

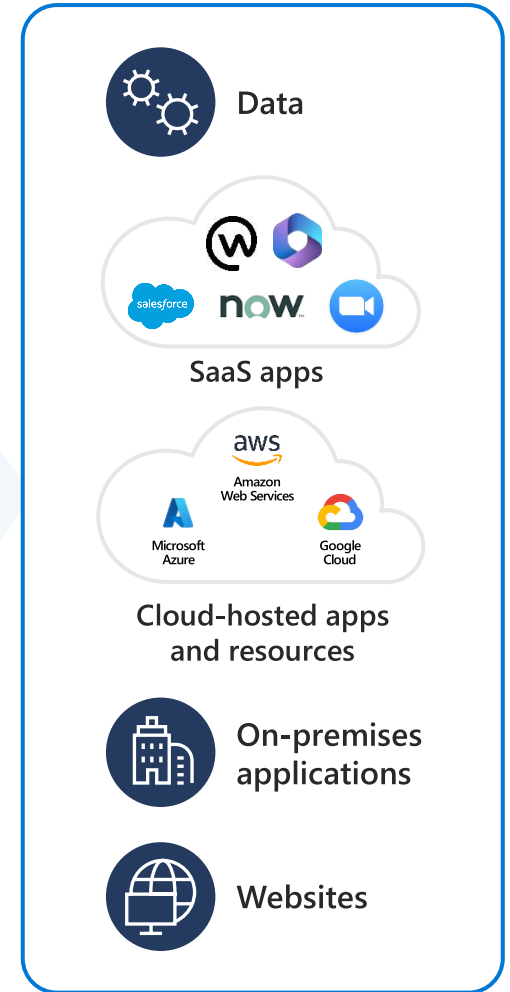
# Microsoft Entra

Rohit Gulati  
Principal Product Manager  
Identity & Network Access Division



# 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 ID

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



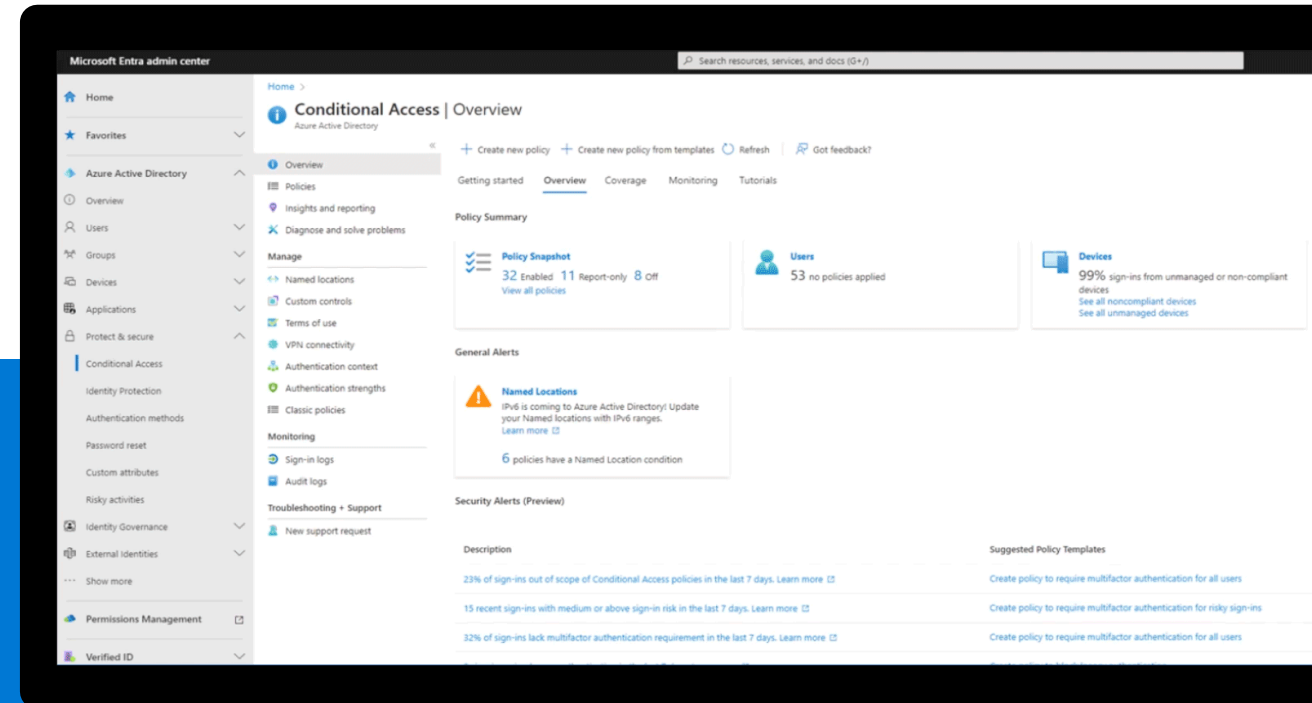
Secure adaptive access



Seamless user experiences



Unified identity management

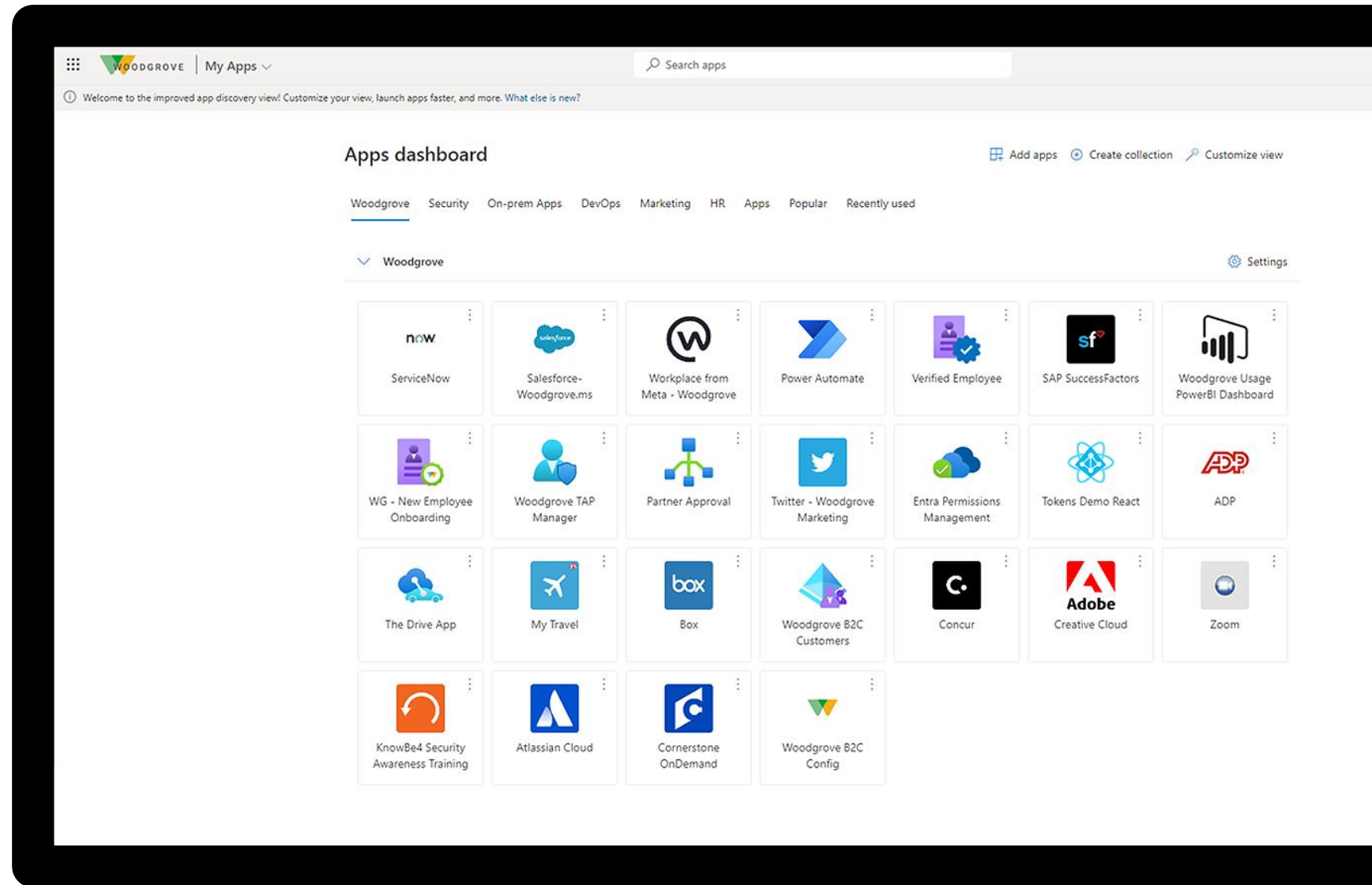


## Market challenge:

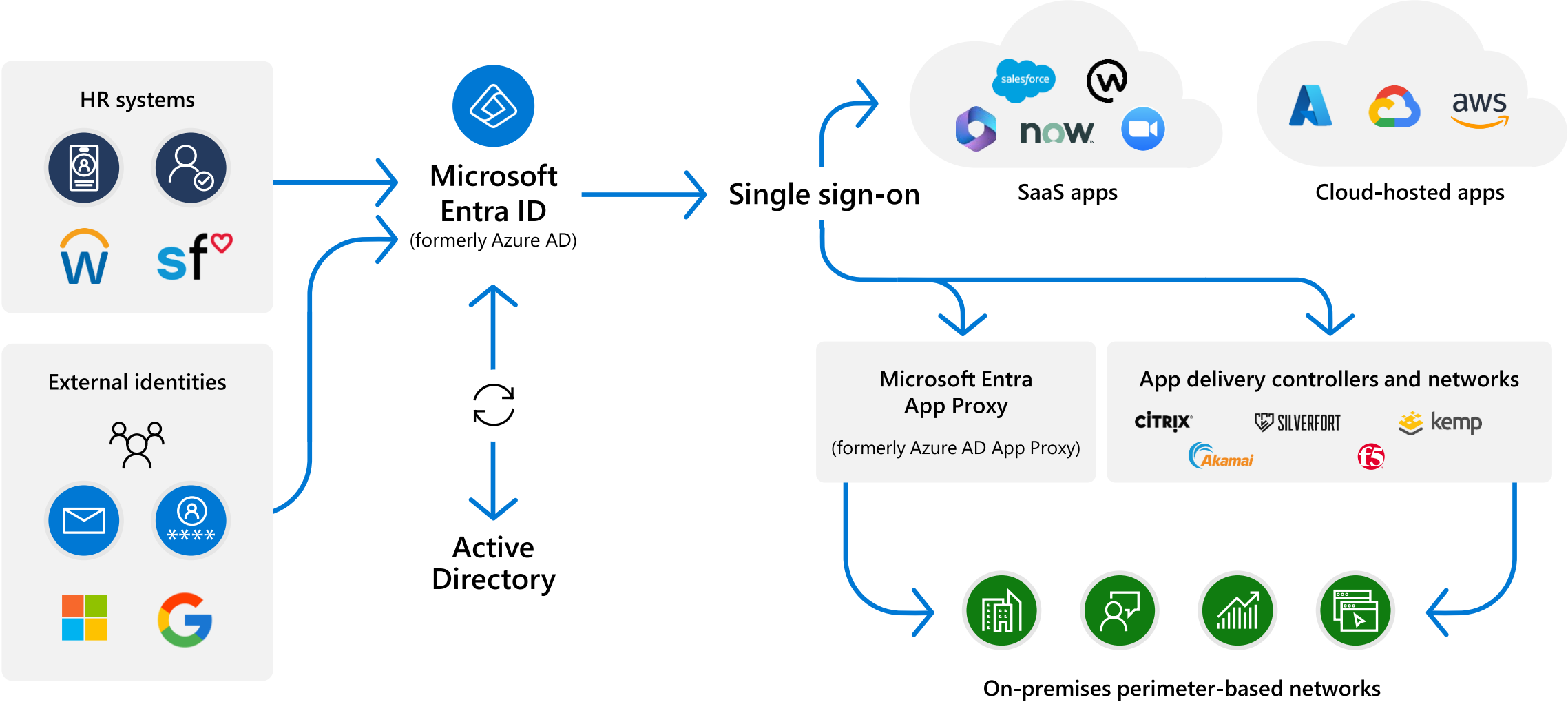
Organizations require a comprehensive IAM solution across hybrid and cloud environments that provides security, simplifies user authentication, and enables secure access to resources

