

An abstract graphic on the left side of the slide. It features a blue silhouette of a person climbing a rope. The rope is represented by several thick, curved lines in shades of blue and green. The person is positioned on the left, with their arms and legs extended as if climbing. The background is white.

Absicherung und Management von Microsoft Entra Workload Identities

Thomas Naunheim

Microsoft MVP, Cloud Security Architect
@glueckkanja-gab AG



Thomas Naunheim

Cyber Security Architect
@glueckkanja-gab AG

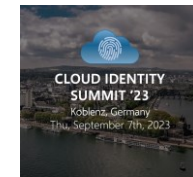
Koblenz, Germany



@Thomas_Live



cloud-architekt.net





WAS SIND WORKLOAD IDENTITIES?



VARIANTEN VON
WORKLOAD IDENTITIES



LIFECYCLE MANAGEMENT
UND DELEGIERUNG

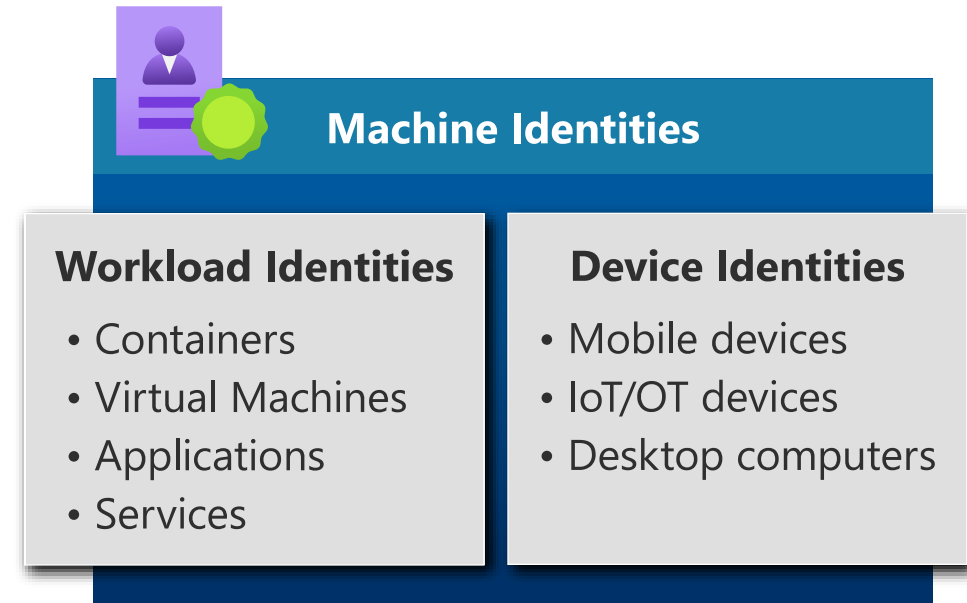


ZUGRIFFSSCHUTZ UND
SECURITY MONITORING

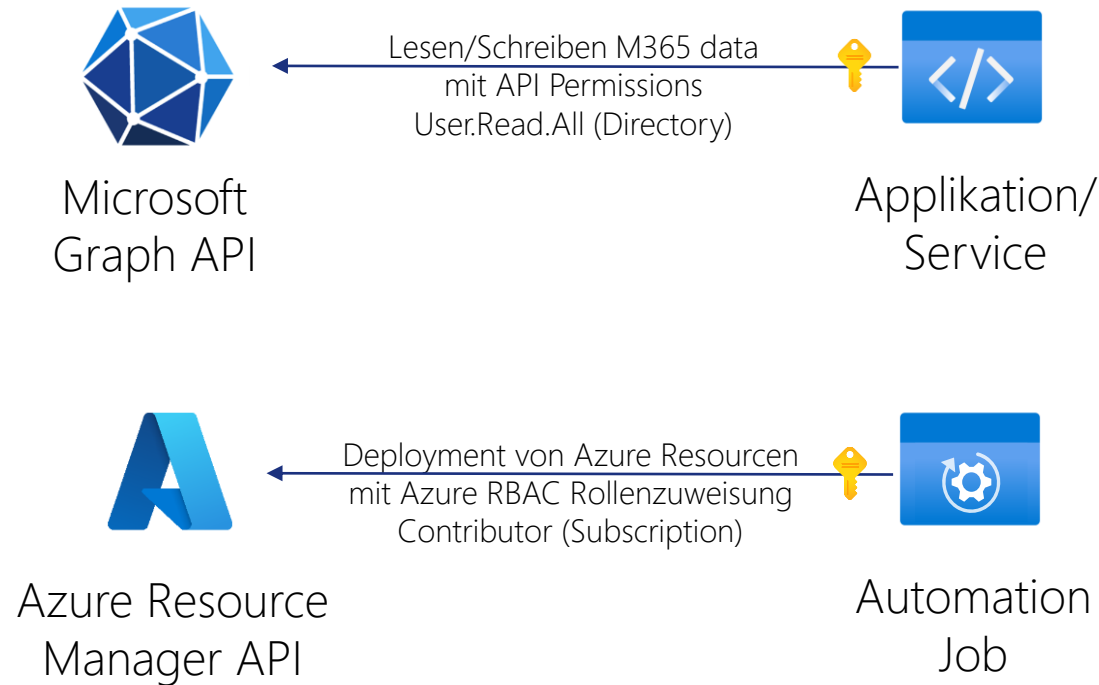


WAS SIND WORKLOAD IDENTITIES?

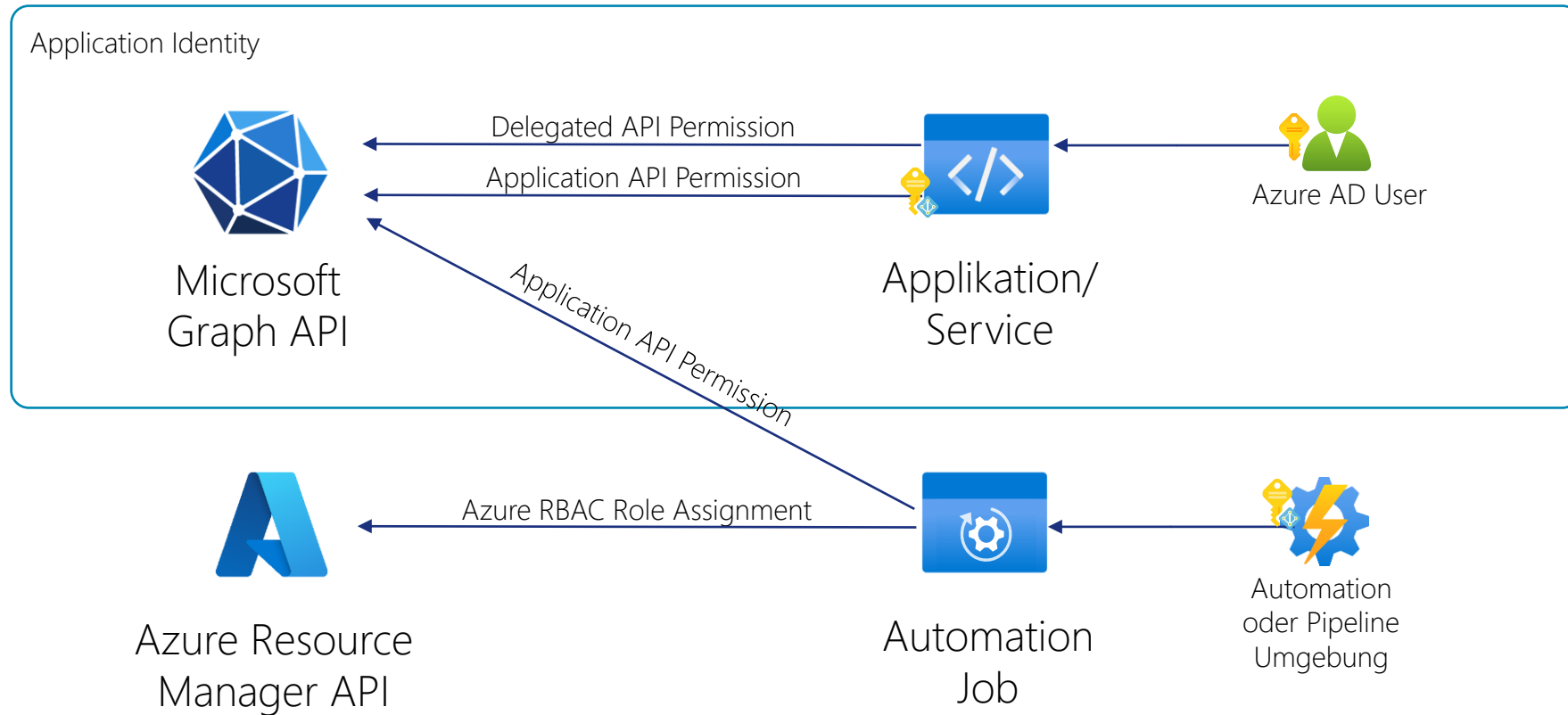
Was sind Workload Identities?

