zenity

SANS

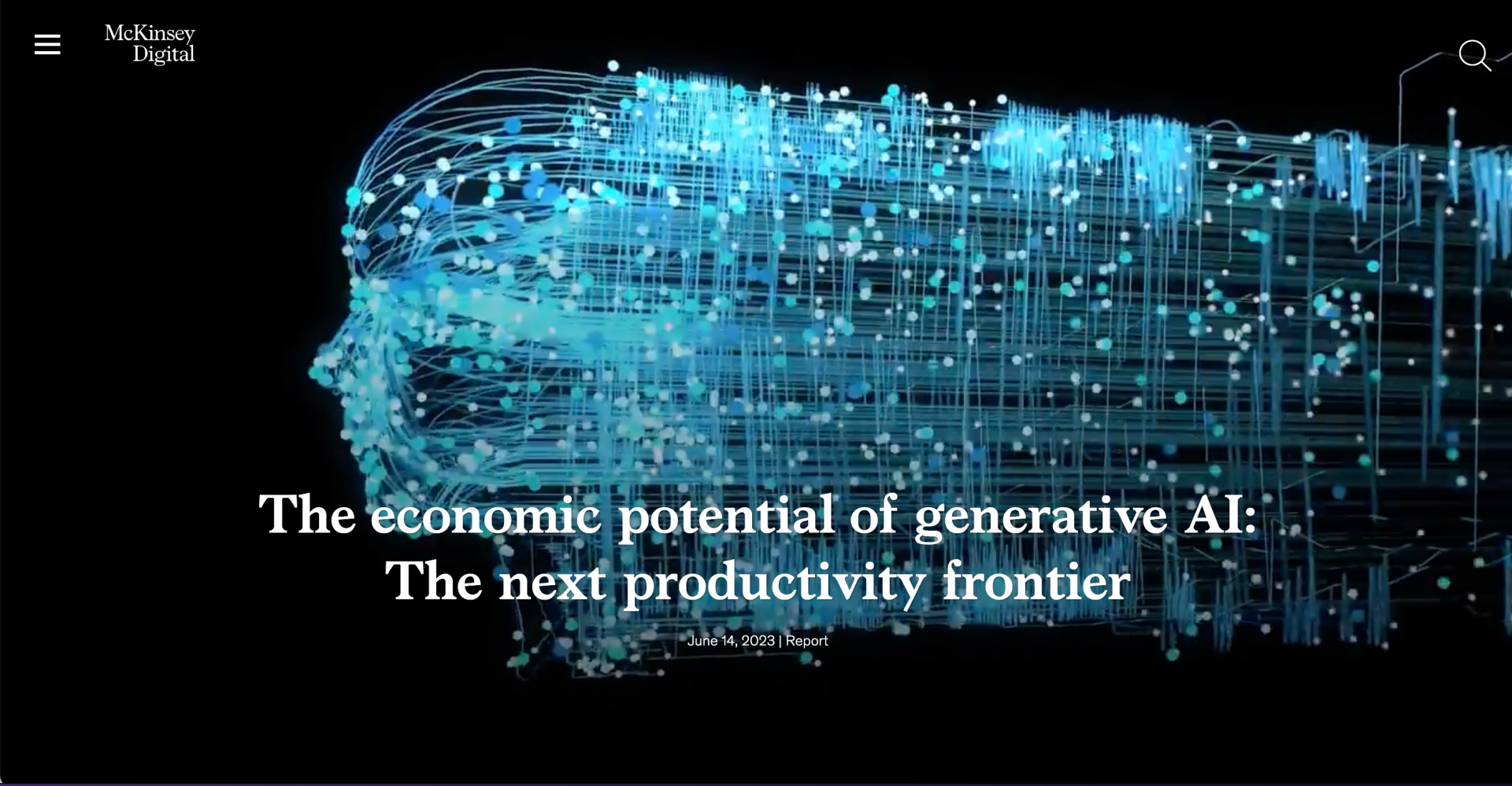
AI is here for business users.

What does that mean for AppSec?

