Entra Private Access

Zero-Trust Network Access to any legacy resources with the Power of Entra Private Access

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Your hosts

Pim Jacobs

Principal Consultant
InSpark

Ronny de Jong

Security Technology Specialist,
Microsoft

Pim Jacobs

Principal Consultant @ InSpark &
Microsoft Security MVP

- Focus on the full Microsoft Entra portfolio
- One of the organisers of the **Dutch Microsoft Entra Community**, join our meetup page!

- Blog: **identity-man.eu**
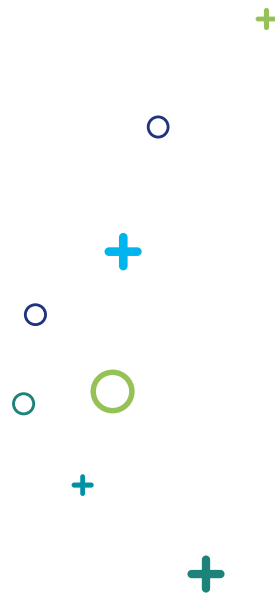- Skiing | Soccer | F1 | Family time

What are we going to discuss?

1. The why

2. What does GSA consist of

3. What is Entra Private Access

4. From Quick Access…

5. …to Per-App access

6. Next Steps & Takeaways

1. Rise of cloud & Hybrid Workforce

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-prem 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
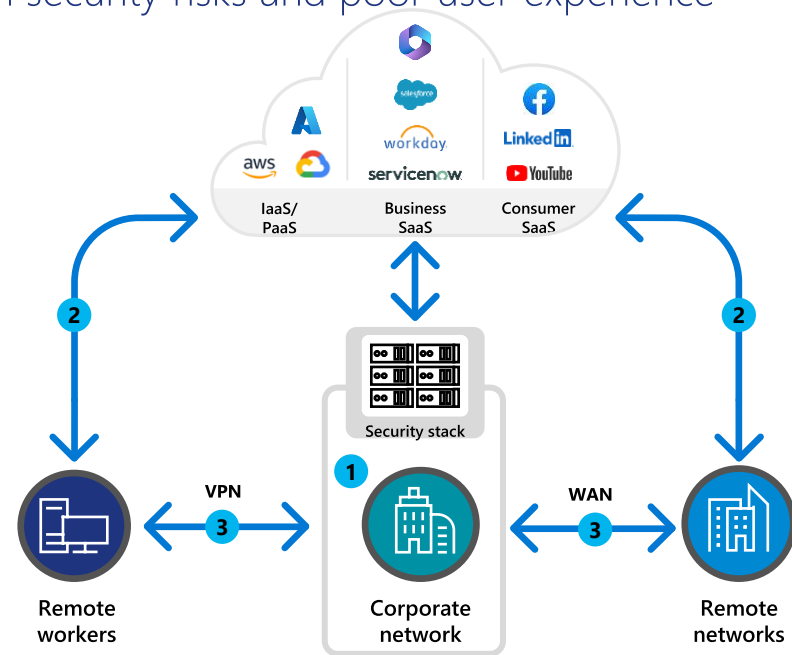
1. The intro of two new SSE products

Beneath the Microsoft Entra Global Secure Access umbrella

Explore New Product Announcements for Microsoft Entra   ...

By Irina Nechaeva

Published Jul 11 2023 09:00 AM   👁 8,462 Views   🎧

Today at our Reimagine Secure Access with Microsoft Entra digital event, Microsoft Security leaders and industry experts presented the next set of innovations from Microsoft Entra. Check out our Microsoft Security blog to learn more about the product announcements.

A brief overview of what we shared at the event:

To provide secure access for any identity to any resource and protect all digital interactions, we announced two new Security Service Edge (SSE) products—**Microsoft Entra Internet Access** and **Microsoft Entra Private Access**. Microsoft Entra Internet Access is an identity-centric, cloud-delivered Secure Web Gateway (SWG) to protect access to internet, SaaS, and Microsoft 365 apps, while Microsoft Entra Private Access is an identity-centric Zero Trust Network Access to secure access to private apps and resources.

