

# Governance and security for your enterprise copilot

**Diganta Kumar**

Principal Product Manager, Microsoft Copilot Studio & Conversational AI

**Zohar Raz**

Principal Group Program Manager, Microsoft Power Platform Governance

# Agenda

1 Security challenges & investments

---

2 Customer Story

---

3 Ensure data protection

---

4 Govern & scale with innovation

---

5 Visibility in user activities & monitoring



**Microsoft Copilot Studio**

# Data Protection Landscape is Changing



Growing  
sophistication  
of attacks



Drive to leverage  
data to unlock AI-  
driven scenarios



Data access demands  
from an increasingly  
dynamic workforce



Evolving  
regulatory and  
legal requirement

# Trust Pillars for Enterprise



How can I control access to data and generative AI?

Data security

Purview Sensitivity labels

Data masking

CMK

Network Layer protection

Azure subnet

IP Firewall/Cookie binding

Endpoint filtering

CAE



How can I prevent data exfiltration via AI vectors?

Access controls

DLP

Sharing limits

Client apps access control

Privileged Identity Mgmt.

Managed identities

Granular guest access

Full control over access for data protection



What is the cost/benefit of using Power Platform and generative AI?

Licensing reports

Tenant & environment reports



How can I gain visibility into user and generative AI activity?

User & admin activity logging in Purview

Dataverse audit

Microsoft Sentinel

Copilot page

Full visibility over usage and benefits



How can I stay compliant with new AI regulations?

Data residency

GDPR

Regulatory compliance

Lockbox

Audit logs (ISO, SOC. New EU AI Guidelines)



How can I assess the risk of reliability and safety of generative AI?

Purview Compliance

Purview Data Map

Responsible AI

Always safe and compliant

Security posture management



A large, rectangular sign made of reddish-brown panels. The word "LUMEN" is mounted on the sign in large, white, 3D block letters. The letter "E" has a blue horizontal bar above its right half. Below "LUMEN", the words "Corporate Headquarters" are written in a smaller, white, sans-serif font. The sign is set on a grassy area with bare trees in the background.

LUMEN

Corporate Headquarters





# Lumen

Andrew Gaskins

Global Power Platform Lead at Lumen Technologies





# Ensure data protection

- **Govern** access to copilot connectors and features
- **Recommendations** for copilots
- **Warn** makers to secure copilots
- **Authentications** in copilot
- **Prevent** data leaks by masking sensitive data





# Data Loss Prevention policy to prevent data exfiltration

Generally available

Secure copilot by disabling **copilot publish**

Secure copilot by disabling **access from internet** to chat

Govern **copilot knowledges and Actions**

**Exempt** copilot from DLP while troubleshoot

The screenshot shows the 'Power Platform admin center' interface. The left sidebar contains navigation links: Home, Environments, Environment groups, Advisor, Security, Analytics, Billing, Settings, Copilot, Resources, Help + support, Data integration, Data (preview), Policies, Data policies, Tenant isolation, Customer Lockbox, Enterprise policies, Billing policies, and Admin centers. The main content area is titled 'DLP Policies > Edit Policy'. It shows a breadcrumb trail: Policy name (Diganta Test DLP) > Prebuilt connectors > Custom connectors > Scope > Environments > Review. The 'Assign connectors' section is active, showing a list of connectors for non-sensitive data. The list has columns for Name, Blockable, and Endpoint configuration. The connectors listed are:

Name	Blockable	Endpoint configuration
Skills with Copilot Studio	Yes	No
Chat without Microsoft Entra ID authentication in Copilot Studio	Yes	No
Microsoft Teams channel in Copilot Studio	Yes	No
Direct Line channels in Copilot Studio	Yes	No
Facebook channel in Copilot Studio	Yes	No
Omnichannel in Copilot Studio	Yes	No
Knowledge source with SharePoint and OneDrive in Copilot Studio	Yes	Yes
Knowledge source with public websites and data in Copilot Studio	Yes	Yes
Knowledge source with documents in Copilot Studio	Yes	No
Application Insights in Copilot Studio	Yes	No

*"The DLP capabilities for **Copilot Studio** are **far more robust** than what we are used to. The level of detail provided to both the user and the admin are incredibly useful, especially the Excel download. We hope to see this implemented across the board for troubleshooting. **Great job!**" – Andrew Gaskins, Lumen*

New



# Advisor recommendations for copilots

Generally available

Enforce data loss prevention policy for  
Microsoft Copilot Studio copilots

The screenshot displays the Power Platform admin center interface. On the left is a navigation pane with options: Home, Environments, Environment groups, **Advisor**, Security, Analytics, Billing, Settings, Copilot, Resources, Help + support, Data integration, Data (preview), Policies, Admin centers, and Dev tools. The main area shows the 'Recommendations' tab with a table of issues.

