

Microsoft Purview capabilities in Security Copilot

Contents

Introduction	2
Prerequisites to access Microsoft Security Copilot	3
Microsoft Purview experiences using Security Copilot.....	3
Microsoft Purview capabilities in Security Copilot a.k.a. Standalone experience:.....	3
<i>Security copilot embedded in Microsoft Purview a.k.a. Embedded experience:</i>	3
Microsoft Purview Security Copilot – Data Risk.....	4
Introduction	4
Prerequisites	4
How to get started	4
Evaluating Security Copilot – Data Risk.....	6
Support and Feedback	7
Microsoft Purview Security Copilot – User Risk.....	8
Introduction	8
Prerequisites	8
How to get started	8
Evaluating Security Copilot – User Risk.....	10
Support and Feedback.....	11
Data processing and privacy	11
Summarize Data Loss Prevention Alerts using Security Copilot.....	11
Introduction	11
Prerequisites	12
How to get started	12
Evaluating Security Copilot – Summarize Alert.....	13
Support and Feedback	14
Data processing and privacy	14
Summarize Insider Risk Management Alerts using Security Copilot.....	15
Introduction	15
Prerequisites	15

How to get started	16
Evaluating Security Copilot – Summarize Alert	17
Support and Feedback.....	18
Data processing and privacy	18
Security Copilot for Communication Compliance- private preview guide.....	18
Introduction	19
Generate contextual summary of content in a policy.....	19
Prerequisites	19
Accessing Security Copilot in Communication Compliance	20
Evaluating Security Copilot in Communication Compliance.....	24
Limitations.....	24
Support and Feedback.....	24
Security Copilot for Purview eDiscovery (Premium)	25
Introduction	25
Scenario 1. Generate an eDiscovery search query with Copilot (Coming Soon)	25
Scenario 2. Gain contextual summary of items in review sets	26
Prerequisites	27
Accessing Security Copilot - Purview eDiscovery	28
Gain summary of an item in a review set.....	28
Generate a search query using Security copilot (COMING SOON)	31
Evaluating Security Copilot - Purview eDiscovery	35
Limitations and known issues	36
Support and Feedback.....	36

Introduction

We are excited to announce that Microsoft Purview integration with Security Copilot is in private preview now. With Microsoft Purview capabilities in Security Copilot, your security teams gain unprecedented visibility across the security data – bringing signals together from Defender, Sentinel, Intune, Entra and Purview into a single pane of glass. Purview brings **user risk** and **data risk** insights to help the SOC with comprehensive and enriched signals to understand the full attack story and impact of a security incident.

Additionally, data security and compliance admins will be able to leverage Security Copilot powered summarization capabilities and natural language support, embedded directly into Microsoft Purview solutions. These capabilities help you accelerate time to action and enable analysts at all levels to conduct advanced investigations.

Prerequisites to access Microsoft Security Copilot

Before you start using Security Copilot, the following prerequisites need to be met:

- You need to be enrolled in the Microsoft Security Copilot Early Access Program or be nominated by CxE to participate in the private preview. To learn how to access the early access program, licensing requirements, general guidance on onboarding, please refer: [Get started with Microsoft Security Copilot Early Access Program | Microsoft Learn](#)
- Microsoft Security Copilot wiki: [Microsoft Security Copilot documentation | Microsoft Learn](#)

Microsoft Purview experiences using Security Copilot

Microsoft Purview capabilities using Security Copilot are available as two experiences:

Microsoft Purview capabilities in Security Copilot a.k.a. Standalone experience:

Security teams need integrated insights to drive operational efficiency. Research shows that [62% of data security teams collaborate with SOC teams](#) and are more confident in proactively addressing data security than those who do not. With Microsoft Purview skills in Security Copilot, you gain valuable data and user risk insights to help identify the source of an attack and any sensitive data that may be at risk. This end-to-end visibility across platforms helps reduce investigation time and uncover insights that would have otherwise been missed.

Here are the scenarios we support as part of the standalone experience:

- [Microsoft Purview Security Copilot – Data Risk](#)
- [Microsoft Purview Security Copilot – User Risk](#)

Security copilot embedded in Microsoft Purview a.k.a. Embedded experience:

We're natively embedding Security Copilot into Microsoft Purview solutions to help with your data security and compliance scenarios. You can now leverage summarization capabilities, real time guidance, and natural language support to catch what others miss, accelerate investigation, and strengthen your team's expertise. Imagine the power at your fingertips: with a single click, you can instantly generate a comprehensive and concise summary of your top alerts to focus on critical investigation paths forward.

