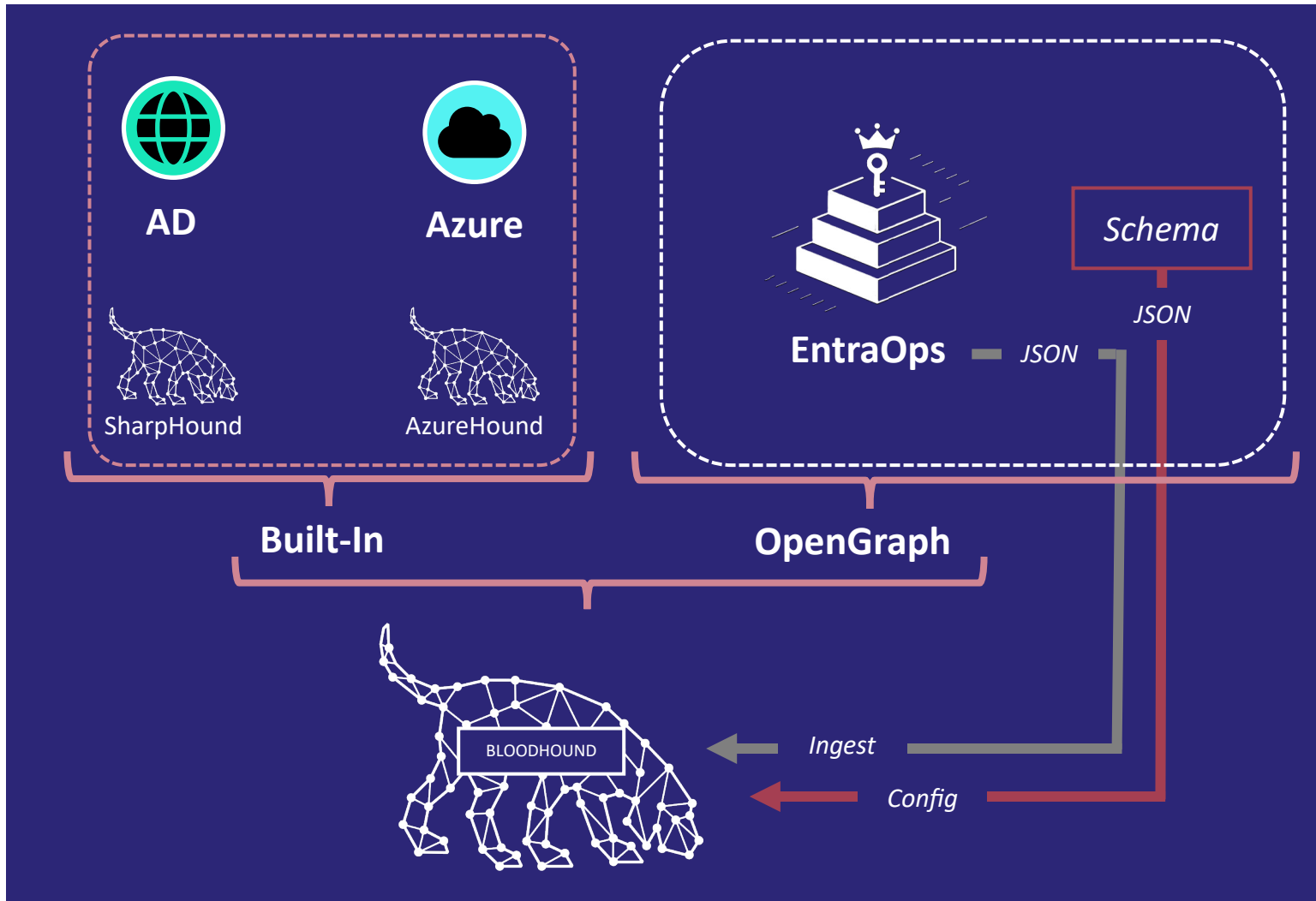


BloodHound OpenGraph



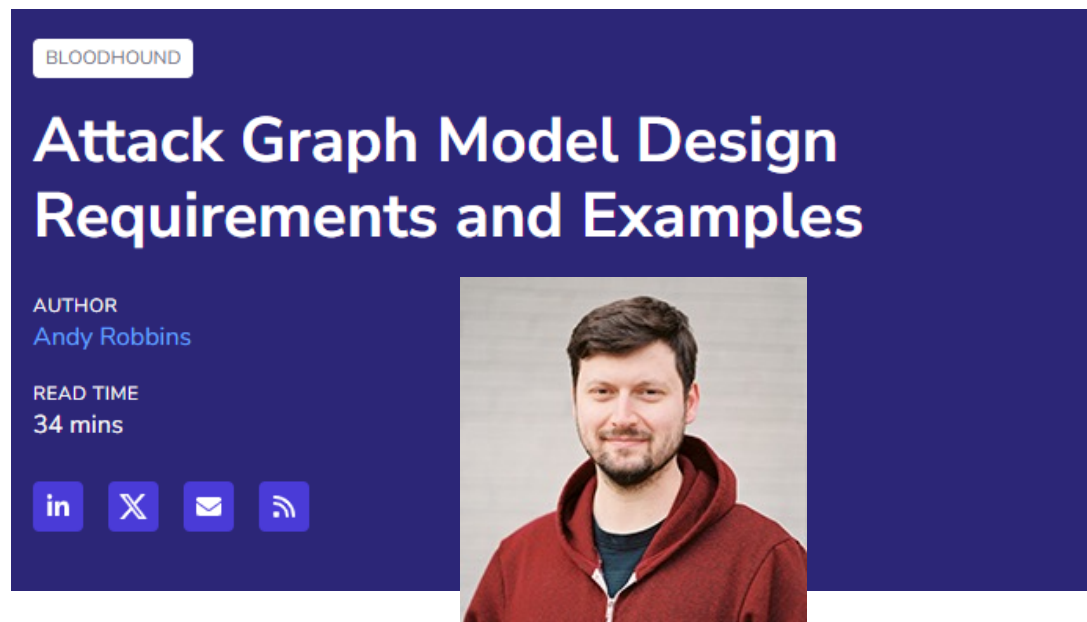
specterops.io/opengraph

BloodHound OpenGraph