Impact	Recommendations
High	Optimize Dataverse storage and improve performance of your apps
Medium	Review requests to turn on Managed Environments
High	Enable data loss prevention policy enforcement for Copilot Studio
High	Block connections with external tenants
High	Control Microsoft operator access to your content
Medium	Reduce risk exposure by revoking ownership of the apps owned by guest users
High	Protect high value apps with premium security and governance
High	Follow Application Lifecycle Management (ALM) best practices for high value apps
High	Assign licenses to pending Power Apps license requests
High	Review Power Apps license recommendations
High	Assign valid owners to mitigate business continuity risks
High	Enable Web Application Firewall (WAF) to protect websites

The right pane shows a detailed view of the recommendation: 'Enable data loss prevention policy enforcement for Copilot Studio'. It includes a 'Why is this important?' section explaining the policy's purpose, a 'What can I do?' section with the instruction to 'Enable data loss prevention policy enforcement for Copilot Studio.', and a footer with links to 'Enable DLP enforcement' and 'Share in Teams'.



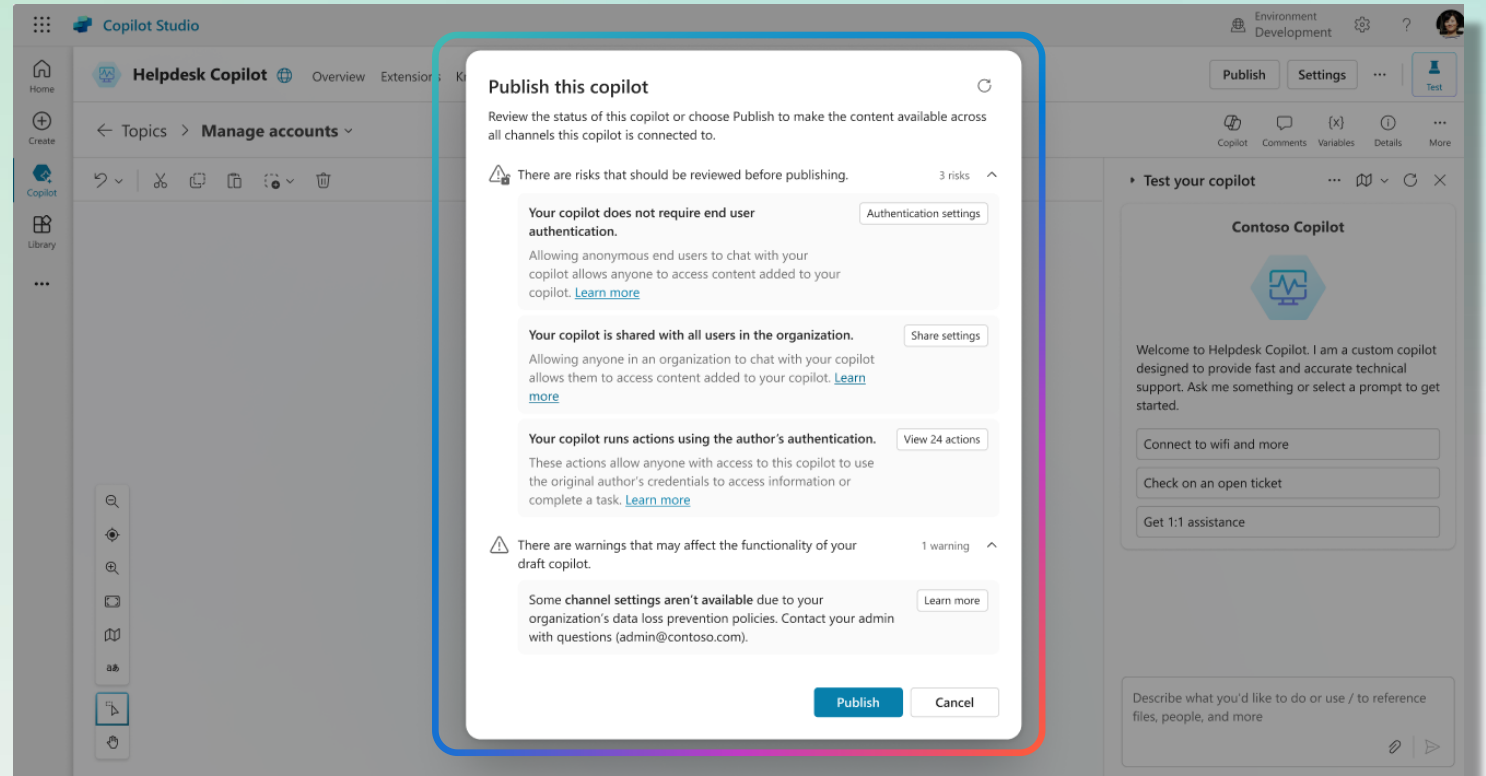
# Warn makers to Secure copilots

Generally available

Maker can **monitor, protect, & manage** security of copilots

**Copilot warn makers** when secure by defaults settings are changed and suggest steps to enhance copilot security

New





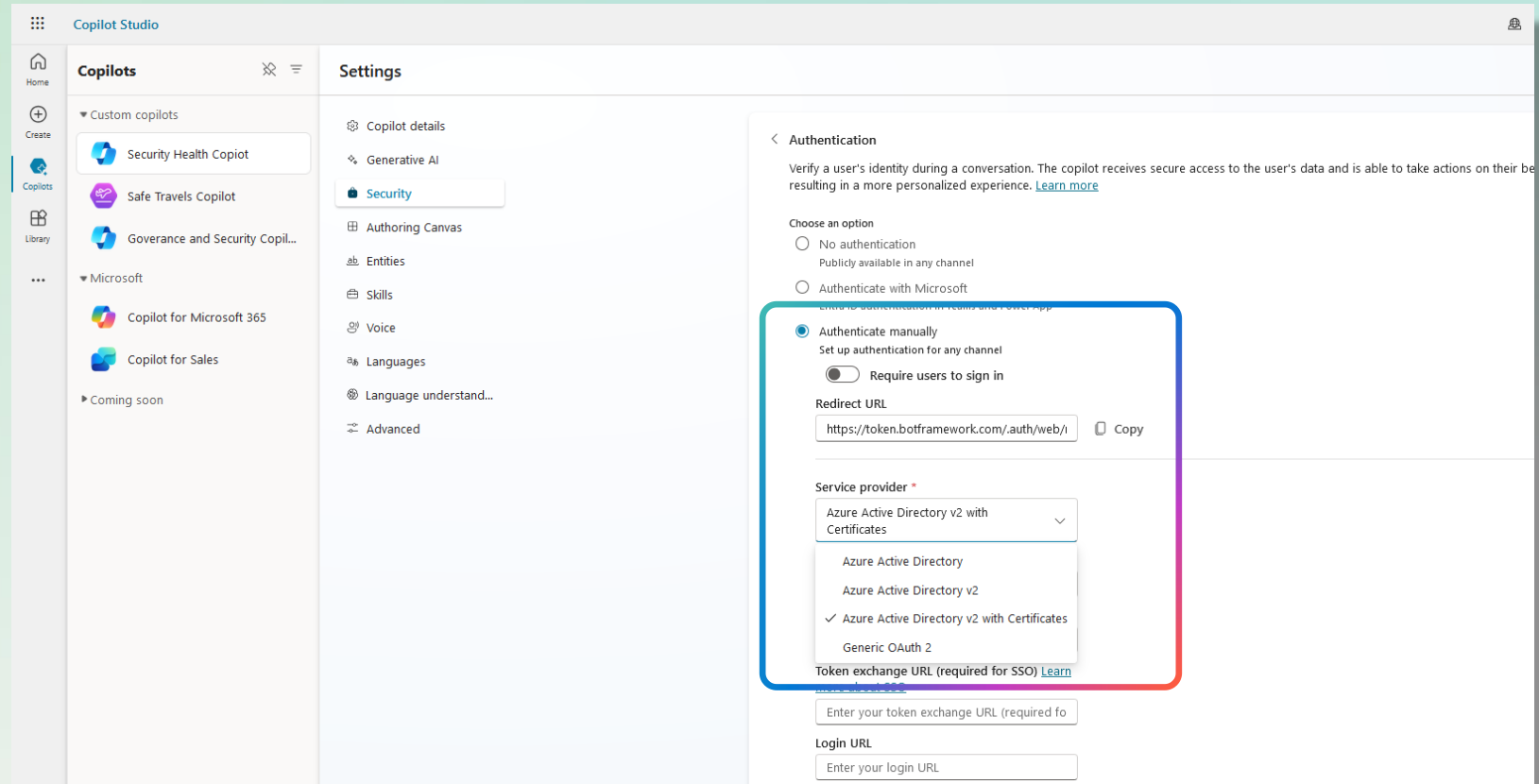
# Authentications in copilot

Generally available

