Microsoft Entra. Zgolj novo ime za Azure Active Directory?

Slavko Kukrika
(Slavko.Kukrika@Outlook.com)
MCT in prijazen fant

Agenda

➡️ Azure AD is renamed to Microsoft Entra ID

➡️ What is Microsoft Entra?

➡️ Microsoft Entra ID main features

➡️ Overview of other Microsoft Entra solutions

➡️ Questions & Answers

Azure Active Directory highlights

Over **100** datacenters across the planet
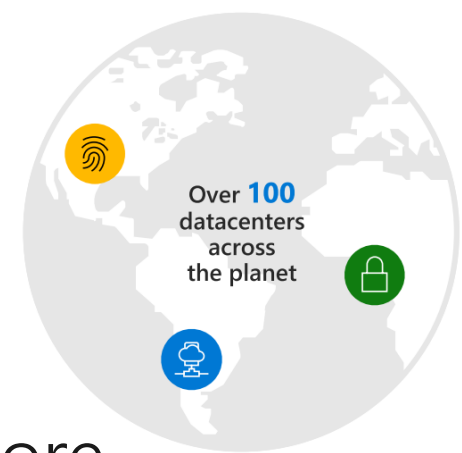
Released on October 28th 2008

Identity service for Azure, Microsoft 365, Intune and many more

Cloud service – no on-premises infrastructure needed

 Global scale, reliability and 99,99% SLA availability

 Can be synchronized with Active Directory

99.99%
New Azure AD
Service Level Agreement
(in effect from April 1st, 2021)

Can be used for device management – Windows, Android and iOS

720K+
Organizations
Using Azure AD

425M+
Azure AD
Monthly active users

30B+
Azure AD
Daily authentication requests

Azure AD is renamed to Microsoft Entra ID

Same capabilities.

Continue to use or deploy with zero interruptions.

All existing deployments, configurations and integrations continue to function.

Continue to access via Azure portal, M365 admin center, or Microsoft Entra admin center.

Same login URLs, APIs, PowerShell cmdlets, Microsoft authentication libraries (MSAL).

Same developer experience.

Microsoft identity platform still encompasses all identity and access developer assets.

No changes to functionality of:
Microsoft Graph
Microsoft Graph PowerShell
Windows Server Active Directory
Active Directory Federation Services
Active Directory Domain Services
Azure AD B2C

Same licensing.

Same features, pricing, terms, service level agreements, compliance certifications, support and licensing.

from...	to...
Azure AD Free	**Microsoft Entra ID Free**
Azure AD Premium P1 Also included in Microsoft 365 E3	**Microsoft Entra ID P1** Also included in Microsoft 365 E3
Azure AD Premium P2 Also included in Microsoft 365 E5	**Microsoft Entra ID P2** Also included in Microsoft 365 E5
Azure AD External Identities	**Microsoft Entra External ID**

Azure Active Directory → Microsoft Entra ID

Azure AD Conditional Access → Microsoft Entra Conditional Access

Azure AD tenant → Microsoft Entra tenant

Azure AD joined → Microsoft Entra joined

Azure AD registered → Microsoft Entra registered

Hybrid Azure AD joined → Microsoft Entra hybrid joined

Azure AD Connect → Microsoft Entra Connect

Microsoft Entra ID features

Groups with assigned and dynamic membership

Administrative units

Self-Service Password Reset

Multi-factor and passwordless authentication

Device compliance (with Microsoft Intune)

Synchronization with on-premises Active Directory

Conditional access

Policy Conditions

User
- ○ User identity
- ○ Group membership
- ⚠ Session Risk

Device
- ○ OS Platform
- ○ Is Compliant / Domain joined
- ○ Is lost or stolen
- ⚠ Device Risk

App
- ○ Mobile or Cloud app
- ○ Per app policy

Location
- ○ IP range
- ○ Country / Region

Microsoft Entra Identity Protection

Windows Defender
Lookout
Skycure

Policy Controls

Access Control
- ✓ Allow sign-in
- ✗ Block sign-in
- Enforce MFA
- Terms of Use
- Partners

