



Demystify Microsoft Entra Workload Identities

Thomas Naunheim



resco



PROMISE
GRUPA APN PROMISE

502nm

ANW



EUROPEAN CLOUD SUMMIT

cloudtechtallinn.com

GOLD



NORDIC KOOLITUS



FORCEWORKS  GLOBAL



QUBIX

O I X I O Digital



CRM

netspore

DYNAMICS MINDS



BRONZE

CTTT



Thomas Naunheim

Cyber Security Architect @glueckkanja AG

Focus on Identity + Security in Microsoft Azure and Microsoft Entra
Community Speaker, Blogger and Podcast (Cloud Inspires)
Co-Organizer Azure Meetup Bonn and Cloud Identity Summit
Live in Lahnstein/Koblenz, Germany



thomas@naunheim.net



cloud-architekt.net



[@Thomas_Live](https://twitter.com/Thomas_Live)



[/in/ThomasNaunheim](https://in/ThomasNaunheim)

Agenda

- Different Types of Workload Identities
- Lifecycle Management and Operations
- Securing Access and Advanced Monitoring

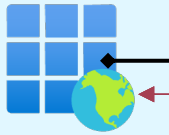


Different Types of Workload Identities

Application Identities (Client Secrets)

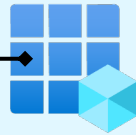
Workload Identity

Application Instance

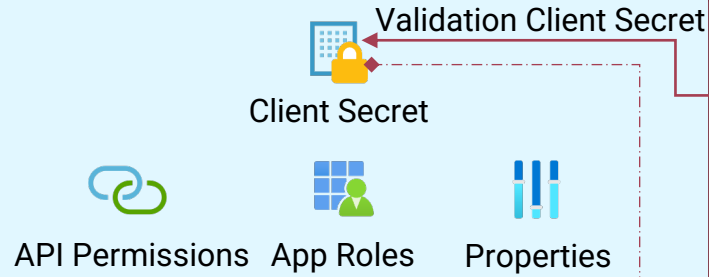


Service Principal
(Enterprise App)

Application Definition



Application
(App Registration)



Membership



Entra ID Roles



Group Membership

API Access

Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



Microsoft Graph

Defines Required
Delegated/App Permissions

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

**/token
Endpoint**

Request
with
Shared
secret

Token with
API Scope
& Groups

Workload Env.