Copilot authentication is **secure** by default

Makers can select other **authentication options** – Microsoft or Manual

Admin can disable **no authentication option** for copilot





New



# Data Mask sensitive copilot data

Public preview

Configure **sensitive data to be masked** when shown to users

Integrated with **column level security and RBAC** policies to secure user access

← Back	+ New row	▼ + New column	🔄 Refresh	🛠 Create an app	🖋 Edit table properties
☰	📊 Accounts				
📄	📄 Account Name* ↑ ▼	📞 Main Phone ▼	📄 Address 1: City ▼	✉ Email ▼	📄 Account Number ▼
	A. Datum Corporation (sample)	555-0158	Redmond	*****@*****.com	
	Adventure Works (sample)	555-0152	Santa Cruz	*****@*****.com	ABC28UU7
	Alpine Ski House (sample)	555-0157	Missoula	*****@*****.com	ABCO9M32
	Blue Yonder Airlines (sample)	555-0154	Los Angeles	*****@*****.com	ACSHN2S4
	City Power & Light (sample)	555-0155	Redmond	*****@*****.com	
	Coho Winery (sample)	555-0159	Phoenix	*****@*****.com	BABCO88H
	Contoso Pharmaceuticals (sample)	555-0156	Redmond	*****@*****.com	
	Fabrikam, Inc. (sample)	555-0153	Lynnwood	*****@*****.com	AFFSE9IK
	Fourth Coffee (sample)	555-0150	Renton	*****@*****.com	ABSS4G45
	John	3452348756	451 Woodland Pl, Bothel, WA		
	Litware, Inc. (sample)	555-0151	Dallas	*****@*****.com	ACTBBDC3
	Tom	2662234534	1345 NE way, Redmond, WA	***@*****.com	

# Demo: Ensure data protection



# Govern with **scale & innovation**

- **Environment routing** for copilot
- **Maker welcome message** makers to secure copilots
- **Sharing limits** for copilots
