Privileged Identity Management for your daily Entitlement Management

Azure Active Directory

Microsoft Office 365

Enterprise Applications

Art of the possible

Permissions Management for on-demand multi Cloud Infrastructure Entitlement Management

Azure Cloud Resources

Amazon Web Services

Google Cloud Platform

Demo of EPM

The art of the possible with PIM for your PAM solution.

Martyn Gill

Senior Architect

Kocho

Kocho

BECOME GREATER

Privileged Identity Management

The Privileged Access Management service, providing lifecycle to your privileged resources.

Contents

Overview of Privileged Identity Management

- Microsoft's cloud Privileged Access Management service
- Azure Active Directory, Premium Plan 2 feature
- Protect and control access to your privileged resources
- Improving security posture with risk reduction in your organisation
- How to use other Premium Plan 2 features to enrich and expand the PIM capabilities

Core capabilities

- Time-bound eligible or active assignments to privileged resources.
- On-demand with just-in-time elevation of privileged access.
- Workflows for assignment, activation and notifications.
- Approval process where required, with the addition of Multi-Factor Authentication.
- Traceability of access requests with recorded justification, and downloadable audit history for compliance.
- Evergreen security posture alerting, and discovery with insights ensuring best-practice of the service usage.

Consumers and Privileged Resources

Consumers of Azure AD PIM can include employees (Member user accounts), third-party partners or suppliers (Guest user accounts) and system workload identities (e.g., service principals)

Azure AD Built-in roles

- → Out-of-the-box pre-defined roles
- → Around 100 in total
- → Consider PIM migration with high-privileged roles, like Global Administrator

Azure AD Custom roles

- → Define your own roles with just-enough access
- → Fine-grained permissions
- → Hundreds of permissions to choose from

Microsoft Azure Cloud

- → Azure Subscriptions & Management Groups
- → Discovery of resources
- → IAM Roles for Azure Cloud

Privileged Access Groups

Privileged Access Management for anything that can use Groups

- → Role Based Access Control
- → PAM capabilities for Applications that can use Groups
- → Integration with Entitlement Management Access Packages
- → Extend PAM capabilities on-premises with Group Writeback

Role Based Access Control

Aligning your organisations business roles with the right technology privileges, by granting just enough access to all the privileged resources.

- → Privileged Access Groups assignment to multiple resources
  - → Azure AD Built-in roles
  - → Azure AD Custom roles
  - → Microsoft Azure Cloud IAM roles