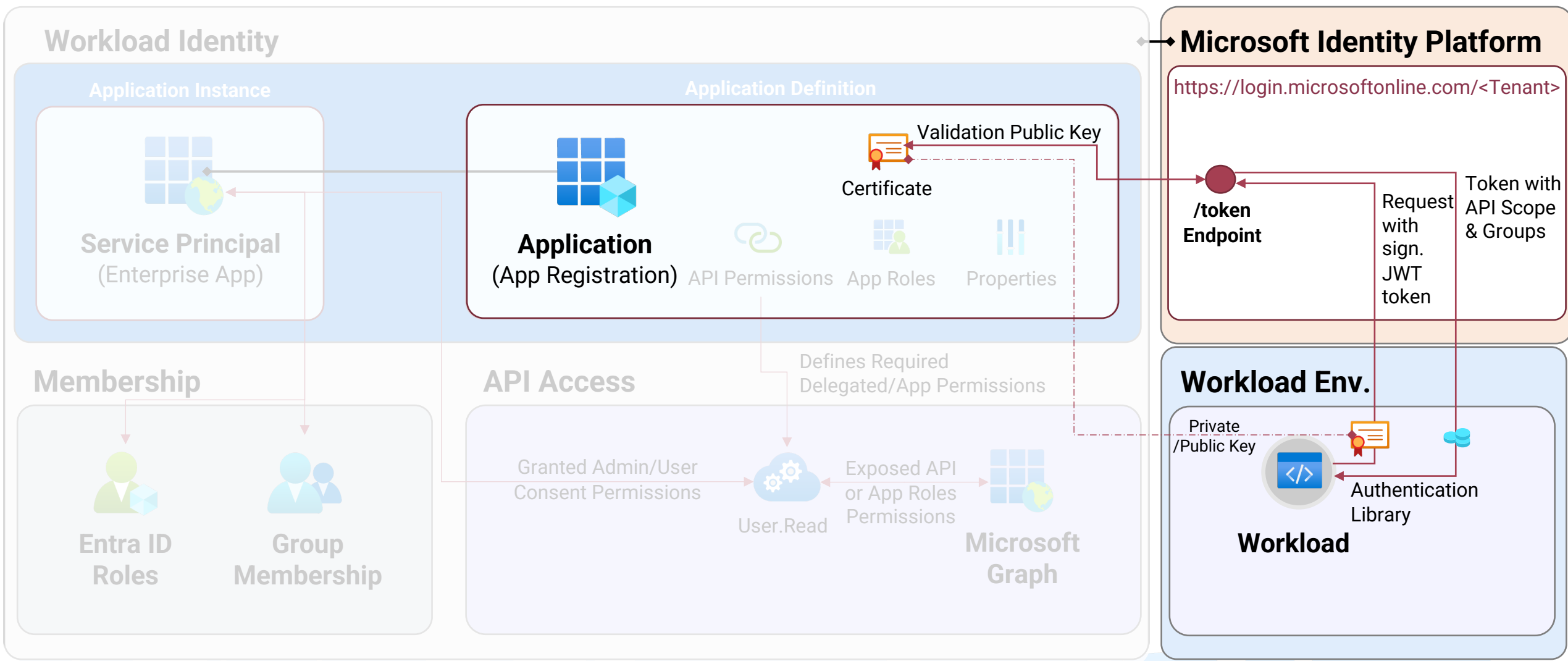
Shared
Secret



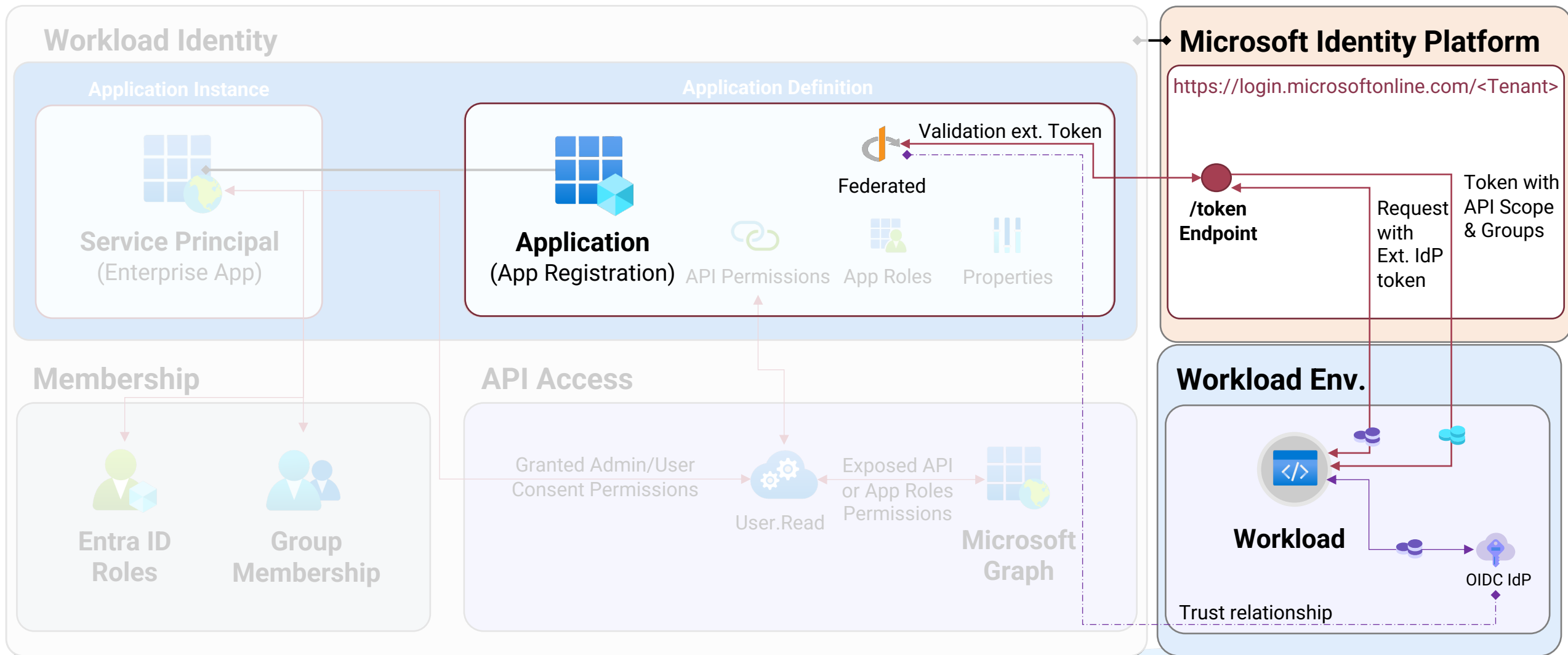
Workload

Authentication
Library

Application Identities (Certificates)