Session Restrictions
- Restrict download
- Disable print
- Prevent data leak

Applications

Microsoft Cloud
Microsoft Azure
Office 365

3rd Party SaaS Apps
box now

On Premises Apps

Demo
Managing dynamic group
Active Directory sync
Conditional access

Microsoft Entra

Identity & access management

- Microsoft Entra ID
- Microsoft Entra ID Governance
- Microsoft Entra External ID

New identity categories

- Microsoft Entra Verified ID
- Microsoft Entra Permissions Management
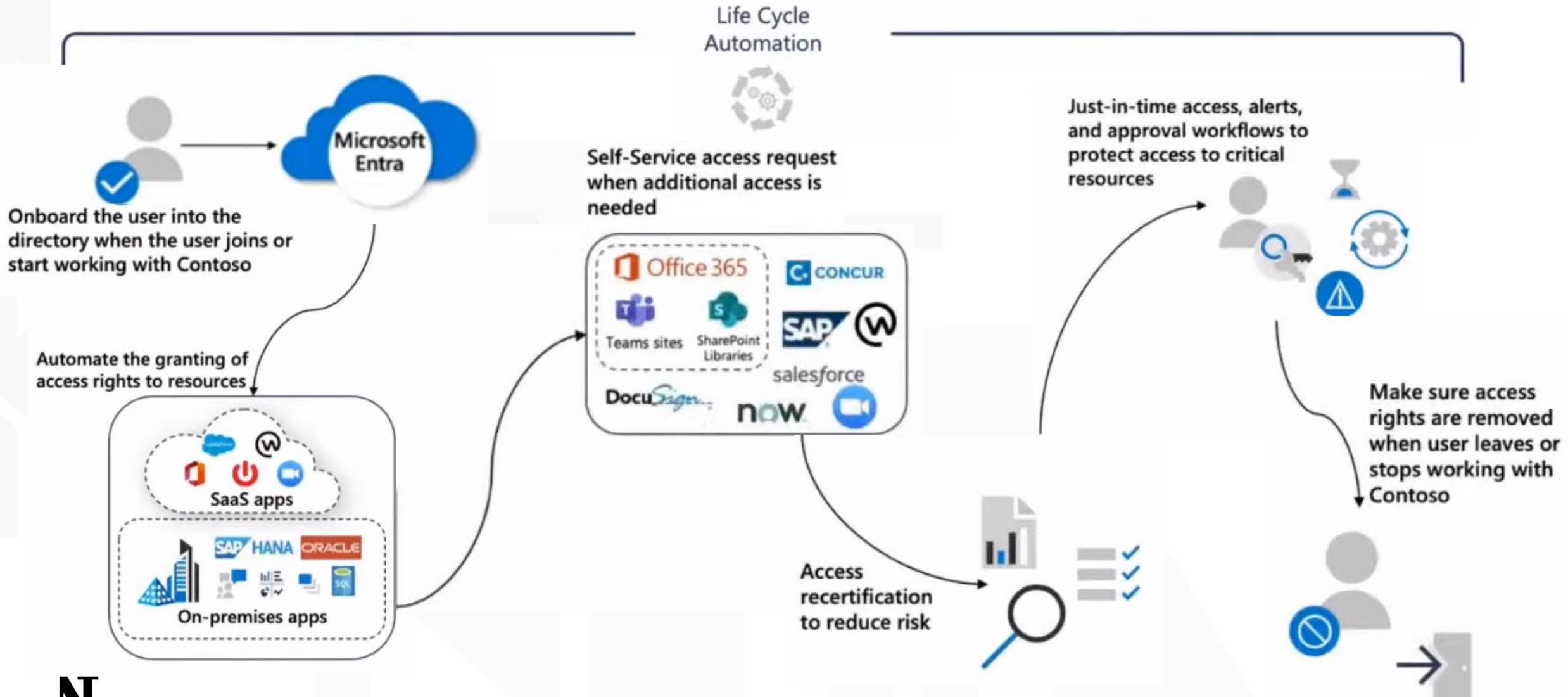- Microsoft Entra Workload ID

