Microsoft

Best Practices for How to Manage All Your Access from the Cloud:

The Next Frontier in Your Security Journey

Jef Kazimer /in/jefkazimer
Bailey Bercik /in/baileybercik
Product Managers – Microsoft

425Show

Agenda

Destination: Cloud

Security challenges faced in the first cloud era

The next frontier in your security journey

Controls for the complete access lifecycle

Go-Do's

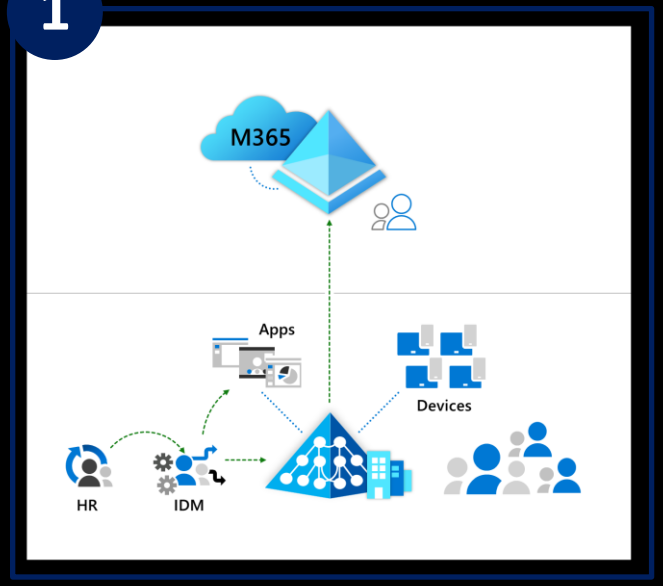
IT Evolution

- Identity
- Resources
- Authentication (AuthN)
- Authorization (AuthZ)

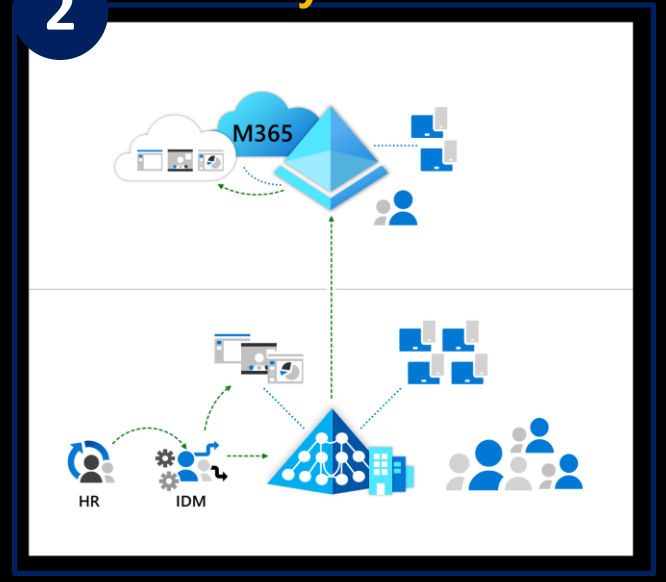
5 States of Transformation

aka.ms/ad2entraid

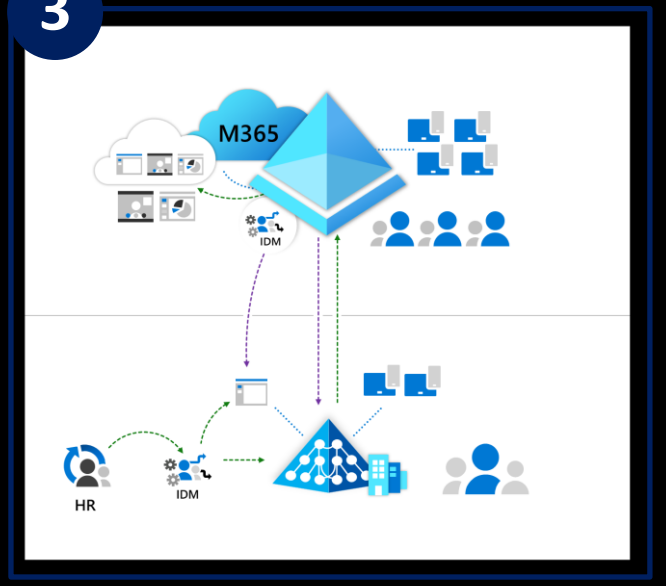
1 Cloud attached



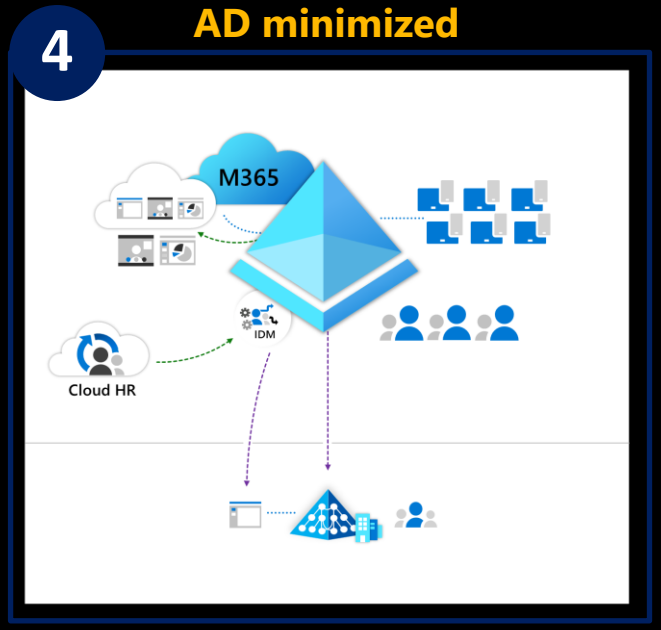
2 Hybrid



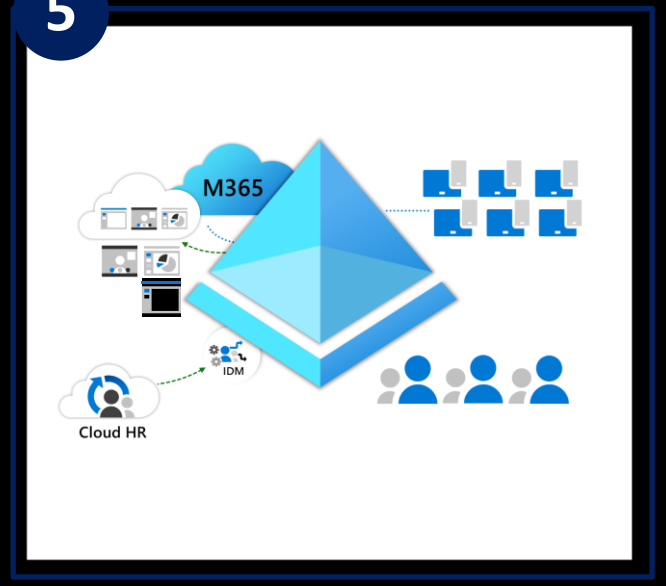
3 Cloud-First



4 AD minimized



5 100% Cloud



Agenda

Destination: Cloud

Security challenges faced in the first cloud era

The next frontier in your security journey

Controls for the complete access lifecycle

Go-Do's

Modernization of Access Security in the Cloud & AI Era

Single Sign On (SSO) to reduce credential friction and increase user experience

Consolidate AuthN Control Plane

Access Management for ensuring access assignments are appropriate, timely, and effective

Secure The Access

Secure The Session

Additional Controls to secure access to assigned resources (MFA, Passwordless, Risk Based, Device identity etc.)