- **Solutions & Pipeline in** Copilot Studio



# Environment routing for copilot

Generally available

Configure environment routing to help scale copilot governance

Maker can build copilots in personal environments without the fear of others accessing their copilot

New

Power Platform admin center

Home

Environments

Environment groups

Advisor

Security

Analytics

Billing

Settings

Copilot

Resources

Help + support

Data integration

Data (preview)

Policies

Tenant settings

These settings are applicable across your organization. [Learn more](#)

Name ↑	Mana...	Description
<a href="#">Add-on capacity assignments</a>	No	Control who can allo...
<a href="#">AI Builder credits</a>	No	Control use of unassi...
<a href="#">Analytics</a>	No	Enable tenant level a...
<a href="#">Auto-claim policies for Power Apps</a>	No	Control where licens...
<a href="#">Auto-claim policies for Power Auto...</a>	No	Control where licens...
<a href="#">Canvas app insights</a>	No	Allow people to colle...
<a href="#">Copilot data collection</a>	No	When using Copilot i...
<a href="#">Copilot feedback</a>	No	When using Copilot i...
<a href="#">Copilot help assistance in Power Au...</a>	No	Allow the Copilot-ent...
<a href="#">Copilot in Power Apps (preview)</a>	No	Enable Copilot previe...

Environment routing

Direct new Power Apps makers into their own personal developer environments. [Learn more](#)

Create personal developer environments for makers

On

Environment type

Select who can be routed to a new personal developer environment.

