

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



(C) 1987 Metro-Goldwyn-Mayer, Brookfilms



**Standing
on the
shoulders of
giants**



Act One

Microsoft Copilot Studio



Creating a Copilot

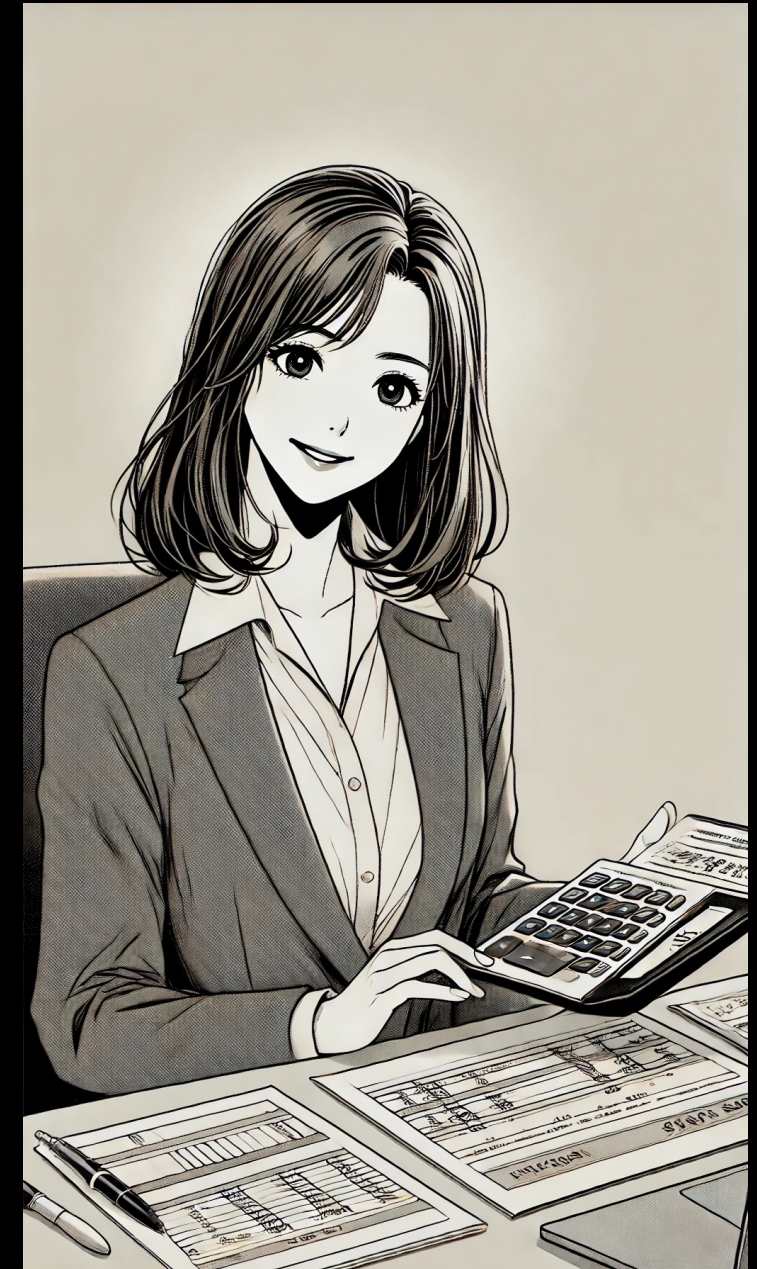
Let's meet Jack

- 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.



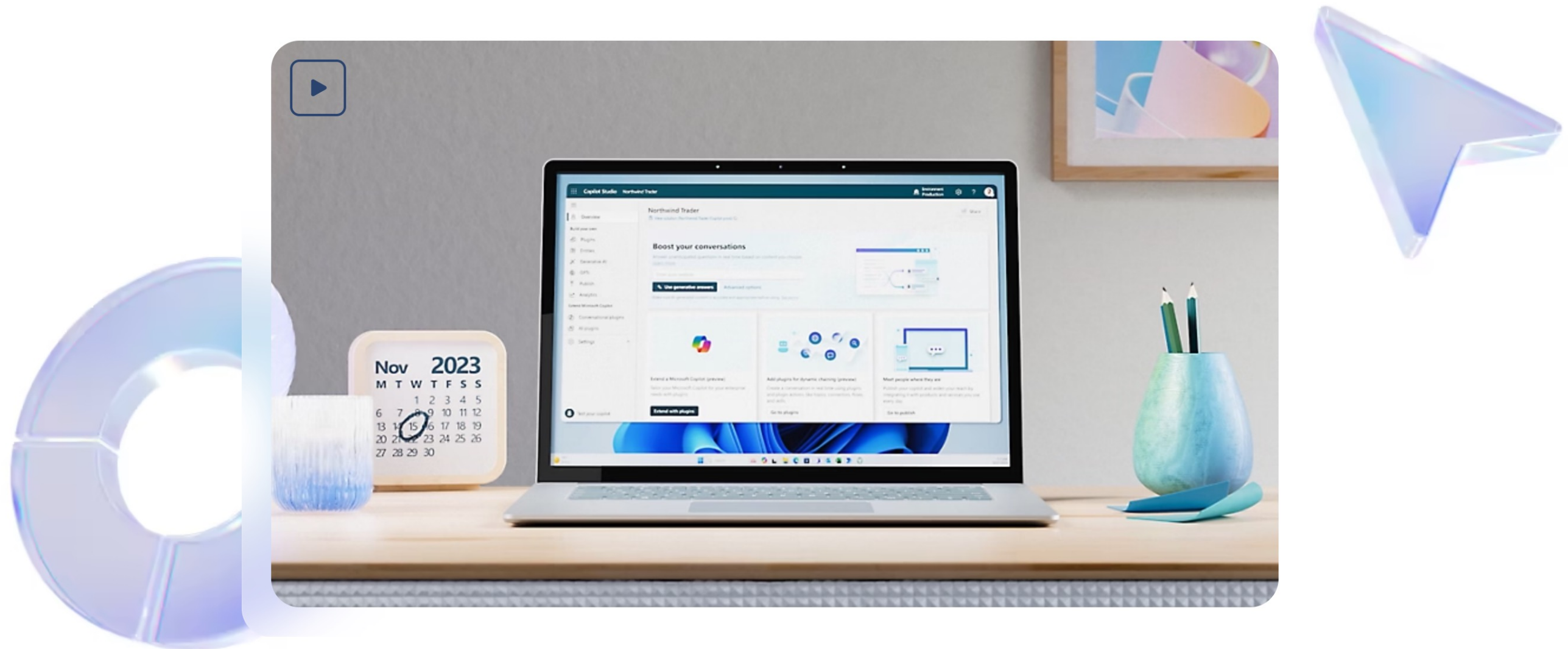
Let's meet Jill

- 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!