specterops.io/opengraph

RBAC Model Design



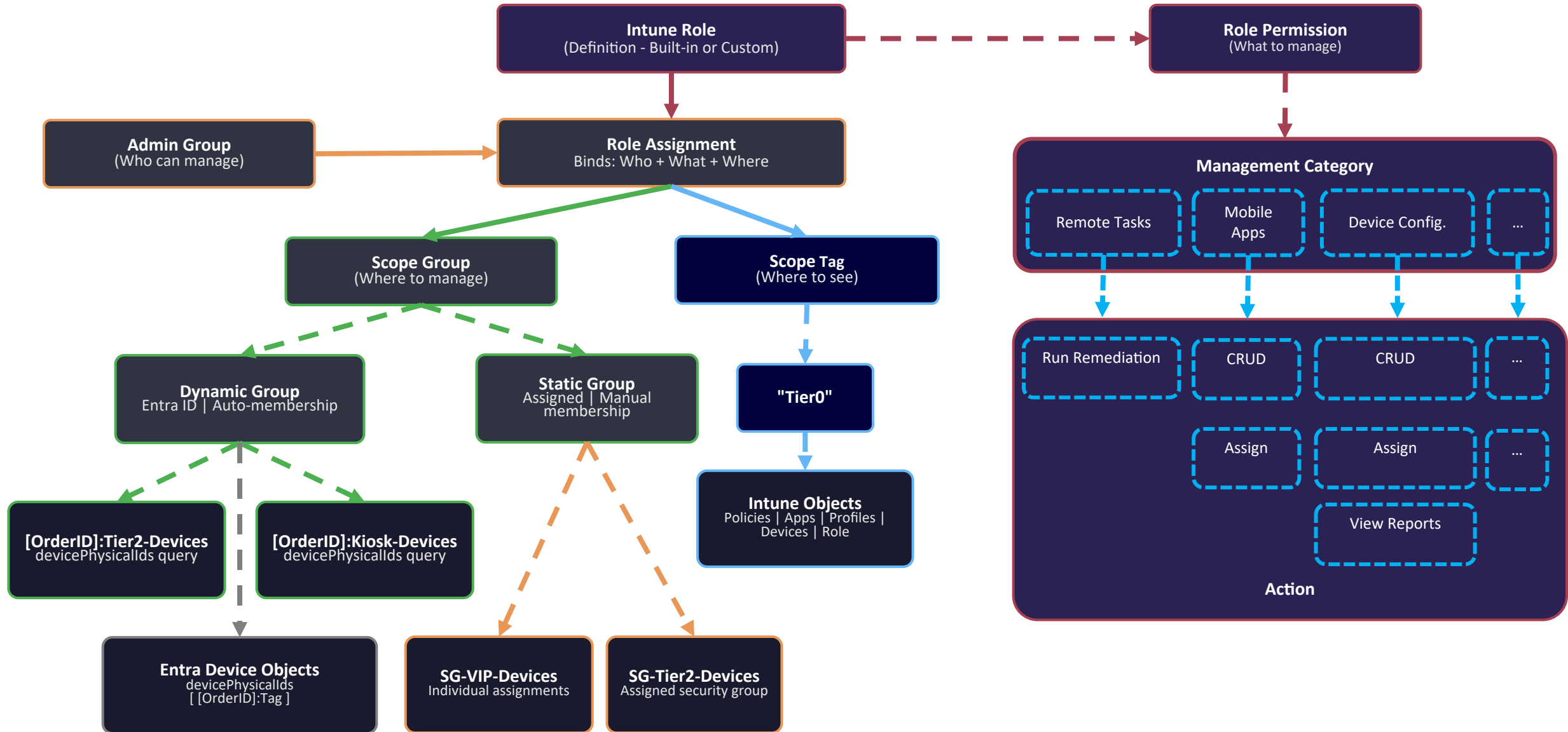
[SpecterOps Blog – Attack Graph Model Design Requirements and Examples](#)



