



Understand your identity landscape with Microsoft Entra Permissions Management (CloudKnow)
- Getting a grasp around the landscape- Level 200

Peter Selch Dahl - Cloud Architect



Speaker intro



Peter Selch Dahl
Cloud Architect

Twitter: @PeterSelchDahl
www: www.peterdahl.net
Blog : http://blog.peterdahl.net
Mail : psd@apento.com

Microsoft MCSA: Cloud Platform - Certified 2018,
Microsoft MCSA: Office 365 - Certified 2018,
Microsoft MCSE: Cloud Platform and Infrastructure - Certified 2018
Microsoft MCSA: 2016 Windows Server 2016,
Microsoft MCSA: 2012 Windows Server 2012,
Microsoft MCITP: 2008 Server and Enterprise Administrator,
Microsoft MCSA: 2008 Windows Server 2008,
Microsoft MCSA/MCSE : 2003 Security,
Microsoft MCSA/MCSE : 2000 Security,
VMWare Certified Professional VI3/VI4/VI5,
CompTIA A+, Network+,
EC-Council: Certified Ethical Hacker (CEH v7),
And more



Understand your identity landscape with Microsoft Entra Permissions Management

Hold gerne mødet interaktivt! Stil gerne spørgsmål

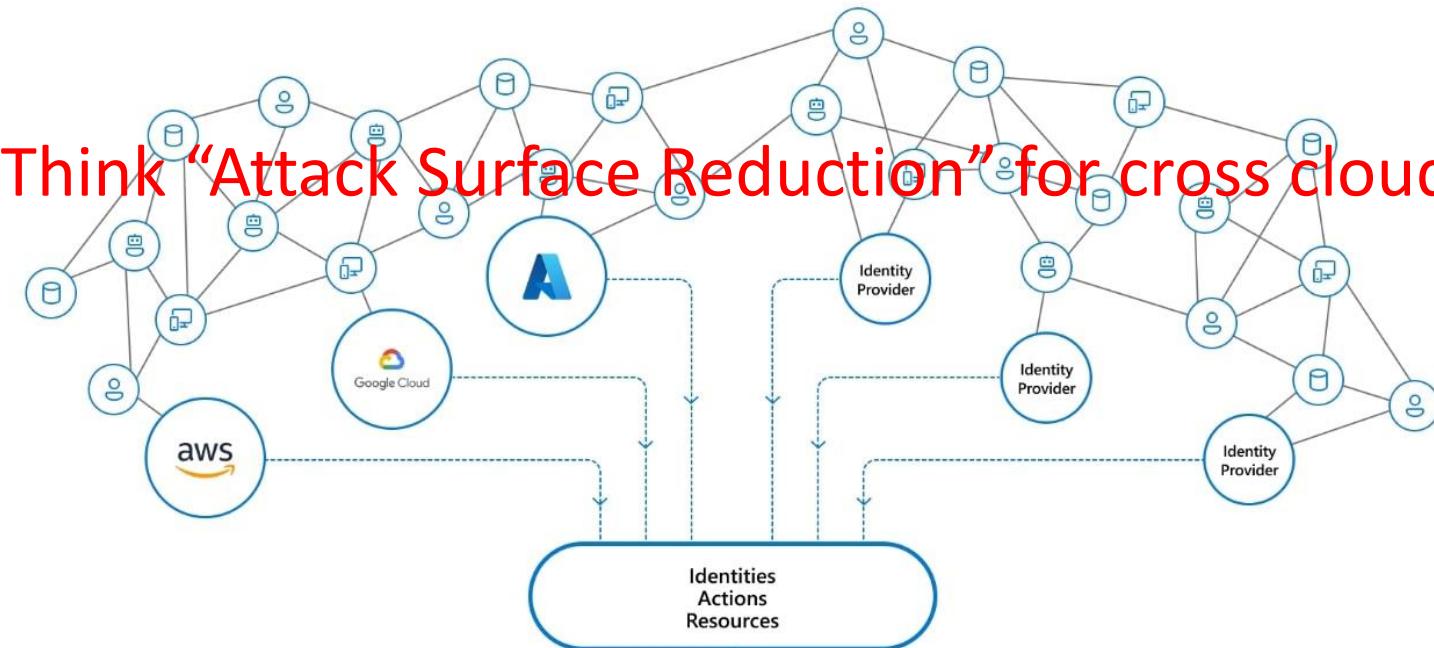




Understand your identity landscape with Microsoft Entra Permissions Management

Why do we need a new tool for managing the landscape?

Think “Attack Surface Reduction” for cross cloud!



Improve your security posture by ensuring the principle of least privilege across identities and resources in your IaaS infrastructure

Microsoft Entra Permissions
Management





Understand your identity landscape with Microsoft Entra Permissions Management

- Doing a large deployment af 20.000+ users company.
 - Azure Subscriptions
 - Amazon AWS Subscription
 - Google Subscriptions
 - YouTube
 - GCP
 - Etc.
- Part of the "Microsoft Entra Permissions Management Advisors"
- Clean Up of privileges – New job role, vendors, subcontractors, employees, etc.

Technologies that I will talk about today....



For Context and understanding

- Cloud Identities – Explosion
- Enterprise App Consent
- Defender for Cloud Apps (MCAS) – Shadow IT
- Azure AD Access Review
- Azure AD PIM for Everything (ex. SAP)

What we solve with:

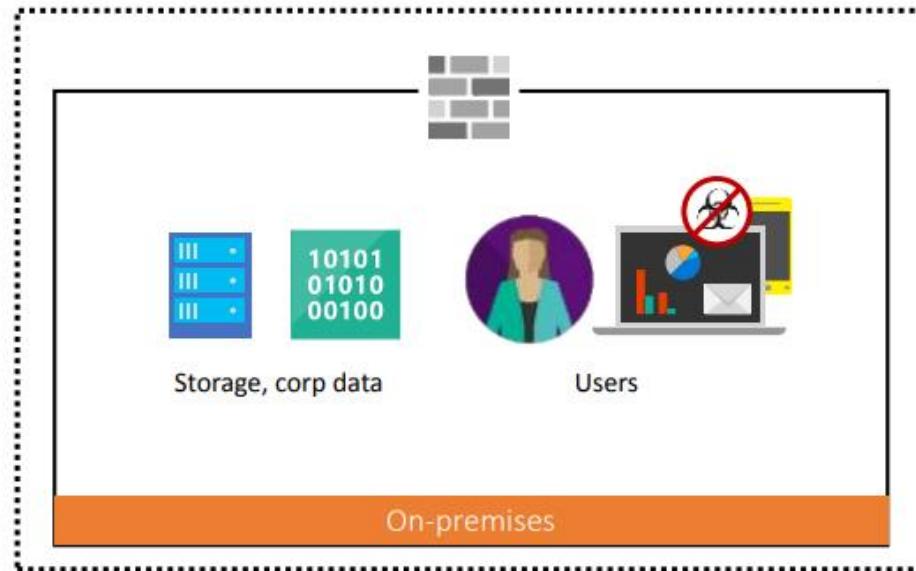
- Entra Permission Management (CloudKnow)