2. What are the Global Secure Access components?

- Users & Devices
- Three possible tunnels to the Microsoft Edge
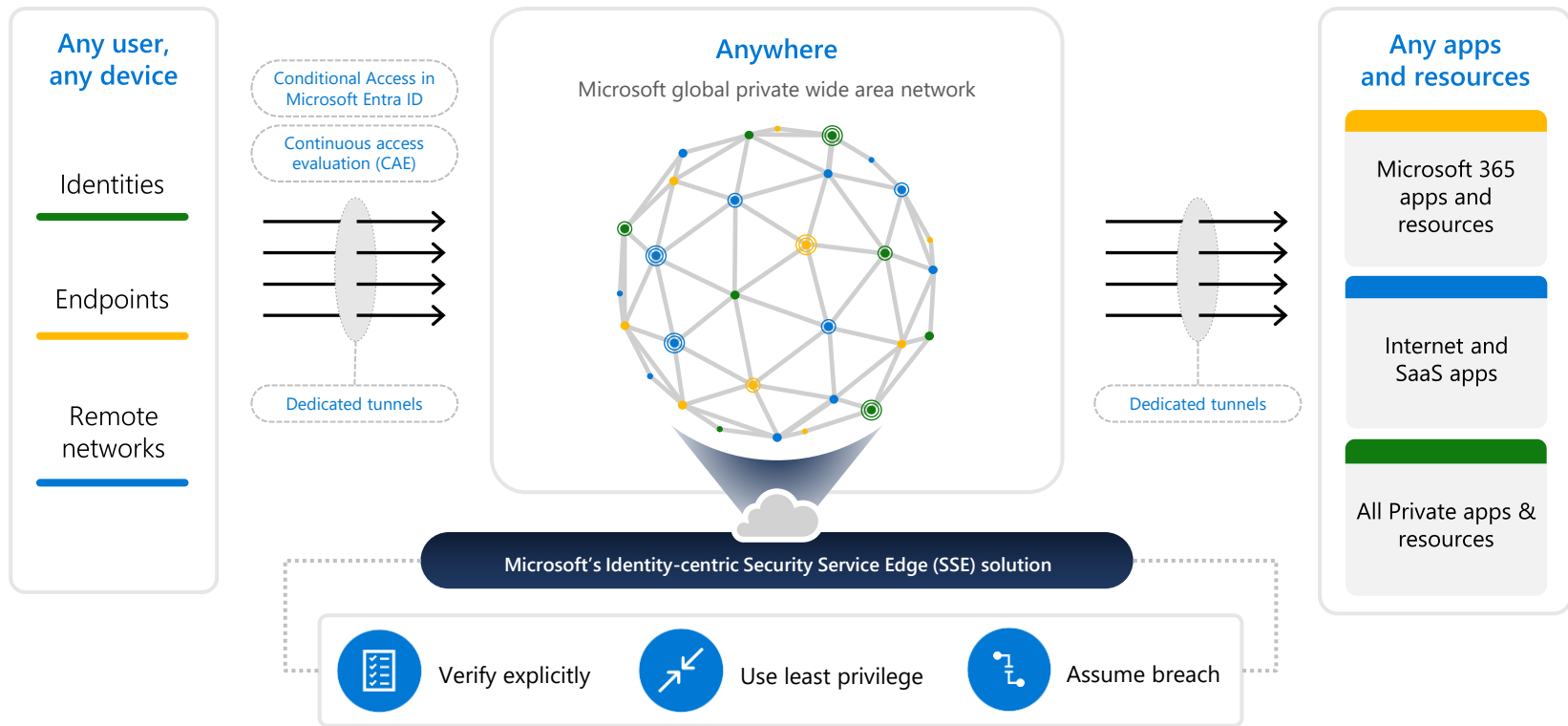- Secure by design & Conditional Access
- Provide Access to on-prem resources, M365 and the Internet
- IPSec tunnel support (not for private access)

