# Real world attacks abusing your Entra ID application misconfigurations

Workplace Ninjas

# Thank you Sponsors



## Platinum Sponsor

robopack
empowered by SOFTWARE CENTRAL

DEVICIE

## Gold Sponsors

RECAST SOFTWARE

glueck kanja

control UP

Microsoft

PATCH MY PC

inforcer

## Silver Sponsors

juriba

numecent
CLOUDPAGING DELIVERS

nerdio

liquidware

LOGINVSI

Rimo3

FERROQUE SYSTEMS

# About us


**Eric Woodruff**

Schenectady, New York
@ericonidentity
/in/ericonidentity
ericonidentity.com
semperis

**Chris Brumm**

Hamburg, Germany
@cbrhh
/in/christopherbrumm
chris-brumm.com
glueckkanja AG


Identity Ninjas
Microsoft MVPs

# Agenda

**The many ways of “what could possibly go wrong?”**

- ✓Mess things up with poor permissions management!
- ✓Get compromised with illicit consent!
- ✓Screw it up with improper app settings!
- ✓Get hacked with poor credential handling!




SECURITY INDUSTRY
ENTERPRISE APPLICATION
IS THIS A NON-HUMAN IDENTITY?

# What is a non-human identity?

In the context of Entra ID

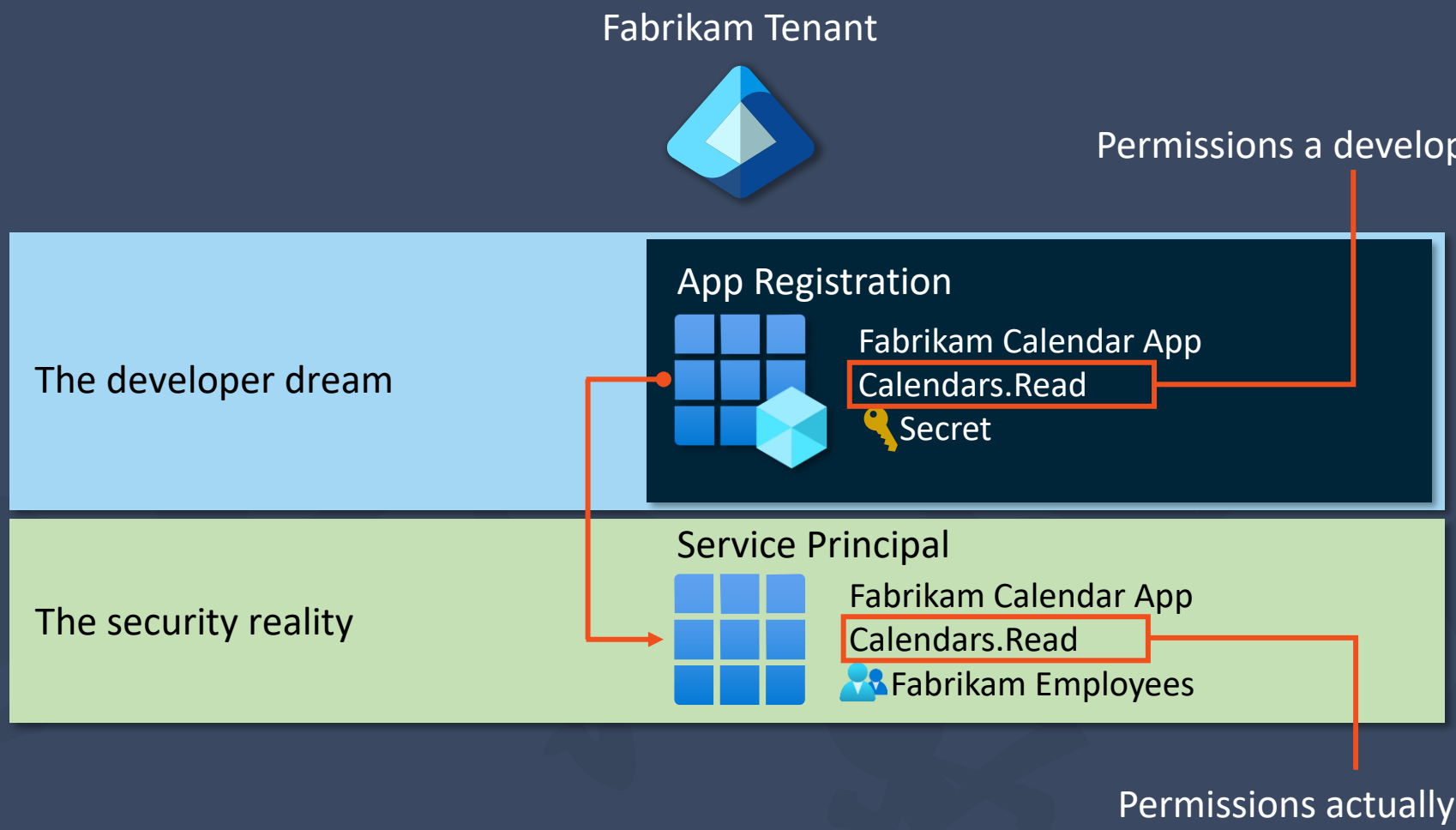
**Service Principal**
Application
[Enterprise Application]

**Service Principal**
Managed Identity

**User Account**
Acting as a service



# Service principals and app registrations






Mess things up with poor permissions management!

