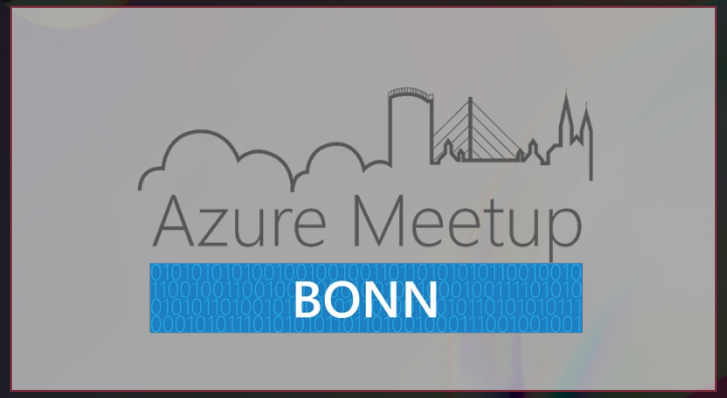


WHAT'S NEW IN MICROSOFT ENTRA?

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

Supported by

DEBEKA INNOVATION CENTER

Community Event by

Azure Meetup BONN

Sponsered by

adesso business. people. technology.

glueckkanja gab

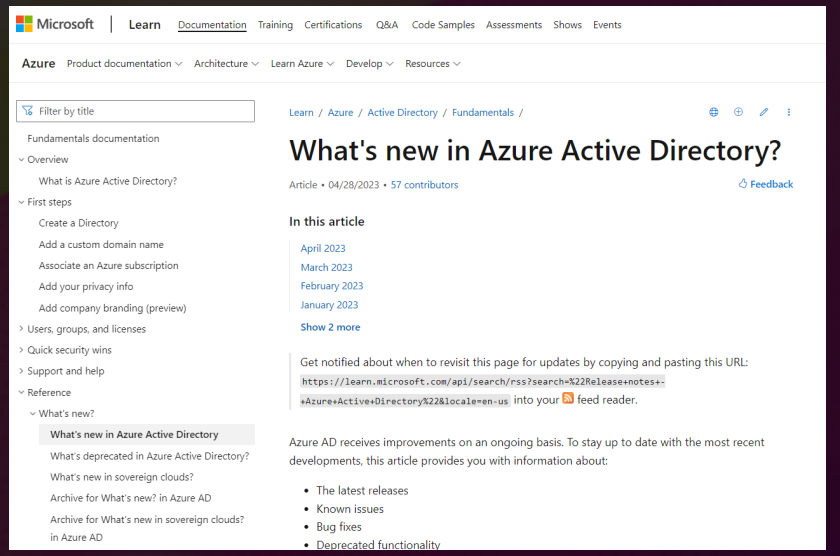
RECENT EVENTS & ANNOUNCEMENTS

Virtual
April 13, 2023

RECENT EVENTS & ANNOUNCEMENTS

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

Microsoft Build
Seattle
May 23 - 25, 2023



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?

Issuer

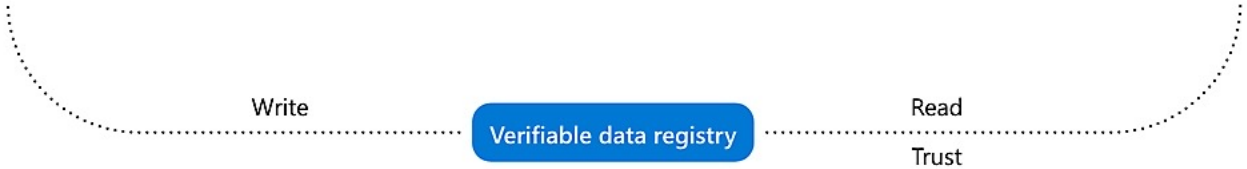
Attests to claims and grants a digitally signed credential to user. An **issuer** could be an identity verification provider a government agency, a previous employer, a university or any other organization that can provide proof of Becca's credentials.

Individual

Receives and approves credential request from issuer, stores and manages credentials in wallet, then presents to verifier.

Verifier

Requests proof and, upon receipt, verifies that claims in credentials satisfy requirements. A **verifier** could be a prospective employer, an airline, a mortgage company or any organization that is requesting proof of Becca's credentials.

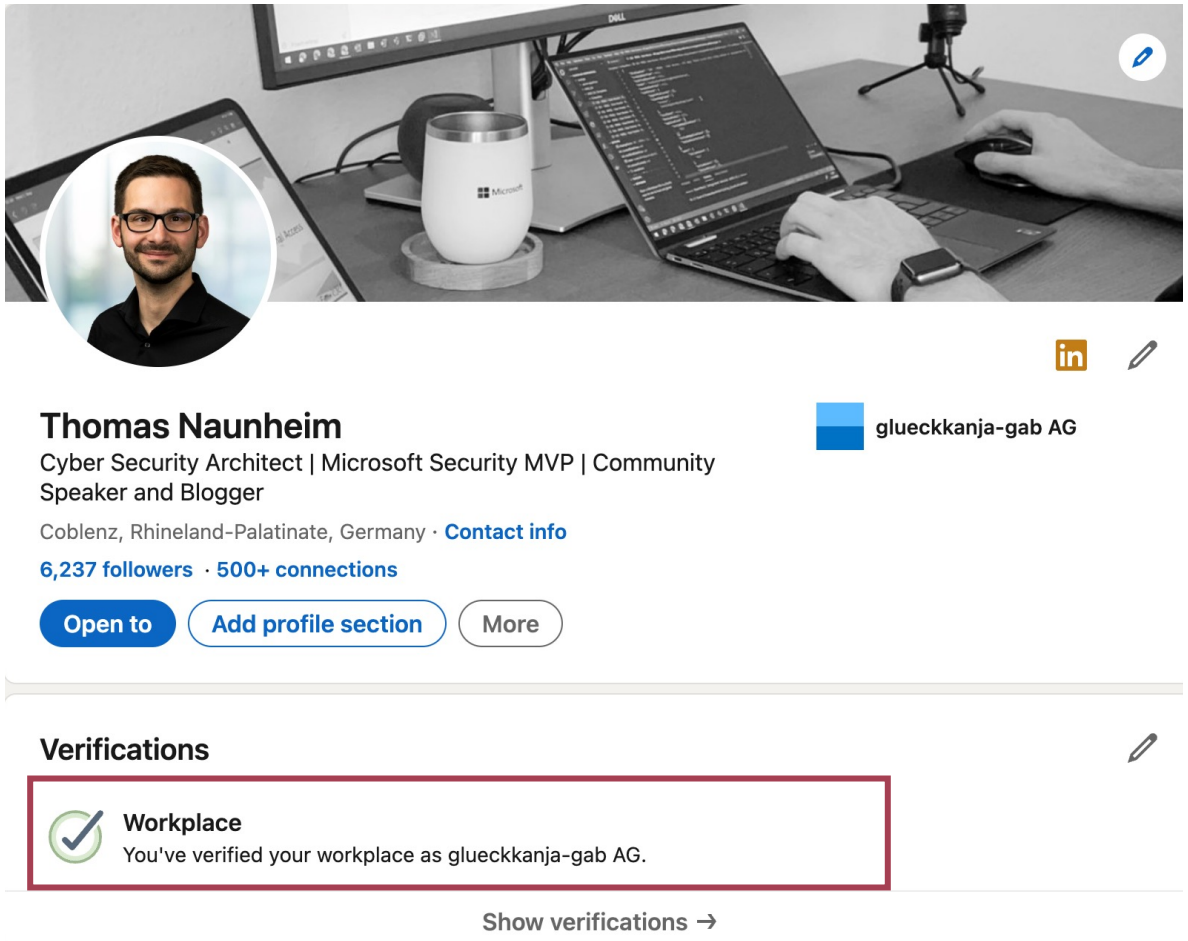


More details: "Microsoft Entra Verified ID | Microsoft Security"

Onboarding and Entitlement Management with Verified ID

LIVE DEMO

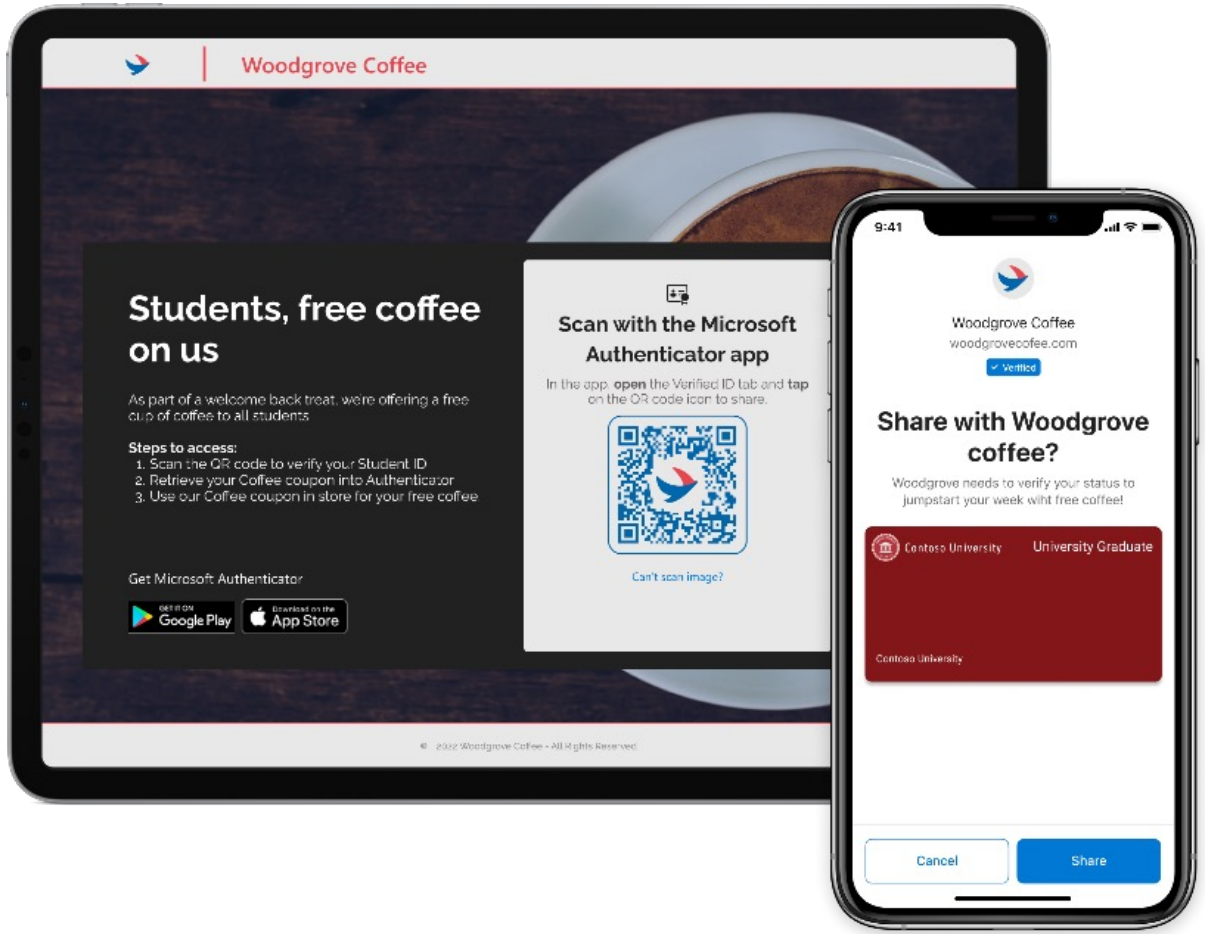
USE CASE FOR B2E
WORK VERIFICATION ON LINKEDIN



- LinkedIn and Microsoft Entra introduce a new way to verify your workplace

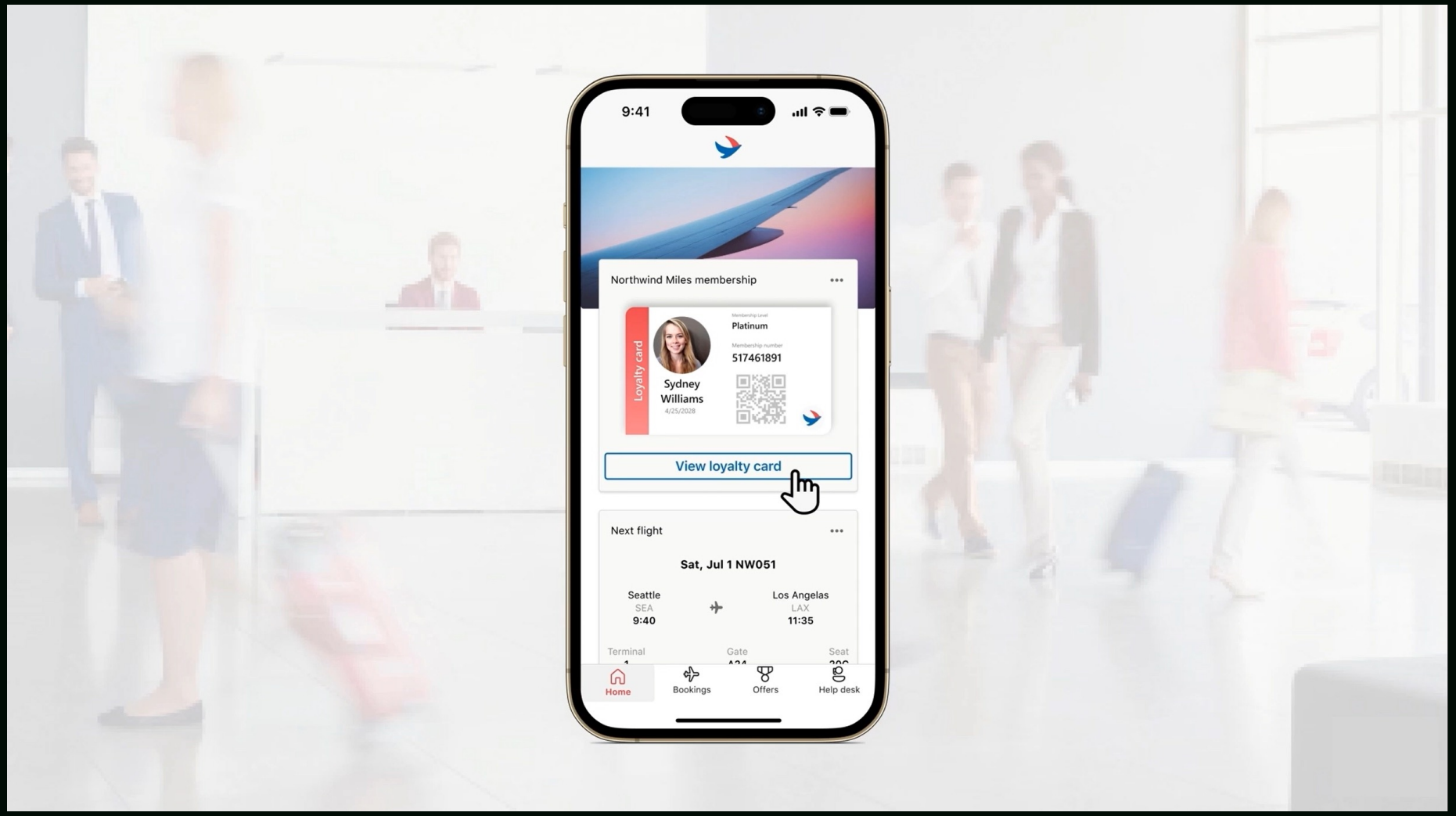
- Microsoft Learn: Setting up LinkedIn workplace verification

USE CASE FOR B2C:
LOYALTY / CUSTOMER CARD



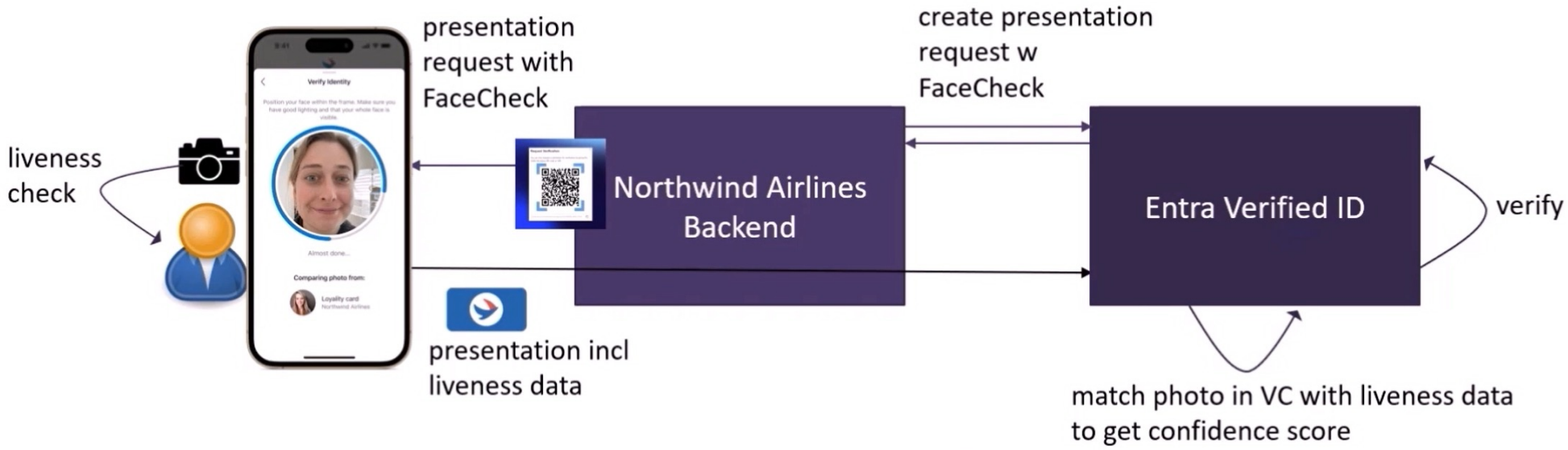
Source/more details: "Reduce fraud and improve engagement using Digital Wallets | OD30"

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

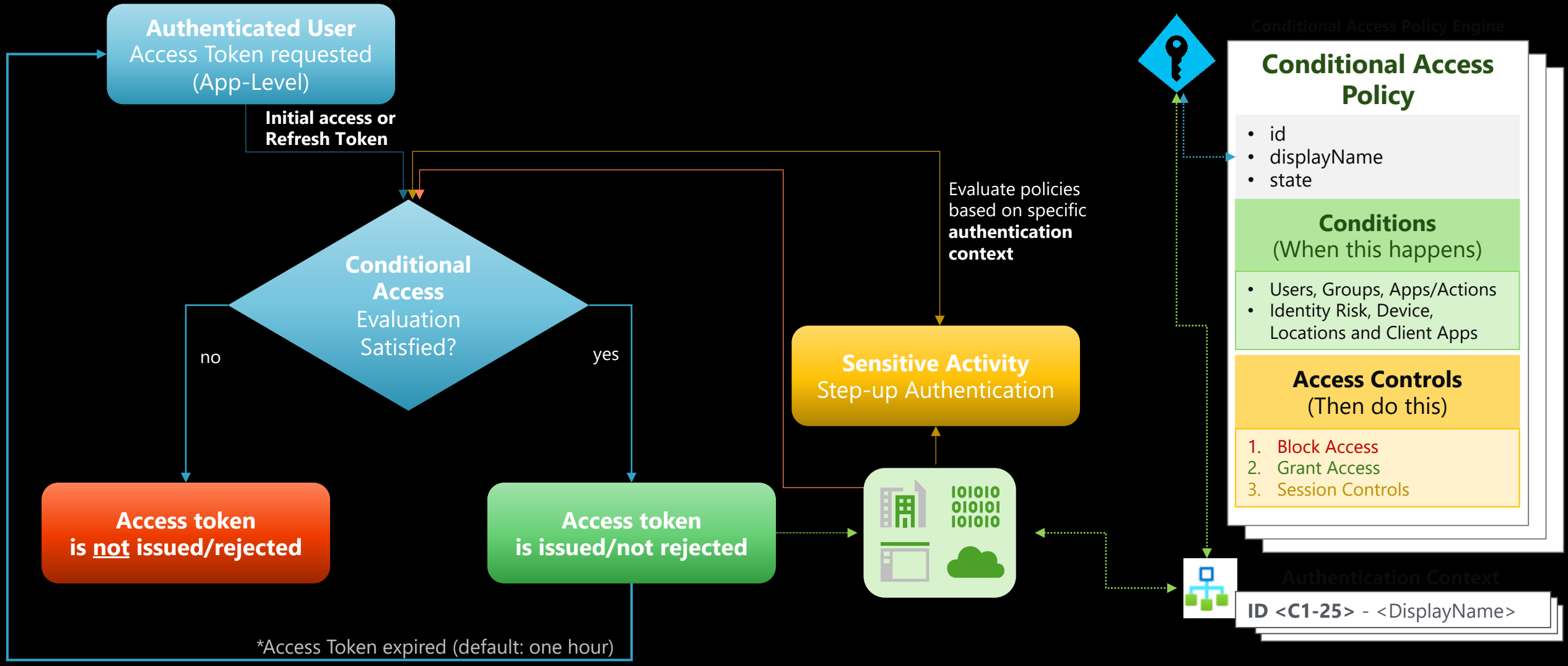



```
{
  ...
"requestedCredentials": [
  {
    "type": "NorthwindAirlinesMilesClub",
    "acceptedIssuers": [ "did:web:northwindairlines.com" ],
    "configuration": {
      "validation": {
        "faceCheck": {
          "sourcePhotoClaimName": "photo",
          "matchConfidenceThreshold": 70
        }
```

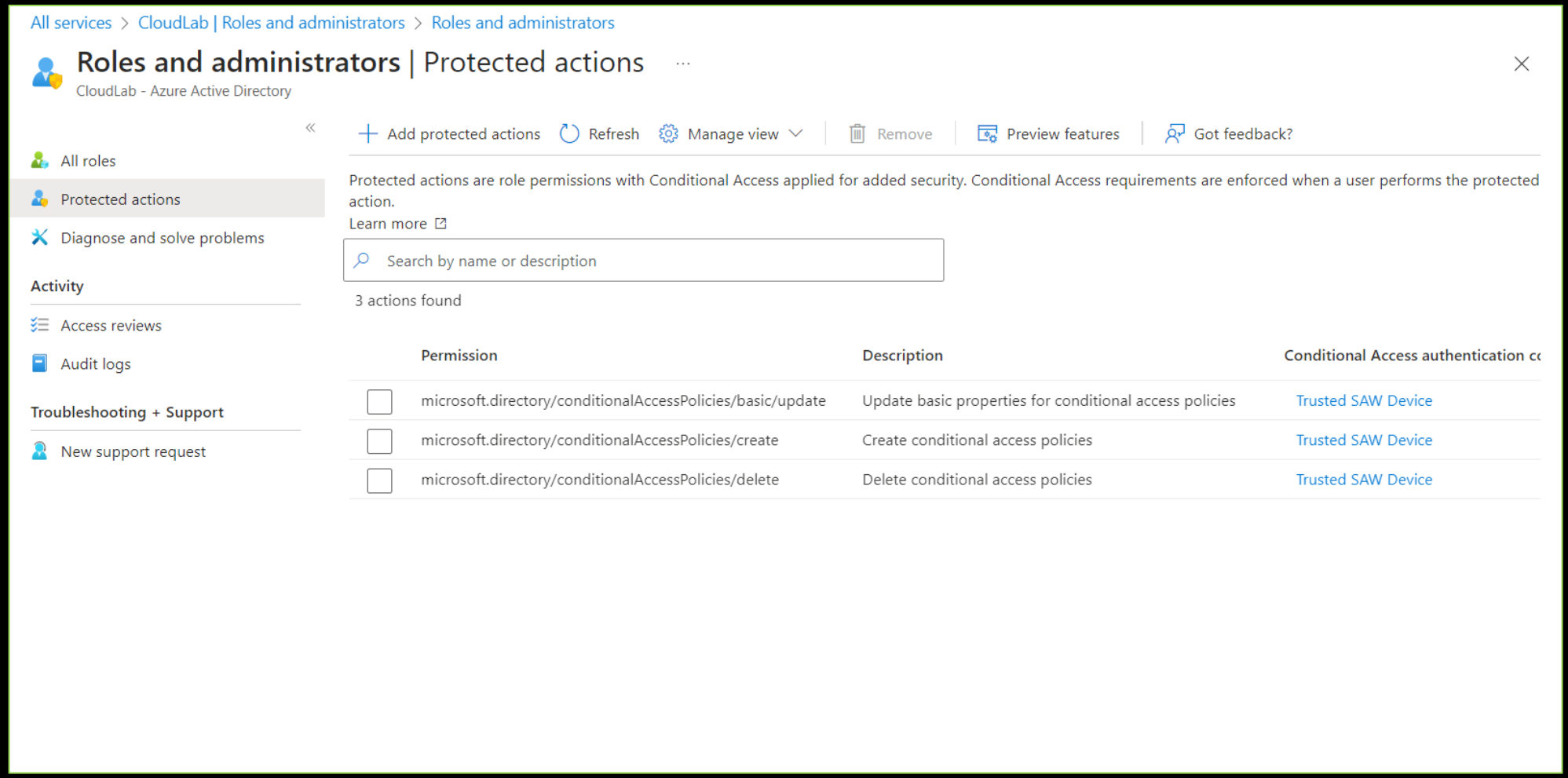
Source/more details: "Reduce fraud and improve engagement using Digital Wallets | OD30"

MICROSOFT AZURE ACTIVE DIRECTORY

MICROSOFT AZURE ACTIVE DIRECTORY
AUTHENTICATION CONTEXT

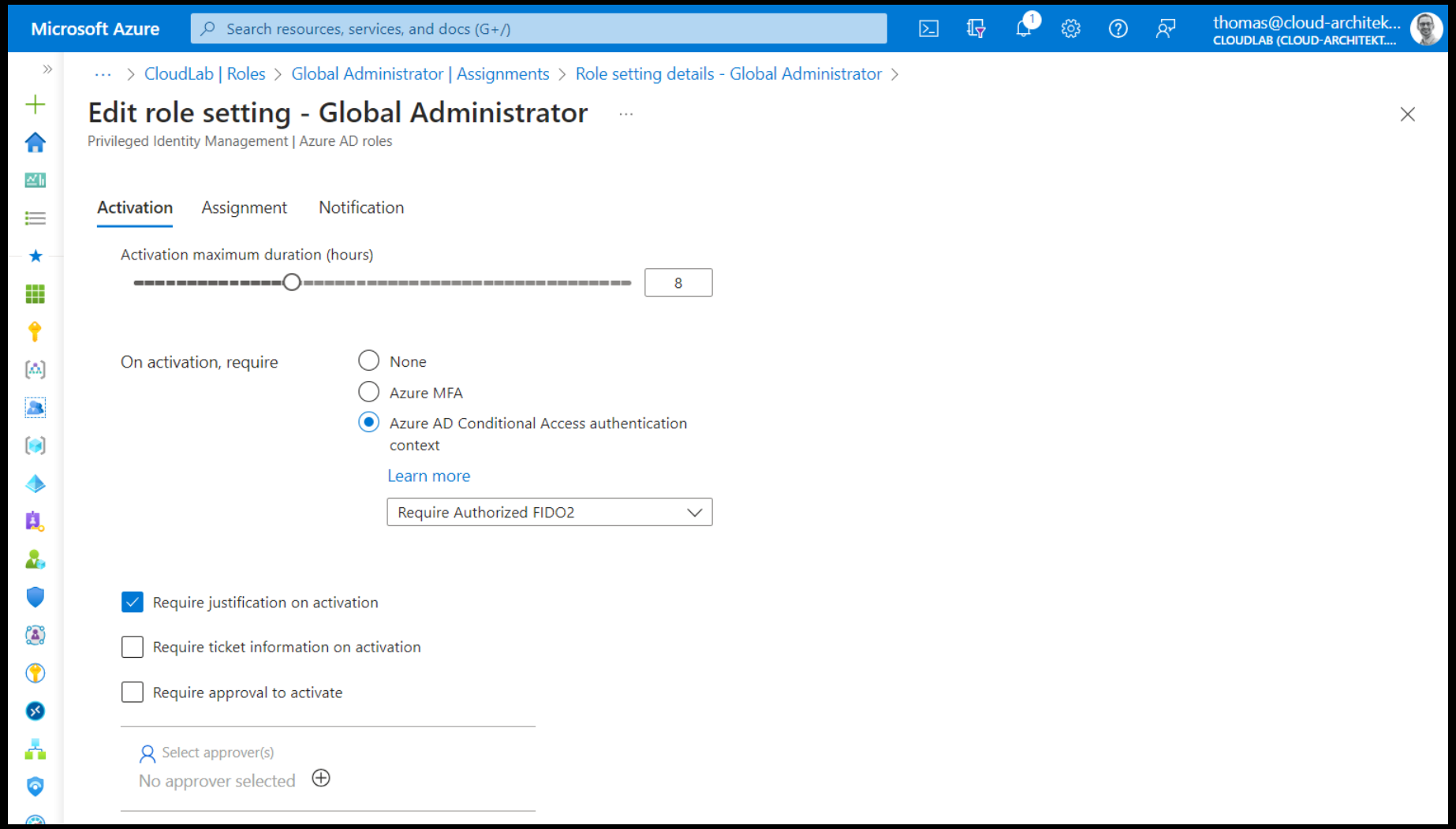


MICROSOFT AZURE ACTIVE DIRECTORY
AUTHENTICATION CONTEXT IN “PROTECTED ACTIONS”



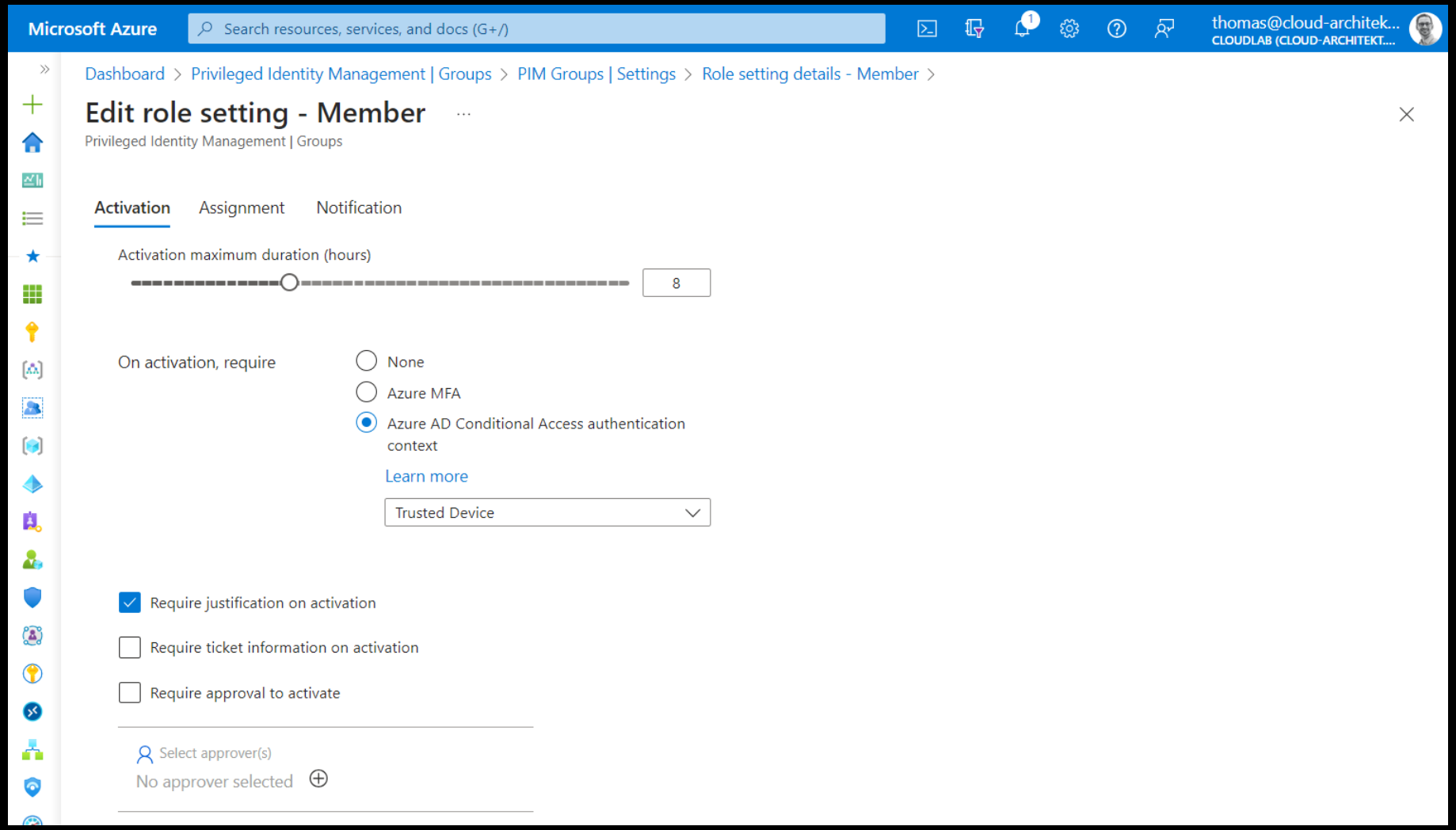
Microsoft Docs: What are protected actions in Azure AD? (preview) - Microsoft Entra | Microsoft Learn

MICROSOFT AZURE ACTIVE DIRECTORY
AUTHENTICATION CONTEXT IN PIM

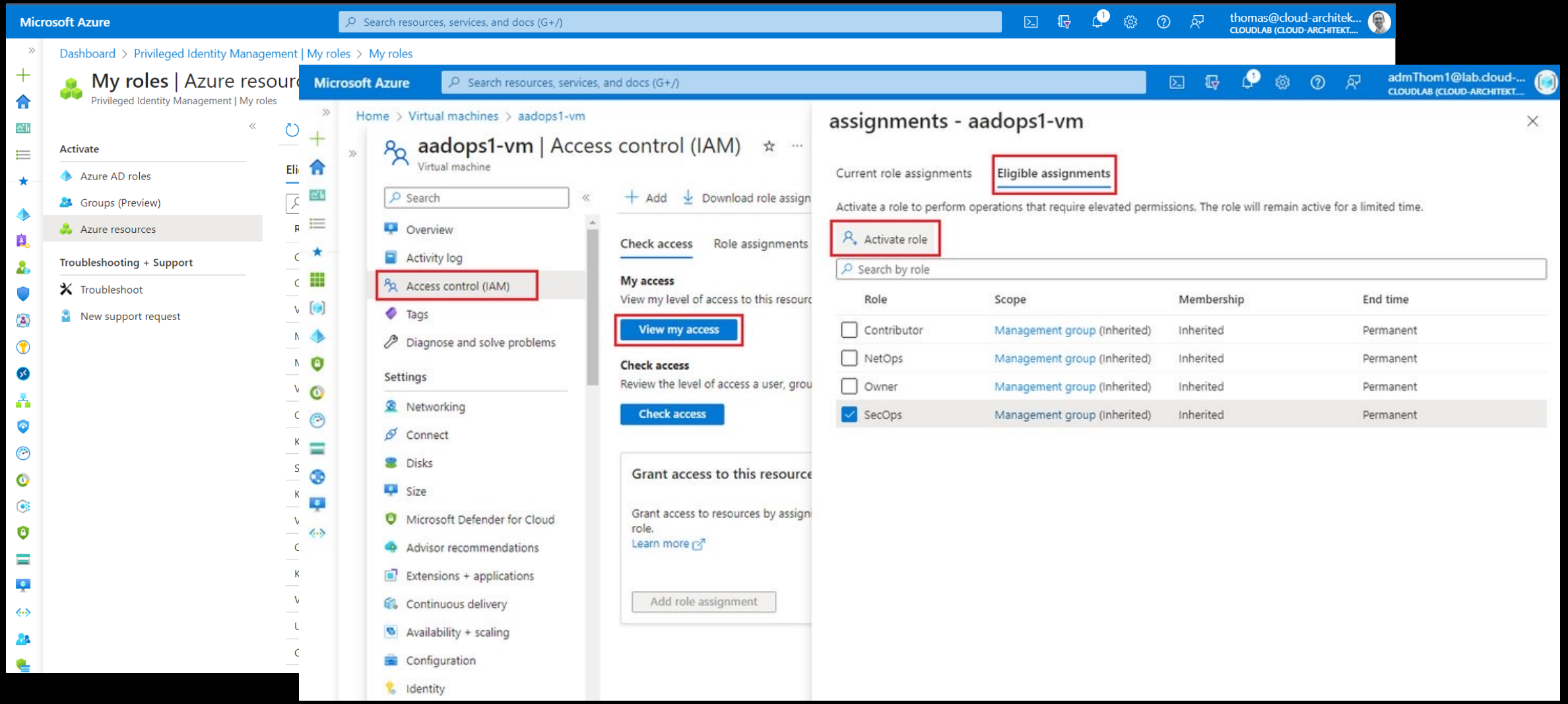


Session: Build secure applications with External Identities in Microsoft Entra | BRK261

MICROSOFT AZURE ACTIVE DIRECTORY
SECURITY GROUPS IN PIM



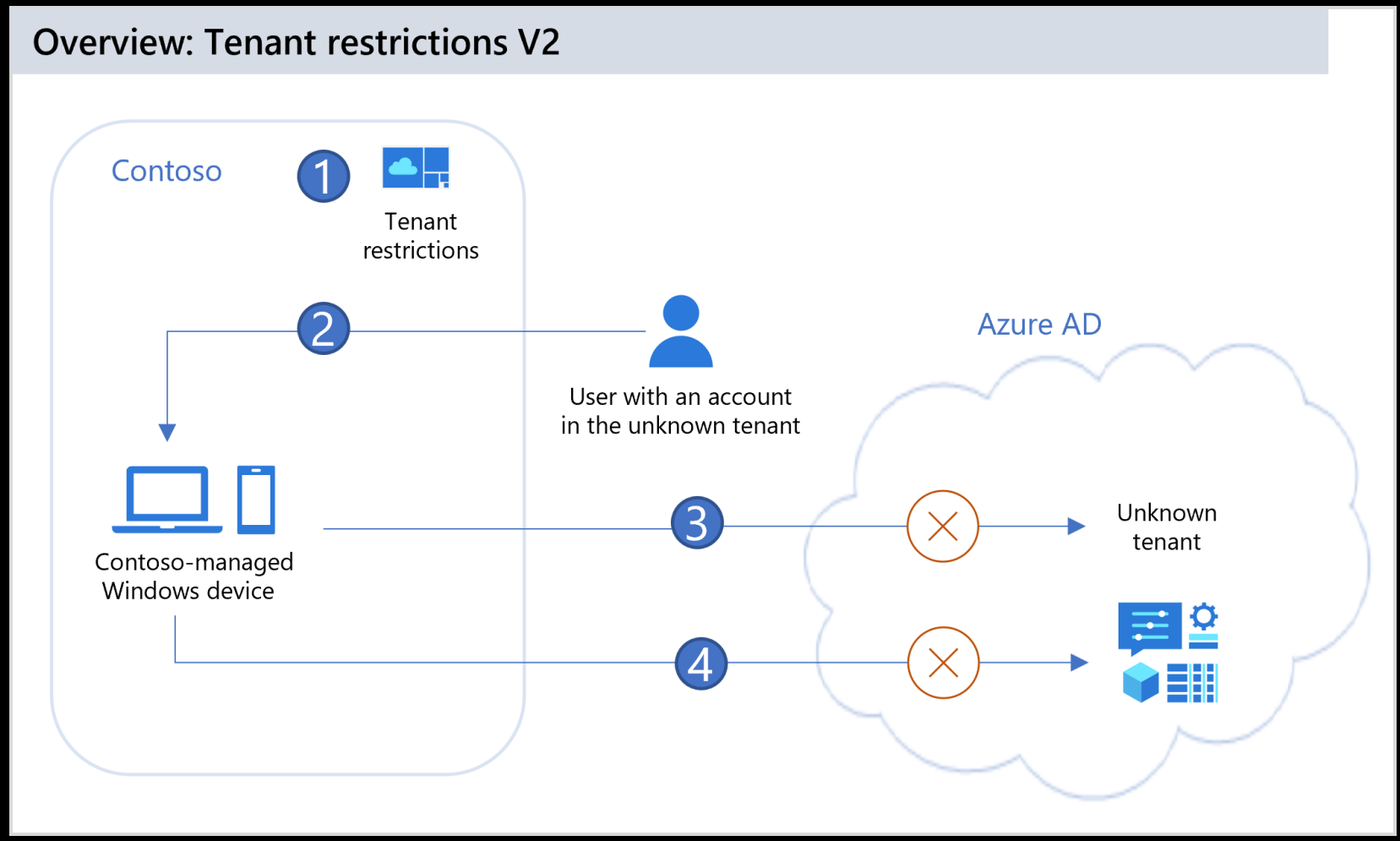
MICROSOFT AZURE + AZURE AD
AZURE PIM ELIGIBLE ROLES



Authentication Context in Azure (AD) PIM

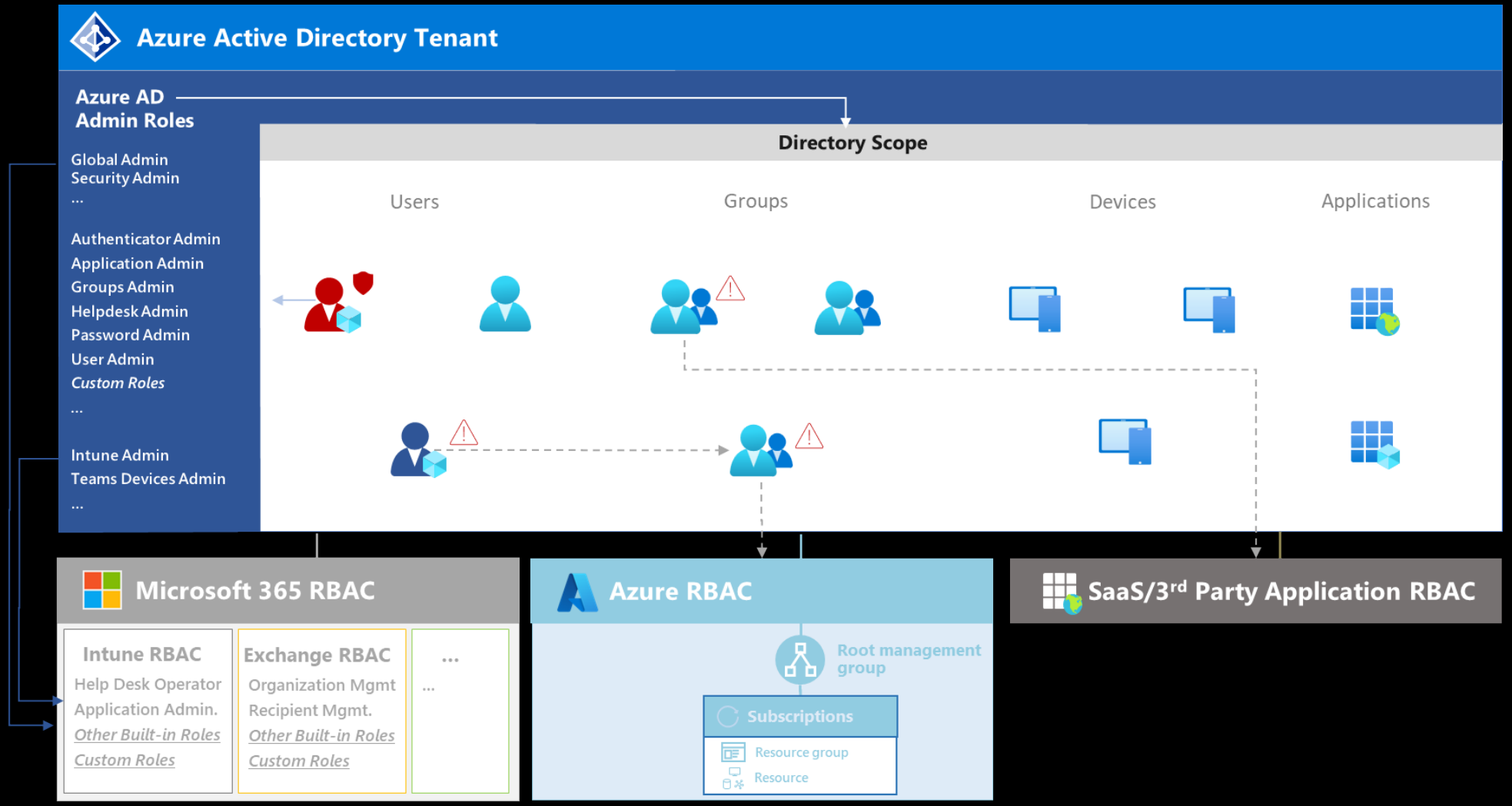
LIVE DEMO

MICROSOFT AZURE ACTIVE DIRECTORY
TENANT RESTRICTION V2



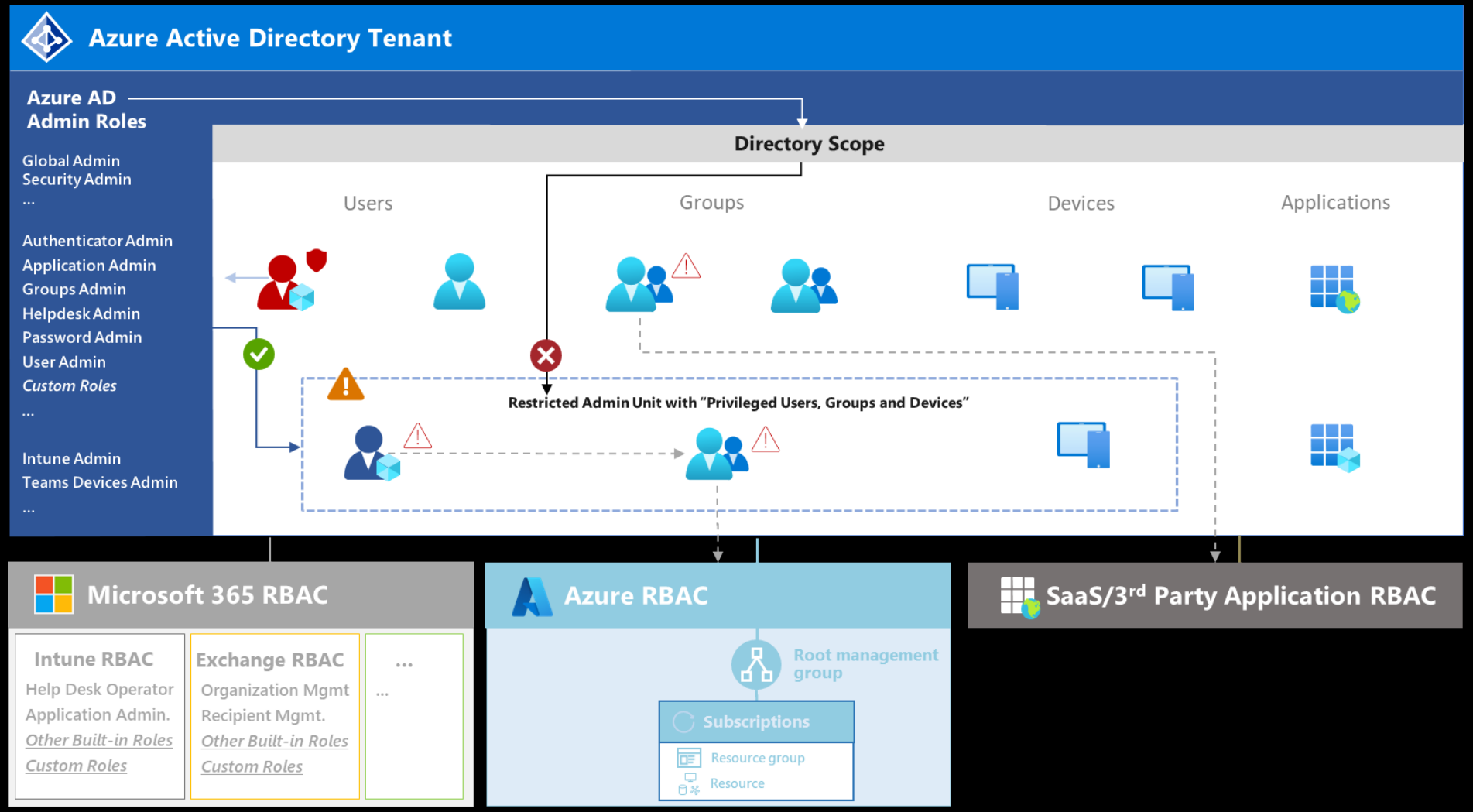
Docs Article: Configure tenant restrictions - Azure AD - Microsoft Entra | Microsoft Learn

MICROSOFT AZURE ACTIVE DIRECTORY
ADMINISTRATIVE UNITS



Docs Article: Configure tenant restrictions - Azure AD - Microsoft Entra | Microsoft Learn

MICROSOFT AZURE ACTIVE DIRECTORY
RESTRICTED MANAGEMENT ADMINISTRATIVE UNITS

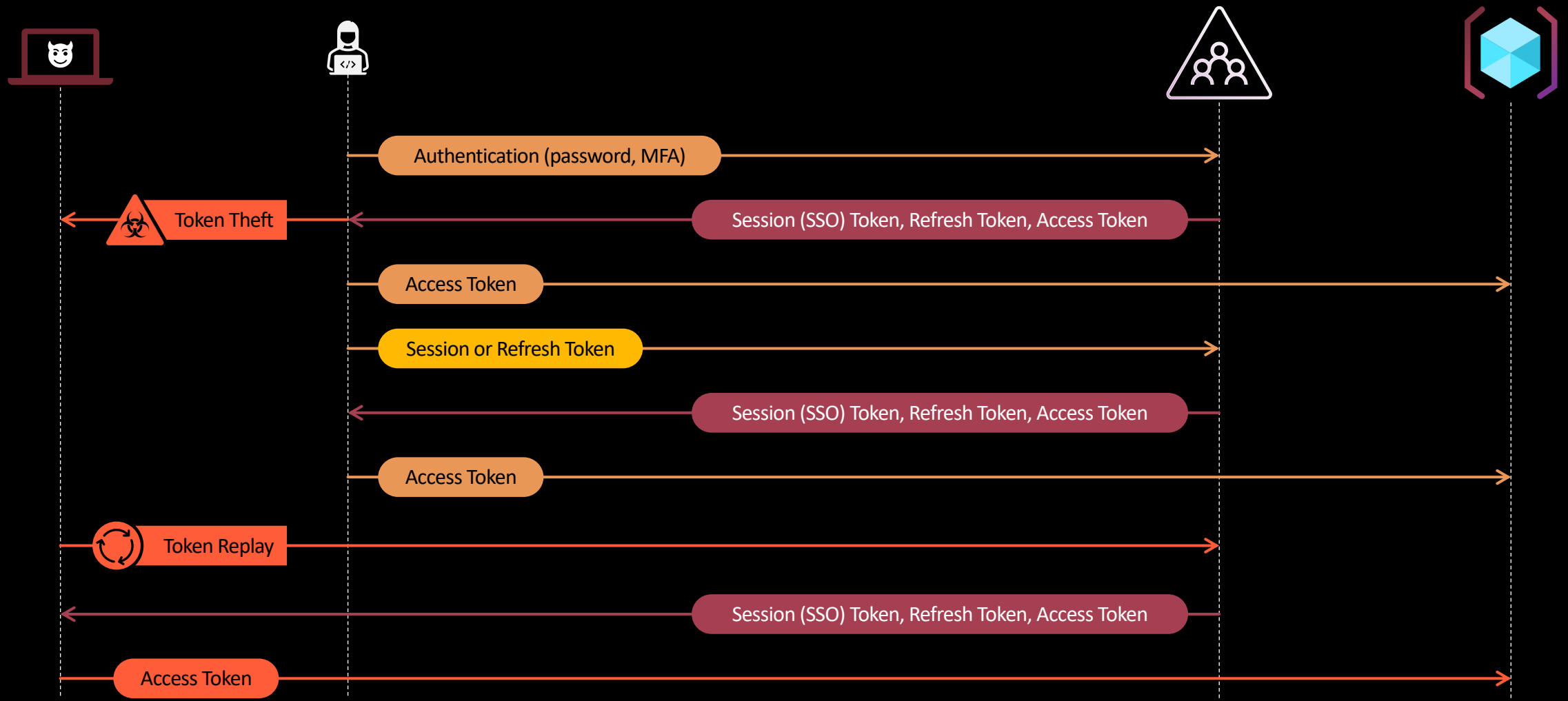


Docs Article: Configure tenant restrictions - Azure AD - Microsoft Entra | Microsoft Learn

MICROSOFT AZURE ACTIVE DIRECTORY
TOKEN PROTECTION

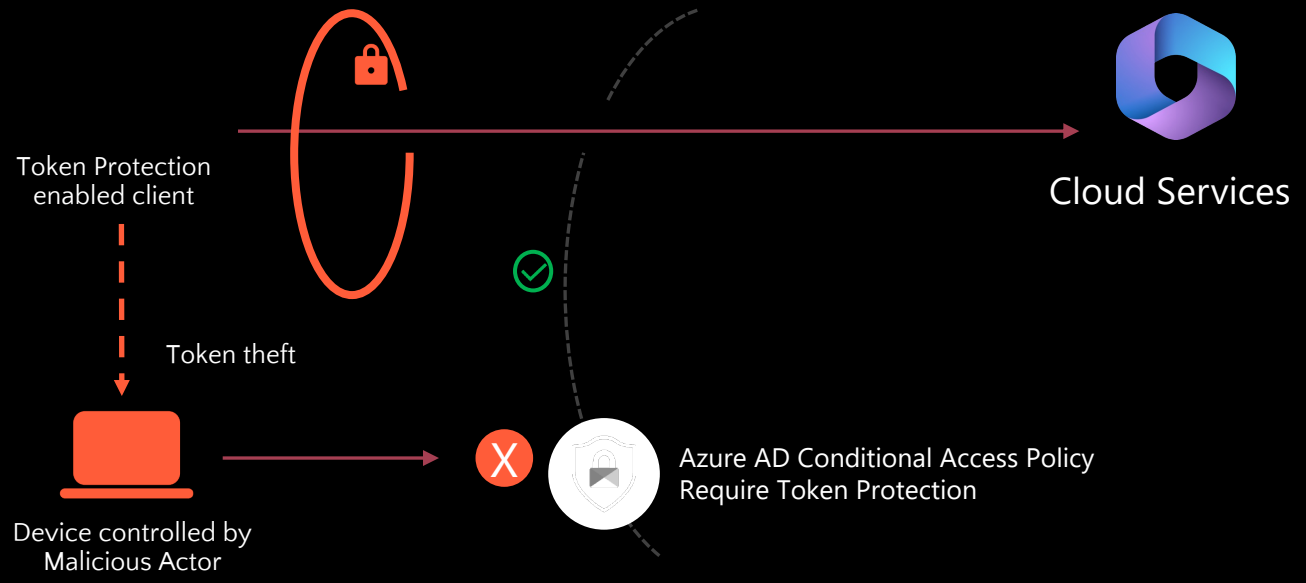
Attackers 💖 Cookies and Tokens

MICROSOFT AZURE ACTIVE DIRECTORY
TOKEN PROTECTION



Source/Session: How identity security protects the bottom line (Microsoft Secure)

MICROSOFT AZURE ACTIVE DIRECTORY
TOKEN PROTECTION



Source/Session: How identity security protects the bottom line (Microsoft Secure)

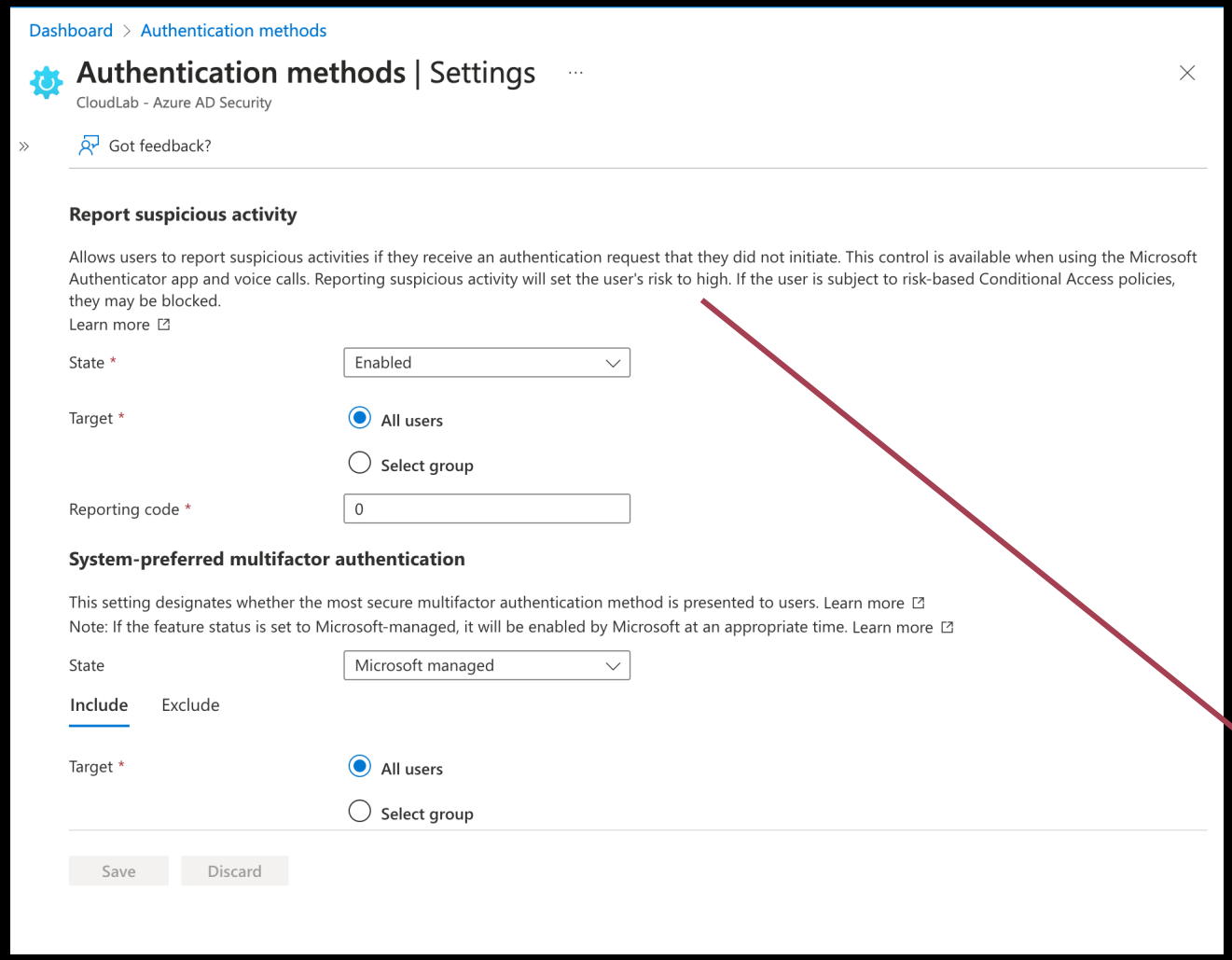
MICROSOFT AZURE + AZURE AD
POWERSHELL & AZURE CLI WAM SUPPORT

```
# Enable WAM for Azure CLI
az config set core.allow_broker = true
az account clear
az login

# Enable WAM for Azure PowerShell
Update-AzConfig -EnableLoginByWam $true
Connect-AzAccount
```

More Details: Azure Command-line Tools Build 2023 Announcements

AUTHENTICATION METHODS
REPORT SUSPICIOUS ACTIVITY & SYSTEM-PREFERRED MFA



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 reported it as suspicious activity. An MFA prompt that wasn't initiated by the user may mean that the user's credentials have been compromised.

More details: What is risk? Azure AD Identity Protection - Microsoft Entra | Microsoft Learn

Overview of Token Protection and Restricted AU Management

LIVE DEMO

MICROSOFT SECURITY SOLUTIONS

MICROSOFT SECURITY SOLUTIONS
SECURING 3RD PARTY APPS

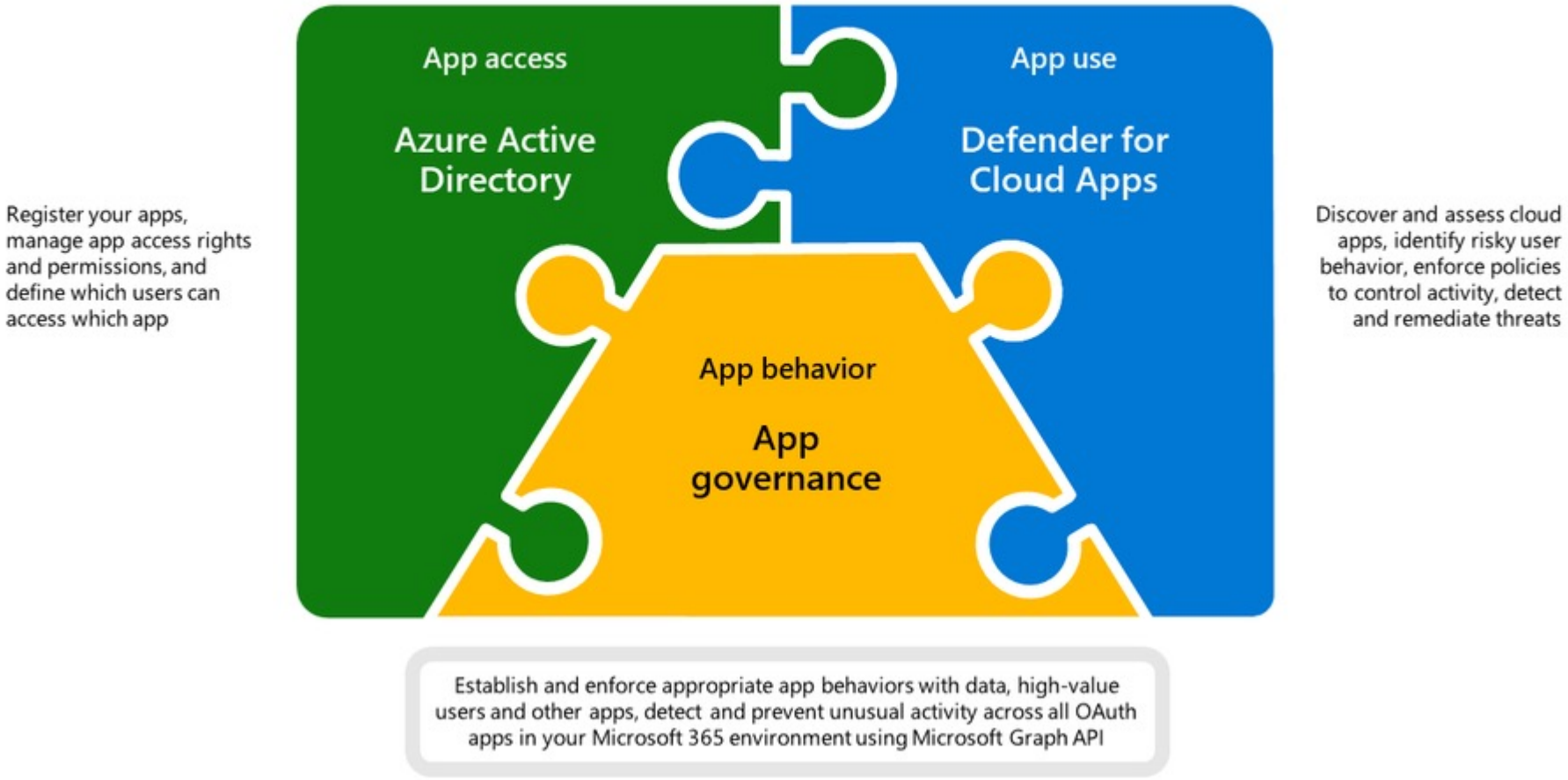


Image source: app governance (microsoft.com)

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.

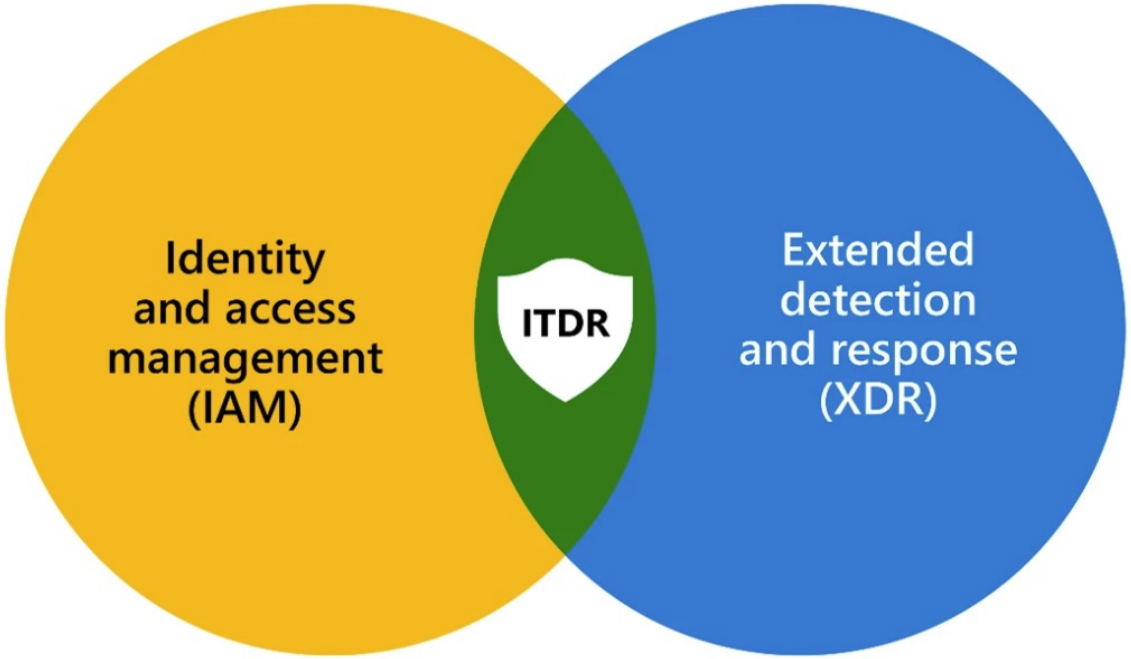
This means that all customers with a standalone, E5 Security, or Microsoft 365 E5, or any other license that includes Defender for Cloud Apps, will have access to App Governance, **at no additional cost**. For existing App Governance customers, on June 1, depending on which channel you've purchased the 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.

Blog Article: RSA News: Taking XDR for SaaS apps to the next level (microsoft.com)

MICROSOFT SECURITY SOLUTIONS
IDENTITY THREAT DETECTION RESPONSE

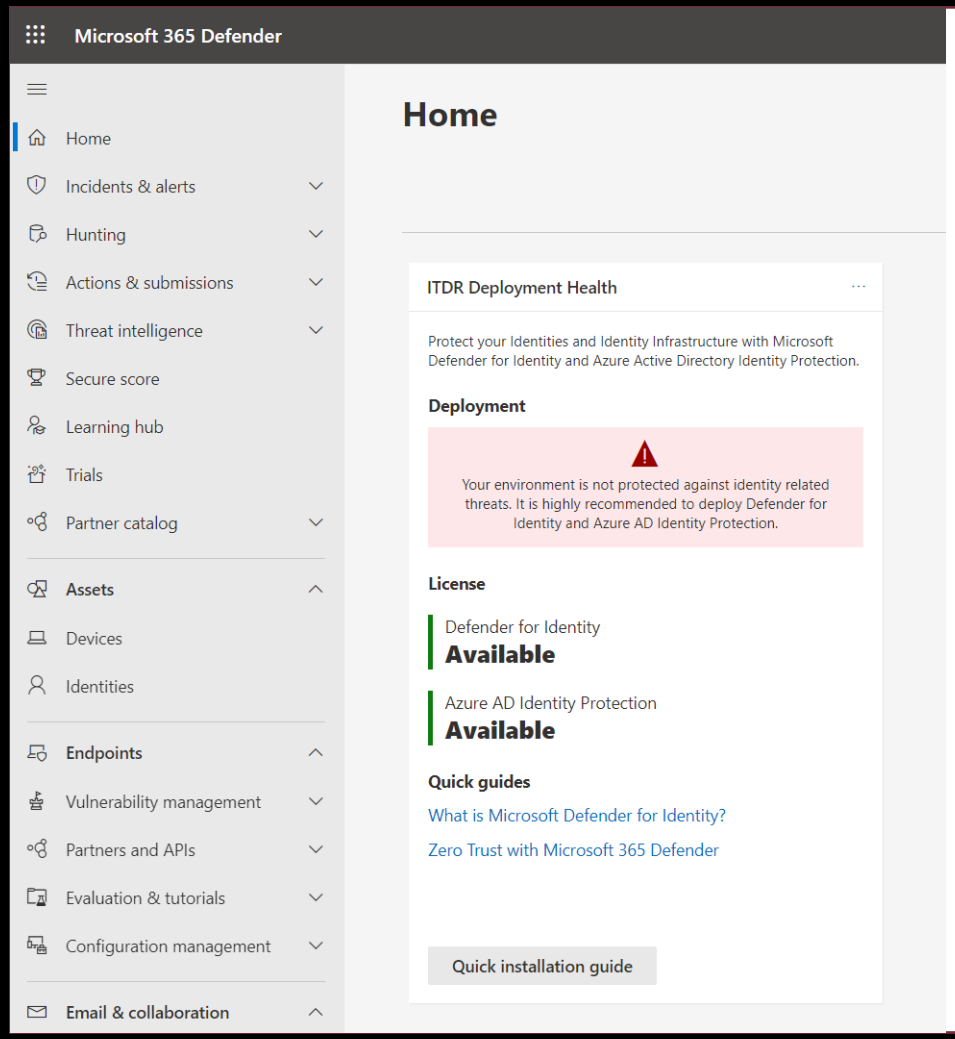
Microsoft is your partner for ITDR

Leverage our expertise as a leader in both IAM and XDR



Blog Article: RSA News: Taking XDR for SaaS apps to the next level (microsoft.com)

MICROSOFT SECURITY SOLUTIONS
IDENTITY THREAT DETECTION RESPONSE



Blog Article: RSA News: Taking XDR for SaaS apps to the next level (microsoft.com)

MICROSOFT SECURITY SOLUTIONS
IDENTITY THREAT DETECTION RESPONSE

Image source: Identity Threat Detection and Response (ITDR) | Microsoft Security

MICROSOFT SECURITY SOLUTIONS
DETECTIONS AS BEHAVIORS

Detection	Scenario
Impossible travel	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.
Infrequent country activity	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.
Multiple Failed Logins	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.

More details : Transform the way you investigate by using Behaviors & new detections in XDR, starting w/SaaS apps - Microsoft Community Hub

MICROSOFT SECURITY SOLUTIONS
NEW RISK-BASED DETECTION IN M365D

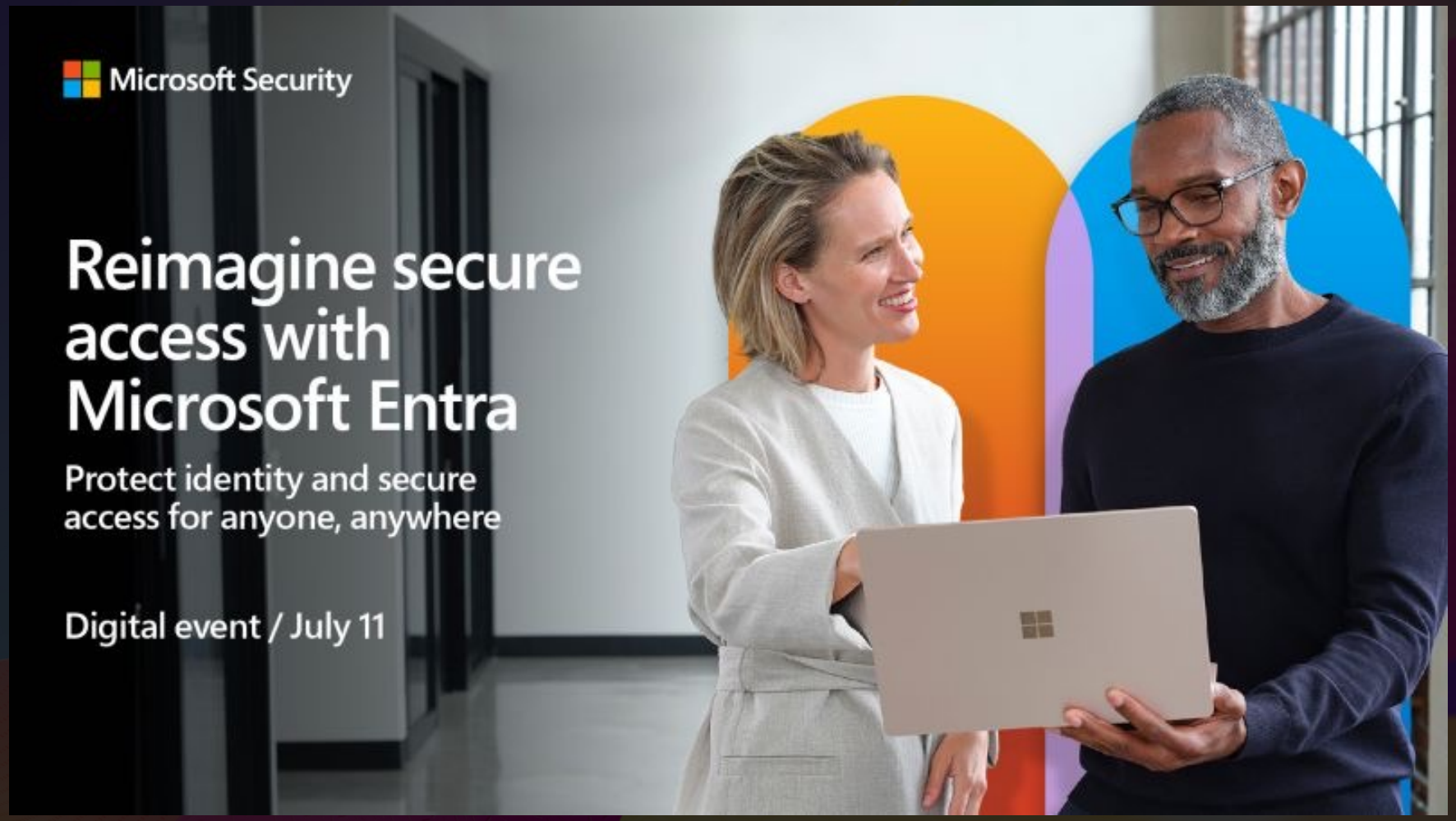
Detection	Scenario
Suspicious Azure activities related to possible cryptocurrency mining	Detect potential crypto-mining activities done in one or more of the tenant's subscriptions.
New external user account created by risky user	Detect when risky user invited new external account to the tenant.
Azure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

More details : Transform the way you investigate by using Behaviors & new detections in XDR, starting w/SaaS apps - Microsoft Community Hub

MDA App Governance and Behavior Table in M365D

LIVE DEMO

NEXT EVENTS AND ANNOUNCEMENTS



CLOUD IDENTITY SUMMIT '23

Koblenz, Germany

Thu, September 7th, 2023

www.identitysummit.cloud

Supported by

DEBEKA INNOVATION CENTER

Community Event by

Azure Meetup BONN

Sponsered by

adesso business. people. technology.

glueckkanja gab

Azure Meetup
BONN

THANK YOU

…UNTIL NEXT TIME!

@AZUREBONN