

# Unleashing the power of the Secure Service Edge

## Microsoft Entra Private and Internet Access

Danilo Verhaert  
*Technical Specialist Security @ Microsoft*



# Danilo Verhaert

- Technical Specialist Security, Microsoft
- Previously: Cybersecurity consultant @Deloitte
- Gamer, runner, tech enthusiast





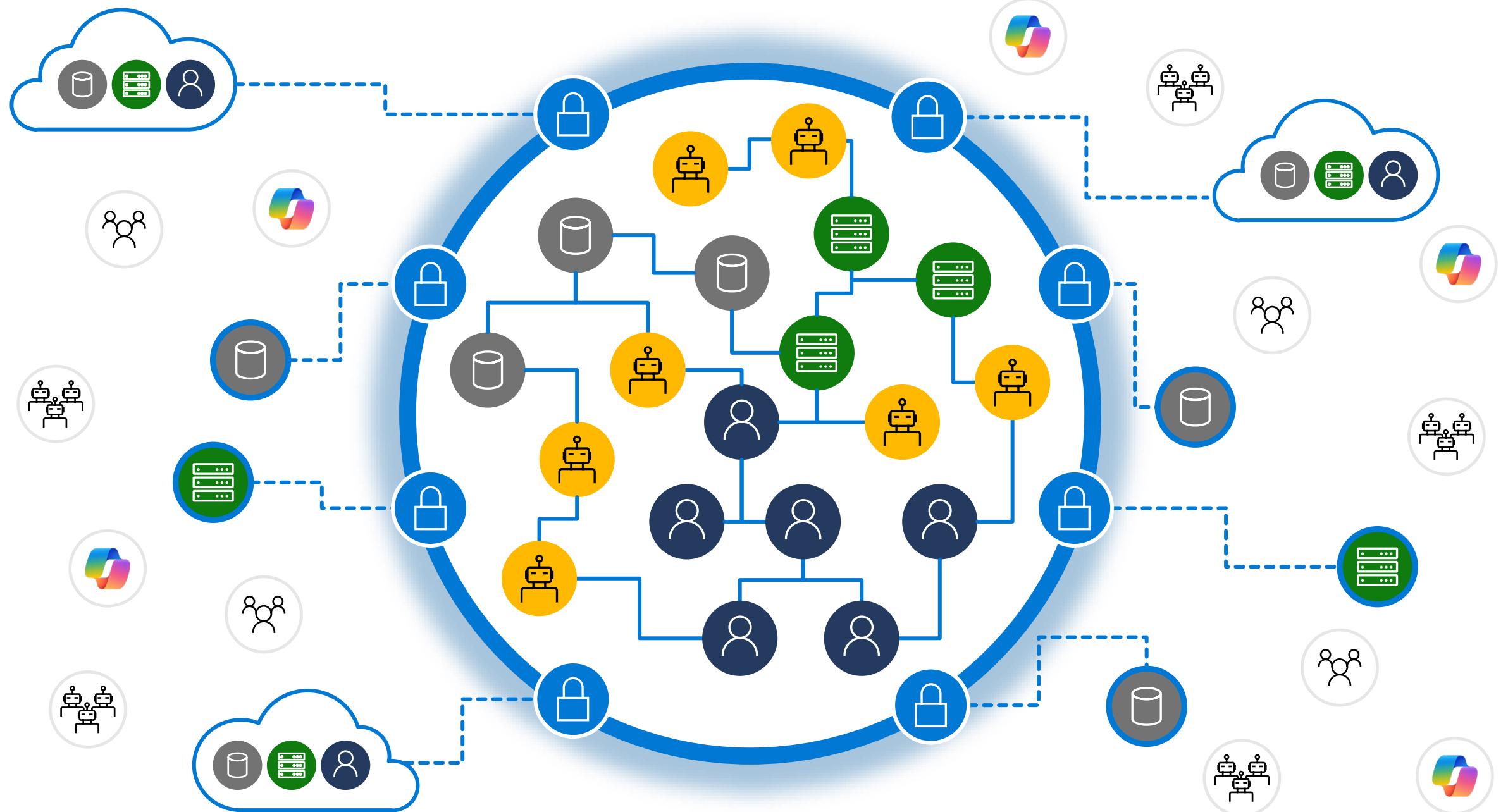
**Danilo Verhaert**  
Technical Specialist Security at Microsoft



# Agenda

- › Legacy network security challenges
- › Microsoft's Security Service Edge (SSE) solution
  - › Microsoft Entra Internet Access
  - › Microsoft Entra Private Access
- › Learn more







