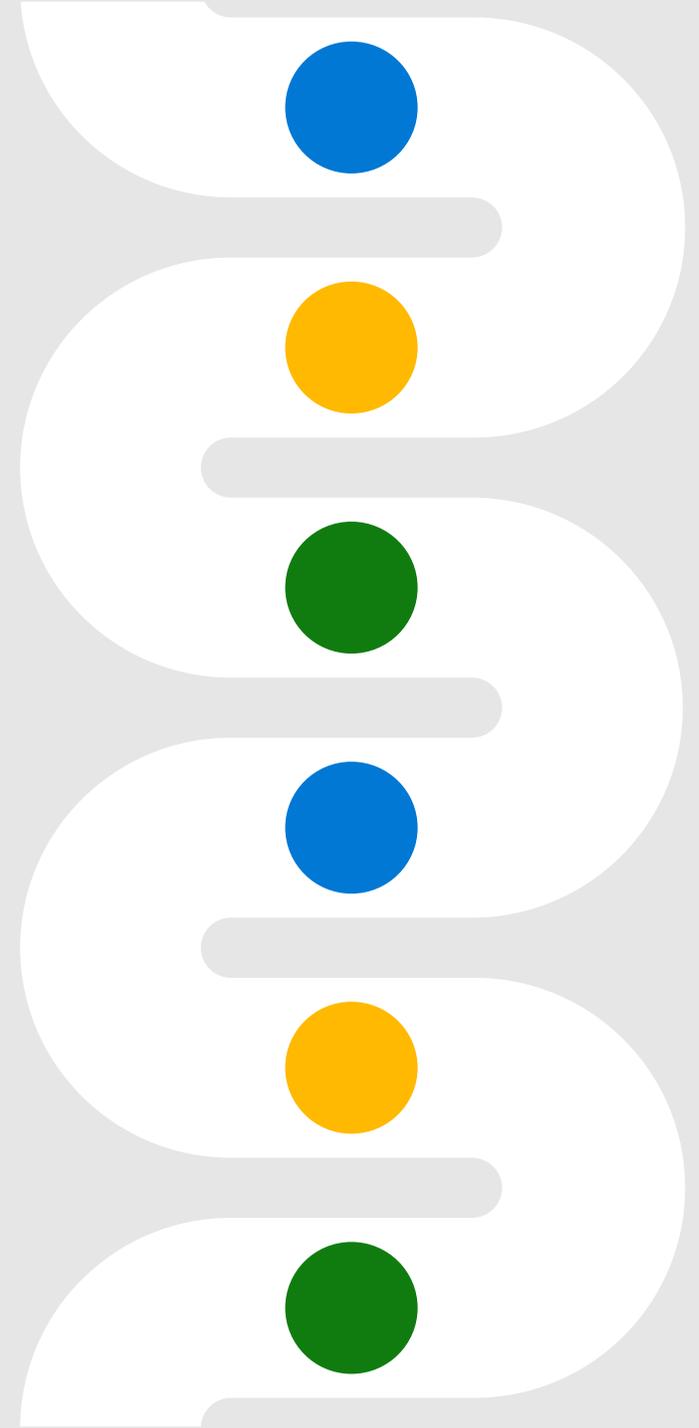


Microsoft Entra Permissions Management (EPM)

Angelica Faber



Overall Agenda



- Entra Permissions Management Overview
- Architecture
- Demo
- Trial and Pricing.

Multicloud adoption brings new permission challenges



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



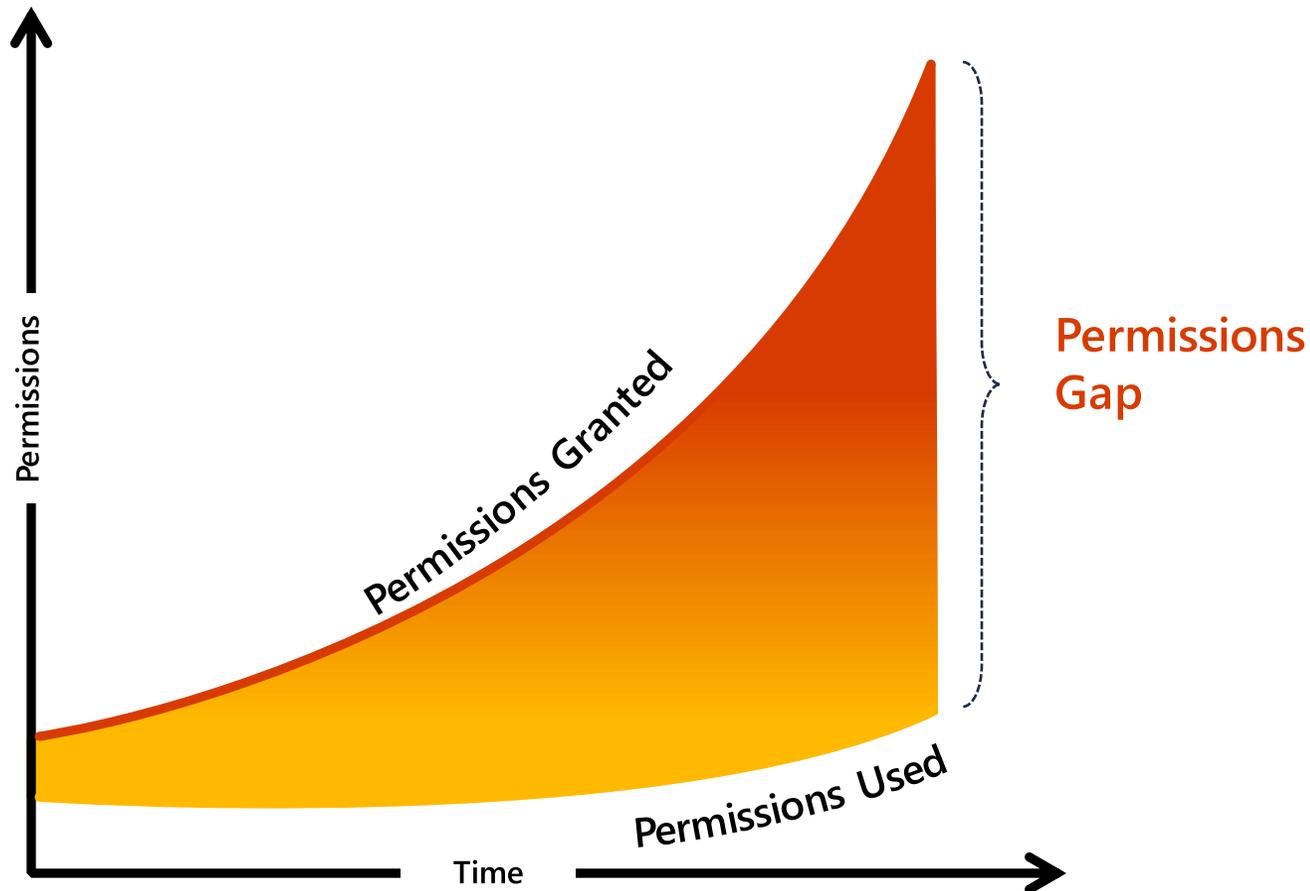
>90% of identities are using **<5% of permissions** granted



