SwissMicrosoft
SECURITY SUMMIT

FANTASTIC TOKENS and cookies...
IN MICROSOFT ENTRA ID
... AND HOW TO PROTECT THEM

Thomas Naunheim
Cyber Security Architect @glueckkanja AG

THOMAS NAUNHEIM

Cyber Security Architect @glueckkanja AG
Microsoft MVP (Identity & Access, Cloud Security)

Live in Koblenz/Lahnstein, Germany

cloud-architekt.net

Naunheim.cloud

thomasnaunheim

Thomas_Live


SwissMicrosoft
SECURITY SUMMIT


scopewyse
we are what's next


Ontinue


INGRAM
MICRO


EPIC FUSION
BRING IT ALL TOGETHER


Microsoft


water
IT Security & Defense


GRABX


Swiss Post
Cybersecurity


techtask


iC CONSULT


Mediawerk

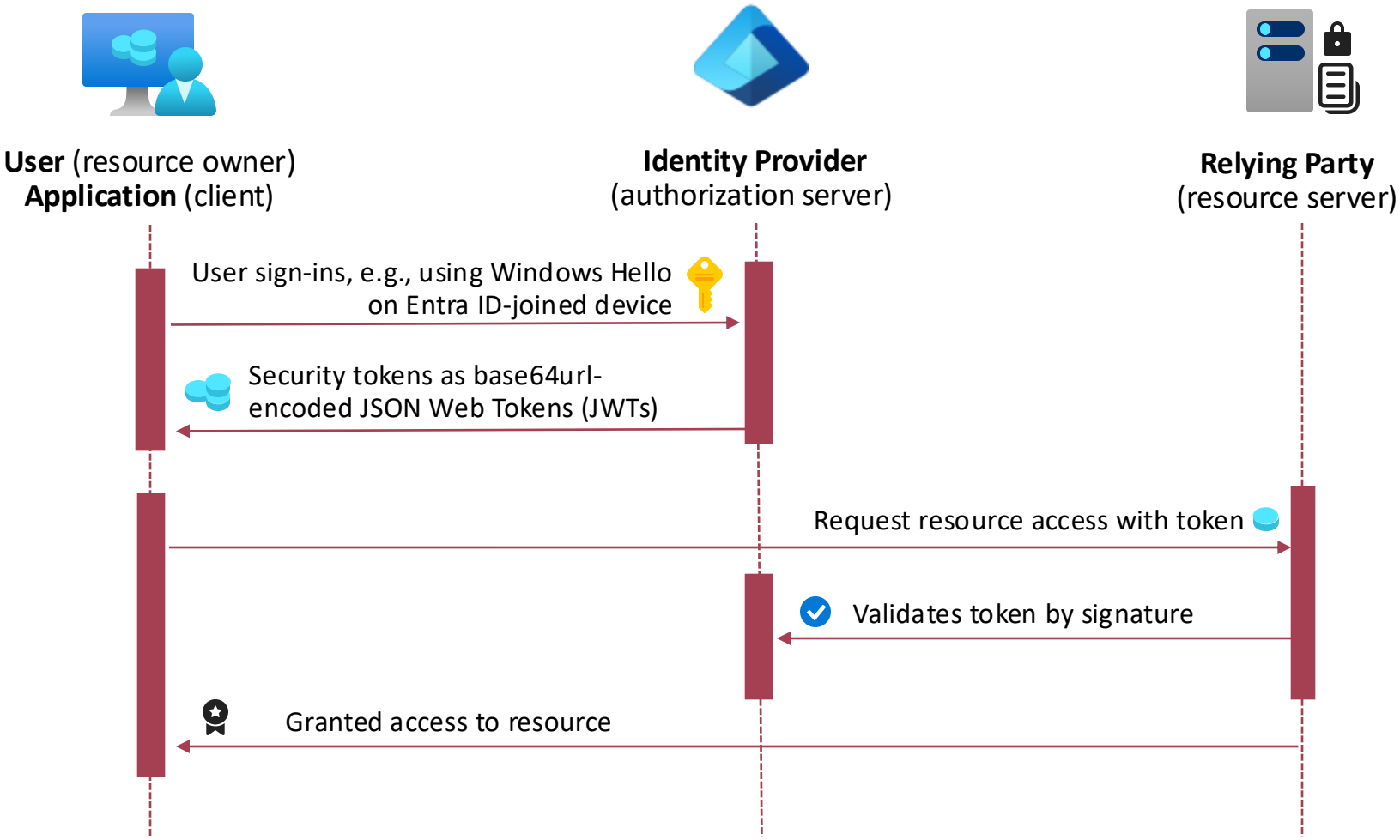
SwissMicrosoft
SECURITY SUMMIT

AGENDA

- **Introduction on token-based authentication**
- **Attack scenarios and mitigations on token theft**
- **Detection and hunting of token replay/theft**

INTRODUCTION ON TOKEN-BASED AUTHENTICATION

Security Tokens in Microsoft Entra



Payload Claims in Security Token

Issuer (Entra ID Tenant), audience (resource) and scopes (App Roles) to determine authorization, Token lifetime

```
.{
"iss": "https://sts.windows.net/<TenantId>/",
"aud": "https://management.core.windows.net/",
"scp": "user_impersonation",
"iat": 1720340188,
"nbf": 1720340188,
"exp": 1720344461,
"acr": "1",
"aio": "AXQAi/8XAAAA…
"rh":  "0.AYEAqV6VNo7JSUe2A__v5(…)",
"uti": "YZP7nqZGVkG6Vqm4j_NvAA",
"ver": "1.0",
"amr": [
"fido",
"mfa"
],
"deviceid": <EntraIdDeviceId>,
```

Payload Claims in Security Token

Token identifier and internal claims

```
.{
"iss": "https://sts.windows.net/<TenantId>/",
"aud": "https://management.core.windows.net/",
"scp": "user_impersonation",
"iat": 1720340188,
"nbf": 1720340188,
"exp": 1720344461,
"acr": "1",
"aio": "AXQAi/8XAAAA…
"rh":  "0.AYEAqV6VNo7JSUe2A__v5(…)",
"uti": "YZP7nqZGVkG6Vqm4j_NvAA",
"ver": "1.0",
"amr": [
"fido",
"mfa"
],
"deviceid": <EntraIdDeviceId>,
```

Payload Claims in Security Token

```
.{
"iss": "https://sts.windows.net/<TenantId>/",
"aud": "https://management.core.windows.net/",
"scp": "user_impersonation",
"iat": 1720340188,
"nbf": 1720340188,
"exp": 1720344461,
"acr": "1",
"aio": "AXQAi/8XAAAA…
"rh":  "0.AYEAqV6VNo7JSUe2A__v5(…)",
"uti": "YZP7nqZGVkG6Vqm4j_NvAA",
"ver": "1.0",
"amr": [
"fido",
"mfa"
],
"deviceid": <EntraIdDeviceId>,
```

Identifies the method and DeviceId which has been used for authentication

Payload Claims in Security Token

```
"idtyp": "user",
"family_name": "Naunheim",
"given_name": "Thomas",
"ipaddr": "91.16.141.22",
"oid": "0e1e6c34-9d5c-4b24-bba6-aafb0995a6e0",
"puid": "10032000E0AADE98",
"sub": "9YdwW5_2ub(…)",
"tid": "36955ea9-c98e-4749-b603-ffefe652dd90",
"unique_name": "thomas@cloud-architekt.net",
"upn": "thomas@cloud-architekt.net",
"groups": [
        <GroupId>
],
"wids": [
        <RoleDefinitionTemplateId>
],
```

Group Memberships and Entra ID Role Definition Template Ids

Overview of Token Artifacts

- Phishing-resistant authentication
- Device-Bounded or Cross-Device
- Device Identity proven by private key of certificate

Primary Refresh Token (PRT)

- Long-lived and Microsoft-specific artifact for SSO on a device
- Used to acquire token artifacts for any client/app
- Combines user and device identity, bounded to device

Refresh Tokens (RT)

- Long-lived artifacts to keep user logged-in
- Used on a scope of specific Client or "Family of Client IDs"
- Incl. authorization (groups, claims), device and user attributes

Access Tokens (AT)

- Shorter-lived artifacts for accessing resource
- Scope of Client ID and API permissions, restricted on client and resource (workload) combination

Token issuance (security and policy flow)
(Conditional Access, Risk-based Evaluation, User Assignment, User Consent Policy)

What about (Session) Cookies?

Session cookies

- Long-lived artifacts used for browser-based SSO after authentication
- Issued by IdP and service (resource owner)

Learn / Microsoft Entra / Microsoft Entra ID / Authentication /

Web browser cookies used in Microsoft Entra authentication

Article • 10/23/2023 • 6 contributors

Feedback

During authentication against Microsoft Entra ID through a web browser, multiple cookies are involved in the process. Some of the cookies are common on all requests. Other cookies are used for specific authentication flows or specific client-side conditions.

Persistent session tokens are stored as persistent cookies on the web browser's cookie jar. Non-persistent session tokens are stored as session cookies on the web browser, and are destroyed when the browser session is closed.

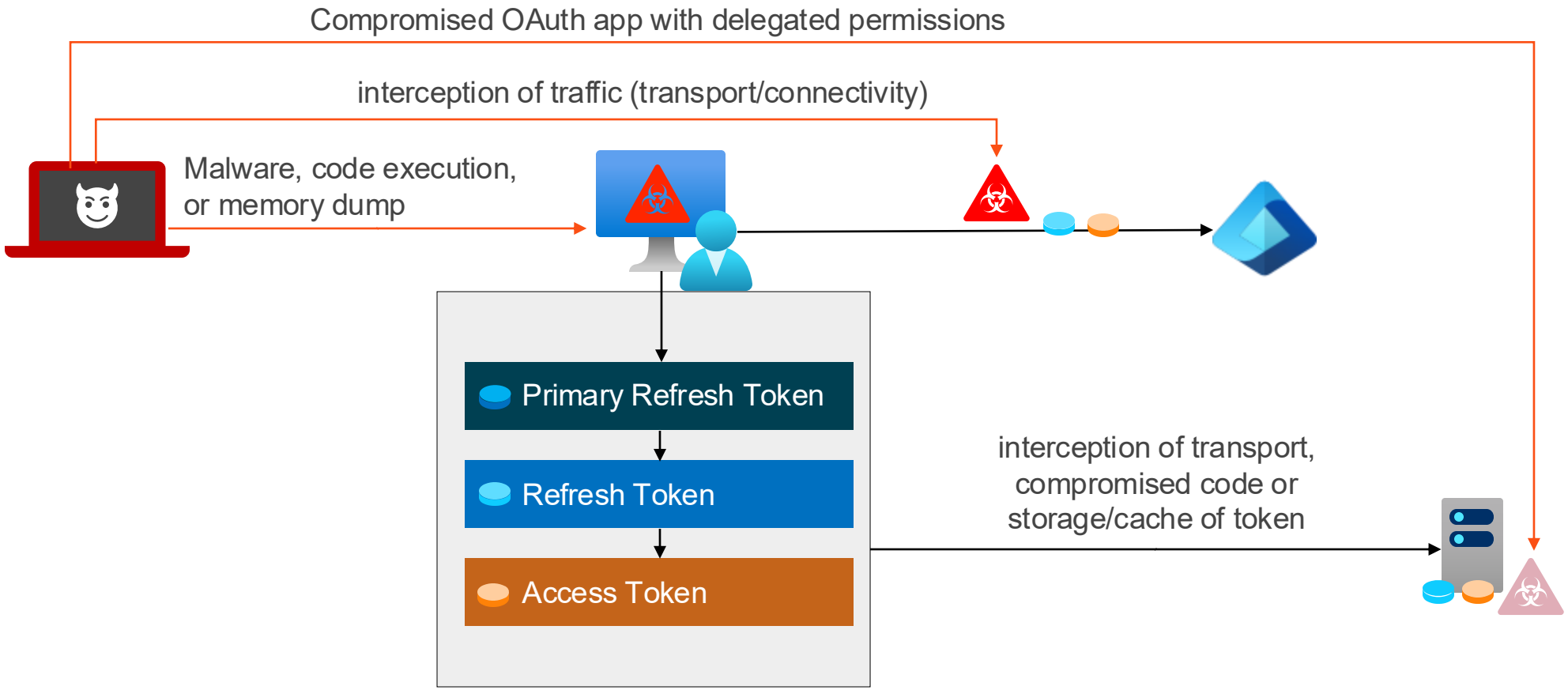
Expand table

Cookie Name	Type	Comments
ESTSAUTH	Common	Contains user's session information to facilitate SSO. Transient.