Proliferation of identities

**>300B**

passwords in use by humans and machines



Employees access more than

**1,500**

applications in the average enterprise



Increase in cybercrime

**7,000**

password attacks per second in 2024



Token Replay attacks

**2x**

increase since 2023

# Microsoft Entra product family

Establish Zero Trust  
access controls



Microsoft Entra ID  
P1

Secure access for  
your employees



Microsoft Entra Suite

Secure access for  
customers / partners



Microsoft Entra  
External ID

Secure access in  
any cloud



Microsoft Entra  
Permissions Management



Microsoft Entra  
Workload ID



Microsoft Copilot for Security



Secure access for your employees

# Introducing the Microsoft Entra Suite



Microsoft Entra  
Private Access



Microsoft Entra  
Internet Access



Microsoft Entra  
ID Governance



Microsoft Entra  
ID Protection



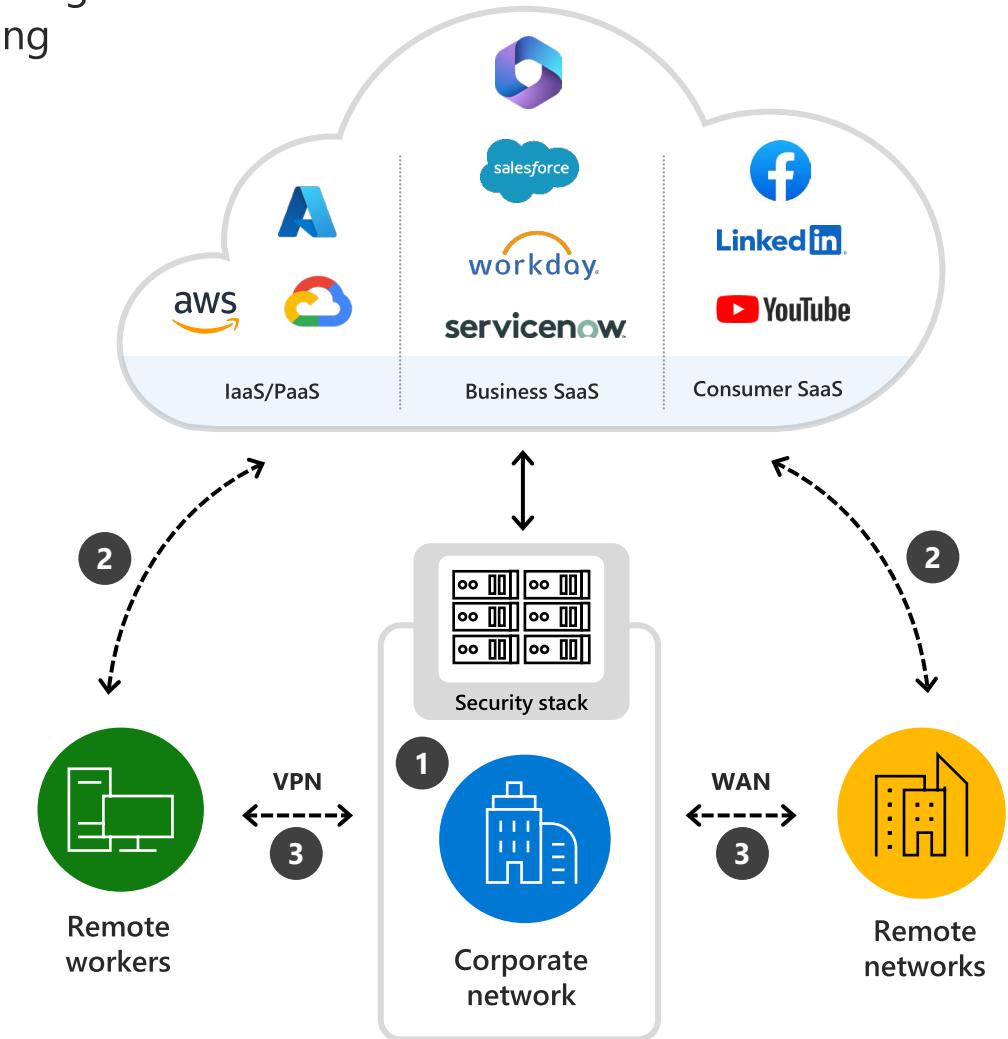
Microsoft Entra  
Verified ID  
Premium

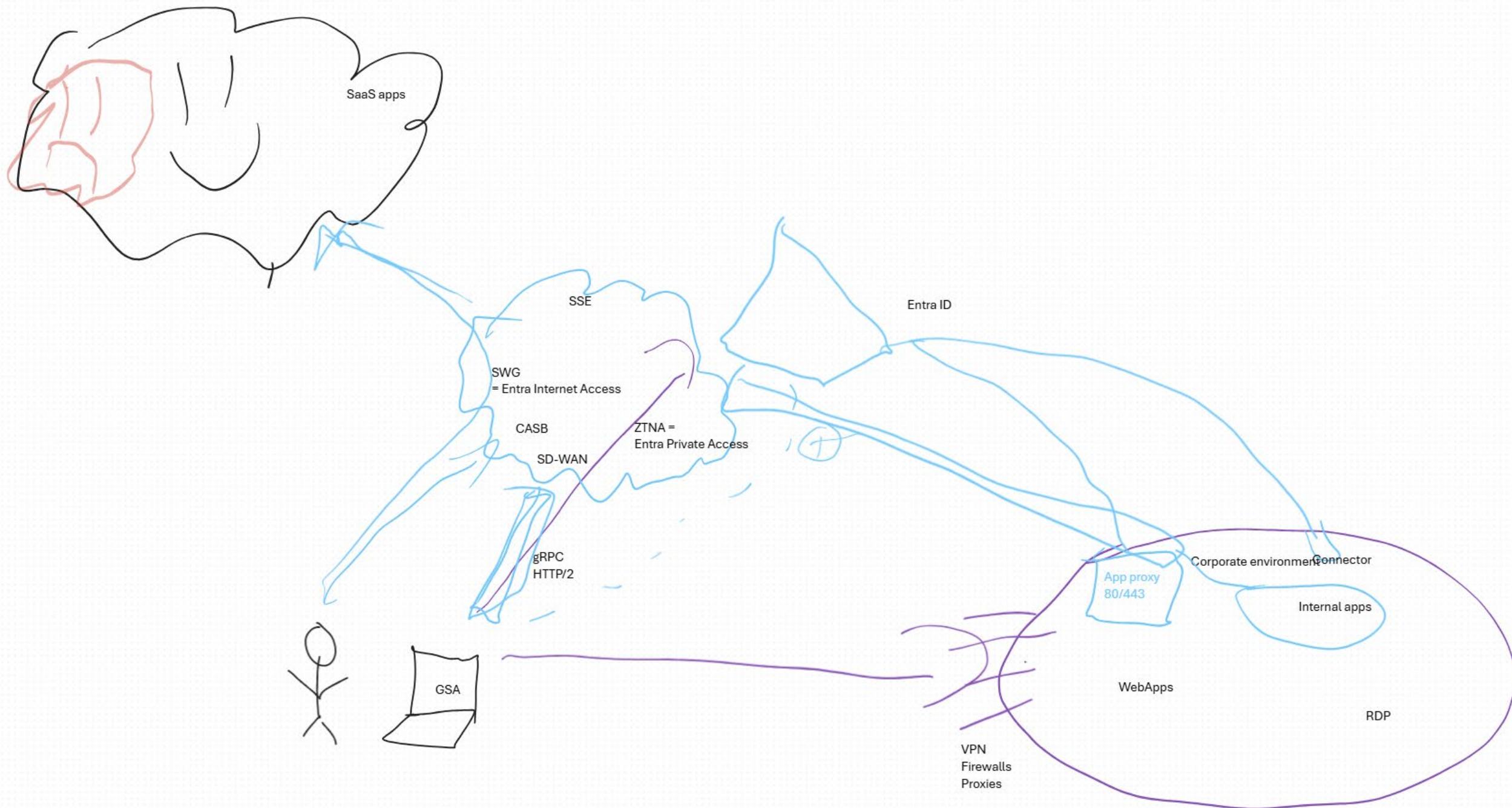
# Legacy network security approaches are no longer sufficient

The rise of cloud workloads and mobile workers is increasingly straining traditional corporate networks and network security models, resulting in security risks and poor user experience

## Challenges with conventional approaches

- 1 Dramatic traffic increase strains network capacity and on-premises security stack. Sub-optimal user experience on account of traffic hair-pinning.
- 2 Users circumvent IT controls and access resources directly
- 3 Compromised users/devices can move laterally on traditional corporate networks





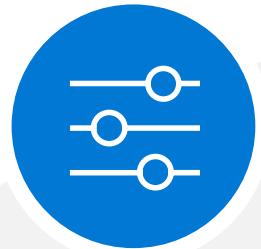


# Microsoft's Security Service Edge (SSE) solution

# Microsoft's Security Service Edge (SSE) solution

## Enforce Conditional Access Controls

Extend Conditional Access and continuous access evaluation to any application or resource



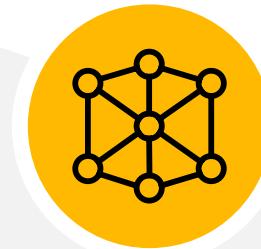
## Streamline network security

Escape the complexity and cost of traditional stand-alone network security tools with comprehensive cloud-delivered services.