Questions

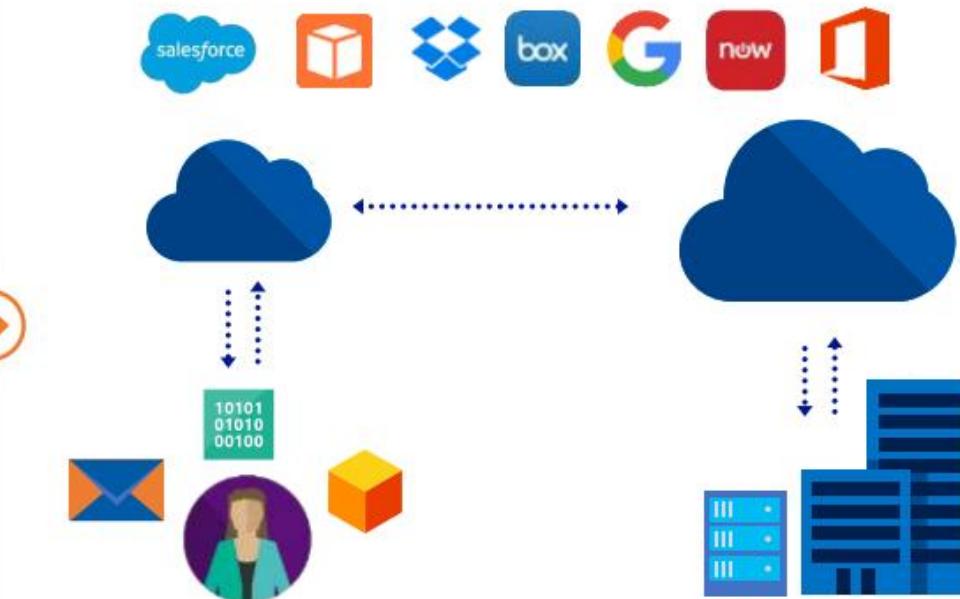
- And more – Expert Panel AMA ☺

Understand your identity landscape with Microsoft Entra Permissions Management

Life before cloud



Life with cloud



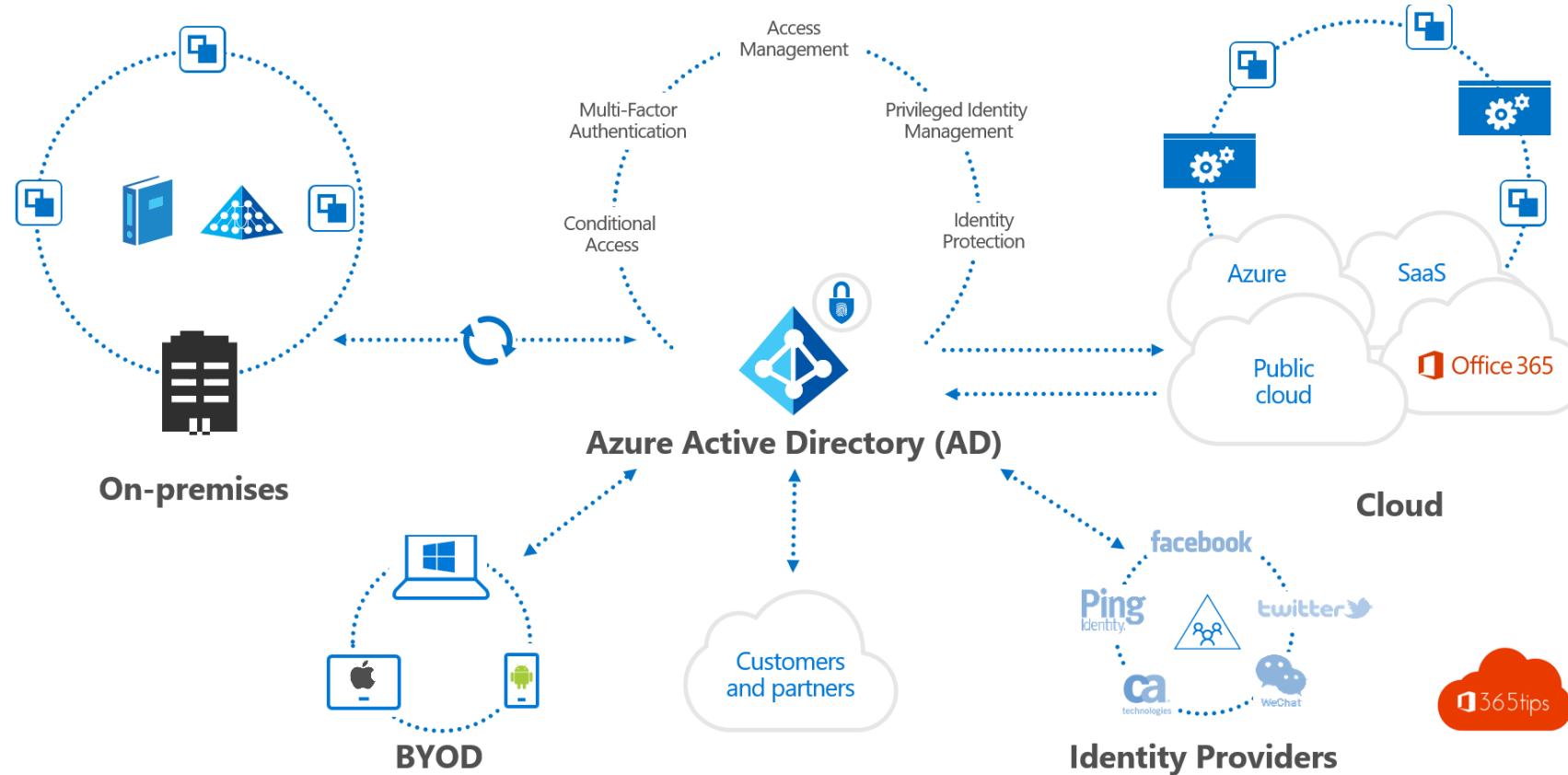
- Only sanctioned apps are installed
- Resources accessed via managed devices/networks
- IT had layers of defense protecting internal apps
- IT has a known security perimeter

- User chooses apps (unsanctioned, shadow IT)
- User can access resources from anywhere
- Data is shared by user and cloud apps
- IT has limited visibility and protection



Understand your identity landscape with Microsoft Entra Permissions Management

Azure Conditional Access, Azure AD PIM, Azure Access Review, etc.

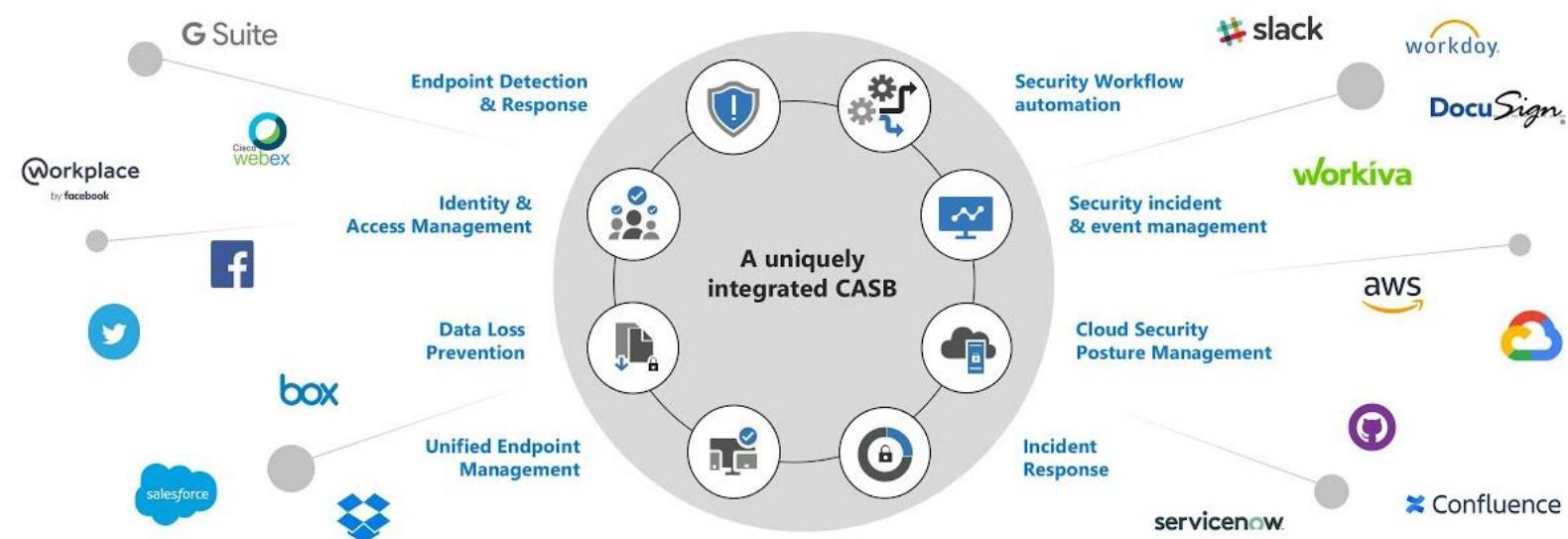




Understand your identity landscape with Microsoft Entra Permissions Management

Defender for Cloud Apps

Provides insight into shadow cloud apps





Understand your identity landscape with Microsoft Entra Permissions Management

What roles, access and application do I have assigned?

The screenshot shows two side-by-side views of the Microsoft Entra admin center.

Left View: The user is viewing their assigned roles for the user "Peter Selch Dahl". The "Assigned roles" section is highlighted with a red box. It shows two active assignments:

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Application Administrator	psd@apento.com	Directory	Direct	Active	3/23/2021, 2:52:26 PM	Permanent	Remove Update
Global Administrator	psd@apento.com	Directory	Direct	Active	12/9/2022, 4:20:11 AM	12/9/2022, 8:20:11 PM	Remove Update

Right View: The user is viewing their Azure role assignments. The "Azure role assignments" section is highlighted with a red box. It shows four assignments across different resources:

Role	Resource Name	Resource Type	Assigned To
Owner	APENTO - Microsoft Azure Sponsorship	Subscription	Subscription admins
Owner	APENTO-DesktopAnalytics	Log Analytics workspace	M365 Analytics Client Admins (Log ...)
Owner	APENTO - Microsoft Azure Spo...	Subscription	Peter Selch Dahl
Desktop Virtualization User	apento-wvd-customer-hostpo...	Application group	Peter Selch Dahl

Do I still need these permissions and do I use them?

What about other SaaS Apps? GCP, AWS, VMware, etc.?



Hard to understand the
landscape



Understand your identity landscape with Microsoft Entra Permissions Management

Management capabilities for Privileged Access groups (preview) and Azure AD Connect group writeback (Refresh)



Azure AD Privileged Identity Management

A screenshot of the Microsoft Azure portal showing the "My roles | Privileged access groups (Preview)" page. It displays a list of assignments under the "Eligible assignments" tab, with a search bar and sorting options for Role, Group, and Group type. A note at the bottom mentions "SAP, AWS, GCP, Etc." and "Domain Admin - Group WriteBack".

A screenshot of the SAP Integration Suite interface. The main screen shows a welcome message: "Welcome to SAP Integration Suite Simplify and accelerate enterprise integration". A modal dialog box in the top right corner says "Your session has expired. Press OK to login again." with an "OK" button.



Understand your identity landscape with Microsoft Entra Permissions Management

Least privilege access principle for users and workload identities.

TECH 1/14/2014 @ 12:03PM | 4,378 views

Attackers Scrape GitHub For Cloud Service Credentials, Hijack Account To Mine Virtual Currency

My \$2375 Amazon EC2 Mistake

Bots Scanning GitHub To Steal Amazon EC2 Keys

Posted by [Soulskill](#) on Friday January 02, 2015 @11:09PM from the [with-many-bots-all-virus-are-shallow](#) dept.