>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Today's static, outdated approach

~~Grants permissions based on job roles and responsibilities~~



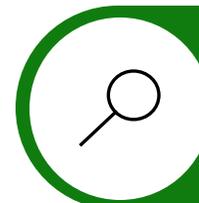
Grants permissions based on historical usage and activity

~~IAM admins manually grant permissions which are not time-bound~~



Allow temporary access to high-risk permissions on-demand

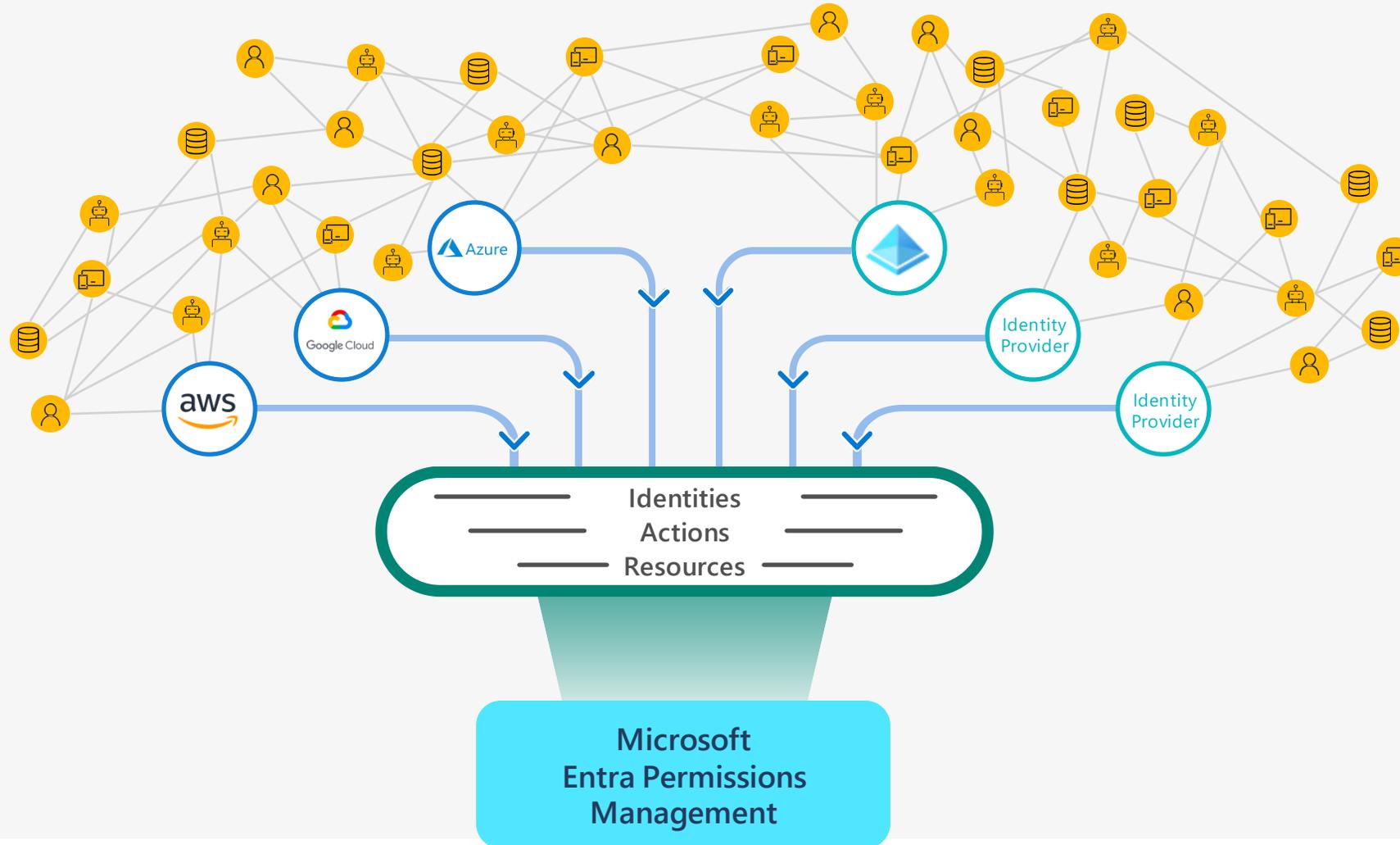
~~Permission clean-up is done manually on an as-need basis~~



Continuously monitor and right-size identities to prevent privilege creep

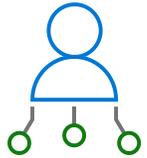
Microsoft Entra Permissions Management (CIEM)

Manage permissions based on historical usage and activities



Microsoft Entra Permissions Management

Improve your security posture by ensuring least privilege across your multicloud infrastructure



