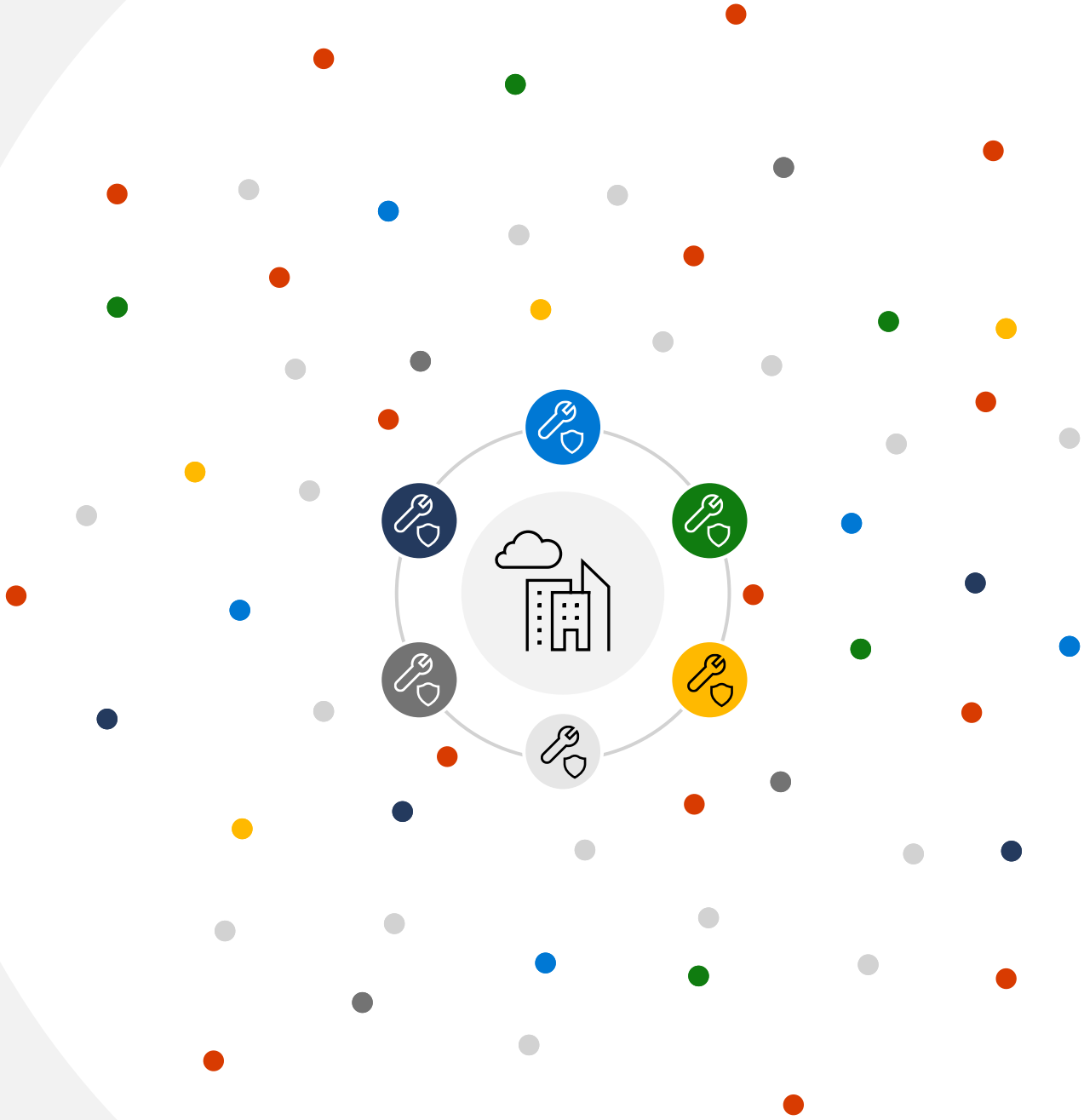
Microsoft Security

Microsoft Entra

Secure access for a connected world

Today’s digital landscape and its challenges

- Rapid expansion of diverse access points
- Increasing volume and sophistication of attacks
- Overlapping identity and access security tools



What is Microsoft Entra

Microsoft Entra is a product family name for Microsoft's identity and access solutions.

It is not a replacement of Azure Active Directory (Azure AD). Azure AD is our hero identity solution and part of Microsoft Entra.

We introduced a new name because we expanded in several new categories and needed a name to convey modern access security across broad range of products.

Microsoft Entra

Secure access for a connected world.

Azure
Active Directory

Microsoft Entra
Permissions Management

Microsoft Entra
Verified ID

Microsoft Entra
Identity Governance

Microsoft Entra
Workload Identities

Protect access to any app or resource

Safeguard your organization by protecting access to every app and every resource for every user.

Secure and verify every identity

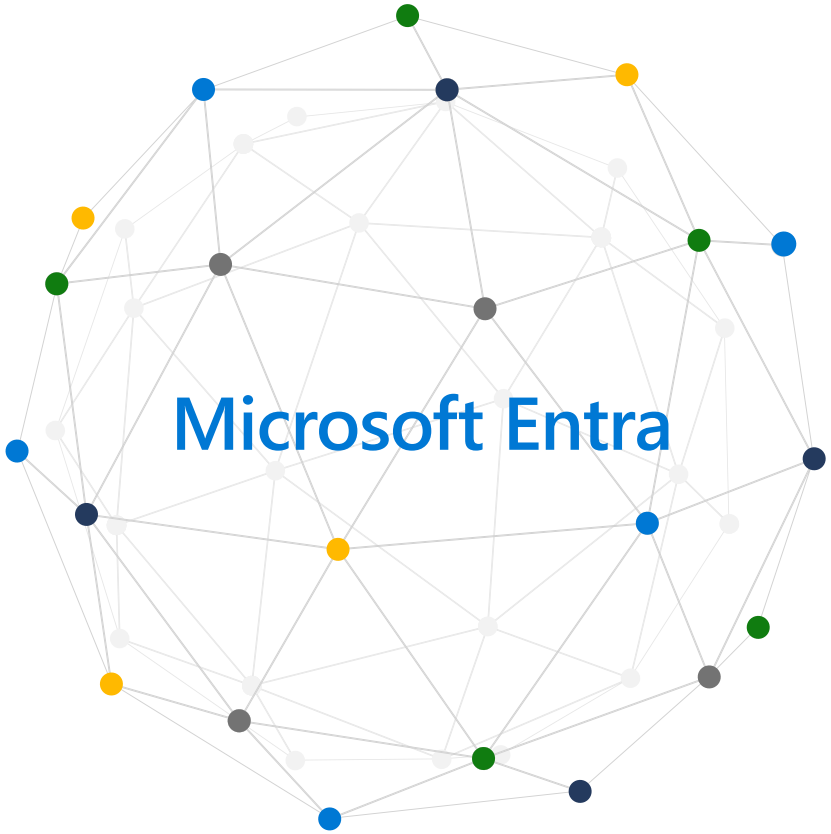
Effectively secure every identity including employees, customers, partners, apps, devices, and workloads across every environment.

Provide only necessary access

Discover and right-size permissions, manage access lifecycles, and ensure least privilege access for any identity.

Simplify the experience

Keep your users productive with simple sign-in experiences, intelligent security, and unified administration.



Secure access for a connected world.

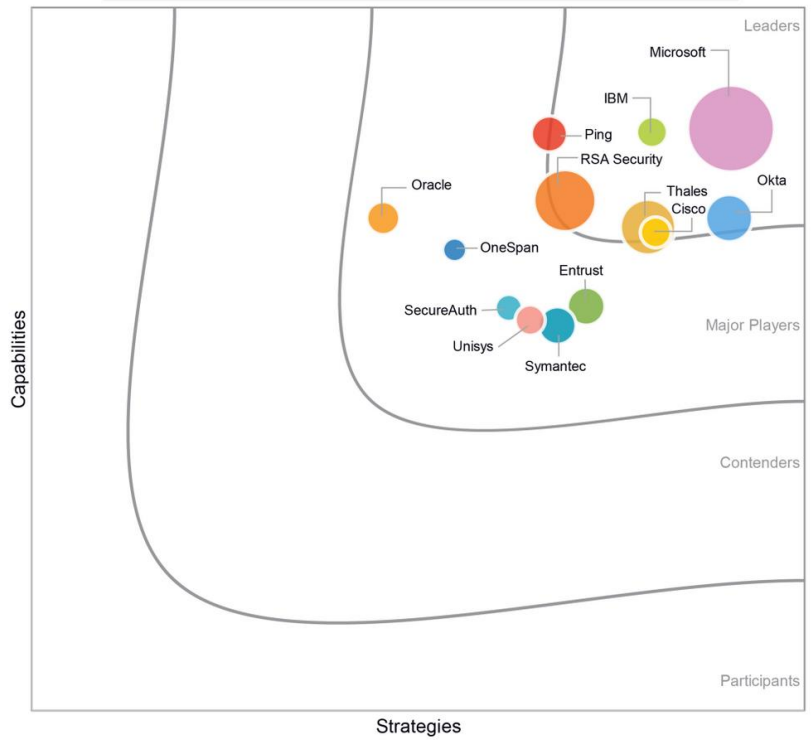
Microsoft Entra

Microsoft - Consistently recognized as a Leader by industry analysts

Gartner

Source: Gartner Magic Quadrant for Access Management, November 2022

IDC



Source: IDC MarketScape Worldwide Advanced Authentication for Identity Security, 2021

Microsoft Entra

Secure access for a connected world.

Azure
Active Directory

Microsoft Entra
Permissions Management

Microsoft Entra
Verified ID

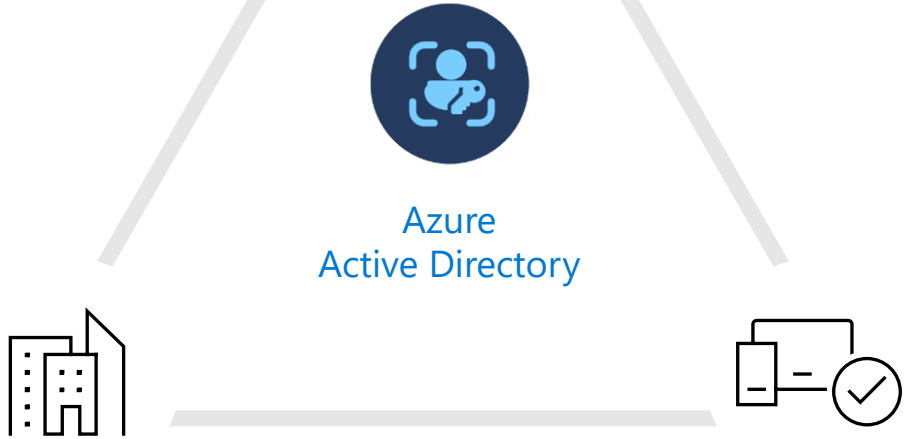
Microsoft Entra
Identity Governance

Microsoft Entra
Workload Identities

Azure AD - the world's largest cloud identity service

Thousands of organizations, millions of active users, billions of daily requests

300K+
Azure AD
Premium organizations



425M+
Azure AD
Monthly active users

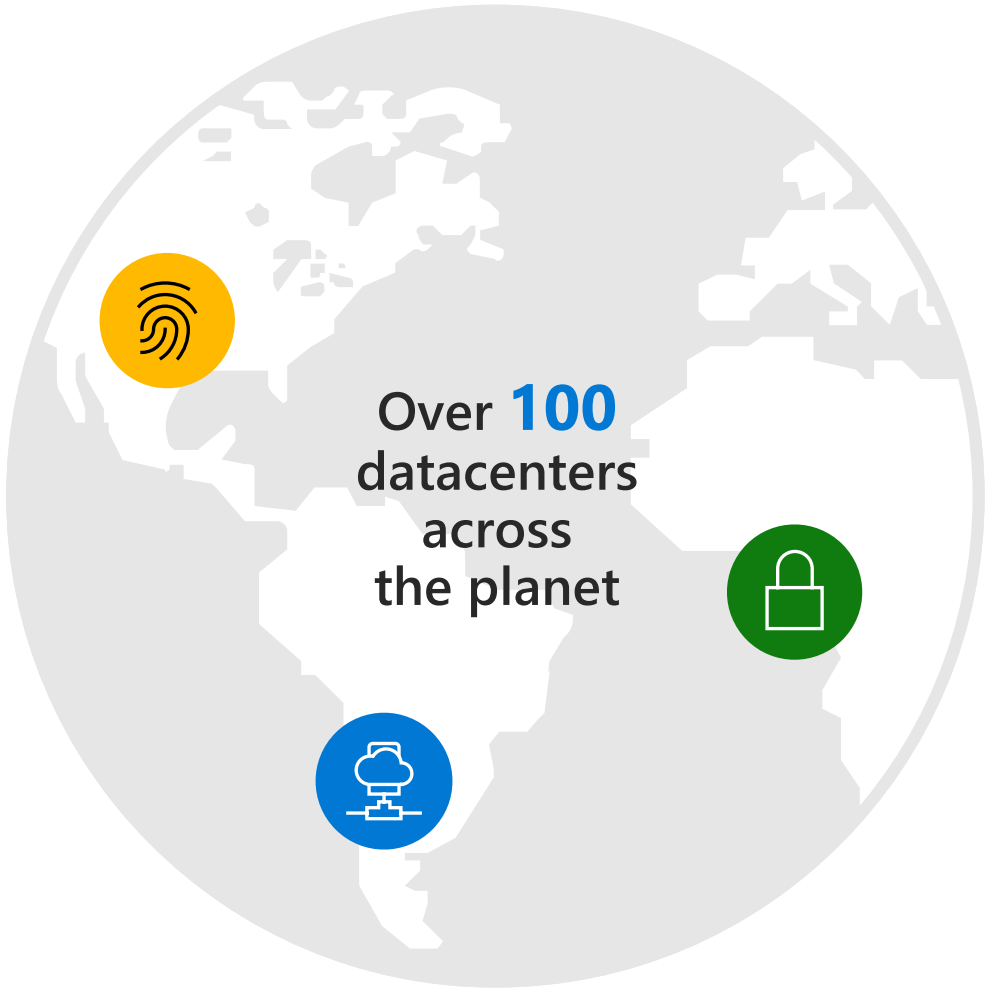
30B+
Azure AD
Daily authentication requests

Engineered for availability and security

Cloud-native, hyper-scale, multi-tenant architecture

Each **physical datacenter** protected with world-class, multi-layered protection, and engineered for maximum availability

