

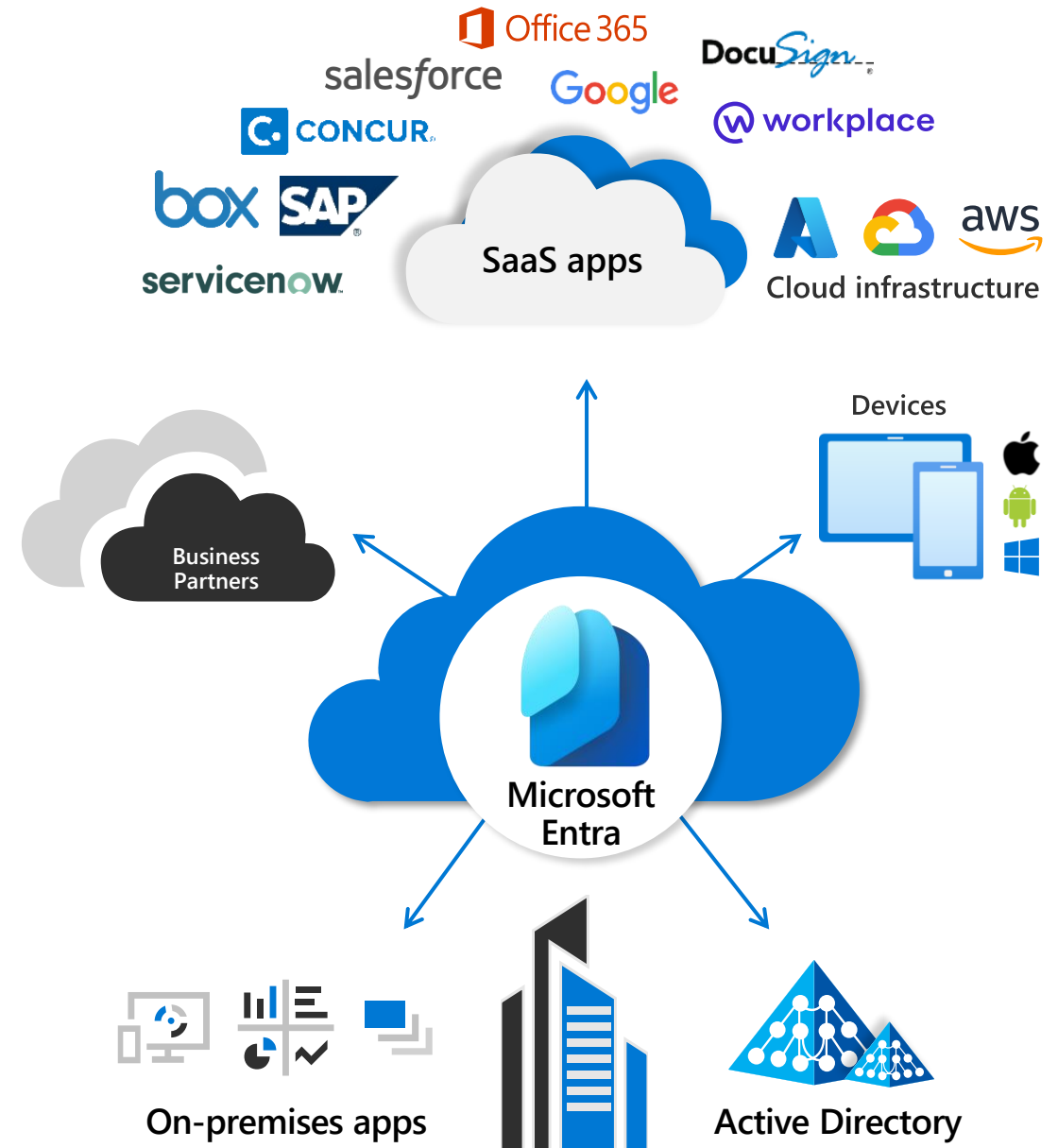
# Entra ID Identity & Access Management

**Daniel von Büren**  
Swiss Security Officer



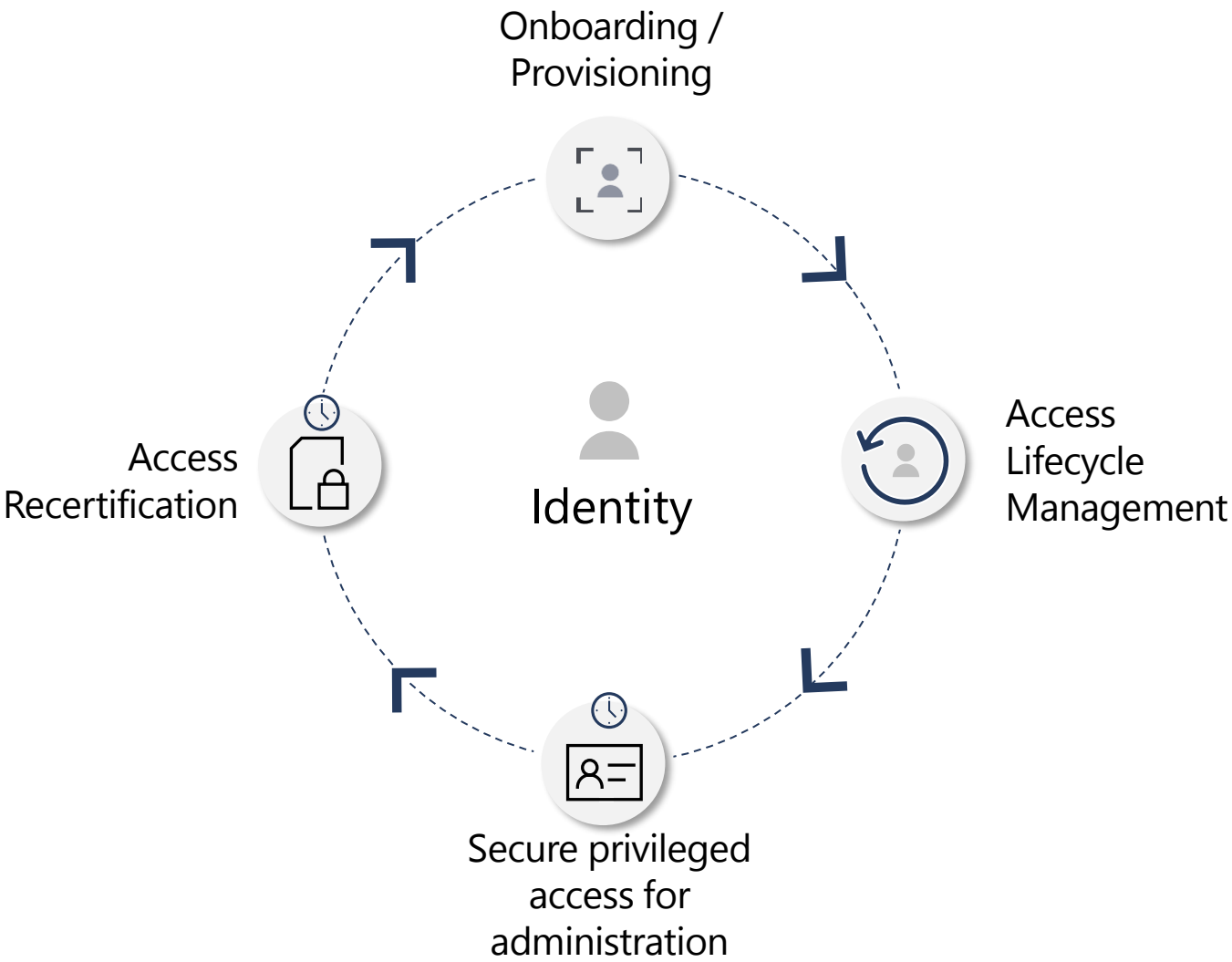
# Microsoft's Entra ID

- Controls for employees, business partners, consumers, workload identities and their access
- Manage and govern identities (human and system) at scale
- Enable true SSO across on premise and cloud applications
- Enforce controls for access to applications and resources anywhere -- via connectors, standards-based APIs, and partnerships
- Security for emerging and ongoing threats
- Remove dependencies on on-premises identity management infrastructure
- Enhance security by managing company owned and personal owned devices