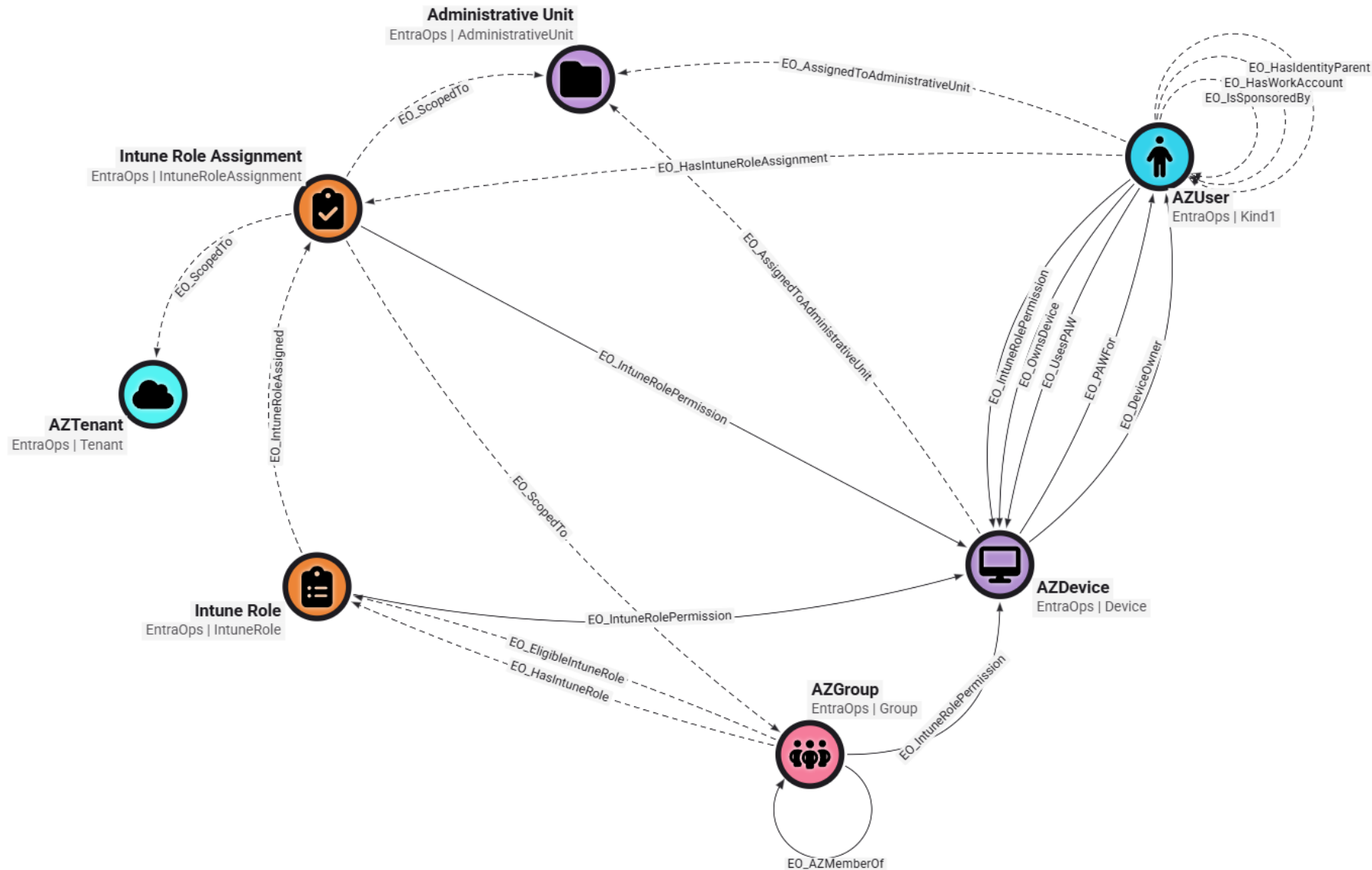
1. Shortest path calculations
2. Scoped assignments
3. Custom roles
4. Static representation of roles
5. Accurate findings and remediations

