



Absicherung und Management von Azure AD Workload Identities

Thomas Naunheim

Cloud Security Architect,
@glueckkanja-gab AG



Absicherung und Management von Azure AD Workload Identities



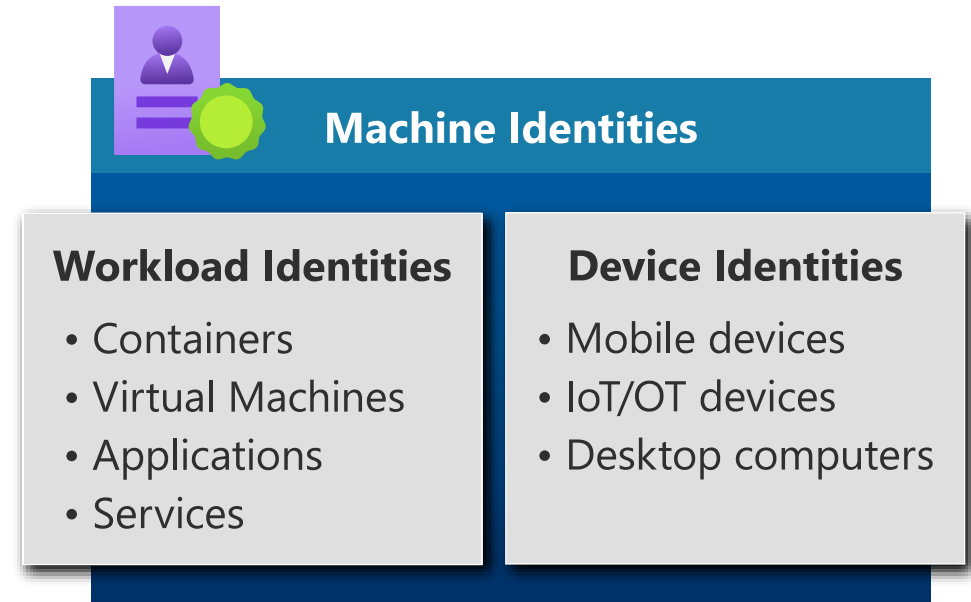
Thomas Naunheim

Cloud Security Architect @glueckkanja-gab AG
Microsoft MVP

Twitter: @Thomas_Live

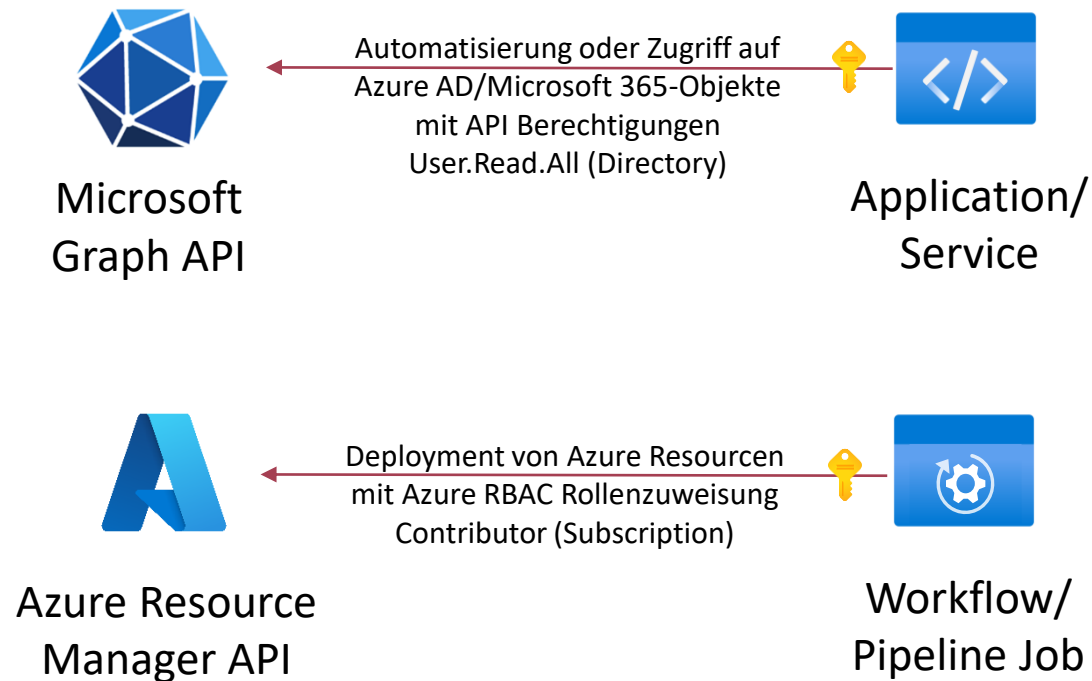
Blog: www.cloud-architekt.net

Was sind Workload Identities?



