

No Code No Risk? What Happens When We Leave No Code up for Grabs

Michael Bargury @ Zenity

About me

- CTO and co-founder @ Zenity
- Ex MSFT cloud security
- OWASP *'Top 10 LCNC Security Risks'* project lead
- Dark Reading columnist



@mbrg0



bit.ly/lcsec



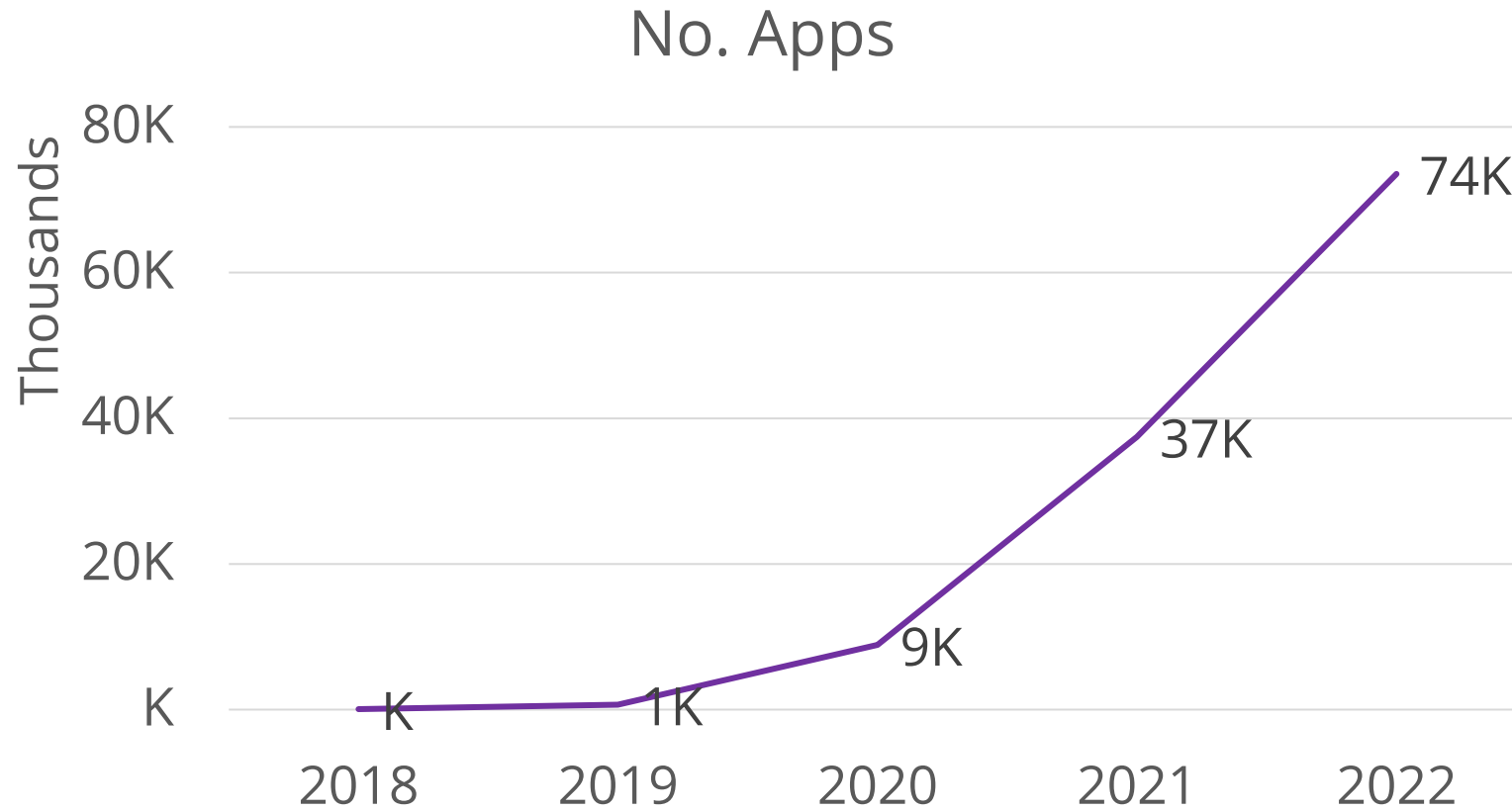
Outline

- How pervasive is it?
- Low Code / No Code growth and evolution
- The “hit-save” SDLC
- OWASP Top 10 LCNC Security Risks
- Learn more

Business-Led Development Is Here

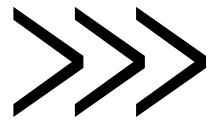


Exponential Growth in Business Development



The Low-Code/No-Code Evolution: How did we get here?

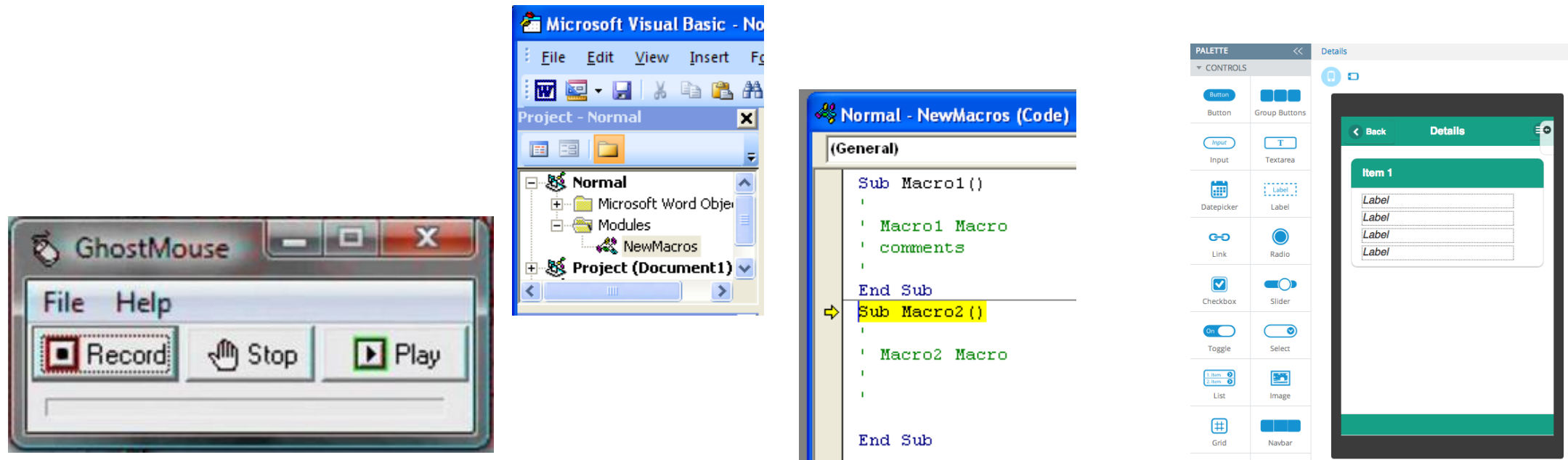
Business Needs



IT Capacity



If it sounds familiar, its because it is



Tech evolution

Build everything

- If this than that automation
- Integrations
- Business apps
- Whole products
- Mobile apps

The image displays three overlapping screenshots from the Zapier interface, illustrating different stages of building an automation:

- Top Screenshot:** Shows a Zap configuration for "Save Gmail attachments to your Google Drive". The trigger is "When a new email arrives" (1s), which outputs fields like "From" (michaelbargury@zenity.io) and "Subject" (Fwd: Remote desktop links). This triggers the action "Apply to each attachment" (7s), which then triggers "Upload to Google Drive" (5s). The "Upload to Google Drive" action has input fields for "Folder path" (/Attachments) and "File name" (hi.rdp).
- Middle Screenshot:** Shows the "Trigger" configuration for "1. New Mention in Slack". It includes a "Choose app & event" section and a "Choose account" dropdown menu. The dropdown shows two options: "Slack @michaelbargury (pwntoso)" (used in 1 Zap) and "Slack @michaelbargury (CTOs)" (used in 0 Zaps), both marked as "Personal". A "+ Connect a new account" button is visible at the bottom.
- Bottom Screenshot:** Shows the "Insert" menu with a search bar and a list of components: Popular (Text label, Edit form, Text input, Vertical gallery), Rectangle, Date picker, Button, Input, Display, Layout, Media, Icons, Shapes, Charts, AI Builder, and Mixed Reality.

Available in every major enterprise



zapier*

mx mendix



make
formerly Integromat



servicenow™



Betty Blocks



Microsoft

outsystems

Appian

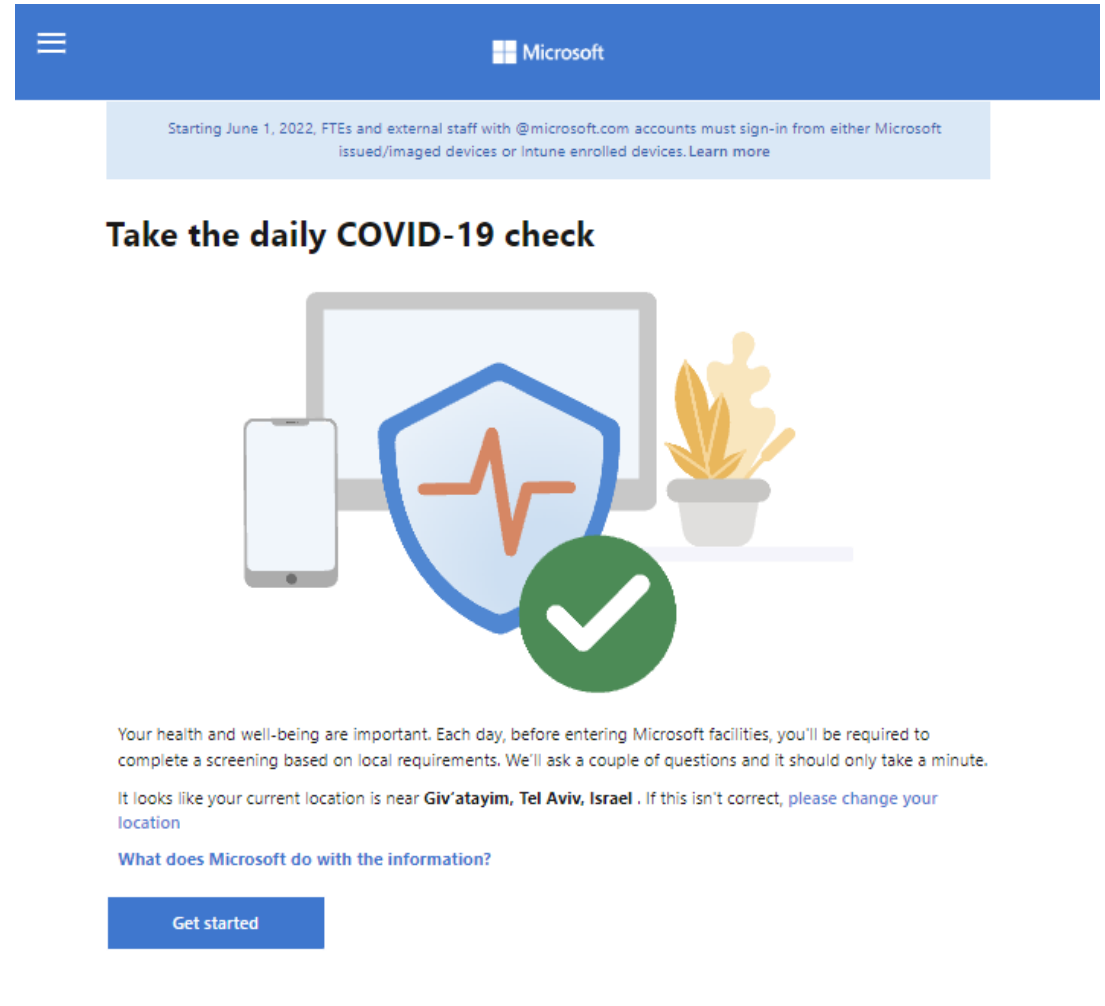
Build Business Apps Faster

How low code / no code accelerates development:

- Ease of use lowers barrier to entry
- Off-the-shelf integrated components
- Key app features are baked-in (AuthN, AuthZ, ..)
- Connectors to on-prem, cloud and SaaS
- “Save” to deploy
- No infra to maintain

COVID health check app by Microsoft

<https://aka.ms/healthcheck>



The screenshot shows the Microsoft COVID-19 health check app landing page. At the top, there is a blue header with the Microsoft logo and a navigation menu icon. Below the header, a light blue banner contains the text: "Starting June 1, 2022, FTEs and external staff with @microsoft.com accounts must sign-in from either Microsoft issued/imaged devices or Intune enrolled devices. Learn more". The main heading is "Take the daily COVID-19 check". Below this is an illustration featuring a laptop, a smartphone, a shield with a red heartbeat line, and a green checkmark in a circle. To the right of the shield is a potted plant. The text below the illustration reads: "Your health and well-being are important. Each day, before entering Microsoft facilities, you'll be required to complete a screening based on local requirements. We'll ask a couple of questions and it should only take a minute. It looks like your current location is near **Giv'atayim, Tel Aviv, Israel**. If this isn't correct, [please change your location](#)". Below this is a link: "What does Microsoft do with the information?". At the bottom of the main content area is a blue button labeled "Get started".

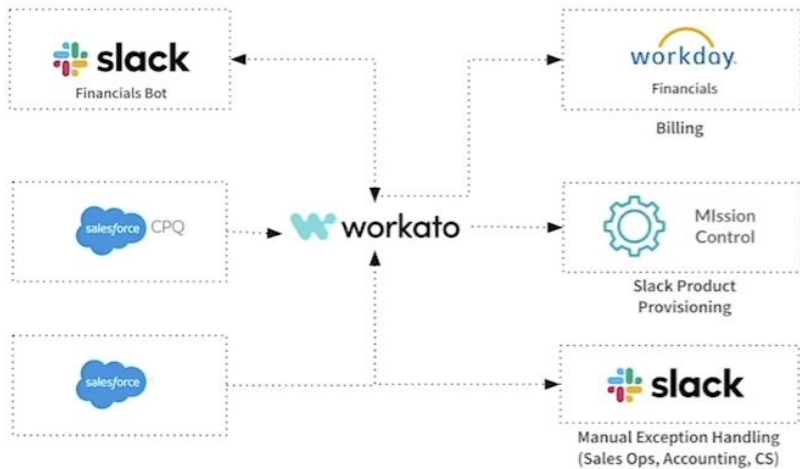
For issues or concerns contact IT Global Helpdesk globalhd@microsoft.com

[Microsoft Data Privacy Notice](#) [Identity Terms of Use](#) [Feedback](#)

© 2021 Microsoft



Automating order to cash fulfillment



💰 90% no touch orders

💰 95% orders processed in less than 5 minutes

❤️ Delightful experience from Sales Opportunity to Product Fulfillment

“Choose tools that make developing and managing Integrations a joy.”