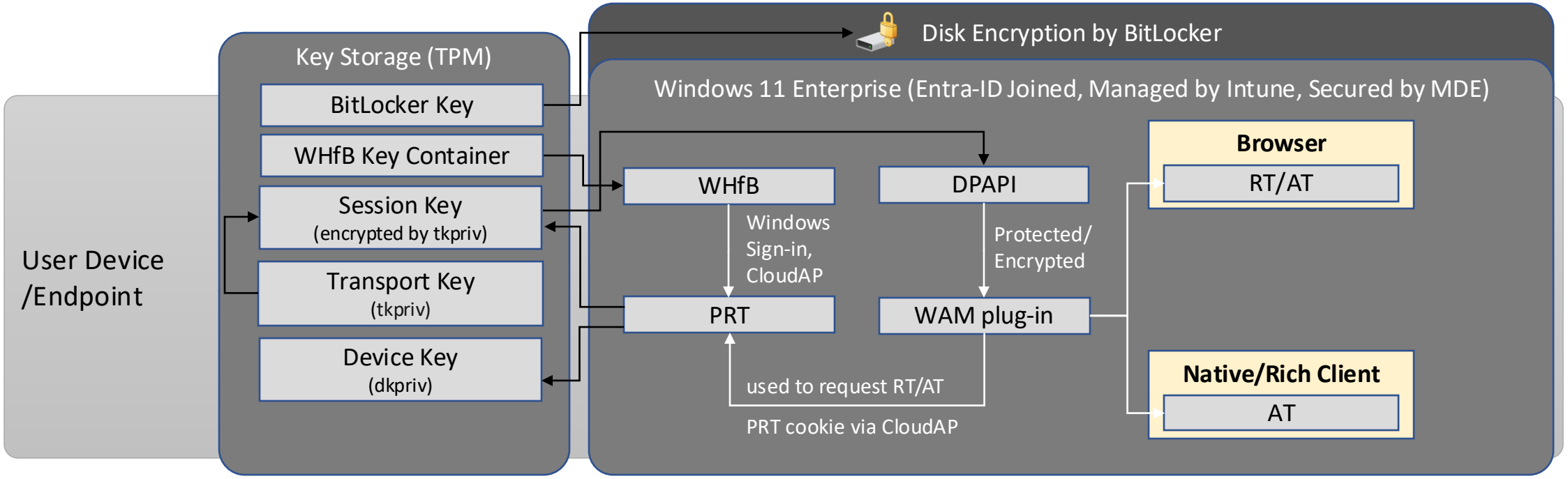
Source: Microsoft Learn | Web browser cookies used in Microsoft Entra authentication, Details about "Pass-the-cookie" attacks

ATTACK SCENARIOS AND MITIGATIONS ON TOKEN THEFT

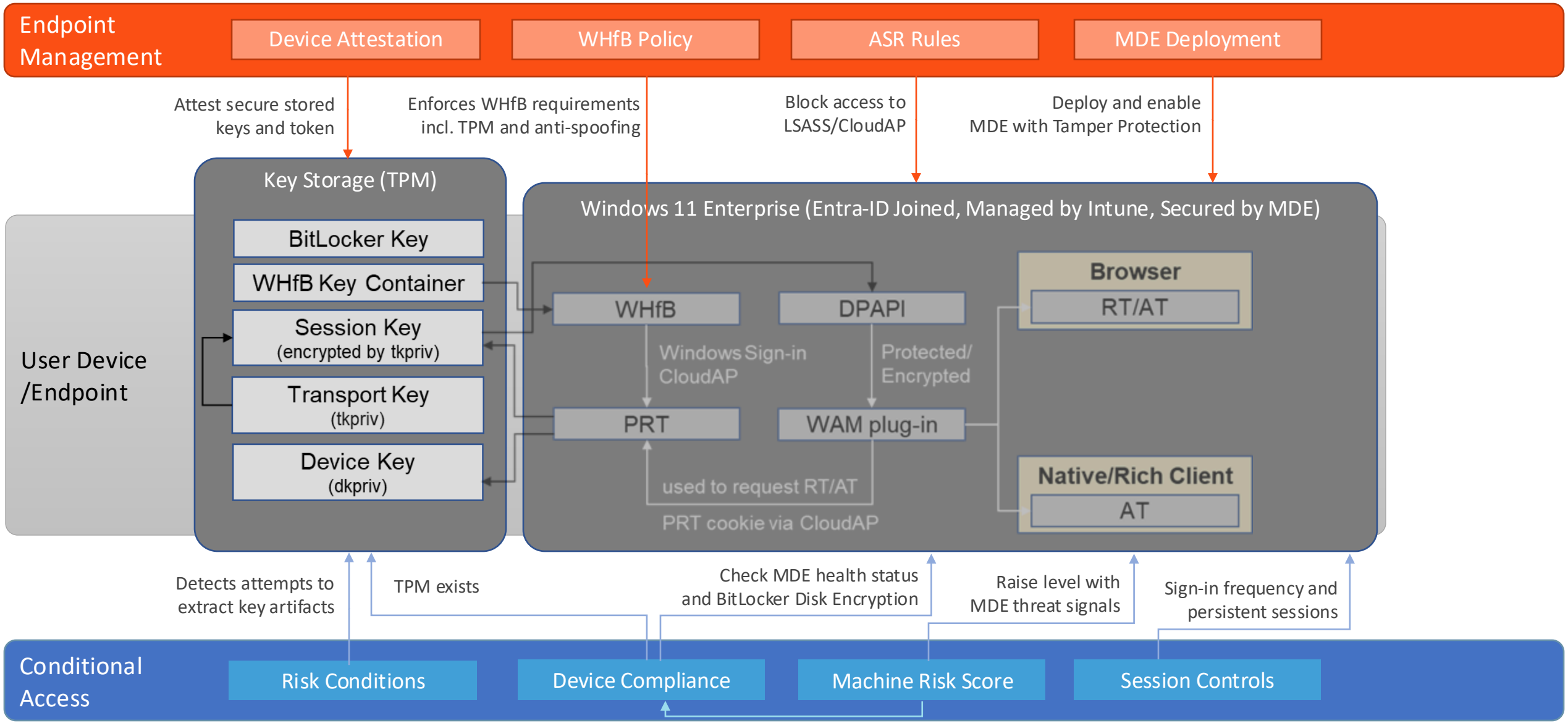
Overview of attack techniques on token artifacts



Primary Refresh Token on Windows 11



Primary Refresh Token on Windows 11



Exfiltration of PRT from CloudAP

```
   ___    ___    ____ ____      __                          __
  /   |  /   |  / __ \/ _/___  / /___  _____________ _____/ /___
 / /| | / /| | / / / // // __ \/ __/ _ \/ ___/ __ \/ __ `/ / ___/
/ ___ |/ ___ |/ /_/ _/ // / / / /_/  __/ /  / / / / /_/ / (__  )
/_/  |_/_/  |_/_____/___/_/ /_/\__/\___/_/  /_/ /_/\__,_/_/____/

 by @DrAzureAD (Nestori Syynimaa)

WARNING: Transport key stored to TPM, exporting not possible!
Exception: C:\Program Files\WindowsPowerShell\Modules\AADInternals\0.8.0\Device_utils.ps1:54
Line |
  54 |              Throw "Unable to get SoftwareTransportKeyName from $regis …
     |              ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     | Unable to get SoftwareTransportKeyName from
     |
HKLM:\SYSTEM\CurrentControlSet\Control\Cryptography\Ngc\KeyTransportKey\PerDeviceKeyTransportKey\335f83adcbc
fc0f173f2be88f14d73677df7beedb055130fea2519b8dc8ab573\0b9cc3031aa7d77d175035b79369c29acfb1661953b9629071aa5d
6becd0621d
```

WAM support in Microsoft Pwsh / CLI

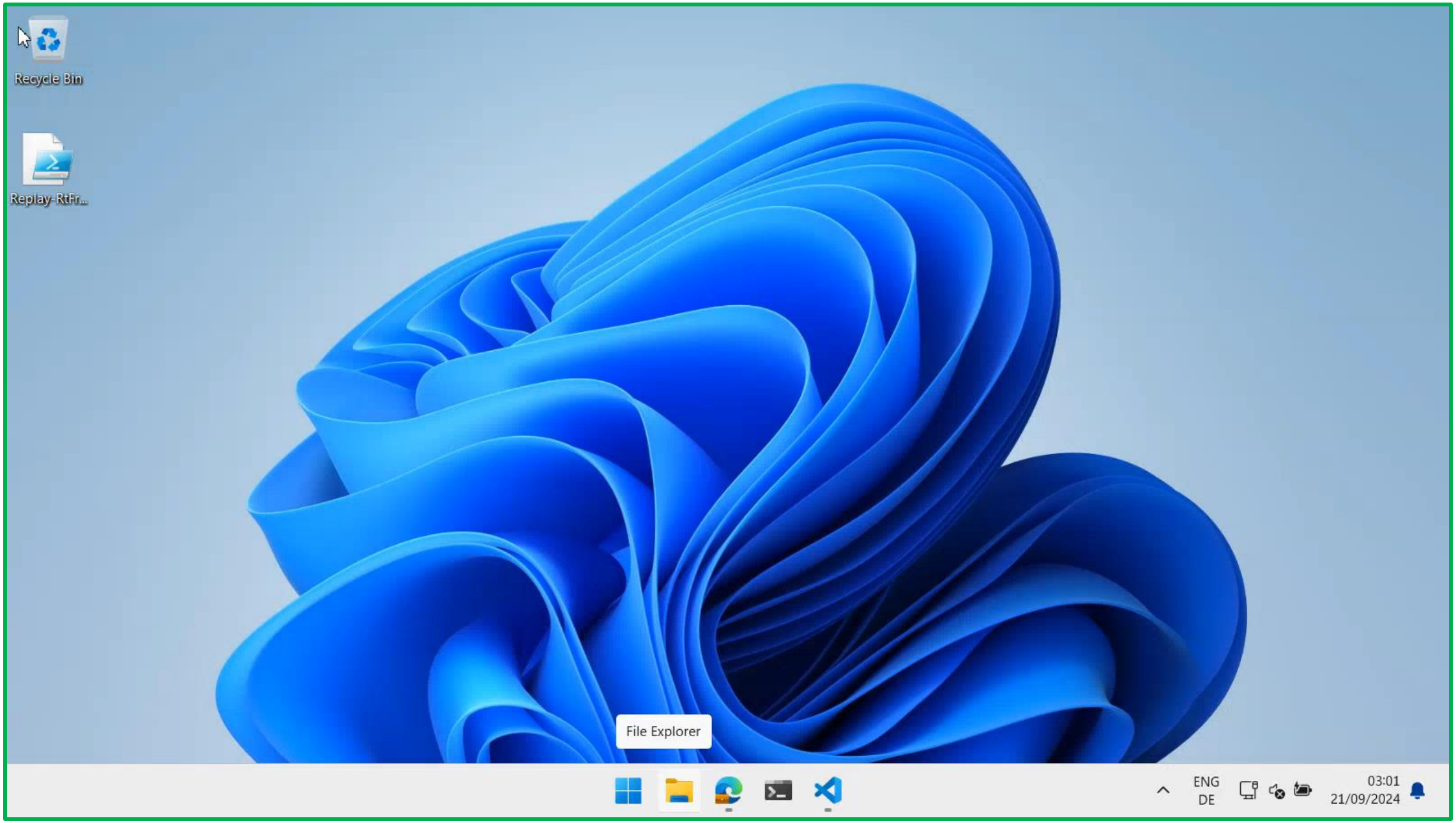
```
PS /Users/thomas.naunheim> Get-MgGraphOption

EnableWAMForMSGraph
-------------------
              False
```

