MICROSOFT ENTRA
IGNITE 2022 RECAP

Azure Meetup
BONN

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.

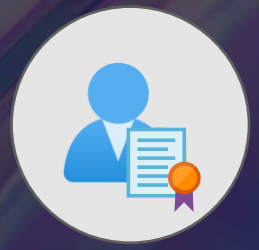
Source: Microsoft Entra Portal

HIGHLIGHTS OF MICROSOFT IGNITE 2022

MICROSOFT ENTRA

ZERO TRUST &
CONDITIONAL ACCESS

SECURING DEVOPS AND
WORKLOAD IDENTITIES

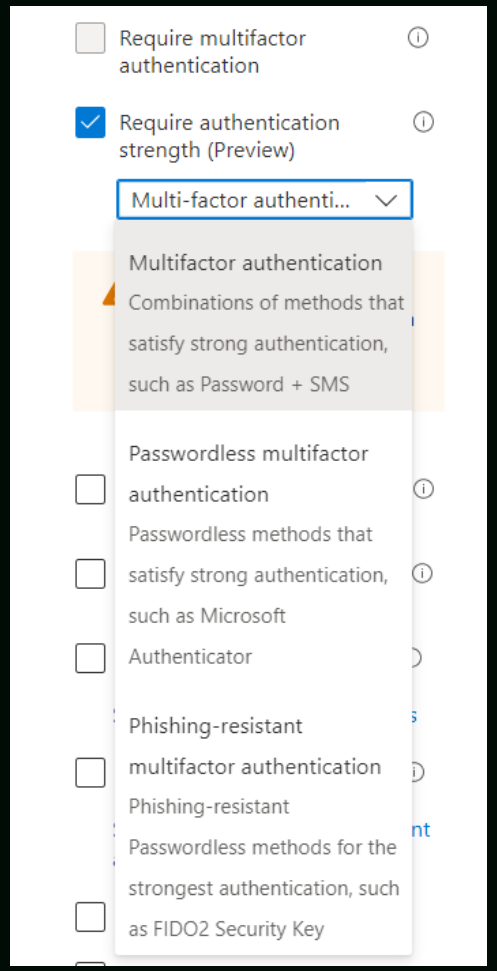


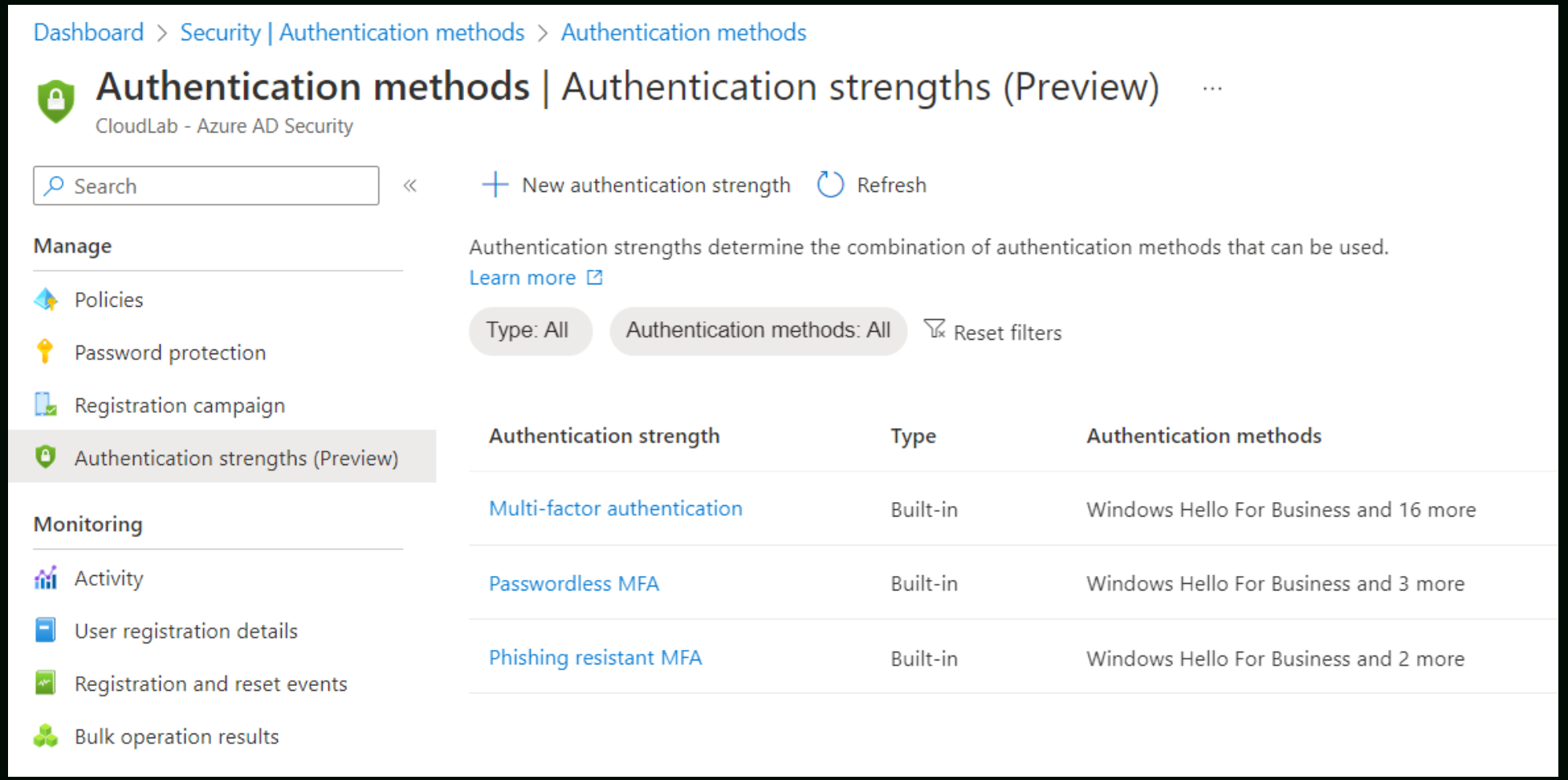
IDENTITY LIFECYCLE
& GOVERNANCE

MODERNIZING IDENTITY
& MIGRATE FROM ON-PREM

ZERO TRUST AND CONDITIONAL ACCESS