Global cloud infrastructure with secure hardware and data segregation

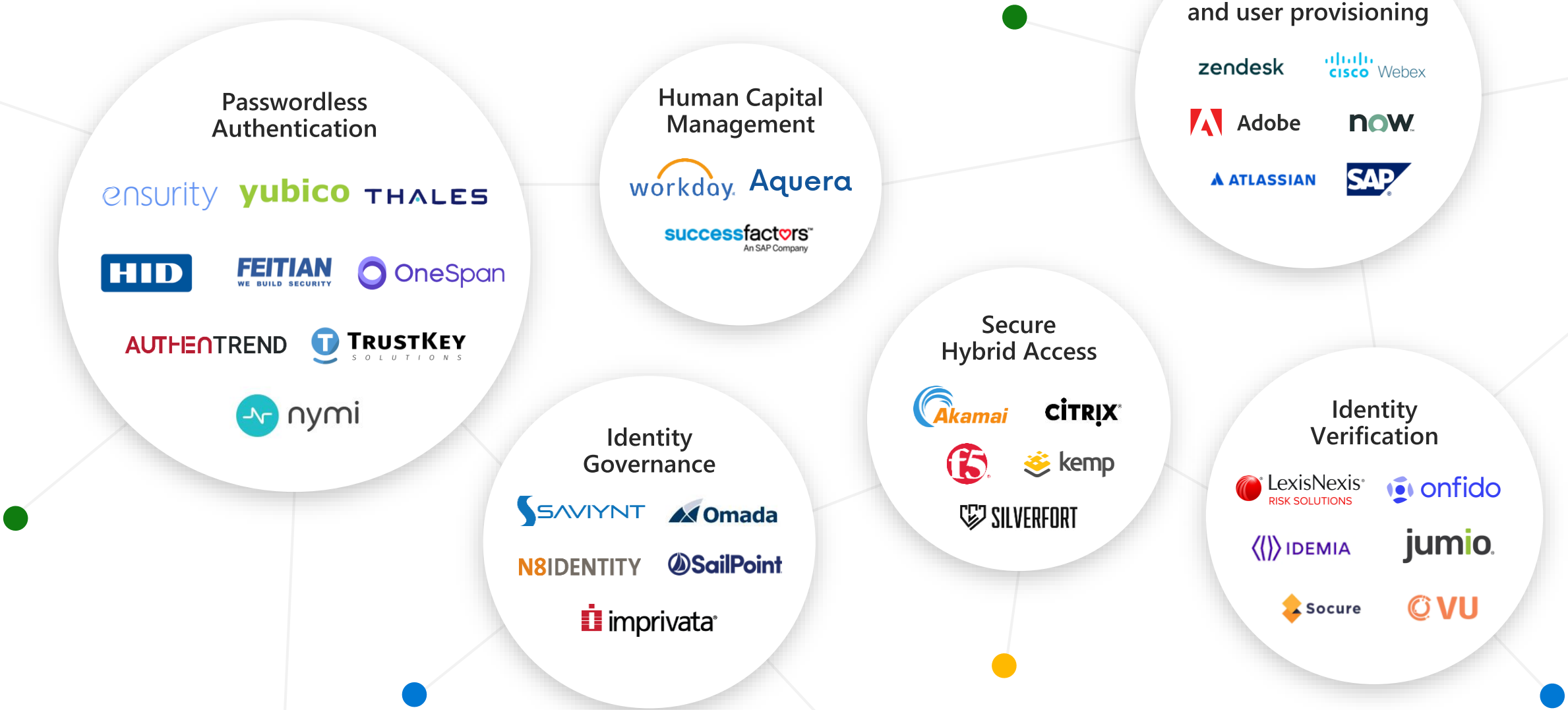


99.99%
New Azure AD Service Level Agreement
(in effect from April 1st, 2021)

Secured with cutting-edge **operational security**

- → Restricted access
- → 24x7 monitoring
- → Global security experts

Open and interoperable ecosystem



Azure Active Directory

Protect your users, apps, workloads, and devices.

Secure adaptive access

Seamless user experiences

Unified identity management

Secure adaptive access

Protect access to resources and data with strong authentication and risk-based access policies

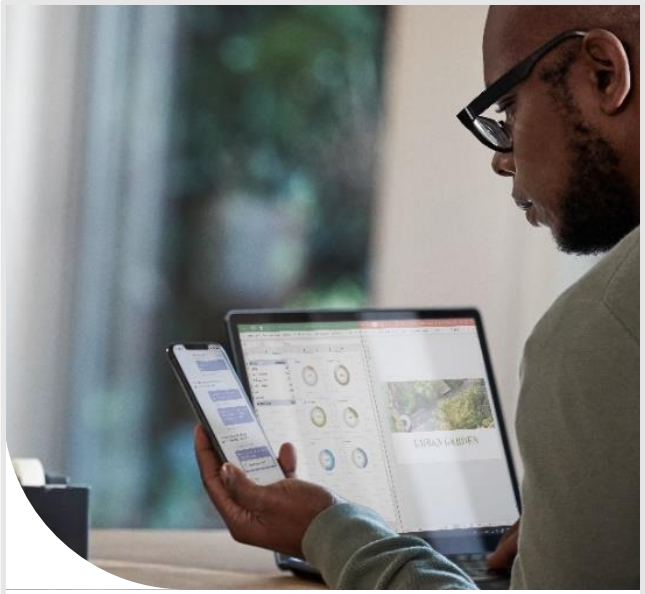
User-friendly multifactor authentication (MFA) support

Configurable Conditional Access policies based on context and risk assessment

User and entity behavior analytics (UEBA) to automatically protect against identity compromise

Multi-factor authentication

Verify user identities with strong authentication



We support a **broad range of multi-factor authentication options**

Including passwordless technology

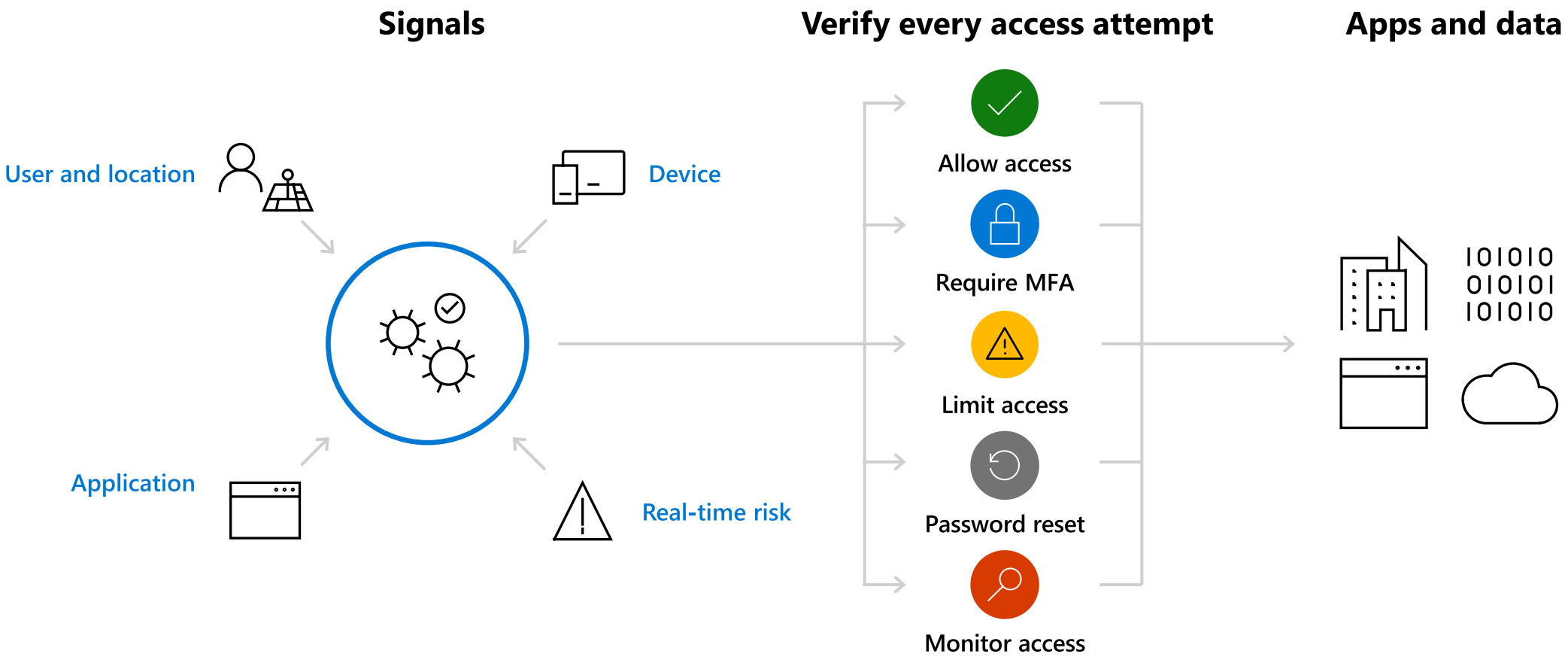
- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics

- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multi-factor authentication **prevents 99.9% of identity attacks**

Protect resources with Conditional Access

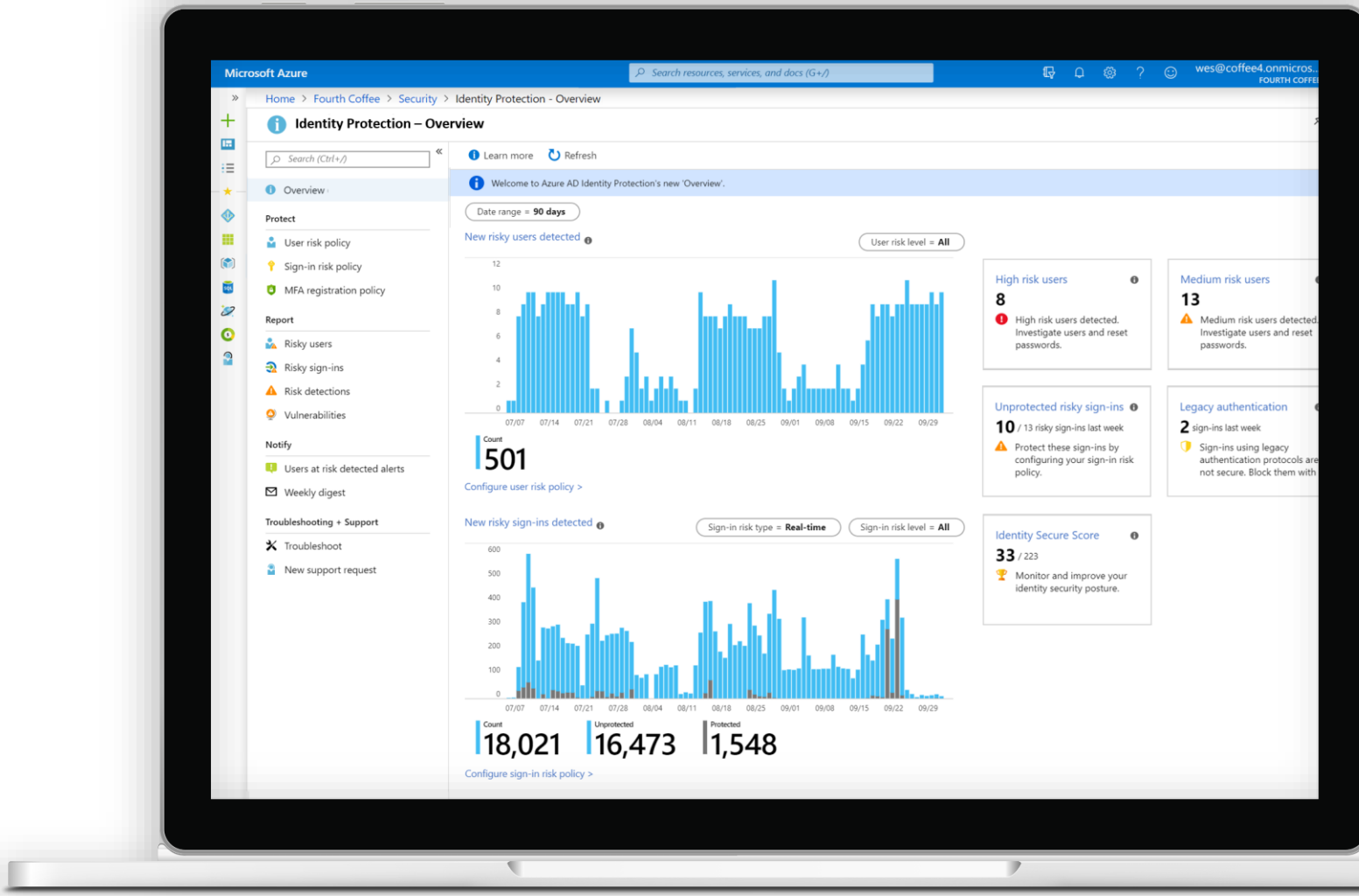
Enable Zero Trust with strong authentication and adaptive policies



Identity protection

Intelligently detect and respond to compromised accounts

- Enhanced logging
- Threat alerts
- Risk scores
- Sign-in reports
- Privileged access insights



Azure Active Directory

Protect your users, apps, workloads, and devices.