Here are the scenarios we support as part of embedded experience:

- [**Gain comprehensive summary of Data Loss Prevention alerts**](#)
- [**Gain comprehensive summary of Insider Risk Management alerts**](#)
- [**Gain contextual summary of Communication Compliance policy matches**](#)
- [**Gain contextual summary of evidence collected in eDiscovery review sets**](#)
- [**Generate keyword query language from natural language prompt in eDiscovery**](#)

Microsoft Purview Security Copilot – Data Risk

Introduction

Enhancing data security requires strong teamwork across departments. Research shows that 62% of data security teams collaborate with their SOC team to improve their data security posture, and for those who do, they tend to be more confident and proactive in data security. To support this collaboration and in response to the growing need for efficient and comprehensive security investigations, we are excited to announce the private preview of **Microsoft Purview Data Security Insights in Security Copilot**.

This includes insights from Microsoft Purview Data Loss Prevention, that allow the SOC team with the relevant role permissions to quickly gain context on the data at risk in a security incident.

Prerequisites

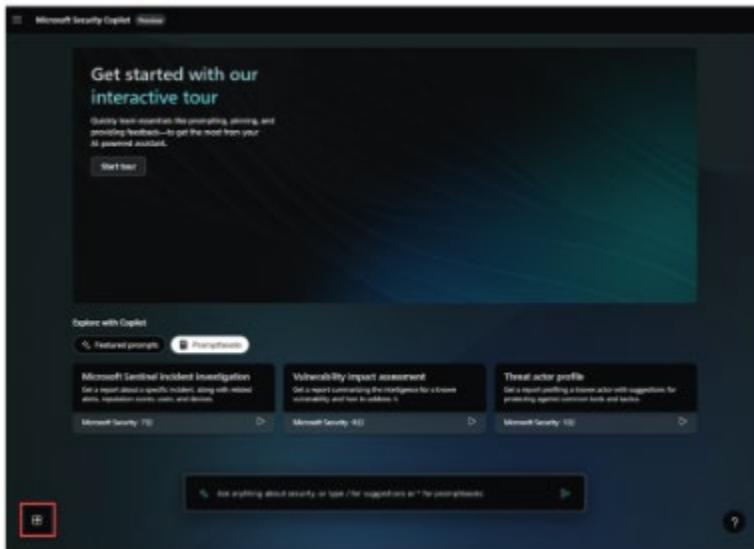
- You need to be enrolled in the [Microsoft Security Copilot Early Access Program](#) or be added to Security Copilot by Microsoft.
- Your organization should be onboarded to Microsoft Purview Data Loss Prevention and meets the [licensing requirements](#).
- Microsoft Security Copilot assumes the permissions of the user when it tries to access the data to answer the queries. You need to have the required permissions to access the data.

How to get started

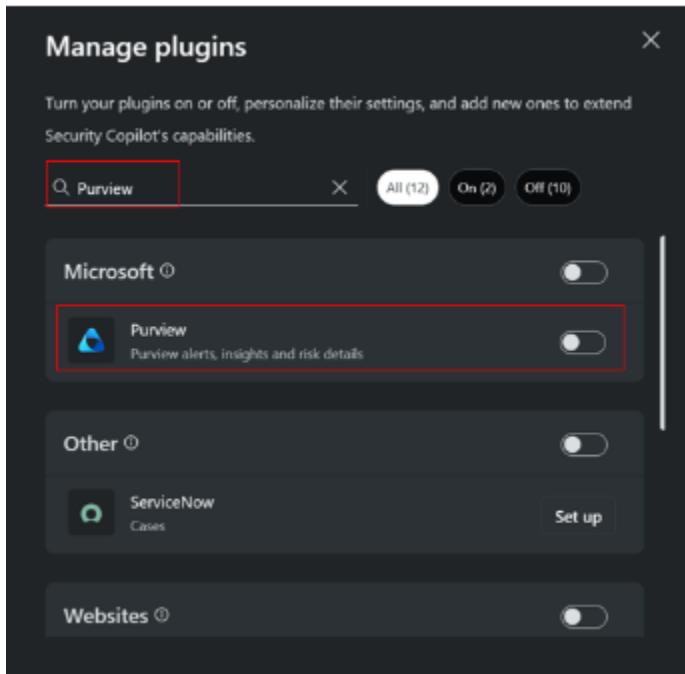
1. Go to [Microsoft Security Copilot](#) and sign in with your credentials.