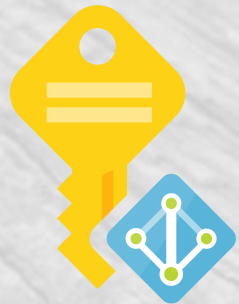


Anwendungsfälle von Workload Identities



Anwendungsfälle von Workload Identities





VARIANTEN VON WORKLOAD IDENTITIES

Application Identities (Client Secrets)

Workload Identity

Application Instance

Service Principal
(Enterprise App)

Application Definition

Application
(App Registration)

Validierung Secret
Client Secret
API Permissions
App Roles
Properties

Membership

Azure AD
Roles

Group
Membership

API Access

Admin/User
Consent Permissions

User.Read

Zuweisung von
Delegated/App Permissions

Exposed API
oder App Roles
Permissions

Microsoft
Graph

Microsoft Identity Platform

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

/token
Endpoint

Anfrage mit
Shared
secret
Token mit
API Scope
& Groups

Workload Env.

Shared
Secret

Workload

Authentication
Library

Application Identities (Certificates)

Workload Identity

Application Instance

Service Principal
(Enterprise App)

Application Definition

Application
(App Registration)

API Permissions

Certificate

App Roles

Properties

Validierung Public Key

Microsoft Identity Platform

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

/token
Endpoint

Anfrage mit
sign.
JWT
token

Token mit
API Scope
& Groups

Membership

Azure AD
Roles

Group
Membership

API Access

Granted Admin/User
Consent Permissions

User.Read

Exposed API
or App Roles
Permissions

Microsoft
Graph

Zuweisung von
Delegated/App Permissions

Workload Env.

Private
/Public Key

Workload

Authentication
Library

Application Identities (Federated Credentials)

Workload Identity

Application Instance

Service Principal
(Enterprise App)

Application Definition

Application
(App Registration)

