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

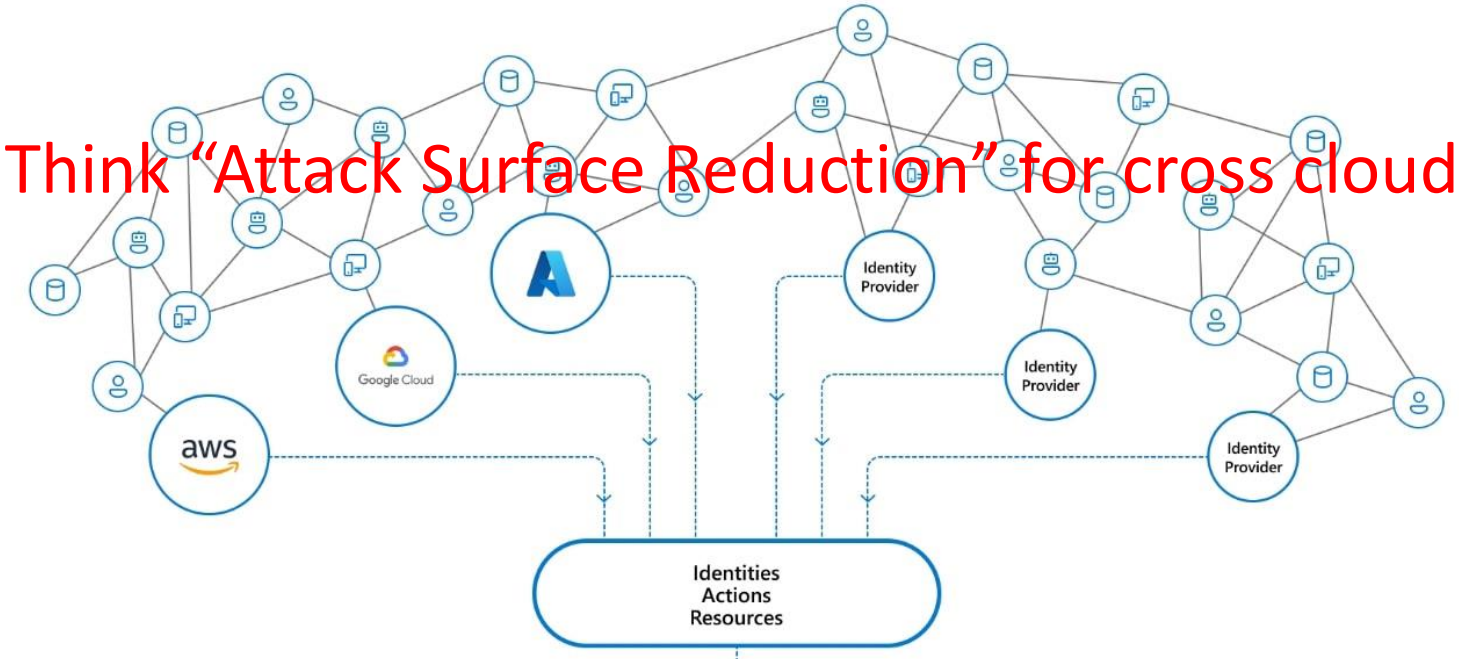
Microsoft MCSA: Cloud Platform - Certified 2018,
Microsoft MCSA: Office 365 - Certified 2018,
Microsoft MCSE: Cloud Platform and Infrastructure - Certified 2018
Microsoft MCSA: 2016 Windows Server 2016,
Microsoft MCSA: 2012 Windows Server 2012,
Microsoft MCITP: 2008 Server and Enterprise Administrator,
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?



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:

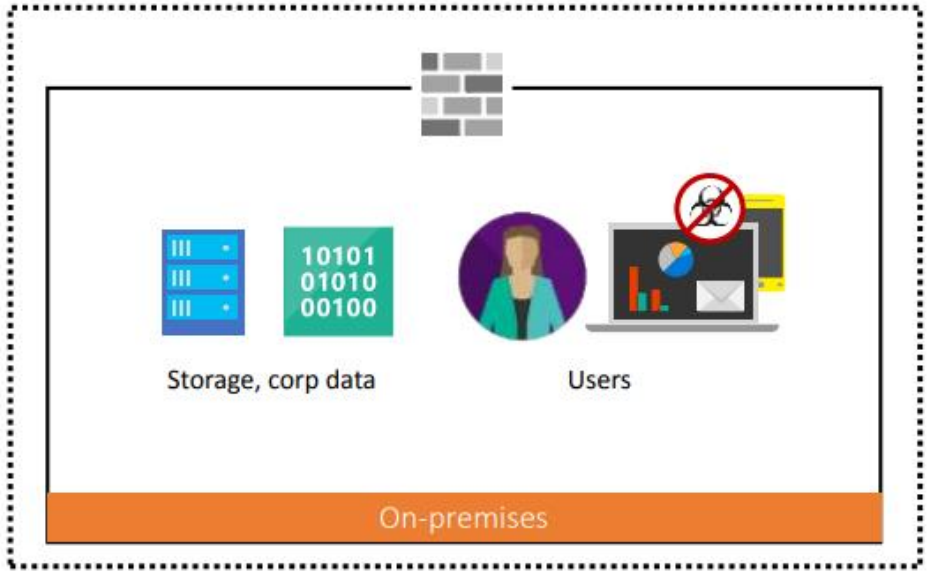
- Entra Permission Management (CloudKnow)

Questions

- And more – Expert Panel AMA ☺

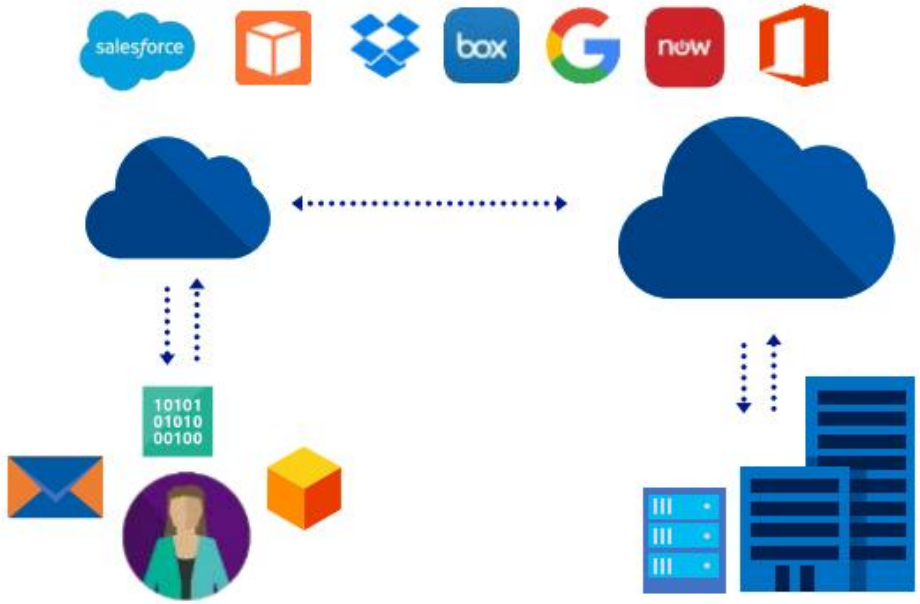
Understand your identity landscape with Microsoft Entra Permissions Management

Life before cloud



- 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

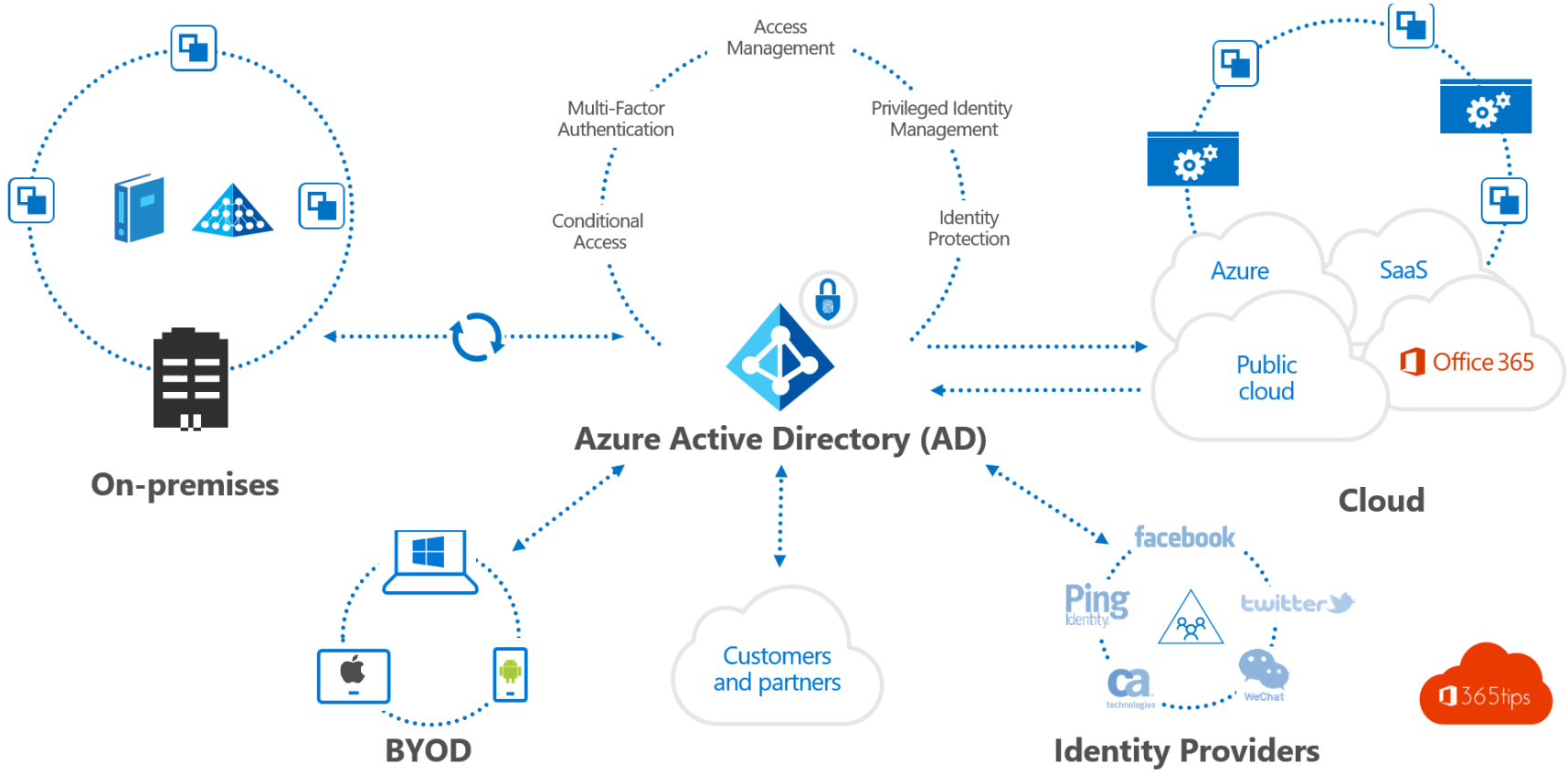
Life with cloud



- 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.



