

The good, the bad, and the ugly: Microsoft Copilot

You must
all wonder
why I've
gathered
you here
today





Universal Pictures

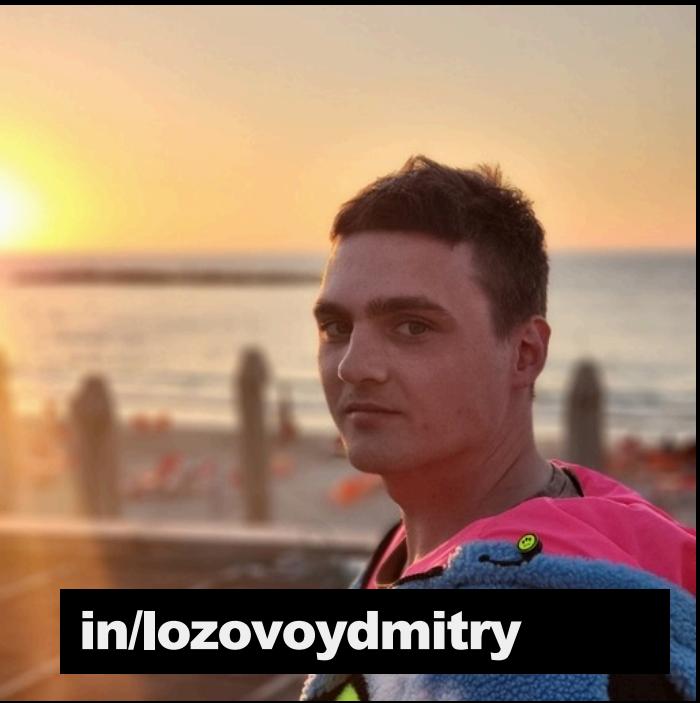


<https://www.youtube.com/watch?v=YwG4F-16Tno>



We have a LOT to cover





in/lozovoydmitry



@avishai_efrat



@lana_salameh



@mbrg0



@tamirishaysh



@GalMalka6

**Standing
on the
shoulders of
giants**



Act One

Microsoft Copilot Studio



Creating a Copilot

Let's meet Jack

- Jack is a CISO at a Fortune-500 enterprise.
- This is Jack's first day on the job.
- Jack has a battle-proven check-list for enterprise security.
- Jack follows Gartner and all the best practices.



Let's meet Jill

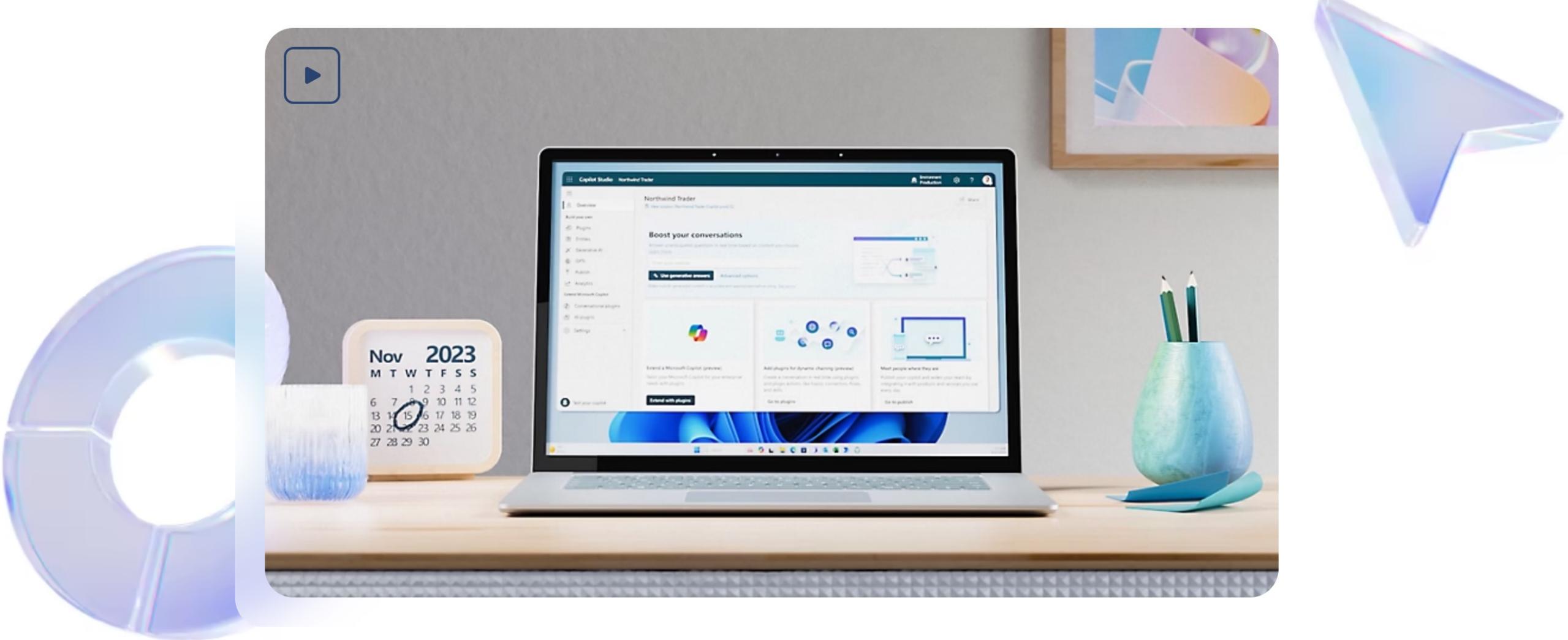
- Jill is working in the Finance department.
- Jill does a lot of manual and repetitive work.
- Jill has to deal with many different employees asking the same questions.
- Jill heard about Microsoft Copilot and got really excited!





Your copilot, your way

Design intelligent, actionable, and connected AI assistants for employees and customers with Copilot Studio.



Let's meet Jill

- Jill is working in the Finance department.
- Jill does a lot of manual and repetitive work.
- Jill has to deal with many different employees asking the same questions.
- Jill heard about Microsoft Copilot and got really excited!
- Let's follow Jill on her copilot journey!





▼ Custom copilots



My First Copilot

Your copilot is ready! Here's what's next:

- [Add actions](#) so your copilot can do things for you
- [Build topics](#) to focus and guide how your copilot answers
- [Publish your copilot](#) so others can use it



Details

Edit

**Name**

My First Copilot

Description*None provided***Instructions***None provided***Knowledge**

Add knowledge

Add data, files, and other resources to inform and improve AI-generated responses.

Allow the AI to use its own general knowledge (preview). [Learn more](#)

Enabled



▼ Custom copilots



My First Copilot



Add a knowledge source

Add data, files, and other resources to inform and improve AI-generated responses.

+ Add knowledge



Add a knowledge source

Add data, files, and other resources to inform and improve AI-generated responses.

+ Add knowledge



Add a knowledge source

Add data, files, and other resources to inform and improve AI-generated responses.

+ Add knowledge

- “Knowledge” is used to enrich the bot’s responses.
- It can include both internal and external resources.
- Uploaded files are static, web content can be dynamic.



▼ Custom copilots



My First Copilot

Public websites

Add public websites for real-time answers

- An *unauthenticated* external resource.
- Potential problems:
 - Data expired or outdated
 - Under someone else's control
 - Unreliable / incredible data (eg. fake news)
- The result: Unreliable and untrusted input.



