Identity Master Class

February 24th, 2026

09:00 – 16:00

Experts Live Denmark

THANK YOU TO OUR AMAZING SPONSORS !

Identity Master Class - The Team

- Merill Fernando
  - Principal Product Manager, Microsoft
- Thomas Naunheim
  - Microsoft MVP | Cyber Security Architect @glueckkanja AG
- Klaus Bierschenk
  - Microsoft MVP for Security | Director Consulting Expert @CGI Germany
- Pim Jacobs
  - Microsoft MVP & Technology Lead Security @InSpark
- Jan Vidar Elven
  - Senior Architect @ Evidi, MVP Security





Agenda

- 09:00 – Start and Welcome – User Lifecycle
  - User Lifecycle Story
  - Entra ID Governance – Lifecycle Workflows
  - Lab Break 1
- 10:30 – Snacks / Fruit / Coffee
- 10:45 – Governance & Identity Security
  - Entra ID Governance - Access Management
  - Lab Break 2
  - Securing Identities
  - Privileged User Lifecycle Story
  - Lab Break 3
  - Securing Privileged Access
- 12:00 – Lunch

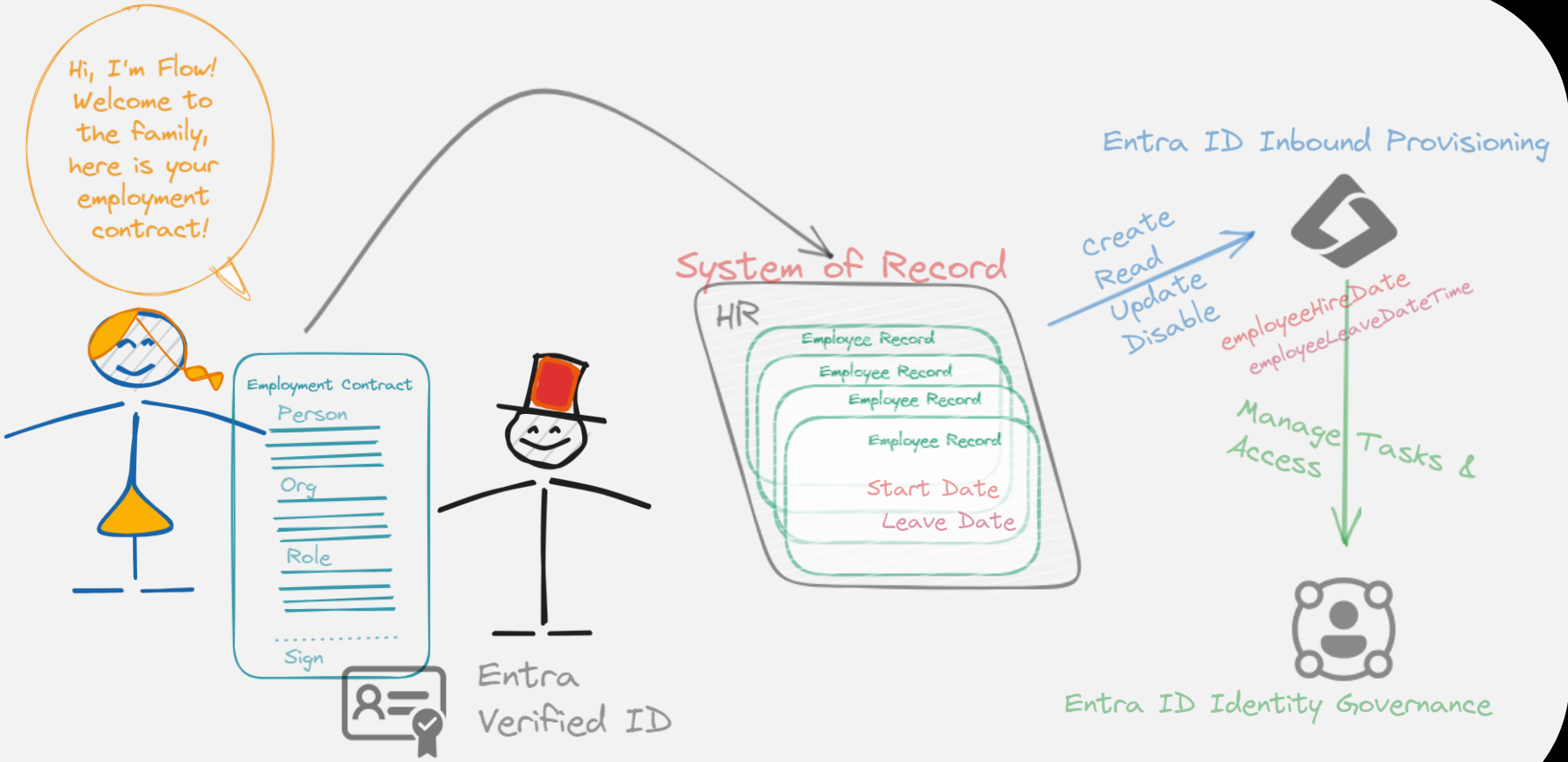
Agenda (cont.)

- 12:45 – Agent ID
  - Securing agentic AI using Microsoft Entra Agent ID
  - Lab break 4
- 14:15 – Cake / Snacks / Fruit / Coffee
- 14:45 – Maintaining, Security Exposure & Monitoring
  - Monitoring, Maintaining, Disaster Recovery
  - Optimize Identity Security Exposure
  - Lab break 5
  - Interactive closure and QA with audience

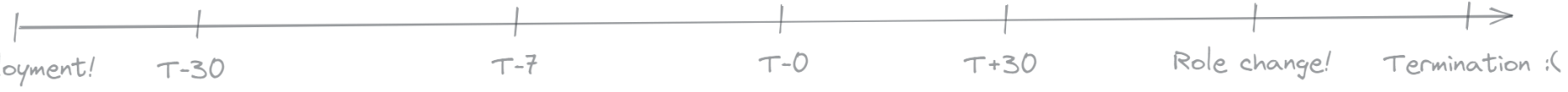
Entra ID Inbound Provisioning & Lifecycle Workflows

Mød Holger Danske!

A new recent hire to the Elven organization!


Hi, I'm Flow! Welcome to the family, here is your employment contract!
Employment Contract
Person
Org
Role
Sign
Entra Verified ID
System of Record
HR
Employee Record
Employee Record
Employee Record
Employee Record
Start Date
Leave Date
Create
Read
Update
Disable
Entra ID Inbound Provisioning
employeeHireDate
employeeLeaveDateTime
Manage Access
Tasks &
Entra ID Identity Governance

Identity & Access Lifecycle



Record in HR
Provision to
Entra ID

ERP
SaaS

M365 License
Mailbox
Calendar
Add to Groups
& Teams

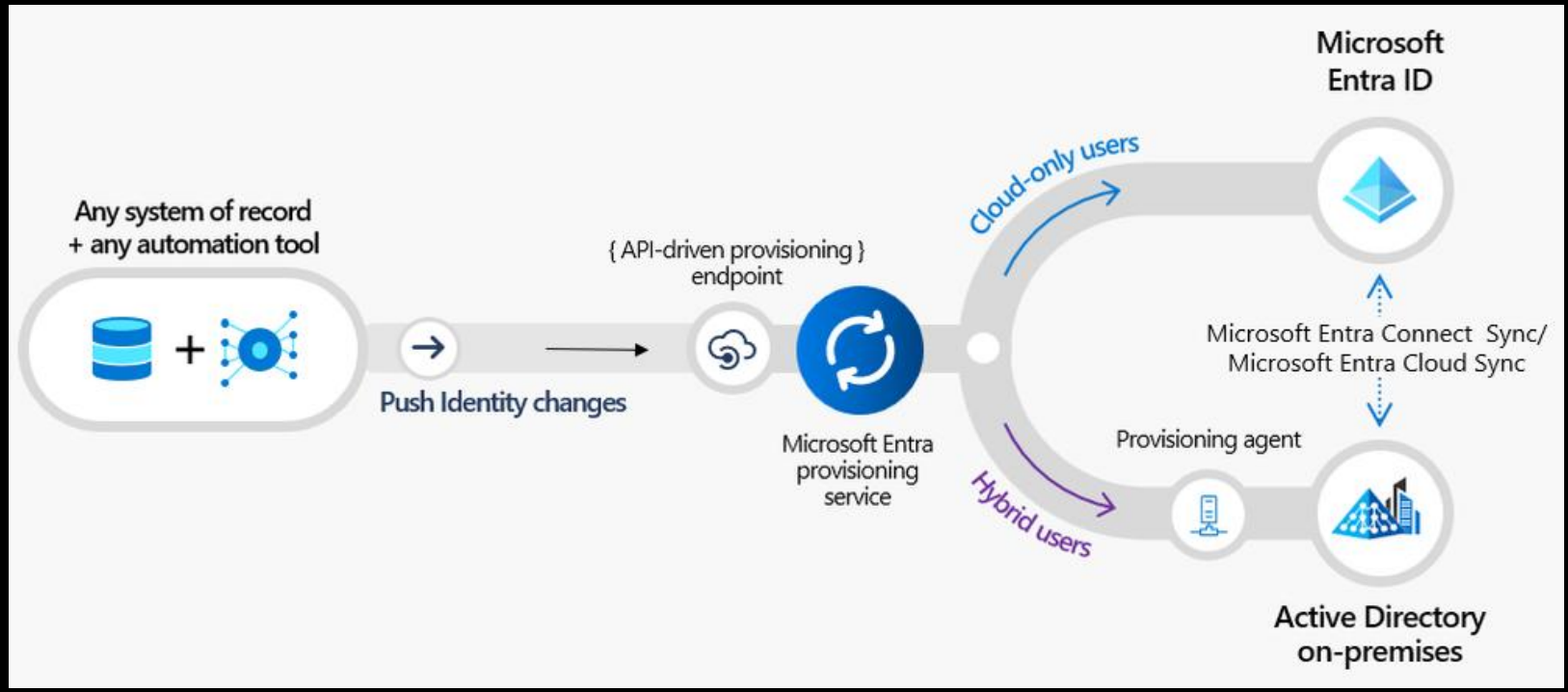
User Enable
Bootstrap
Security
Methods
Device Join
LMS

LMS+
Follow-ups

Remove & Add
Groups, Teams,
Apps

Disable User
Remove Groups,
Teams, Apps

Entra ID Provisioning API

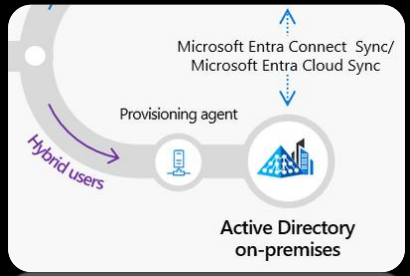


Connect Sync vs. Cloud Sync

Entra Connect Sync:

- Do you know MIIS, ILM or FIM, MIM?
- Sync Srv Dates back to the early 2000s
- 20 years of Metadirectory Experience
- Sync Service is very robust
  like a Swiss Army Knife …
- Large on-premises
  infrastructure footprint
- Management, Connect Server, SQL

Entra Cloud Sync:



- GA since 2021
- Modern Architecture, Cloud based
- Lightwight On-Premises Agents
- Not the entire feature set but
- also major improvements over
  Entra Connect Sync
- Is this right for you?
  Use the comparison tool in EAC

Connect Sync vs. Cloud Sync

(My) top features from Cloud Sync:

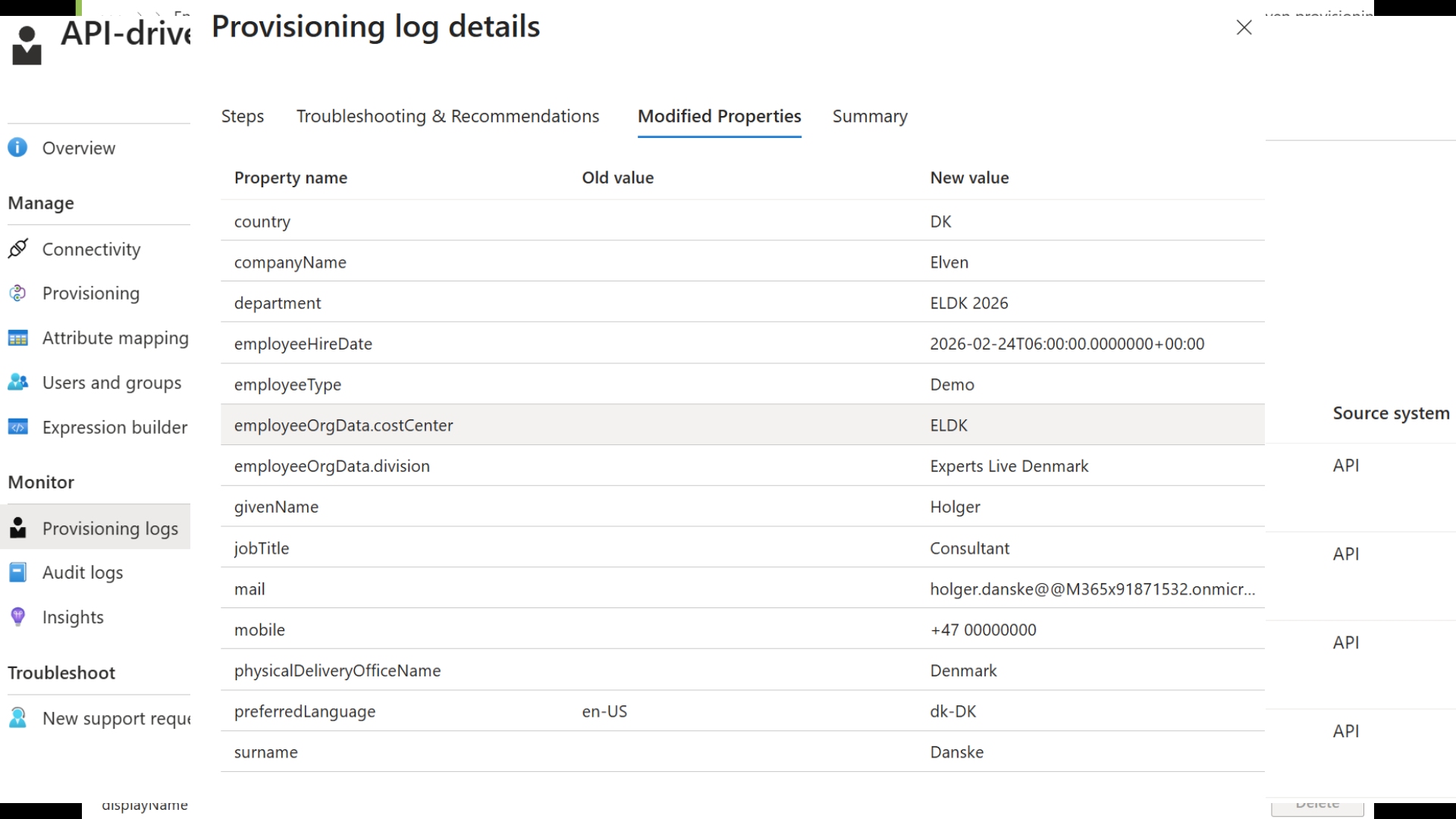
- Disconnected Forest Option
- On-Premises agent failover
- Cloud Management in EAC
- Group Writeback

Thinking about migration?

- Comparison Tool (EAC) helpful
- Both technologies can run in parallel
- Strategy considerations
- Where is your source of authority?

https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/migrate-azure-ad-connect-to-cloud-sync

https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync


API-drive
Provisioning log details
Overview
Manage
Connectivity
Provisioning
Attribute mapping
Users and groups
Expression builder
Monitor
Provisioning logs
Audit logs
Insights
Troubleshoot
New support requ
Steps
Troubleshooting & Recommendations
Modified Properties
Summary
Property name
Old value
New value
country
DK
companyName
Elven
department
ELDK 2026
employeeHireDate
2026-02-24T06:00:00.0000000+00:00
employeeType
Demo
employeeOrgData.costCenter
ELDK
employeeOrgData.division
Experts Live Denmark
givenName
Holger
jobTitle
Consultant
mail
holger.danske@@M365x91871532.onmicr...
mobile
+47 00000000
physicalDeliveryOfficeName
Denmark
preferredLanguage
en-US
dk-DK
surname
Danske
Source system
API
API
API
API
displayName

Entra ID Governance

01

Identity Lifecycle Management
Inbound Provisioning,
Lifecycle Workflows

02

Access Lifecycle Management
Lifecycle Mover Workflows,
Access Packages,
Access Reviews

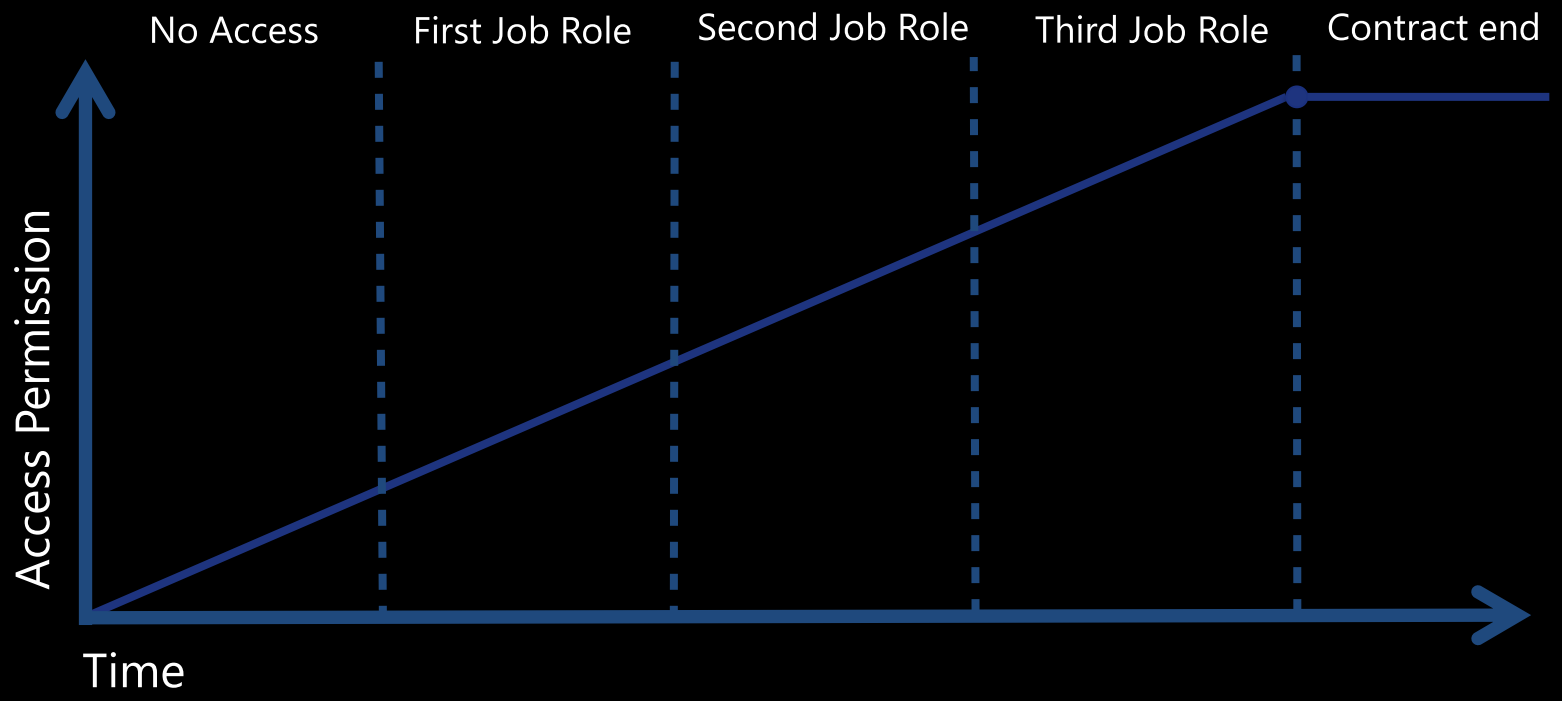
03

Outbound provisioning
Provisioning and access to 3rd party applications

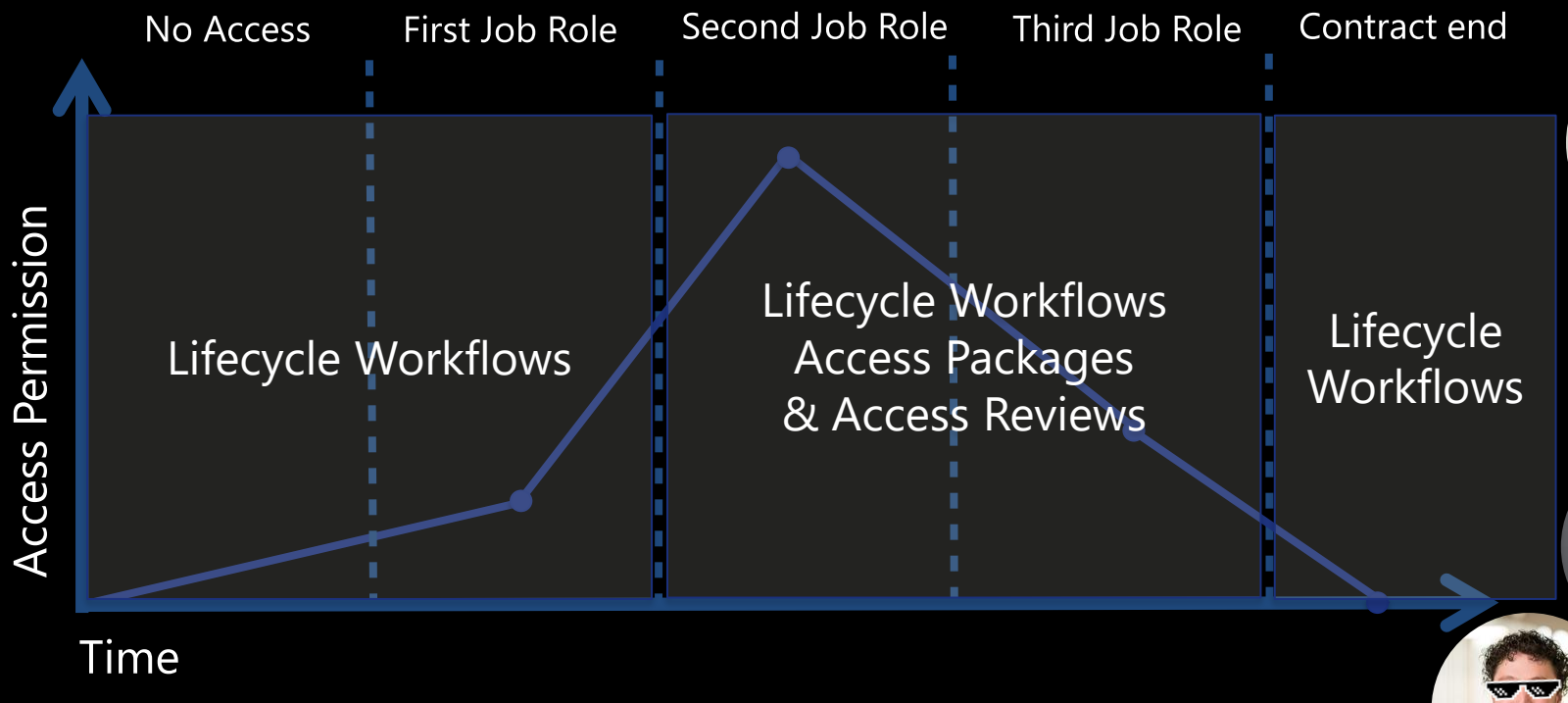
04

Least Privileged Access
Just in time just enough access

Historic Access Lifecycle Management



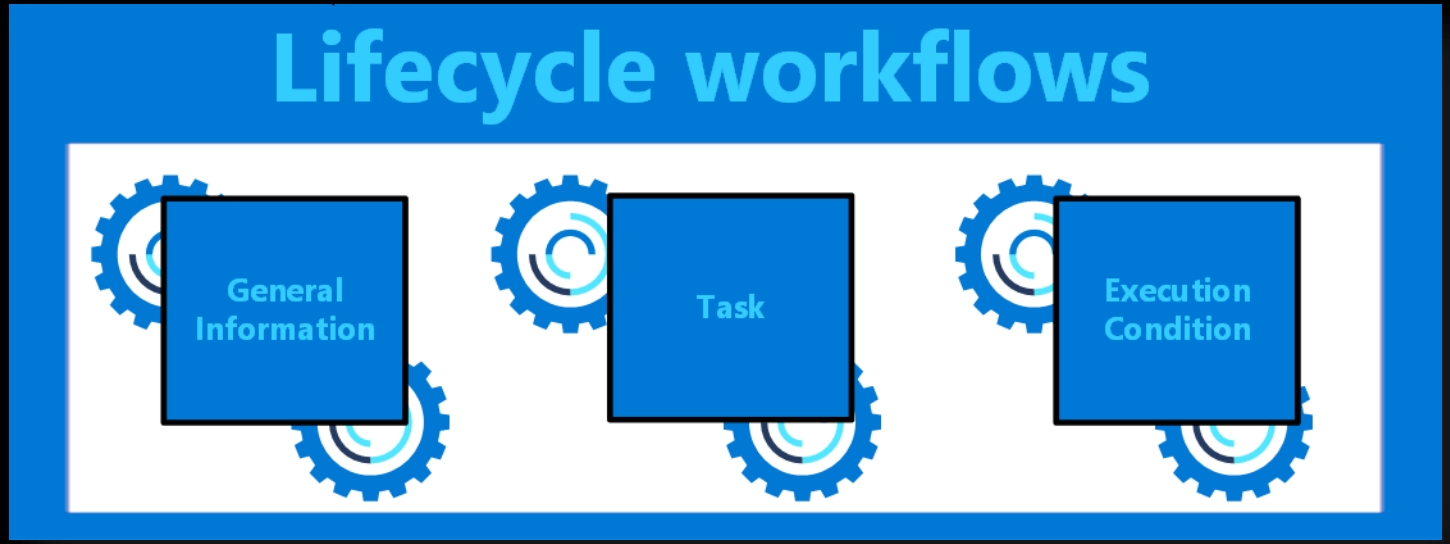
Modern Access Lifecycle Management





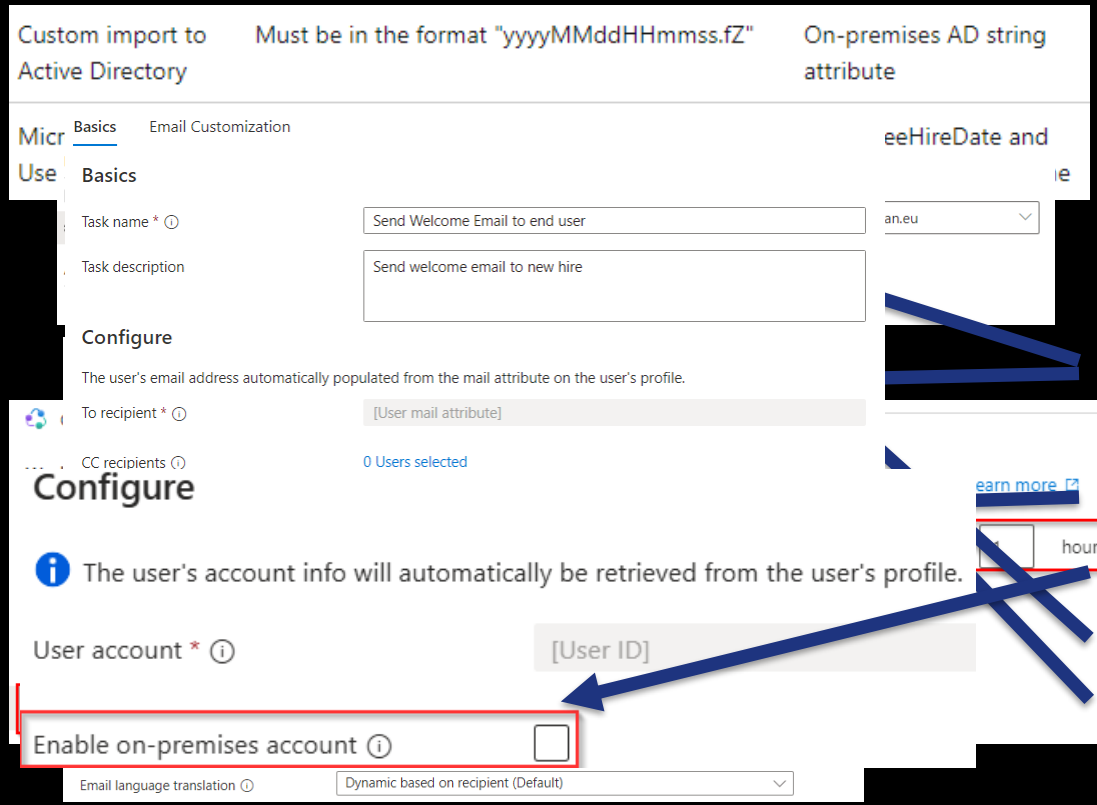


Understanding Lifecycle Workflows



Automated **Joiner, Mover & Leaver**

Lifecycle Workflows facts



- Runs each 3 hours
- Interval is customizable (1-24)
- Max 100 Workflows per tenant
- 25 per tasks per workflow
- Preferred Language
- Email customizations (Logo, Domain & Text)
- Built-in native tasks for Microsoft Entra
- Option to continue workflow on error
- Native hybrid integration for enable, disable and delete
- EmployeeHireDate
- EmployeeLeaveDateTime

Latest Lifecycle Workflows updates

Reprocess failed users and workflows in Lifecycle Workflows

Visibility of sensitivity labels on group tasks in Lifecycle Workflows

Trigger workflows for inactive employees and guests in Lifecycle Workflows

Agent identity sponsor lifecycle support in Lifecycle Workflows

Delegated Workflow Management with AUs in Lifecycle Workflows

Expanded attribute support in Lifecycle Workflows attribute changes trigger (like CSA)

Basic HTML support in Lifecycle Workflow

Entra ID Governance guest billing meter enforcement

Custom task extensions

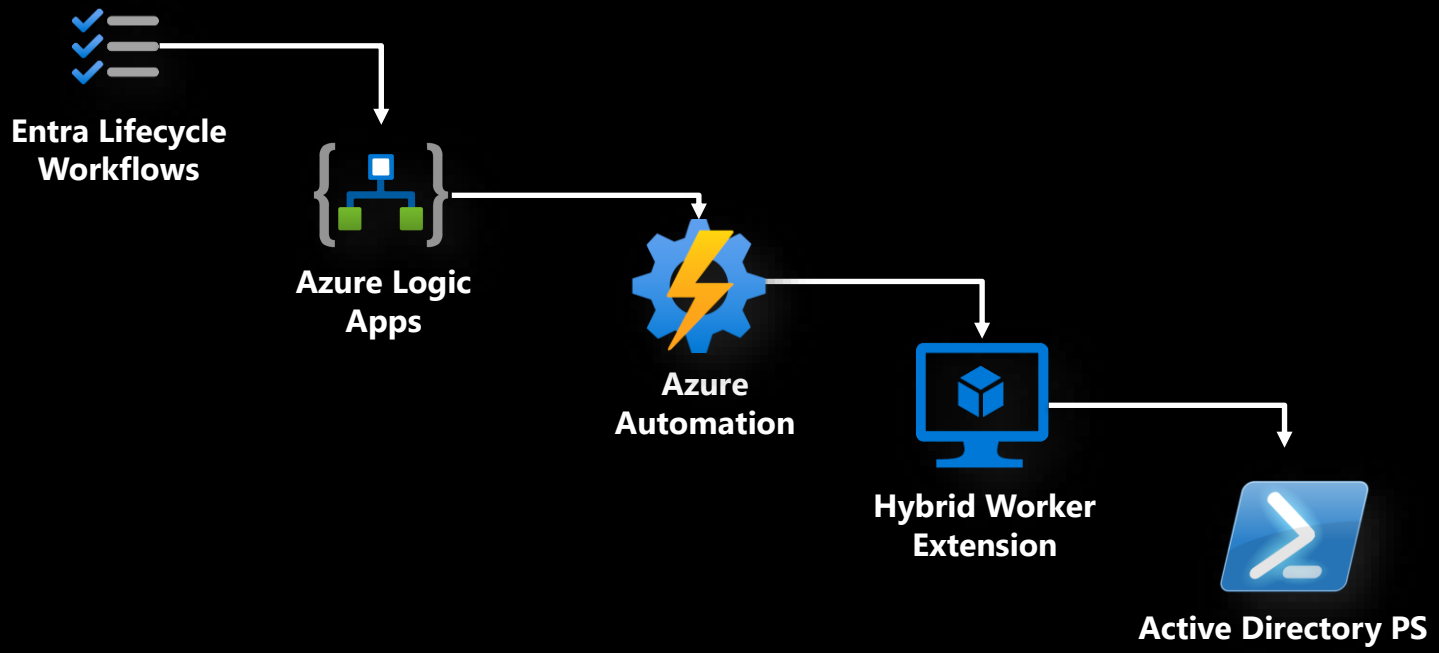
Lifecycle workflows

Logic Apps

Custom Extension examples

- Setting the out of office for the user and hiding user from address list
- Converting the mailbox to shared
- Wiping Intune managed devices (MAM/MDM)
- Disabling admin / test accounts associated to user account
- Deleting admin / test accounts associated to user account

Executing tasks on Active Directory?