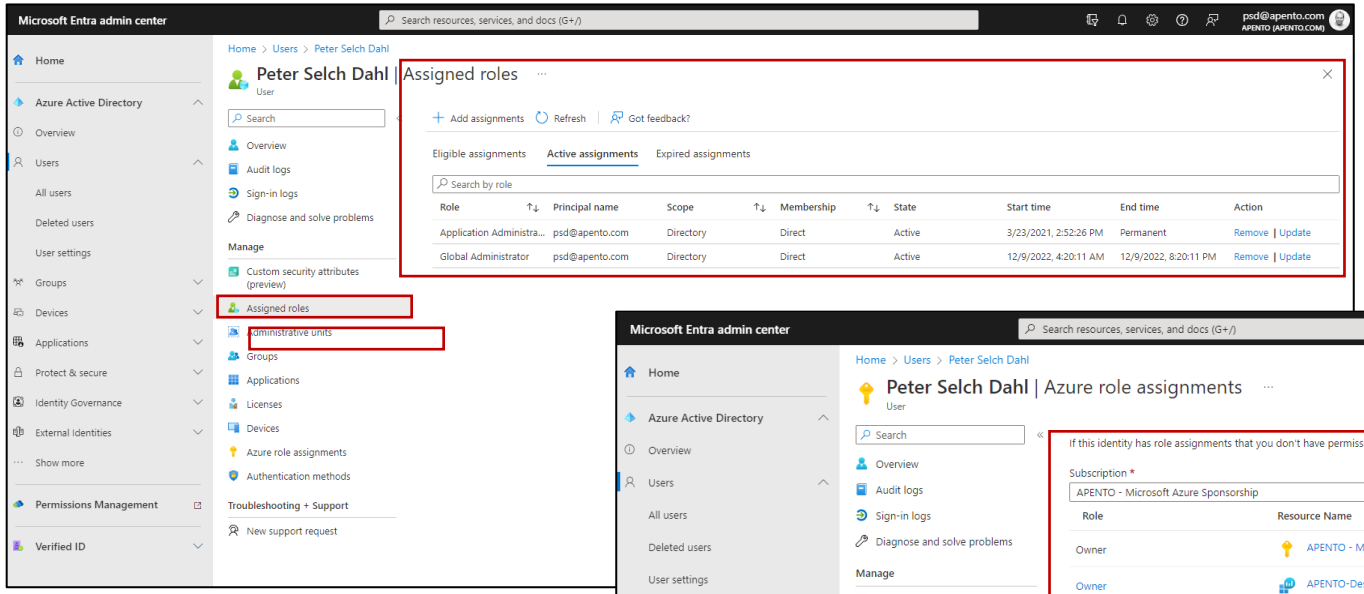
Understand your identity landscape with Microsoft Entra Permissions Management

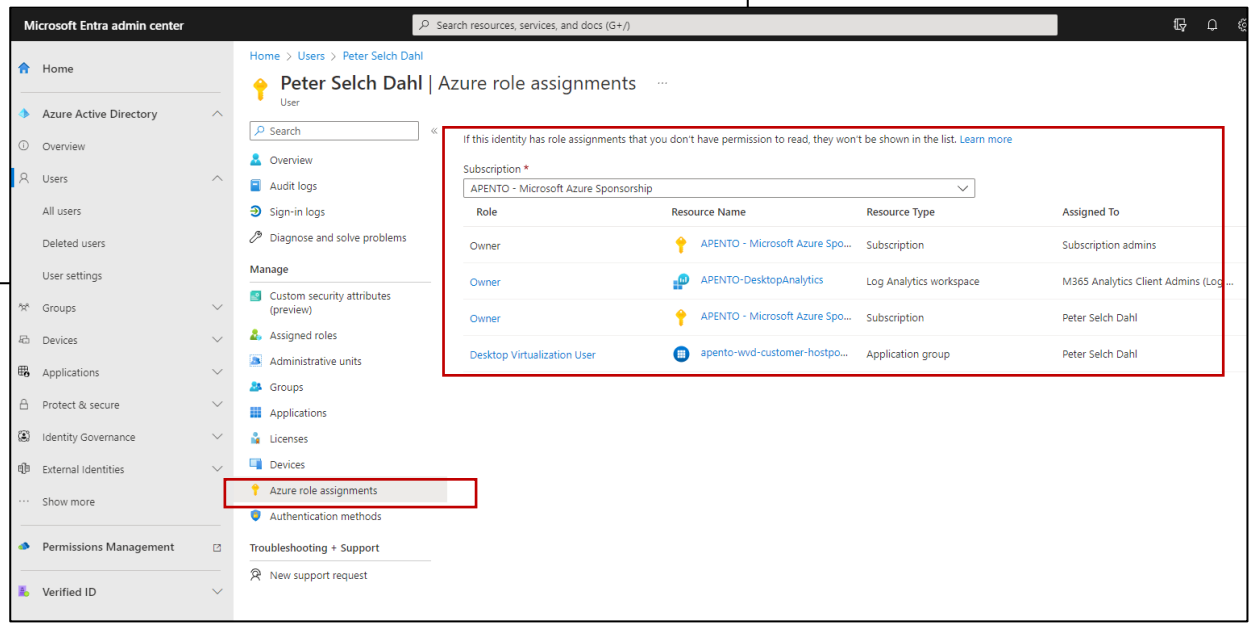
Defender for Cloud Apps

Provides insight into shadow cloud apps

Understand your identity landscape with Microsoft Entra Permissions Management

What roles, access and application do I have assigned?





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

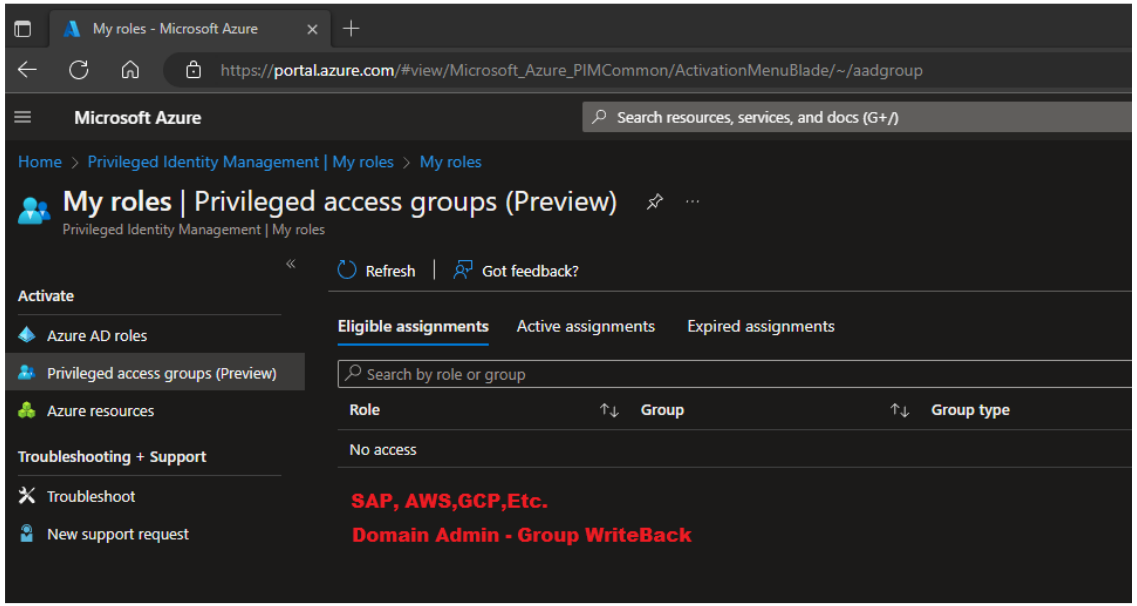
Do I still need these permissions and do I use them?

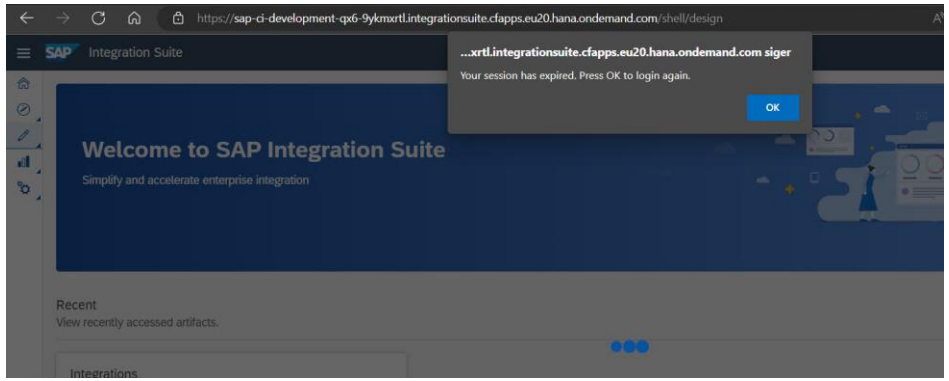
Hard to understand the landscape

Understand your identity landscape with Microsoft Entra Permissions Management

Workplace Ninja User Group Denmark

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





Understand your identity landscape with Microsoft Entra Permissions Management

Workplace Ninja User Group Denmark

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-vulns-are-shallow dept.