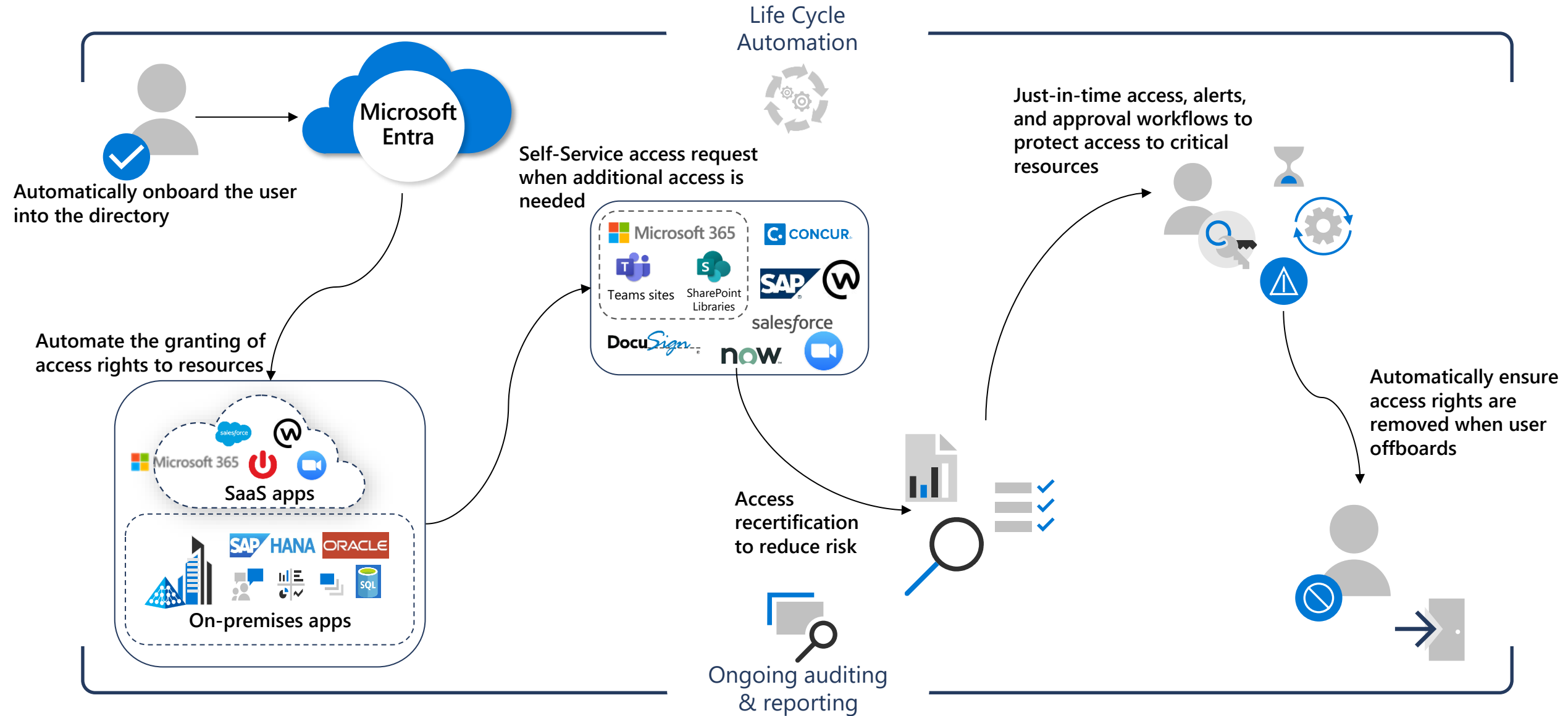


# Microsoft Entra ID Governance

# Microsoft Entra ID Governance



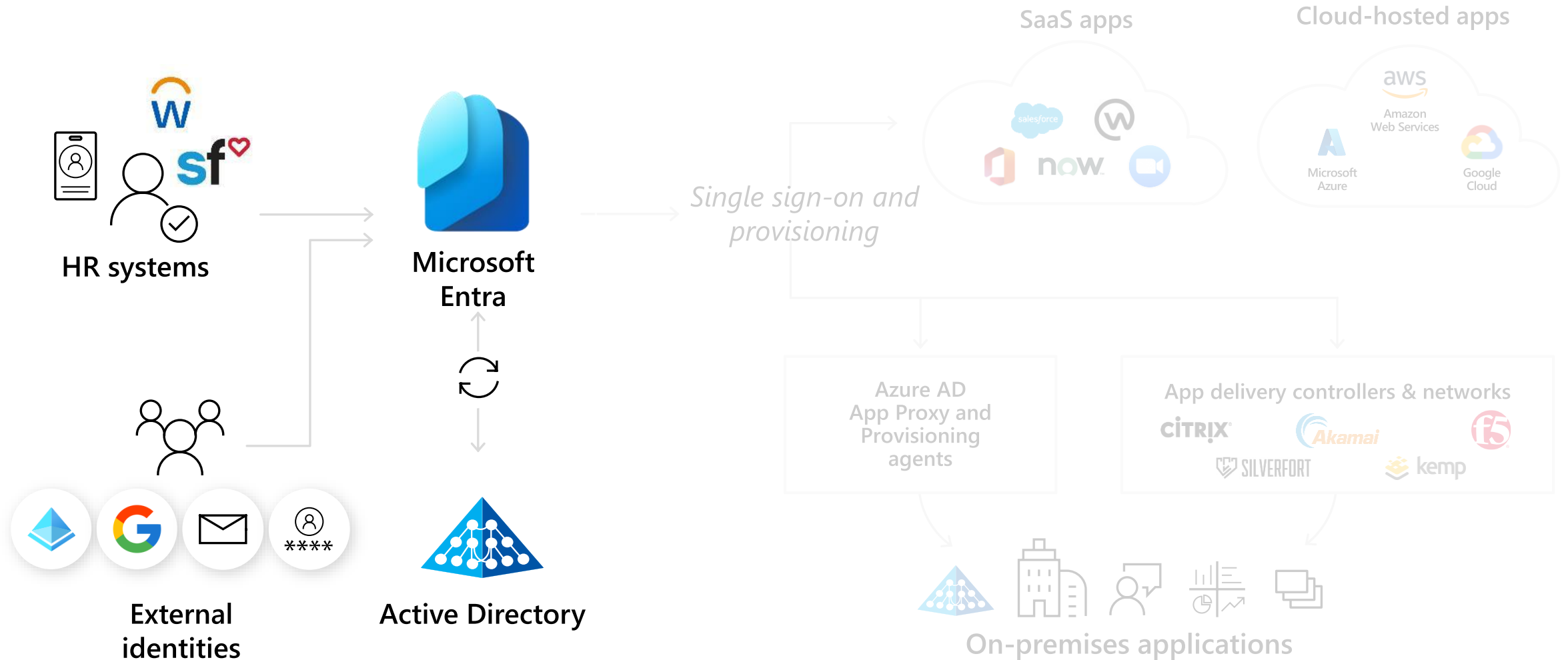
# A user journey



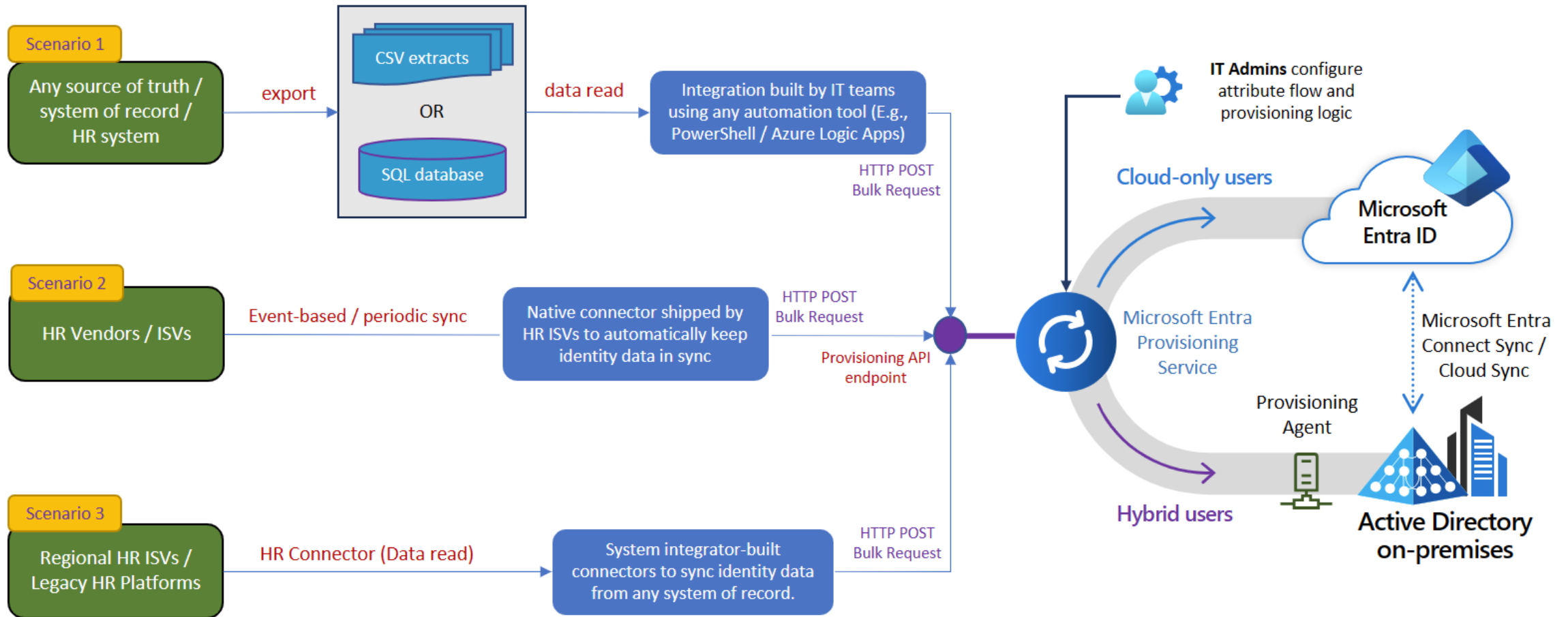