Network access
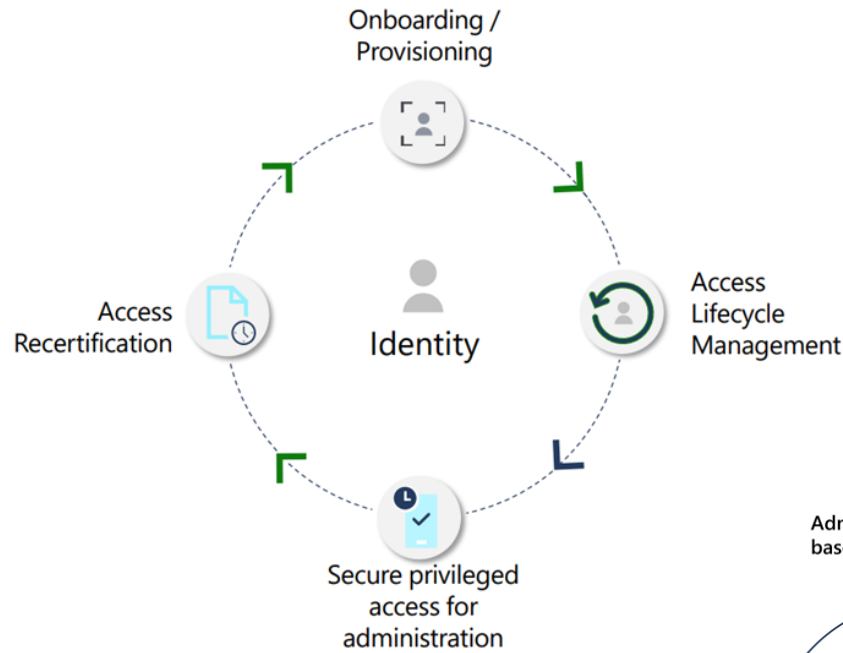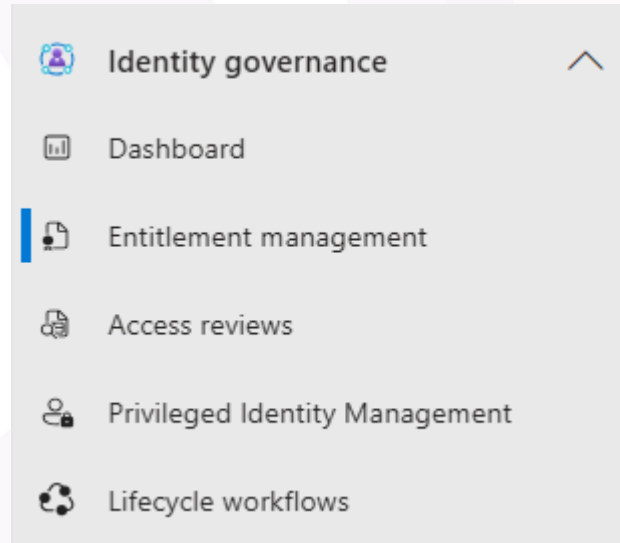
- Microsoft Entra Internet Access
- Microsoft Entra Private Access

Microsoft Entra ID Governance

Life Cycle Automation

Onboard the user into the directory when the user joins or start working with Contoso

Automate the granting of access rights to resources

SaaS apps

On-premises apps

Self-Service access request when additional access is needed

Office 365

CONCUR

Teams sites

SharePoint Libraries

SAP

salesforce

DocuSign

now

Just-in-time access, alerts, and approval workflows to protect access to critical resources

Make sure access rights are removed when user leaves or stops working with Contoso

Access recertification to reduce risk

Microsoft Entra ID Governance

Identity governance
- Dashboard
- Entitlement management
- Access reviews
- Privileged Identity Management
- Lifecycle workflows

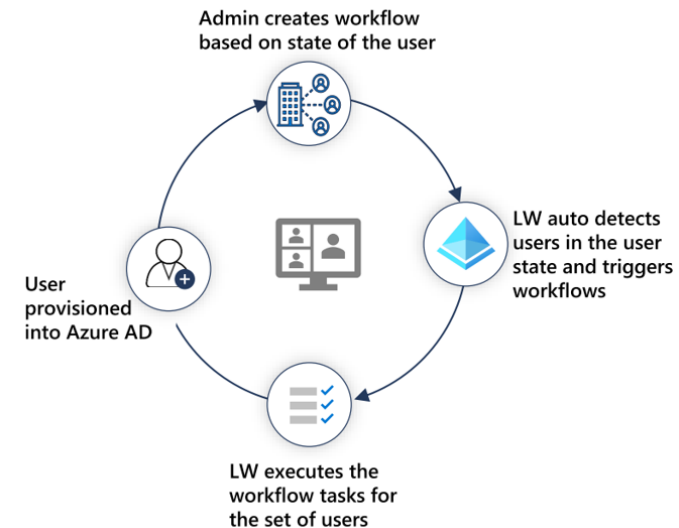**01** Who has/should have access to which resources?