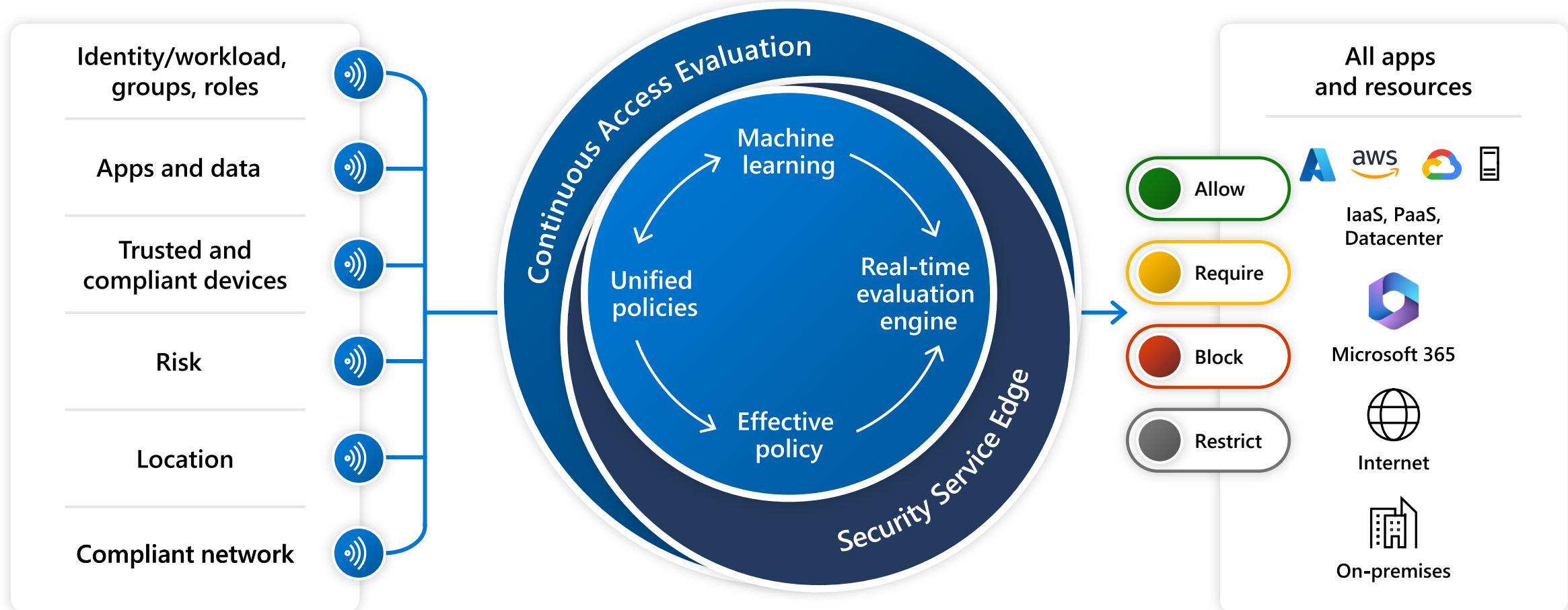


## Deliver fast, consistent hybrid work experience

Boost hybrid work productivity with fast and seamless access through a globally distributed secure network edge, with over 70 Azure regions and 190+ Edge sites to connect through



# Enhance Conditional Access with new conditions and controls



## Global Secure Access

Over the coming months, Internet Access for Microsoft Services (part of Entra Global Secure Access) will be deployed to Windows devices company-wide to support the Secure Future Initiative (SFI).

Once it's assigned to your work profile, your access to Exchange, OneDrive, and SharePoint resources will be secured by GSA.

This is just the first step in our GSA journey—more features will be rolled out in the future!

### What is Global Secure Access?

Microsoft Entra Global Secure Access (GSA) is part of [Microsoft's Security Service Edge \(SSE\)](#), a new type of cloud-based security solution developed for our hybrid world. An SSE **combines multiple security functions**—like identity verification, safe browsing, and cloud app protection—into a unified service.



#### Built for a hybrid workforce

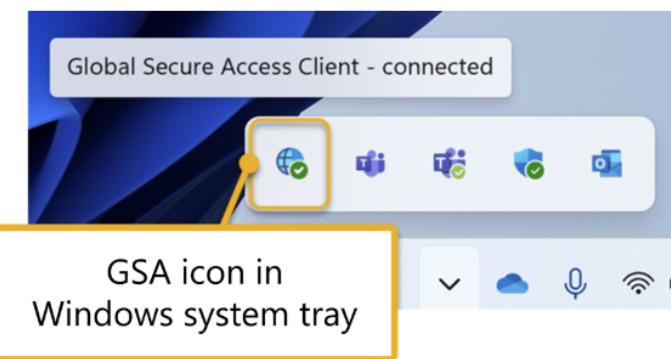
Built on the principles of [Zero Trust](#), GSA provides the right people with the right access to the right information. For example, if you need to visit a private SharePoint site, GSA verifies your identity and device before granting access. And it only grants access to *that site*—not the entire network. This means that even if you're working from a coffee shop or any other remote location, your connection remains secure, and you can get the resources you need without any hassle. [Learn more about GSA on Microsoft Learn](#).

#### What to expect

As of January 2025, [Internet Access for Microsoft Services](#) (part of GSA) is being rolled out by organization.

Except for the new icon in your taskbar, you shouldn't notice any difference in how you work. GSA will install silently and automatically in the background on your Windows device(s). Once installed, you'll benefit from GSA's enhanced security when connecting to Exchange, OneDrive, and SharePoint resources.

GSA includes multiple security functions; Internet Access for Microsoft Services is just the first step. More GSA features will be available in the



# Enable traffic forwarding profiles

The screenshot shows the Microsoft Entra admin center interface. The left sidebar includes sections like Devices, Applications, Protection, Identity governance, External Identities, and Global Secure Access (Preview). Under Global Secure Access (Preview), the 'Traffic forwarding' option is selected. The main content area is titled 'Traffic forwarding' and contains a section titled 'Manage traffic forwarding profiles'. It explains that traffic forwarding profiles allow admins to select which traffic should be acquired and forwarded to Global Secure Access. It notes that once selected, the forwarding profiles are assigned to any device in the tenant that is running the Global Secure Access client. It also mentions that the ability to assign forwarding profiles to users and groups will be added in the future. Below this, it states that traffic forwarding profiles for Microsoft 365 and Internet can be assigned to remote networks/branch connections to support client less devices, with a link to 'Learn more'. Three traffic forwarding profiles are listed: 'Microsoft 365 access profile' (Enabled, last modified on 10/16/2023, 02:18 PM), 'Private access profile' (Enabled, last modified on 10/16/2023, 02:18 PM), and 'Internet access profile' (Enabled, last modified on not available). Each profile has details about its application scope, linked Conditional Access policies, and remote network assignments. The 'Microsoft 365 access profile' is highlighted with a yellow border.

**Microsoft 365 access profile**  
Enabled  
Last modified on 10/16/2023, 02:18 PM

Applies to: All Microsoft 365 traffic

Microsoft 365 traffic policies: 3 policies [View](#)

Linked Conditional Access policies: None

Remote network assignments: 0 assigned remote networks [View](#)

