Microsoft Security

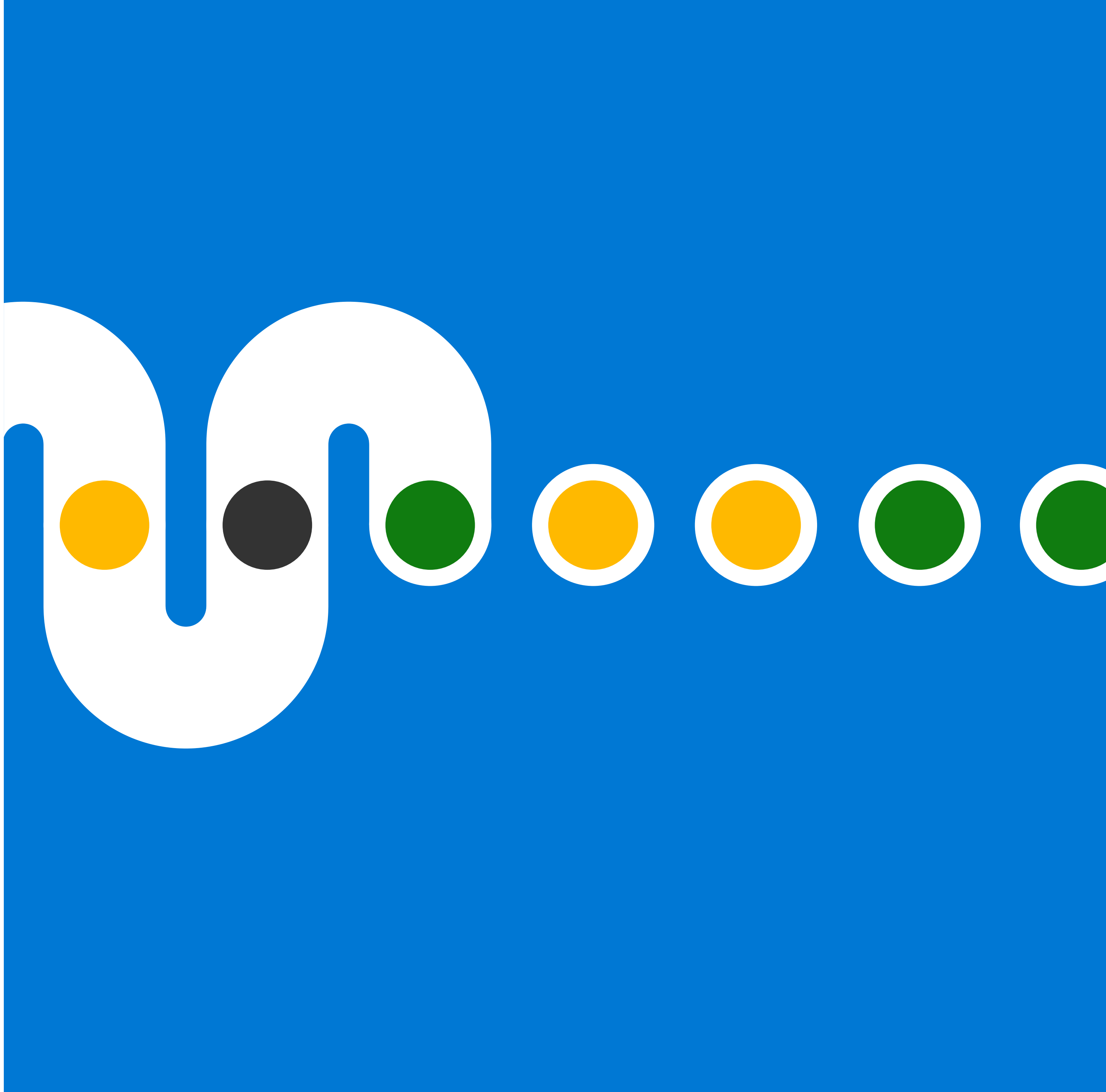
Microsoft Identity Governance Entitlements Management, Access Reviews, and Lifecycle Workflows (Preview)

Angelica Faber

Agenda

- Entitlements Management & Access Reviews w/Demo
- Lifecycle Workflows (Preview) w/Demo
- PIM w/Demo

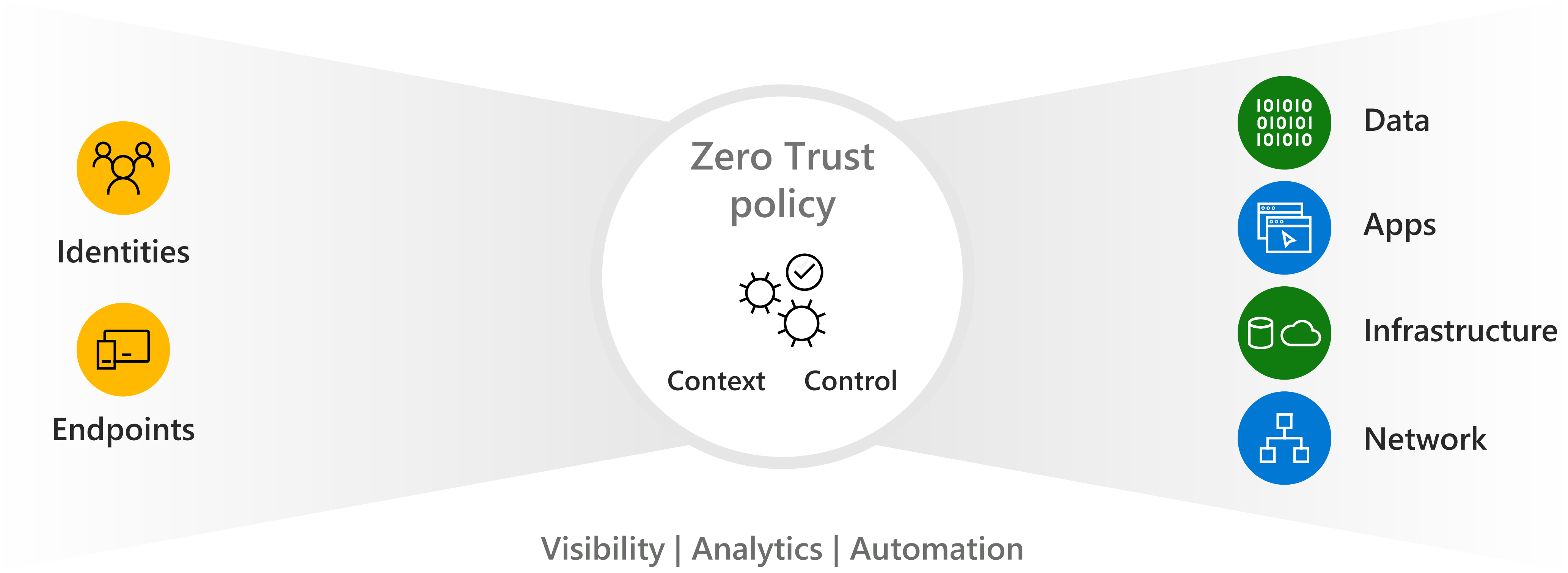
Identity Governance: Entitlement Management & Access Reviews



