Conditional Access in Zeiten von Global Secure Access

Christopher Brumm

Experts Live Germany

Christopher Brumm

Cloud Security Architect @glueckkanja

Focus

Identity + Security
in Microsoft Cloud

From

Hamburg, Germany

My Blog

chris-brumm.com

Certs and Titles

CISSP, MVP Identity & Access,
various MS certs

Hobbies

Family, Traveling, Pen & Paper
RPG

Contact

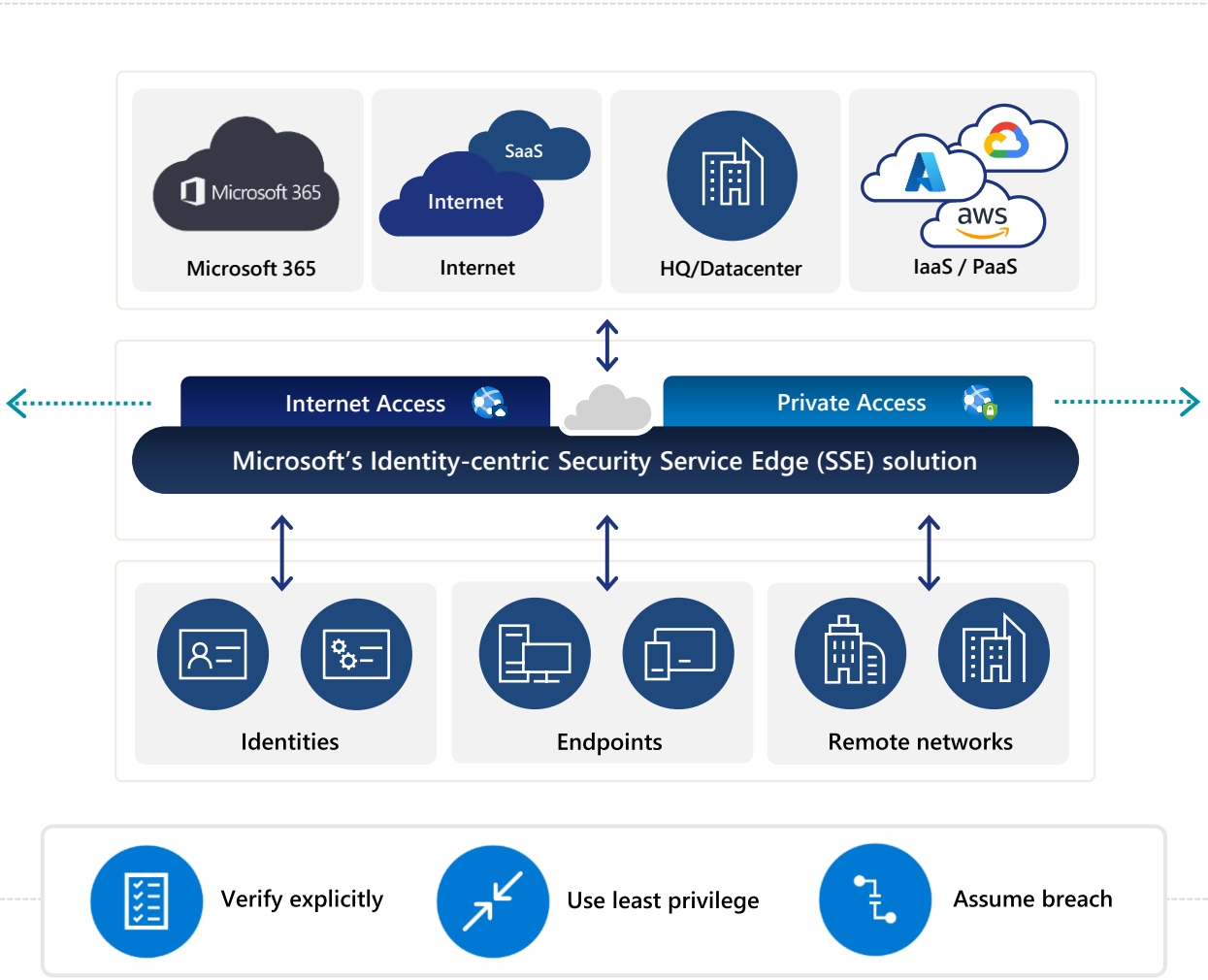
/christopherbrumm

Experts Live Germany

Microsoft's Identity-centric SSE solution

Microsoft Entra Internet Access

Secure access to all internet, SaaS, and Microsoft 365 apps and protect against malicious internet traffic with an **identity-centric Secure Web Gateway (SWG).**

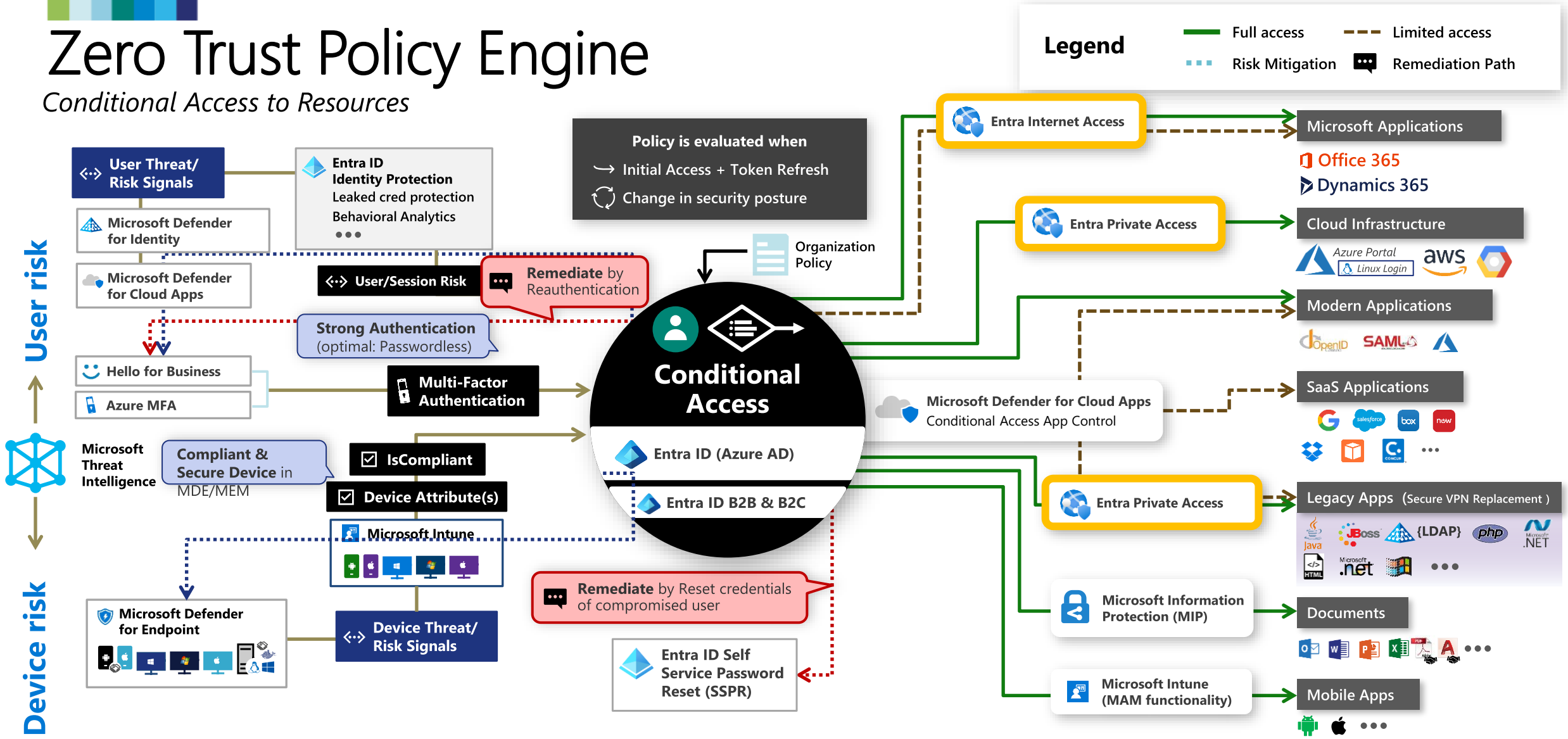


Microsoft Entra Private Access

Secure access to all private apps and resources, for users anywhere, with an **identity-centric Zero Trust Network Access (ZTNA).**

