



TUNEDIN
MEETUPS

TunedIn: **Leeds**

Microsoft Entra Internet & Private Access FTW





Speaker



Gerry Hampson

Senior Consultant, Microsoft MVP



@GerryHampson

Can't see the slides? Can't hear? Need to repeat the question?

We will NOT be talking about.....



Agenda

- » Legacy network security challenges
- » Microsoft's Security Service Edge Solution
- » Microsoft Entra Internet Access (Preview)
- » Microsoft Entra Private Access (Preview)
- » It's just Entra ID Application Proxy, right?
- » Steps to enable Entra Internet Access
- » Steps to enable Entra Private Access
- » Entra Private & Internet Access in action

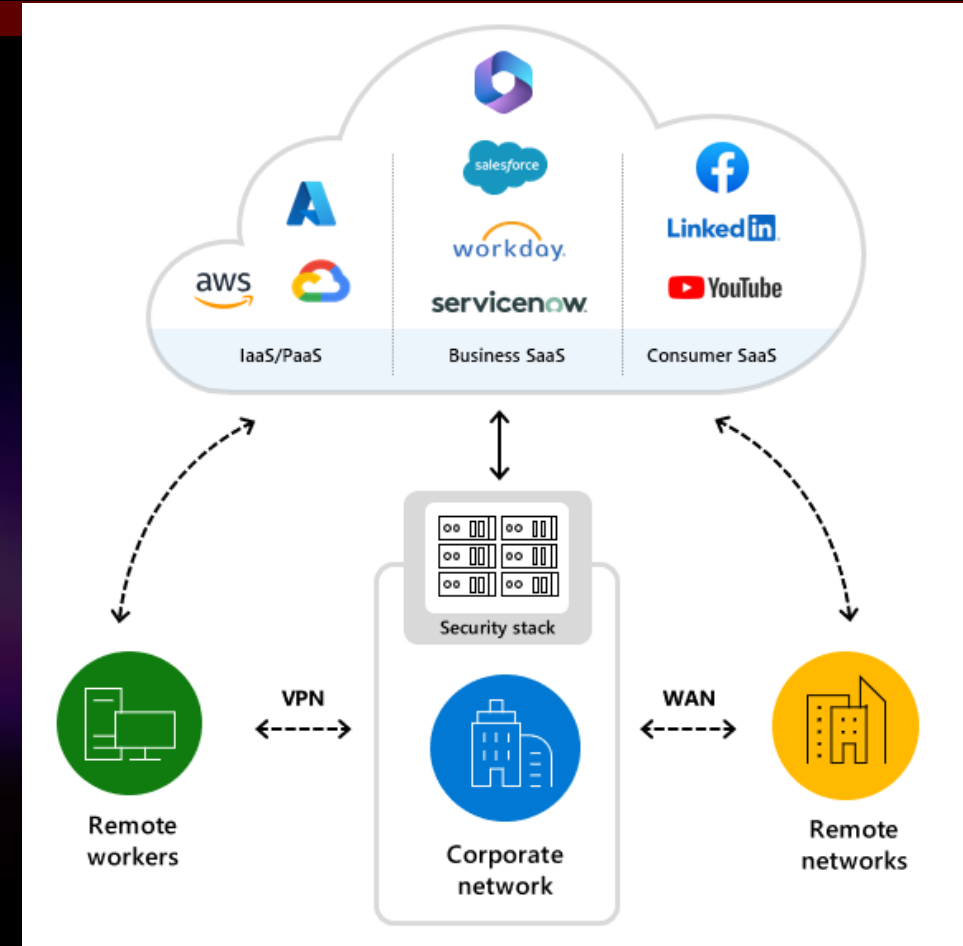


TunedIn: Leeds



Legacy network security no longer sufficient

- » Inconsistent and inefficient security controls
- » Security gaps from siloed solutions and policies
- » Higher operational complexities and cost
- » Poor user experience
- » Limited resources and technical skills



