Welcome to the next gen VPN with Global Secure Access

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Gregor Reimling

Eric Berg

Gregor Reimling (he/him)

Chief Azure Technologist @ adesso SE, Germany

Gregor is awarded with the Microsoft MVP for Microsoft Azure and Security. He works as Chief Azure Technologist for adesso SE and is technical lead for Azure . His main areas are Microsoft Azure, Enterprise scale architectures, Cloud Security, Governance, Hybrid and Migration.

/in/GregorReimling

GregorReimling

GregorReimling

reimling.eu

2Pint

PATCH
MY PC

robopack

wortell

INGRAM MICRO®

The Collective

bechtle

lebon.IT

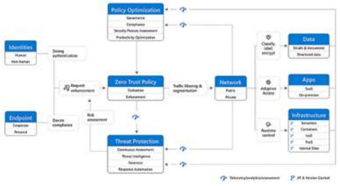
ConXioN
The new style of IT

VirtualMetric

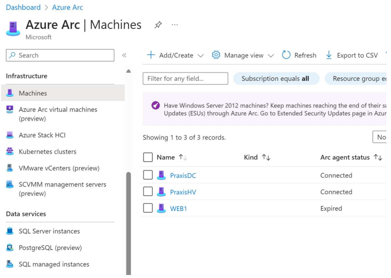
veeam

evri

Agenda



Zero Trust Architecture & Network Definitions



Dashboard > Azure Arc

Azure Arc | Machines

Microsoft

Search

+ Add/Create | Manage view | Refresh | Export to CSV

Infrastructure
- Machines
- Azure Arc virtual machines (preview)
- Azure Stack HCI
- Kubernetes clusters
- VMware vCenters (preview)
- SCVMM management servers (preview)

Data services
- SQL Server instances
- PostgreSQL (preview)
- SQL managed instances

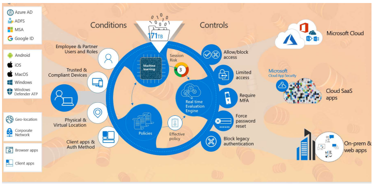
Filter for any field... | Subscription equals **all** | Resource group e

Have Windows Server 2012 machines? Keep machines reaching the end of their su Updates (ESUs) through Azure Arc. Go to Extended Security Updates page in Azur

Showing 1 to 3 of 3 records.

Name	Kind	Arc agent status
PraxisDC		Connected
PraxisHV		Connected
WEB1		Expired

Entra Suite



Global Secure Access

BuildClouds

Get Started with the dashboard | Got feedback? | Last 24 hours

Global Secure Access snapshot

Traffic type : All

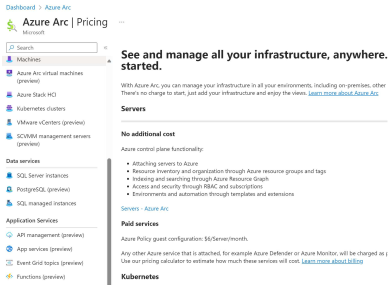
The Global Secure Access snapshots provides quick access to the users, devices, and destinations with network traffic captured by Microsoft Entra Private Access and Microsoft Entra Internet Access.

Out of 18 devices, 1 have the Global Secure Access Client installed. 5.6%

Usage profiling PREVIEW

Display by : Transactions | Date : Last month

Private Access



Dashboard > Azure Arc

Azure Arc | Pricing

Microsoft

Search

- Machines
- Azure Arc virtual machines (preview)
- Azure Stack HCI
- Kubernetes clusters
- VMware vCenters (preview)
- SCVMM management servers (preview)

Data services
- SQL Server instances
- PostgreSQL (preview)
- SQL managed instances

Application Services
- API management (preview)
- App services (preview)
- Event Grid topics (preview)
- Functions (preview)

See and manage all your infrastructure, anywhere. started.

With Azure Arc, you can manage your infrastructure in all your environments, including on-premises, other There's no charge to start, just add your infrastructure and enjoy the views. Learn more about Azure Arc

Servers

No additional cost

Azure control plane functionality:

- Attaching servers to Azure
- Resource inventory and organization through Azure resource groups and tags
- Indexing and searching through Azure Resource Graph
- Access and security through RBAC and subscriptions
- Environments and automation through templates and extensions

Servers - Azure Arc

Paid services

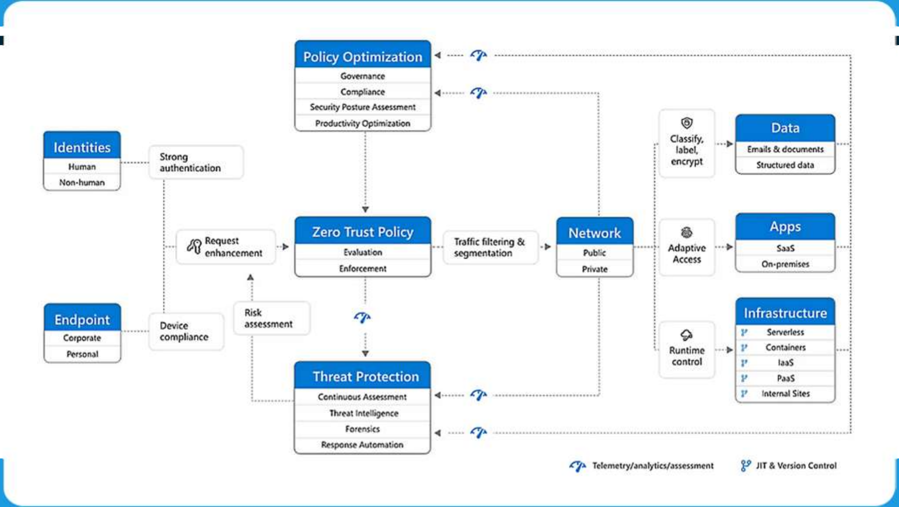
Azure Policy guest configuration: $6/Server/month.

Any other Azure service that is attached, for example Azure Defender or Azure Monitor, will be charged as p Use our pricing calculator to estimate how much these services will cost. Learn more about billing

Kubernetes

Release process

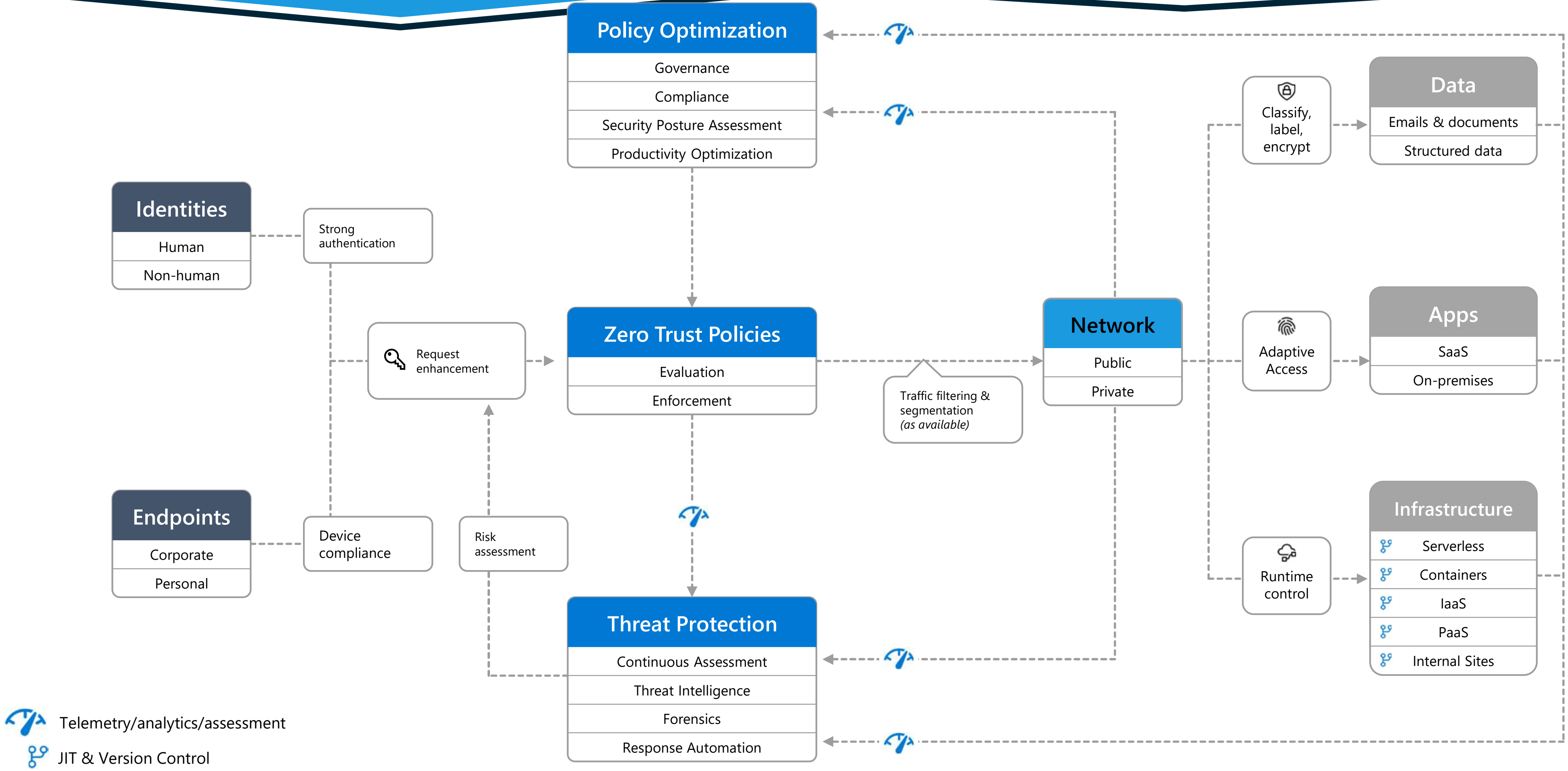
Zero Trust Architecture & Network Definitions