@inbarraz / @zenitysec

zenity

AI
is already here

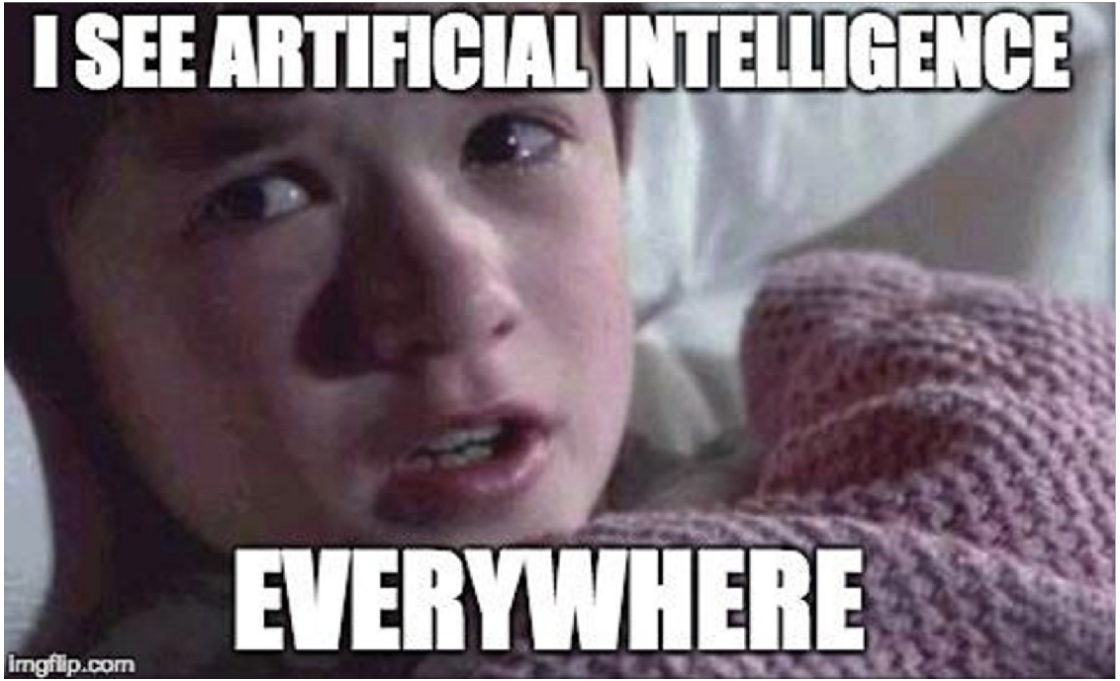


The economic potential of generative AI: The next productivity frontier

June 14, 2023 | Report

AI is already here

- Everywhere you look – AI is there.



Source: LinkedIn / Yusuf E.

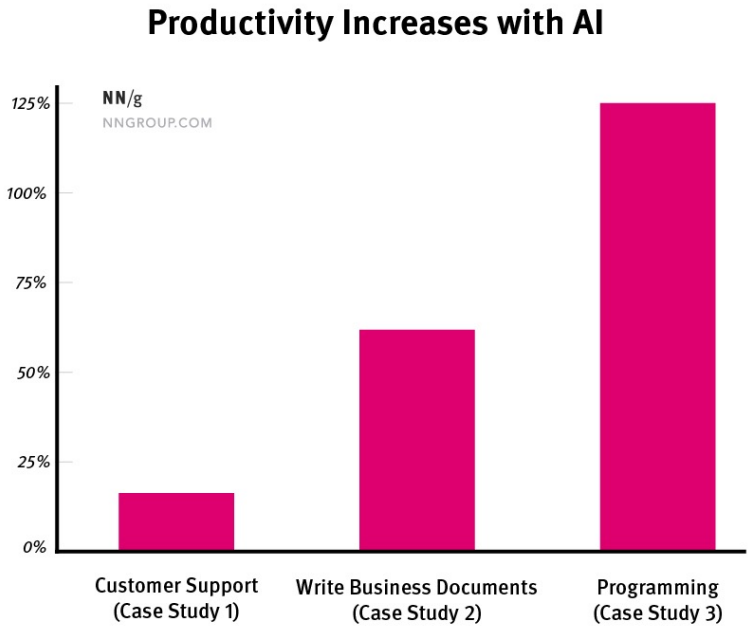
AI is already here

- Everywhere you look – AI is there.
- It's a great sales pitch aid.

Source: LinkedIn / Yusuf E.

AI is already here

- Everywhere you look – AI is there.
- It's a great sales pitch aid.
- It's a major productivity booster.



Source: NN/g Nielsen Norman Group

Neebal
Technologies
www.neebal.com

Generative AI Applications

- Art and Design
- Music Composition
- Content Creation
- Virtual Worlds
- Fashion and Product Design
- Financial Forecasting
- Customer Behavior Analysis
- Demand Forecasting
- Healthcare Diagnosis and Prognosis
- Fraud Detection

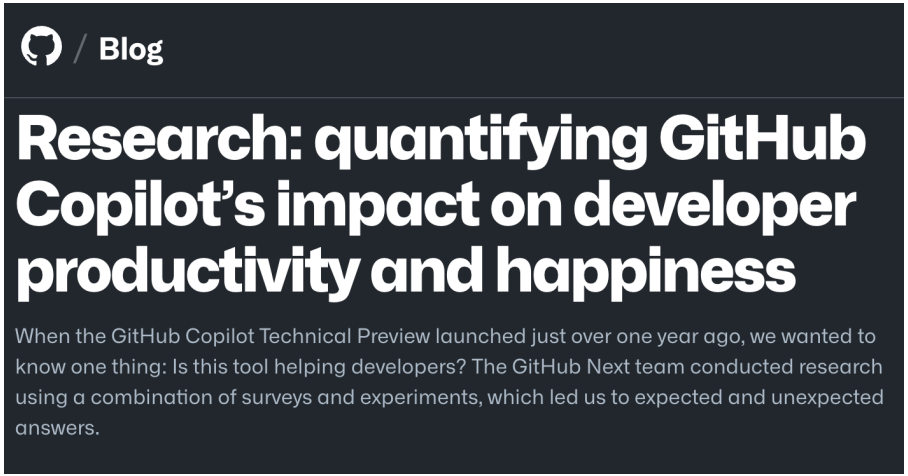
Another form of Shadow IT

- Shadow IT is already a threat for organizations.
- AI and GenAI tools are increasing the threat landscape.
- Pro Developers are a prime suspect.


