STILL BEHIND FIREWALLS?

USE MICROSOFT GLOBAL SECURE ACCESS

scopewyse

Alain Schneiter

Partner | Solutions Architect

scopewyse GmbH
alain.schneiter@scopewyse.com

blog.alschneiter.com
@alschneiter
alschneiter

About me | Tech

Microsoft MVP Security

Microsoft Certified Trainer

About me | Private

Community worker, Biker, Skier and World traveler

scopewyse

scopewyse

Microsoft Solutions Partner

Security

Specialist

Identity and Access Management

Threat Protection

Microsoft Solutions Partner

Infrastructure

Azure

Specialist

Azure Virtual Desktop

Microsoft Solutions Partner

Digital & App Innovation

Azure

Microsoft Solutions Partner

Modern Work

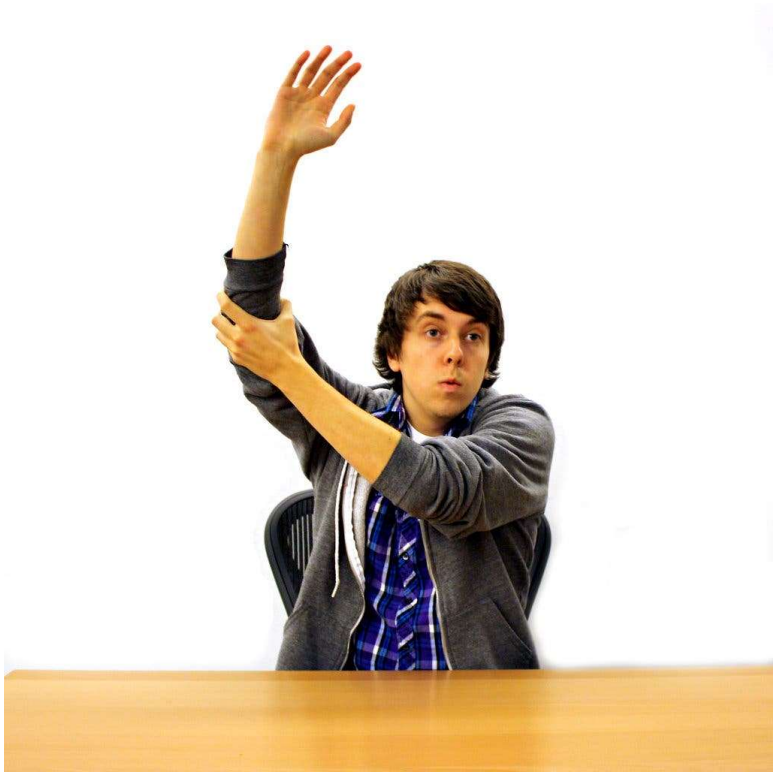
Agenda

- Zero Trust Model
- Project scope, bla bla
- Microsoft Global Secure Access
  - SSE (Security Secure Edge)
  - Internet Access
  - Private Access

Short poll!