# Onboard any user

## Inbound provisioning

---



# API-driven inbound provisioning

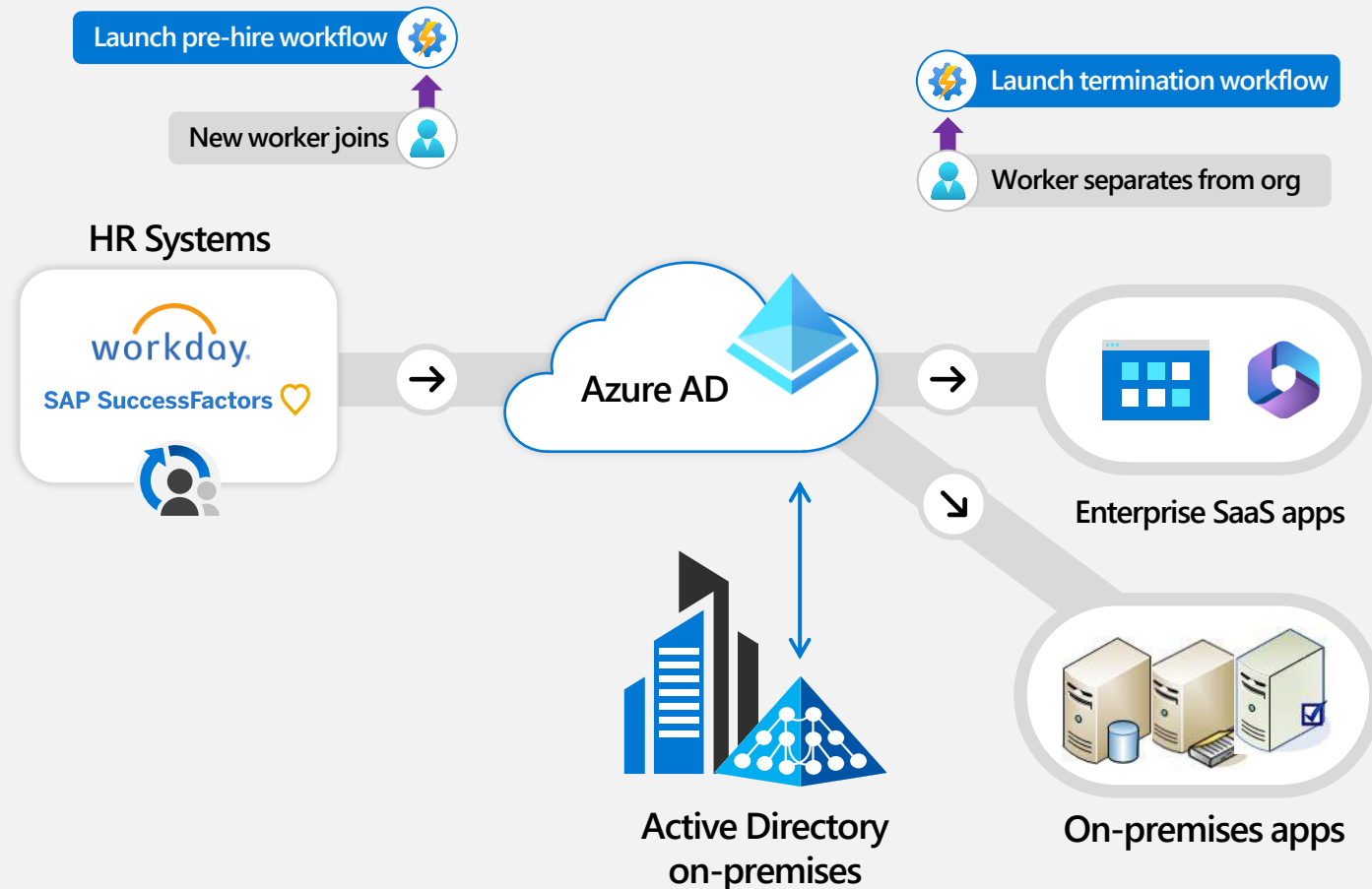


# Lifecycle Workflows

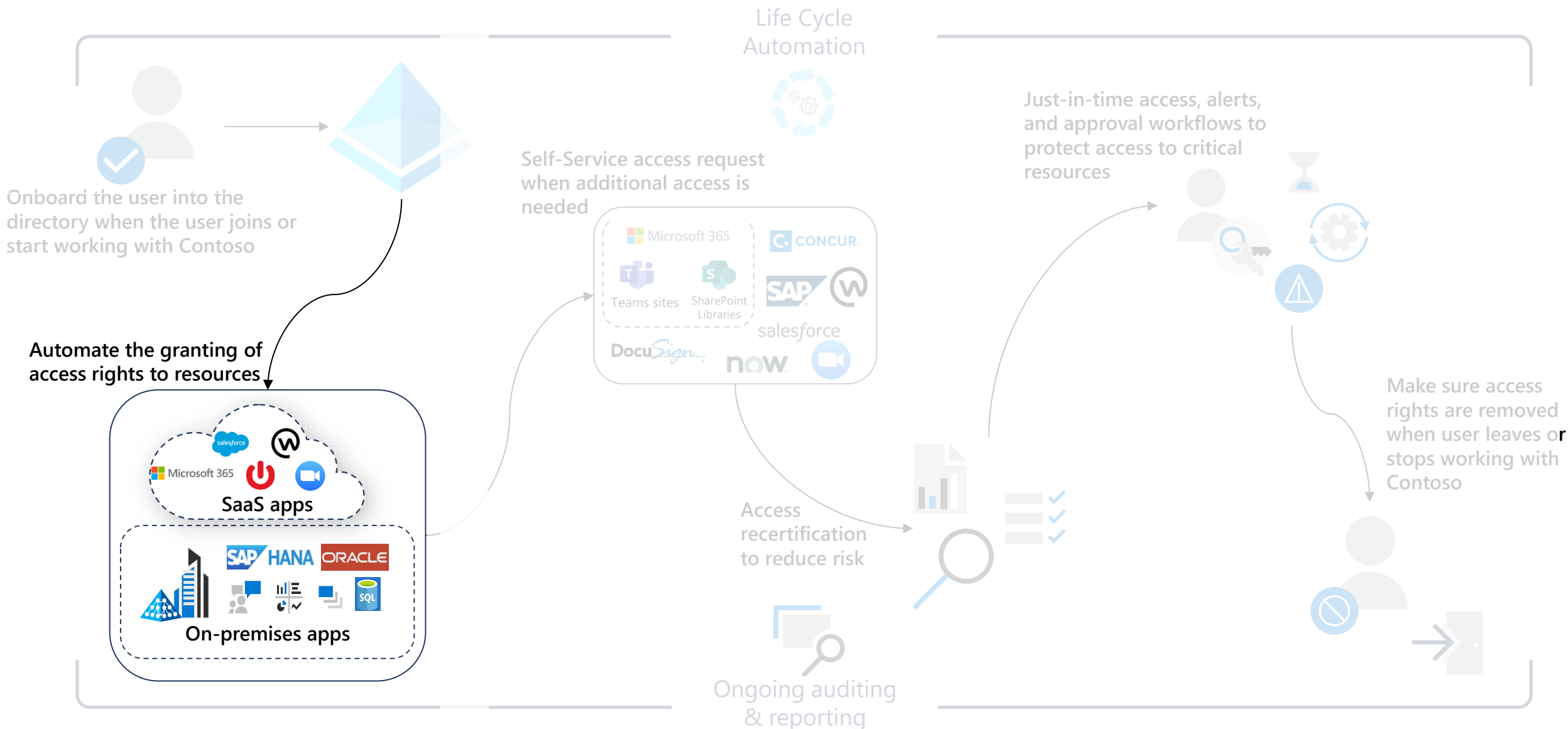
## Automate join/move/leave employee lifecycle events

- Organizations can schedule tasks to occur before, at or after a join or leave date; these can also be run on-demand.
- 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.

