Microsoft Security

Unleashing the power of the Secure Service Edge

Microsoft Entra Private and Internet Access

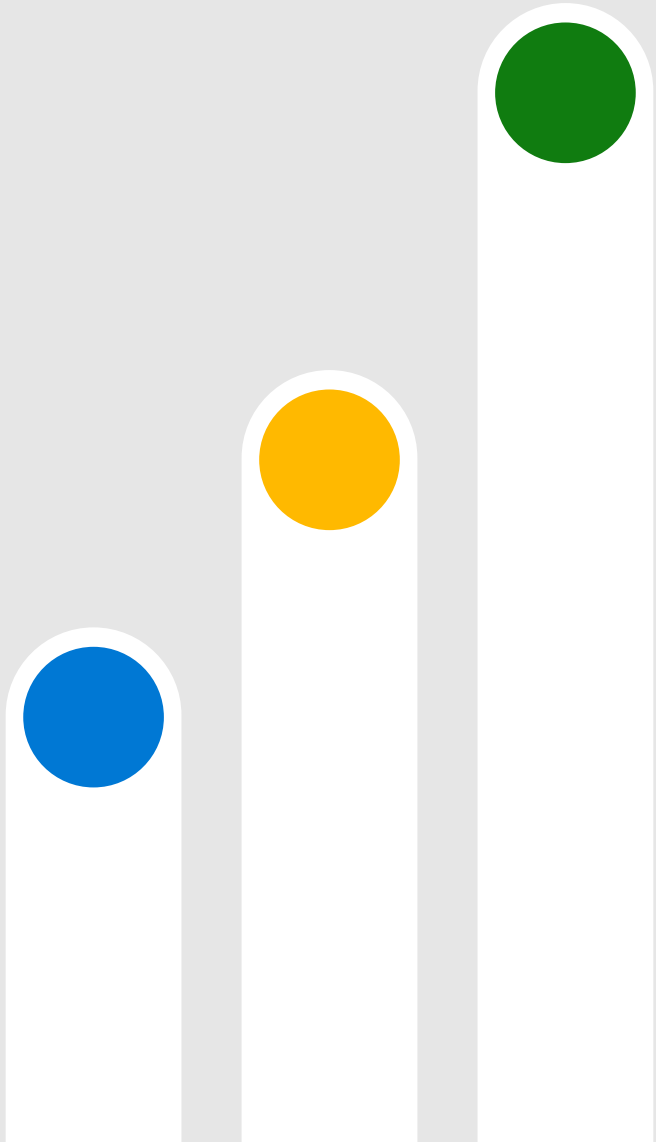
Danilo Verhaert
Technical Specialist Security @ Microsoft

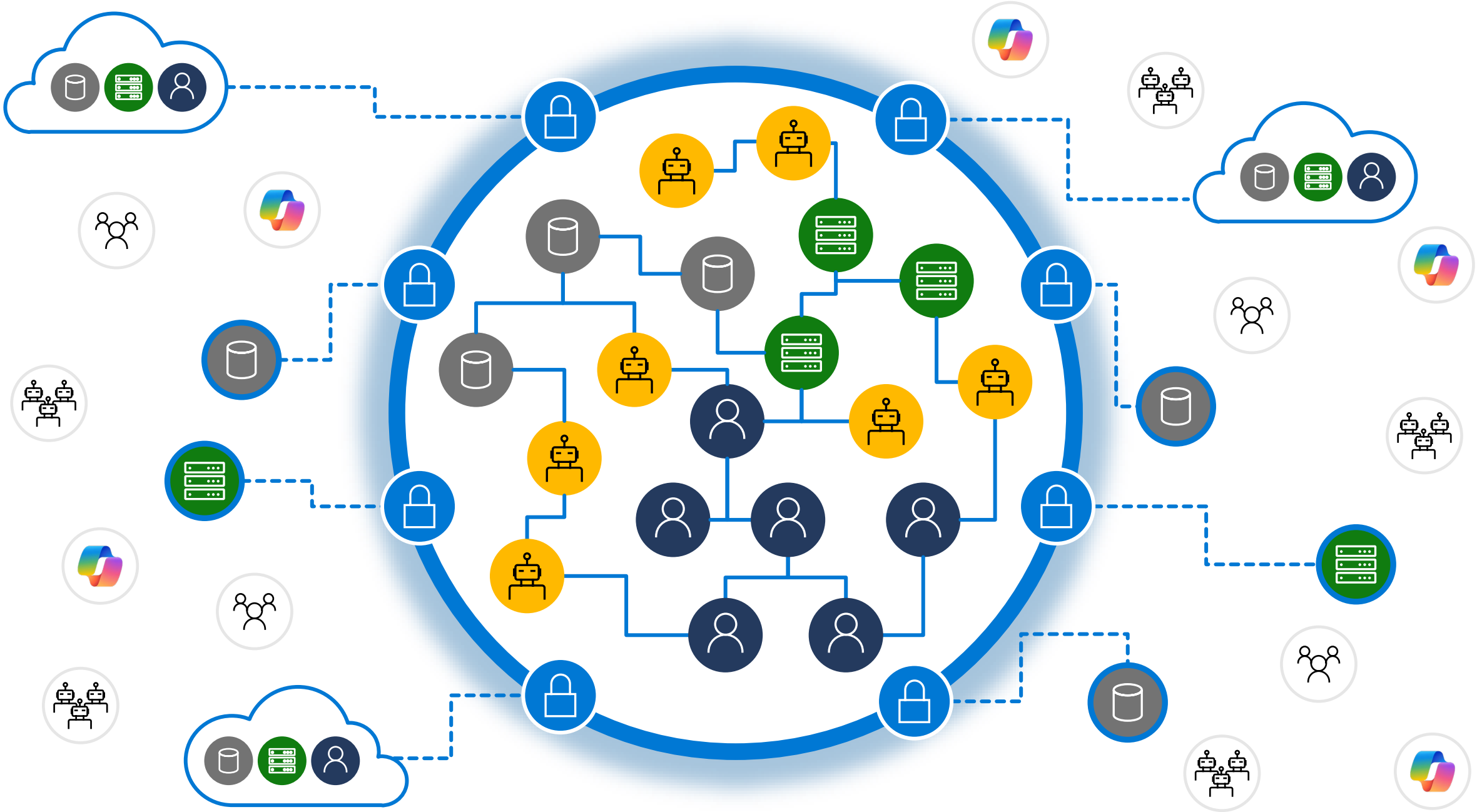
Danilo Verhaert

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

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	Secure access for your employees	Secure access for customers / partners	Secure access in any cloud
Microsoft Entra ID P1	Microsoft Entra Suite	Microsoft Entra External ID	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