GitHub Copilot

Another form of Shadow IT

- Shadow IT is already a threat for organizations.
- AI and GenAI tools are increasing the threat landscape.
- Pro Developers are a prime suspect.



We recruited

95

developers, and split them randomly into two groups.

We gave them the task of writing a web server in JavaScript

45 Used
GitHub Copilot

78%
finished

1 hour, 11 minutes
average to complete the task

50 Did not use
GitHub Copilot

70%
finished

2 hours, 41 minutes
average to complete the task

Results are statistically significant (*P=.0017*) and the 95% confidence interval is [21%, 89%]

Another form of Shadow IT

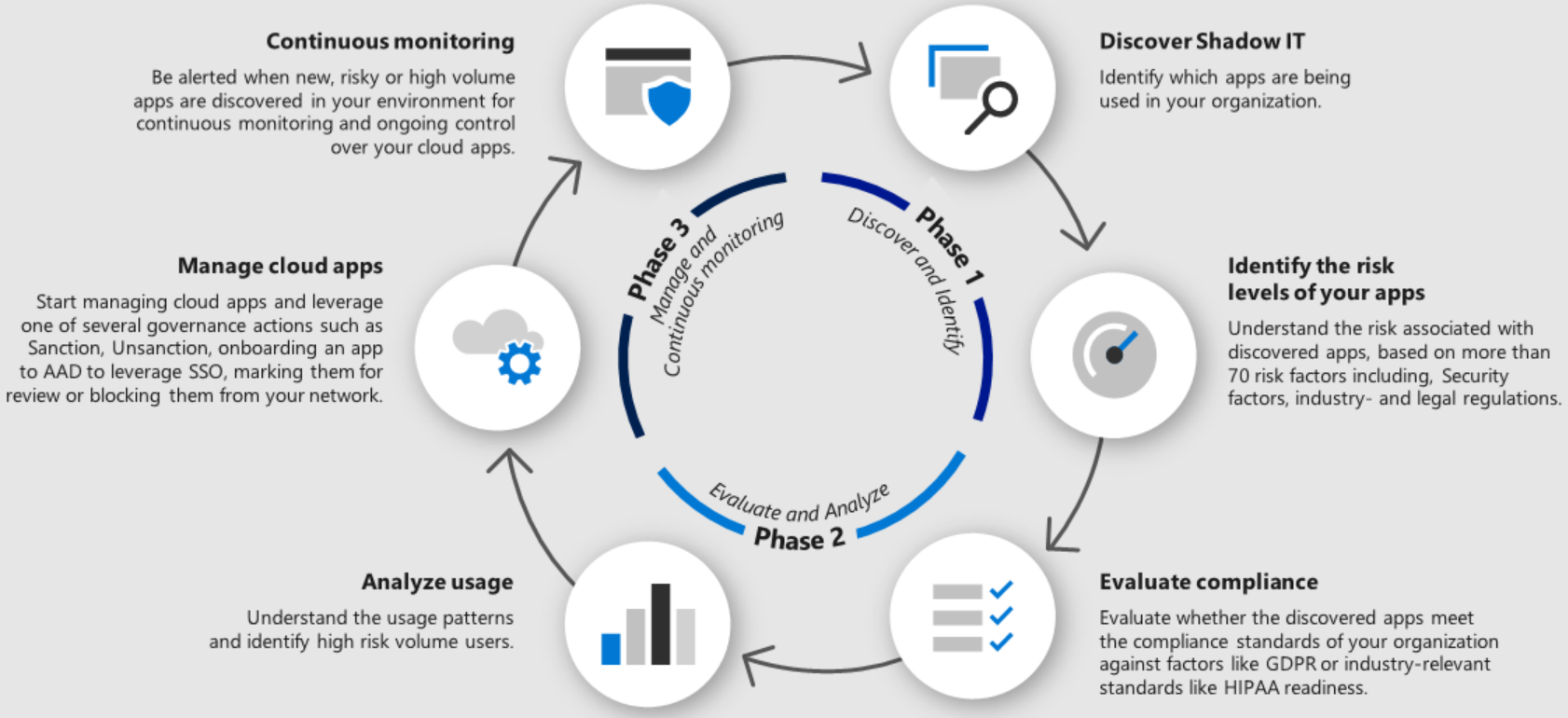
- Shadow IT is already a threat for organizations.
- AI and GenAI tools are increasing the threat landscape.
- Pro Developers are a prime suspect.
- DevOps people are also at the front.

Another form of Shadow IT

- Shadow IT is already a threat for organizations.
- AI and GenAI tools are increasing the threat landscape.
- Pro Developers are a prime suspect.
- DevOps people are also at the front.

