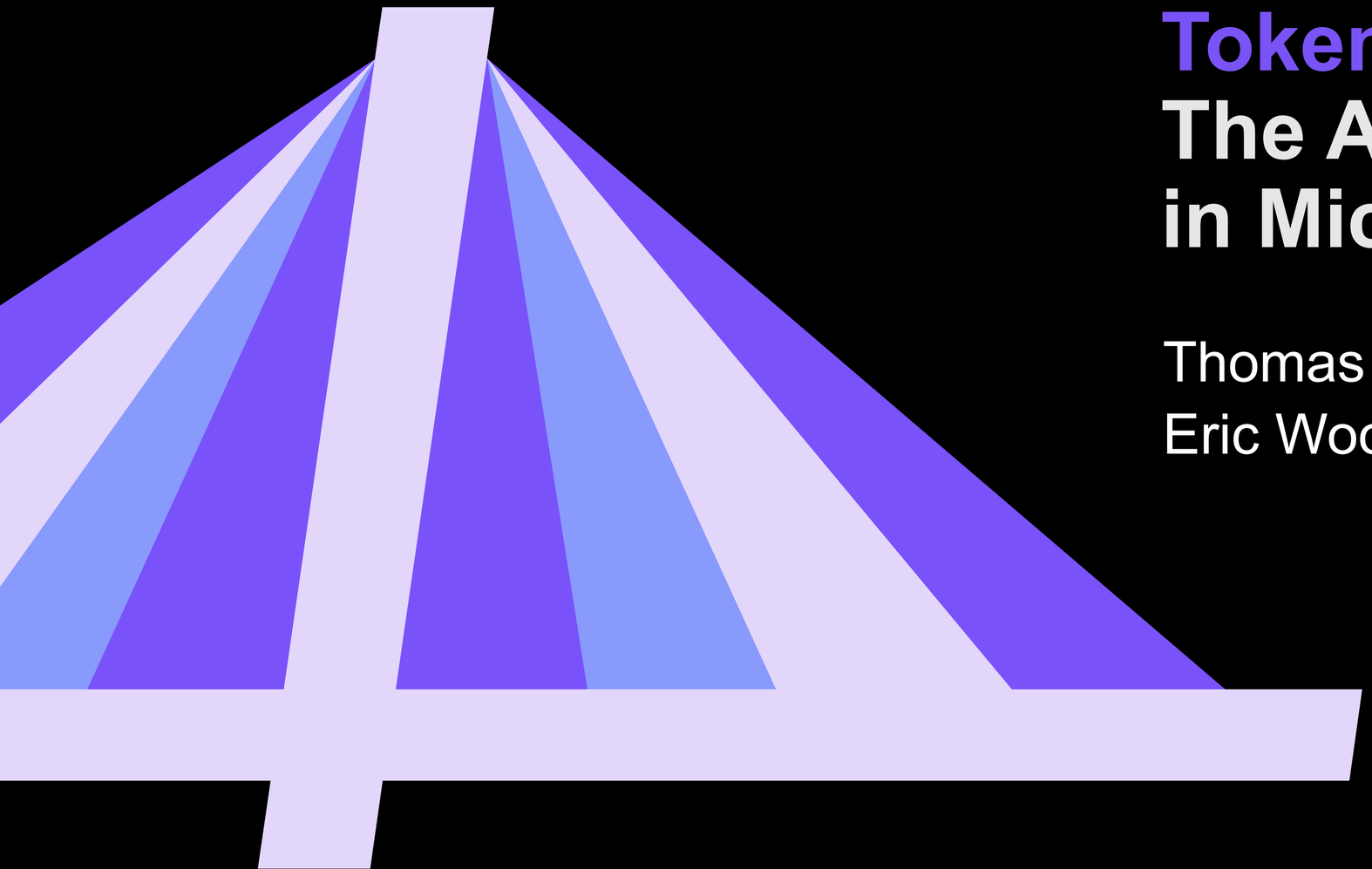
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



Password Sprays & Token Plays: The Art of Staying Secure in Microsoft Entra

Thomas Naunheim
Eric Woodruff

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Thomas Naunheim

Cyber Security Architect @glueckkanja AG

- From Koblenz/Lahnstein, Germany
- Microsoft MVP (Identity & Access, Cloud Security)

@naunheim.cloud

@Thomas_Live

/in/ThomasNaunheim

cloud-architekt.net

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Eric Woodruff

Chief Identity Architect @ Semperis

- From Schenectady, New York
- Microsoft MVP (Identity & Access)

@ericonidentity.com
@ericonidentity
/in/ericonidentity
@ericonidentity@infosec.exchange
ericonidentity.com

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Identity is (still) under attack…

600 million

identity attacks per day…

Microsoft Entra data, Microsoft Digital Defense Report 2024

99%

are password attacks.

Microsoft Entra data, Microsoft Digital Defense Report 2024

111%

increase in token replay attacks.

Microsoft Entra data, How to break the token theft cyber attack chain, 2024

146%

rise in AiTM phishing attacks.

Microsoft Entra data, Microsoft Digital Defense Report 2024

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Agenda

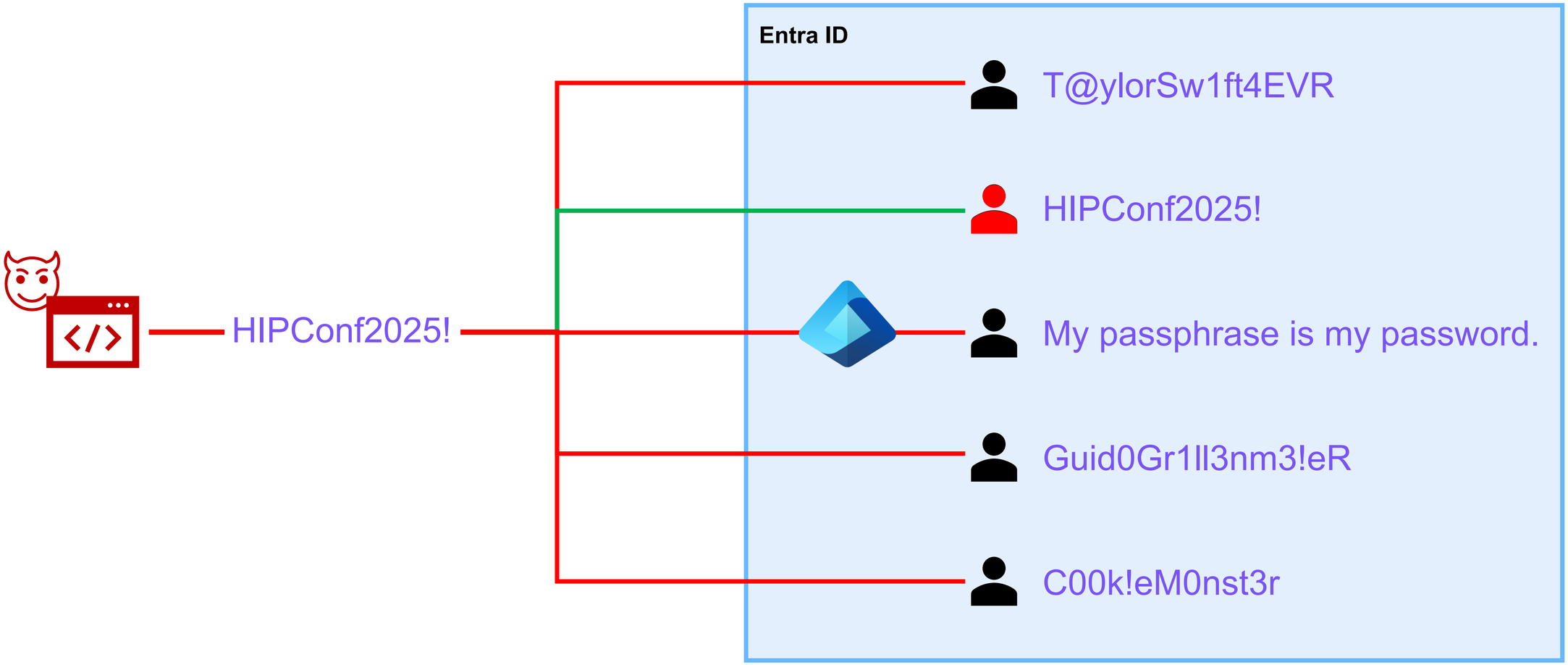
- Password-based attacks
- Token theft & replay
- Abusing privileges of OAuth2 applications
- Mitigation

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Password-based attacks

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Overview of password spray attacks



PowerShell

PS C:\Repo\Spray365>

Password spray attack

Search

9:20 AM
7/15/2025

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Always MFA? Find your single factor auth…

- Exclusion for (trusted) locations
- Service accounts and service principals
- SaaS applications
  - Local user accounts
  - Multiple identity providers

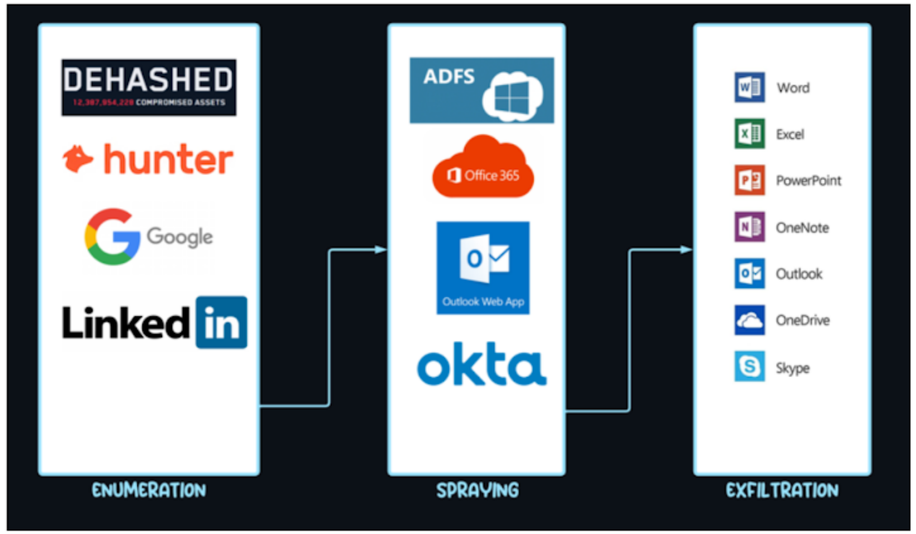
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Are password spray attacks still a risk?