Discover

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



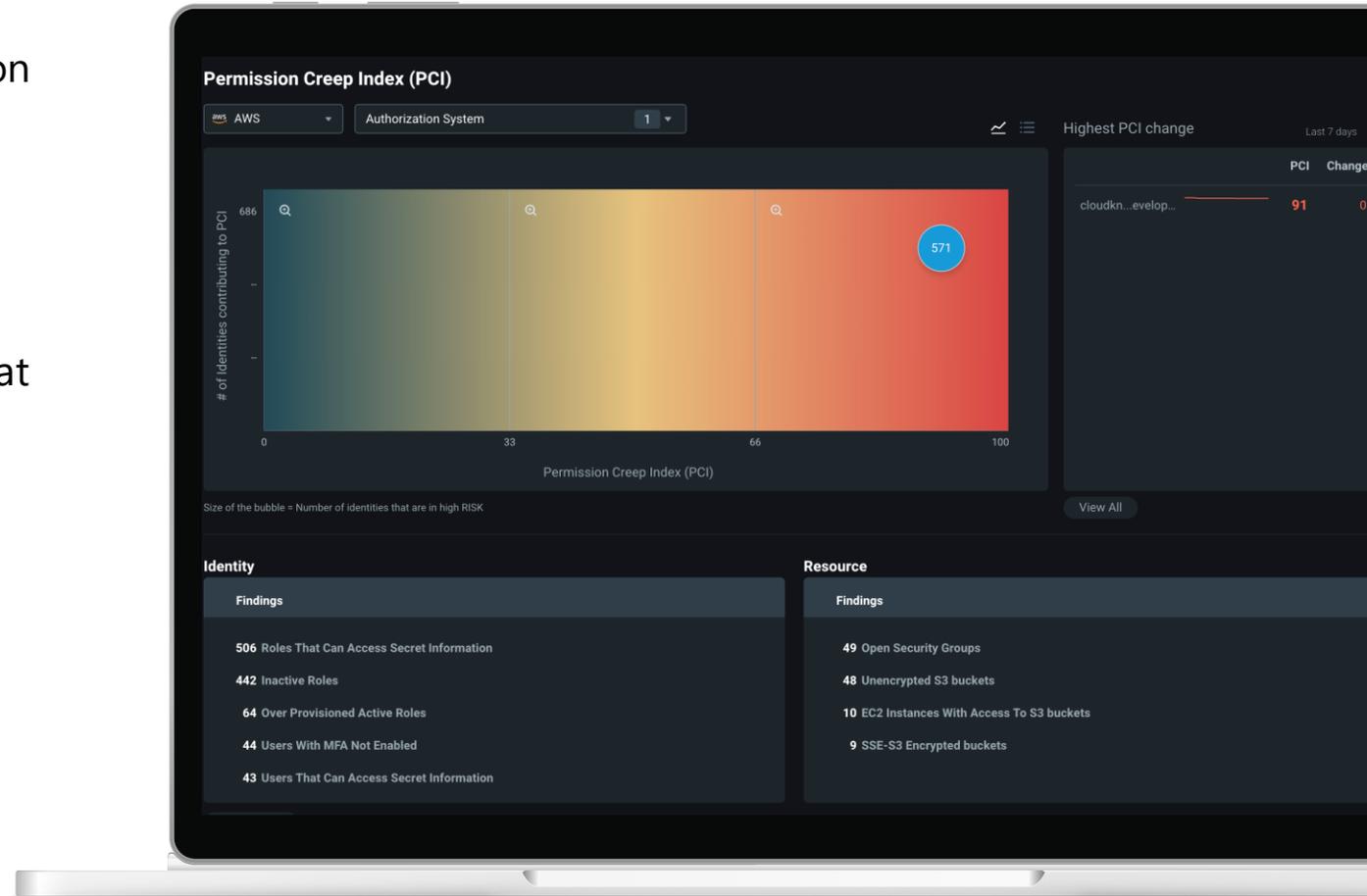
Remediate

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

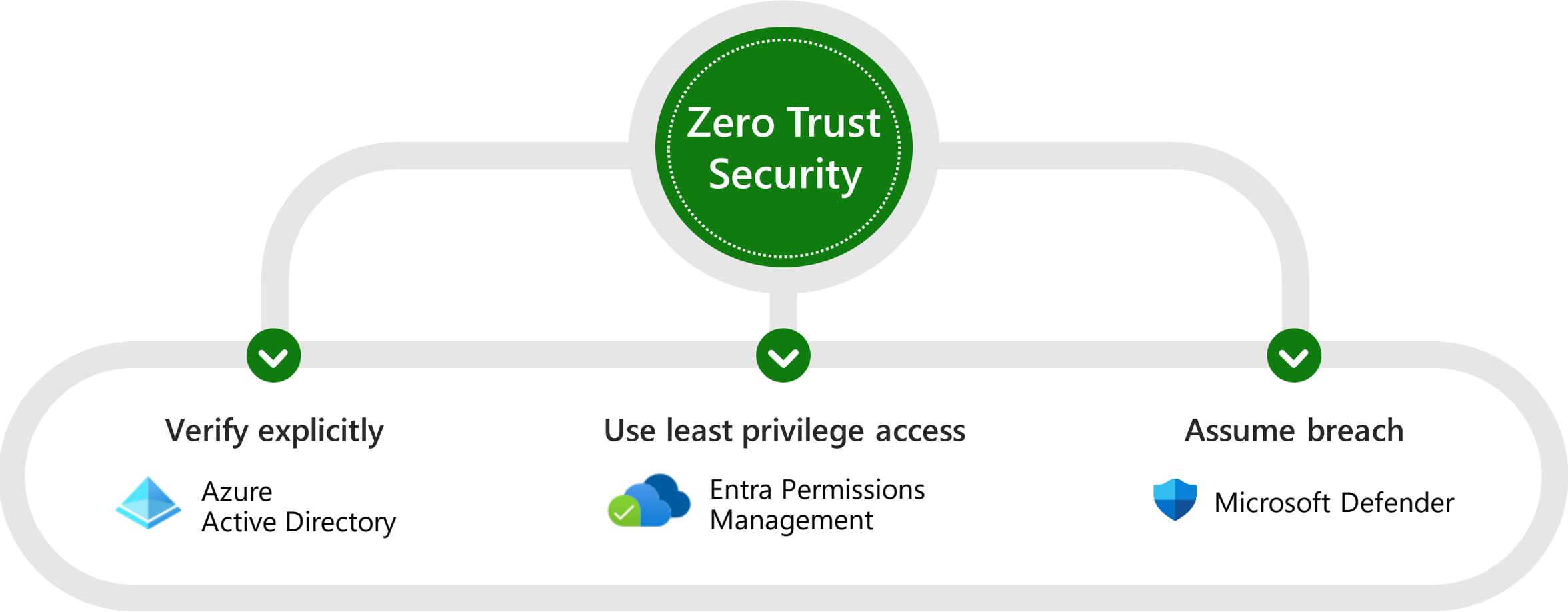


Monitor

Detect anomalous permission usage and generate detailed forensic reports.

