

Microsoft Entra ID Global Secure Access

Identity Days – Webinars

Quoi de neuf depuis ?

Seyfallah Tagrerout

CEO and Founder STC Consulting | Cloud and Security Architect
Microsoft Azure Specialist | Microsoft Zero Trust Specialist
Microsoft MVP Security and Microsoft Regional Director
Author | Speaker | Trainer





- NEWS 😊
- Global Secure Access
- News
- Demo
- Questions



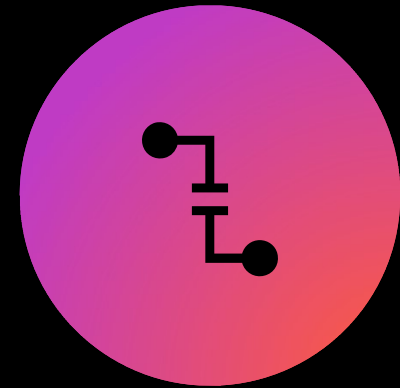
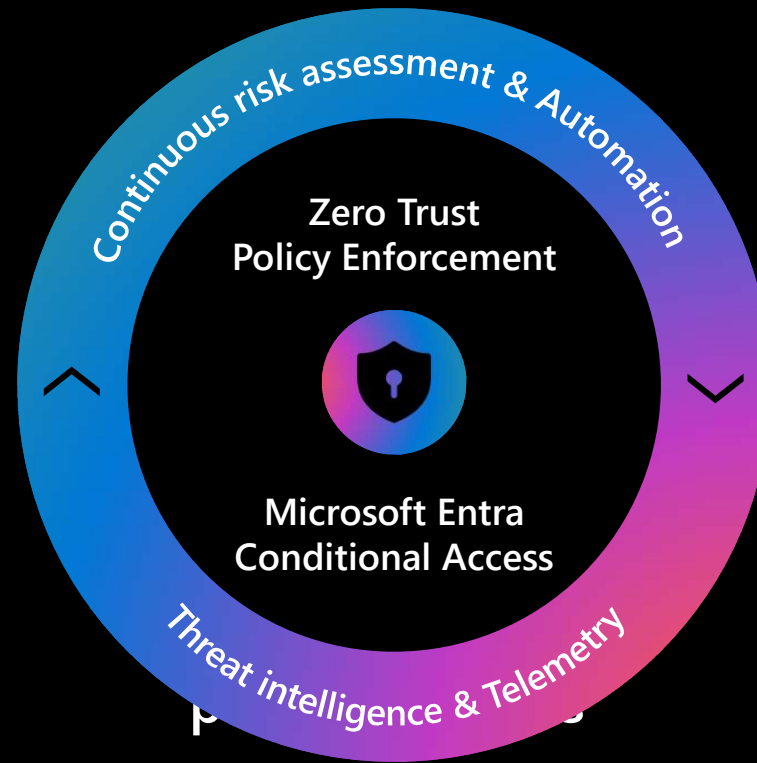
ZERO TRUST

