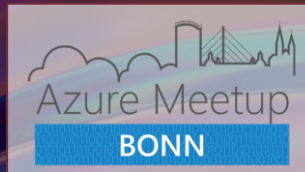




MICROSOFT ENTRA IGNITE 2022 RECAP





THOMAS NAUNHEIM

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany



@Thomas_Live



cloud-architekt.net

MICROSOFT ENTRA PRODUCT FAMILY

Secure your entire identity infrastructure with identity management and beyond. Protect your business with decentralized identity, identity protection, governance and more in a multi-cloud environment.



Azure Active Directory

Secure and manage identities to connect them with apps, devices and data.



Permissions Management

Discover, remediate, and monitor permission risks for any identity or resource.



Verified ID

Create, issue and verify decentralized identity credentials for secure interactions.



Workload Identities

Manage, secure and govern your workloads with Azure AD Workload Identities.



Identity Governance

Manage access rights with entitlement management, access reviews and lifecycle workflows.

HIGHLIGHTS OF MICROSOFT IGNITE 2022

MICROSOFT ENTRA



**ZERO TRUST &
CONDITIONAL ACCESS**



**SECURING DEVOPS AND
WORKLOAD IDENTITIES**



**IDENTITY LIFECYCLE
& GOVERNANCE**



**MODERNIZING IDENTITY
& MIGRATE FROM ON-PREM**



ZERO TRUST AND CONDITIONAL ACCESS

ZERO TRUST AND CONDITIONAL ACCESS

NEW CONDITIONS AND CONTROLS

☐ Require multifactor authentication ⓘ

☒ Require authentication strength (Preview) ⓘ

Multi-factor authenti... ▾

- Multifactor authentication
- Combinations of methods that satisfy strong authentication, such as Password + SMS
- Passwordless multifactor authentication ⓘ
- Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator ⓘ
- Phishing-resistant multifactor authentication ⓘ
- Phishing-resistant Passwordless methods for the strongest authentication, such as FIDO2 Security Key

Dashboard > Security | Authentication methods > Authentication methods

Authentication methods | Authentication strengths (Preview) ...

CloudLab - Azure AD Security

Search << + New authentication strength Refresh

Manage

- Policies
- Password protection
- Registration campaign
- Authentication strengths (Preview)**

Authentication strengths determine the combination of authentication methods that can be used. [Learn more](#)

Type: All Authentication methods: All Reset filters

Authentication strength	Type	Authentication methods
Multi-factor authentication	Built-in	Windows Hello For Business and 16 more
Passwordless MFA	Built-in	Windows Hello For Business and 3 more
Phishing resistant MFA	Built-in	Windows Hello For Business and 2 more

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

ZERO TRUST AND CONDITIONAL ACCESS

NEW CONDITIONS AND CONTROLS

Users ⓘ

Specific users included and specific users excluded

✖ "Select users and groups" must be configured

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

☐ None

☐ All users

☒ Select users and groups

☒ Guest or external users ⓘ

B2B direct connect users (previ... ▼

Specify external Azure AD organizations (preview)

☐ All

☒ Select

Select

0 Azure AD organizations selected

✖ Please select at least one external tenant

schaengel.onmicrosoft.com ✕

☒ Schaengel
4c627b77-fa10-4cd2-bd14-95b4f8fc8151

Selected items

Schaengel
4c627b77-fa10-4cd2-bd14-95... Remove

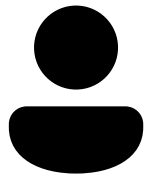
ZERO TRUST AND CONDITIONAL ACCESS

IMPROVEMENTS ON ENDPOINTS

- **Windows LAPS and Azure Active Directory**
 - Available only in Windows 11 Insider Preview Build 25145 and later
 - Deploy and configure policy for LAPS via Microsoft ~~Endpoint Manager~~ Intune or manually
 - Retrieve and store password in Azure AD (Microsoft Graph: Device.LocalCredentials.*)
- **Intune Endpoint Privilege Management (part of Intune Premium)**
 - Manage and elevate standard users' permission to admin (to perform specific task)
 - For example, Install applications or peripheral devices (e.g. printers)

ZERO TRUST AND CONDITIONAL ACCESS

NEW IDENTITY PROTECTION DETECTION TYPES!?