Secure adaptive access

Seamless user experiences

Unified identity management

Seamless user experiences

Provides an easy, fast sign in experience to keep your users productive, reduce time managing passwords, and increase end user productivity

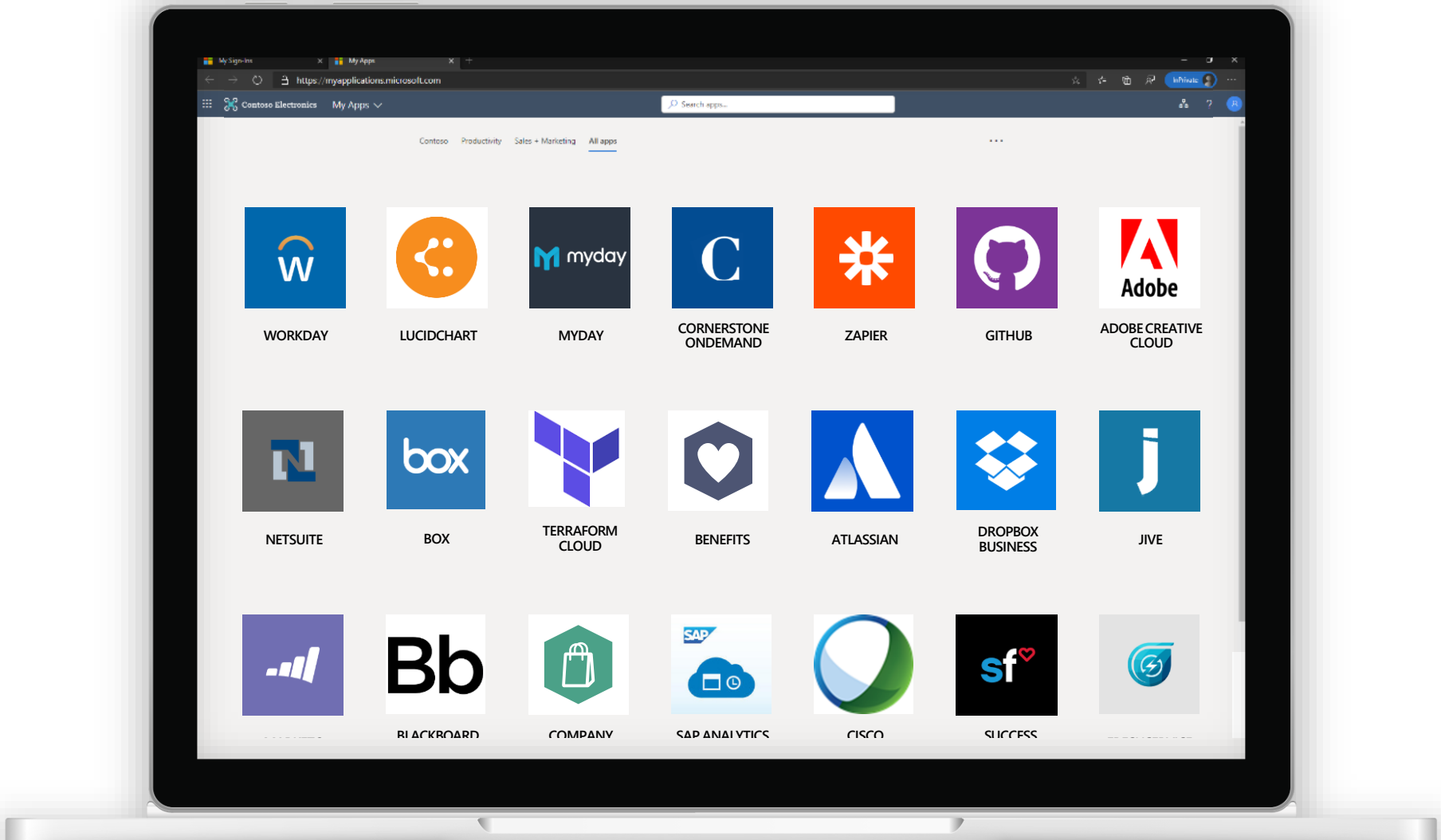
Single sign-on (SSO) for any user type and any app

End user self-service portal to discover and launch applications, request access, and manage profile

Convenient, phishing resistant passwordless credentials

Enable seamless user experience with single sign-on

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



Enable employees to manage their own identity

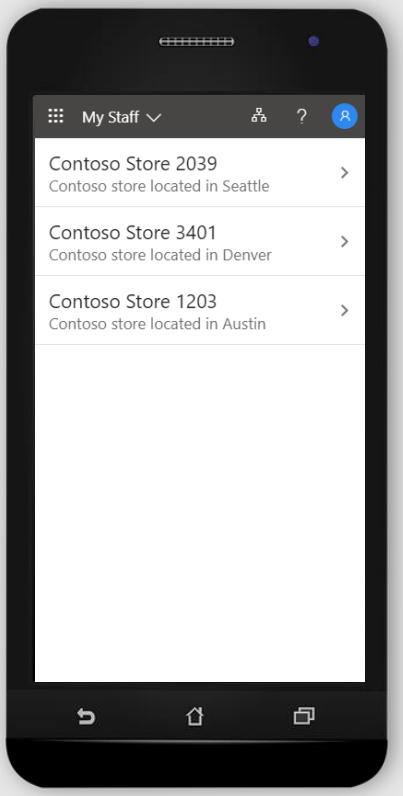
Simplify access to resources and self-service to keep your users productive and minimize IT friction

- Centralized application launch and discovery portal
- User account management and self-service password reset
- Detect and report risky sign-in behavior

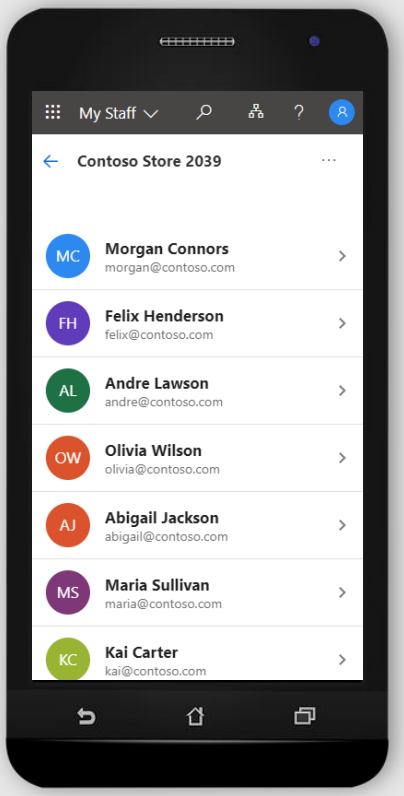
Azure AD can help IT reduce help-desk calls for password resets by up to 75%

Empower Frontline Managers and Workers

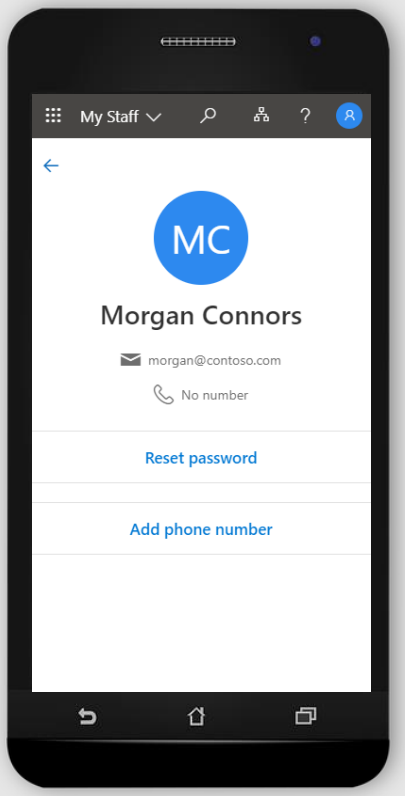
Delegated user management for Frontline Managers



Manage multiple teams



View your team members



Manage passwords and phone numbers

Changing the game with passwordless

Make sign-in even more seamless and secure

Windows Hello

Microsoft Authenticator

FIDO2 Security Keys

Passwordless Momentum

200M+

Active passwordless users

Azure Active Directory

Protect your users, apps, workloads, and devices.

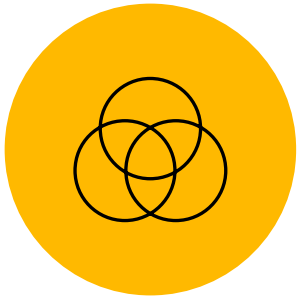
Secure adaptive access

Seamless user experiences

Unified identity management

Unified identity management

Manage all your identities and access to all your applications in a central location for cloud and on-premises to improve visibility and control



Provide a common identity for your users and manage your hybrid identity from the cloud

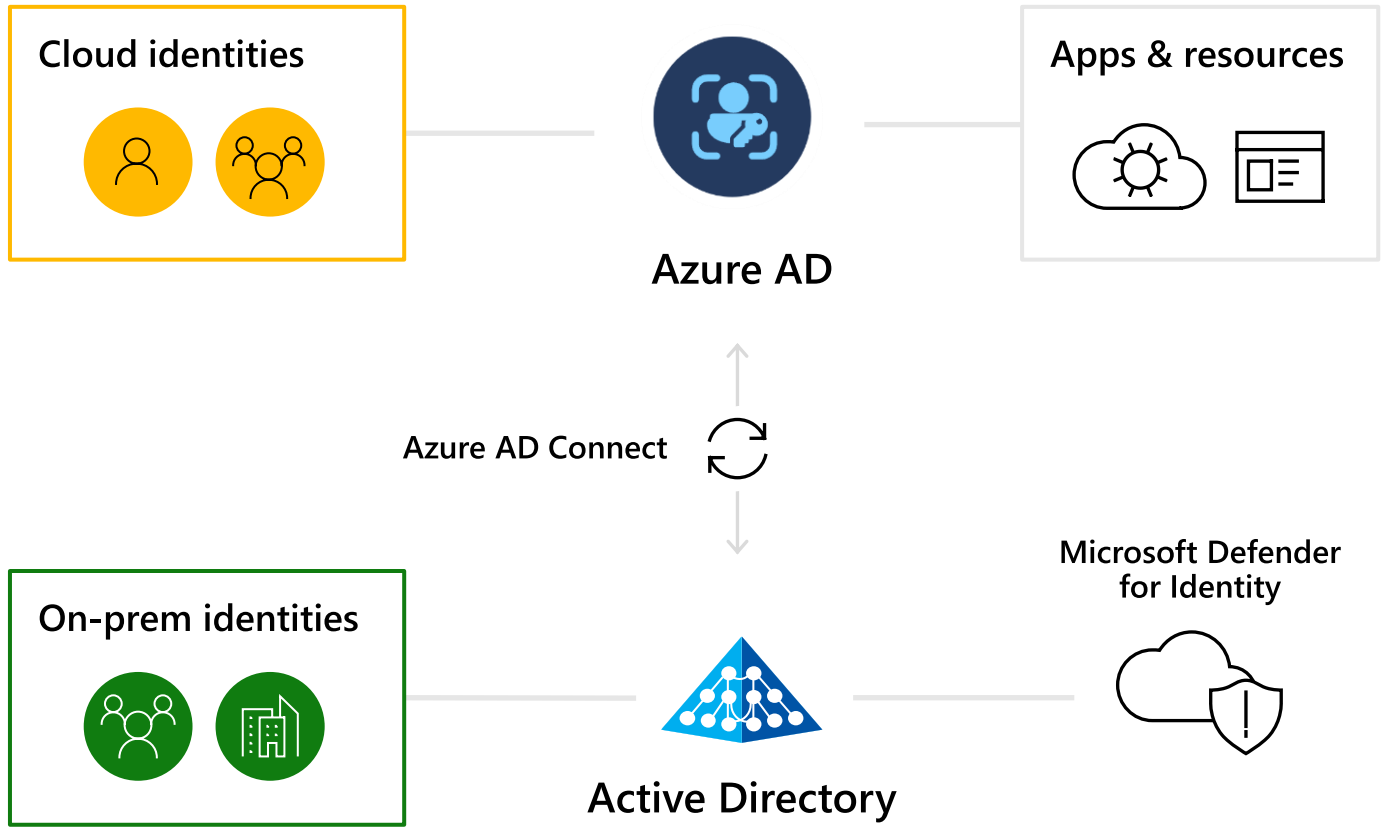
Connect any app in any cloud or datacenter across your hybrid environment

Efficient identity management and administration for employees, partners, and customers

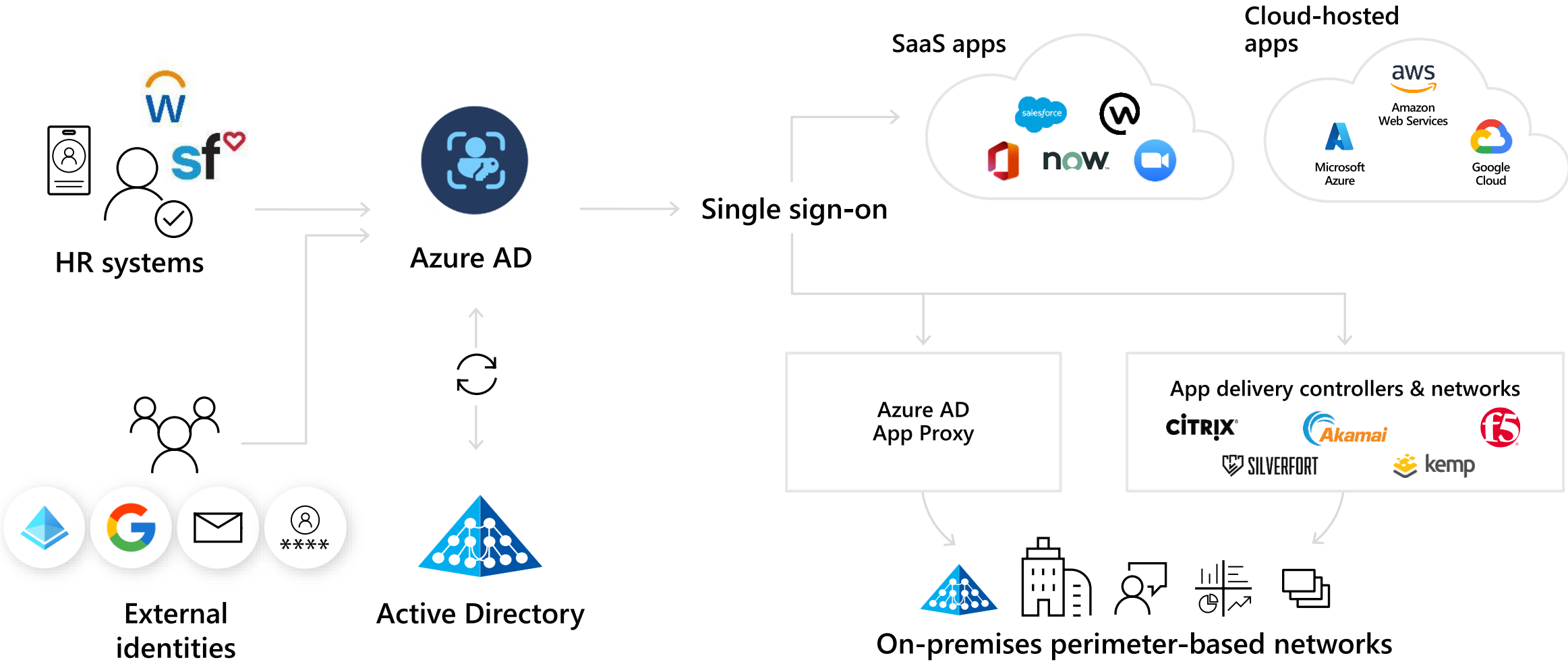
Provide a common identity for your users

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

- Sync identities with 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 & resolve vulnerabilities and assess threats efficiently with Microsoft Defender for Identity and advanced protection with Azure AD