Consolidate the AuthZ Control Plane

Managing the access assignments alongside where you are already managing the authentication

New Capabilities; New Challenges

SAAS Applications

- Shadow IT

External Collaboration

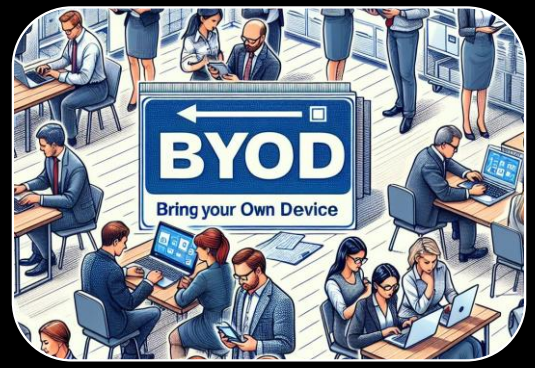
- Data Exfiltration
- Lifecycle

Cloud Infrastructure

- Permission Sprawl

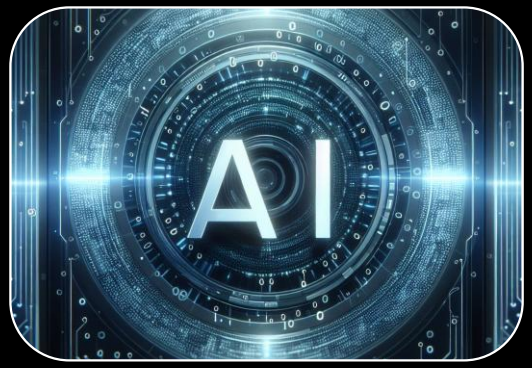
Work From Anywhere

- Attack From Anywhere



BYOD

- Unmanaged Devices



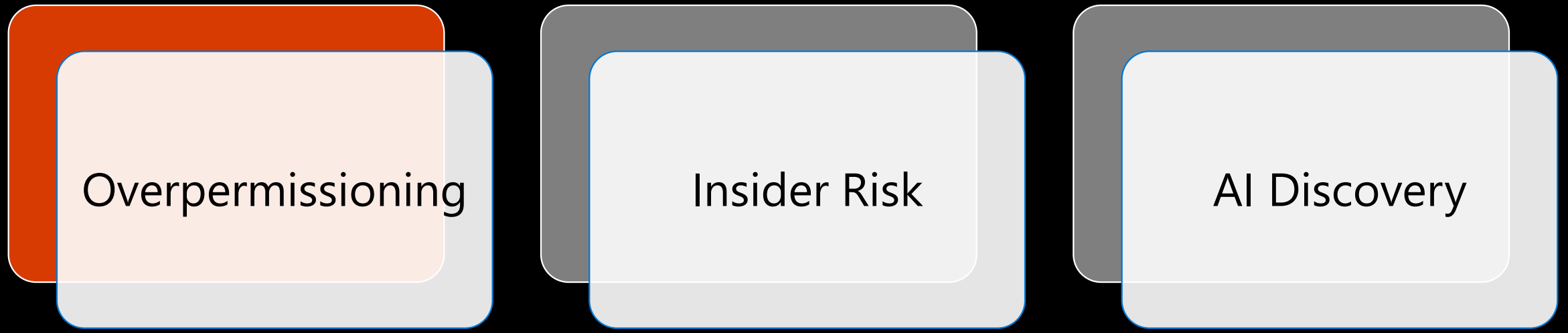
AI

- Shadow Access Discovery

Agenda

Destination: Cloud
Security challenges faced in the first cloud era
The next frontier in your security journey
Controls for the complete access lifecycle
Go-Do's

Post-Authentication Access Management



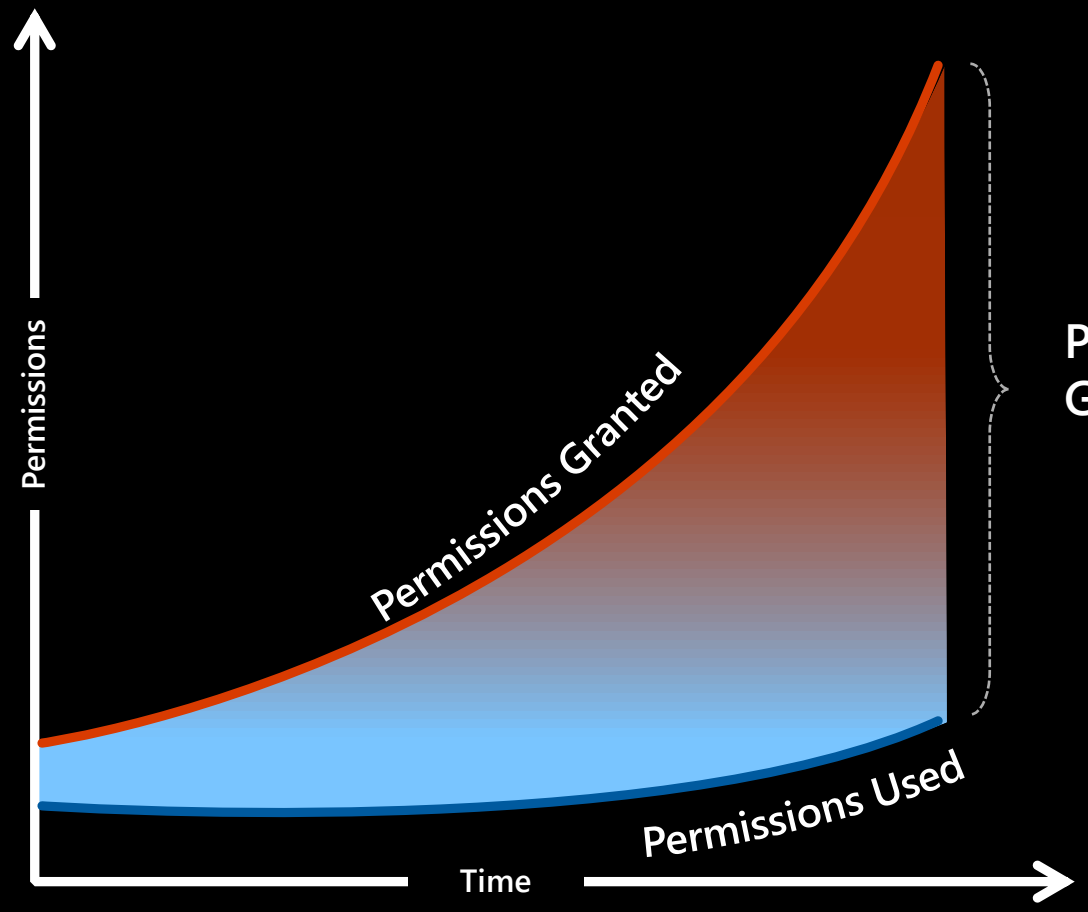
(Multi-)cloud adoption brings new permission challenges

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 the attack surface



Permissions Gap

Lack of comprehensive visibility into identities, permissions and resources

Increased complexity for IAM and security teams to manage permissions across multi-cloud environments

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

CIEM: Cloud Infrastructure Entitlement Management

"The challenge of managing privileges in IaaS is worsening, with thousands of services added in recent years by cloud providers. Security and risk management leaders must combine traditional IAM approaches with CIEM to achieve efficient **identity-first security** management results."

- Gartner

Cloud infrastructure entitlement management (CIEM) offerings are:

- Specialized identity-centric SaaS solutions focused on managing cloud access risk via administration-time controls for the governance of entitlements in **hybrid and multi-cloud** IaaS.
- Typically use analytics, machine learning (ML) and other methods to **detect anomalies** in account entitlements, like **accumulation of privileges**, **dormant and unnecessary entitlements**.
- CIEM ideally provides remediation and enforcement of **least privilege** approaches.

- Gartner

Recommended Actions – Overpermissioning

Find the right stakeholders & be aware of seasonal access

Start with non-human accounts

- Repeatable access patterns/least likely to change
- Super workload identities (serverless functions, apps, etc.)
- Access to crown jewel resources

Human accounts with high privilege move to Just in Time/Just Enough Access (JIT/JEA)

- Not ‘taking away’ permissions, just no standing access...
- Monitor usage, eventually ‘take away’ entirely

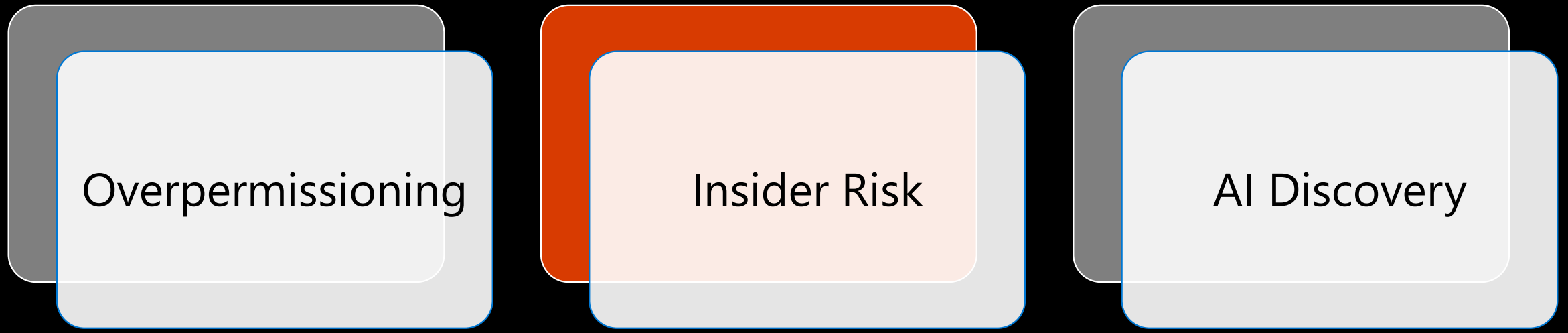
Process changes

- How did we get here? Policy improvements (Owner access is given to ‘their stuff’)
- Show improvement to leadership, repeat/keep going.
- This is going to take a while. Any improvement is good!