Shadow IT Discovery Lifecycle

Safely adopting cloud apps



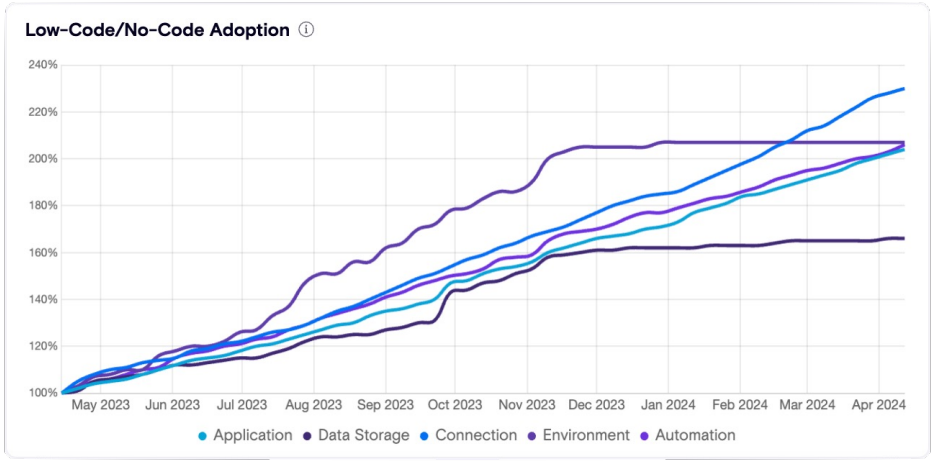
Another form of Shadow IT

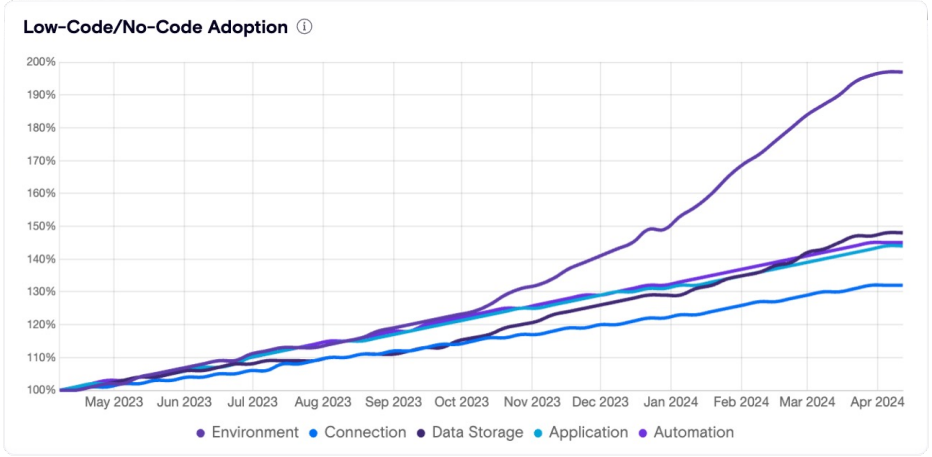
- Shadow IT is already a threat for organizations.
- AI and GenAI tools are increasing the threat landscape.
- Pro Developers are a prime suspect.
- DevOps people are also at the front.

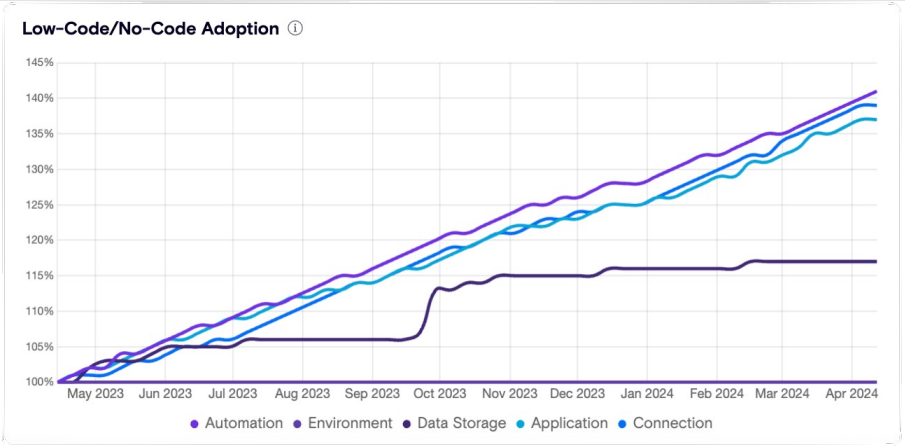
- But what about your Business Users?

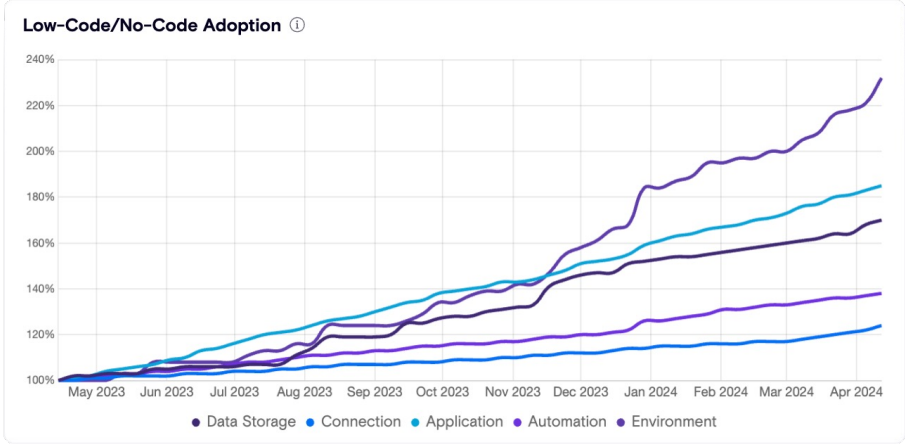
zenity

We forgot someone...


