zenity

Learn more: mbgsec.com
Twitter: @mbrg0

All You Need Is Guest

Michael Bargury @ Zenity
t2’24

zenity

DEMO

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

1 of 59

Zenity Demo invited you to access applications within their organization External

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

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

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

Organization: Zenity Demo
Domain: zenitydemo.onmicrosoft.com

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

Accept invitation

Block future invitations from this organization.

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

My Apps

Search apps

H

Apps

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

Apps dashboard

Add apps | Create collection | Customize view

Apps

Apps

Settings

There are no apps to show.

Zenity Demo

Sign out

H

Hacker5

hacker5@pwntoso.onmicroso...

View account

Switch organization

Sign in with a different account

powerpwn - Credentials

- All Resources
- Credentials
- Automations
- Applications
- Connectors

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

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":

@mbrg0
mbgsec.com
t2’24

Hi there👋

- CTO and Co-founder @ Zenity
- OWASP LCNC Top 10 project lead
- Dark Reading columnist
- BlackHat, Defcon, BSides, OWASP

- Hiring top researchers, engs & pms!

@mbrg0
github.com/mbrg
darkreading.com/author/michael-bargury

zenity

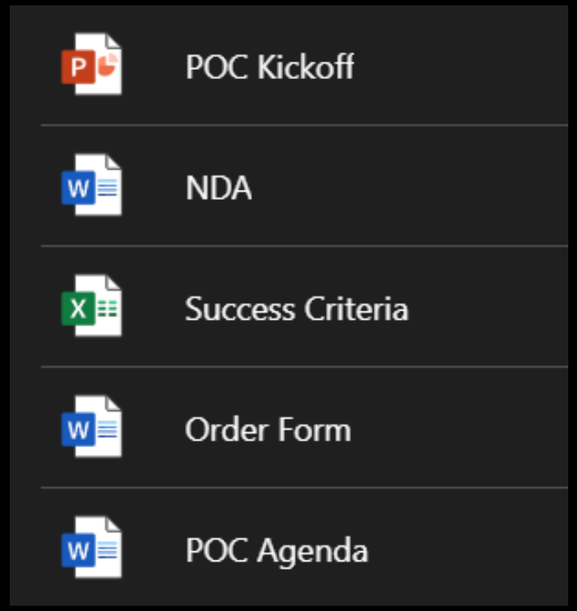
@mbrg0
mbgsec.com
t2’24

Why invite guests in?
And the promise of deny-by-default access

@mbrg0
mbgsec.com
t2’24

How can two parties collaborate over a bunch of files?

F1000 enterprise



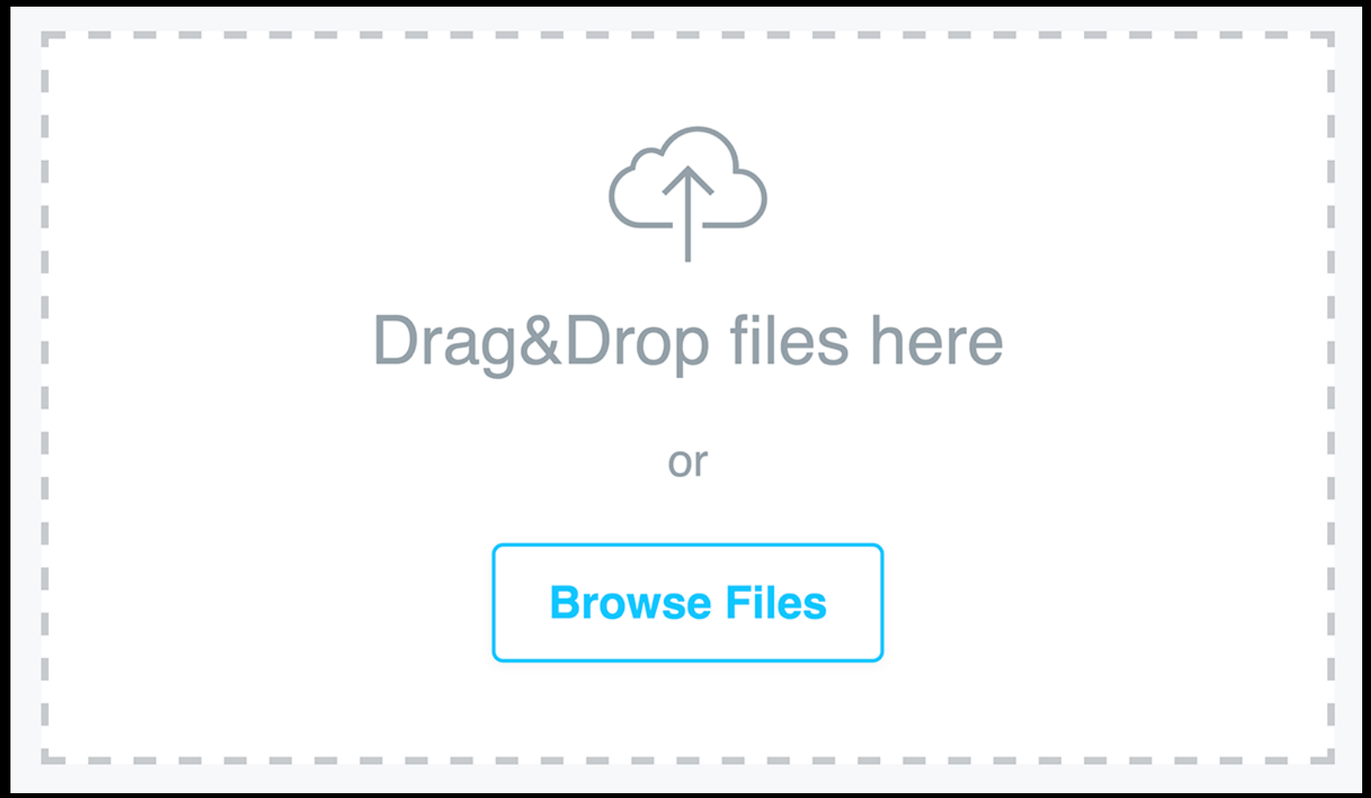
Small vendor

@mbrg0
mbgsec.com
t2’24

Option 1: just email sensitive files around

@mbrg0
mbgsec.com
t2’24

Option 2: trust a rando on the internet



@mbrg0
mbgsec.com
t2’24

Option 2: trust a rando IRL

Source: deaddrops.com

@mbrg0
mbgsec.com
t2’24

Option 3: invite them in

F1000 tenant

@mbrg0
mbgsec.com
t2’24

Option 3: invite them in

Microsoft Documentation

Learn / Azure / Active Directory /

External Identities in Azure Active Directory

“external users can "bring their own identities."
... and you manage access to your apps … to keep your resources protected.“

F1000 tenant

@mbrg0
mbgsec.com
t2’24

Safe guest access must be:

(a) Easy for vendors to onboard

@mbrg0
mbgsec.com
t2’24

Safe guest access must be:

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

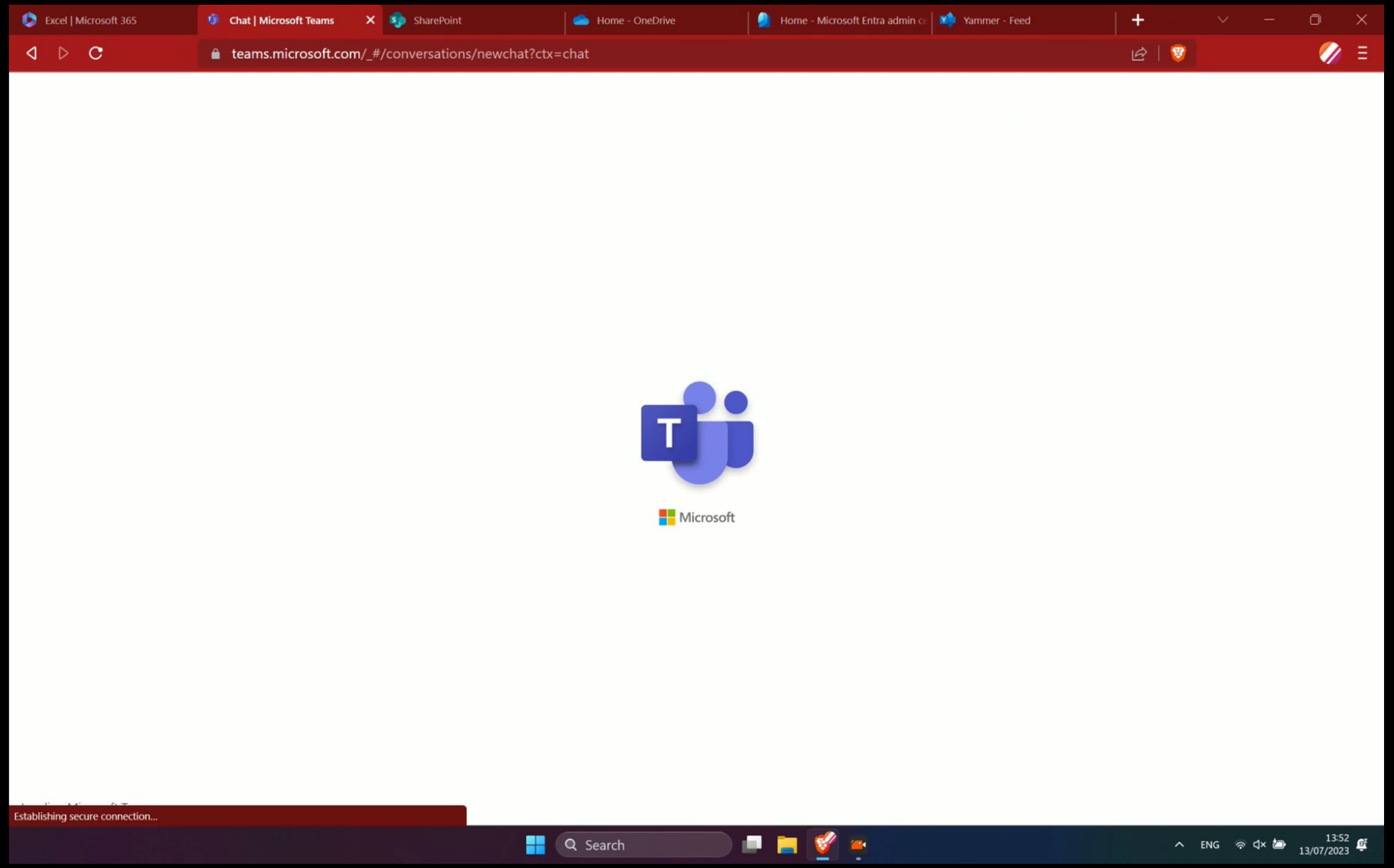
@mbrg0
mbgsec.com
t2’24

Safe guest access must be:

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

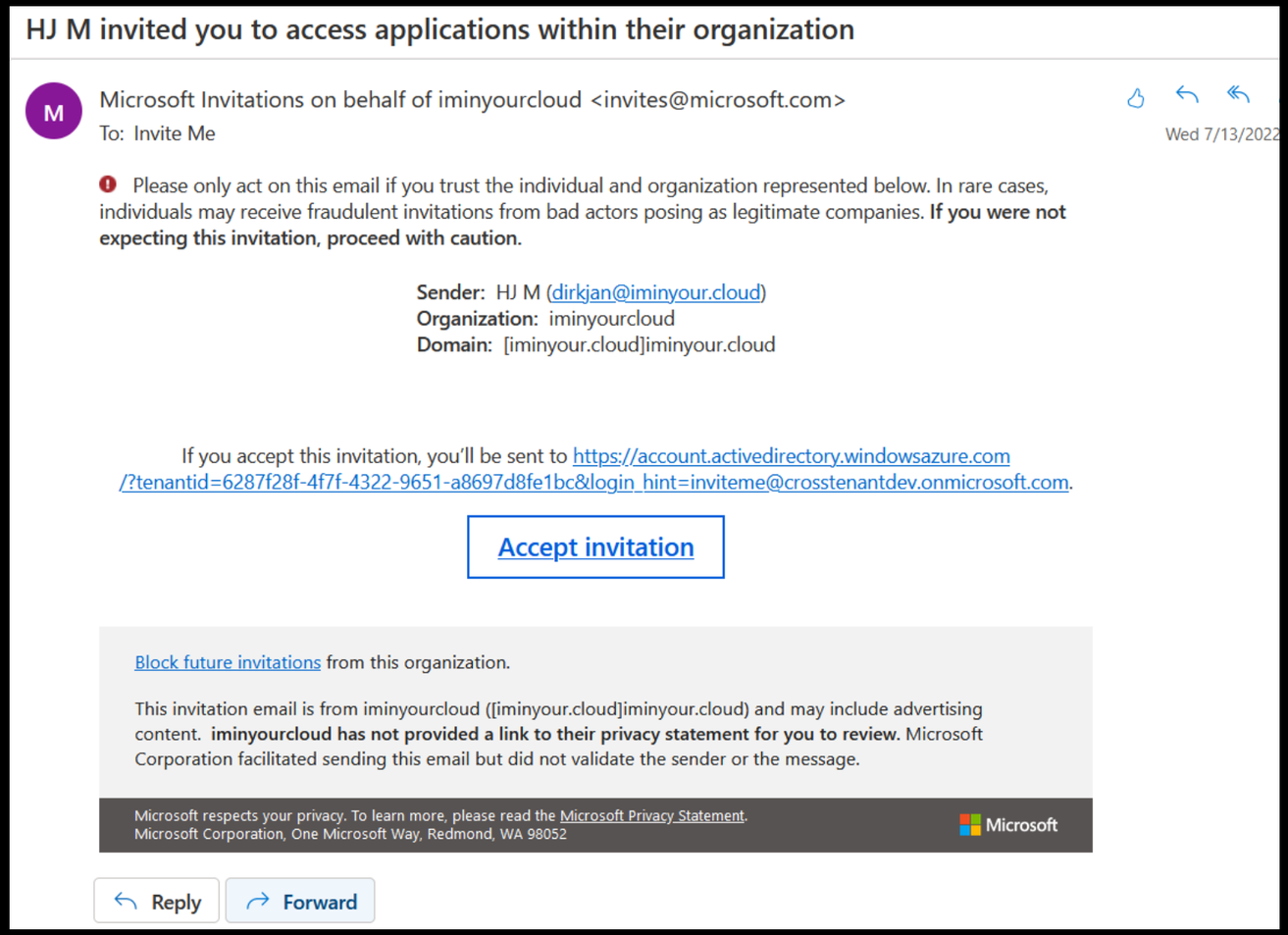
@mbrg0
mbgsec.com
t2’24

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



@mbrg0
mbgsec.com
t2'24

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



HJ M invited you to access applications within their organization

M

Microsoft Invitations on behalf of iminyourcloud <invites@microsoft.com>

To: Invite Me

Wed 7/13/2022

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

Sender: HJ M (dirkjan@iminyour.cloud)
Organization: iminyourcloud
Domain: [iminyour.cloud]iminyour.cloud

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

Accept invitation

Block future invitations from this organization.

This invitation email is from iminyourcloud ([iminyour.cloud]iminyour.cloud) and may include advertising content. **iminyourcloud has not provided a link to their privacy statement for you to review.** Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the Microsoft Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Reply Forward

Source: @_dirkjan at BHUSA 2022

@mbrg0
mbgsec.com
t2'24

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

Perhaps too easy?

black hat USA 2022

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


```
{
    "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects",
    "value": [
        {
            "odata.type": "Microsoft.DirectoryServices.User",
            "userPrincipalName": "guest_outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com",
            "inviteTicket": [
                {
                    "type": "Invite",
                    "ticket": "3557db4d-b514-4602-aa88-9c23f82ca61c"
                }
            ],
            "userType": "Guest",
            "invitedAsMail": "guest@outsidersecurity.nl"
        }
    ]
}
```


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

@mbrg0
mbgsec.com
t2'24

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

Perhaps too easy?

black hat USA 2022

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.

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

@mbrg0
mbgsec.com
t2’24

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

Perhaps too easy?