[YouTube – Mapping RBAC in BloodHound | SO-CON 26](#)

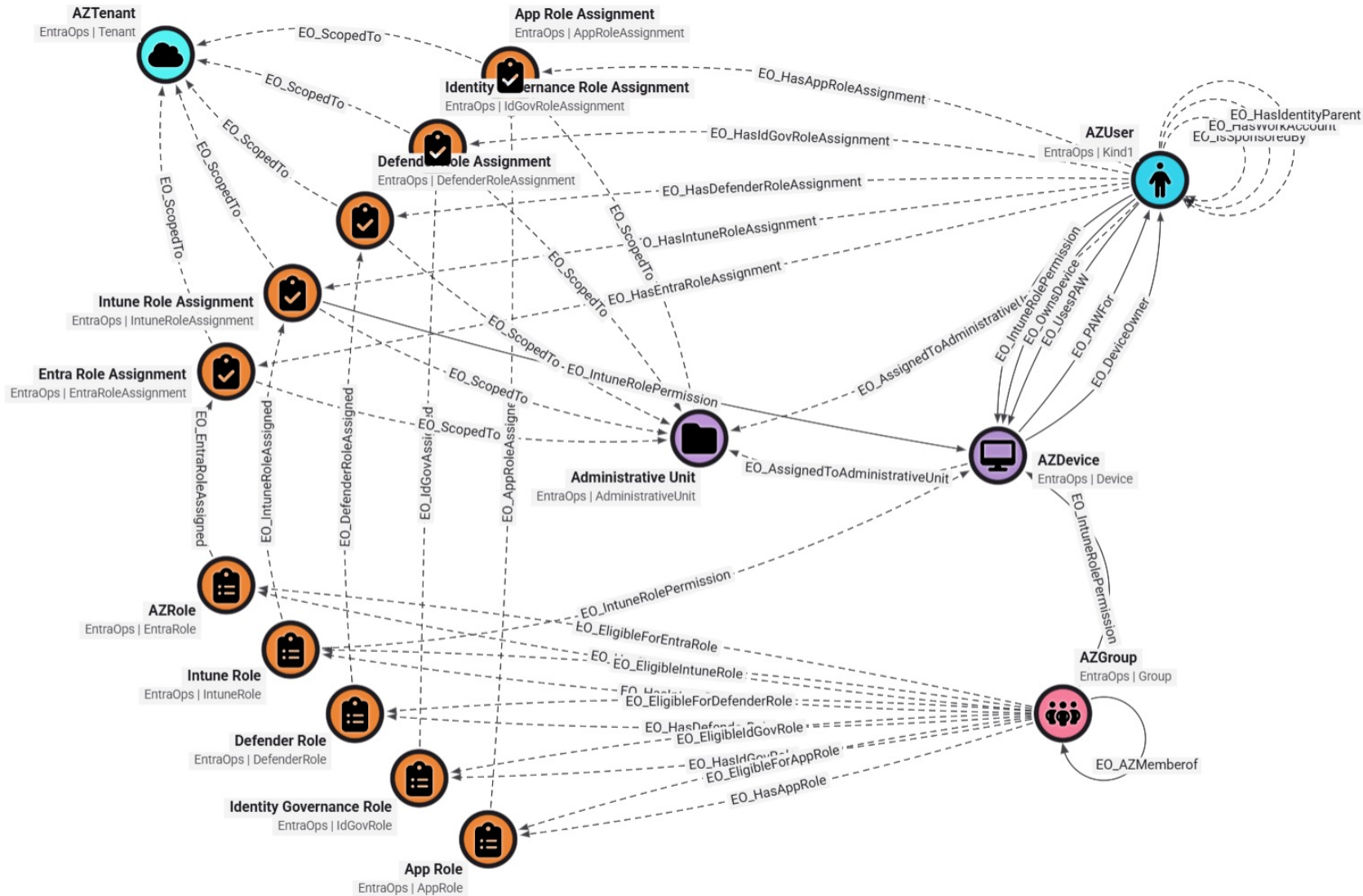
Role Assignment and Scopes



EntraOps Graph Model: Intune



EntraOps Graph Model



DEMO

BloodHound Integration of
Intune RBAC and Classification
by EntraOps





●

Start Node

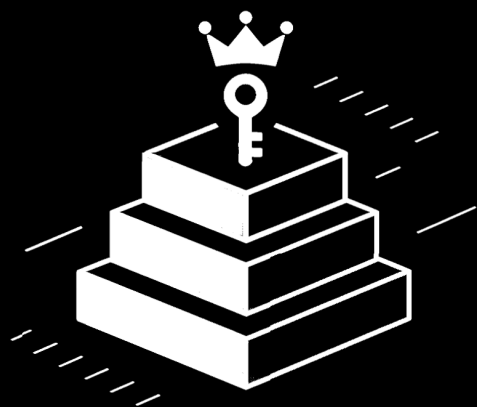
⋮

◎

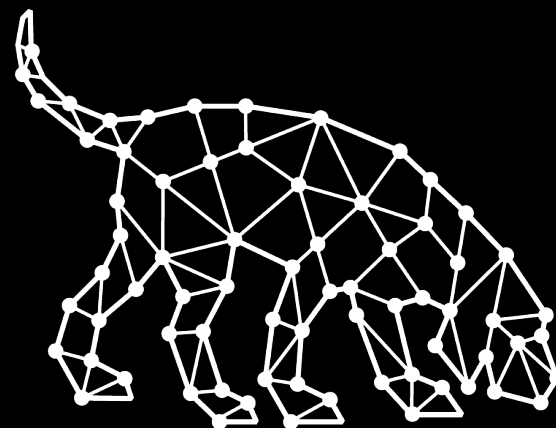
Destination Node

↕

▼



EntraOps



BLOODHOUND

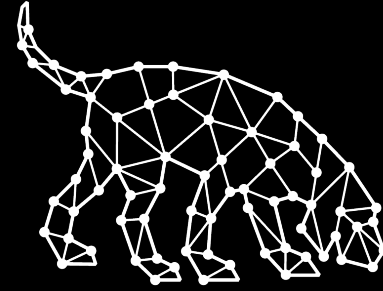


USAGE INSTRUCTIONS

Exporting EntraOps to
