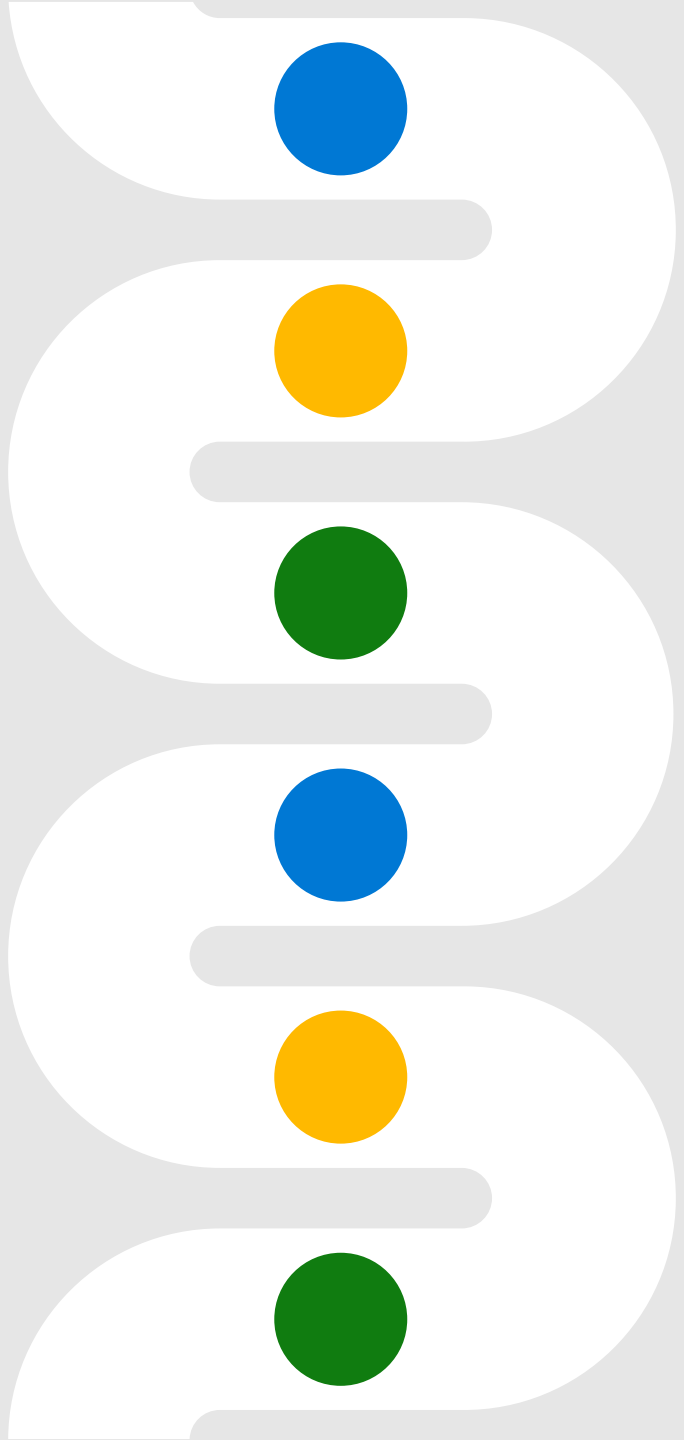
Microsoft Security

Microsoft Entra Permissions Management

Angelica Faber



Overall Agenda

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

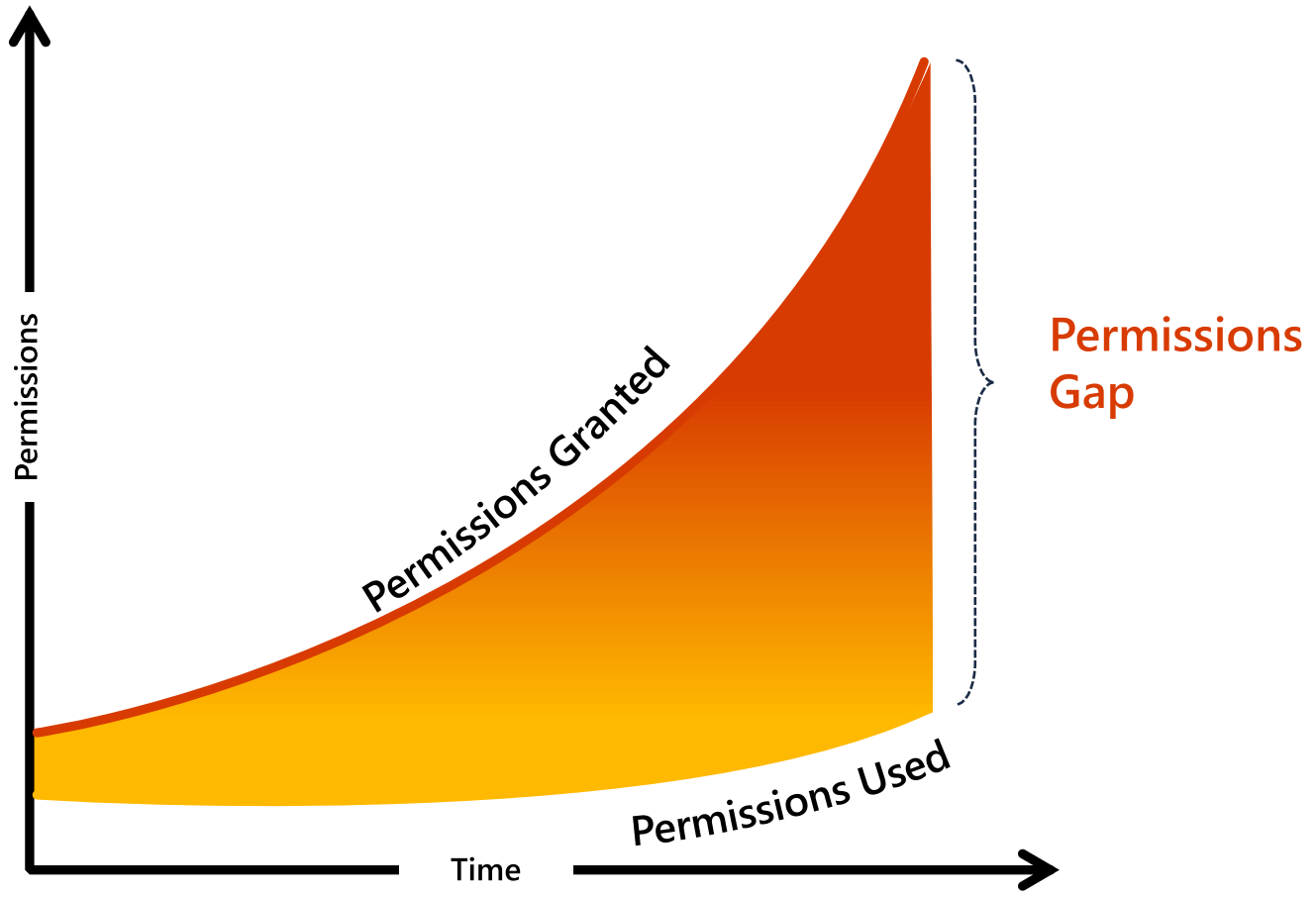
