

# Deep-dive to Entra ID Token Theft Protection

Dr Nestori Syynimaa (@DrAzureAD)



# Contents

Token based authentication attacks

Token Theft attacks

Conditional Access Policies

Token Protection

Continuous Access Evaluation (CAE)



# Who am I?

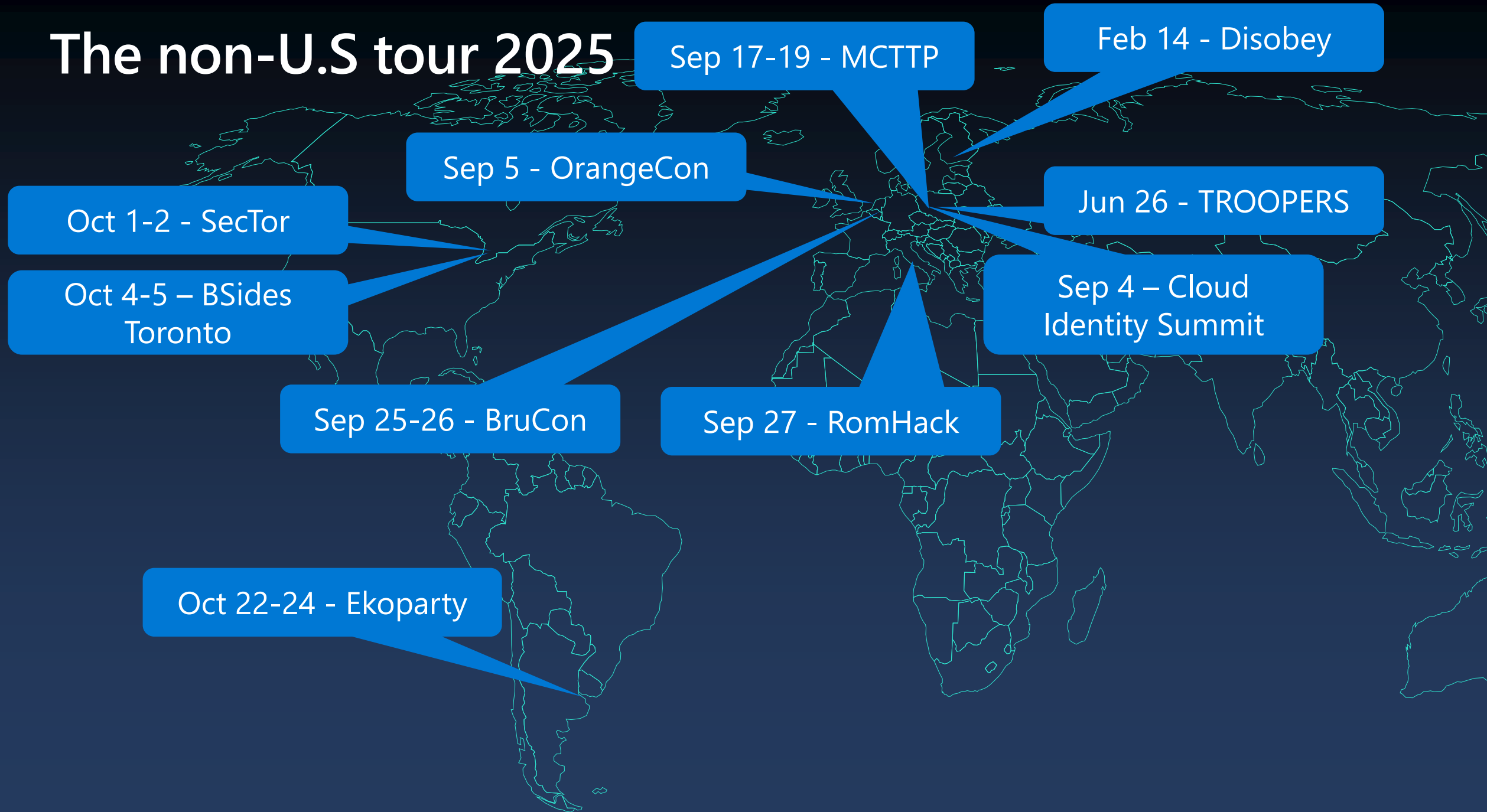
- Dr Nestori Syynimaa (DrAzureAD)
- Principal Identity Security Researcher
- Cloud, Application, and Identity Research (CAIR)

nsyynimaa@microsoft.com

@DrAzureAD

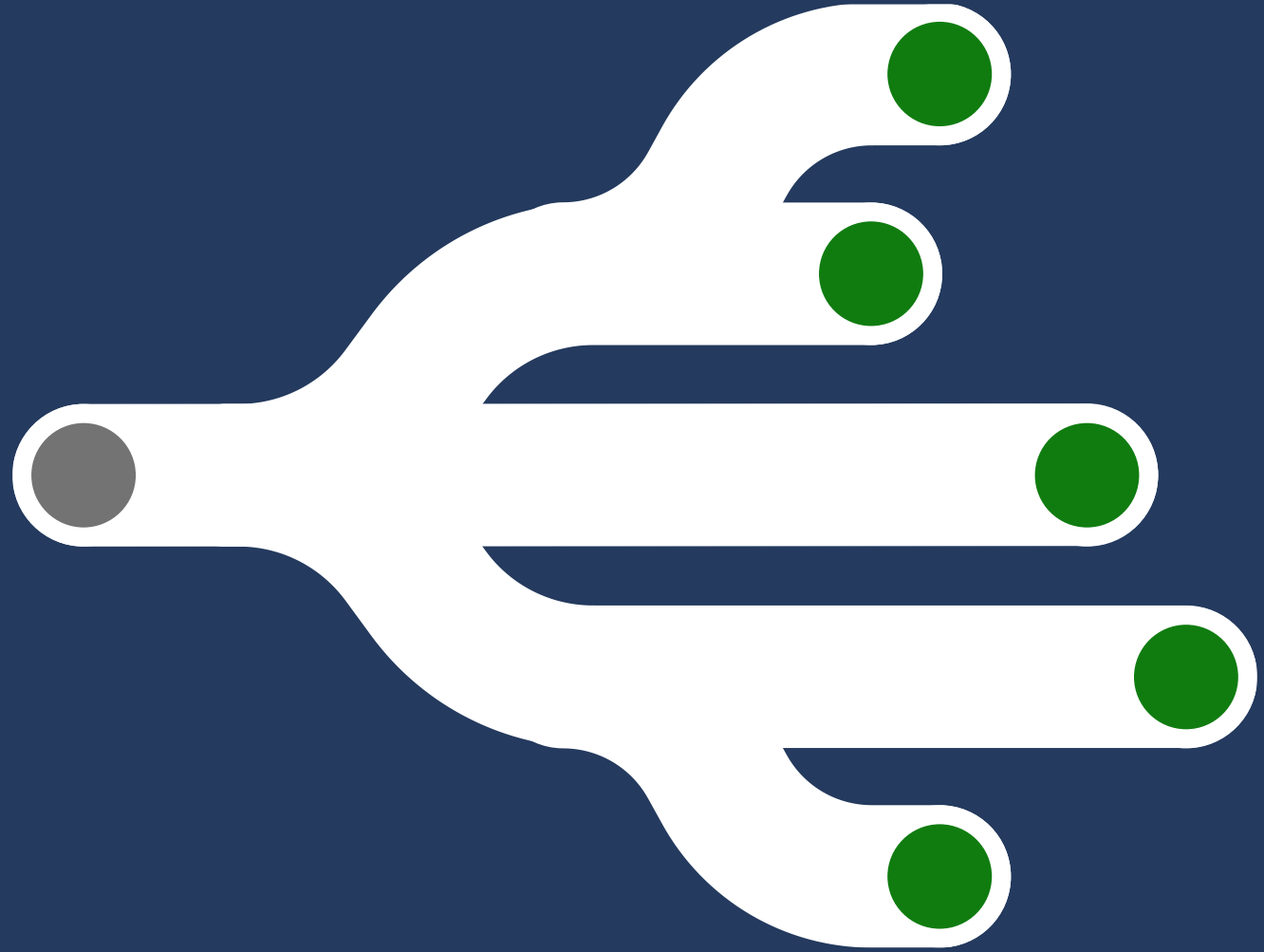


# The non-U.S tour 2025





# Token based authentication attacks



# Key concepts of token-based authentication



User

- Consumes services



Service Provider  
(SP)

