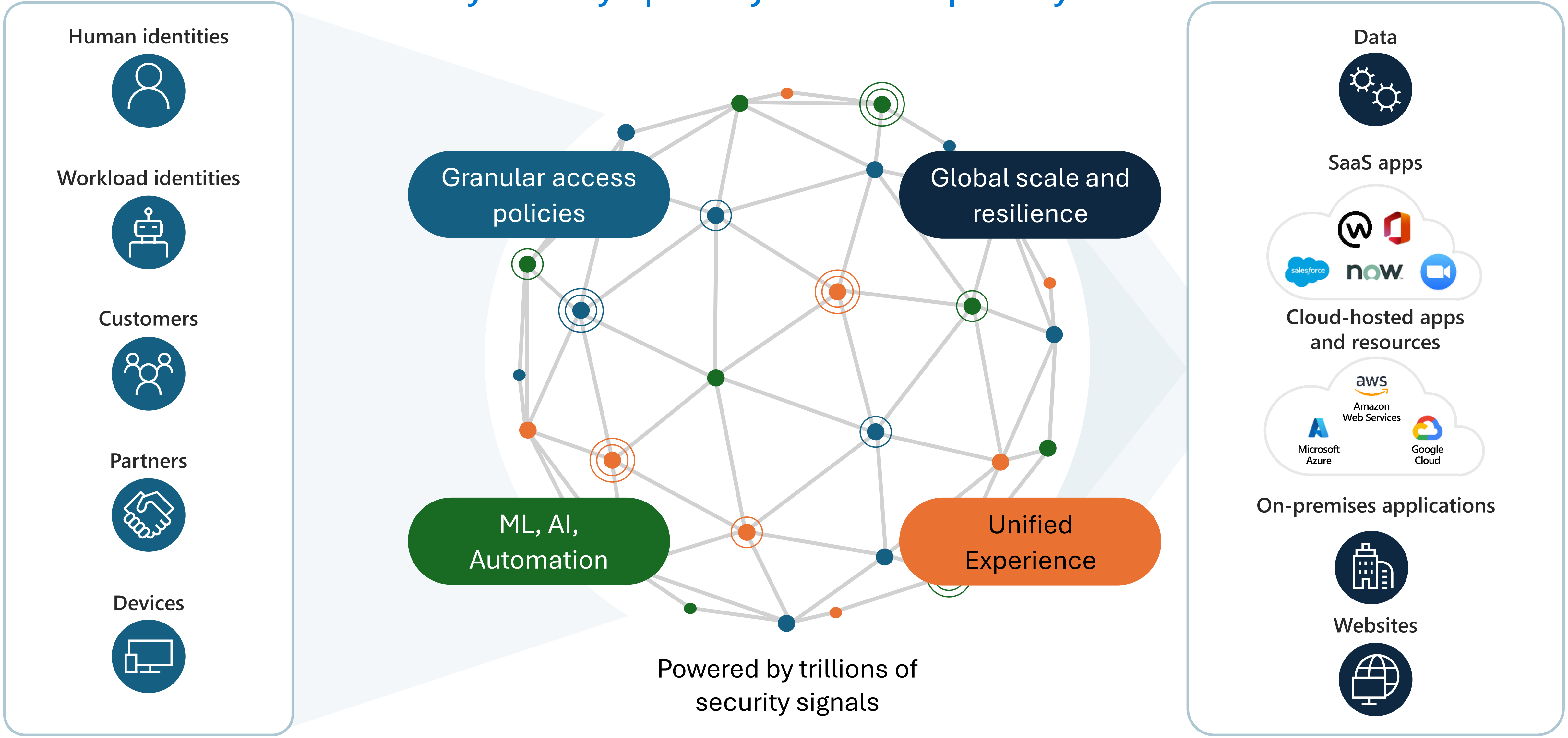
Microsoft Security

Entra ID Governance technical training for services partners

Microsoft NDA Confidential

Microsoft Entra: Secure access for a connected world

Every Identity | Every Resource | Everywhere



Human identities

Workload identities

Customers

Partners

Devices

Granular access policies

Global scale and resilience

ML, AI, Automation

Unified Experience

Powered by trillions of security signals

Data

SaaS apps

Cloud-hosted apps and resources

On-premises applications

Websites

Azure AD is becoming Microsoft Entra ID.

New name. Same capabilities. Same licensing.

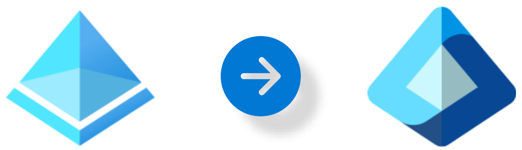
No customer action is needed.

Azure AD is becoming
Microsoft Entra ID.

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

Detailed naming guidance available on Microsoft Learn

Azure Active Directory	→	**Microsoft Entra ID**



Azure AD Conditional Access	→	**Microsoft Entra Conditional Access**
Azure AD accounts	→	**Microsoft Entra accounts**
Azure AD joined	→	**Microsoft Entra joined**
Azure AD tenant	→	**Microsoft Entra tenant**

Microsoft Entra Product Family

Identity & access management

- Microsoft Entra ID
  Formerly Azure AD
- Microsoft Entra ID Governance
- Microsoft Entra External ID
  Formerly Azure AD External Identities

New Identity categories

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

Network Access

- Microsoft Entra Internet Access
- Microsoft Entra Private Access

Agenda

- Overview of Microsoft Entra ID Governance SKU
- Scenario deep dive
  - Employee Lifecycle
  - Govern Access to Resources
  - Govern External Identities

