Sure, Let Business Users Build Their Own. What Could Go Wrong?

Michael Bargury @mbrg0

Zenity

SECTOR

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

Agenda

1. Business users are building their own
2. What could go wrong?
3. Why does it go wrong?
4. How can we fix it?

SECTOR
BRIEFINGS

Enterprise citizen devs – EVERYONE is a dev

@mbrg0

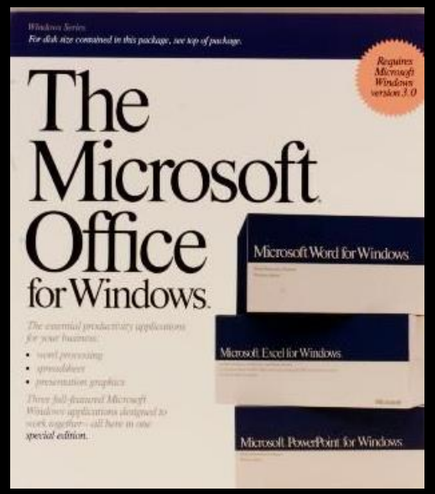
Business Needs

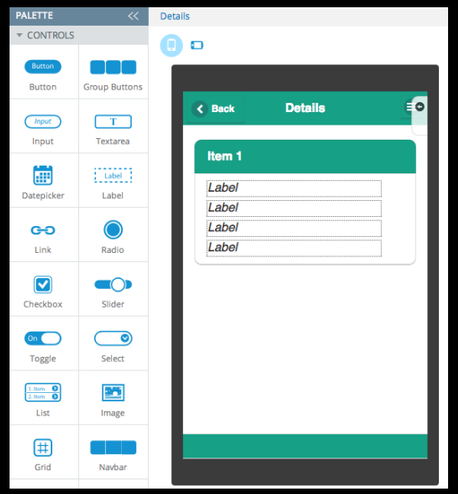
>>>

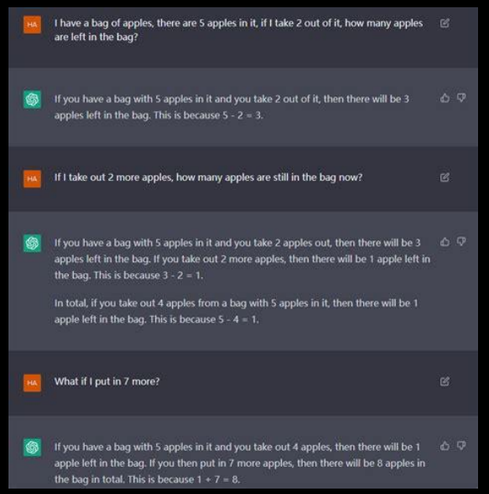
IT Capacity

SECTOR

If this sounds familiar, its because it is

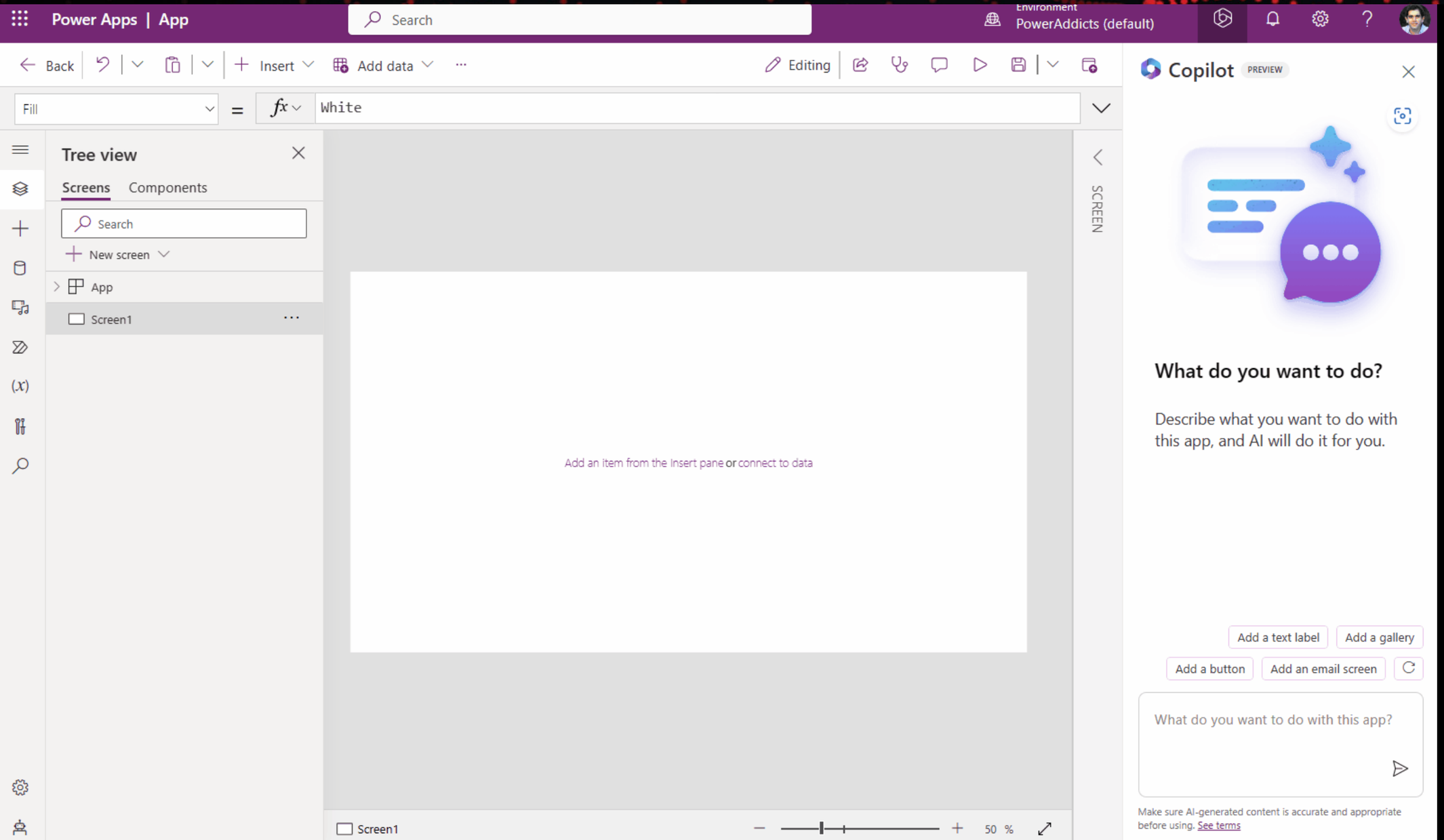






Tech evolution

SECTOR

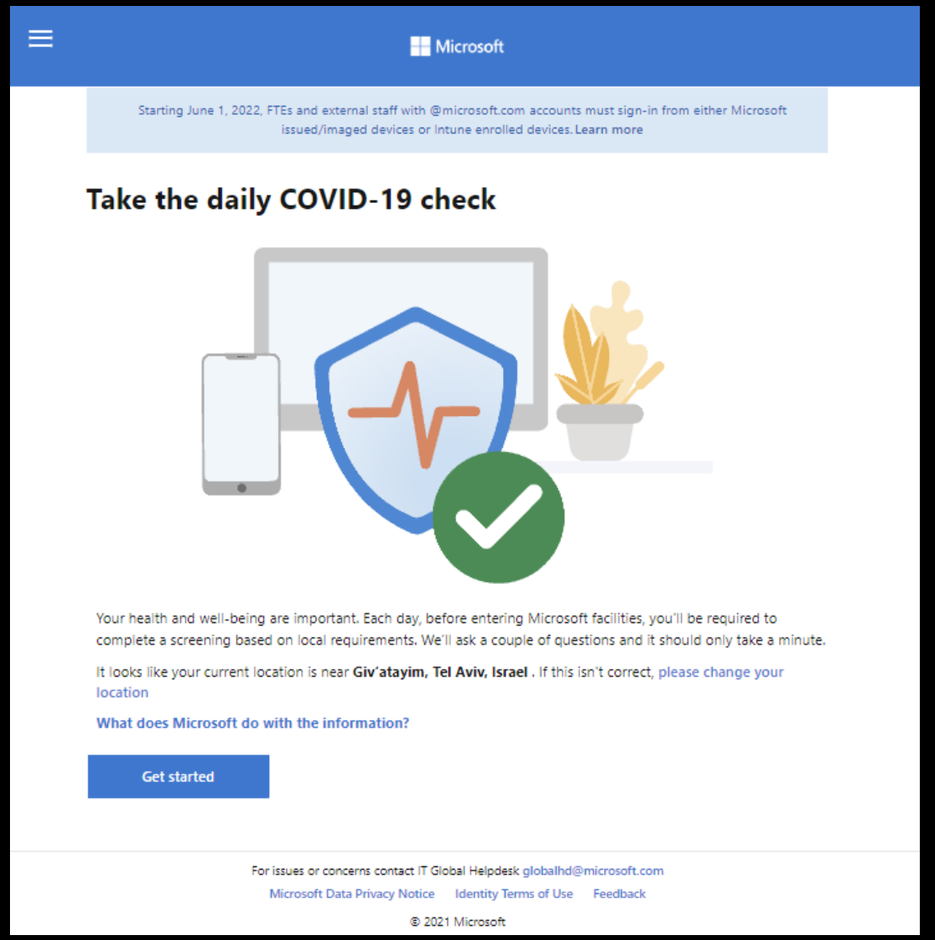


Source: @RezaDorrani

@mbrg0

#SECTORCA @SecTorCA

COVID health check app by Microsoft



https://aka.ms/healthcheck

Product launch management

* This is an example of a business-critical app built by a citizen developer. We did not search for or identify any security vulnerabilities in this app.

https://www.microsoft.com/insidetrack/blog/how-citizen-developers-modernized-microsoft-product-launches/

Financial risk management

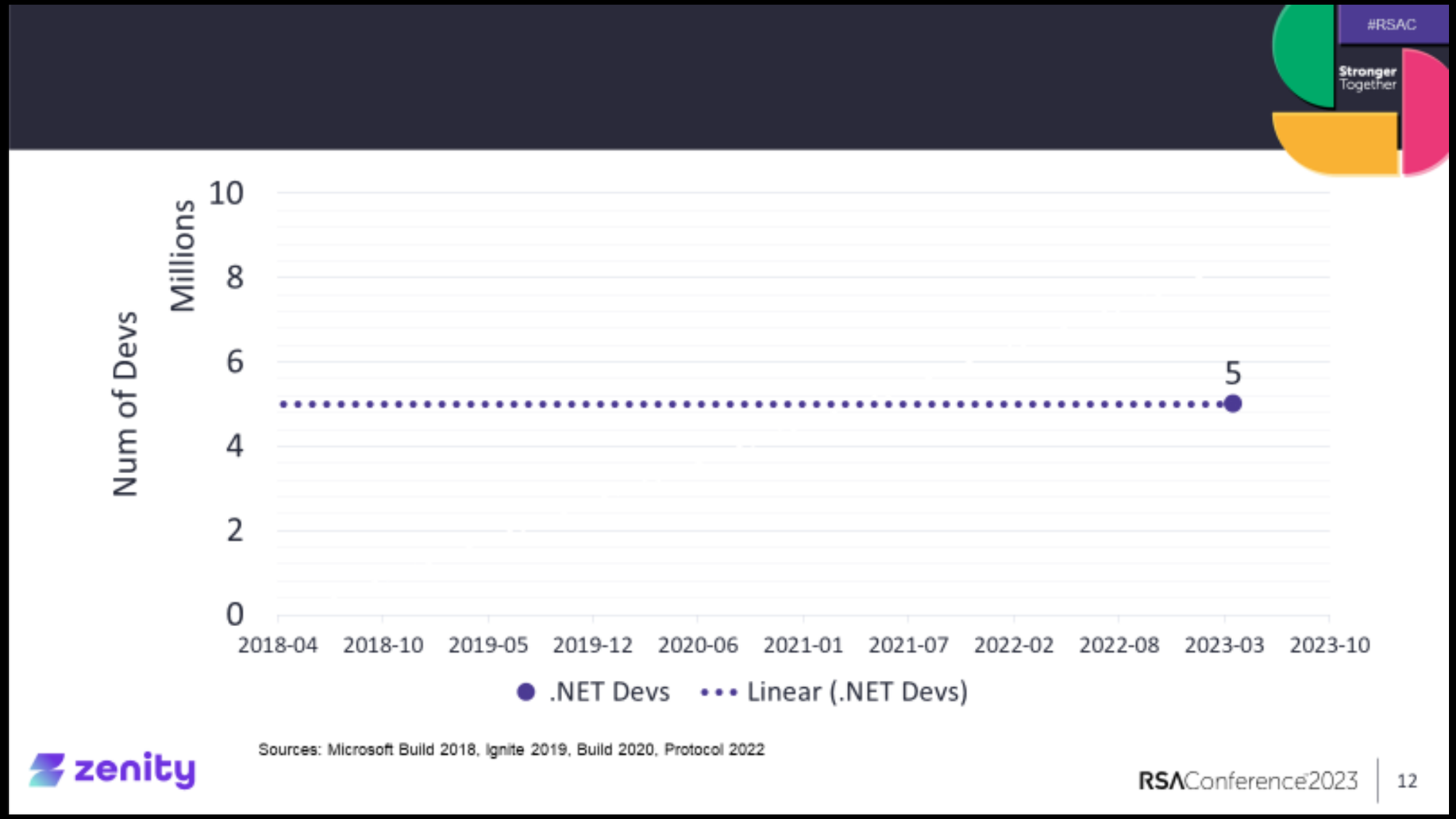
- Facilitates the process of credit assignment
- Determines whether or not a person is assigned credit
- Streamlines risk assessment and decision-making

SECTOR

Your business is already there, it's time for security to keep up.

