

Microsoft Entra

Azure Architects Connect

31.01.2024



Your Microsoft Entra Nerds



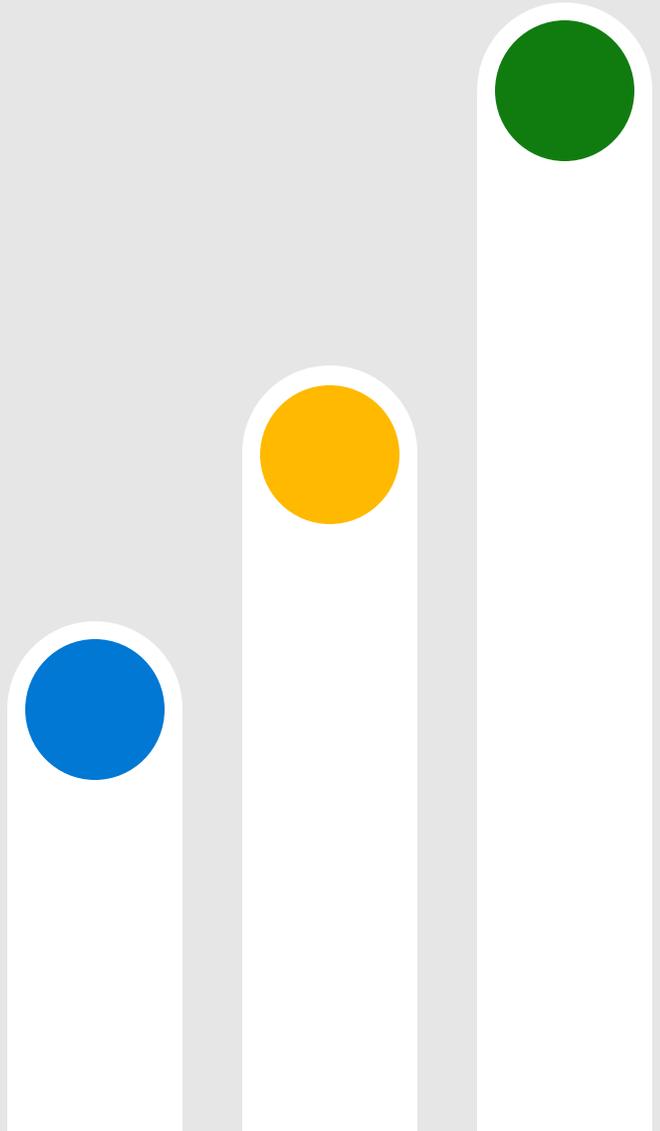
Jacqueline Herzog
Cloud Solution Architect
Security, Compliance & Identity
Microsoft



Yusuf Dikmenoglu
Cloud Solution Architect
Security, Compliance & Identity
Microsoft

Agenda

- Einführung in die Microsoft Entra Suite
- Neuigkeiten rund um Microsoft Entra
- Einblick in die Microsoft Secure Service Edge (SSE) Lösung
- Q & A



Einführung in die Microsoft Entra Suite

Today's identity and access challenges demand a holistic solution



Accelerated growth of identities and apps, on and off the corporate network, requiring secure, user-friendly access



Massive rise in identity cyberattacks—more than 4,000 password cyberattacks per second¹—increasing risk of compromised accounts

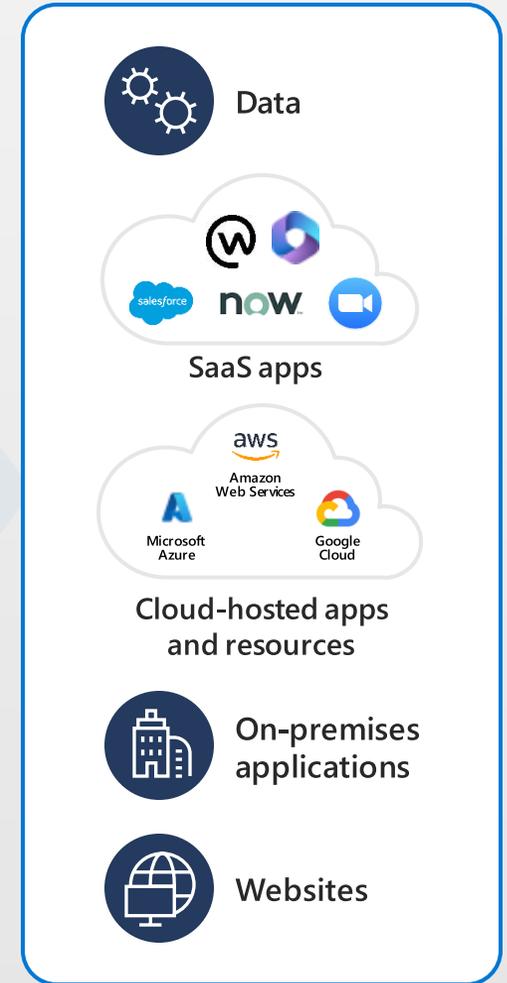
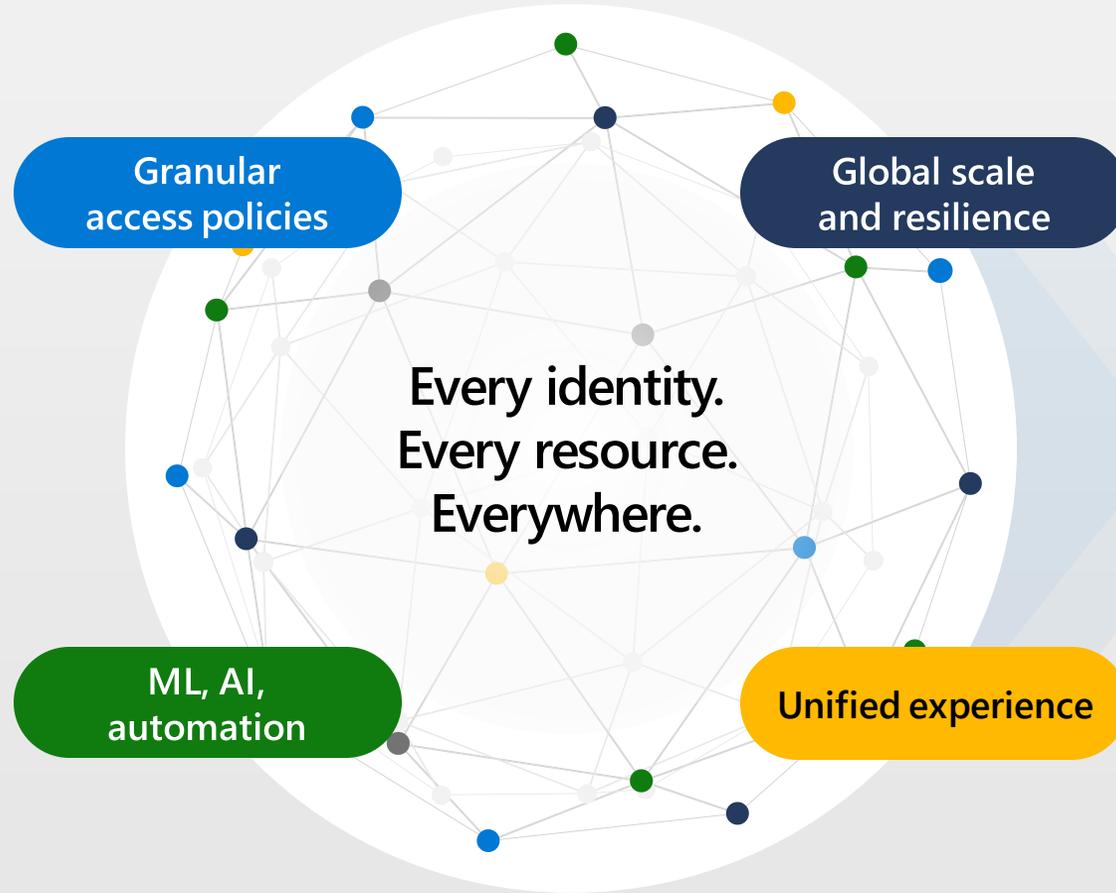


Evolving regulations and compliance requirements for protecting identities and auditing access rights

¹Microsoft Entra expands into Security Service Edge and Microsoft Entra ID becomes Microsoft Entra ID and Microsoft Security Blog

Microsoft Entra

Secure access for a connected world



Powered by trillions of security signals

Microsoft Entra product family

Secure access for a connected world

**Identity
and access
management**

Microsoft Entra ID
(formerly Azure AD)

Microsoft Entra
ID Governance

Microsoft Entra
External ID

**New
identity
categories**

Microsoft Entra
Verified ID

Microsoft Entra
Permissions
Management

Microsoft Entra
Workload ID

Microsoft Entra
Internet Access

Microsoft Entra
Private Access

Network access



Microsoft Entra product family

Secure access for a connected world

Identity and access management

Microsoft Entra ID
(formerly Azure AD)

Microsoft Entra ID Governance

Microsoft Entra External ID

Microsoft Entra Verified ID

Microsoft Entra Permissions Management

Microsoft Entra Workload ID

New identity categories

Microsoft Entra Internet Access

Microsoft Entra Private Access

Network access





Microsoft Entra ID

Go to section >>

Help organizations protect access to resources and data using strong authentication and real-time, risk-based adaptive access policies without compromising user experience



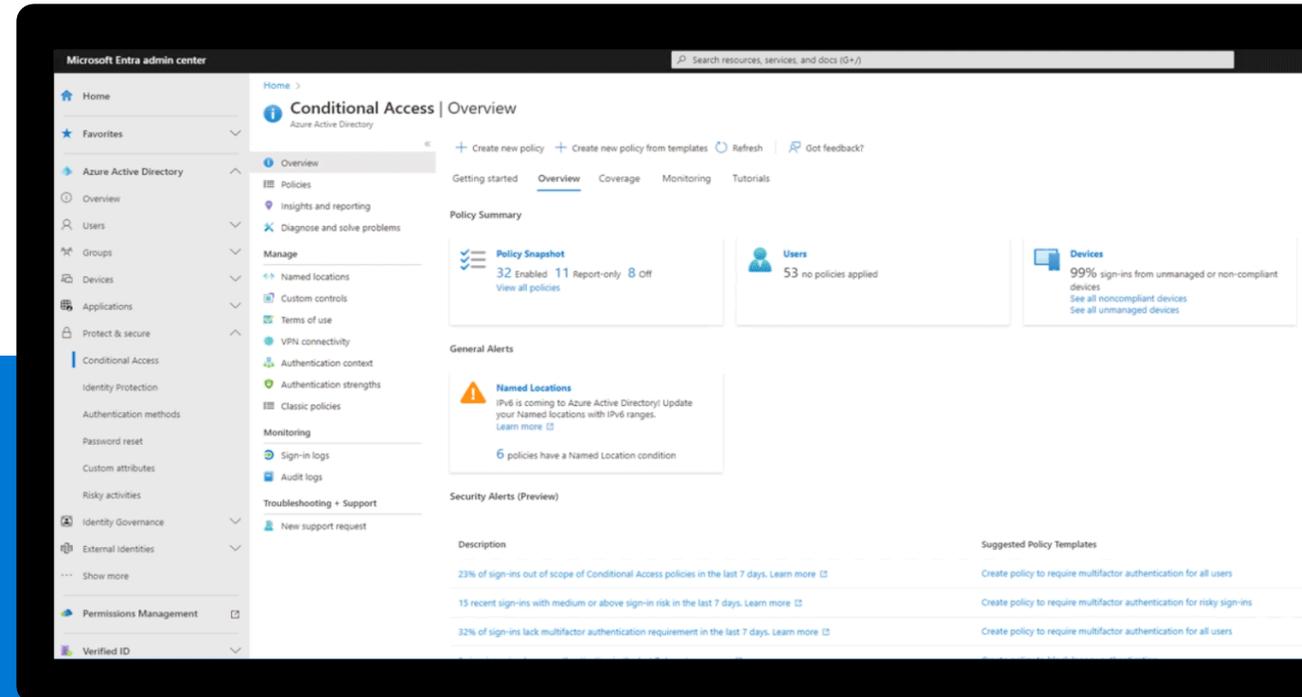
Secure adaptive access



Seamless user experiences



Unified identity management



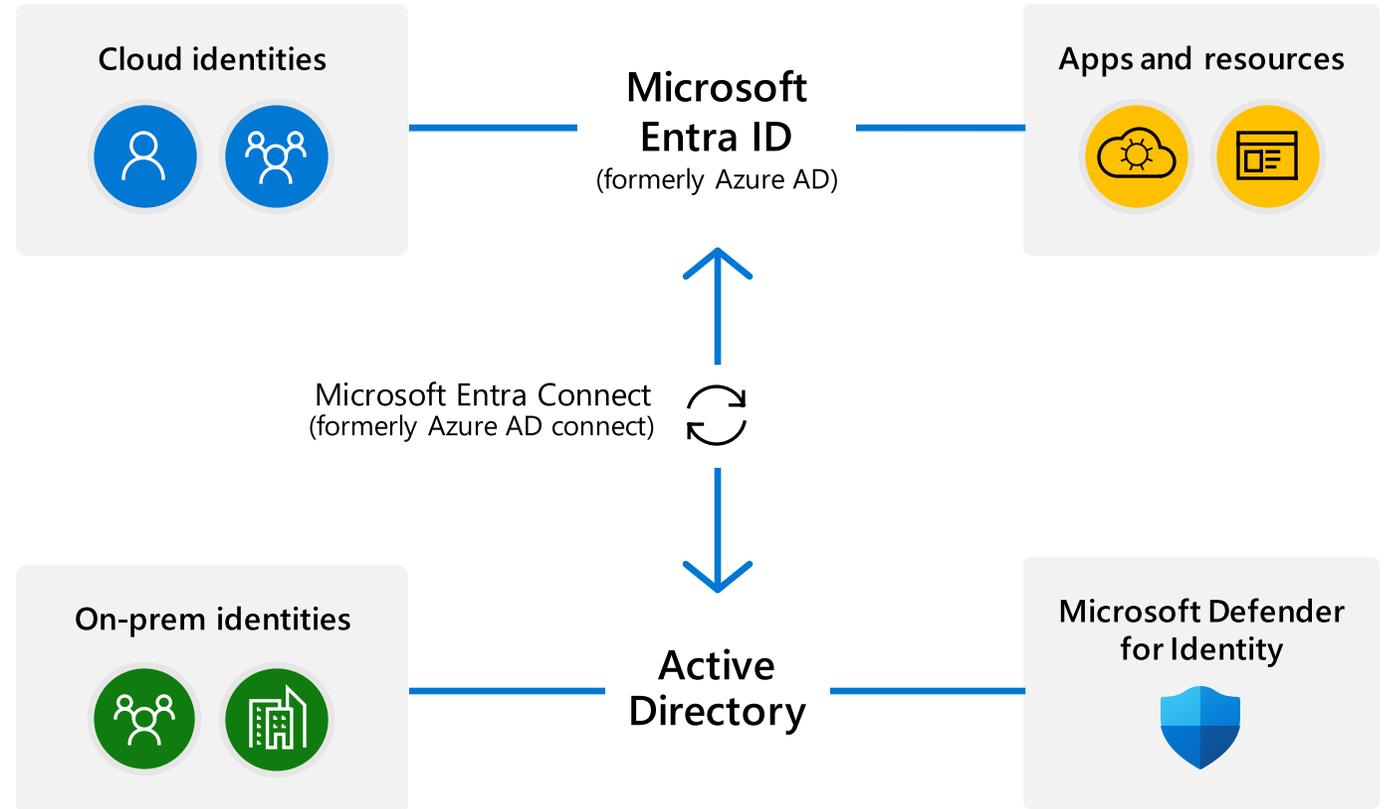
Market challenge:

Organizations require a comprehensive IAM solution across hybrid and cloud environments that provides security, simplifies user authentication, and enables secure access to resources

Provide a common identity for your users

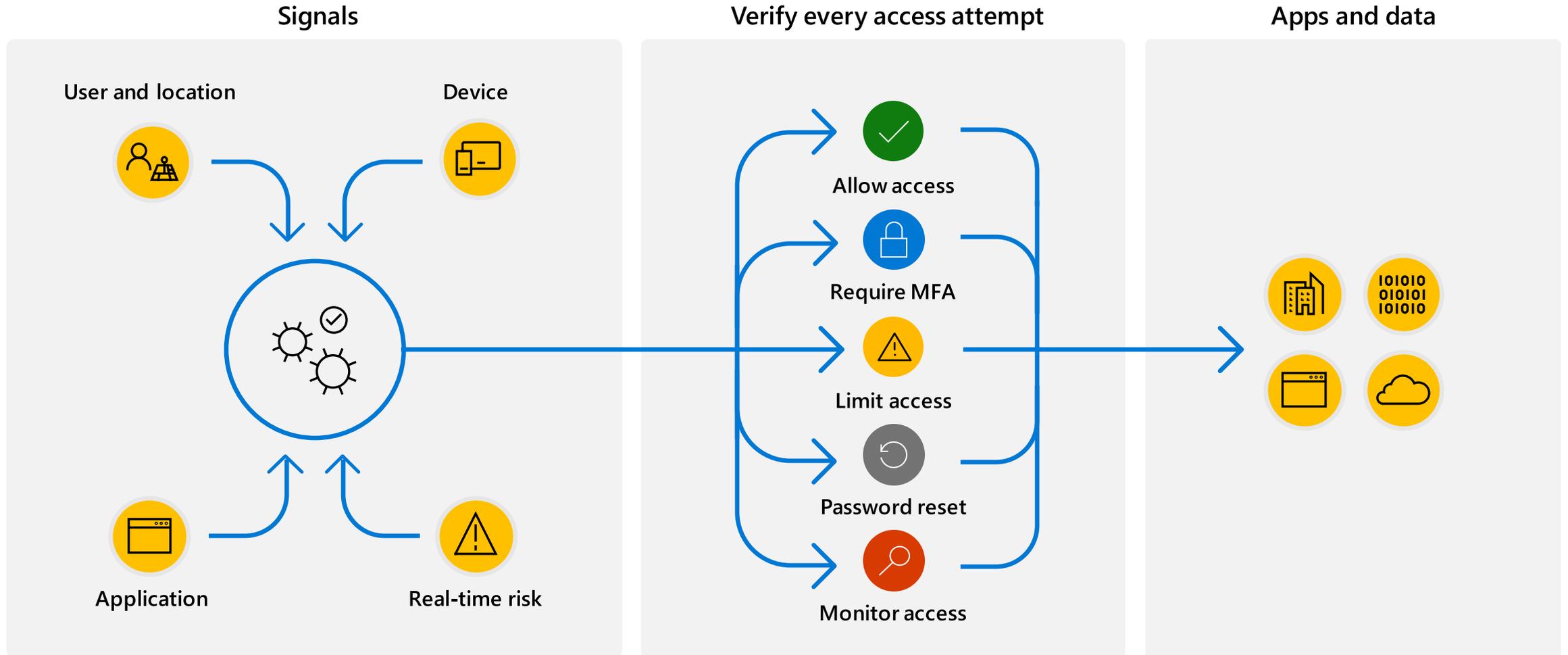
Manage your hybrid identity from the cloud for greater security and control

- > Sync identities with Microsoft Entra Connect (formerly Azure AD Connect) so users gain a common identity for access to resources no matter where they are
- > Embrace cloud authentication and upgrade from AD FS, reducing your on-premises footprint
- > Identify and resolve vulnerabilities and assess threats efficiently with Microsoft Defender for Identity and advanced protection with Microsoft Entra ID (formerly Azure AD)



Protect resources with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



ID Protection

Block identity takeover in real-time



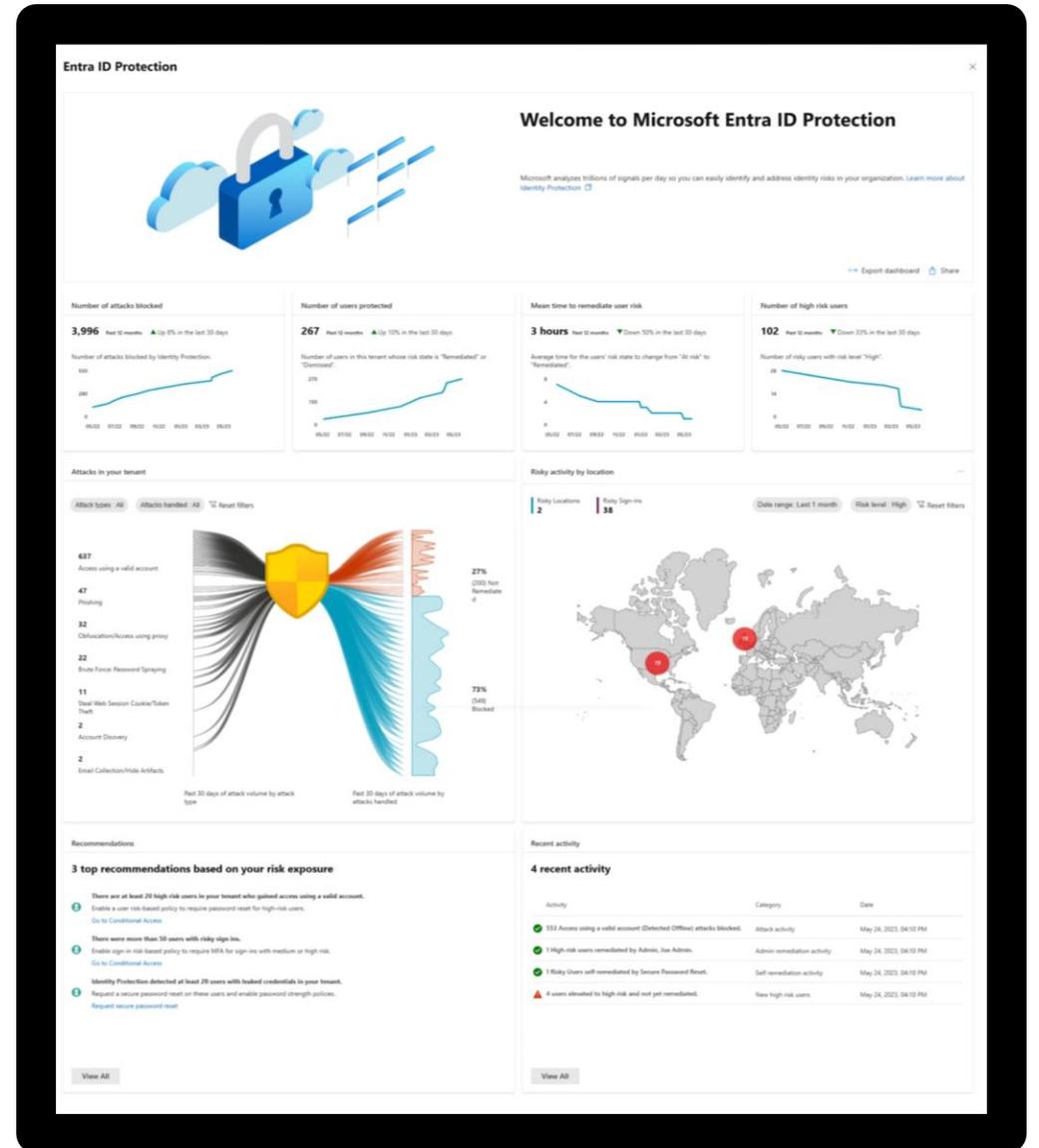
Prevent identity compromise



Enforce policies



Seamlessly integrate



Learn more about Microsoft Entra ID



Start a free trial for [Microsoft Entra ID](#)