Microsoft Entra ID Governance

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

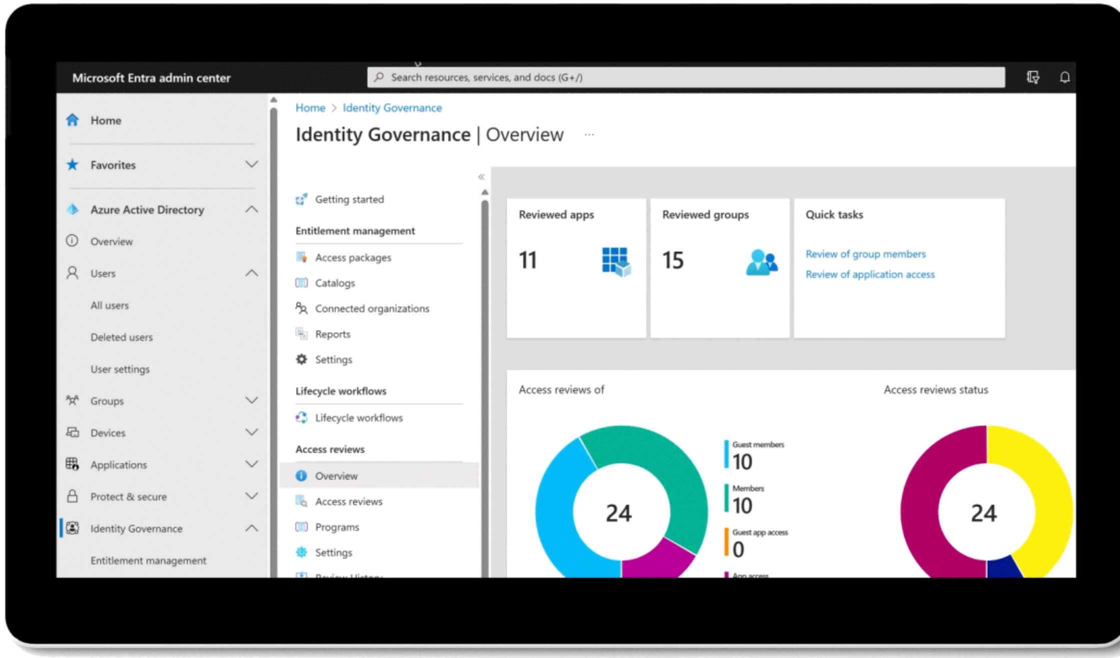
Market Challenge

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

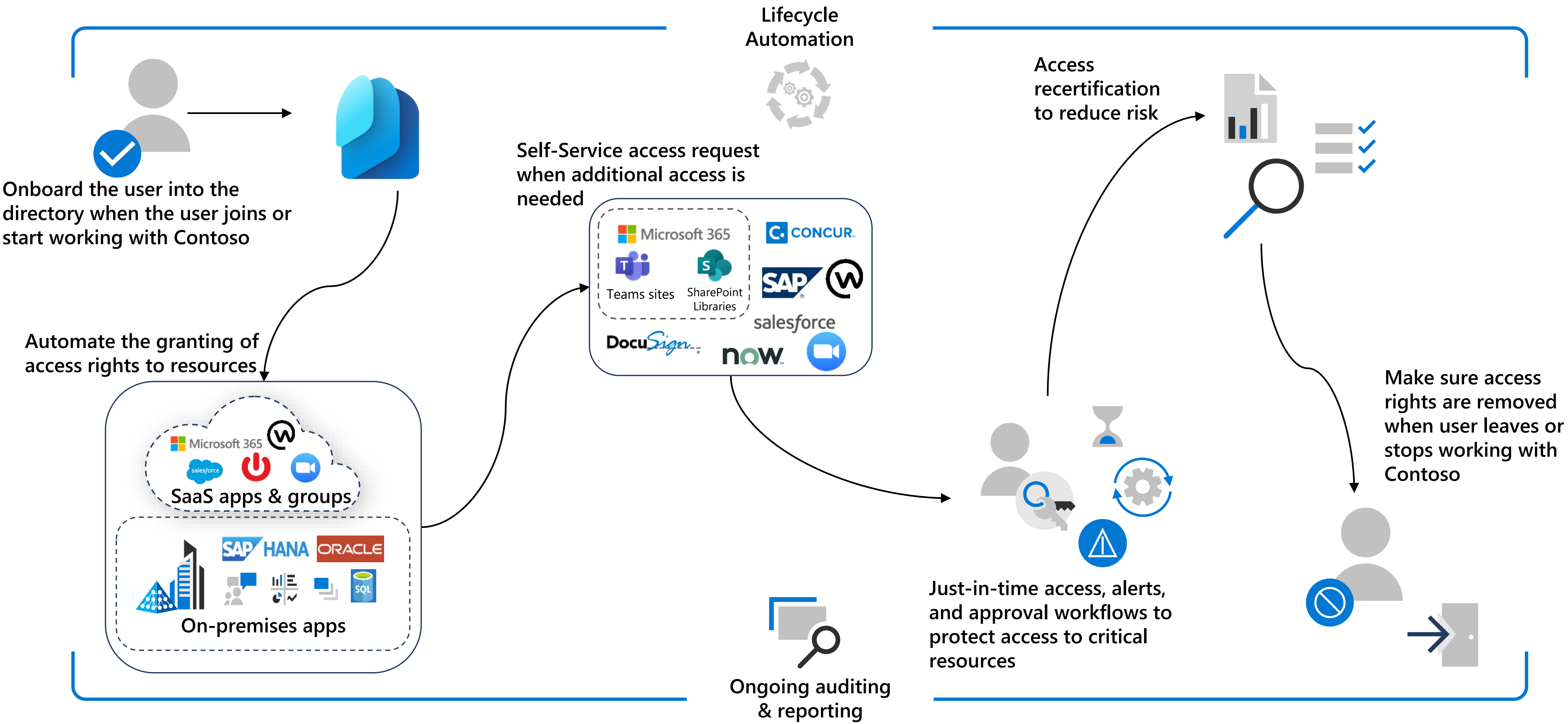
Improve Productivity

Strengthen Security

Automate routine tasks



Contoso's user journey



Lifecycle Automation

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

Automate the granting of access rights to resources

Self-Service access request when additional access is needed

Access recertification to reduce risk

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

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

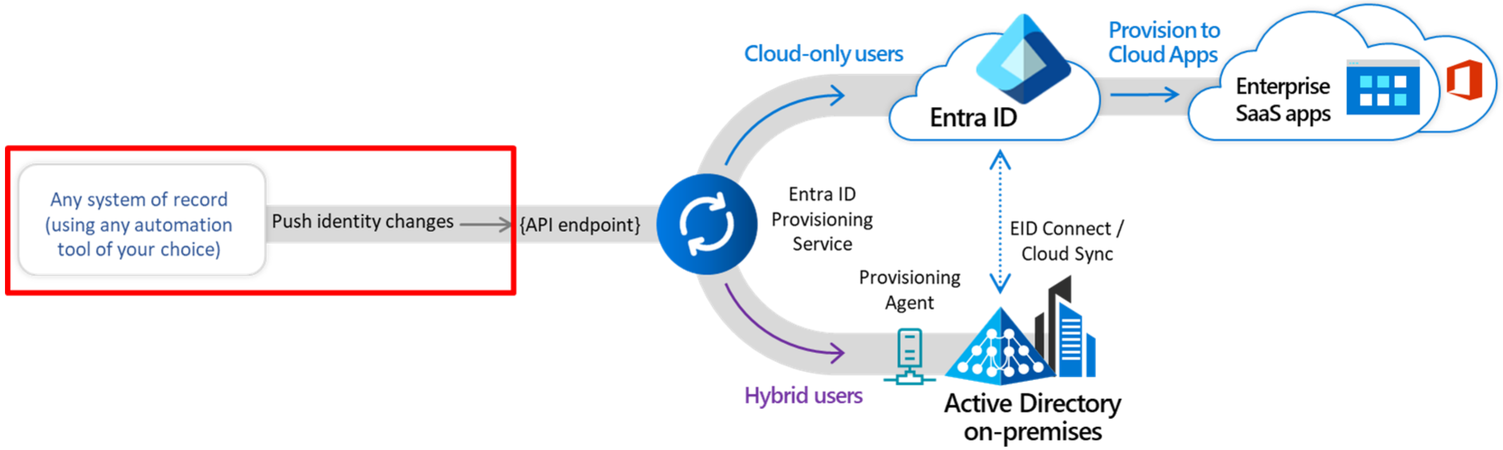
Ongoing auditing & reporting

Generic Inbound Provisioning API

PUBLIC PREVIEW

Key benefits

- Connect Entra ID tenant to *any* authoritative system of record for inbound identity provisioning.
- This system of record could be an HR app like UltiPro, a payroll app like ADP, a spreadsheet in Google Cloud or an on-premises Oracle database.
- Decouples HR data export from how data is cleansed before import into Entra ID.
- IT admins retain control on identity data flow, transformations and mapping.