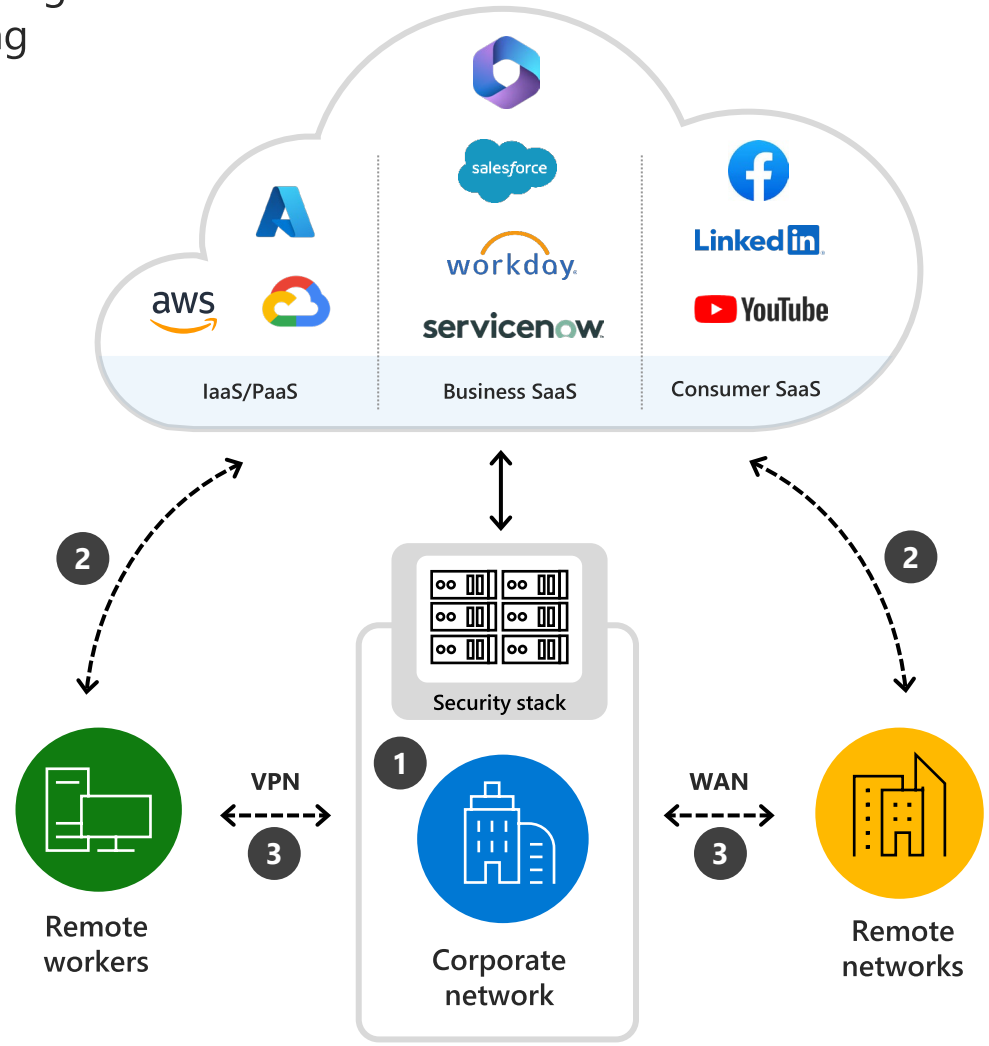
Microsoft Entra
Verified ID
Premium

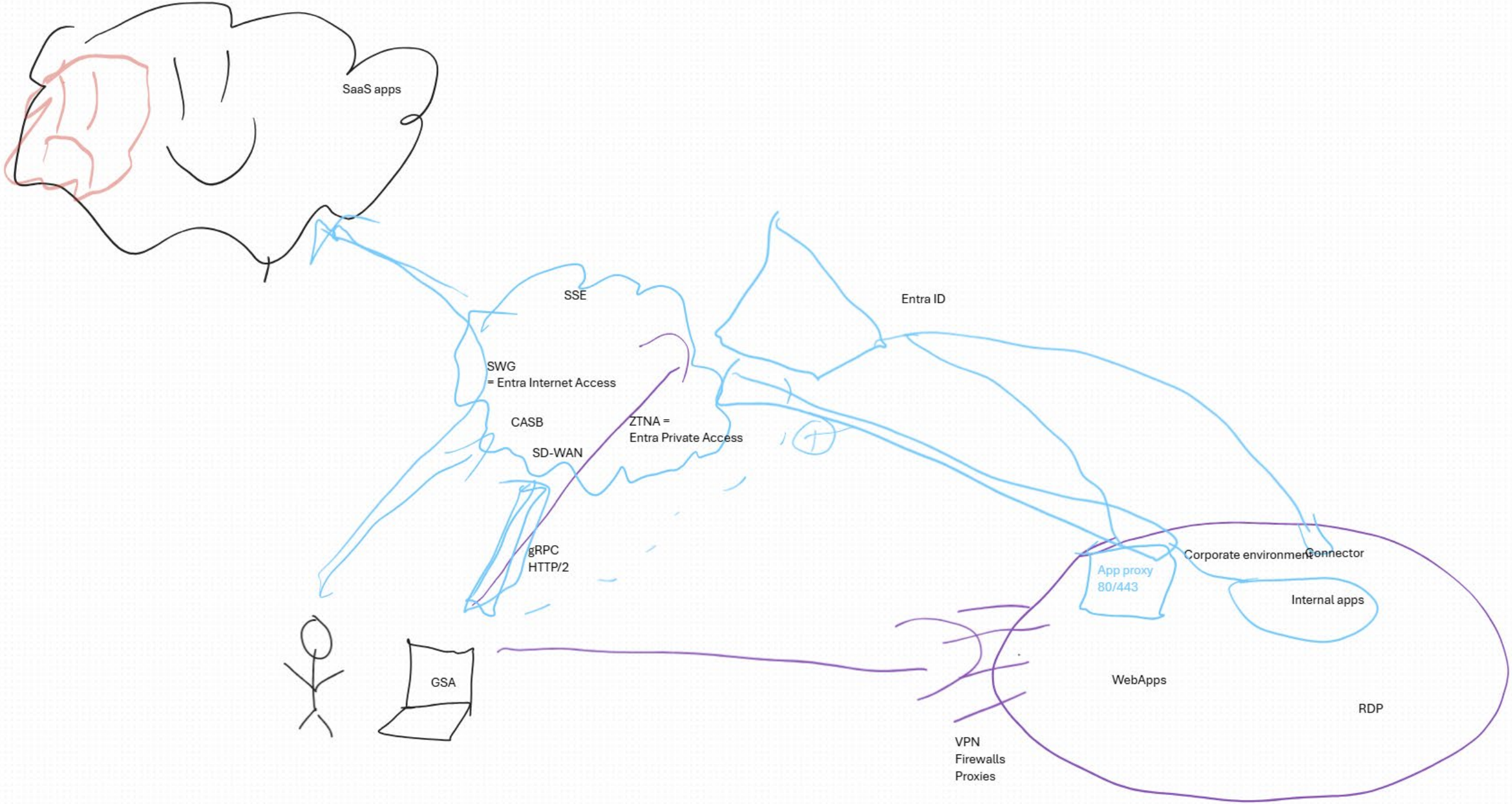
Legacy network security approaches are no longer sufficient

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




SaaS apps
SSE
Entra ID
SWG
= Entra Internet Access
CASB
ZTNA =
Entra Private Access
SD-WAN
gRPC
HTTP/2
GSA
Corporate environment
Connector
App proxy
80/443
Internal apps
WebApps
RDP
VPN
Firewalls
Proxies

Microsoft’s Security Service Edge (SSE) solution

Microsoft's Security Service Edge (SSE) solution

Enforce Conditional Access Controls

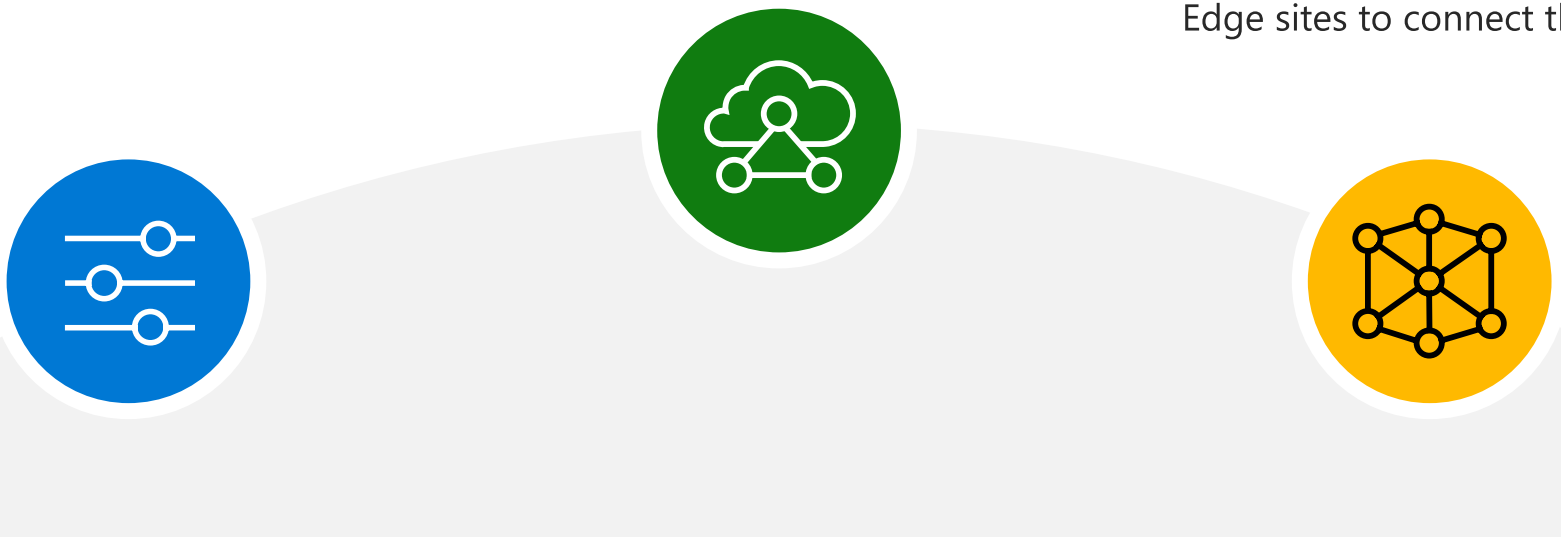
Extend Conditional Access and continuous access evaluation to any application or resource