API Permissions

Federated
App Roles

Properties

Validierung ext. Token

Microsoft Identity Platform

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

/token
Endpoint

Anfrage
mit
Ext. IdP
token

Token mit
API Scope
& Groups

Membership

Azure AD
Roles

Group
Membership

API Access

Granted Admin/User
Consent Permissions

User.Read

Exposed API
or App Roles
Permissions

Microsoft
Graph

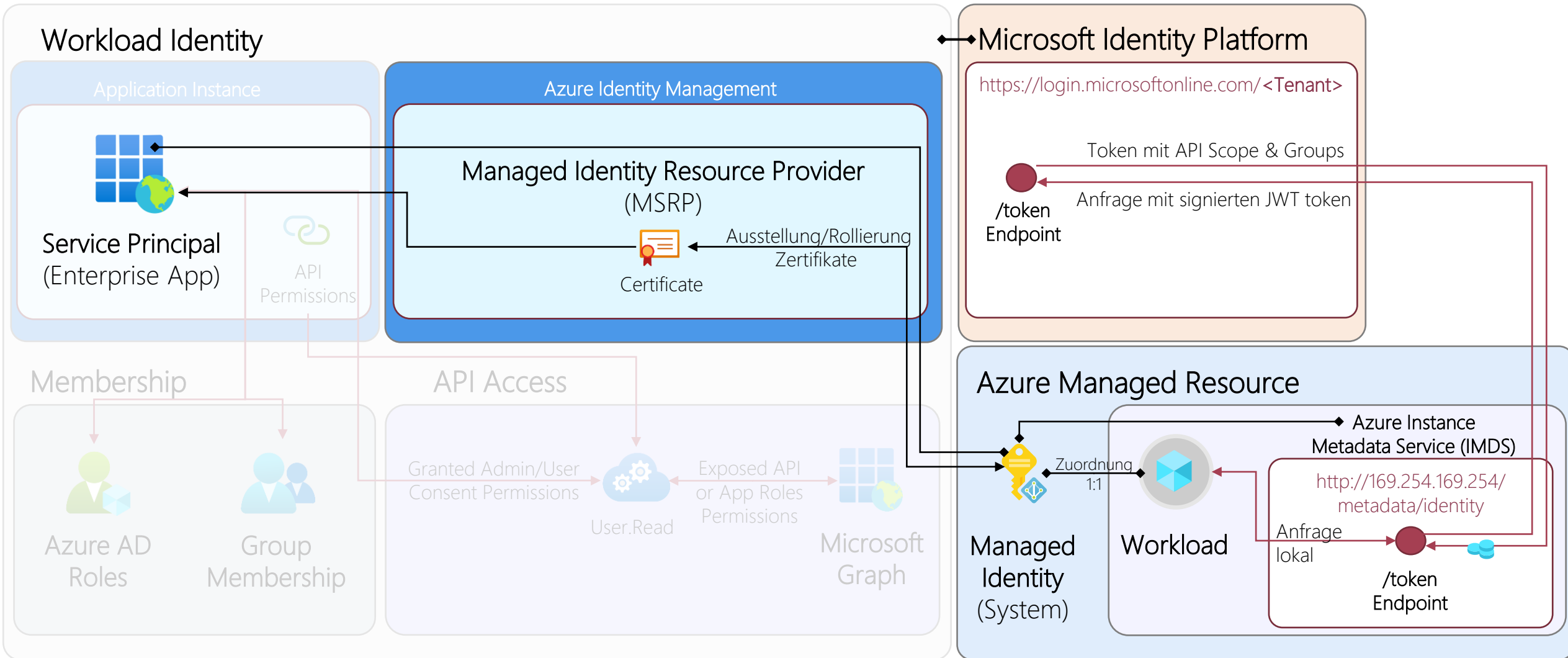
Workload Env.

Workload

OIDC IdP

Trust relationship

System-Assigned Managed Identity



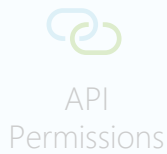
User-Assigned Managed Identity

Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Managed Identity Resource Provider
(MSRP)



Certificate

Ausstellung/Rollierung
Zertifikate

Membership



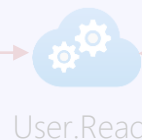
Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



Microsoft
Graph

Microsoft Identity Platform

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

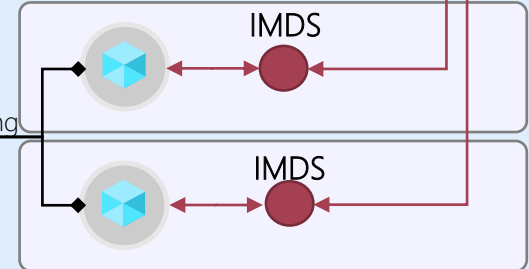
Anfrage mit signierten JWT token/
Token mit API Scope & Groups