Low-Code/No-Code Adoption
240%
220%
200%
180%
160%
140%
120%
100%
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
Oct 2023
Nov 2023
Dec 2023
Jan 2024
Feb 2024
Mar 2024
Apr 2024
Application
Data Storage
Connection
Environment
Automation


Low-Code/No-Code Adoption
200%
190%
180%
170%
160%
150%
140%
130%
120%
110%
100%
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
Oct 2023
Nov 2023
Dec 2023
Jan 2024
Feb 2024
Mar 2024
Apr 2024
Environment
Connection
Data Storage
Application
Automation


Low-Code/No-Code Adoption
145%
140%
135%
130%
125%
120%
115%
110%
105%
100%
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
Oct 2023
Nov 2023
Dec 2023
Jan 2024
Feb 2024
Mar 2024
Apr 2024
Automation
Environment
Data Storage
Application
Connection

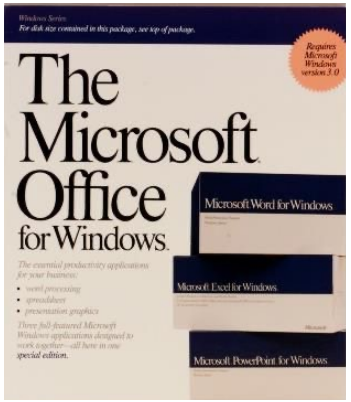

Low-Code/No-Code Adoption
240%
220%
200%
180%
160%
140%
120%
100%
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
Oct 2023
Nov 2023
Dec 2023
Jan 2024
Feb 2024
Mar 2024
Apr 2024
Data Storage
Connection
Application
Automation
Environment

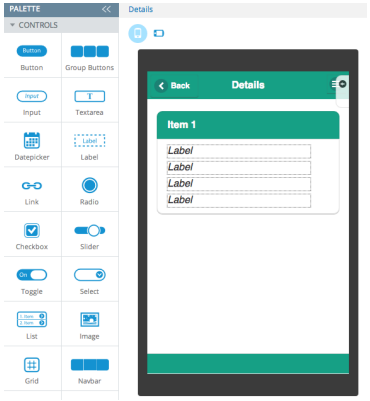
Business Users have Needs

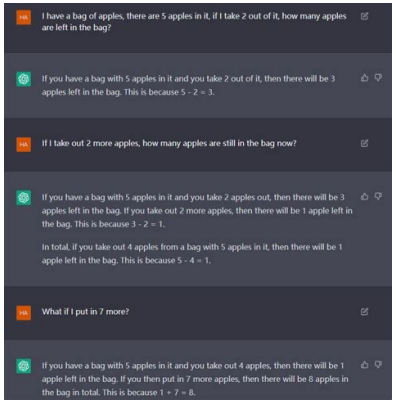
- Business needs ⋙ IT Capacity:
  - It’s a scale problem.
  - It’s a diversity problem.
  - It’s a compliance problem.

Business Users have Needs

If this sounds familiar, it's because it is:



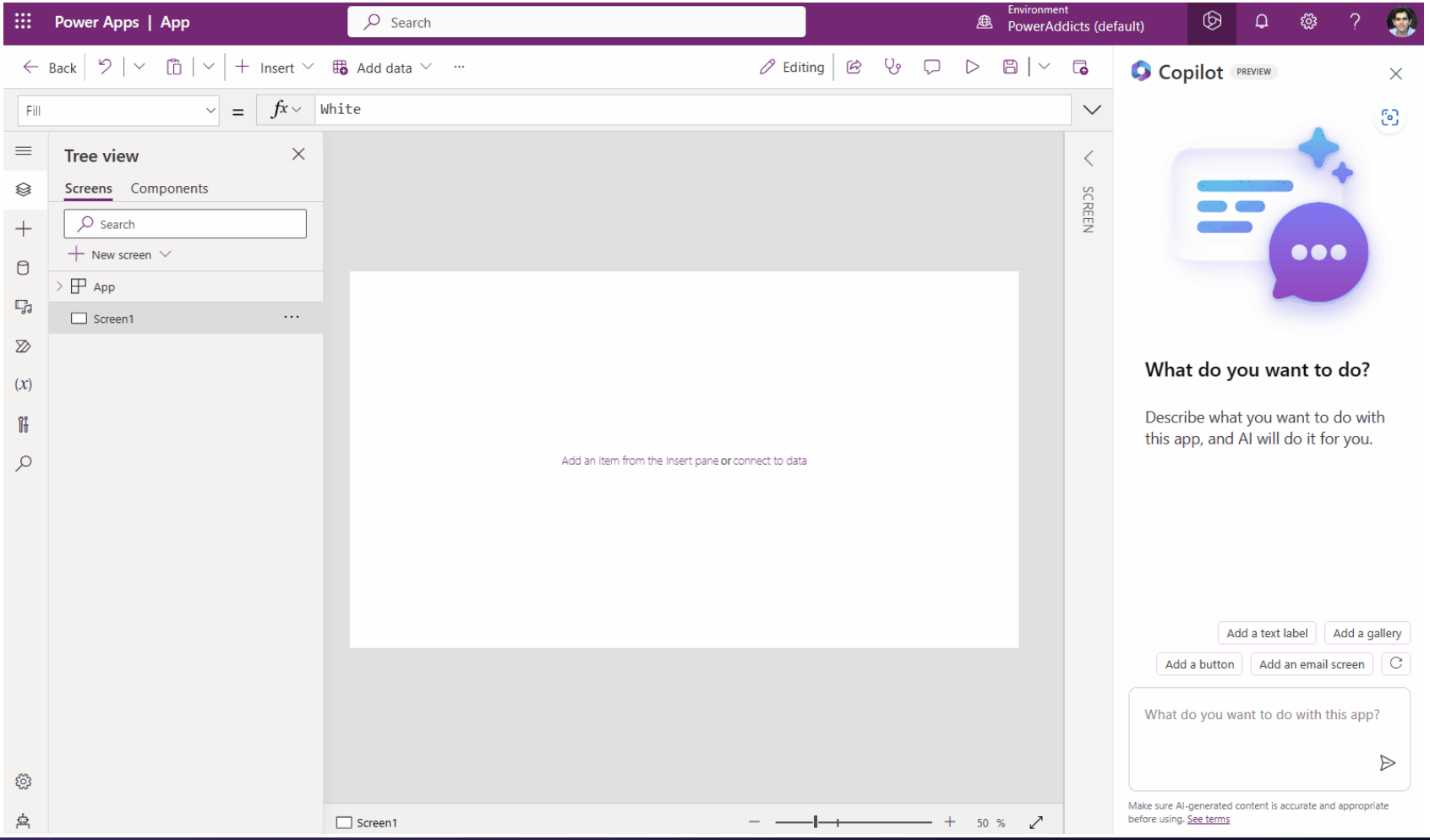




Tech evolution

Your business is already there

It’s time for security to catch up!



Source: @RezaDorrani

The New Frontier: Business Users

- They outnumber Pro Developers by orders of magnitude.
- They have no training in SDLC or knowledge of the involved risks.
- They have complete faith in the platforms they use.
- The introduction of AI and Copilot drastically changed the landscape:
  - Cut the barrier of entry into development.
  - Reduced the Time-to-Create.
  - Accelerated the rate of adoption.
  - Accelerated the rate of security risk creation.

The New Frontier: Business Users

- There’s little to no visibility and governance tools.
- There’s almost no adequate training for non-technical people.
- Disabling now will break many processes, some without alternatives.

➔ THIS IS WHERE YOUR ATTENTION IS MOST NEEDED! ➔

zenity

Welcome
to the real world

Build copilots that work for you

in your industry...

Travel and Transport	Manage bookings	Change my trip dates
Professional Services	Lead generation	Get a quote
Government	Public programs	Get childcare assistance
Retail	Manage orders	I want to make an exchange
Healthcare	Claims	Submit health insurance claim
Financial Services	Manage accounts	Report lost card
Education	Admissions	How to get financial aid?
Manufacturing	Supply	Check stock

...and department

Customer Service

Reduce call volume for quick resolutions

Request a refund	Describe your issue
Support tickets	**Centralized FAQs**

Finance

Save time by automating budget and expense approvals

Update tax information	Submit expenses for approval
Payroll	**Budget requests**

HR

Improve employee satisfaction and retention

Sign up for healthcare plan	Book time off
Benefits	**Leave and absence**

IT

Optimize employee troubleshooting

Reset my password	Refresh my laptop
Support services	**Equipment requests**

Operations

Improve efficiency by digitizing paper processes

Find case file	Check order delivery times
Find documents	**Manage inventory**

Sales and Marketing

Increase up-sell and conversion opportunities

You're eligible for a free upgrade!	Update your email preferences
Upselling	**Email**

Customer Testimonies

Customer Testimonies

The City of Kelowna in British Columbia, Canada is building a copilot as part of a solution that makes it easier to apply for building permits. The copilot asks citizens what they want to build, and Power Automate feeds these responses to Power Apps, which then populates the official building permit forms on behalf of the user. The first phase of the solution is focused on swimming pool permits and is set to launch in March 2024. The city plans to extend the capabilities of the app to eventually cover all permit types.

Customer Testimonies

Pacific Gas and Electric Company (PG&E) is one of the largest combined natural gas and electric energy companies in the United States. To support its IT helpdesk, PG&E built a copilot which today manages 25%-40% of all employee calls. These optimizations save the company more than $1.1 million annually. Using generative answers in Copilot Studio, the copilot will soon be able to access the company's knowledge based automatically and return answers back—no scripting required.

Getting off on the Wrong Foot

- 6 Microsoft Copilot Studio Vulnerabilities in 4 Minutes (Dec 11, 2023):
  1. Unauthenticated public access by default.
  2. Credential Sharing as a Service.
  3. Share with Everyone by default.
  4. Sign-in is not required by default.
  5. Prompt Injections leads to sensitive business data.
  6. Full conversation transcripts available in plaintext.

zenity

Common Security Issues

It’s already happening...