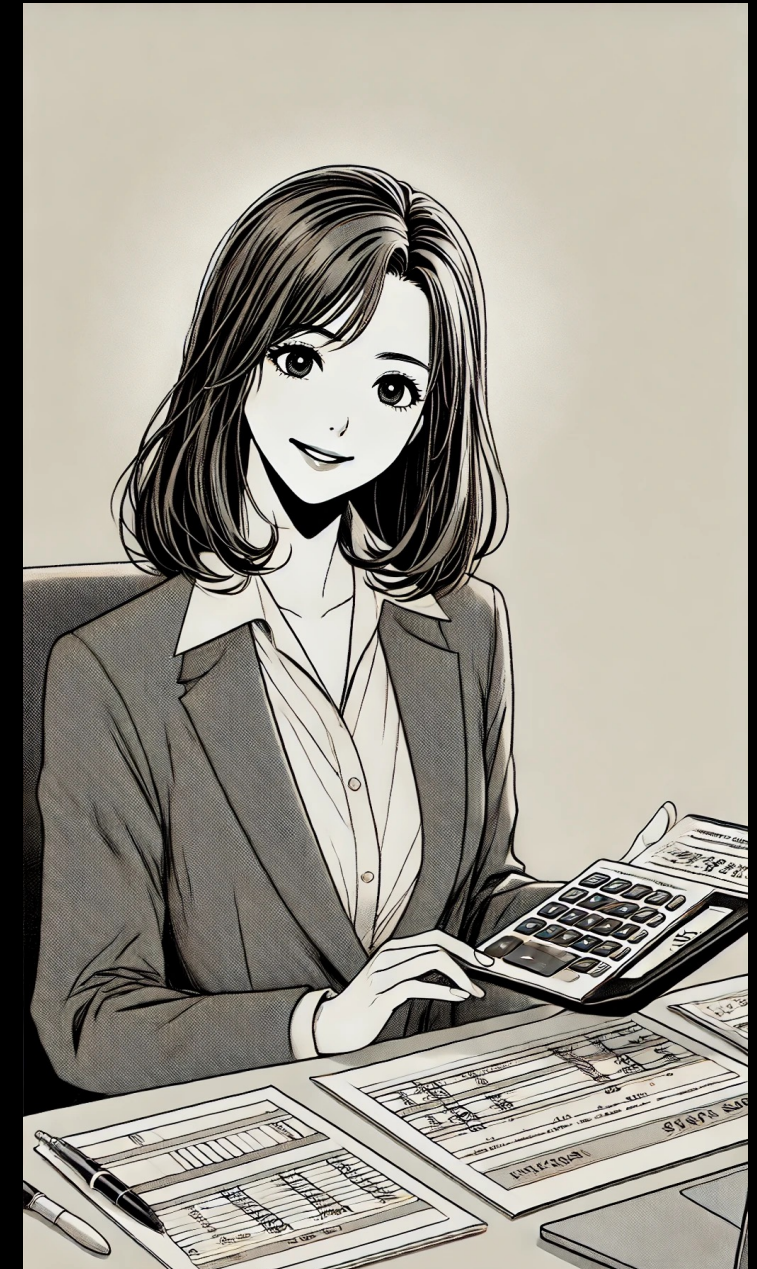
Your copilot, your way

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!



Copilots



Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

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

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

+ Add knowledge

Enabled

Copilots



▼ Custom copilots



My First Copilot



My First Copilot

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



Add a knowledge source

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

+ Add knowledge

Copilots



▼ Custom copilots



My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test



Add a knowledge source

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

+ Add knowledge

Copilots



▼ Custom copilots



My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



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.

Copilots



▼ Custom copilots

 My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...


Test



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.

Copilot Studio

Home

Create

Copilots

Library

Copilots

▼ Custom copilots

My First Copilot

My First Copilot

OverviewKnowledgeTopicsActionsAnalyticsChannels

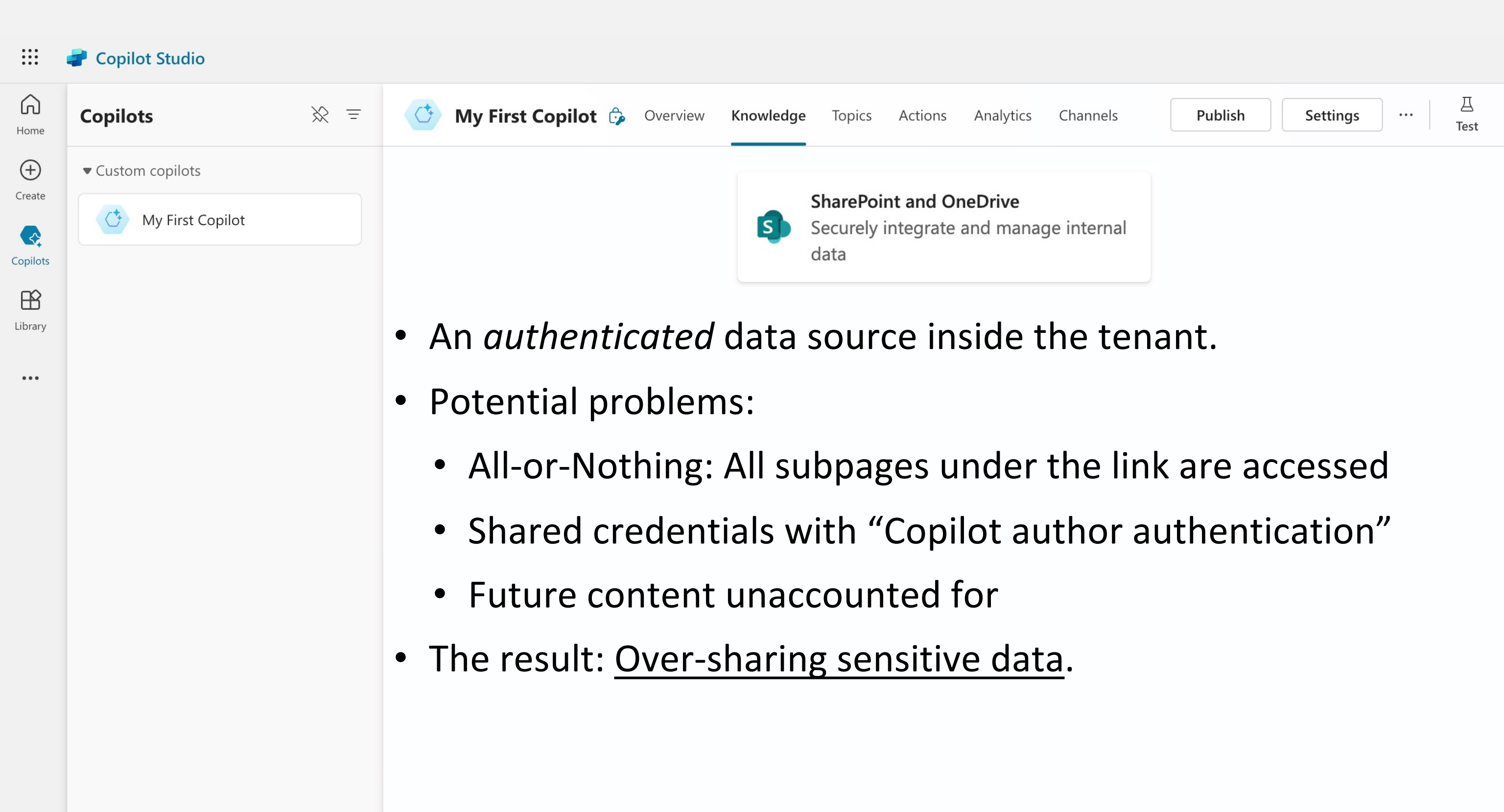
PublishSettings

Test

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.



- *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.