**Private access profile**  
Enabled  
Last modified on 10/16/2023, 02:18 PM

Applies to: Private resources

Private access policies: Quick Access, 0 Applications

Linked Conditional Access policies: None

Remote network assignments: Not applicable

**Internet access profile**  
Enabled  
Last modified on not available

Applies to: All internet traffic except Microsoft 365

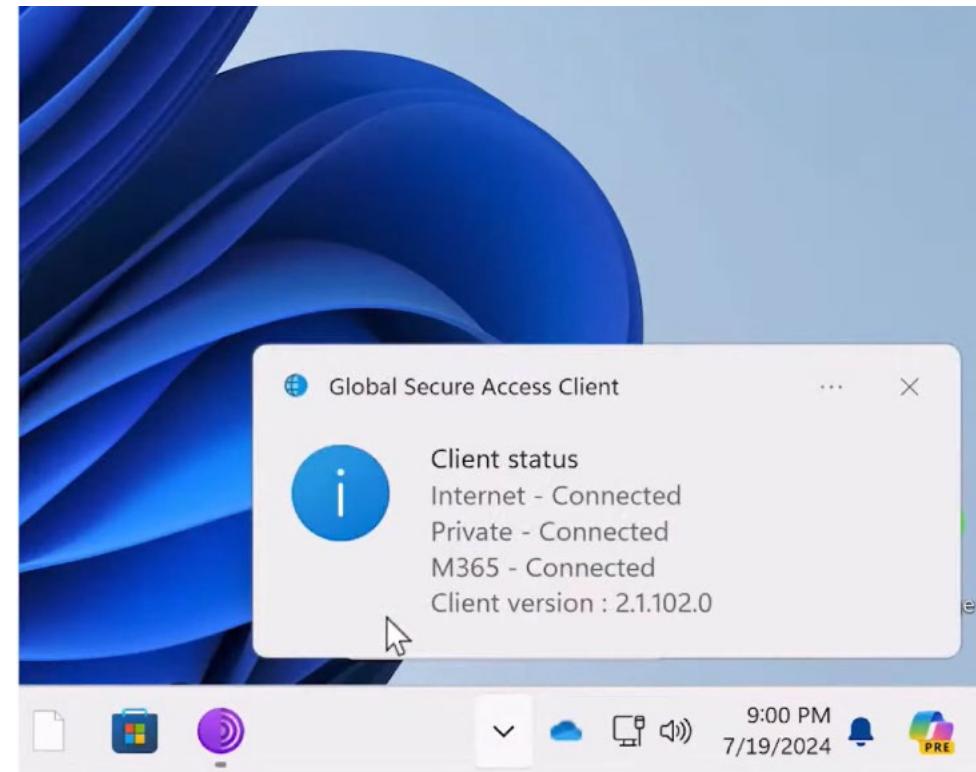
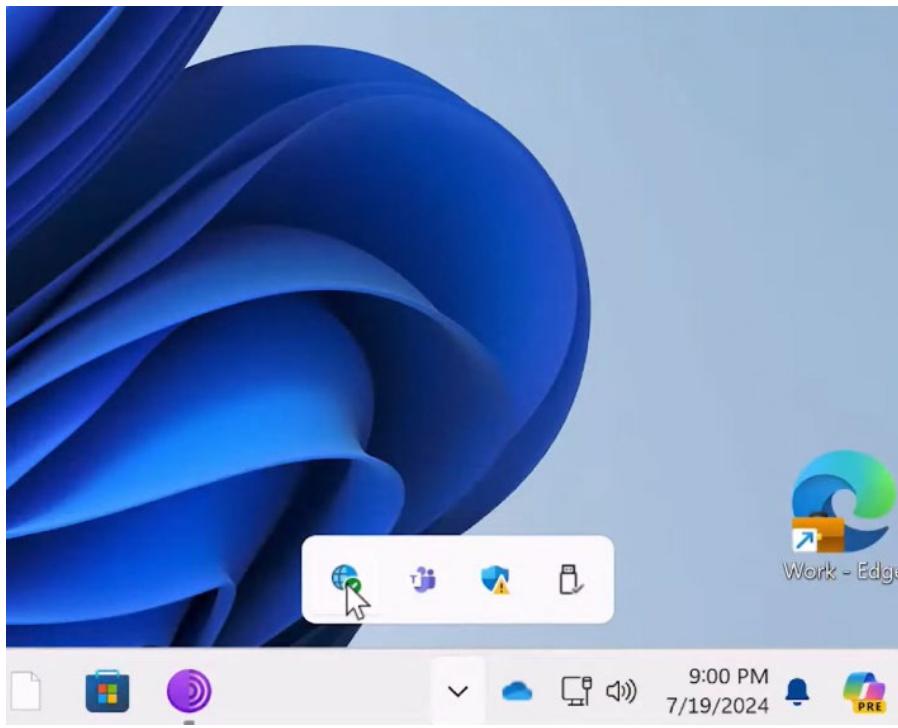
Internet access policies: Web traffic (HTTP/S on TCP over IPv4, assuming standard ports 80/443)

