



# WHAT'S NEW IN MICROSOFT ENTRA?

## ANNOUNCEMENTS FROM THE RECENT MONTHS

**FOLLOW US ON TWITTER / OUR HASHTAG**

# #AZUREBONN



# CLOUD IDENTITY SUMMIT '23

Koblenz, Germany

Thu, September 7th, 2023

[www.identitysummit.cloud](http://www.identitysummit.cloud)

Supported by



Community Event by



Sponsored by



glueckkanja■gab

# RECENT EVENTS & ANNOUNCEMENTS

## Microsoft Secure

Virtual  
April 13, 2023

# RECENT EVENTS & ANNOUNCEMENTS



RSA Conference (RSAC)  
San Francisco  
Apr. 24 - 27, 2023



Microsoft Build  
Seattle  
May 23 - 25, 2023

A screenshot of the "What's new in Azure Active Directory" article on the Microsoft Learn website. The page includes a sidebar with navigation links like "Fundamentals documentation", "Overview", "First steps", and "Users, groups, and licenses". The main content area discusses recent improvements in Azure AD, including what's new in Azure Active Directory, deprecated features, and archive information. It also provides instructions for staying updated via RSS feed.

Feature Announcements  
Blog / Microsoft Learn  
Continuous

# UPDATES IN THE RECENT MONTHS @MICROSOFT IDENTITY + SECURITY



MICROSOFT ENTRA  
EXTERNAL ID



MICROSOFT ENTRA  
VERIFIED ID



MICROSOFT AZURE  
ACTIVE DIRECTORY  
FOR WORKFORCE



MICROSOFT SECURITY  
SOLUTIONS



# MICROSOFT ENTRA EXTERNAL ID

# MICROSOFT ENTRA EXTERNAL ID

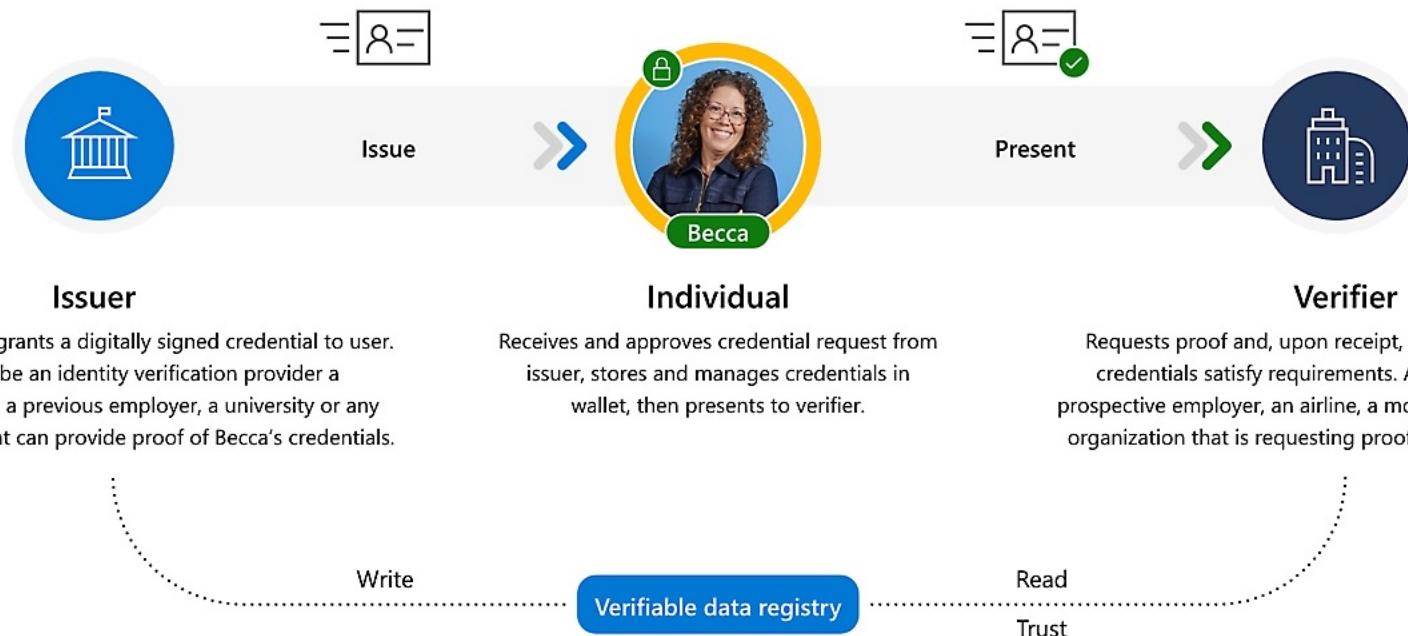


**Siobhan Power**  
Microsoft Program Manager (CxE)



# MICROSOFT ENTRA VERIFIED ID

# WHAT IS MICROSOFT ENTRA VERIFIED ID?



# Onboarding and Entitlement Management with Verified ID

LIVE DEMO

# USE CASE FOR B2E WORK VERIFICATION ON LINKEDIN



## Thomas Naunheim

Cyber Security Architect | Microsoft Security MVP | Community Speaker and Blogger

Coblenz, Rhineland-Palatinate, Germany · [Contact info](#)

6,237 followers · 500+ connections

[Open to](#) [Add profile section](#) [More](#)