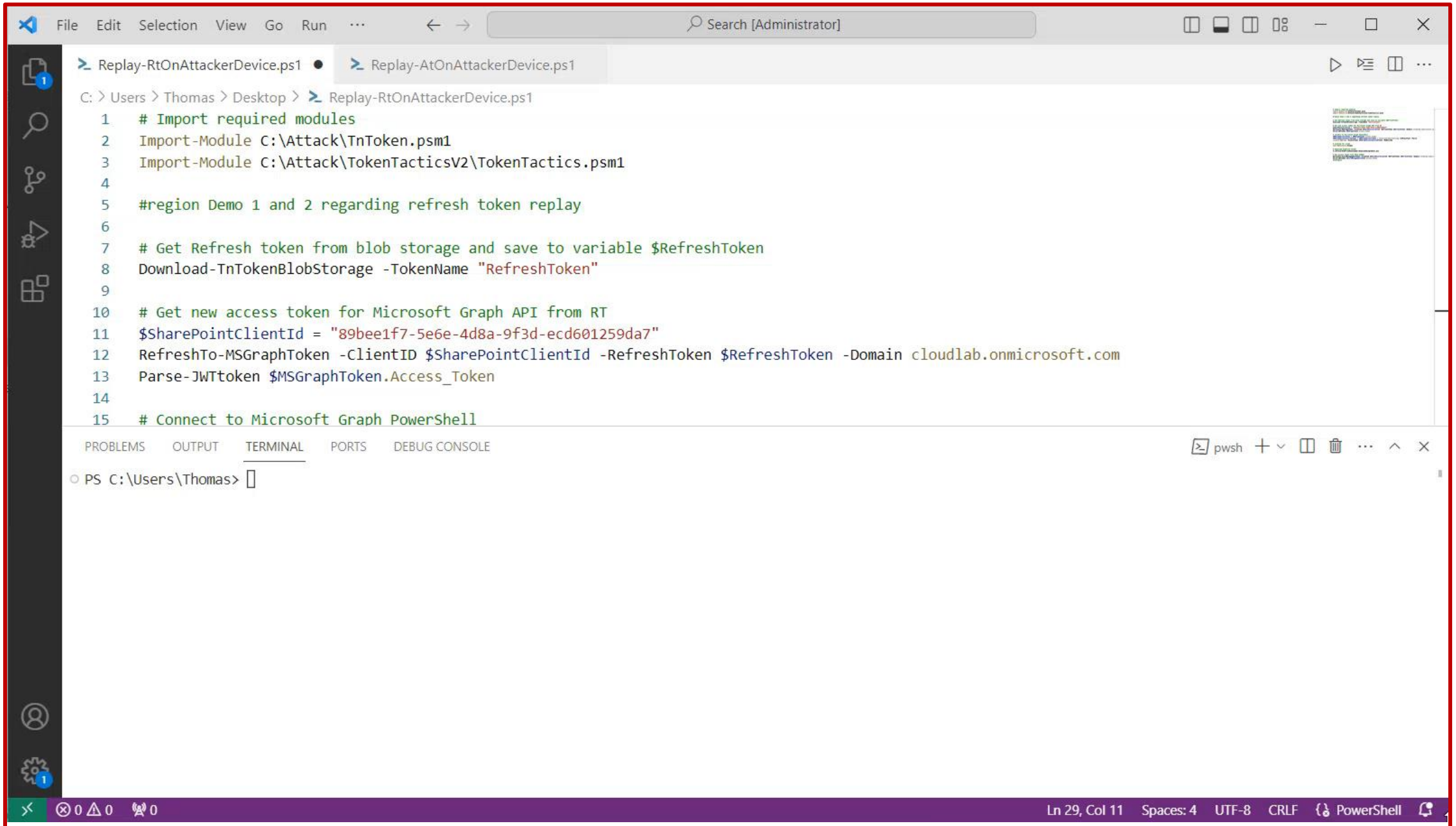
```
PS /Users/thomas.naunheim> Get-AzConfig | ? {$_.key -eq "EnableLoginByWAM"} | fl

Key          : EnableLoginByWam
Value        : True
Scope        : Default
AppliesTo    : Az
HelpMessage  : When enabled, Web Account Manager (WAM) will be the default
               interactive login experience. It will fall back to using the browser
               if the platform does not support WAM. For more details please refer
               to https://go.microsoft.com/fwlink/?linkid=2272007
DefaultValue : True
```

VICTIM DEVICE | EXFILTRATION OF REFRESH TOKEN FROM A BROWSER (WINDOWS 11 ENTERPRISE DEVICE)

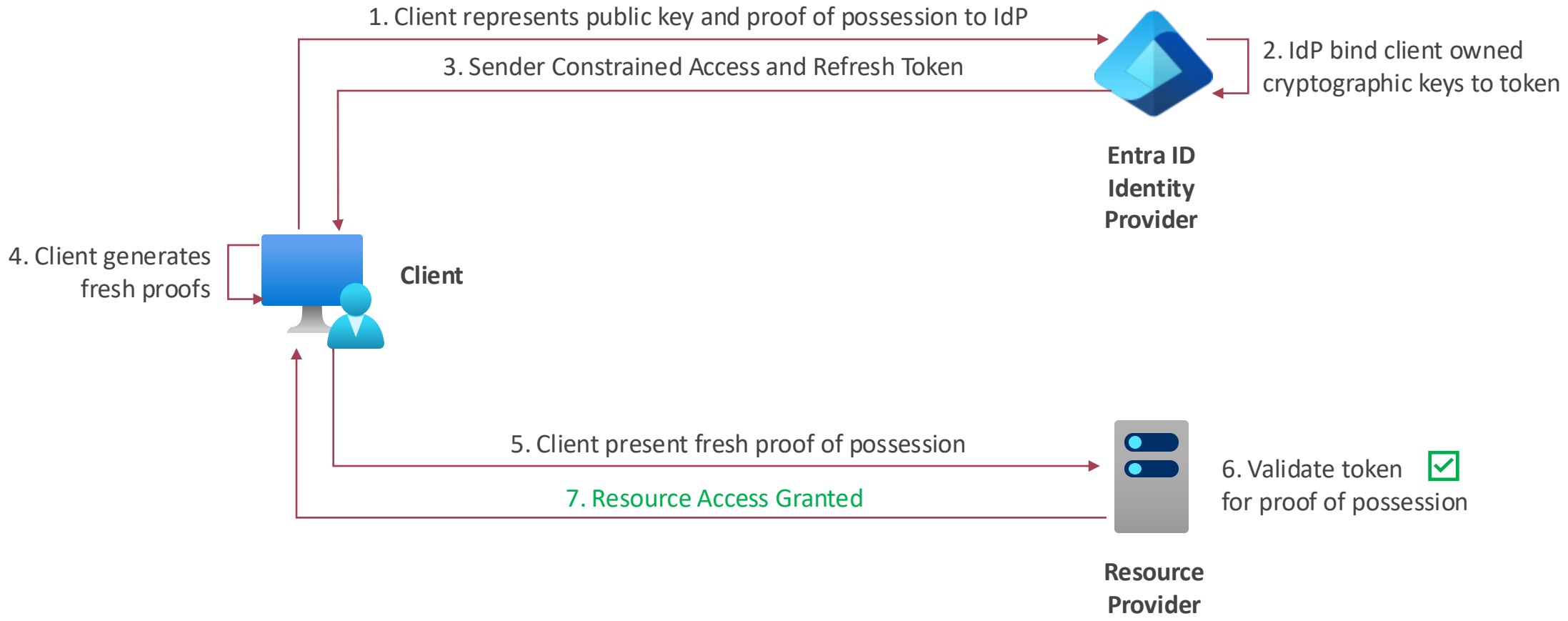


ATTACKER DEVICE | REPLAY OF REFRESH TOKEN FROM A BROWSER (WINDOWS 11 ENTERPRISE DEVICE)



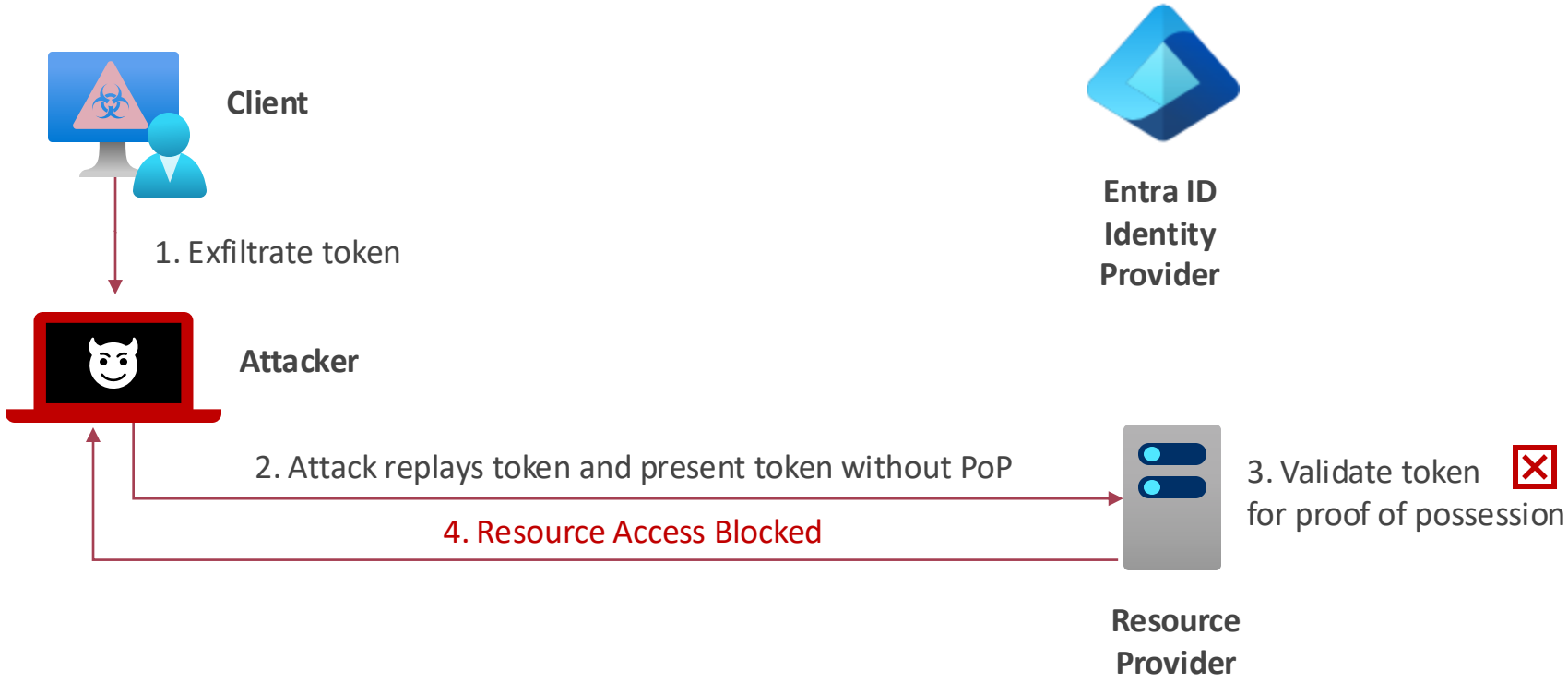
Token Binding (proof-of-possession)

Prevent token replay by enforcing cryptographically secure tie between the token and the device