Onboarding example

Account created as disabled in MS Entra

Assign license with mailbox and assign user to groups

Enable User account

Generate Temporary Access Pass

Send temporary access pass for bootstrapping to manager

Create access package request for application access

Secure onboarding by end users with TAP to register MFA

Adele Vance

Still phishable

Pre-hire workflow

New-hire workflow

DEMO

LAB 1: Inbound Provisioning API & Lifecycle Workflows

https://aka.ms/eldk26

Entra ID Governance Access Management

Entra ID Governance

01

Identity Lifecycle Management
Inbound Provisioning,
Lifecycle Workflows

02

Access Lifecycle Management
Lifecycle Mover Workflows,
Access Packages,
Access Reviews

03

Outbound provisioning
Provisioning and access to 3rd party applications

04

Least Privileged Access
Just in time just enough access

Understanding Access Packages

- Teams
- Groups
- Applications
- SharePoint sites
- Entra Roles
- API Permissions

Access Package + Approval

- Periodic reviews
- Self-review
- Recommendations

Access Review

Policies

Who can request?

- Members and/or guests

Assignments

- Admin assignment (manual)
- On demand (user can request)
- Dynamic assignment (attribute based)

Catalogs

Group resources for:

- Delegation to key users in your org
- Governance (visibility and protection for guests)

Custom Extensions for:

- Pre-expiration workflow
- Request workflow

Note: Moving access packages between catalogs isn't possible!

Separation of Duties

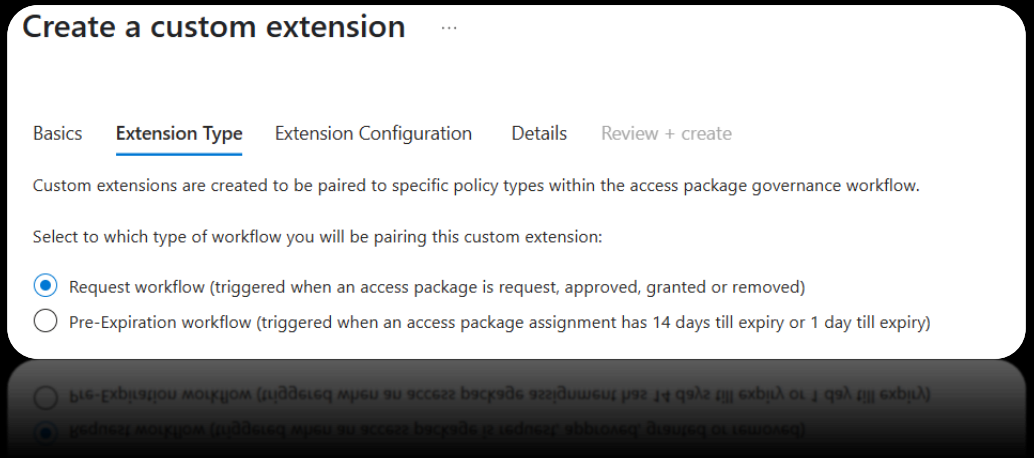
Deny access based on:

- Current group membership
- Incompatible Access Packages

Examples:

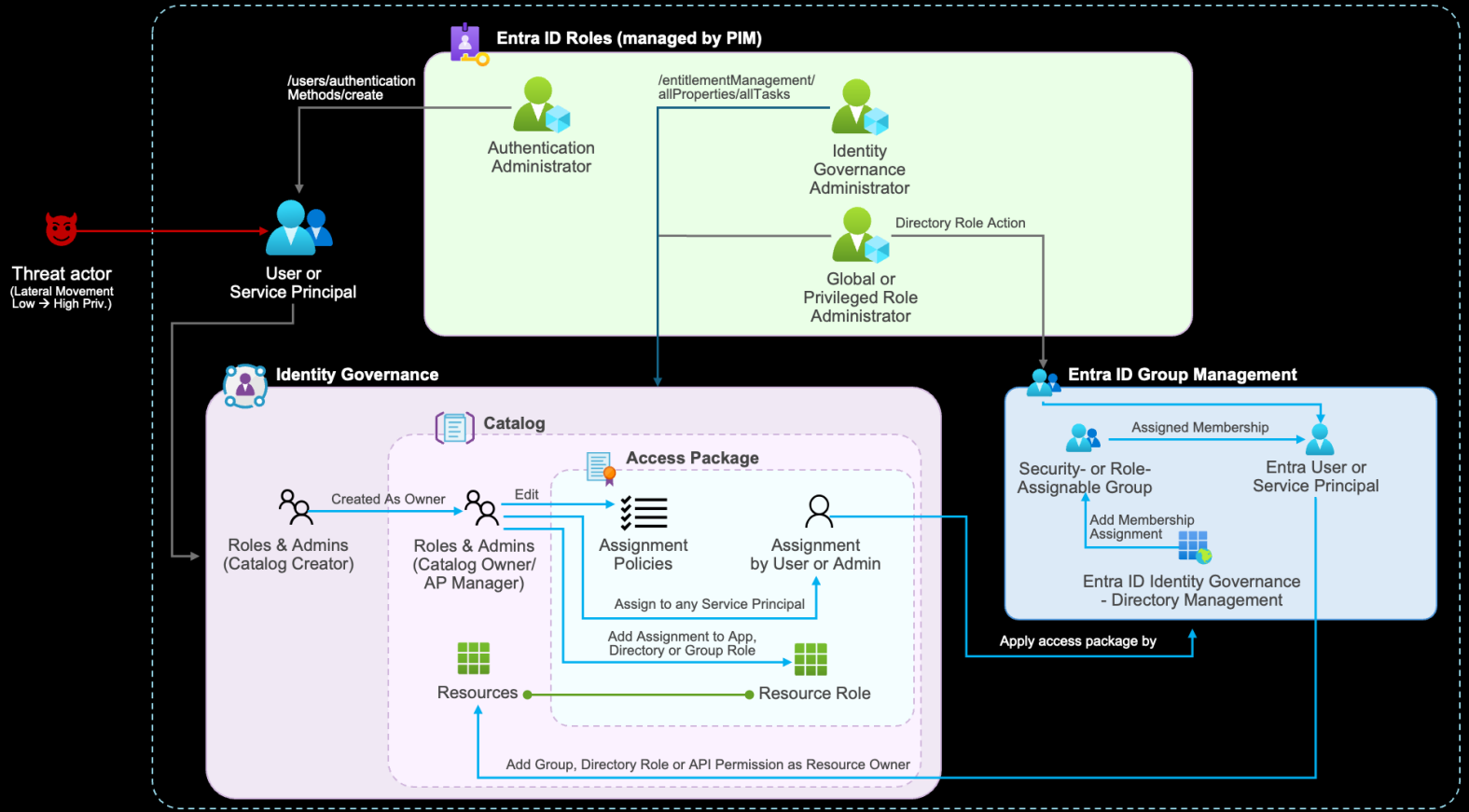
- Update rings (Fast vs. Slow ring)
- License groups

Custom Extensions

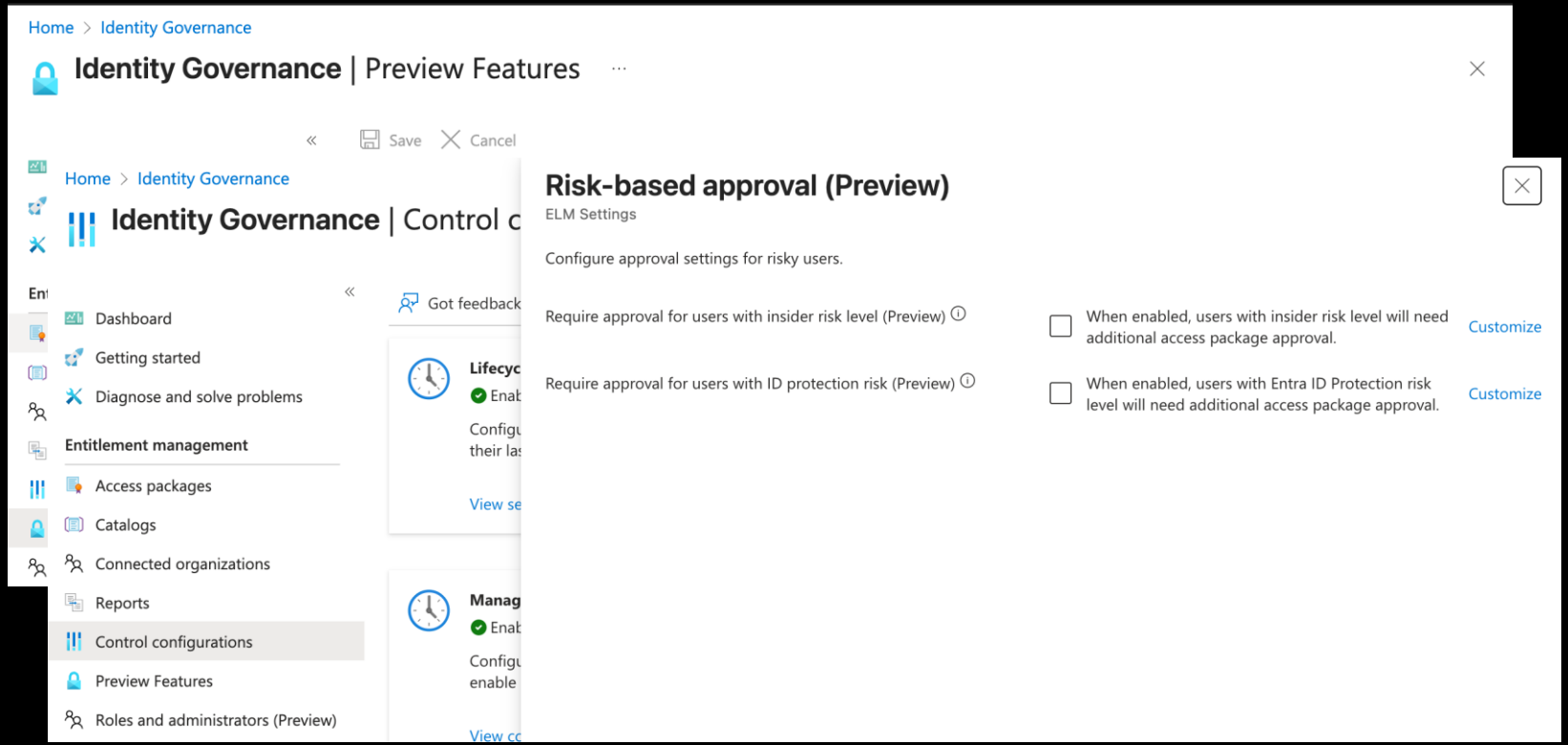


- Created in Catalog
- Linked to a logic app
- Use app authorization for security
- Request Workflow type
  (Created, Approved, Granted or removed)
- Pre-Expiration Workflow
  (1 or 14 days)
- Fire and Forget or Fire and Wait

ELM Delegation and Attack Paths



ELM Settings for Hardening

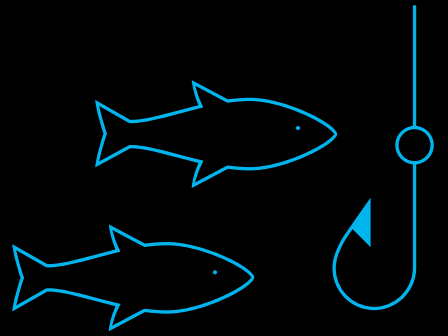


DEMO

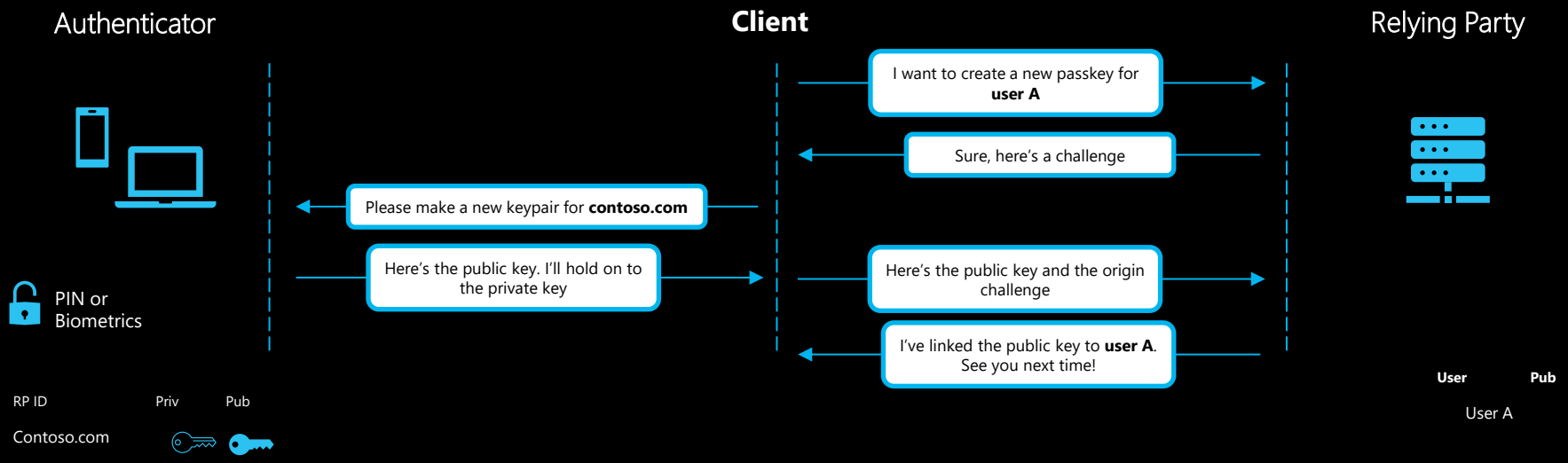
LAB 2: Access Management – Entra ID Governance

https://aka.ms/eldk26

Phishing Resistant



How passkeys work (Registration)



Device-bound or Synced Passkeys

Device-bound passkeys

Synced passkeys

Passkey Profiles

Steps to enable Passkeys in Microsoft Entra ID

Gather list of AAGUIDs of current passkeys (security keys) in Microsoft Entra

Determine scope for Passkey enrollment

Enable Passkeys Authentication Method in Microsoft Entra

Configure passkey profiles (example: device-bound for admin, synced for regular users)

Provide adoption materials to end users!

Onboarding example

Account created as disabled in MS Entra

Assign license with mailbox and assign user to groups

Enable User account

Generate Temporary Access Pass

Send temporary access pass for bootstrapping to manager

Create access package request for application access

Secure onboarding by end users with TAP to register passkey

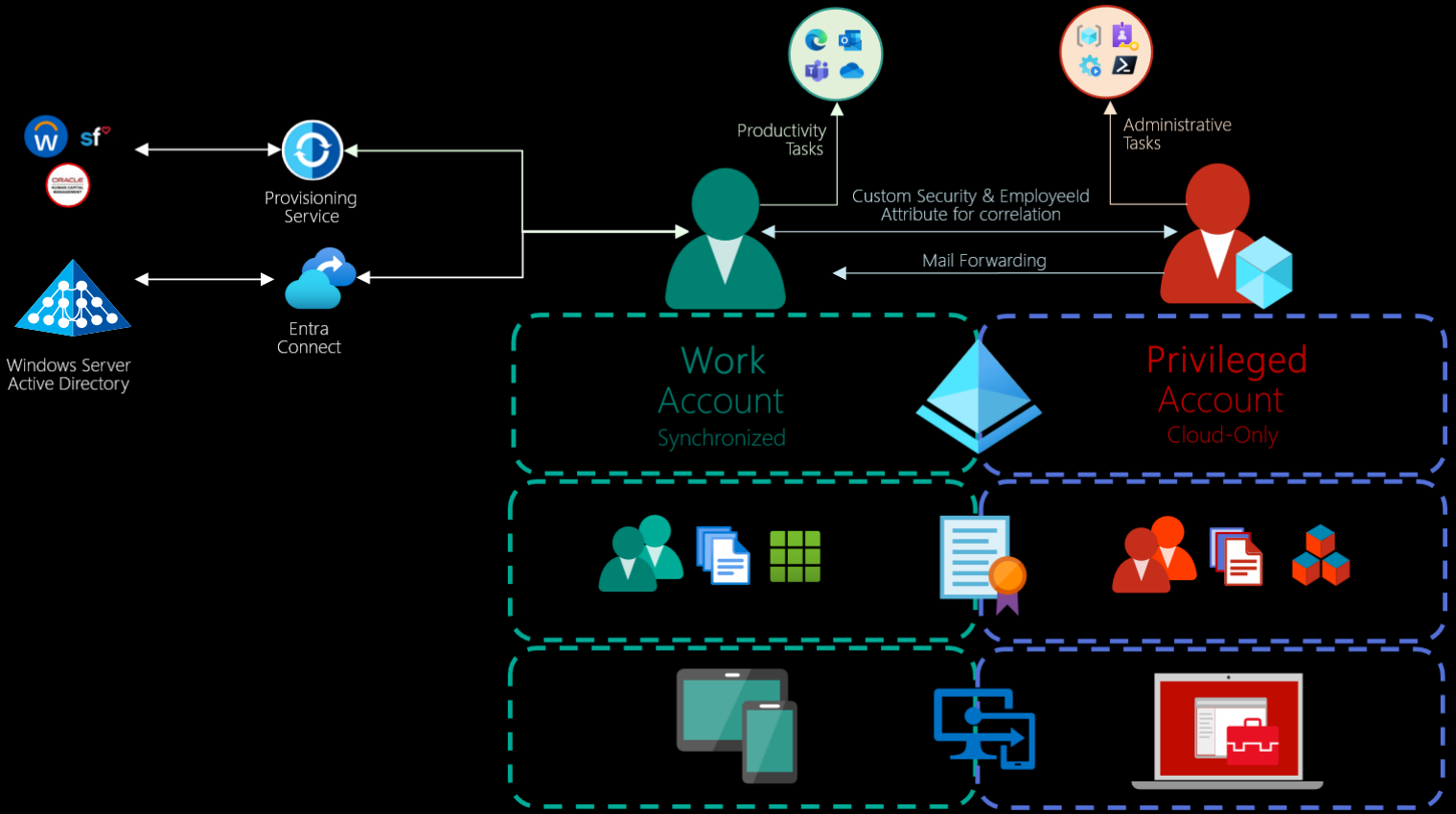
Adele Vance
Unphishable

Pre-hire workflow

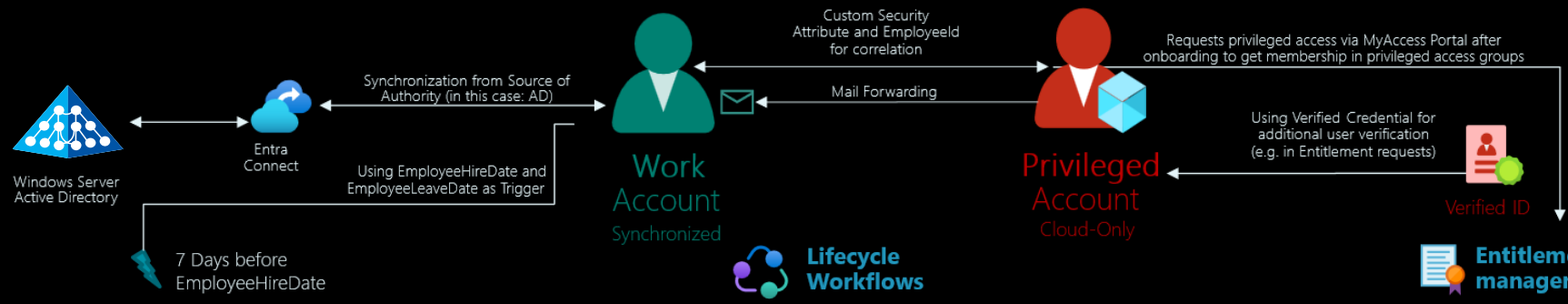
New-hire workflow

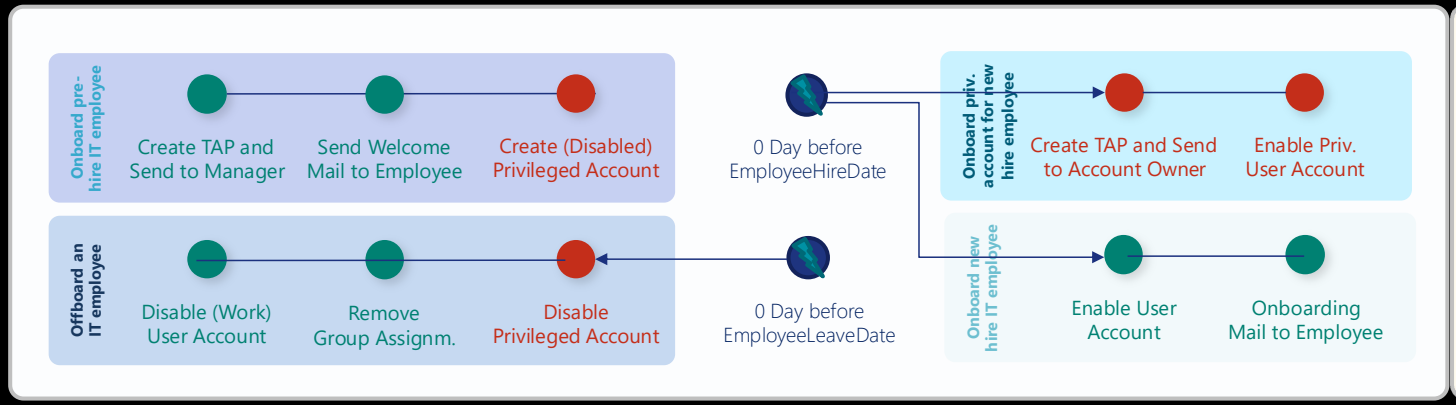
Privileged User Lifecycle Story

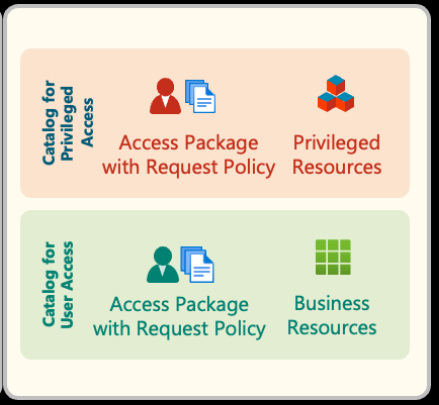
Work and Privileged Account Separation



Privileged Account Lifecycle Workflow







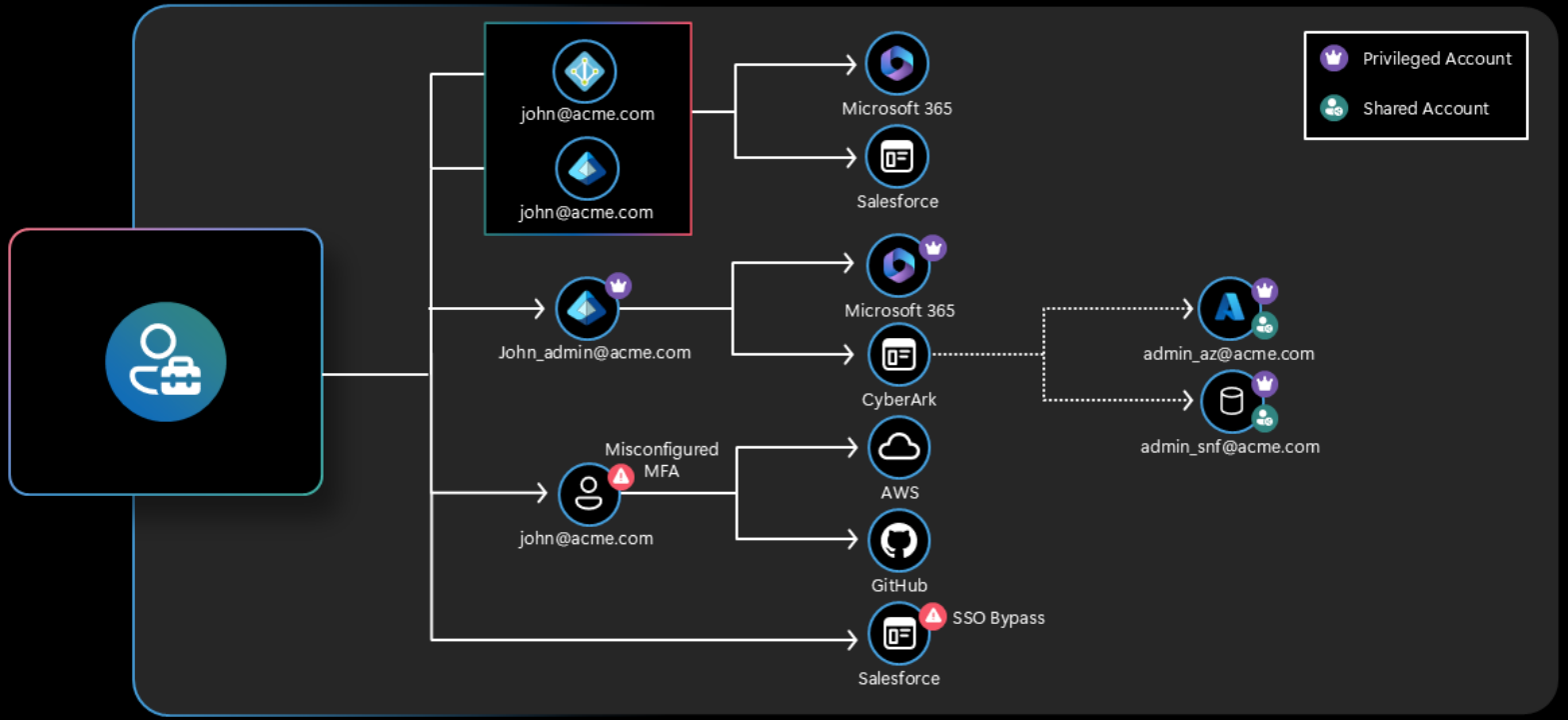
Options for Privileged Account Provisioning

Lifecycle Workflows and Custom Logic App
Advantage: Direct automation and linkage to the lifecycle of the "work account".
Disadvantage: Requires a filter/condition; requires an Entra ID Governance P2 license.