FRENCH COMMUNITY

Zero Trust principles

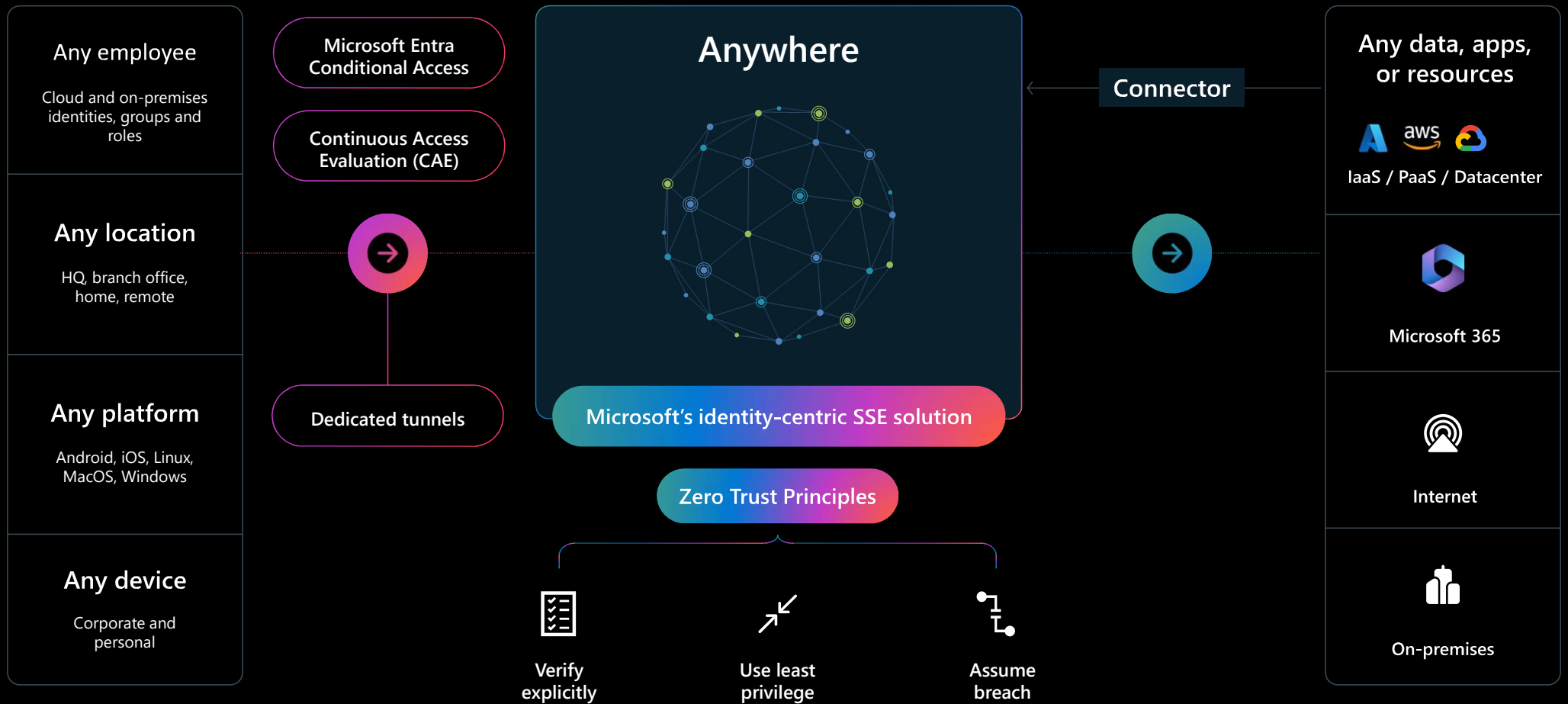


**Verify
explicitly**

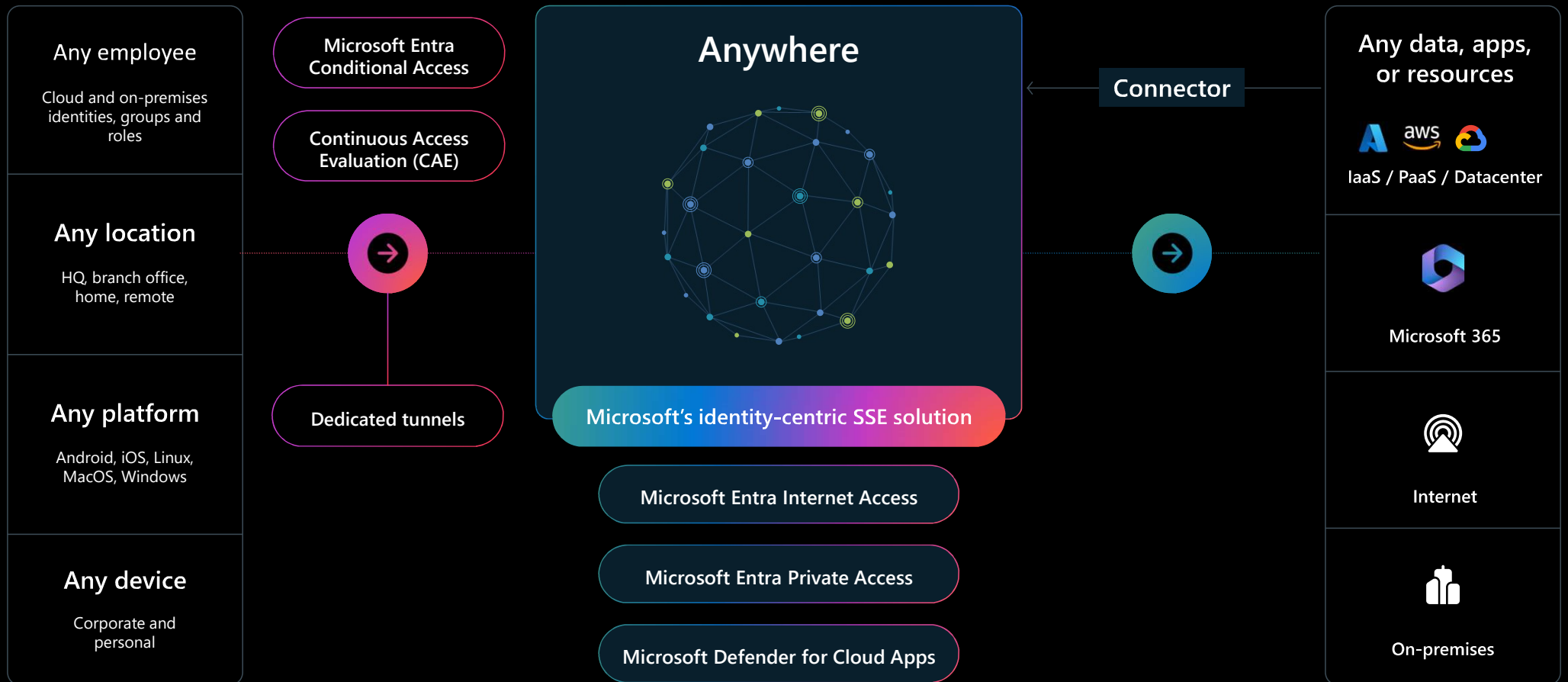


**Assume
breach**

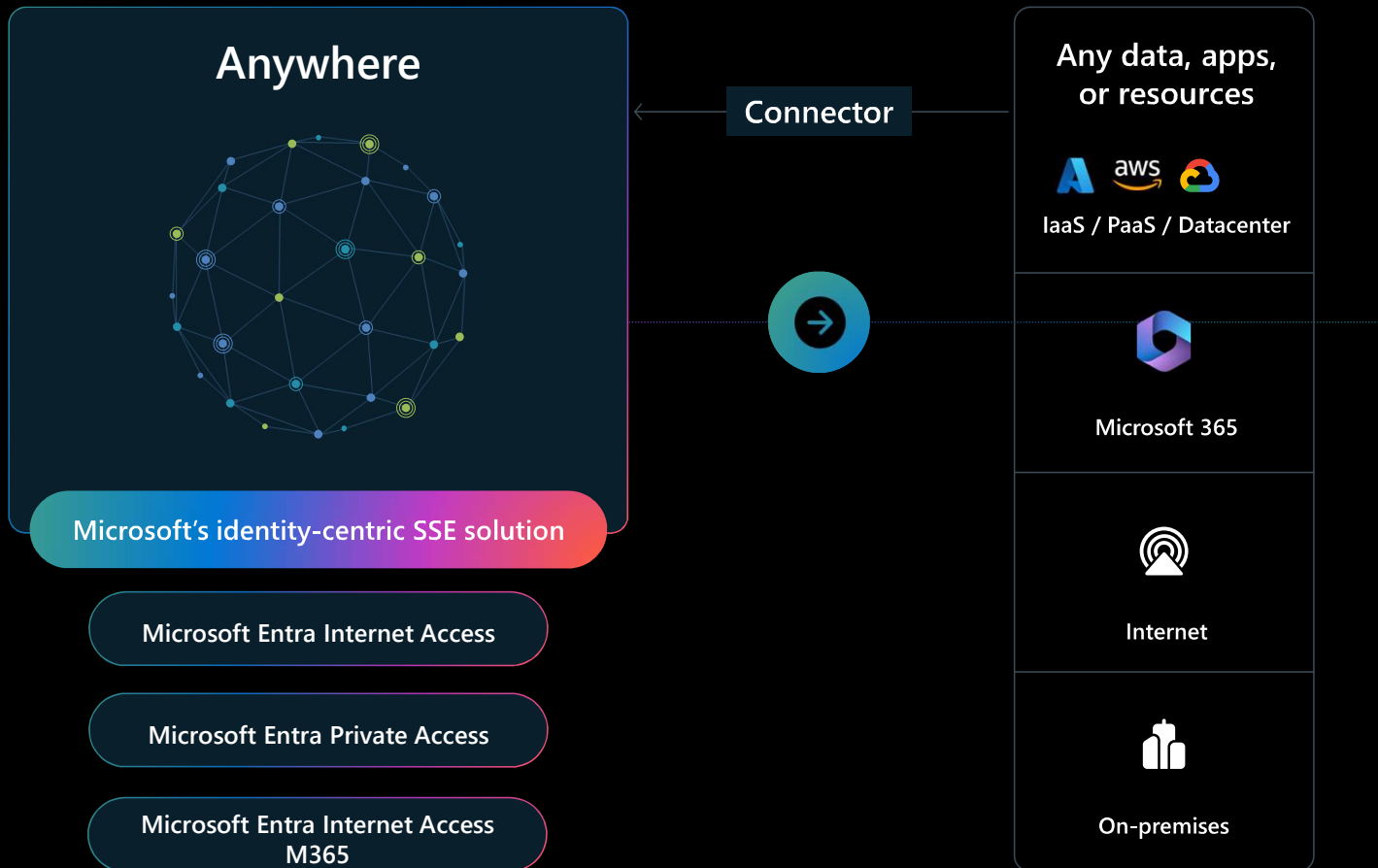
Microsoft's identity-centric SSE solution