SECTOR

Is this actually being used?



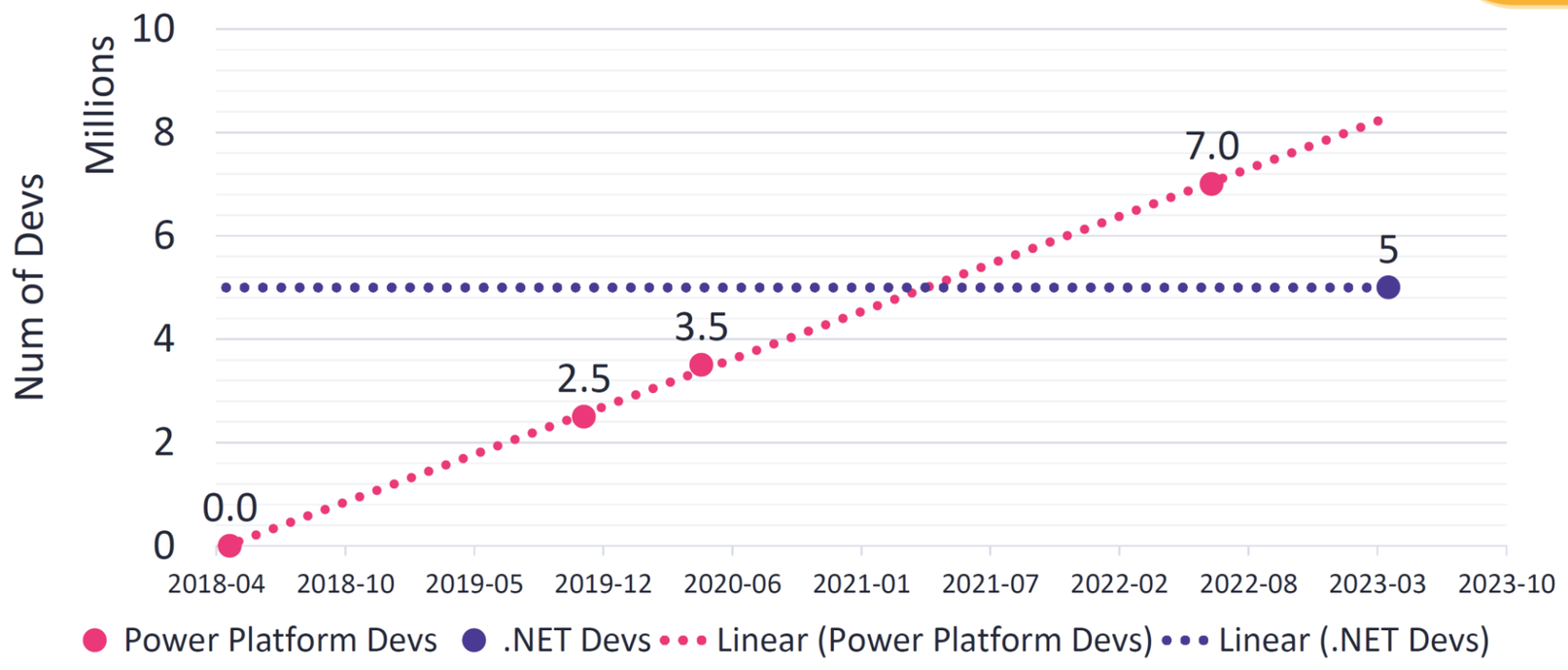
Credential Sharing as a Service: The Dark Side of No Code

Michael Bargury
RSAC 2023

SECTOR

~8M active Power devs today!

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



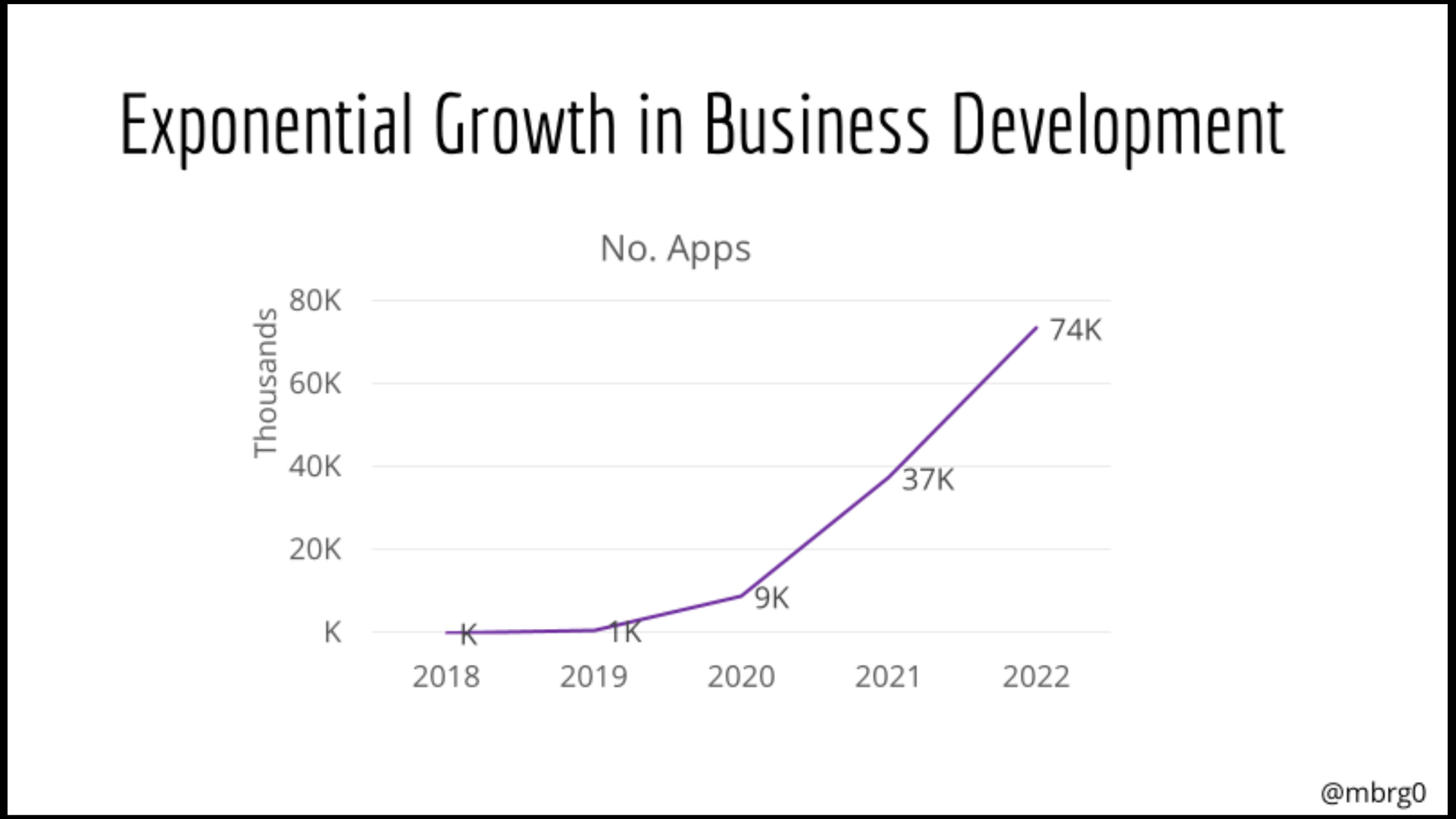
Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

zenity

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

Michael Bargury
RSAC 2023

A single F500 organization



Michael Bargury
BSidesSF 2023

SECTOR

Recap: You can’t opt out of citizen development

- The next big productivity boost (Excel-level impact)
- Powers critical business workflows, predicted to power 70% of enterprise apps by 2025
- Available on every major enterprise, yours too
- Millions of new (business) developers and growing fast

SECTOR
BRIEFINGS

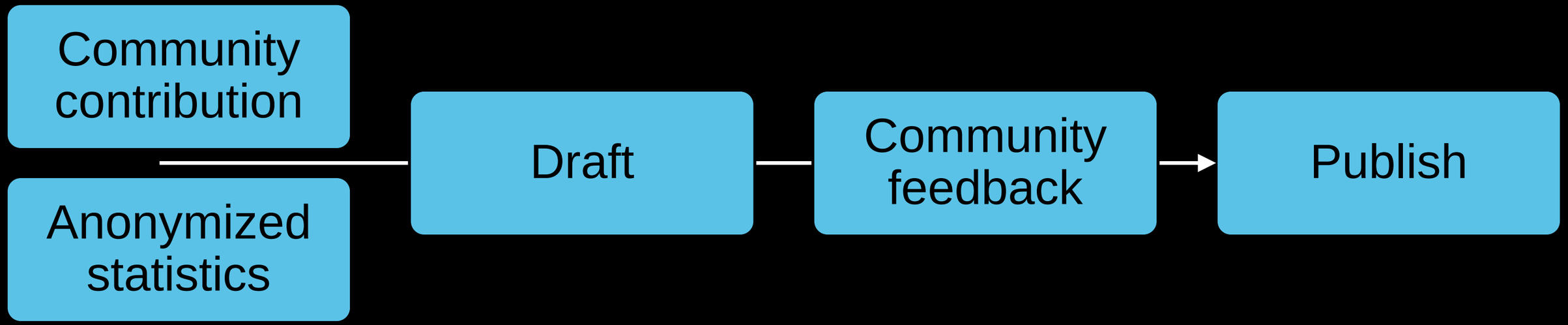
What could go wrong?

SECTOR

OWASP LCNC Top 10

- LCNC-SEC-01: Account Impersonation
- LCNC-SEC-02: Authorization Misuse
- LCNC-SEC-03: Data Leakage and Unexpected Consequences
- LCNC-SEC-04: Authentication and Secure Communication Failures
- LCNC-SEC-05: Security Misconfiguration
- LCNC-SEC-06: Injection Handling Failures
- LCNC-SEC-07: Vulnerable and Untrusted Components
- LCNC-SEC-08: Data and Secret Handling Failures
- LCNC-SEC-09: Asset Management Failures
- LCNC-SEC-10: Security Logging and Monitoring Failures

Methodology loop



>1M apps and automations
>8M credentials

Ty to all collaborations and contributors!

SECTOR
BRIEFINGS

Real-world stories

SECTOR
BRIEFINGS

Story #1 – employee onboarding

SECTOR

@mbrg0

Power Apps

Search

Environment
Zenity Stage (default)

AA

Home

Create

Learn

Apps

Tables

Connections

Solutions

Flows

More

Power Platform

Ask a virtual agent

Start from

Blank app

Create an app from scratch and then add your data

Watch video

Dataverse

Start from a Dataverse table to create a three-screen app

Watch video

SharePoint

Start from a SharePoint list to create a three-screen app

Watch video

Excel

Start from an Excel file to create a three-screen app

SQL

Start from a SQL data source to create a three-screen-app

Image

Upload an image of an app and we'll convert it into an app

SECTOR

@mbrg0

Power Apps

Search

Environment
Zenity Stage (default)

AA

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

Start from

Blank app

Create an app from scratch and then add your data

Watch video

Dataverse

Start from a Dataverse table to create a three-screen app

Watch video

SharePoint

Start from a SharePoint list to create a three-screen app

Watch video

Excel

Start from an Excel file to create a three-screen app

SQL

Start from a SQL data source to create a three-screen-app

Image

Upload an image of an app and we'll convert it into an app

SECTOR

@mbrg0

Power Apps | Employee Onboarding

Search

AA

Back | Insert | Add data | ... | Editing

Fill = fx White

Tree view

Screens | Components

Search

New screen

- App
- Screen1
  - Label2_4
  - TextInput1_5
  - Textinput_1
  - LblAppName3_1
  - IconAccept1_1
  - IconCancel1_1
  - Label2_3

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

Screen1 — 30 %

SCREEN

Screen1

Properties | Advanced | Ideas

Fill

Background image: None

Image position: Fit

SECTOR

@mbrg0

Power Apps | Employee Onboarding

Search

Back | Insert | Add data | ... | Editing

Fill = fx White

Data

Search

Add data

Sensitive Inputs
Microsoft Dataverse - Current environm...

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SCREEN

Screen1

Properties | Advanced | Ideas

Fill

Background image: None

Image position: Fit

Screen1

30 %

SECTOR

@mbrg0

Power Apps | Employee Onboarding

Search

Back | Insert | Add data | ... | Editing

Fill = fx White

Data

Search

Add data

Sensitive Inputs
Microsoft Dataverse - Current environm...

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SCREEN

Screen1

Properties | Advanced | Ideas

Fill

Background image: None

Image position: Fit

Screen1

30 %

SECTOR

@mbrg0

Power Apps | Employee Onboarding

Search

Back | Insert | Add data | ... | Editing

Fill

Data

Search

Add data

Sensitive Inputs
Microsoft Datavers

Ideas

None

Fit

Microsoft Power Platform

The low code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone apps.

Power BI
Business analytics

Power Apps
App development

Power Automate
Process automation

Power Virtual Agents
Intelligent virtual agents

Power Pages
External-facing websites

Data connectors

AI Builder

Dataverse

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

ZH

Update Employee Info in HR system

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

Ask a chatbot

When a row is added, modified or deleted

Send email (V2)

*To: hrorg@cloudcore.com

Subject: New Employee Update info

Body: Font | 12 | B | I | U

SSN | Contact | Email | Address | Employee Name

Attachments Name - 1
Title of the attachment.