New submitter [uniq](#) writes:

As one developer found out, [posting your Amazon keys to GitHub on accident can be a costly mistake if they are not revoked immediately.](#)

My \$500 Cloud Security Screwup—UPDATED

Analysis, Security, Best Practices, Bitcoin, Hacking

WHY EXPOSED API KEYS AND SENSITIVE DATA ARE GROWING CAUSE FOR CONCERN

CRYPTOCURRENCY JACKING —

Tesla cloud resources are hacked to run cryptocurrency-mining malware

Crooks find poorly secured access credentials, use them to install stealth miner.

DAN GOODIN - 2/20/2018, 8:21 PM



Understand your identity landscape with Microsoft Entra Permissions Management

Azure Access Review

The screenshot displays four overlapping windows from the Microsoft Entra Permissions Management interface:

- Groups:** Shows a list of selected groups: Accounting Dept, All Guests, All Intune Licensed Users, Azure, CalebGroup, Chris group, Custom Medium Risk Group, Enterprise Social Apps, Legal Dept, MobileTeam, Sales Team, and Sales Team and 6 others.
- Apps:** Shows a list of selected applications: Salesforce, ServiceNow, and Twitter.
- Azure AD Roles:** Shows a list of selected roles: Application Administrator, Application Developer, and Authentication Administrator.
- Azure Resource Roles:** Shows a list of selected roles: AcDeleteV2-Test, AcrPush, and AcRPull.

The background shows the main "Create an access review" page with settings like Review name, Start date, Duration (in days), and Users to review.

The bottom right window shows the "Access reviews" blade for the "License_Visio_Online_P2" group, listing one active review entry:

Name	Resource	Status	Created On
Licence - Visio Online P2	Group License_Visio_Online_P2	Active	3/14/2019



Understand your identity landscape with Microsoft
Entra Permissions Management

Building Great Cloud Security Guardrails

A photograph of a long, horizontal guardrail made of metal poles and red and white striped plastic covers. The guardrail stretches across a dry, brown field. In the background, there is a vast, cloudy sky at either sunrise or sunset, with orange and blue hues.



Understand your identity landscape with Microsoft Entra Permissions Management

Getting started with Entra Permission Management

1. Go to the Microsoft Entra portal "<https://entra.microsoft.com>"
2. Click "Permissions Management"
3. Enabled 90 Days Trial
4. Check your assets and the cost! 😊

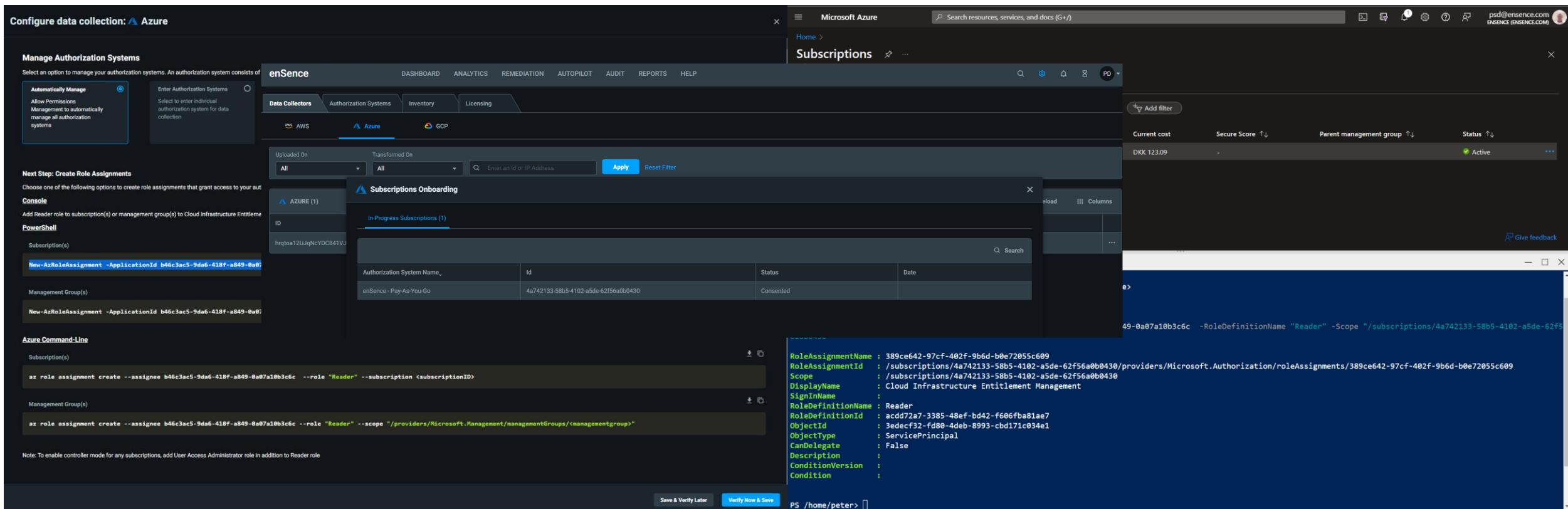
A screenshot of the Microsoft Entra admin center interface. The left sidebar shows navigation options like Home, Azure Active Directory, Users, Groups, Devices, Applications, Protect & secure, Identity Governance, External Identities, and Permissions Management. The main area displays the Microsoft Entra admin center logo and a brief description of securing identity infrastructure.

A screenshot of the Entra Permissions Management trial page. It shows a red warning message: "You must have a license to use Entra Permissions Management". Below it, the "Welcome to Entra Permissions Management" heading is visible, along with a note about needing a trial or license and a link to sign up for a free 90-day trial.



Understand your identity landscape with Microsoft Entra Permissions Management

- Onboard Azure in seconds 😊



The screenshot displays the enSense platform integrated with Microsoft Azure. On the left, the 'Subscriptions Onboarding' section shows a table with one entry: 'enSense - Pay-As-You-Go' with ID '4a742133-58b5-4102-a5de-62f56a0b0430'. The status is 'Consented'. On the right, the 'Microsoft Azure' interface shows the 'Subscriptions' blade with a single subscription listed. Below the subscriptions, the 'Azure Command-Line' section shows PowerShell commands for creating role assignments:

```
az role assignment create --assignee b46c3ac5-9da6-418f-a849-0a07a10b3c6c --role "Reader" --subscription <subscriptionID>
az role assignment create --assignee b46c3ac5-9da6-418f-a849-0a07a10b3c6c --role "Reader" --scope "/providers/Microsoft.Management/managementGroups/<managementgroup>"
```

A detailed JSON object is shown at the bottom right, representing a role assignment:

```
RoleAssignmentName : 389ce642-97cf-402f-9b6d-b0e72055c609
RoleAssignmentId : /subscriptions/4a742133-58b5-4102-a5de-62f56a0b0430/providers/Microsoft.Authorization/roleAssignments/389ce642-97cf-402f-9b6d-b0e72055c609
Scope : /subscriptions/4a742133-58b5-4102-a5de-62f56a0b0430
DisplayName : Cloud Infrastructure Entitlement Management
SignInName :
RoleDefinitionName : Reader
RoleDefinitionId : acdd72a7-3385-48ef-bd42-f606fba81ae7
ObjectId : 3edecf32-fd80-4deb-8993-cbd171c034e1
ObjectType : ServicePrincipal
CanDelegate :
Description :
ConditionVersion :
Condition :
```



Understand your identity landscape with Microsoft Entra Permissions Management

- Onboard Azure in seconds ☺

The screenshot displays two views of the enSense platform interface.

Top View: Shows the "Subscriptions Onboarding" section under the "Authorization Systems" tab. It lists one "In Progress Subscriptions" entry:

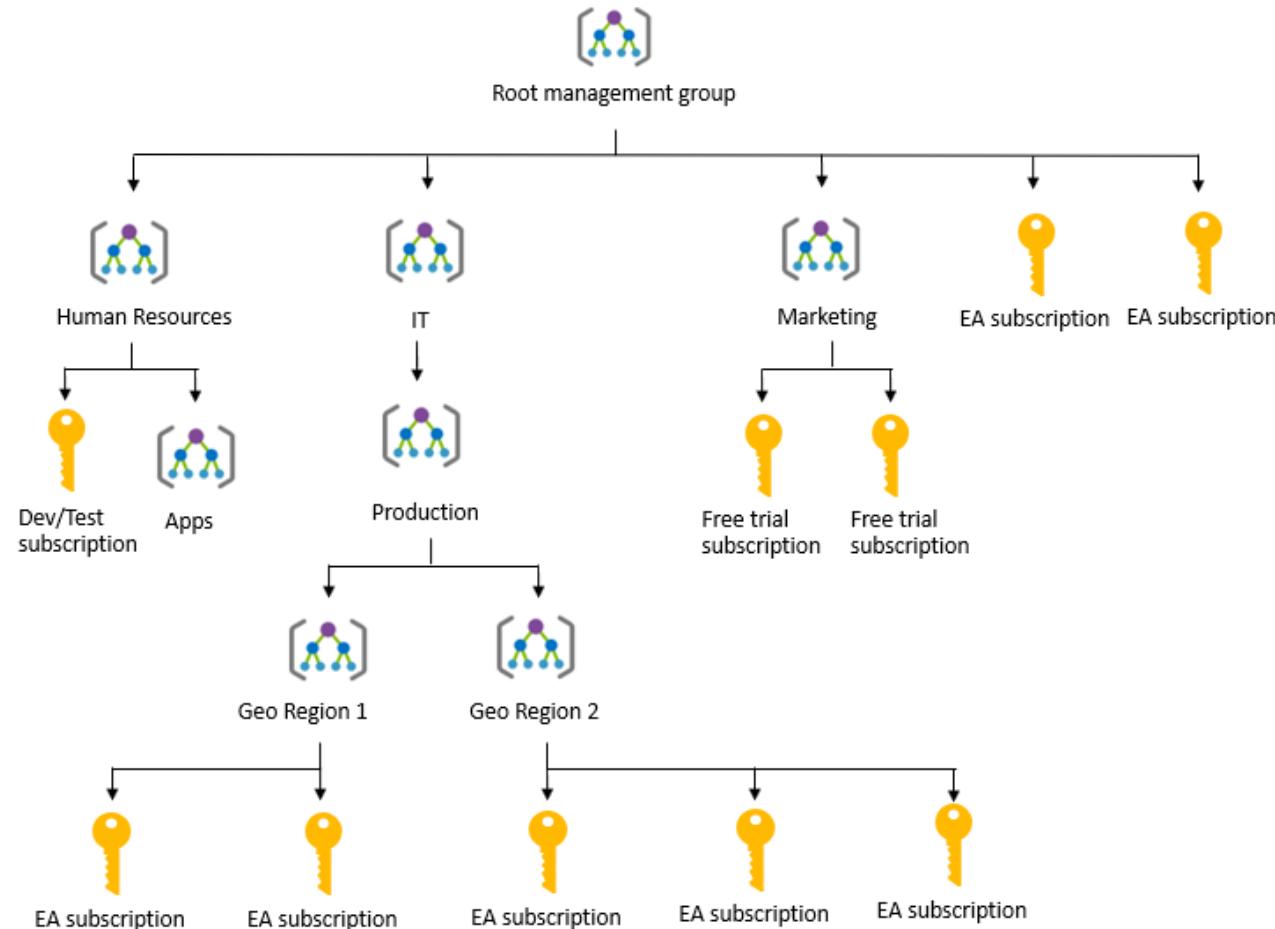
Authorization System Name	ID	Status	Date
enSense - Pay-As-You-Go	4a742133-58b5-4102-a5de-62f56a0b0430	Consented	