Secure your organization with Zero Trust

A modern security framework with identity as its foundation

Verify explicitly | **Use least-privileged access** | Assume breach



Identities

Endpoints

Zero Trust policy

Context Control

Data

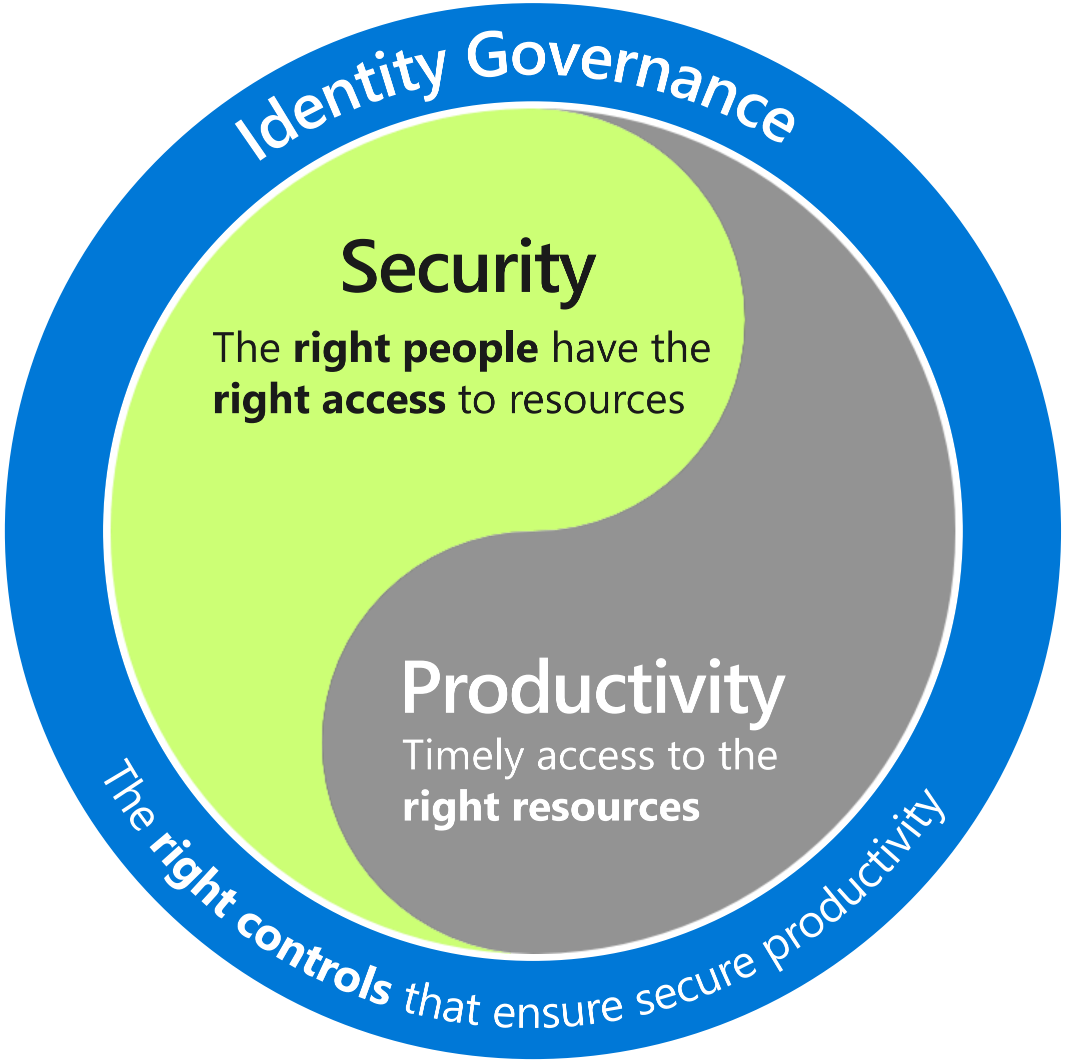
Apps

Infrastructure

Network

Visibility | Analytics | Automation

Identity Governance


Identity Governance
Security
The **right people** have the **right access** to resources
Productivity
Timely access to the **right resources**
The **right controls** that ensure secure productivity

Who has / should have access to which resources?

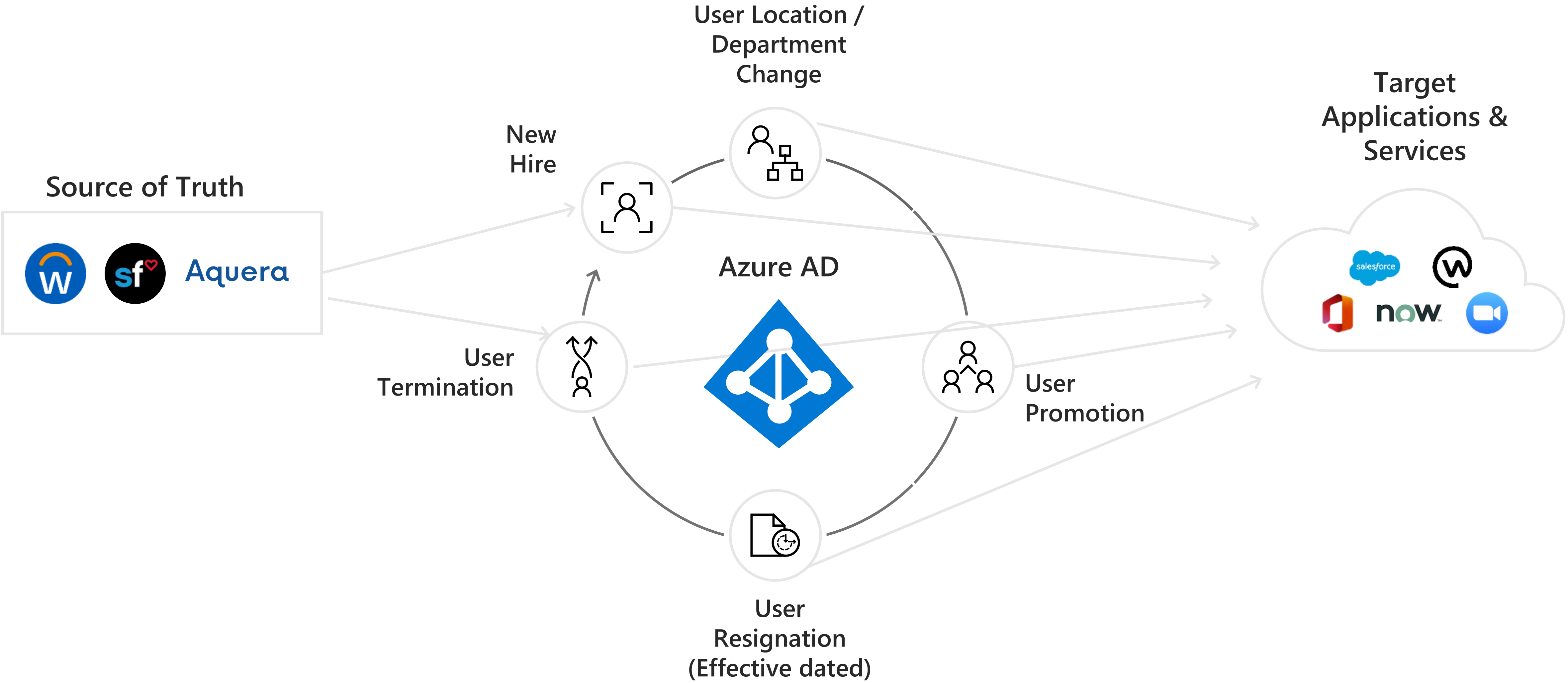
What are they doing with that access?