Application Identities (Federated Credentials)



DEMO

Abuse and replay of token from
Federated Workload
(GitHub Actions)

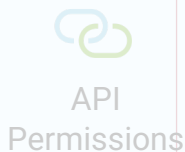
System-Assigned Managed Identity

Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Azure Identity Management

**Managed Identity Resource Provider
(MSRP)**



Certificate

issues certificates
and rolling secrets

Microsoft Identity Platform

<https://login.microsoftonline.com/Tenant>

Token with API Scope & Groups

**/token
Endpoint**

Request with signed JWT token

Membership



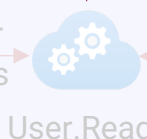
**Entra ID
Roles**



**Group
Membership**

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



**Microsoft
Graph**

Azure Managed Resource

**Managed
Identity
(System)**

Assigned
1:1

Workload

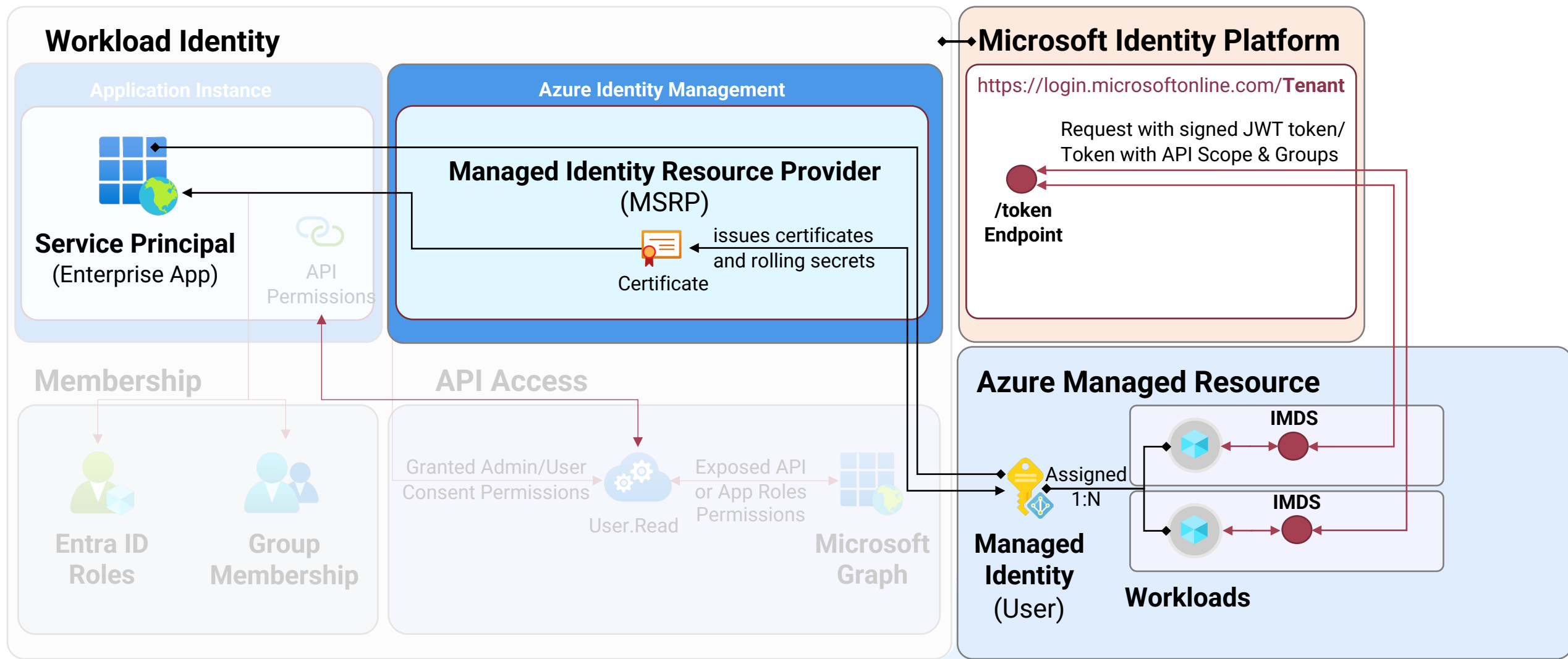
**Azure Instance
Metadata Service (IMDS)**

