semperis

Getting Developers to Follow Standards is Easy and Other Lies We Tell Ourselves

TROOPERS 2025

whoami

Microsoft Most Valuable Professional

Eric Woodruff

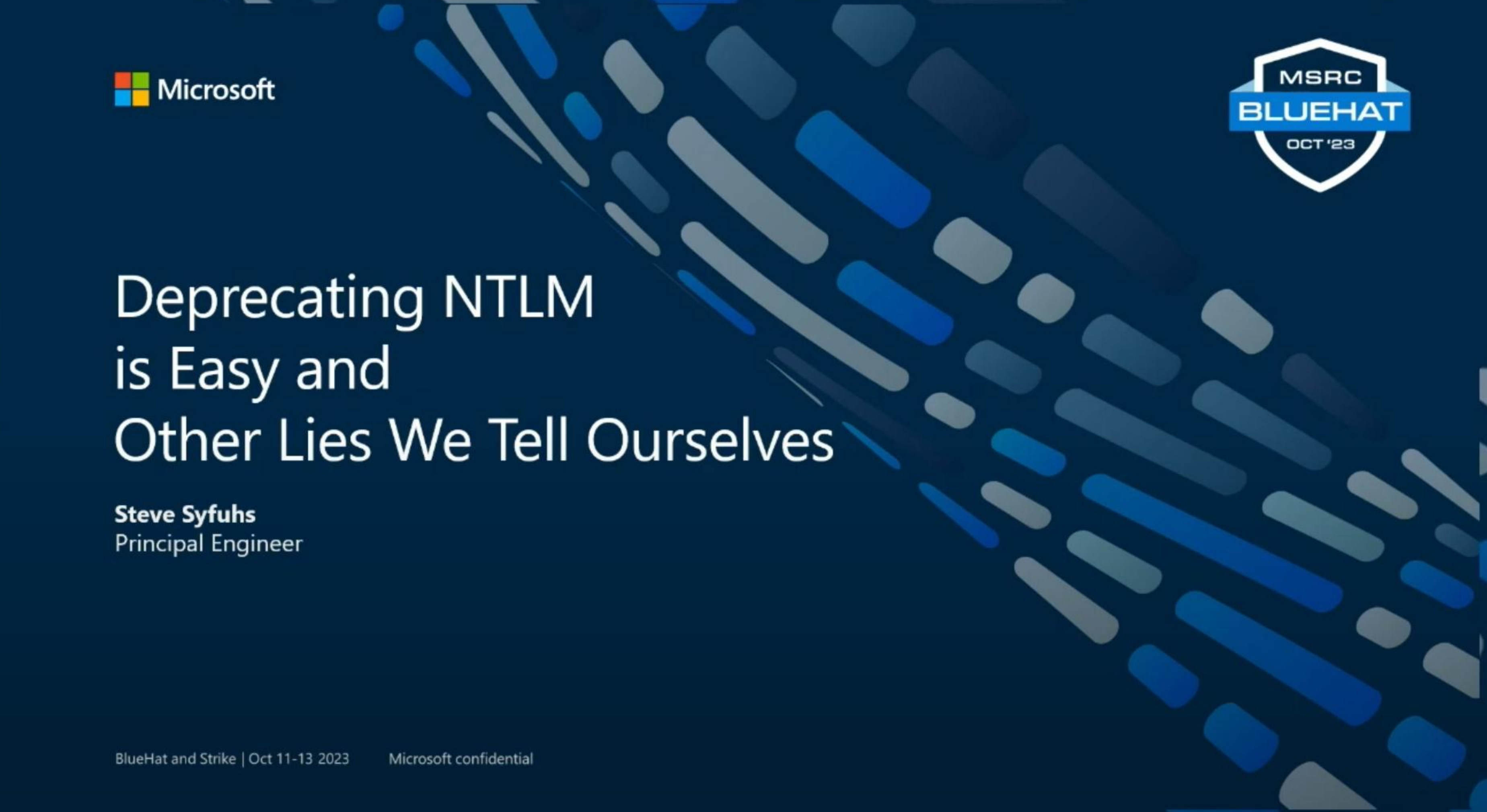
semperis

Chief Identity Architect
Microsoft Security MVP
IDPro Certified Identity Professional (CIDPRO)

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

semperis

The backstory

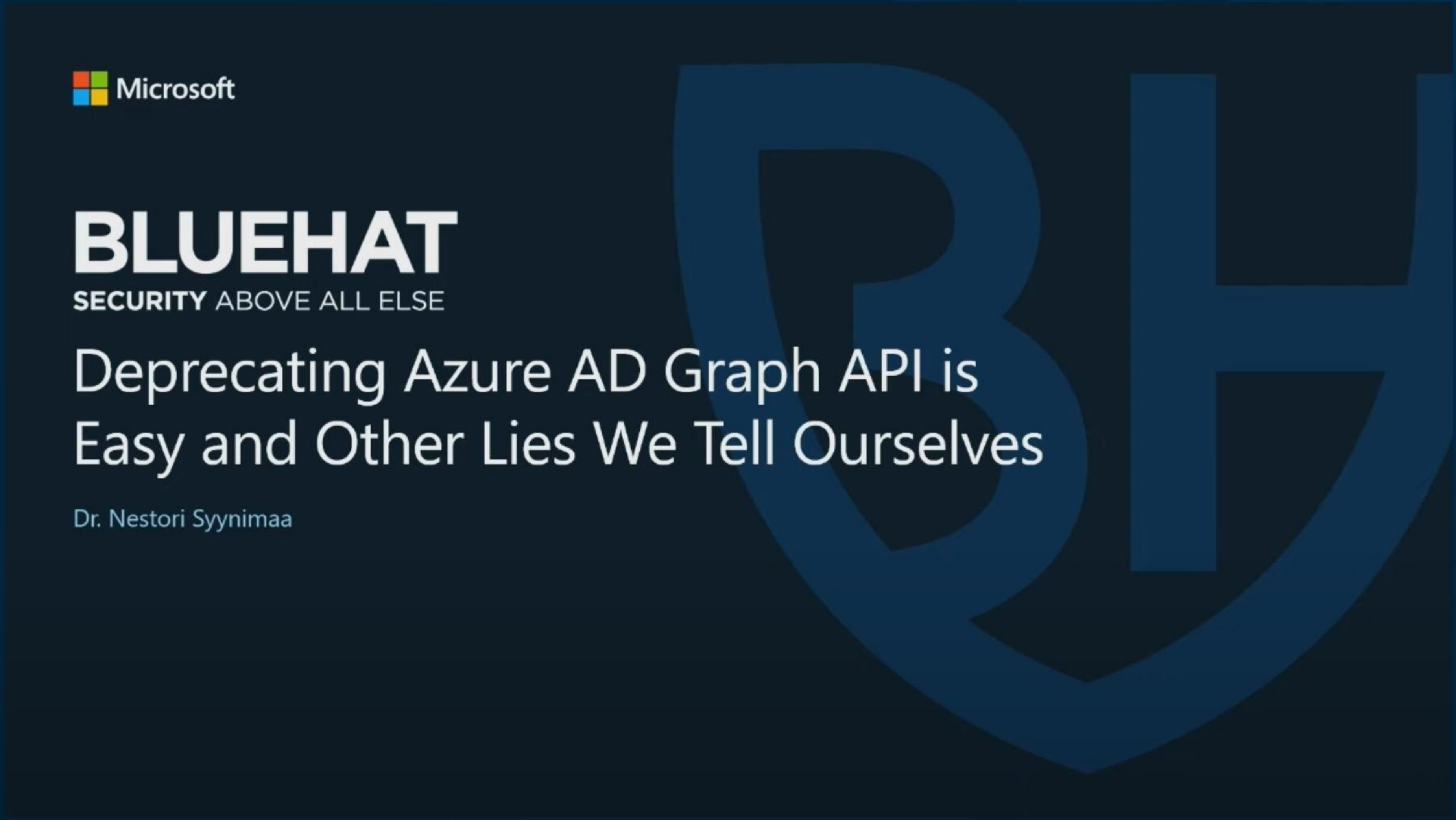


Deprecating NTLM is Easy and Other Lies We Tell Ourselves

Steve Syfuhs
Principal Engineer

Microsoft

Nestori Syynimaa



Microsoft

BLUEHAT

SECURITY ABOVE ALL ELSE

Deprecating Azure AD Graph API is Easy and Other Lies We Tell Ourselves

Dr. Nestori Syynimaa

BLUEHAT

nOAuth

Disclosed by Omer Cohen of Descope on June 20th, 2023

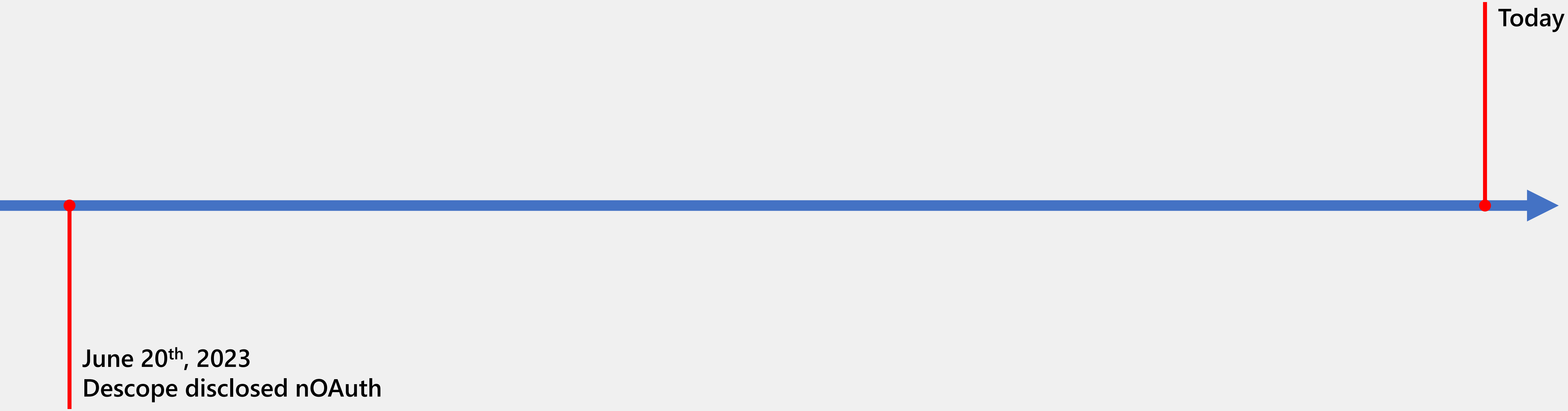
Vulnerability in apps using OpenID Connect with Entra ID

Vulnerability is rooted in identity **anti-patterns** for OIDC

Vulnerable applications allow for **takeover (impersonation) of any user** in the application if you know the target email address

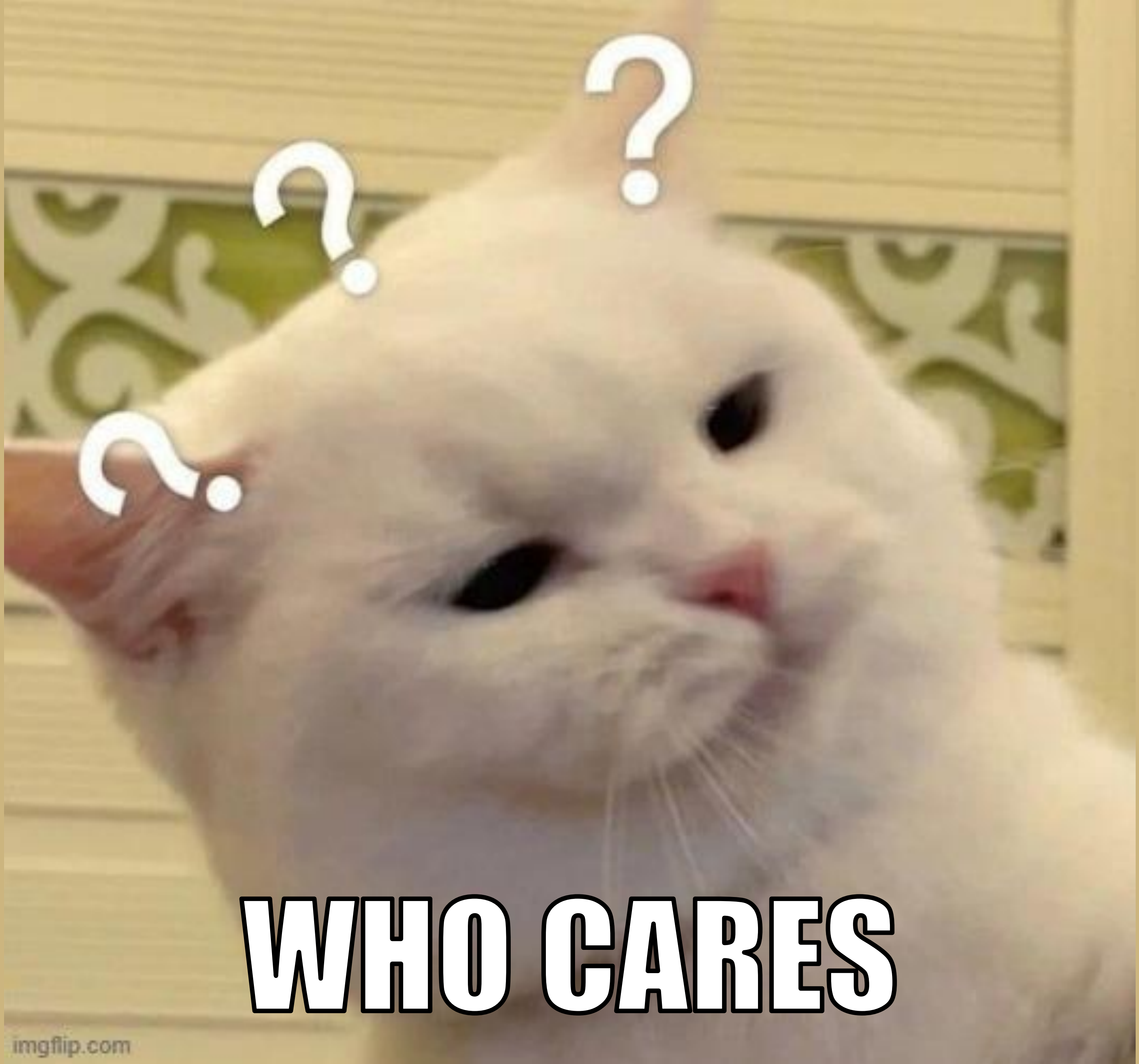
Cross-IdP attack

Timeline



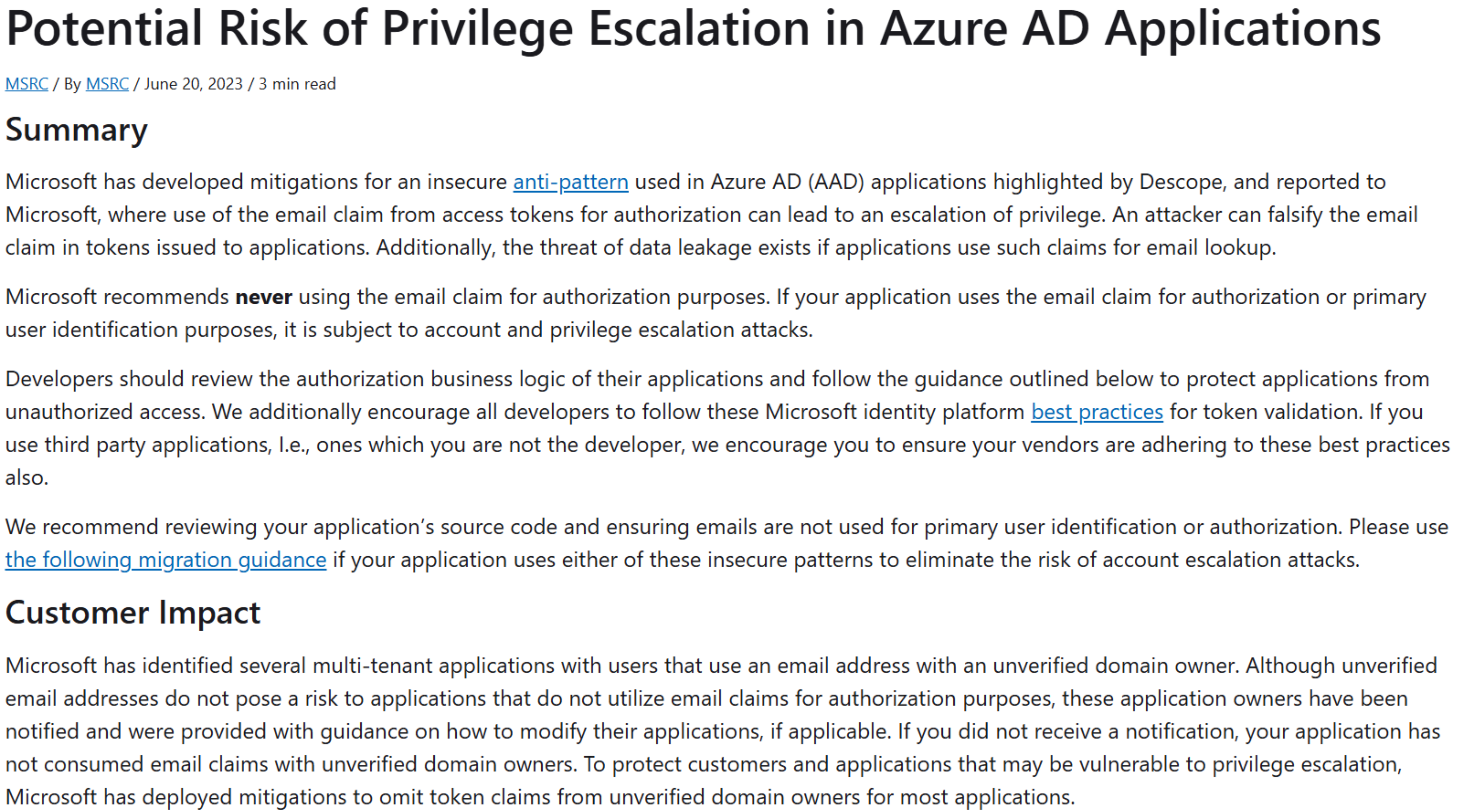
Today

June 20th, 2023
Descope disclosed nOAuth



WHO CARES
imgflip.com

https://msrc.microsoft.com/blog/2023/06/potential-risk-of-privilege-escalation-in-azure-ad-applications/



Potential Risk of Privilege Escalation in Azure AD Applications

MSRC / By MSRC / June 20, 2023 / 3 min read

Summary

Microsoft has developed mitigations for an insecure anti-pattern used in Azure AD (AAD) applications highlighted by Descope, and reported to Microsoft, where use of the email claim from access tokens for authorization can lead to an escalation of privilege. An attacker can falsify the email claim in tokens issued to applications. Additionally, the threat of data leakage exists if applications use such claims for email lookup.

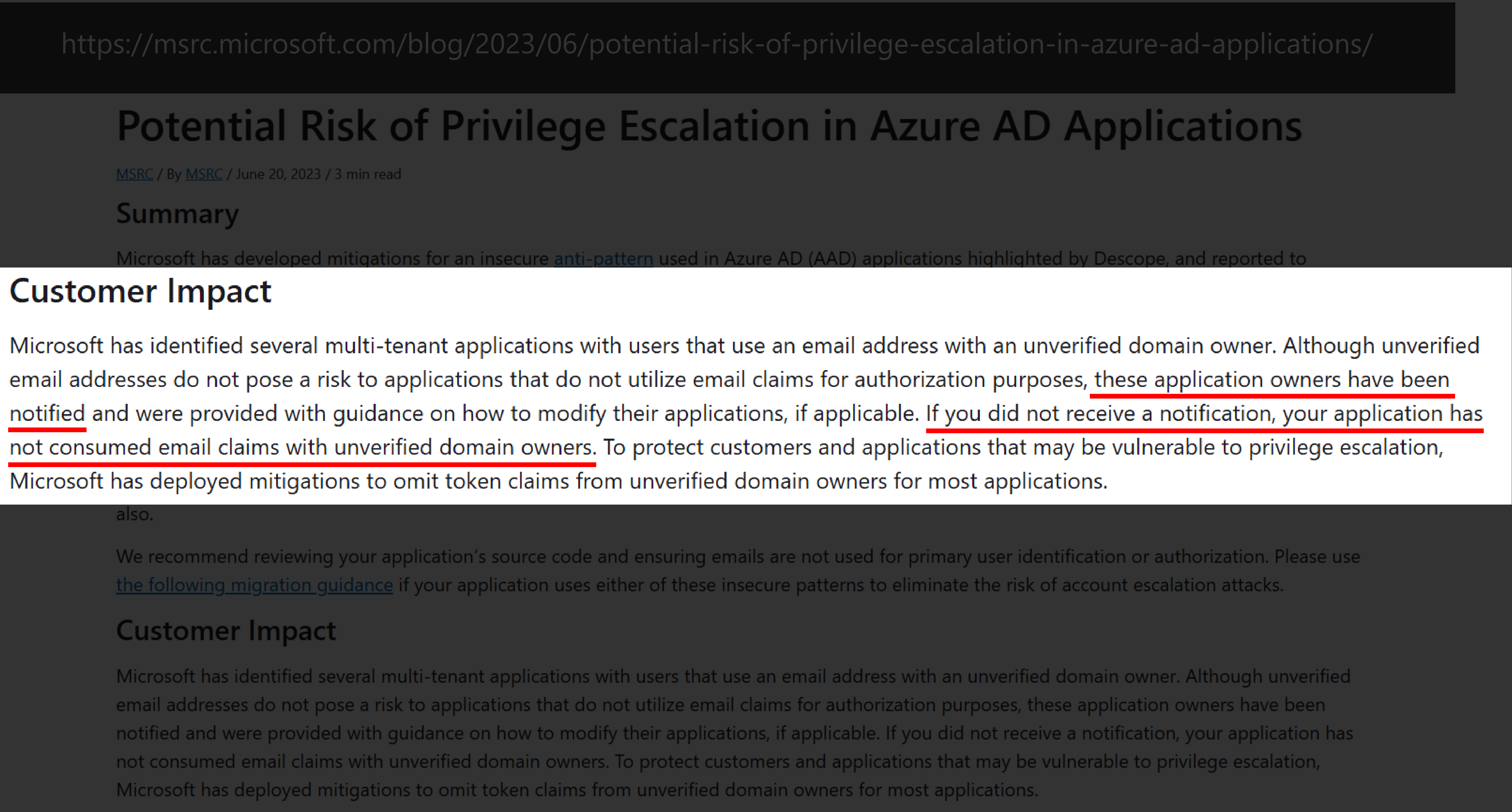
Microsoft recommends **never** using the email claim for authorization purposes. If your application uses the email claim for authorization or primary user identification purposes, it is subject to account and privilege escalation attacks.

Developers should review the authorization business logic of their applications and follow the guidance outlined below to protect applications from unauthorized access. We additionally encourage all developers to follow these Microsoft identity platform best practices for token validation. If you use third party applications, I.e., ones which you are not the developer, we encourage you to ensure your vendors are adhering to these best practices also.

We recommend reviewing your application’s source code and ensuring emails are not used for primary user identification or authorization. Please use the following migration guidance if your application uses either of these insecure patterns to eliminate the risk of account escalation attacks.

Customer Impact

Microsoft has identified several multi-tenant applications with users that use an email address with an unverified domain owner. Although unverified email addresses do not pose a risk to applications that do not utilize email claims for authorization purposes, these application owners have been notified and were provided with guidance on how to modify their applications, if applicable. If you did not receive a notification, your application has not consumed email claims with unverified domain owners. To protect customers and applications that may be vulnerable to privilege escalation, Microsoft has deployed mitigations to omit token claims from unverified domain owners for most applications.



https://msrc.microsoft.com/blog/2023/06/potential-risk-of-privilege-escalation-in-azure-ad-applications/

Potential Risk of Privilege Escalation in Azure AD Applications

MSRC / By MSRC / June 20, 2023 / 3 min read

Summary

Microsoft has developed mitigations for an insecure anti-pattern used in Azure AD (AAD) applications highlighted by Descope, and reported to

Customer Impact

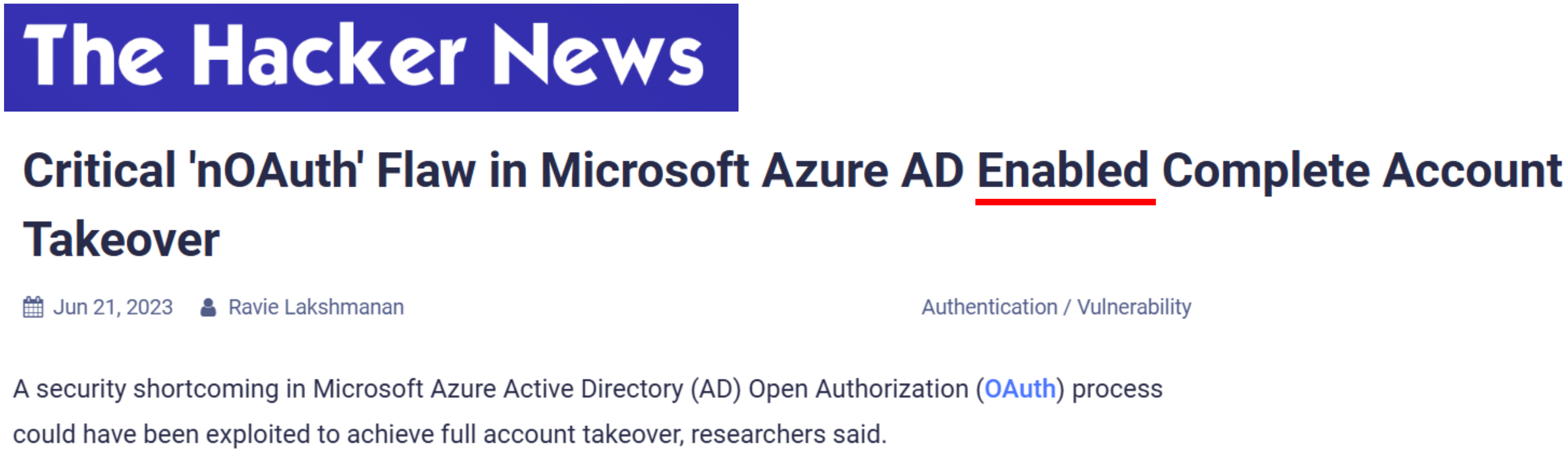
Microsoft has identified several multi-tenant applications with users that use an email address with an unverified domain owner. Although unverified email addresses do not pose a risk to applications that do not utilize email claims for authorization purposes, these application owners have been notified and were provided with guidance on how to modify their applications, if applicable. If you did not receive a notification, your application has not consumed email claims with unverified domain owners. To protect customers and applications that may be vulnerable to privilege escalation, Microsoft has deployed mitigations to omit token claims from unverified domain owners for most applications.

also.

We recommend reviewing your application's source code and ensuring emails are not used for primary user identification or authorization. Please use the following migration guidance if your application uses either of these insecure patterns to eliminate the risk of account escalation attacks.

Customer Impact

Microsoft has identified several multi-tenant applications with users that use an email address with an unverified domain owner. Although unverified email addresses do not pose a risk to applications that do not utilize email claims for authorization purposes, these application owners have been notified and were provided with guidance on how to modify their applications, if applicable. If you did not receive a notification, your application has not consumed email claims with unverified domain owners. To protect customers and applications that may be vulnerable to privilege escalation, Microsoft has deployed mitigations to omit token claims from unverified domain owners for most applications.

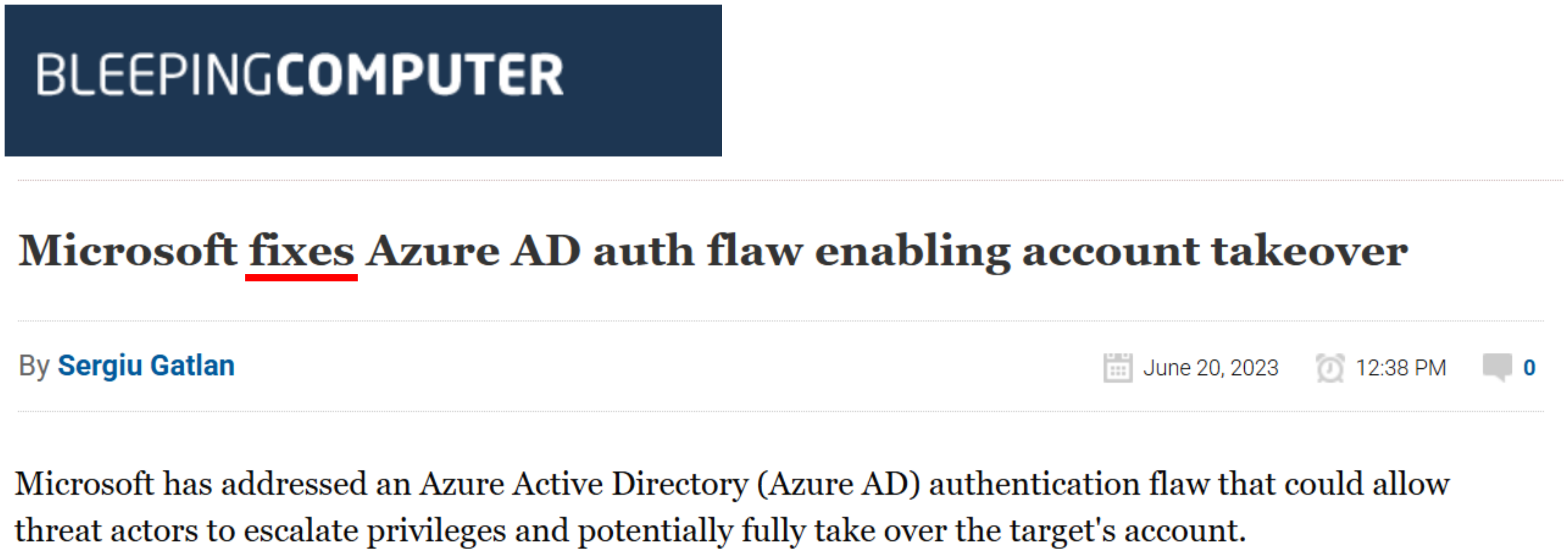


The Hacker News

Critical 'nOAuth' Flaw in Microsoft Azure AD Enabled Complete Account Takeover

Jun 21, 2023 Ravie Lakshmanan Authentication / Vulnerability

A security shortcoming in Microsoft Azure Active Directory (AD) Open Authorization (OAuth) process could have been exploited to achieve full account takeover, researchers said.

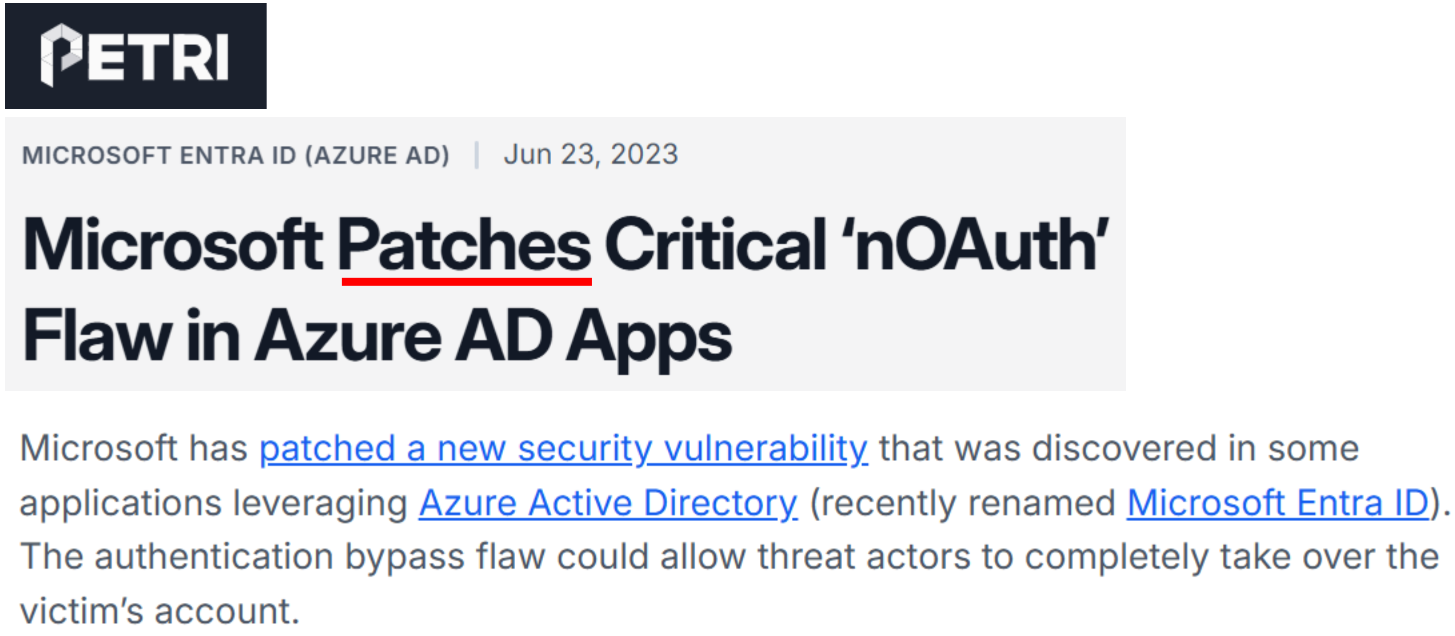


BLEEPINGCOMPUTER

Microsoft fixes Azure AD auth flaw enabling account takeover

By Sergiu Gatlan June 20, 2023 12:38 PM 0

Microsoft has addressed an Azure Active Directory (Azure AD) authentication flaw that could allow threat actors to escalate privileges and potentially fully take over the target's account.

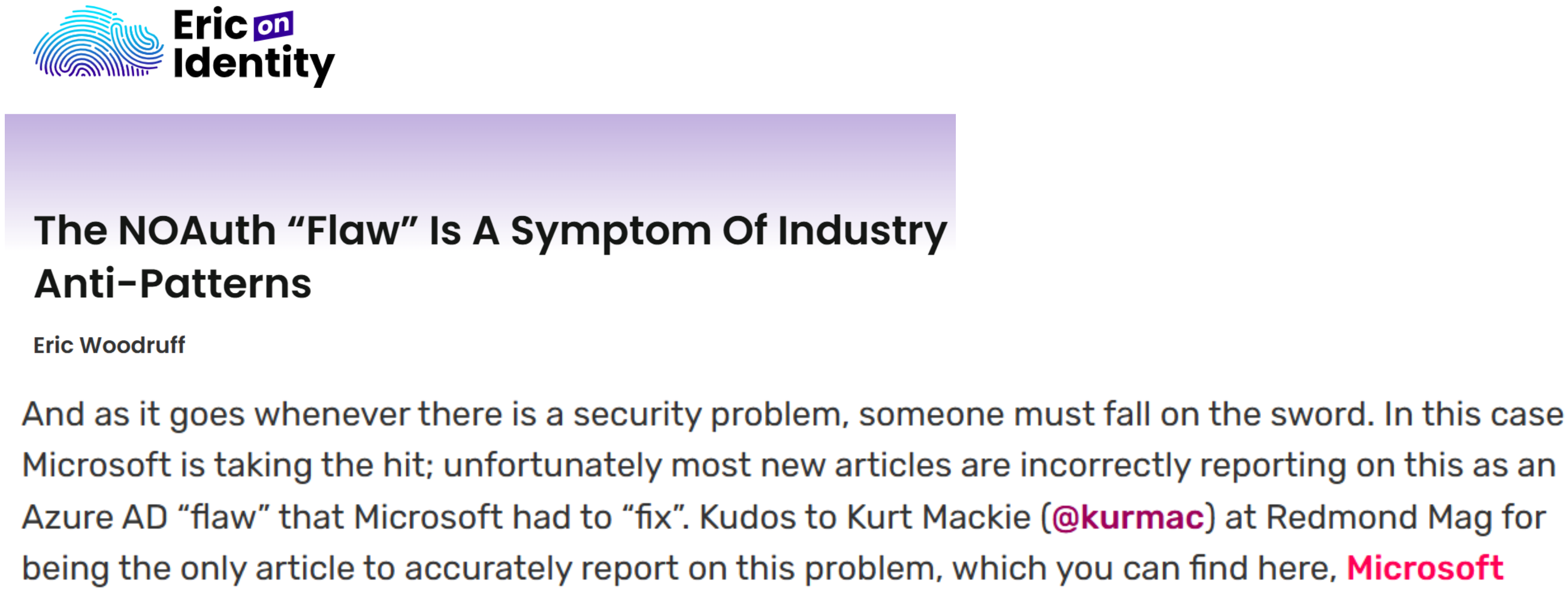


PETRI

MICROSOFT ENTRA ID (AZURE AD) | Jun 23, 2023

Microsoft Patches Critical 'nOAuth' Flaw in Azure AD Apps

Microsoft has patched a new security vulnerability that was discovered in some applications leveraging Azure Active Directory (recently renamed Microsoft Entra ID). The authentication bypass flaw could allow threat actors to completely take over the victim's account.



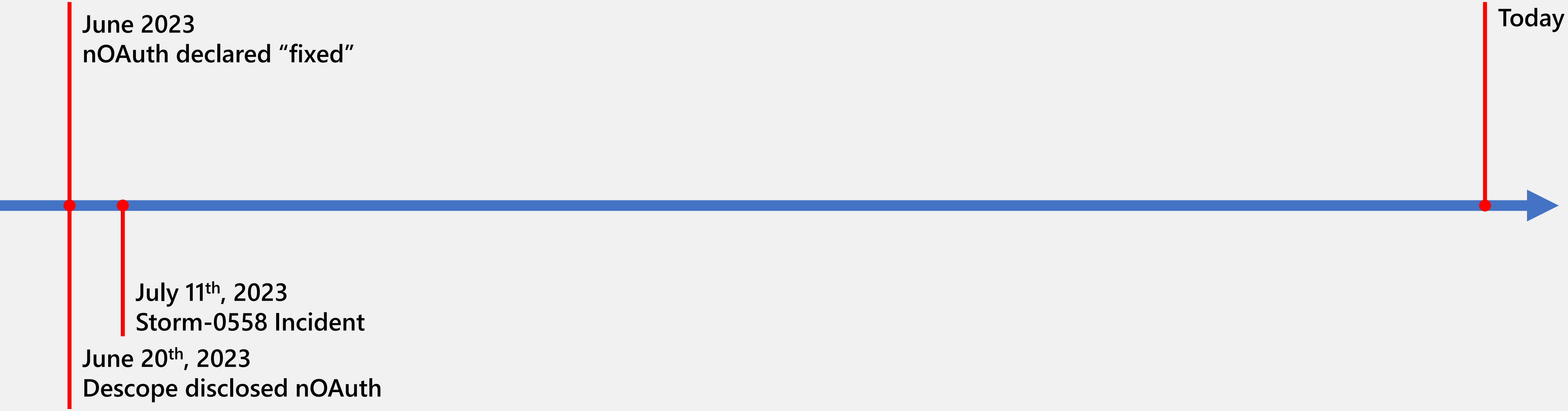
Eric on Identity

The NOAuth "Flaw" Is A Symptom Of Industry Anti-Patterns

Eric Woodruff

And as it goes whenever there is a security problem, someone must fall on the sword. In this case Microsoft is taking the hit; unfortunately most new articles are incorrectly reporting on this as an Azure AD "flaw" that Microsoft had to "fix". Kudos to Kurt Mackie (@kurmac) at Redmond Mag for being the only article to accurately report on this problem, which you can find here, Microsoft

Timeline

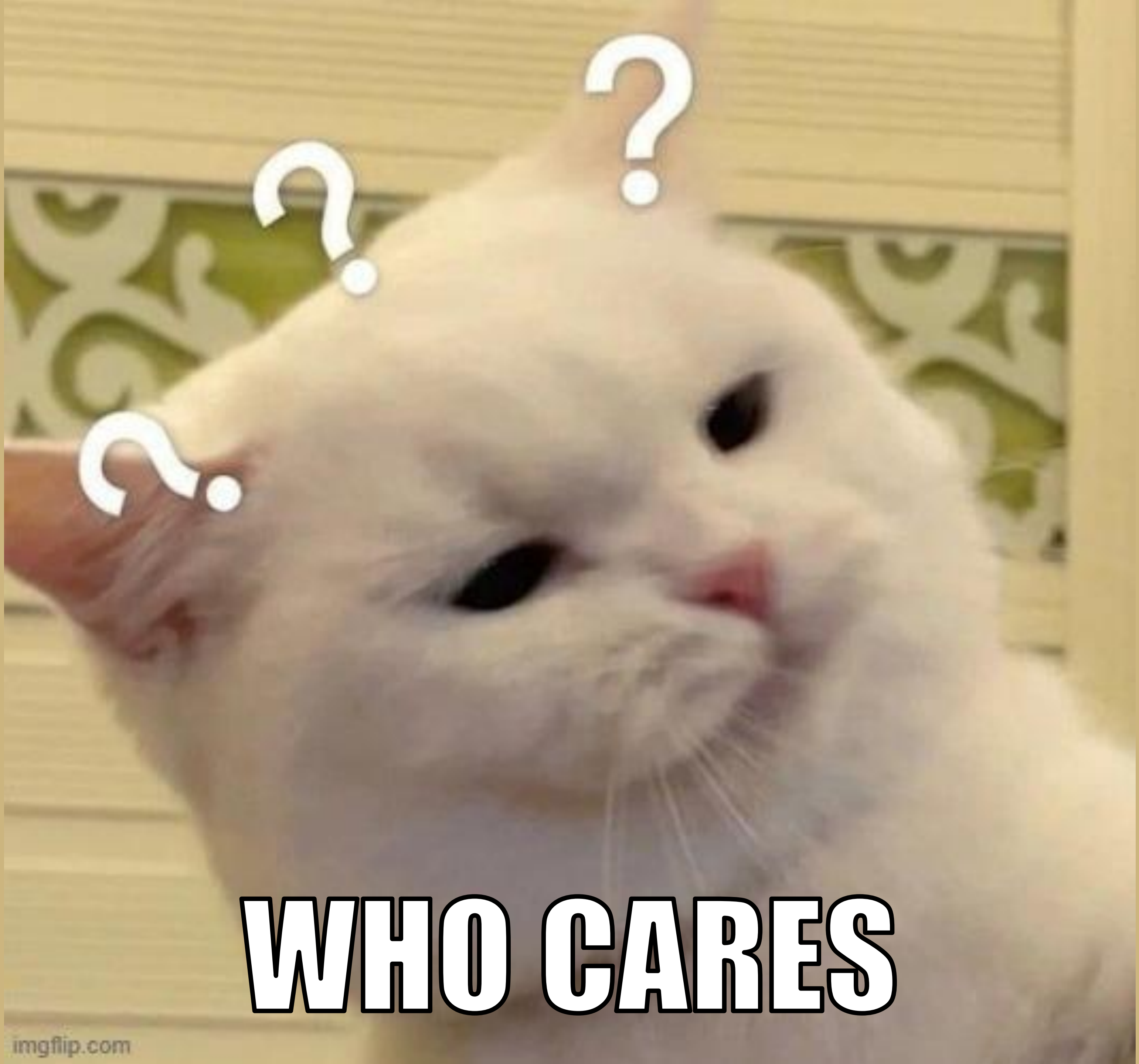


June 2023
nOAuth declared “fixed”

June 20th, 2023
Descope disclosed nOAuth

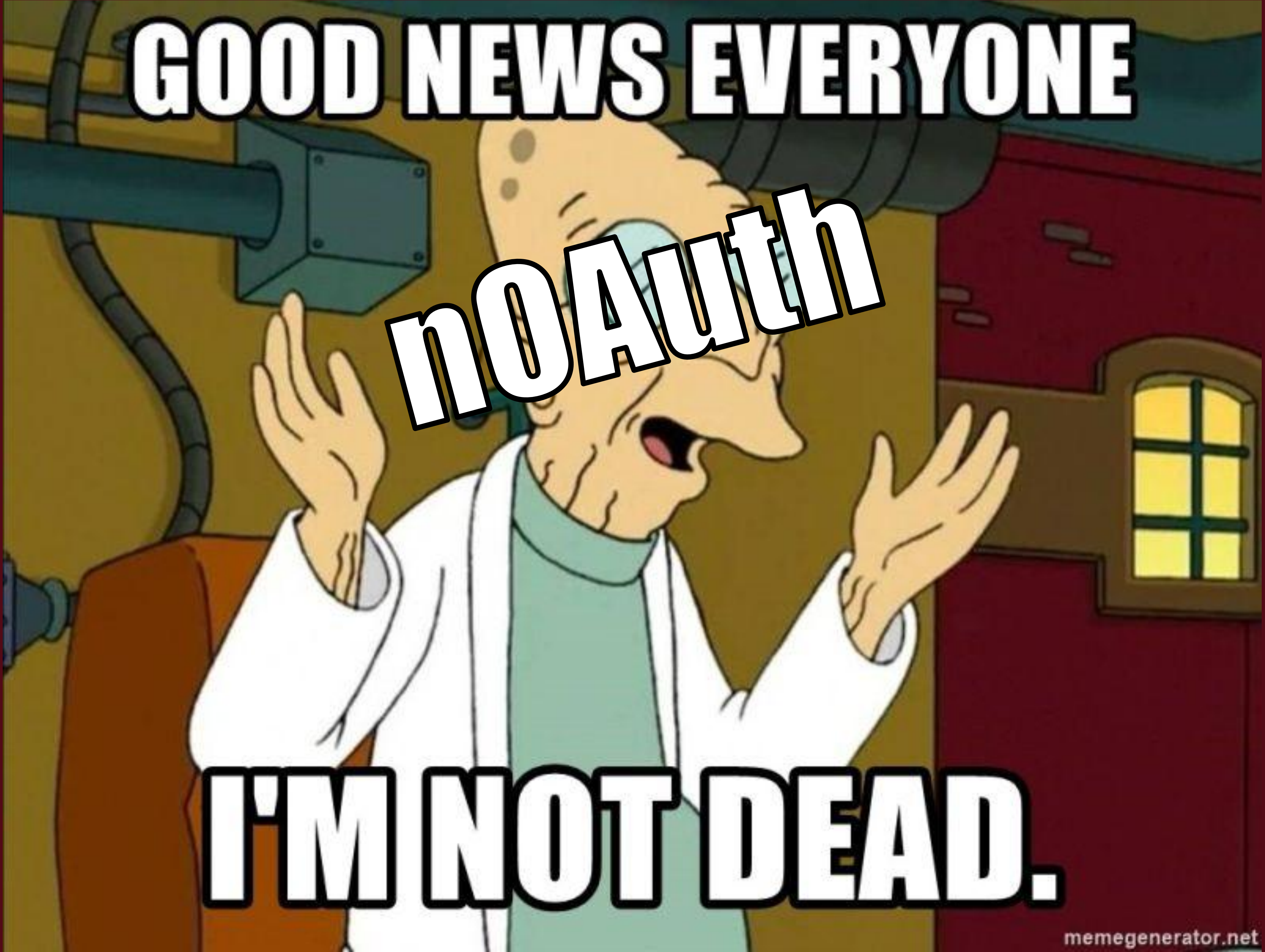
July 11th, 2023
Storm-0558 Incident

Today

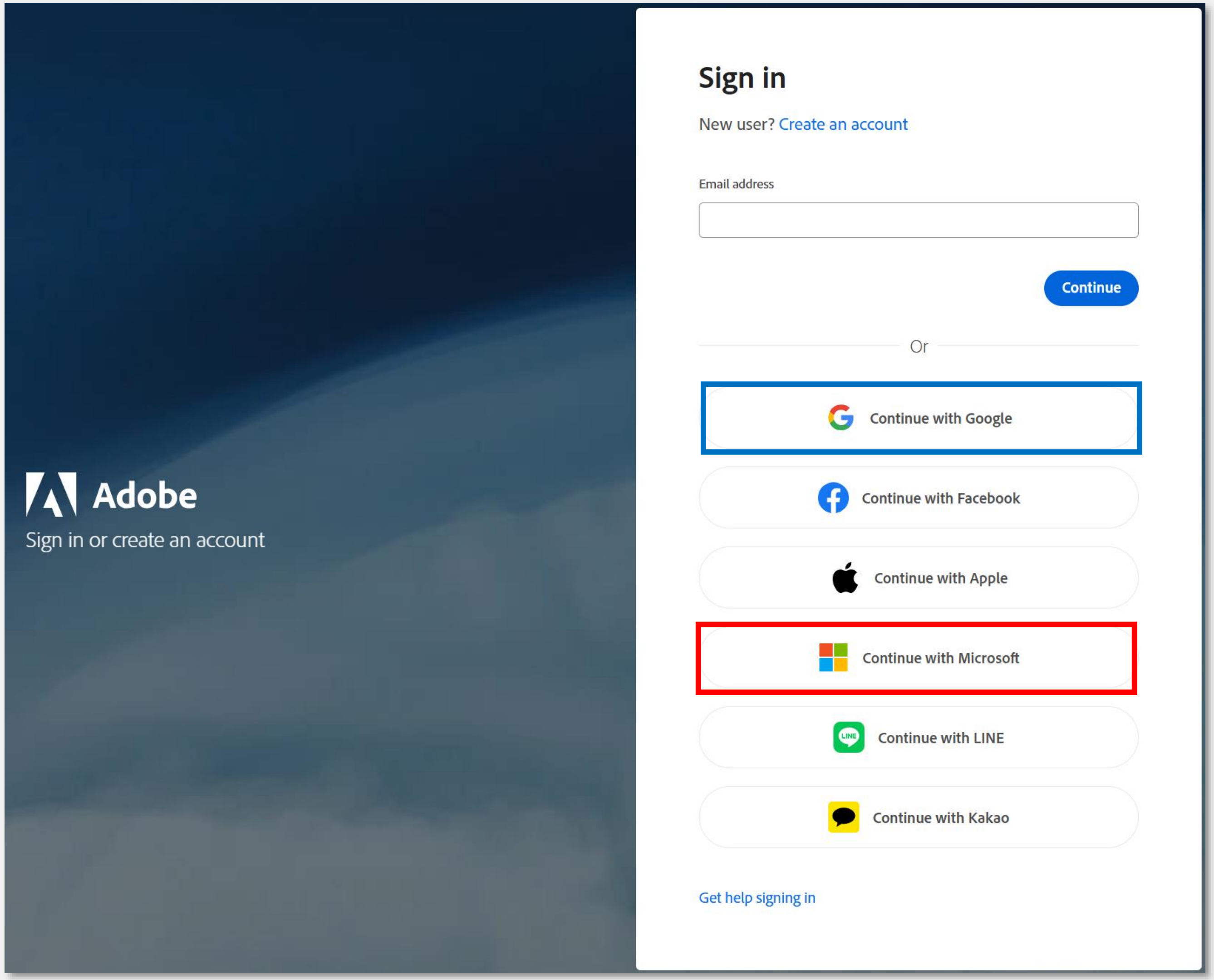

? ? ?
WHO CARES
imgflip.com

semperis

New research into nOAuth


GOOD NEWS EVERYONE
nOAuth
I'M NOT DEAD.
memegenerator.net

Descope focus



Adobe

Sign in or create an account

Sign in

New user? Create an account

Email address

Continue

Or

Continue with Google

Continue with Facebook

Continue with Apple

Continue with Microsoft

Continue with LINE

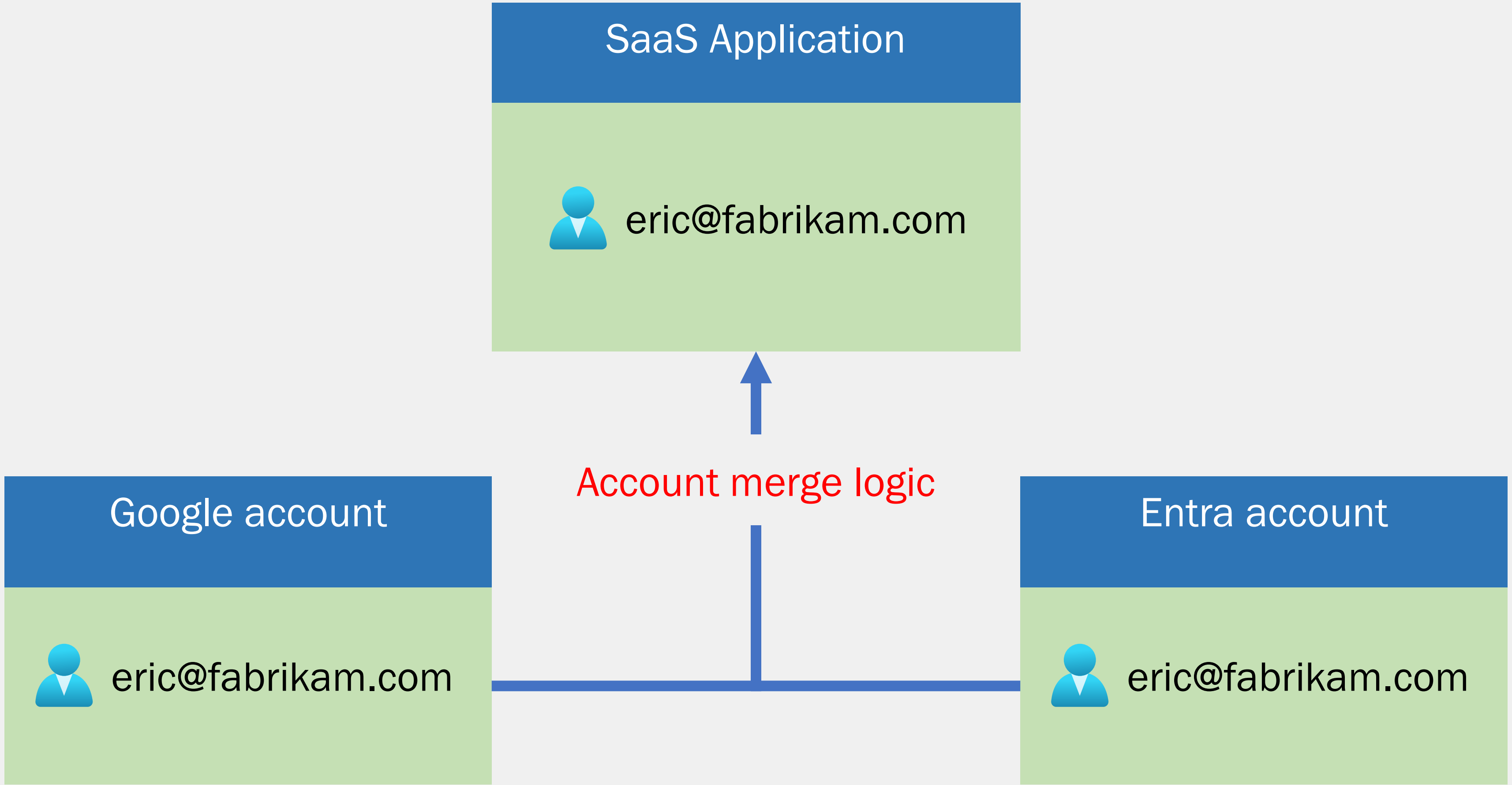
Continue with Kakao

Get help signing in

Using Adobe as an example, it is not vulnerable to nOAuth

1. Legitimate user authenticates with Google
2. Attacker configures attack Entra tenant
3. Attacker authenticates with Entra with unverified email attribute
4. Application account merge logic does not verify email ownership
5. Attacker overtakes account with a cross-IdP type attack

Descope focus



SaaS Application

eric@fabrikam.com

Account merge logic

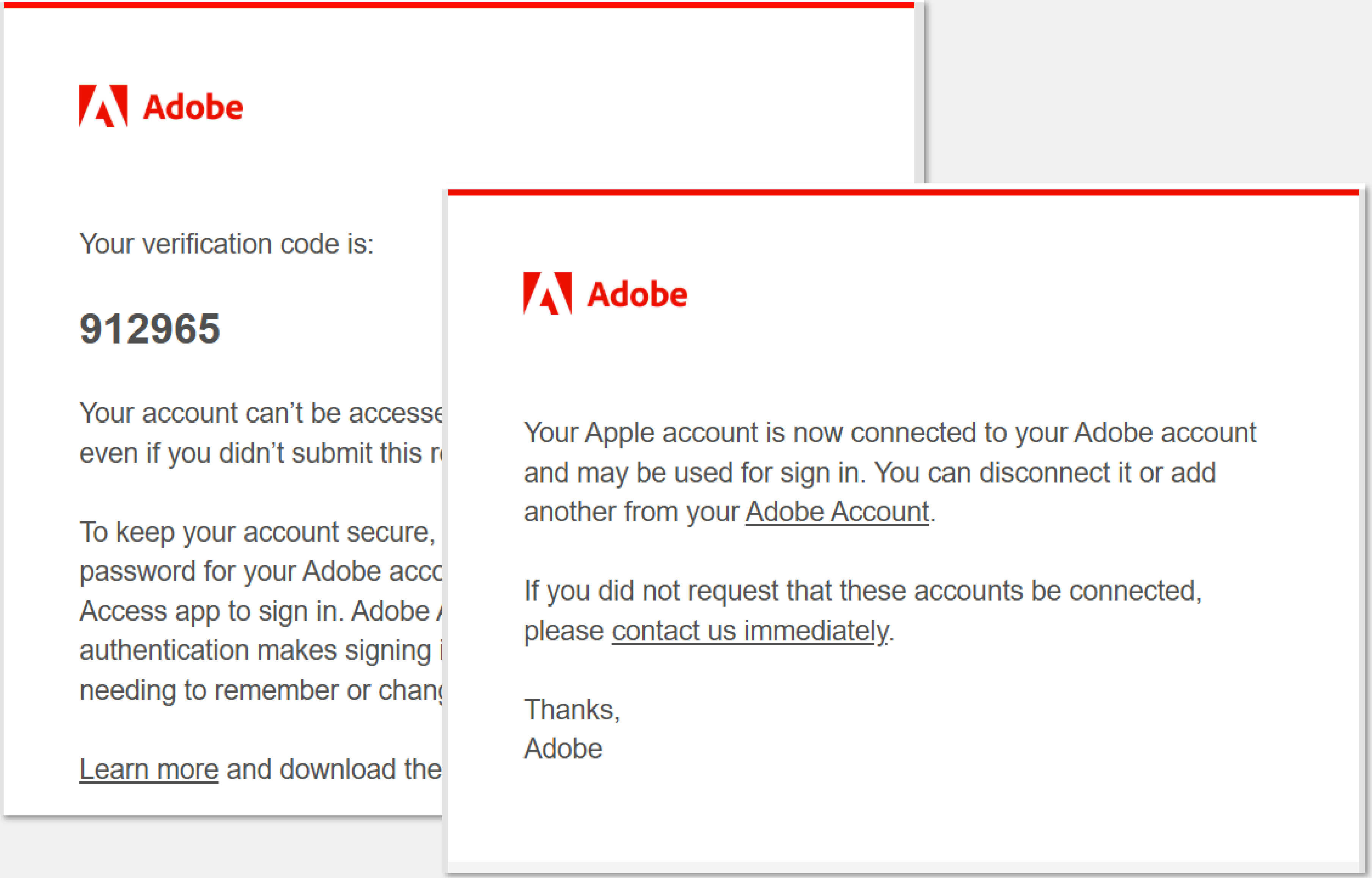
Google account

eric@fabrikam.com

Entra account

eric@fabrikam.com

Descope focus



Adobe

Your verification code is:

912965

Your account can't be accesse
even if you didn't submit this r

To keep your account secure,
password for your Adobe acco
Access app to sign in. Adobe A
authentication makes signing i
needing to remember or chang

Learn more and download the

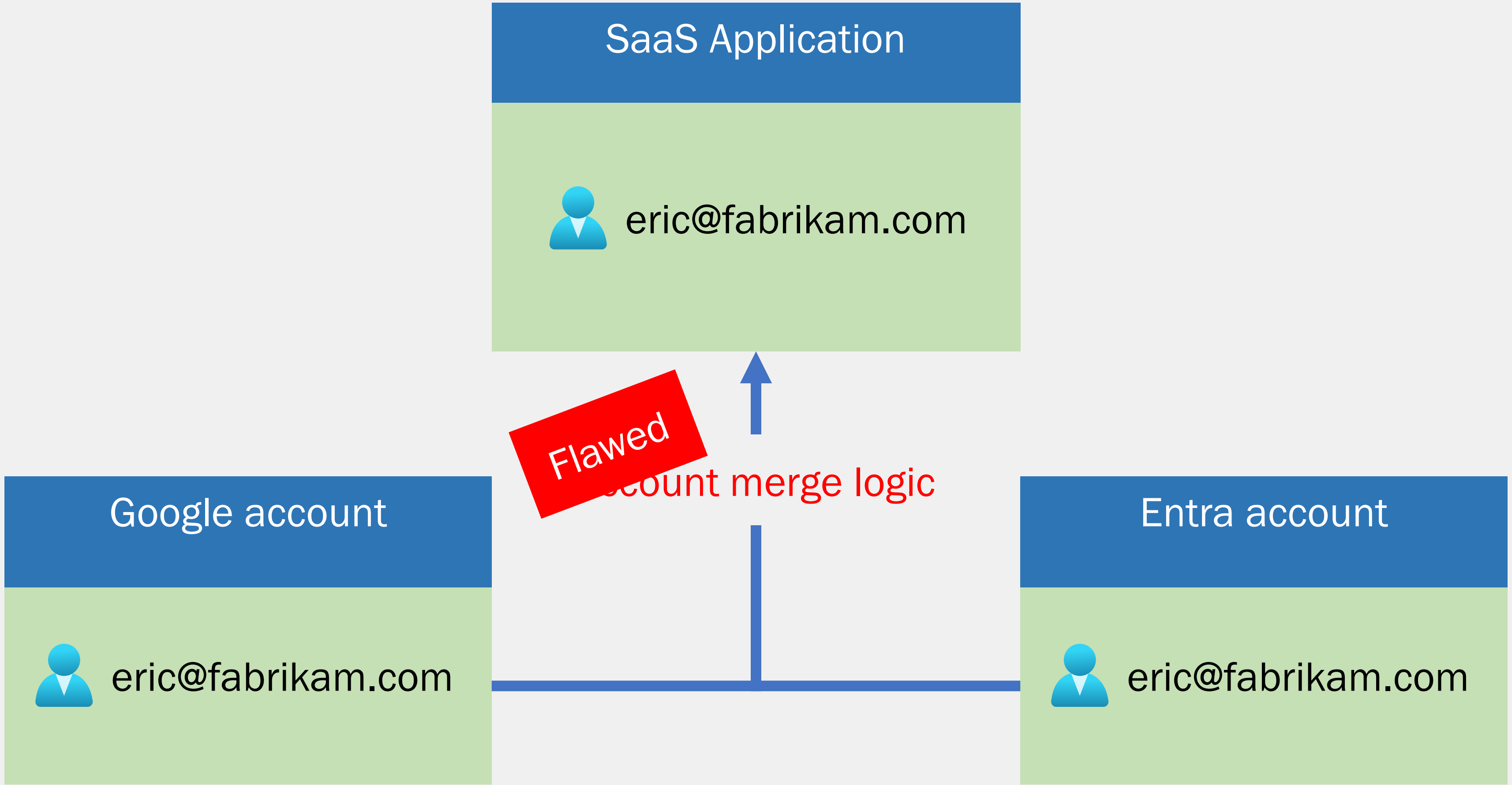
Adobe

Your Apple account is now connected to your Adobe account and may be used for sign in. You can disconnect it or add another from your Adobe Account.

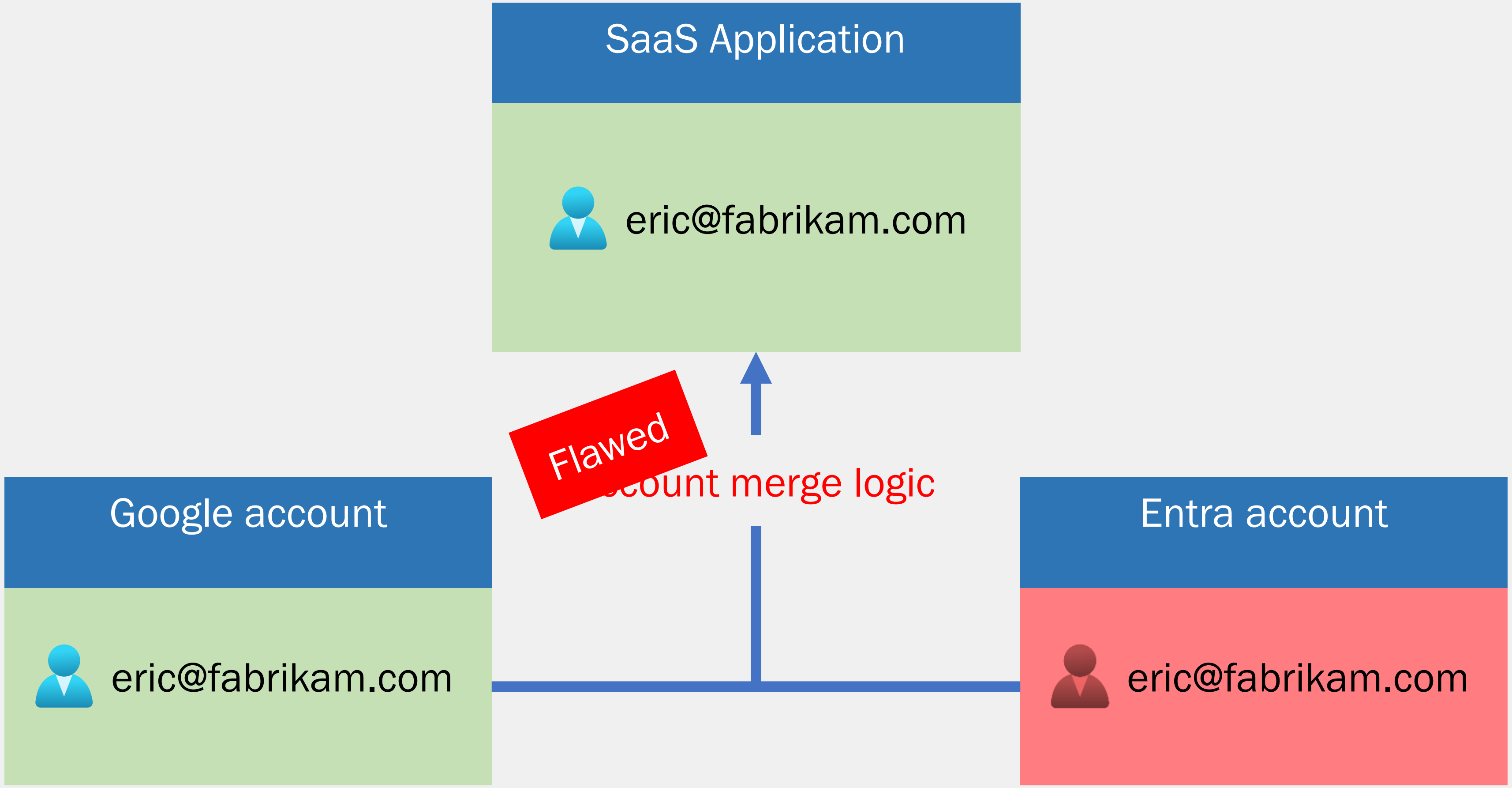
If you did not request that these accounts be connected, please contact us immediately.

Thanks,
Adobe

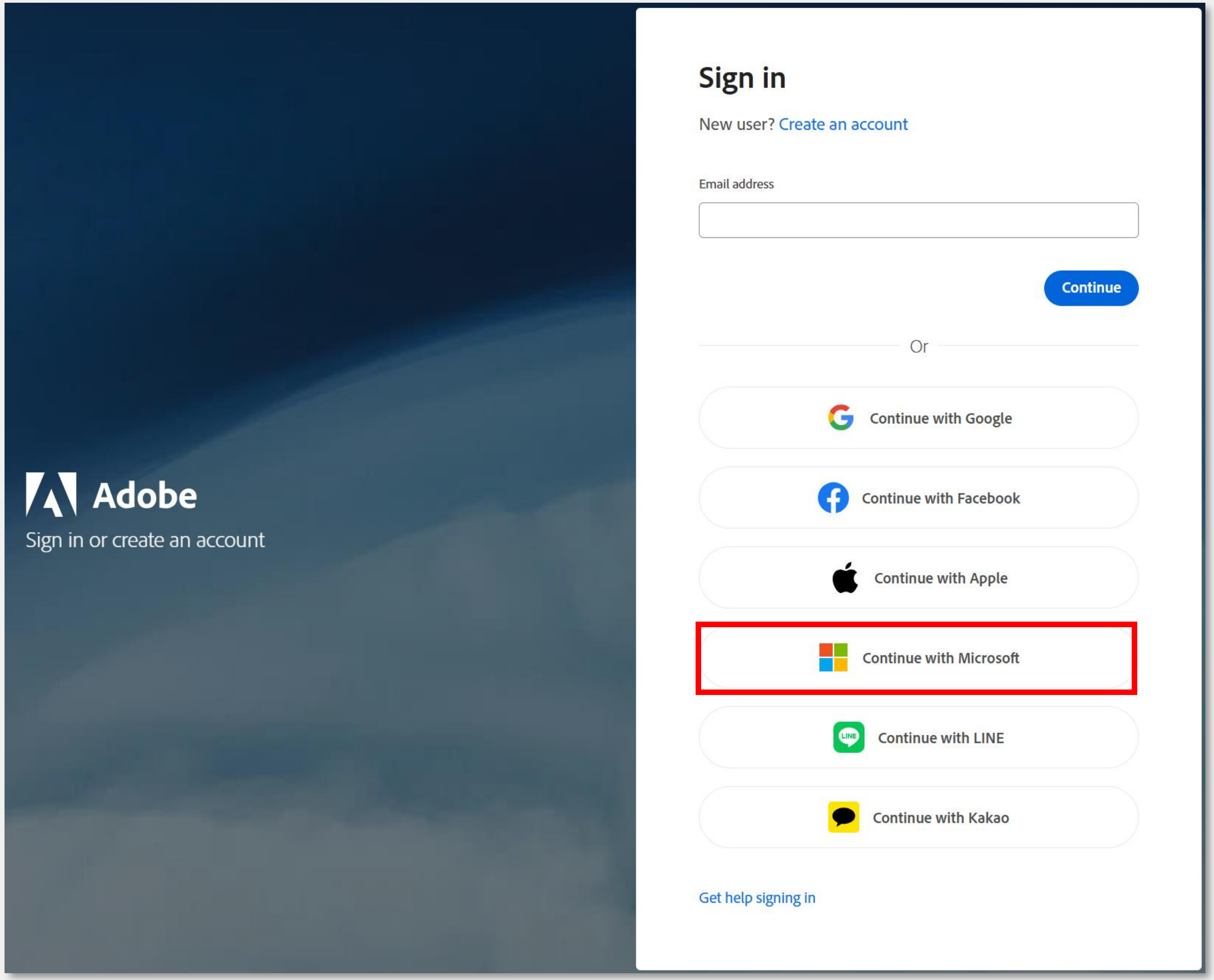
Descope focus



Descope focus



Building on Descopes research



Adobe

Sign in or create an account

Sign in

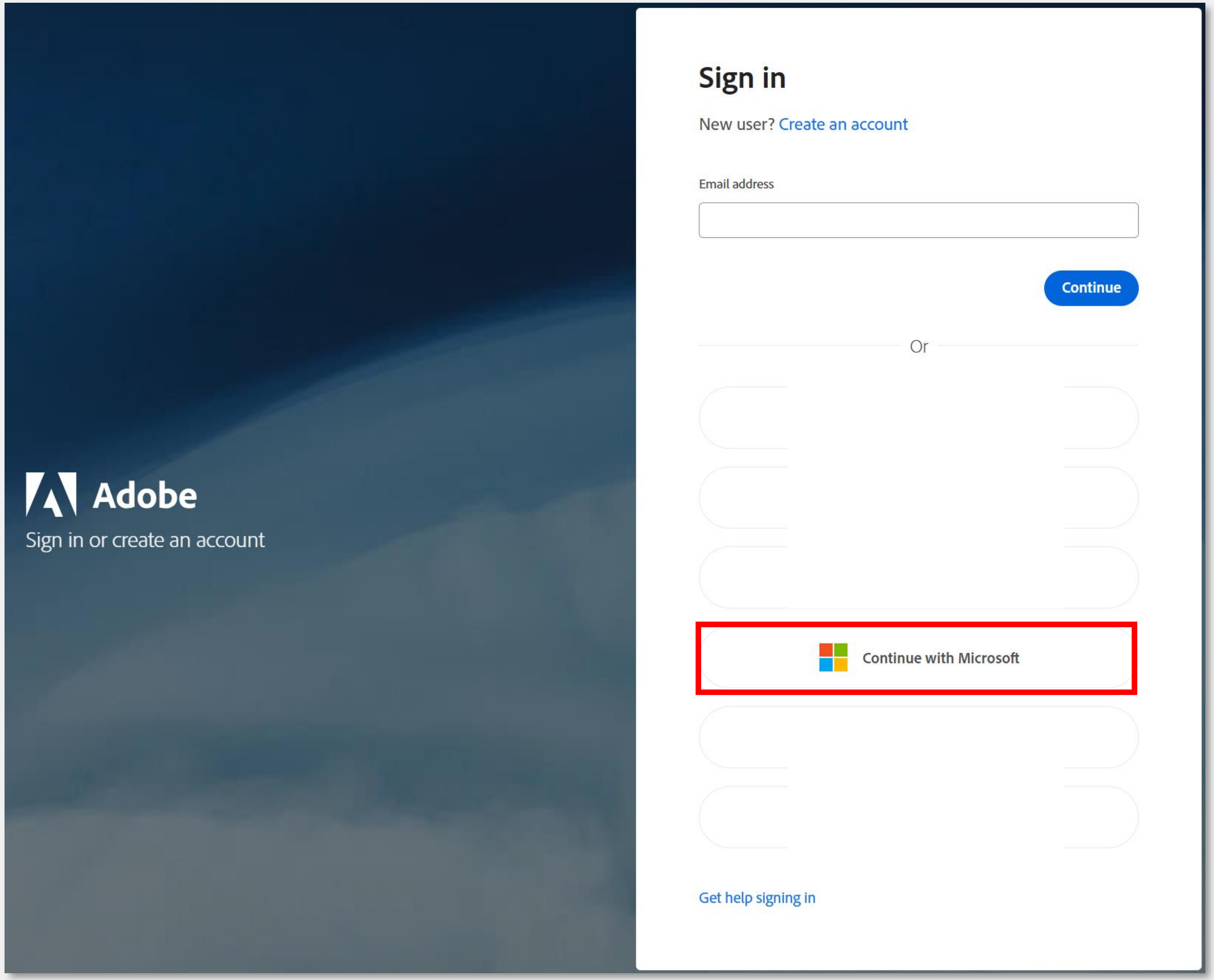
New user? Create an account

Email address

Using Adobe as an example, it is not vulnerable to nOAuth

1. Legitimate user authenticates with Entra
2. Attacker configures attack Entra tenant
3. Attacker authenticates with Entra with unverified email attribute
4. Application is not following OpenID Connect standards
5. Attacker overtakes account with a cross-tenant type attack

Building on Descopes research



Adobe

Sign in or create an account

Sign in

New user? Create an account

Email address

Continue

Or

Continue with Microsoft

Get help signing in

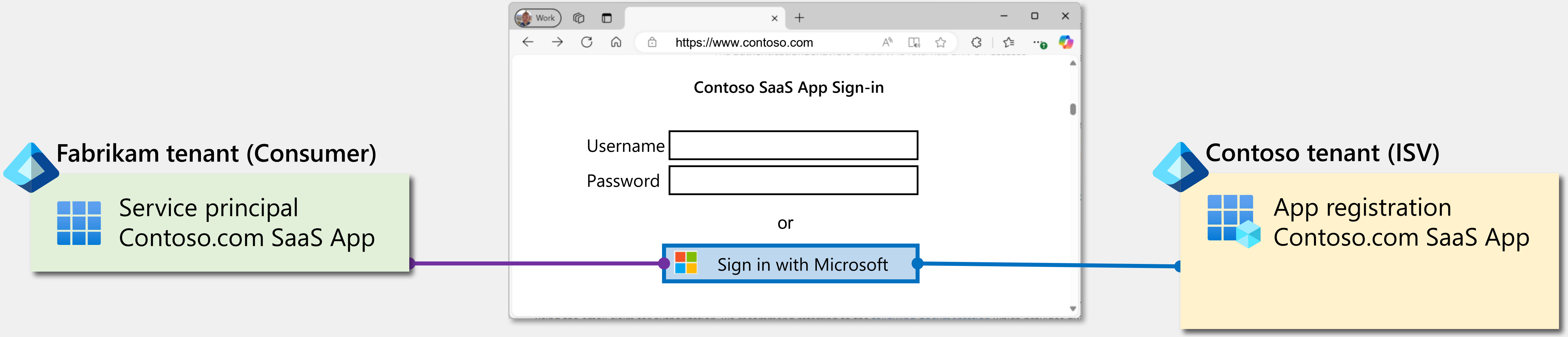
Using Adobe as an example, it is not vulnerable to nOAuth

1. Legitimate user authenticates with Entra
2. Attacker configures attack Entra tenant
3. Attacker authenticates with Entra with unverified email attribute
4. Application is not following OpenID Connect standards
5. Attacker overtakes account with a cross-tenant type attack

semperis

The Cross-tenant attack problem

App registrations and service principals



Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

https://www.contoso.com

Contoso SaaS App Sign-in

Username

Password

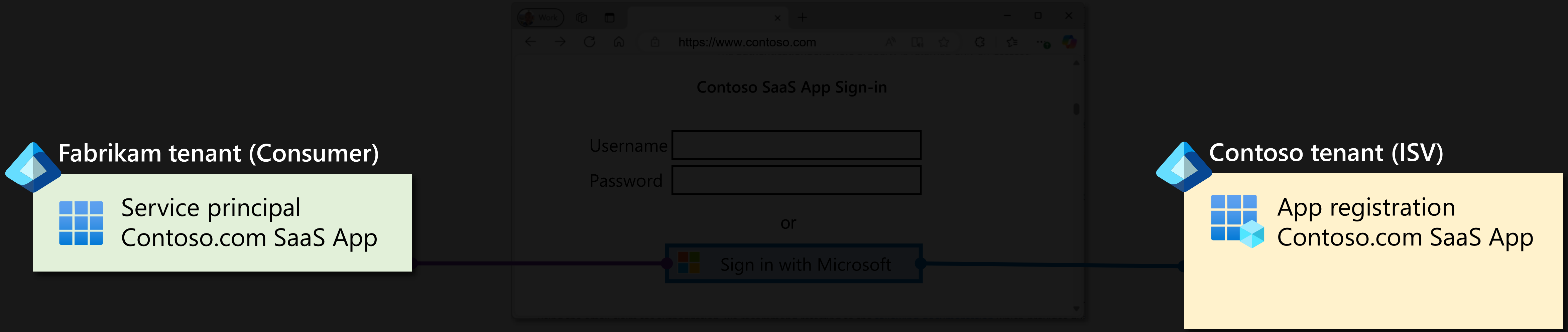
or

Sign in with Microsoft

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

App registrations and service principals



Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

https://www.contoso.com

Contoso SaaS App Sign-in

Username
Password

or

Sign in with Microsoft

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

App registrations and service principals

Service principal

Security principal in consuming tenant

Customer consents to app on first use

Enables AuthN/AuthZ

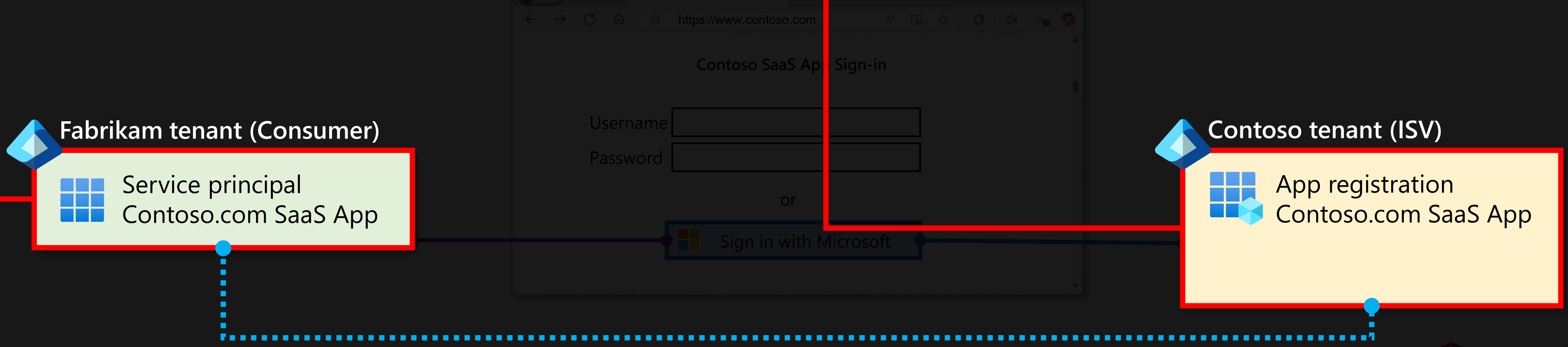
App registration

Defines what the developer needs

Public or confidential client

Redirect URIs

Claims

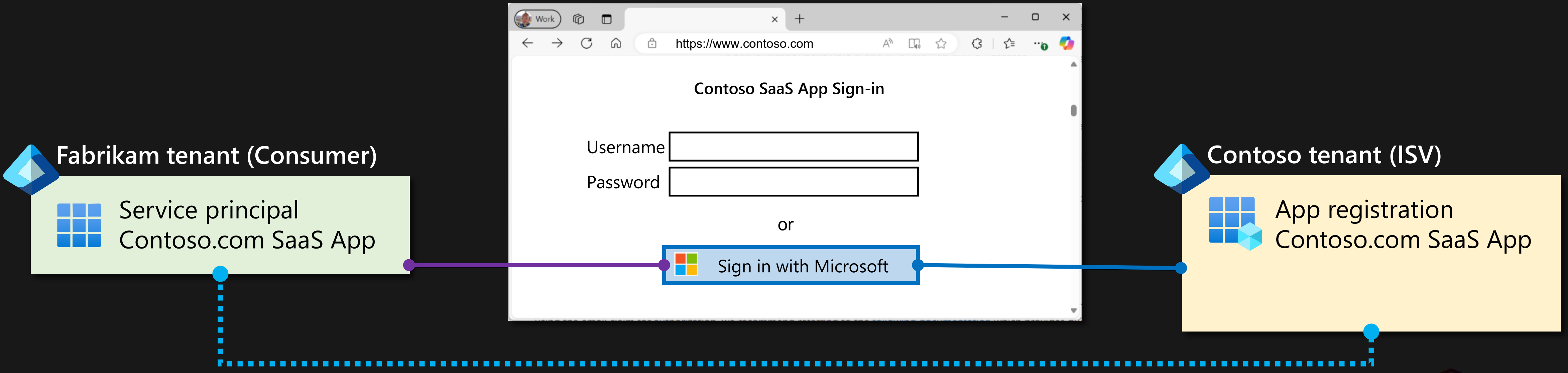


Multi-tenant OAuth / OIDC endpoints

Common Endpoints

Enabled multi-tenant applications

```
https://login.microsoftonline.com/common/oauth2/v2.0/authorize
https://login.microsoftonline.com/common/oauth2/v2.0/token
```



Contoso SaaS App Sign-in

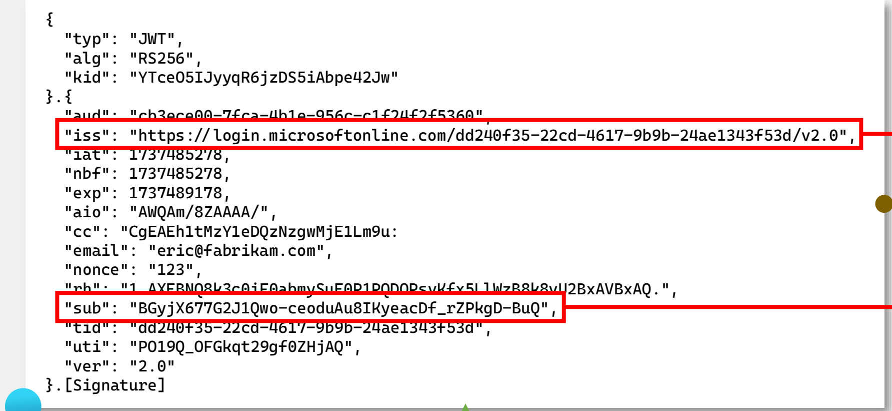
Username

Password

or

Sign in with Microsoft

Following the OpenID Connect spec



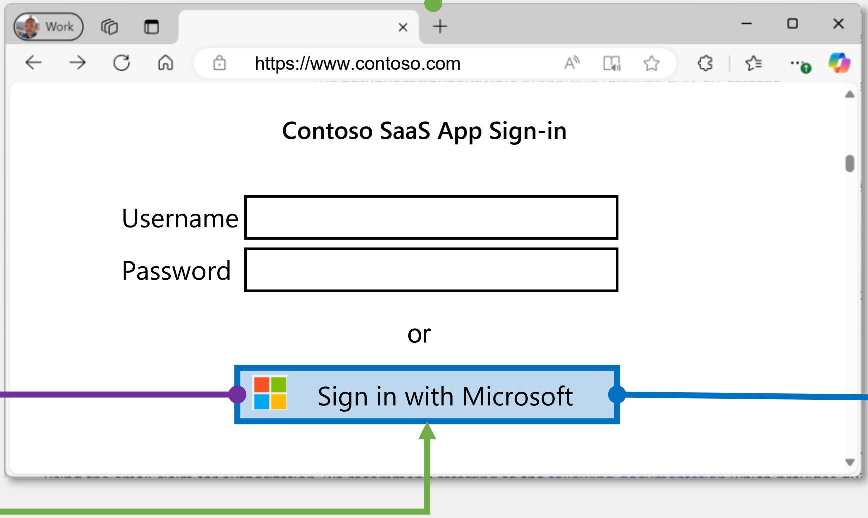
```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/dd240f35-22cd-4617-9b9b-24ae1343f53d/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAEh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iE0abmySuE0R1PQDQPsyKfx5LlWzB8k8yU2BxAVBxAQ.",
  "sub": "BGyjX677G2J1Qwo-ceoduAu8IKyeacDf_rZPkgD-BuQ",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
Sub:  BGyjX677G2J1Qwo-ceod…
Iss:  dd240f35-22cd…
```

Unique, immutable identifier



Contoso SaaS App Sign-in

Username

Password

or

Sign in with Microsoft

Fabrikam tenant (Consumer)

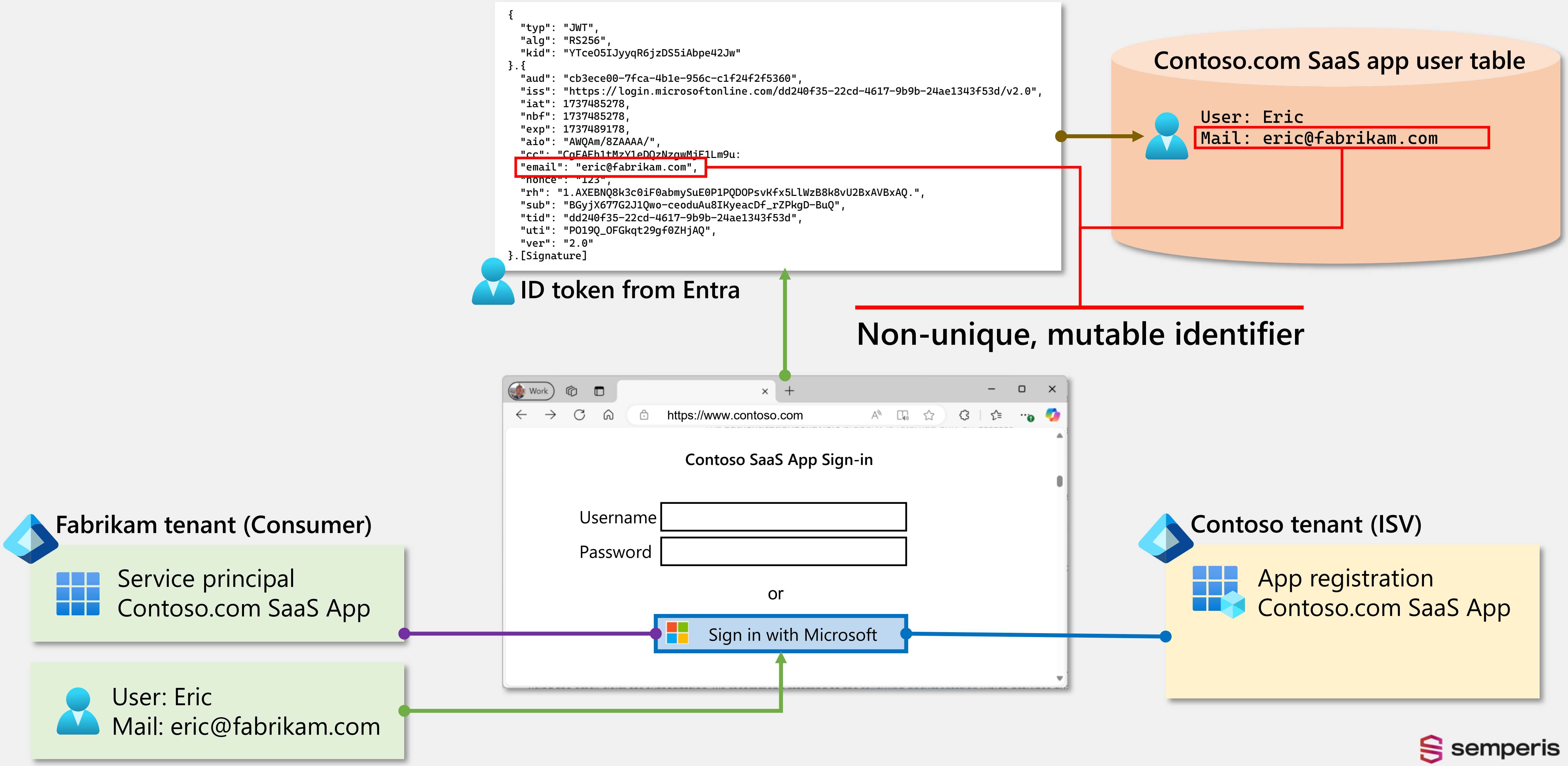
Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

nOAuth vulnerable app



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/dd240f35-22cd-4617-9b9b-24ae1343f53d/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "BGyjX677G2J1Qwo-ceoduAu8IKyeacDf_rZPkgD-BuQ",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Non-unique, mutable identifier

Contoso SaaS App Sign-in

Username

Password

or

Sign in with Microsoft

Fabrikam tenant (Consumer)

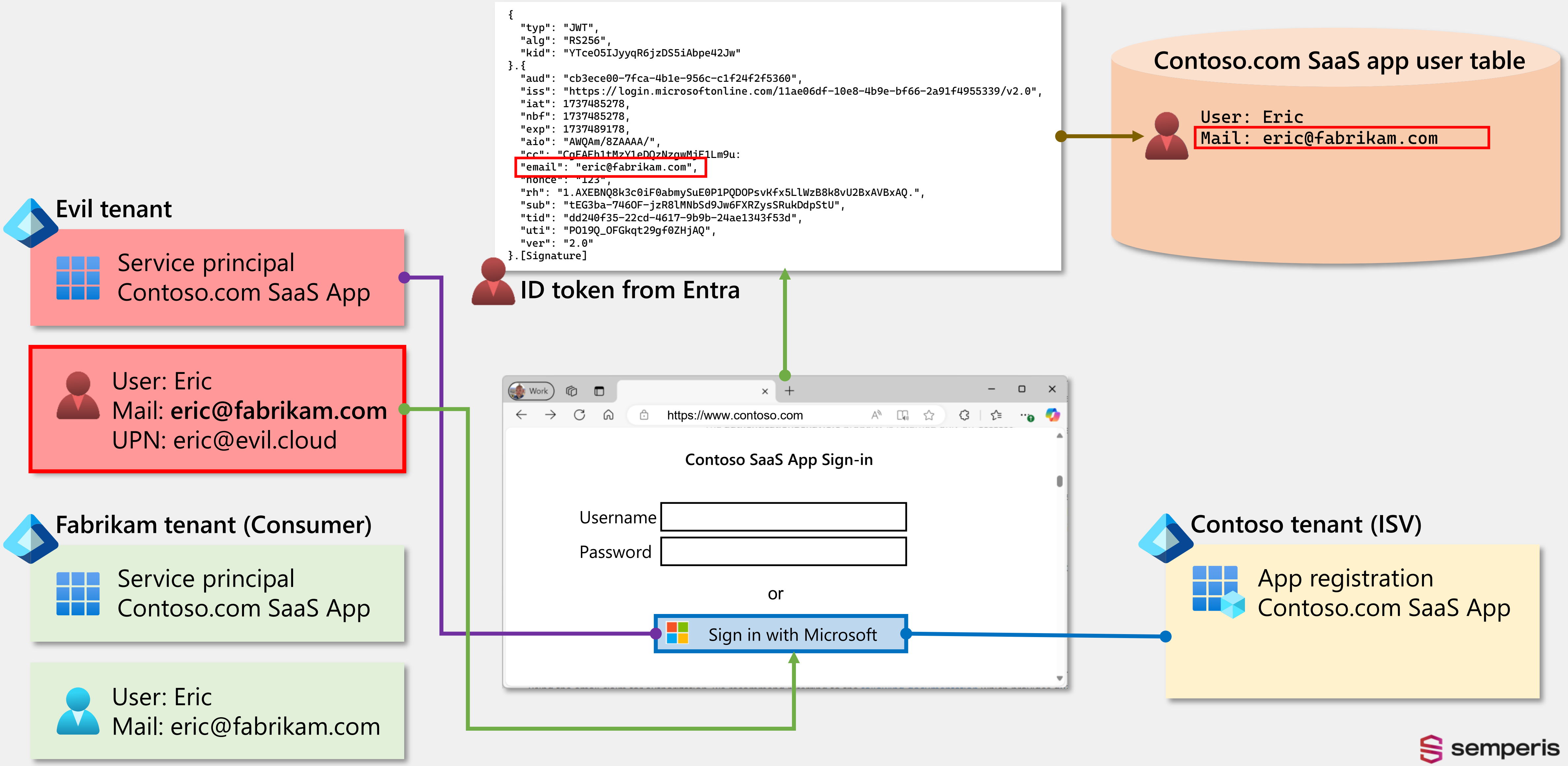
Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

Abusing a nOAuth vulnerable app



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso SaaS App Sign-in

Username
Password

or

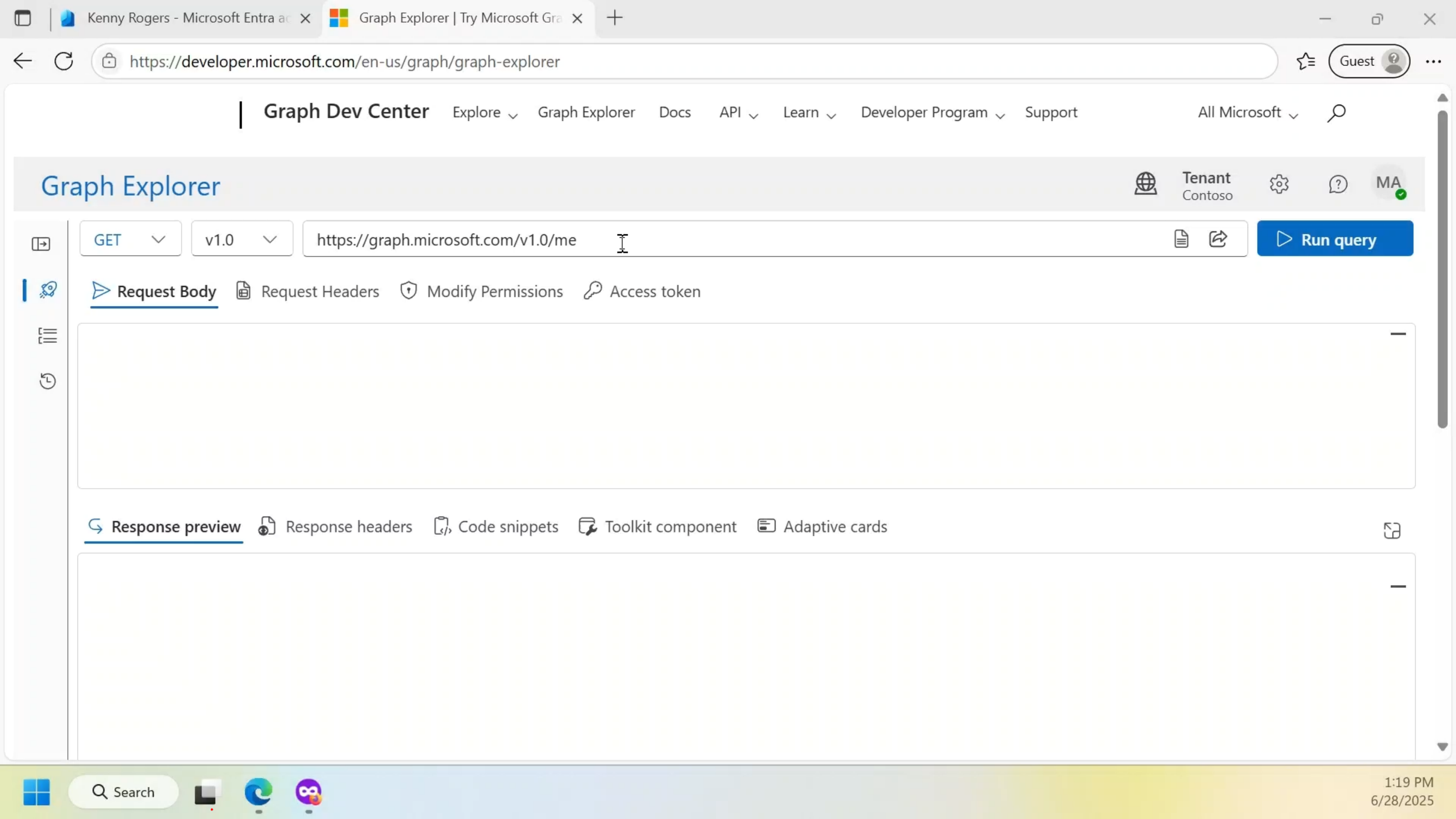
Sign in with Microsoft

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

semperis

Setting an unverified email addresses



https://developer.microsoft.com/en-us/graph/graph-explorer

GET v1.0 https://graph.microsoft.com/v1.0/me

Other methods for setting unverified email address

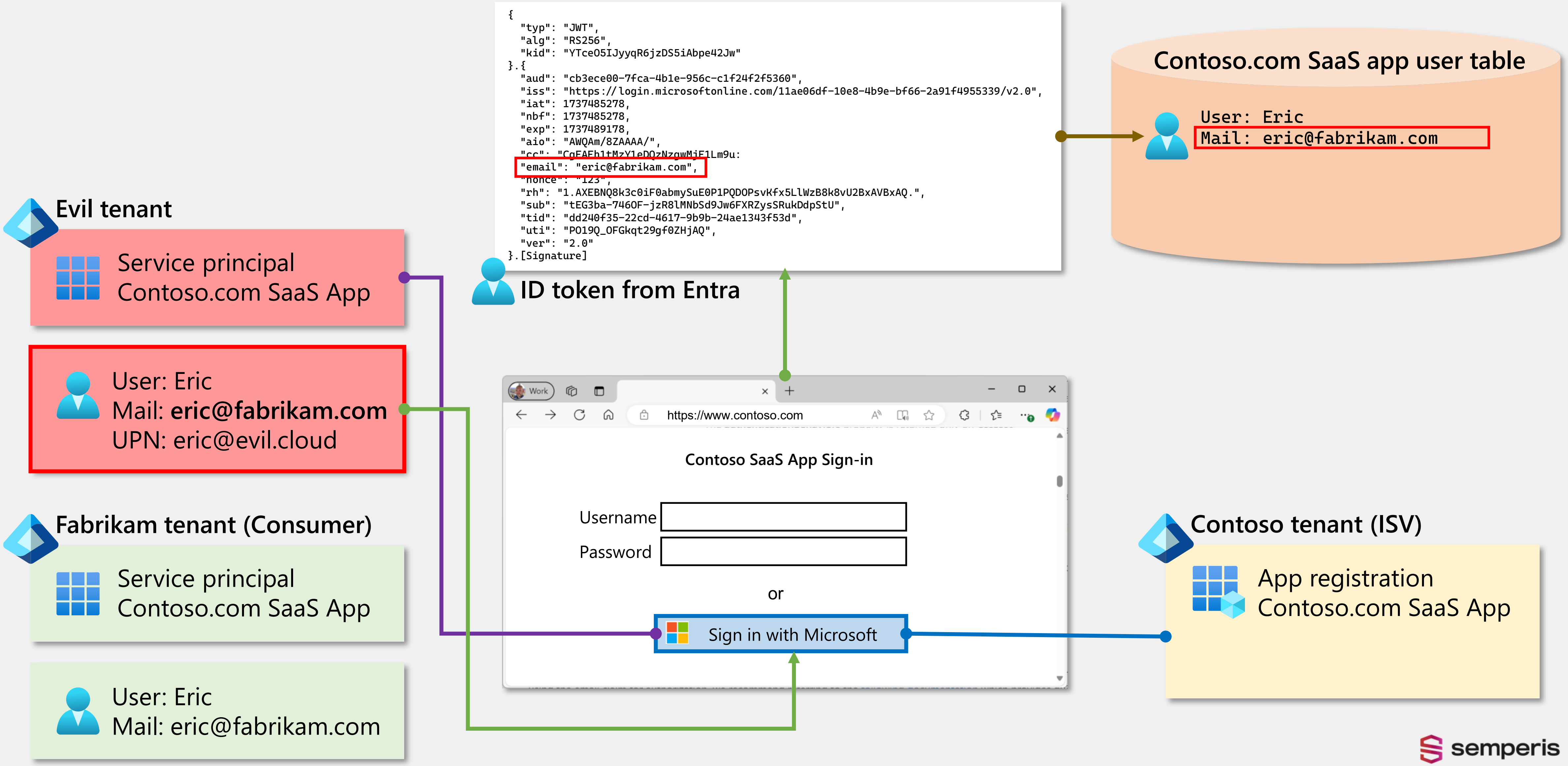
Convert guest invite to member

Hybrid synced user

semperis

Examining claims with jwt.ms

Abusing a nOAuth vulnerable app



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

User: Eric
Mail: eric@fabrikam.com

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

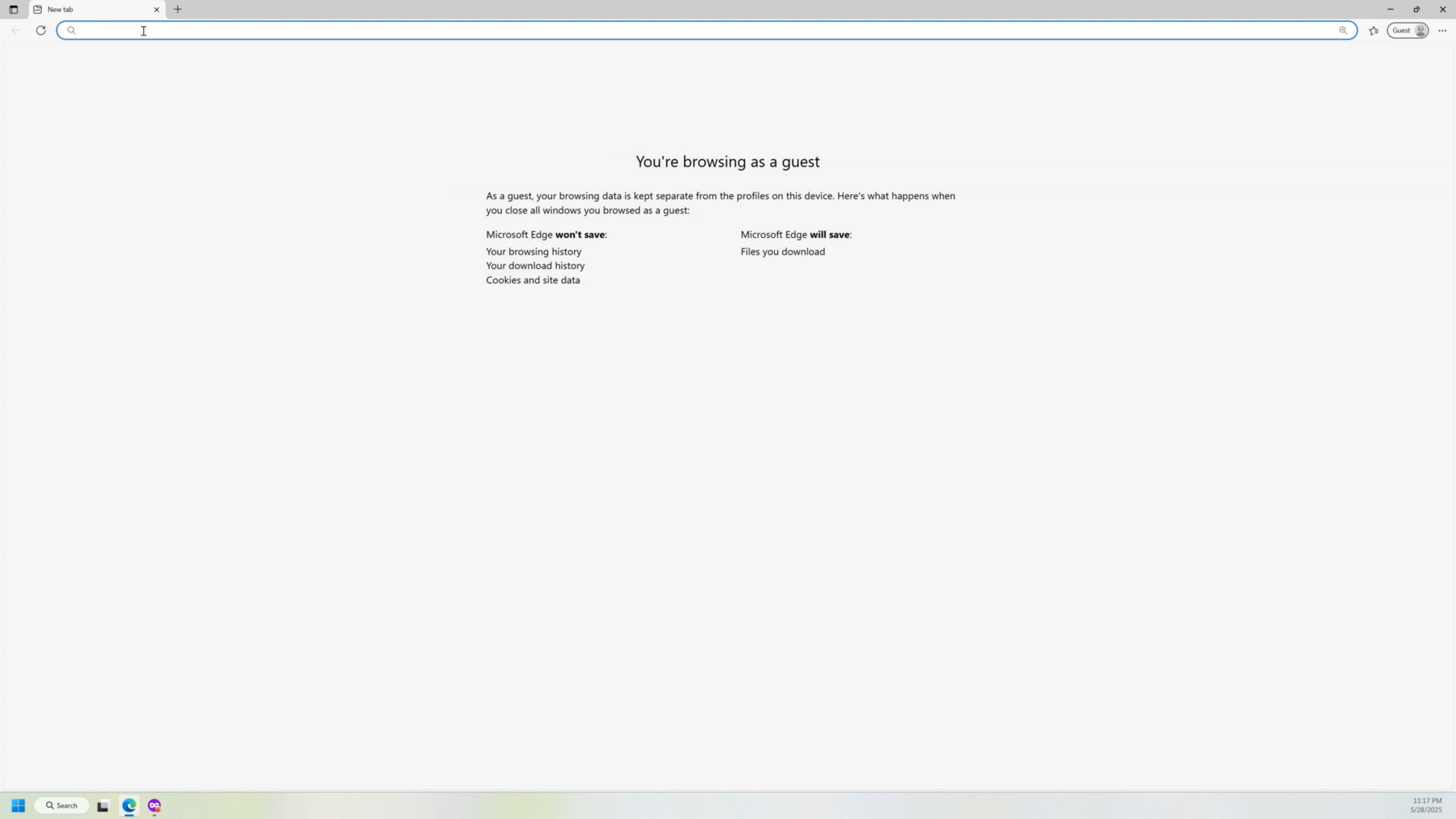
Contoso SaaS App Sign-in

Username

Password

or

Sign in with Microsoft



You're browsing as a guest

As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:

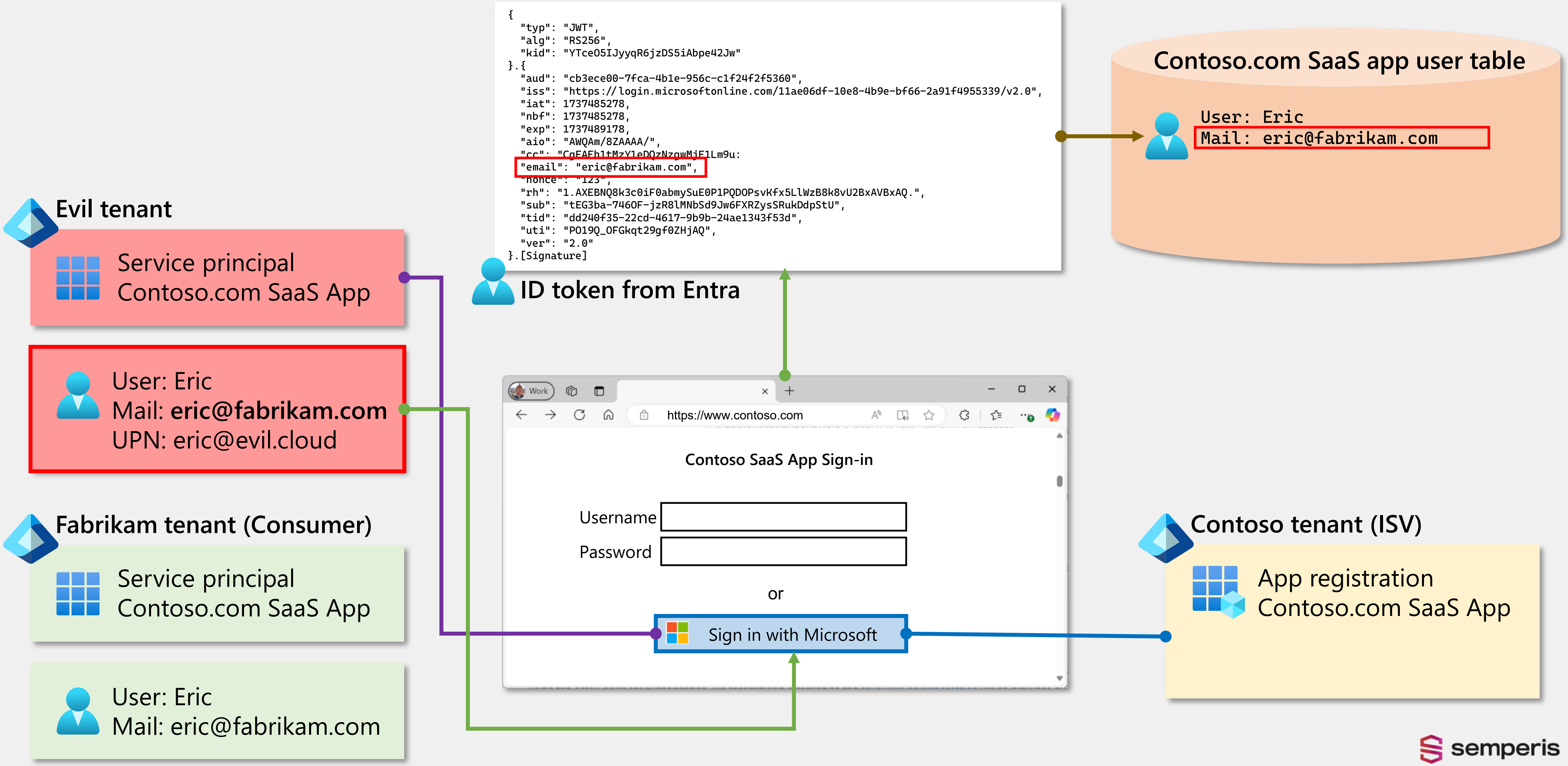
Microsoft Edge **won't save**:

Your browsing history
Your download history
Cookies and site data

Microsoft Edge **will save**:

Files you download

Abusing a nOAuth vulnerable app



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

Contoso SaaS App Sign-in

Username

Password

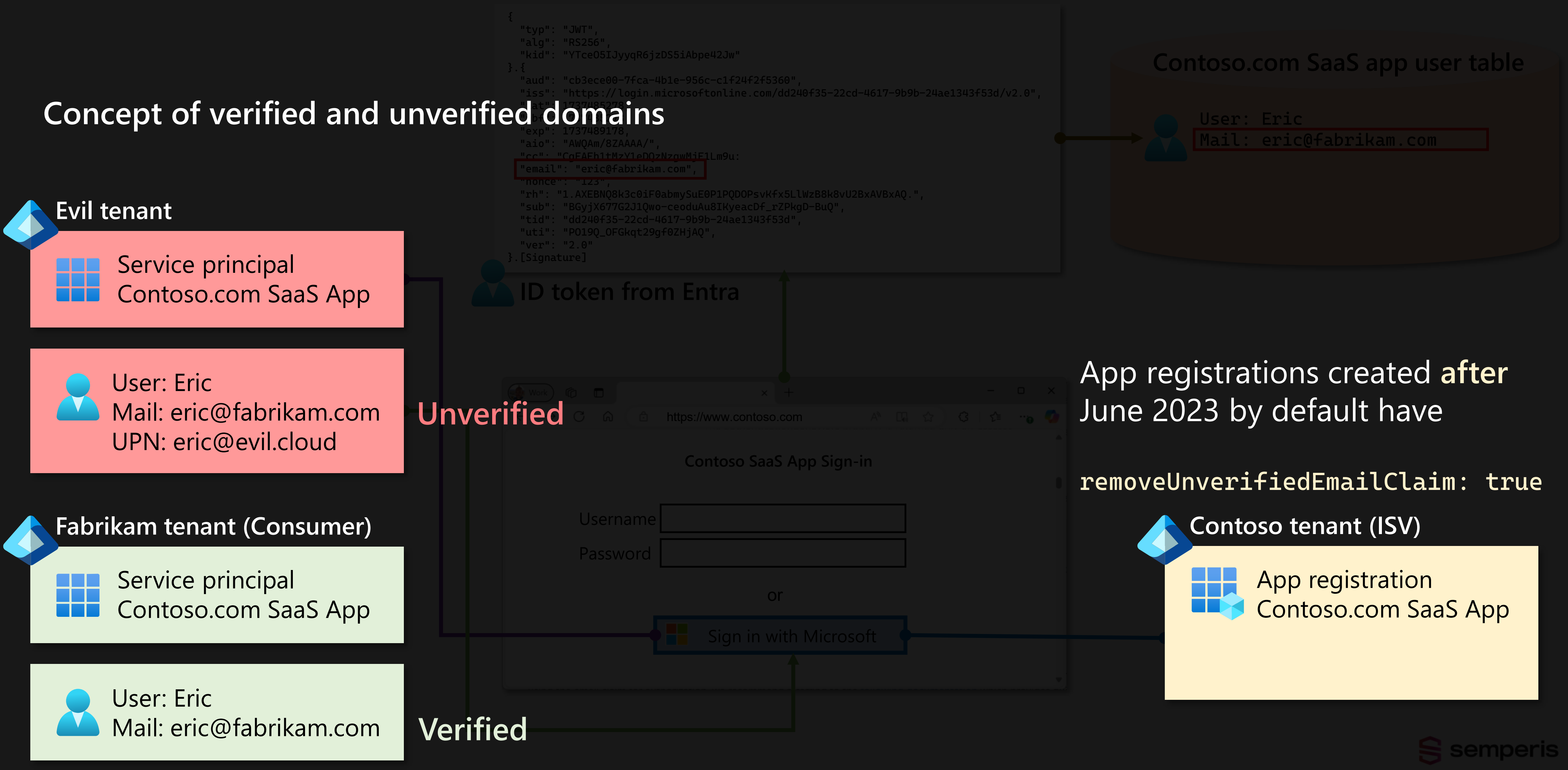
or

Sign in with Microsoft

semperis

Microsoft mitigating controls

Concept of verified and unverified domains



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/dd240f35-22cd-4617-9b9b-24ae1343f53d/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "BGyjX677G2J1Qwo-ceoduAu8IKyeacDf_rZPkgD-BuQ",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

User: Eric
Mail: eric@fabrikam.com

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com
UPN: eric@evil.cloud

Unverified

Contoso SaaS App Sign-in

Username

Password

or

Sign in with Microsoft

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Verified

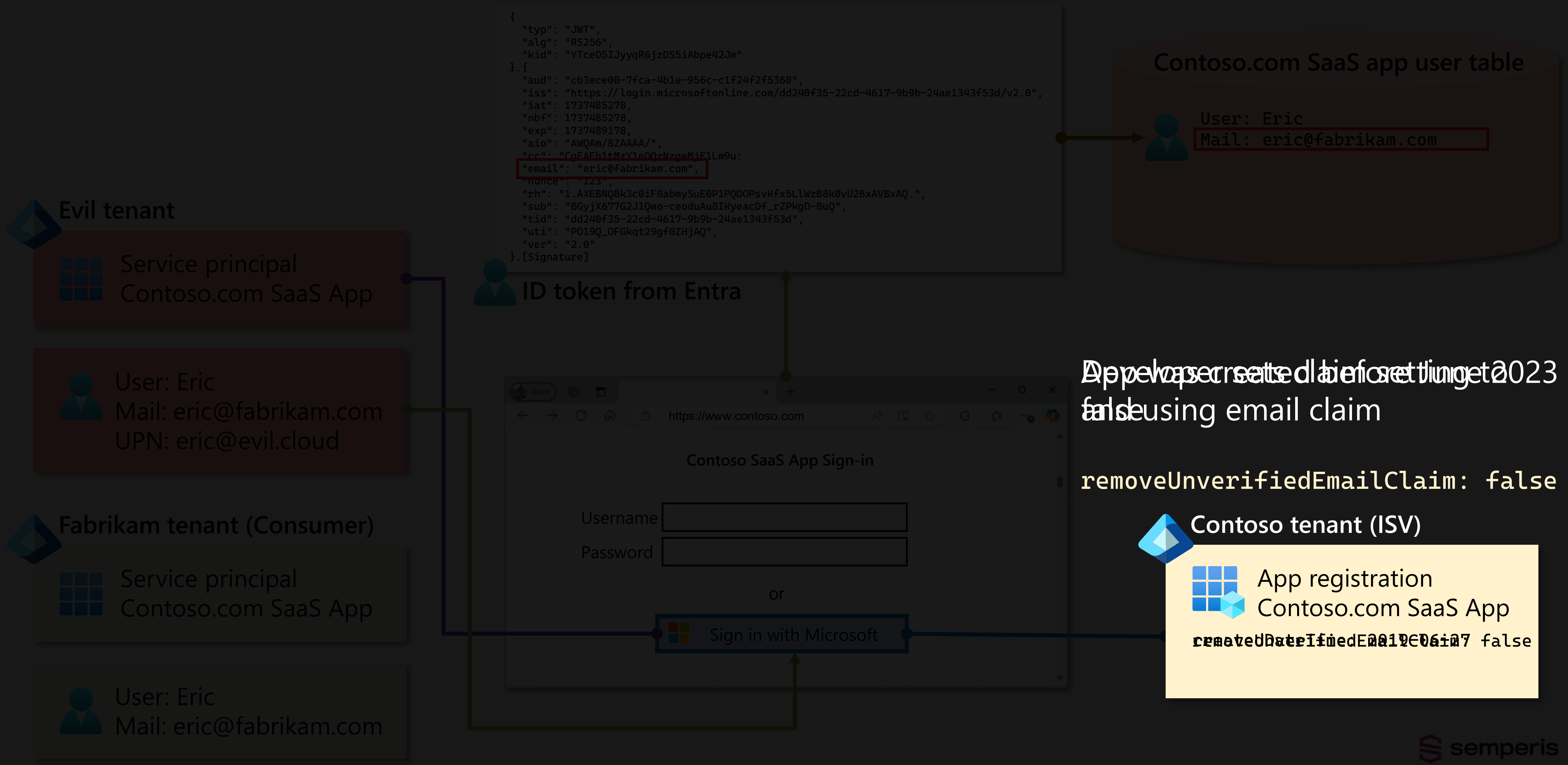
App registrations created **after** June 2023 by default have

`removeUnverifiedEmailClaim: true`

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

Microsoft mitigation bypasses



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/dd240f35-22cd-4617-9b9b-24ae1343f53d/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "BGyjX677G2J1Qwo-ceoduAu8IKyeacDf_rZPkgD-BuQ",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

Developers set claim setting to false

Apps created before June 2023 and using email claim

`removeUnverifiedEmailClaim: false`

Contoso tenant (ISV)

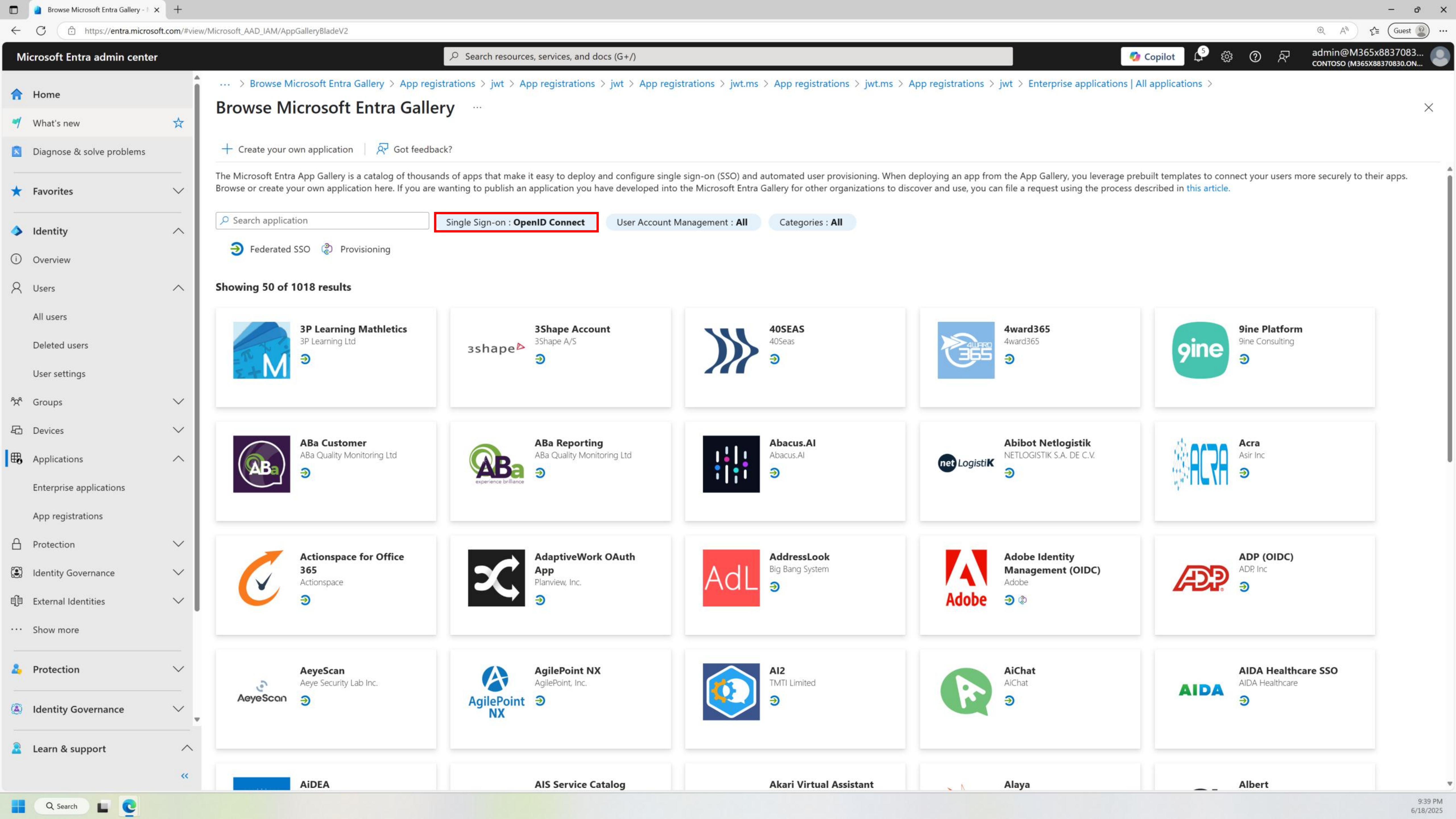
App registration
Contoso.com SaaS App

`createdDateTime 2019-06-27`

`removeUnverifiedEmailClaim: false`

semperis

Researching the Entra Gallery



Browse Microsoft Entra Gallery
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AppGalleryBladeV2
Guest
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
admin@M365x8837083...
CONTOSO (M365X88370830.ON...
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Enterprise applications
App registrations
Protection
Identity Governance
External Identities
Show more
Protection
Identity Governance
Learn & support
... > Browse Microsoft Entra Gallery > App registrations > jwt > App registrations > jwt > App registrations > jwt.ms > App registrations > jwt.ms > App registrations > jwt > Enterprise applications | All applications >
Create your own application
Got feedback?
Search application
Single Sign-on : OpenID Connect
User Account Management : All
Categories : All
Federated SSO
Provisioning
Search
9:39 PM
6/18/2025

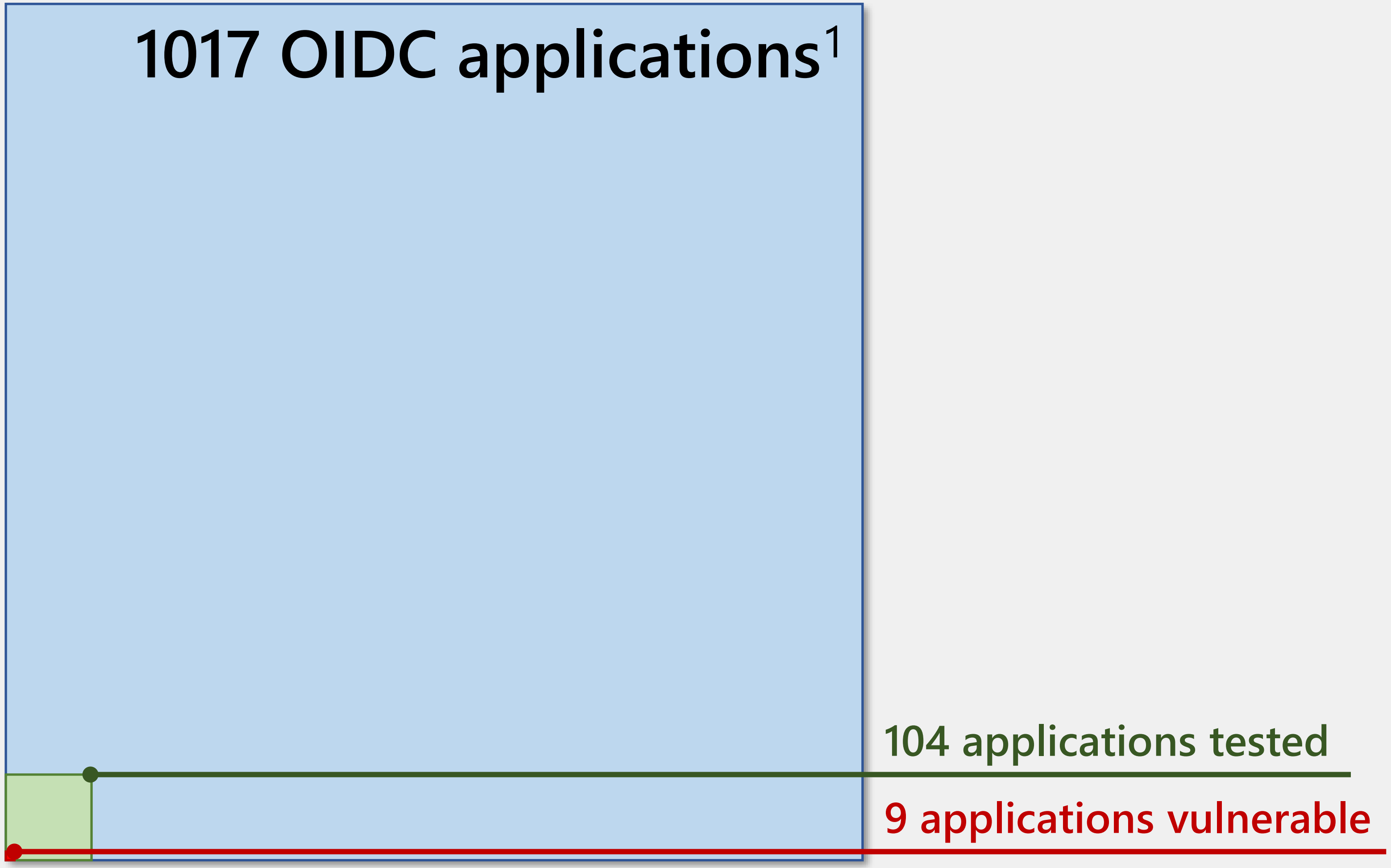
Browse Microsoft Entra Gallery

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Showing 50 of 1018 results

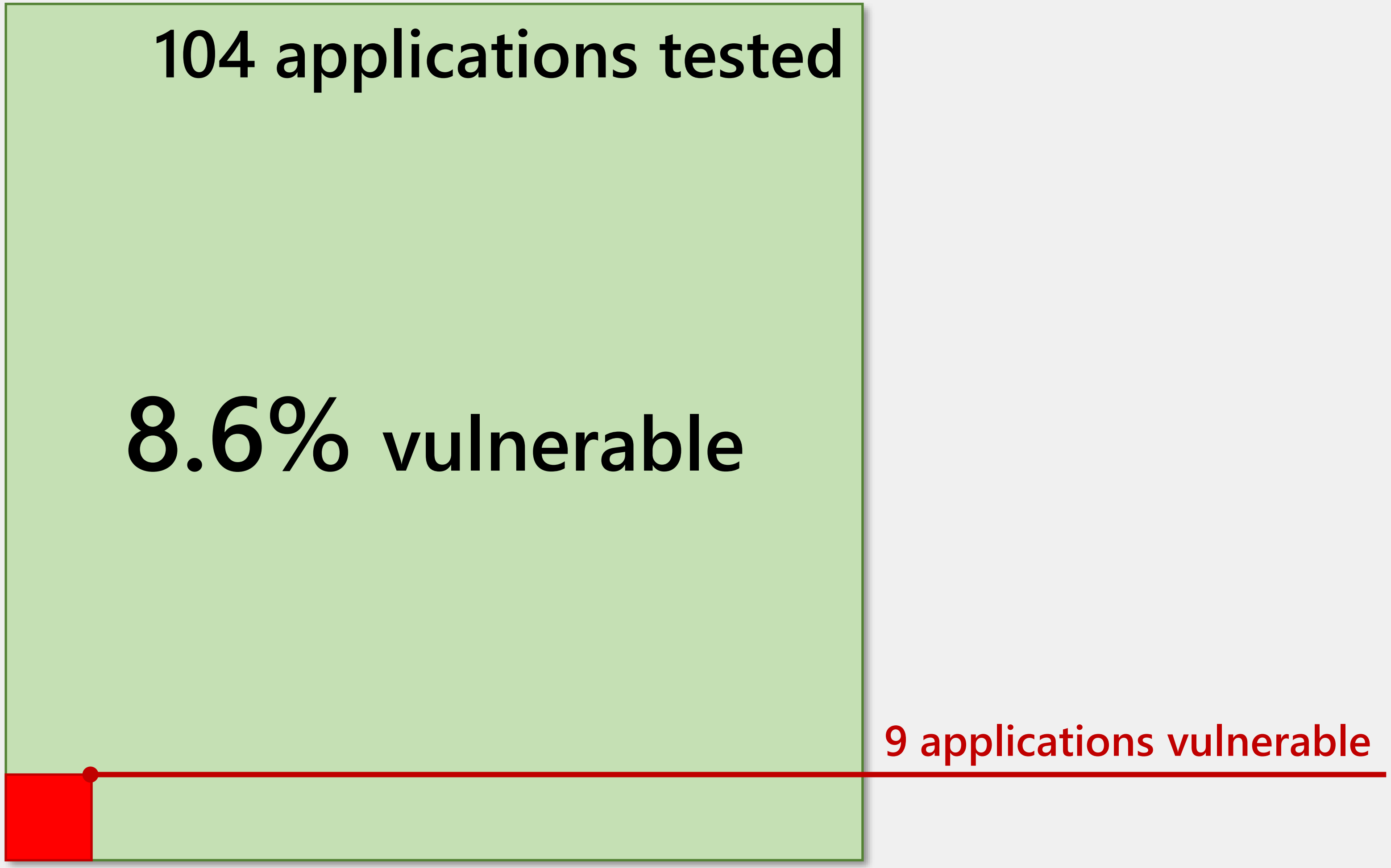
3P Learning Mathletics 3P Learning Ltd	3Shape Account 3Shape A/S	40SEAS 40Seas	4ward365 4ward365	9ine Platform 9ine Consulting
ABa Customer ABa Quality Monitoring Ltd	ABa Reporting ABa Quality Monitoring Ltd	Abacus.AI Abacus.AI	Abibot Netlogistik NETLOGISTIK S.A. DE C.V.	Acra Asir Inc
Actionspace for Office 365 Actionspace	AdaptiveWork OAuth App Planview, Inc.	AddressLook Big Bang System	Adobe Identity Management (OIDC) Adobe	ADP (OIDC) ADP, Inc
AeyeScan Aeye Security Lab Inc.	AgilePoint NX AgilePoint, Inc.	AI2 TMTI Limited	AiChat AiChat	AIDA Healthcare SSO AIDA Healthcare
AiDEA	AIS Service Catalog	Akari Virtual Assistant	Alaya	Albert

Microsoft Entra Gallery



[1] *1017 OIDC applications at time of research, Fall 2024*

Microsoft Entra Gallery



104 applications tested

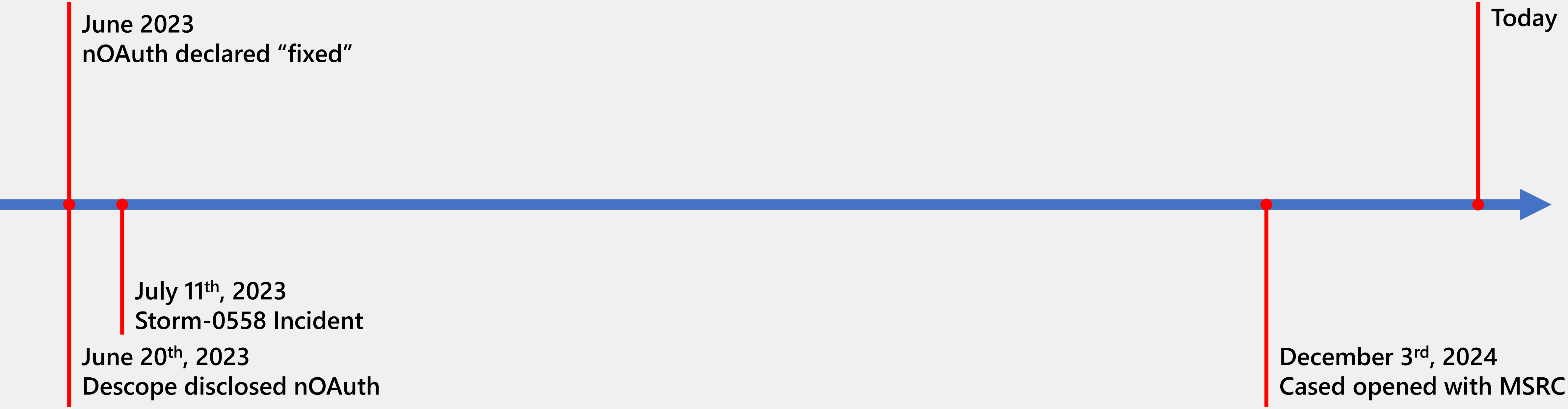
8.6% vulnerable

9 applications vulnerable

How many applications are vulnerable?

- Nobody can really know
- It’s probably more than 10
- Microsoft should know how many apps consuming using unverified email claim
- Consumption != vulnerable

Timeline



June 2023
nOAuth declared “fixed”

June 20th, 2023
Descope disclosed nOAuth

July 11th, 2023
Storm-0558 Incident

December 3rd, 2024
Cased opened with MSRC

Today

The nine applications

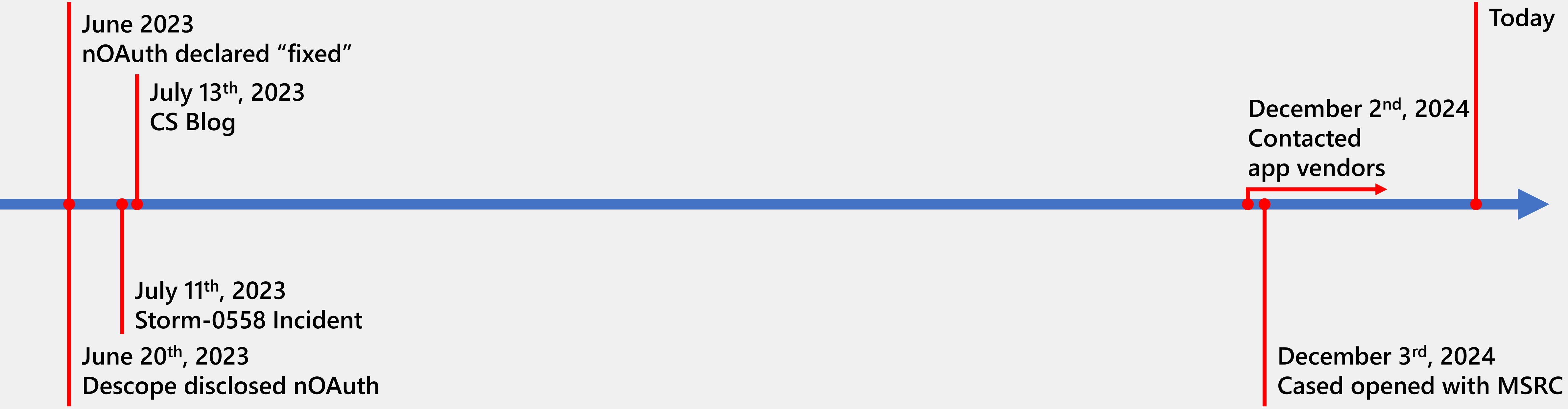
The applications

- HRMS (human resources) platform with PII
- Redacted platform with PII
- Three knowledge sharing/collaboration platforms
- Redacted platform with 45,000+ customers (vendor claimed)
- Business coaching platform with O365 integration
- Construction site management platform
- Meeting scheduling platform with O365 integration

semperis

The application vendor response

Timeline



June 2023
nOAuth declared “fixed”

June 20th, 2023
Descope disclosed nOAuth

July 11th, 2023
Storm-0558 Incident

July 13th, 2023
CS Blog

December 2nd, 2024
Contacted
app vendors

December 3rd, 2024
Cased opened with MSRC

Today

Application vendor response

- Quickest resolution was within one week
- Longest resolution is still ongoing

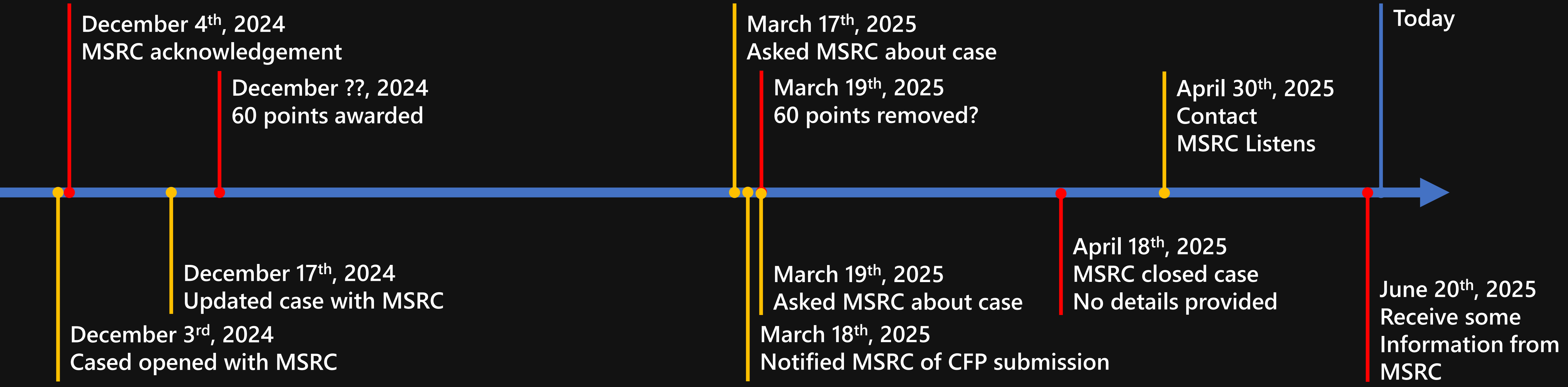
- Variation in how easy it was to report the problem
- Variation in how the vendor responded, if at all

- Some systems appear to have removed Entra integration
- Some systems have put up a paywall that prohibits testing

semperis

The MSRC Case

MSRC Case



December 3rd, 2024
Cased opened with MSRC

December 4th, 2024
MSRC acknowledgement

December 17th, 2024
Updated case with MSRC

December ??, 2024
60 points awarded

March 17th, 2025
Asked MSRC about case

March 18th, 2025
Notified MSRC of CFP submission

March 19th, 2025
60 points removed?

March 19th, 2025
Asked MSRC about case

April 18th, 2025
MSRC closed case
No details provided

April 30th, 2025
Contact
MSRC Listens

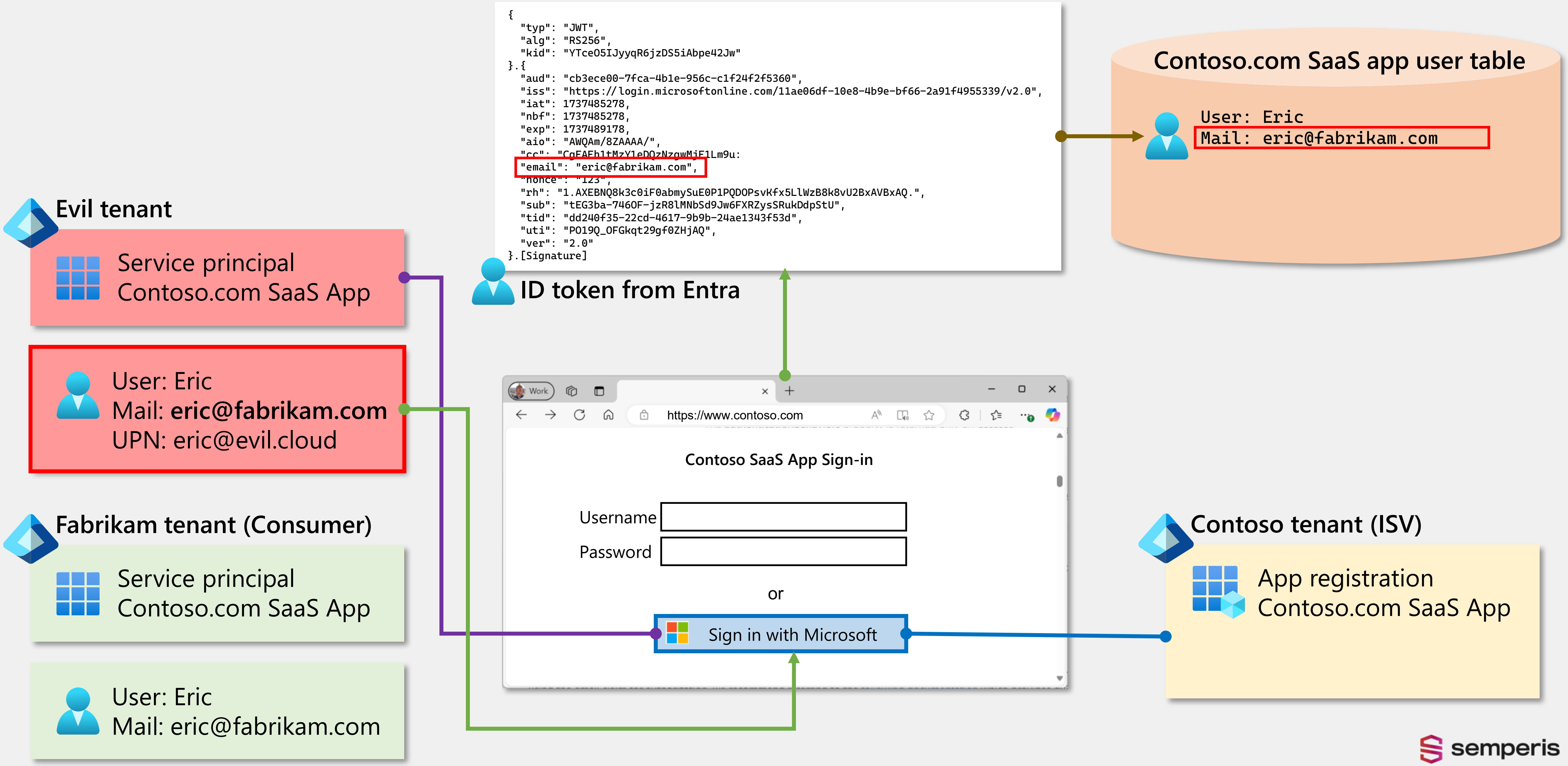
June 20th, 2025
Receive some
Information from
MSRC

Today

semperis

Defense and Mitigation

Mitigation and defense: Customer side



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTce05IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

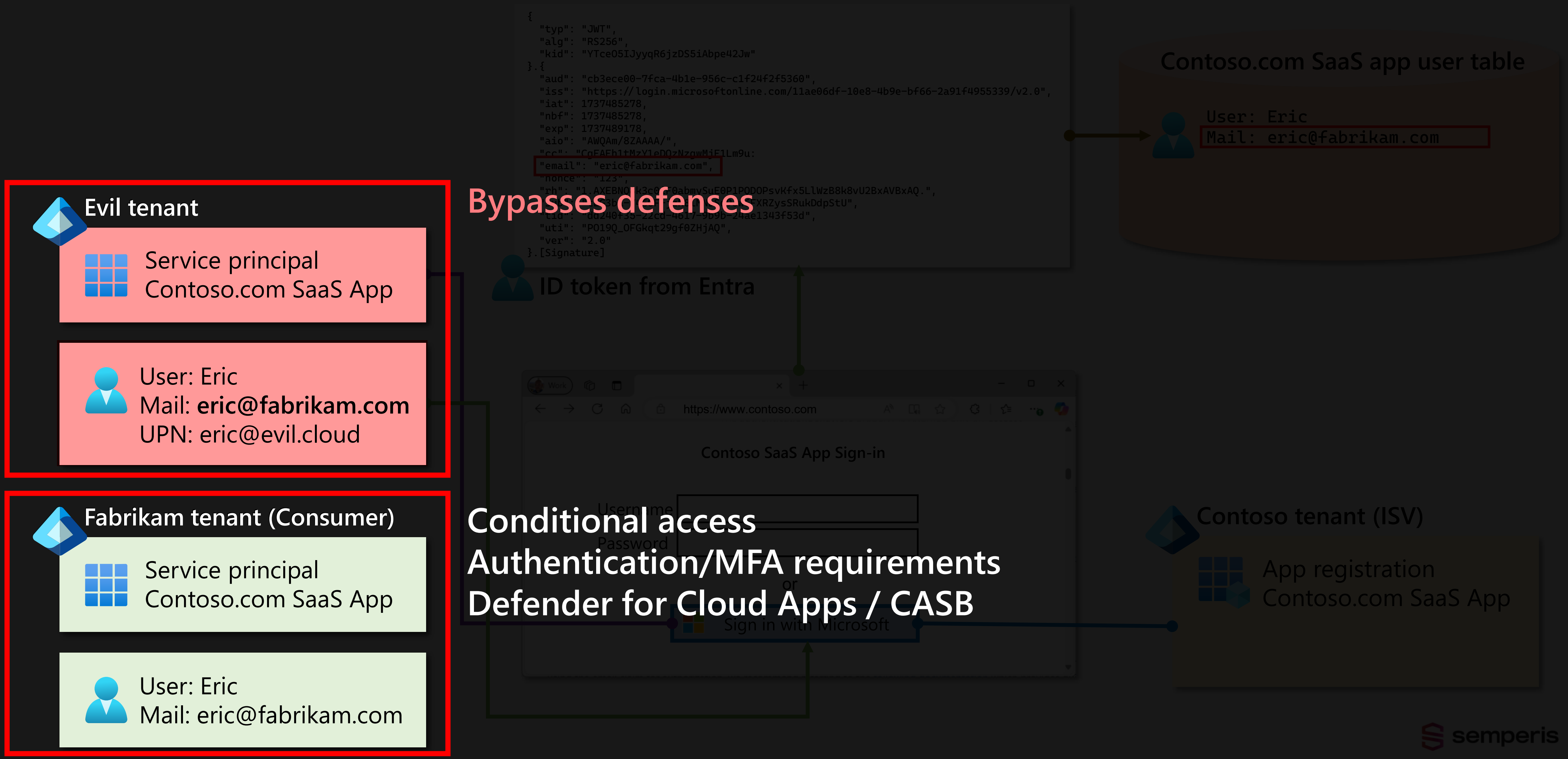
User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

semperis

Mitigation and defense: Customer side



Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Bypasses defenses

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Conditional access
Authentication/MFA requirements
Defender for Cloud Apps / CASB

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFb1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ[illegible]k3c0[illegible]F0abmySuE0P1PODOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "[illegible]FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

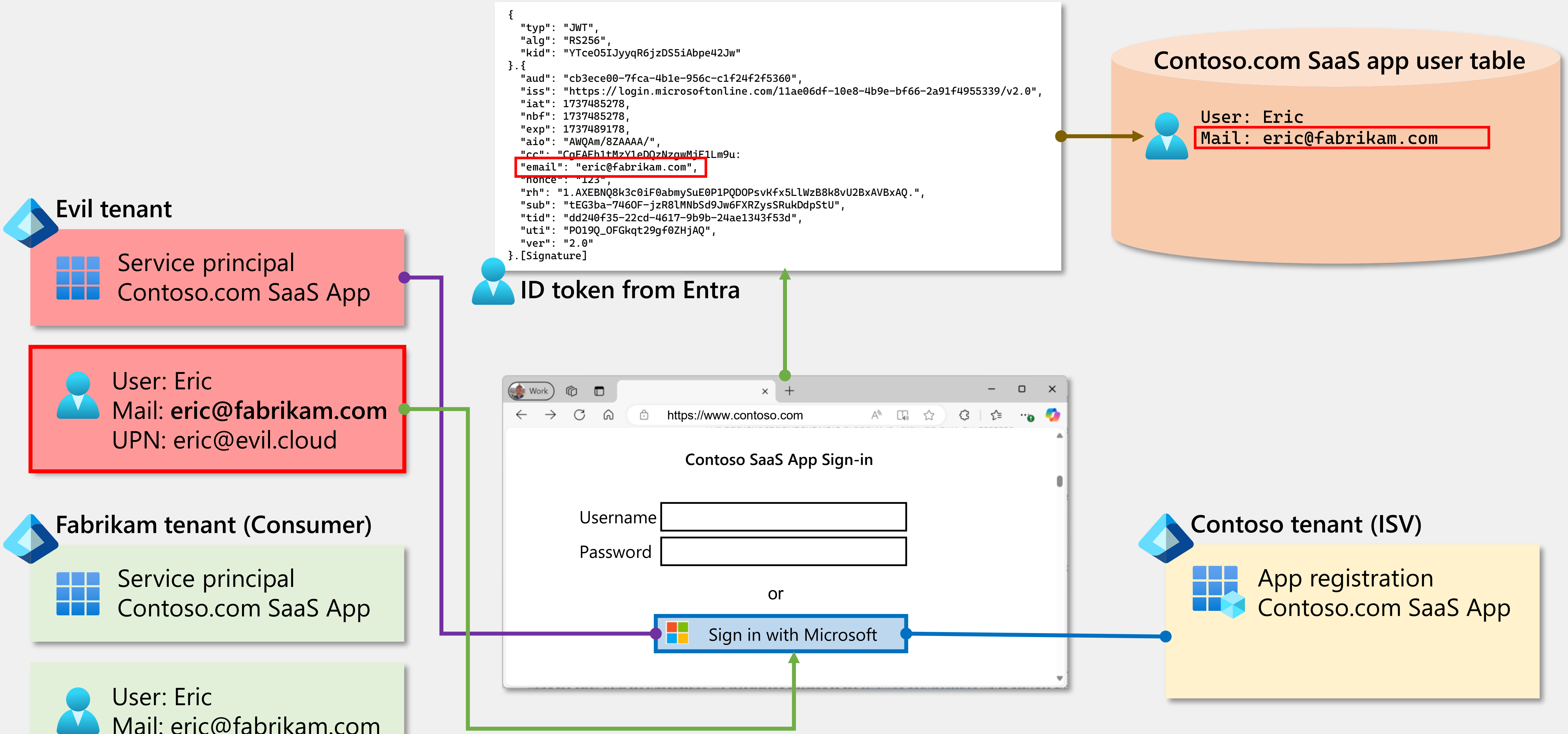
Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

Mitigation and defense: Customer side



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso SaaS App Sign-in

Username

Password

or

Sign in with Microsoft

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

semperis

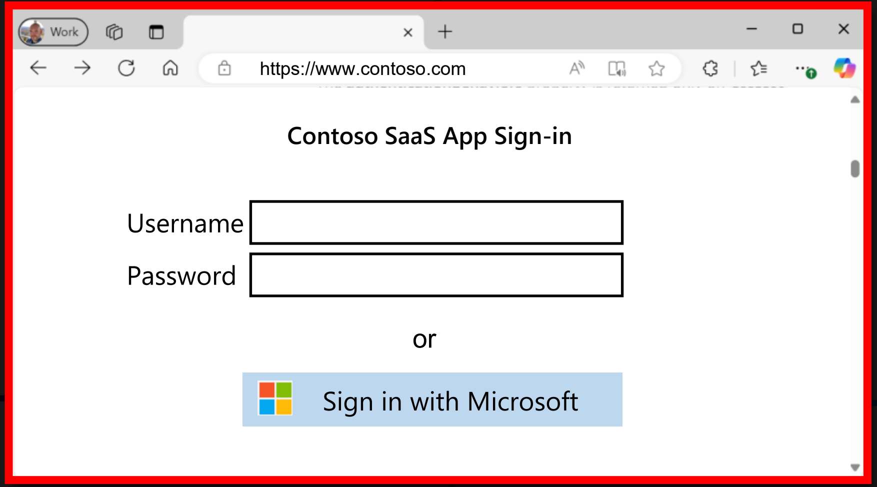
Mitigation and defense: Customer side

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFh1tMzY1eDQzNzgwMjF1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

- ❌ SaaS Security Posture Management (SSPM)
- ❌ Browser Extensions



https://www.contoso.com

Contoso SaaS App Sign-in

Username

Password

or

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

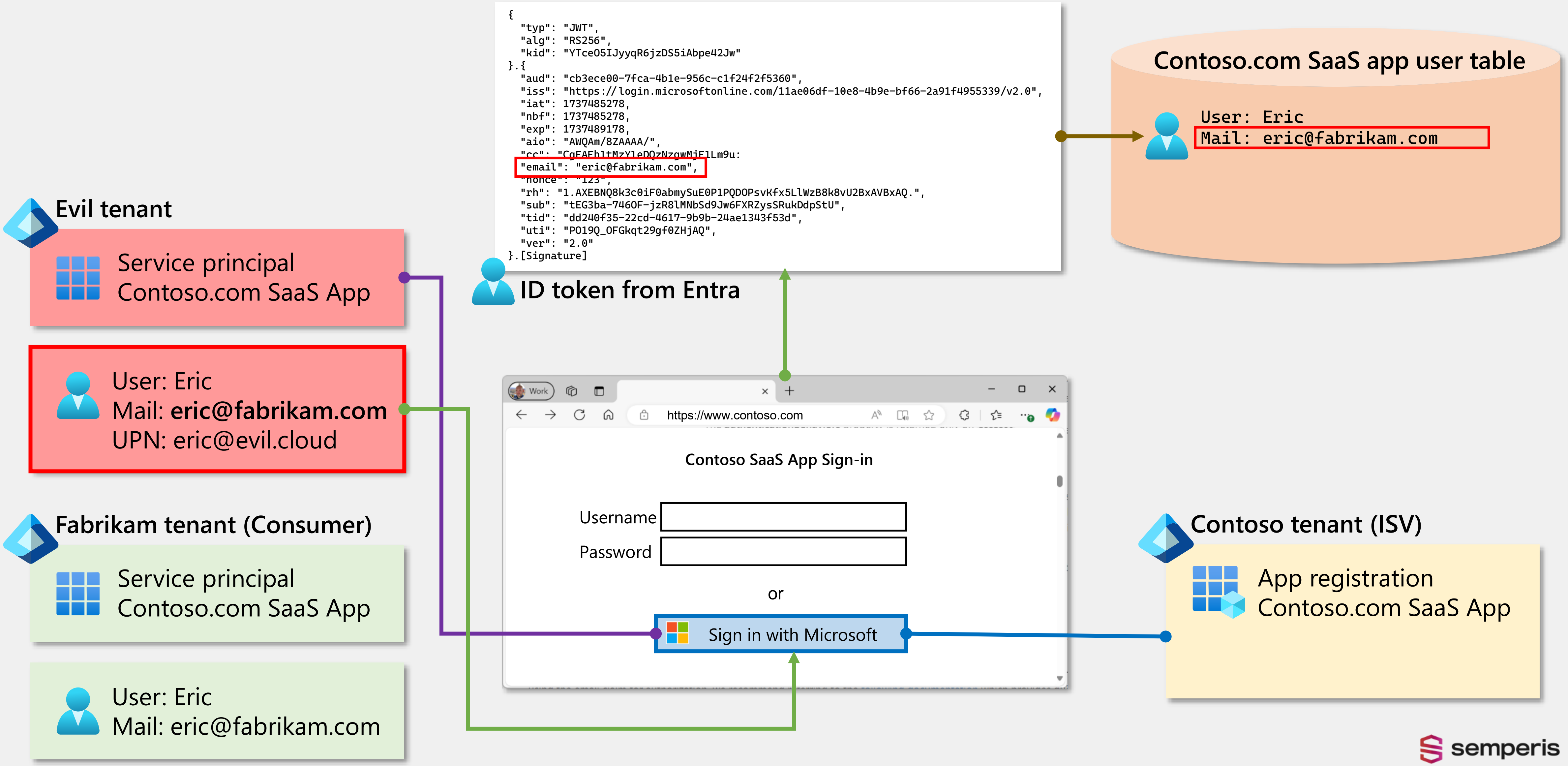
Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

Detection: customer side



```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "YTceO5IJyyqR6jzDS5iAbpe42Jw"
}.{
  "aud": "cb3ece00-7fca-4b1e-956c-c1f24f2f5360",
  "iss": "https://login.microsoftonline.com/11ae06df-10e8-4b9e-bf66-2a91f4955339/v2.0",
  "iat": 1737485278,
  "nbf": 1737485278,
  "exp": 1737489178,
  "aio": "AWQAm/8ZAAAA/",
  "cc": "CgEAFb1tMzY1eDQzNzgwMjE1Lm9u:
  "email": "eric@fabrikam.com",
  "nonce": "123",
  "rh": "1.AXEBNQ8k3c0iF0abmySuE0P1PQDOPsvKfx5LlWzB8k8vU2BxAVBxAQ.",
  "sub": "tEG3ba-746OF-jzR8lMNbSd9Jw6FXRZysSRukDdpStU",
  "tid": "dd240f35-22cd-4617-9b9b-24ae1343f53d",
  "uti": "PO19Q_OFGkqt29gf0ZHjAQ",
  "ver": "2.0"
}.[Signature]
```

ID token from Entra

Contoso.com SaaS app user table

```
User: Eric
Mail: eric@fabrikam.com
```

Evil tenant

Service principal
Contoso.com SaaS App

User: Eric
Mail: **eric@fabrikam.com**
UPN: eric@evil.cloud

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

Contoso SaaS App Sign-in

Username

Password

or

Sign in with Microsoft

semperis

Detection: customer side log correlation

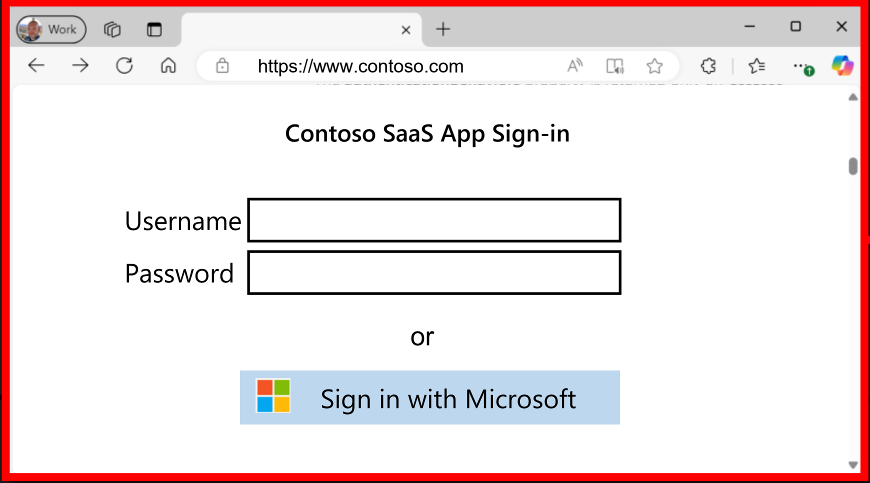
Entra Sign-in	Time	App Sign-in	Time
eric@fabrikam.cloud	2025-06-11T14:05	eric@fabrikam.cloud	2025-06-11T14:05
bill@fabrikam.cloud	2025-06-11T15:03	bill@fabrikam.cloud	2025-06-11T15:03
		eric@fabrikam.cloud	2025-06-11T15:04
melissa@fabrikam.cloud	2025-06-11T16:30	melissa@fabrikam.cloud	2025-06-11T16:30

Evil te

Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com
UPN: eric@evil.cloud

ID token from Entra



Contoso SaaS App Sign-in

Username

Password

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

App registration
Contoso.com SaaS App

er table

Detection: customer side log correlation

```
{
  "typ": "JWT",
```

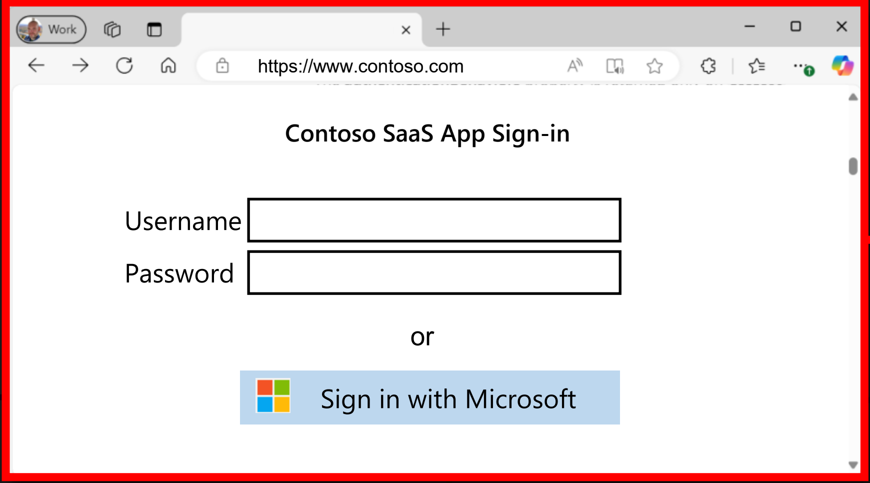
Entra Sign-in	Time	App Sign-i	er table
eric@fabrikam.cloud	2025-06-11T14:05		
bill@fabrikam.cloud	2025-06-1		11T15:03
		d	2025-06-11T15:04
meli		ssa@fabrikam.cloud	2025-06-11T16:30

Next to impossible

Evil te

Con

User: E
Mail: er m.com
UPN: eri @evil.cloud



Contoso SaaS App Sign-in

Username
Password

or

Sign in with Microsoft

Fabrikam tenant (Consumer)

Service principal
Contoso.com SaaS App

User: Eric
Mail: eric@fabrikam.com

Contoso tenant (ISV)

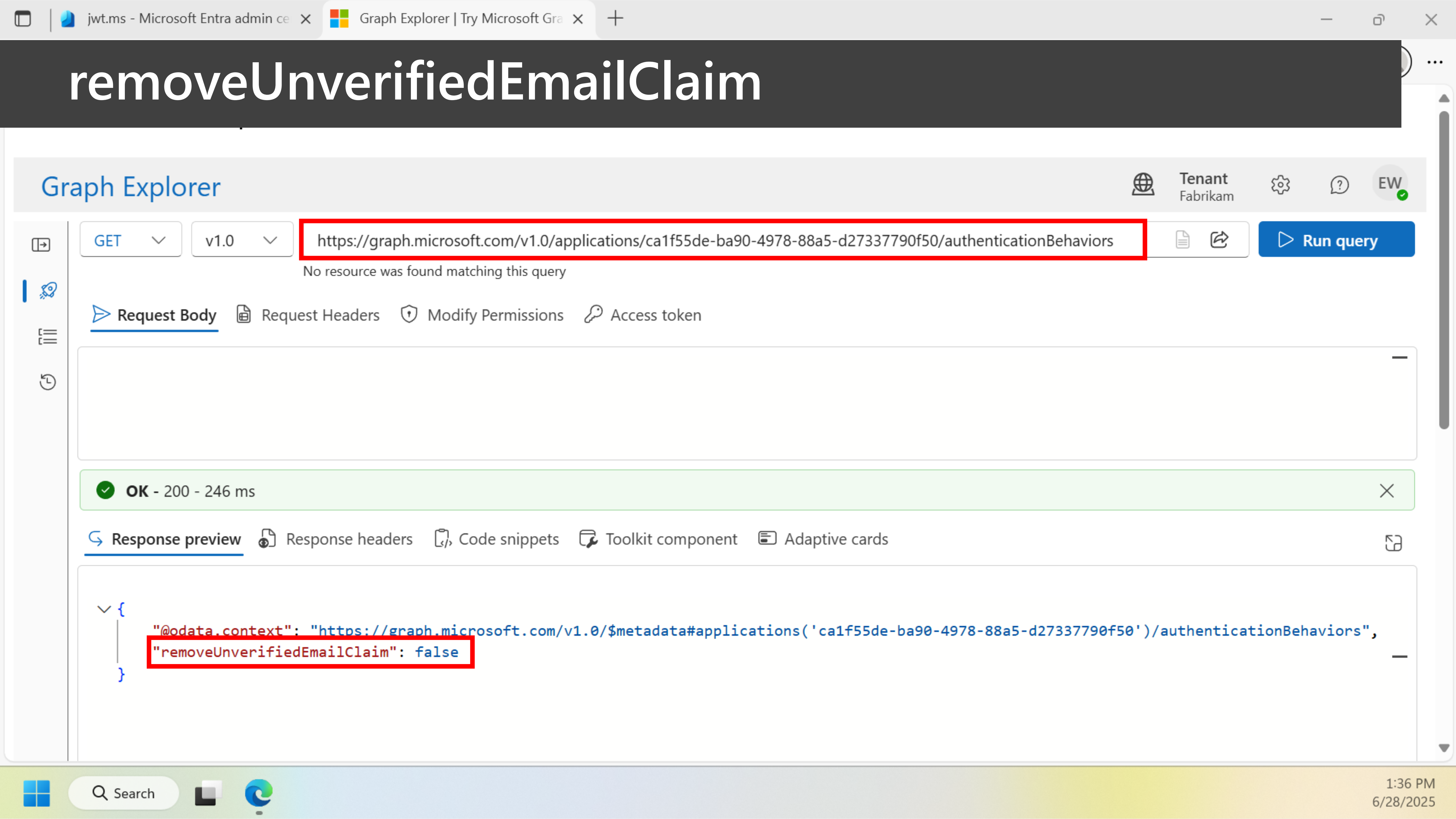
App registration
Contoso.com SaaS App

Mitigation: Vendor / developer side

- Fix your application
- Check app reg for removeUnverifiedEmailClaim
- Test your application
- Test your application
- Fix your application
- Test your application
- Fix your application
- Test your application

semperis

removeUnverifiedEmailClaim



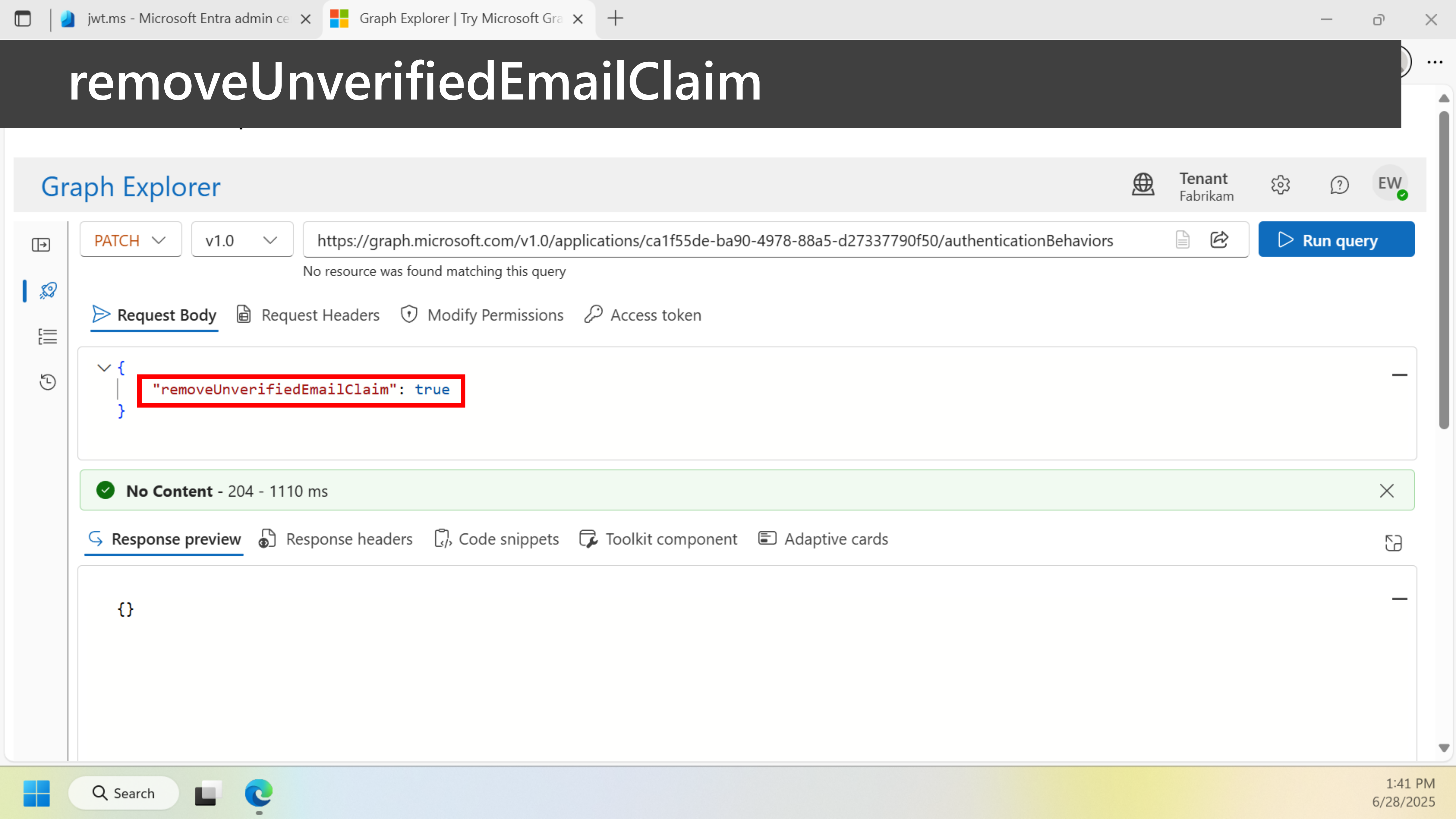
https://graph.microsoft.com/v1.0/applications/ca1f55de-ba90-4978-88a5-d27337790f50/authenticationBehaviors

No resource was found matching this query

OK - 200 - 246 ms

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#applications('ca1f55de-ba90-4978-88a5-d27337790f50')/authenticationBehaviors",
    "removeUnverifiedEmailClaim": false
}
```

removeUnverifiedEmailClaim



PATCH v1.0 https://graph.microsoft.com/v1.0/applications/ca1f55de-ba90-4978-88a5-d27337790f50/authenticationBehaviors Run query

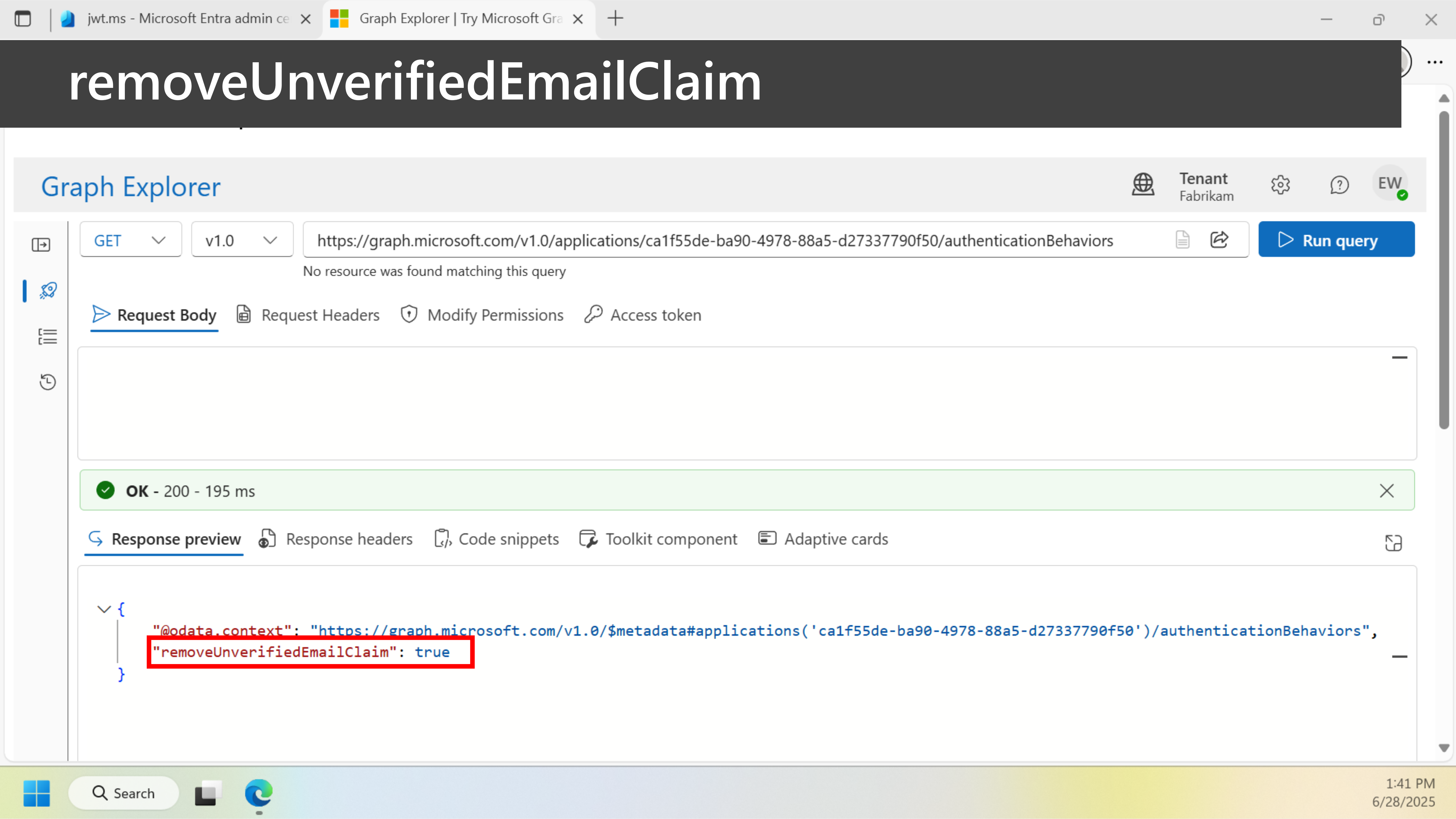
No resource was found matching this query

```
{
  "removeUnverifiedEmailClaim": true
}
```

No Content - 204 - 1110 ms

```
{}
```

removeUnverifiedEmailClaim



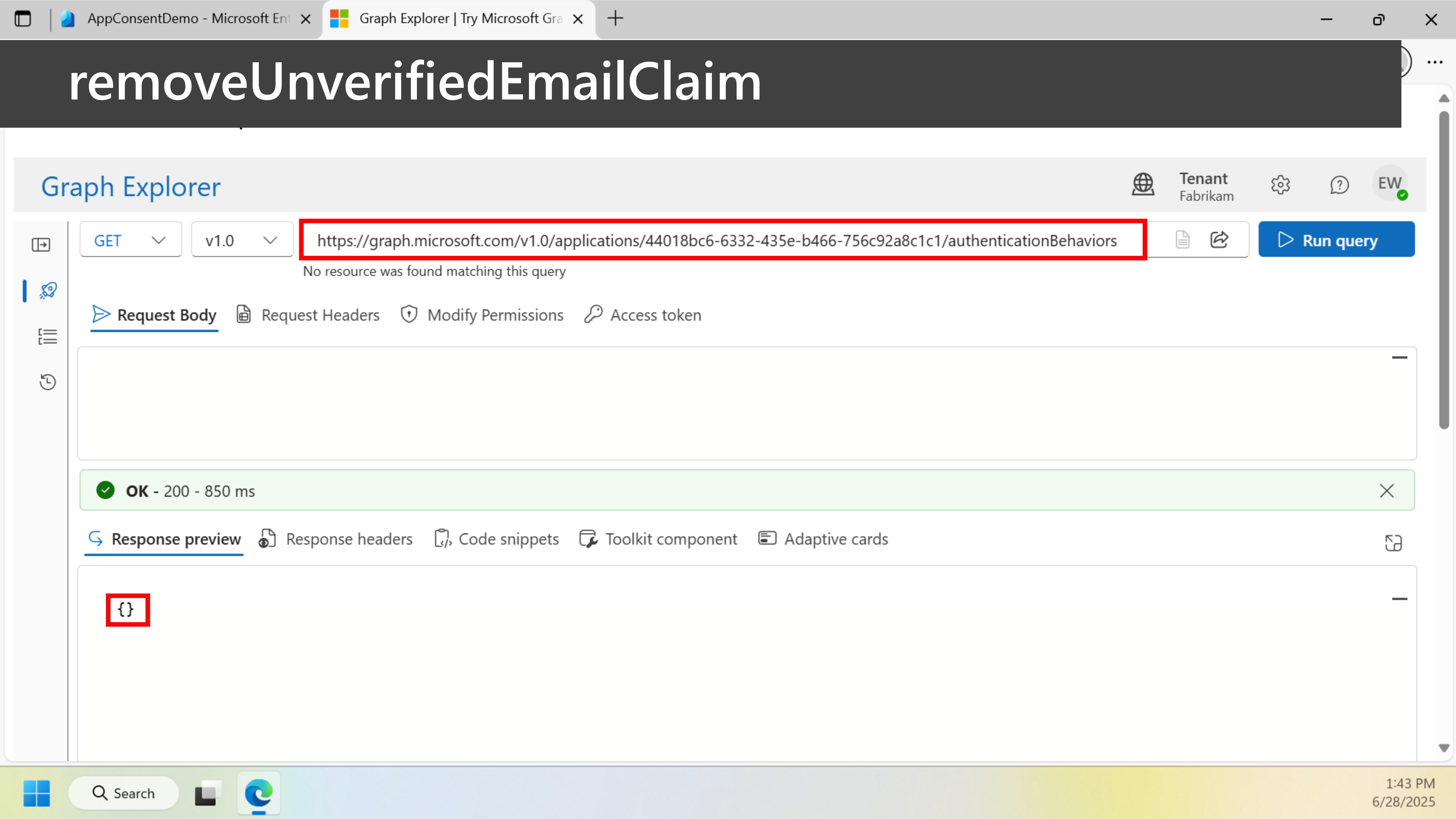
https://graph.microsoft.com/v1.0/applications/ca1f55de-ba90-4978-88a5-d27337790f50/authenticationBehaviors

No resource was found matching this query

OK - 200 - 195 ms

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#applications('ca1f55de-ba90-4978-88a5-d27337790f50')/authenticationBehaviors",
    "removeUnverifiedEmailClaim": true
}
```

removeUnverifiedEmailClaim



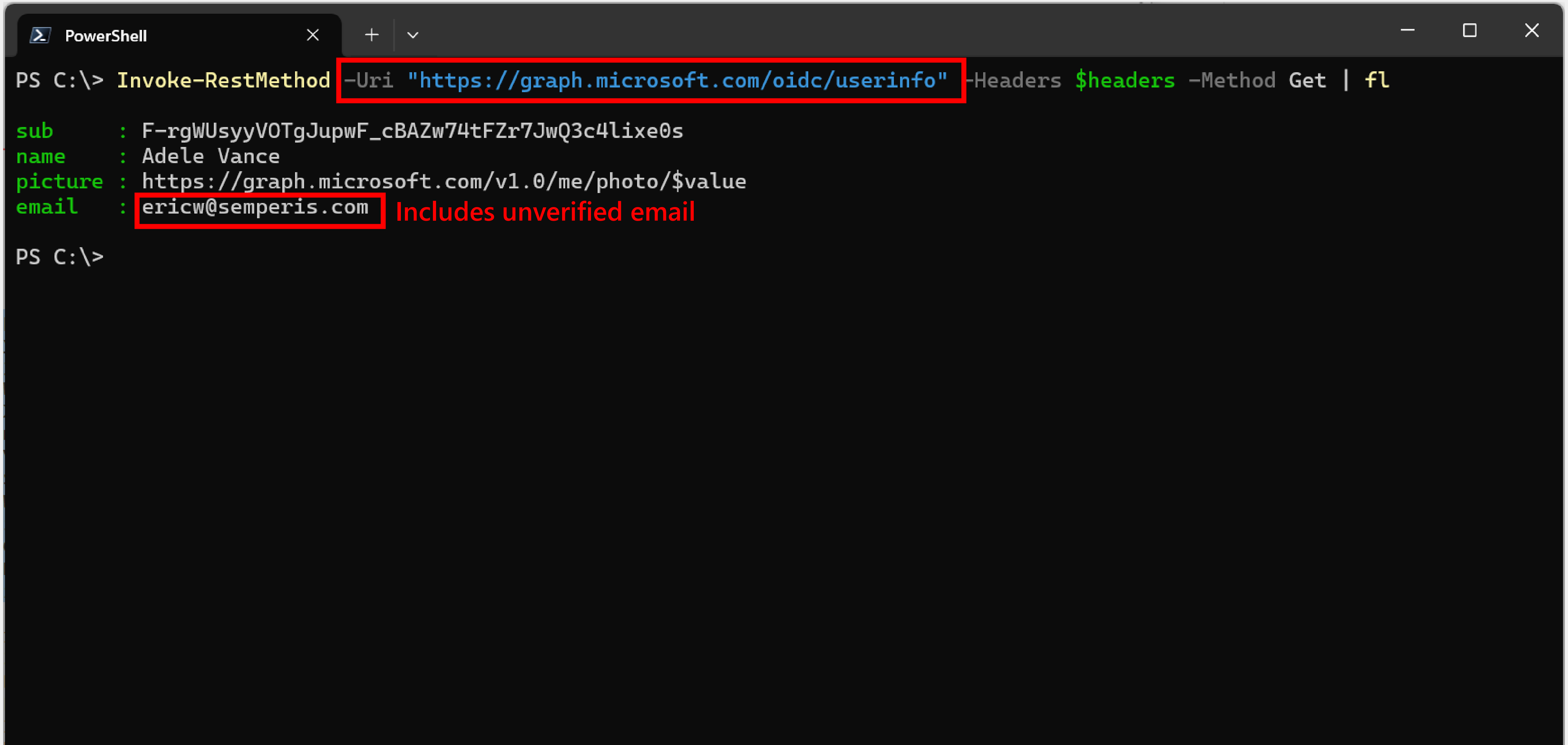
```
https://graph.microsoft.com/v1.0/applications/44018bc6-6332-435e-b466-756c92a8c1c1/authenticationBehaviors
```

No resource was found matching this query

OK - 200 - 850 ms

```
{}
```

Userinfo endpoint



```
PS C:\> Invoke-RestMethod -Uri "https://graph.microsoft.com/oidc/userinfo" -Headers $headers -Method Get | fl

sub     : F-rgWUsyyVOTgJupwF_cBAZw74tFZr7JwQ3c4lixe0s
name    : Adele Vance
picture : https://graph.microsoft.com/v1.0/me/photo/$value
email   : ericw@semperis.com

PS C:\>
```

Includes unverified email

New nOAuth blog post

https://sl.entra.ms/noauth

semperis

Key takeaways

Key takeaways

nOAuth is extremely dangerous

nOAuth will continue to exist

Customers of vulnerable apps have no real protection

https://sl.entra.ms/noauth

semperis

Questions?

@ericonidentity.com

@ericonidentity

/in/ericonidentity

@ericonidentity@infosec.exchange