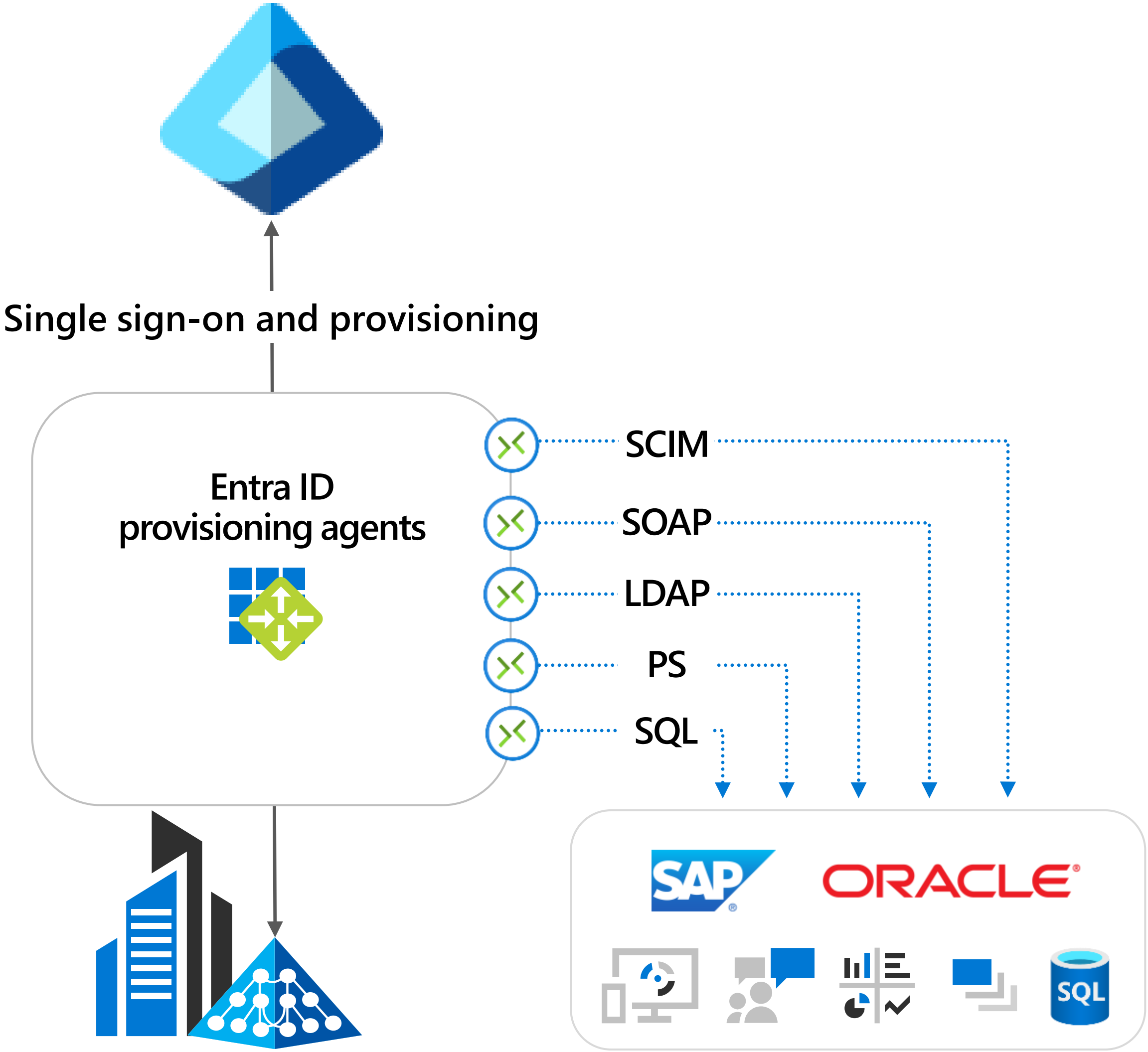
Provisioning to on-premises applications

Users and schema defined in the cloud

- Supports provisioning from custom schema extensions to app-specific properties.

Translation to the provisioning protocols expected by apps

- Microsoft-delivered connectors: LDAP, SQL, etc.
- Ecosystem of third-party connectors for other apps requiring custom API integrations
- Customers can re-use their existing MIM configuration