[http://169.254.169.254/
metadata/identity](http://169.254.169.254/metadata/identity)

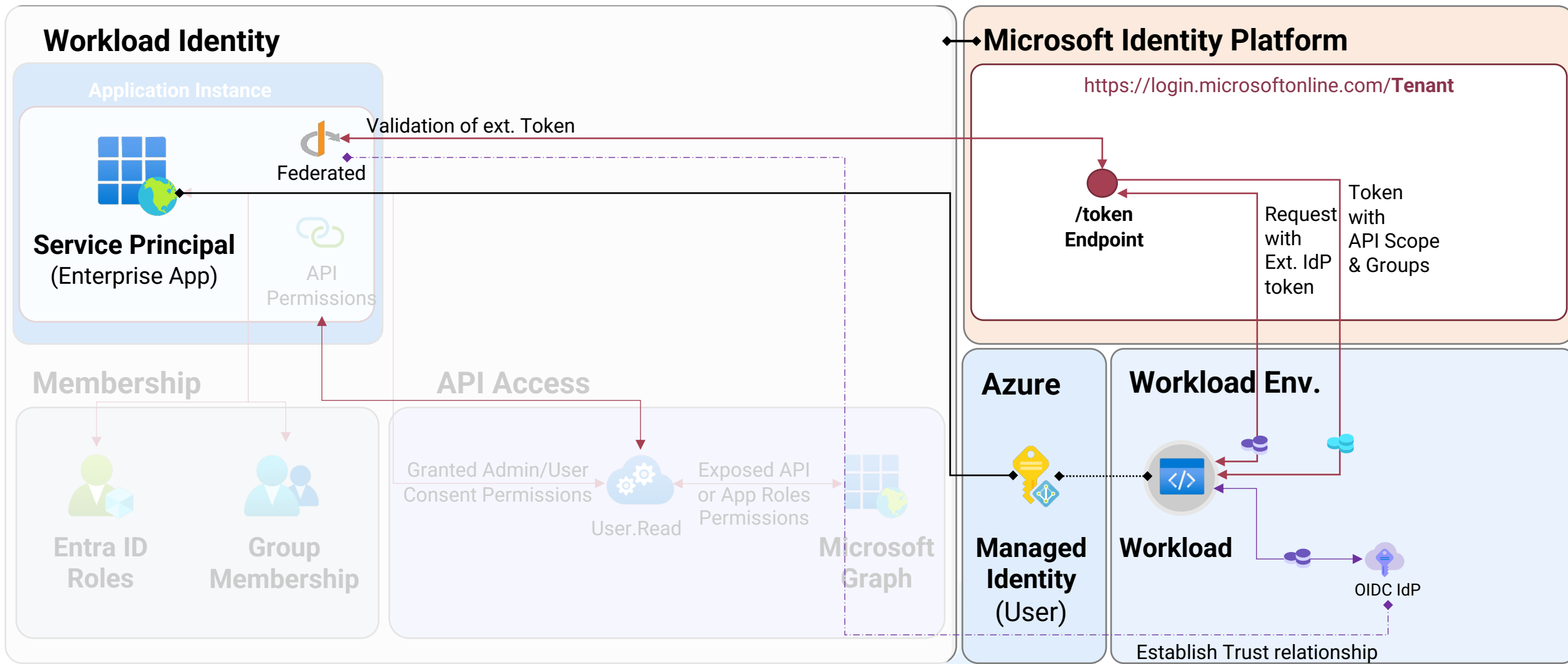
Local
Request

**/token
Endpoint**

User-Assigned Managed Identity



User-Assigned Managed Identity (Federated)