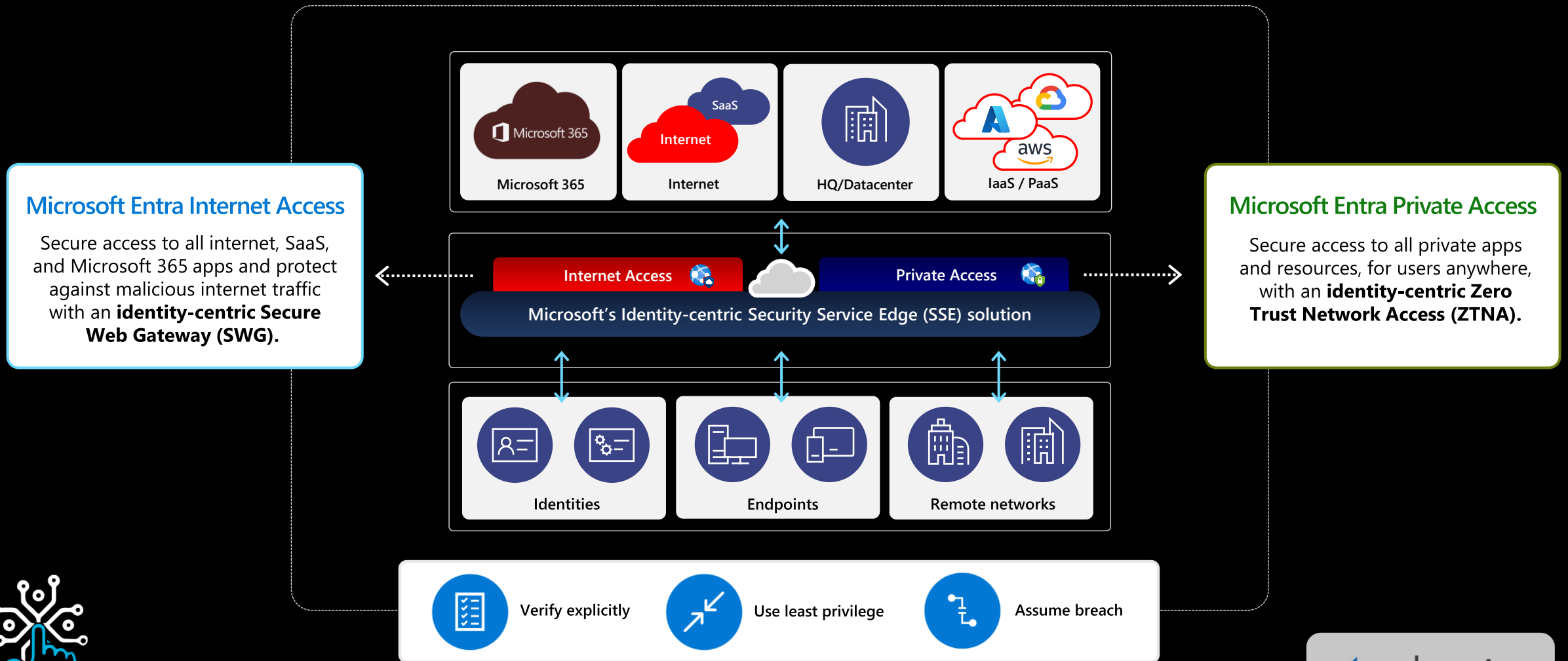
Microsoft's Security Service Edge (SSE) Solution