Over 80,000 Microsoft Entra ID Accounts Targeted Using Open-Source TeamFiltration Tool

Jun 12, 2025 Ravie Lakshmanan

The UNK_SneakyStrike activity has been described as "large-scale user enumeration and password spraying attempts," with the unauthorized access efforts occurring in "highly concentrated bursts" targeting several users within a single cloud environment. This is followed by a lull that lasts for four to five days.



Source: HackerNews, Image Source: Proofpoint

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

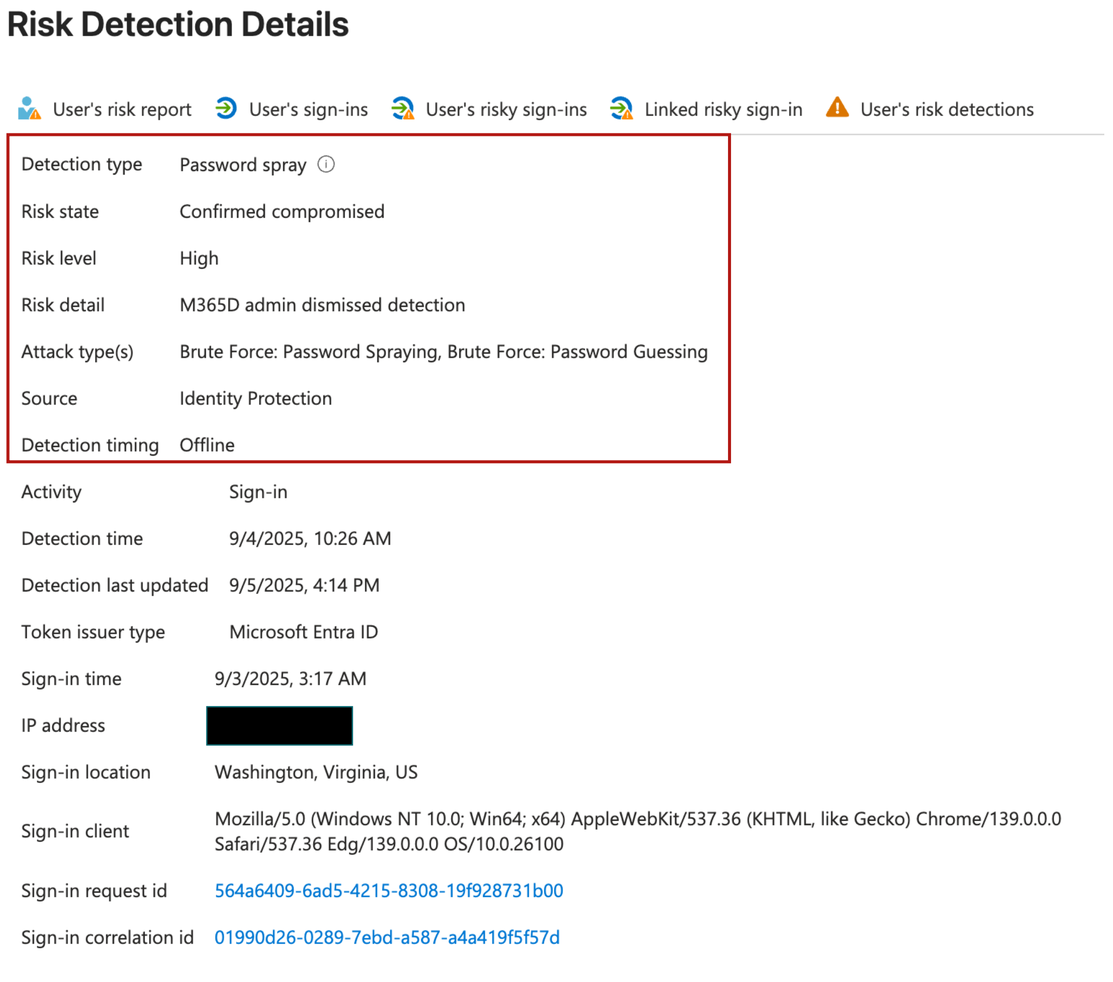
Password spray in Entra ID Protection

January 2025

General Availability - Real-time Password Spray Detection in Microsoft Entra ID Protection

A password spray attack is where multiple identities are attacked using common passwords in a unified brute force manner. The risk detection is triggered when an account's password is valid and has an attempted sign in. This detection signals that the user's password was correctly identified through a password spray attack, not that the attacker was able to access any resources.

- Calculated in real-time or offline
- License requirement: Microsoft Entra ID P2
- Tips for investigating password spray detections.

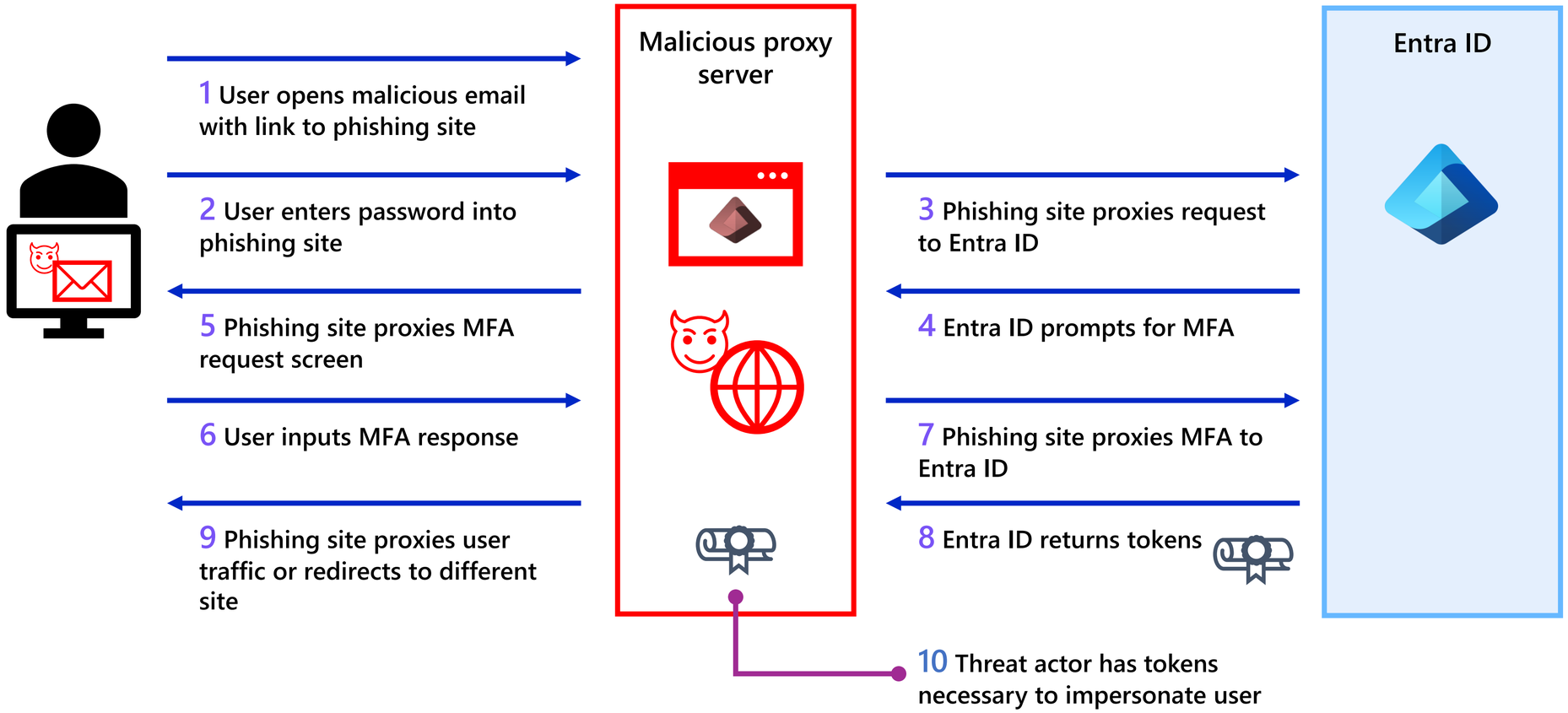


HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Token theft & replay

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Overview of attacker-in-the-middle (AiTM)



Attacker-in-the-middle (AiTM)

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AiTM attack disruption in Microsoft Defender XDR

High | Resolved | u101@a.alpineskihouse.co | BEC Fraud | Credential Phish | AiTM attack | Attack Disruption | AlpineSkiHouse | SAPClient

Attention! Attack disruption initiated multiple response actions. For more details, go to the Action center.