- > **Microsoft Security ID blog**
aka.ms/identityblog
- > **Microsoft Entra ID product page**
aka.ms/EntraID
- > **Microsoft Entra product family page**
microsoft.com/Entra
- > **Microsoft Entra ID Beginners Tutorial Video**
[microsoftmechanics_youtube](https://microsoftmechanics.youtube)



Microsoft Entra ID Governance

Go to section >>

Ensuring that the right people have the right access to the right resources, at the right time



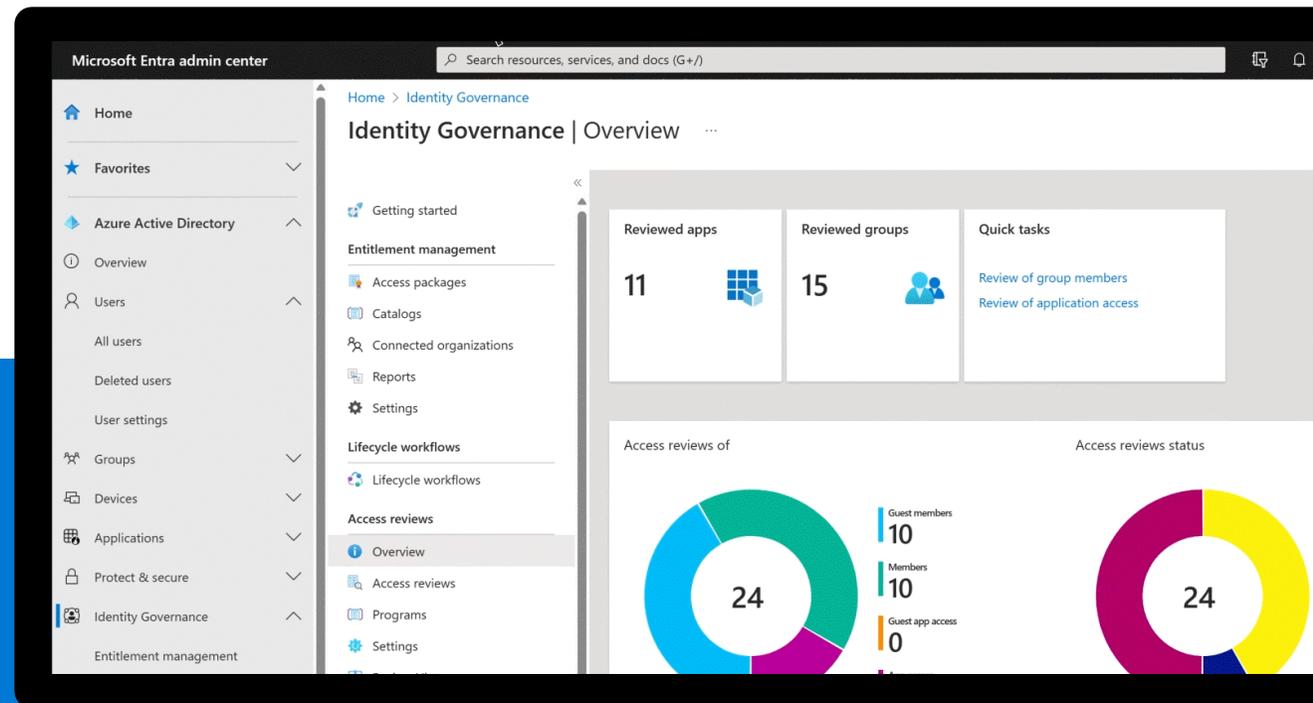
Improve productivity



Strengthen security



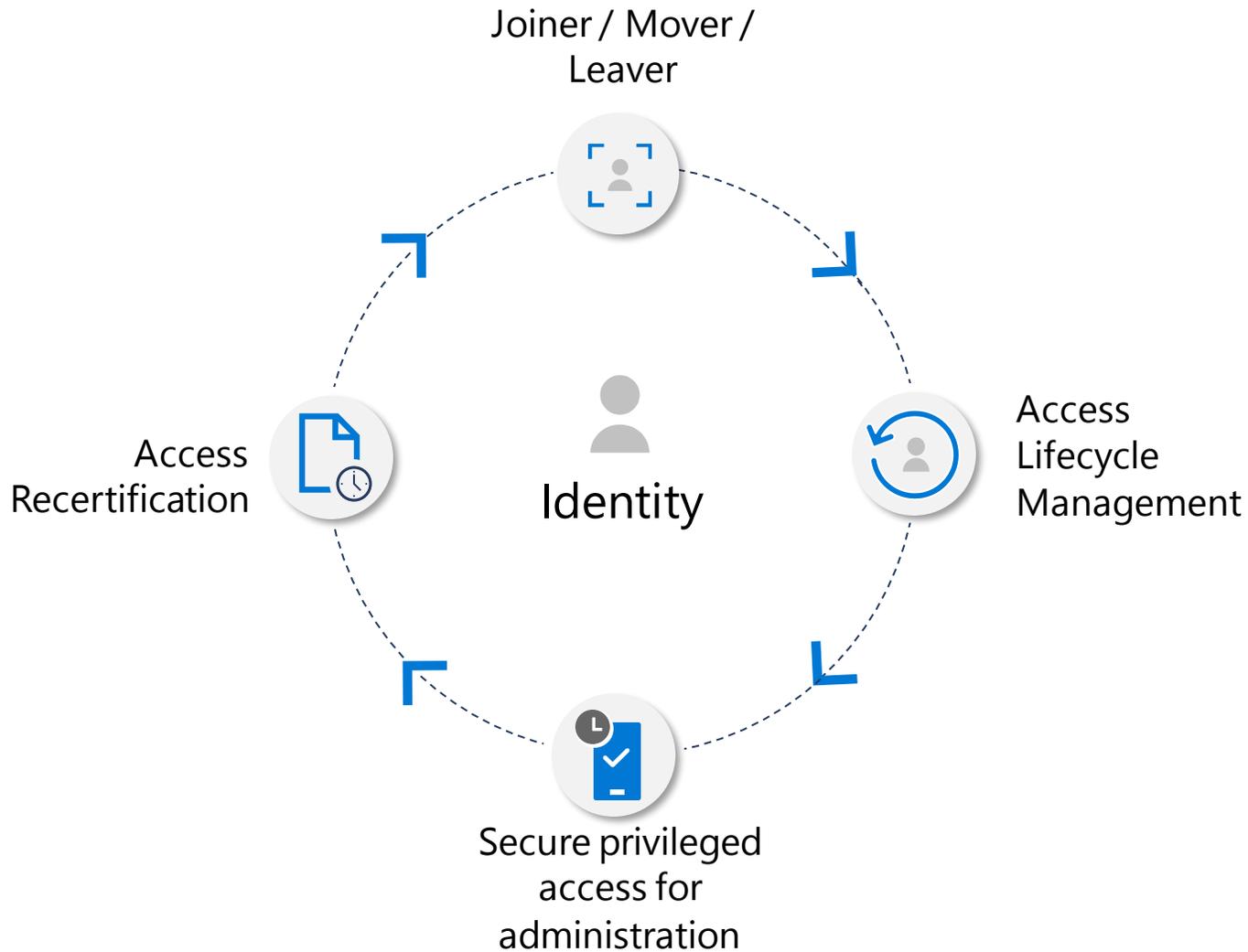
Automate routine tasks



Market challenge:

Managing user identities, access rights, and entitlements across IT environments to ensure proper access controls, mitigate risk, and maintain compliance with regulatory requirements

What is Microsoft Entra ID Governance?



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?

Automate identity processes with lifecycle workflows

Manual processes are slow for users, and error-prone for IT

> Joiner

Templates and automated actions through workflows make the identity process efficient and infallible for IT admins and enables access quicker for new team members

> Mover*

Team members who have experienced change get access to new resources immediately, while outdated accesses are removed without IT

> Leaver

Customizable workflow templates for common offboarding tasks ensures timely, reliable resource access removal for IT, and peace of mind for former team members

The screenshot displays the Microsoft Entra admin center interface. The breadcrumb navigation shows: Home > Identity Governance | Lifecycle workflows > Lifecycle workflows | Workflows. The main heading is "Offboard an employee - voluntary departure | Tasks", with "Workflow" underneath. A search bar is present. On the right, there are controls: "+ Add task", "Disable", "Enable", "Reorder", and a trash icon. Below this, a text note states: "Tasks can be added, modified, or reordered to define the set of actions for this workflow." A table lists tasks with columns for "Task order" and "Name".

Task order	Name
1	Disable User Account
2	Remove user from all groups
3	Remove user from all Teams

* To be supported in the future

Learn more about Microsoft Entra ID Governance



Start a free trial for [Microsoft Entra ID Governance](#)

> **Microsoft Security ID blog**
aka.ms/identityblog

> **Microsoft Entra product family page**
microsoft.com/entra

> [Watch the Microsoft Mechanics video](#)

> [Demo the Interactive Guide](#)



Microsoft Entra External ID

[Go to section >>](#)

A complete customer identity and access management solution that allows you to personalize and secure access to any application for customers and partners



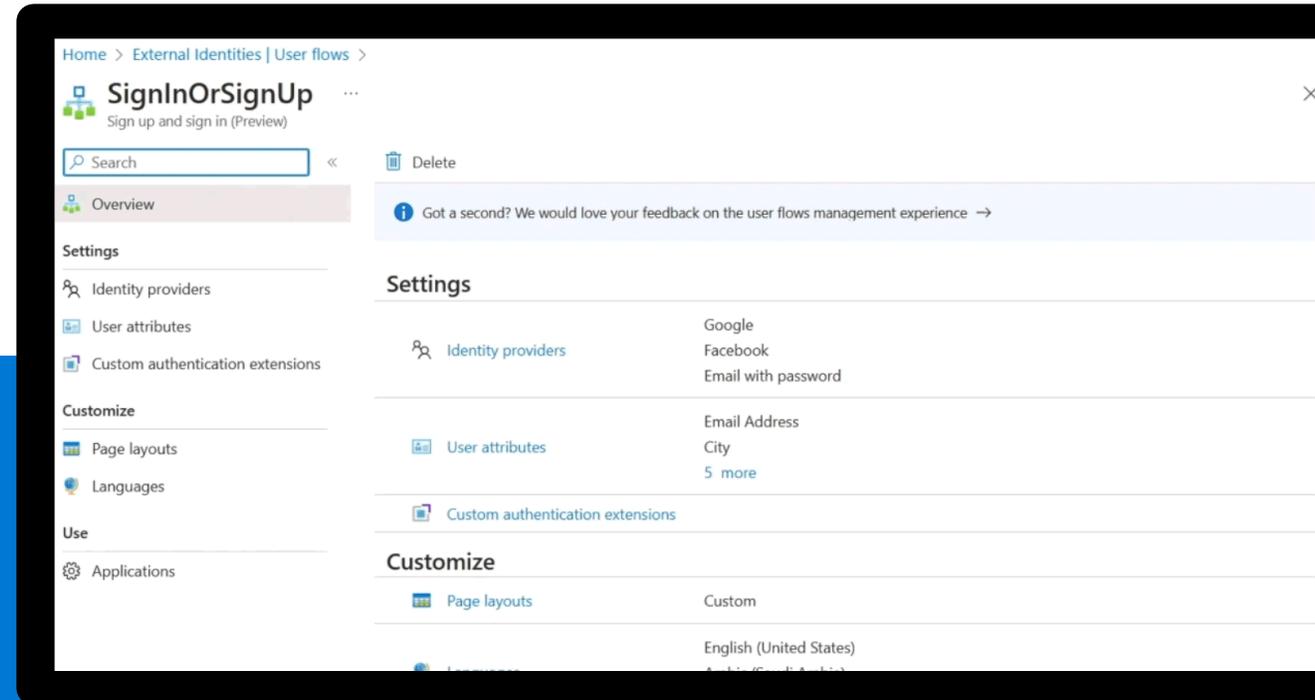
Secure partner and customer access



Create people-centric experiences



Accelerate development of secure applications



Market challenge:

Rapid increase of external identities that need to collaborate with customers, partners, and employees

Personalize and secure access to any application for customers and partners



Personalized user experiences



Secure, scalable and resilient



Developer friendly

Learn more about Microsoft Entra External ID



Learn more about our capabilities and the future of customer identity and access management on our [product page](#). Or dive into resources such as documentation, videos, demos, and code sharing on our new developer experience, [the Developer Center](#)

> Microsoft Security ID blog

aka.ms/identityblog

> Microsoft Entra product family page

microsoft.com/entra

> External ID product page

aka.ms/External-ID

> The Dev Center

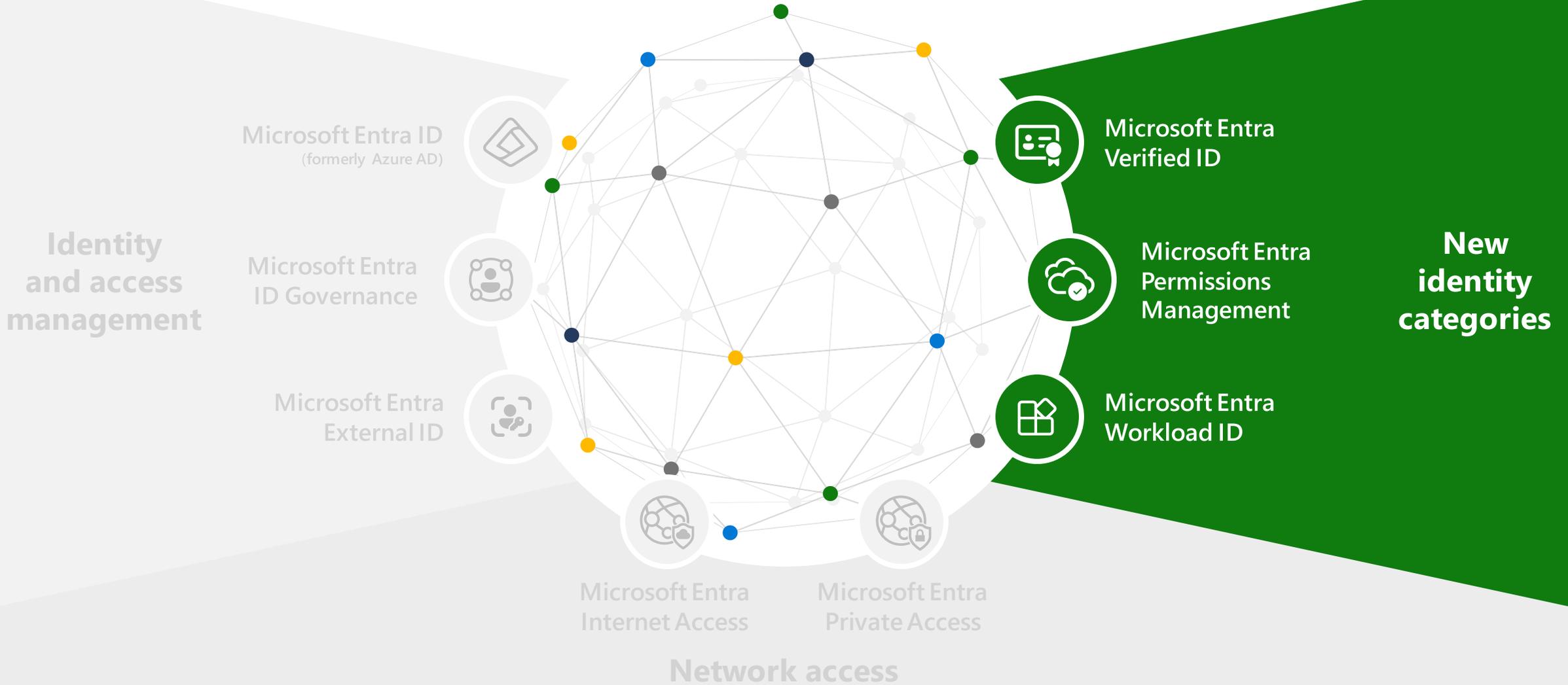
aka.ms/ciam/dev

> Microsoft Identity Developer Blog

devblogs.microsoft.com/identity/

Microsoft Entra product family

Secure access for a connected world





Microsoft Entra Verified ID

Confidently issue and verify workplace credentials, citizenship, education status, certifications, or any unique identity attributes in a global ecosystem designed for more secure interaction between people, organizations, and things



Fast remote onboarding

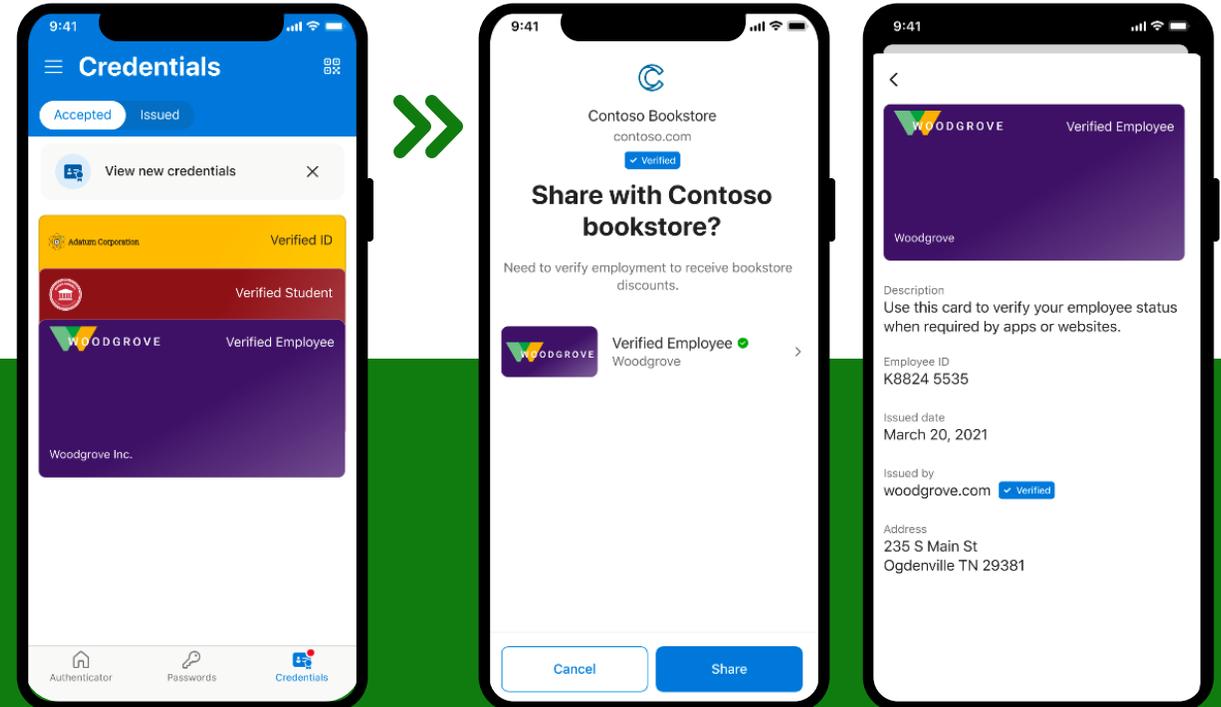


More secure access



Easy account recovery

Go to section >>



Market challenge:

People don't own their identity data and individuals lack visibility on how their data is used and how to get it back

Building a trust fabric for tomorrow: decentralized Identity



For everyone

Own and control your digital identity and protect your privacy with highly secure user experiences



For organizations

Engage with less risk, use electronic data verification, and improve transparency and auditability



For developers

Design user-centric apps and services and build true serverless apps that store data with users

Learn more about Microsoft Entra Verified ID



Learn more about Verified ID at aka.ms/verifyonce or jump straight to the configuration instructions

- > **Landing page**
aka.ms/verifyonce
- > **[Read the customer stories](#)**
- > **[Read the white paper](#)**
- > **Verify your workplace on LinkedIn**
aka.ms/VerifyOnLinkedIn



Microsoft Entra Permissions Management

A cloud infrastructure entitlement management (CIEM) product that provides comprehensive visibility and control over permissions for any identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP)