@mbrg0
mbgsec.com
t2’24

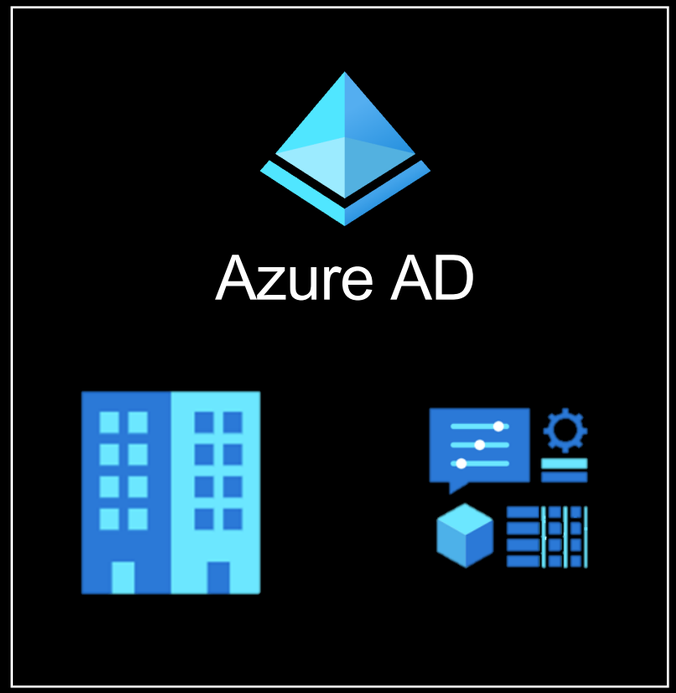
Safe guest access must be:

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

@mbrg0
mbgsec.com
t2’24

(b) Understanding how control works

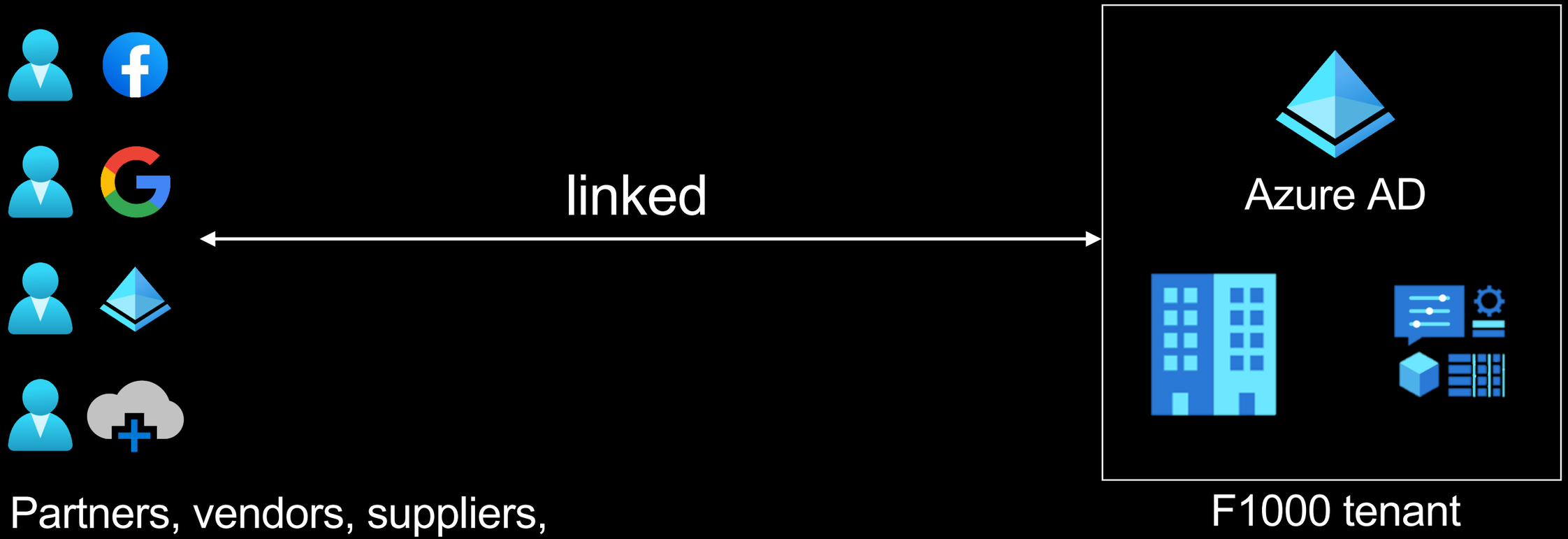
Partners, vendors, suppliers, other collaborators



F1000 tenant

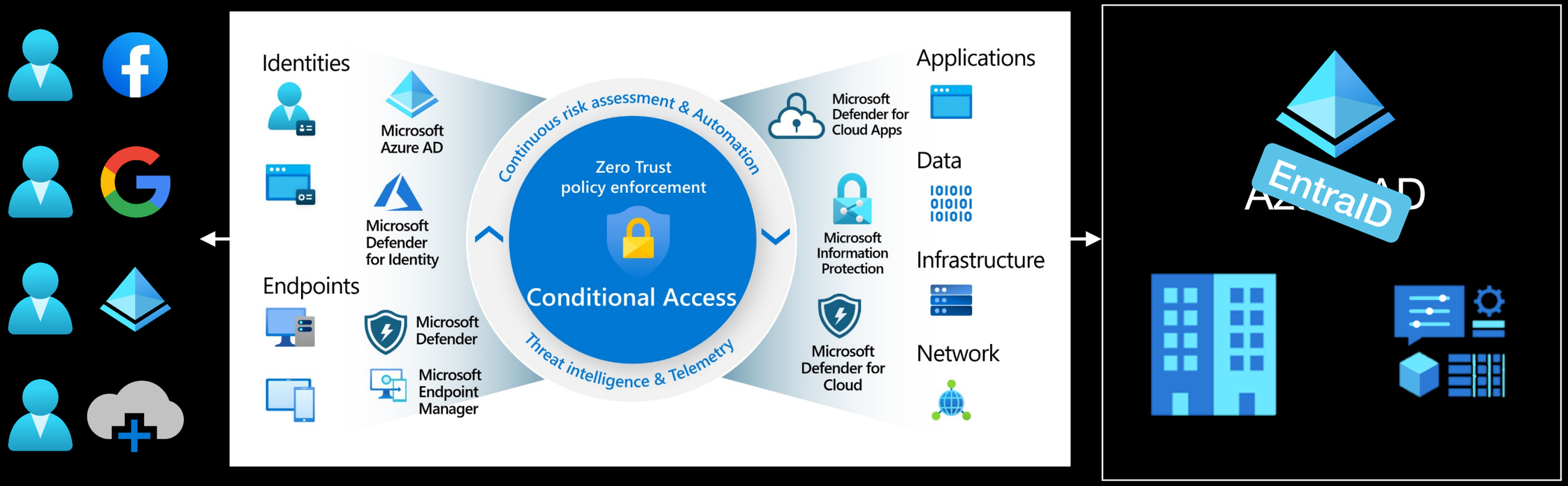
@mbrg0
mbgsec.com
t2’24

(b) Understanding how control works



@mbrg0
mbgsec.com
t2’24

(b) Control guests like employees



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

@mbrg0
mbgsec.com
t2’24

(b) Applying security controls to guests

Need guest access ➔ Require security controls

@mbrg0
mbgsec.com
t2’24

(b) Applying security controls to guests

Need guest access ➔ Require security controls

Security controls ➔ Require AAD account

@mbrg0
mbgsec.com
t2'24

(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. …?

@mbrg0
mbgsec.com
t2'24

(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

@mbrg0
mbgsec.com
t2’24

EntraID guest recap

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

zenity

@mbrg0
mbgsec.com
t2’24

Guest accounts in practice
The real implication of guests

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

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
Greg Winston	VP of IT			Owner

Members and guests (2)

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

Microsoft Teams

Search

Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help

Teams

Your teams

Vo Vendor onboarding

Vo Vendor onboarding
Vendor onboarding

Add member

Tags

Role

Owner

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.