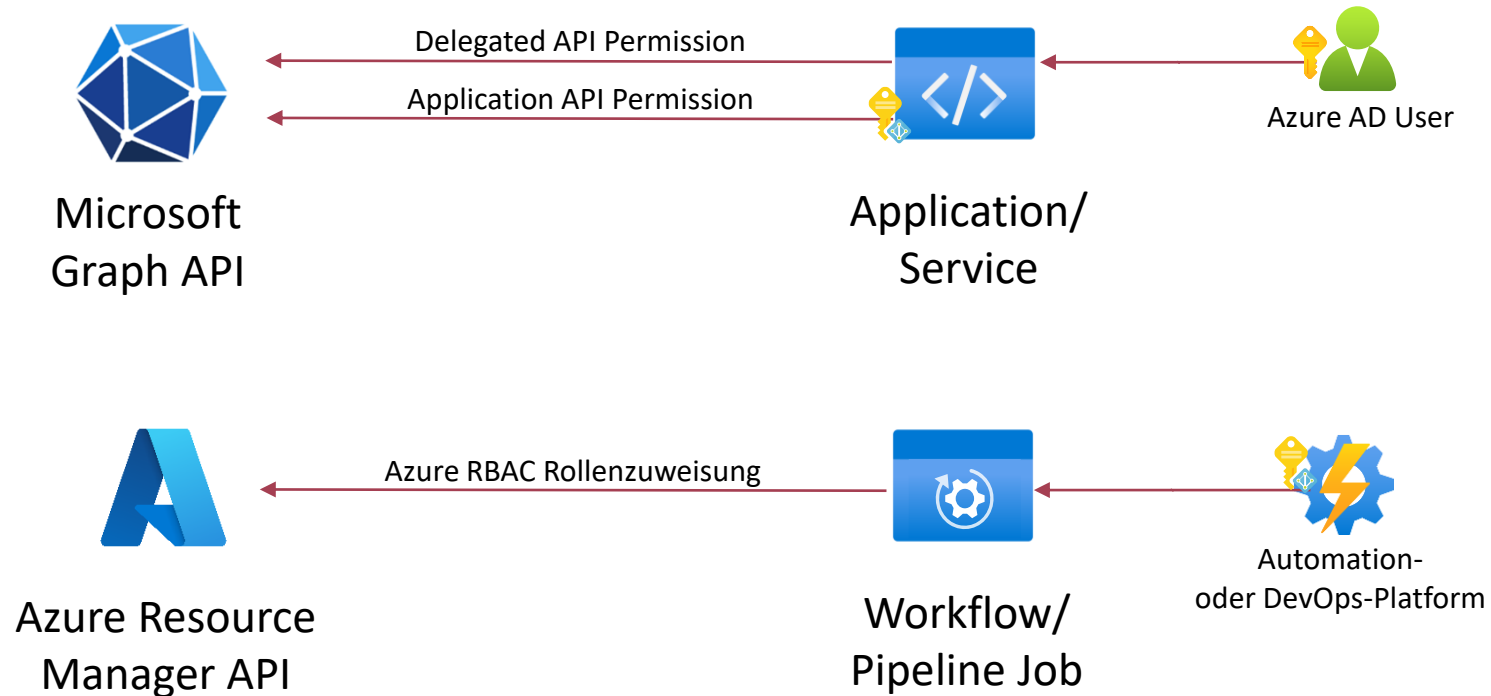
Was sind Workload Identities?

Authentifizierung zwischen Services



Was sind Workload Identities?