Human
Identities

Auto refresh : Off

Detection time : Last 7 days

Show dates as : Local

Detection type : Anomalous user activity

Risk state : 2 selected

Risk level : None Selected

+ Add filters

User detections

Workload identity detections

Detection time ↑↓

User ↑↓

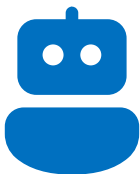
IP address ↑↓

Location

No risk events found

Detection type

- ☐ Activity from anonymous IP address
- ☐ Admin confirmed user compromised
- ☐ Anomalous token
- ☒ Anomalous user activity



Workload
Identities

Auto refresh : Off

Detection time : Last 7 days

Show dates as : Local

Detection type : None Selected

Risk state : 2 selected

Risk level : None Selected

+ Add filters

User detections

Workload identity detections

Detection time ↑↓

Service principal name ↑↓

Detection type ↑↓

No risk events found

Detection type

- ☒ Anomalous service principal activity
- ☐ Azure AD threat intelligence
- ☐ Leaked credentials
- ☐ Malicious application

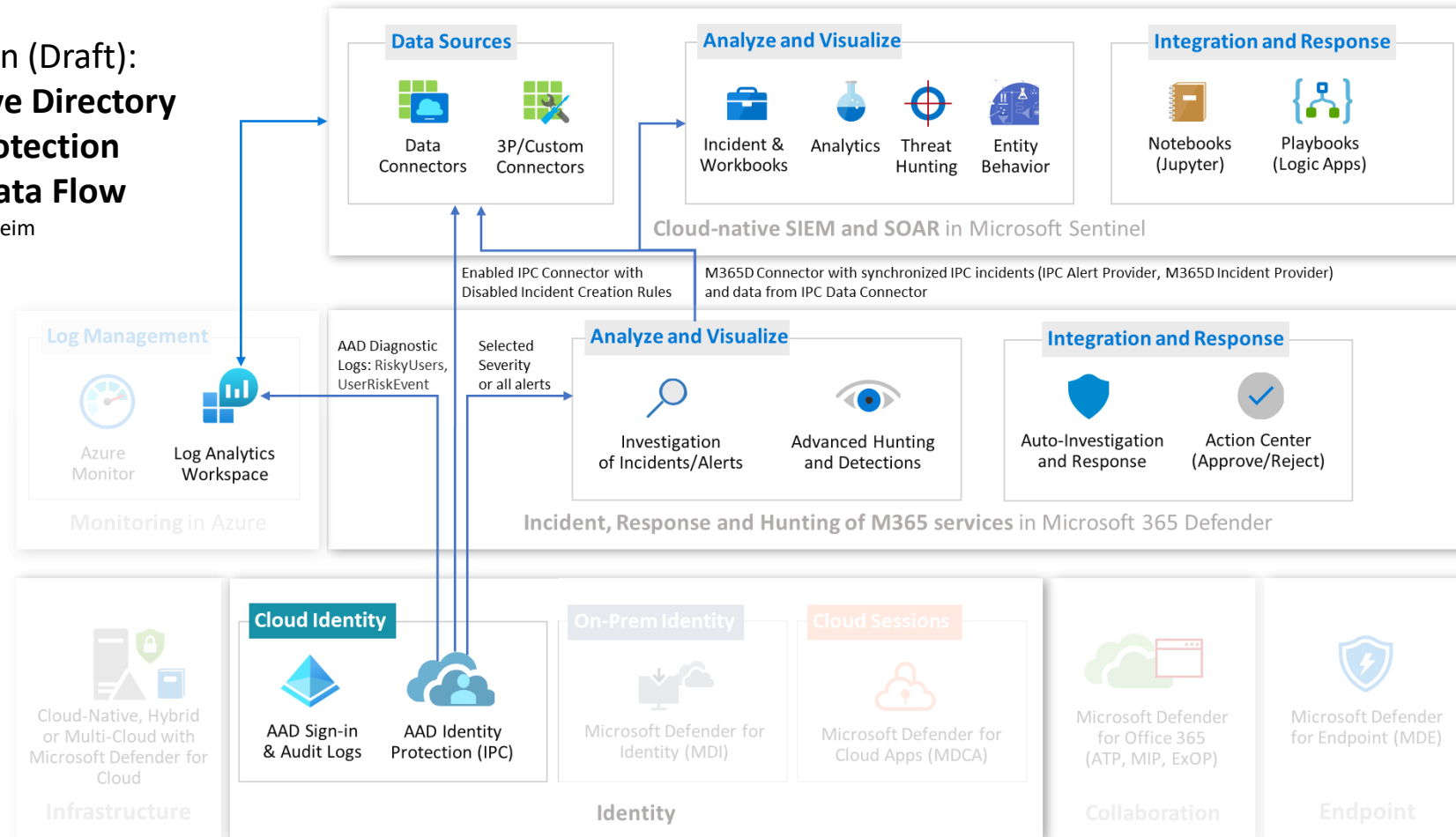
Authentication Strengths in Conditional Access