TunedIn: Leeds



Microsoft's Identity-centric SSE solution



Universal Conditional Access

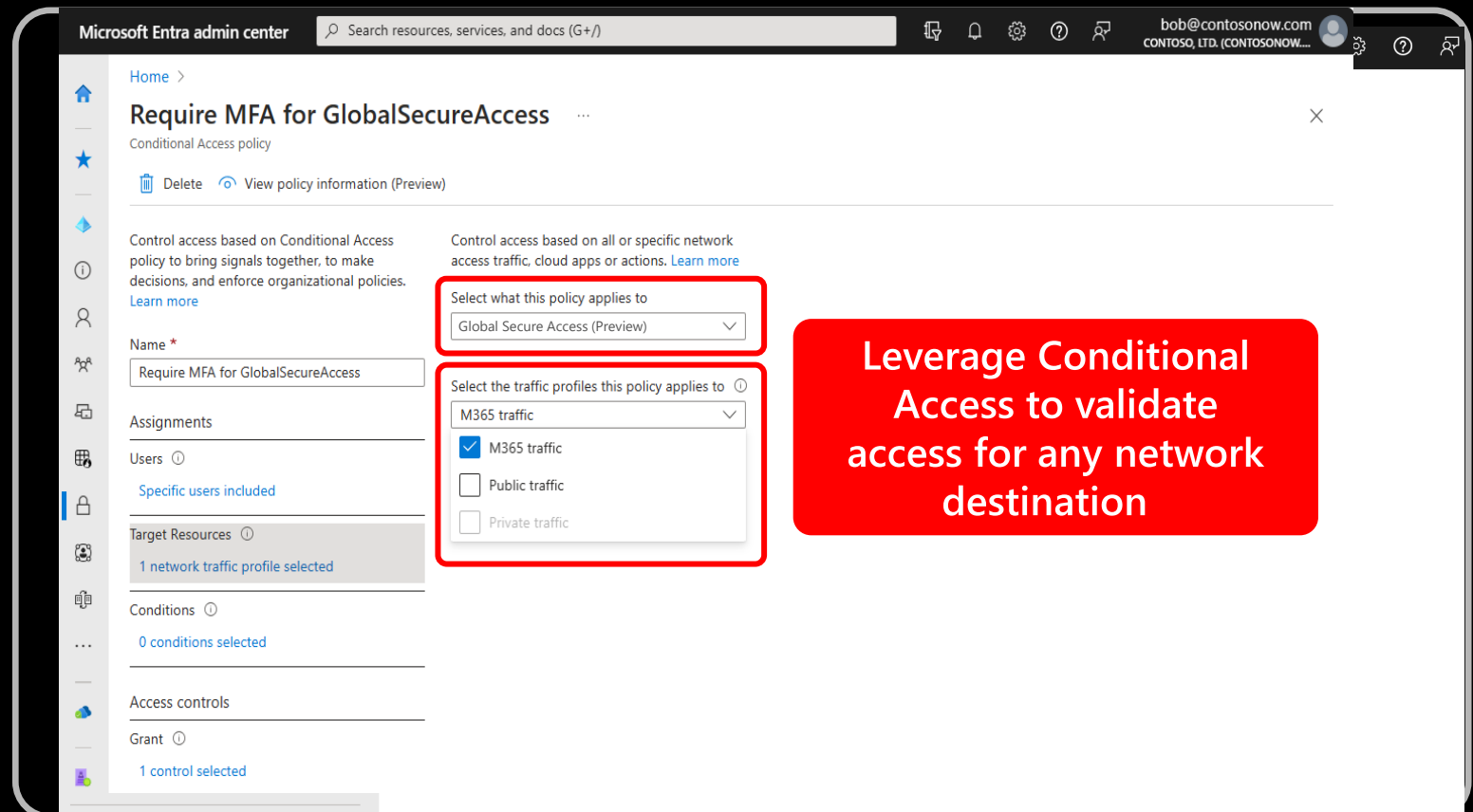
Extend the power of Conditional Access to any network destination

- » Applies Conditional Access to network scope
 - » Introduces Global Secure Access as a new resource type in Conditional Access
 - » Integrated construct to enforce adaptive access controls when connecting to SSE
- » Support for differentiated Conditional Access policies across Microsoft 365, Internet and Private traffic profiles
- » Extend seamless Zero Trust access controls to all network destinations, agnostic of client or application readiness
- » Continuous access evaluation to instantaneously revoke access on changing conditions
- » Source IP Restoration