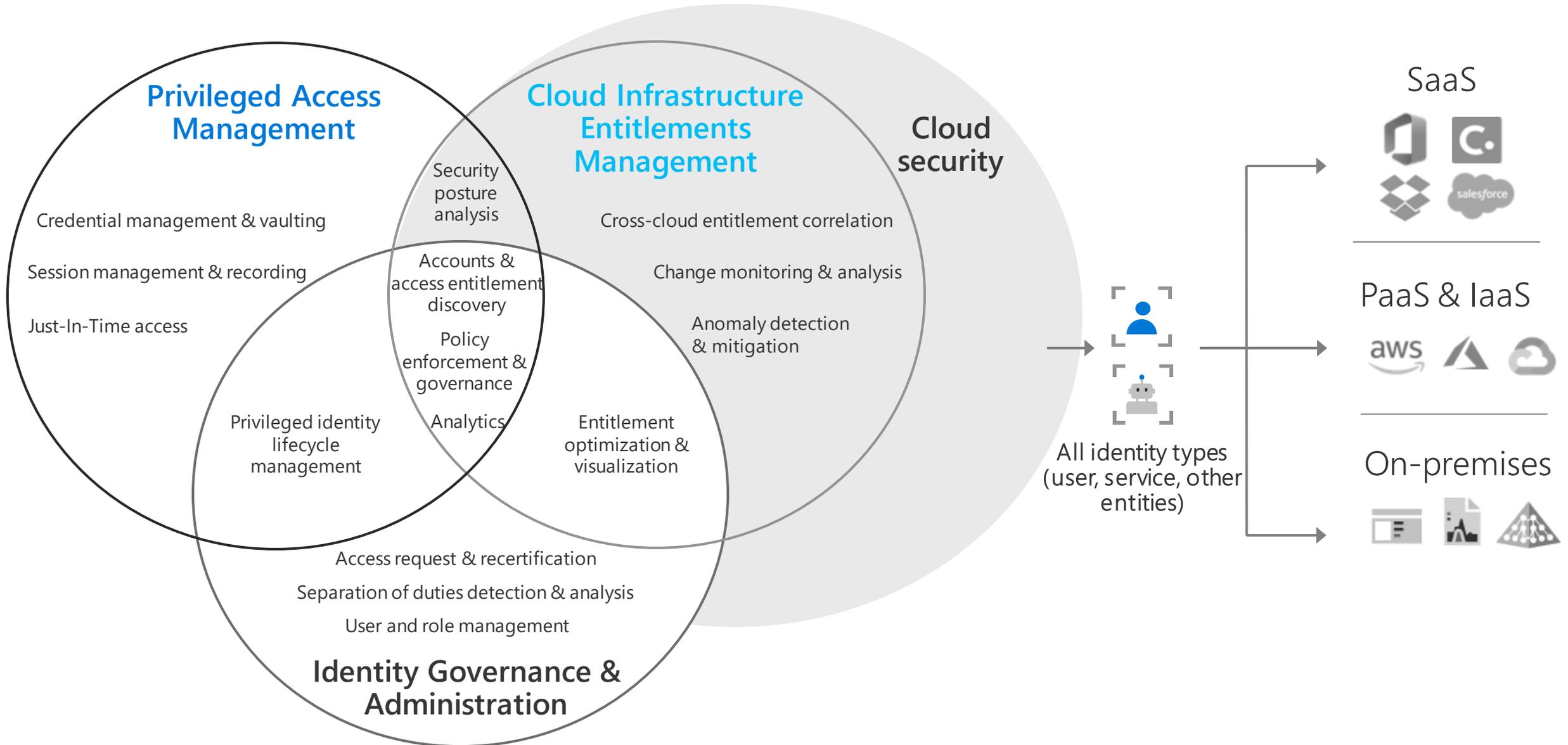


Entra Permissions Management empowers Zero Trust

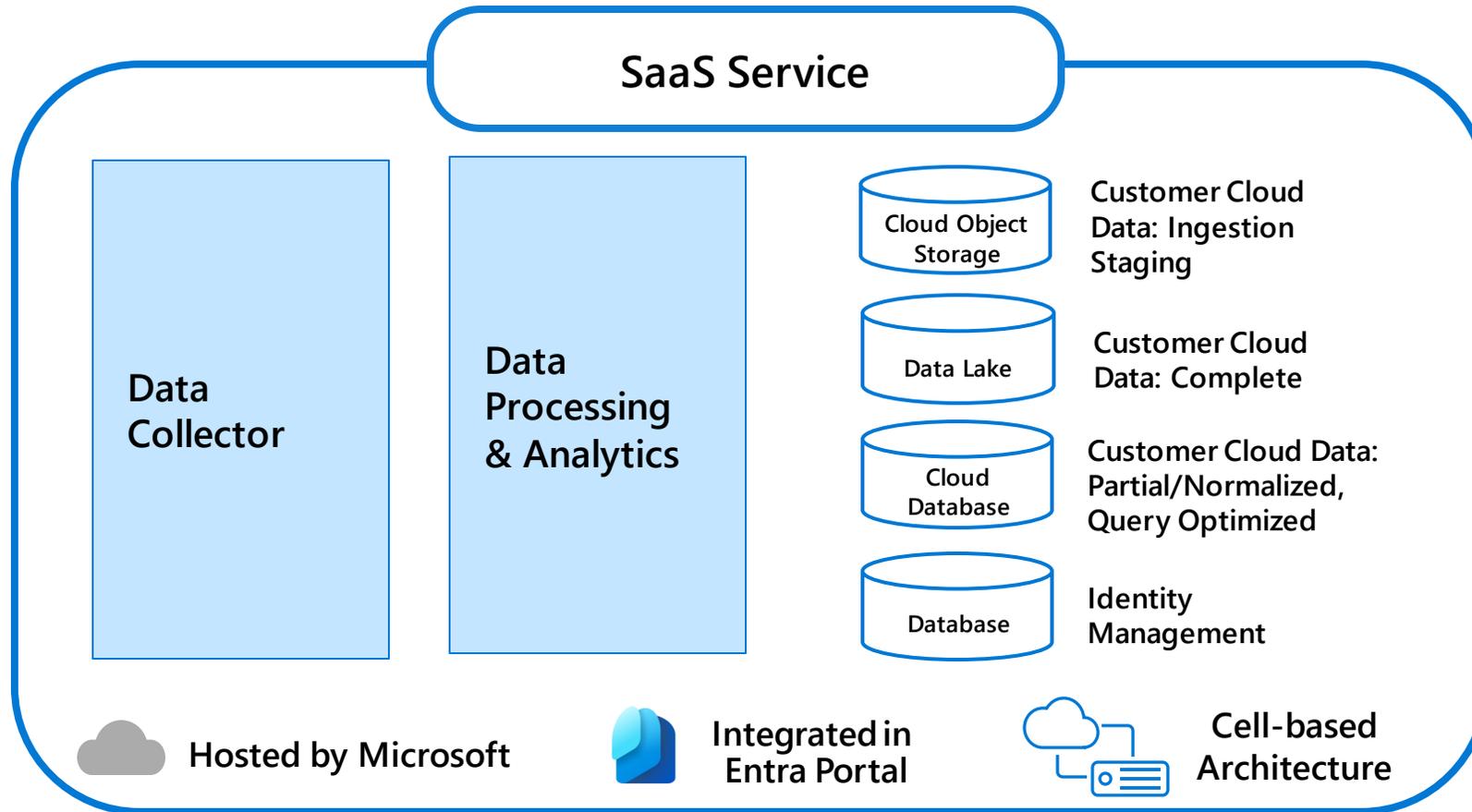


Multicloud | Multi-Platform

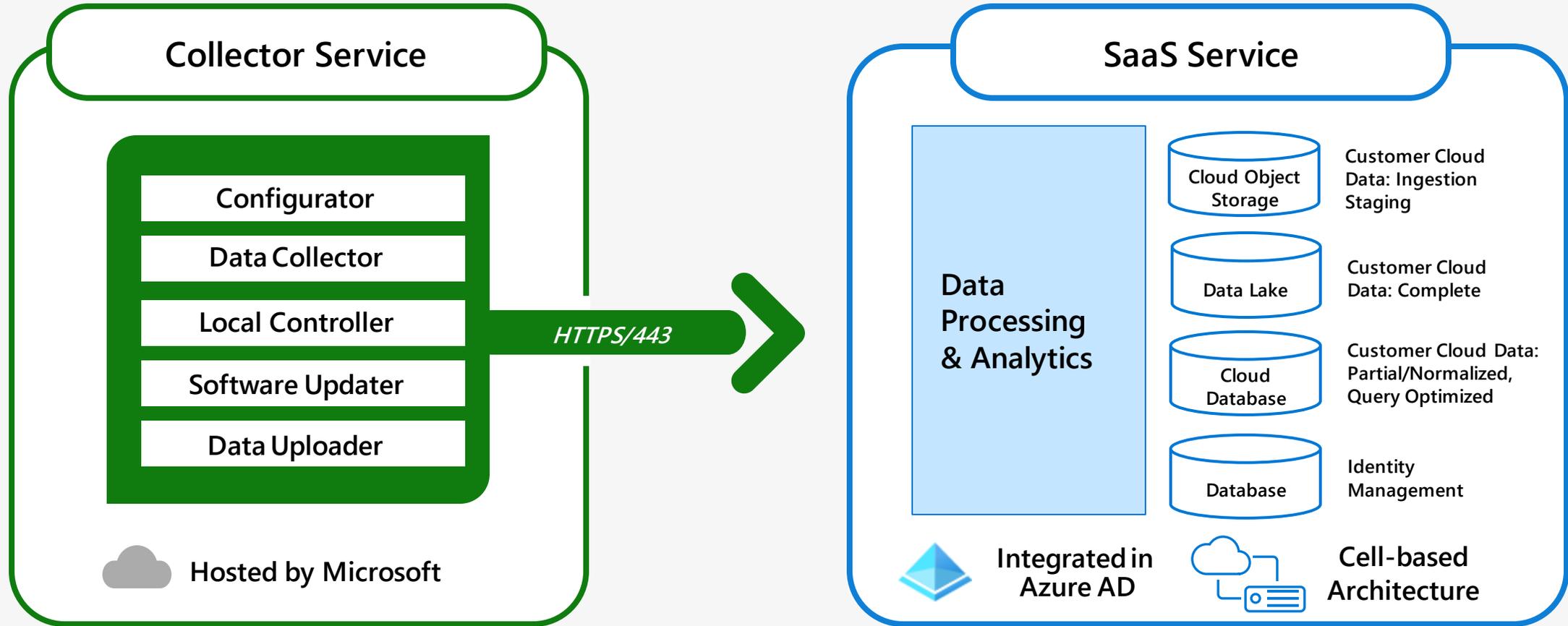
The CIEM compliments PAM & IGA



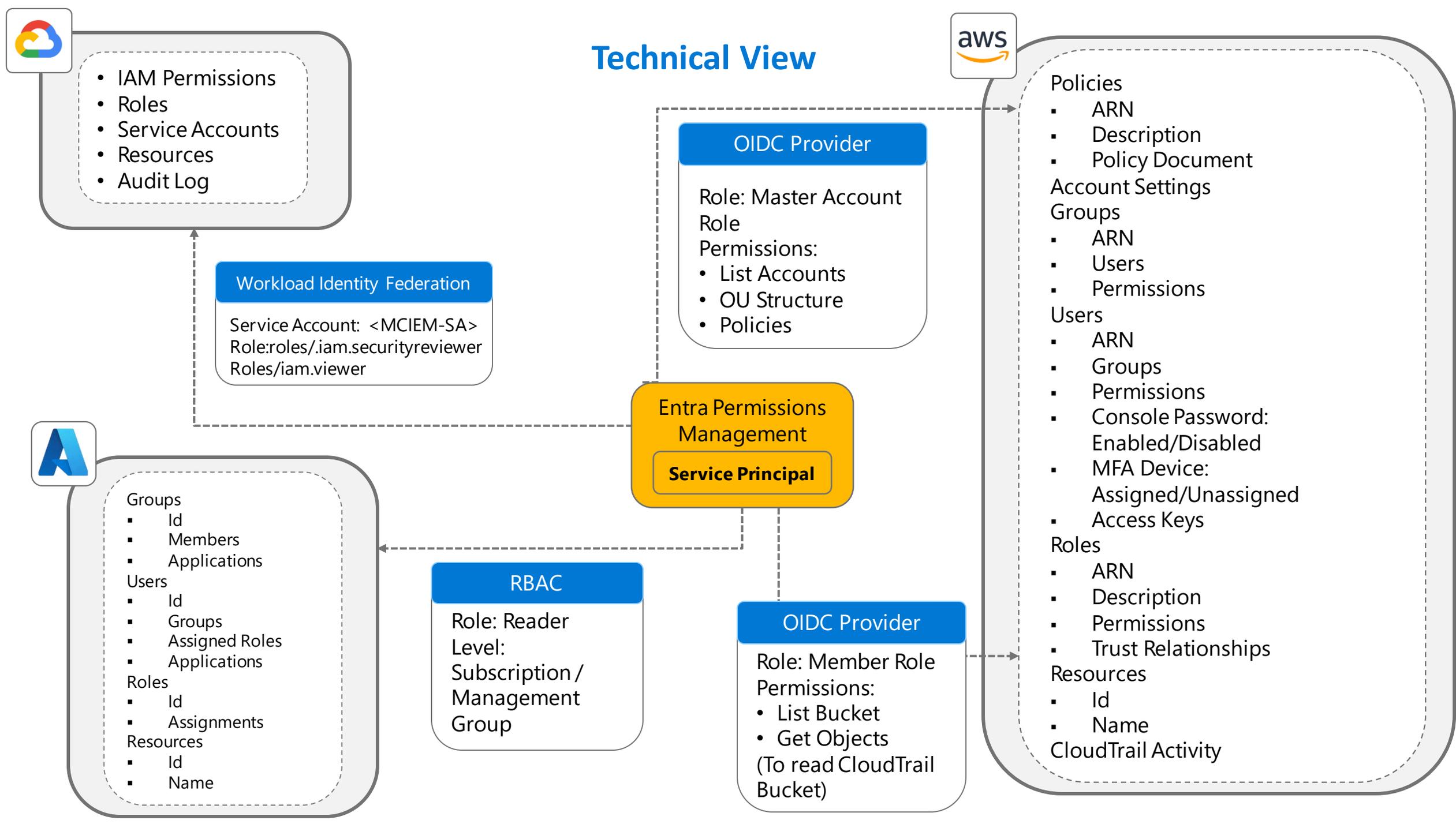
Product Architecture



Product Architecture



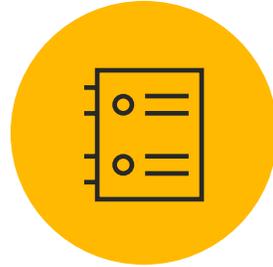
Technical View



Cloud Infrastructure Risk Assessment Preparation



Identify 10-15
accounts,
subscriptions, or
projects for the
Risk Assessment



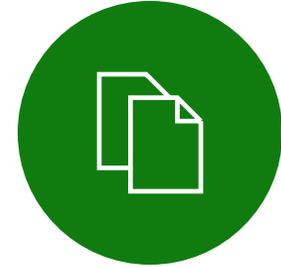
Permissions
Management needs
read role to collect:

Identities

Permissions (Roles/Policies)

Activity logs

Resource metadata (ID,
name & tags)



Begin Data Collection

Cloud Infrastructure Risk Assessment Post-Deployment

» Post deployment the data is ready to view within 24 hours

» Comprehensive assessment report generated



Evaluate where you are today and where you need to be to meet your risk mitigation goals



Identify the areas of greatest risk for mitigation so you know where to focus your resources



Improve your risk posture with actionable insights and prescriptive recommendations

Risk Assessment Key Findings

Finding

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

Cross-account access is frequently granted to external identities

Lack of separation of duties: Users with excessive roles/policies in both development and production subscriptions/accounts

Workload identities are over-provisioned and >40% inactive

Implication

Excessively permissioned active identities are exposed to credential theft risks

Cross-account access enables identities to access all resources in target accounts, leading to data leakage or malicious service disruption

Leveraging the same roles/policies and permissions in development and production environments exposes your infrastructure to insider threats and malicious external threats

Inactive identities leave organizations open to credential misuse or exploitation for malicious activities