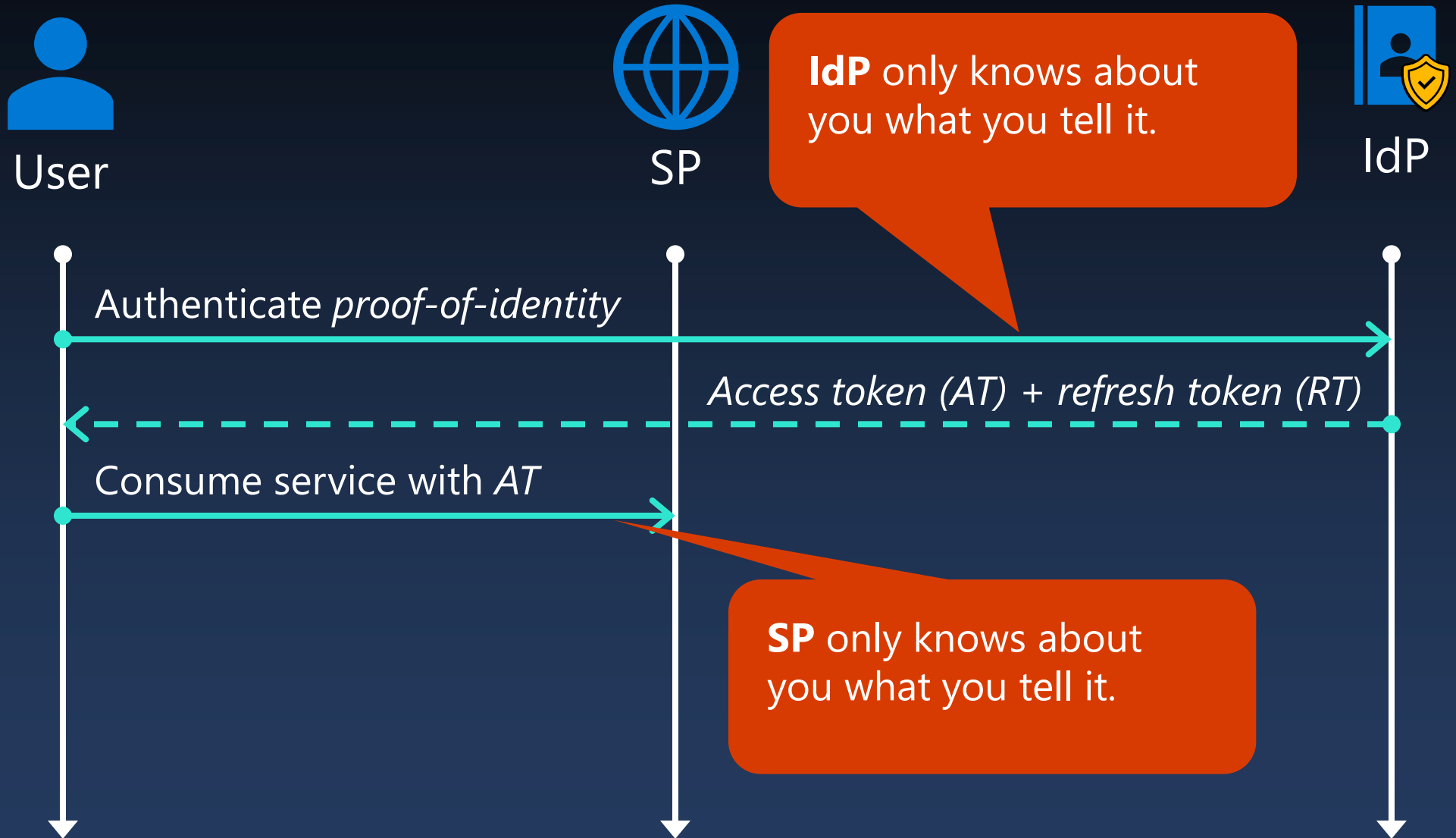
- Provides services



Identity Provider  
(IdP)

- Provides identity and access management

# How the cloud works





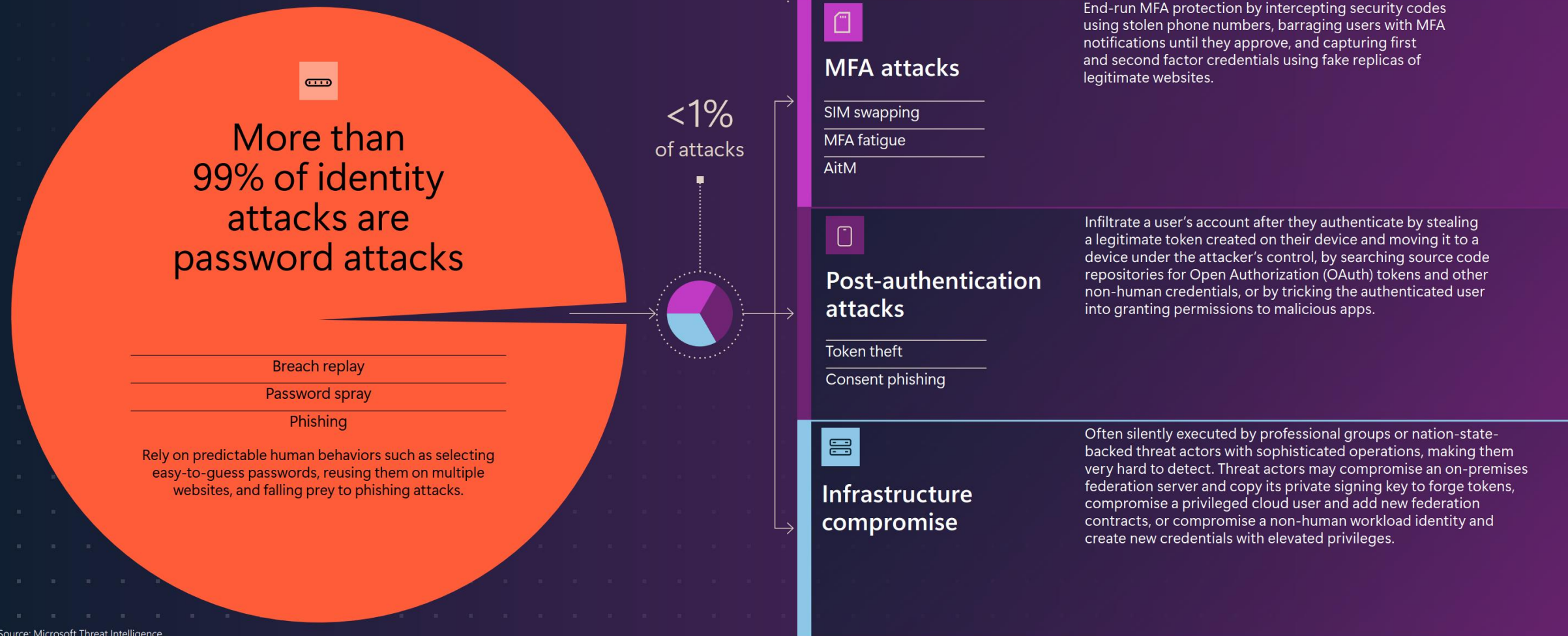


Hackers don't break in, they log in

Corey Nachreiner  
CSO, WatchGuard

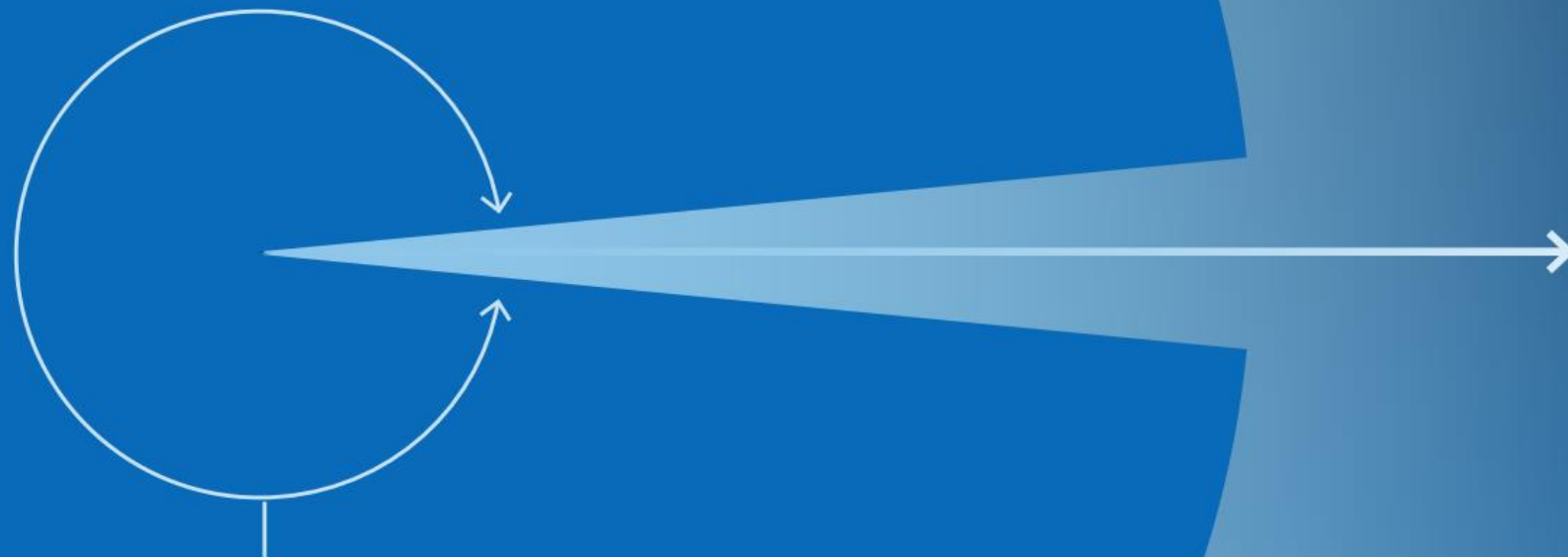
# Identity attacks in perspective

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



Source: Microsoft Threat Intelligence

# Identity attacks in perspective



More than **97%**  
of identity attacks are  
password spray or  
brute force attacks

Less than 3%  
of attacks are...