Zero Trust Policy Engine

Conditional Access to Resources



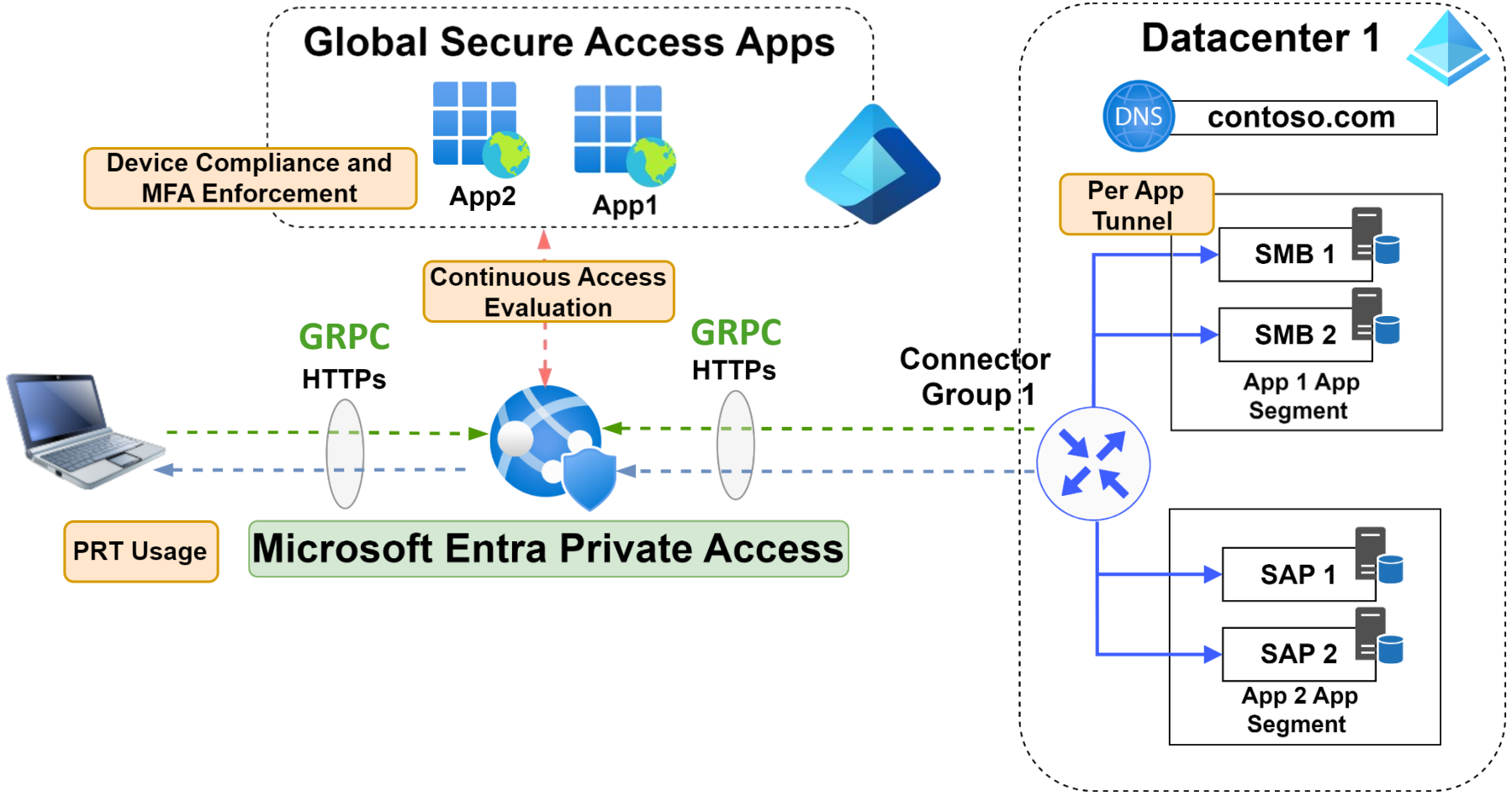
Signal
to make an informed decision

Decision
based on organizational policy

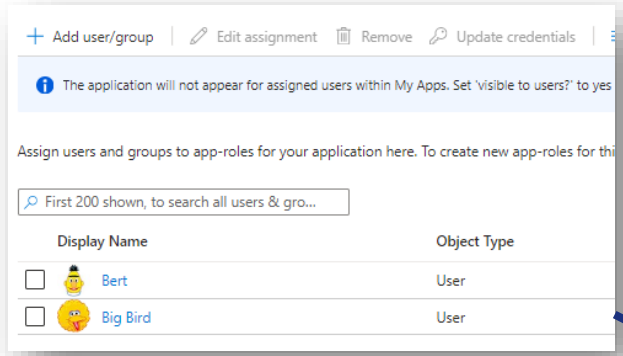
Enforcement
of policy across resources

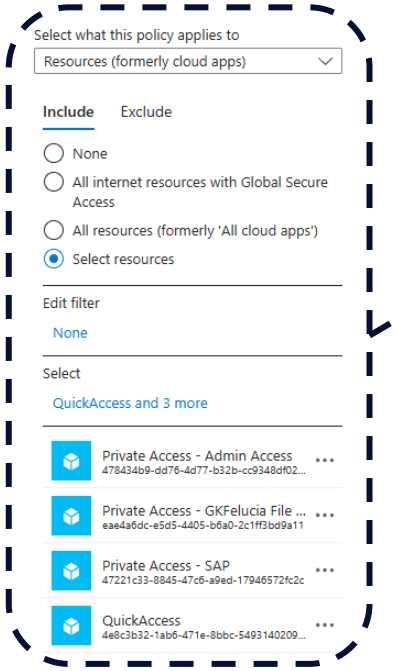
Experts Live Germany

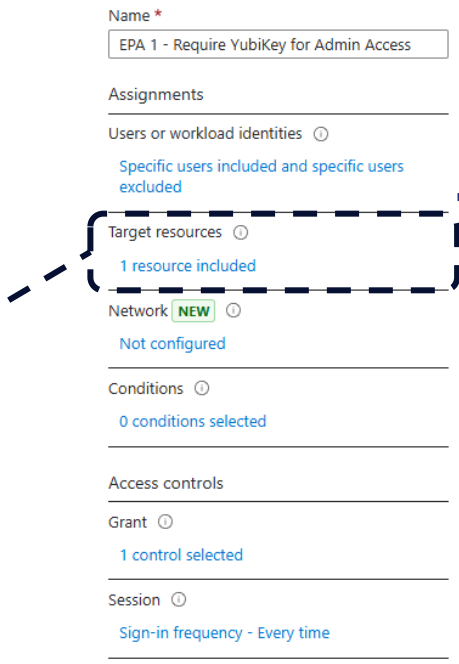
Entra Private Access

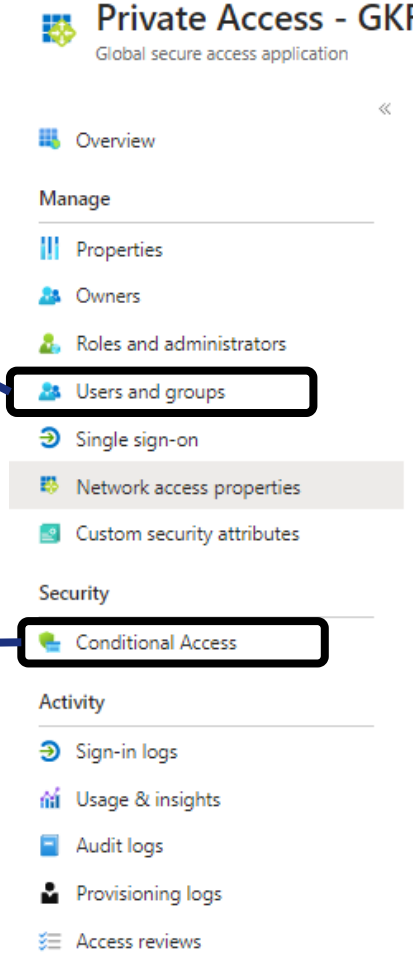


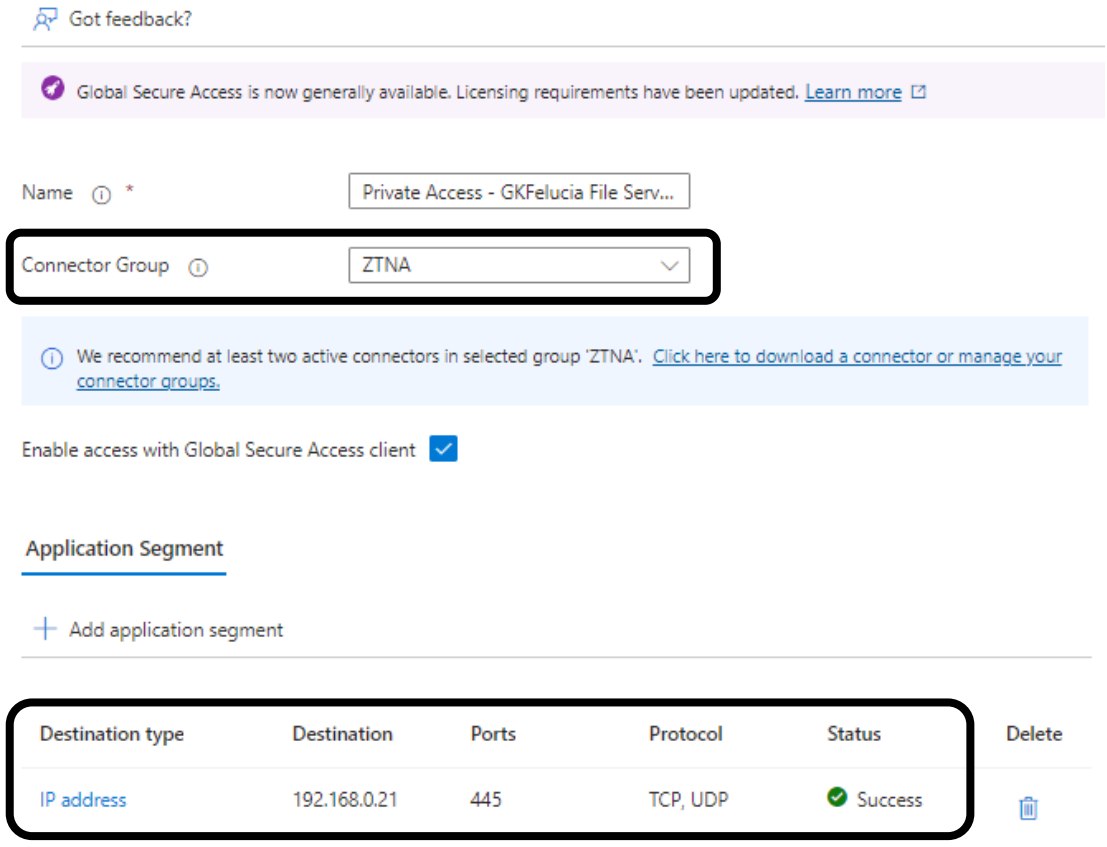
Entra Private Access App – Portal View





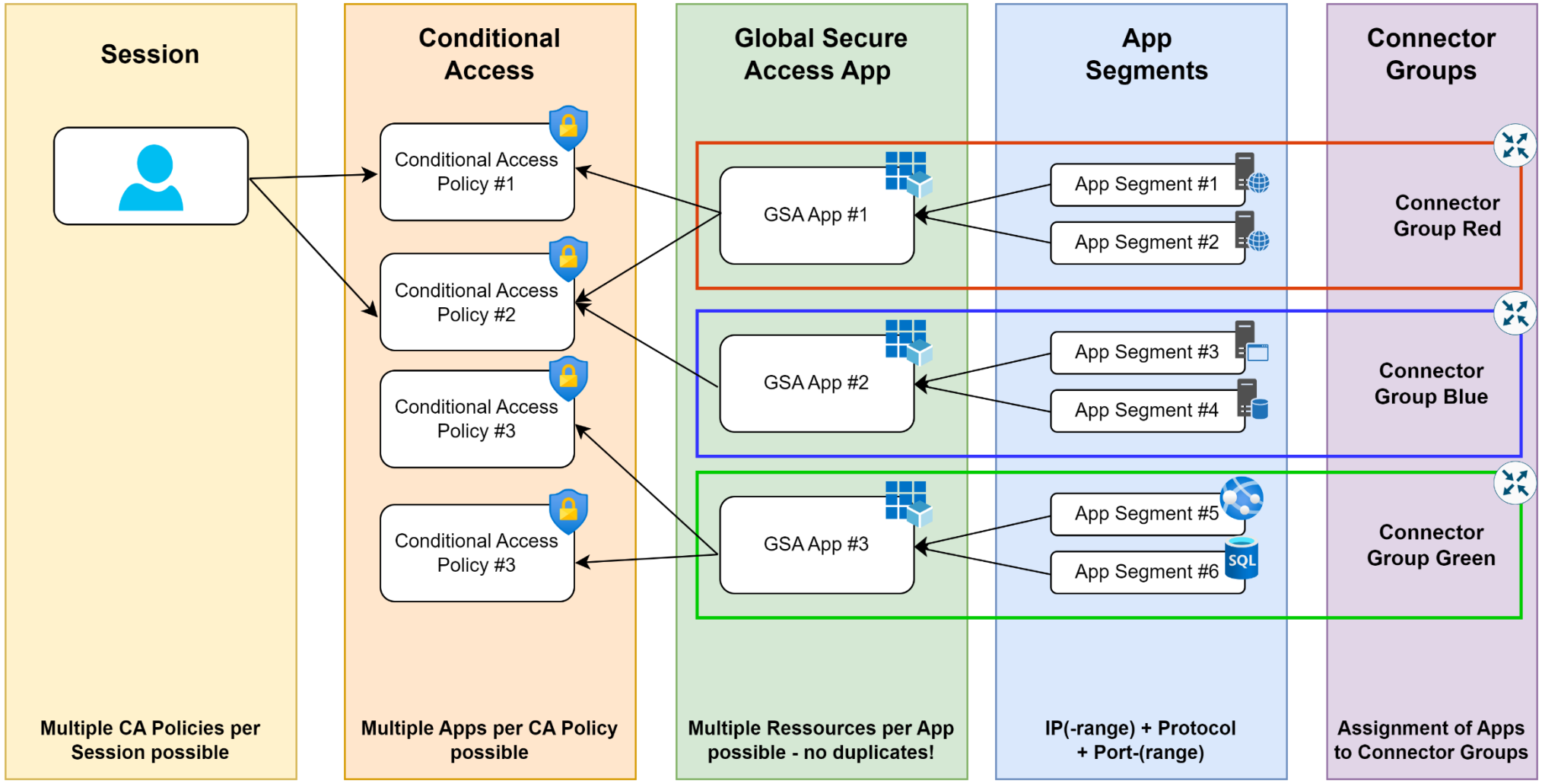




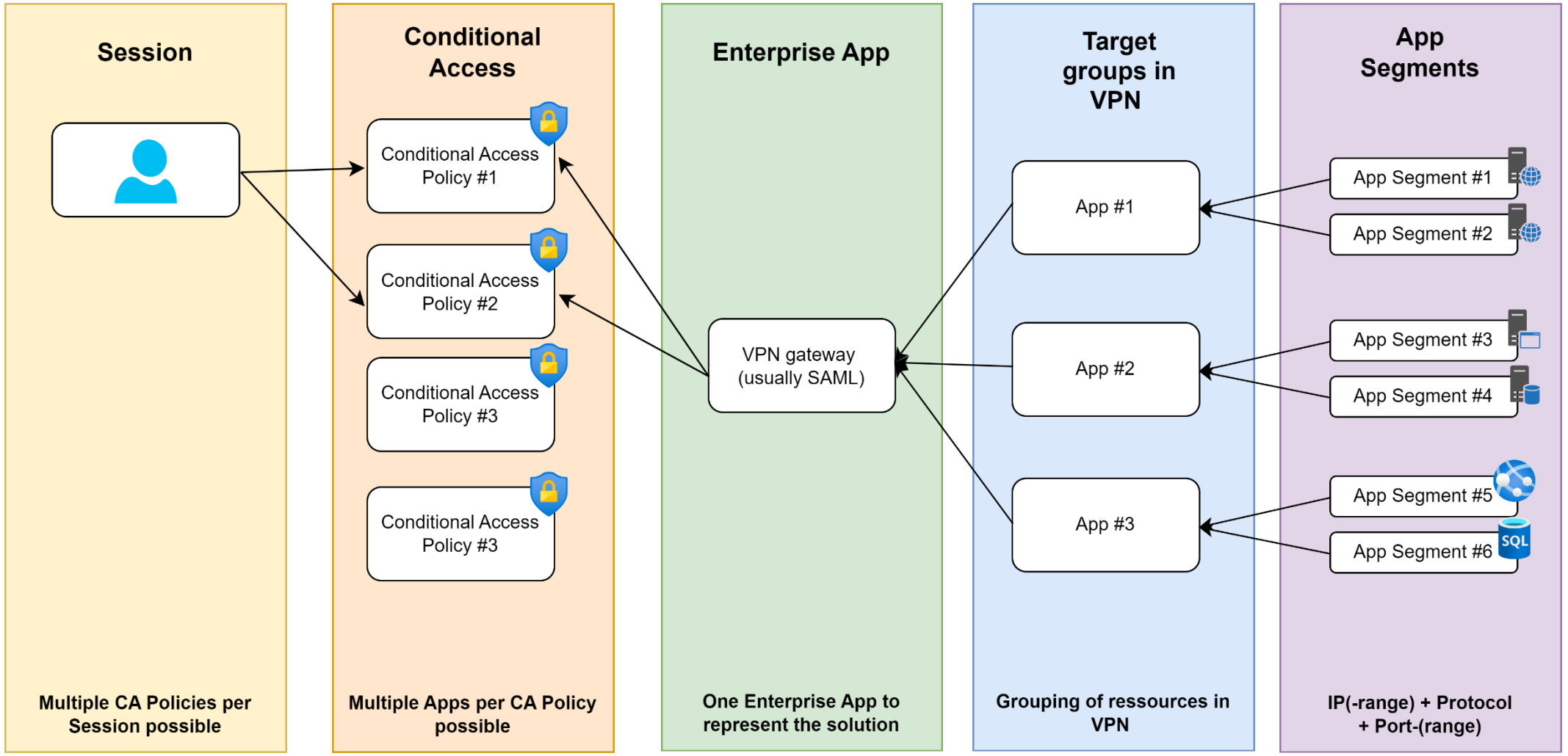


Experts Live Germany

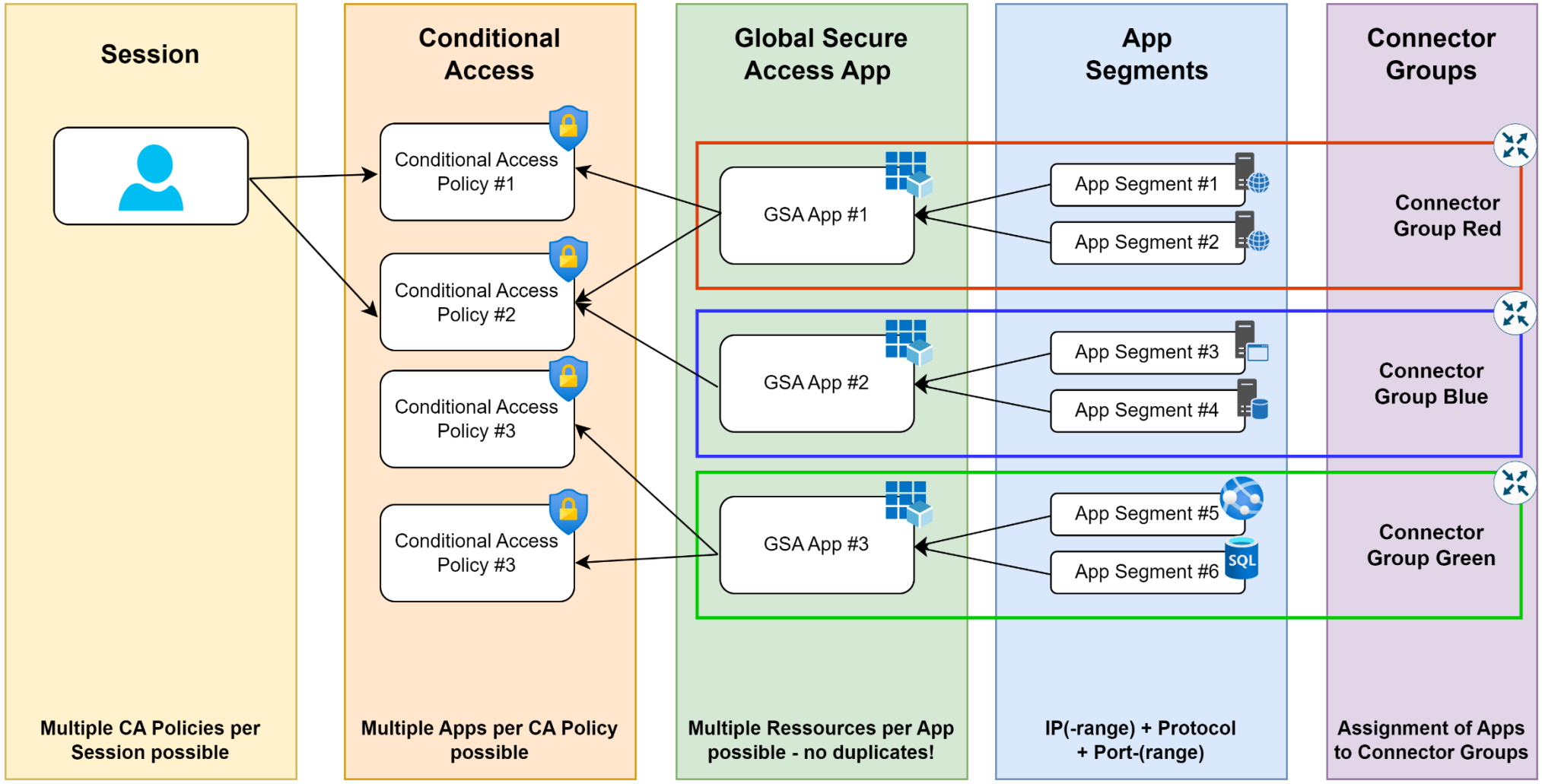