Attachments Content - 1
Body of the attachment.

Attachments Content-Type - 1
Type of content in the attachment.

Add new item

Show advanced options

+ New step

Save

Employee onboarding – findings

SECTOR

@mbrg0

Power Apps | Employee Onboarding

Search

KS

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SECTOR

@mbrg0

Power Apps

Search

Environment
Zenity Stage (default)

KS

New table | Import | Export | Search

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

Tables

Recommended | Custom | All

Table	Name	Type	Managed	Customizable	Tags
Account	account	Standard	Yes	Yes	Core
Address	customeraddress	Standard	Yes	Yes	Standard
AppFlow Relation	cr6e4_appflowrel...	Standard	No	Yes	Custom
Appointment	appointment	Activity	Yes	Yes	Productivit
asjs	cr6e4_asjs	Standard	No	Yes	
Attachment	activitymimeatta...	Standard	Yes	Yes	

SECTOR

@mbrg0

Power Apps | Search | Environment Zenity Stage (default) | KS

New table | Open | Edit | Import | Export | Properties | ... | Search

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

Position	position	Standard	Yes	Yes	System
Query	cr6e4_querytest	Standard	No	Yes	Custom
Recurring Appointment	recurringappoint...	Activity	Yes	Yes	Standard
res	cr6e4_res	Standard	No	Yes	Custom
Sensitive Input	cr6e4_sensitivein...	Standard	No	Yes	Custom
table_for_app_with_im...	cr6e4_table_for_...	Standard	No	Yes	Custom
Task	task	Activity	Yes	Yes	Productivit
Team	team	Standard	Yes	Yes	System
Team template	teamtemplate	Standard	Yes	Yes	
ttv	cr6e4_ttv	Standard	No	Yes	
User	systemuser	Standard	Yes	Yes	Standard

SECTOR

@mbrg0

Power Apps | Search | Environment Zenity Stage (default) | KS

Back | New row | New column | Refresh | Create an app | Edit table properties | Update forms and views

Sensitive Inputs

Data saved

Employee Name *	SSN	Address	Contact	+19 more
Jamie Reading	209-97-1111	jamier@zenitydemo.OnMicrosoft....		
Brooklyn Gonzalez	209-97-9876	brooklynd@zenitydemo.OnMicros...		
Henry Mitchell	209-97-0987	henryd@zenitydemo.OnMicrosoft...		
Savannah Perez	209-97-7890	savannahp@zenitydemo.OnMicro...		
Ella Gonzalez	209-97-9876	ellaq@zenitydemo.OnMicrosoft.c...		
Riley Mitchell	209-97-0987	rileyp@zenitydemo.OnMicrosoft.c...		
Nathan Perez	209-97-7890	nathanh@zenitydemo.OnMicroso...		
Daniel Martin	209-97-6789	danielm@zenitydemo.OnMicrosof...		
Layla Gonzalez	209-97-9876	laylam@zenitydemo.OnMicrosoft...		

Employee onboarding – findings

- Data accessible to all (Authorization Misuse)

Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)

SECTOR

@mbrg0

Power Apps | Employee Onboarding

Environment
Zenity Stage (default)

ZH

Employee onboarding form

Full legal name	Daniel Wood
Address	New York 3rd street
Date of birth	11 Jan 1990
Personal email	Danielw124@gmail.co
Phone number	202-555-0117
Social Security Number	78-05-1120

Save

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

ZH

Update Employee Info in HR system

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

Ask a chatbot

When a row is added, modified or deleted

Send email (V2)

*To: hrorg@cloudcore.com

Subject: New Employee Update info

Body: Font | 12 | B | I | U

SSN | Contact | Email | Address | Employee Name

Attachments Name - 1
Title of the attachment.

Attachments Content - 1
Body of the attachment.

Attachments Content-Type - 1
Type of content in the attachment.

Add new item

Show advanced options

+ New step

Save

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

Update Employee Info in HR system • Ran at 8/7/2023 7:40:51 PM

Your flow ran successfully.

Home
Approvals
My flows
Create
Templates
Connectors
Data
Monitor
AI Builder
Process mining
Solutions
Learn

Ask a chatbot

When a row is added, modified or deleted

INPUTS

Change type

4

Table name

cr6e4_sensitiveinput

Scope

4

OUTPUTS

body


```
"cr6e4_name": "Daniel Wood",
"_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
"_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname"
"_modifiedby_type": "systemusers",
"cr6e4_ssn": "78051120",
"createdon": "2023-08-07T16:40:48Z",
"ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
```


Connection: zivh@zenitystage.com

When a row is added, modified or deleted

When a row is added, modified or deleted


```
{
  "headers": {
    "Expect": "100-continue",
    "Host": "prod-52.westeurope.logic.azure.com",
    "x-ms-correlation-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-client-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-user-id": "7cb2f429-a54a-46c3-8e4f-df3a3032f249",
    "Content-Length": "1258",
    "Content-Type": "application/json"
  },
  "body": {
    "cr6e4_email": "daniel1ds@gmail.com",
    "_owningbusinessunit_value": "edfdf52a-e501-ec11-94ee-0022488[illegible]00bc",
    "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "bu
    "_owningbusinessunit_type": "businessunits",
    "statecode": 0,
    "_statecode_label": "Active",
    "cr6e4_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e[illegible]b",
    "statuscode": 1,
    "_statuscode_label": "Active",
    "cr6e4_contact": "202-555-0117",
    "_createdby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_createdby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser"
    "_createdby_type": "systemusers",
    "cr6e4_dateofbirth": "10.10.1990",
    "_ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_ownerid_type": "systemusers",
    "modifiedon": "2023-08-07T16:40:48Z",
    "cr6e4_address": "116 E 60TH ST NEW YORK USA",
    "cr6e4_name": "Daniel Wood",
    "_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser
    "_modifiedby_type": "systemusers",
    "cr6e4_ssn": "78051120",
    "createdon": "2023-08-07T16:40:48Z",
    "ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8[illegible]
    "SdkMessage": "Create",
    "RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d[illegible]
```


Power Automate | Search | Environments Zenity Stage (default) | ZH

Update Employee Info in HR system | Edit

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn
- Ask a chatbot

Owners

Adding an owner gives them full control of this flow, so make sure you only share with people you trust. They'll be able to add or remove other users as owners, access the run history, and can update, edit or delete this flow.
Learn more

Add a user or group as owner

Enter names, emails, or user groups

Ziv Hagbi

HR-All

Embedded connections

Everyone listed as an owner will have access to all these connections and will only be able to use them in this flow.
Learn more

Connections in use

Connections listed are actively being used in this flow. Manage connections

zivh@zenitystage.com
Microsoft Dataverse

maortzury@gmail.com
Gmail

SECTOR

Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)
- Sensitive data written to logs (Data Leakage)

Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)
- Sensitive data written to logs (Data Leakage)

SECTOR
BRIEFINGS

Story #2 – productivity sync

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Sync Outlook to Gmail

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining

When a new email arrives (V3)

Send email (V2)

* To

KS Kris Smith

Subject

Subject

Body

Font | 12 | B | I | U

Body

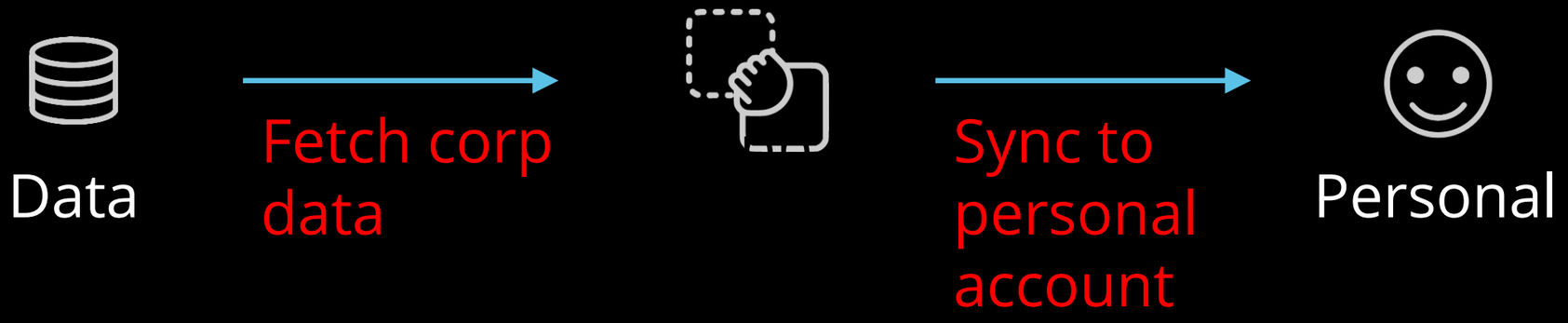
Attachments

Attachments

Productivity sync – findings

Productivity sync – findings

- Business data to personal account (Data Leakage)



SECTOR

@mbrg0

Power Apps | Set up your email sync

Environment
Zenity Stage (default)

KS

Back | Insert | Open Sans | 15 | Semibold | ... | Editing

OnSelect = SyncOutlookhistorytoGmail.Run(NumberInput,EmailInput)

Power Automate

Search

Add flow

In your app

Sync Outlook history to Gmail
SyncOutlookhistorytoGmail

Sync Outlook history to Gmail

Email address | Text input

How many emails to sync

Sync your email

BUTTON

Button1

Properties | Advanced | Ideas

Search for a property ...

ACTION

OnSelect

```
SyncOutlookhistorytoGmail.Run
(NumberInput,EmailInput)
```

DATA

Text

"Sync your email"

Tooltip

""

Sync Outlook history to Gmail

Email address: Text input

How many emails to sync: Text input

Sync your email

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Sync Outlook history to Gmail

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

PowerApps (V2)

Get last X emails with attachments

For each email

* Select an output from previous steps

value ×

Send email to myself

* To: MyEmailAddress ×

Subject: Subject ×

Body: Font | 12 | B I U

Body ×

Power Apps

Search

Edit Play Share

Home
Create
Learn
Apps
Tables
Flows
Chatbots
AI models
Solutions
Cards
Choices
Connections
Dataflows
More

Apps > Set up your en

Details Versions Conne

Owner
Kris Smith

Description
Not provided

Created
8/8/2023, 1:34:51 AM

Modified
8/8/2023, 1:34:51 AM

Web link
https://apps.powerapps.com/p
5594523476b3&sourcetime=2

Mobile QR code

Share Set up your email sync

Add people as Users and Co-owners to your app. Make sure your data connections have been shared with all users.

every

EC Everyone in CloudCore

KS Kris Smith
Owner

Email message

Let colleagues know what your app does and how it can help them.

Include an image
Add an image to the email to showcase what your app looks like.
Tip: Use an image that is 4:3 aspect ratio and smaller than 1MB.

Choose a file to upload or drag and drop it here.

Upload

Select or add a user to set their permissions

Power Apps

Search

Edit Play Share

Home
Create
Learn
Apps
Tables
Flows
Chatbots
AI models
Solutions
Cards
Choices
Connections
Dataflows
More

Apps > Set up your em

Details Versions Conne

Owner
Kris Smith

Description
Not provided

Created
8/8/2023, 1:34:51 AM

Modified
8/8/2023, 1:34:51 AM

Web link
https://apps.powerapps.com/p
5594523476b3&sourcetime=2

Mobile QR code

Share Set up your email sync

Add people as Users and Co-owners to your app. Make sure your data connections have been shared with all users.

Enter a name, email address, or Everyone

New users

EC Everyone in CloudCore
User

Shared with Sort by Name

KS Kris Smith
Owner

Choose a file to upload or drag and drop it here.

Upload

Everyone in CloudCore

Everyone can use this app.

An organization can't edit or share apps.

Co-owner
Can use, edit, share app but not delete or change owner.

Data permissions

Make sure your users have access to the data used in your app, including gateways, APIs, connectors, and tables.

Logic flows

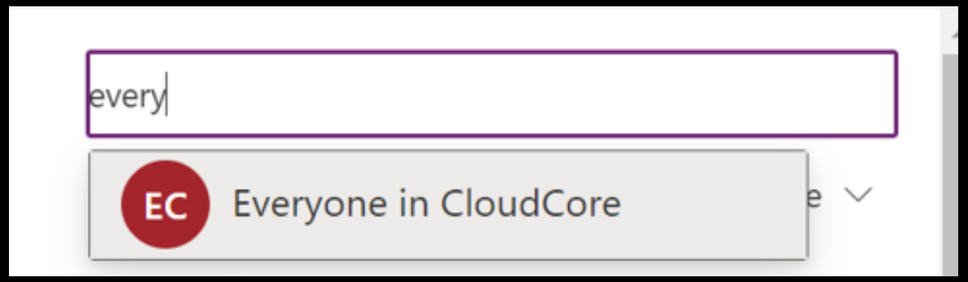
Office 365 Outlook

Gmail

Productivity sync – findings

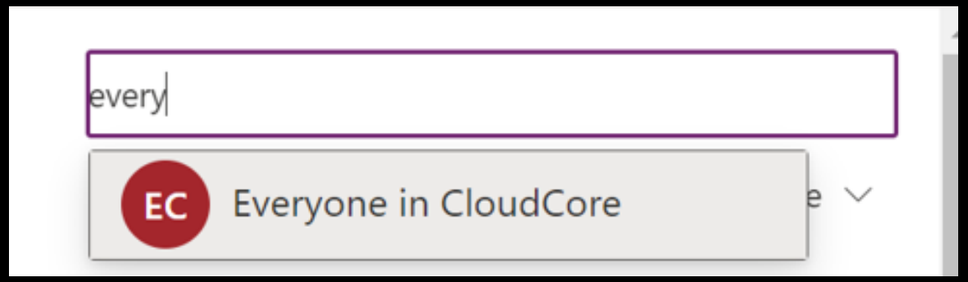
- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)

Everyone means EVERYONE, including guests by-default



Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)



Everyone means EVERYONE, including guests by-default

Check out the talk ***All You Need Is Guest*** for an attacker's perspective!