Access Package and Custom Extension (Logic App)
Advantage: Flexibility and process control for the provisioning of admin accounts.
Disadvantage: A request is required; the offboarding trigger must be implemented separately.

API-driven inbound provisioning with Logic App, PowerShell or other low-code client
Advantage: High flexibility, a fully featured sync process with direct data source integration
Disadvantage: Effort required for customization and integration of the API client.

Linked Identities in Defender XDR



Source: Enhancing visibility into your identity fabric with Microsoft Defender

DEMO

LAB 3: Privileged Accounts

https://aka.ms/eldk26

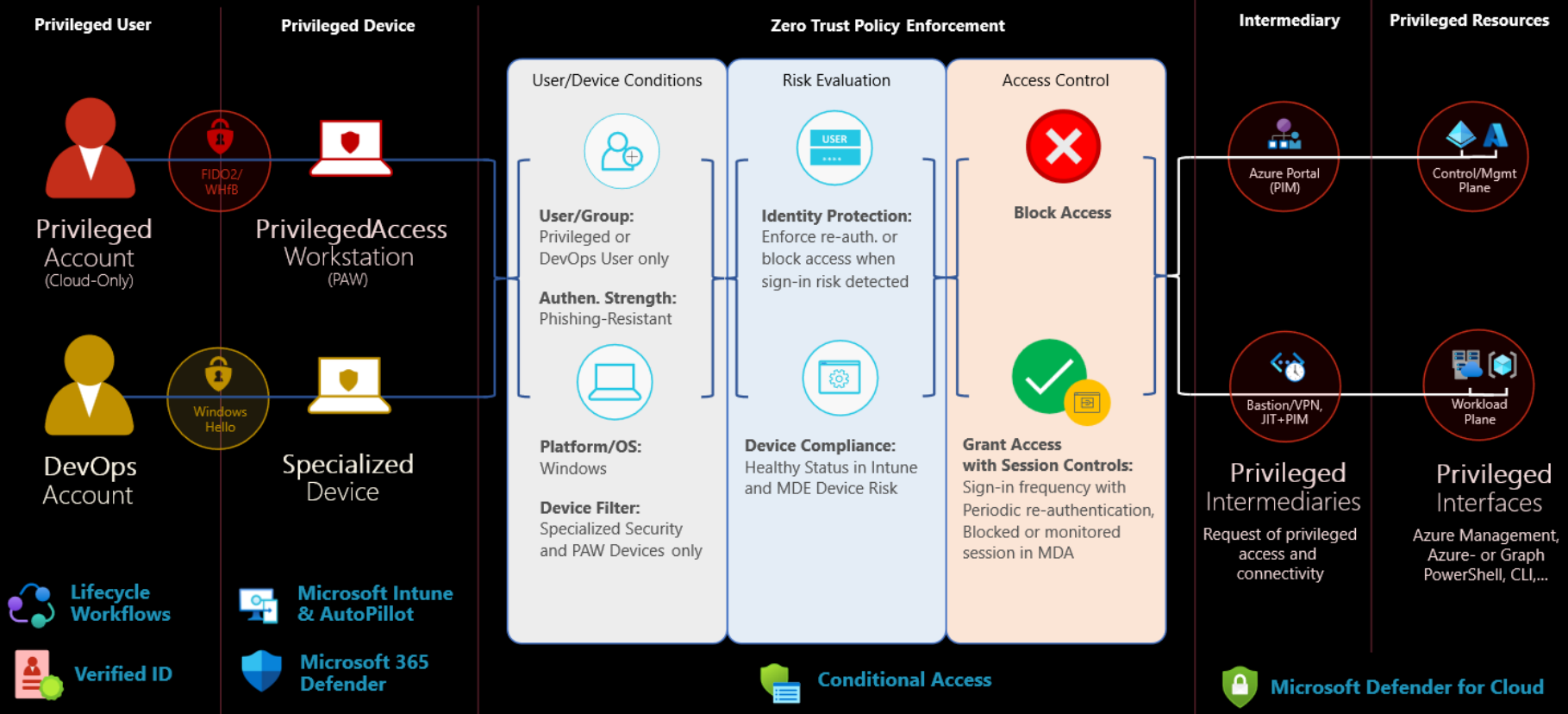
Securing Privileged Access

Golden Rules for Privileged IAM

Separation of User Accounts
Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.

Strong Security Policies
Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.

Strong CA Policies for Privileged Users



Foundation of Privileged Endpoints

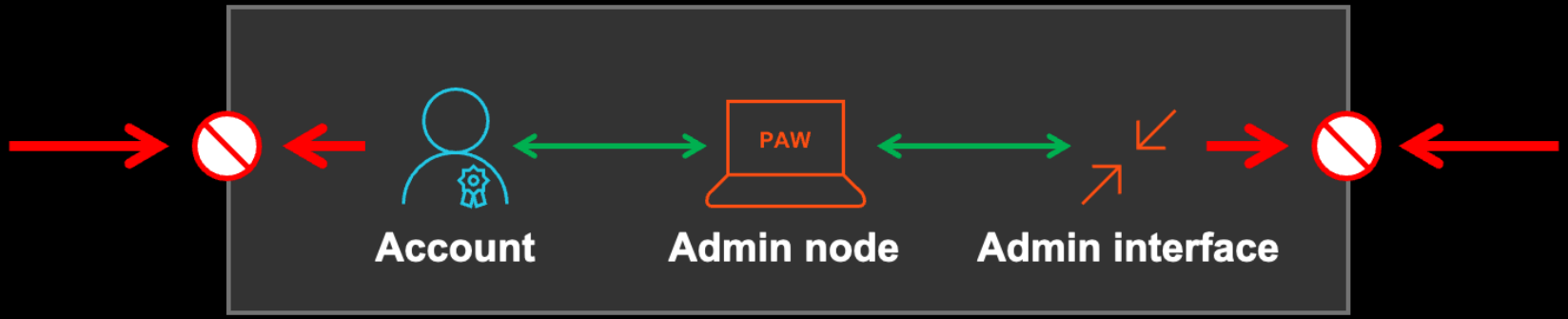


Image source: "Microsoft CISO Workshop 4a - Threat Protection Strategy"

Comparison of Virtualized vs. Physical PAW

Criteria	Physical PAW (Hardware)	Virtual "PAW" (Windows 365)
🛡️ **Security Model**	**Hardware Isolation:** Zero reliance on host OS integrity; physical separation protects against host-level malware.	**Logical Isolation:** Relies on the security of the hosting device, vulnerable if the access point is compromised.
💼 **Usability**	**Low:** Requires carrying two distinct physical laptops	**High:** Access secure admin desktop from standard productivity device.
🚀 **Deployment**	**Dependencies:** Procurement, shipping (days/weeks)	**Instant:** Automated provisioning via Intune/Windows 365 portal (minutes/hours).
💰 **Cost Strategy**	**CAPEX High:** Expensive bespoke hardware, shipping, and replacement costs.	**OPEX Predictable:** Fixed monthly license per admin; uses existing physical hardware.
🌐 **Connectivity**	**Hybrid/Offline:** Can work offline for local AD/Datacenter admin tasks.	**Online Only:** Requires stable internet; unusable without connectivity.
🏗️ **Maintenance**	**High Touch:** Firmware updates, battery swelling, physical repairs require swaps.	**Zero Touch:** Microsoft manages backend; "Reprovision" feature resets environment instantly.
🚦 **Ideal Use Case**	IAM Platform, Zero Trust and Privilege Access Management, PKI-Infrastructure	Azure Platform (exclude Control Plane or Root Scope) and Workloads

Golden Rules for Privileged IAM

Separation of User Accounts
Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.

Strong Security Policies
Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.

Restricted Delegation
Use “Restricted Management Administrative Units” and/or role-assignable groups to limit access to privileged objects.

Tiered Administration
Create a clear classification of sensitive roles and their scopes to segment administrative access areas.

Quiz: Who wants to be Control Plane?

WHICH OF THESE DIRECTORY ROLES ARE TIERO?

A. Authenticator Administrator

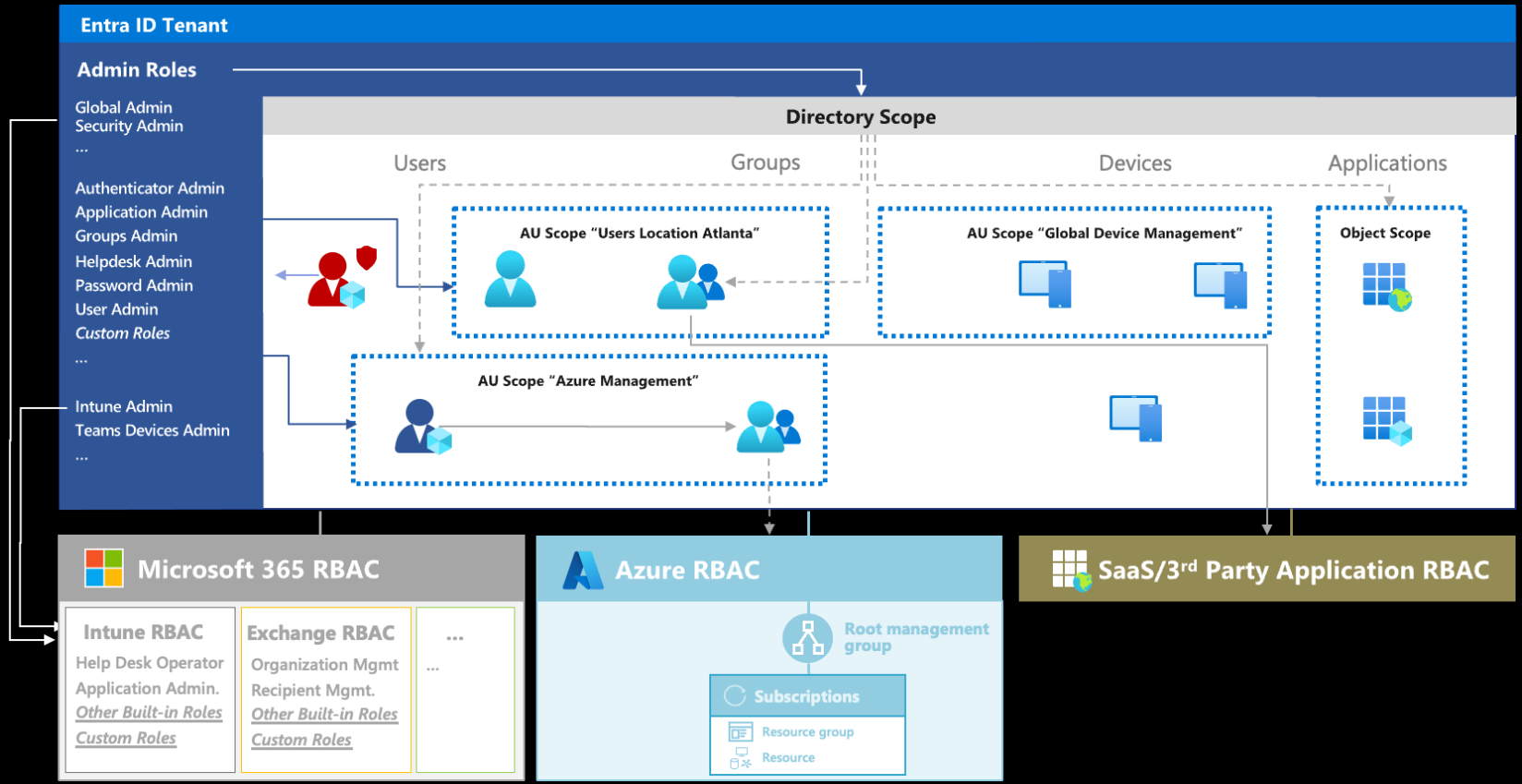
B. Cloud Application Administrator

C. Groups Administrator

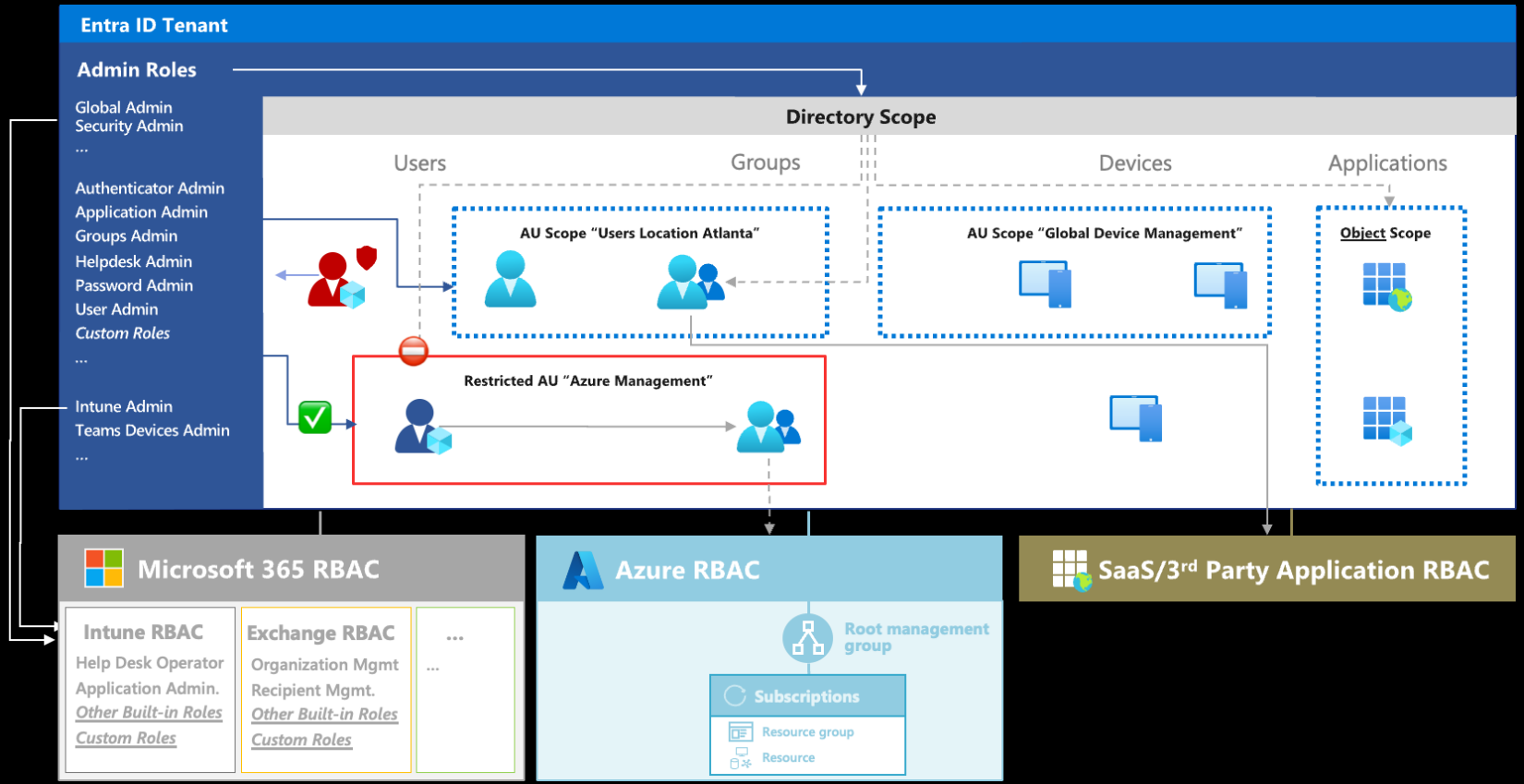
D. User Administrator

"It Depends"

Delegation on Directory or AU-Level scope



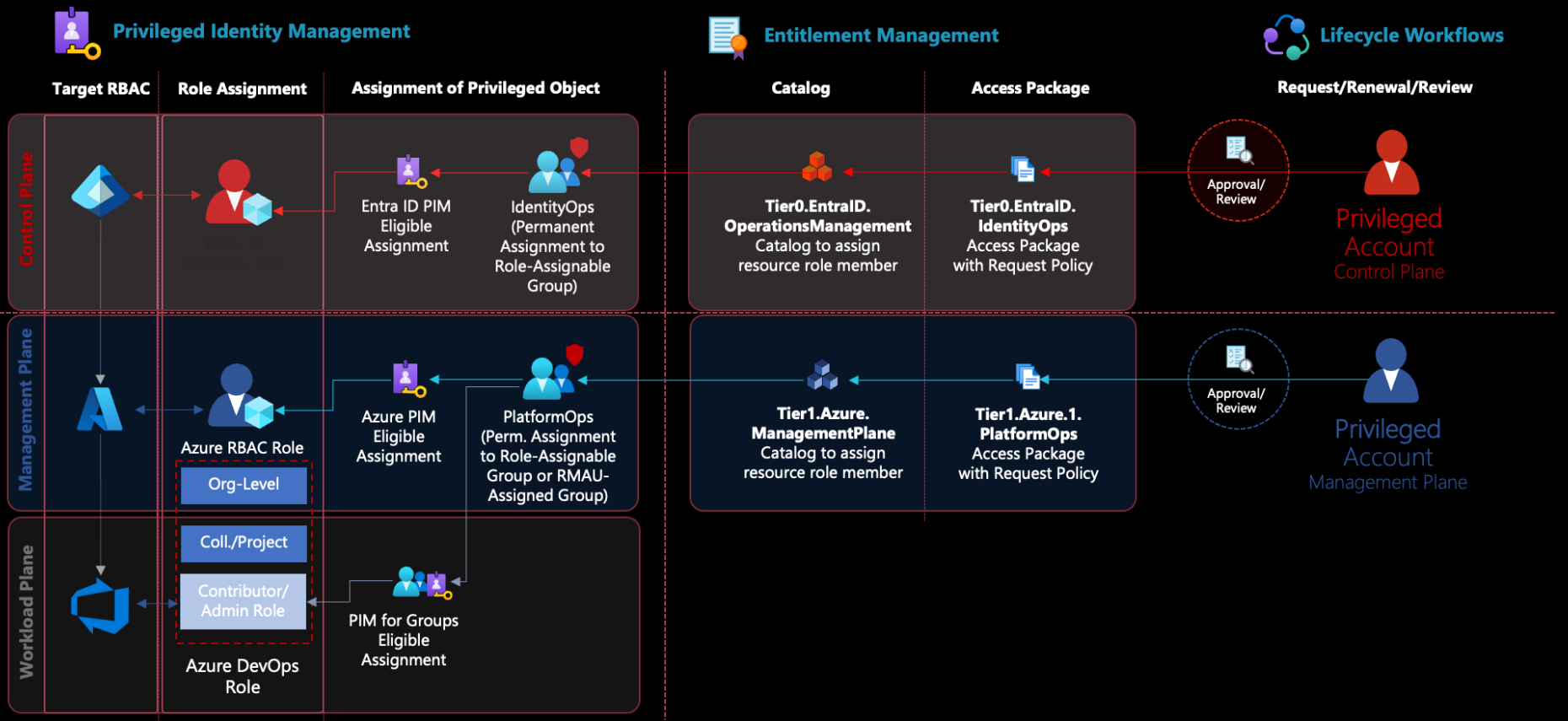
Delegation on Directory or AU-Level scope



Types of Groups and Protection Capabilities

	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

Delegation of Control/Management Plane



Delegation by Roles vs. Ownership

Role Actions by Condition "IsOwner"

"microsoft.directory/applications/appRoles/update",
"microsoft.directory/applications/credentials/update",
"microsoft.directory/applications/delete",
"microsoft.directory/applications/owners/update",
"microsoft.directory/applications/permissions/update",
"microsoft.directory/deletedItems.applications/delete",
"microsoft.directory/deletedItems.applications/restore",
"microsoft.directory/deletedItems.groups/restore",
"microsoft.directory/devices/disable",
"microsoft.directory/groupsAssignableToRoles/allProperties/update",
"microsoft.directory/groupsAssignableToRoles/delete",
"microsoft.directory/groupsAssignableToRoles/restore",",
"microsoft.directory/groups/delete",
"microsoft.directory/groups/groupType/update",
"microsoft.directory/groups/members/update",
"microsoft.directory/groups/owners/update",
"microsoft.directory/groups/restore",
"microsoft.directory/policies/basic/update",
"microsoft.directory/policies/delete",
"microsoft.directory/policies/owners/update",
"microsoft.directory/servicePrincipals/appRoleAssignedTo/update",
"microsoft.directory/servicePrincipals/basic/update",
"microsoft.directory/servicePrincipals/credentials/update",
"microsoft.directory/servicePrincipals/delete",
"microsoft.directory/servicePrincipals/owners/update",
"microsoft.directory/servicePrincipals/permissions/update",
…

Golden Rules for Privileged IAM

Separation of User Accounts
Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.

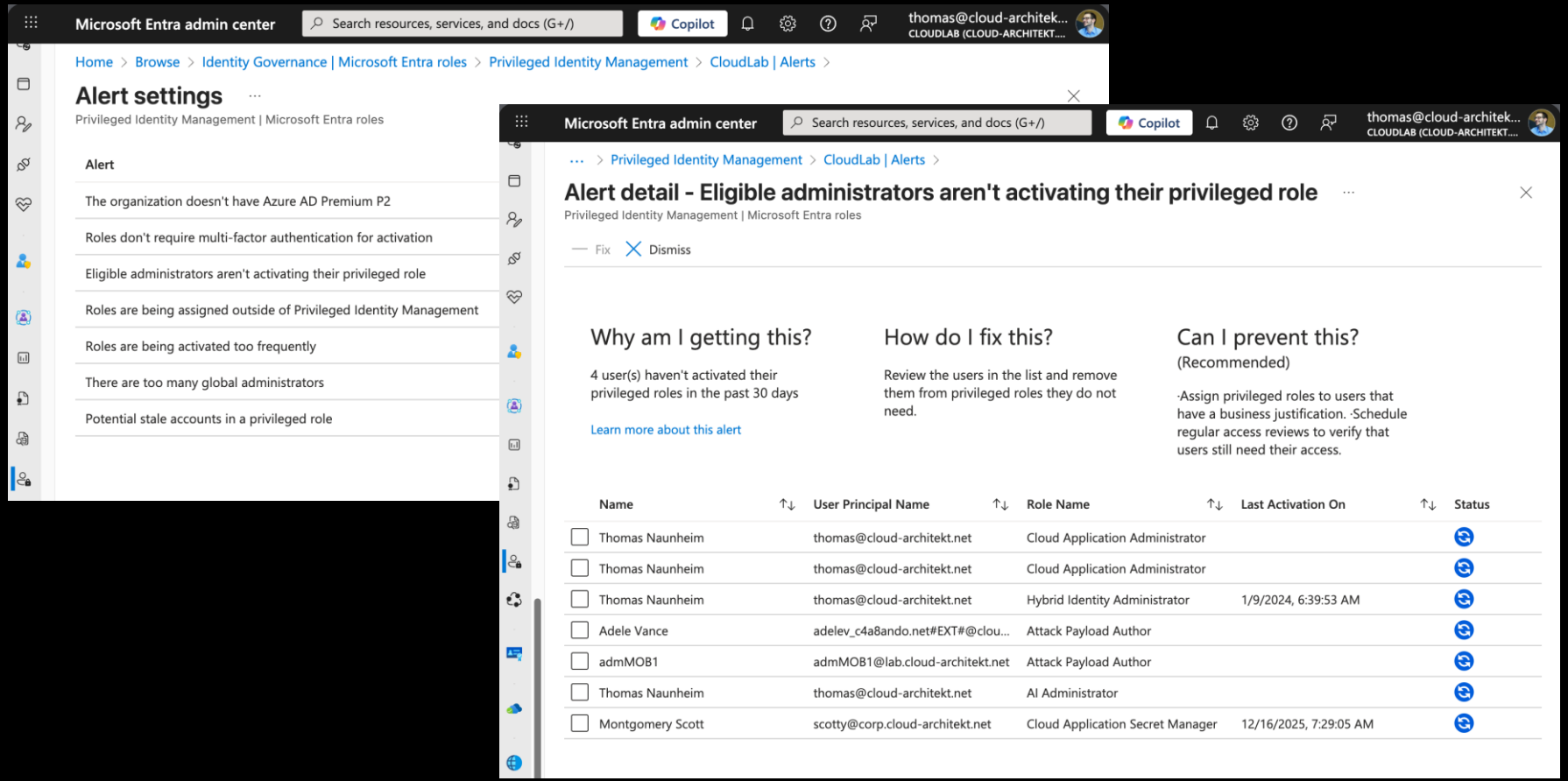
Strong Security Policies
Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.

Restricted Delegation
Use “Restricted Management Administrative Units” and/or role-assignable groups to limit access to privileged objects.

Tiered Administration
Create a clear classification of sensitive roles and their scopes to segment administrative access areas.

Review and Monitoring
Regularly review assigned, eligible, and active permissions to detect anomalies, outdated permissions, or misuse.

PIM Alerts


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
thomas@cloud-architek...
CLOUDLAB (CLOUD-ARCHITEKT....
Home > Browse > Identity Governance | Microsoft Entra roles > Privileged Identity Management > CloudLab | Alerts >
Alert settings
Privileged Identity Management | Microsoft Entra roles
Alert
The organization doesn't have Azure AD Premium P2
Roles don't require multi-factor authentication for activation
Eligible administrators aren't activating their privileged role
Roles are being assigned outside of Privileged Identity Management
Roles are being activated too frequently
There are too many global administrators
Potential stale accounts in a privileged role
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
thomas@cloud-architek...
CLOUDLAB (CLOUD-ARCHITEKT....
Privileged Identity Management > CloudLab | Alerts >
Alert detail - Eligible administrators aren't activating their privileged role
Privileged Identity Management | Microsoft Entra roles
Fix
Dismiss
Why am I getting this?
4 user(s) haven't activated their privileged roles in the past 30 days
Learn more about this alert
How do I fix this?
Review the users in the list and remove them from privileged roles they do not need.
Can I prevent this?
(Recommended)
·Assign privileged roles to users that have a business justification. ·Schedule regular access reviews to verify that users still need their access.
Name
User Principal Name
Role Name
Last Activation On
Status
Thomas Naunheim
thomas@cloud-architekt.net
Cloud Application Administrator
Thomas Naunheim
thomas@cloud-architekt.net
Cloud Application Administrator
Thomas Naunheim
thomas@cloud-architekt.net
Hybrid Identity Administrator
1/9/2024, 6:39:53 AM
Adele Vance
adelev_c4a8ando.net#EXT#@clou...
Attack Payload Author
admMOB1
admMOB1@lab.cloud-architekt.net
Attack Payload Author
Thomas Naunheim
thomas@cloud-architekt.net
AI Administrator
Montgomery Scott
scotty@corp.cloud-architekt.net
Cloud Application Secret Manager
12/16/2025, 7:29:05 AM

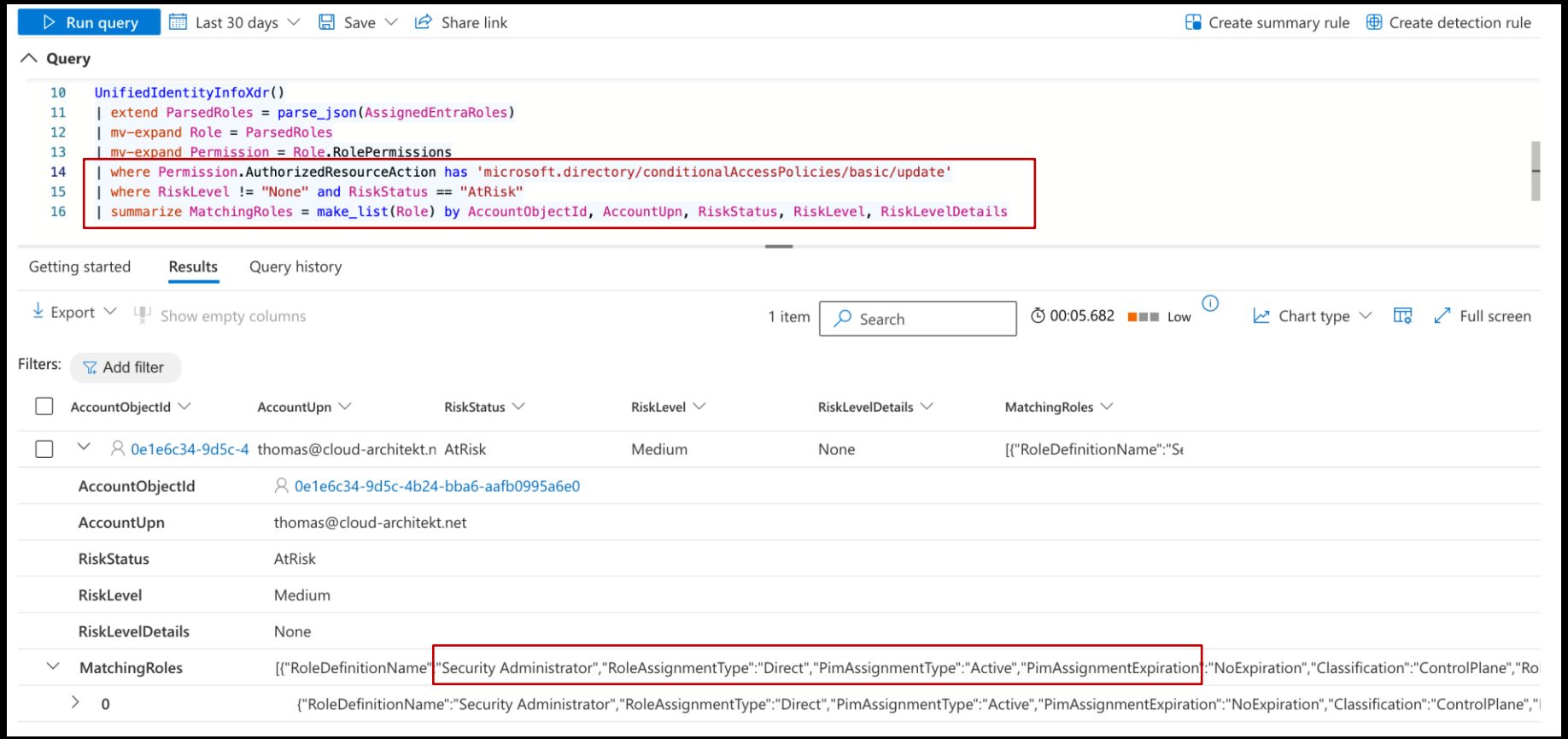
KQL function for Privileged Access Hunting

UnifiedIdentityInfoXDR

TimeGenerated	AccountObjectId	AccountDisplayName	AccountStatus	Type	CriticalityLevel	CriticalAssetDetails	Classification	AssignedAzureRoles

AccountDisplayName	admThom0-B2C
AccountStatus	Enabled
Type	User
CriticalityLevel	0
CriticalAssetDetails	[{"CriticalityLevel":"0","RuleName":"B2C Resources"}]
Classification	ControlPlane
AssignedEntraRoles	[{"RoleDefinitionName":"Cloud Application Administrator","RoleAssignmentType":"Indirect","PimAssignmentType":"Eligible","PimAssignmentExpiration":"NoExpiration","Classification":"ControlPlane","RoleIsPrivileged":tr
0	{"RoleDefinitionName":"Cloud Application Administrator","RoleAssignmentType":"Indirect","PimAssignmentType":"Eligible","PimAssignmentExpiration":"NoExpiration","Classification":"ControlPlane","RoleIsPrivileged"
RoleDefinitionName	Cloud Application Administrator
RoleAssignmentType	Indirect
PimAssignmentType	Eligible
PimAssignmentExpiration	NoExpiration
Classification	ControlPlane
RoleIsPrivileged	true
RoleCategories	identity
RolePermissions	[{"AuthorizedResourceAction":"microsoft.directory/adminConsentRequestPolicy/allProperties/allTasks","Category":"Application and Workload Identity","EAMTierLevelName":"ControlPlane","EAMTierLevelTagValu

KQL function for Privileged Access Hunting



Golden Rules for Privileged IAM

Separation of User Accounts
Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.