BloodHound OpenGraph,
schema & ingestion
guidance



EntraOps



BLOODHOUND



GRAPH MODEL

Mermaid charts detailing
legacy and modern RBAC
models

Available now

entraops.com

github.com/Cloud-Architekt/EntraOps



RBAC

Assignments: *Intune*,
Entra, *Defender*, *AppRole*,
Id Governance
Pathfinding: *Intune*



PRIVILEGE ZONE RULES

Based on EntraOps
classifications



PIM-FOR-GROUPS

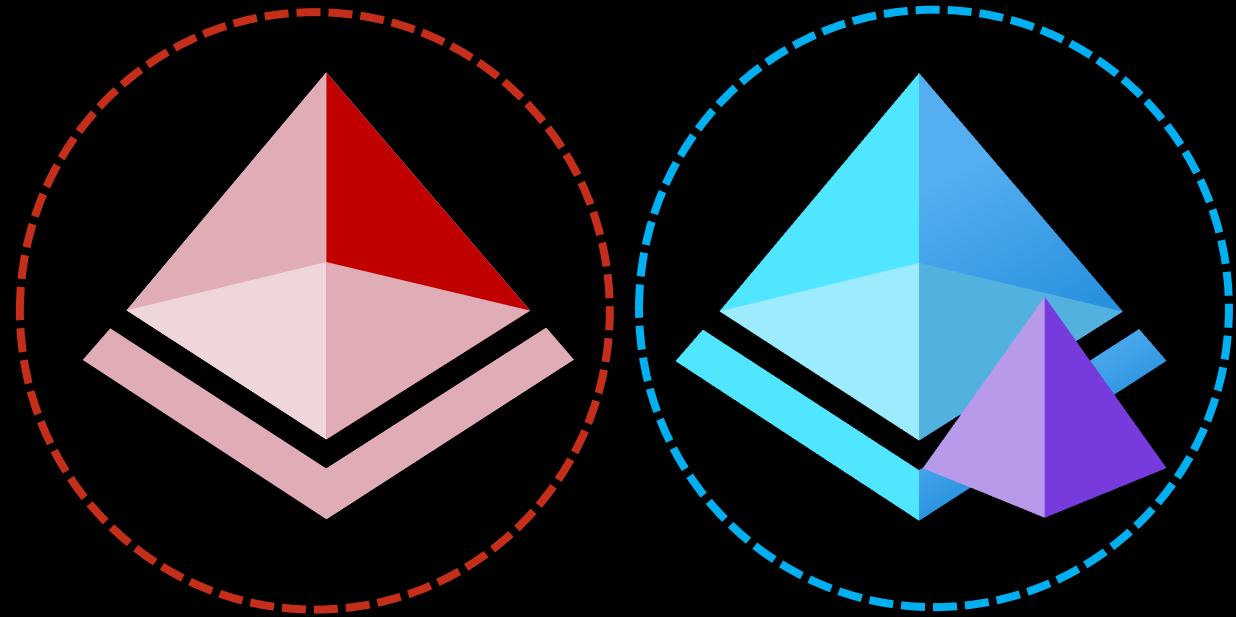
Identify and visualize
Privileged Identity
Management for groups