Zero Trust Security Model

- … is a **security framework** that assumes **no implicit trust** is granted to assets or user accounts **based** solely **on** their **physical** or **network location**. Instead, it requires **continuous verification** of the **identity** and **integrity** of **devices** and **users**, **regardless** of whether they are **inside** or **outside** the network perimeter

Zero Trust Architecture



Policy Optimization
- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Identities
- Human
- Non-human

Strong authentication

Request enhancement

Zero Trust Policies
- Evaluation
- Enforcement

Traffic filtering & segmentation *(as available)*

Network
- Public
- Private

Classify, label, encrypt

Data
- Emails & documents
- Structured data

Adaptive Access

Apps
- SaaS
- On-premises

Endpoints
- Corporate
- Personal

Device compliance

Risk assessment

Threat Protection
- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Runtime control

Infrastructure
- Serverless
- Containers
- IaaS
- PaaS
- Internal Sites

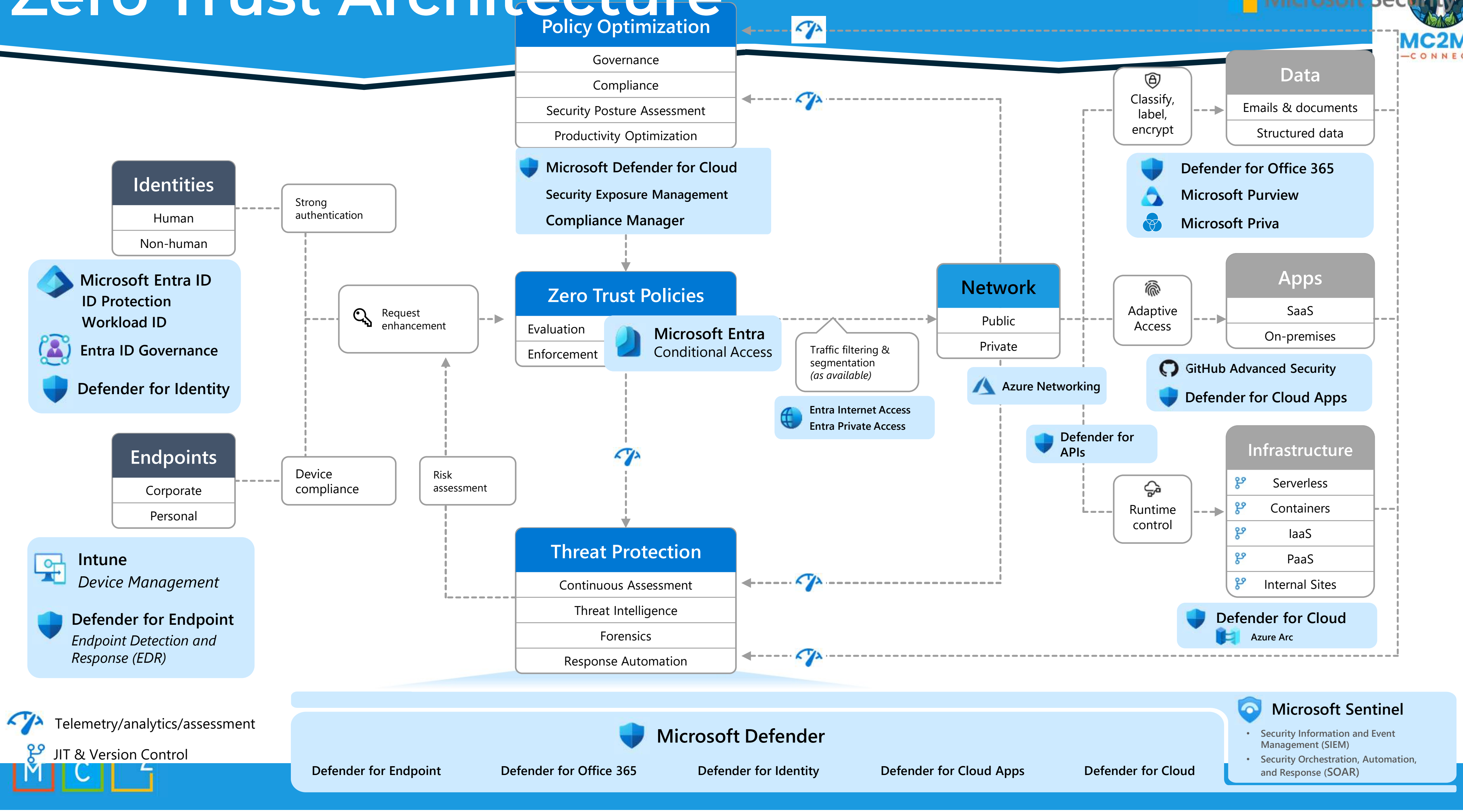
Telemetry/analytics/assessment

JIT & Version Control

Zero Trust Architecture

Microsoft Security

MC2MC CONNECT



Policy Optimization

- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Microsoft Defender for Cloud
Security Exposure Management
Compliance Manager

Identities

- Human
- Non-human

Microsoft Entra ID
ID Protection
Workload ID
Entra ID Governance
Defender for Identity

Strong authentication

Request enhancement

Zero Trust Policies

- Evaluation
- Enforcement

Microsoft Entra Conditional Access

Traffic filtering & segmentation *(as available)*

Entra Internet Access
Entra Private Access

Network

- Public
- Private

Azure Networking

Defender for APIs

Endpoints

- Corporate
- Personal

Intune
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

Device compliance

Risk assessment

Threat Protection

- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Data

- Emails & documents
- Structured data

Classify, label, encrypt

Defender for Office 365
Microsoft Purview
Microsoft Priva

Apps

- SaaS
- On-premises

Adaptive Access

GitHub Advanced Security
Defender for Cloud Apps

Infrastructure

- Serverless
- Containers
- IaaS
- PaaS
- Internal Sites

Runtime control

Defender for Cloud
Azure Arc

Telemetry/analytics/assessment

JIT & Version Control

Microsoft Defender

Defender for Endpoint | Defender for Office 365 | Defender for Identity | Defender for Cloud Apps | Defender for Cloud

Microsoft Sentinel

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Secure Access Service Edge (SASE)

- … is a **network architecture** that combines wide area networking (**WAN**) capabilities with comprehensive security functions, such as secure web gateways (**SWG**), cloud access security brokers (**CASB**), and zero trust network access (**ZTNA**), into a **single cloud-delivered service model**. SASE aims to provide **secure** and **efficient access** to applications and data, **regardless** of user **location**.
- Examples: Prisma SASE, FortiSASE

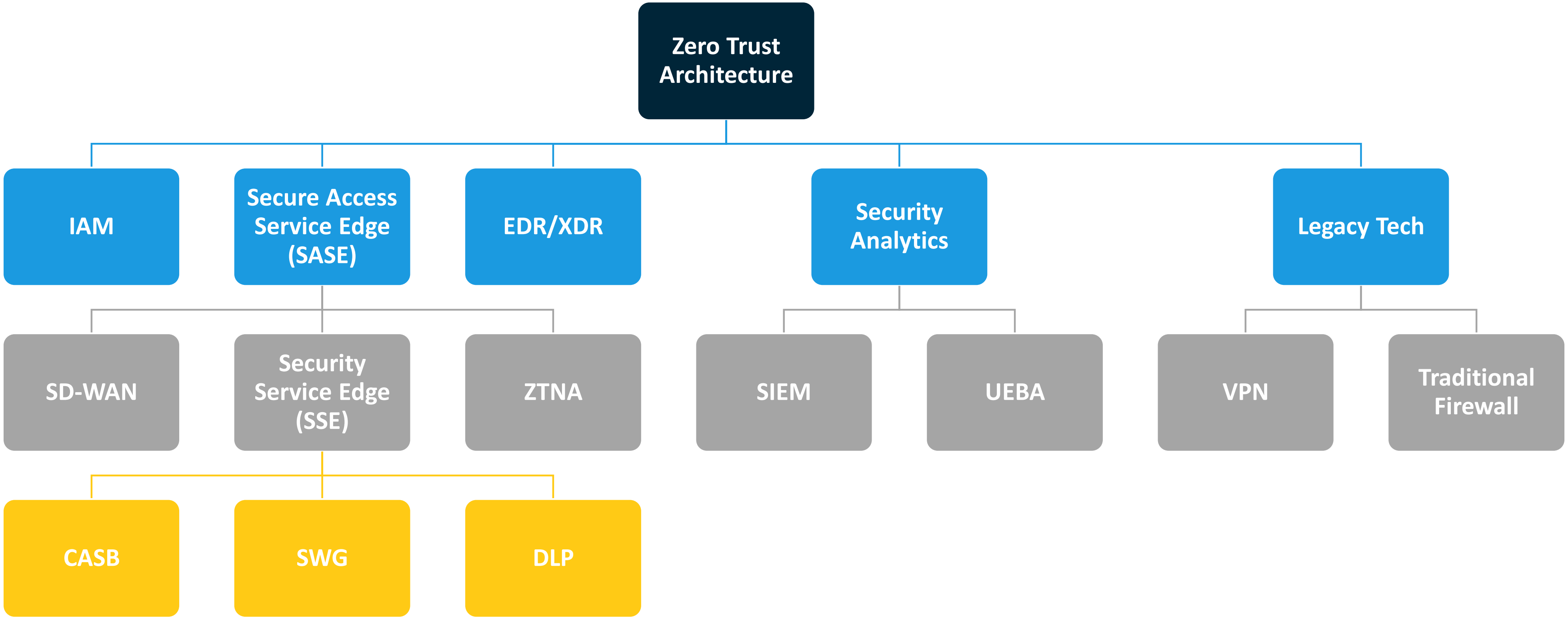
Security Service Edge (SSE)