(A) Token theft by malware

**2.4042%**

(B) Infrastructure

**0.1692%**

(C) AiTM

**0.2375%**

(D) Attacks on MFA

**0.0033%**

(E) Consent phishing

**0.0005%**

(A)

(B)

(C) (D) (E)

Source: Microsoft Defender XDR and Entra ID Protection alerts (April-June 2025)

<https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/>



**Biggest problem with network defense is that defenders think in lists. Attackers think in graphs.**


**As long as this is true, attackers win.**

John Lambert

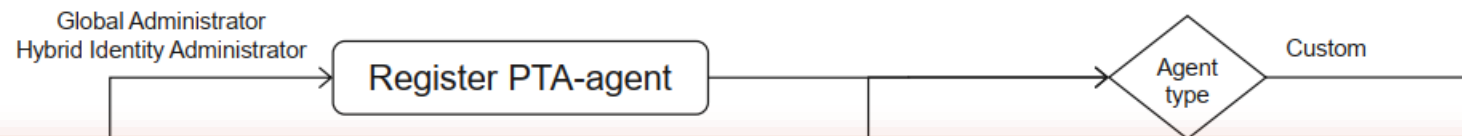
Corporate Vice President, Security Fellow, Microsoft

# Exploring Attack Paths Using Graph Theory

## Case: Microsoft Entra ID Pass-Through Authentication

Nestori Syynimaa 

Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland



So my first question is: where is there graph theory or attack graphs in this paper?

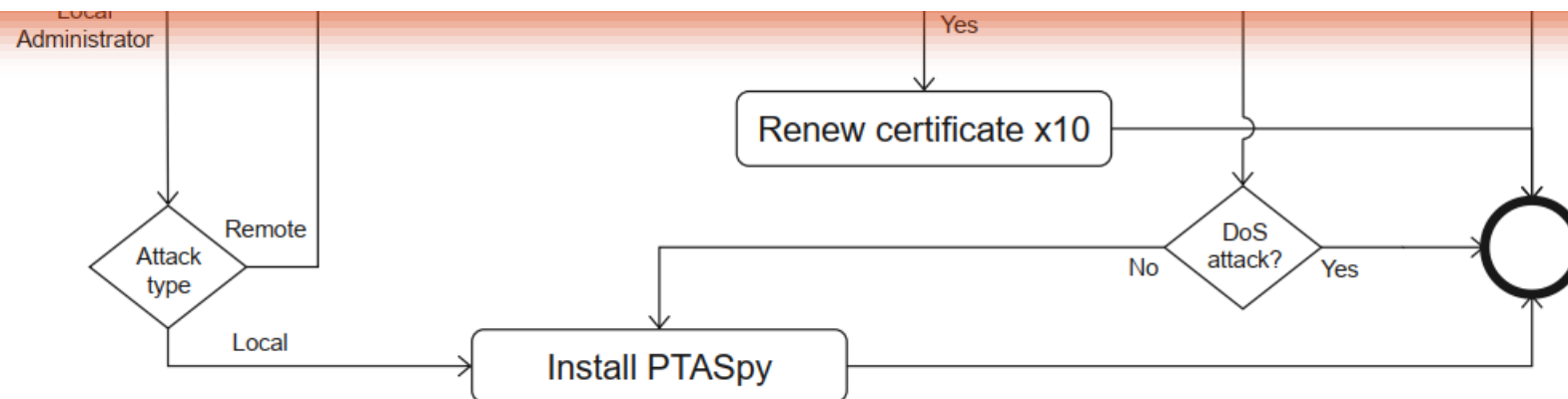
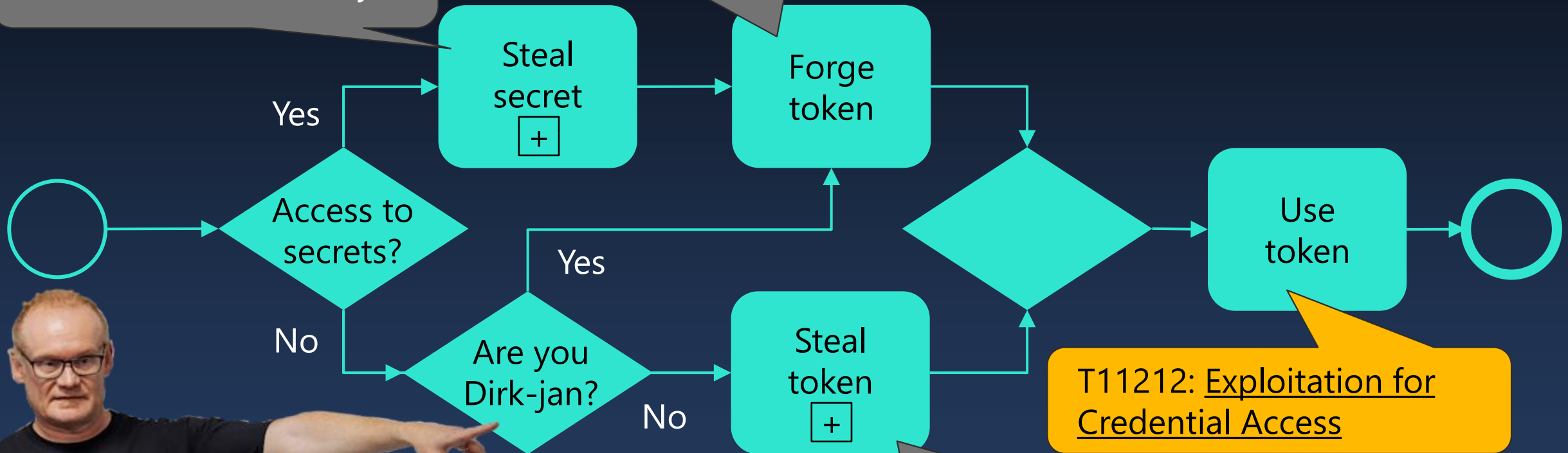


Figure 13. PTA Attack Graph v2

# Token-based authentication attack graph

T1552.004: Unsecured Credentials: Private Keys

T1606: Forge Web Credentials

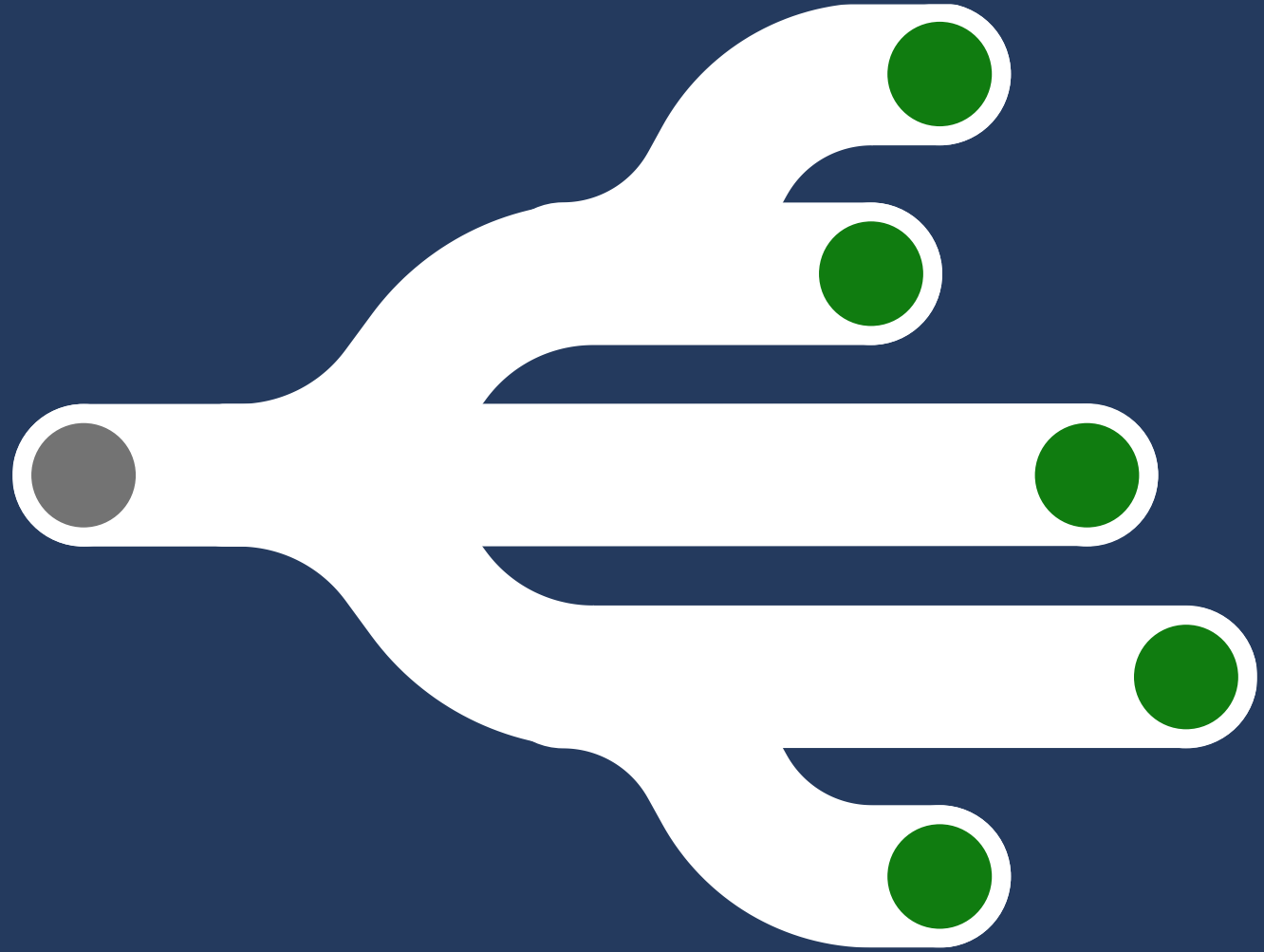


T11212: Exploitation for Credential Access

T1134.001: Access Token Manipulation: Token Impersonation/Theft



Token Theft





# Meet our bad guys:

## @L364CYB173

- Writes shellcode with HxD
- Can remotely spawn calc.exe on patched Windows
- Limitless resources