TUNEDIN
MEETUPS

TunedIn: Leeds



adaptiva

Microsoft Entra Internet Access

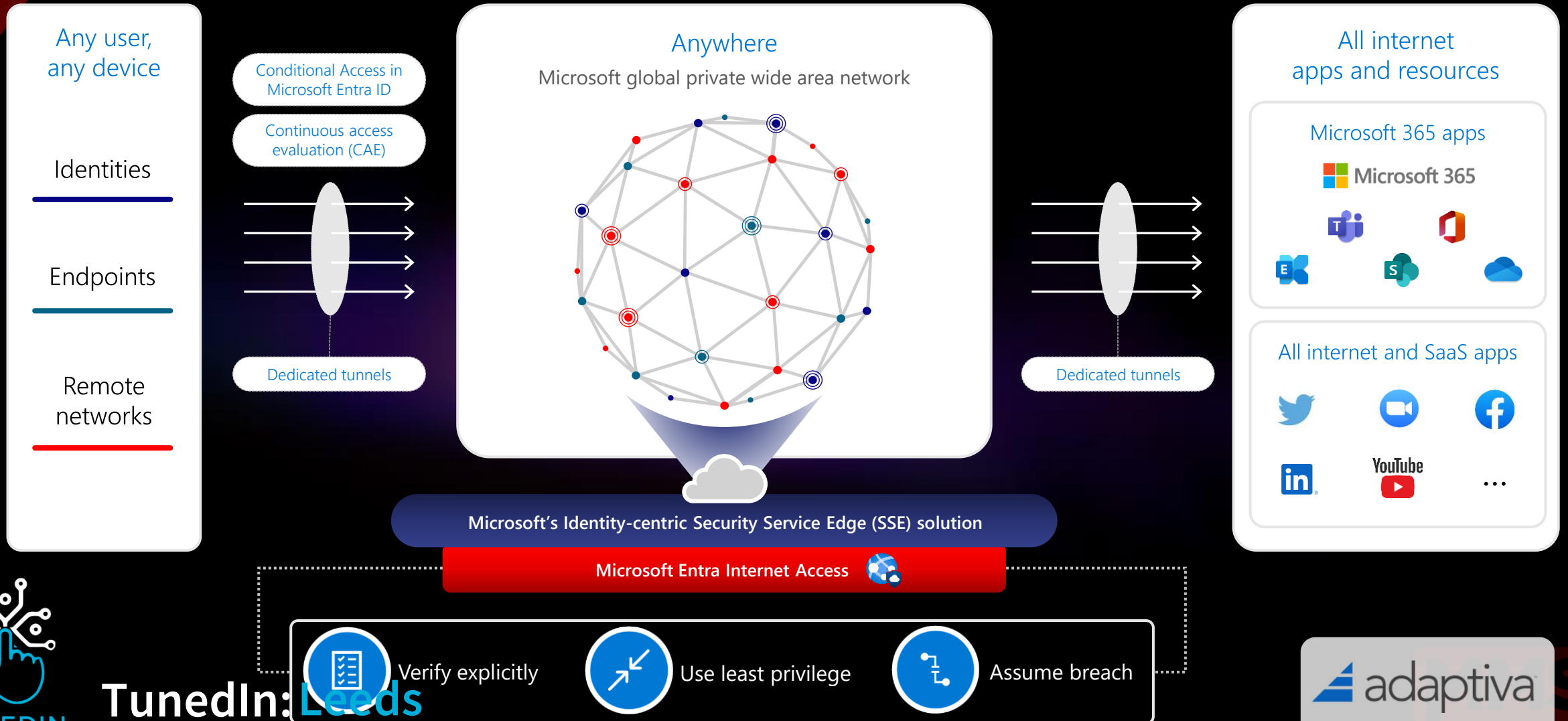


TunedIn: Leeds



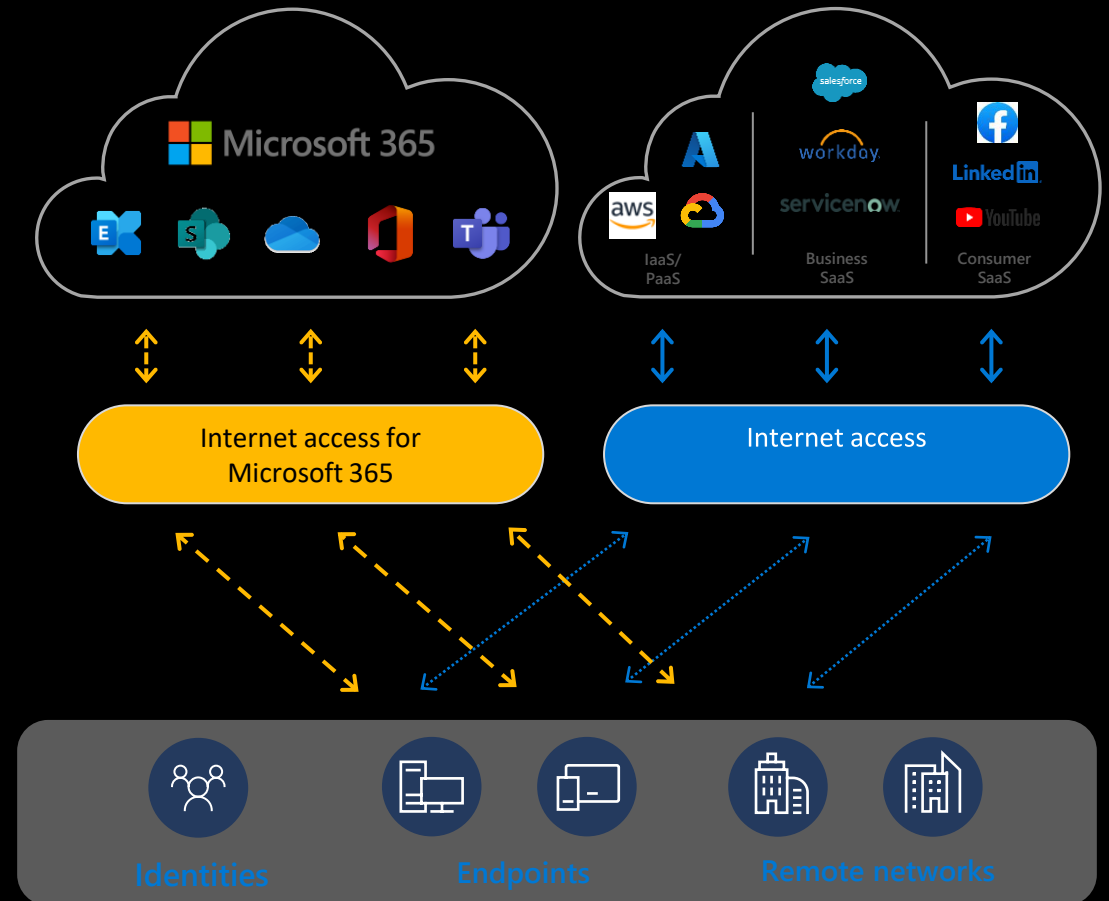
Microsoft Entra Internet Access

An identity-centric Secure Web Gateway (SWG) solution



Microsoft Entra Internet Access

- Easy to activate, zero maintenance
- Adaptive access controls
- Gain visibility into your environment
- Optimized end-user experience
- Web filtering