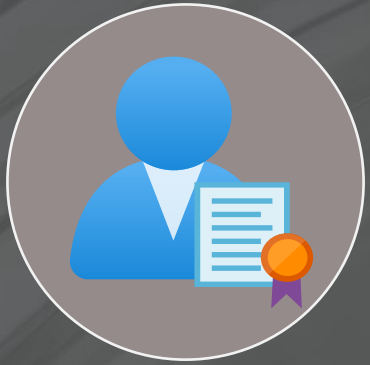
LIVE DEMO

ZERO TRUST AND CONDITIONAL ACCESS

IPC-INTEGRATION IN M365 DEFENDER PORTAL

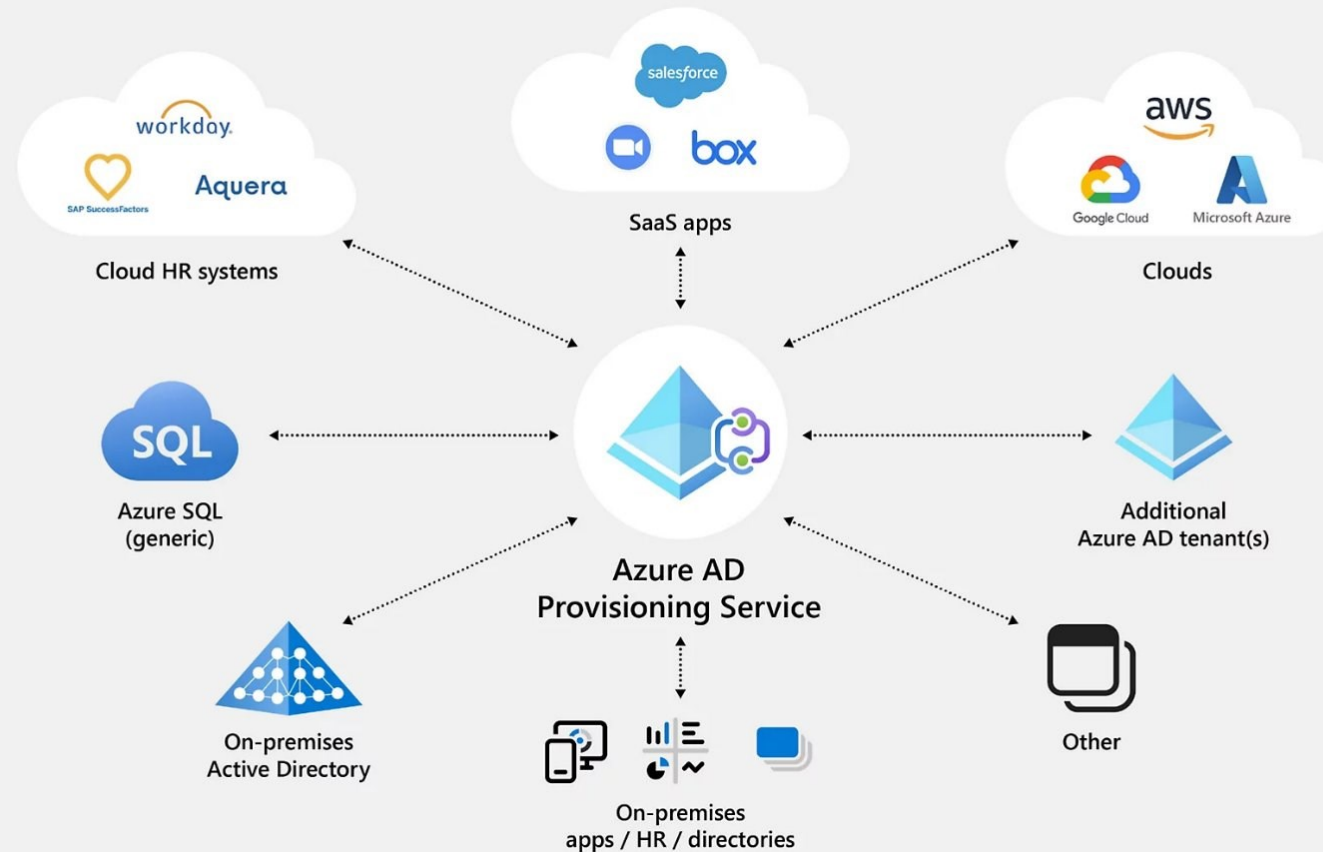
Visualization (Draft):
**Azure Active Directory
Identity Protection
Incident/Data Flow**
By Thomas Naunheim