- … is a **subset of SASE** that focuses specifically on the **security services** aspect. It includes capabilities like zero trust network access (**ZTNA**), secure web gateways (**SWG**), and cloud access security brokers (**CASB**) to ensure secure access to web, cloud, and private applications
- Examples: Zscaler (going to SASE, Cloudflare One,)

Global Secure Access (GSA)

- … refers to a **comprehensive security solution** that integrates various **security services** to provide secure **remote access** to applications, data, and resources across the globe. It typically includes features like **identity verification**, **access control**, and **threat protection** to ensure secure and seamless connectivity for remote users

And now … all together …



Zero Trust Architecture

IAM

Secure Access Service Edge (SASE)

EDR/XDR

Security Analytics

Legacy Tech

SD-WAN

Security Service Edge (SSE)

ZTNA

SIEM

UEBA

VPN

Traditional Firewall

CASB

SWG

DLP

Azure Bastion

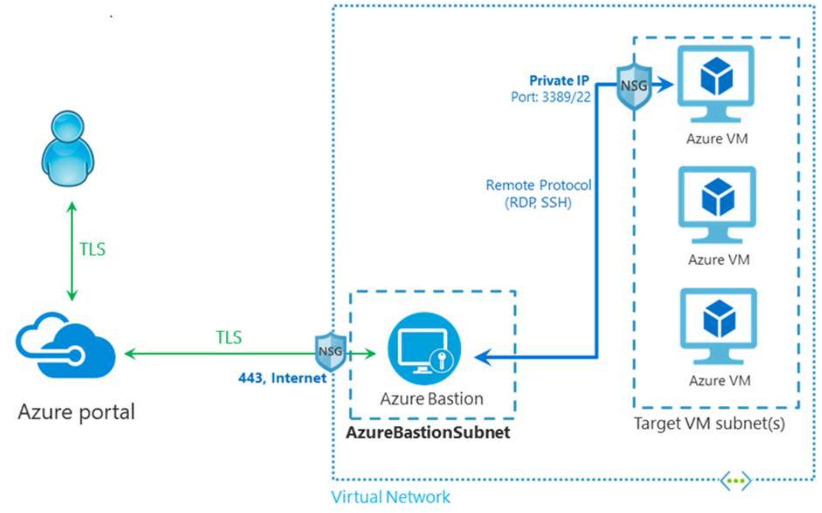
Azure Bastion provides secure RDP/SSH connectivity to your VMs without exposing ports to the public internet.

Bastion Premium

- Secure sensitive workloads end-to-end with enhanced auditing and monitoring features
- Graphically record, monitor, and store VM sessions for full visibility and compliance needs

Bastion Developer

- Secure-by-default connectivity to Azure VMs with just one click – at no extra cost.



Azure ExpressRoute

Azure ExpressRoute Metro

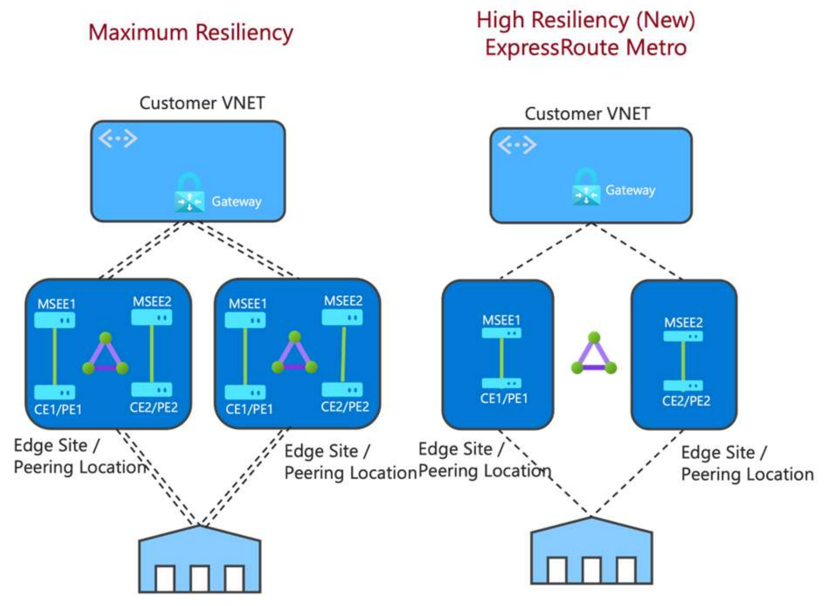
- Built-in site resiliency across two distinct peering locations in a metro city

Seamless gateway migration

- Migrate ExpressRoute Gateways to zone-redundant deployments with zero downtime

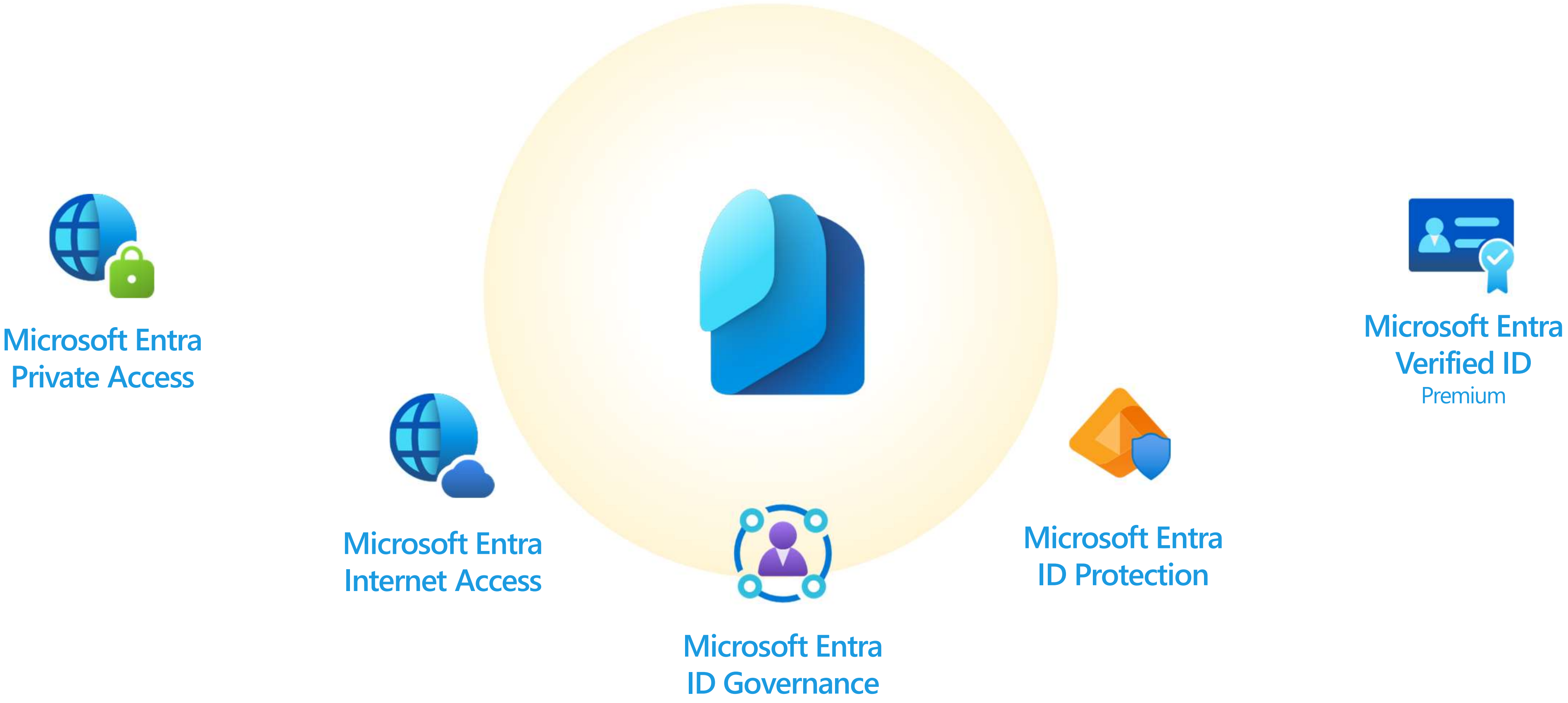
Scalable Gateway

- Auto scale for up to 40Gbps connectivity via ExpressRoute Gateway to the VNet



MSEE = Microsoft Enterprise Edge Device; CE = Customer Edge Device; PE = Provider Edge Device