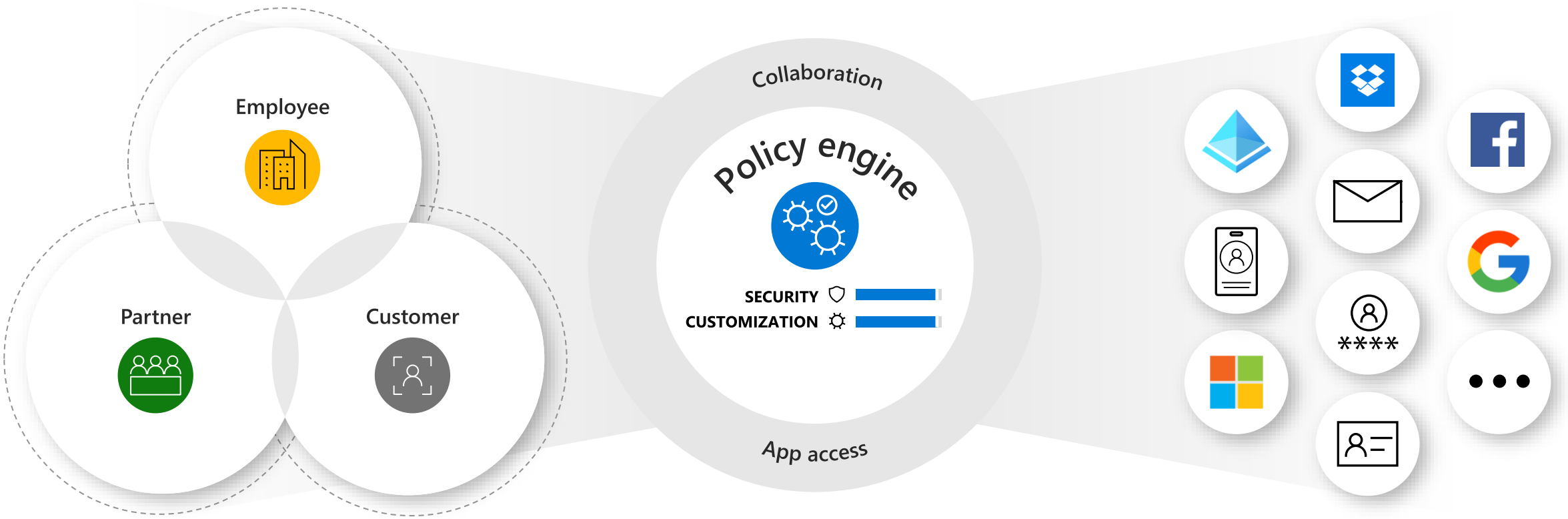


Connect your workforce to any app



Efficiently manage external identities

Grant secure access to your employees, partners, and customers and facilitate B2B collaboration



Microsoft Entra

Secure access for a connected world.

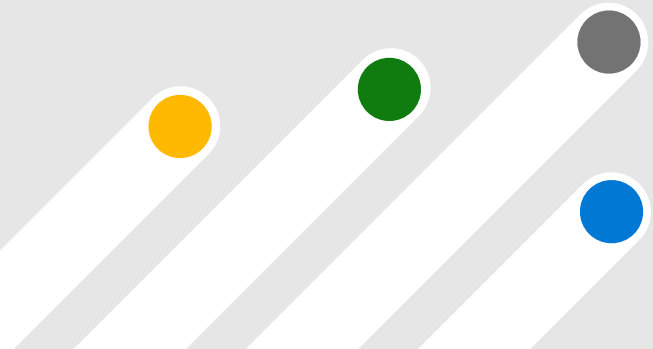
Azure
Active Directory

Microsoft Entra
Permissions Management

Microsoft Entra
Verified ID

Microsoft Entra
Identity Governance

Microsoft Entra
Workload Identities



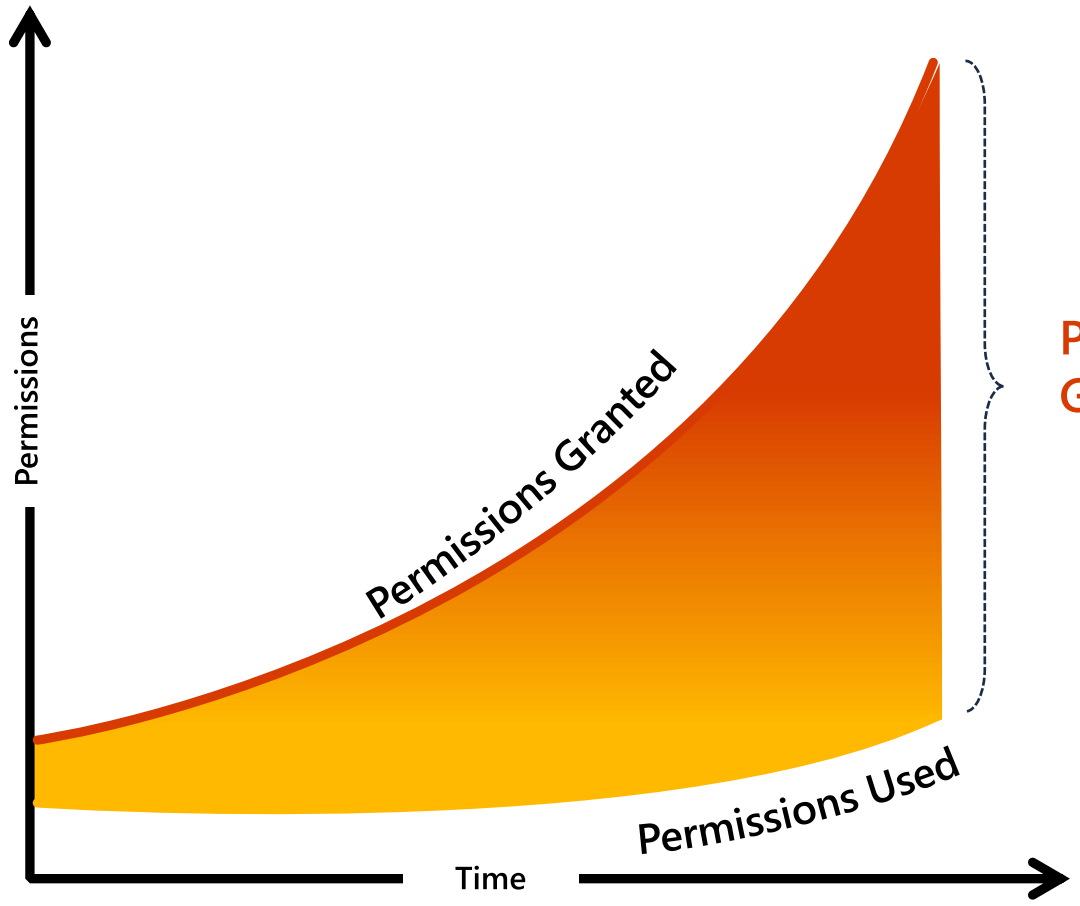
Multicloud adoption brings new permission challenges

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

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

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

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 multicloud environments

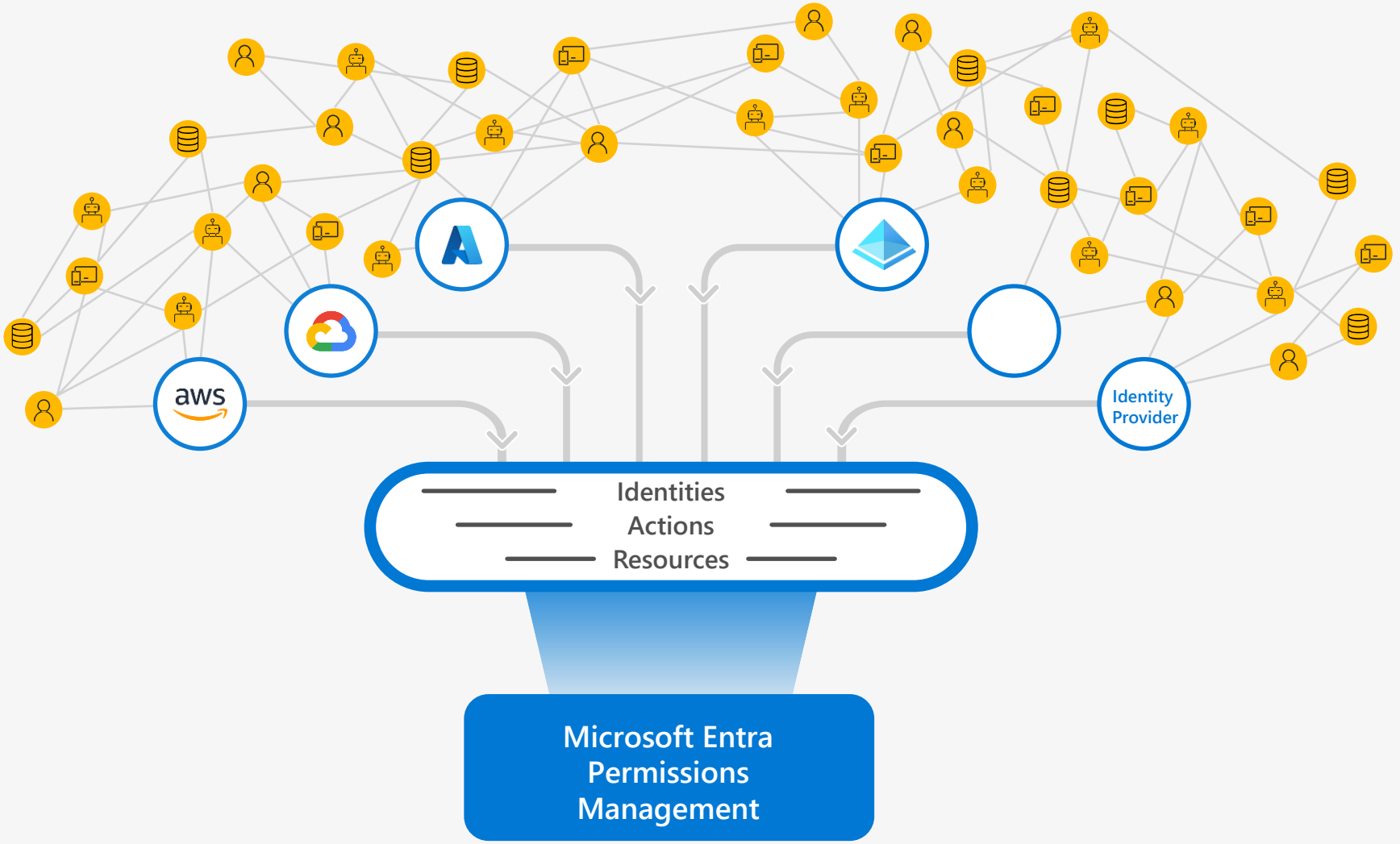
Increased risk of breach from accidental or malicious permission mis-use

Managing permissions across multicloud environments requires a new approach

Today's static, outdated approach	A new, dynamic approach
~~Grants permissions based on job roles and responsibilities~~	Grants permissions based on historical usage and activity
~~IAM admins manually grant permissions which are not time-bound~~	Allow temporary access to high-risk permissions on-demand
~~Permission clean-up is done manually on an as-need basis~~	Continuously monitor and right-size identities to prevent privilege creep

Microsoft Entra Permissions Management

Manage permissions based on historical usage and activities



Permissions Management

One unified model to manage permissions of any identity across any cloud.

Discover & Access

Get a **comprehensive view** of every action performed by **any identity** on any resource.

Remediate & Manage

Right-size permissions based on usage and activity and enforce **permissions on-demand** at cloud scale.

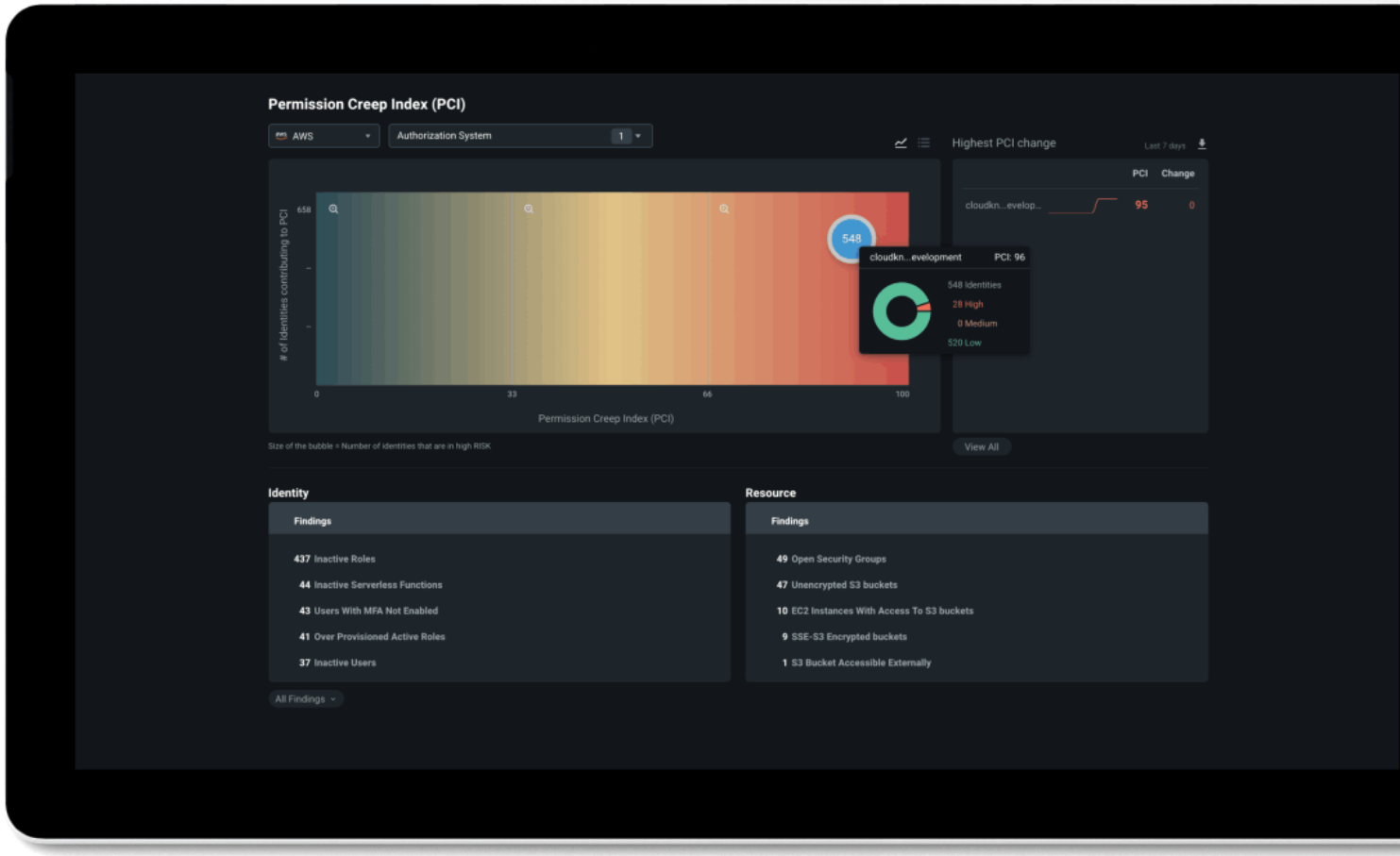
Monitor & Alert

Detect **anomalous permission usage** and generate detailed **forensic reports**.