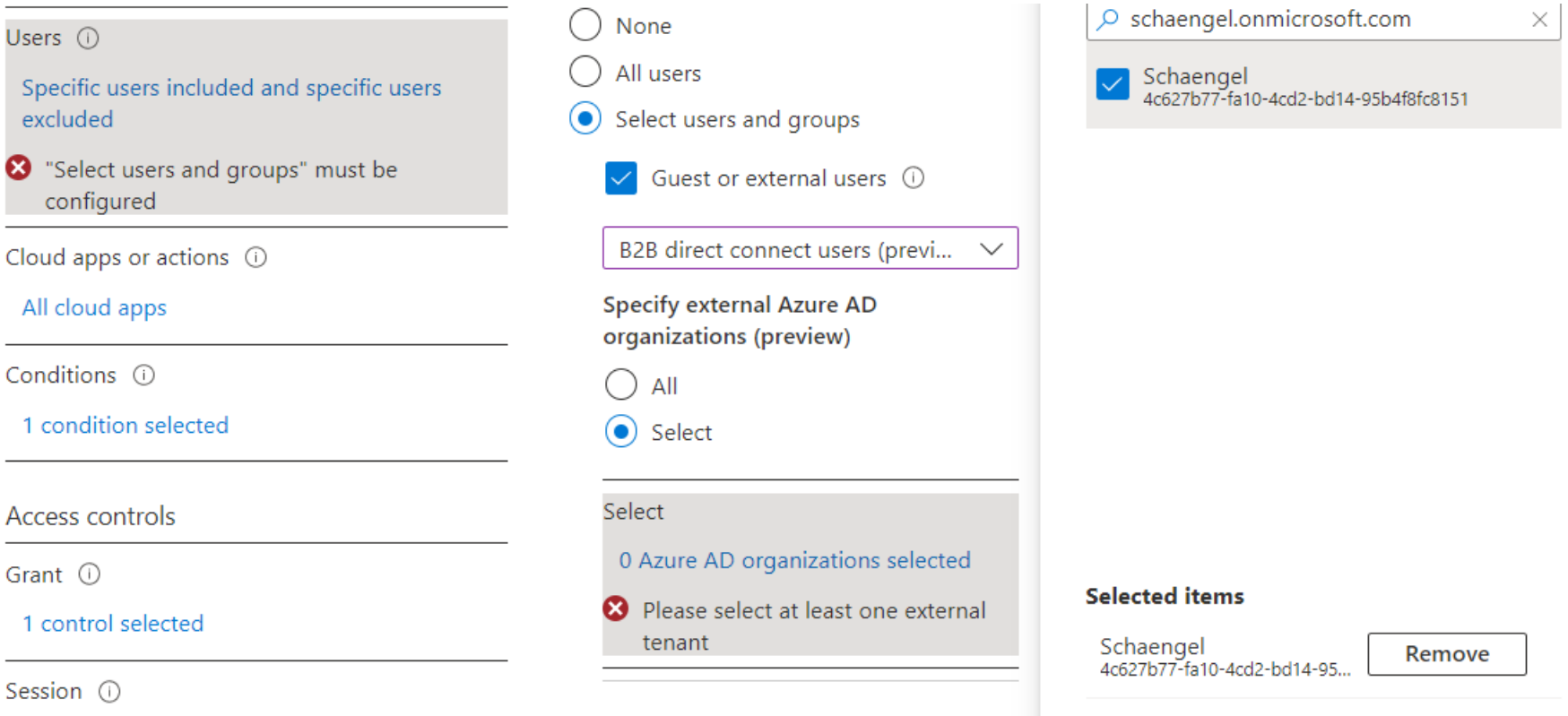
ZERO TRUST AND CONDITIONAL ACCESS
NEW CONDITIONS AND CONTROLS





More details: "Conditional Access authentication strength (Microsoft Docs)"

ZERO TRUST AND CONDITIONAL ACCESS
NEW CONDITIONS AND CONTROLS



More details: "Assigning Conditional Access policies to external user types (Microsoft Docs)"

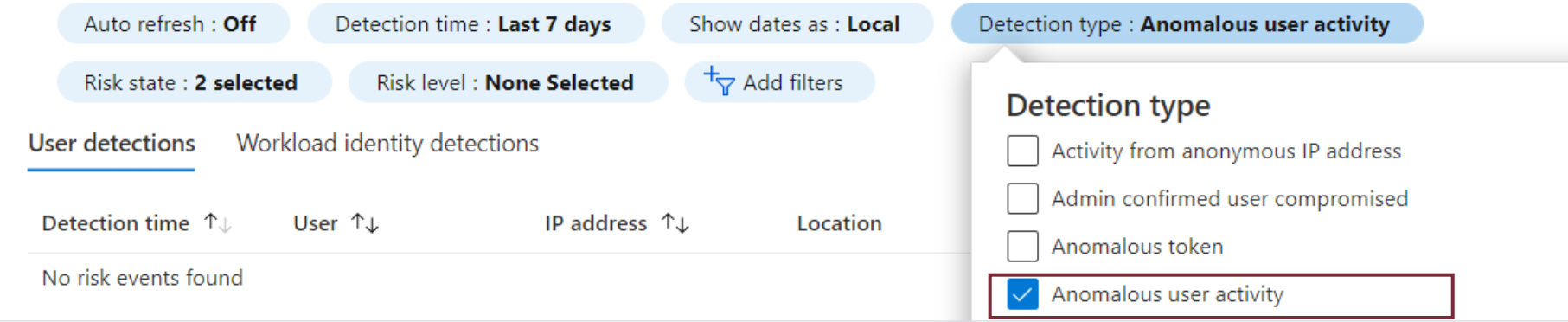
ZERO TRUST AND CONDITIONAL ACCESS
IMPROVEMENTS ON ENDPOINTS

- **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.*)