2. Microsoft's Identity-centric SSE solution

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

Any apps and resources

Microsoft 365 apps and resources

Internet and SaaS apps

All Private apps & resources

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

Verify explicitly

Use least privilege

Assume breach

rubrik

DELL Technologies

SquaredUp

infinity

INTERSTELLAR

kpn Partner Network

INSPARK

cegeka

2. Microsoft's Identity-centric SSE solution

An identity-centric security service edge (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 365 apps	All internet apps

Microsoft Entra Private Access

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

Private web apps	All private apps

Legenda

GA	Public preview

rubrik   DELL Technologies   SquaredUp   infinity   INTERSTELLAR   kpn Partner Network   INSPARK   cegeka

2. Trip down memory lane

Entra Private Access all started in.....

July 2020
Development
PoC

June 2023
Public Preview

Silence.....

December
2020 Feature
prioritization

April/May
2023 Private
Preview
available

??? 2024
Generally
Available?

2. Trip down memory lane

Entra Private Access all started in July 2020.....


```
PS C:\Porto\Connector> .\portoconnector.ps1
Create firewall rule for Porto Connector

2020/07/23 23:32:58 Porto Con
2020/07/23 23:32:58 Load conf
2020/07/23 23:32:58 Registrin
2020/07/23 23:32:58 127.0.0.1
2020/07/23 23:32:58 127.0.0.1
2020/07/23 23:32:58 127.0.0.1
2020/07/23 23:32:58 Create tu
2020/07/23 23:32:58 Start Tcp
2020/07/23 23:32:58 Start Udp
2020/07/23 23:32:58 Listen on
2020/07/23 23:32:58 UDP echo
2020/07/23 23:32:58 TCP echo
```

```
PS C:\Porto\agent> .\portoagent.ps1
Create firewall rule for Porto Agent UI

2020/07/23 23:33:50 Porto Agent v0.4
2020/07/23 23:33:50 Load config: C:\Port
2020/07/23 23:33:50 DNS register
2020/07/23 23:33:50 DNS register SRV _ke
2020/07/23 23:33:50 DNS register sql
2020/07/23 23:33:50 DNS register azr
2020/07/23 23:33:50 DNS register azr
2020/07/23 23:33:50 Starting DNS server
2020/07/23 23:33:50 Create tun tun-porto
2020/07/23 23:33:55 Route static IP 10.
2020/07/23 23:33:55 Route static IP 10.1
2020/07/23 23:33:56 Configure Windows
2020/07/23 23:34:00 Waiting for incoming
2020/07/23 23:34:04 DNS resolved A query
2020/07/23 23:34:04 Prompt user for log
2020/07/23 23:34:05 Connecting to AppPro
1:445
2020/07/23 23:34:05 DNS resolved A query
2020/07/23 23:34:05 Connect failed. Igno
ebsocket: bad handshake
2020/07/23 23:34:09 No app for 10.211.5.
2020/07/23 23:34:10 No app for 10.211.5.
2020/07/23 23:34:12 No app for 10.211.5.
2020/07/23 23:34:16 No app for 10.211.5.
```

[action required] Project Porto - Prioritization ask

Summar

DM To   12/16/2020
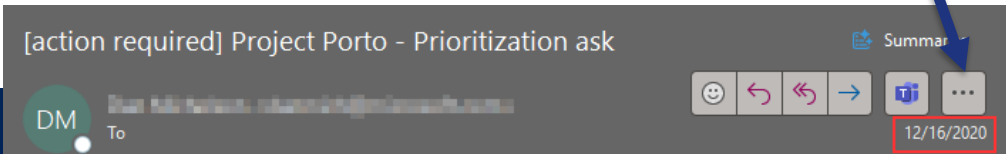
Dear Porto Design Partner,

We need your assistance in prioritizing 7 important pillars in Porto.
We are willing to catch the top minimal contents that will enable deployment in your organization.
This way we'll make the right choices to bring you Porto as fast as possible.