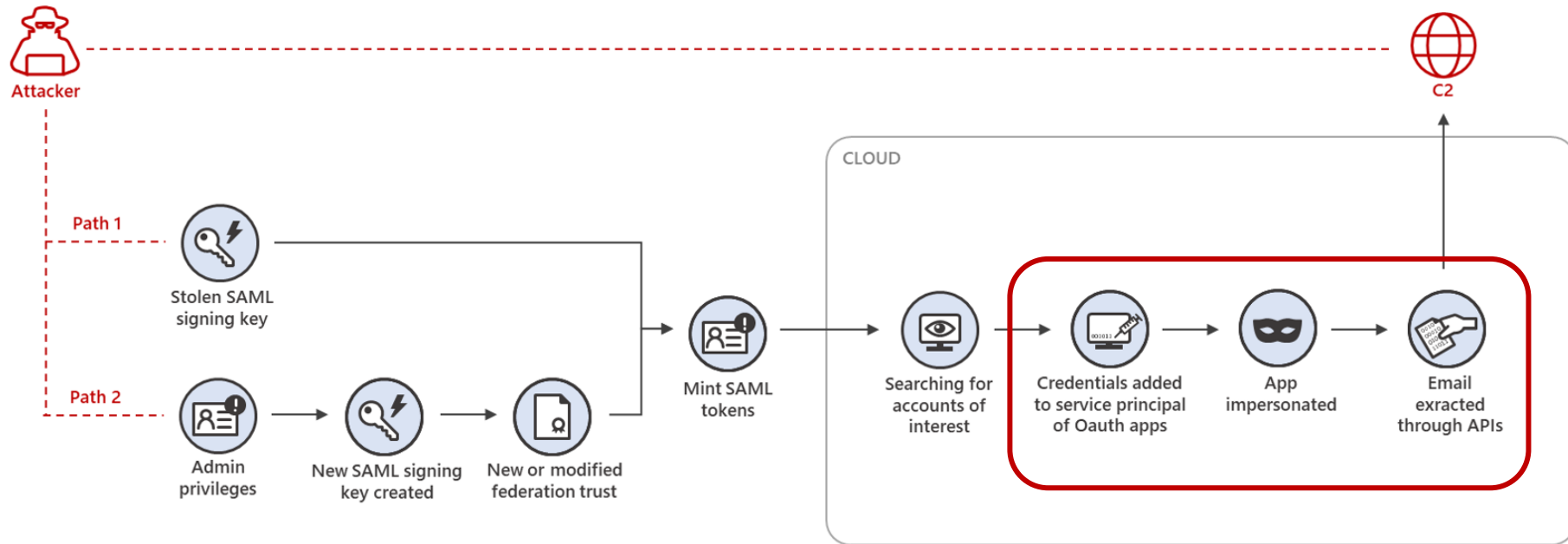
Authentifizierung zwischen Services



Was sind Workload Identities?

Beispiel für bekannte Angriffspfade

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



Absicherung und Management von Azure AD Workload Identities



Varianten von Workload Identities



Lifecycle Management und Delegation



Schutz und Absicherung des Zugriffs



Erweitertes Auditing und Monitoring



Varianten von Workload Identities

Application Identities (Client Secrets)

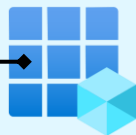
Workload Identity

Application Instance



Service Principal
(Enterprise App)

Application Definition



Application
(App Registration)



API Permissions



Client Secret



App Roles



Properties

Validierung Client Secret

Membership



Azure AD
Roles



Group
Membership

API Access

Admin/User
Consent Permissions



User.Read

Exposed API
oder App Roles
Permissions



Microsoft
Graph

Zuweisung von
Delegated/App Permissions

Microsoft Identity Platform

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

/token
Endpoint

Anfrage mit
Shared
secret

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

Validierung Public Key

App Roles

Properties

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

Microsoft Identity Platform

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

/token
Endpoint

Token mit
API Scope
& Groups

Anfrage
mit
sign.
JWT
token

Workload Env.

Private
/Public Key


Authentication
Library

Workload


Application Identities (Federated Credentials)


Workload Identity


Application Instance



Service Principal
(Enterprise App)


Application Definition


Application
(App Registration)

 API Permissions


 App Roles

 Properties

 **Federated**

Validierung ext. Token


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

Microsoft Identity Platform

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


/token
Endpoint

Anfrage
mit
Ext. IdP
token

Token mit
API Scope
& Groups

Workload Env.