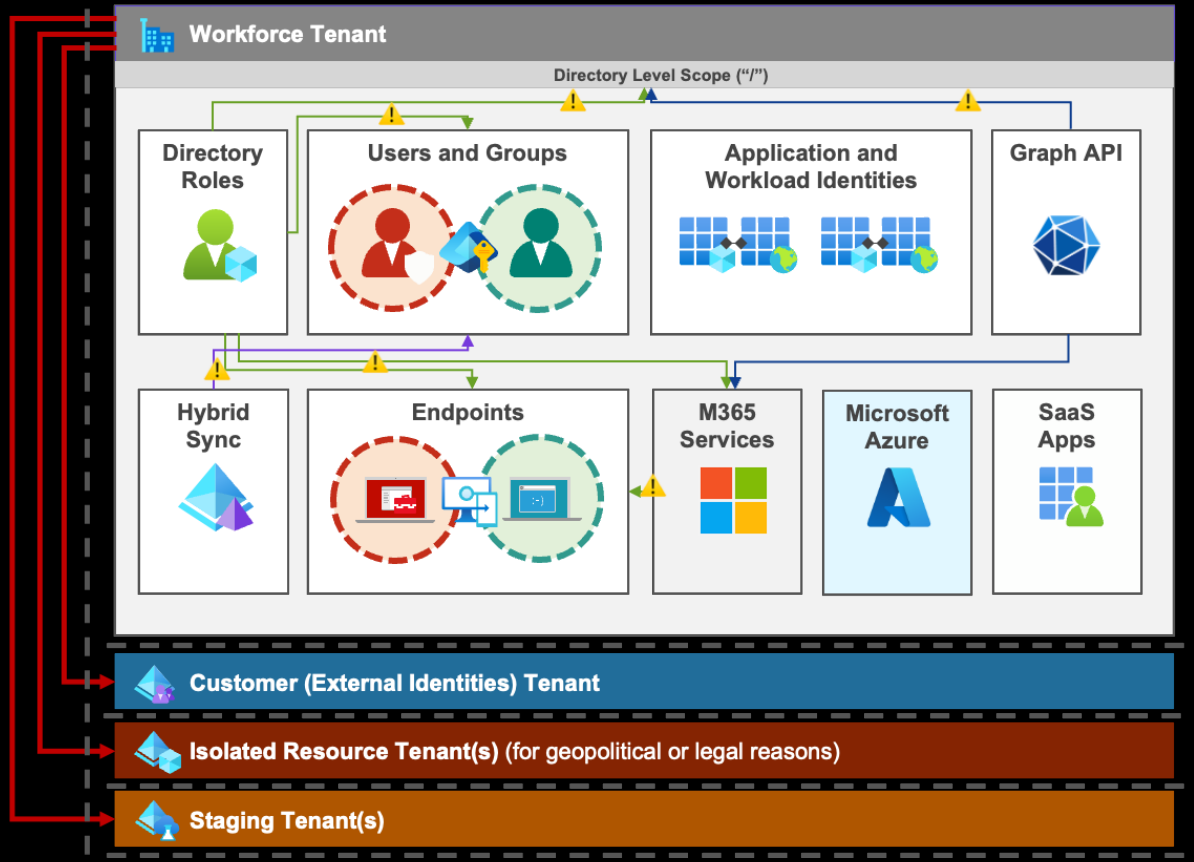
Strong Security Policies
Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.

Restricted Delegation
Use “Restricted Management Administrative Units” and/or role-assignable groups to limit access to privileged objects.

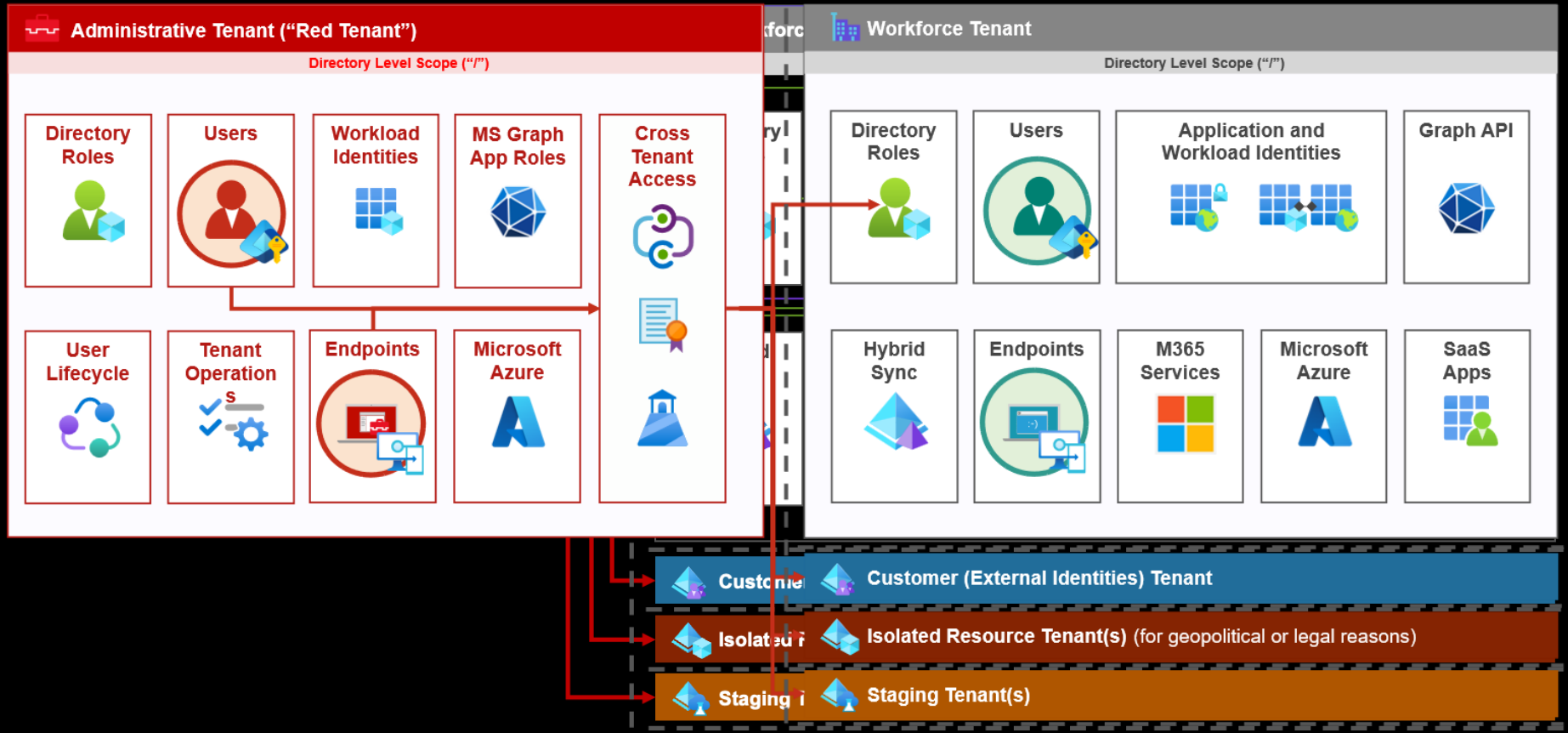
Tiered Administration
Create a clear classification of sensitive roles and their scopes to segment administrative access areas.

Review and Monitoring
Regularly review assigned, eligible, and active permissions to detect anomalies, outdated permissions, or misuse.

Intra-Tenant Isolation

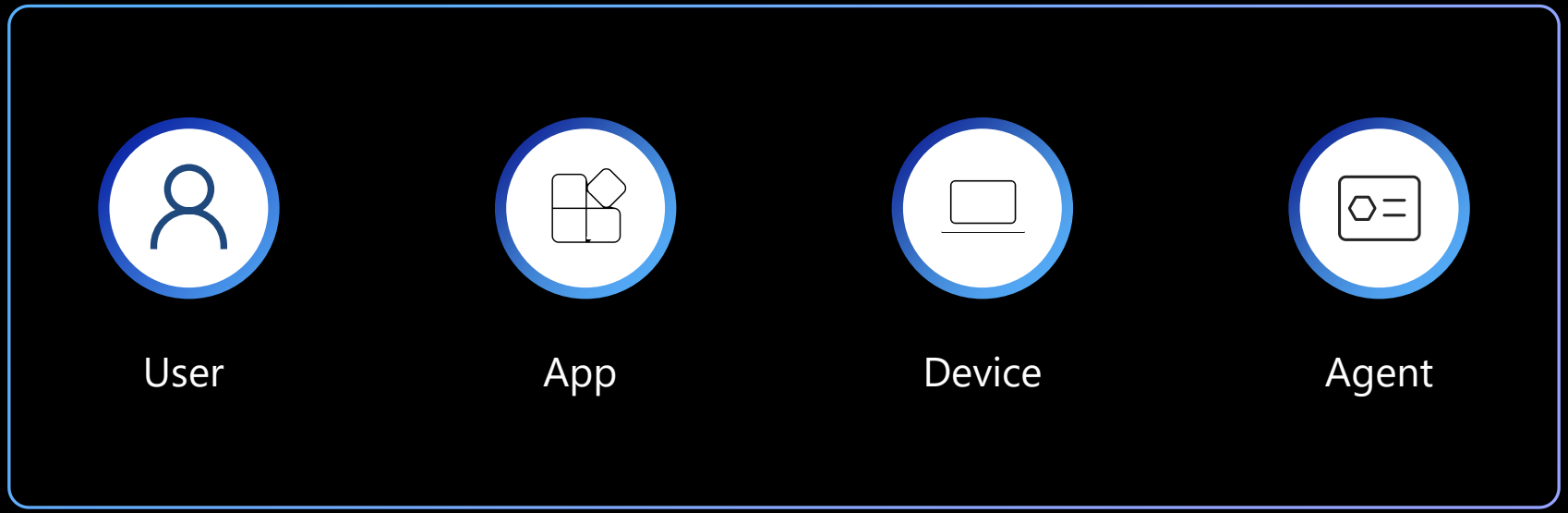


Inter-Tenant Isolation with Red Tenant



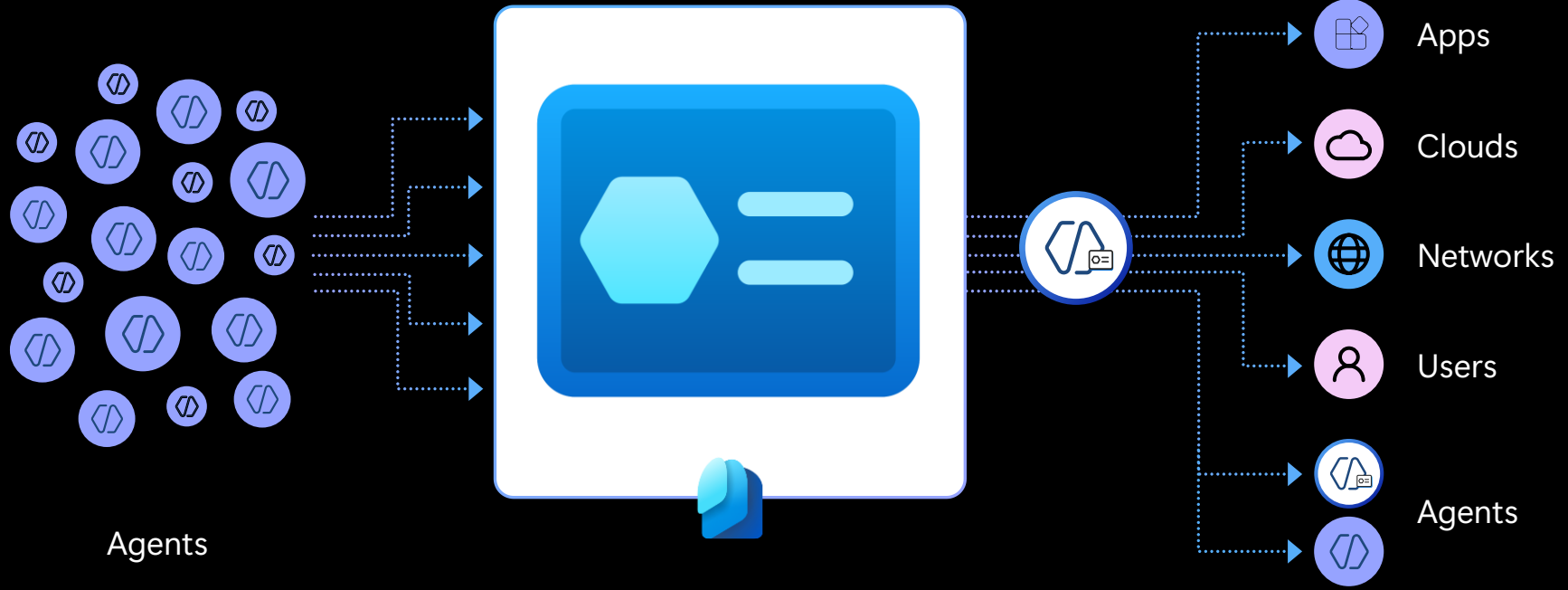
Securing agentic AI using Microsoft Entra Agent ID

Agents are a new type of identity



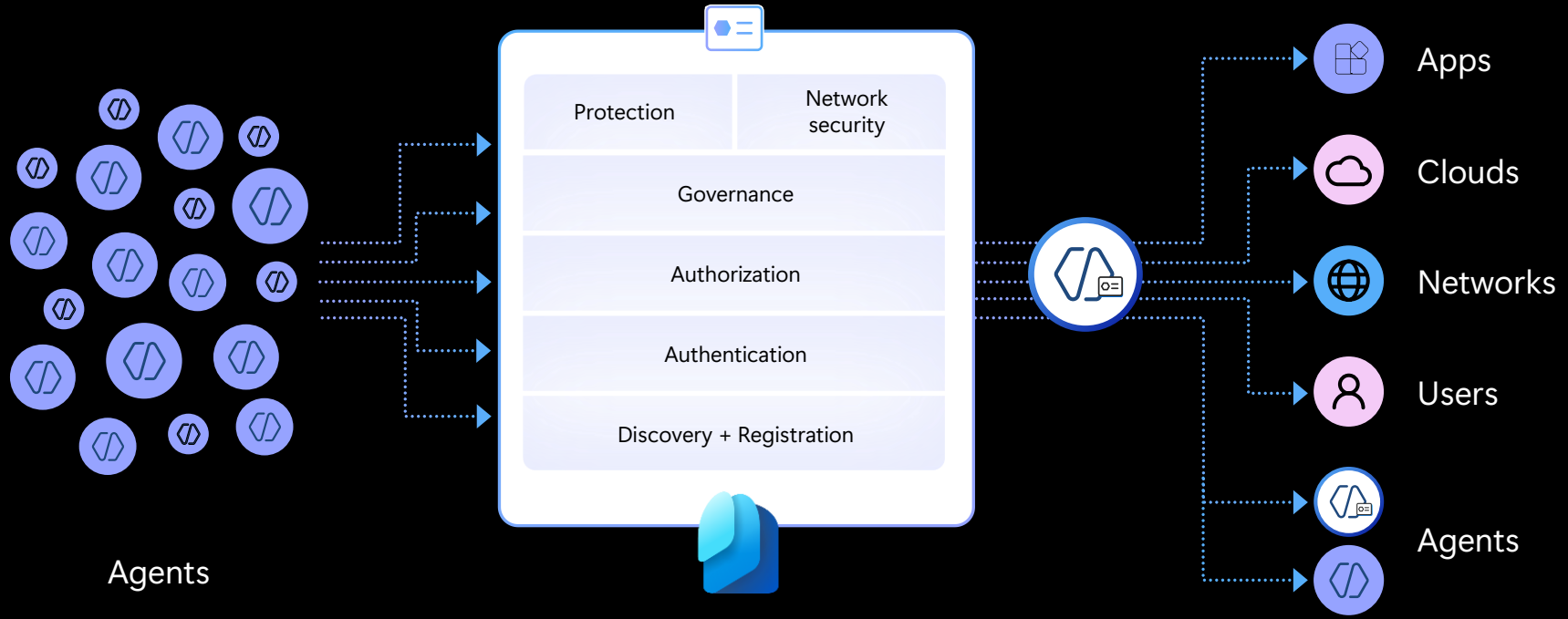
Microsoft Entra Agent ID

Secure access for AI agents - just as you do for employees - with enterprise-grade access management, protection, and governance of agent identities.



Microsoft Entra Agent ID

Secure access for AI agents - just as you do for employees - with enterprise-grade access management, protection, and governance of agent identities.



Public Preview

Microsoft Entra Agent ID

Secure access for AI agents

Register and manage agents

Govern agent identities and lifecycle

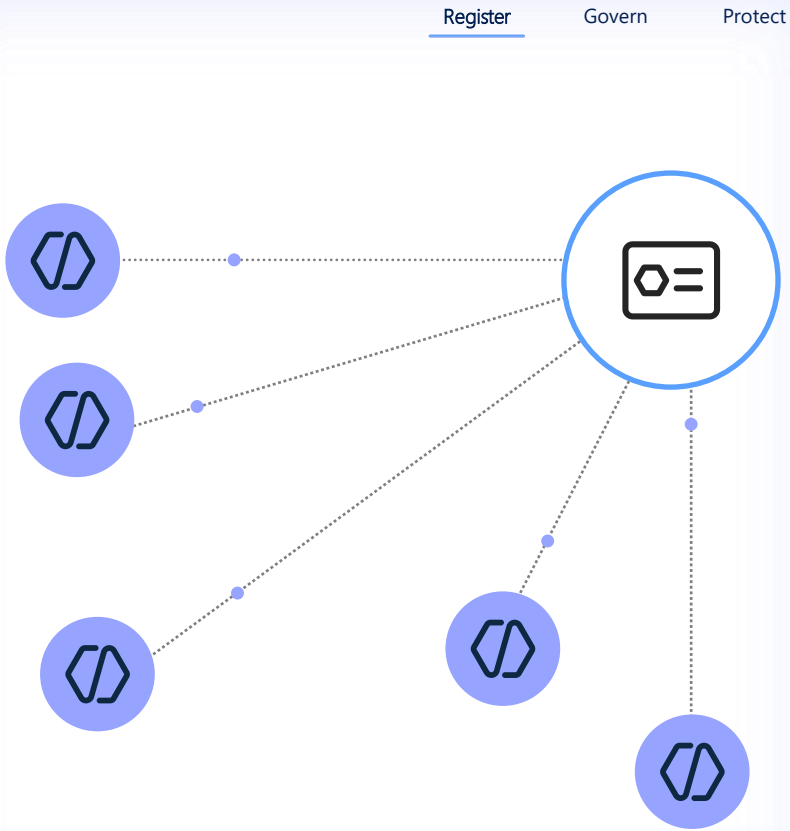
Protect agent access to resources

aka.ms/EntraAgentID

Register and manage agents

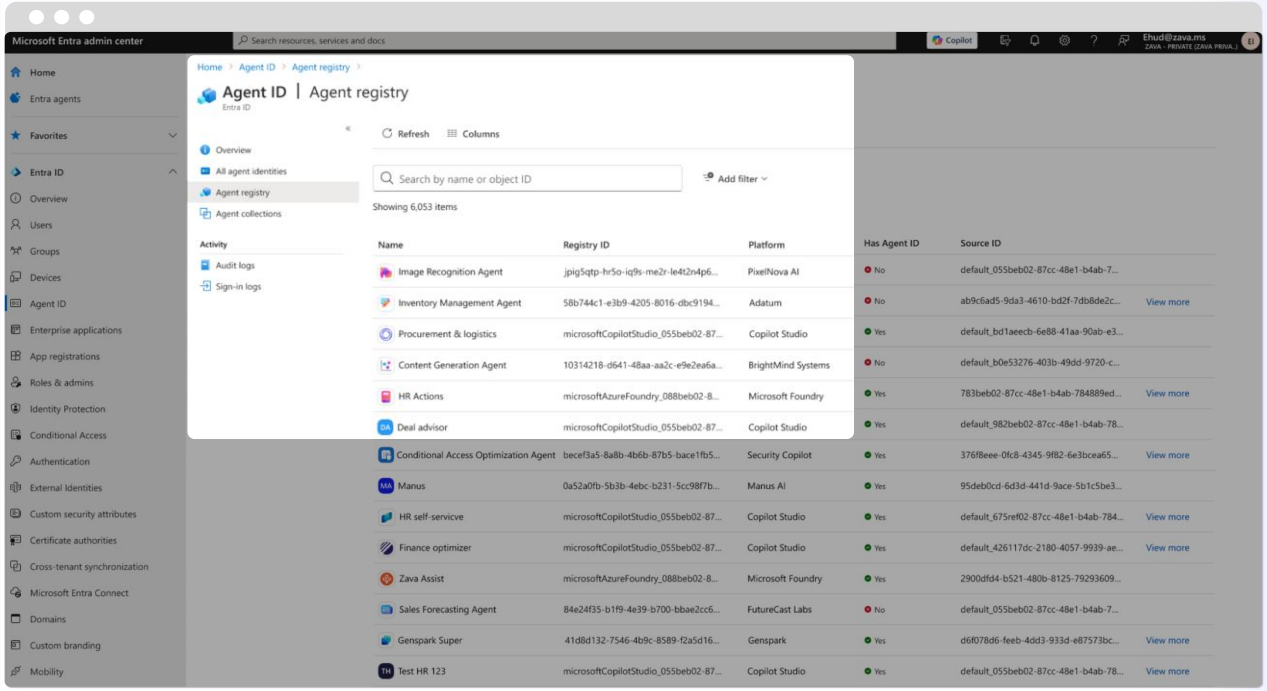
Get a complete inventory of your agent fleet and ensure agents are created with a built-in identity.

- Gain visibility into agents in your environment.
- Ensure that new agents have an agent ID built-in.
- Empower developers to build enterprise-ready agents.



Unify agents in a registry

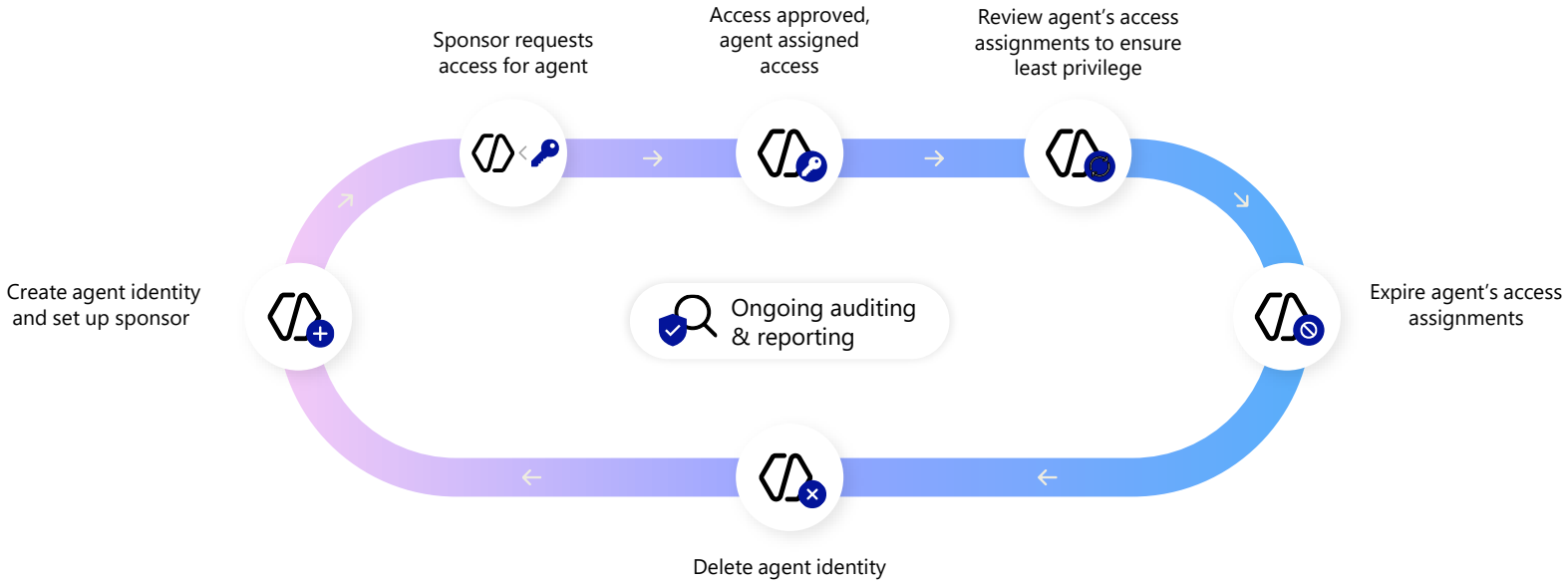
Discover and bring all agents under management with IT-defined guardrails using agent collections.



Govern agent identities and lifecycle

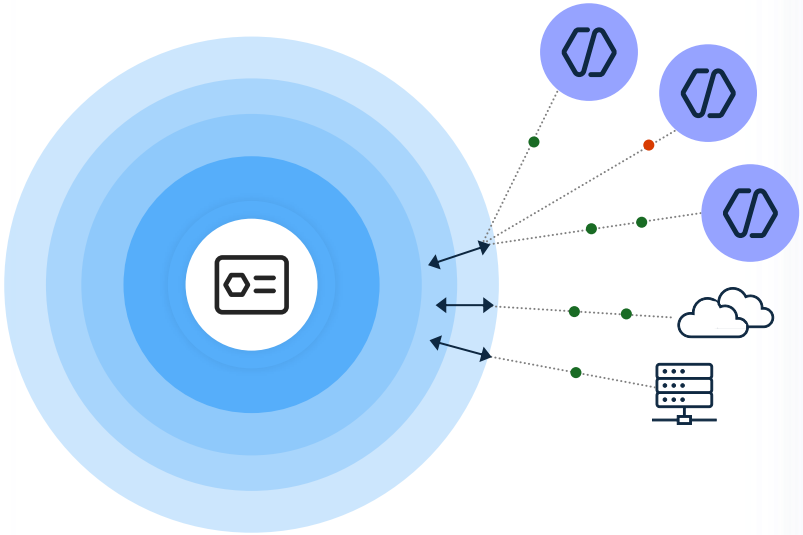
Keep your agent fleet under control with lifecycle management and pre-defined guardrails.