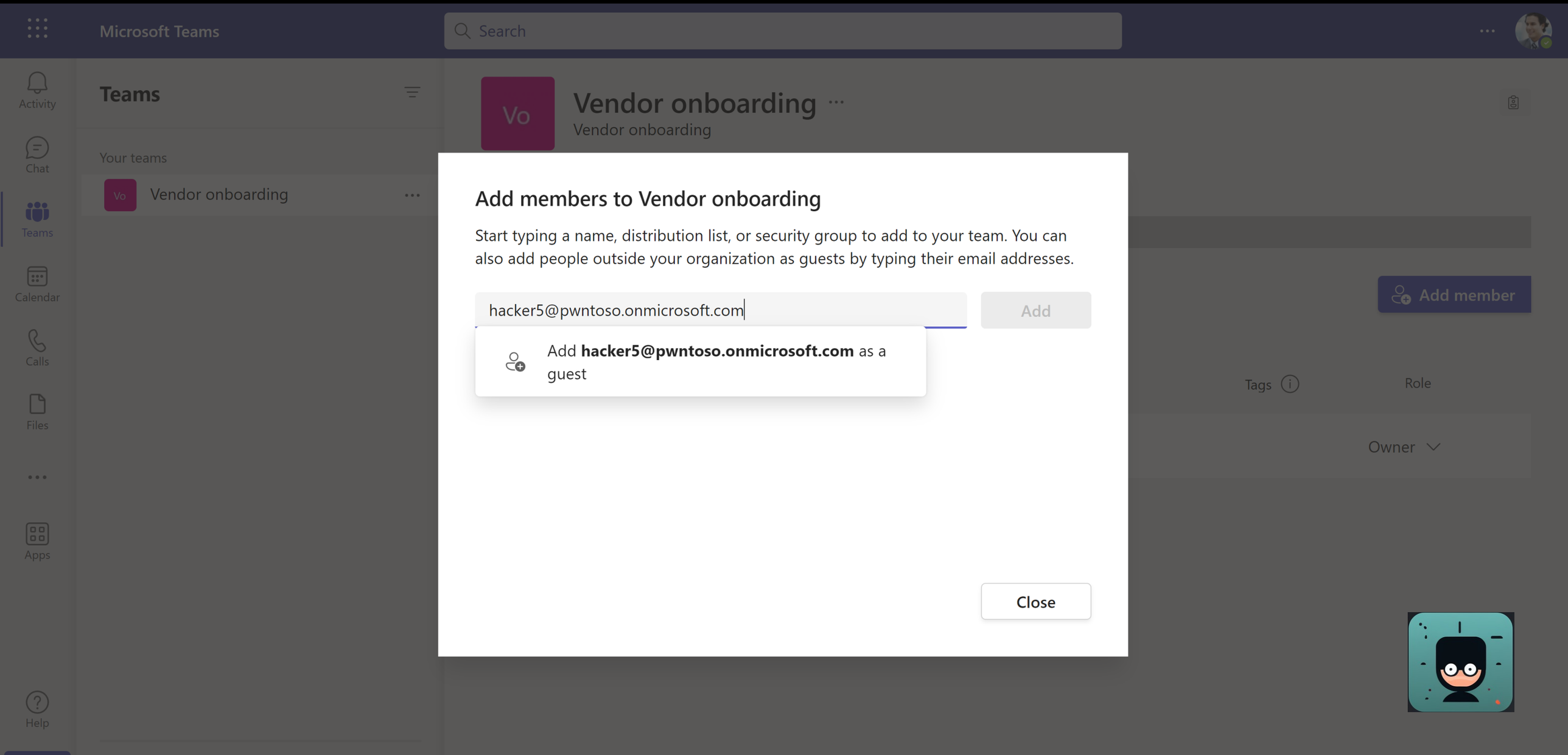
Start typing a name or group

Add

Close

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

Microsoft Teams

Search

Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help

Teams

Your teams

Vo Vendor onboarding

Vo Vendor onboarding
Vendor onboarding

Add member

Tags

Role

Owner

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

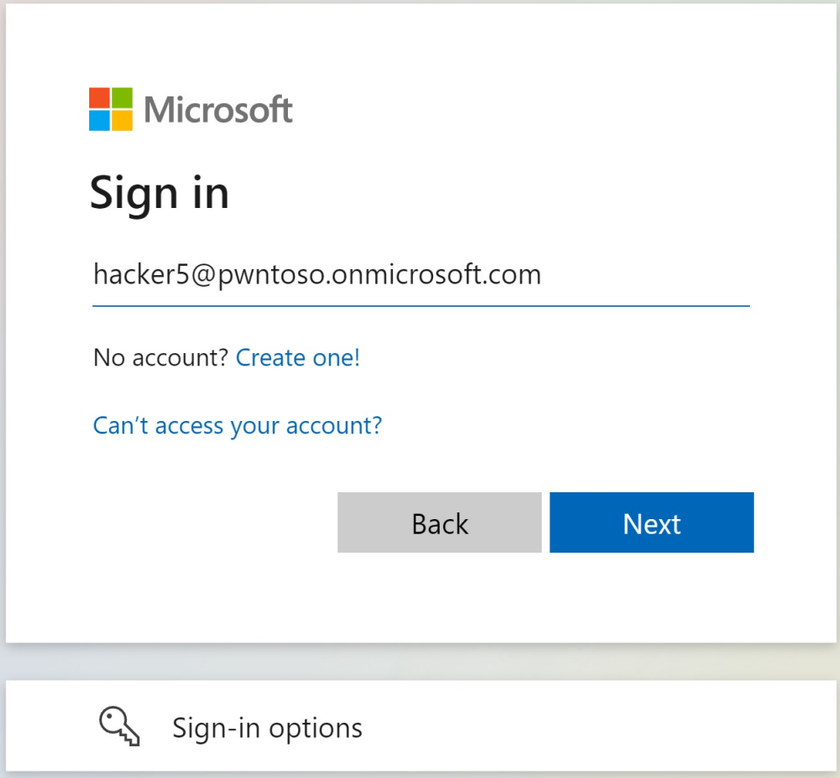
Add

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

Close

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Microsoft

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

My Apps

Search apps

H

Apps

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

Apps dashboard

Add apps | Create collection | Customize view

Apps

Apps

Settings

There are no apps to show.

Zenity Demo

Sign out

H

Hacker5

hacker5@pwntoso.onmicroso...

View account

Switch organization

Sign in with a different account

@mbrg0
mbgsec.com
t2’24

Everything works as expected ?

@mbrg0
mbgsec.com
t2’24

Everything works as expected ? ??

@mbrg0
mbgsec.com
t2’24

Guest exploitation state of the art

@mbrg0
mbgsec.com
t2’24

Guest exploitation state of the art

1. Phishing via Teams

@mbrg0
mbgsec.com
t2'24

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.