/token
Endpoint

Azure Managed Resource

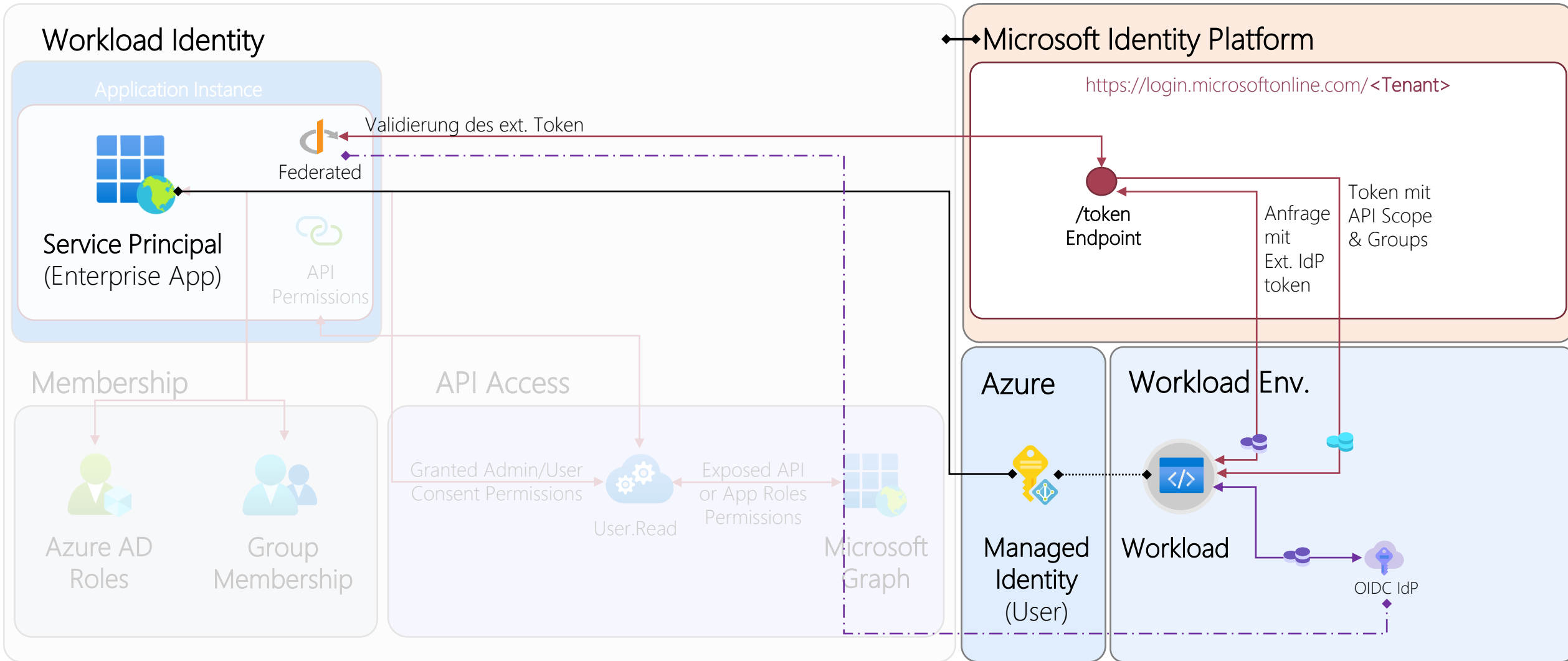
Managed
Identity
(User)

Zuordnung
1:N



Workloads

User-Assigned Managed Identity (Federated)








DEMO

“Secretless Workload Authentifizierung” mit Federated Credentials und Managed Identities sowie deren Sicherheitsrisiken

