



Microsoft's Security Service Edge (SSE) solution

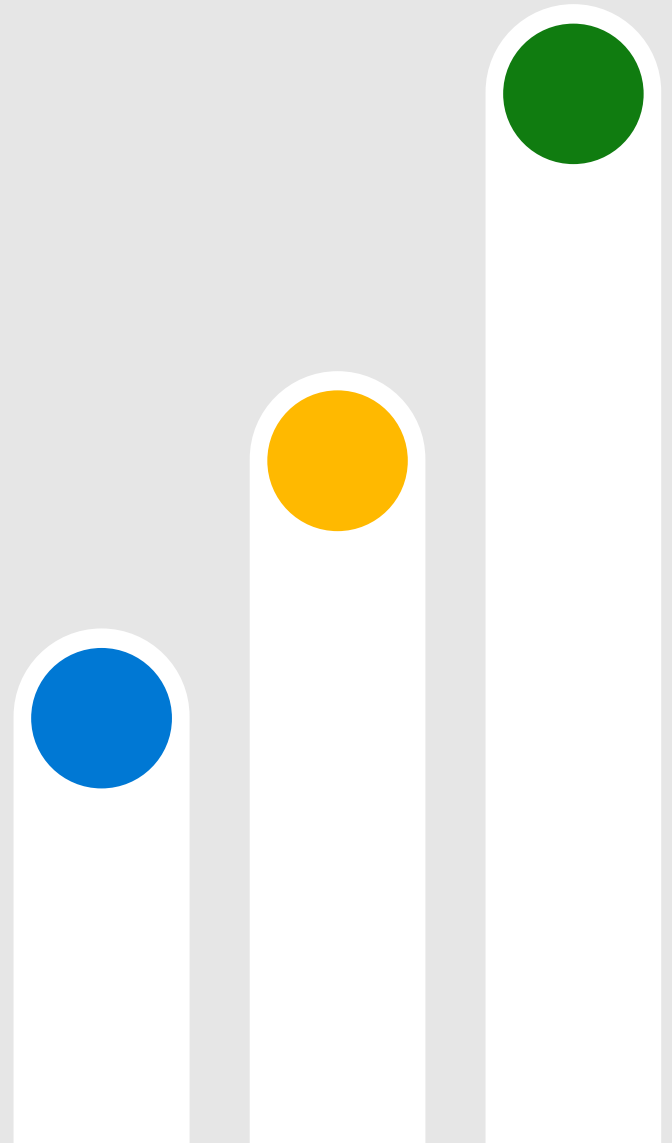
Sean McNeill, Sr. Technical Specialist – Cloud Endpoint

Microsoft Entra Internet Access
Microsoft Entra Private Access



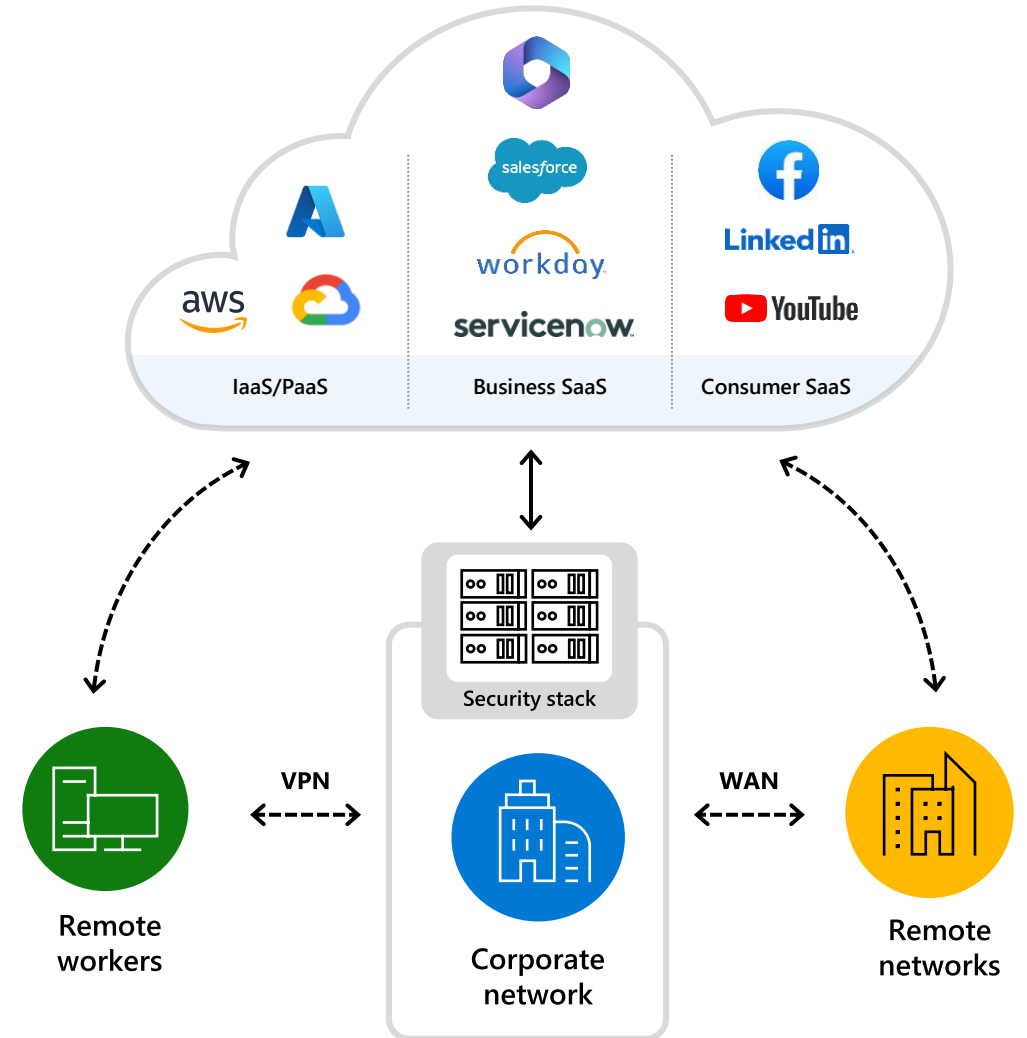
Agenda

- » Legacy network security challenges
- » Microsoft's Security Service Edge Solution
- » **Microsoft Entra Internet Access (Preview)**
- » Microsoft Entra Private Access (Preview)
- » Learn more and join product previews



Legacy network security approaches are no longer sufficient

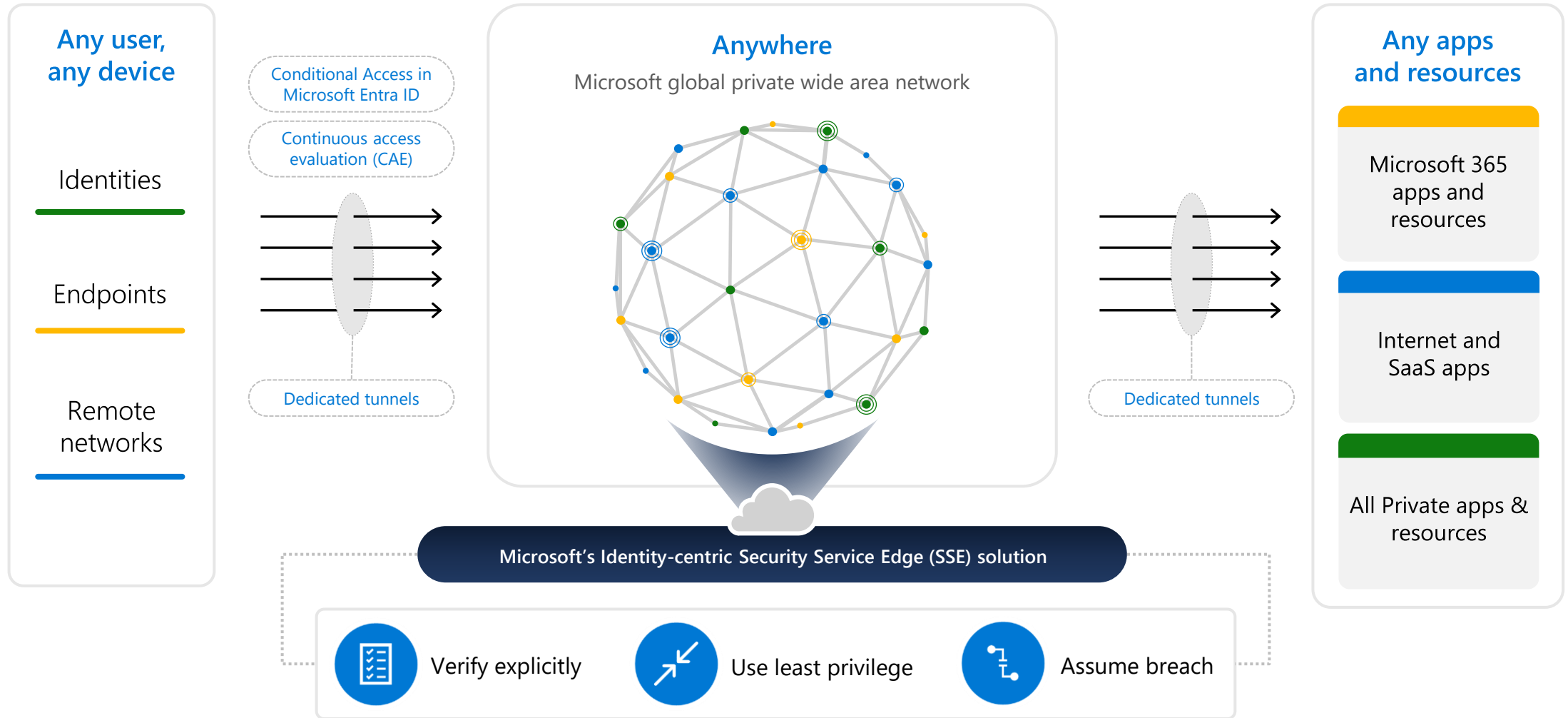
- » Inconsistent and inefficient security controls
- » Security gaps from siloed solutions and policies
- » Higher operational complexities and cost
- » Poor user experience
- » Limited resources and technical skills