Almost there ...

Set up your email sync needs your permission to use the following. Please allow the permissions to proceed.

Office 365 Outlook
admin@zenitystage.com
Signed in View permissions

Switch account

Gmail
maortzury@gmail.com
Signed in

Switch account

Allow

Don't Allow

Sync Outlook history to Gmail

Email address: maortzury@gmail.com

How many emails to sync: 20

Sync your email

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Sync Outlook history to Gmail • Ran at 8/8/2023 1:48:09 AM

Resubmit | Cancel | Edit | Help

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

PowerApps (V2) 0s

Get last X emails with attachments 2s

For each email 32s

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Sync Outlook history to Gmail • Ran at 8/8/2023 1:48:09 AM

Resubmit Cancel Edit

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

For each email 5s

Previous Previous failed Show 1 of 5 Next failed Next

Send email to myself 1s

INPUTS Show raw inputs

To

imkrissmith@gmail.com

Subject

Admin Admin1 has shared the Weekly Timesheet app with you

Body

```
<p><html lang="en" style="min-height:100%; background:#ffffff"><hea
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!--
@media only screen and (max-width: 640px) {
 .wrap-dangler
```

Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)

Almost there ...

Set up your email sync needs your permission to use the following. Please allow the permissions to proceed.

Office 365 Outlook
admin@zenitystage.com
Signed in View permissions

Switch account

Gmail
maortzury@gmail.com
Signed in

Switch account

Allow

Don't Allow

Phishing made easy

Can we fool users to create connections for us?

- Set up a bait app that does something useful
- Generate connections on-the-fly
- Fool users to use it
- Pwn their connection (i.e. account)

☑ Account takeover

Low Code High Risk: Enterprise Domination via Low Code Abuse

Michael Bargury
DEFCON 30

Check out power-pwn on GitHub!

Productivity sync – findings

- Data Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)

SECTOR
BRIEFINGS

Story #3 – self-service

What happens when a maker leaves the org?

What happens when a maker leaves the org?

- Asset Management Failures

SECTOR

@mbrg0

Power Apps | Management App

Search

ZH

My Management App

My Employees

Kris Smith

Get Access

This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them.

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

ZH

Get Access to Employee Apps

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

Ask a chatbot

PowerApps (V2)

Email

Please enter an e-mail address

+ Add an input

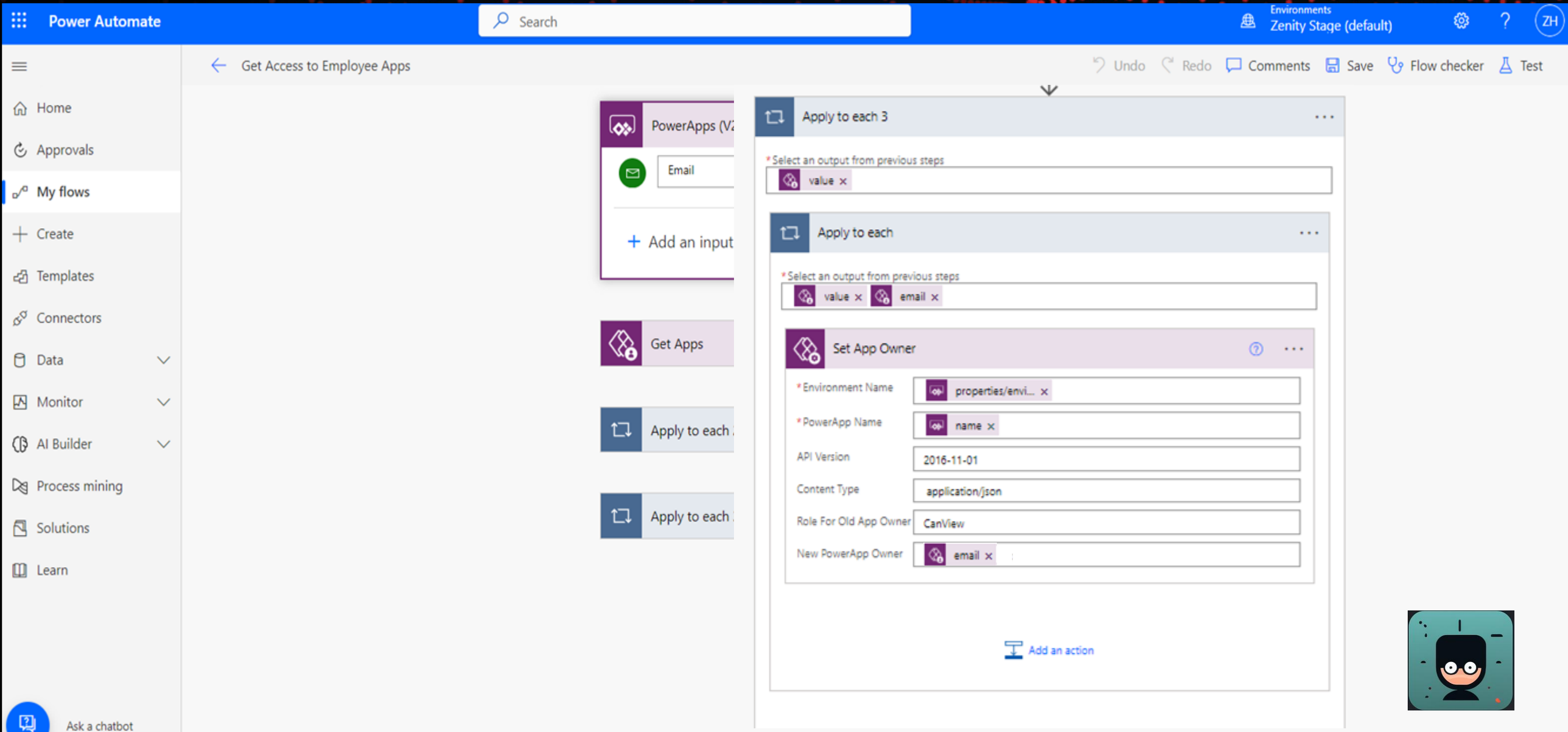
Get Apps

Apply to each 2

Apply to each 3

+ New step

Save


Power Automate
Search
Environments
Zenity Stage (default)
ZH
Get Access to Employee Apps
Undo
Redo
Comments
Save
Flow checker
Test
Home
Approvals
My flows
Create
Templates
Connectors
Data
Monitor
AI Builder
Process mining
Solutions
Learn
Ask a chatbot
PowerApps (V
Email
Add an input
Get Apps
Apply to each
Apply to each
Apply to each 3
*Select an output from previous steps
value
Apply to each
*Select an output from previous steps
value
email
Set App Owner
*Environment Name
properties/envi...
*PowerApp Name
name
API Version
2016-11-01
Content Type
application/json
Role For Old App Owner
CanView
New PowerApp Owner
email
Add an action

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

ZH

Get Access to Employee Apps

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

Ask a chatbot

PowerApps (V2)

Email

+ Add an input

Get Apps

Apply to each

Apply to each

Apply to each 3

*Select an output from previous steps

value ×

Apply to each

*Select an output from previous steps

value × email ×

Set App Owner

*Environment Name: properties/envi... ×

*PowerApp Name: name ×

API Version: 2016-11-01

Content Type: application/json

Role For Old App Owner: CanView

New PowerApp Owner: email ×

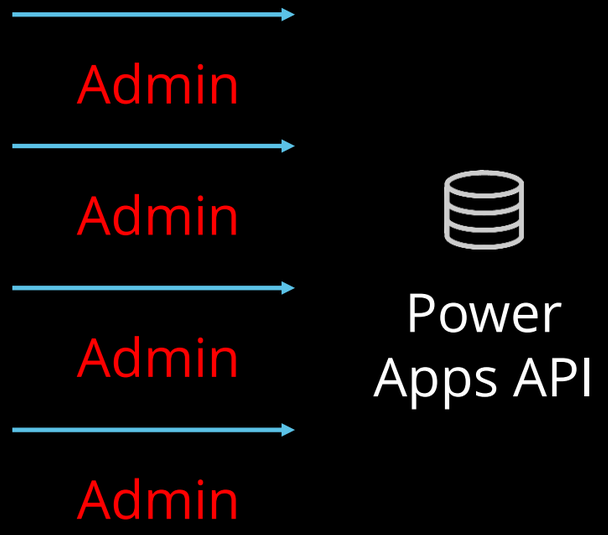
Add an action

SECTOR

Self-service – findings

Self-service – findings

SOC Panics!



Self-service – findings

- App embedded with admin ID (Account Impersonation)

Power Apps | Management App

Search

ZH

My Management App

My Employees

Kris Smith

Get Access

This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them.

Elements | Console | Sources | Network | Performance | Memory | Application | Lighthouse | Security | Recorder

19 5 71

Search

Preserve log | Disable cache | No throttling

Filter | Invert | Hide data URLs | All | Fetch/XHR | JS | CSS | Img | Media | Font | Doc | WS | Wasm | Manifest | Other | Has blocked cookies

Blocked Requests | 3rd-party requests

20000 ms | 40000 ms | 60000 ms | 80000 ms | 100000 ms | 120000 ms | 140000 ms | 160000 ms

Path

- /invoke
- /Collector/3.0
- /Collector/3.0
- /Collector/3.0
- /powerapps/apps/bc428f80-8f28-4877-a490-f40a0d3cae7...
- /config/v1/PowerApps/1.0.0.0
- /config/v1/PowerApps/1.0.0.0

7 requests | 2.8 kB transferred | 1.3 kB resources

Headers | Payload | Preview | Response | Initiator | Timing

Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
Sec-Fetch-Dest:	empty
Sec-Fetch-Mode:	cors
Sec-Fetch-Site:	cross-site
User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
X-Ms-Client-App-Id:	/providers/Microsoft.PowerApps/apps/bc428f80-8f28-4877-a490-f40a0d3cae75
X-Ms-Client-Environment-Id:	/providers/Microsoft.PowerApps/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3
X-Ms-Client-Object-Id:	7cb2f429-a54a-46c3-8e4f-df3a3032f249
X-Ms-Client-Request-Id:	769a604e-cb2f-4bda-899d-1898d8781bfc
X-Ms-Client-Session-Id:	7f7754ee-d98c-43d2-bcff-3c1745ac7cf8
X-Ms-Client-Tenant-Id:	32f814a9-68c8-4ca1-93aa-5594523476b3
X-Ms-Request-Method:	POST
X-Ms-Request-Url:	/apim/logicflows/f818501a-d1ce-42db-873a-5f5261671cc7/triggers/manual/run?api-version=2015-02-01-preview
X-Ms-User-Agent:	PowerApps/3.23074.15 (Web AuthoringTool; AppName=bc428f80-8f28-4877-a490-f40a0d3cae75)

Power Apps | Management App

Search

ZH

My Management App

Elements Console Sources Network Performance Memory Application Lighthouse Security Recorder 19 5 71

Search

Preserve log Disable cache No throttling

Filter Invert Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other

Has blocked cookies Blocked Requests 3rd-party requests

500 ms 1000 ms 1500 ms 2000 ms 2500 ms 3000 ms 3500 ms 4000 ms 4500 ms

Path

/invoke

/Collector/3.0

Headers Payload Preview Response Initiator Timing

Request Payload view source

```
{email: "zivh@cloudcore.com"}
  email: "zivh@cloudcore.com"
```

2 requests 1.4 kB transferred 0 B resources

Self-service – findings

- App embedded with admin ID (Account Impersonation)
- IDOR (Injection handling failures)

Self-service – findings

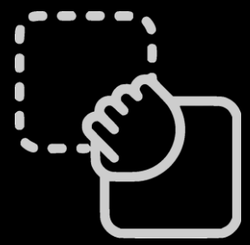
- App embedded with admin ID (Account Impersonation)
- IDOR (Injection handling failures)

SECTOR
BRIEFINGS

Story #4 – customer care

The Customer Care team at a large eCommerce company wanted to improve customer service.