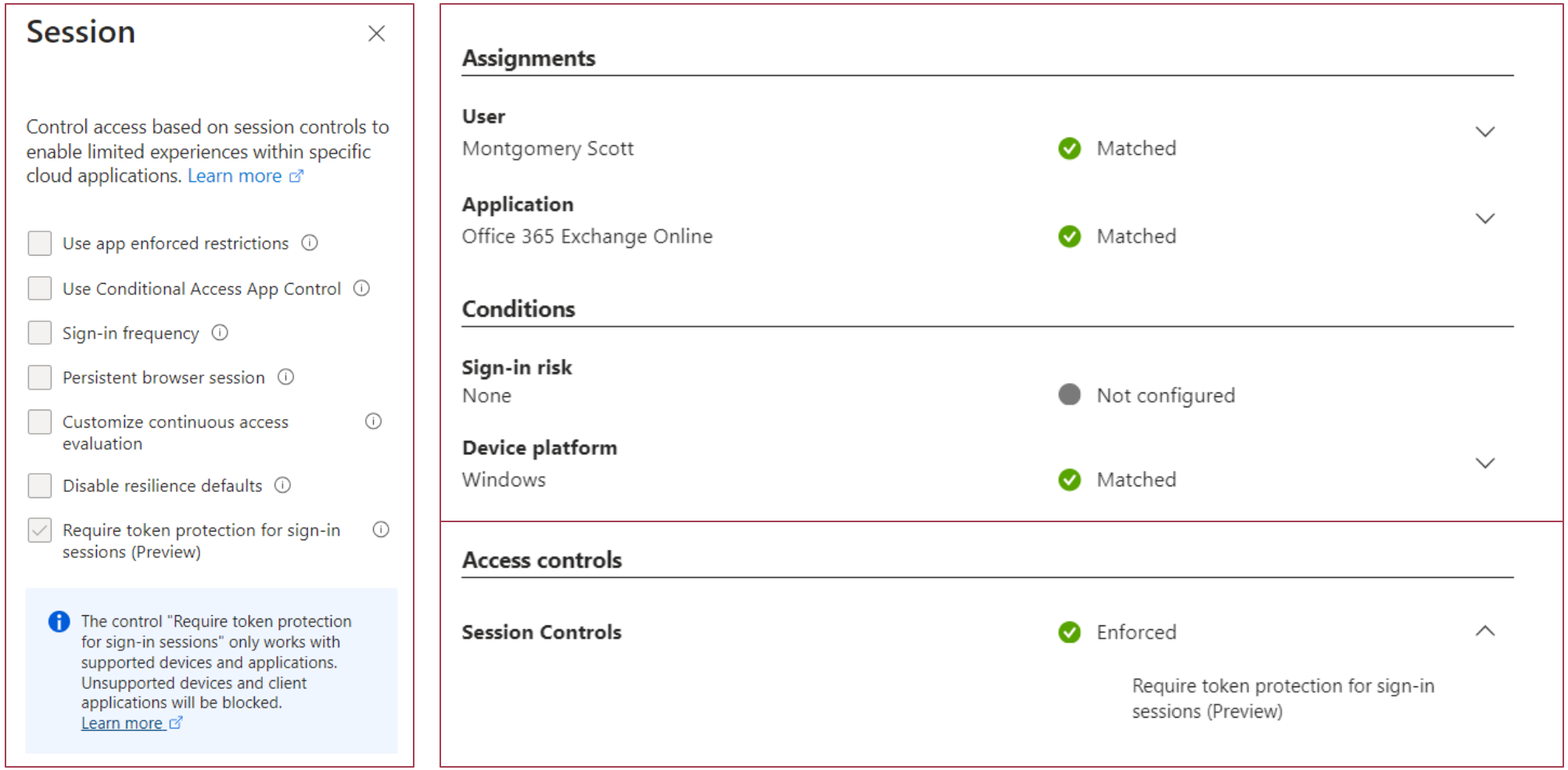


Token Binding (proof-of-possession)

Prevent token replay by enforcing cryptographically secure tie between the token and the device



Token Protection Enforced for Outlook/ExO



Blocked Token acquisition

Activity Details: Sign-ins

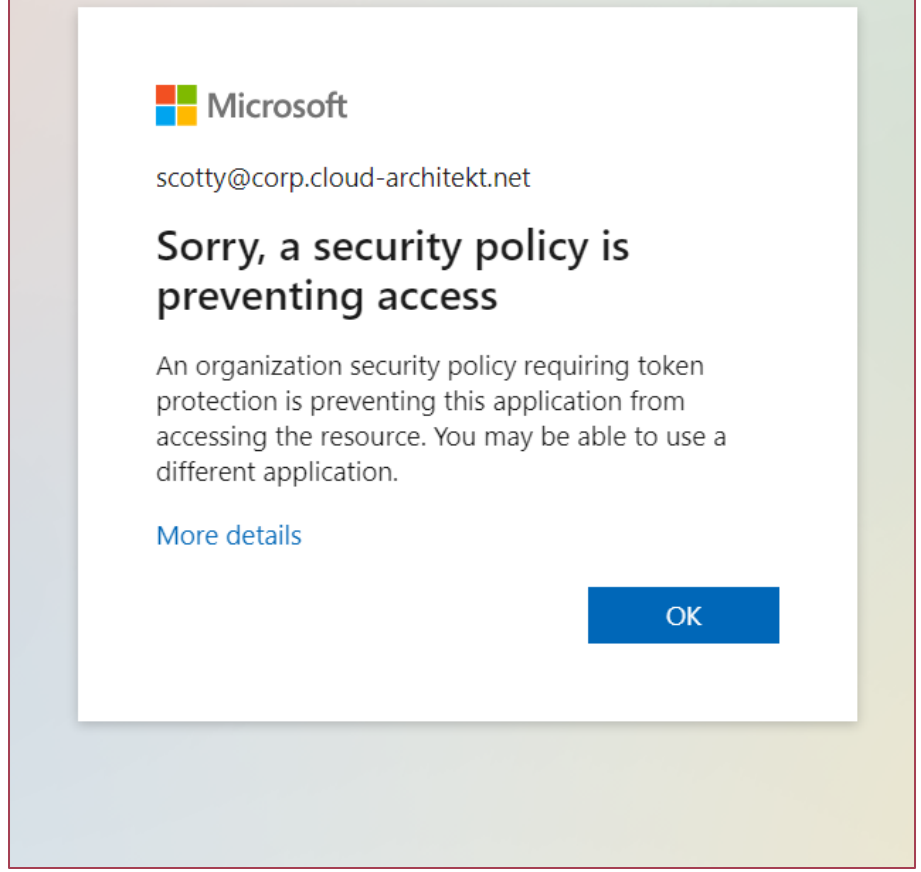
Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Date	8/5/2024, 9:06:46 PM
Request ID	7ccd491d-7526-4642-85aa-0df14e6b0200
Correlation ID	c8f8ec7f-fd9f-41fc-a987-62ba6ccdc331
Authentication requirement	Multifactor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	53003
Failure reason	Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.

Access controls

Session Controls — Not satisfied

Require token protection for sign-in sessions (Preview)



Device Bound Session Credentials (DBSC) in Chrome

Device Bound Session Credentials (DBSC) is a new web capability designed to protect user sessions from cookie theft and session hijacking. This feature is now available for testing as an Origin Trial in Chrome 135.

How it works

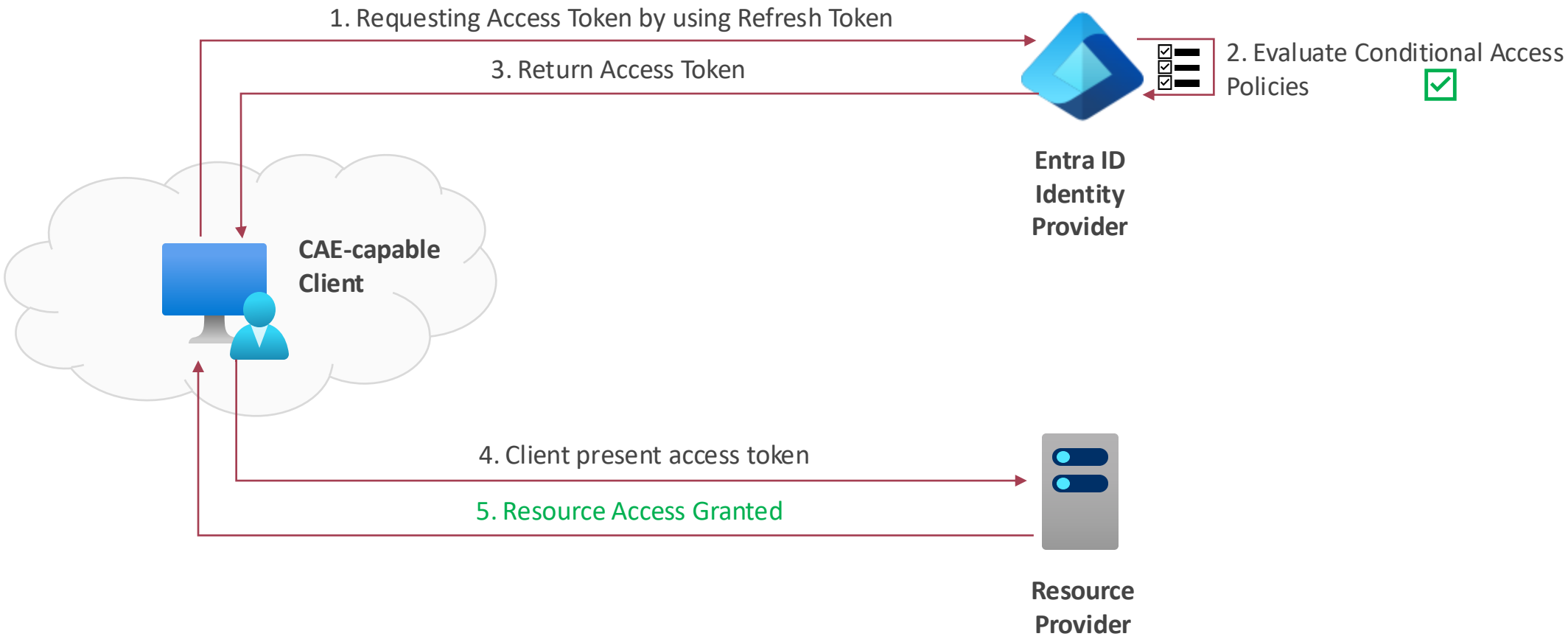
DBSC introduces a new API that allows servers to create an authenticated session that is bound to a device. When a session is initiated, the browser generates a public-private key pair, storing the private key securely using hardware-backed storage such as a Trusted Platform Module (TPM) when available.

The browser then issues a regular session cookie. During the session lifetime, the browser periodically proves possession of the private key and refreshes the session cookie. The cookie's lifetime can be set short enough so that stealing the cookie won't be a benefit for attackers.

Source: Chrome for Developers | Origin trial: Device Bound Session Credentials in Chrome

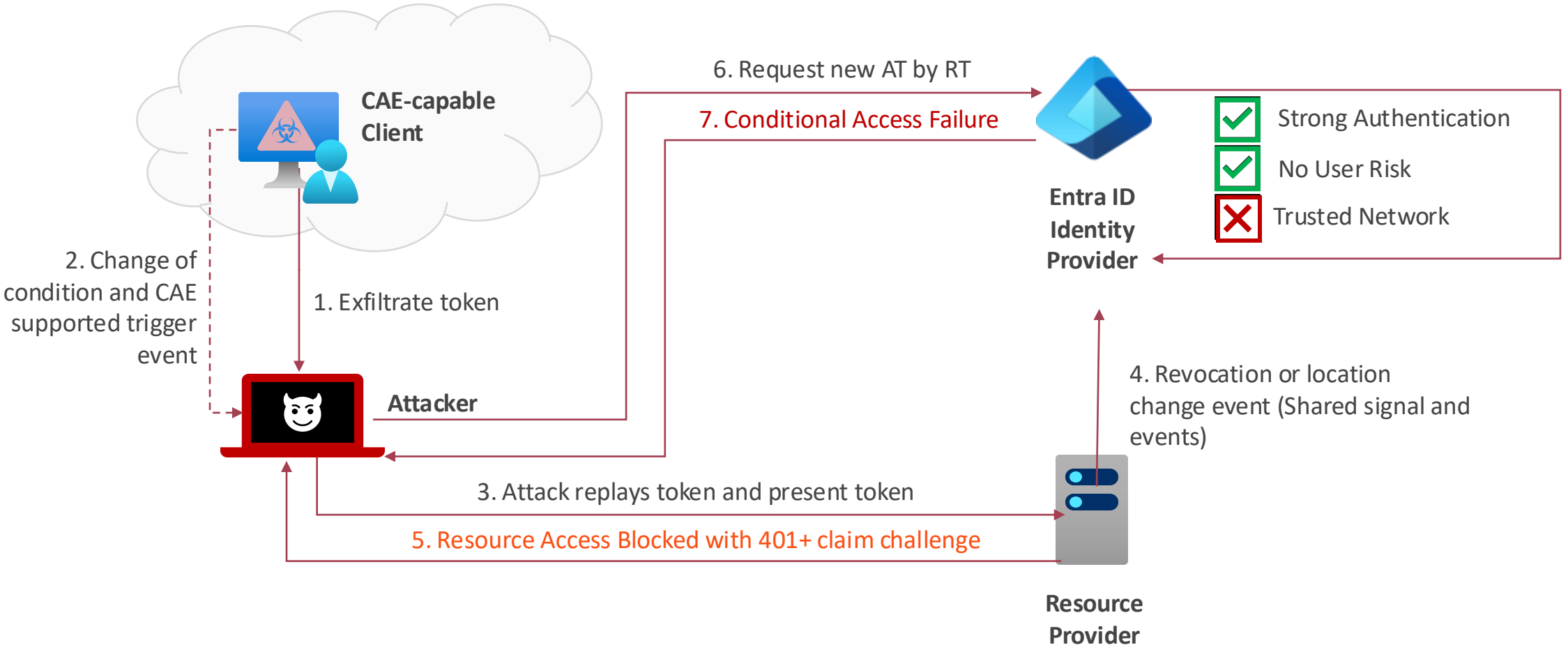
Continuous Access Evaluation (CAE)