IDENTITY LIFECYCLE & GOVERNANCE

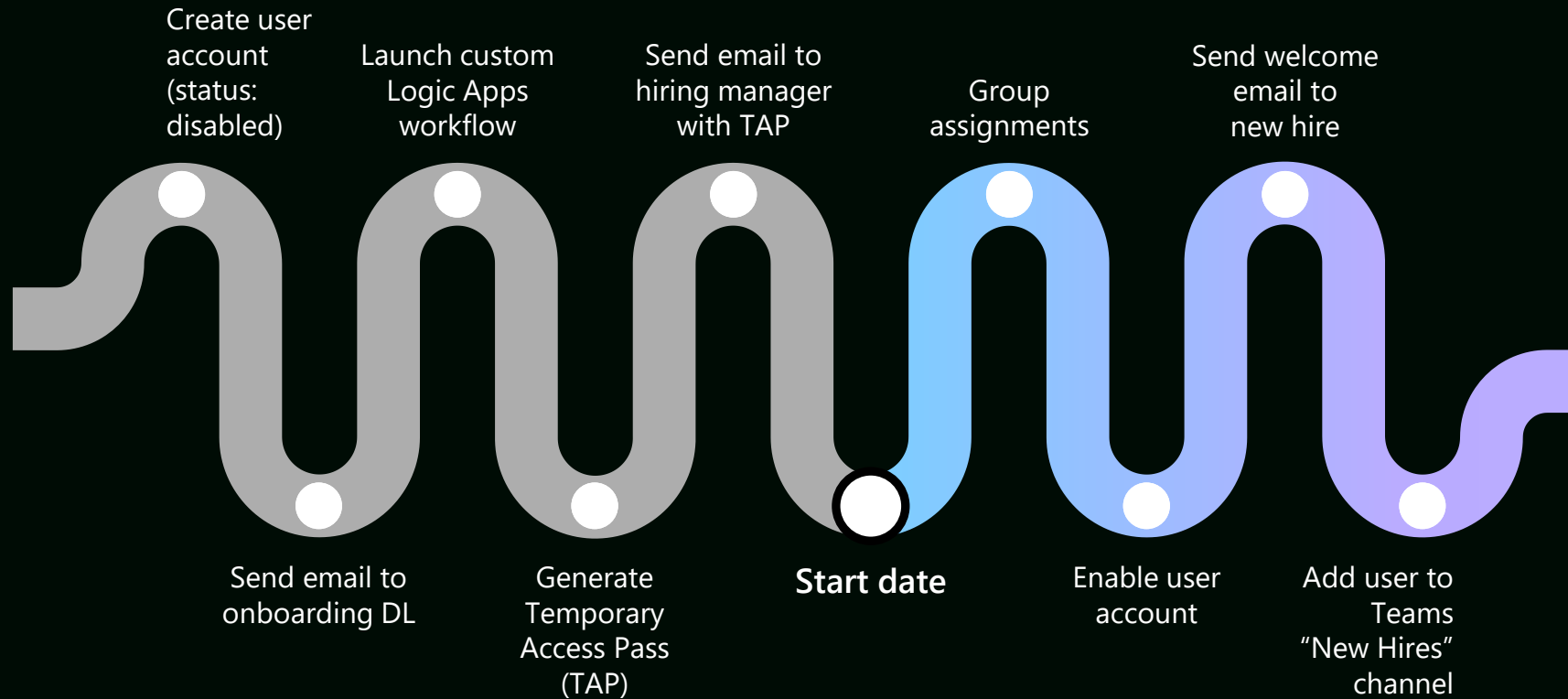
MICROSOFT ENTRA IDENTITY GOVERNANCE IN PUBLIC PREVIEW



Source: "[Microsoft Entra Identity Governance \(Product page\)](#)"