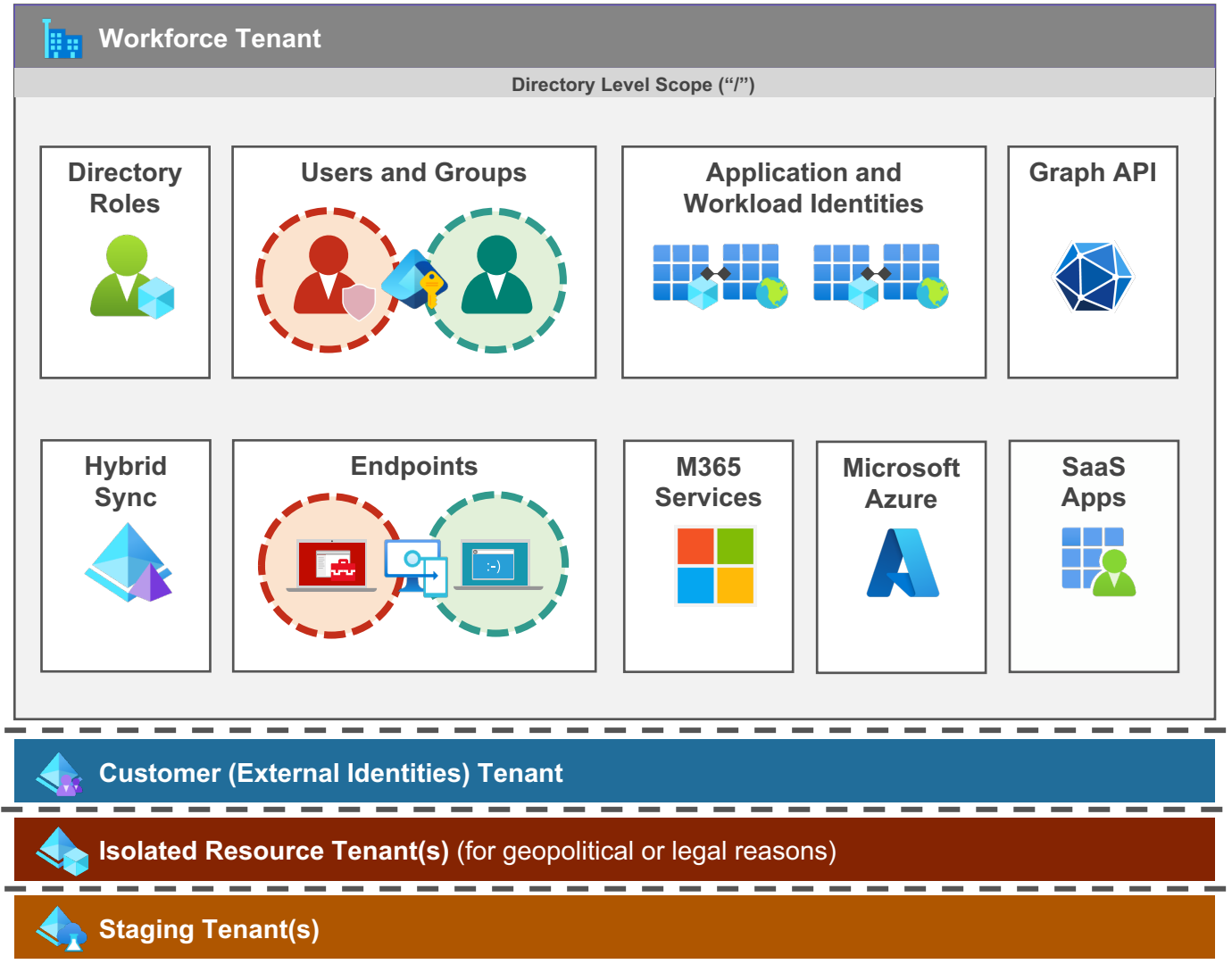
CYPHER QUERIES

Analyze direct & nested
role assignments, device
wipe privileges,
administrative units, and
more