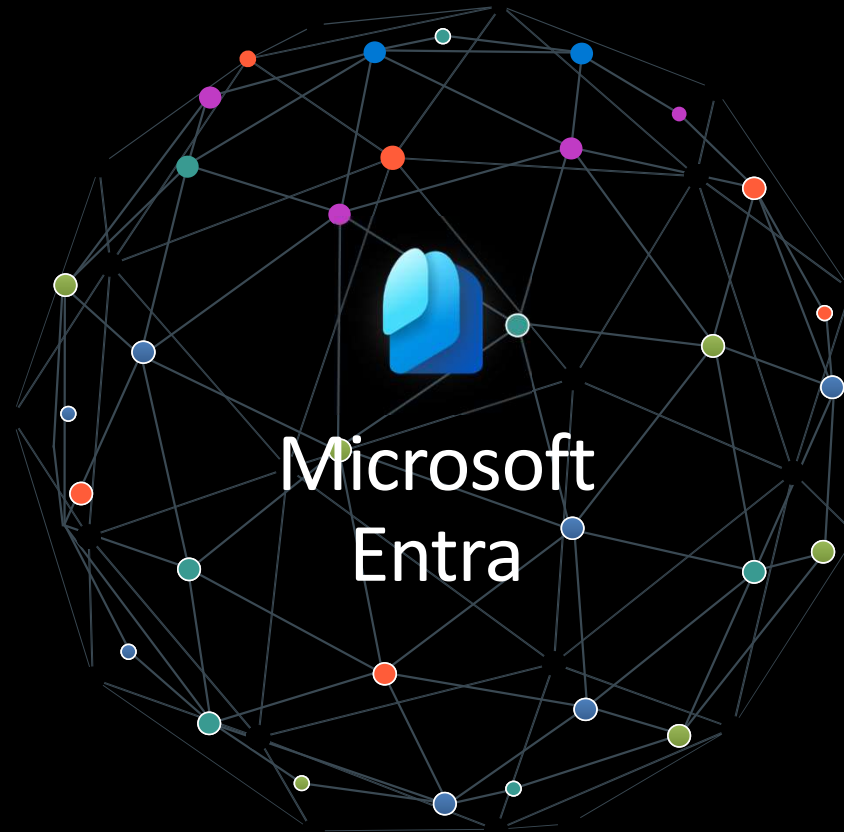


Microsoft's identity-centric SSE solution



Microsoft's identity-centric SSE solution





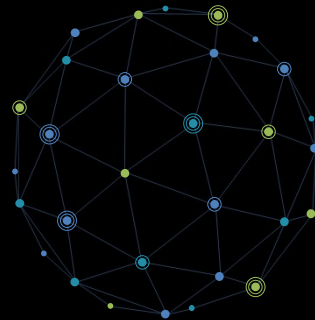
Secure access for any identity,
from anywhere, to any app, AI, or resource

Global Secure Access

Internet and Private Access coupled with Defender for cloud app (CASB)

SSE Microsoft Edge
Converges : Network – Identity – Endpoint
Unified portal

Feature delivered from Microsoft Wide area network (140 regions + 190 network edge locations)



This private network, which is one of the largest in the world, enables organizations to optimally connect users and devices to public and private resources seamlessly and securely.

Microsoft Entra Internet Access

Microsoft Entra Private Access

Microsoft Defender for Cloud Apps

A New **Era** of Secure Access

Microsoft Entra
Global Secure Access Offer

Seyfallah Tagrerout
MS MVP & RD



Other features

Entra ID Governance

premium Microsoft Entra
Verified ID features

advanced Identity
Protection Microsoft Entra

Global Secure Access



Microsoft Entra
Internet Access



Microsoft Entra
Private Access

Microsoft 365



Universal conditional
access



Universal tenant
restrictions



Compliant network
check



Logs and
monitoring

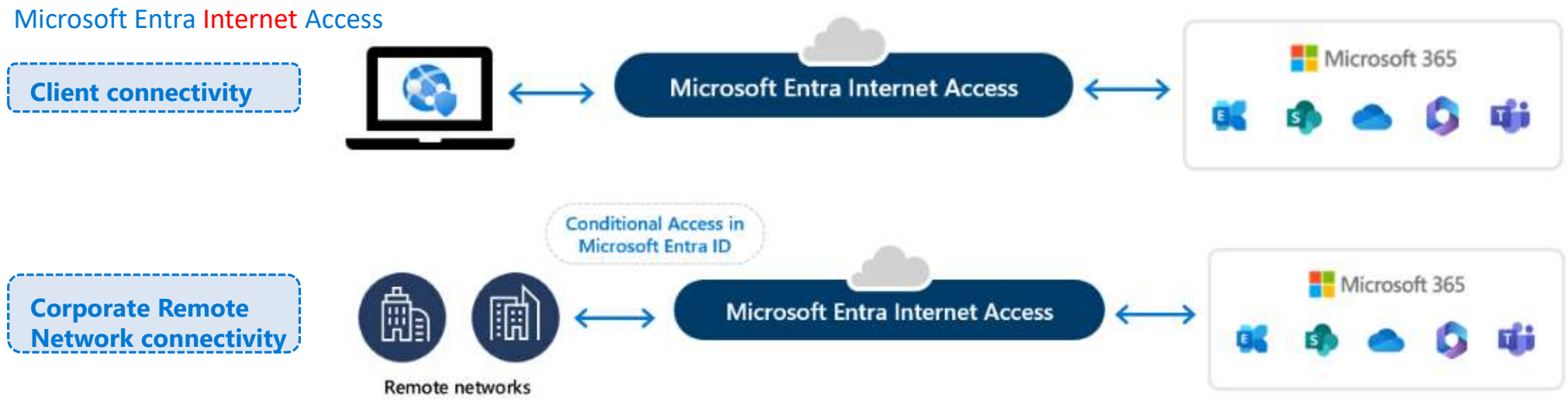


Remote networks



Traffic forwarding
profiles

Microsoft ZTNA: How it runs with Internet Access?

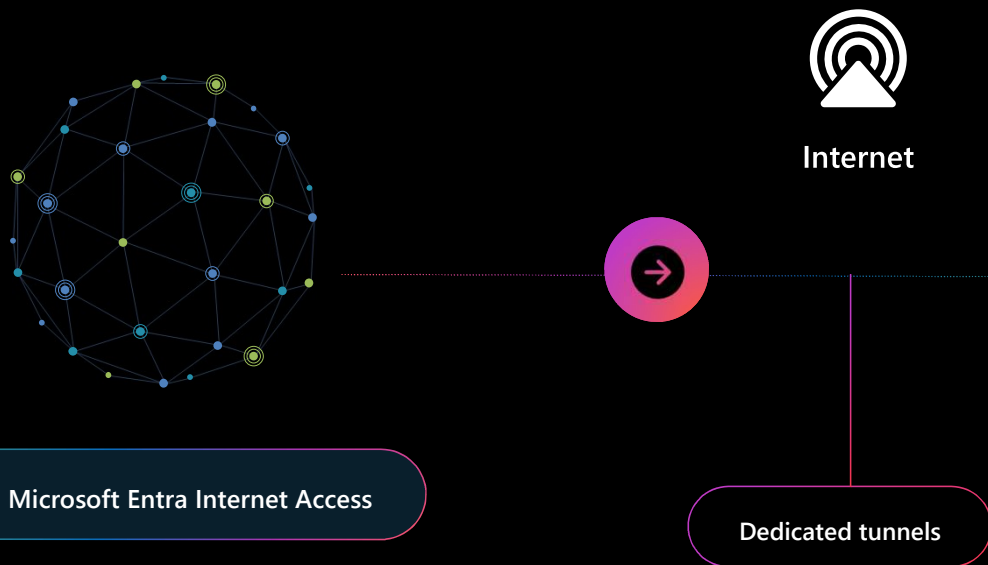


Microsoft Entra ID

Microsoft Entra Internet Access isolates the traffic for M365 Apps and resources, such as Exchange Online and SharePoint Online. Users can access these resources by connecting to the Global Secure Access Client or through a remote network, such as in a branch office location

Identity and Network Access Solution together

Global Secure Access – Internet Access



The key introductory feature of Microsoft Entra Internet Access for all apps is **Web Content Filtering**.