Workload


OIDC IdP

Trust relationship



Live Demo

- Token Replay von Federated Workload (GitHub Actions)

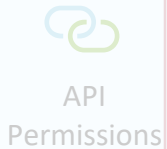
System-Assigned Managed Identity

Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Azure Identity Management

Managed Identity Resource Provider
(MSRP)



Certificate

Austellung Zertifikate
und Rollierung

Microsoft Identity Platform

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

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

Membership



Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions

User.Read

Exposed API
oder App Roles
Permissions



Microsoft
Graph

Azure Managed Resource

Assigned 1:1
Managed Identity (System)
Workload
Azure Instance
Metadata Service (IMDS)

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

Anfrage
lokal
/token
Endpoint

User-Assigned Managed Identity

Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Membership



Azure AD
Roles



Group
Membership

Azure Identity Management

Managed Identity Resource Provider
(MSRP)



Certificate

Austellung Zertifikate
und Rollierung

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)

Assigned
1:N

Workloads

IMDS

IMDS

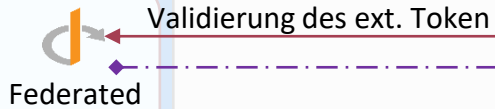
User-Assigned Managed Identity (Federated Credentials)

Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Membership



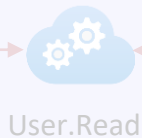
**Azure AD
Roles**



**Group
Membership**

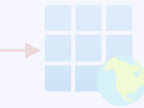
API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



**Microsoft
Graph**

Microsoft Identity Platform

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

/token
Endpoint

Anfrage mit
Ext. IdP
token

Token mit
API Scope
& Groups

Azure

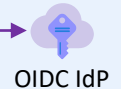


**Managed
Identity
(User)**

Workload Env.



Workload



OIDC IdP




Establish Trust relationship



Live Demo

- Sicherheitsbetrachtung von Managed Identities
- Relation von User-Assigned Identities zur Resource

Vergleich von Workload Identities

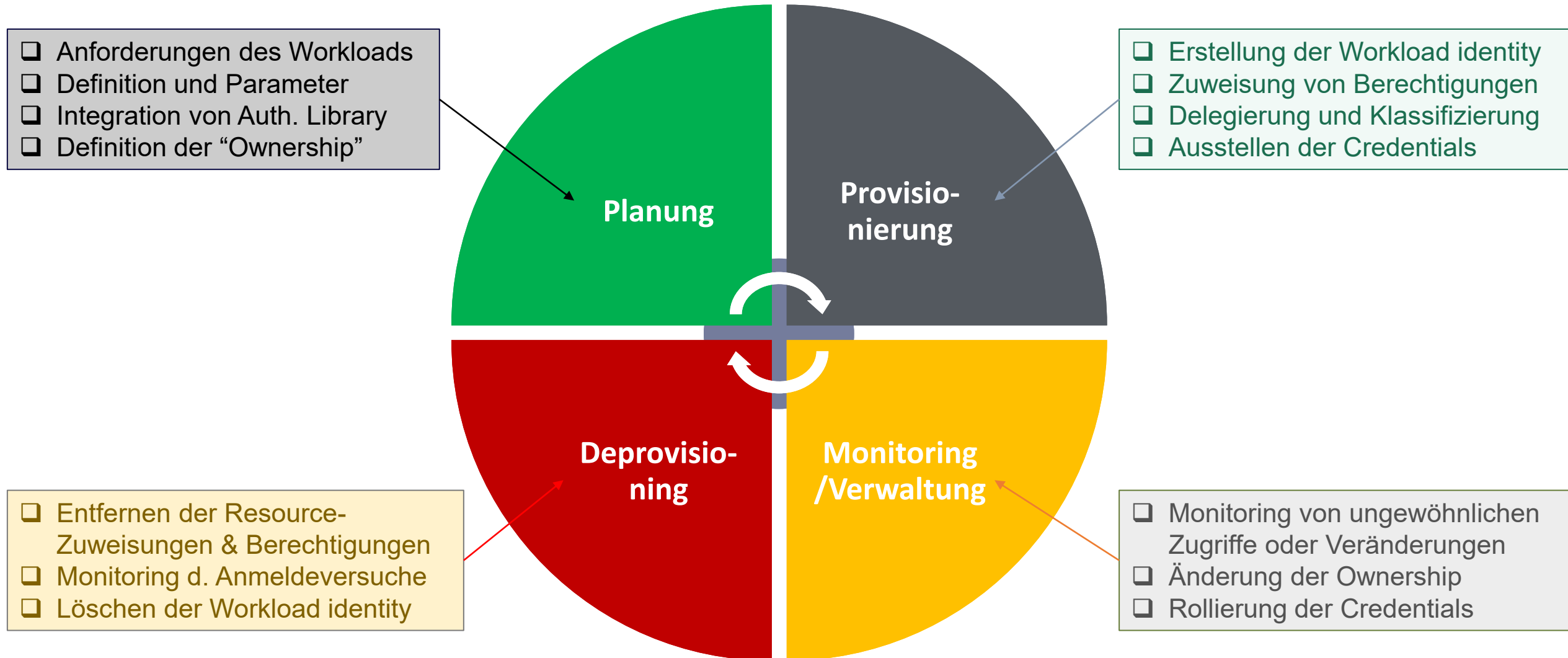
	 Application Identity (Key/Certificate)	 Application Identity (Federated Credentials)	 Managed Identity (System/User Assign.)
Use Cases	Keine Einschränkungen	Eingeschränkt, unterstützte Workloads und Identity Provider	Eingeschränkt, unterstützte Workloads (Azure-managed Resources)
Security Boundary	Single- oder Multi-Tenant	Single- oder Multi-Tenant	Single-Tenant*
Relation zu Workload	Keine direkte Zuweisung	Beziehung zu Issuer/Entity	Beziehung zu Resource(n) System (1:1), User (N:1)
Workload Umgebung	Unabhängig	external OIDC-compliant IdP	Azure- und Azure Arc-Ressourcen
Token Lifetime / Cache	1 Stunde (Default), 24 Stunden (CAE)	Abhängig von Issuer IdP (15-60 Minuten), 1 Stunde (Azure AD Token)	24 Stunden (Caching der Resource URI)