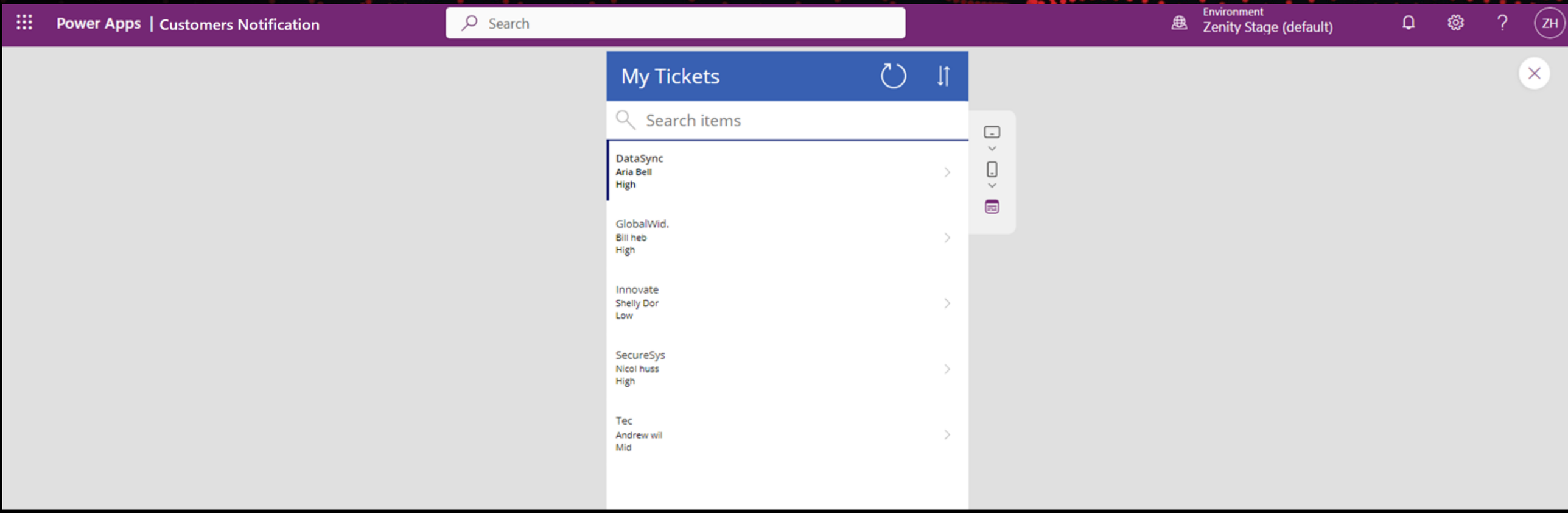
Goal: improve customer service
Method: build an app that lets relevant company employees view customer support history and latest purchases
Challenge: employees don't have permissions to the customer database



Customer care app

SECTOR

@mbrg0



SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Update customer ticket record

Undo | Redo | Comments | Save | Flow checker | Test

- Home
- Approvals
- My flows
- Create
- Templates
- Connectors
- Data
- Monitor
- AI Builder
- Process mining
- Solutions
- Learn

PowerApps (V2)

Update row (V2)

Respond to a PowerApp or flow

+ New step

Save

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Edit | Share | Save As | Delete | Run | Send a copy

Home
Approvals
My flows
Create
Templates
Connectors
Data
Monitor
AI Builder
Process mining
Solutions
Learn

Owner
Kris Smith

Created
Aug 8, 10:45

Modified
Aug 8, 10:5

Type
Instant

Plan
The user wh

28-day run history

Edit columr

Your flow hasn't been run yet. Select **Run** to see it work.

Manage run-only permissions

Invite users or groups

Let others run this flow and see the results, but not edit in any way.

Enter names, emails, or user groups

Currently shared with

All Company
allcompany@zenitystage.on...

Connections Used

These connections will provide the users listed here to have run-only access to this flow. Unless providing their own connection, run-only users will not have access to these connections outside this flow.

SQL Server
Access to this connection is provided by the owne
flow.

Use this connection (kris@zenitystage.com)

Impact:

- ✓Employees are happy
- ✓Customers are happy
- ✓Customer Care team is happy

Customer care – findings

SECTOR

@mbrg0

Power Automate

Search

Environments
Zenity Stage (default)

KS

Edit | Share | Save As | Delete | Run | Send a copy

Home
Approvals
My flows
Create
Templates
Connectors
Data
Monitor
AI Builder
Process mining
Solutions
Learn

Owner
Kris Smith

Created
Aug 8, 10:45

Connections Used

These connections will provide the users listed here to have run-only access to this flow. Unless providing their own connection, run-only users will not have access to these connections outside this flow.

SQL Server
Access to this connection is provided by the owner of the flow.

Use this connection (kris@zenitystage.com)

28-day run

Your flow hasn't been run yet. Select **Run** to see it work.

Manage run-only permissions

ps

ow and see the results, but not edit in any way.

ails, or user groups

th

pany
any@zenitystage.on...

Connections Used

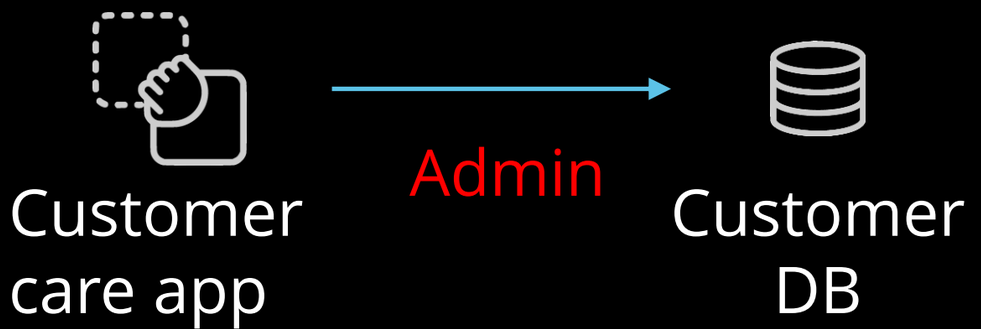
These connections will provide the users listed here to have run-only access to this flow. Unless providing their own connection, run-only users will not have access to these connections outside this flow.

SQL Server
Access to this connection is provided by the owne
flow.

Use this connection (kris@zenitystage.com)

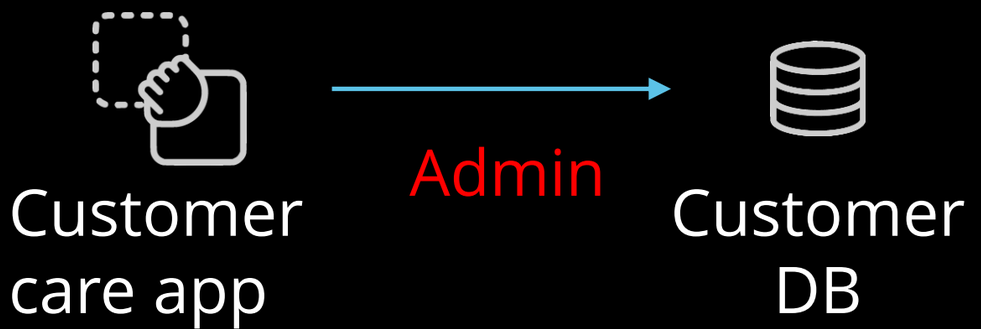
Impact:

- ✓Employees are happy
- ✓Customers are happy
- ✓Customer Care team is happy



Impact:

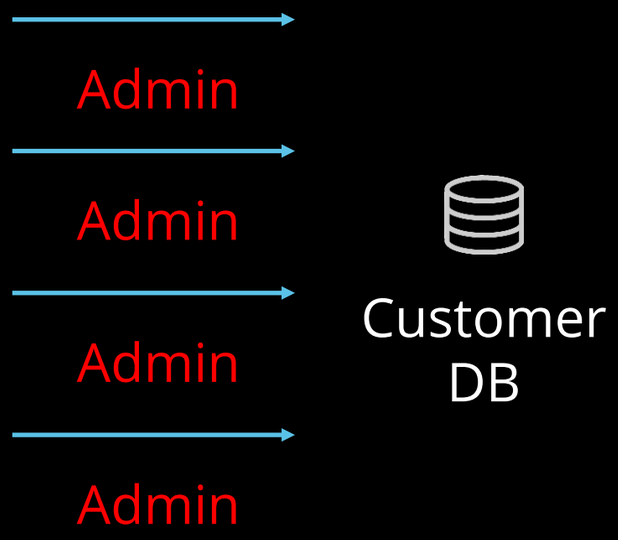
- ✓Employees are happy
- ✓Customers are happy
- ✓Customer Care team is happy



- ✓SOC panics

Customer care – findings

- App embedded with admin ID (Account Impersonation)



SECTOR
BRIEFINGS

Story #5 – predictable-misconfiguration

By Design: How Default Permissions on Microsoft Power Apps Exposed Millions

UpGuard Team
Published Aug 23, 2021

Anonymous API access

Anonymous API access

Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

portal.powerappsportals.com/_odata

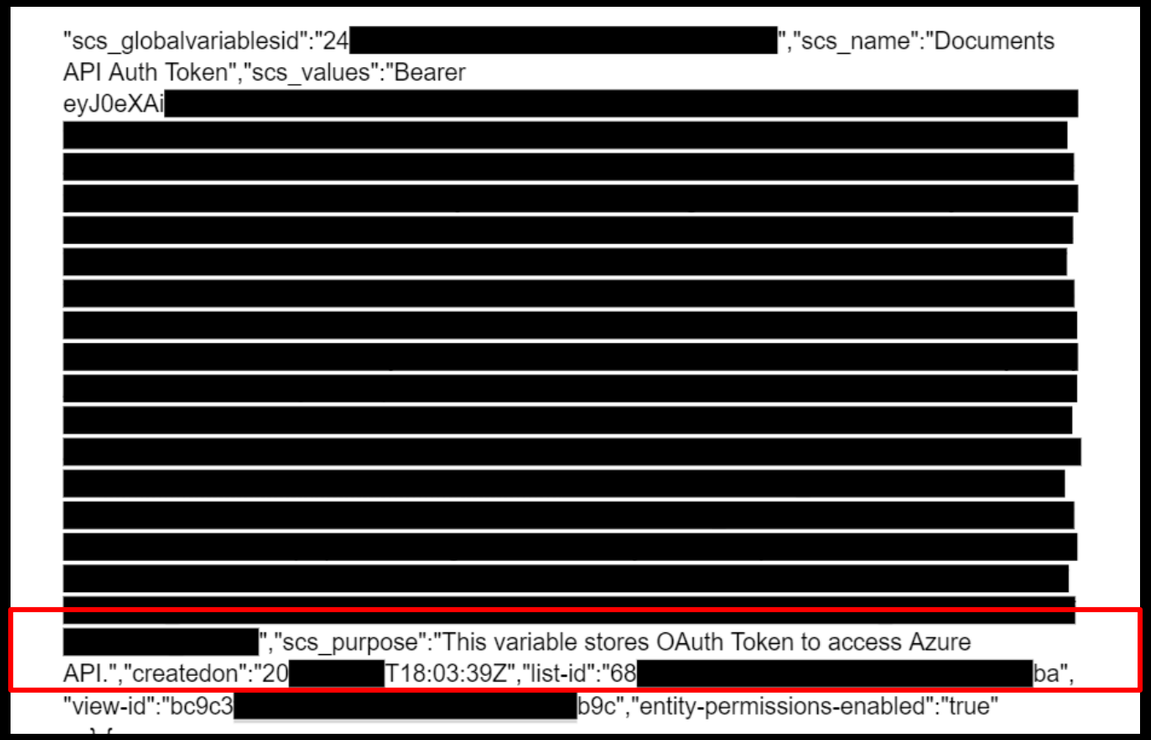
zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

SECTOR

Nothing to see here

/_odata

/globalvariables:



SECTOR
BRIEFINGS

Story #6 – extendibility

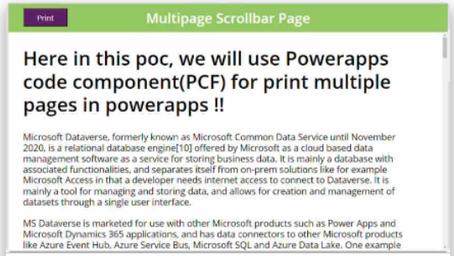
SECTOR

@mbrg0

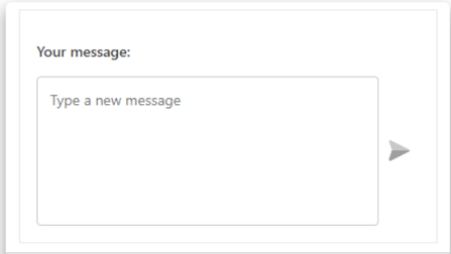
PCF Gallery

Categories | Please select | Search | Authors | Ideas | About | Submit a new PCF Control

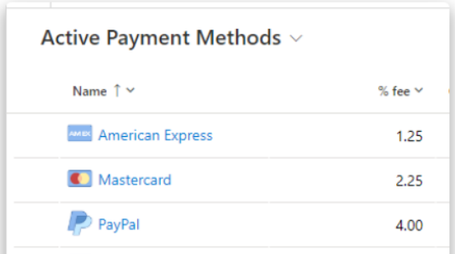
We launched a new website: Community Events .IT