Attack story | Alerts (16) | Assets (5) | Investigations (0) | Evidence and Response (20) | Recommended actions (22) | Summary | Similar incidents (0)

Play attack story | Unpin all | Show all

Mar 10, 2025 2:28 PM Resolved
Risky sign-in after clicking a possible AiTM phishing URL
Cameron V

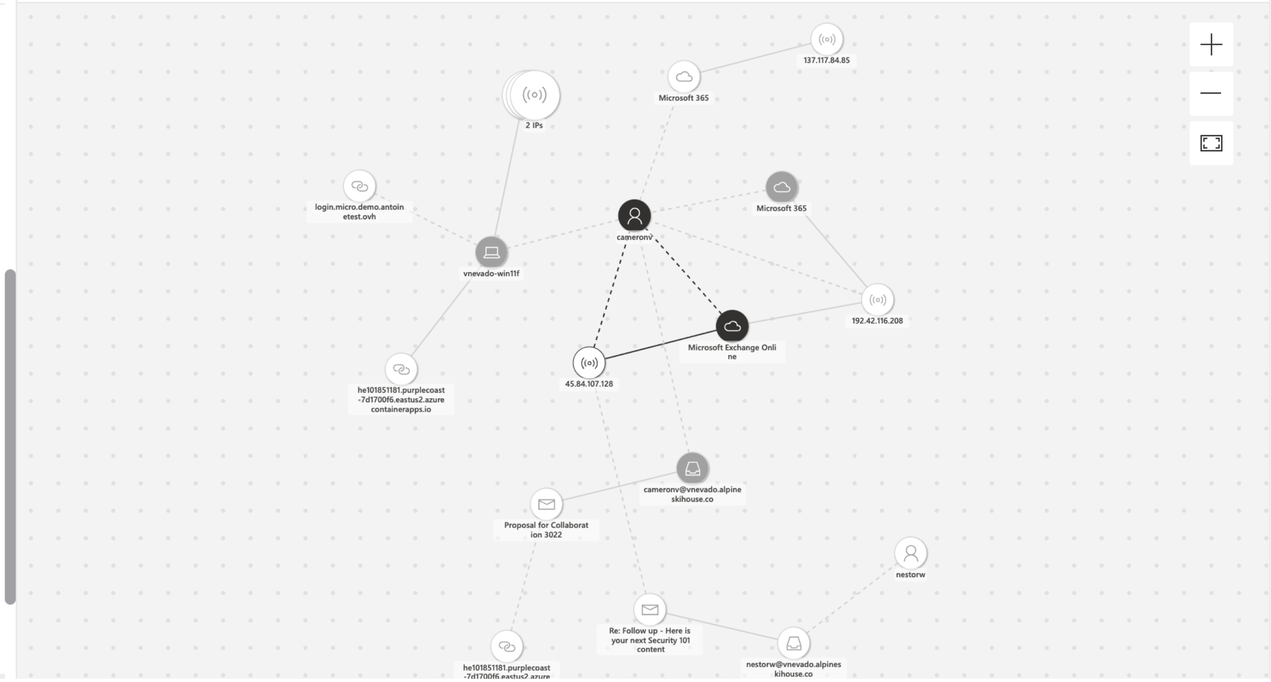
Mar 10, 2025 2:29 PM Resolved
Activity from a Tor IP address
Cameron V

Mar 10, 2025 2:29 PM Resolved
Compromised user account in a recognized attack pattern
Cameron V

Mar 10, 2025 2:31 PM Resolved
Suspicious Outlook rules
Cameron V

Mar 10, 2025 2:31 PM Resolved
BEC financial fraud
Cameron V

Incident graph | Layout | Group similar nodes



Attack disruption

Automated response took place.

Disruption incident summary and impact

Attacker leveraged 1 compromised accounts.