02 What are they doing with that access?

03 Are there effective organizational controls for managing access?

04 Can auditors verify that the controls are working?

Onboarding / Provisioning

Access Recertification

Identity

Access Lifecycle Management

Secure privileged access for administration

Report status to admin

Request sent to users and resource owners

Remove stale memberships

Access Reviews

Review current memberships

Confirm which memberships to keep

Admin creates workflow based on state of the user

User provisioned into Azure AD

LW auto detects users in the user state and triggers workflows

LW executes the workflow tasks for the set of users

#ntk23

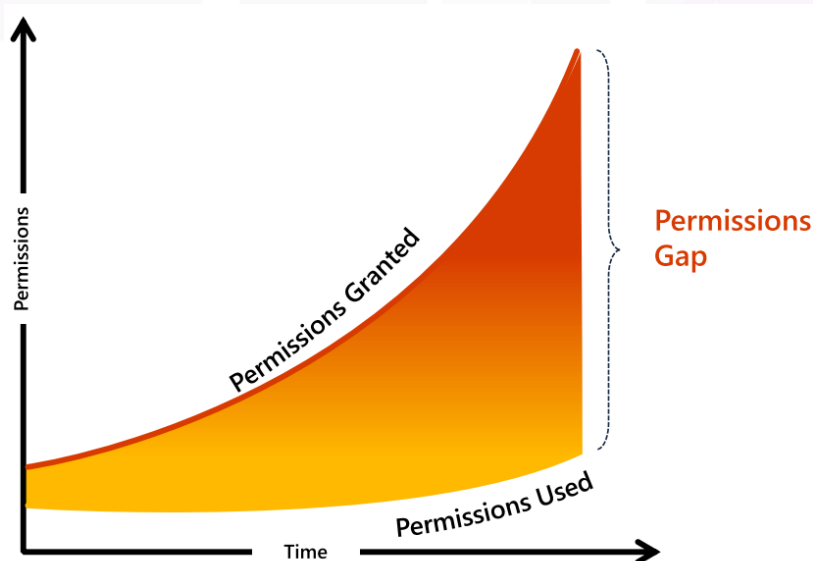# Microsoft Entra Permissions Management

Multicloud adoption brings new permission challenges

Exponential growth of identities, machines, functions and scripts in the cloud infrastructure

>90% of identities are using <5% of permissions granted

>50% of permissions are high-risk and can cause catastrophic damage

Cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into assigned permissions

Permissions

Permissions Gap

Permissions Granted

Permissions Used

Time

Grants permissions based on historical usage and activity

Allow temporary access to high-risk permissions on-demand

Continuously monitor and right-size identities to prevent privilege creep

#ntk23

Microsoft Entra Permissions Management

Discover & Assess

Permission Creep Index - gap between granted and used permissions

Usage analytics – uncover every action performed by any identity on any resource

Remediate & Manage

Remove unused and excessive permissions and create new policies / roles

Use least privilege derived templates to enforce Just-In-Time access

Grant permissions on-demand for a time-limited period or on an as-needed basis

Monitor & Alert

Track permissions usage patterns and with customizable alerts

Strengthen security posture with machine learning-based anomaly detections

Generate detailed reports and cyber kill chain analysis to speed up threat investigation

Discover ⟶ Remediate ⟶ Monitor

Demo
Microsoft Entra ID Governance
Microsoft Entra Permissions Management

Microsoft Entra Workload ID

Workload identity is assigned to a workload (such as an application, service, script, or container) to authenticate and access other resources
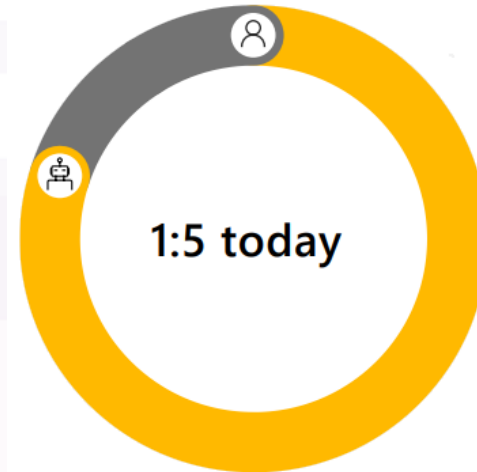
Applications

