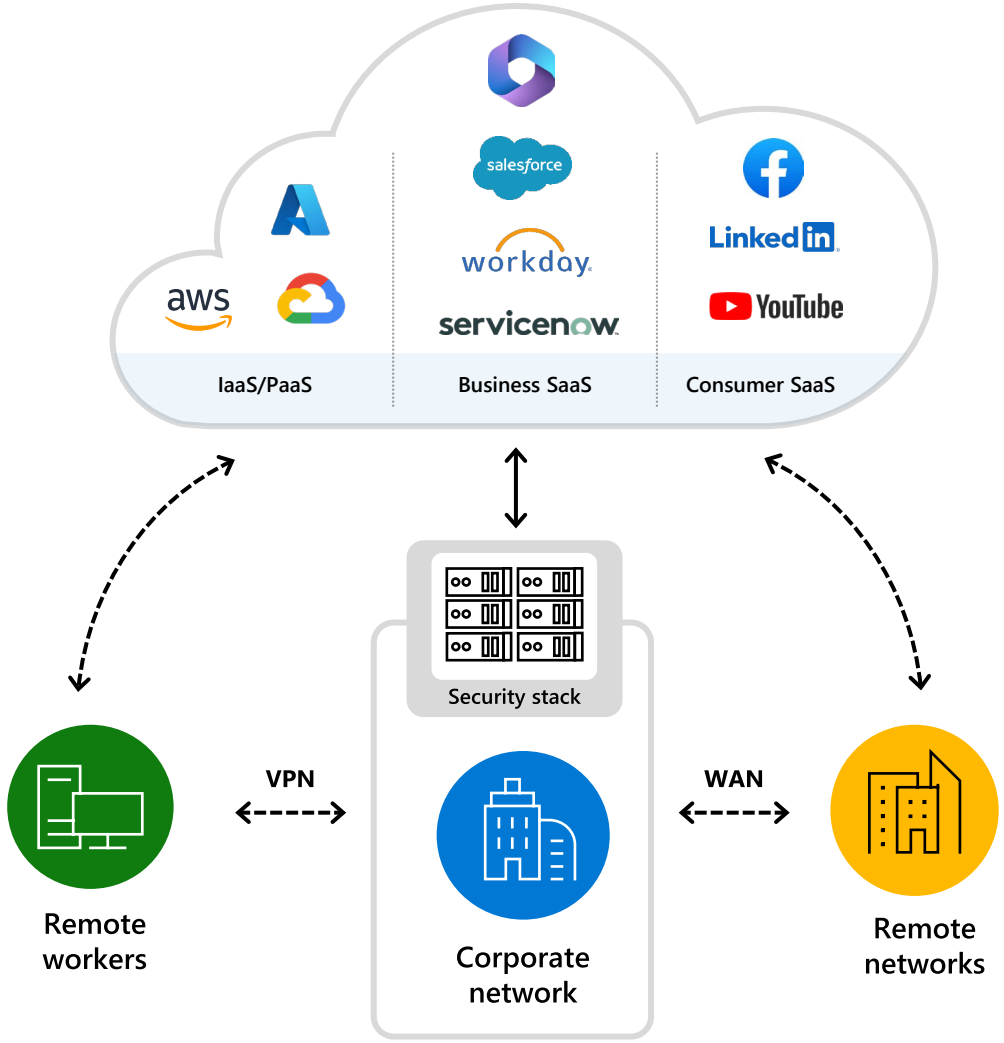
Microsoft Security

Microsoft's Security Service Edge

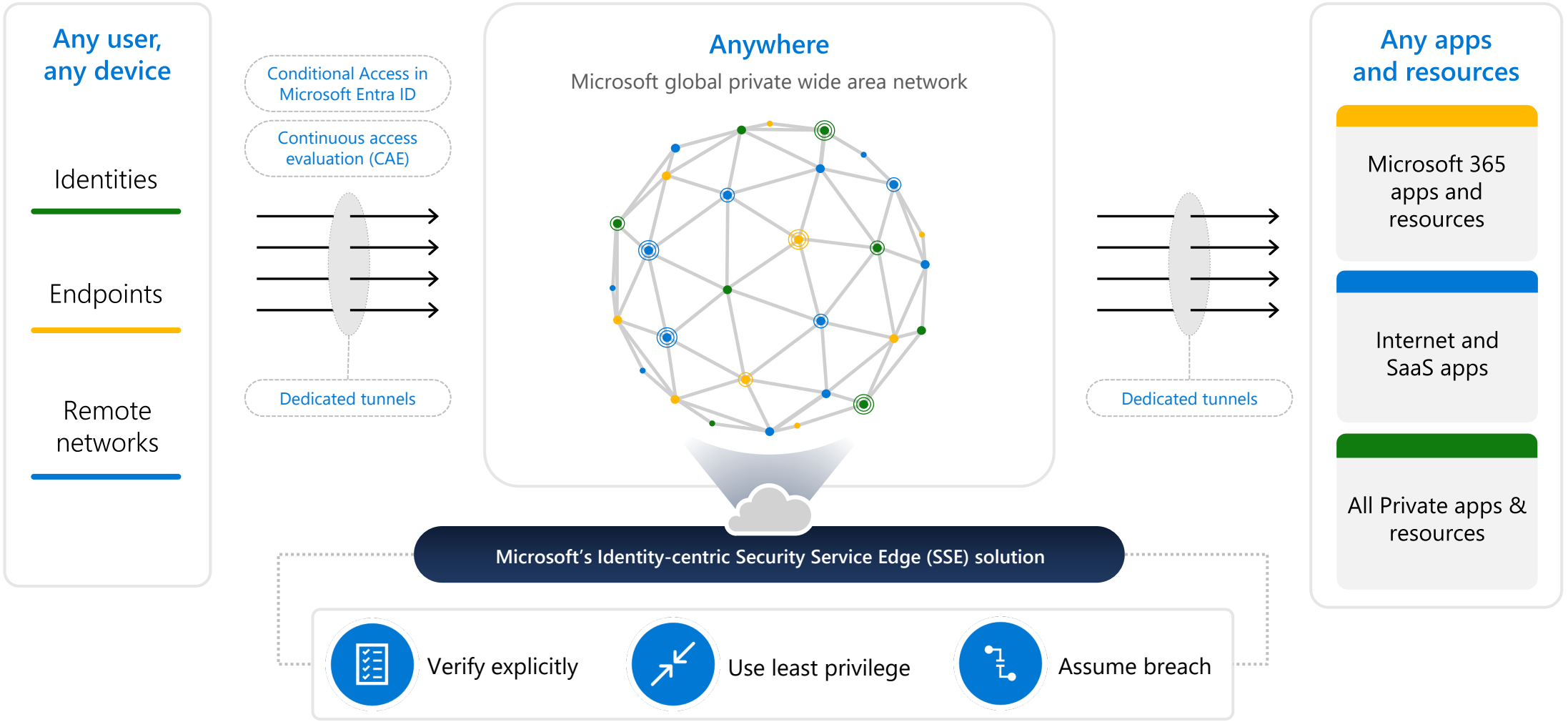
Tim Stock

Legacy network security approaches are 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



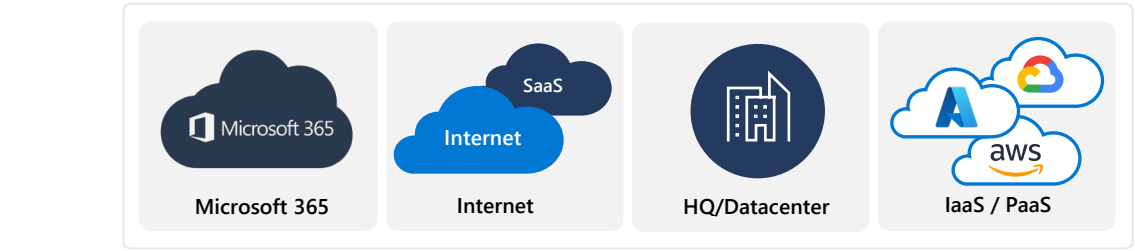
Microsoft's Identity-centric SSE solution