Streamline network security

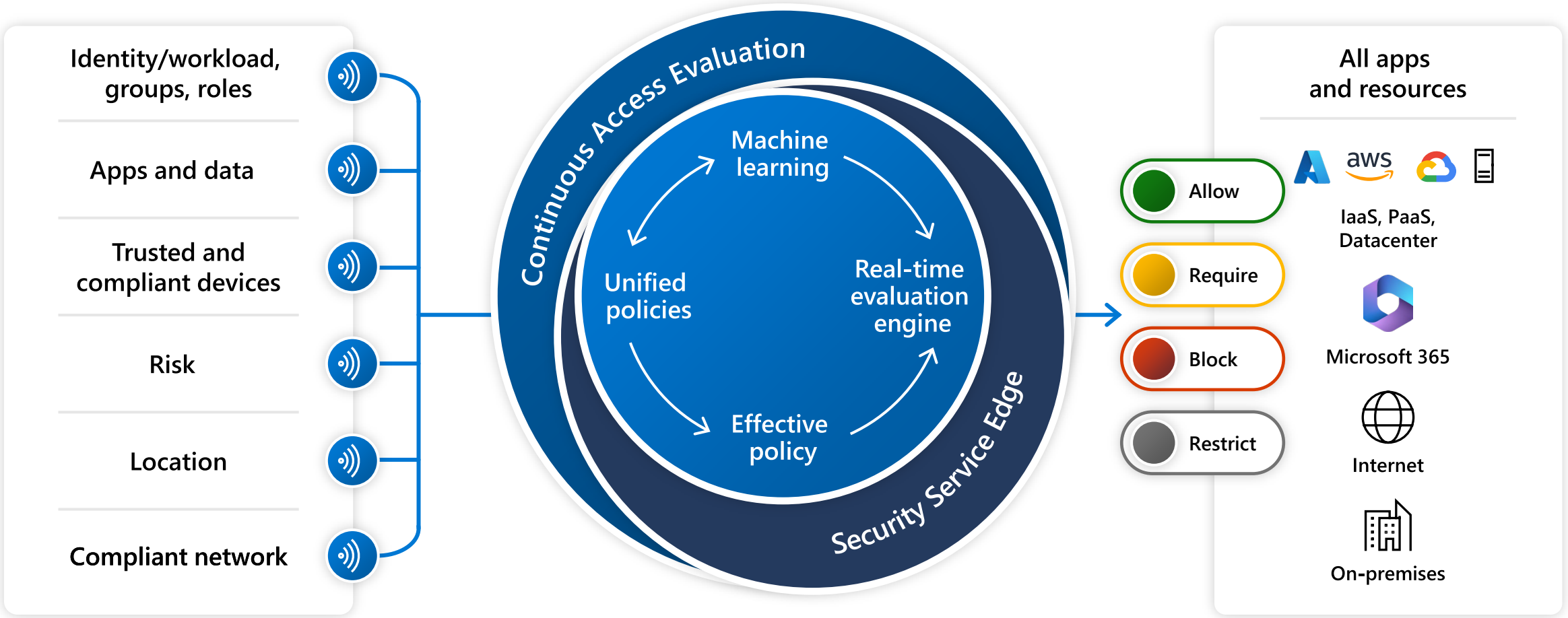
Escape the complexity and cost of traditional stand-alone network security tools with comprehensive cloud-delivered services.

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 the 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

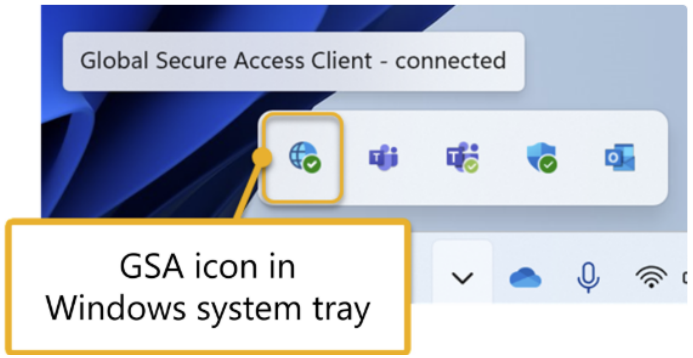
Built on the principles of Zero Trust, **GSA provides the right people with the right access to the right information**. For example, if you need to visit a private SharePoint site, GSA verifies your identity and device before granting access. And it only grants access to *that site*—not the entire network. 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

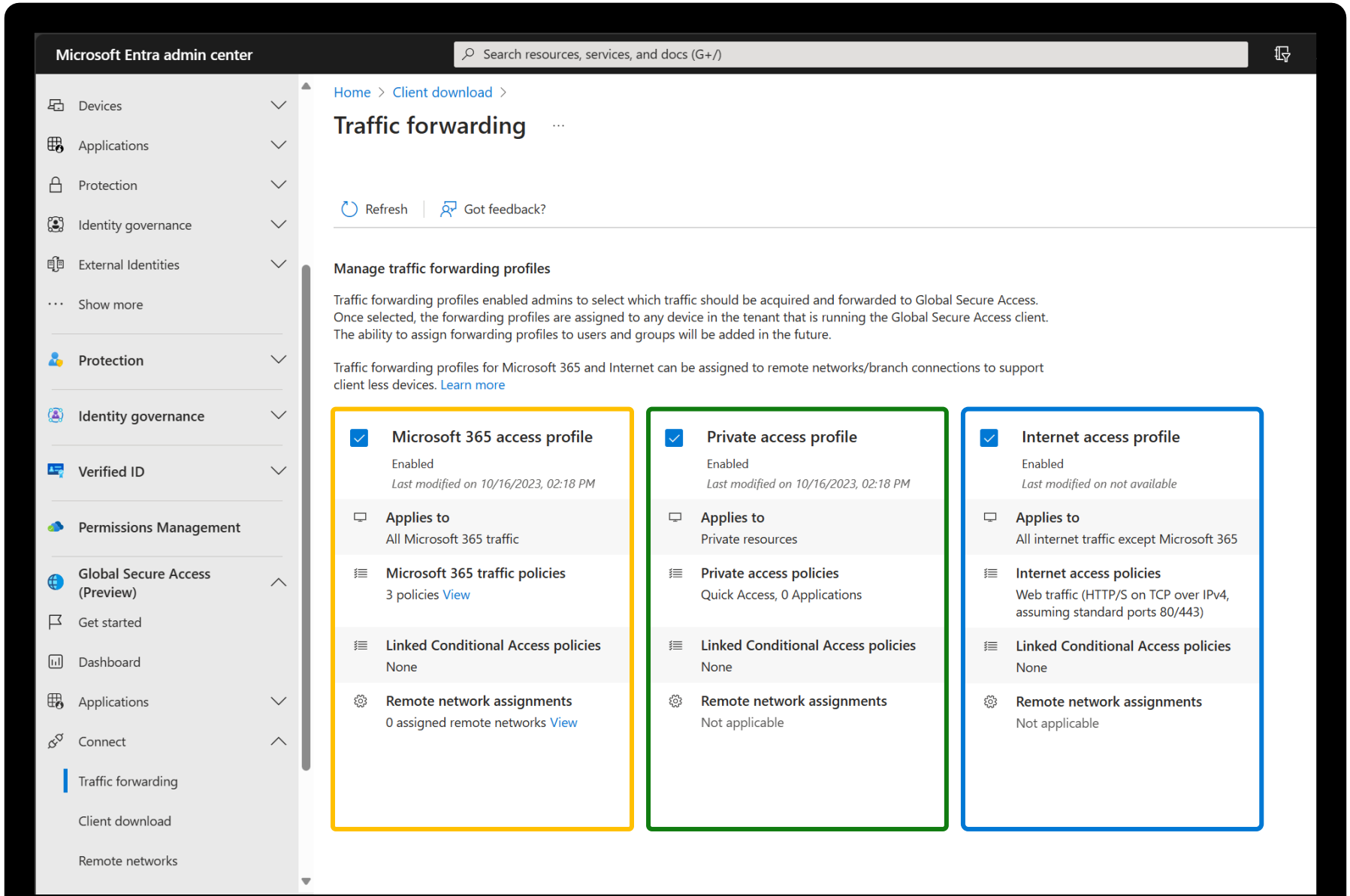
As of January 2025, Internet Access for Microsoft Services (part of GSA) is being rolled out by organization.