More Overpermissioning Guidance

aka.ms/SANS/CIEM

Post-Authentication Access Management



Insider Risk

- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

AutoSave Off | Document1 - Word | Confidential | Alex Wilber

File Home Insert Draw Design Layout References Mailings Review View Help | Comments | Editing | Share

Paste | Clipboard | Font | Paragraph | Styles | Editing | Dictate | Voice | Sensitivity | Add-ins | Editor | Copilot

POLICY TIP Your organization automatically applied the sensitivity: Confidential\Project Obsidian. OK

FAQ for Project Obsidian

A brief guide to the features and benefits of the project

What is Project Obsidian?

Project Obsidian is a platform that allows users to create, share and monetize interactive stories using natural language processing and artificial intelligence. Users can write stories in plain English and the platform will generate rich media content such as images, sounds and animations to enhance the storytelling experience.

Who can use Project Obsidian?

Anyone who loves storytelling and wants to express their creativity can use Project Obsidian. Whether you are a professional writer, a hobbyist, a student, a teacher, or just someone who enjoys reading and writing stories, you can find something for you on Project Obsidian. You can also collaborate with other users and join communities based on your interests and preferences.

How can I get started with Project Obsidian?

To get started with Project Obsidian, you need to create an account on the platform and choose a subscription plan that suits your needs. You can then access the dashboard where you can create new stories, edit existing ones, browse other stories, and manage your profile and settings. You can also use the tutorials and guides available on the platform to learn how to use the features and tools.

What are the benefits of using Project Obsidian?

Project Obsidian offers many benefits for users who want to create and enjoy interactive stories. Some of the benefits are:

- You can write stories in natural language without any coding or technical skills.
- You can use the platform's AI to generate content such as images, sounds and animations based

Page 1 of 2 | 384 of 384 words | Text Predictions: On | Accessibility: Good to go | Focus | 125%

ChatGPT

New chat

Previous 30 Days

Proj. Obsidian: Digitizing Mesopota

Upgrade plan
Get GPT-4, DALL·E, and more

Alex Weber

ChatGPT 3.5

How can I help you today?

Recommend a dish
to impress a date who's a picky eater

Design a database schema
for an online merch store

Give me ideas
about how to plan my New Years resoluti...

Write a message
that goes with a kitten gif for a friend on a...

Message ChatGPT...

ChatGPT can make mistakes. Consider checking important information.

Unintentional Insider Risk

- Putting confidential data into an unapproved AI solution
- Sharing confidential information
  - With internal groups who shouldn’t have access
  - With third parties
- Requesting something unnecessary
  - Access to an artifact
  - Privileged role elevation

Recommended Actions – Insider Risk

Gaining Access

- Leverage controls to prevent user from acquiring unnecessary privileges

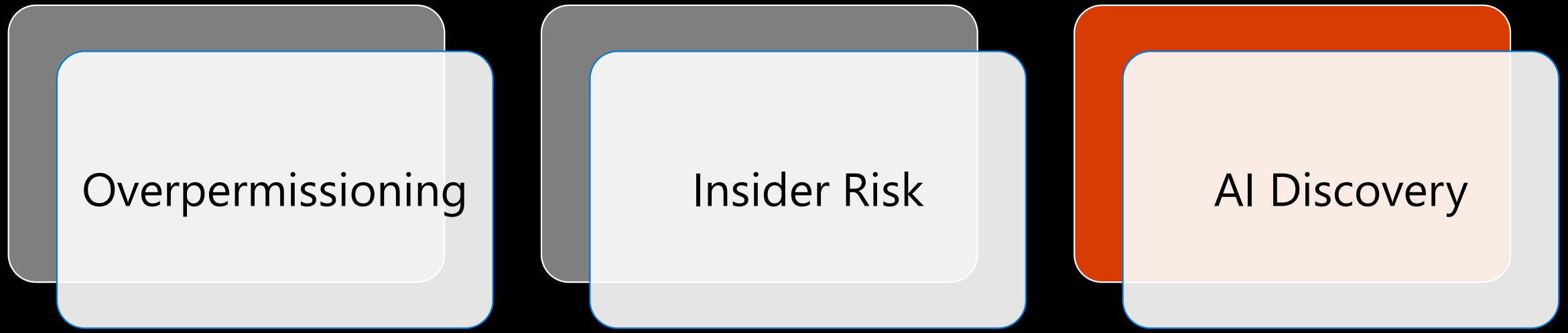
Using Access

- Data Loss Protection (DLP) Labelling
  - Properly classify and label data based on sensitivity
  - Restrict user access to confidential information
- Data Isolation Capabilities
  - Restrict collaboration of users and groups to avoid conflicts of interest

Revoking Access

- Regularly review user access and privileges
- Apply additional preventative actions when insider risk is detected

Post-Authentication Access Management



AI Discovery

Users

AI empowers users to find resources they have access to efficiently

Bad Actors

AI empowers bad actors to see full sprawl of user access and target resources efficiently

Unintentional AI Discovery

- User unintentionally discovering content not intended for them
- Examples:
  - Confidential projects and product launches
  - Mergers and acquisitions
  - Personally Identifiable Information (PII) or other sensitive data
- Caused by
  - Lingering or excessive access
  - Improper DLP labelling
  - Lack of data isolation

Project Obsidian Secret Access Key

Samples:

string AmazonWebServicesSecretToken = "abcdefghijklmnopqrst0123456789/+ABCDEFGH";

Help Link:

https://docs.aws.amazon.com/toolkit-for-eclipse/v1/user-guide/setup-credentials.html