## @CL0UD3N16M4

- Lives in parents' cellar
- Knows how the f\*ck the cloud works
- 25000 ARS weekly allowance





# ~~Man-in-the-Middle (MitM)~~

## Adversary-in-the-Middle (AitM)

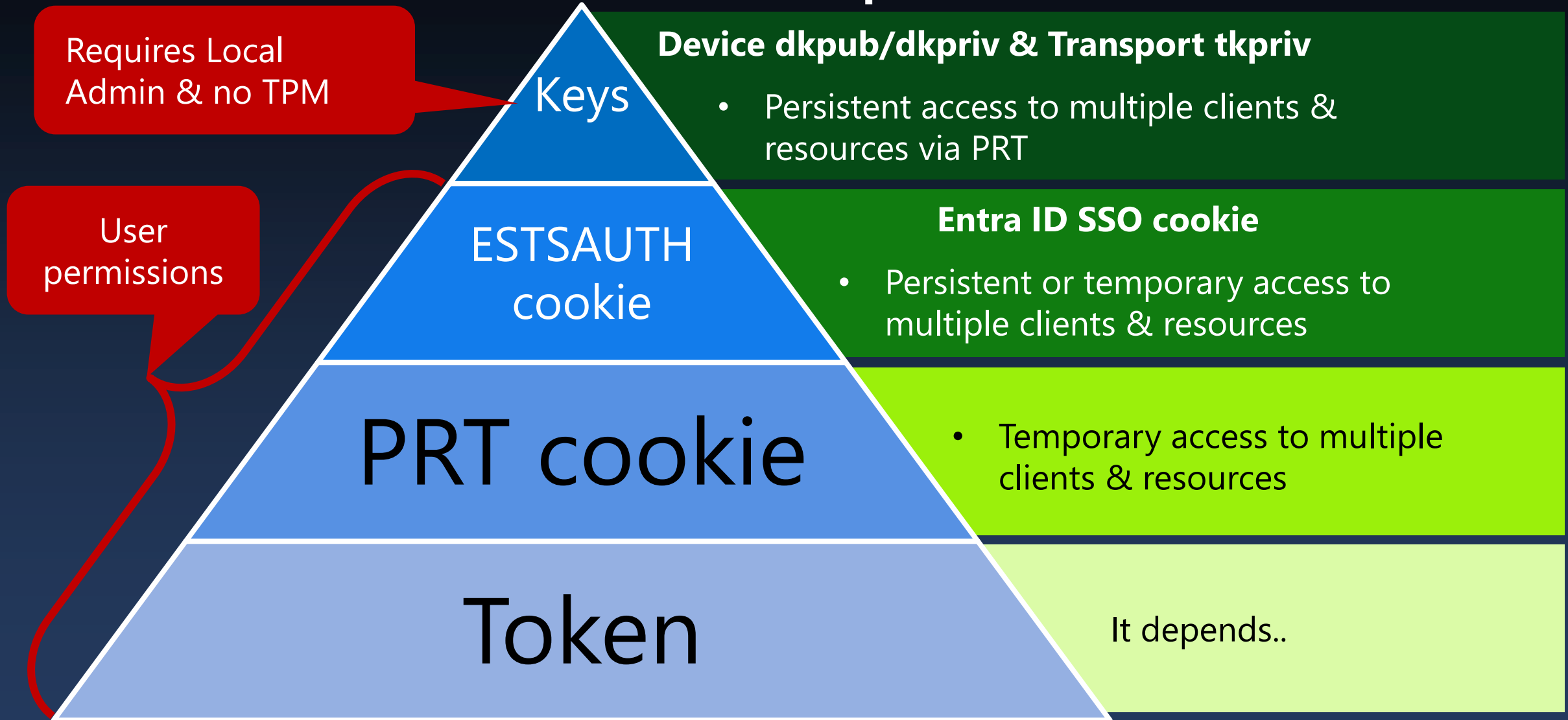
- An attack where the **adversary positions** himself **in between** the **user** and the **system** so that he can intercept and alter data traveling between them.<sup>1</sup>