Accounts

Contained
1

View actions in action center

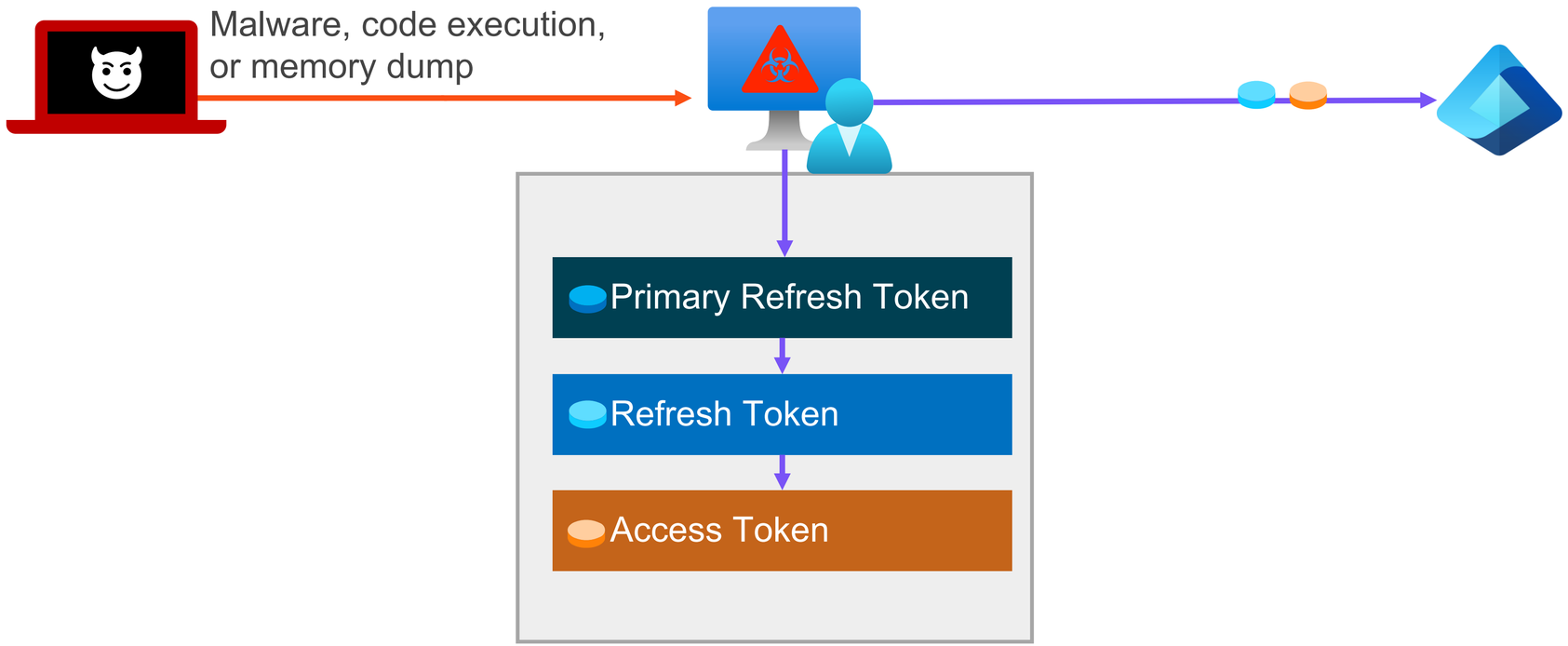
RECOMMENDATIONS

Phishing Incident response playbook

View phishing investigation and response recommended steps for this incident

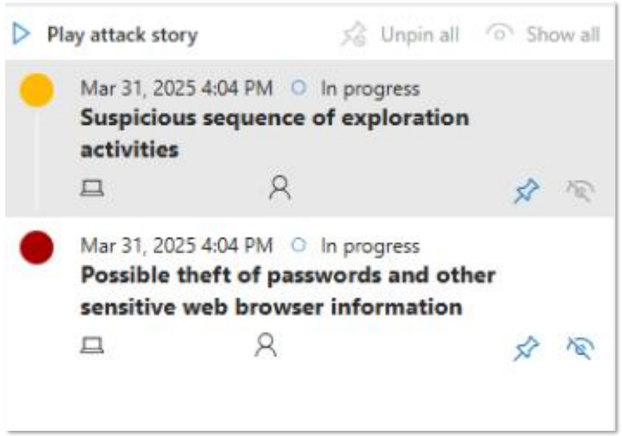
Open phishing playbook

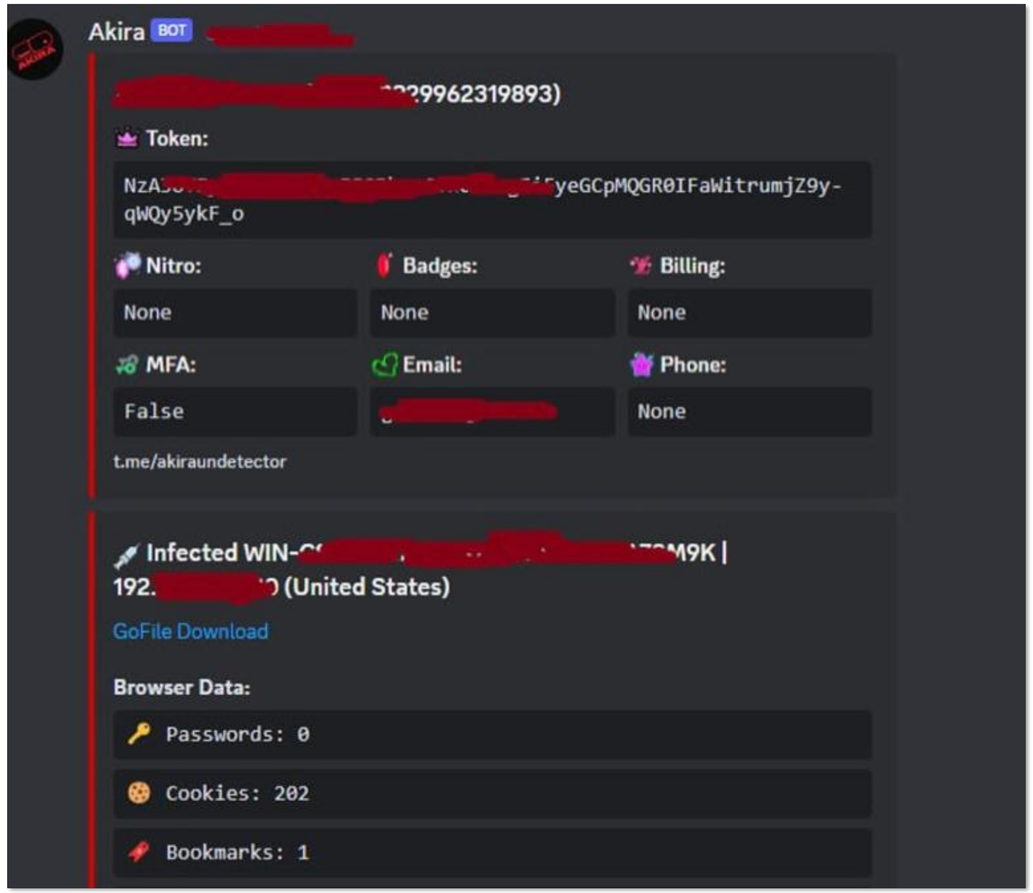
Exfiltrate token from Entra ID-joined device



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Real world story: Akira Stealer

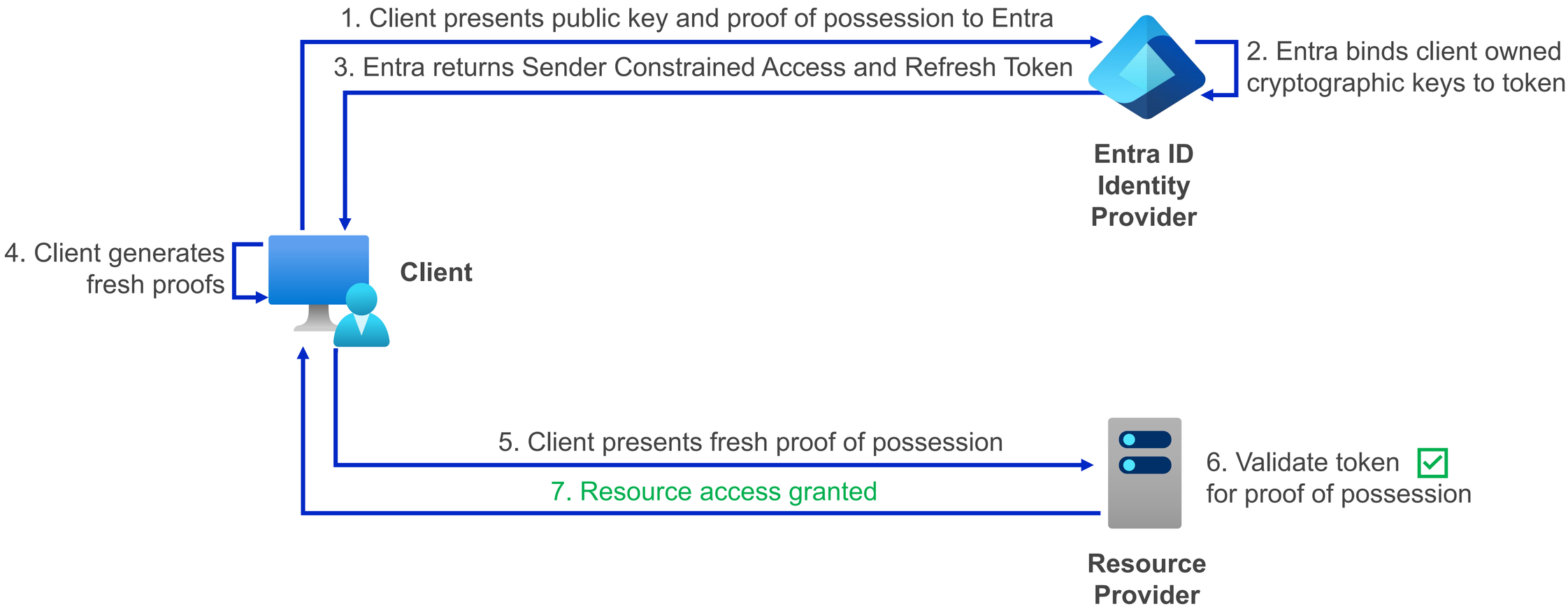




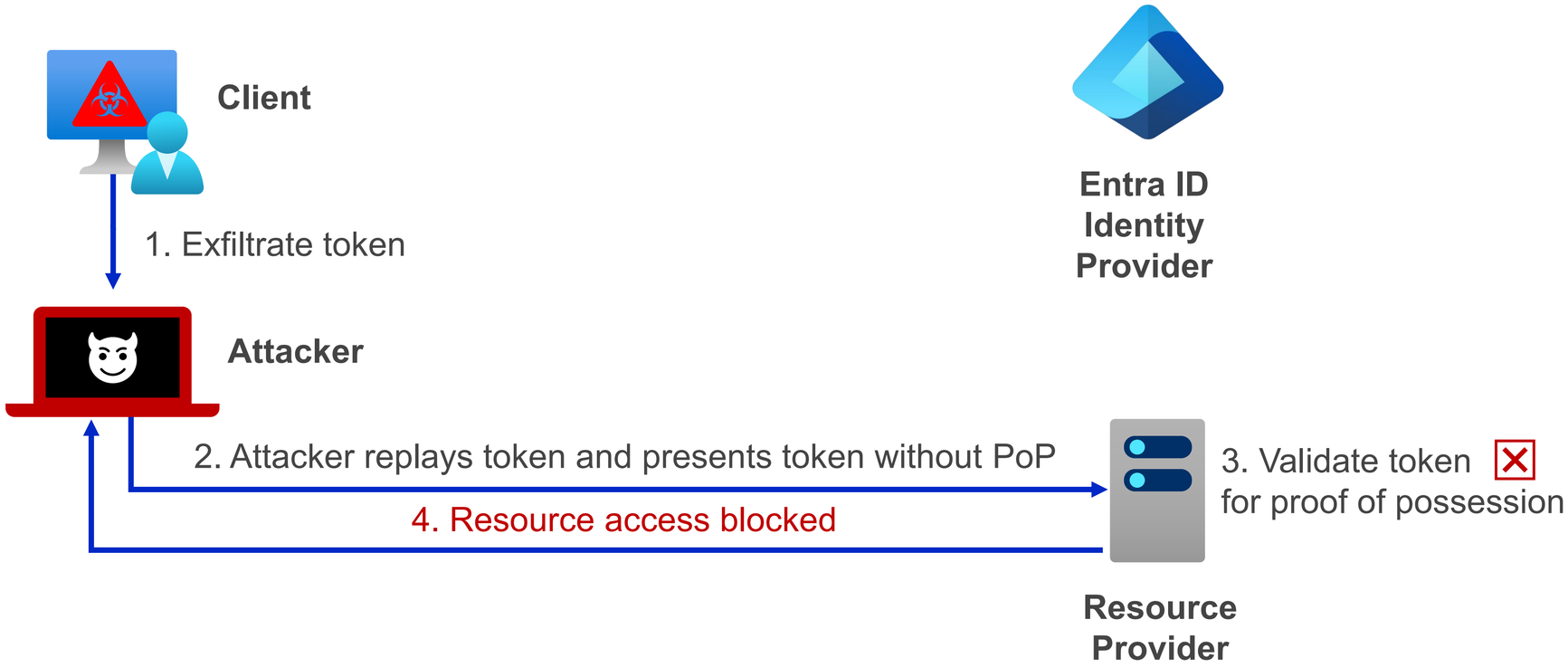
Source: Inside Akira Stealer: A full technical analysis of a modular stealer

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Mitigation by token binding (proof-of-possession)



Mitigation by token binding (proof-of-possession)



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

... did you say cookies?