Monica Wilkinson
Lead Architect

Order-to-cash automation by Slack

Business users become business developers

Microsoft | Inside Track Search content Audience ▾ Topic ▾ Content Suites Videos Blog Careers

How citizen developers modernized Microsoft product launches

Mar 20, 2020 | Serah Delaini

[f](#) [t](#) [in](#) [p](#)

A photograph showing three people in an office setting. On the left, a man with short grey hair wearing a blue jacket is smiling. In the center, a man with glasses and a maroon jacket is also smiling. On the right, a woman with long brown hair wearing a purple and white striped sweater is smiling. They appear to be in a collaborative meeting or discussion.

“... A Business Operations program manager, and her team, were searching for a way to optimize the launch process for the 150 employees who ran product launches across the company.

... Within months, the app would become a widely used internal tool”

A Humble Beginning – Low Code as Extendibility

“With Dynamics, ..., we also launched this very powerful platform, the Power Platform -- ... which acts as the extensibility framework for Microsoft Graph, extensibility framework for Dynamics, as well as Microsoft 365, and embeddable by every SaaS ISV.”

Satya Nadella, Microsoft Build 2018

Shift to Empowerment of Business Users

"Anyone can be a developer, completely transforming how your business operates"

"... we need to empower citizen developers with tools that are low-code/no-code tools so that they can build out these applications In fact, there are already 2.5 million citizen developers using Power Platform ..."

"Once Excel was introduced, a lot of people were able to build spreadsheets and become numerical and analytical ... think about all the white-collar-ish jobs that were created ... we want the same thing to happen with low-code/no-code."

Satya Nadella, Microsoft Ignite 2019

Business Users are Leading The Way

“By 2025, 70% of new applications deployed for the enterprise will use low-code or no-code tools, up from less than 25% in 2020.”

“With Power Platform, we have the leading business process automation and productivity suite for domain experts in every industry, with 20 million monthly active users.”

Satya Nadella, Microsoft Inspire 2022



The Race for a New Excel

Big vendors
have a strong
incentive to
empower
business users



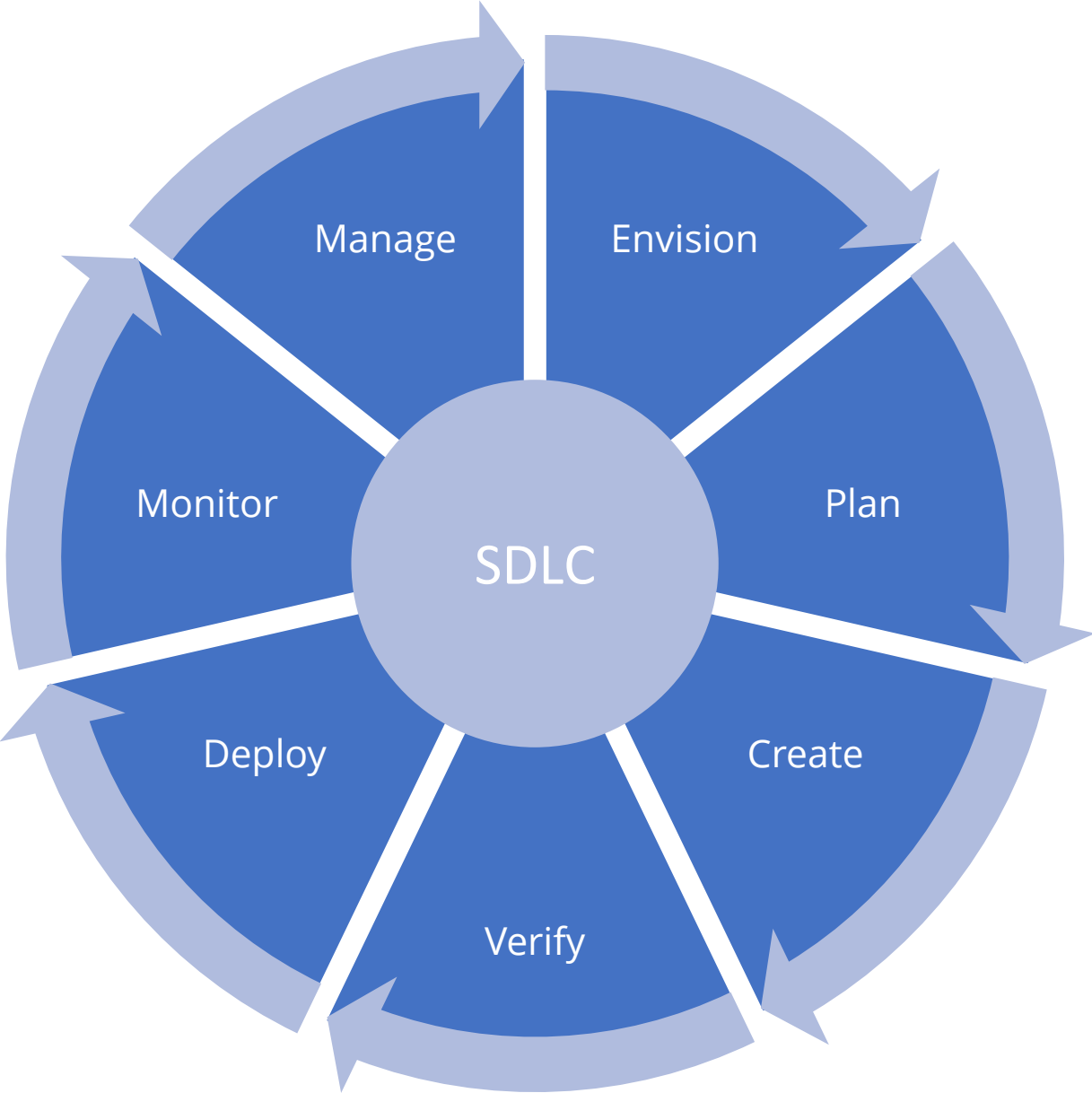
Companies are
lacking IT
resources and
need a
solution for
accelerated
development