Porto is expanding the current private access solution, AAD App Proxy in two dimensions:
1) Expanding to support all non-http protocols
2) Expanding to support more auditing and security capabilities

We ask you to:
- Consult with the stake holders in your org
- Stack rank the pillars
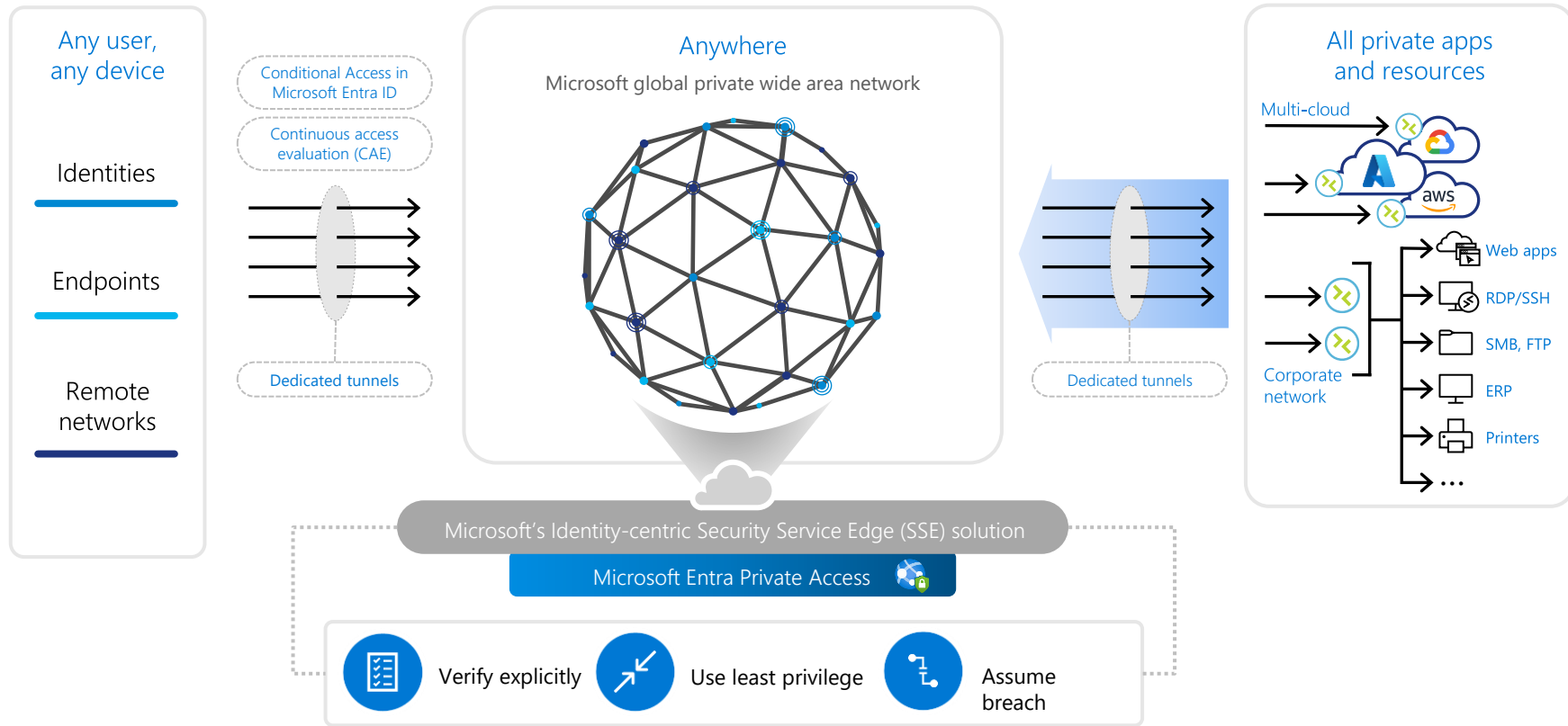- Tell us your inclusive cutline that will enable deployment in your org.