New submitter juniq 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 —

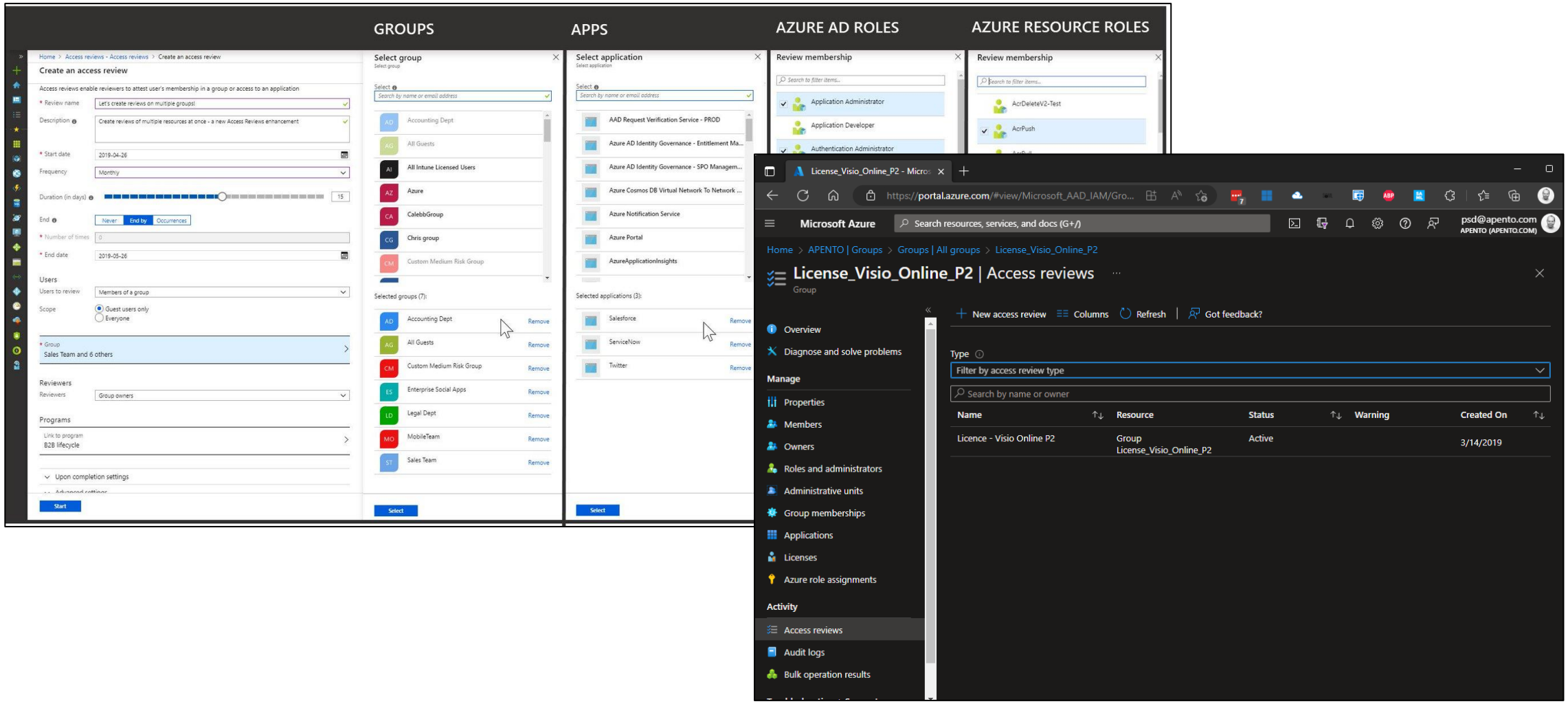
Tesla cloud resources are hacked to run cryptocurrency-mining malware

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

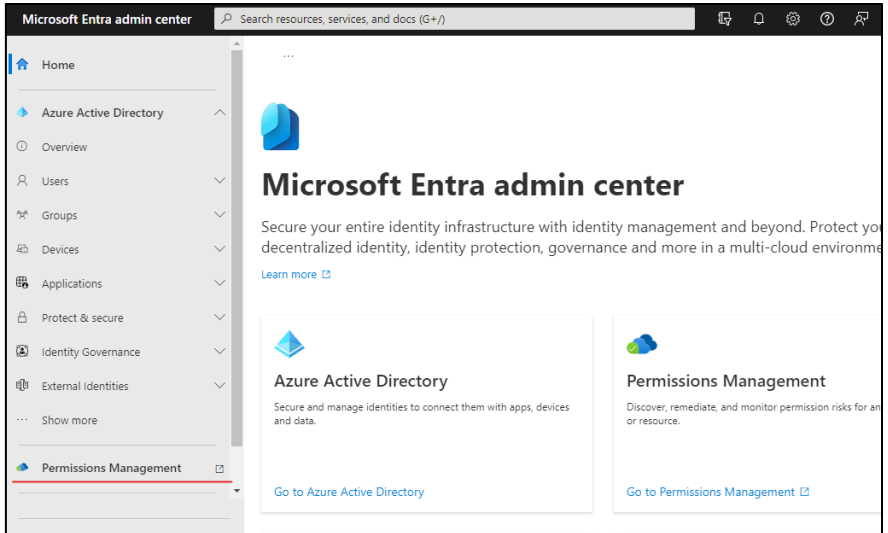


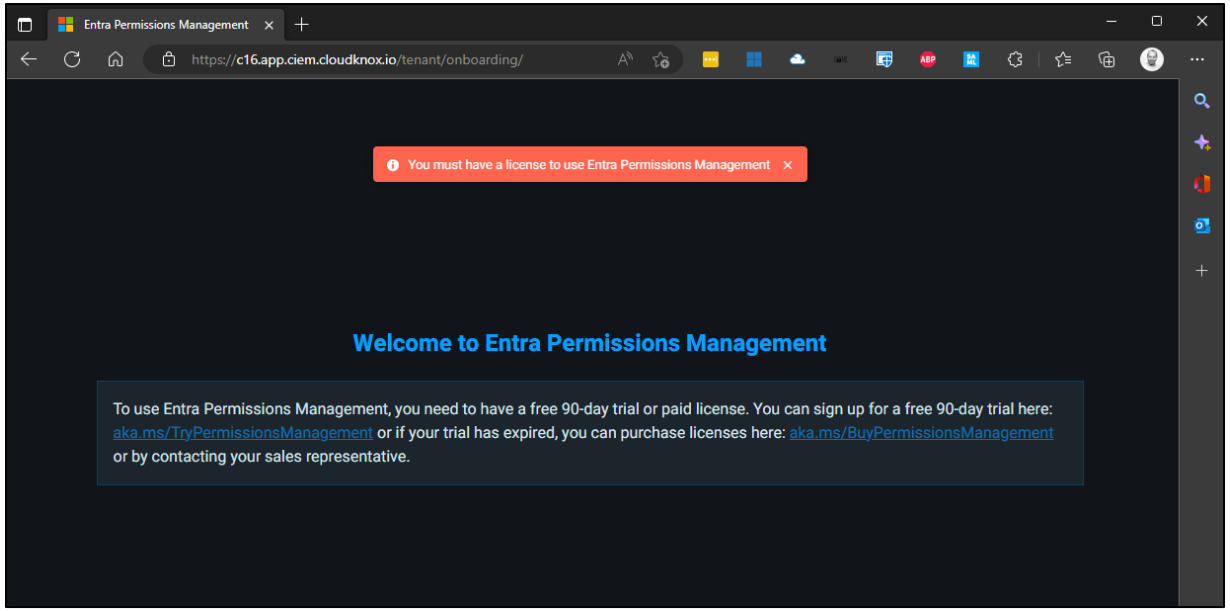
Understand your identity landscape with Microsoft Entra Permissions Management

Understand your identity landscape with Microsoft Entra Permissions Management

Getting started with Entra Permission Management

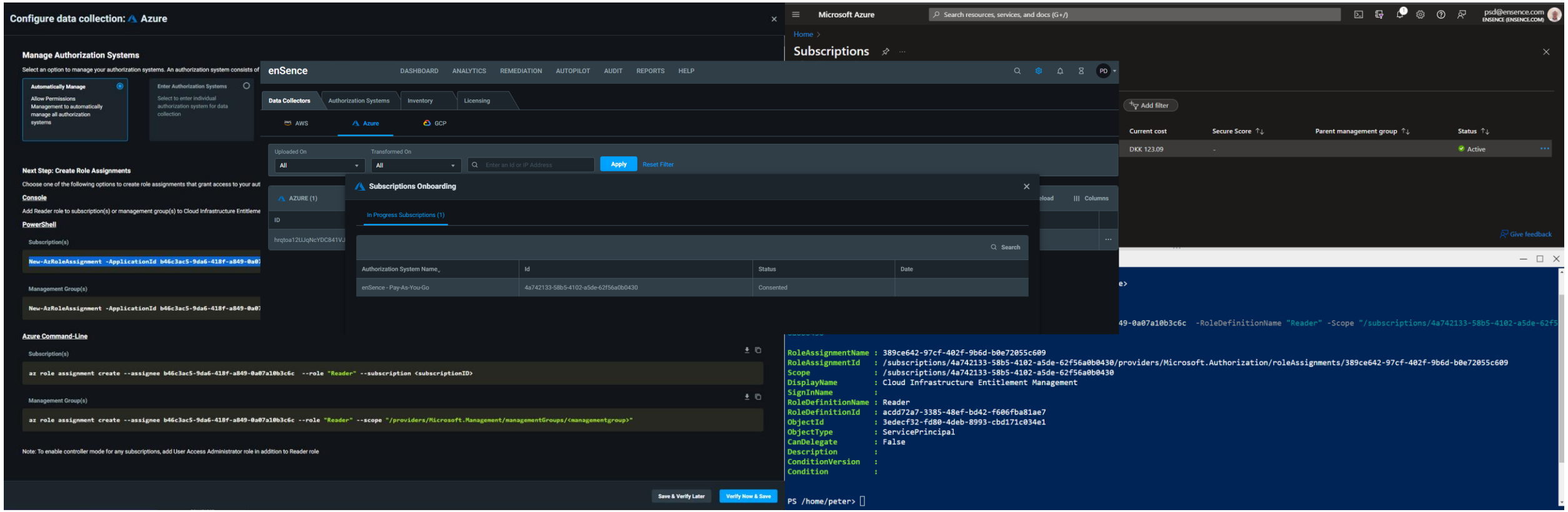
1. Go to the Microsoft Entra portal ” https://entra.microsoft.com”
2. Click ”Permissions Management”
3. Enabled 90 Days Trial
4. Check your assets and the cost! ☺