Discover & Assess

Get a multi-dimensional view of your permission risk

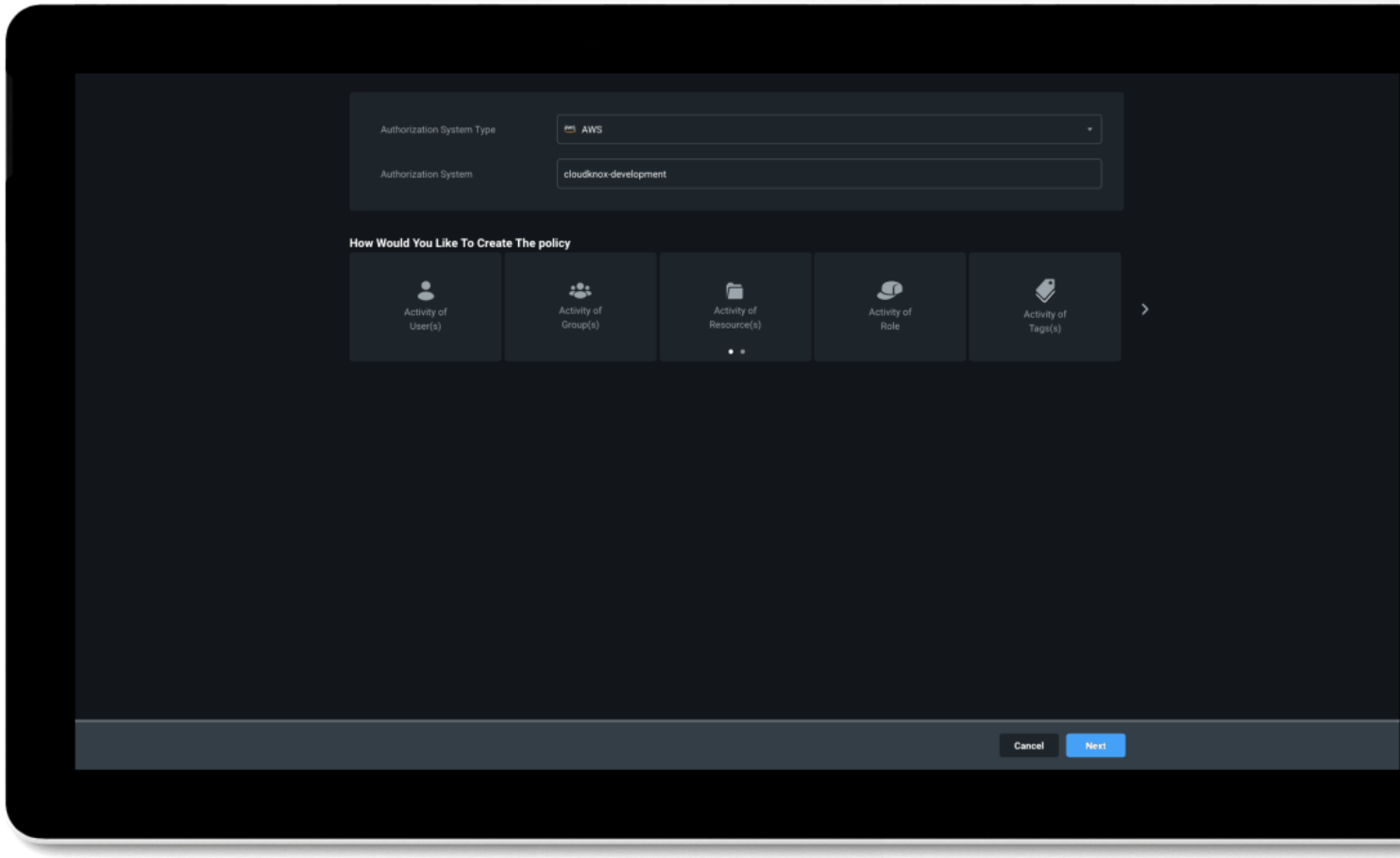
- Understand your risk profile with the Permission Creep Index, a single metric that evaluates the gap between permissions granted and permissions used
- Get detailed usage analytics and uncover every action performed by any identity on any resource



Remediate & Manage

Automate least privilege policies

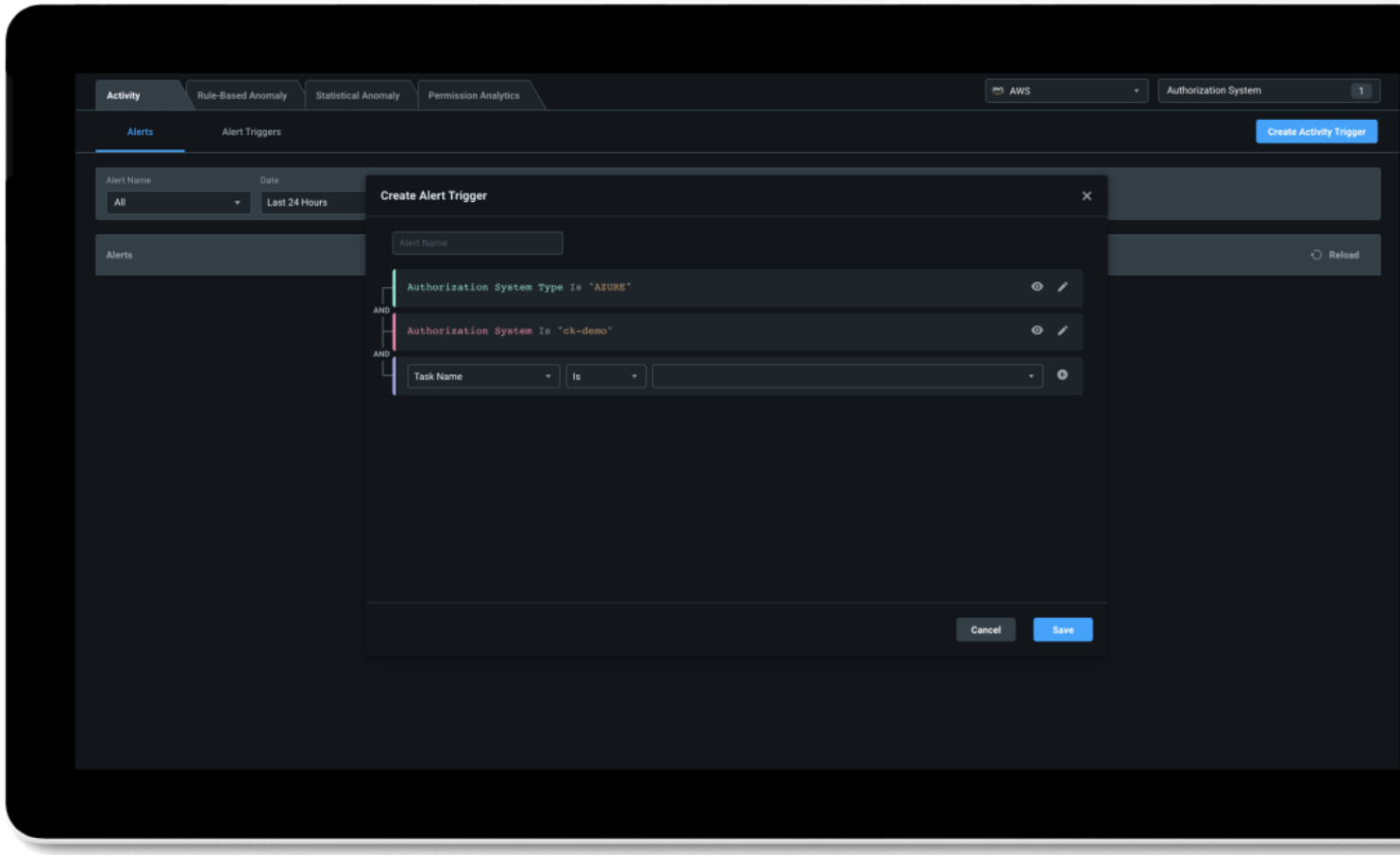
- Remove unused and excessive permissions by creating new policies/roles in a few clicks and use least privilege derived templates to enforce Just-In-Time access
- Grant identities permissions on-demand for a time-limited period or an as-needed basis



Monitor & Alert

Streamline anomaly detection and accelerate incident response

- Track permissions usage patterns and with customizable alerts
- Strengthen your security posture with high-precision machine learning-based anomaly detections
- Generate detailed reports and cyber kill chain analysis to speed up threat investigation and remediation



Microsoft Entra

Secure access for a connected world.

25.6 billion
attempts to hijack enterprise customer accounts detected and blocked by Microsoft from Jan – Dec 2021.

Identity is the New Battleground, Cyber Signals, February 2022

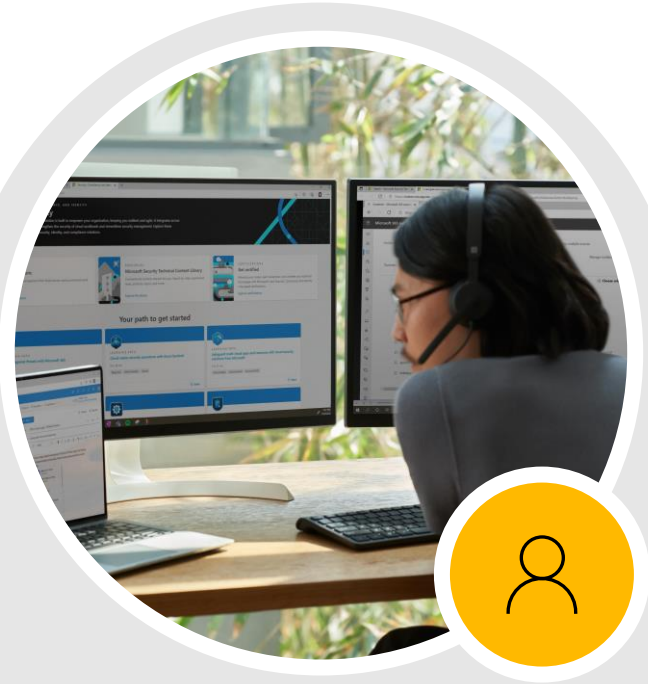
Identity & Access Management
Trends & Challenges

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

Regulations are increasing
65% of the world's population will be covered by privacy regulations by 2023

Modern workplace is hybrid
Remote identity proofing processes are unsatisfactory for 82% of organizations

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.

Verified ID

Enable more secure interactions while respecting privacy with an industry-leading global platform.

Fast remote onboarding

Validate identity information for trustworthy self-service enrollment and reduced time-to-hire.

More secure access

Quickly verify an individual's credentials and status to grant least-privilege access with confidence.

Easy account recovery

Replace support calls and security questions with a streamlined self-service process to verify identities.

Custom business solutions

Easily build solutions for a wide range of use cases with our developer kit, APIs, and documentation.

92% of organizations perform identity verification today

82% wish there was a better way...

- Onboarding for employees, contractors, customers
- Access to high-value apps and resources
- Self-service account recovery

Source Microsoft, survey of 3000 US-based companies, greater than 500 users

How verifiable credentials works

Verifier

Requests proof of claims. Verifies satisfaction of requirements.

Approves requests via wallet. Presents credentials to verifier.

Issuer

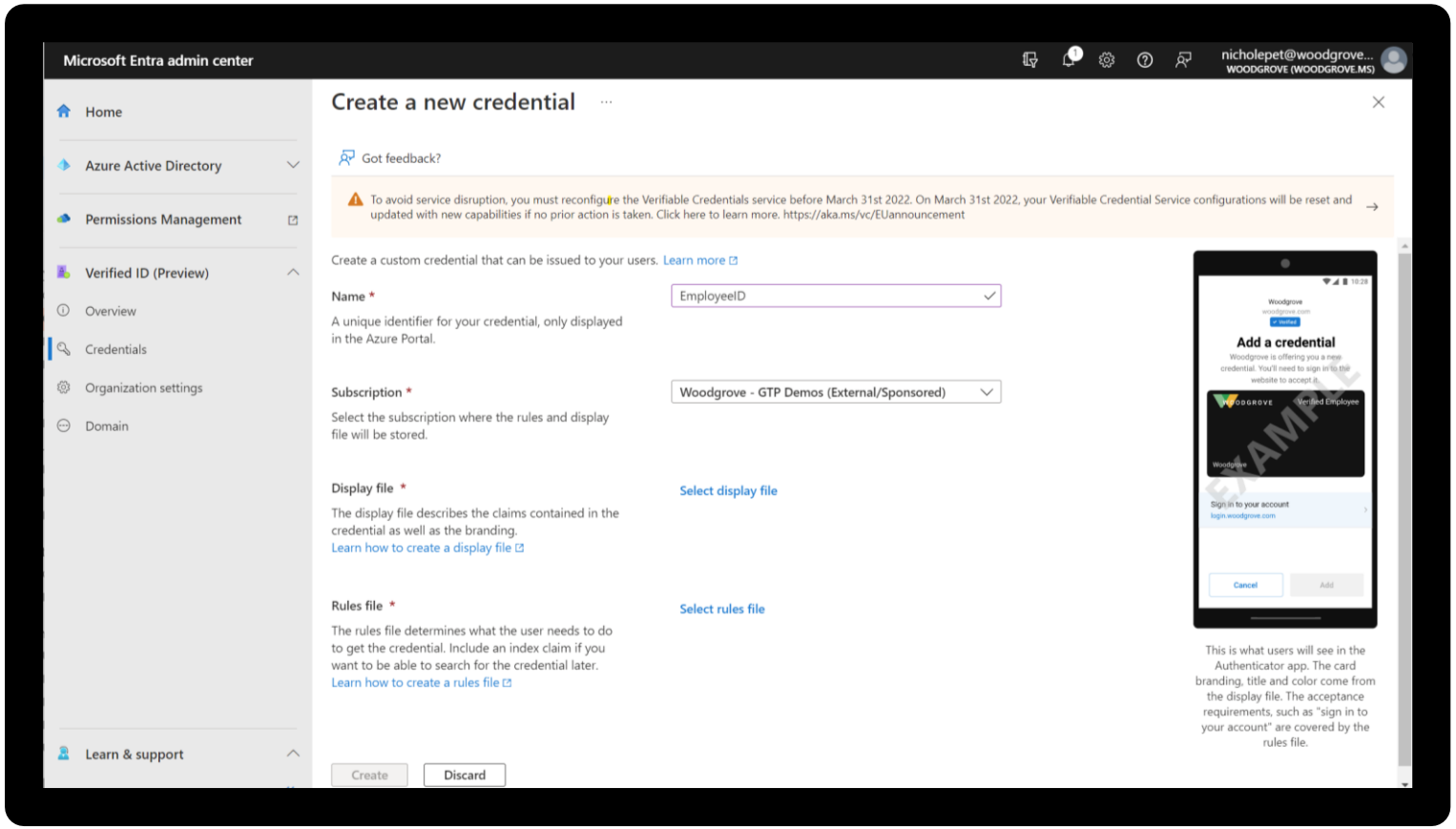
Attests to claims. Grants digitally signed credentials to user.