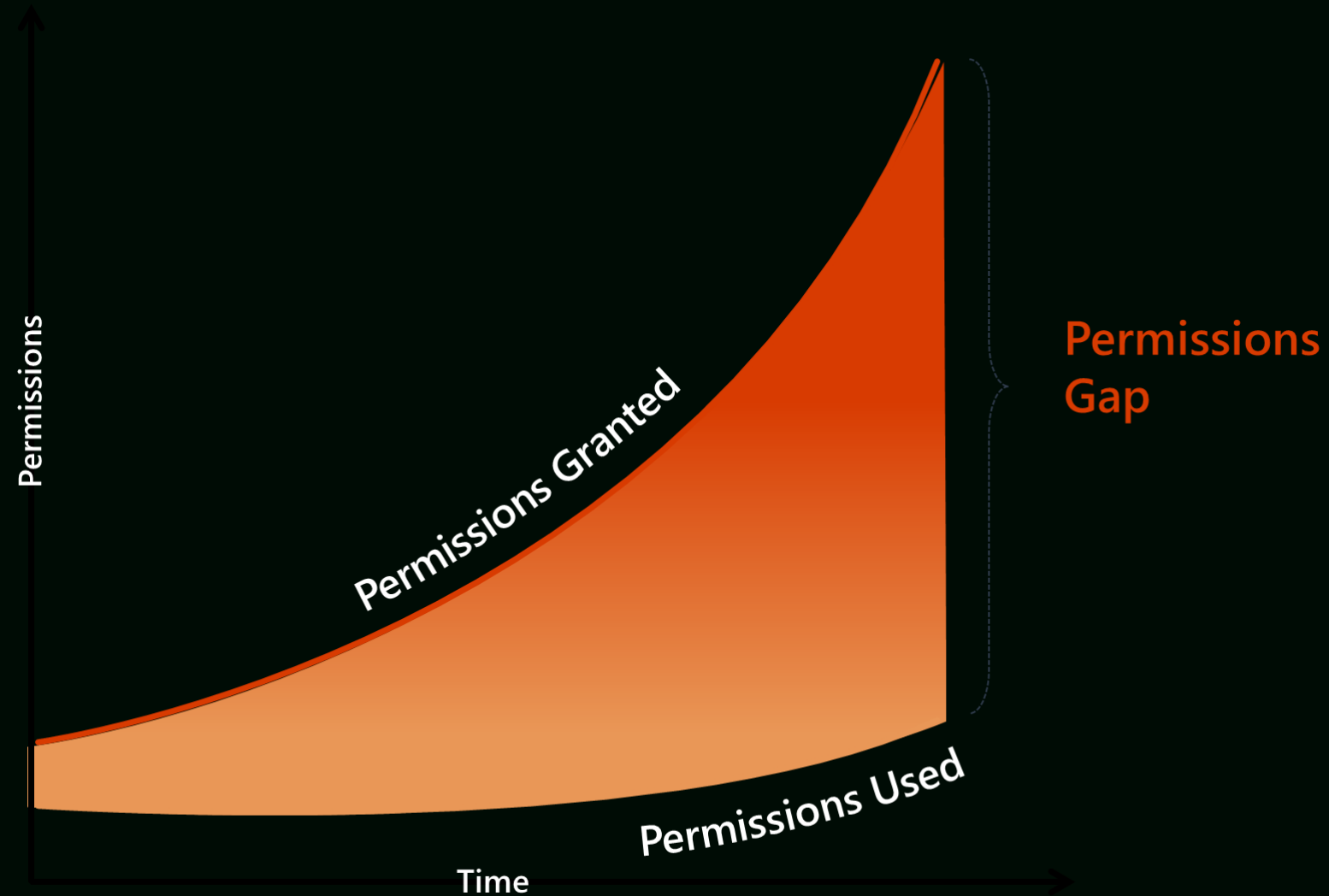
IDENTITY LIFECYCLE & GOVERNANCE

LIFECYCLE WORKFLOWS



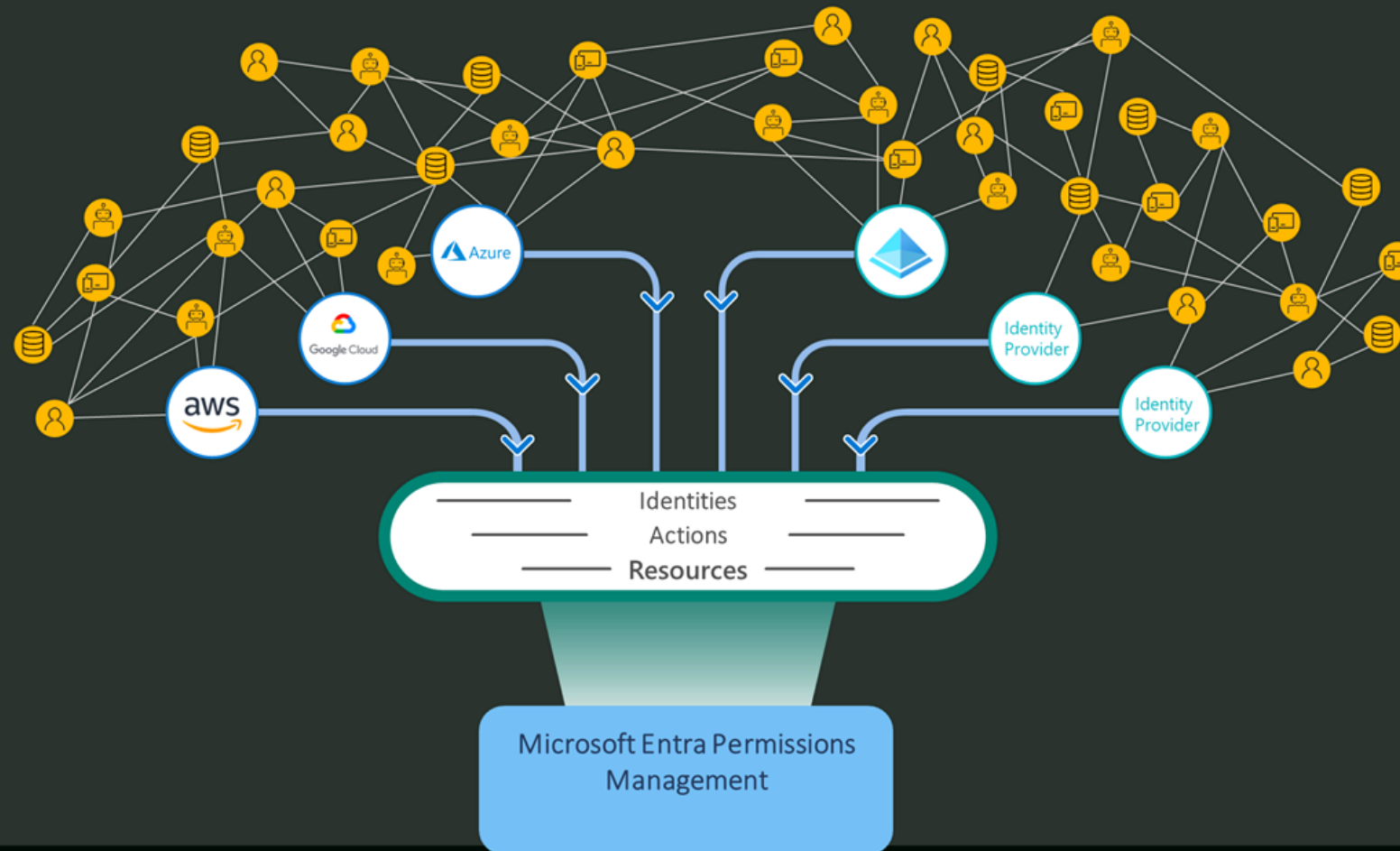
IDENTITY LIFECYCLE & GOVERNANCE

PERMISSIONS MANAGEMENT



IDENTITY LIFECYCLE & GOVERNANCE

PERMISSIONS MANAGEMENT IN MULTI-CLOUD ENVIRONMENTS



Identity Workflows and Entra Permissions Management

LIVE DEMO

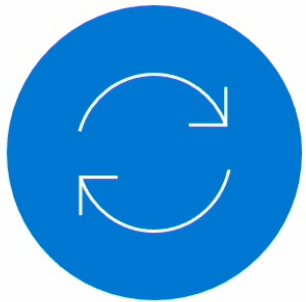