Service principals

Managed identities

Workload identity characteristics

No formal lifecycle process

Can be configured with multiple credentials
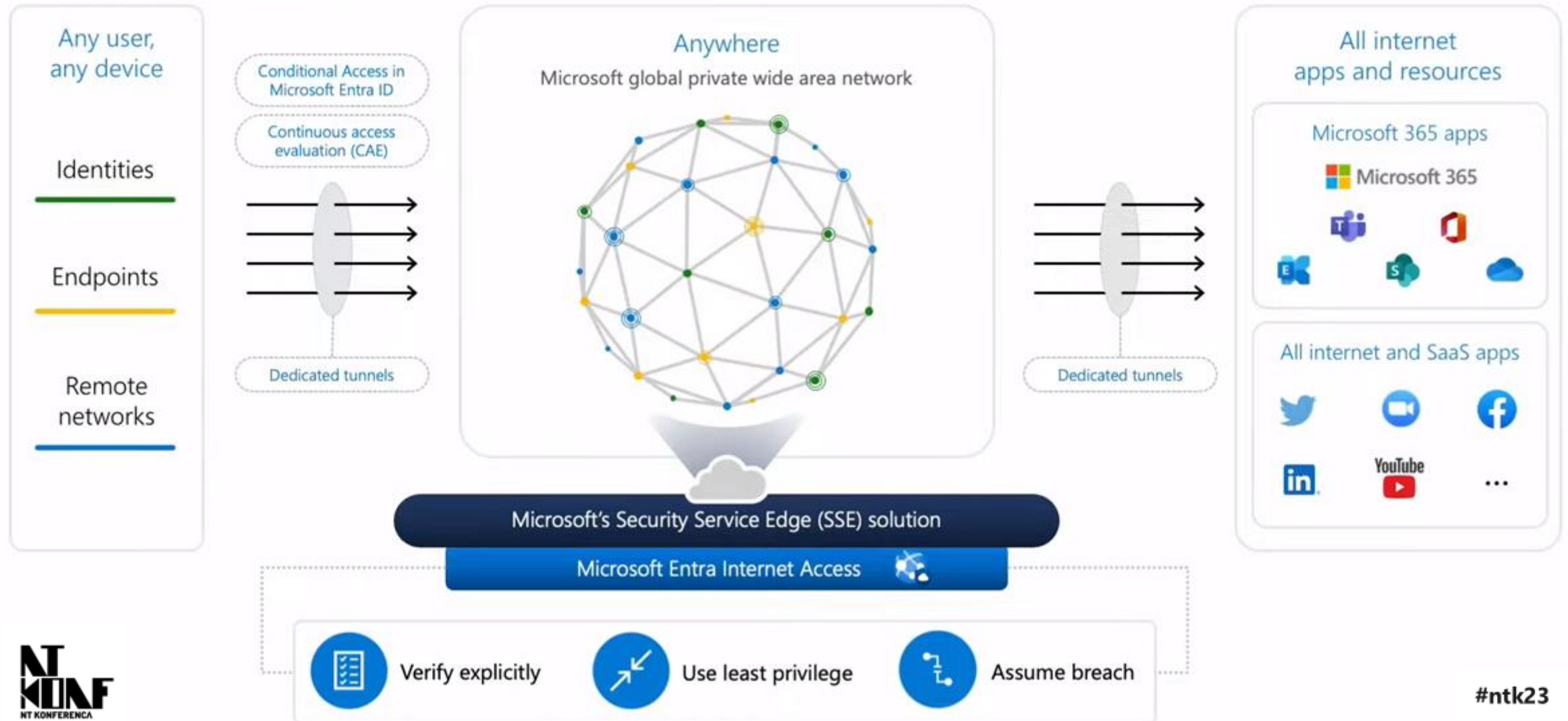
May have multiple identities