2. Enable the Purview plugin.

- Click on the icon on bottom left hand corner (highlighted in red)



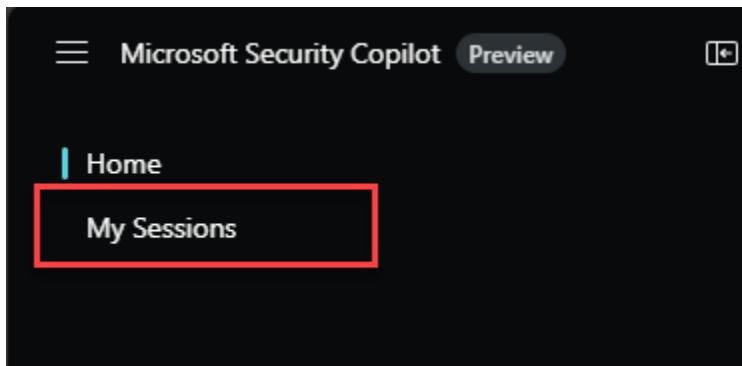
- Search for Purview and enable it by toggling the control next to "Purview"



3. Enter your prompt

Given below are some sample prompts:

- Which Purview Data Loss Prevention alerts should I prioritize today?
 - Can you summarize the first purview alert?
 - What was the data or action that triggered this alert?
 - What are the data risks related to this alert?
 - For the files related to the alert, show me all activities done in last 7 days?
 - Can you get me the status of labeling on these files?
 - What Suspicious Actions Have Been Performed On This Files?
 - What other DLP alerts are present for this user?
 - According to Purview, What is the implication of these DLP Alerts?
 - How many DLP policies have adaptive protection configured?
4. Be clear and specific with your prompts. It might also help to add **Purview** to your prompt, like: **According to Purview, what is the risk associated with this user.**
 5. Experiment with different prompts and variations to see what works best for your use case. Chat AI models vary, so iterate and refine your prompts based on the results you receive.
 6. Security Copilot saves your prompt sessions. To see the previous sessions, in Security Copilot, go to the menu > **My Sessions**:



7. For a walkthrough on Security Copilot, including the pin and share feature, go to [Navigating Microsoft Security Copilot](#).
8. For more information on writing Security Copilot prompts, go to [Microsoft Security Copilot prompting tips](#)

Evaluating Security Copilot – Data Risk

As you use Security Copilot for evaluating data risk, we encourage you to think about the following questions and scenarios:

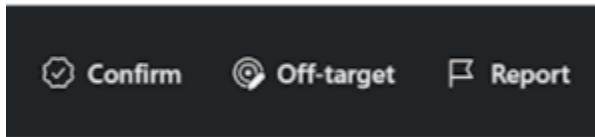
- How useful was the data risk context from Purview in incident investigation?

- Which prompts were the most useful from an incident management perspective?
- What are the capabilities(prompts) that you would like to see added or improved for data risk assessment?
- Which prompts did not perform according to your expectations and what would you like to improve?
- How would you rate the performance, reliability, and usability of the user risk prompts?
- What would you prefer - standalone vs embedded experience for Microsoft Purview Security Copilot scenarios and why?

Support and Feedback

We appreciate your participation in the private preview of Security Copilot for Purview, and your feedback will help us in the development of this feature.

To provide feedback, in Security Copilot, use the feedback buttons at the bottom of each completed prompt:



Your options:

- **Confirm:** The results match expectations.
- **Off-target:** The results don't match expectations.
- **Report:** The results are harmful in some way.

Whenever possible, and when the result is **Off-target**, write a few words explaining what can be done to improve the outcome. If you entered Purview-specific prompts and the results aren't Purview related, then include that information.

Data processing and privacy

When you interact with the Security Copilot to get Purview data, Security Copilot pulls that data from Purview. The prompts, the Purview data that's retrieved, and the output shown in the prompt results are processed and stored within the Security Copilot service.

For more information about data privacy in Security Copilot, go to [Privacy and data security in Microsoft Security Copilot](#).

Microsoft Purview Security Copilot – User Risk

Introduction

Enhancing data security requires strong teamwork across departments. Research shows that 62% of data security teams collaborate with their SOC team to improve their data security posture, and for those who do, they tend to be more confident and proactive in data security. To support this collaboration and in response to the growing need for efficient and comprehensive security investigations, we are excited to announce the private preview of **Microsoft Purview Data Security Insights in Security Copilot**.