* Zugriffe auf Azure Resources in angebundene Subscriptions aus anderen Tenants per Azure Lighthouse






Lifecycle Management und Delegation

Lifecycle Management von Workload Identities



Vergleich von Workload Identities

	 Application Identity (Key/Certificate)	 Application Identity (Federated Credentials)	 Managed Identity (System/User Assign.)
Use Cases	Keine Einschränkungen	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 zu Workload	Keine direkte Zuweisung	Beziehung zu Issuer/Entity	Beziehung zu Resource(n) System (1:1), User (N:1)
Lifecycle management	Verwaltet durch Admin/Prozess	Verwaltet durch Admin/Prozess	System: Geteilter Lifecycle mit Resource, User: Unabhängig, "Manueller Lifecycle"
Administrative Delegierung	Application/Enterprise App Owner Azure AD Role (Directory, Object)		Enterprise App Owner, Azure AD Role Azure RBAC Role/Resource Owner
Recovery Optionen	Soft deleted		Nicht verfügbar

* Zugriffe auf Azure Resources in angebundene Subscriptions aus anderen Tenants per Azure Lighthouse



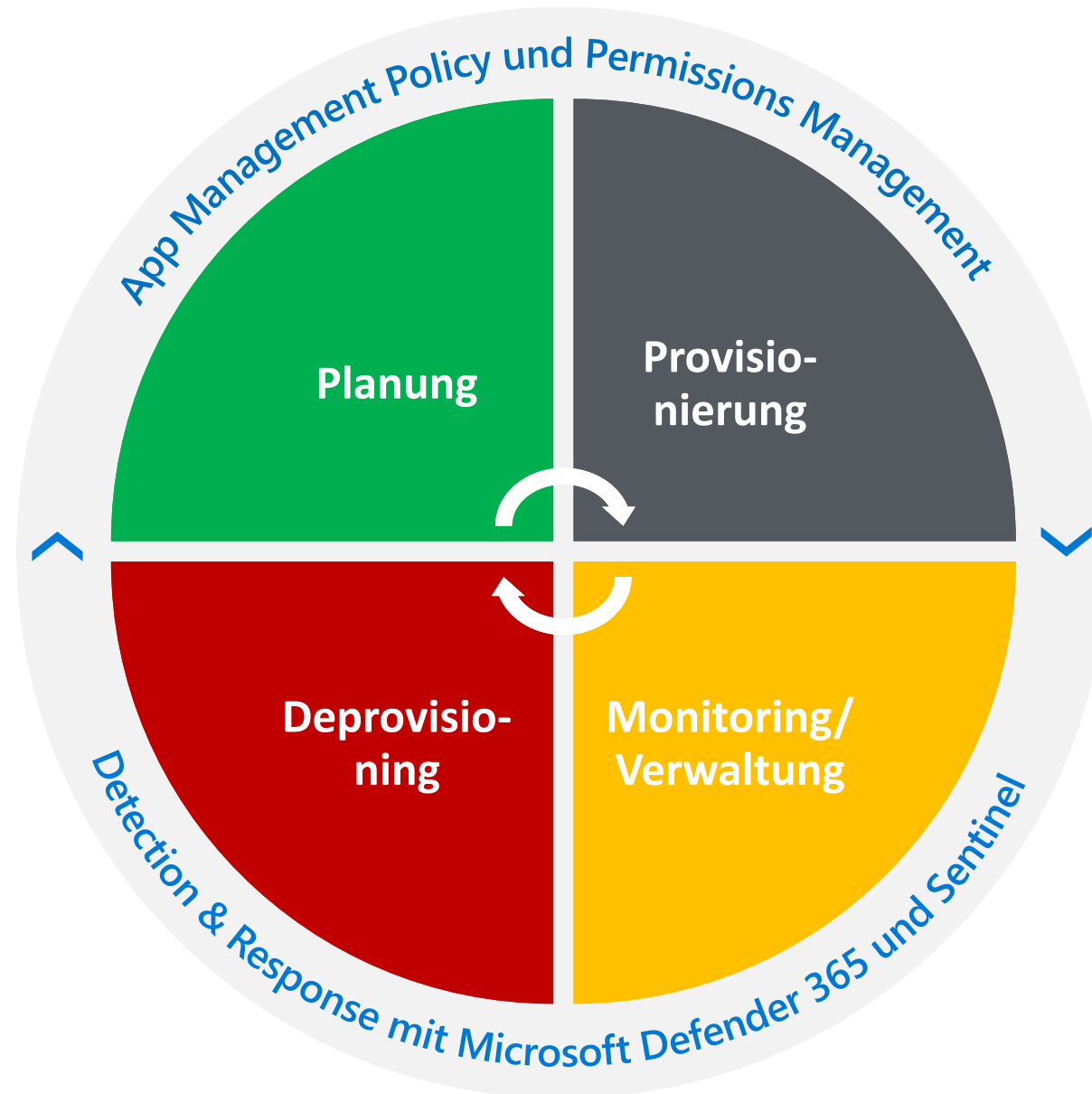
Live Demo

- Default Permissions und Custom Roles für Delegated Management
- App Management Policies
- Klassifizierung von Workload Identities

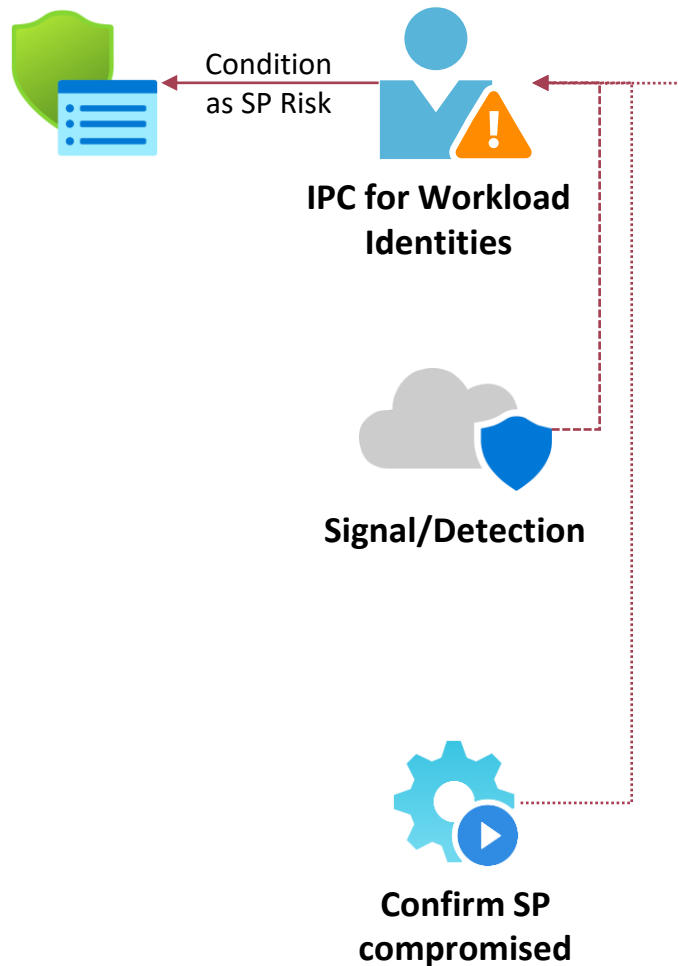


Schutz und Absicherung des Zugriffs

Security & Governance im Lifecycle



Threat Intelligence und Conditional Access



Azure AD Identity Protection (IPC)