Demo



# What to steal from user's endpoint?



# Which token to steal?

Requires Local  
Admin & user creds  
& no TPM

PRT

**Primary Refresh Token (+session key)**

**90 d**

- Persistent access to multiple clients & resources

User  
permissions

FRT

**Family Of Client IDs (FOCI) Refresh Token** **90 d**

- Persistent access to FOCI clients & multiple resources

Refresh Token

**90 d**

- Persistent access to single client & multiple resources

Access / ID token

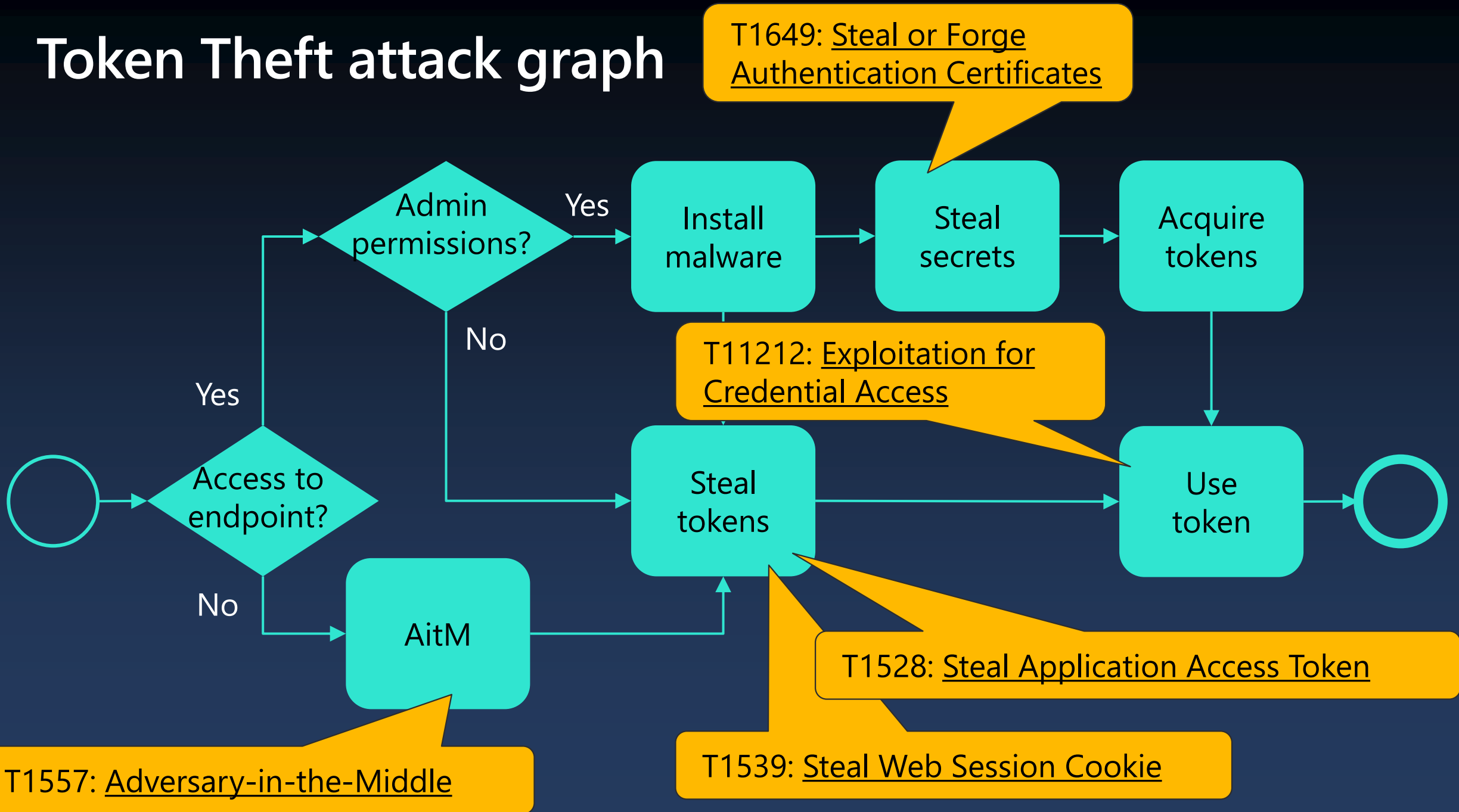
**1-28 h**

- Temporary access to single client & resource

Demo



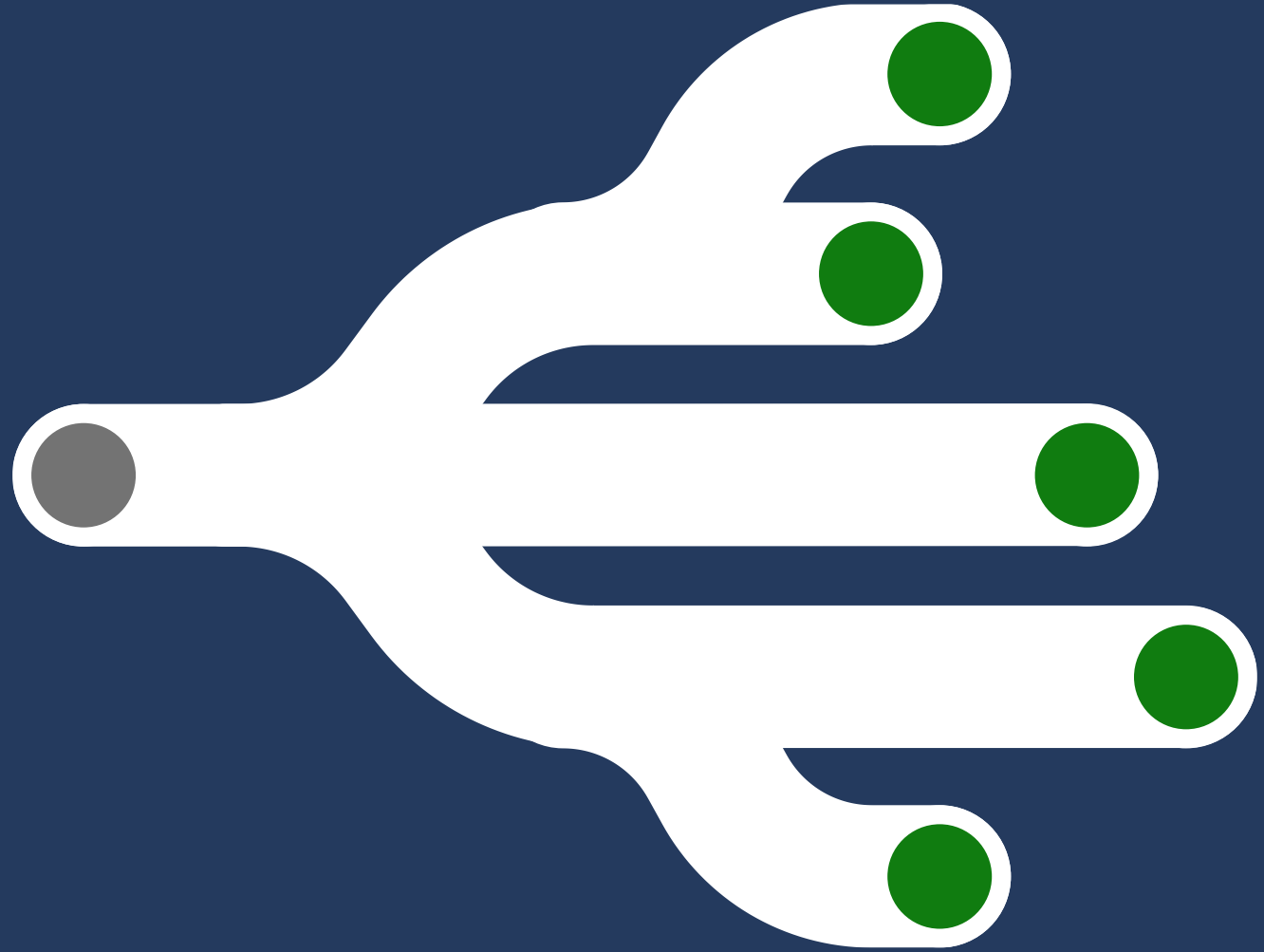
# Token Theft attack graph



# Token security best practices

- **Conditional Access Policies:** Use Conditional Access policies to enforce compliant network checks. **This ensures that tokens are only used from trusted networks and devices.**
- **Token Binding:** Implement Token Protection (formerly known as token binding) to cryptographically tie tokens to client secrets. **This prevents token replay attacks from different devices.**
- **Continuous Access Evaluation (CAE):** Implement CAE to **continuously evaluate the security state of the session**. This helps in detecting and revoking tokens if there are changes in the user's security posture, such as network location changes.