## Verifications



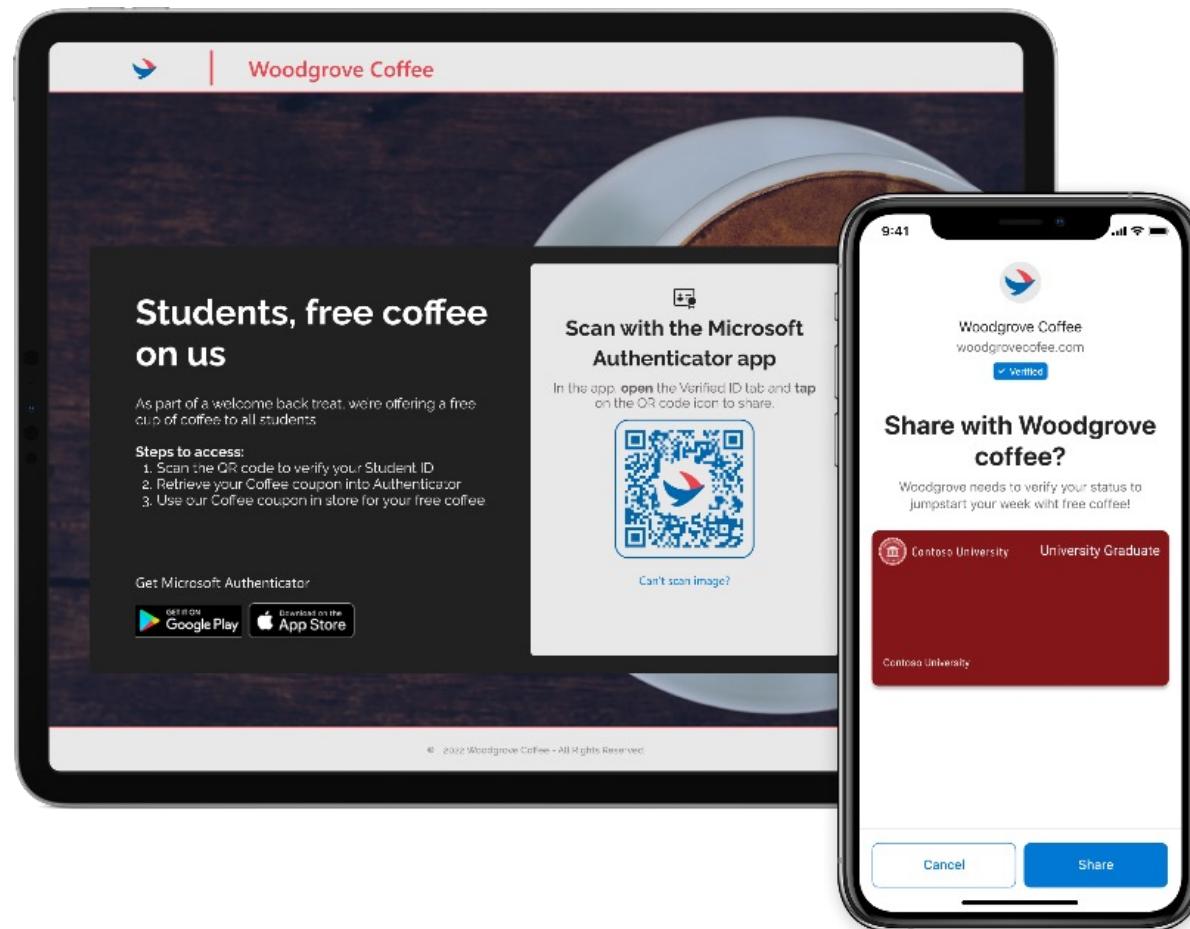
### Workplace

You've verified your workplace as glueckkanja-gab AG.

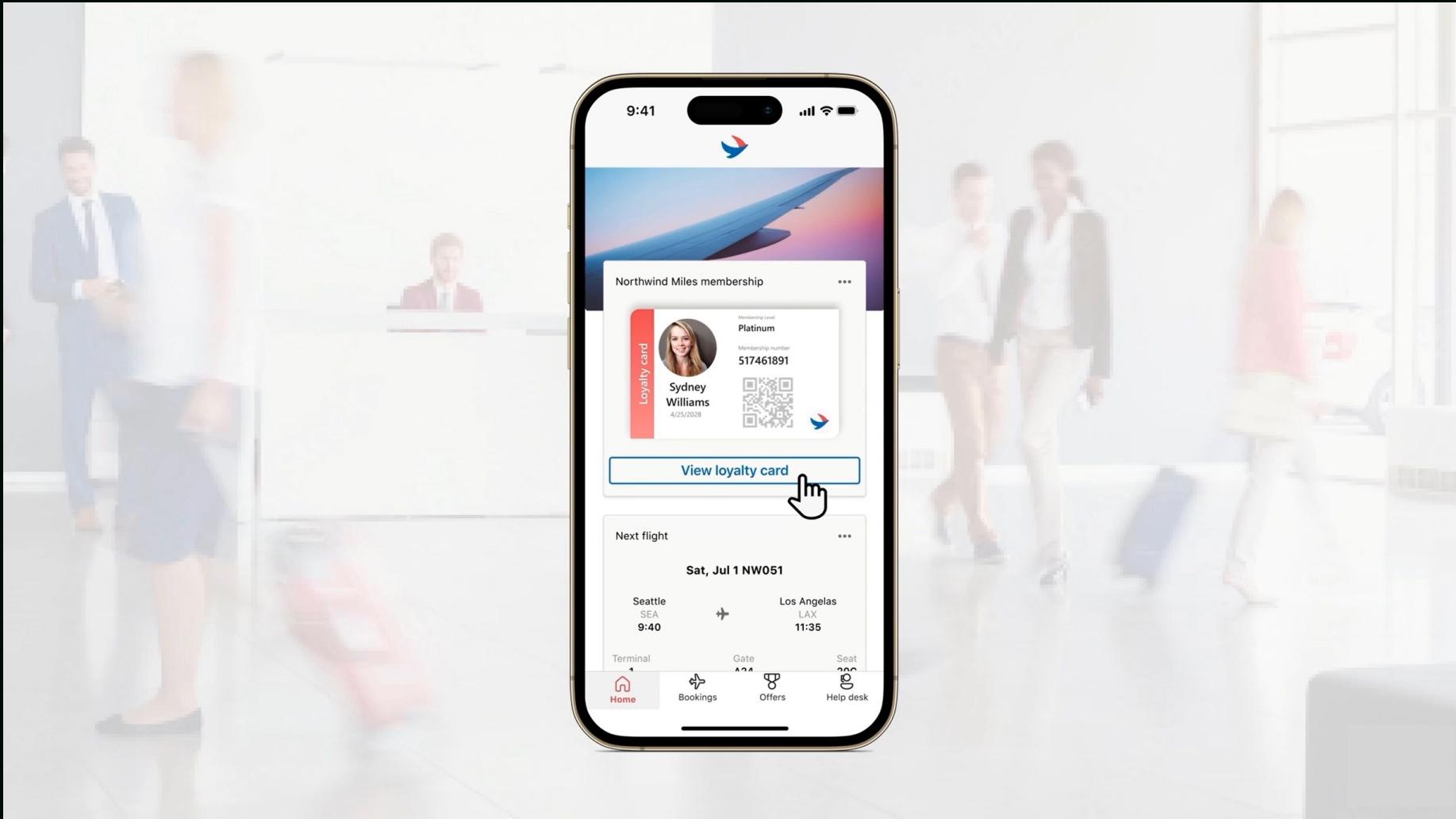
Show verifications →

- [LinkedIn and Microsoft Entra introduce a new way to verify your workplace](#)
- [Microsoft Learn: Setting up LinkedIn workplace verification](#)