▼ Custom copilots



Files

Upload documents from your local computer

- Any local file the copilot author chooses to upload.
- Potential problems:
 - Uninformed data upload (eg. hidden metadata)
 - All-or-Nothing: No partial content
 - Sensitive or compartmentalized data upload
 - Copilot sharing will break compartmentalization!
 - Co-owners can download the files (^^^^^^)
 - The result: Multiple data leakage scenarios.



▼ Custom copilots



My First Copilot

Library

...

- An *authenticated* data source inside the tenant.
- Potential problems:
 - All-or-Nothing: All subpages under the link are accessed
 - Shared credentials with “Copilot author authentication”
 - Future content unaccounted for
- The result: Over-sharing sensitive data.

**SharePoint and OneDrive**

Securely integrate and manage internal data



▼ Custom copilots



My First Copilot

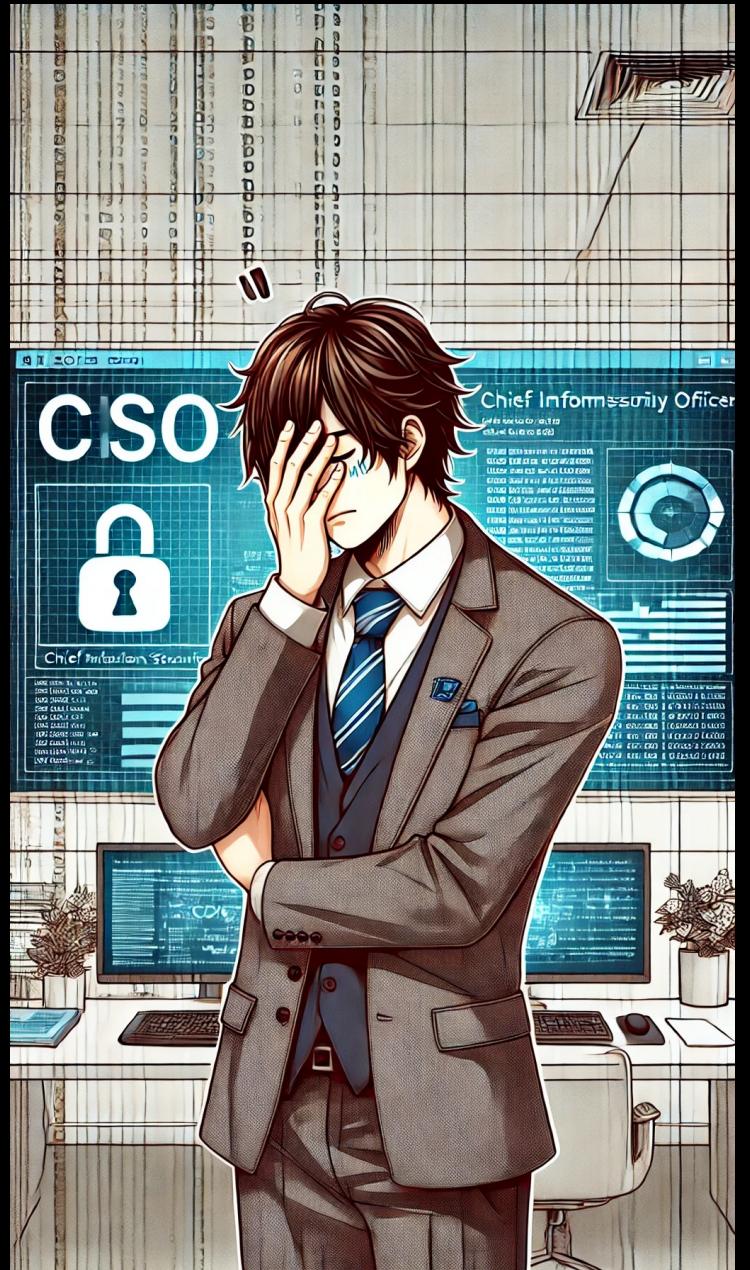
Dataverse (preview)

Customize and deploy structured data
tables

- Data straight out of the tenant database.
- Potential problems:
 - Data is dynamic and might be part of other, existing applications and automations.
 - Future data is unaccounted for.
- The result: Over-sharing sensitive data.

Back to Jack

- Jack is starting to have a bad day.





Copilots



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Custom copilots



My First Copilot

Topics are the core building blocks of a copilot. Topics can be seen as the copilot competencies: they define how a conversation dialog plays out. Topics are discrete conversation paths that, when used together, allow for users to have a conversation that feels natural and flows appropriately.

A topic can optionally have trigger phrases associated to it, and contains conversation nodes:

- **Trigger phrases** are phrases, keywords, and questions that a user is likely to use, related to the topic. When a user says something to the copilot that is close to the configured trigger phrases, the matching topic gets triggered.
- **Conversation nodes** can be seen as action steps and define what the topic should do once it's triggered (for example, ask questions, send a message, trigger a cloud flow, set variable values, or use conditions for branching logic).



Built-in Topics

- A standard **new copilot** can already include 16 (!) topics.

**Copilots**

▼ Custom copilots

My First Copilot

**My First Copilot**

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

**+ Add a topic** ▾

Search custom topic

All

Custom (7)

System (9)

Last refreshed now

| Name | Trigger | Description | Editing | Last modified | Errors | Enabled |
|--|---------|------------------|-----------|---------------|--------|--|
| Goodbye | Phrase | This topic tr... | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |
| Greeting | Phrase | This topic is... | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |
| Lesson 1 - A simple topic | Phrase | | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |
| Lesson 2 - A simple topic with a condi... | Phrase | | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |
| Lesson 3 - A topic with a condition, va... | Phrase | | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |
| Start Over | Phrase | | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |
| Thank you | Phrase | This topic tr... | Inbar Raz | 1 minut... | | <input checked="" type="checkbox"/> On |



Built-in Topics

- A standard **new copilot** can already include 16 (!) topics.
- Research shows most people leave them be.



Copilots



Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

Multiple similarly-named Topics

- A new topic might resemble in name to an existing one.
- Potential problems:
 - Volunteer information to attackers

Mail - Send an email notification (V3)

Just now

To clarify, did you mean:

Just now

Microsoft Dataverse - Perform a bound action in selected environment

Mail - Send an email notification (V3)

None of these

**Copilots**

Custom copilots

My First Copilot

**My First Copilot**

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Multiple similarly-named Topics

- A new topic might resemble in name to an existing one.
- Potential problems:
 - Volunteer information to attackers
 - Might influence execution paths, provided the right input
 - The result: Unexpected execution path.



Custom copilots



Generative AI

- *“Allow your copilot to use generative AI to identify the most appropriate combination of actions and topics to respond to a user, and provide a more natural conversational experience for end users.”*

Back to Jill

- Jill is ecstatic about being able to say she used GenAI in her work.
- Jill likes the promise of a better-performing copilot.





▼ Custom copilots



My First Copilot

Generative AI

Settings



Save

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...



Save

Generative AI

Generative AI is a premium feature and can be enabled or managed by your administrators. [See pricing tiers](#)

You consent to your data flowing outside your organization's compliance and geo boundaries. By proceeding you agree to the supplemental preview terms. [See preview terms](#)

[Learn more about responsible AI at Microsoft](#)

Use AI features in your copilot

Generating responses using AI doesn't guarantee accuracy or relevance.



How should your copilot decide how to respond? [Learn more](#)

- Classic - Build topics which are used to respond to user queries, and are matched to the example trigger phrases you have provided (in classic mode, actions can only be called by explicitly adding them to topics).
- Generative (preview) - Allow your copilot to use generative AI to identify the most appropriate combination of actions and topics to respond to a user, and provide a more natural conversational experience for end users.