Verlgeich der Workload Identity types

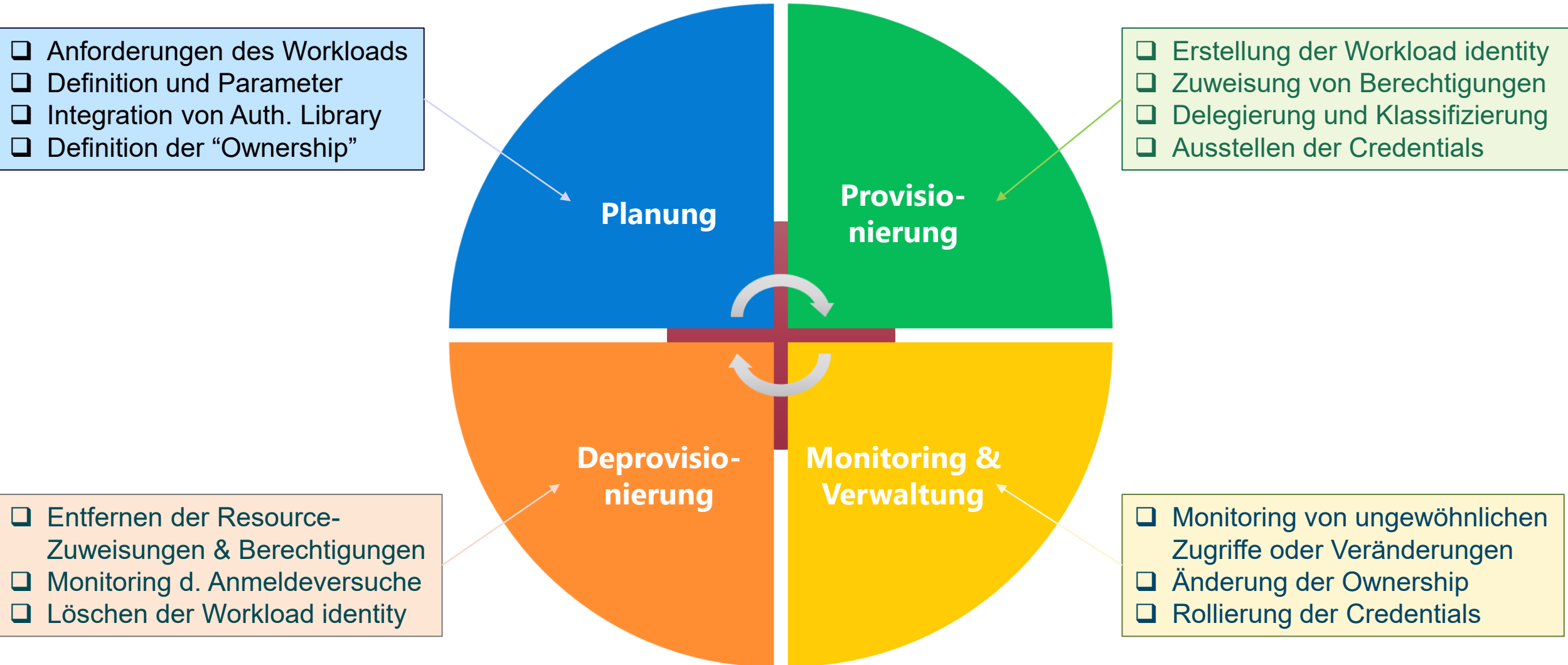
	 Service Principal (Key/Certificate)	 Service Principal (Federated Credentials)	 Managed Identity (System/User Assign.)
Supported Use Case	Keine Einschränkung	Eingeschränkt, unterstützte Workloads und Identity Provider	Eingeschränkt, unterstützte Workloads (Azure-managed Resources)
Security Boundary	Single- oder multi-tenant	Single- oder multi-tenant	Single-tenant*
Relation to Workload	Keine direkte Beziehung	Beziehung zu Issuer/Entity	Beziehung zu Ressourcen System (1:1), User (N:1)
Workload Environment	Unabhängig	Supported OIDC Federated IdP	Azure- und Azure Arc-enabled Resources
Token Lifetime / Cache	1h (Default), 24h (CAE)	1h (Default)	24h (<u>Caching per Resource URI</u>)

* access to Azure Resources from onboarded subscriptions via Azure Lighthouse



LIFECYCLE MANAGEMENT UND DELEGIERUNGEN

Lifecycle Management of Workload Identities



App Management Policies

GET beta https://graph.microsoft.com/beta/policies/appManagementPolicies Run query