Linked Conditional Access policies: None

Remote network assignments: Not applicable

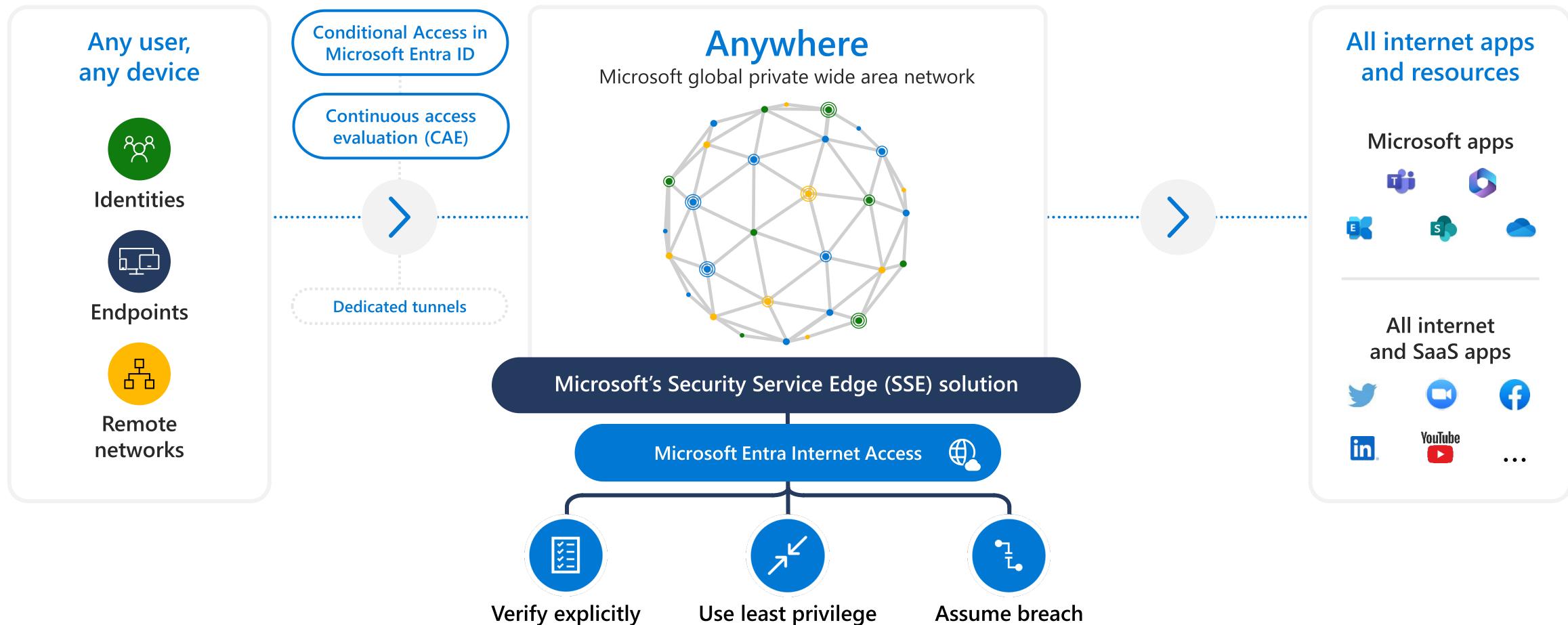
# Microsoft Entra Internet Access





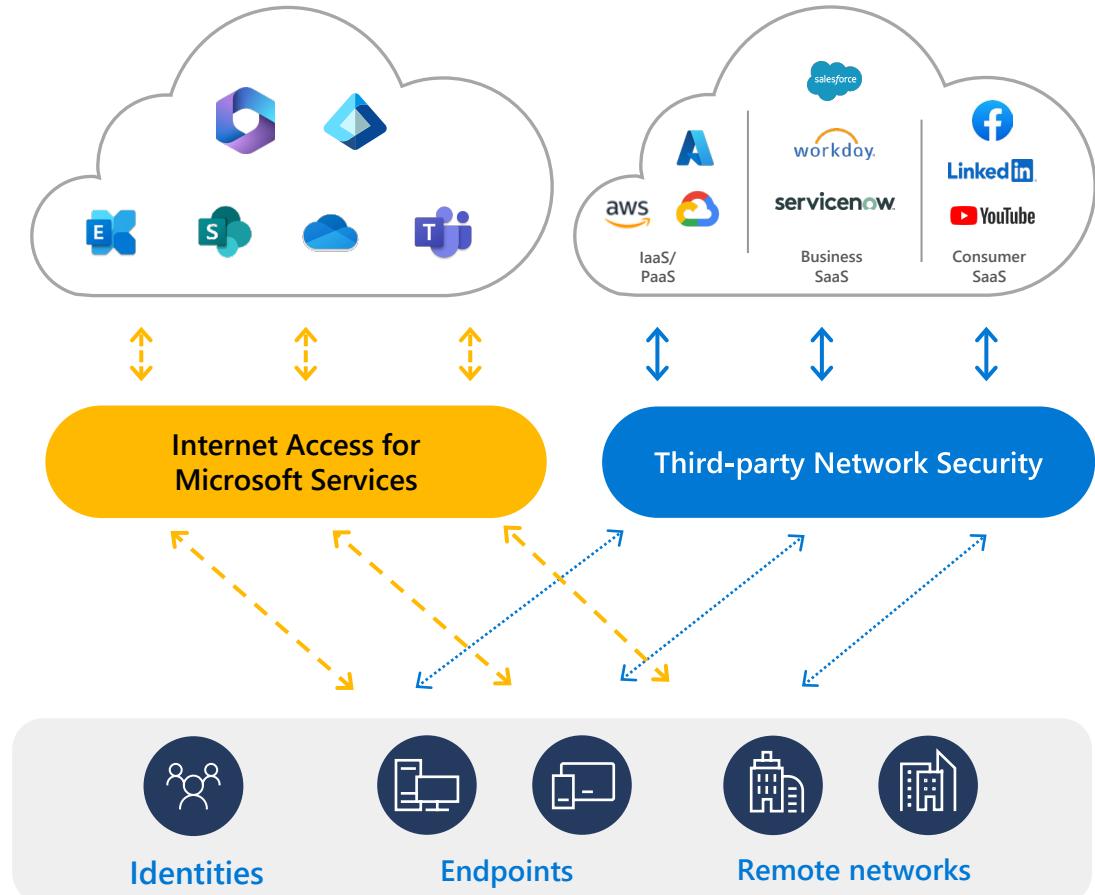
# Microsoft Entra Internet Access

An identity-centric secure web gateway (SWG)



# Enhance Microsoft Entra ID capabilities with direct connectivity to supported Microsoft services

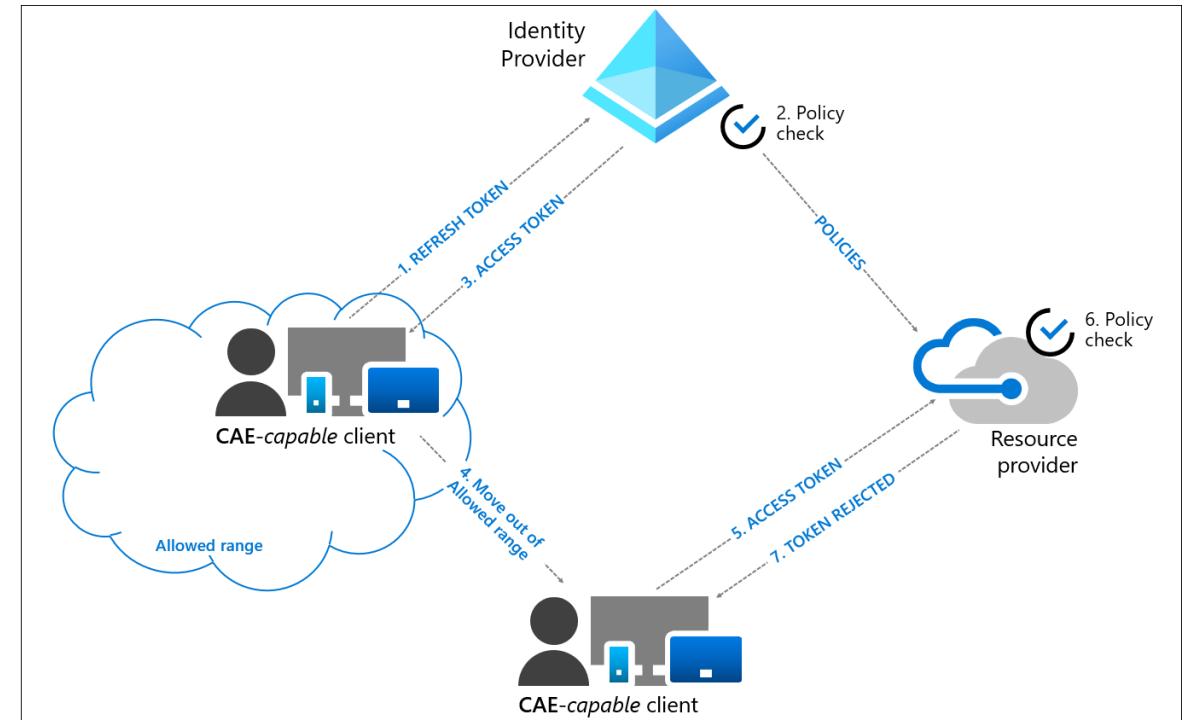
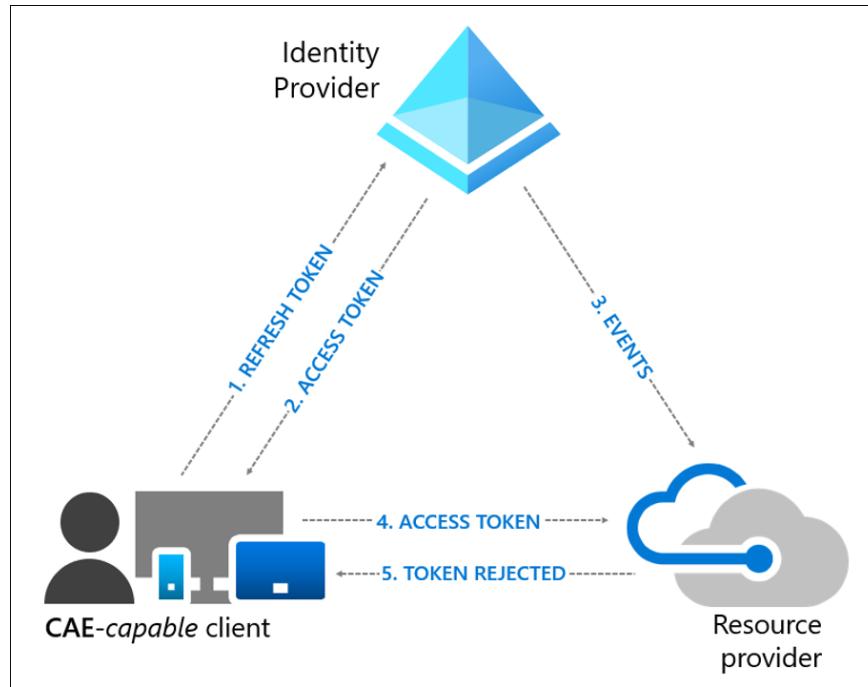
- › Deliver secure, fast, & consistent access to Microsoft services. Send traffic directly to Microsoft services with any device and from any network.
- › Strengthen access controls for any network by enhancing Microsoft Entra ID Conditional Access and Tenant Restrictions v2 access controls.
- › Gain visibility and respond to threats faster with enhanced activity logs, original source IP in Entra ID sign-in logs, and enriched security event data for faster threat detection and response.



Works side-by-side with other solutions for private and public network access.