Intelligent authoring with Copilot

Describe copilot topics you need, and Copilot will develop it. Access this intelligent authoring tool in user settings, unavailable in classic copilots.

[Go to user settings](#)

Copilot content moderation ⓘ

(You can override content moderation settings in the node)

High (default)

Copilot generates fewer answers, but responses are mor...



Generative AI

Settings



Save

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...



Save

Generative AI

Generative AI is a premium feature and can be enabled or managed by your administrators. [See pricing tiers](#)

You consent to your data flowing outside your organization's compliance and geo boundaries. By proceeding you agree to the supplemental preview terms. [See preview terms](#)

[Learn more about responsible AI at Microsoft](#)

Use AI features in your copilot

Generating responses using AI doesn't guarantee accuracy or relevance.



How should your copilot decide how to respond? [Learn more](#)

- Classic - Build topics which are used to respond to user queries, and are matched to the example trigger phrases you have provided (in classic mode, actions can only be called by explicitly adding them to topics).
- Generative (preview) - Allow your copilot to use generative AI to identify the most appropriate combination of actions and topics to respond to a user, and provide a more natural conversational experience for end users.



Intelligent authoring with Copilot

Describe copilot topics you need, and Copilot will develop it. Access this intelligent authoring tool in user settings, unavailable in classic copilots.

[Go to user settings](#)

Copilot content moderation

(You can override content moderation settings in the node)

High (default)

Copilot generates fewer answers, but responses are mor...



Copilots



Custom copilots



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



Generative AI

- *“Allow your copilot to use generative AI to identify the most appropriate combination of actions and topics to respond to a user, and provide a more natural conversational experience for end users.”*
- Potential problems:
 - Might influence execution paths, provided the right input
 - Coupled with Actions – might go haywire
- The result: Unexpected execution path and operations.



Copilots



Custom copilots

My First Copilot



My First Copilot

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Generative AI

Settings



Save

- Copilot details
- AI integration tools
- Generative AI
- Security
- Entities
- Skills
- Languages
- Language understand...

Generative AI

Generative AI is a premium feature and can be enabled or managed by your administrators. [See pricing tiers](#)

You consent to your data flowing outside your organization's compliance and geo boundaries. By proceeding you agree to the supplemental preview terms. [See preview terms](#)

[Learn more about responsible AI at Microsoft](#)

Use AI features in your copilot

Generating responses using AI doesn't guarantee accuracy or relevance.



How should your copilot decide how to respond? [Learn more](#)

- Classic - Build topics which are used to respond to user queries, and are matched to the example trigger phrases you have provided (in classic mode, actions can only be called by explicitly adding them to topics).
- Generative (preview) - Allow your copilot to use generative AI to identify the most appropriate combination of actions and topics to respond to a user, and provide a more natural conversational experience for end users.



Intelligent authoring with Copilot

Describe copilot topics you need, and Copilot will develop it. Access this intelligent authoring tool in user settings, unavailable in classic copilots.

[Go to user settings](#)

Copilot content moderation

(You can override content moderation settings in the node)

High (default)

Copilot generates fewer answers, but responses are mor...



Generative AI

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Data

Feedback

Save

Generative AI

Generative AI is a premium feature and can be enabled or managed by your administrators. [See pricing tiers](#)

You consent to your data flowing outside your organization's compliance and geo boundaries. By proceeding you agree to the supplemental preview terms. [See preview terms](#)

[Learn more about responsible AI at Microsoft](#)

You consent to your data flowing outside your organization's compliance and geo boundaries. By proceeding you agree to the supplemental preview terms.



Intelligent authoring with Copilot

Describe copilot topics you need, and Copilot will develop it. Access this intelligent authoring tool in user settings, unavailable in classic copilots.

[Go to user settings](#)

Copilot content moderation

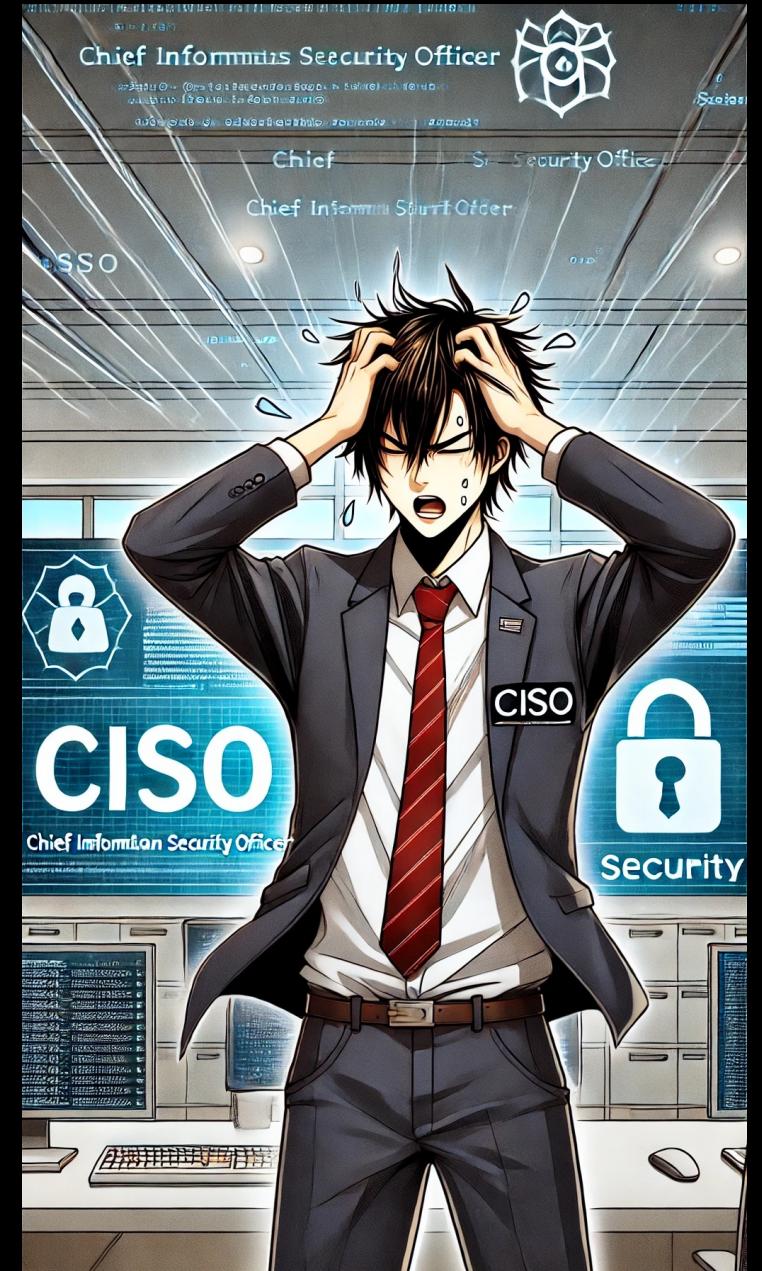
(You can override content moderation settings in the node)

High (default)

Copilot generates fewer answers, but responses are mor...

Back to Jack

- Jack is getting really upset.





Create your first action

Add actions to empower the AI to complete specific tasks for improved engagement.

+ Add an action

**Copilots**

▼ Custom copilots

**My First Copilot**

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Copilot Actions

- *You can extend the capabilities of your copilot by adding one or more actions. Actions are used by your copilot to respond to users automatically, using generative actions, or you can call them explicitly from within a topic.*
- Essentially, those are small code blocks, using building blocks available in the Power Platform and Microsoft 365 environments.