Microsoft Entra Internet Access- prerequisites

» Entra

- Entra ID P1 license
- M365 E3 (for Microsoft 365 traffic forwarding)
- Role: Global Secure Access Administrator, Application Administrator, Security Administrator
- Test user

» Infrastructure

- Test Windows client
 - Windows 10/11 64-bit
 - Entra ID or hybrid
 - Internet connection, no VPN
 - Need to be able to install Global Secure Access agent (Intune or local admin)
- Disable DNS over HTTP
- Prefer IPv4 over IPv6

Disable DNS over HTTP

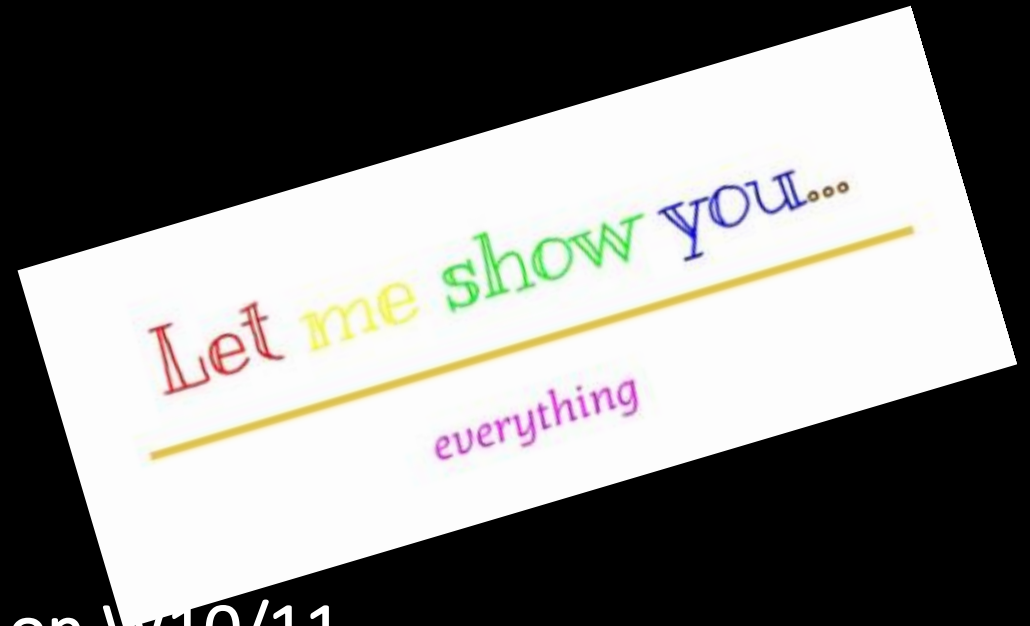
```
>> function CreateIfNotExists
>> {
>>     param($Path)
>>     if (-NOT (Test-Path $Path))
>>     {
>>         New-Item -Path $Path -Force | Out-Null
>>     }
>> }
>> $disableBuiltInDNS = 0x00
>> # This disables browser based secure DNS lookup for the Microsoft Edge browser:
>> CreateIfNotExists "HKLM:\SOFTWARE\Policies\Microsoft"
>> CreateIfNotExists "HKLM:\SOFTWARE\Policies\Microsoft\Edge"
>> Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Edge" -Name "DnsOverHttpsMode" -Value "off"
>> Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Edge" -Name "BuiltInDnsClientEnabled" -Type DWord -
Value $disableBuiltInDNS
>> # This disables browser based secure DNS lookup for the Google Chrome browser:
>> CreateIfNotExists "HKLM:\SOFTWARE\Policies\Google"
>> CreateIfNotExists "HKLM:\SOFTWARE\Policies\Google\Chrome"
>> Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "DnsOverHttpsMode" -Value "off"
>> Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Google\Chrome" -Name "BuiltInDnsClientEnabled" -Type DWord -
Value $disableBuiltInDNS
```

Prefer IPv4 over IPv6

```
Set-ItemProperty -Path  
"HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip  
6\Parameters" -Name "DisabledComponents" -Type  
DWord -Value $setIpv6Value
```