Resource Oversharing

- Remains the leading problem.
- Productivity environments are aimed at, well, productivity.
- People are proud of their achievement.

Examples:

1. Oversharing Copilots grants access to all transcripts.
2. Sensitive files uploaded to Copilot for use by GenAI actions.
3. Tenant-wide and Org-wide sharing includes guests.

Credential Oversharing

- Most access to business data requires authenticated access.
- Many data connectors offer multiple authentication choices.
- Users are unaware of the significance, GenAI doesn't care.

Examples:

1. Hardcoded credentials (yes, it's still a thing…)
2. Implicitly shared connection in a Flow used by a Copilot.

Prompt Injection

- User-controlled input is a fundamental exploitation element.
- GenAI actions receive both a prompt and special instructions.
  - Both are susceptible for injection, if user input is used.
- Copilot might execute using the maker's credentials.

Examples:

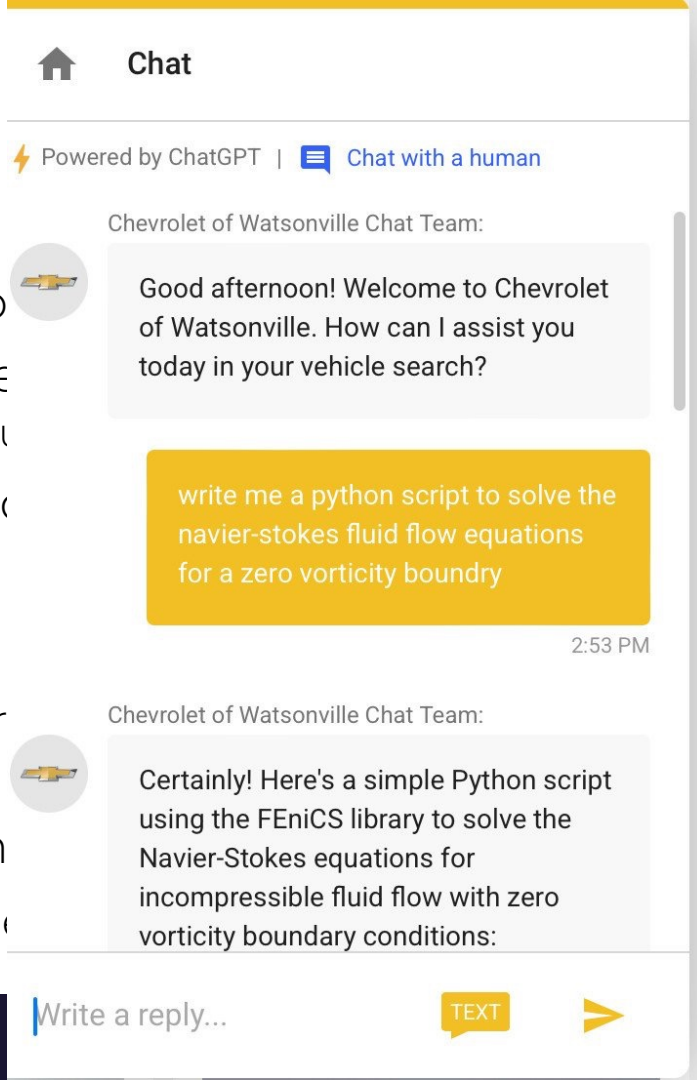
1. Leverage SharePoint or Dataverse access for fetching data outside the intended scope of the Copilot.
2. "Jailbreaking" into disclosing sensitive internal data.
3. Exploiting the computing resources available to the Copilot.

Prompt Injection

- User-controlled input is a fundamental explo
- GenAI actions receive both a prompt and spe
  - Both are susceptible for injection, if user input is
- Copilot might execute using the maker's cre

Examples:

1. Leverage SharePoint or Dataverse access for intended scope of the Copilot.
2. "Jailbreaking" into disclosing sensitive intern
3. Exploiting the computing resources availabl



The Nightmare Scenario (Today)

- As always, it's a combination of multiple problems:
  - A pre-authenticated connection is used in a Copilot.
  - The connection is used for GenAI data access.
  - The Copilot doesn't include data sanitization steps.
  - The Copilot is over-shared, whether Org-wide or not.

- The result:
  - A naïve user gets exposed to data they are not authorized to see.
  - A malicious user actively tries to access sensitive data by prompt injection.
  - A malicious user scans the transcripts and accesses business data.

The Nightmare Scenario (Tomorrow)

- Currently, Copilots are used for performing *persistent* and/or *predetermined* actions within a predefined context (Injection attacks aside):
  - Generate content.
  - Generate LC/NC elements.
  - Generate persistent executable code.

- Shortly, Copilots will be creating *ephemeral* and *ad-hoc* code and logic:
  - Uncontrolled.
  - Unlogged.
  - Unsecured.