1:5 today
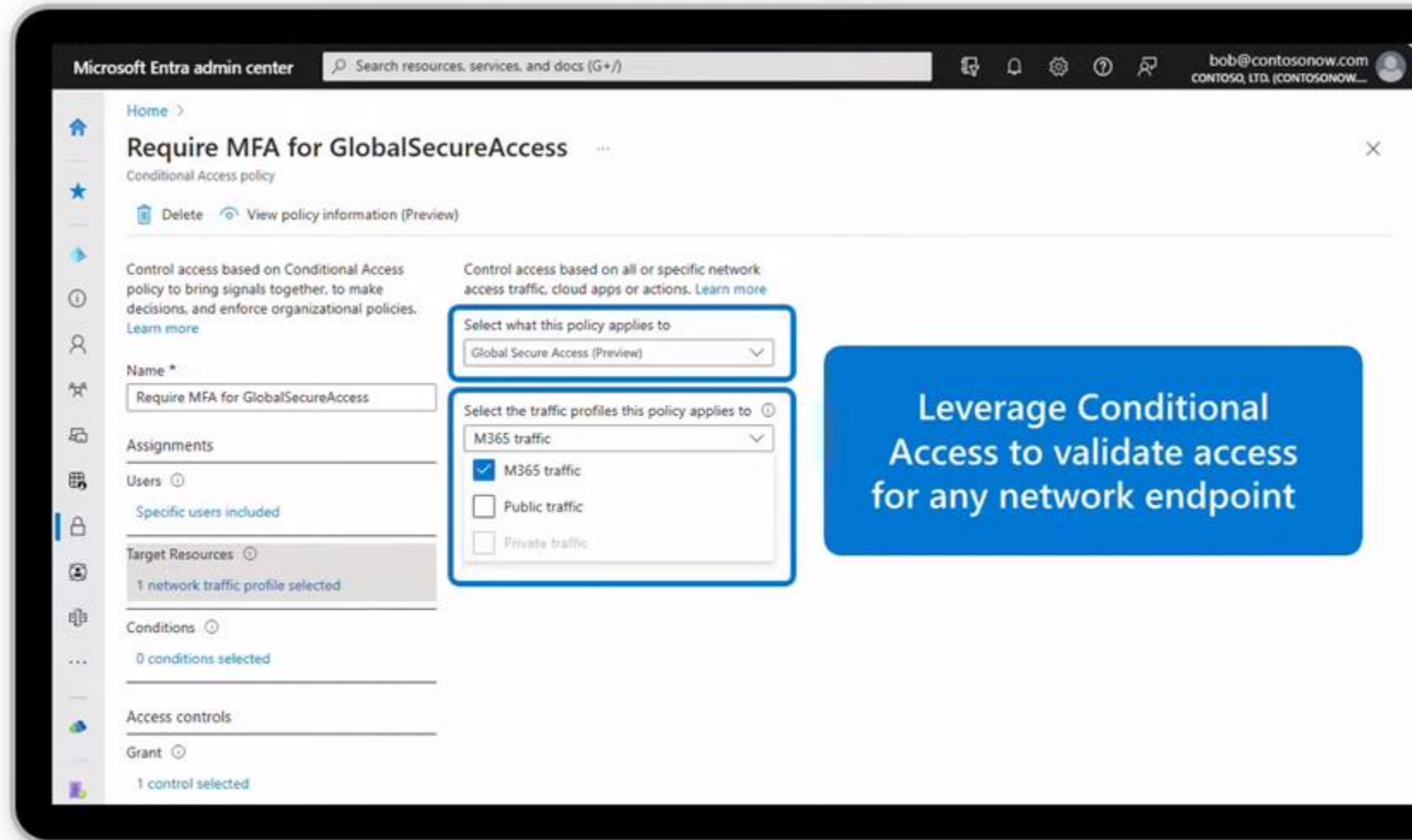
1:20 in five years

User identity   Workload identity