Are there effective organizational controls for managing access?

Can auditors verify that the controls are working?

Identity & Access Lifecycle

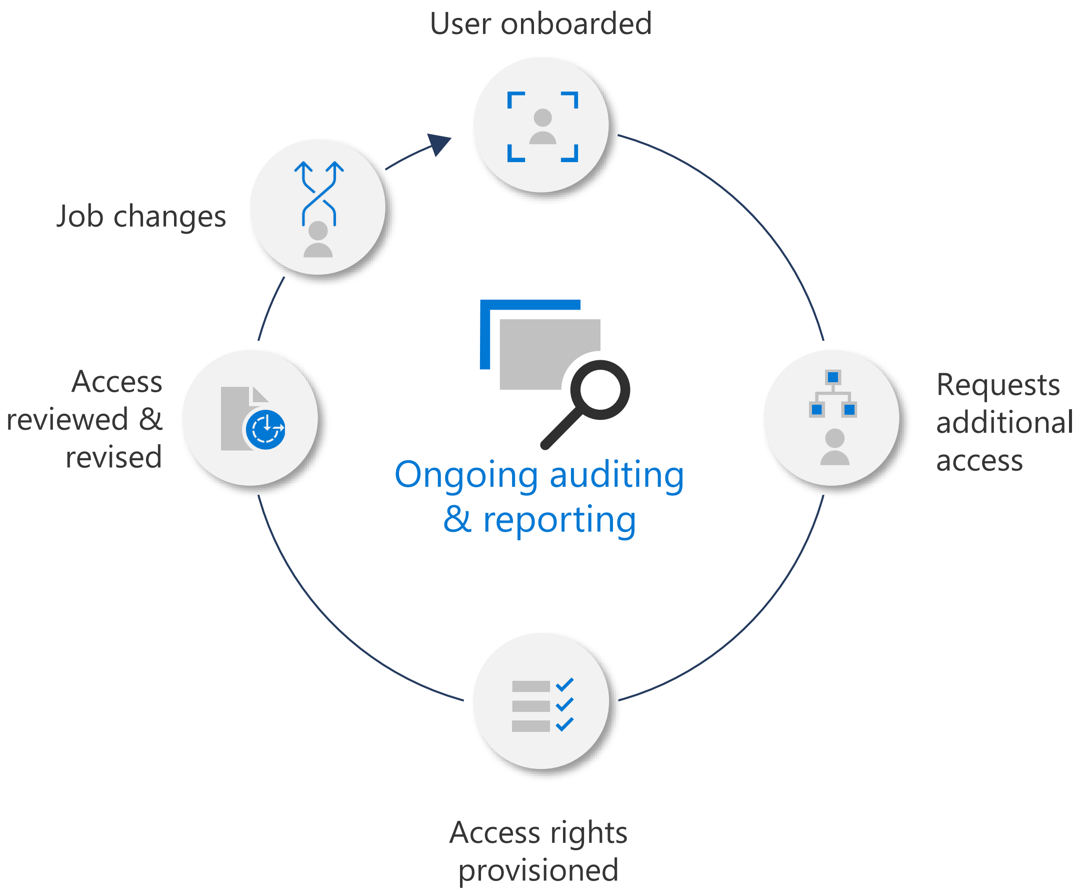
Joiners – Movers - Leavers


Source of Truth
Aquera
User Location / Department Change
New Hire
Azure AD
User Termination
User Promotion
User Resignation (Effective dated)
Target Applications & Services
salesforce
now

Entitlement Management

Automate access request workflows, access assignments, reviews and expiration

- Manage Office 365 groups, Teams, SharePoint Online sites, and Enterprise Applications.
- Delegate access to non-admins using catalogs
- Access packages with expiration dates and approvals ensure that access to resources are time-limited and appropriate
- Easy user experiences for employees and business partners to request access
- Self-service policy and workflow definition by app, group or site owners
- Multi-stage approval workflow and recurring access reviews


User onboarded
Requests additional access
Access rights provisioned
Access reviewed & revised
Job changes
Ongoing auditing & reporting

Access Reviews

Validation of access for apps and groups, remove excessive access, block guest access, and delete accounts.

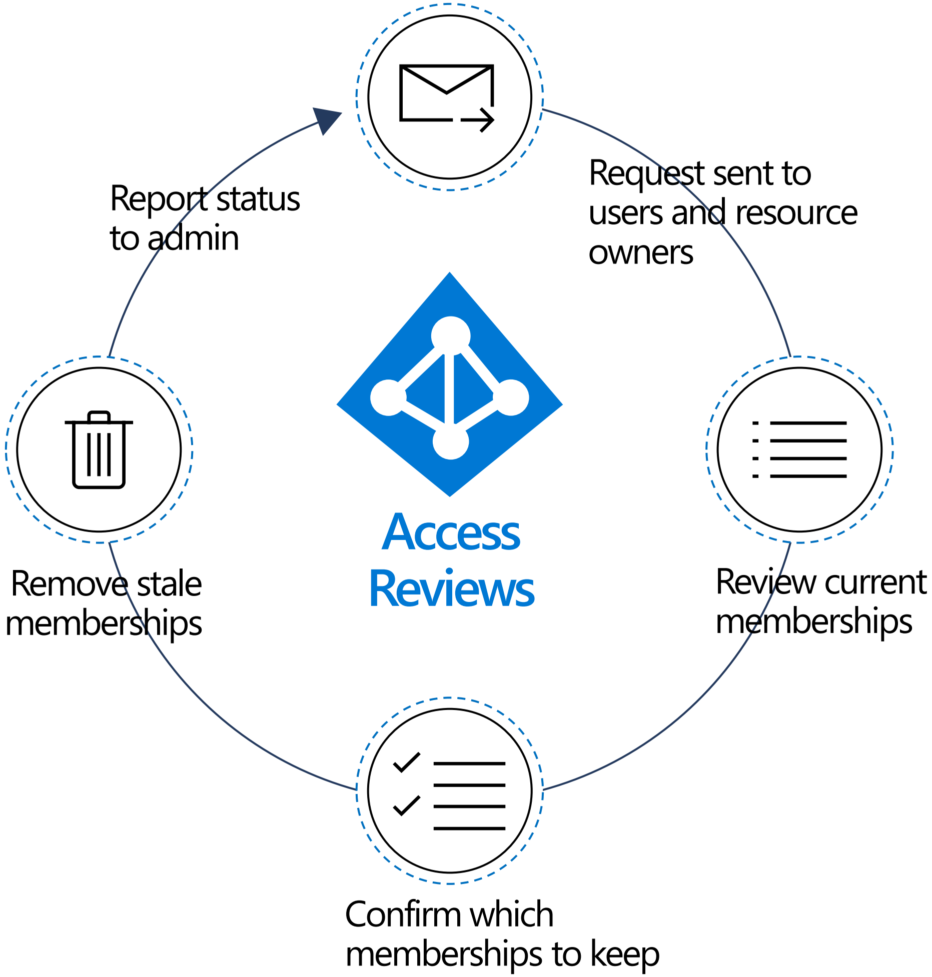
- Access review controls to track reviews for compliance or risk-sensitive applications specific to your organization