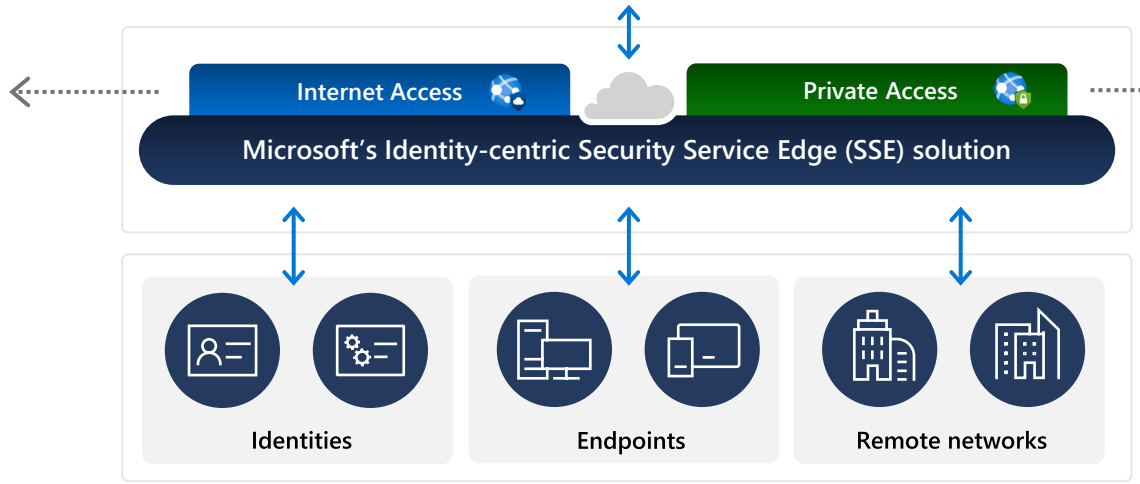


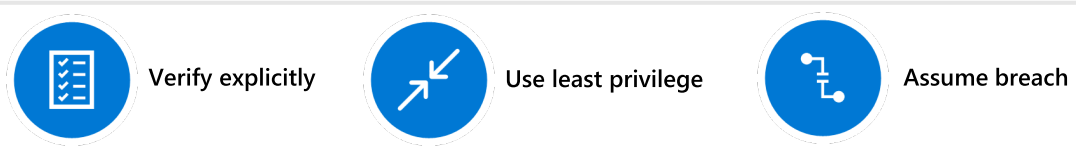
Microsoft's Identity-centric SSE solution

Microsoft Entra Internet Access

Secure access to all internet, SaaS, and Microsoft 365 apps and protect against malicious internet traffic with an **identity-centric Secure Web Gateway (SWG).**