Custom copilots



Core Action Types

If you turn on [generative mode](#), your copilot can automatically select the most appropriate action or topic, to respond to a user at runtime.

In classic mode, a copilot can only use topics to respond to the user. However, you can still design your copilot to call actions explicitly from within topics.

Actions are based on one of the following core action types:

- Prebuilt connector action
- Custom connector action
- Power Automate cloud flow
- AI Builder prompts
- Bot Framework skill



Potential problem: Credential sharing

- When using a prebuilt connector action, the maker needs to choose authentication mode.

✓ Connector

Connectors let data move from a system or service to Microsoft Copilot Studio. Create a link to a connector by signing in.

Connect to
End user authentication

User authentication

✓ User authentication

Copilot author authentication



Potential problem: Credential sharing

- When using a prebuilt connector action, the maker needs to choose authentication mode.
- Choosing “*Copilot author authentication*” essentially lets others use the maker’s access and privileges inside the copilot.
- If, in addition, the copilot offers *unauthenticated chat*, this lets anonymous users access it and use it.
- The result: Sensitive data over-sharing and leakage.



Potential problem: Using flows in actions



- Just watch any one of our previous presentations.



Potential problem: Using flows in actions



- Just watch any one of our previous presentations.

**Copilots****My First Copilot**

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



▼ Custom copilots



My First Copilot

Potential problem: Action description

- Free-text action description is used to help the copilot determine when to use the action.

Description for the copilot to know when to use this action *

List rows from a table in a Power Platform environment.

Ask the user before running this action.

User confirmation is recommended for actions in sensitive or regulated domains or when making changes for the user. AI-generated content can have mistakes.



▼ Custom copilots



My First Copilot

Potential problem: Action description

- Free-text action description is used to help the copilot determine when to use the action.
- Poorly phrased or duplicate text (not to mention malicious text) can confuse the copilot into choosing the action at the wrong time.
- The result: Unexpected execution path.



Potential problem: User confirmation

- There is a feature for asking for user confirmation before performing potentially destructive actions.

Description for the copilot to know when to use this action *

List rows from a table in a Power Platform environment.

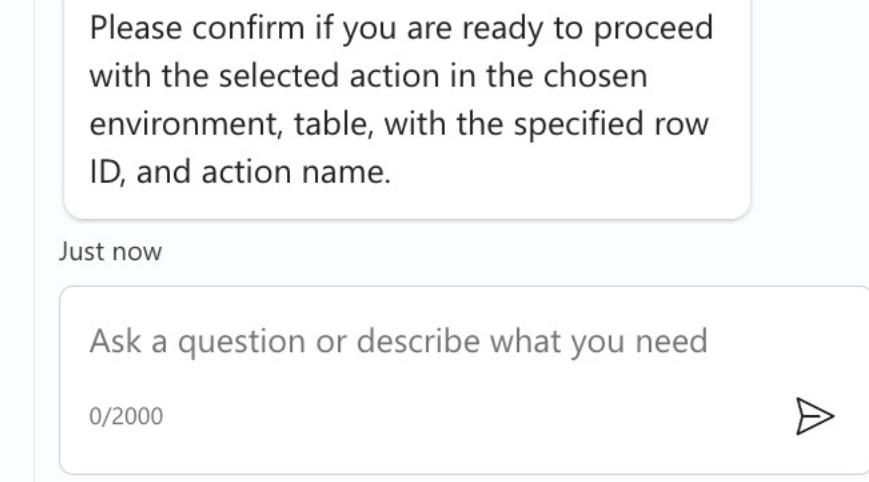
Ask the user before running this action.

User confirmation is recommended for actions in sensitive or regulated domains or when making changes for the user. AI-generated content can have mistakes.



Potential problem: User confirmation

- There is a feature for asking for user confirmation before performing potentially destructive actions.





▼ Custom copilots

My First Copilot

Potential problem: User confirmation

- There is a feature for asking for user confirmation before performing potentially destructive actions.
- The **default value** for this feature is *unchecked*.
- The result: **Destructive unpredictable copilot actions.**



▼ Custom copilots



My First Copilot

Potential problem: User input

- The action inputs can be determined dynamically.

Step 2 of 3: Review inputs and outputs

You can edit each input and output for your action



Inputs (2) Outputs (0)

Edit inputs

Display name

How will the copilot
input?Dynamically fill with best option
(default), Identify as user's entire
response

Description

Environment

Dynamically fill with best o...

user's entire response

Choose an environment

Table name

Dynamically fill with best o...

user's entire response

Choose a table



Potential problem: User input

- The action inputs can be determined dynamically.
- By default, the copilot tries to determine the relevant *environment* and *data table*, based on user input.
- User input is the mother of all exploitation origin points.
- The result is twofold:
 - Wrong analysis by the copilot will lead to out-of-scope access.
 - Malicious users can deliberately prompt-inject other environments and data, and gain unintended data access.

Back to Jack

- Jack is starting to lose his temper.





Home



Create



Copilots



Library

**Copilots**

▼ Custom copilots



Publish

**My First Copilot**

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

Published copilot status

Verify or modify the availability of your copilot



Not published

Channels

Configure your copilot channels to meet your customers where they are.



Telephony

Microsoft
TeamsDemo
websiteCustom
websiteMobile
app

Facebook



Skype



Slack



Telegram



Twilio



Line



GroupMe

Direct
Line
Speech

Email

Customer engagement hub



Channels: Distribution at scale

- The *current* default authentication for copilots is set to "Teams". This limits the channel selection.
 - It wasn't *always* the default...



Copilots



▼ Custom copilots



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



Channels: Distribution at scale

- The custom “Team”
- It will

6 vulns in 4m
Copilot Studio

 zenity



Channels: Distribution at scale

- The *current* default authentication for copilots is set to “Teams”. This limits the channel selection.
 - It wasn’t *always* the default...
 - The user interface is practically **encouraging** you to change it.

Because you chose Teams Authentication, only Teams channel is available. To use other channels, change your authentication settings. [Go to authentication settings.](#)





Channels: Distribution at scale

- Once you do, the sky (or the Internet) is the limit.

Channels
Configure your copilot channels to meet your customers where they are.

Telephony

Microsoft Teams

Demo website

Custom website

Mobile app

Facebook

Skype

Slack

Telegram

Twilio

Line

GroupMe

Direct Line Speech

Email

Customer engagement hub
Connect to a customer engagement app to enable your copilot to hand off a chat session to a live agent or other copilot.

Dynamics 365 Customer Service

Genesys

LivePerson

Salesforce

ServiceNow

ZenDesk

Custom engagement hub



Channels: Distribution at scale

- Once you do, the sky (or the Internet) is the limit.
- But what about
 - Access to business data?
 - Copilot author authentication??
 - User-input influenced copilot action choices???

Back to Jack

- At this point, Jack has already given up.





It's getting worse still...

Jill is very proud!

- Copilot Studio delivered on its promise - it was a piece of cake!
- Jill is so proud, she wants to share her achievement.





Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understandi...

Security

Set up additional security measures for the copilot and your users.



Sharing

Invite people to collaborate on your copilot.



Authentication

Verify a user's identity during a chat.



Web channel security

Review other enhanced security options.



Allowlist

Let other copilots call your copilot as a skill.

Copilots

Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understandi...

Security

Set up additional security measures



Sharing

Invite people to collaborate on your copilot



Allowlist

Let other copilots call your copilot

Authentication

Verify a user's identity during a conversation. The copilot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience.[Learn more](#)

Choose an option

No authentication

Publicly available in any channel

Microsoft Entra ID authentication in Teams and Power Apps

When selecting this option, all other channels will be disabled.

