



Leveraging Global Secure Access to fortify Hybrid Identity Management

Christopher Brumm
Cyber Security Architect



Christopher Brumm

Cyber Security Architect @ glueckkanja AG

From Hamburg, Germany

Focused on Identity + Security

Microsoft Security MVP Identity & Access

Certified Information Systems Security Professional

My Blog

chris-brumm.com





Agenda

- How to attack a hybrid identity infrastructure
- Use Entra Private Access to protect your Active Directory environment
- Use Entra Internet Access to prevent Token Replay
- Are there any logs?

How I would attack a hybrid identity infrastructure

1 VPN compromise

- CVEs at VPN Appliances
- Weak Authentication Methods
- No Managed Device / PAW Enforcement
- Weak Detection/Response Capabilities
- No Network Segmentation

2 AD compromise

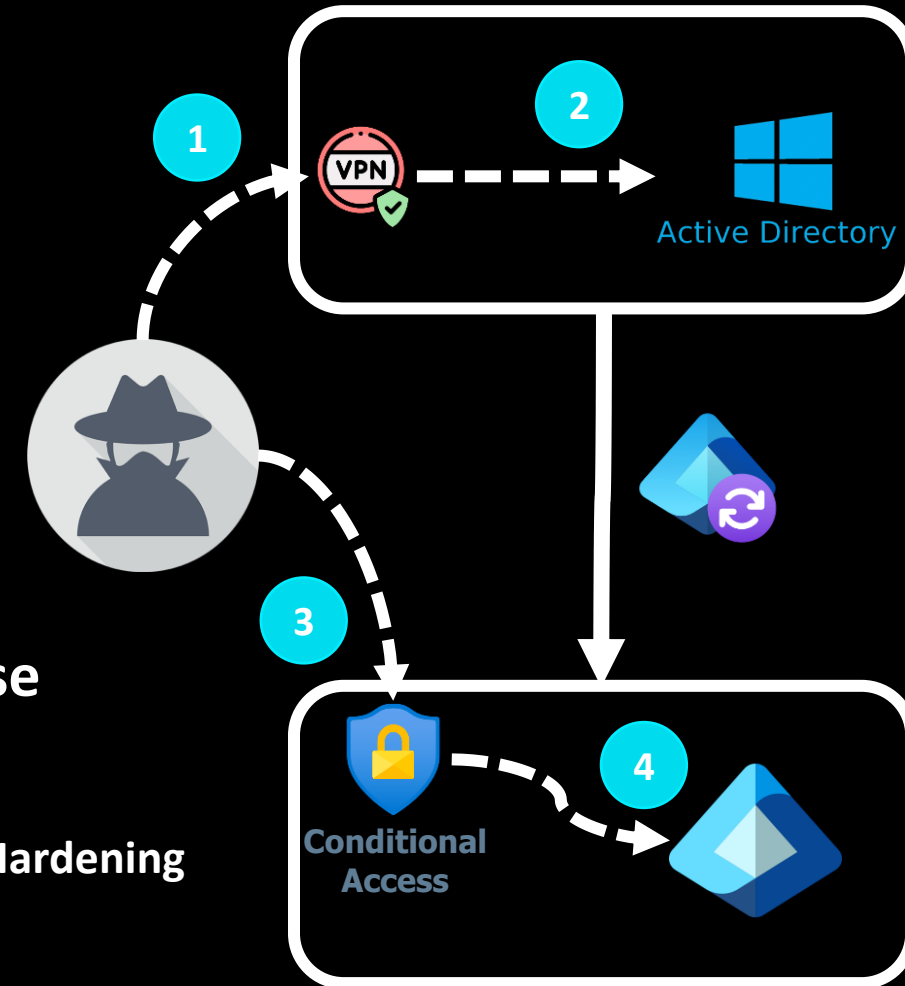
- Missing AD Tiering / Hardening
- Weak Detection / Response Capabilities
- Old Protocols

3 Conditional Access bypass

- Trusted Network Exclusions
- Weak Authentication Methods
- No Managed Device / PAW Enforcement

4 Entra ID compromise

- Seamless SSO / ADFS
- Synced Admins
- Missing Entra Tiering / Hardening
- Missing Monitoring

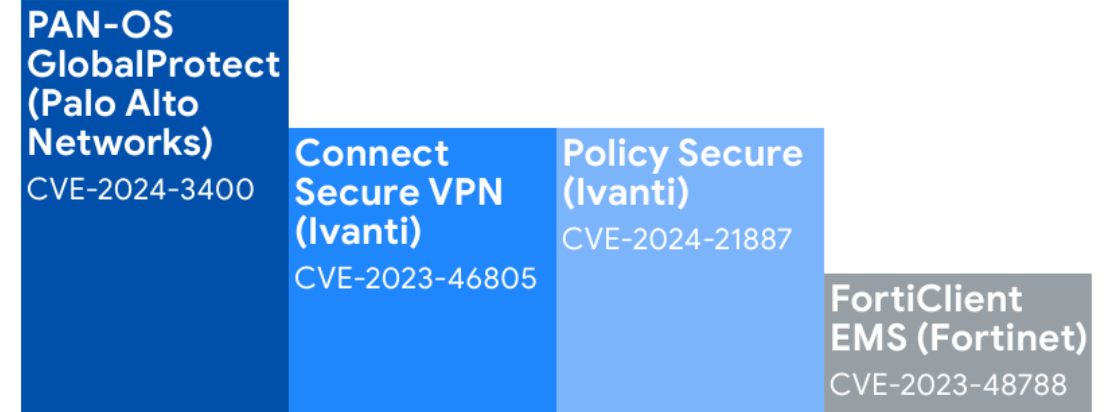




M-Trends

2025 Report

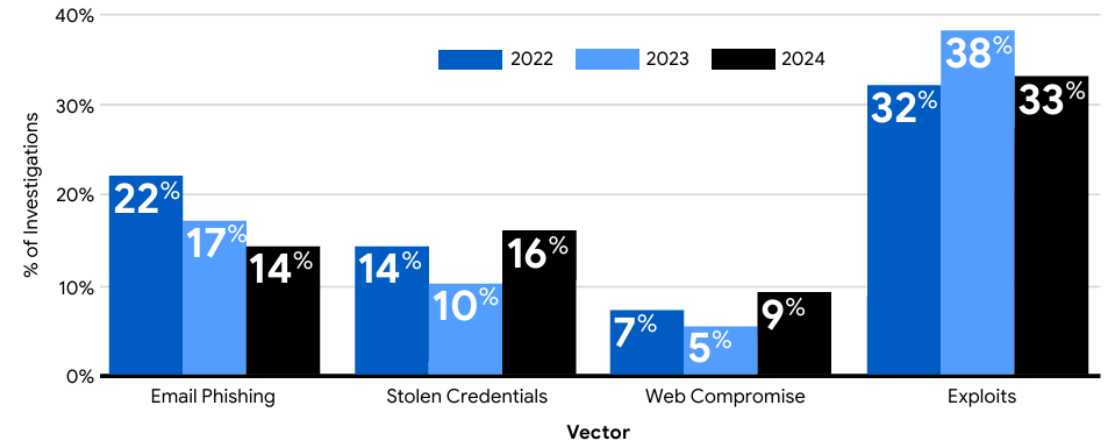
Most Frequently Exploited Vulnerabilities



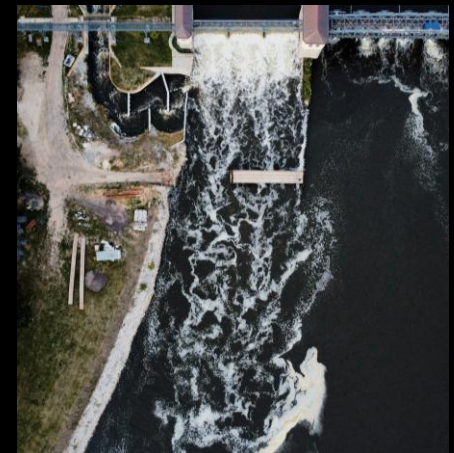
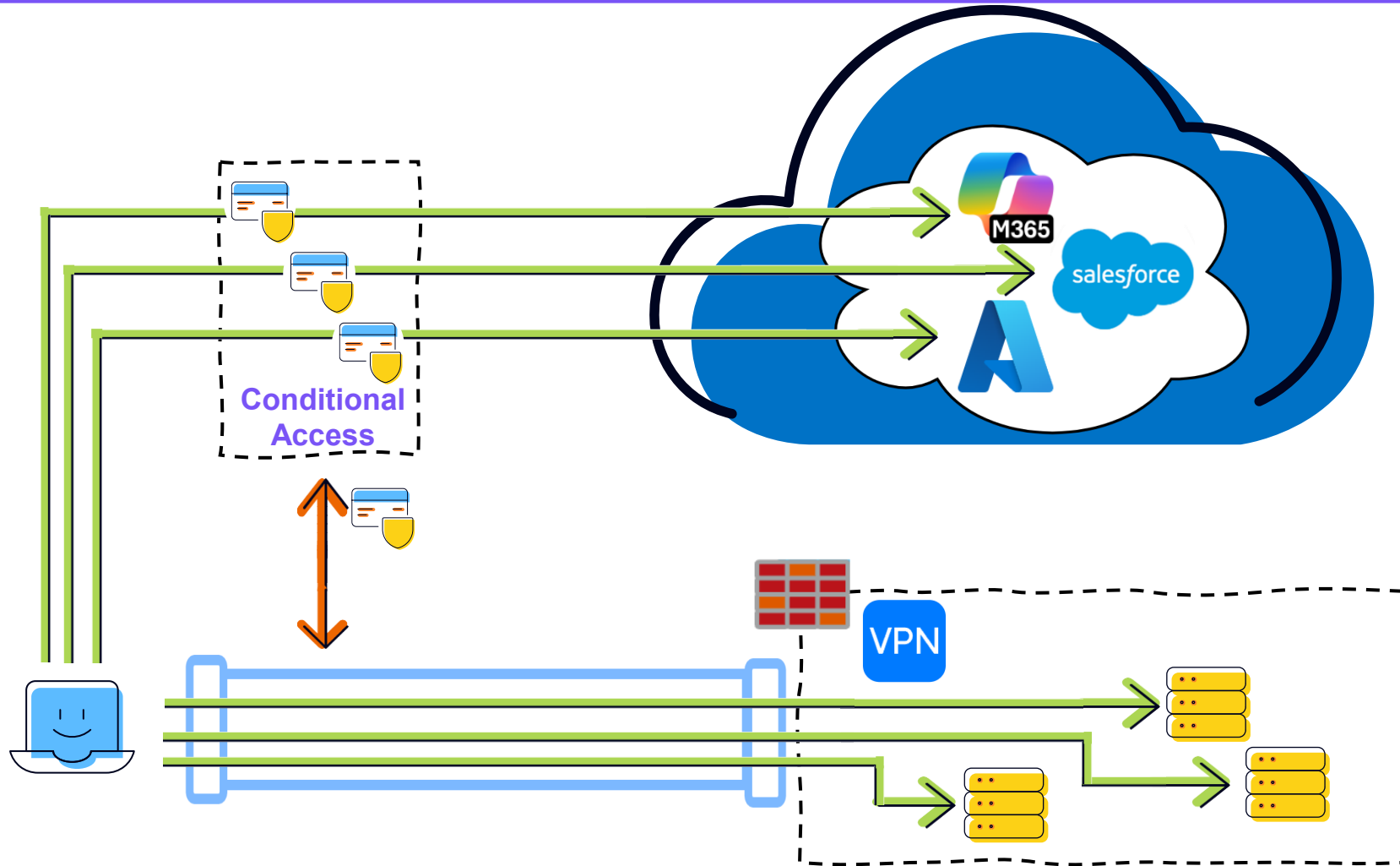
Initial Infection Vector, 2024