https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys

---

Cs

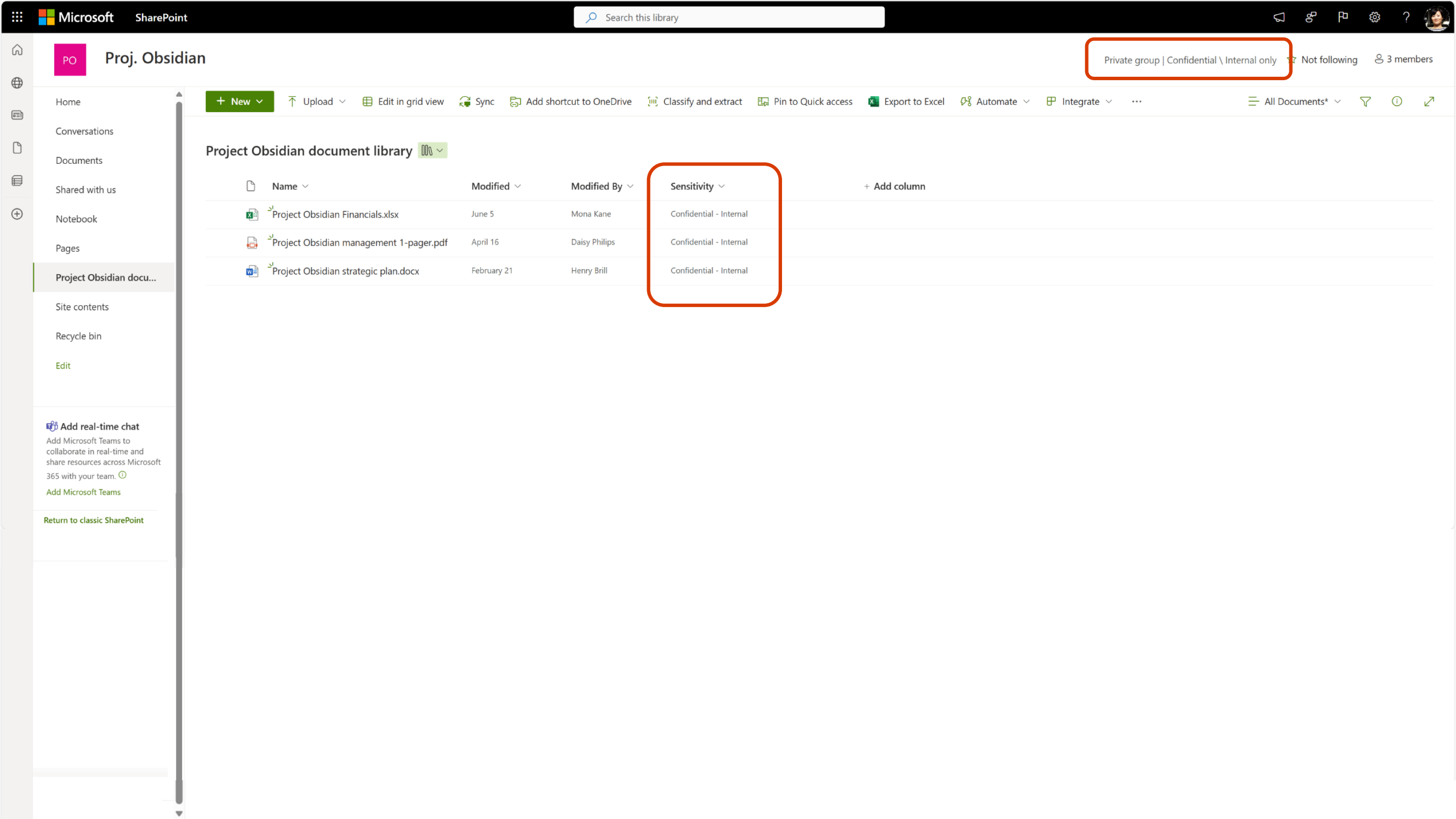
Communication site

TestLabelPublish

Documents

Name	Modified	Modified By	Sensitivity	+ Add column
348-295-SchoolImmReqforParents2019-20...	June 7	Admin Admin	Highly Confidential \ High	
348-295-SchoolImmReqforParents2019-20...	July 18	Admin Admin		
351.pdf	Tuesday at 9:06 AM	Admin Admin		
CC 1000 Employee Records2.xlsx	Tuesday at 9:54 AM	Admin Admin	Confidential	
Project Obsidian	Sunday at 10:41 PM	Admin Admin	Highly Confidential \ High	
ContosoNoLabelUploadTest.pdf	July 4	Admin Admin	Gen	
DATALOSS_WARNING_README.txt	June 28	Shyam		
Document.docx	Tuesday at 3:17 AM	Admin Admin	Confidential	
Document1.docx	5 days ago	Admin Admin	Confidential	
Document10.docx	December 20, 2021	Admin Admin	Label which requires MFA	
Document11.docx	April 17	Admin Admin	Highly Confidential \ High	
Document12.docx	May 9	Admin Admin	General	

This file has been automatically labelled


Microsoft
SharePoint
Search this library
PO
Proj. Obsidian
Private group | Confidential \ Internal only
Not following
3 members
Home
Conversations
Documents
Shared with us
Notebook
Pages
Project Obsidian docu...
Site contents
Recycle bin
Edit
Add real-time chat
Add Microsoft Teams to collaborate in real-time and share resources across Microsoft 365 with your team.
Add Microsoft Teams
Return to classic SharePoint
New
Upload
Edit in grid view
Sync
Add shortcut to OneDrive
Classify and extract
Pin to Quick access
Export to Excel
Automate
Integrate
All Documents*
Project Obsidian document library
Name
Modified
Modified By
Sensitivity
Add column
Project Obsidian Financials.xlsx
June 5
Mona Kane
Confidential - Internal
Project Obsidian management 1-pager.pdf
April 16
Daisy Philips
Confidential - Internal
Project Obsidian strategic plan.docx
February 21
Henry Brill
Confidential - Internal

Home
Create
My Content
Feed
Apps
M365 Chat
Outlook
Teams
Word
Excel
PowerPoint

M365 Chat
what is Project Obsidian about...

New chat ···

Copilot chats and more

November 8, 2023 at 02:42 PM

what is Project Obsidian about?

I'm sorry, but I couldn't find any specific information about Project Obsidian in my search results. Could you provide more context or details about the project so I can better assist you?

Copy

1/30 AI-generated content may be incorrect

Who is the project lead? | What is the goal of the project? | Can you help me with something else?

Ask a work question or use / to reference people, files, and more

Recommended Actions – AI Discovery

Identify Sprawl

- Use AI tools to see the full sprawl of user permissions
- Get to least privilege

Determine Correct Level of Access

- Leverage authoritative data about account holders to determine access
- aka.ms/SecOpsUserAccounts and aka.ms/SecOpsPrivAccounts

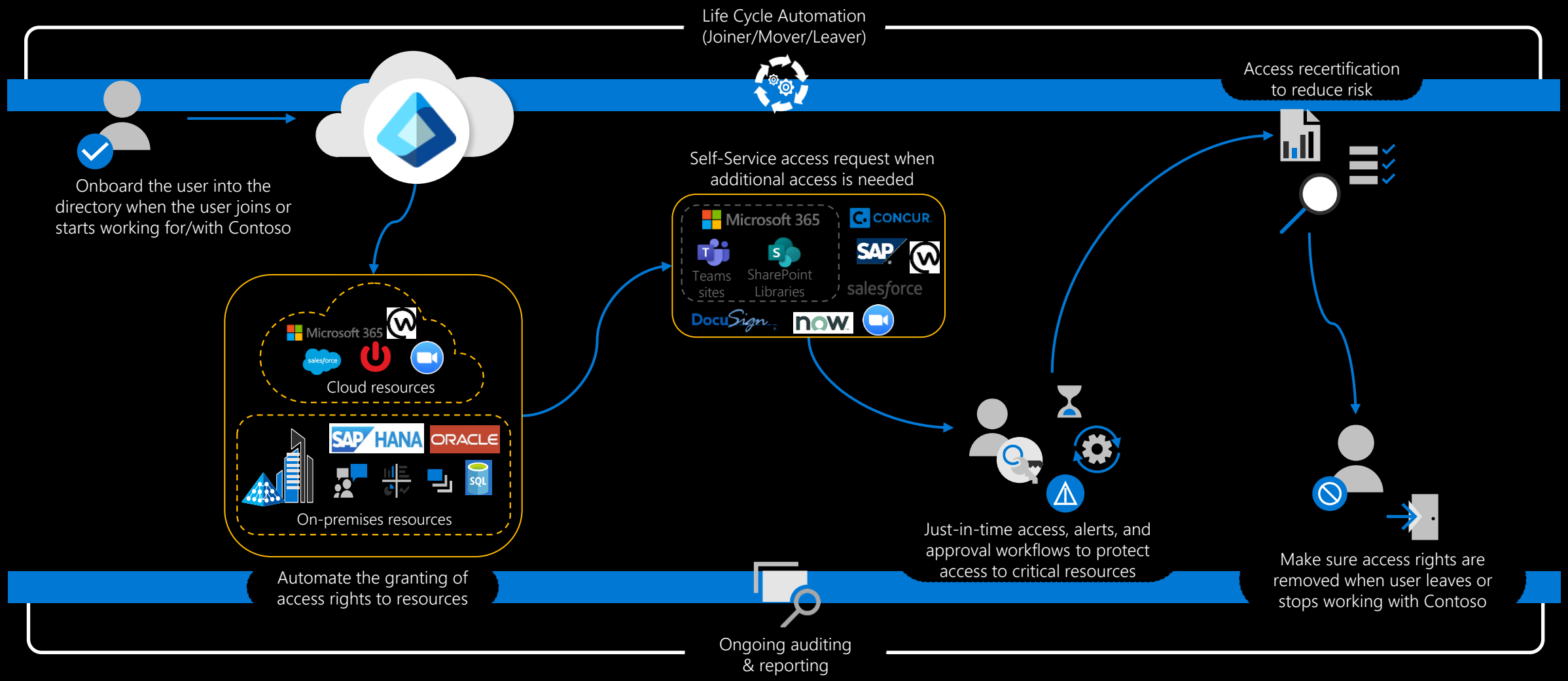
Maintenance

- Regularly review existing access
- Challenge lingering accounts
- Flag atypical actions