Bottom View: Shows the "Authorization Systems" list view. It lists one entry under the "Azure" controller:

Name	ID	Controller Status	Entitlements Status
enSense - Pay-As-You-Go	4a742133-58b5-4102-a5de-62f56a0b0430	Disabled	-



Understand your identity landscape with Microsoft Entra Permissions Management



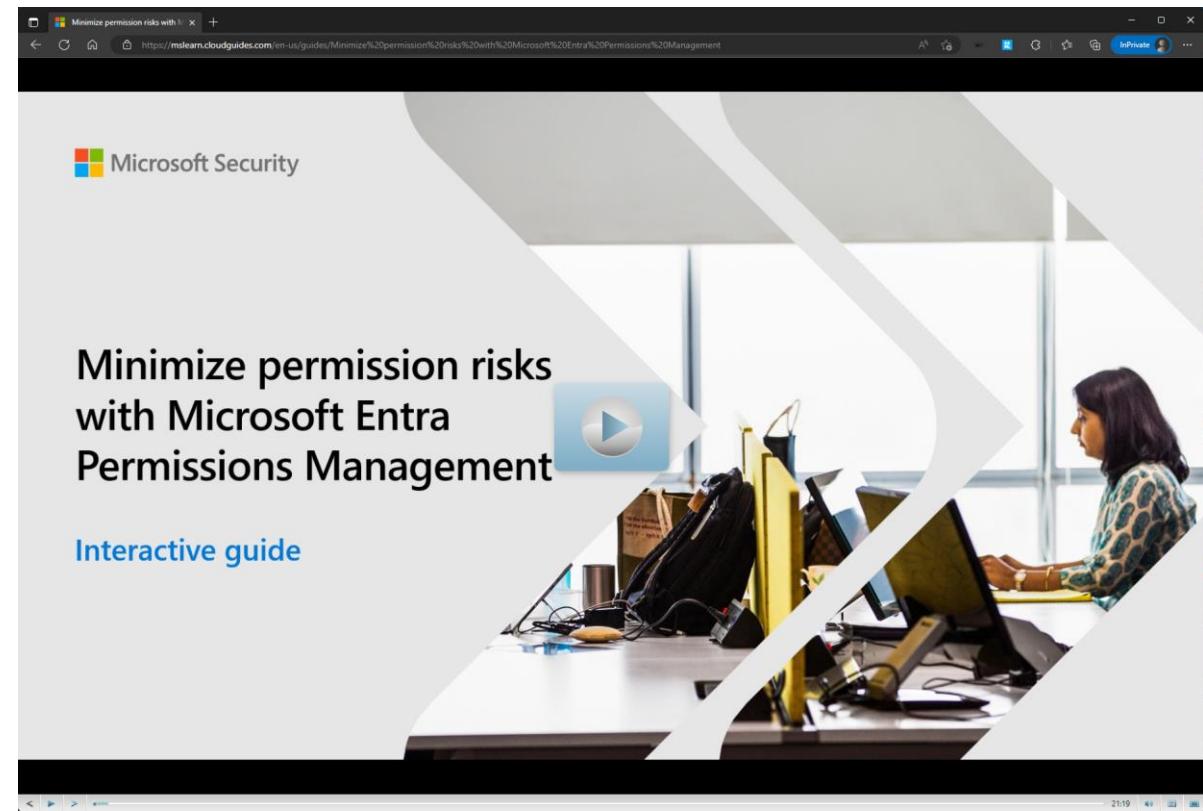
```
New-AzRoleAssignment -ApplicationId b46c3ac5-9da6-418f-a849-0a07a10b3c6c -RoleDefinitionName "Reader" -Scope "/providers/Microsoft.Management/managementGroups/<managementgroup>"
```



Understand your identity landscape with Microsoft Entra Permissions Management

Play around without now trial needed ☺

1. Go to <https://425.show/epm-click-thru>
2. Try EPM today ☺





Understand your identity landscape with Microsoft Entra Permissions Management

- Licensing

EPM is “Asset” based licensing!

**Microsoft Entra
Permissions
Management**
\$10.40 resource/month

[Buy now](#)
[Try for free >](#)

Microsoft Entra Permissions Management allows you to:

- Get a multi-dimensional view of your risk by assess identities, permissions and resources.
- Automate least privilege policy enforcement consistently in your entire multicloud infrastructure.
- Prevent data breaches caused by misuse and malicious exploitation of permissions with anomaly and outlier detection.

Resources supported¹: common resources, container clusters, serverless functions, and databases across Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

Free 90-Day Trial Available: Try Permissions Management for free and run a risk assessment to identify the top permission risks across your multicloud infrastructure.

Microsoft 365 E5 License

A photograph showing a man with long dark hair and a beard, wearing a teal shirt, standing behind a woman with curly hair, wearing a white top. They are both looking at a computer monitor on a desk. The monitor displays some graphical interface. The background is a warm-toned room.

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



Understand your identity landscape with Microsoft Entra Permissions Management

Monitoring “Assets”

Navigate to the Resource

Graph: <https://portal.azure.com/#view/HubsExtension/ArgQueryBlade>

“Make sure you select the right scope, the directory would be a good one as it gives all resources. You can change it a certain management group as well.”

Paste this KQL query:

```
resources
| project name, resourceGroup, location, type, kind, subscriptionId, tags
| join kind=leftouter (resourcecontainers
| where type == "microsoft.resources/subscriptions"
| project SubID=subscriptionId, SubName = name)
on $left.subscriptionId == $right.SubID
| project name, resourceGroup, location, type, kind, SubID, tags, SubName
| where type in ("microsoft.compute/virtualmachines","microsoft.web/sites","microsoft.servicefabric/clusters","microsoft.servicefabricmesh/applications","microsoft.kubernetes/connectedclusters","microsoft.sql/servers","microsoft.sql/servers/databases","microsoft.cache/redis","microsoft.documentdb/databaseaccounts")
| project name, resourceGroup, location, type, kind, SubID, tags, SubName
```

AZURE (3)	Compute (1)	Serverless (2)	Compute Containers (0)	Databases (0)	Total Number of Licenses (3)
enSence - Pay-As-You-Go (3)	1	2	0	0	3
	VM (1)	Azure Function (2)	Container instances (0) Kubernetes services (0) Mesh applications (0) Service Fabric clusters (0)	Azure Cache for Redis (0) Cosmos DB (0) SQL databases (0) SQL servers (0)	

Microsoft Entra Permissions Management

- Get granular cross-cloud visibility
- Enforce principle of least privilege
- Continuously monitor permissions