Phishing Declines as an Initial Infection Vector, 2022-2024



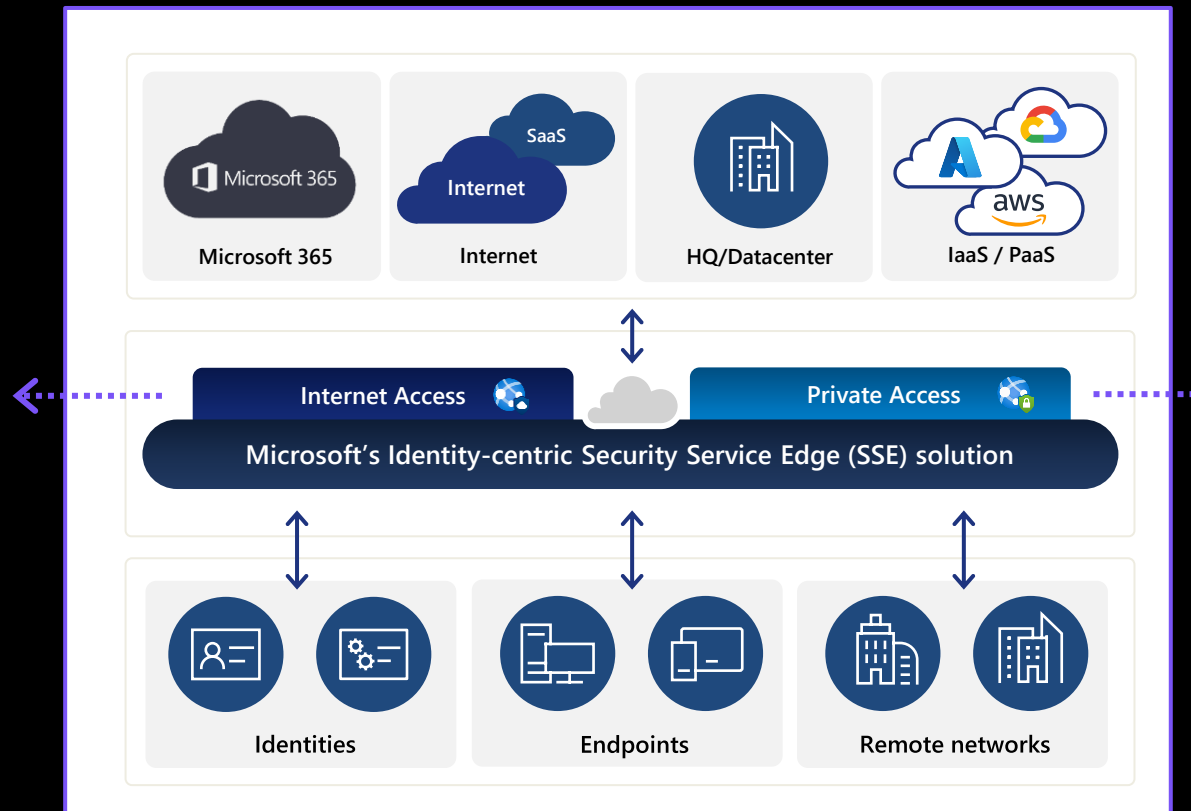
The OnPrem access control gap



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)**.



Verify explicitly



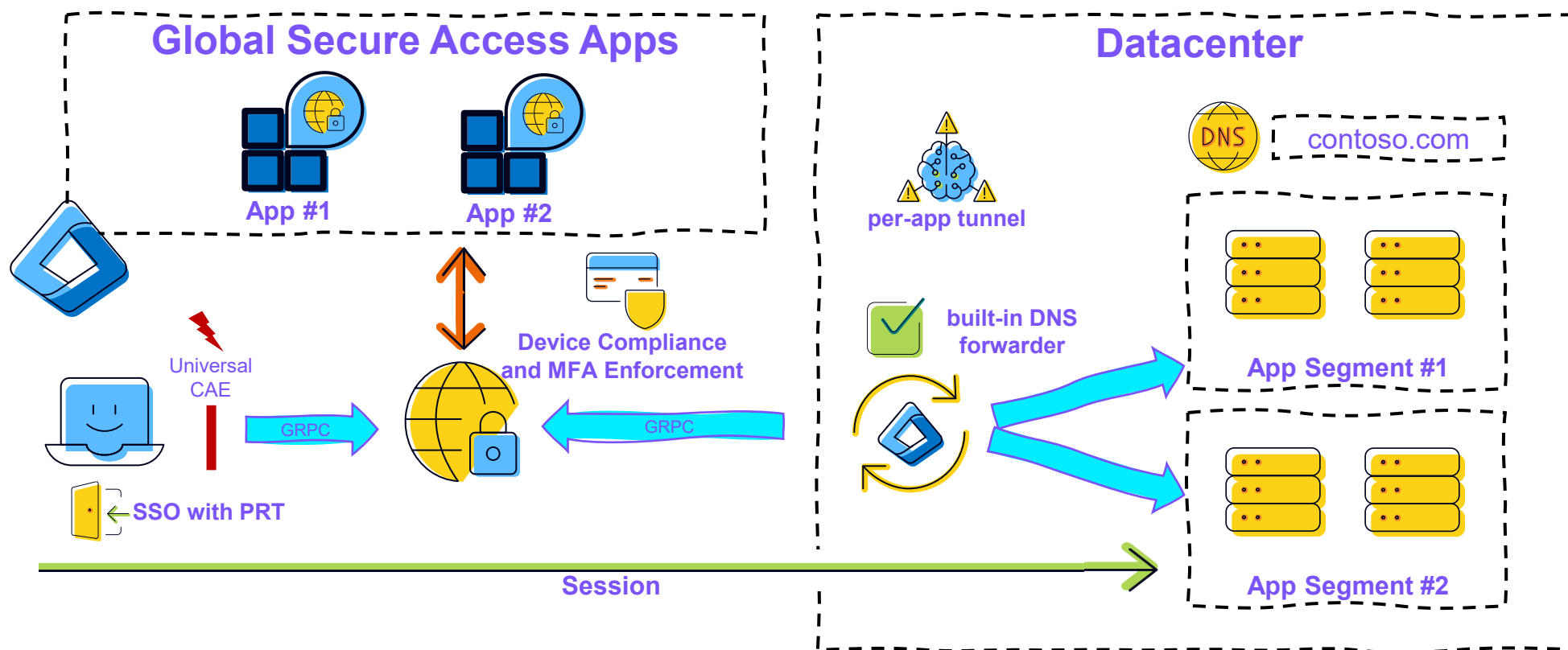
Use least privilege



Assume breach

Entra Private Access

Overview Entra Private Access



DEMO

Using Privileged Identity Management in Entra Private Access



CookieConnections - Remote Desktop Connection Manager - Sysinternals: www.sysinternals.com

FileEditSessionViewRemote DesktopsToolsHelp

CookieConnections

- gkfelucia-t0-cookie
 - DC1

DC1

Disconnected

Global Secure Access Client - Advanced diagnostics

OverviewHealth checkTraffic...

Network traffic

Collect and analyze this device's network traffic. [Learn more about Traffic page](#)

Start collectingExport CSV...

Process name != GlobalSecureAccessClient.exe

Action == Tunnel

Timestamp beginConnection statusProtocol

No data was collected yet.

Activate Windows
Go to Settings to activate Windows.

APC8
-3,08%

Search

ENG
DE

10:47
01/08/2025

Friday 1 August 2025

Fri 10:47 (Local time)

Entra Private Access App – Portal View

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

Edit filter

None

Select

QuickAccess and 3 more

- Private Access - Admin Access
478434b9-dd76-4d77-b32b-cc9348d02...
- Private Access - GKFelucia File ...
eae4a6dc-e5d5-4a05-b6a0-2c1f3bd9a11
- Private Access - SAP
47221c33-8845-47c6-a9ed-17946572fc2c
- QuickAccess
4e8c3b32-1ab6-471e-8bbc-5493140209...

Name *

EPA 1 - Require YubiKey for Admin Access

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

1 resource included

Network **NEW** ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Sign-in frequency - Every time

Private Access - GKFelucia File Service | Network access properties

Global secure access application

Overview

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups**
- Single sign-on
- Network access properties
- Custom security attributes

Security

- Conditional Access**

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Got feedback?

Global Secure Access is now generally available. Licensing requirements have been updated. [Learn more](#)

Name ⓘ *

Private Access - GKFelucia File Serv...

Connector Group ⓘ


ZTNA ▾

ⓘ We recommend at least two active connectors in selected group 'ZTNA'. [Click here to download a connector or manage your connector groups.](#)

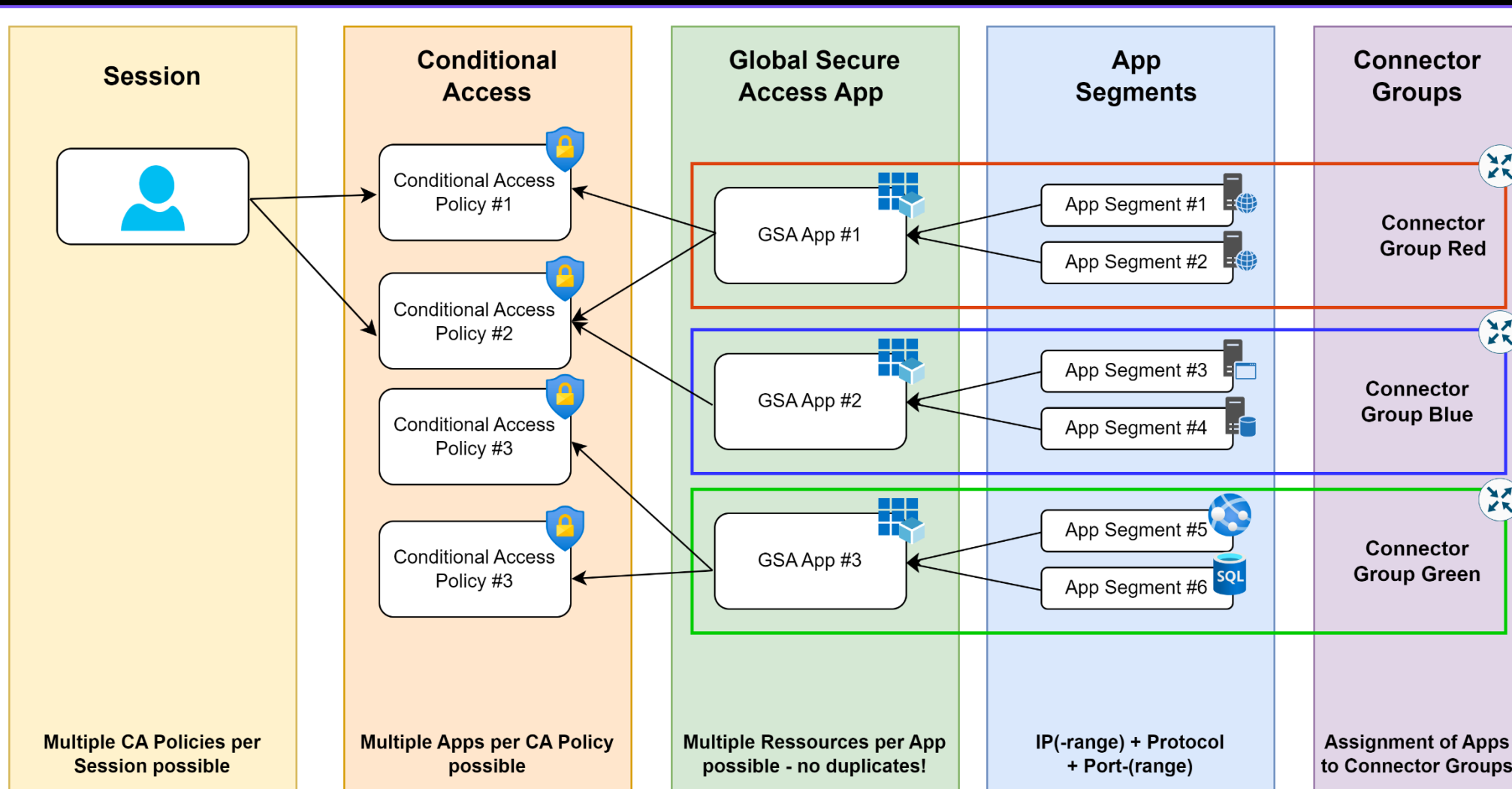
Enable access with Global Secure Access client ☒