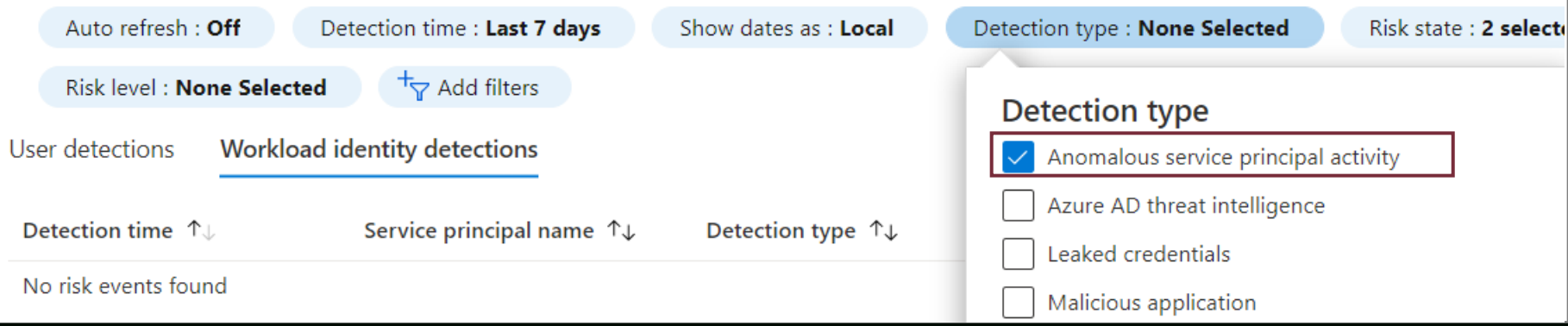
- **Intune Endpoint Privilege Management (part of Intune Premium)**
  - Manage and elevate standard users' permission to admin (to perform specific task)
  - For example, Install applications or peripheral devices (e.g. printers)

ZERO TRUST AND CONDITIONAL ACCESS
NEW IDENTITY PROTECTION DETECTION TYPES!?

Human Identities



Workload Identities



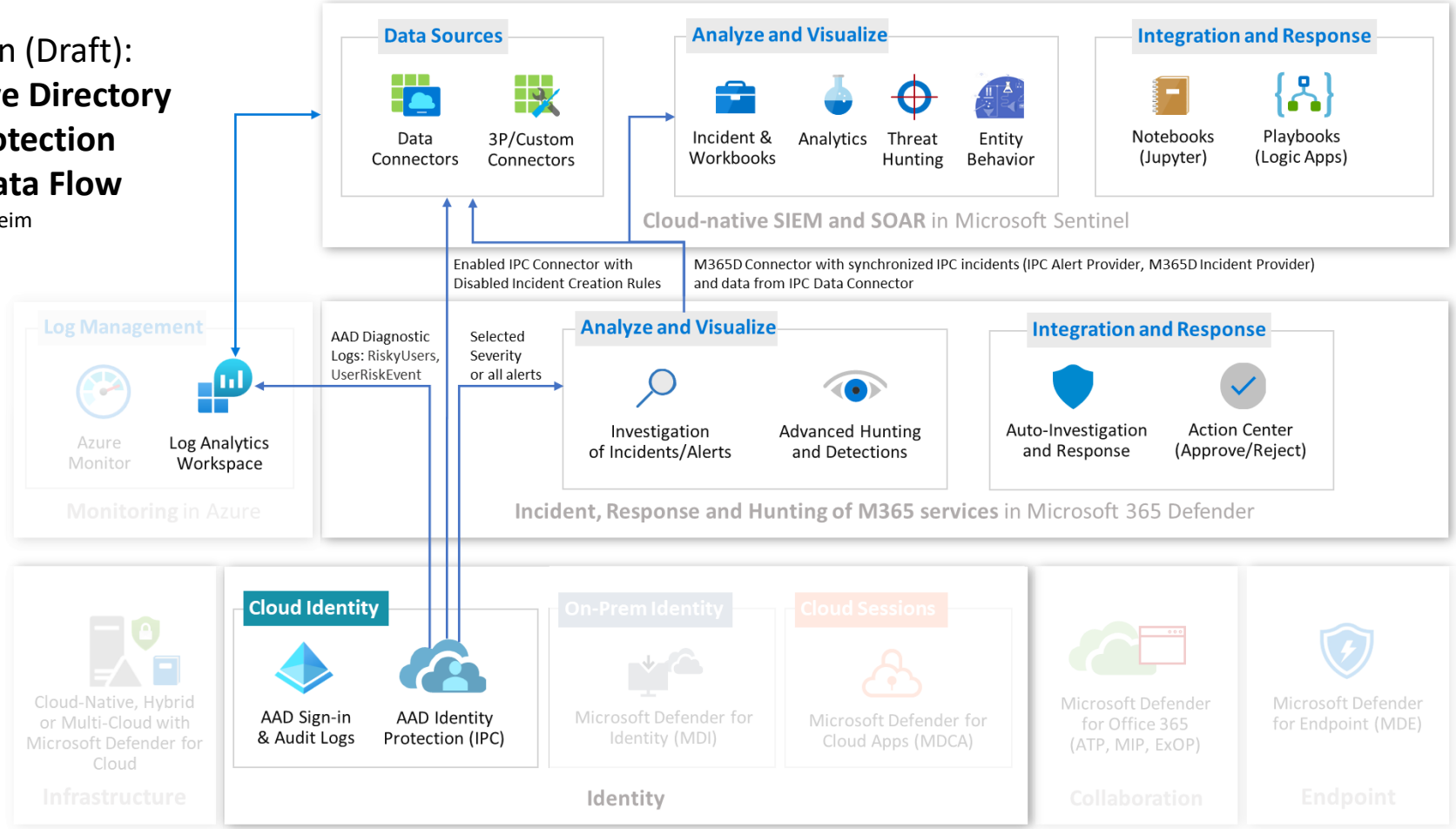
More Details: "Azure AD Identity Protection: Risk types and detection (Microsoft Docs)"