- Prevent stolen tokens from being replayed with the compliant network check-in Conditional Access.
- Apply universal tenant restrictions to prevent data exfiltration to other tenants or personal accounts including anonymous access.
- Enriched logs with network and device signals currently supported for SharePoint Online traffic.
- Improve the precision of risk assessments on users, locations, and devices.
- Deploy side-by-side with non-Microsoft SSE solutions.
- Acquire network traffic from the desktop client or from a remote network, such as a branch location.
- Dedicated public internet traffic forwarding profile.
- Protect user access to the public internet while using Microsoft's cloud-delivered, identity-aware SWG solution.
- Enable web content filtering to regulate access to websites based on their content categories and domain names.
- Apply universal Conditional Access policies for all internet destinations, even if not federated with Microsoft Entra ID, through integration with Conditional Access session controls.

Updates

Microsoft Entra Internet Access

Secure Web Gateway

Public Preview

Universal continuous
access evaluation (CAE)

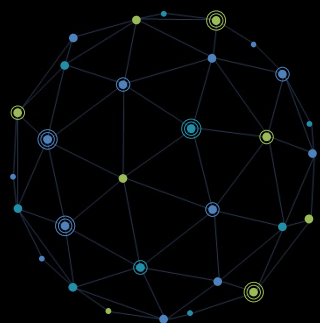
In public preview, makes it possible for Conditional Access to revoke network access in near real-time when it detects an increase in session risk that may signify an attack.

Private Preview

TLS inspection

•**TLS inspection**, in private preview, provides comprehensive visibility of encrypted traffic and enables enhanced URL web category filtering based on full URLs.

Global Secure Access – Internet Access M365



Microsoft Entra Private Access



M365 - ADMIN



Dedicated tunnels

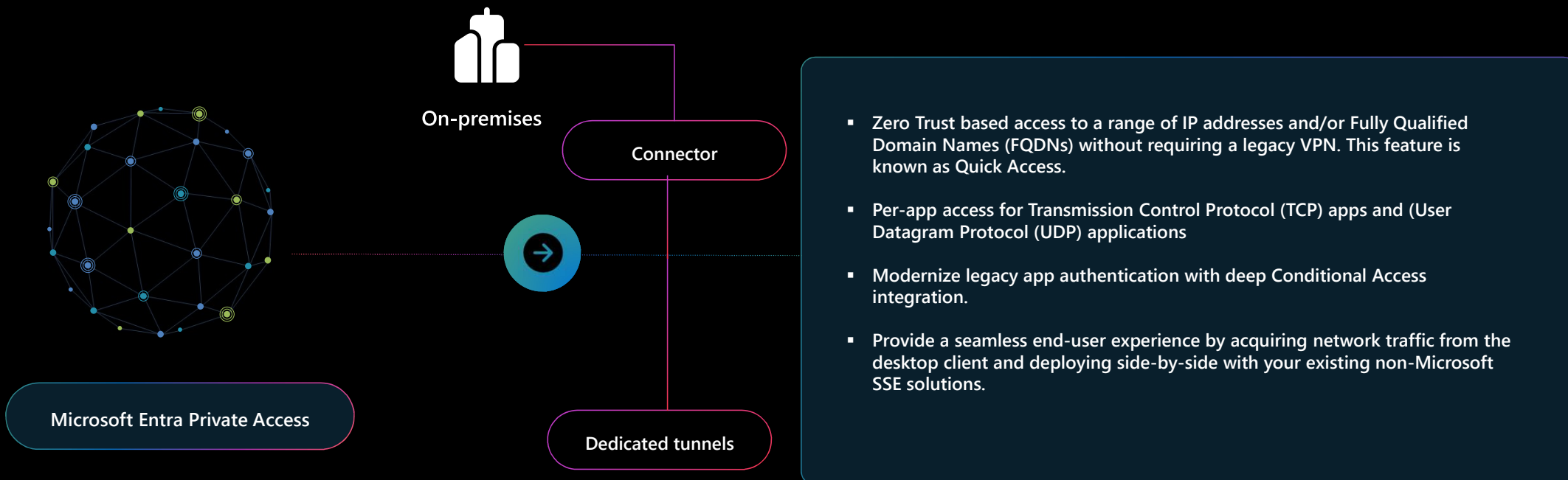
- Access to :
 - Exchange Online
 - Skype for business online and Microsoft Teams
 - SharePoint Online and Onedrive for Business
 - Microsoft 365 Common and Office online
- 2 actions
 - ByPass : public traffic thought internet routing
 - Forward : traffic is encapsuled thought Microosft Edge Service
- Transport protocol
 - TCP

This profile can be used for "Privileged Account hardening"

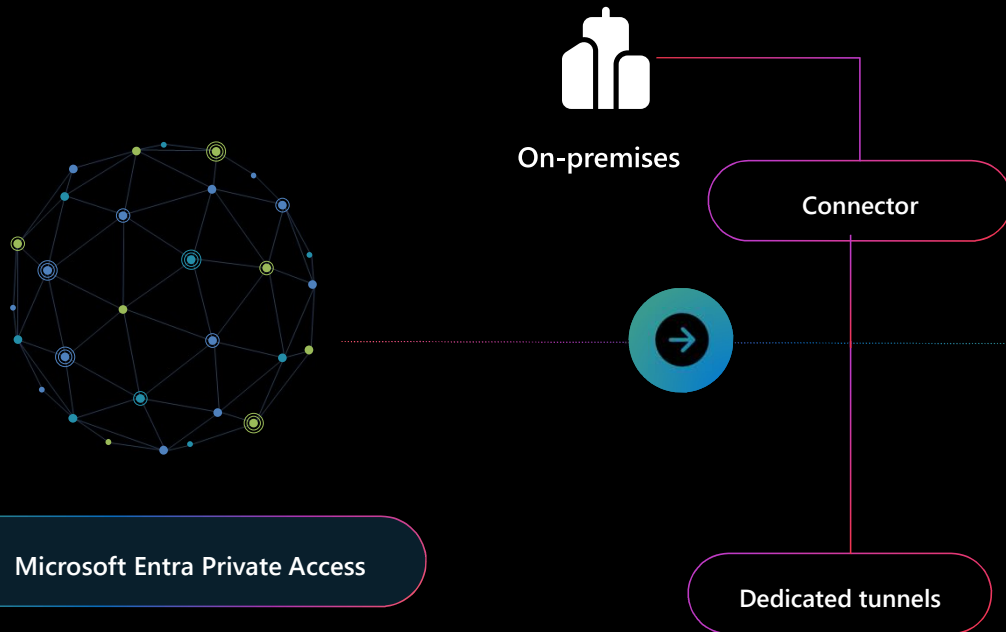
Microsoft Entra Internet Access for Microsoft services capabilities are included in a Microsoft Entra ID P1 or Microsoft Entra ID P2 license.