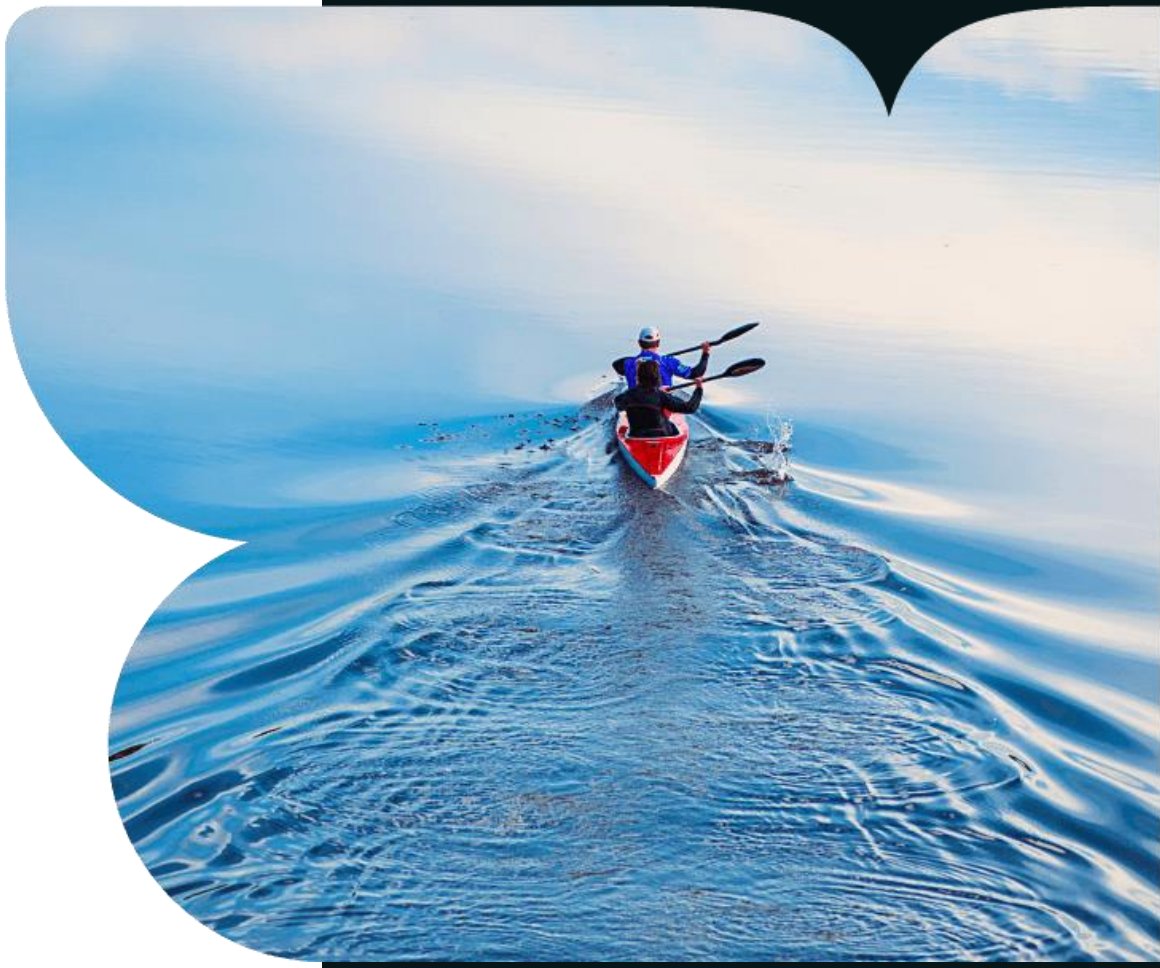
Enterprise Applications

PAM capabilities for Enterprise Applications using Privileged Access Groups

- → Single Sign-On to privileged Applications
- → Single Sign-On Role or Group claims granting Application privileges
- → User Provisioning of Groups granting Application privileges
- → Password-based Single Sign-On for password proxy of Application local privileged credentials

Management

- Self-service request fulfilment to Access Packages, using the My Access web portal
- Multi-approval steps
- Customisable questions
- Include multiple resources
- Separation of duties
- Custom workflows with Logic Apps
- Dynamic eligibility with criteria-based groups
- Automatic assignment



Group Writeback

Use Privileged Access Groups with Group Writeback for PAM capabilities on-premises

- → Uses Azure AD Connect
- → Choose which Groups to Writeback to Active Directory
- → Active Directory Group with Cloud Display Name
- → Nest group in existing privileged Group roles, like Domain Admins

- → Other automation options available for just-in-time access, and third-party Guest user accounts

Recertification

Governing privileged entitlements ensures that the access is granted to the authorised consumers, especially when organisations continually change.

Using regular recertification to validate privileged access for employee's, third-parties, and applications, can be performed using Identity Governance Access Reviews.

- → Access Reviews using the My Access web portal with recommendations
- → Frequency and duration of review cycles
- → Automatically apply results and take actions
- → Integrates directly with PIM, Access Packages, and more...

PIM service in operations

Enabling the right capabilities to provide a secure and operational service ready for your organisational needs

Securing end-points

Ensuring privileged access can only be used by secure end-points can be accomplished with Conditional Access. This provides access conditions which must be met to grant access.

PIM roles and Privileged Access Groups can be defined as consumers of a policy, enabling consumers of privileged access to be secured as required. For example:

- → Enforce MFA when accessing the Application
- → Connecting from a specified IP or location
- → Using a compliant managed device
- → Using a modern authentication client
- → Have a low sign-in or user risk level, and more...

Additional security for the service

As part of operationalisation of the PIM service, you'll need to consider the following

Emergency break-glass solution

- Critical to ensuring mitigation against lock-out scenarios:
- Accounts are federated, and the federation is unavailable.
- MFA is enforced, and all devices or service is unavailable.
- The Global Administrator has left the company and the account has been disabled or deleted from on-premises.

Administrative Units for securing directory resources

- Logical separation of users, groups and devices
- Restricted administrative permissions
- Removes default access that might be granted
- Consider for Privileged Access Groups and accounts you use for privileged access

Integration capabilities

The Azure AD services is automation-ready with the Microsoft Graph API, and provides many options for integration with your organisations Security Information and Event Management (SIEM)

Microsoft Graph API

- → Services are built API first
- → Enabling scripts or third-party applications for automation of the services
- → Easy to setup with an app registration, granting permissions and assigning a secure key