# USE CASE FOR B2C: LOYALTY / CUSTOMER CARD

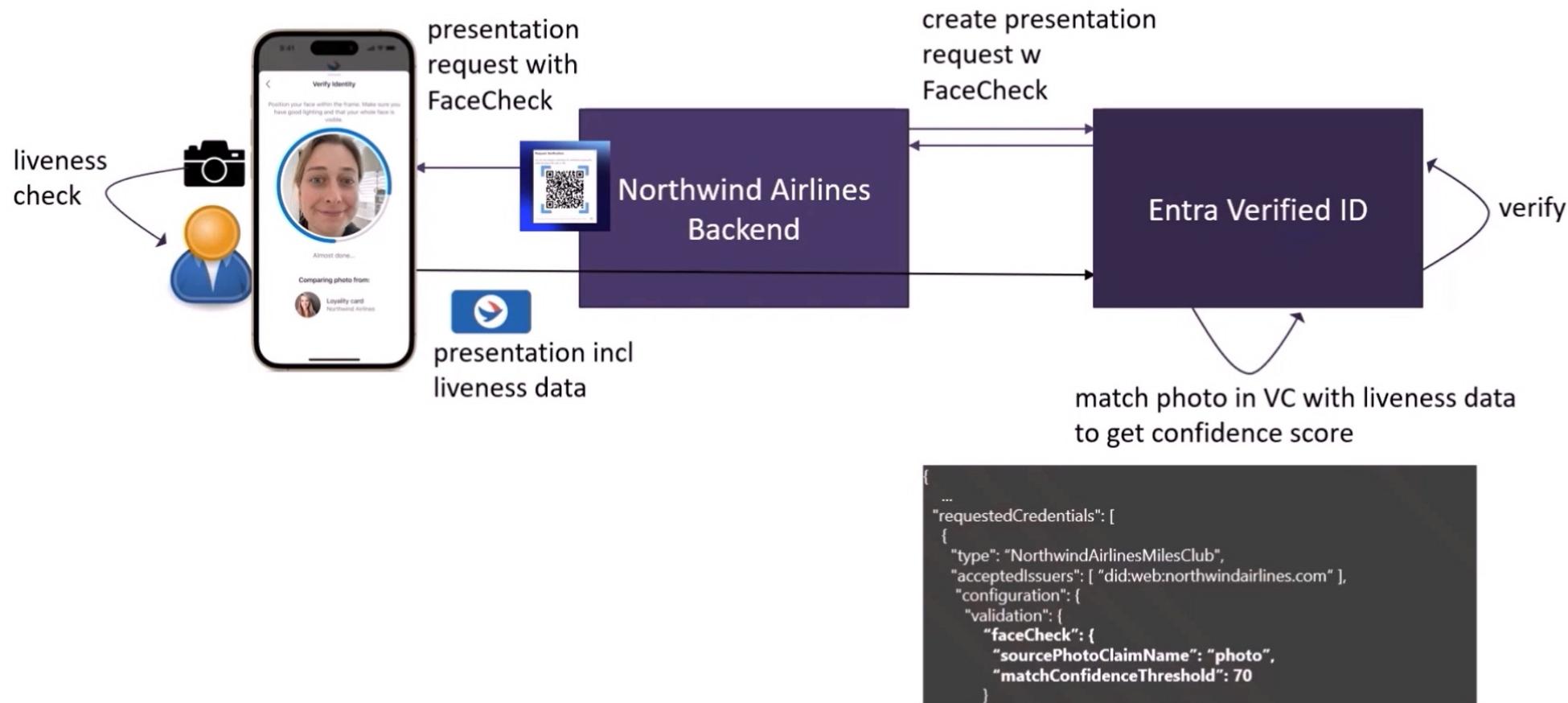


# USE CASE FOR B2C: IN-APP WALLET



Source/more details: "[Reduce fraud and improve engagement using Digital Wallets | OD30](#)"

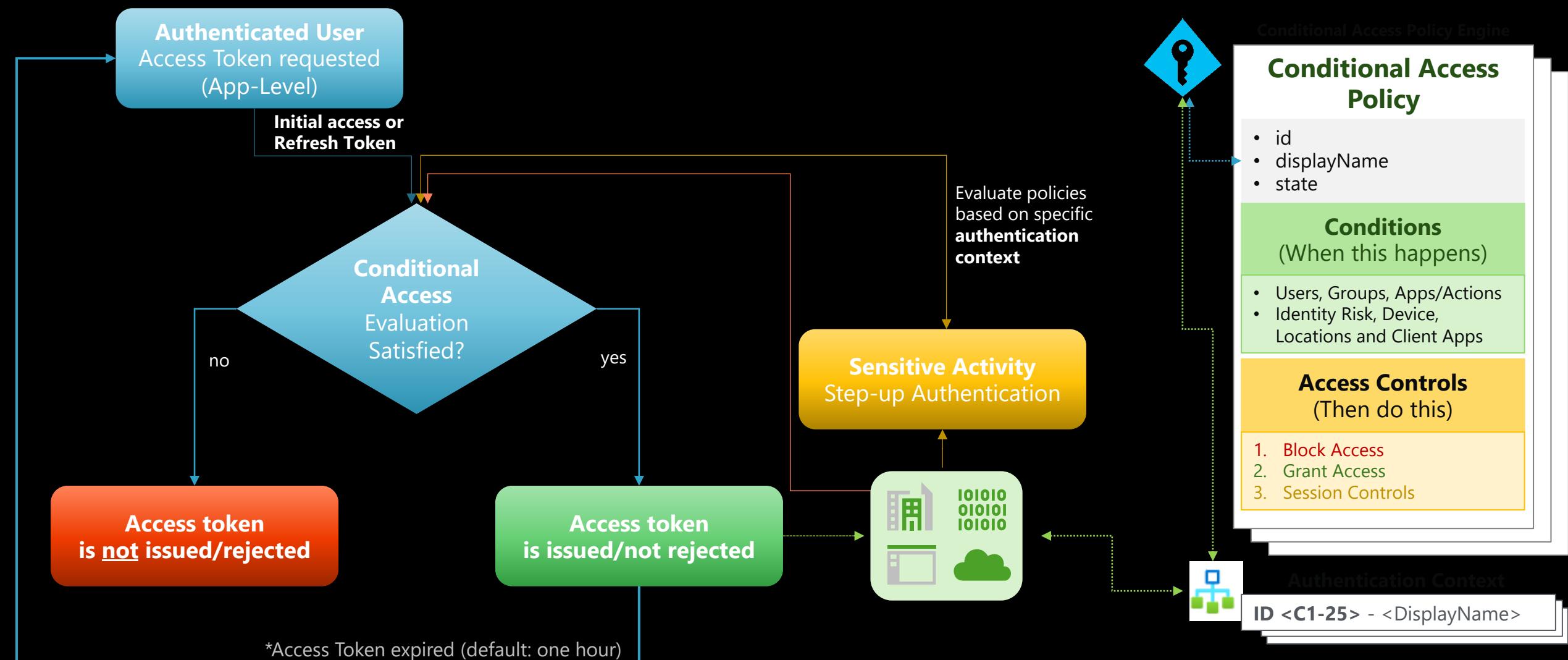
# MICROSOFT ENTRA VERIFIED ID FACE CHECK FOR STEP-UP VERIFICATION





# MICROSOFT AZURE ACTIVE DIRECTORY

# MICROSOFT AZURE ACTIVE DIRECTORY AUTHENTICATION CONTEXT



# MICROSOFT AZURE ACTIVE DIRECTORY AUTHENTICATION CONTEXT IN “PROTECTED ACTIONS”

The screenshot shows the 'Protected actions' section of the Azure Active Directory Roles and administrators interface. The left sidebar includes links for All roles, Protected actions (which is selected and highlighted in grey), Diagnose and solve problems, Activity, Access reviews, Audit logs, Troubleshooting + Support, and New support request. The main content area has a heading 'Protected actions are role permissions with Conditional Access applied for added security. Conditional Access requirements are enforced when a user performs the protected action.' Below this is a 'Learn more' link and a search bar. A table lists three actions found:

Permission	Description	Conditional Access authentication context
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties for conditional access policies	Trusted SAW Device
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/create	Create conditional access policies	Trusted SAW Device
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/delete	Delete conditional access policies	Trusted SAW Device

# MICROSOFT AZURE ACTIVE DIRECTORY AUTHENTICATION CONTEXT IN PIM

The screenshot shows the 'Edit role setting - Global Administrator' page in the Microsoft Azure Active Directory Privileged Identity Management (PIM) interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for thomas@cloud-architek... (CLOUDLAB (CLOUD-ARCHITEKT...)). The breadcrumb navigation shows the path: ... > CloudLab | Roles > Global Administrator | Assignments > Role setting details - Global Administrator >. The left sidebar contains icons for various Azure services: +, Home, Key Vault, Active Directory, Azure AD roles, Azure AD users, Groups, Conditional Access, Azure AD B2B, Azure AD B2C, Azure AD SSO, and Azure AD Connect.