# Enable seamless user experience with SSO

SSO access to popular SaaS apps, on-premises and custom-built apps on any cloud, for any user type, and any identity



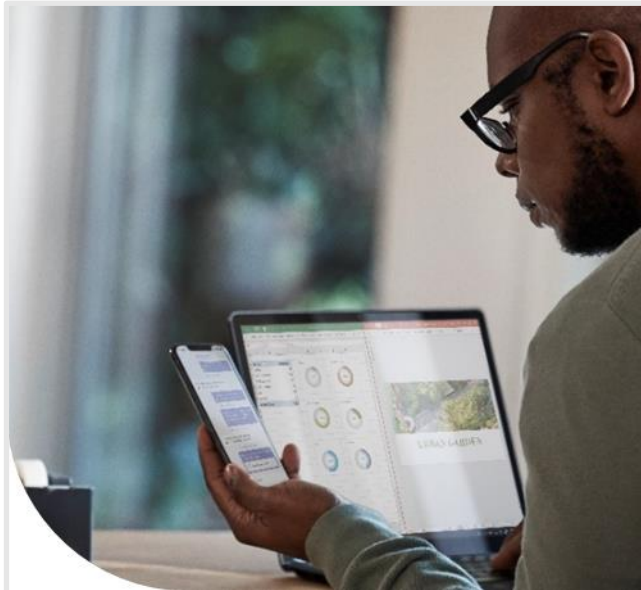
# Connect your workforce to any app





# Multifactor authentication (MFA)

Verify user identities with strong authentication



We support a broad range of multifactor authentication options

Including passwordless technology



Microsoft Authenticator



Windows Hello



FIDO2 Security key



Biometrics



Cert-based Auth

● = Including phishing-resistant technology



Push Notification



Soft Tokens OTP



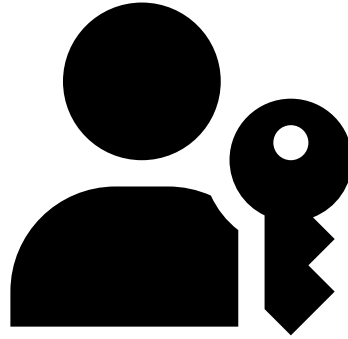
Hard Tokens OTP



SMS, Voice



Multifactor authentication addresses 99.9% of identity cyberattacks



**tech savvy  
edition**

# passkey

pass·key | \ 'pas-, kē \

***noun***

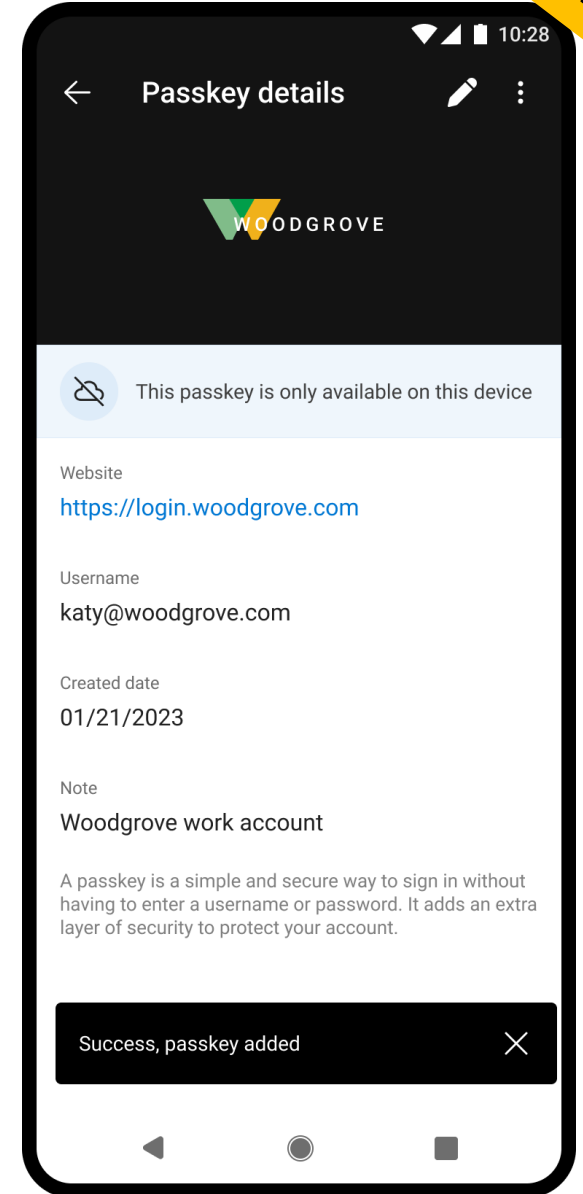
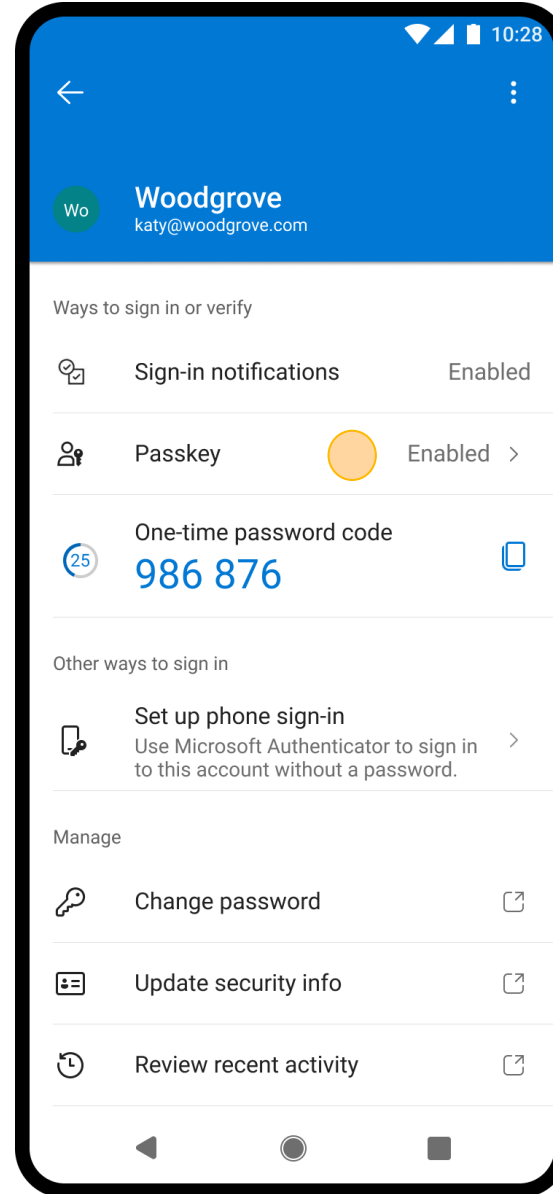
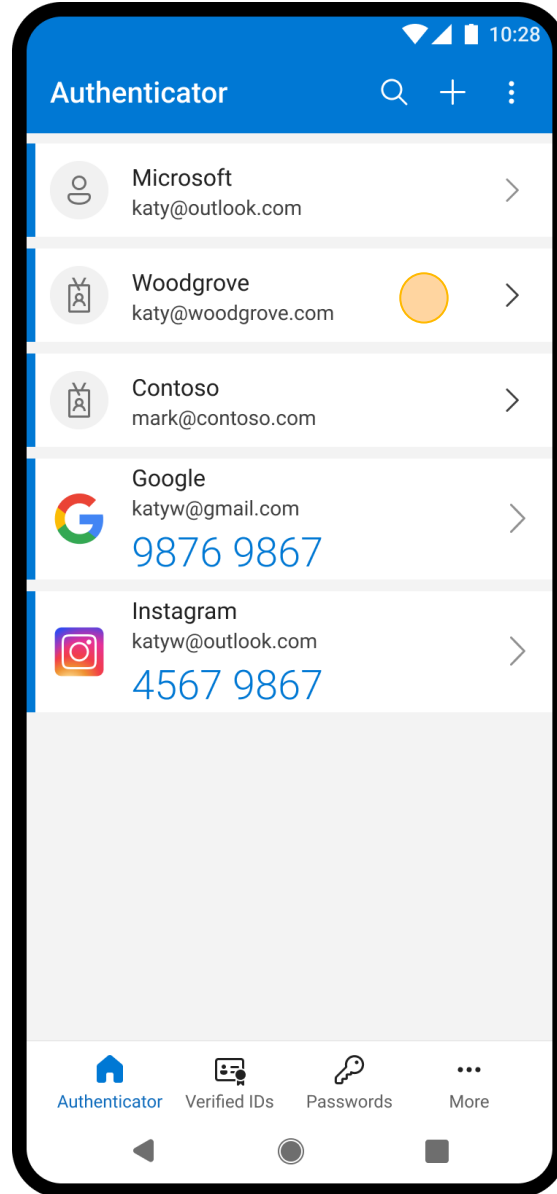
a phishing resistant, password replacement  
W3C WebAuthn credential, usable across all your devices



Preview

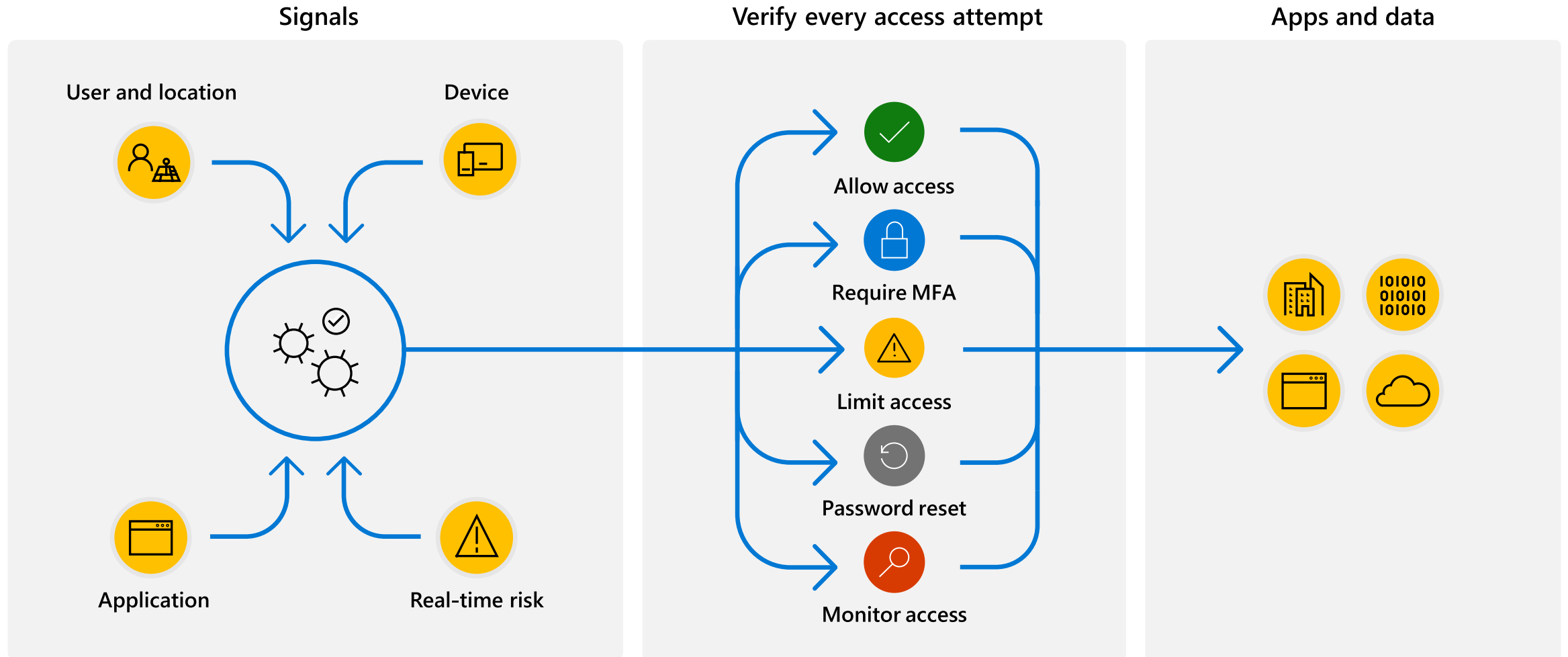
# Enter:

## Passkeys in Microsoft Authenticator



# Protect resources with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



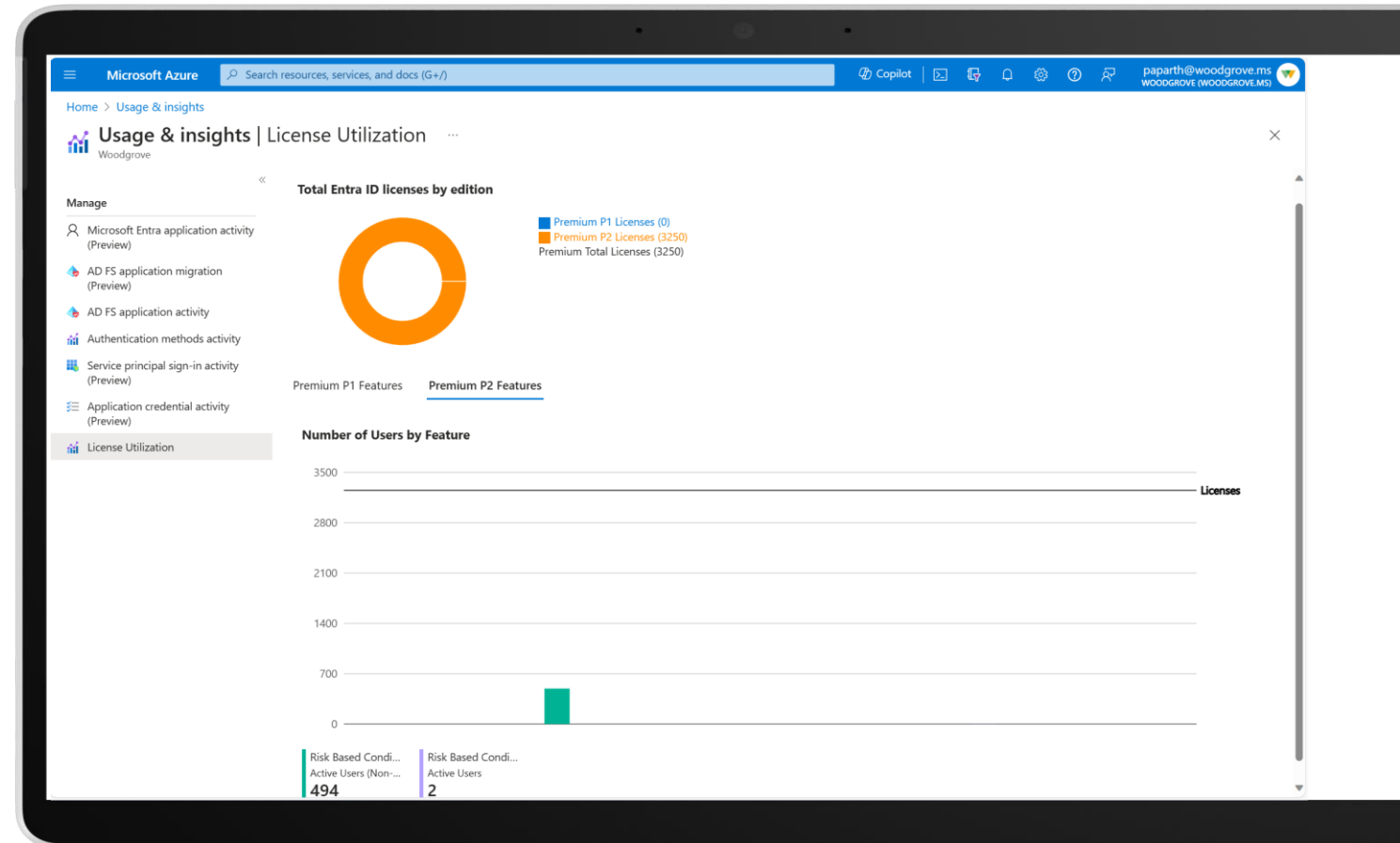
# License Utilization

Dashboard for Conditional Access license utilization

## Key benefits

- Helping customers understand their license count and license usage, as well as helping to resolve over usage issues.

PUBLIC PREVIEW



# Feature roadmap · Authorization

PUBLIC PREVIEW

## Other Features in Public Preview

### Conditional Access

- PIM + CA Integration

### ID Protection

- Post-authn anomalous activity detection for workload identities

### Others

- New RBAC V2 permissions to only add or remove group members

# ID Protection

Block identity takeover in real-time



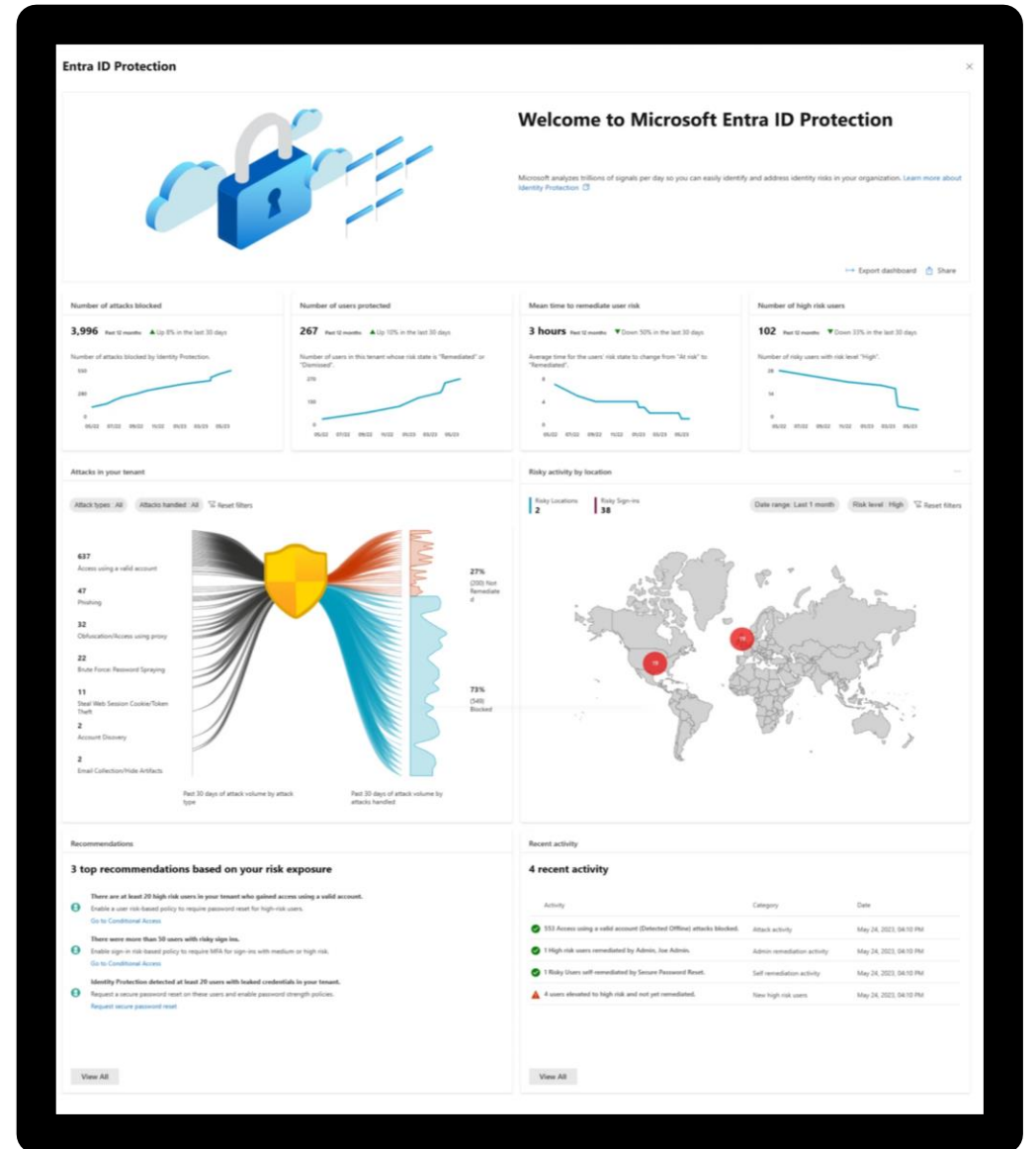
Prevent identity compromise



Enforce policies



Seamlessly integrate



# Feature roadmap · Authorization

PUBLIC PREVIEW

## Features in Public Preview

### Conditional Access/ MFA

- CAE Strictly Enforce Location Policies
- In portal guide to configure multi-factor authentication

### ID Protection

- On-premises password reset remediates user risk of compromise
- Attacker in the Middle detection alert in IP

Identity and access management



## Microsoft Entra ID Governance



**Improve productivity**



Automate employee, supplier, and business partner access to apps and services at enterprise scale



**Strengthen security**



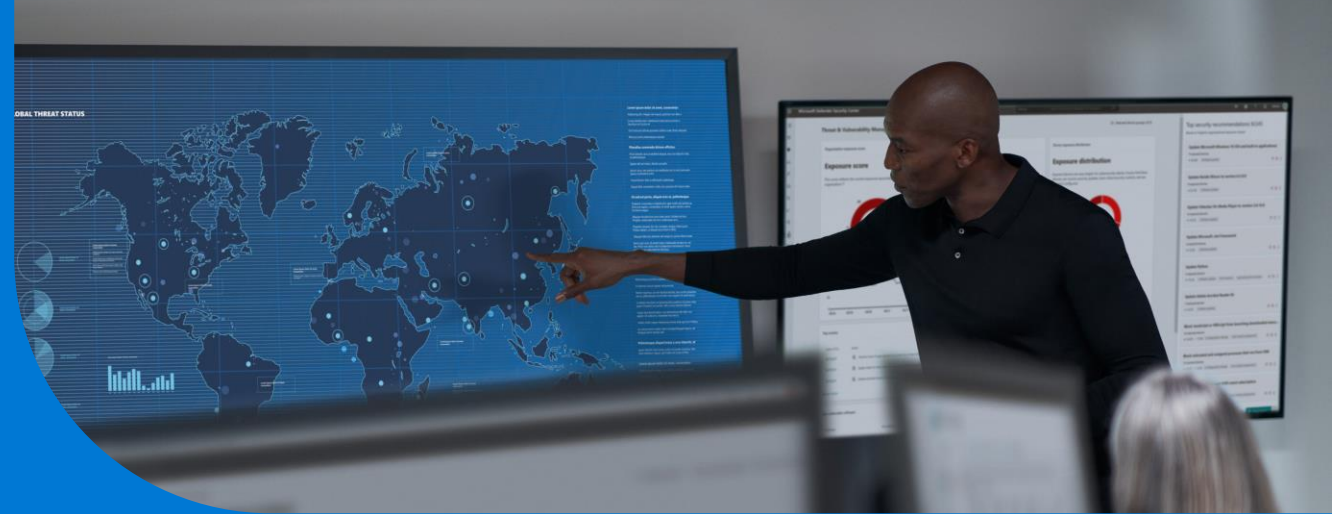
Reduce risk arising from access abuse and make smart access decisions based on machine learning