Multicloud adoption brings new permission challenges



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



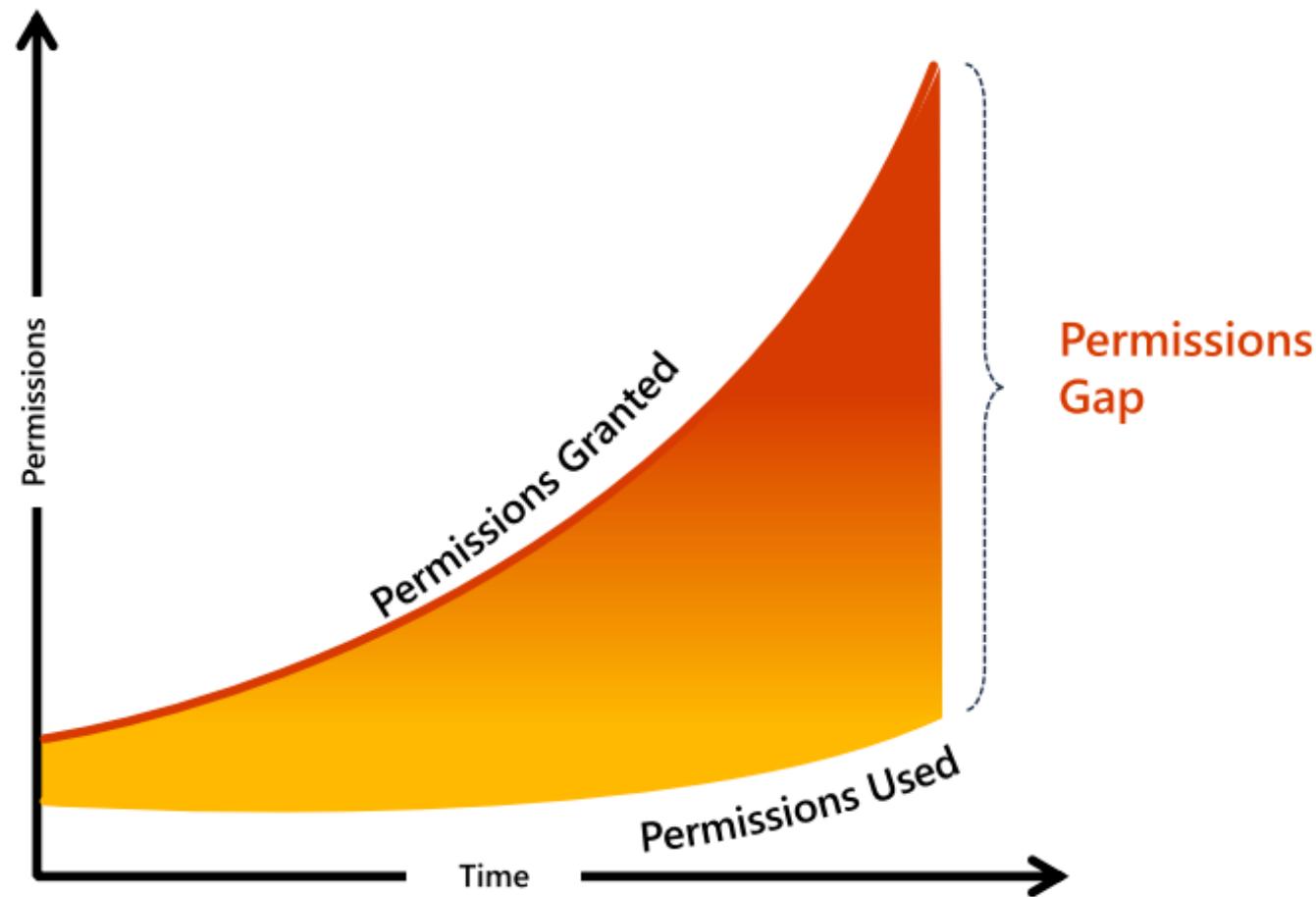
>90% of identities are using <5% of permissions granted



>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

IAM admins manually grant permissions
which are not time-bound

Permission clean-up is done manually
on an as-needed basis

A new, dynamic
approach



Grants permissions based on
historical usage and activity



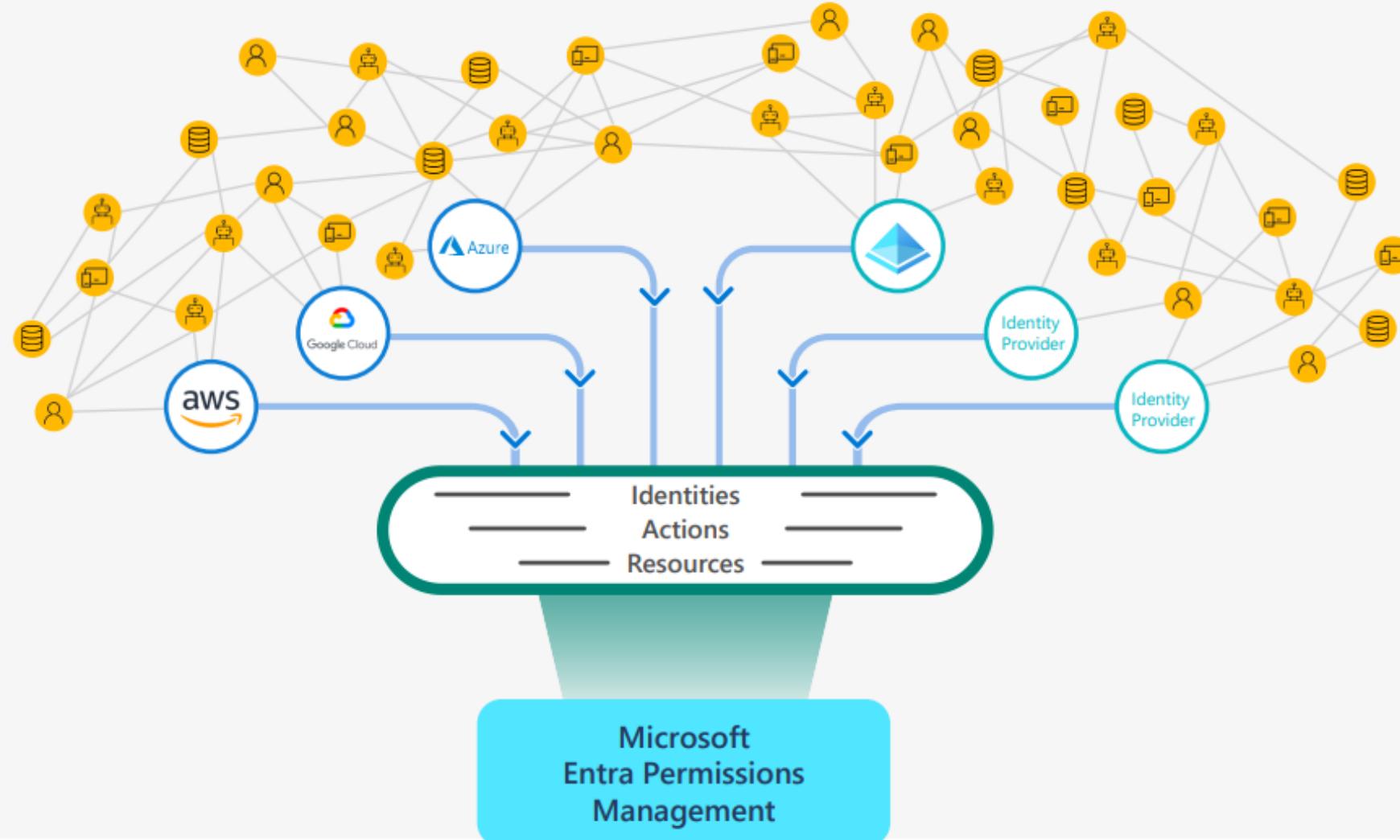
Allow temporary access to high-risk
permissions on-demand



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.