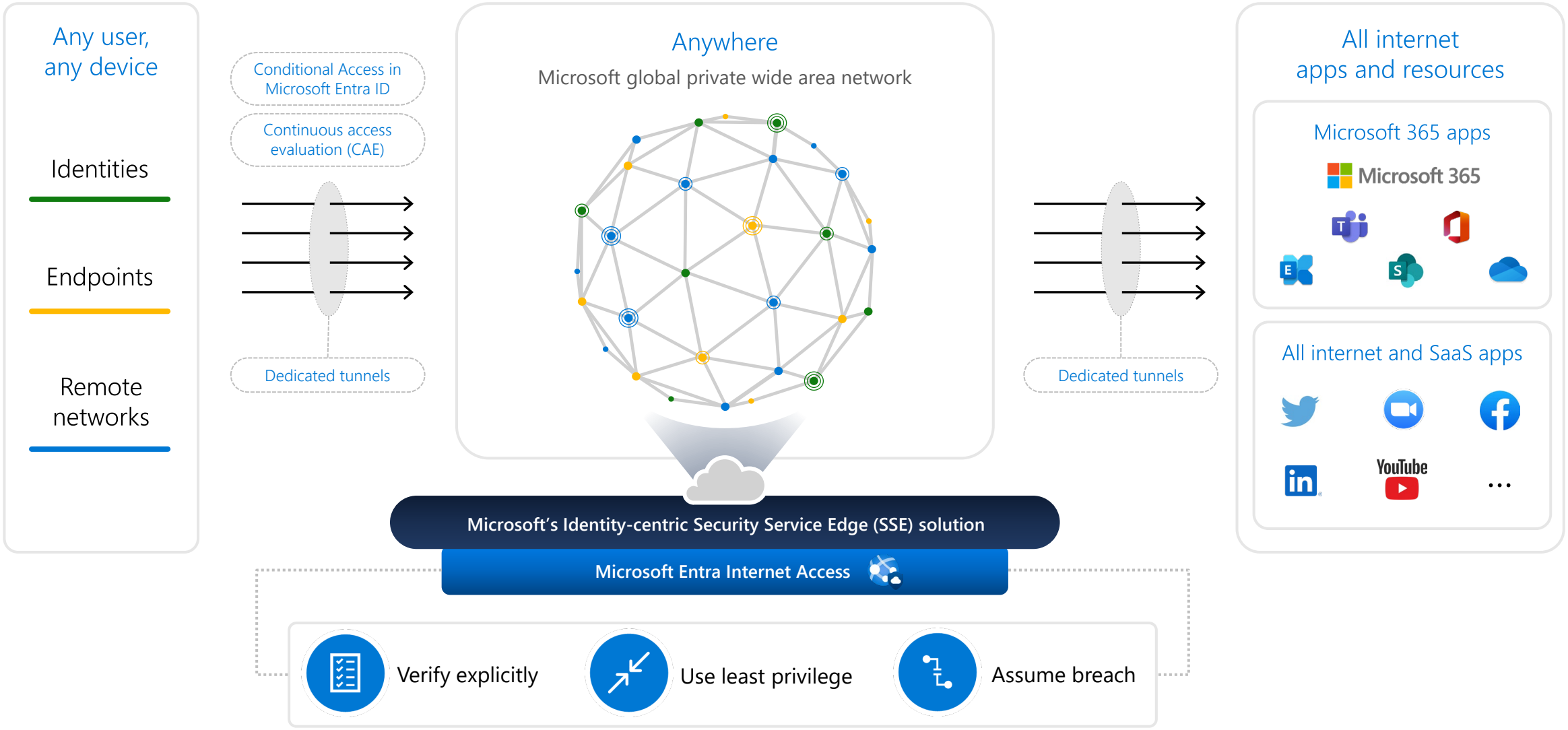
Microsoft Entra Private Access

Secure access to all private apps and resources, for users anywhere, with an **identity-centric Zero Trust Network Access (ZTNA).**

Microsoft Entra Internet Access

Microsoft Entra Internet Access

An identity-centric Secure Web Gateway (SWG) solution



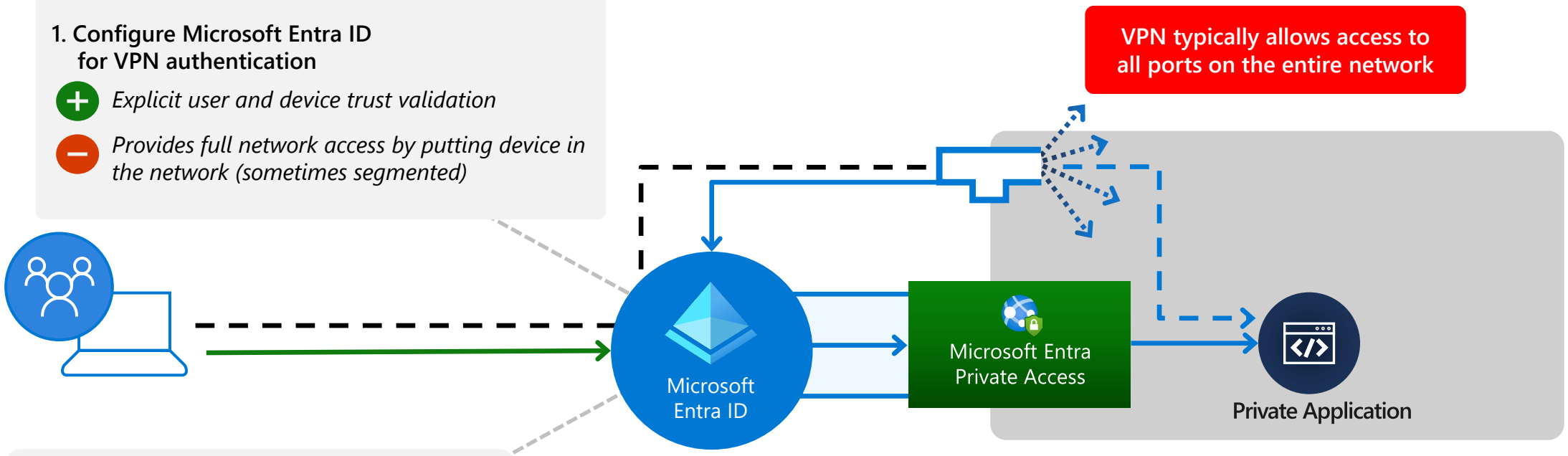
Microsoft Entra Private Access

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)*



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*

Microsoft Entra Private Access

An identity-centric Zero Trust Network Access (ZTNA)