Demo

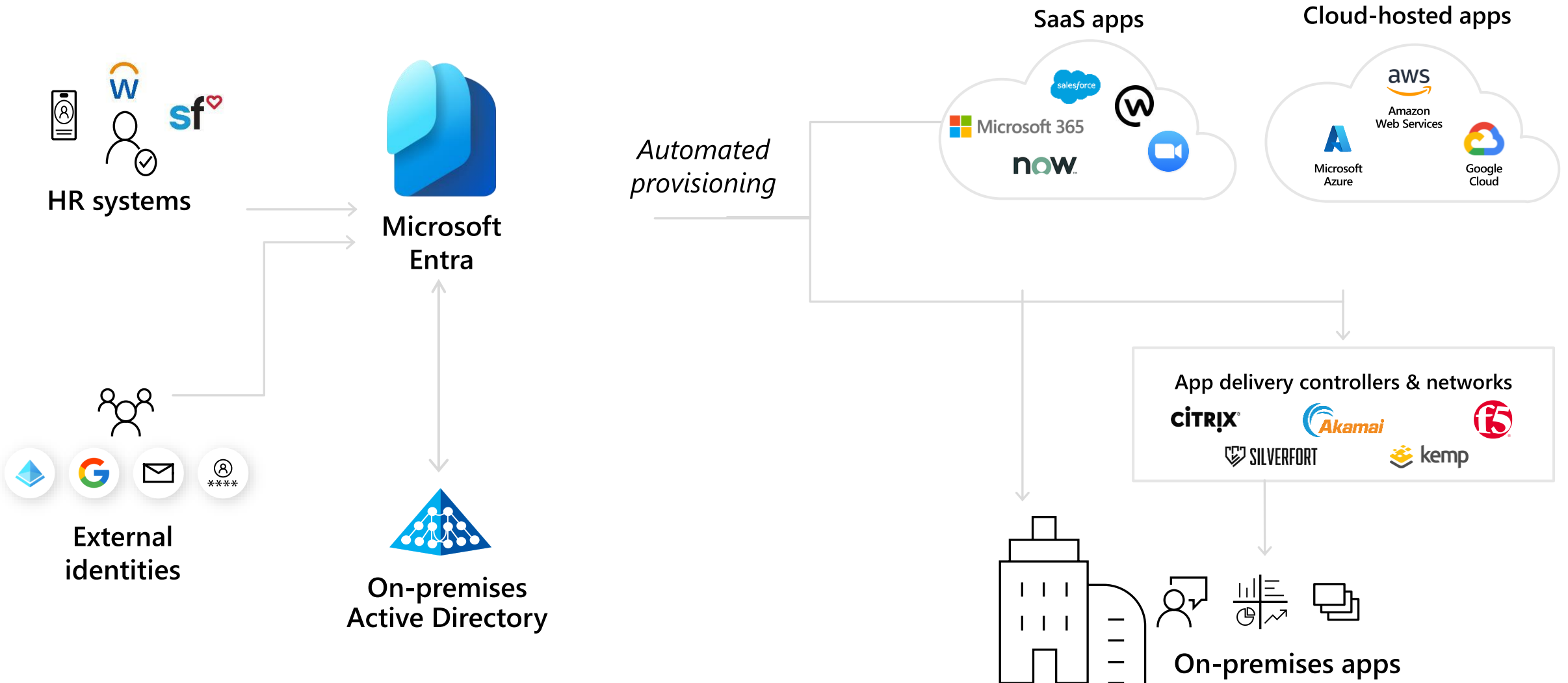


# Contoso's user journey



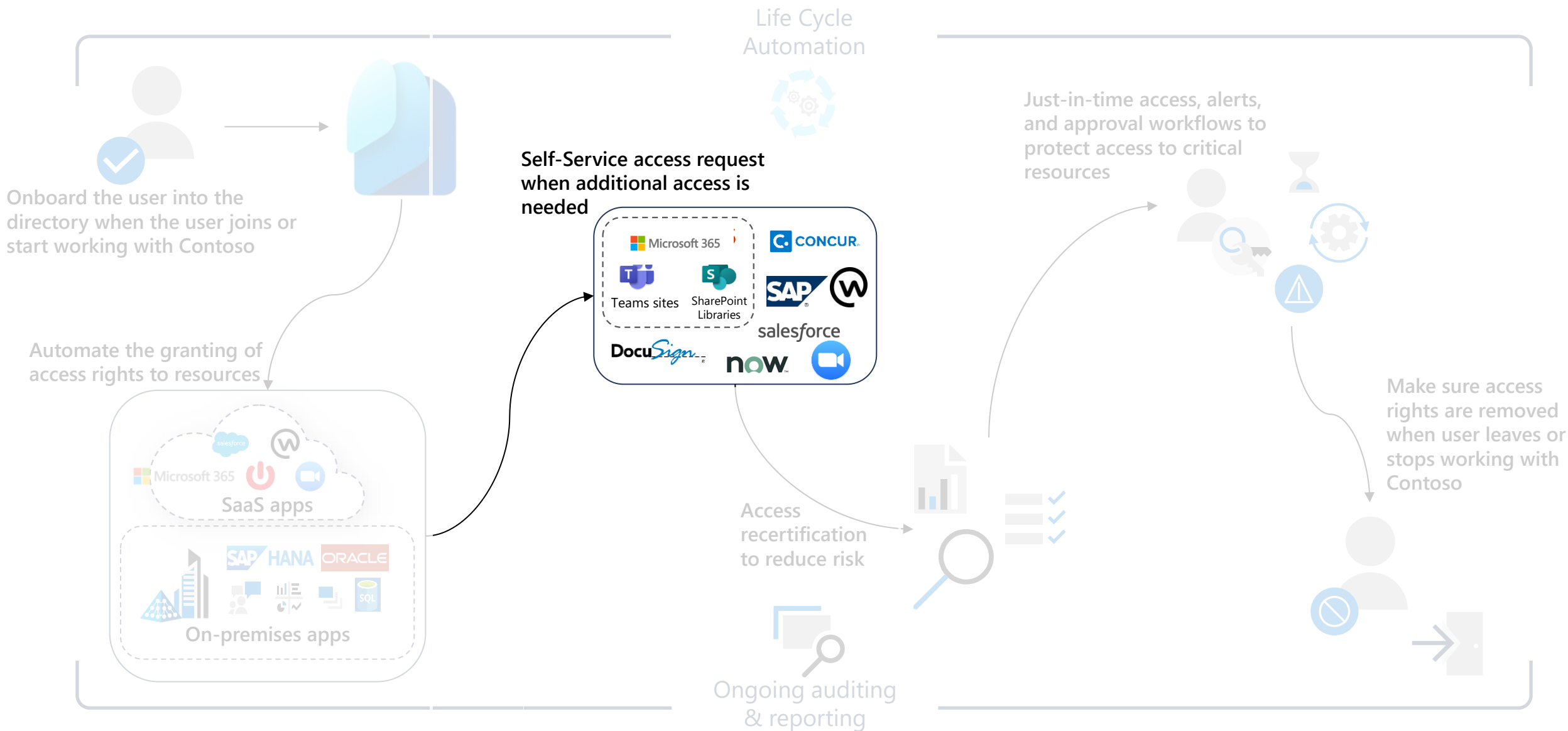
# Connect your workforce to any app

## Single sign-on and outbound provisioning



# Contoso's user journey

Demo



# Access requests, workflow and approvals

## Entitlement management

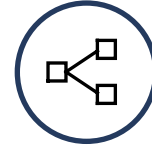
Demo



Let users request access (to any connected app, group, Teams site and more) while automating access assignments, approval, workflows, reviews and expiration for all human identity types (users, guests, etc.)



Self-service policy and workflow can be defined by app, group or site owners



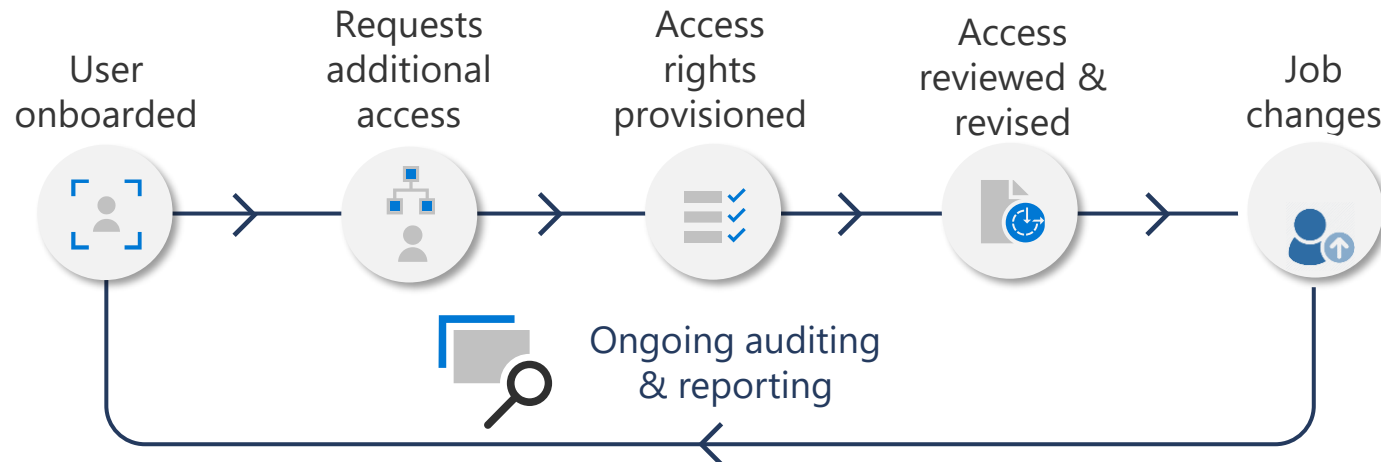
Supports multi-stage approval workflow, separation of duties enforcement and recurring access recertification