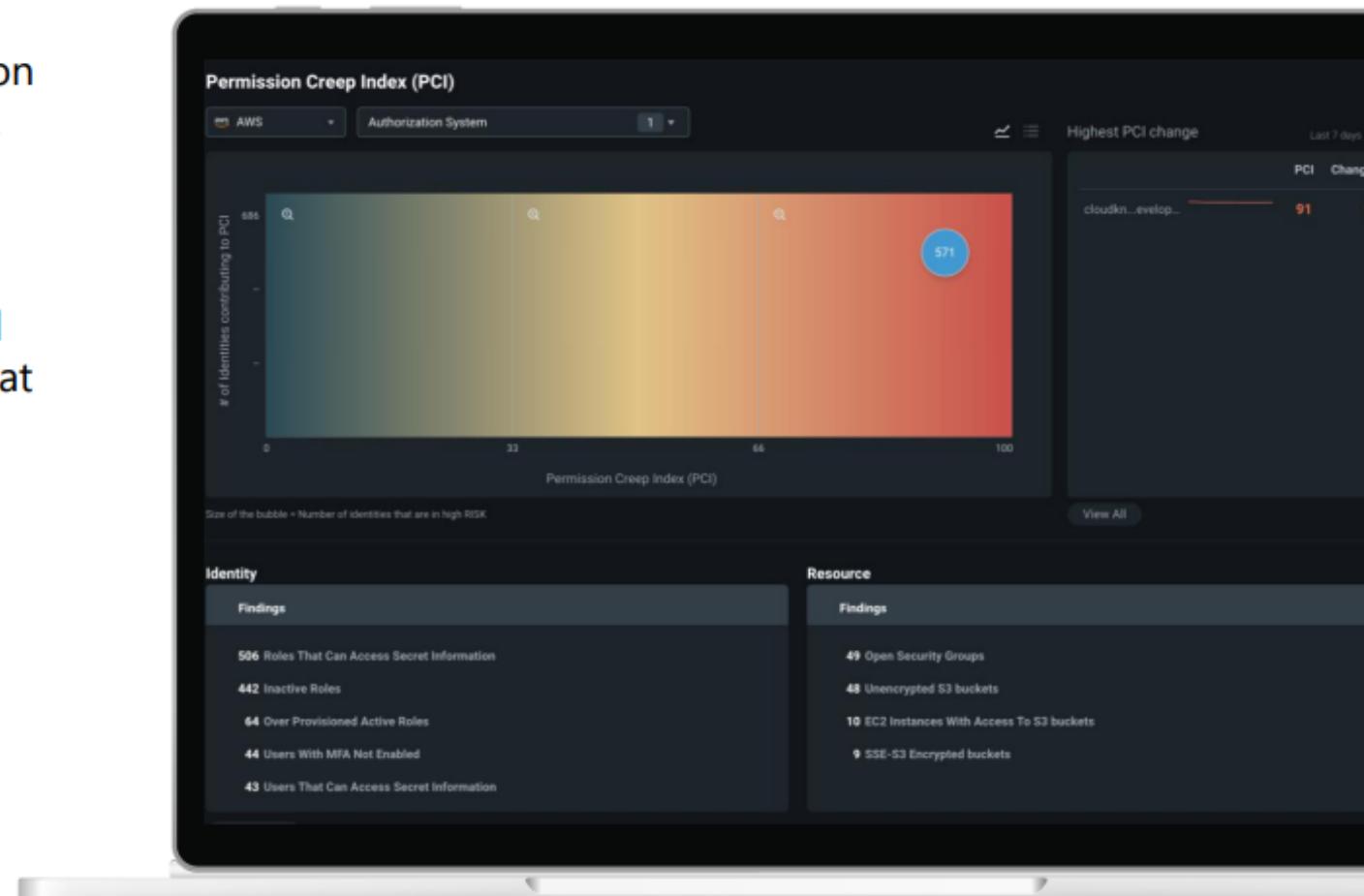
Remediate

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

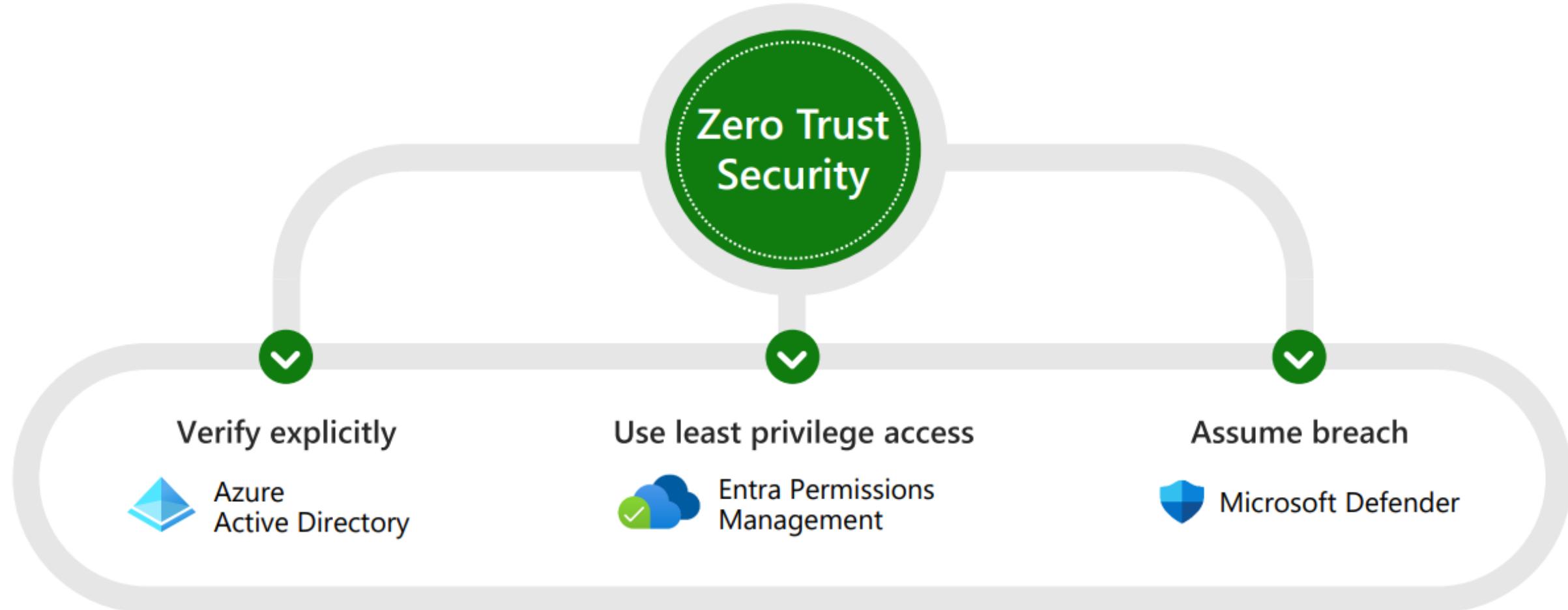


Monitor

Detect anomalous permission usage and generate detailed forensic reports.