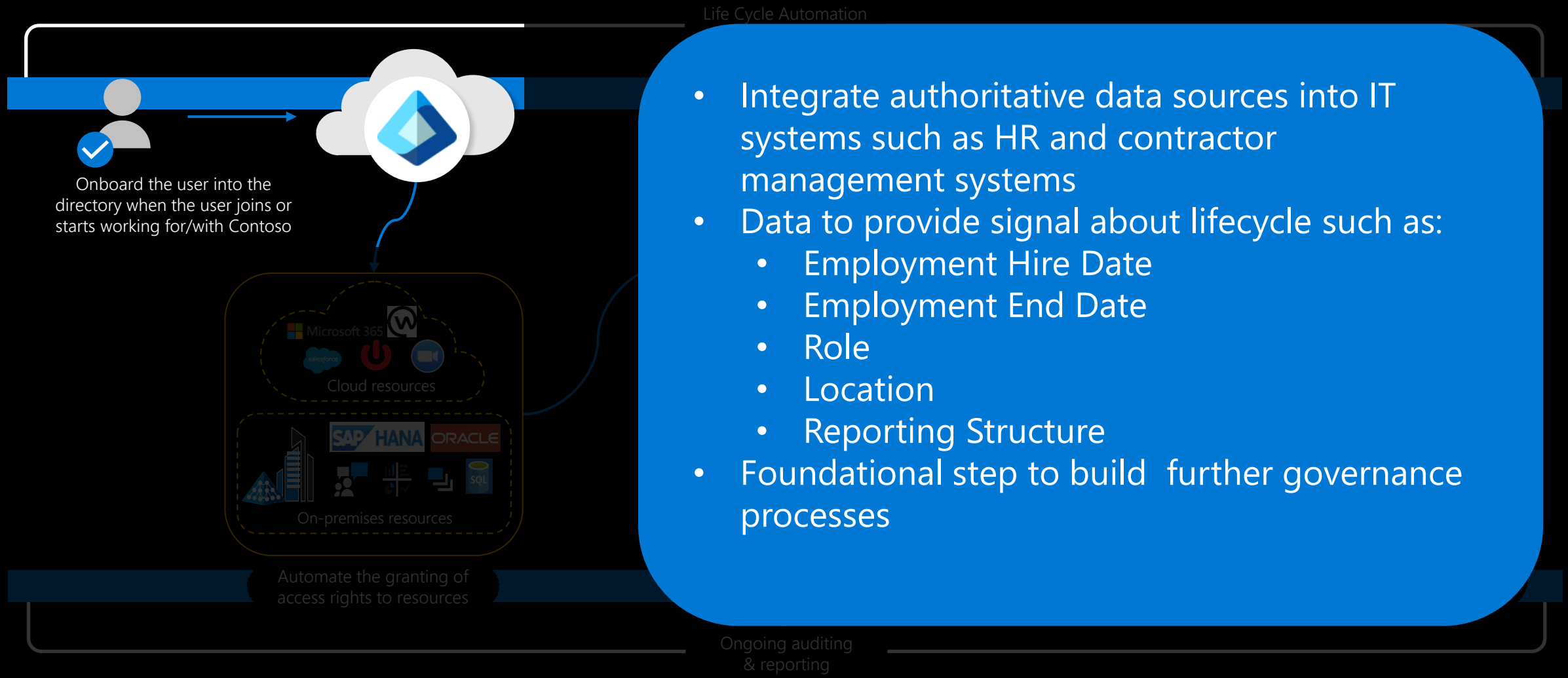
Agenda

Destination: Cloud
Security challenges faced in the first cloud era
The next frontier in your security journey
Controls for the complete access lifecycle
Go-Do's

Govern access to your resources

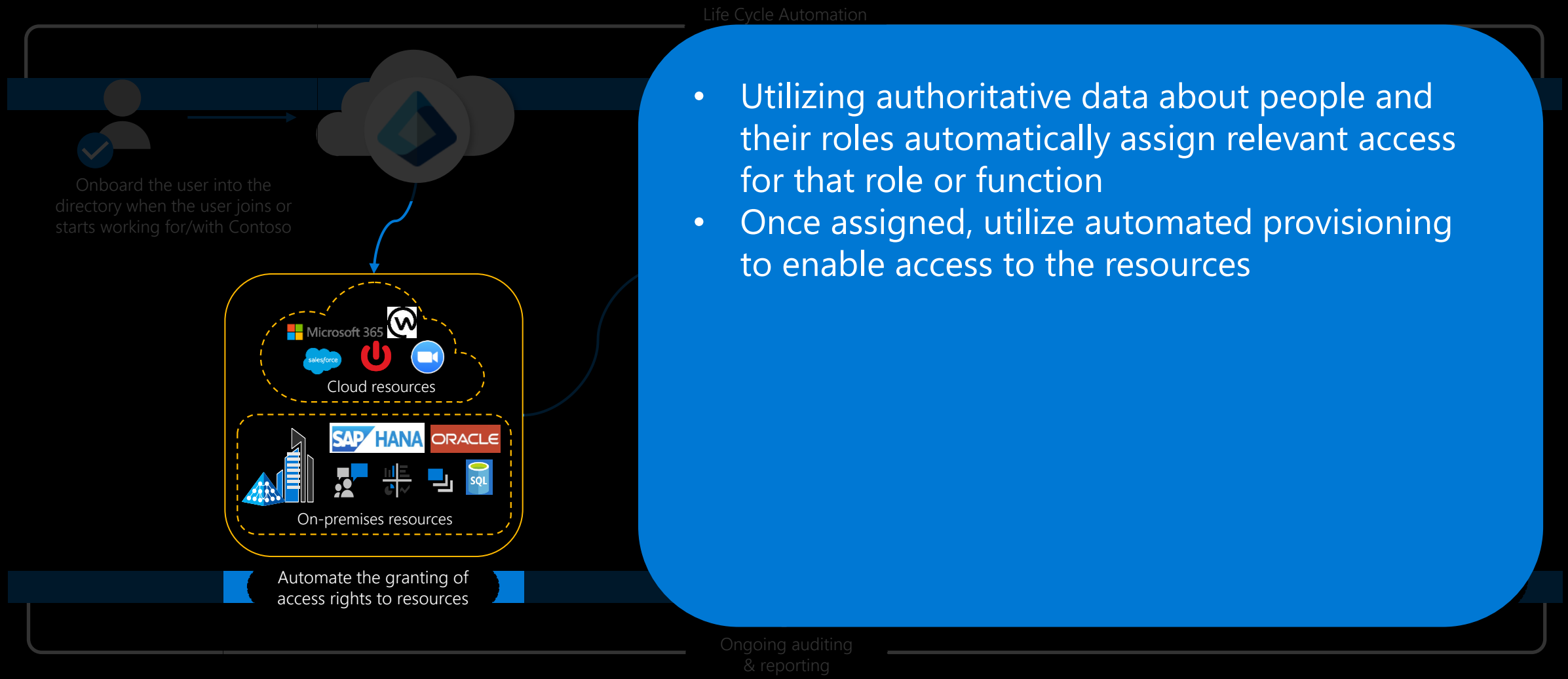


Govern access to your resources



- Integrate authoritative data sources into IT systems such as HR and contractor management systems
- Data to provide signal about lifecycle such as:
  - Employment Hire Date
  - Employment End Date
  - Role
  - Location
  - Reporting Structure
- Foundational step to build further governance processes