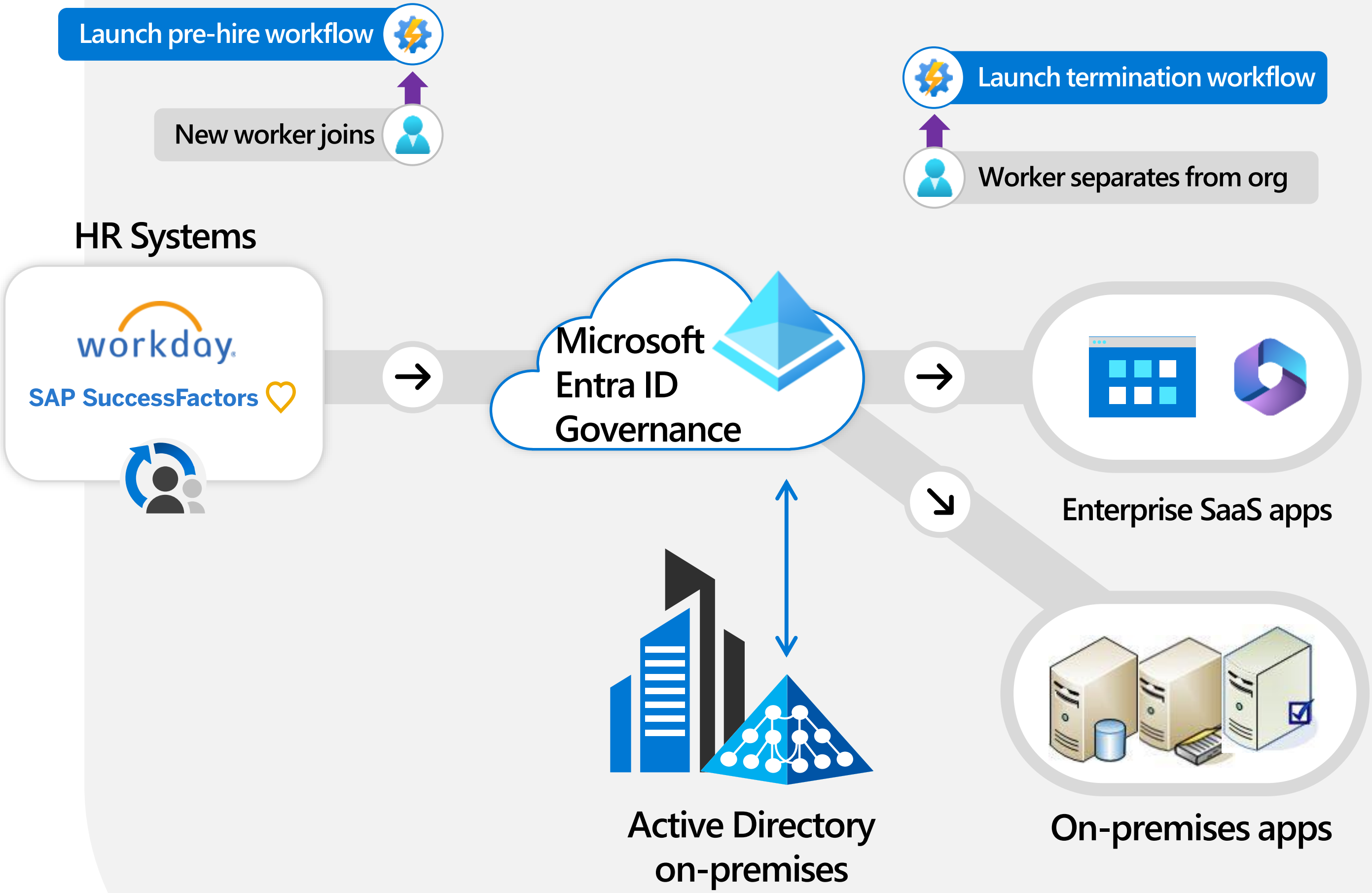
Single sign-on and provisioning

Entra ID provisioning agents

Lifecycle Workflows

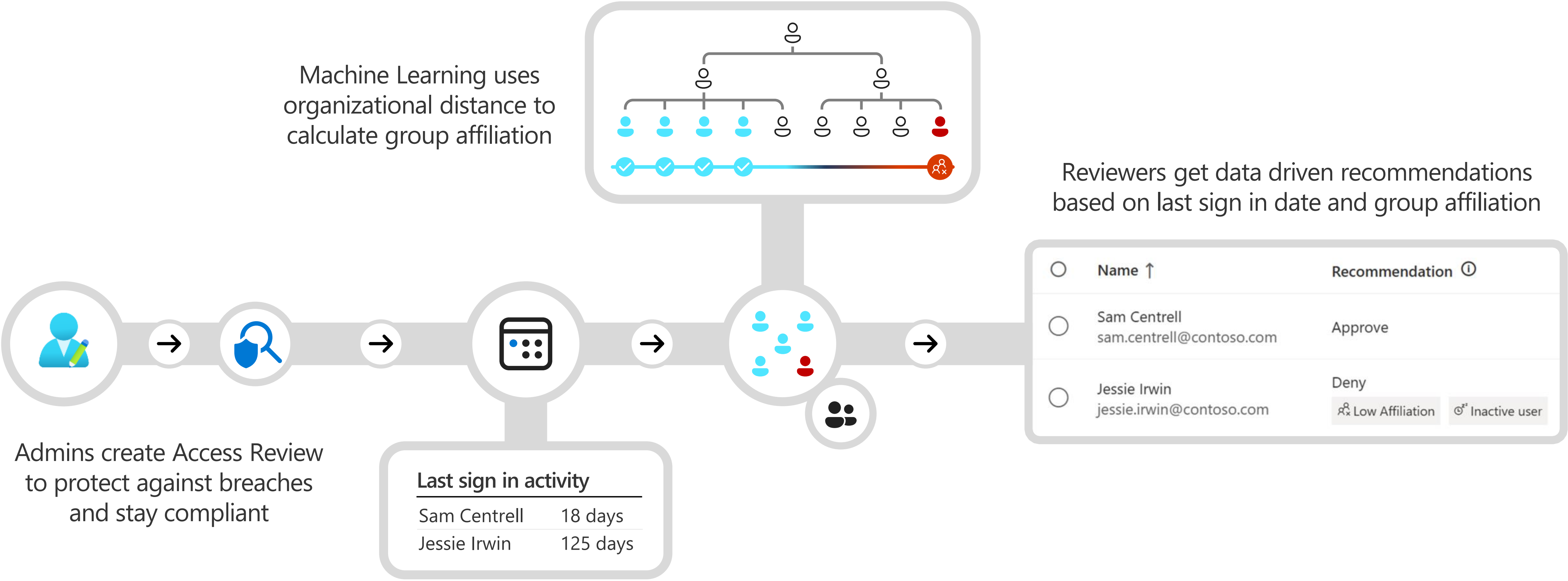
Automate join/move/leave employee lifecycle events

- Customers can schedule tasks to occur before, at or after a join or leave date.
- Built-in tasks include generating temporary credentials, sending emails, updating user attributes, and memberships, and removing licenses.
- Customers and partners can extend lifecycle workflows with additional tasks via Azure Logic Apps.



Machine Learning based recommendations in Access Reviews

User-to-Group Affiliation



Machine Learning uses organizational distance to calculate group affiliation

Reviewers get data driven recommendations based on last sign in date and group affiliation

○	Name ↑	Recommendation ⓘ
○	Sam Centrell sam.centrell@contoso.com	Approve
○	Jessie Irwin jessie.irwin@contoso.com	Deny Low Affiliation Inactive user

Admins create Access Review to protect against breaches and stay compliant

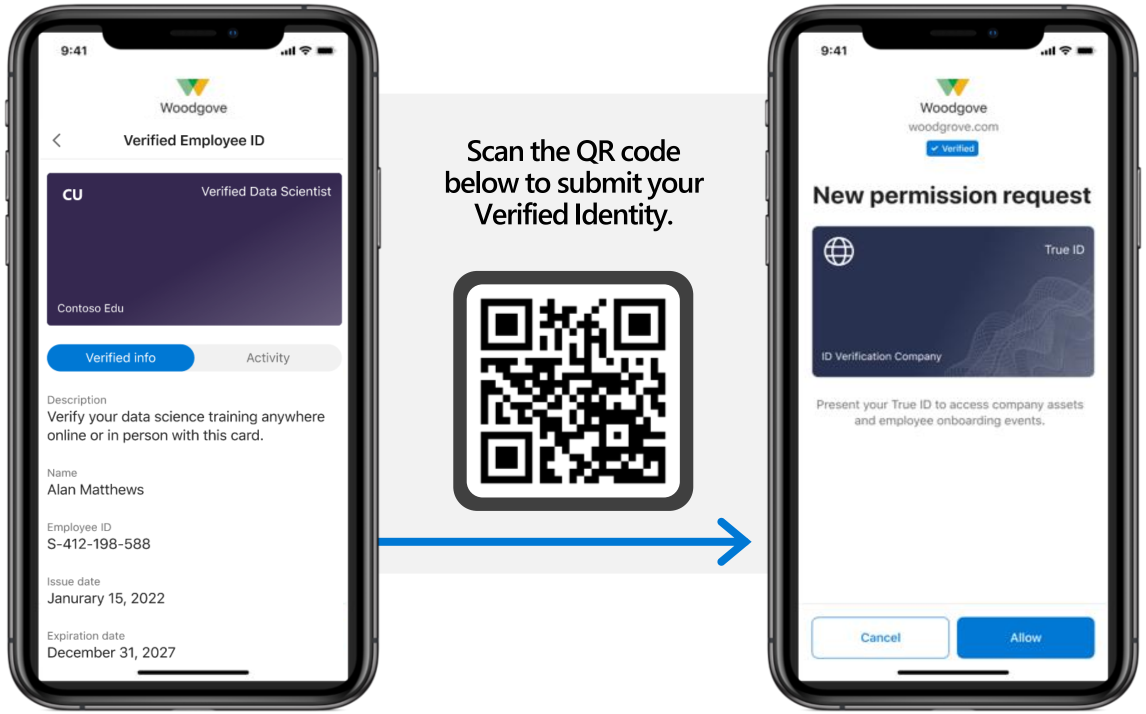
Last sign in activity	
Sam Centrell	18 days
Jessie Irwin	125 days