Microsoft Entra Internet Access- implementation steps

- »Enable Global Secure Access
- »Enable Traffic Forwarding
- »Create a web content filtering policy
- »Create a security profile
- »Create a conditional access policy
- »Install the Global Secure Access client on W10/11
- »Test and verify Entra Internet access



Entra Internet Access

DEMO

Activity Details

Basic info

```
{
  "createdDateTime": "01/21/2024, 03:47 PM",
  "tenantId": "47d6fc49-9fed-418b-af99-bf57cc26dae5",
  "destinationIp": "192.168.100.19",
  "destinationPort": 3389,
  "destinationFQDN": "",
  "sourceIp": "20.166.58.13",
  "sourcePort": 61507,
  "deviceId": "50c68153-f639-42a6-9223-fb02daea4da1",
  "deviceOperatingSystem": "Windows 11 Enterprise",
  "deviceOperatingSystemVersion": "10.0.22621",
  "userId": "cd6c3b97-81d6-4a2a-b974-493283a6cc57",
  "userPrincipalName": "Fred@emslab.ie"
}
```


DEMO

[Home](#) > [Client download](#) > [Welcome to Global Secure Access \(Preview\)](#) > [Get started](#) >

Welcome to Global Secure Access (Preview) ...

Activate the Global Secure Access preview, which includes Microsoft Entra Internet Access and Microsoft Entra Private Access. [Learn more](#)



1. Global Secure Access prerequisites

- ✓ You have the required administrator role to activate the preview.
- ✓ You have the required license to start using Global Secure Access.

A Global Secure Access Administrator, Security Administrator, or Global Administrator must be assigned to activate and manage Global Secure Access features. [Learn more](#)



2. Activate Global Secure Access in your tenant

To activate Global Secure Access, click the activate button below. Note activation will not impact any workload in your tenant until preview features are enabled.

[Activate](#)



3. Get started with Global Secure Access

Learn about Global Secure Access and the next steps for getting started.

[Get Started](#)