Microsoft Entra Suite



Microsoft Entra Private Access

Microsoft Entra Internet Access

Microsoft Entra ID Governance

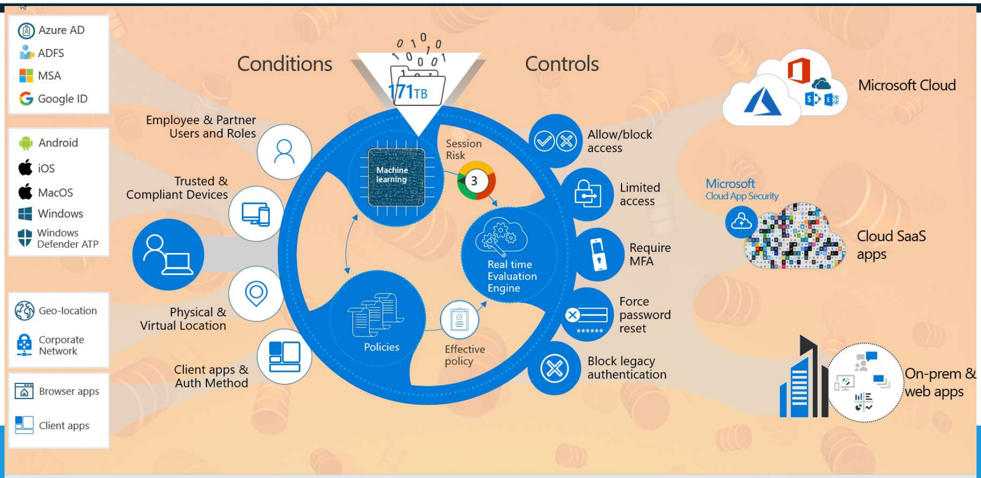
Microsoft Entra ID Protection

Microsoft Entra Verified ID
Premium

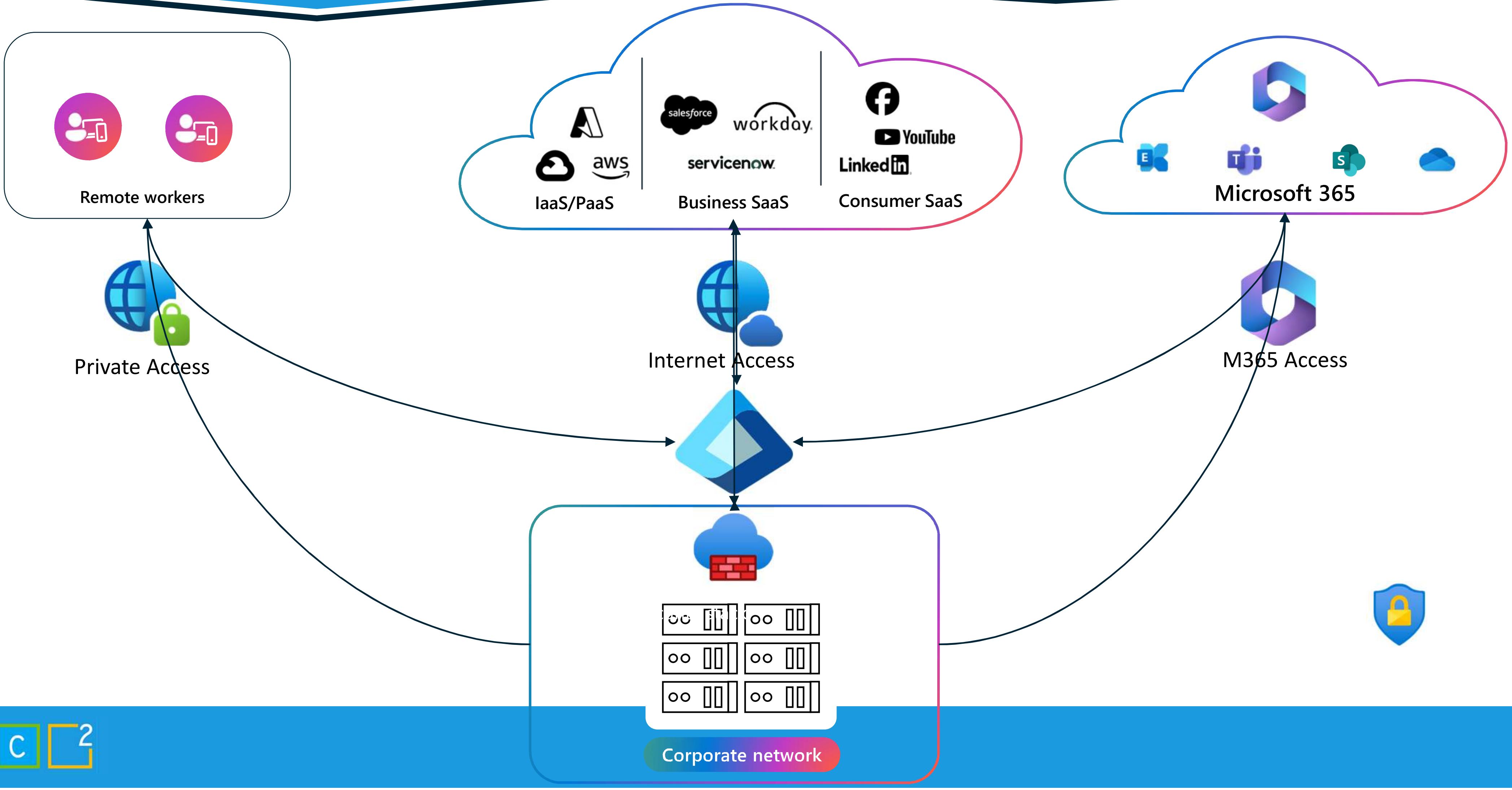
Journey to SSE – Decision to move

Traditional VPN		Microsoft Entra Suite
Complex, requires networking experts to configure and maintain	**Maintenance**	Simple to configure and maintain with basic networking knowledge and Entra experience
Not designed for Zero Trust and challenging to implement	**Zero Trust**	Architected from the ground up for Zero Trust
Minimal native security features for authentication	**Security**	Native to Entra, secured by Conditional Access and Entra SSO

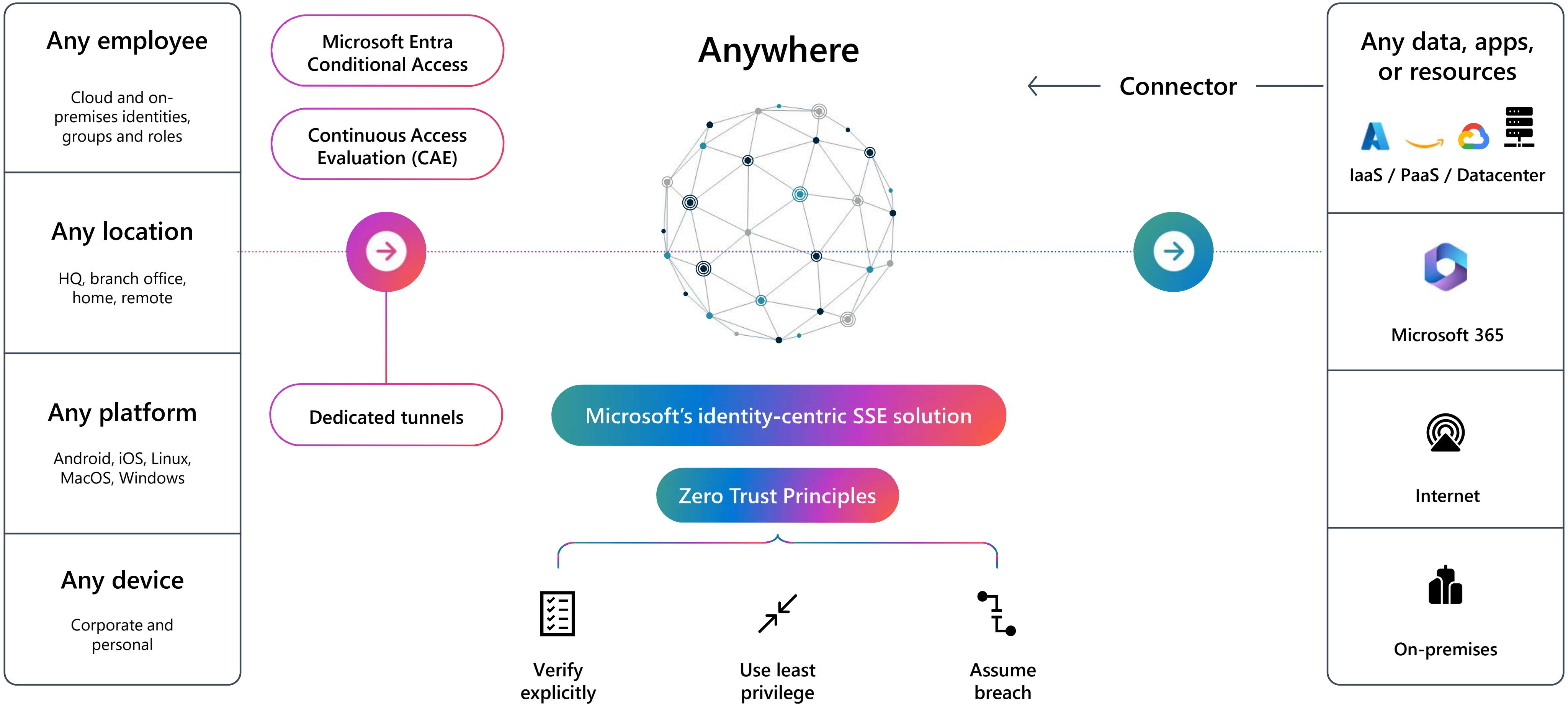
Global Secure Access



Global Secure Access



Global Secure Access (GSA)