Application Segment

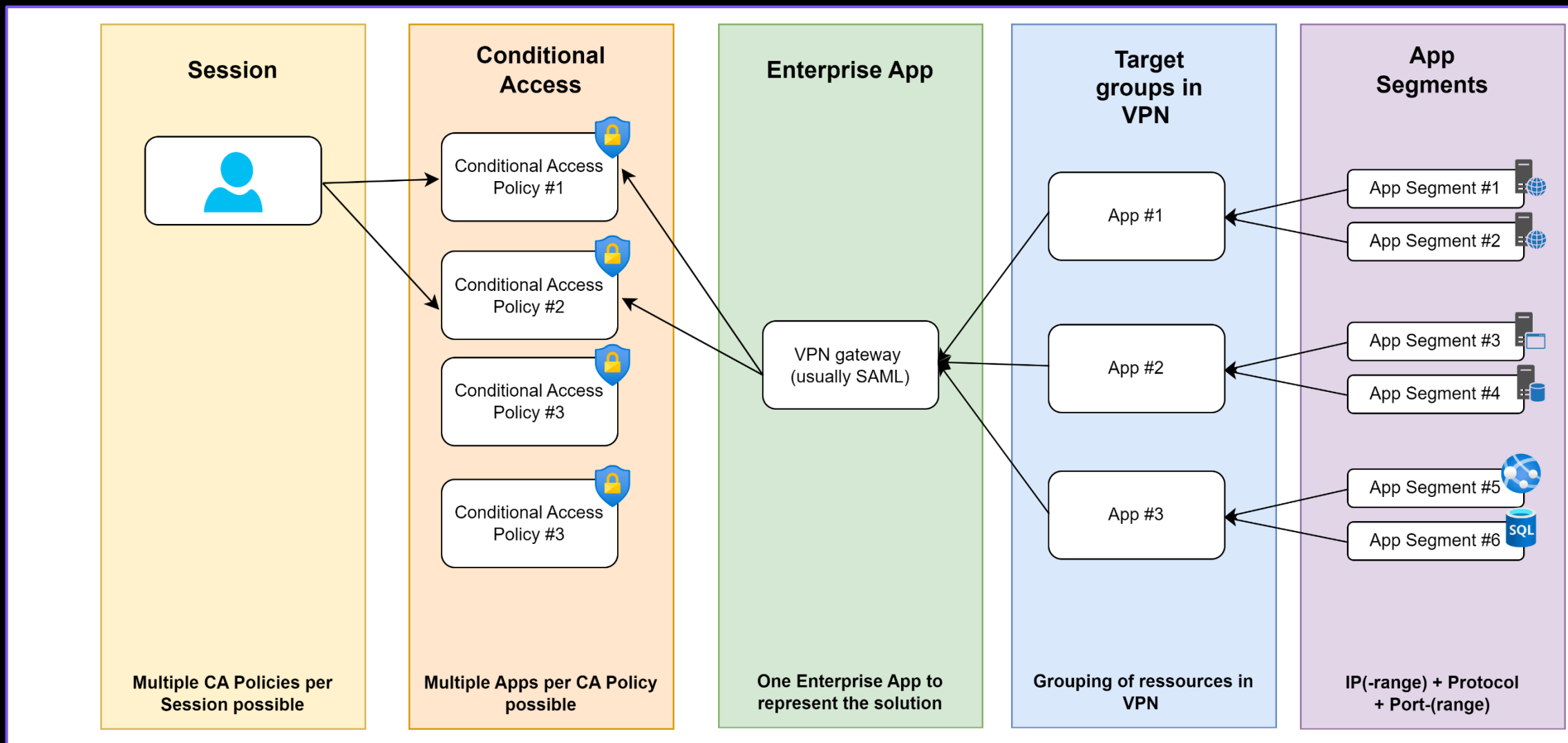
+ Add application segment

Destination type	Destination	Ports	Protocol	Status	Delete
IP address	192.168.0.21	445	TCP, UDP	Success	

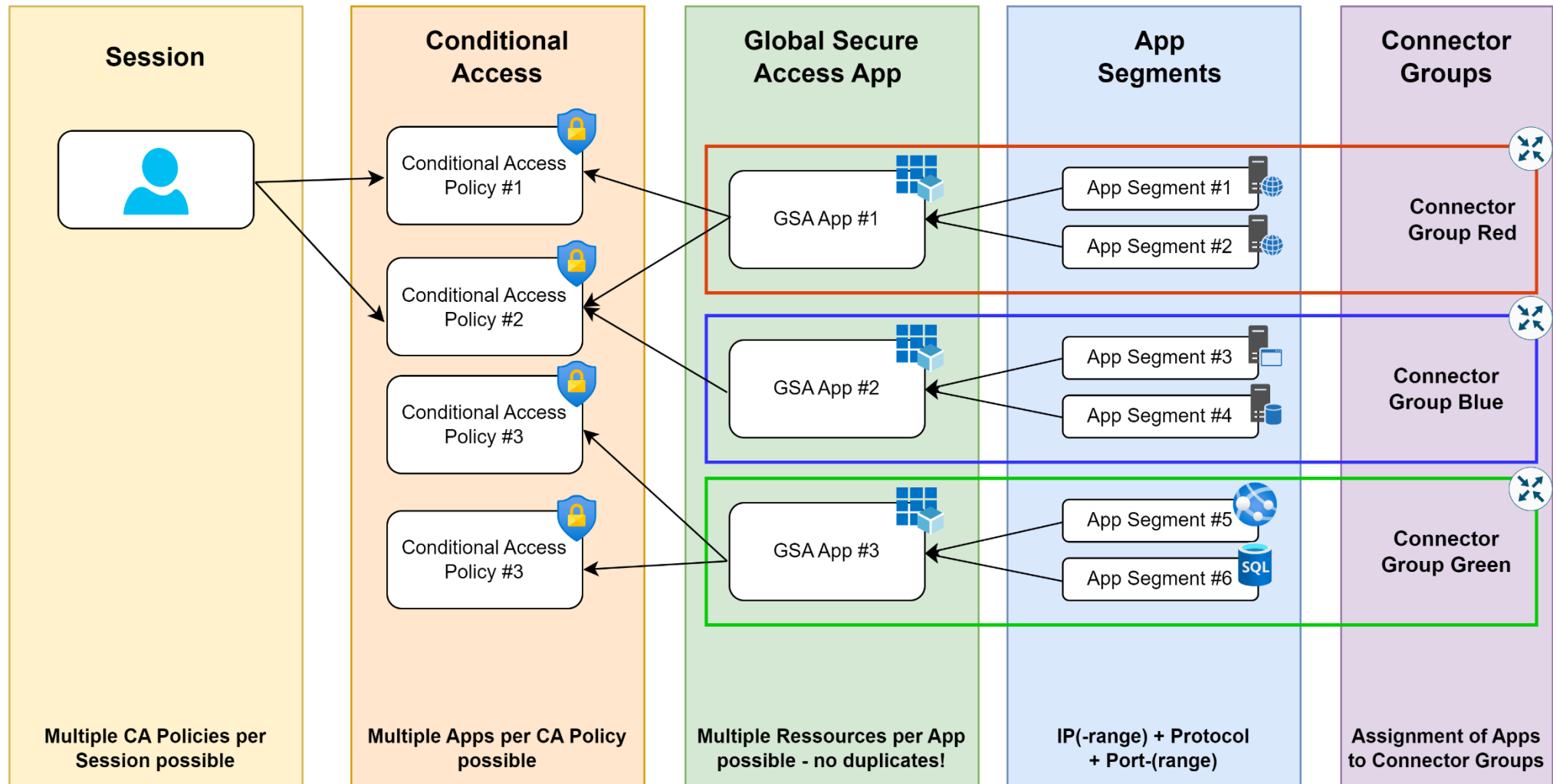
EPA Conditional Access Integration



Conditional Access Integration for VPN



EPA Conditional Access Integration



DEMO

Step-up auth for
specific app
segments

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 ⓘ

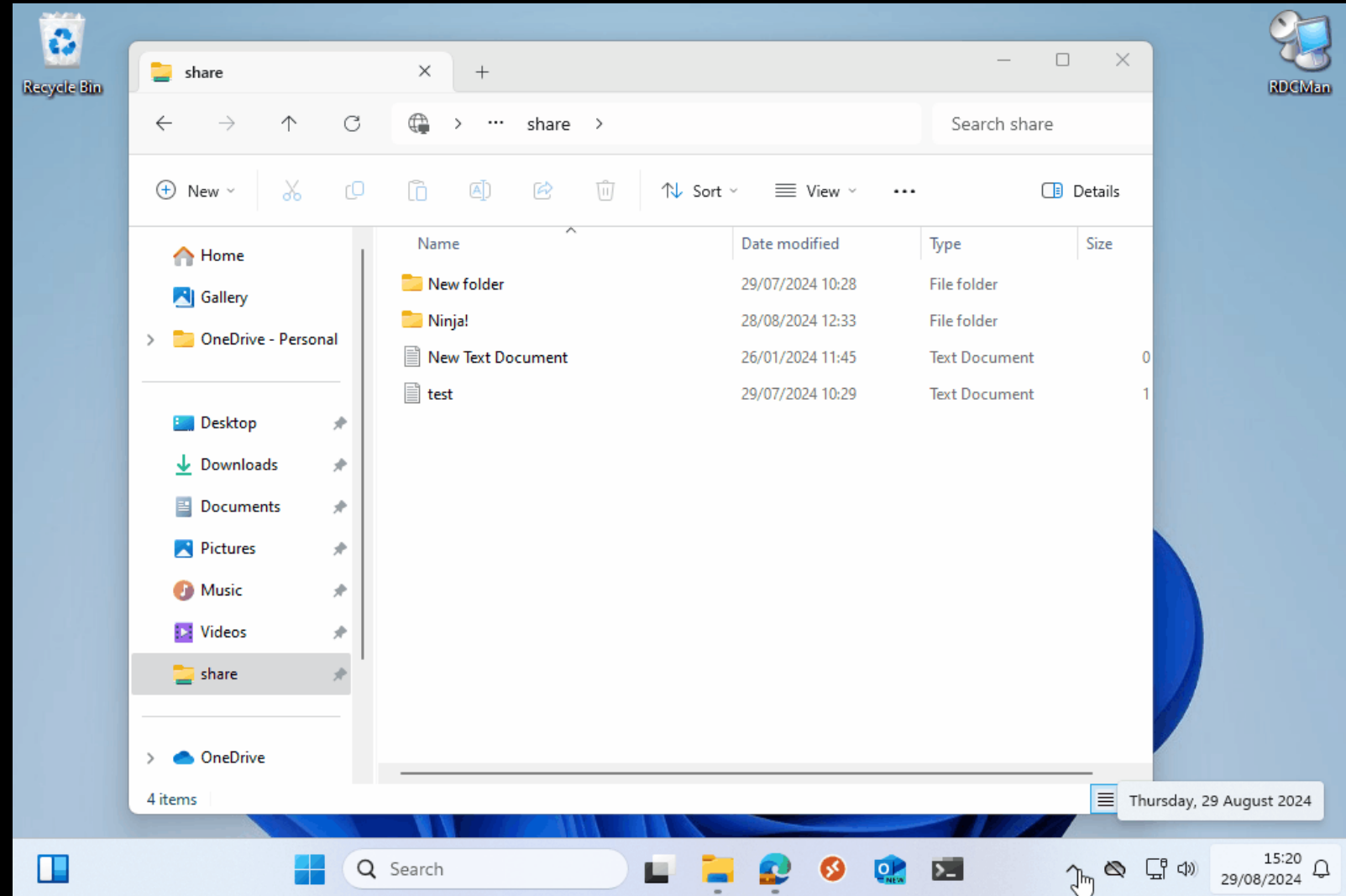
☐ Require Microsoft Entra hybrid joined device ⓘ