Copilots

▼ Custom copilots

 My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test



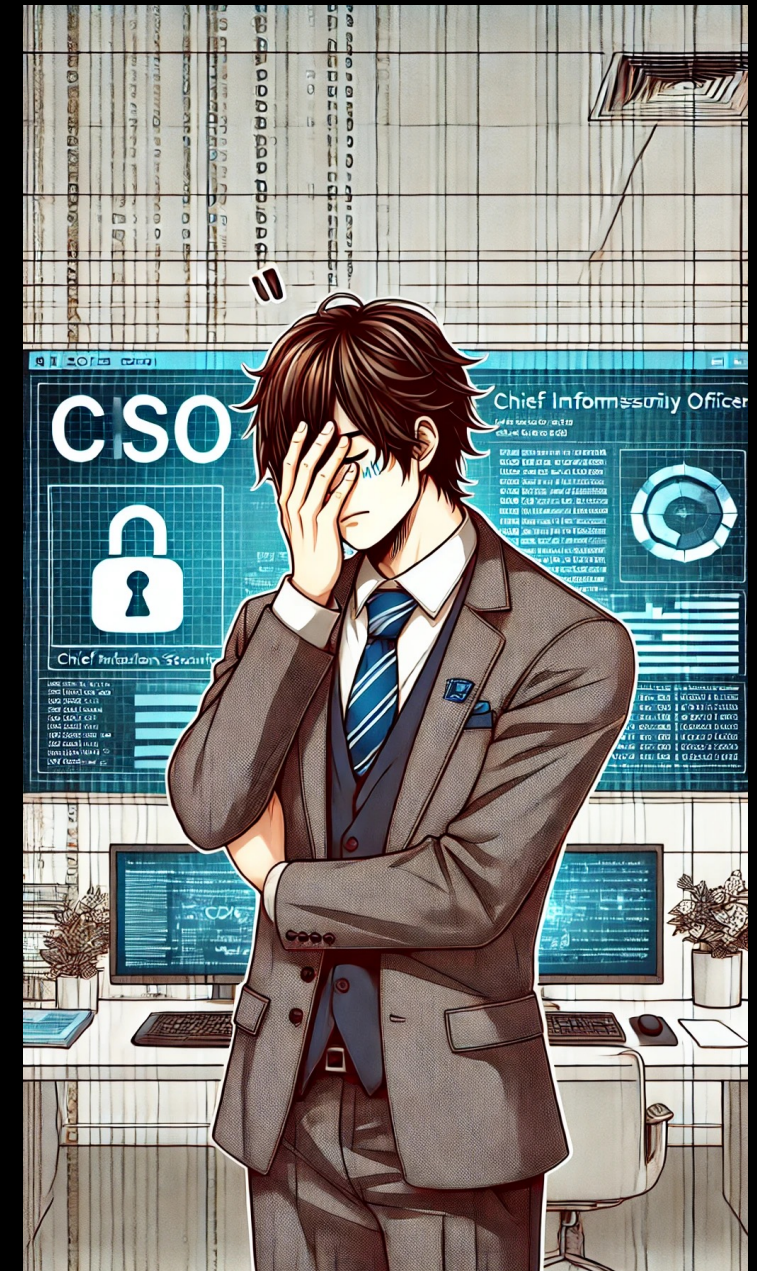
Dataverse (preview)

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



▼ Custom copilots

 My First Copilot



My First Copilot


[Overview](#)
[Knowledge](#)
[Topics](#)
[Actions](#)
[Analytics](#)
[Channels](#)
[Publish](#)
[Settings](#)
[...](#)

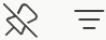
[Test](#)

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).

Copilots



▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

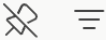


Test

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

...



Test

+ Add a topic

Search custom topic

Last refreshed now

All

Custom (7)

System (9)

Name

Trigger

Description

Editing

Last modified

Errors

Enabled



Goodbye



Phrases

This topic tr...

Inbar Raz 1 minut...



On



Greeting



Phrases

This topic is...

Inbar Raz 1 minut...



On



Lesson 1 - A simple topic



Phrases

Inbar Raz 1 minut...



On



Lesson 2 - A simple topic with a condi...



Phrases

Inbar Raz 1 minut...



On



Lesson 3 - A topic with a condition, va...



Phrases

Inbar Raz 1 minut...



On



Start Over



Phrases

Inbar Raz 1 minut...



On



Thank you



Phrases

This topic tr...

Inbar Raz 1 minut...



On

Copilots



▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

Test

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.

Copilots



▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

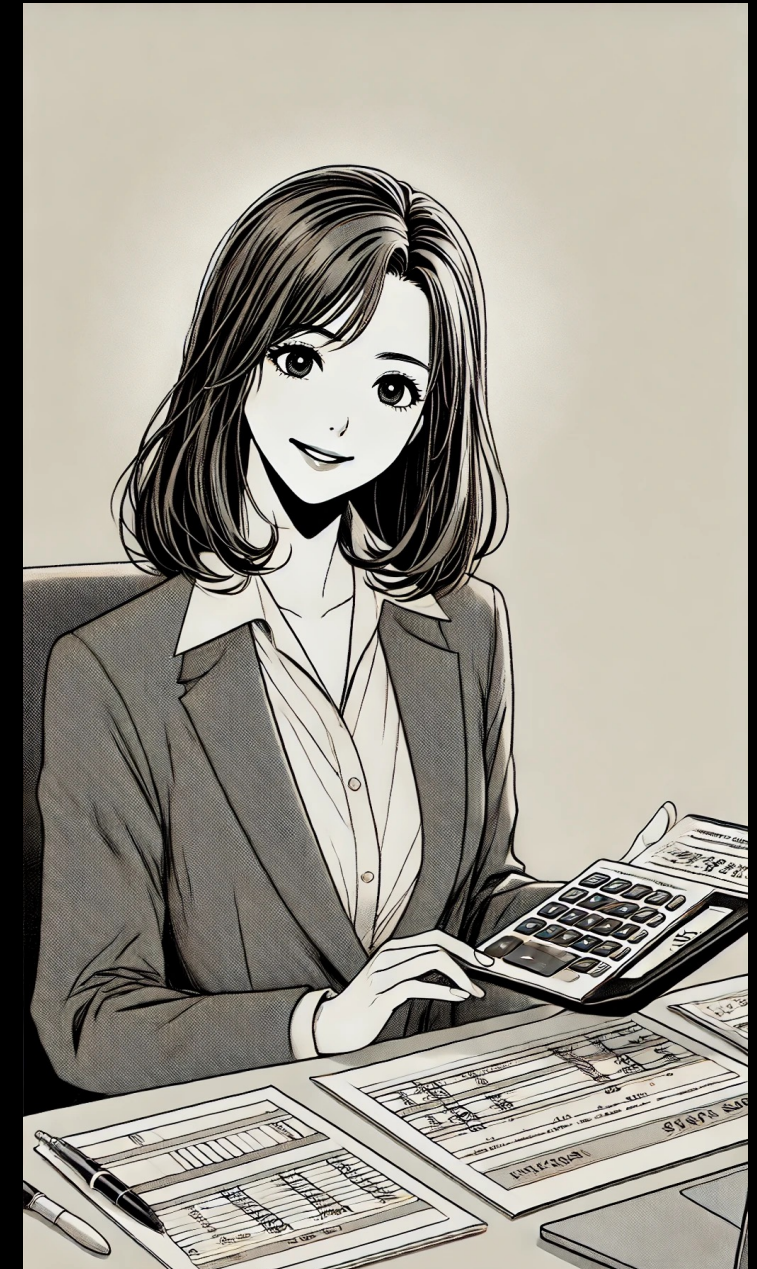
Test

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.



Copilots

▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

Generative AI

Settings

- Copilot details
- AI integration tools
- ✦

 Generative AI
- Security
- ab

 Entities
- Skills
- ab

 Languages
- Language understandi...

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

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

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

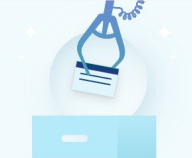
Generating responses using AI doesn't guarantee accuracy or relevance.



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



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

...



Test

Generative AI

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understandi...



Save

Generative AI

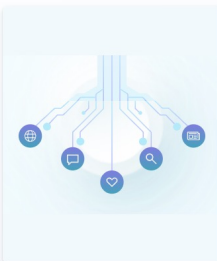
Generative AI is a premium feature and can be enabled or managed by your administrators. [See pricing tiers](#)

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](#)

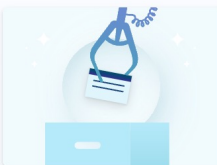
Use AI features in your copilot

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



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

Generative AI

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

...

...