Thanks,

3. Entra Private Access

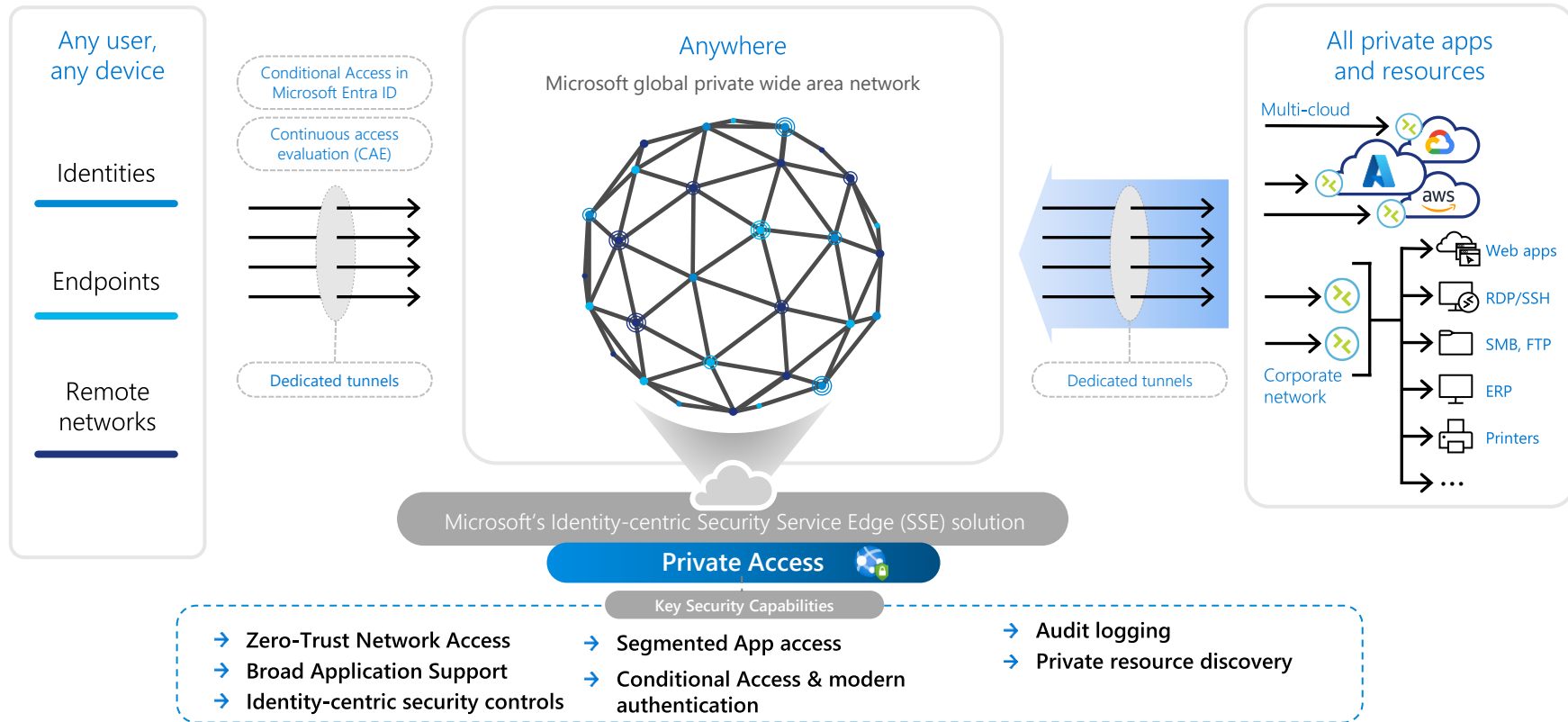## Any user, any device

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

Corporate network

- Web apps
- RDP/SSH
- SMB, FTP
- ERP
- Printers
- ...