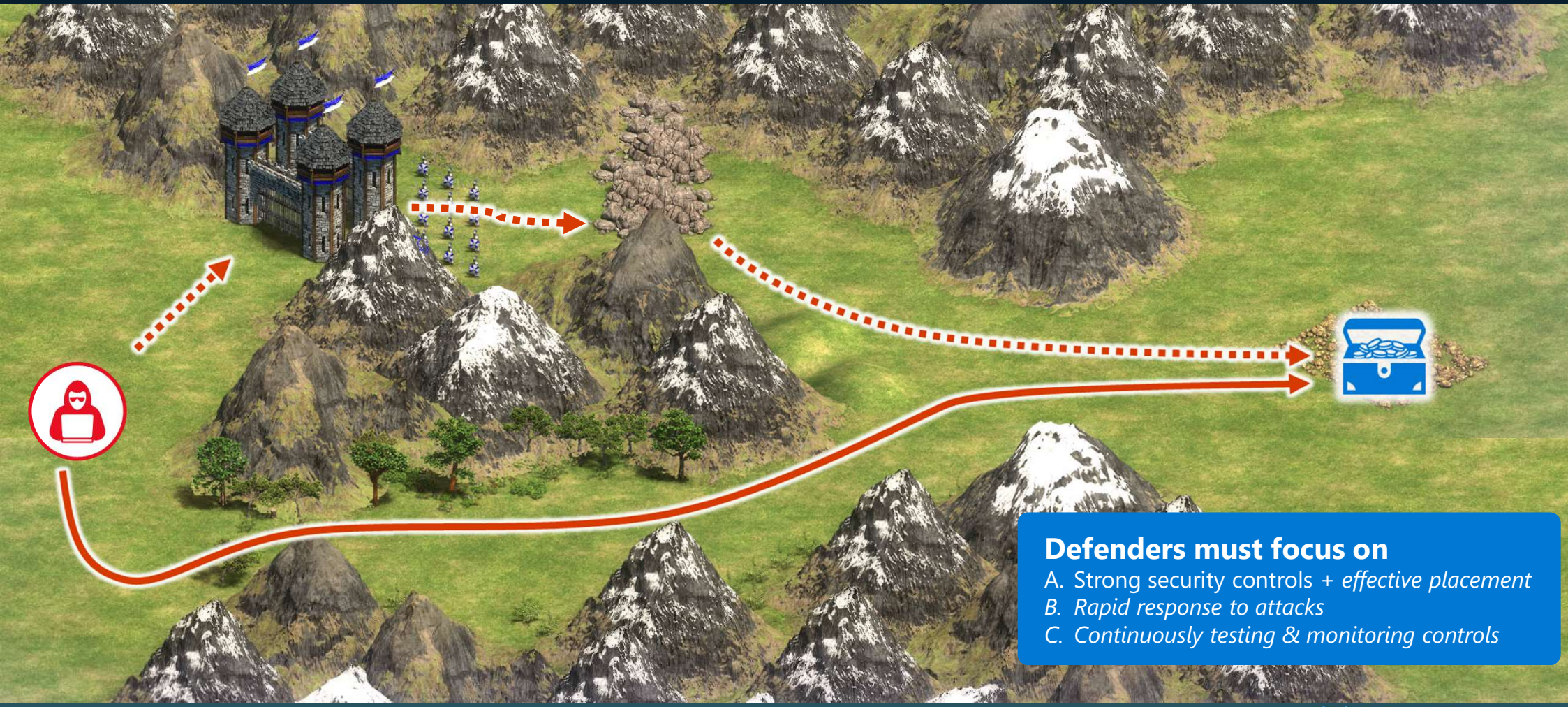
just raise your hand

- Do you use VPN for business reasons?
- Do you tunnel all traffic trough a VPN?
- Did you implement Zero Trust in your envoirnment?
- Do you join devices to EntraID?
  - EntraID Hybrid join
  - EntraID join



scopewyse

Still behind firewalls?



Defenders must focus on

A. Strong security controls + *effective placement*
B. Rapid response to attacks
C. Continuously testing & monitoring controls

Security Modernization with Zero Trust Principles

Business Enablement
Align security to the organization's mission, priorities, risks, and processes

Security Strategy and Program

Assume Breach (Assume Compromise)
Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

Verify Explicitly
Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry.