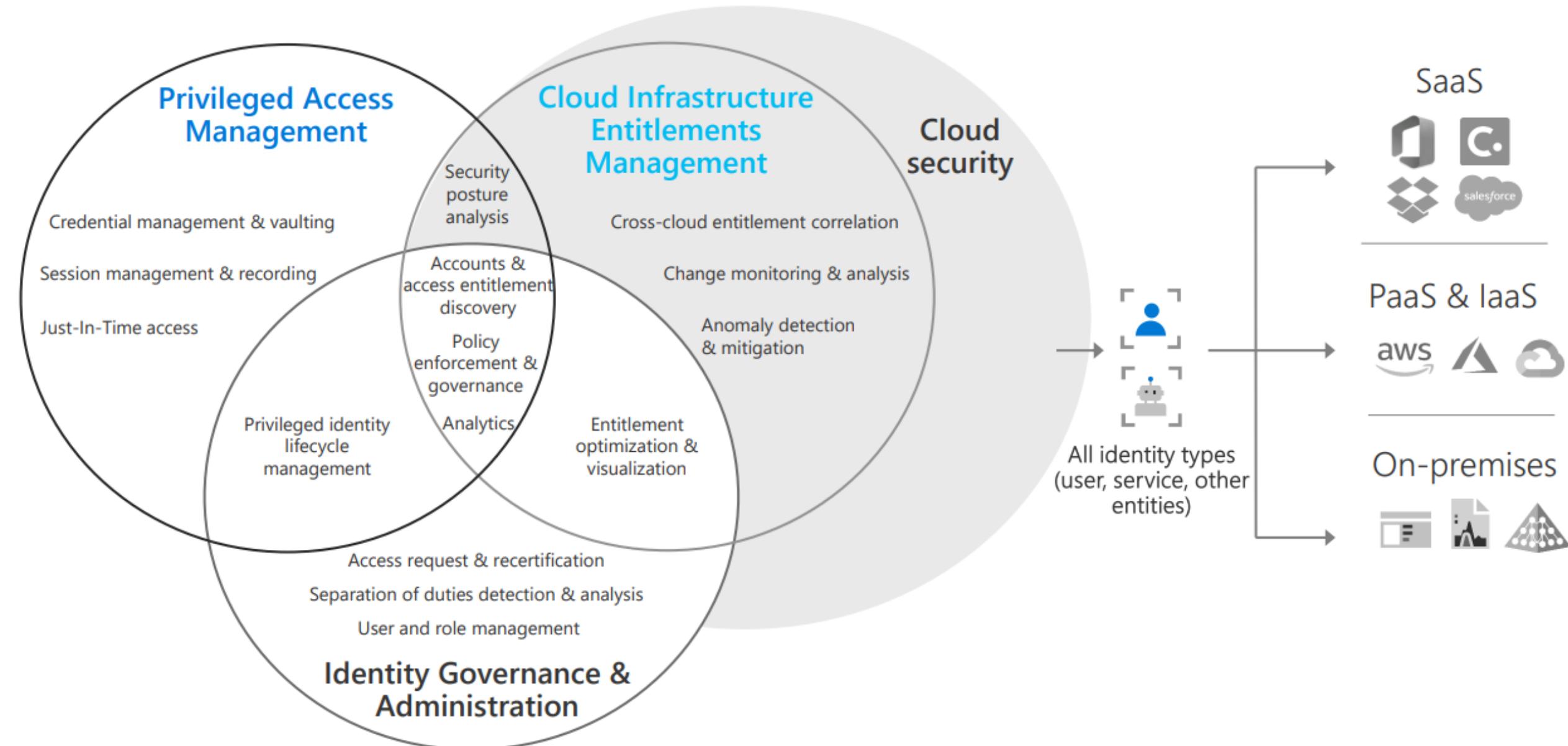


Entra Permissions Management empowers Zero Trust

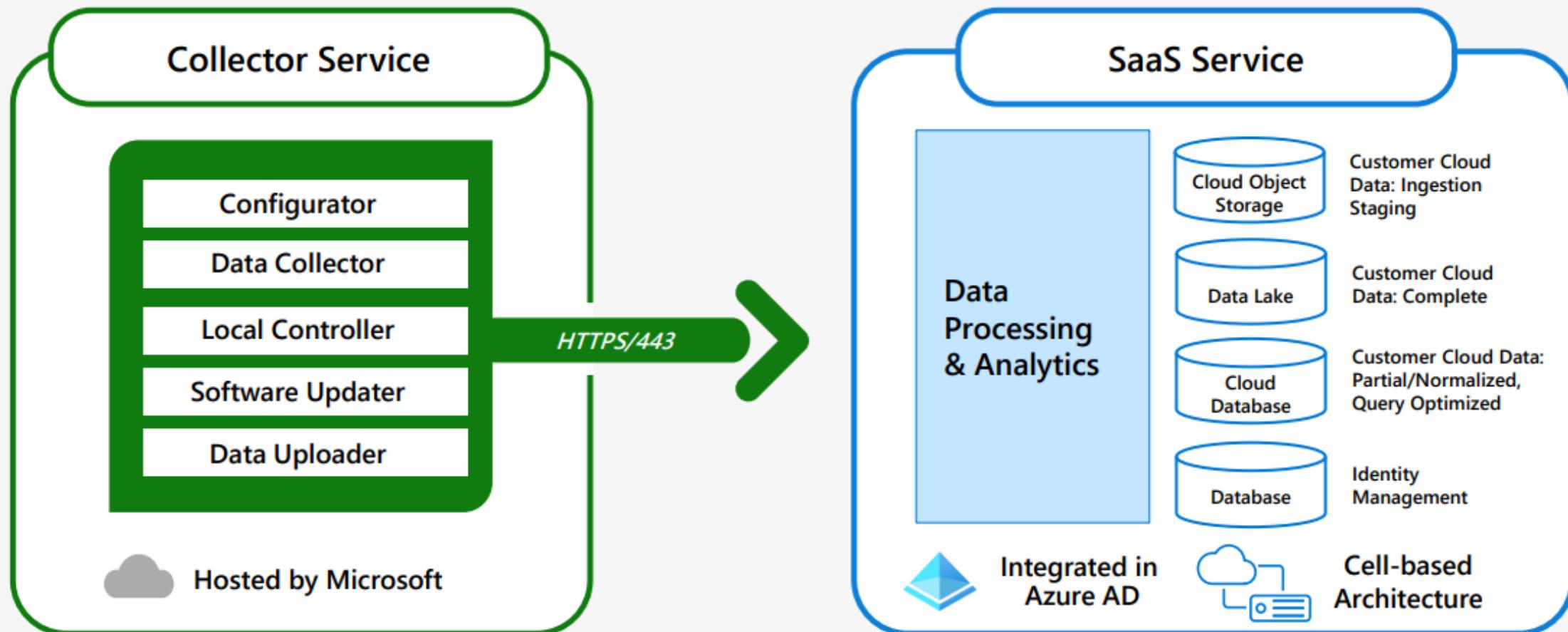


Multicloud | Multi-Platform

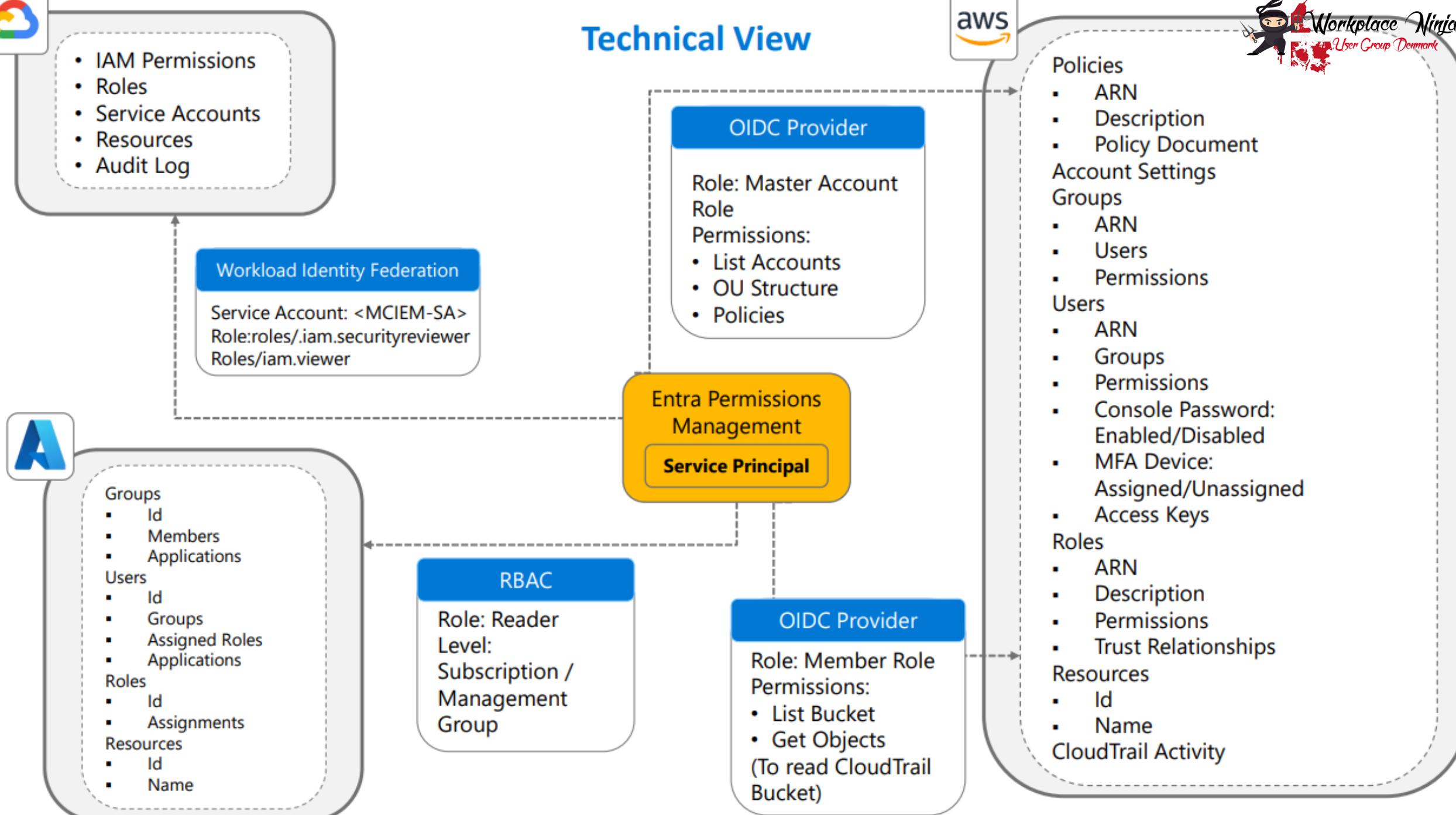
The CIEM complements PAM & IGA



Product Architecture



Technical View

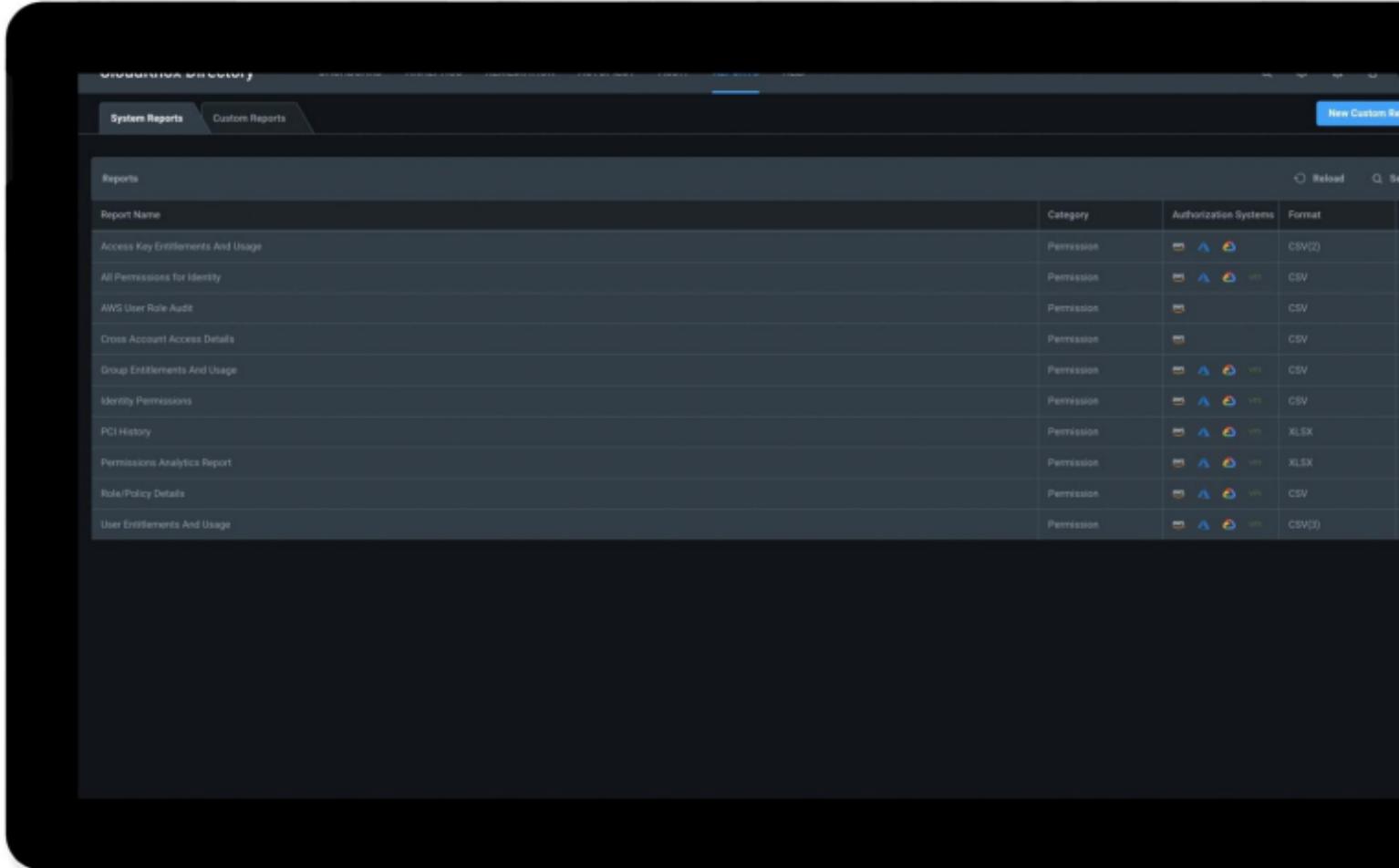


Risk Assessment Key Findings

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 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



Report Name	Category	Authorization Systems	Format
Access Key Entitlements And Usage	Permission	AWS, Lambda, VPC	CSV(2)
All Permissions for Identity	Permission	AWS, Lambda, VPC	CSV
AWS User Role Audit	Permission	AWS	CSV
Cross Account Access Details	Permission	AWS	CSV
Group Entitlements And Usage	Permission	AWS, Lambda, VPC	CSV
Identity Permissions	Permission	AWS, Lambda, VPC	CSV
PCI History	Permission	PCI	XLSX
Permissions Analytics Report	Permission	AWS, Lambda, VPC	XLSX
Role/Policy Details	Permission	AWS, Lambda, VPC	CSV
User Entitlements And Usage	Permission	AWS, Lambda, VPC	CSV(3)