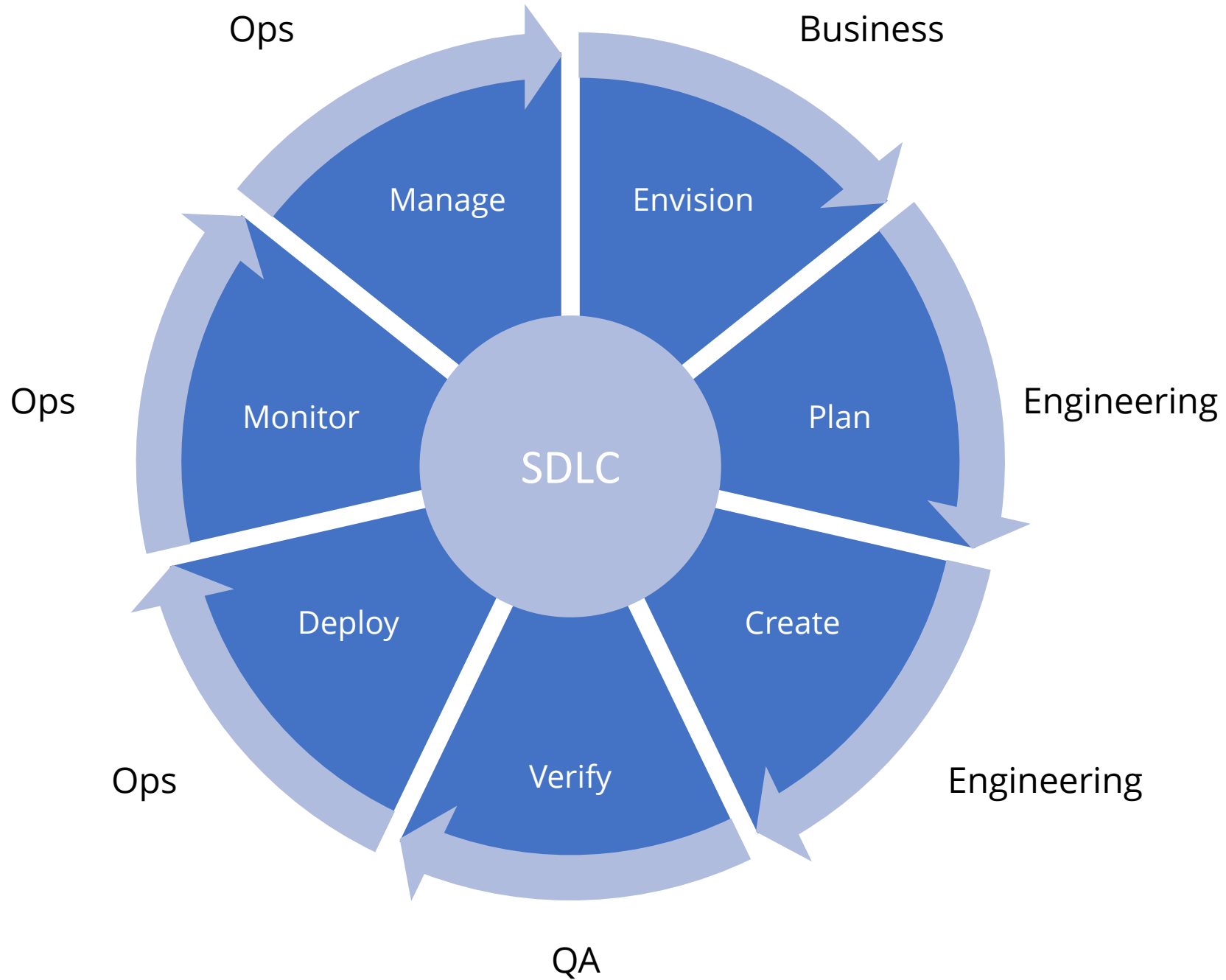
The tech is
already there -
business users
are actually
using it

No Code No SDLC?