Request body Request headers Modify permissions Access token

OK - 200 - 139ms

Response preview Response headers Code snippets Toolkit

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#policies/appManagementPolicies",
  "value": [
    {
      "id": "943754b8-3000-4fb6-b715-1205becf1d00",
      "deletedDateTime": null,
      "displayName": "Certificates only policy",
      "description": "Disable client secrets and enforce certificate-based authentication",
      "isEnabled": true,
      "restrictions": {
        "passwordCredentials": [
          {
            "restrictionType": "passwordAddition",
            "maxLifetime": null,
            "restrictForAppsCreatedAfterDateTime": "2019-01-01T00:00:00.0000000"
          }
        ],
        "keyCredentials": [
          {
            "restrictionType": "asymmetricKeyLifetime",
            "maxLifetime": "P90D",
            "restrictForAppsCreatedAfterDateTime": "2014-01-01T00:00:00.0000000",
            "certificateBasedApplicationConfigurationIds": []
          }
        ]
      }
    }
  ]
}
```

Home > C4A8 Ando | App registrations > aadops-privilegedaccess-sp

aadops-privilegedaccess-sp | Certificates & secrets

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.



Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

Client secrets are blocked by a tenant-wide policy. Contact your tenant administrator for more information.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
identityops-kva	5/29/2023 ⚠	Cm6*****	b8934654-76c2-41fa-81b0-539025a8e...  



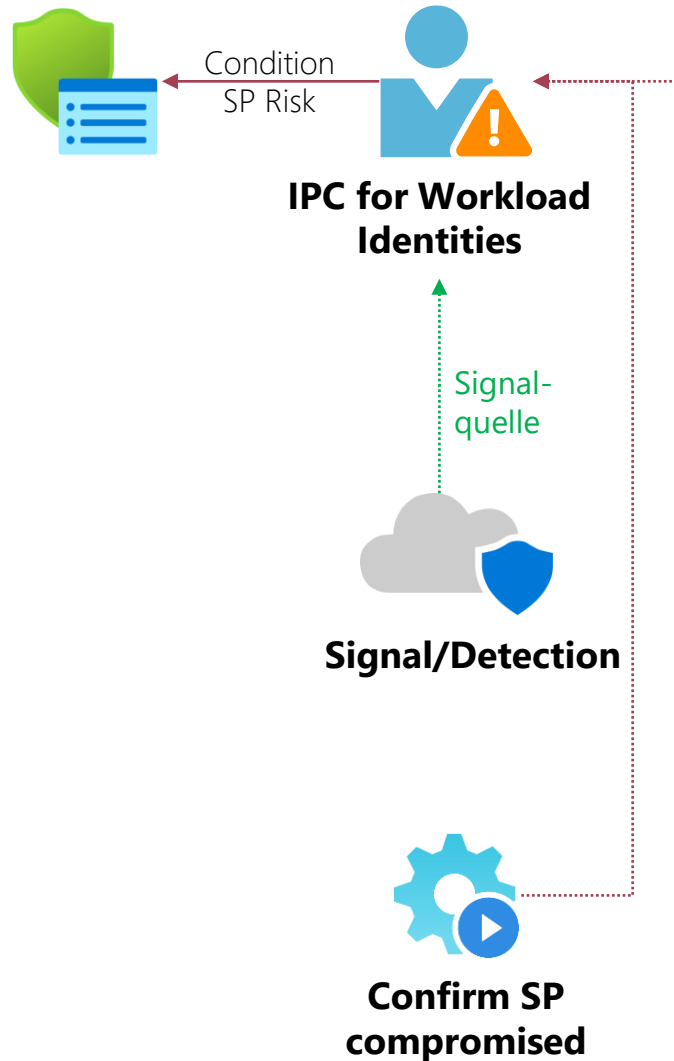
DEMO

Standardberechtigungen,
Azure AD Recommendations,
Delegierung und Klassifizierung



ZUGRIFFSSCHUTZ UND SECURITY MONITORING

Threat Intelligence und CA Integration



Azure AD Identity Protection (IPC)

- 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

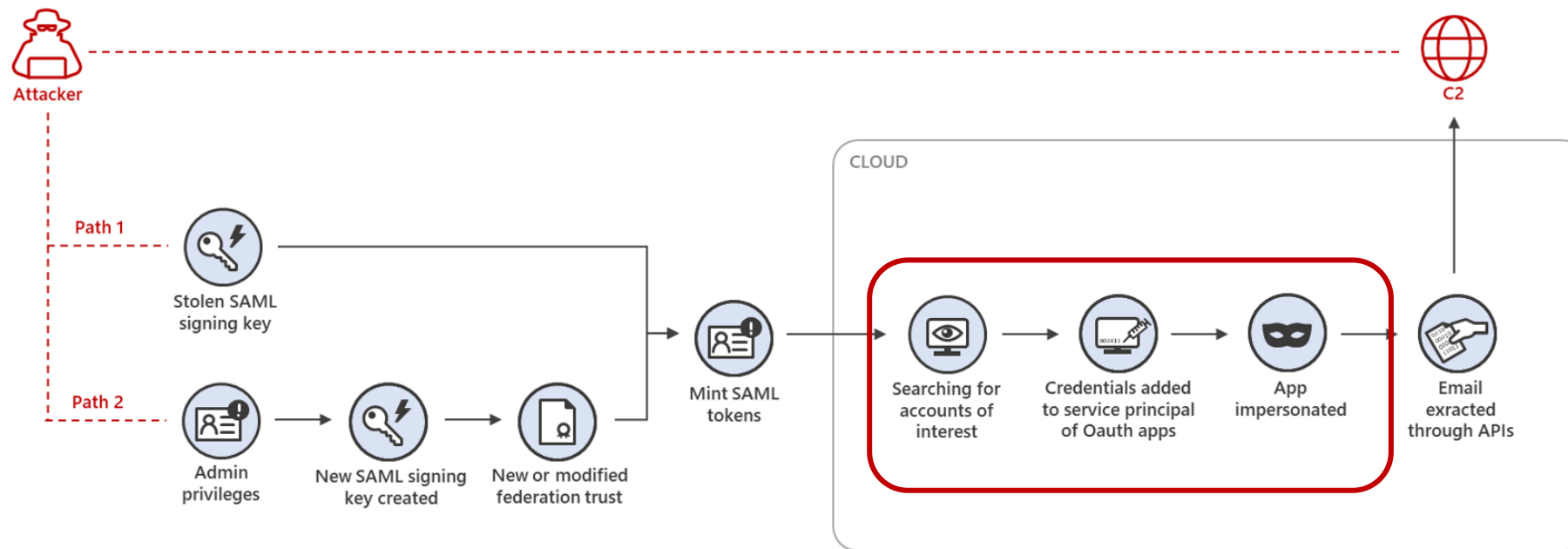
Microsoft Sentinel Analytics Rules (Custom Detections)

- Change of Application Owner or Redirect URI