**Automate routine tasks**



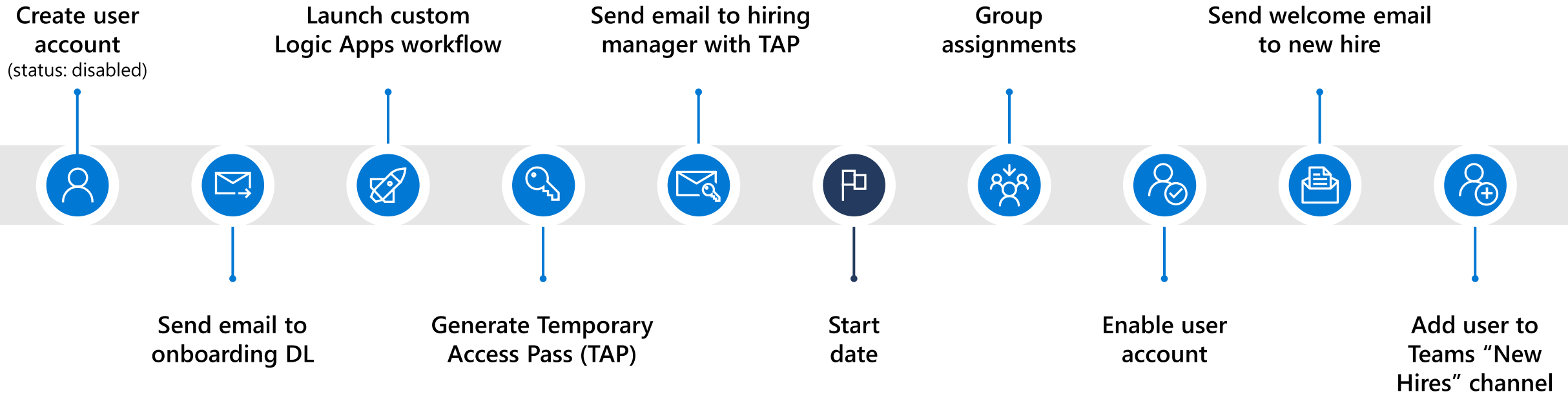
Delegate day-to-day access requests to relevant business groups and automate the approval process





# Manual processes for user scenarios are slow and error-prone

## Employee onboarding example



# 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 main heading is 'Offboard an employee - voluntary departure | Tasks'. Below the heading, there is a search bar and a list of tasks. The tasks are:

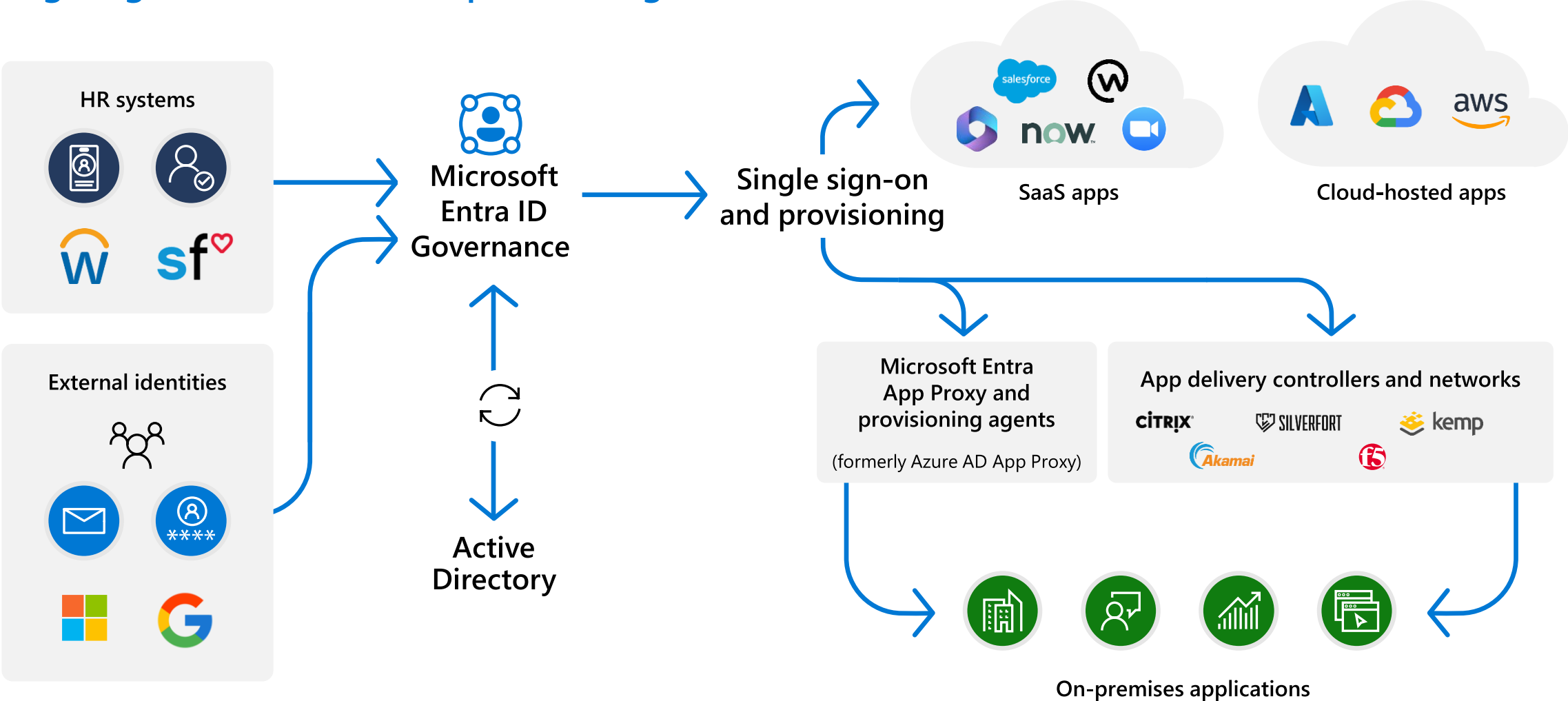
Task order	Name
1	Disable User Account
2	Remove user from all groups
3	Remove user from all Teams

The interface also includes a sidebar with navigation options like 'Overview', 'Manage', 'Properties', 'Tasks', 'Execution conditions', and 'Version'. The 'Tasks' option is currently selected.

\* To be supported in the future

# Connect your workforce to any app

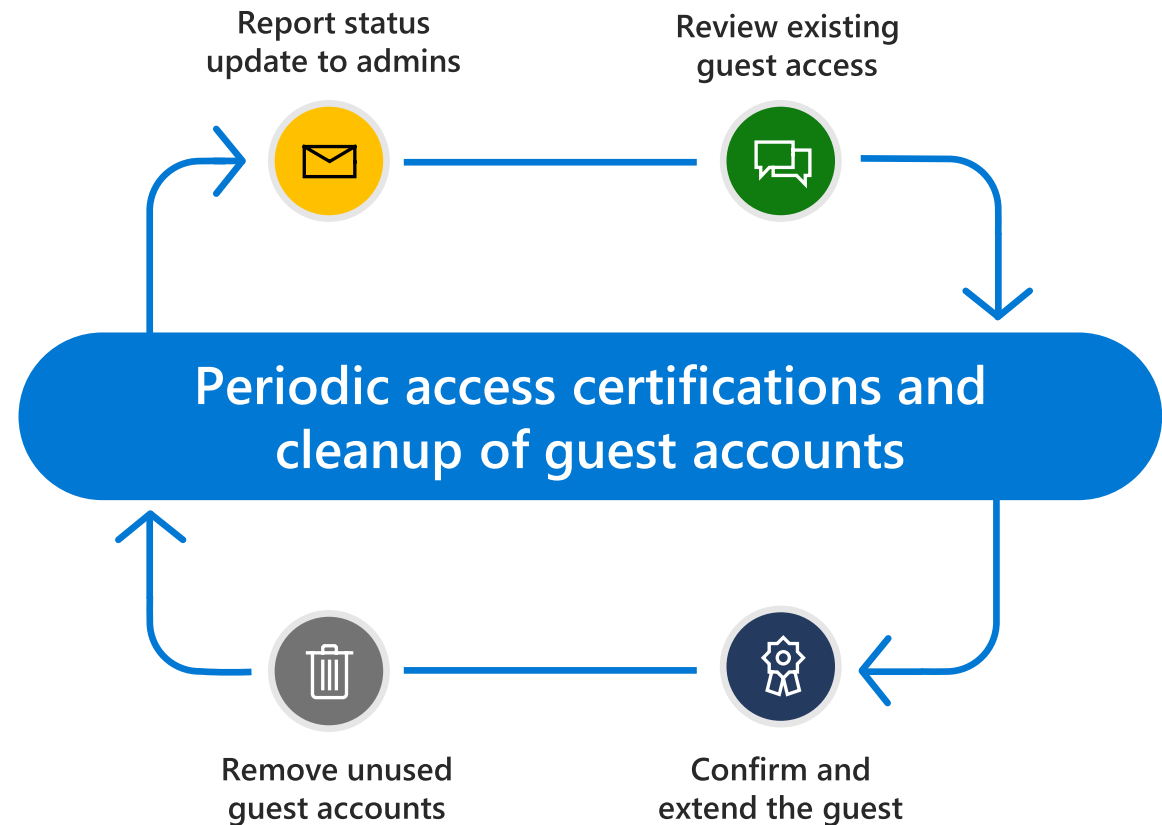
Single sign-on and outbound provisioning



# Strengthen security posture while maintaining productivity

Securely provision sensitive app access to employees and guests at scale

- > Put control in the hands of line of business managers who are suited to make sensitive data access decisions for business guests
- > Ensure only the required access to employees and guests by reviewing, extending, or revoking access rights—with machine learning assistance
- > Reduce risk of unauthorized access by periodically reviewing and cleaning up access to sensitive resources



# Multi-tenant organizations

## Synchronization across tenants

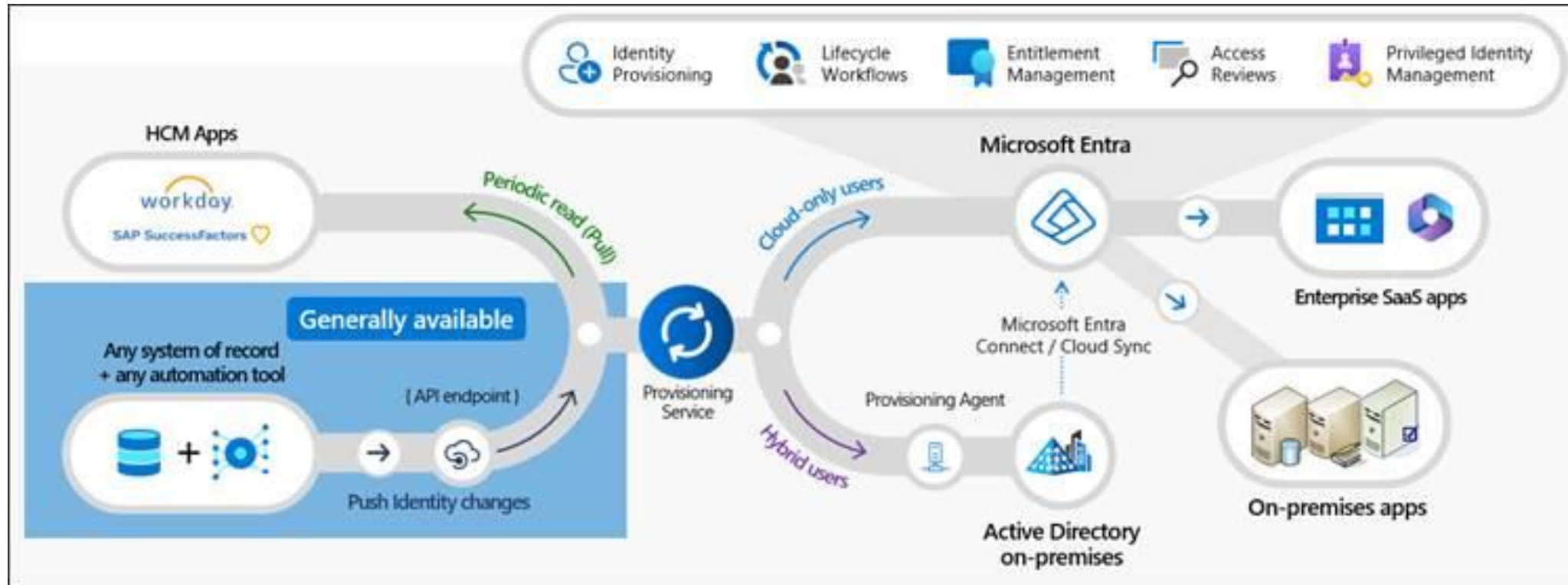
- Flexible attribute mapping and scoping
- Rich reporting and auditing
- Simple, streamlined configuration