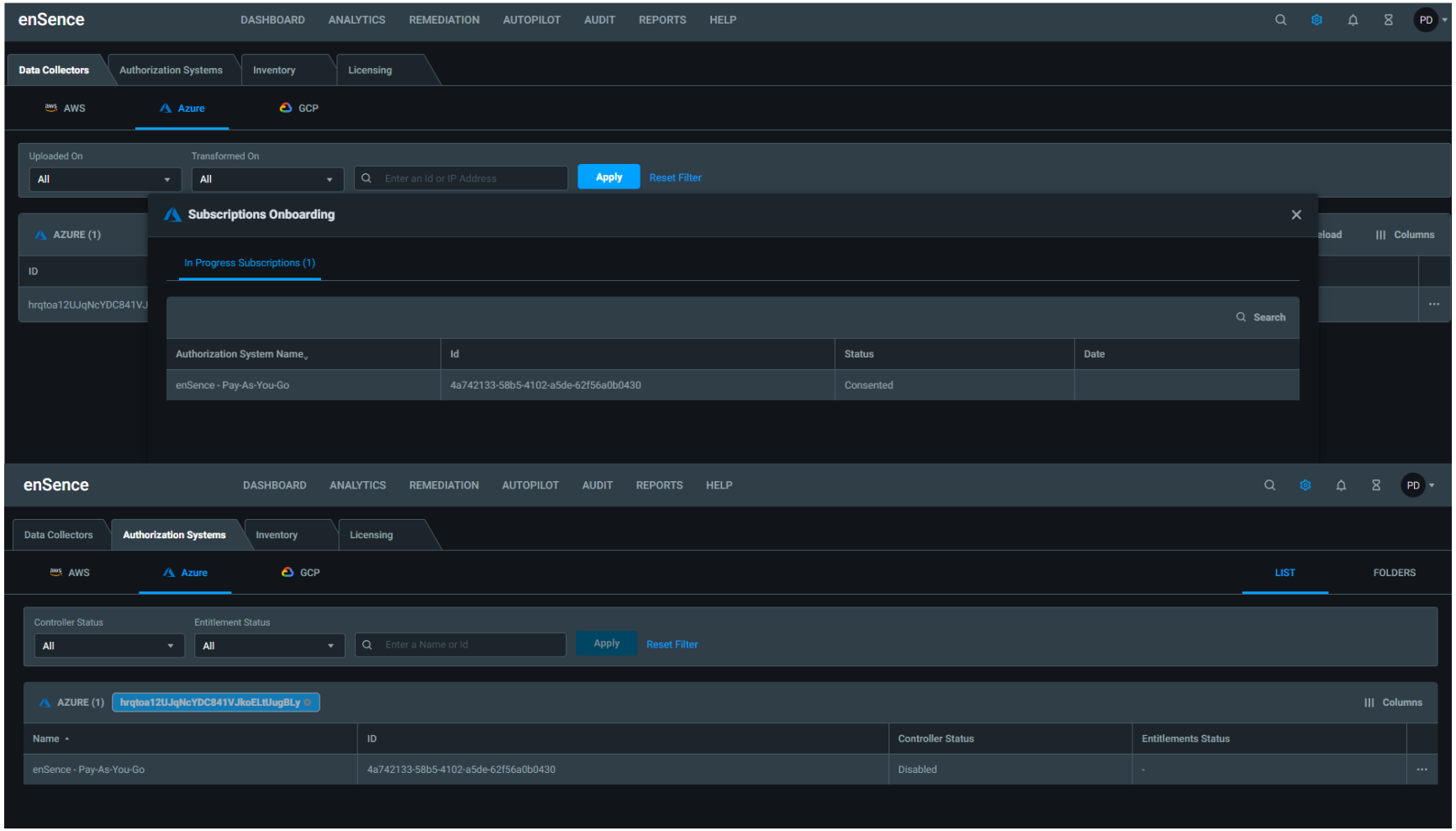
Understand your identity landscape with Microsoft Entra Permissions Management