- Anomalous service principal activity *
- Azure AD Threat Intelligence *
- Suspicious Sign-ins *
- Leaked Credentials (from GitHub) *

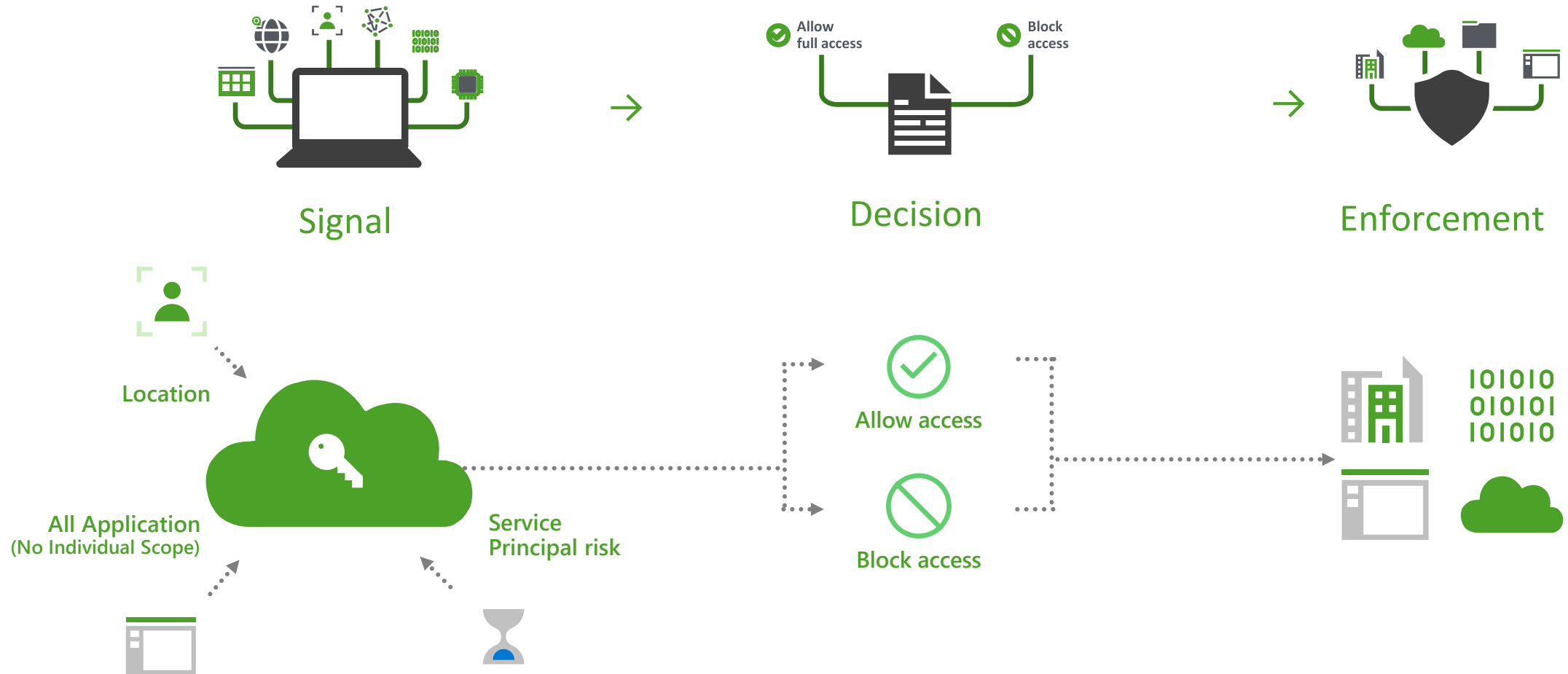
Microsoft Defender for Cloud Apps (MDA)

- Unusual addition of credentials to an OAuth app*
- Unusual ISP for an OAuth app
- ...