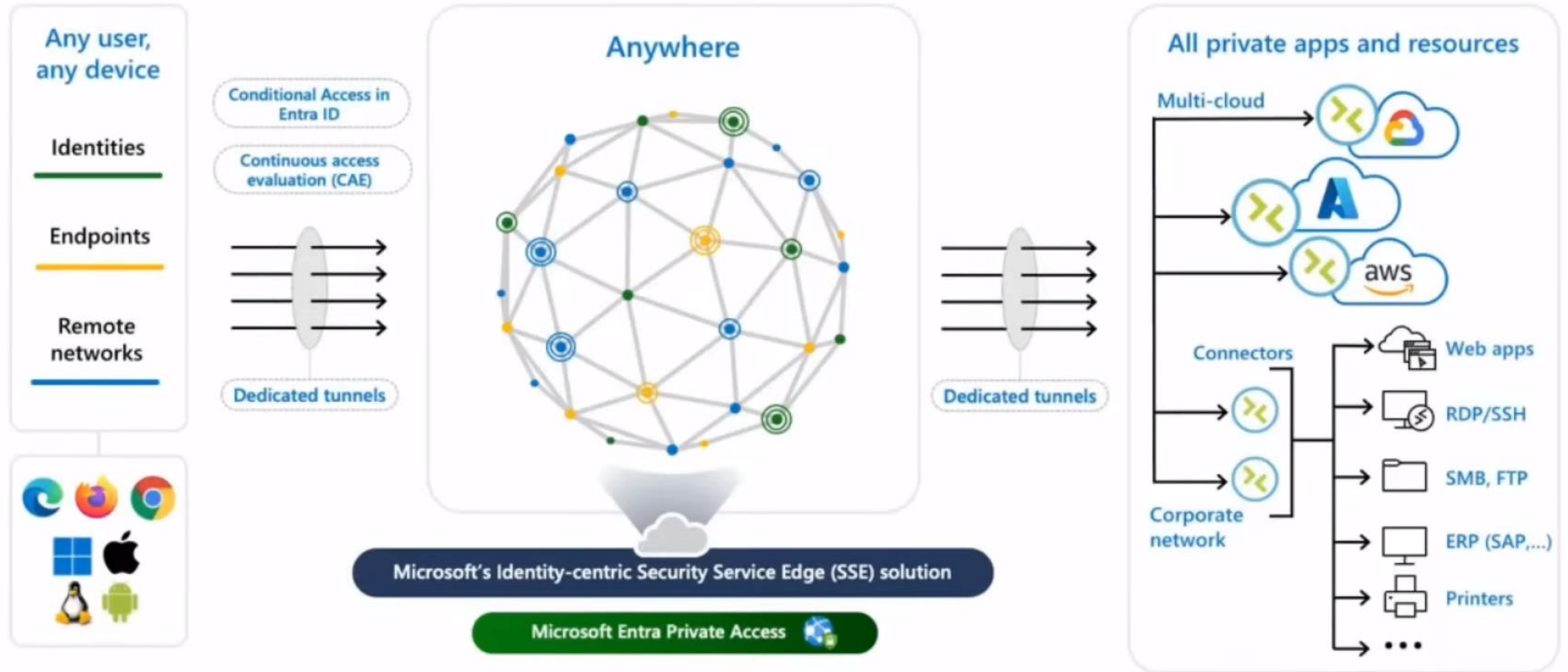
Microsoft Entra Internet Access
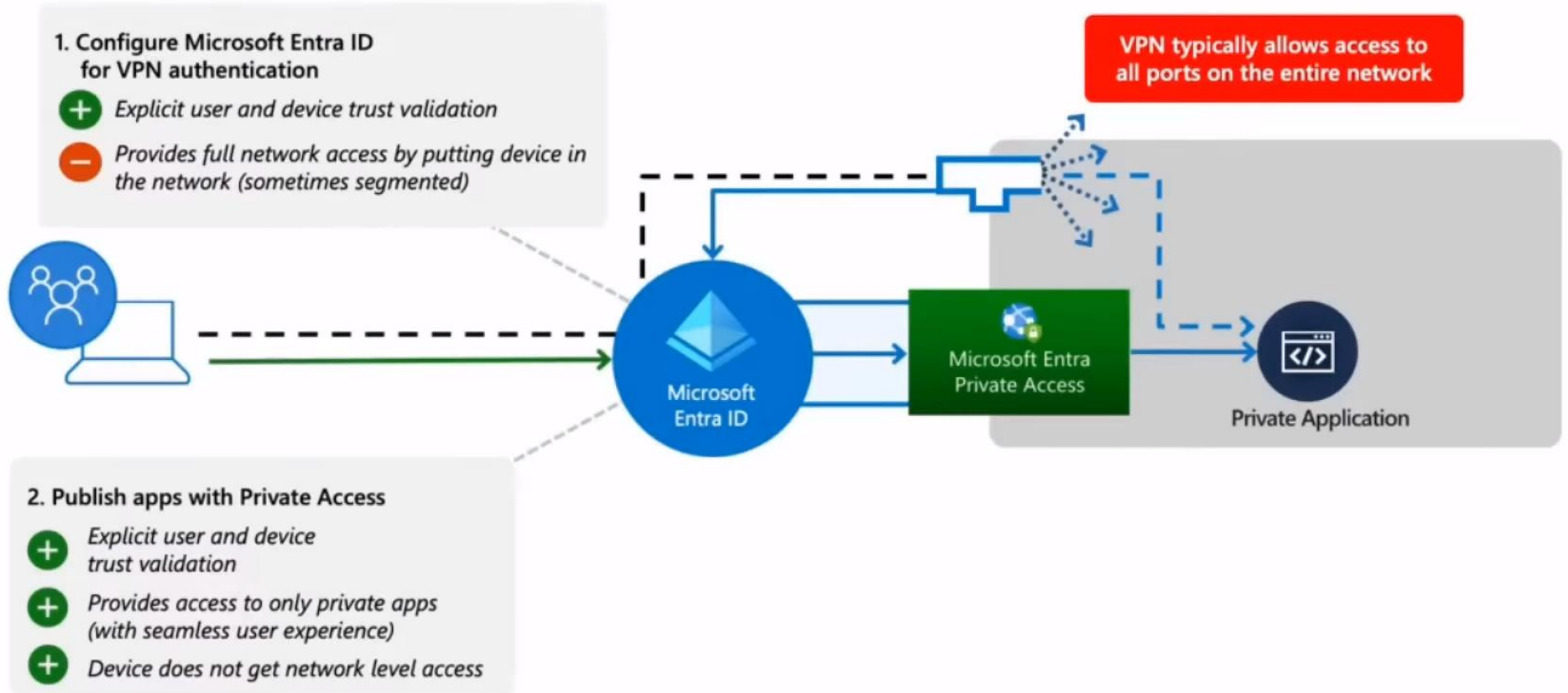
Universal Conditional Access