## Unlocks collaboration scenarios

- Share applications across tenants
- Simplify collaboration across tenants in M365
  - Teams calls, sharing, notifications
- Secure and govern users across your entire organization



# Establish identity sync from any HR system with API-driven provisioning





# Microsoft Entra External ID

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



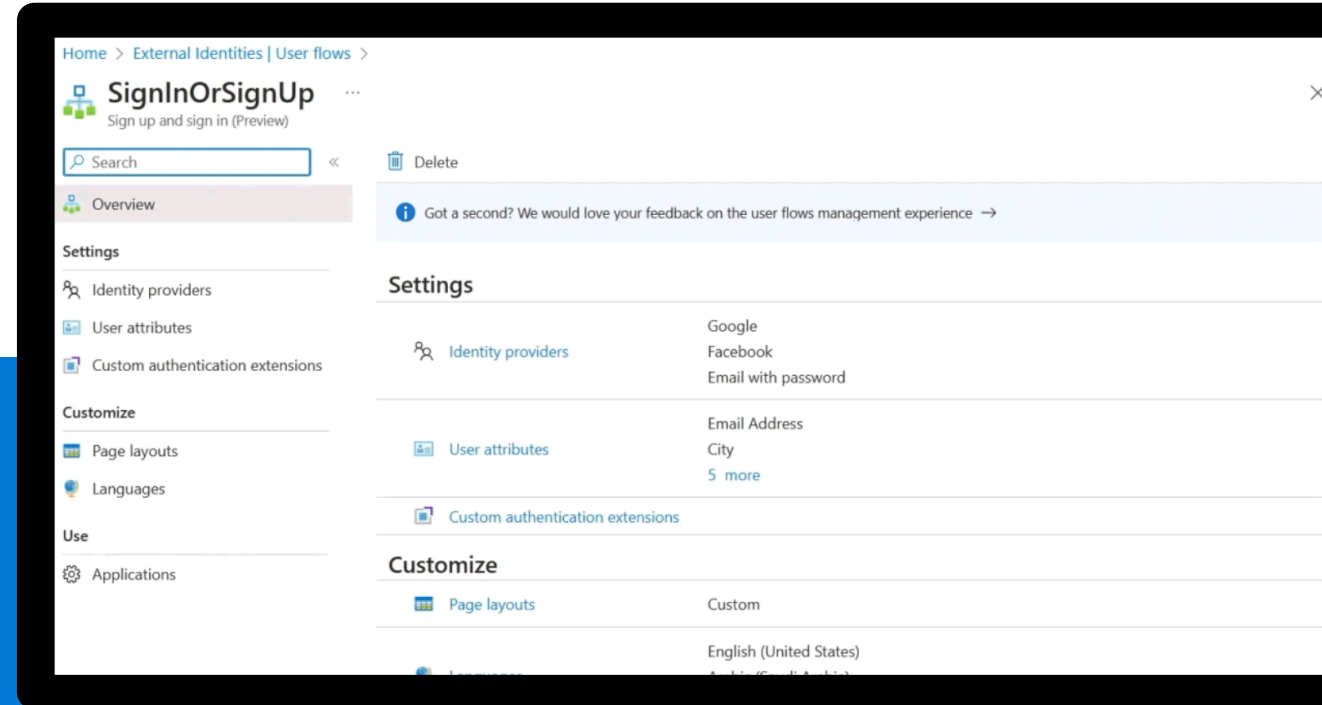
Secure partner and customer access



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



# Boundaryless collaboration with external identities

## Generally available

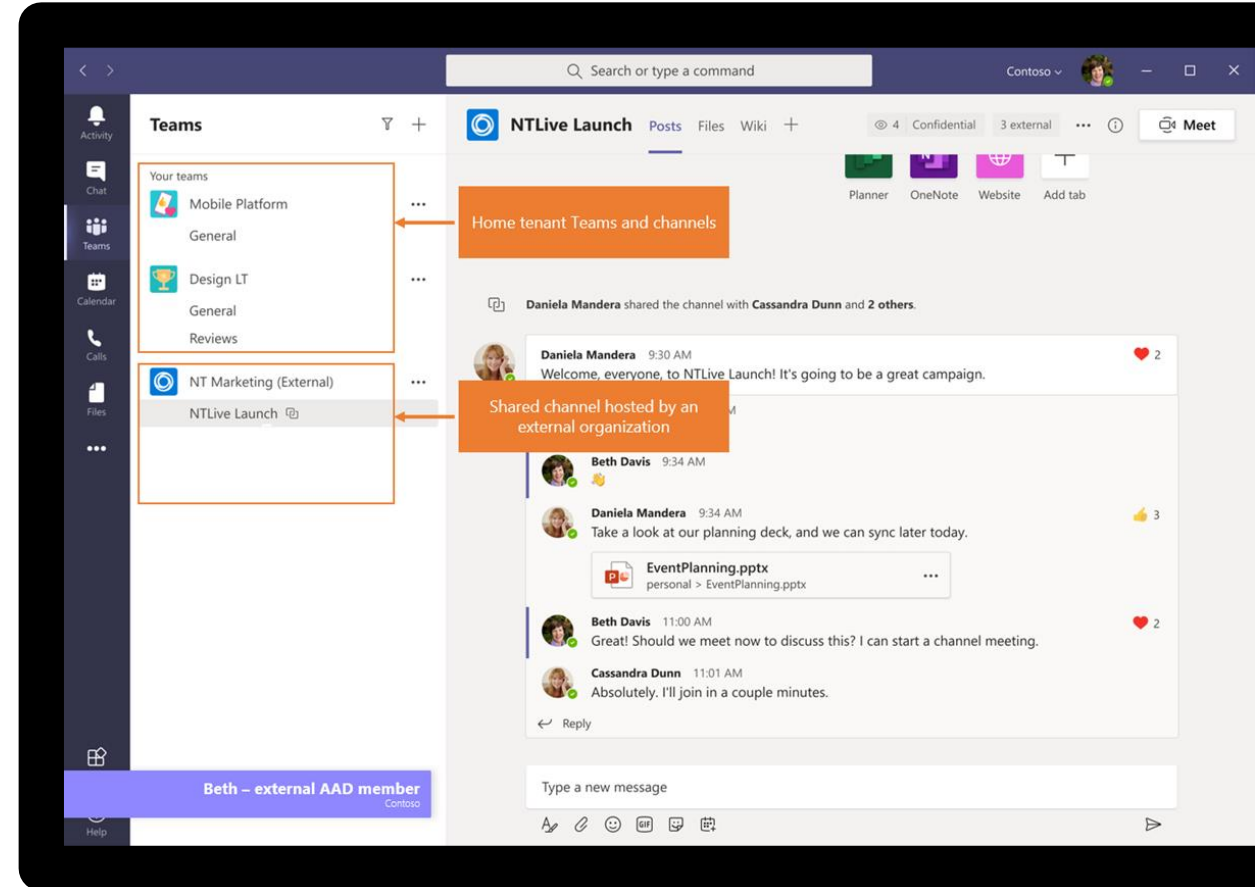
- On Teams, share a specific Channel with no tenant-switching needed for external users
- Collaborate with external users using WS-Fed/SAML
- Trust MFA guest users perform in their home tenant
- Collaborate across public and sovereign clouds with cross-cloud B2B

## Public preview

- Allow or block your users from accessing external resources using external-org issued accounts with Tenant Restrictions v2

## In progress

- Customize how users redeem their B2B invitation





# 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



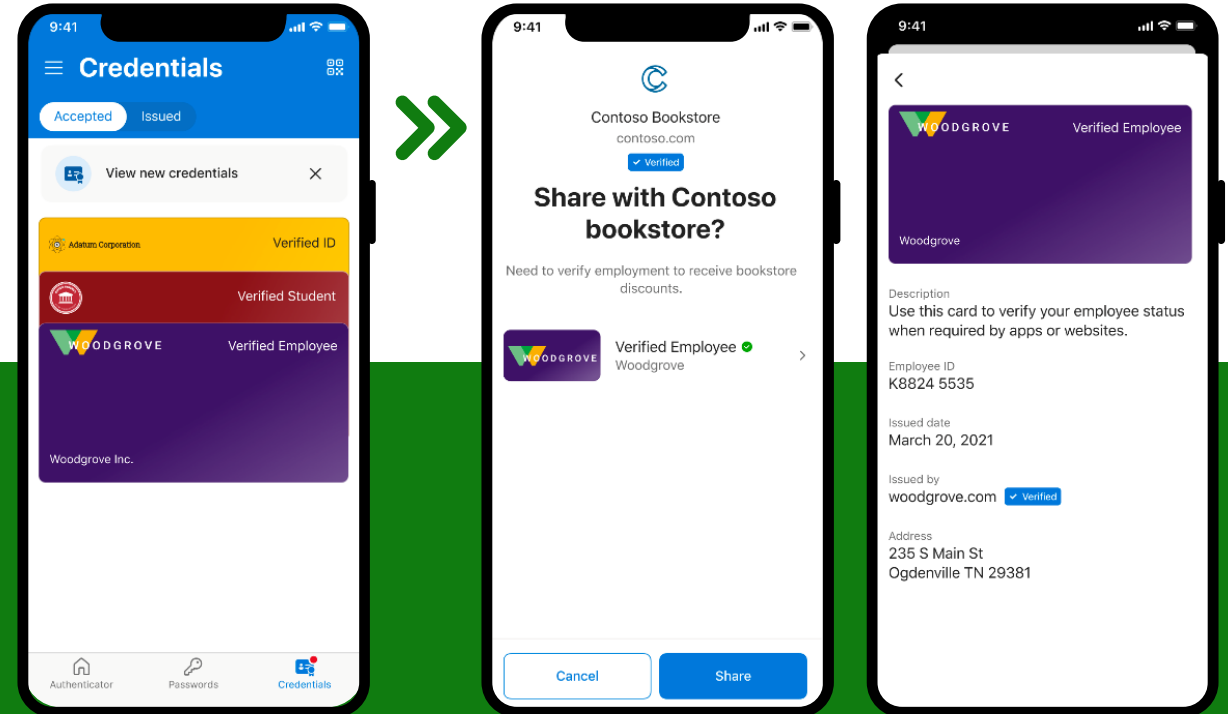
Fast remote onboarding



More secure access



Easy account recovery



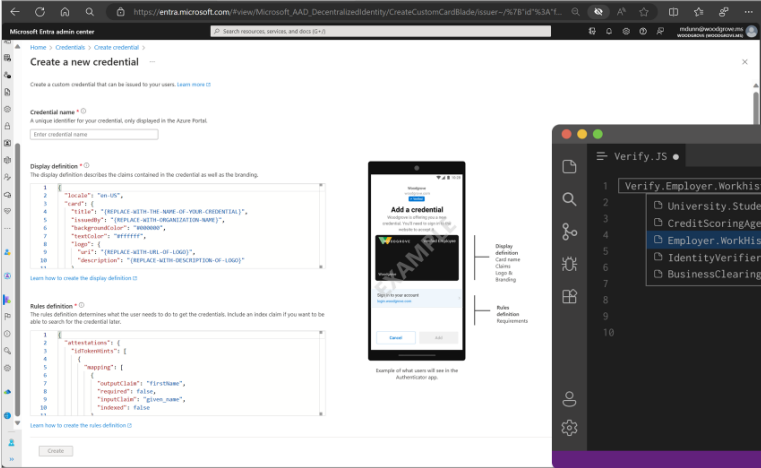
## Market challenge:

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

# One API

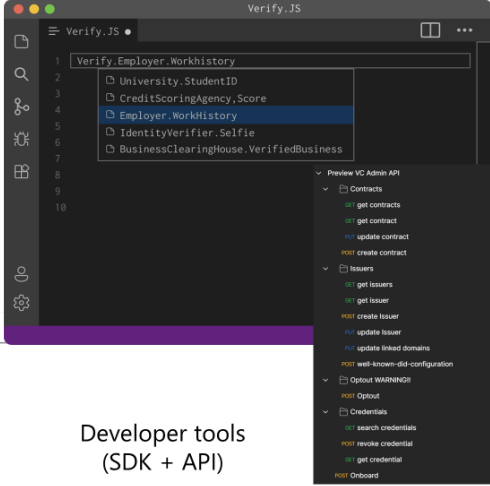
- 1. 5 mins to unlock verification!
- 2. 100s of credential types
- 3. All enterprises can issue & verify credentials
- 4. One API to verify identity attributes via 3<sup>rd</sup> party partners across 192 countries
- 5. Open-source library to integrate into branded app

## Decentralized Identity Platform by Microsoft



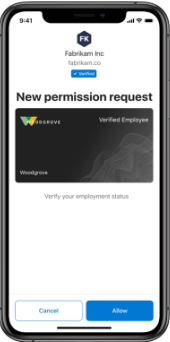
The screenshot shows the Microsoft Entra admin center interface for creating a new credential. It includes fields for 'Credential name', 'Display definition' (with a code editor), and 'Rules definition' (with a code editor). A preview of a mobile app interface is shown on the right, displaying 'Add a credential' and 'Verify' buttons.

Issuer interface (Entra portal)



The screenshot shows the Verify.JS developer tools interface. It displays a list of API endpoints under the 'Verify\_Employer\_Workhistory' namespace, including 'University\_StudentID', 'CreditScoringAgency\_Score', 'Employer\_WorkHistory', 'IdentityVerifier\_Selfie', and 'BusinessClearingHouse\_VerifiedBusiness'. A sidebar on the right shows a 'Preview VC Admin API' with various endpoints like 'get contacts', 'create contract', 'get issuers', etc.

Developer tools (SDK + API)



The screenshot shows a mobile app interface for a 'New permission request' dialog. The app is branded with 'Fabrikam Inc' and 'Microsoft Authenticator'. The dialog asks the user to 'Verify your employment status' and provides 'Cancel' and 'Allow' buttons.

End user wallet (Microsoft Authenticator)

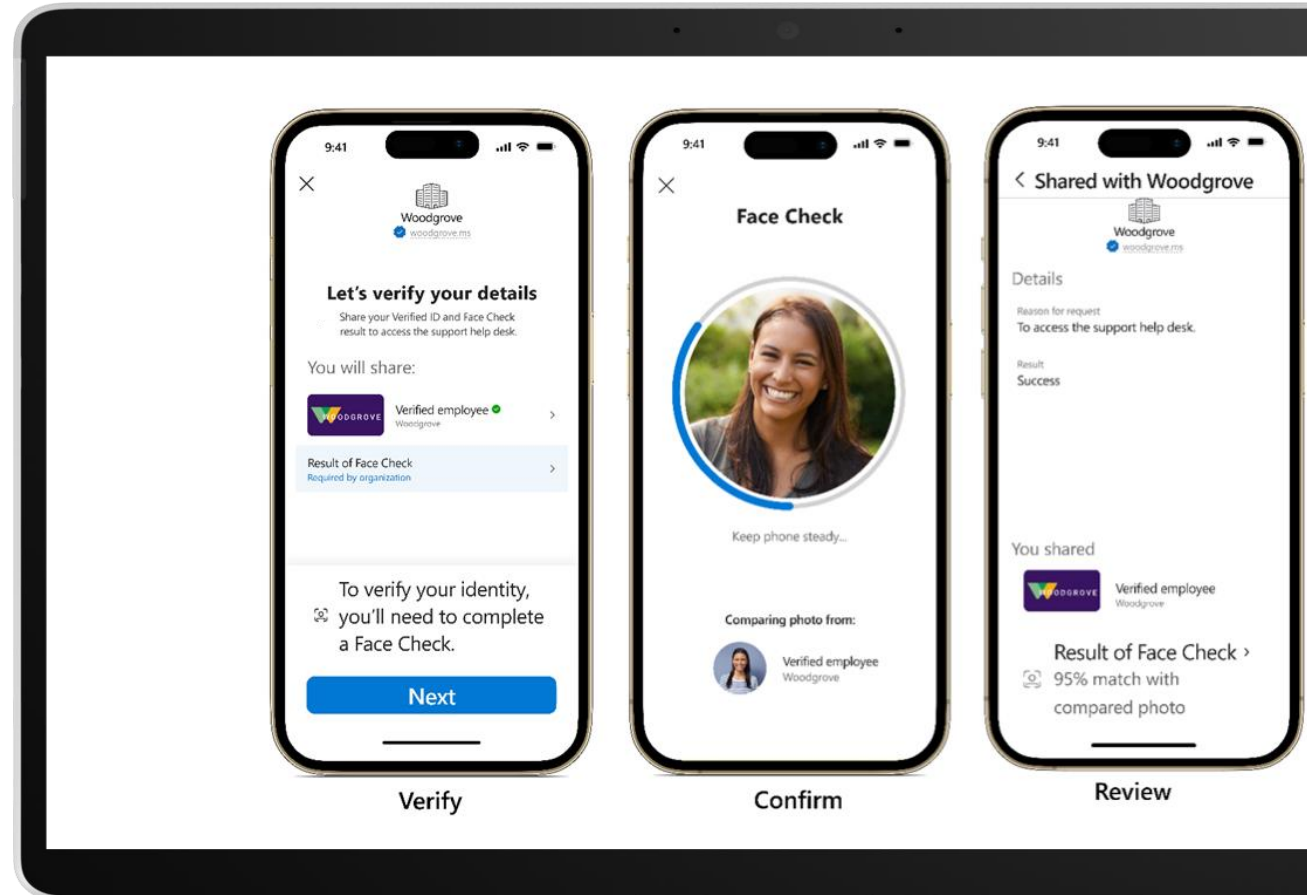
# Face Check using Entra Verified ID

A privacy-respecting facial matching feature for high-assurance verifications

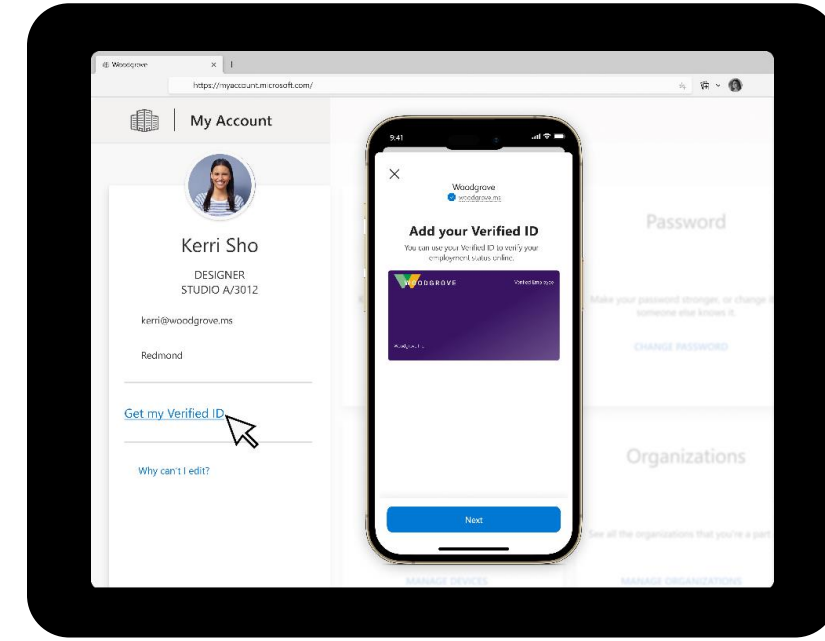
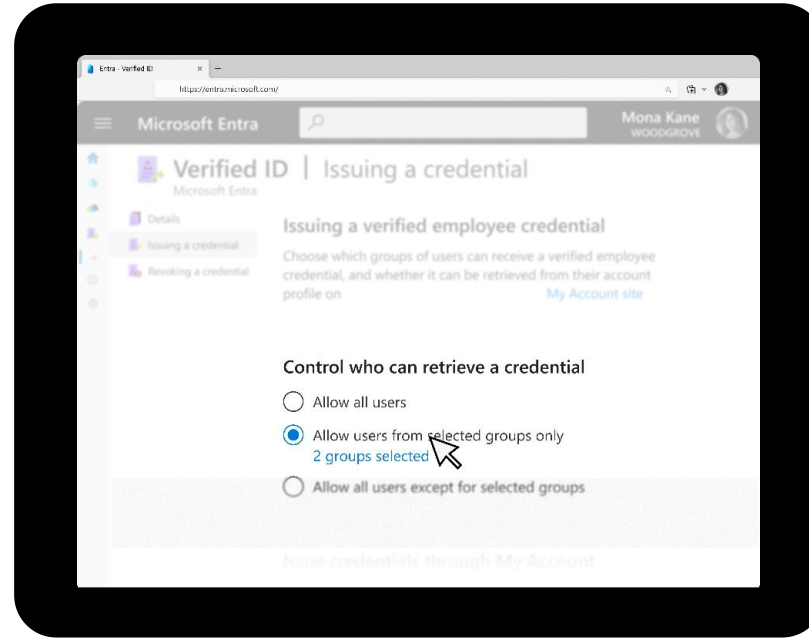
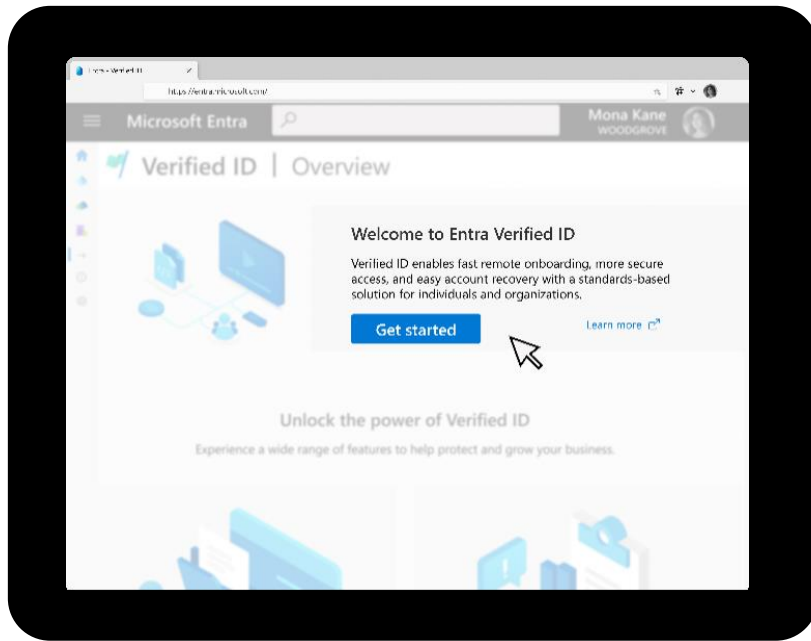
## Key Benefits

- Allows enterprises to perform high-assurance verifications securely, simply, and at scale.
- Face Check adds a critical layer of trust by performing facial matching between a user's real-time selfie and a photo.