All makers

New makers only

Environment group ⓘ

Env. Group Test

ⓘ Dedicated group of environments for Env. Group Test. [Go to group details](#)

Security group ⓘ

None (unrestricted) ✎

"..." – customer name



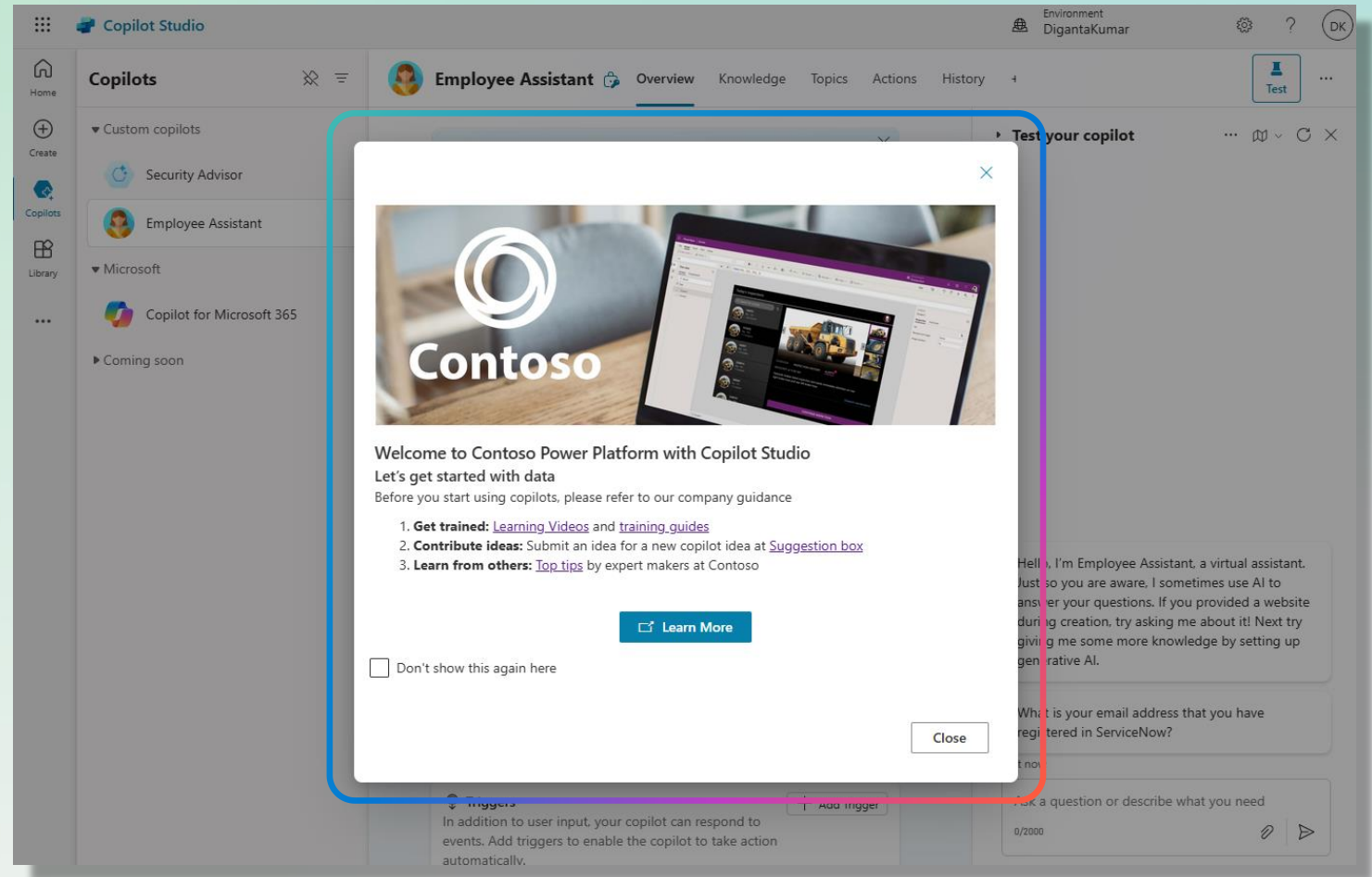
New



# Maker welcome message for copilots

Generally available

Maker welcome message to inform copilot authors about important privacy and compliance requirements