Best Practices

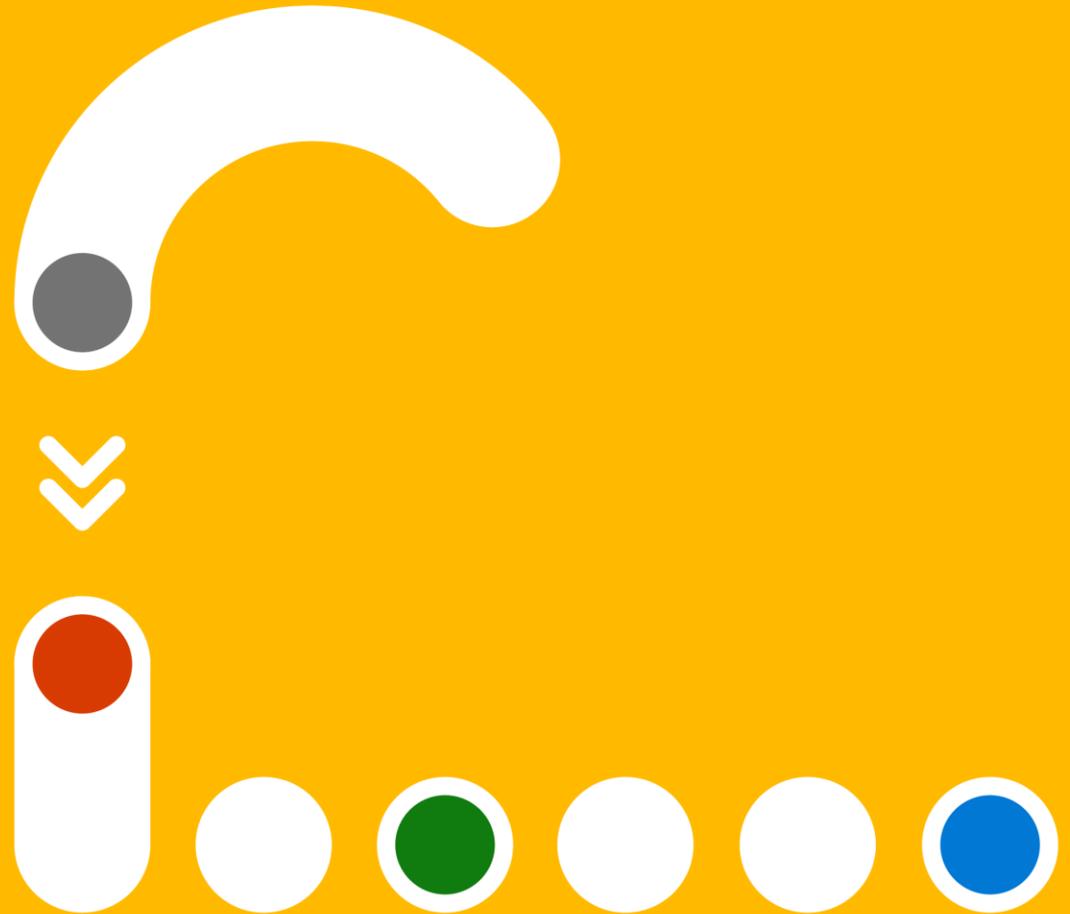
Remove inactive roles/ policies and identities to avoid unauthorized access to resources

Right-size permissions based on the past activities of these identities and grant additional permissions on an on-demand basis

Right-size permissions in development environments and clone permissions into production only as a starting point, then rightsize permissions to tighten controls

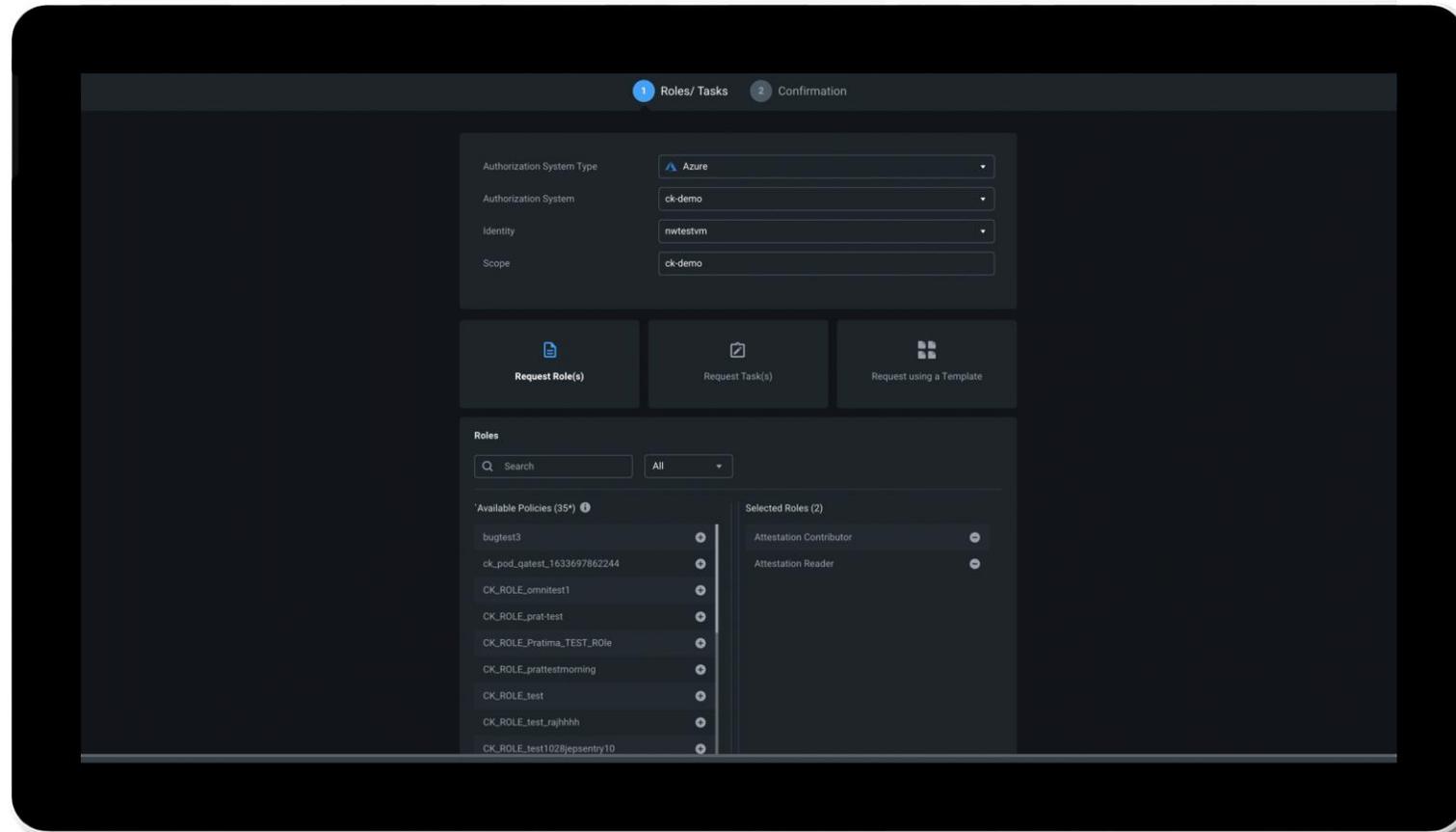
Right-size scope of roles/ policies to access limited resources and limit access to specific identities in other accounts