Workplace Ninjas

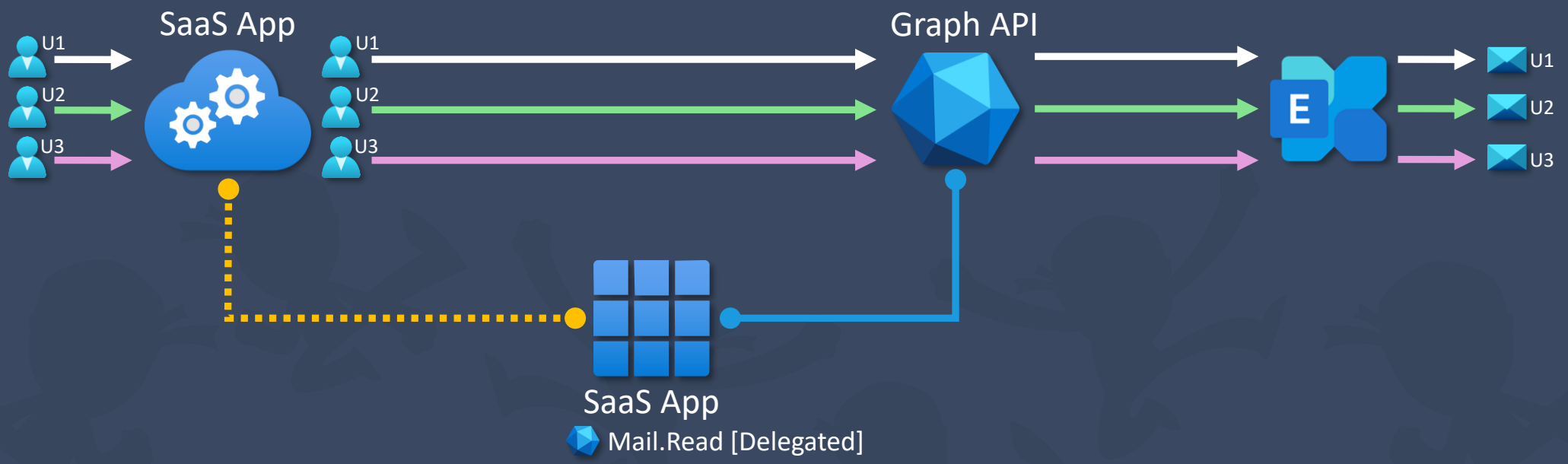
# Types of permissions

**App Permission**

**Delegated Permission**

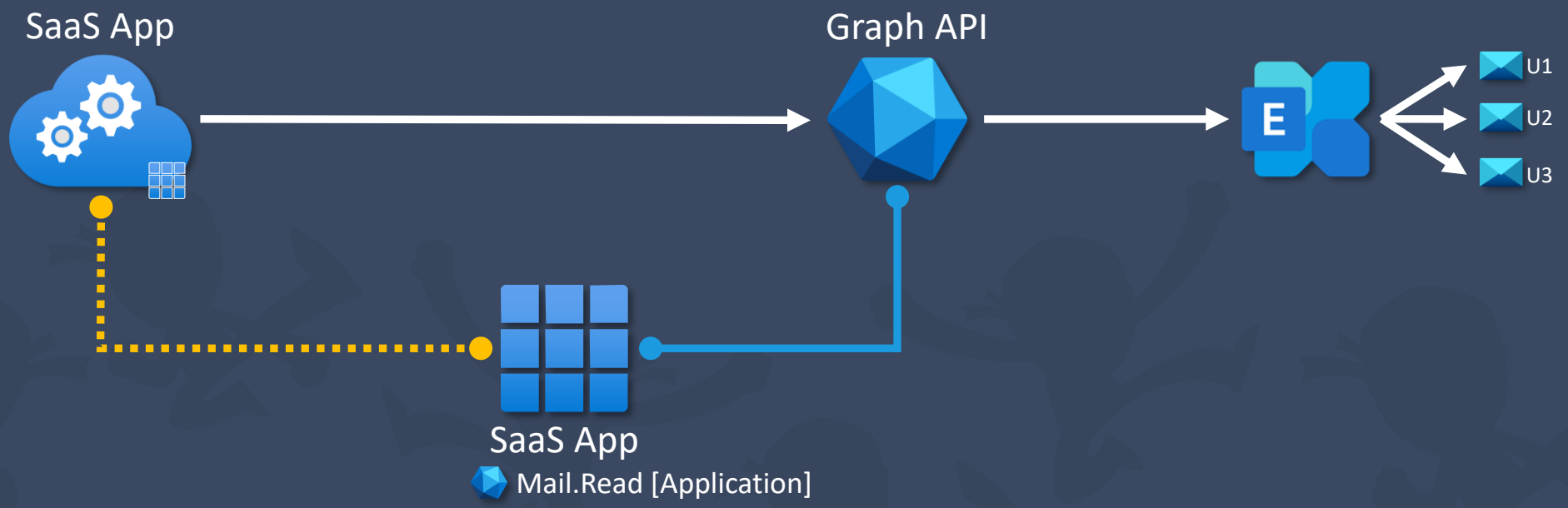


# Delegated Permissions



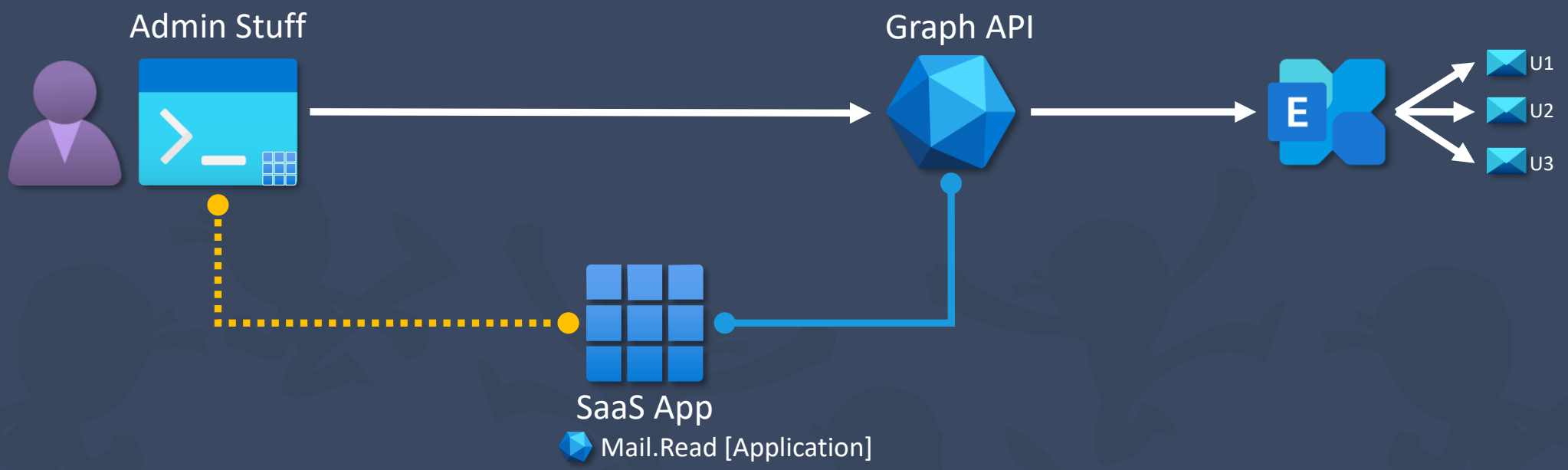



# Application Permissions



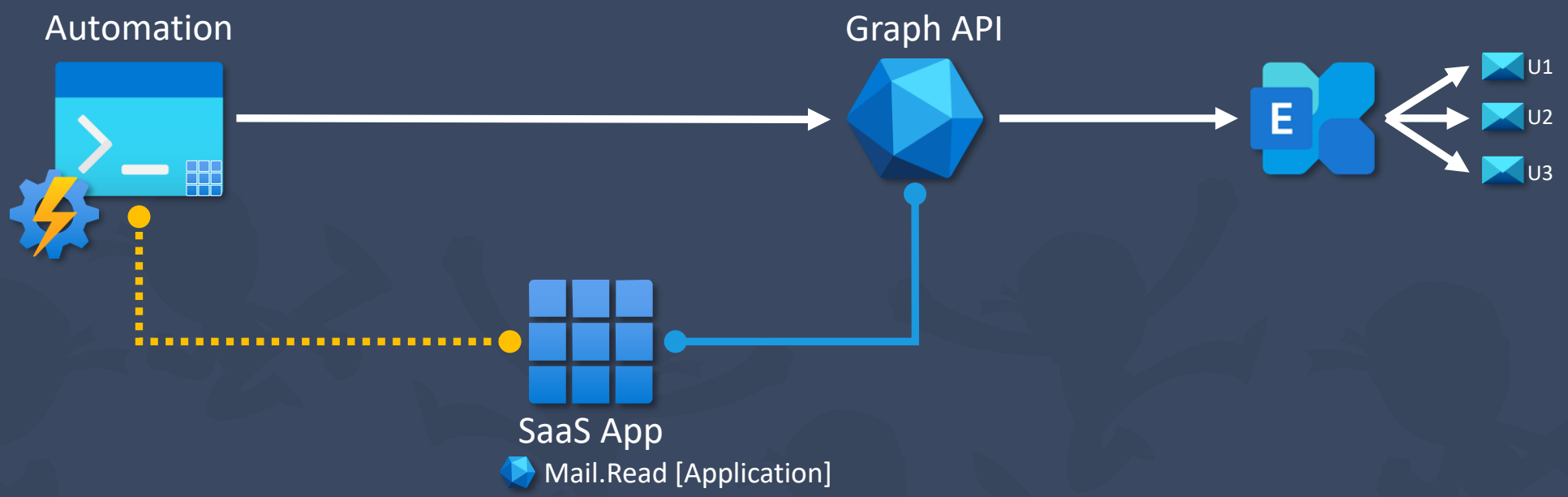



# Application Permissions






# Application Permissions






# A summary so far

## App Permission

Permissions assigned to the app itself.

Used for e.g. scheduled jobs independent from the user

**Example:** Backup of all mailboxes by a 3rd Party Product

## Delegated Permission

Permissions from the logged in user are temporary delegated to the app.

Used for accessing Services for the user.

**Example:** Creating an appointment in the calendar of the user.



# Permissions on Apps

## Entra Roles

Global Administrator
Application Admin
Cloud Application Admin

**Scope: Tenant or App**

## Default Permissions

User can register apps
creator assigned as Owner

**Scope: App**

## Owner Permission

**have full control**
**are not protected like admins**

**Scope: App**



# What's the problem with owners?

As a best practice, we recommend proactive monitoring applications in your environment to ensure there are at least two owners, where possible, to avoid the situation of ownerless apps. Additionally, you should utilize the serviceManagementReference property on the application object to reference the team contact information from your enterprise Service or Asset Management Database. The serviceManagementReference property ensures you have team contact even if an individual leaves the organization.

https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/overview-assign-app-owners



# What’s the problem with owners?

## No *Admin Protection*

Auth Admin vs. Priv Auth Admin

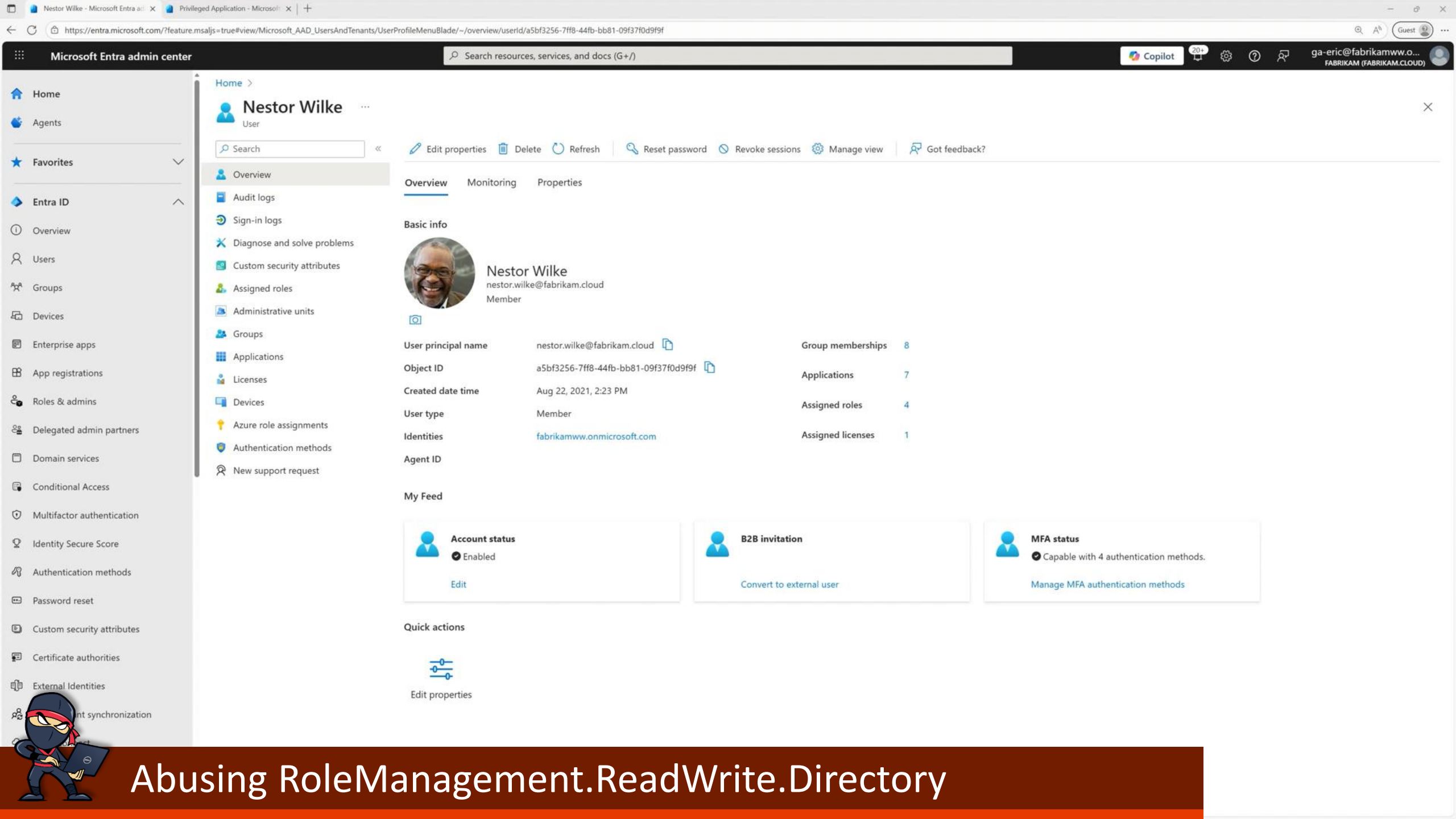
## No granularity

Always full control

## No just-in-time

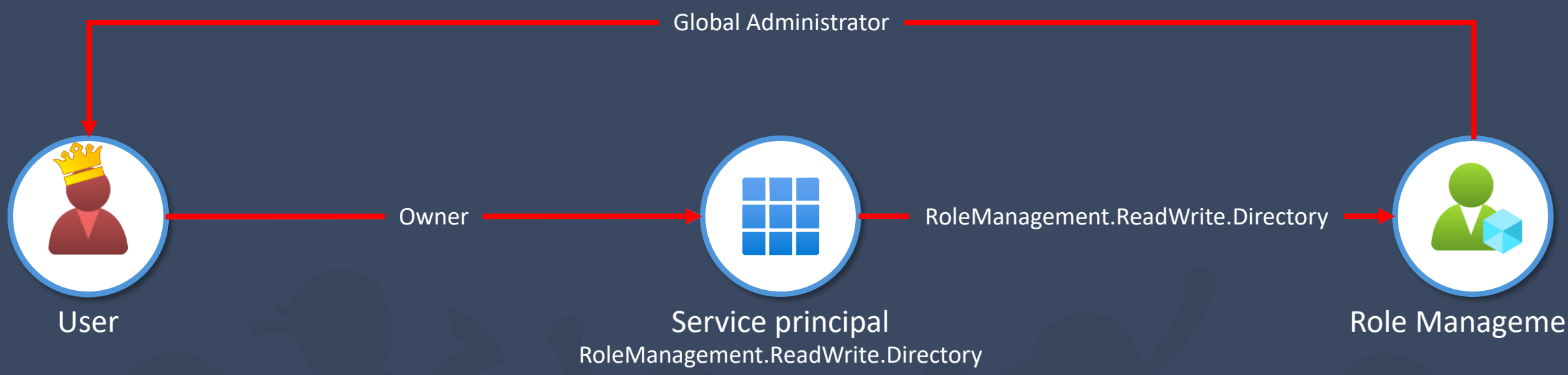
Always full control






# Abusing RoleManagement.ReadWrite.Directory

# RoleManagement.ReadWrite.Directory






Users - Microsoft Entra admin cer | Privileged Application - Microsoft | Graph Explorer | Try Microsoft Gra

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Overview/appId/49878ee9-8eb6-4f42-a199-f49a551da31e/isMSAApp~/false

Microsoft Entra admin center | Search resources, services, and docs (G+/) | Copilot | ga-eric@fabrikamww.o... FABRIKAM (FABRIKAM.CLOUD)

- Home
- Agents
- Favorites
- Entra ID
  - Overview
  - Users
  - Groups
  - Devices
  - Enterprise apps
  - App registrations
  - Roles & admins
  - Delegated admin partners
  - Domain services
  - Conditional Access
  - Multifactor authentication
  - Identity Secure Score
  - Authentication methods
  - Password reset
  - Custom security attributes
  - Certificate authorities
  - External Identities
  - nt synchronization

Home > Enterprise applications | All applications > Privileged Application | Overview > App registrations >

# Privileged Application

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

**Support + Troubleshooting**

- New support request

Delete | Endpoints | Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

**Essentials**

| | | | |
|---|---|---|---|
| Display name | : Privileged Application | Client credentials | : 0 certificate, 1 secret |
| Application (client) ID | : 49878ee9-8eb6-4f42-a199-f49a551da31e | Redirect URIs | : Add a Redirect URI |
| Object ID | : 6ca90b6a-0c1c-42a7-83b1-85ee59f3ed29 | Application ID URI | : Add an Application ID URI |
| Directory (tenant) ID | : 11ae06df-10e8-4b9e-bf66-2a91f4955339 | Managed application in l... | : Privileged Application |
| Supported account types | : My organization only | | |

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Get Started | Documentation

## Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

### Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API permissions

### Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

View all quickstart guides

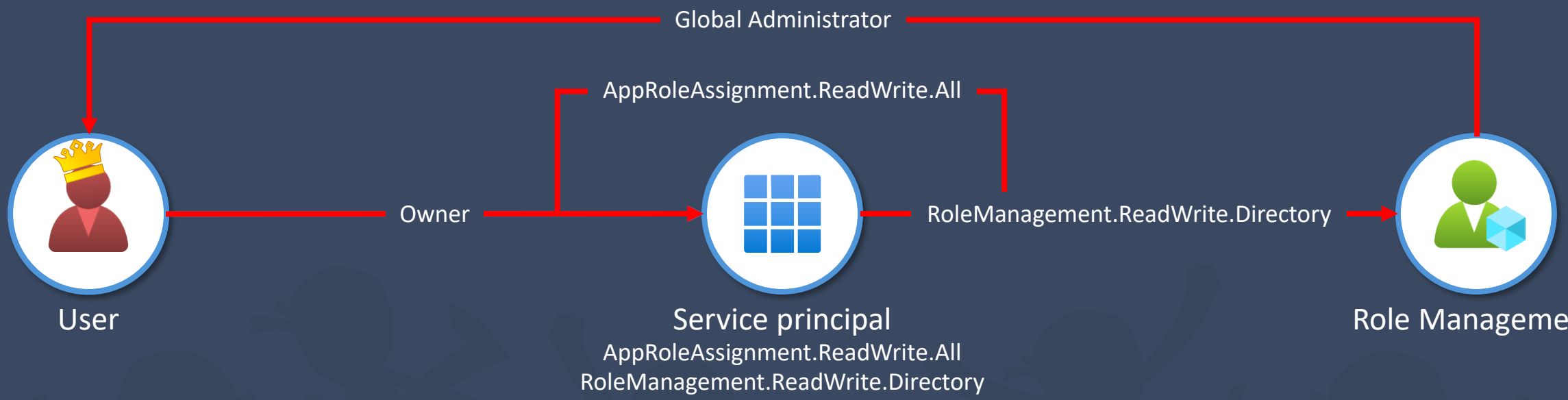
### Configure for your organization

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

Go to Enterprise applications

# Abusing AppRoleAssignment.ReadWrite.All

# AppRoleAssignment.ReadWrite.All






# How did the attacker find the victim?


Cloud-Architekt/
**EntraOps**

Community project to classify, identify and protect your privileges based on Enterprise Access Model (EAM)

2 Contributors · 12 Issues · 186 Stars · 24 Forks

RedByte1337/
**GraphSpy**

Initial Access and Post-Exploitation Tool for AAD and O365 with a browser-based GUI

3 Contributors · 2 Used by · 893 Stars · 101 Forks

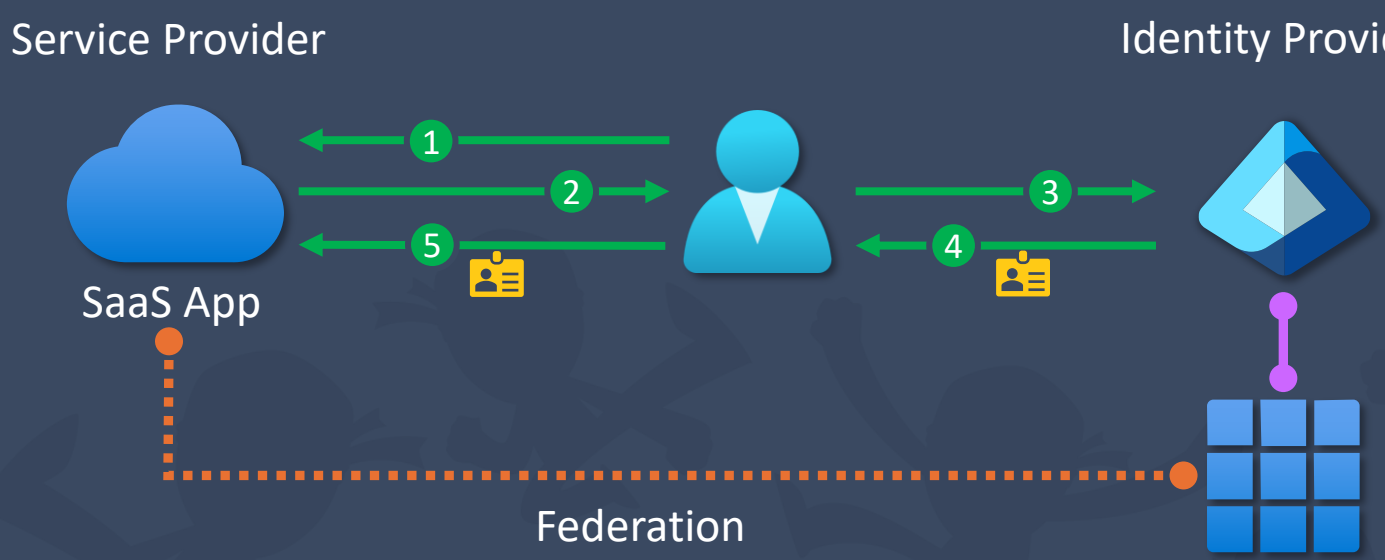
JulianHayward/
**AzADServicePrincipalIns...**

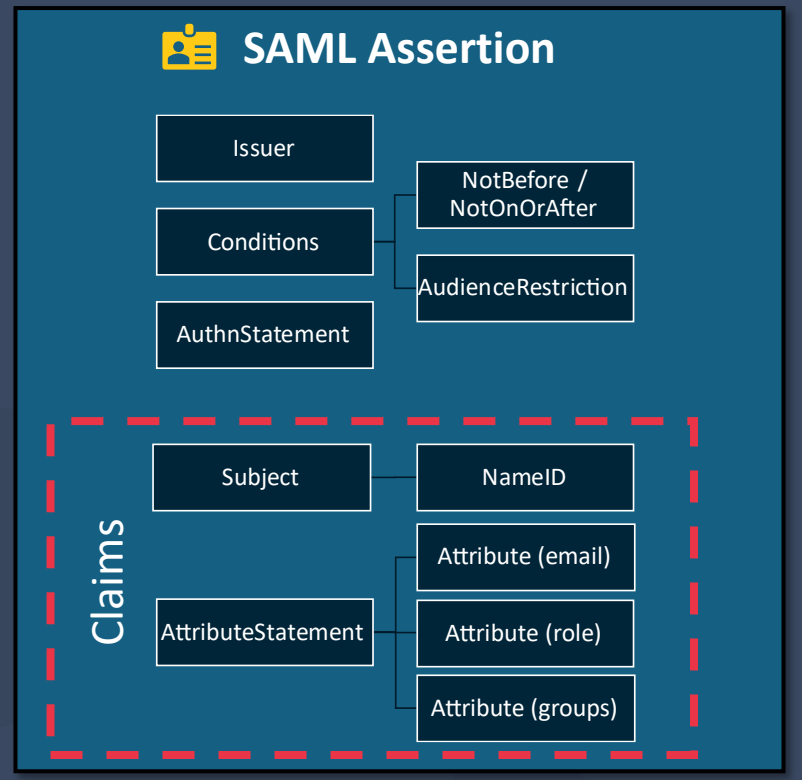
Insights and change tracking on Microsoft Entra ID Service Principals (Enterprise Applications, Applications and Managed Identities)

7 Contributors · 0 Issues · 239 Stars · 52 Forks

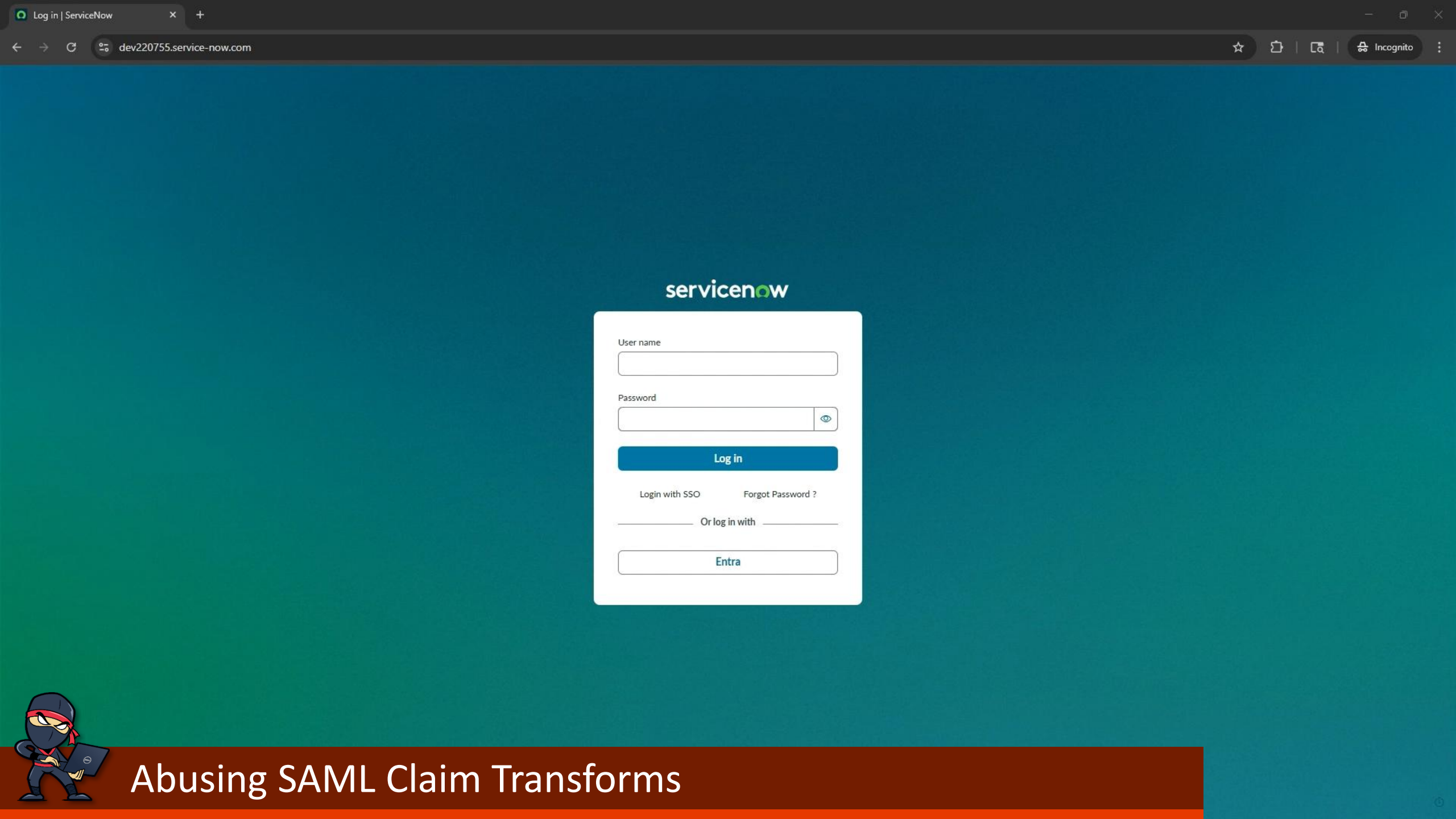


# SAML and Federation






# Abusing SAML Claim Transforms

# Protecting Against bad permission…

~~Owner~~

*Service management reference* attribute or *Security Attributes*

*Cloud App Admin* scoped to the App

~~Office Accounts~~

Admin Accounts ideally with PAW and FIDO

Perform regular and ongoing reviews of permissions



Get compromised with illicit consent!

Workplace Ninjas

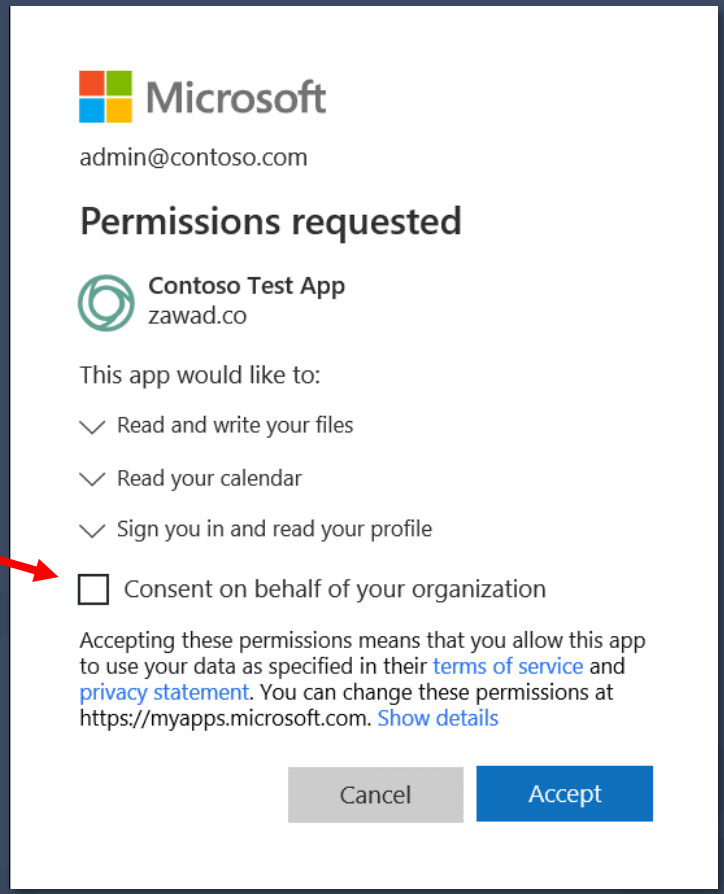
# App consent

## Types of consent

- User permissions
  - limited permissions
  - per user
- Admin permissions
  - extensive permissions
  - per organization

## Granularity of permissions

- Depending on type
  - Application / delegated
- Depending on API
  - Graph, Office 365 Mail API,…






# App Registration and (Illicit) Consent Grant

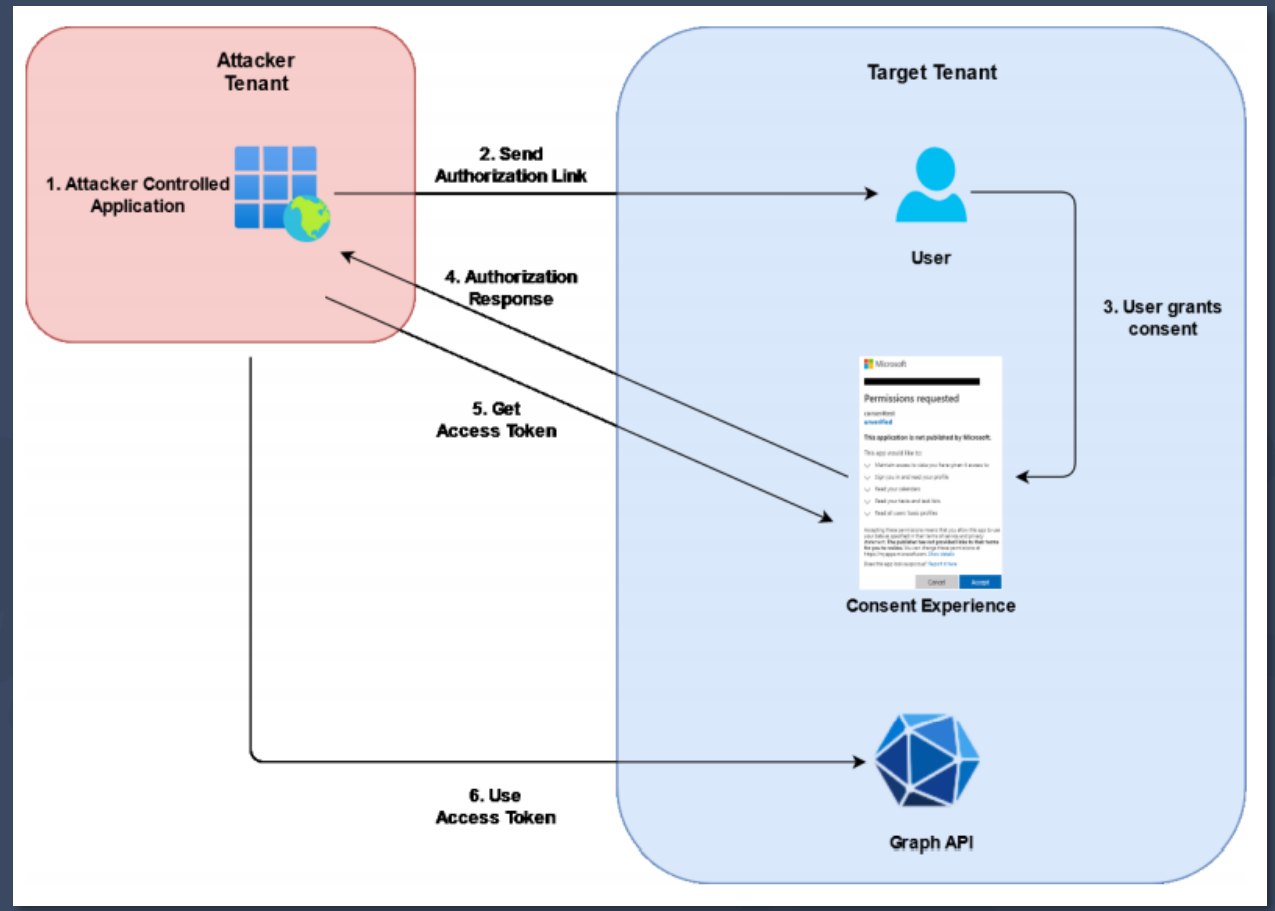
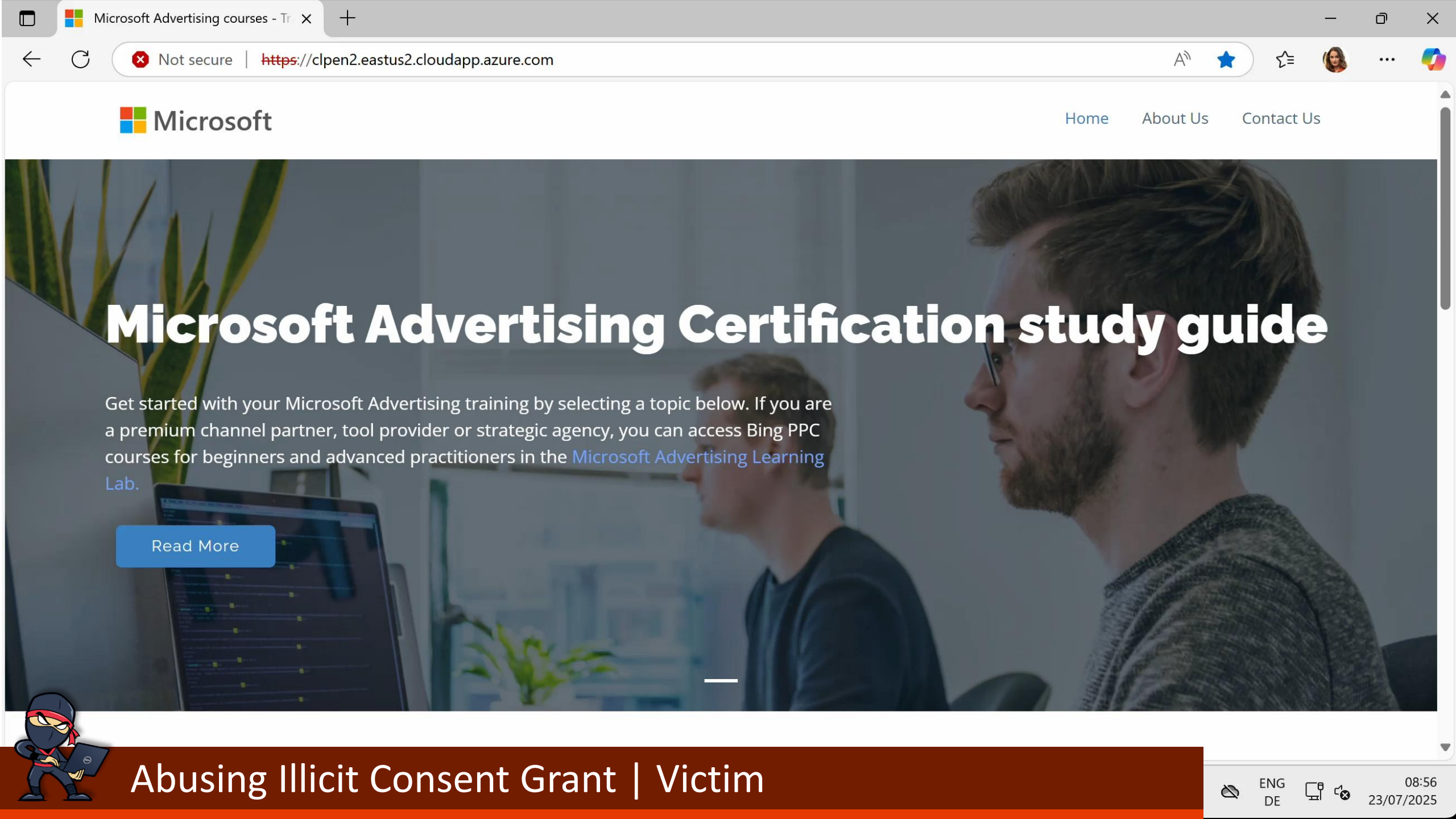



*Image source: Introduction To 365-Stealer by Altered Security*


Microsoft Advertising courses - Tr
Not secure | https://clpen2.eastus2.cloudapp.azure.com
Microsoft
Home
About Us
Contact Us
Microsoft Advertising Certification study guide
Get started with your Microsoft Advertising training by selecting a topic below. If you are a premium channel partner, tool provider or strategic agency, you can access Bing PPC courses for beginners and advanced practitioners in the Microsoft Advertising Learning Lab.
Read More
Abusing Illicit Consent Grant | Victim
ENG
DE
08:56
23/07/2025

365-Stealer Management | New Tab | clpen2.eastus2.clouda...

Not secure https://localhost:8443/365-Stealer/yourVictims/?dir=

**365-STEALER** Home JWT Decoder root


Turn On Auto Refresh | 365-Stealer Configuration | Run 365-Stealer | Shutdown 365-Stealer | Refresh All User's Data

**Index**

**Folders (1)**

@Altered Security | 365-Stealer

# Abusing Illicit Consent Grant | Attacker

ENG DE 6:59 AM 7/23/2025

# Protecting Against Illicit Consent

Microsoft recently changed the default behavior for app consent

Admin consent workflows are a must at this point

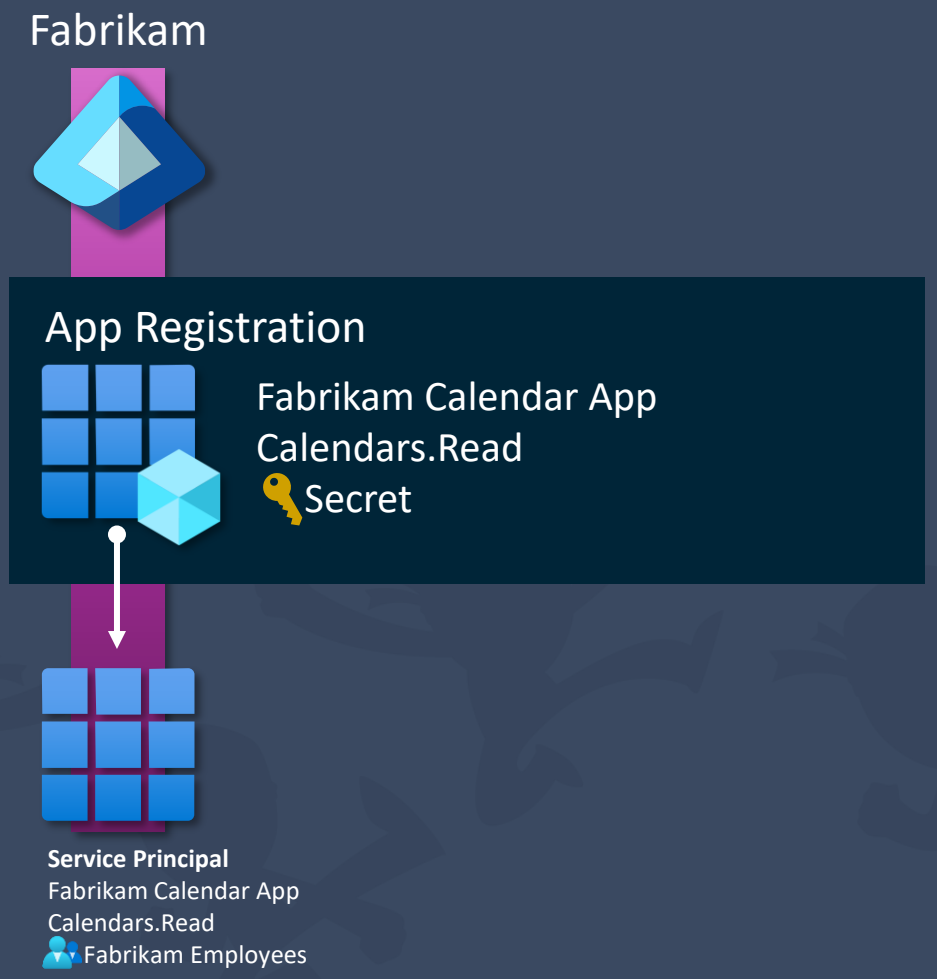
You should evaluate your existing applications for what has been consented



Screw it up with
improper app settings!

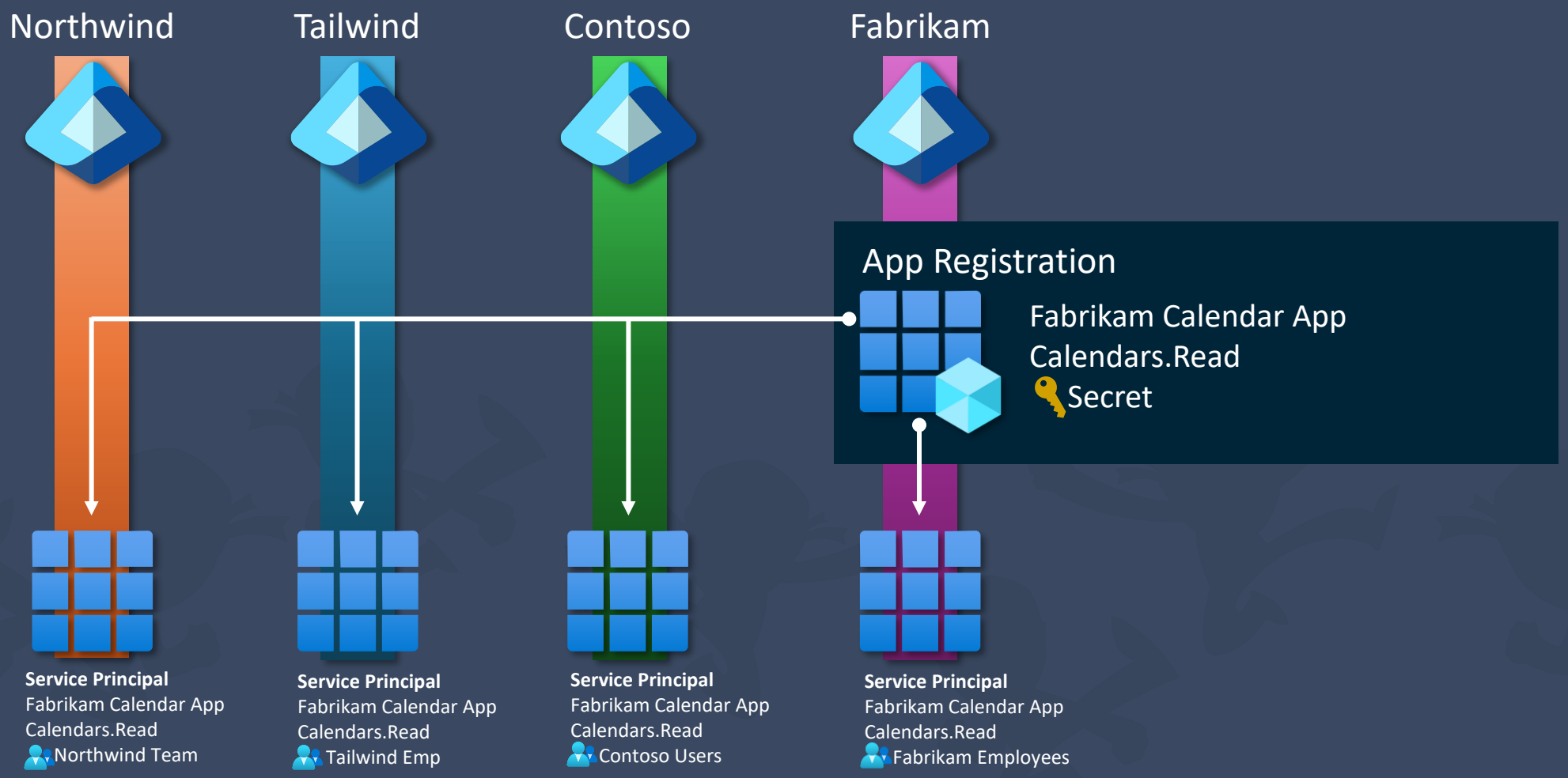
Workplace Ninjas

# Single tenant applications






# Multi-tenant applications






# Accidental multi-tenant applications

Supported account types

Who can use this application or access this API?

- (●) Accounts in this organizational directory only (The Bread Company only - Single tenant)
- ( ) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ( ) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ( ) Personal Microsoft accounts only



# Accidental multi-tenant applications

WIZ Platform Solutions Pricing Resources Customers Company Get a demo

← Blog

## BingBang: AAD misconfiguration led to Bing.com results manipulation and account takeover

How Wiz Research found a common misconfiguration in Azure Active Directory that compromised multiple Microsoft applications, including a Bing management portal

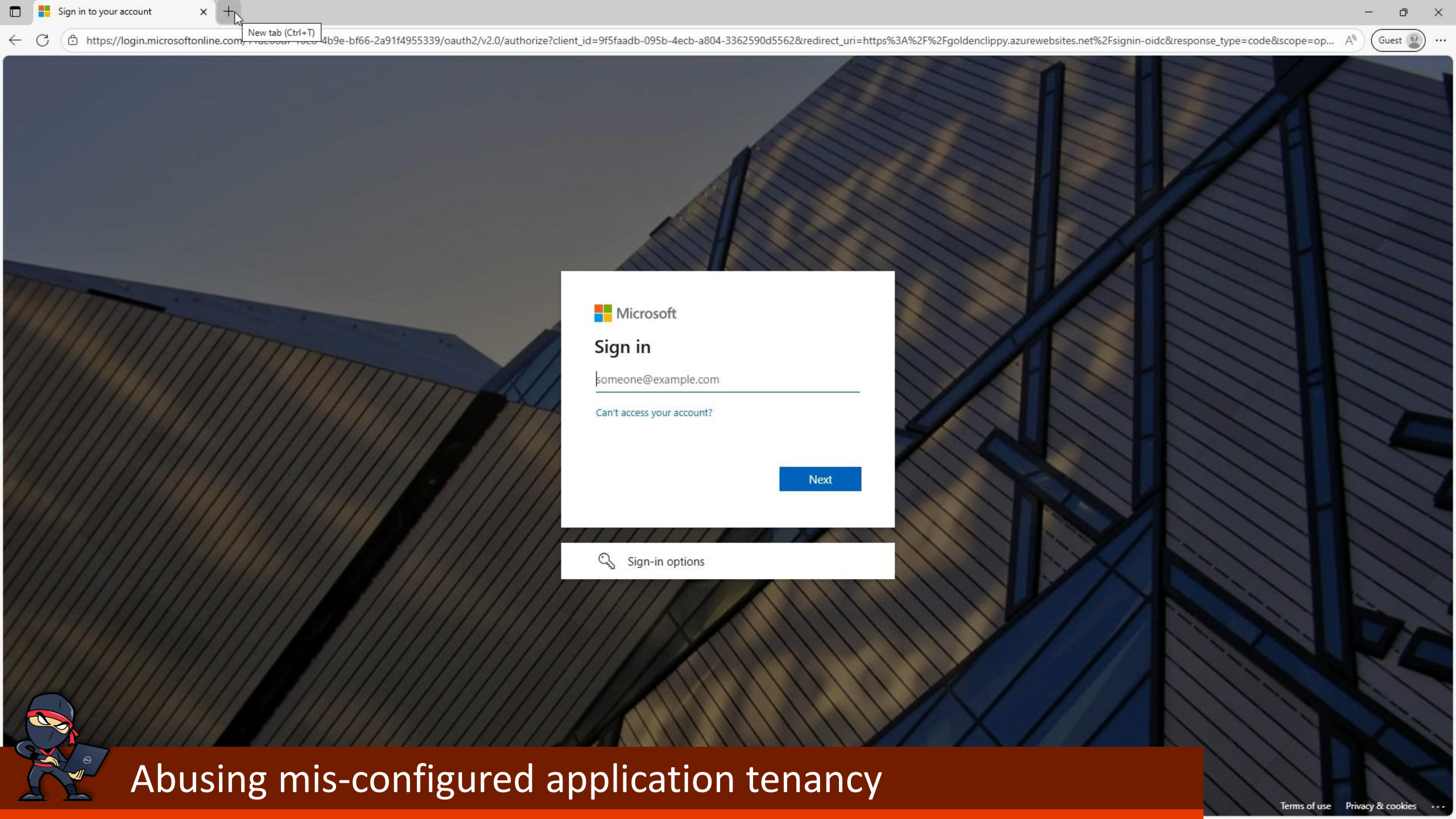
Hillai Ben-Sasson
March 29, 2023
9 minute read

Blog / 2025 / 11 / msrc variant hunting from multi tenant authorization to model context protocol

## INTERN(al) MSRC variant hunting: From multi-tenant authorization to Model Context Protocol

MSRC / By Cameron Vincent / November 10, 2025




Sign in to your account
New tab (Ctrl+T)
https://login.microsoftonline.com/
4b9e-bf66-2a91f4955339/oauth2/v2.0/authorize?client_id=9f5faadb-095b-4ecb-a804-3362590d5562&redirect_uri=https%3A%2F%2Fgoldenclippy.azurewebsites.net%2Fsignin-oidc&response_type=code&scope=op...
Guest
Microsoft
Sign in
someone@example.com
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies
Abusing mis-configured application tenancy

# nOAuth

nOAuth vulnerable applications do not properly implement OpenID Connect

A cross-tenant type attack, the attacker only needs the email address of the victim

Almost impossible to detect and defend against

At its core is developers following anti-patterns with OIDC



# nOAuth | Following OIDC Standards

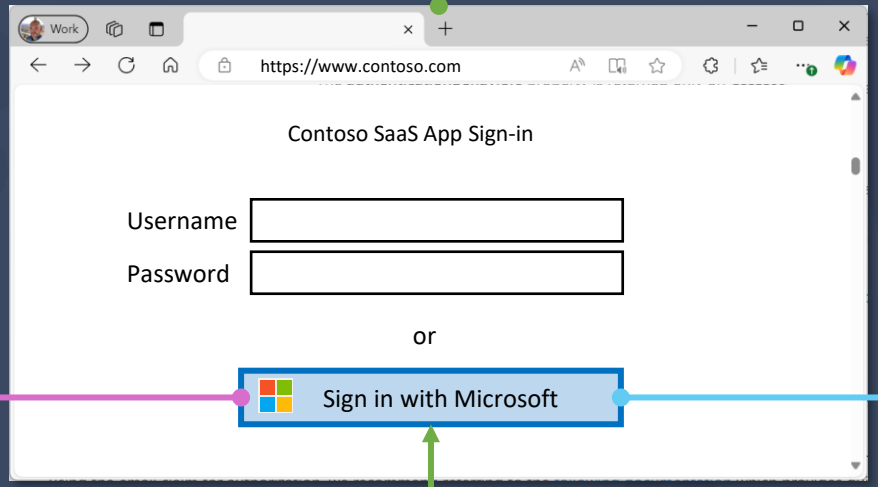

```
{
 "typ": "JWT",
 "alg": "RS256",
 "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
 "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
 "iss": "https://login.microsoftonline.com/dd240f35-22cd-4617-9b9b-24ae1343f53d/v2.0",
 "iat": 1737485278,
 "nbf": 1737485278,
 "exp": 1737489178,
 "aio": "AWQAm/8ZAAAA/",
 "cc": "CgEAEh1tMzY1eDQzNzgwMjE1Lm9u:
 "email": "eric@fabrikam.com",
 "nonce": "123",
 "rh": "1.AXEBNO8k3c0iE0abmySuE0P1PQDQPsvKfy5UWzB8k8vUJBxAVBxAQ.",
 "sub": "BGyjX677G2J1Qwo-ceoduAu8IKyeacDf_rZPkgD-BuQ",
 "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
 "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
 "ver": "2.0"
}.[Signature]
```


ID token from Entra

Contoso.com SaaS app user table

User: Eric
Mail: eric@fabrikam.com
Sub: BGyjX677G2J1Qwo-ceod…
Iss: dd240f35-22cd…

Unique, immutable identifier




Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App



# nOAuth | Vulnerable application

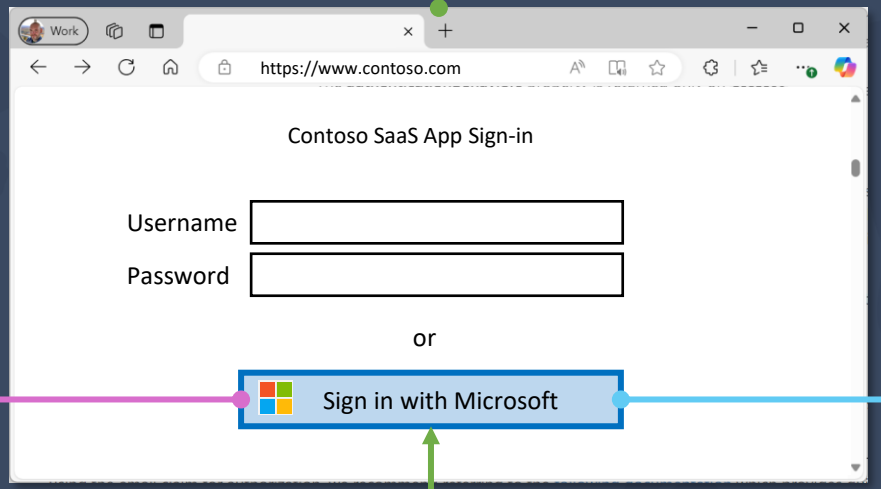

```
{
 "typ": "JWT",
 "alg": "RS256",
 "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
 "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
 "iss": "https://login.microsoftonline.com/dd240f35-22cd-4617-9b9b-24ae1343f53d/v2.0",
 "iat": 1737485278,
 "nbf": 1737485278,
 "exp": 1737489178,
 "aio": "AWQAm/8ZAAAA/",
 "cc": "CgEAEh1tMzY1eDQzNzgwMiF1Lm9u",
 "email": "eric@fabrikam.com",
 "nonce": "123",
 "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
 "sub": "BGyjX677G2J1Qwo-ceoduAu8IKyeacDf_rZPkgD-BuQ",
 "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
 "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
 "ver": "2.0"
}.[Signature]
```


ID token from Entra

Contoso.com SaaS app user table

User: Eric
Mail: eric@fabrikam.com

Non-unique, mutable identifier




Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App



# nOAuth | Abusing a vulnerable app

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com
UPN: eric@evil.cloud

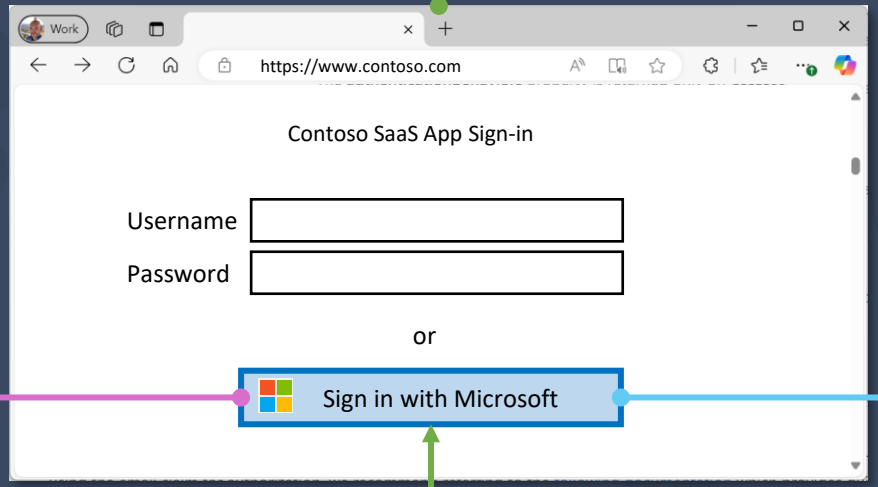
Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com


```
{
 "typ": "JWT",
 "alg": "RS256",
 "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
 "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
 "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
 "iat": 1737485278,
 "nbf": 1737485278,
 "exp": 1737489178,
 "aio": "AWQAm/8ZAAAA/",
 "cc": "CgEAEh1tMzY1eDQzNzgwMiF1Lm9u",
 "email": "eric@fabrikam.com",
 "nonce": "123",
 "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
 "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
 "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
 "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
 "ver": "2.0"
}.[Signature]
```


ID token from Entra



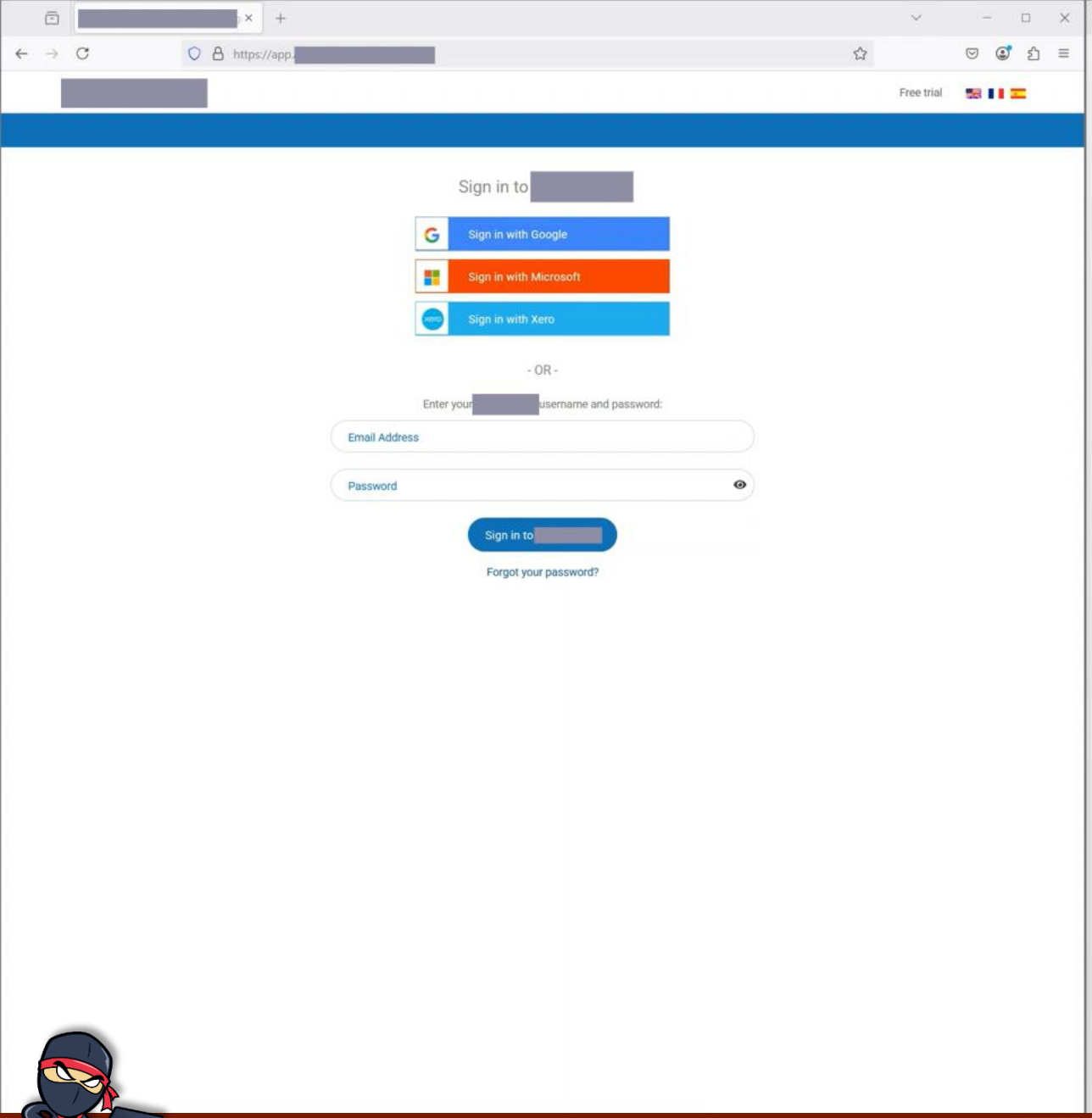

Contoso.com SaaS app user table

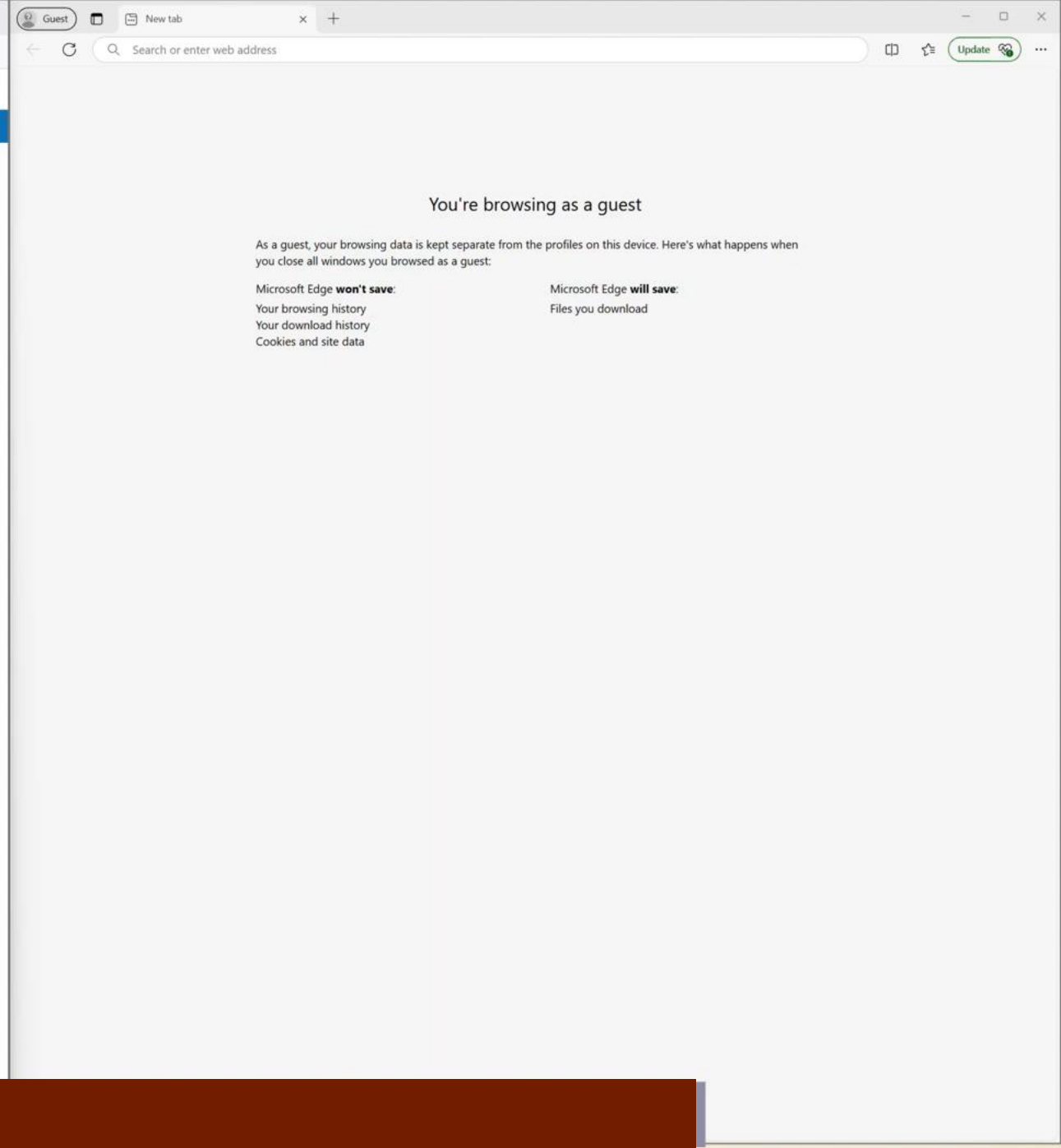
User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App








# A real-world nOAuth attack

# Protecting Against Misconfigurations

Use the *integration assistant* and follow the recommendations



# Security of App Integration

Microsoft Azure | Search resources, services, and docs (G+/) | thomas@cloud-architek... CLOUDLAB

Home > CloudLab > BusinessApp-Auth-WebAPI

**BusinessApp-Auth-WebAPI | Integration assistant**

Search (Ctrl+/)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Refresh | Got feedback?

**Here's the integration assistant for BusinessApp-Auth-WebAPI**

Application type : **Desktop App, Web API** Edit
Calls APIs : **Yes**

Summary | Develop | Test | Release | Monitor

**Recommended configurations**

| Item | Status |
|---|---|
| Configure a redirect URI for a desktop app by adding a platform. | Action required |
| Configure API permissions. | Action required |
| Configure a valid credential. | Action required |
| Configure a unique Application ID URI. | Action required |
| If expecting API requests on behalf of users, define scopes your API exposes. | Action required |
| If expecting API requests on behalf of apps directly, define app roles. | Action required |
| Assign users that should be able to view and edit this application registration as owners. | Complete |

**Discouraged configurations**

| Item | Status |
|---|---|
| If you are using the authorization code flow, disable the implicit grant settings. | Complete |

More details:

- Azure AD application registration security best practices
- Microsoft identity platform best practices and recommendations



# Protecting Against Misconfigurations

Use the *integration assistant* and follow the recommendations

Take additional care for Multitenant Apps

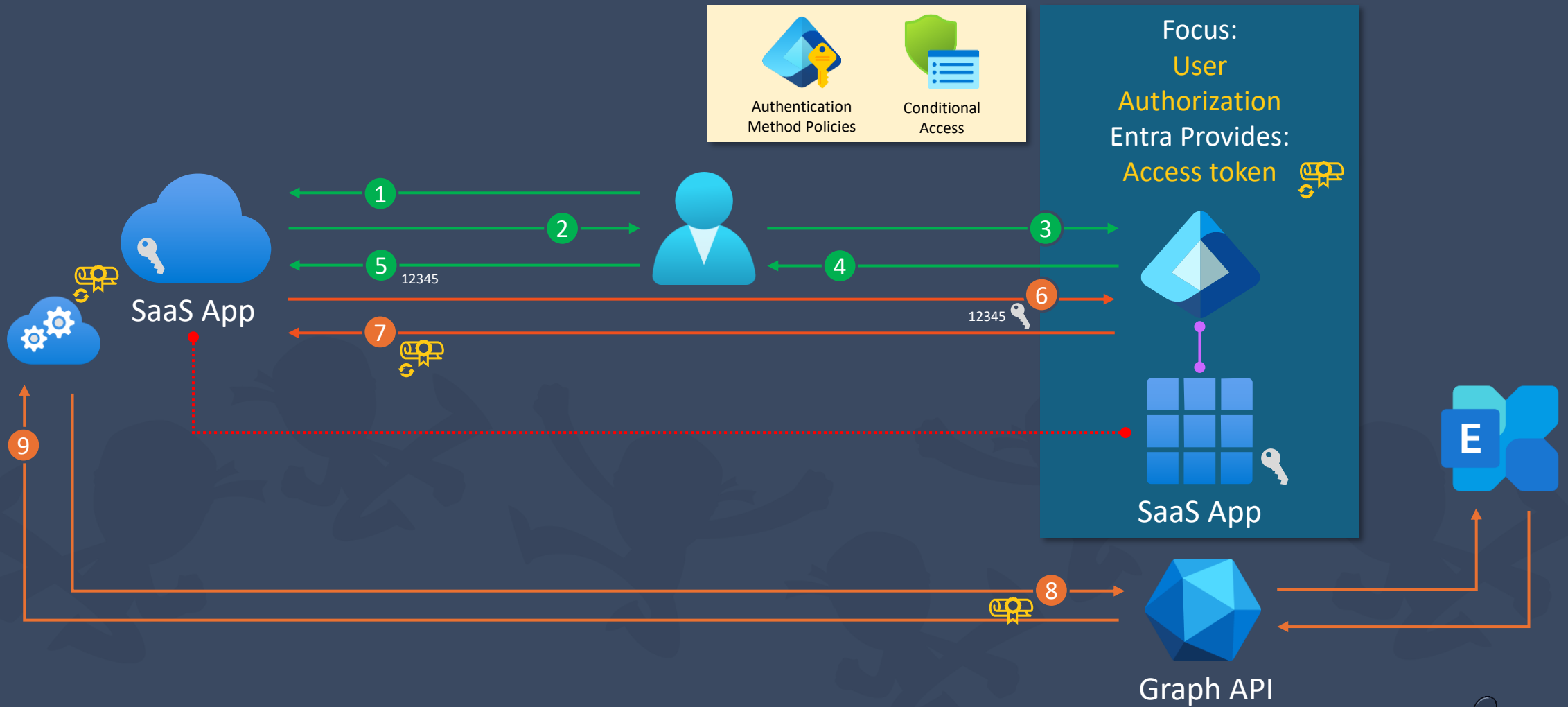
Work with your developers to ensure they are implementing authentication properly



Get hacked with poor credential handling!

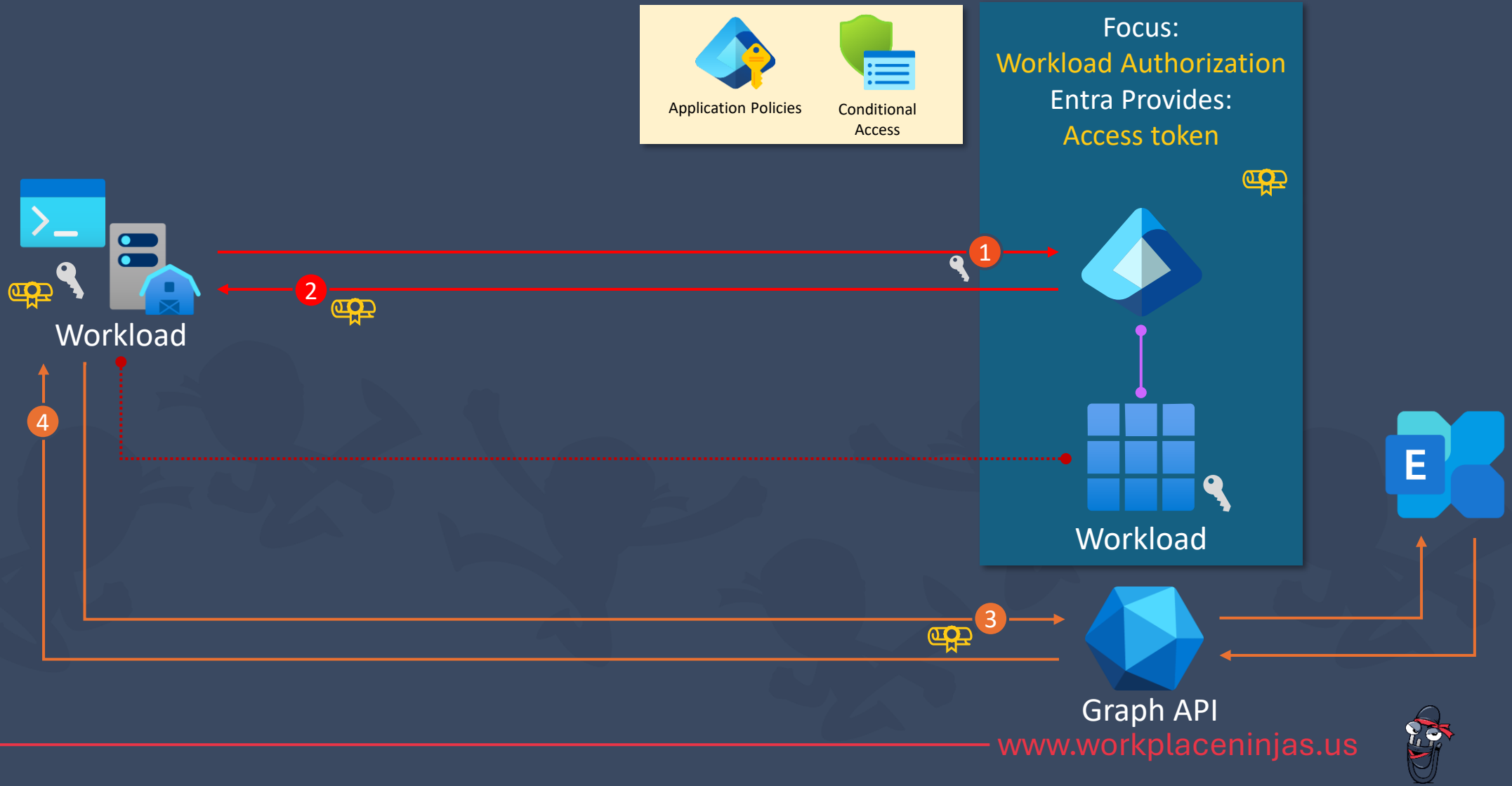
Workplace Ninjas

# User Authentication






# Application Authentication



# Types of credentials

In the context of Entra ID

**Symmetric**
-> Passwords

**Asymmetric**
-> Certificates

**Federated**
-> example: GitHub Action



# SHA1-HULUD 2.0: ONGOING SUPPLY CHAIN ATTACK

new techniques
in Sha1-Hulud 2.0

Wiz Blog
11/24/2025

bun_environment.js
payload

## Initial Compromise

Attacker

Infected Package

Developer Machine

CI Runner

500+ packages
100M+ monthly downloads

## Local Activity

25k repos
500+ unique users

Inject Malicious Workflow

Sha1-Hulud Runner (Backdoor)

Conditional Wiper

local .env
cloud creds
trufflehog
workflow secrets

Secrets Collection

NPM Publish

exfil & C2

GitHub keys found

GitHub keys not found

## CI/CD Pipleline (GitHub Actions)

Victim's CI/CD Pipleline

Secrets Exfiltration

Remote Control (Backdoor)

Other Victim's CI/CD Pipleline

Secrets Exfiltration

possible impact

## Cloud Env (AWS/Azure/GCP)

Credential Theft

Privilege Escalation

worm-like propagation

## Supply Chain

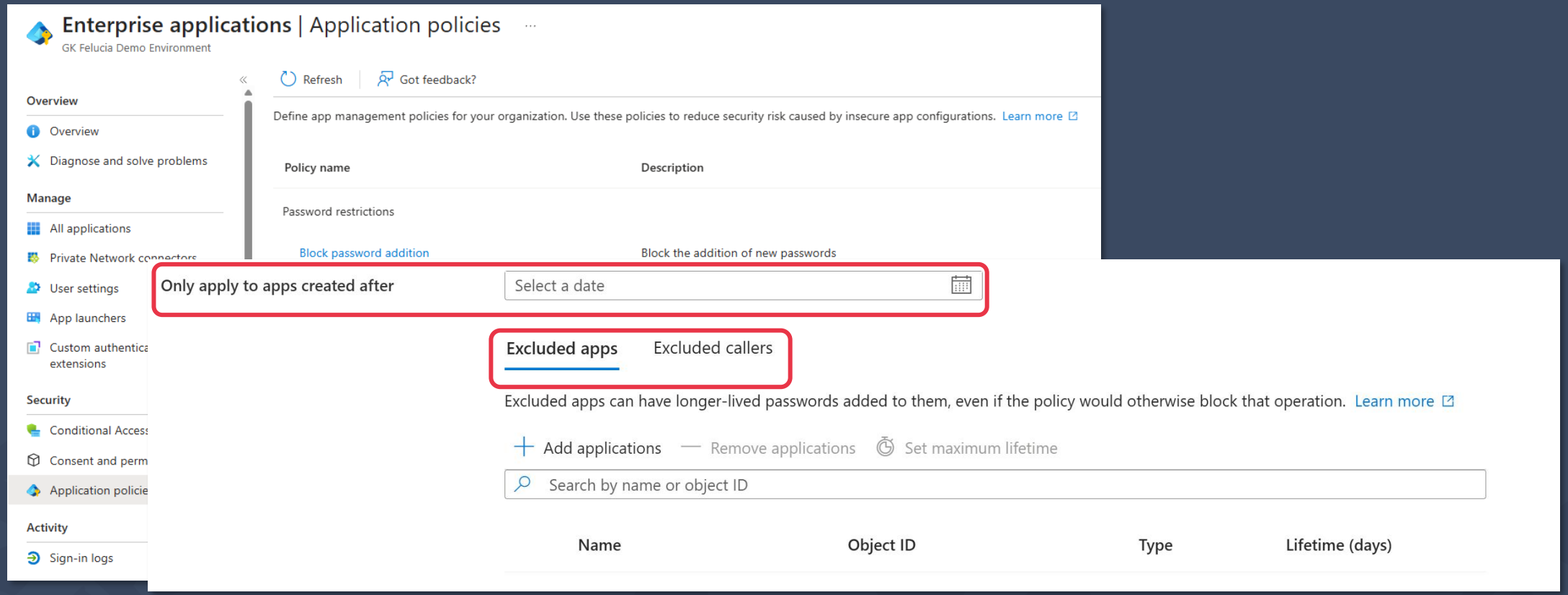
preinstall script

setup_bun.js

bun_environment.js

WIZ Research

# Application Management Policies



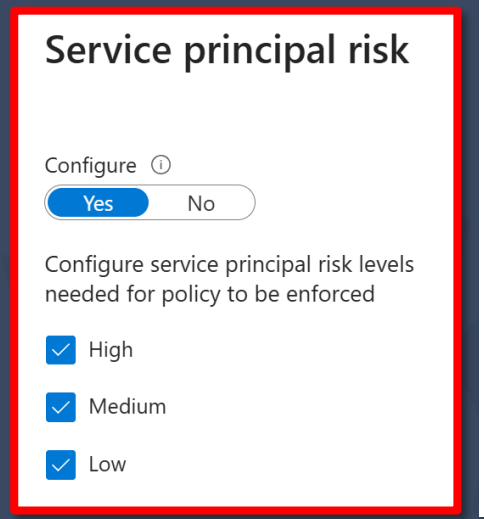


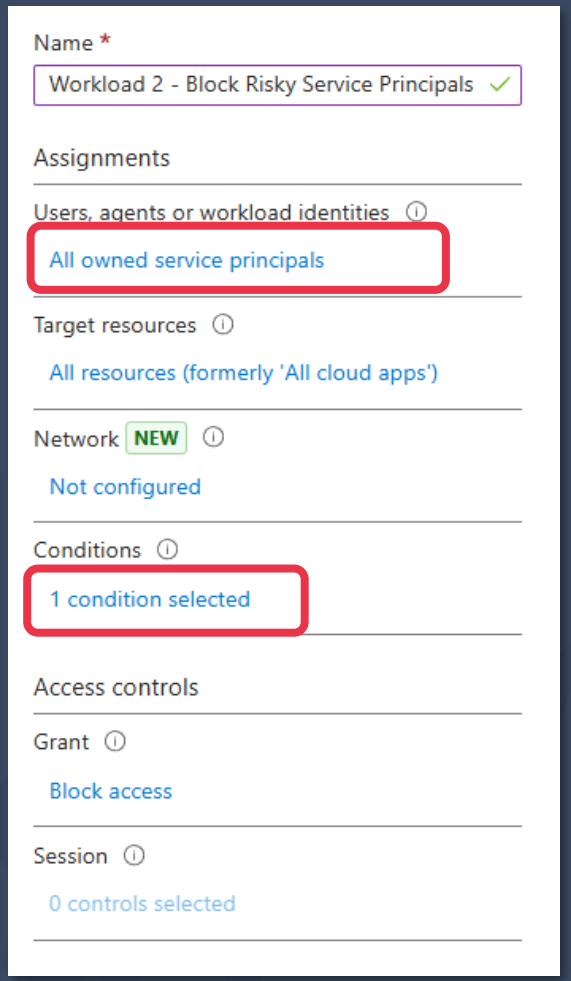

# Conditional Access for workload identities

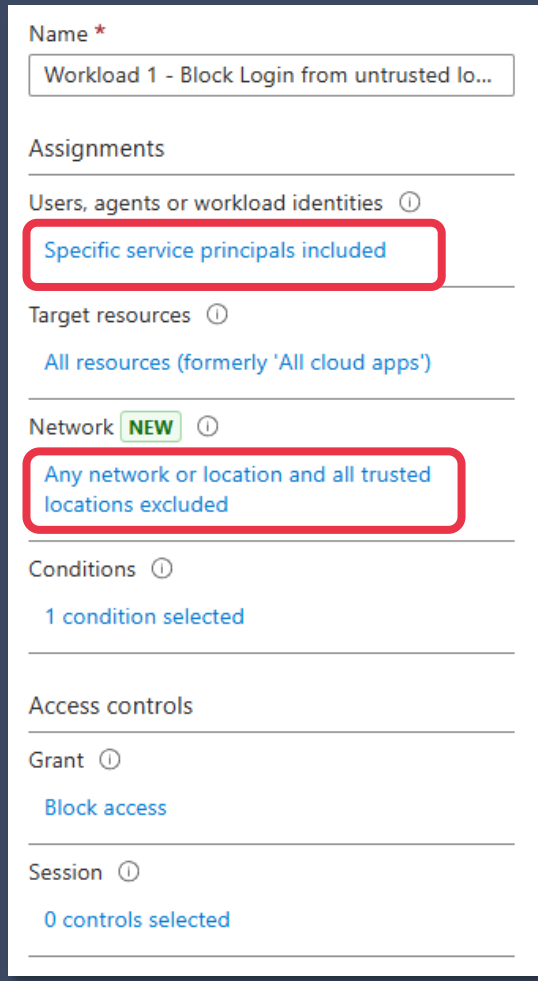
You are able to restrict the access to **trusted locations!**

➔Requires fixed IPs

You are able to restrict the access to SPs without a risk!

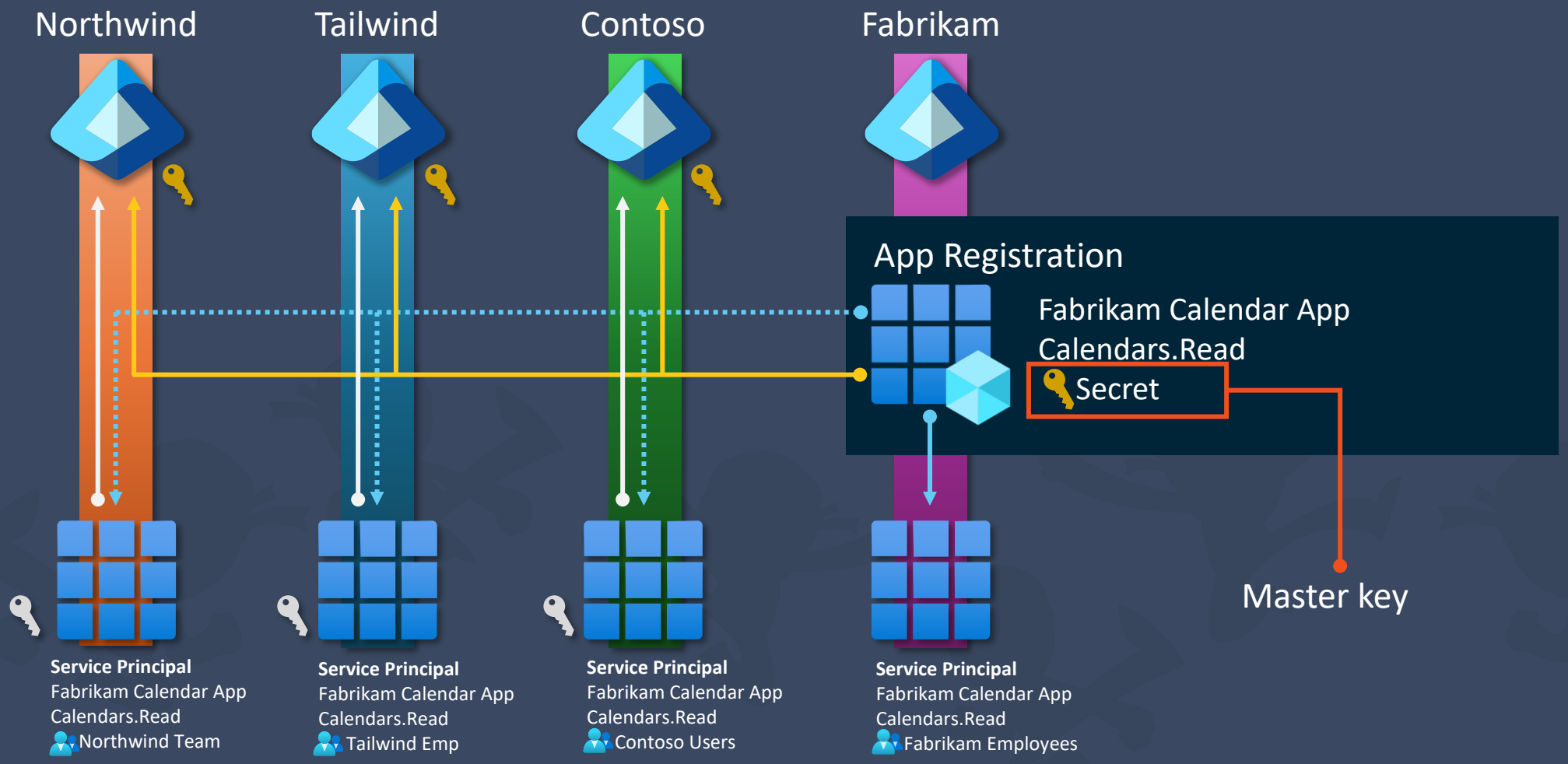





# Multi-tenant applications






# App instance property lock

Dashboard > CloudLab | App registrations > BusinessApp-Auth-WebAPI

**BusinessApp-Auth-WebAPI | Authentication**

Search

Got feedback?

- Overview
- Quickstart
- Integration assistant

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

**Support + Troubleshooting**

- Troubleshooting
- New support request

Access tokens (used for implicit flows)

ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (CloudLab only - Sing

Accounts in any organizational directory (Any Azure AD directory -

Help me decide...

Due to temporary differences in supported functionality, we don't rec accounts for an existing registration. If you need to enable personal a editor. Learn more about these restrictions.

Advanced settings

**Allow public client flows**

Enable the following mobile and desktop flows:

App instance lock allows sensitive properties of an application to be locked. When configured and enabled, the service principal of the application would not allow modification of the selected sensitive properties.

App instance property lock

Configure the application instance modification lock. Learn more

## App instance property lock

BusinessApp-Auth-WebAPI

Prevent malicious attacks by blocking the modification of sensitive properties on instances of this application.

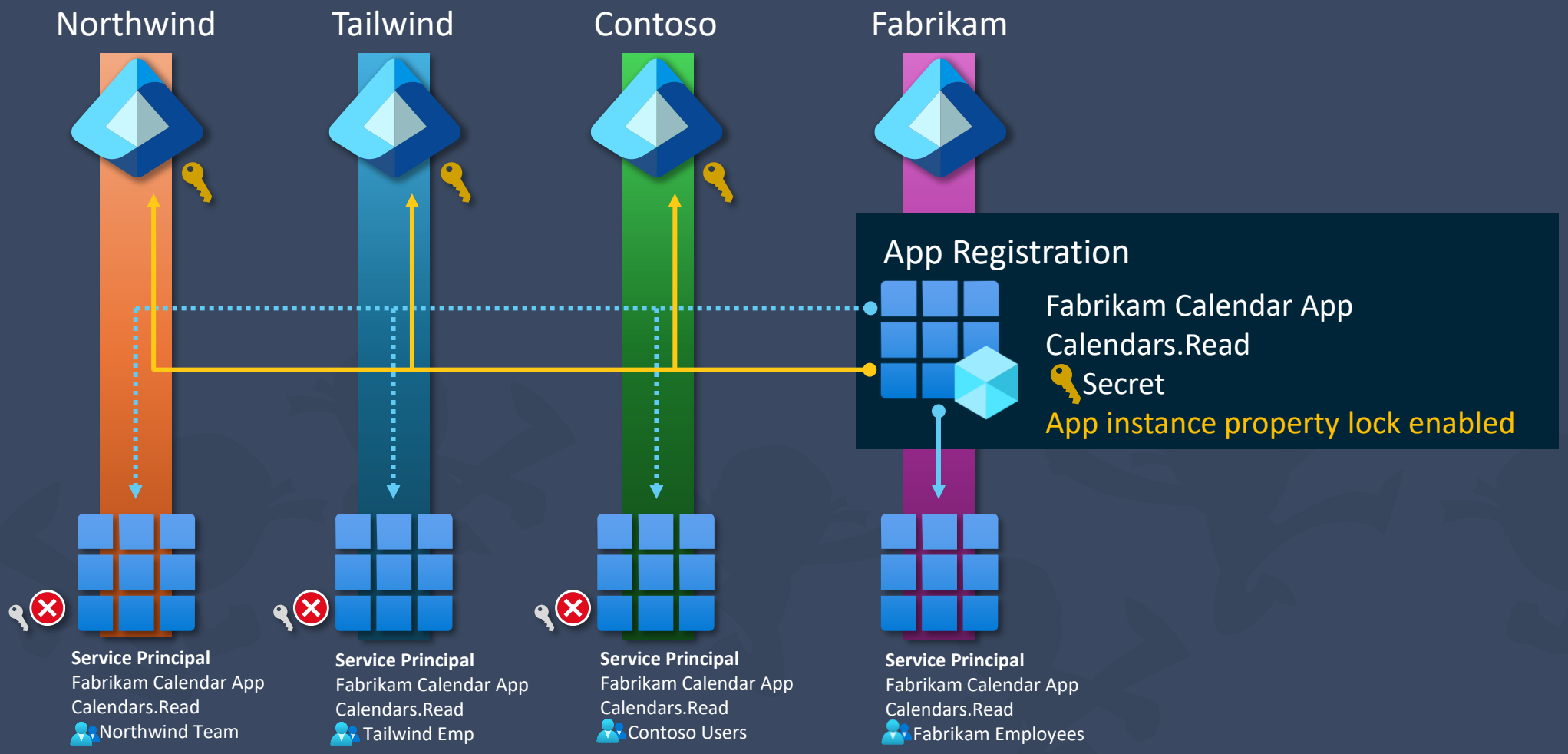
Enable property lock

Locked properties

Credentials used for verification



# App instance property lock






# Protecting Against Credential Abuse

~~Secrets/passwords~~

Use Certificates, Managed Identities or Federated Creds

Introduce the Workload ID features
Identity Protection and Conditional Access

Monitor your Workload Identities with Sentinel

*Anomalies, Credential-adding, …*



# Summary

Free tools can help you be a ninja

BLOODHOUND COMMUNITY EDITION

forest druid

Maester

EntraOps

purple knight

ENOW AppGov

AzADSPI

Agent ID is only going to complicate things more if you don't have strong workload identity management

Caring for workload identities must be a critical part of your identity governance strategy



# Questions?

# Thank You!