Automate agent identity lifecycle workflows

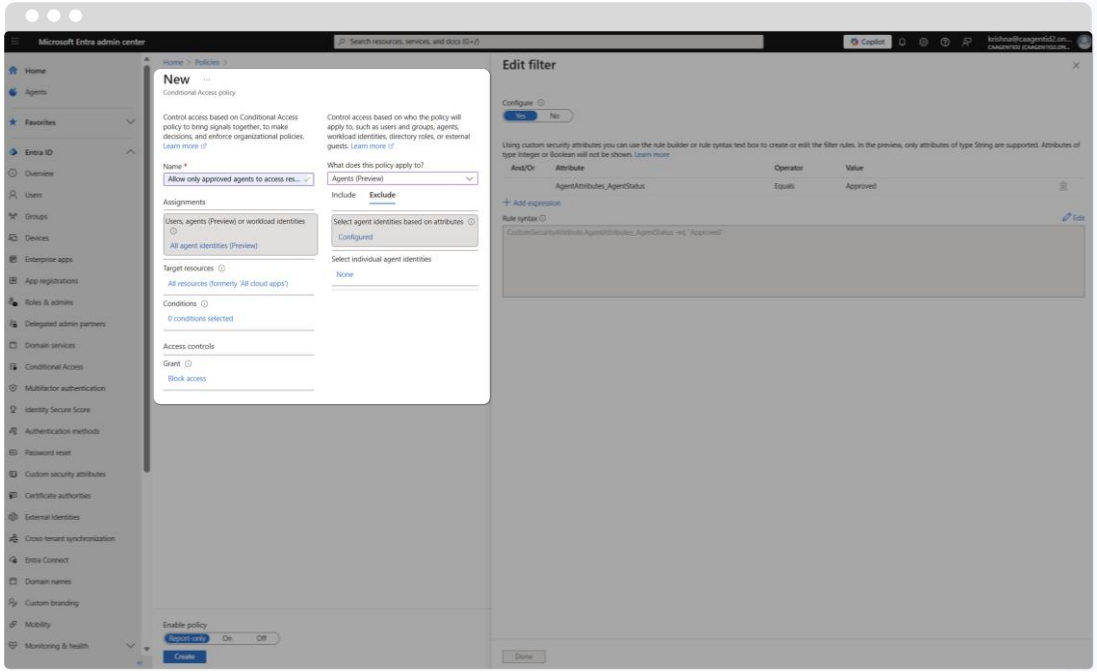


Protect agent access to resources

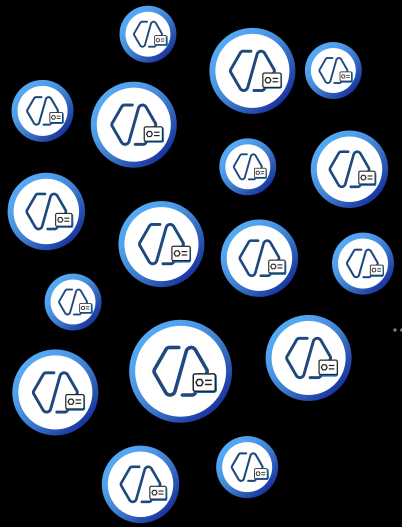
Reduce risk of breaches and prevent malicious agent access to resources.



Apply Conditional Access for agents



Safeguard agents with network controls



Microsoft Copilot Studio agents

Threat intelligence filtering

Web content and URL filtering

Network file filtering

Secure Web + AI Gateway

Microsoft

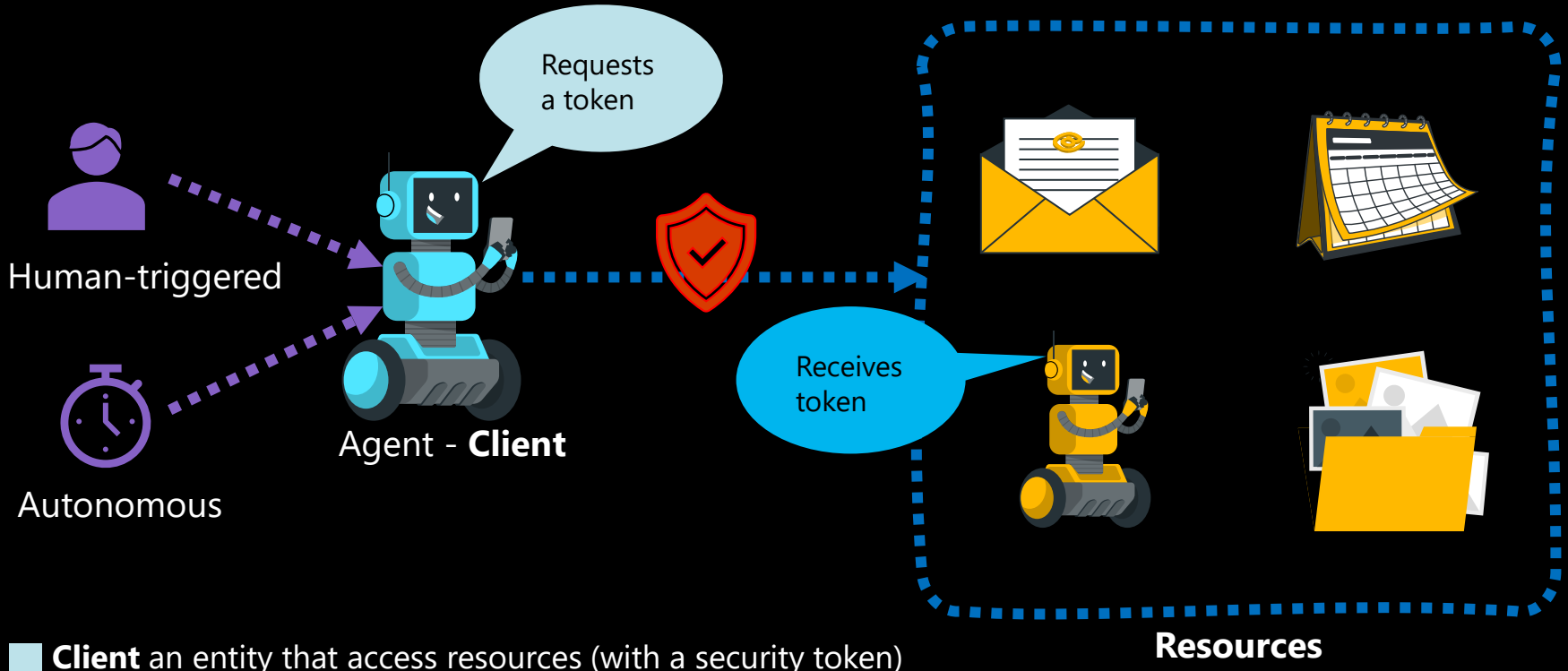
Internet SaaS

+ Knowledge Sources

Protect agent access to resources

Agent Flows

Agent interaction patterns



- **Client** an entity that access resources (with a security token)
- **Resource** a service or system being accessed for the data

Agent Flows

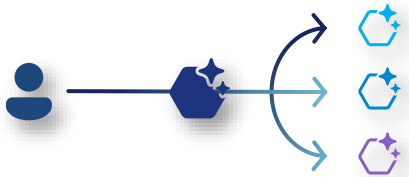
Interactive Agent

Single, specific, defined, repetitive tasks
"Summarize this email."

Acts on-demand on user's behalf

Autonomous Agent

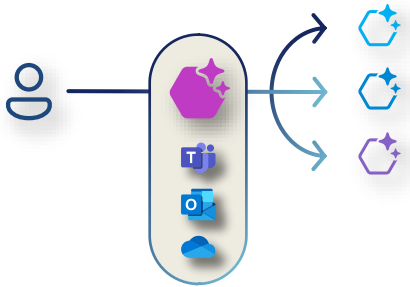
Complex, goal-oriented
Creates plans to achieve outcomes



Coordinates actions on user's behalf and on user's schedule

Digital Colleague

Learning-driven
Emulates human decision making



Provisioned its own access and resources; achieves goals on own behalf and schedule

On behalf of flow

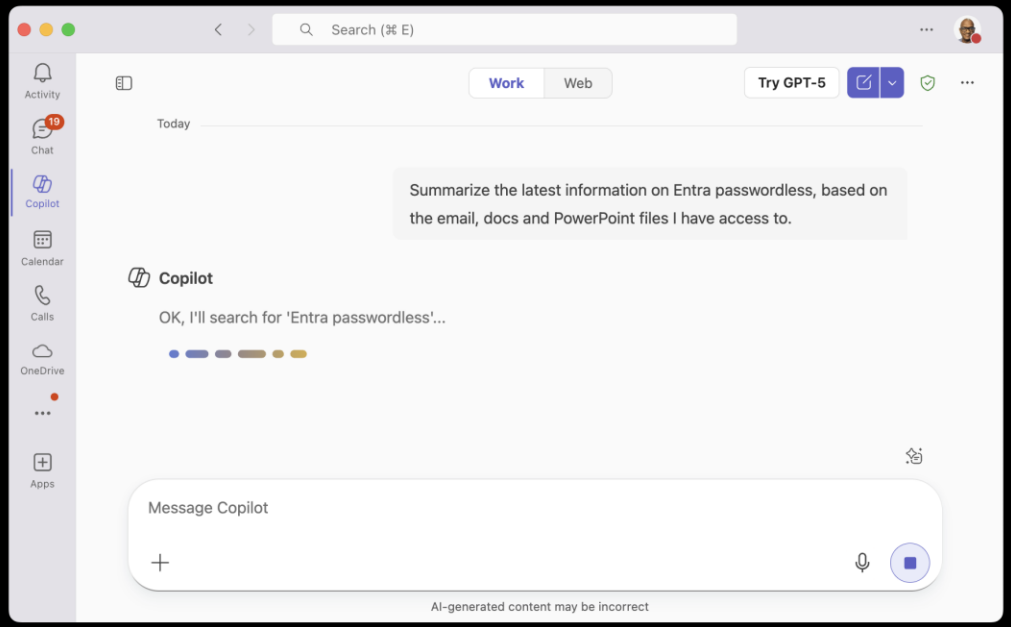
Autonomous App Flow

Agentic User Flow

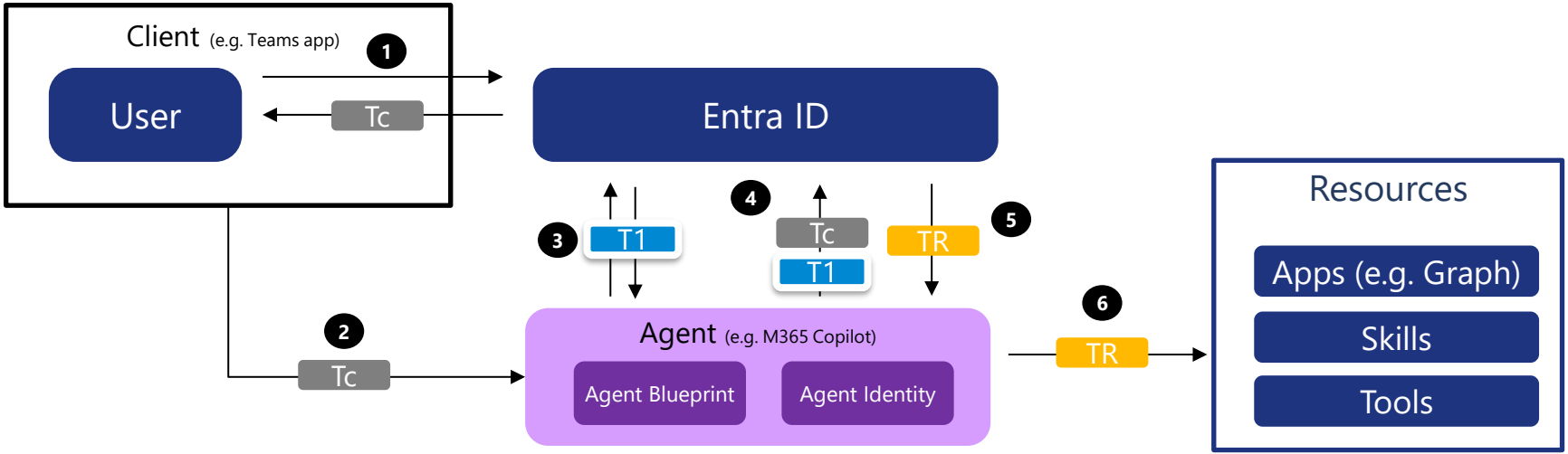
On behalf of flow - summary

Agent Identity operates on behalf of regular user

In the example below, M365 copilot Agent uses signed-in user's identity to make graph API calls on behalf of the user

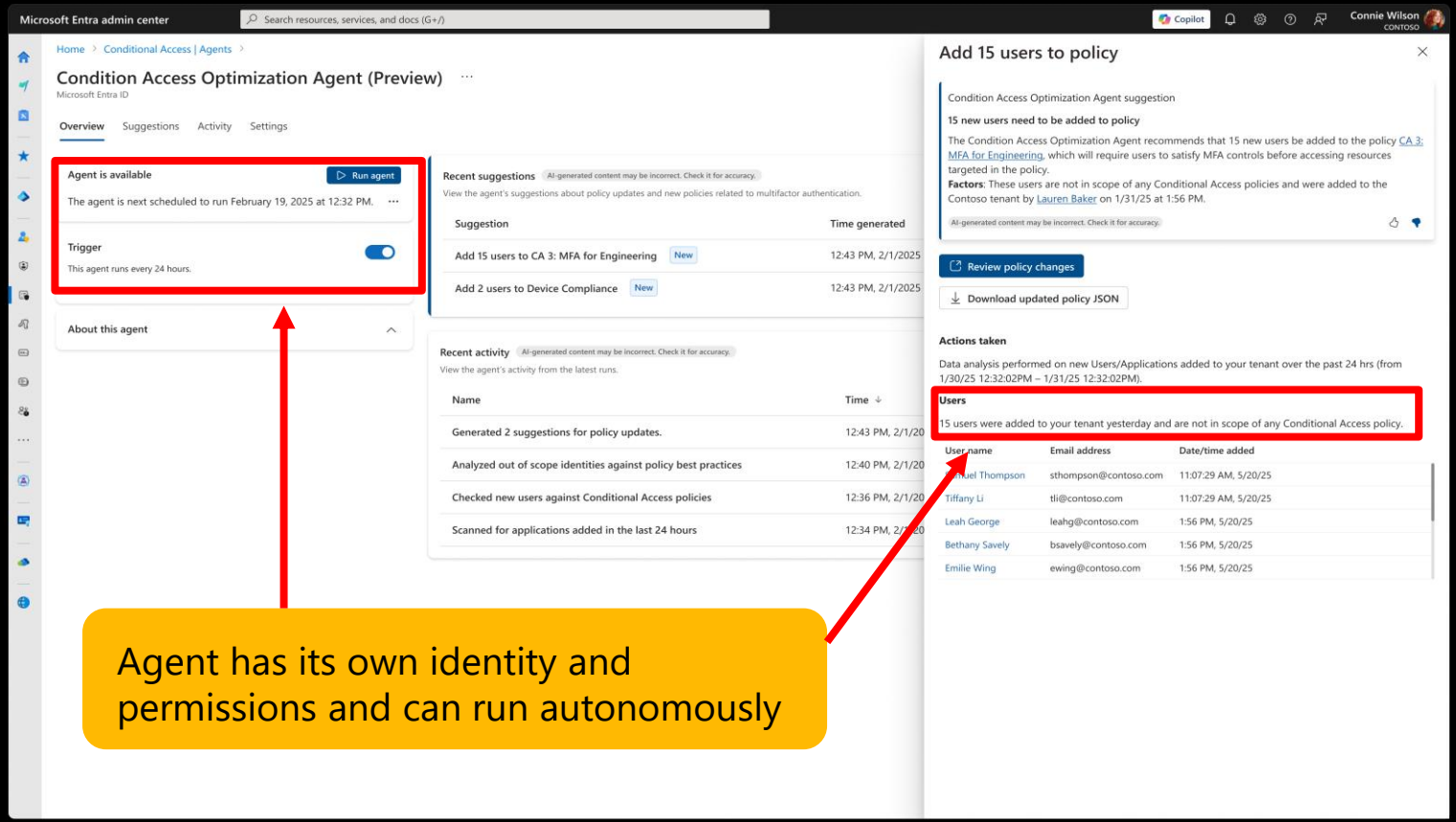


On behalf of flow - diagram

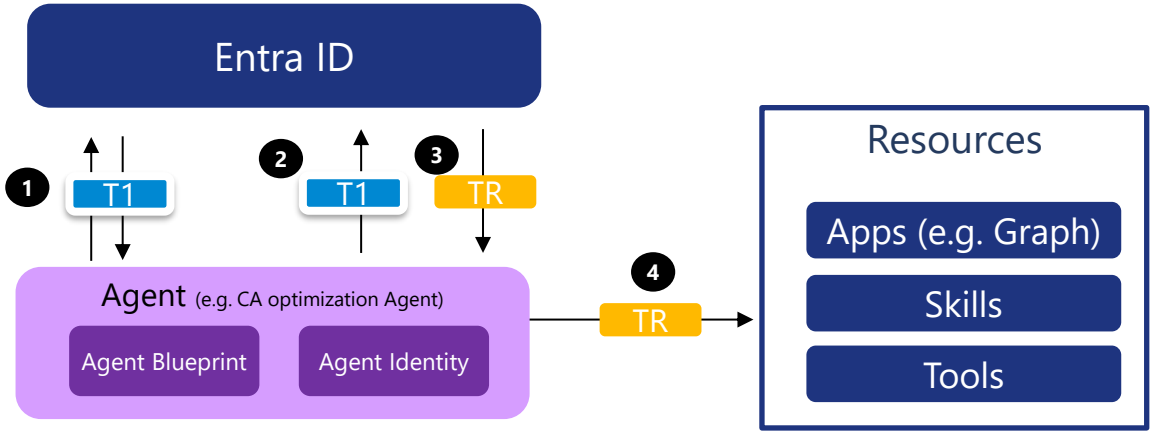


1. User authenticates with the Client and obtains a User Access Token (Tc)
2. Client sends the User Access Token (Tc) to the Agent Blueprint to act on behalf of the user
3. Agent Blueprint requests a FIC Exchange Token (T1) from Entra ID using MSI, Entra ID returns the T1 to Agent
4. Agent Identity sends an OBO token exchange request to Entra ID, including both T1 and the User Access Token (TC)
5. Entra ID issues a Resource Access Token (TR) to the Agent Identity after validating both T1 and TC
   - T_1.Aud == AgentIdentity.ParentApp == Agent Blueprint
   - T_C.Aud == Agent Blueprint
6. Agent Identity accesses the Resource using the Resource Access Token (TR)

Autonomous App flow - summary

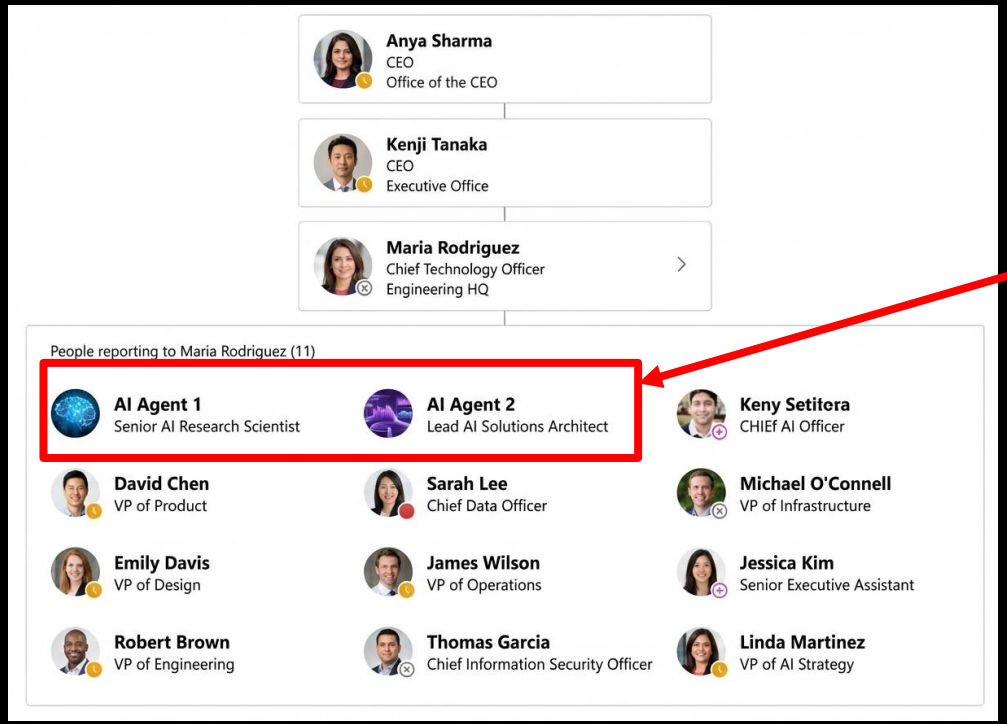


Autonomous App flow



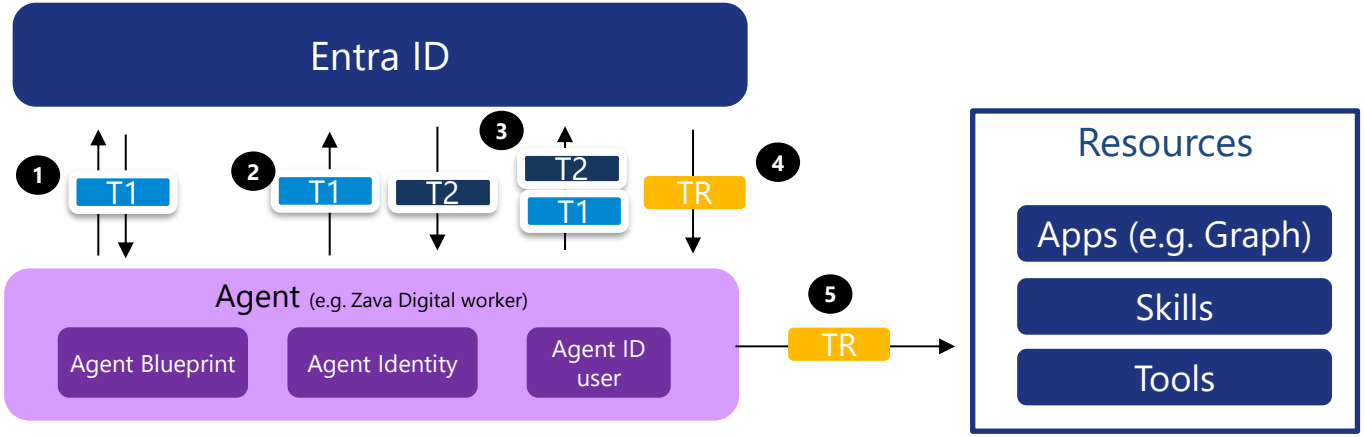
1. Agent Blueprint requests a FIC Exchange Token (T1) from Entra ID using MSI, Entra ID returns the T1 to Agent
2. Agent Identity sends an OBO token exchange request to Entra ID, including T1
3. Entra ID issues a Resource Access Token (TR) to the Agent Identity after validating T1
   - T_1.Aud == AgentIdentity.ParentApp == Agent Blueprint
4. Agent Identity accesses the Resource using the Resource Access Token (TR).

Agentic user flow - summary



Autonomous human-like agent that can use Teams, Outlook and other applications just like a real person.
The agent's identity is in HR and other systems.
The Agent user has delegate permission to Graph and other resources.

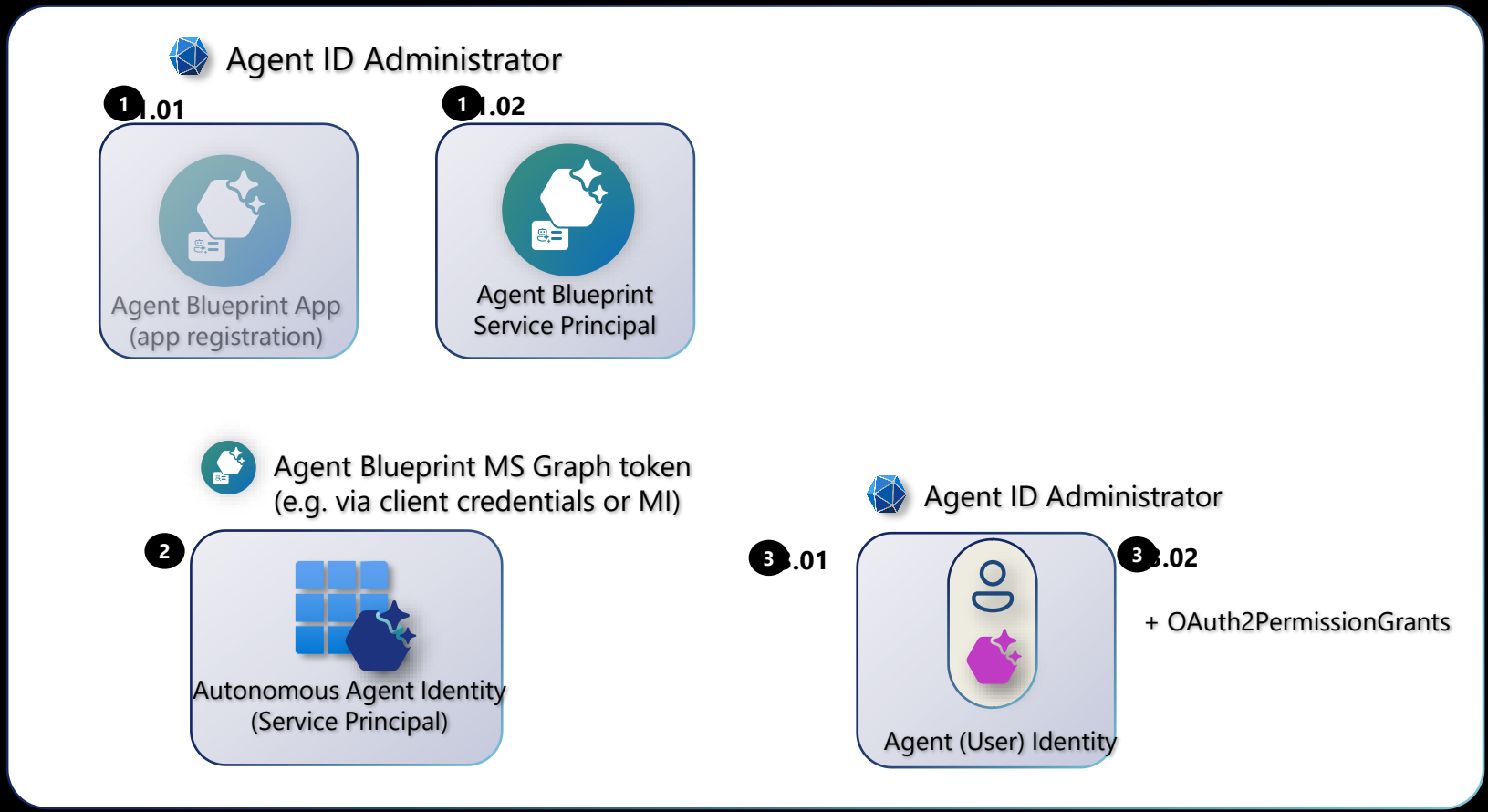
Agentic user flow



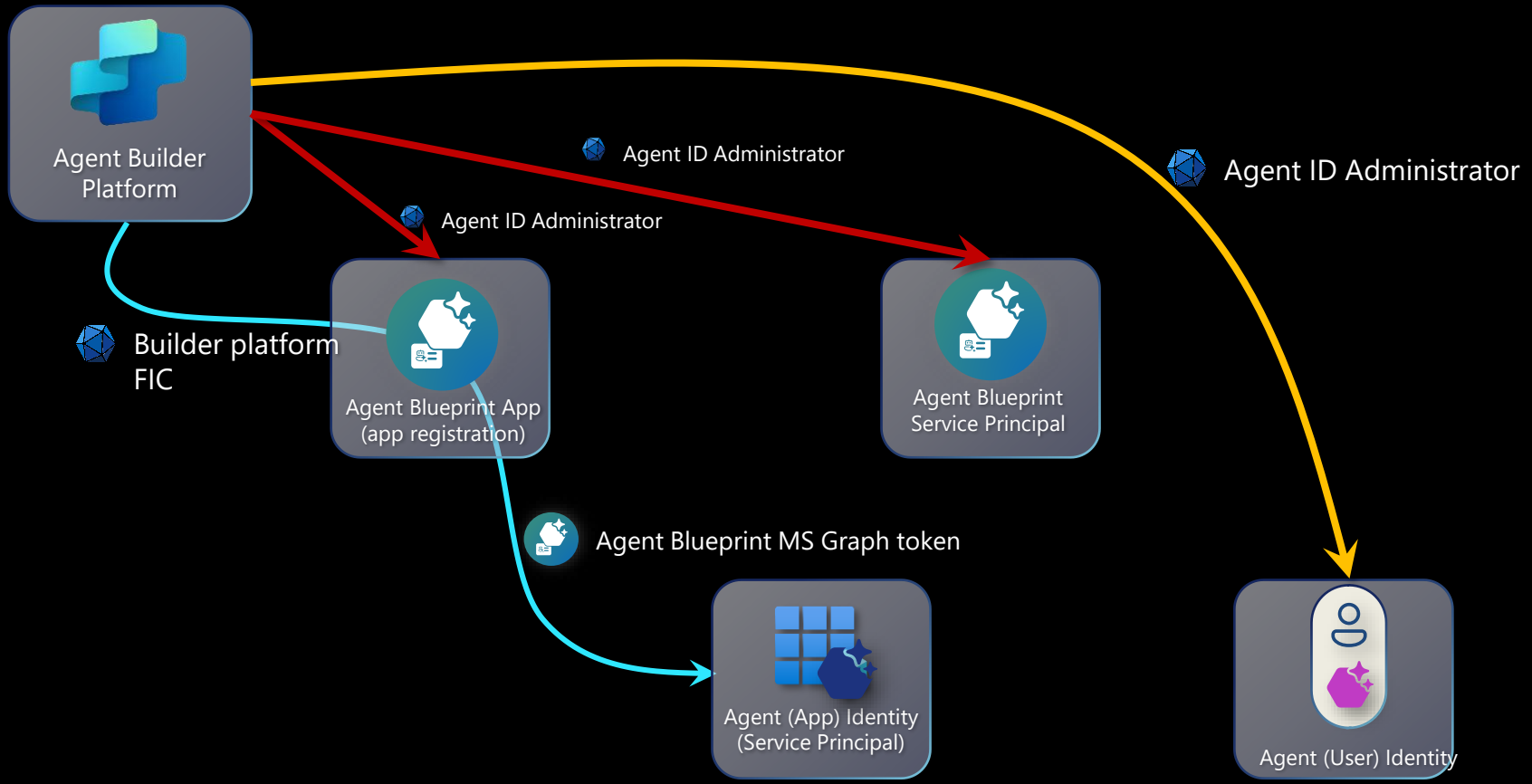
1. Agent Blueprint requests a FIC Exchange Token (T1, for Agent Identity impersonation) from Entra ID using MSI, Entra ID returns the T1 to Agent
2. Agent Identity requests a FIC Exchange Token (T2, for Agent ID user impersonation) using T1, Entra ID returns the T2 to Agent Identity
   - Entra ID validates T1.Aud == AgentIdentity.ParentApp == Agent Blueprint
3. Agent Identity sends an OBO token exchange request to Entra ID, including both T1 and T2
   - Entra ID validates T2.Aud == Agent ID User.ParentApp == Agent Identity
4. Entra ID issues a Resource Access Token (TR) to the Agent Identity after validating both T1 and T2
5. Agent ID user accesses the Resource using the Resource Access Token (TR).