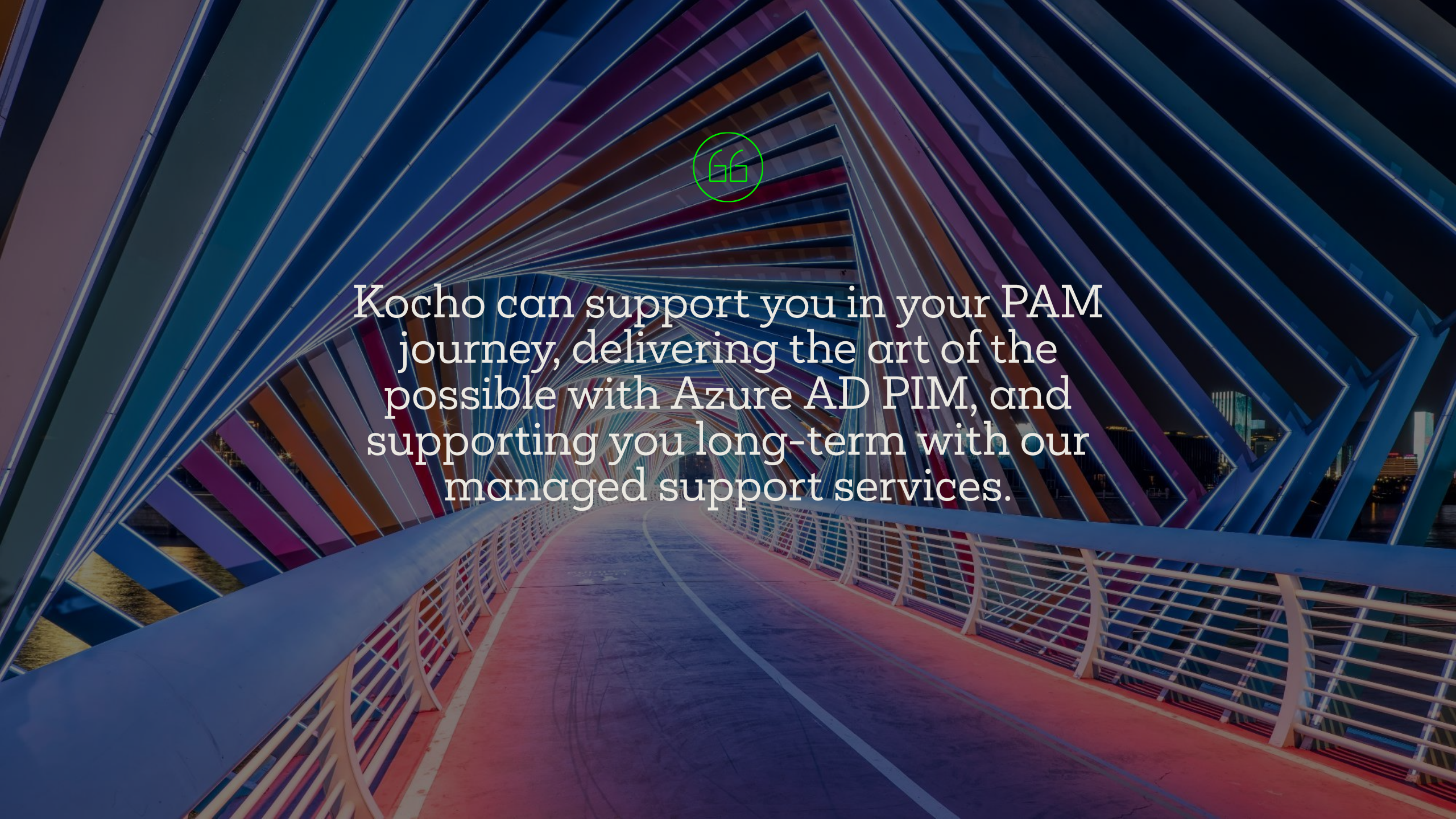
Azure AD Logging

- → Includes PIM, Access Packages, Access Reviews & more
- → View in Azure portal, short retention and downloadable
- → Azure AD logs can be made available to; Log Analytics, Storage accounts, Event Hubs and more for your SIEM
- → Including the many log categories; sign-in, audit, non-interactive, provisioning and more

Operating the service

- Analytics and Reporting on the usage in forms of Workbooks and Dashboards
- Alerting for service-related misconfigurations, with recommended remediations
- Recommendations on PIM role usage with Discovery and Insights
- Downloadable audit history for compliance

Questions?


Kocho can support you in your PAM journey, delivering the art of the possible with Azure AD PIM, and supporting you long-term with our managed support services.


Journey to the multi-cloud privileged
management solution.

Microsoft Entra Permissions Management

Walkthrough and Demo

Tom Urwin

Identity Architect

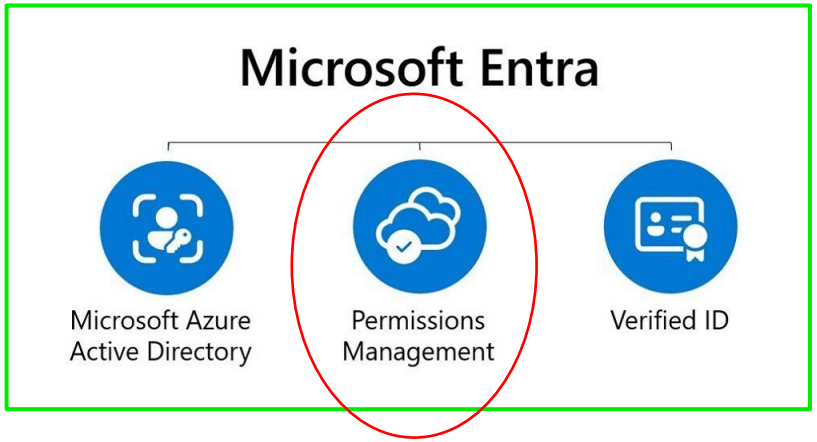
Kocho

Kocho

BECOME GREATER

What is Entra?

Microsoft Entra is a new family of products that includes Azure AD and new product categories for CIEM and decentralized identity.



What is Entra Permissions Management?

Known as a Cloud Infrastructure Entitlement Management service, or CIEM, Permissions Management offers continuous permissions monitoring and proactive responses to stay on top of access *before* it becomes a problem.

- Discover what resources every identity is accessing across your cloud platforms – Azure, AWS and GCP
- Use usage analytics to ensure identities have the right permissions at the right time
- Implement consistent security policies across your cloud infrastructure
- Ability to remove unused permissions, i.e. permissions assigned vs permissions used

Why Permissions Management?