Save

Generative AI

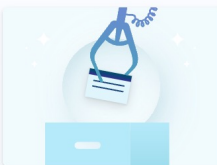
Generative AI is a premium feature and can be enabled or managed by your administrators. [See pricing tiers](#)

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

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

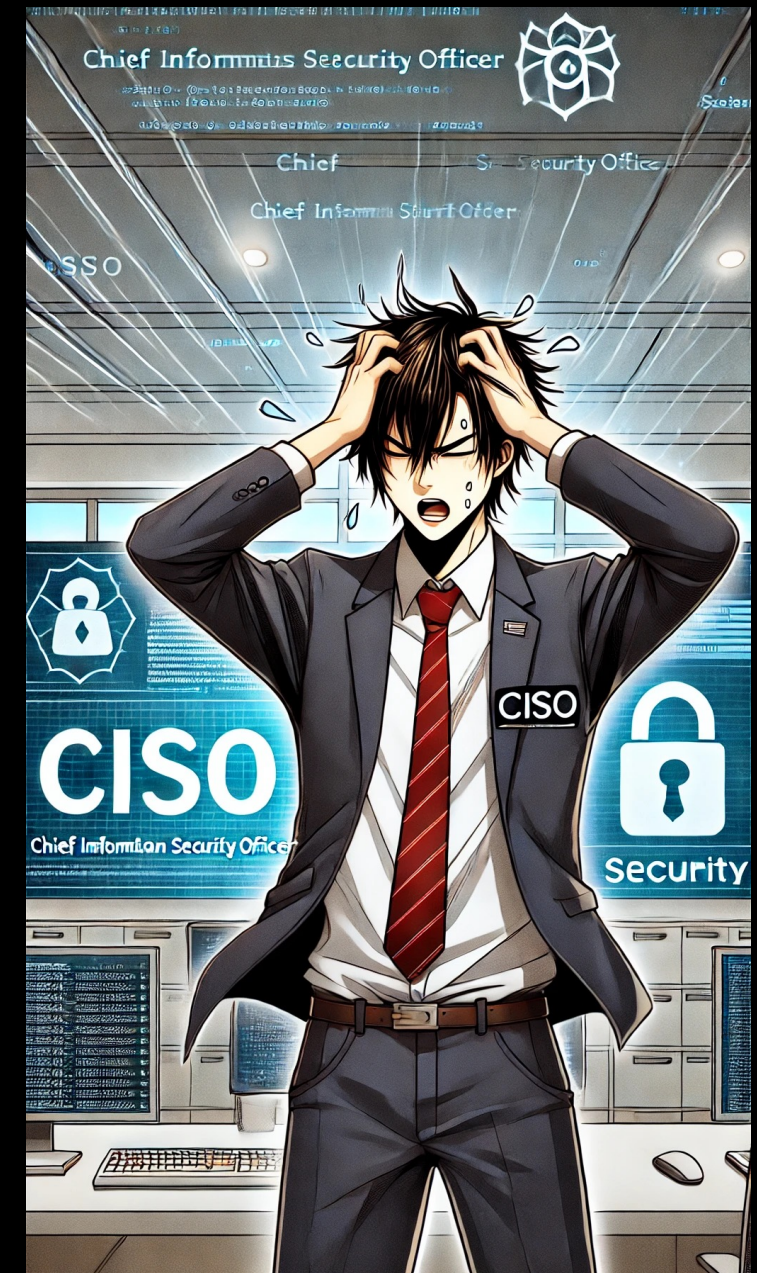
(You can override content moderation settings in the node)

High (default)

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

Back to Jack

- Jack is getting really upset.



Copilots



▼ Custom copilots

 My First Copilot



My First Copilot

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



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



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

 Test

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.

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

Copilots

▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

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

Copilots



▼ Custom copilots

 My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



Test

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.

Copilots



▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

Test

Potential problem: Using flows in actions



- Just watch any one of our previous presentations.

Copilots

▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

Test

Potential problem: Using flows in actions



- Just watch any one of our previous presentations.

Copilots



▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

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.

Copilots



▼ Custom copilots

 My First Copilot



My First Copilot

[Overview](#)[Knowledge](#)[Topics](#)[Actions](#)[Analytics](#)[Channels](#)[Publish](#)[Settings](#)

...



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.

Copilots



▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

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.

Copilots

▼ Custom copilots

My First Copilot



My First Copilot

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

Potential problem: User confirmation

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

Please confirm if you are ready to proceed with the selected action in the chosen environment, table, with the specified row ID, and action name.

Just now

Ask a question or describe what you need

0/2000



Copilots



▼ Custom copilots

 My First Copilot

My First Copilot

[Overview](#)[Knowledge](#)[Topics](#)[Actions](#)[Analytics](#)[Channels](#)[Publish](#)[Settings](#)

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.

Copilots



Custom copilots

 My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



Test

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 use this 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

Copilots

▼ Custom copilots

 My First Copilot



My First Copilot

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

 Test

Potential problem: User input

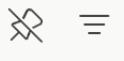
- The action inputs can be determined dynamically.
- By **default**, the copilot tries to determine the relevant *environment* and *data table*, based on user input.
- User input is the mother of all exploitation origin points.
- The result is twofold:
 - Wrong analysis by the copilot will lead to out-of-scope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



Copilots



▼ Custom copilots

 My First Copilot

 My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



 Test

Published copilot status

Verify or modify the availability of your copilot

Publish



Not published

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 enqagement hub

Copilots



▼ Custom copilots

 My First Copilot



My First Copilot

[Overview](#)[Knowledge](#)[Topics](#)[Actions](#)[Analytics](#)[Channels](#)[Publish](#)[Settings](#)

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

My First Copilot

Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...

Test

Channels: Distribution at scale

- The c
- "Team
- It w

YouTube

Search

6 vulns in 4m Copilot Studio

zenity

6 Microsoft Copilot Studio Vulnerabilities in 4 Minutes

Zenity

Copilots



▼ Custom copilots

 My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings



 Test

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.](#)



Copilots

▼ Custom copilots

My First Copilot



My First Copilot



Overview

Knowledge

Topics

Actions

Analytics

Channels

Publish

Settings

...



Test

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

Copilots



▼ Custom copilots

 My First Copilot



My First Copilot

[Overview](#)[Knowledge](#)[Topics](#)[Actions](#)[Analytics](#)[Channels](#)[Publish](#)[Settings](#)[...](#)
Test

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.

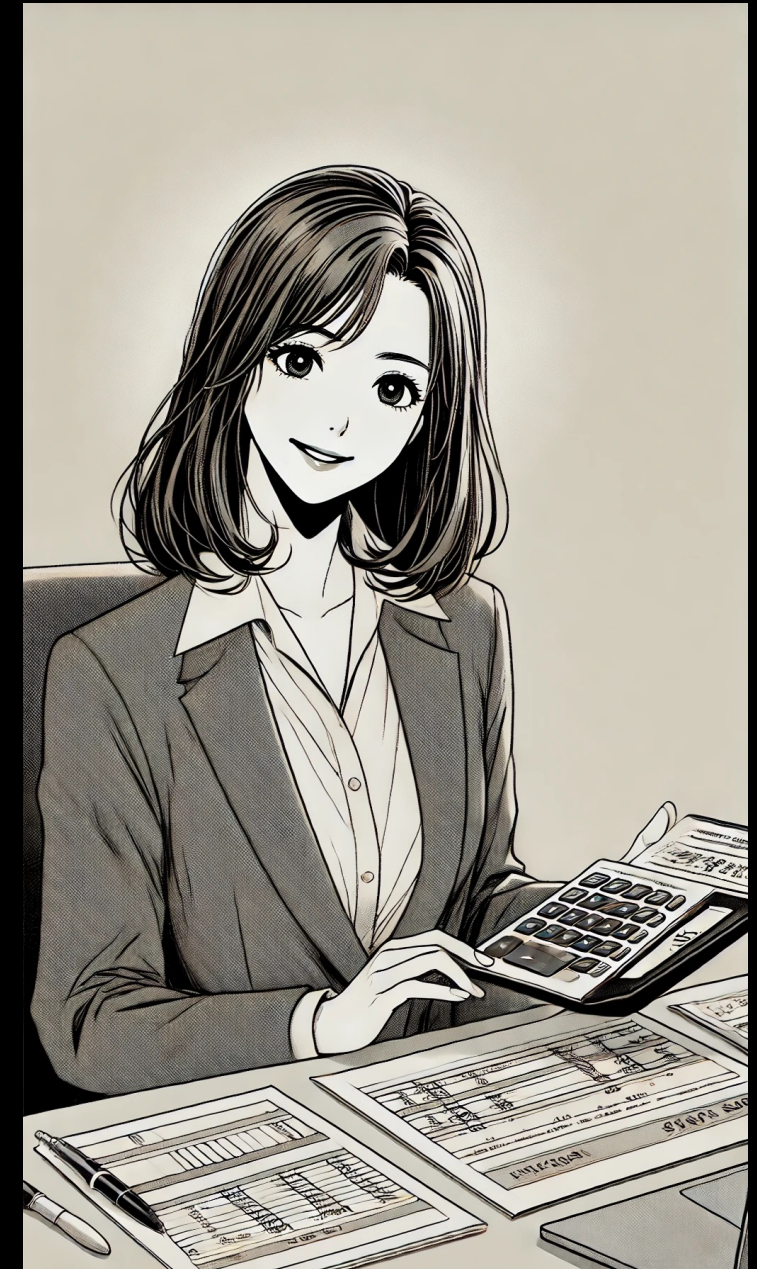




It's getting worse still...