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.

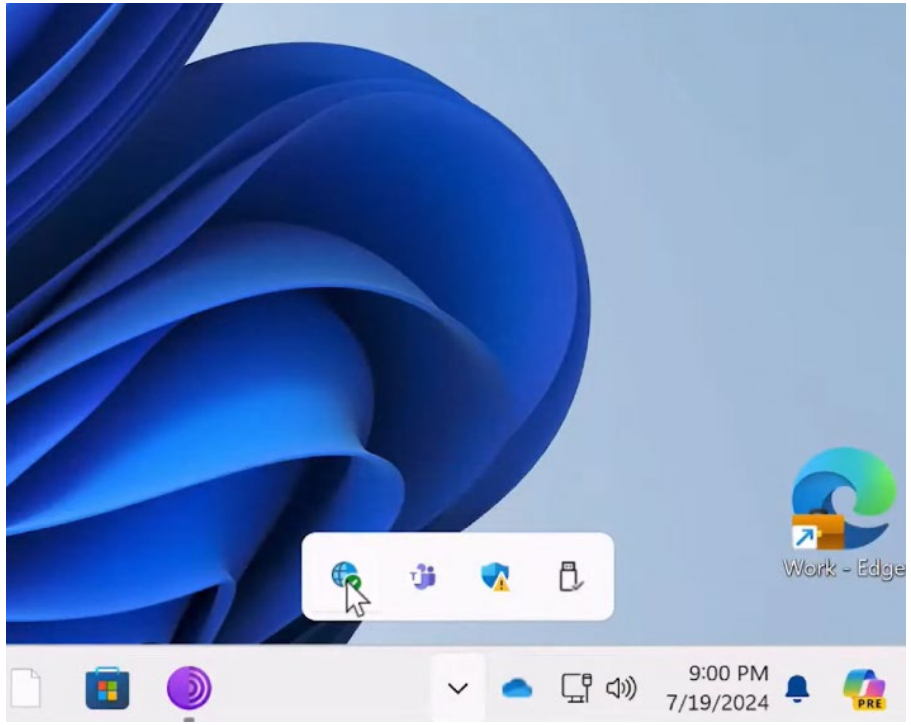
GSA includes multiple security functions; Internet Access for Microsoft Services is just the first step. More GSA features will be available in the

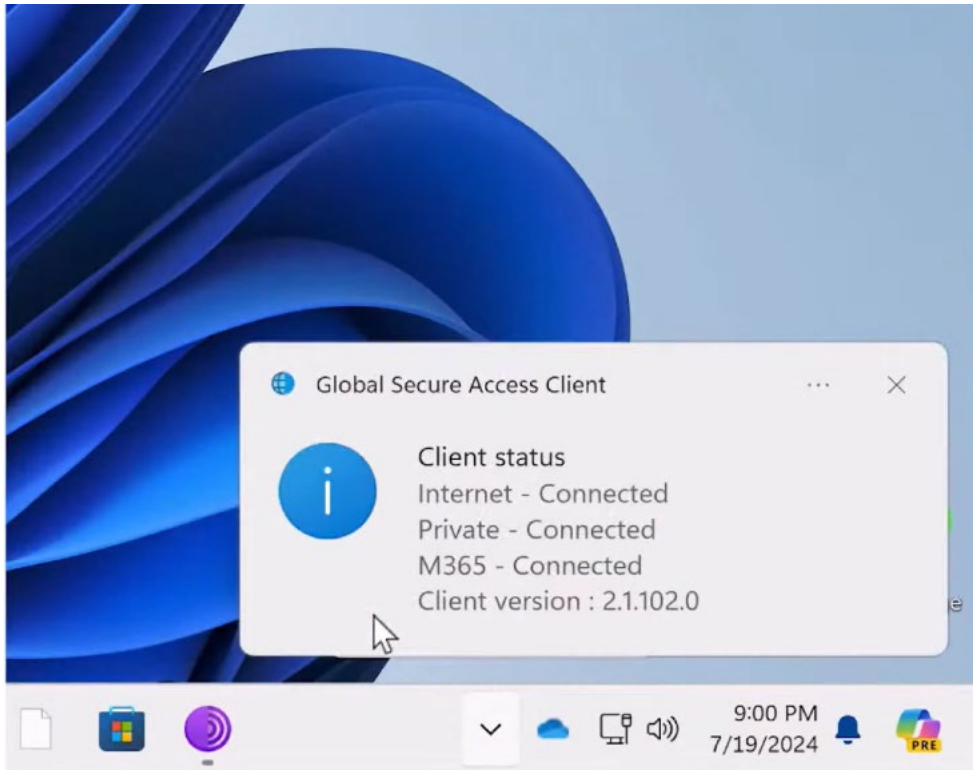


Enable traffic forwarding profiles



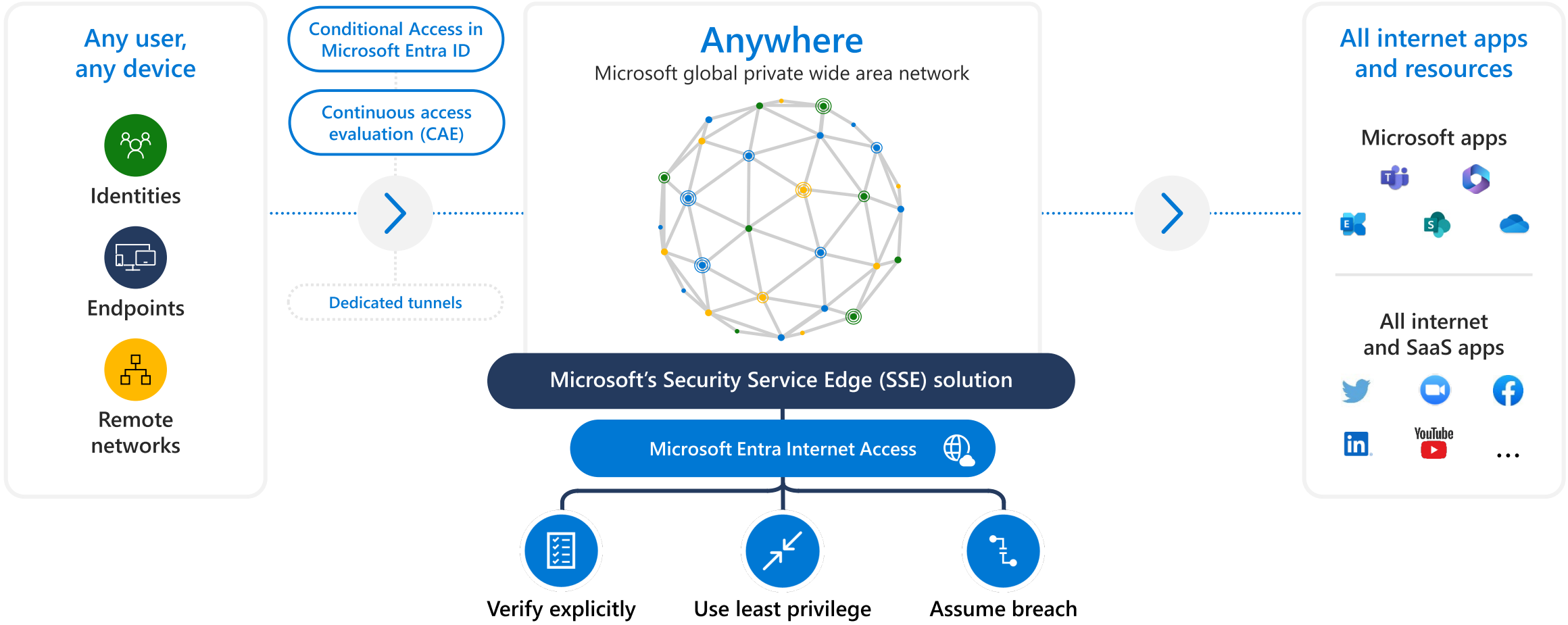
Microsoft Entra Internet Access


Work - Edge
9:00 PM
7/19/2024
PRE


Global Secure Access Client
Client status
Internet - Connected
Private - Connected
M365 - Connected
Client version : 2.1.102.0
9:00 PM
7/19/2024
PRE