Agent ID – Building Blocks

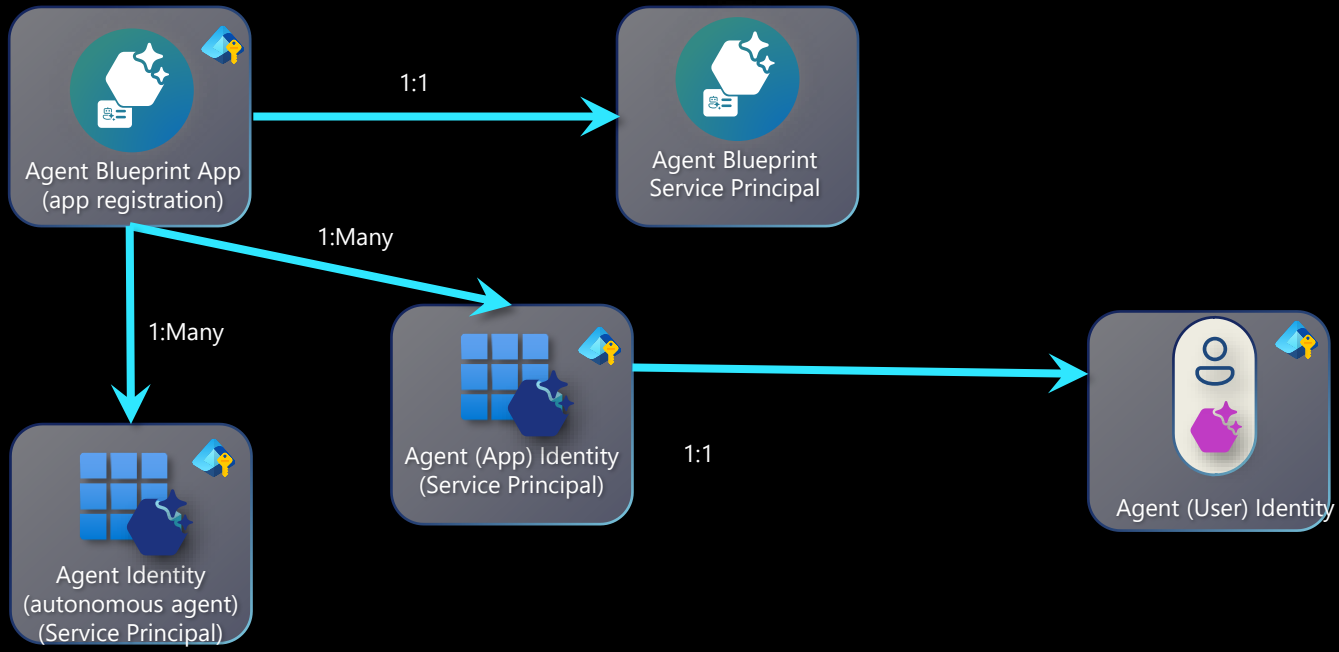
Agent ID - Deconstructed



Artifacts creation



Artifacts relationships



Developer

Create

Agent Platforms

Create

Agent Identity Blueprint

Composed of

AgentIdentityBlueprintApplication
+
AgentIdentityBlueprintServicePrincipal

Create (1:M) + Impersonate

Agent Identity

Represented by

Service Principal
@odata.type: agentIdentity

[Optional] Create

Agent ID User

Represented by

User Principal
@odata.type: agentUser

Permissions for agent IDs

Option 1

- Each agent ID will request the permissions that the agent needs when needed.
- Users or admins can grant consent
- Each agent needs the permission request/grant experience

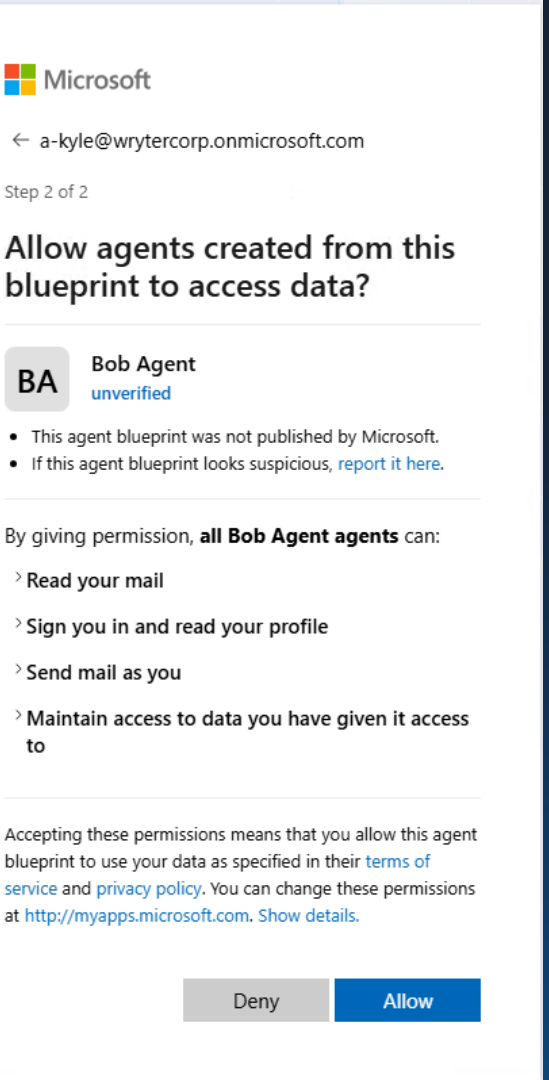
Option 2

- Agents inherit some or all of the permissions granted to the blueprint
- Admin grants consent for all users in the tenant
- Add inheritable permissions to the blueprint
- If not granted, can not be inherited

Option 3

- Use both option 1 and option 2

```
beta/applications/microsoft.graph.agentIdentityBlueprint/
<blueprintID>/inheritablePermissions
```


Microsoft
a-kyle@wrytercorp.onmicrosoft.com
Step 2 of 2
Allow agents created from this blueprint to access data?
BA
Bob Agent
unverified
This agent blueprint was not published by Microsoft.
If this agent blueprint looks suspicious, report it here.
By giving permission, all Bob Agent agents can:
Read your mail
Sign you in and read your profile
Send mail as you
Maintain access to data you have given it access to
Accepting these permissions means that you allow this agent blueprint to use your data as specified in their terms of service and privacy policy. You can change these permissions at http://myapps.microsoft.com. Show details.
Deny
Allow

High Privilege Access (HPA) Permissions

Entra prevents HPA permissions from being granted to agents.

Neither users nor admins can grant consent to these permissions

Entra's goal is to move toward fine-grained, task-specific access so agents can perform critical operations safely with minimal risk.

Example of Application HPA permissions

AgentIdentity.Create

AgentIdentityBlueprint.Create

Application.ReadWrite.All

Directory.ReadWrite.All

RoleManagement.ReadWrite.All

User.ReadWrite.All

Example Delegated HPA permissions

Directory.AccessAsUser.All

Directory.ReadWrite.All

User.ReadWrite.All

https://aka.ms/agentid-blocked-perms

Where do agent identity blueprints come from?

- Microsoft products
  - Copilot Studio, Microsoft AI Foundry, Agent 365
  - When you create your agent on a Microsoft agent platform you don't need the details
- Microsoft Graph APIs
  - PowerShell (https://github.com/AzureAD/MSIdentityTools)
  - Any app that can call Microsoft Graph (https://github.com/azure-Samples/ms-identity-agent-identities)
- Microsoft Entra ID consent experience
  - Multi-tenant blueprint
  - Create the Agent identity blueprint principal in the tenant

Microsoft

a-kyle@wrytercorp.onmicrosoft.com

Step 1 of 2

Add this agent blueprint to your organization?

BA

Bob Agent

unverified

This adds the agent blueprint to your organization and **allows it to create agent accounts**. These accounts will be visible in MyAgents.

Learn more about agents, access, and permissions.

This agent blueprint was not published by Microsoft. If it looks suspicious, report it here.

Adding this agent blueprint means you accept its terms of service and privacy policy.

No | Yes

Create an agent identity blueprint

Need AgentIdentityBlueprint.Create permission (admin consent only)
Need an Agent ID Administrator or Agent ID Developer role
Alternatively, an app with AgentIdentityBlueprint.Create as an app permission
Can create 250 agent identity blueprints

Required to provide an owner or a sponsor. Sponsor preferred.

Limits

Apps using app-only permissions can create 250 Blueprints per tenant

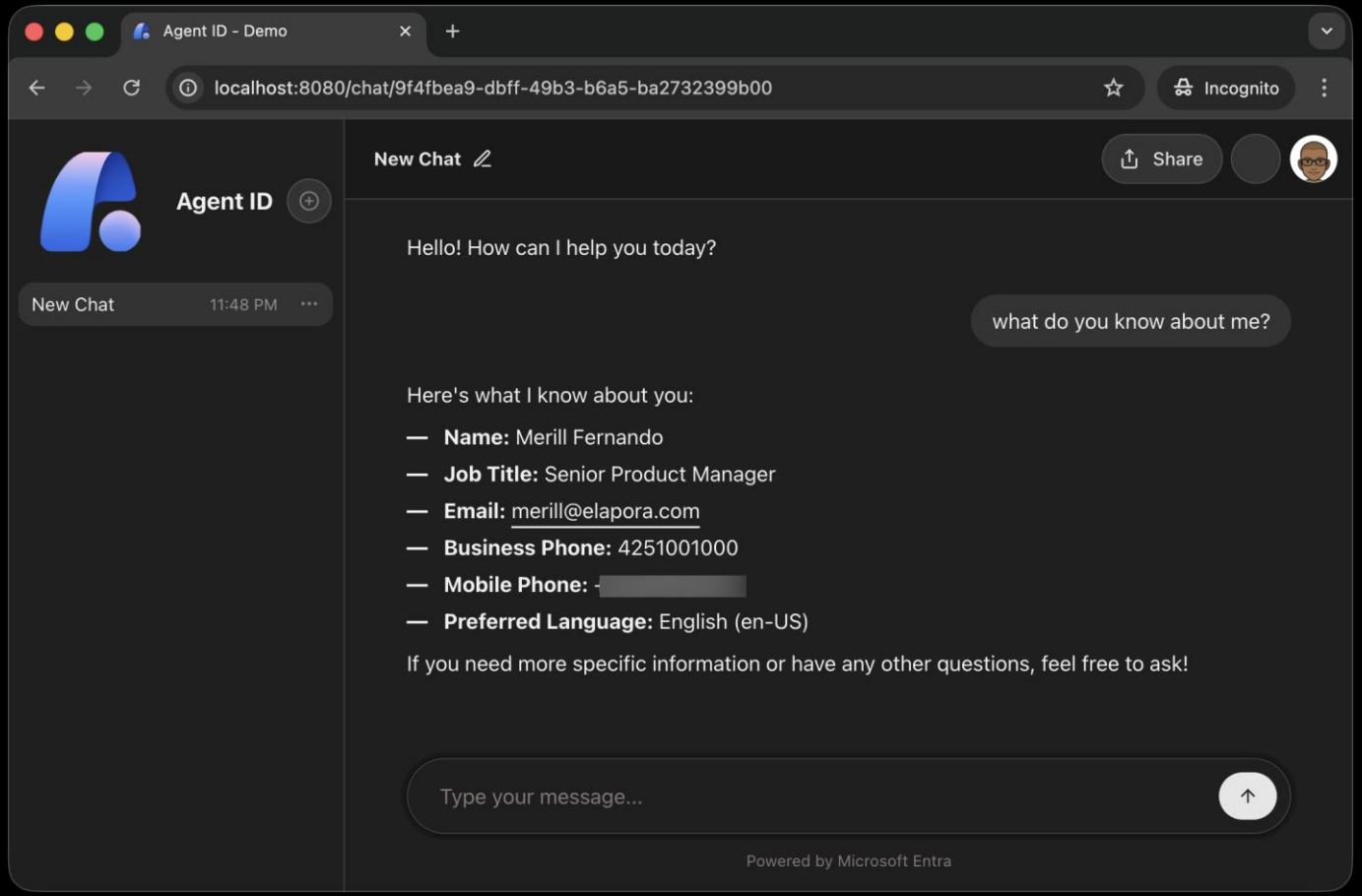
250 Agent IDs per blueprint

Deleted agents count until hard deleted

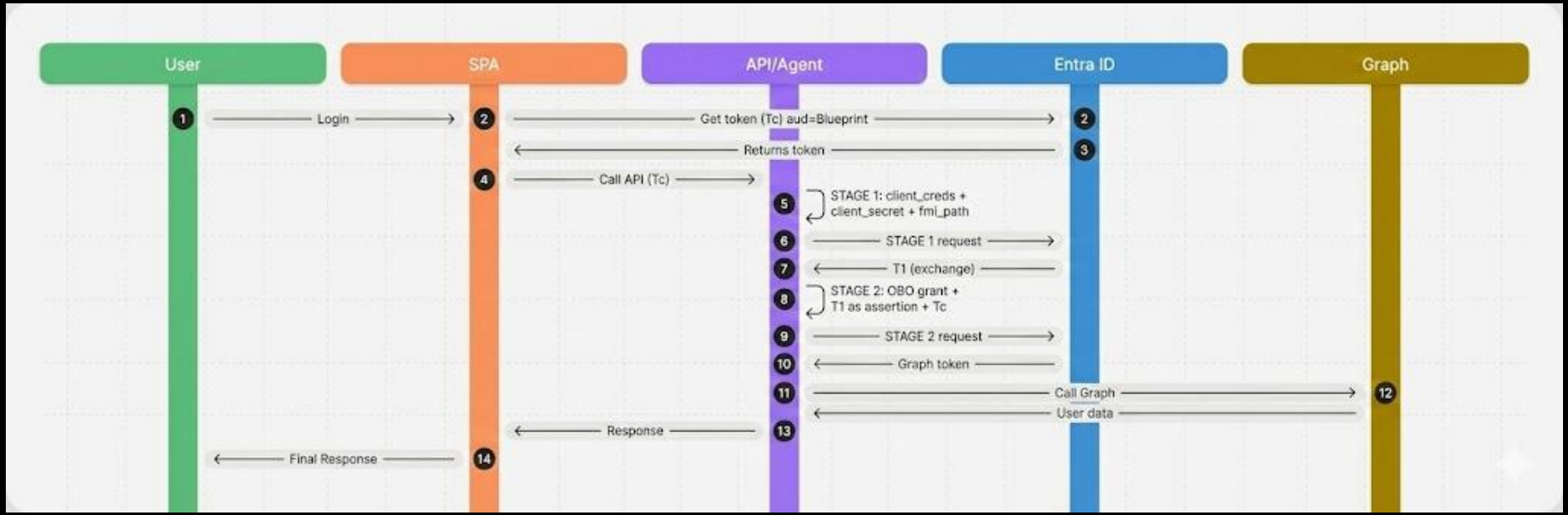
Overall tenant limits apply

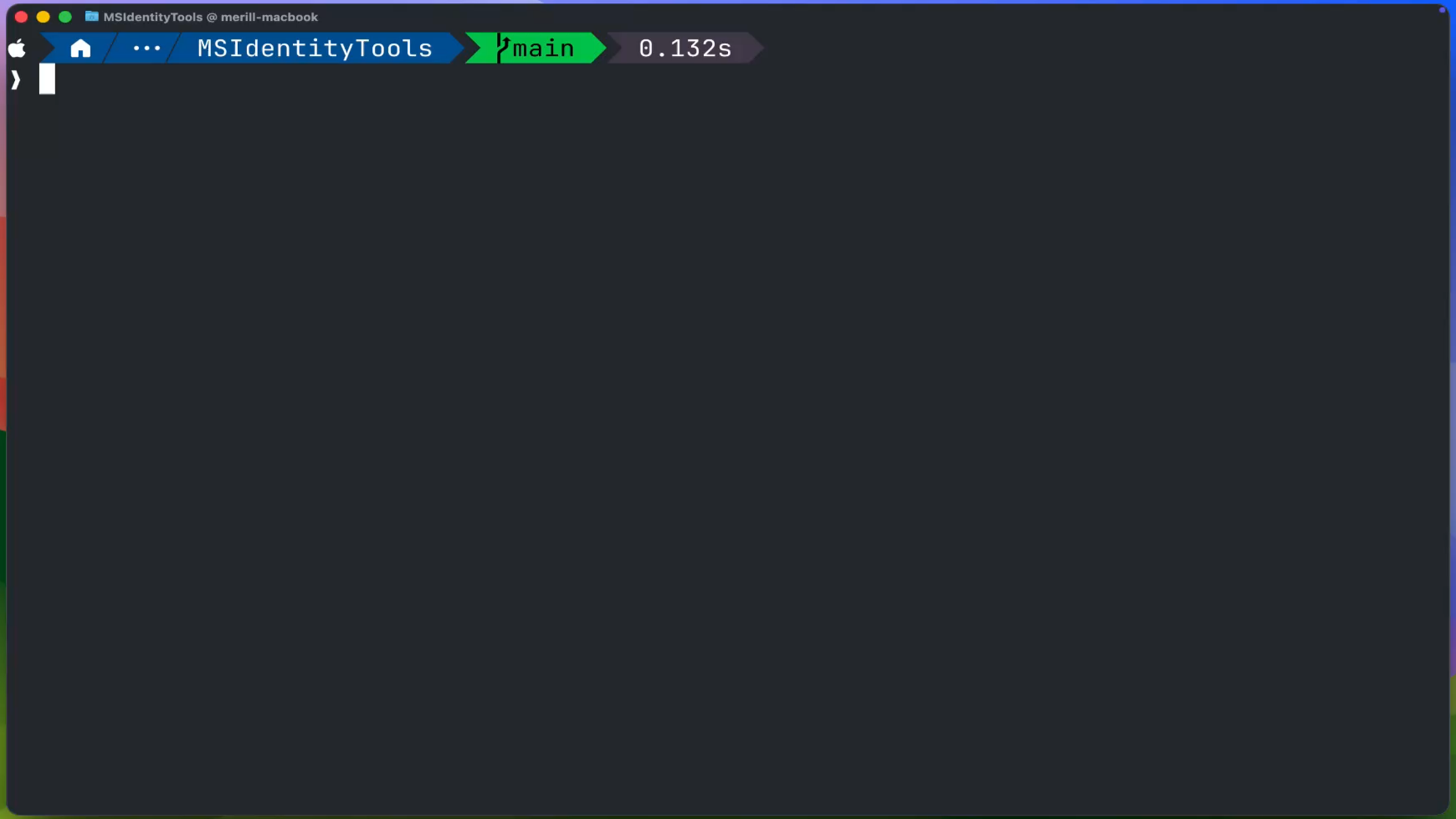
Agent ID

Lab Overview



Agent ID – Lab Overview




MSIdentityTools @ merill-macbook
MSIdentityTools
main
0.132s

DEMO

LAB 4: Creating a custom agent with Agent ID

https://aka.ms/eldk26

Monitoring, Maintaining, Disaster Recovery

Backup Restore

Entra object restore – reality check

Object type	Soft delete	Restore?
User object	✓	30d Recyc
Security group	✓	~~No restore~~
M365 group	✓	30d Recyc
Device object	✗	No restore
Enterprise Application	✓	Multi-Tena Single-Ten
App Registration	✓	Recycle Bi
Administrative Unit	✓	Deleted Ite
Conditional Access	✓	Deleted Ite

Restore via Recycle Bin, no Restore at all, Restore via API


```
{
  "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
  "templateId": null,
  "displayName": "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA",
  "createdDateTime": "2022-07-05T17:05:36.8206457Z",
  "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
  "state": "enabled",
  "deletedDateTime": null,
  "partialEnablementStrategy": null,
  "sessionControls": null,
  "conditions": {
    "userRiskLevels": [],
    "signInRiskLevels": [],
    "clientAppTypes": [ ···
    ],
    "platforms": null,
    "locations": null,
    "times": null,
    "deviceStates": null,
    "devices": null,
    "clientApplications": null,
    "applications": { ···
    },
    "users": {
      "includeUsers": [ ···
      ],
      "excludeUsers": [
        "08a644d4-6533-4931-9158-edee7db7fffa",
        "349c5270-e777-4727-b655-43f99f454dc2"
      ],
      "includeGroups": [],
      "excludeGroups": [
        "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
      ],
      "includeRoles": [],
```

Hard deleted? And now what?

- No support recovery option after hard delete
- Object must be recreated
- Object becomes a new ID
- Previous JSON export required (EntraExporter)
- Example article on rebuilding a hard-deleted Administrative Unit. Additional read:

📖 https://nothingbutcloud.net/2025-08-30-DeletedEntraObjects/

To make sure it never comes down to a restore …

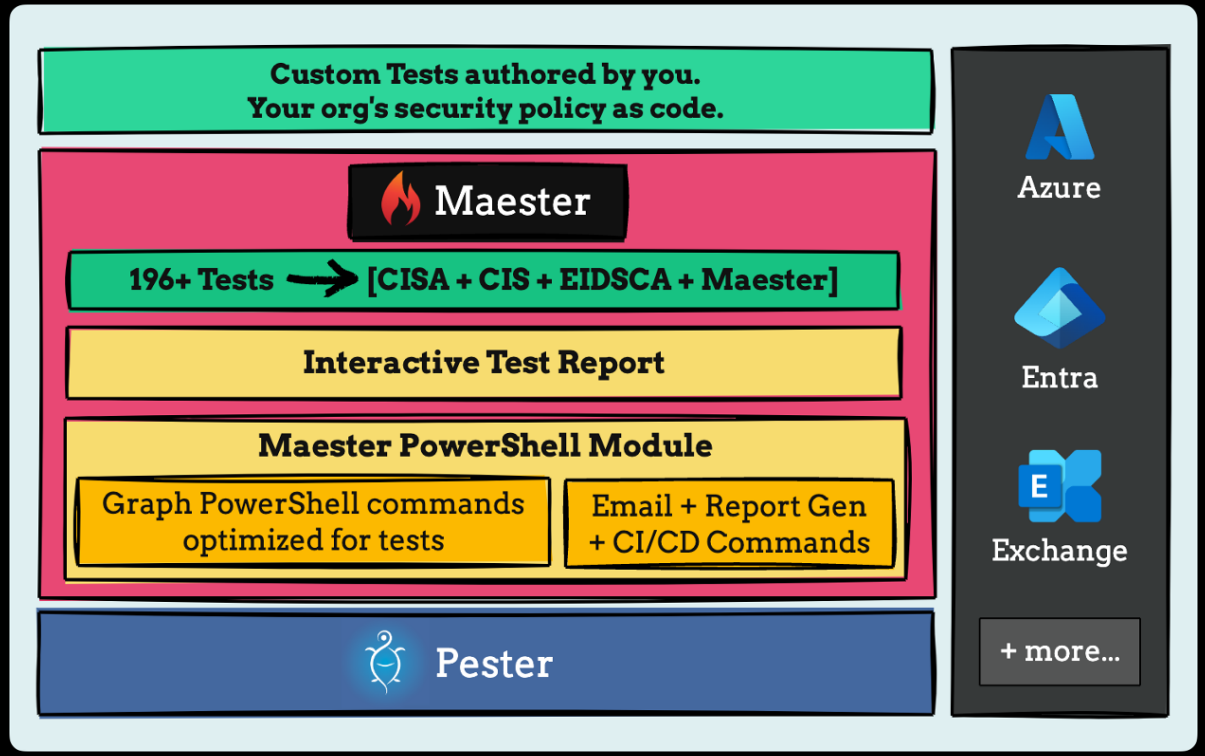
- Protect sensitive Groups with „PIM Protected Groups“
  -> possible, but should you?
- AU – Restricted Management (GA since June 2025)
- Protected Actions for hard deletions (GA since January 2025)
- Smart Alerting for important Resources
  Example implementation. Additional read:

📖 https://nothingbutcloud.net/2025-12-16-ZeroTrust-Monitoring

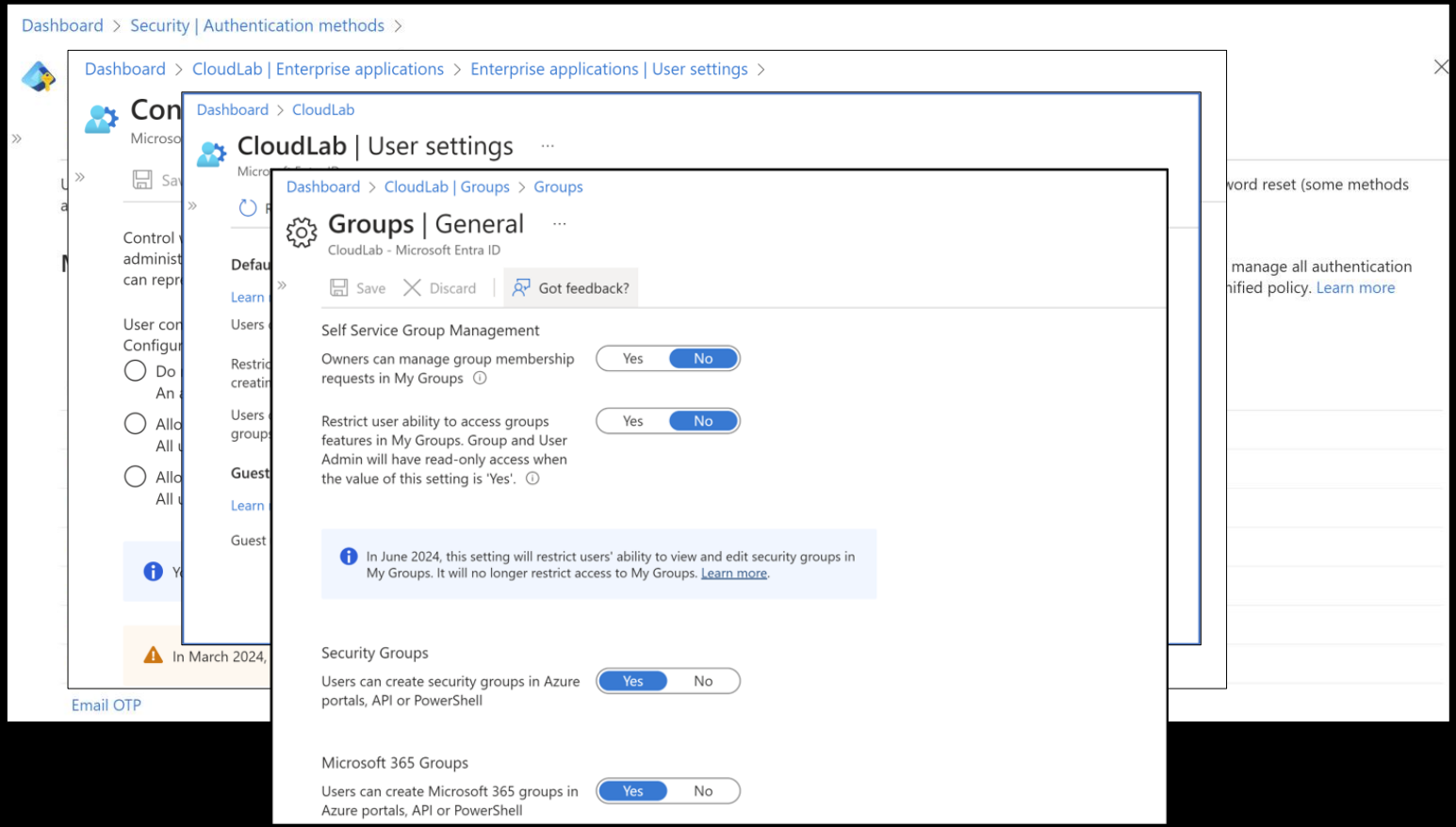
Demo …

Optimize Identity Security Exposure

Overview of Maester Framework



Tenant Hardening of Default Settings



Authorization Policy (Microsoft Graph API)