Identity verification for your organization

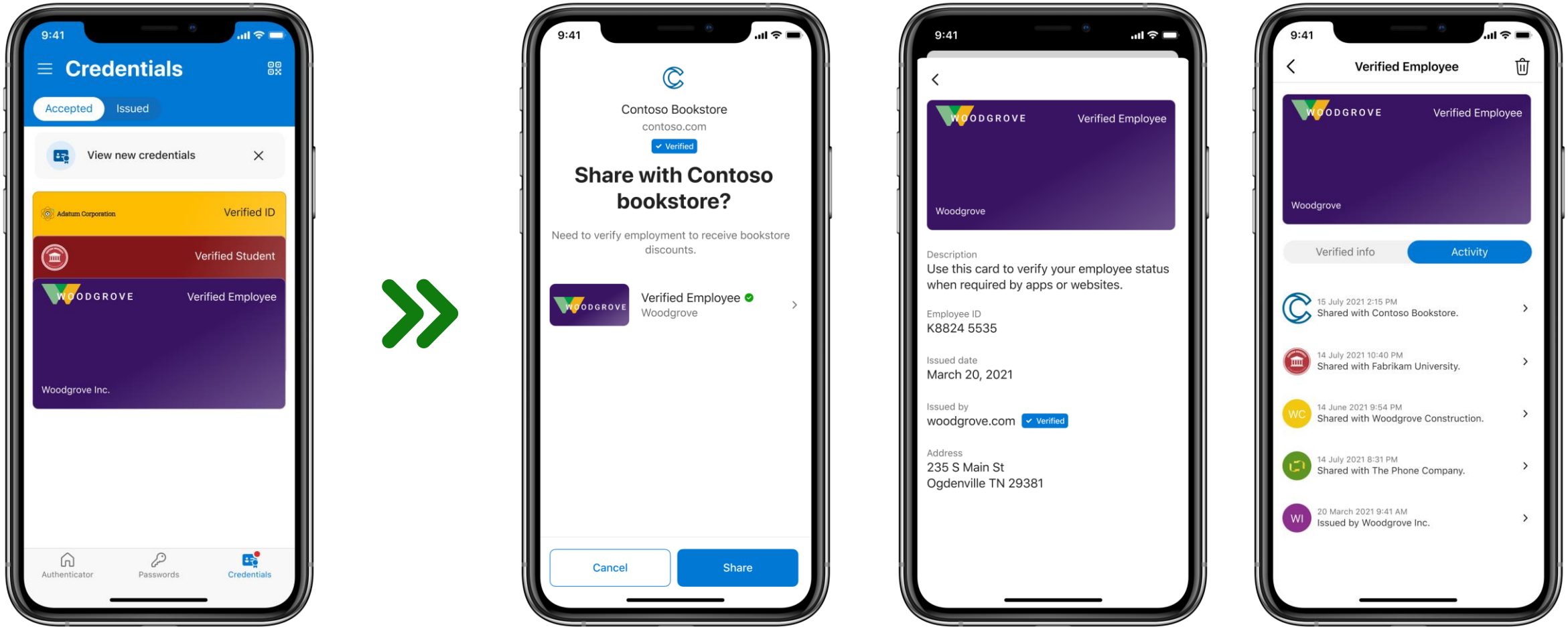
Issue easily
Use templates or simple steps to create verifiable credentials for employees, partners and customers.

Verify confidently
Rapidly validate attestations from the issuer with explicit approval from the holder.

Use anywhere
Verified ID credentials are based on open standards; supported by identity verification partners



End user experience: Verification



Easy to use and secure

Verifiable

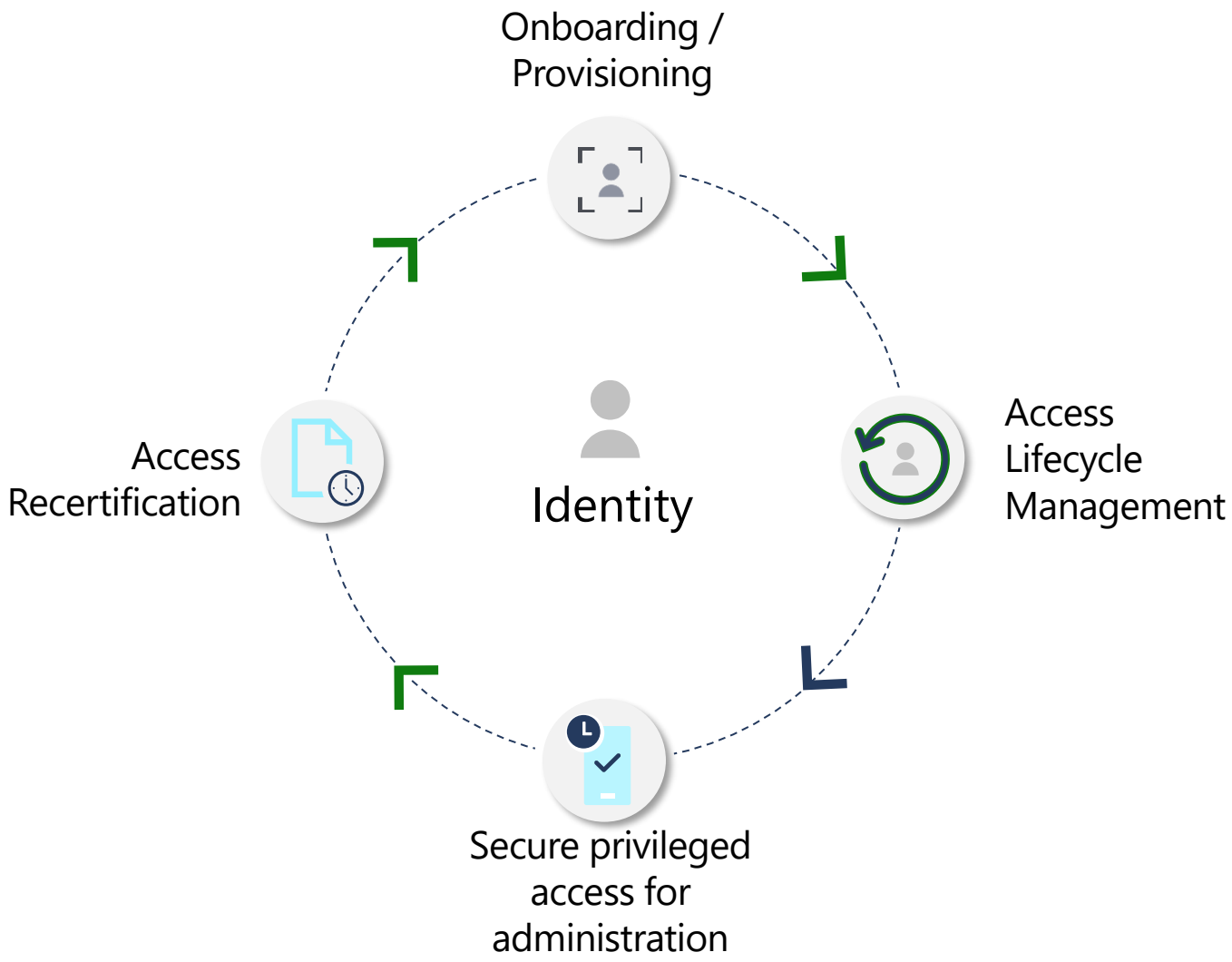
Transparent

Convenient

Microsoft Entra

Secure access for a connected world.

What is Microsoft Entra Identity 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?

Identity Governance

Identity governance increases employee productivity and helps meet compliance and regulatory requirements.

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.

Simply powerful. Powerfully simple.

Cloud-based, for straightforward deployment and operation. Support both cloud and on-premises apps and resources.

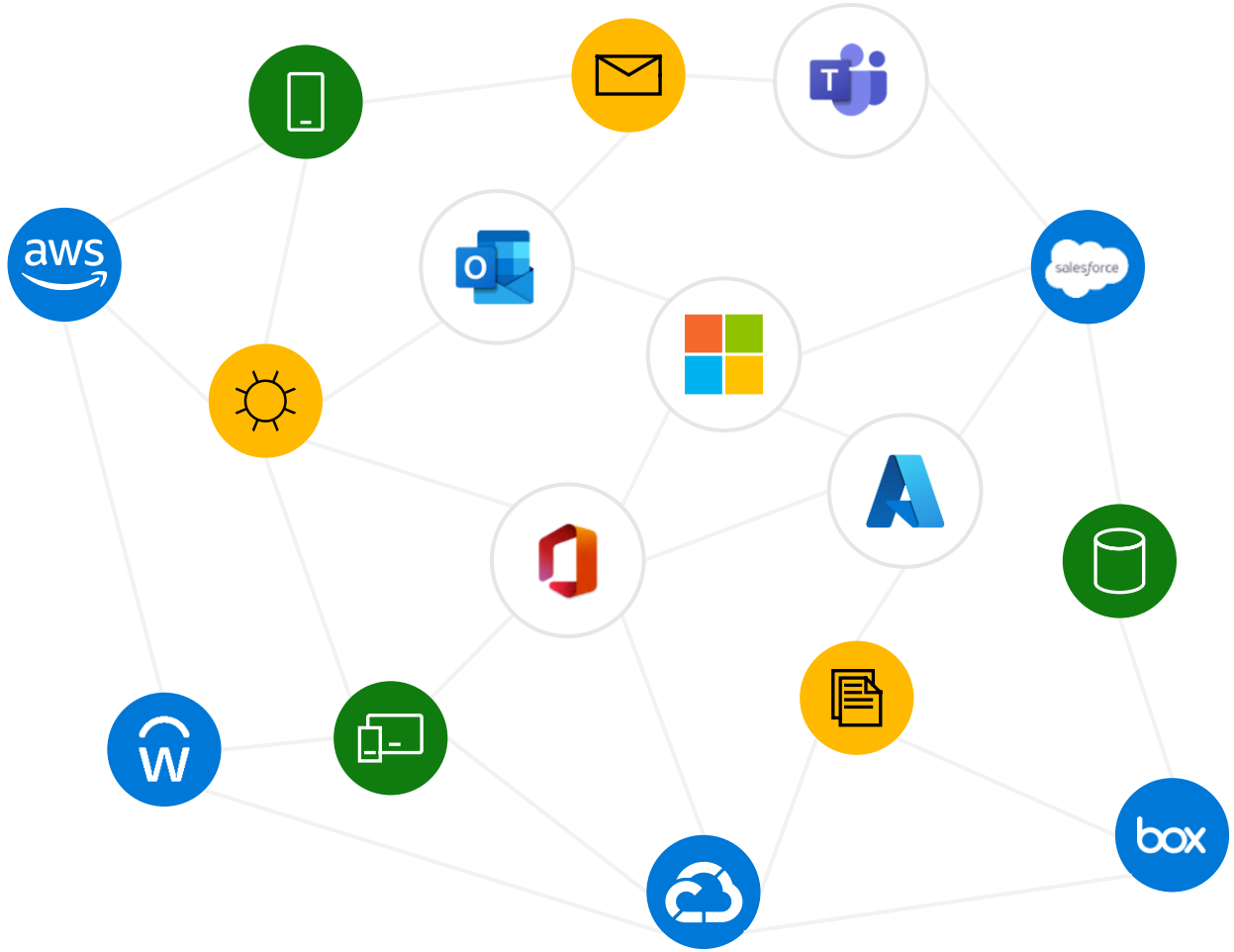
Automate routine tasks

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

Empower employees and guests to be productive quickly

Rapidly onboard new users using a cloud-native, extensible, and a cost-effective Azure AD service

- Modernize your on-premise lifecycle solutions by migrating to cloud without impacting existing app integrations
- Shorten time to value by consolidating software vendors and using Azure AD for all lifecycle management needs
- Quickly provision access changes for pre-hires, emergency hire and front-line hires by using pre-built workflows



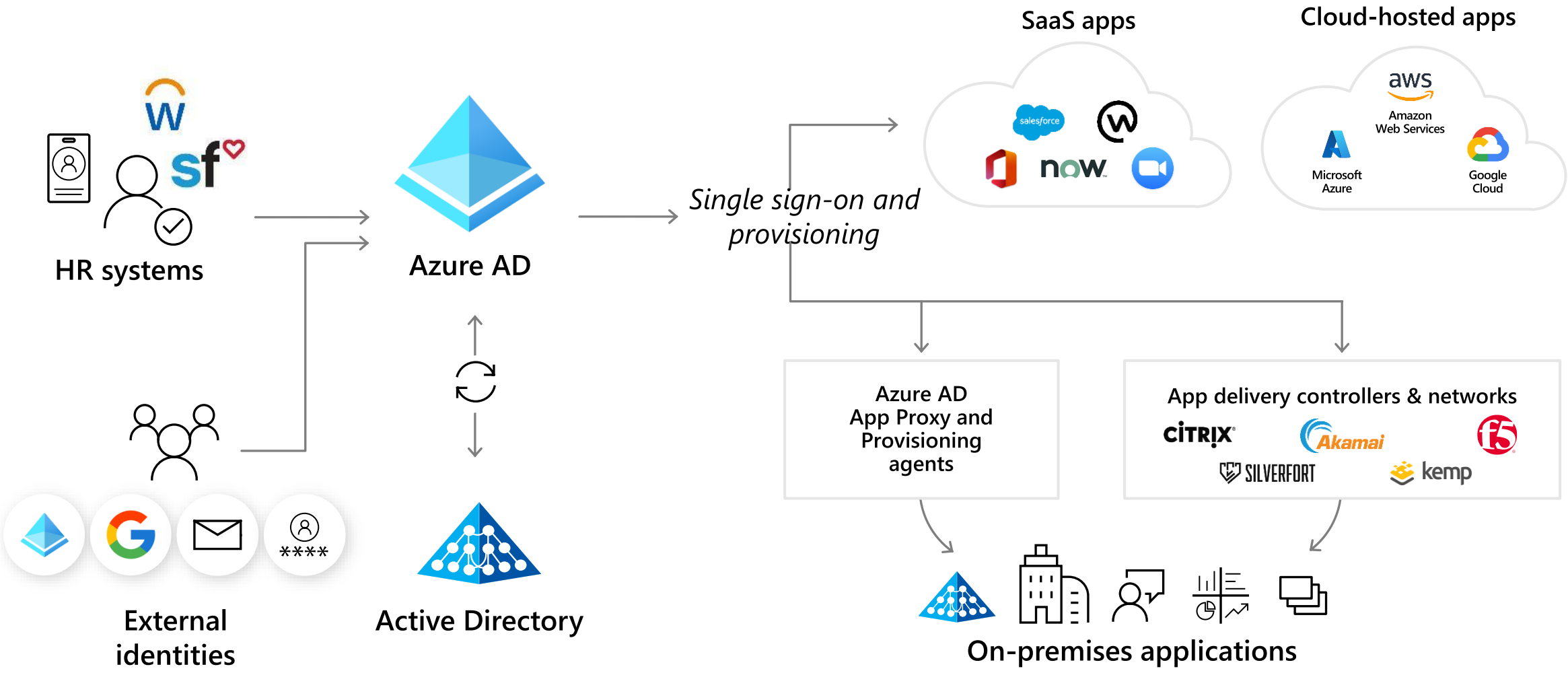
Strengthen security posture while maintaining productivity