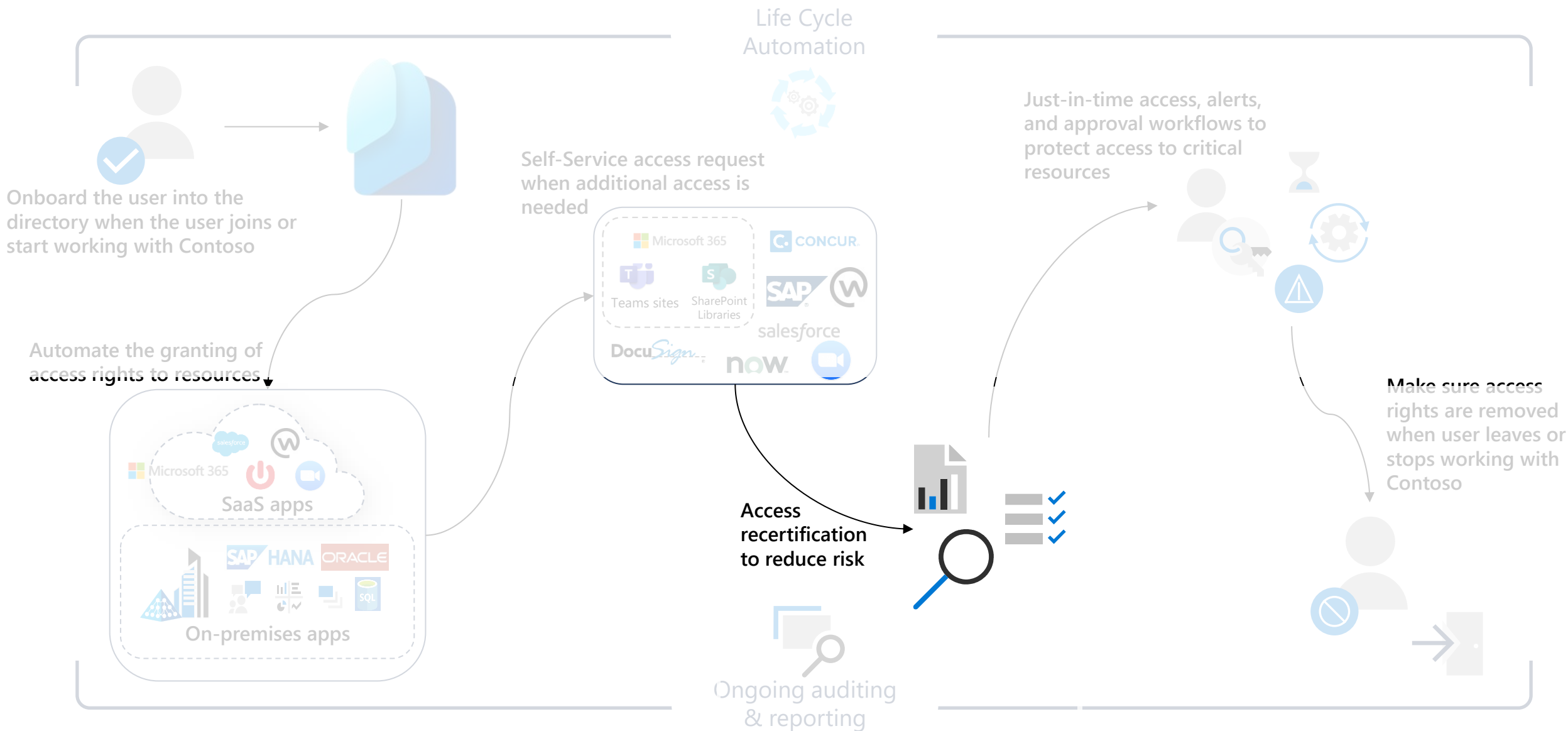
Supports custom workflows for access lifecycle (through Logic Apps integration)



Access time-limited, guests removed when last access expires



# Contoso's user journey



# Access recertification to reduce risk

## Access Reviews

---



---

Natively built-in to  
Microsoft Entra

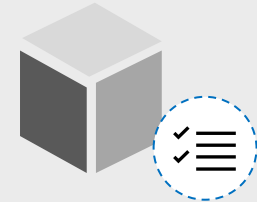
---



---

Manage risk and meet  
compliance for users,  
guests and workload  
identities

---



---

Ensure access to  
sensitive Teams, Groups,  
Apps, Roles is reviewed  
periodically

---

# Access recertification to reduce risk

## Access Reviews

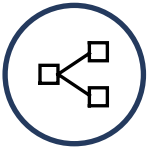
Demo



**Policy-based** access certification for automation



**Intelligent recommendations** based on sign-in history



**Multi-stage** reviews



**Audit history** for compliance reviews



Native support for **B2B guest** users, privileged roles, non-human workload identities