@mbrg0
mbgsec.com
t2'24

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/

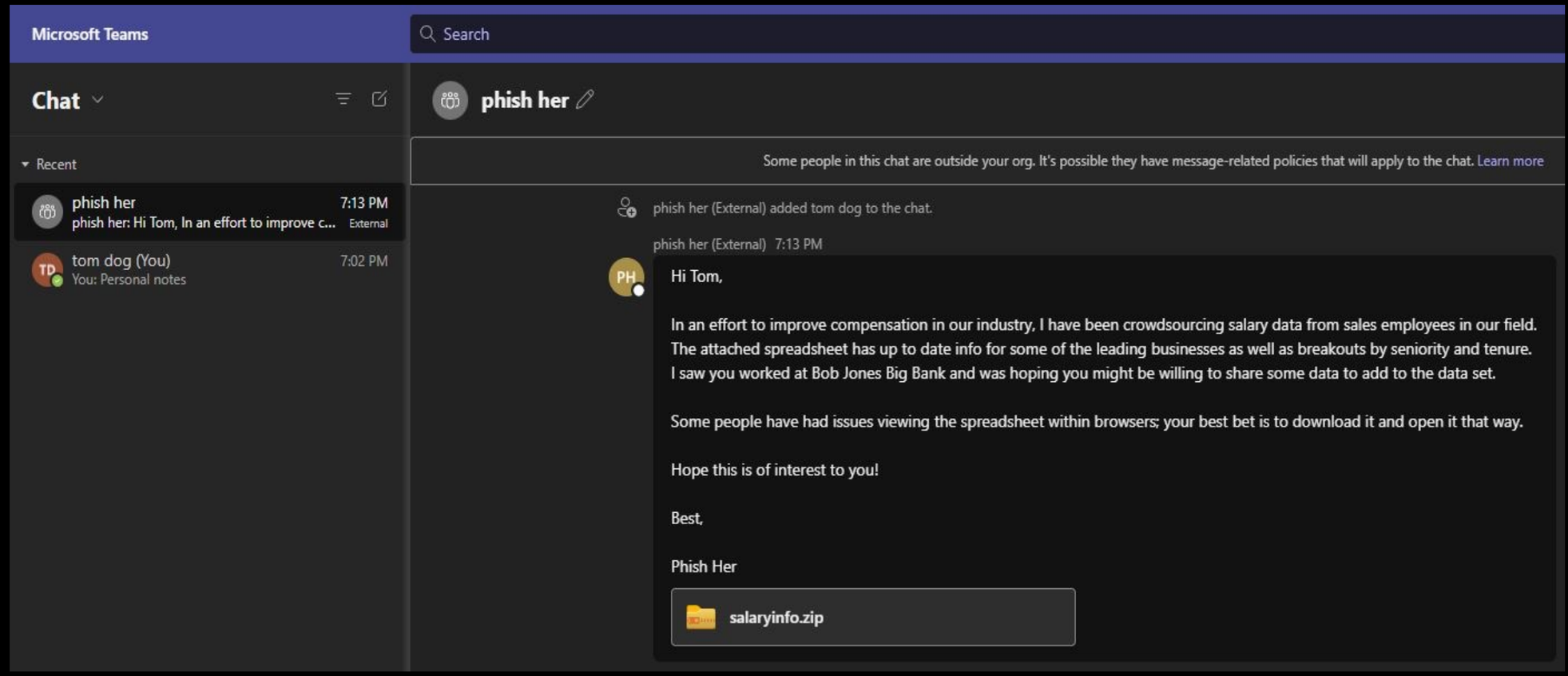
New Teams-based phishing activity

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.