C:\WINDOWS\system32\cmd.

```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\AdeleVance>dsregcmd /status

+----------------------------------------------------------------------+
```

Session cookie replay

Using Cookie Bite PoC by Varonis

Victim

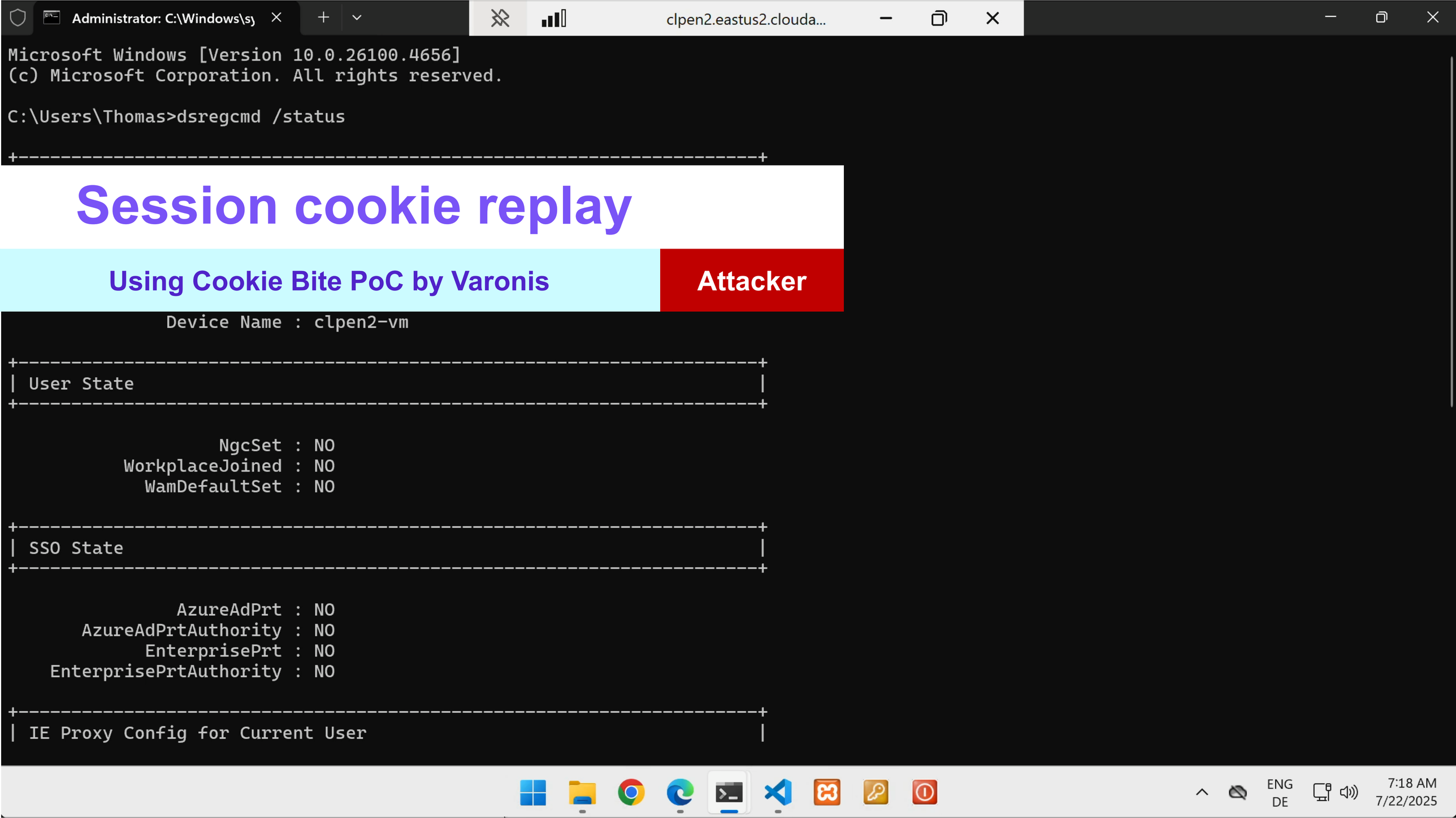
```
             Device Name : DESKTOP-1NS51H1

+----------------------------------------------------------------------+
| Device Details                                                       |
+----------------------------------------------------------------------+

                DeviceId : 7e27c2f6-3f52-4d90-ac8c-35ad1998dce7
              Thumbprint : 1322844BF6D2509EFAF743CC9D84BD70BEBA4E0E
 DeviceCertificateValidity : [ 2025-07-16 08:18:39.000 UTC -- 2035-07-16 08:48:39.000 UTC ]
           KeyContainerId : 976b97a2-30a5-4c85-89e3-209b8c0cb4f0
              KeyProvider : Microsoft Platform Crypto Provider
            TpmProtected : YES
         DeviceAuthStatus : SUCCESS

+----------------------------------------------------------------------+
| Tenant Details                                                       |
+----------------------------------------------------------------------+

              TenantName : C4A8 Ando
                TenantId : 19e61dac-ecff-427a-94c0-df49ff2f2331
             AuthCodeUrl : https://login.microsoftonline.com/19e61dac-ecff-427a-94c0-df49ff2f2331/oauth2/authorize
```


Administrator: C:\Windows\sy
clpen2.eastus2.clouda...
Microsoft Windows [Version 10.0.26100.4656]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Thomas>dsregcmd /status
+----------+
Session cookie replay
Using Cookie Bite PoC by Varonis
Attacker
Device Name : clpen2-vm
+----------+
| User State |
+----------+
NgcSet : NO
WorkplaceJoined : NO
WamDefaultSet : NO
+----------+
| SSO State |
+----------+
AzureAdPrt : NO
AzureAdPrtAuthority : NO
EnterprisePrt : NO
EnterprisePrtAuthority : NO
+----------+
| IE Proxy Config for Current User |
ENG
DE
7:18 AM
7/22/2025

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Sign-in logs from victim vs attacker

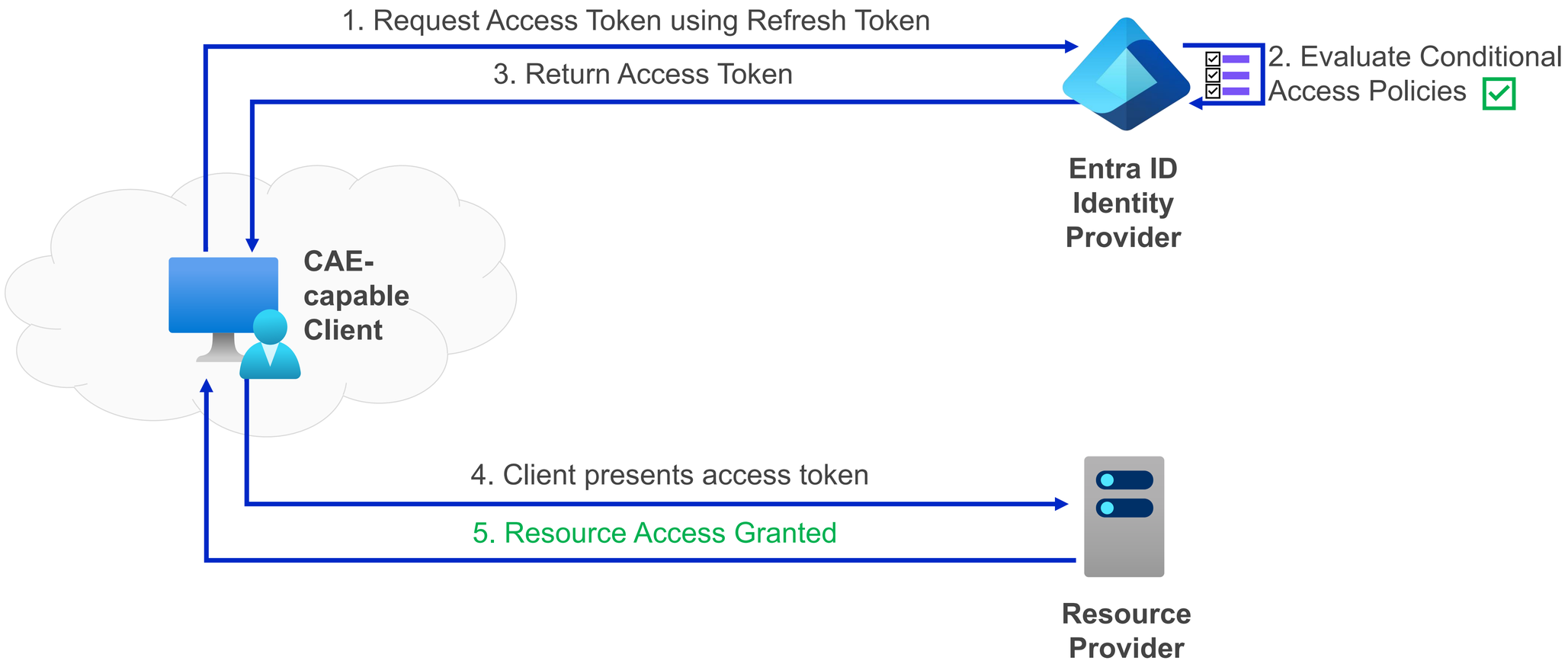
AppDisplayName	OfficeHome	OfficeHome
ClientAppUsed	Browser	Browser
BrowserDetails	Chrome 138.0.0	Chrome 138.0.0
Location	DE	US
DeviceTrustType	Azure AD joined	Azure AD joined
IsCompliant	true	true
IPAddress	87.163.7.44	132.196.242.136
UserAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Grant Controls ↑↓	Result ↑↓
Require multifactor authentication	Success
Require compliant device	Success