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

Microsoft Entra Private Access

Verify explicitly

Use least privilege

Assume breach

rubrik   DELL Technologies   SquaredUp   infinity   INTERSTELLAR   kpn Partner Network   INSPARK   cegeka

3. Entra Private Access

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

Corporate network

- Web apps
- RDP/SSH
- SMB, FTP
- ERP
- Printers
- …

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

Private Access

Key Security Capabilities

- → Zero-Trust Network Access
- → Broad Application Support
- → Identity-centric security controls
- → Segmented App access
- → Conditional Access & modern authentication
- → Audit logging
- → Private resource discovery

rubrik | DELL Technologies | SquaredUp | infinity | INTERSTELLAR | kpn Partner Network | INSPARK | cegeka

3. Moving beyond VPNs

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)*

VPN typically allows access to all ports on the entire network

Microsoft Entra ID

Microsoft Entra Private Access

Private Application

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*

All it takes is 1 compromised user or 1 compromised device to hold hostage everything in your network!!!!

infinity   INTERSTELLAR   kpn Partner Network   INSPARK   cegeka
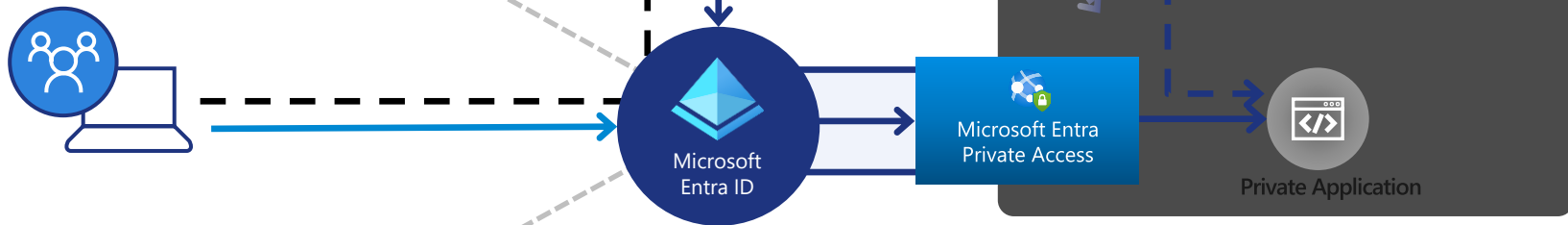
3. Moving beyond Remote Desktops

1. Configure Microsoft Entra ID for RDS authentication

+ *Explicit user and device trust validation*

− *Provides full network access by putting device in the network (sometimes segmented)*

RDS typically allows access to all ports on the entire network

Microsoft Entra ID

Microsoft Entra Private Access

Private Application

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*

All it takes is 1 compromised user or 1 compromised device to hold hostage everything in your network!!!!

infinity   INTERSTELLAR   kpn Partner Network   INSPARK   cegeka

3. The Requirements

Me checking the system requirements

Meeting the minimum requirements

I'm still worthy!

Windows, MacOS have GSA client installed

Android or iOS via Defender for Endpoint App

Hybrid Identities in Entra ID

Entra Private Access Connector installed in on-premises domain

Private Access Connector needs outbound connection on port 80 & 443

Enable new diagnostic logging setting(s) in Entra ID

Hybrid Entra Joined or Entra Joined

rubrik Technologies infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

3. Implementing Entra Private Access

Deploy clients and Private Access Connectors

Enable **traffic profiles** in Global Secure Access

Configure **QuickAccess** to migrate away from VPNs, RDS / AVD to ZTNA for all private apps with a single policy