Multicloud adoption brings new permission challenges

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

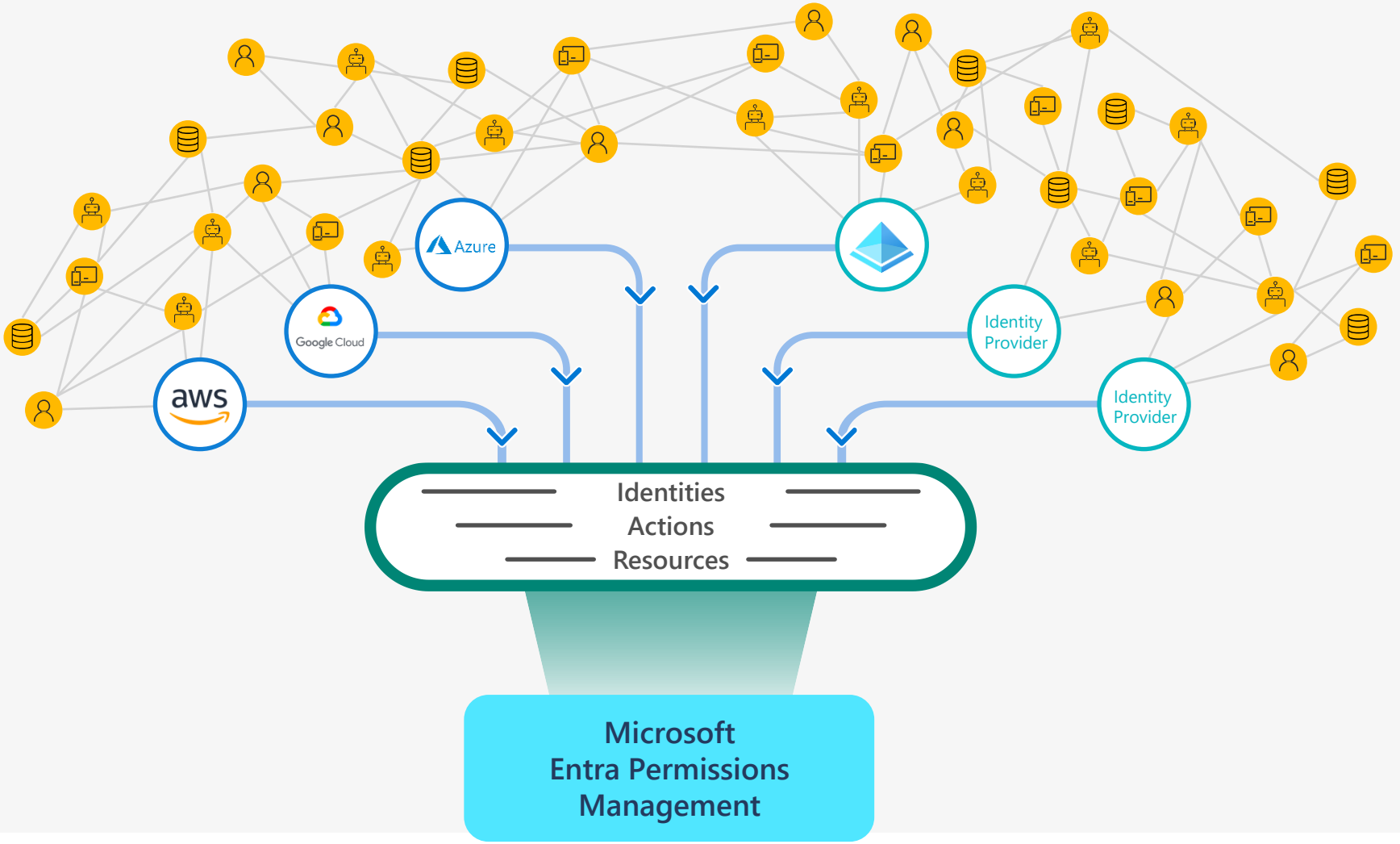
Increased risk of breach from accidental or malicious permission mis-use