Inactive user recommendation considers activity based on last sign in date

Access requests for users with decentralized IDs

Entitlement Management with verifiable credentials

- Reduces need for self-attestation by business partners. Users requesting access will be able to obtain identity attributes from a wide set of issuers.
- Simplifies approval processes, as approvers do not need to vet requestor's authenticity of claims.
- Simplifies compliance posture with reduced need for manual validation.
- Example of better together Microsoft Entra combinations; others include ID Governance + Workload IDs, ID Governance + External IDs



9:41

Woodgove

Verified Employee ID

CU

Verified Data Scientist

Contoso Edu

Description
Verify your data science training anywhere online or in person with this card.

Name
Alan Matthews

Employee ID
S-412-198-588

Issue date
Janurary 15, 2022

Expiration date
December 31, 2027

Scan the QR code below to submit your Verified Identity.

9:41

Woodgove
woodgrove.com
✓ Verified

New permission request

True ID

ID Verification Company

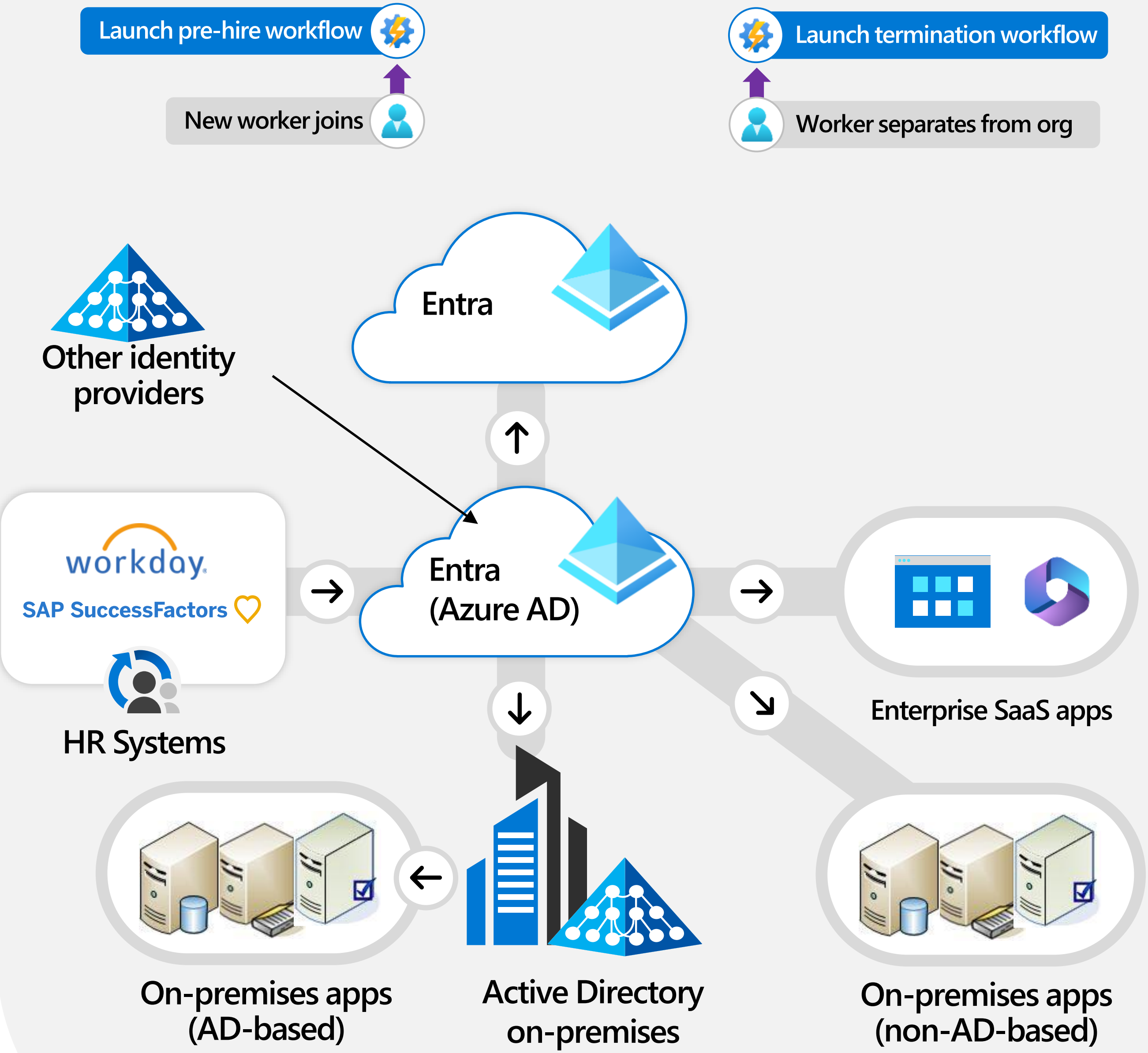
Present your True ID to access company assets and employee onboarding events.

Integrations with SAP

Automate join/move/leave employee lifecycle and on-demand time-limited access for all users

- Microsoft Entra ID Governance leverages SuccessFactors
  - Provisions and updates AD, Azure AD and app identities for new hires, profile updates, terminations, rehires
  - Lifecycle workflows can trigger additional automation

- Microsoft Entra ID Governance assigns birthright roles and on-request time-limited access across SAP applications:
  - S/4HANA public cloud, private cloud and on-premises
  - SAP R/3 ECC
  - Concur and other SaaS