Microsoft Entra Internet Access for Microsoft services enhances Microsoft Entra ID capabilities with direct connectivity to supported Microsoft services, improving security, performance, and resilience.

Global Secure Access – Private Access



Global Secure Access – Private Access



Requirements :

- License (Private Access or Entra suite)
- On-Premises connector:
 - Windows Server 2012 R2 or newer
 - Outbound port : 80 and 443
 - Server inside a private network (important)
 - he minimum .NET version required for the connector is v4.7.1+
 - We recommend having more than one Windows server.
 - TLS 1.2
 - Connector group with multiple connectors for each network (if needed)
 - Dedicated server
- GSA Client :
 - Requirement : please see the GSA client slide

Private Network connectors

+ New Connector Group | Download connector service | + Configure an app | Disable Private Network connectors | Got feedback?

Microsoft Entra Private Network provides single sign-on (SSO) and secure remote access for web applications hosted on-premises.
[Learn more about Microsoft Entra Private Network connectors](#)

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

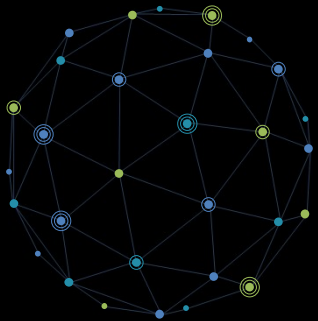
H...	Groups	IP	Status	Country/Region
!	▼ Default			Europe
		STC-AAD01.stc.lan	20.161.58.127	Active

Quick Access
Application

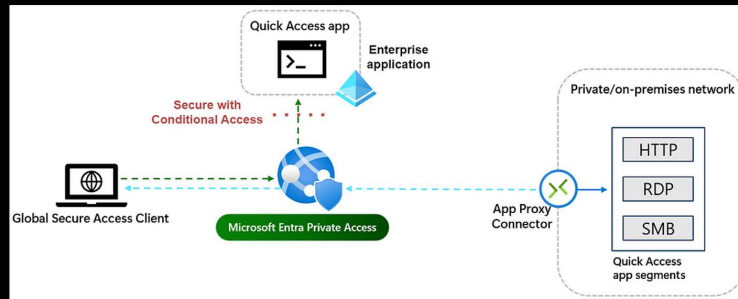
Quick Access
Application

NEW – Global Secure
Access Application

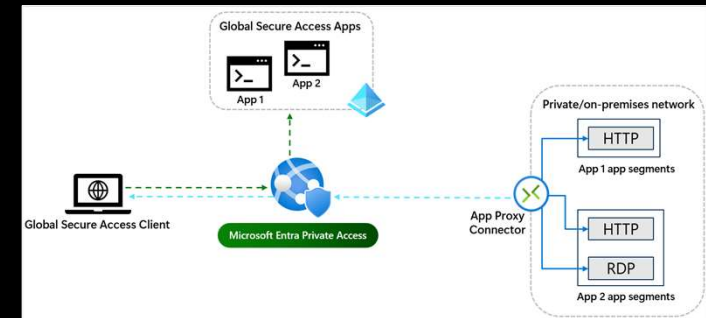
Global Secure Access – Private Access



Quick Access Application



Quick Access Application



Microsoft Entra Private Access

Global Secure Access – Private Access:

- Private DNS

DNS sur TCP:

- DNS uses UDP port 53 for name resolution. Some browsers have their own DNS client, which also supports TCP port 53. Currently, the Global Secure Access client does not support DNS TCP port 53. To mitigate this issue, disable the browser's DNS client by setting the following registry values:

Microsoft Edge

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge] "BuiltInDnsClientEnabled" = **dword:00000000**

Chrome

[HKEY_CURRENT_USER\Software\Policies\Google\Chrome] "BuiltInDnsClientEnabled" = **dword:00000000**

Update
s

Microsoft Entra Private Access

Zero Trust Network Access

Available

Quick access
policies

December

App
discovery

Public Preview

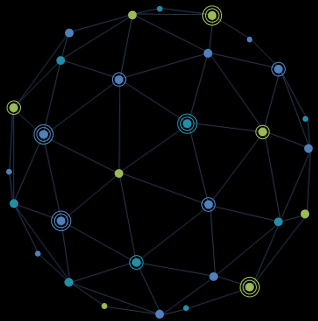
Private
DNS

Public Preview

Connectors in
marketplaces

- **Quick Access**, already generally available, makes it easy to onboard private apps to Microsoft Entra.
- **App Discovery**, in public preview, makes it easy to discover all your private apps.
- **Private DNS**, in public preview, makes it easy for users to access IP-based app segments across private apps using Fully Qualified Domain Names (FQDNs).
- **Connectors** available in Microsoft Azure, AWS, and Google Cloud marketplaces, in public preview, make it easier to deploy private network connectors.

Global Secure Access – Client

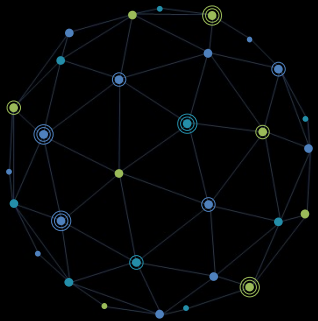


GSA Client



- **OS Types supported**
 - Windows - GA
 - MAC OS – Preview
 - Android – GA
 - IOS – Preview
- **Prerequisites:**
 - AVD single
 - Windows 365
 - Win 11 / Win 10
 - Device **Ms Entra Joined** or **Ms entra Hybrid Joined**
 - Local admin for installation
 - License «slide Licence»

Global Secure Access – Client



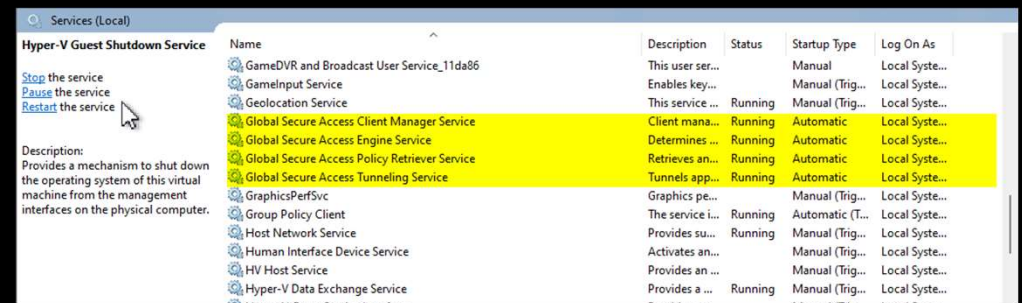
GSA Client

Icon	Message	Description
	Global Secure Access	The client is initializing and checking its connection to Global Secure Access.
	Global Secure Access - Connected	The client is connected to Global Secure Access.
	Global Secure Access - Disabled	The client is disabled because services are offline or the user disabled the client.
	Global Secure Access - Disconnected	The client failed to connect to Global Secure Access.
	Global Secure Access - Some channels are unreachable	The client is partially connected to Global Secure Access (that is, the connection to at least one channel failed: Microsoft Entra, Microsoft 365, Private Access, Internet Access).
	Global Secure Access - Disabled by your organization	Your organization disabled the client (that is, all traffic forwarding profiles are disabled).
	Global Secure Access - Private Access is disabled	The user disabled Private Access on this device.
	Global Secure Access - could not connect to the Internet	The client couldn't detect an internet connection. The device is either connected to a network that doesn't have an Internet connection or a network that requires captive portal sign in.