Managing permissions across multicloud environments requires a new approach

Today's static, outdated approach	A new, dynamic approach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

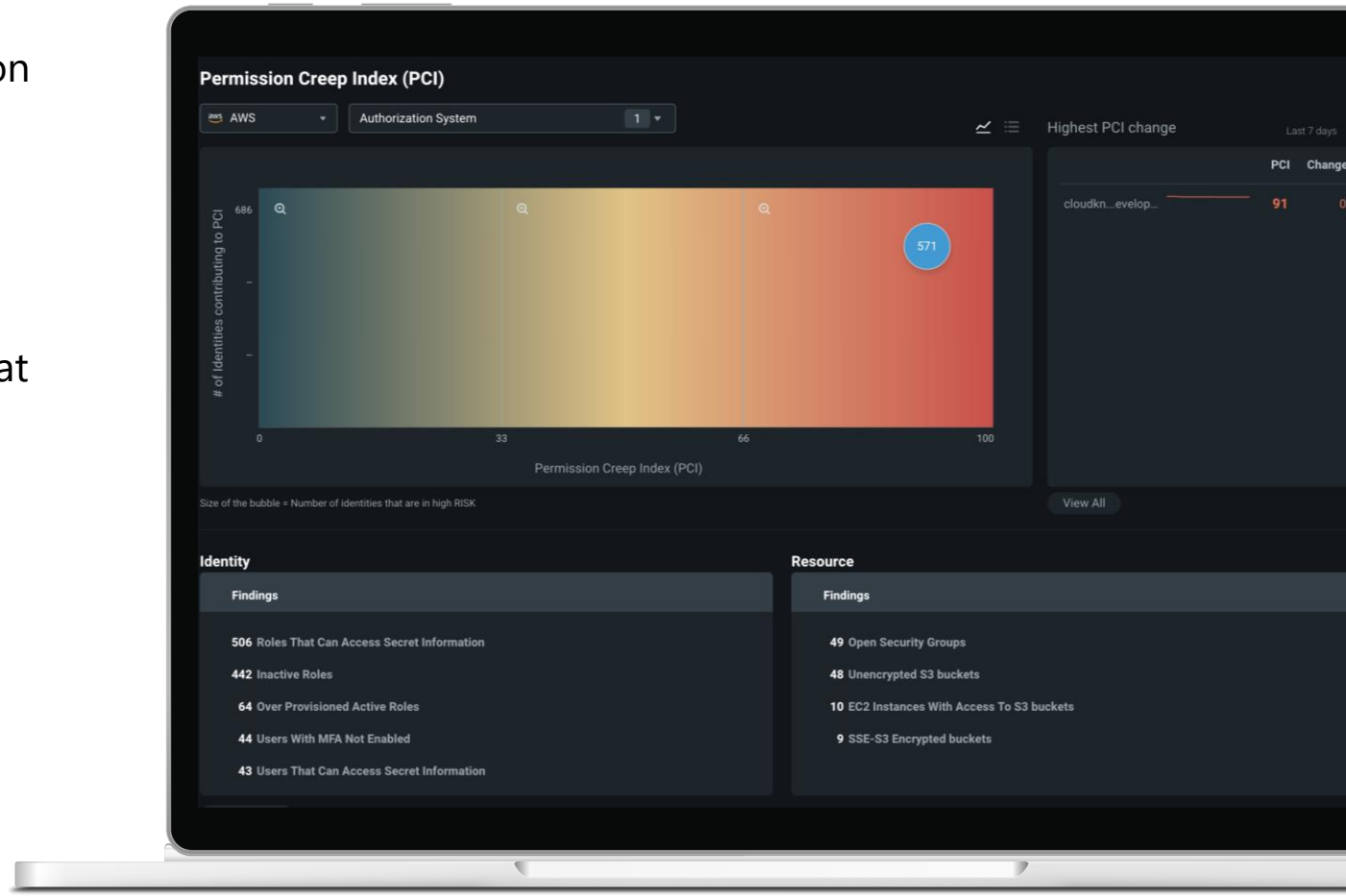
Obtain a comprehensive view of every action performed by any identity on any resource.