Microsoft Sentinel Analytics Rules (Custom Detections)

- Service Principal Authentication Attempt from New Country
- Federated Credential has been created for GitHub entity outside of organization
- ...

Conditional Access for Workload Identities








Live Demo

- Conditional Access und Identity Protection
- Detection and Response with Microsoft Sentinel
- MDA App Governance and Entra Permissions Management

Vergleich von Workload Identities

	 Application Identity (Key/Certificate)	 Application Identity (Federated Credentials)	 Managed Identity (System/User Assign.)
Use Cases	Keine Einschränkungen	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 zu Workload	Keine direkte Zuweisung	Beziehung zu Issuer/Entity	Beziehung zu Resource(n) System (1:1), User (N:1)
Lifecycle management	Verwaltet durch Admin/Prozess	Verwaltet durch Admin/Prozess	System: Geteilter Lifecycle mit Resource, User: Unabhängig, "Manueller Lifecycle"
Administrative Delegierung	Application/Enterprise App Owner Azure AD Role (Directory, Object)		Enterprise App Owner, Azure AD Role Azure RBAC Role/Resource Owner
Recovery Optionen	Soft deleted		Nicht verfügbar
Sicherheitsaspekte	Absicherung der Speicherung der Credentials, Schutz des App/SP Object	Sicherheit des Federated Workload/IdP, Schutz des App/SP Object	Eingeschränkter Zugriff und Schutz der Azure Resource(n) und SP Object
Einschränkung und Validierung des Zugriff	Conditional Access (nur für Single Tenant), CAE support		Nicht verfügbar
Erkennung von Angriffen	Identity Protection, Sign-in logs	Identity Protection, Korrelation zwischen AAD und Trusted IdP AuthN/AuthZ logs	Eingeschränkte Sign-in logs



Erweitertes Auditing und Monitoring

Automatische Klassifizierung

Klassifizierung von Berechtigung (Action) und deren Scope

```
[
  {
    "EAMTierLevelName": "ControlPlane",
    "EAMTierLevelTagValue": "0",
    "TierLevelDefinition": [
      {
        "Category": "Microsoft.Azure",
        "Service": "Management",
        "RoleAssignmentScopeName": [
          "/",
          "/providers/Microsoft.Management/managementGroups/36955ea9-c98e-",
          "/providers/Microsoft.Management/managementGroups/lab",
          "/providers/Microsoft.Management/managementGroups/lab-platform",
          "/providers/Microsoft.Management/managementGroups/lab-saezone"
        ],
        "RoleDefinitionActions": [
          "Microsoft.Authorization/*",
          "*"
        ]
      }
    ]
  }
]
```

Tiered Level der Workload Identity

```
{
  "ObjectId": "4fbc88a-18b5-42cf-82ac-30ca6d4f6919",
  "ObjectType": "ServicePrincipal",
  "ObjectDisplayName": "azops-msi",
  "Classification": [
    {
      "AdminTierLevel": "0",
      "AdminTierLevelName": "ControlPlane",
      "Service": "Management"
    }
  ],
  "RoleAssignments": [
    {
      "RoleAssignmentId": "/providers/Microsoft.Authorization/roleAssignments/a308c801",
      "RoleAssignmentScope": "/",
      "RoleAssignmentType": "Direct",
      "PIMManagedRole": "False",
      "PIMAssignmentType": "Permanent",
      "RoleDefinitionName": "Owner",
      "RoleDefinitionId": "8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
      "ObjectId": "4fbc88a-18b5-42cf-82ac-30ca6d4f6919",
      "ObjectDisplayName": "azops-msi",
      "ObjectType": "ServicePrincipal",
      "Classification": [
        {
          "AdminTierLevel": "0",
          "AdminTierLevelName": "ControlPlane",
          "Service": "Management",
          "TaggedBy": "JSONwithAction"
        }
      ]
    }
  ]
}
```




Live Demo

- Klassifizierung nach Enterprise Access Model
- Erweitertes Hunting mit Microsoft Sentinel
- Review und Reporting mit "AzADServicePrincipalInsights"

Workload Identities | 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](#) and [AzADServicePrincipalInsights](#) von Julian Hayward)

Fragen?



@Thomas_Live



Thomas@Naunheim.net

Vielen Dank!