# Continuous Access Evaluation

- Entra side: Can revoke tokens directly
  - On token expiry, resource providers will reject tokens and ask for a claim challenge
  - For SSE, this can happen instantly. For other services, an enabling service/resource is required



# Microsoft Entra Private Access

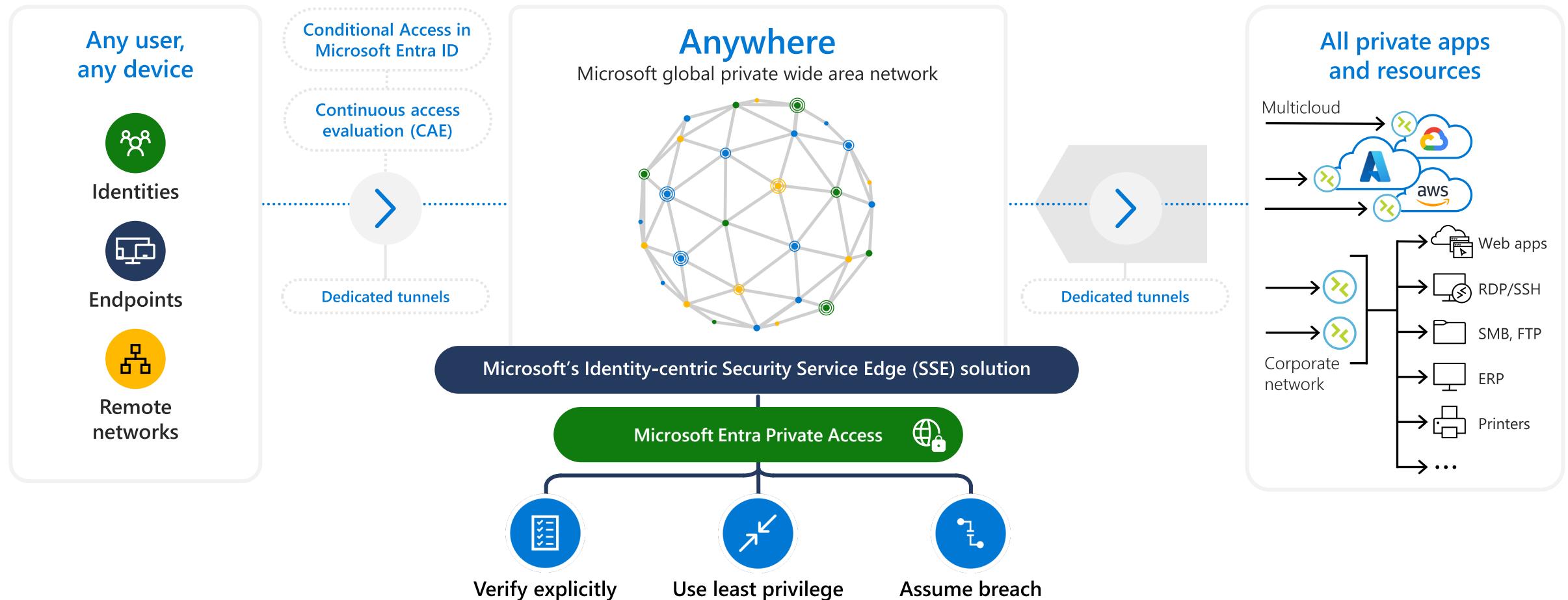


# Key selling points

- Power of conditional access to everything
  - On-prem workloads
  - Custom applications
  - MFA everywhere!
- More granular than legacy VPN
  - Only access to specific apps and not everything
  - Port-level granularity
  - Can block certain content/URLs/FQDNs
- Deep monitoring and insights
- Fast consistent access everywhere through the MS SWG/WAN

# Microsoft Entra Private Access

An identity-centric Zero Trust Network Access (ZTNA)



# Key scenarios and use cases



**Replace legacy VPNs with Zero Trust Network Access (ZTNA)** and secure access to any private app or resource—without a VPN—to reduce your attack surface, mitigate lateral threat movement, while reducing operational complexity



**Reduce risk by enforcing adaptive Conditional Access** controls across all your private apps and resources



**Enforce adaptive multifactor authentication (MFA) on on-premises private apps and resources** including legacy and custom apps, command line access tools, file shares, databases, and more



**Deliver fast and easy access at global scale** and enable secure connectivity from different OS platforms (Windows, Android, iOS\*, MacOS\*)



**Enable single sign-on (SSO)** – support for non-https apps with SSO for legacy protocols like Kerberos

# Private app discovery

Discover and onboard private applications for segmented per-app access

## › Discover apps

Discover app segments

Create private apps using discovered app segments

## › Analytics

See app usage trends and relevant insights like usage over time, and more

## › Auto re-discovery

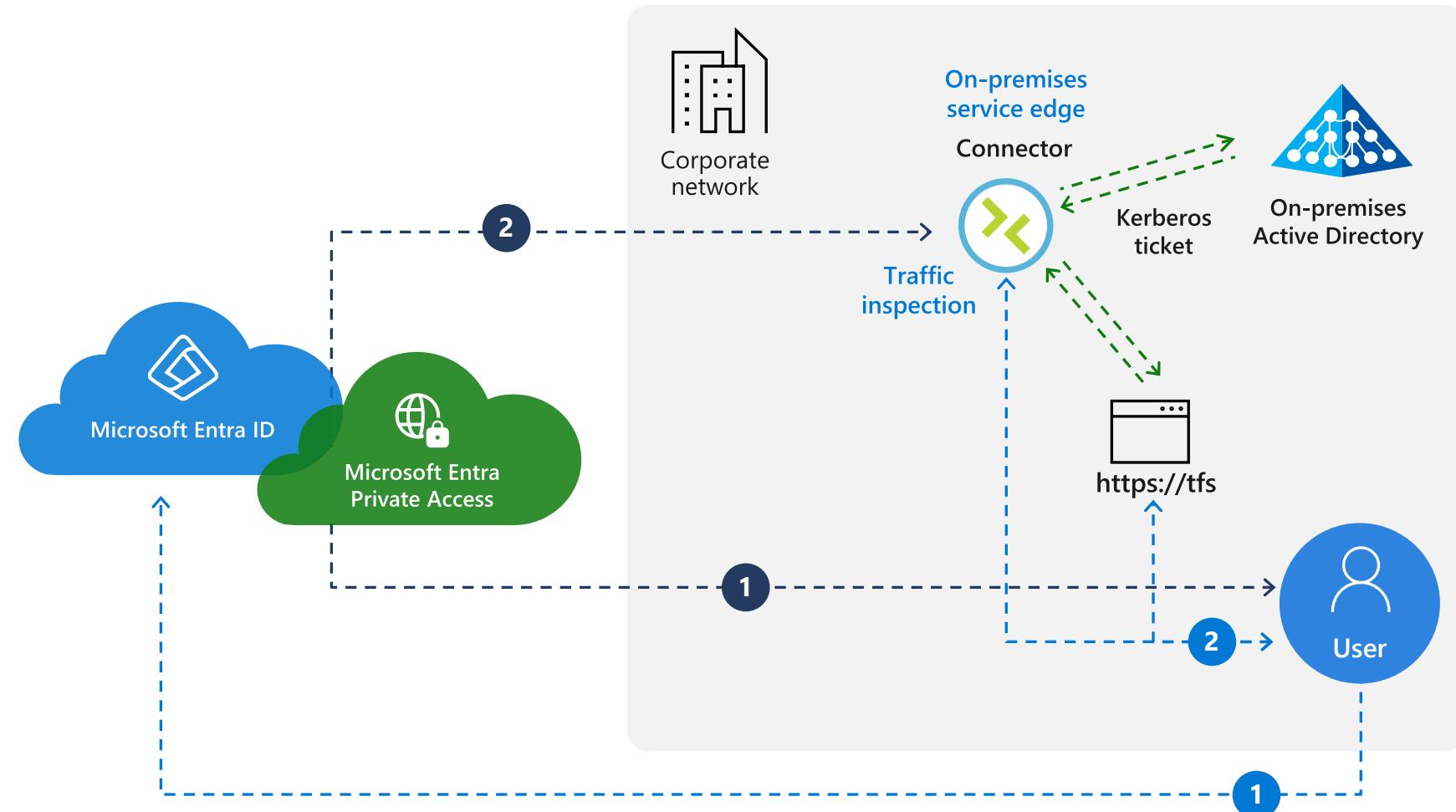
Intelligently add new discovered app segments to existing apps as additional app segments