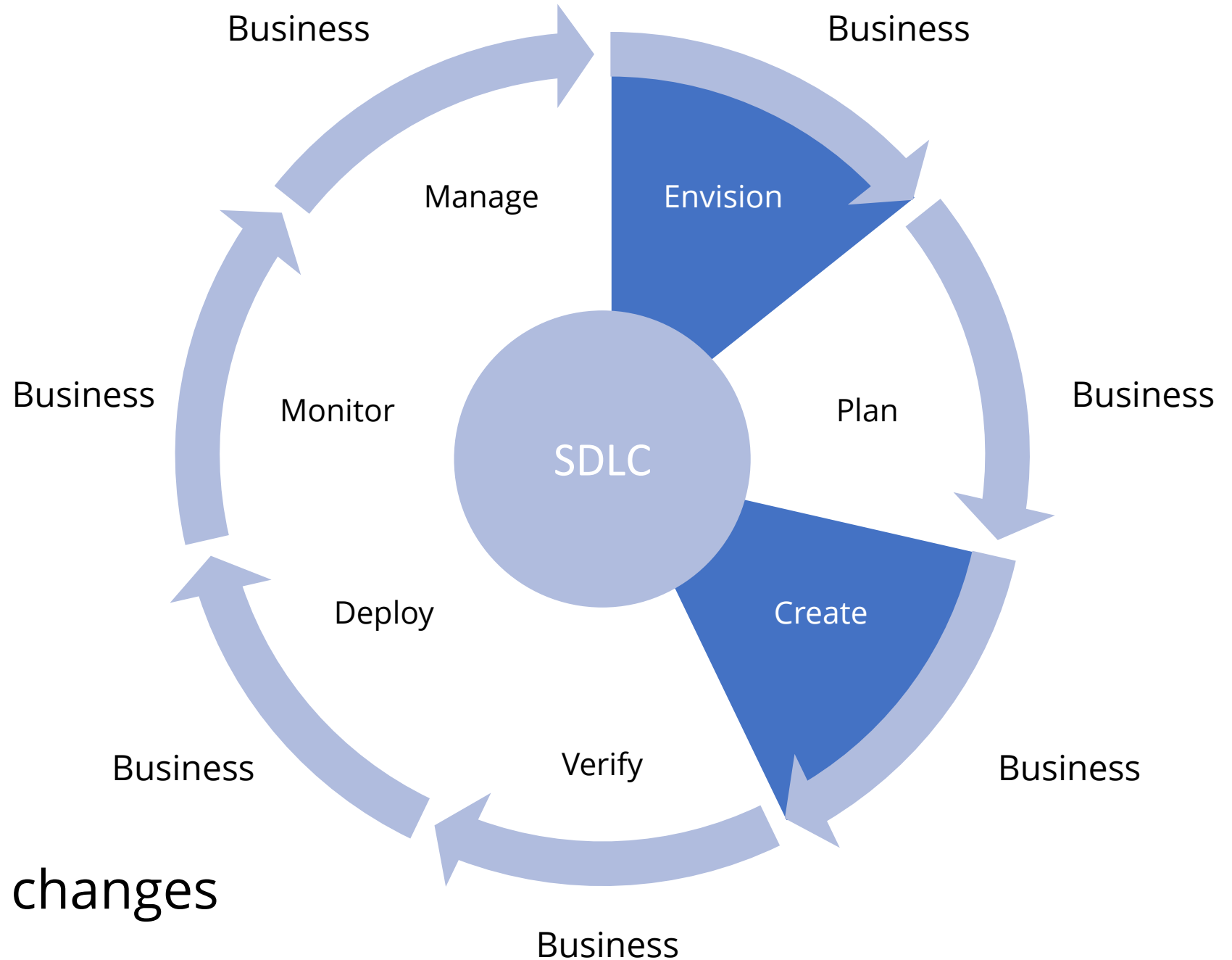
Software Development Lifecycle



Software Development Lifecycle

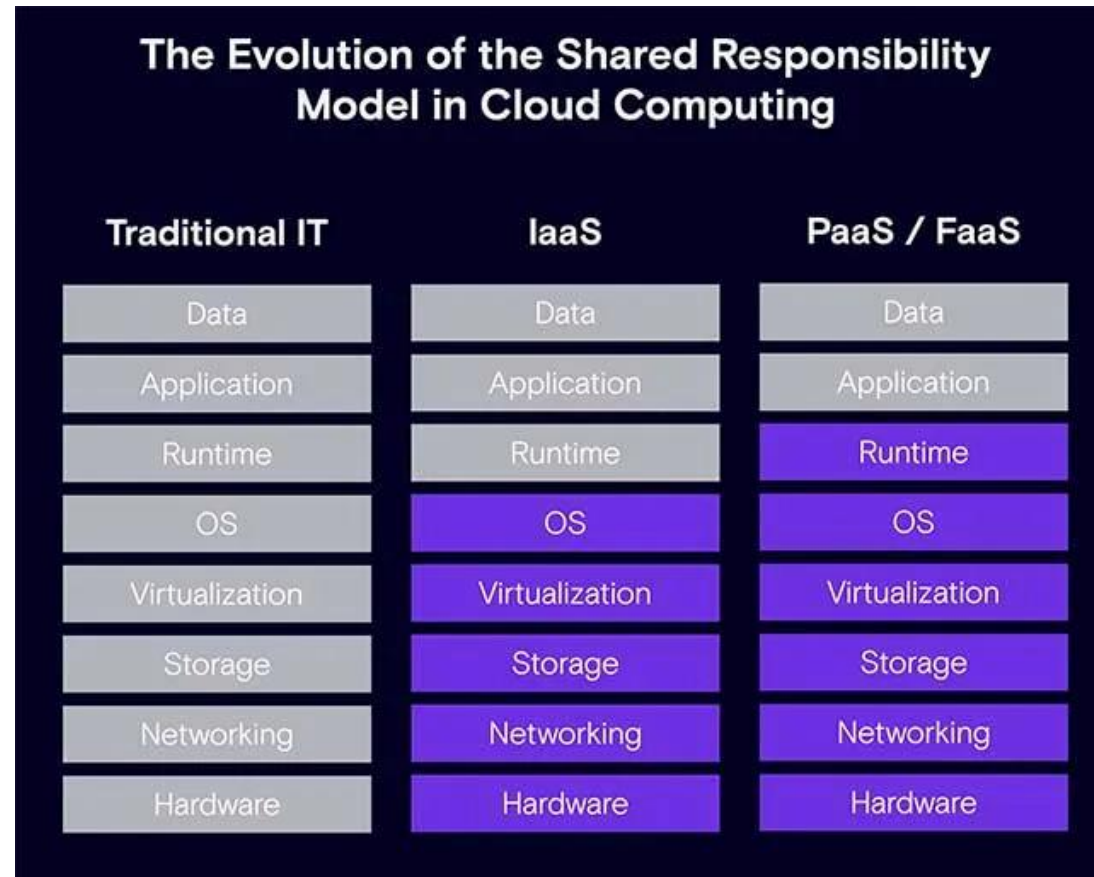


No Code
SDLC?



Hit Save to deploy changes

The Shared Responsibility Model



OWASP Top 10 Low-Code/No-Code Security Risks



OWASP

low-code/no-code

Top 10 Security Risks



<https://owasp.org/www-project-top-10-low-code-no-code-security-risks>

OWASP Top 10 Security Risks for LCNC

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



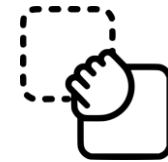
LCNC-SEC-01: Account Impersonation

Low-code/no-code applications can be embedded with user identities which are used implicitly by any application user. This creates a direct path towards Privilege Escalation, allows an attacker to hide behind another user's identity, and circumvents traditional security controls.

Better Customer Care - The Problem

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

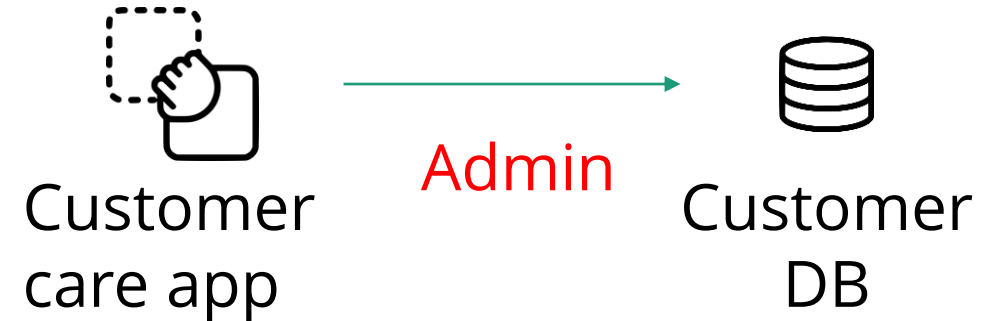


Customer
care app

Better Customer Care - The Solution

Impact:

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



Better Customer Care - The Solution

Impact:

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

- ✓ SOC team panics



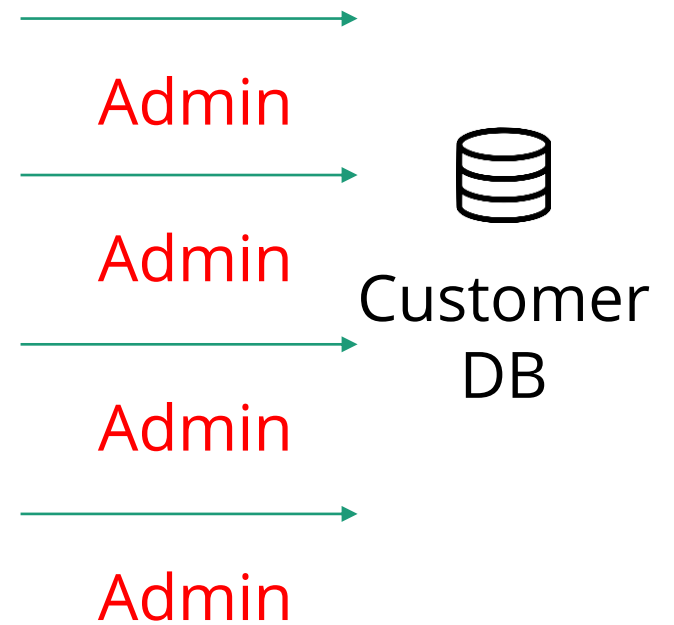
Meanwhile, At the SOC

Abnormal activity detected:

Customer DB is being scraped?

- Lots of queries
- Multiple IPs and hosts
- Spread across time

An investigation shows that all connections use single account. Was it compromised?



Better Customer Care - Summary



LCNC-SEC-02: Authorization Misuse

Service connections are first class objects in most low-code/no-code platforms. This means they can be shared between applications, with other users or with entire organizations.