☐ Require approved client app ⓘ

See list of approved client apps

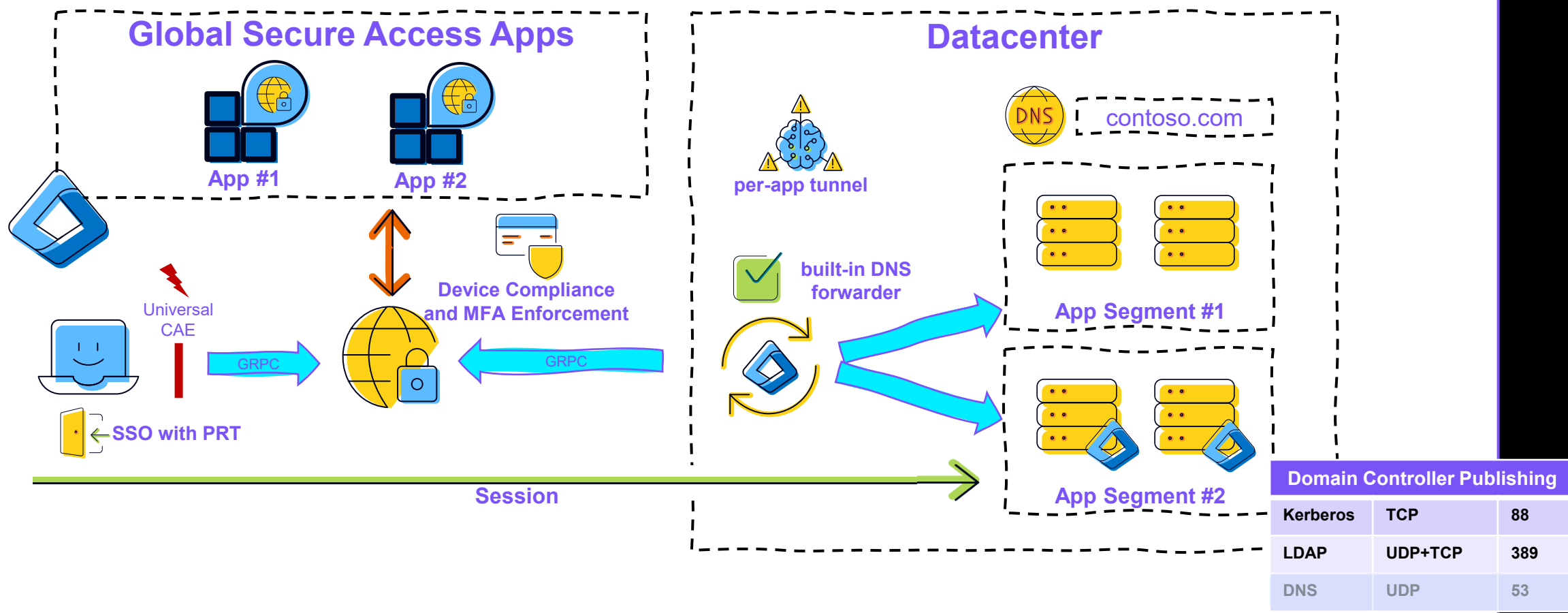
☐ Require app protection policy ⓘ

See list of policy protected client apps

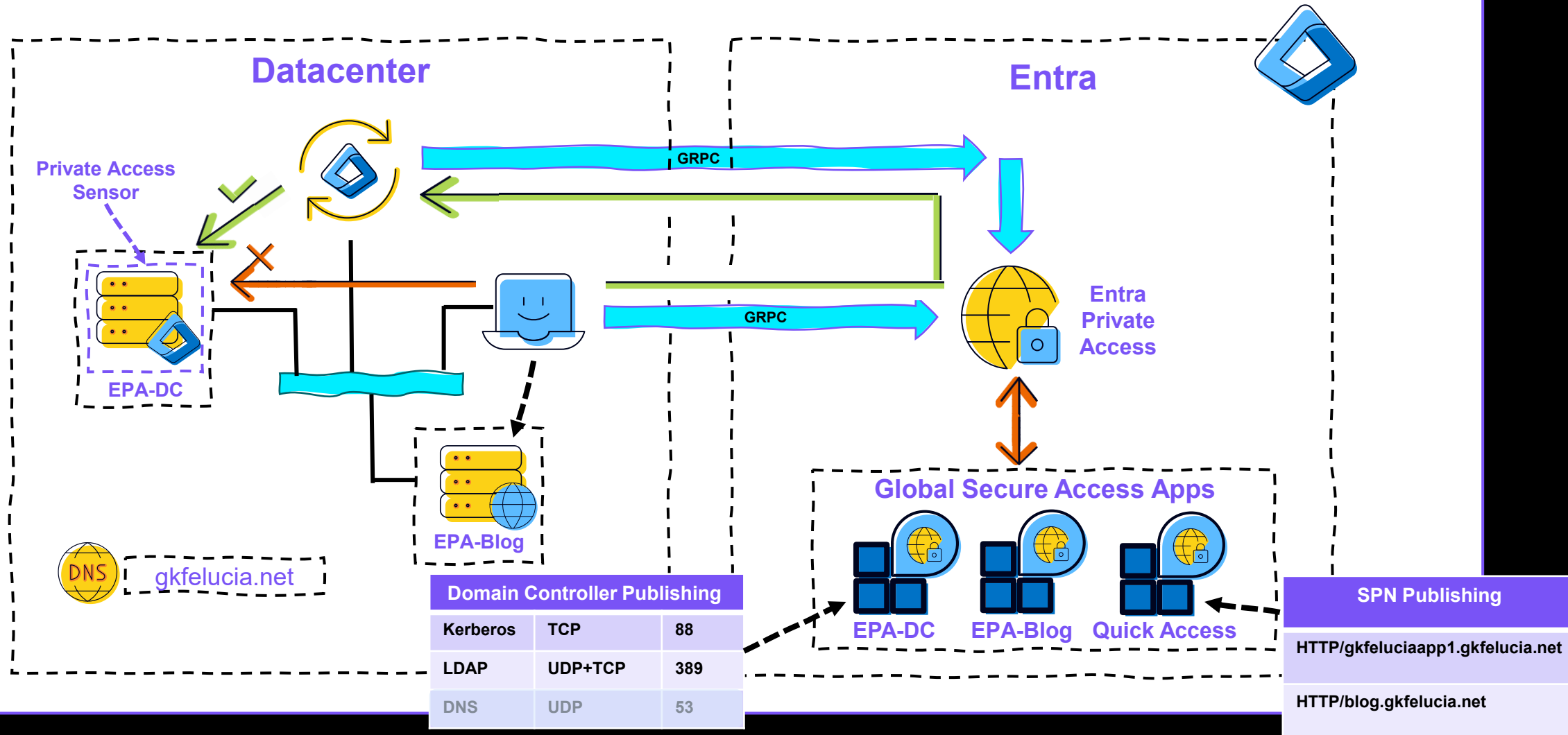


Kerberos 🍷

Using Kerberos in Private Access

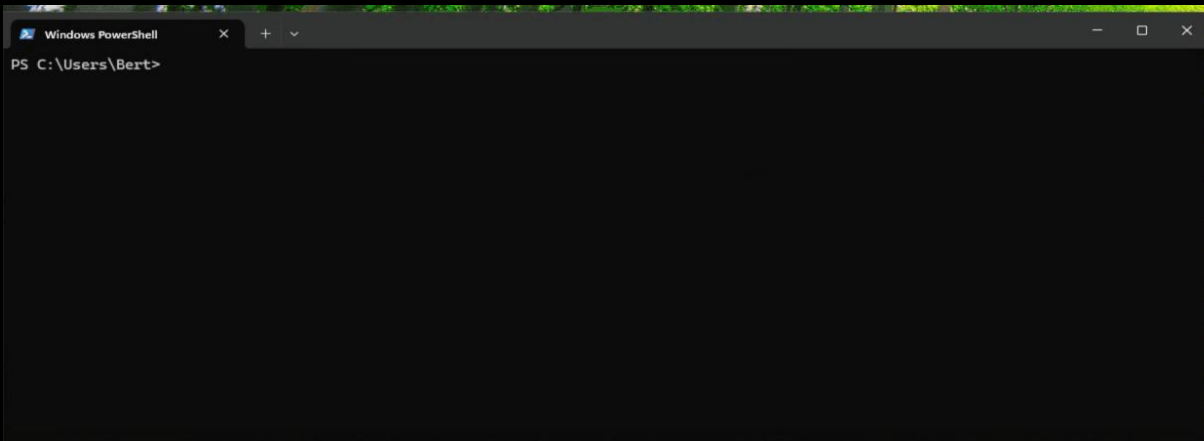


Private Access for Domain Controllers



DEMO

Private Access for Domain Controllers



Global Secure Access

Connections

Troubleshooting

Bert

Settings

Connections

Status

Private access disabled

Private Access is disabled by user

Organization:

Channels

Private

Disabled

Enable

Entra

Connected

M365

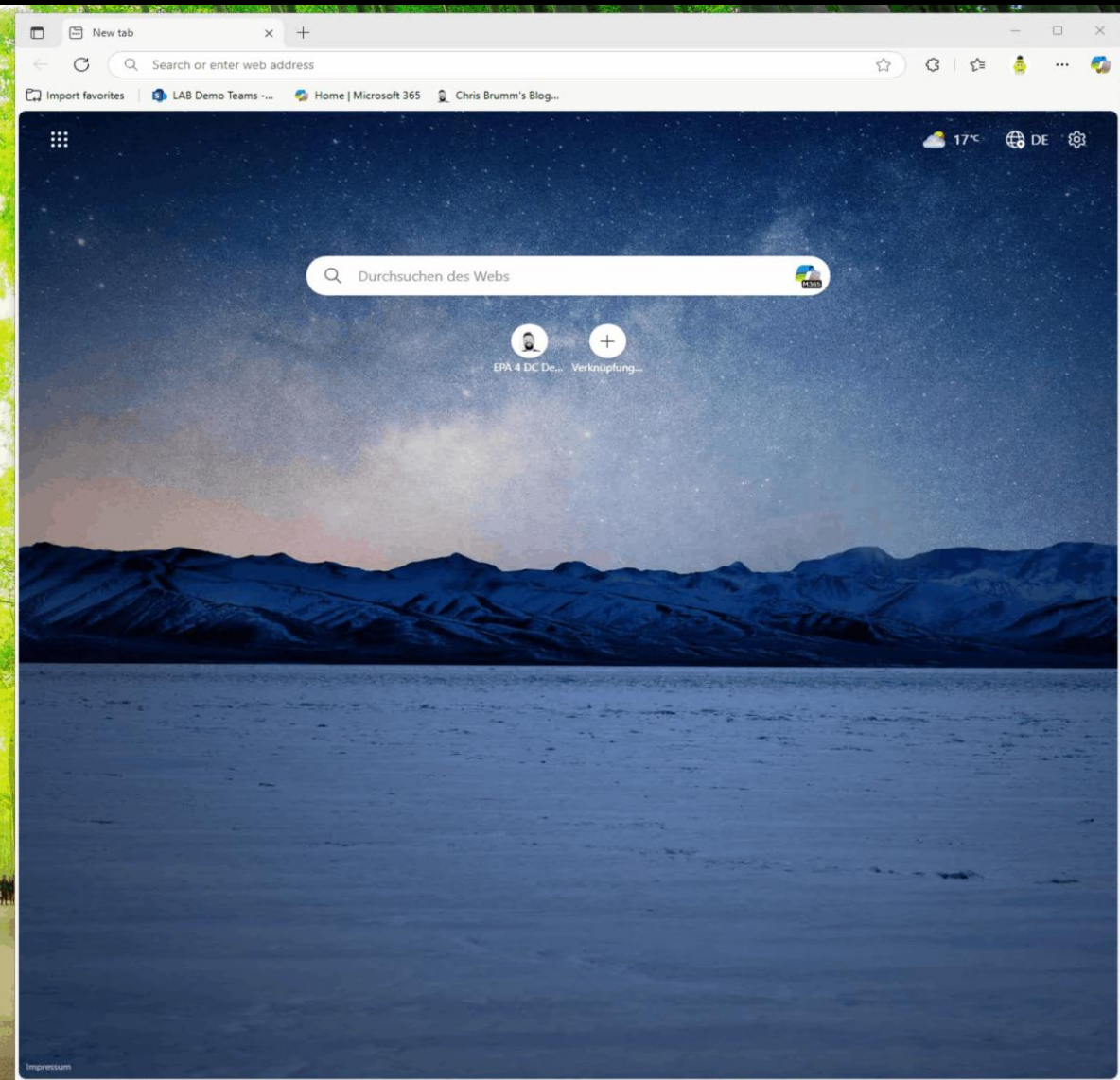
Connected

Additional details

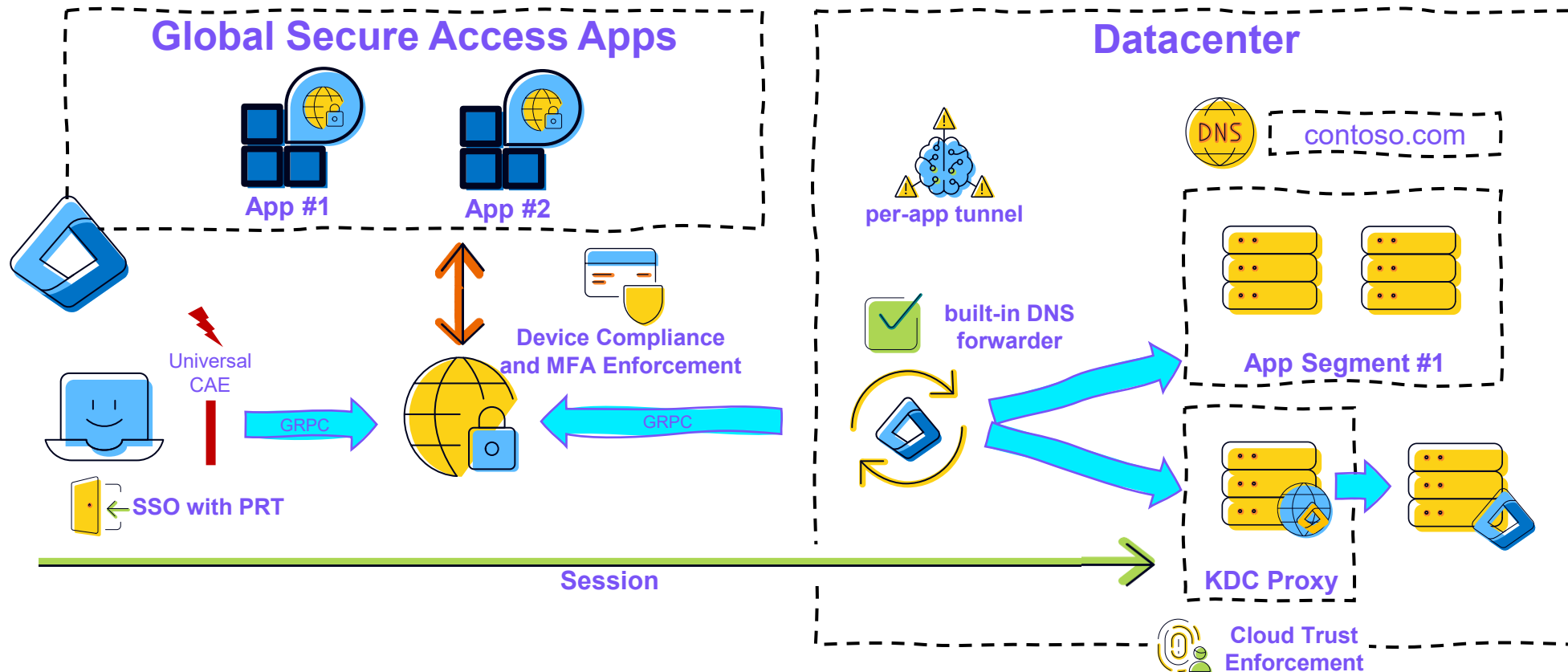
Account: Bert@gkfelucia.net

Tenant id: 0f642f1e-8030-465d-91cf-5252c6ca581b

Show more details



Using the KDC Proxy in Private Access



A comparison...

KDC proxy

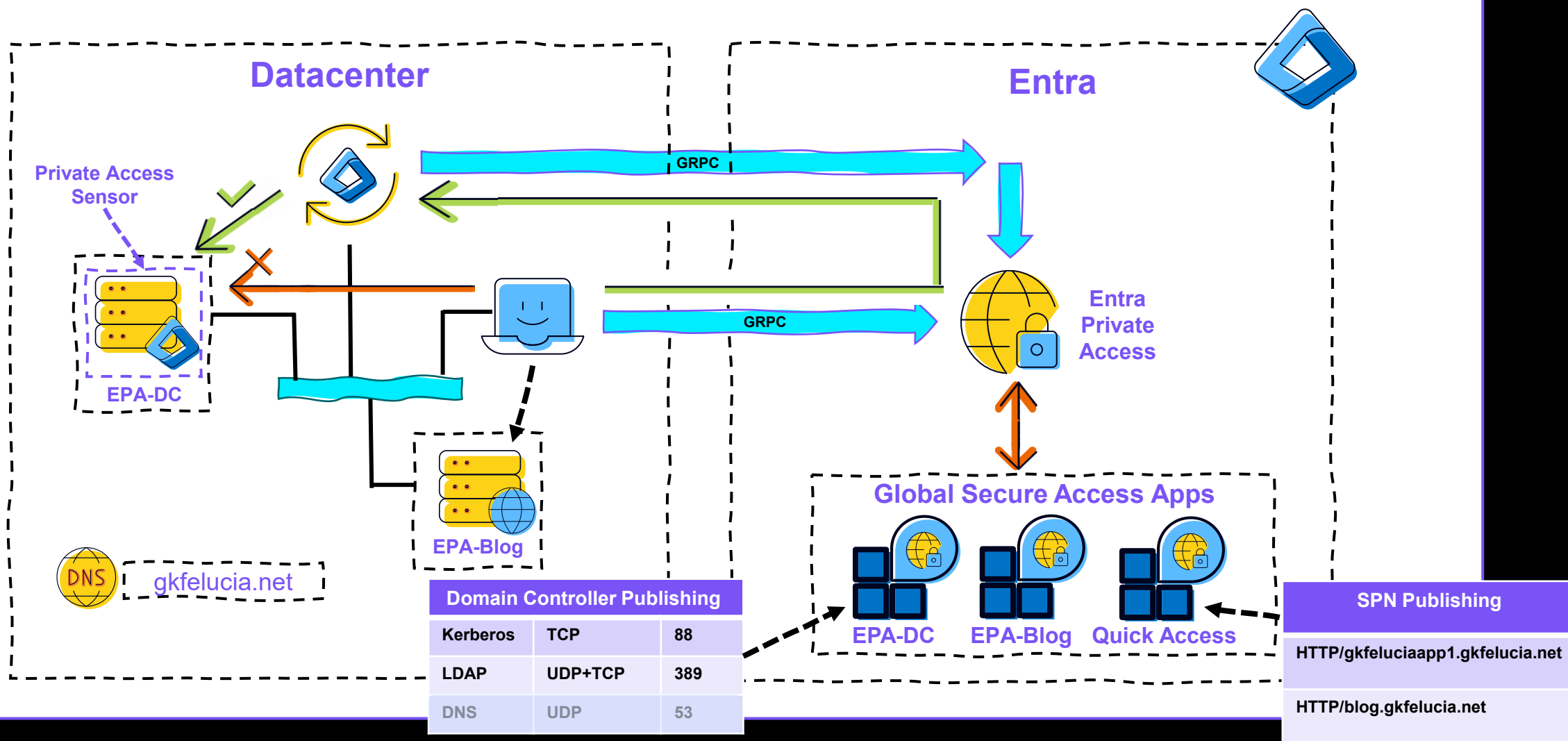
- Windows Hello / Cert-based Authentication
- No direct connection to a domain controller
- No Timeouts because of Negative DC locator caching

Extra Private Access for Domain Controllers

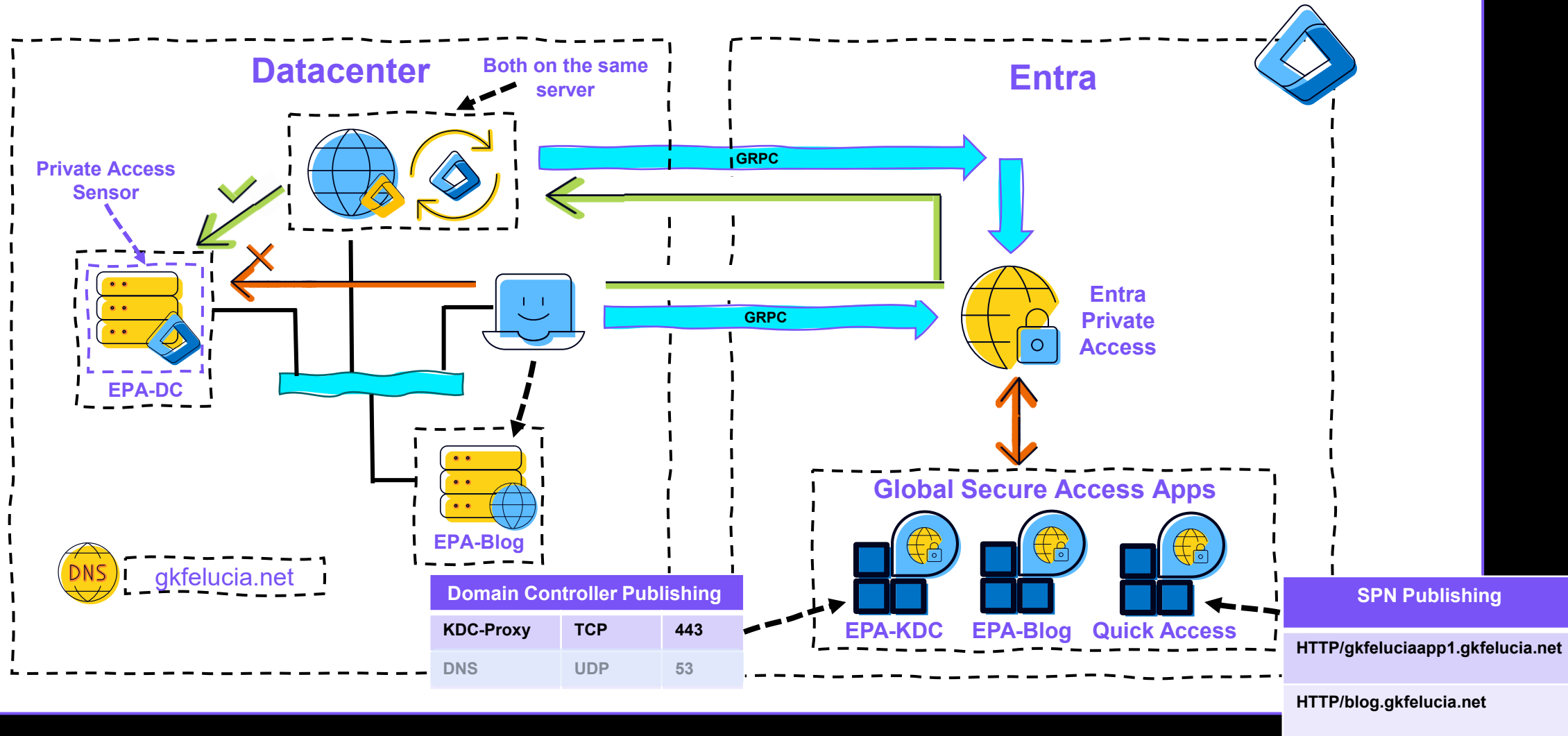
- Full Conditional Access Support
- Blocking of Kerberos TGS Requests for specific combinations of users/SPNs/IPs