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes 'Microsoft Entra admin cent...', a search bar, and user information 'bob@contoso.com'. Below the navigation, the breadcrumb path is 'Home > Secure access > Application discovery'. The main title is 'Application discovery' with a 'Contoso' subtitle. There are two tabs: 'Overview' and 'Discovered records', with 'Discovered records' selected. A search bar and a time range filter ('Time range : Last 24 hours') are present. The main content area displays a table of discovered records:

Discovered records ↑	Users ↑	Destination IP ↑↓	Destination port ↑↓	Protocol ↑↓	Last access ↑
nssfw.safemarch.com	1,000	192.0.2.1	80	TCP/IP	2/10/2020, 3:3
www7.checklist.com	500	192.0.2.1	1024	HTTP	2/10/2020, 3:3
mail.example.com	3,000	192.0.3.1	4000	HTTP	2/10/2020, 3:3
mail.example.com	2,500	10.255.255.25	8080	FTP	2/10/2020, 3:3
mail.example.com	1,200	192.168.255	65535	FTP	2/10/2020, 3:3
mail.example.com	3,000	192.0.3.1	4000	HTTP	2/10/2020, 3:3
mail.example.com	2,500	10.255.255.25	8080	FTP	2/10/2020, 3:3
mail.example.com	1,200	192.168.255	65535	FTP	2/10/2020, 3:3

# Local access to private apps

Intelligent, smart, and adaptive





Recycle

Bin



Microsoft

Edge

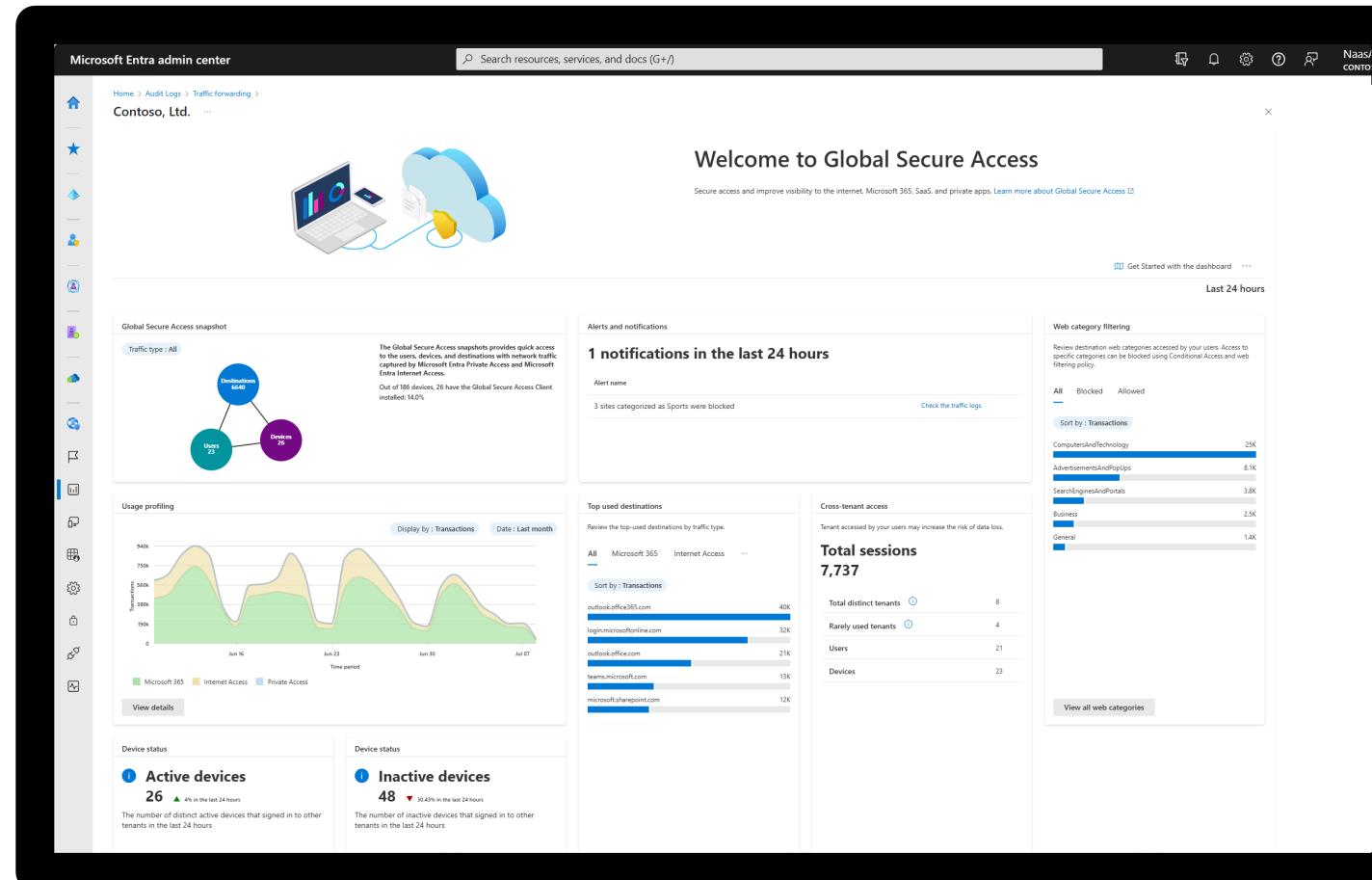
Windows PowerShell

PS C:\> ssh 10

# Comprehensive in-product dashboards and reports

## Deep insights and network analytics

- User, device, endpoint relationship maps and active/inactive device analytics
- Cross-tenant user activity monitoring
- Top destinations and usage profiling by transaction, user, devices, bytes sent/received
- Operational and security alerts\*
- Network security policy analytics\*