# Conditional Access Policies (CAP)





# How CAP works?



User

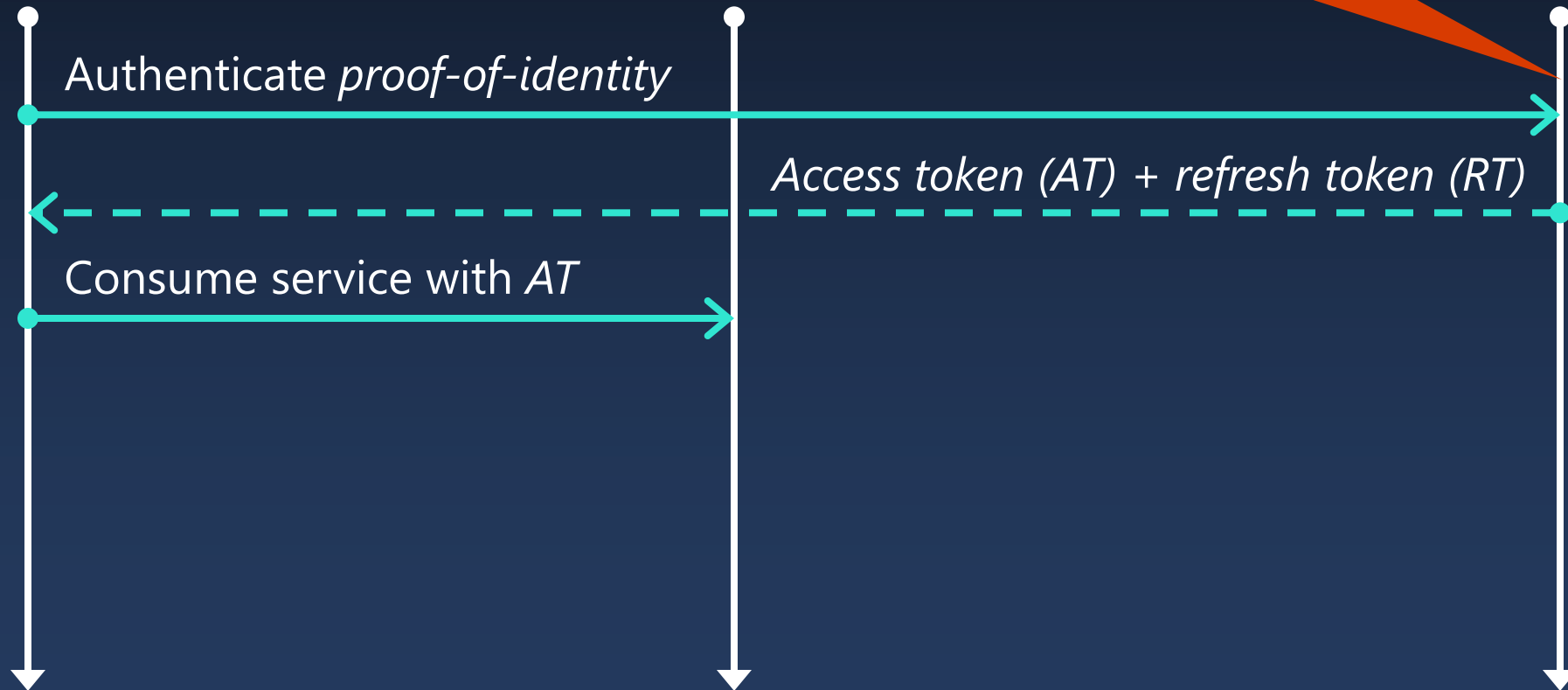


SP

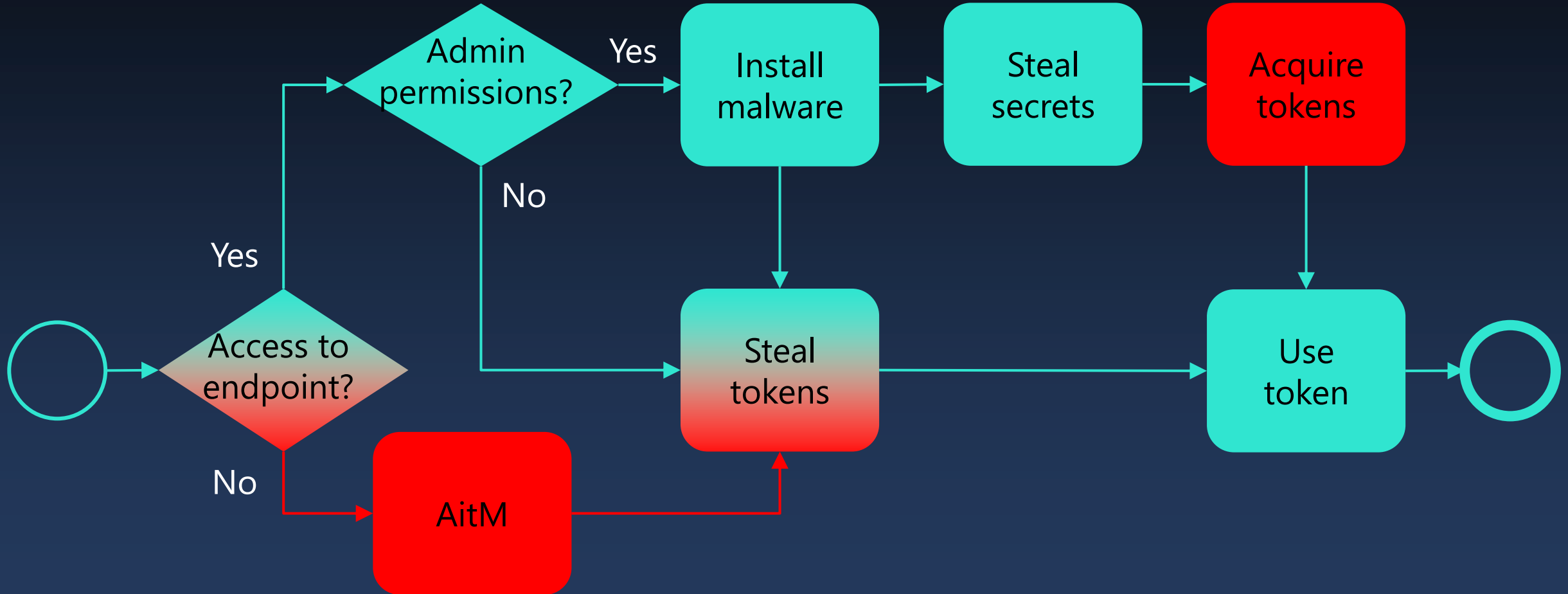


IdP

CAPs evaluated.  
Access allowed or  
denied. MFA etc. may be  
required.



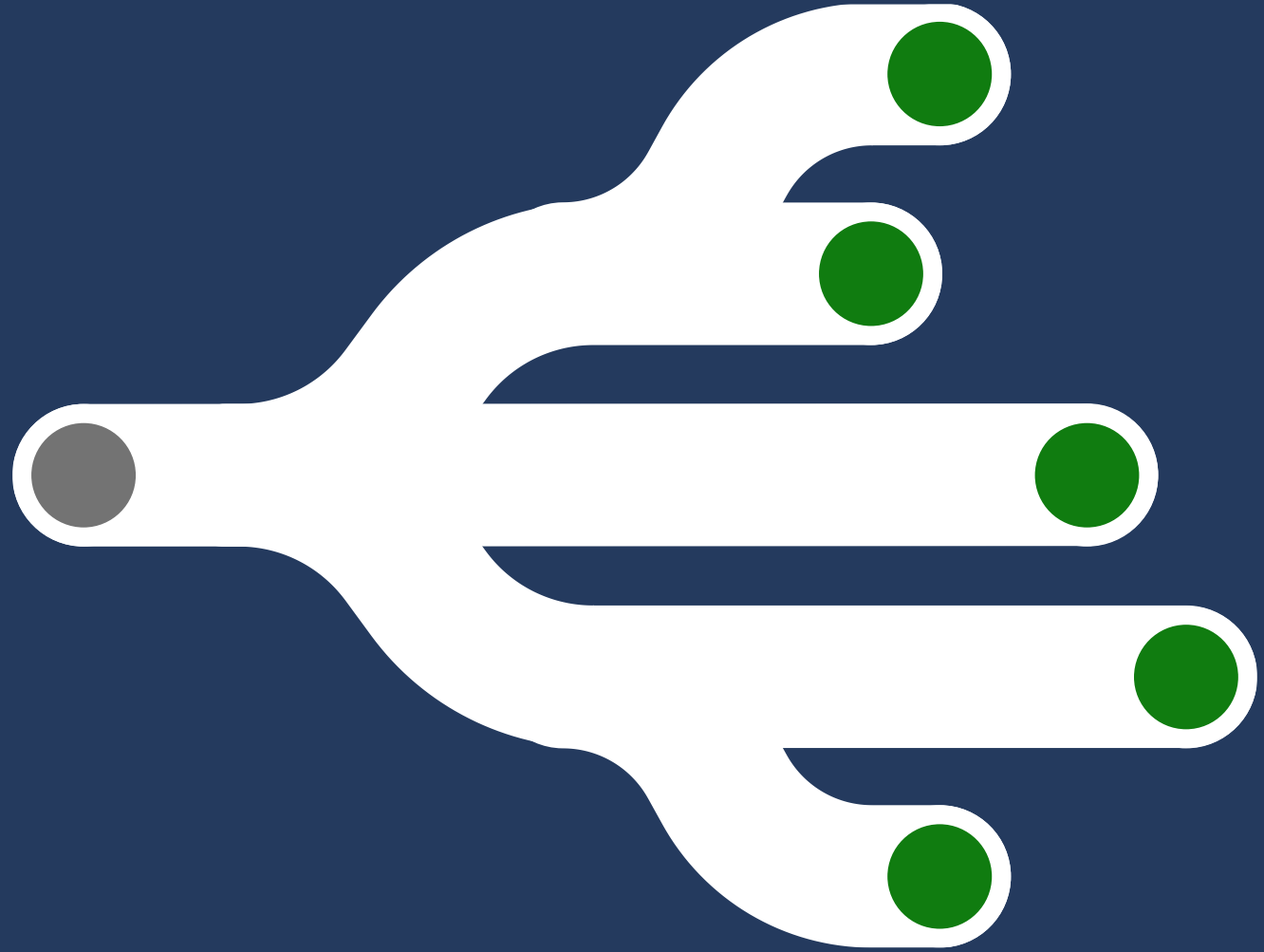
# CAP *may* protect against AitM and Acquire token



Demo



# Token Protection



# Token protection 1/4

- Supports:
  - Office 365 Exchange Online, SharePoint Online, Teams
  - Azure Virtual Desktop
  - Windows 365
- Requirements:
  - Microsoft Entra registered, joined, or hybrid joined Windows 10+ (or hybrid joined WSE 2019+), *preview for MacOS & iOS*
  - Supported native client (OneDrive, Teams, etc.)
  - Entra ID ~~P2~~ P1
- Deployment:
  - Conditional access policy

# Token protection 2/4

“Token Protection ensures that tokens can only be used on the intended device. When enforced through Conditional Access policies, tokens authorizing access to resources must come from the device where the user originally signed in. This provides the best available protection for your high-value users and data against breaches involving token theft.”

“We’re targeting **Refresh Tokens** for protection first as they tend to be longer-lived and more broadly scoped than other types of tokens and are therefore more valuable for an attacker to steal. ”

<https://techcommunity.microsoft.com/blog/microsoft-entra-blog/public-preview-token-protection-for-sign-in-sessions/3815756>

# Token Protection 3/4

"A key part of Microsoft's protections against token theft is the use of tokens that are cryptographically tied to the device they own. This is often called **token binding**, but may also be called sender constrained tokens, or token proof of possession. **Token protection makes it harder to execute the main types of attacks** designed to steal tokens, including network-based attacks and those using malware on the device **by restricting use of the stolen token from devices they weren't issued to.**"