Increase security based on per app model in **Conditional Access**
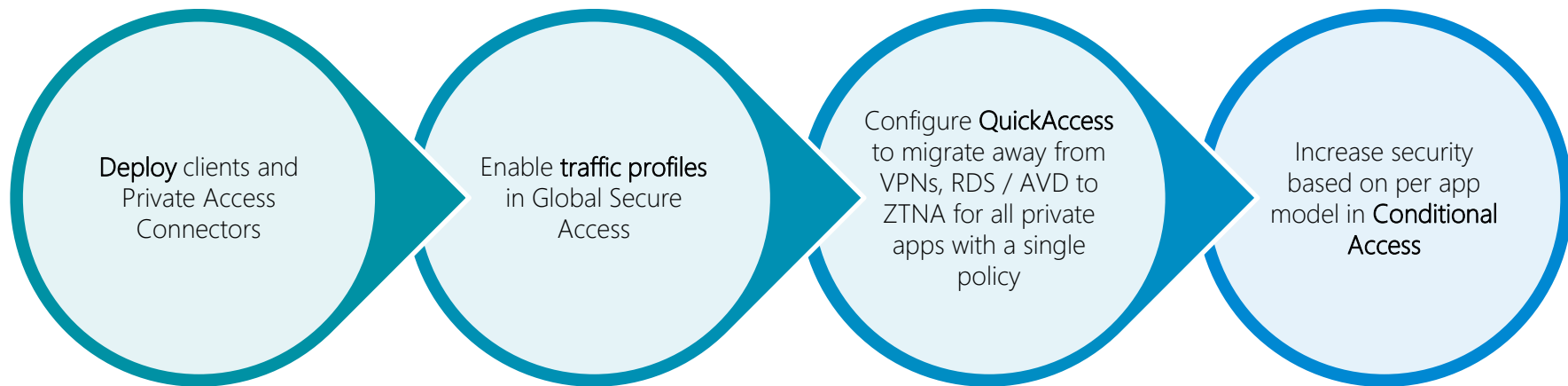
4. Quick Access

Fast & easy migration from legacy VPN to identity-centric Zero Trust Network Access (ZTNA)

» Quick experience

First step for Zero Trust Network Access to private resources

Minimal config to get started

Start with broad access

» Flexibility

Supports IP range, IP addresses, FQDNs, or wildcard suffixes
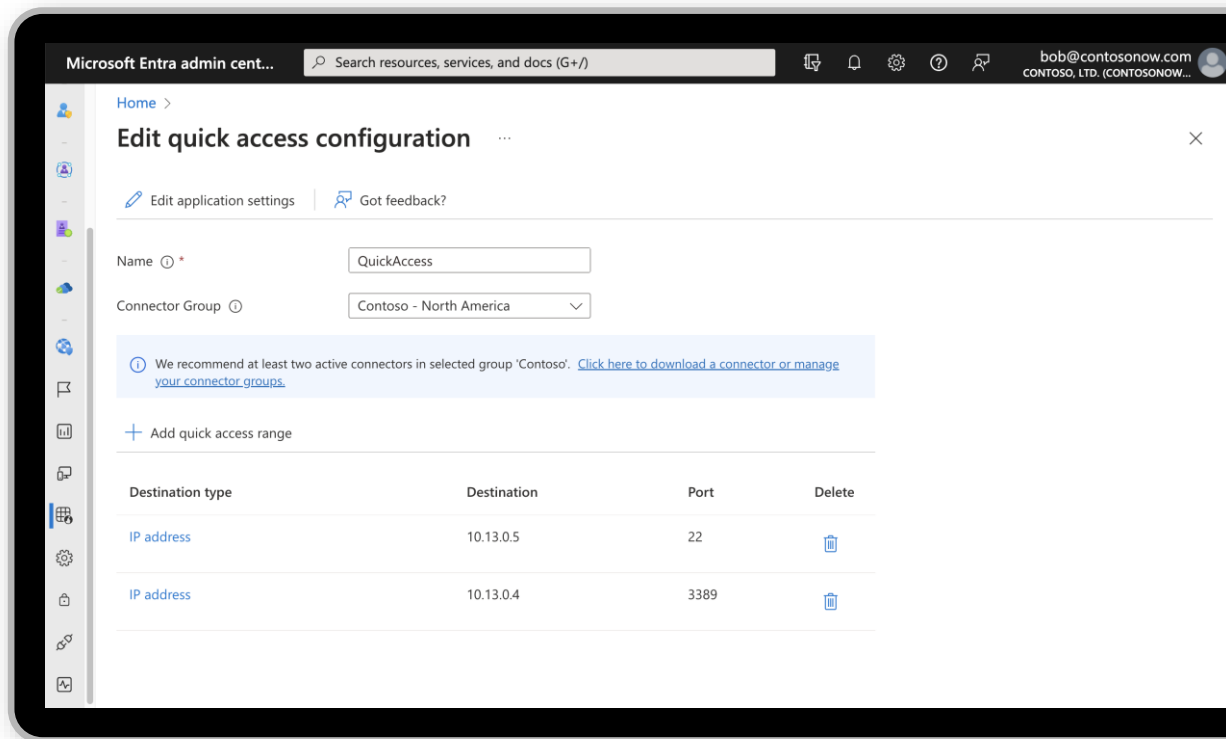
Demo #1