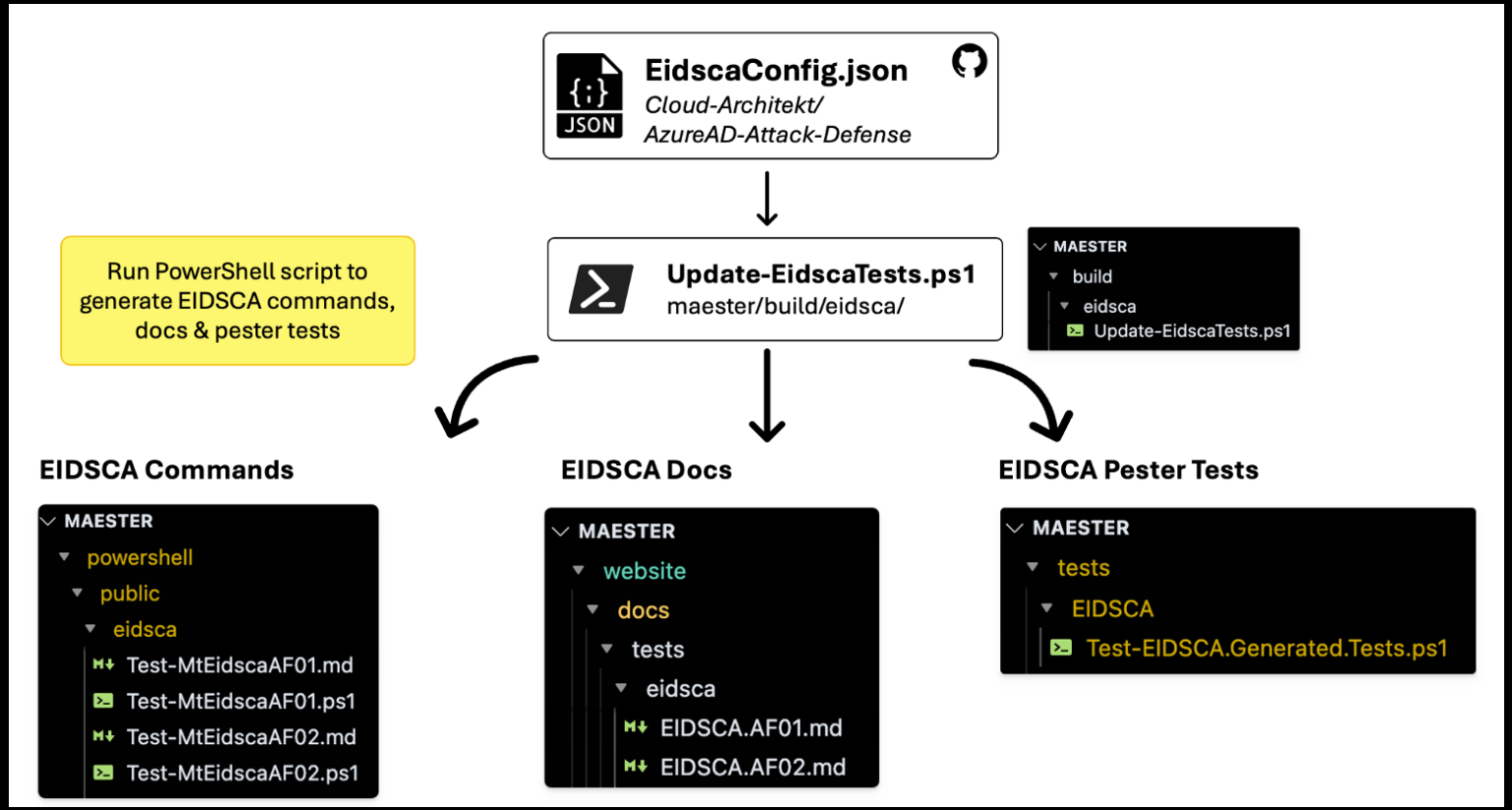
```
GET "https://graph.microsoft.com/beta/authorizationPolicy"
```


```
"@odata.context":
"https://graph.microsoft.com/beta/$metadata#policies/authorizationPolicy",

"value": [
    {
        "displayName": "Authorization Policy",
        "id": "authorizationPolicy",
        "allowInvitesFrom": "adminsAndGuestInviters",
        "allowedToSignUpEmailBasedSubscriptions": true,
        "allowedToUseSSPR": true,
        "defaultUserRolePermissions": {
            "allowedToCreateApps": true,
            "allowedToCreateSecurityGroups": true,
            "allowedToCreateTenants": false,
            "allowedToReadBitlockerKeysForOwnedDevice": true,
            "allowedToReadOtherUsers": true
        }
    }
]
```

Authorization Check (EIDSCA)

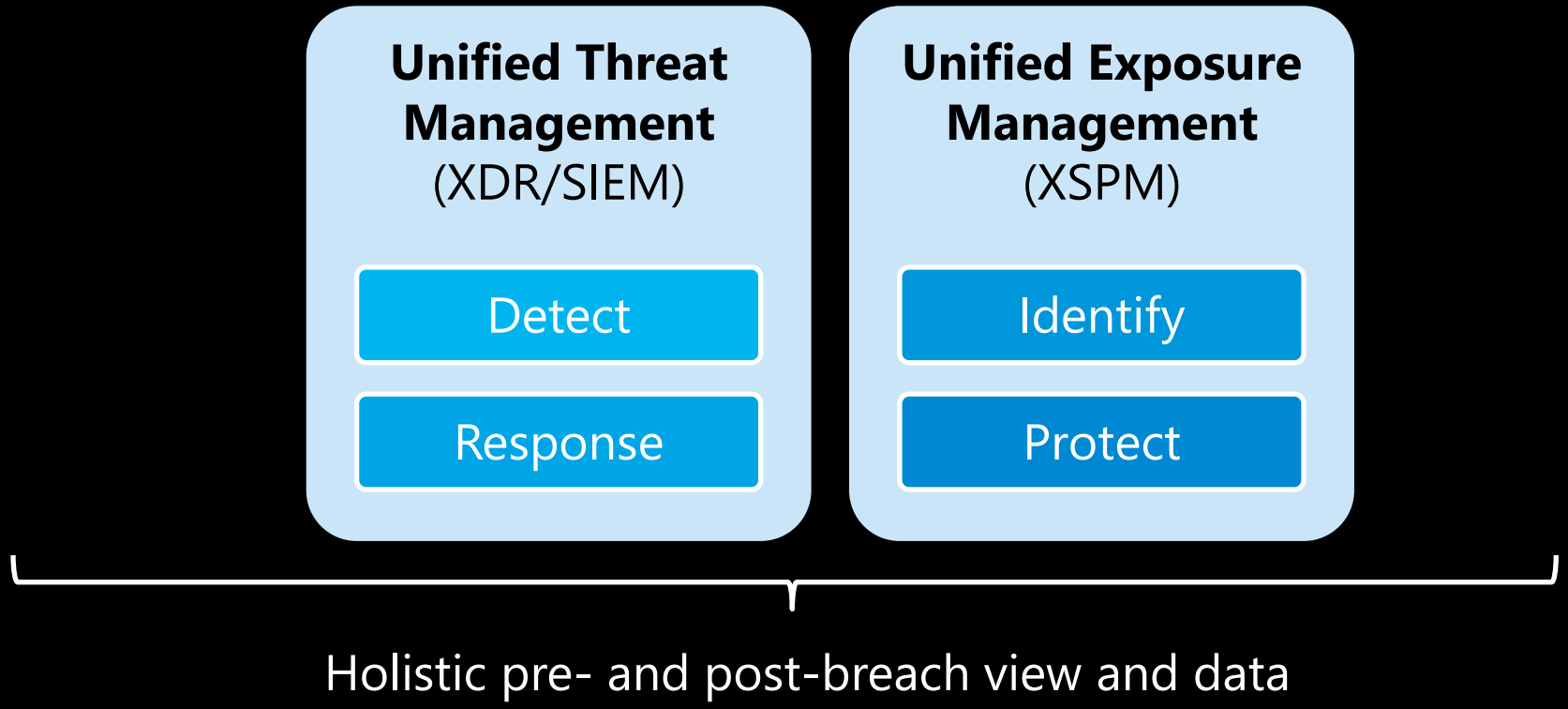
```
"Name": "allowedToCreateApps",
"DisplayName": "Default User Role Permissions - Allowed to create Apps",
"CheckId": "EIDSCA.AP10",

"SkipCondition": "",
"SkipReason": "",

"CurrentValue": "defaultUserRolePermissions.allowedToCreateApps",
"DefaultValue": "true",
"RecommendedValue": "false",

"Recommendation": "CISA SCuBA 2.6: Only Administrators SHALL Be Allowed To Register 3rd Apps",
"Severity": "High",

"MitreTactic": ["TA0001 - Initial Access", ...],
"MitreTechnique": ["T1566.002", ...],
"MitreMitigation": ["M1017", ...],

"PortalDeepLink": "https://entra.microsoft.com/.../UserManagementMenuBlade/~/UserSettings",
"Description": "Controls if non-admin users may register custom-developed applications (...)",
"HowToFix": "Microsoft Graph PowerShell: Update-MgPolicyAuthorizationPolicy (...)"
```

EIDSCA Checks in Maester

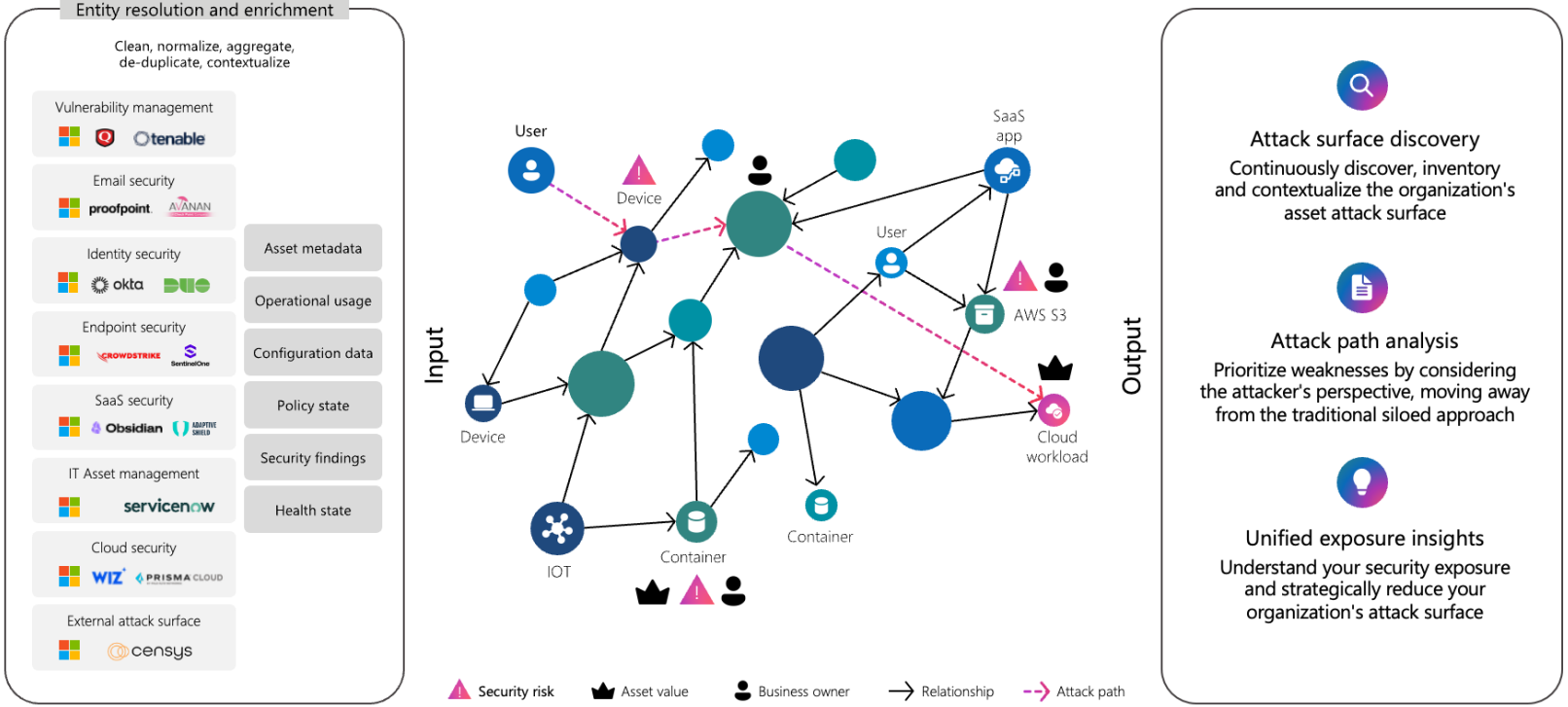


Exposure Management

Exposure Management Overview



Exposure Management Overview



Source "Proactive security with continuous exposure management" (Microsoft Ignite)

Attack paths - Microsoft Defend | Attack paths - Microsoft Defend | Map - Microsoft Defender

https://security.microsoft.com/security-graph?nodeIds=%5B"8fc95387211d4fcf81cb02dfbc6c3a72"%2C"4133eb7cfe9c42cda6f1c152fa1ee124"%2C"0e447a7d9dcd433797d19b21a0d75663"%2C"a7d1a307d9394032a5a79bf...

Zava | Microsoft Defender | Search | Michael Mukasine MM

Map

Scope filter : Off

Search

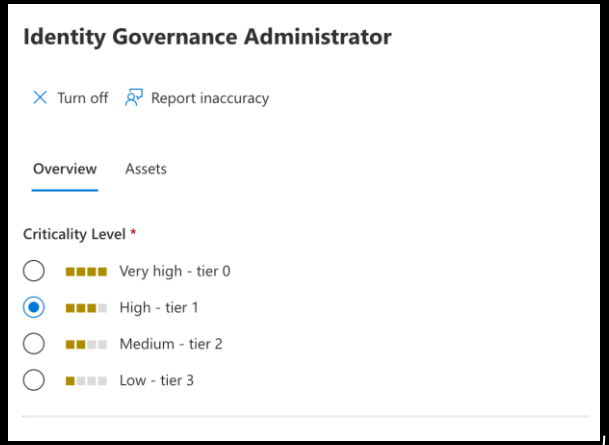
Layers

Discovery Source

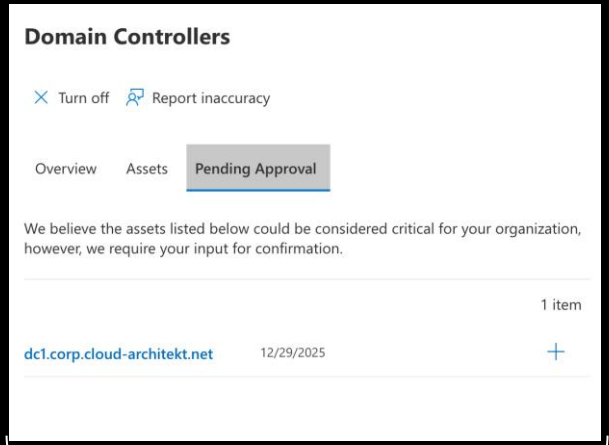
Export | Search

Key	Value
containsSensitiv...	
containsSensitiv...	Sensitivity
criticalityLevel.c...	Critical
criticalityLevel.r...	Critical
criticalityLevel.r...	Databases with Sensitive Data
criticalityLevel.r...	Internet facing
criticalityLevel.r...	criticalResource
criticalityLevel.t...	CriticalityLevel
environmentNa...	Azure
exposedToInter...	76.182.132.142
exposedToInter...	InternetExposure
hierarchyIdentif...	34d58fcf-b44c-4c75-b18d-37a49e3018c9
hierarchyType	subscriptionid
nativeEnvironm...	eastus2
tags.type	TagsData

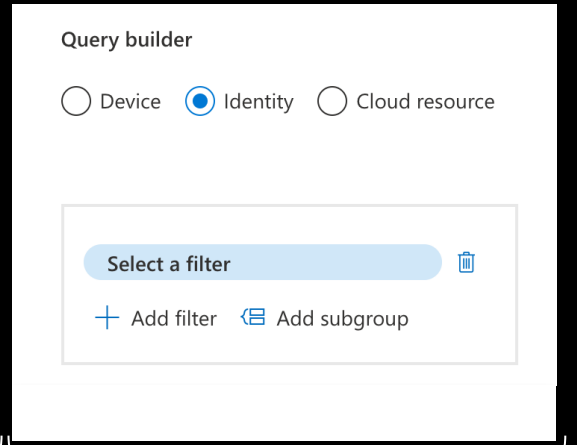
Critical Asset Management



Review Criticality Level
Tier != Tier



Check Pending
Approvals

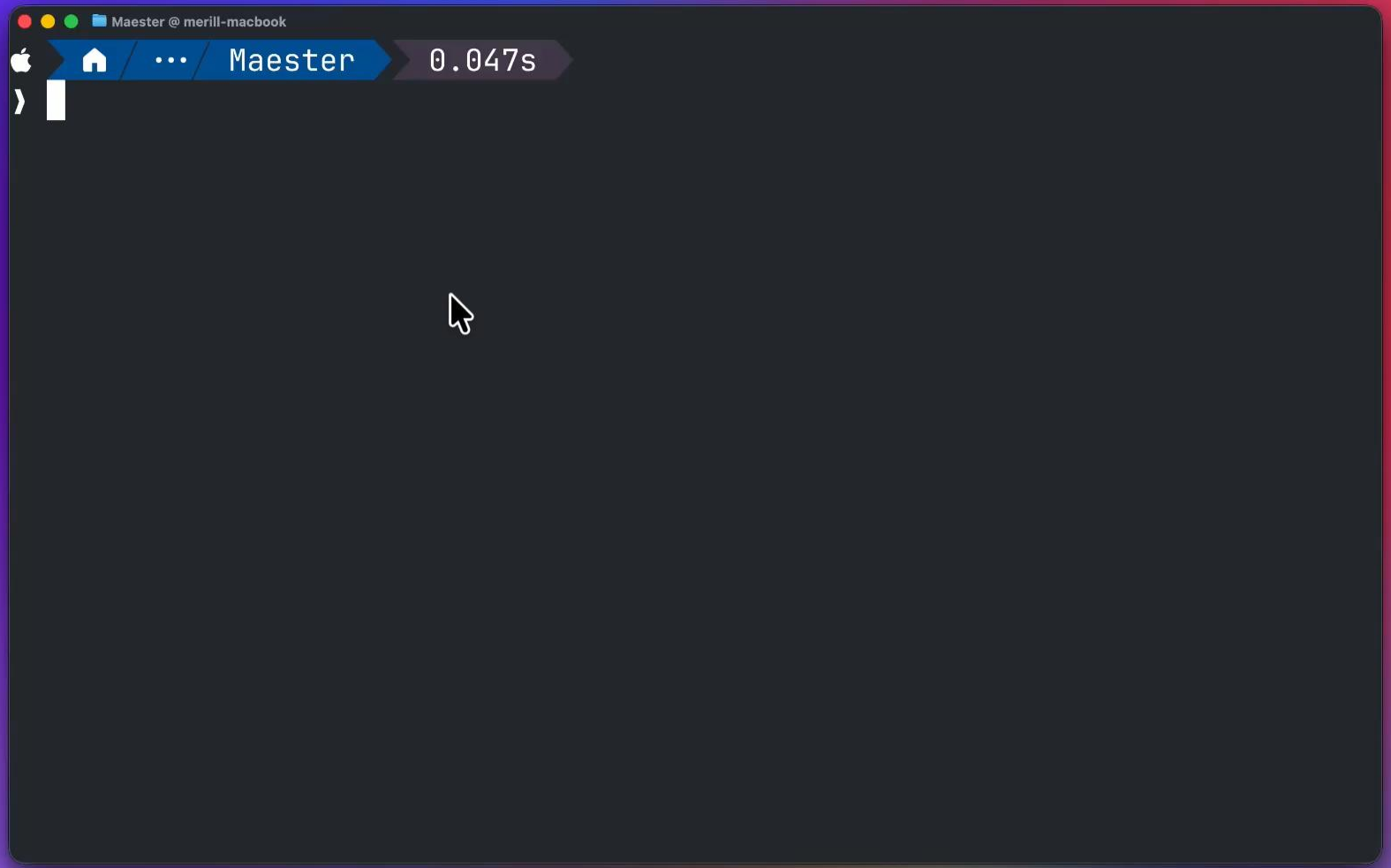


No custom classification
for Groups and
Non-Human Identities

DEMO

LAB 5: Maester and Identity Security Posture

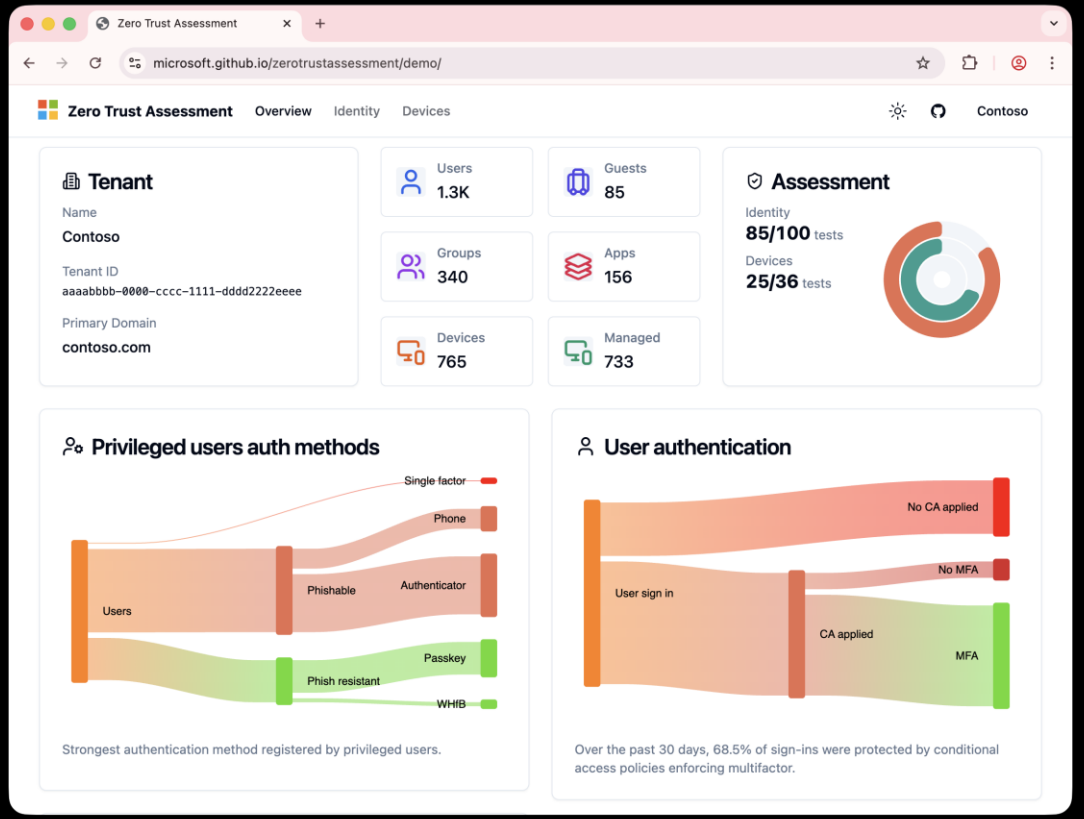
https://aka.ms/eldk26


Maester @ merill-macbook
Maester
0.047s

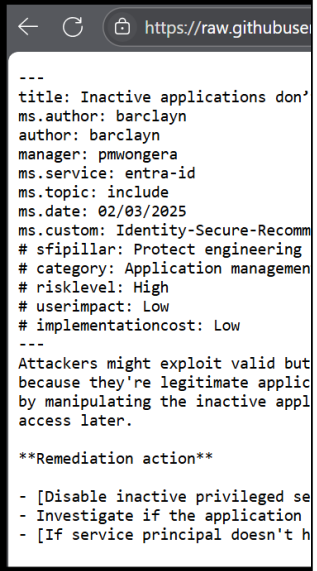
Zero Trust Assessment

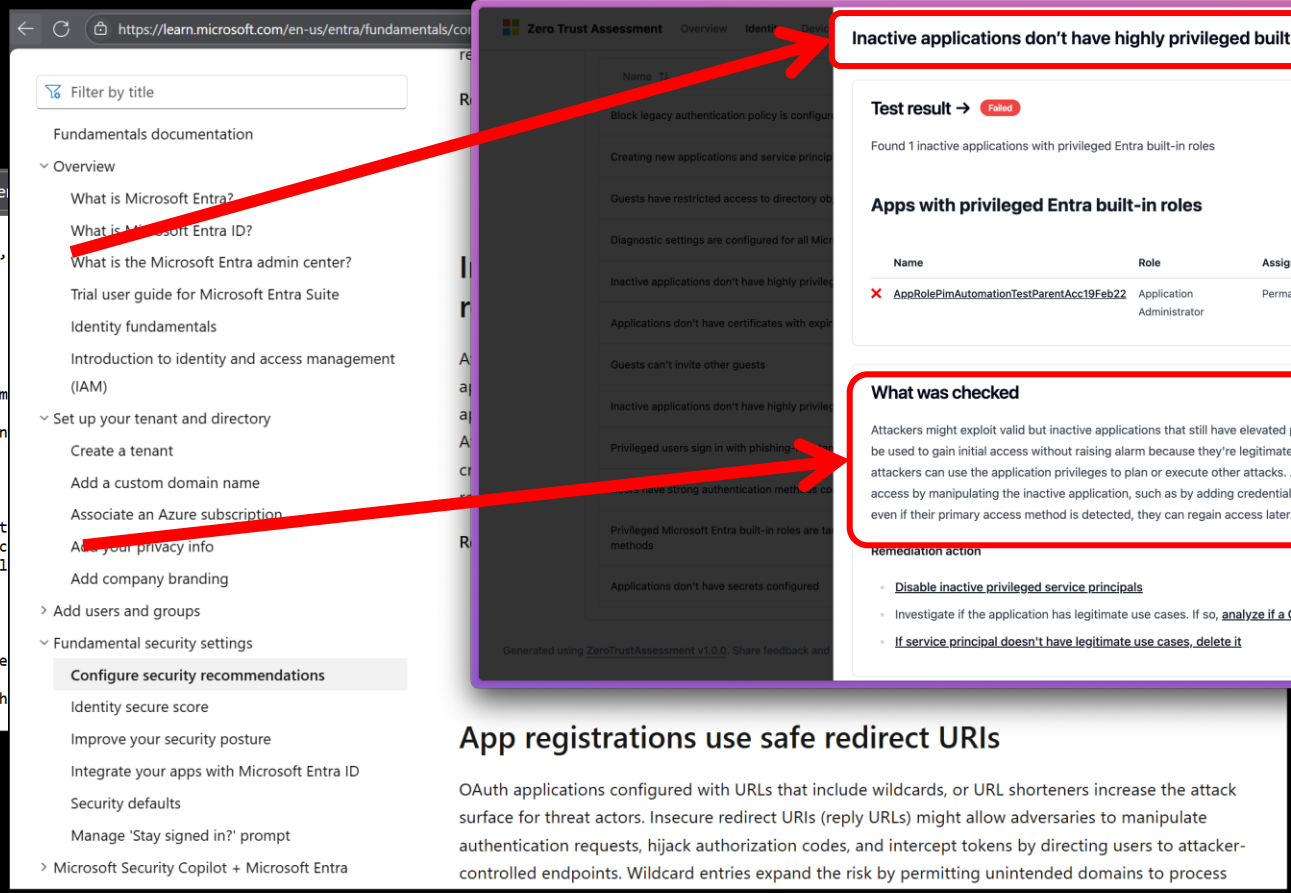
- PowerShell module that you install on your desktop
- Run an intensive scan against your tenant to generate a report with recommendations

```
Install-Module ZeroTrustAssessment
Connect-ZtAssessment
Invoke-ZtAssessment -Path C:\Report
```



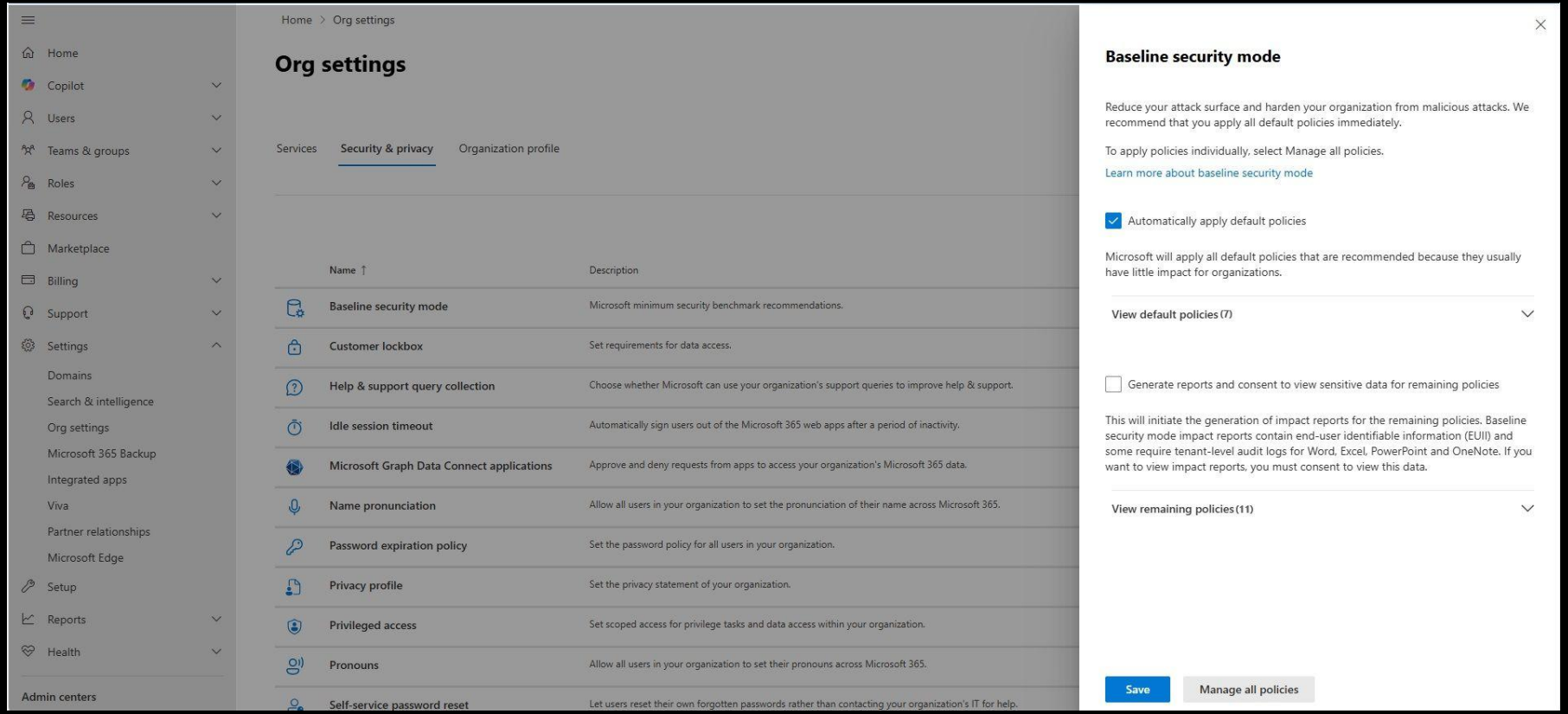
Zero Trust Assessment





Baseline Security Mode

Adoption of strong secure-by-default settings and eliminating vulnerabilities caused by legacy configurations



Home
Copilot
Agents
Users
Devices
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Show all

Enable Dark mode

Baseline security mode

Report settings

Manage these policies to reduce your attack surface and harden your Microsoft 365 organization from malicious attacks. Each policy is recommended to reach the minimum security benchmark.