Enforce re-evaluation of Conditional Access in response to policy violations or security issues



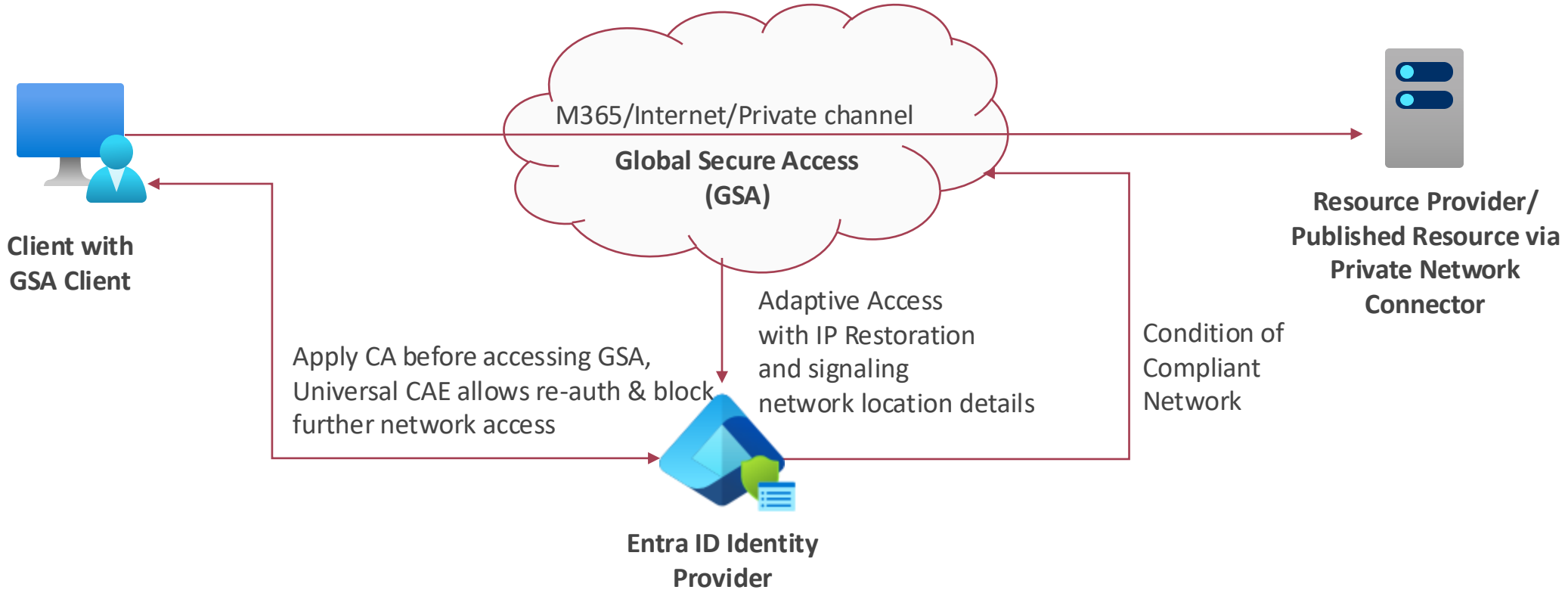
Continuous Access Evaluation (CAE)

Enforce re-evaluation of Conditional Access in response to policy violations or security issues



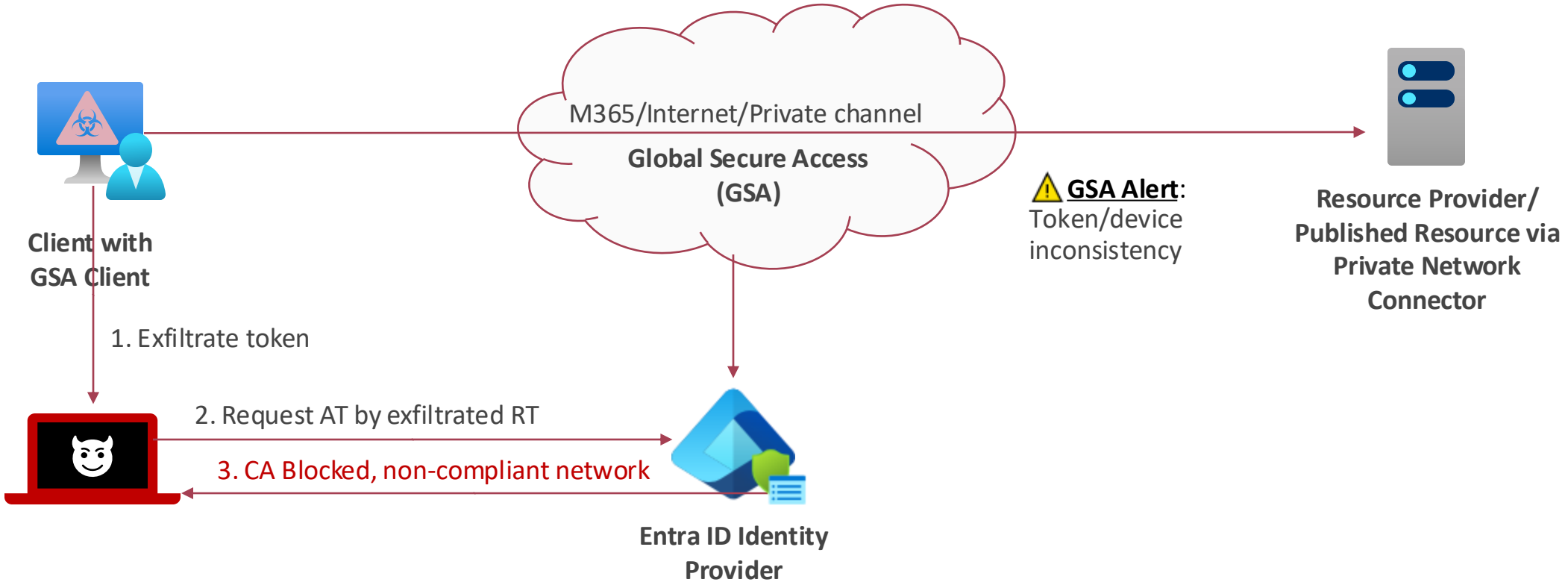
Compliant Network with Global Secure Access