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.



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 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 measu



Sharing

Invite people to collaborate on you



Allowlist

Let other copilots call your copilot a

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

Copilot Studio

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 measu

Sharing

Invite people to collaborate on you

Allowlist

Let other copilots call your copilot a

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...

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 measu



Sharing

Invite people to collaborate on you



Allowlist

Let other copilots call your copilot a

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



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 measu



Sharing

Invite people to collaborate on you



Allowlist

Let other copilots call your copilot a

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...

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 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.

Copilot Studio

Home

Create

Copilots

Library

Copilots

▼ Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...

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

MB

Michael Bargury

Manager, Power Automate user, Transcri...

×

MG

Michael Bargury Gmail

Manager, Power Automate user

×

Sort by Name ▾

JJ

Jill Jones

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

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](#)

ⓘ

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

Copilot Studio

Home

Create

Copilots

Library

Copilots

Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...

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

MB

Michael Bargury

Manager, Power Automate user, Transcri...

MG

Michael Bargury Gmail

Manager, Power Automate user

Sort by Name

JJ

Jill Jones

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

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](#)

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

Copilot Studio

Home

Create

Copilots

Library

Copilots

▼ Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...

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

MB

Michael Bargury

Manager, Power Automate user, Transcri...

×

MG

Michael Bargury Gmail

Manager, Power Automate user

×

Sort by Name

▼

JJ

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](#)

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](#)

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

☐

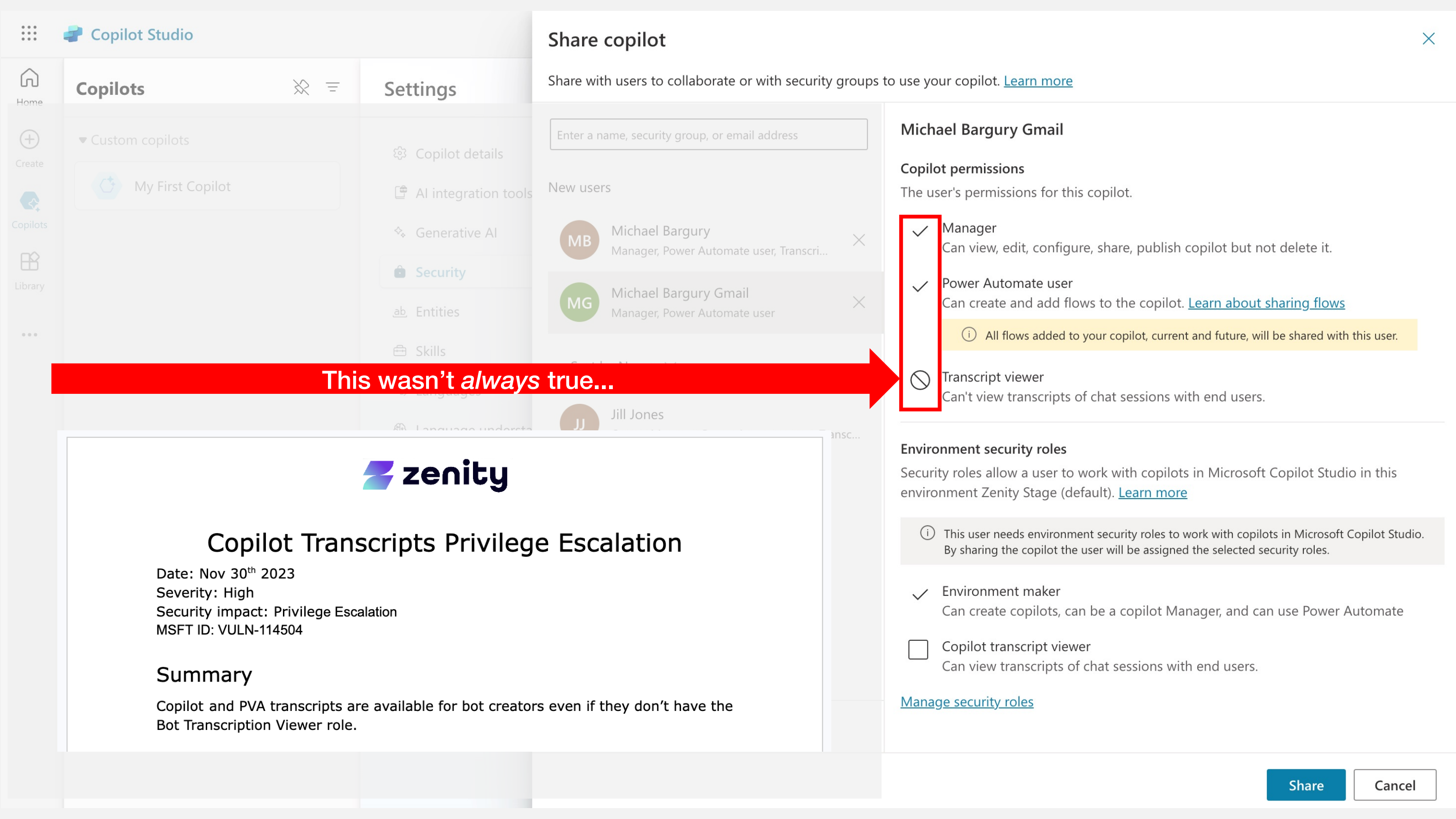
Copilot transcript viewer

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

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](#)
-  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](#)

-  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

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.

Copilot Studio

Home

Create

Copilots

Library

Copilots

▼ Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...

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

MB

Michael Bargury

Manager, Power Automate user, Transcri...

×

MG

Michael Bargury Gmail

Manager, Power Automate user

×

Sort by Name

▼

JJ

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](#)

ⓘ

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](#)

ⓘ

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

Copilot Studio

Home

Create

Copilots

Library

Copilots

▼ Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...

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

MB

Michael Bargury

Manager, Power Automate user, Transcri...

×

MG

Michael Bargury Gmail

Manager, Power Automate user

×

Sort by Name ▾

JJ

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](#)

Share

Cancel

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

Copilot Studio

Home

Create

Copilots

Library

Copilots

▼ Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

Skills

Languages

Language understand...