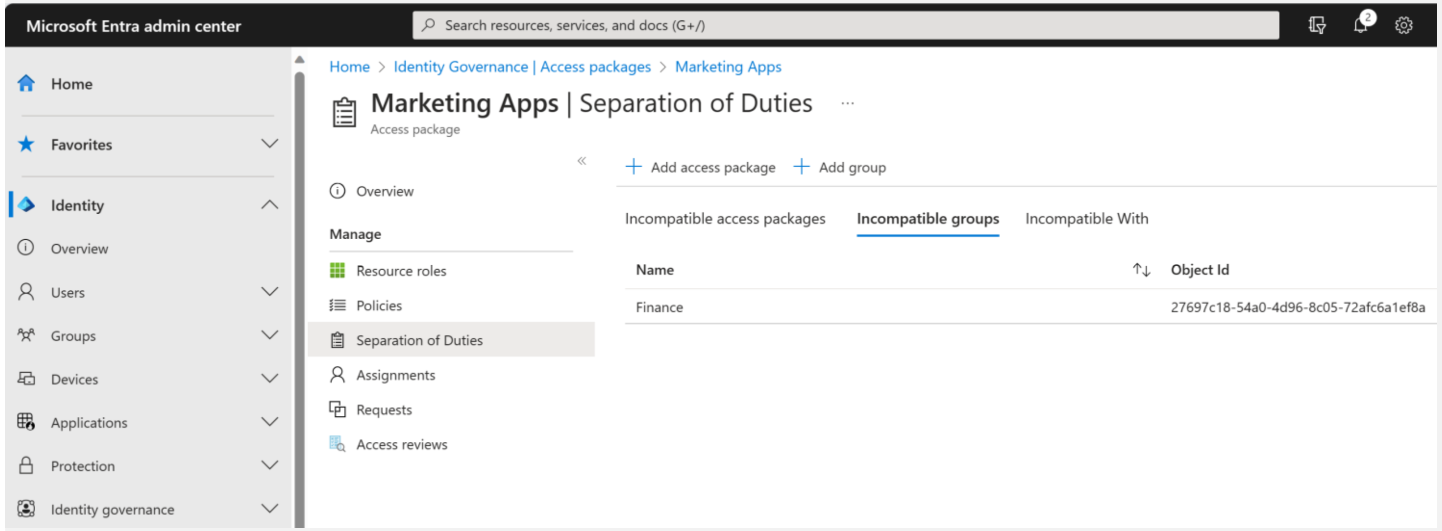


GRC checks and integrations

Built-in reports and separation of duties (SoD) checks

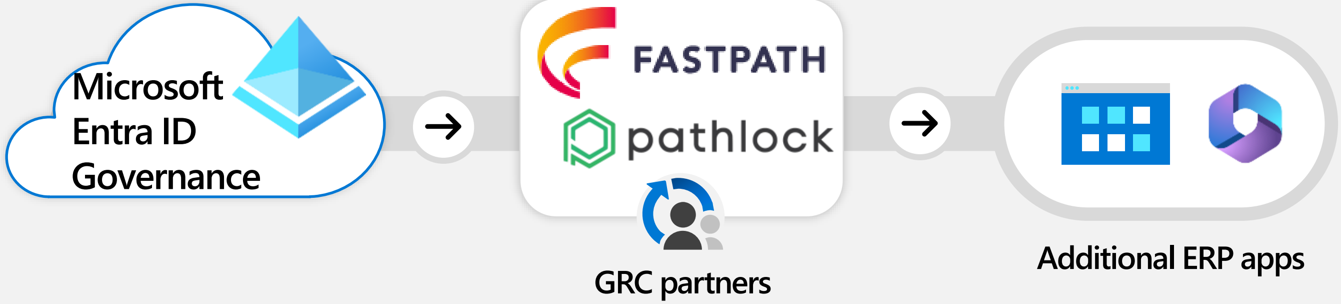
- Provides reports and alerts on users who have incompatible access rights across entitlement management and groups
- Restricts users from requesting an access package if it is incompatible with the user's existing access

GRC partners FastPath and Pathlock integrate with Microsoft Entra ID Governance to extend support for finer-grained separation of duties checks in additional business apps.



Marketing Apps | Separation of Duties

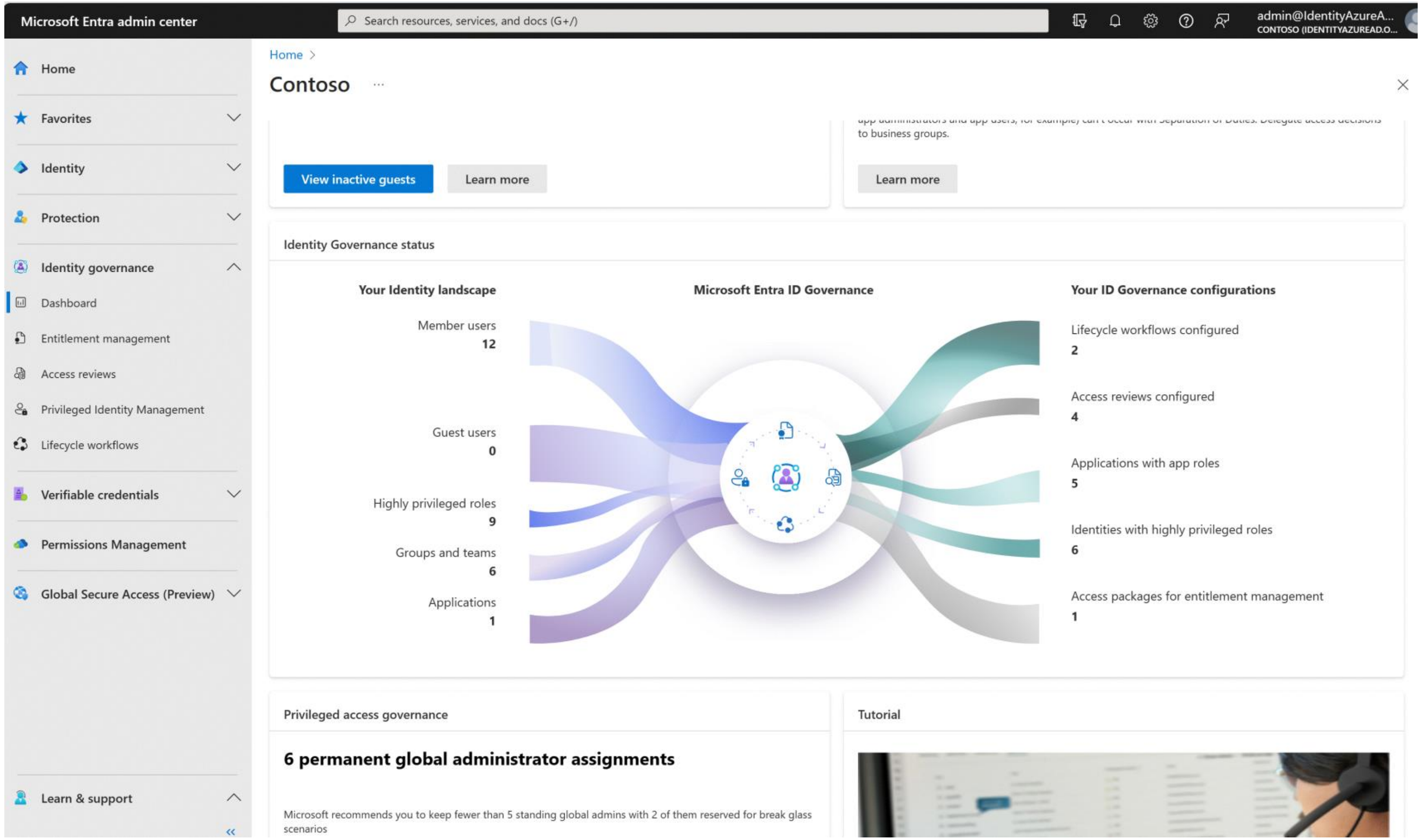
Name	Object Id
Finance	27697c18-54a0-4d96-8c05-72afc6a1ef8a



Actionable dashboard

Visual report of identity governance posture, with recommended actions

- Understand the current environment
- Quick links to graphical reporting
- ML-based recommendations
- Additional information at your fingertips



app administrators and app users, for example) can't occur with Separation of Duties. Delegate access decisions to business groups.