Get granular
cross-cloud visibility

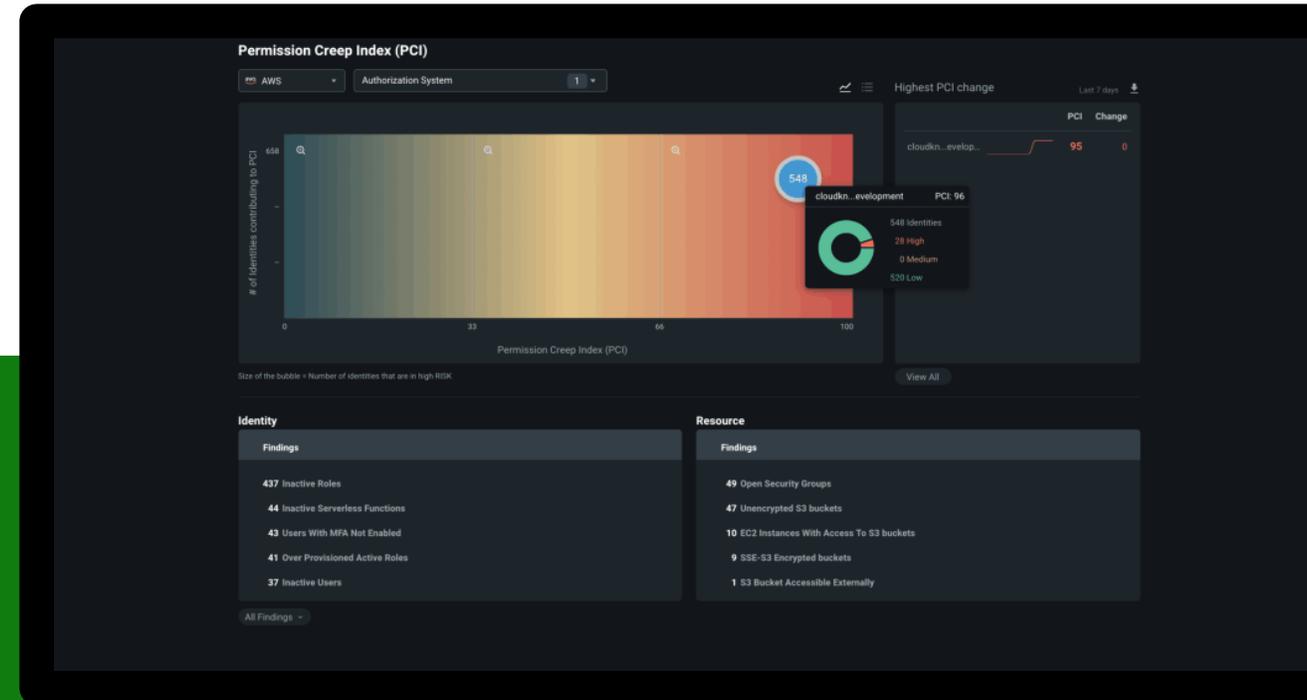


Enforce the principle of
least privilege



Reduce permission risk

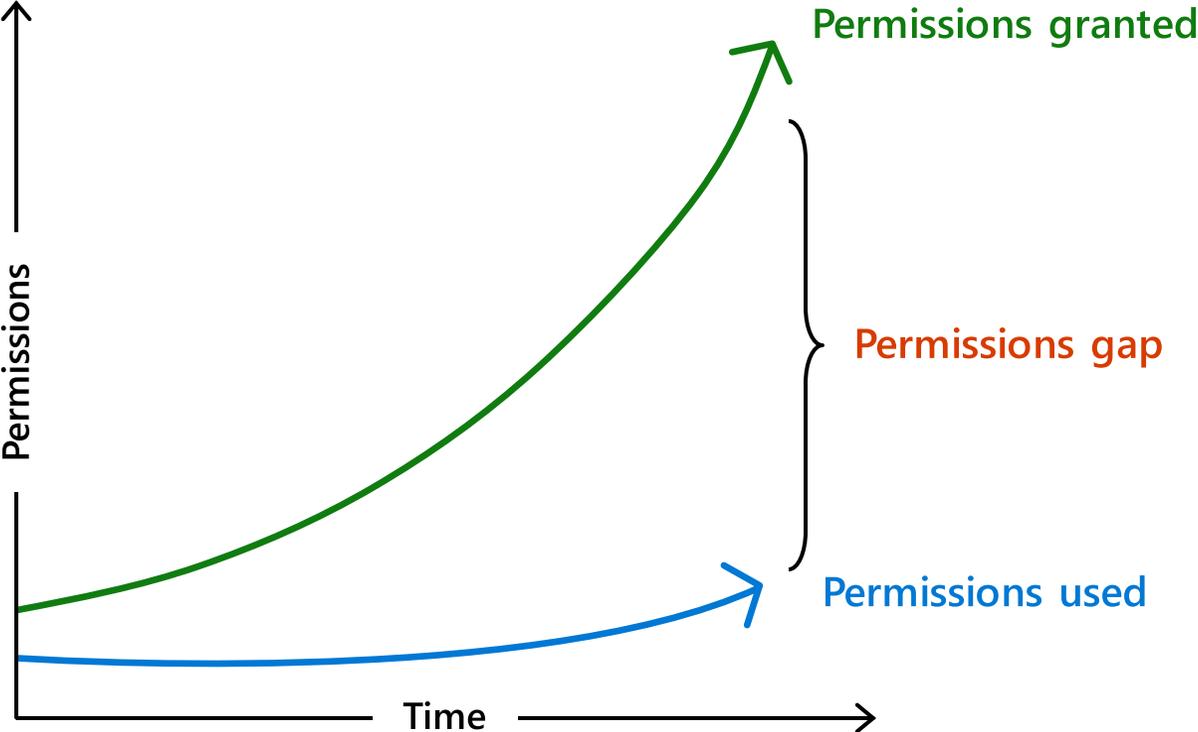
Go to section >>



Market challenge:

There are over 40,000 permissions that can be granted across AWS, GCP and Azure. Identities are only using 1% of permissions granted

Unmanaged permissions are expanding your attack surface



Lack of comprehensive visibility into identities, permissions and resources



Increased complexity for IAM and security teams to manage permissions across multcloud environments



Increased risk of breach from accidental or malicious permission misuse

Managing permissions across multicloud environments requires a new approach

Today's static, outdated approach

Grants permissions based on job roles and responsibilities



IAM admins manually grant permissions which are not time-bound



Permission clean-up is done manually on an as-need basis



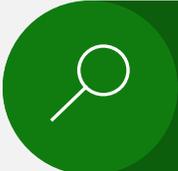
A new, dynamic approach



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

Learn more about Microsoft Entra Permissions Management



Try Permissions Management for free and run a risk assessment to identify the top permission risks across your multicloud infrastructure: <https://aka.ms/TryPermissionsManagement>

- > **Permissions Management Website**
aka.ms/PermissionsManagement
- > **Permissions Management Documentation**
aka.ms/CIEM



Microsoft Entra Workload ID

Go to section >>

A comprehensive set of features that helps secure adaptive access, detect and respond to compromised workload identities, and simplify their lifecycle management



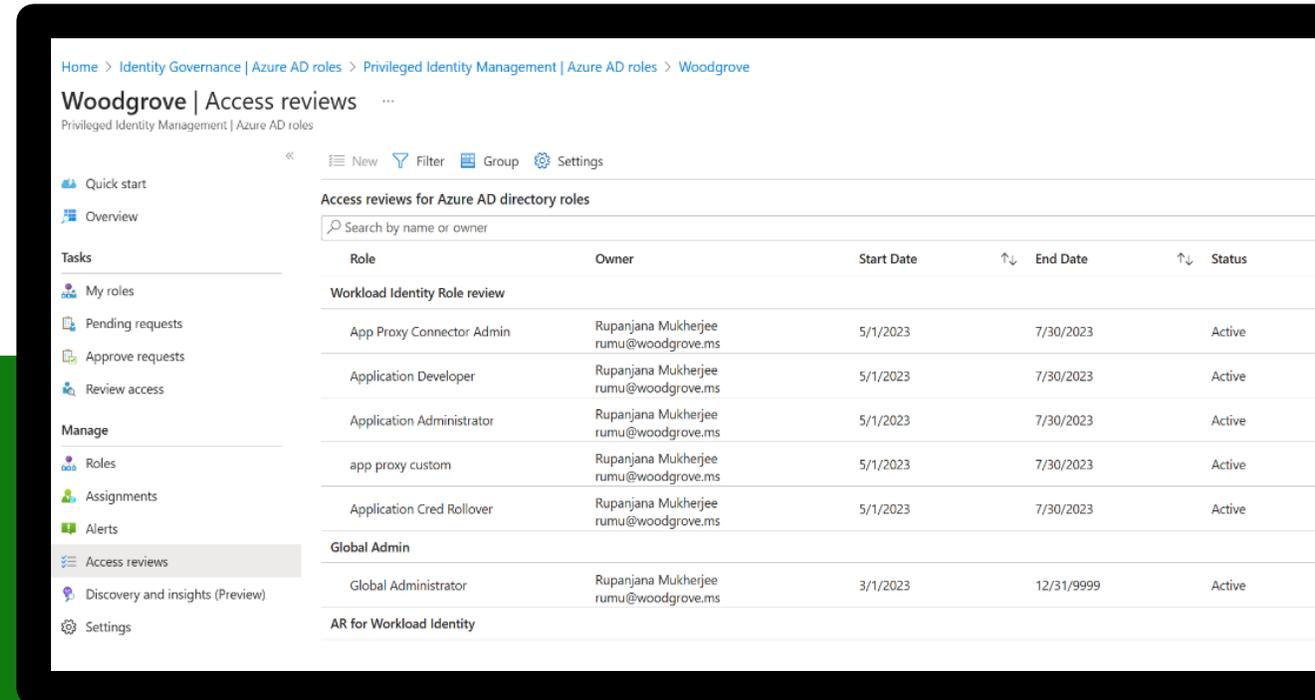
Secure access with adaptive access policies



Detect compromised workload identities



Simplify lifecycle management



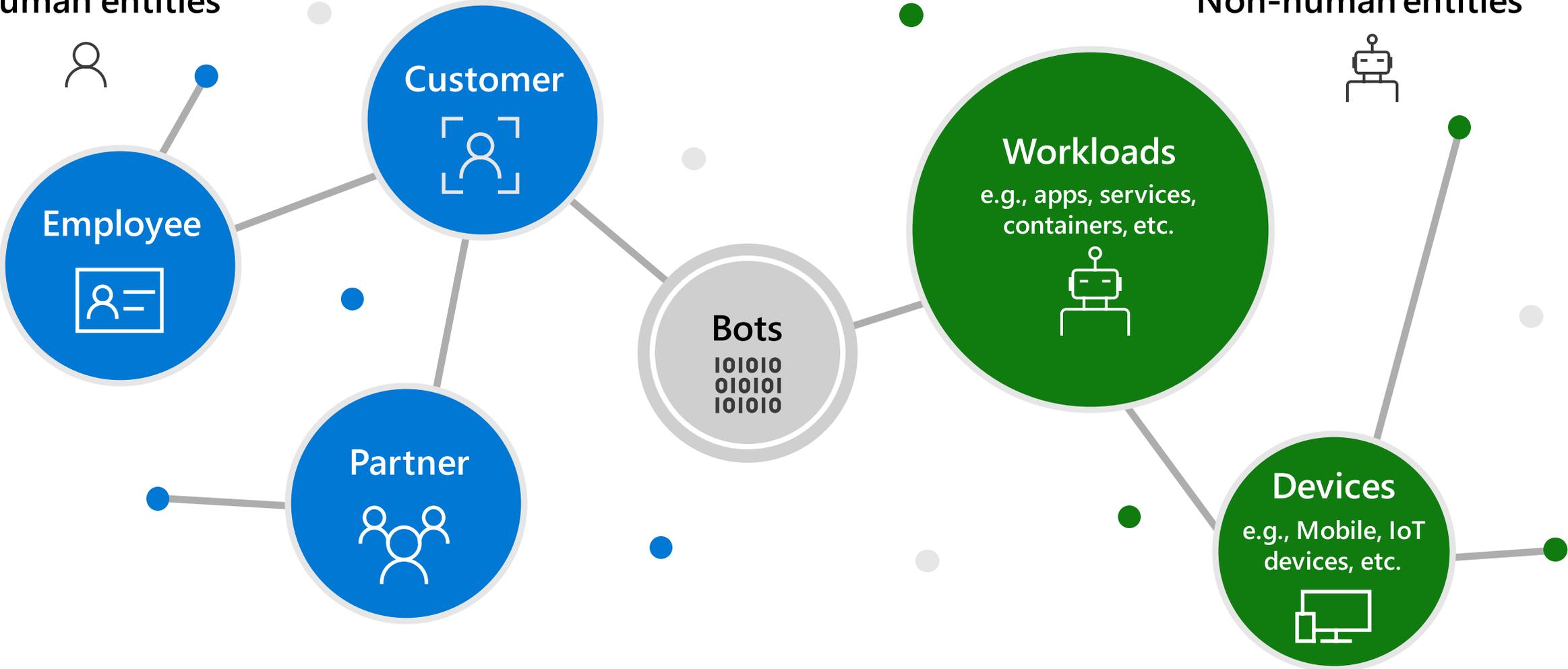
Market challenge:

The number of workload identities accessing critical infrastructure are increasing, now outnumbering human identities 10:1

What are workload identities?

Human entities

Non-human entities





Introducing Microsoft Entra Workload ID

An identity and access management (IAM) solution that provides security controls for applications and services and helps manage their lifecycle



Secure access with adaptive access policies



Detect compromised workload identities



Simplify lifecycle management

Learn more about Microsoft Entra Workload ID



Start a free trial on Microsoft Entra Admin Center at entra.microsoft.com

> Microsoft Security ID blog
aka.ms/identityblog

> Workload ID Docs
aka.ms/workloadidentities

> Microsoft Entra product family page
microsoft.com/entra

> Workload ID Website
aka.ms/EntraWorkloadIdentities

Microsoft Entra product family

Secure access for a connected world



Microsoft Entra ID
(formerly Azure AD)

Microsoft Entra
ID Governance

Microsoft Entra
External ID

Identity
and access
management

Microsoft Entra
Internet Access

Microsoft Entra
Private Access

Network access

Microsoft Entra
Verified ID

Microsoft Entra
Permissions
Management

Microsoft Entra
Workload ID

New
identity
categories



Microsoft Entra Internet Access

Secure access to all internet, SaaS, and Microsoft 365 apps and resources while protecting your organization against internet cyberthreats, malicious network traffic, and unsafe or non-compliant content with an identity-centric Secure Web Gateway (SWG)



Extend Conditional Access to your network

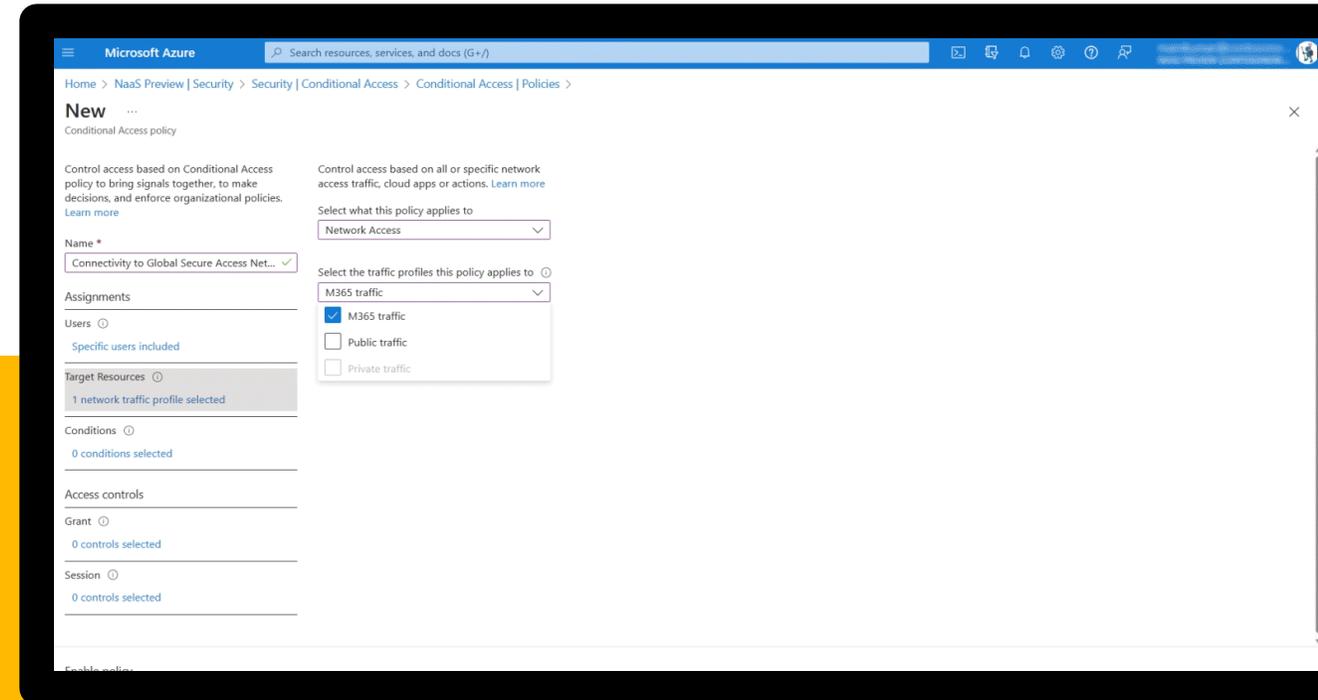


Modernize network security to protect users, apps, and resources



Enhance security and visibility for Microsoft 365 access

Go to section >>



Market challenge:

Control web traffic with advanced threat protection, content filtering, and policy enforcement to ensure safe and productive internet usage for employees



Microsoft Entra Private Access

Remove the risk and operational complexity of legacy VPNs while boosting user productivity. Quickly and securely connect remote users from any device and any network to private apps—on-premises, across clouds, and anywhere in between



Modernize private app access with an identity-centric ZTNA

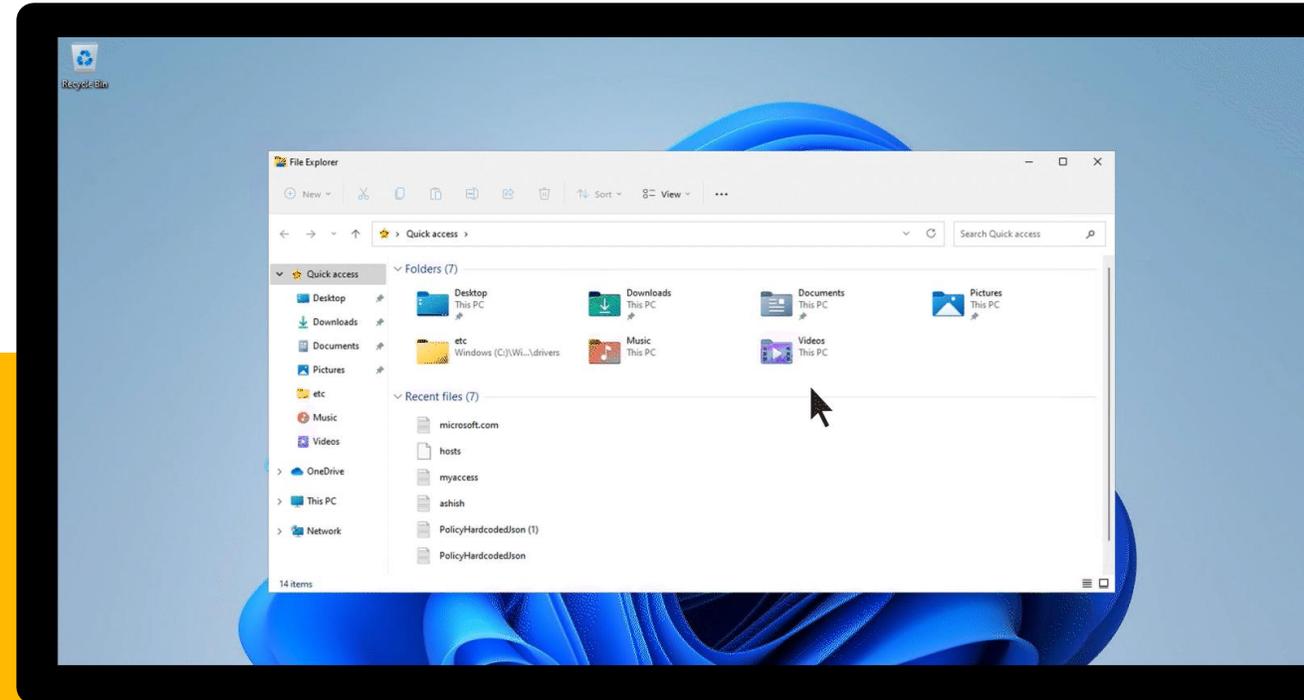


Prevent breaches with adaptive access controls



Enhance security through granular app segmentation

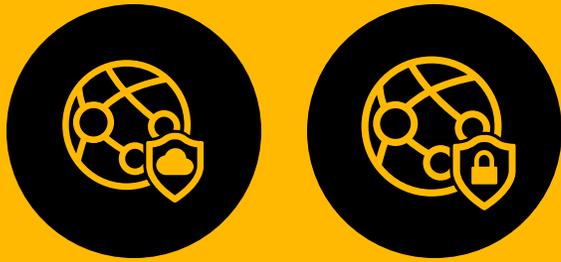
Go to section >>



Market challenge:

Simplify organization's network architecture to enhance security and reduce operational complexities by converging multiple security and networking functions into a unified cloud-based service

Learn more about Microsoft's SSE solution



> Microsoft Entra Internet Access

<https://aka.ms/InternetAccess>

> Microsoft Entra Private Access

<https://aka.ms/PrivateAccess>

> MS Docs page

<https://aka.ms/InternetandPrivateAccessDocs>

Neuigkeiten rund um Microsoft Entra

Microsoft Entra's Top 20 Features of 2023 (1/2)

1. **Secure Access in the Era of AI** - at Microsoft Ignite 2023, we announced that Microsoft [Security Copilot](#) is coming to Microsoft Entra ([in Private Preview](#)) to help you automate common tasks, troubleshoot faster, interpret complex policies, and design workflows. This monumental inclusion is only one component of maintaining strong and consistent **identity security**.
2. Upcoming support for [passkeys](#) offering **phishing-resistant alternative to physical FIDO2 security keys** supporting our enterprises and government customers.
3. **Secure by default**, through the [auto-rollout of Microsoft Entra Conditional Access policies](#) protecting tenants based on risk signals, licensing, and usage.
4. Conditional Access enforcement of [token protection for sign-in sessions \(Public Preview\)](#) to **combat token theft and replay attacks**.
5. [Conditional Access for protected actions](#) enabling organizations to **safeguard critical administrative operations**, such as altering Conditional Access policies, adding credentials to an application, or changing federation trust settings etc.
6. [Conditional Access overview dashboard](#) offering a comprehensive view of Conditional Access posture and [templates](#) providing a convenient method to deploy new policies aligned with Microsoft recommendations.
7. [Conditional Access authentication strength](#) to enable organizations to tailor authentication method requirements based on the user's sign-in risk level or the sensitivity of the accessed resource, **empowering those in highly regulated industries** or with strict compliance requirements.
8. Implement Zero Trust access control by invalidating tokens that violate your IP-based location policies and **prevent token replay attacks** in near real-time through the [strict enforcement of location policies \(Public Preview\)](#).
9. The new [Entra ID Protection dashboard \(Public Preview\)](#) is a central hub aiding identity admins and IT practitioners in understanding security posture and implementing effective protections against identity compromises.
10. New Entra ID Protection signals: [verified threat actor ID](#) and [attacker in the middle](#), to help protect organizations from malicious actors and activities.