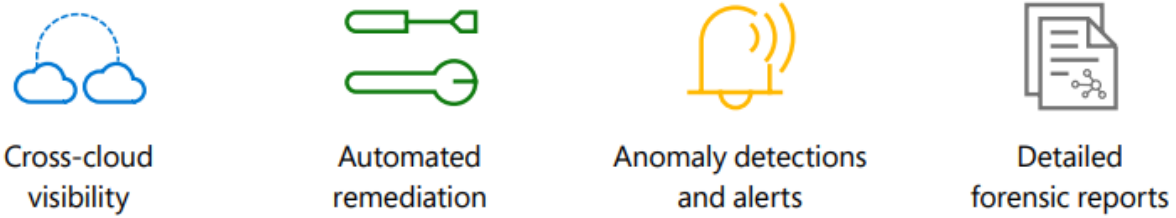
As organisations massively adopt a multicloud strategy, several trends are stressing the need for better visibility and tighter control for cross-cloud access management.

→ Number of identities is on the rise

→ Explosion of cloud workloads

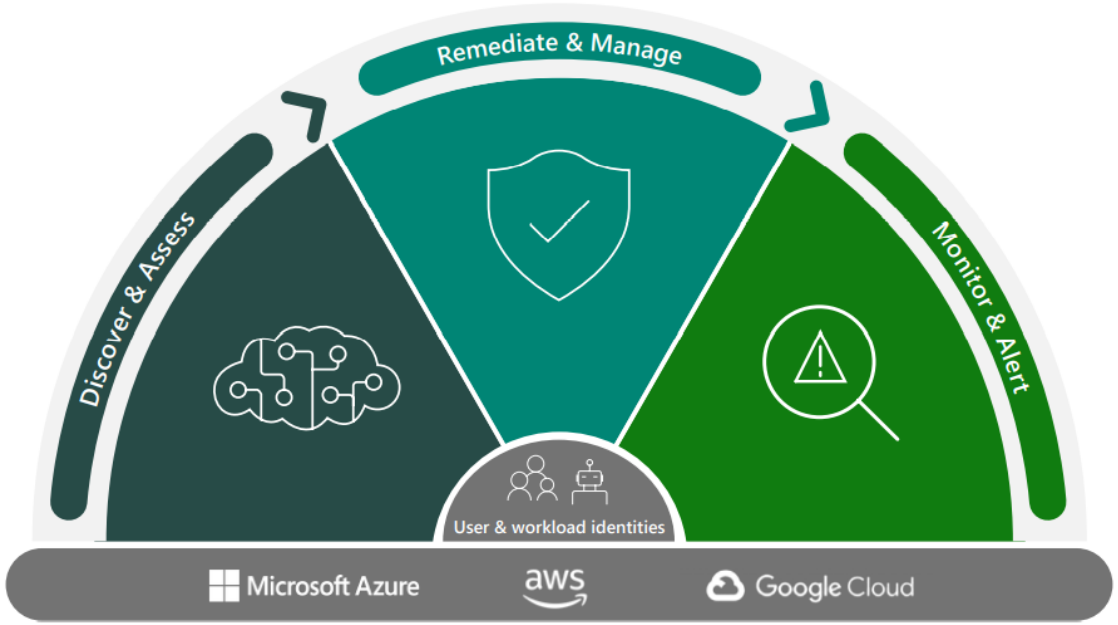
→ Increasing permissions gap

→ Inconsistent access management models



Why Permissions Management?

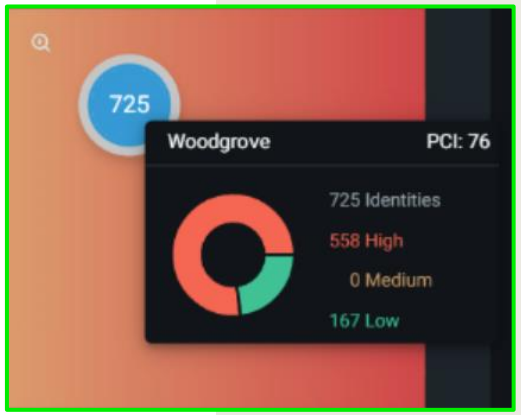
- → Get granular cross-cloud visibility
- → Enforce least privilege – at the right time
- → Uncover permission risk
- → Monitor and detect anomalies



How does Permissions Management work?

- ‘Controllers’ are configured for each workload and tied to an Azure subscription, AWS account or GCP project
- Permissions Management continuously monitors for unusual changes or permission creep over time
- Suggestions and response options are available directly in the UI
- By default, controllers have *Read* access only
- Custom roles can be created and applied to different systems
- Permissions On Demand allows for just-in-time style access requests, based on built-in or custom roles across all clouds
- Reports can be generated for both high-level and detailed perspectives