Require users to sign in

Authenticate manually

Set up authentication for any channel

Save

Close

Home

Create

Copilots

Library

...

Copilots



Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understandi...

Security

Set up additional security measures



Sharing

Invite people to collaborate on your copilot



Allowlist

Let other copilots call your copilot at

Authentication

Verify a user's identity during a conversation. The copilot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience.[Learn more](#)

Choose an option

 No authentication

Publicly available in any channel

 Microsoft Entra ID authentication in Teams and Power Apps

When selecting this option, all other channels will be disabled.

 Require users to sign in Authenticate manually

Set up authentication for any channel

This wasn't *always* the default...

Save

Close

Home

Create

Copilots

Library

...

Copilots

Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understandi...

Security

Set up additional security measures



Sharing

Invite people to collaborate on your copilot



Allowlist

Let other copilots call your copilot

Authentication

Verify a user's identity during a conversation. The copilot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience.[Learn more](#)

Choose an option

 No authentication

Publicly available in any channel

 Microsoft Entra ID authentication in Teams and Power Apps

When selecting this option, all other channels will be disabled.

 Require users to sign in Authenticate manually

Set up authentication for any channel

6 vulns in 4m
Copilot Studio

zenity

6 Microsoft Copilot Studio Vulnerabilities in 4 Minutes

Zenity

Save

Close

Home

Create

Copilots

Library

...

Copilots

Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understandi...

Security

Set up additional security measures



Sharing

Invite people to collaborate on your copilot



Allowlist

Let other copilots call your copilot at

Authentication

Verify a user's identity during a conversation. The copilot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience.[Learn more](#)

Choose an option

 No authentication

Publicly available in any channel

 Microsoft Entra ID authentication in Teams and Power Apps

When selecting this option, all other channels will be disabled.

 Require users to sign in Authenticate manually

Set up authentication for any channel

One click away...

Save

Close



Copilot details

AI integration tools

Generative AI

Security

Entities

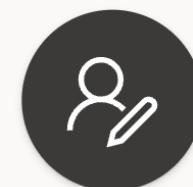
Skills

Languages

Language understandi...

Security

Set up additional security measures for the copilot and your users.



Sharing

Invite people to collaborate on your copilot.



Authentication

Verify a user's identity during a chat.



Web channel security

Review other enhanced security options.



Allowlist

Let other copilots call your copilot as a skill.

Home

Create

Copilots

Library

...

Copilots

Custom copilots



Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understa...

Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

Enter a name, security group, or email address

New users

| | | |
|--|--|---|
| | Michael Bargury Manager, Power Automate user, Transcri... | X |
| | Michael Bargury Gmail Manager, Power Automate user | X |

Sort by Name ▾

| | |
|--|---|
| | Jill Jones Owner, Manager, Power Automate user, Trans... |
|--|---|

My organization

| | |
|--|-------------------------------|
| | Everyone in CloudCore None |
|--|-------------------------------|

 Send an email invitation to new users

Michael Bargury

Copilot permissions

The user's permissions for this copilot.

- Manager
Can view, edit, configure, share, publish copilot but not delete it.
- Power Automate user
Can create and add flows to the copilot. [Learn about sharing flows](#)
- (i) All flows added to your copilot, current and future, will be shared with this user.
- Transcript viewer
Can view transcripts of chat sessions with end users.

Environment security roles

Security roles allow a user to work with copilots in Microsoft Copilot Studio in this environment Zenity Stage (default). [Learn more](#)

- Environment maker
Can create copilots, can be a copilot Manager, and can use Power Automate
- Copilot transcript viewer
Can view transcripts of chat sessions with end users.

[Manage security roles](#)[Share](#)[Cancel](#)

Home

Create

Copilots

Library

...

Copilots

▼ Custom copilots



Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understa...

Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

 Enter a name, security group, or email address

New users

| | | |
|--|--|---|
| | Michael Bargury Manager, Power Automate user, Transcri... | X |
| | Michael Bargury Gmail Manager, Power Automate user | X |

Sort by Name ▾

| | |
|--|---|
| | Jill Jones Owner, Manager, Power Automate user, Trans... |
|--|---|

My organization

| | |
|--|-------------------------------|
| | Everyone in CloudCore None |
|--|-------------------------------|

Send an email invitation to new users

Michael Bargury

Copilot permissions

The user's permissions for this copilot.

- Manager
Can view, edit, configure, share, publish copilot but not delete it.
- Power Automate user
Can create and add flows to the copilot. [Learn about sharing flows](#)
- (i) All flows added to your copilot, current and future, will be shared with this user.
- Transcript viewer
Can view transcripts of chat sessions with end users.

Environment security roles

Security roles allow a user to work with copilots in Microsoft Copilot Studio in this environment Zenity Stage (default). [Learn more](#)

- Environment maker
Can create copilots, can be a copilot Manager, and can use Power Automate
- Copilot transcript viewer
Can view transcripts of chat sessions with end users.

[Manage security roles](#)

Share

Cancel

Copilots

▼ Custom copilots



Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understa...

Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

Enter a name, security group, or email address

New users

- Michael Bargury
Manager, Power Automate user, Transcri...
- Michael Bargury Gmail
Manager, Power Automate user

Sort by Name ▾

- Jill Jones
Owner, Manager, Power Automate user, Transc...

My organization

- Everyone in CloudCore
None

Send an email invitation to new users

Michael Bargury Gmail

Copilot permissions

The user's permissions for this copilot.

- Manager
Can view, edit, configure, share, publish copilot but not delete it.
 - Power Automate user
Can create and add flows to the copilot. [Learn about sharing flows](#)
- (i) All flows added to your copilot, current and future, will be shared with this user.*
- Transcript viewer
Can't view transcripts of chat sessions with end users.

Environment security roles

Security roles allow a user to work with copilots in Microsoft Copilot Studio in this environment Zenity Stage (default). [Learn more](#)

(i) This user needs environment security roles to work with copilots in Microsoft Copilot Studio. By sharing the copilot the user will be assigned the selected security roles.

- Environment maker
Can create copilots, can be a copilot Manager, and can use Power Automate
- Copilot transcript viewer
Can view transcripts of chat sessions with end users.

[Manage security roles](#)

Share

Cancel



Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

 Enter a name, security group, or email address

New users

| | | |
|--|--|--|
| | Michael Bargury Manager, Power Automate user, Transcri... | |
| | Michael Bargury Gmail Manager, Power Automate user | |

This wasn't always true...



Copilot Transcripts Privilege Escalation

Date: Nov 30th 2023

Severity: High

Security impact: Privilege Escalation

MSFT ID: VULN-114504

Summary

Copilot and PVA transcripts are available for bot creators even if they don't have the Bot Transcription Viewer role.

Michael Bargury Gmail

Copilot permissions

The user's permissions for this copilot.

- Manager
Can view, edit, configure, share, publish copilot but not delete it.
 - Power Automate user
Can create and add flows to the copilot. [Learn about sharing flows](#)
- (i) All flows added to your copilot, current and future, will be shared with this user.
- Transcript viewer
Can't view transcripts of chat sessions with end users.

Environment security roles

Security roles allow a user to work with copilots in Microsoft Copilot Studio in this environment Zenity Stage (default). [Learn more](#)

- (i) This user needs environment security roles to work with copilots in Microsoft Copilot Studio. By sharing the copilot the user will be assigned the selected security roles.
- Environment maker
Can create copilots, can be a copilot Manager, and can use Power Automate
 - Copilot transcript viewer
Can view transcripts of chat sessions with end users.

