

Microsoft Security
USER GROUP



Navigating Entra ID: Safeguarding Applications and Operations

Anders Kristiansen
Azure Security Lead - Devoteam M-Cloud

We will talk about:



Entra ID application types and configurations options

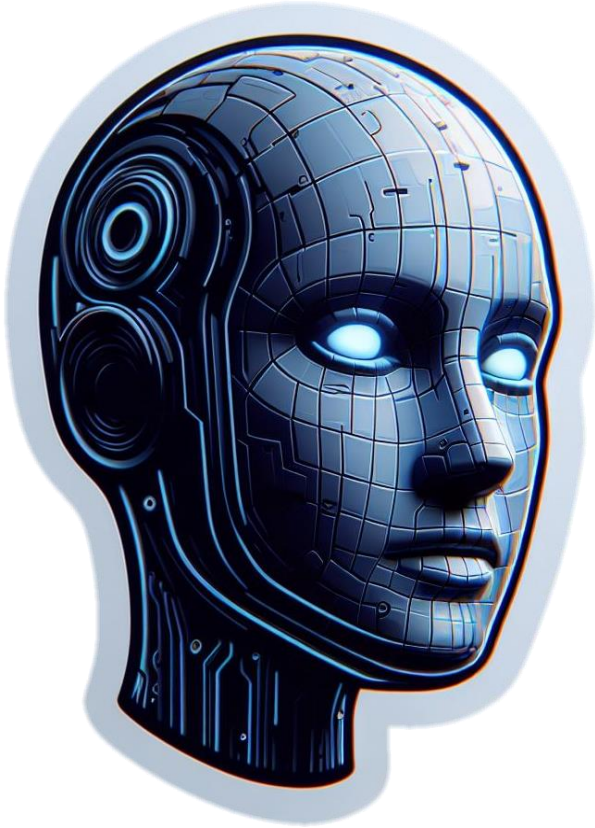


Protection and detection options



Showcasing tools and methods for getting valuable insight of applications

AI



Phishing



PIM

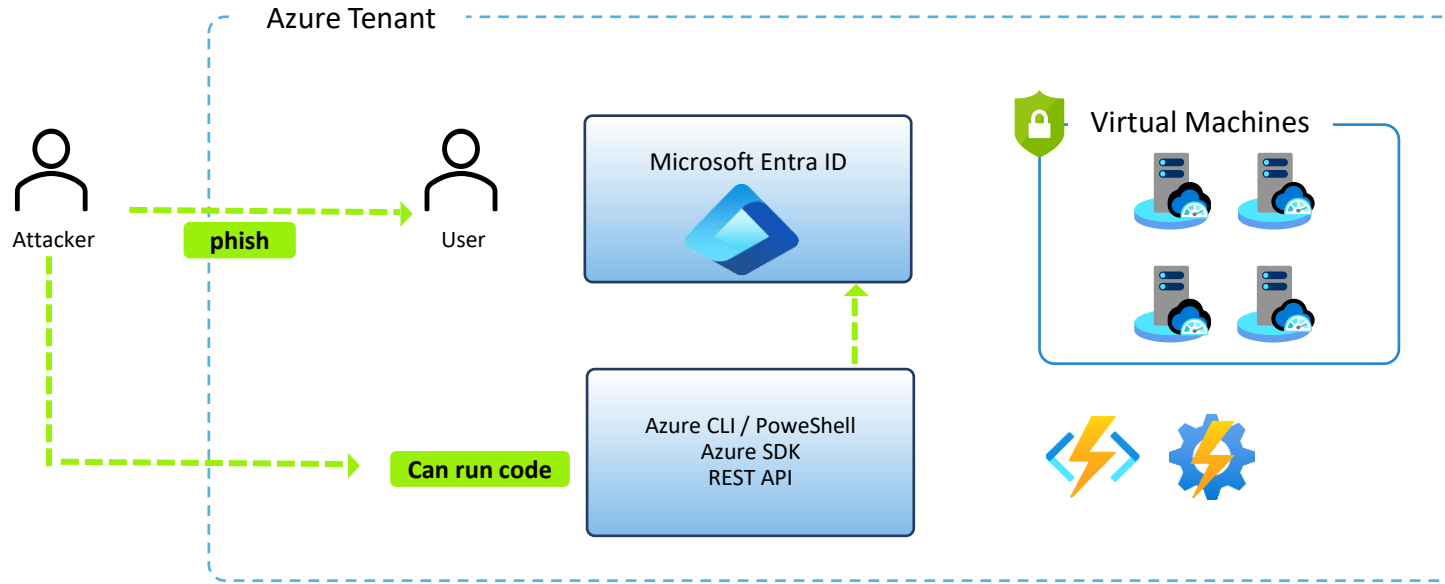


Will **not** be talking about this

Navigating Entra ID: Current state

- Identities are using only 1% of their granted permissions
- 85% of companies have identities with over-permissive contributor roles
- 70% of identities have not used any of their permissions granted in the last 90 days
- Workload identities outnumber human identities 10:1, which is double what was recorded in 2021
- 45% of identities are Super Admins

Attack path - Reconnaissance





Demo time
MFASweep

Navigating Entra ID: Apps everywhere!

1st party apps

- Developed by Microsoft and are designed to work seamlessly with the Microsoft Ecosystem
- These apps tend to be forgotten but can have a quite large attack surface.
- These apps don't always result in a service principal being created in your tenant. This can lead to confusion.

Own applications

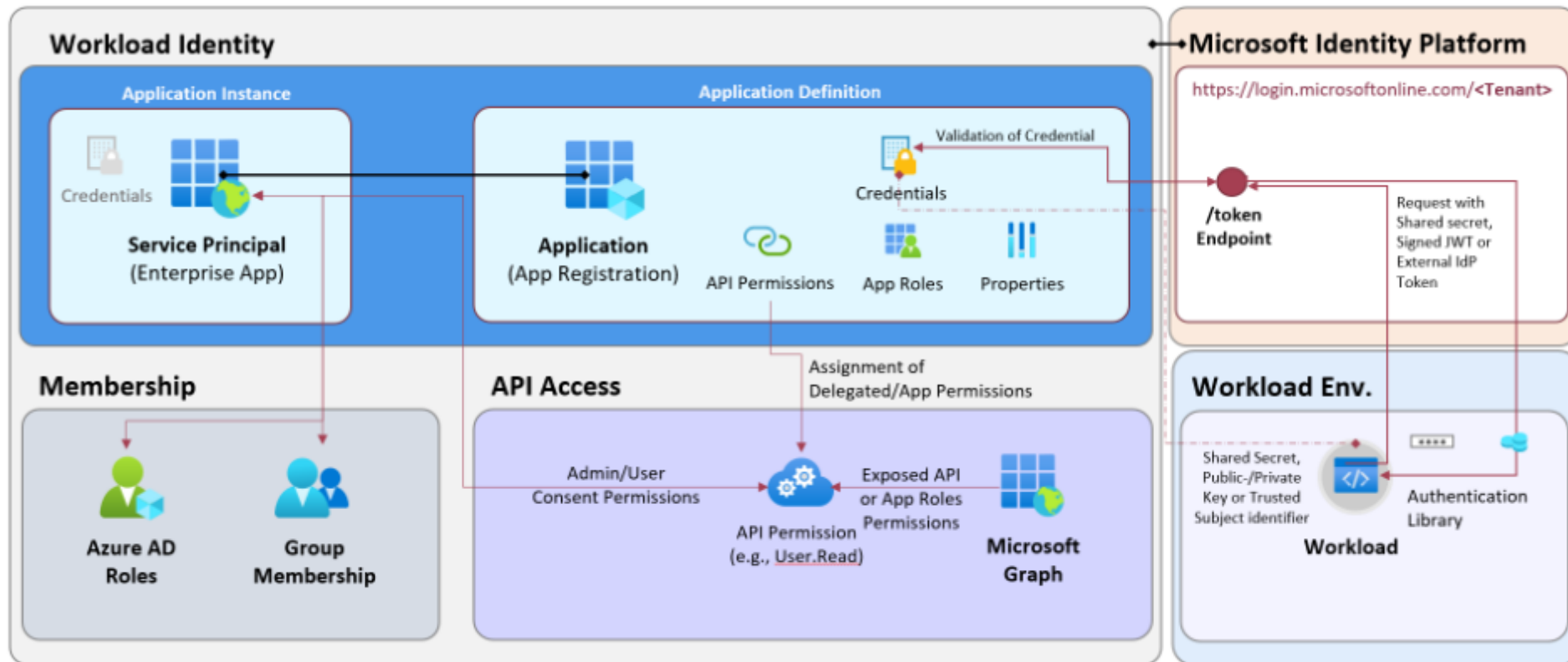
- Developed or created by the organization
- Typical misconfiguration issues with broad access (owners)
- Poor credential management
- Conditional Access
- Lack of monitoring of these apps

3rd party apps

- Managing access can be more complex than 1st party.
- Supply chain review of 3rd party apps is rarely conducted. (NSM Report)
- Conditional Access policy misconfigurations.
- Too broad access
- Lack of risk detection and monitoring

Application type == **Microsoft Applications** ✕

Entra ID Objects of Application Identities



Source: cloud-architekt.net/

Navigating Entra ID: What is this app we just tested?

Check sign-in logs

Date	Request ID	User	Application	Status
3/1/2024, 12:52:03 PM	c162140b-1e24-4baa-ba4c-3...	Allan Deyoung	Azure Active Directory PowerShell	Success

```
----- Microsoft Graph API -----  
[*] Authenticating to Microsoft Graph API...  
[*] SUCCESS! AllanD@M365x62188674.OnMicrosoft.com was able to authenticate to the Microsoft Graph API  
[***] NOTE: The "MSOnline" PowerShell module should work here.
```

Application	Azure Active Directory PowerShell
Application ID	1b730954-1685-4b74-9bfd-dac224a7b894
Authentication requirement	Single-factor authentication

The list of applications that are maintained by your organization are in [application registrations](#).

Application type: Enterprise Applications

Applications status: Any

Application visibility: Hidden

Apply

Reset

1b730954-1685-4b74-9bfd-dac224a7b894

Name	Homepage URL
Didn't find what you're looking for? Click 'Add' above to add a new application.	

Important

Azure AD Powershell is planned for deprecation on **March 30, 2024**. For more details on the deprecation plans, see the [deprecation update](#). We encourage you to continue migrating to [Microsoft Graph PowerShell](#), which is the recommended module for interacting with Azure AD. In addition, Microsoft Graph PowerShell allows you access to all Microsoft Graph APIs and is available on PowerShell 7. For answers to frequent migration queries, see the [Migration FAQ](#).

Demo time
Apps behind
the scenes



But why bother?

- Make sure guests do not access the endpoints
- Make sure regular users do not access the endpoints
- Require allowed users to activate the PIM before use. (implies PIM)
- Protect the endpoint in the event a user token was stolen and a replay was attempted.
- PowerShell endpoints are easy targets for password sprays.
- Data Exposure: Can access sensitive data from your tenant, including user data, group data, and more. You should control who has access to this data.



Apps we might want to limit or have control of

**Microsoft Graph
PowerShell /
Microsoft Graph
Command Line Tools**
(14d82eec-204b-
4c2f-b7e8-
296a70dab67e)

Microsoft Graph
PowerShell (Recommended)

**Azure Active
Directory PowerShell**
(1b730954-1685-
4b74-9bfd-
dac224a7b894)

Planned for deprecation March 30!

**Azure Active
Directory PowerShell**
(1950a258-227b-
4e31-a9cf-
717495945fc2)

Planned for deprecation March 30!

Graph Explorer
(de8bc8b5-d9f9-48b1-
a8ad-b748da725064)

Powerful tool that allows you to make
requests and see responses against
Microsoft Graph

Protecting 1st party apps with CAP

Conditional Access Policy (you will not find the two appID in deprecation):

Target resources ⓘ

2 apps included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ


0 controls selected


Edit filter

None

Select

Microsoft Graph Command Line Tools and 1 more

 Graph Explorer
de8bc8b5-d9f9-48b1-a8ad-b748da725064 ...

 Microsoft Graph Command Lin...
14d82eec-204b-4c2f-b7e8-296a70dab67e ...

Navigating Entra ID: Detection and Ops

Detection with log analytics → Monitor alert. Sentinel incident or hunting

Costs graph activity of this log?

Devoteam 200 users

40K users

Table	Ingestion Volume
MicrosoftGraphActivityLogs	38.27MB
MicrosoftGraphActivityLogs	1.12GB

Diagnostic setting name

AuditAAD

Logs

Categories

☒ AuditLogs

☒ SignInLogs

Before deprecation, you might want to find out if there is usage?

If Entra ID diagnostics is not configured? -> signings via portal or GraphSDK

```
Name                                ConditionalAccessStatus Count
-----
anders@anderskristiansen.com, success 2
anders@anderskristiansen.com, failure 1
```

Adding apps to Entra ID so we can govern them



Microsoft Azure PowerShell | Overview ...

Enterprise Application



Overview



Deployment Plan



Diagnose and solve problems

Manage



Properties



Owners



Roles and administrators



Users and groups



Single sign-on



Provisioning



Custom security attributes

Security



Permissions



Token encryption

Activity



Sign-in logs



Usage & insights

Properties



Name ⓘ

Microsoft Azure PowerShell

Application ID ⓘ

1950a258-227b-4e31-a9cf-...

Object ID ⓘ

0687def6-b615-4109-bdef-...

Getting Started



1. Provision User Accounts

You'll need to create user accounts in the application

[Learn more](#)

What's New



Sign in charts have moved!

The new Insights view shows sign in info along with other use

Try to see what's different with this application compared to the one I will demo

```
> Did not found service principal with AppId 1950a258-227b-4e31-a9cf-717495945fc2 so created one
Updated assignment required for 1950a258-227b-4e31-a9cf-717495945fc2 with display name Microsoft Azure PowerShell
```



Demo time
detect and
protect 1st
party apps

Setup basic application governance



Setup Entra ID User settings

- Only administrators are Allowed to register applications.
- Only administrators are allowed to consent to applications.
- An admin consent workflow be configured for applications.
- Group owners should not be allowed to consent to applications.

⊗ Caution

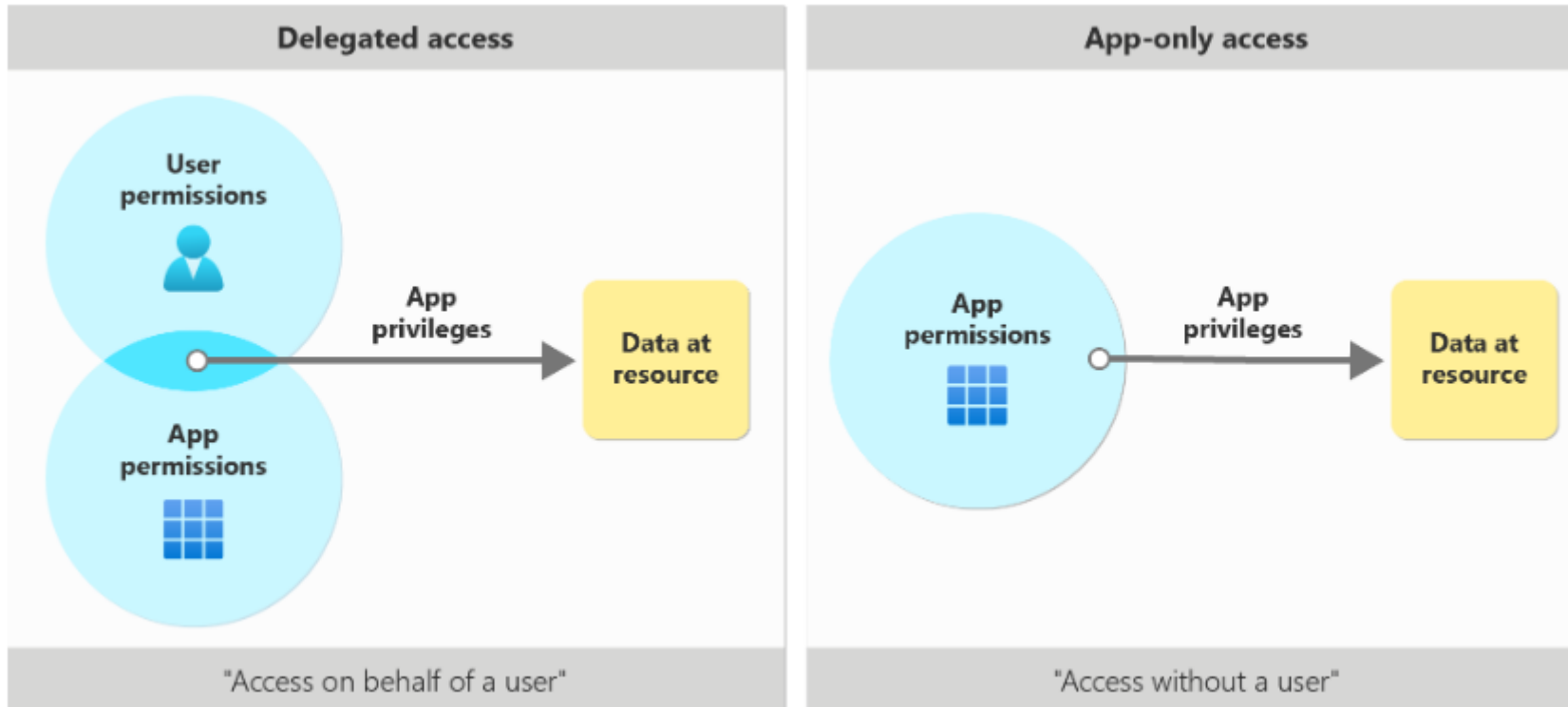
Using the Restrict access to Microsoft Entra administration portal switch is NOT a security measure. For more information on the functionality, see the table below.

Toolkits for Entra ID Ops

- MFA Sweep
- Native Tools
 - Entra ID portal: Microsoft Entra application activity and workbooks ++
 - Security portal: App Governance
- MSIdentityTools
- Azurehound (limit 1gb on bloodhound CE version)
- AzADServicePrincipalInsights by JulianHayward
- ScubaGear – State against CISA baselines
- <https://graphpermissions.merill.net/>

Navigating Entra ID: Consents

Delegated vs application



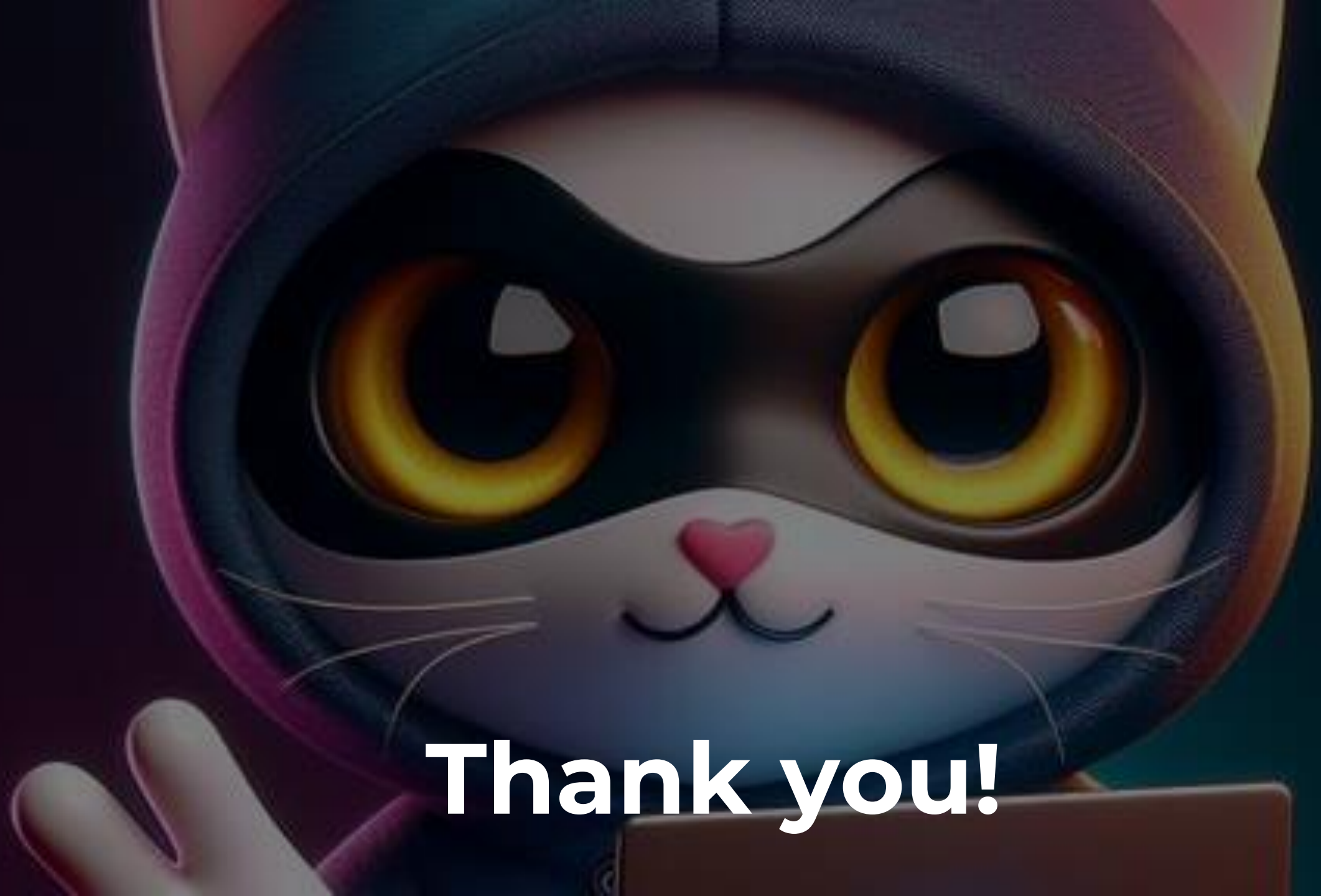
A 3D rendered cat character with large, expressive yellow eyes, a small pink heart-shaped nose, and a blue hoodie with a pink inner lining. The cat is holding a laptop with a glowing blue 'M' logo on its lid. The background is a soft gradient of white and light blue.

Demo time
tools for
admins

My recommendations



Assess and monitor	Assess and monitor identities and application continuously
Alerting	Implement alerting (automation if possible) for high value assets and applications
Process	Have a process to remove inactive, over-permissive apps and “global admins”
3 rd party control	Have routines for dealing with 3rd party vendors, service providers, and applications.



Thank you!