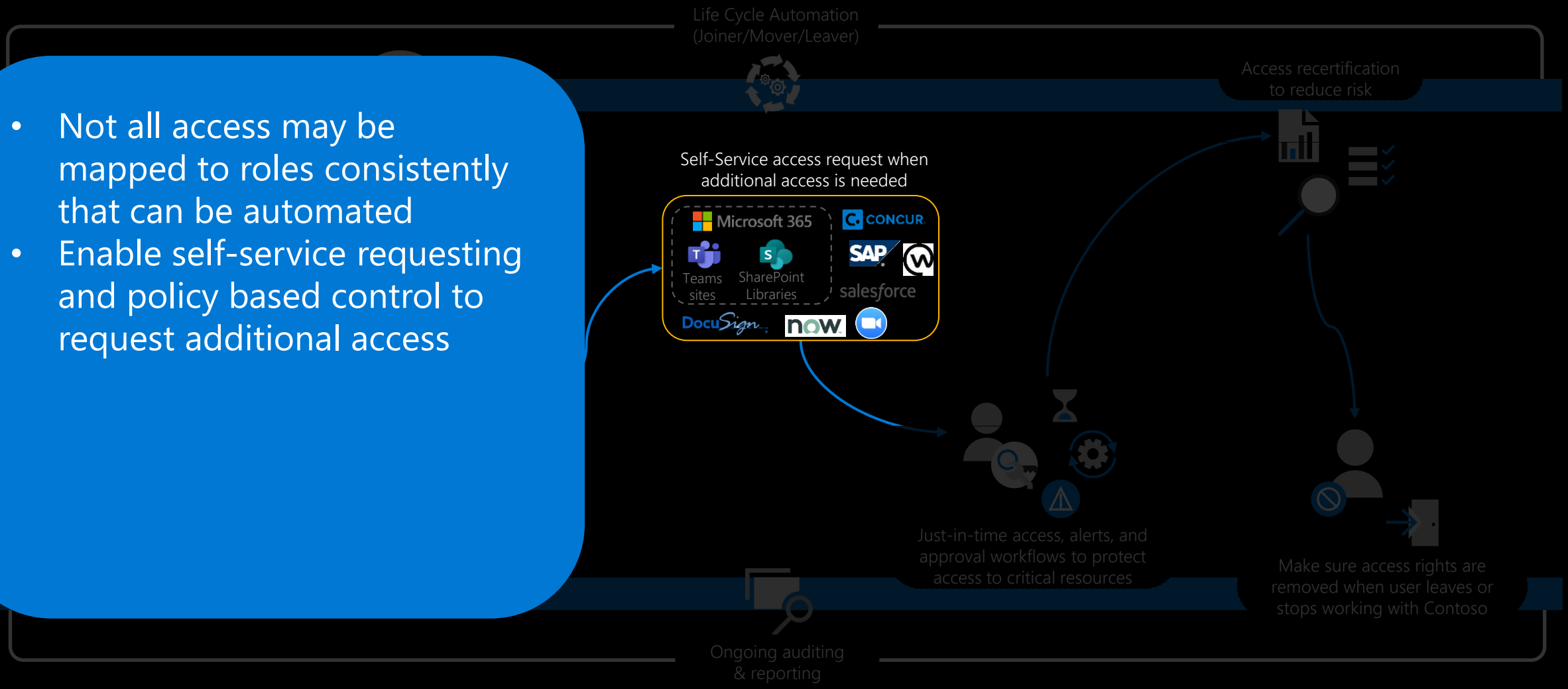
Govern access to your resources



- Utilizing authoritative data about people and their roles automatically assign relevant access for that role or function
- Once assigned, utilize automated provisioning to enable access to the resources

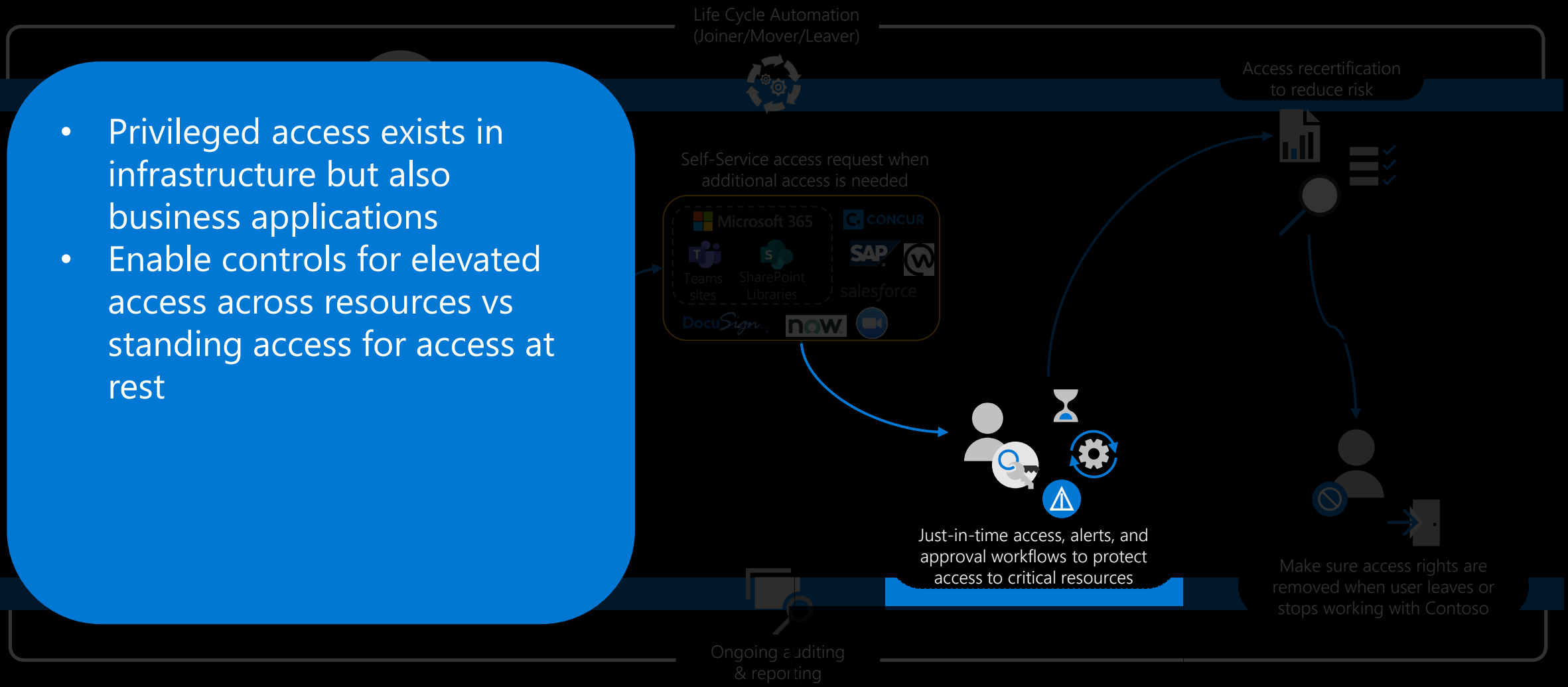
Govern access to your resources

- Not all access may be mapped to roles consistently that can be automated
- Enable self-service requesting and policy based control to request additional access