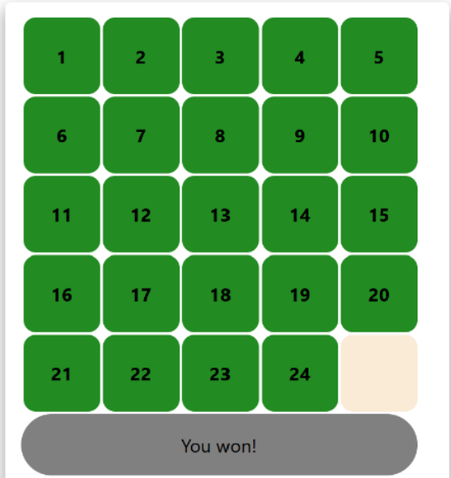
Scrollable Screen Multi Page Print PCF



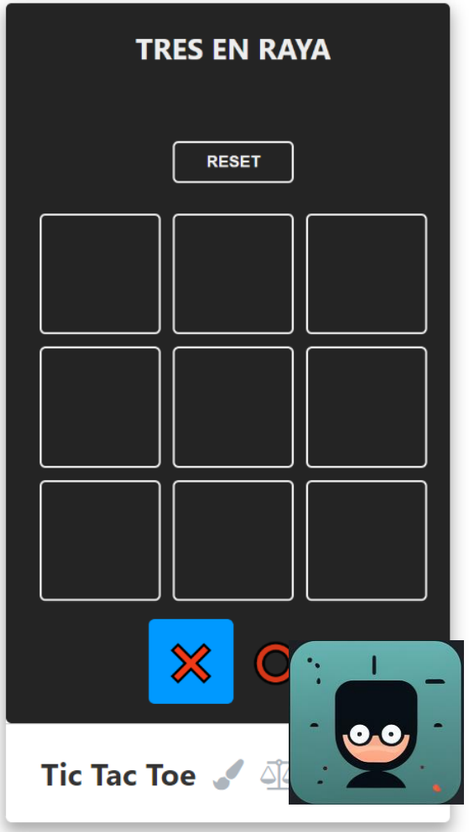
Enhanced Textarea



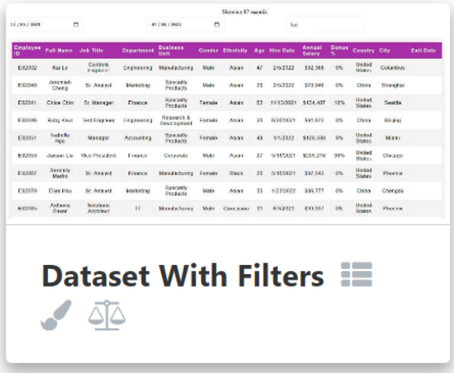
RecordImage Cell Renderer



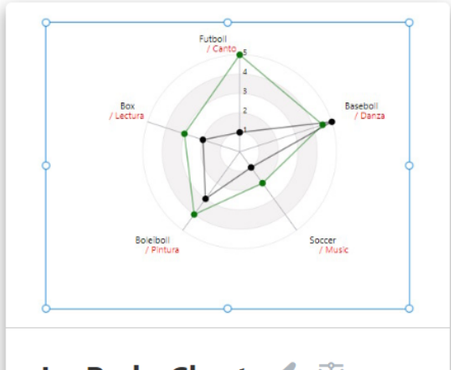
Slide Puzzle



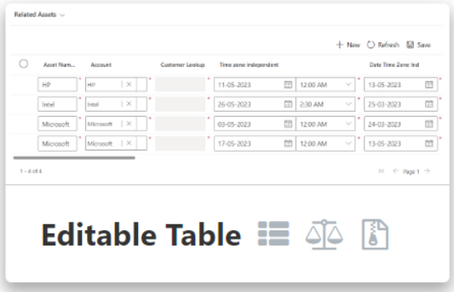
Tic Tac Toe



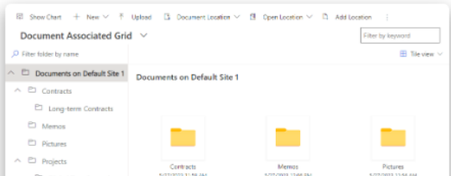
Dataset With Filters



InaRadarChart



Editable Table



Power Apps

Search

New solution | Import solution | Open AppSource | Publish all customizations | ...

11 environment variables need to be updated.

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

Solutions

Solutions | Publishers | History

Display name	Name	Created	Version
AI Solution Anchor	msdyn_AISolutionAn...	2 minutes ago	202307.2.32.3
AI Privilege Overrides Solution	msdyn_AIPrivilegeOv...	3 minutes ago	202307.2.32.3
AI Solution deprecated templates	msdyn_AISolutionDe...	7 minutes ago	202307.2.32.3
AISolutionFullAdditions	msdyn_AISolutionFul...	10 minutes ago	202307.2.32.3
InavantRadarChartSolution	InavantRadarChartS...	5 days ago	1.0
pwntoso	pwntoso	1 week ago	1.0.0.1
PowerPortals Program Registration	PowerPortals_Progra...	2 weeks ago	1.2304.3.0
Program Registration Controls	PowerPortals_Progra...	2 weeks ago	1.2304.4.0
PowerPortals Program Registration Anchor	PowerPortals_Progra...	2 weeks ago	1.2304.3.0
Dynamics 365 Portals - Automate	MicrosoftPortalAuto...	2 weeks ago	9.3.2304.0
slider	slider	2 weeks ago	1.0
lanasol	lanasol	3 weeks ago	1.0
Power Platform Catalog Manager	mspcat_CatalogMan...	1 month ago	1.1.5.500

Import a solution

Environment
Zenity Stage (default)

Select a file

Browse for the solution file to import.

Browse SearchBoxPCF-main.zip

Try pipelines for effortless imports

Use pipelines to simplify and automate the deployment process in your organization. Pipelines is a feature of Managed Environments.
Learn more

Next | Cancel

Power Apps | Search

New solution | Import solution | Open AppSource | Publish all customizations | ...

11 environment variables need to be updated.

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

Solutions

Solutions | Publishers | History

Display name				
AI Solution Anchor				
AI Privilege Overrides Solution				
AI Solution deprecated templates				
AISolutionFullAdditions				
InavantRadarChartSolution				
pwntoso				
PowerPortals Program Registration	⋮	PowerPortals_Progra...	2 weeks ago	1.2304.3.0
Program Registration Controls	⋮	PowerPortals_Progra...	2 weeks ago	1.2304.4.0
PowerPortals Program Registration Anchor	⋮	PowerPortals_Progra...	2 weeks ago	1.2304.3.0
Dynamics 365 Portals - Automate	⋮	MicrosoftPortalAuto...	2 weeks ago	9.3.2304.0
slider	⋮	slider	2 weeks ago	1.0
lanasol	⋮	lanasol	3 weeks ago	1.0
Power Platform Catalog Manager	⋮	mspcat_CatalogMan...	1 month ago	1.1.5.500

Import a solution

Environment
Zenity Stage (default)

Select a file

Browse for the solution file to import.

Browse SearchBoxPCF-main.zip

Import a solution

Environment
Zenity Stage (default)

Select a file

Browse for the solution file to import.

Browse SearchBoxPCF-main.zip

Try pipelines for effortless imports

Use pipelines to simplify and automate the deployment process in your organization. Pipelines is a feature of Managed Environments.
Learn more

Next | Cancel

Extendibility – findings

- Vulnerable and Untrusted Components

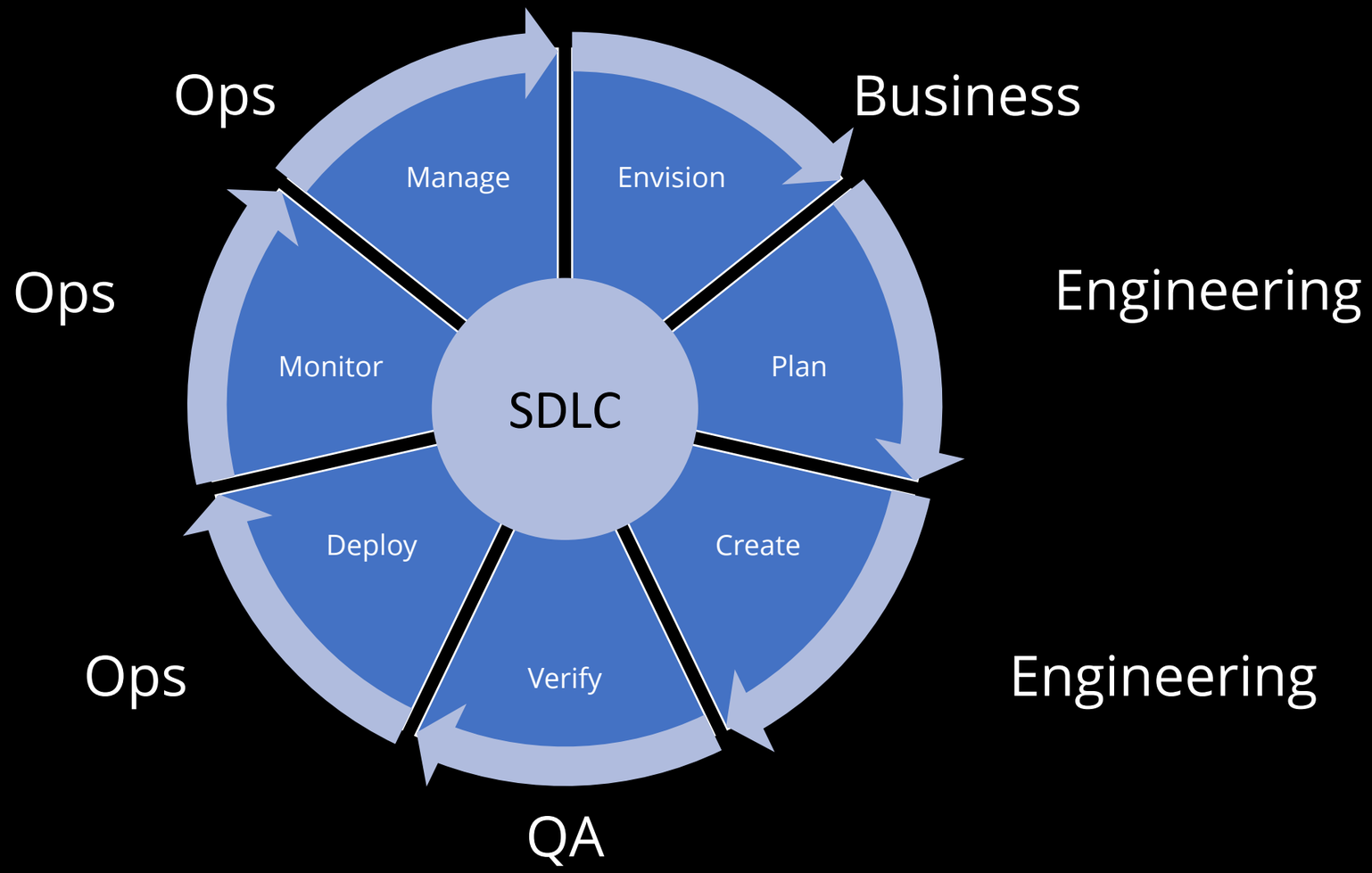
Recap:

- We are leaving heavy security decisions in the hands of business users
- When choosing between productivity and security, the choice is obvious

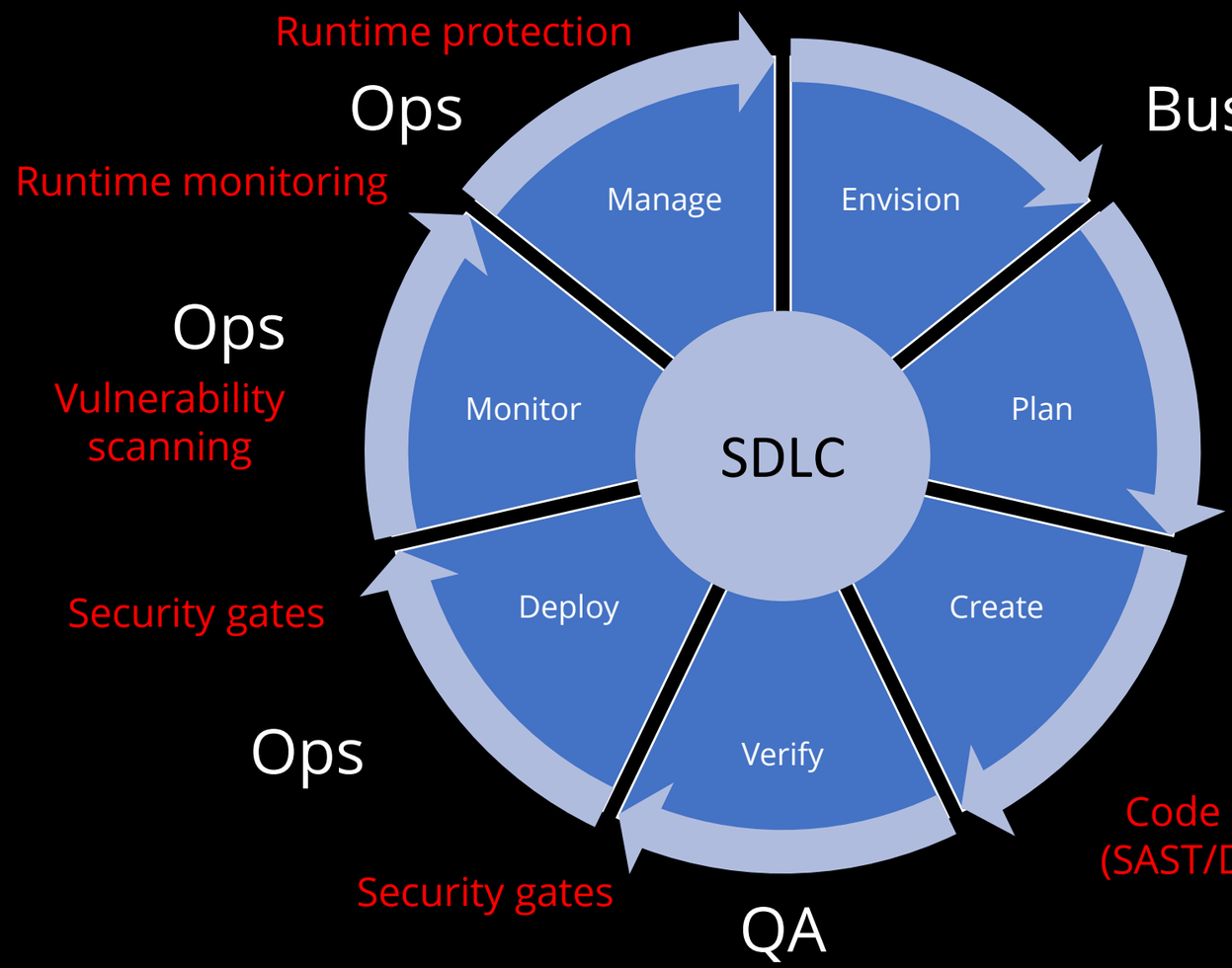
SECTOR
BRIEFINGS

Why does it go wrong?