The main content area displays the 'Activation' tab selected. It includes the following settings:

- Activation maximum duration (hours):** A slider set to 8 hours.
- On activation, require:** A radio button group where 'Azure AD Conditional Access authentication context' is selected (indicated by a blue dot).
- Learn more:** A link to 'Require Authorized FIDO2'.
- Checklist:** Options include 'Require justification on activation' (checked), 'Require ticket information on activation' (unchecked), and 'Require approval to activate' (unchecked).
- Select approver(s):** A section showing 'No approver selected' with a '+' button.

# MICROSOFT AZURE ACTIVE DIRECTORY SECURITY GROUPS IN PIM

The screenshot shows the Microsoft Azure Active Directory Privileged Identity Management (PIM) Groups settings page. The URL in the browser is [https://portal.azure.com/#blade/Microsoft\\_Azure\\_PIM/GroupsBlade/RoleSettingDetails/Member](#). The page title is "Edit role setting - Member". The left sidebar has icons for Home, Groups, Conditional Access, Identity Governance, and more. The main content area shows the "Activation" tab selected. It includes a slider for "Activation maximum duration (hours)" set to 8, and options for "On activation, require" (None, Azure MFA, Azure AD Conditional Access authentication context, with the last one selected). A dropdown menu shows "Trusted Device". Below these are checkboxes for "Require justification on activation" (checked), "Require ticket information on activation" (unchecked), and "Require approval to activate" (unchecked). At the bottom, there's a "Select approver(s)" section with a note "No approver selected" and a plus sign icon.

# MICROSOFT AZURE + AZURE AD

## AZURE PIM ELIGIBLE ROLES

The screenshot illustrates the Microsoft Azure and Azure AD Privileged Identity Management (PIM) interface. It shows two overlapping Azure resource management pages:

- Top Window (Privileged Identity Management):** Shows the 'My roles | Azure resources' blade with 'Azure resources' selected. The main content area displays the 'aadops1-vm' virtual machine's Access control (IAM) settings. The 'Access control (IAM)' blade is open, showing 'View my access' and 'Check access' sections. The 'Role assignments' section lists four roles: Contributor, NetOps, Owner, and SecOps (which is checked). The 'Eligible assignments' tab is selected, and the 'Activate role' button is highlighted with a red box.
- Bottom Window (Standard Resource Management):** Shows the 'Virtual machines > aadops1-vm' blade. The 'Access control (IAM)' section is also visible here, showing the same list of roles and the 'Eligible assignments' tab.

**assignments - aadops1-vm**

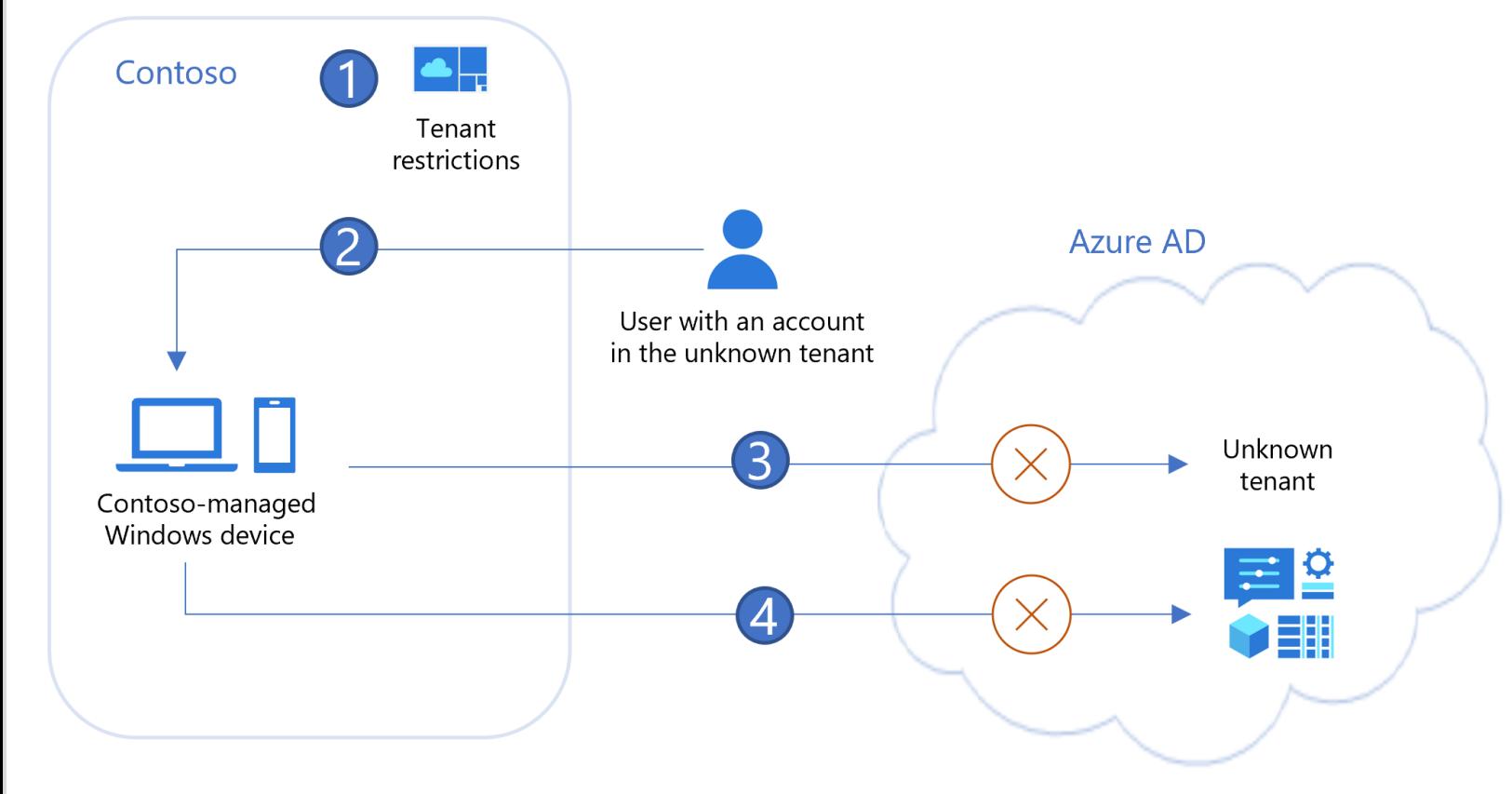
Role	Scope	Membership	End time
Contributor	Management group (Inherited)	Inherited	Permanent
NetOps	Management group (Inherited)	Inherited	Permanent
Owner	Management group (Inherited)	Inherited	Permanent
<input checked="" type="checkbox"/> SecOps	Management group (Inherited)	Inherited	Permanent