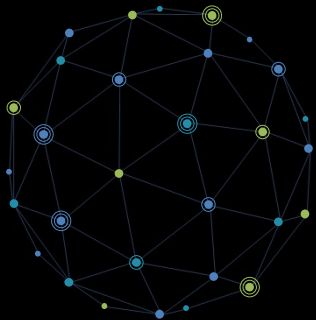
```
sc query GlobalSecureAccessTunnelingService
```

```
sc query GlobalSecureAccessEngineService
```

```
sc query GlobalSecureAccessDriver
```



Global Secure Access – Client - Hardening



GSA Client

Restrict nonprivileged users

Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Global Secure Access Client
RestrictNonPrivilegedUsers REG_DWORD

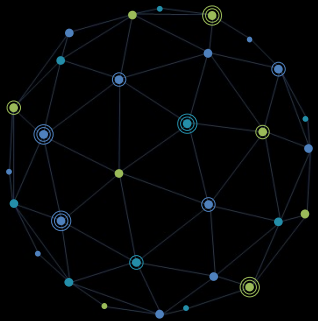
Data	Description
0x0	Nonprivileged users on the Windows device can disable and enable the client.
0x1	Nonprivileged users on the Windows device are restricted from disabling and enabling the client. A UAC prompt requires local administrator credentials for disable and enable options. The administrator can also hide the disable button (see Hide or unhide system tray menu buttons).

Disable or enable Private Access on the client

Computer\HKEY_CURRENT_USER\Software\Microsoft\Global Secure Access Client

Value	Type	Data	Description
IsPrivateAccessDisabledByUser	REG_DWORD	0x0	Private Access is enabled on this device. Network traffic to private applications goes through Global Secure Access.
IsPrivateAccessDisabledByUser	REG_DWORD	0x1	Private Access is disabled on this device. Network traffic to private applications goes directly to the network.

Global Secure Access – Client - Hardening



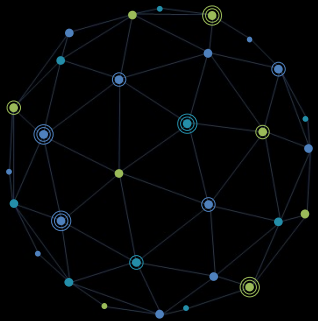
GSA Client

Hide or unhide system tray menu buttons

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client
Expand table

- HideSignOutButton
- HideDisablePrivateAccessButton
- HideDisableButton

Global Secure Access – Client - Hardening



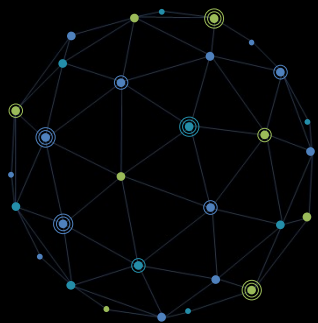
GSA Client

Hide or unhide system tray menu buttons

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client
Expand table

- HideSignOutButton
- HideDisablePrivateAccessButton
- HideDisableButton

Global Secure Access – Conditional Access



Microsoft Entra admin center

Search resources, services, and docs (G+)

Home

Identity governance

Verifiable credentials

Permissions Management

Global Secure Access (Preview)

Get started

Dashboard

Devices

Applications

Global settings

Session management

Logging

Secure

Connect

Monitor

Learn & support

Session Management

Got Feedback?

Tenant Restrictions Adaptive Access

Adaptive access settings allow admins to enable features used by Microsoft Entra Conditional Access and Microsoft Entra Identity Protection.

Global Secure Access signaling enables client IP restoration, which is used by Conditional Access, Continuous Access Evaluation, Identity Protection, and Microsoft Entra ID sign-in logs. [Learn more](#)

Global Secure Access signaling provides network location information to Conditional Access, enabling admins to create policies that restrict user access to specific apps based on their use of the Global Secure Access client or a remote network. [Learn more](#)

Enable Global Secure Access signaling in Conditional Access

Save

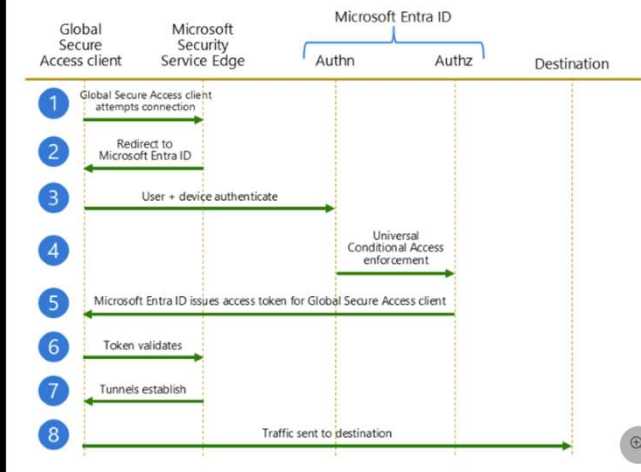


1 named location found

Name	Location type	Trusted	Conditional Access policies
All Compliant Network locations	Network Access	No	CA001: Standard Users : Block fro...

Access control - ZTNA

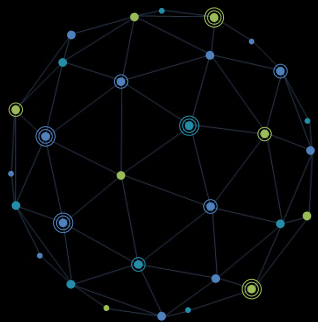
Internet Access – Universal CA



Step	Description
1	The Global Secure Access client attempts to connect to Microsoft's Security Service Edge solution.
2	The client redirects to Microsoft Entra ID for authentication and authorization.
3	The user and the device authenticate. Authentication happens seamlessly when the user has a valid Primary Refresh Token.
4	After the user and device authenticate, Universal Conditional Access policy enforcement occurs. Universal Conditional Access policies target the established Microsoft and internet tunnels between the Global Secure Access client and Microsoft Security Service Edge.
5	Microsoft Entra ID issues the access token for the Global Secure Access client.
6	The Global Secure Access client presents the access token to Microsoft Security Service Edge. The token validates.
7	Tunnels establish between the Global Secure Access client and Microsoft Security Service Edge.
8	Traffic starts being acquired and tunneled to the destination via the Microsoft and Internet Access tunnels.