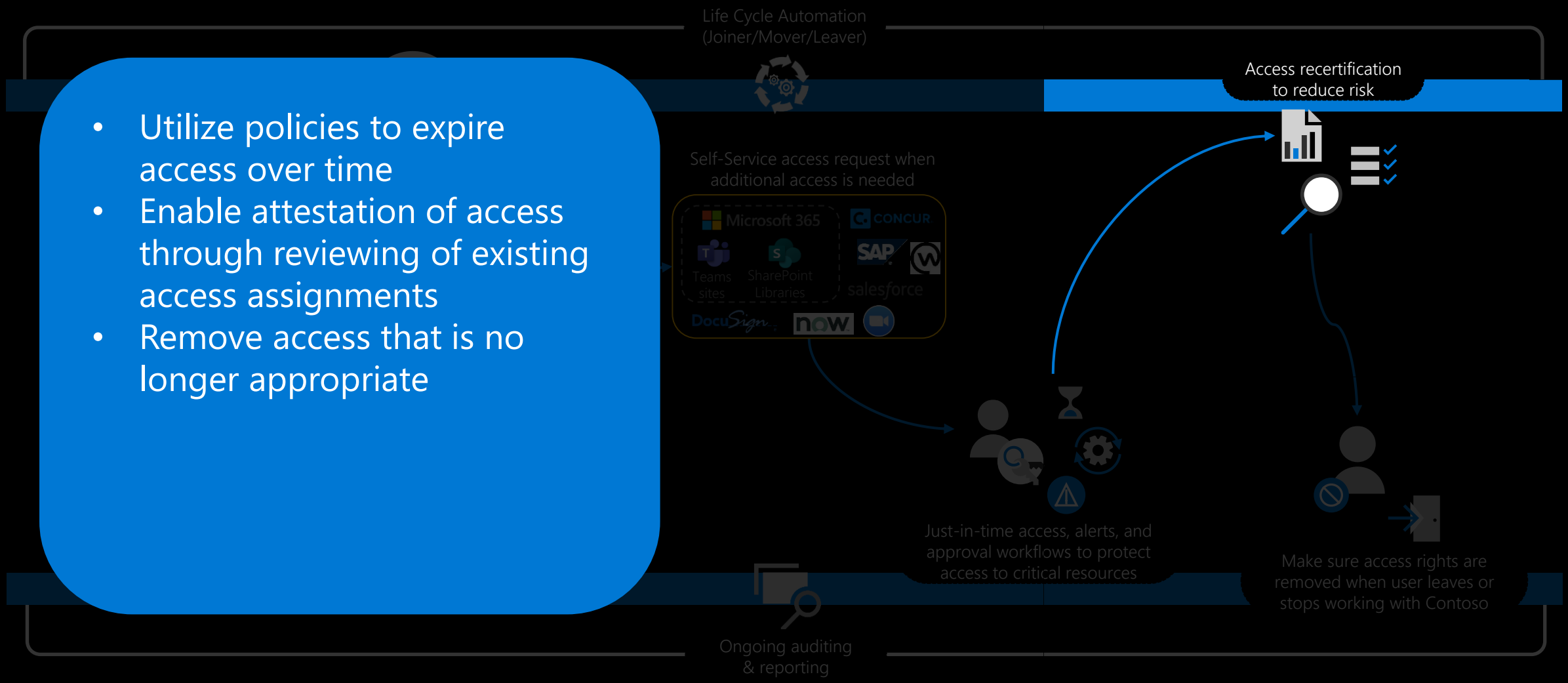
Govern access to your resources

- Privileged access exists in infrastructure but also business applications
- Enable controls for elevated access across resources vs standing access for access at rest



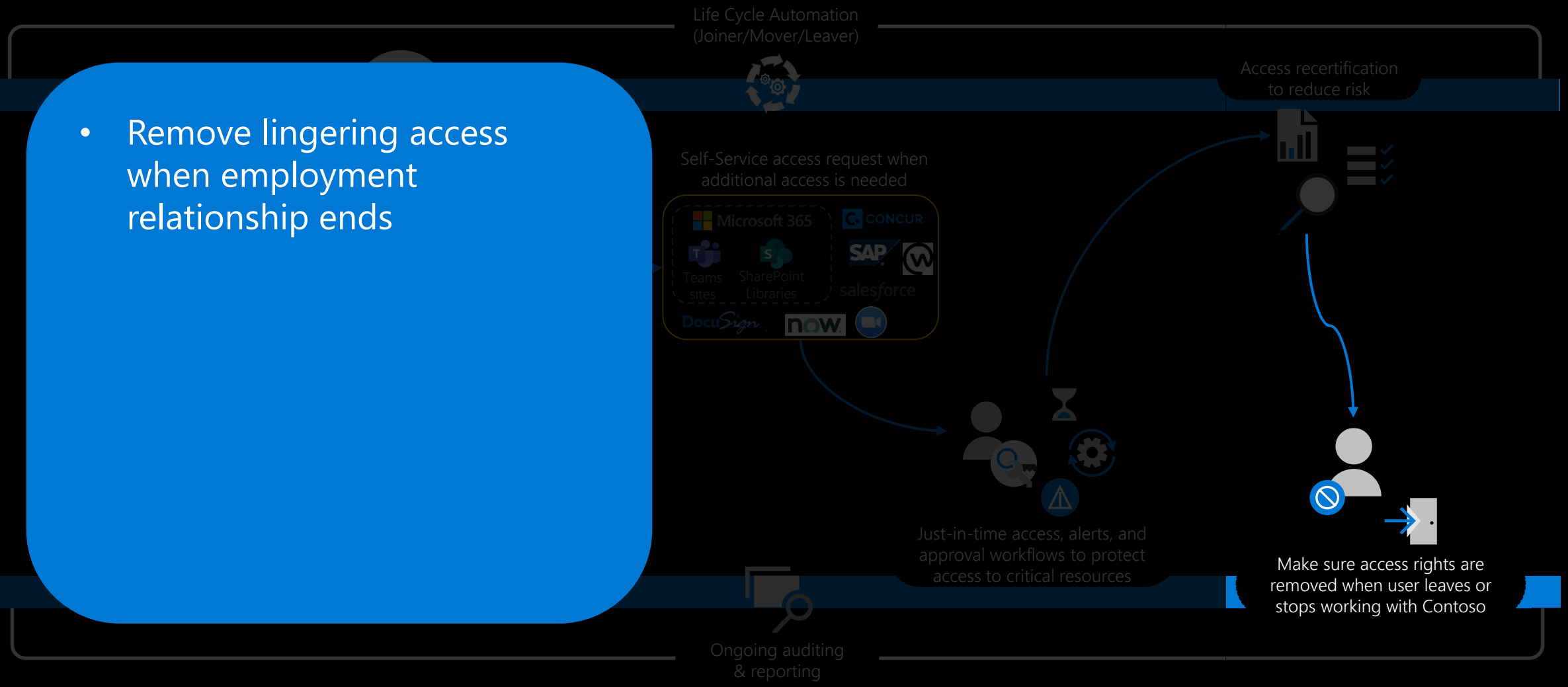
Govern access to your resources

- Utilize policies to expire access over time
- Enable attestation of access through reviewing of existing access assignments
- Remove access that is no longer appropriate



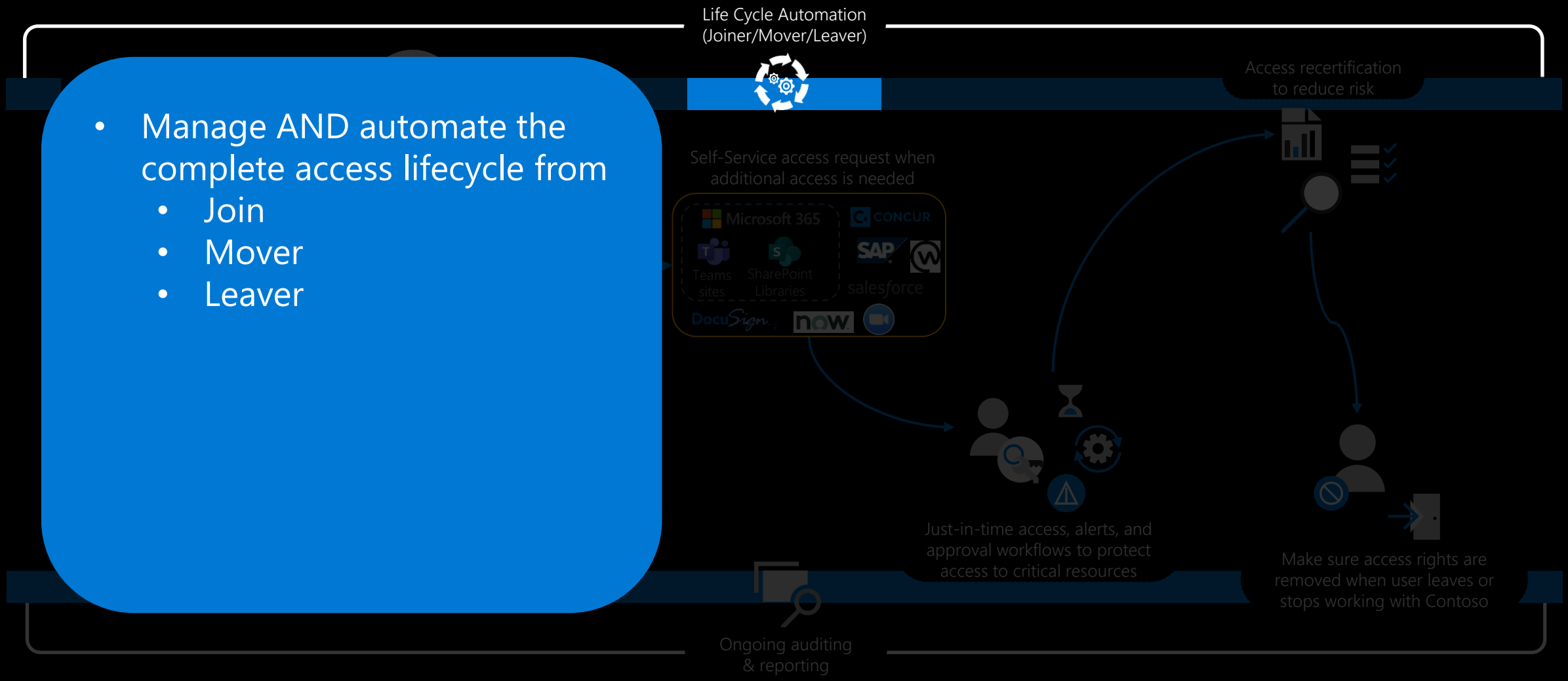
Govern access to your resources

- Remove lingering access when employment relationship ends



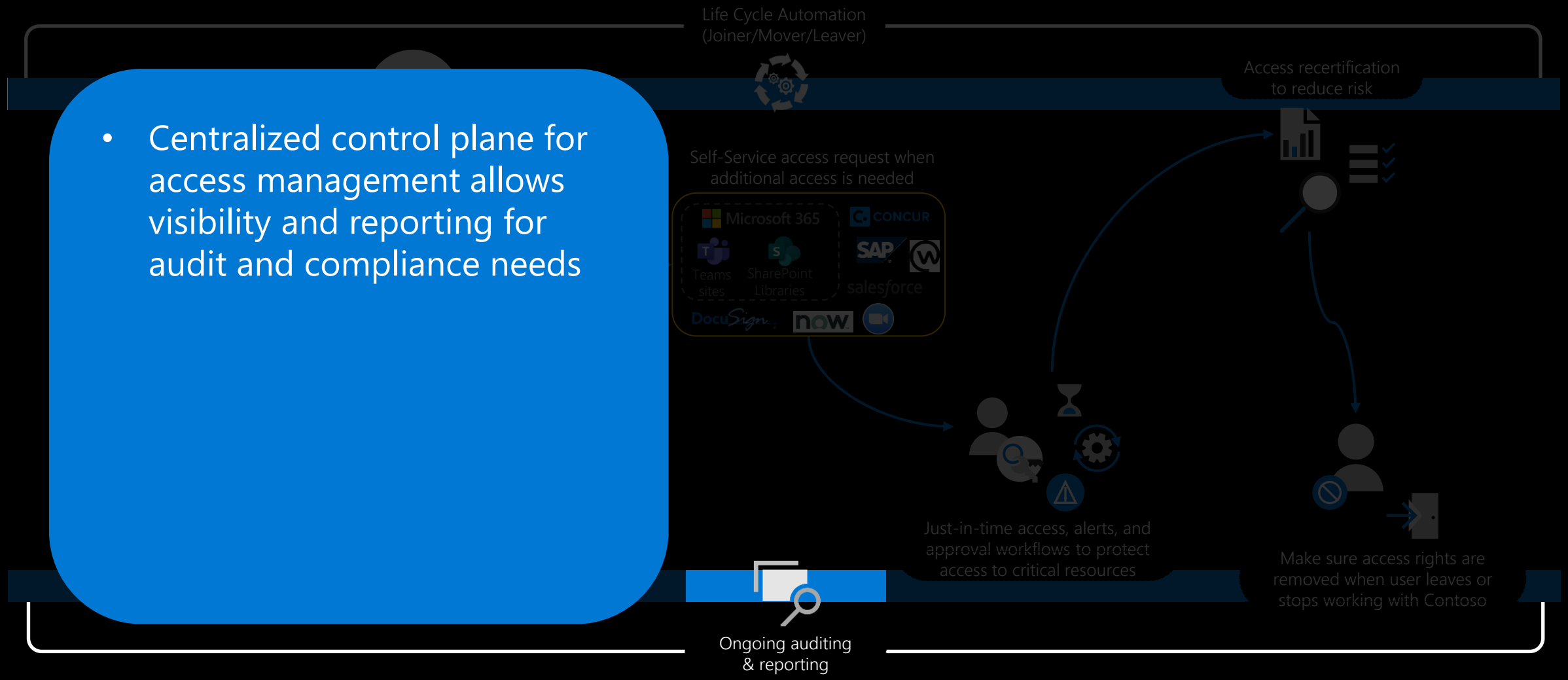
Govern access to your resources

- Manage AND automate the complete access lifecycle from
  - Join
  - Mover
  - Leaver

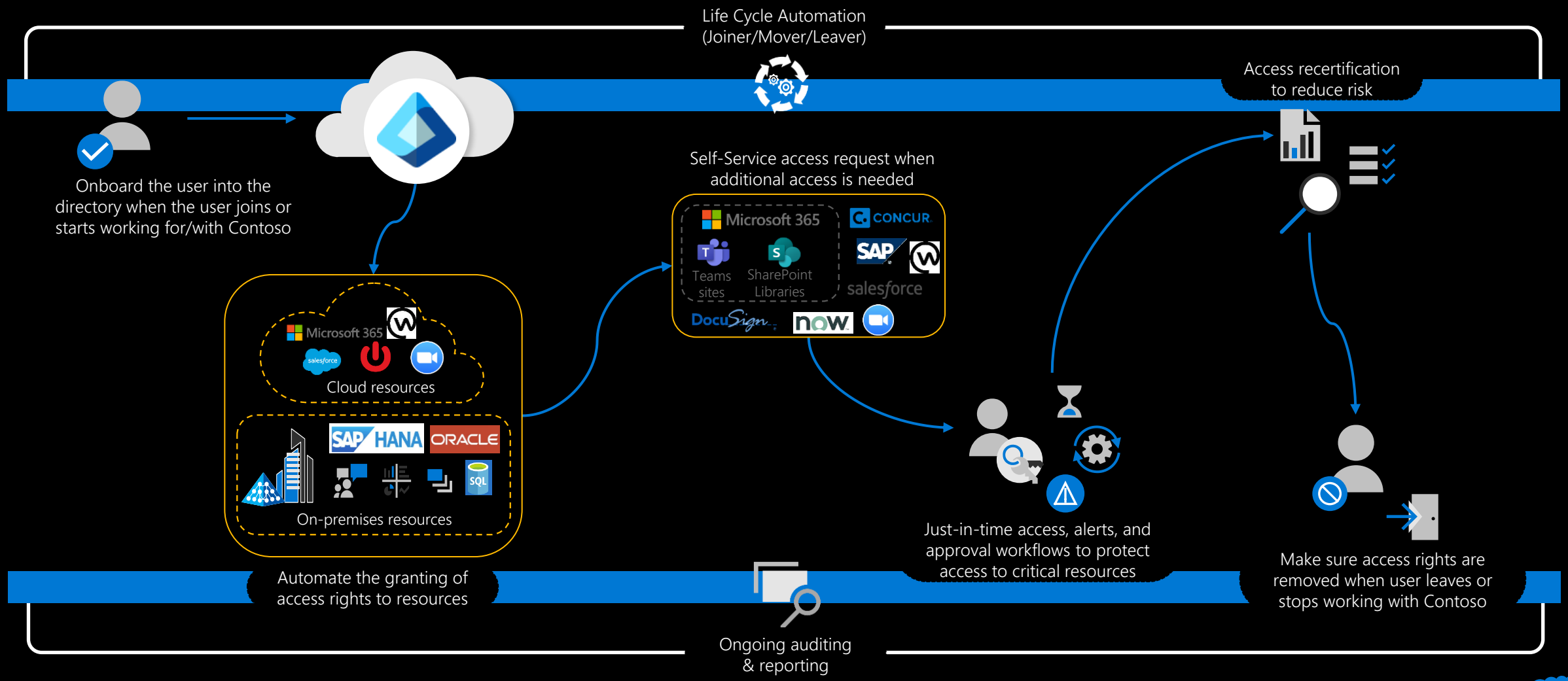


Govern access to your resources

- Centralized control plane for access management allows visibility and reporting for audit and compliance needs



Govern access to your resources



Agenda

Destination: Cloud
Security challenges faced in the first cloud era
The next frontier in your security journey
Controls for the complete access lifecycle
Go-Do's

Go-Do's

- Continuously monitor and cleanup overpermissioned users
- Leverage DLP and data isolation technologies to reduce insider risk
- Use AI tools to see full sprawl of user access
- Review and automate lifecycle processes for employees
  - And don't forget external partners!
- Having good identity governance is key to defending against AI discovery-based attacks
  - Right access for the right user at the right time
- Get this full deck at aka.ms/SANSDeck2024