PUBLIC PREVIEW



# Quick Start – 5 mins to issue !



Follow the [tutorial](#) to create a Face Check-ready Verified Workplace Credential

**Time: 1 minute**

Configure who can request a Verified ID by selecting all users or specific groups of users.

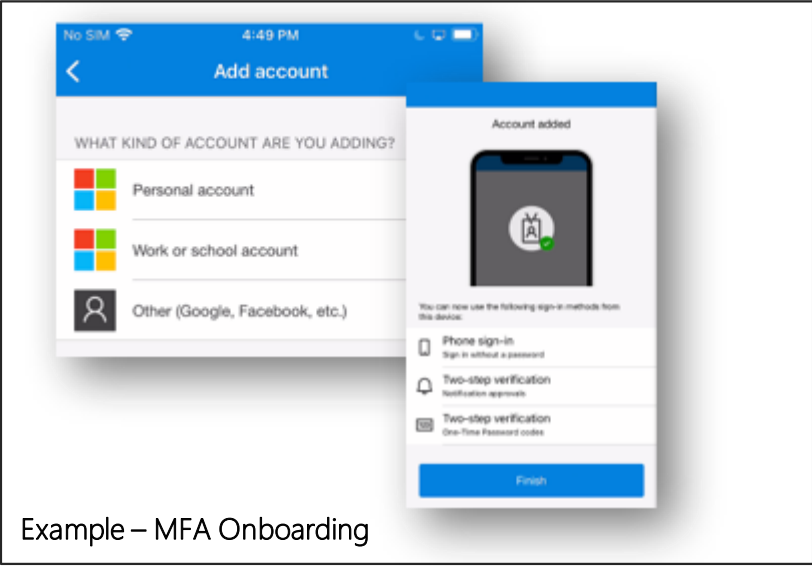
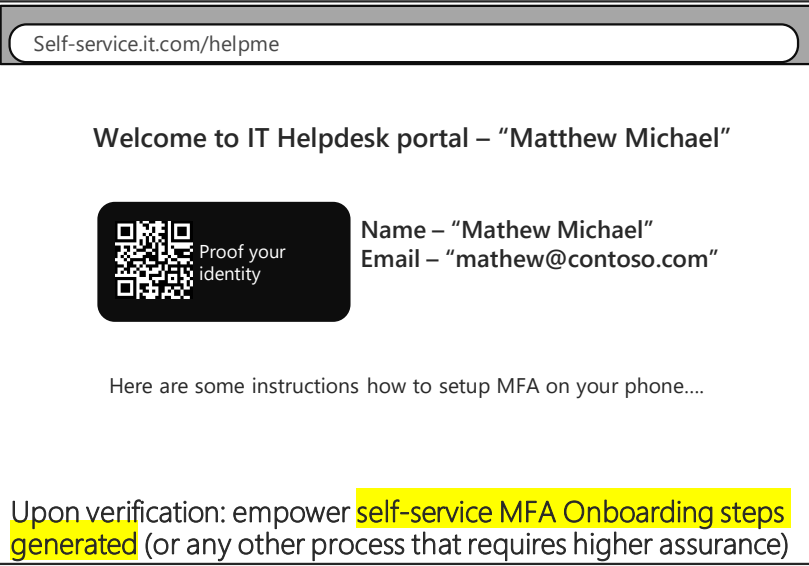
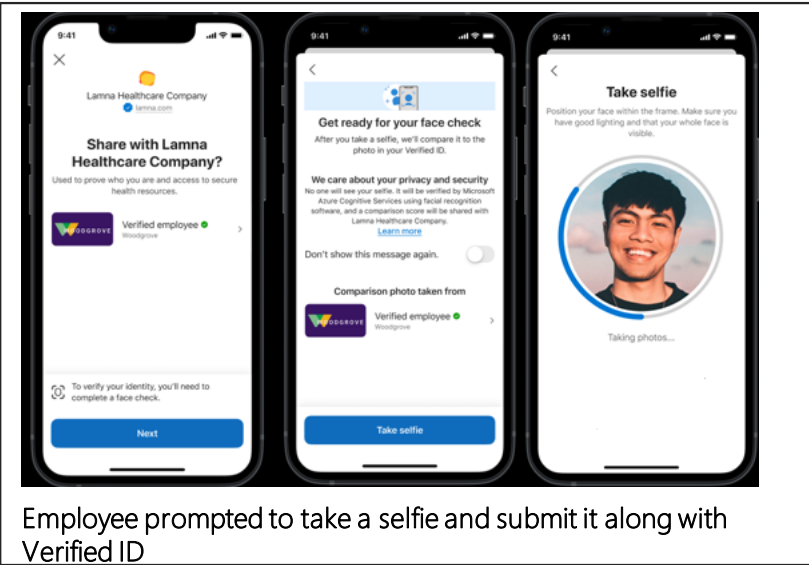
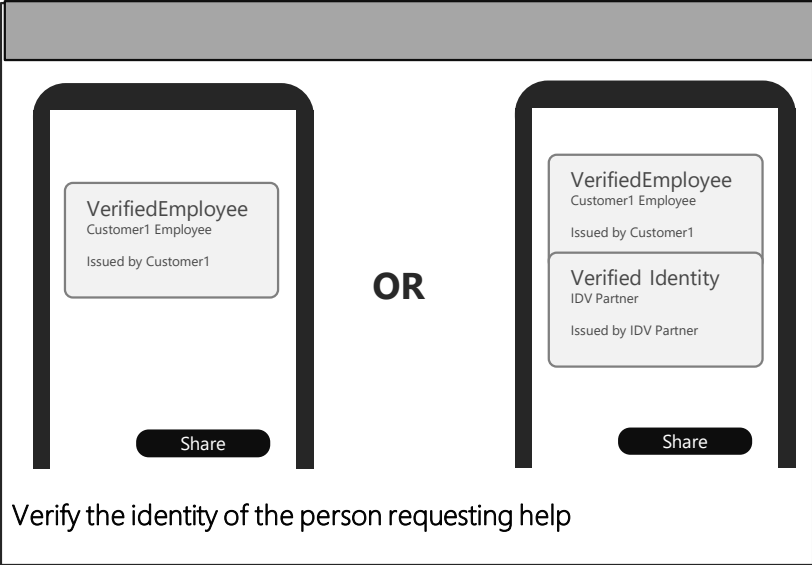
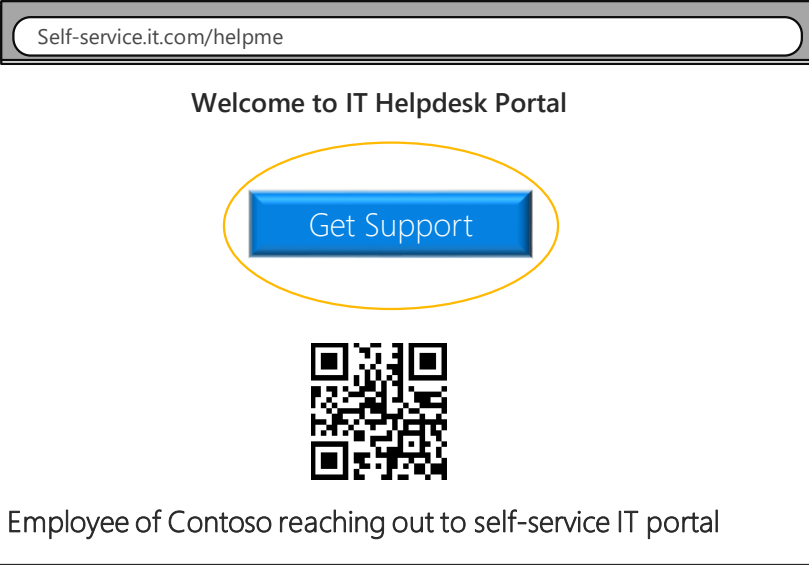
**Time: 3 minutes**

Sign-in to <http://myaccount.microsoft.com>

Get Face Check ready cred using Authenticator

**Time 1 minute**

# Adding verification to IT helpdesk



GitHub sample for generating a TAP code once the user is Verified –

<https://aka.ms/vcsample> (Navigate to .NET repository for samples and select sample5( with TAP) or sample6 (generic site))