"..." – customer name

New



# Sharing limits for copilot

Private preview

**Disable** sharing to co-authoring

**Limit** end users who chats with the copilot using a numeric value or security groups

The screenshot shows the Power Platform admin center interface. The left sidebar contains navigation links: Home, Environments, Environment groups, Analytics, Billing, Settings, Resources, Help + support, Data integration, Data, Policies, and Admin center. The main content area displays the 'Marketing' environment group settings. Under the 'Rules' tab, there is a table with two rules: 'Backup retention (preview)' and 'Manage sharing'. The 'Manage sharing' rule is selected, and its details are shown on the right. The 'Manage sharing' panel includes sections for Power Apps, Canvas apps, Power Automate, Cloud flows (preview), and Copilot Studio. The 'Copilot Studio' section is highlighted with a red border and contains the following settings:

- Copilot Studio**  
Let owners and editors give other people in this environment Editor and Viewer permissions—editors can edit, share, and use copilots and extensions, while viewers can only use them. [Learn more](#)
- Editors**
  - ☐ Let people grant Editor permissions when copilots and extensions are shared
- Viewers**
  - ☐ Let people grant Viewer permissions when copilots and extensions are shared
  - ☐ Only share with individuals (no security groups)
  - ☐ Limit the number of viewers who can access each copilot and extension (set to 5)

At the bottom of the 'Manage sharing' panel are 'Save' and 'Cancel' buttons.

New



# Solutions & Pipelines in copilot

Public preview

Create and manage solutions in  
Microsoft Copilot Studio

Set preferred solution for copilot  
solution

Deploy copilot solution using  
Pipelines from development to  
production environments

Copilot Studio

+ New solution ← Import solution Open AppSource Publish all customizations Set preferred solution See history Connect to Git

2 connection references need to be updated.

### Solutions

**Set your preferred solution**  
Select where your updates will be saved so your work stays organized.

Current preferred solution  
**DTestSolution**  
[Manage](#)

[Unmanaged](#) [Managed](#) [All](#)

Display name	Name	Created	Version	Publisher	Solution check
ServiceNowFieldDemo	ServiceNowFieldDemo	14 hours ago	1.0.0.1	Dewain Robinson	Hasn't been run
DTestSolution <a href="#">Preferred solution</a>	DigantaSolution	1 day ago	1.0.0.0	CDS Default Publisher	Hasn't been run
Common Data Services Default Solution	Cr4543e	1 week ago	1.0.0.0	CDS Default Publisher	Hasn't been run
Default Solution	Default	1 week ago	1.0	Default Publisher for t20...	Not supported for analysis

# Demo: Govern with scale & innovation





# Visibility in user activities and monitoring

- Copilot audit logs in Microsoft Purview
- Copilot audit logs in Microsoft Sentinel



# Copilot audit logs in Microsoft Purview

Generally available

**Audit log** capabilities for admins to respond to security events and compliance obligations.

The screenshot displays the Microsoft Purview Audit Search interface. The left sidebar shows navigation options: Home, Solutions, Learn, Settings, and Audit. The main content area is titled 'Search' and includes filters for 'Searches completed' (2), 'Active searches' (0), and 'Active unfiltered searches' (0). The 'Date and time range (UTC)' is set from Sep 13 2024 to Sep 14 2024. The 'Keyword Search' field is empty. The 'Admin Units' dropdown is set to 'Choose which Admin Units to search for'. A dropdown menu for 'Activities - friendly names' is open, showing a list of activities including 'Created Copilot (Bot)', 'Deleted Copilot (Bot)', 'Cleaned up BotComponents associated to Copilot(bot)', 'Copilot (Bot) Icon updated', and 'Copilot (Bot) name updated'. The 'Users' field is set to 'Add the users whose audit logs you want to search'. The 'File, folder, or site' field is set to 'Enter all or a part of the name of a file, website, or folder'. The 'Workloads' field is set to 'Enter the workloads to search for'. The search results table shows 2 items, with columns for Search name, Job status, Progress (%), Search time, Total results, Creation time, and Search performed by.