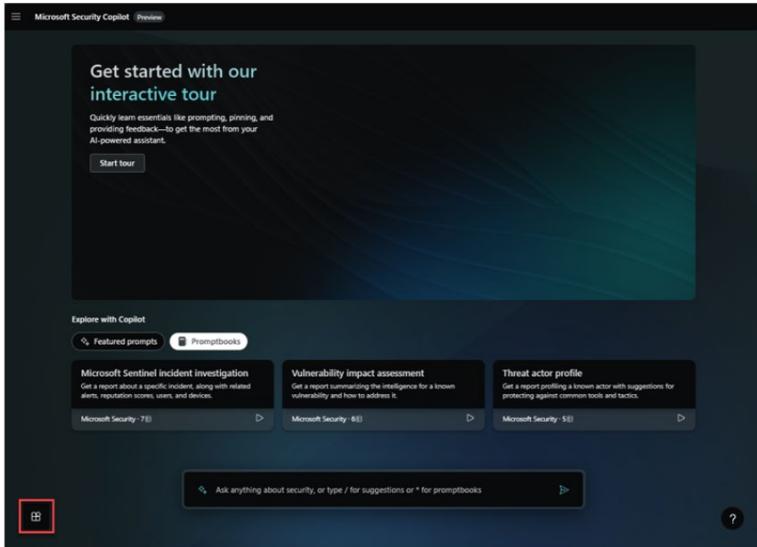
This includes user insights from Microsoft Purview Insider Risk Management, that allow the SOC team with Insider Risk Management role permissions to quickly gain context on the risk associated with the users involved in a security incident. The RBAC and the anonymization controls within Insider Risk Management will be respected in the standalone experience, so only when all the conditions are met, user info will be shared.

Prerequisites

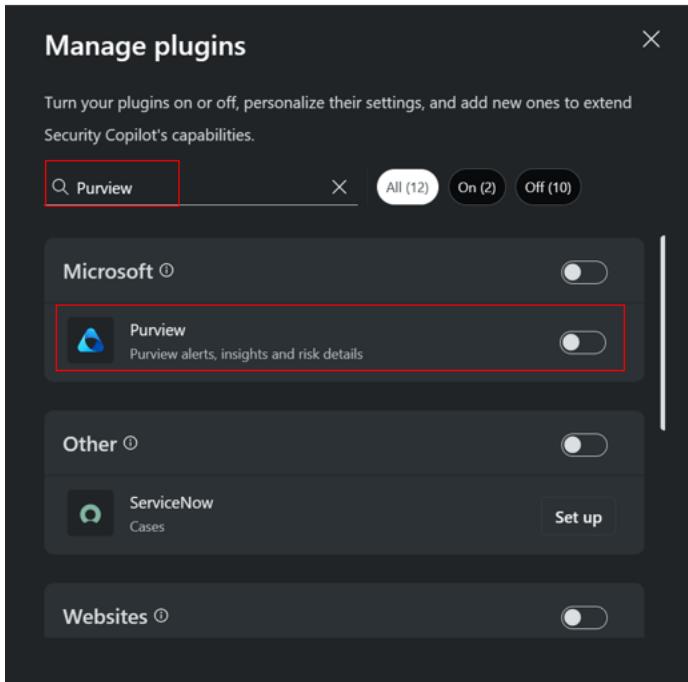
- You need to be enrolled in the [Microsoft Security Copilot Early Access Program](#).
- Your organization should be onboarded to Microsoft Purview Insider Risk Management and meets the [licensing requirements](#).
- Microsoft Security Copilot assumes the permissions of the user when it tries to access the data to answer the queries. You need to have the [required permissions](#) to access the data.
- User specific queries might not get answered if pseudo-anonymization is enabled for your tenant. We respect the privacy controls you have set up in the standalone experience as well. [Update your privacy setting](#).