- Onboard Azure in seconds ☺

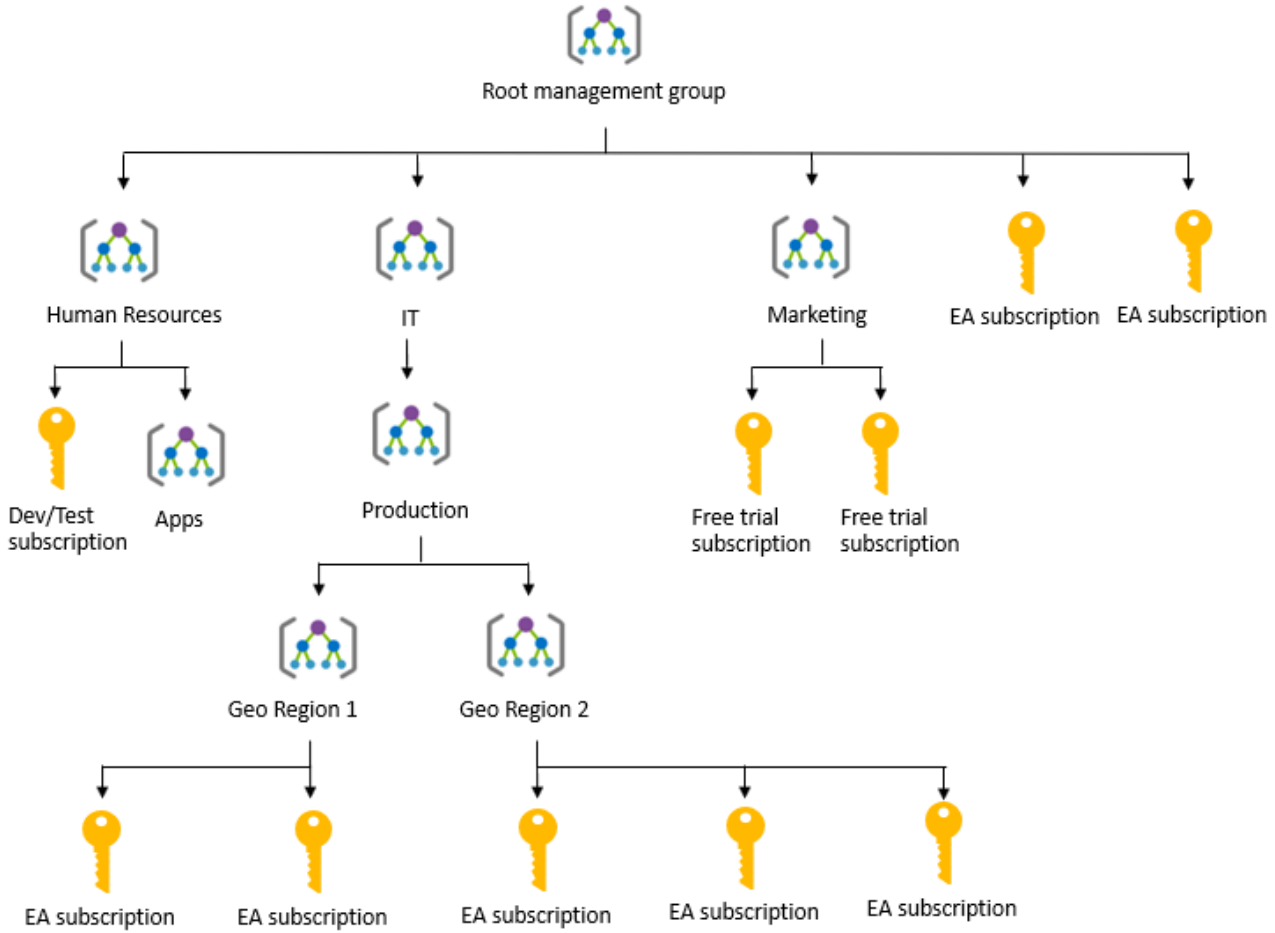


Understand your identity landscape with Microsoft Entra Permissions Management

- Onboard Azure in seconds ☺



Understand your identity landscape with Microsoft Entra Permissions Management

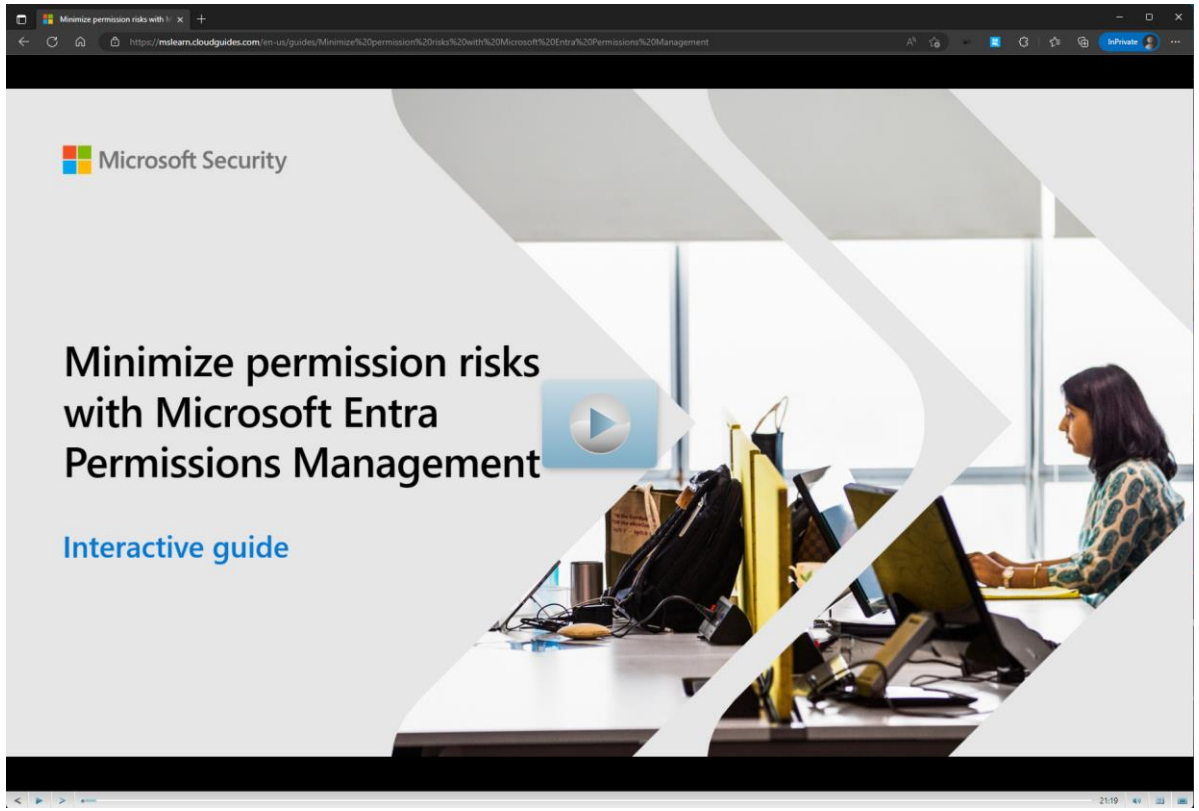



```
New-AzRoleAssignment -ApplicationId b46c3ac5-9da6-418f-a849-0a07a10b3c6c -RoleDefinitionName "Reader" -Scope
"/providers/Microsoft.Management/managementGroups/<managementgroup>"
```

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

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

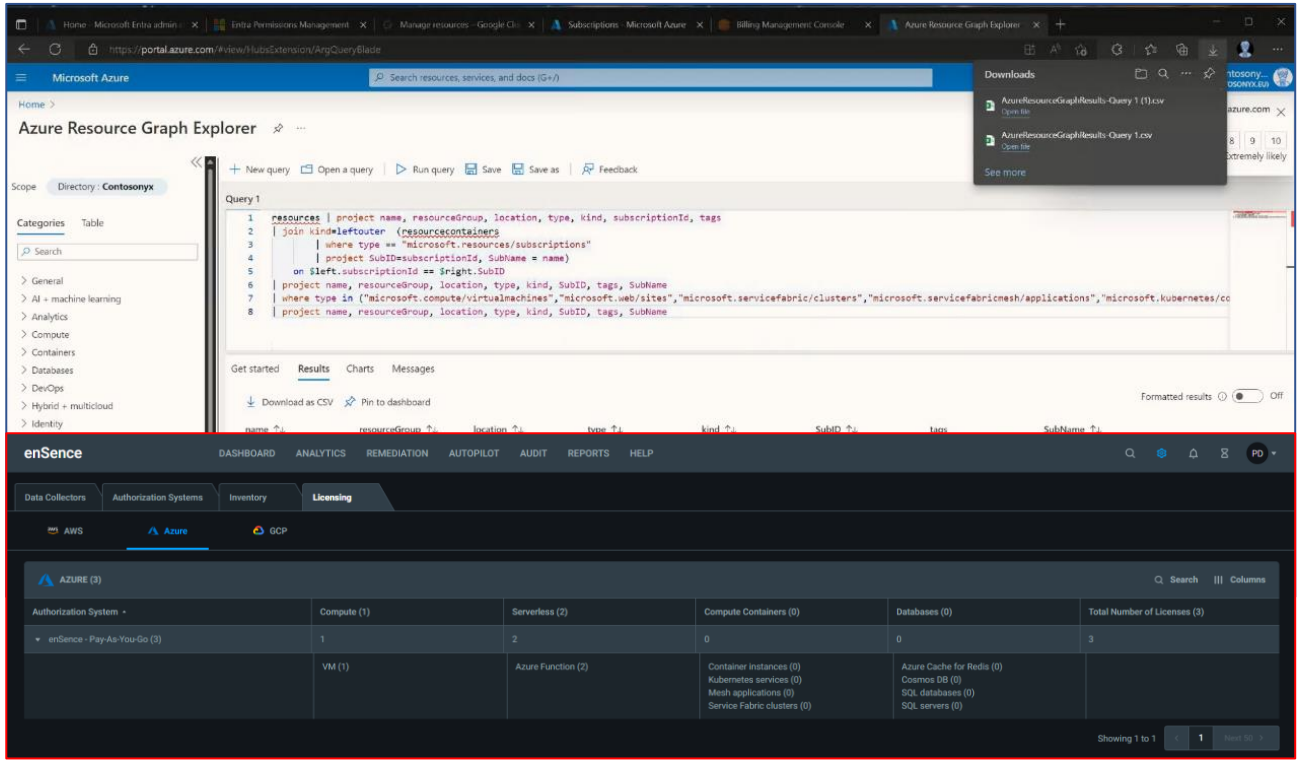
Monitoring “Assets”

Navigate to the Resource Graph: https://portal.azure.com/#view/HubsExtension/ArgQueryBlade

“*Make sure your 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:

```
4resources
| project name, resourceGroup, location, type, kind, subscriptionId, tags
5| join kind=leftouter  (resourcecontainers
6        | where type == "microsoft.resources/subscriptions"
7        | project SubID=subscriptionId, SubName = name)
8    on $left.subscriptionId == $right.SubID
9| project name, resourceGroup, location, type, kind, SubID, tags, SubName
1| 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")
1| project name, resourceGroup, location, type, kind, SubID, tags, SubName
```



Microsoft Security

Workplace Ninja User Group Denmark

Microsoft Entra Permissions Management

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

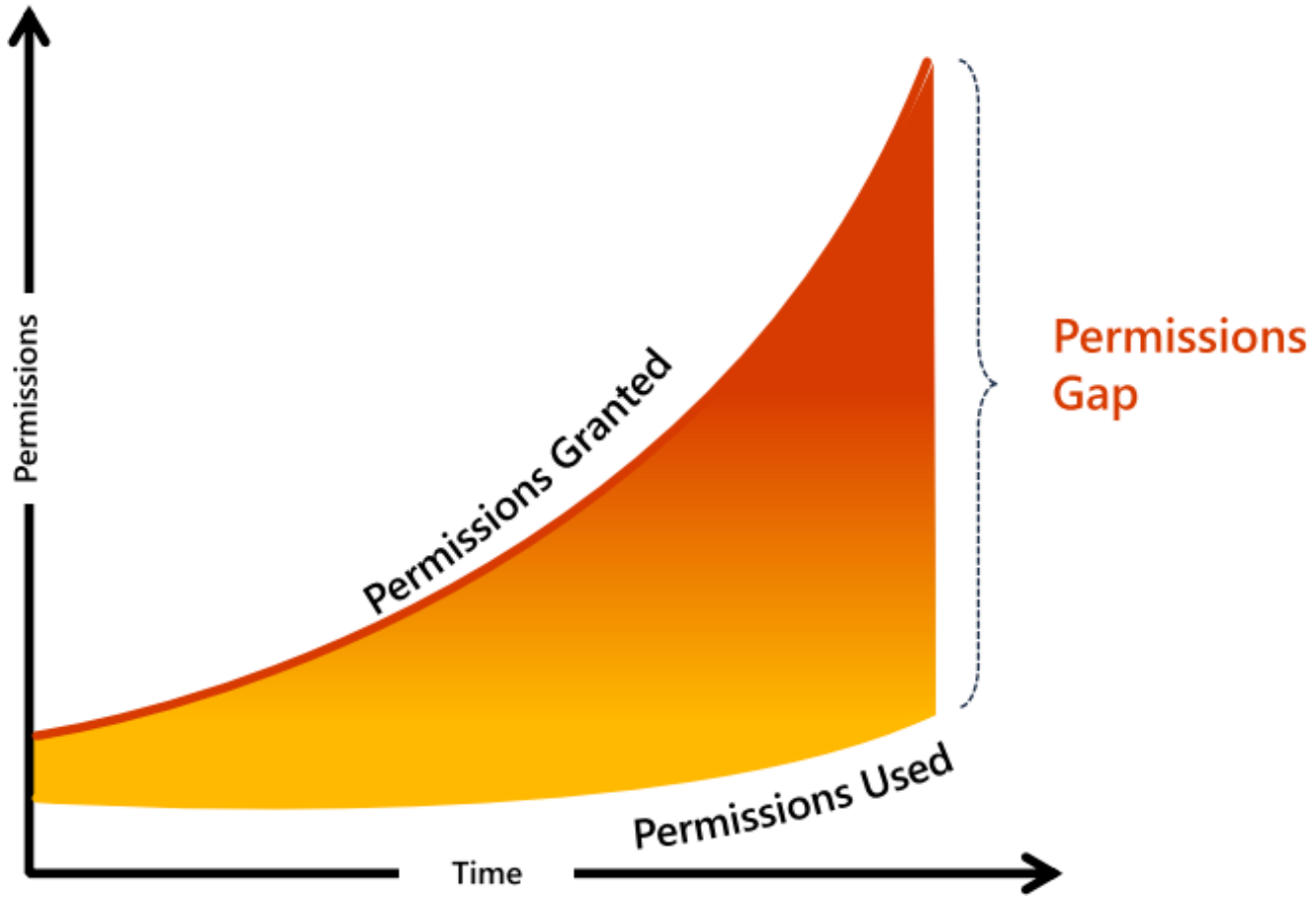
Multicloud adoption brings new permission challenges