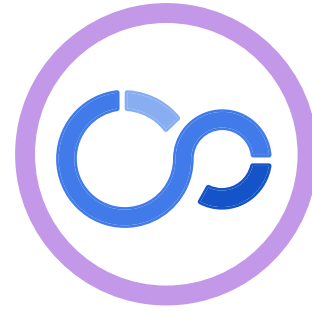
DEMO

Security considerations of Azure Managed Identities

Different Types of Workload Identities

Comparison

	 Service Principal (Key- or Certificate)	 Service Principal (Federated Credentials)	 Managed Identity (System/User Assign.)
Supported Use Case	No limitation	Limited to supported Workloads (outside of Azure)	Limited to Azure-managed Resources
Security Boundary	Single- or multi-tenant	Single- or multi-tenant	Single-tenant*
Relation to Workload	Unassigned	Assigned to Issuer/Entity	Assigned to Resource(s) System (1:1), User (N:1)
Workload Environment	Everywhere	Supported OIDC Federated IdP	Azure- and Azure Arc-enabled resources
Token Lifetime / Cache	1h (Default), 24h (CAE)	less than or equal to 1h	24h (<u>Cache per resource URI</u>)
Credentials	Automation to rotate and issue secret or certificates	Managed by Trusted Issuer	Managed by Microsoft



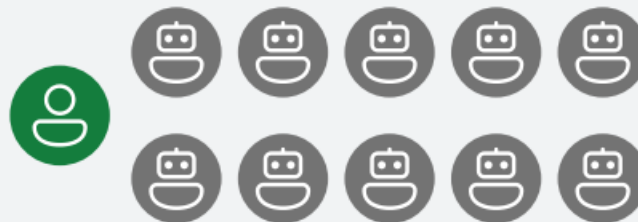
Lifecycle Management and Delegation

Lifecycle Management and Delegation

State of Workload Identity Management

1:10

User identities to
workload identities



>80%

Of workload identities are
inactive, double the percentage
reported in 2021.

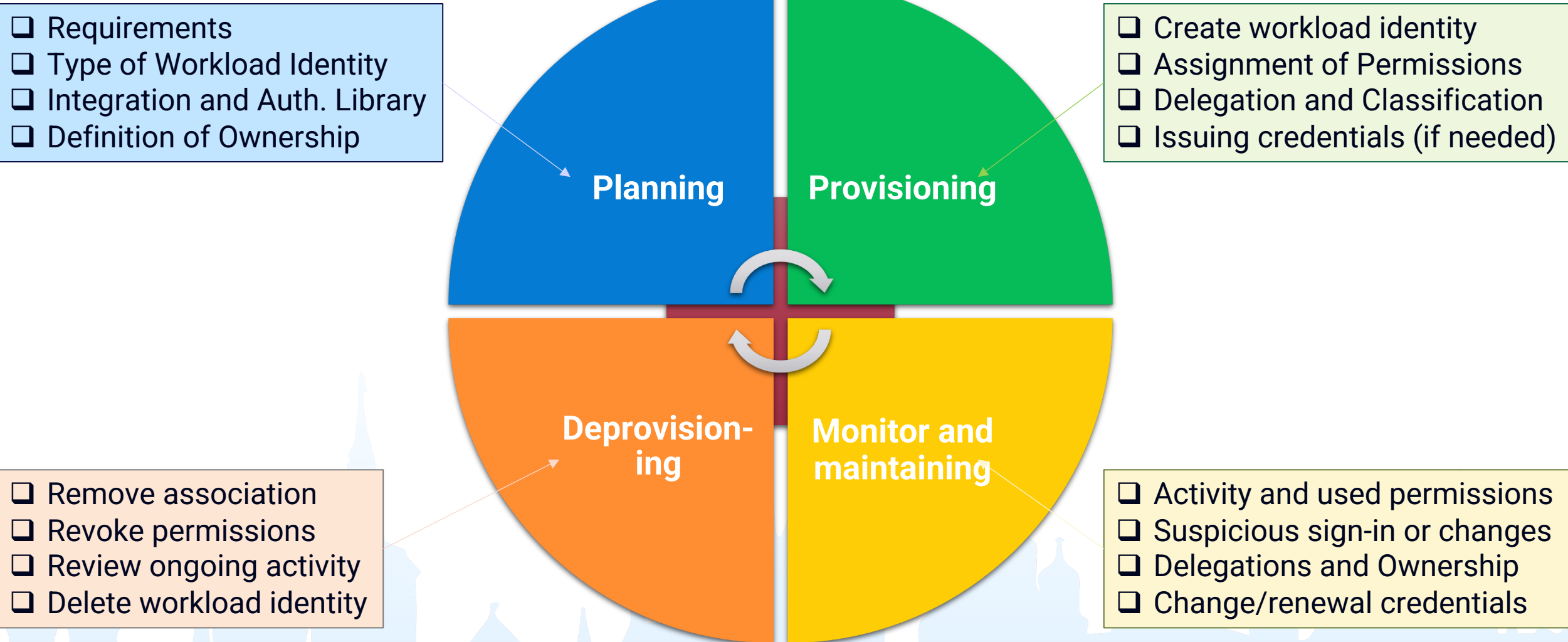


<5%

of permissions are
actually used

Source: [2023 State of Cloud Permission Risks Report \(microsoft.com\)](https://microsoft.com)