Permission Creep Index (PCI)

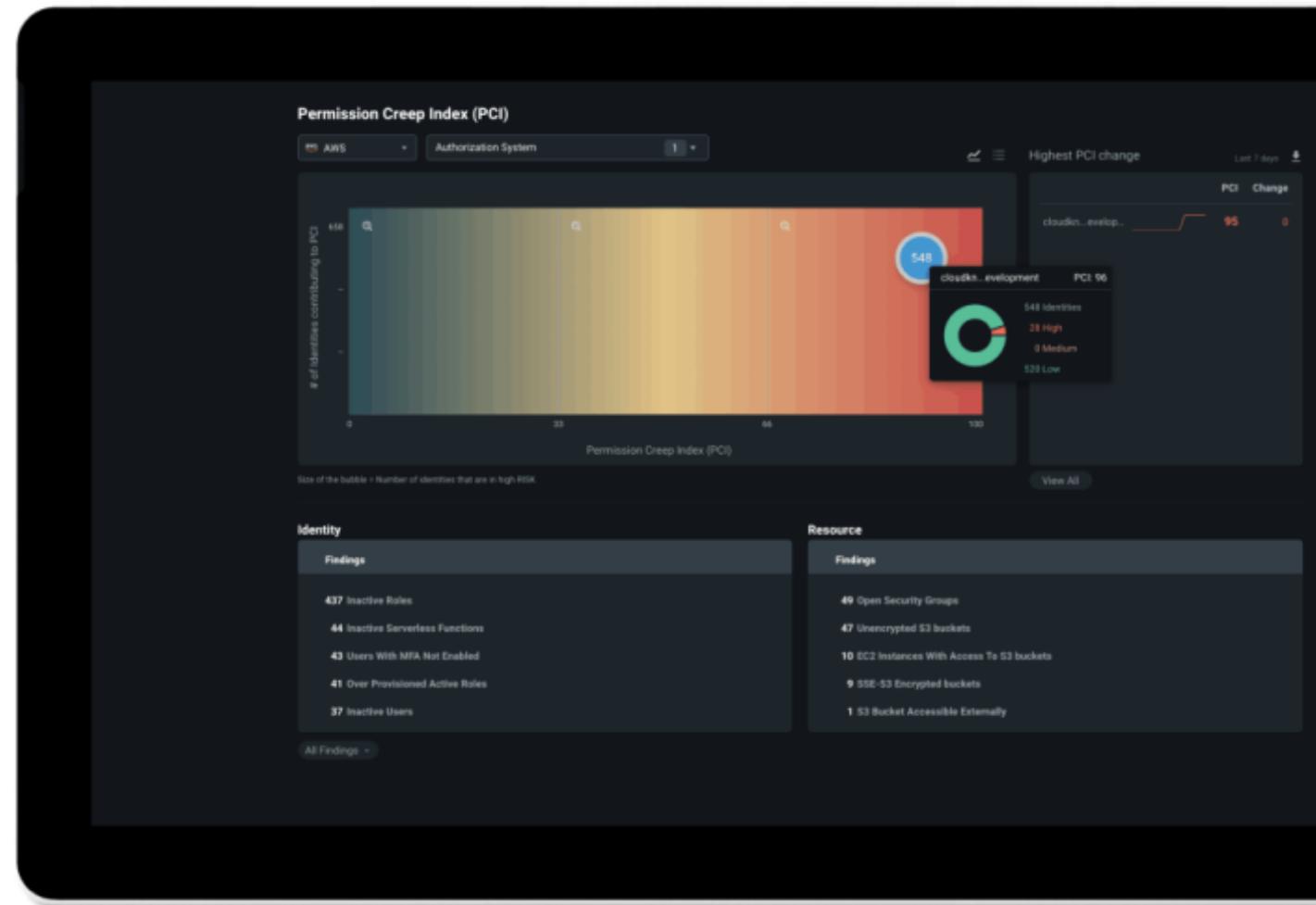
What is it?

An aggregated metric (0-100) that evaluates the level of risk associated with permissions across identities and resources by comparing permissions granted vs. permissions used.

How is it calculated?

The PCI formula considers

- Permissions Gap
- Unused high-risk permissions
- Resource reach



Permissions Creep Index (PCI)

What is it?

An aggregated metric that evaluates the level of risk associated with permissions across identities and resources by comparing permissions granted vs. permissions exercised.

How is it calculated?

The Permissions Creep Index is calculated by a formula with two terms multiplied together for a given identity:

- A factor score between 0 to 100 based on high-risk permissions an identity has not used within the last 90 days
- A factor score between 0 to 100 based on how many resources the identity can impact across the entire authorization system. [Learn more here.](#)

What metrics do not contribute to the PCI?

Identities with "read-only" roles or "exclude from PCI" tags will not increase the PCI.

Woodgrove

DASHBOARD

ANALYTIC

REMEDIATION

AUTOPIL

AU

IT REPORT

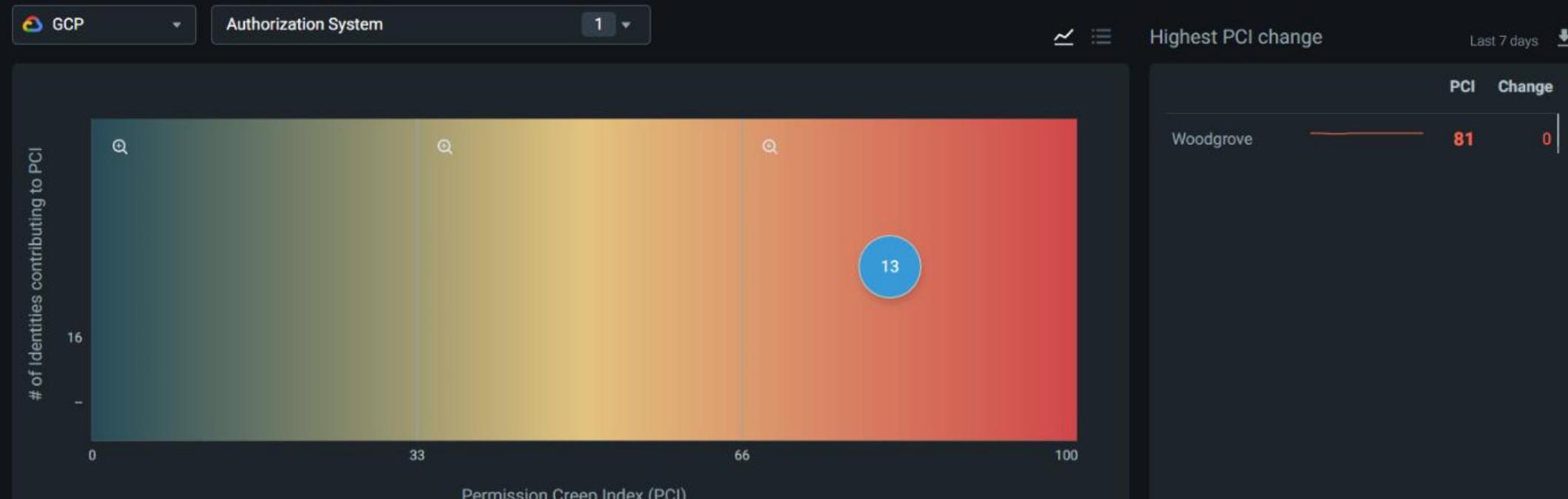
S HE

Q



AW

Permission Creep Index (PCI)



Identity

Findings

9 Privilege Escalation Service Accounts

6 Inactive Users

6 Super Users

2 Over Provisioned Active User

Resource

Finding

Findings are not available

Permission Creep Index (PCI)

Azure

Authorization System

1



Highest PCI change

Last 7 days



< Woodgrove



706 Total Users
554 High
0 Medium
152 Low



14 Total Applications
4 High
0 Medium
10 Low



5 Total Managed Identities
0 High
0 Medium
5 Low

PCI Trend

PCI
76

100

50

0

Apr 19, 2022

Weeks

Woodgrove

76

0

Identity

Findings

643 Inactive Users

84 Inactive Apps

63 Over Provisioned Active Users

12 Super Users

Resource

Findings

33 Microsoft Managed Keys

23 Open Network Security Groups

6 Blob Containers Accessible Externally



Understand your identity landscape with Microsoft Entra Permissions Management



Questions and Answers

THANK YOU!



Join Microsoft Entra Permissions Management Advisors

Become part of the advisor community!

The screenshot shows the Microsoft Teams interface for the "Entra Permissions Management Advisors" group. The header includes the group name, a blue checkmark icon, and a "PRIVATE" label. A "Joined" button is visible. Below the header, there are tabs for "NEW CONVERSATIONS", "ALL CONVERSATIONS", "FILES", and "SEARCH". The main content area displays a post from Sophia Pandey, dated 22 hours ago, announcing an upcoming session on June 29th. The post includes a detailed session description about Microsoft Entra Permissions Management. Below the post, there are buttons for "LIKE", "REPLY", "SHARE", "EDIT", and "...". The post has been seen by 20 people. On the right side of the screen, there are sections for "MEMBERS (104)", "INFO", "GROUP ACTIONS", "NETWORK RESOURCES", and "RELATED GROUPS". The "INFO" section contains a brief description of the group's purpose and a note about NDA status.

<https://aka.ms/EntraPermissionsManagementAdvisors>

Join <http://425.show/epm-advisors>

A shift in IT focus.....