**Customizable notifications** to reviewers



**Downloadable reports** to see how reviewers are performing



**Out-of-the-box integration** with Microsoft Teams

← Access reviews

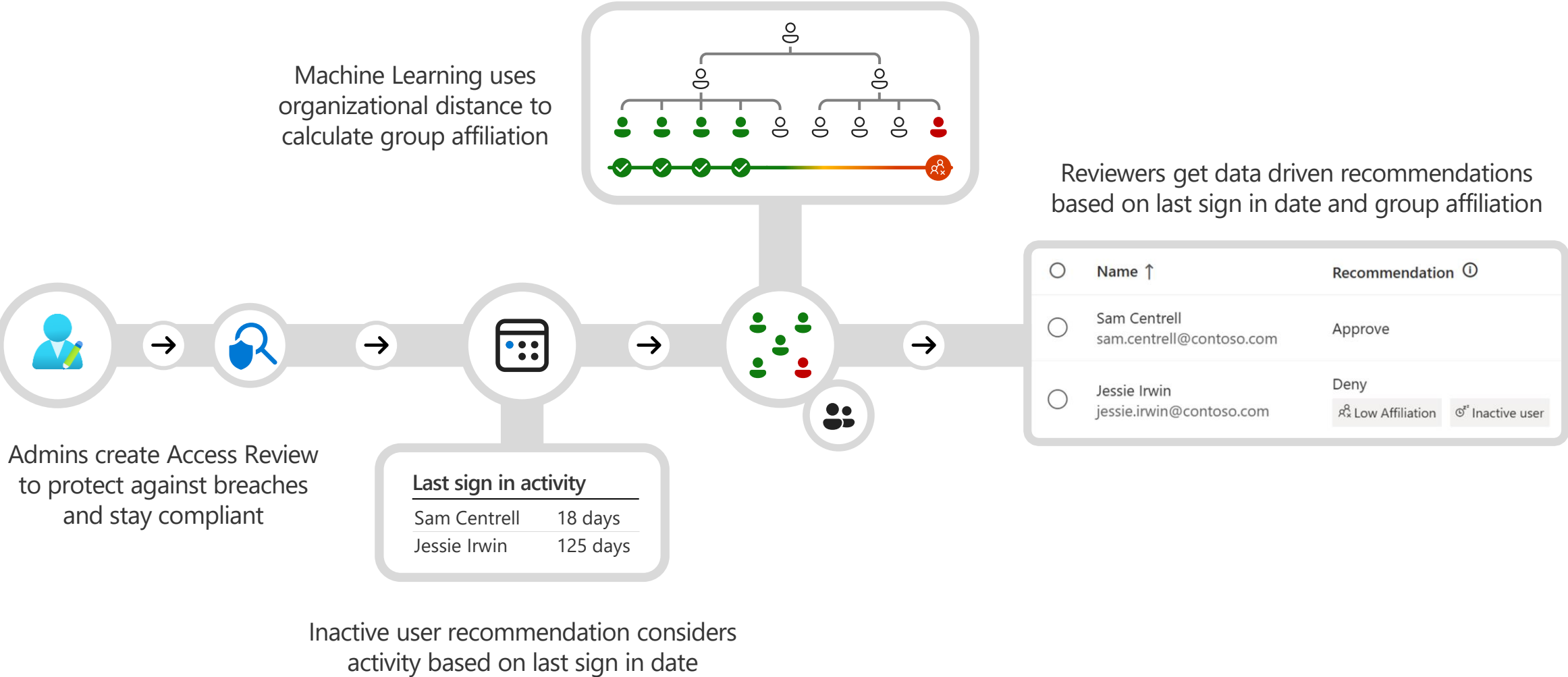
FY22 Quarterly review

Please review members of 'FY22 Planning' [See details](#)

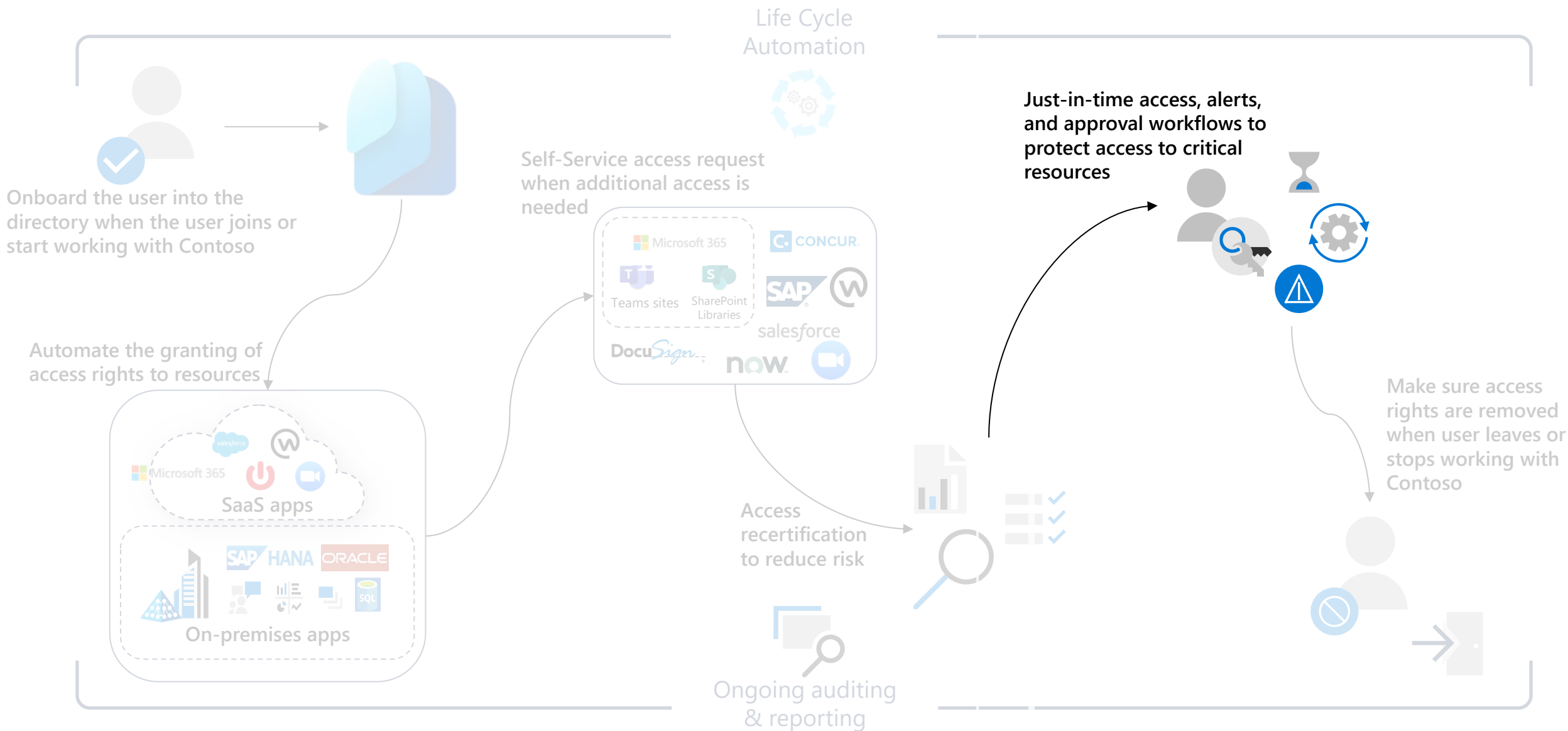
✓ Approve ✕ Deny ? Don't know ↺ Reset decisions 🗒 Accept recommendations

Name ↑	Recommendation	Decision
<input checked="" type="checkbox"/> abhijeet sinha absinh@fimdev.net	Approve Last signed in (Jul 1, 2021) less than 30 days before review began	
<input checked="" type="checkbox"/> Barclay Neira barclayn@fimdev.net	Deny Last sign-in date unknown	
<input checked="" type="checkbox"/> Bhaskar Kamasani vikama@microsoft.com	Deny Last signed in (May 6, 2021) more than 30 days before review began	
<input type="checkbox"/> Bhavesh Patel bpatel@microsoft.com	Approve Last signed in (Jun 30, 2021) less than 30 days before review began	
<input type="checkbox"/> Blake Nelson Blake.Nelson@microsoft.com	Approve Last signed in (Jun 21, 2021) less than 30 days before review began	
<input type="checkbox"/> Bob Grumpy bobgrumpy@fimdev.net	Deny Last signed in (Apr 5, 2021) more than 30 days before review began	
<input type="checkbox"/> Cassie King cassie@fimdev.net	Deny Last signed in (May 8, 2020) more than 30 days before review began	
<input type="checkbox"/> Chris Griffis chgriff@fimdev.net	Deny Last signed in (May 12, 2020) more than 30 days before review began	
<input type="checkbox"/> Chris Wood chrwood@microsoft.com	Deny Last signed in (Nov 19, 2020) more than 30 days before review began	
<input type="checkbox"/> ChrisGreenUAA ChrisGreenUAA@fimdev.net	Deny Last sign-in date unknown	
<input type="checkbox"/> Dalki	Approve	