Lifecycle Management and Delegation



DEMO

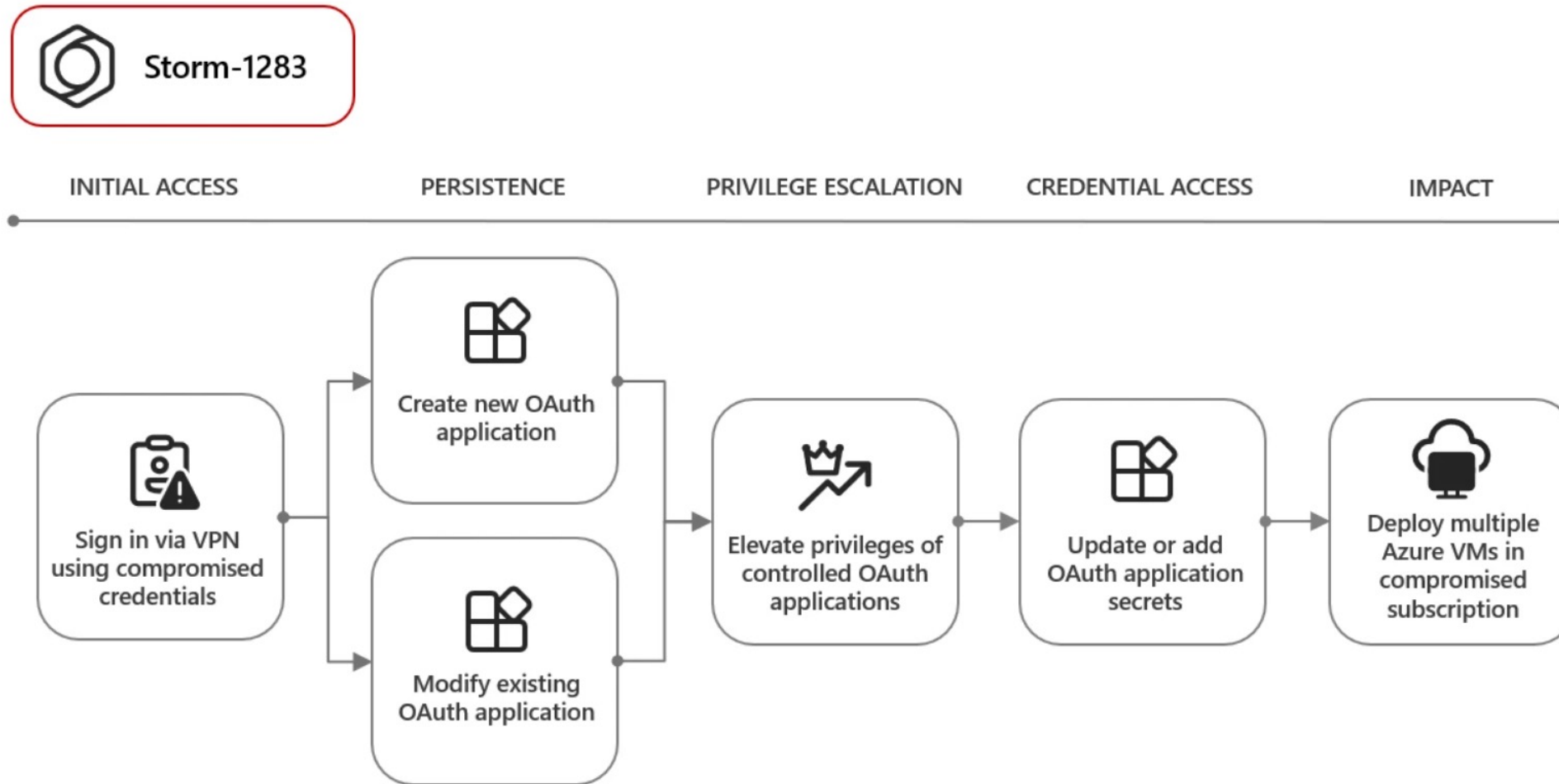
Default Permissions and Delegations, Maintenance and Classification



Securing Access and Advanced Monitoring

Attackers 💖 Service Principals

OAuth applications to deploy VMs for cryptomining



Source: [Threat actors misuse OAuth applications to automate financially driven attacks](#)

Attackers 💖 Service Principals

Nation-state attack on Microsoft by Threat actor “Midnight Blizzard”

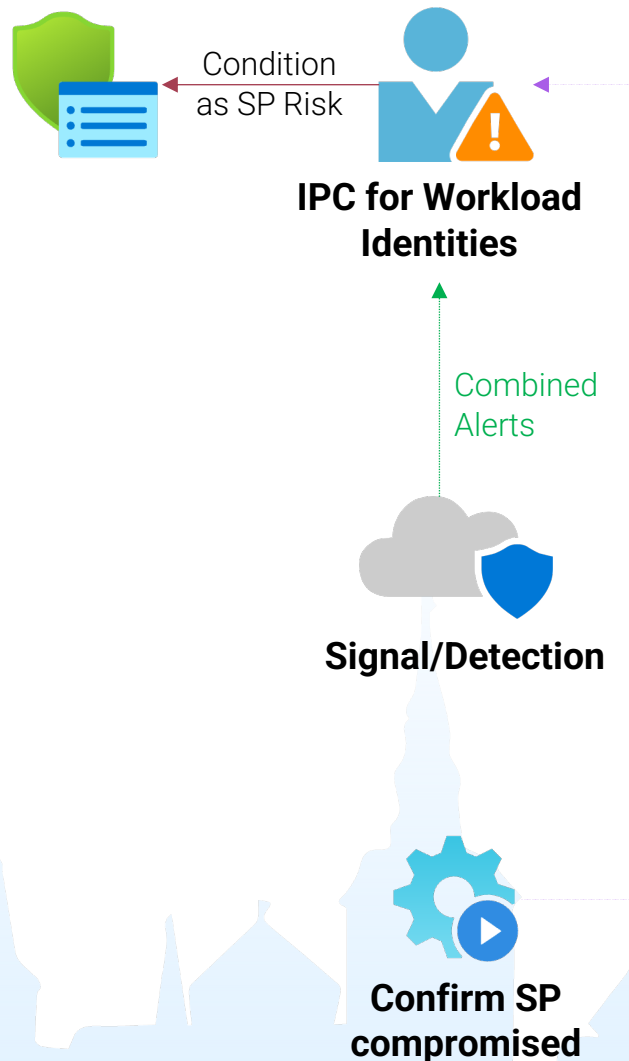
Malicious use of OAuth applications

Threat actors like Midnight Blizzard compromise user accounts to create, modify, and grant high permissions to OAuth applications that they can misuse to hide malicious activity. The misuse of OAuth also enables threat actors to maintain access to applications, even if they lose access to the initially compromised account. Midnight Blizzard leveraged their initial access to identify and compromise a **legacy test OAuth application that had elevated access to the Microsoft corporate environment.** The actor created additional malicious OAuth applications. They created a new user account to grant consent in the Microsoft corporate environment to the actor controlled malicious OAuth applications. The threat actor then used the legacy test OAuth application to grant them the Office 365 Exchange Online ***full_access_as_app* role, which allows access to mailboxes.**

Source: [Midnight Blizzard: Guidance for responders on nation-state attack | Microsoft Security Blog](#)

Securing Access and Advanced Monitoring

Threat Intelligence and Conditional Access-Integration



Microsoft Entra ID Protection

- Suspicious Sign-ins
- Leaked Credentials (from GitHub)
- Anomalous service principal activity
- ...

Microsoft Defender for Cloud Apps (MDA)

- Malicious application, Suspicious application
- Unusual addition of credentials to an OAuth app, Unusual ISP for an OAuth app
- ... Azure AD app registration by risky user

Microsoft Sentinel Analytics Rules (Custom Detections)

- Credential added to sensitive Workload Identity by lower-privileged user
- Federated Credential has been created for GitHub entity outside of organization
- ...

DEMO

CA and ID Protection, Sentinel Analytics Rules & Enrichment of Threat Intelligence



Blog Post series about
Microsoft Entra Workload Identities
[Cloud-Architekt.net](https://cloud-architekt.net)



Please rate this session!

Your feedback will help with

- speaker evaluation
- content relevance
- decision making for future events
- quality improvement

#7

Thank you!

Q&A