Authentication Strengths in Conditional Access

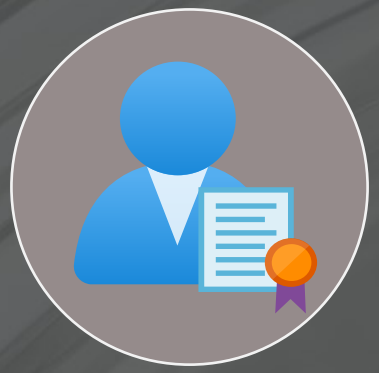
LIVE DEMO

ZERO TRUST AND CONDITIONAL ACCESS
IPC-INTEGRATION IN M365 DEFENDER PORTAL

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

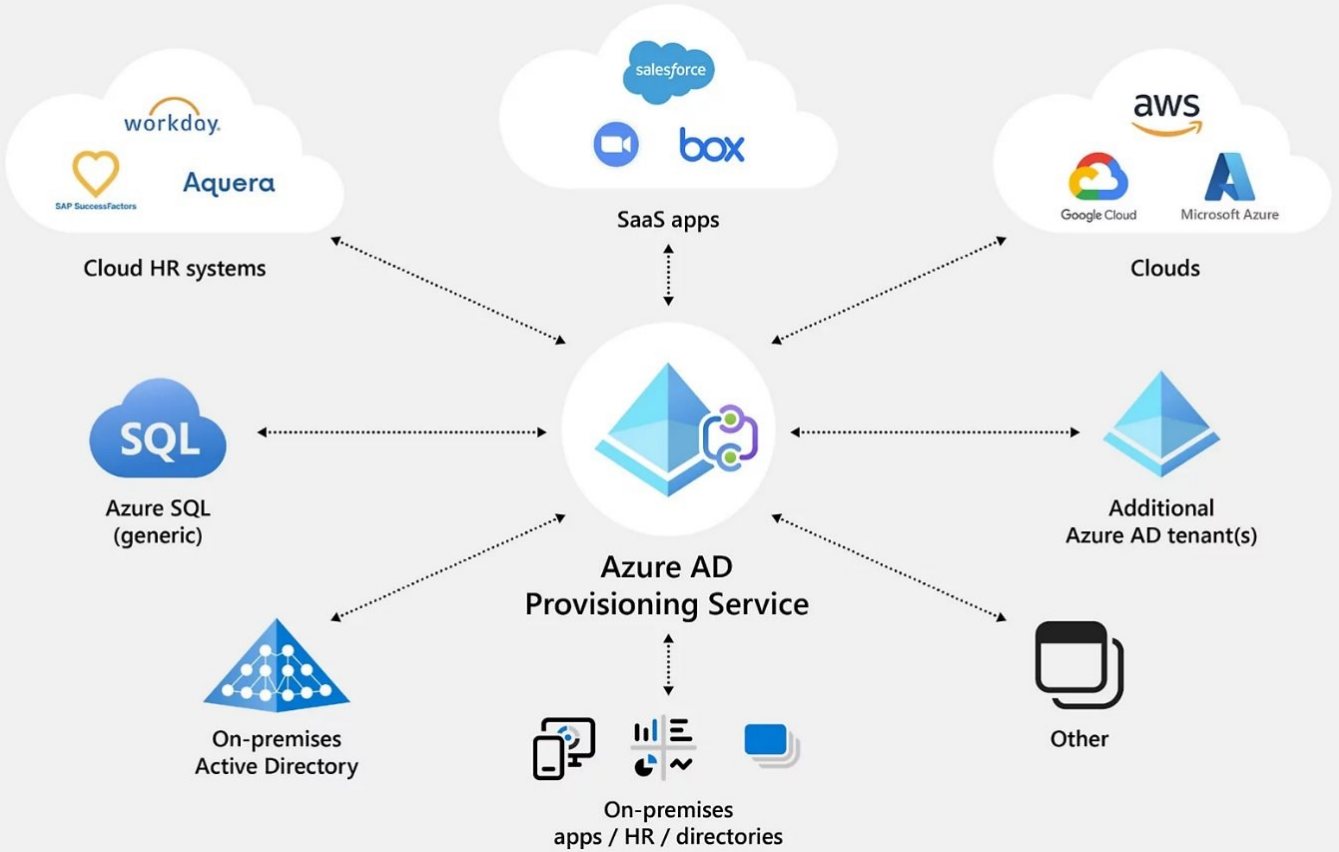


More Details: "Microsoft 365 Defender now integrates Azure Active Directory Identity Protection (Microsoft Docs)"