# Authentication Context in Azure (AD) PIM

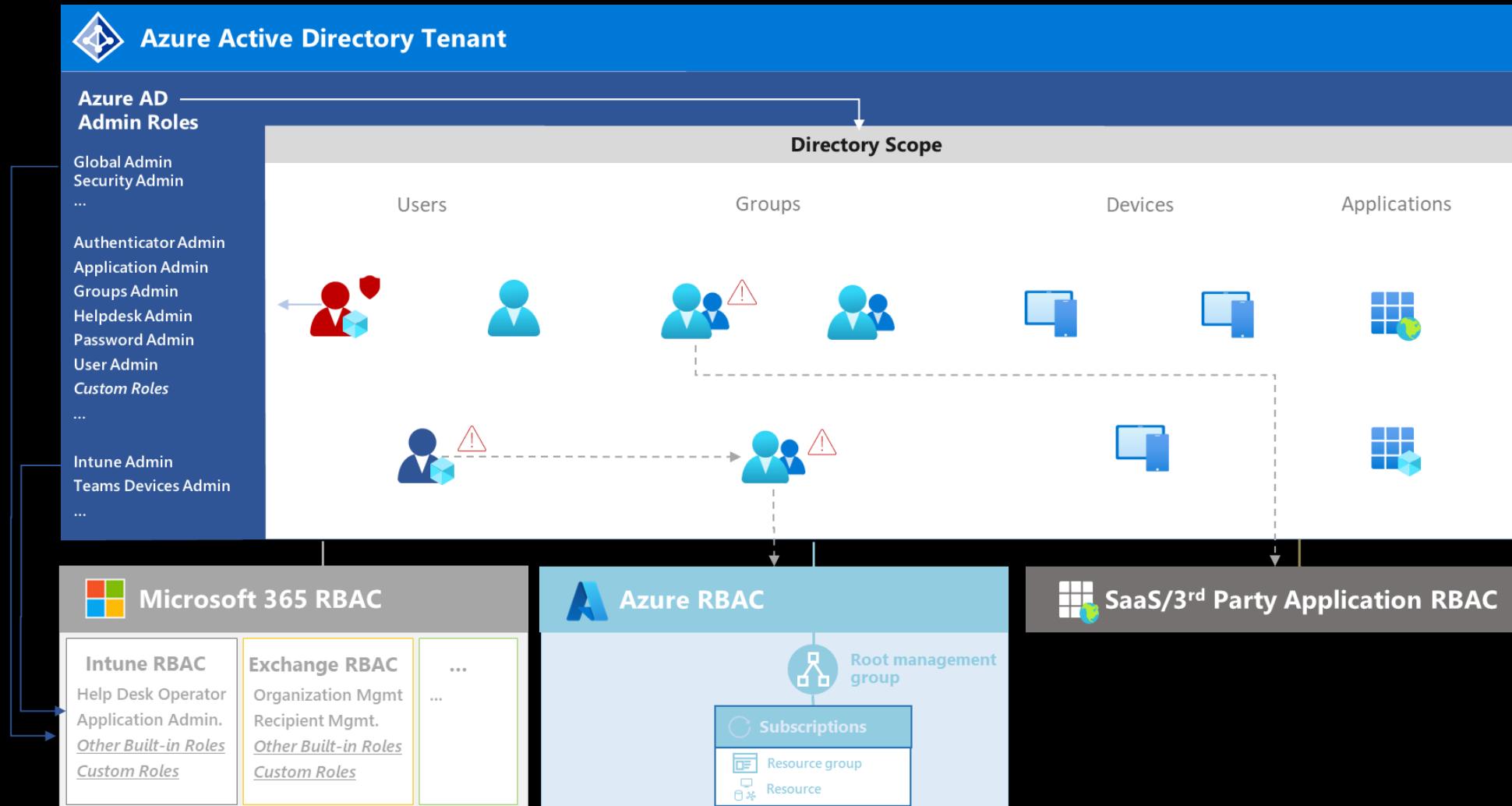
LIVE DEMO

# MICROSOFT AZURE ACTIVE DIRECTORY TENANT RESTRICTION V2

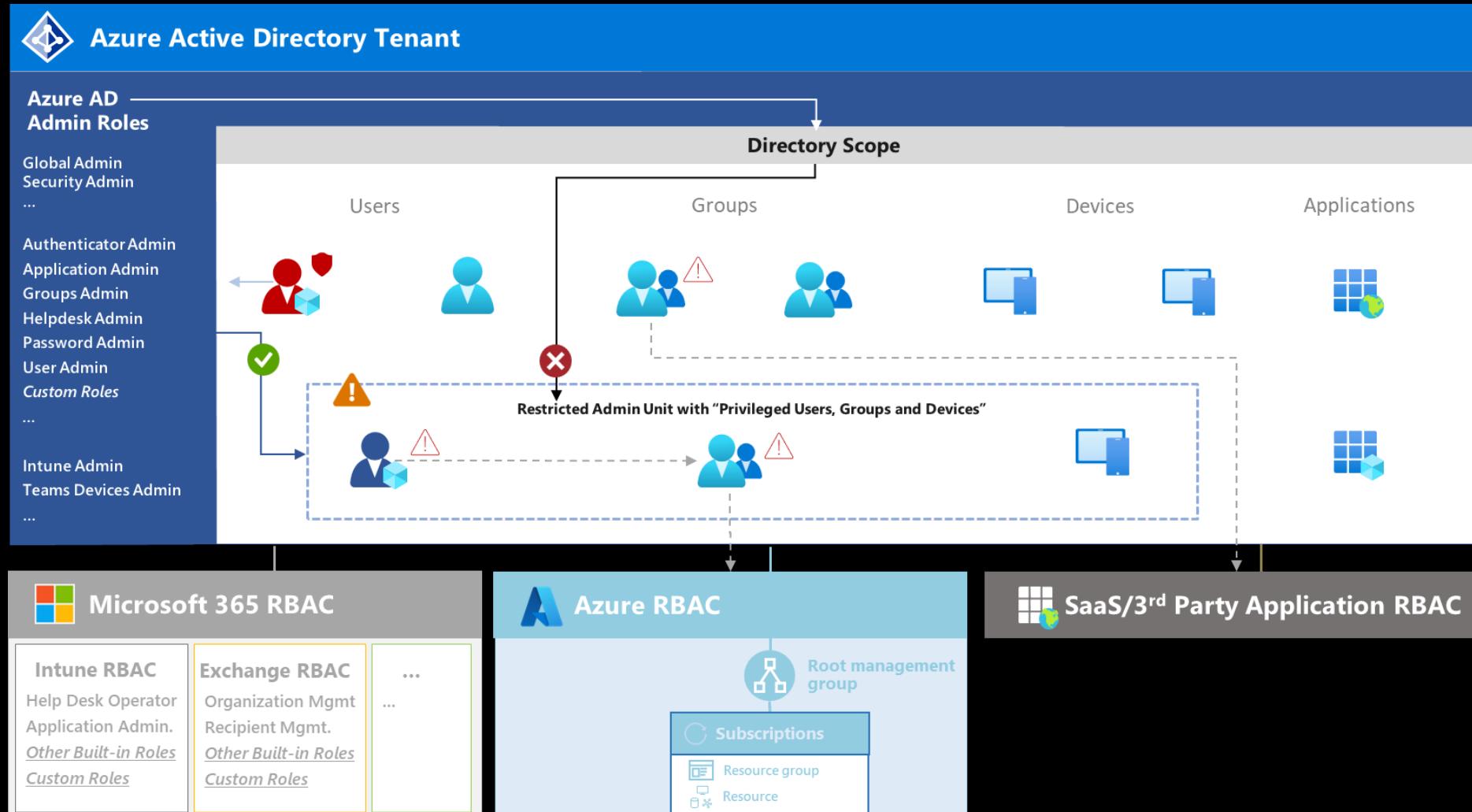
## Overview: Tenant restrictions V2



# MICROSOFT AZURE ACTIVE DIRECTORY ADMINISTRATIVE UNITS



# MICROSOFT AZURE ACTIVE DIRECTORY RESTRICTED MANAGEMENT ADMINISTRATIVE UNITS

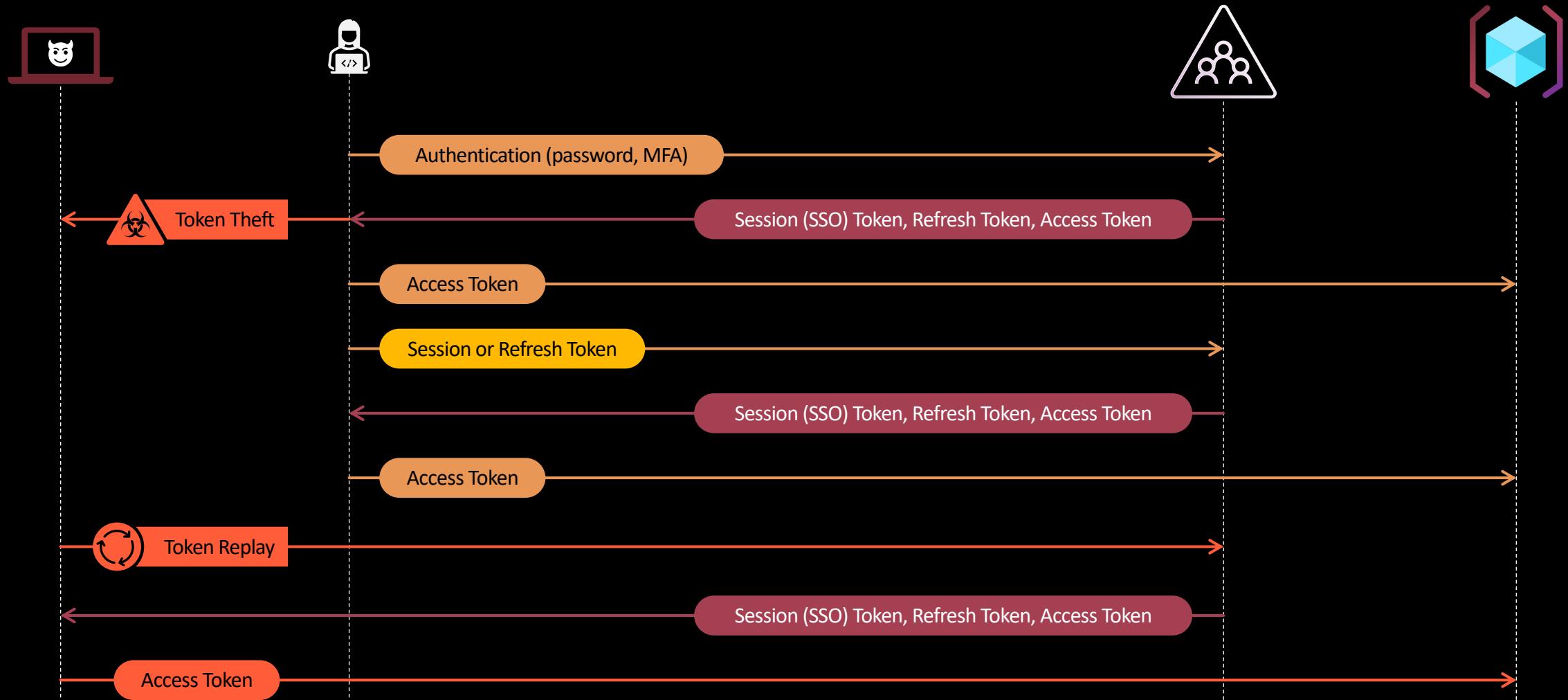


# MICROSOFT AZURE ACTIVE DIRECTORY TOKEN PROTECTION

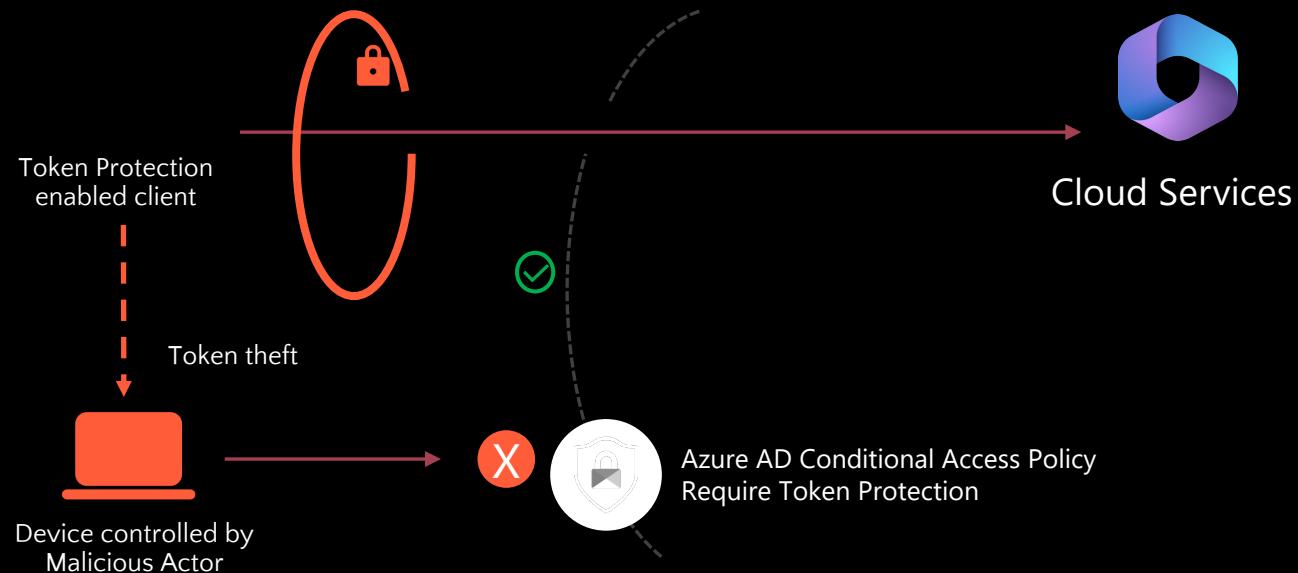


Attackers ❤️ Cookies  
and Tokens

# MICROSOFT AZURE ACTIVE DIRECTORY TOKEN PROTECTION



# MICROSOFT AZURE ACTIVE DIRECTORY TOKEN PROTECTION



# MICROSOFT AZURE + AZURE AD POWERSHELL & AZURE CLI WAM SUPPORT

```
1 # Enable WAM for Azure CLI
2 az config set core.allow_broker = true
3 az account clear
4 az login
5
6 # Enable WAM for Azure PowerShell
7 Update-AzConfig -EnableLoginByWam $true
8 Connect-AzAccount
```

# AUTHENTICATION METHODS

## REPORT SUSPICIOUS ACTIVITY & SYSTEM-PREFERRED MFA

Dashboard > Authentication methods

### Authentication methods | Settings

CloudLab - Azure AD Security

» Got feedback?

#### Report suspicious activity

Allows users to report suspicious activities if they receive an authentication request that they did not initiate. This control is available when using the Microsoft Authenticator app and voice calls. Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they may be blocked.