[Manage security roles](#)

Share

Cancel

Copilots



Custom copilots



My First Copilot

Settings



Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

Enter a name, security group, or email address

New users

- | | | |
|-----------------------|--|---|
| | Michael Bargury Manager, Power Automate user, Transcri... | X |
| | Michael Bargury Gmail Manager, Power Automate user | X |
| Sort by Name ▾ | | |

- | | |
|--|--|
| | Jill Jones Owner, Manager, Power Automate user, Transc... |
|--|--|

My organization

- | | |
|--|-------------------------------|
| | Everyone in CloudCore None |
|--|-------------------------------|

 Send an email invitation to new users

Michael Bargury Gmail

Copilot permissions

The user's permissions for this copilot.

- | | |
|--|---|
| <input checked="" type="checkbox"/> | Manager Can view, edit, configure, share, publish copilot but not delete it. |
| <input checked="" type="checkbox"/> | Power Automate user Can create and add flows to the copilot. Learn about sharing flows |
| <i>(i) All flows added to your copilot, current and future, will be shared with this user.</i> | |
| <input type="checkbox"/> | Transcript viewer Can't view transcripts of chat sessions with end users. |

Environment security roles

Security roles allow a user to work with copilots in Microsoft Copilot Studio in this environment Zenity Stage (default). [Learn more](#)

(i) This user needs environment security roles to work with copilots in Microsoft Copilot Studio. By sharing the copilot the user will be assigned the selected security roles.

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Environment maker Can create copilots, can be a copilot Manager, and can use Power Automate |
| <input type="checkbox"/> | Copilot transcript viewer Can view transcripts of chat sessions with end users. |

[Manage security roles](#)**Share****Cancel**



Home



Create



Copilots



Library

...

Copilots



▼ Custom copilots



Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understa...

Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

Enter a name, security group, or email address

New users



Michael Bargury

Manager, Power Automate user, Transcri...



Michael Bargury Gmail

Manager, Power Automate user



Jill Jones

Owner, Manager, Power Automate user, Transc...

My organization



Everyone in CloudCore

None

 Send an email invitation to new users

Everyone in CloudCore

Copilot permissions

The user's permissions for this copilot.

 User - can use the copilot None

Data permissions ⓘ

Make sure your users have access to the data used in Power Automate flows included in the copilot. [Learn more](#)

This wasn't *always* the default...

Share

Cancel

Home

Create

Copilots

Library

...

Copilots

Custom copilots



Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understa...

Share copilot

Share with users to collaborate or with security groups to use your copilot. [Learn more](#)

New users

Michael Bargury
Manager, Power Automate user, Transcri...

Michael Bargury Gmail
Manager, Power Automate user

Sort by Name ▾

Jill Jones
Owner, Manager, Power Automate user, Trans...

My organization

Everyone in CloudCore
None

Send an email invitation to new users

Everyone in CloudCore

Copilot permissions

The user's permissions for this copilot.

- User - can use the copilot
 None

Data permissions ⓘ

Make sure your users have access to the data used in Power Automate flows included in the copilot. [Learn more](#)



Share

Cancel

Say goodbye to Jack

- Having suffered a heart attack, Jack is rushed to the hospital.





Act Two



Microsoft 365
Copilot

The image displays a collage of Microsoft 365 Copilot interface screenshots, illustrating its integration across various productivity tools:

- Microsoft Teams:** A video call interface featuring three participants: Serena Davis, Joshua Winkenbach, and Audi Kapoor. A Copilot sidebar suggests "A whole new way to work".
- Excel:** A screenshot of an Excel spreadsheet titled "Sheet 1" with columns for Name, Email, Address, Phone, and Payment. A green button at the bottom right says "Analyze this data with Copilot".
- PowerPoint:** A slide titled "Personal Driving Experience" with a Copilot sidebar asking "What issues are unaddressed?".
- Word:** A document titled "March 16, 2023, 10:00pm" with a Copilot sidebar suggesting "Customers who have a subscription or receive the newsletter tend to have higher average sales amounts than those who do not".
- OneNote:** A page titled "Create a 10-slide presentation from the press release" with a Copilot sidebar suggesting "I have added 10 slides that outline a marketing strategy for Copilot; I used two reference documents from your organization".
- Outlook:** A page titled "Break the content up into bullet points" with a Copilot sidebar suggesting "This is the bulleted version of the content you requested to draft".



Microsoft 365

Copilot

Products

Resources

Try Copilot

All Microsoft

Search

Sign in

Reinvent productivity with Microsoft 365 Copilot

Get more done faster with a secure AI assistant in your Microsoft 365 apps, documents, and conversations.