SECURING DEVOPS WORKLOAD IDENTITIES

SECURING WORKLOAD IDENTITIES

ANNOUNCEMENTS

Challenges of securing workload identities



No defined joiner/mover/leaver lifecycle to manage



Higher potential for leaked secrets or credentials



Lacking capabilities for managing access to resources

Workload identities are proliferating

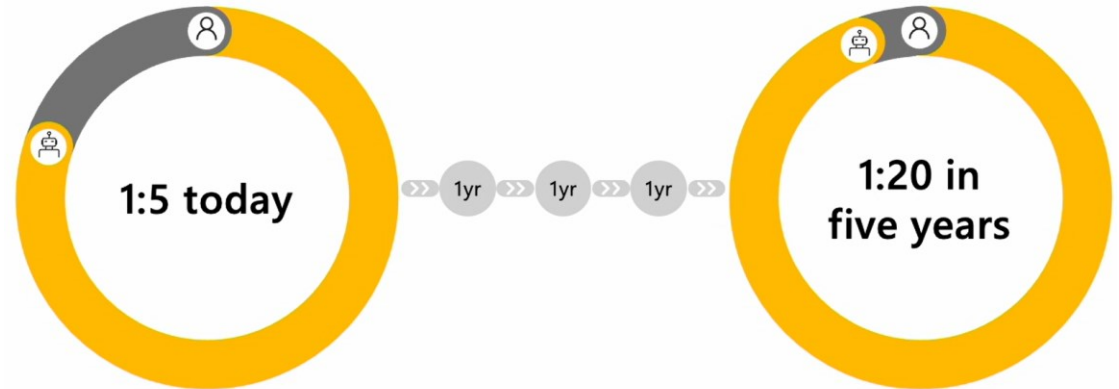
Ratio of user identities vs. workload identities