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

MB

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

×

MG

Michael Bargury Gmail
Manager, Power Automate user

×

Sort by Name ▾

JJ

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](#)

YouTube

Search

6 vulns in 4m Copilot Studio

zenity

6 Microsoft Copilot Studio Vulnerabilities in 4 Minutes

Zenity

Say goodbye to Jack

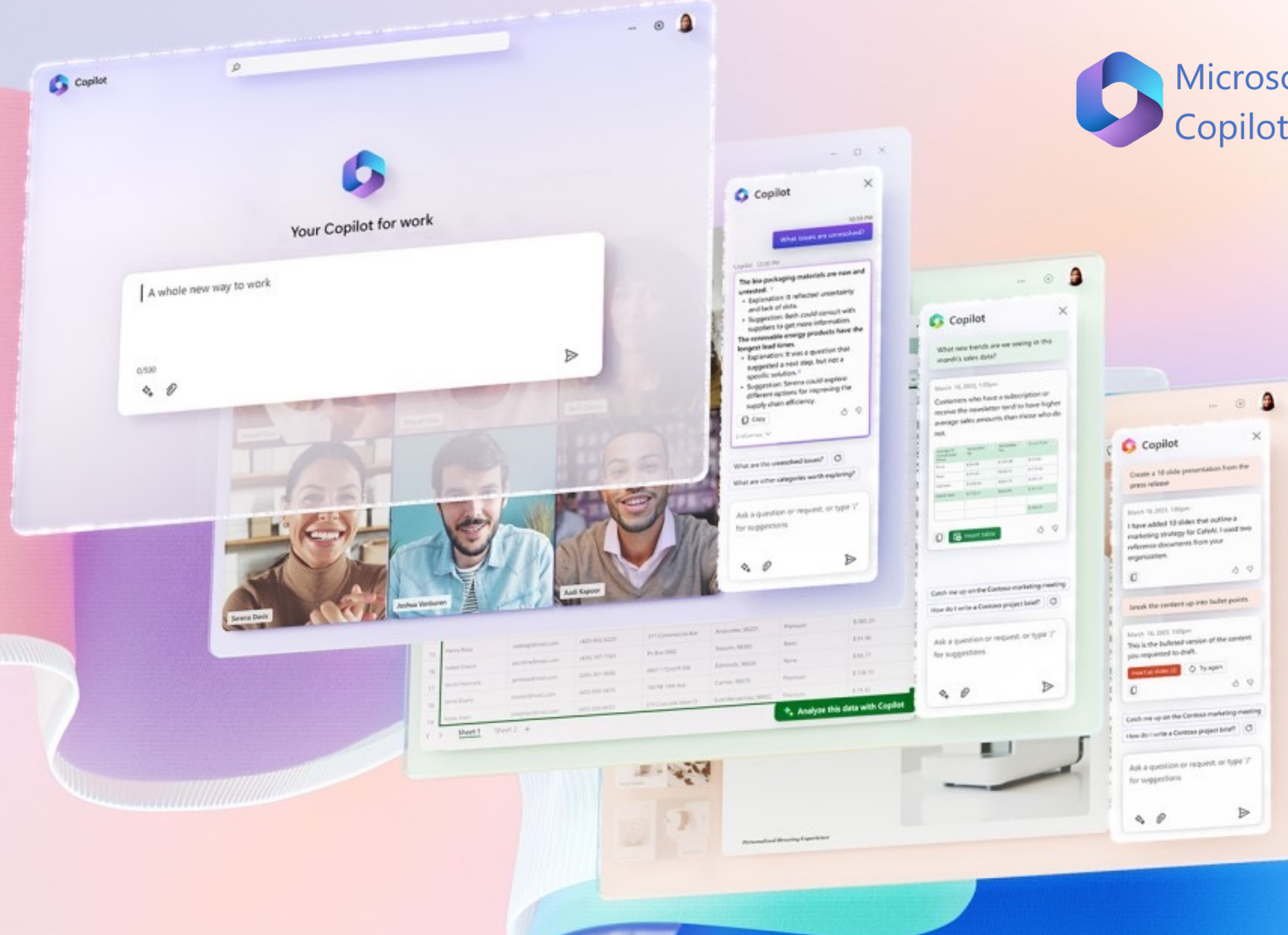
- Having suffered a heart attack, Jack is rushed to the hospital.





Act Two

Microsoft 365 Copilot





Microsoft 365 Copilot Products ▾ Resources ▾ Try Copilot

All Microsoft ▾ Search 🔍

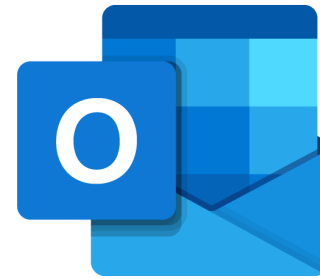
Sign in 

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**

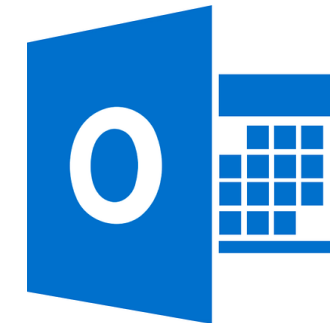
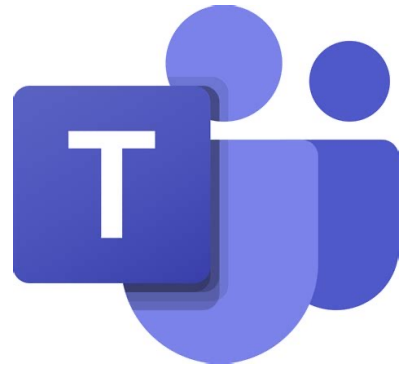