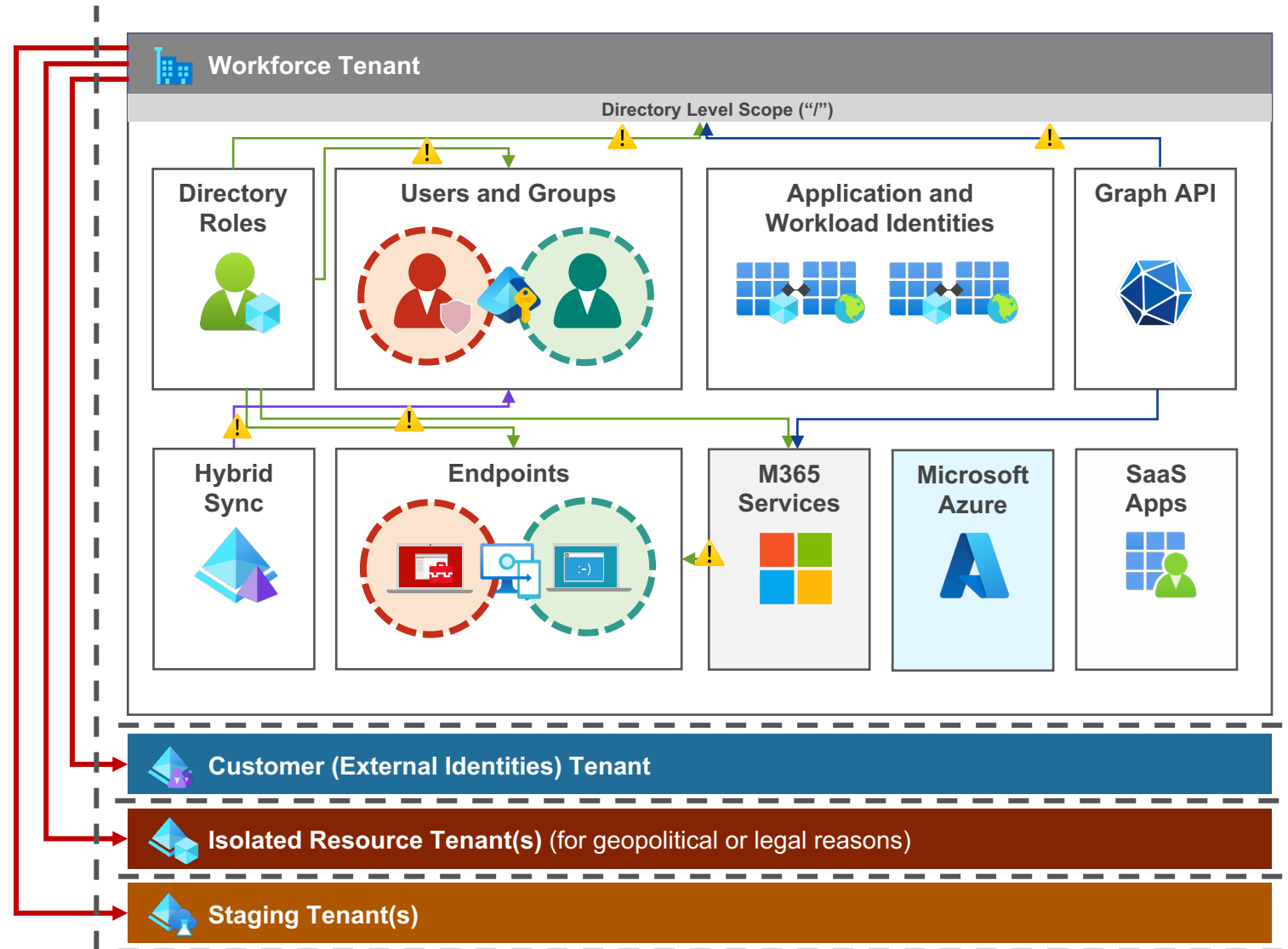
INTER-TENANT ISOLATION WITH RED TENANT



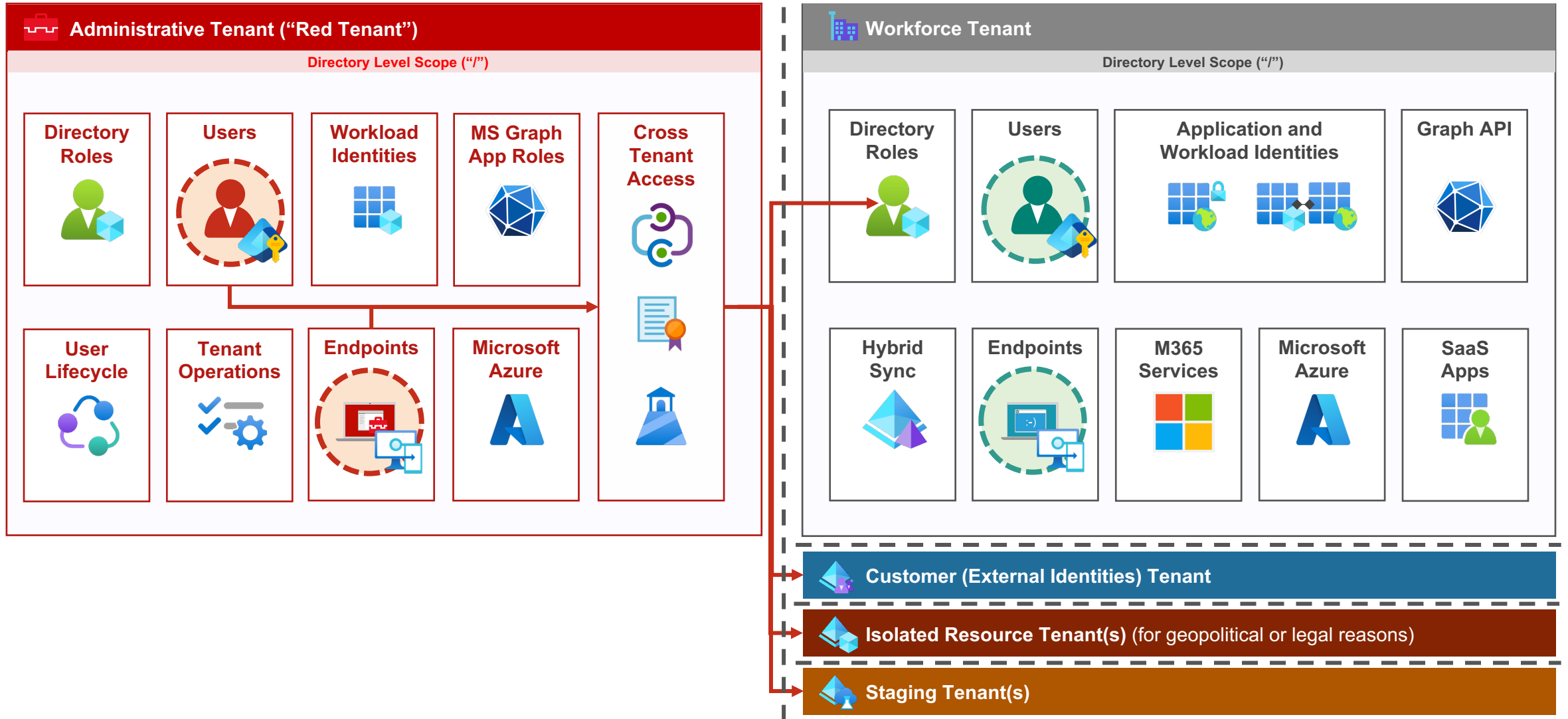
Challenges of Intra-Tenant Isolation



Challenges of Intra-Tenant Isolation



Inter-Tenant Isolation with Red Tenant



SUMMARY | DON'T BREAK YOUR TIERS



Consideration of Design and Limitations

Some Intune RBAC roles cannot be scoped, or features do not support scope tags
Limitations on RMAUs (integration to Intune RBAC, restrict first party actions)



Attack Path Detections

Analyze EntraOps output of RBAC Assignment and Classification
Integration of EntraOps in SOC for Detection, Enrichment and Reporting of Tier Breach
Discover indirect attack paths by Entra ID, Defender, Graph App or Identity Governance Roles
Identify attack paths by Intune RBAC in BloodHound and EntraOps



(Limited) Mitigation options to reduce attack surface in intra-tenant isolation

Assign only scopeable permissions to non-Tier0 administrators
Avoid dynamic assignments on attributes that can be manipulated
Implement approval flow and strict monitoring of scope assignments



Mitigation by inter-tenant isolation

Adoption of Red Tenant to take benefit of “tenant boundary” as strong and clear separation
Control Plane access from User and Devices from Red Tenant only (via strong Cross Tenant Access Policies)

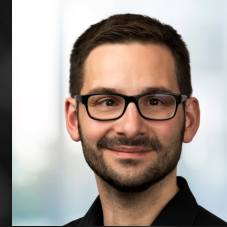
THANK YOU

Q&A



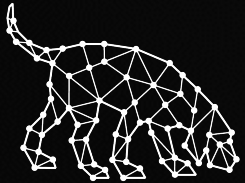
MARTIN SOHN CHRISTENSEN

@martinsohndk
martinsohn.dk



THOMAS NAUNHEIM

@glueckkanja
cloud-architekt.net



BLOODHOUND

bloodhound.specterops.io
specterops.io/opengraph



ENTRAOPS

entraops.com
github.com/Cloud-Architekt/EntraOps