Identity Governance status

Your Identity landscape		Your ID Governance configurations	
Member users	12	Lifecycle workflows configured	2
Guest users	0	Access reviews configured	4
Highly privileged roles	9	Applications with app roles	5
Groups and teams	6	Identities with highly privileged roles	6
Applications	1	Access packages for entitlement management	1

Privileged access governance

6 permanent global administrator assignments

Microsoft recommends you to keep fewer than 5 standing global admins with 2 of them reserved for break glass scenarios

Tutorial

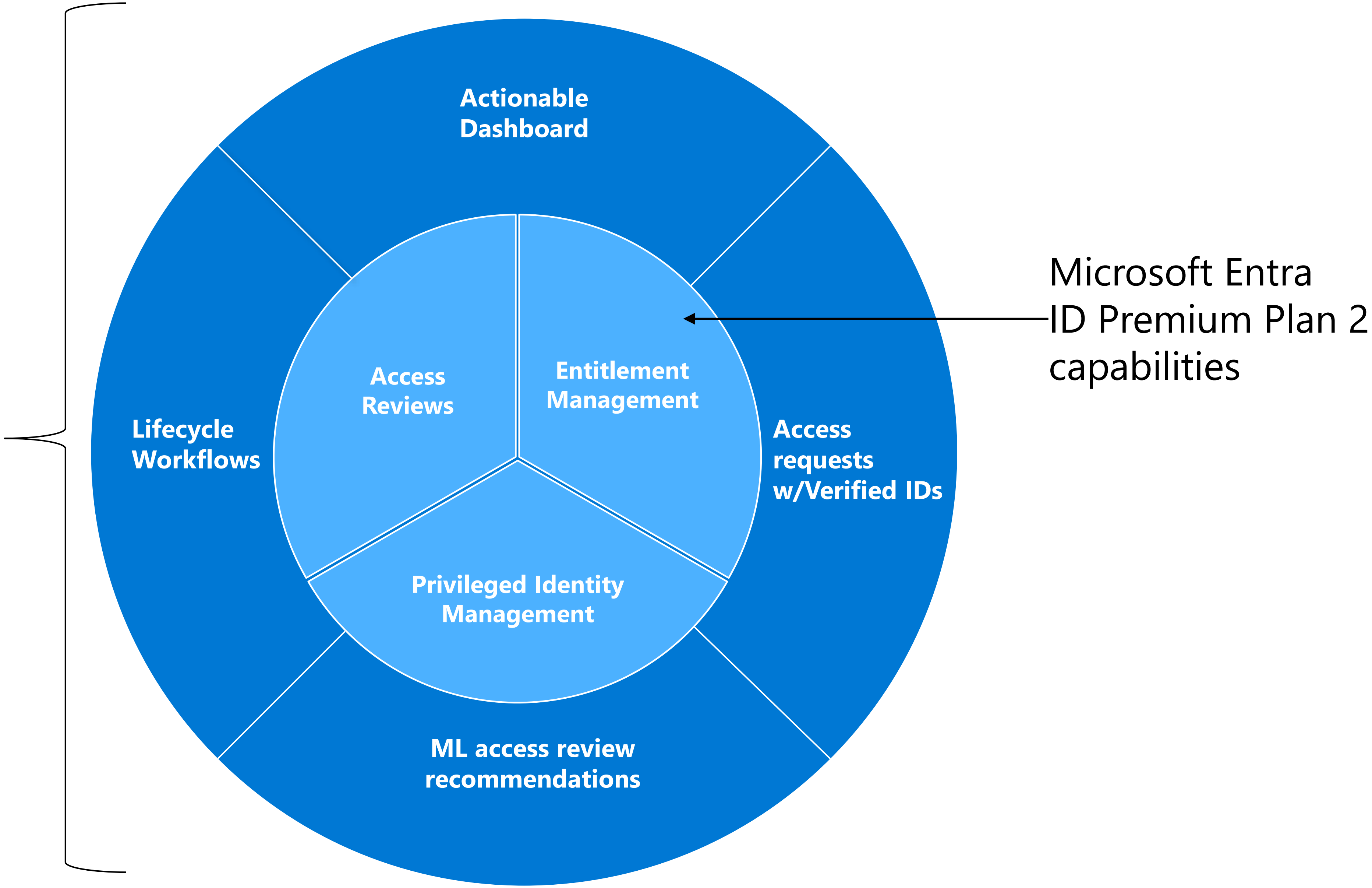
Feature to new sku mapping

New sku features that extend Access Reviews and Entitlement management

- User-to-group affiliation
- Inactive users
- Access Reviews of PIM for Groups (Public Preview)
- EM + Custom extensions
- EM + Verified IDs
- EM - Auto Assignment policies
- EM - Invite + Assign Any
- EM - Sponsors Policy

Microsoft Entra ID Governance

A premium identity governance product, built on the Microsoft Entra ID framework


Actionable Dashboard
Access Reviews
Entitlement Management
Lifecycle Workflows
Access requests w/Verified IDs
Privileged Identity Management
ML access review recommendations
Microsoft Entra ID Premium Plan 2 capabilities

Microsoft Entra ID Governance capabilities

Identity Governance – feature comparison

	Microsoft Entra ID Free	Microsoft Entra ID Premium P1 (P1 standalone, M365 Biz Premium, M365 E3)	Microsoft Entra ID Premium P2 (P2 standalone, M365 E5)	Microsoft Entra ID Governance **$7.00 user/month (requires P1)** ~~$4.00~~ **$2.5 user/month (requires P2)**
– Identity Governance	✓	✓	✓	✓
Automated user provisioning to apps	✓	✓	✓	✓
Automated group provisioning to apps		✓	✓	✓
HR-driven provisioning		✓	✓	✓
Terms of use attestation		✓	✓	✓
Access certifications and reviews			✓	✓
Entitlement management			✓	✓
Privileged identity management (PIM), PIM for Groups			✓	✓
Lifecycle workflows				✓
AI-driven access reviews				✓
Actionable dashboard				✓
Entitlement management + Verified ID				✓

Microsoft Entra Identity Governance

Capability	Scenario	Feature
Identity lifecycle (employees)	Admins can enable user account provisioning from Workday or SuccessFactors cloud HR, or on-premises HR.	Cloud HR to Azure AD user provisioning
Identity lifecycle (guests)	Admins can enable self-service guest user onboarding from another Microsoft Entra tenant, direct federation, One Time Passcode (OTP) or Google accounts. Guest users are automatically provisioned and deprovisioned subject to lifecycle policies.	Entitlement management using B2B
Entitlement management	Resource owners can create access packages containing apps, Teams, Microsoft Entra, and Microsoft 365 groups, and SharePoint Online sites.	Entitlement management
Lifecycle Workflows	Admins can enable the automation of the lifecycle process based on user conditions.	Lifecycle Workflows
Access requests	End users can request group membership or application access. End users, including guests from other organizations, can request access to access packages.	Entitlement management
Workflow	Resource owners can define the approvers and escalation approvers for access requests and approvers for role activation requests.	Entitlement management and PIM
Policy and role management	Admin can define conditional access policies for run-time access to applications. Resource owners can define policies for user's access via access packages.	Conditional access and Entitlement management policies
Access certification	Admins can enable recurring access recertification for: SaaS apps, on-premises apps, cloud group memberships, Microsoft Entra, or Azure Resource role assignments. Automatically remove resource access, block guest access and delete guest accounts.	Access reviews, also surfaced in PIM
Fulfillment and provisioning	Automatic provisioning and deprovisioning into Microsoft Entra connected apps, including via SCIM, LDAP, SQL and into SharePoint Online sites.	User provisioning
Reporting and analytics	Admins can retrieve audit logs of recent user provisioning and sign on activity. Integration with Azure Monitor and 'who has access' via access packages.	Azure AD reports and monitoring
Privileged access	Just-in-time and scheduled access, alerting, approval workflows for Microsoft Entra roles (including custom roles) and Azure Resource roles.	Azure AD PIM
Auditing	Admins can be alerted of creation of admin accounts.	Azure AD PIM alerts