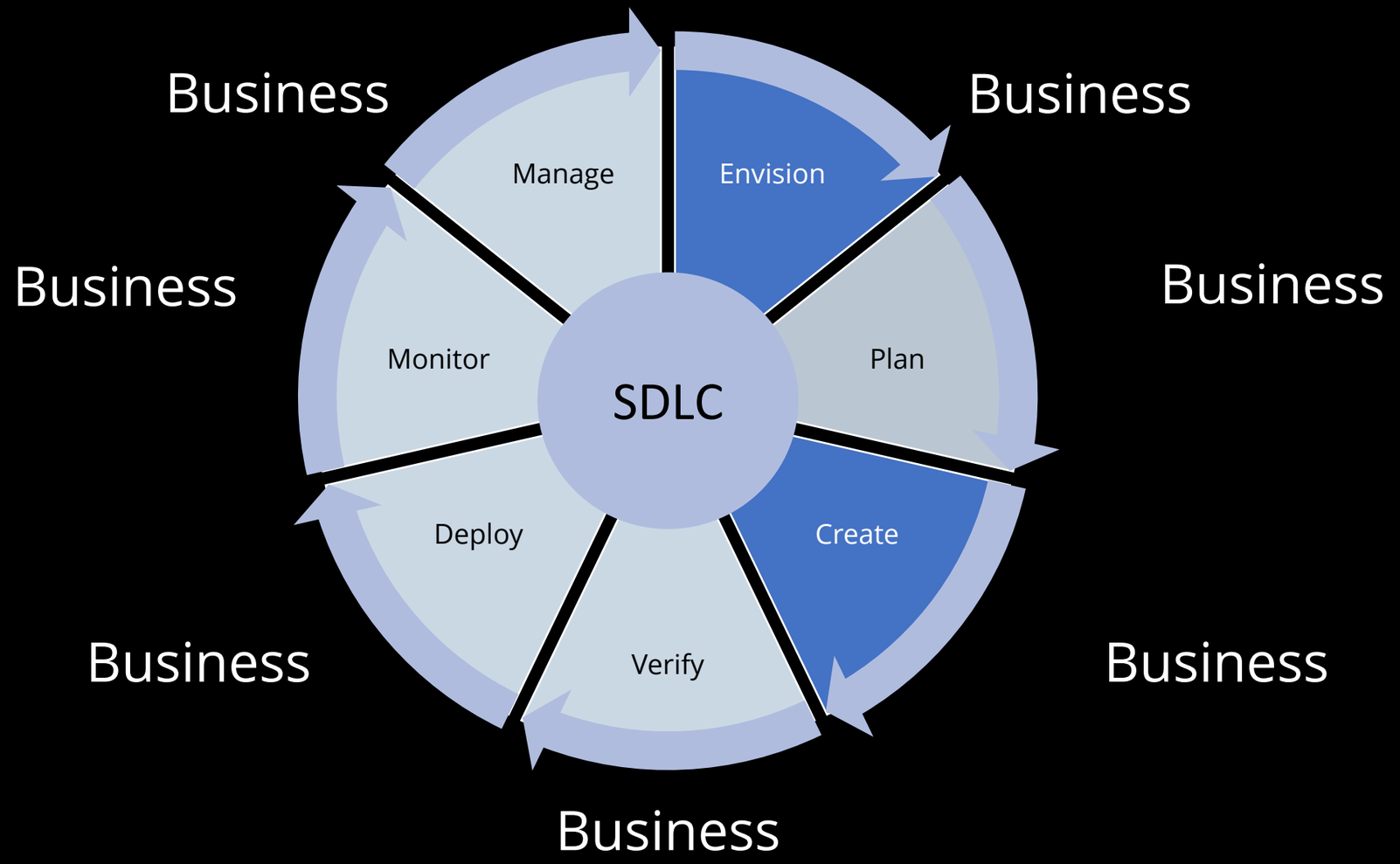
Pro Code SDLC



Pro Code SDLC



No Code
No SDLC?

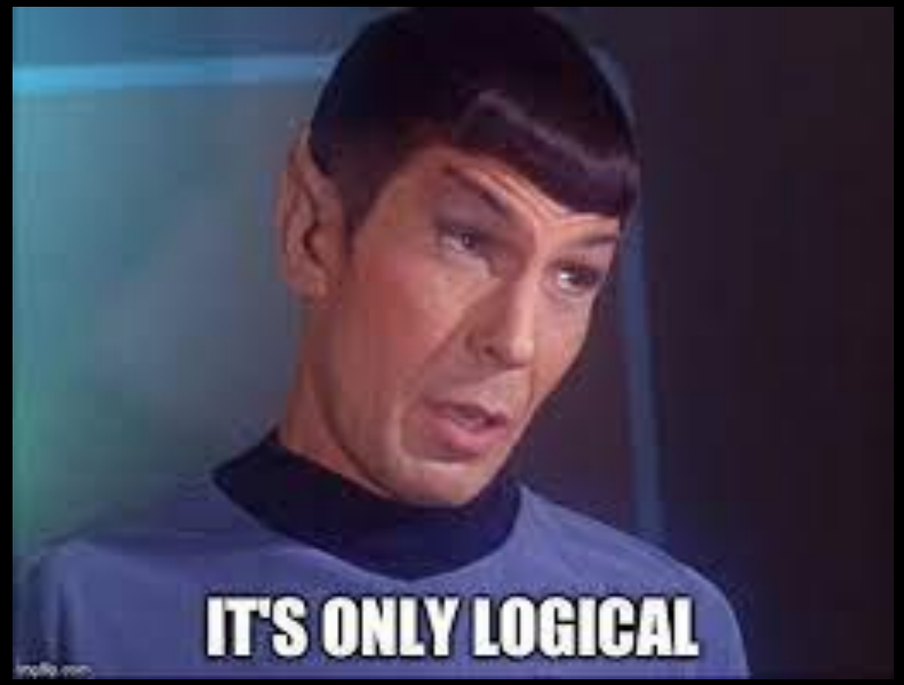


We've given business users:

- Dev-level power
- Missing best practice
- No controls
- No guardrails

We've given business users:

- Dev-level power
- Missing best practice
- No controls
- No guardrails



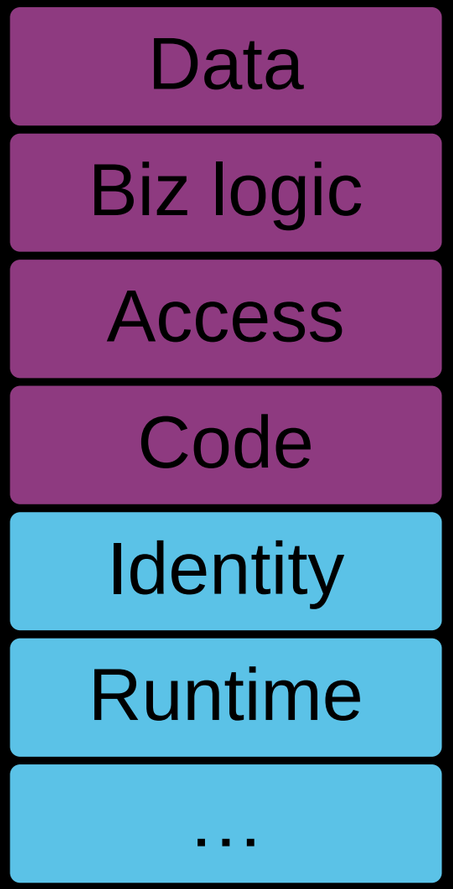
Could we really expect anything else?