Workflow Automations



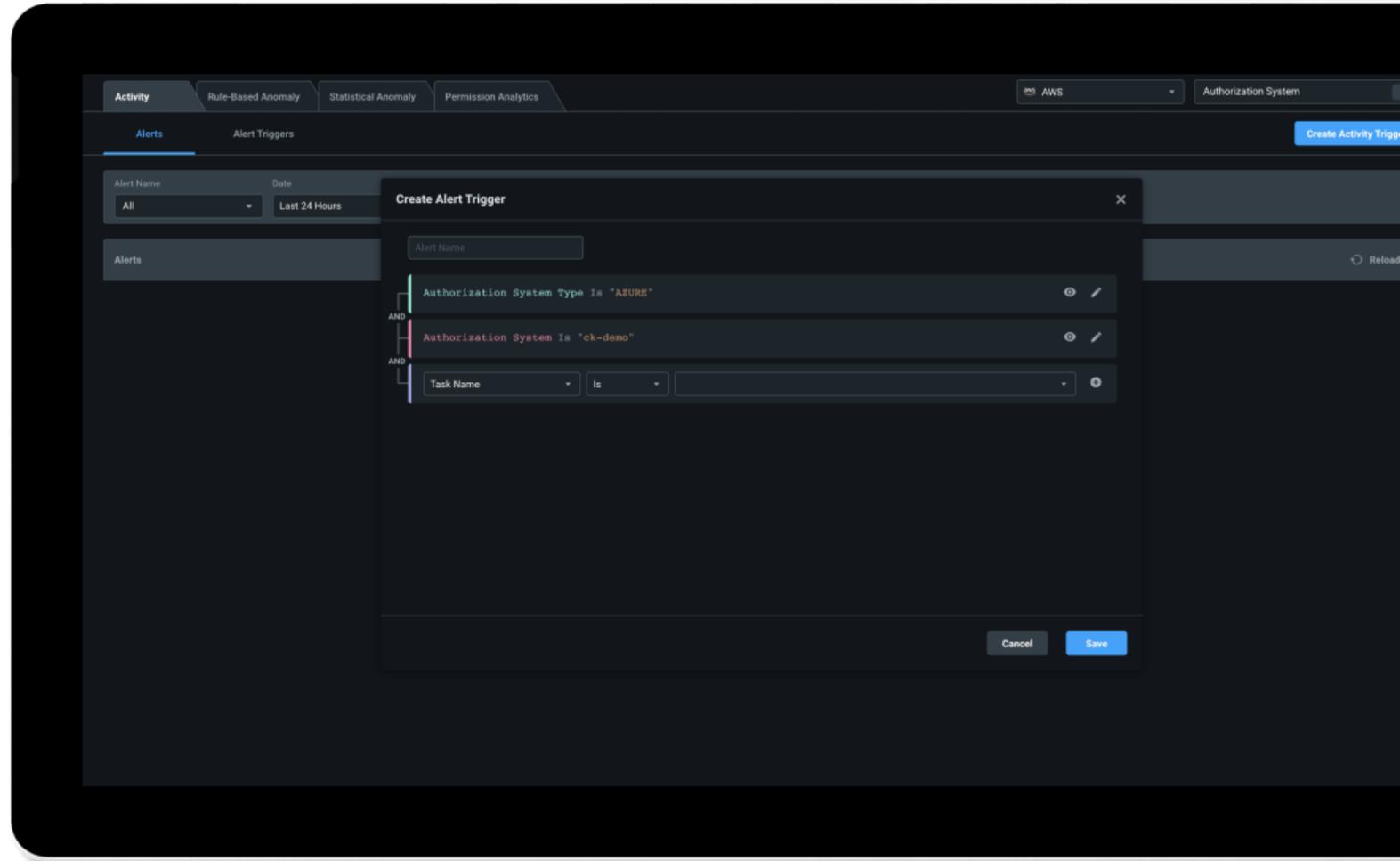
Best practice workflows for permissions on-demand

- **Requesting Delete Permissions:** No user will have delete permissions unless they request them and are approved.
- **Requesting Privileged Access:** High-privileged access is only granted through just-enough permissions and just-in-time access.
- **Requesting Periodic Access:** Schedule reoccurring daily, weekly, or monthly permissions that is time-bound and revoked at the end of period.



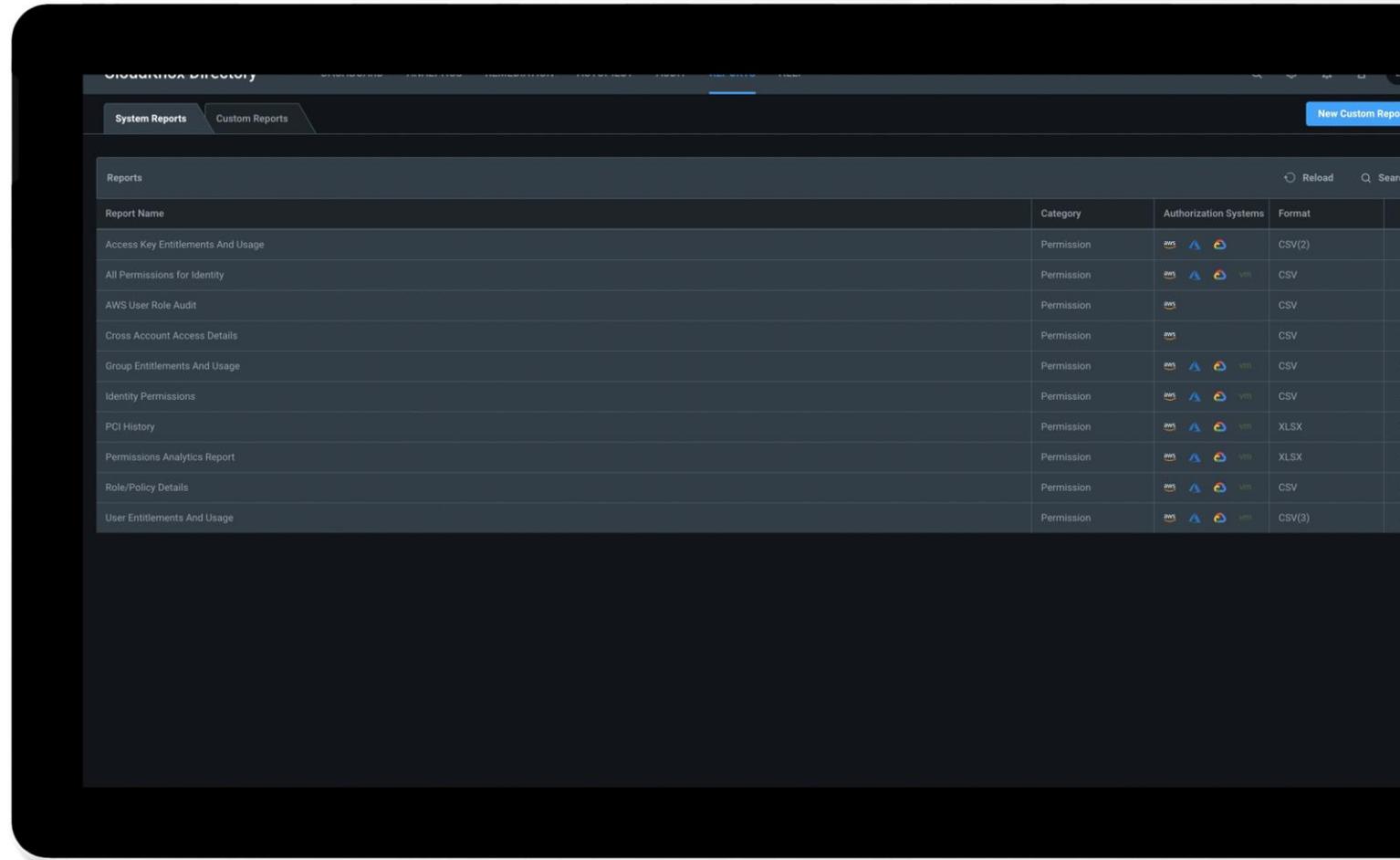
Best Practices for Custom Alerts

- Permission assignments done outside of approved administrators
- Access to critical sensitive resources
- Use of break glass accounts like root in AWS, global admin in azure AD accessing subscriptions, etc.