Any employee

Cloud and on-premises identities, groups and roles

Any location

HQ, branch office, home, remote

Any platform

Android, iOS, Linux, MacOS, Windows

Any device

Corporate and personal

Microsoft Entra Conditional Access

Continuous Access Evaluation (CAE)

Dedicated tunnels

Anywhere

Connector

Microsoft's identity-centric SSE solution

Zero Trust Principles

- Verify explicitly
- Use least privilege
- Assume breach

Any data, apps, or resources

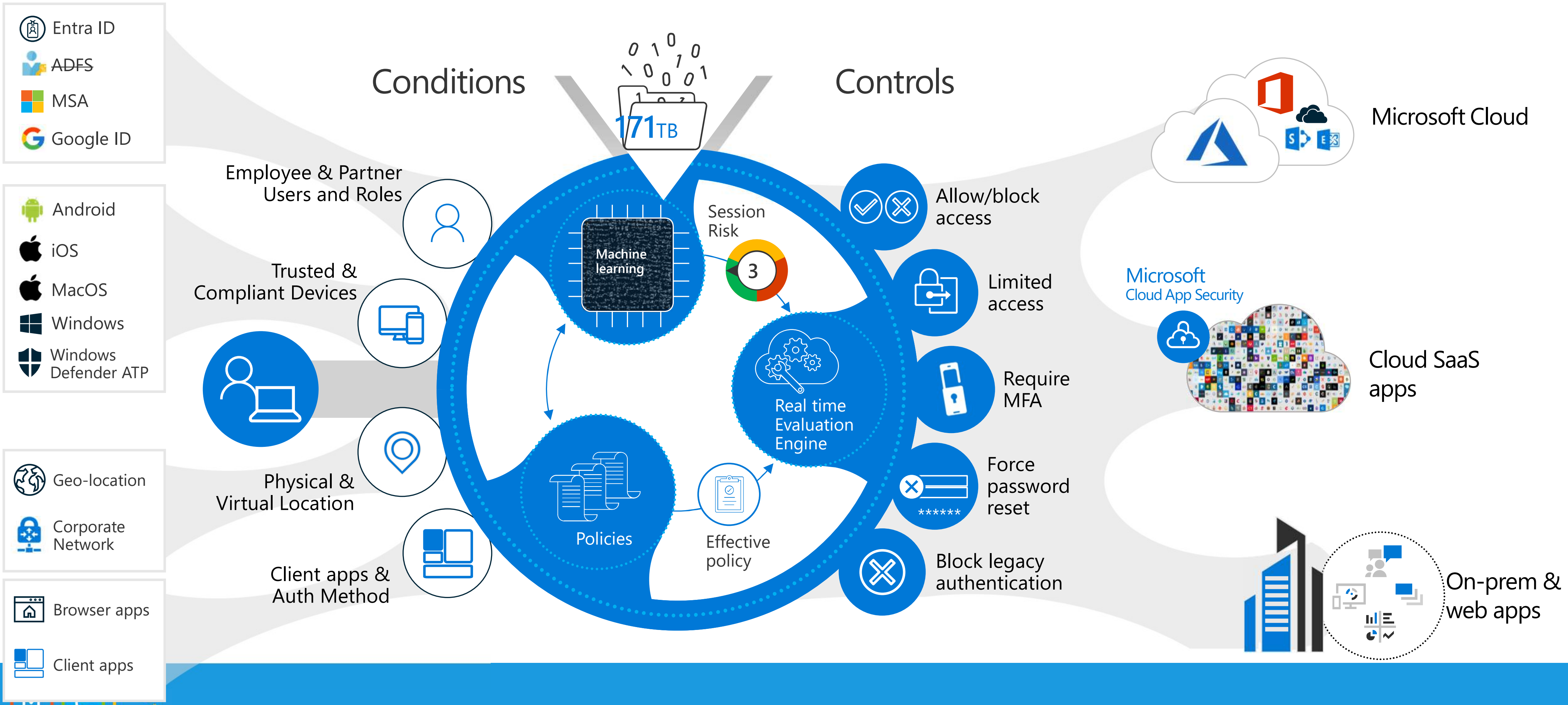
IaaS / PaaS / Datacenter

Microsoft 365

Internet

On-premises

Conditional Access



Entra ID

~~ADFS~~

MSA

Google ID

Android

iOS

MacOS

Windows

Windows Defender ATP

Geo-location

Corporate Network

Browser apps

Client apps

Conditions

Employee & Partner Users and Roles

Trusted & Compliant Devices

Physical & Virtual Location

Client apps & Auth Method

0 1 0 0 1 0 0 1 0 1 0 1 0 1

171TB

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow/block access

Limited access

Require MFA

Force password reset

******

Block legacy authentication

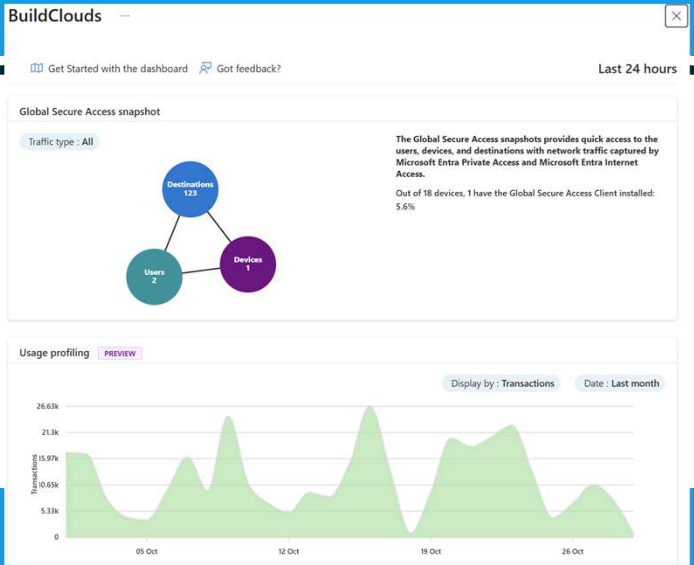
Microsoft Cloud

Microsoft Cloud App Security

Cloud SaaS apps

On-prem & web apps

Private Access



BuildClouds

Get Started with the dashboard Got feedback? Last 24 hours

Global Secure Access snapshot

Traffic type : All

The Global Secure Access snapshots provides quick access to the users, devices, and destinations with network traffic captured by Microsoft Entra Private Access and Microsoft Entra Internet Access.

Out of 18 devices, 1 have the Global Secure Access Client installed: 5.6%

Usage profiling PREVIEW

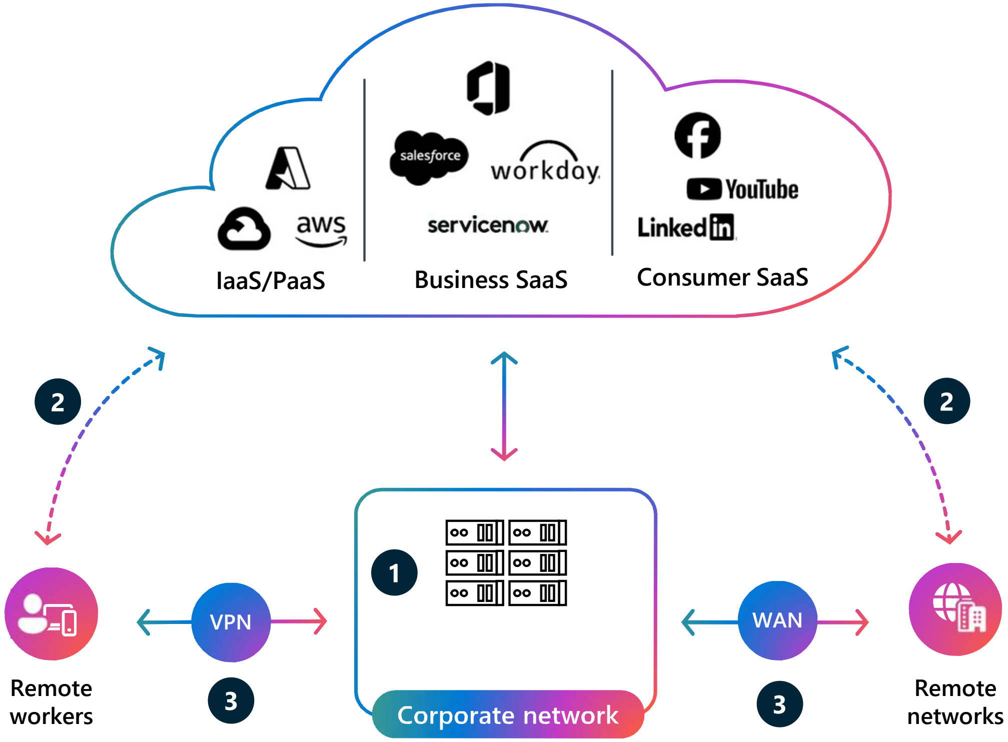
Display by : Transactions Date : Last month