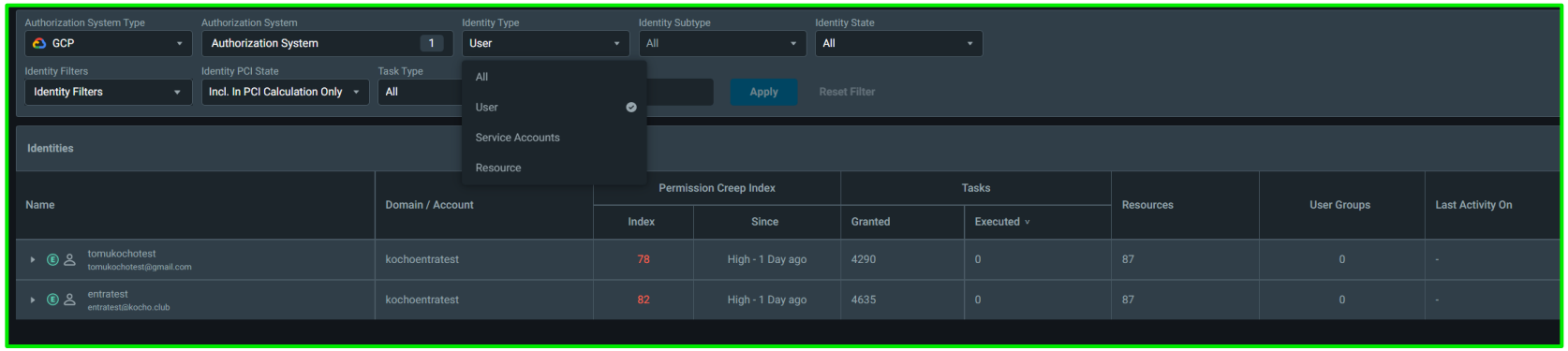
Analytics



Dashboard

- The Permission Creep Index (PCI) gives us an overview of permission changes found over time. It separates users into different levels of permission creep – Low, Medium and High
- The PCI represents permissions used vs permissions granted
- The Identity card shows us general findings around inactivity, privileges and security. The cards vary depending on the service
- The Resource card may spot a Managed Key in Azure and in in AWS an S3 bucket with public access

Analytics



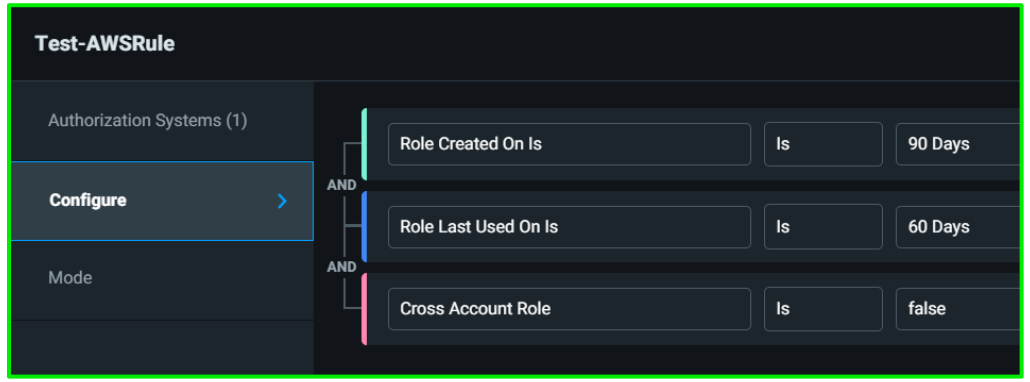
- The Analytics screen allows us to search and filter the events that have been detected
- You can filter between Users, Groups, Apps and other resources
- Results can be further drilled down to reveal more specific information

Remediation

- The Remediation screen allows you to easily view and even amend permissions across resources, including roles, policies and users
- Custom roles can also be created and used, including based on the recent activities of an existing user
- Permissions On Demand allows for specific permissions be assigned just-in-time or on a schedule
- Quickly revoke unused and high-risk tasks (actions), either via the UI or script