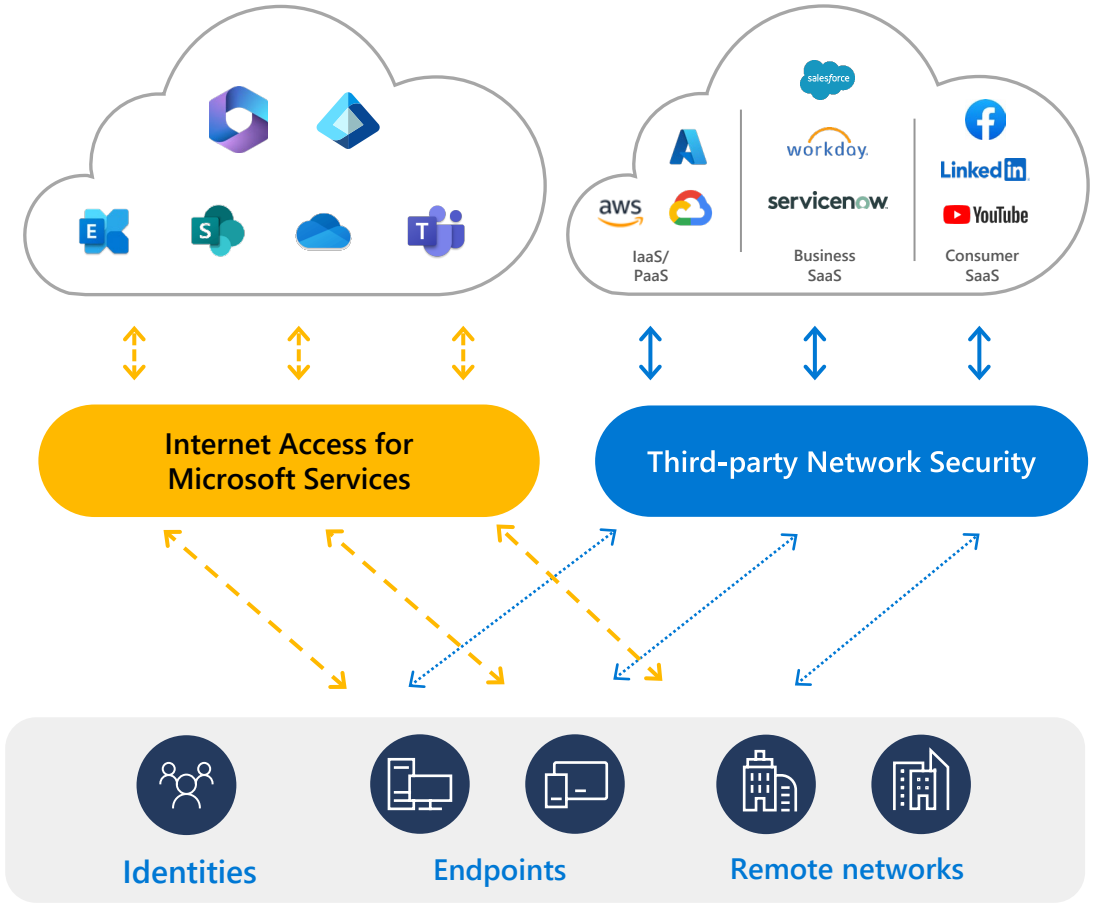
Microsoft Entra Internet Access

An identity-centric secure web gateway (SWG)



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

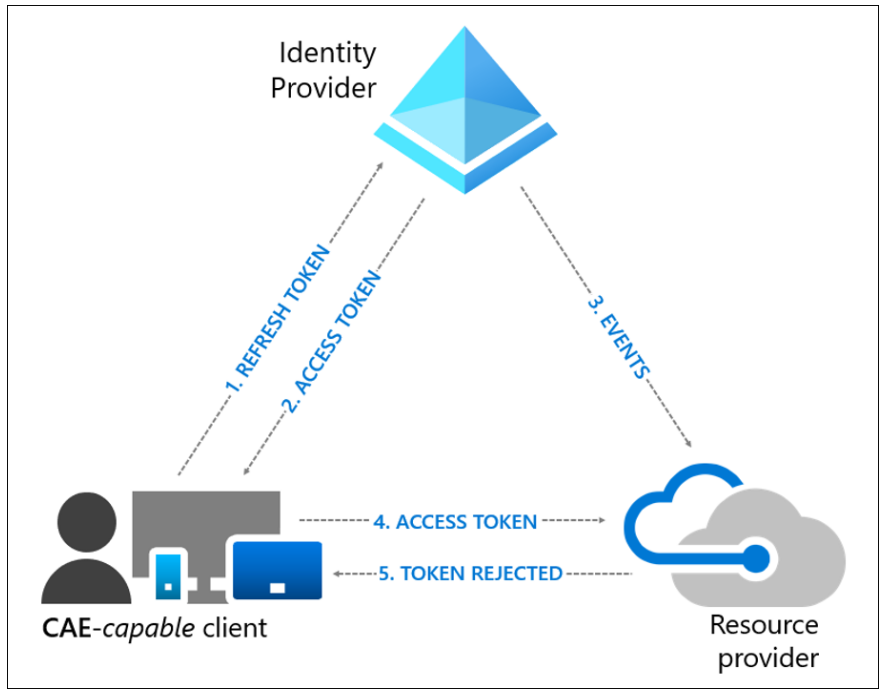
- **Deliver secure, fast, & consistent access to Microsoft services.** Send traffic directly to Microsoft services with any device and from any network.
- **Strengthen access controls for any network** by enhancing Microsoft Entra ID Conditional Access and Tenant Restrictions v2 access controls.
- **Gain 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.