Credential Sharing as a Service

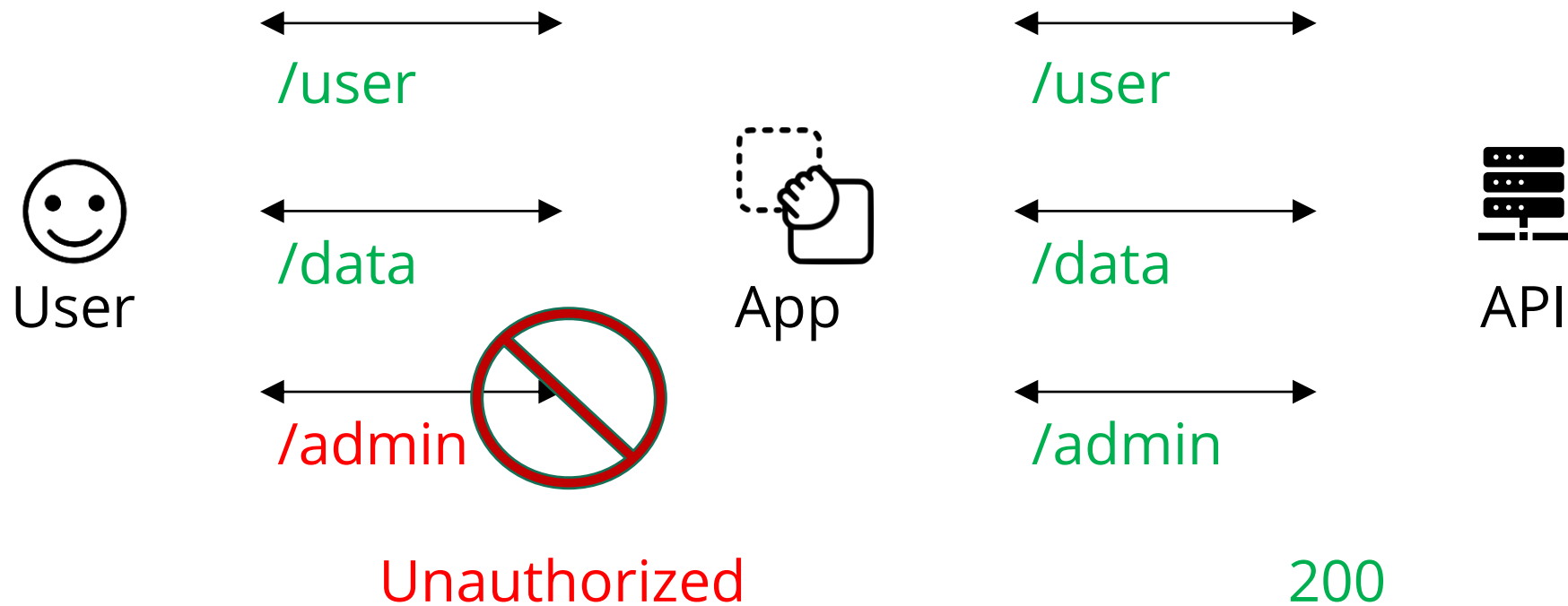
The screenshot displays the Power Automate interface. On the left is a navigation sidebar with options like Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area is titled 'Connections in Zenity Stage (default)' and contains a table of connections. A 'New connection' button is at the top left of this section. Below the table is a 'zapier Apps' panel with categories: My apps, Shared with me, and Custom integrations. On the right, an 'Assets' panel shows a list of connected assets with details like name, status, and creation time. A 'Create connection' button is at the top right of the Assets panel.

Name	Modified
ConnectionToFadiStorageAccount Azure Blob Storage	10 mo ago
[redacted] azure-sql-server.database.wind... SQL Server	8 mo ago
[redacted] stage.com Azure Blob Storage	11 mo ago
[redacted] stage.com Microsoft Dataverse	
Connective eSignatures Connective eSignatures (preview)	
Connective eSignatures Connective eSignatures (preview)	
23 DB2	
File System File System	
Notifications Notifications	
Vendor Server FTP	
FTP FTP	
[redacted] oa2g@gmail.com Gmail	1 wk ago

Asset Name	Status	Created	Recipes
[redacted] Management	Connected	May 22 at 1:47 am	4
dev_HTTP account [redacted]	Connected	Feb 6 at 1:21 am	0
dev_HTTP account [redacted]	Connected	Feb 6 at 1:21 am	0
dev_twitter [redacted]	Connected	Feb 10 at 1:40 am	1
FTP at test.rebex.net [redacted]	Connected	Apr 9, 2021, at 7:05 am	932
[redacted]@gmail.com gmail [redacted]	Connected	Apr 9, 2021, at 5:05 am	1

App Reader <> API Admin

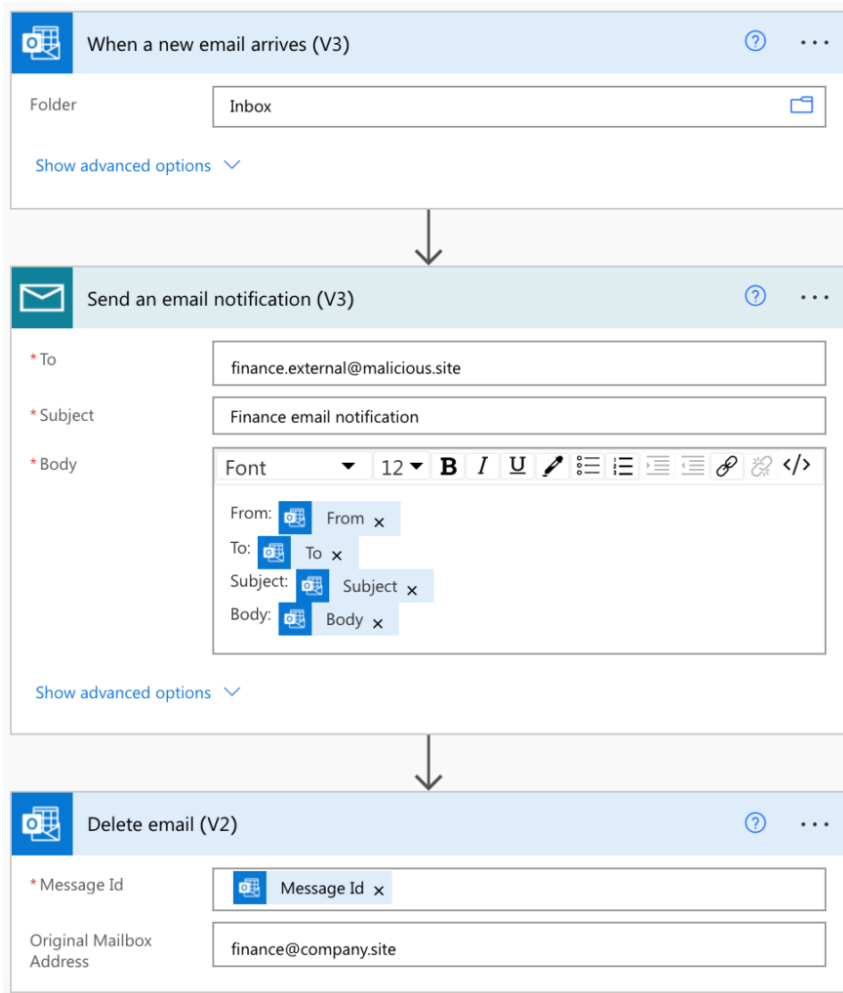
Authorization as front-end logic



LCNC-SEC-03: Data Leakage and Unexpected Consequences

Low-code/no-code applications often sync data or trigger operations across multiple systems, which creates a path for data to find its way outside the organizational boundary. This means that operations in one system can have unexpected consequences in another.