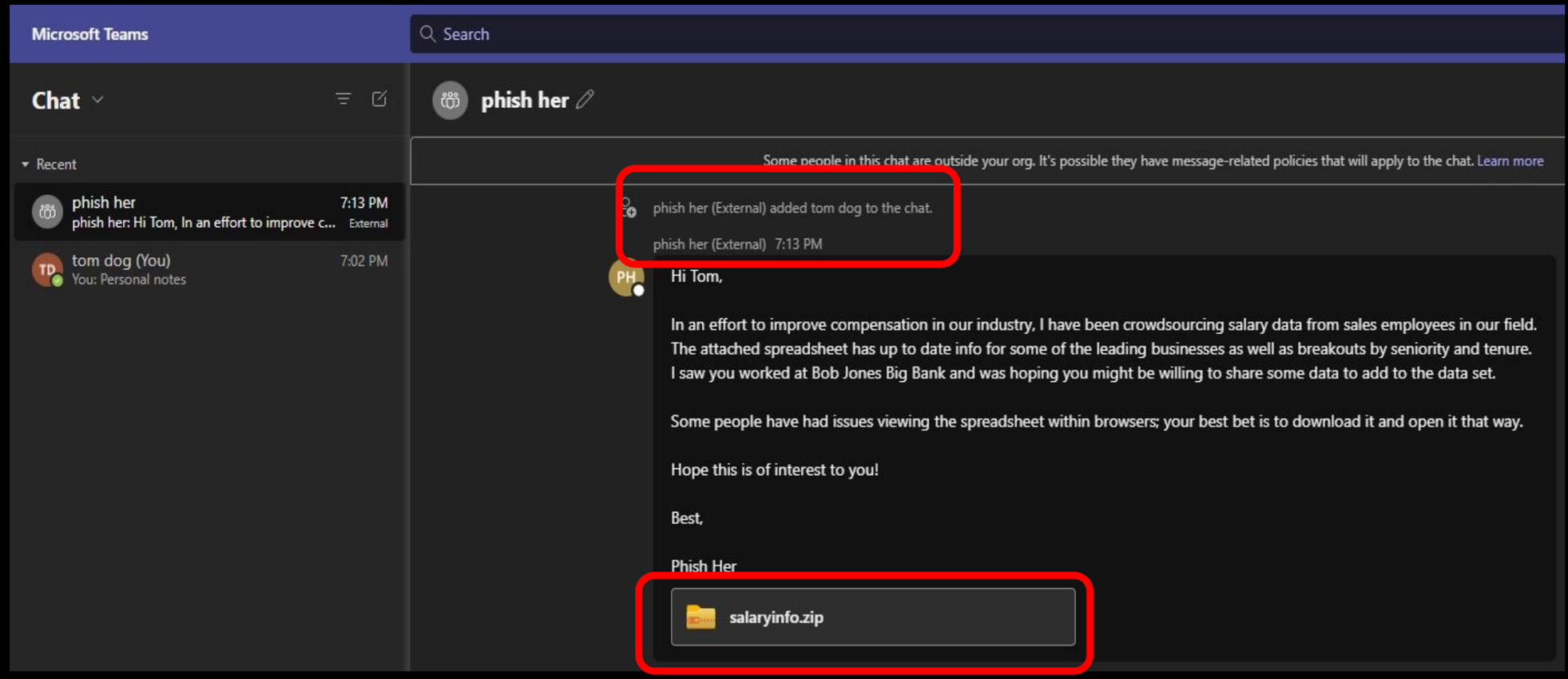
@mbrg0
mbgsec.com
t2’24

Guest exploitation 1. Phishing via Teams state of the art



@mbrg0
mbgsec.com
t2’24

Guest exploitation 1. Phishing via Teams state of the art



@mbrg0
mbgsec.com
t2’24

Guest exploitation state of the art

```
AADInternals 0.9.0
PS @mbrg0\BHUSA2023\All-You-Need-Is-Guest> $results.Users | Select-Object displayName,userPrincipalName

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

1. Phishing via Teams
2. Directory recon

@DrAzureAD at aadinternals.com/post/quest_for_guest/

@mbrg0
mbgsec.com
t2’24

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

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

All You Need Is Guest

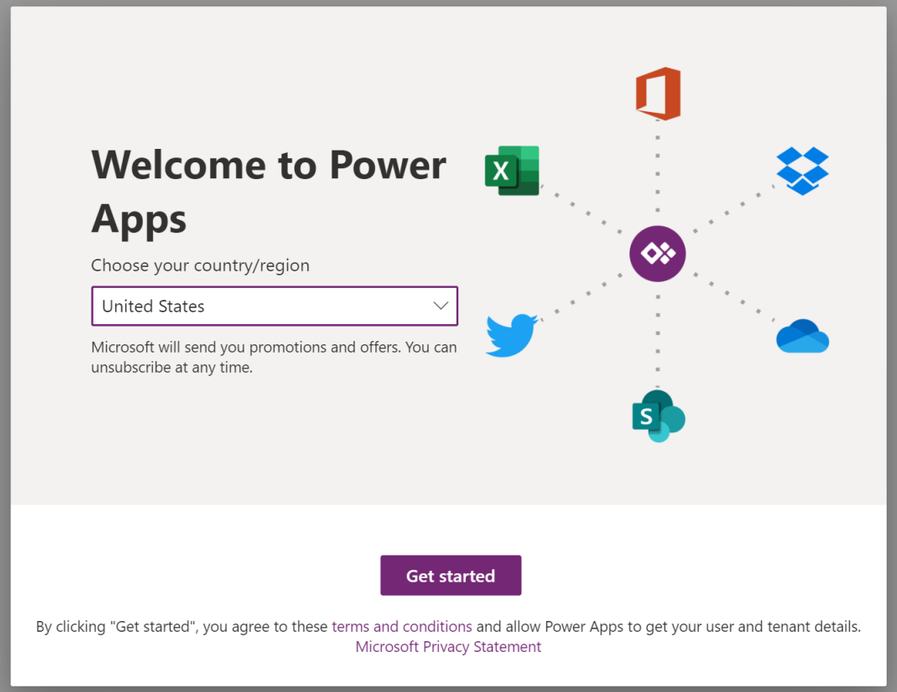
@mbrg0
mbgsec.com
t2’24

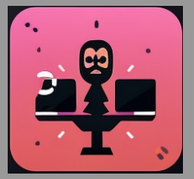
https://make.powerapps.com/environments/Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43/connections

Go have an early lunch

All You Need Is Guest

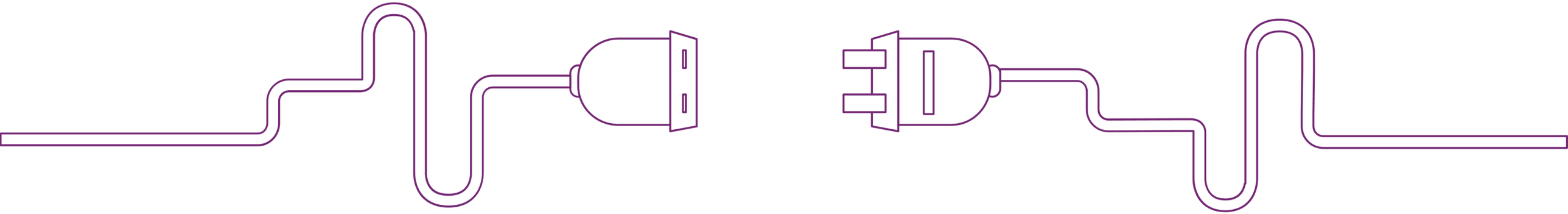
@mbrg0
mbgsec.com
t2’24





All You Need Is Guest

@mbrg0
mbgsec.com
t2’24



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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Pwntoso (default) | H

Try the new Power Apps

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

Welcome, Hacker5!

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

Ways to create an app

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

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

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

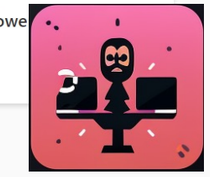
Your apps

Name	Modified ↓	Owner	Type
Package Management View	1 month ago	SYSTEM	Model-driven
Solution Health Hub	1 year ago	SYSTEM	Model-driven

See more apps →

Learning for every level See all

Get started with Power Apps	Beginner	51 min
Author a basic formula to change properties in a canvas app	Beginner	42 min
Work with external data in a Power Apps canvas app	Intermediate	1 hr 4 min
Manage and share apps in Powe	Beginner	



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Pwntoso (default) | H

Try the new Power Apps

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

Welcome, Hacker5!

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

Ways to create an app

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

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

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

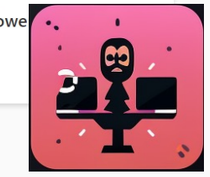
Your apps

Name	Modified ↓	Owner	Type
Package Management View	1 month ago	SYSTEM	Model-driven
Solution Health Hub	1 year ago	SYSTEM	Model-driven

See more apps →

Learning for every level See all

Get started with Power Apps	Beginner	51 min
Author a basic formula to change properties in a canvas app	Beginner	42 min
Work with external data in a Power Apps canvas app	Intermediate	1 hr 4 min
Manage and share apps in Powe	Beginner	



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Pwntoso (default) | H

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

Welcome, Hacker5!

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

Pwntoso Sign out

H

Hacker5

hacker5@pwntoso.onmicroso...

View account

Switch directory

Ways to create an app

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

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

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

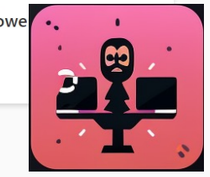
Your apps

Name	Modified ↓	Owner	Type
Package Management View	1 month ago	SYSTEM	Model-driven
Solution Health Hub	1 year ago	SYSTEM	Model-driven

See more apps →

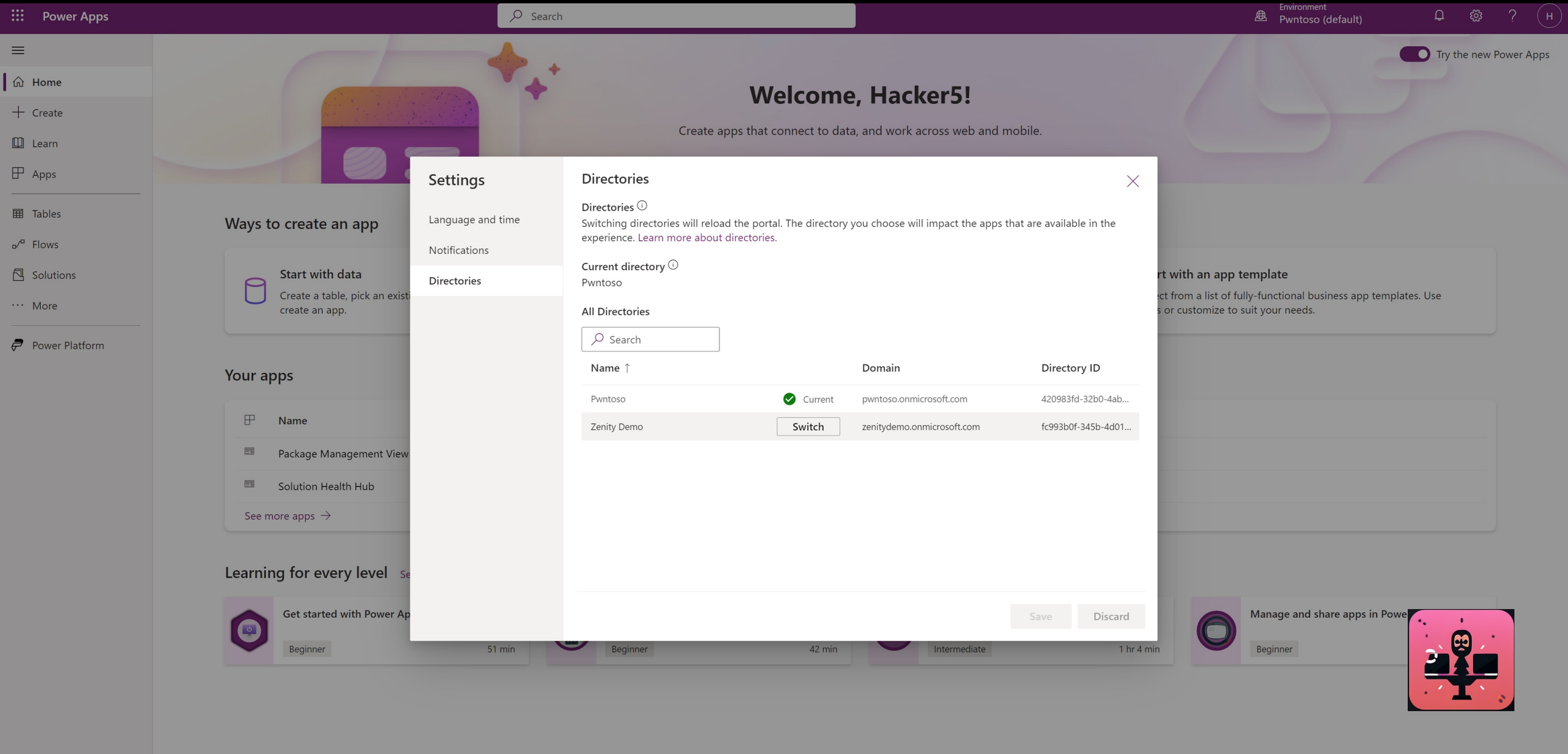
Learning for every level See all

- Get started with Power Apps — Beginner — 51 min
- Author a basic formula to change properties in a canvas app — Beginner — 42 min
- Work with external data in a Power Apps canvas app — Intermediate — 1 hr 4 min
- Manage and share apps in Powe — Beginner



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

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

New connection | Search

Connections in Zenity Demo (default)

Canvas

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

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