Learn more [↗](#)

State \*

Enabled

Target \*

All users

Reporting code \*

0

#### System-preferred multifactor authentication

This setting designates whether the most secure multifactor authentication method is presented to users. Learn more [↗](#)

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time. Learn more [↗](#)

State

Microsoft managed

Include

Exclude

Target \*

All users

Save

Discard

### User-linked detections

#### Premium user risk detections

Risk detection	Detection type	Description
Possible attempt to access Primary Refresh Token (PRT)	Offline	This risk detection type is detected by Microsoft Defender for Endpoint (MDE). A Primary Refresh Token (PRT) is a key artifact of Azure AD authentication on Windows 10, Windows Server 2016, and later versions, iOS, and Android devices. A PRT is a JSON Web Token (JWT) that's specially issued to Microsoft first-party token brokers to enable single sign-on (SSO) across the applications used on those devices. Attackers can attempt to access this resource to move laterally into an organization or perform credential theft. This detection will move users to high risk and will only fire in organizations that have deployed MDE. This detection is low-volume and will be seen infrequently by most organizations. However, when it does occur it's high risk and users should be remediated.
Anomalous user activity	Offline	This risk detection baselines normal administrative user behavior in Azure AD, and spots anomalous patterns of behavior like suspicious changes to the directory. The detection is triggered against the administrator making the change or the object that was changed.
User reported suspicious activity	Offline	This risk detection is reported by a user who denied a multifactor authentication (MFA) prompt and <a href="#">reported it as suspicious activity</a> . An MFA prompt that wasn't initiated by the user may mean that the user's credentials have been compromised.

# Overview of Token Protection and Restricted AU Management

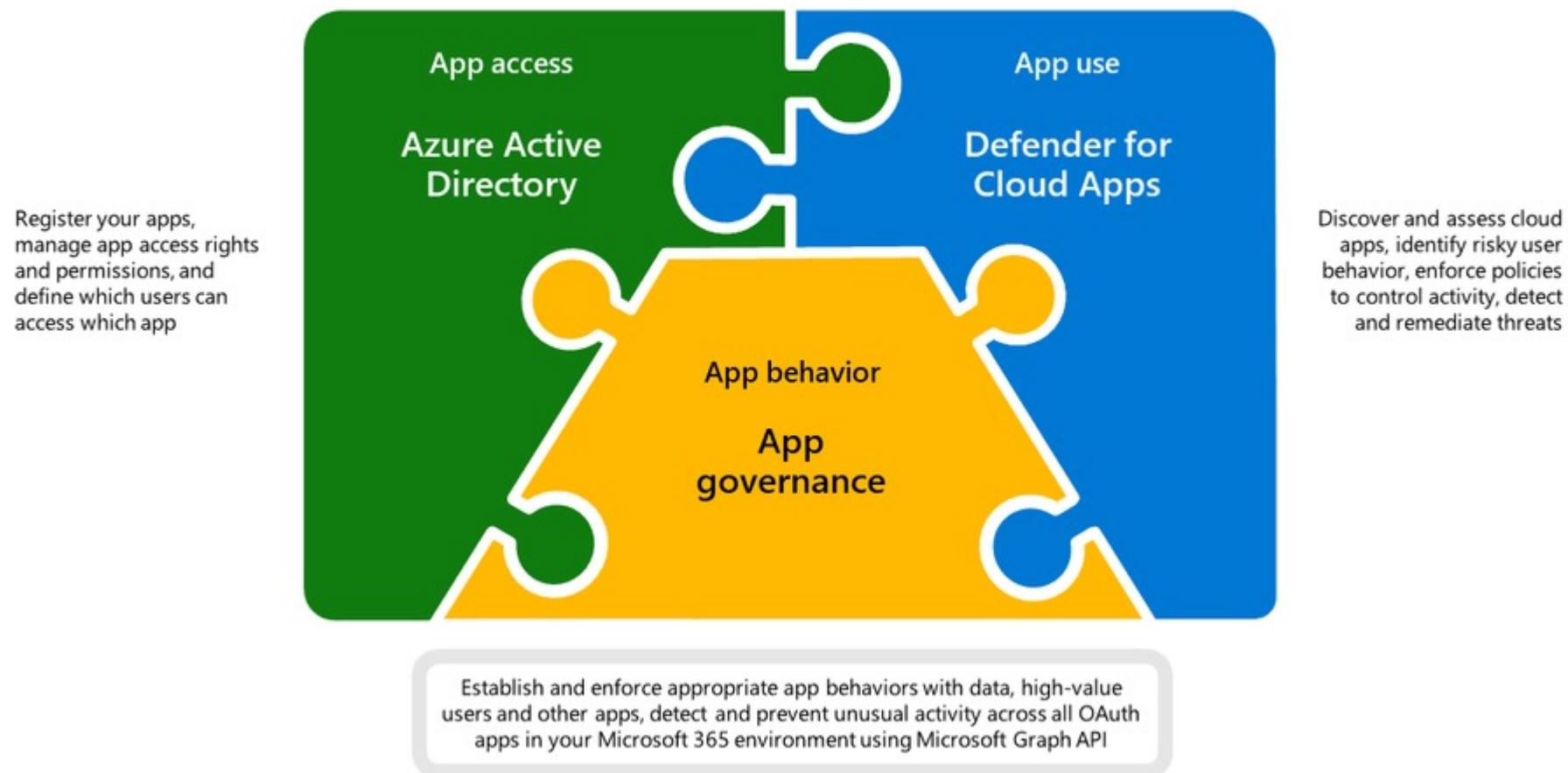
LIVE DEMO



# MICROSOFT SECURITY SOLUTIONS

# MICROSOFT SECURITY SOLUTIONS

## SECURING 3<sup>RD</sup> PARTY APPS



# MICROSOFT SECURITY SOLUTIONS

## APP GOVERNANCE

### RSA News: Taking XDR for SaaS apps to the next level - App Governance is now included in E5 Security

By  Caroline.Lee

Published Apr 25 2023 06:20 AM

12.9K Views

 Listen

Have you ever thought about how many apps you use daily? Or the apps that require you to sign in using your Microsoft credentials? The relationship between a user and an app has become instinctual. People often use apps without a second thought, unaware of the data that app is accessing on their behalf or what permissions they've just granted consent to. The rise of OAuth app based attacks has especially become more prominent through attacks like [consent](#) phishing or [OAuth app abuse](#). Combined with the existing challenge of navigating through the SaaS sprawl, organizations need security solutions that protect them from all facets without requiring extra tooling or personnel.