Microsoft Entra Private Access

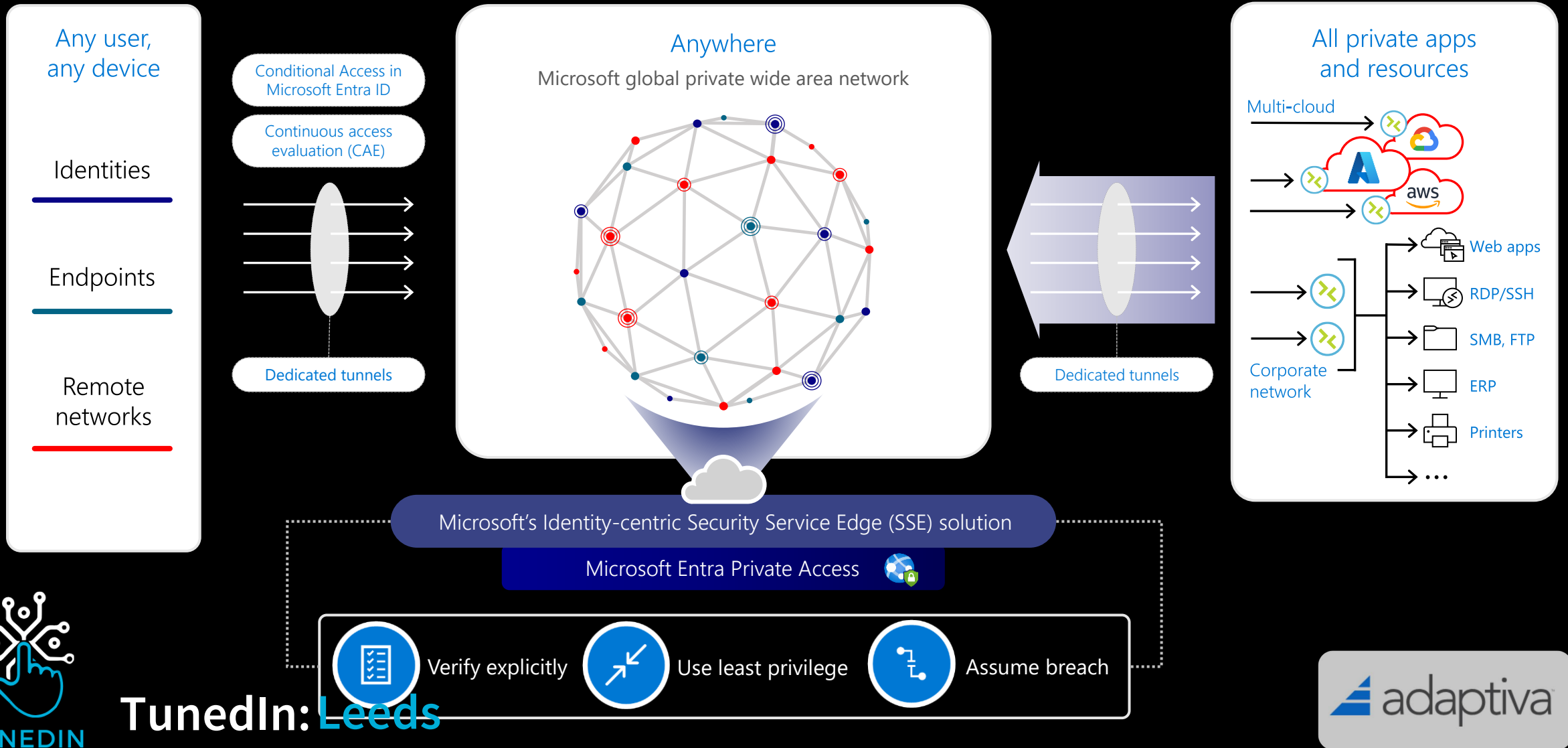


TunedIn: Leeds



Microsoft Entra Private Access

An identity-centric Zero Trust Network Access (ZTNA)

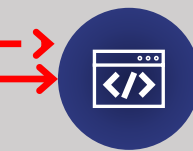
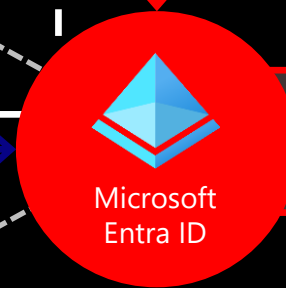
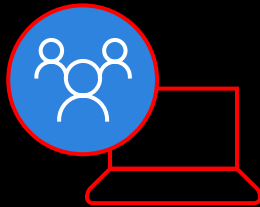


Moving beyond VPNs

Move to identity-centric ZTNA and modernize access to private applications

1. Configure Microsoft Entra ID for VPN authentication

- + Explicit user and device trust validation
- Provides full network access by putting device in the network (sometimes segmented)



Private Application

VPN typically allows access to all ports on the entire network

2. Publish apps with Private Access

- + Explicit user and device trust validation
- + Provides access to only private apps (with seamless user experience)
- + Device does not get network level access



TUNEDIN
MEETUPS

TunedIn: Leeds



Microsoft Entra Private Access- prerequisites

» Entra

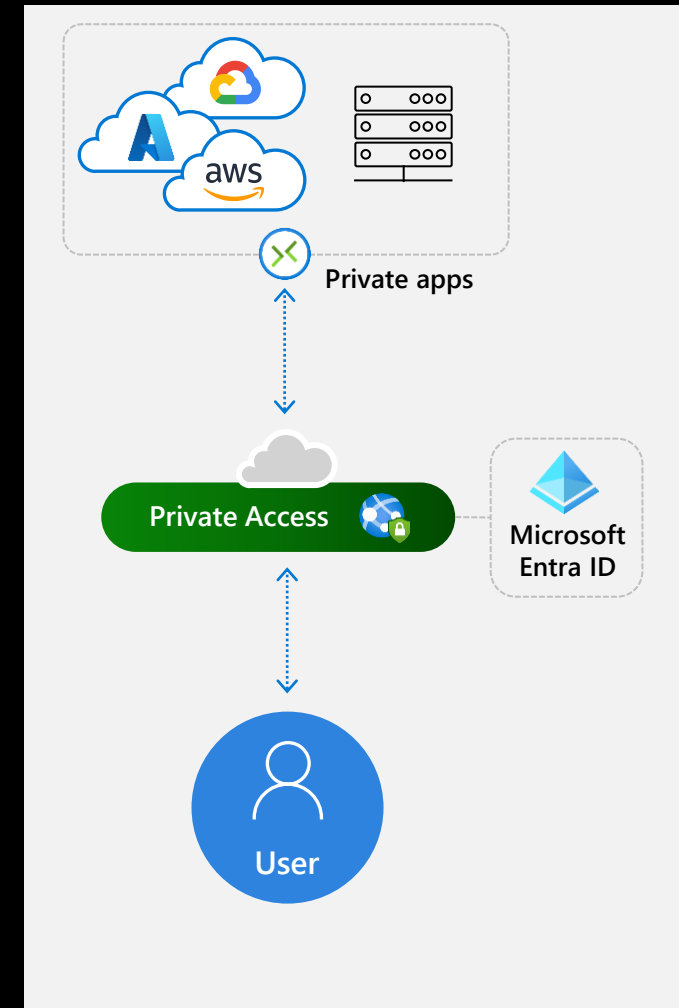
- Entra ID P1 license
- Role: Global Secure Access Administrator, Application Administrator, Security Administrator
- Test user