Private Access for Domain Controllers



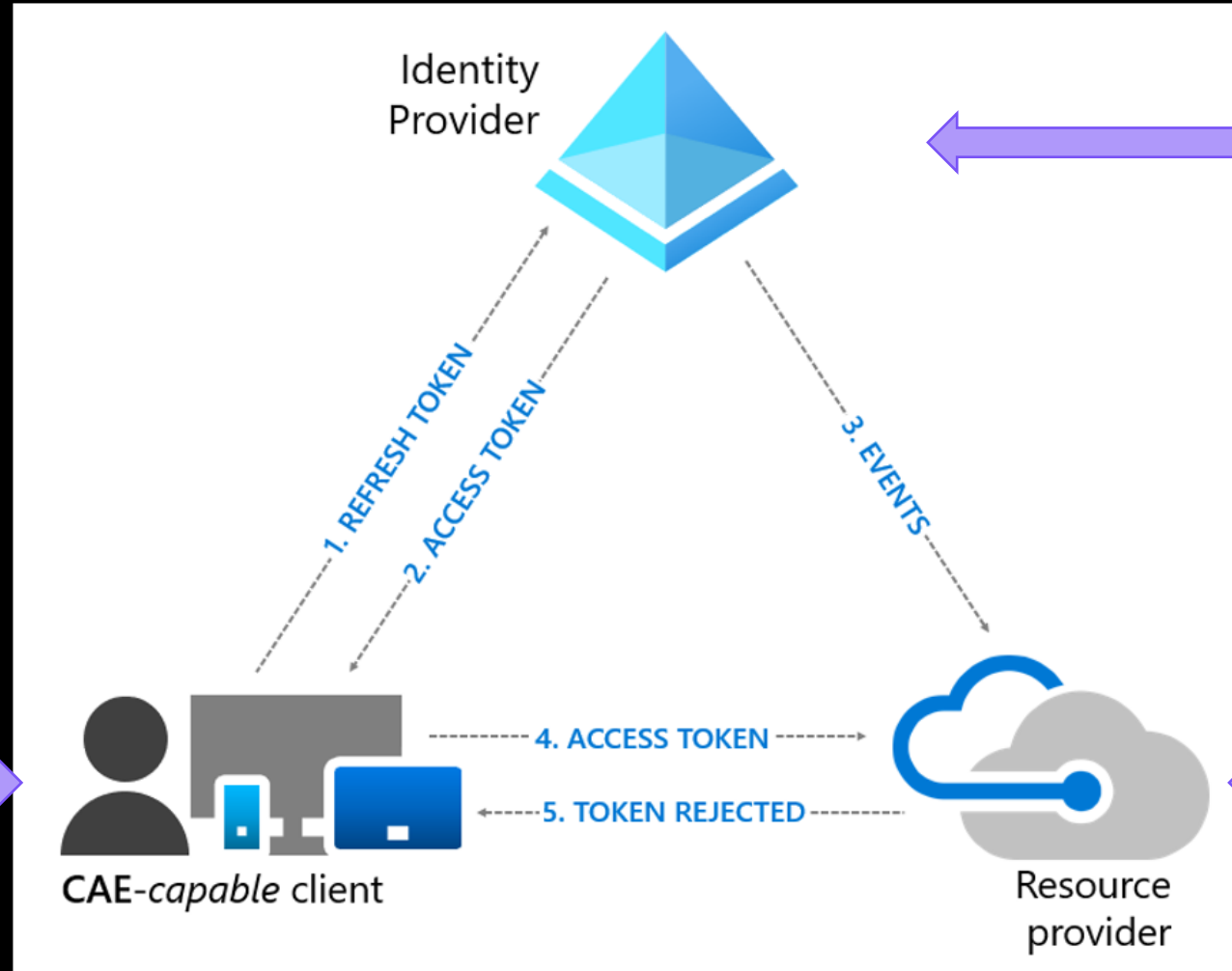
Combine KDC proxy and EPA4DC



Universal Continuous Access Evaluation

Universal Continuous Access Evaluation

**GSA
Client**



Entra ID

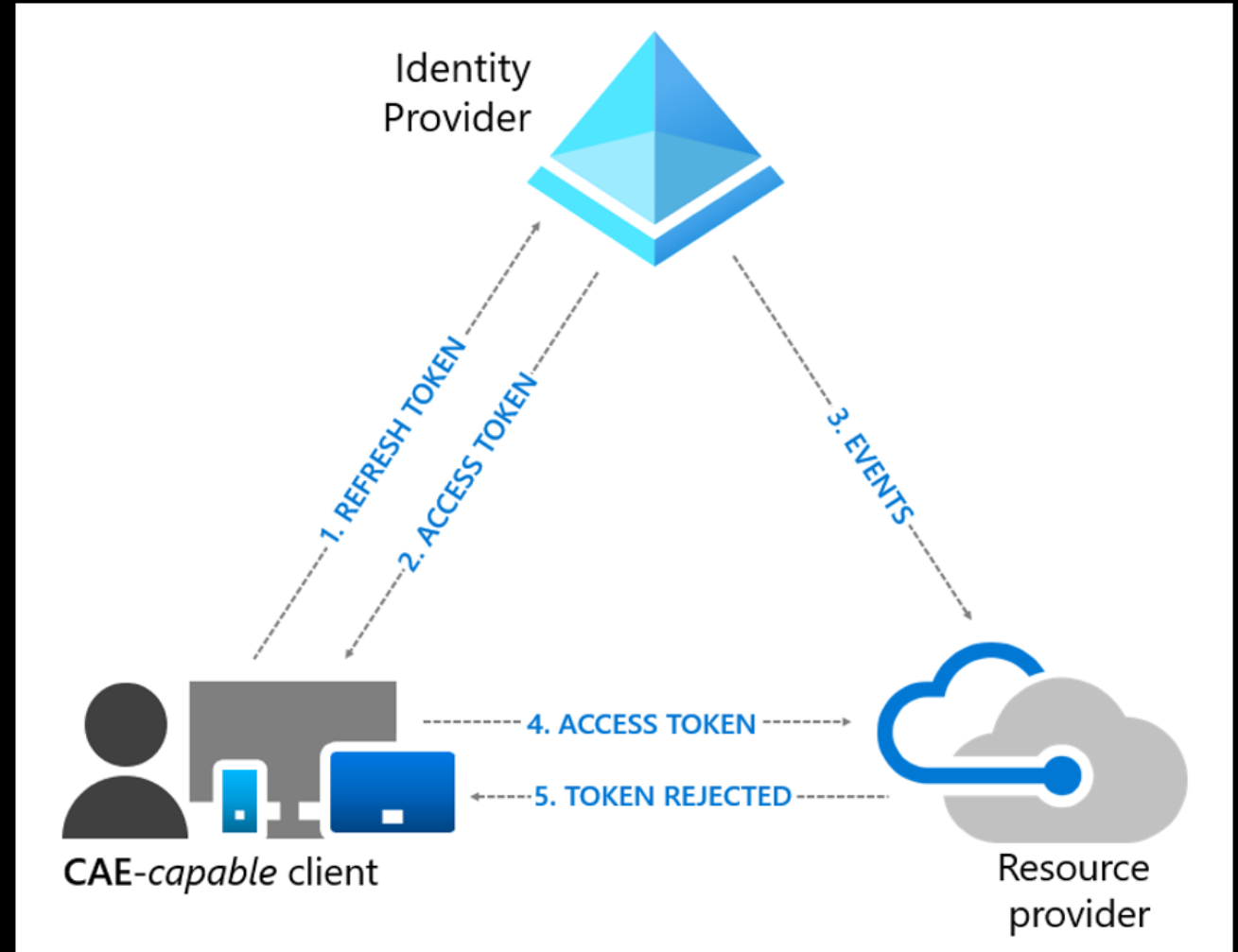


**Global
Secure
Access**

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



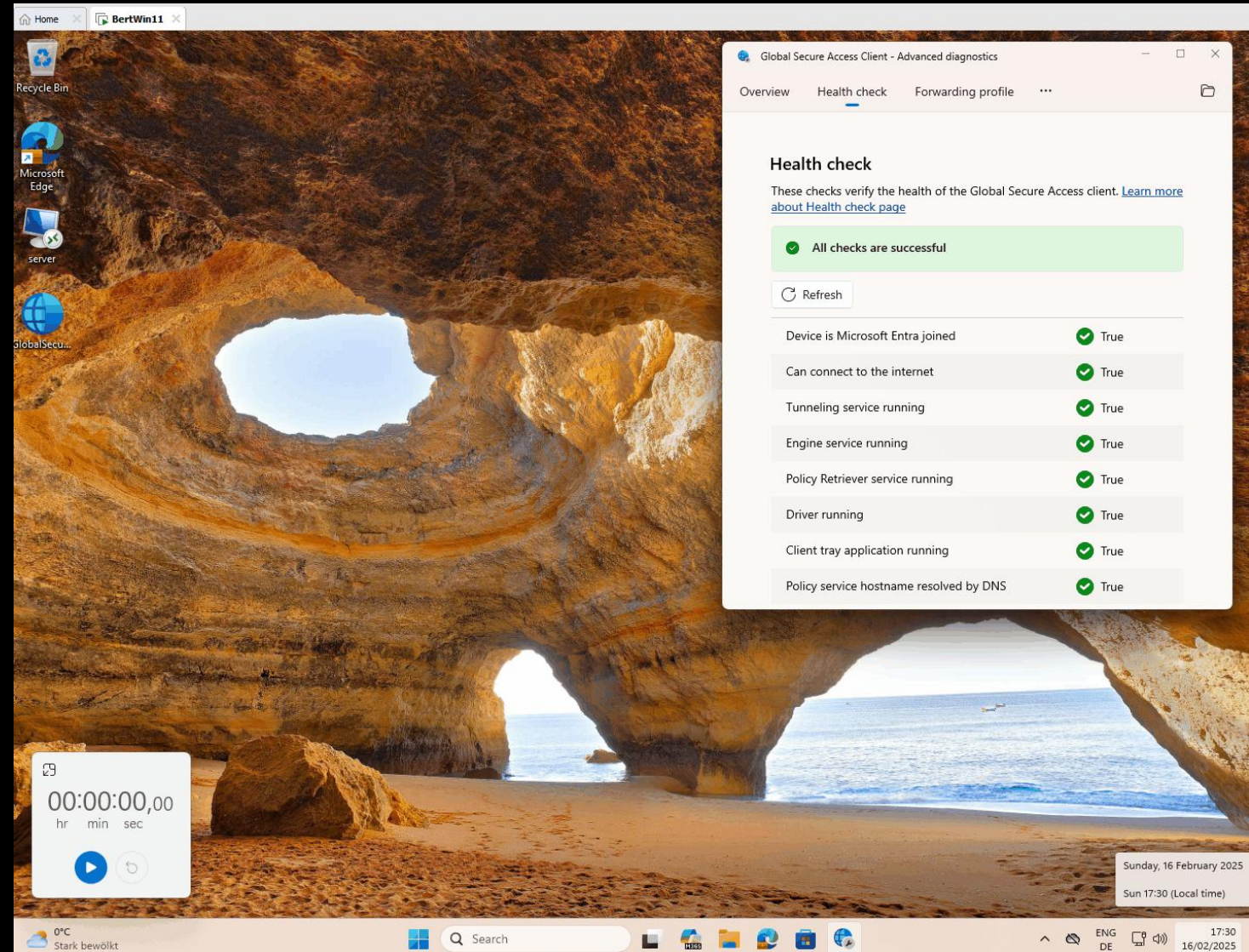
DEMO

Universal Continuous Access Evaluation

Universal Continuous Access Evaluation

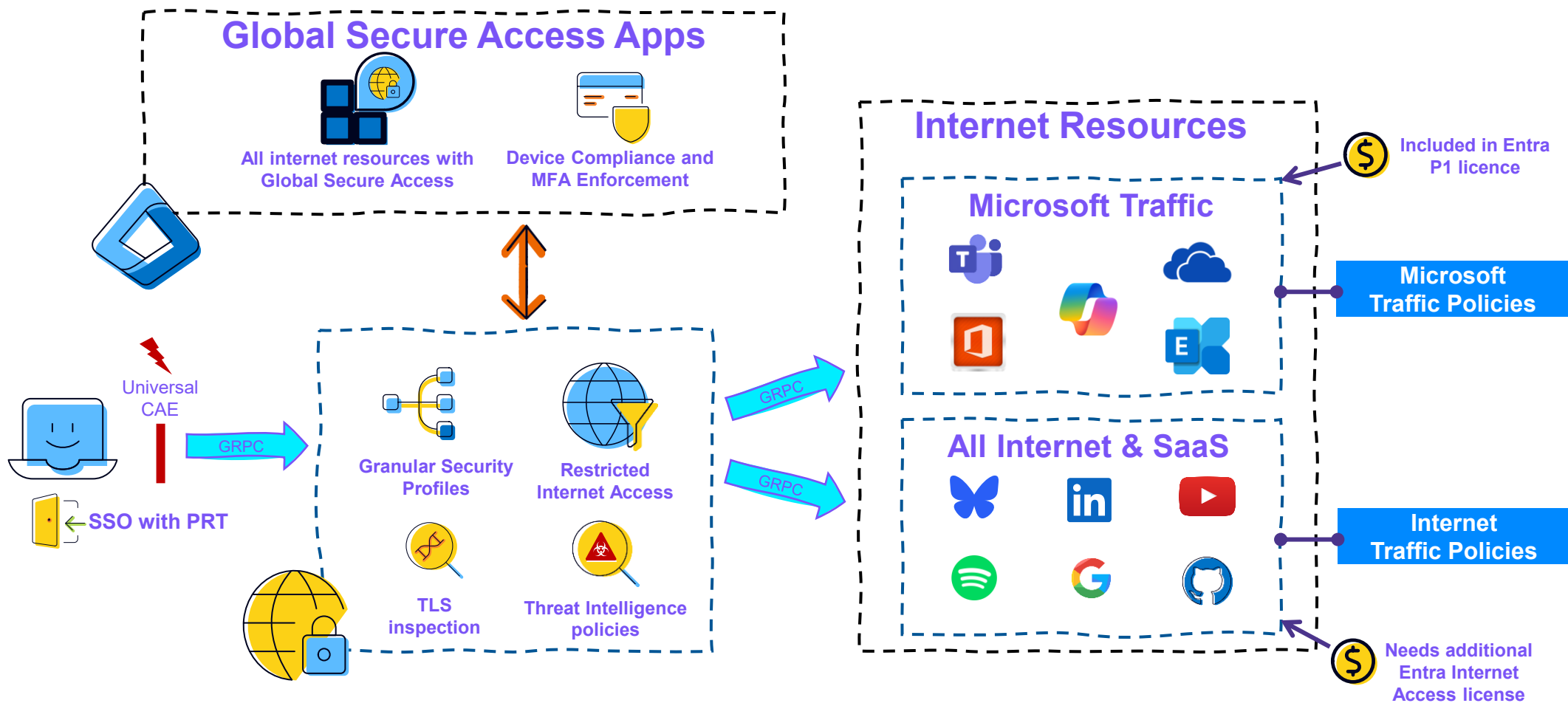
Trigger events for Universal CAE:

- 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


Overview Entra Internet Access



The Compliant Network Condition

Select

1 user

 Herbert Stadler
stadler@gkfelucia.net ...