Securely provision sensitive data access to employees and guests at scale

- Put control in the hands of business managers who are best suited to provide sensitive data access to guests
- Securely provide access to employees and guests by periodically reviewing, extending, or revoking access rights
- Reduce risk of unauthorized access by periodically reviewing and cleaning up access to sensitive resources

Connect your workforce to any app

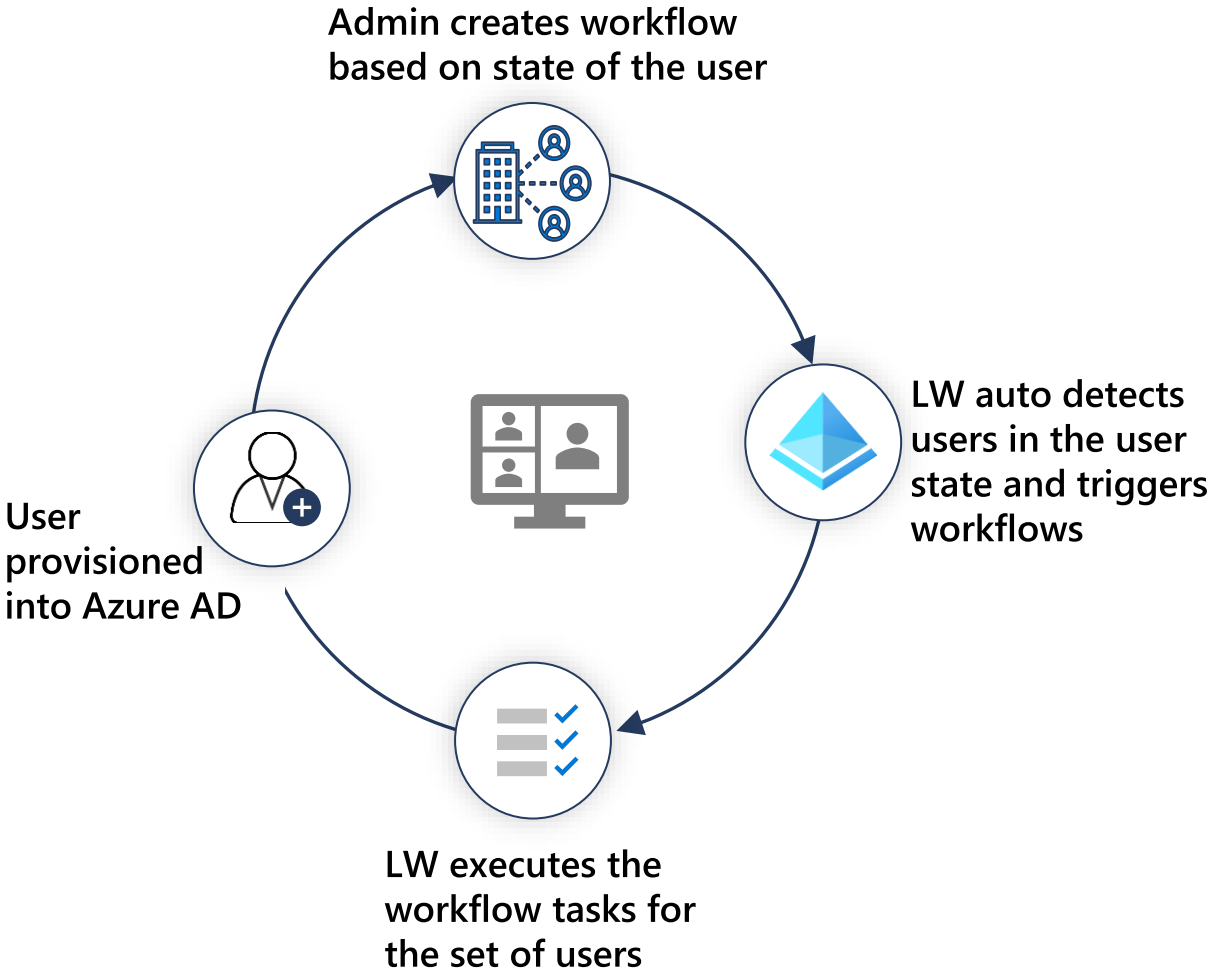
Single sign-on and outbound provisioning



Lifecycle Workflows

Manage users by automating Joiner/Mover*/Leaver processes

- Pre-defined workflow templates for most common user tasks.
- Automatic trigger based on attribute state changes of user.
- Custom policies for triggering workflows based on pre-defined or custom user states.
- Extensibility and flexibility with Logic Apps.



* To be supported in future

Microsoft Entra

Secure access for a connected world.

Azure
Active Directory

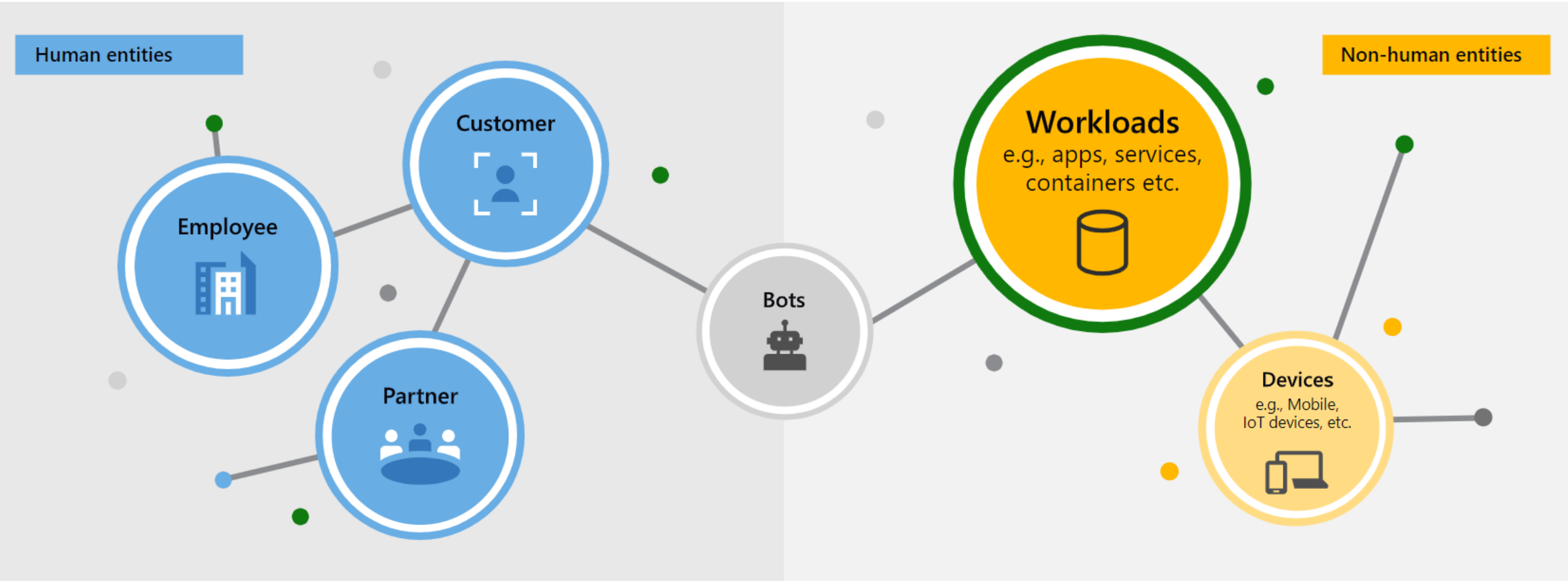
Microsoft Entra
Permissions Management

Microsoft Entra
Verified ID

Microsoft Entra
Identity Governance

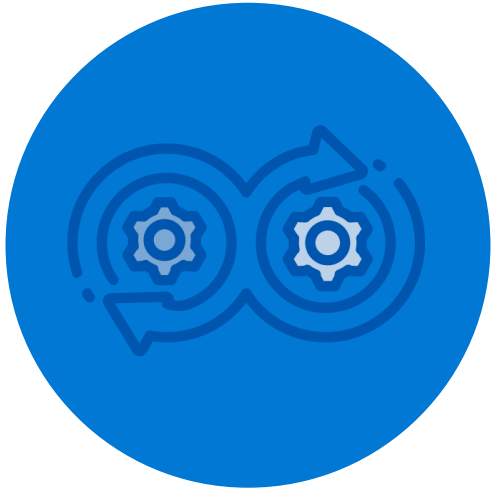
Microsoft Entra
Workload Identities

What are workload identities?



Challenges of managing and securing workload identities

Many traditional IAM capabilities do not apply to workload identities



Difficult to manage workload identity lifecycle:

How to get insights into the activity of workload identities

Higher potential for secrets or credentials to leak:

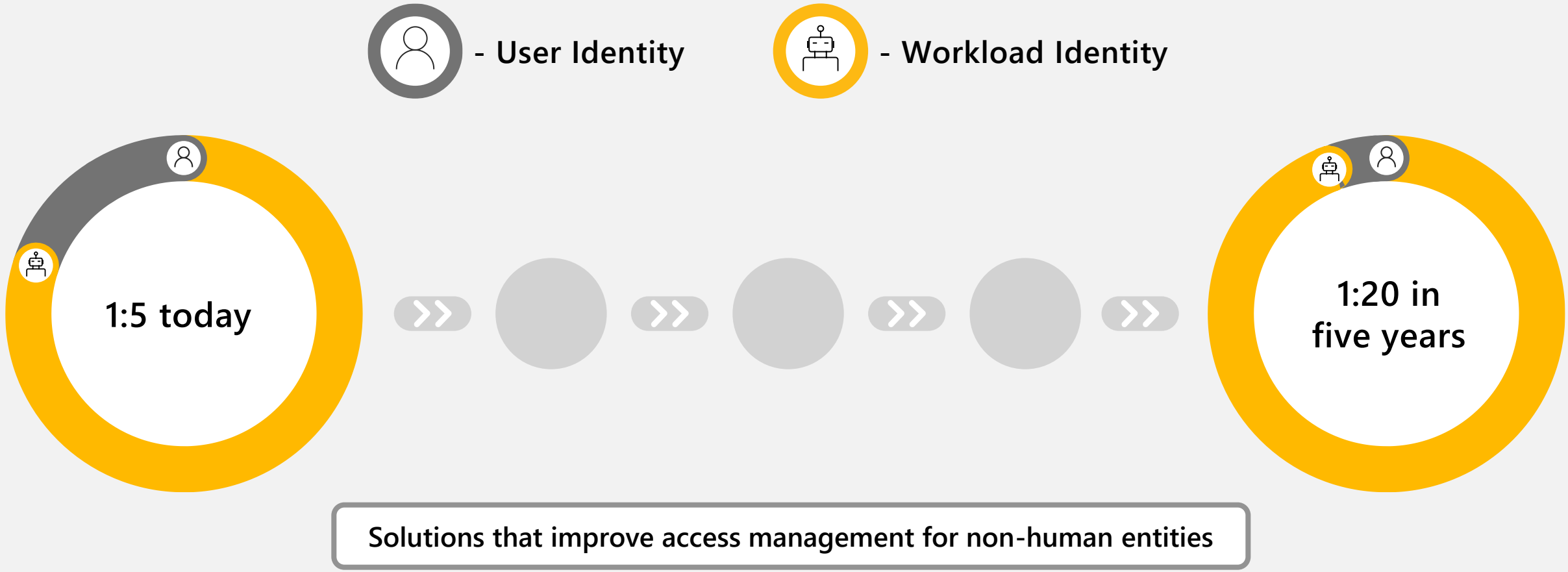
How to ensure that workload identities are not breached

Lacking capabilities for securing access:

How to remove unnecessary or overprivileged access

Key investment areas for identity portfolio expansion

Ratio of user identities vs. workload identities



Sources: Internal Microsoft marketing research 2021, CloudKnox 2021

Workload Identities

An identity and access management (IAM) solution that manages and secures access by applications and services.

Secure access with adaptive access policies

Secure adaptive access by enforcing granular access control for apps and services

Detect compromised workload identities

Intelligently detect and respond to compromised workload apps and services.