Learn about baseline security mode and why it's important

Progress to meet standard 94%

Your progress ▼Standard benchmark You have applied 17 out of 18 recommendations

Recommended setting automation
Microsoft recommended setting adjustments as of Tue Nov 11 2025

Filters: Category: all Workload: all Status: all Reset all filters

Setting recommendation	Status	Service
Authentication (12)		
Require phishing-resistant authentication for admins	In review	Entra ID
Block legacy authentication	Meets standard	Entra ID
Block new password credentials in apps	Meets standard	Entra ID
Turn on restricted management user consent settings	Meets standard	Entra ID
Block access to Exchange Web Services	Meets standard	Exchange
Block basic authentication prompts	Meets standard	Microsoft 365 apps
Block files from opening with insecure protocols	Meets standard	Microsoft 365 apps
Block files from opening with FPRPC protocol	Meets standard	Microsoft 365 apps
Block legacy browser authentication connections to SharePoint	Meets standard	SharePoint
Block IDCRL protocol connections to SharePoint	Meets standard	SharePoint

Unified Tenant Configuration Management

Unified Tenant Configuration Management

Configuration-as-Code platform for all Microsoft Clouds

Supports configurations for 7 of the major M365 Workloads

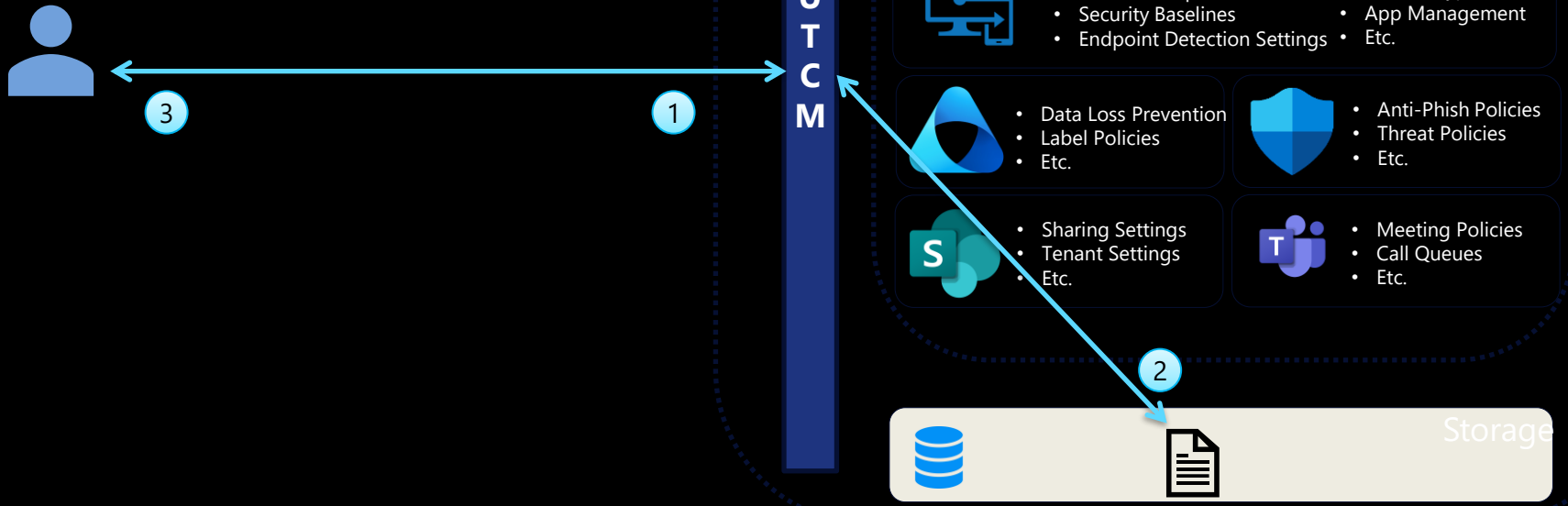
Works for organizations with 1 or 1,000+ tenants



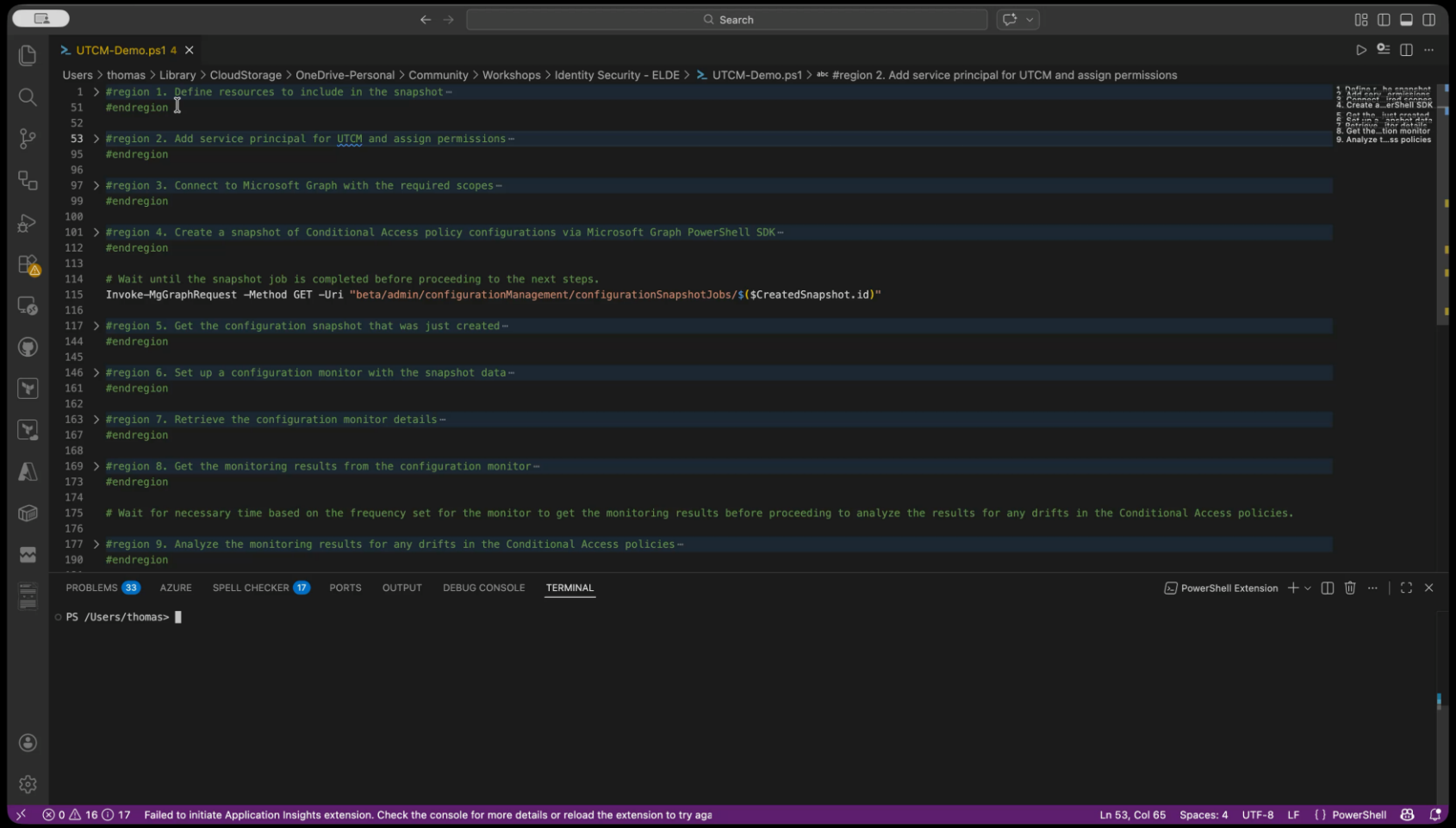




1. Requests a Snapshot for components (eg. EXO Transport Rules, Purview Label Policies and Teams Call Queues)
2. XTA stores the extracted configuration in the tenant's internal storage.
3. User retrieves the extracted configuration baseline and stores it back in his environment (e.g., Azure DevOps source control)

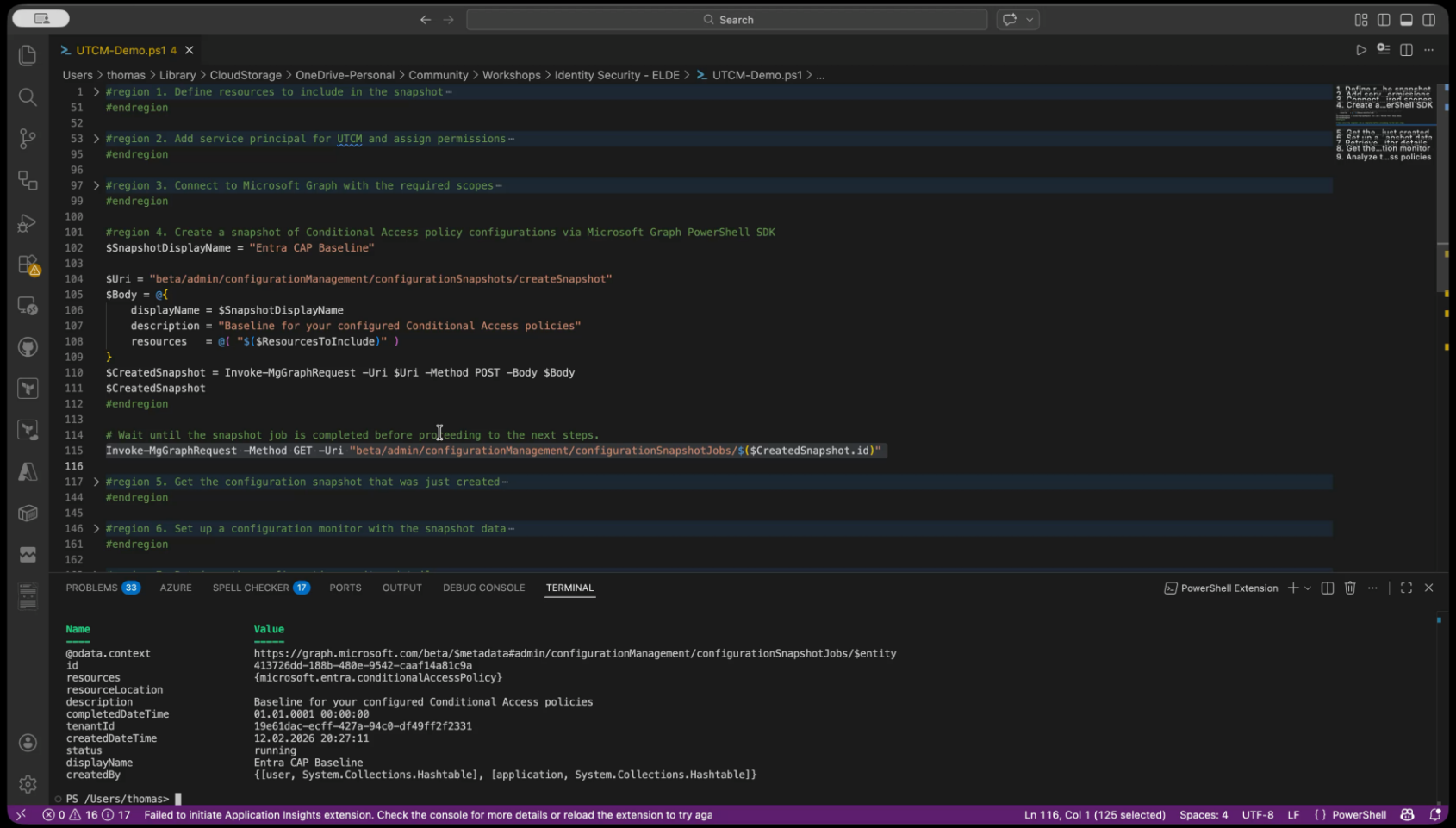


Step 1: Configure Service Principal and create Snapshot Job



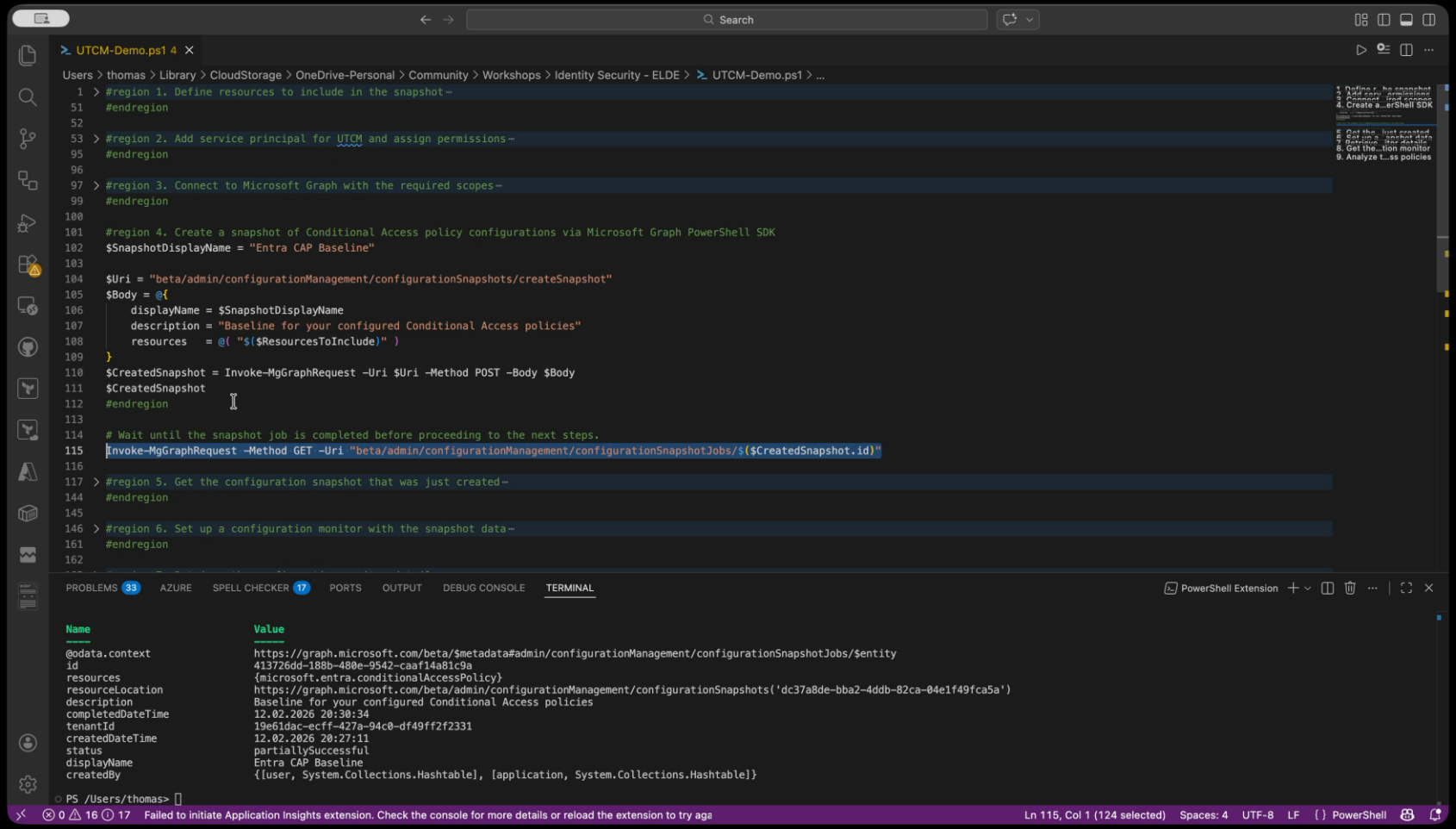

A FEW
MOMENTS LATER

Waiting for completion of Snapshot job



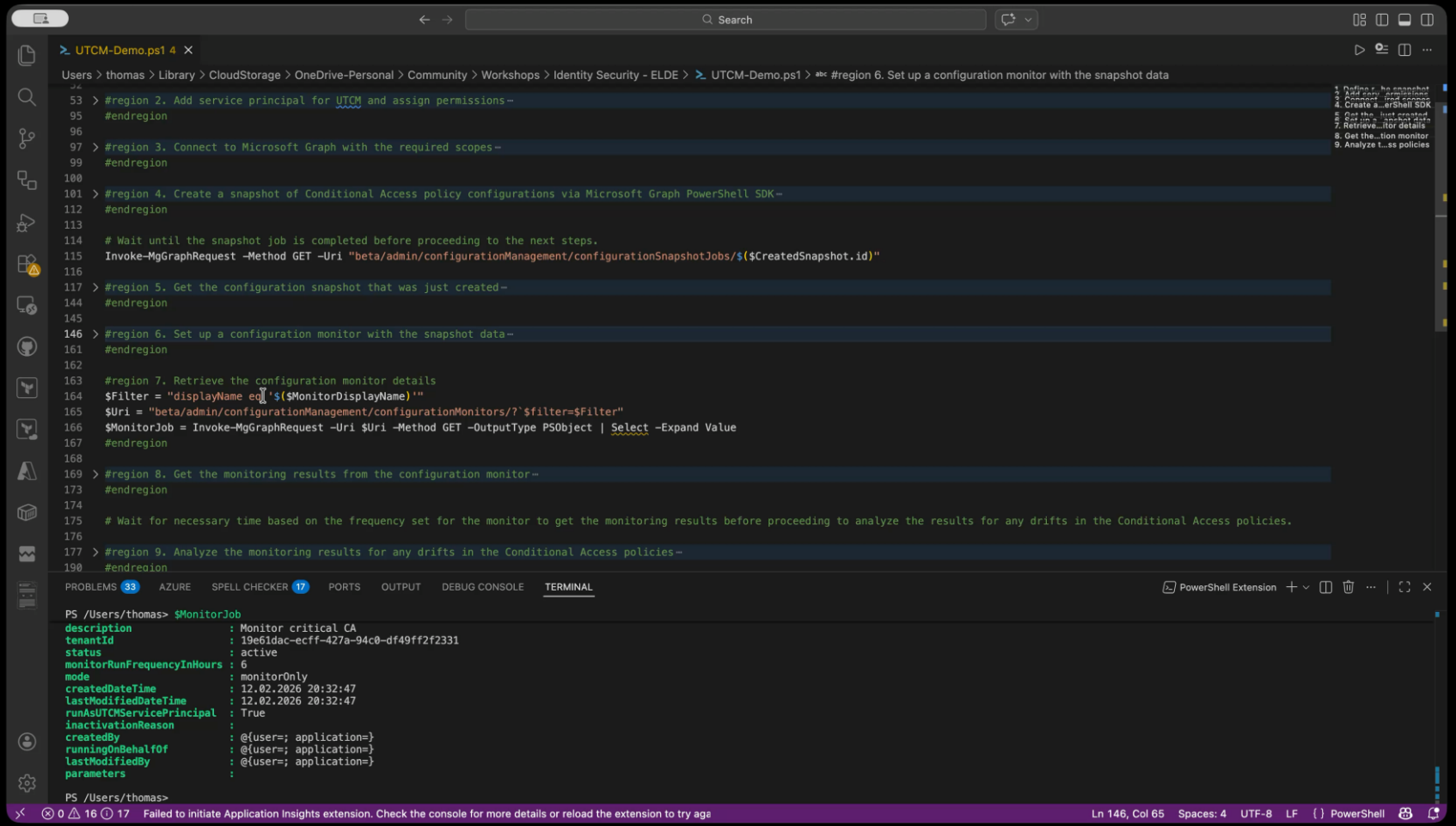

A FEW
MOMENTS LATER

Configure Monitoring of selected resources from Snapshot

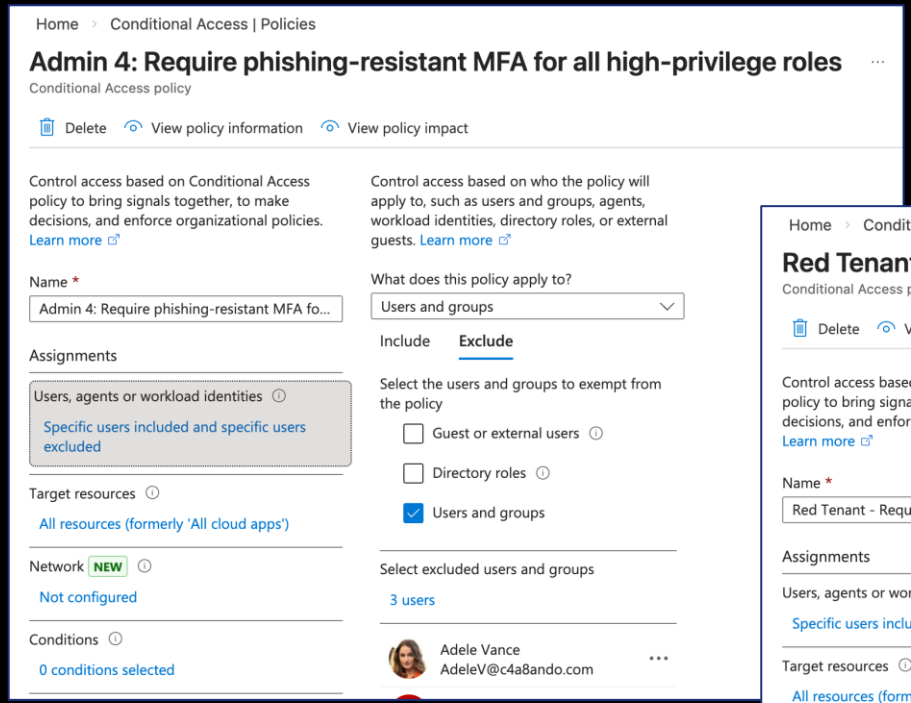


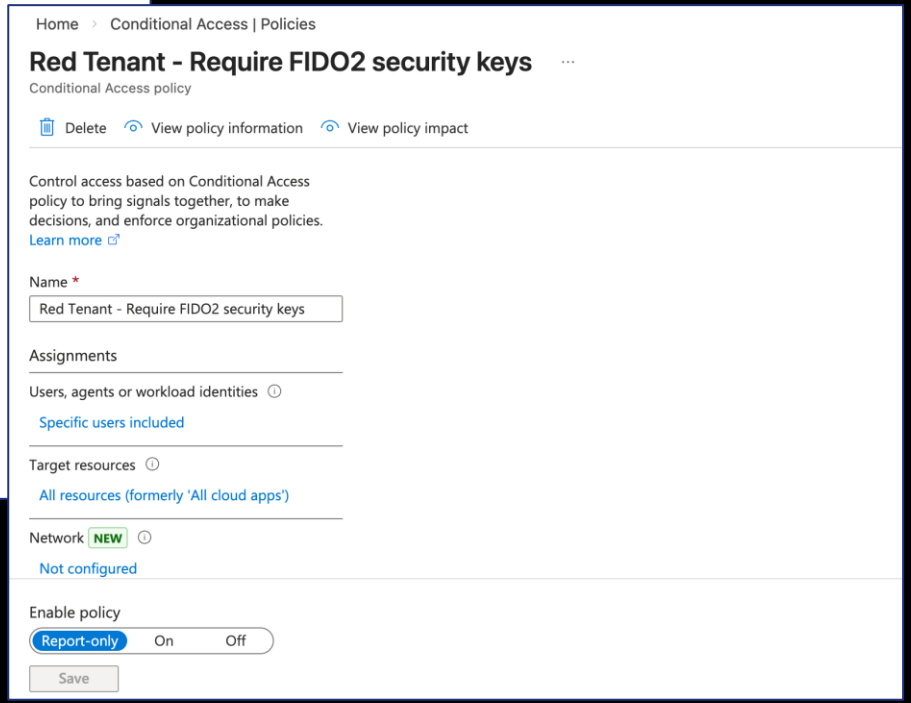

THREE
HOURS LATER

Initial run of configuration monitor



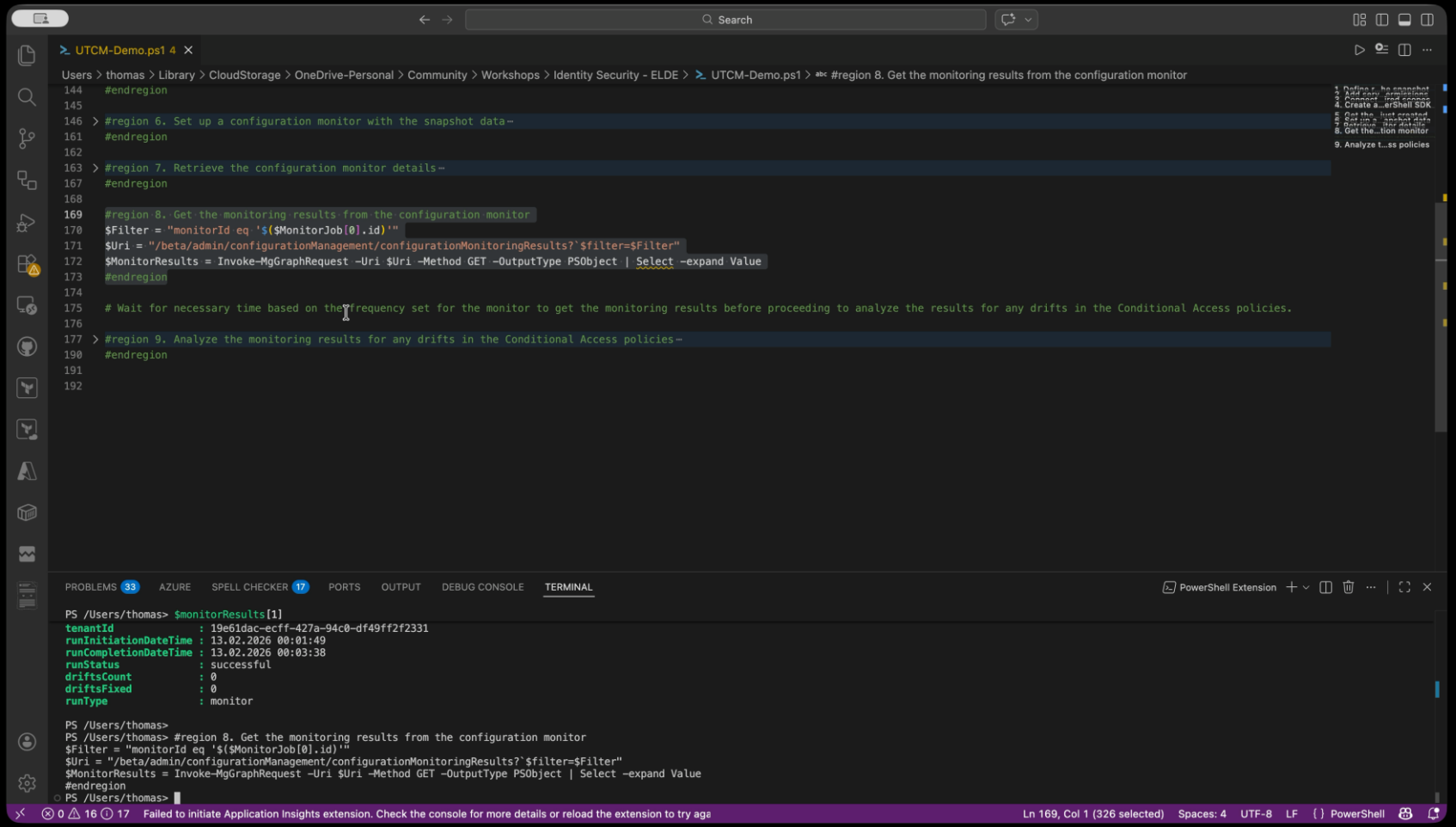
Changed configurations of Conditional Access Policies






SIX HOURS LATER

Identify configuration drift on Conditional Access Policies



Summary & QA

Session Feedback – THANK YOU ☺

Please evaluate this session using QR Code **during next 30 min**

- or -

Make your session feedback on your way out of the room

https://smiley.link/DJWTGBTN