New connection | Edit | Share | Delete | Details

Connections in Zenity Demo (default)

Canvas

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

New connection | Edit | Share | Delete | Details

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

Connections in Zenity Demo (default)

Canvas

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

- Edit
- Share
- Delete
- Details

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps

Search

Environment
Zenity Demo (default)

Home
Create
Learn
Apps
Tables
Flows
Solutions
Connections
More
Power Platform

Share jamieredingcustomerdata.file.core.windows.net

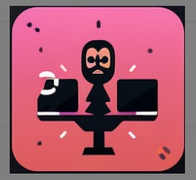
Enter names, email addresses, user groups, service principal names, or service principal app id

Shared with

Name	Email	Permission
Shared with org		Can use
Jamie Reding	jamier@zenitydemo.on...	Owner
jamiercontoso	jamiercontoso@outlook....	Can use + share

Cancel Save

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



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps

Search

Environment
Zenity Demo (default)

Home
Create
Learn
Apps
Tables
Flows
Solutions
Connections
More
Power Platform

Share jamieredingcustomerdata.file.core.windows.net

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

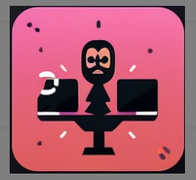
Shared with

Name	Email	Permission
Shared with org		Can use
Jamie Reding	jar	r
jamiercontoso	jar	se + share

Save

enterprisecustomers customerc
SQL Server

nected



All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

New connection | Edit | Share | Delete | Details

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

Connections in Zenity Demo (default)

Canvas

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

Edit
Share
Delete
Details

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

Edit | Share | Delete

Home
Create
Learn
Apps
Tables
Flows
Solutions
Connections
More
Power Platform

Connections > jamieredingcustomerdata.file.core.windows.net

Details | Apps using this connection | Flows using this connection

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Zenity Demo (default)

Edit | Share | Delete

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

Connections > jamieredingcustomerdata.file.core.windows.net

Details | Apps using this connection | Flows using this connection

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Zenity Demo (default)

Edit | Share | Delete

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

Connections > jamieredingcustomerdata.file.core.windows.net

Details | Apps using this connection | Flows using this connection

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

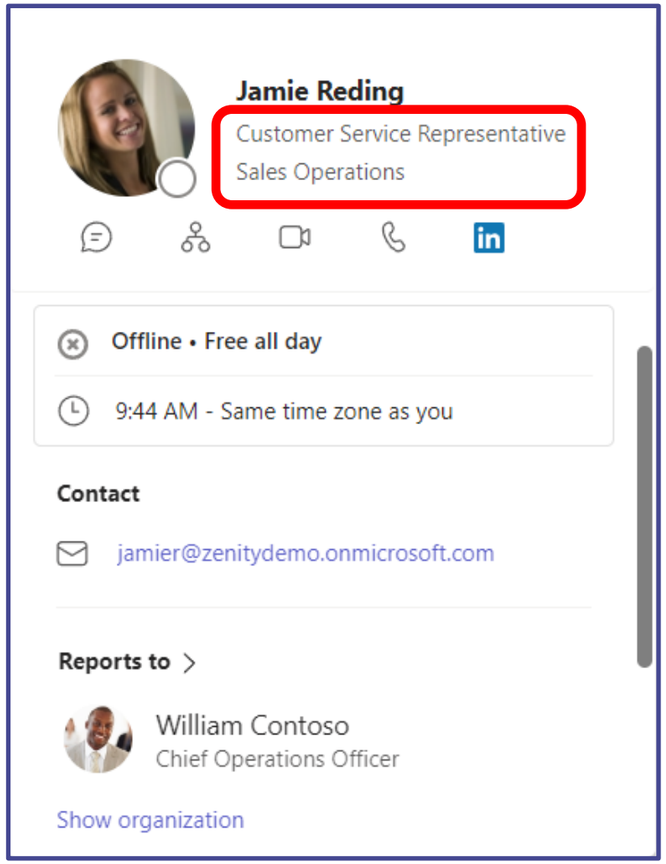
Jamie Reding

Created

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

Modified

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

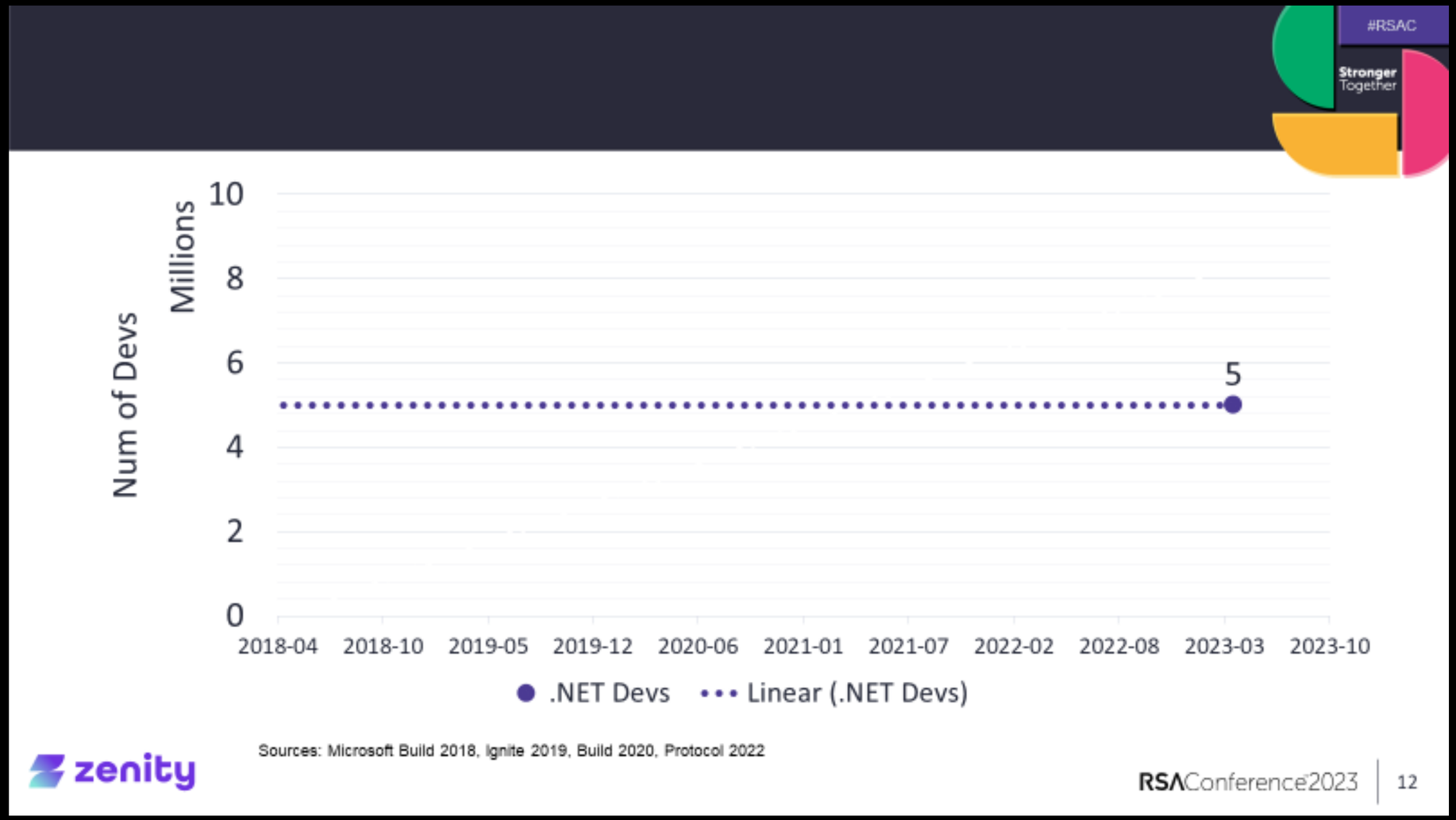


@mbrg0
mbgsec.com
t2’24

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

@mbrg0
mbgsec.com
t2'24

Is this actually being used?



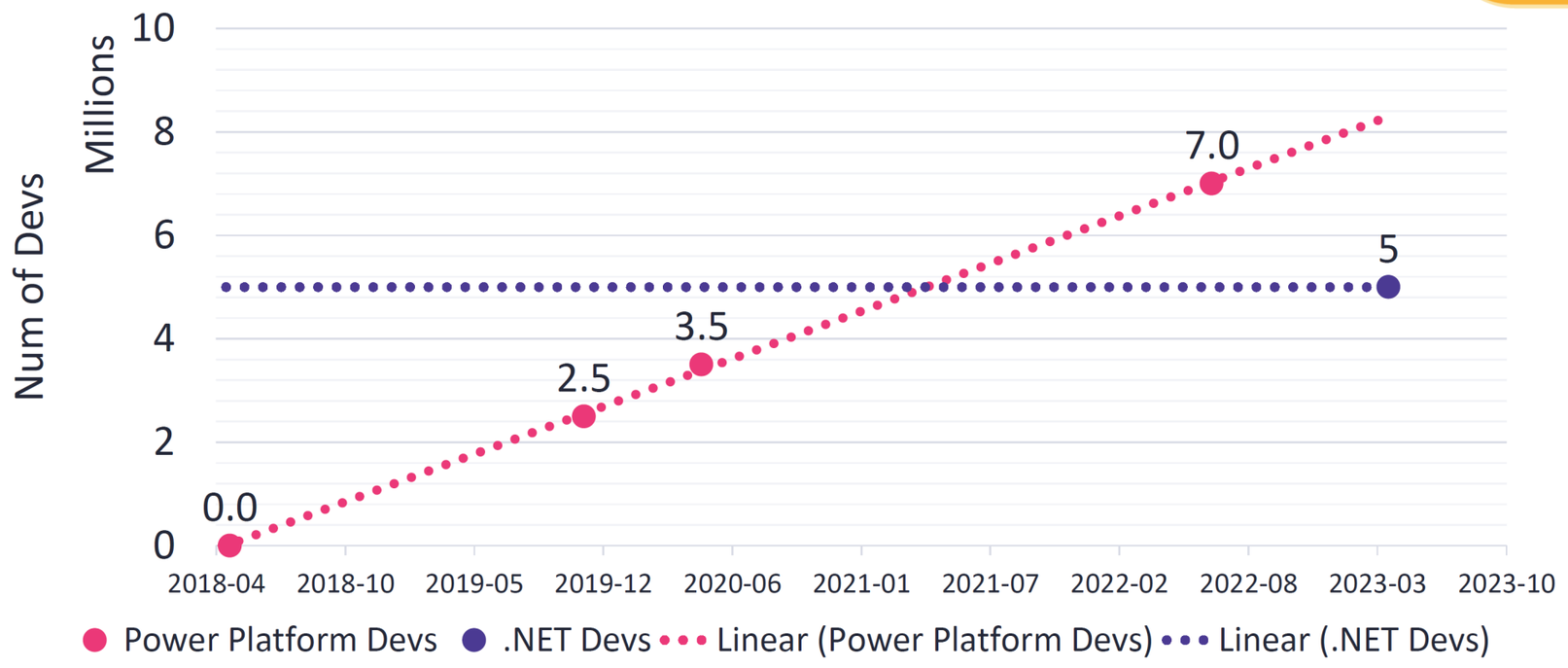
Credential Sharing as a Service: The Dark Side of No Code

Michael Bargury
RSAC 2023

@mbrg0
mbgsec.com
t2'24

~8M active Power devs today!

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



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

zenity

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

Michael Bargury
RSAC 2023

zenity

@mbrg0
mbgsec.com
t2’24

Exploit

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

Edit | Share | Delete

Home
Create
Learn
Apps
Tables
Flows
Solutions
Connections
More
Power Platform

Connections > jamieredingcustomerdata.file.core.windows.net

Details | Apps using this connection | Flows using this connection

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Zenity Demo (default)

Edit | Share | Delete | Search

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

Connections > jamieredingcustomerdata.file.core.windows.net

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

Name
Customer Insights Azure

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment Zenity Demo (default)

Edit | Share | Delete | Search

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