http://aka.ms/IdentityGovernanceOverview

Resources

- Microsoft Entra identity blog
  aka.ms/IdentityBlog
- Microsoft Entra product page
  aka.ms/entra/identitygovernance
- Microsoft Identity solution page
  microsoft.com/Identity
- Microsoft Entra technical documentation
  aka.ms/Entra/IDGovDocs
- Try Microsoft Entra ID Governance free
  aka.ms/EntraIDGovTrial
- Entra ID Governance Licensing Fundamentals
  https://aka.ms/EntraIG/LicDocs

Resources (Continued)

- Interactive Guides (https://aka.ms/EntraIDGovGuides). These are click-through demos that follow a single path through a scenario, with some popup callouts, that run in a browser. There are currently four scenarios, with two more in progress.

- CDX demo with ID Governance trial (https://cdx.transform.microsoft.com/ for demo pre-populated one year or 90-day M365 tenant; https://aka.ms/EntraIDGovTrial to enable ID Governance trial). Fully functional M365 enterprise tenant with content, and a 30-day trial of ID Governance.

- CDX demo with ID Governance demo (https://cdx.transform.microsoft.com/ for demo pre-populated one year or 90-day M365 tenant, with a checkbox to add one year of ID Governance. Fully functional M365 enterprise tenant with content, and fully functional ID Governance.

Microsoft Entra ID Governance Engineering-led videos

Automate Identity Workflows
Microsoft Entra admin center
Onboard new hire employee
Workflow tasks
Task order
Name
Enabled
Enable User Account
Generate Temp Access Pass
Send Welcome Email
Order Standard PC and Peripherals
Set up workspace
Add user to groups
Microsoft

https://aka.ms/425show/EntraIDG/Overview

Entra Quick Learn Playlist

Automate onboarding & offboarding tasks with Microsoft Entra | Identity Lifecycle Management - YouTube

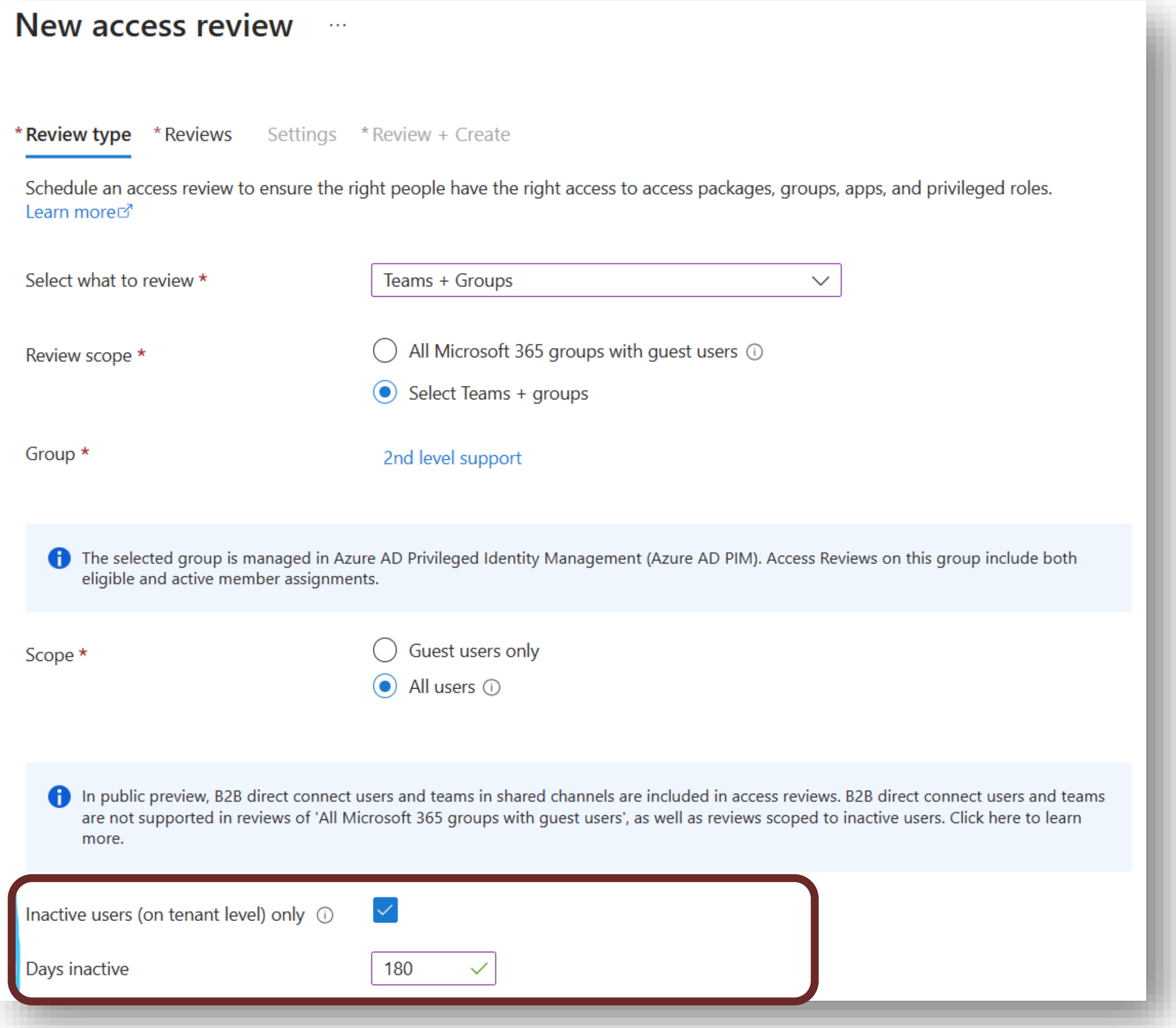
Appendix and additional slides

AR – Inactive Users

General Availability

Review inactive users

- Review and address stale accounts that haven't been active for a specified period
- Includes interactive and non-interactive sign-ins
- You define what inactive means
- Automatically remove stale accounts



New access review ···

*Review type *Reviews Settings *Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles. Learn more

Select what to review *: Teams + Groups

Review scope *: ○ All Microsoft 365 groups with guest users ⓘ ● Select Teams + groups

Group *: 2nd level support

ⓘ The selected group is managed in Azure AD Privileged Identity Management (Azure AD PIM). Access Reviews on this group include both eligible and active member assignments.

Scope *: ○ Guest users only ● All users ⓘ

ⓘ In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ ☑

Days inactive: 180 ✓