Attack on Token

Attack on Token

Why post-auth attacks are the next frontier

Workplace Ninjas Norway

#WPNinjasNO

Thank you sponsors

Workplace Ninjas Norway

Community Sponsors

Microsoft

Gold Sponsors

PATCH MY PC

robopack empowered by SOFTWARE CENTRAL

ZERO TOUCH

POINT:TAKEN

Silver Sponsors

Evidi

nerdio

bsure.

Fortytwo.io

CloudWay

twoday

controlUP

#WPNinjasNO

About Fabian

Focus

Cyber Security, Identity,
Microsoft SIEM & XDR @ glueckkanja

From

Hamburg, Germany

My Blog

cloudbrothers.info

Certifications

Microsoft MVP

Hobbies

Concerts, KQL, User Groups

Contact

Socials (BlueSky, Mastodon, Twitter)

What are tokens?

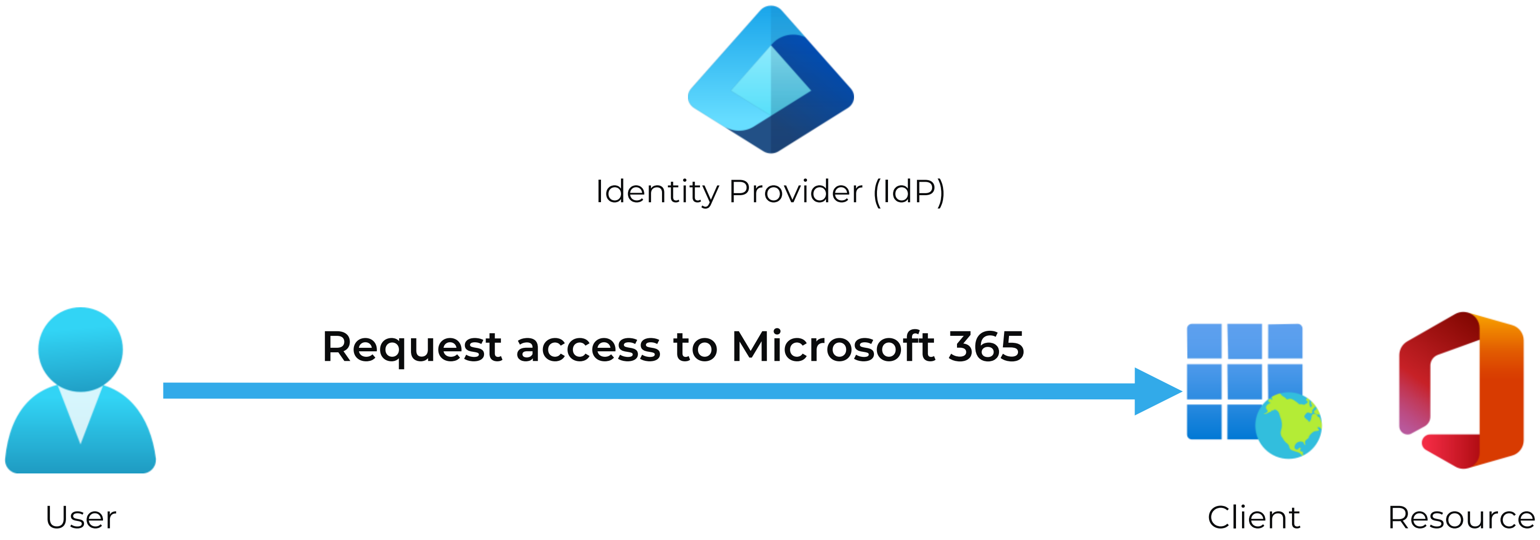
- Like a key to access a resource
- Issued after authentication
- Well known and used protocols
  - OAuth 2.0
  - OpenID Connect (OIDC)
  - Security Assertion Markup Language (SAML)

Token in Entra ID

- Bearer Token
  - Access Token (60 - 90 minutes)
  - ID Token (1 hours)
  - Refresh Token (1 day / 90 days)
- Primary Refresh Token (14 days)
- JSON Web Token (JWT) - ey...

Access token

Access Token in Entra ID



Identity Provider (IdP)

Request access to Microsoft 365

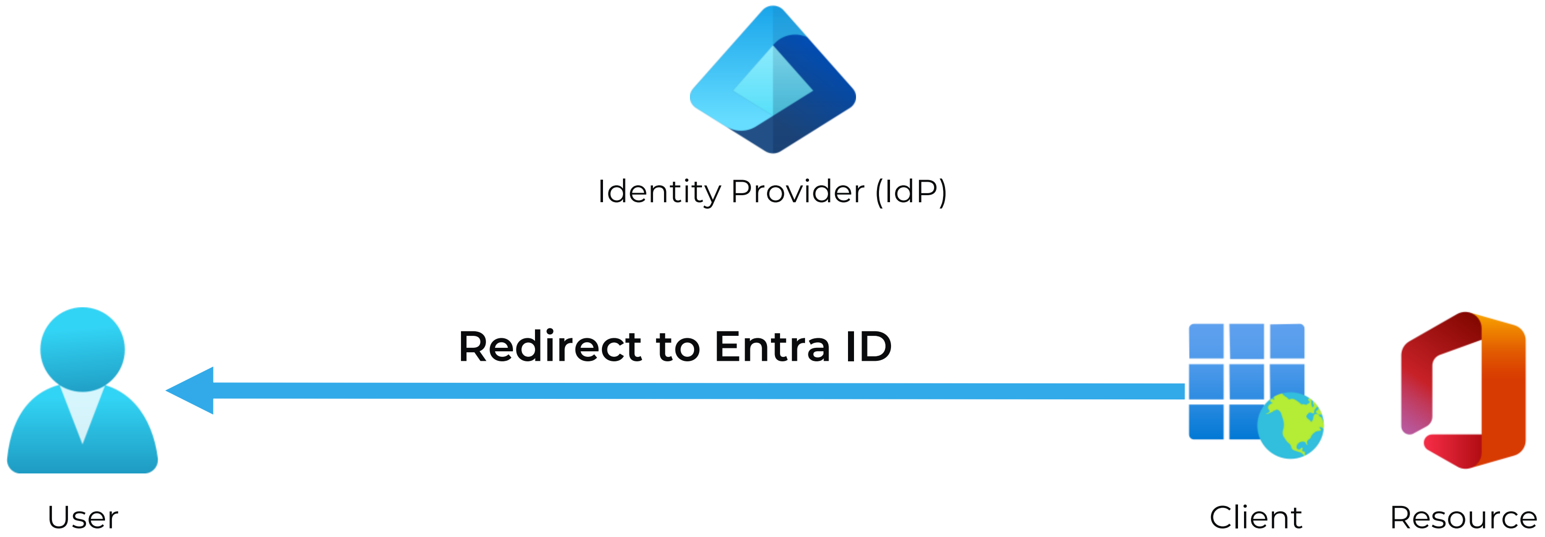
User

Client

Resource

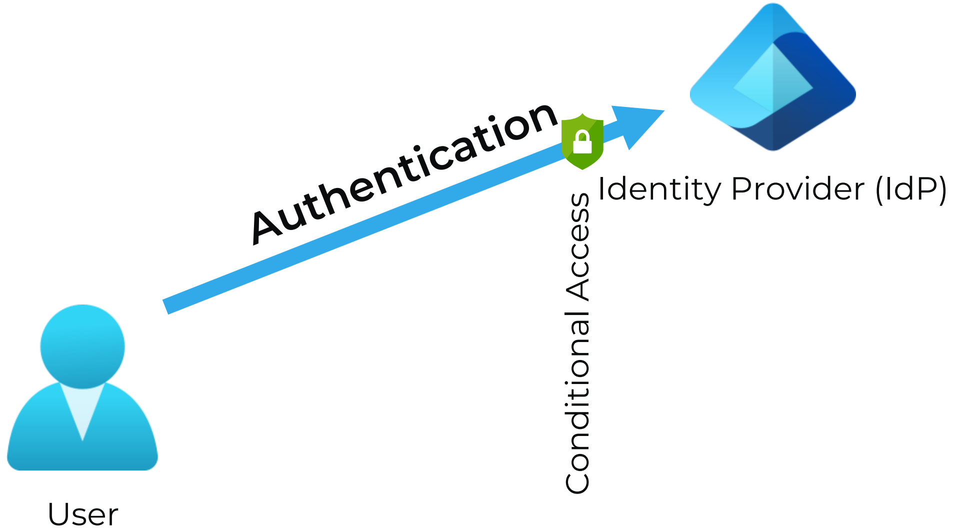
Simplified Version!

Access Token in Entra ID



Simplified Version!

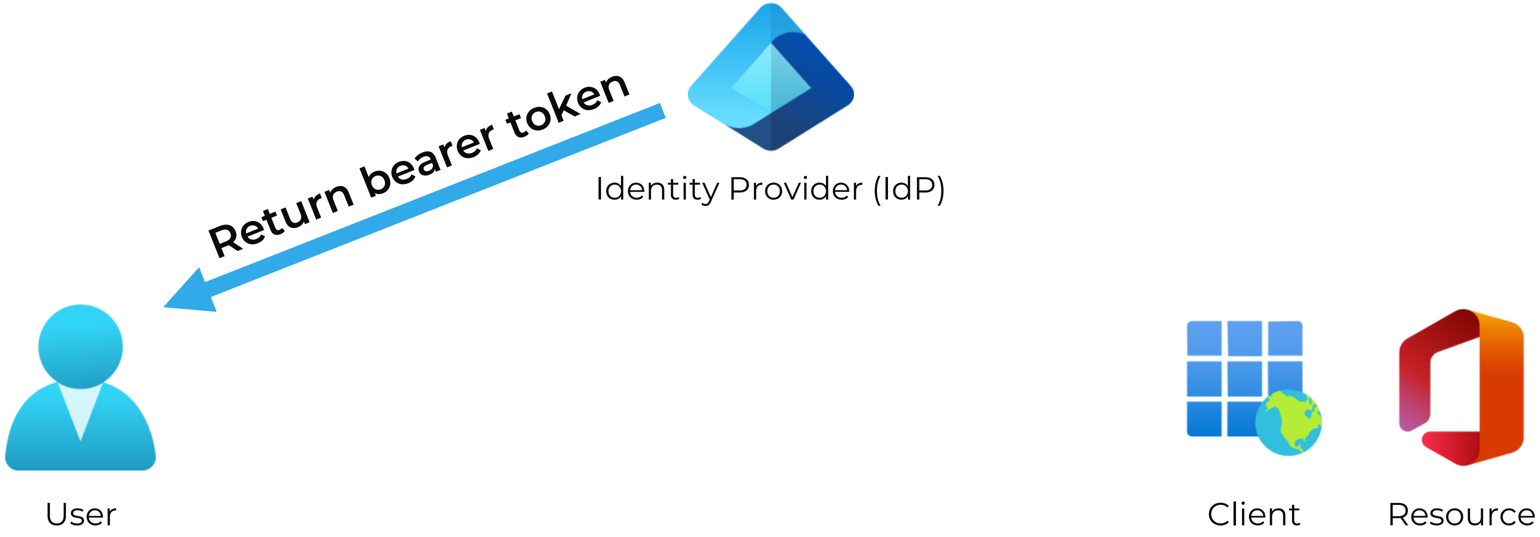
Access Token in Entra ID



Client
Resource

Simplified Version!