Key Reports to Monitor

- **Permissions Analytics Report:** lists the key permission risks including Super identities, Inactive identities, Over-provisioned active identities, and more
- **Group entitlements and Usage reports:** Provides guidance on cleaning up directly assigned permissions
- **Access Key Entitlements and Usage reports:** Identifies high risk service principals with old secrets



Demo





Pricing and Packaging

Microsoft Entra Permissions Management is a standalone offering priced at [\\$125 per resource](#) per year

- Resources include compute resources, container clusters, serverless functions and databases
- Support resources from AWS, Azure and GCP
- 90-Day Free Trial Available

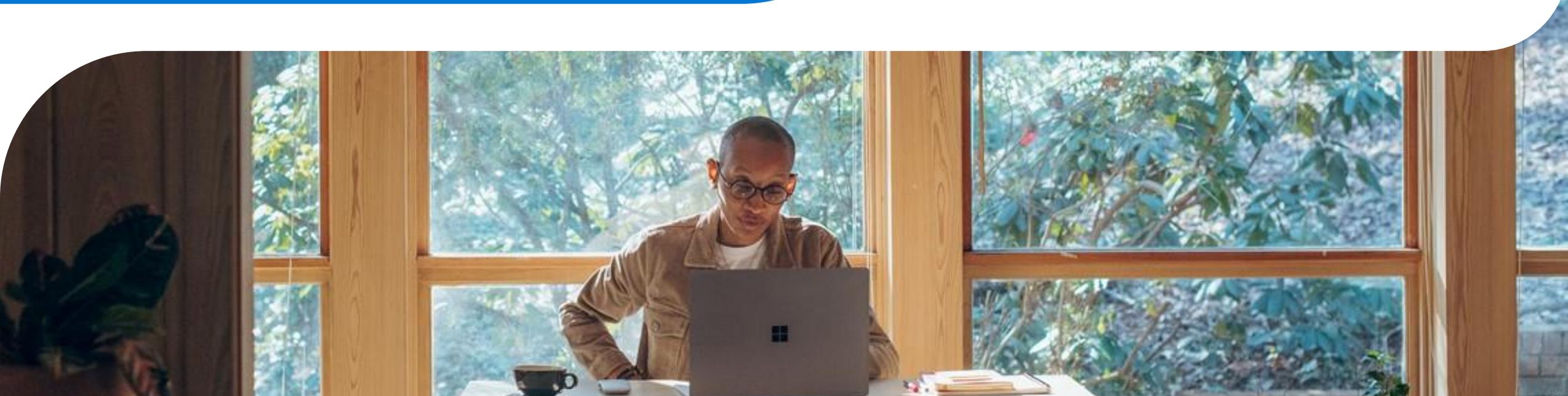
Try Permissions Management now



Try Permissions Management and run a free risk assessment to identify the top permission risks across your multicloud environment. Request a 90-day trial today: <https://aka.ms/TryPermissionsManagement>



Learn more at aka.ms/PermissionsManagement



Resources



Web

aka.ms/PermissionsManagement >>

Docs

aka.ms/CIEM >>

Datasheet

aka.ms/PermissionsManagementDataSheet >>

Microsoft Entra Announcement Blog

aka.ms/EntraAnnouncement >>

Solution Brief

aka.ms/PermissionsManagementSolutionBrief >>

White Paper

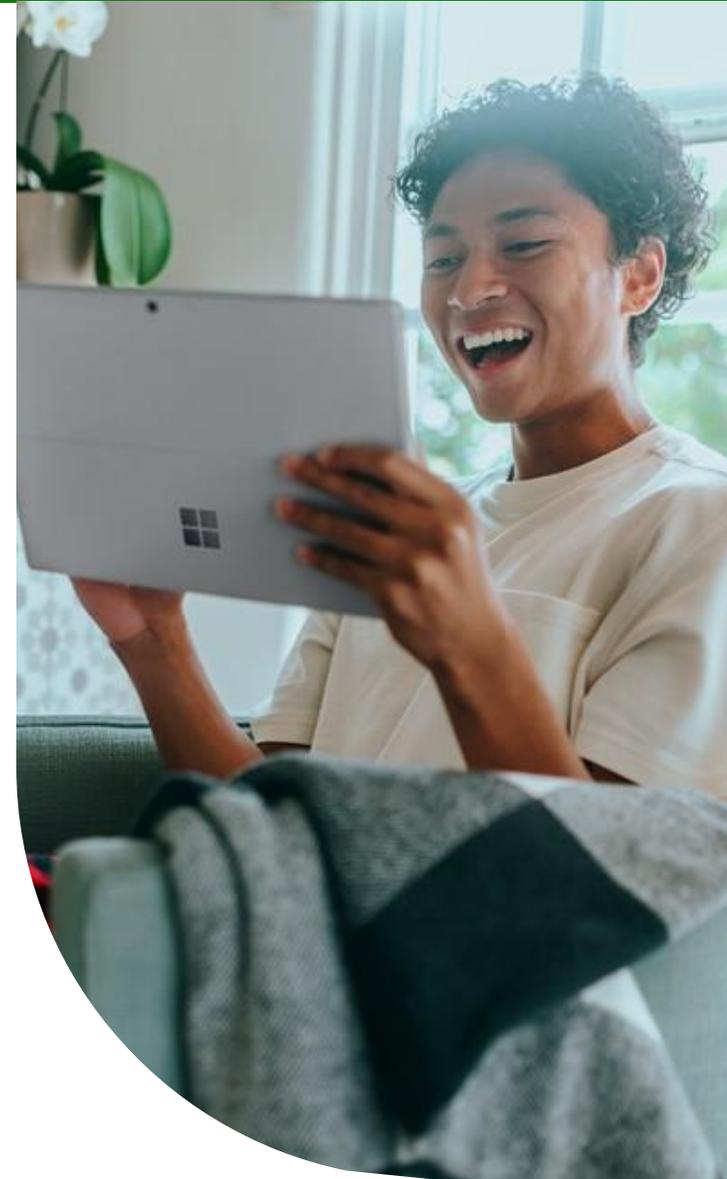
aka.ms/CIEMWhitePaper >>

Infographic

aka.ms/PermissionsRisksInfographic >>

2021 State of Cloud Permissions Risks Report

aka.ms/PermissionsRisksReport >>



Thank you!

Please share any EPM engagements here:
<https://aka.ms/epmpipeline>

For Partners Only