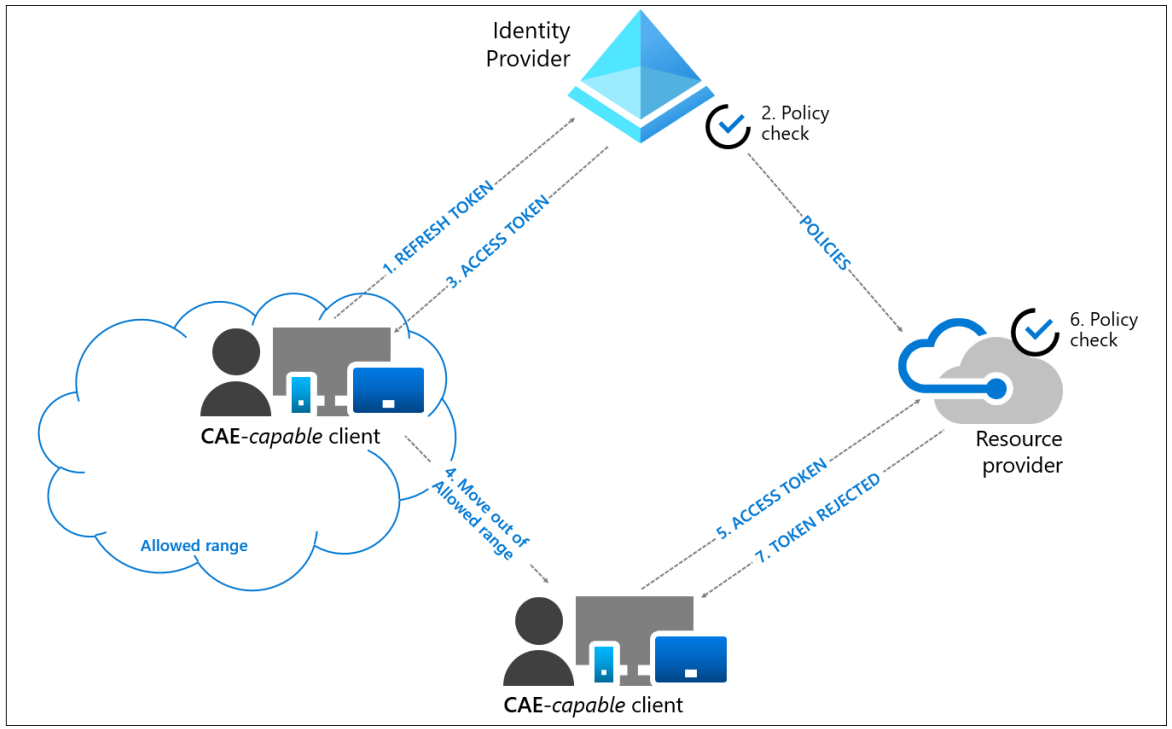


Works side-by-side with other solutions for private and public network access.

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





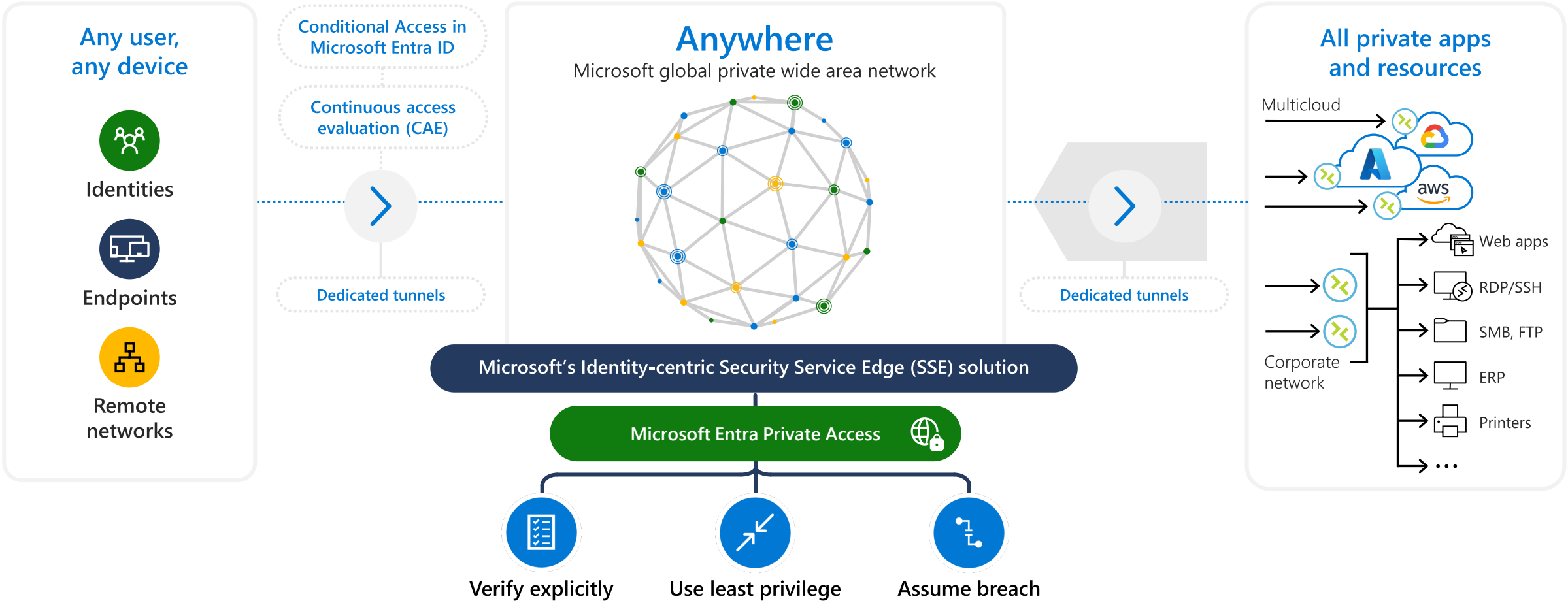
Microsoft Entra Private Access

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

*Public Preview

Private app discovery

Discover and onboard private applications for segmented per-app access

Discover apps

Discover app segments

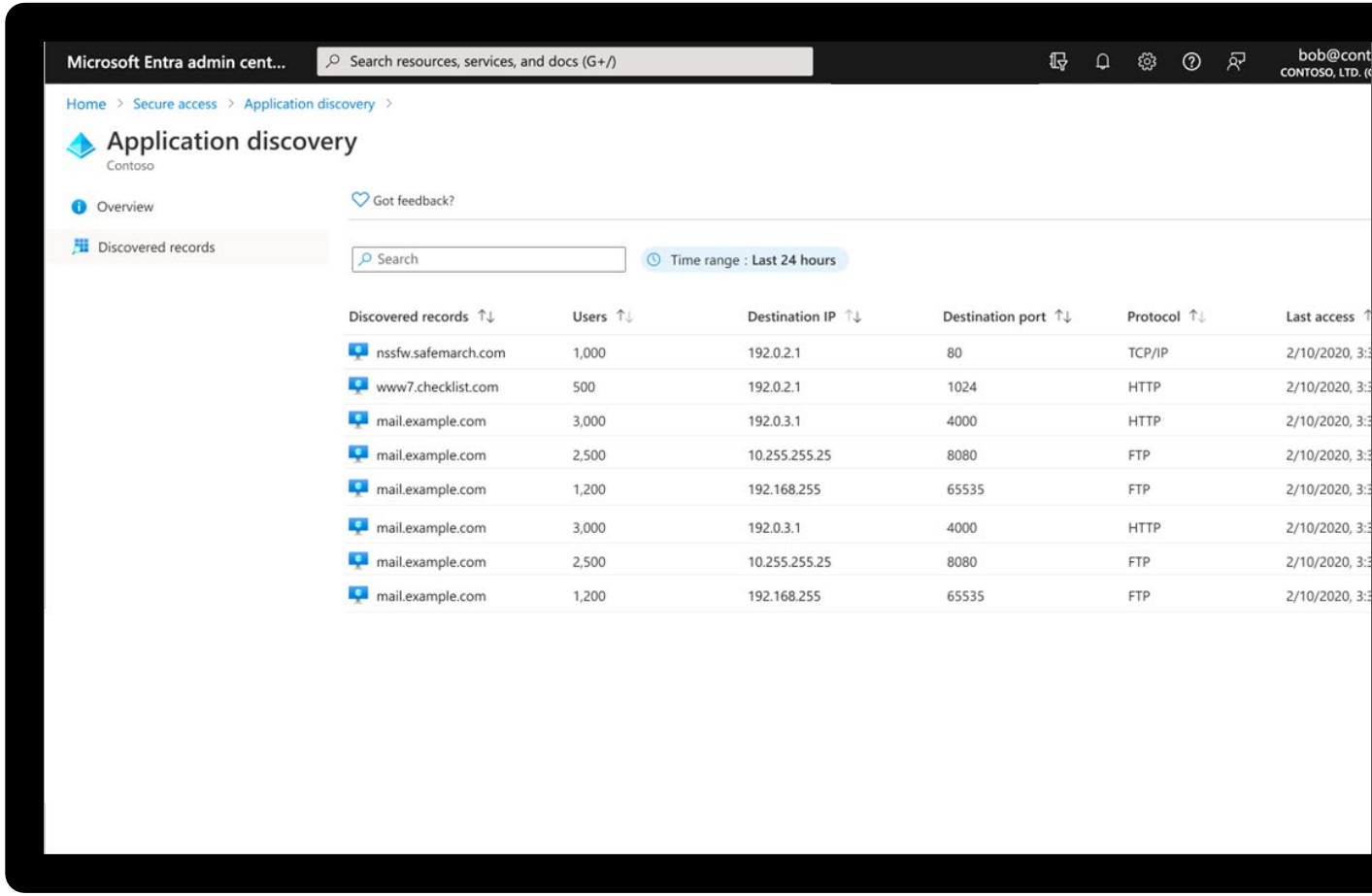
Create private apps using discovered app segments