- User Identity



- Workload Identity



Source: Microsoft Security internal research 2021

SECURING WORKLOAD IDENTITIES ANNOUNCEMENT

- CA, IPC and Access Reviews will be generally available in November 2022



SECURING DEVOPS PLATFORMS

MICROSOFT DEFENDER FOR DEVOPS

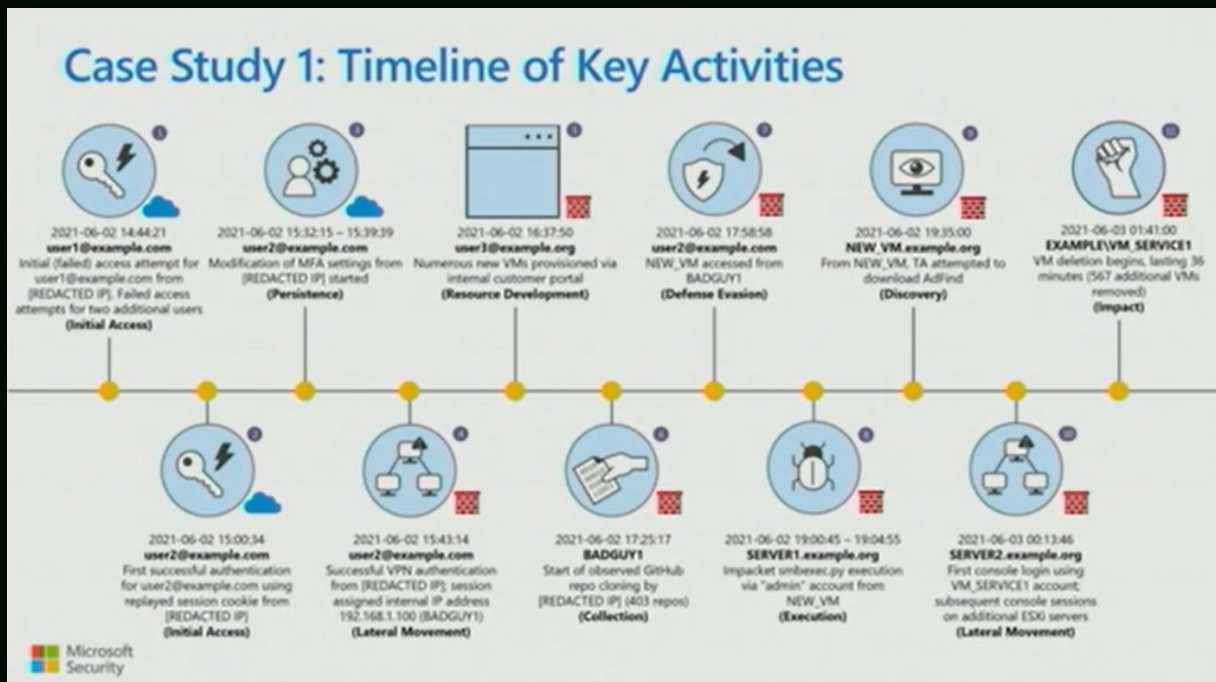
- **Microsoft Defender for DevOps**
 - Available for GitHub (Enterprise) and Azure DevOps
 - Manage posture management and critical issues in supply chain (incl. pipelines)
 - More DevOps platforms will be supported in future
- **GitHub Advanced Security for Azure DevOps**
 - CodeQL code scanner to identify vulnerabilities
 - Identify and fix exposed secrets and vulnerable open-source dependencies