Legacy network security stacks are no longer sufficient

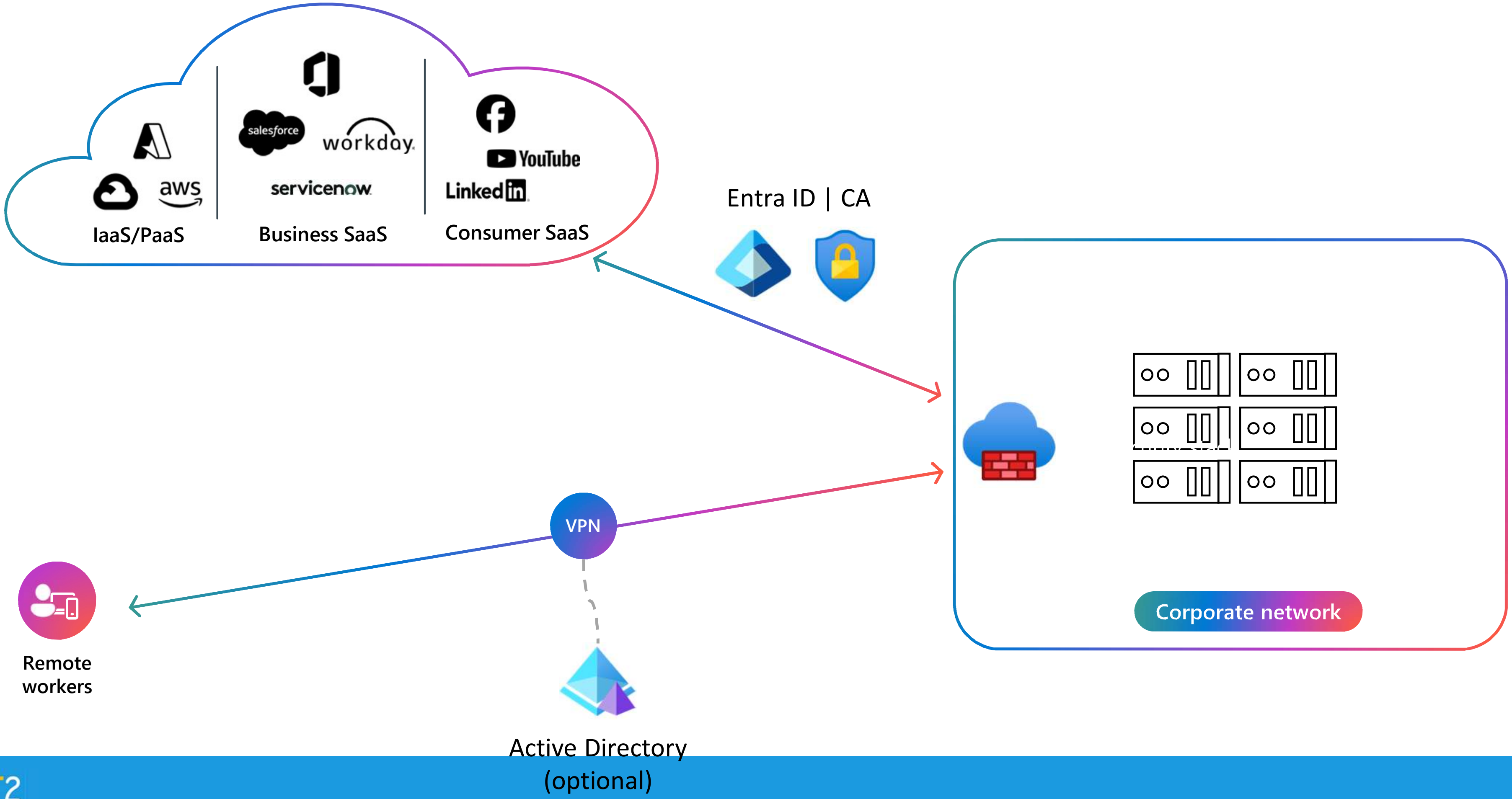
1 Dramatic traffic increase strains network capacity and on-prem security stack. Sub-optimal user experience on account of traffic hair-pinning.

2 Users circumvent IT controls and access resources directly.

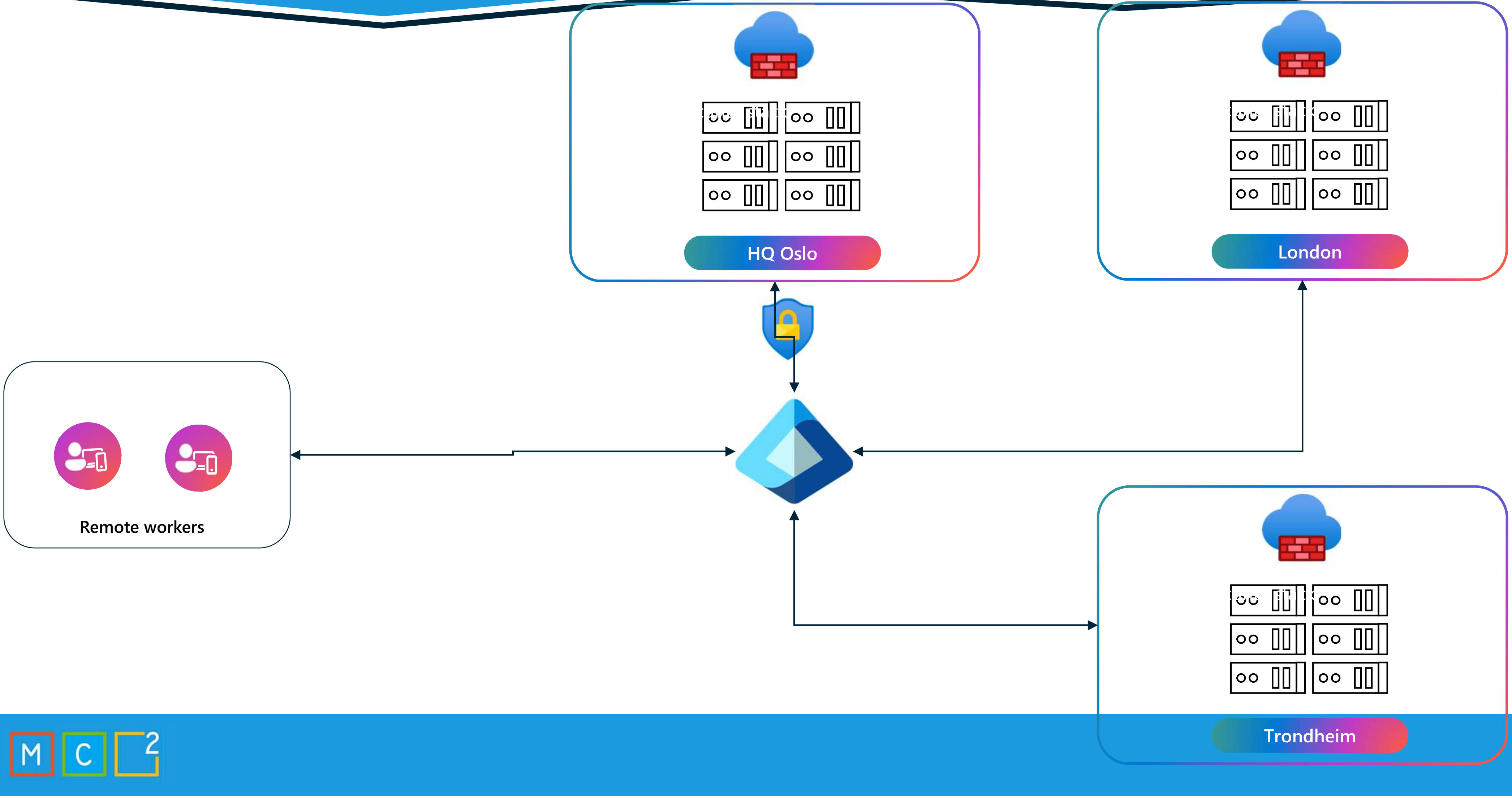
3 Compromised users/devices can move laterally on traditional corporate networks.