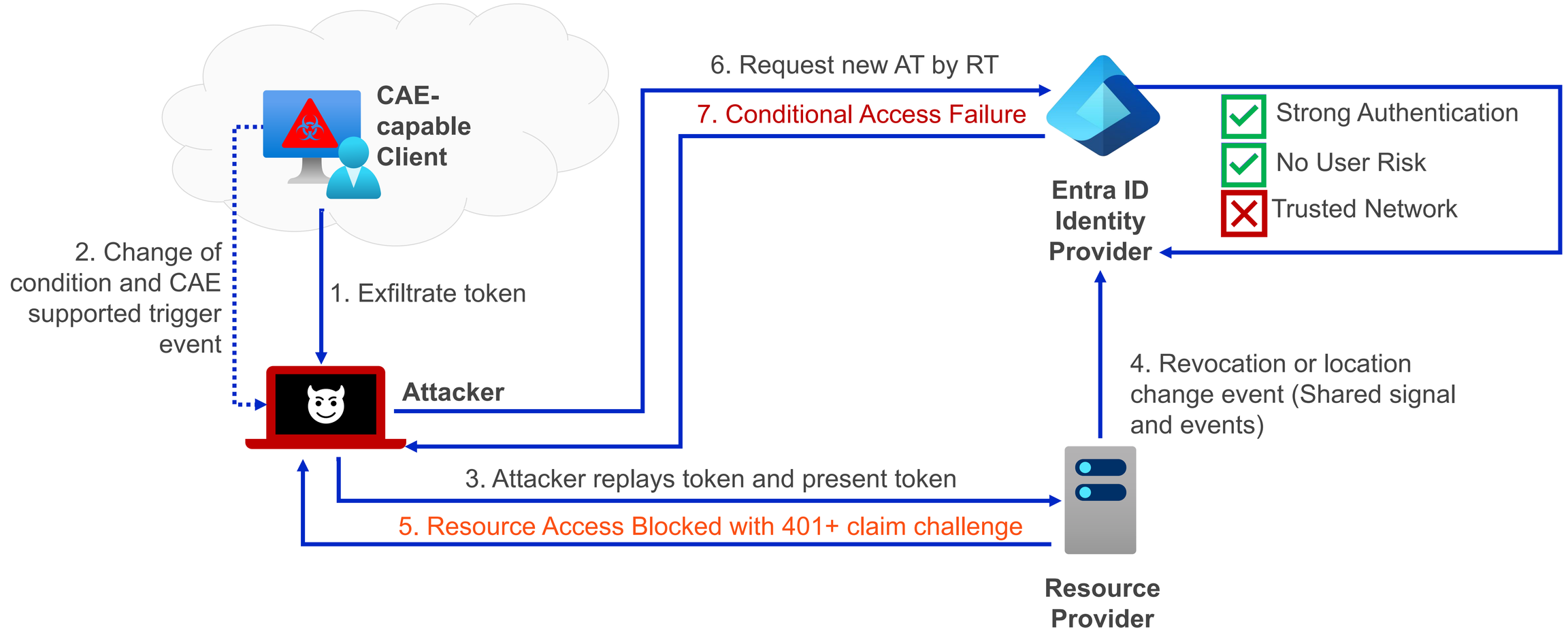
Grant Controls ↑↓	Result ↑↓
Require multifactor authentication	Success
Require compliant device	Success

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Token acquisition using refresh token

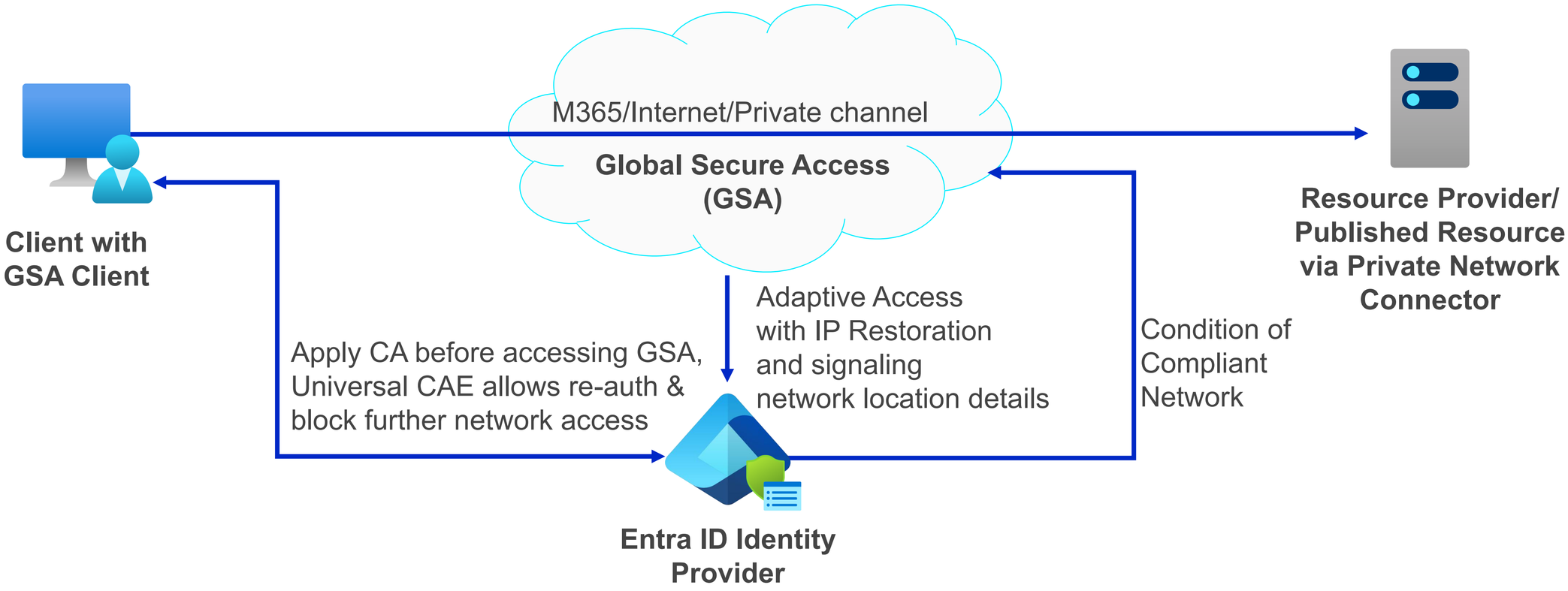


Revoke issued AT (Continuous Access Evaluation)

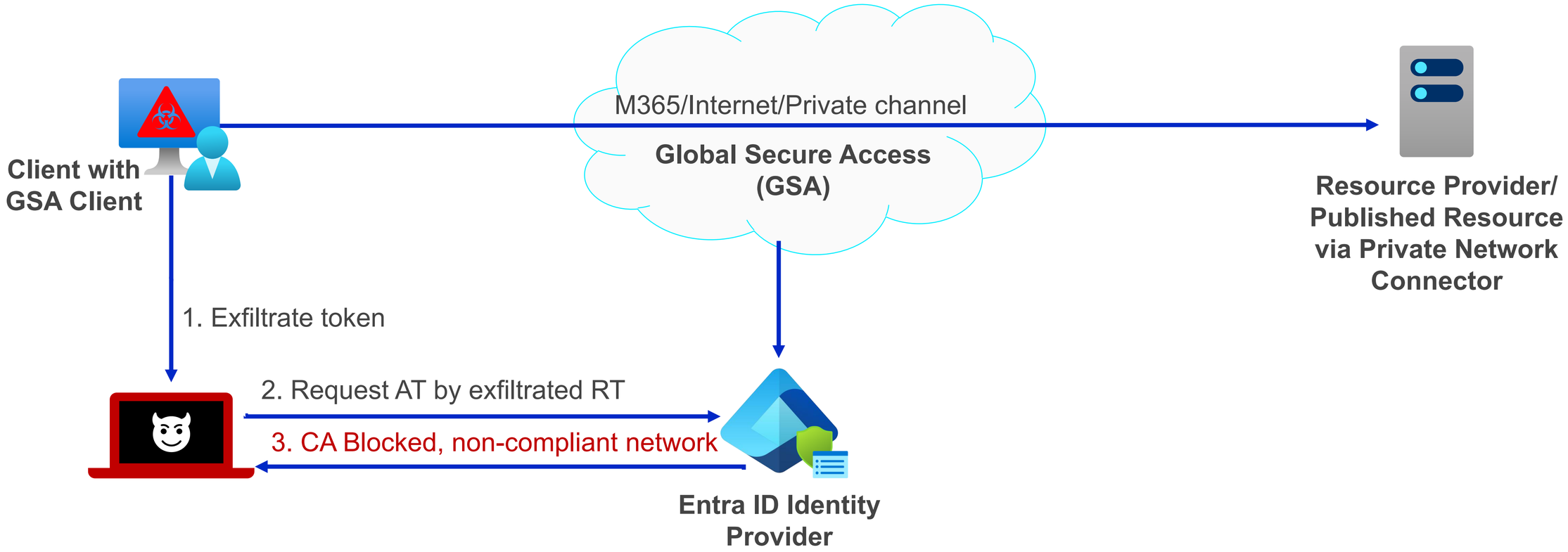


HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Mitigation by compliant network (GSA) signal



Mitigation by compliant network (GSA) signal



HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Abusing privileges of OAuth applications

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Change in user consent as part of Microsoft Secure Future Initiative (SFI)

Require admin consent for third-party apps accessing files and sites	Users allowing third-party apps to access file and site content can lead to overexposure of an organization's content. Requiring admins to consent to this access can help reduce overexposure. With this change, Microsoft managed App Consent Policies will be enabled, and users will be unable to consent to third party applications accessing their files and sites by default. Instead, they can request administrators to consent on their behalf. To configure admin consent, follow instructions here: Configuring the Admin Consent workflow. Customers who have already blocked user consent, turned on our previously recommended consent settings, or applied custom user consent settings will not be affected by this change. Admins can also configure granular app access policies, such as limiting user access to the application for specific users or groups. Learn more here.