Remediate

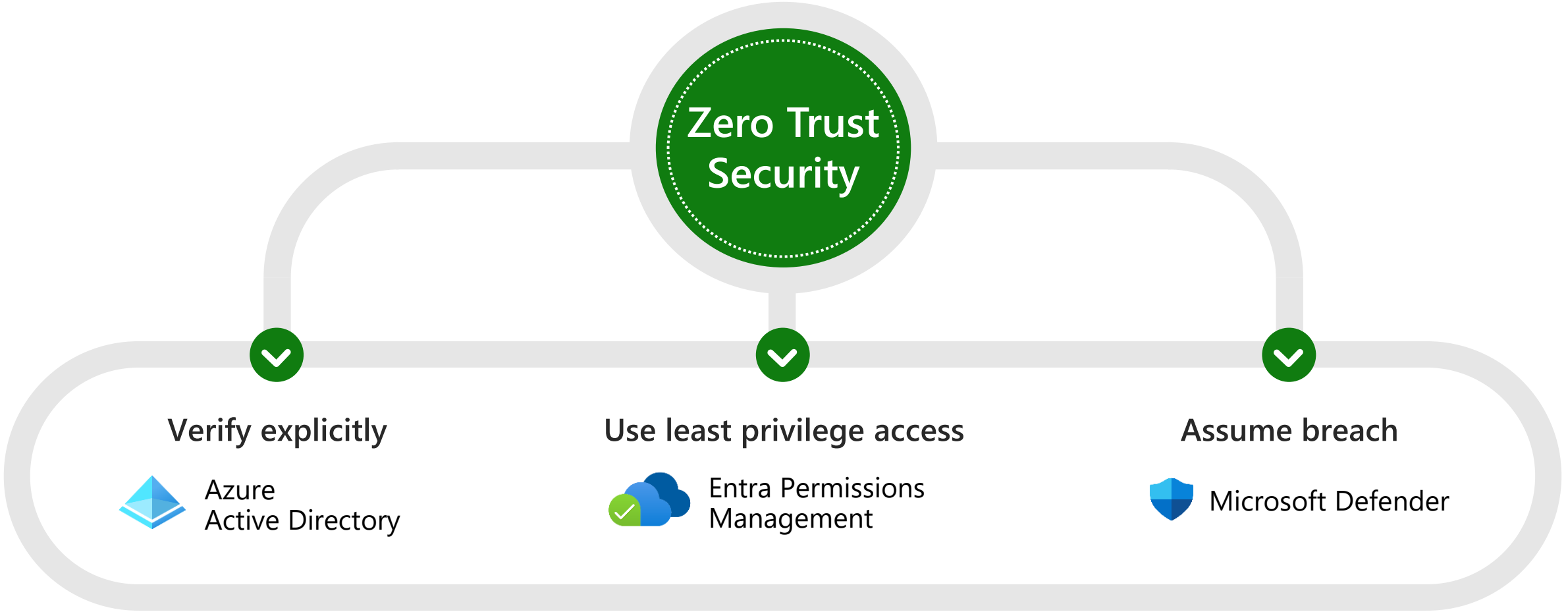
Right-size permissions based on usage and activity and grant permissions on-demand at cloud scale.

Monitor

Detect anomalous permission usage and generate detailed forensic reports.

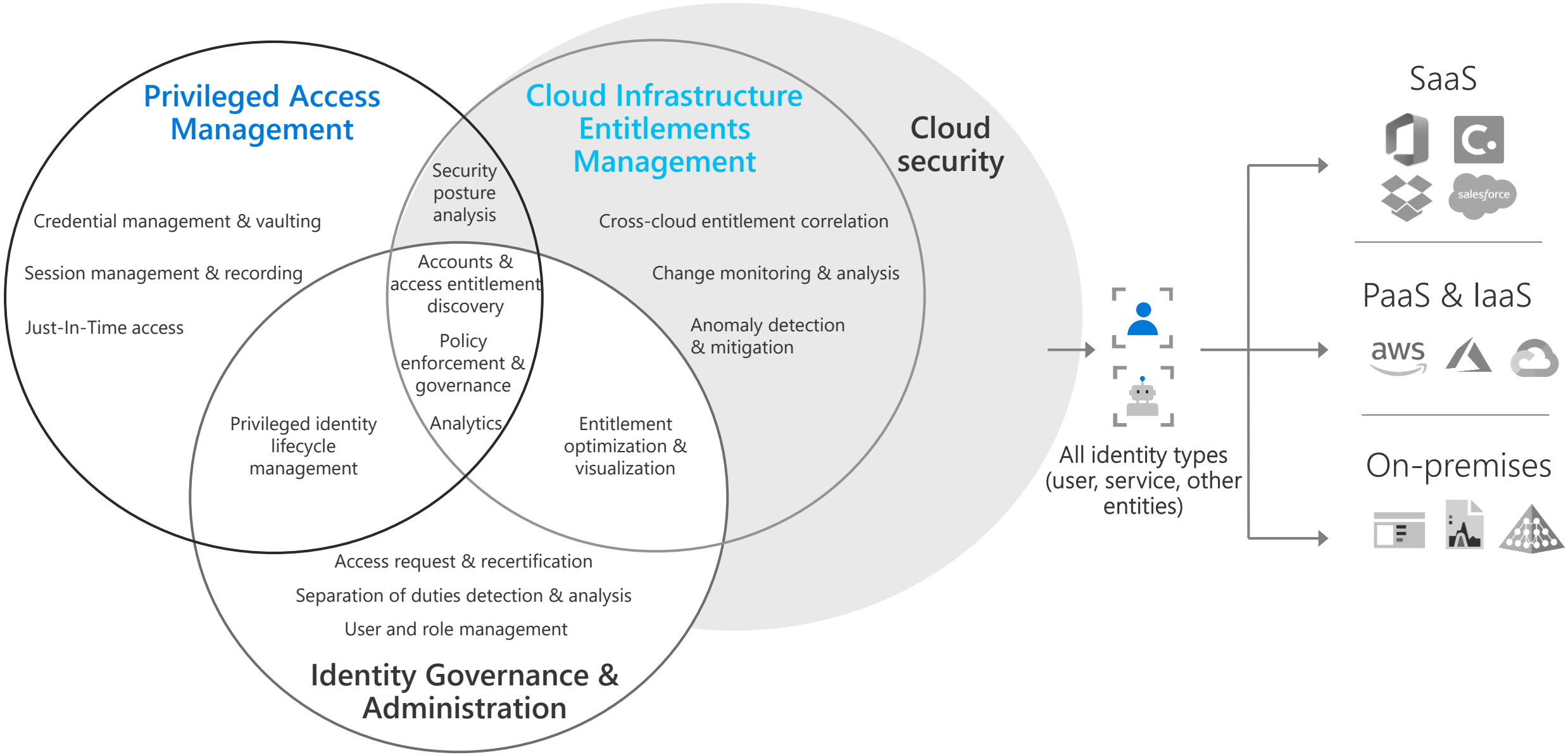


Entra Permissions Management empowers Zero Trust

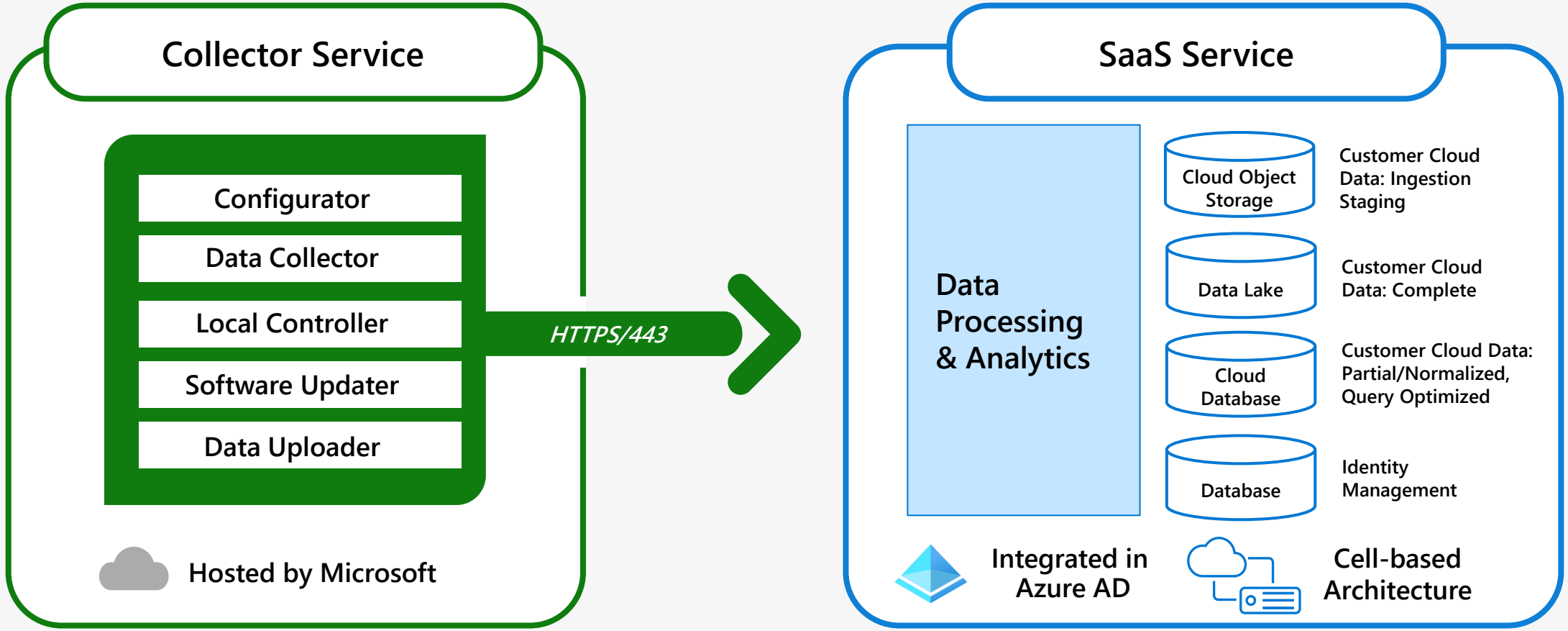


Multicloud | Multi-Platform

The CIEM compliments PAM & IGA



Product Architecture



Technical View

- IAM Permissions
- Roles
- Service Accounts
- Resources
- Audit Log

Workload Identity Federation

Service Account: <MCIEM-SA>
Role:roles/.iam.securityreviewer
Roles/iam.viewer

OIDC Provider

Role: Master Account Role
Permissions:
- List Accounts
- OU Structure
- Policies

Policies
- ARN
- Description
- Policy Document

Account Settings

Groups
- ARN
- Users
- Permissions

Users
- ARN
- Groups
- Permissions
- Console Password: Enabled/Disabled
- MFA Device: Assigned/Unassigned
- Access Keys

Roles
- ARN
- Description
- Permissions
- Trust Relationships

Resources
- Id
- Name

CloudTrail Activity

Entra Permissions Management

Service Principal

Groups
- Id
- Members
- Applications

Users
- Id
- Groups
- Assigned Roles
- Applications

Roles
- Id
- Assignments

Resources
- Id
- Name

RBAC

Role: Reader
Level: Subscription / Management Group

OIDC Provider

Role: Member Role
Permissions:
- List Bucket
- Get Objects

(To read CloudTrail Bucket)

Risk Assessment Key Findings

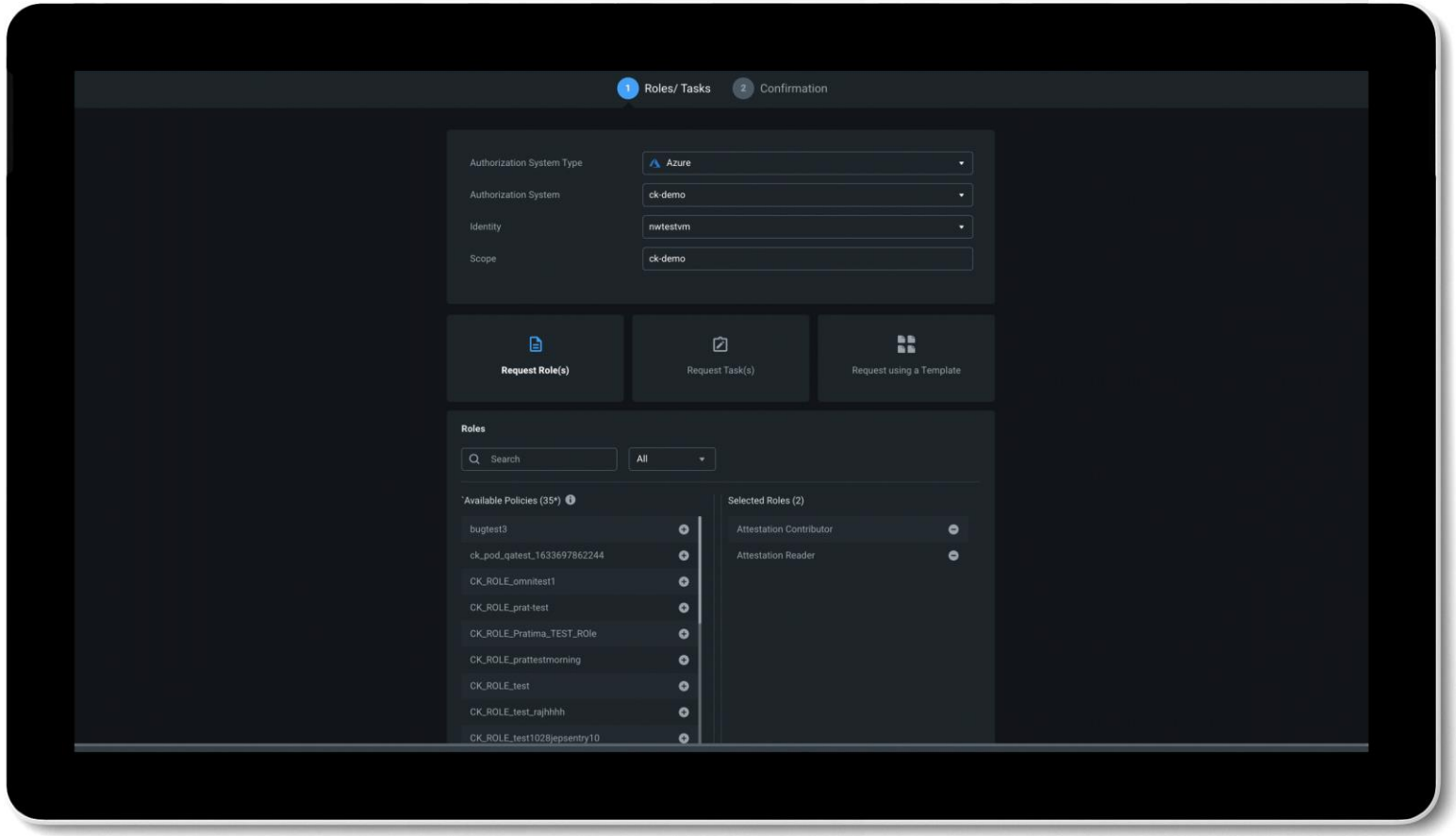
Finding	Implication	Best Practices
>90% of identities using <5% of permissions granted	Excessively permissioned active identities are exposed to credential theft risks	Remove inactive roles/ policies and identities to avoid unauthorized access to resources
Cross-account access is frequently granted to external identities	Cross-account access enables identities to access all resources in target accounts, leading to data leakage or malicious service disruption	Right-size permissions based on the past activities of these identities and grant additional permissions on an on-demand basis
Lack of separation of duties: Users with excessive roles/policies in both development and production subscriptions/accounts	Leveraging the same roles/policies and permissions in development and production environments exposes your infrastructure to insider threats and malicious external threats	Right-size permissions in development environments and clone permissions into production only as a starting point, then rightsize permissions to tighten controls
Workload identities are over-provisioned and >40% inactive	Inactive identities leave organizations open to credential misuse or exploitation for malicious activities	Right-size scope of roles/ policies to access limited resources and limit access to specific identities in other accounts

*Key findings across AWS, Azure and GCP

Workflow Automations

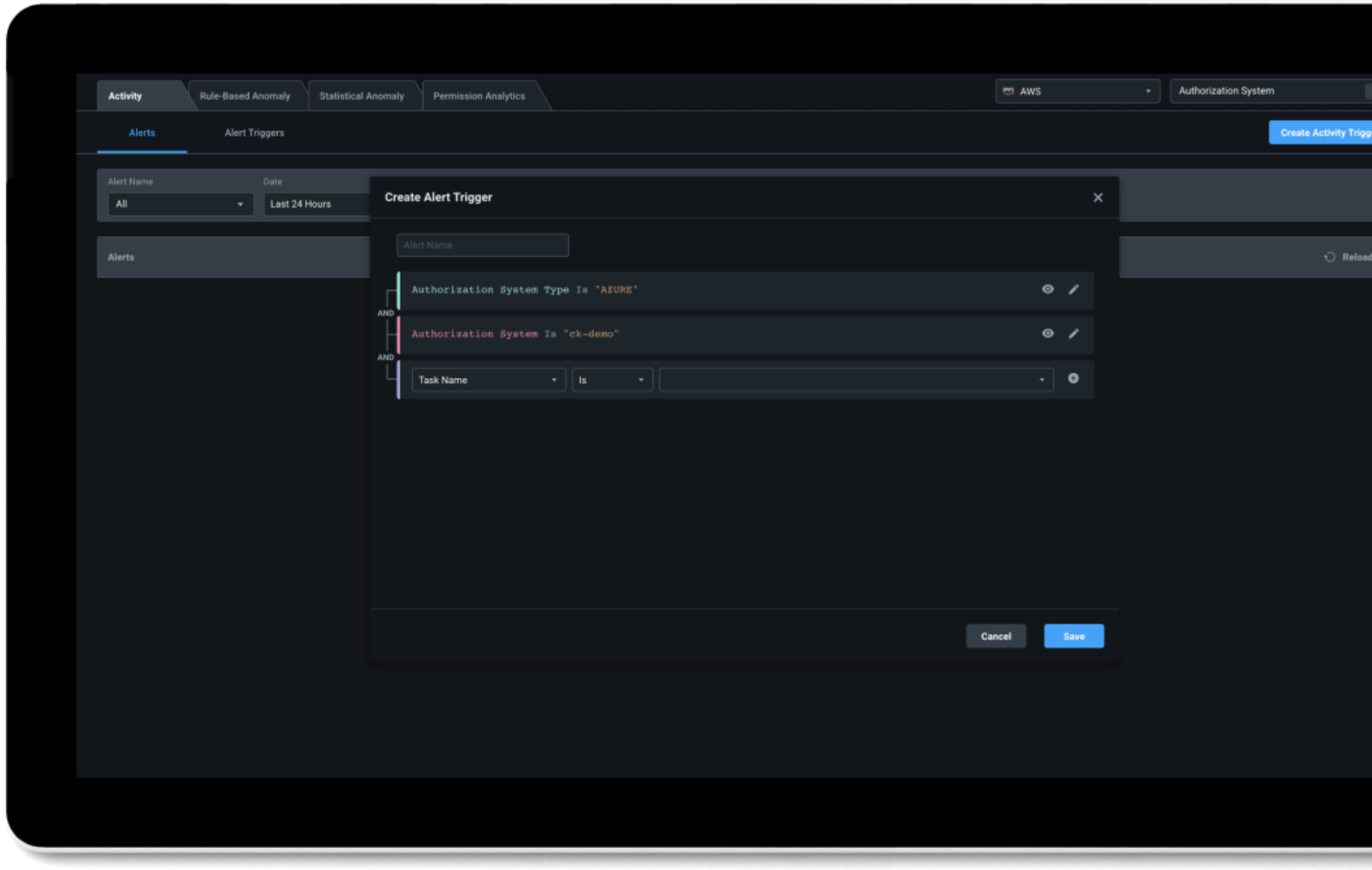
Best practice workflows for permissions on-demand

- **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.



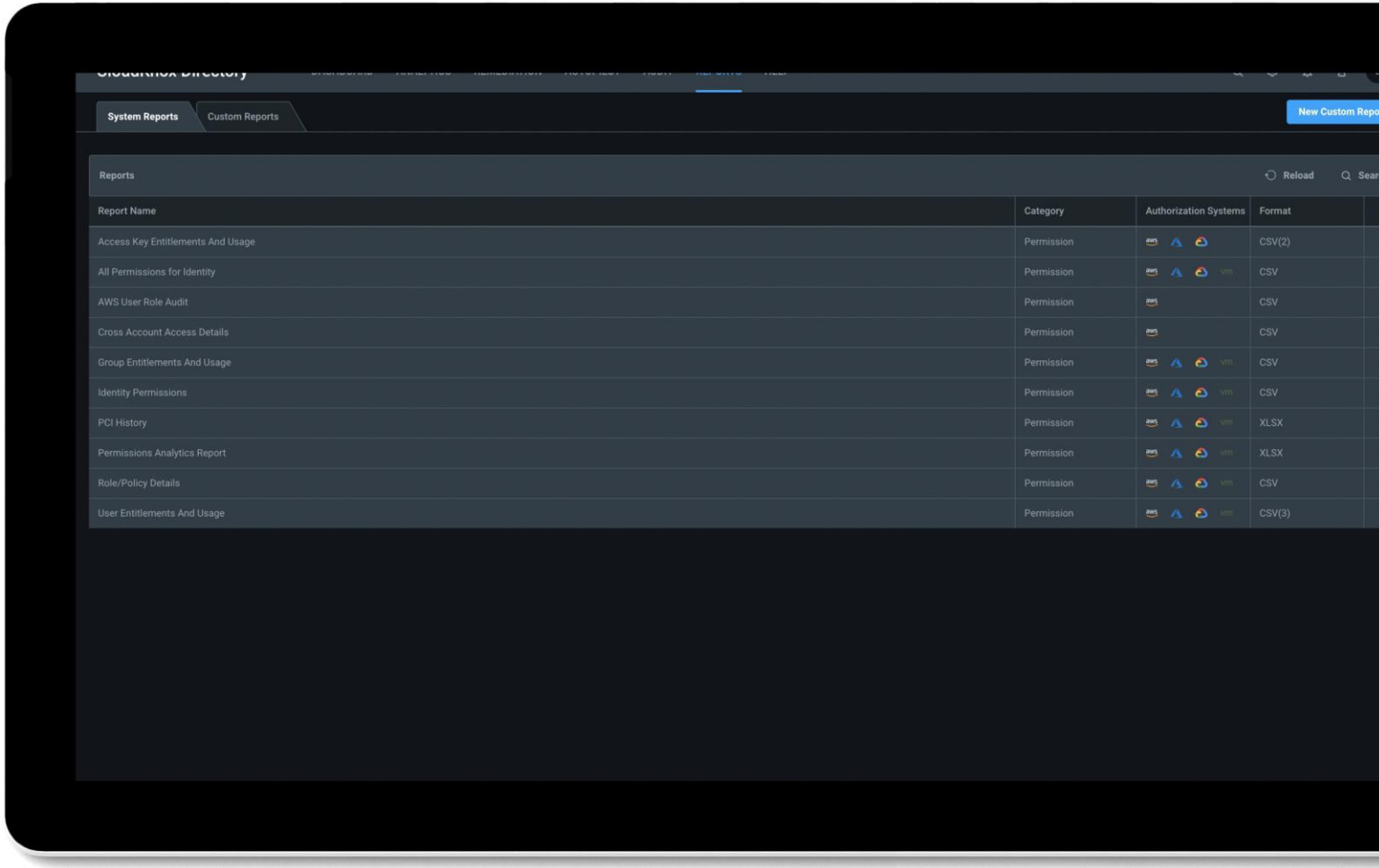
Best Practices for Custom Alerts

- 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 identity 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/Permissions Management

Solution Brief
aka.ms/PermissionsManagement SolutionBrief

Docs
aka.ms/CIEM

White Paper
aka.ms/CIEMWhitePaper

Datasheet
aka.ms/PermissionsManagement DataSheet

Infographic
aka.ms/PermissionsRisks Infographic

Microsoft Entra Announcement Blog
aka.ms/EntraAnnouncement

2021 State of Cloud Permissions Risks Report
aka.ms/PermissionsRisks Report

Thank you!

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

For Partners Only