Global Secure Access – Conditional Access



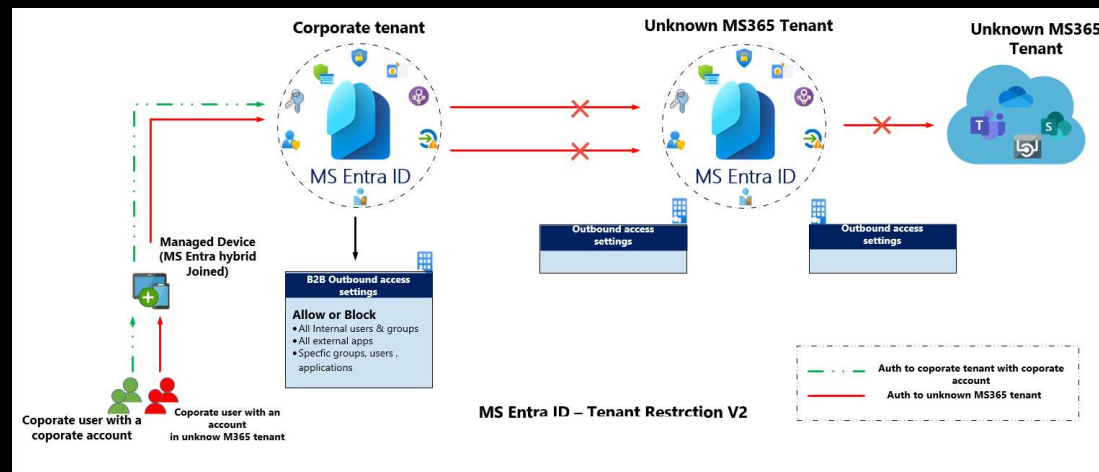
This new release gives IT admins **more control over external tenant access** within their organization.

It's also possible to create granular partner-specific collaboration policies for external tenants

Tenant restrictions vs. Inbound and Outbound settings:

- Inbound settings control external account access to your internal apps
- Outbound settings control internal account access to external apps
- **Tenant restrictions control external account access to external apps**

Access control - ZTNA



sta@stc-consulting.ch

Access is blocked

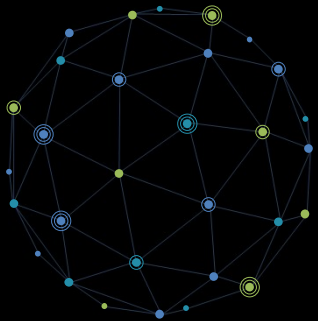
The STC Consulting dev IT department has restricted which organizations can be accessed. Contact the STC Consulting dev IT department to gain access.

[Read more about tenant restrictions](#)