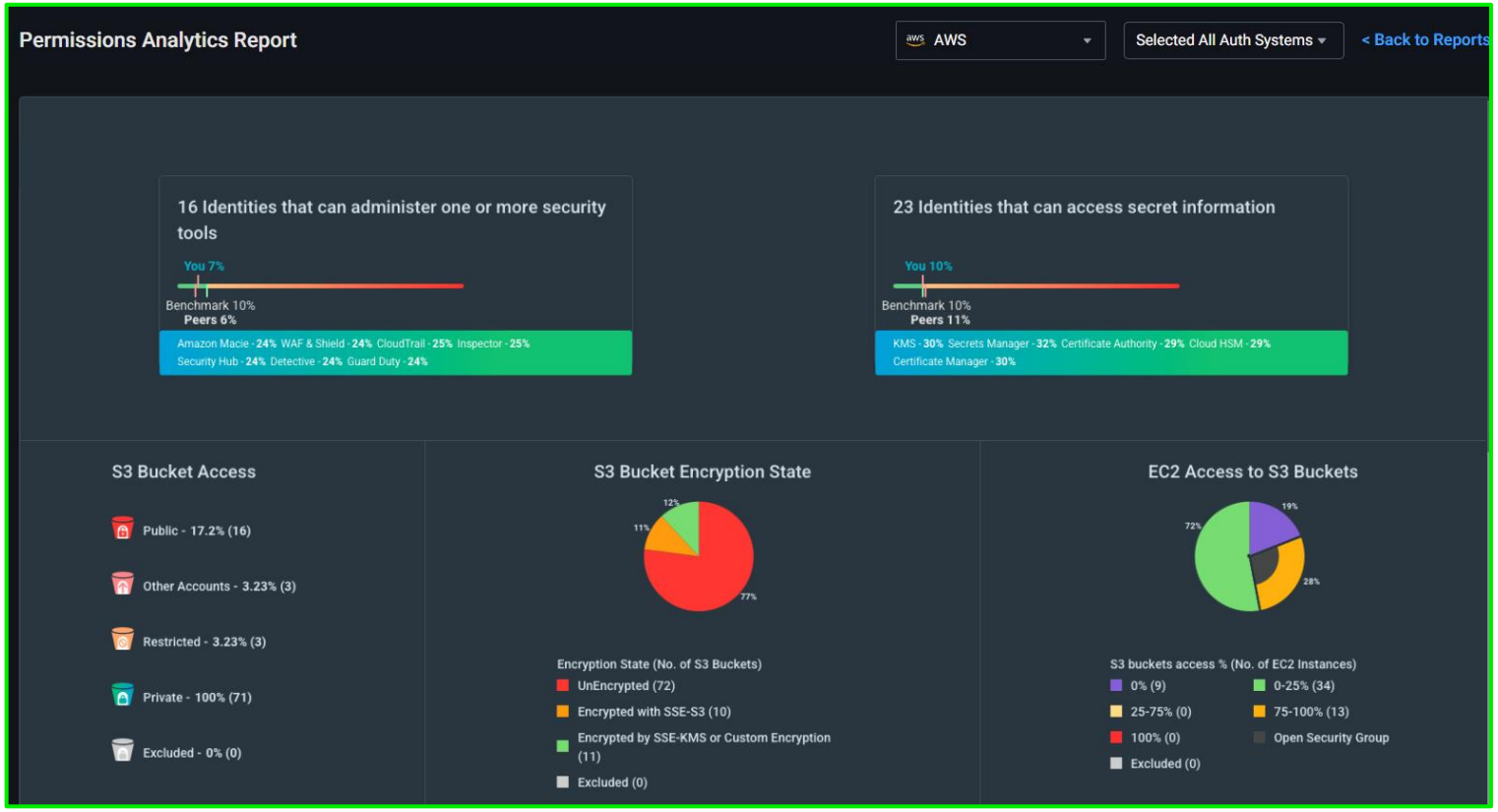
Autopilot

- Allows you to setup rules to automatically make recommendations to remediate access issues, both around users and roles
- Examples include removing unused AWS roles and removing permissions from unused service accounts
- Recommendations and be applied via the UI, and “unapplied” if the action leads to issues



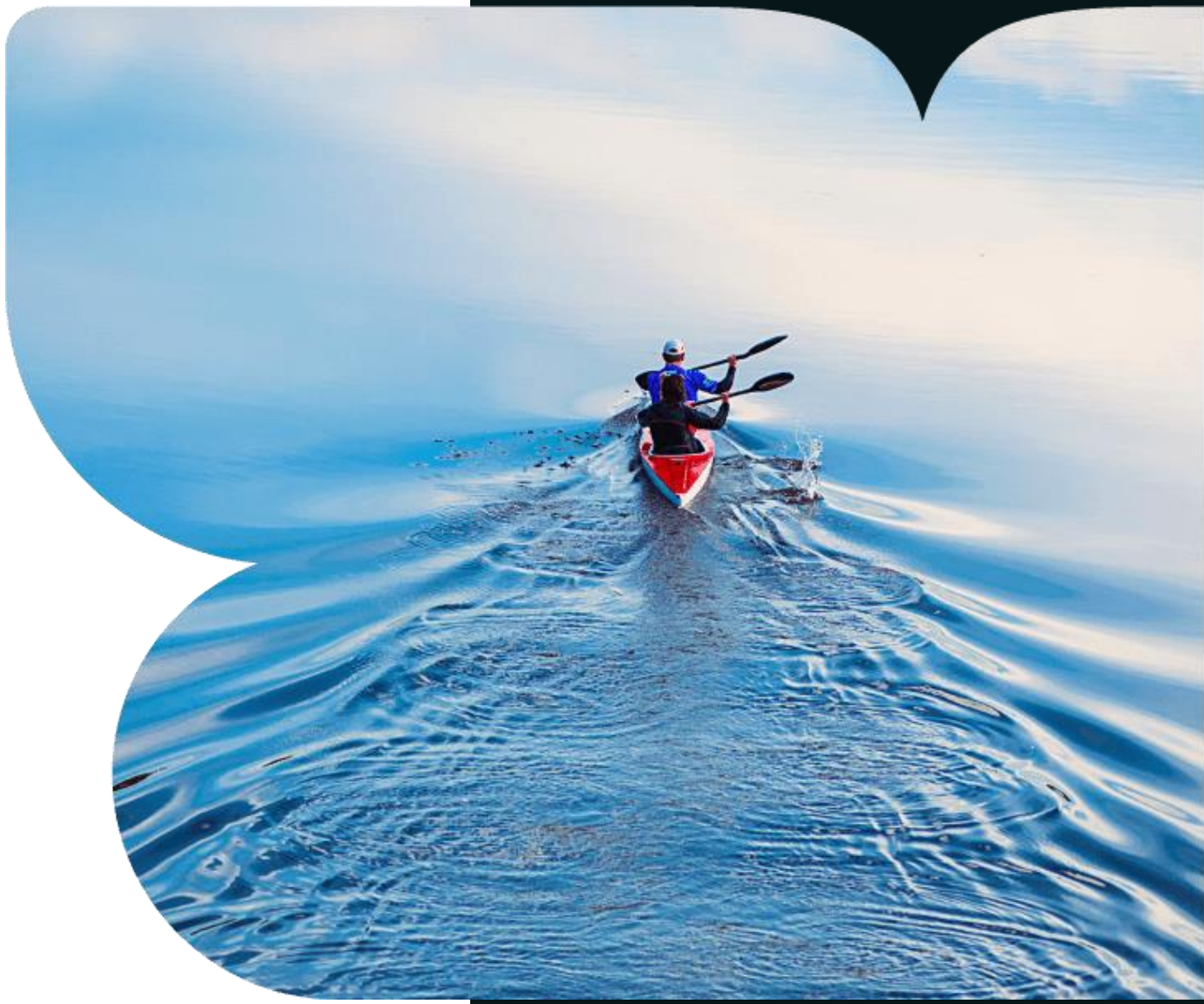
Audit and Report

- Audit allows us to search across each authorisation system for any relevant changes over a given time period
- Reports allows us to run a pre-built permission reports, as well as creating custom ones