Provide network condition with identity-awareness in Conditional Access

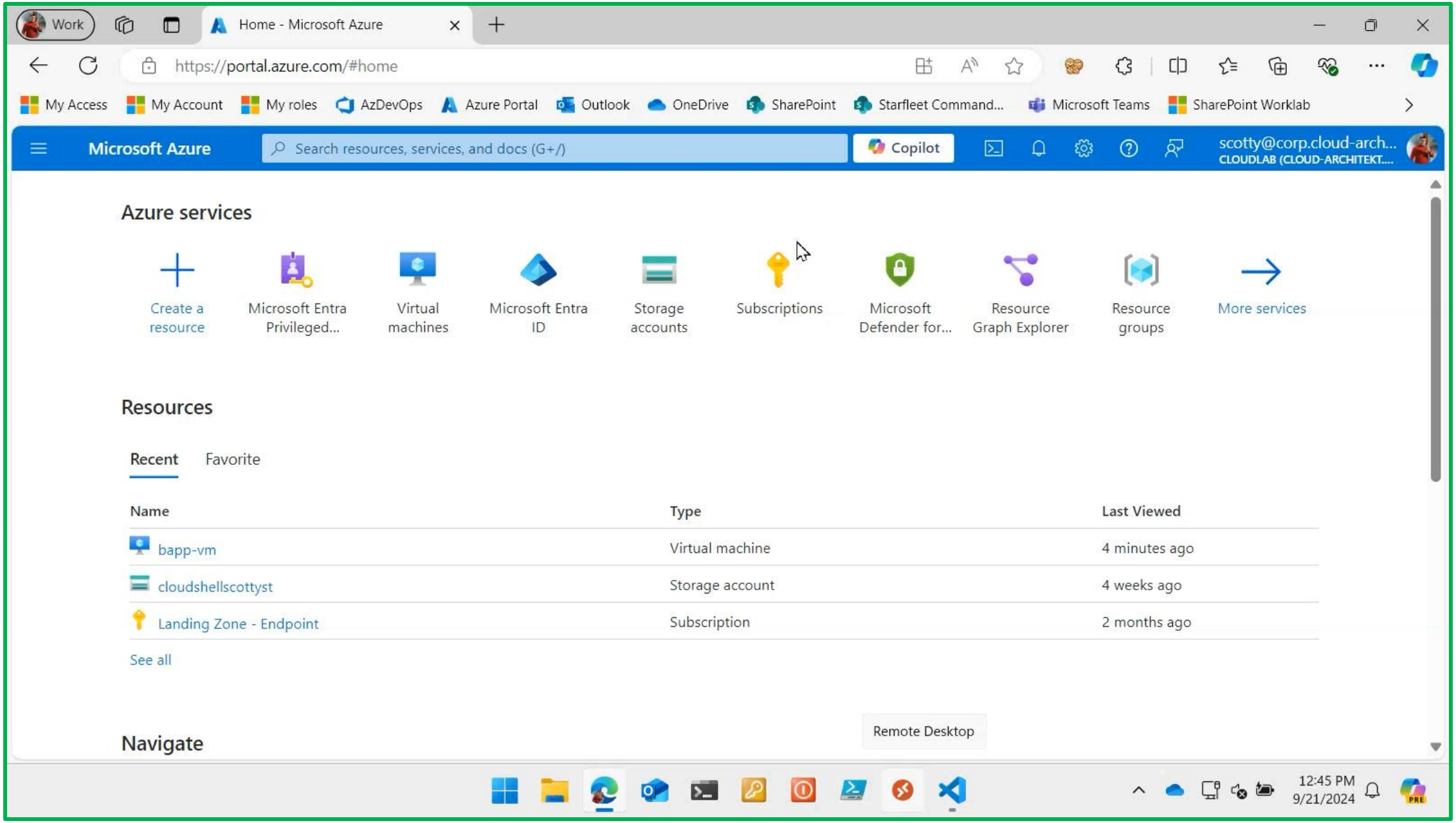


Compliant Network with Global Secure Access

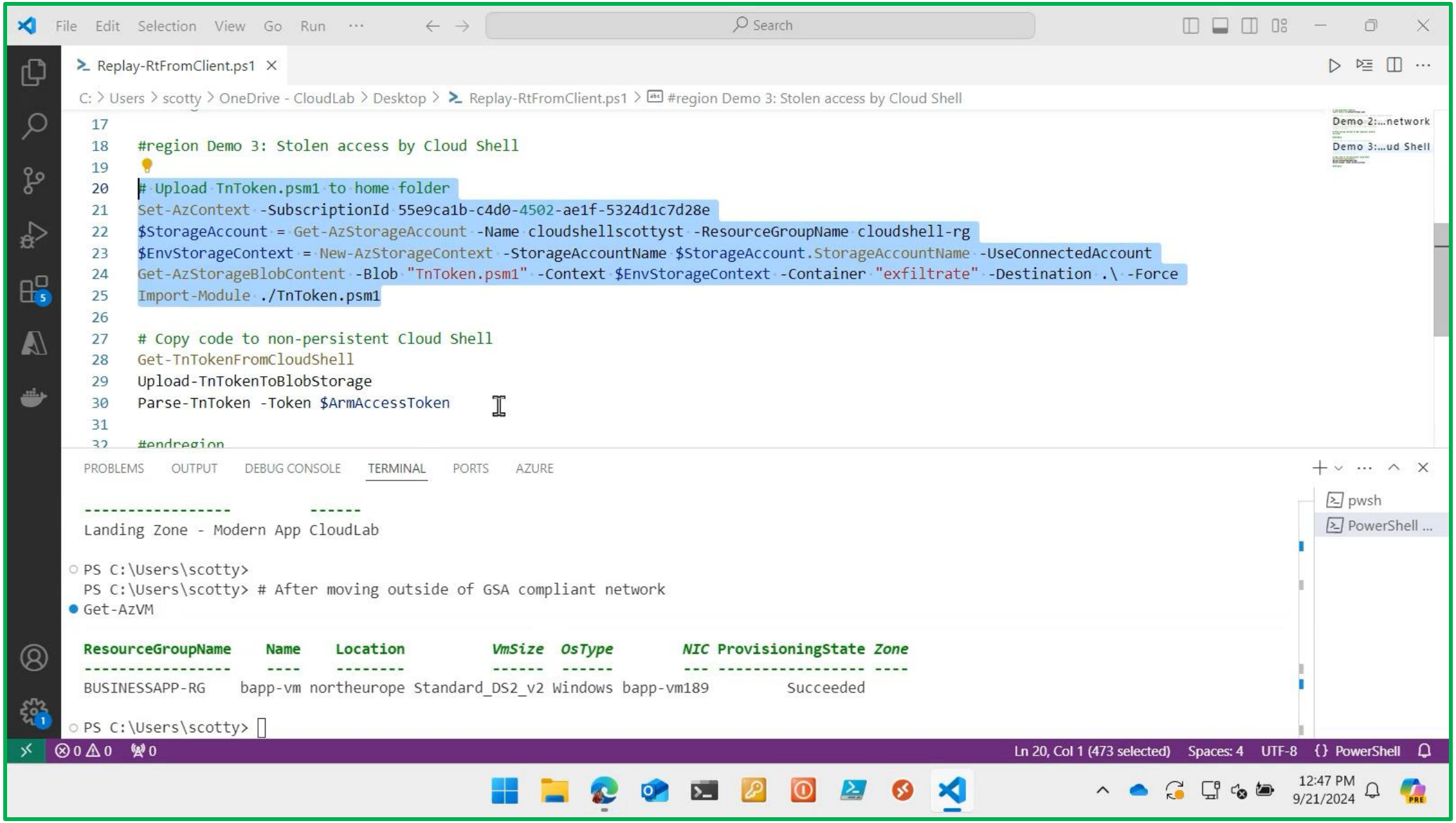
Provide network condition with identity-awareness in Conditional Access



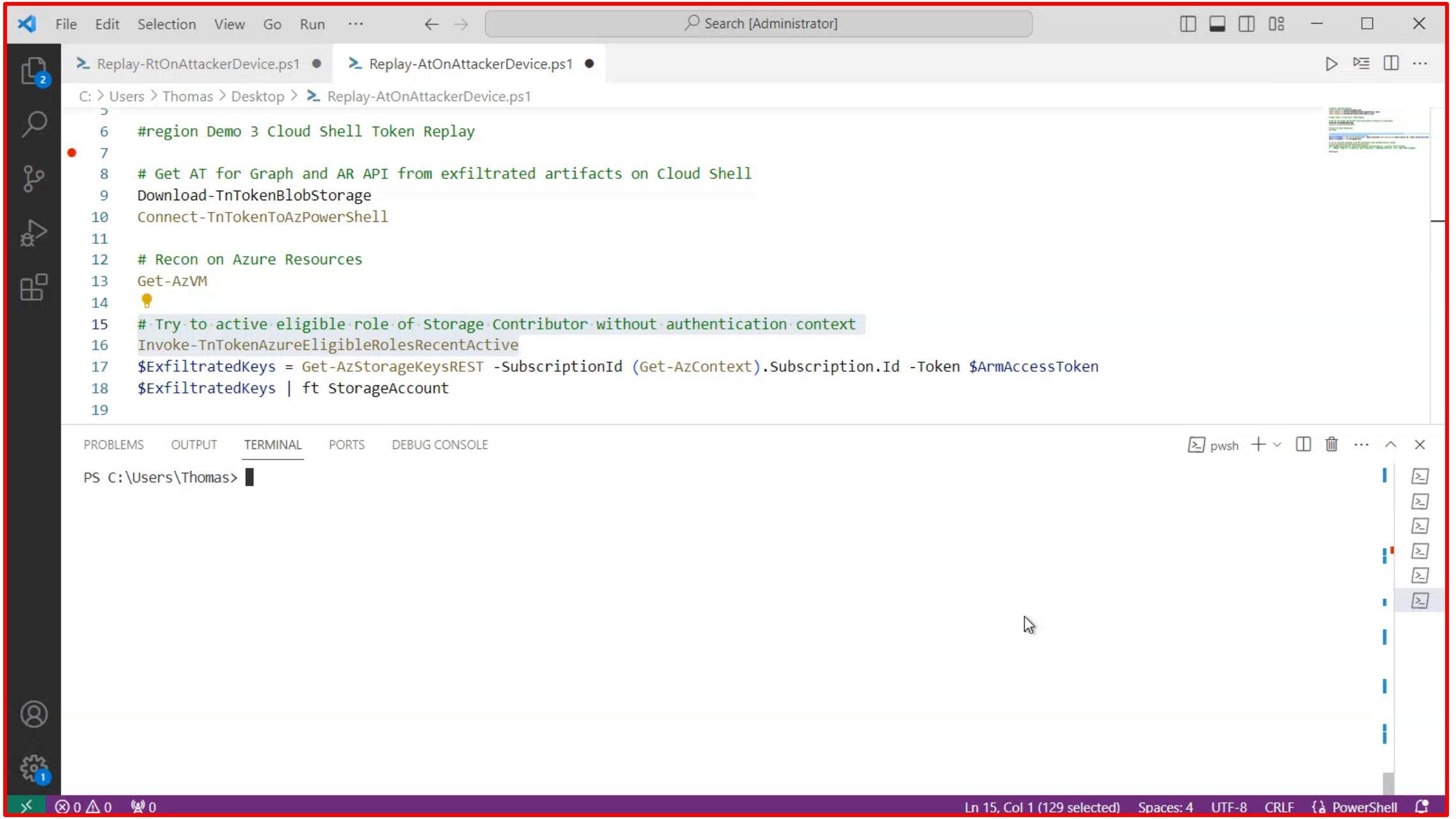
VICTIM DEVICE | AZURE CLOUD SHELL ON WINDOWS 11 ENTERPRISE DEVICE (CONNECTED TO GLOBAL SECURE ACCESS)



VICTIM DEVICE | AZURE CLOUD SHELL ON WINDOWS 11 ENTERPRISE DEVICE (CONNECTED TO GLOBAL SECURE ACCESS)

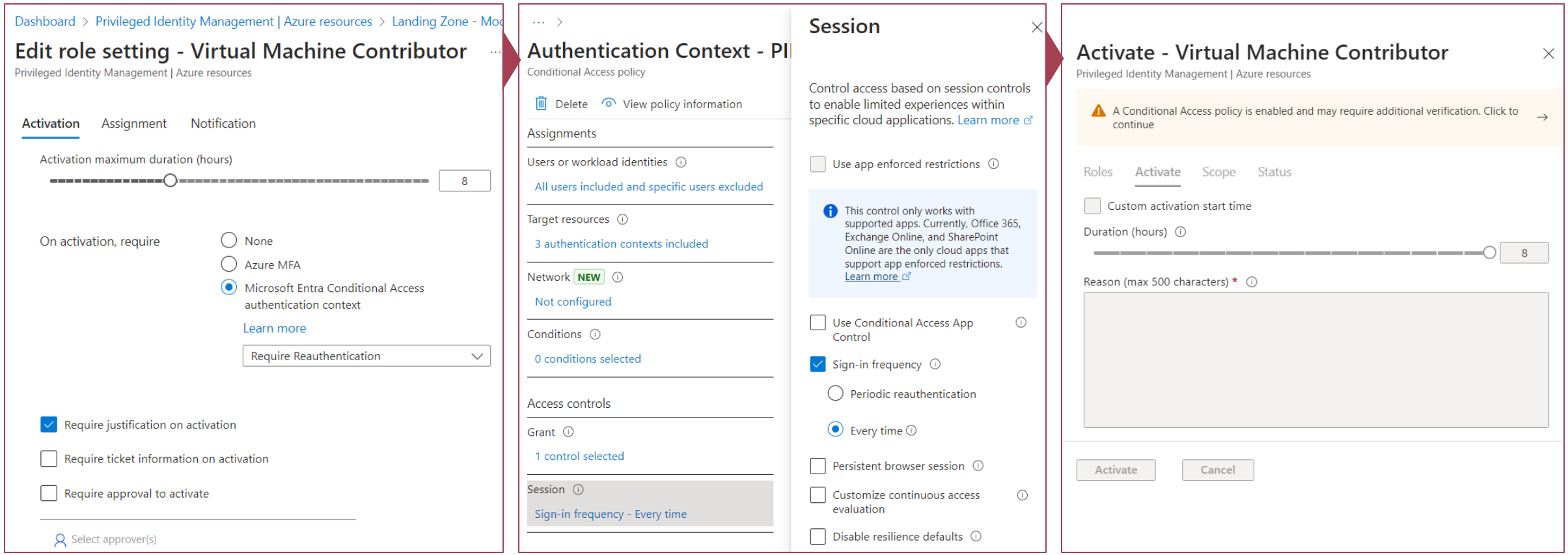


ATTACKER DEVICE | REPLAY ACCESS TOKEN (FROM AZURE CLOUD SHELL)



Authentication Context

Step-up authentication or enforce re-authentication on sensitive actions



Comparison of mitigation options

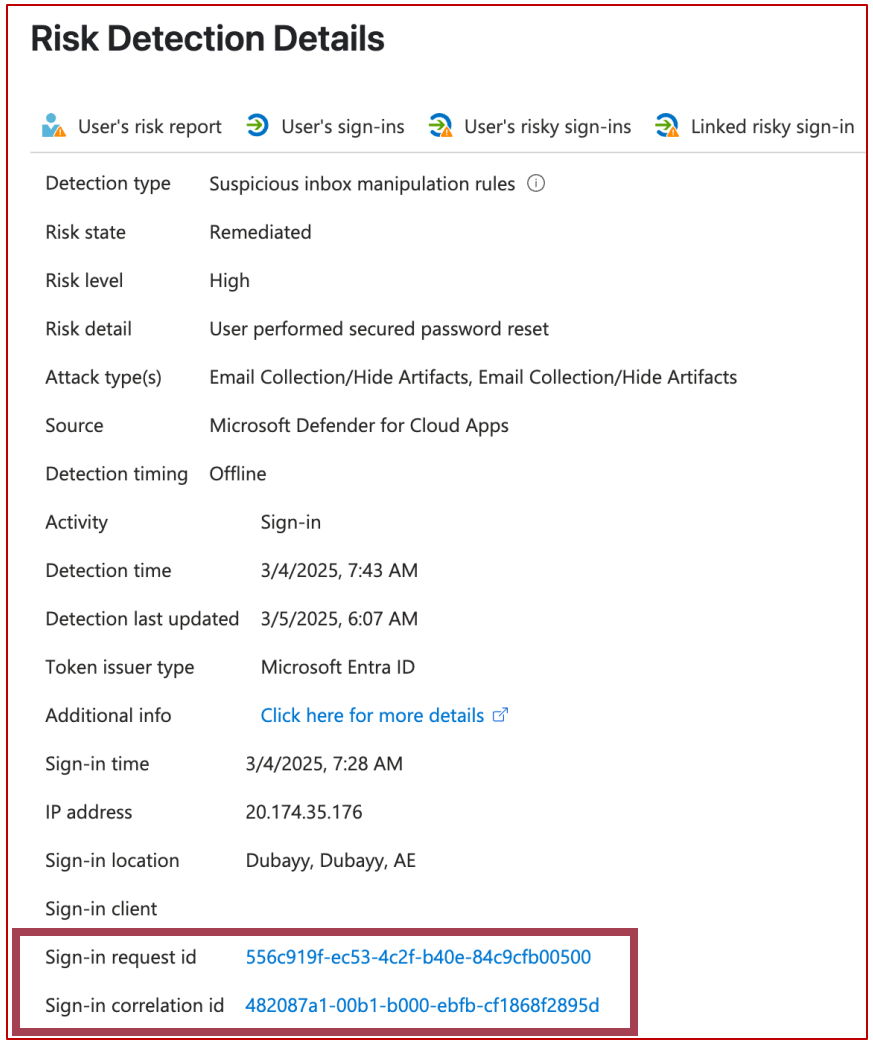
	Device Compliance + Block Device Code	Token Protection	Compliant Network + Universal CAE	Continuous Access Evaluation	Authentication Context
Device Platform	All	Windows	Windows	All	All
Client Type	All	Desktop apps	All	Supported Client apps	Supported apps to handle claim challenge
Client Apps/ Resource Provider	All	Exchange Online, SharePoint Online **Windows App (AVD, W365)**	All, Private Access not supported (GSA)	Supported RP	Need implementation of Auth Context
Protection Level	**Enforces to use PRT** to satisfy Device Identity and blocks **„phishing“ PRT** by Device Code Flow	Enforces to use Token Broker and binding session key from (hardware) cryptographic provider on **RT**	**Blocks to use RT** to gain/renew AT **outside of network**, CAE trigger to block GSA access	Trigger allows to enforce user to re-evaluate Conditional Access for issued **AT**	Enforce CA policy (e.g., re-authenticate user) on sensitive actions or requests for **AT**
Requirements	Microsoft Intune	Device Registration, Hybrid Joined- or Entra-Joined Device, P2 License	Global Secure Access, GSA Client >v1.8.239.0	Support of client and resource provider by implementing MSAL	Implementation on client-side and resource provider