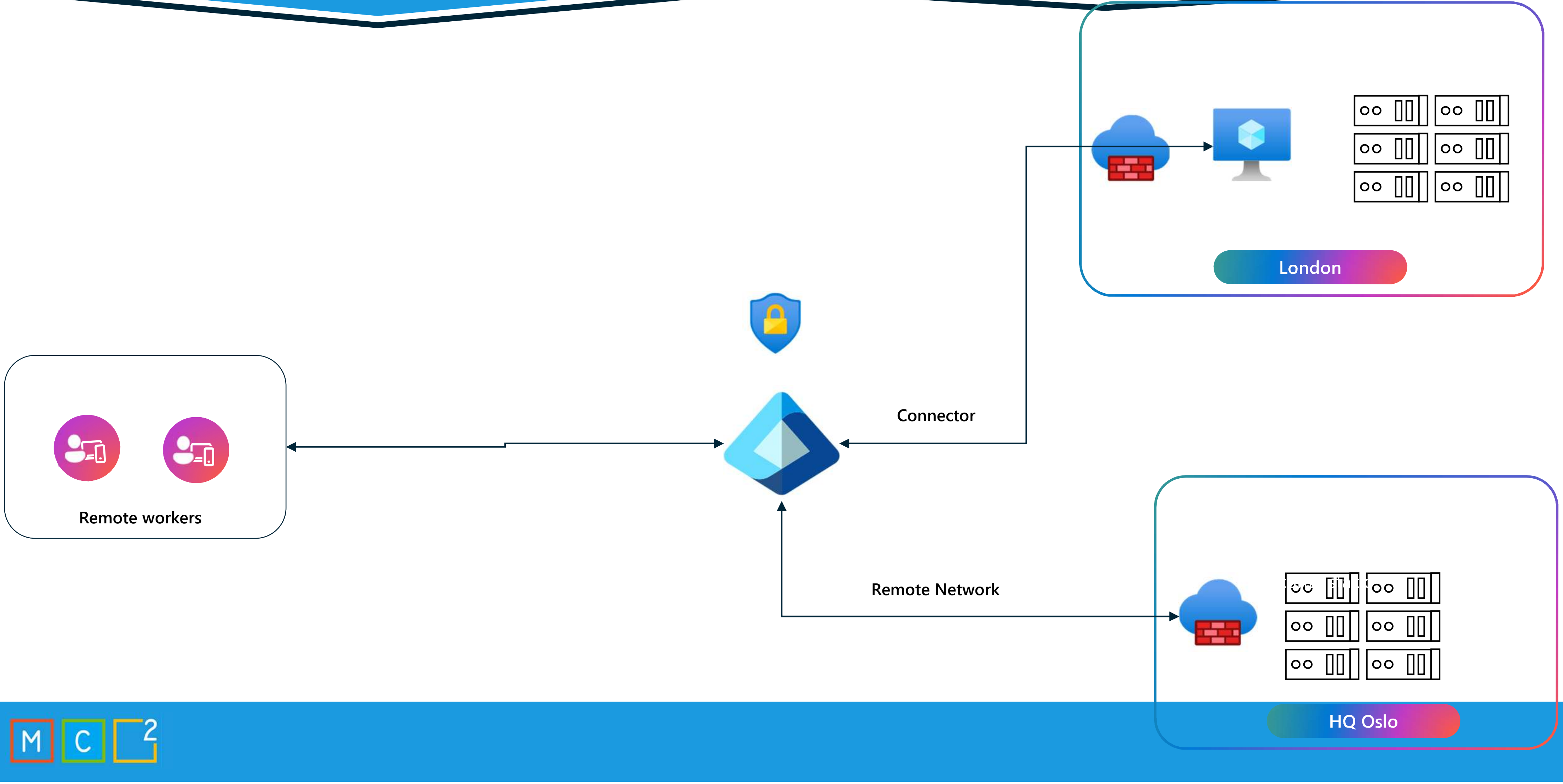
Classic VPN


salesforce
workday.
servicenow
YouTube
LinkedIn
aws
IaaS/PaaS
Business SaaS
Consumer SaaS
Entra ID | CA
VPN
Remote workers
Active Directory (optional)
Corporate network

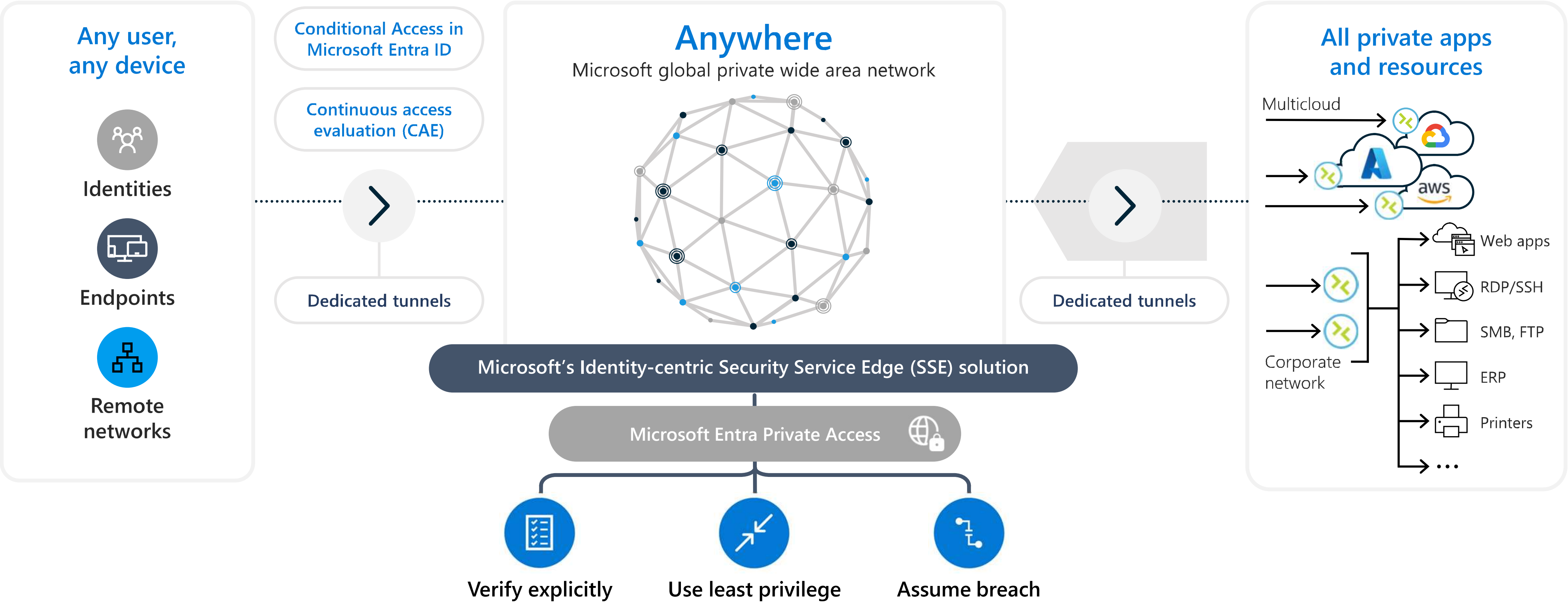
Private Access



Connect ressources via Private Access



Entra Private Access
An identity-centric Zero Trust Network 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

Multicloud

Corporate network

Web apps

RDP/SSH

SMB, FTP

ERP

Printers

…

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

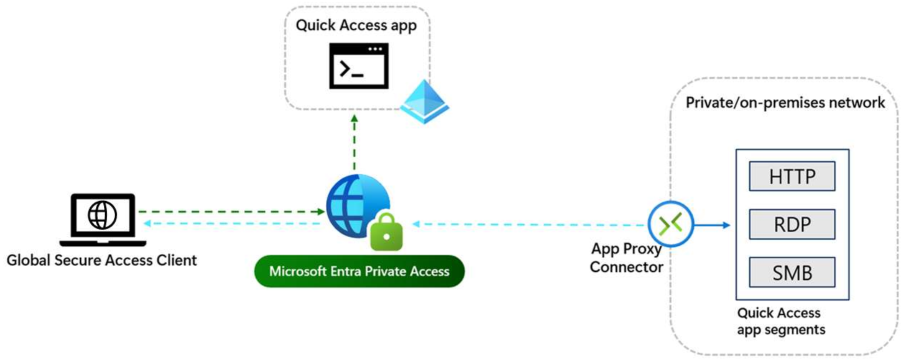
Microsoft Entra Private Access

Verify explicitly

Use least privilege

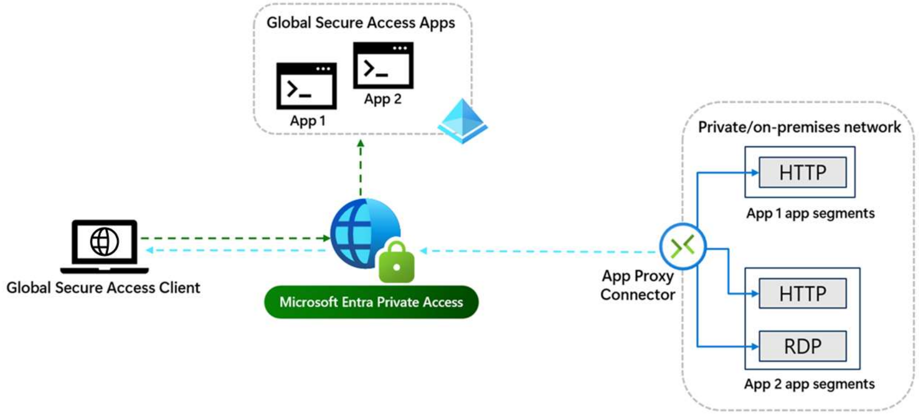
Assume breach

Quick Access app


Quick Access app
Private/on-premises network
HTTP
RDP
SMB
Quick Access app segments
Global Secure Access Client
Microsoft Entra Private Access
App Proxy Connector

- primary group of FQDNs and IP addresses that should be always available
- Like as baseline for GSA connectivity