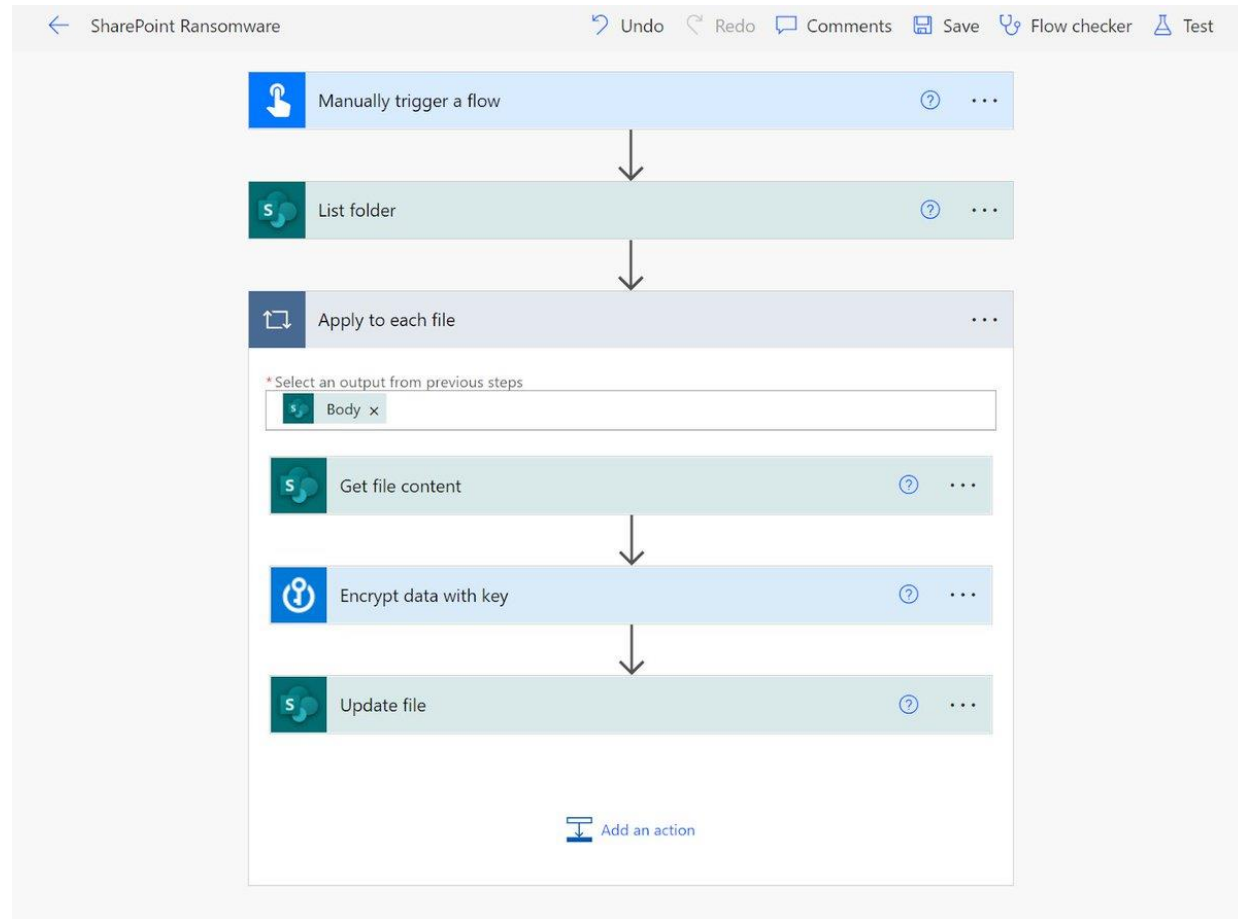
LCNC-SEC-03: Data Leakage and Unexpected Consequences



Data is being copied between two separate services using two separate identities – existing defense mechanisms fail

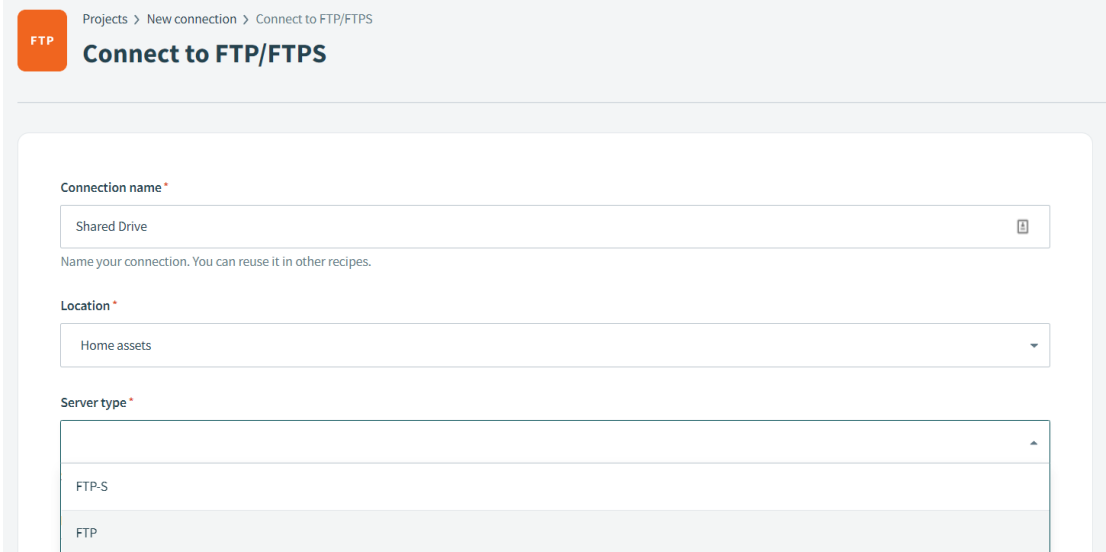
LCNC-SEC-03: Data Leakage and Unexpected Consequences

If <file found>
Then <encrypt
file>



LCNC-SEC-04: Authentication and Secure Communication Failures

Low-code/no-code applications typically connect to business-critical data via connections set up by business users, which can often result in insecure communication.



The screenshot shows a web interface for configuring an FTP connection. The breadcrumb trail is 'Projects > New connection > Connect to FTP/FTPS'. The main heading is 'Connect to FTP/FTPS'. The form contains three sections: 'Connection name' with a text input field containing 'Shared Drive' and a help icon; 'Location' with a dropdown menu showing 'Home assets'; and 'Server type' with a dropdown menu showing 'FTP-S' and 'FTP' (the latter is highlighted).

Projects > New connection > Connect to FTP/FTPS

FTP Connect to FTP/FTPS

Connection name *

Shared Drive

Name your connection. You can reuse it in other recipes.

Location *

Home assets

Server type *

FTP-S

FTP

LCNC-SEC-05: Security Misconfiguration

Misconfigurations can often result in anonymous user access to sensitive data or operations, unprotected public endpoints, unprotected secrets and oversharing.