- Federated Credential has been created for GitHub entity outside of organization
-

Attackers Service Principals

SOLORIGATE ATTACK

Stage 3: Hands-on-keyboard attack in the cloud



Quelle: [Using Microsoft 365 Defender to protect against Solorigate \(Microsoft\)](#)

More details: [Solorigate AzureAd IOCs \(microsoft.com\)](#)



DEMO

Workload Identity Premium Features,
MDA App Governance
Anreicherung für Analytics Rules/Detections



Zusammenfassung



Sichere Implementierung einer “Authentication Library” sowie Speicherung der Credentials und Tokens
Keine lange Laufzeiten von Credentials, Absicherung von “Trusted Entities” bei Workload Identity Federation
Implementierung von “Application management policy” zur Steuerung der Ausstellung von Credentials



Etablierung und Automatisierung von Prozessen für ein Lifecycle management
Einschränkung der Azure AD Rollen und Ownership mit Berechtigung auf Application/Service Principal Objekten
Klassifizierung um “Privilege escalation paths” und Kritikalität der “Workload Identity” nachzuvollziehen



Implementierung von “Conditional Access Policies for Service Principals” und Monitoring von “Risk Detections”
Monitoring von nicht genutzten Berechtigungen und Aktivitäten nach Authentifizierung/Authorisierung
Implementierung von Playbooks für “Automated Response” bei ungewöhnlichen Zugriffen und Authentifizierungen



Implementierung und Anpassung der vorhandenen “Rule templates” für Service Principals in Microsoft Sentinel
Monitoring der “Trusted Entities/IdP” (bei Federated Credentials) und Ressourcen mit zugewiesenen MSI
Review und Integration von Reports ([AzGovViz](#) und [AzADServicePrincipalInsights](#) von Julian Hayward)

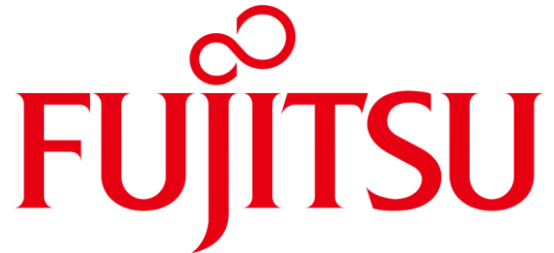


Vielen Dank an unsere Sponsoren!

Platinum



Mainzer
Datenfabrik



Gold





Bitte gebt uns euer Feedback

Feedbackbogen abgeben und Geschenk mitnehmen

Vielen Dank!



@Thomas_Live



Cloud-Architekt.net