DETECTION AND HUNTING OF TOKEN REPLAY/THEFT

Richness of token details in sign-in logs

TimeGenerated [UTC]	SessionId	IncomingTokenType	TokenProtection...	AppDisplayName	ResourceDisplayName	ClientAppUsed
3/8/2025, 1:41:55.676 PM	001eb379-5b08...	primaryRefreshToken	bound	Windows Sign In	Windows Azure Active Directory	Mobile Apps and Desktop
3/8/2025, 1:41:55.692 PM	001eb379-5b08...	refreshToken	bound	Microsoft Application Comman...	Microsoft Device Directory Serv...	Mobile Apps and Desktop
3/8/2025, 1:41:56.608 PM	001eb379-5b08...	primaryRefreshToken	bound	Microsoft Authentication Broker	Microsoft Graph	Mobile Apps and Desktop
3/8/2025, 1:42:06.291 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	IrisSelectionFrontDoor	Browser
3/8/2025, 1:42:06.613 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	Microsoft Graph	Browser
3/8/2025, 1:42:07.830 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	Marketplace Extensions Runtime	Browser
3/8/2025, 1:42:10.192 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	Marketplace Extensions Runtime	Browser
3/8/2025, 1:42:15.205 PM	001eb379-5b08...	primaryRefreshToken	bound	Microsoft Teams	Skype Presence Service	Mobile Apps and Desktop
3/8/2025, 1:42:16.049 PM	001eb379-5b08...	primaryRefreshToken	bound	Microsoft Teams	Office 365 SharePoint Online	Mobile Apps and Desktop
3/8/2025, 1:42:26.497 PM	001eb379-5b08...	primaryRefreshToken	bound	Microsoft Edge	Edge Sync	Mobile Apps and Desktop
3/8/2025, 1:42:28.614 PM	001eb379-5b08...	primaryRefreshToken	bound	Microsoft Teams	IC3 Gateway	Mobile Apps and Desktop
3/8/2025, 1:42:33.741 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	Office 365 Exchange Online	Browser
3/8/2025, 1:42:34.200 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	Office 365 Exchange Online	Browser
3/8/2025, 1:42:38.264 PM	001eb379-5b08...	primaryRefreshToken	bound	Windows Insider Program	Windows Azure Active Directory	Mobile Apps and Desktop
3/8/2025, 1:42:38.809 PM	001eb379-5b08...	none	unbound	Microsoft Teams Services	Microsoft 365 App Catalog Ser...	Browser
3/8/2025, 1:42:40.788 PM	001eb379-5b08...	primaryRefreshToken	bound	Microsoft Teams	Microsoft Teams Services	Mobile Apps and Desktop
3/8/2025, 1:42:43.226 PM	001eb379-5b08...	primaryRefreshToken	bound	ZTNA Network Access Client -- ...	Privileged Quick Access	Mobile Apps and Desktop

Signals in Microsoft Entra ID Protection



Source: Detecting token theft in real-time and post-breach

Risk Detections:

- Anomalous token (offline detection)
- Attempted access of PRT (by MDE)
- Unfamiliar sign-in properties
- Unfamiliar sign-in
- Post-Authentication activity from MDA

Automated Response:

Risk-based CA policies to enforce re-authentication of affected users, Trigger for CAE

Signals in Microsoft Entra ID Protection

Token theft related detections

With a recent update to our detection architecture, we no longer autoremediate sessions with MFA claims when a token theft related or the Microsoft Threat Intelligence Center (MSTIC) Nation State IP detection triggers during sign-in.

The following ID Protection detections that identify suspicious token activity or the MSTIC Nation State IP detection are no longer auto-remediated:

- Microsoft Entra threat intelligence
- Anomalous token
- Attacker in the Middle
- MSTIC Nation State IP
- Token issuer anomaly

Resolve RequestId to Session ID

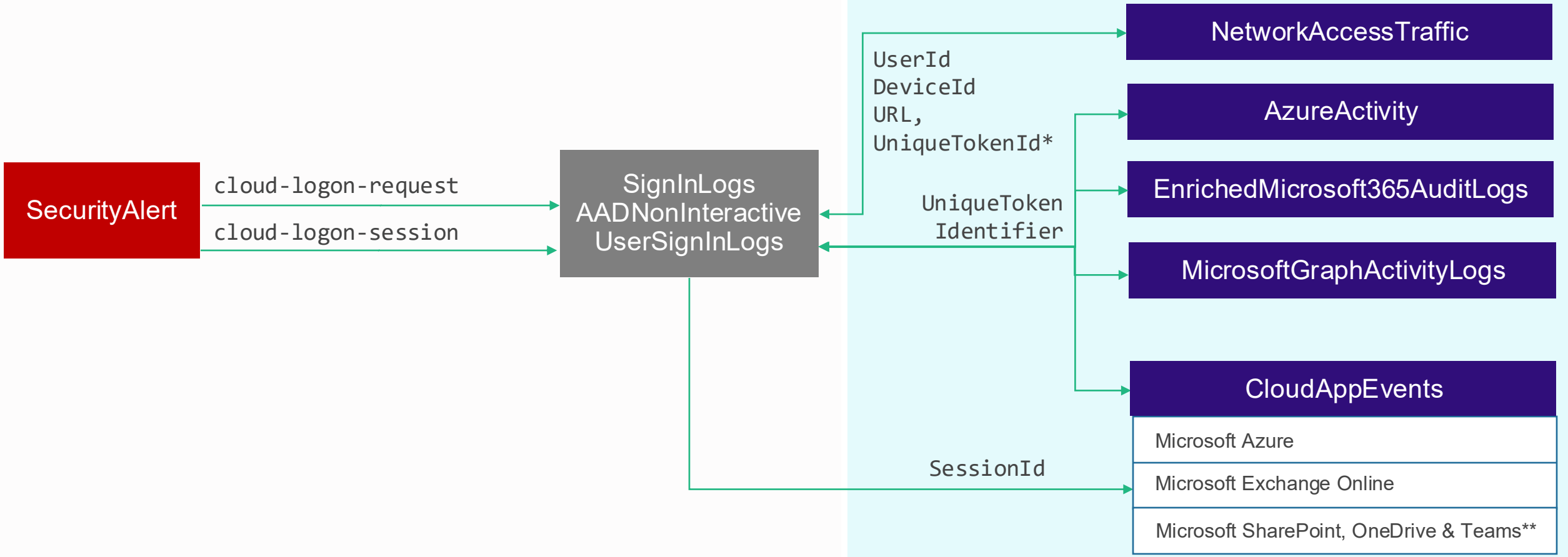
```
union SigninLogs, AADNonInteractiveUserSignInLogs
| where TimeGenerated >ago(365d)
| where SessionId == "002e6ae9-7103-62ef-69ef-abbf8777c103"
| project CreatedDateTime, SessionId, AppDisplayName, ResourceDisplayName, OriginalRequestId, ResultType, ResultDescription, UniqueTokenIdentifier
```

CreatedDateTim...	SessionId	AppDisplayName	ResourceDisplayName	OriginalRequestId	Result...	UniqueTokenIdentifier
3/4/2025, 6:25:28....	002e6ae9-7103-6...	OfficeHome	OfficeHome	fc4ca712-5b6c-4564...	0	EqdM_GxbZEWP5JHx7-0FAA
3/4/2025, 6:25:29....	002e6ae9-7103-6...	OfficeHome	OfficeHome	f2a40bf0-e0ab-4cce...	0	8Auk8qvgzkyazXb6_moGAA
3/4/2025, 6:25:29....	002e6ae9-7103-6...	OfficeHome	O365 Suite UX	0bfdd39b-6aca-4f60...	0	m9P9C8pqYE-heHw_cPcEAA
3/4/2025, 6:25:29....	002e6ae9-7103-6...	OfficeHome	Olympus	59e82d86-cfe8-491...	0	hi3oWejPF0mtUnvitpY8AA
3/4/2025, 6:25:30....	002e6ae9-7103-6...	Olympus	OCaaS Client Interaction Service	00a4b17a-6978-45e...	0	erGkAHhp5UWtvf8a7zoHAA
3/4/2025, 6:25:36....	002e6ae9-7103-6...	OfficeHome	OfficeHome	aea775af-3889-4957...	0	r3Wnrok4V0mylbl4cElGAA
3/4/2025, 6:25:38....	002e6ae9-7103-6...	OfficeHome	Microsoft 365 App Catalog Ser...	f4dd18f4-2925-4bfe...	0	9Bjd9CUp_kuHMB0D6iAHAA
3/4/2025, 6:28:22....	002e6ae9-7103-6...	SharePoint Online Web Client E...	OCaaS Client Interaction Service	b8a418a2-f857-4e8...	0	ohikuFf4jU6GyhSDvtYGAA
3/4/2025, 6:28:23....	002e6ae9-7103-6...	SharePoint Online Web Client E...	OCaaS Client Interaction Service	610a1f42-d3c2-418f...	0	Qh8KYcLTj0GMLUVrwp4GAA
3/4/2025, 6:28:24....	002e6ae9-7103-6...	Office365 Shell WCSS-Client	Office365 Shell WCSS-Server	70bfa5ec-05eb-4b1...	0	7KW_cOsFE0uXAQv3Kz8_AA
3/4/2025, 6:28:25....	002e6ae9-7103-6...	Office365 Shell WCSS-Client	Microsoft Graph	71cab544-1e92-4e8...	0	RLXKcZIejE6v9cJP-rsFAA
3/4/2025, 6:28:46....	002e6ae9-7103-6...	Office 365 SharePoint Online	Media Analysis and Transforma...	556c919f-ec53-4c2f-...	0	n5FsVVPsL0y0DoTJz7AFAA

Sign-in, alert and activity log mapping

Correlation XDR/SIEM Incident to suspicious sign-in

Correlation of token/session to activity



* limited to traffic for Entra ID token endpoint

** limited to specific ActionTypes of M365 workloads

Sign-in, alert and activity log mapping

```
98      // sensitive Operations outside of GSA
99      | where OutsideOfGsa == true
100     | mv-expand parse_json(Operations) | where Operations.IsSensitive == "true" | project-reorder Operations
101     | project Operations.TimeGenerated, OutsideOfGsa, IsTokenCAE, AppDisplayName, Operations.OperationNameValue, IsSensitive = Operations.IsSensitive, GsaCaStatus,
    SignInIpAddress, ActivityIpAddress
102     | sort by tostring(Operations_TimeGenerated)
```