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

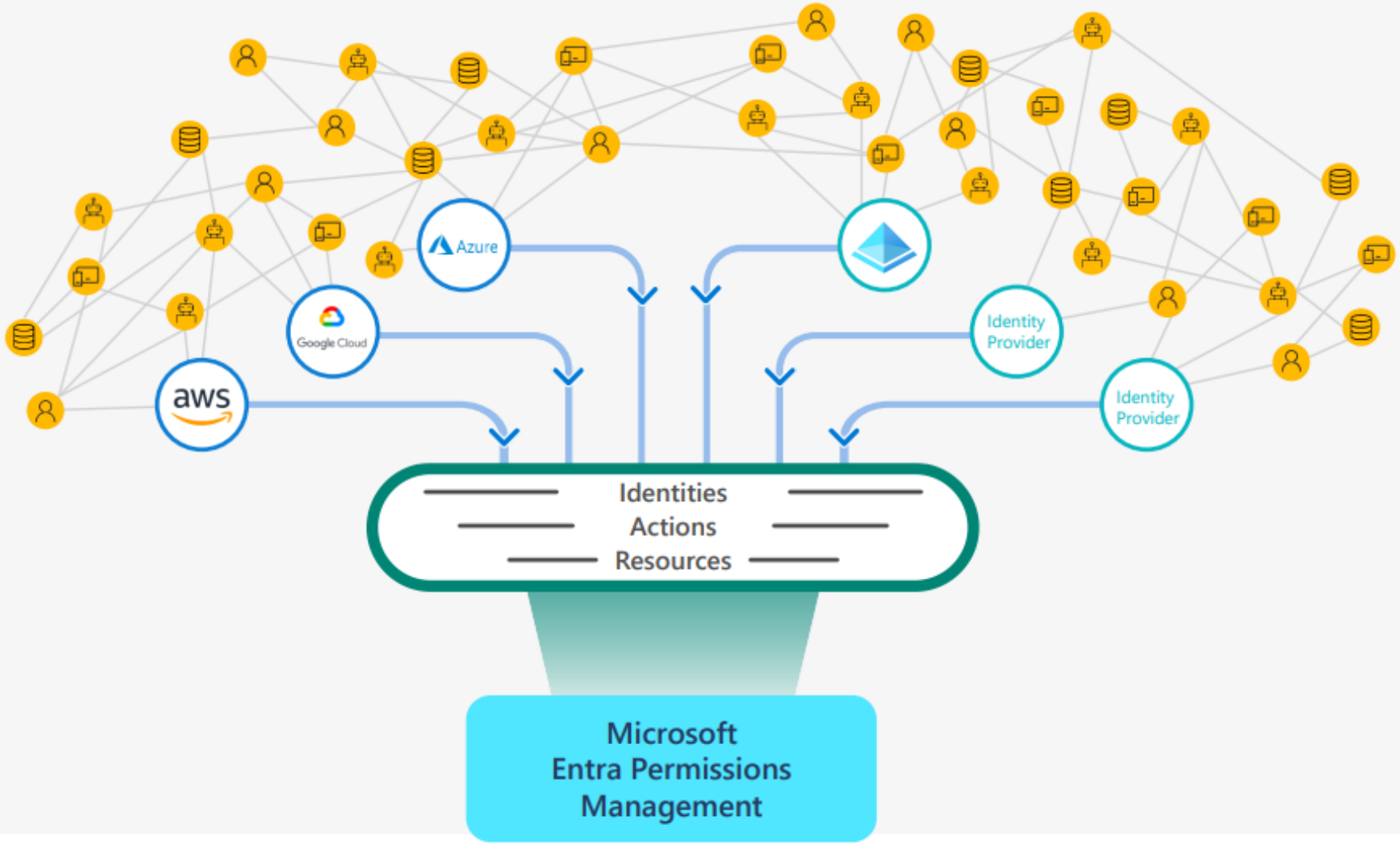
Increased risk of breach from accidental or malicious permission mis-use

Managing permissions across multicloud environments requires a new approach

Today's static, outdated approach	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



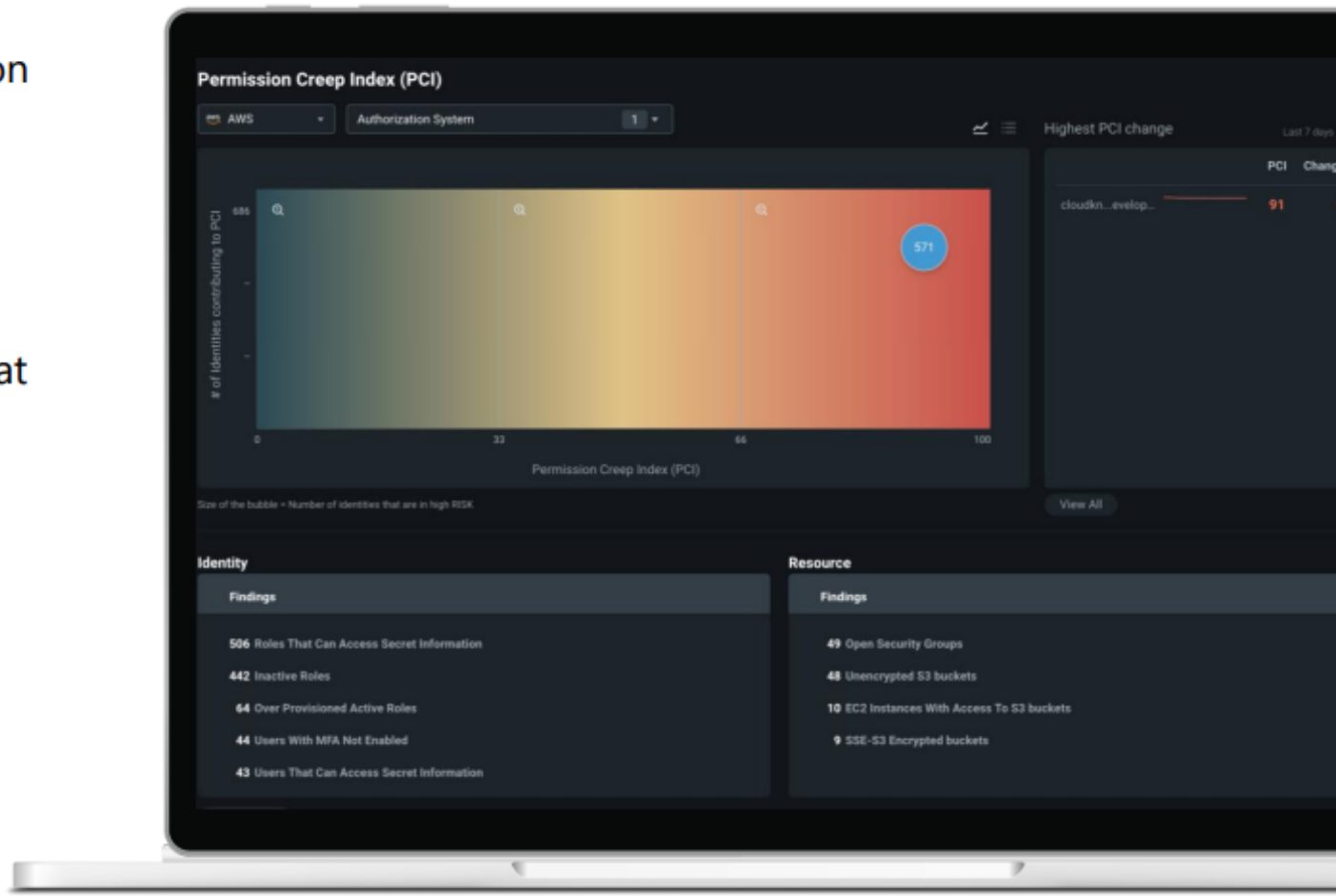
Microsoft Entra Permissions Management

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

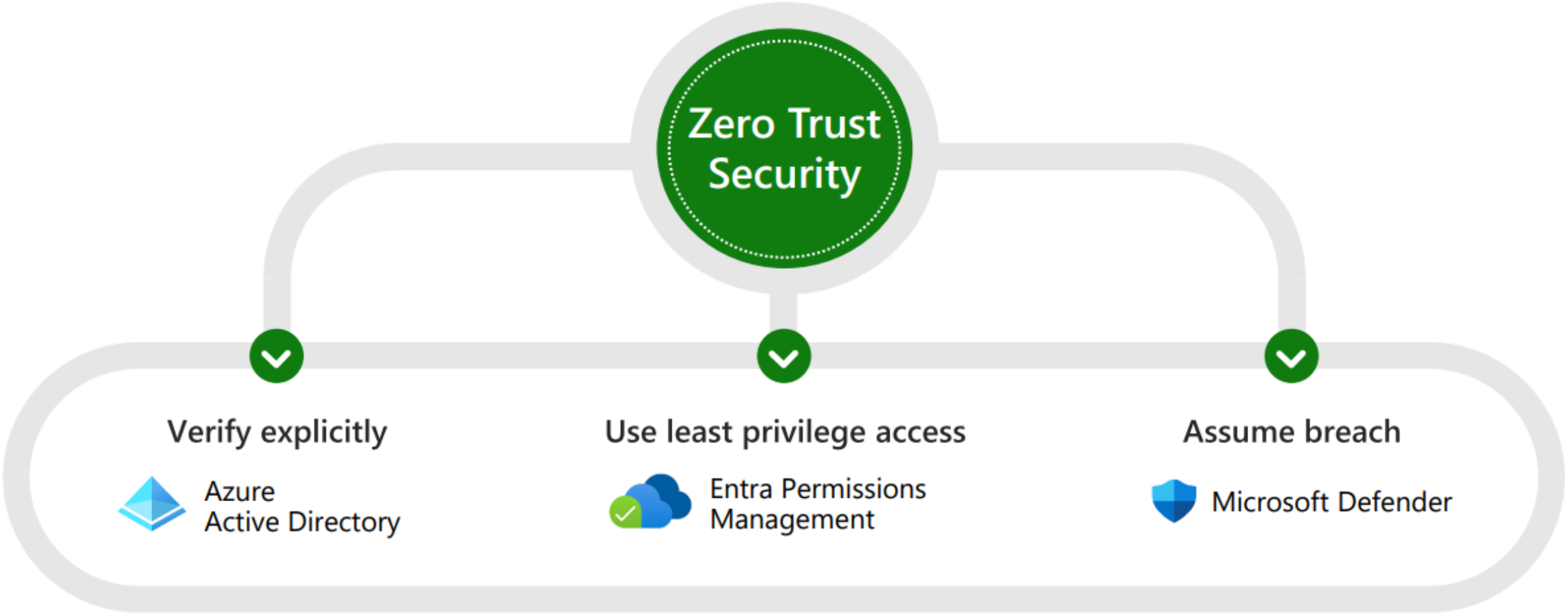
Discover
Obtain a comprehensive view of every action performed by any identity on any resource.

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.

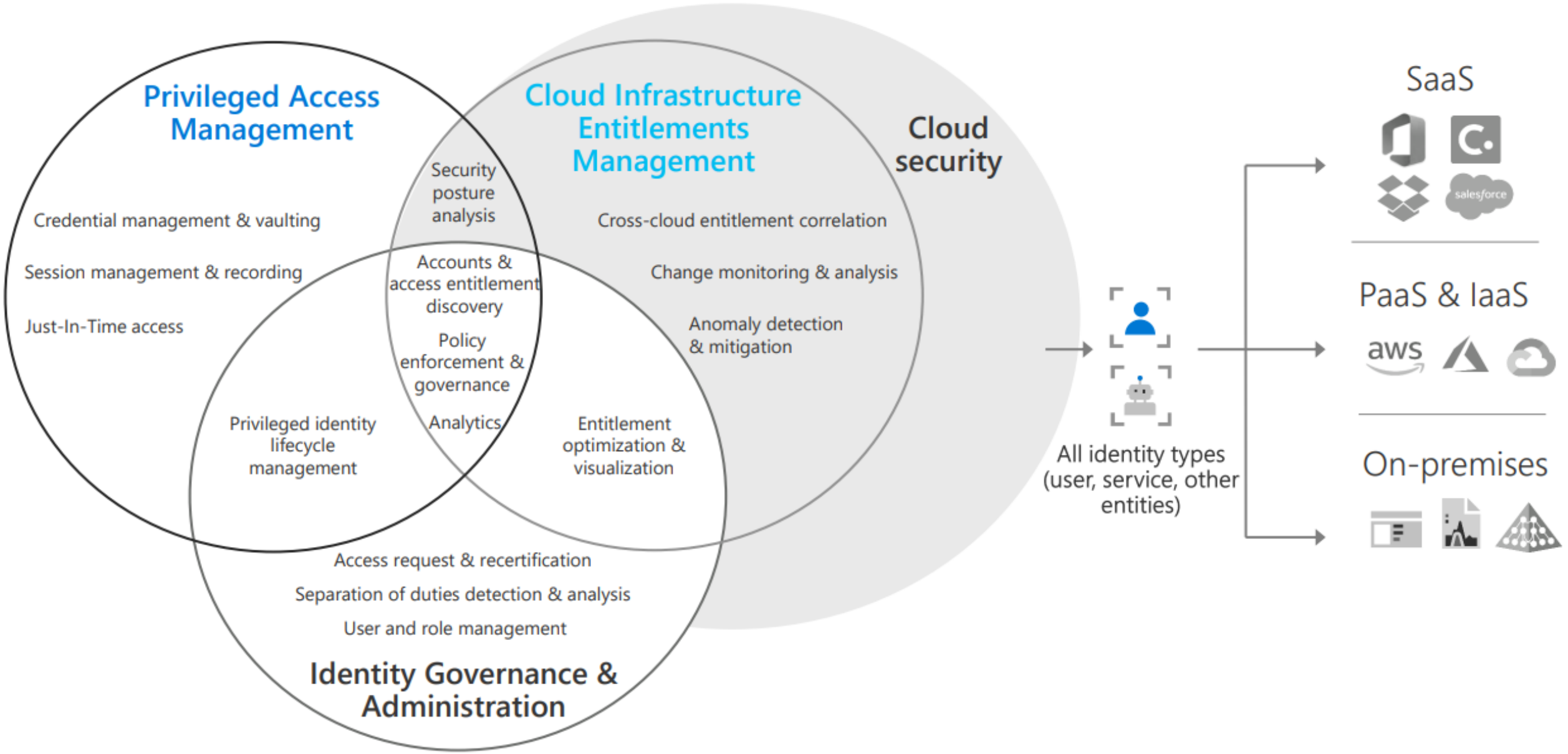


Entra Permissions Management empowers Zero Trust

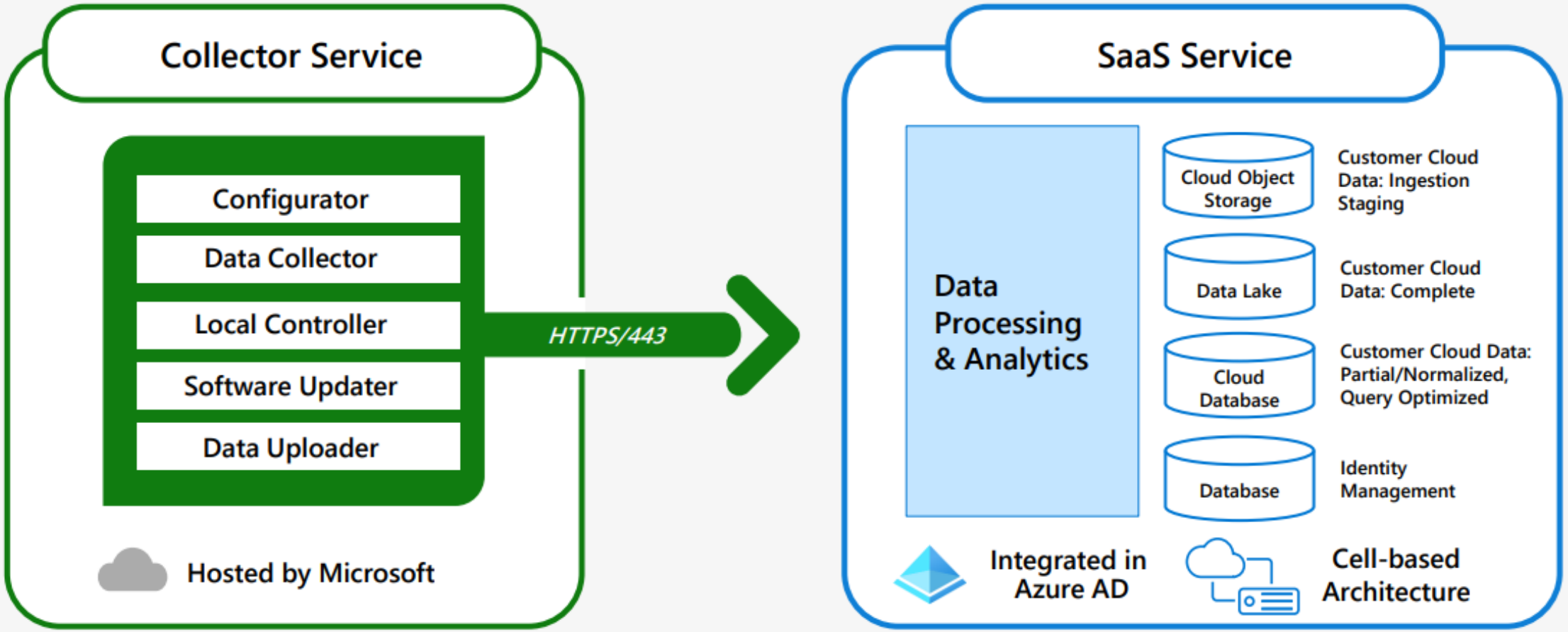


Multicloud | Multi-Platform

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

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)

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

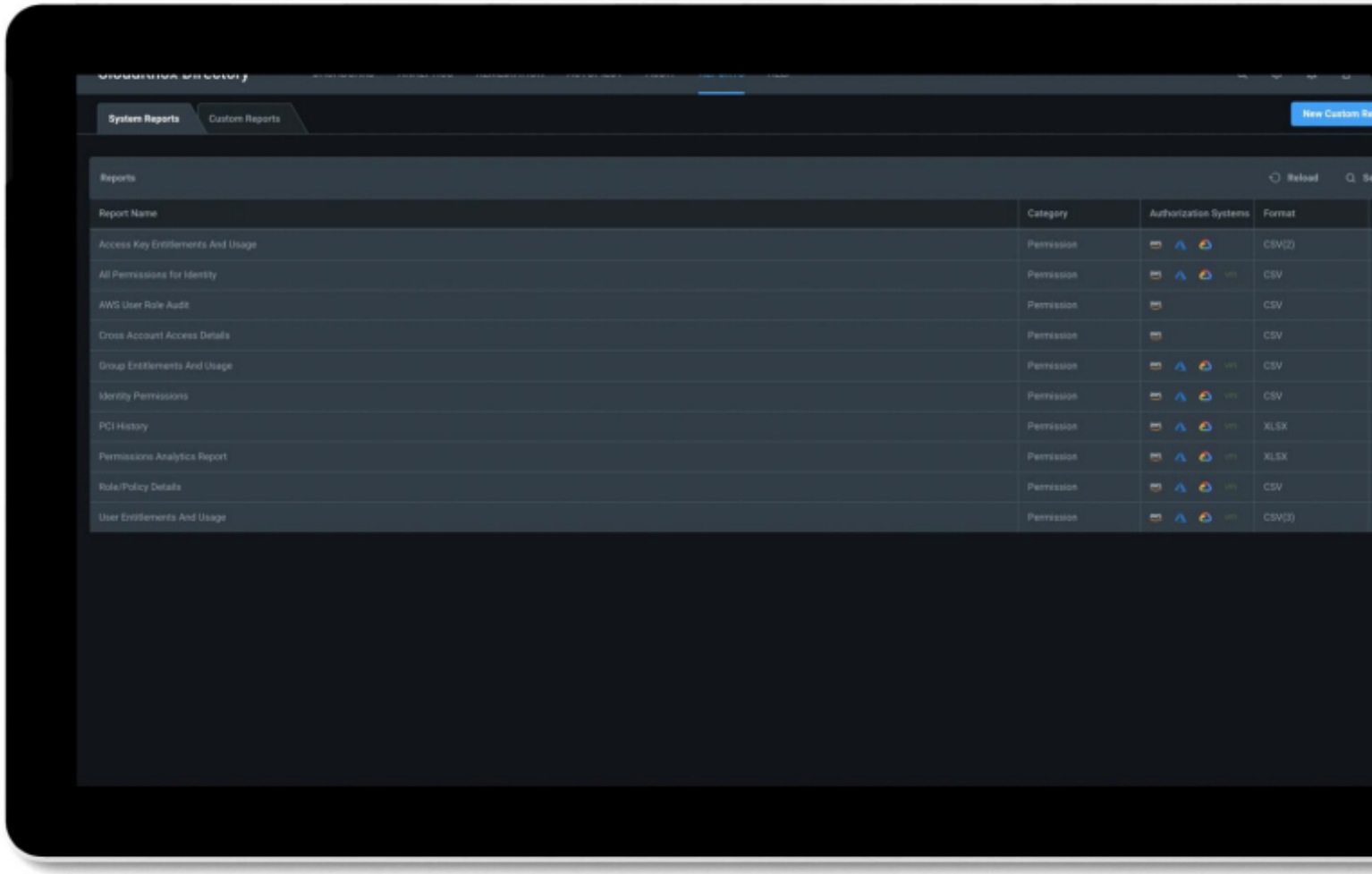
Risk Assessment Key Findings

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

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



Permission Creep Index (PCI)