Microsoft Entra's Top 20 Features of 2023 (2/2)

11. Entra ID Protection now offers [real-time threat intelligence detections](#) to apply risk-based Conditional Access policies to protect identities.
12. [Manage the permissions of identities across a multicloud infrastructure](#) - Improve the security posture of your **identities for multicloud** infrastructure by managing their permissions and ensuring the principle of least privilege.
13. Leverage Entra ID Protection - [Allow on-premises password change to reset user risk \(Public Preview\)](#) to effectively **manage user risk in hybrid environments**.
14. [Integration of Entra ID Protection with Microsoft 365 Defender](#) to investigate incidents efficiently and effectively, gaining a **comprehensive understanding of end-to-end attacks** and facilitating a quicker response to identity compromises.
15. [System-preferred authentication for MFA](#) to sign in users with the most secure method they've registered and the method that's enabled by admin policy.
16. Configure phishing-resistant MFA on mobile without having to provision certificates on the user's mobile device using [certificate-based authentication \(CBA\) on mobile](#).
17. [New features and enhancements](#) in certificate-based authentication (CBA) enabling government organizations to comply with Executive Order 14028 requirements and helping customers migrate from Active Directory Federation Services.
18. Use [Quick setup for Microsoft Entra Verified ID](#), removing several configuration steps and admin needs to complete your initial Verified ID set up with a single click.*
19. [Converged Authentication Methods](#) - Manage multi-factor authentication (MFA) and self-service password reset (SSPR) in one policy alongside passwordless methods like FIDO2 security keys and certificate-based authentication (CBA).
20. **Secure non-human identities** using Microsoft Entra Workload Identities [App Health Recommendations](#).

Automatic Microsoft-managed Conditional Access policies in Microsoft Entra

At launch **Microsoft is deploying the following three policies** where our data tells us they would increase an organization's security posture:

1. Multifactor authentication for admins accessing Microsoft Admin Portals (P1/P2 licensed tenants)
 2. Multifactor authentication for per-user multifactor authentication users (users with P1/P2 licenses using per-user MFA, if in total less than 500 per-user MFA users)
 3. Multifactor authentication and reauthentication for risky sign-ins (P2 licenses for all users + all users registered for MFA)
- **Not every policy will appear in every tenant!**
 - You will be informed via Message Center if and which policies will be enabled in your tenant
 - The policies will be created in **report-only mode** and **cannot be deleted, only modified/disabled**

Microsoft will enable these policies after no less than 90 days after they're introduced in your tenant **if they're left in the Report-only state** (approx. earliest enforcement date: beginning of February 2024).

Conditional Access: Token protection for sign-in sessions

Token protection (also known as token binding) attempts to **reduce attacks using token theft** by ensuring a token is usable **only** from the **intended device**.

Currently, this **only** works with **supported Windows devices** and **desktop applications**:

- **Exchange Online**
- **SharePoint Online**

Unsupported devices and client applications will be blocked.

The screenshot displays the configuration interface for a **Token Protection Policy** in the Azure AD Conditional Access console. The main configuration area includes:

- Name:** Token Protection Policy
- Assignments:** Specific users included
- Users:** Specific users included
- Cloud apps or actions:** 2 apps included (Office 365 Exchange Online and Office 365 SharePoint Online)
- Conditions:** 2 conditions selected
- Access controls:** 0 controls selected
- Grant:** 0 controls selected
- Session:** Require token protection for sign-in sessions

Four configuration panels are open, with red arrows indicating their relationship to the main policy settings:

- Token Protection Policy (main):** Shows the policy name and a list of assigned cloud apps and actions.
- Device platforms:** Shows the policy is applied to **Windows** devices.
- Client apps:** Shows the policy is applied to **Mobile apps and desktop clients**.
- Session:** Shows the **Require token protection for sign-in sessions** control is selected.

A blue information box at the bottom right of the Session panel states: "The control 'Require token protection for sign-in sessions' only works with supported Windows devices and a limited set of applications. Unsupported devices and applications are blocked. Learn more"

Protected actions in Conditional Access

Protected actions in Microsoft Entra ID (formerly Azure Active Directory) are **permissions that have been assigned Conditional Access policies**. When a user attempts to perform a protected action, they must first **satisfy** the **Conditional Access** policies assigned to the required permissions.

Example: To allow administrators to update Conditional Access policies, you can require that they first satisfy the Phishing-resistant MFA policy.

Add protected actions (Preview) ...

Select a Conditional Access authentication context and then the permissions you want to protect. [Learn more](#)

Conditional Access authentication context ⓘ *

Permissions ⓘ

Permission
No permissions added

Search for permissions to protect. For example, search for "conditionalAccess" to find permissions related to Conditional Access.

ⓘ Each permission can be tagged with one Conditional Access authentication context. Permissions that are not tagged in a protected action are not listed.

7 actions found

<input type="checkbox"/>	Permission
<input type="checkbox"/>	microsoft.directory/conditionalAccessPolicies/basic/update
<input type="checkbox"/>	microsoft.directory/conditionalAccessPolicies/create
<input type="checkbox"/>	microsoft.directory/conditionalAccessPolicies/delete

Conditional Access overview dashboard

Home > Woodgrove | Security > Security | Conditional Access >

Conditional Access | Overview

Microsoft Entra ID

+ Create new policy + Create new policy from templates Refresh | Got feedback?

Getting started **Overview** Coverage Monitoring (Preview) Tutorials

Policy Summary

Policy Snapshot

47 Enabled 17 Report-only 10 Off

[View all policies](#)

Users

114 users signed in during the last 7 days without any policy coverage

[See all unprotected sign-ins](#)

Devices

100% of sign-ins in the last 7 days were from unmanaged or non-compliant devices

[See all noncompliant devices](#)

[See all unmanaged devices](#)

Applications

Browse a list of applications that are not protected by your policies.

[View top unprotected apps](#)

What's new

Named Locations

Microsoft Entra ID now supports IPv6! Update your Named locations with IPv6 ranges.

[Learn more](#)

13 policies have a Named Location condition

Security Alerts (Preview)

Description	Suggested Policy Templates
63% of sign-ins out of scope of Conditional Access policies in the last 7 days. Learn more	Create policy to require multifactor authentication for all users
36 recent sign-ins with medium or above sign-in risk in the last 7 days. Learn more	Create policy to require multifactor authentication for risky sign-ins
65% of sign-ins lack multifactor authentication requirement in the last 7 days. Learn more	Create policy to require multifactor authentication for all users
81 sign-ins using legacy authentication in the last 7 days. Learn more	Create policy to block legacy authentication

Manage

- [Named locations](#)
- [Custom controls \(Preview\)](#)
- [Terms of use](#)
- [Authentication contexts](#)
- [Authentication strengths](#)
- [Classic policies](#)

Monitoring

- [Sign-in logs](#)
- [Audit logs](#)

Troubleshooting + Support

- [New support request](#)

Conditional access authentication strength for members, external users and FIDO2 restrictions

- **Authentication strength** is a **Conditional Access control** that allows administrators to specify **which authentication methods** can be used to access a resource.
- For example, they can make only **phishing-resistant** authentication methods available to access a sensitive resource.

Conditional Access | Authentication strengths

Microsoft Entra ID

Overview Policies Insights and reporting Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication contexts
- Authentication strengths

+ New authentication strength Refresh

Authentication strengths determine the combination of authentication methods that can be used. [Learn more](#)

Type: All Authentication methods: All Reset filters

Authentication strength	Type	Authentication methods
Multifactor authentication	Built-in	Windows Hello For Business and 16 more
Passwordless MFA	Built-in	Windows Hello For Business and 3 more
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more

Dashboard > Conditional Access | Overview (Preview) >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Example: 'Device compliance app policy'

Assignments

Users or workload identities
0 users or workload identities selected

Cloud apps or actions
No cloud apps, actions, or authentication contexts selected

Conditions
0 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
[Report-only](#) On Off

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access
 Grant access

Require multifactor authentication

Require authentication strength

Multifactor authentic...

Multifactor authentication
Combinations of methods that satisfy strong authentication, such as Password + SMS

Passwordless MFA
Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator

Phishing-resistant MFA
Phishing-resistant Passwordless methods for

Strictly enforce location policies using continuous access evaluation (CAE)

- Strictly enforce location policies is a **new enforcement mode** for continuous access evaluation (CAE), used in Conditional Access policies.
- It allows tenant admins to **investigate IP addresses** seen by resource providers to **utilize CAE to promptly invalidate tokens** that violate location policies.

The screenshot displays the 'New' Conditional Access policy configuration page in Azure AD. The policy name is 'Strict location enforcement policy'. The 'Session' section is highlighted with a yellow box, showing the following options:

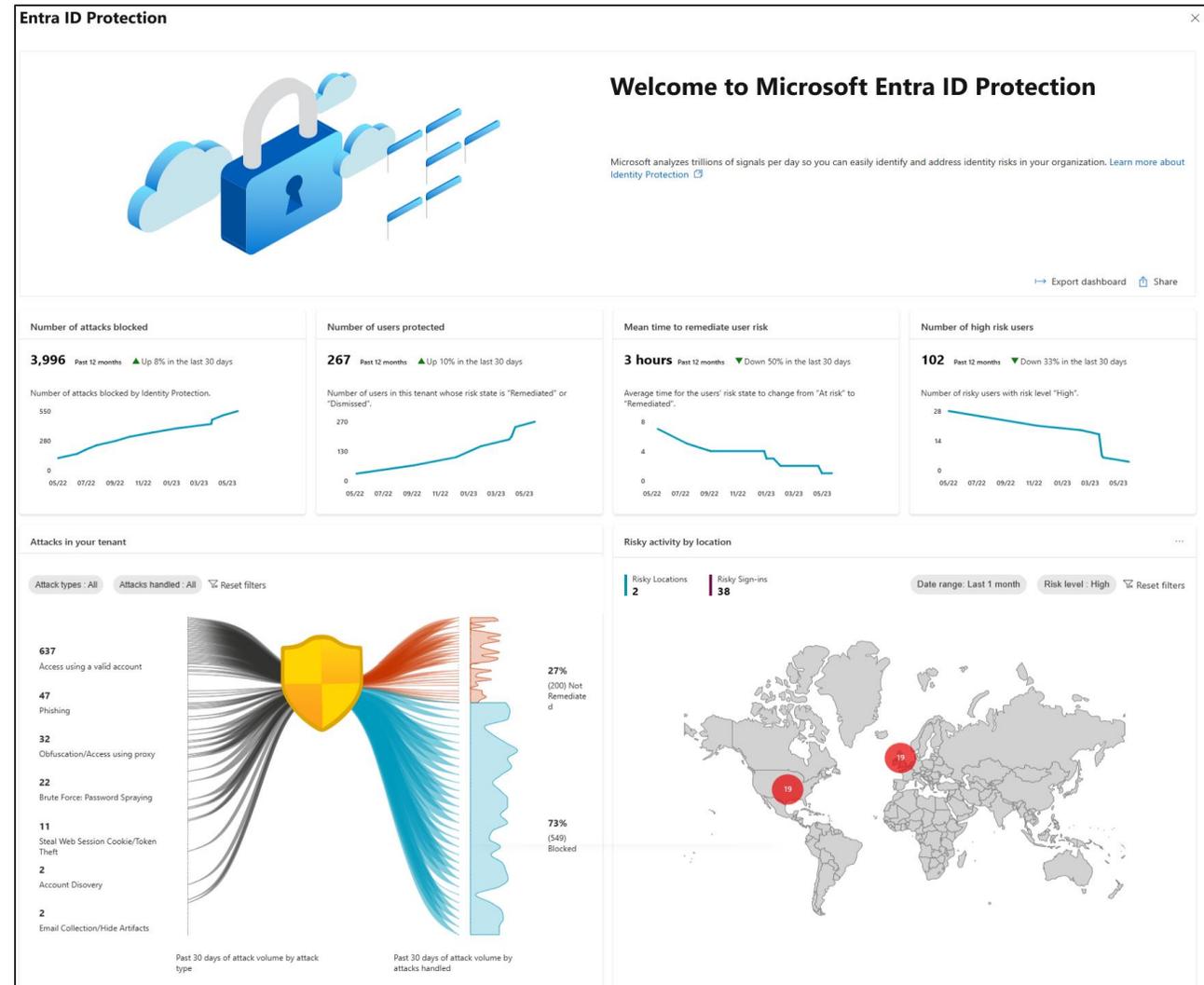
- Customize continuous access evaluation
 - Disable
 - Strictly enforce location policies (Preview)
- Use app enforced restrictions
- Use Conditional Access App Control
- Sign-in frequency
- Persistent browser session
- Disable resilience defaults
- Require token protection for sign-in sessions (Preview)

Other sections visible include 'Assignments' (Users: All users included and specific users excluded; Target resources: 2 apps included; Conditions: 1 condition selected), 'Access controls' (Grant: Block access), and 'Enable policy' (On/Off toggle, Create button).

Entra ID protection dashboard

The new Microsoft Entra ID Protection dashboard is designed as a **central hub** to empower IT admins and SOC teams with **rich insights and actionable recommendations** tailored to your tenant.

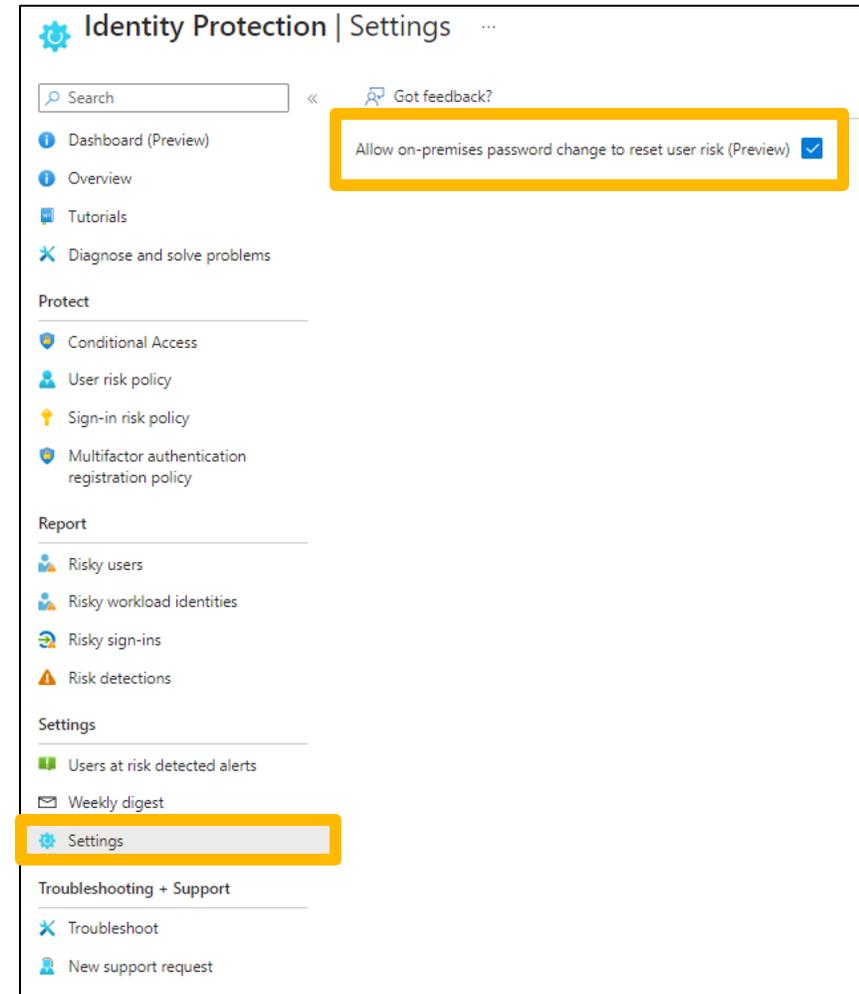
By providing a **deeper view into the security posture** of your organization, the dashboard enables you to **implement effective protections accordingly**.



Allow on-premises password reset to remediate user risk

By enabling **allow on-premises password change** to reset user risk you can **remediate risky users** through on-premises password resets.

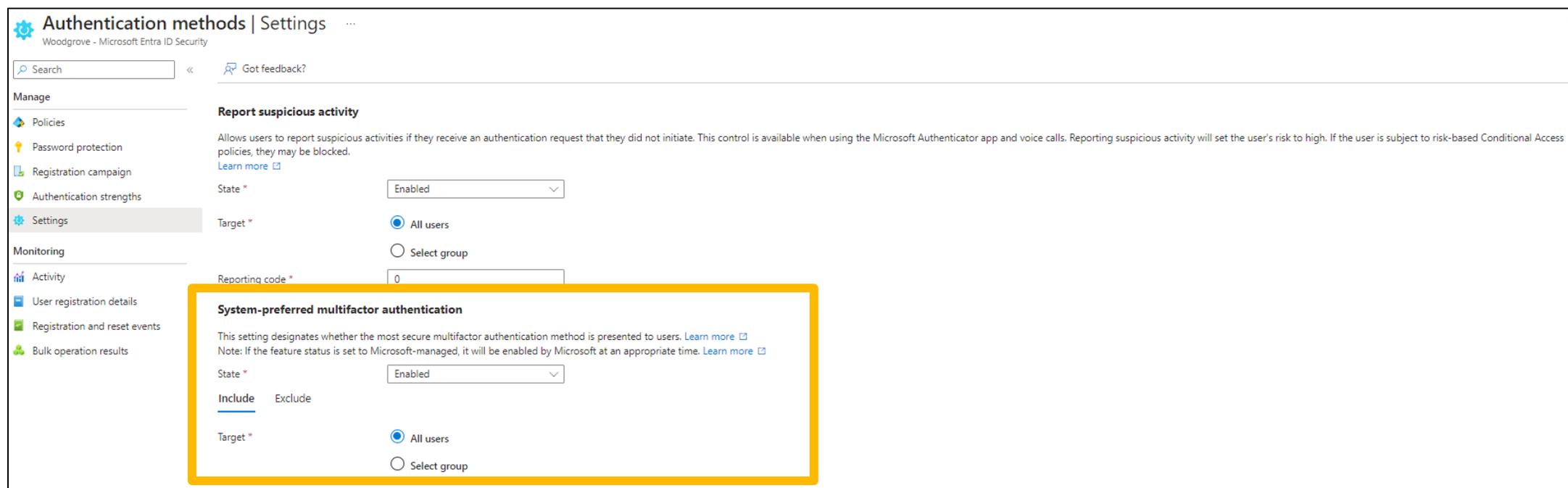
- Organizations can proactively deploy **user risk policies** that require password changes to confidently protect their hybrid users.
- This option strengthens your organization's security posture and **simplifies security management**, even in **complex hybrid** environments.



System-preferred multifactor authentication method

System-preferred multifactor authentication (MFA) enables IT admins to make the decision to **prompt their users for the most secure multi-factor authentication method** users have registered.

- We evaluate the different methods a user has at run time and **present them with the most secure method**. The **order** of authentication methods is **dynamic** and continuously updated.
- If users cannot access the method they are prompted for, they can **select another option**.



Authentication methods | Settings
Woodgrove - Microsoft Entra ID Security

Search Got feedback?