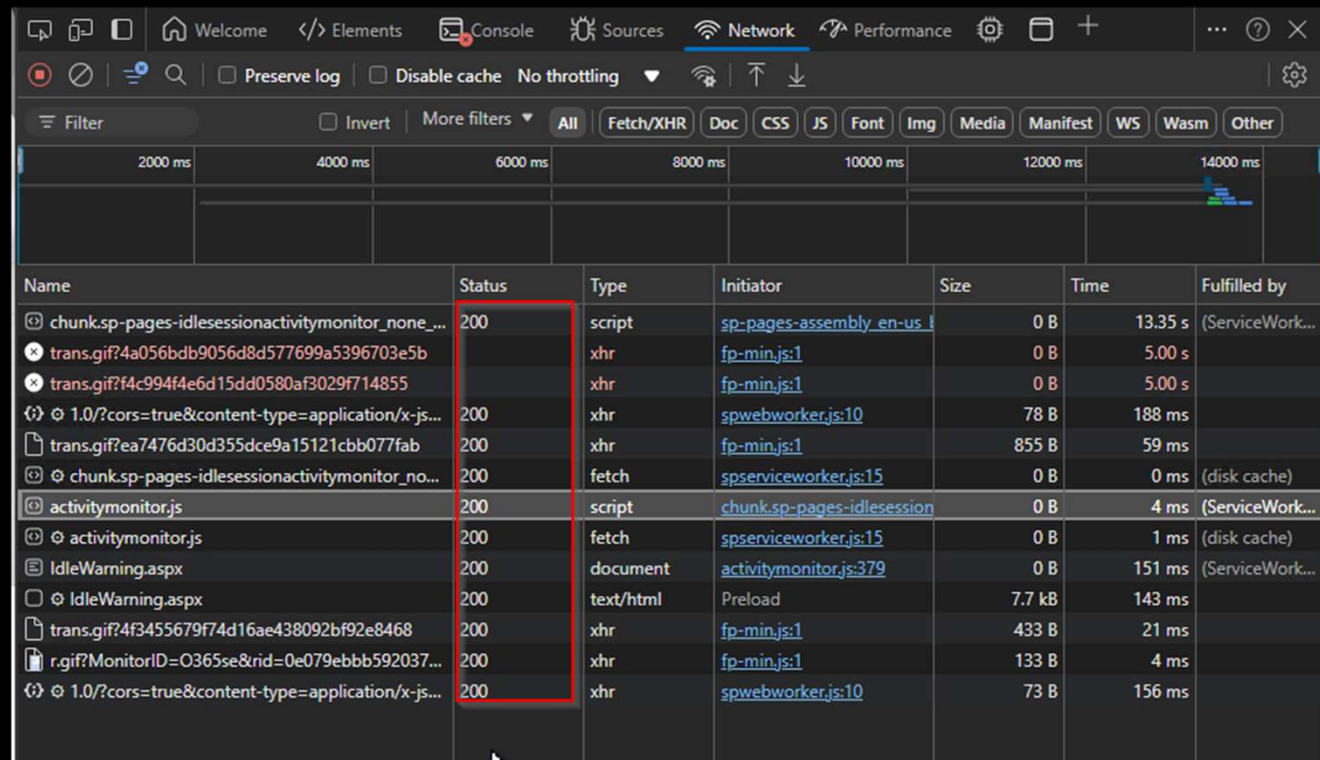
DEMO

Global Secure Access – Conditional Access

Data Plan protection – Tenant Restriction



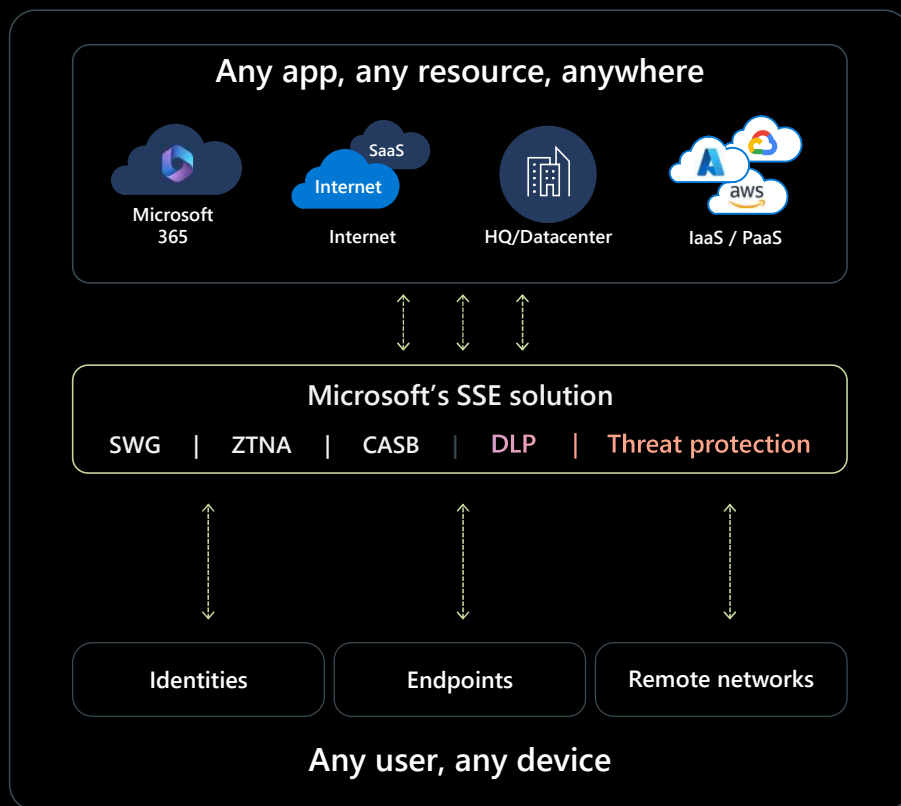
Access control - ZTNA



Name	Status	Type	Initiator	Size	Time	Fulfilled by
chunk.sp-pages-idlesessionactivitymonitor_none...	200	script	sp-pages-assembly_en-us...	0 B	13.35 s	(ServiceWork...
trans.gif?4a056bdb9056d8d577699a5396703e5b	200	xhr	fp-min.js:1	0 B	5.00 s	
trans.gif?f4c994f4e6d15dd0580af3029f714855	200	xhr	fp-min.js:1	0 B	5.00 s	
1.0/?cors=true&content-type=application/x-js...	200	xhr	spwebworker.js:10	78 B	188 ms	
trans.gif?ea7476d30d355dce9a15121cbb077fab	200	xhr	fp-min.js:1	855 B	59 ms	
chunk.sp-pages-idlesessionactivitymonitor_no...	200	fetch	spserviceworker.js:15	0 B	0 ms	(disk cache)
activitymonitor.js	200	script	chunk.sp-pages-idlesession	0 B	4 ms	(ServiceWork...
activitymonitor.js	200	fetch	spserviceworker.js:15	0 B	1 ms	(disk cache)
IdleWarning.aspx	200	document	activitymonitor.js:379	0 B	151 ms	(ServiceWork...
IdleWarning.aspx	200	text/html	Preload	7.7 kB	143 ms	
trans.gif?4f3455679f74d16ae438092bf92e8468	200	xhr	fp-min.js:1	433 B	21 ms	
r.gif?MonitorID=0365se&rid=0e079ebbb592037...	200	xhr	fp-min.js:1	133 B	4 ms	
1.0/?cors=true&content-type=application/x-js...	200	xhr	spwebworker.js:10	73 B	156 ms	

SASE Ecosystem

Seamless Network Security Integrations



Seamless operation through Microsoft Entra unified solution

Flexibility in choosing additional network security modules to add to Microsoft Entra

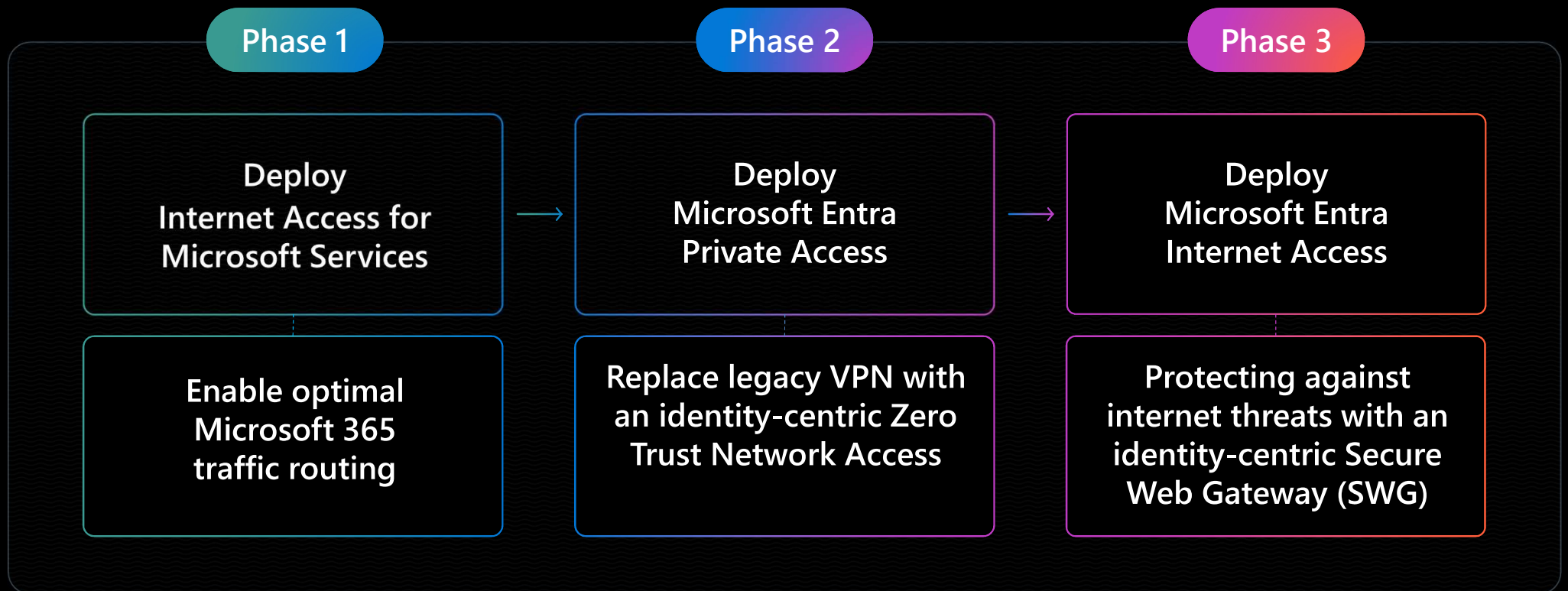
Enhanced network security through integrated capabilities

Netskope One DLP and ATP integrate seamlessly with Microsoft's SSE solution.



And more....

Security Service Edge Journey



Microsoft public Roadmap – Ignite 2024

Q4 2024

- Private application discovery
- Private DNS for Private Access
- Private network connectors for Azure, AWS, GCP
- Universal Continuous Access Evaluation (CAE)
- TLS Inspection for Internet Access
- MacOS client for cross OS Platform
- iOS client for Microsoft and Private Access traffic
- In-product marketplace for 3p integrated solutions
- SD-WAN / Connectivity partnerships with other SASE providers

H1 2025

- Multi-geo connectors
- Private Access for Domain Controllers
- Threat intelligence filtering
- iOS client for Internet Access traffic
- US Gov cloud support

H2 2025+

- BYOD / unmanaged device support
- Network DLP / file type policy
- Cloud firewall
- Intrusion prevention
- Anti-malware

...

Thank you 😊