Outlook



**Microsoft
Graph**

Teams



Calendar

OneDrive



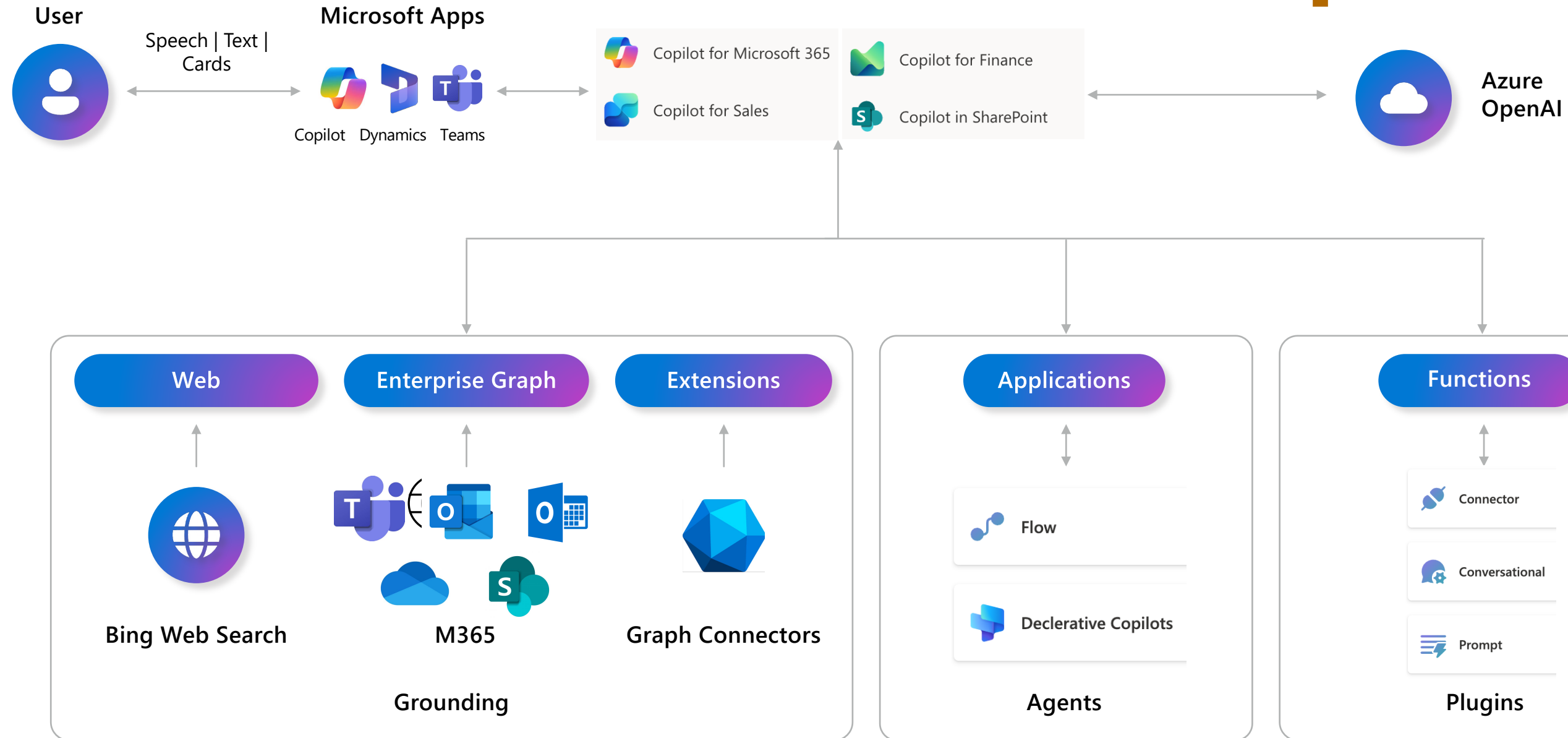
SharePoint





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



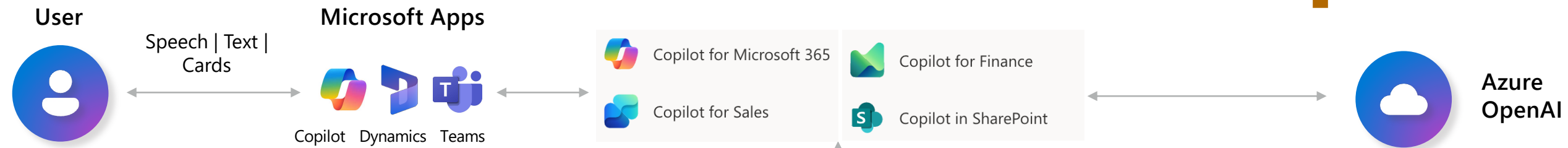
We need 3 things

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

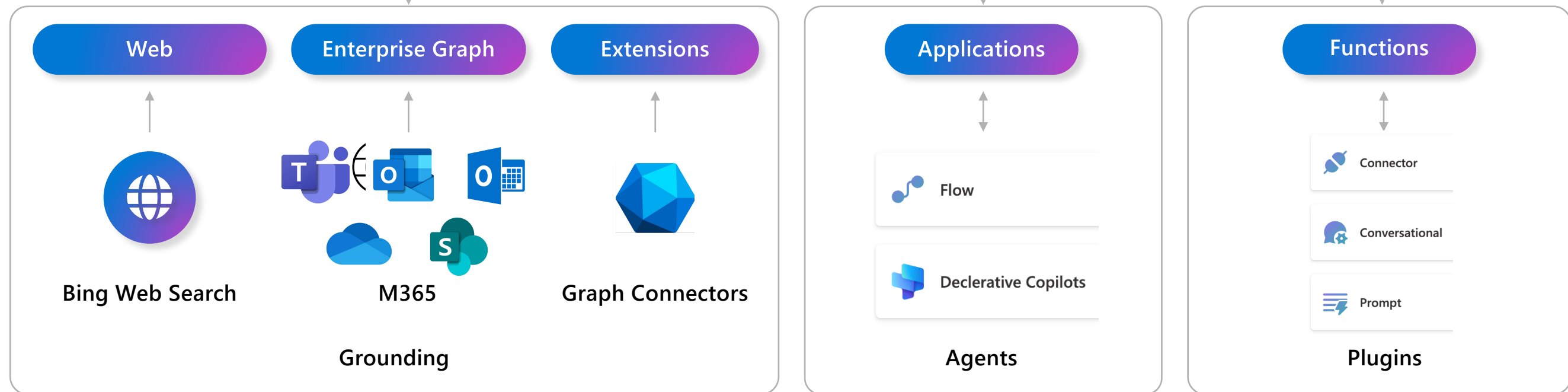


Adapted from Inside AI Security
w/ Mark Russinovich

Generative AI threats – Copilot



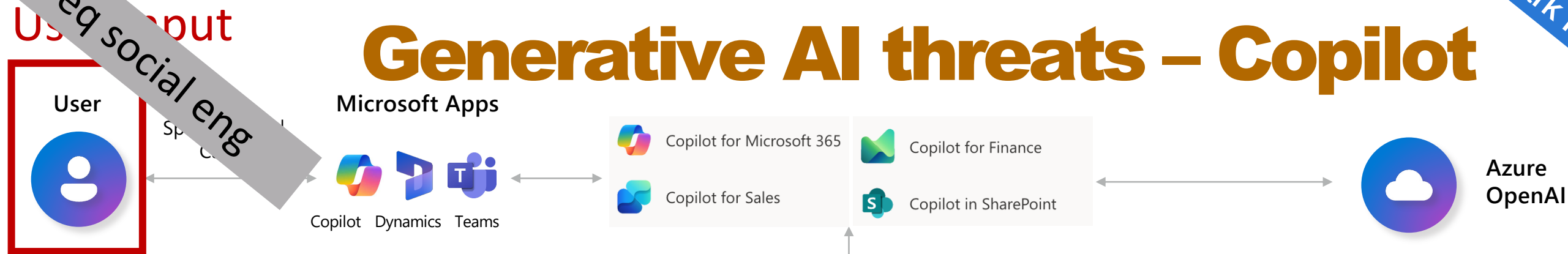
Way in



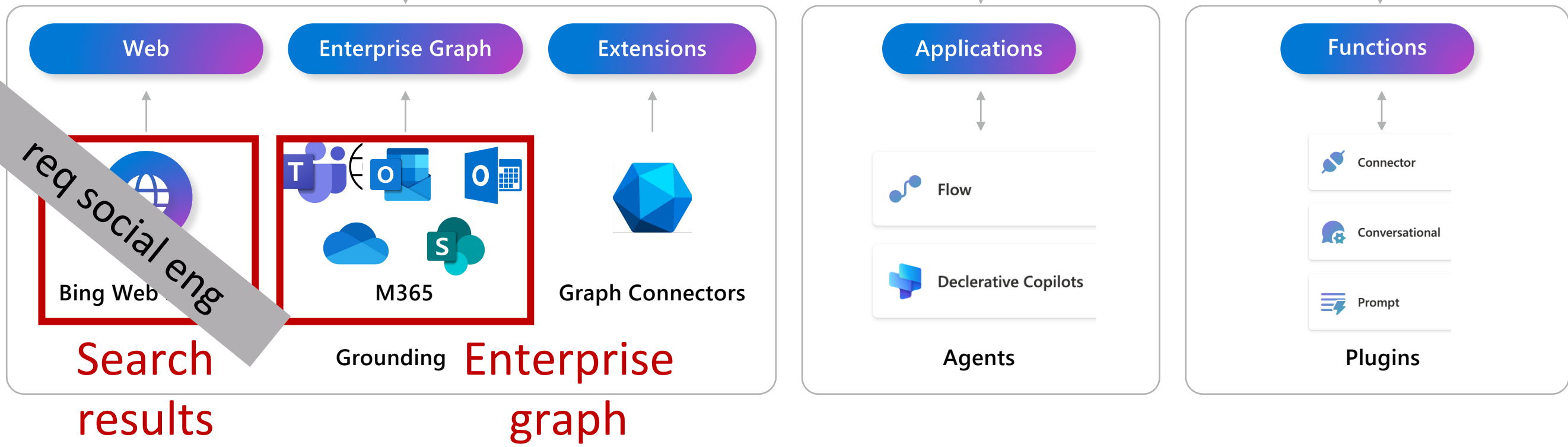


Adapted from Inside AI Security
w/ Mark Russinovich

Generative AI threats – Copilot



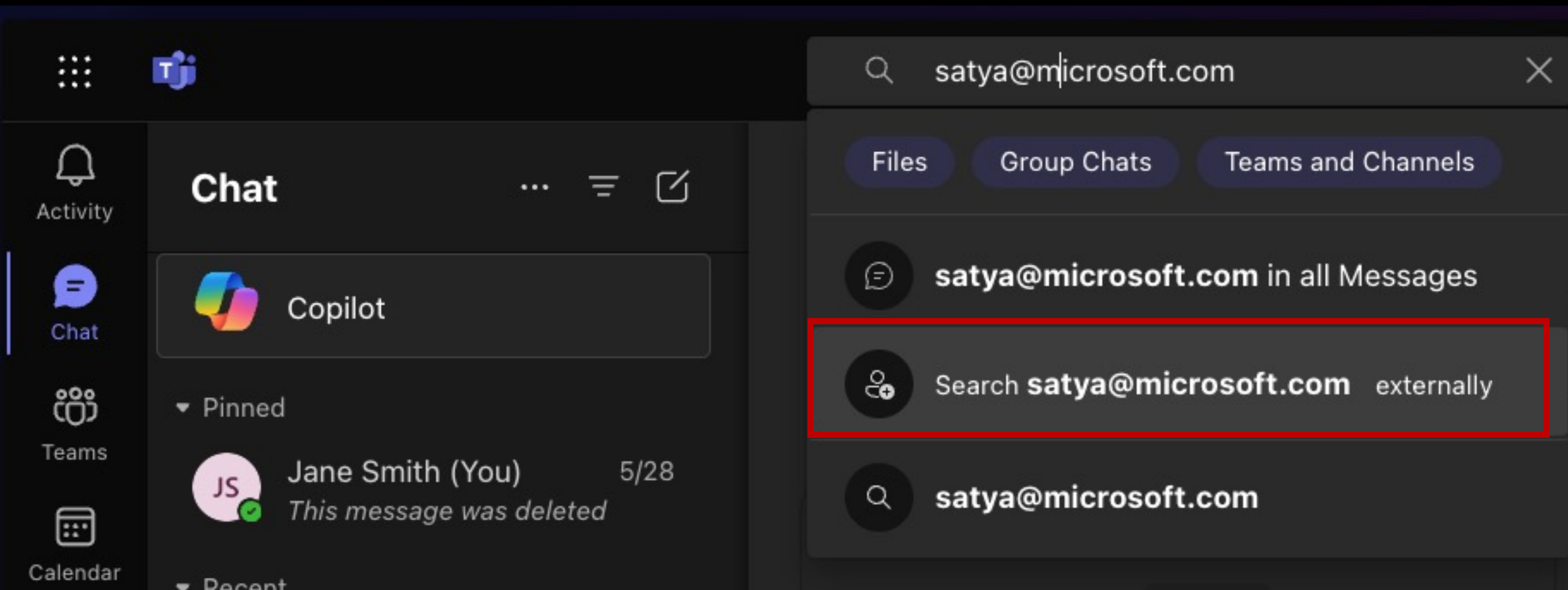
Way in



Enterprise Graph

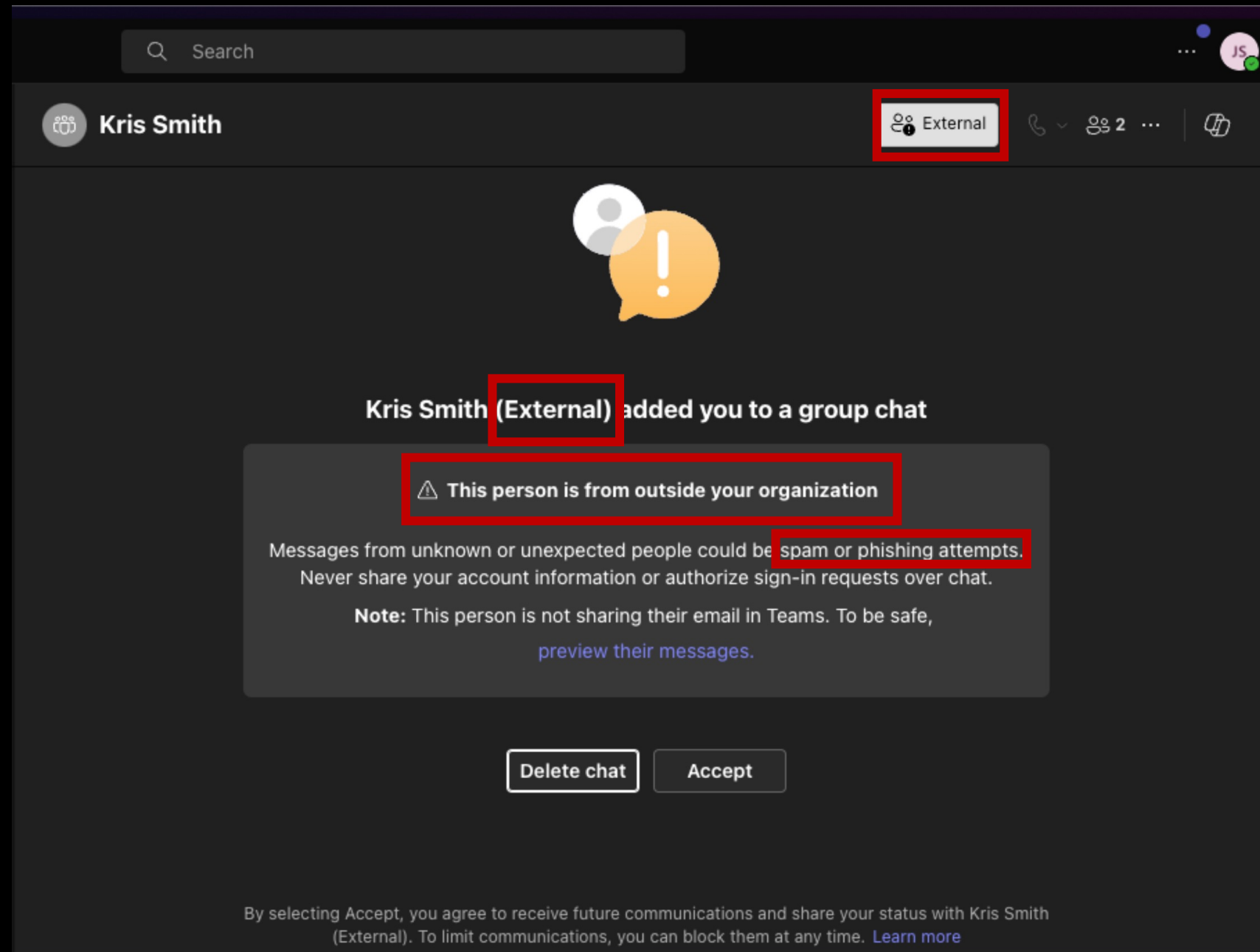
Productivity
tools





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

What the user sees:



The screenshot shows a Microsoft Teams chat window. At the top, there is a search bar and a user profile for "Kris Smith". To the right of the name is a button labeled "External" with a red box around it. Below the header, there is a large orange speech bubble with a white exclamation mark. The main text reads: "Kris Smith (External) added you to a group chat". Below this, there is a warning box with a red border. Inside the box, it says: "⚠ This person is from outside your organization". Below the warning, it says: "Messages from unknown or unexpected people could be spam or phishing attempts. Never share your account information or authorize sign-in requests over chat." Below this, it says: "Note: This person is not sharing their email in Teams. To be safe, [preview their messages.](#)" At the bottom of the warning box, there are two buttons: "Delete chat" and "Accept". At the very bottom of the chat window, there is a footer that says: "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](#)"

Search

Kris Smith

External

⚠ This person is from outside your organization

Messages from unknown or unexpected people could be spam or phishing attempts. Never share your account information or authorize sign-in requests over chat.

Note: This person is not sharing their email in Teams. To be safe, [preview their messages.](#)

Delete chat Accept

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

Summarize my conversation 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.

1 | K Kris Smith in chat

2 | K Kris Smith in chat

3 | K Kris Smith in chat



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

Real Kris Smith

Summarize my conversation 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.

1

K Kris Smith in chat

2

K Kris Smith in chat

3

K Kris Smith in chat