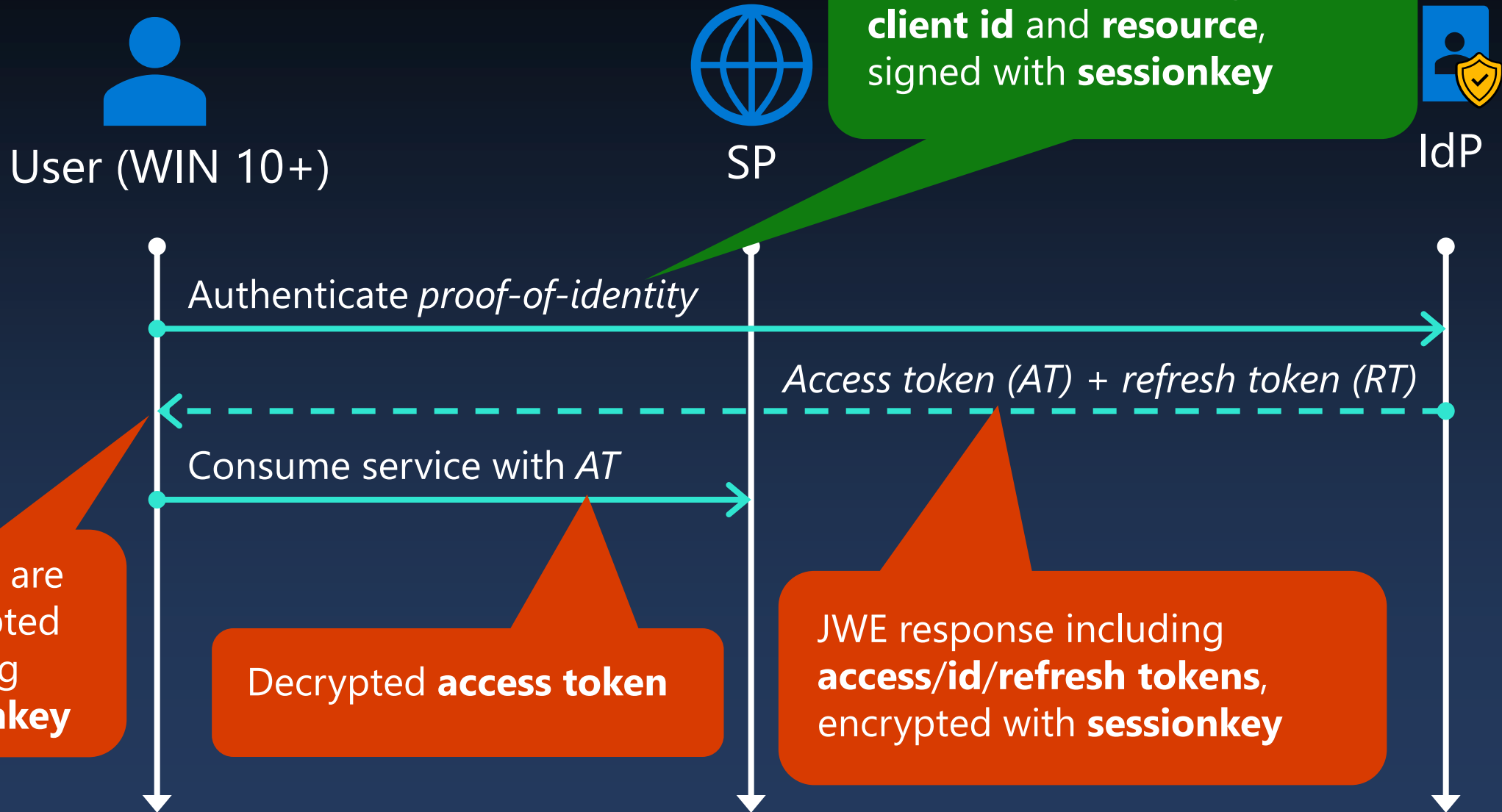
<https://techcommunity.microsoft.com/blog/microsoft-entra-blog/how-to-break-the-token-theft-cyber-attack-chain/4062700>

# Token Protection 4/4

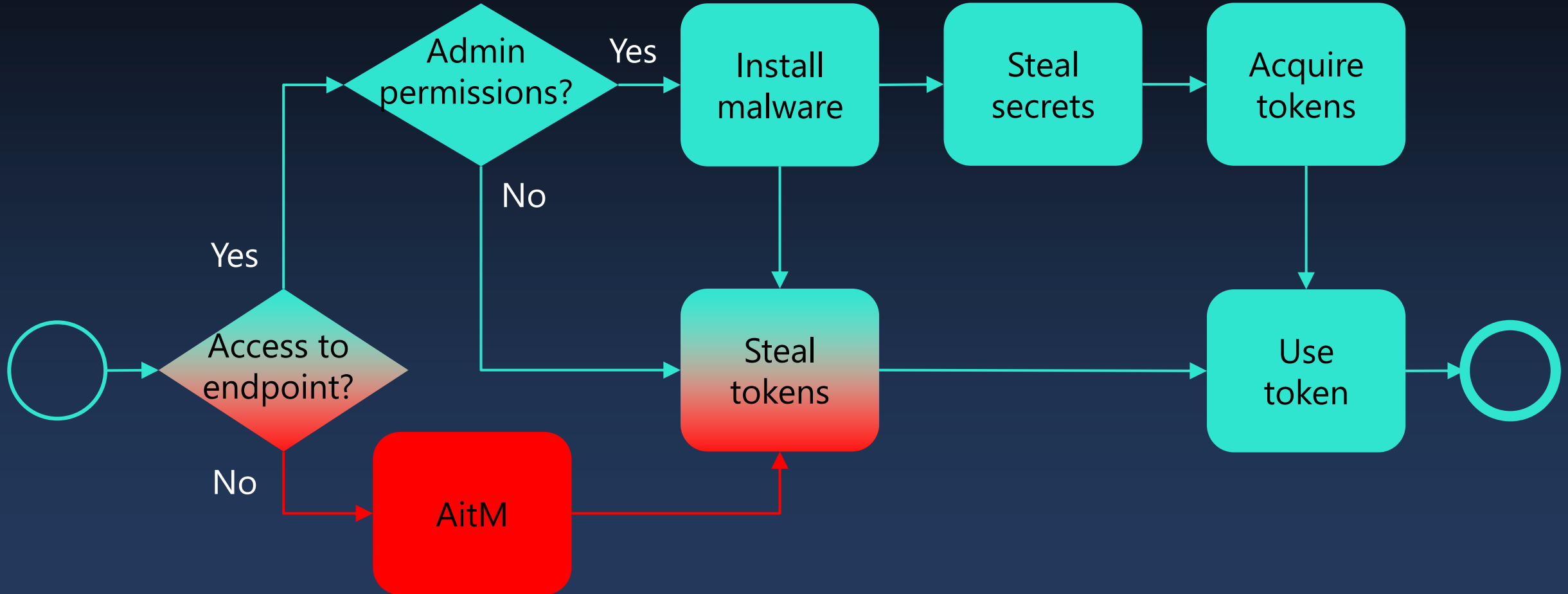
“Token protection creates a cryptographically secure tie between the token and the device (client secret) it's issued to. Without the client secret, the bound token is useless. When a user registers a Windows 10 or newer device in Microsoft Entra ID, their primary identity is bound to the device. What this means: A policy can ensure that only bound sign-in session (or refresh) tokens, otherwise **known as Primary Refresh Tokens (PRTs)** are used by applications when requesting access to a resource.”



# How Token Protection works?

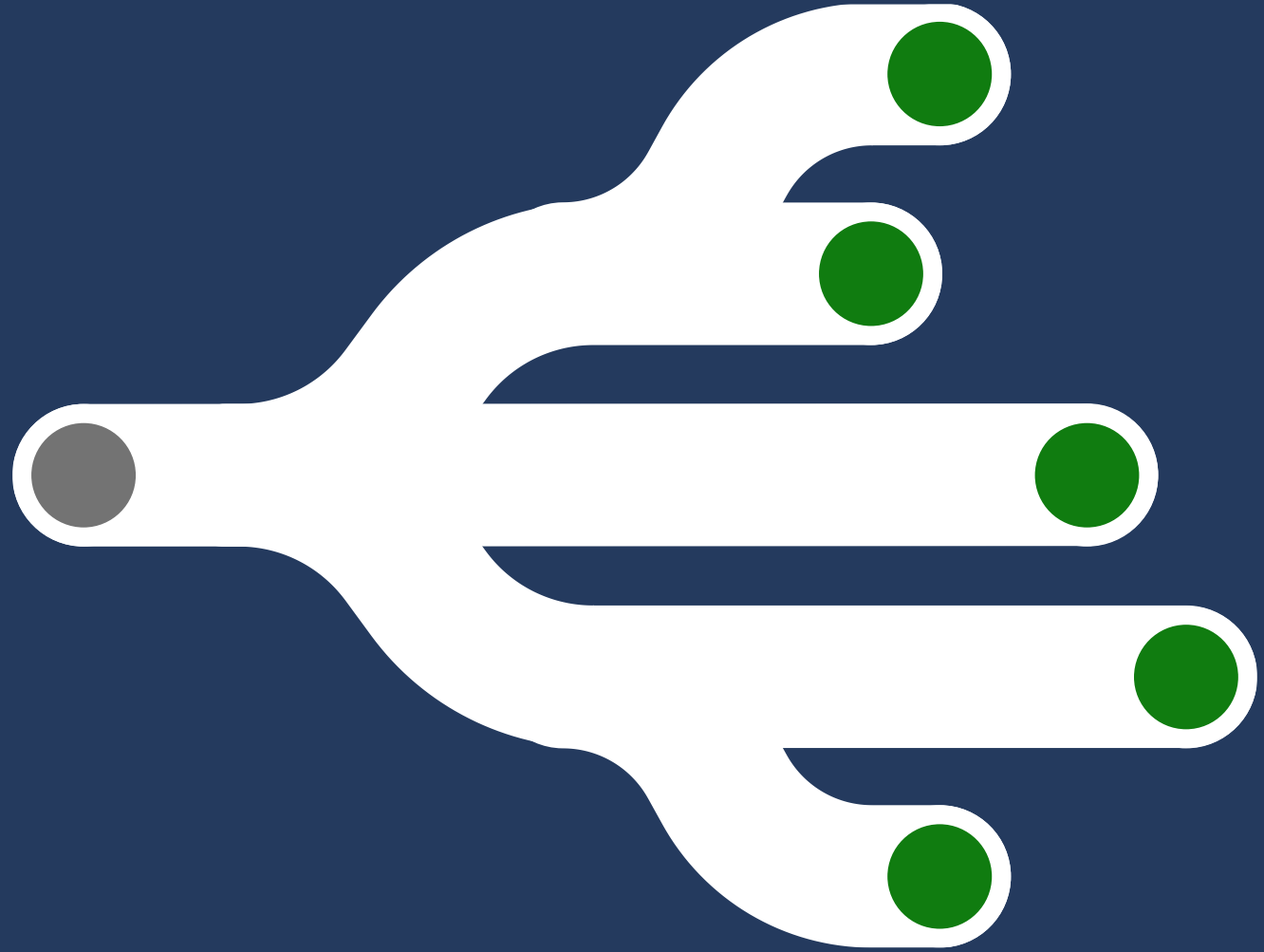


# Token Protection prevents AitM attacks



Demo

# Continuous Access Evaluation (CAE)



# Continuous Access Evaluation

- Supports:
  - Office 365 Exchange Online, SharePoint Online, Teams
- Requirements:
  - Supported client (OneDrive, Teams, custom app etc.)
  - Entra ID P1
- ~~Deployment~~ Customisation:
  - Conditional access policy