- Use the insights to efficiently decide whether guests should have continued access

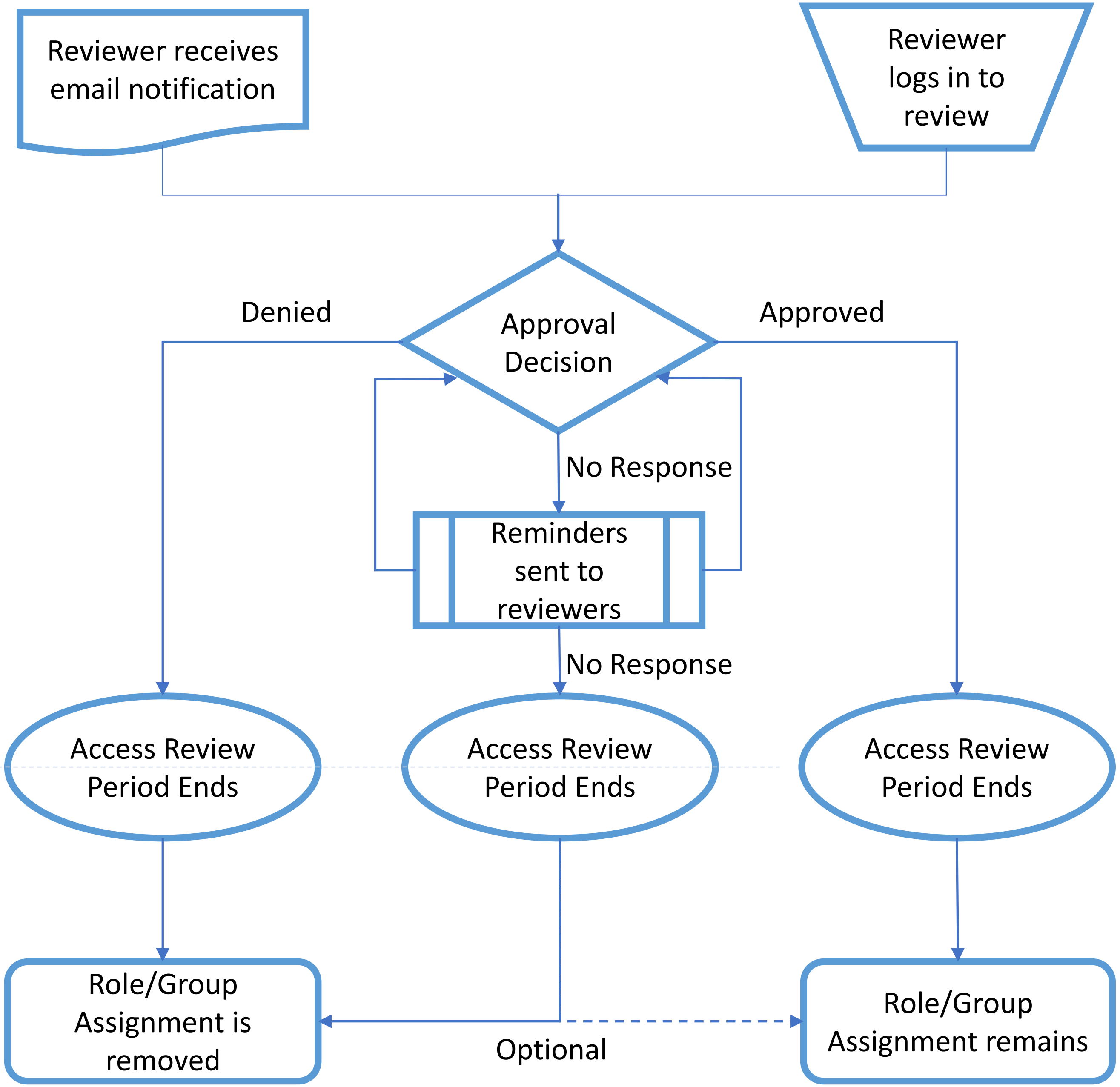
- Configure frequency and action policies to automate the re-certification process

- Schedule recurring access reviews and have decisions automatically applied after the review completes

- Set policies for group lifecycle

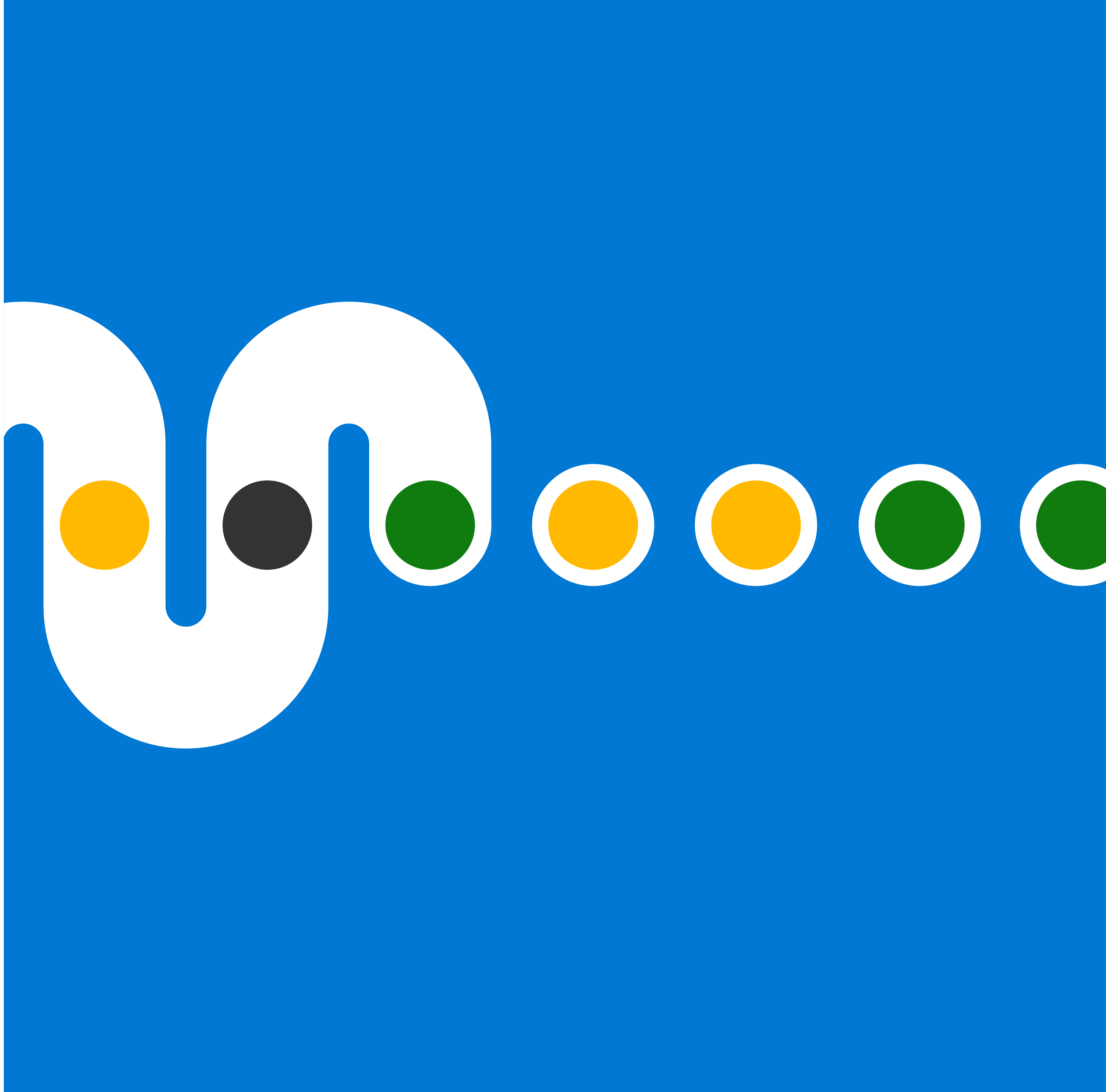

Access Reviews
Request sent to users and resource owners
Review current memberships
Confirm which memberships to keep
Remove stale memberships
Report status to admin

Access Reviews - Sample


Reviewer receives email notification
Reviewer logs in to review
Approval Decision
Denied
Approved
No Response
Reminders sent to reviewers
No Response
Access Review Period Ends
Access Review Period Ends
Access Review Period Ends
Role/Group Assignment is removed
Optional
Role/Group Assignment remains

Demo

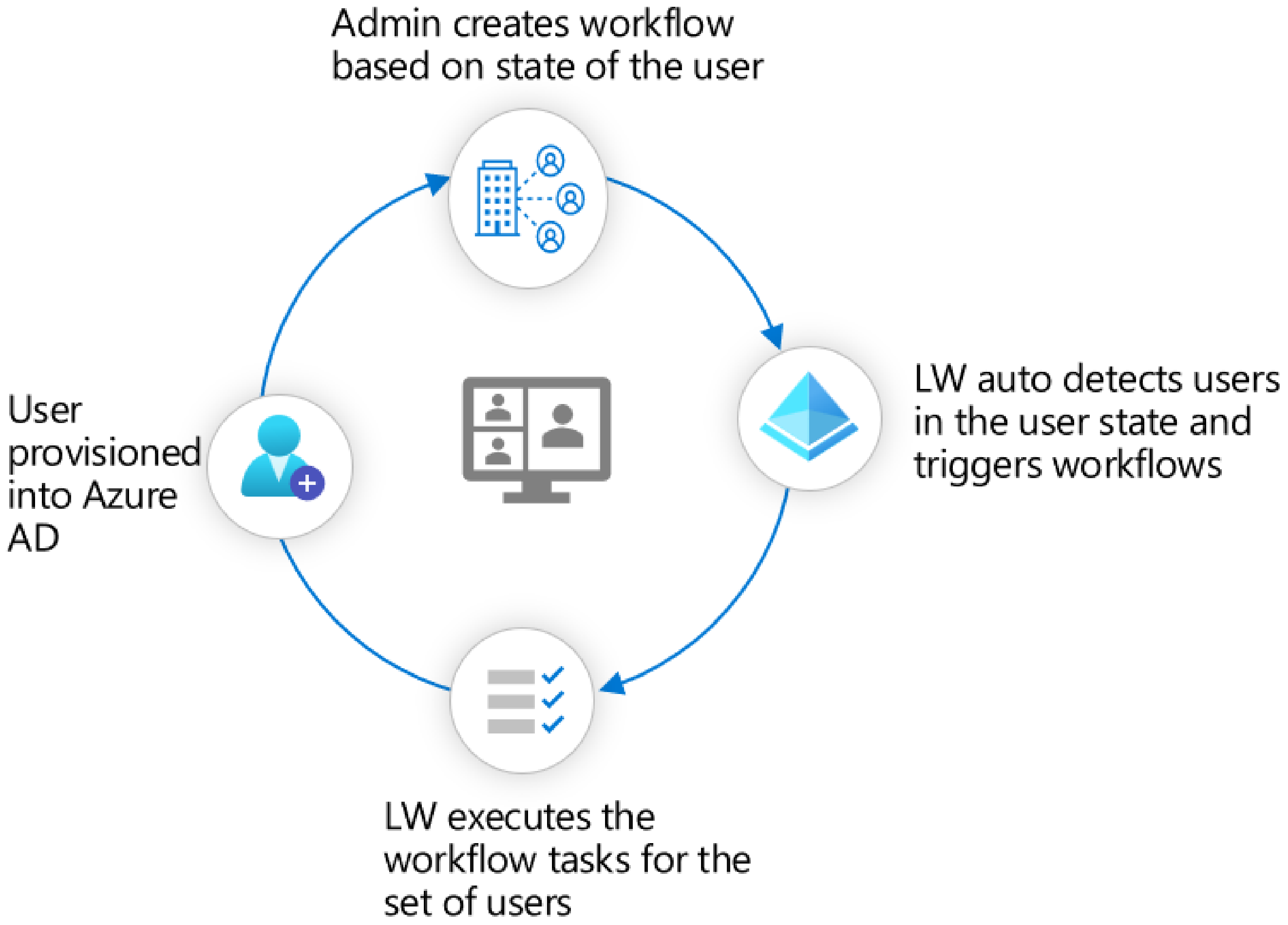
Identity Governance: Lifecycle Workflows



Microsoft

Lifecycle Workflows:
How it works

IT admins can manage workflows after users provisioned into Azure AD



Admin creates workflow based on state of the user

LW auto detects users in the user state and triggers workflows

LW executes the workflow tasks for the set of users

User provisioned into Azure AD

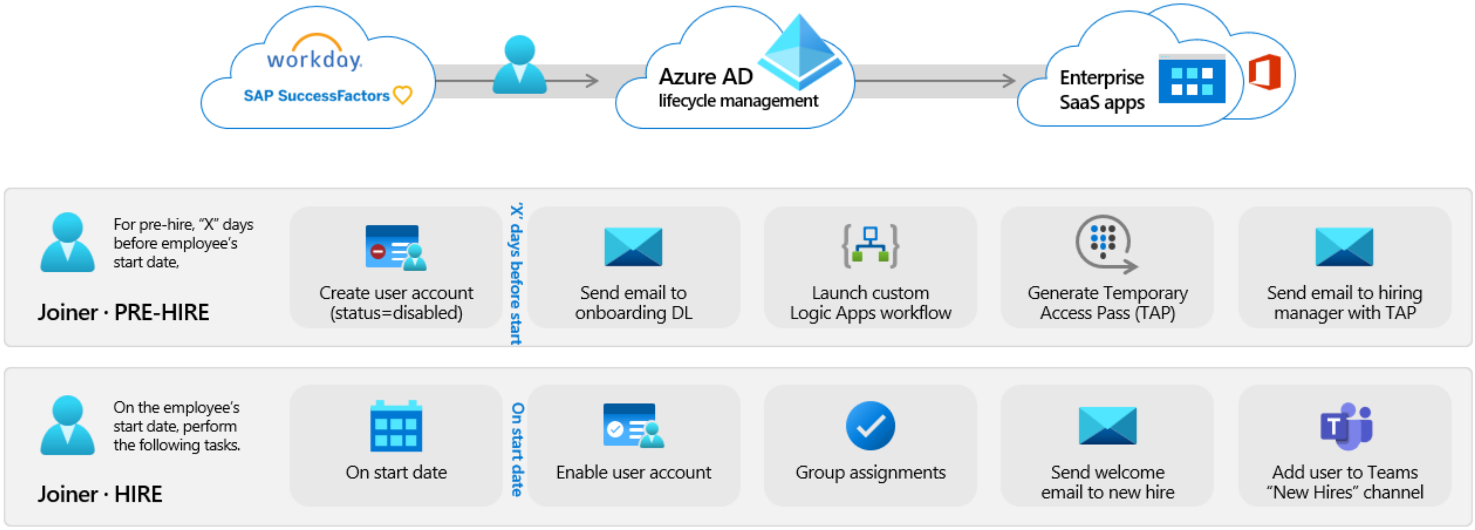
Microsoft

Current Capabilities

- New MS Graph APIs for managing workflows and tasks
- Customizable workflow templates for most common Joiner tasks
- Support for automatic scheduled runs or manual on demand runs for selected users
- Workflow versioning support and status reporting for compliance and auditing
- Basic extensibility with Logic Apps and M365 Teams integration

Public Preview – Joiner scenario

Now, admins can configure workflows in Azure AD to automate onboarding tasks, so new employees are productive on day one.



workday.

SAP SuccessFactors

Azure AD
lifecycle management

Enterprise
SaaS apps

Joiner · PRE-HIRE

For pre-hire, "X" days before employee's start date,

Create user account (status=disabled)

'X' days before start

Send email to onboarding DL

Launch custom Logic Apps workflow

Generate Temporary Access Pass (TAP)

Send email to hiring manager with TAP

Joiner · HIRE

On the employee's start date, perform the following tasks.

On start date

On start date

Enable user account

Group assignments

Send welcome email to new hire

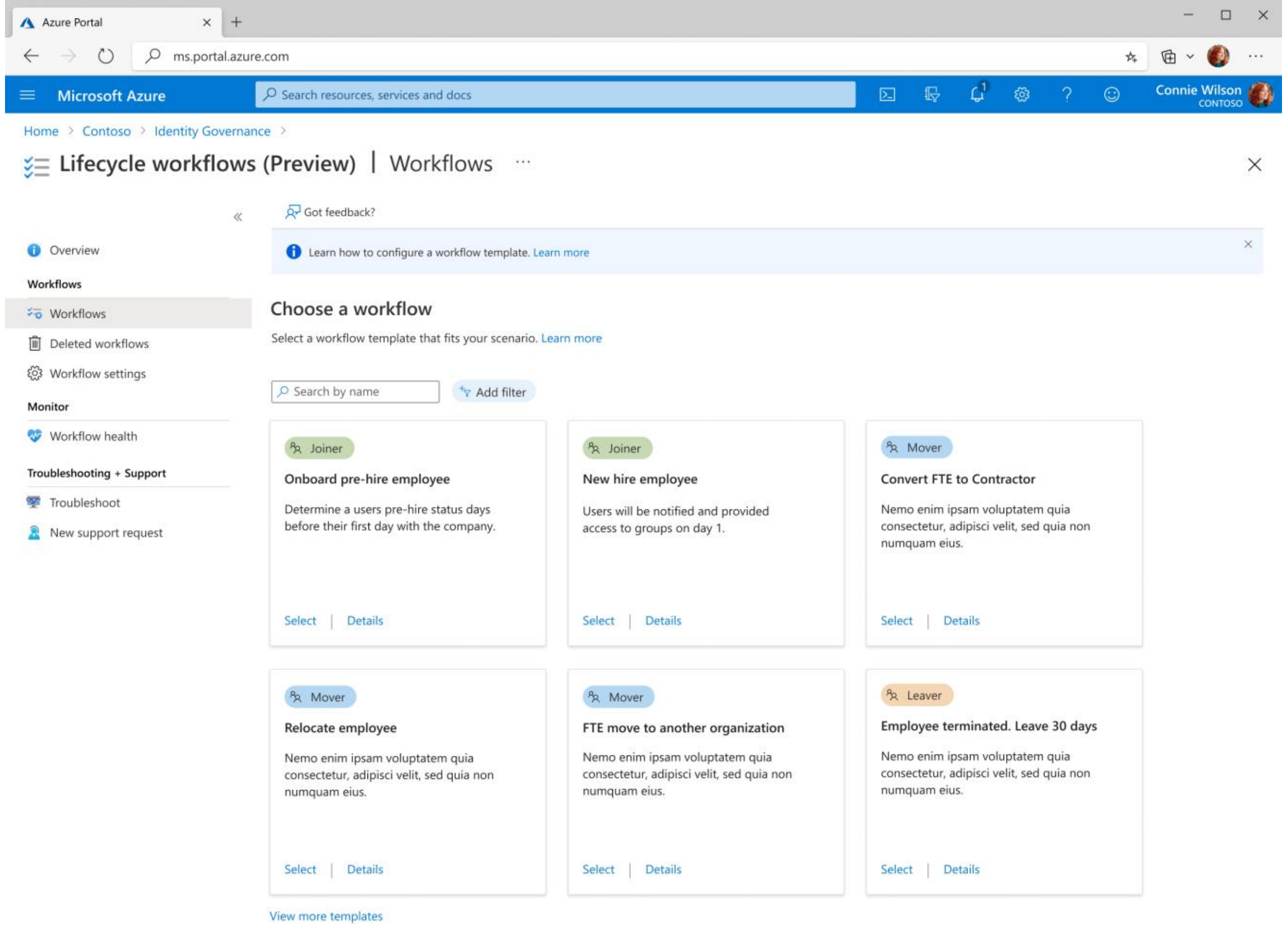
Add user to Teams "New Hires" channel

Microsoft

Other Capabilities

- Delegated management via new Azure portal UI and Lifecycle Workflows admin role
- Customizable workflow templates for most common Leaver termination tasks
- Custom workflow schedule options
- Rich workflow status reporting and audit logs
- Expanded extensibility with Logic Apps parameters and call backs

Public Preview – Joiner + Leaver scenarios



Learn how to configure a workflow template. Learn more

Choose a workflow

Select a workflow template that fits your scenario. Learn more

Joiner
Onboard pre-hire employee
Determine a users pre-hire status days before their first day with the company.
Select | Details

Joiner
New hire employee
Users will be notified and provided access to groups on day 1.
Select | Details

Mover
Convert FTE to Contractor
Nemo enim ipsam voluptatem quia consectetur, adipisci velit, sed quia non numquam eius.
Select | Details

Mover
Relocate employee
Nemo enim ipsam voluptatem quia consectetur, adipisci velit, sed quia non numquam eius.
Select | Details

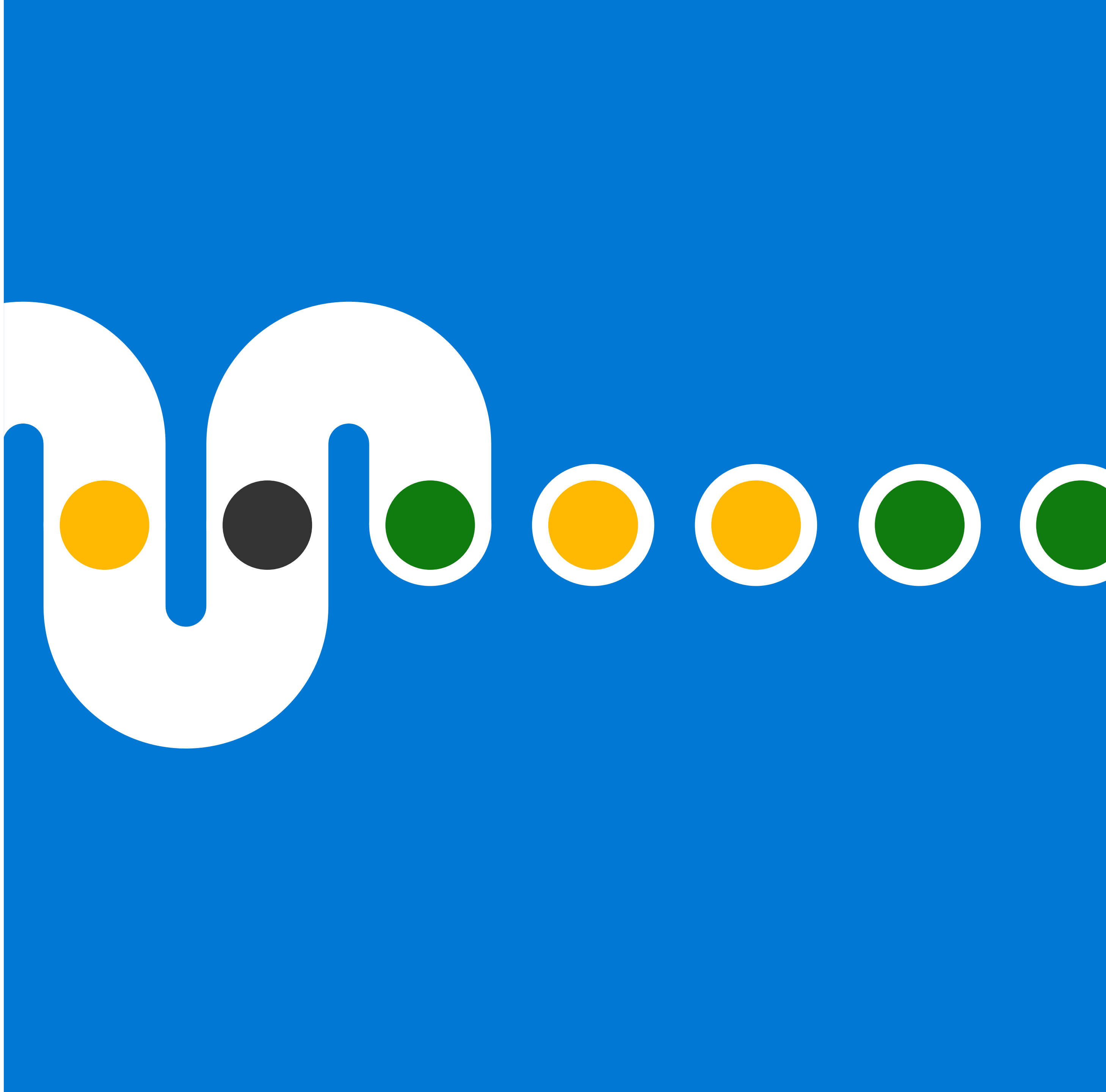
Mover
FTE move to another organization
Nemo enim ipsam voluptatem quia consectetur, adipisci velit, sed quia non numquam eius.
Select | Details

Leaver
Employee terminated. Leave 30 days
Nemo enim ipsam voluptatem quia consectetur, adipisci velit, sed quia non numquam eius.
Select | Details

View more templates

Demo

Identity Governance: Privileged Identity Management



Privileged Identity Management

Management and auditing of admin roles across Azure and Office 365 services

See which users are assigned privileged roles.

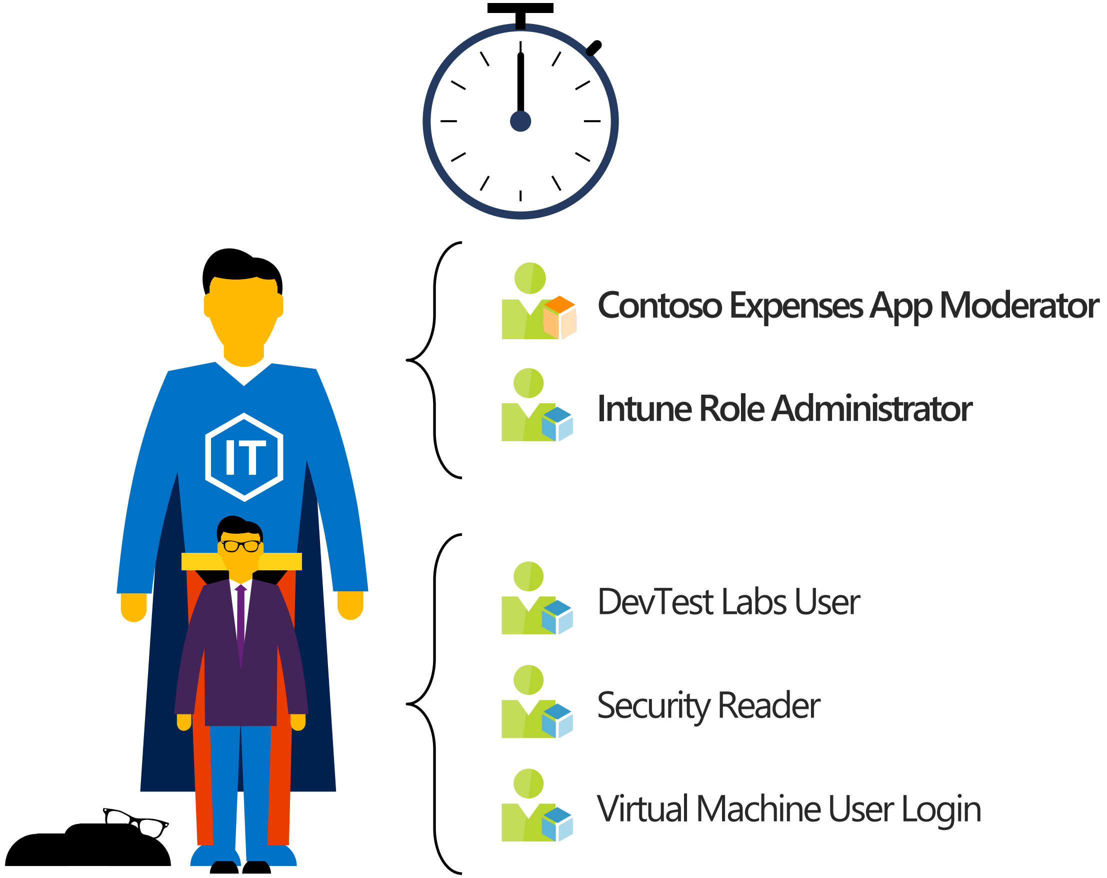
Enable on-demand, "just in time" administrative access.

Set up approval flows for privilege activation.

Get alerts and view a history of administrator activation and actions.

Review administrative roles and require users to provide justification to retain membership.

Manage built-in Azure resource roles, as well as custom (RBAC) roles.


IT
Contoso Expenses App Moderator
Intune Role Administrator
DevTest Labs User
Security Reader
Virtual Machine User Login

Key Capabilities

Just-in-time

privileged access to Azure AD and Azure resources

Time-bound

access to resources using start and end dates

Approval

to activate privileged roles

Enforce MFA

to activate any role

Justification

to understand why users activate privileged role

Notification

when privileged roles are activated

Access reviews

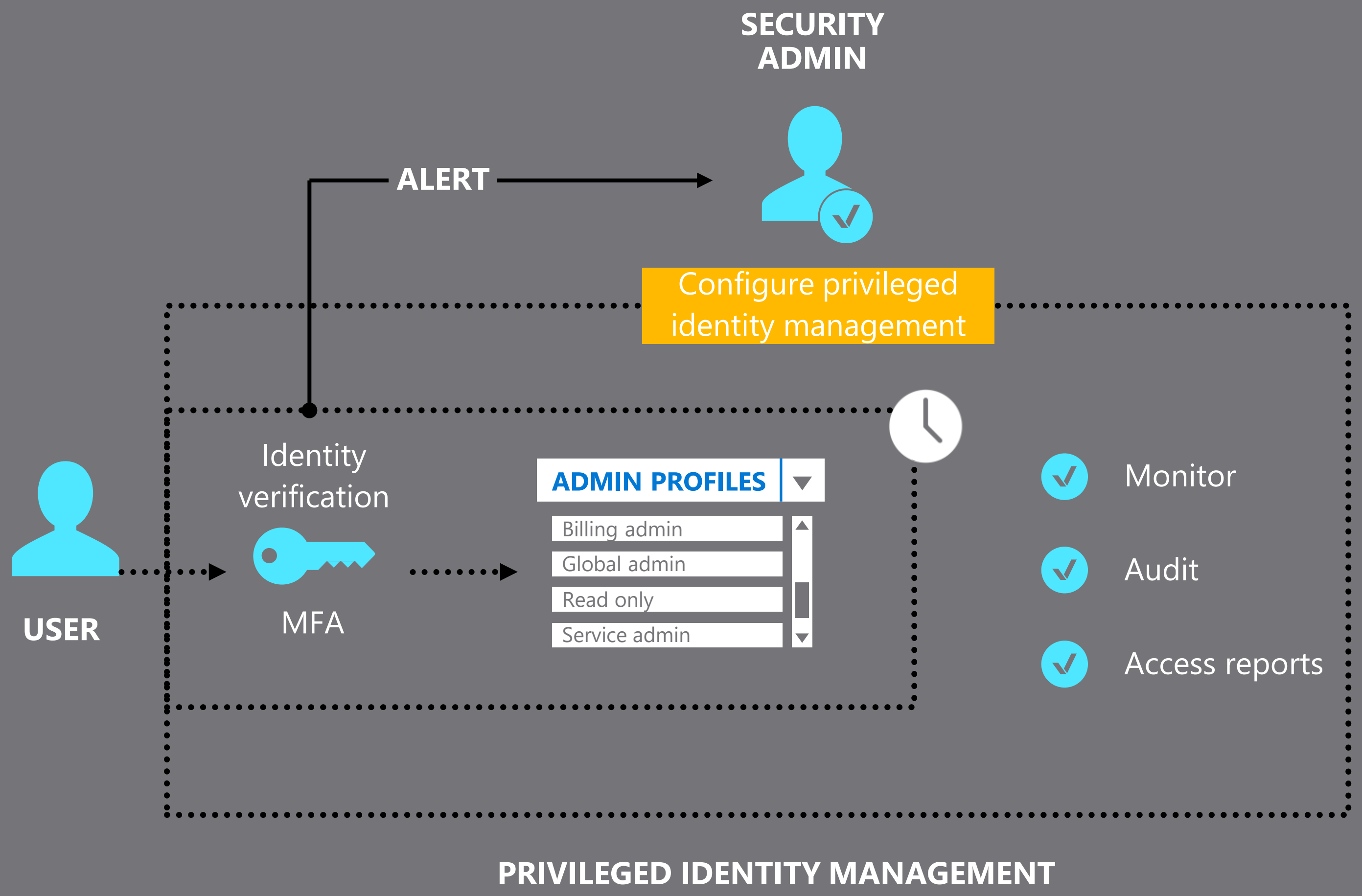
to ensure users still need privileged roles

Audit history

Internal and external audit for regulations and standard compliance

How It Works?

- Users need to activate their privileges to perform a task
- Multi-factor authentication (MFA) is enforced during the activation process
- Alerts inform administrators about out-of-band changes
- Users retain their privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports, and review everyone who is eligible to activate using access reviews



Demo

Thank you!!