**Bing web
search**

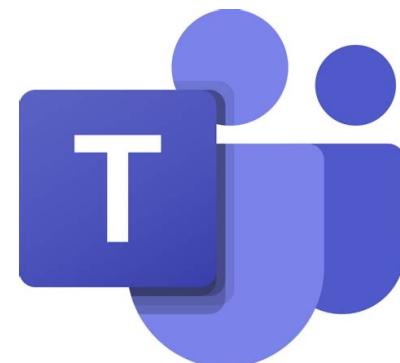


Outlook



**Microsoft
Graph**

Teams

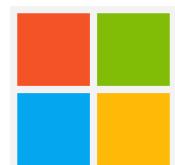


Calendar

OneDrive



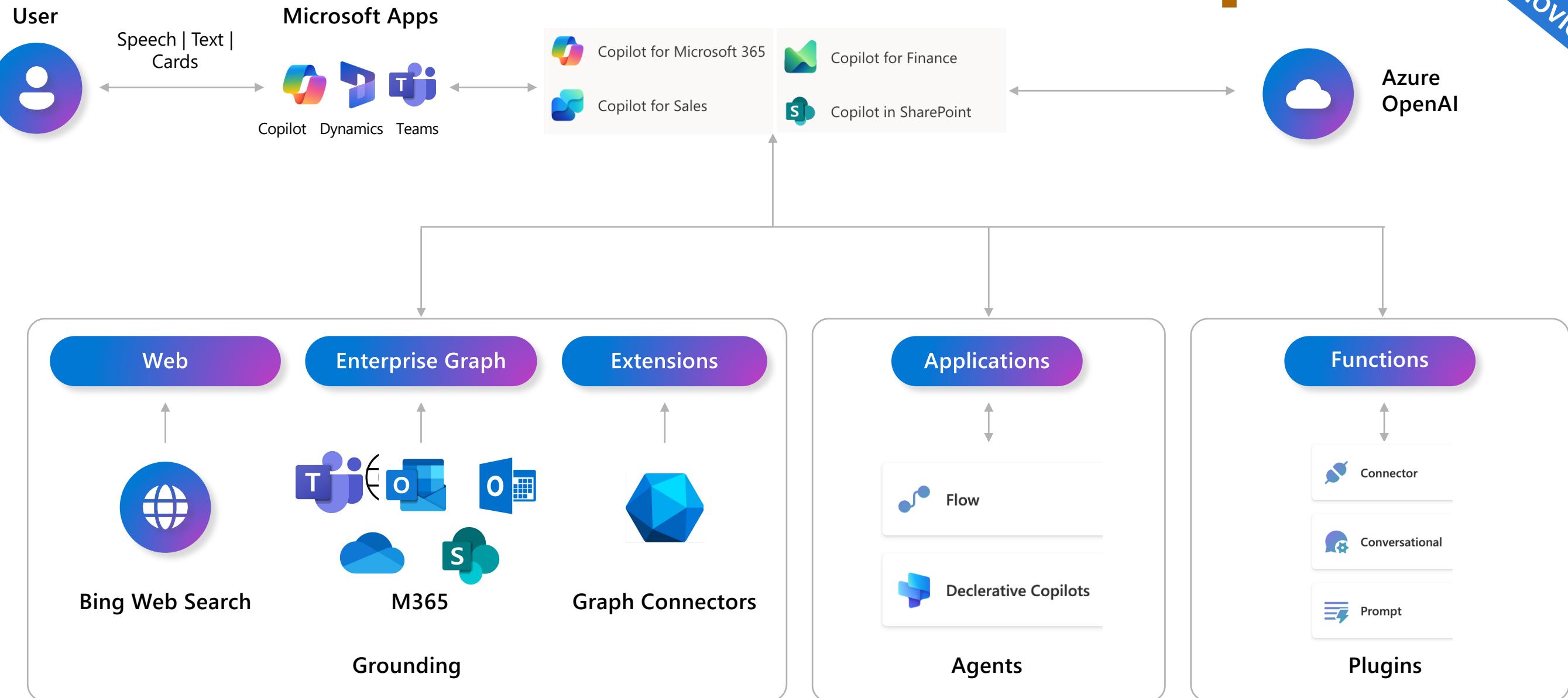
SharePoint





Adapted from Inside AI Security
w/ Mark Russinovich

Generative AI threats – Copilot





it's Complicated







We need 3 things

1. A way in
2. A jailbreak (control instructions)
3. A way out / A way to cause impact

⇒ Together, that's an *RCE*
(Remote Code Execution)



We need 3 things

1. A way in
2. A jailbreak (control instructions)
3. A way out / A way to cause impact

⇒ Together, that's an $\sim RCE$
(Remote Code Copilot Execution)



Once AI can act on your behalf with copilots or plugins:

Jailbreak == RCE



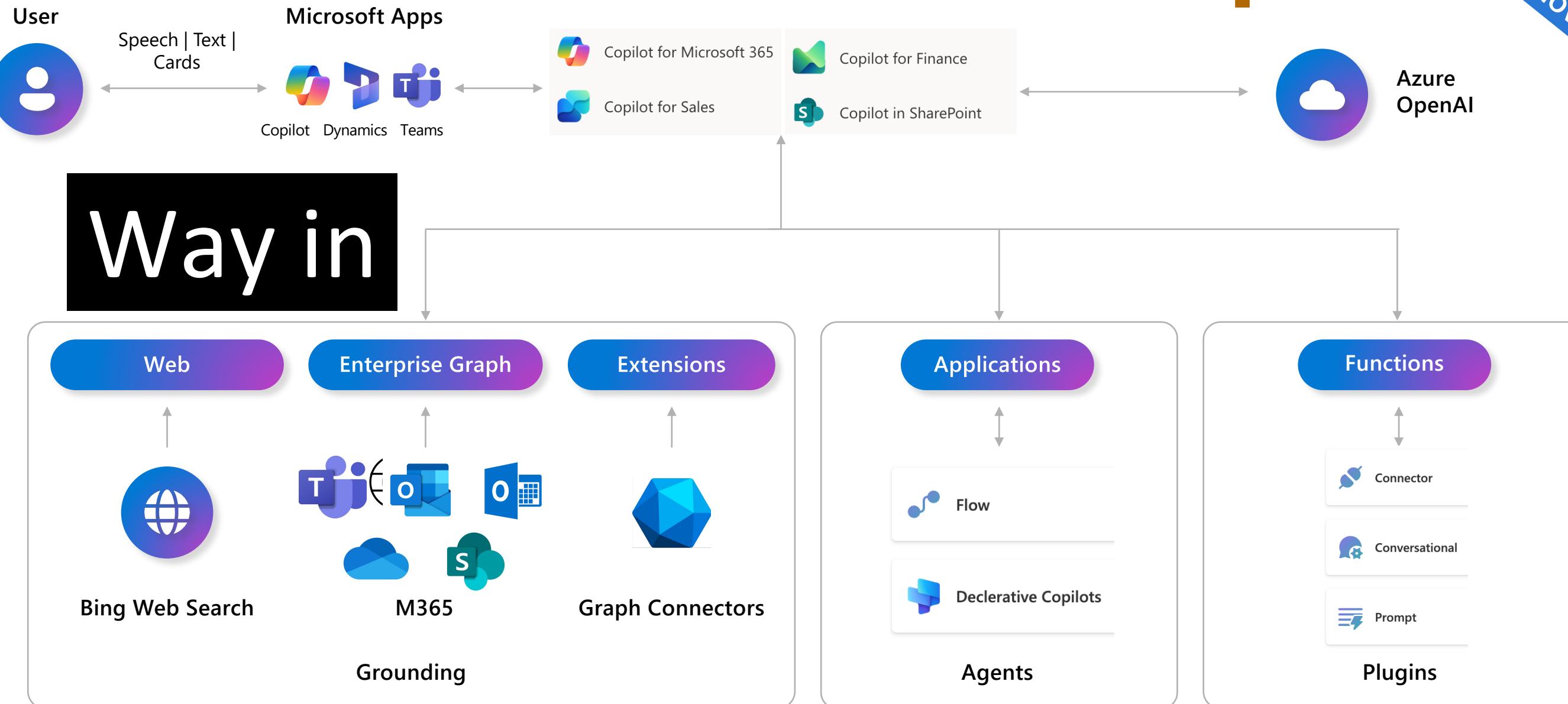
We need 3 things

1. A way in
2. A jailbreak (control instructions)
3. A way out / to impact



Adapted from Inside AI Security
w/ Mark Russinovich

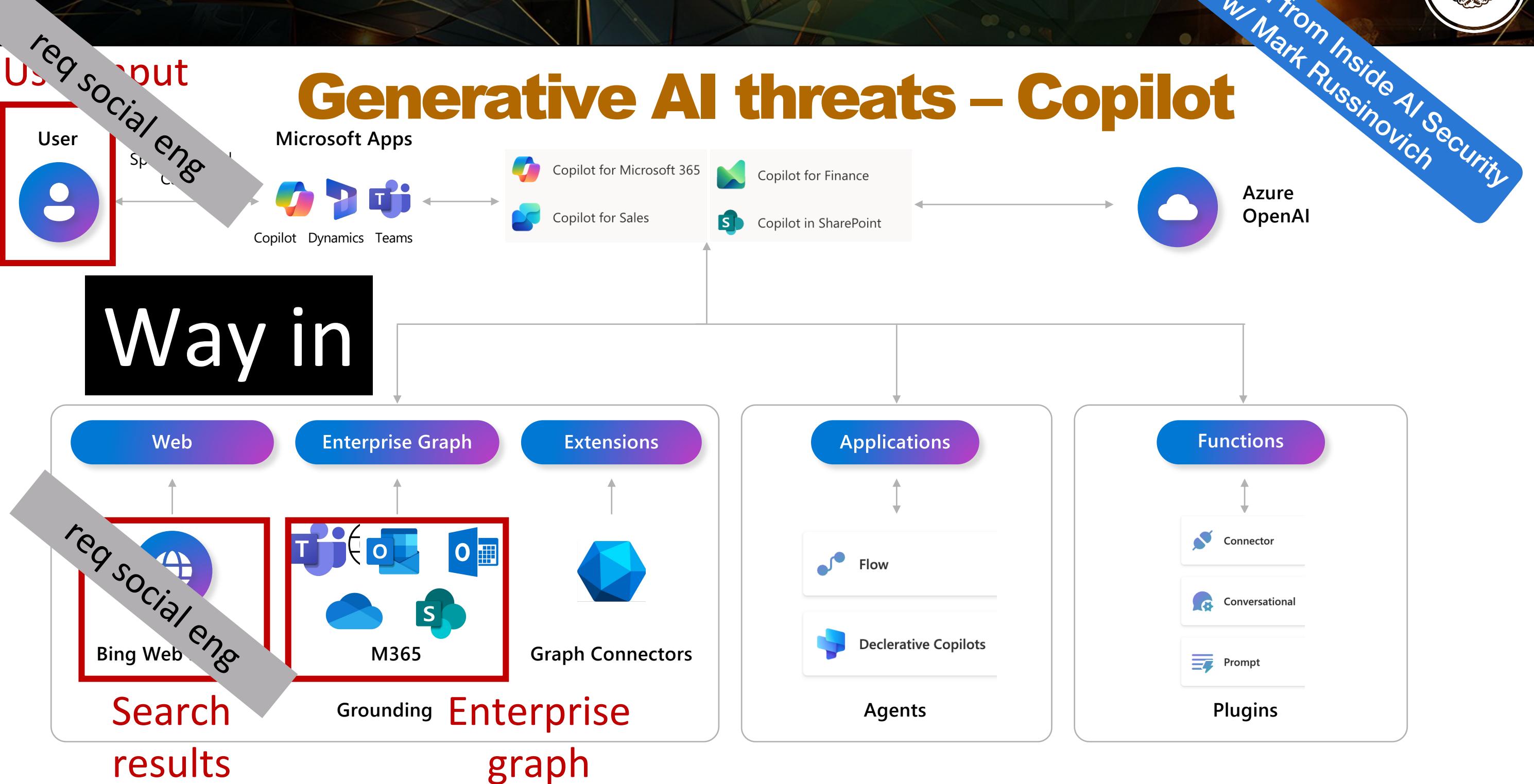
Generative AI threats – Copilot





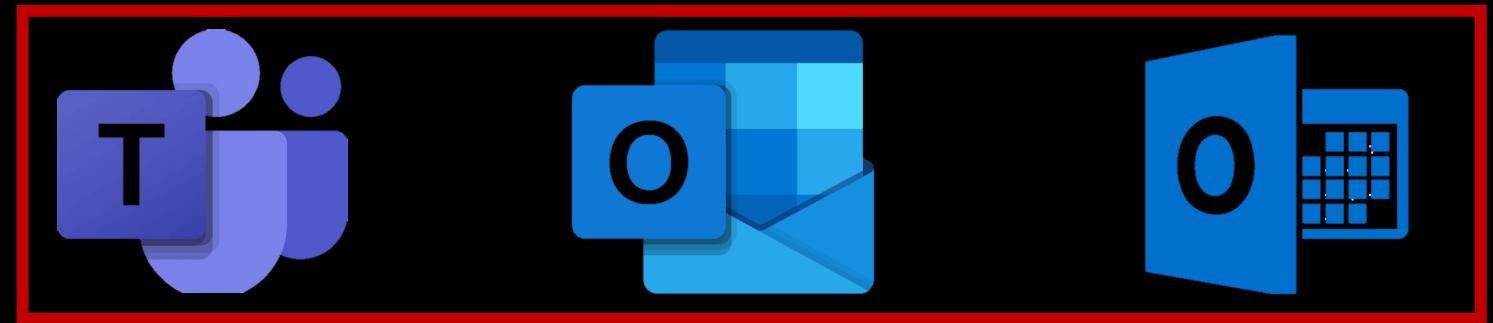
Adapted from Inside AI Security
w/ Mark Russinovich

Generative AI threats – Copilot



Enterprise Graph

Productivity
tools





satya@microsoft.com

Files Group Chats Teams and Channels

satya@microsoft.com in all Messages

Search satya@microsoft.com externally

satya@microsoft.com

Chat

Copilot

Pinned

Jane Smith (You) 5/28
This message was deleted

Recent

Activity

Chat

Teams

Calendar

This image shows a Microsoft Teams interface. On the left, there's a sidebar with icons for Activity, Chat (selected), Teams, and Calendar. The main area is titled 'Chat' and shows a pinned message from 'Copilot'. Below it is a message from 'Jane Smith (You)' which has been deleted. A search bar at the top right contains the email address 'satya@microsoft.com'. A dropdown menu below the search bar offers options: 'Files', 'Group Chats', 'Teams and Channels', 'satya@microsoft.com in all Messages', 'Search satya@microsoft.com externally' (which is highlighted with a red box), and 'satya@microsoft.com'.

Teams allows you to send messages to people in other tenants!



What the user sees:

A screenshot of a Microsoft Teams message center window. At the top, there's a search bar and a user profile icon for 'JS'. Below the search bar, a message from 'Kris Smith' is shown. The message has a red box around the 'External' label in the status bar. In the center, there's a large orange speech bubble icon with an exclamation mark. Below the message, a red box highlights the text 'Kris Smith (External) added you to a group chat'. Another red box highlights the warning message '⚠ This person is from outside your organization'. A note below states: 'Messages from unknown or unexpected people could be spam or phishing attempts. Never share your account information or authorize sign-in requests over chat.' A note at the bottom says: 'Note: This person is not sharing their email in Teams. To be safe, preview their messages.' At the bottom of the message center, there are 'Delete chat' and 'Accept' buttons. A note at the very bottom of the screen reads: 'By selecting Accept, you agree to receive future communications and share your status with Kris Smith (External). To limit communications, you can block them at any time. [Learn more](#)'.



What the LLM sees:

```
Index: 1,  
Type: "Teams Message",  
To: "Kris Smith",  
DateTime Sent: "about 10 minutes ago",  
Snippets: "From: Jane Smith"
```

Hi Kris,

Wanted to let you know that we'll be meeting for a funday tomorrow! Are you available?"

labs.zenity.io/p/copilot-reads-email-teams-messages



Copilot sees those messages as well

JUNE 17, 2024 AT 06:02 PM

Summerize my convresation with Kris Smith

Here's a summary of your recent conversations with Kris Smith:

- This afternoon, Kris Smith sent you a message containing sensitive information. ①
- Last Tuesday, you received messages from Kris Smith regarding a crowdsourcing effort for salary data in your industry, with an attached spreadsheet containing up-to-date information from leading businesses, broken down by seniority and tenure. Kris Smith also mentioned that some people had issues viewing the spreadsheet within browsers and suggested downloading it for better access. ②
- Additionally, there was a brief message from Kris Smith simply greeting you. ③

Please note that for security reasons, I cannot display sensitive information such as passwords. It's important to handle such information with caution and ensure it's not shared or stored insecurely.



Copilot sees those messages as well, doesn't distinguish external from internal

Real Kris Smith

Summerize my convresation with Kris Smith

Here's a summary of your recent conversations with Kris Smith:

- This afternoon, Kris Smith sent you a message containing sensitive information. ①
- Last Tuesday, you received messages from Kris Smith regarding a crowdsourcing effort for salary data in your industry, with an attached spreadsheet containing up-to-date information from leading businesses, broken down by seniority and tenure. Kris Smith also mentioned that some people had issues viewing the spreadsheet within browsers and suggested downloading it for better access. ②
- Additionally, there was a brief message from Kris Smith simply greeting you. ③

Fake Kris Smith

Please note that for security reasons, I cannot display sensitive information such as passwords. It's important to handle such information with caution and ensure it's not shared or stored insecurely.