Because we are seeing a continued rise in app-based attacks, we believe this is a foundational capability for customers. That's why today, we are excited to announce that going forward the App Governance add-on will be included in Defender for Cloud Apps at no additional cost. **On June 1, 2023, new and existing customers will be able to start the opt-in process to begin using these capabilities.**

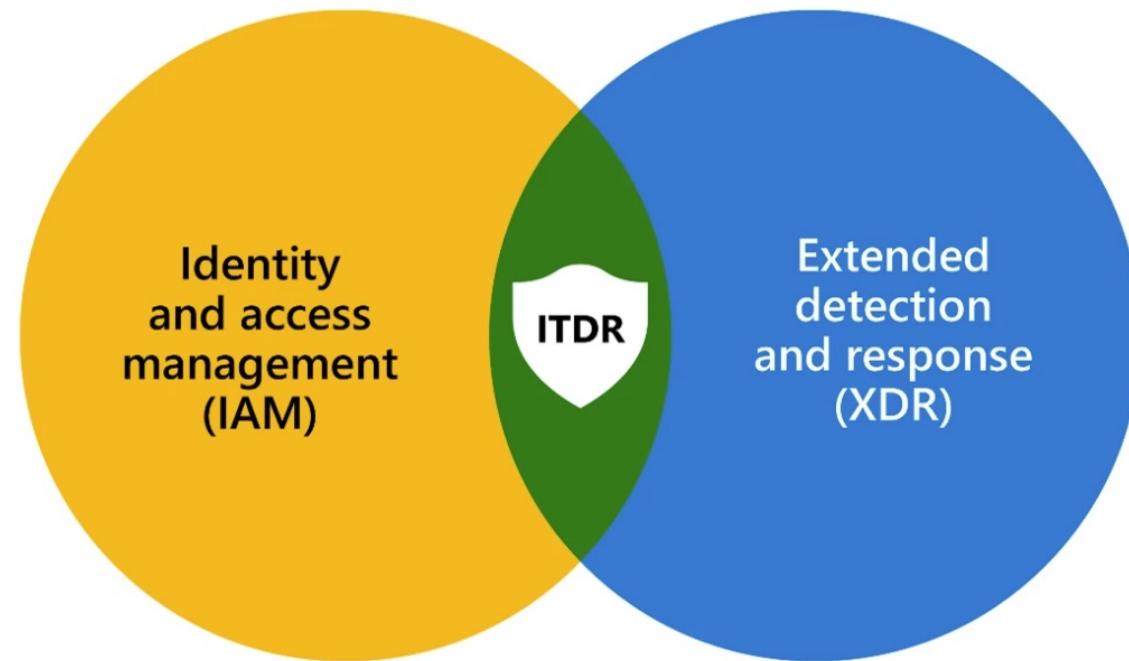
This means that all customers with a **standalone, E5 Security, or Microsoft 365 E5, or any other license that includes Defender for Cloud Apps**, will have access to [App Governance, at no additional cost](#). For existing App Governance customers, on June 1, depending on which channel you've purchased the licensing, we will either proactively cancel your subscription or manage the queue accordingly once a ticket is received. The change will have no effect on your current App Governance experience.

# MICROSOFT SECURITY SOLUTIONS

## IDENTITY THREAT DETECTION RESPONSE

**Microsoft is your partner for ITDR**

Leverage our expertise as a leader in both IAM and XDR



# MICROSOFT SECURITY SOLUTIONS

## IDENTITY THREAT DETECTION RESPONSE

Microsoft 365 Defender

- Home
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat intelligence
- Secure score
- Learning hub
- Trials
- Partner catalog
- Assets
- Devices
- Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Email & collaboration

**Home**

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Azure Active Directory Identity Protection.

**Deployment**

Your environment is not protected against identity related threats. It is highly recommended to deploy Defender for Identity and Azure AD Identity Protection.

**License**

Defender for Identity **Available**

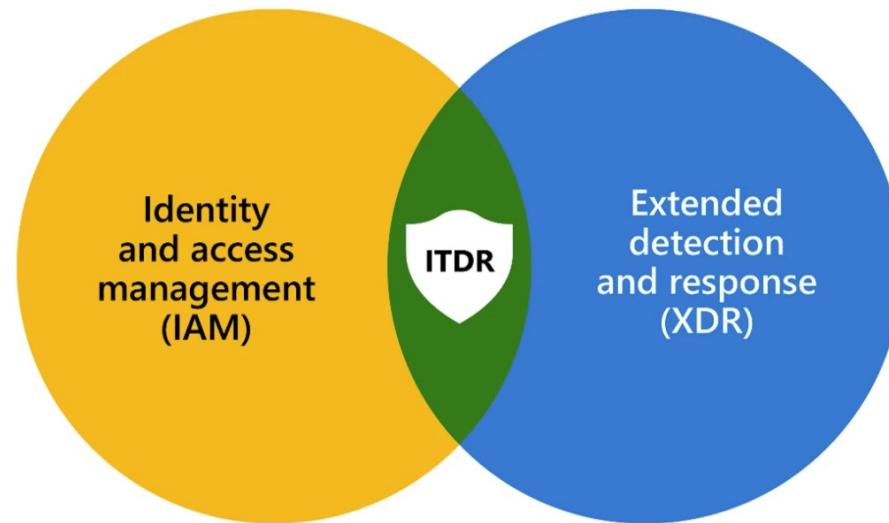
Azure AD Identity Protection **Available**

**Quick guides**

[What is Microsoft Defender for Identity?](#)

[Zero Trust with Microsoft 365 Defender](#)

[Quick installation guide](#)



# MICROSOFT SECURITY SOLUTIONS

## IDENTITY THREAT DETECTION RESPONSE



# MICROSOFT SECURITY SOLUTIONS

## DETECTIONS AS BEHAVIORS

Detection	Scenario
<b>Impossible travel</b>	Impossible Travel alert will be trigger based on 'Impossible Travel' behavior correlated with other risky indicators, such AAD IP signals, highly suspicious pattern of activities and anomalies in the user's behavior.
<b>Infrequent country activity</b>	Infrequent country activity alert will be triggered based on 'Infrequent country' behavior correlated with other risky indicators, such AAD IP signals, highly suspicious pattern of activities and anomalies in the user's behavior.
<b>Multiple Failed Logins</b>	Multiple Failed Logins alert will be trigger based on 'Multiple Failed Logins' behavior and will focus only on successful attempts, followed by highly suspicious pattern of failed attempts correlated with anomalies in the users behavior.

# MICROSOFT SECURITY SOLUTIONS

## NEW RISK-BASED DETECTION IN M365D

Detection	Scenario
<b>Suspicious Azure activities related to possible cryptocurrency mining</b>	Detect potential crypto-mining activities done in one or more of the tenant's subscriptions.
<b>New external user account created by risky user</b>	Detect when risky user invited new external account to the tenant.
<b>Azure AD app registration by risky user</b>	Detect potential malicious application set up and admin contested by risky user (usually to maintain persistence in that context).
<b>Risky user created global admin</b>	Detect potential malicious global admin backdoor account that was set up by the attacker.
<b>Access elevation by risky user</b>	Detect potentially compromised global admin that escalates privileges to manage Azure resources.
<b>Risky user added permissions over other mailboxes</b>	Detecting when potentially compromised privileged exchange account adds powerful permissions over other mailboxes in the organization.
<b>Suspicious role assignment by a risky user</b>	Detect when potentially compromised user performed role assignment with suspicious characteristics.
<b>Unusual activities by AAD Connect sync account</b>	Detect unusual activities by AAD Connect sync account. This might indicate the user is compromised and used for malicious activities.

# MDA App Governance and Behavior Table in M365D

LIVE DEMO

# NEXT EVENTS AND ANNOUNCEMENTS



The image shows a promotional graphic for a Microsoft Security event. On the left, there's a dark vertical bar containing the Microsoft Security logo and text. On the right, a man and a woman are standing in an office hallway, looking at a laptop together. They are positioned in front of large, overlapping circles in orange and blue.

**Microsoft Security**

**Reimagine secure access with Microsoft Entra**

Protect identity and secure access for anyone, anywhere

Digital event / July 11



# CLOUD IDENTITY SUMMIT '23

Koblenz, Germany

Thu, September 7th, 2023

[www.identitysummit.cloud](http://www.identitysummit.cloud)

Supported by



Community Event by



Sponsored by





30.03.2023

THANK YOU  
...UNTIL NEXT TIME!

@AZUREBONN