LCNC-SEC-05: Security Misconfiguration



CYBER SECURITY NEWS · 6 MIN READ

**Microsoft Power Apps Data Leak Fallout:
38 Million Records Exposed, State and
City Governments Among Those
Breached**

SCOTT IKEDA · AUGUST 27, 2021

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



UpGuard Team

Published Aug 23, 2021

Anonymous API Access

“An open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way.”

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

[*portal.powerappsportals.com/_odata*](portal.powerappsportals.com/_odata)

Anonymous API Access

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

portal.powerappsportals.com/_odata

```
▼<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xml:base=  
  ▼<workspace>  
    <atom:title type="text">Default</atom:title>  
    ▼<collection href="EntityFormSet">  
      <atom:title type="text">EntityFormSet</atom:title>  
    </collection>  
    ▼<collection href="globalvariables">  
      <atom:title type="text">globalvariables</atom:title>  
    </collection>  
  </workspace>  
</service>
```

Nothing to see here

/_odata/globalvariables:

```
"scs_globalvariablesid":"24[REDACTED]","scs_name":"Documents  
API Auth Token","scs_values":"Bearer  
eyJ0eXAi[REDACTED]
```

```
[REDACTED]","scs_purpose":"This variable stores OAuth Token to access Azure  
API.,"createdon":"20[REDACTED]T18:03:39Z","list-id":"68[REDACTED]ba",  
"view-id":"bc9c3[REDACTED]b9c","entity-permissions-enabled":"true"
```

LCNC-SEC-06: Injection Handling Failures

Low-code/no-code applications ingest user provided data in multiple ways, including direct input or retrieving user provided content from various services. Such data can contain malicious payloads that may introduce risk to the application.



LCNC-SEC-07: Vulnerable, Unmanaged and Untrusted Components

Low-code/no-code applications rely heavily on ready-made components out of the marketplace, the web or custom connectors built by developers. These components are often unmanaged, lack visibility and expose applications to supply chain-based risks.



LCNC-SEC-08: Data and Secret Handling Failures

Low-code/no-code applications often store data or secrets as part of their "code" or on managed databases offered by the platform, which needs to be properly stored in compliance with regulation and security requirements.

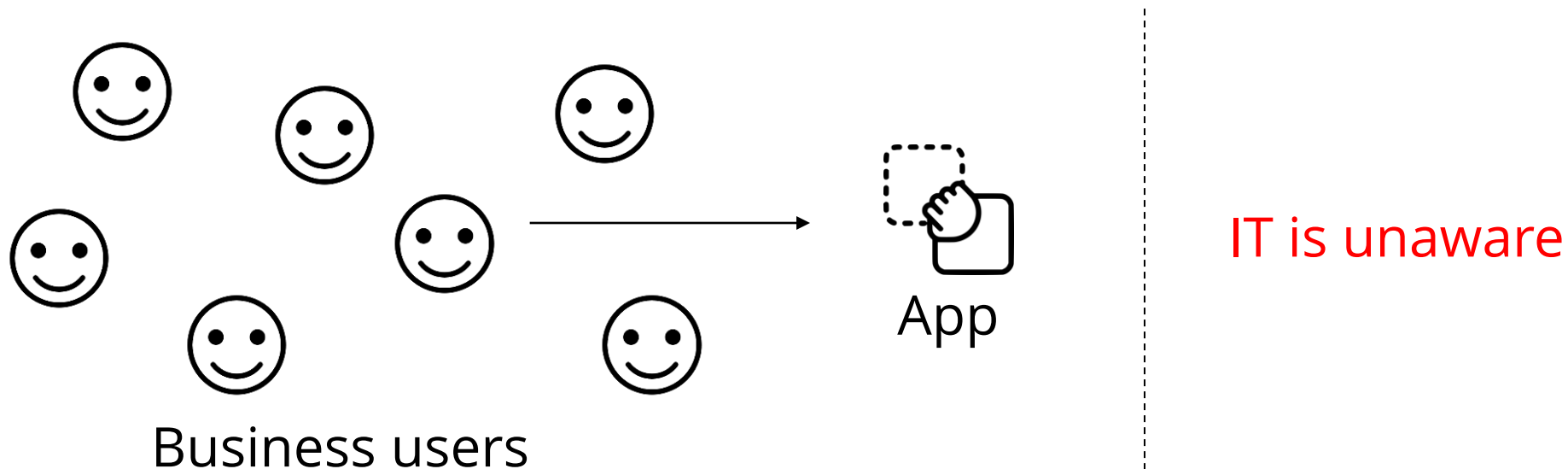


Give-Aware Campaign

- HR team at a large IT company kicked off a Giveaway campaign
- App let's you choose your donation, charity and plug in your credit card
- Cards are stored in plaintext on an environment available to everyone, including tenant guests
- Compliance audit

LCNC-SEC-09: Asset Management Failures

Low-code/no-code applications are easy to create and have relatively low maintenance costs, which makes them prone to abandonment, while still remaining active. Furthermore, internal applications can gain popularity rapidly, without addressing business continuity concerns.



LCNC-SEC-10: Security Logging and Monitoring Failures

Low-code/no-code applications often lack a comprehensive audit trail, produce none or insufficient logs, and fail to scrub sensitive data from logs.

The screenshot displays a workflow configuration and its execution history. The workflow is triggered 'When a new email arrives' and is currently active (0s). The configuration shows an input field for 'Label' set to 'INBOX'. The output fields show the email details: 'From: admin@zentoso.com', 'Sender's Name: Zentoso', and 'To: kris@zenitystage.com'. The email body is visible, showing 'Password reset instructions' and a snippet of HTML code: '<title> Password reset instructions </title>' and '<style id="mediaqueries">@media only screen and (max-width:'. The execution history table shows 12 successful runs over a 28-day period.

Start	Duration	Status
Jun 11, 12:26 PM (2 d ago)	28 ms	Succeeded
Jun 8, 05:13 PM (4 d ago)	31 ms	Succeeded
Jun 6, 10:31 AM (1 wk ago)	46 ms	Succeeded
Jun 2, 06:15 PM (1 wk ago)	45 ms	Succeeded
May 30, 10:58 AM (2 wk ago)	50 ms	Succeeded
May 28, 03:07 PM (2 wk ago)	59 ms	Succeeded
May 28, 03:06 PM (2 wk ago)	17 ms	Succeeded
May 27, 10:16 AM (2 wk ago)	41 ms	Succeeded
May 27, 01:01 AM (2 wk ago)	11 ms	Succeeded
May 26, 06:24 PM (2 wk ago)	35 ms	Succeeded

Summary



What have we seen

- Low Code / No Code is growing rapidly
 - Probably already in your org
 - Shift focus to business users
- Missing SDLC
- OWASP Top 10 LCNC Security Risks
 - Get involved
 - Learn more

Opportunities - Champion Low Code / No Code AppSec in your org

- Create a Low Code / No Code Security Framework
- No Code SDLC
- Approved user cases
- Guide business users
- Join OWASP Top 10 LCNC Security Risks
- Reach out to be @mbrg0

No Code No Risk? What Happens When We Leave No Code up for Grabs

Michael Bargury @ Zenity