Include Exclude

Select the locations to exempt from the policy

☐ All trusted networks and locations

☒ All Compliant Network locations

☐ Selected networks and locations

Name *

EIA 3 - Require Compliant Network to acces...

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps') included and 2 resources excluded

Network **NEW** ⓘ

Any network or location and 1 excluded

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Include Exclude

Select the resources to exempt from the policy

☐ None

☐ All internet resources with Global Secure Access


☒ Select resources


Edit filter

None

Select

Microsoft Intune Enrollment and 1 more

 Microsoft Intune
0000000a-0000-0000-c000-000000000000...

 Microsoft Intune Enrollment
d4ebce55-015a-49b5-a083-c84d1797ae...

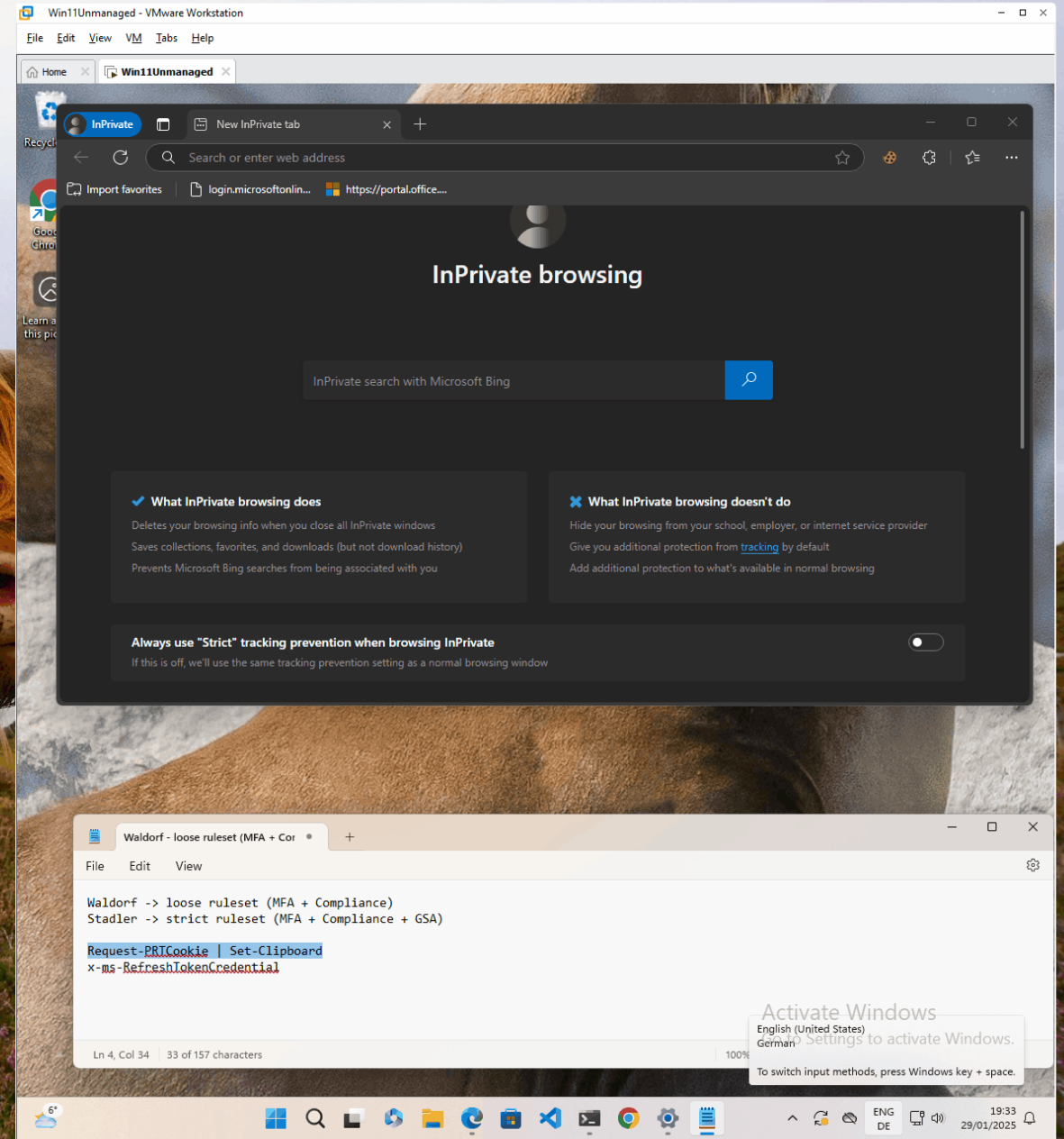
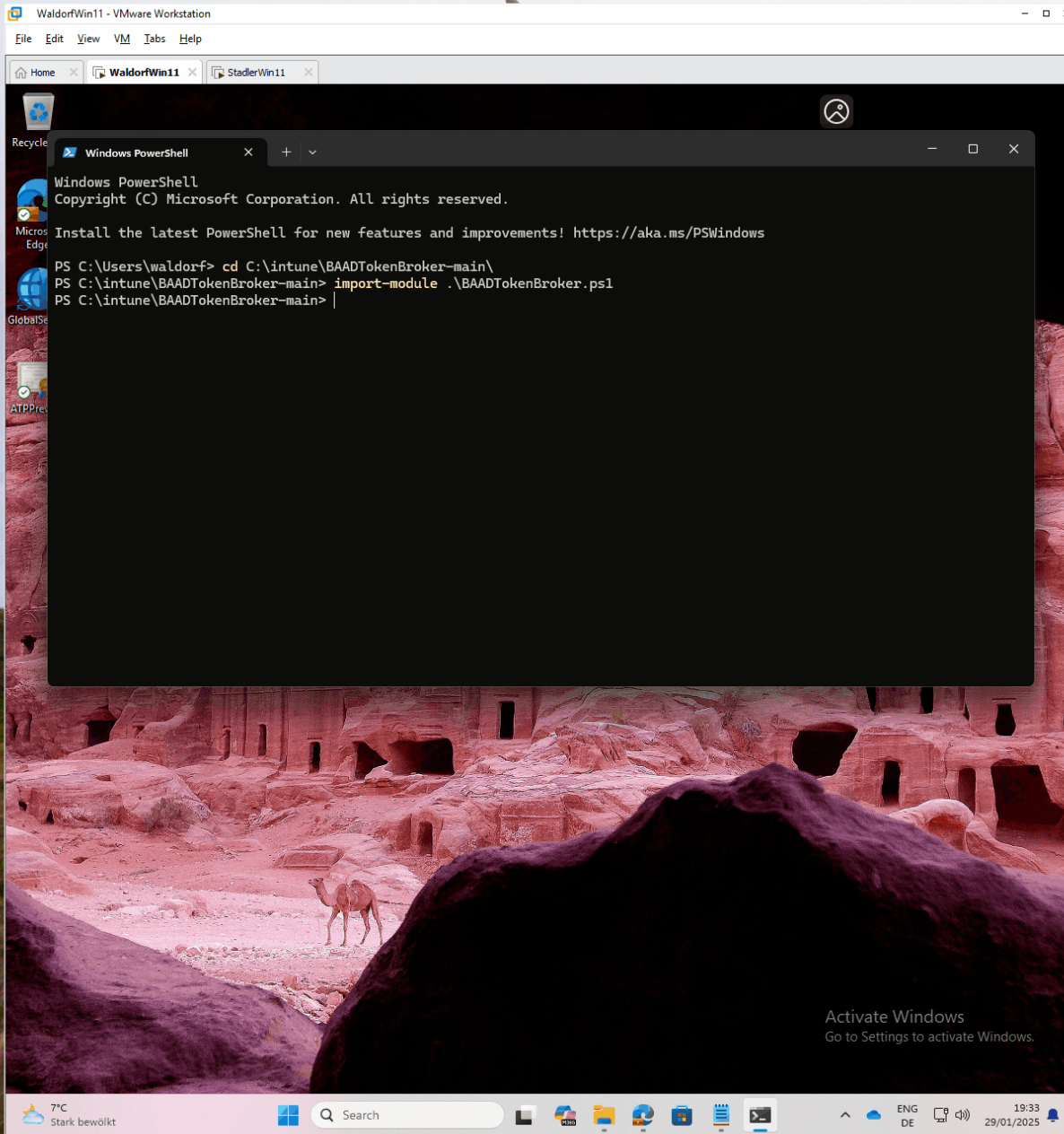
Examples for additional exclusions:

Azure Windows VM Sign-In

Azure Virtual Desktop
Windows 365
Microsoft Remote Desktop
Windows Cloud Login

DEMO

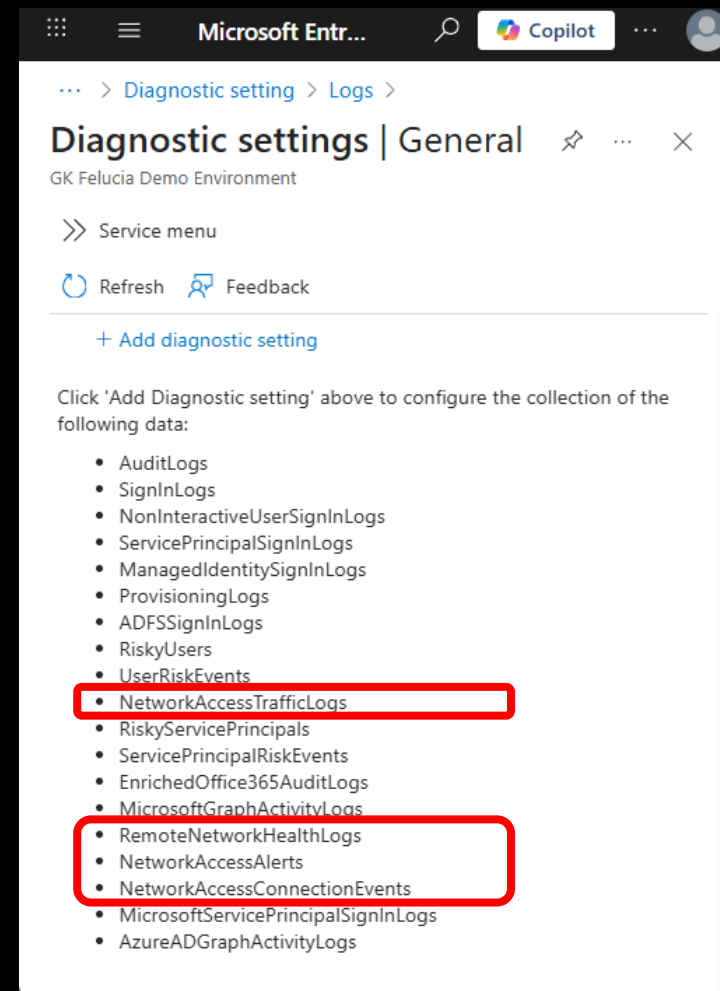
The Compliant Network Condition



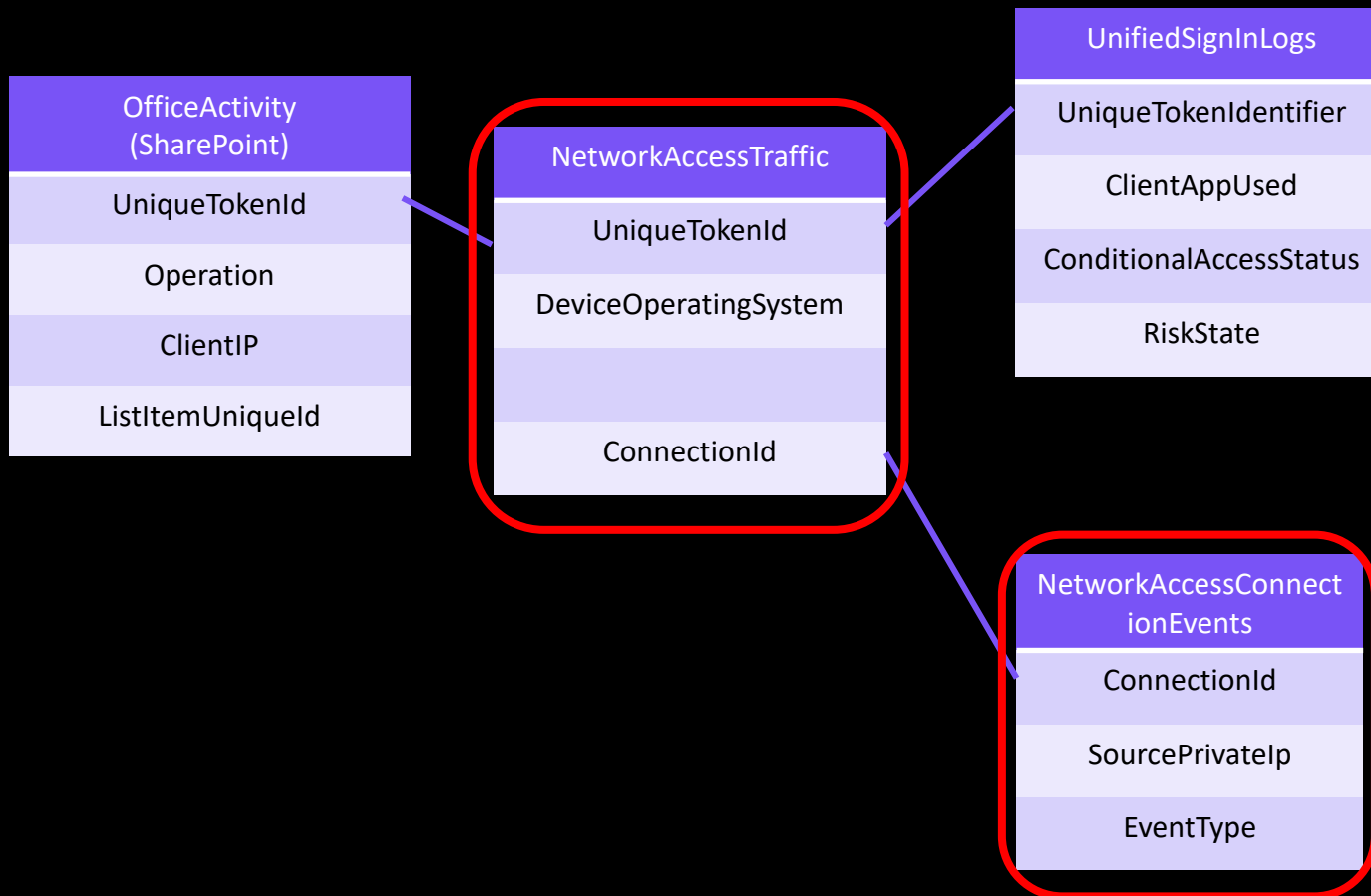
Logging

Easy Sentinel ingest

via Entra Diagnostic Settings
+ Defender XDR with Unified
Security Operations Platform



Entra Internet Access - Log Integration



Inspect record

Process tree

All details

TimeGenerated
Sep 14, 2025 4:37:10 PM

UserPrincipalName1
waldorf@gkfelucia.net

Operation
SharingSet

Network

Key	Value
SeenByEntra	149.224.97.105
PreGSA	149.224.97.105
SeenByOffice	128.94.22.145
PostGSA	128.94.22.110
IsThroughGlobalSecureAccess	true

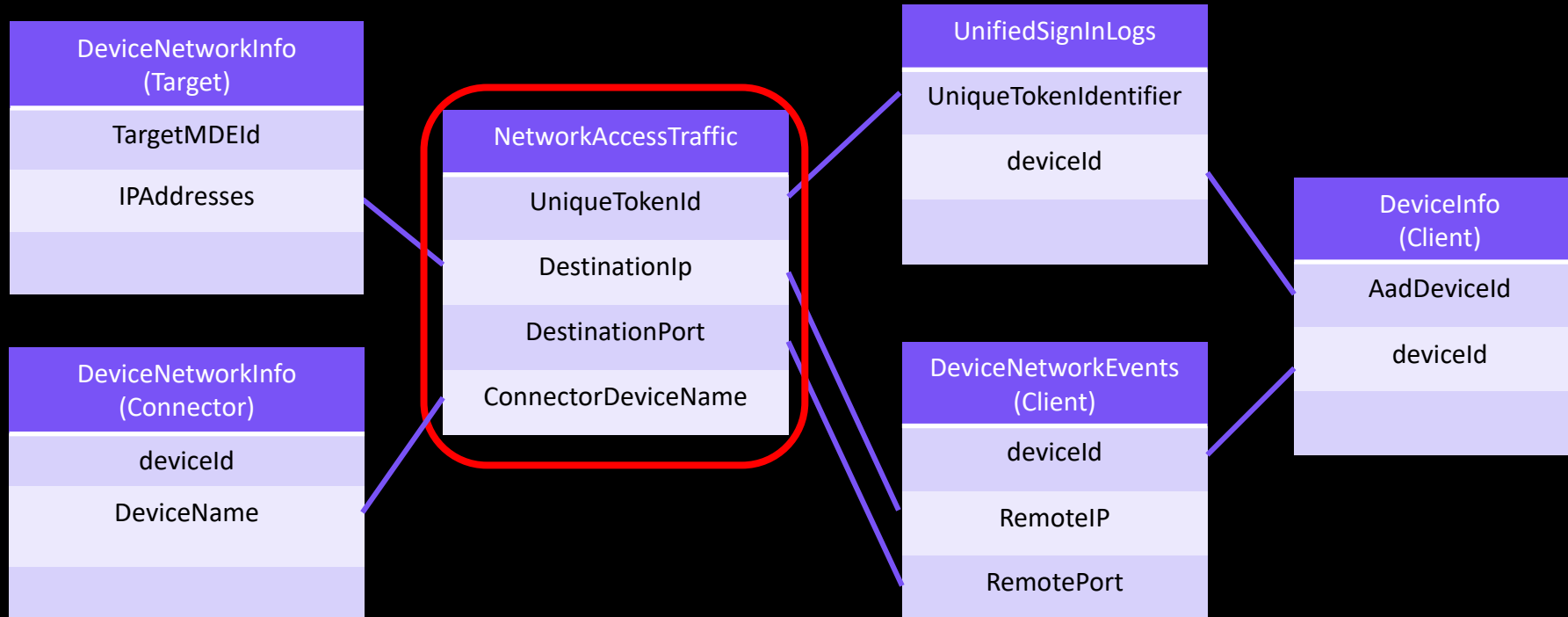
Session

Key	Value
UniqueTokenIdentifier	IAtsMOFmkUqnkNKhdY2AA
SignInResult	SUCCESS
ConditionalAccessStatus	success
RiskState	none
IncomingTokenType	primaryRefreshToken
TokenProtectionStatusDetails	("signInSessionStatus";"bound";"signInSe

DeviceDetail

Key	Value
deviceId	e75147f2-43c8-4260-9502-9b56d311d8
displayName	WaldorfWin11
operatingSystem	Windows10
browser	Edge 140.0.0
isCompliant	true
isManaged	true
trustType	Azure AD joined

Entra Private Access - Log Integration



Inspect record

Assets

Process tree

All details

TimeGenerated

Feb 10, 2025 10:00:13 AM

UserPrincipalName

Bert@gkfelucia.net

ClientDeviceName

bertwin11

TargetDeviceName

gkfeluciadc1.gkfelucia.net

ConnectorDeviceName

appproxy1.gkfelucia.net

ConditionalAccessStatus

success

InitiatingProcessName

lsass.exe

TrafficType

private

AccessType

QuickAccess

ApplId

4e8c3b32-1ab6-471e-8bbc-549314020941

DestinationIp

192.168.0.10

TransportProtocol

Tcp

DestinationPort

88

ConnectorInternalIP

IPAddress

SubnetPrefix

AddressType

192.168.0.40

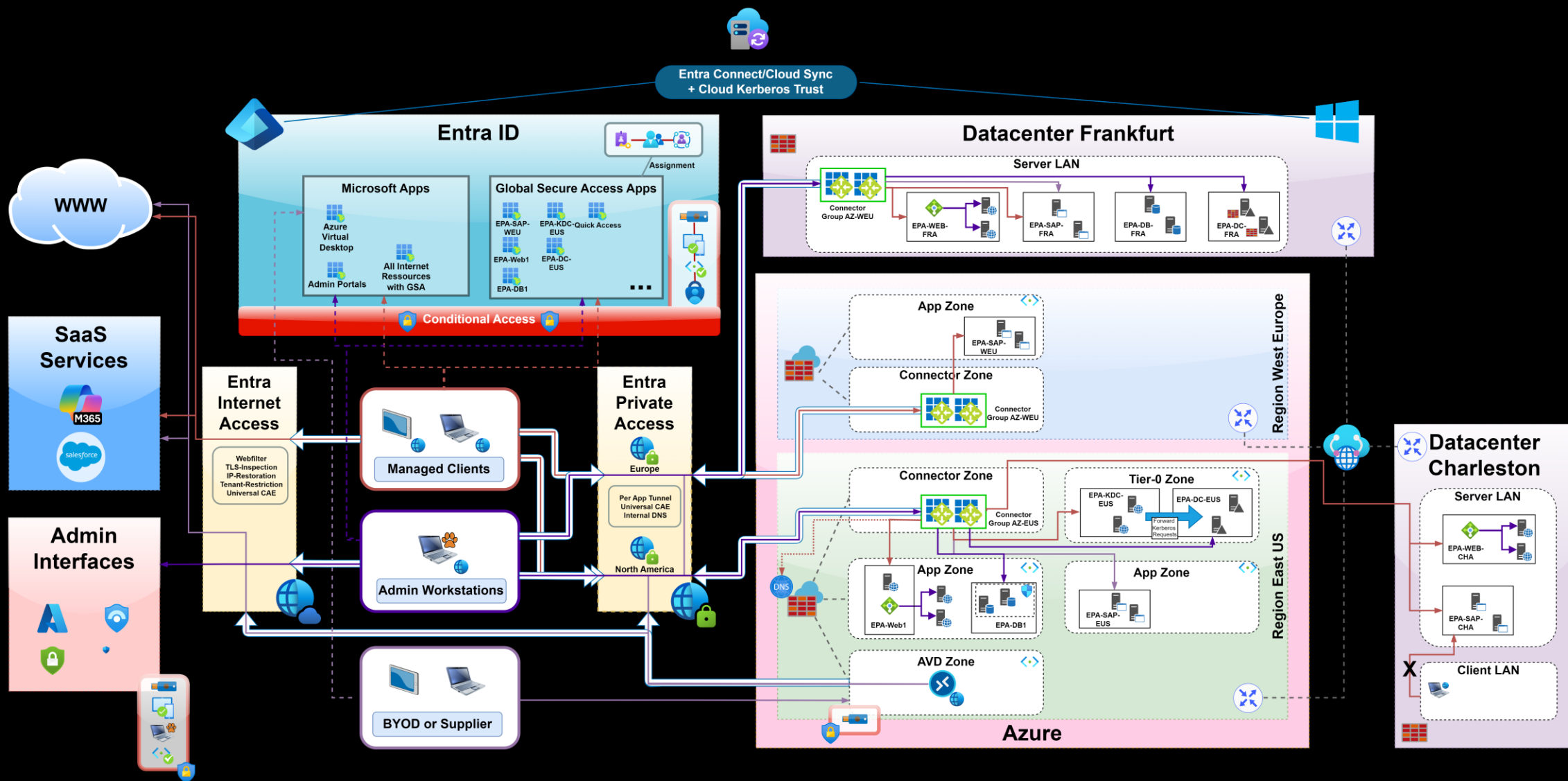
24

Private

SourceIp

93.196.7.233

Putting it all together



Questions?



HYBRID
IDENTITY
PROTECTION
conf25