Replace VPN solution with **Quick Access**

5. Preparing for per app access

Configure diagnostic settings within Microsoft Entra ID

Load Workbook within Log Analytics Workspace

Analyze workbook data and summarize application groups

Create **per app access configuration** in Global Secure Access

Create Entra ID **Groups** and **assign groups** to per app access

Remove per app access configuration from **quick access**
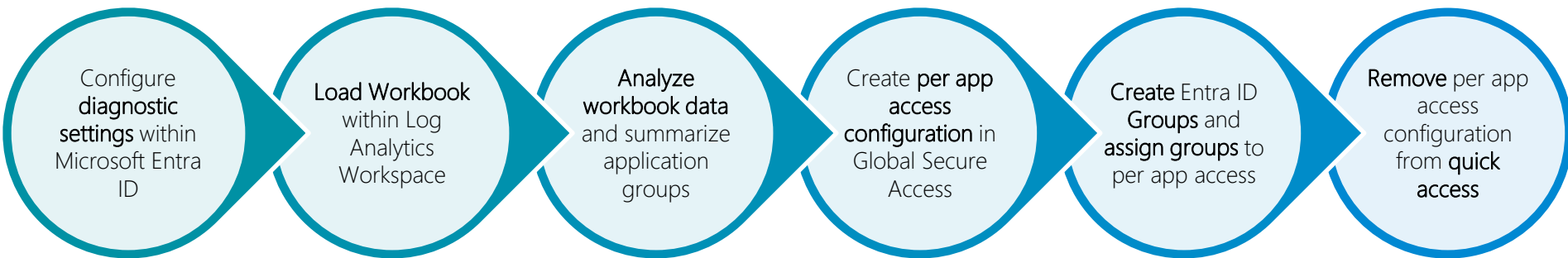
Demo #2

Move from Quick Access to **Per-App Access** with workbooks and move to a least privilege mode.

6. Keep in mind that…..

- OOBE Process breaks if client is installed during this process
- Tunnels can't be excluded from Conditional Access today
- UDP Support not there (yet) so WHfB hybrid won't work (yet)
- Traffic profiles are today enabled on tenant level for all users
- Remote networks don't support Private Access Today
- Avoid overlap between Quick Access and Per App Access.
- Private Access does not support multi-geo tenants

6. Key Takeaways

SSE offers a more comprehensive, flexible, and modern approach to secure network access.

SSE caters to cloud-based environments and remote work scenarios.

Zero Trust model, ensuring that access is granted based on identity, device posture, and context.

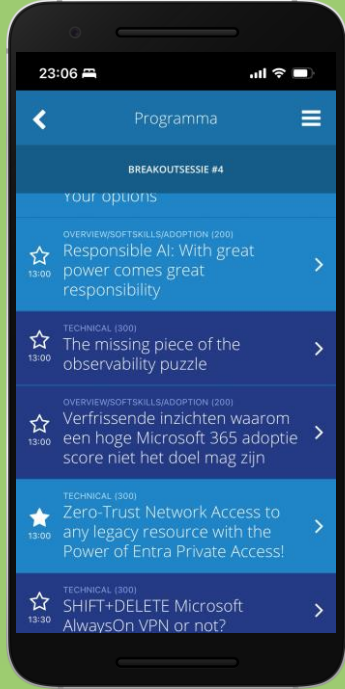Allows granular control over access to specific applications, improving security and reducing risk.

Next session 14:00 – 14:50

Securing your Entra Identities in 2024