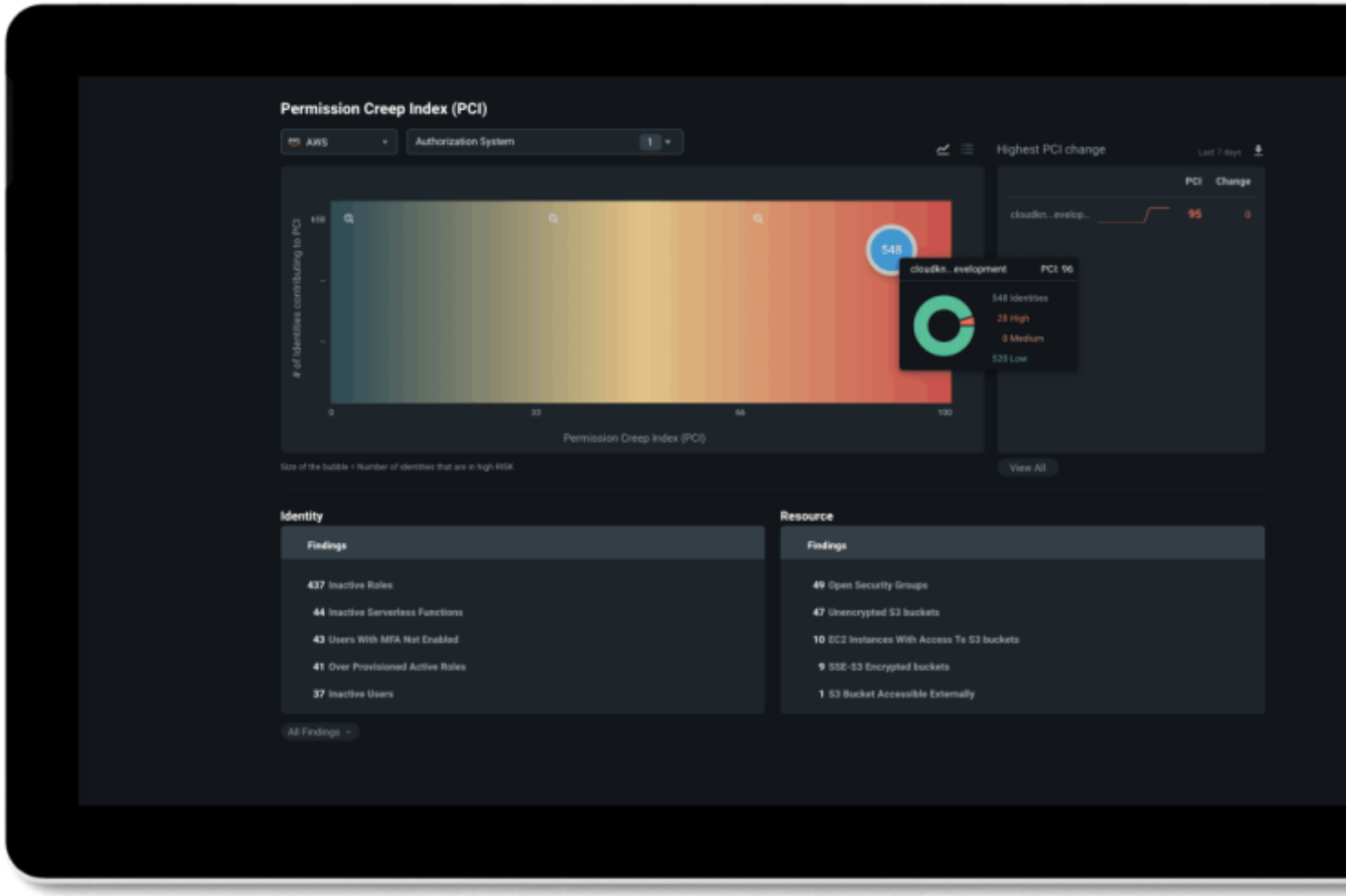
What is it?

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.

Permission Creep Index (PCI)

GCP | Authorization System 1

Size of the bubble = Number of identities that are in high RISK

Highest PCI change

Last 7 days

	PCI	Change
Woodgrove	81	0

View All

Identity

Findings

- 9 Privilege Escalation Service Accounts
- 6 Inactive Users
- 6 Super Users
- 2 Over Provisioned Active Users

Resource

Findings

Findings are not available

Permission Creep Index (PCI)

Azure | Authorization System 1

Woodgrove

Users

706 Total Users
554 High
0 Medium
152 Low

Applications

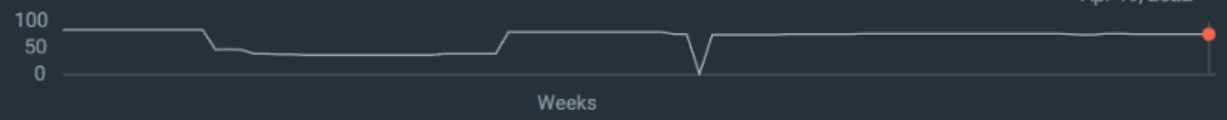
14 Total Applications
4 High
0 Medium
10 Low

Managed Identities

5 Total Managed Identities
0 High
0 Medium
5 Low

PCI Trend

PCI 76



Highest PCI change

Last 7 days

	PCI	Change
Woodgrove	76	0

View All

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

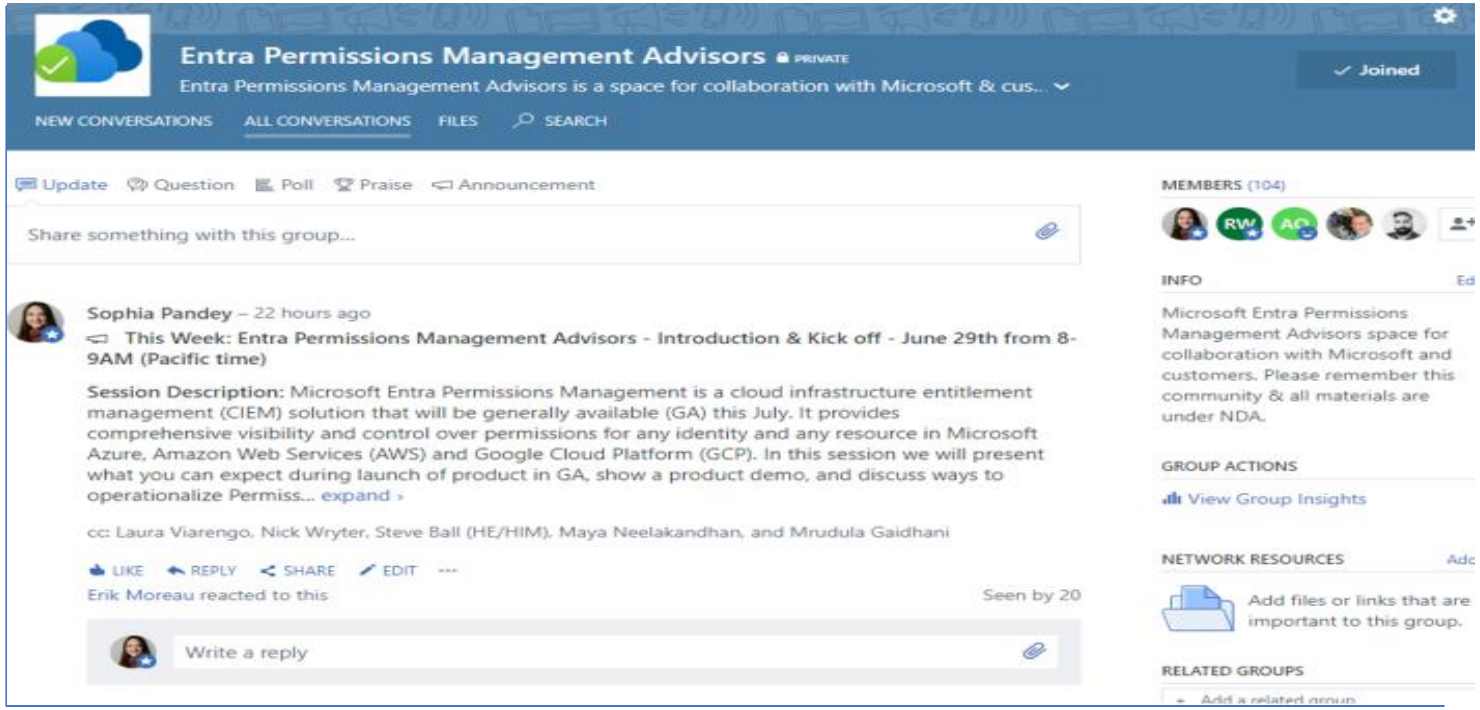
Questions and Answers

THANK YOU!

Twitter: @PeterSelchDahl
Mail : psd@apento.com

Join Microsoft Entra Permissions Management Advisors

Become part of the advisor community!



https://aka.ms/EntraPermissionsManagementAdvisors

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

A shift in IT focus…..