# How CAE works?

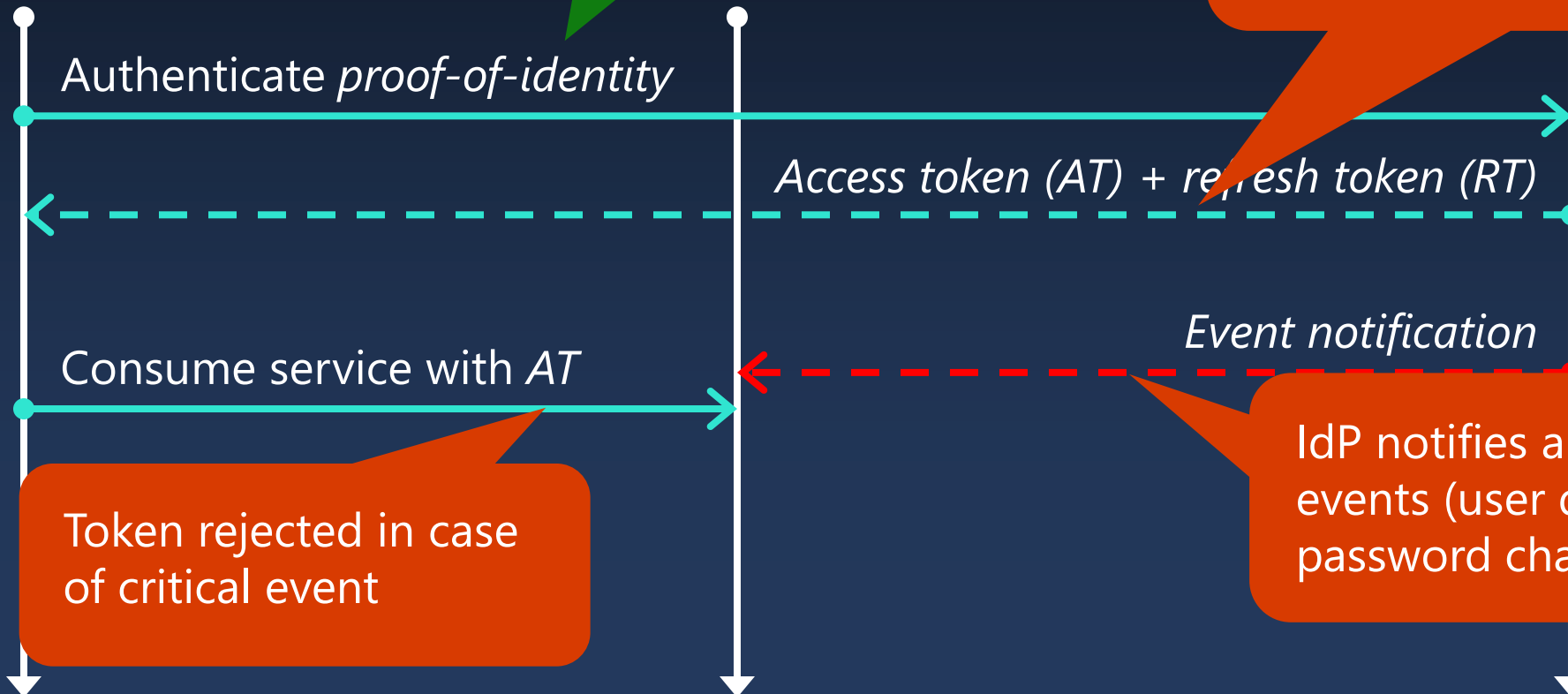


User

Include **claims** attribute with value **xms\_cc={cp1}** \*

SP

Access token will include **xms\_cc={cp1}** claim and lifetime up to **28** hours



Token rejected in case of critical event

IdP notifies about critical events (user disabled, password change, etc.)

\* <https://learn.microsoft.com/en-us/entra/identity-platform/claims-challenge?tabs=dotnet#how-to-communicate-client-capabilities-to-microsoft-entra-id>

# CAE *may* prevent token replay



\* <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-evaluation#conditional-access-policy-evaluation>

# Exploiting CAE

- CAP requires Entra ID P1 license
  - Token Protection is enforced by CAP
  - CAE can be customized using CAP
- You can *request* CAE tokens without P1 license
  - Allows threat actors to get tokens with much longer lifetime (up to 28 hours vs 1 hour)



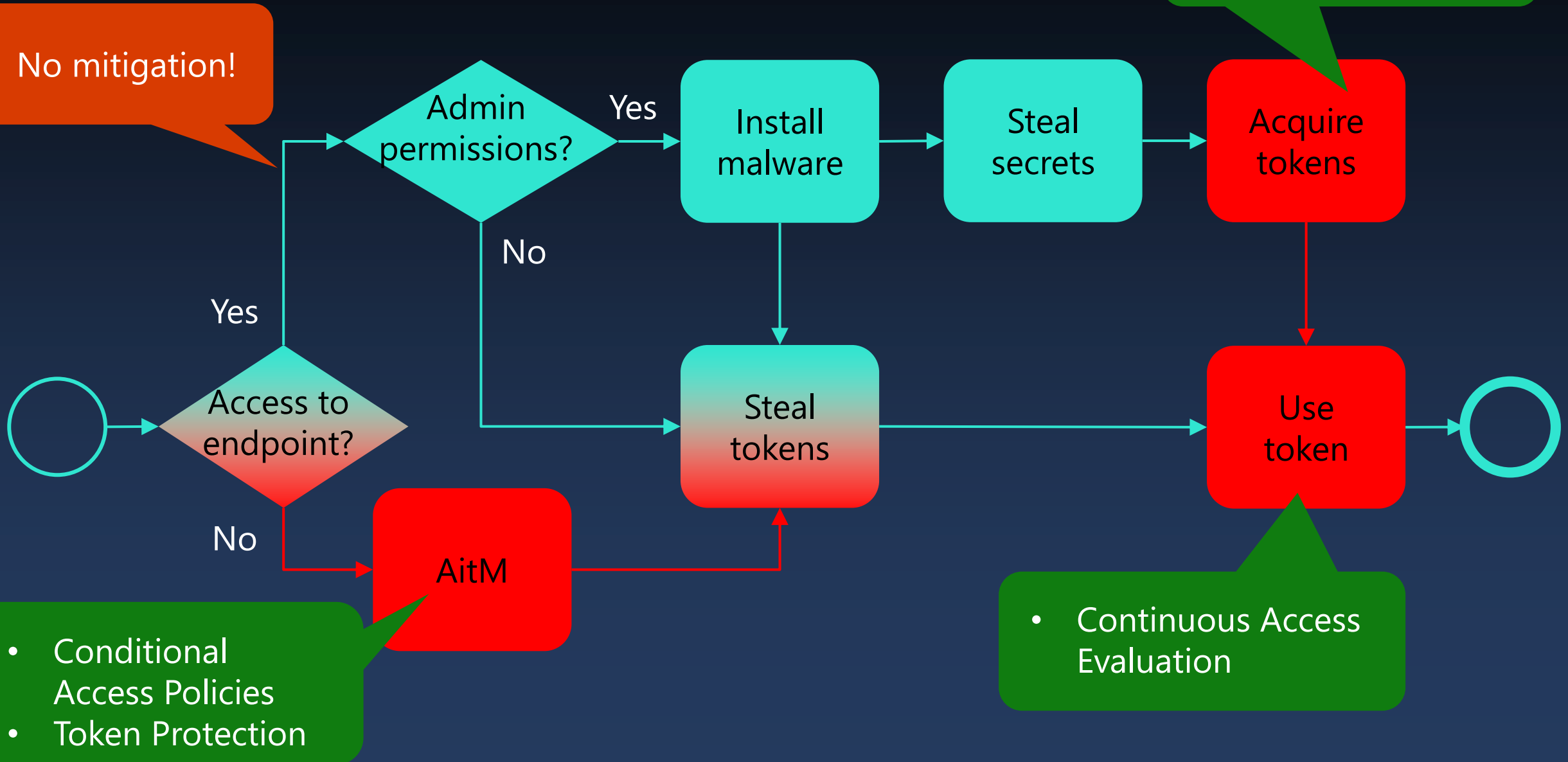
# Detecting CAE abuse

```
union isfuzzy=true SigninLogs, AADNonInteractiveUserSignInLogs  
| mv-expand todynamic(AuthenticationProcessingDetails)  
| where AuthenticationProcessingDetails.key has "Is CAE Token"  
| where AuthenticationProcessingDetails.value has "true"  
| project TimeGenerated, AppId, ResourceIdentity, UserPrincipalName
```

Demo



# Token security best practices coverage



**¡GRACIAS!**

**J\*DER!**

**N00b!!**