# 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)



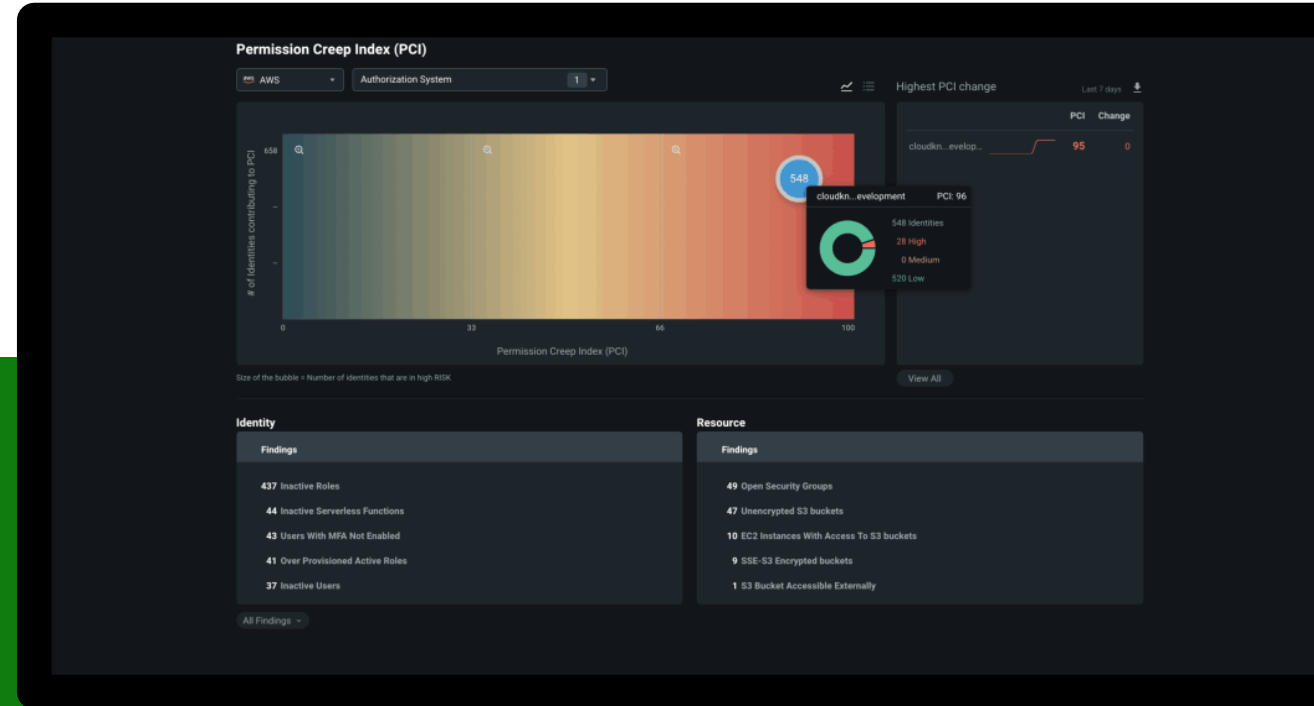
Get granular  
cross-cloud visibility



Enforce the principle of  
least privilege



Reduce permission risk



## 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





# 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)



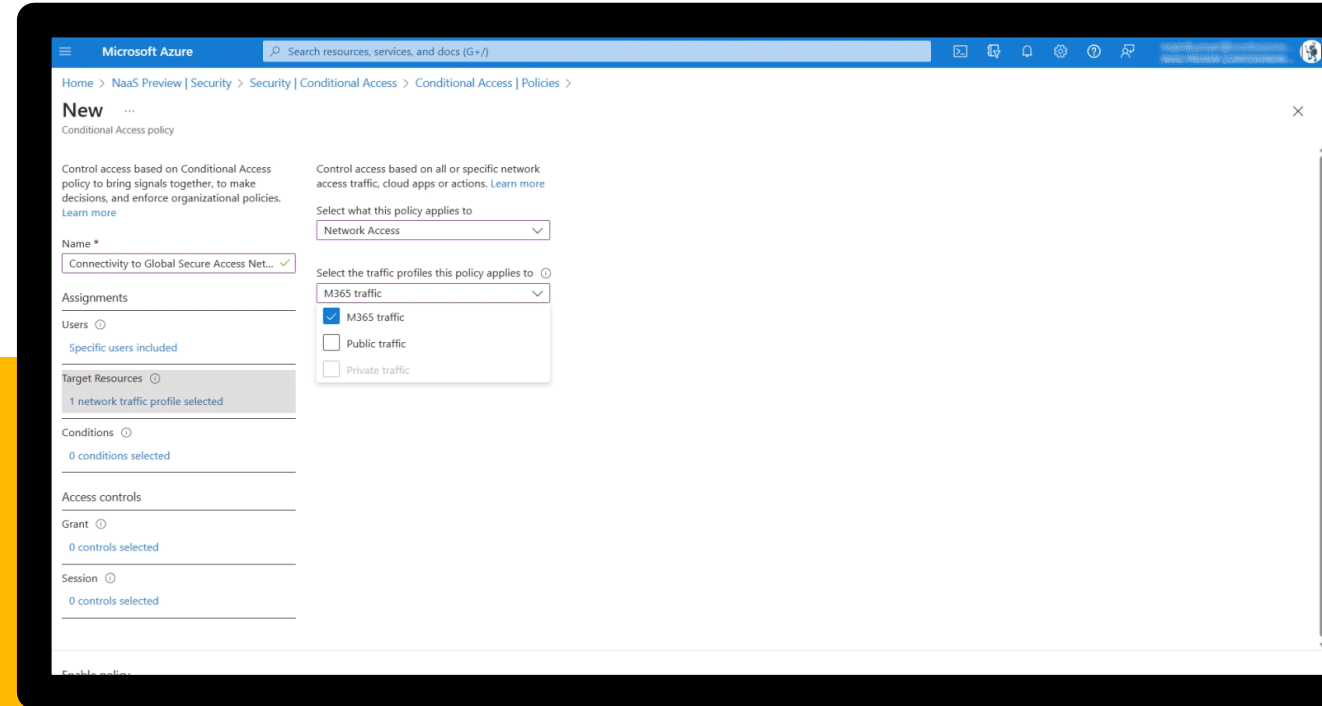
**Extend Conditional Access to your network**



**Modernize network security to protect users, apps, and resources**



**Enhance security and visibility for Microsoft 365 access**



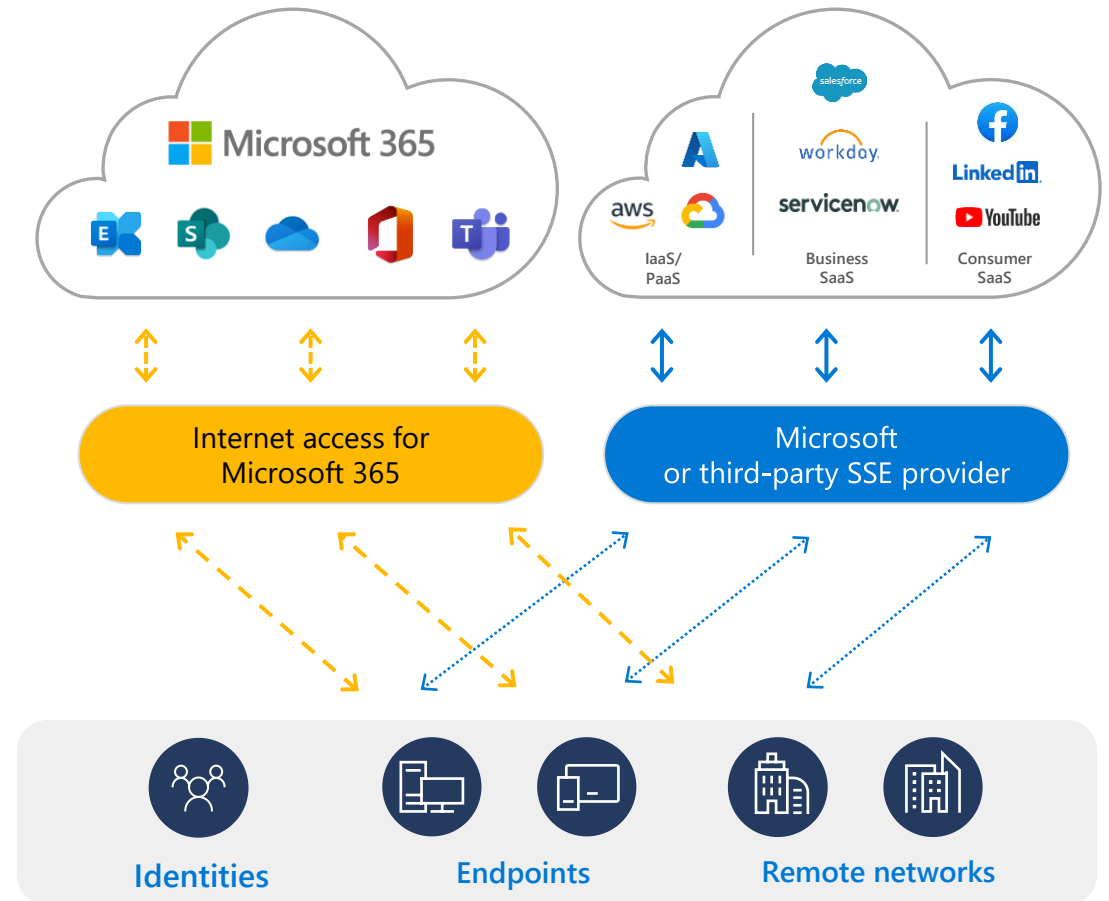
## Market challenge:

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

# Microsoft Entra Internet Access for Microsoft 365

Superior Microsoft 365 experience, visibility, and security

- **Easy to activate, zero maintenance**  
All OS types supported, in-built into Windows  
No new agent—integrated with Endpoint Manager, Microsoft Defender for Endpoint
- **Adaptive access controls**  
New network signals for Conditional Access  
Data exfiltration with tenant restrictions on any OS or client
- **Gain visibility into your environment**  
Faster threat detection with enriched context  
Near-real-time Microsoft 365 enriched security logs  
Threat correlation with cross-tenant, cross-workload insights
- **Optimized end-user experience**  
Optimal path routing for best-in-class performance and availability



Works side-by-side with third party solutions for private and public network access



# 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



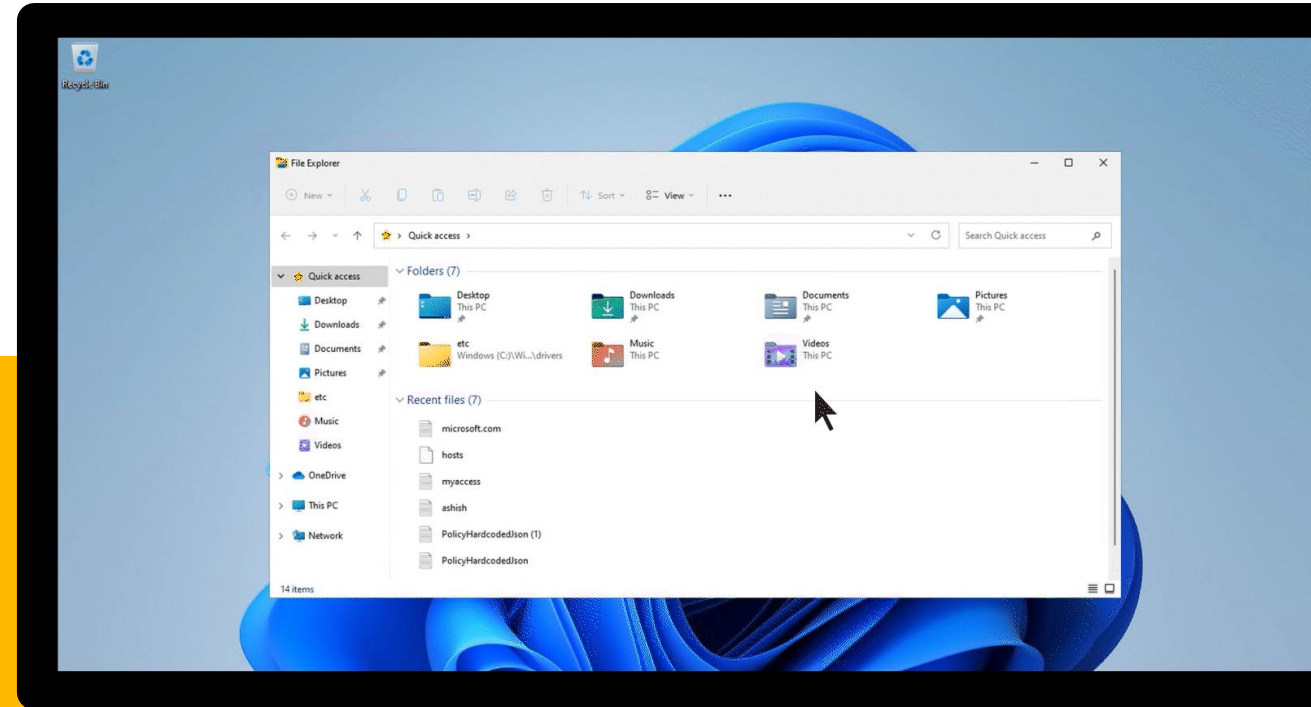
Modernize private app access with an identity-centric ZTNA



Prevent breaches with adaptive access controls



Enhance security through granular app segmentation



## 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

# 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

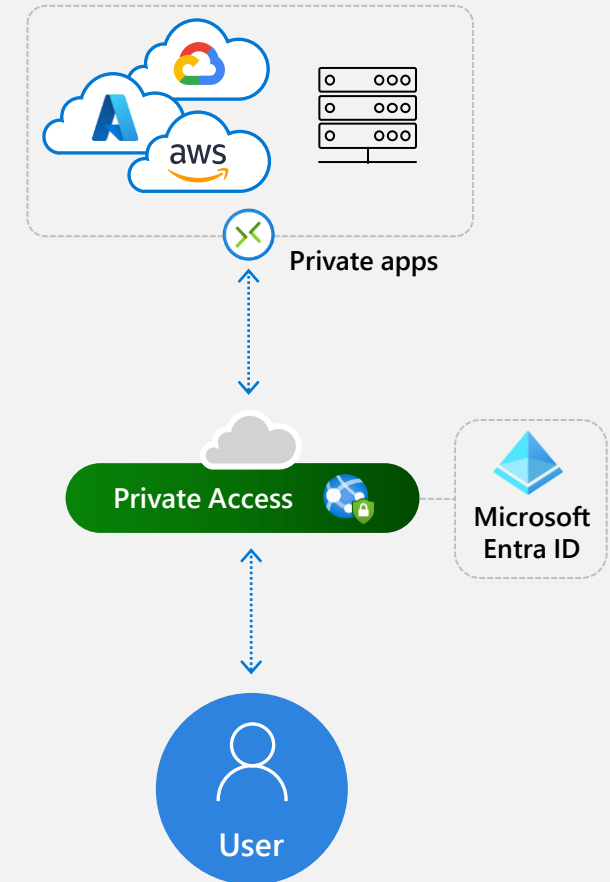
**Coming soon:** Micro-segment based on process identity

## » 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)

**Thank You!**