» **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**

» **Coming Soon:** Continuous access evaluation to instantaneously revoke access on changing conditions

Microsoft Entra Private Access

#ntk23

Microsoft Entra Private Access – Move Beyond VPN

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

#ntk23

How does it work?

Microsoft Azure

Microsoft Entra Application Proxy Service

Request/Response Queue

https://app.contoso.com

On-Premises Network

Connector

Connector

Expense App

Benefits App

#ntk23

Summary

Microsoft Entra ID is new name for Azure Active Directory (Azure AD)

Microsoft Entra ID has the same features, licensing, ... as Azure AD

  Microsoft Entra admin center

  Name is/will be updated in the GUI in the following months

Microsoft Entra product family includes multiple products

  Microsoft Entra ID

  Microsoft Entra External ID

  Microsoft Entra Permissions Management

  Microsoft Entra ID Governance

  Microsoft Entra Verified ID

  Microsoft Entra Workload ID

  Microsoft Entra Internet Access

  Microsoft Entra Private Access

Identity centric security service edge (SSE)

Additional information

New name for Azure Active Directory

https://aka.ms/rename, https://aka.ms/AADRebrandFAQ

Meet Microsoft Entra

https://go.Microsoft.com/fwlink/?linkid=2237754

Microsoft Entra Documentation

https://learn.microsoft.com/entra/

Microsoft Entra Tech Accelerator: technical skilling on demand

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/microsoft-entra-tech-accelerator-technical-skilling-on-demand/ba-p/2520433

What's Microsoft Entra Permissions Management?

https://learn.microsoft.com/azure/active-directory/cloud-infrastructure-entitlement-management/overview

Questions?

Slavko.Kukrika@Outlook.com

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ

This is not school, but we love to get grades. Please fill out our questoineers and leave us your feedback. You may even win some cool rewards.