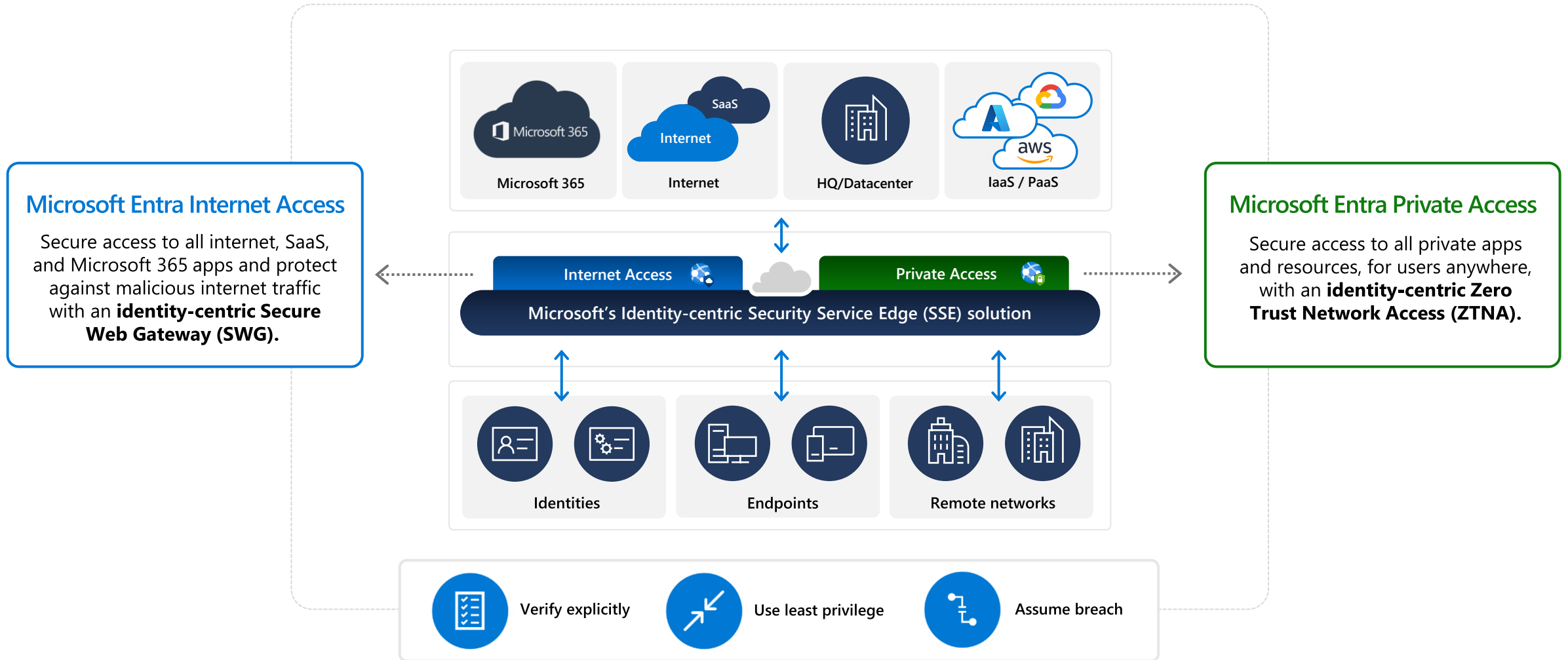
Microsoft's Security Service Edge (SSE) Solution



Microsoft's Identity-centric SSE solution



Microsoft's Identity-centric SSE solution



Microsoft's identity-centric SSE solution

An identity-centric security service edge (SSE) solution

Microsoft Entra Internet Access

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

Microsoft 365 apps

All internet apps

Microsoft Entra Private Access

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

Private web apps

All private apps

July 11th, 2023

Legend

GA

Public preview

Private preview

Microsoft's SSE unique differentiations

Deep integration with identity

The diagram features a central globe with a network of nodes and connections. Surrounding the globe are six circular icons: the Microsoft 'A' logo, a shield, a hexagonal icon, a shield with a Wi-Fi symbol, the Microsoft logo, and a computer monitor icon. A dashed white line connects these icons in a circle around the globe.

Integrated fabric that **converges identity and network protection policies with Conditional Access**

Microsoft's vast global network

The diagram shows a globe with a network of nodes and connections across all continents. Below the globe are four data points in rounded rectangles: 70 Azure regions, 170+ edge sites, 225k+ miles of fiber, and 20k+ peering connections.

70 Azure regions
170+ edge sites
225k+ miles of fiber
20k+ peering connections

Fast and seamless access to all apps and resources, milliseconds away from any resource with Microsoft's global private wide area network

Enhance security and visibility

The diagram illustrates the integration of various services. At the top, there are two clouds: a yellow one for 'Microsoft 365 apps' and a blue one for 'Internet apps and private apps'. Below them are two bars: a yellow one for 'Microsoft Entra Internet Access' and a blue one for 'Third-party SSE'. At the bottom are three dark blue boxes: 'Identities', 'Endpoints', and 'Remote networks'. Bidirectional arrows connect the top two clouds to their respective bars, and the bars to the bottom boxes. Cross-connections also exist between the bars and the bottom boxes.

Microsoft 365 apps
Internet apps and private apps
Microsoft Entra Internet Access
Third-party SSE
Identities
Endpoints
Remote networks

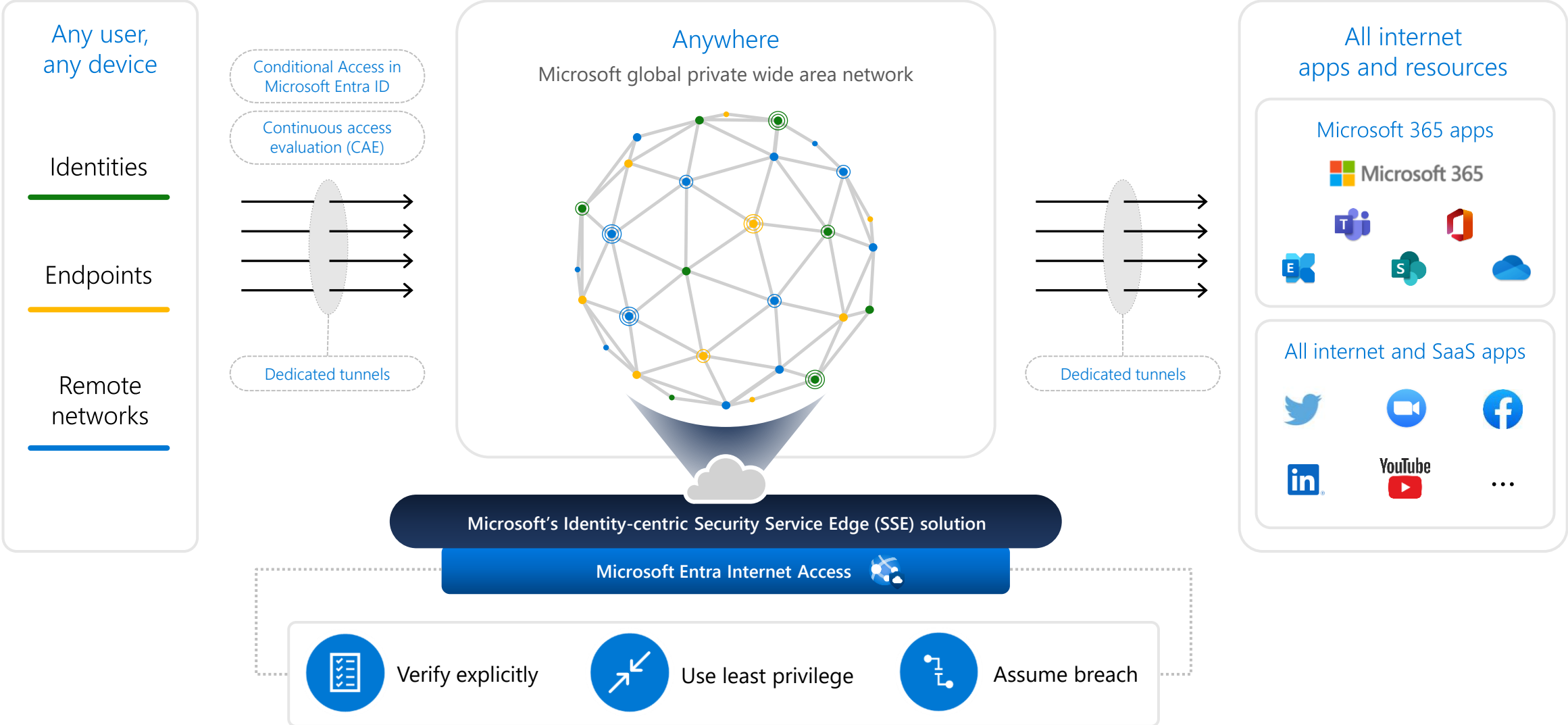
Unique **Microsoft 365 value**, with open platform that enables side-by-side deployment with other SSE solutions

Microsoft Entra Internet Access (Preview)



Microsoft Entra Internet Access

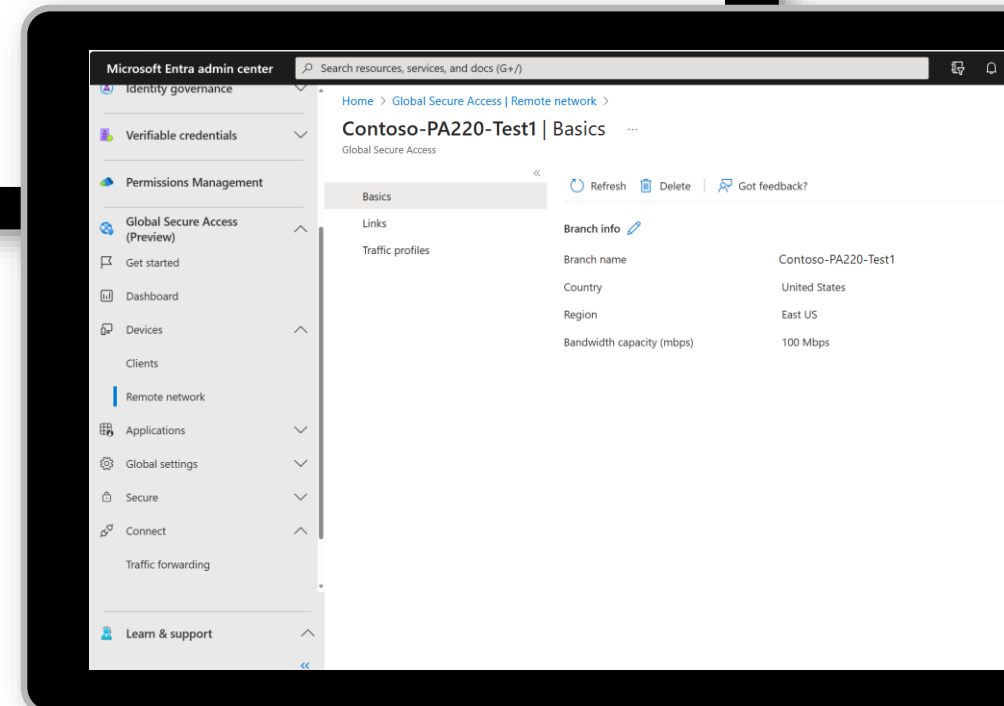
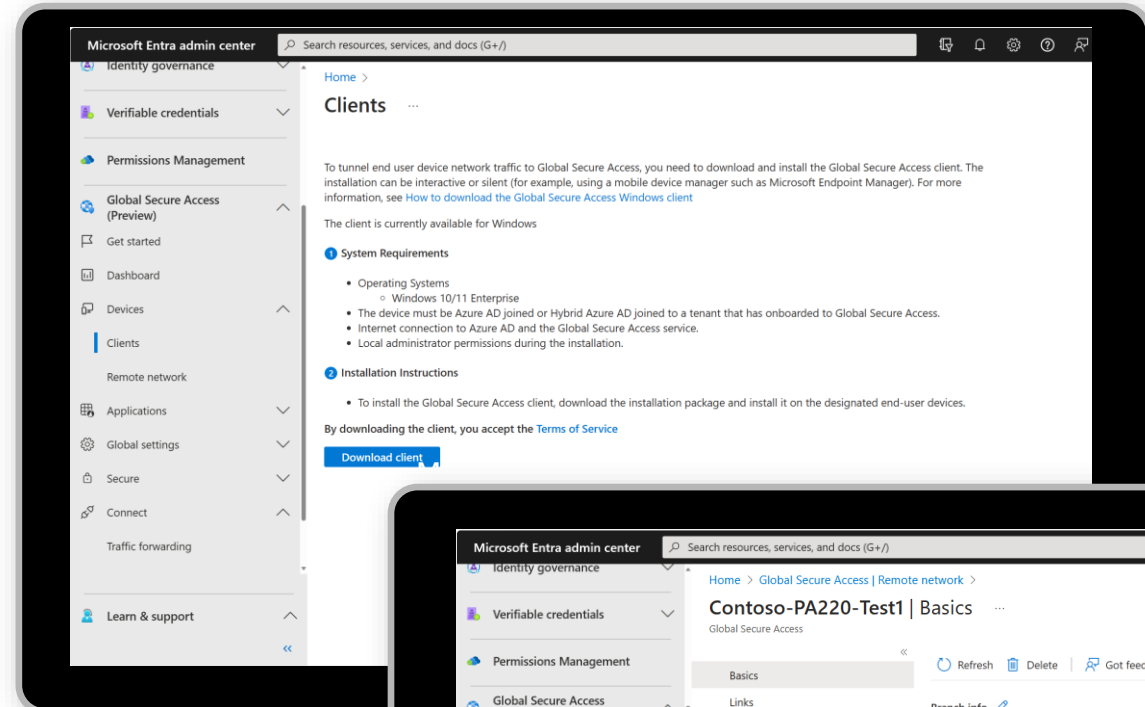
An identity-centric Secure Web Gateway (SWG) solution



Client and branch connectivity

Connect from any device, any network

- » All OS types supported for client connectivity
 - » **Public preview:** Support for Windows
 - » **Coming soon:** MacOS, Android, 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



Security Capabilities - User and Context-Aware SWG

» Identity Integrations

- » **Public preview:** Location checks and data exfiltration controls for all Microsoft Entra ID integrated Cloud Apps
- » **Public preview:** Universal Conditional Access for any network destination

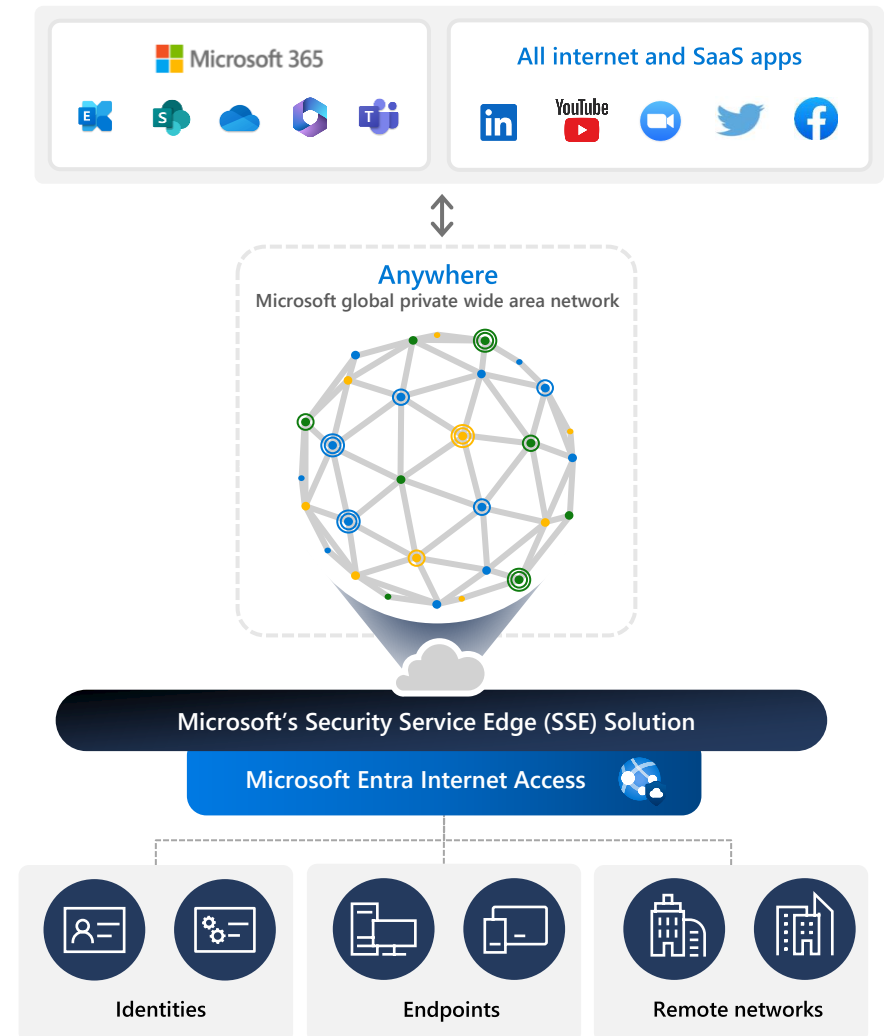
» Access control

- » **Private preview:** User/ Context aware URL/ FQDN and web category filtering
- » **Coming soon:** User/ Context aware cloud firewall (5-tuple)
- » **Coming soon:** Universal continuous access evaluation for any destination

» Threat protection

- » **Coming soon:** TLS termination and inspection
- » **Coming soon:** Threat detection & Intrusion Detection and Prevention

Features will continue to roll-in, on the road to general availability!





Seamless Microsoft 365 traffic acquisition

Zero-touch maintenance of Microsoft 365 traffic profile

- » Acquisition by Port, Protocol, IP, FQDN
- » Pre-populated Microsoft 365 traffic profile
 - » Easy to split Microsoft 365 traffic from 3rd Party SSE in side-by-side scenario
- » Easy assignment of traffic profile for acquisition
 - » Profile auto-detected by domain-joined devices
 - » Assign profile to any Customer Premises Equipment device
 - » **Coming soon:** User Group, Device Group support
- » Customizable options to either forward (acquire) or bypass specific traffic
- » **Coming soon:** Internet Access Traffic Profile

The screenshot displays the Microsoft Entra admin center interface. The left sidebar shows navigation options like Identity governance, Verifiable credentials, Permissions Management, Global Secure Access (Preview), Get started, Dashboard, Devices, Applications, Global settings, Secure, Connect, Traffic forwarding, Connectors, Monitor, and Learn & support. The main content area is titled 'Traffic forwarding' and shows a 'Microsoft 365 profile' that is enabled and applies to all Microsoft 365 traffic. It lists 'Microsoft 365 traffic policies' (3 policies) and 'Linked Conditional Access policies' (None). The 'Assignments' section shows it is applied to all client devices across 1 assigned branch. A table on the right, titled 'Microsoft 365 traffic policies', lists rules for Exchange Online and SharePoint Online and OneDrive for Business. The table has columns for Destination type, Destination, Port, Category, Protocol, and Action.

Destination type	Destination	Port	Category	Protocol	Action
Exchange Online					
FQDN	outlook.office.com	80, 443	Optimized	TCP	Bypass
IP subnet	13.107.6.152/31	80, 443	Optimized	TCP	Forward
FQDN	*.outlook.com	80, 443	Default	TCP	Forward
FQDN	*.protection.outlook...	443	Allow	TCP	Bypass
IP subnet	40.92.0.0/15	443	Allow	TCP	Forward
FQDN	autodiscover.*.onmic...	80, 443	Default	TCP	Forward
SharePoint Online and OneDrive for Business					
FQDN	*.sharepoint.com	80, 443	Optimized	TCP	Bypass
IP subnet	13.107.136.0/22	80, 443	Optimized	TCP	Forward
FQDN	sww.live.com	443	Default	TCP	Forward
FQDN	*.search.production...	443	Default	TCP	Forward
FQDN	*.wms.windows.com	80, 443	Default	TCP	Forward

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

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 is named "Require MFA for GlobalSecureAccess". The configuration is as follows:

- Name:** Require MFA for GlobalSecureAccess
- Control access based on:** 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

Demo - Universal Conditional Access

The screenshot displays the Microsoft Entra admin center interface for configuring a Conditional Access policy. The browser address bar shows the URL: `https://entra.microsoft.com/?Microsoft_AAD_ConditionalAccess=stage1&feature.canmodifystamps=true&feature.caNetworkAccess=true#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/6f155ce...`

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

Home > Conditional Access | Policies >

Require Compliant Device for Global Secure Access

Conditional Access policy

Delete | View policy information (Preview)

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

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Name *
Require Compliant Device for Global Secure...

Assignments

Users ⓘ
Specific users included

Target resources ⓘ
2 network traffic profiles selected

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Enable policy
Report-only | **On** | Off

Save

The interface includes a left-hand navigation pane with icons for Home, Favorites, and various services. The right-hand side shows the user profile for bob@contosonow.com. A mouse cursor is positioned over the '2 network traffic profiles selected' link in the Target resources section.

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 configuration includes:

- Name:** Only PR Dept can access Social Media
- Assignments:** All users included and specific users excluded
- Target Resources:** 1 network traffic profile selected
- Conditions:** 0 conditions selected
- Access controls:** Grant, 0 controls selected
- Session:** Conditional Access Network Control selected

The right-hand pane shows the "Session" control configuration with the following options:

- 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)

The selected control is "Block Social Media sites". A blue callout box in the center of the screen reads: "User and context aware network policies".

Demo – Network Filtering



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" for User risk, Sign-in risk, Device platforms, Client apps, and Filter for devices.
- Control access based on their physical location:** "Yes" (selected) for the "Include/Exclude" toggle. Under "Exclude", "Selected locations" is chosen, and "All Network Access locations of my tenant" is selected for the location list.

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

Demo - Compliant Network Check

The screenshot displays the Microsoft Entra admin center interface. The browser address bar shows the URL: `https://entra.microsoft.com/?Microsoft_Azure_Network_Access_adaptiveAccess=true&feature.caNetworkAccess=true&shown=true#view/HubsExtension/AssetMenuBlade/~/-/security/assetName/NetworkAccess...`. The page title is "Microsoft Entra admin center" and the user is logged in as "bob@contosonow.com".

The main content area is titled "Global Secure Access | Session Management". It features a search bar, a "Got Feedback?" link, and two tabs: "Tenant Restrictions" and "Adaptive Access". The "Adaptive Access" tab is active, showing a description: "Adaptive Access settings enable admins to control whether Global Secure Access signaling propagates to Azure AD Conditional Access settings. For example, enabling this feature allows Global Secure Access to restore the original client IP address of a user for IP-based policies in Azure AD."

A callout box provides additional information: "This feature adds Global Secure Access client and branch locations as Named Locations in Azure AD, and silently enables client IP restoration, when the IP is obfuscated by Global Secure Access."

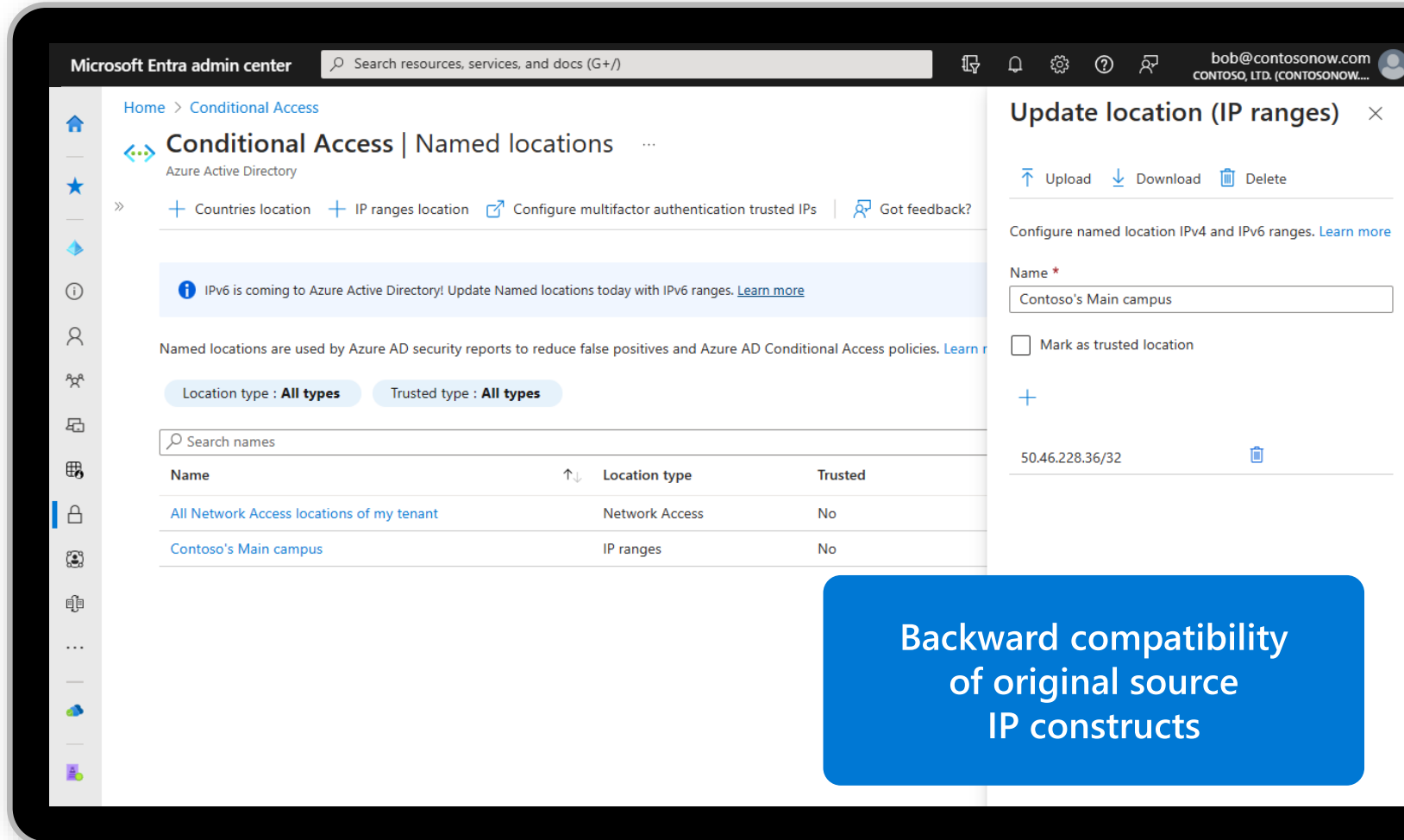
The primary setting is "Enable Global Secure Access signaling in Conditional Access", which is currently turned on (indicated by a blue toggle switch).

The left-hand navigation pane includes sections for "Global settings" (with "Session Management" selected), "Connect" (with "Traffic forwarding"), and "Monitor" (with "Traffic logs"). A "Save" button is visible at the bottom of the page.

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 editing a location named "Contoso's Main campus".

Named locations table:

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

Update location (IP ranges) pane:

- Name: Contoso's Main campus
- Mark as trusted location:
- IP range: 50.46.228.36/32

Blue callout box: Backward compatibility of original source IP constructs

Demo - Source IP Restoration

The screenshot displays the Microsoft Entra admin center interface. The main content area shows the 'Conditional Access | Sign-in logs' page for the user 'mamkumar@contosonow.com'. The logs are filtered for the last 24 hours and show a list of sign-in events. The table below contains the following data:

Date	User	Application	Status	IP address
6/8/2023, 12:54:38 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:54:35 PM	Mamta Kumar	Office 365 Exchange Online	Success	147.243.242.112
6/8/2023, 12:54:32 PM	Mamta Kumar	Office 365 Exchange Online	Interrupted	147.243.242.112
6/8/2023, 12:54:08 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:54:08 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:54:08 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:54:08 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:54:00 PM	Mamta Kumar	Office 365 Exchange Online	Success	147.243.242.112
6/8/2023, 12:53:55 PM	Mamta Kumar	Office 365 SharePoint Online	Success	147.243.242.112
6/8/2023, 12:53:50 PM	Mamta Kumar	Office 365 SharePoint Online	Interrupted	147.243.242.112
6/8/2023, 12:52:00 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:51:53 PM	Mamta Kumar	Office 365 Exchange Online	Success	147.243.242.112
6/8/2023, 12:51:48 PM	Mamta Kumar	Office 365 SharePoint Online	Success	147.243.242.112
6/8/2023, 12:51:46 PM	Mamta Kumar	Office 365 SharePoint Online	Interrupted	147.243.242.112
6/8/2023, 12:51:17 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:51:14 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112
6/8/2023, 12:51:12 PM	Mamta Kumar	SharePoint Online Web Client Extensibility	Success	147.243.242.112
6/8/2023, 12:51:10 PM	Mamta Kumar	Office365 Shell WCSS-Client	Success	147.243.242.112

Universal Tenant Restriction

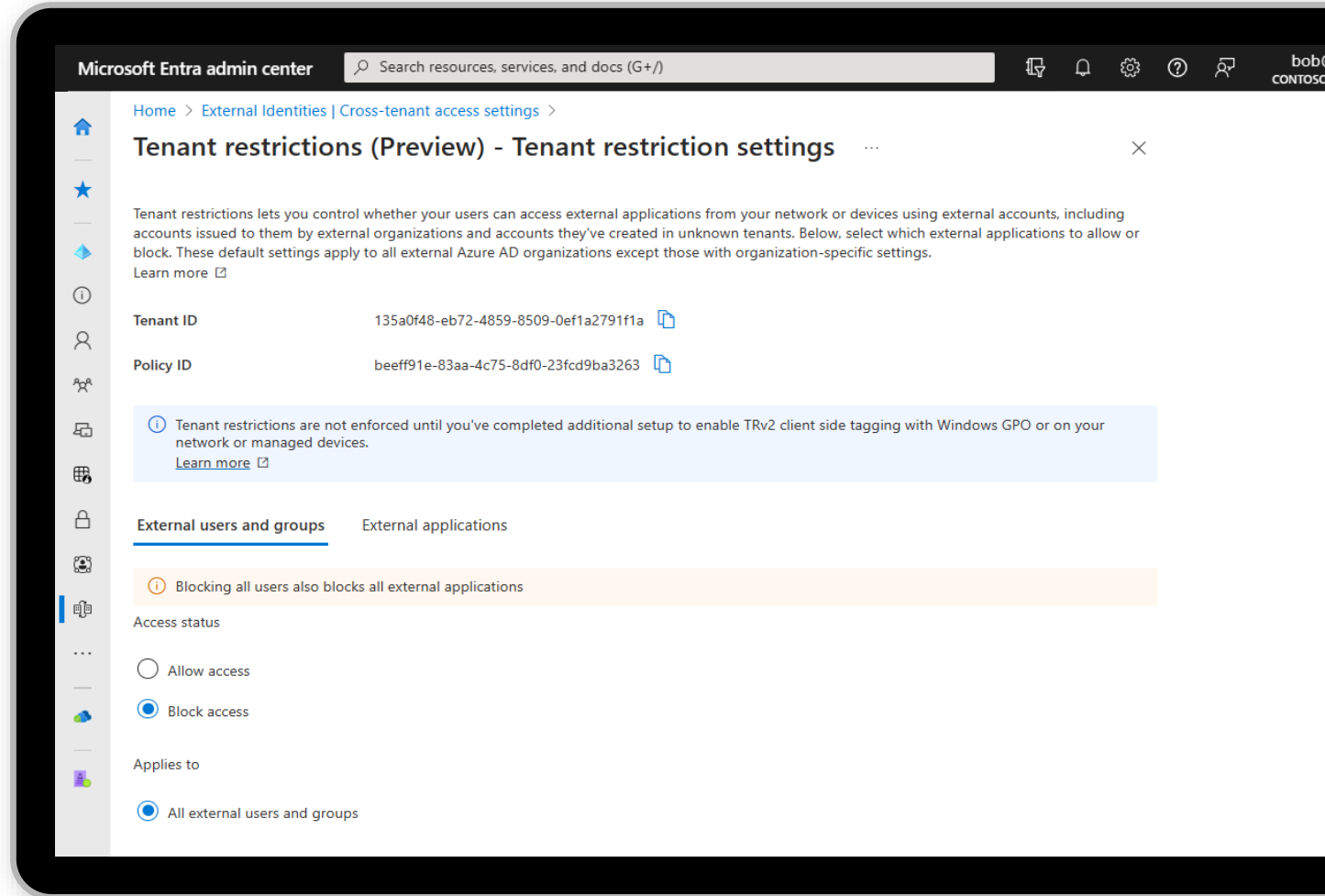
Strong data exfiltration controls

» 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



Demo - Universal Tenant Restriction



Visibility and Insights

Rich Network and Policy Analytics

» In-Product Logging and Reporting

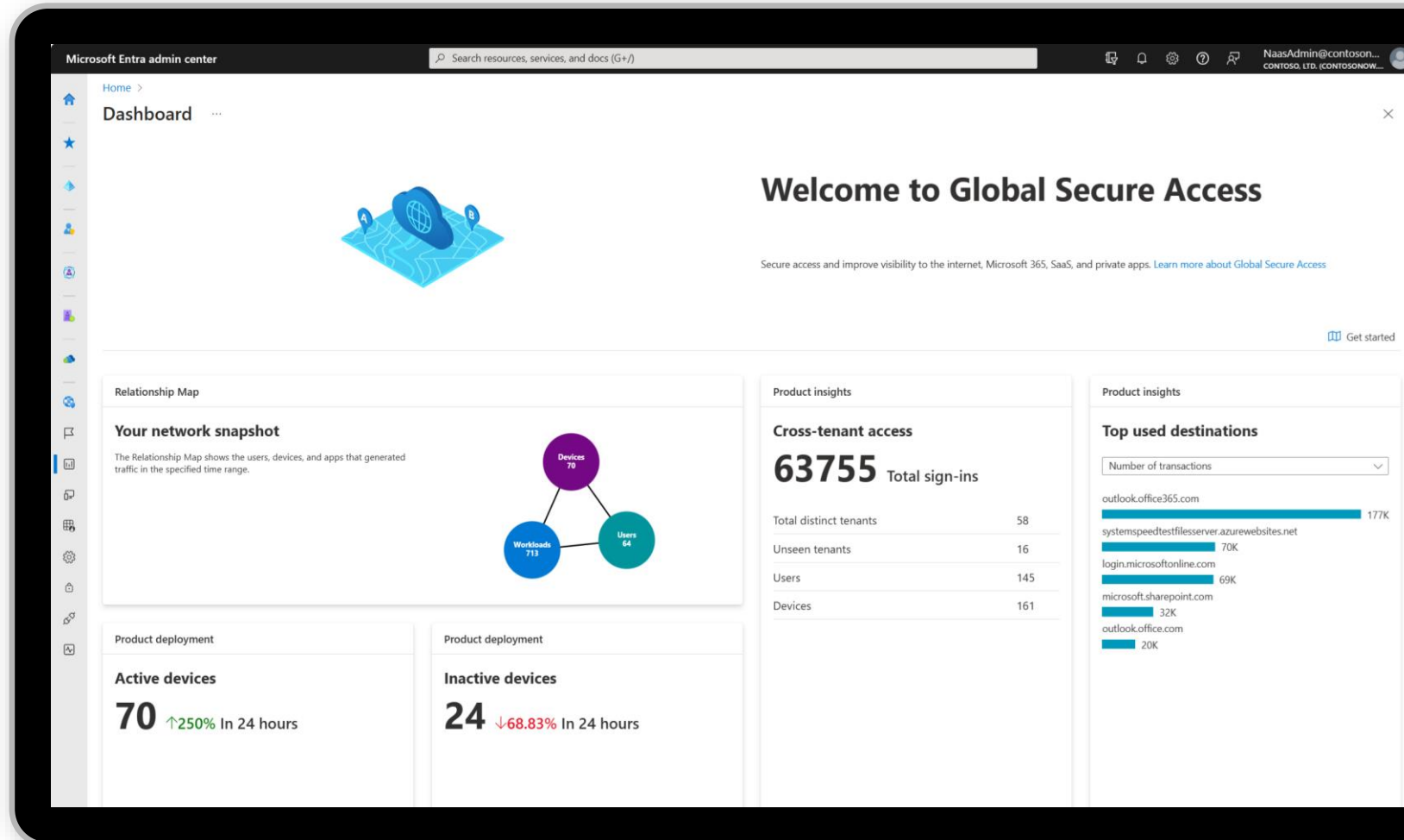
- » **Public Preview:** Network traffic logs
- » **Public Preview:** Enriched Microsoft 365 logs (export only)
- » **Coming Soon:** Network security policy logs

» In-Product Dashboards

- » **Public Preview:** User, Device, Endpoint relationship map
- » **Public Preview:** Cross tenant user activity monitoring
- » **Public Preview:** Top destinations by user, sessions, devices
- » **Coming Soon:** Advanced Application and NW discovery
- » **Coming Soon:** Network security policy analytics

» Extensive Data Export Capabilities

- » **Public Preview:** Log analytics and Workbook integrations
- » **Public Preview:** Log export APIs
- » **Public Preview:** Integration with 1st Party and 3rd Party SIEM systems



Demo – Traffic Logs

Home > Traffic logs

Download Refresh Columns Got feedback?

All Connections 261K Private Access 40 Microsoft 365 Access 261K

Timespan : Last 24 hours Add filter

Traffic Type	Transaction ID	Agent Version	Created Date Time	Device ID	Device OS	Device OS Vers...	Source IP	Source Port
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:24 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:23 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:23 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:23 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:22 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:22 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:21 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:20 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:20 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022
Microsoft 365	20230607T092...	1.5.527	06/07/2023, 12:20 PM	db6478aa-ab38...	Windows 11 En...	10.0.22621	167.220.196.208	18022

Microsoft 365 visibility features

Enriched logging and real-time visibility



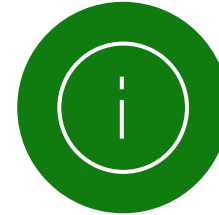
» Detect threats faster without break and inspect

Security sensitive events delivered from SharePoint

Deep insights into workload activities without break and inspect

Coming soon: Predictable, consistent SLA and near real-time detections

Coming soon: Security sensitive events from Microsoft Exchange and Microsoft Teams



» In-line metadata enrichment for better threat co-relation

Device context such as OS type and version, device ID, device name, device security posture/score, initiating process, machine group, logged on users (SID, user ID)

Network context such as tunnel and tenant info, ports and protocols, Egress IP, NW location (office/home/roaming), geo location – country, city, state, GPS

User and token context such as user, department, native/guest, user risk, token ID, tenant ID, token issued at, token application ID, token expiration time

Coming soon: Threat intel such as threat type, name, report, organization, confidence

Demo - Enriched logging and real-time visibility

Home >

Logging

The Microsoft 365 integration allows you to stream selected activity logs to Global Secure Access for additional enrichment with network, device and user information. Once data is enriched, you can export the data in near real time to your selected resource such as Event Hubs and Storage Accounts.

Prerequisites

- ✓ Tenant permissions: 'Global Administrator' or 'Security Administrator'.
By enabling Global Secure Access integration with Microsoft 365, Global Secure Access may transfer your Office 365 audit logs, for processing only, outside of the geographic location where your Office 365 audit log data are stored.

Configuration

Connect Office 365 activity logs to Global Secure Access.
Select the record types you want to collect from your tenant and click **Apply changes**.

- SharePoint
- Teams
- Exchange

Apply changes

Configure diagnostic settings

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, risks, 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

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.

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 restrictions, 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.

Any user, any device
Identities
Endpoints
Remote networks

Anywhere
Microsoft global private edge network

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) ...

- 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/InternetAccessPreview>

Private Preview

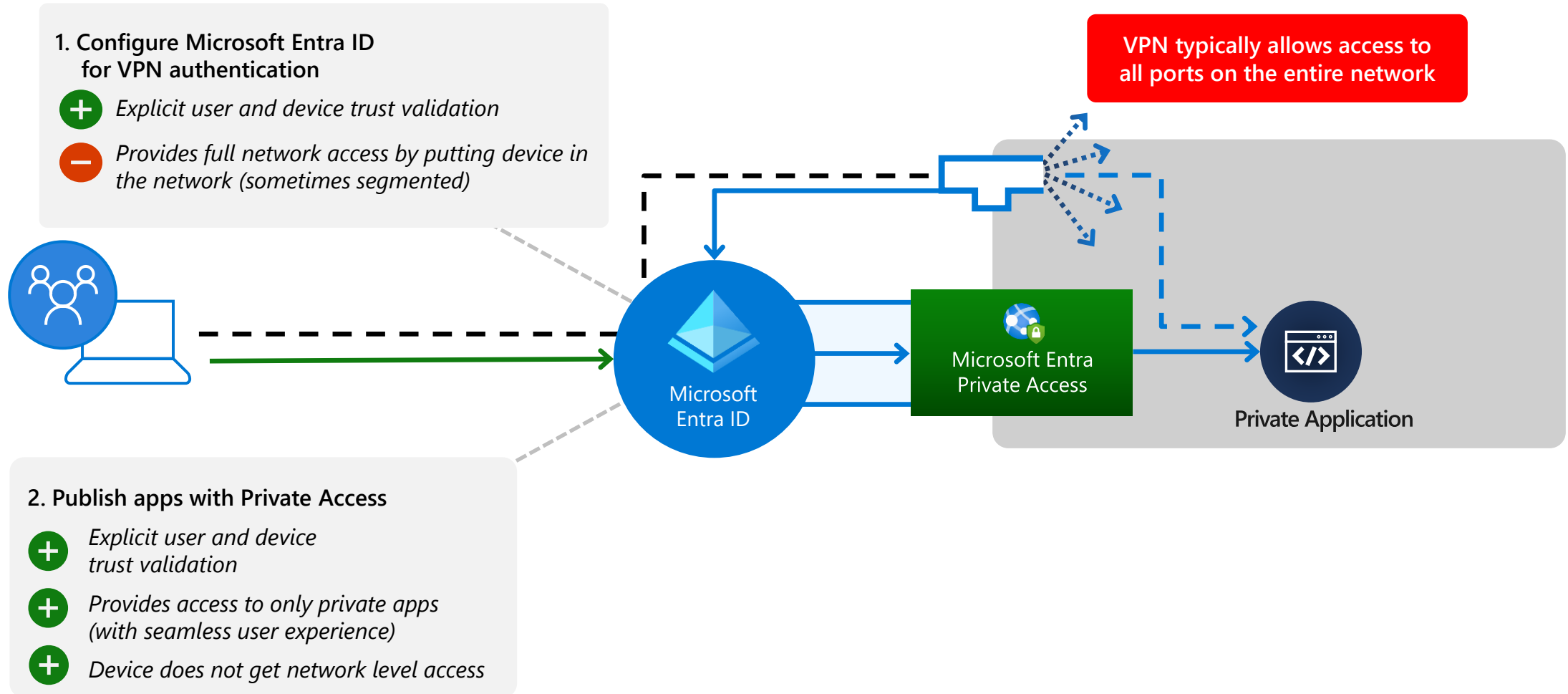
» <https://aka.ms/InternetAccessPrivatePreview>

Microsoft Entra Private Access (Preview)



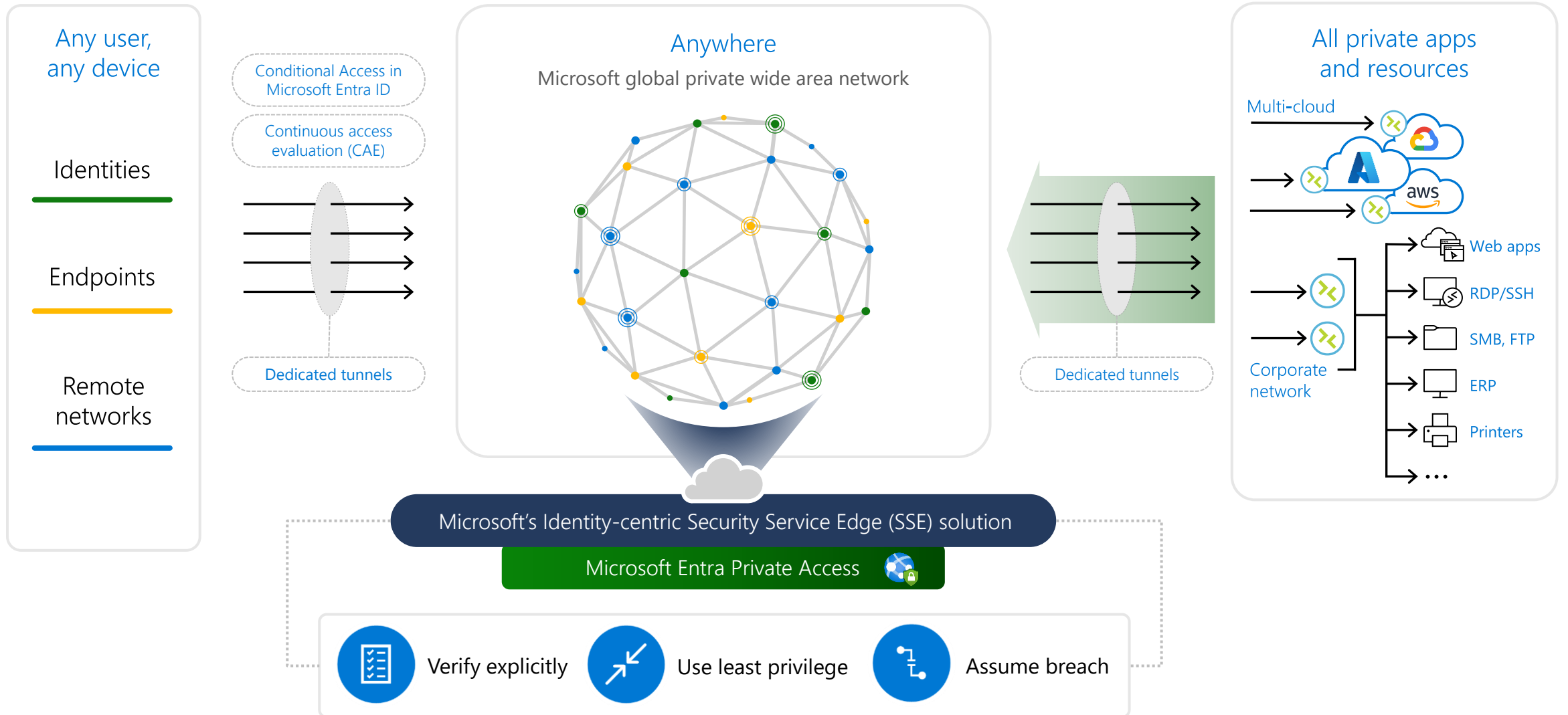
Moving beyond VPNs

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

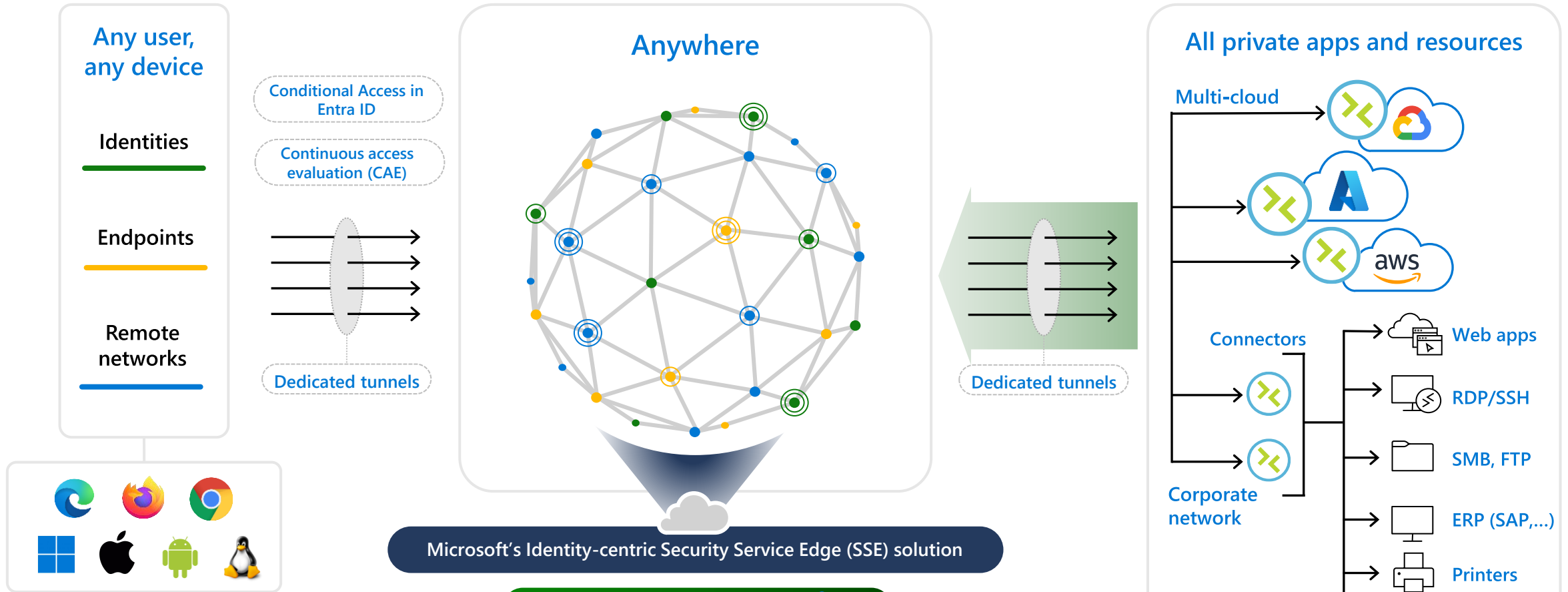


Microsoft Entra Private Access

An identity-centric Zero Trust Network Access (ZTNA)



Microsoft Entra Private Access - How it works



Private Access

Key Security Capabilities

- Zero-Trust Network Access
- Broad Application Support
- Identity-centric security controls
- Segmented App access
- Conditional Access & modern authentication
- Private resource discovery
- Intelligent Local Access (Coming soon)
- Audit logging
- TLS termination and inspection (Coming soon)
- Web application firewall (Coming soon)

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

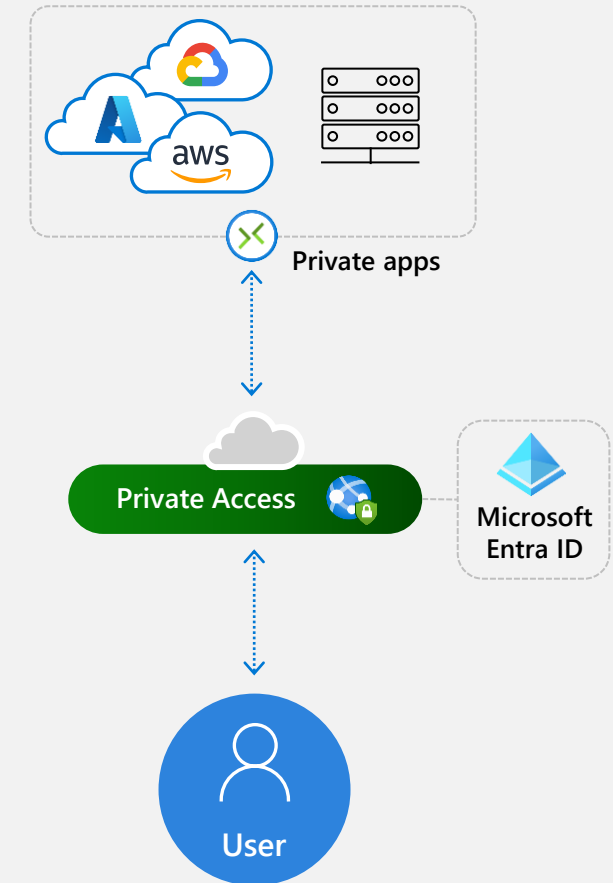
Coming soon: Micro-segment based on process identity

» 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

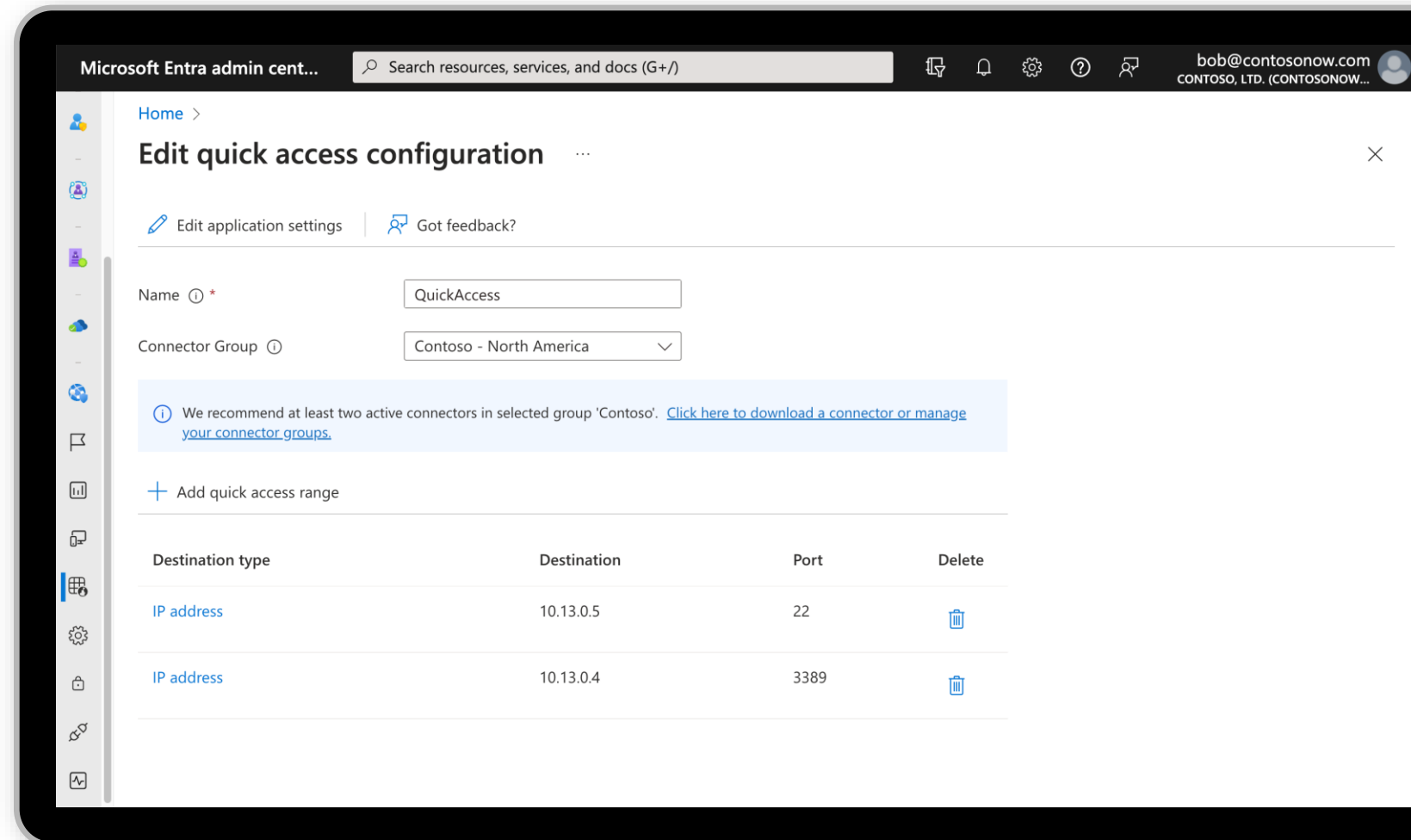
» Flexibility

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 user information for "bob@contosonow.com" from "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, Custom security attributes (preview)), 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

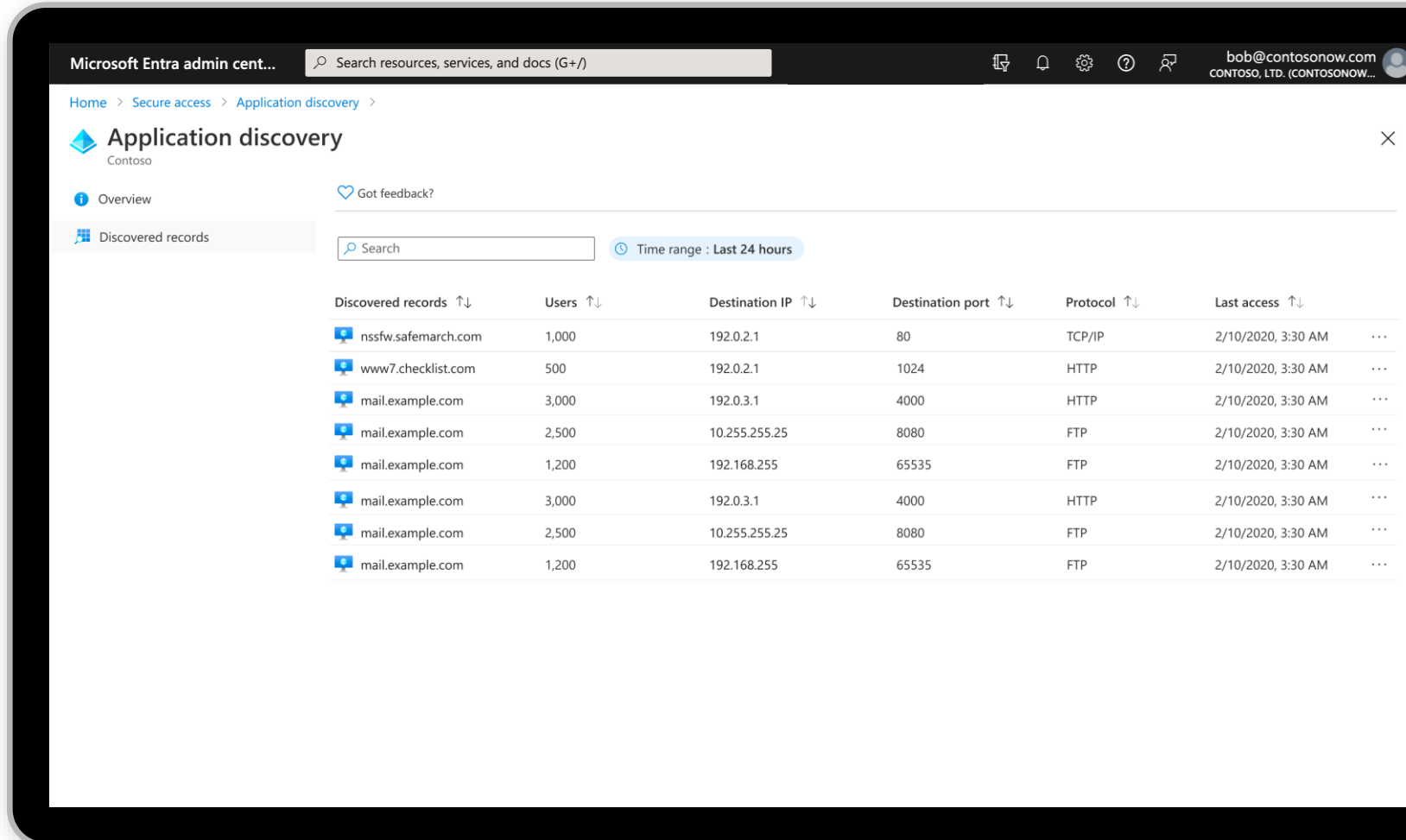
Create private apps using discovered app segments

» 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



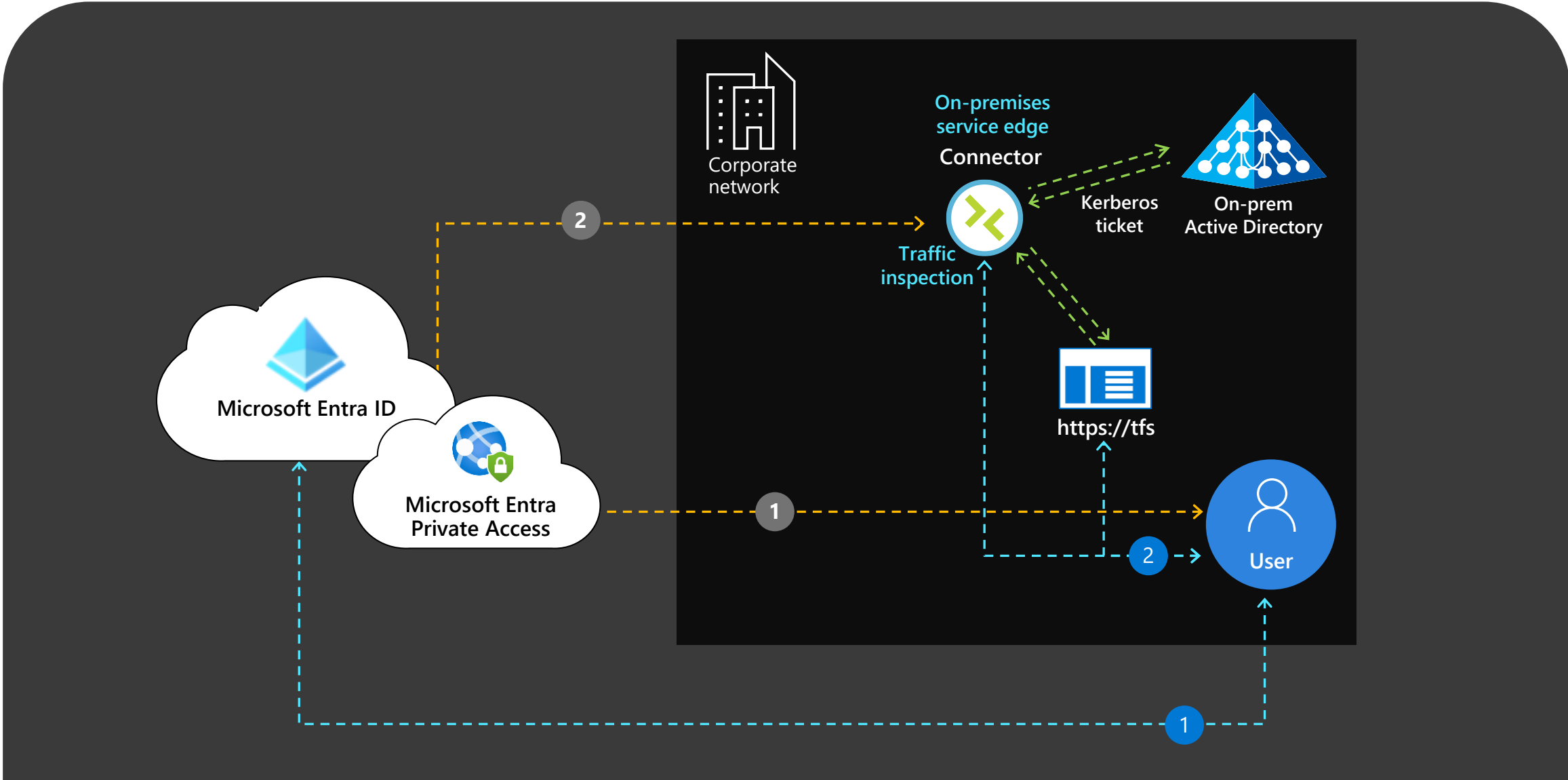
The screenshot displays the Microsoft Entra admin center interface for Application discovery. The page title is "Application discovery" for the organization "Contoso". The navigation menu includes "Overview" and "Discovered records". A search bar and a "Time range : Last 24 hours" filter are visible. 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 navigation pane on the left shows the path: Home > Enterprise applications > myRDP app. The current view is 'myRDP app | Network access properties', described as a 'Global secure access application'. A sidebar menu lists various management options: Overview, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Network access properties, Custom security attributes (preview)), Security (Conditional Access), and Activity (Sign-in logs). The 'Edit Process Segment' dialog is open, showing 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 highlights the three input fields. A notification message states: 'We recommend at least two active connector groups.' The 'Destination type' section is partially visible, showing 'IP address'.

Thank you!