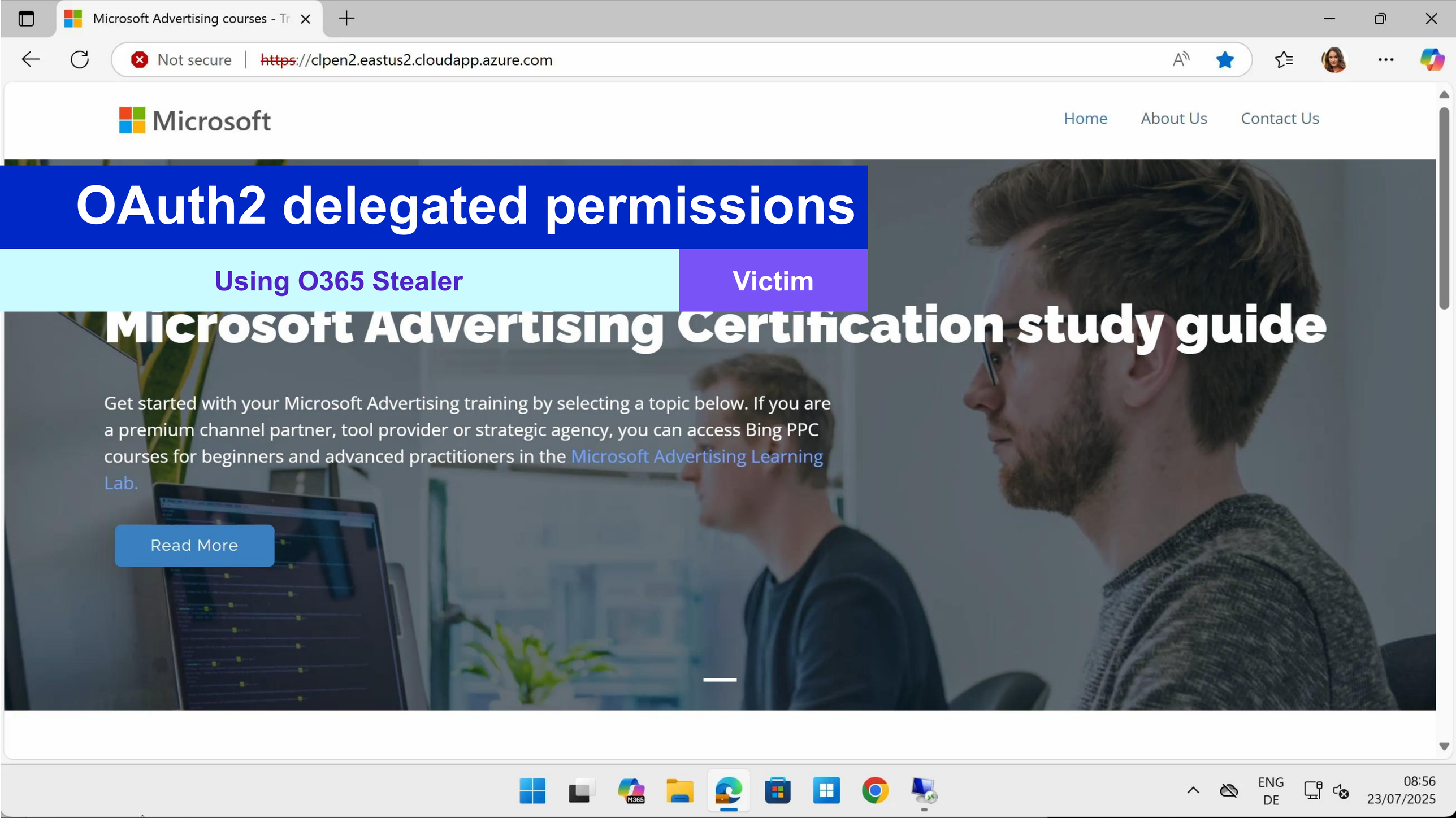
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Who has admin consent permissions?

Granting tenant-wide admin consent requires you to sign in as a user that is authorized to consent on behalf of the organization.

To grant tenant-wide admin consent, you need:

- A Microsoft Entra user account with one of the following roles:
  - Privileged Role Administrator, for granting consent for apps requesting any permission, for any API.
  - Cloud Application Administrator or Application Administrator, for granting consent for apps requesting any permission for any API, *except* Microsoft Graph app roles (application permissions).
  - A custom directory role that includes the permission to grant permissions to applications, for the permissions required by the application.


Microsoft Advertising courses - Tr
Not secure | https://clpen2.eastus2.cloudapp.azure.com
Microsoft
Home
About Us
Contact Us
OAuth2 delegated permissions
Using O365 Stealer
Victim
Microsoft Advertising Certification study guide
Get started with your Microsoft Advertising training by selecting a topic below. If you are a premium channel partner, tool provider or strategic agency, you can access Bing PPC courses for beginners and advanced practitioners in the Microsoft Advertising Learning Lab.
Read More
ENG
DE
08:56
23/07/2025

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

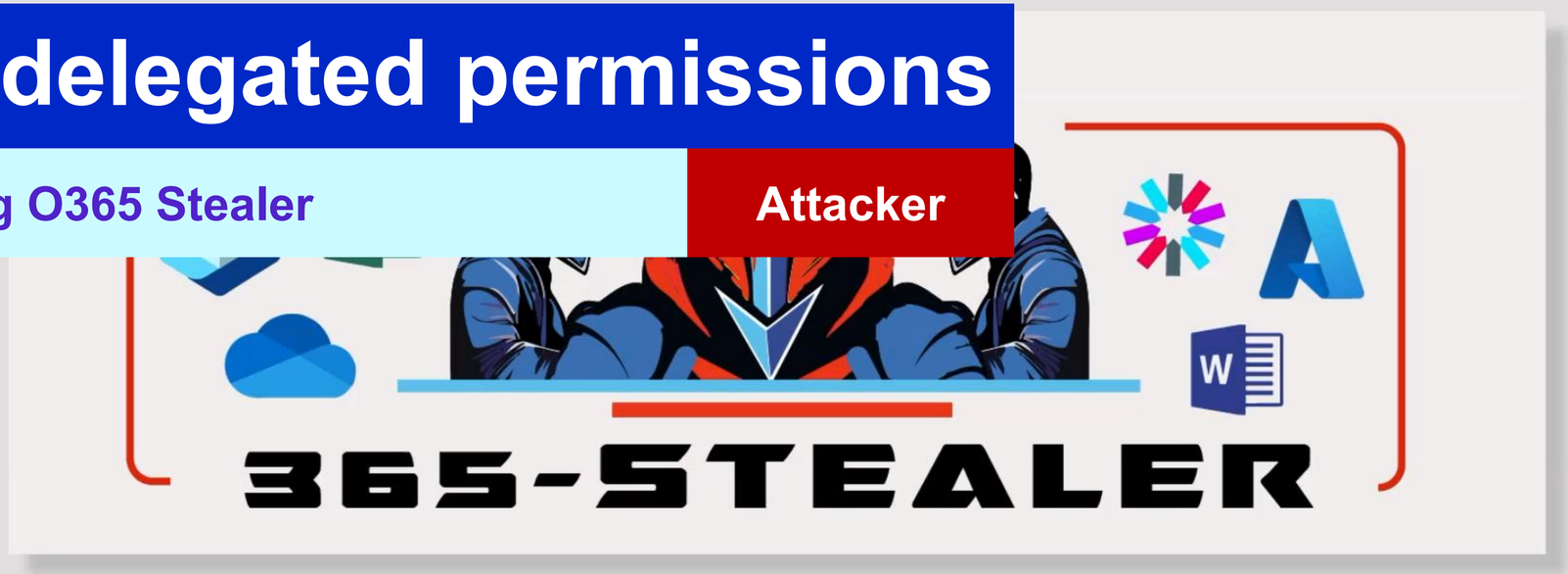
Not secure https://localhost:8443/365-Stealer/yourVictims/?dir=

365-STEALER Home JWT Decoder root

OAuth2 delegated permissions

Using O365 Stealer

Attacker



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

Index

Folders (1)

@Altered Security | 365-Stealer

ENG DE 6:59 AM 7/23/2025

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Disruption of malicious OAuth app created by user

Compromised user account used to create a malicious OAuth application (attack ...

Copilot | Manage incident | Tasks | ...

High | Resolved | u2330@ash.alpineskihouse.co | Critical asset | OAuth App Abuse | Attack Disruption

Attention! Attack disruption initiated a disable app action on a rogue OAuth app. For more details go to the Action center.

Attack story | Alerts (12) | Assets (4) | Investigations (0) | Evidence and Response (17) | Summary | Similar incidents (0)

Play attack story | Unpin all | Show all

Aug 22, 2025 7:42 AM Resolved
Malicious OAuth application registration by a compromised user
Abbi Montf... M1cr0s0ft-Conf...