Connections > jamieredingcustomerdata.file.core.windows.net

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

Name
Customer Insights Azure

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Apps | Search | Environment: Zenity Demo (default)

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

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

Apps > **Customer Insights Azure**

Details | Versions | Connections | Flows

Owner
Jamie Reding

Description
Not provided

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

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

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

Mobile QR code

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

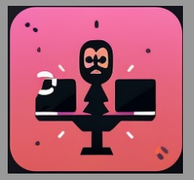
Power Apps |

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



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

Power Apps |

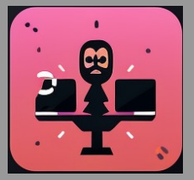
You need a Power Apps plan

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



All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

Power Apps |

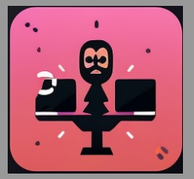
You need a Power Apps plan

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



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.

Microsoft

You've selected Microsoft Power Apps for Developer

1 Let's get you started

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

Email

hacker5@pwntoso.onmicrosoft.com

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

Learn More

Next

2 Create your account

3 Confirmation details

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

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

@mbrg0
mbgsec.com
t2'24

Microsoft

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2’24

Customer Insights

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.

More

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 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.

@mbrg0
mbgsec.com
t2’24

So we were able to bypass the license requirement

But blocked by… DLP?

Filter by title

Data loss prevention policies
Overview
Create a DLP policy
Manage DLP policies
Data loss prevention SDK
Basic connector classification
Connector action control
Connector endpoint filtering (preview)
DLP for custom connectors
DLP for Power Automate
DLP for desktop flows
Disable new connectors
View policies and policy scope
Effect of multiple policies
Impact on apps and flows
Exempt apps and flows

Data loss prevention policies

Article • 07/12/2023 • 7 contributors

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

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

Power Platform admin center

150% Reset

DLP Policies > New Policy

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

Name your policy

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

Find SSN

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

Power Platform admin center

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	N

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

Power Platform admin center

DLP Policies > New Policy

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

Move to Business | Block | Configure connector | Set default group

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

Assign connectors

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

Search connectors

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

Name	Blockable	Endpoint config
SharePoint	No	No
OneDrive for Business	No	N

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

Power Platform admin center

DLP Policies > New Policy

Home
Environments
Anal
Billin
Setti
Reso
Help
Data
Data
Polic

Policy name

Move to Business | Block | Configure connector | Set default group

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

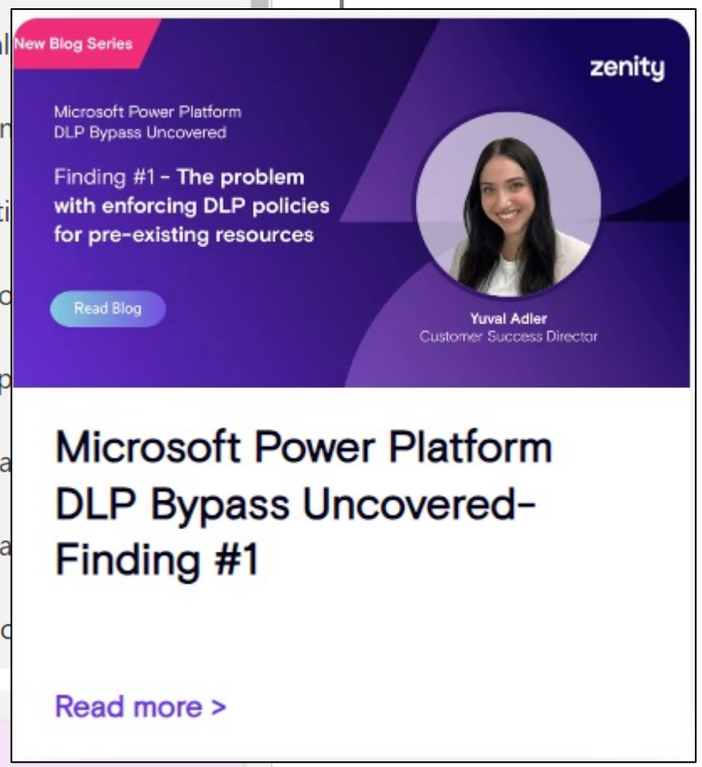
Assign connectors

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

Search connectors

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

Name	Blockable	Endpoint config
SharePoint	No	No
OneDrive for Business	No	N



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

Register now

Back | Next | Cancel

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24