» Infrastructure

- Test Windows client
 - Windows 10/11 64-bit
 - Entra ID or hybrid
 - Internet connection, no VPN
 - Need to be able to install Global Secure Access agent (Intune or local admin)
- Server to install connector (Proxy)
 - Server and client should not be on same network and able to communicate
 - Use Hyper V host with HV virtual switch NAT translation

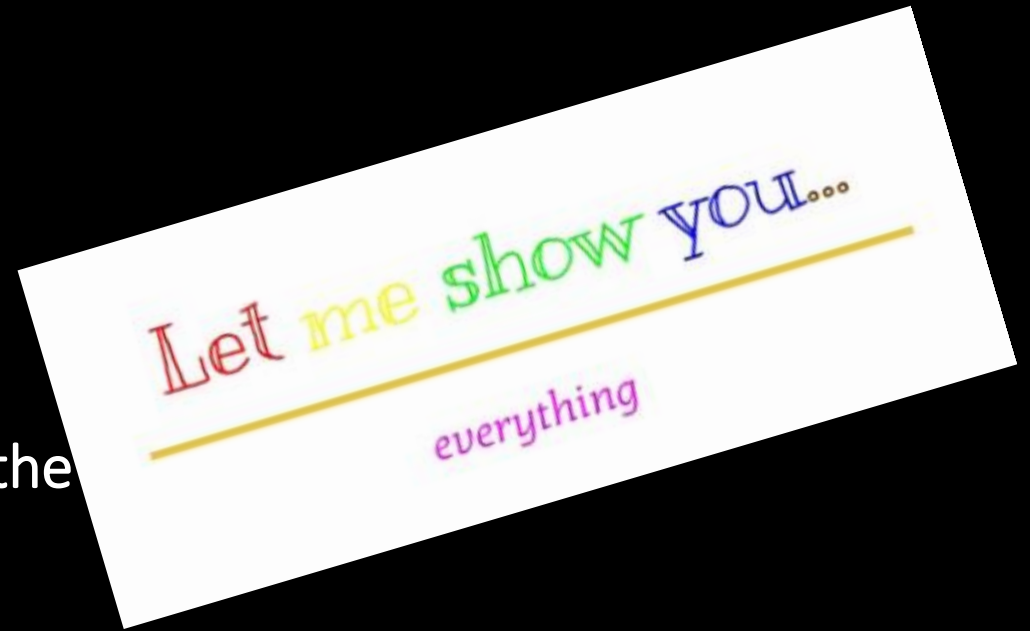
Target for services

TunedIn:Leeds



Microsoft Entra Private Access- implementation steps

- » Enable Global Secure Access
- » Enable Traffic Forwarding
- » Install the Application Proxy connector
- » Create Connector group
- » Create and publish a private application for the
- » Assign user/group to private application
- » Enable Adaptive Access
- » Install the Global Secure Access client on W10/11
- » Test and verify Entra Private access



Entra Private Access

DEMO

Activity Details

Basic info

```
{
  "createdDateTime": "01/21/2024, 03:47 PM",
  "tenantId": "47d6fc49-9fed-418b-af99-bf57cc26dae5",
  "destinationIp": "192.168.100.19",
  "destinationPort": 3389,
  "destinationFQDN": "",
  "sourceIp": "20.166.58.13",
  "sourcePort": 61507,
  "deviceId": "50c68153-f639-42a6-9223-fb02daea4da1",
  "deviceOperatingSystem": "Windows 11 Enterprise",
  "deviceOperatingSystemVersion": "10.0.22621",
  "userId": "cd6c3b97-81d6-4a2a-b974-493283a6cc57",
  "userPrincipalName": "Fred@emslab.ie"
```

Mobile devices



Global Secure Access - Android

- Legacy Device Administrator
- Supported Android Enterprise scenarios:
 - Corporate—owned fully managed, user devices
 - Corporate-owned devices with a work profile
 - Personal devices with a work profile

Web Filtering – Who Wins?

If implementing Web Filtering from both MDE and SSE:

- ◆ MDE will filter on the device first
- ◆ If allowed, will pass traffic to SSE
- ◆ SSE will evaluate and allow/block

What else? – I don't know all the answers

- Disabling Global Secure Access in Defender app on Android
- Pause GSA client on Windows
- Entra Private Access and routing to external addresses
- Entra Private Access to Exchange on-premises
- Using Entra Private Access for device management (CMG replacement)

Summary

Q&A

Thank you to our Sponsor