IDENTITY LIFEYCLE & GOVERNANCE

MICROSOFT ENTRA IDENTITY GOVERNANCE
IN PUBLIC PREVIEW

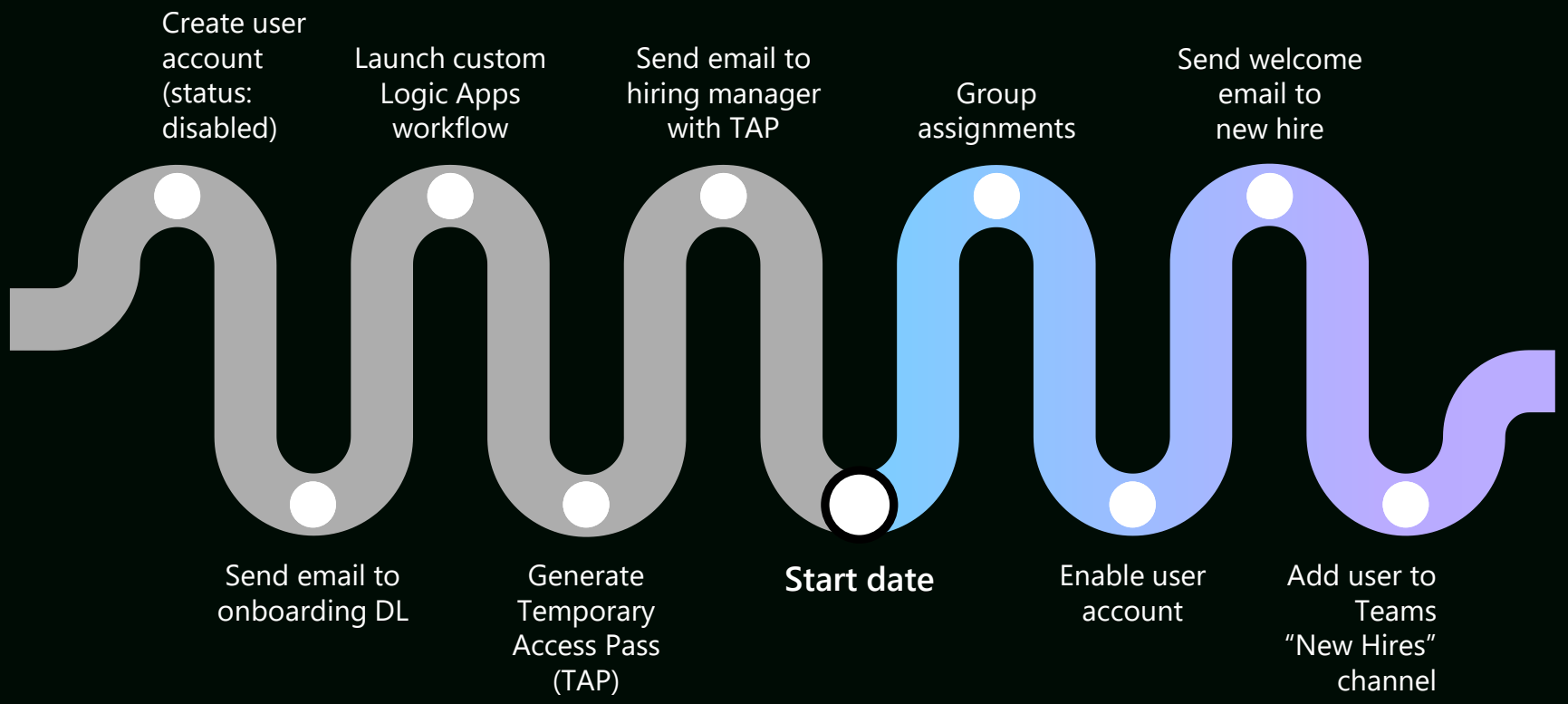


Source: "Microsoft Entra Identity Governance (Product page)"

Session: "Automate your complex user lifecycle processes with Azure AD Lifecycle Workflows and its extensibility capabilities to integrate custom logic and external systems"

IDENTITY LIFECYCLE & GOVERNANCE

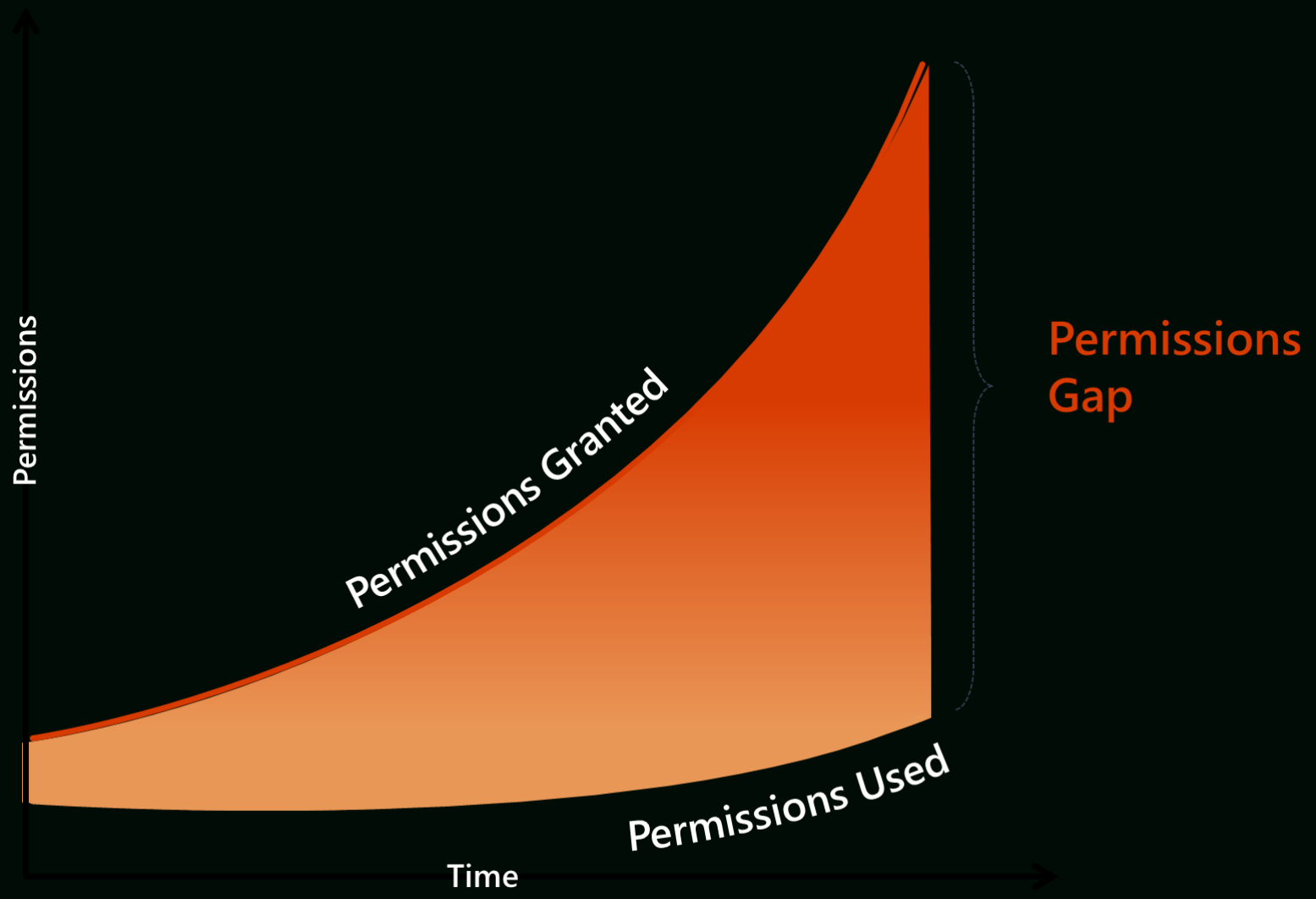
LIFECYCLE WORKFLOWS



Session: "Automate your complex user lifecycle processes with Azure AD Lifecycle Workflows and its extensibility capabilities to integrate custom logic and external systems"