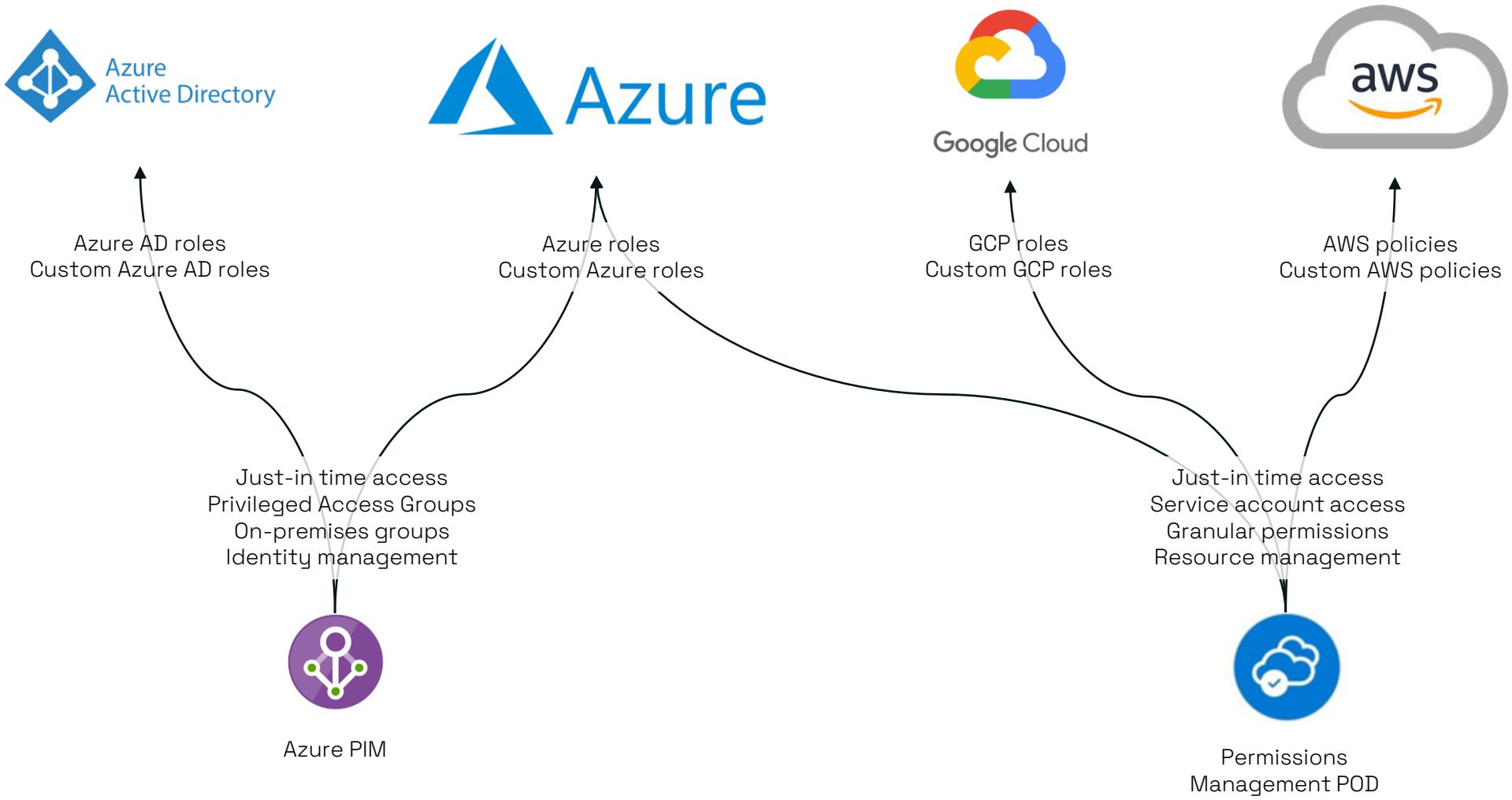


Activity Triggers

- Activity and Anomaly Triggers allow you to configure alerts, based on custom or built-in triggers
- For example, we can create alerts for when a certain user in GCP hits an authorization failure rule, or if overprovisioned users are detected