Manage

- Policies
- Password protection
- Registration campaign
- Authentication strengths
- Settings**

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Report suspicious activity

Allows users to report suspicious activities if they receive an authentication request that they did not initiate. This control is available when using the Microsoft Authenticator app and voice calls. Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they may be blocked. [Learn more](#)

State *

Target * All users Select group

Reporting code *

System-preferred multifactor authentication

This setting designates whether the most secure multifactor authentication method is presented to users. [Learn more](#)

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time. [Learn more](#)

State *

[Include](#) [Exclude](#)

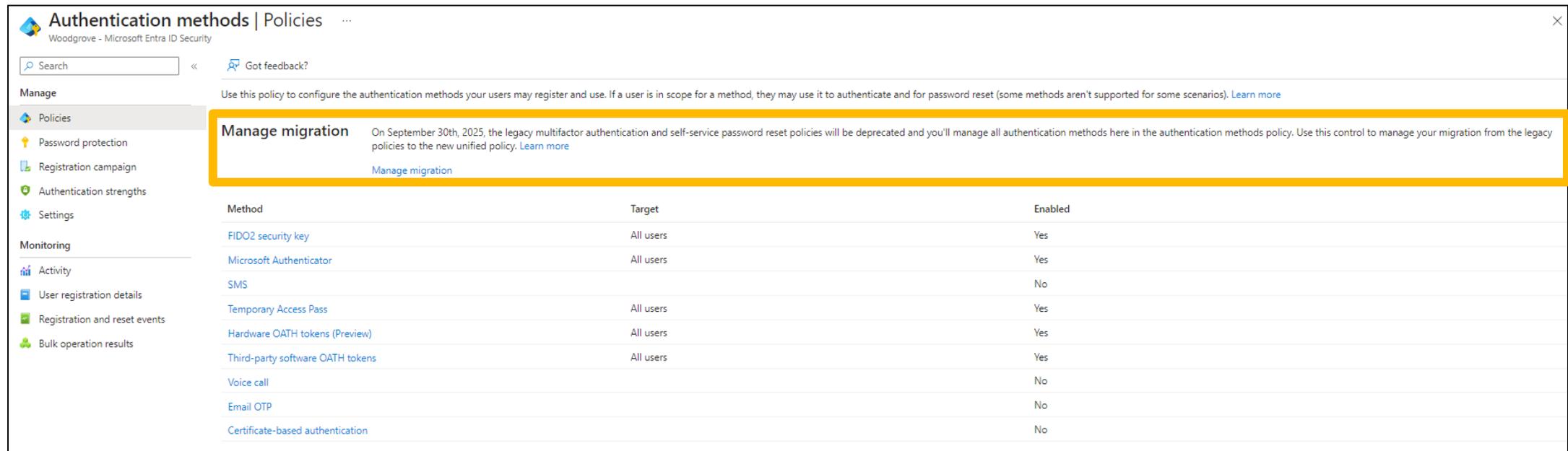
Target * All users Select group

Converged Authentication Methods Policy

The Converged Authentication Methods Policy enables you to manage **all authentication methods** used for **MFA and SSPR** in one policy and **migrate off the legacy MFA and SSPR policies**.

Settings aren't synchronized between legacy and authentication method policies.

- Entra ID respects the settings in **all of the policies**.
- To prevent users from using a method, it must be disabled in all policies.



Authentication methods | Policies

Woodgrove - Microsoft Entra ID Security

Search << Got feedback?

Manage

Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)

Manage migration On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. [Learn more](#)

[Manage migration](#)

Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)	All users	Yes
Third-party software OATH tokens	All users	Yes
Voice call		No
Email OTP		No
Certificate-based authentication		No

Conditional Access: Filter for applications*

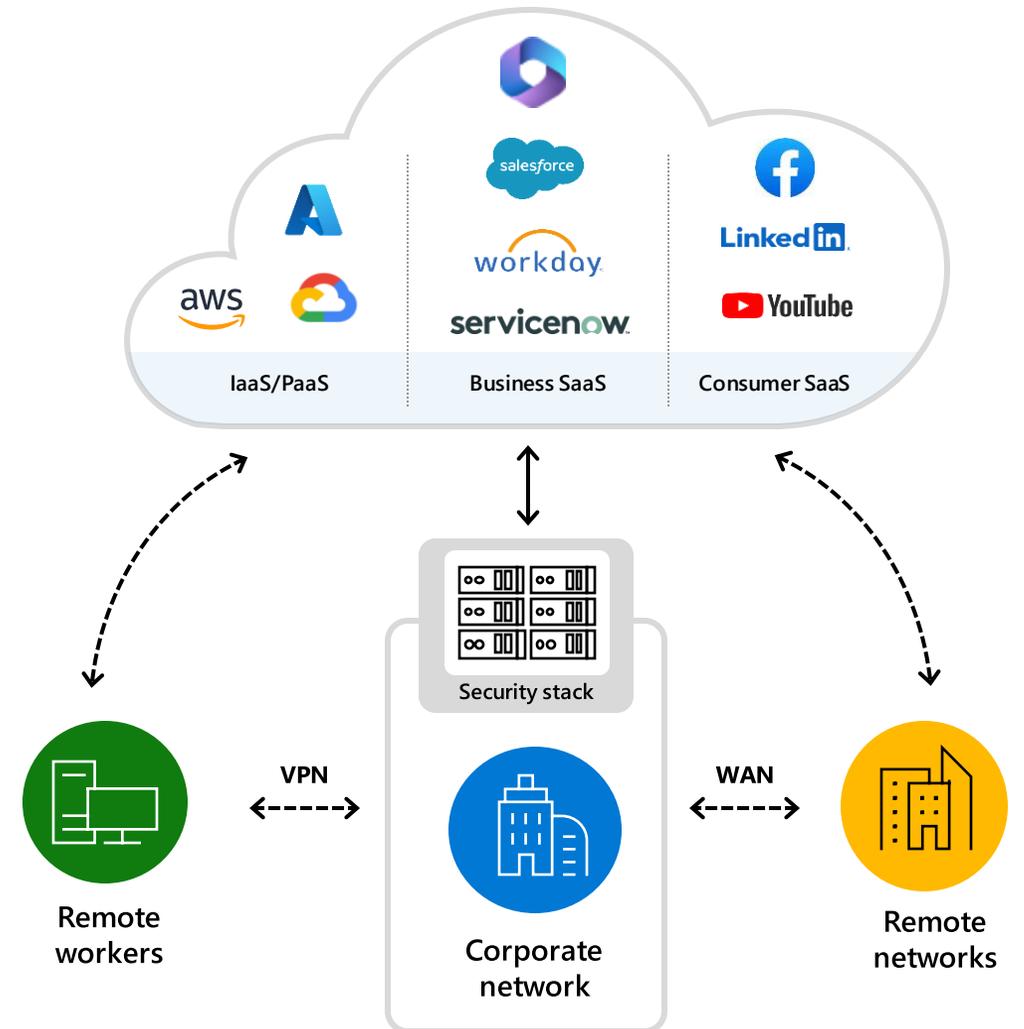
- Filters for apps in conditional access allow admins to tag apps with **custom security attributes** and target them in policies, avoiding direct assignments.
- With this feature you can scale up your policies as the **policy size won't increase when more apps are added**.
- **Workload identities** can also be targeted with the new filter capability.

The screenshot displays the 'New' Conditional Access policy configuration page. The main form includes sections for Name, Assignments, Target resources, Conditions, and Access controls. The 'Target resources' section shows a red error message: "Select apps" must be configured. On the right, the 'Edit filter' dialog is open, showing a configuration step for 'Select what this policy' with 'Cloud apps' selected. Below this, there are radio buttons for 'Include' (selected) and 'Exclude', with options: 'None', 'All cloud apps', and 'Select apps'. The 'Edit filter' dialog also shows a 'Configure' toggle set to 'Yes', a warning message: "You do not have the permissions needed to edit this filter", and a section for adding expressions with a dropdown for 'Attribute' and a text input for 'Rule syntax'.

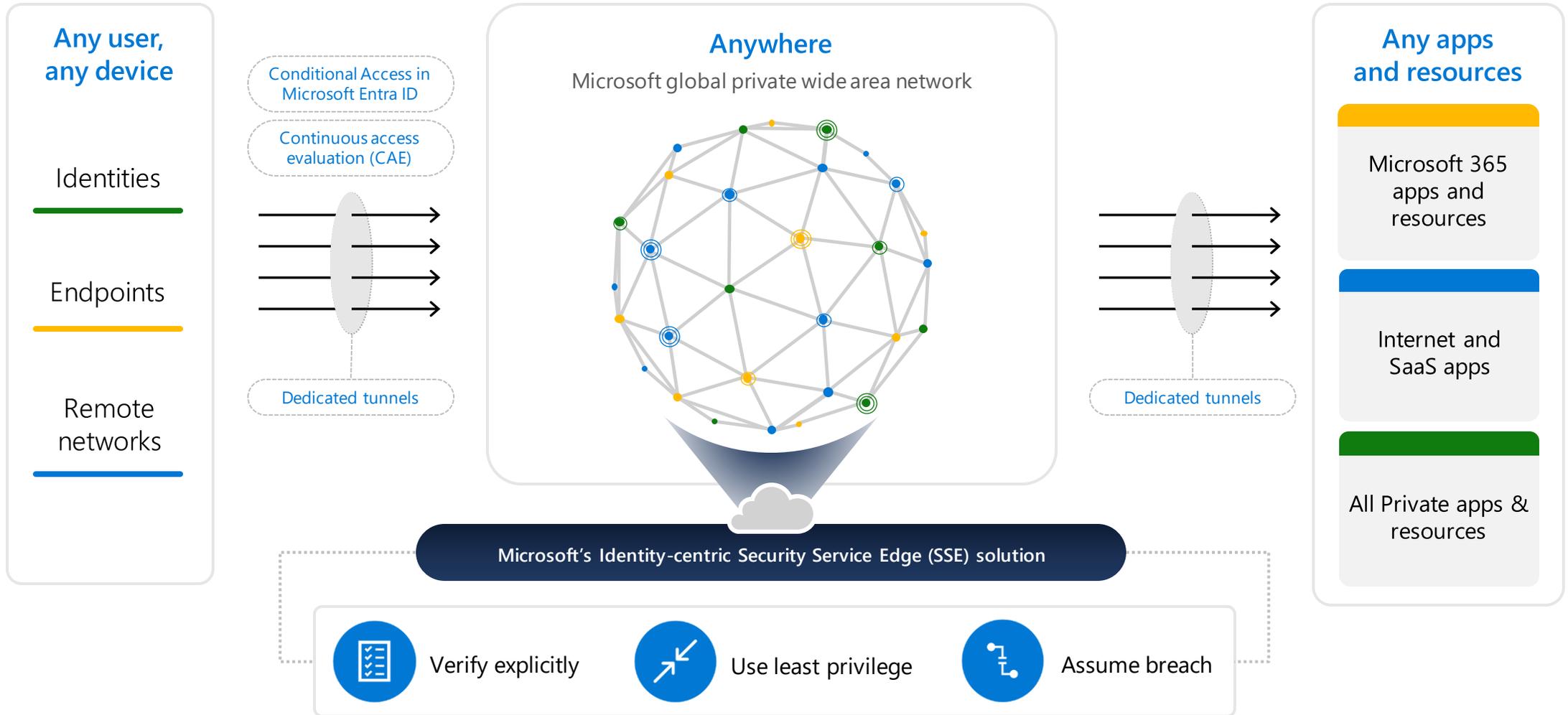
Einblick in die Microsoft Secure Service Edge (SSE) Lösung

Legacy network security approaches are no longer sufficient

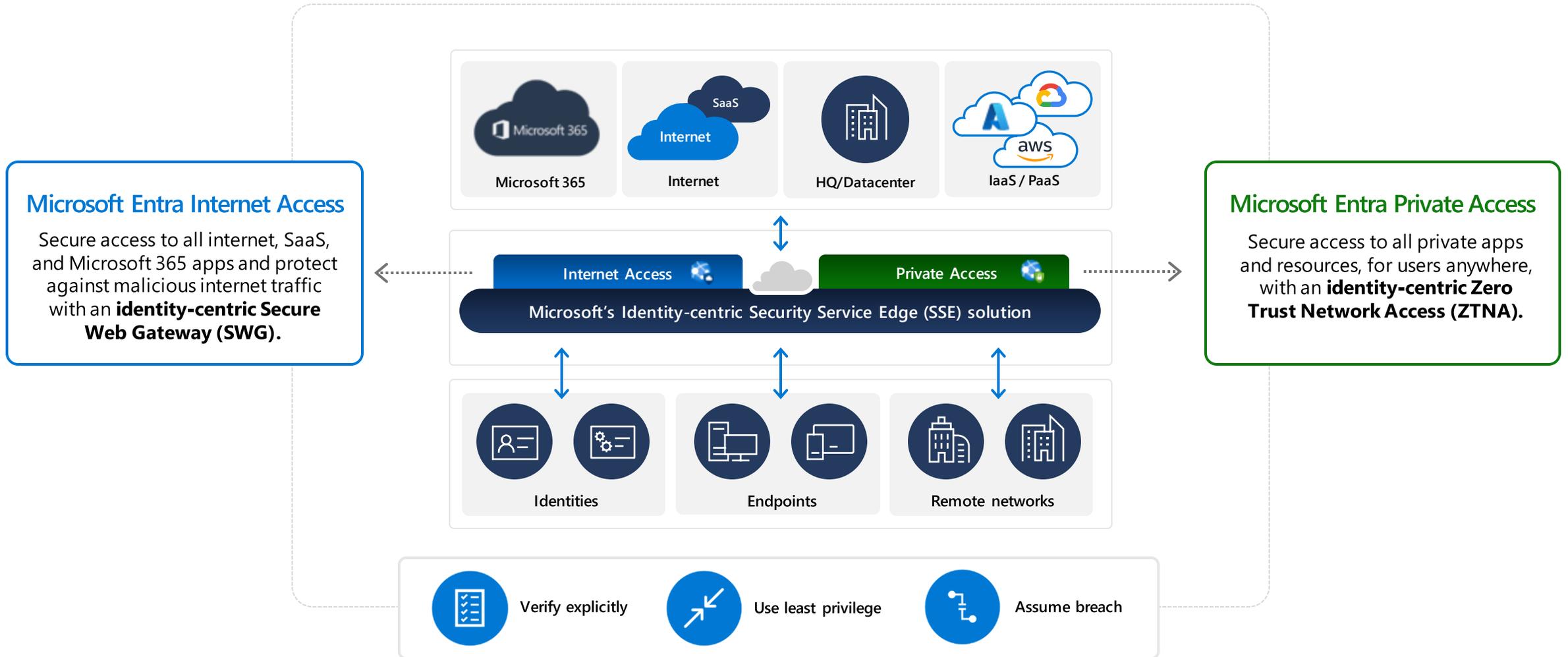
- » Inconsistent and inefficient security controls
- » Security gaps from siloed solutions and policies
- » Higher operational complexities and cost
- » Poor user experience
- » Limited resources and technical skills



Microsoft's Identity-centric SSE solution



Microsoft's Identity-centric SSE solution

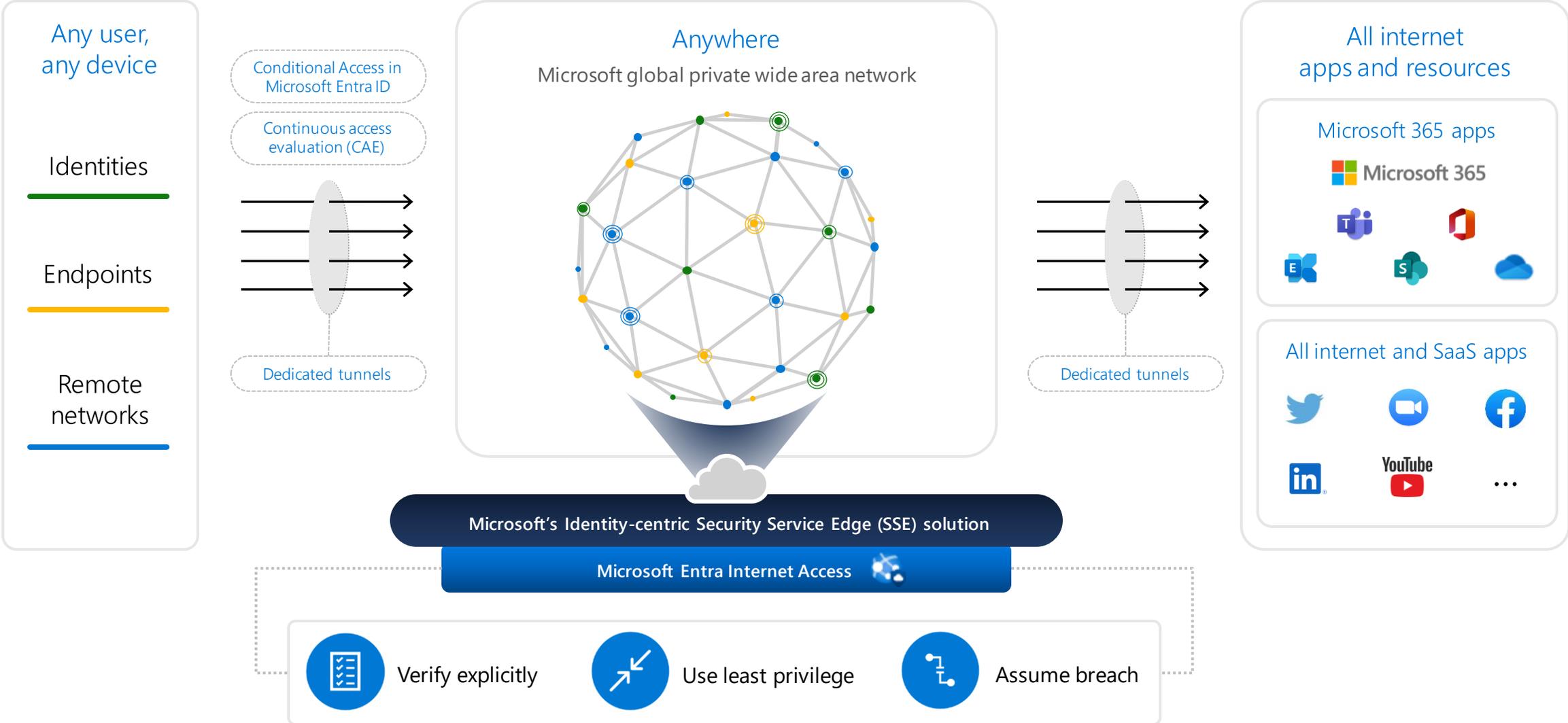


Microsoft Entra Internet Access (Preview)



Microsoft Entra Internet Access

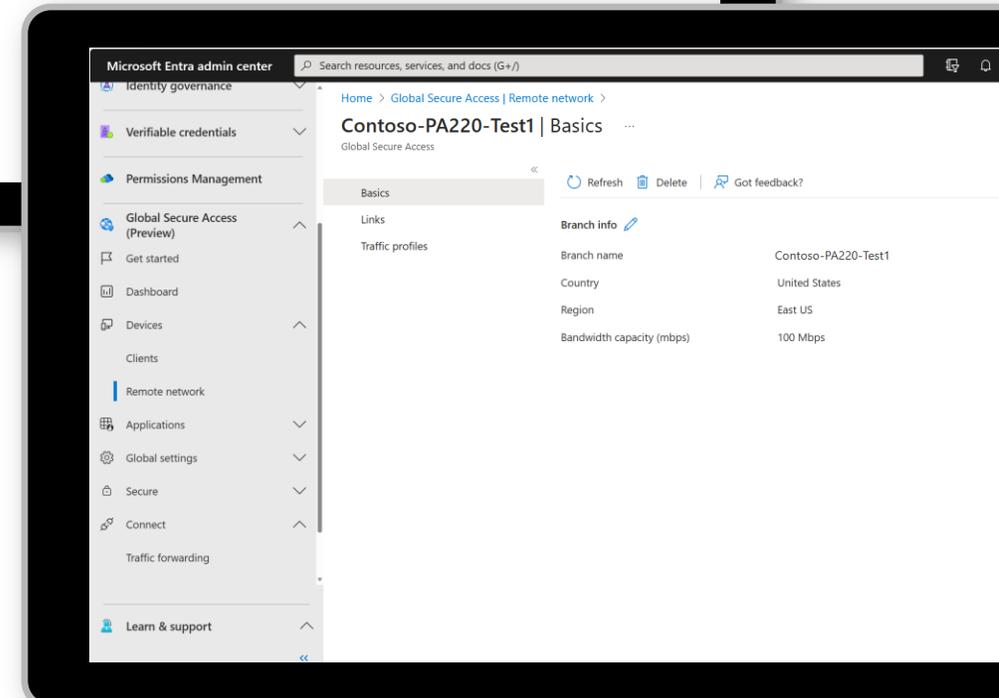
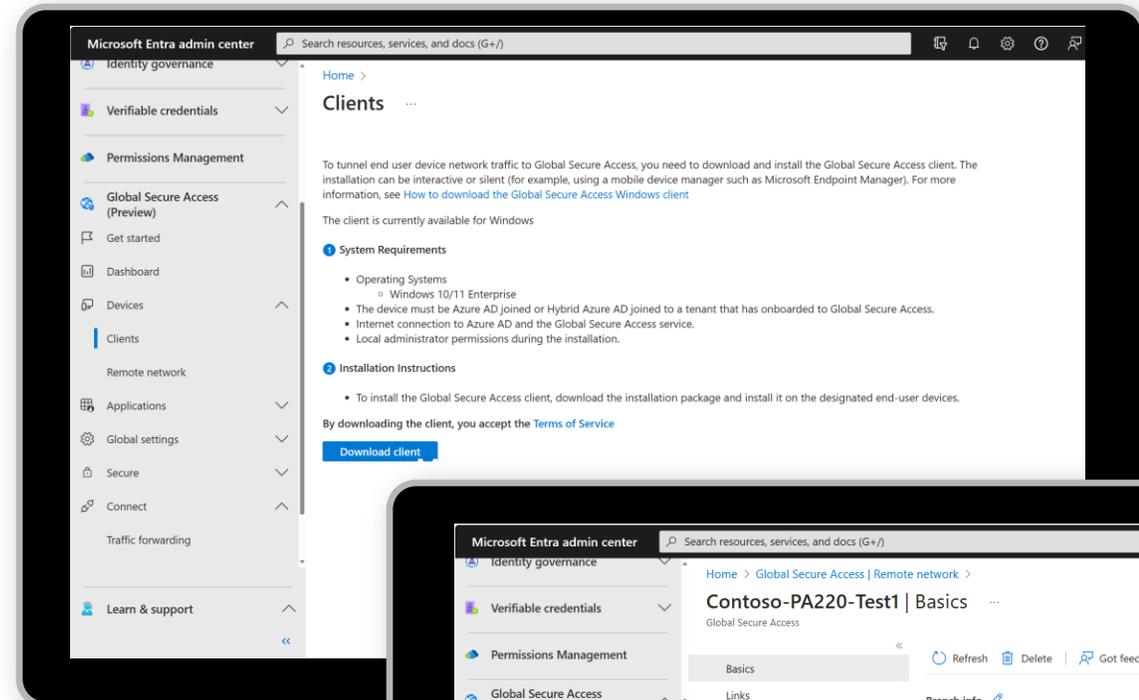
An identity-centric Secure Web Gateway (SWG) solution



Client and branch connectivity

Connect from any device, any network

- » All OS types supported for client connectivity
 - » **Public preview:** Support for Windows, Android
 - » **Coming soon:** MacOS, iOS
 - » **Coming soon:** Inbuilt into Windows OS stack
 - » **Coming soon:** One Client (Integrated with Microsoft Endpoint Manager, Microsoft Defender for Endpoint)
- » Branch office support through IPSec VPN tunnels
 - » **Private preview:** Support for all mainstream CPE providers
- » Side-by-side support with 3rd Party SSE / Traditional DMZ



Deep Identity Integrations



Zero Trust access

Universal Conditional Access and **continuous access evaluation** to any endpoint

- » Verify users and conditions before granting access to network
- » Block access to any network destination if Conditional Access checks fail
- » Instantaneously revoke access when conditions change – continuous access evaluation



Token theft protection

Easy to manage location controls integrated with Conditional Access

- » Defense in depth against token theft – verify user access from your tenant's trusted connectivity
- » Easy to manage and no hair-pinning of users necessary
- » Restore user's original Source IP in Conditional Access, Risk detection, activity logs



Data exfiltration control

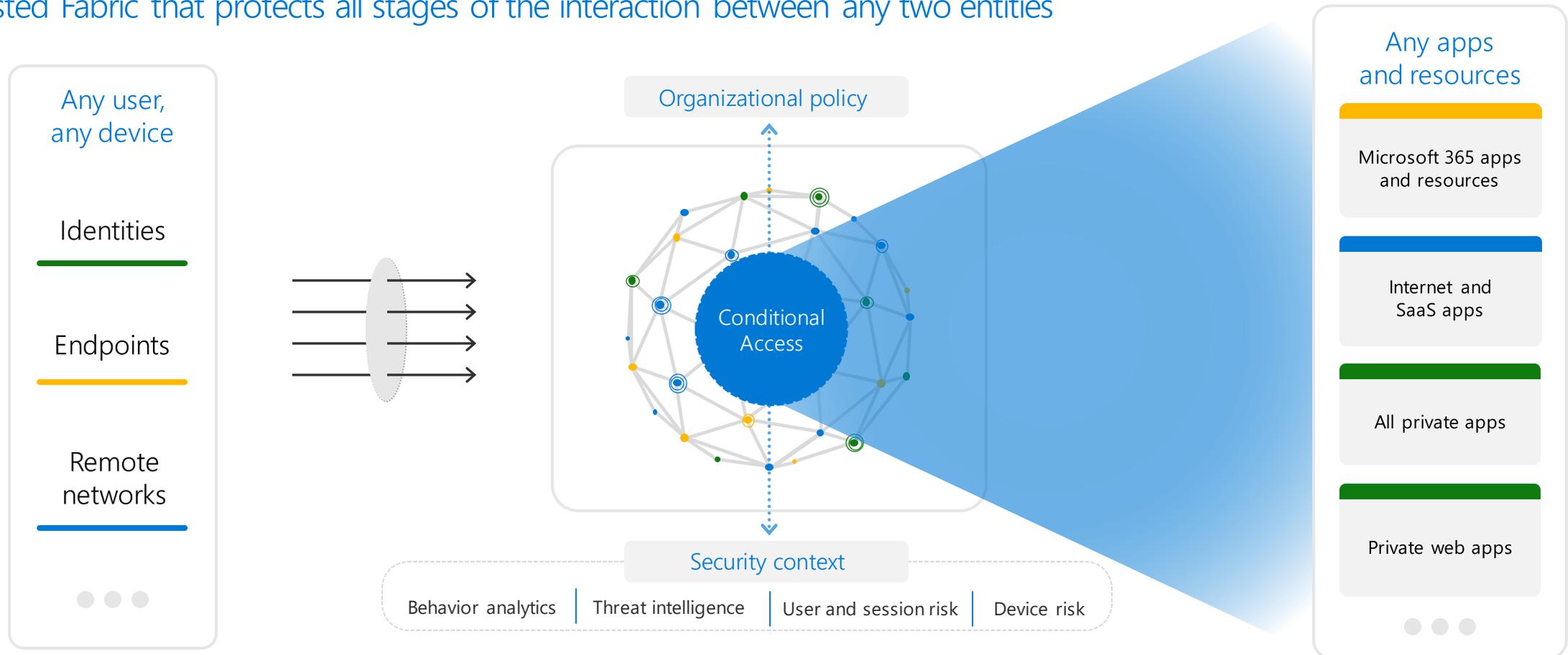
Manage insider attacks by controlling foreign identities usage in your enterprise

- » Enforce granular list of foreign users and applications to allow
- » Protect Microsoft 365 apps against token infiltration and anonymous access
- » Protection without compromising user productivity and performance

Conditional Access - Microsoft's Adaptive Access Vision

Trusted Fabric that protects all stages of the interaction between any two entities

<https://aka.ms/MCRA>



Centralized control

Unified Zero Trust architecture and policy engine simplifies management of access controls and technologies (Directory, SSO, Federation, RBAC, proxy, and more)

Consistent enforcement

Centralized policy is consistently applied across all resources where the action happens (identity, data, network + infra and apps across cloud, on-premises, IoT, OT, and more)

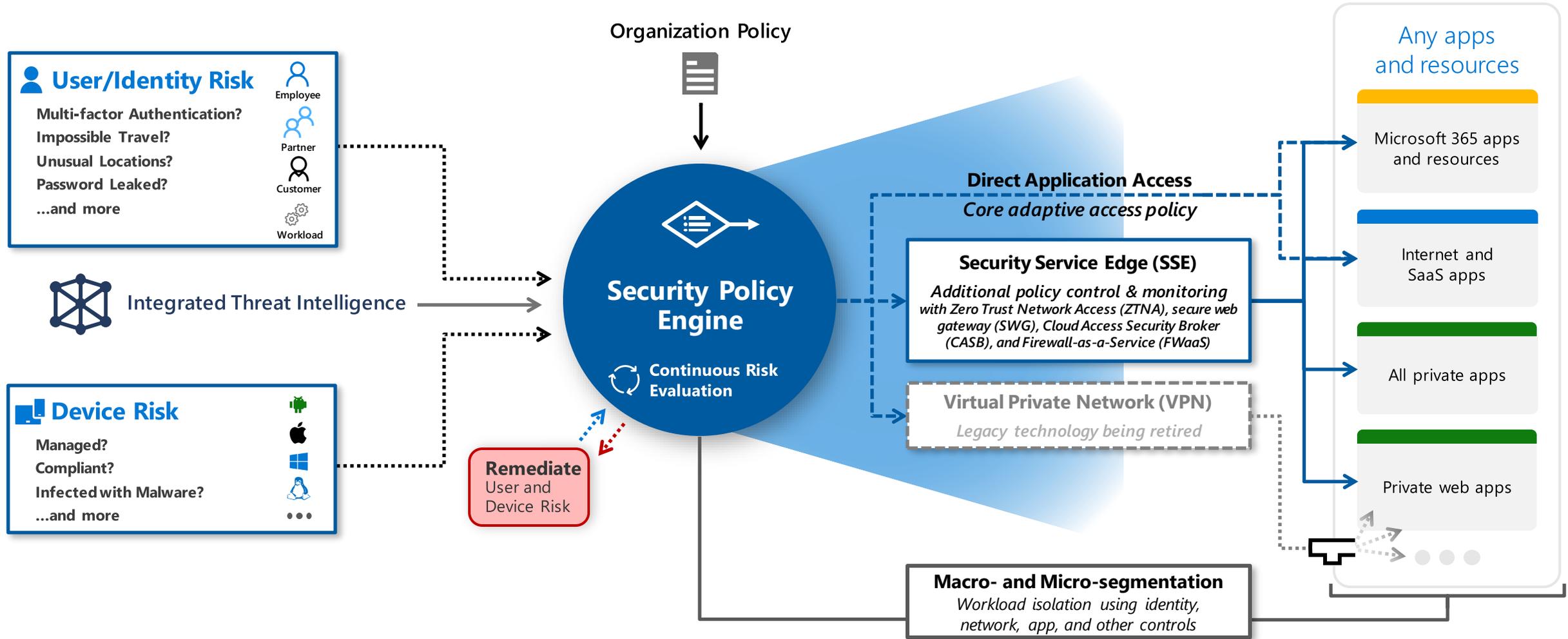
Access Management Capabilities

Adaptive Access applying Zero Trust Principles

Legend

- Trust Signal
- Adaptive Access Policy
- Threat Intelligence
- Additional Policy & Monitoring

Can be implemented today using Microsoft and partner capabilities



Signal

to make an informed decision



Decision

based on organizational policy



Enablement and Enforcement

of policy across resources

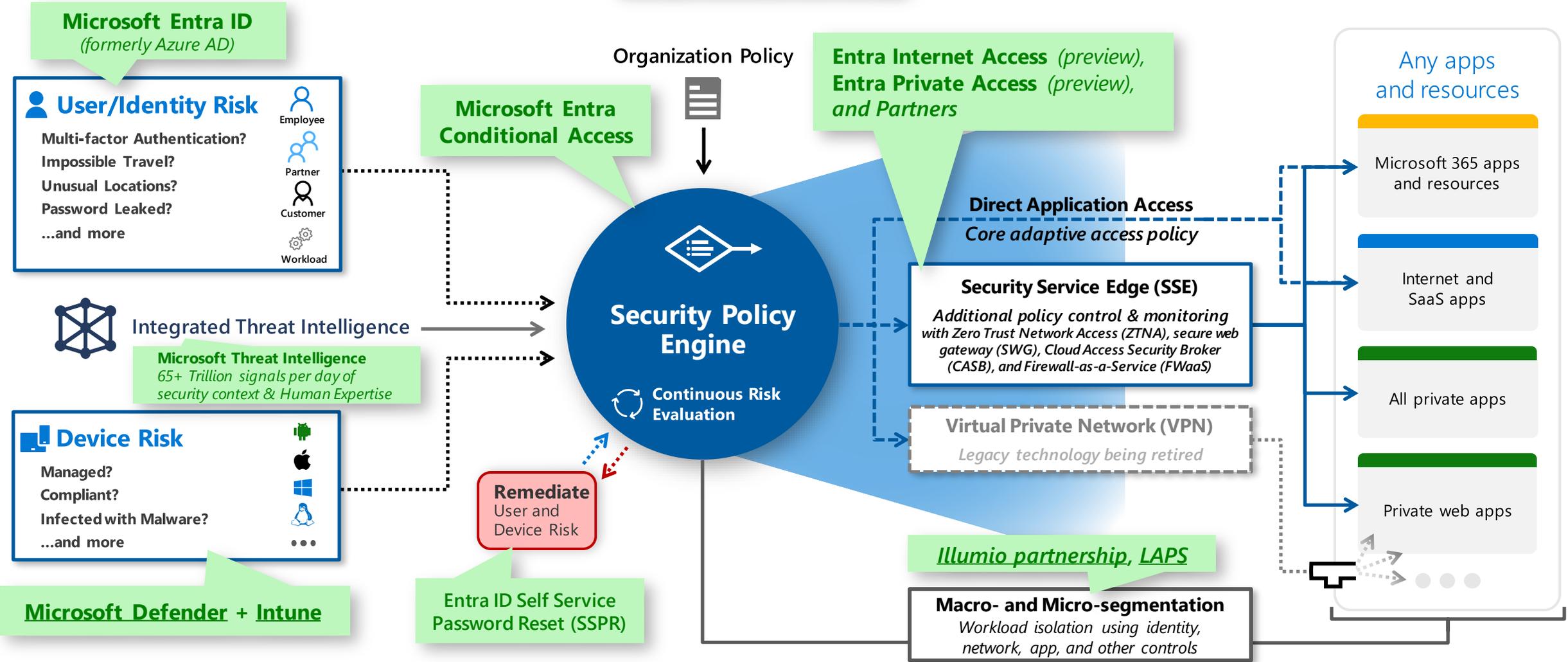
<https://aka.ms/MCRA>

Access Management Capabilities

Adaptive Access applying Zero Trust Principles *Using Microsoft Technology*

Legend
 Trust Signal
 --- Threat Intelligence
 - - - Adaptive Access Policy
 — Additional Policy & Monitoring

Can be implemented today using Microsoft and partner capabilities



Signal
to make an informed decision

Decision
based on organizational policy

Enablement and Enforcement
of policy across resources

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

The screenshot displays the Microsoft Entra admin center interface for configuring a Conditional Access policy. The policy name is "Require MFA for GlobalSecureAccess". The configuration is as follows:

- Select what this policy applies to:** Global Secure Access (Preview)
- Select the traffic profiles this policy applies to:**
 - M365 traffic
 - Public traffic
 - Private traffic
- Target Resources:** 1 network traffic profile selected
- Conditions:** 0 conditions selected
- Access controls:** 1 control selected

Leverage Conditional Access to validate access for any network destination

Extend Condition Richness to Network Filtering

Leverage rich user, device, location awareness of Conditional Access for Network security policy enforcement

The screenshot displays the Microsoft Entra admin center interface for configuring a Conditional Access policy. The policy name is "Only PR Dept can access Social Media". The policy is based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. The policy is assigned to "All users included and specific users excluded". The target resources are "1 network traffic profile selected". The conditions are "0 conditions selected". The access controls are "0 controls selected". The session condition is "Conditional Access Network Control selected".

Session

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

- Use app enforced restrictions ⓘ
- Use Conditional Access App Control ⓘ
- Sign-in frequency ⓘ
- Persistent browser session ⓘ
- Customize continuous access evaluation ⓘ
- Disable resilience defaults ⓘ
- Require token protection for sign-in sessions (Preview) ⓘ
- Use Conditional Access Network Control (Preview) ⓘ

Block Social Media sites

User and context aware network policies

Compliant Network Check

Stop user bypass of edge security stack & protect against token theft

» Prevent token thefts

- » Validate user is connecting from verified device/network of your tenant
- » Inbuilt support for tenant level granularity

» Ensures that user has not bypassed underlying security controls of SWG/SSE

» It's the better Location Control

- » All the security, without any of the Source IP management overhead
- » No need to hairpin remote users to central egress points to enforce Source IP checks
- » Integrated with Trusted location construct

» **Coming soon:** Continuous access evaluation and B2B integration

- » Integrated for instantaneous access revocation for Microsoft 365 applications
- » Availability in XTAP-B2B scenarios to validate access from partner tenants

The screenshot displays the Microsoft Entra admin center interface for configuring a Conditional Access policy. The policy is titled "Protect All Apps behind Compliant Network" and is currently "Not configured". The configuration page is divided into several sections:

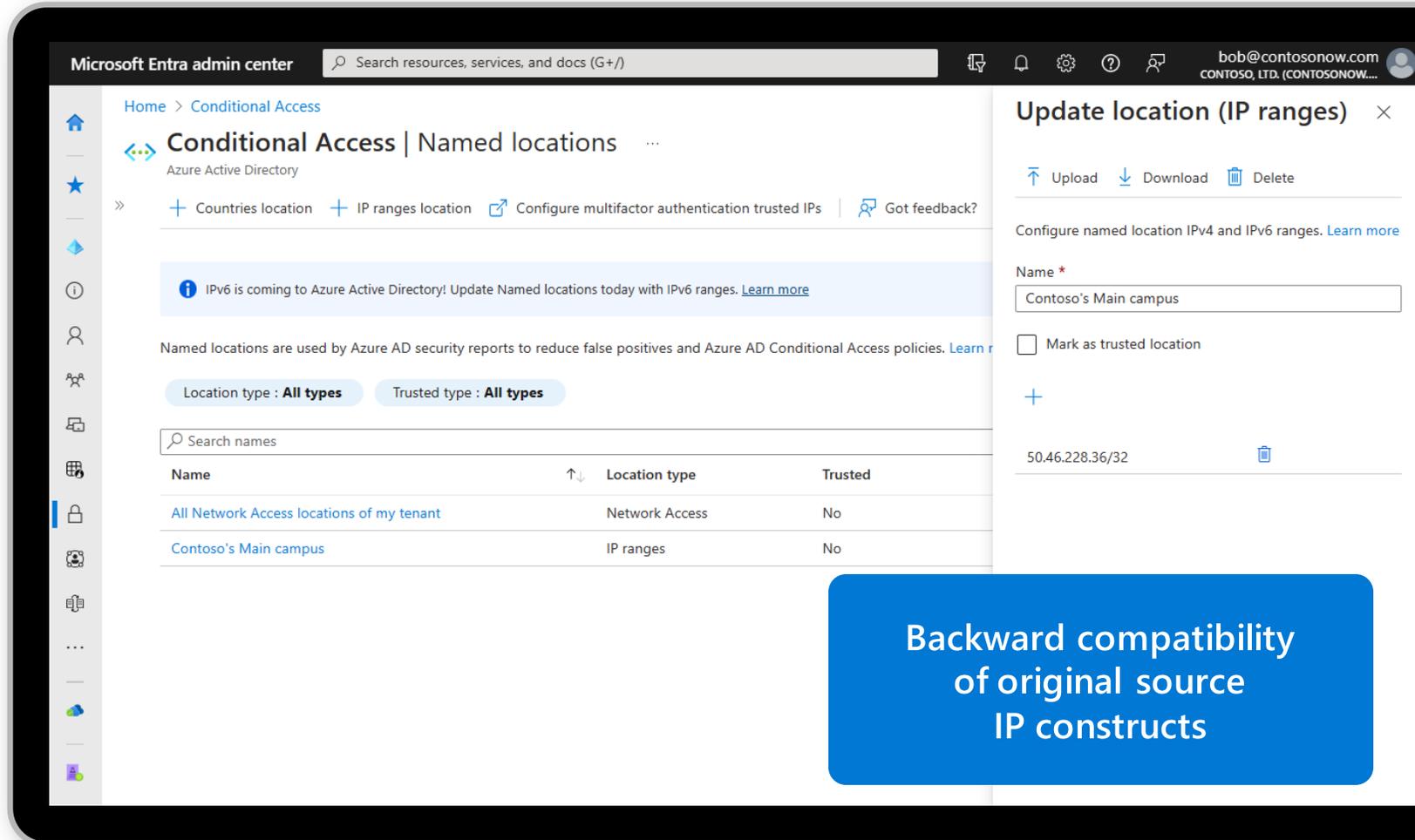
- Name:** "Protect All Apps behind Compliant Network"
- Assignments:** "Specific users included"
- Target Resources:** "All cloud apps"
- Conditions:** "1 condition selected"
- Access controls:** "Block access"
- Control access based on signals from conditions:** "Not configured" (includes User risk, Sign-in risk, Device platforms, Client apps, and Filter for devices).
- Control access based on their physical location:** "Not configured" (includes a "Configure" toggle set to "Yes" and "Include/Exclude" options).

A blue callout box in the bottom right corner of the screenshot contains the text: "Simplified management of trusted location checks".

Source IP Restoration

Backward compatibility and continuity

- » **Maintain backward compatibility** for Source IP based location checks in Conditional Access (CA)
- » **Maintain backward compatibility** for Source IP continuous access evaluation (CAE) location checks in Microsoft 365 applications (Datapath)
- » **Restore Source IP context** for all Microsoft Entra ID risk assessment – User Risk, Sign-in Risk
- » **Restore Source IP context** for all Microsoft Entra ID activity logs



The screenshot shows the Microsoft Entra admin center interface. The main content area is titled "Conditional Access | Named locations" and includes a table of named locations. A right-hand pane is open for updating a location's IP ranges.

Name	Location type	Trusted
All Network Access locations of my tenant	Network Access	No
Contoso's Main campus	IP ranges	No

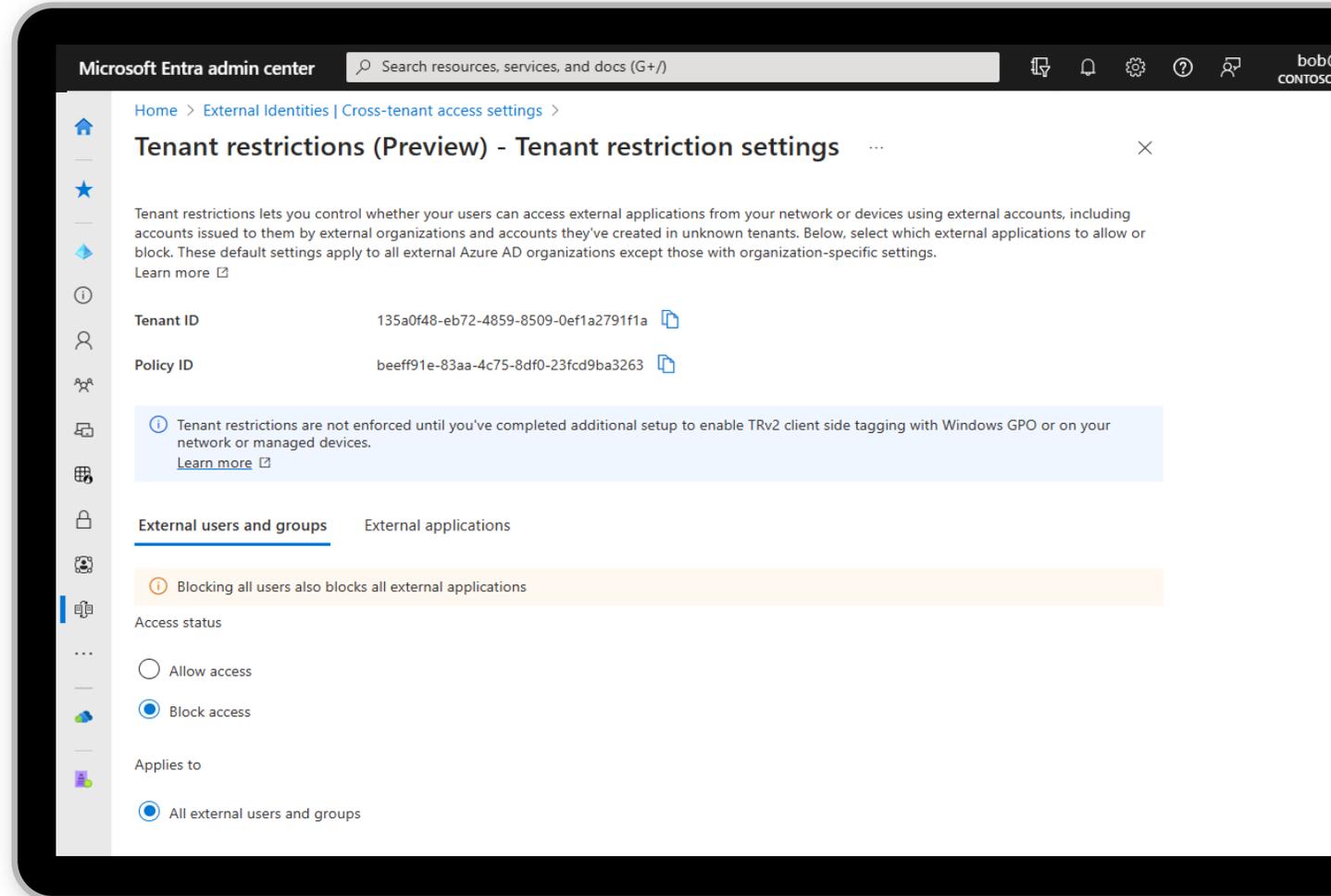
The right-hand pane, titled "Update location (IP ranges)", shows the "Name" field set to "Contoso's Main campus" and a "Mark as trusted location" checkbox. Below the table, the IP range "50.46.228.36/32" is listed with a delete icon.

Backward compatibility of original source IP constructs

Universal Tenant Restriction

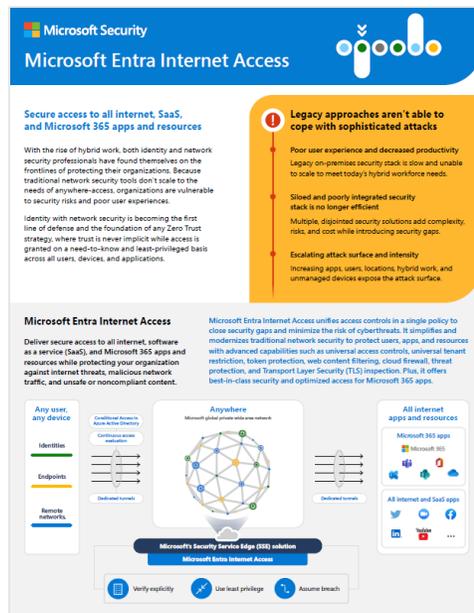
Strong data exfiltration controls

- » Microsoft Entra Internet Access integration enables Universal Tenant Restriction across all managed devices and networks (branch) agnostic of OS and Browser platform
 - » Eliminates need for enterprise managed Network proxies
 - » No need to share enterprise certs for inserting TRv2 headers
 - » Secures access for your enterprise without compromising performance/ user experience.
 - » Facilitates Cross-tenant Access monitoring
- » Microsoft Entra ID Tenant Restriction v2 (TRv2) protects against data exfiltration by foreign identities to foreign tenants
 - » TRv2 supports tenant, user, group and application granularity
 - » TRv2 enables data path coverage to protect against token infiltration and anonymous access
 - » TRv2 also has provision to control MSA access



Learn more and join Internet Access Previews

Learn more



Microsoft Security
Microsoft Entra Internet Access

Secure access to all internet, SaaS, and Microsoft 365 apps and resources

With the rise of hybrid work, both identity and network security professionals have found themselves on the frontlines of protecting their organizations. Because traditional network security tools don't scale to the needs of anywhere-access, organizations are vulnerable to security risks and poor user experiences.

Identity with network security is becoming the first line of defense and the foundation of any Zero Trust strategy, where trust is never implicit while access is granted on a need-to-know and least-privileged basis across all users, devices, and applications.

Legacy approaches aren't able to cope with sophisticated attacks

- Poor user experience and decreased productivity
Legacy on-premise security stack is slow and unable to scale to meet today's hybrid workforce needs.
- Siloed and poorly integrated security stack is no longer efficient
Multiple, digitized security solutions add complexity, risk, and cost while introducing security gaps.
- Escalating attack surface and intensity
Increasing apps, users, locations, hybrid work, and unmanaged devices expose the attack surface.

Microsoft Entra Internet Access

Microsoft Entra Internet Access unifies access controls in a single policy to close security gaps and minimize the risk of cyberthreats. It digitizes and modernizes traditional network security to protect users, apps, and resources with advanced capabilities such as universal access controls, universal tenant restriction, token protection, web content filtering, cloud firewall, threat protection, and Transport Layer Security (TLS) Inspection. Plus, it offers best-in-class security and optimized access for Microsoft 365 apps.

Deliver secure access to all internet, software as a service (SaaS), and Microsoft 365 apps and resources while protecting your organization against internet threats, malicious network traffic, and unsafe or noncompliant content.

Any user, any device
Identities
Endpoints
Remote networks

Anywhere
Microsoft global private wide area network
Dedicated tunnels

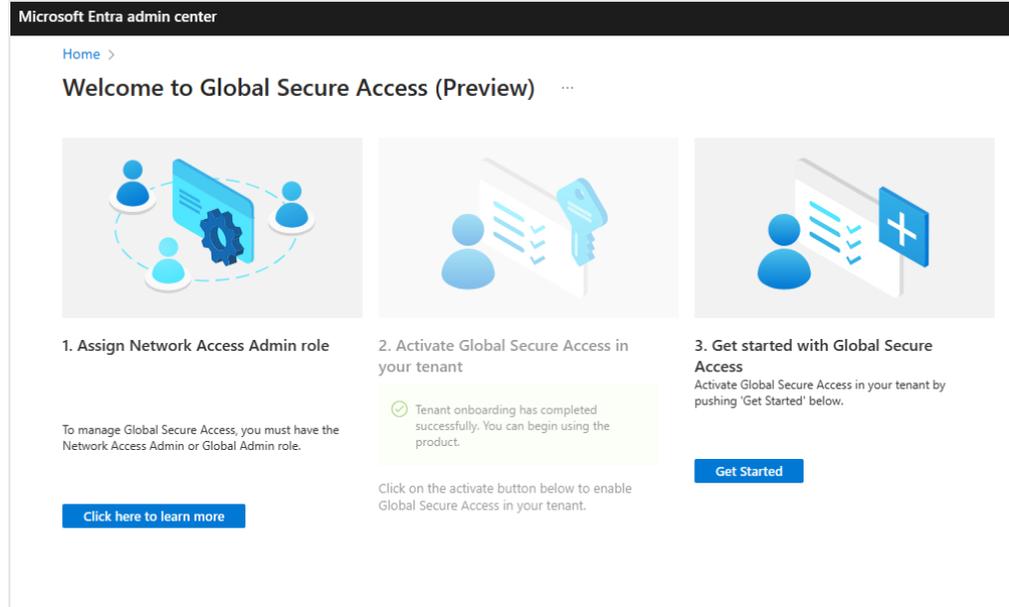
All internet apps and resources
Microsoft 365 apps
All internet and SaaS apps

Microsoft's Security Service Edge (SSE) solution
Microsoft Entra Internet Access

Verify explicitly Use least privilege Assume breach

» <https://aka.ms/InternetAccess>

Public Preview



Microsoft Entra admin center

Home >

Welcome to Global Secure Access (Preview) ...

- Assign Network Access Admin role**
To manage Global Secure Access, you must have the Network Access Admin or Global Admin role.
[Click here to learn more](#)
- Activate Global Secure Access in your tenant**
Tenant onboarding has completed successfully. You can begin using the product.
Click on the activate button below to enable Global Secure Access in your tenant.
- Get started with Global Secure Access**
Activate Global Secure Access in your tenant by pushing 'Get Started' below.

[Get Started](#)

» <https://aka.ms/InternetAccessPreview>

Private Preview



Microsoft Entra Internet Access

Configuration interface for Microsoft Entra Internet Access, showing various settings and options for activation and management.

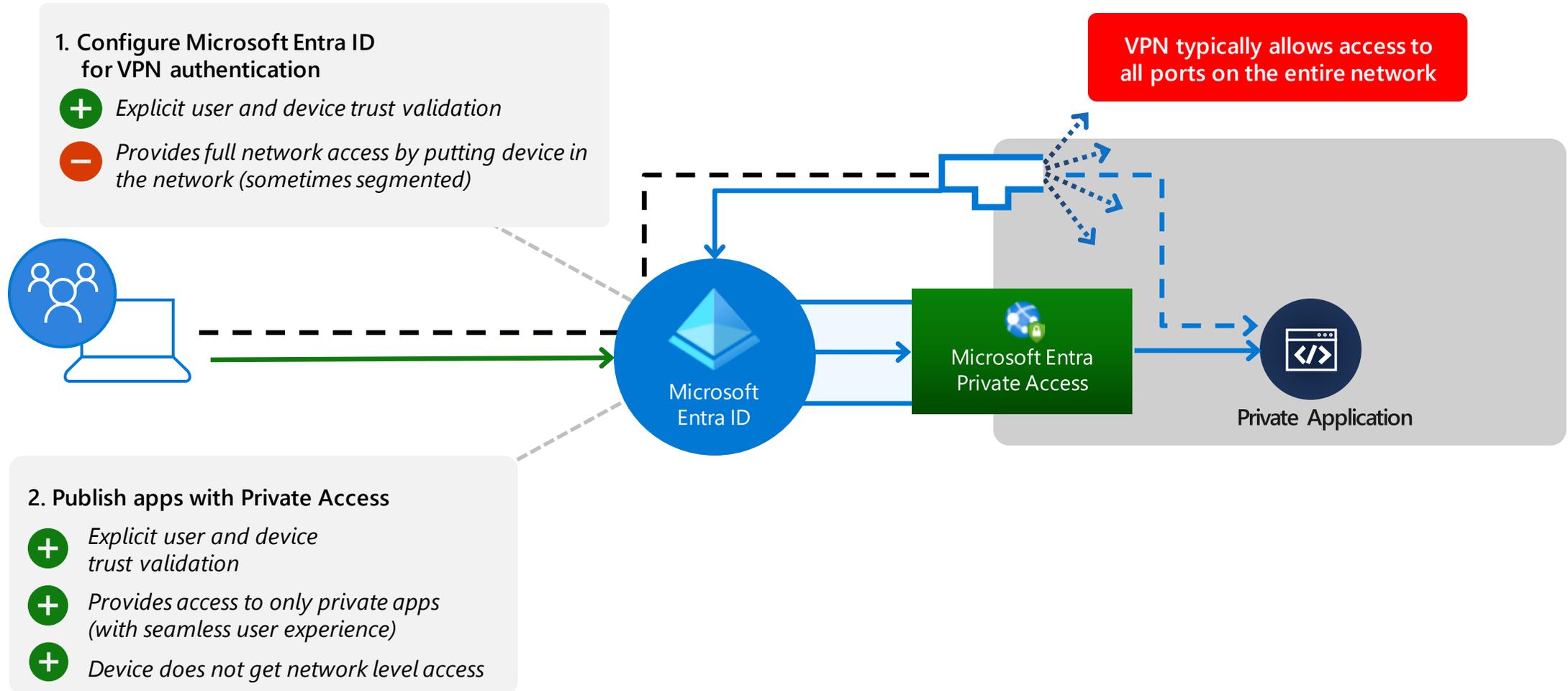
» <https://aka.ms/InternetAccessPrivatePreview>

Microsoft Entra Private Access (Preview)

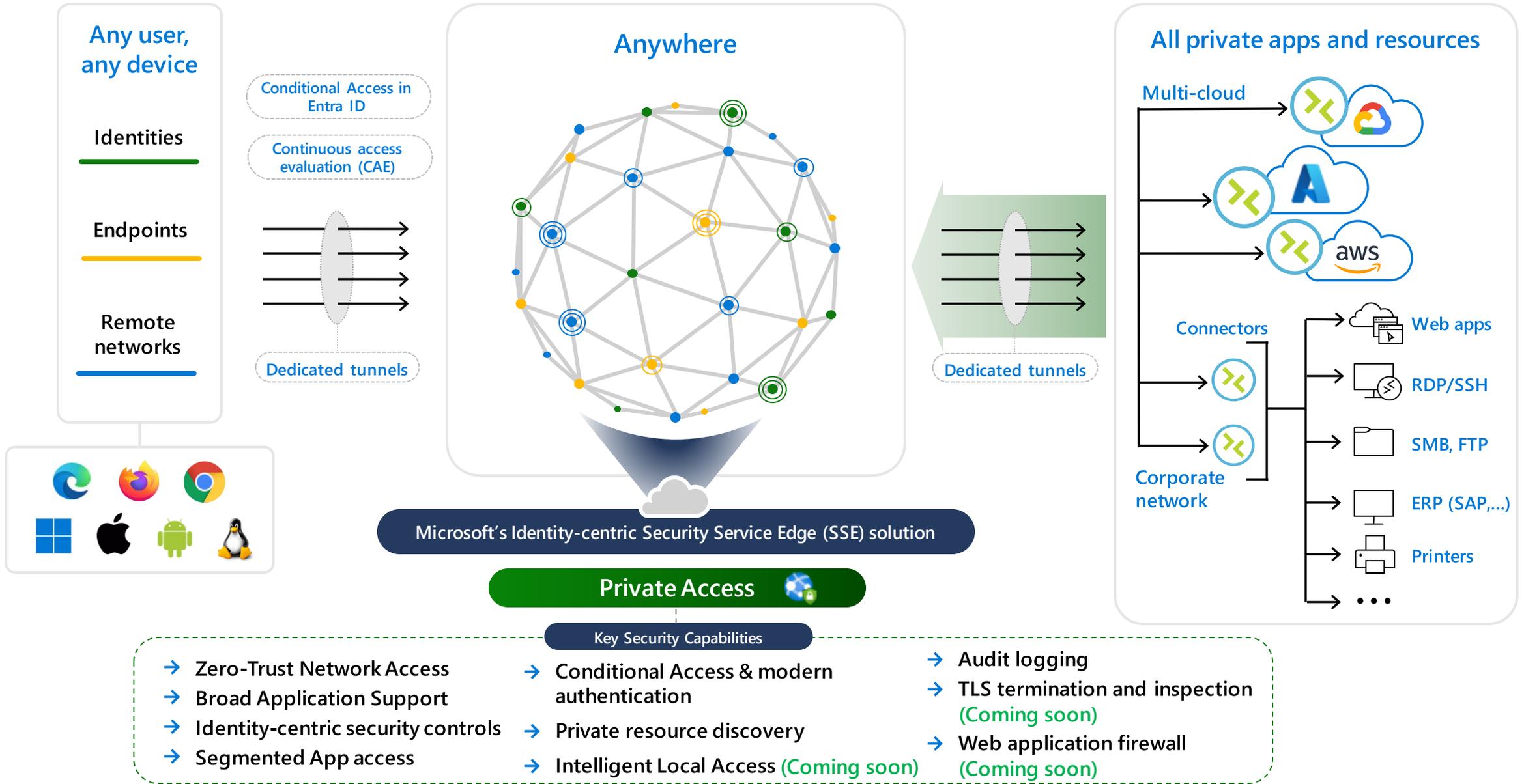


Moving beyond VPNs

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



Microsoft Entra Private Access - How it works



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

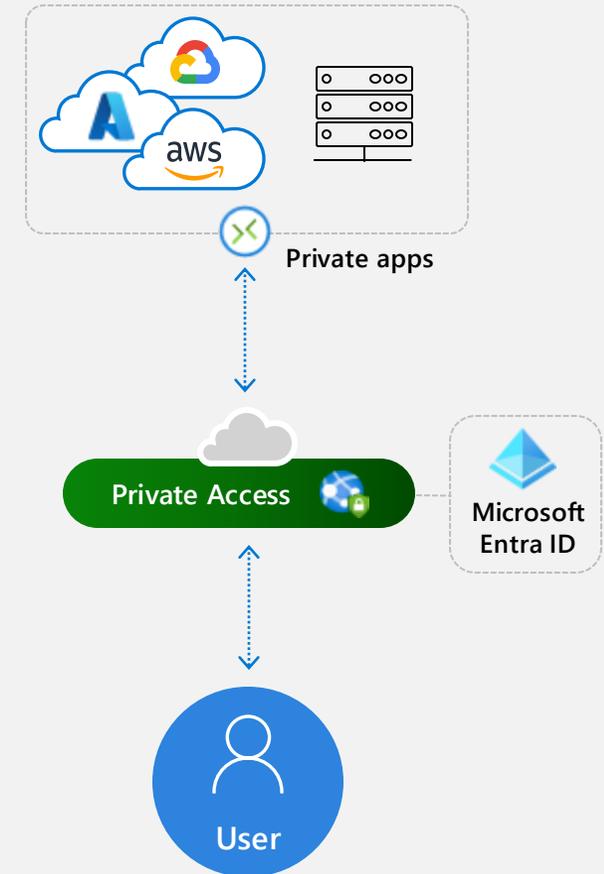
Coming soon: Micro-segment based on process identity

» 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)

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

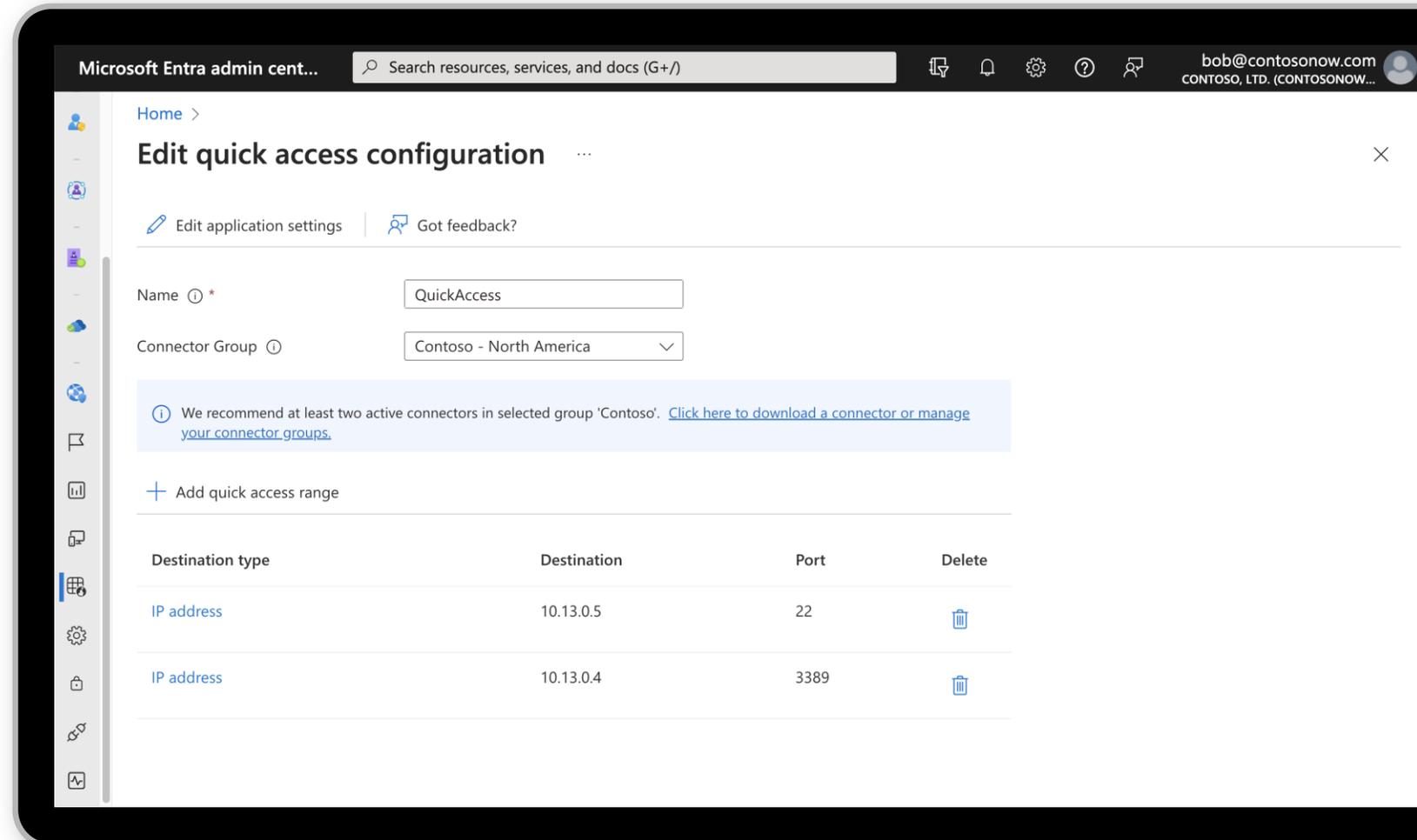
» Flexibility

Supports IP range, IP addresses, FQDNs, or wildcard suffixes

» Segmented Private Access

Next step in Zero Trust Network Access journey

Onboard/register discovered apps to Entra ID



Segmented Per-app Access

Segment your traditional network-based access to specific private apps

The screenshot displays the Microsoft Entra admin center interface. The top navigation bar includes the text "Microsoft Entra admin cent...", a search bar with the placeholder "Search resources, services, and docs (G+)", and a user profile for "bob@contosonow.com" with the organization "CONTOSO, LTD. (CONTOSONOW...)". The breadcrumb path is "Home > Enterprise applications > myRDP app". The main heading is "myRDP app | Network access properties" with a sub-label "Global secure access application". A left-hand navigation pane lists various management options: Overview, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Network access properties), Security (Conditional Access), and Activity (Sign-in logs). The "Network access properties" section contains a "Got feedback?" link, a "Name" field with the value "myRDP app", and a "Connector Group" dropdown menu set to "Contoso - North America". A blue informational banner states: "We recommend at least two active connectors in selected group 'Contoso'. [Click here to download a connector or manage your connector groups.](#)" Below this is a checkbox for "Enable access with Global Secure Access client" which is currently unchecked. A "+ Add network access segment" button is present. At the bottom, a table lists the configured network access segments.

Destination type	Destination	Port	Delete
IP address	10.13.0.6	3389	

Private App Discovery

Discover and onboard private applications for segmented per-app access

» Discover apps

Discover app segments

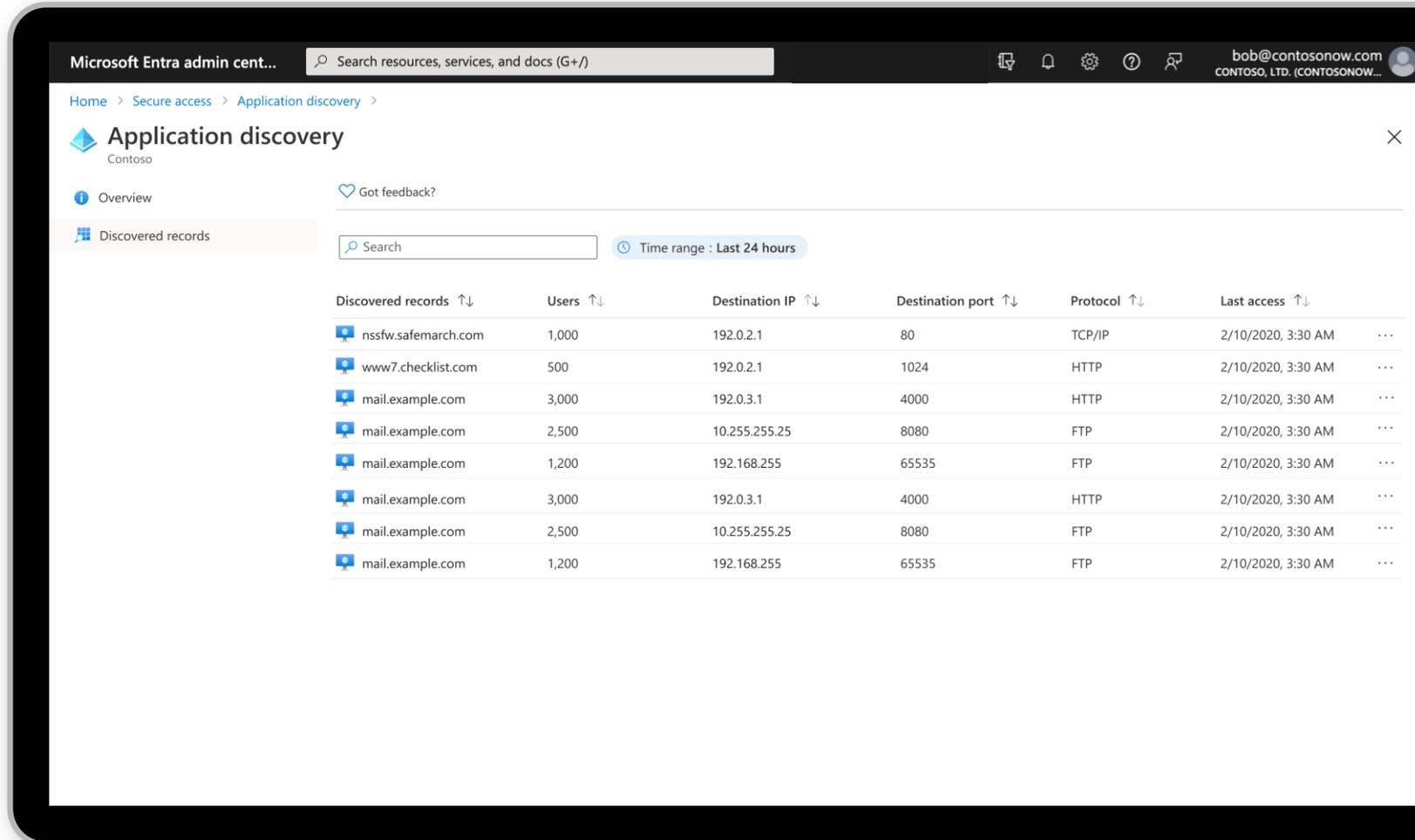
Create private apps using discovered app segments

» Analytics

See app usage trends and relevant insights like usage over time, and more

» Auto re-discovery

Intelligently add new discovered app segments to existing apps as additional app segments



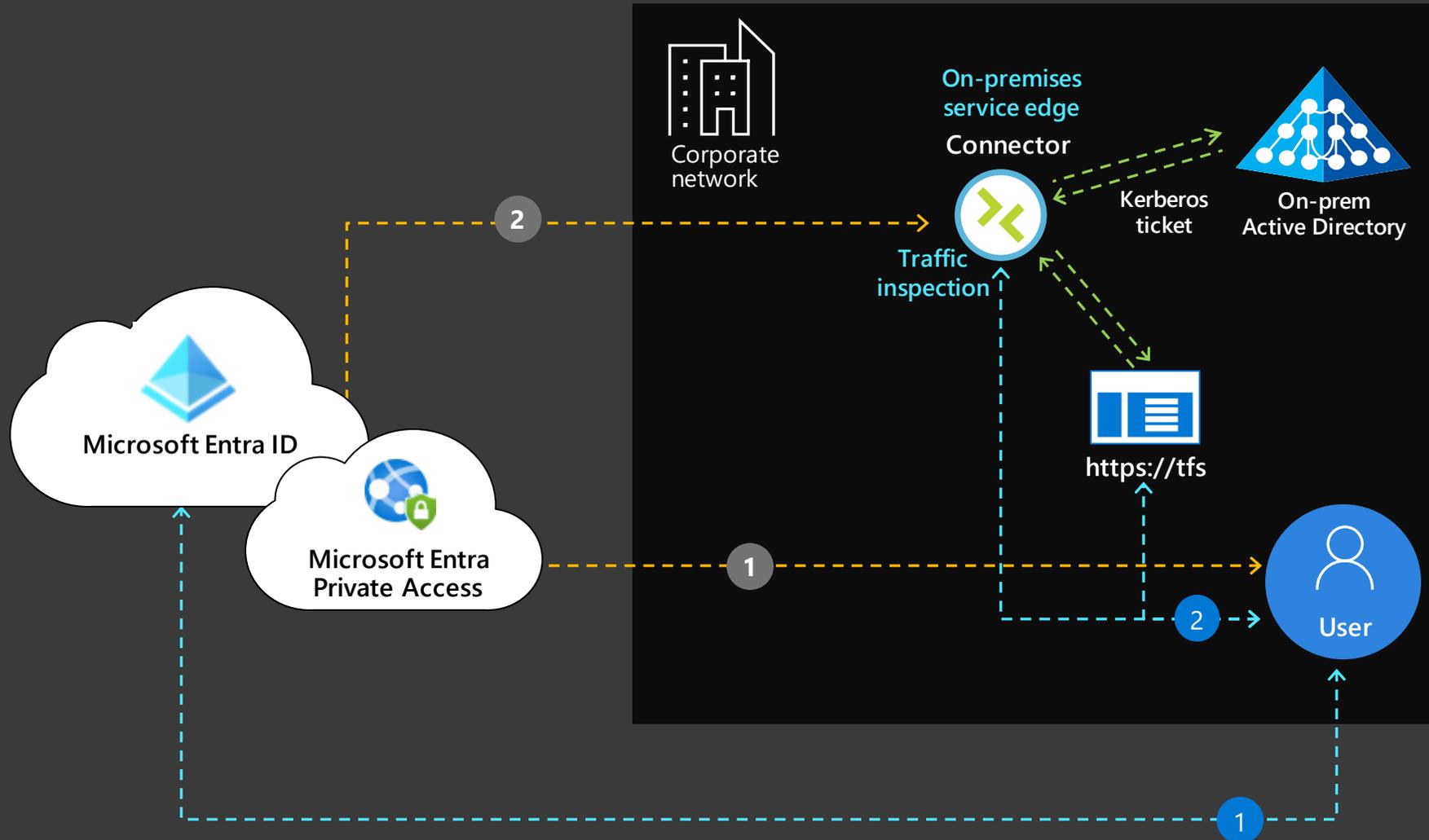
The screenshot displays the Microsoft Entra admin center interface for Application discovery. The page title is "Application discovery" for the organization "Contoso". The navigation menu includes "Overview" and "Discovered records". A search bar and a "Time range" filter set to "Last 24 hours" are visible. The main content area shows a table of discovered records with the following columns: "Discovered records", "Users", "Destination IP", "Destination port", "Protocol", and "Last access".

Discovered records	Users	Destination IP	Destination port	Protocol	Last access
nssfw.safemarch.com	1,000	192.0.2.1	80	TCP/IP	2/10/2020, 3:30 AM
www7.checklist.com	500	192.0.2.1	1024	HTTP	2/10/2020, 3:30 AM
mail.example.com	3,000	192.0.3.1	4000	HTTP	2/10/2020, 3:30 AM
mail.example.com	2,500	10.255.255.25	8080	FTP	2/10/2020, 3:30 AM
mail.example.com	1,200	192.168.255	65535	FTP	2/10/2020, 3:30 AM
mail.example.com	3,000	192.0.3.1	4000	HTTP	2/10/2020, 3:30 AM
mail.example.com	2,500	10.255.255.25	8080	FTP	2/10/2020, 3:30 AM
mail.example.com	1,200	192.168.255	65535	FTP	2/10/2020, 3:30 AM

Local Access to Private Apps

Intelligent, Smart, and Adaptive

Coming soon



Process Level Segmentation

Coming soon

The screenshot displays the Microsoft Entra admin center interface. The main content area shows the 'myRDP app | Network access properties' page. A modal dialog titled 'Edit Process Segment' is open, allowing configuration of a process-level segment. The dialog includes the following fields:

- Source type: Process
- Process Name: headtrax.exe
- Process Identity Hash or Signing Certificate Thumbprint: C05a5cdbcc40e770938c06525258591...

Below these fields are 'Apply' and 'Discard changes' buttons. A blue bracket on the right side of the dialog groups the three input fields. The background page shows a navigation pane on the left with options like Overview, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Network access properties, Custom security attributes (preview), Security, Conditional Access, and Activity. A notification banner at the bottom of the main content area reads: 'We recommend at least two active connector groups.'

Learn more and join Private Access Preview

Learn more

Microsoft Security
Microsoft Entra Private Access

Secure access to all private apps and resources—for users anywhere

With the rapid shift to a hybrid work model in recent years—plus the accelerated migration of apps and resources to the cloud—identity and network security professionals are finding themselves on the frontline of protecting their organizations. In adapting their security architecture and measures to meet today's cybersecurity challenges, identity with network security is becoming the first line of defense and the foundation of any Zero Trust strategy.

Unlike traditional approaches such as VPNs, security professionals can help to eliminate excessive access to apps and resources across the entire enterprise estate by embracing a strategy where trust is never implicit while access is granted on a need-to-know and least-privileged basis across all users, devices, and applications.

Legacy technologies may increase cybersecurity risk and complexity

- Inadequate and inconsistent network access controls**
Legacy network access tools like VPNs provide excessive access, expanding attack surface and lateral threat movement.
- Increased operational complexity**
Managing multiple solutions from different vendors across identity, network access and reporting increases security risk, cost, and complexity.
- Poor hybrid workforce experience**
Slow and inconsistent access impacts user performance and productivity.

Microsoft Entra Private Access

Built on Zero Trust principles, Microsoft Entra Private Access removes the risk and operational complexity of legacy VPNs while boosting user productivity. Quickly and securely connect remote users from any device and any network to private apps—on-premises, across clouds, and anywhere in between. Eliminate excessive access and stop lateral threat movement with automatic app discovery, easy onboarding, adaptive per-app access controls, granular app segmentation, and intelligent local access.

Microsoft Entra Private Access delivers secure, fast, and identity-driven Zero Trust Network Access (ZTNA) to private apps and resources for your hybrid workforce from anywhere.

Any user, any device
Identities
Endpoints
Remote networks

Anywhere
Microsoft global private wire network

All private apps and resources
Multicloud
On-premises
Customer network

Microsoft's Security Service Edge (SSE) solution
Microsoft Entra Private Access

Verify explicitly, Use least privilege, Assume breach

» <https://aka.ms/PrivateAccess>

Private Access Public Preview

Microsoft Entra admin center

Home >

Welcome to Global Secure Access (Preview) ...



1. Assign Network Access Admin role

To manage Global Secure Access, you must have the Network Access Admin or Global Admin role.

[Click here to learn more](#)



2. Activate Global Secure Access in your tenant

✓ Tenant onboarding has completed successfully. You can begin using the product.

Click on the activate button below to enable Global Secure Access in your tenant.



3. Get started with Global Secure Access

Activate Global Secure Access in your tenant by pushing 'Get Started' below.

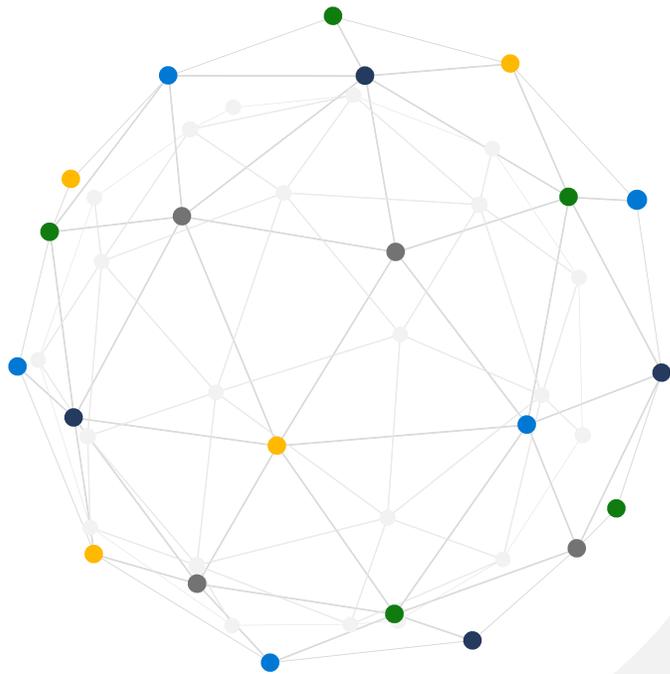
[Get Started](#)

» <https://aka.ms/PrivateAccessPreview>



Q & A

All in one place: Microsoft Entra admin center



Microsoft Entra admin center Search resources, services, and docs (G+/)

Home > Identity Governance | Azure AD roles > Privileged Identity Management | Azure AD roles > Woodgrove

Woodgrove | Access reviews

Privileged Identity Management | Azure AD roles

<< New Filter Group Settings

Access reviews for Azure AD directory roles

Search by name or owner

Role	Owner	Start Date	End Date
Workload Identity Role review			
App Proxy Connector Admin	Rupanjana Mukherjee rumu@woodgrove.ms	5/1/2023	7/30/2023
Application Developer	Rupanjana Mukherjee rumu@woodgrove.ms	5/1/2023	7/30/2023
Application Administrator	Rupanjana Mukherjee rumu@woodgrove.ms	5/1/2023	7/30/2023
app proxy custom	Rupanjana Mukherjee rumu@woodgrove.ms	5/1/2023	7/30/2023
Application Cred Rollover	Rupanjana Mukherjee rumu@woodgrove.ms	5/1/2023	7/30/2023
Global Admin			
Global Administrator	Rupanjana Mukherjee rumu@woodgrove.ms	3/1/2023	12/31/9999
AR for Workload Identity			

Quick start
Overview
Tasks
My roles
Pending requests
Approve requests
Review access
Manage
Roles
Assignments
Alerts
Access reviews
Discovery and insights (Preview)
Settings

Microsoft Entra product family

Secure access for a connected world

**Identity
and access
management**

Microsoft Entra ID
(formerly Azure AD)

Microsoft Entra
ID Governance

Microsoft Entra
External ID

**New
identity
categories**

Microsoft Entra
Verified ID

Microsoft Entra
Permissions
Management

Microsoft Entra
Workload ID

Microsoft Entra
Internet Access

Microsoft Entra
Private Access

Network access



Customer success stories across every industry



Financial services

"With conditional access policies to mandate that devices are enrolled in Azure AD, Intune, Privileged Identity Management, and multifactor authentication, creating a consolidated basis for Zero Trust is a straightforward process."



Government

"That's the power of the solution for us. It supports the integration of legacy applications, in whatever state they are in, to talk to the new identity management component."



Healthcare

"Conditional Access in Microsoft Entra ID is essential for us. Having that level of security across domains, being able to lock down identities from countries we don't deal with but are known for malware, and using multifactor authentication improves our security posture and reduces stress for my team."



Higher education

"With Microsoft Entra ID, we've built a robust ecosystem to ensure that people are who they say they are, using their attributes in multiple ways, like role-based access control. It makes everyone's life easier."



Retail and consumer goods

"Microsoft's commitment to improving security and the cloud is clear. It is the relationship that has allowed us to securely implement Microsoft Entra ID at our scale."



Professional services

"It was a eureka moment for our employees to sign in, see their tools, and not have to sign in to different systems for other tasks... there was no pushback—our Microsoft Entra ID rollout provided a fantastic experience."



Manufacturing

"There aren't too many vendors on the planet that can create a solution capable of providing consolidated insights into large, complex environments like ours. That's why we chose Microsoft."

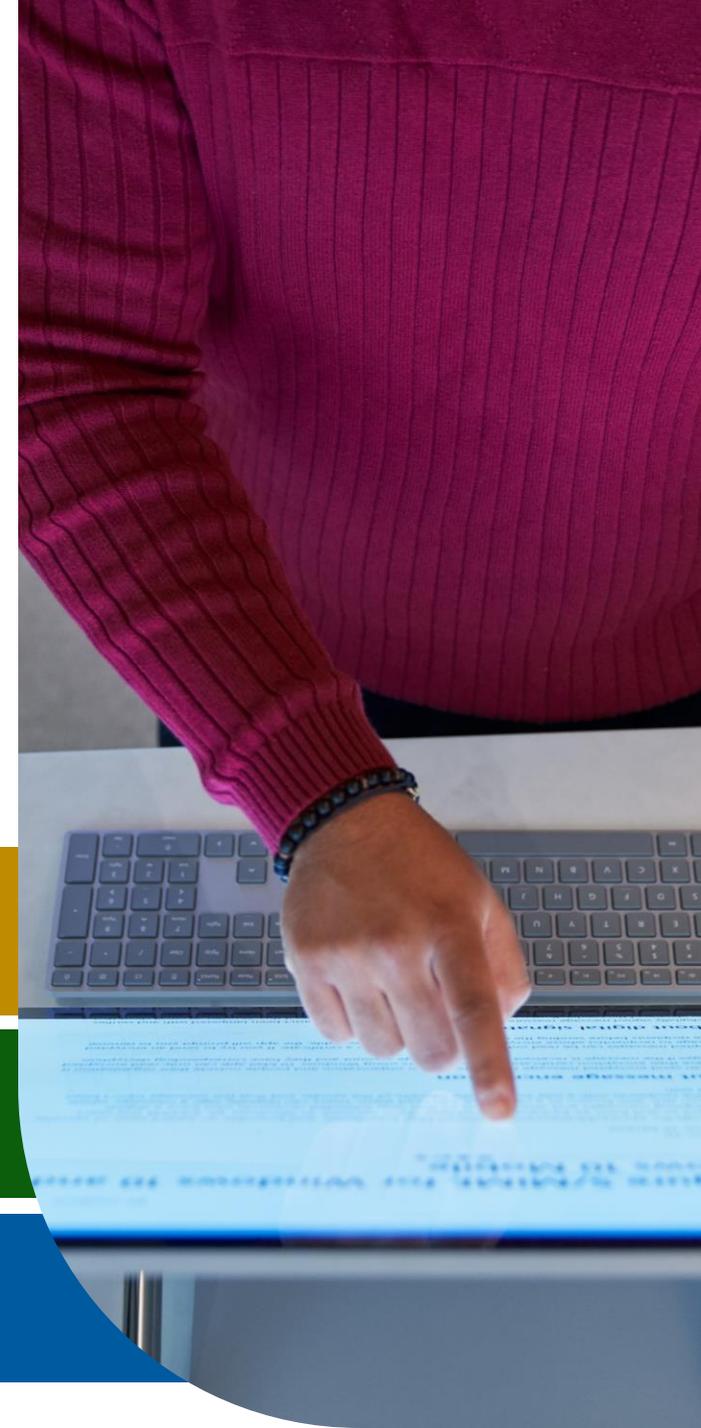


Non-profit

"Enabling a Zero Trust approach with the strong authentication of Microsoft Entra ID and endpoint management of Microsoft Endpoint Manager ensures the high level of security and compliance Derby County Community Trust requires."

Best resources

- > Microsoft Security identity blog
aka.ms/identityblog
- > Microsoft Entra product family page
microsoft.com/entra
- > Microsoft Entra admin center
entra.microsoft.com
- > Product trials
aka.ms/securityfreetrial
- > Microsoft Entra ID product page
aka.ms/EntraID
- > Permissions Management product page
aka.ms/PermissionsManagement
- > External ID product page
aka.ms/External-ID
- > Microsoft Internet Access product page
aka.ms/InternetAccess
- > Microsoft Private Access product page
aka.ms/PrivateAccess
- > Verified ID product page
aka.ms/verifyonce
- > ID Governance product page
aka.ms/identitygovernance
- > Workload ID product page
[Microsoft Entra Workload Identities](https://Microsoft.com/Entra/WorkloadIdentities)
[Microsoft Security](https://Microsoft.com/Security)





Thank you.



Microsoft Entra and Security Copilot

Working together to protect at machine speed



Enable IT admins to **discover high risk users, overprivileged access and suspicious sign-ins**



Investigate identity risks and help troubleshoot daily identity tasks



Get instant risk summaries, steps to remediate, and recommended guidance for each identity at risk



Create Lifecycle Workflows to **streamline the process** of provisioning user access and **eliminate configuration gaps**

Benefits of AI for security

- > **Efficiency:** Prioritization and automation
- > **Speed:** Ability to understand unique cyberthreats in real time
- > **Scale:** Ability to process large volumes of data