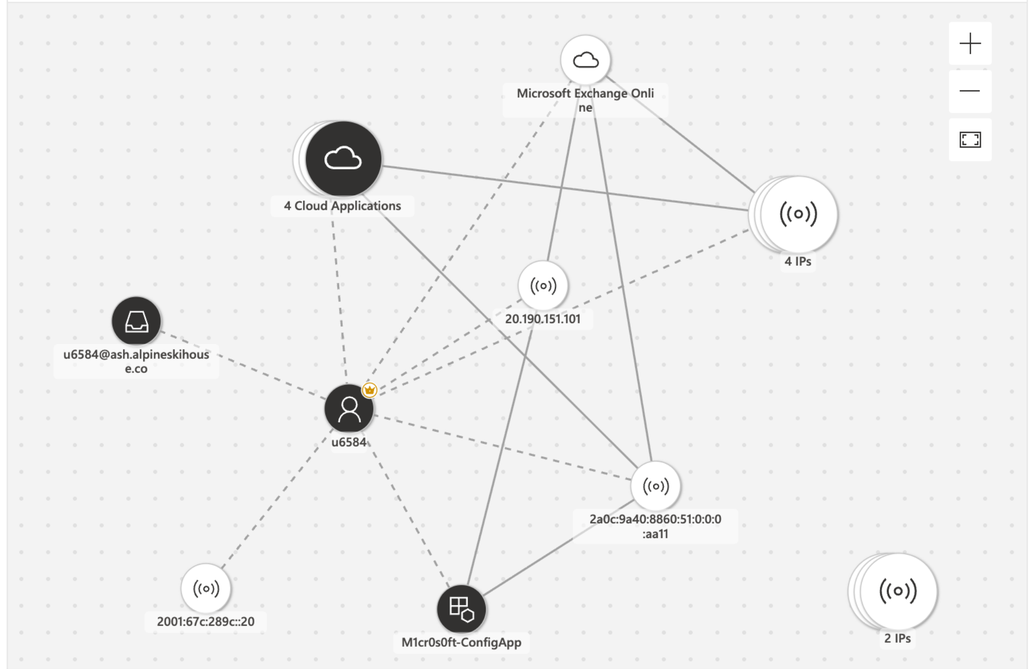
Aug 22, 2025 7:42 AM Resolved
Suspicious OAuth app registered through Azure CLI or PowerShell
Abbi Montfulleda

Aug 22, 2025 7:42 AM Resolved
Suspicious OAuth app registration
Abbi Montfulleda

Aug 22, 2025 7:42 AM Resolved
Risky user updated an app that accessed Email and performed Email activity through Graph API
Abbi Montfulleda

Aug 22, 2025 7:45 AM Resolved
Suspicious inbox rule created by an OAuth app
Abbi Montfulleda

Incident graph | Layout | Group similar nodes



RELATED THREATS

Activity Profile: OAuth apps used in BEC and phishing
48 impacted assets
View threat analytics report

Threat Overview Profile: Cloud identity abuse
29 impacted assets
View threat analytics report

Incident details

Assigned to
u2330@ash.alpineskihouse.co

Incident ID
18046

Classification

Categories

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Mitigation

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

User Mitigation

Authentication methods and credentials	Advanced policies to protect sensitive access	Zero Trust signals	ITDR and identity security posture	Device compliance and endpoint security
Stronger AD password policy	Restrict use of device code flow	Risk-based Conditional Access Policies	Restrict user consent and enable admin approval	Require device state or compliance in CA baseline
Banned password protection	Restrict access from unmanaged devices by Session Policy	No location-based CA exclusions	Avoid delegation of Application Admin and Ownership	Require TPM for Windows Hello and Secure Enclave for macOS
Adoption of passwordless authentication	Defender for Cloud Apps in combination with Edge MAM	Implement compliant network checks as condition in CA and take benefit of Universal CAE	Track exposed token and session cookies in Exposure Management	Enable Defender EDR capabilities
Require phishing-resistant authentication	Implement authentication context for sensitive actions	Access to cloud apps and on-premises resources by Global Secure Access	Adopt detection and hunting for unusual activities in post-authentication	Device compliance in combination with requiring low machine risk score
User doesn’t know their password (SCRIL in AD)	Implement Token Protection for applicable cloud applications	Enable strict enforcement of CAE for applicable applications	Automated incident response playbook to revoke tokens for compromised identities	Windows Enrollment attestation and monitor browser extension in Defender TVM

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

User Mitigation Foundational

Authentication methods and credentials	Advanced policies to protect sensitive access	Zero Trust signals	ITDR and identity security posture	Device compliance and endpoint security
Stronger AD password policy	Restrict use of device code flow	Risk-based Conditional Access Policies	Restrict user consent and enable admin approval	Require device state or compliance in CA baseline
Banned password protection	Restrict access from unmanaged devices by Session Policy	No location-based CA exclusions	Avoid delegation of Application Admin and Ownership	Require TPM for Windows Hello and Secure Enclave for macOS
Adoption of passwordless authentication	Defender for Cloud Apps in combination with Edge MAM	Implement compliant network checks as condition in CA and take benefit of Universal CAE	Track exposed token and session cookies in Exposure Management	Enable Defender EDR capabilities
Require phishing-resistant authentication	Implement authentication context for sensitive actions	Access to cloud apps and on-premises resources by Global Secure Access	Adopt detection and hunting for unusual activities in post-authentication	Device compliance in combination with requiring low machine risk score
User doesn't know their password (SCRIL in AD)	Implement Token Protection for applicable cloud applications	Enable strict enforcement of CAE for applicable applications	Automated incident response playbook to revoke tokens for compromised identities	Windows Enrollment attestation and monitor browser extension in Defender TVM

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

User Mitigation

Intermediate

Authentication methods and credentials	Advanced policies to protect sensitive access	Zero Trust signals	ITDR and identity security posture	Device compliance and endpoint security
Stronger AD password policy	Restrict use of device code flow	Risk-based Conditional Access Policies	Restrict user consent and enable admin approval	Require device state or compliance in CA baseline
Banned password protection	Restrict access from unmanaged devices by Session Policy	No location-based CA exclusions	Avoid delegation of Application Admin and Ownership	Require TPM for Windows Hello and Secure Enclave for macOS
Adoption of passwordless authentication	Defender for Cloud Apps in combination with Edge MAM	Implement compliant network checks as condition in CA and take benefit of Universal CAE	Track exposed token and session cookies in Exposure Management	Enable Defender EDR capabilities
Require phishing-resistant authentication	Implement authentication context for sensitive actions	Access to cloud apps and on-premises resources by Global Secure Access	Adopt detection and hunting for unusual activities in post-authentication	Device compliance in combination with requiring low machine risk score
User doesn't know their password (SCRIL in AD)	Implement Token Protection for applicable cloud applications	Enable strict enforcement of CAE for applicable applications	Automated incident response playbook to revoke tokens for compromised identities	Windows Enrollment attestation and monitor browser extension in Defender TVM

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

User Mitigation

Mature

Authentication methods and credentials	Advanced policies to protect sensitive access	Zero Trust signals	ITDR and identity security posture	Device compliance and endpoint security
Stronger AD password policy	Restrict use of device code flow	Risk-based Conditional Access Policies	Restrict user consent and enable admin approval	Require device state or compliance in CA baseline
Banned password protection	Restrict access from unmanaged devices by Session Policy	No location-based CA exclusions	Avoid delegation of Application Admin and Ownership	Require TPM for Windows Hello and Secure Enclave for macOS
Adoption of passwordless authentication	Defender for Cloud Apps in combination with Edge MAM	Implement compliant network checks as condition in CA and take benefit of Universal CAE	Track exposed token and session cookies in Exposure Management	Enable Defender EDR capabilities
Require phishing-resistant authentication	Implement authentication context for sensitive actions	Access to cloud apps and on-premises resources by Global Secure Access	Adopt detection and hunting for unusual activities in post-authentication	Device compliance in combination with requiring low machine risk score
User doesn't know their password (SCRIL in AD)	Implement Token Protection for applicable cloud applications	Enable strict enforcement of CAE for applicable applications	Automated incident response playbook to revoke tokens for compromised identities	Windows Enrollment attestation and monitor browser extension in Defender TVM

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

User Mitigation Progressive

Authentication methods and credentials	Advanced policies to protect sensitive access	Zero Trust signals	ITDR and identity security posture	Device compliance and endpoint security
Stronger AD password policy	Restrict use of device code flow	Risk-based Conditional Access Policies	Restrict user consent and enable admin approval	Require device state or compliance in CA baseline
Banned password protection	Restrict access from unmanaged devices by Session Policy	No location-based CA exclusions	Avoid delegation of Application Admin and Ownership	Require TPM for Windows Hello and Secure Enclave for macOS
Adoption of passwordless authentication	Defender for Cloud Apps in combination with Edge MAM	Implement compliant network checks as condition in CA and take benefit of Universal CAE	Track exposed token and session cookies in Exposure Management	Enable Defender EDR capabilities
Require phishing-resistant authentication	Implement authentication context for sensitive actions	Access to cloud apps and on-premises resources by Global Secure Access	Adopt detection and hunting for unusual activities in post-authentication	Device compliance in combination with requiring low machine risk score
User doesn't know their password (SCRIL in AD)	Implement Token Protection for applicable cloud applications	Enable strict enforcement of CAE for applicable applications	Automated incident response playbook to revoke tokens for compromised identities	Windows Enrollment attestation and monitor browser extension in Defender TVM

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON