

RSACTMConference2024

San Francisco | May 6 – 9 | Moscone Center

SESSION ID: HTA-M02

All You Need Is Guest

THE ART OF
POSSIBLE

#RSAC

Michael Bargury

Cofounder and CTO

Zenity

@mbrg0

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2024 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Agenda

- Why invite guests in?
- Security research and threat actor exploitation, exposing the real attack surface of guests
 - Teams-based phishing
 - Enumeration
 - Power-pwn
- How to protect your organization

WHY invite guests in?

And the promise of deny-by-default access

How can two parties collaborate over a bunch of files?

F1000
enterprise

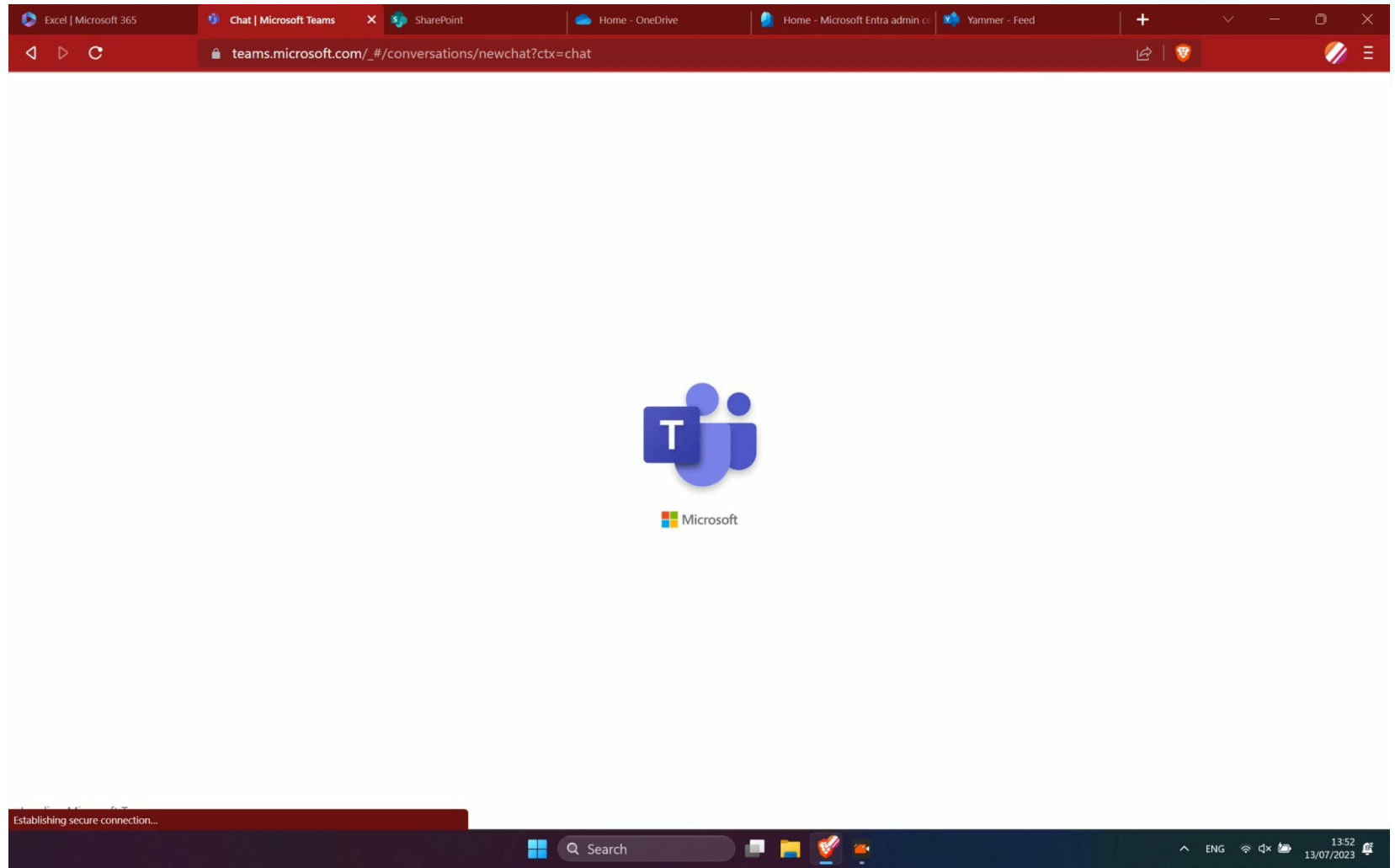
	POC Kickoff
	NDA
	Success Criteria
	Order Form
	POC Agenda

Small
vendor

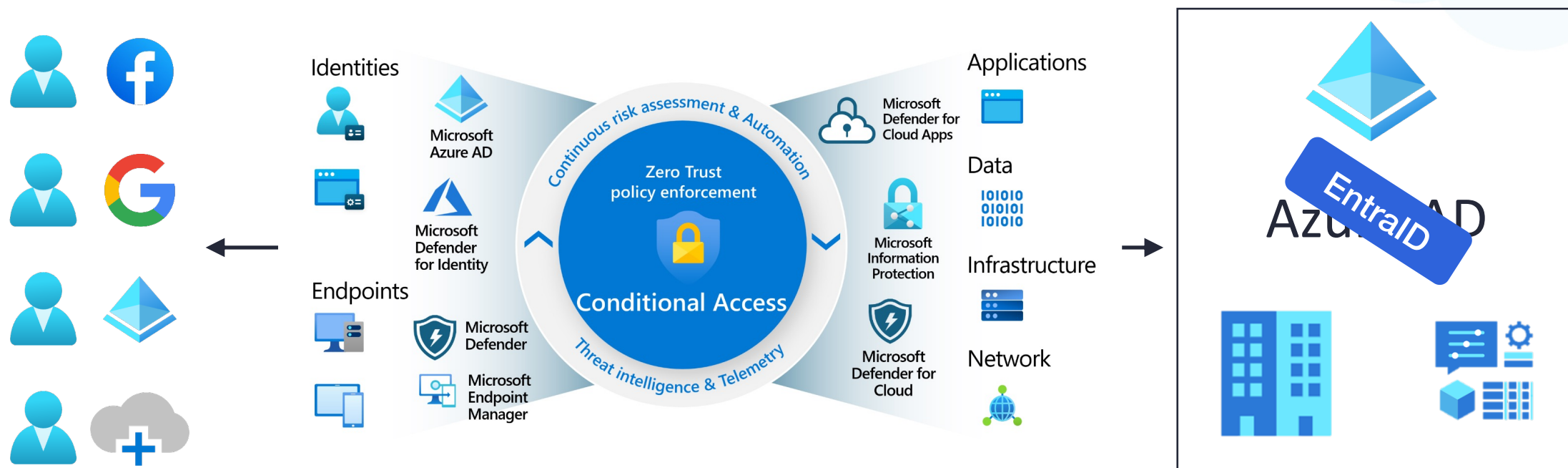
Safe guest access must be:

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

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



(b) Control guests like employees



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

F1000 tenant

(b) Applying security controls to guests

Need guest access → Require security controls

(b) Applying security controls to guests

Need guest access → Require security controls

Security controls → Require AAD account

(b) Applying security controls to guests

Need guest access → Require security controls

Security controls → Require AAD account

AAD account → Grants full access

Q.E.D.?

(b) Applying security controls to guests

Need guest access → Require security controls

Security controls → Require AAD account

AAD account → Grants full deny-by-default access

EntraID guest recap

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

RSACConference™2024

Guest accounts in practice

Security research into the real implication of
guests

#RSAC
@mbrg0



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



Role



Greg Winston

VP of IT

Owner



► Members and guests (2)



Teams

Your teams

Vo 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	Role
------	-------	----------	------	------

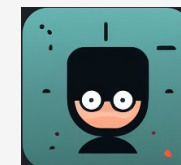


Greg Winston

VP of IT

Owner

Members and guests (2)





Teams

Your teams

Vo Vendor onboarding ...



Vendor onboarding ...

Vendor onboarding



Add members to Vendor onboarding

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

Start typing a name or group

Add

+ Add member

Tags ⓘ

Role

Owner ▾

Close





Teams

Your teams

Vo 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

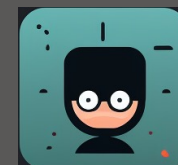
Close

Add member

Tags

Role

Owner



Teams

Your teams

Vo 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!](#)

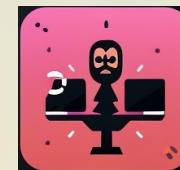
[Can't access your account?](#)

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

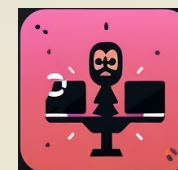
You should only accept if you trust Zenity Demo. **Zenity Demo has not provided links to their terms for you to review.** You can update these permissions at <https://myaccount.microsoft.com/organizations>.

[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

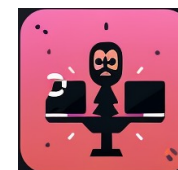
Sign out



Hacker5
hacker5@pwnতোso.onmicroso...
[View account](#)
[Switch organization](#)



Sign in with a different account



Everything works as expected ?

Everything works as expected ? ?

Teams-based phishing

The real attack surface of guests

Phishing via Teams: exploited by Storm-0324

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

Malware distributor Storm-0324 facilitates ransomware access

By Microsoft Threat Intelligence

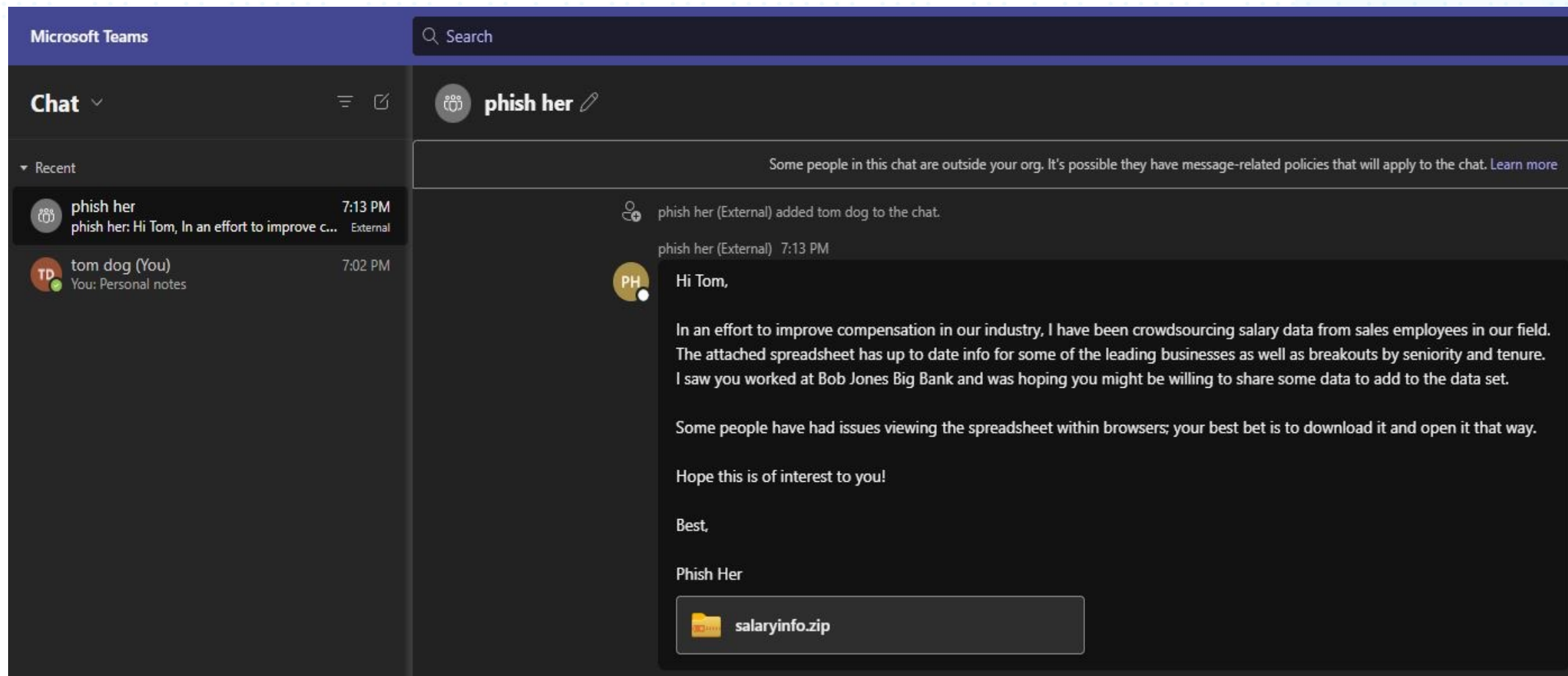
New Teams-based phishing activity

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

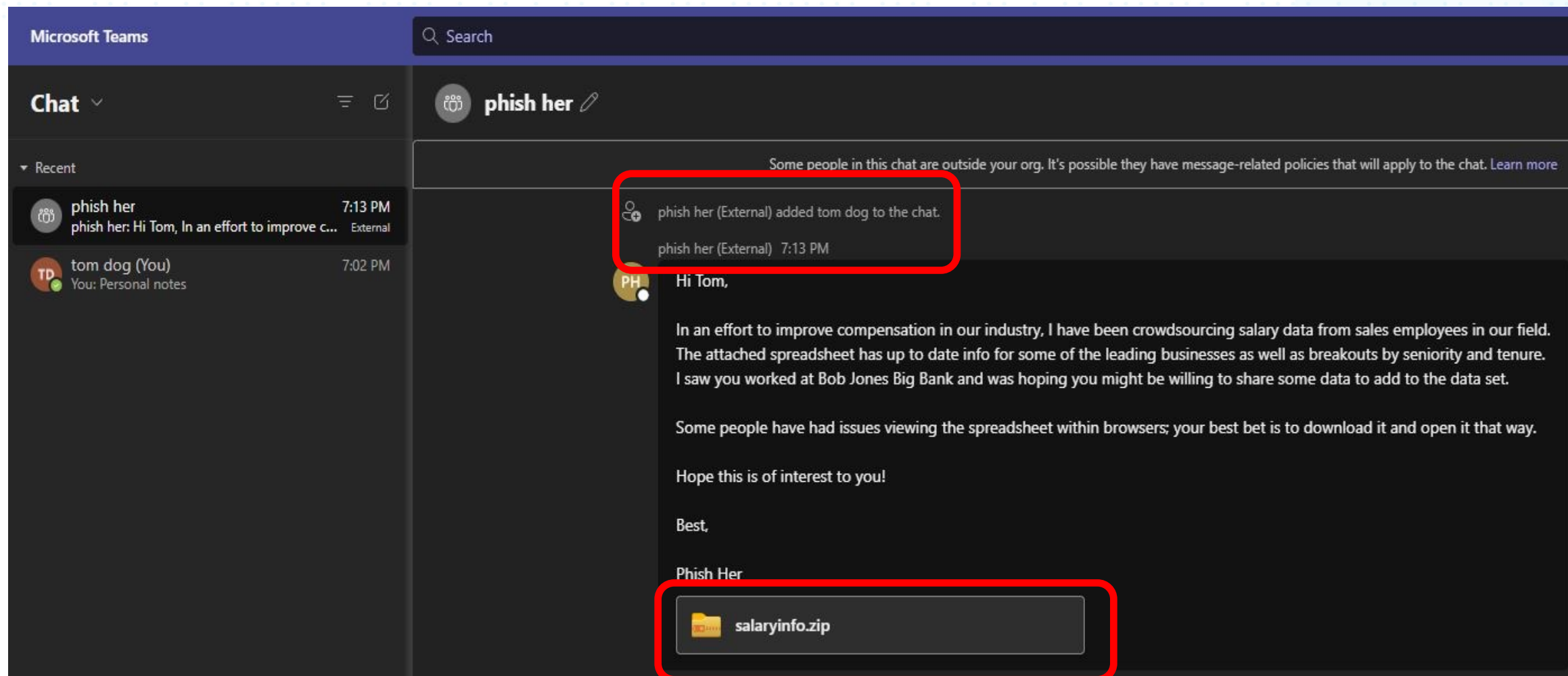
Microsoft takes these phishing campaigns very seriously and has rolled out several improvements to better defend against these threats. In accordance with Microsoft policies, we have suspended identified accounts and tenants associated with inauthentic or fraudulent behavior. We have also rolled out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

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

Phishing via Teams



Phishing via Teams



Social engineering via Teams: exploited via Midnight Blizzard

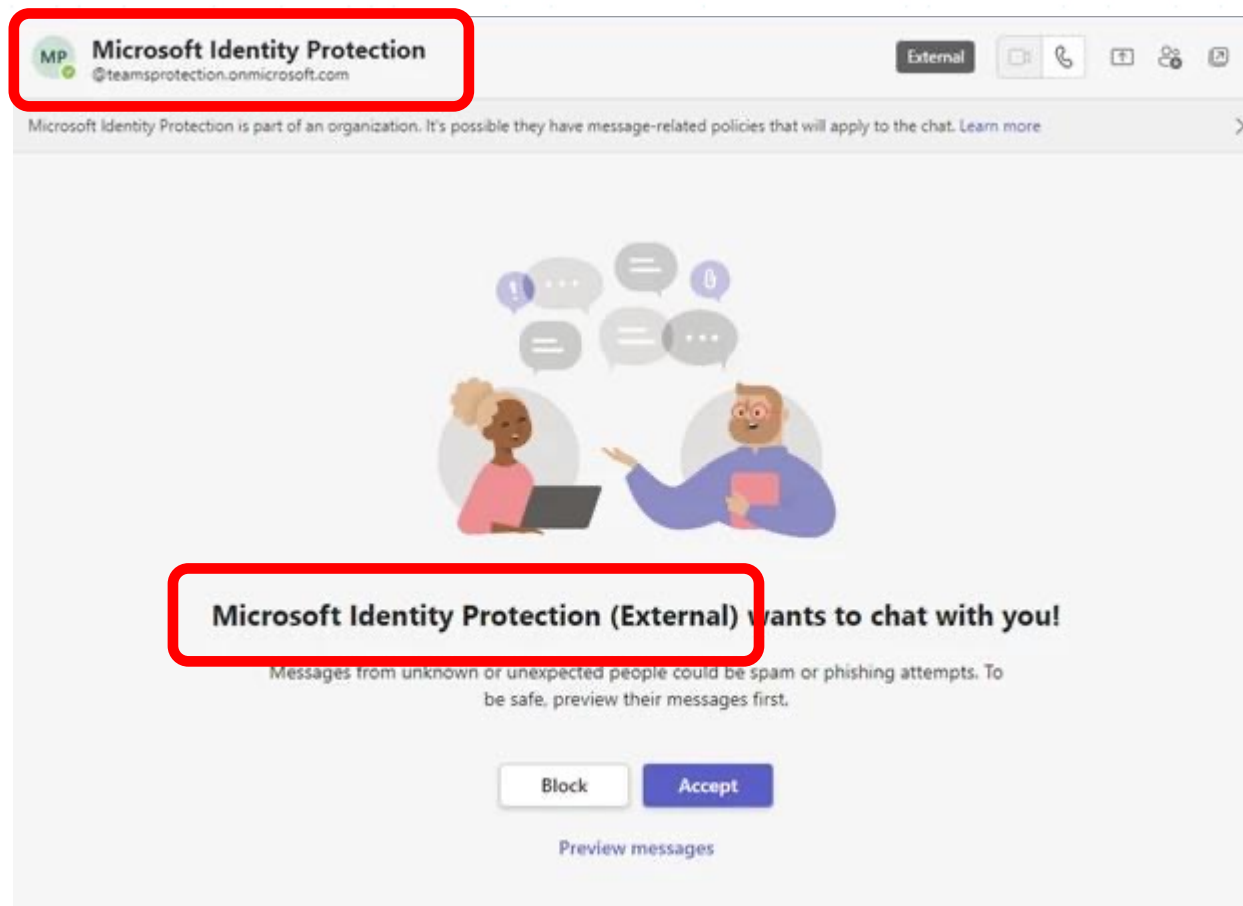
[Research](#) [Threat intelligence](#) [Social engineering / phishing](#) · 6 min read

Midnight Blizzard conducts targeted social engineering over Microsoft Teams

By [Microsoft Threat Intelligence](#)

<https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/>

Social engineering via Teams: exploited via Midnight Blizzard



RSACConference™2024

Tenant enumeration

The real attack surface of guests

 - Microsoft Entra ID



Insufficient privileges to complete the operation.

Summary

Session ID
d0ffd160abee439486af1315dea4e52c

Extension
Microsoft_AAD_UsersAndTenants

Error code
403

Resource ID
Not available

Content
UserManagementMenuBlade

AADInternals 0.9.0

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

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

Hackers are after more

- Can guests access unauthorized company data?
- Edit or delete data?
- Perform operations?

RSAConference™2024

Power-pwn

The real attack surface of guests

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



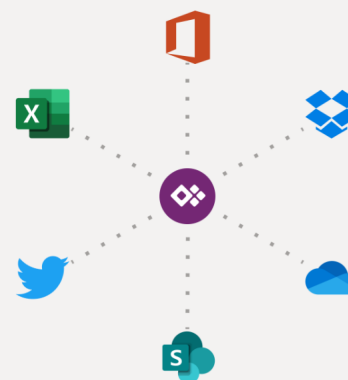
Go have an early lunch

Welcome to Power Apps

Choose your country/region

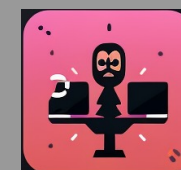
United States

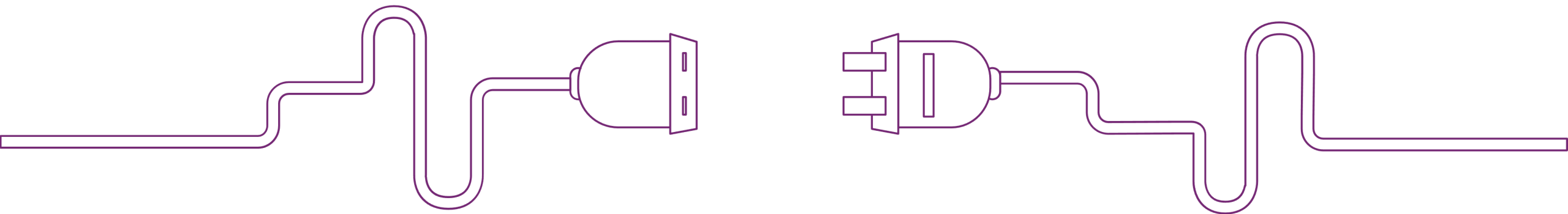
Microsoft will send you promotions and offers. You can unsubscribe at any time.



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](#)

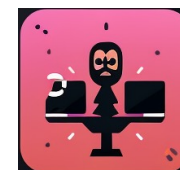


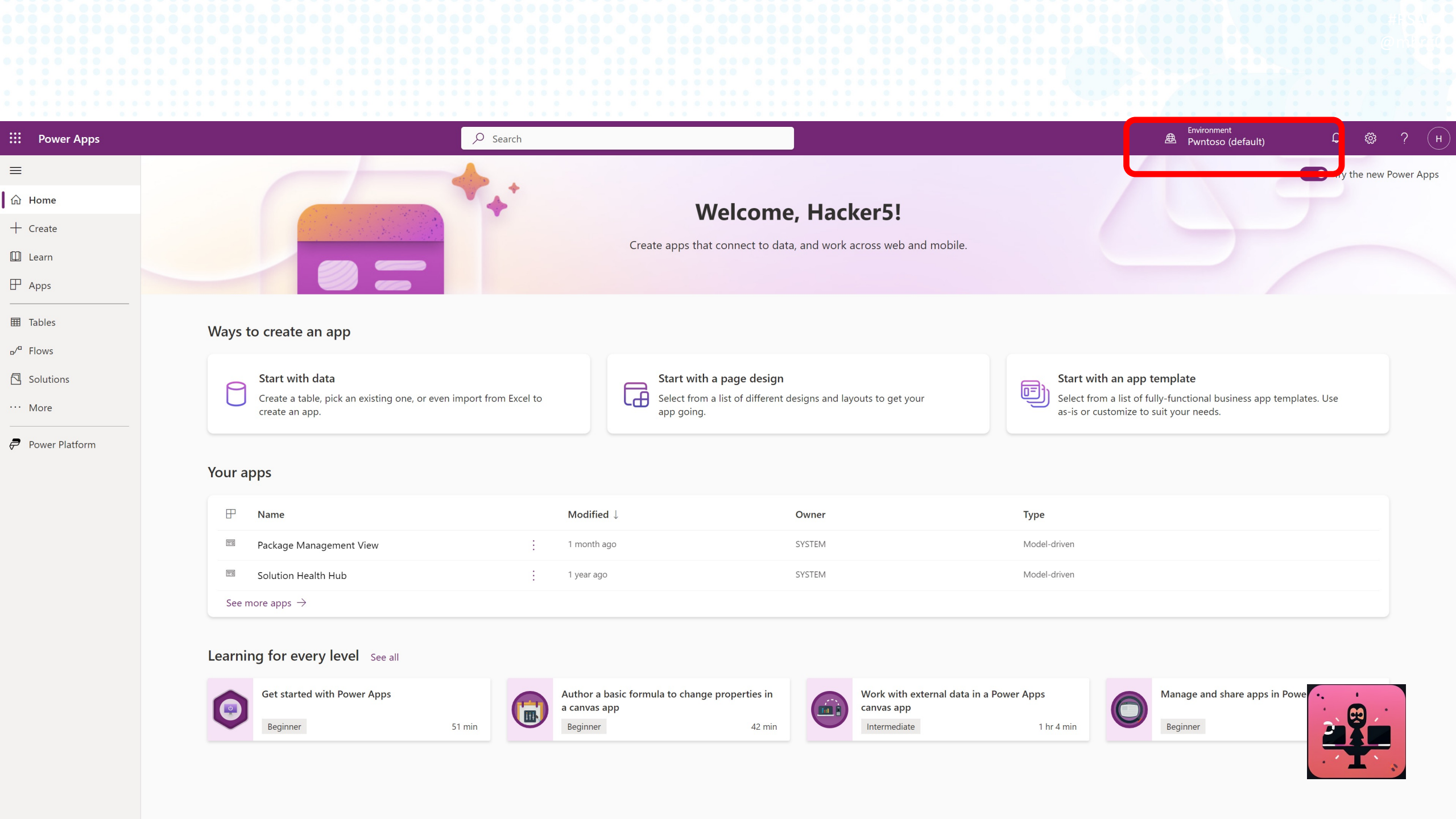


Sorry, there's been a disconnect

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

[Go to home page](#)





- 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 →					

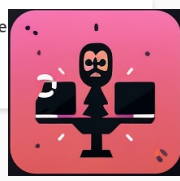
Learning for every level [See all](#)

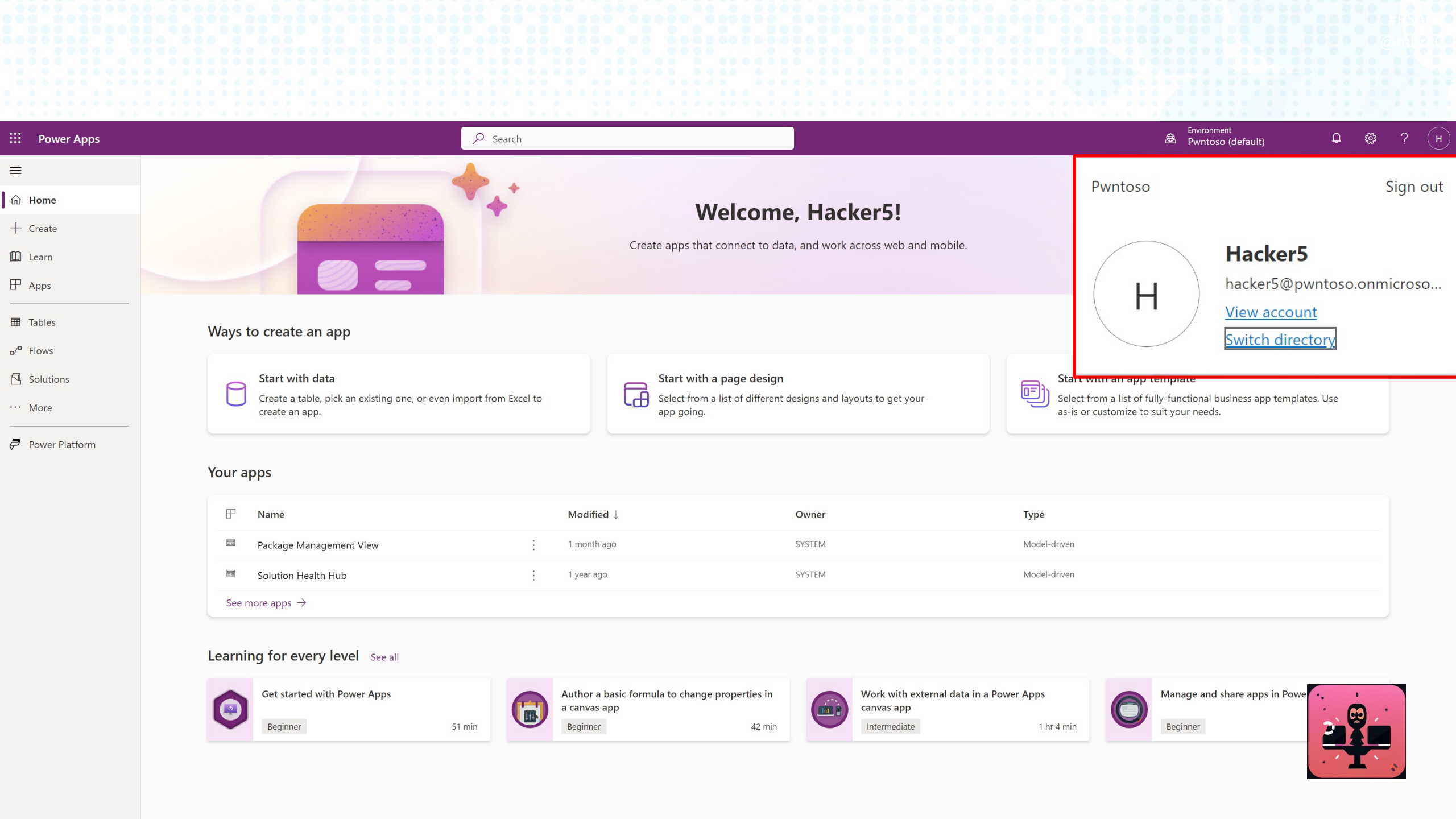
**Get started with Power Apps**
Beginner 51 min

**Author a basic formula to change properties in a canvas app**
Beginner 42 min

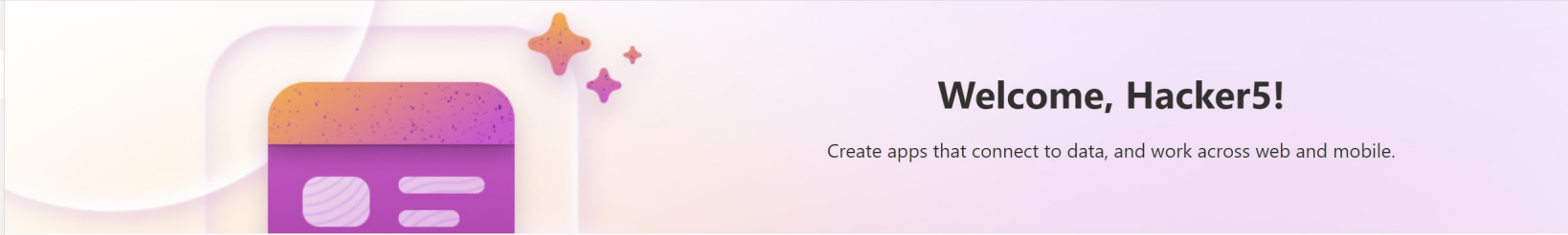
**Work with external data in a Power Apps canvas app**
Intermediate 1 hr 4 min

**Manage and share apps in Power Apps**
Beginner





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



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

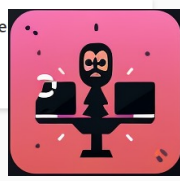
Beginner

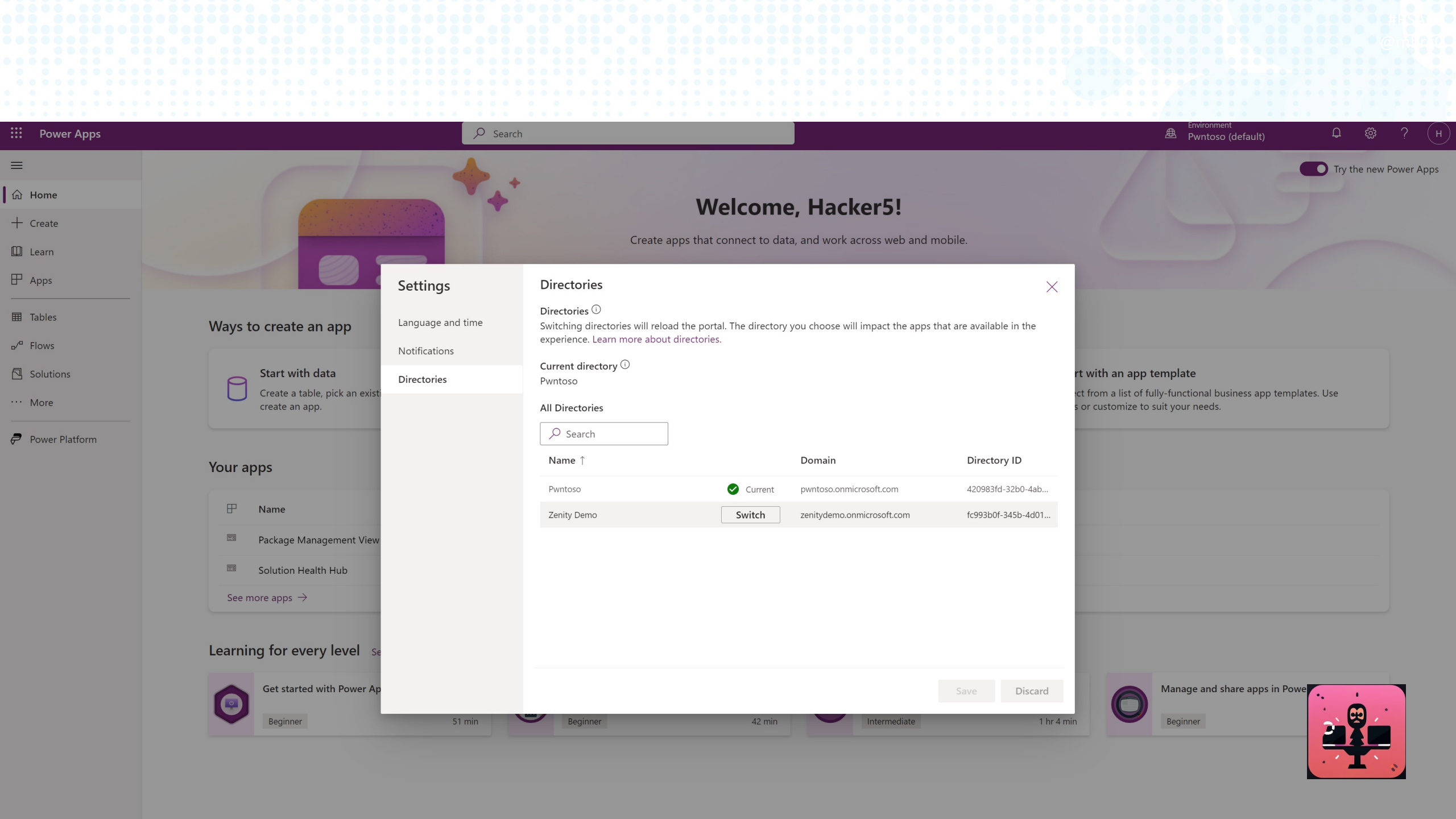
42 min
- Work with external data in a Power Apps canvas app

Intermediate

1 hr 4 min
- Manage and share apps in Power Apps

Beginner





Settings

Language and time

Notifications

Directories

Directories ⓘ

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

Current directory ⓘ

Pwntoso

All Directories

Search

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

Save

Discard

- ☰
- 🏠 Home
- + Create
- 📖 Learn
- 🗃 Apps
- 📊 Tables
- 📄 Flows
- 📁 Solutions
- 🔗 **Connections** ⚙️
- ⋮ More
- 🛠 Power Platform

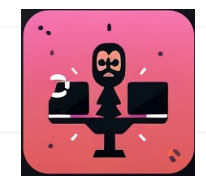
+ New connection

Search

Connections in Zenity Demo (default)

🖌 Canvas

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

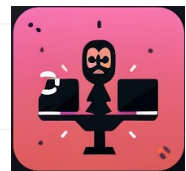


New connection Edit Share Delete Details

Connections in Zenity Demo (default)

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** 

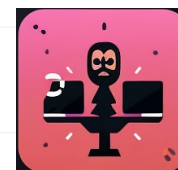
... More

 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	 14 min ago	Connected
  jamieredincustomerdata.file.core.windows.net Azure File Storage	 13 min ago	Connected
 Azure Queues Azure Queues		Connected
 jamieredincustomerdata.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



Jamie Reding

jamier@zenitydemo.on...

Owner



jamiercontoso

jamiercontoso@outlook....

Can use + share



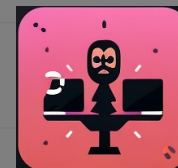
Cancel

Save

enterprisecustomers customercareinsights.database.wi...
SQL Server

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



Jamie Reding

jam

er



jamiercontoso

jam

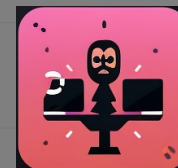
se + share



Save

enterprisecustomers customerc
SQL Server

connected





Home

+ Create

 Learn Apps Tables Flows Solutions Connections 

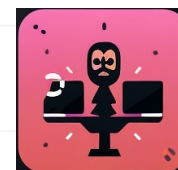
... More

 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
	 jamieredincustomerdata.file.core.windows.net Azure File Storage	...	18 min ago	Connected
	Azure Queues Azure Queues			Connected
	jamieredincustomerdata.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



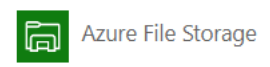
-
- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More
- Power Platform

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

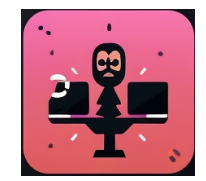
Jamie Reding

Created

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

Modified

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



 Home Create Learn Apps Tables Flows Solutions **Connections** More Power Platform Edit  Share  DeleteConnections > **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

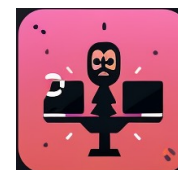
Jamie Reding

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

Power Platform

 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



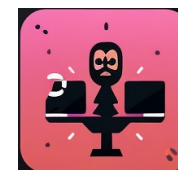
Jamie Reding

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?



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



RSAConference2023 | 12

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

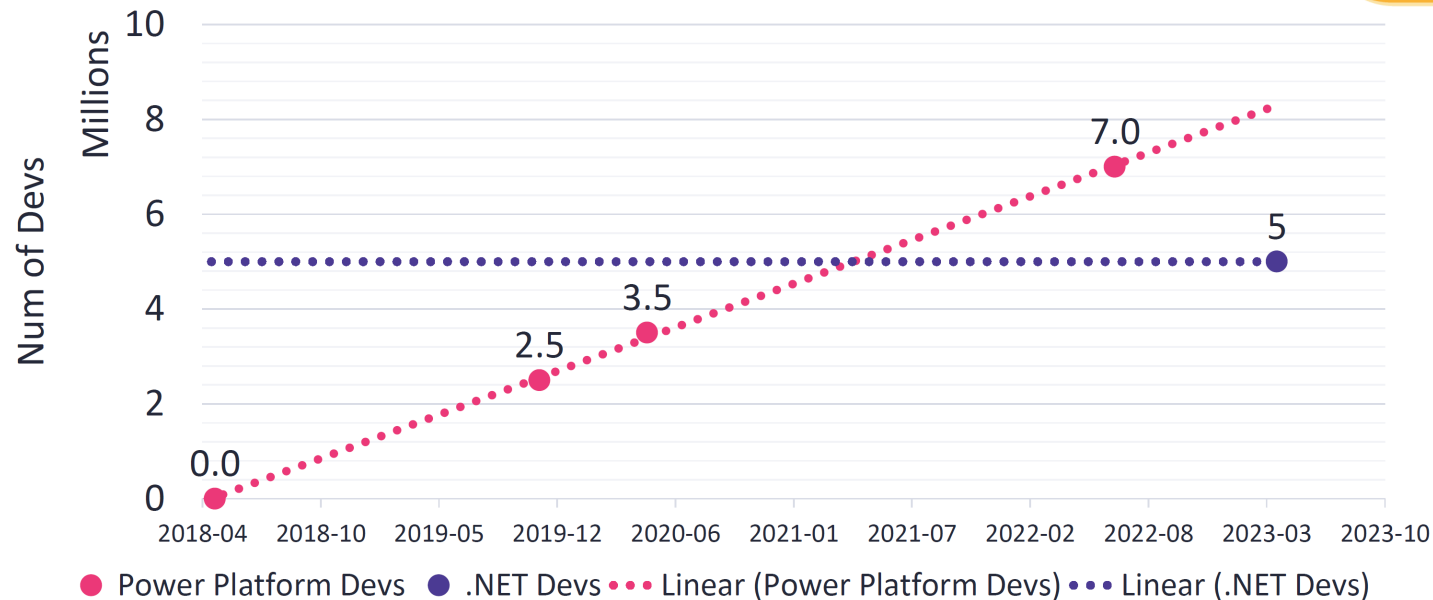
Michael Bargury
RSAC 2023



RSAConference2024

~8M active Power devs today!

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



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



RSAConference2023

12

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

Michael Bargury
RSAC 2023



RSAConference™2024

Exploit



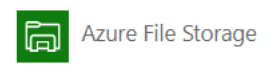
-
- Home
- Create
- Learn
- Apps
- Tables
- Flows
- Solutions
- Connections**
- More
- Power Platform

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

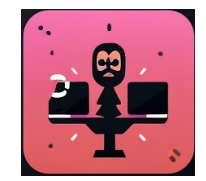
Jamie Reding

Created

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

Modified

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



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

Details

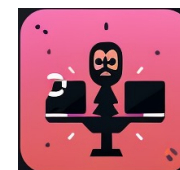
Apps using this connection

Flows using this connection

Name



Customer Insights Azure





Home

+ Create

Learn

Apps

Tables

Flows

Solutions

More

Power Platform

Ask a virtual agent

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

Apps > Customer Insights Azure

Details

Versions

Connections

Flows

Owner

Jamie Reding

Description

Not provided

Created

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

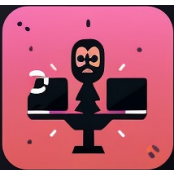
Modified

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

Web link

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

Mobile QR code





You need a Power Apps plan

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

[More](#)

OK





You need a Power Apps plan

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

[Less](#)

You're seeing this page because you don't have a license that allows you to use the capabilities used by the app. You can start a trial for a premium license or ask your admin for a Power Apps license.

Your plans: None

App license designation: Premium

Per app plans allocated in environment: No

App configured to consume per app plans: Yes

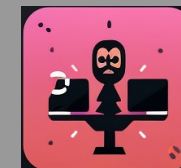
App is running: Standalone

Type of environment: Full

Premium features used by the app: premium connectors

Session ID: a40f9795-d274-4bab-8441-facd5ddd249c

OK



You need a Power Apps plan

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

Less

You're seeing this page because you don't have a license that allows you to use the capabilities used by the app. You can start a trial for a premium license or ask your admin for a Power Apps license.

Your plans: None

App license designation: Premium

Per app plans allocated in environment: No

App configured to consume per app plans: Yes

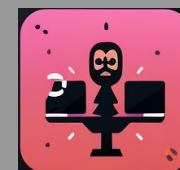
App is running: Standalone

Type of environment: Full

Premium features used by the app: premium connectors

Session ID: a40f9795-d274-4bab-8441-facd5ddd249c

OK



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

Power Apps Developer Plan

Build and test Power Apps for free

[Get started free >](#)

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



Free for development and testing

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



Developer-friendly

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



Dataverse included

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





You've selected Microsoft Power Apps for Developer

1 Let's get you started

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

Email

hacker5@pwntoso.onmicrosoft.com

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

[Learn More](#)

Next

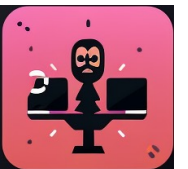
2 Create your account

3 Confirmation details



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

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





You've selected Microsoft Power Apps for Developer

- 1 Let's get you started
- 2 Create your account
- 3 Confirmation details

Thanks for signing up for Microsoft Power Apps for Developer

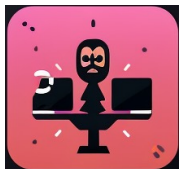
Your username is **hacker5@pwntoso.onmicrosoft.com**

[Get Started](#)



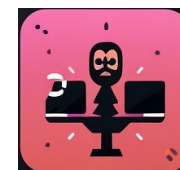
The Developer Plan makes it easy for anyone to build and test apps with user-friendly low-code tools – for free. Including, ongoing free access to:

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





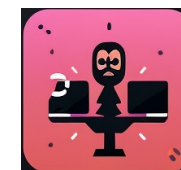
Customer Insights



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

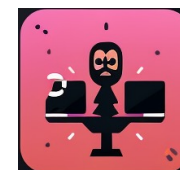
It looks like this app isn't compliant with the latest data loss prevention policies.

[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.

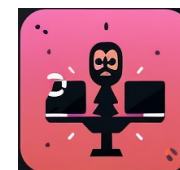


This app isn't opening correctly

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?

▼ 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

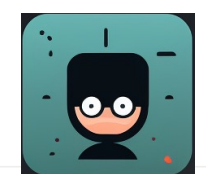
DLP Policies > New Policy

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

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

Find SSN

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

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 (deprecated)		Yes	No

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

Move to Business Block Configure connector

Set default group

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

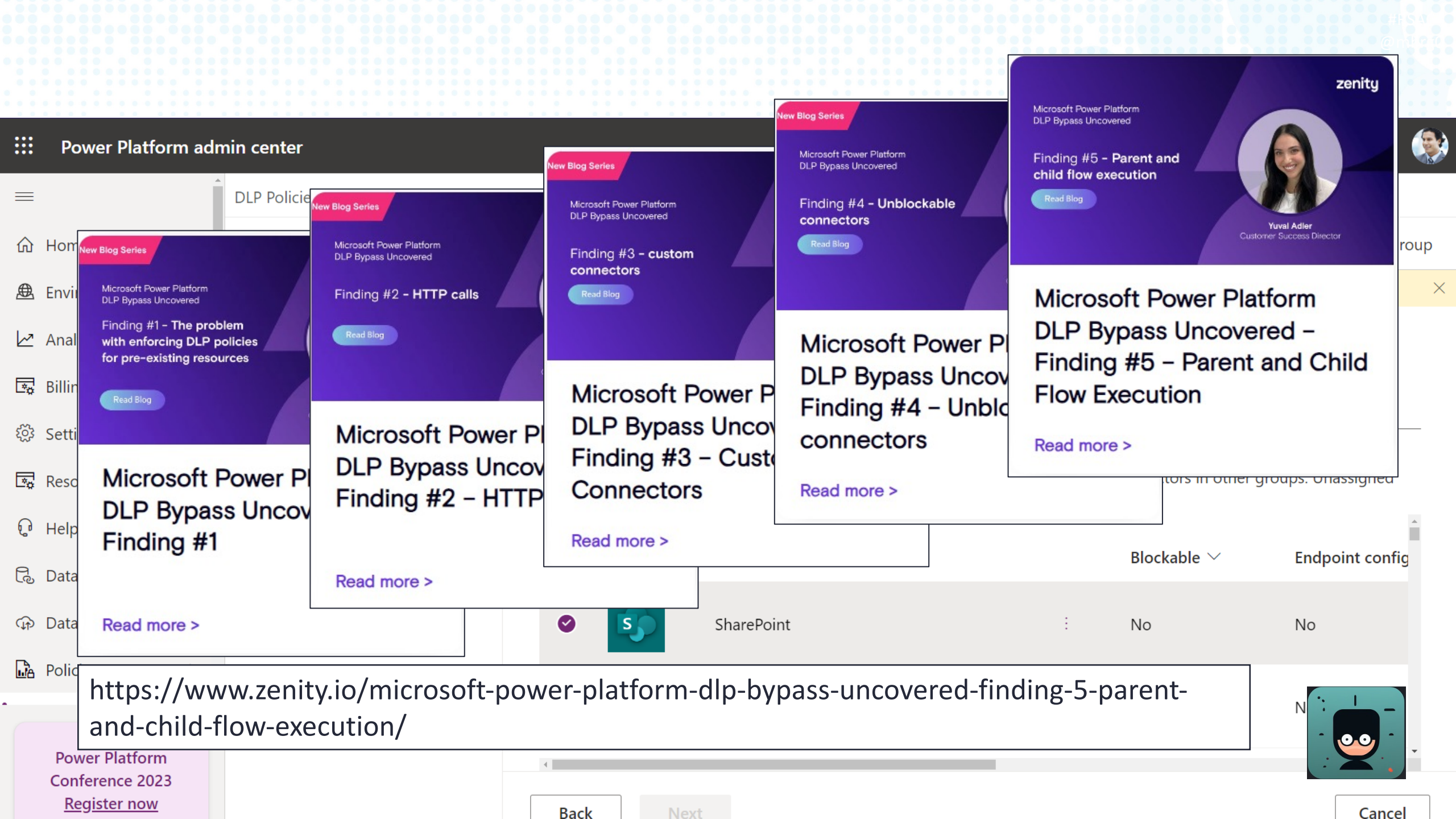
Assign connectors

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
☒	SharePoint	No	No
	OneDrive for Business	No	No



New Blog Series

Microsoft Power Platform
DLP Bypass Uncovered

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

Read Blog

Microsoft Power 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

Finding #5 - Parent and
child flow execution

Read Blog


Yuval Adler
Customer Success Director

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

Read more >

Blockable ▾

Endpoint config

No

No

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

This app isn't opening correctly

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

[Less](#)

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



[DLP Policies](#) > [Edit Policy](#)

✓ Policy name
Deny SQL

- ✔ Prebuilt connectors

- Custom connectors

✓ Scope

 Review

 [Move to Business](#)

 Move to Non-business

 Configure connector

 Set default group

Assign connectors

Business (0)

Non-business (1055) | Default

Blocked (1)

 Search connectors

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



Name 

Blockable 

Endpoint configu.



SQL Server



Yes

Yes



[Back](#)

Next

Cancel



Customer Insights



Almost there ...

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



SQL Server Premium

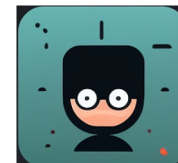
enterprisecustomers

customerinsights.database.windows.net

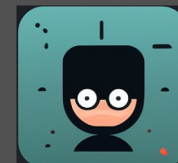
Signed in

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

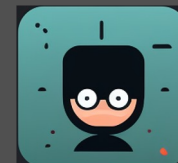
Aiden

LastName

Brown

SocialSecurityNumber

209-97-8888



 Search items

Aiden
Brown

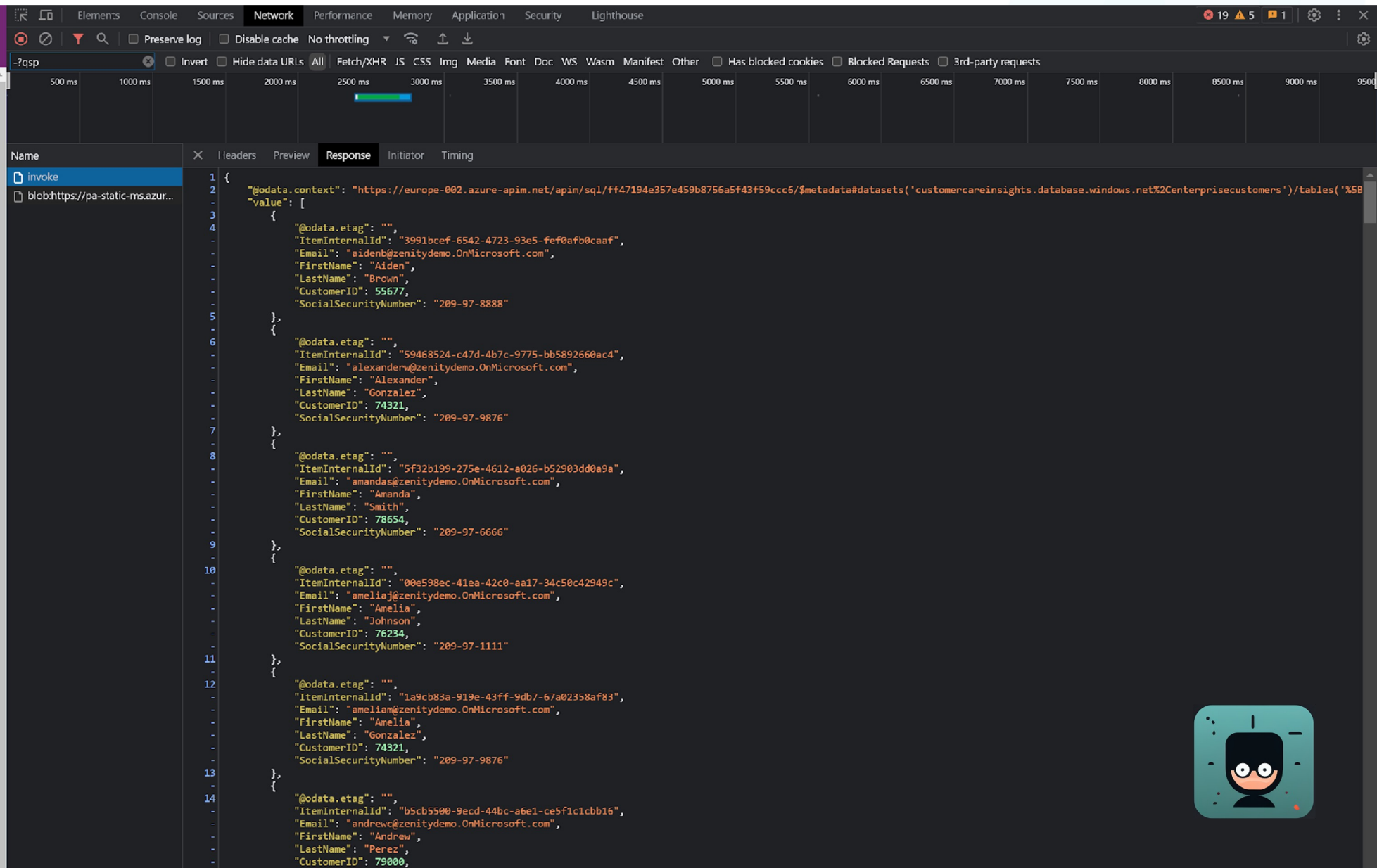
Alexander
Gonzalez

Amanda
Smith

Amelia
Johnson

Amelia
Gonzalez

A. I.



[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	

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Lighthouse

23

8

1

Preserve log

Disable cache

No throttling

Fetch/XHR

JS

CSS

Img

Media

Font

Doc

WS

Wasm

Manifest

Other

Has blocked cookies

Blocked Requests

3rd-party requests

5000 ms

10000 ms

15000 ms

20000 ms

25000 ms

30000 ms

35000 ms

40000 ms

45000 ms

50000 ms

55000 ms

60000 ms

65000 ms

70000 ms

Name

×

Headers

Preview

Response

Initiator

Timing

invoke

blob:https://pa-static-ms.azure...

General

Request URL:

Request Method:

Status Code:

Remote Address:

Referrer Policy:

Response Headers

Access-Control-Allow-Origin:

Access-Control-Expose-Headers:

Cache-Control:

Content-Encoding:

Content-Type:

Date:

Expires:

Pragma:

Strict-Transport-Security:

Timing-Allow-Origin:

Vary:

X-Content-Type-Options:

X-Frame-Options:

X-Ms-Apihub-Cached-Response:

X-Ms-Apihub-Obo:

X-Ms-Environment-Id:

X-Ms-Request-Id:

X-Ms-User-Agent:

Request Headers

:Authority:

:Method:

:Path:

:Scheme:

Accept:

Accept-Encoding:

Accept-Language:

Authorization:

https://europe-002.azure-apim.net/invoke

POST

200

20.86.93.35:443

no-referrer

Access-Control-Allow-Origin:

Content-Encoding, Transfer-Encoding, Vary, x-ms-request-id, x-ms-correlation-id, x-ms-user-agent, Strict-Transport-Security, X-Content-Type-Options, X-Frame-Options, Date, x-ms-connection-gateway-object-id, x-ms-connection-parameter-set-name, x-ms-environment-id, Timing-Allow-Origin, x-ms-apihub-cached-response, x-ms-apihub-obo

no-cache, no-store

gzip

application/json; charset=utf-8; odata.metadata=minimal

Sun, 16 Jul 2023 12:01:30 GMT

-1

no-cache

max-age=31536000; includeSubDomains

*

Accept-Encoding

nosniff

DENY

true

false

default-fc993b0f-345b-4d01-9f67-9ac4a140dd43

3b699bdc-5186-4a69-8043-fbf014885564

PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)

:Authority:

:Method:

:Path:

:Scheme:

Accept:

Accept-Encoding:

Accept-Language:

Authorization:

europe-002.azure-apim.net

POST

/invoke

https

application/json

gzip, deflate, br

en-US

Bearer



 Search items

Aiden

Br

a

Al

G

a

A

Sr

a

A

10

Amelia

Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

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

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

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

GET https://europe-002.azure-apim.net/apim

/sql/ff47194e357e459b8756a5f43f59ccc6

/v2/datasets/customercareinsights.database.windows.net,enterpris
ecustomers

/tables/%255Bdbo%255D.%255BCustomers%255D/items

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

GET https://europe-002.azure-apim.net/apim

/sql/ff47194e357e459b8756a5f43f59ccc6

**/v2/datasets/customercareinsights.database.windows.net,enterpri
secustomers**

/tables/%255Bdbo%255D.%255BCustomers%255D/items

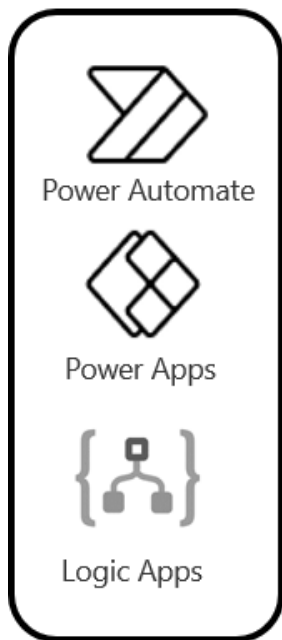
Power App is using azure-apim.net to fetch connection data

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

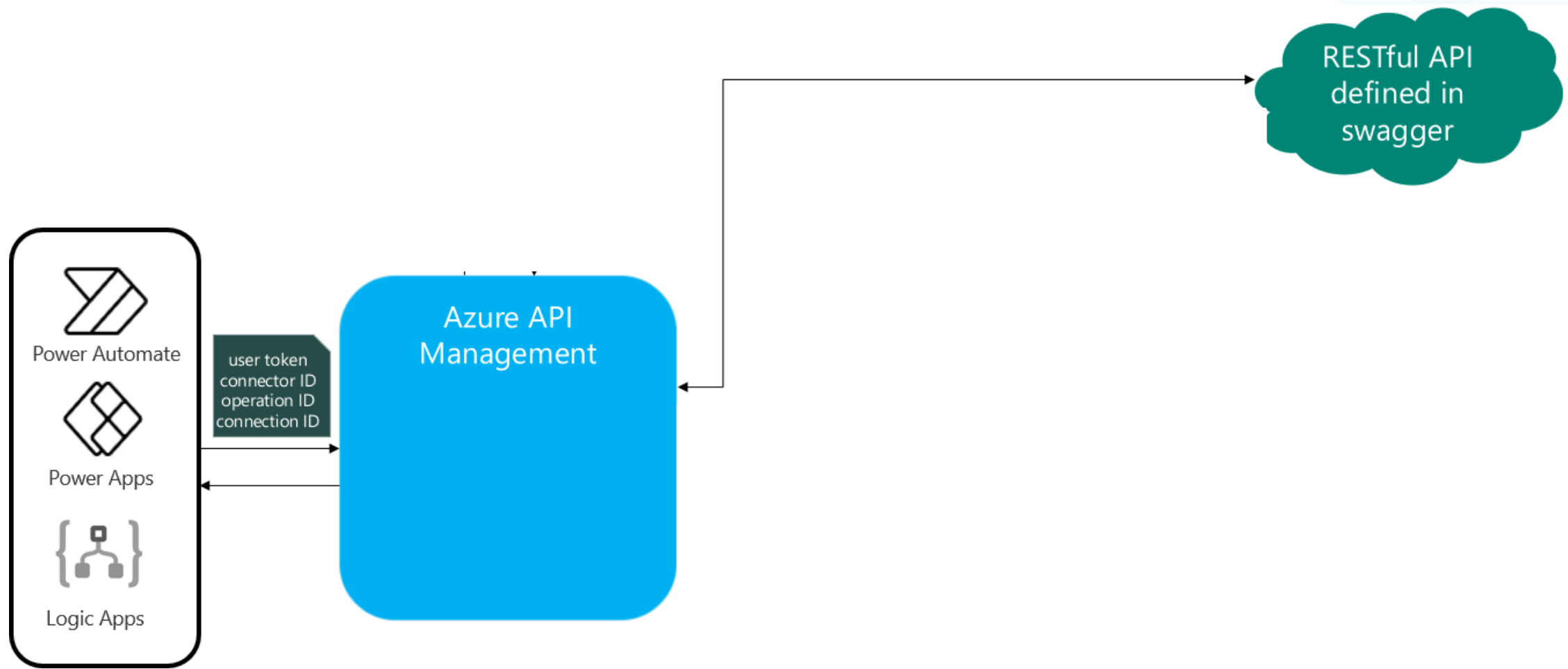
Power App is using azure-apim.net to fetch connection data

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

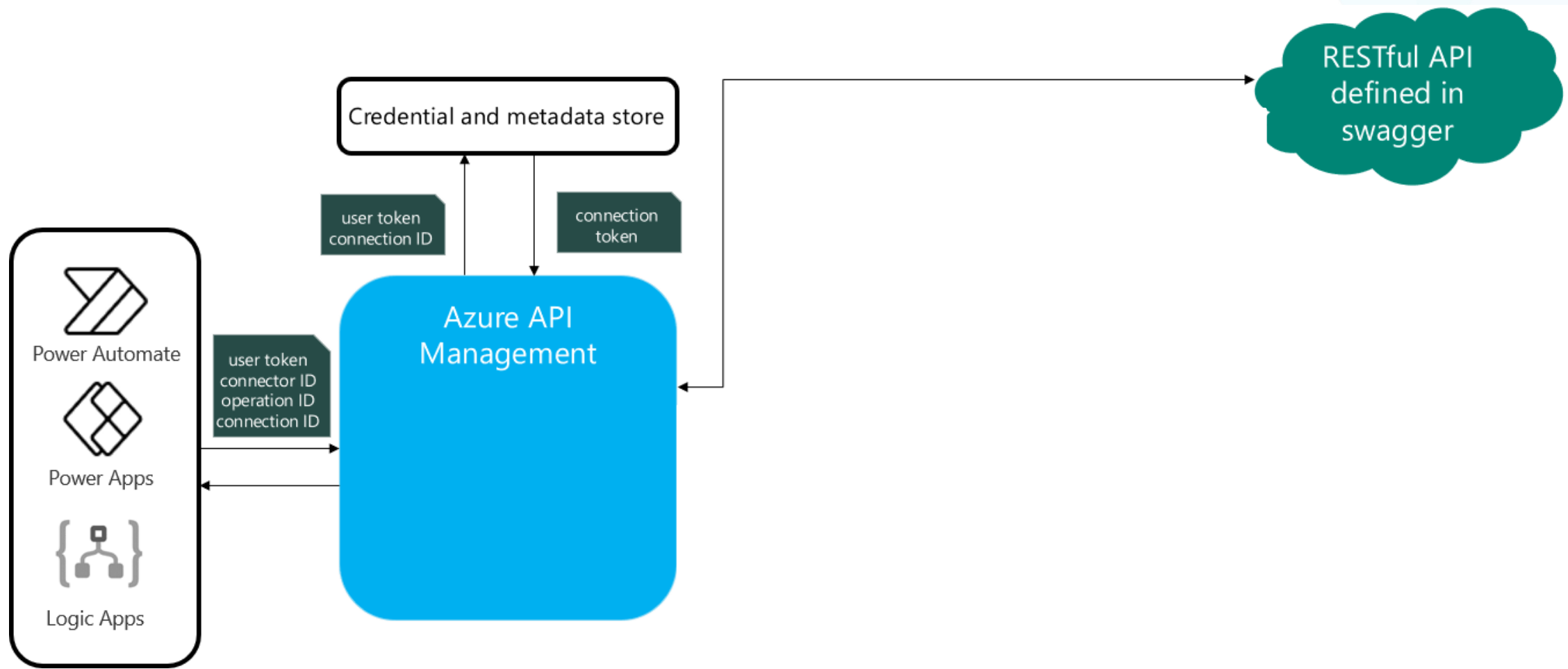
RESTful API
defined in
swagger



Microsoft Docs

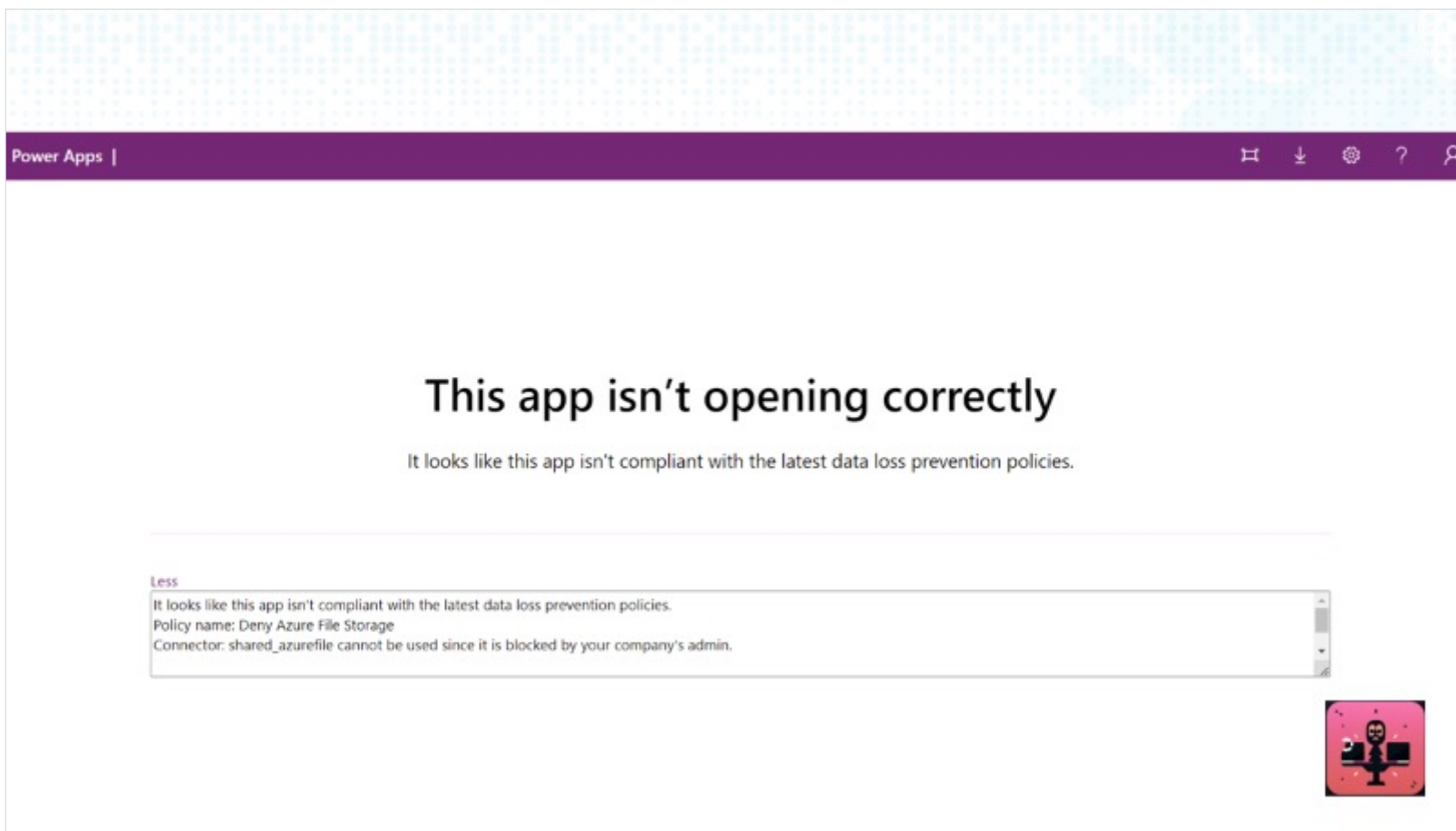


Microsoft Docs

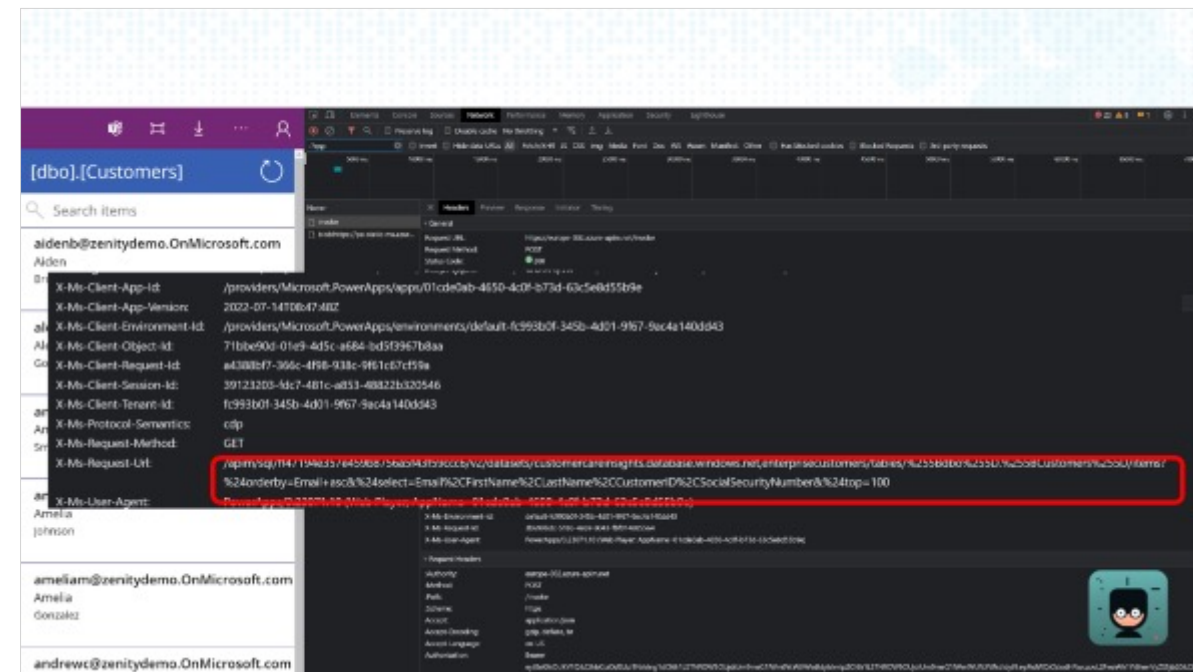
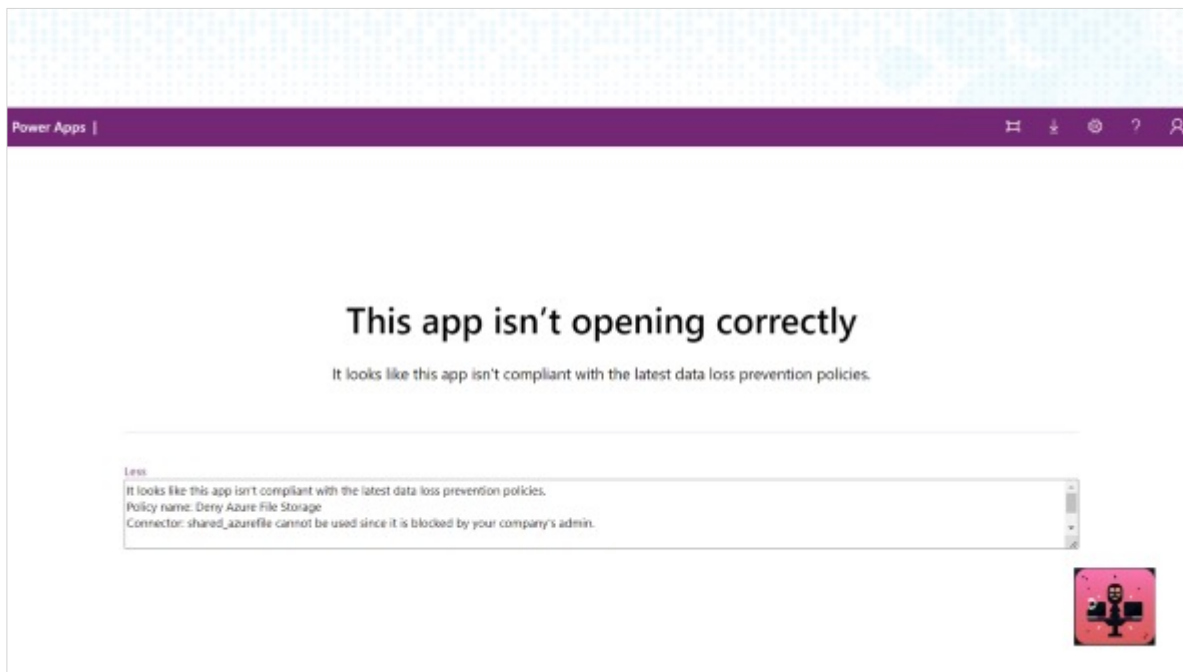


Microsoft Docs

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



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



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

```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest:] $ curl 'https://europe-002.azure-apim.net/invoke' \  
> -X 'POST' \  
> -H 'authority: europe-002.azure-apim.net' \  
> -H 'accept: application/json' \  
> -H 'accept-language: en-US' \  
> -H 'authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG  
> -H 'x-ms-client-object-id: 71bbe90d-01e9-4d5c-a684-bd5f3967b8aa' \  
> -H 'x-ms-client-request-id: b0fcb515-3898-496b-af84-89a0058b4f2e' \  
> -H 'x-ms-client-session-id: 1972191d-bec7-447a-a0ac-47267adfec24' \  
> -H 'x-ms-client-tenant-id: fc993b0f-345b-4d01-9f67-9ac4a140dd43' \  
> -H 'x-ms-protocol-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/%25Bdbo%25D.%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-paste browser API Hub call to bypass DLP

```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest:] $ curl 'https://europe-002.azure-apim.net/invoke' \
> -X 'POST' \
> -H 'authority: europe-002.azure-apim.net' \
> -H 'accept: application/json' \
> -H 'accept-language: en-US' \
> -H 'authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW50UjdiUm9meG
> -H 'x-ms-client-object-id: 71b1-001-01-0-415-684-1-15-62067b8-1' \
> -H 'x-ms-client-request-id: b0' \
> -H 'x-ms-client-session-id: 19' \
> -H 'x-ms-client-tenant-id: fc9' \
> -H 'x-ms-protocol-semantic: c' \
> -H 'x-ms-request-method: GET' \
> -H 'x-ms-request-url: /apim/sql/ff47194e357e459b8756a5f43f59ccc6/
ights.database.windows.net,enterpr
4orderby=Email+asc&%24select=Email
4top=100' \
> -H 'x-ms-user-agent: PowerApps
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
```



Encoded

PASTE A TOKEN HERE

ey30eXAl015Rv1Q1LC5HbGCl01530Z11N1151ng
1dCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWk
dldyIsImtpZCI6Ii1LSTNR0W50UjdiUm9meG1lW
m9YcWJIWkdldyJ9.eyJhdWQiOiJodHRwczovL2F
waWh1Yi5henVyZS5jb20iLCJpc3MiOiJodHRwcz
ovL3N0cy53aW5kb3dzLm5ldC9mYzk5M2IwZi0zN
DVilTRkMDEtOWY2Ny05YWM0YTE0MGRkNDMvIiwi
aWF0IjoxNjg5ODI4MTIwLCJuYmYiOiJlE2ODk4Mjg
xMjAsImV4cCI6MTY4OTgzMjk1MiwiYWNYIjojMS
IsImFpbyI6IkFVUUF1LzhUQUFBQTZtWks1WUpoS
ExWZVRzZGkvM1N3TDVhajIzU1RQZWNERWJjYWx0
ZEh1Zy9HTlZNUEtDZXdoajRmeUhtY0E2UyszNis
1NUJtMFFNUlVlOGphRStyQkRnPT0iLCJhbHRzZW
NpZCI6IjU6OjEwMDMyMDAyQzFGODM0ODEiLCJhb
YT0iOiJodHkiLCJpc3MiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mYzk5M2IwZi0zN

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

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

A scope away

Can we generate a token to API Hub?

A scope away

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

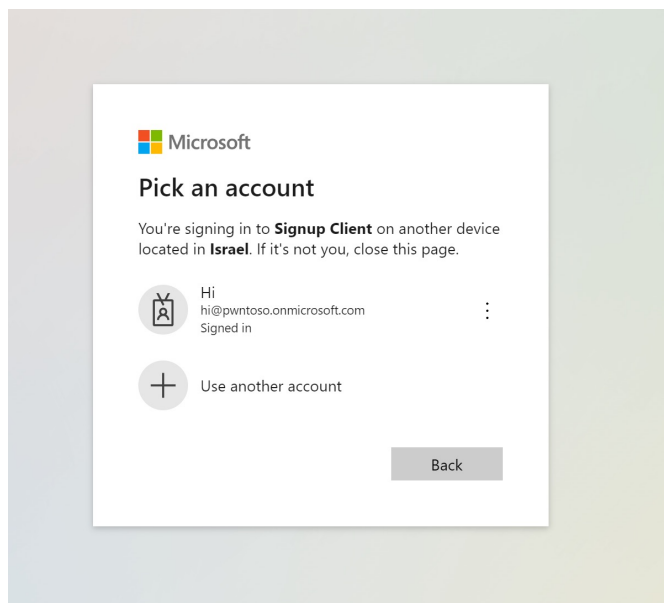
Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

```
>>> 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

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

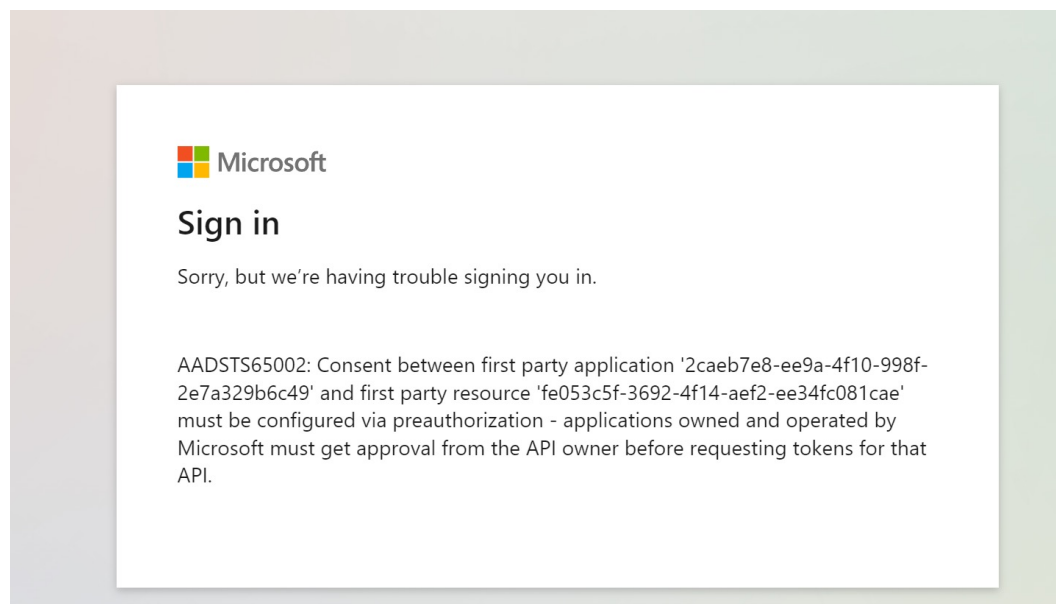
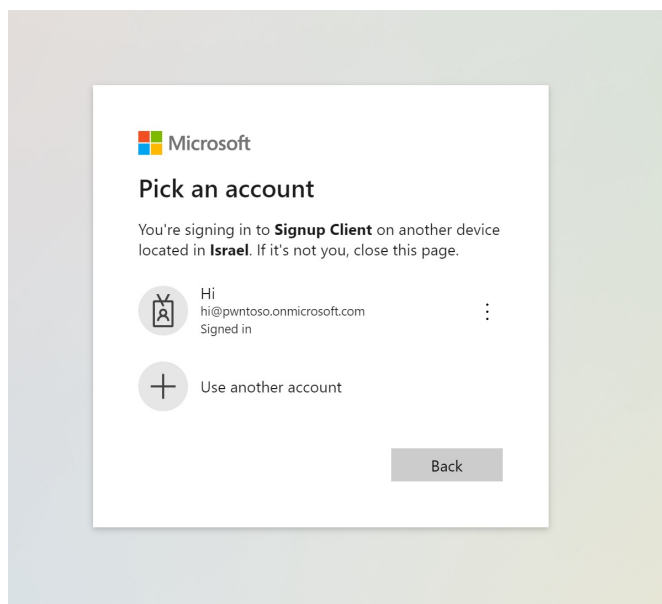
Using a built-in public client app?



A scope away

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.**

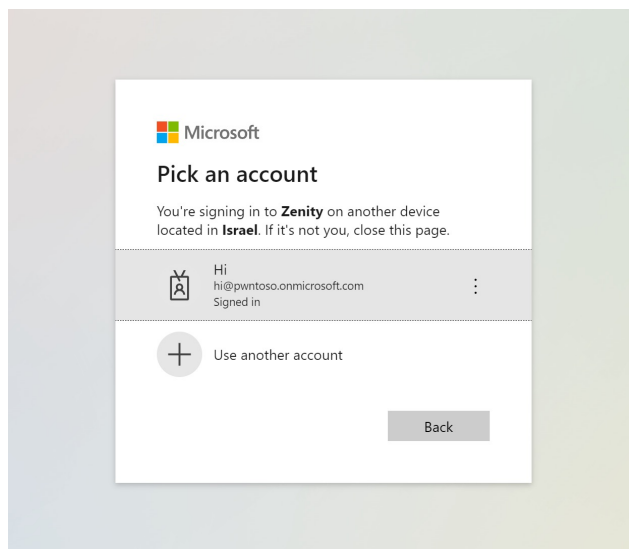


A scope away

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?

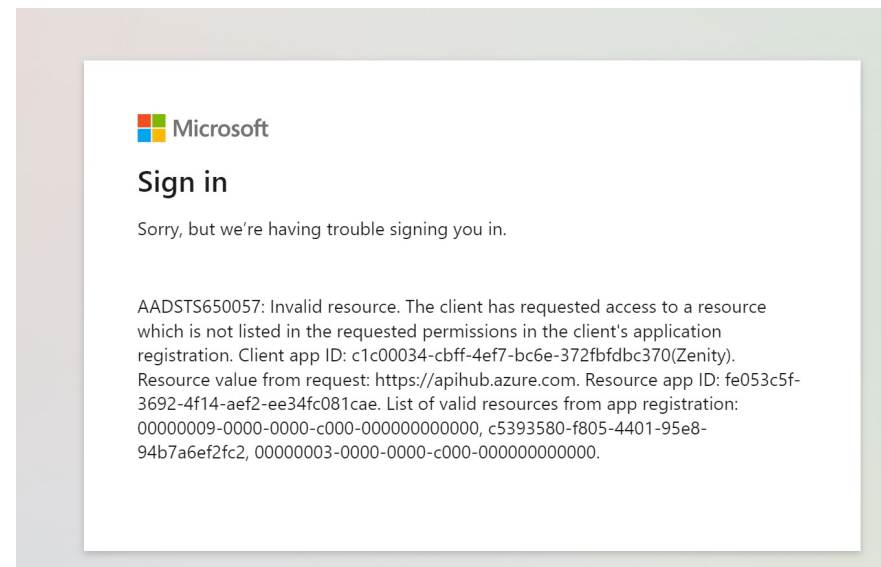
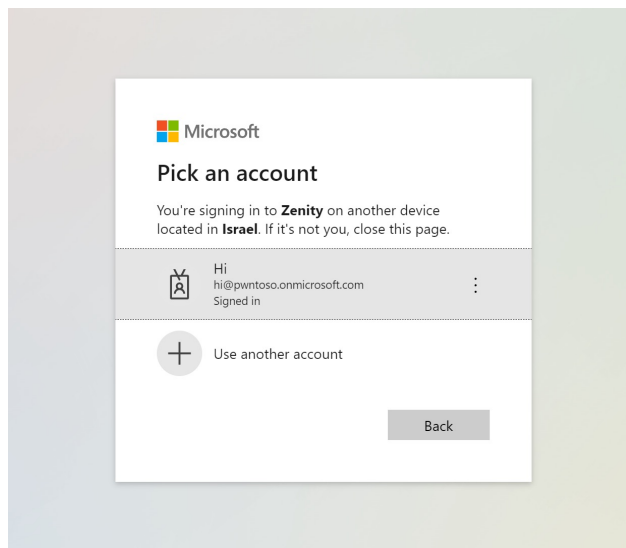


A scope away

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

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

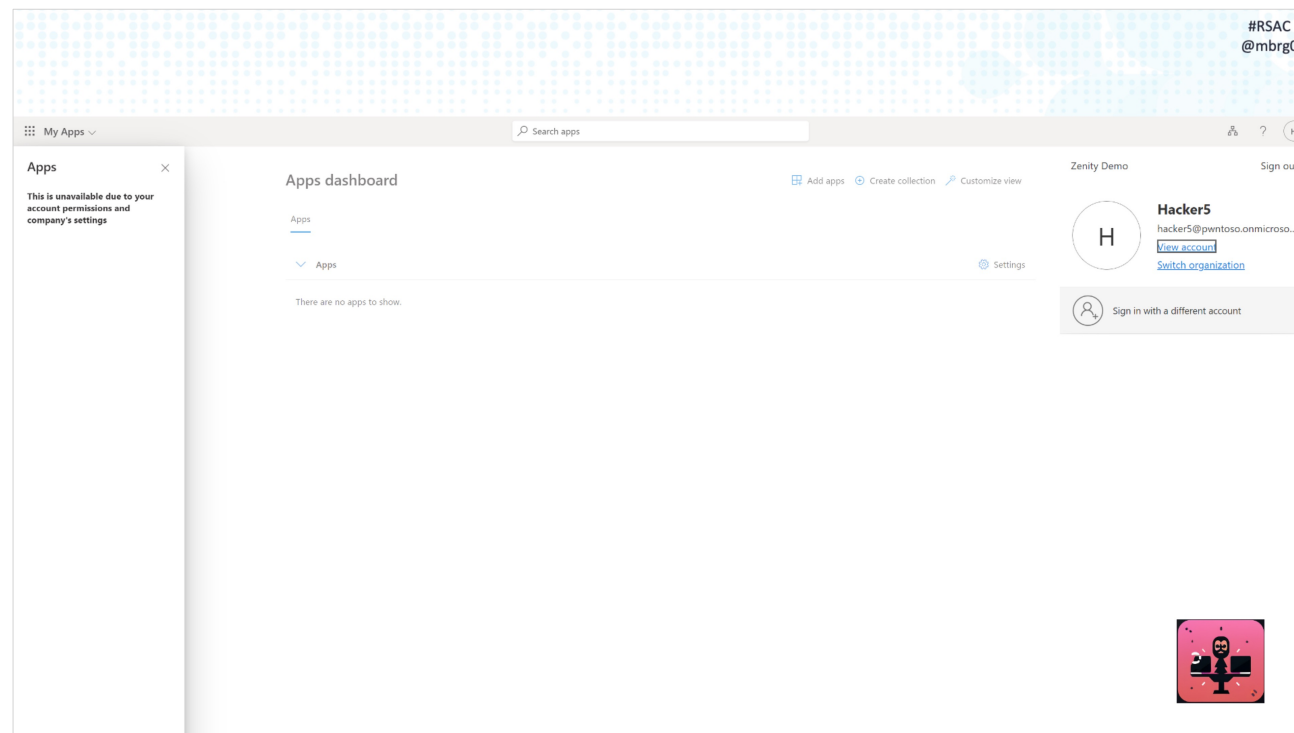
Using a built-in public client app? **No.**

Using our own app? **No.**



Where are we again?

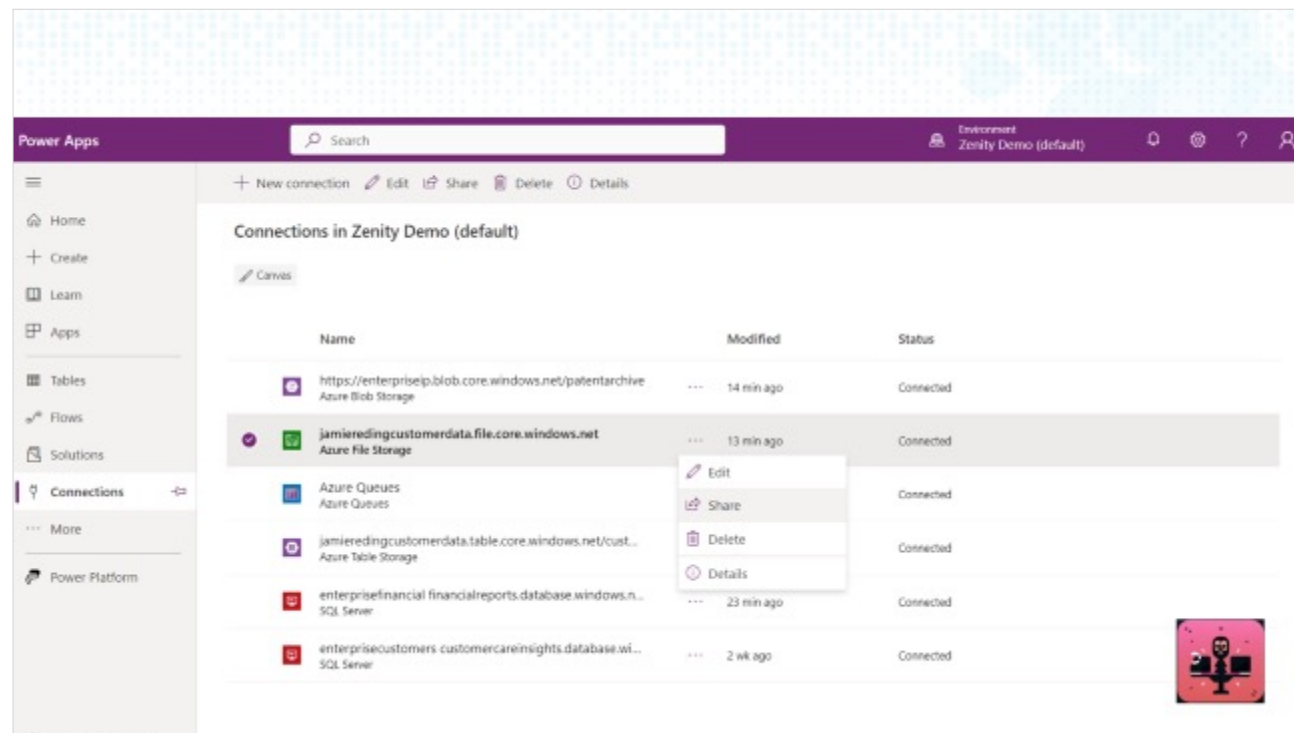
Got guest access.



Where are we again?

Got guest access.

Found a bunch of creds on Power Apps.

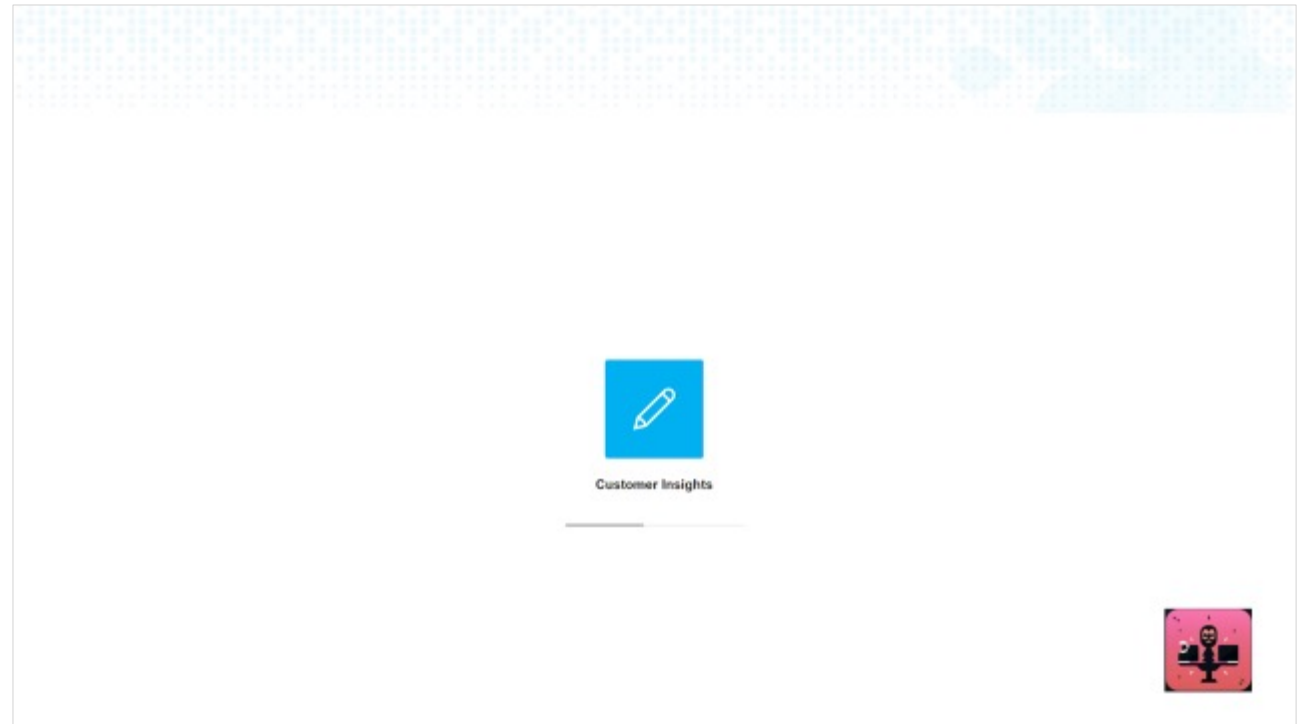


Where are we again?

Got guest access.

Found a bunch of creds on Power Apps.

Tried to access



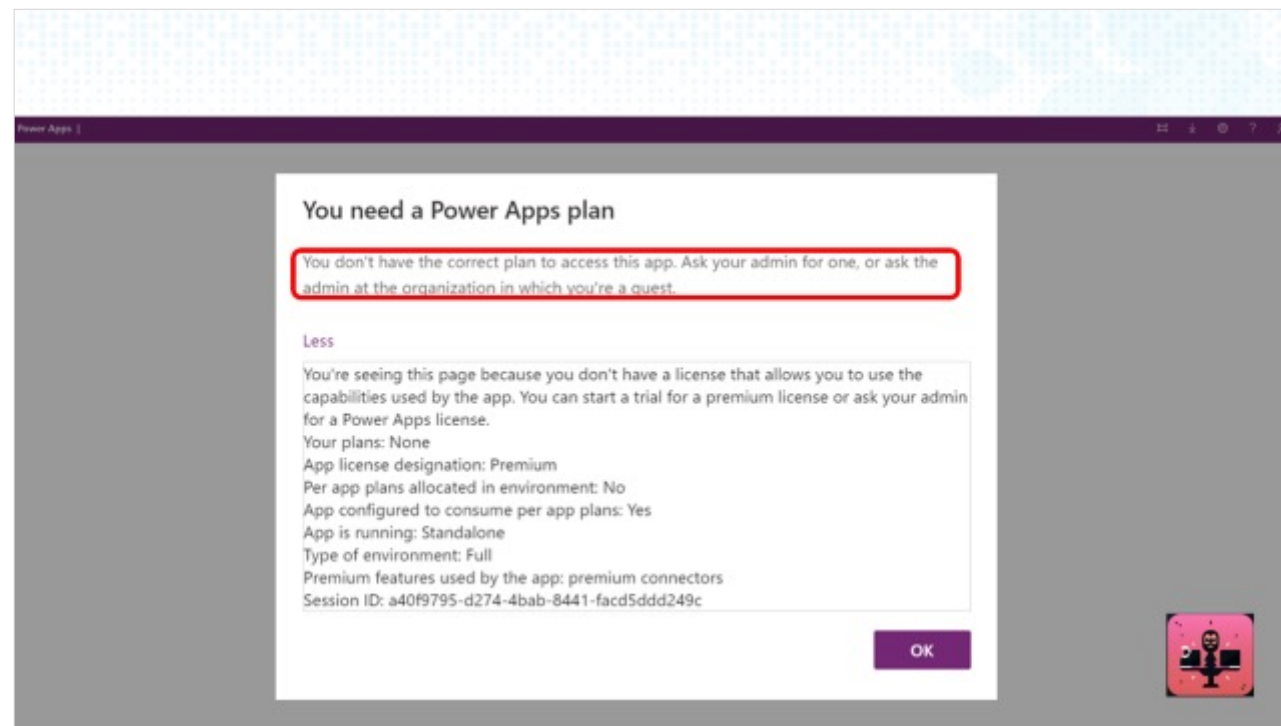
Where are we again?

Got guest access.

Found a bunch of creds on Power Apps.

Tried to access

→ Blocked by license



Where are we again?

Got guest access.

Found a bunch of creds on Power Apps.

Tried to access

→ Blocked by license → Got a license

Where are we again?

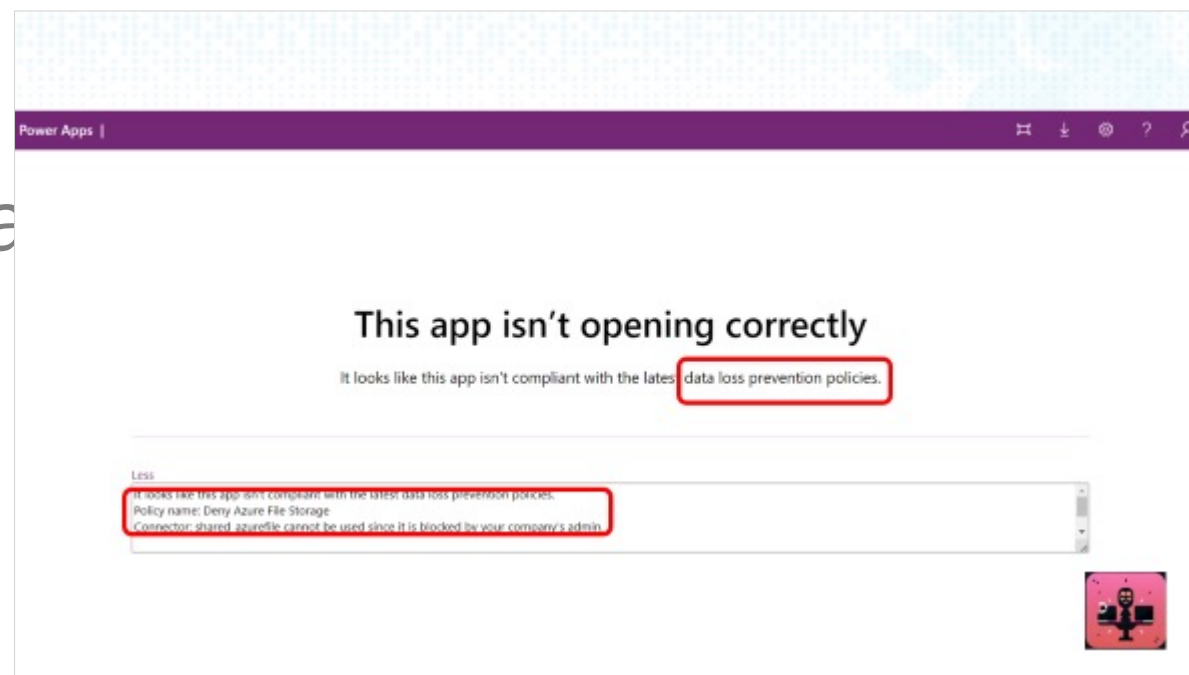
Got guest access.

Found a bunch of creds on Power Apps.

Tried to access

→ Blocked by license → Got a

→ **Blocked by DLP**



Where are we again?

Got guest access.

Found a bunch of creds on Power Apps.

Tried to access

→ Blocked by license → Got a license

→ Blocked by DLP → Copy-paste DLP bypass

Where are we again?

Got guest access.

Found a bunch of creds on Power Apps.

Tried to access

- Blocked by license → Got a license
- Blocked by DLP → Copy-paste D
- Block by prog access to API Hub

#RSAC
@mbrg0

A scope away

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.**



zenity

106

RSAConference2024

Solving for scope

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

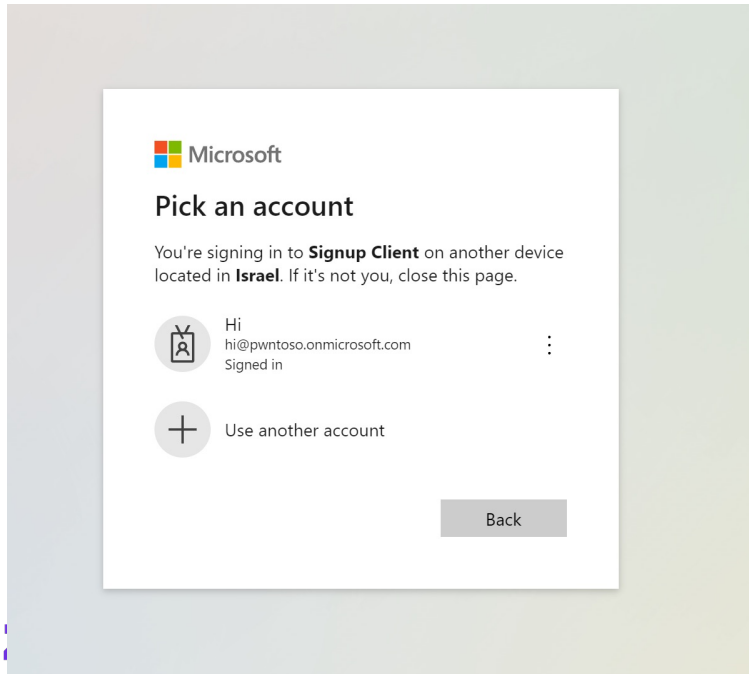
Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

```
>>> 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)

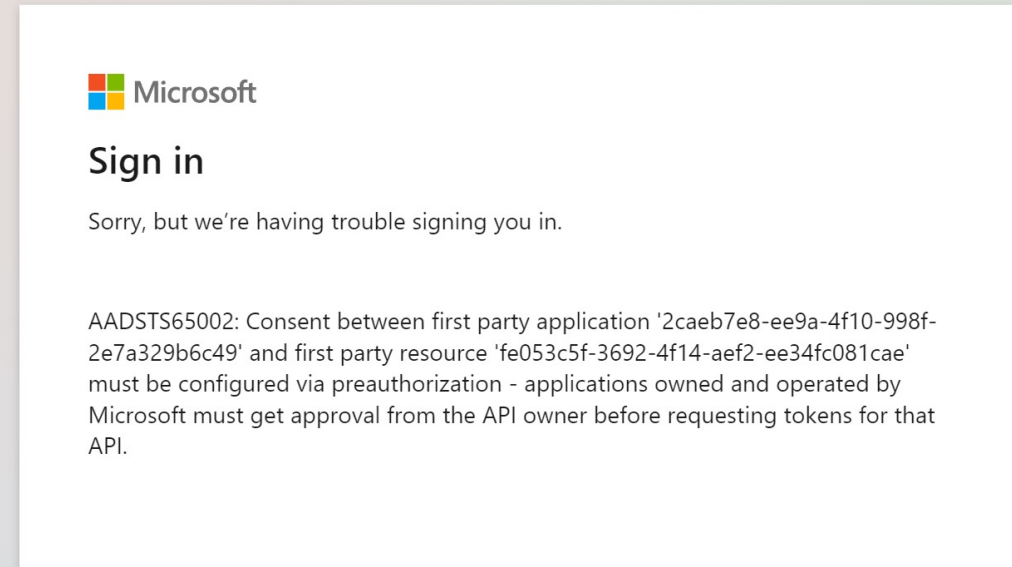
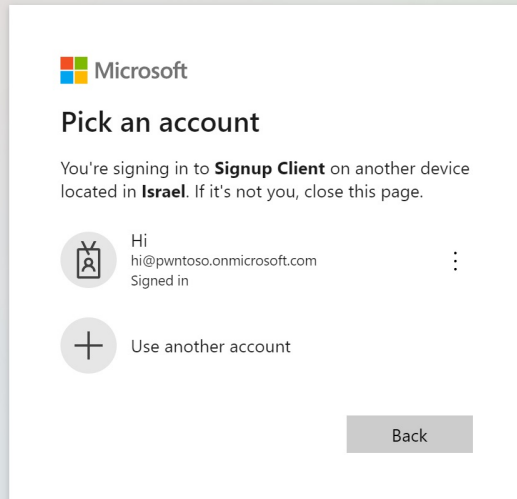
Using a built-in public client app?



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.**

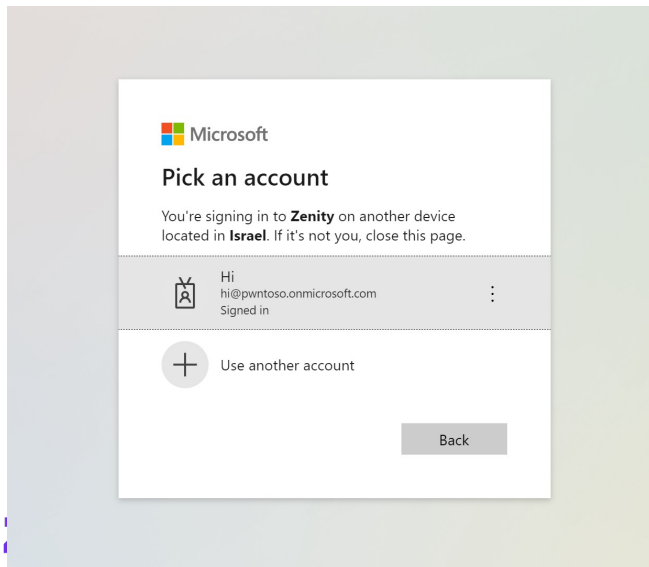


A scope away from victory

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?

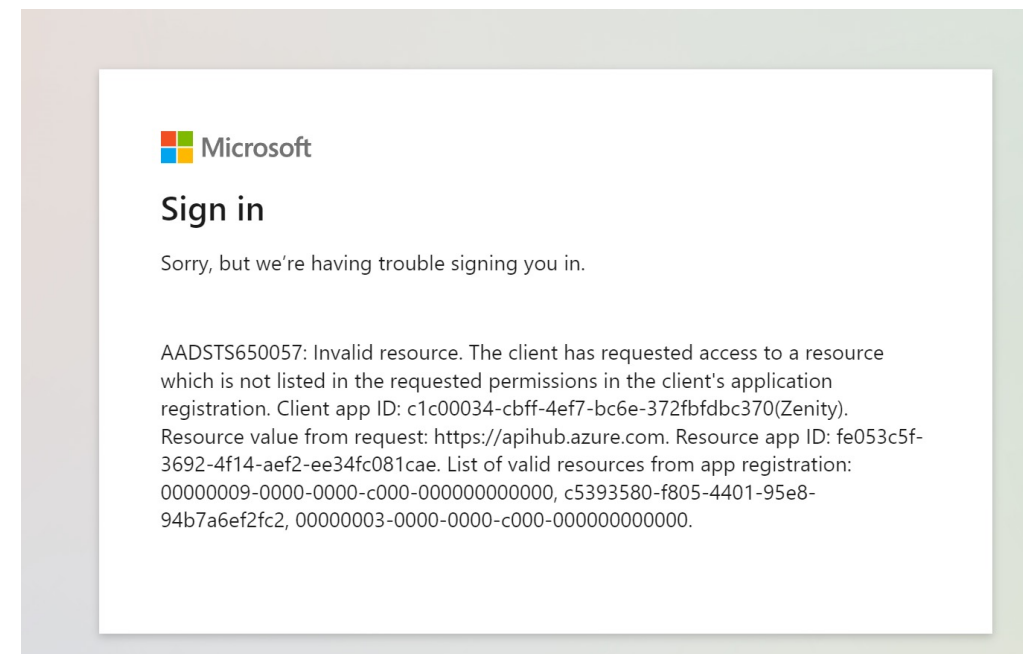
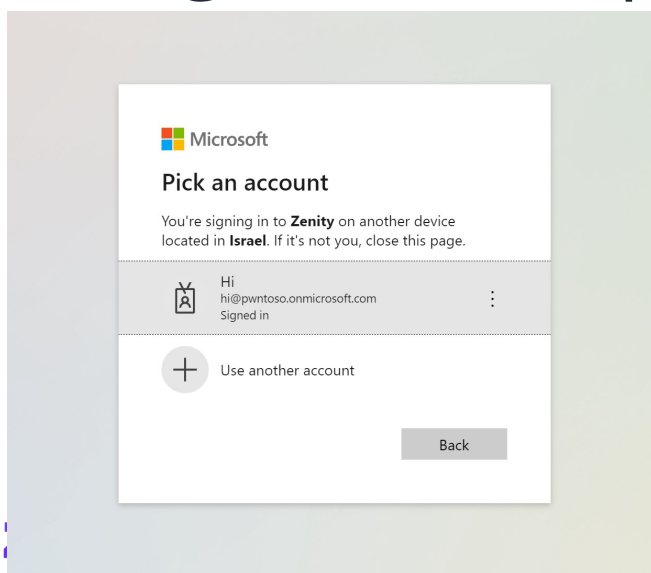


A scope away from victory

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.**



Solving for scope

- We need to find an AAD app that is:

Solving for scope

- We need to find an AAD app that is:
 - Is on by-default (available in every tenant)

Solving for scope

- We need to find an AAD app that is:
 - Is on by-default (available in every tenant)
 - Pre-approved to query API Hub (get internal resource)

Solving for scope

- We need to find an AAD app that is:
 - Is on by-default (available in every tenant)
 - Pre-approved to query API Hub (get internal resource)
 - Public client (generate tokens on demand)

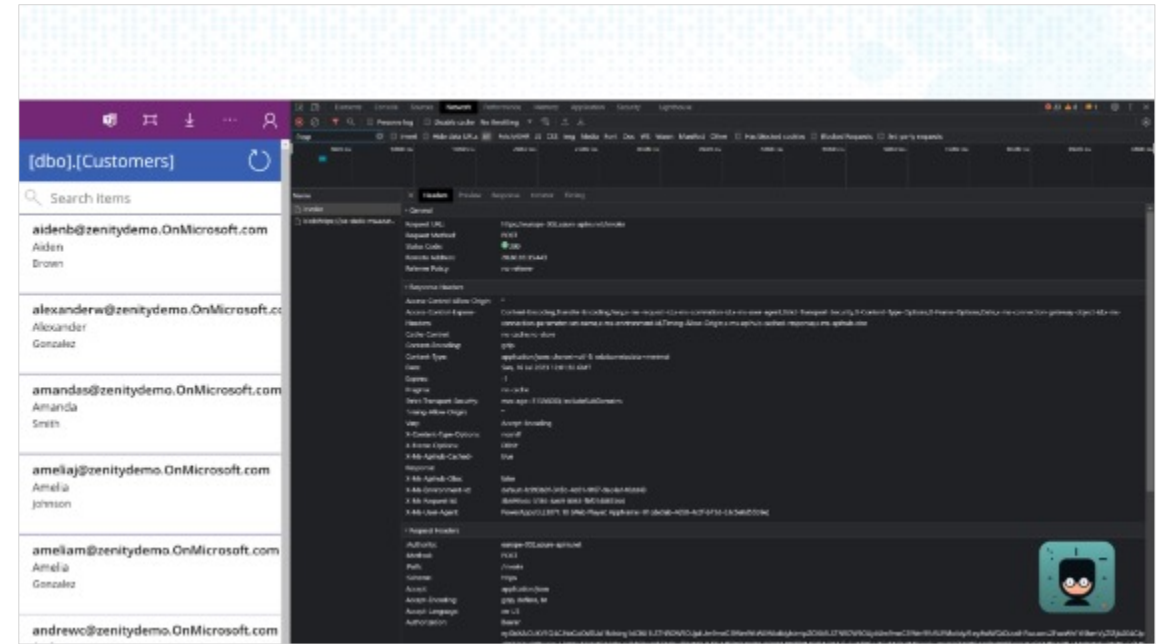
Solving for scope

- We need to find an AAD app that is:
 - Is on by-default
 - Pre-approved to query API Hub
 - Public client

Solving for scope

- We need to find an AAD app that is:
 - Is on by-default
 - Pre-approved to query API Hub
 - Public client

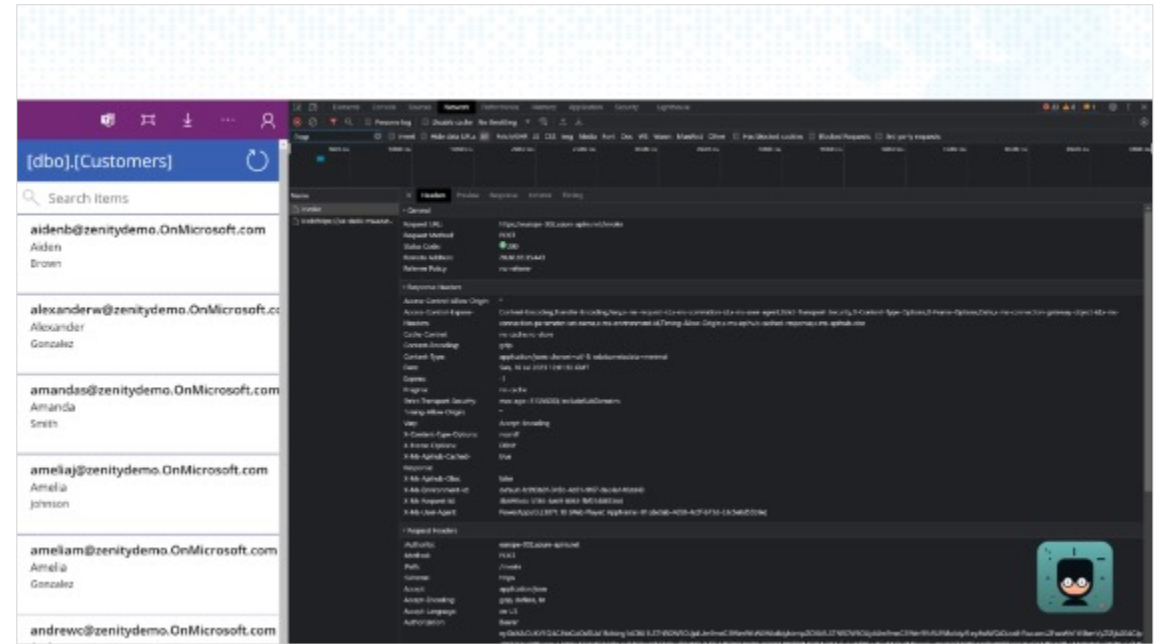
Well, we know about
the PowerApps portal!



Solving for scope

- We need to find an AAD app that is:
 - Is on by-default
 - Pre-approved to query API Hub
 - Public client

Well, we know about
the PowerApps portal!

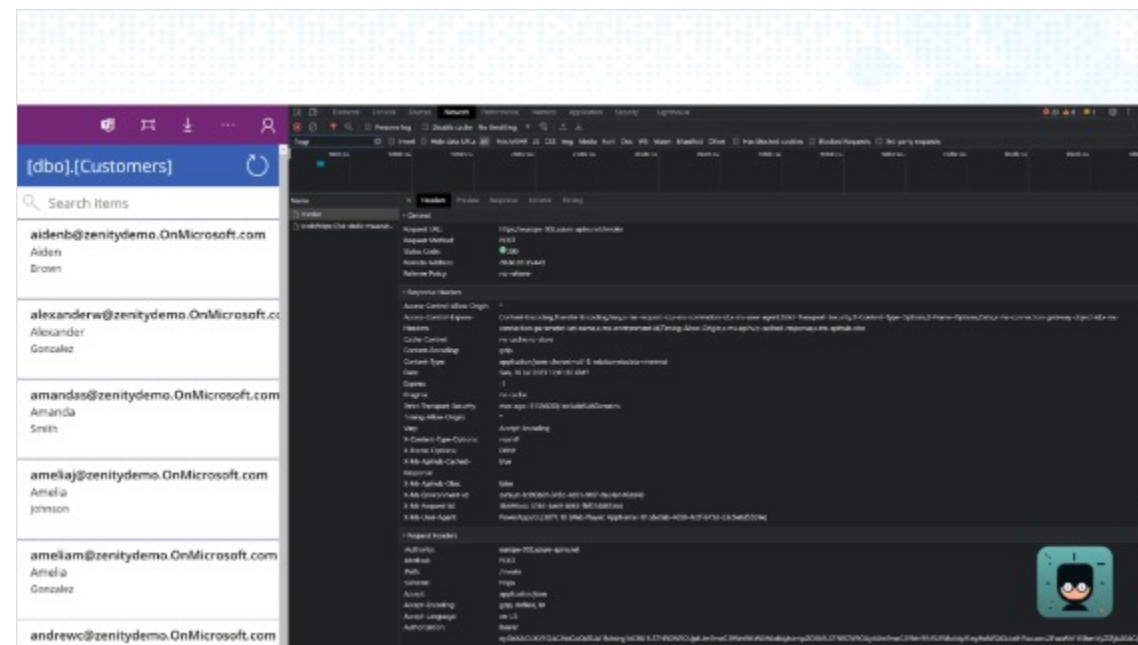


Solving for scope

- We need to find an AAD app that is:
 - Is on by-default
 - Pre-approved to query API Hub
 - **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



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

application_name

Office 365 Management

Microsoft Azure CLI

Microsoft Azure PowerShell

Microsoft Teams

Windows Search

Outlook Mobile

Microsoft Authenticator App

OneDrive SyncEngine

Microsoft Office

Visual Studio

OneDrive iOS App

Microsoft Bing Search for Microsoft Edge

Microsoft Stream Mobile Native

Microsoft Teams - Device Admin Agent

Microsoft Bing Search

Office UWP PWA

Microsoft To-Do client

PowerApps

Microsoft Whiteboard Client

Microsoft Flow

Microsoft Planner

Microsoft Intune Company Portal

Accounts Control UI

Yammer iPhone

OneDrive

Microsoft Power BI

SharePoint

Microsoft Edge

Microsoft Tunnel

Microsoft Edge

SharePoint Android

Microsoft Edge

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

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

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

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

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

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

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

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

Family of client IDs

Microsoft
Azure CLI

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

Research into Undocumented Behavior of Azure AD
Refresh Tokens

1
Contributor

0
Issues

97
Stars

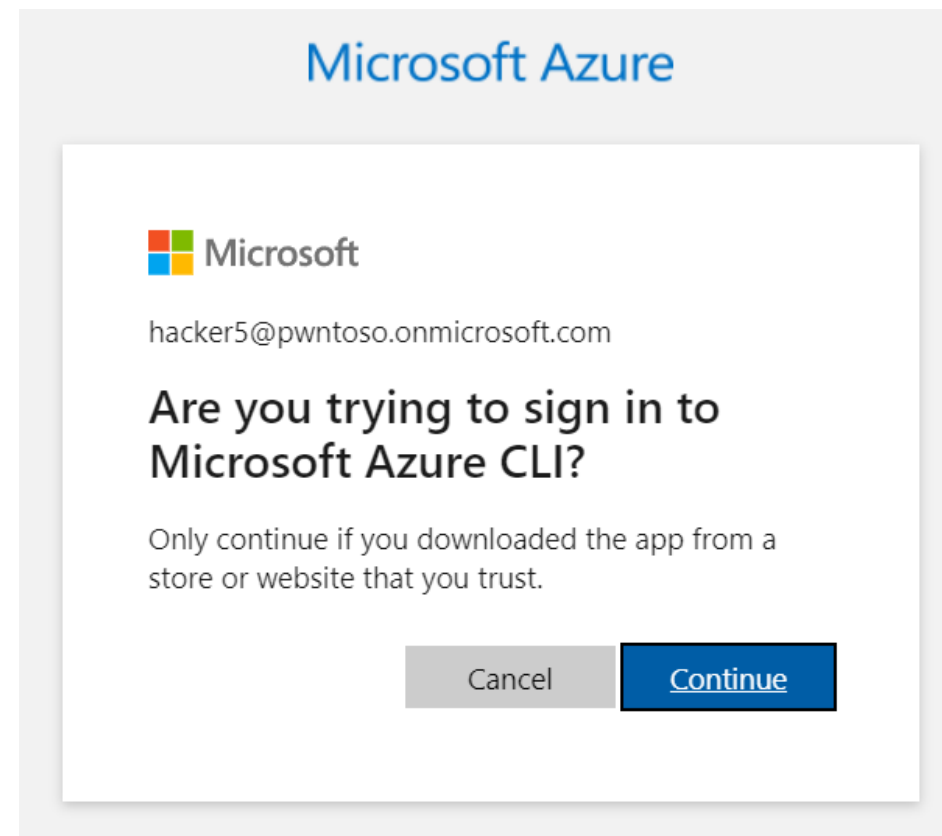
10
Forks



API Hub
token

Exchange tokens to win

- We need to find an AAD app that is:
 - Is on by-default
 - Pre-approved to query API Hub
 - Public client



Implications

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

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

positional arguments:

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

command

```
dump          Recon for available data connections and dump their content.
```

```
gui          Show collected resources and data via GUI.
```

```
backdoor          Install a backdoor on the target tenant
```

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

phishing Deploy a trustworthy phishing app.

optional arguments:

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

```
-l LOG_LEVEL, --log-level LOG_LEVEL
```

Configure the logging level.




```
-----
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
posit     Deploy a trustworthy phishing app.
```

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

optional arguments:

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

```
-l LOG LEVEL, --log-level LOG LEVEL
```

Configure the logging level.



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

powerpwn



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.

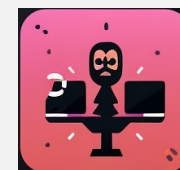


Hacker5
hacker5@pwntoso.onmicrosoft.com
Signed in



Use another account

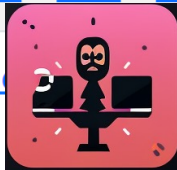
Back



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	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

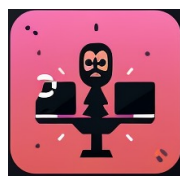
- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by			
 shared_azurefile	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		Dump

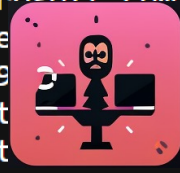


.cache / data / Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43 / connections / shared_sql / ff47194e357e459b8756a5f43f59cccc6 / table

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




```
[{"@odata.etag": "", "ItemInternalId": "7eb41684-4b64-4f39-9eab-90fbe30ba62c", "CustomerID": 34553, "FirstName": "Jamie", "LastName": "Reding", "Email": "jamier@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1111"}, {"@odata.etag": "", "ItemInternalId": "566a2e62-1c95-4e49-bdc6-c141023d66ac", "CustomerID": 98256, "FirstName": "Christa", "LastName": "Geller", "Email": "christag@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-2222"}, {"@odata.etag": "", "ItemInternalId": "43288280-ae24-450e-9feb-f6605d9c1ec2", "CustomerID": 76234, "FirstName": "David", "LastName": "Brenner", "Email": "davidb@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-3333"}, {"@odata.etag": "", "ItemInternalId": "52f7ad4a-9159-486e-885c-69c78fa59138", "CustomerID": 43256, "FirstName": "Laura", "LastName": "Miller", "Email": "lauram@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4444"}, {"@odata.etag": "", "ItemInternalId": "e53da160-f087-4e08-b3fb-eb16283781c5", "CustomerID": 67322, "FirstName": "Robert", "LastName": "Thompson", "Email": "robertt@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5555"}, {"@odata.etag": "", "ItemInternalId": "f6ce0c32-b846-4c4a-ad61-2f3bf74d0d06", "CustomerID": 78654, "FirstName": "Amanda", "LastName": "Smith", "Email": "amandas@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6666"}, {"@odata.etag": "", "ItemInternalId": "e998798e-2e21-408f-b3e6-2ff7fde41510", "CustomerID": 89322, "FirstName": "John", "LastName": "Davis", "Email": "johnd@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-7777"}, {"@odata.etag": "", "ItemInternalId": "9219f091-1238-4cf8-b9a7-f4b7e3f3a958", "CustomerID": 11245, "FirstName": "Emily", "LastName": "Harris", "Email": "emilyh@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-8888"}, {"@odata.etag": "", "ItemInternalId": "8ba98fcc-b7f8-401f-abf5-842065f37d56", "CustomerID": 55677, "FirstName": "Michael", "LastName": "Sanders", "Email": "michaels@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9999"}, {"@odata.etag": "", "ItemInternalId": "425f5a25-0f8d-4295-a3bf-7ab0388f8d7a", "CustomerID": 68984, "FirstName": "Sophie", "LastName": "Carter", "Email": "sophie@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": 45, "FirstName": "Jason", "LastName": "Mitchell", "Email": "jasonm@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-09"}, {"@odata.etag": "", "ItemInternalId": "bc932b1b-5ff2-4c8d-a28f-6ac86eed4529", "CustomerID": 74321, "FirstName": "Sarah", "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"}, {"@odata.etag": "", "ItemInternalId": "66b0f513-b405-4005-8000-000000000000", "CustomerID": 12345, "FirstName": "Alice", "LastName": "Johnson", "Email": "alicej@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1234"}]
```



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



SqlPassThroughNativeQuery



POST

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

^

🔒

Parameters

Try it out

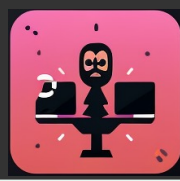
Name	Description
------	-------------

dataset * required string (path)	dataset
---	--------------------------------------

language * required string (path)	language
--	---------------------------------------

query * required object (body)	Example Value Model <pre>{ "actualParameters": { "additionalProp1": {}, "additionalProp2": {}, "additionalProp3": {} }, "formalParameters": { "additionalProp1": "string", "additionalProp2": "string", "additionalProp3": "string" }, "query": "string" }</pre>
---	--

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.

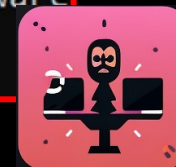
Install with `pip install powerpwn`.

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.

Try it for yourself!

github.com/mbrg/power-pwn



RSACConference™2024

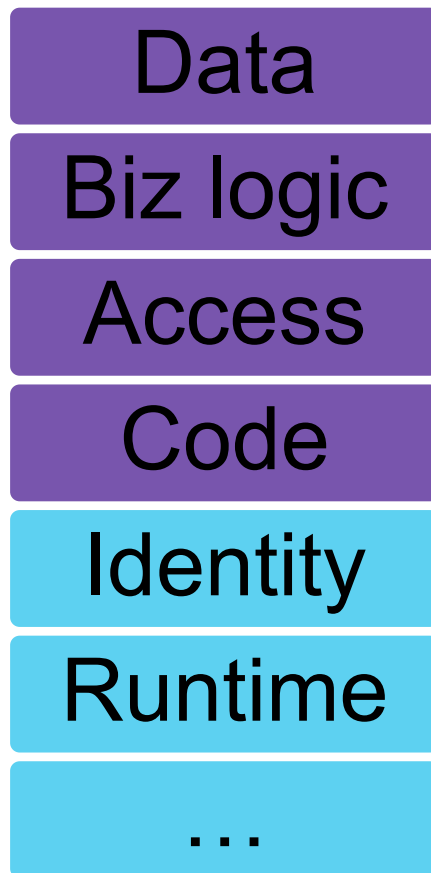
How to protect your org

#RSAC
@mbrg0

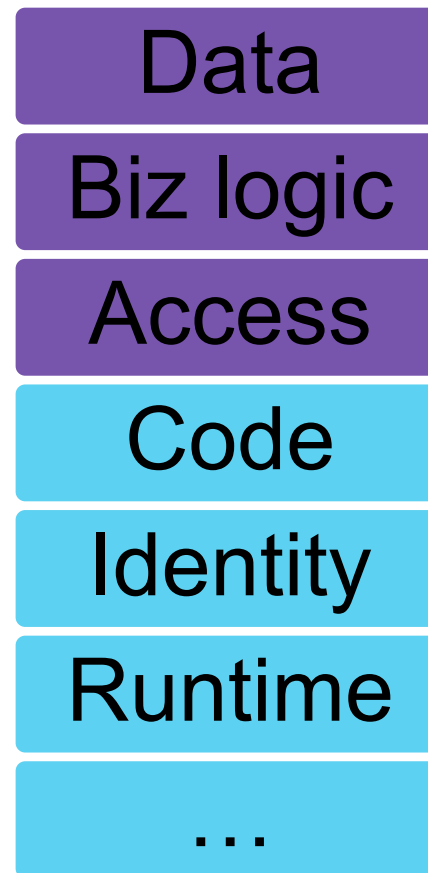
The Shared Responsibility Model

**We must own
our part.**

Cloud



M365



Customer

Platform

Platforms must step up

Data

Biz logic

Access

Code

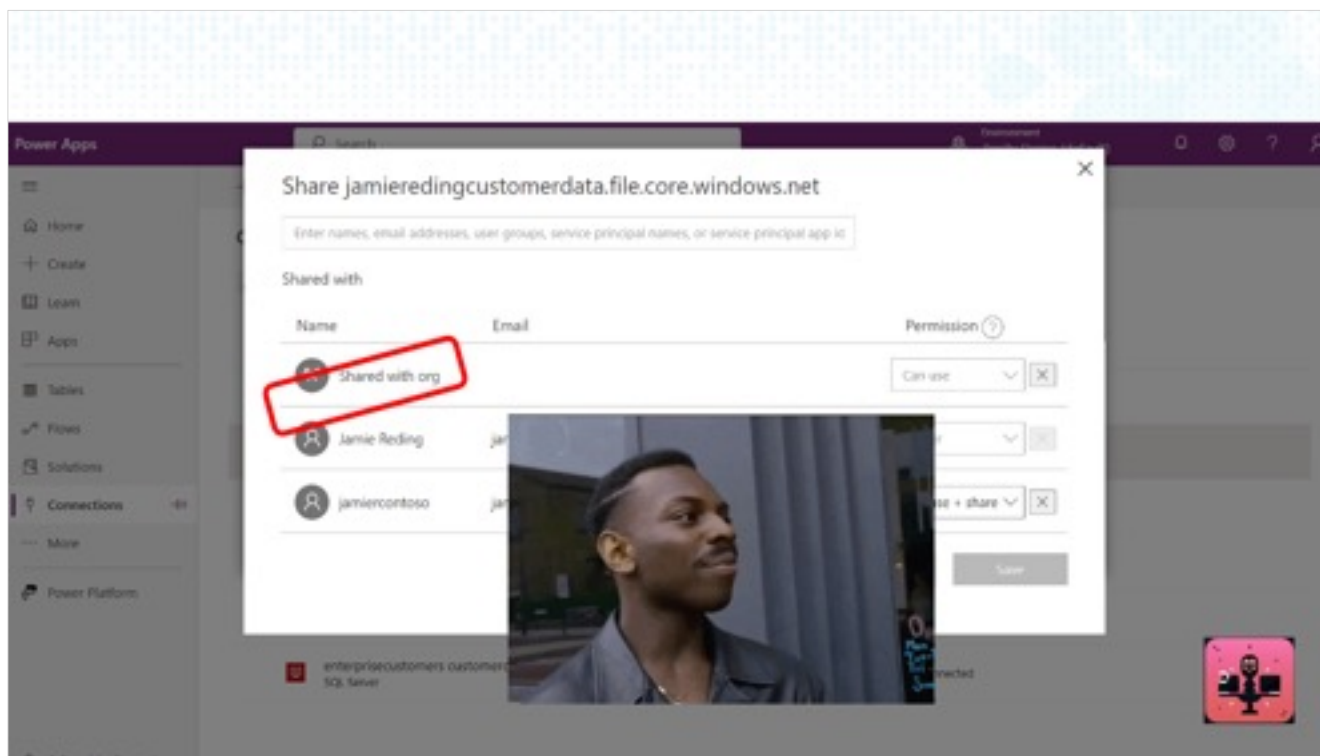
Identity

Runtime

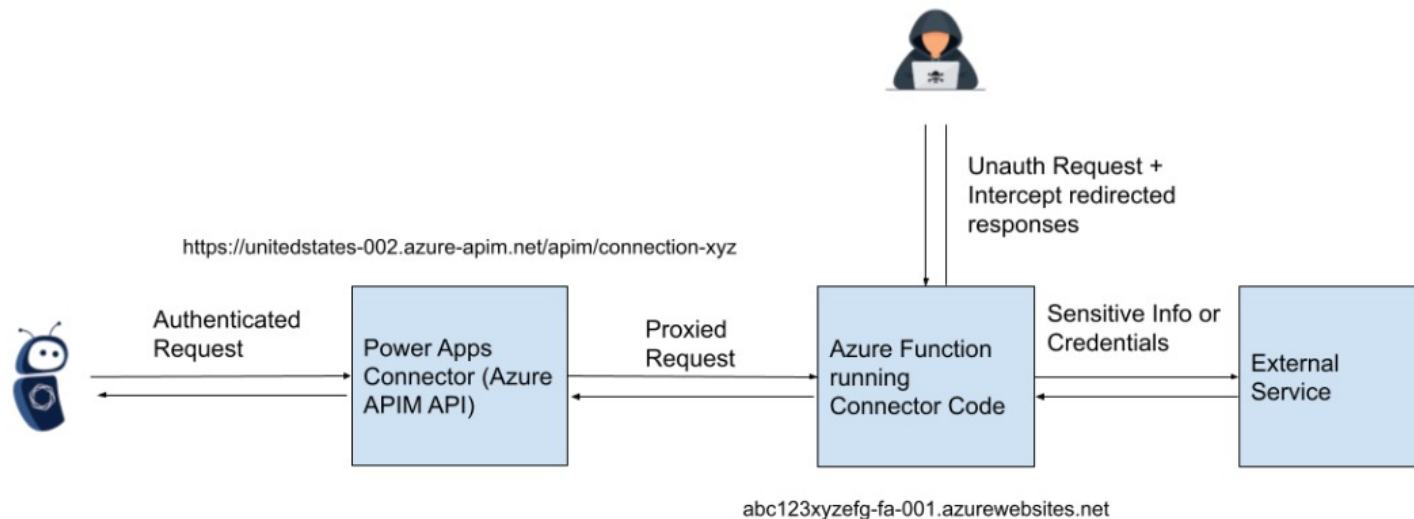
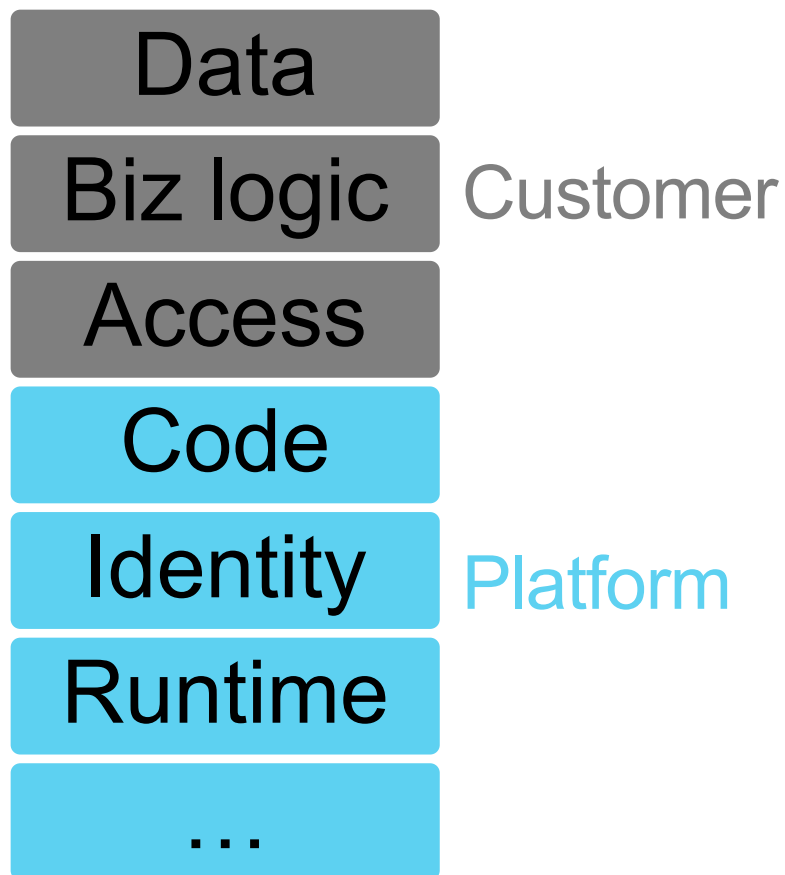
...

Customer

Platform

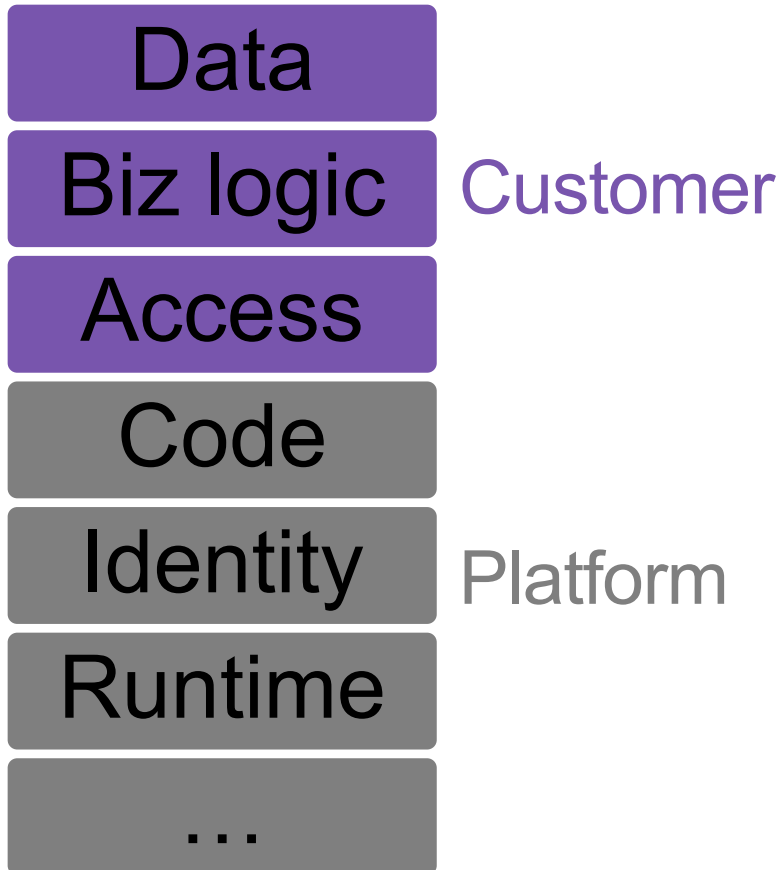


Platforms must step up



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

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



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

Who owns AppSec for apps built by business users?

Apply What You Have Learned Today

configs, links and details → mbgsec.com/rsac2024

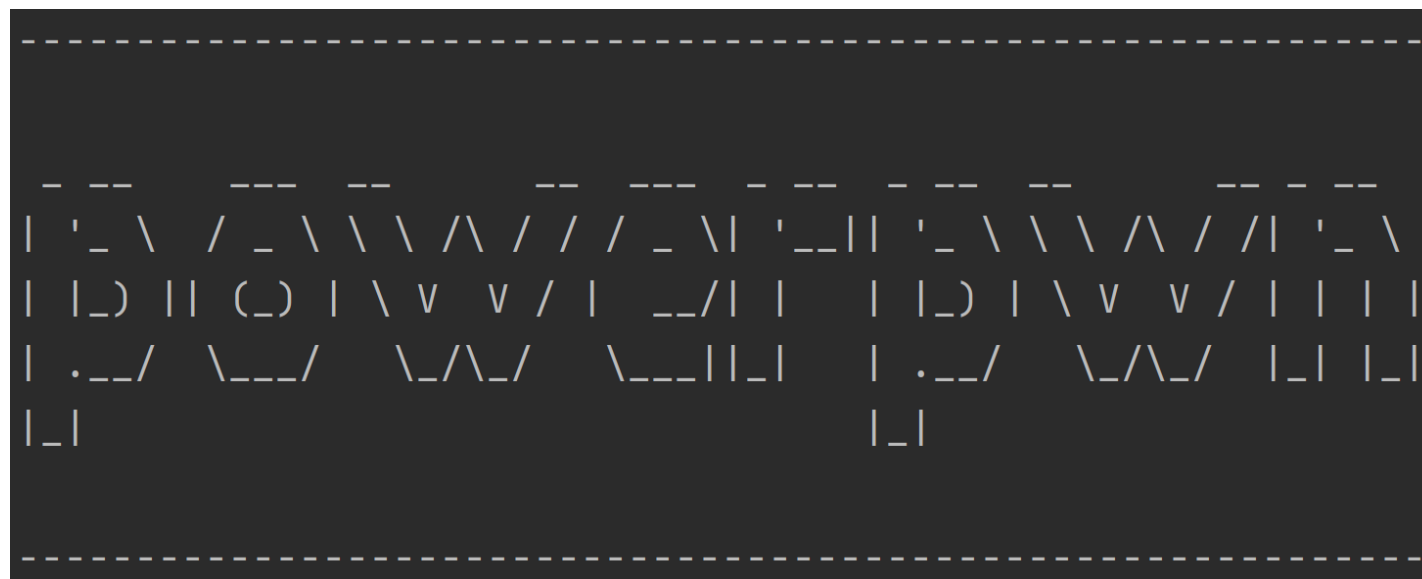
Apply What You Have Learned Today

- Hack your env today

configs, links and details → mbgsec.com/rsac2024

Apply What You Have Learned Today

- Hack your env today
 - powerpwn



configs, links and details → mbgsec.com/rsac2024

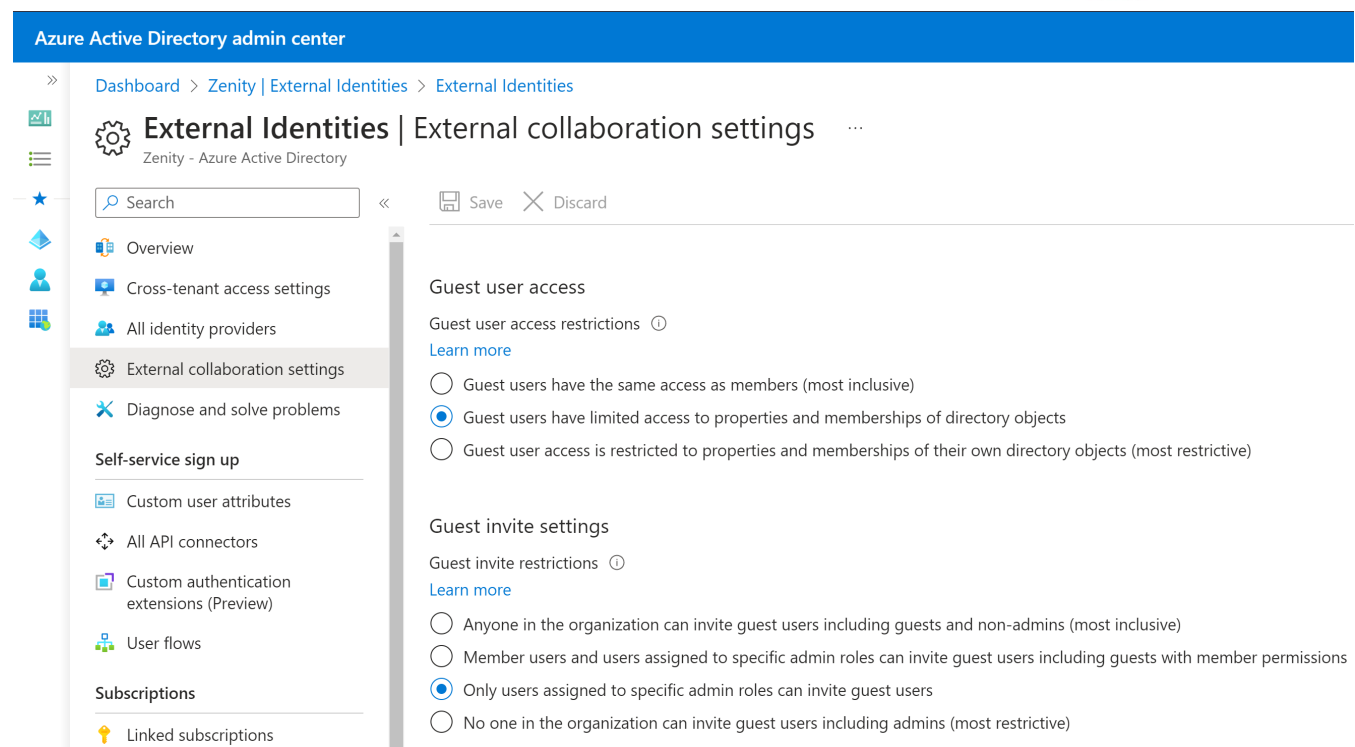
Apply What You Have Learned Today

- Hack your env today
 - powerpwn
- Harden your env this month

configs, links and details → mbgsec.com/rsac2024

Apply What You Have Learned Today

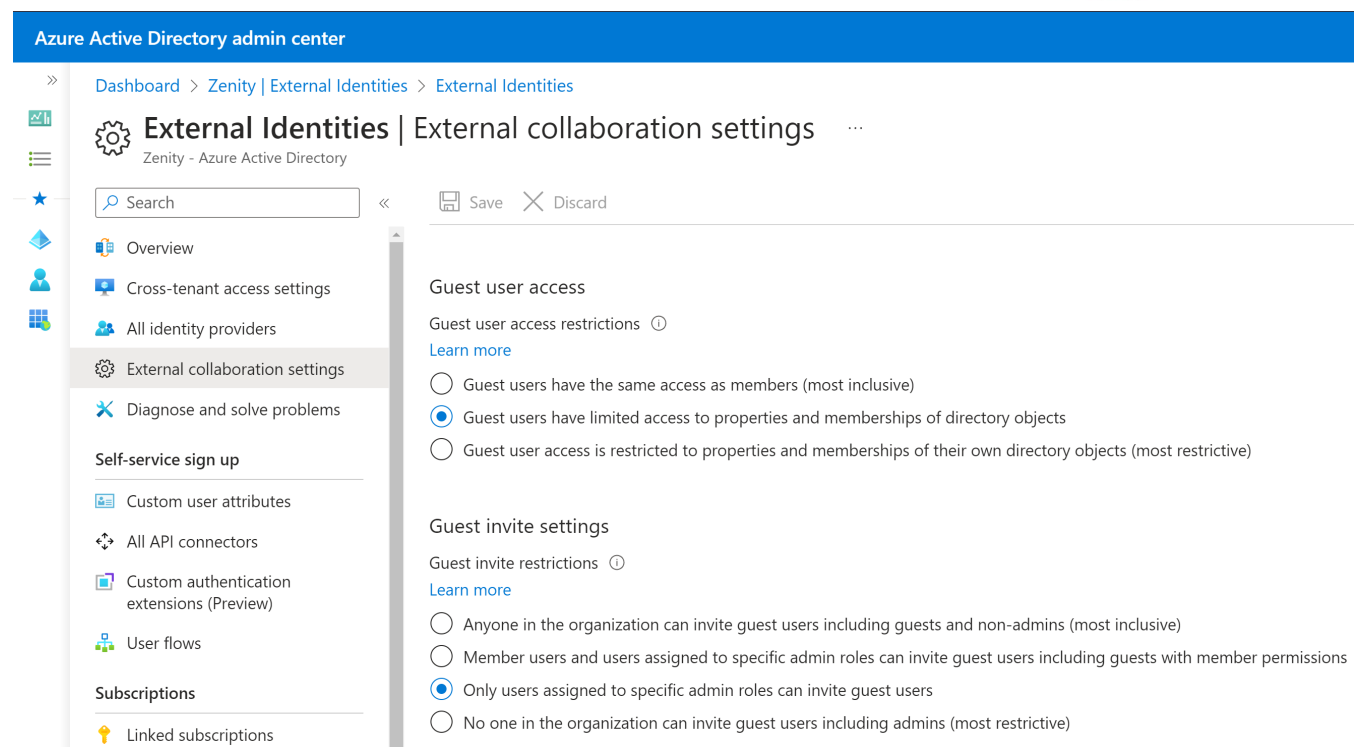
- Hack your env today
 - powerpwn
- Harden your env this month
 - Secure configs



configs, links and details → mbgsec.com/rsac2024

Apply What You Have Learned Today

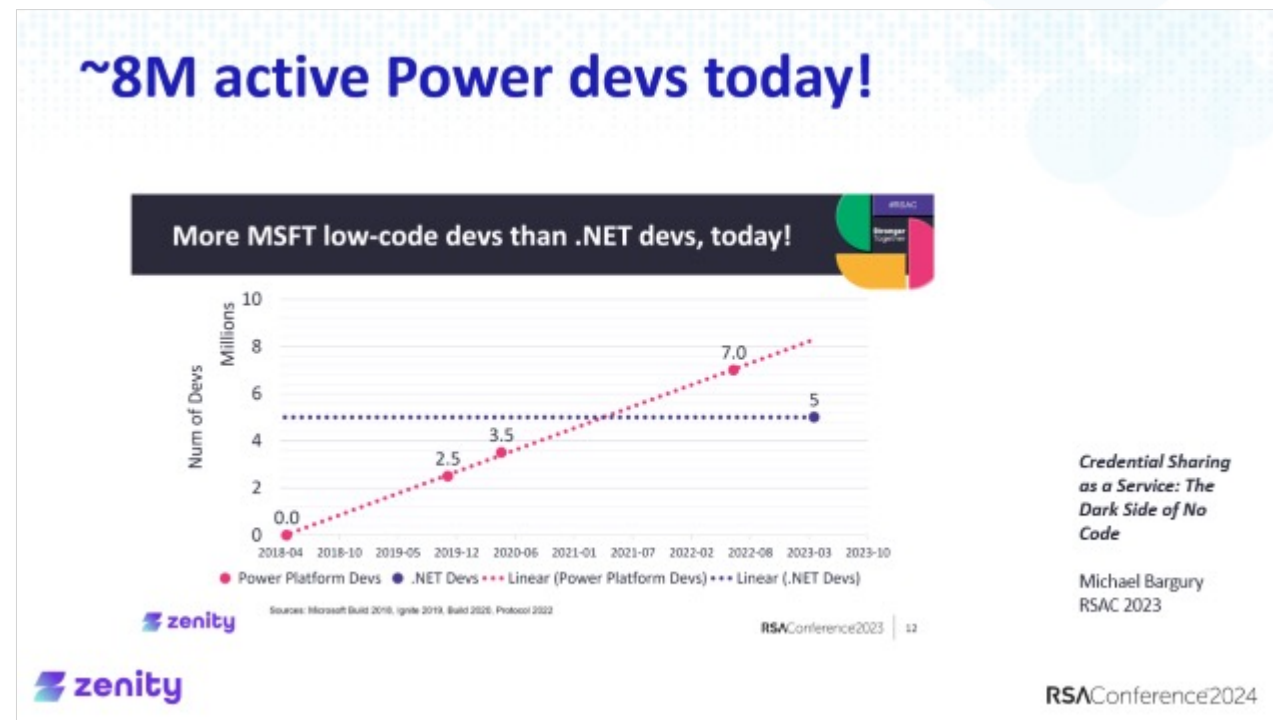
- Hack your env today
 - powerpwn
- Harden your env this month
 - Secure configs
 - Audit logs



configs, links and details → mbgsec.com/rsac2024

Apply What You Have Learned Today

- Hack your env today
 - powerpwn
- Harden your env this month
 - Secure configs
 - Audit logs
- Establish an AppSec program this quarter



configs, links and details → mbgsec.com/rsac2024

Apply What You Have Learned Today

- Hack your env today
 - powerpwn
- Harden your env this month
 - Secure configs
 - Audit logs
- Establish an AppSec program this quarter
 - Set oversharing guardrails

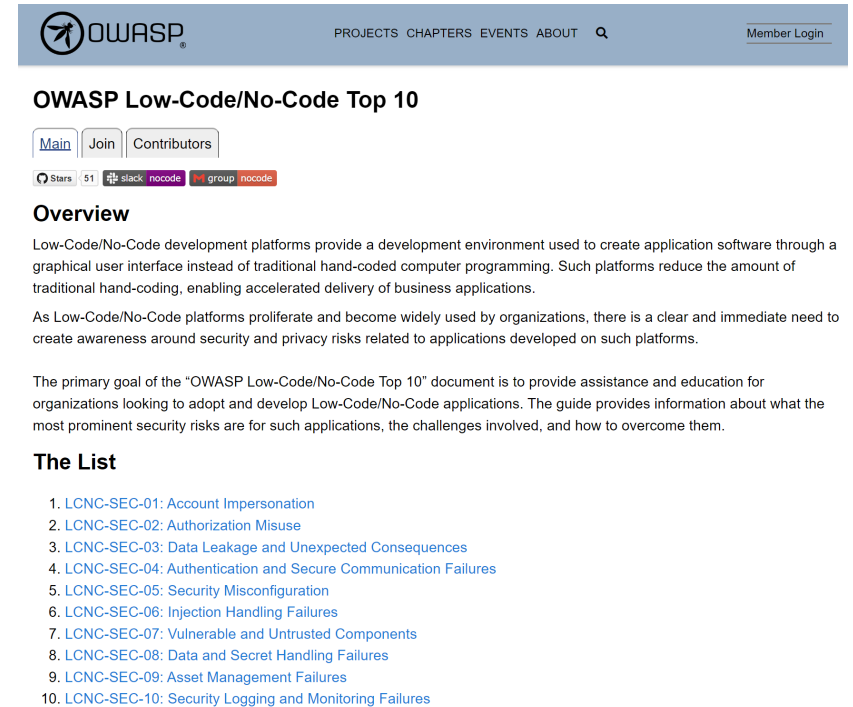


configs, links and details → mbgsec.com/rsac2024

Apply What You Have Learned Today

- Hack your env today
 - powerpwn
- Harden your env this month
 - Secure configs
 - Audit logs
- Establish an AppSec program this quarter
 - Set oversharing guardrails
 - Leverage the OWASP LCNC Top 10

configs, links and details → mbgsec.com/rsac2024



The screenshot shows the OWASP Low-Code/No-Code Top 10 page. The header includes the OWASP logo, navigation links for PROJECTS, CHAPTERS, EVENTS, ABOUT, and a search icon, along with a Member Login link. The main heading is "OWASP Low-Code/No-Code Top 10". Below this are tabs for Main, Join, and Contributors, and social media links for Stars, Slack, NoCode, and a GitHub group. The "Overview" section explains that Low-Code/No-Code development platforms provide a graphical user interface instead of traditional hand-coded programming, reducing the amount of traditional hand-coding. It also states that as these platforms proliferate, there is a need to create awareness around security and privacy risks. The "The List" section contains a numbered list of 10 security categories, such as "LCNC-SEC-01: Account Impersonation" and "LCNC-SEC-10: Security Logging and Monitoring Failures".

OWASP Low-Code/No-Code Top 10

Main Join Contributors

Stars 51 slack nocode github group nocode

Overview

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

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

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

The List

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

RSACTMConference2024

San Francisco | May 6 – 9 | Moscone Center

SESSION ID: HTA-M02

All You Need Is Guest

THE ART OF
POSSIBLE

#RSAC

Michael Bargury

Cofounder and CTO

Zenity

@mbrg0