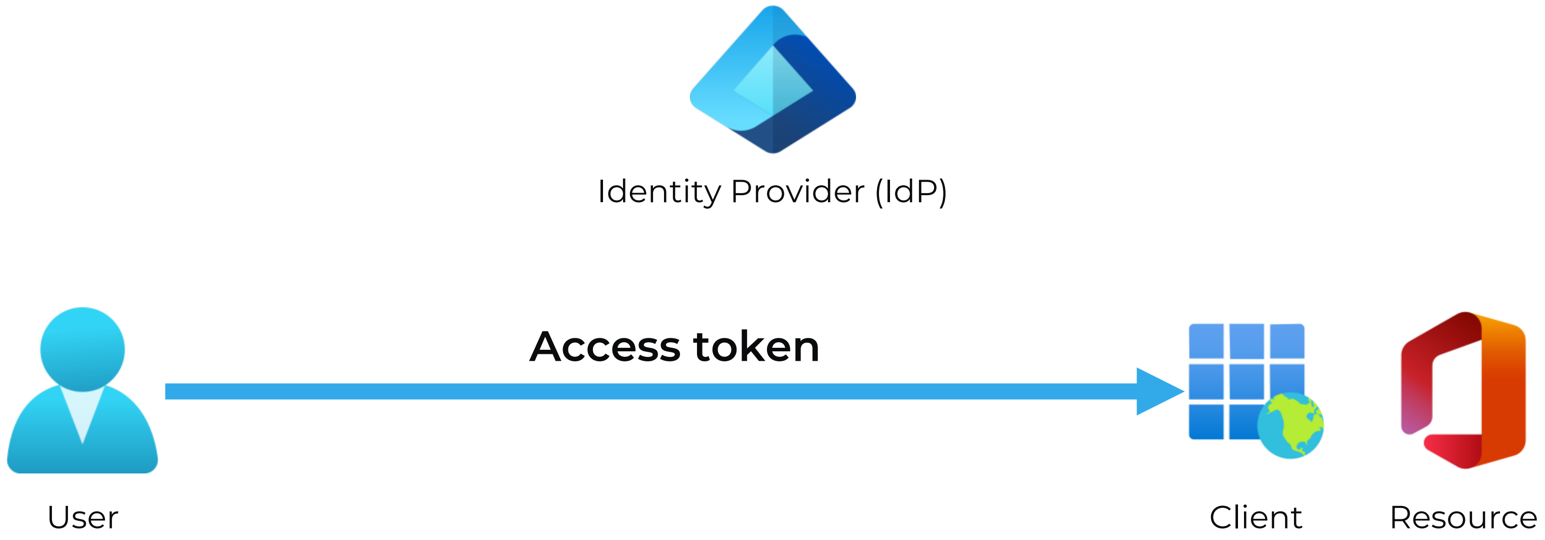
Access Token in Entra ID



Simplified Version!

#WPNinjasNO

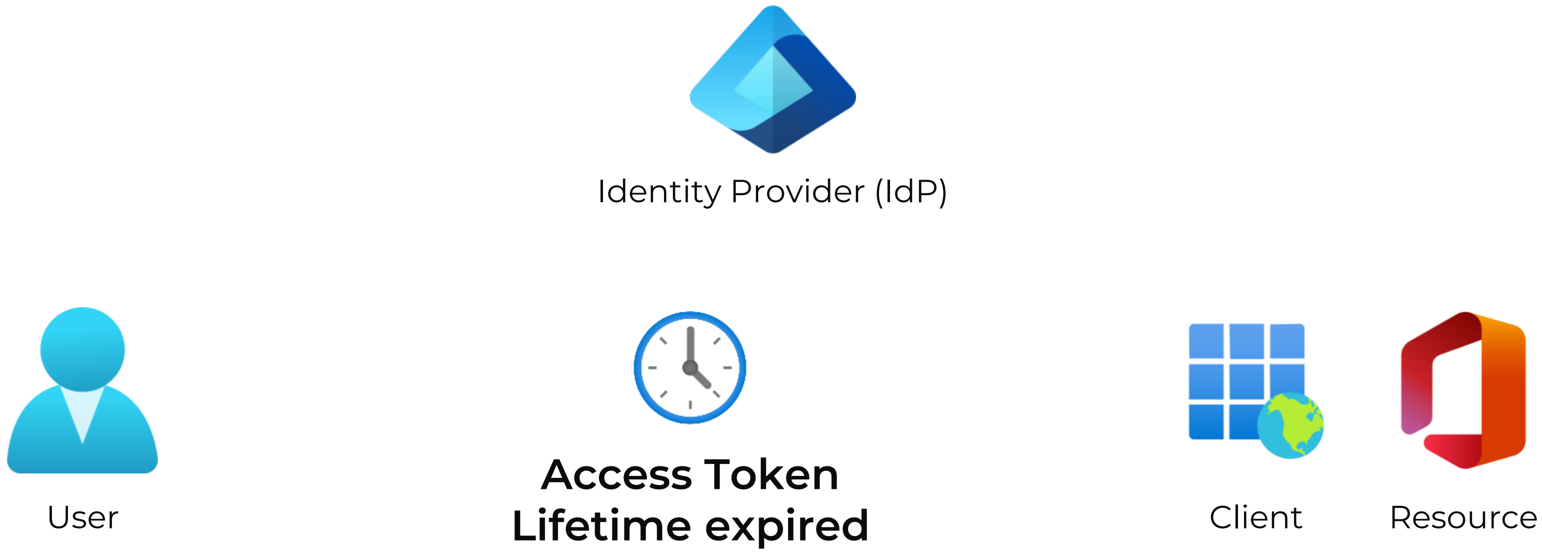
Access Token in Entra ID



Simplified Version!

Refresh token

Refresh Token in Entra ID



Identity Provider (IdP)

User

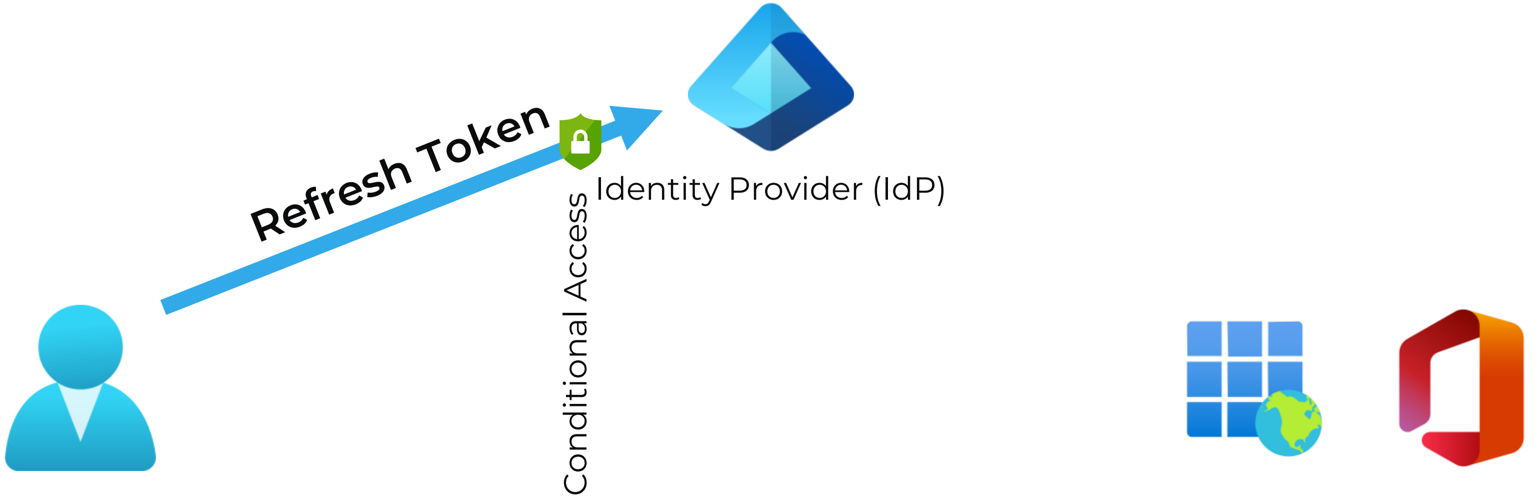
Access Token Lifetime expired

Client

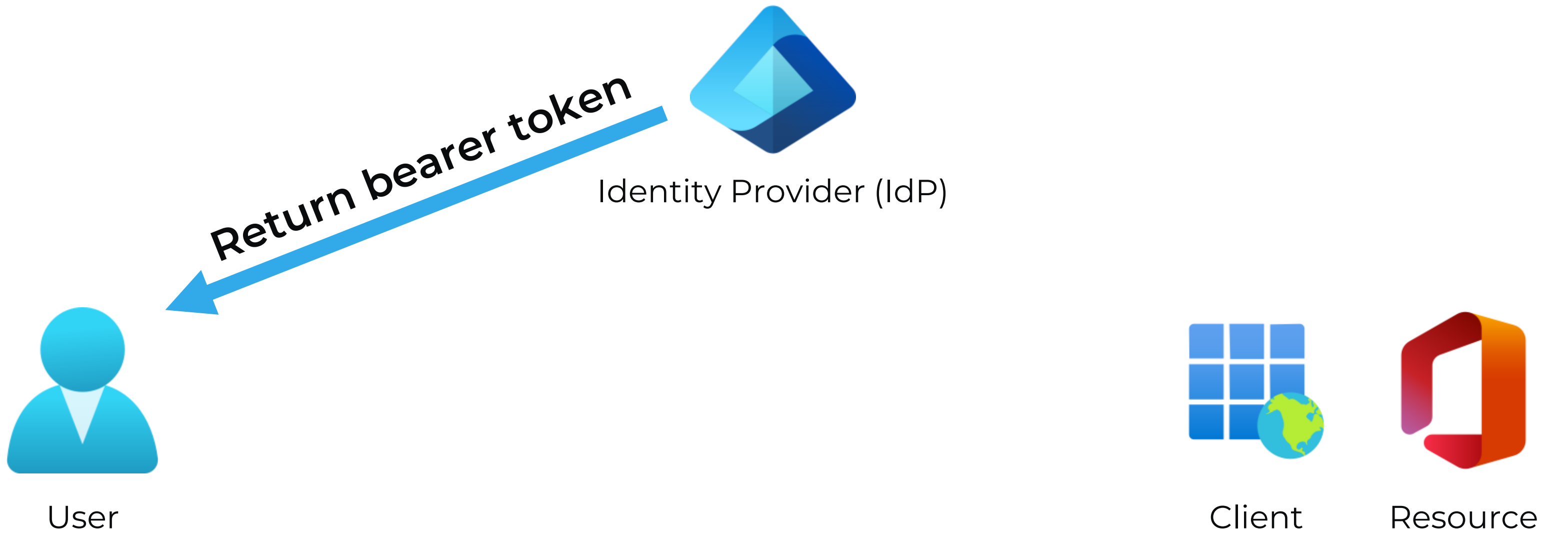
Resource

Simplified Version!