Any user, any device

Identities

Endpoints

Remote networks

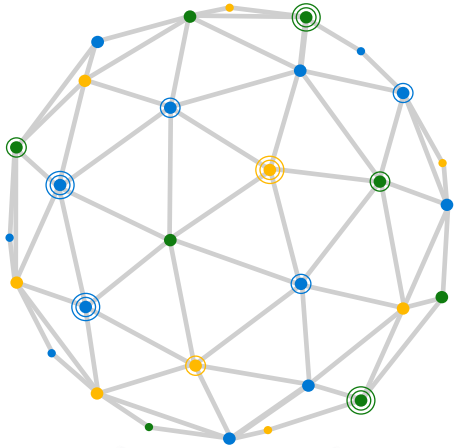
Conditional Access in Microsoft Entra ID

Continuous access evaluation (CAE)

Dedicated tunnels

Anywhere

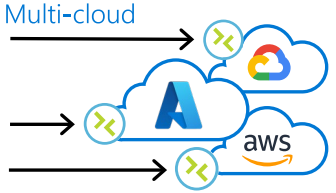
Microsoft global private wide area network



Dedicated tunnels

All private apps and resources

Multi-cloud



Web apps

RDP/SSH

SMB, FTP

Corporate network

ERP

Printers

...

Microsoft's Identity-centric Security Service Edge (SSE) solution

Microsoft Entra Private Access

Verify explicitly

Use least privilege

Assume breach

Microsoft Entra Private Access

Broad application support

Provide secure access to all private apps – any app, any port, any protocol

Access non-web apps (all TCP/UDP incl. RDP, SSH, SMB, FTP, …)

Identity-centric security controls

Control access using Entra Conditional Access (CA) policies

Coming soon: Revoke access using continuous access evaluation (CAE)

Single sign-on to private apps using SAML, Kerberos, header-based, …

Segmented app access

Enable access to specific apps as opposed to full network

Segment private app access based on user and device identity

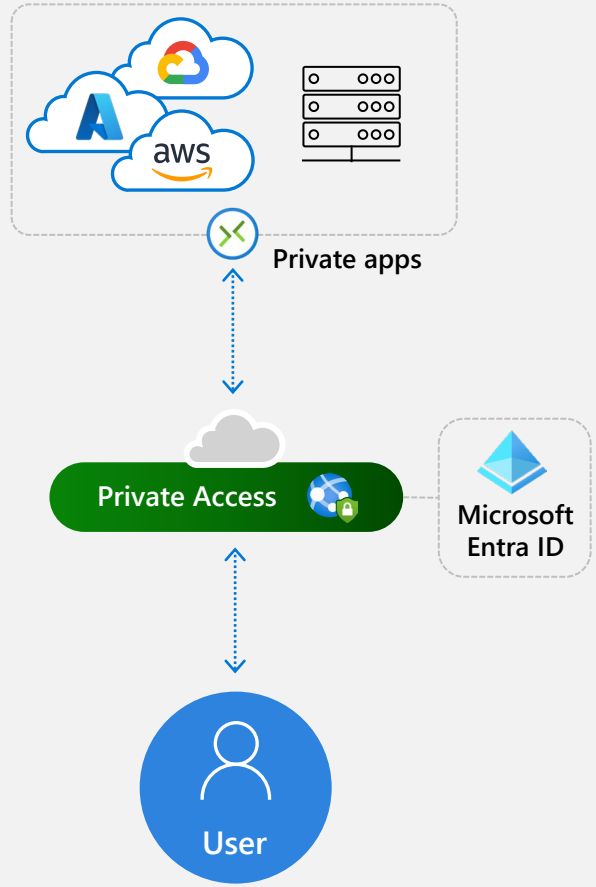
Coming soon: Micro-segment based on process identity

App discovery and onboarding

Discover private apps and onboard them to segment access to resources

Intelligent local access

Coming soon: Adaptive local access to private apps for hybrid users



Adaptive **identity-centric** Zero Trust Network Access (ZTNA)

Scenarios and use cases

QuickAccess

Easy migration from VPNs to zero trust network access to all private apps with a policy

App discovery

Discover apps and onboard/register them in Entra ID

Per app access

Configure access to a well-known private app with a policy

Rich apps and app segments

Support for non-https apps with SSO for legacy protocols like Kerberos

App groups and policies

Assign policies to individual apps or to app group(s)

Thank you!