# Machine Learning based recommendations in Access Reviews



# Contoso's user journey



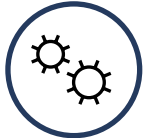



# Implementing least privilege access



## Privileged Identity Management (PIM)

Demo

### Least Privileged Access

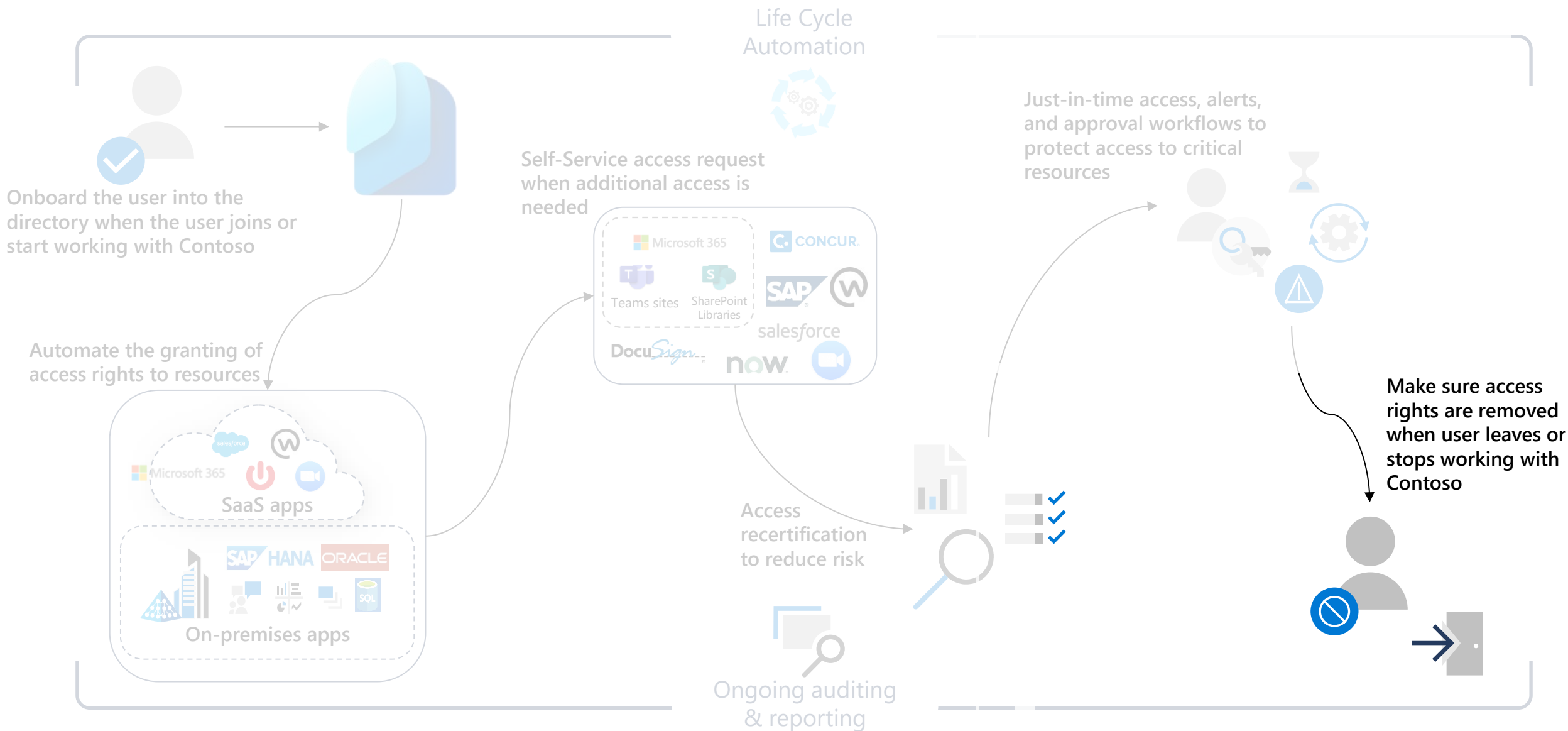
-  On-demand just-in-time administrative access
-  Just enough access with support for roles (built-in and custom) and privileged access groups
-  Approval workflows for privileged activation
-  Audit history of activations and built-in alerts

### Built-in governance controls

-  Periodic access certification for privileged accounts
-  Privileged account discovery and analytics



# Contoso's user journey





# Leaver scenario

## Offboarding users

When team members leave the organization, their personal information must be handled in compliance with regulations and policies.

This puts pressure on IT to ensure that all resource access is removed from the former employee without impacting the organization.

### With Lifecycle Workflows

Using customizable workflow templates for common offboarding tasks ensures timely, reliable, graceful resource access removal for IT, and peace of mind for former team members.



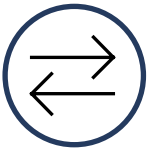
# Removing access



**Reduce risk** by cleaning up accounts that are no longer needed



**Delete** a user from the directory or **block** sign-in



Microsoft Entra provisioning service keeps source and target systems **in sync** and deprovisions accounts that shouldn't have access anymore



**Increase efficiency** and save money (license costs)

Dashboard > Users > Allan Deyoung

Allan Deyoung | Profile

« Edit Reset password Revoke sessions Delete Refresh Got feedback?

Do you want to delete this user?

Yes No

Manage

Profile

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Activity

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

Company name Employee ID

Settings

Block sign in Usage location

Yes United States

Contact info

Street address State or province Country or region Office

N19 W24133 Riverwood Dr., Suite 150 WI United States 24/1106

City ZIP or postal code Office phone Mobile phone

Waukesha 53188 +1 262 555 0106 -- --

Email Alternate email Proxy address View more

AllanD@ninjacat.nl -- -- smtp:AllanD@roodwitteschare.OnMicroso...

Authentication contact info

Use the Authentication methods page to manage authentication contact info for a user

Minors and consent

Learn more about age group and minor consent definitions

Age group Consent provided for minor Legal age group classification

Undefined None Undefined

# Resources

- Microsoft Entra identity blog  
[aka.ms/IdentityBlog](https://aka.ms/IdentityBlog)
- Microsoft Entra product page  
[aka.ms/entra/identitygovernance](https://aka.ms/entra/identitygovernance)
- Microsoft Identity solution page  
[microsoft.com/Identity](https://microsoft.com/Identity)
- Microsoft Entra technical documentation  
[aka.ms/Entra/IDGovDocs](https://aka.ms/Entra/IDGovDocs)
- Try Microsoft Entra ID Governance free  
[aka.ms/EntraIDGovTrial](https://aka.ms/EntraIDGovTrial)



We strive to make the world **a safer place for all.**

**Thank You**

Daniel von Büren

✉ [danvo@microsoft.com](mailto:danvo@microsoft.com)

📱 +41 78 844 68 37