Azure PIM vs Permissions Management POD



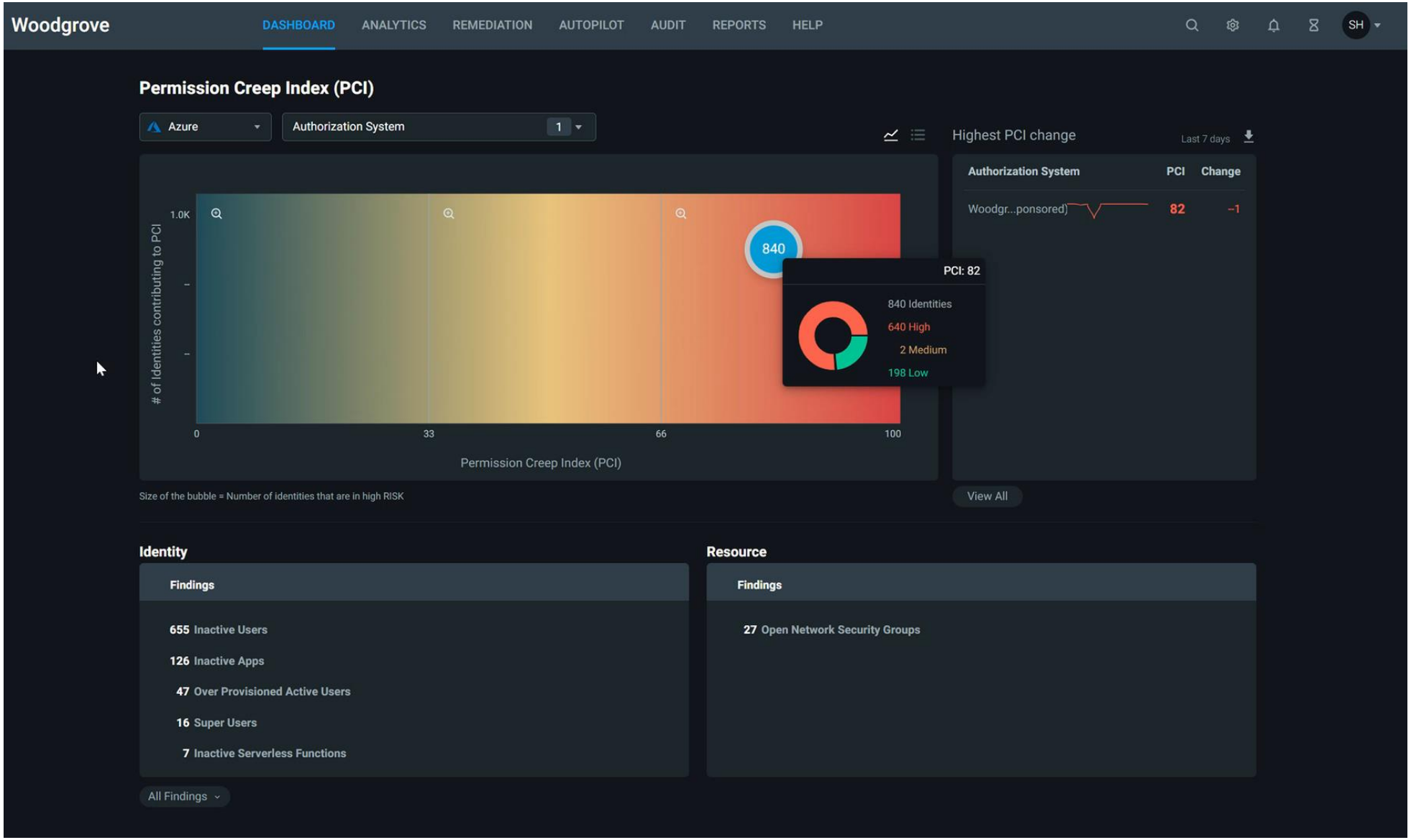
Demo

Shelley Hill

Global Black Belt for Advanced Security Architecture

Microsoft

Demo


Woodgrove
DASHBOARD
ANALYTICS
REMEDIATION
AUTOPILOT
AUDIT
REPORTS
HELP
SH
Permission Creep Index (PCI)
Azure
Authorization System
1
Highest PCI change
Last 7 days
Authorization System
PCI
Change
Woodgr...ponsored)
82
-1
1.0K
# of Identities contributing to PCI
840
PCI: 82
840 Identities
640 High
2 Medium
198 Low
0
33
66
100
Permission Creep Index (PCI)
Size of the bubble = Number of identities that are in high RISK
View All
Identity
Findings
655 Inactive Users
126 Inactive Apps
47 Over Provisioned Active Users
16 Super Users
7 Inactive Serverless Functions
Resource
Findings
27 Open Network Security Groups
All Findings

Permissions Management Pricing

- List price $125 per compute resource, per year
- Resources supported are compute resources, container clusters, serverless functions, and databases across Amazon Web Services, Microsoft Azure, and Google Cloud Platform
- Resource licenses are bought in advance, with any additional resources charged at the following renewal
- It is set to remain a standalone product, not included in the E5 licensing stack

Kocho
BECOME GREATER

Questions?

Summary

- Permissions Management allows you to assess and remediate access, focused around the permission creep index (PCI)
- It is multicloud and includes AWS and GCP as well as Azure
- Roles and permissions can be amended from within the portal, including JIT style requests
- Reporting and alerting allow you to react to potential access issues before they become problematic

Kocho
BECOME GREATER

Thank you

Martyn Gill

Senior Architect

martyn.gill@kocho.co.uk

Tom Urwin

Identity Architect

tom.urwin@kocho.co.uk

hello@kocho.co.uk

0800 044 5009

Links and resources

- PIM Privileged Access Groups
  https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-features
- EPM More Info
  https://aka.ms/PermissionsManagement
- EPM 90-day free trial
  https://aka.ms/TryPermissionsManagement
- EPM Interactive Demo
  https://aka.ms/PermissionsManagementInteractiveDemo