Analytics

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

Auto re-discovery

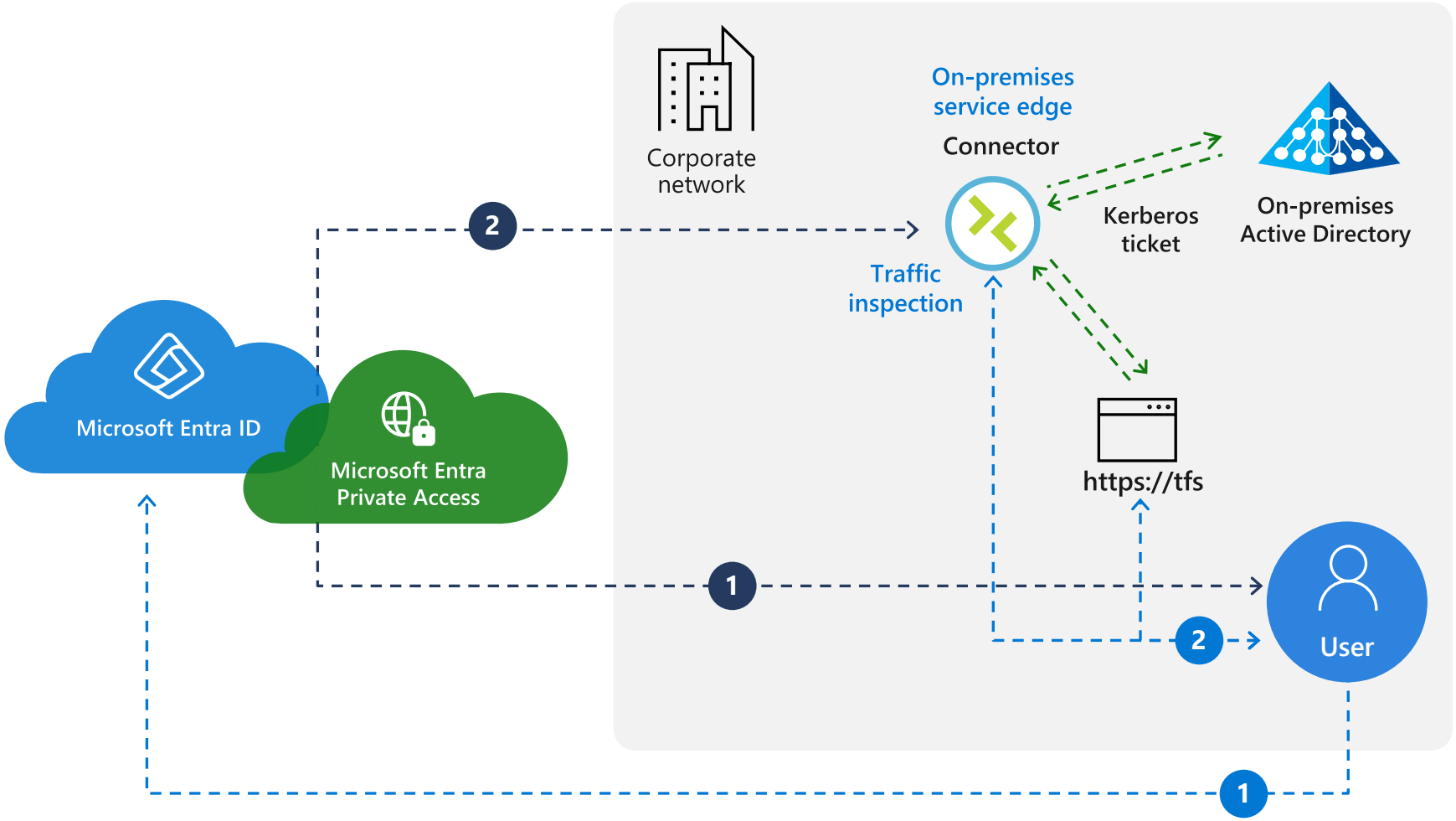
Intelligently add new discovered app segments to existing apps as additional app segments