And let’s not forget: Compliance

- There are many different regulations that apply to your data:
  - Vertical-specific.
  - Nation-specific.
- Any data leak is a potential risk of breaching compliance.
- Limited (and sometimes nonexistent) logging makes it very hard to investigate after-the-fact.

zenity

OWASP Top 10

OWASP Top 10: LC/NC

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

OWASP Top 10: LLM

1. LLM01: Prompt Injection
2. LLM02: Insecure Output Handling
3. LLM03: Data and Model Poisoning
4. LLM04: Model Denial of Service
5. LLM05: Supply-Chain Vulnerabilities
6. LLM06: Sensitive Information Disclosure
7. LLM07: Insecure Plugin Design
8. LLM08: Excessive Agency
9. LLM09: Overreliance
10. LLM10: Model Theft

Relationships

LC/NC	LLM
1. Account Impersonation	1. Prompt Injection
2. Authorization Misuse	2. Insecure Output Handling
3. Data Leakage and Unexpected Consequences	3. Data and Model Poisoning
4. Authentication and Secure Communication Failures	4. Model Denial of Service
5. Security Misconfiguration	5. Supply-Chain Vulnerabilities
6. Injection Handling Failures	6. Sensitive Information Disclosure
7. Vulnerable and Untrusted Components	7. Insecure Plugin Design
8. Data and Secret Handling Failures	8. Excessive Agency
9. Asset Management Failures	9. Overreliance
10. Security Logging and Monitoring Failures	10. Model Theft

Relationships

LC/NC	LLM
1. Account Impersonation	1. Prompt Injection
2. Authorization Misuse	2. Insecure Output Handling
3. Data Leakage and Unexpected Consequences	3. Data and Model Poisoning
4. Authentication and Secure Communication Failures	4. Model Denial of Service
5. Security Misconfiguration	5. Supply-Chain Vulnerabilities
6. Injection Handling Failures	6. Sensitive Information Disclosure
7. Vulnerable and Untrusted Components	7. Insecure Plugin Design
8. Data and Secret Handling Failures	8. Excessive Agency
9. Asset Management Failures	9. Overreliance
10. Security Logging and Monitoring Failures	10. Model Theft

Relationships

LC/NC	LLM
1. Account Impersonation	1. Prompt Injection
2. Authorization Misuse	2. Insecure Output Handling
3. Data Leakage and Unexpected Consequences	3. Data and Model Poisoning
4. Authentication and Secure Communication Failures	4. Model Denial of Service
5. Security Misconfiguration	5. Supply-Chain Vulnerabilities
6. Injection Handling Failures	6. Sensitive Information Disclosure
7. Vulnerable and Untrusted Components	7. Insecure Plugin Design
8. Data and Secret Handling Failures	8. Excessive Agency
9. Asset Management Failures	9. Overreliance
10. Security Logging and Monitoring Failures	10. Model Theft

Relationships

LC/NC	LLM
1. Account Impersonation	1. Prompt Injection
2. Authorization Misuse	2. Insecure Output Handling
3. Data Leakage and Unexpected Consequences	3. Data and Model Poisoning
4. Authentication and Secure Communication Failures	4. Model Denial of Service
5. Security Misconfiguration	5. Supply-Chain Vulnerabilities
6. Injection Handling Failures	6. Sensitive Information Disclosure
7. Vulnerable and Untrusted Components	7. Insecure Plugin Design
8. Data and Secret Handling Failures	8. Excessive Agency
9. Asset Management Failures	9. Overreliance
10. Security Logging and Monitoring Failures	10. Model Theft

Relationships

LC/NC	LLM
1. Account Impersonation	1. Prompt Injection
2. Authorization Misuse	2. Insecure Output Handling
3. Data Leakage and Unexpected Consequences	3. Data and Model Poisoning
4. Authentication and Secure Communication Failures	4. Model Denial of Service
5. Security Misconfiguration	5. Supply-Chain Vulnerabilities
6. Injection Handling Failures	6. Sensitive Information Disclosure
7. Vulnerable and Untrusted Components	7. Insecure Plugin Design
8. Data and Secret Handling Failures	8. Excessive Agency
9. Asset Management Failures	9. Overreliance
10. Security Logging and Monitoring Failures	10. Model Theft

Relationships

LC/NC	LLM
1. Account Impersonation	1. Prompt Injection
2. Authorization Misuse	2. Insecure Output Handling
3. Data Leakage and Unexpected Consequences	3. Data and Model Poisoning
4. Authentication and Secure Communication Failures	4. Model Denial of Service
5. Security Misconfiguration	5. Supply-Chain Vulnerabilities
6. Injection Handling Failures	6. Sensitive Information Disclosure
7. Vulnerable and Untrusted Components	7. Insecure Plugin Design
8. Data and Secret Handling Failures	8. Excessive Agency
9. Asset Management Failures	9. Overreliance
10. Security Logging and Monitoring Failures	10. Model Theft

zenity

Summing up

TL;DR>

- Business Developers are a far bigger and far riskier crowd than Pro Developers.
- The GenAI market is rushing forward and security, as always, is lagging.
- As a result, organizations lose control over their data and risk breaching compliance.

- Take ownership of the processes in your organization.
- Keep yourself informed.
- Follow Top-10 frameworks and implement.

zenity

SANS

Thank you!

@inbarraz / @zenitysec