Use least-privilege access
Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

Zero Trust Architecture

Secure Identities and Access

Infrastructure & Development Security

IoT and OT Security

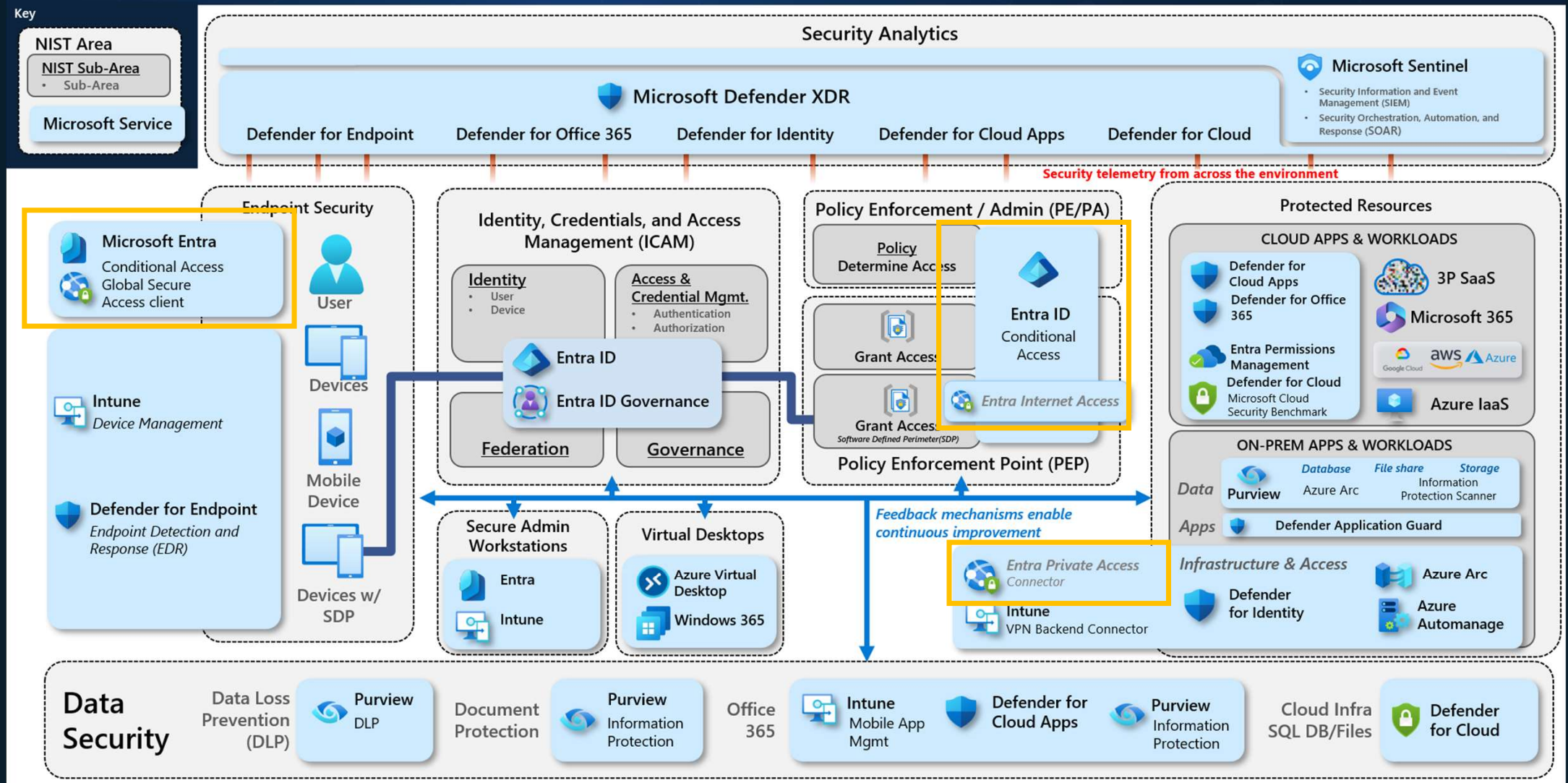
Modern Security Operations (SecOps/SOC)

Data Security & Governance

Microsoft Zero Trust Capability Mapping

Implemented in NCCoE lab (Summer 2023)

National Institute of Standards and technology

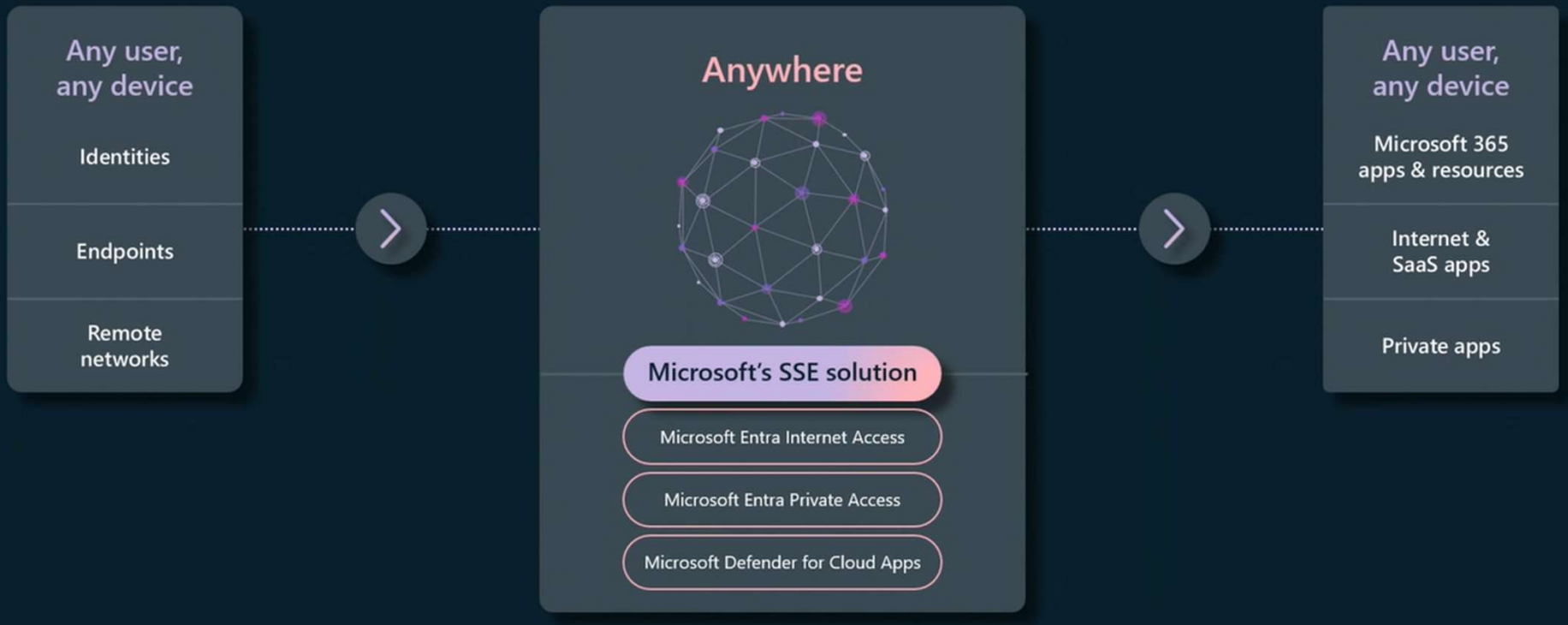


scopewyse

What is GSA?


Any user, any device
Identities
Endpoints
Remote networks
Microsoft Entra Conditional Access
Continuous Access Evaluation (CAE)
Dedicated tunnels
Anywhere
Microsoft's SSE solution
Microsoft Entra Internet Access
Verify explicitly
Use least privilege
Assume breach
Dedicated tunnels
All internet apps & resources
Microsoft 365 apps
All internet & SaaS apps
YouTube

Microsoft's identity-centric Security Service Edge solution



Microsoft’s Security Sevice Edge solution

Microsoft Entra Internet Access (Public Preview)

- Microsoft 365 apps traffic
- Protect against internet threats
- Prevent stolen tokens from being replayed with the **compliant** network check in Conditional Access
- Universal tenant restrictions to prevent data exfiltration to other tenants or personal accounts including anonymous access

Microsoft Entra Internet Access (Private Preview)

Public Preview

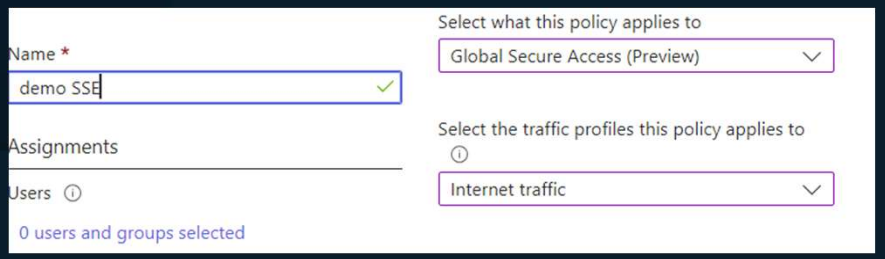
Microsoft Entra Internet Access

Universal Conditional Access for all internet, SaaS, and Microsoft 365 apps and resource

Compliant network check in Conditional Access

Web content filtering

Coming soon



Microsoft Entra Internet Access (Private Preview)

- Dedicated public internet traffic forwarding profile
- Web content filtering through secure web gateway
- Universal Conditional Access policies for all internet destinations

Microsoft Entra Private Access

- Secured access to your private, corporate resources
- Quick Access: Zero Trust based access to a range of IP addresses and/or FQDNs without requiring a legacy VPN
- Per-app access for TCP apps
  - (UDP support in development)
- Deep Conditional Access integration
- Side-by-side with your existing third-party SSE solutions

Client Support

Windows 10/11

System requirements
Windows 10/11
Microsoft Entra joined
Local admin permissions
Uses lightweight filter (LWF)

Android

System requirements
Android 8.0 and above
Mobile phone or tablet
Android Go is not currently supported

Public preview: coming soon!

iOS

System requirements
iOS device

MacOS

System requirements
MacOS device

Get early access to the private view.

DEMO
Client

M365 Traffic forwarding profile

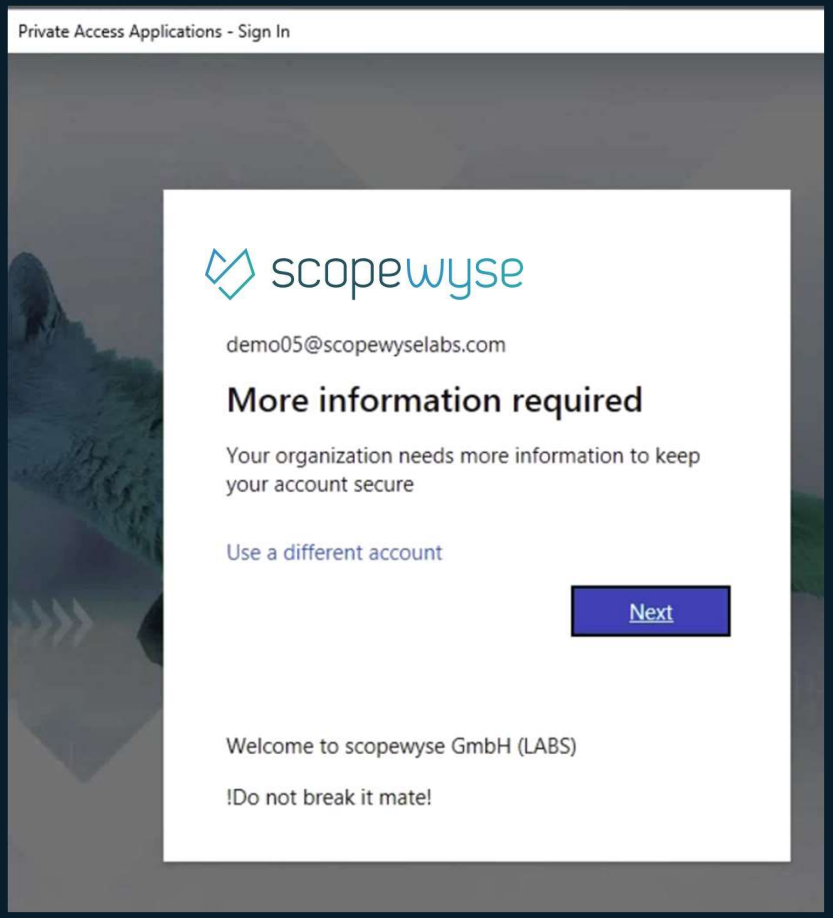
- GSA Administrator role required
- Preview requires a Microsoft Entra ID P1
- Policies for
  - Exchange Online, SharePoint Online & Microsoft 365 Common and Office online
  - Teams is currently not supported as part of the Microsoft 365 Common endpoints
- Actions Forward or Bypass
- Link CA Policies

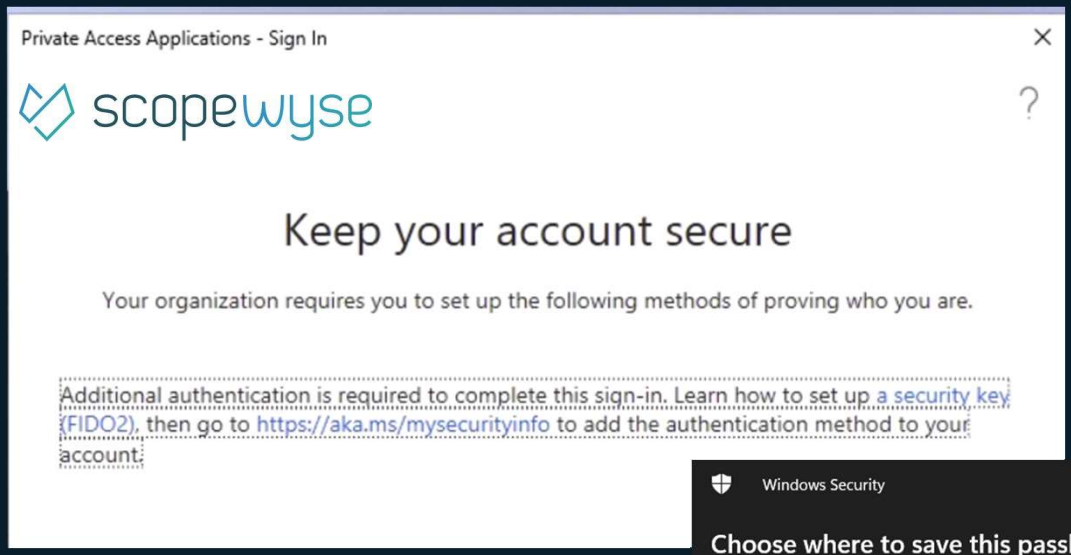
DEMO
Microsoft 365 access profile

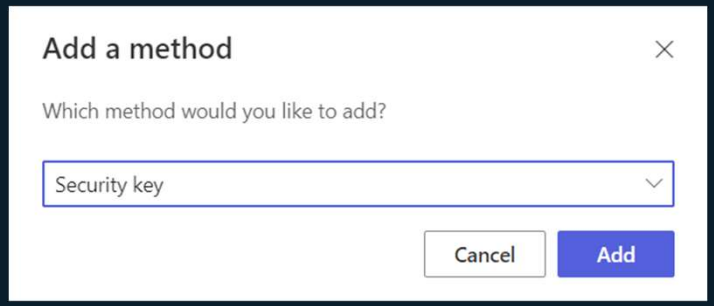
Private access profile

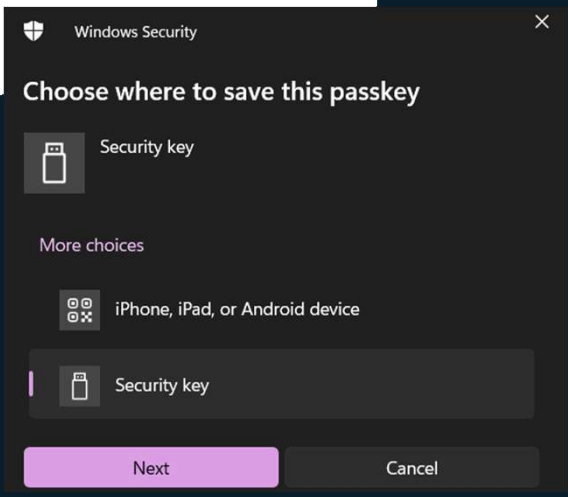
- Require latest application proxy
- Access to RDP, SMB, HTTP, HTTPS and more
- No VPN requirements
- Based on Enterprise Applications
- Fully integrated with Conditional Access

Private access & strong auth









DEMO
Private Access

Universal Tenant restriction

- Tenant restrictions v2 enables enterprises to prevent data exfiltration by users using external tenant identities for Microsoft Entra integrated applications like Microsoft Graph, SharePoint Online, and Exchange Online.
- These technologies work together to prevent data exfiltration universally across all devices and networks.

Microsoft Cloud Security & Modern Work

- Datum: Meetup 08. Februar 2024
- Zeit: Ab 13:30
- Wo: Circle @ Microsoft
- Anmeldung: Link

Feedback