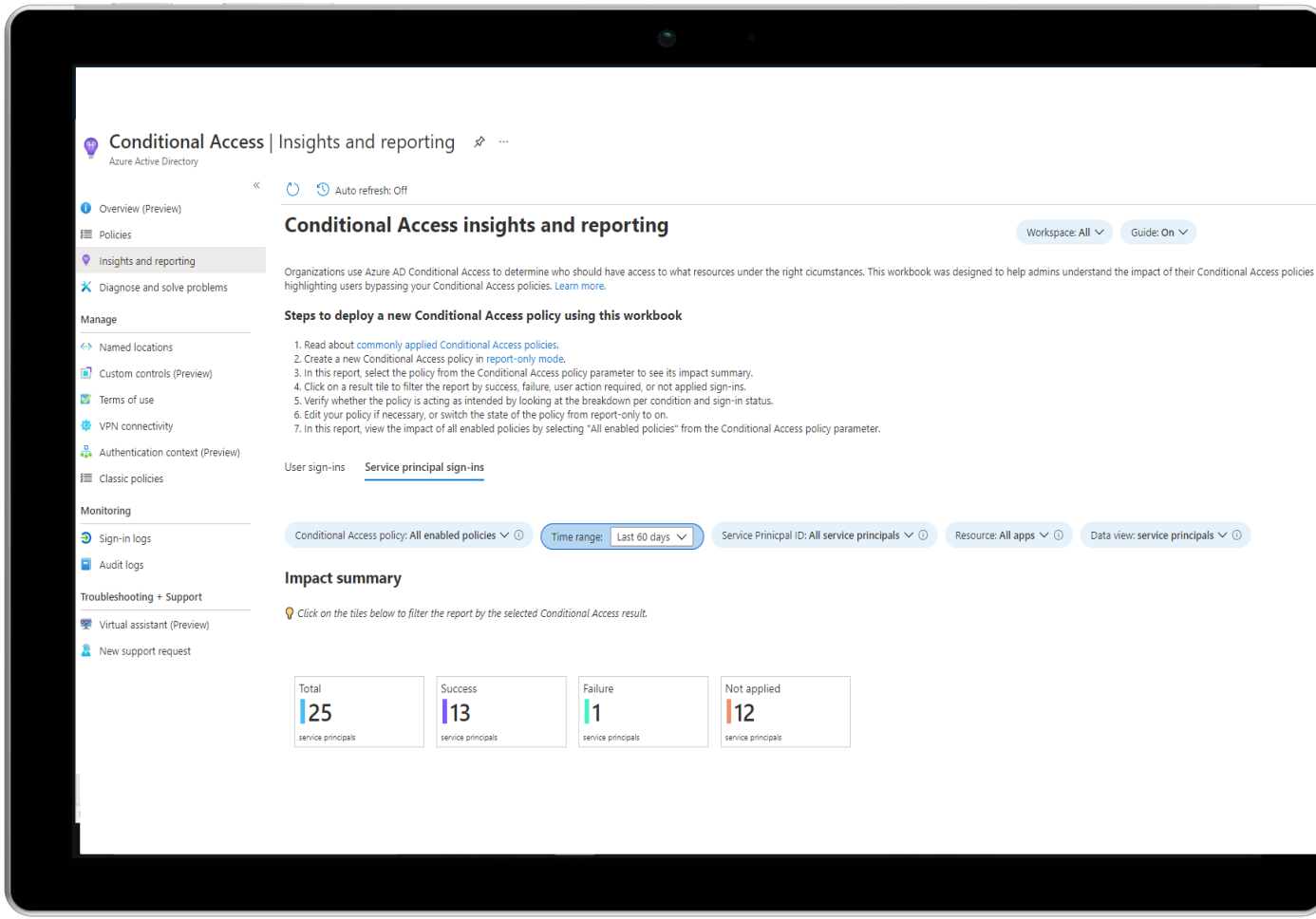
Simplify lifecycle management

Simplify lifecycle management of apps and services with insights.

Conditional Access for workload identities

Protect access to resources by enforcing access control

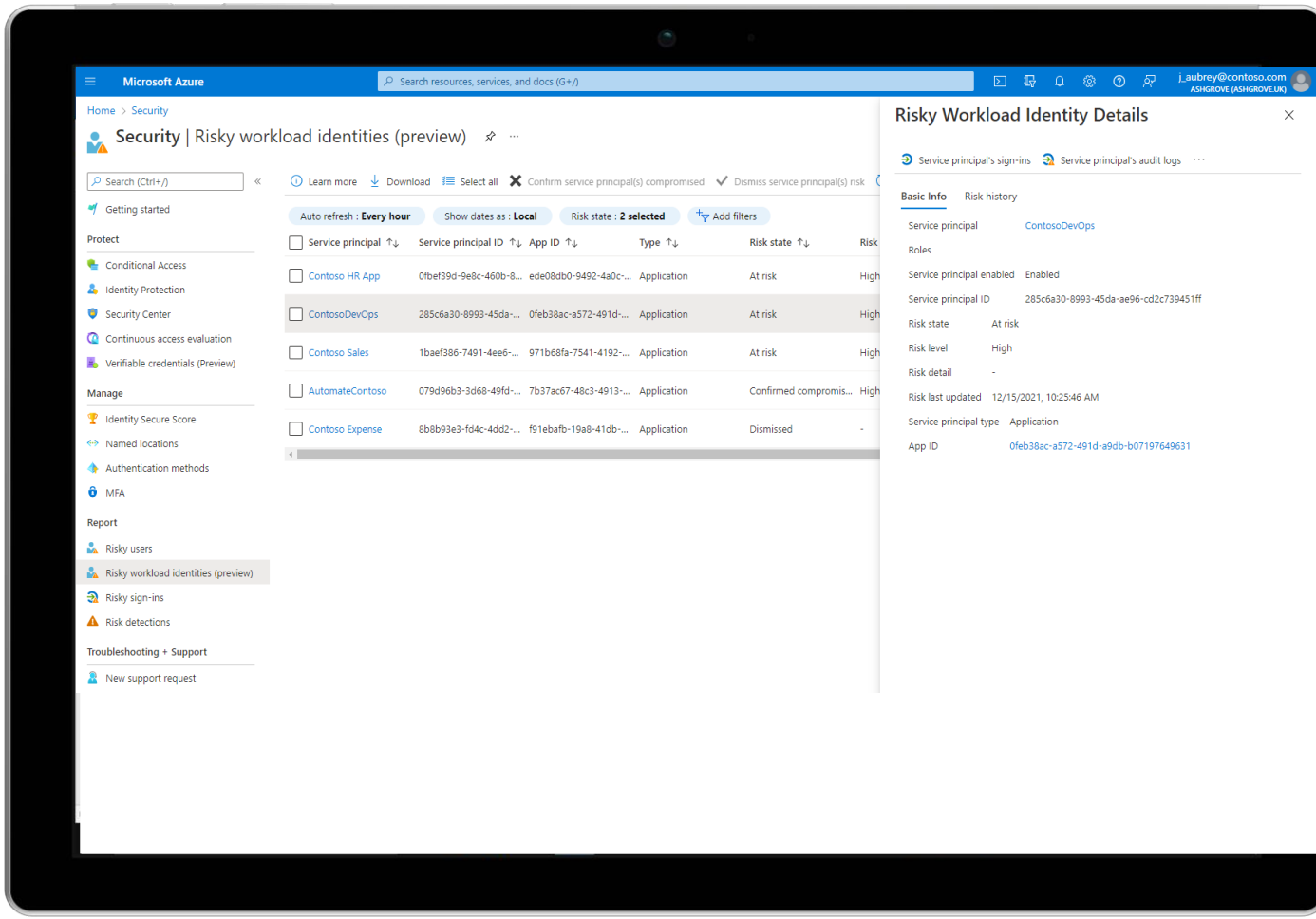
- **Support for Conditional Access** policies applied to workload identities.
- **Define the conditions** under which a workload may access a resource.
- **Enables blocking** workload identities from outside of trusted IP ranges, such as a corporate network public IP ranges.



Identity protection for workload identities

Detect compromised workload identities and block access

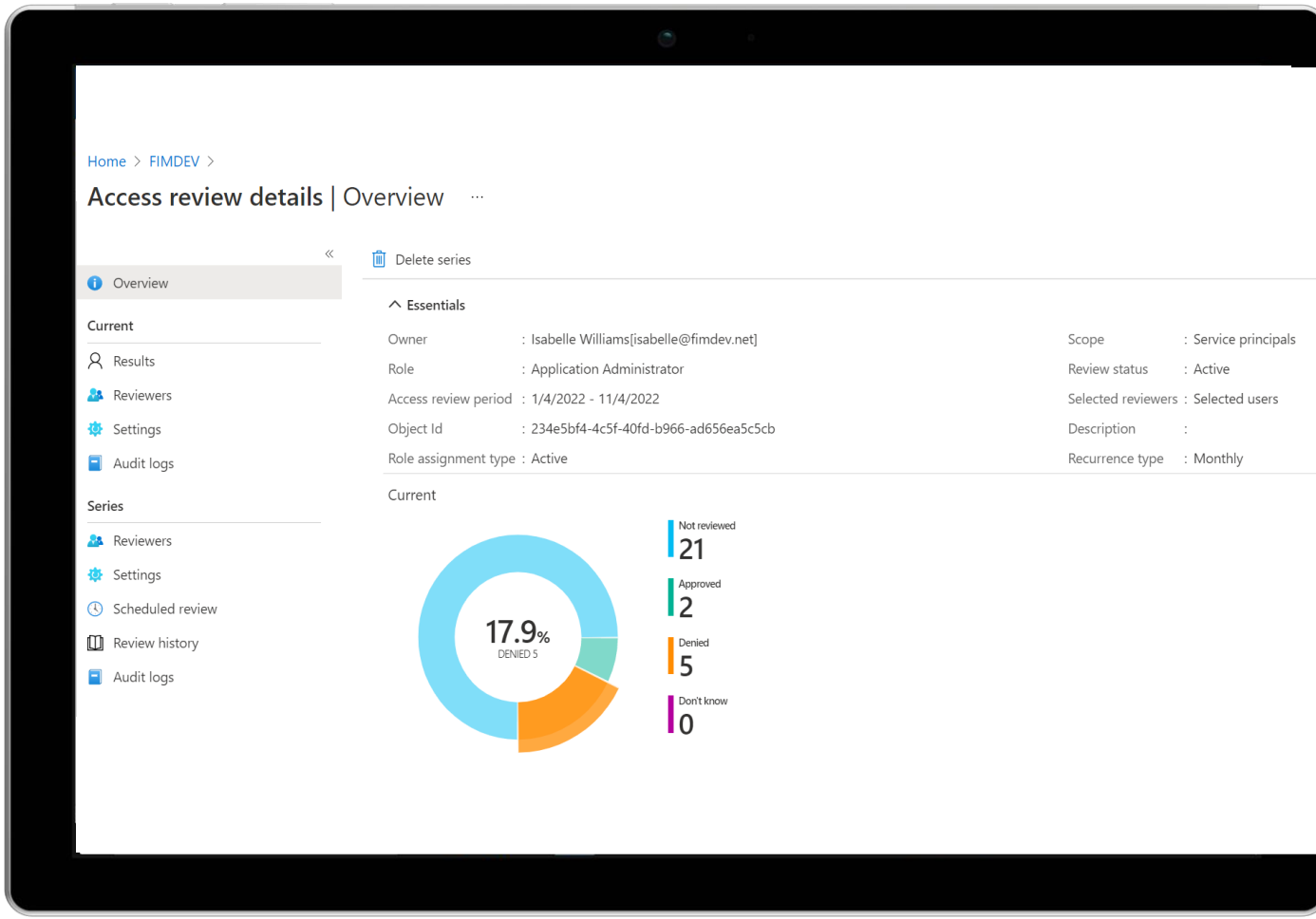
- Support identity protection capabilities, such as detecting, investigating and remediating, to workload identities.
- Detect risk on workload identities across sign-in behavior and offline indicators of compromise.
- Enable applying risk-based conditional access to workload identities.



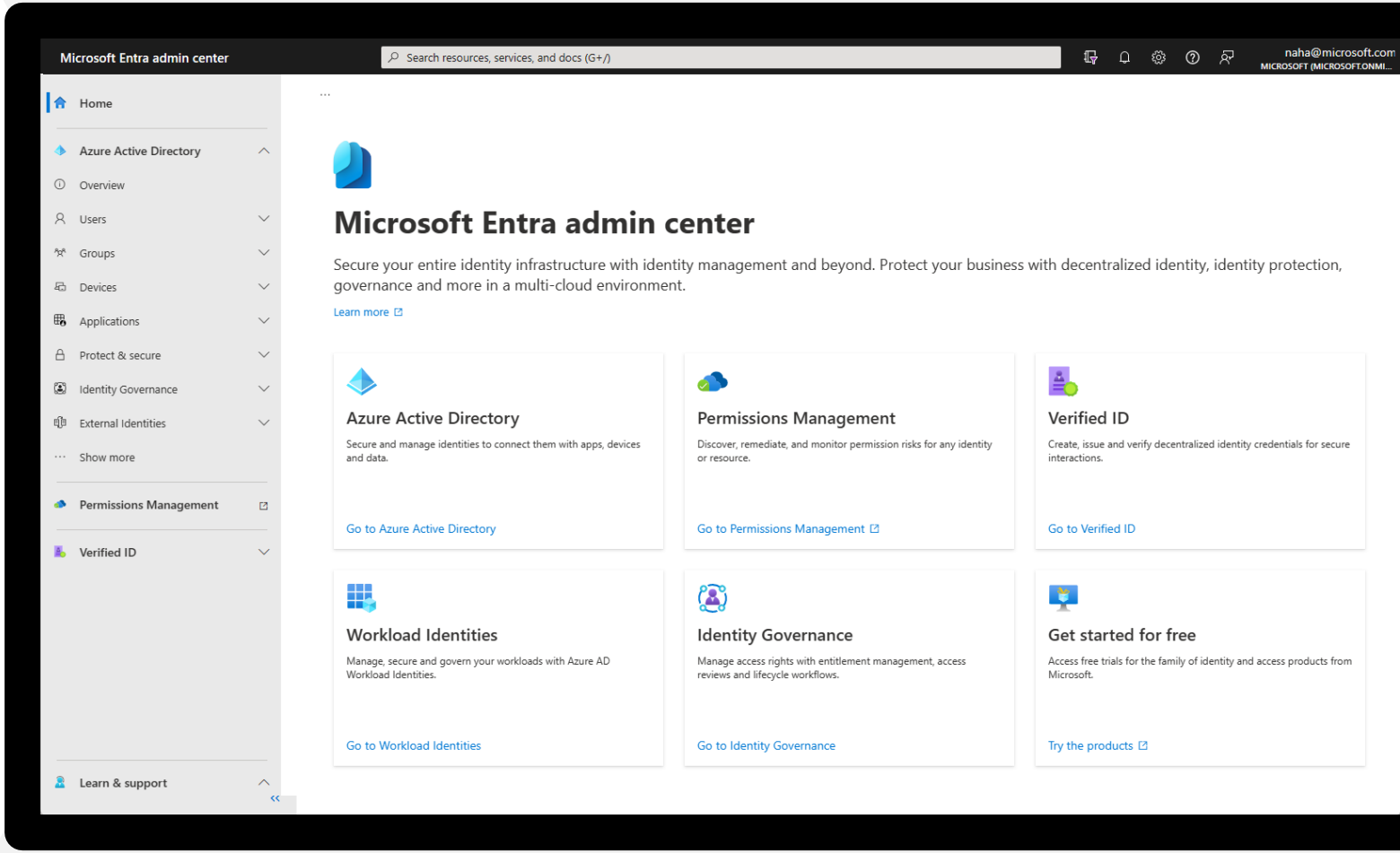
Access reviews for workload identities

Workload identities assigned to privileged roles

- Reduce the risk associated with stale role assignment by configuring recurring reviews of workload identities
- Delegate the reviews to the right people, then automatically revoke access of the denied workload identities.



All in one place:
Microsoft Entra admin center



Microsoft Entra

Secure access for a connected world.

Azure
Active Directory

Microsoft Entra
Permissions Management

Microsoft Entra
Verified ID

Microsoft Entra
Identity Governance

Microsoft Entra
Workload Identities

Microsoft Security

Thank you.