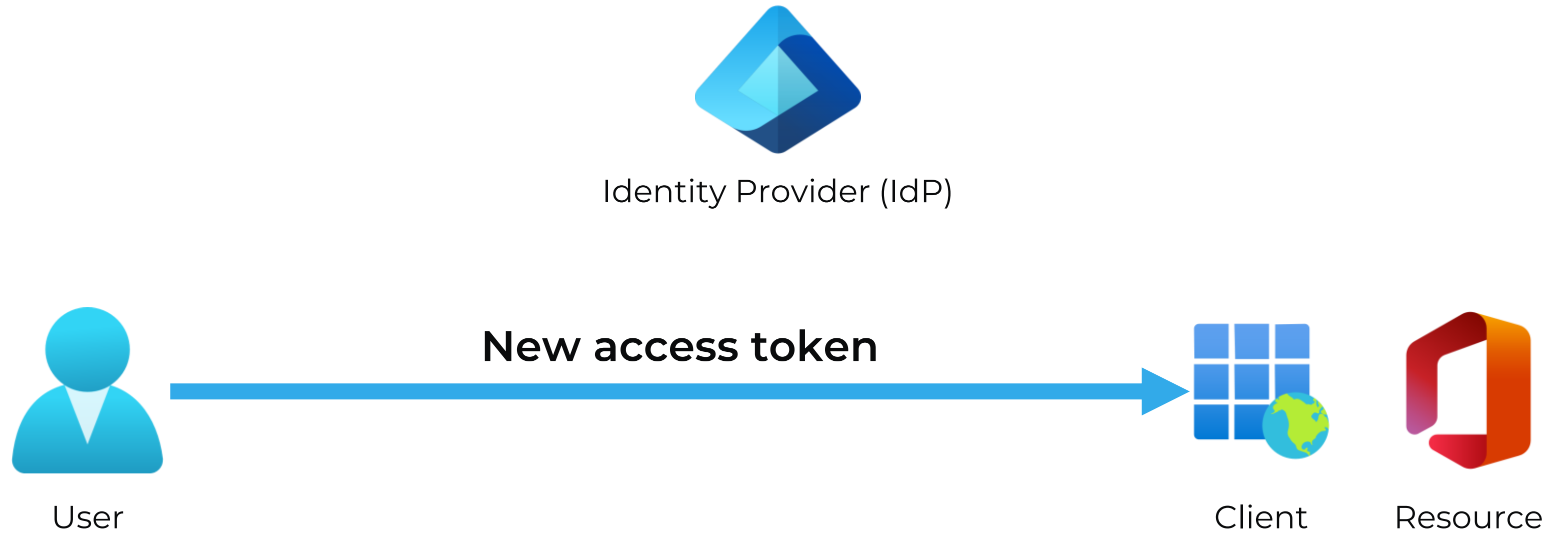
Refresh Token in Entra ID



Refresh Token in Entra ID



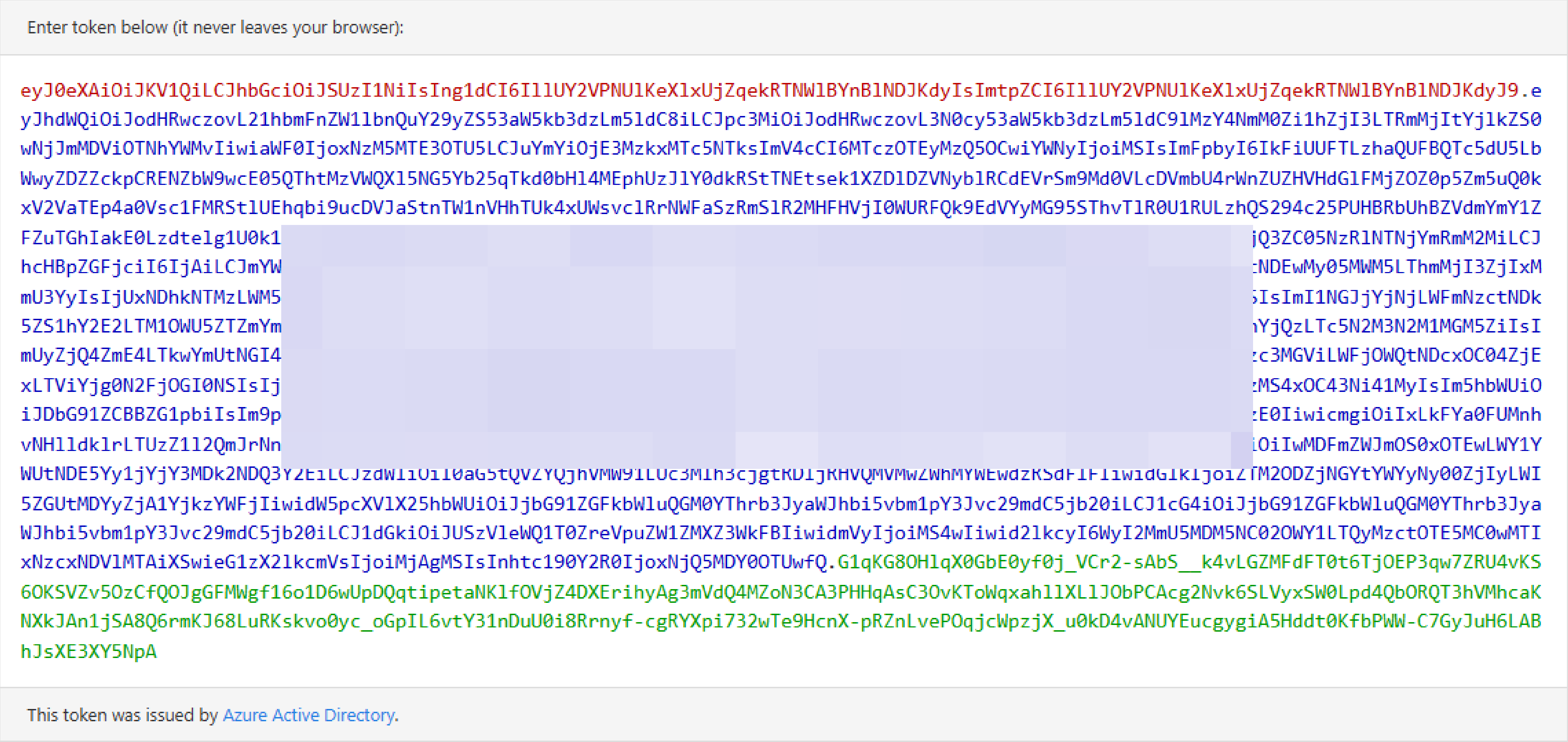
Refresh Token in Entra ID



#WPNinjasNO

JSON Web Token

JSON Web Token Format



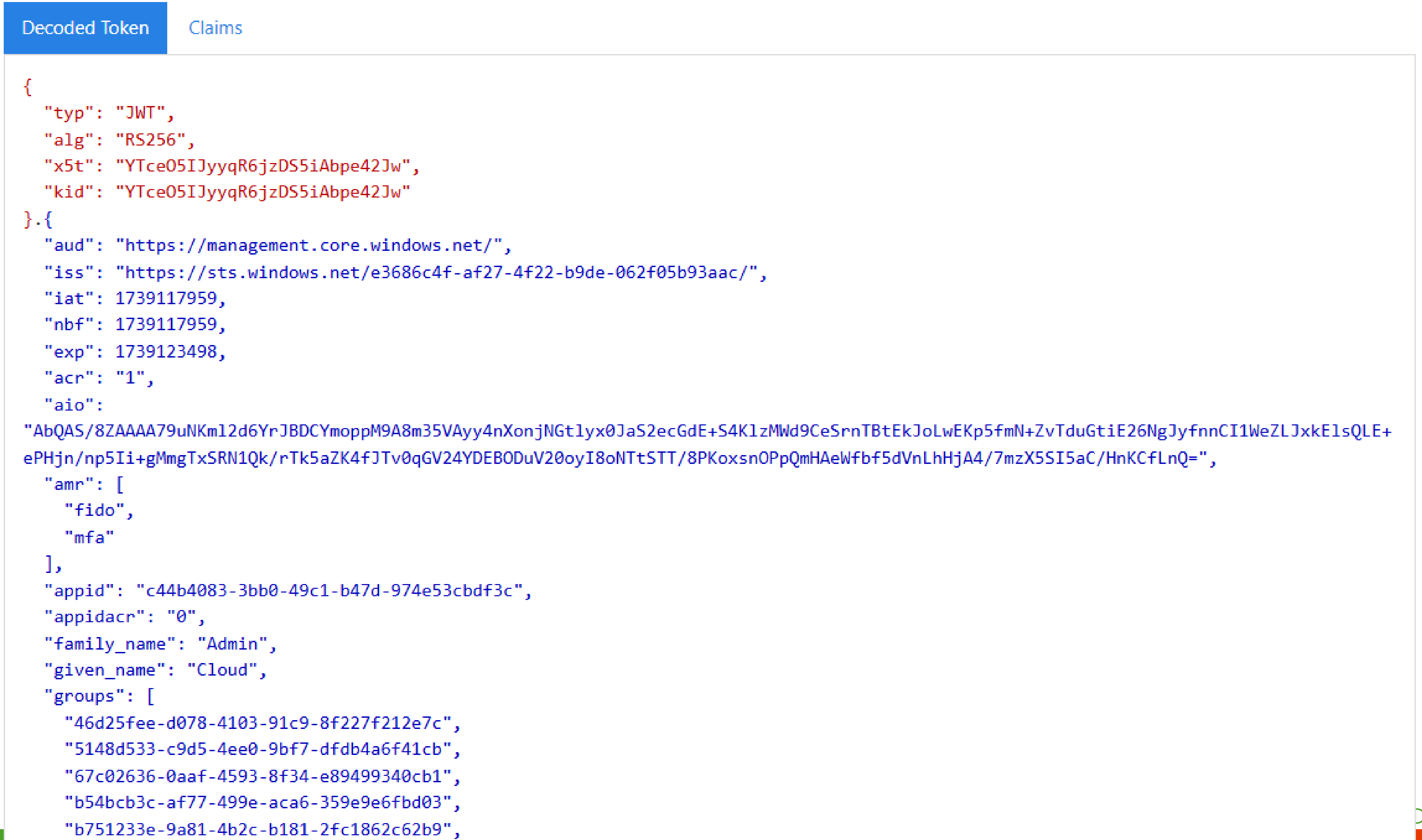
Enter token below (it never leaves your browser):

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IllUY2VPNUlKeXlxUjZqekRTNWlBYnBlNDJKdyIsImtpZCI6IllUY2VPNUlKeXlxUjZqekRTNWlBYnBlNDJKdyJ9.e
yJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuY29yZS53aW5kb3dzLm5ldC8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9lMzY4NmM0Zi1hZjI3LTRmMjItYjlkZS0
wNjJmMDViOTNhYWMvIiwiaWF0IjoxNzM5MTE3OTU5LCJuYmYiOjE3MzkxMTc5NTksImV4cCI6MTczOTEyMzQ5OCwiYWNyIjoiMSIsImFpbyI6IkFiUUFTLzhaQUFBQTc5dU5Lb
WwyZDZZckpCRENZbW9wcE05QThtMzVWQX15NG5Yb25qTkd0bHl4MEphUzJlY0dkRStTNEtsek1XZDlDZVNyblRCdEVrSm9Md0VLcDVmbU4rWnZUZHVHdGlFMjZOZ0p5Zm5uQ0k
xV2VaTEp4a0Vsc1FMRStlUEhqbi9ucDVJaStnTW1nVHhTUk4xUWsvclRrNWFaSzRmSlR2MHFHVjI0WURFQk9EdVYyMG95SThvTlR0U1RULzhQS294c25PUHBRbUhBZVdmYmY1Z
FZuTGhIakE0Lzdtelg1U0k1 [redacted] jQ3ZC05NzR1NTNjYmRmM2MiLCJ
hcHBpZGFjciI6IjAiLCJmYW [redacted] NDEwMy05MWM5LThmMjI3ZjIxM
mU3YyIsIjUxNDhkNTMzLWM5 [redacted] IsImI1NGJjYjNjLWFmNzctNDk
5ZS1hY2E2LTM1OWU5ZTZmYm [redacted] YjQzLTc5N2M3N2M1MGM5ZiIsI
mUyZjQ4ZmE4LTkwYmUtNGI4 [redacted] c3MGViLWFjOWQtNDcxOC04ZjE
xLTViYjg0N2FjOGI0NSIsIj [redacted] MS4xOC43Ni41MyIsIm5hbWUiO
iJDbG91ZCBBZG1pbiIsIm9p [redacted] E0IiwicmgiOiIxLkFYa0FUMnh
vNHlldklrLTUzZ1l2QmJrNn [redacted] OiIwMDFmZWJmOS0xOTEwLWY1Y
WUtNDE5Yy1jYjY3MDk2NDQ3 [redacted] TM2ODZjNGYtYWYyNy00ZjIyLWI
5ZGUtMDYyZjA1YjkzYWFjIiwidW5pcXVlX25hbWUiOiJjbG91ZGFkbWluQGM0YThrb3JyaWJhbi5vbm1pY3Jvc29mdC5jb20iLCJ1cG4iOiJjbG91ZGFkbWluQGM0YThrb3Jya
WJhbi5vbm1pY3Jvc29mdC5jb20iLCJ1dGkiOiJUSzVleWQ1T0ZreVpuZW1ZMXZ3WkFBIiwidmVyIjoiMS4wIiwid2lkcyI6WyI2MmU5MDM5NC02OWY1LTQyMzctOTE5MC0wMTI
xNzcxNDV1MTAiXSwieG1zX2lkcmVsIjoiMjAgMSIsInhtc190Y2R0IjoxNjQ5MDY0OTUwfQ.G1qKG8OHlqX0GbE0yf0j_VCr2-sAbS__k4vLGZMFdFT0t6TjOEP3qw7ZRU4vKS
6OKSVZv5OzCfQOJgGFMWgf16o1D6wUpDQqtipetaNKlfOVjZ4DXErihyAg3mVdQ4MZoN3CA3PHHqAsC3OvKToWqxahllXLlJObPCAcg2Nvk6SLVyxSW0Lpd4QbORQT3hVMhcaK
NXkJAn1jSA8Q6rmKJ68LuRKskvo0yc_oGpIL6vtY31nDuU0i8Rrnyf-cgRYXpi732wTe9HcnX-pRZnLvePOqjcWpzjX_u0kD4vANUYEucgygiA5Hddt0KfbPWW-C7GyJuH6LAB
hJsXE3XY5NpA

This token was issued by Azure Active Directory.

#WPNinjasNO

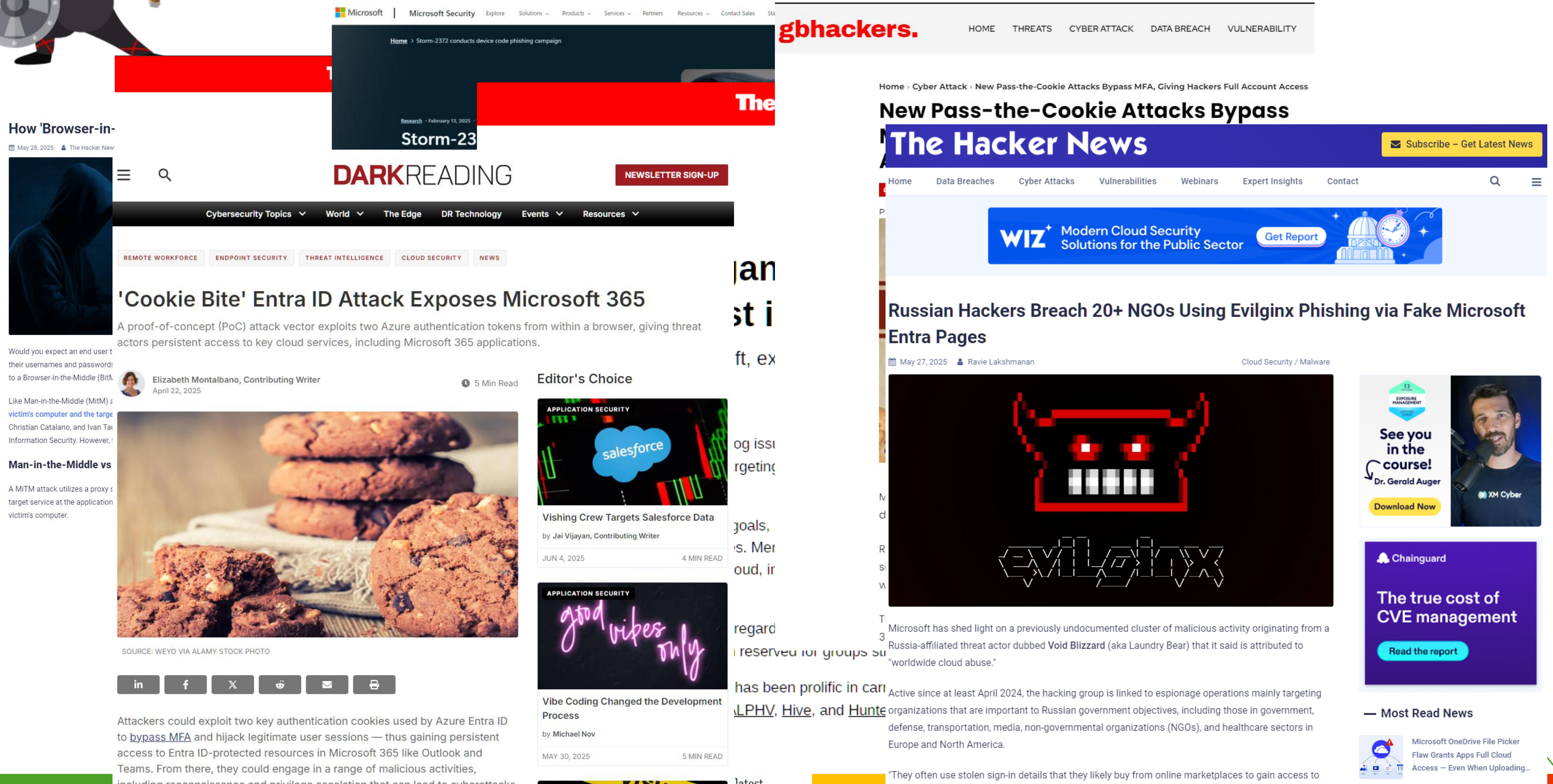
JSON Web Token Format



```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "YTceO5IJyyqR6jzDS5iAbpe42Jw",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "https://management.core.windows.net/",
  "iss": "https://sts.windows.net/e3686c4f-af27-4f22-b9de-062f05b93aac/",
  "iat": 1739117959,
  "nbf": 1739117959,
  "exp": 1739123498,
  "acr": "1",
  "aio":
"AbQAS/8ZAAAA79uNKml2d6YrJBDCYmoppM9A8m35VAyy4nXonjNGtlyx0JaS2ecGdE+S4KlzMWd9CeSrnTBtEkJoLwEKp5fmN+ZvTduGtiE26NgJyfnnCI1WeZLJxkElsQLE+
ePHjn/np5Ii+gMmgTxSRN1Qk/rTk5aZK4fJTv0qGV24YDEBODuV20oyI8oNTtSTT/8PKoxsnOPpQmHAeWfbf5dVnLhHjA4/7mzX5SI5aC/HnKCfLnQ=",
  "amr": [
    "fido",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "appidacr": "0",
  "family_name": "Admin",
  "given_name": "Cloud",
  "groups": [
    "46d25fee-d078-4103-91c9-8f227f212e7c",
    "5148d533-c9d5-4ee0-9bf7-dfdb4a6f41cb",
    "67c02636-0aaf-4593-8f34-e89499340cb1",
    "b54bcb3c-af77-499e-aca6-359e9e6fbd03",
    "b751233e-9a81-4b2c-b181-2fc1862c62b9",
```

Attacks on Token

Attacks on Token



How 'Browser-in-

May 28, 2025 The Hacker New

Would you expect an end user t
their usernames and password
to a Browser-in-the-Middle (BitM

Like Man-in-the-Middle (MitM) a
victim's computer and the targe
Christian Catalano, and Ivan Ta
Information Security. However,

Man-in-the-Middle vs

A MiTM attack utilizes a proxy s
target service at the application
victim's computer.

Microsoft | Microsoft Security Explore Solutions Products Services Partners Resources Contact Sales Sta

Home > Storm-2372 conducts device code phishing campaign

Research · February 13, 2025 ·

Storm-23

REMOTE WORKFORCE ENDPOINT SECURITY THREAT INTELLIGENCE CLOUD SECURITY NEWS

'Cookie Bite' Entra ID Attack Exposes Microsoft 365

A proof-of-concept (PoC) attack vector exploits two Azure authentication tokens from within a browser, giving threat actors persistent access to key cloud services, including Microsoft 365 applications.

Elizabeth Montalbano, Contributing Writer
April 22, 2025

5 Min Read

SOURCE: WEYO VIA ALAMY STOCK PHOTO

Attackers could exploit two key authentication cookies used by Azure Entra ID to bypass MFA and hijack legitimate user sessions — thus gaining persistent access to Entra ID-protected resources in Microsoft 365 like Outlook and Teams. From there, they could engage in a range of malicious activities, including reconnaissance and privilege escalation that can lead to cyberattacks

Editor's Choice

APPLICATION SECURITY
Vishing Crew Targets Salesforce Data
by Jai Vijayan, Contributing Writer
JUN 4, 2025 4 MIN READ

APPLICATION SECURITY
Vibe Coding Changed the Development Process
by Michael Nov
MAY 30, 2025 5 MIN READ

jan
st i
ft, ex

og issu
rgeting

goals,
s. Mer
oud, ir

regard
reserved for groups su

has been prolific in carr
LPHV, Hive, and Hunte

latest

Home › Cyber Attack › New Pass-the-Cookie Attacks Bypass MFA, Giving Hackers Full Account Access

New Pass-the-Cookie Attacks Bypass

The Hacker News
Subscribe – Get Latest News
Home Data Breaches Cyber Attacks Vulnerabilities Webinars Expert Insights Contact

Russian Hackers Breach 20+ NGOs Using Evilginx Phishing via Fake Microsoft Entra Pages

May 27, 2025 Ravie Lakshmanan Cloud Security / Malware

Microsoft has shed light on a previously undocumented cluster of malicious activity originating from a Russia-affiliated threat actor dubbed Void Blizzard (aka Laundry Bear) that it said is attributed to "worldwide cloud abuse."

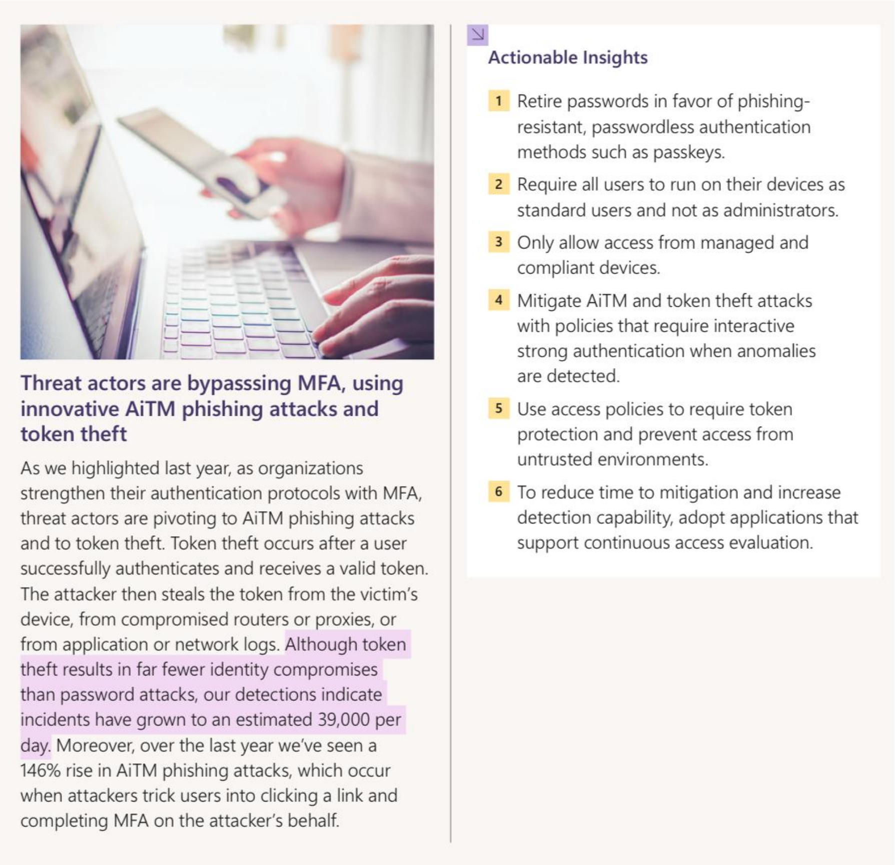
Active since at least April 2024, the hacking group is linked to espionage operations mainly targeting organizations that are important to Russian government objectives, including those in government, defense, transportation, media, non-governmental organizations (NGOs), and healthcare sectors in Europe and North America.

"They often use stolen sign-in details that they likely buy from online marketplaces to gain access to

— Most Read News

Microsoft OneDrive File Picker Flaw Grants Apps Full Cloud Access — Even When Uploading...

Attacks on Token

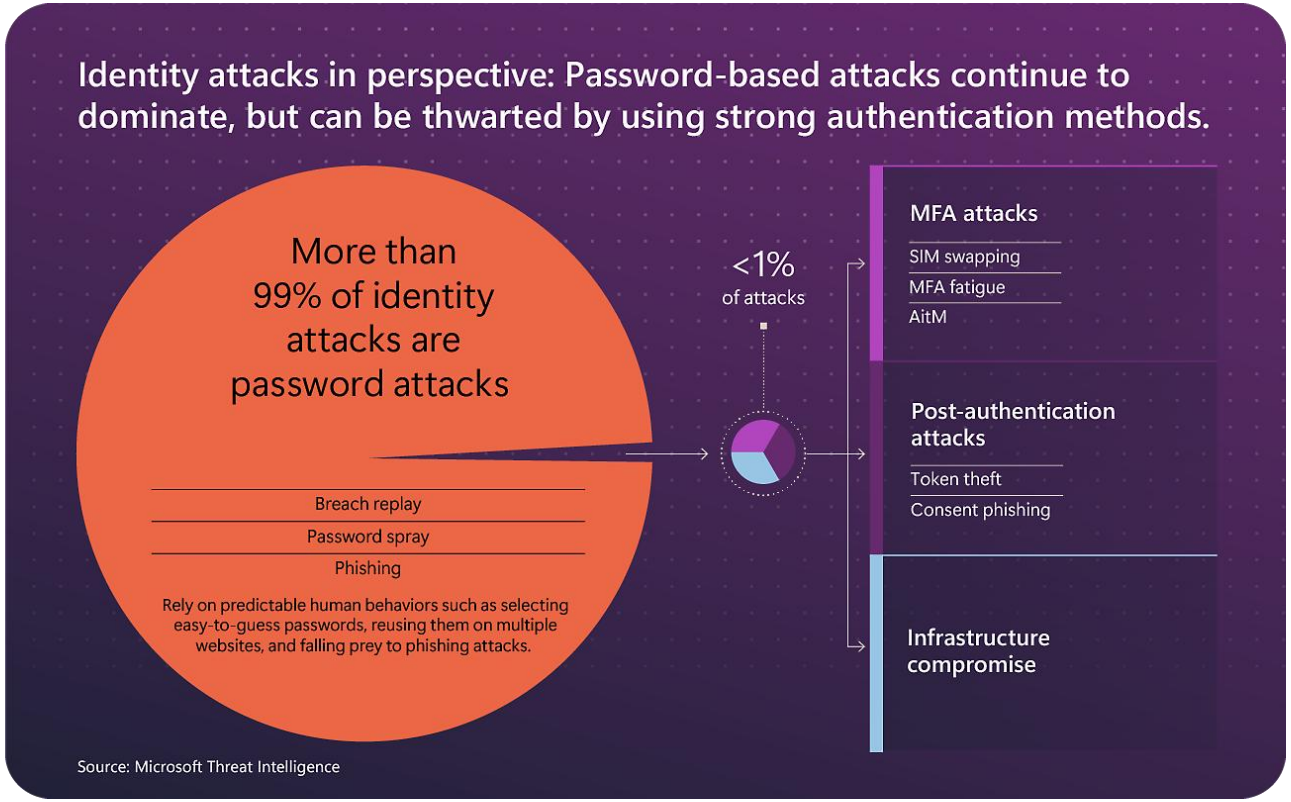


Threat actors are bypasssing MFA, using innovative AiTM phishing attacks and token theft

As we highlighted last year, as organizations strengthen their authentication protocols with MFA, threat actors are pivoting to AiTM phishing attacks and to token theft. Token theft occurs after a user successfully authenticates and receives a valid token. The attacker then steals the token from the victim's device, from compromised routers or proxies, or from application or network logs. Although token theft results in far fewer identity compromises than password attacks, our detections indicate incidents have grown to an estimated 39,000 per day. Moreover, over the last year we've seen a 146% rise in AiTM phishing attacks, which occur when attackers trick users into clicking a link and completing MFA on the attacker's behalf.

Actionable Insights

1. Retire passwords in favor of phishing-resistant, passwordless authentication methods such as passkeys.
2. Require all users to run on their devices as standard users and not as administrators.
3. Only allow access from managed and compliant devices.
4. Mitigate AiTM and token theft attacks with policies that require interactive strong authentication when anomalies are detected.
5. Use access policies to require token protection and prevent access from untrusted environments.
6. To reduce time to mitigation and increase detection capability, adopt applications that support continuous access evaluation.



Identity attacks in perspective: Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks
Breach replay
Password spray
Phishing
Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.
<1% of attacks
MFA attacks
SIM swapping
MFA fatigue
AitM
Post-authentication attacks
Token theft
Consent phishing
Infrastructure compromise

Source: Microsoft Threat Intelligence

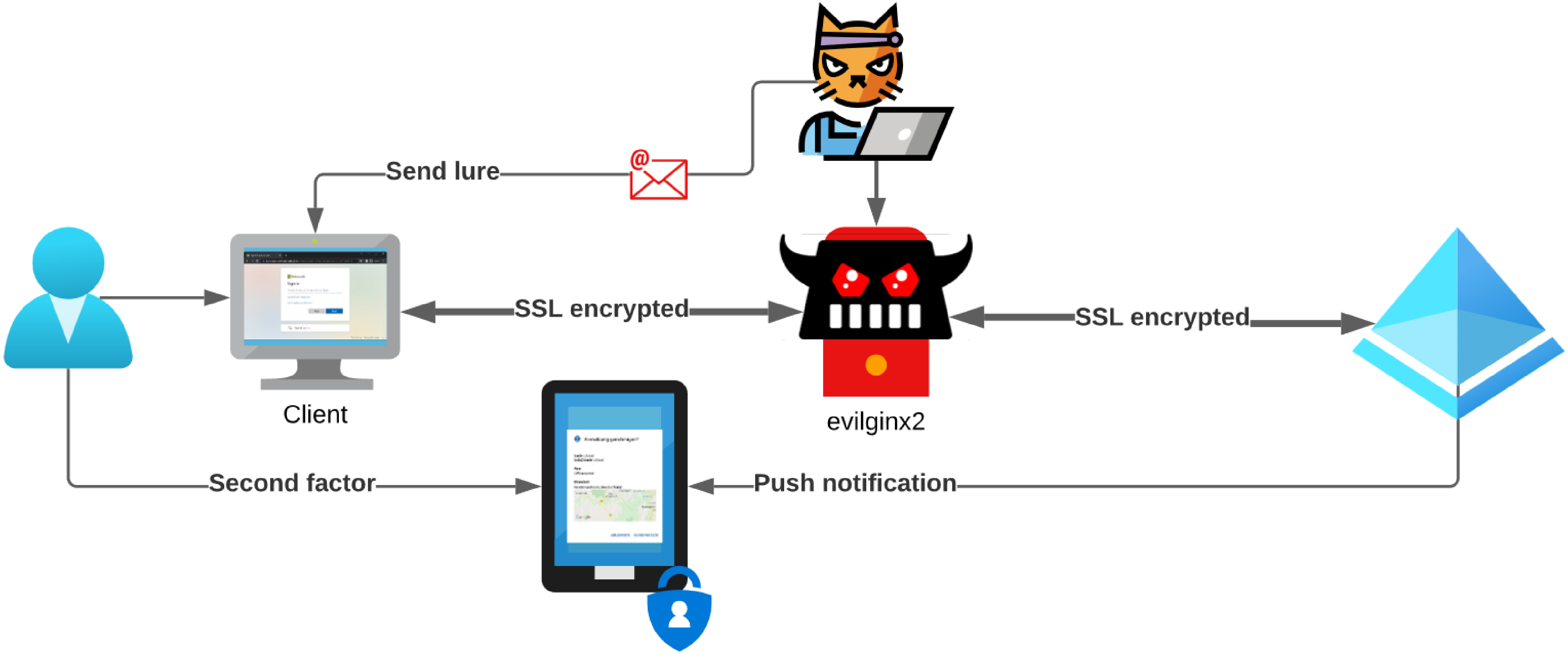
http://aka.ms/mddr2024

Bearer Token theft

- Steal Web Session Cookie (T1539) aka
  - Adversay in the Middle (e.g. Evilginx2)
  - Pass-the-cookie attack (e.g. CookieMiner)

- Steal Application Access Token (T1528)
  - Device Code Phishing (e.g. TokenTactics)

Adversay in the Middle (T1557)



Demo

Cookie Theft (ESTSAUTH)

Primary Refresh Token Theft

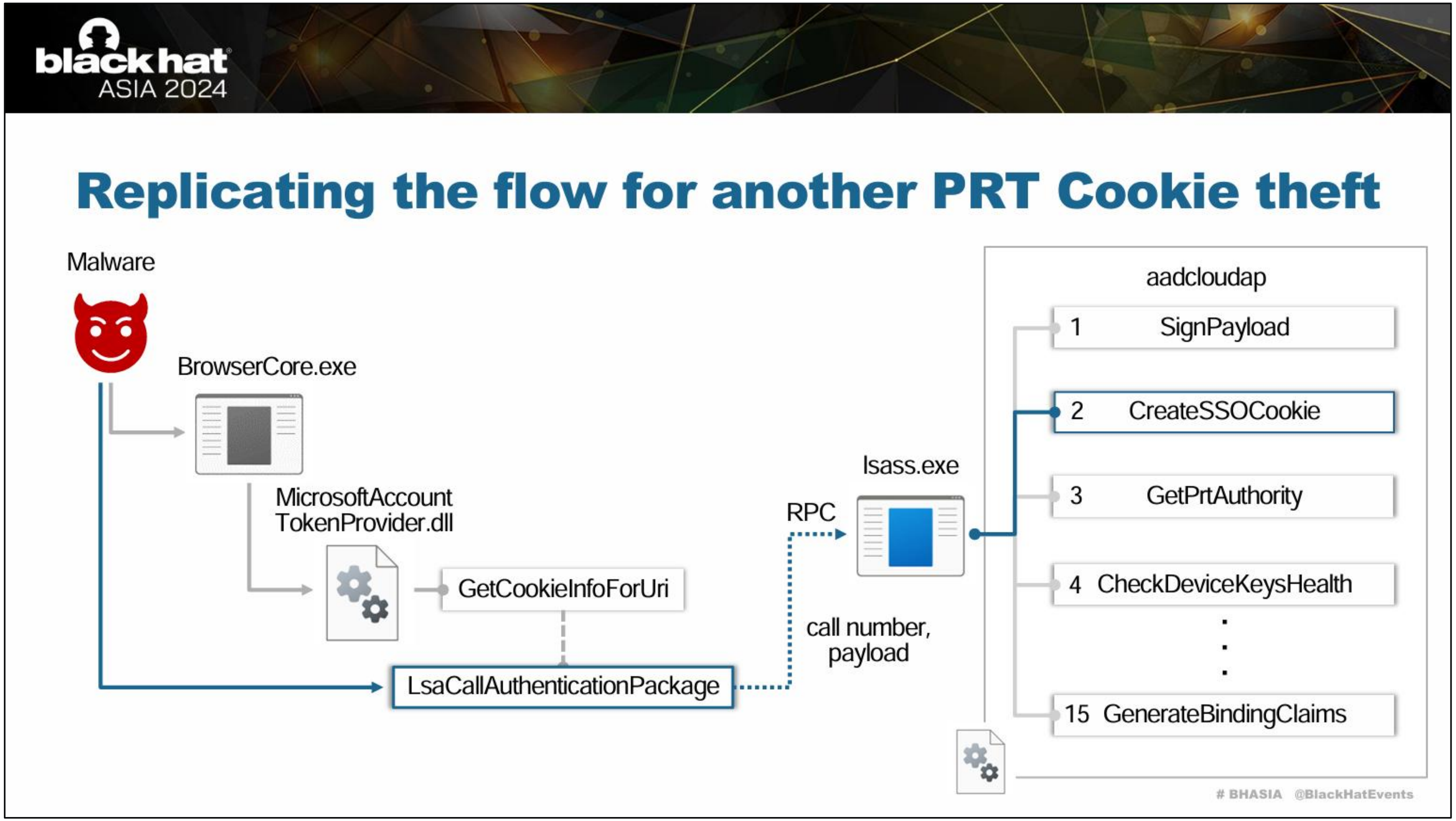
- Attacker has already compromised the endpoint
- Extract PRT certificate

- Generate `x-ms-RefreshTokenCredential`
  - Used for Browser SSO
  - Contains the compliance state of the device
  - No elevated permissions required

Demo

Browser SSO Attack BAADTokenBroker

BAADTokenBroker



black hat ASIA 2024

Replicating the flow for another PRT Cookie theft

Malware

BrowserCore.exe

MicrosoftAccount TokenProvider.dll

GetCookieInfoForUri

LsaCallAuthenticationPackage

RPC

call number, payload

lsass.exe

aadcloudap

1 SignPayload

2 CreateSSOCookie

3 GetPrtAuthority

4 CheckDeviceKeysHealth

.
.
.

15 GenerateBindingClaims

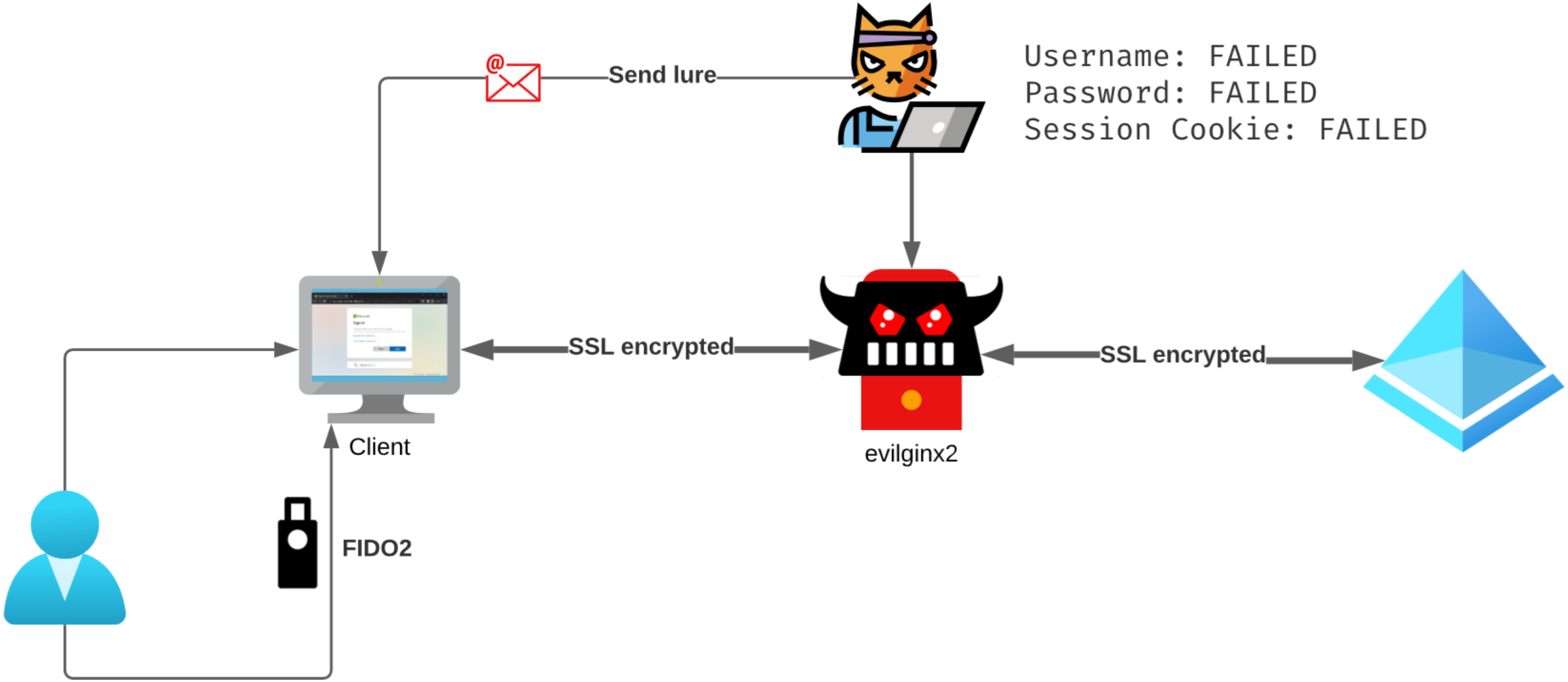
BHASIA @BlackHatEvents

Protections

Protections

- Device Compliance or Hybrid Joined Devices
- Always use TPM 2.0 to store the PRT
- Use Phishing Resistant Authentication methods
  - Passkey / FIDO2
  - Smartcards
  - Windows Hello for Business
- Enforce Authentication Strength to prevent downgrade attacks

Attacker in The Middle

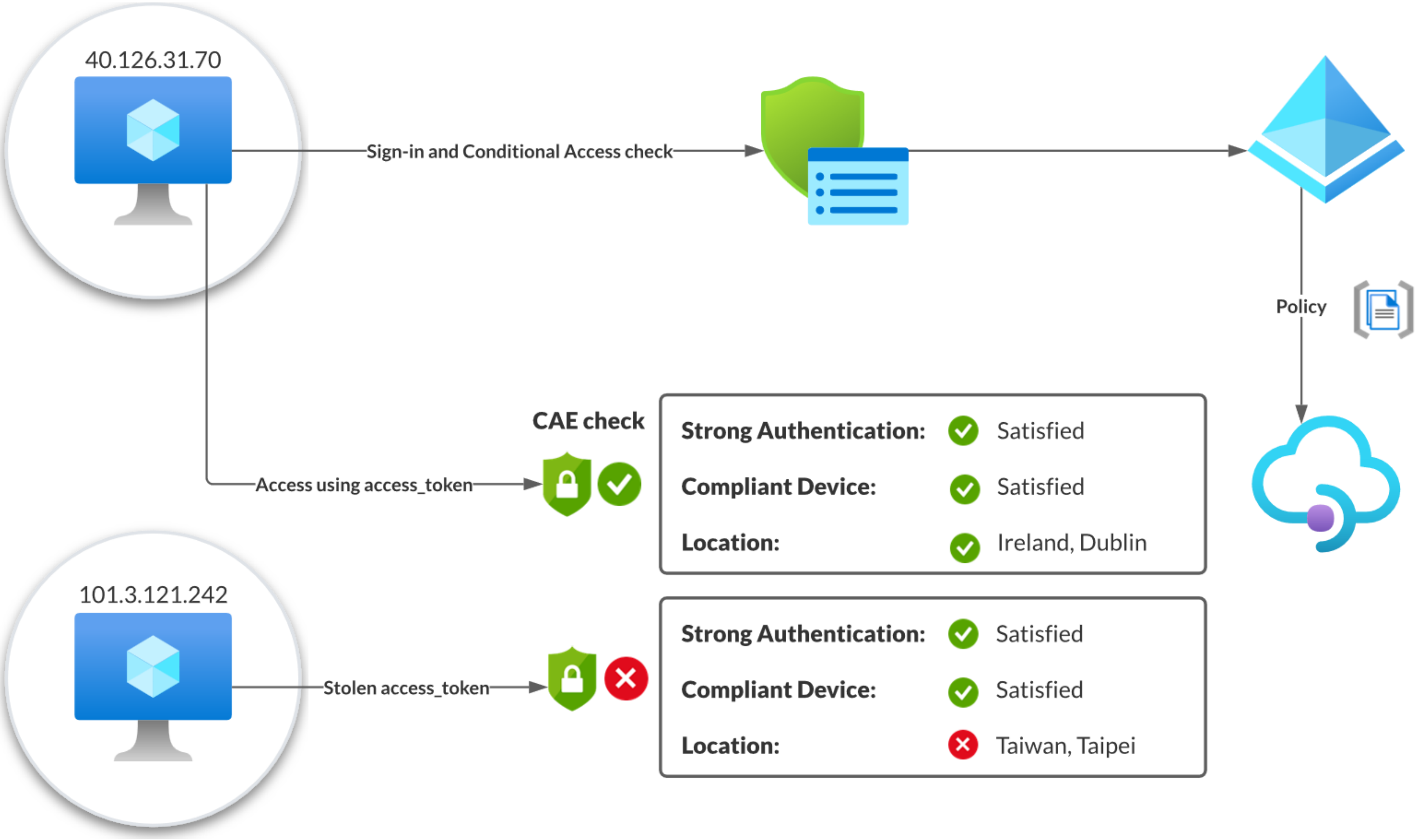


```
Username: FAILED
Password: FAILED
Session Cookie: FAILED
```

Protections

- Block Device Code Flow where not needed
- Do not disable Continuous Access Evaluation

Continuous Access Evaluation



40.126.31.70
Sign-in and Conditional Access check
Policy
CAE check
Access using access_token
101.3.121.242
Stolen access_token

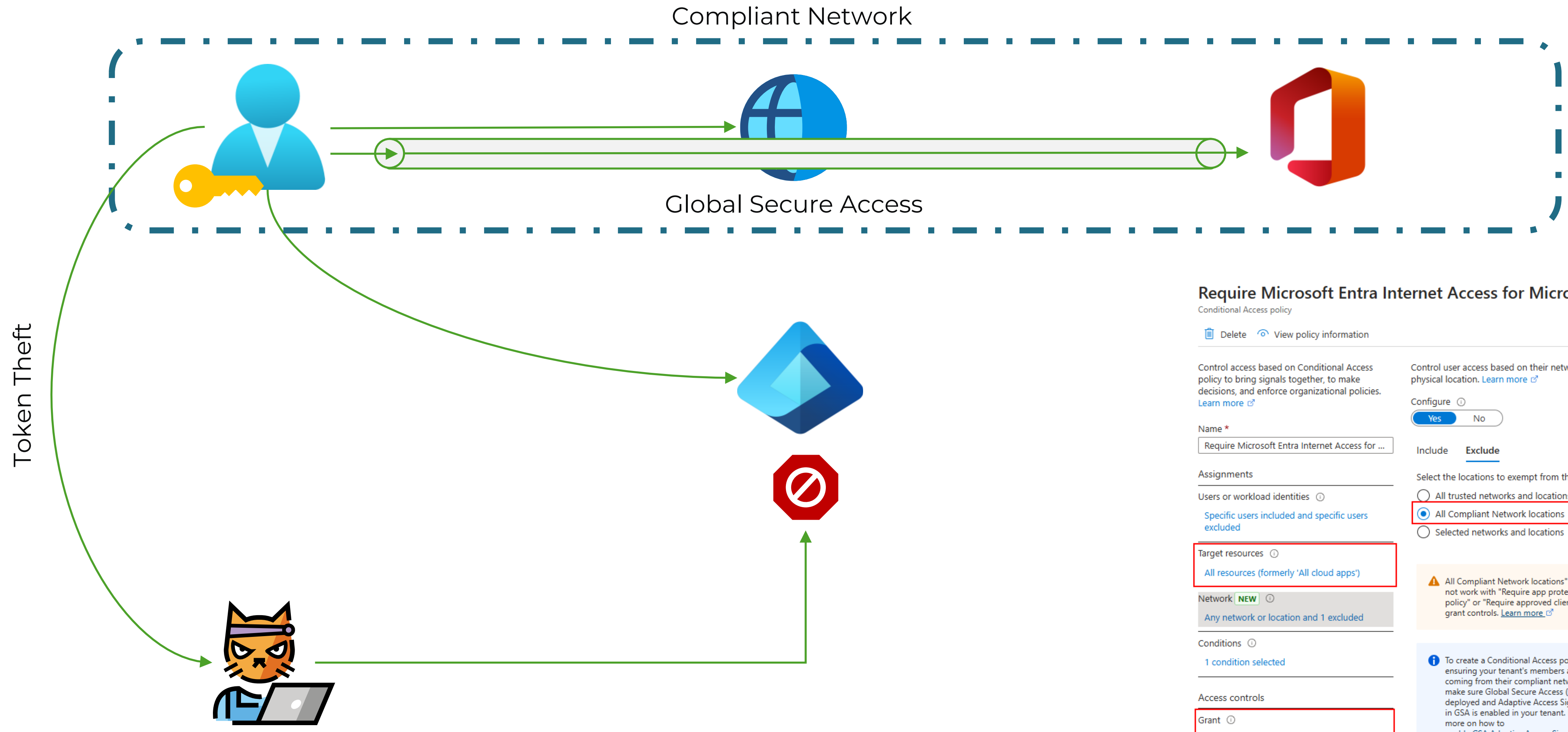
Strong Authentication:	✓	Satisfied
Compliant Device:	✓	Satisfied
Location:	✓	Ireland, Dublin

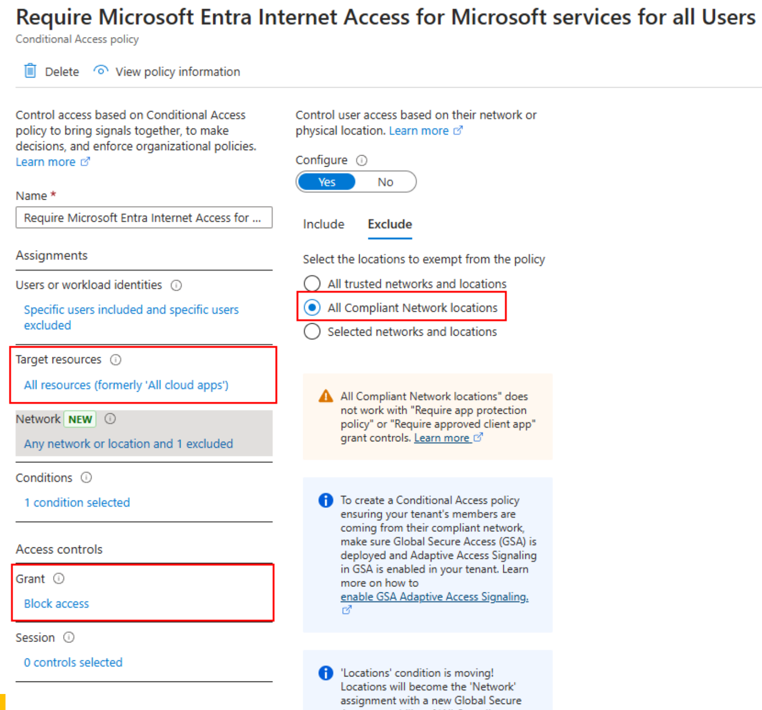
Strong Authentication:	✓	Satisfied
Compliant Device:	✓	Satisfied
Location:	✗	Taiwan, Taipei

Global Secure Access

- Use Microsoft Global Secure Access
  - "Microsoft Entra Internet Access for Microsoft services" is included in Microsoft Entra ID P1 license
- Strict Enforcement mode
  - Only possible if the initial sign-in comes from a known IP address range
  - Only supported for Microsoft resources

Global Secure Access




Require Microsoft Entra Internet Access for Microsoft services for all Users

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Require Microsoft Entra Internet Access for ...

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Any network or location and 1 excluded

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Control user access based on their network or physical location. Learn more

Configure ⓘ

[✓ Yes] No

Include | **Exclude**

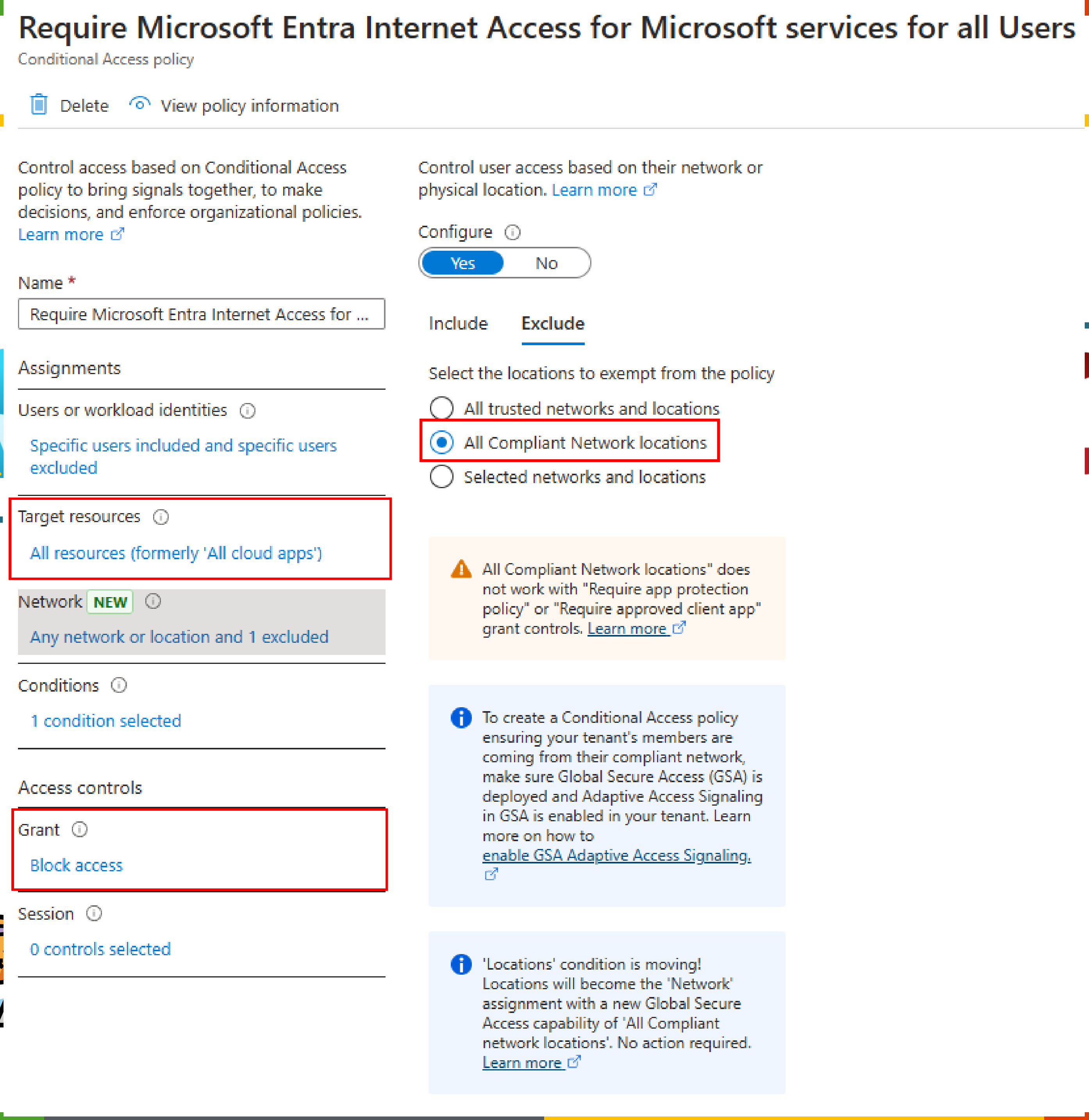
Select the locations to exempt from the policy

○ All trusted networks and locations
● All Compliant Network locations
○ Selected networks and locations

All Compliant Network locations" does not work with "Require app protection policy" or "Require approved client app" grant controls. Learn more

To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to enable GSA Adaptive Access Signaling.

'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure



Require Microsoft Entra Internet Access for Microsoft services for all Users

Conditional Access policy

Delete   View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Require Microsoft Entra Internet Access for ...

Assignments

Users or workload identities

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network NEW

Any network or location and 1 excluded

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Control user access based on their network or physical location. Learn more

Configure

[✓ Yes] No

Include   Exclude

Select the locations to exempt from the policy

○ All trusted networks and locations

● All Compliant Network locations

○ Selected networks and locations

All Compliant Network locations" does not work with "Require app protection policy" or "Require approved client app" grant controls. Learn more

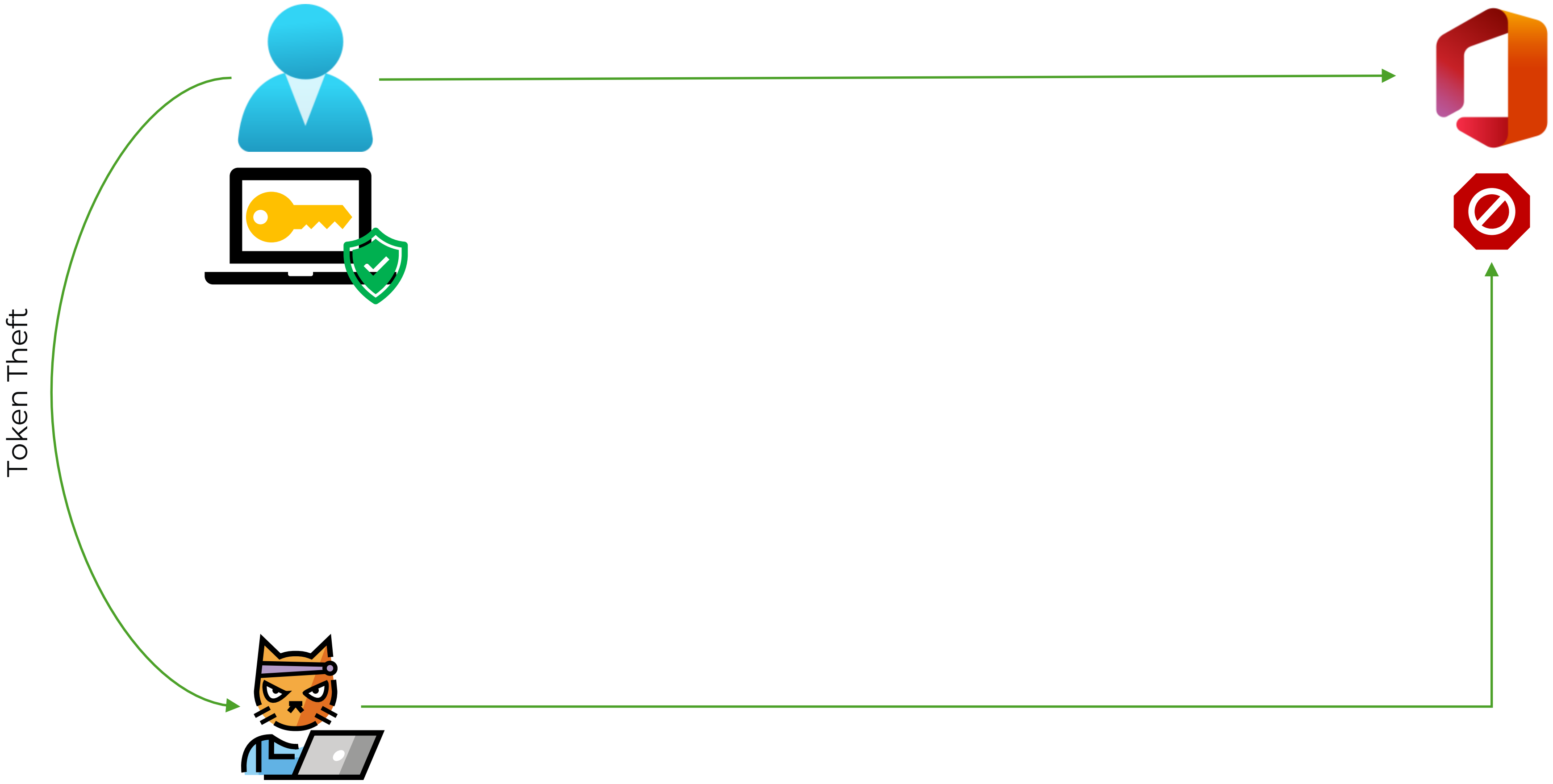
To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to enable GSA Adaptive Access Signaling.

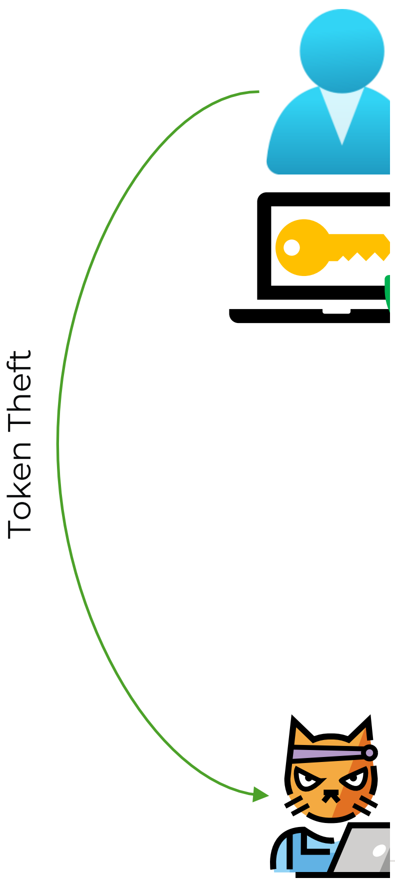
'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure Access capability of 'All Compliant network locations'. No action required. Learn more

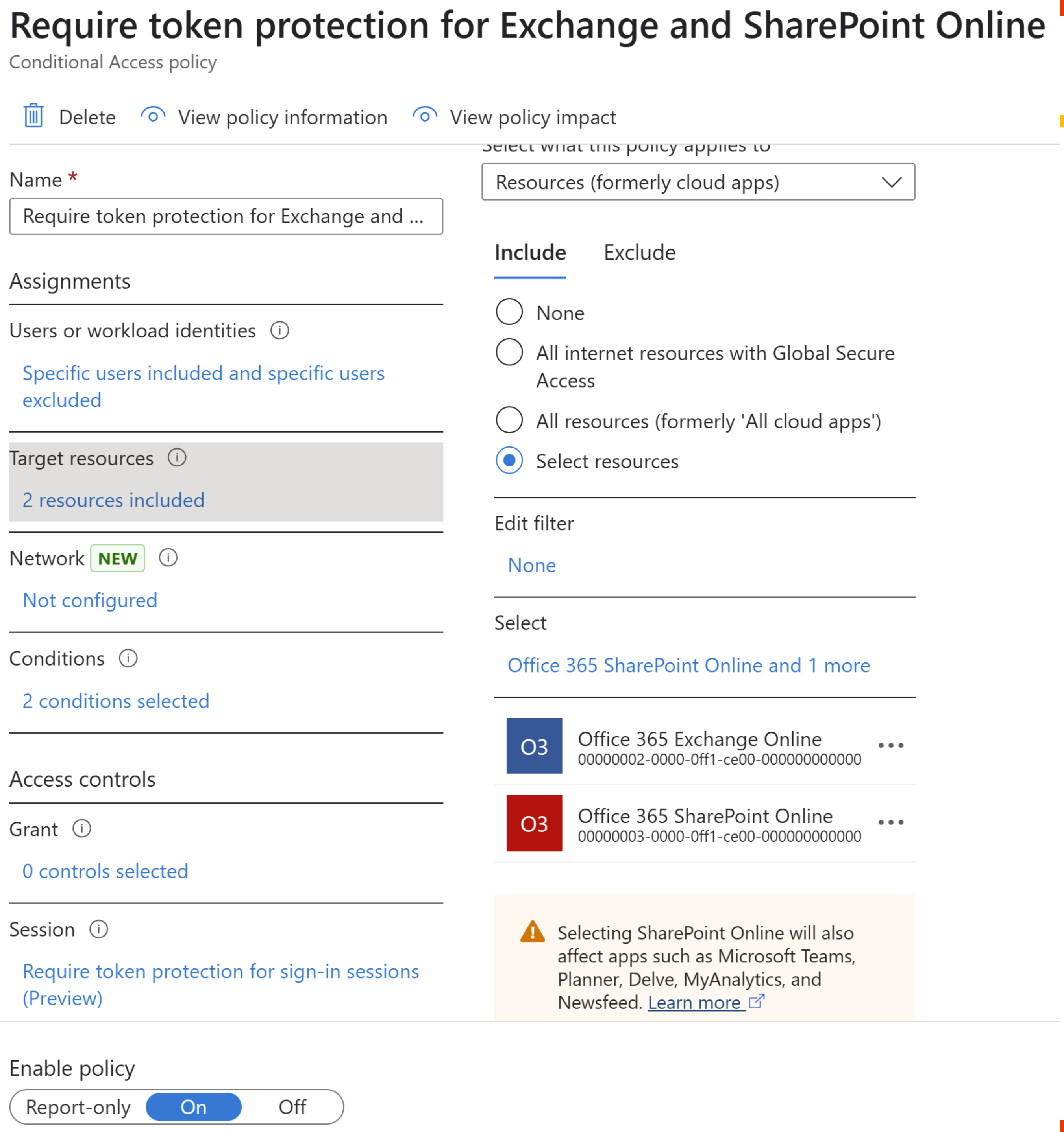
Token Protection

- Token Protection
  - Currently only supported for limited workloads on Windows devices
    - Exchange
    - SharePoint Online
    - Windows 365
    - Azure Virtual Desktop
  - Microsoft Entra ID P2 license required

Token Protection







Require token protection for Exchange and SharePoint Online

Conditional Access policy

Delete | View policy information | View policy impact

Name *

Require token protection for Exchange and ...

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

2 resources included

Network NEW ⓘ

Not configured

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

Require token protection for sign-in sessions (Preview)

Enable policy

Report-only [✓ On] Off

Select what this policy applies to

Resources (formerly cloud apps)

Include Exclude

○ None

○ All internet resources with Global Secure Access

○ All resources (formerly 'All cloud apps')

● Select resources

Edit filter

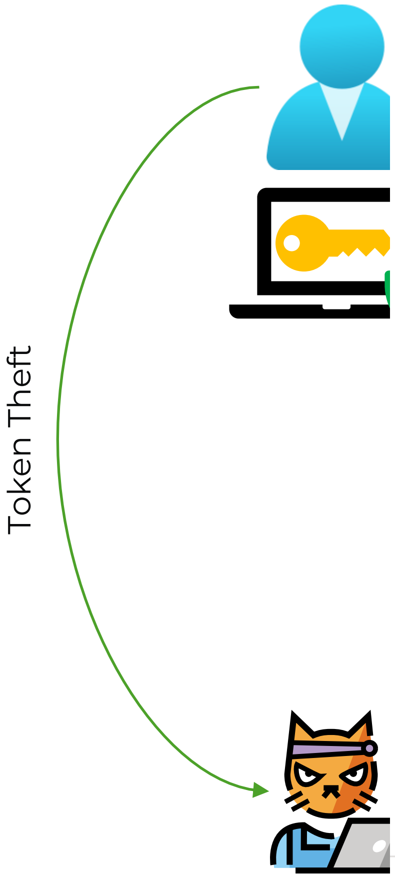
None

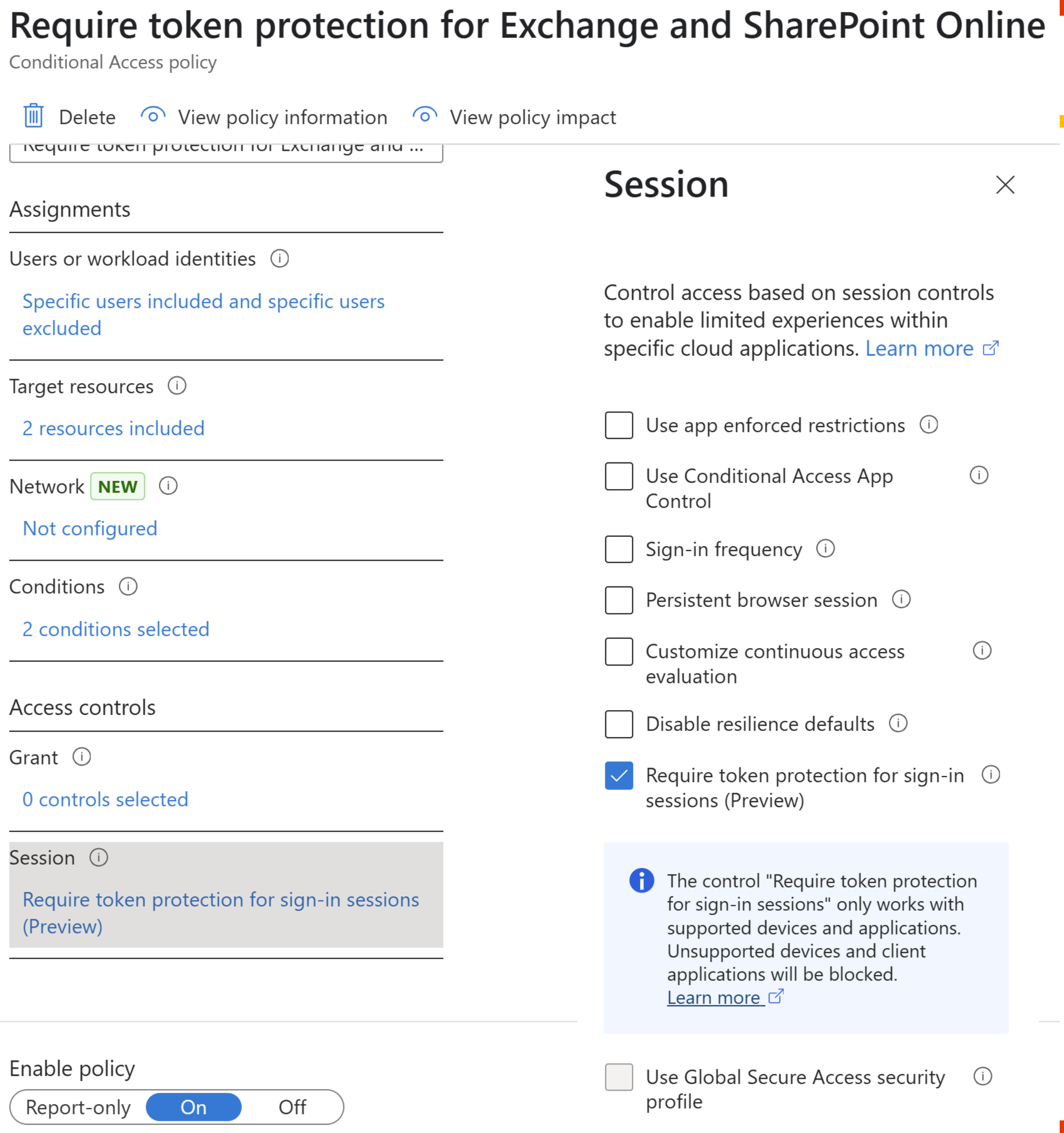
Select

Office 365 SharePoint Online and 1 more

O3	Office 365 Exchange Online 00000002-0000-0ff1-ce00-000000000000	...
O3	Office 365 SharePoint Online 00000003-0000-0ff1-ce00-000000000000	...

⚠ Selecting SharePoint Online will also affect apps such as Microsoft Teams, Planner, Delve, MyAnalytics, and Newsfeed. Learn more





Require token protection for Exchange and SharePoint Online

Conditional Access policy

Require token protection for Exchange and ...

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

2 resources included

Network NEW ⓘ

Not configured

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

Require token protection for sign-in sessions (Preview)

Enable policy

Report-only [✓ On] Off

Session

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

- □ Use app enforced restrictions ⓘ
- □ Use Conditional Access App Control ⓘ
- □ Sign-in frequency ⓘ
- □ Persistent browser session ⓘ
- □ Customize continuous access evaluation ⓘ
- □ Disable resilience defaults ⓘ
- ☑ Require token protection for sign-in sessions (Preview) ⓘ

The control "Require token protection for sign-in sessions" only works with supported devices and applications. Unsupported devices and client applications will be blocked.
Learn more

- □ Use Global Secure Access security profile ⓘ

#WPNinjasNO

Detection & Response

Protections

- Block Device Code Flow where not needed
- Do not disable Continuous Access Evaluation
- Use Microsoft Global Secure Access
  - "Microsoft Entra Internet Access for Microsoft services" is included in Microsoft Entra ID P1 license
- Token Protection
  - Currently only supported for limited workloads on Windows devices
    - Exchange
    - SharePoint Online
    - Windows 365
    - Azure Virtual Desktop
  - Microsoft Entra ID P2 license required

Detection

- Entra ID Protection
- Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Custom Detections
  - Unusual Location change
  - Unusual actions after sign-in
  - Unusual login behavior

https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

BAADTokenBroker

```
UnifiedSignInLogs
| where TimeGenerated > ago(90d)
| where AppDisplayName == "Microsoft Authentication Broker"
| where AppId == "29d9ed98-a469-4536-ade2-f981bc1d605e"
| summarize TokenAcquisitionCreatedDateTime =min(CreatedDateTime) by SessionId,
TokenAcquisitionIPAddress = IPAddress, UserId
| join (UnifiedSignInLogs
    | where AppDisplayName != "Microsoft Authentication Broker"
    | where AppId != "29d9ed98-a469-4536-ade2-f981bc1d605e"
    | summarize arg_min(CreatedDateTime, *) by SessionId, UserId, IPAddress
    )
    on UserId, SessionId
| where TokenAcquisitionIPAddress != IPAddress
| where DeviceDetail.operatingSystem startswith "Windows"
| where IncomingTokenType == "primaryRefreshToken"
| extend TimeBetweenTokenAcquisition = datetime_diff( 'second', CreatedDateTime,
TokenAcquisitionCreatedDateTime)
| where TimeBetweenTokenAcquisition > 0
```

Response

- Immediate response
  - Revoke sessions
  - Mark user compromised
  - Password Reset

- Find the origin origin of the attack
  - What token material was stolen?
  - Compomised endpoint?
  - AiTM attack?

- Establish the Token Theft Playbook
  - https://learn.microsoft.com/en-us/security/operations/token-theft-playbook

Additional ressources

- https://github.com/secureworks/BAADTokenBroker
- Microsoft Entra ID - Attack and Defense Playbook https://github.com/Cloud-Architekt/AzureAD-Attack-Defense
- Microsoft Entra Conditional Access token protection explained
- https://github.com/Cloud-Architekt/AzureSentinel/tree/main/Hunting%20Queries/EID-TokenHunting
- Learn about Universal Continuous Evaluation (Preview) - Global Secure Access

We value your feedback

WPNinjas Norway: Event Session Feedback
https://forms.office.com/e/vZt63PirDv

Track: Lindesnes - Session: Attack on Token

Thank You