Microsoft Entra Workload Identities Security Attack Explorer

LIVE DEMO

MICROSOFT SECURITY RECOMMENDED SESSION

- Stories from DART: Taking the ware out of ransomware

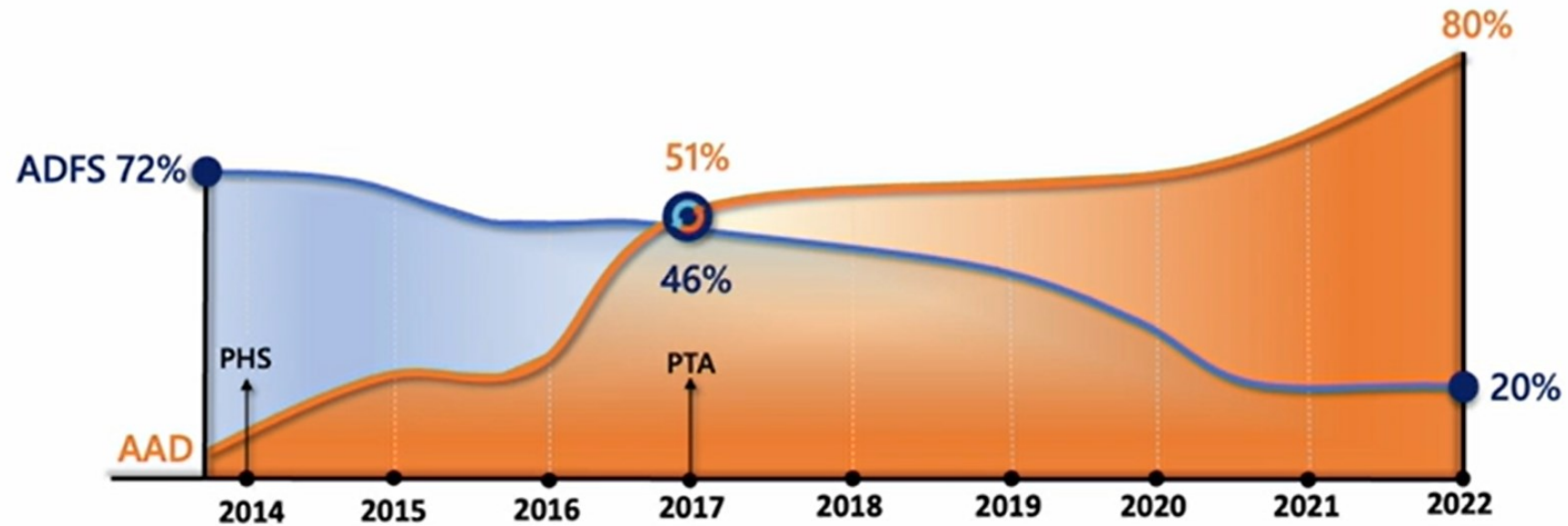




MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

MIGRATING ADFS APPS TO AZURE AD



MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

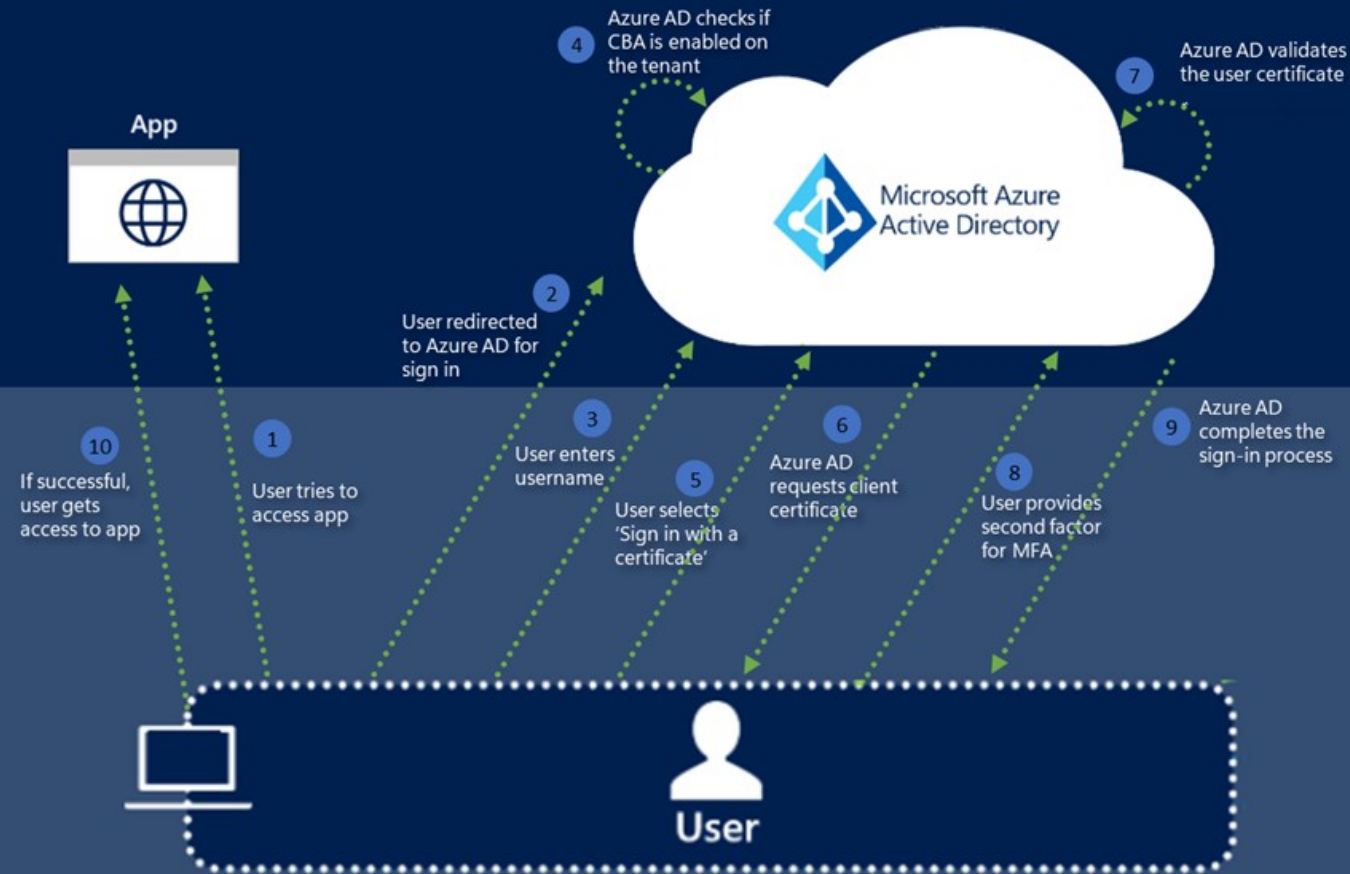
BEYOND AD FS: CAPABILITIES IN AZURE AD



- Basic Conditional Access Policies
- Single Sign-On

- Access Governance & Access Reviews
- Identity Protection
- Continuous Access Evaluation
- B2B Guest Access to Apps
- Passwordless
- User Provisioning to Applications (SCIM)
- Microsoft managed service with 99.99% uptime
- Advanced Conditional Access Policies
- Single Sign-On

MODERNIZE IDENTITY & MIGRATE FROM ON-PREM CERTIFICATE-BASED AUTHENTICATION (CBA)



THANK YOU



@Thomas_Live



Thomas@Naunheim.net

www.cloud-architekt.net