IDENTITY LIFECYCLE & GOVERNANCE

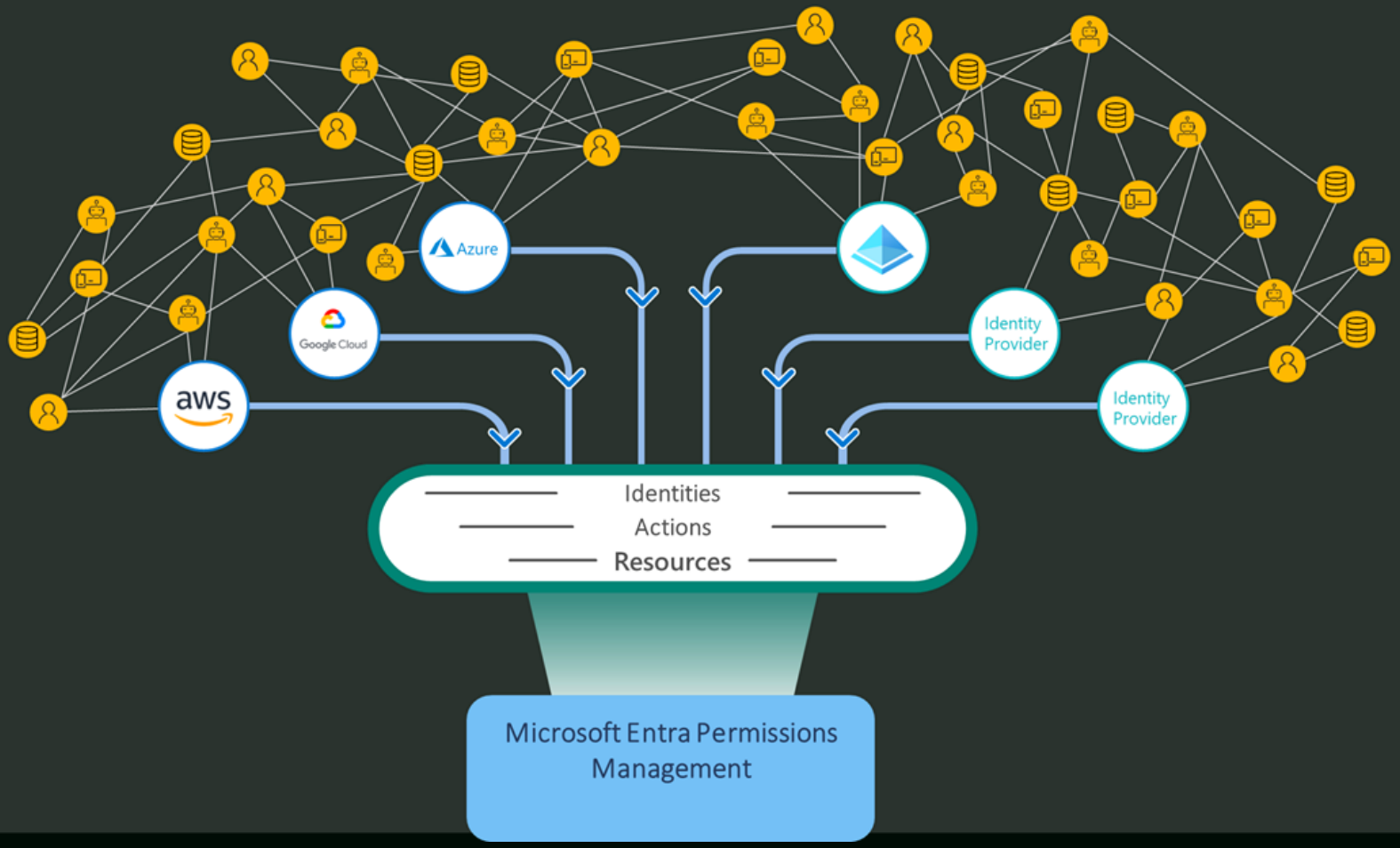
PERMISSIONS MANAGEMENT



Session: “How to achieve zero standing privileges in multicloud”

IDENTITY LIFECYCLE & GOVERNANCE

PERMISSIONS MANAGEMENT IN MULTI-CLOUD ENVIRONMENTS



Session: "How to achieve zero standing privileges in multicloud"

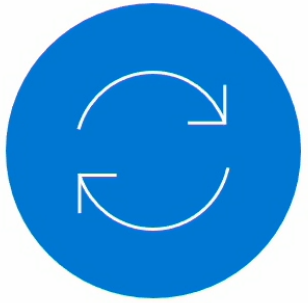
Identity Workflows and Entra Permissions Management

LIVE DEMO

SECURING DEVOPS WORKLOAD IDENTITIES

SECURING WORKLOAD IDENTITIES
ANNOUNCEMENTS

Challenges of securing workload identities



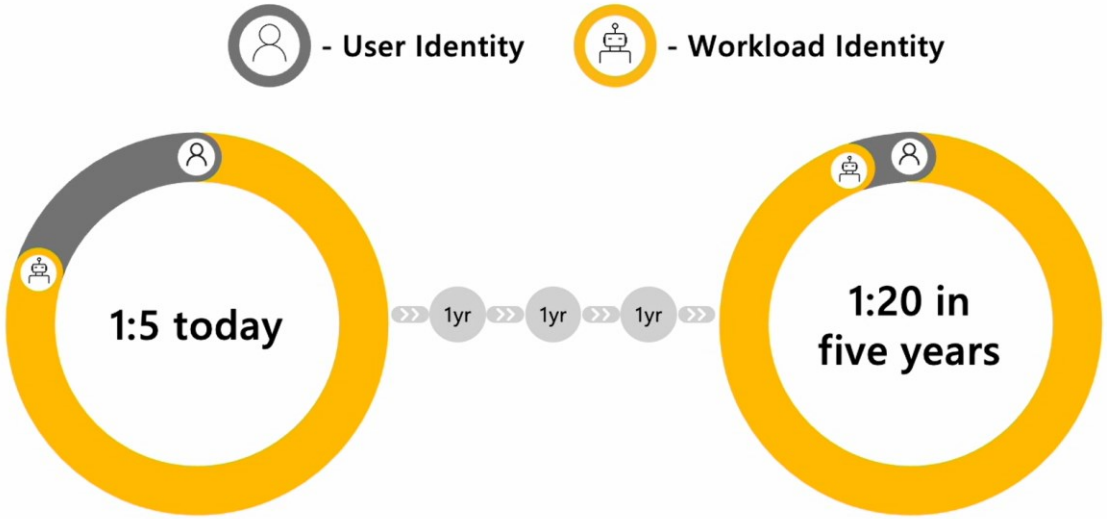
No defined joiner/mover/leaver lifecycle to manage

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



Source: Microsoft Security internal research 2021

Source: Session "Introducing Microsoft Entra Workload Identities"

SECURING WORKLOAD IDENTITIES
ANNOUNCEMENT

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

Source: Session "Introducing Microsoft Entra Workload Identities"