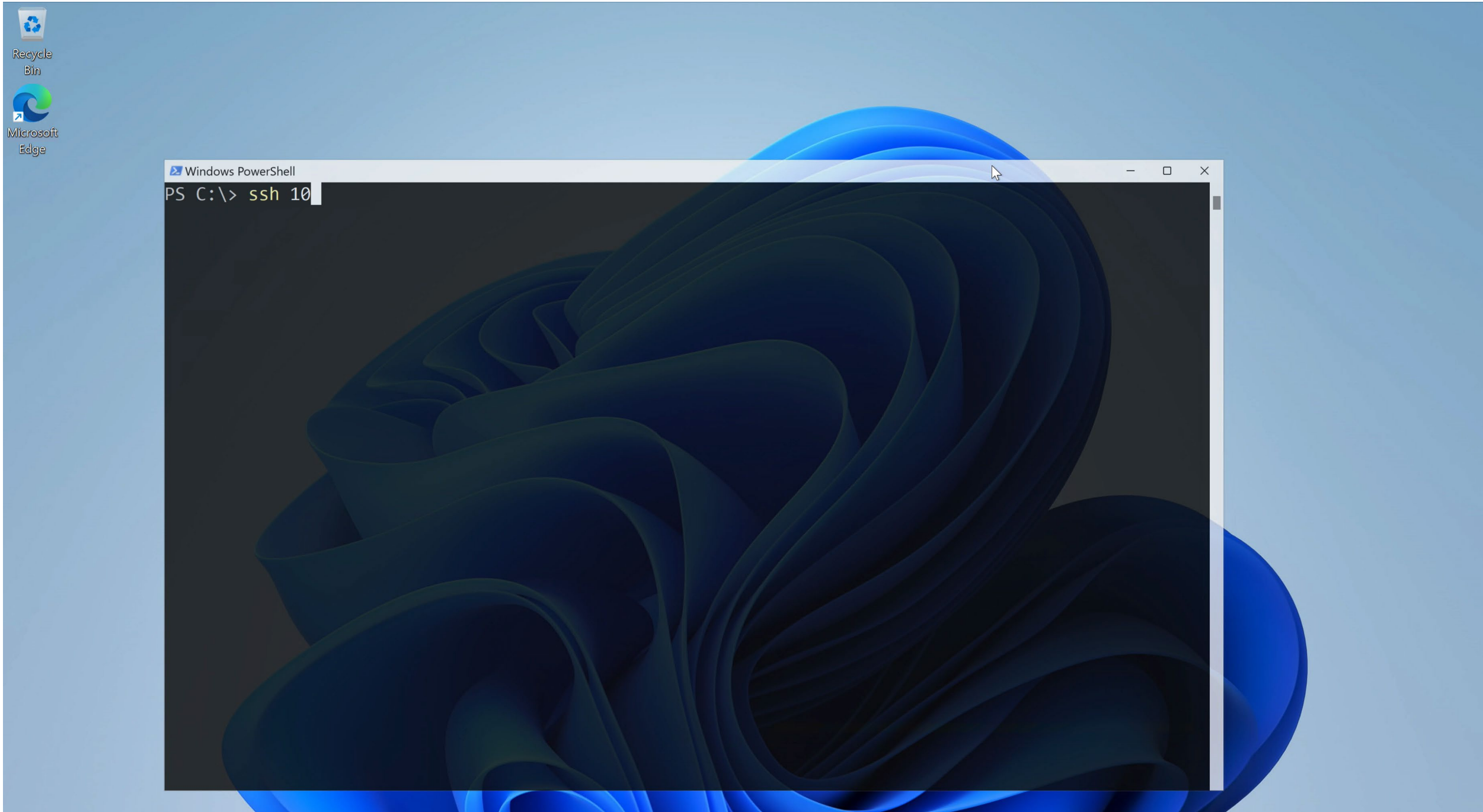


COMING SOON

Local access to private apps

Intelligent, smart, and adaptive

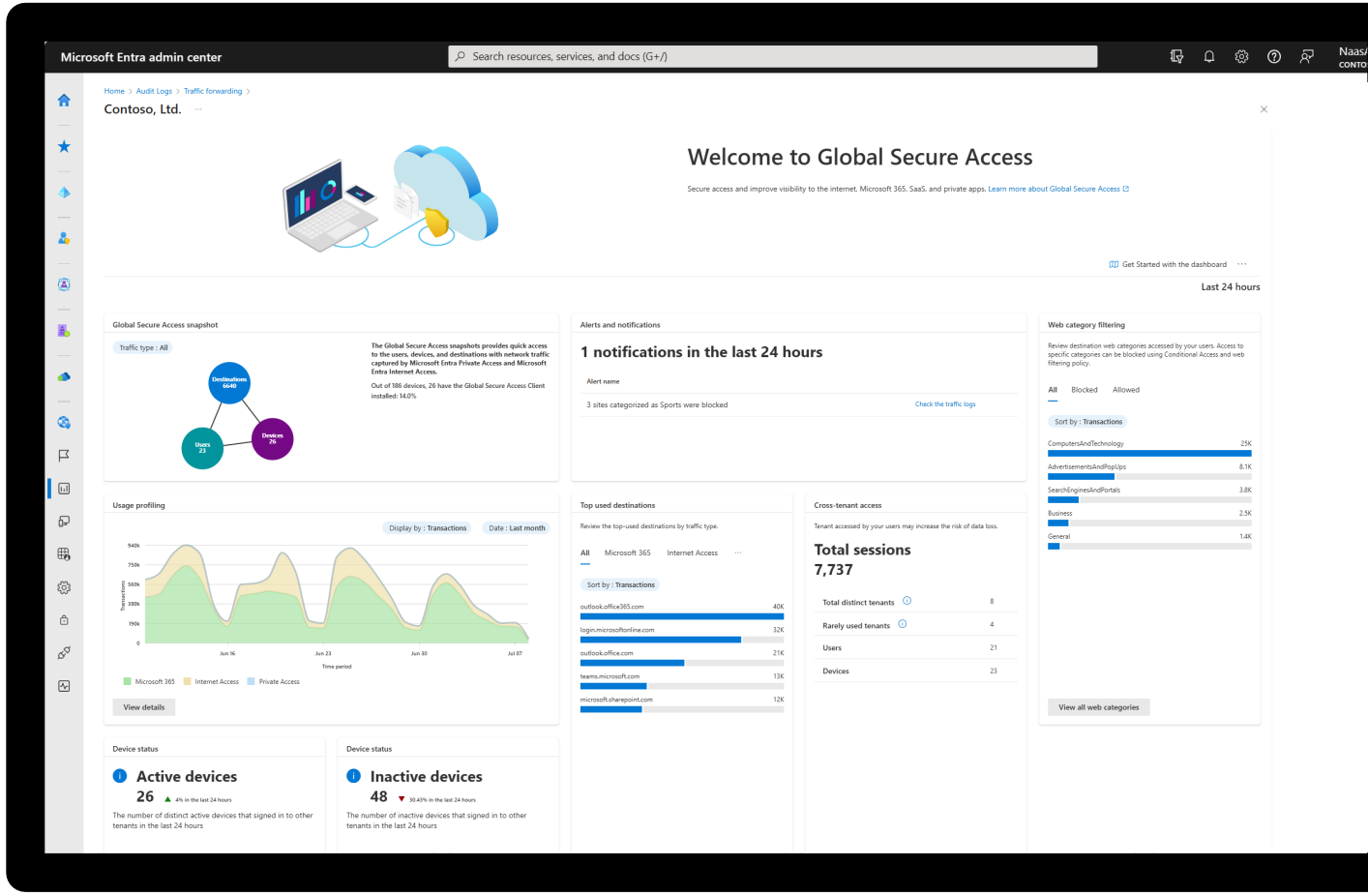



Recycle Bin
Microsoft Edge
Windows PowerShell
PS C:\> ssh 10

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*

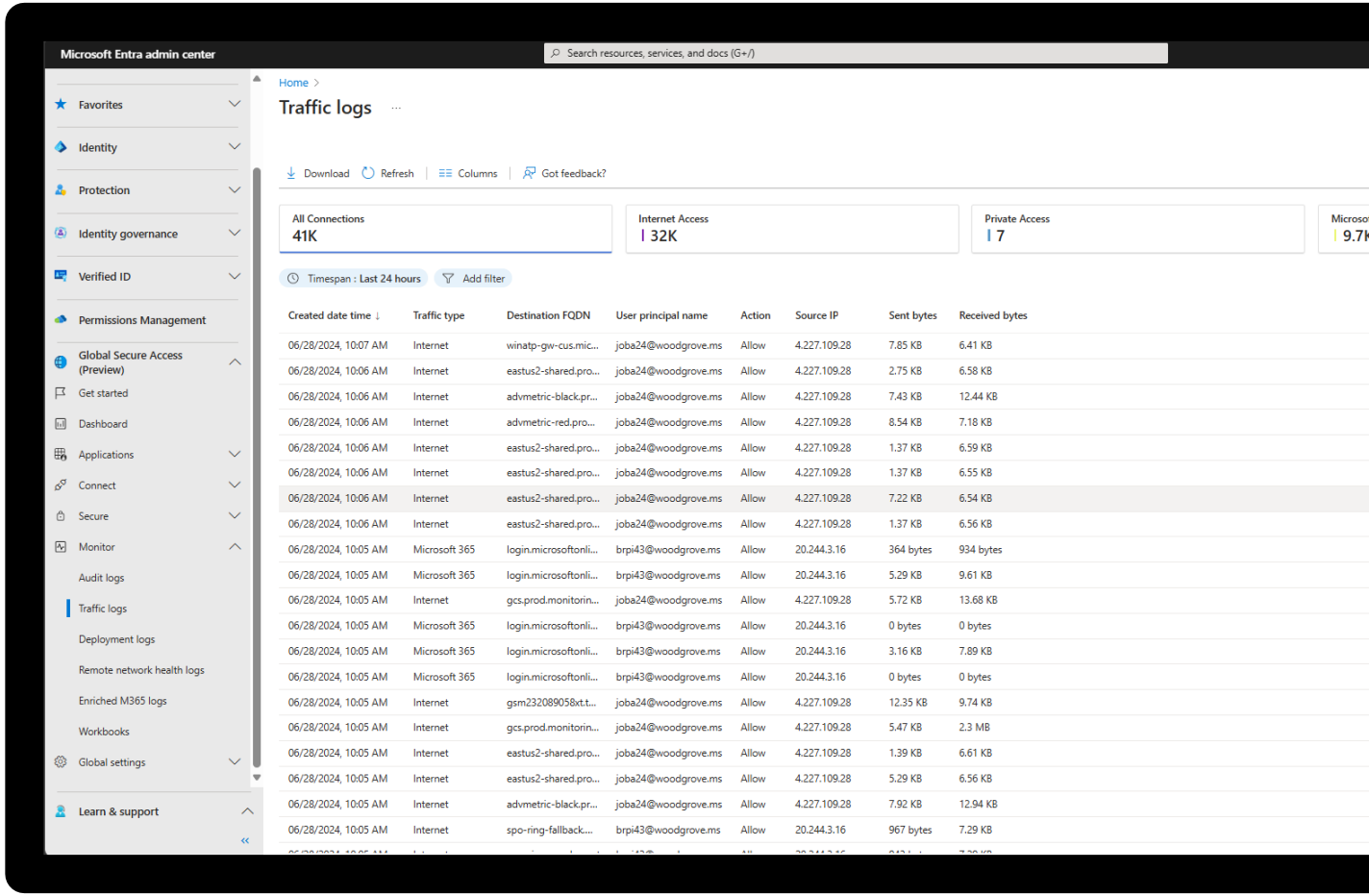


*Public Preview

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)***



*Public Preview
**Roadmap – all timelines are subject to change

COMING SOON

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

Microsoft Security

Thank you!