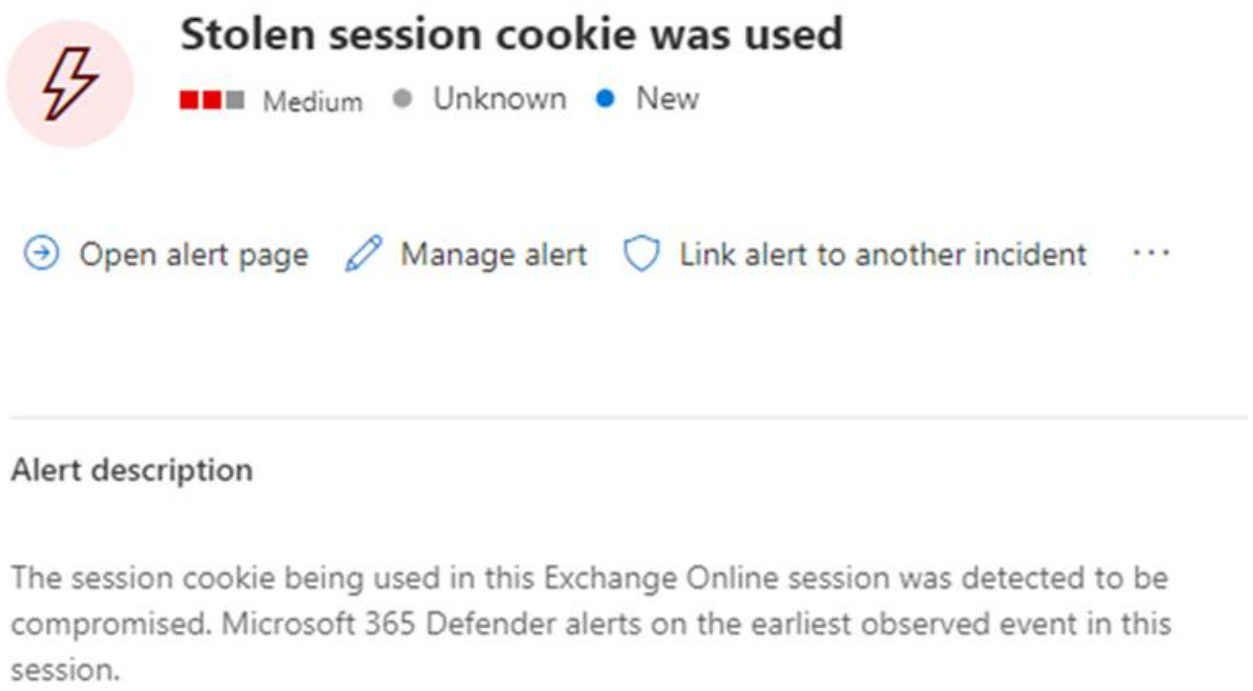
Results | Chart | Add bookmark

Operations_TimeGenerated	OutsideOfGsa	IsTokenCAE	AppDisplayName	Operations_OperationNameValue	IsSensitive	GsaCaStatus	SignInIp...	Act
2024-09-21T11:25:19.0180000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5
2024-09-21T11:25:15.0950000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5
2024-09-21T11:24:52.7260000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:52.5070000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:52.4120000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:52.1780000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:52.1240000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:51.8900000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:51.8110000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:51.5610000Z	true	False	AzurePortal Console App	Microsoft.Storage/storageAccounts/listKeys/action	true	notApplied	93.236.130.38	5
2024-09-21T11:24:45.8760000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5
2024-09-21T11:24:33.4380000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5
2024-09-21T11:17:09.1900000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5
2024-09-21T11:17:04.5970000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5
2024-09-21T11:03:14.3910000Z	true	False	AzurePortal Console App	Microsoft.Authorization/roleAssignmentScheduleRequests/write	true	notApplied	93.236.130.38	5

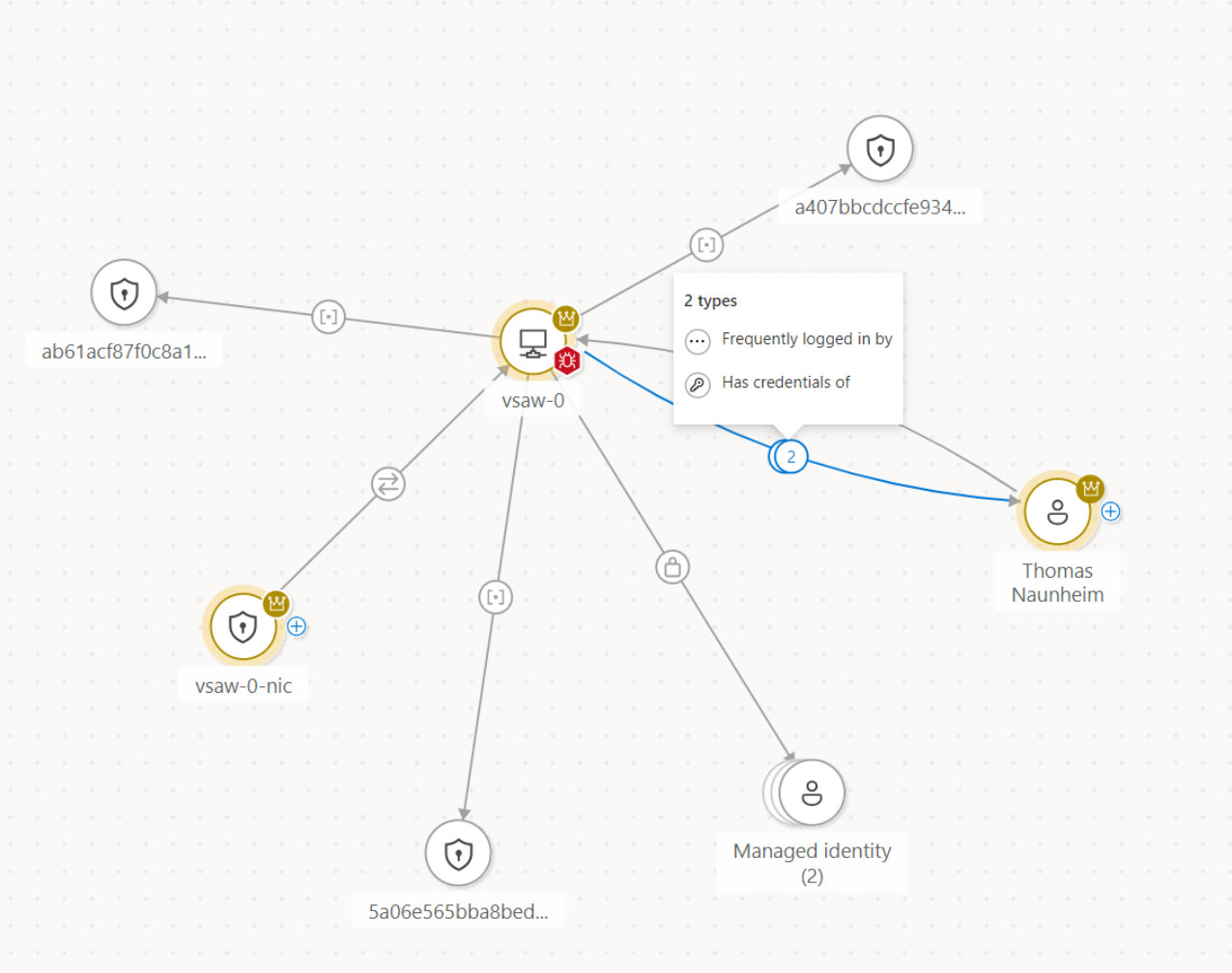
7s 771ms | Display time (UTC+00:00) | Query details | 1 - 15 of 16

... but hey... what about session cookies?

Session cookie theft detection by XDR

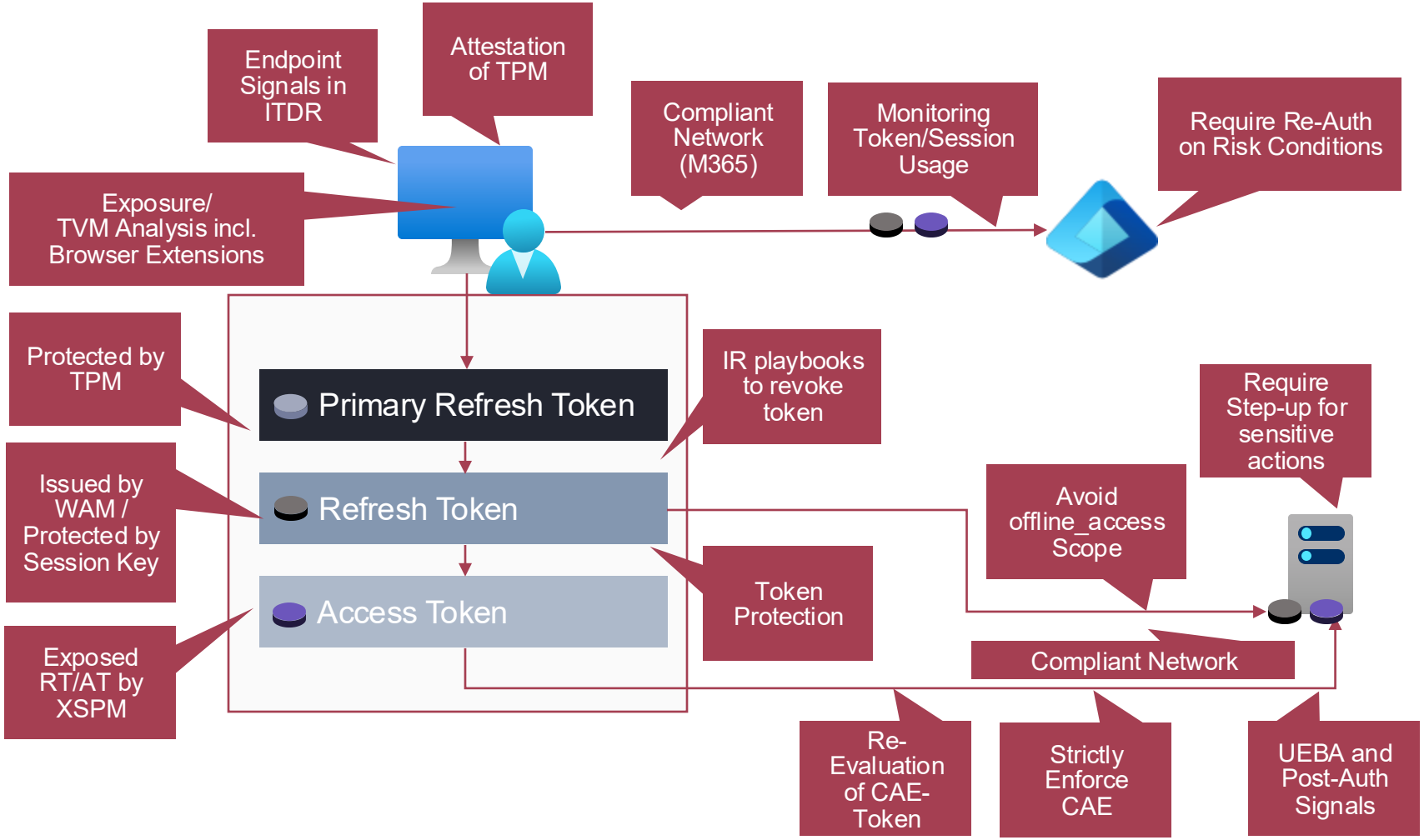


Smart Analysis of Browser Artifacts



SourceNodeName	vsaw-0
SourceNodeLabel	microsoft.compute/virtualmachines
EdgeLabel	has credentials of
browserCookies	{"type":"BrowserCookies","browserCookies":true}
primaryRefreshToken	{"type":"PrimaryRefreshToken","primaryRefreshToken":true}
cloudCliTool	{"type":"CloudCliTool","cloudCliTool":true}

Overview of detection and mitigation



SwissMicrosoft
SECURITY SUMMIT

THANK YOU

www.cloud-architekt.net