\*Public Preview

# Rich insights into network logs

## Visualize every request and response transaction happening

### ➤ In-product logging and reporting

Detailed and insightful network traffic logs

Extensive in-product activity exploration and filtering

Network security policy logs

### ➤ Extensive data export capabilities

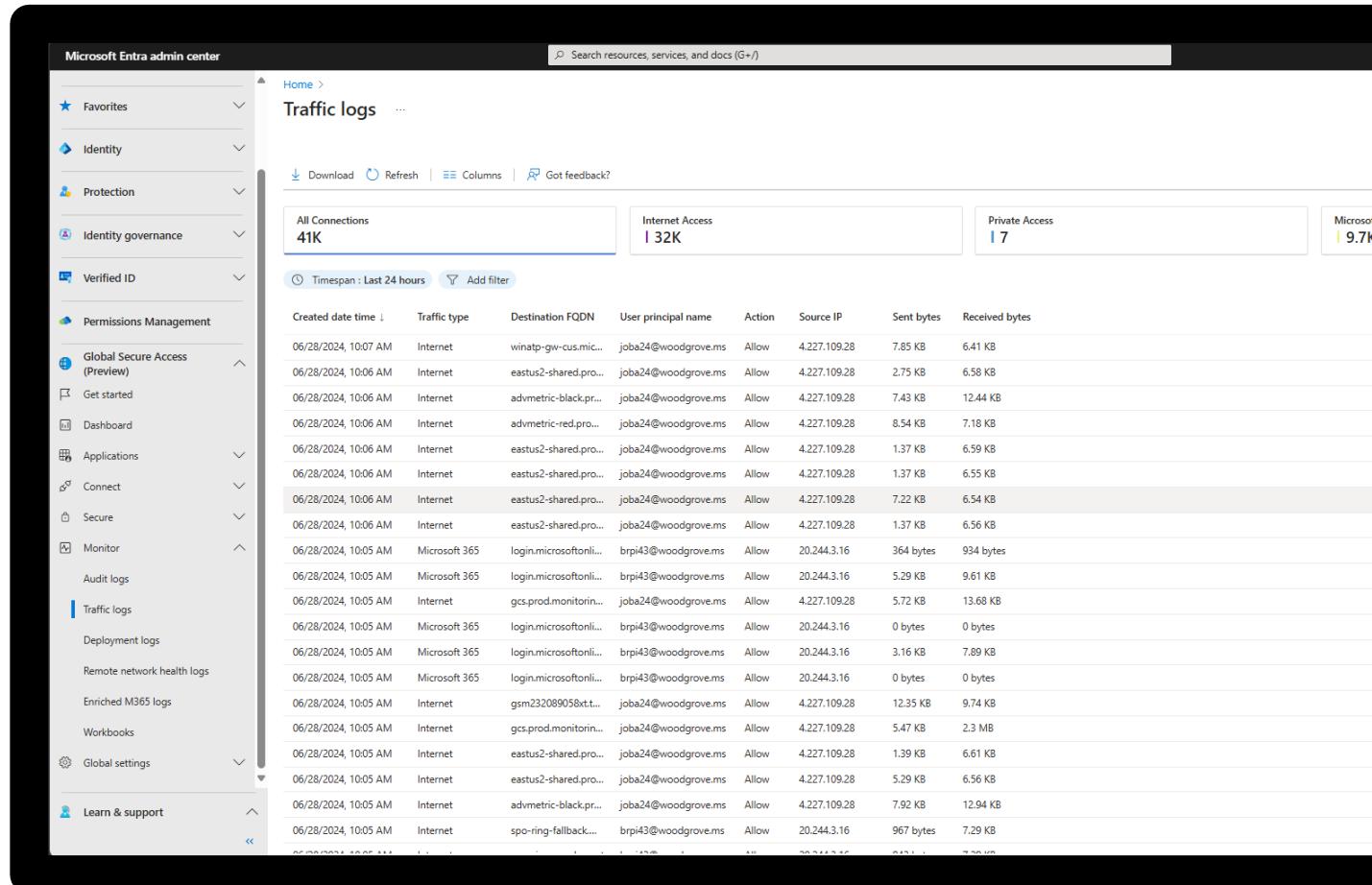
Log analytics and workbook integrations

Log export APIs\*

Integration with first- and third-party SIEM systems

Built-in solution for Sentinel, out-of-the-box reports and metrics\*\*

### ➤ Enriched Microsoft 365 logs (export only)\*



The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with various sections like Favorites, Identity, Protection, Identity governance, Verified ID, Permissions Management, Global Secure Access (Preview), Get started, Dashboard, Applications, Connect, Secure, Monitor, Audit logs, Traffic logs (which is currently selected and highlighted in blue), Deployment logs, Remote network health logs, Enriched M365 logs, Workbooks, Global settings, and Learn & support. The main content area is titled "Traffic logs". It displays three summary cards: "All Connections 41K", "Internet Access 32K", and "Private Access 7". Below these cards is a table with the following columns: Created date time, Traffic type, Destination FQDN, User principal name, Action, Source IP, Sent bytes, and Received bytes. The table lists numerous log entries from June 28, 2024, at 10:05 AM, showing various network interactions between internal users and external destinations like winatp-gw-cus.microsoft.com and eastus2-shared.preview.azurewebsites.net.

Created date time	Traffic type	Destination FQDN	User principal name	Action	Source IP	Sent bytes	Received bytes
06/28/2024, 10:07 AM	Internet	winatp-gw-cus.microsoft.com	joba24@woodgrove.ms	Allow	4.227.109.28	7.85 KB	6.41 KB
06/28/2024, 10:06 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	2.75 KB	6.58 KB
06/28/2024, 10:06 AM	Internet	advmetric-black.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	7.43 KB	12.44 KB
06/28/2024, 10:06 AM	Internet	advmetric-red.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	8.54 KB	7.18 KB
06/28/2024, 10:06 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	1.37 KB	6.59 KB
06/28/2024, 10:06 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	1.37 KB	6.55 KB
06/28/2024, 10:06 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	7.22 KB	6.54 KB
06/28/2024, 10:06 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	1.37 KB	6.56 KB
06/28/2024, 10:05 AM	Microsoft 365	login.microsoftonline.com	brpi43@woodgrove.ms	Allow	20.244.3.16	364 bytes	934 bytes
06/28/2024, 10:05 AM	Microsoft 365	login.microsoftonline.com	brpi43@woodgrove.ms	Allow	20.244.3.16	5.29 KB	9.61 KB
06/28/2024, 10:05 AM	Internet	gcs.prod.monitoring	joba24@woodgrove.ms	Allow	4.227.109.28	5.72 KB	13.68 KB
06/28/2024, 10:05 AM	Microsoft 365	login.microsoftonline.com	brpi43@woodgrove.ms	Allow	20.244.3.16	0 bytes	0 bytes
06/28/2024, 10:05 AM	Microsoft 365	login.microsoftonline.com	brpi43@woodgrove.ms	Allow	20.244.3.16	3.16 KB	7.89 KB
06/28/2024, 10:05 AM	Internet	gsm232089058xtm	joba24@woodgrove.ms	Allow	4.227.109.28	12.35 KB	9.74 KB
06/28/2024, 10:05 AM	Internet	gcs.prod.monitoring	joba24@woodgrove.ms	Allow	4.227.109.28	5.47 KB	2.3 MB
06/28/2024, 10:05 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	1.39 KB	6.61 KB
06/28/2024, 10:05 AM	Internet	eastus2-shared.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	5.29 KB	6.56 KB
06/28/2024, 10:05 AM	Internet	advmetric-black.preview.azurewebsites.net	joba24@woodgrove.ms	Allow	4.227.109.28	7.92 KB	12.94 KB
06/28/2024, 10:05 AM	Internet	spo-ring-fallback	brpi43@woodgrove.ms	Allow	20.244.3.16	967 bytes	7.29 KB

\*Public Preview

\*\*Roadmap – all timelines are subject to change

# Roadmap

- GSA client: **TLS Inspection/Termination**
- Internet Access: Threat intelligence filtering, Remote network connectivity
- Private Access: Multi-geo connectors Intelligent Local Access, Process level segmentation

# Tips for a successful PoC

- Check out the [Global Secure Access Community Resources Hub](#)
- Involve a partner
- Avoid placing connectors on DMZ networks. Place resources close to the resources
- Avoid using proxy servers
- Be good friends with the network/identity/workplace/security team

# Learn more

Community resource: [Global Secure Access Community Resources Hub](#)



Learn more about Microsoft Entra Internet Access

» <https://aka.ms/InternetAccess>

Get started and try Internet Access

» <https://aka.ms/InternetAccessTrial>

Learn more about Microsoft Entra Private Access

» <https://aka.ms/PrivateAccess>

Get started and try Private Access

» <https://aka.ms/PrivateAccessTrial>

Contact your Microsoft  
account representative





# Thank you!