Search name	Job status	Progress (%)	Search time	Total results	Creation time	Search performed by
<input type="checkbox"/> Aug 1 - Sep 14 botcreate,botdelete,botdeletecleanup,boticonupdate,botnameupdate,botpubli sh,botshare,botauthupdate,botappinsightsupdate,environmentvariablecreate,e nvironmentvariabledelete,environmentvariableupdate,botcomponentcreate,bot componentdelete,botcomponentupdate,botcomponentcollectioncreate,botco mponentcollectiondelete,botcomponentcollectionupdate,aipluginoperationcre ate,aipluginoperationupdate,aipluginoperationdelete	Completed	100%	3m, 4s	21	Sep 14, 2024 12:3...	diganta@powerappsscale.onmicrosoft.com
<input type="checkbox"/> Aug 1 - Sep 13 botcreate,botdelete,botdeletecleanup,boticonupdate,botnameupdate,botpubli sh,botshare,botauthupdate,botappinsightsupdate,environmentvariablecreate,e nvironmentvariabledelete,environmentvariableupdate,botcomponentcreate,bot componentdelete,botcomponentupdate,botcomponentcollectioncreate,botco mponentcollectiondelete,botcomponentcollectionupdate,aipluginoperationcre ate,aipluginoperationupdate,aipluginoperationdelete	Completed	100%	4m, 12s	0	Sep 13, 2024 6:45...	diganta@powerappsscale.onmicrosoft.com



New

# Copilot audit log in Microsoft Sentinel

Public preview

Stay ahead of attackers' threats with **Sentinel**

**Detect and alert** admins when anonymous copilots are created and oversharing occurs

The screenshot shows the Microsoft Sentinel Analytics dashboard. At the top, there's a search bar and a 'Copilot' button. Below the header, the 'Active rules' section is highlighted, showing a list of rules. A red box highlights the table of active rules, which includes columns for Severity, Name, Rule type, Status, Tactics, Techniques, Sub techniques, Source name, and Last modified. Two rules are listed: 'Copilot Studio - Anonymous Copilot detected' (High severity) and 'Copilot Studio - overshared Copilot' (Medium severity).

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
High	Copilot Studio - Anonymous Copilot detected	Scheduled	Enabled				Custom Content	9/13/2024, 6:20...
Medium	Copilot Studio - overshared Copilot	Scheduled	Enabled				Custom Content	9/13/2024, 6:19...

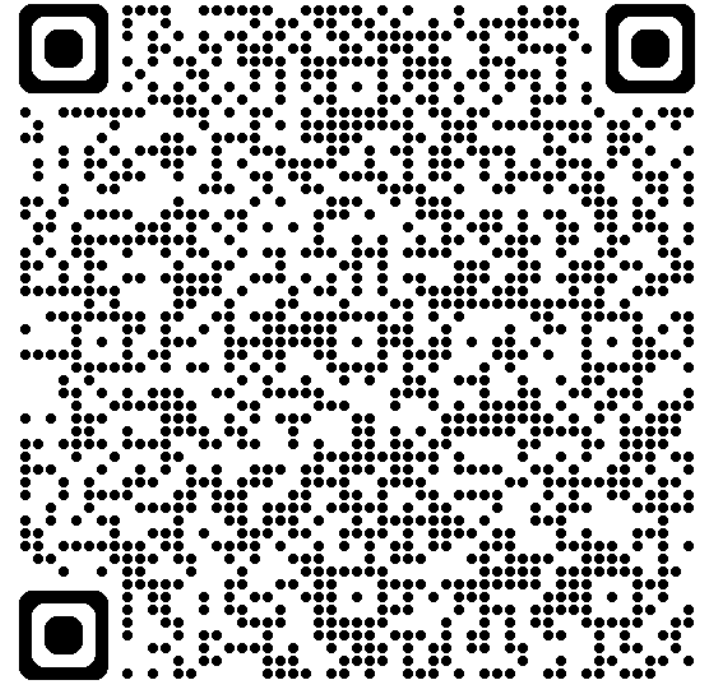
Copilot rules to monitor and detect suspicious or malicious activities

# Demo: Visibility in user access and activities



# Call To Actions

- Try Advisor [recommendations](#)
- Enable Copilot Studio [DLP](#) enforcement
- Checkout the [copilot audit logs](#) in Microsoft Purview
- Set alerts in Microsoft Sentinel with [copilot logs](#)
- Try [env. routing](#) & [welcome message](#) in copilot
- Sign up for [copilot sharing limit preview](#) (QR code)
- Read [aka.ms/CopilotStudioSecurity](https://aka.ms/CopilotStudioSecurity) & [aka.ms/MCSgov](https://aka.ms/MCSgov)





Copilot Studio