SECTOR
BRIEFINGS

The LCNC Shared Responsibility Model

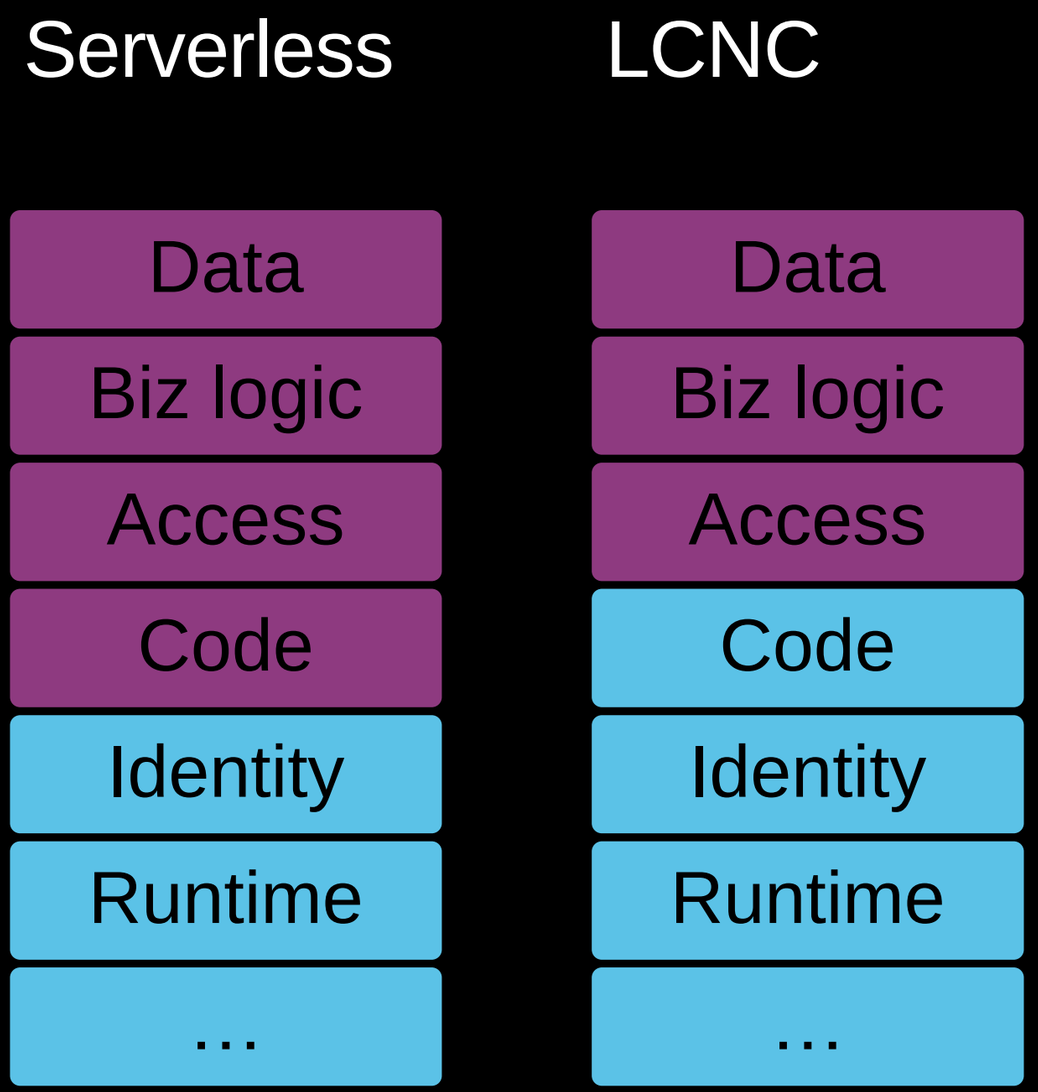
@mbrg0

Serverless

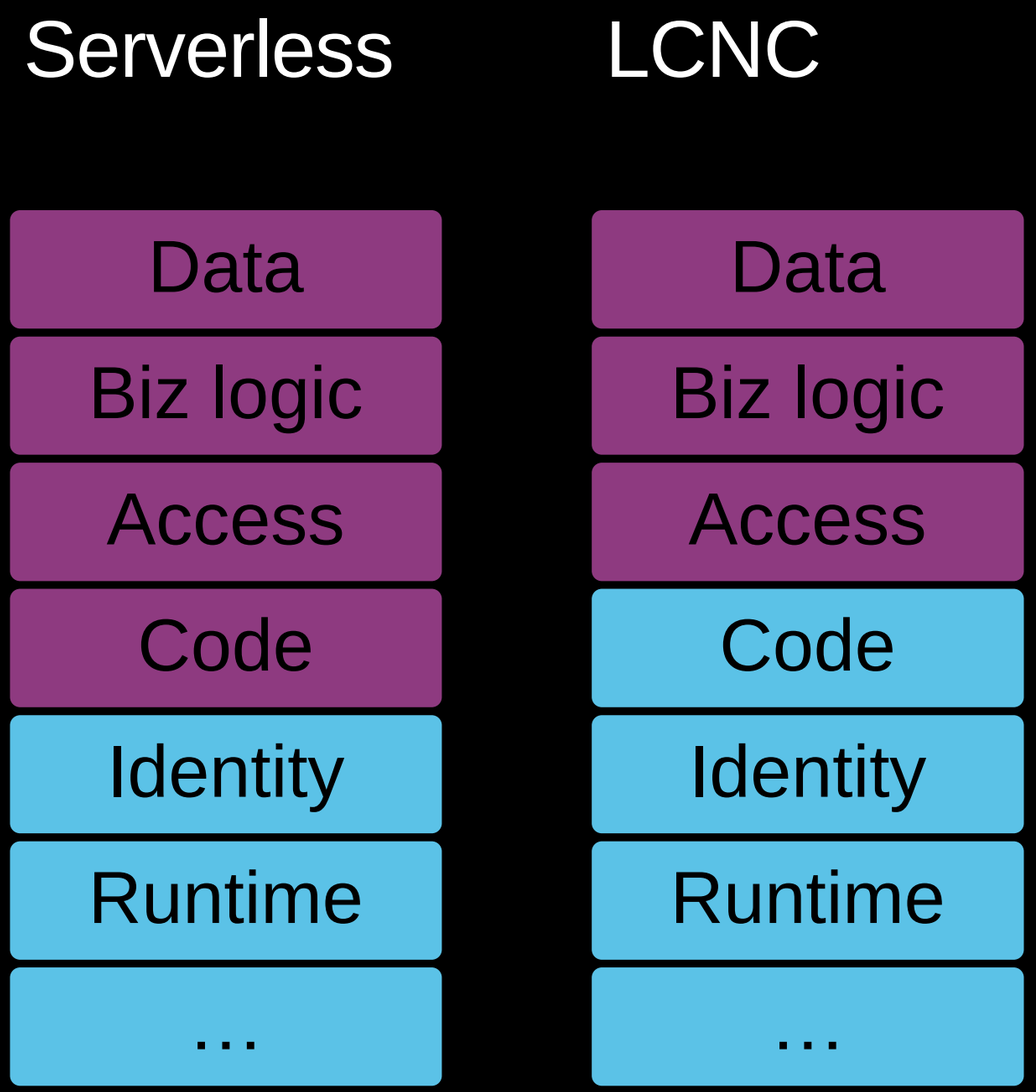


Customer

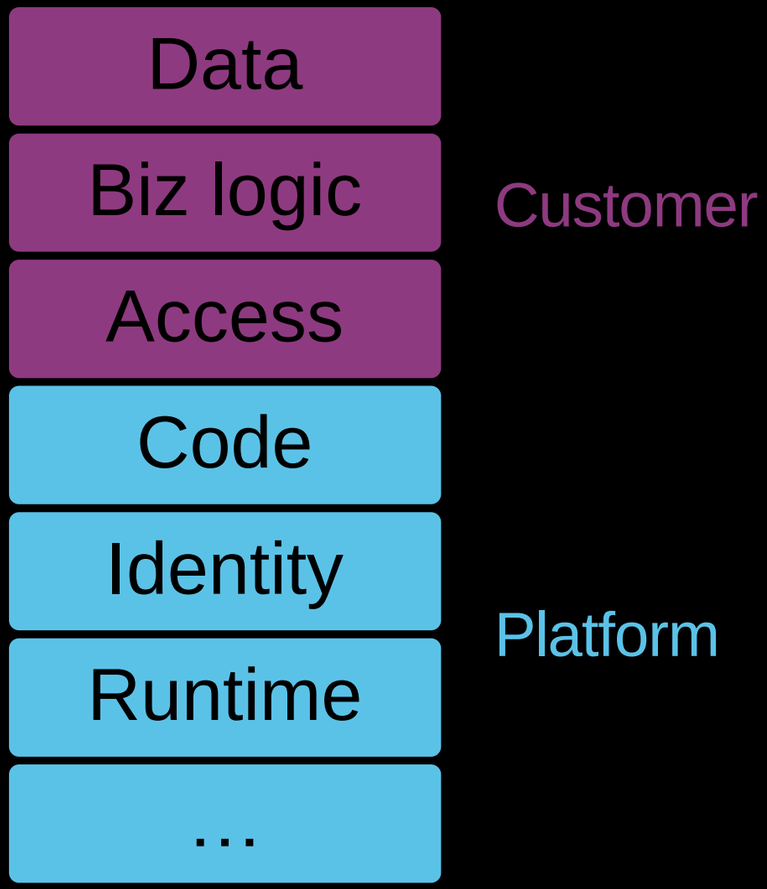
Platform


Serverless
LCNC
Data
Biz logic
Access
Code
Identity
Runtime
…
Data
Biz logic
Access
Code
Identity
Runtime
…
Customer
Platform

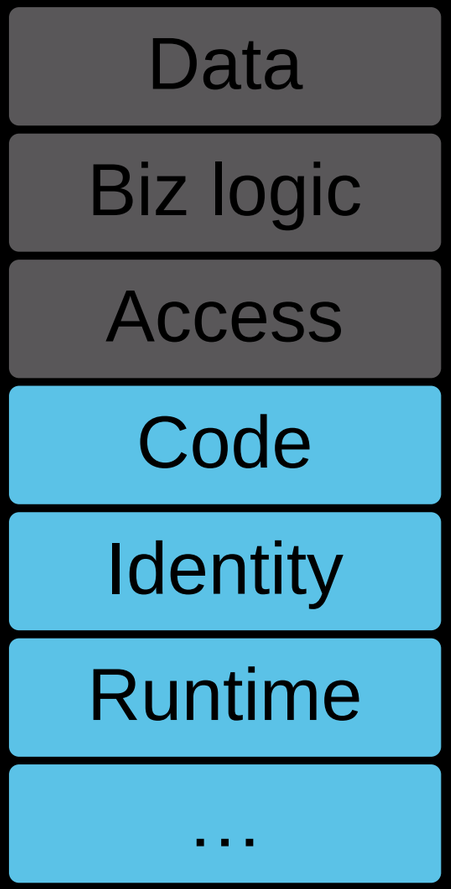
We must own our side of the Shared Responsibility Model



LCNC


Data
Biz logic
Access
Code
Identity
Runtime
…
Customer
Platform

Platforms have to step up



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

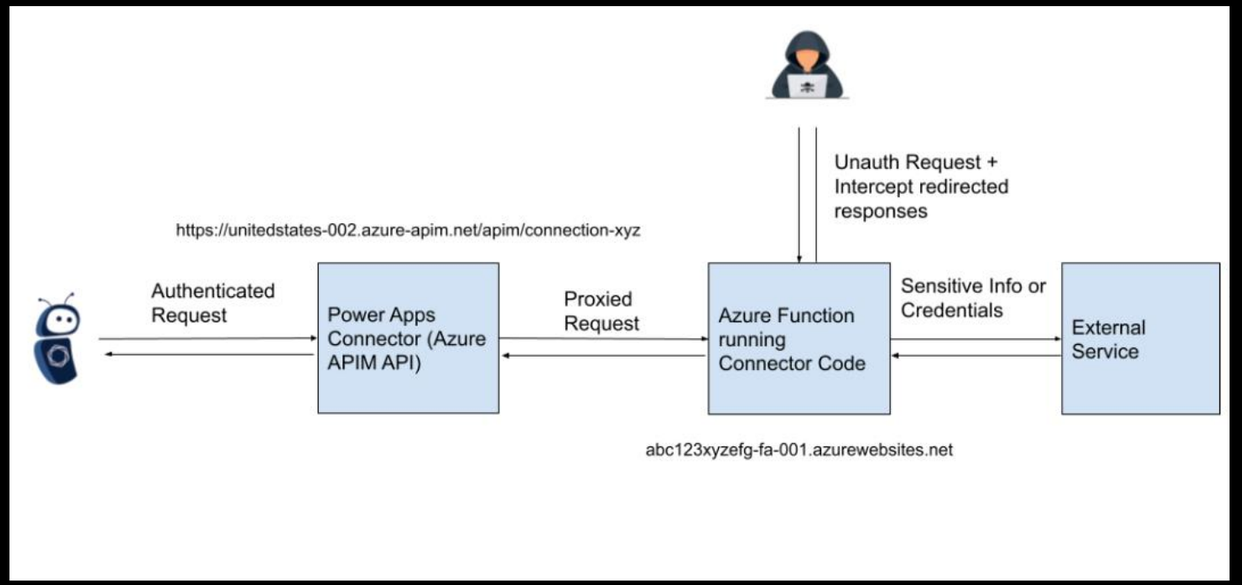
They need to own the code running on their platforms, in addition to the rest of the Shared Responsibility Model.

Platforms have to step up

- Data
- Biz logic
- Access
- Code
- Identity
- Runtime
- …

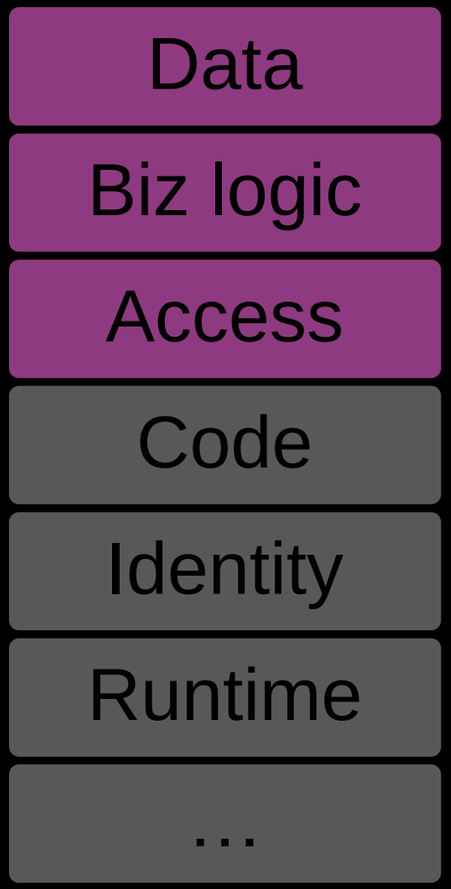
Customer

Platform

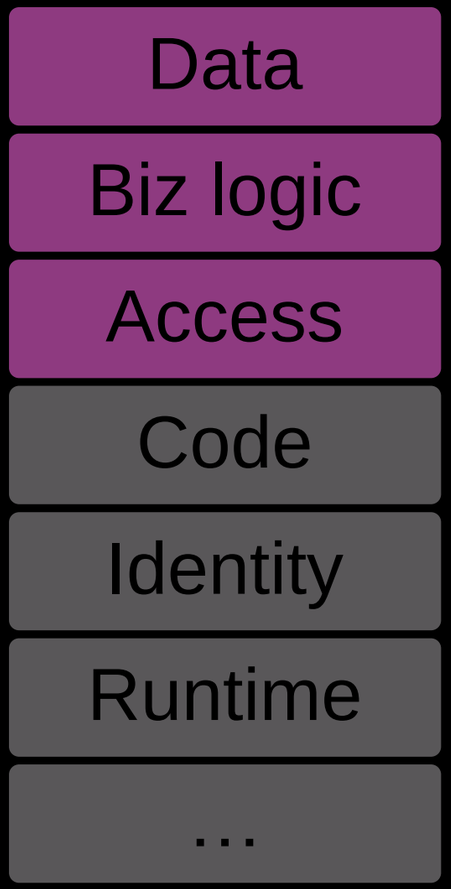


https://www.tenable.com/security/research/tra-2023-25

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



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

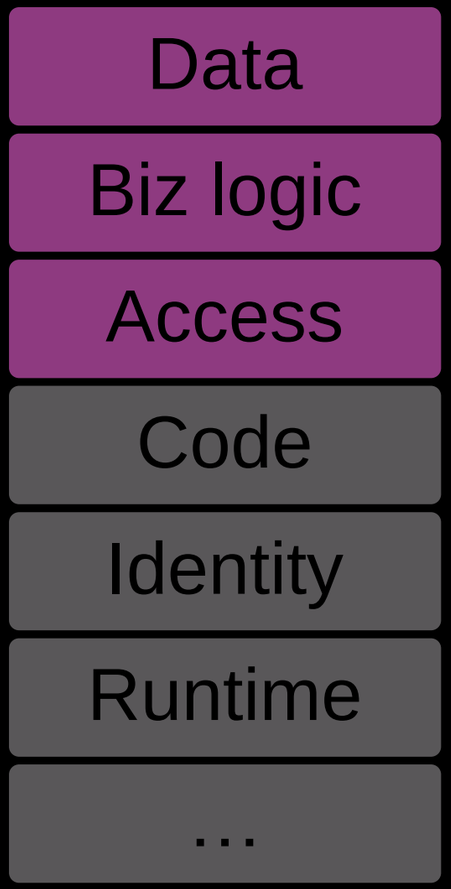


Customer

Platform

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

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



Customer

Platform

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

Who owns AppSec for apps built by business users?

SECTOR
BRIEFINGS

How can we fix it? (Or: LCNC AppSec)

LCNC AppSec is different

AppSec for, well, traditional apps

AppSec for LCNC apps

LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness

AppSec for LCNC apps

1. Business users w/ no awareness

LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC

LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC
3. Secure controls

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don’t apply

LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC
3. Secure controls
4. Hundreds of apps / year

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don’t apply
4. 10x-100x more apps / year

SECTOR

Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don’t apply
4. 10x-100x more apps / year

SECTOR

Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

Example Attack & Misuse Scenarios - Business Users

Scenario #1

A developer builds a No Code/Low Code Robotic Process Automation (RPA) application that connects to a database to update records. The connection uses the Admin's authentication (username and password) to log updates. Although 10 different users use this RPA process, all actions are being recorded as being done by the Admin. Logging systems can no longer track productivity, attribute errors to specific users, or identify malicious behavior.

Scenario #2

A developer builds an application to help the sales team in the field. The developer uses their credentials (username and password) when writing the application, so all sales made through the application are attributed to the developer, not the sales person facilitating the sale.

OWASP LCNC Top 10 sections for business users by John McTiernan and Yianna Paris @punk_fairybread

SECTOR

Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don’t apply
4. 10x-100x more apps / year

<u>LCNC Security Standard:</u>

- Approved use cases
- SDLC
- Environments
- Testing
- Monitoring
- SBOM
- …

SECTOR

Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don’t apply
4. 10x-100x more apps / year

LCNC is an opportunity for more visibility than ever before

SECTOR

Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

SecTor Sound Bytes

1. We're leaving business users alone with security v productivity decisions, what did we expect them to choose?

2. It's time for AppSec to bring citizen developers under the security umbrella

3. There are 5M C# devs today and over 8M citizen devs - we're neglecting the next generation of (business) devs

Sure, Let Business Users Build Their Own. What Could Go Wrong?

Michael Bargury @mbrg0

Zenity