EPA Conditional Access Integration



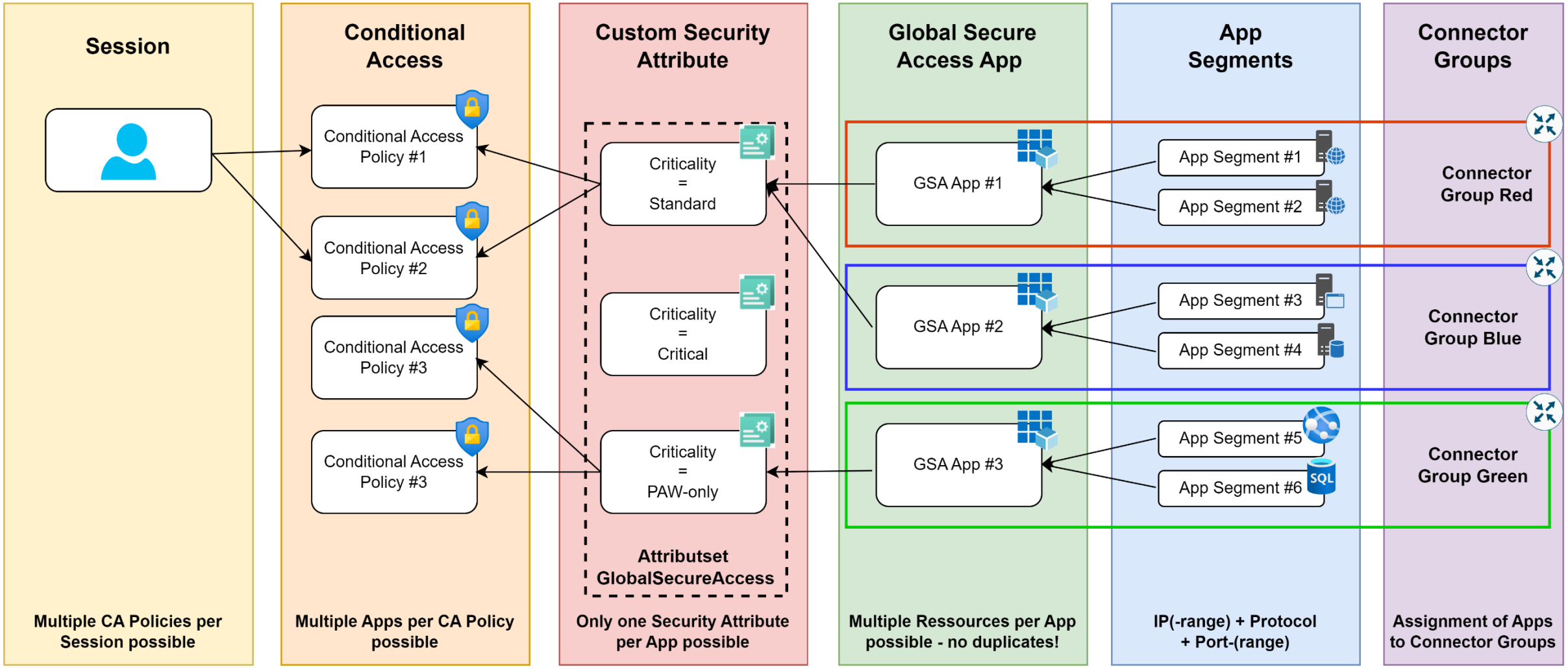
Conditional Access Integration for VPN



GSA Conditional Access Integration



Custom Security Attribute Extension



Step-up auth for specific app segments

Home > Conditional Access | Policies >

EPA 1 - Require YubiKey for Admin Access

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

EPA 1 - Require YubiKey for Admin Access

Assignments

Users or workload identities

Specific users included and specific users excluded

Target resources

1 app included

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

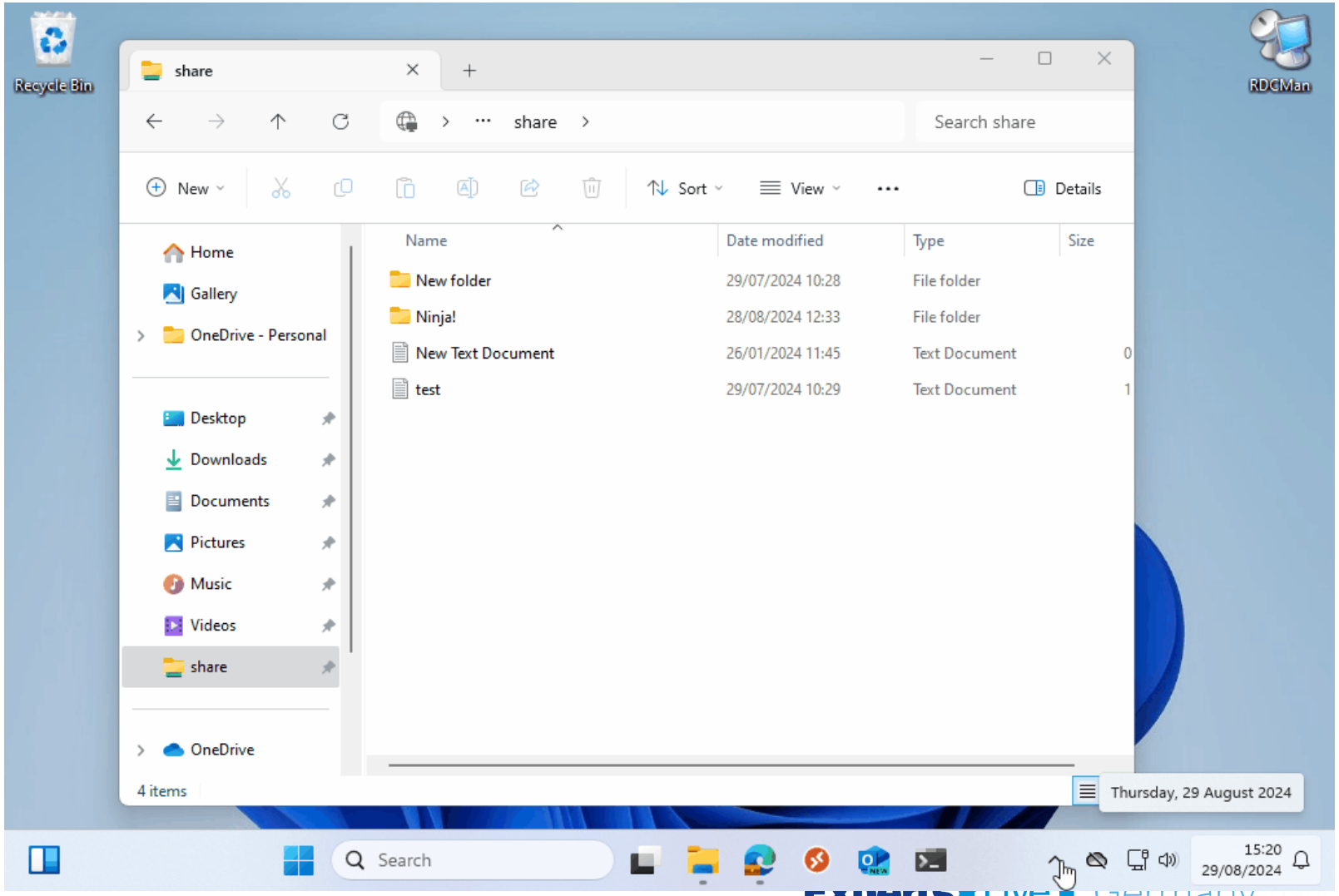
Sign-in frequency - Every time

Grant

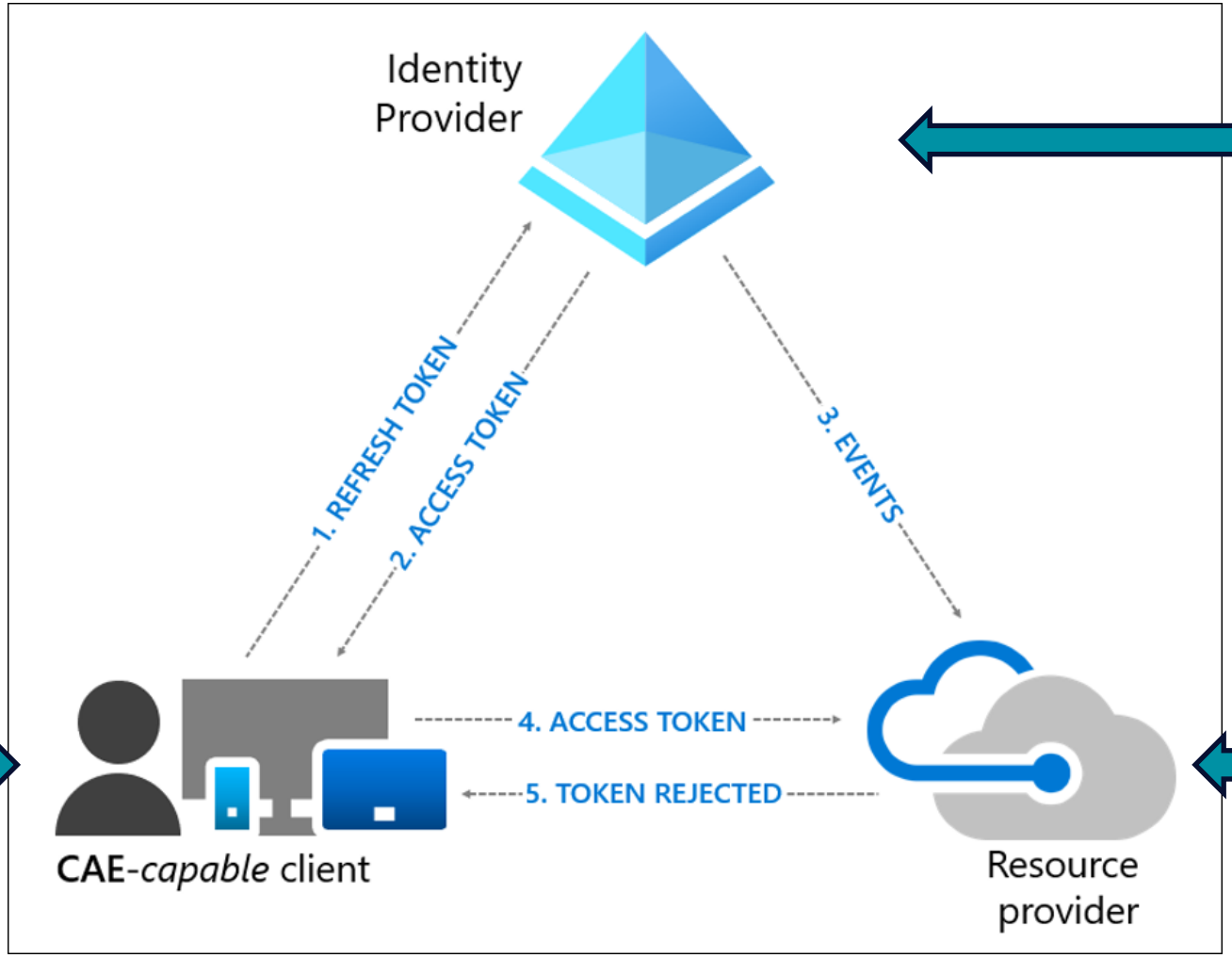
Control access enforcement to block or grant access. Learn more

- Block access
- Grant access

- Require multifactor authentication
- "Require authentication strength" cannot be used with "Require multifactor authentication". Learn more
- Require authentication strength: YubiKey Only
- To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more
- Require device to be marked as compliant
- Require Microsoft Entra hybrid joined device
- Require approved client app — See list of approved client apps
- Require app protection policy — See list of policy protected client apps



Universal Continuous Access Evaluation



Entra ID

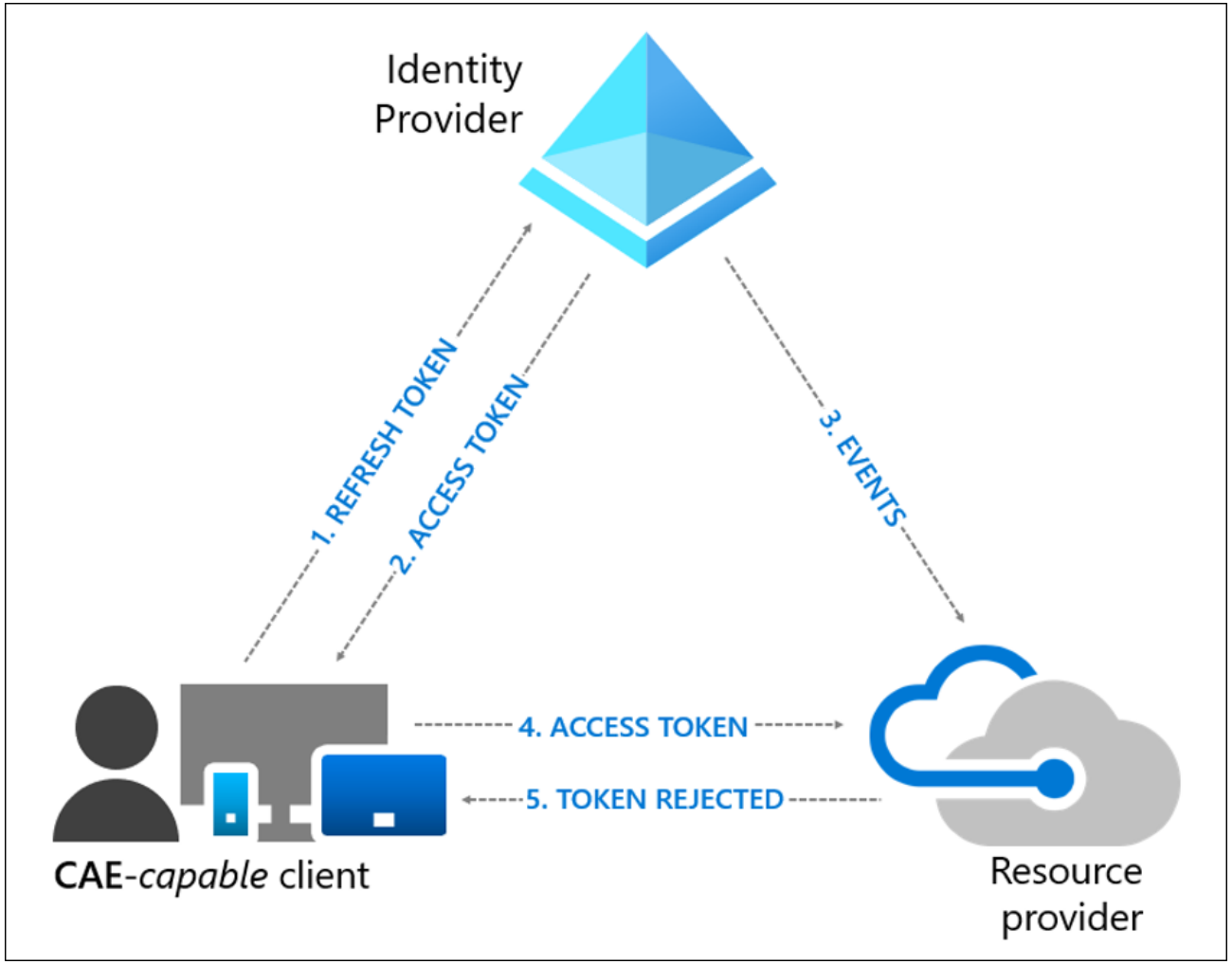
GSA Client

Global Secure Access

Universal Continuous Access Evaluation

Trigger events for Universal CAE:

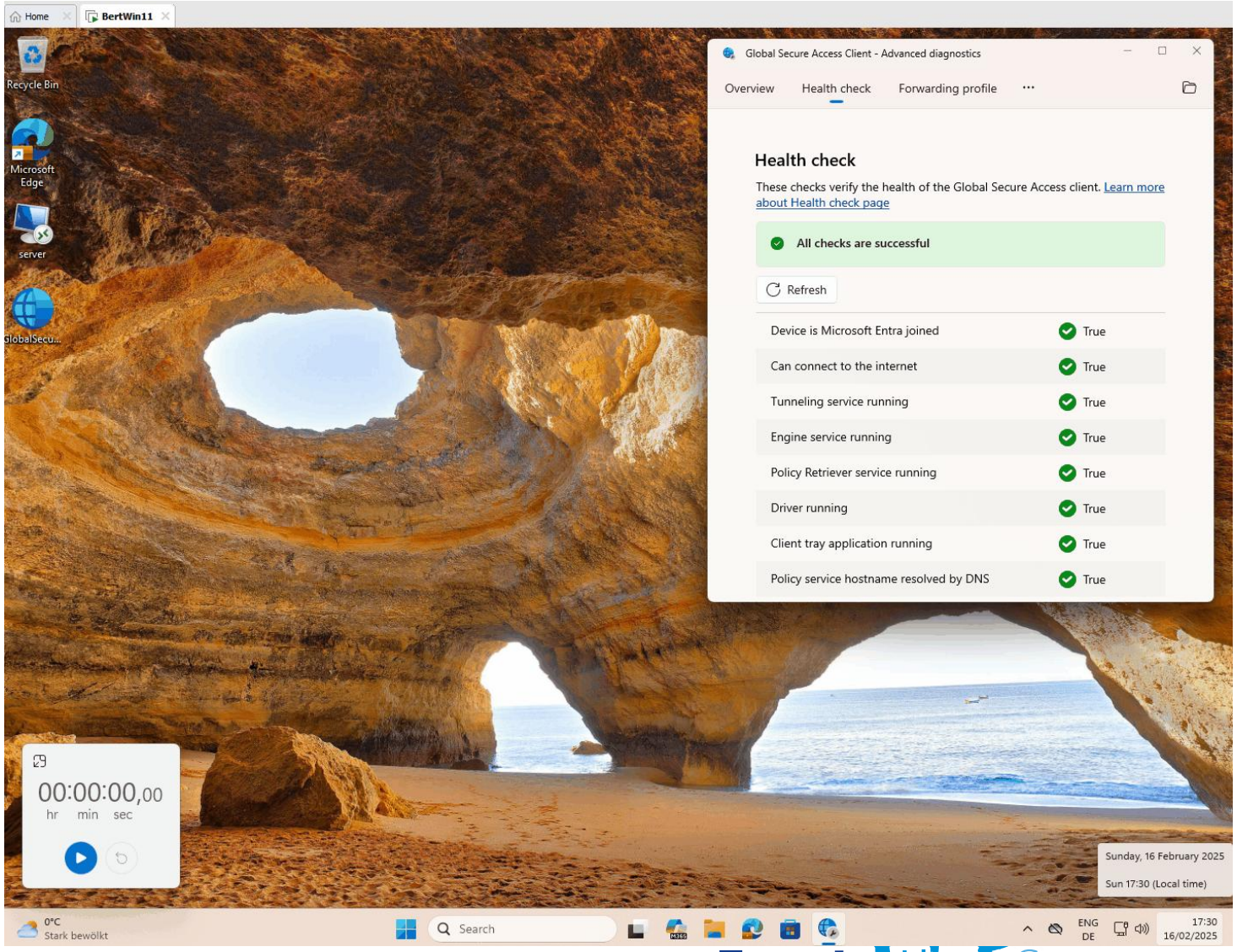
- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection



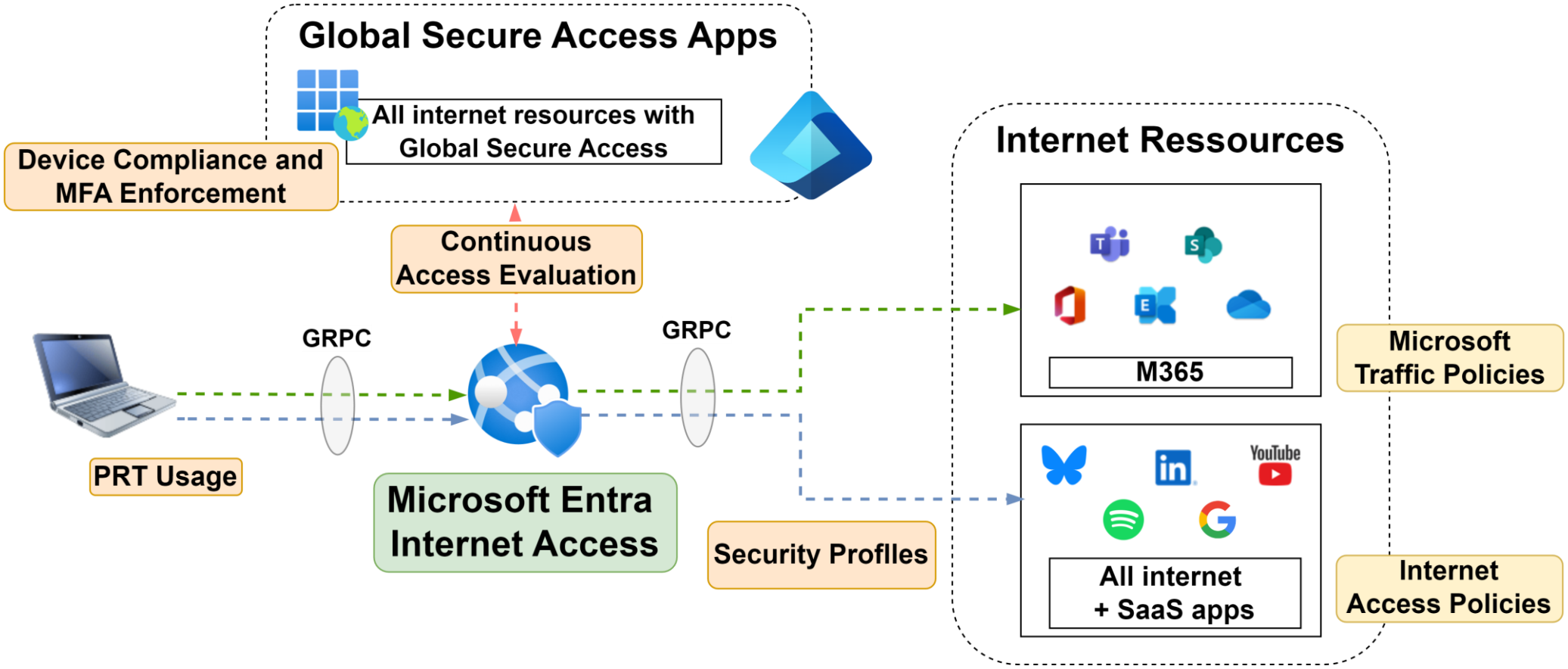
Universal Continuous Access Evaluation

Trigger events for Universal CAE:

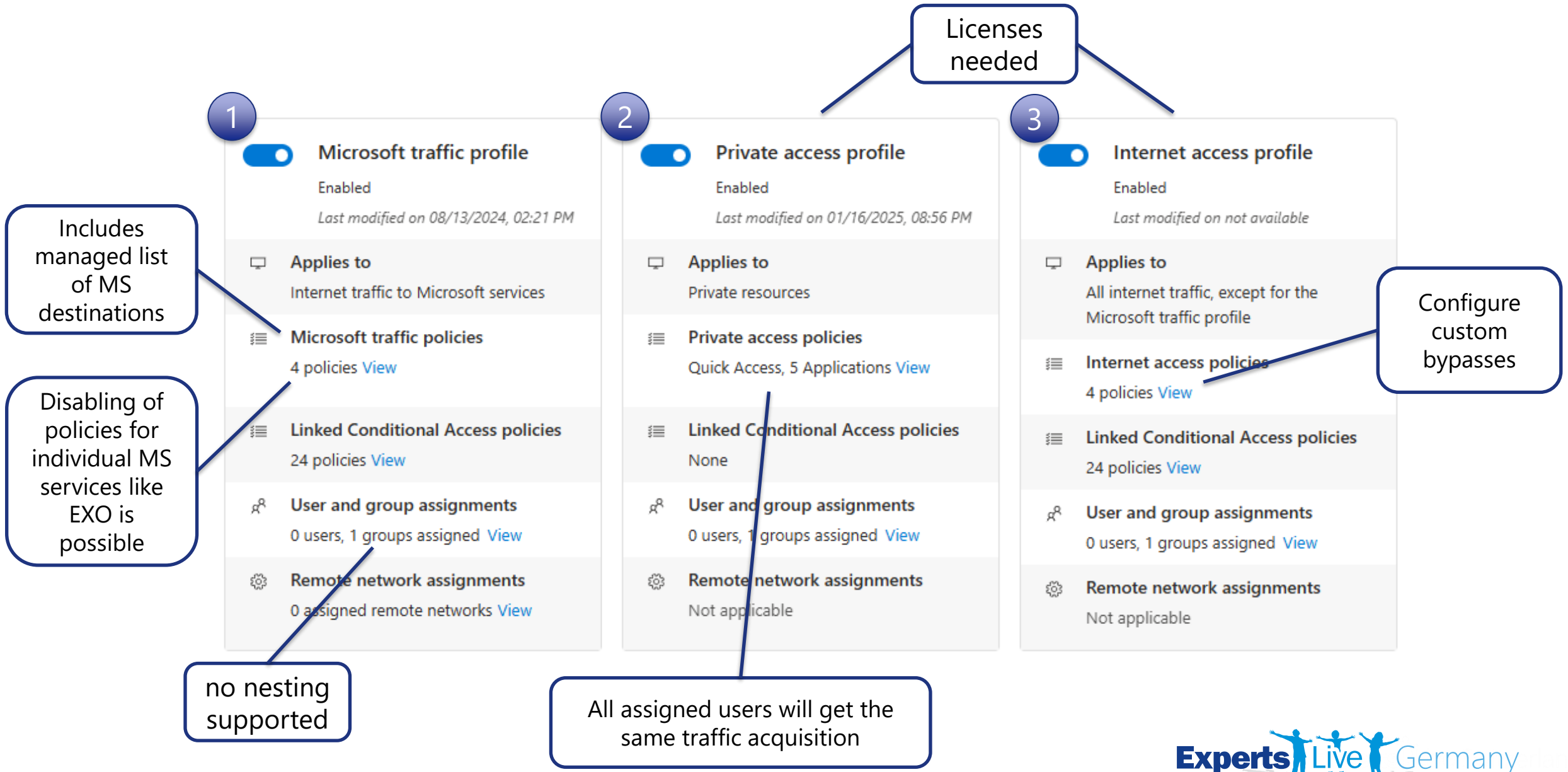
- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection



Entra Internet Access

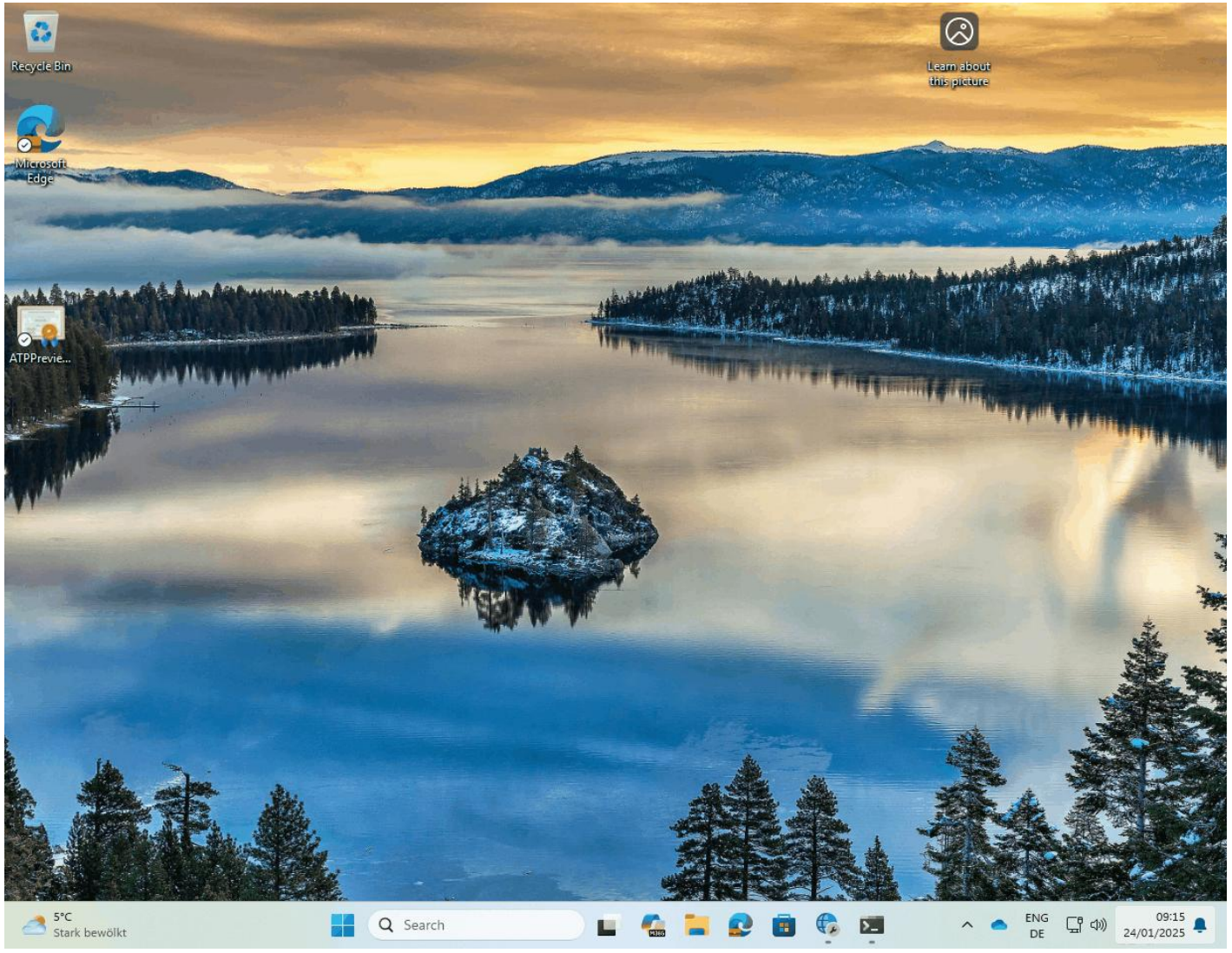


Side note: traffic acquisition



Experts Live Germany

Using the Webfilter in Entra Internet Access



Name *

EIA 1 - Apply Basic Employee Web Filtering

Assignments

Users or workload identities

Specific users included

Target resources

All internet resources with Global Secure Access

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

Conditional Access Network Control selected

Select what this policy applies to

Resources (formerly cloud apps)

Include Exclude

- None
- All internet resources with Global Secure Access
- All resources (formerly 'All cloud apps')
- Select resources

Use Global Secure Access security profile

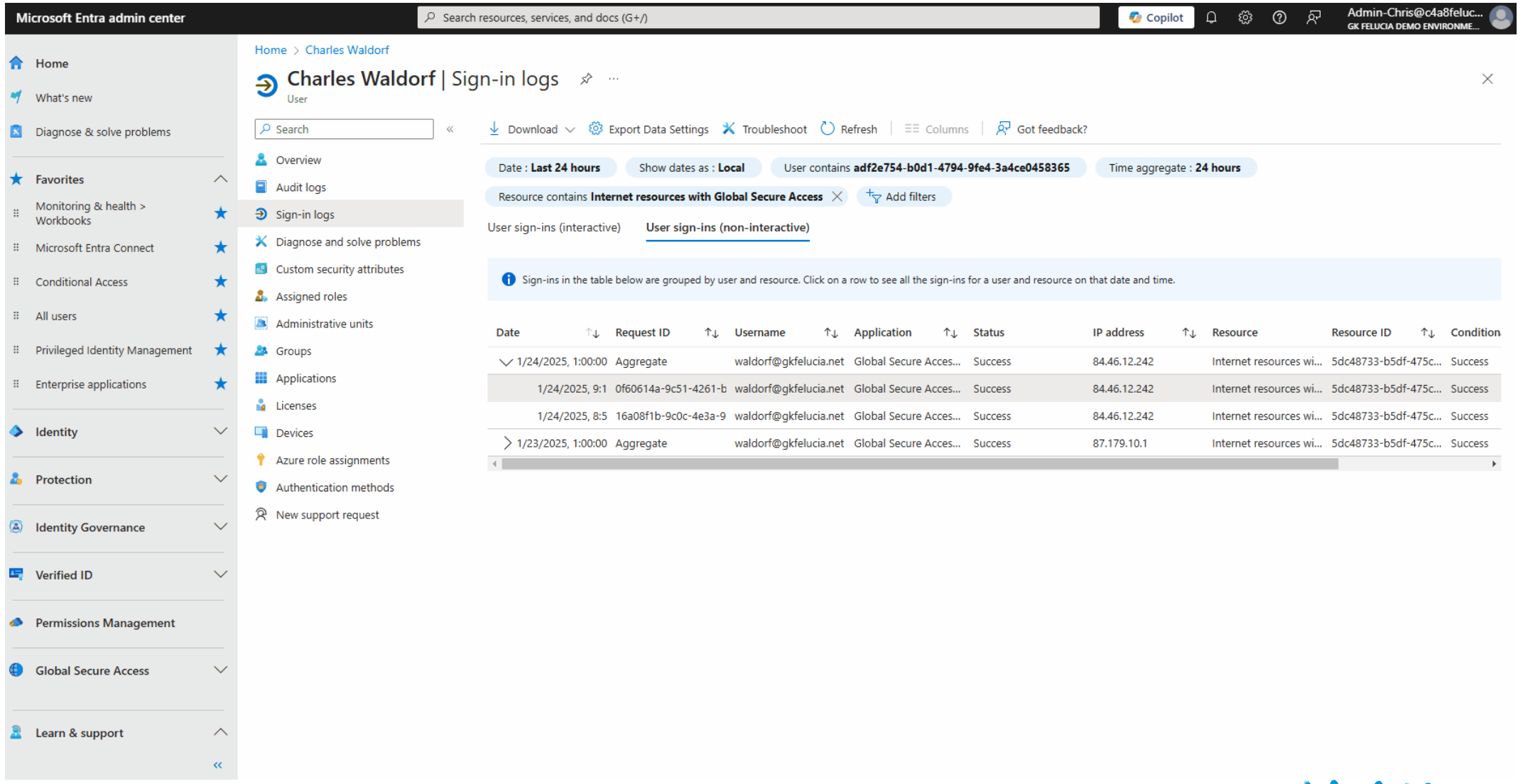
Basic Employee Profile

IT Guys Profile

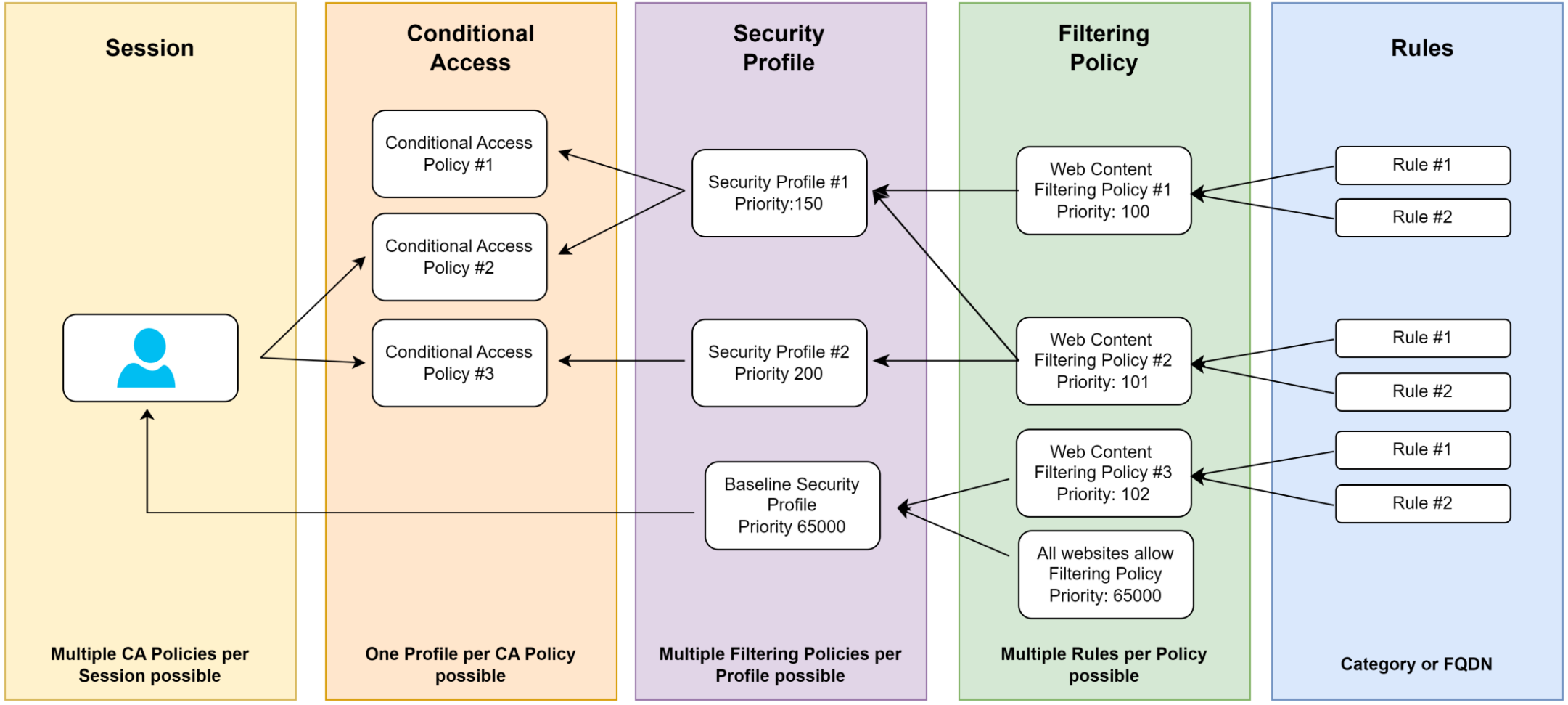
Basic Employee Profile

Experts Live Germany

Using the Webfilter in Entra Internet Access

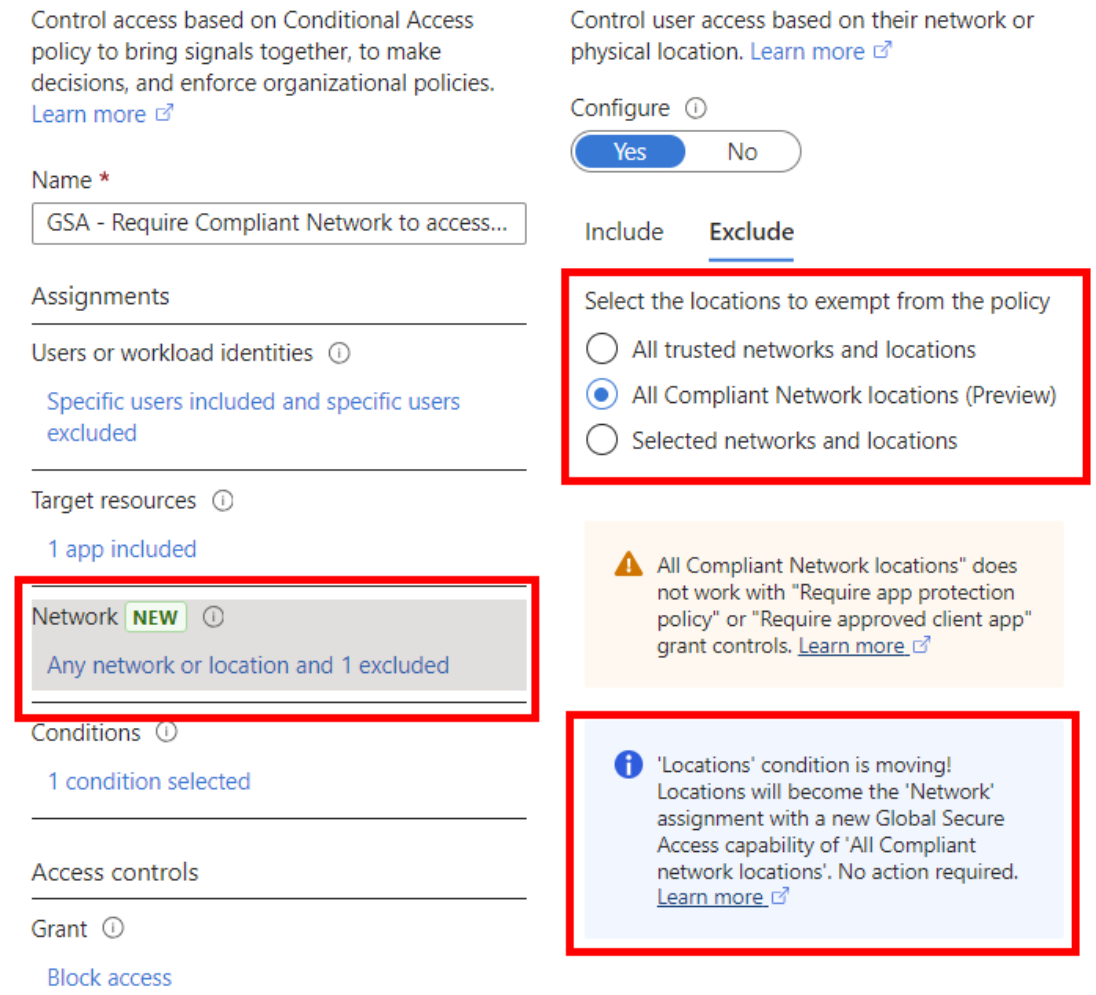


EIA Conditional Access Integration

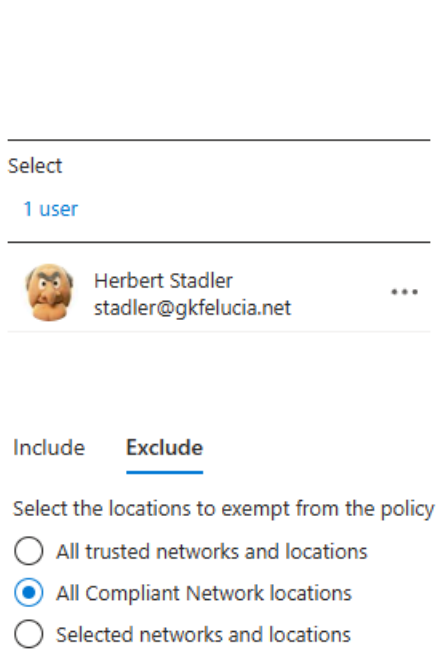


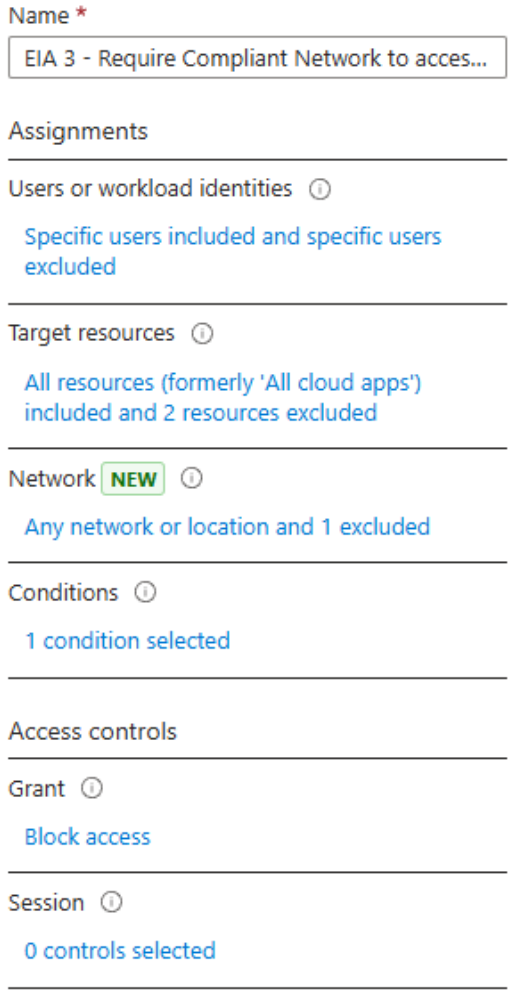
“Compliant Network” Condition

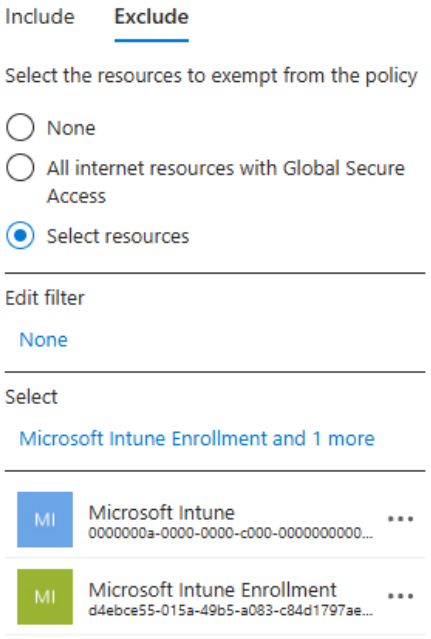
- Reasonable policy:
  - “Require Compliant Network to access Cloud Apps”
- Incompatible with
  - Require app protection policy
  - Require approved client app
  - Use Global Secure Access security profile



The Compliant Network Condition





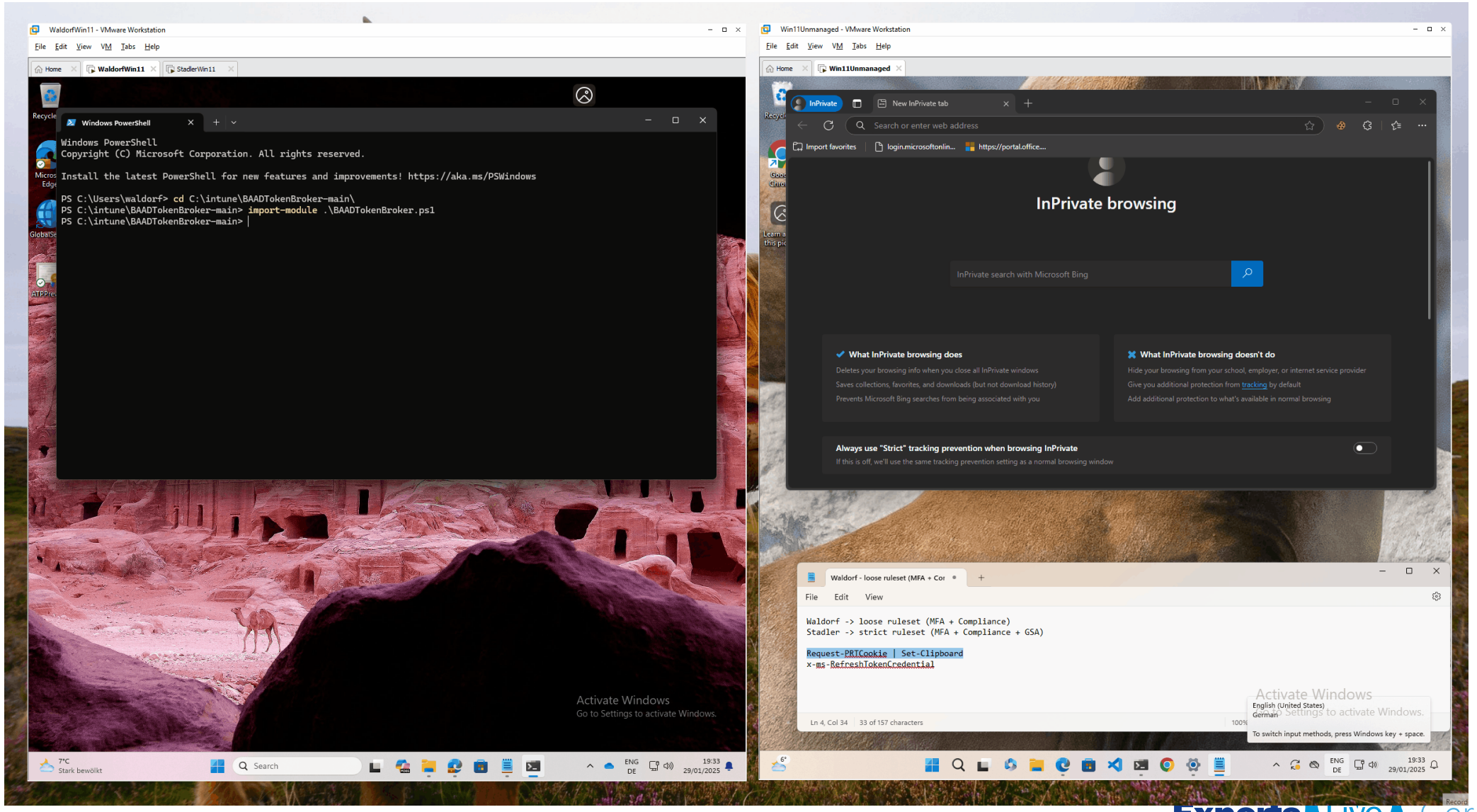


Examples for additional exclusions:

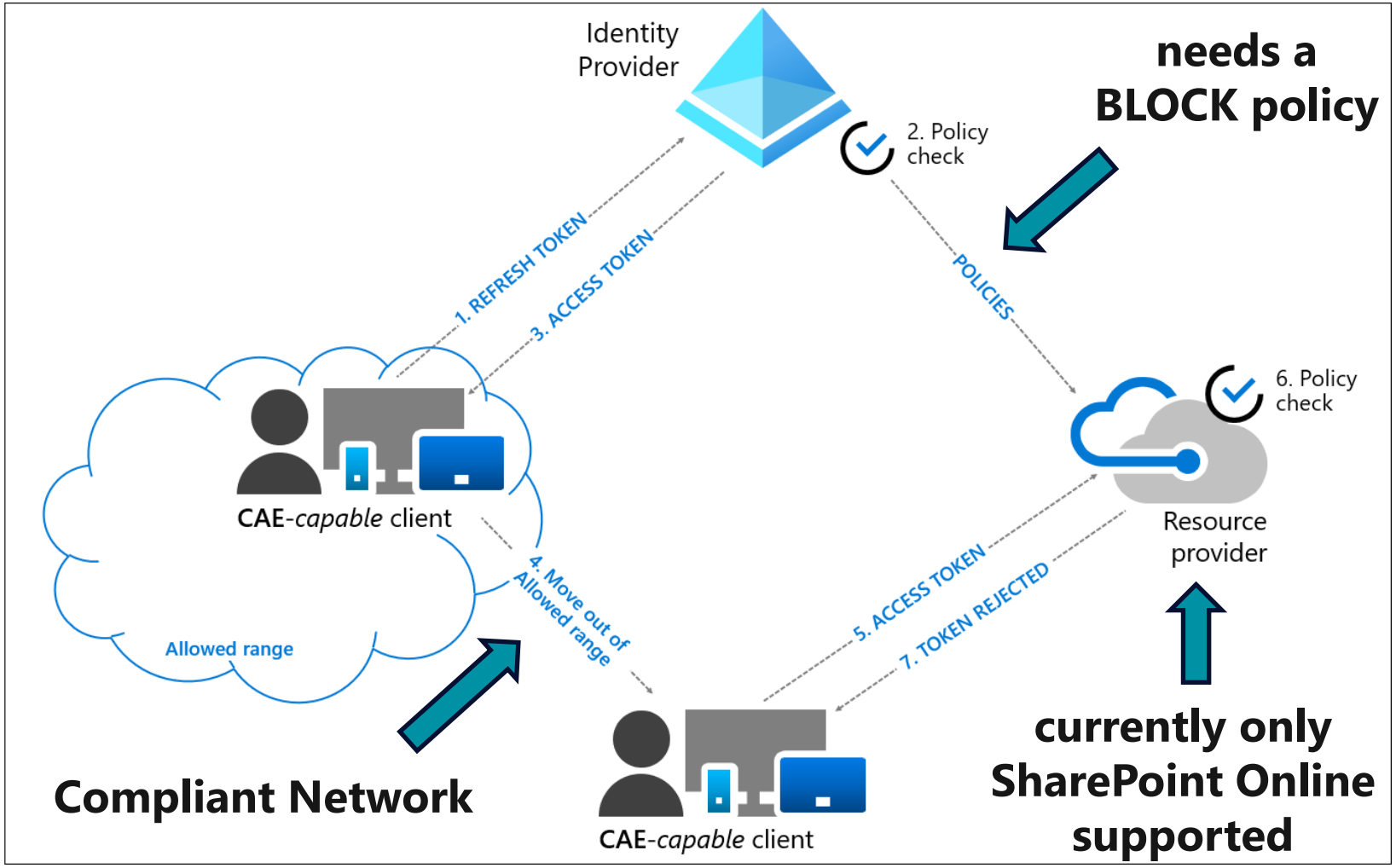
Azure Windows VM Sign-In

Azure Virtual Desktop
Windows 365
Microsoft Remote Desktop
Windows Cloud Login

The Compliant Network Condition

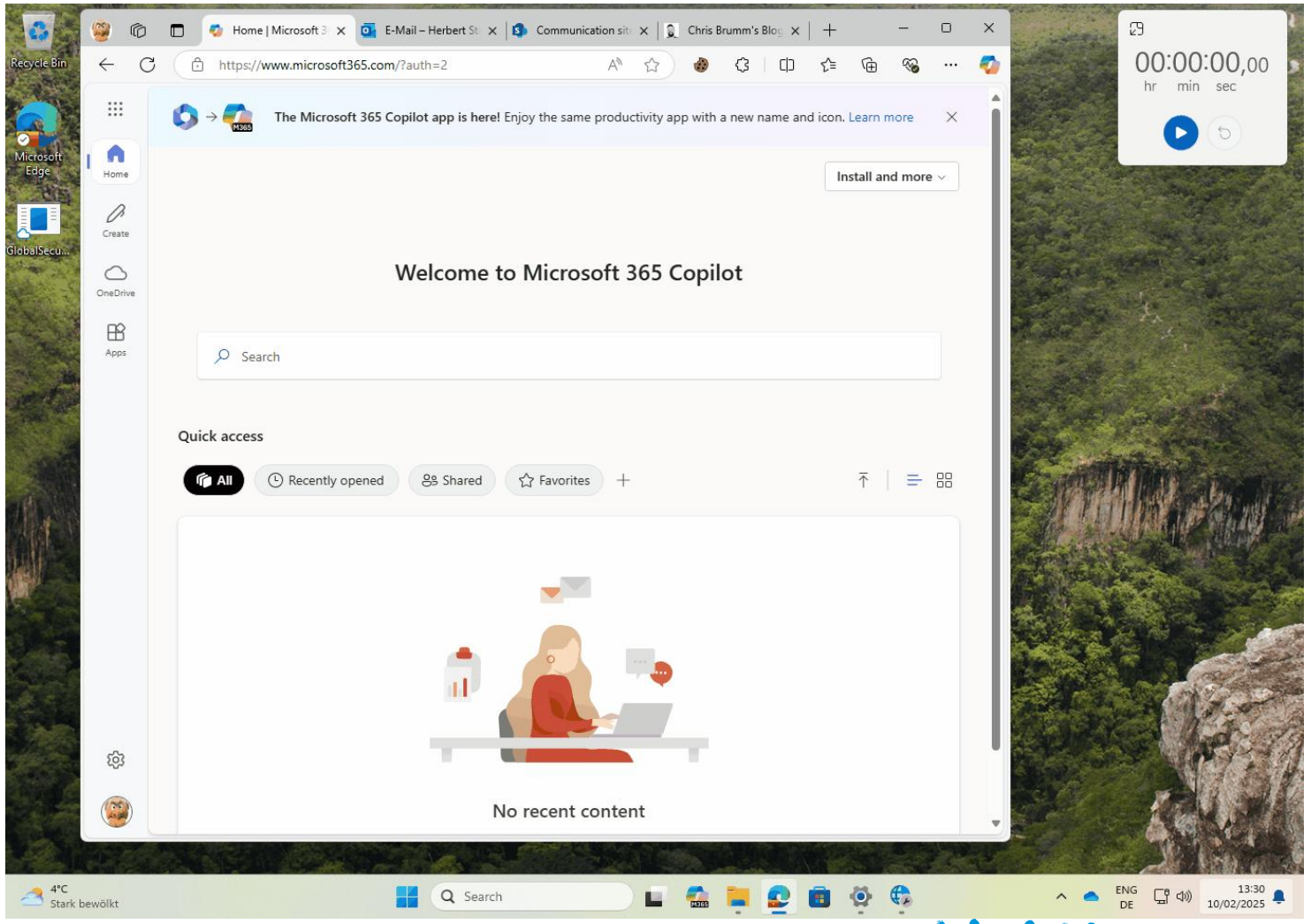


GSA Compliant Network and CAE



Leaving the compliant network

- Data plane enforcement works with services that support Continuous Access Evaluation (CAE) - **currently, only SharePoint Online**.
- With apps that support CAE, stolen access tokens that are replayed outside your tenant's compliant network will be rejected by the application **in near-real time**.
- Without CAE, a stolen access token will last up to its full lifetime (default 60-90 minutes).



Vielen Dank an unsere Sponsoren!

Diamond

bluechip
CREATING COMPUTERS.

AMD

Fsas Technologies
a Fujitsu company

Platinum

TD SYNNEX

robopack
empowered by SOFTWARE CENTRAL

DELL Technologies

ConStraight

RECAST SOFTWARE
presented by VANQUISH

Gold

control UP

SVA

DataON

CODETWO

Mainzer Datenfabrik

ARROW

Experts Live Germany

Bitte gebt uns euer Feedback!

Feedback geben und Geschenk mitnehmen

Vielen Dank!

Experts Live Germany