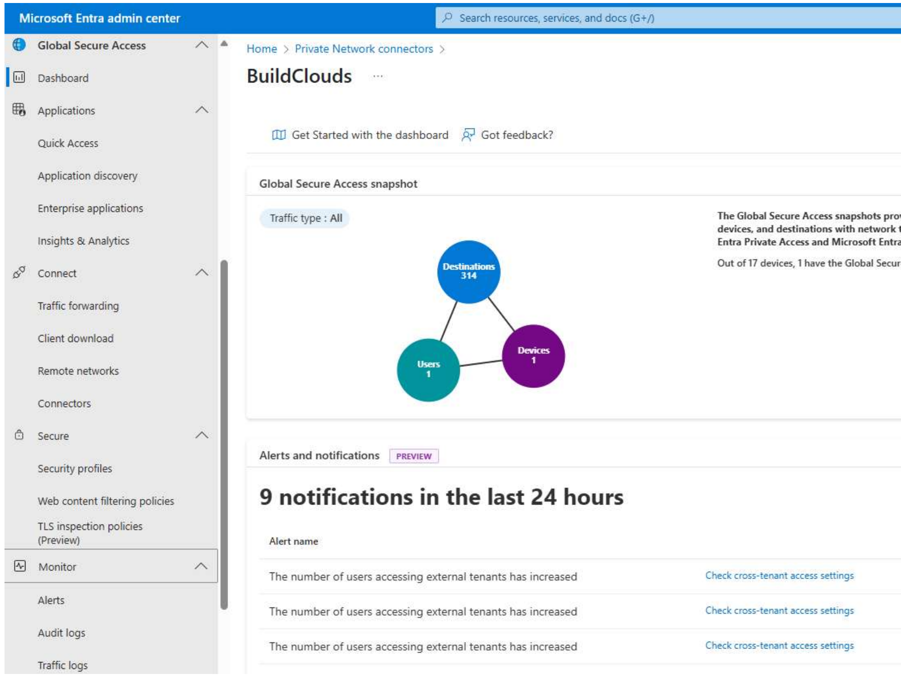
Global Secure Access app


Global Secure Access Apps
App 1
App 2
Private/on-premises network
HTTP
App 1 app segments
HTTP
RDP
App 2 app segments
Global Secure Access Client
Microsoft Entra Private Access
App Proxy Connector

- when different CA Policies are required
- for connectivity for a subset of users

Demo

Global Secure Access



Global Secure Access snapshot

The Global Secure Access snapshots pro
devices, and destinations with network t
Entra Private Access and Microsoft Entra

Out of 17 devices, 1 have the Global Secur

Alerts and notifications

9 notifications in the last 24 hours

Alert name	
The number of users accessing external tenants has increased	Check cross-tenant access settings
The number of users accessing external tenants has increased	Check cross-tenant access settings
The number of users accessing external tenants has increased	Check cross-tenant access settings

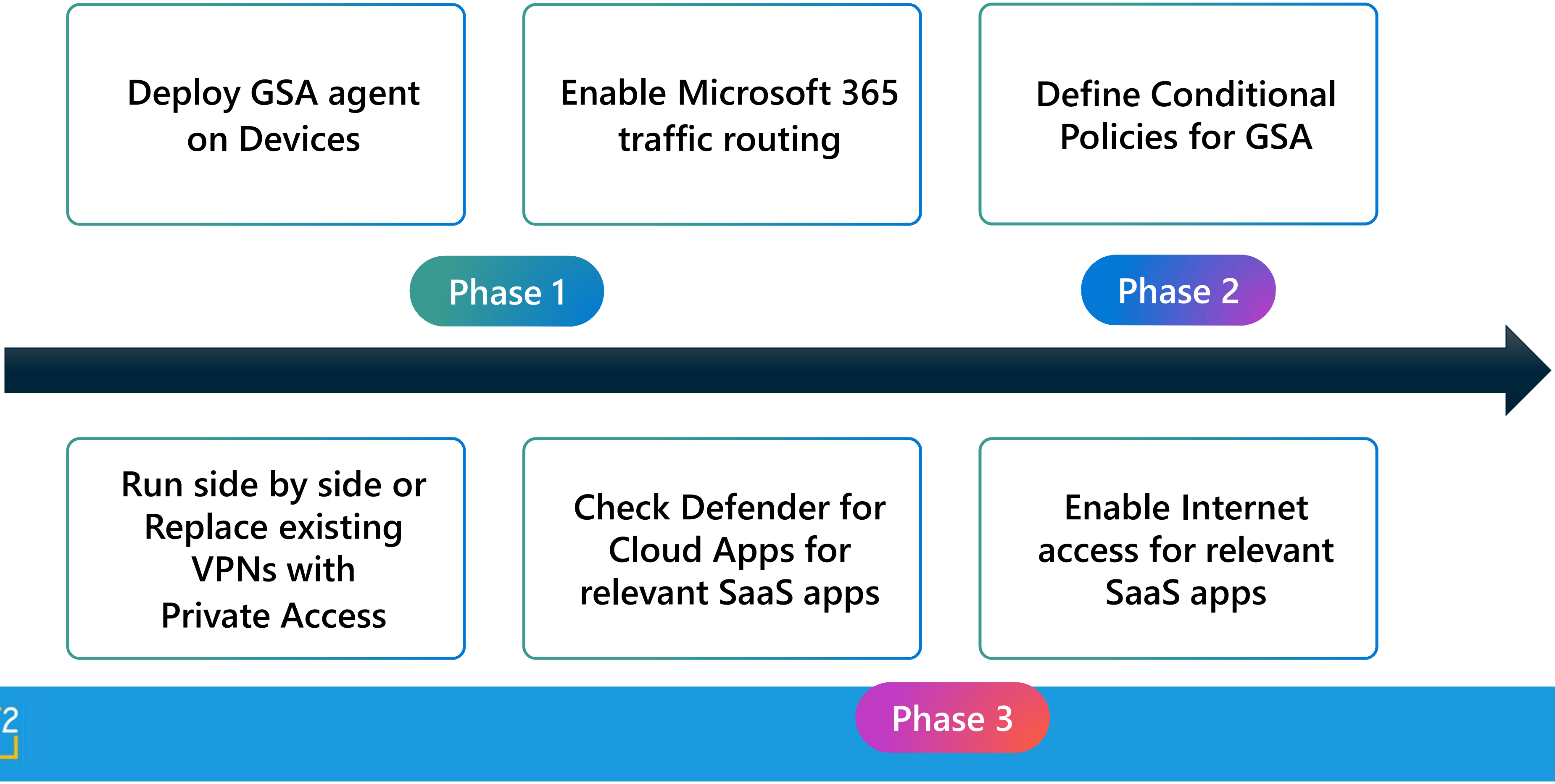
Private Network Connector

- Lightweight agents on a Windows server inside the network
- Create connections to Entra
- Needs open 80 and 443 to Entra
- Minimum of one connector needed
- 2 recommended for Highavailablity
- Connectors can add and remove any time
- Get automatic updates

Conditional Access

- Use additional CA-Policies for GSA
- Think on Network conditions for GSA
- If you have Tiering enable strength auth for accessing
- Please think on a clear naming concept for Conditional Access and GSA policies

GSA Rollout



Deploy GSA agent on Devices

Enable Microsoft 365 traffic routing

Define Conditional Policies for GSA

Phase 1

Phase 2

Run side by side or Replace existing VPNs with Private Access

Check Defender for Cloud Apps for relevant SaaS apps

Enable Internet access for relevant SaaS apps

Phase 3

Pricing

$12 PUPM
Microsoft Entra Suite pricing

Microsoft Entra Suite

- Private
- Internet Access
- ID Governance
- ID Protection
- Verified ID Premium

45%
suite discount

30 day free Trial is available per Service

$22 PUPM
Value of components

1. Private Access	$5 pupm
+	
2. Internet Access	$5 pupm
+	
3. ID Governance[1]	$7 pupm
+	
4. ID ction[2]	$3 pupm
+	
5. Verified ID[3] Premium	$2 pupm

Microsoft Entra ID Plan 1 is a technical and licensing pre-requisite[4]

Notes: (1) Also available for Microsoft Entra ID P2 / ME5 / E5 Security customers at a discounted price; (2) Available as part of Microsoft Entra ID P2; (3) Standalone offer prices may vary; (4) Any offer that includes Microsoft Entra ID P1 (e.g., M365 E3) will also fulfill the pre-requisite requirement.

Knowledge Check (win a book) ☺

- Which three traffic profiles offers GSA?
  - Private traffic, Internet traffic and Microsoft traffic

Links

- Microsoft Cybersecurity Reference Architectures (MCRA)
- What is Global Secure Access? - Global Secure Access
- New Microsoft Entra Suite | Tech Community
- New Microsoft Entra Suite | YouTube
- Global Secure Access documentation - Global Secure Access | Microsoft Learn
- Automating Web Application Creation in Global Secure Access Using PowerShell – christianfrohn.dk
- Global Secure Access and Sentinel Integration…. and brisket? — Blog
- TLS Inspection in Microsoft Entra GSA Internet Access – Complete Configuration Guide
- Entra ID – New version of Entra ID Private Network Connector
- Global Secure Access | Chris Brumm's Blog
- Known Limitations for Global Secure Access - Global Secure Access | Microsoft Learn
- …

Session feedback available in home feed of the app after the session

run events

THANK YOU