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**

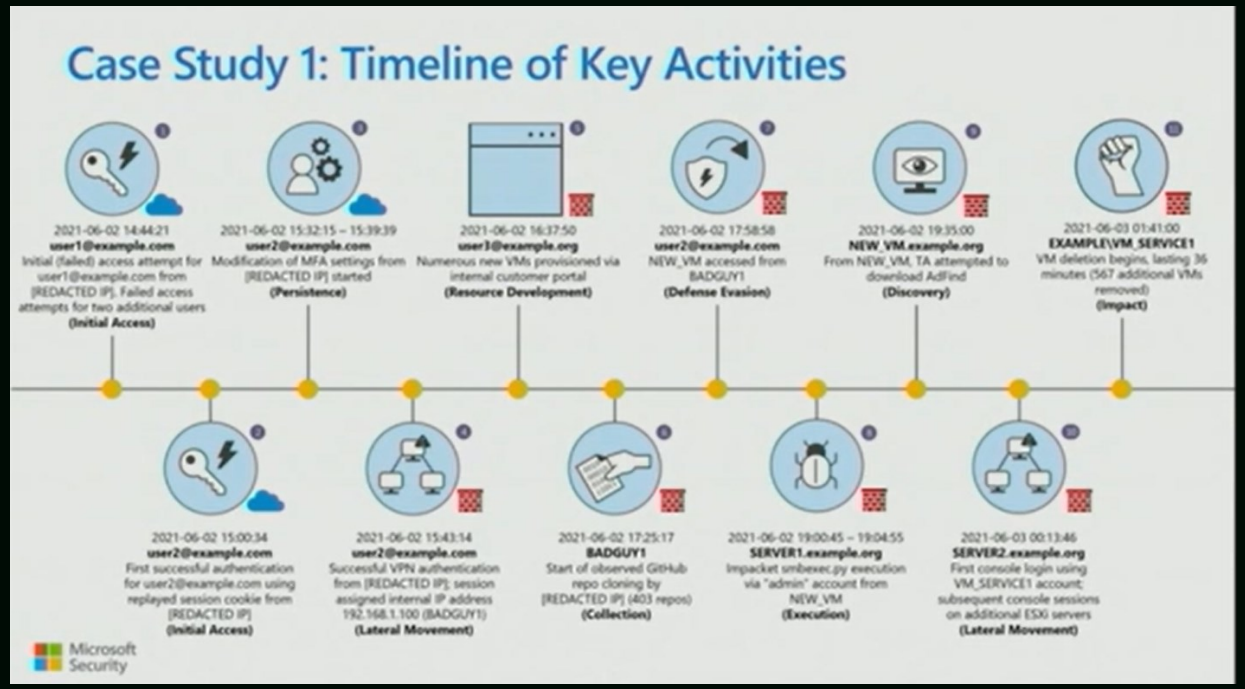
Source/more Details: "Overview of Defender for DevOps (Microsoft Docs)"

Microsoft Entra Workload Identities Security Attack Explorer

LIVE DEMO

MICROSOFT SECURITY
RECOMMENDED SESSION

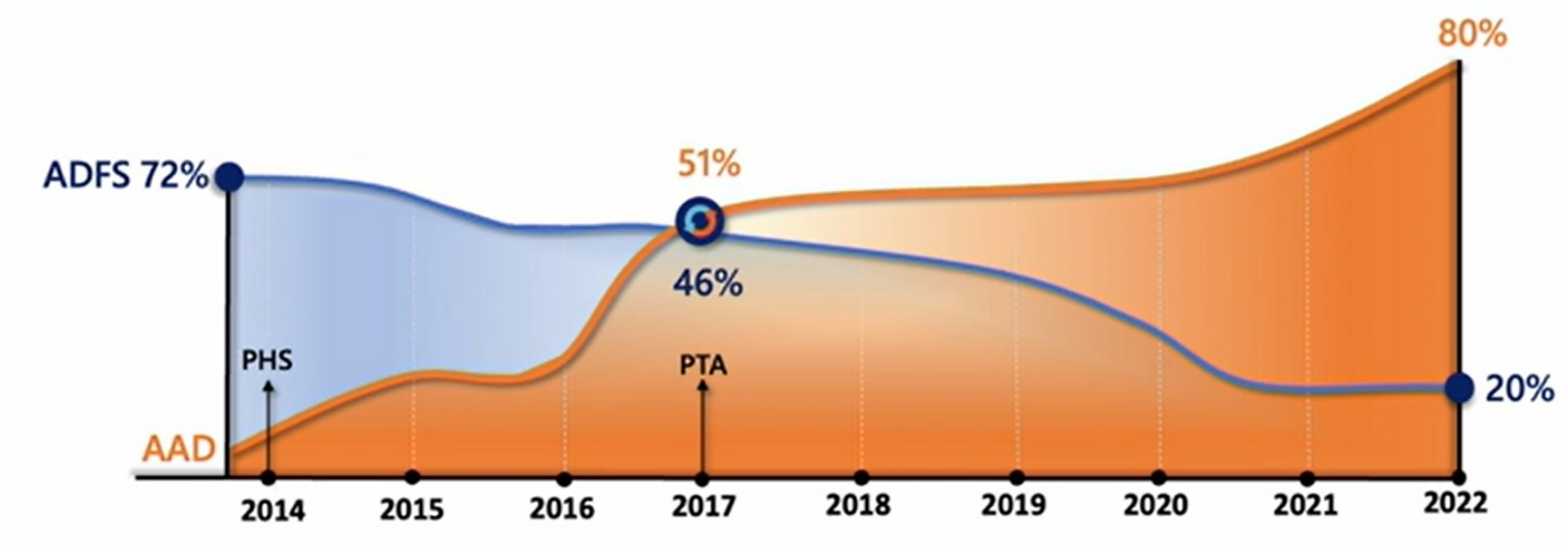
- **Stories from DART: <u>Taking the ware out of ransomware</u>**



MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

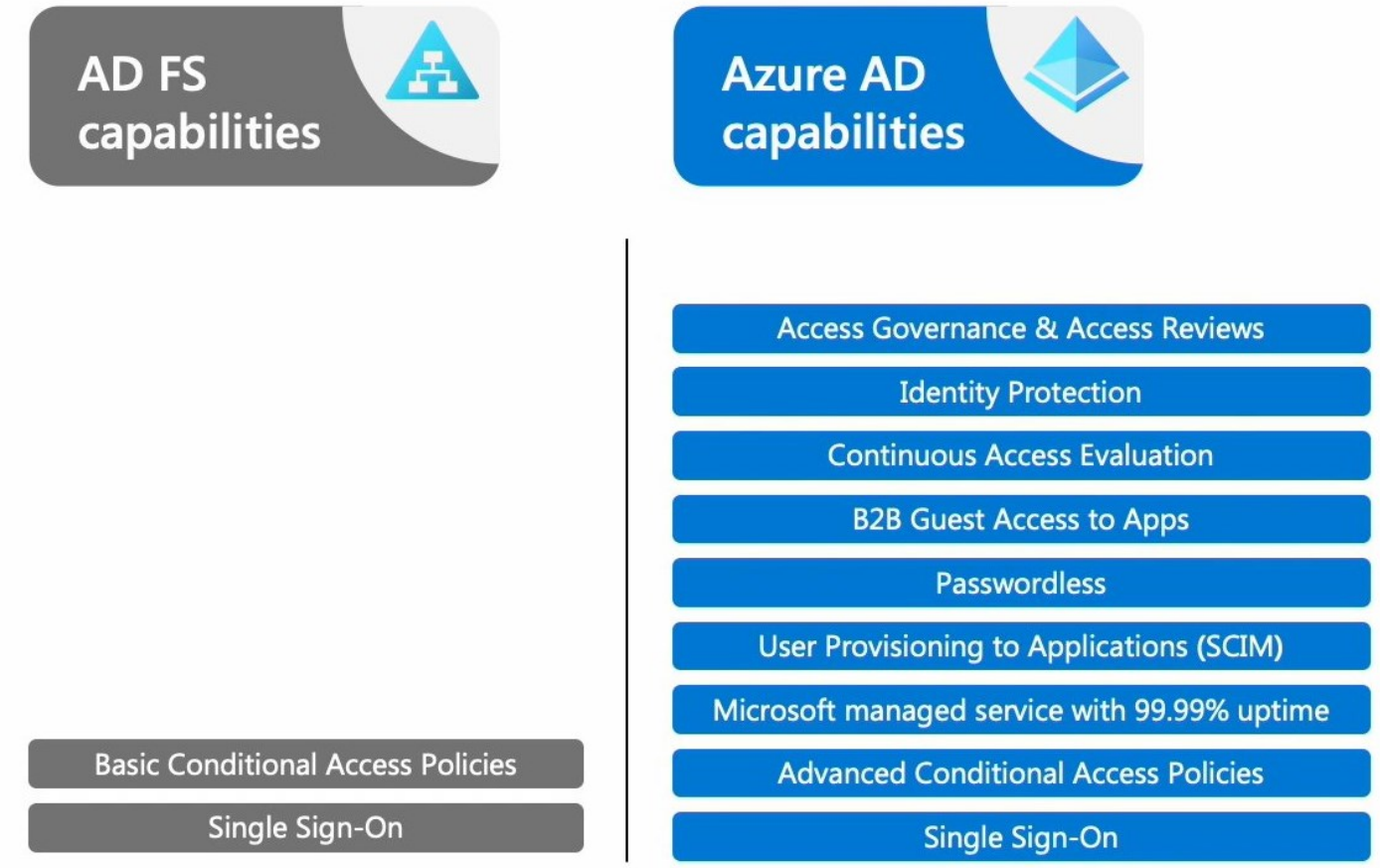
MIGRATING ADFS APPS TO AZURE AD



Source: Session "Migrating ADFS apps to Azure AD"

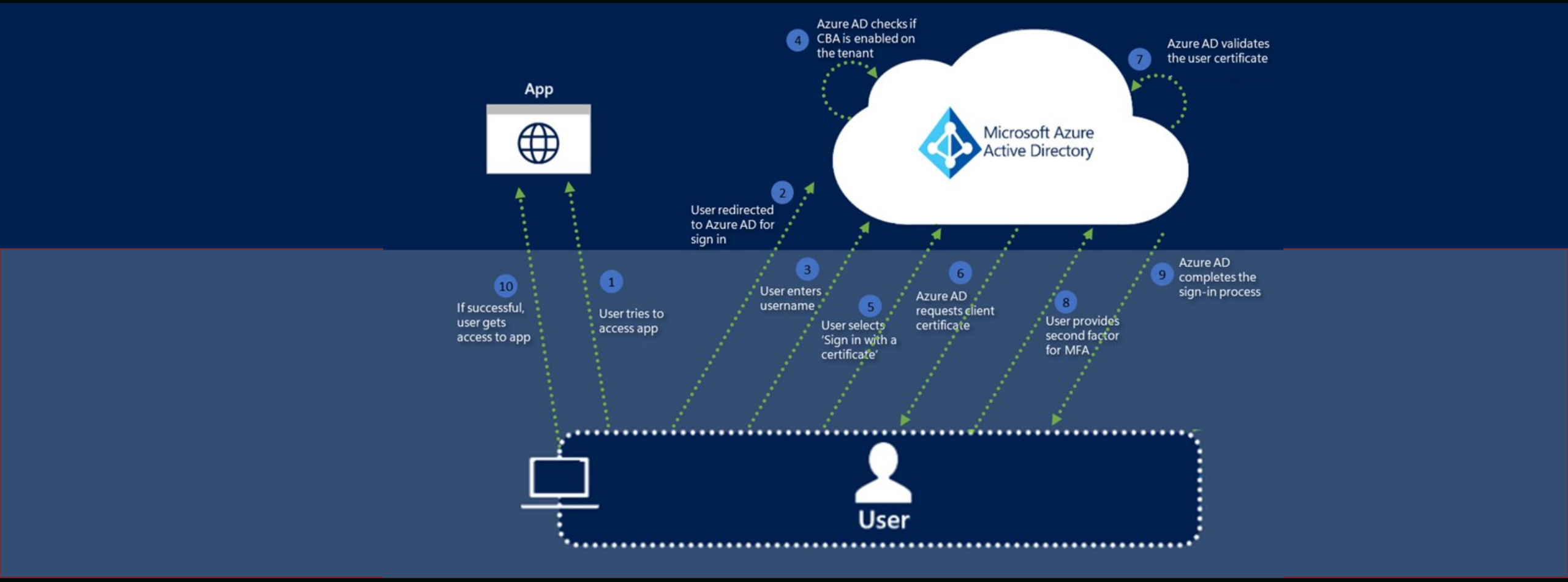
MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

BEYOND AD FS: CAPABILITIES IN AZURE AD



Source: Session "Migrating ADFS apps to Azure AD"

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



Source/More details: "Azure AD certificate-based authentication technical deep dive"

THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net