How to get started

- 1) Go to [Microsoft Security Copilot](#) and sign in with your credentials.
- 2) Enable the Purview plugin.
 - Click on the icon on bottom left hand corner (highlighted in red)



- Search for Purview and enable it by toggling the control next to "Purview"

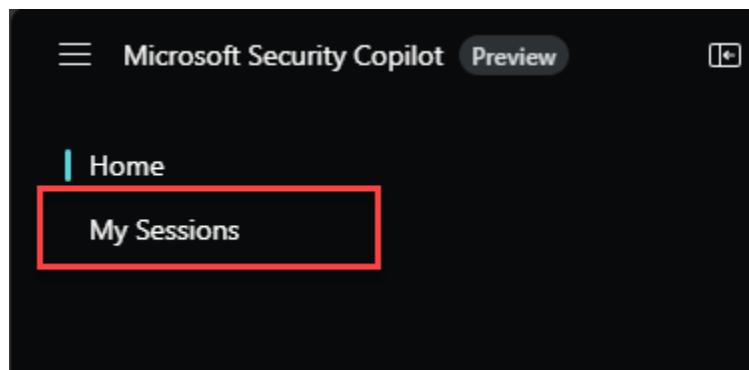


3) Enter your prompt

Given below are some sample prompts.

- Who is the user involved in this alert?
- What is the risk level of this user?
- What information does Purview have about the risk associated with this user?
- Show me all the activities for this user in the last 7 days.

- What type of unusual activities did the user engage in the last 7 days?
 - What type of exfiltration activities did the user engage in the last 5 days?
 - What type of sequential activities did the user engage in the last 10 days?
- 4) Be clear and specific with your prompts. It might also help to add **Purview** to your prompt, like: **According to Purview, what is the risk associated with this user.**
 - 5) Experiment with different prompts and variations to see what works best for your use case. Chat AI models vary, so iterate and refine your prompts based on the results you receive.
 - 6) Security Copilot saves your prompt sessions. To see the previous sessions, in Security Copilot, go to the menu > **My Sessions**:



- 7) For a walkthrough on Security Copilot, including the pin and share feature, go to [Navigating Microsoft Security Copilot](#).
- 8) For more information on writing Security Copilot prompts, go to [Microsoft Security Copilot prompting tips](#)

Evaluating Security Copilot – User Risk

As you use Security Copilot for evaluating user risk, we encourage you to think about the following questions and scenarios:

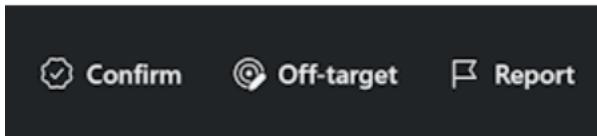
- How useful were the user insights from Purview in incident investigation?
- Which prompts were the most useful from an incident management perspective?
- What are the capabilities(prompts) that you would like to see added or improved for user risk assessment?
- Which prompts did not perform according to your expectations and what would you like to improve?
- How would you rate the performance, reliability, and usability of the user risk prompts?

- What would you prefer - standalone vs embedded experience for Microsoft Purview Security Copilot scenarios and why?

Support and Feedback

We appreciate your participation in the private preview of Security Copilot for Purview, and your feedback will help us in the development of this feature.

To provide feedback, in Security Copilot, use the feedback buttons at the bottom of each completed prompt:



Your options:

- **Confirm:** The results match expectations.
- **Off-target:** The results don't match expectations.
- **Report:** The results are harmful in some way.

Whenever possible, and when the result is **Off-target**, write a few words explaining what can be done to improve the outcome. If you entered Purview-specific prompts and the results aren't Purview related, then include that information.

Data processing and privacy

When you interact with the Security Copilot to get Purview data, Security Copilot pulls that data from Purview. The prompts, the Purview data that's retrieved, and the output shown in the prompt results are processed and stored within the Security Copilot service.

For more information about data privacy in Security Copilot, go to [Privacy and data security in Microsoft Security Copilot](#).

Summarize Data Loss Prevention Alerts using Security Copilot

Introduction

Data security teams receive on an average over 50 data security alerts per day and but these teams can only get review up to 60-70% of them these alerts, leaving them exposed to risks. To help with this challenge, we are thrilled to announce the **integration of Security Copilot into Microsoft**

Purview in private preview, leveraging the power of generative AI to provide **incident summary that helps accelerate investigations.**

This alleviates the time and effort burden security teams once faced when they had to review a multitude of insights to determine the nature of a potential incident. This AI-powered summary can help security teams quickly focus on the key leading evidence and locate the critical investigation paths forward.

Prerequisites

- You need to be enrolled in the [Microsoft Security Copilot Early Access Program](#).
- Your organization should be onboarded to Microsoft Purview Data Loss Prevention and meets the [licensing requirements](#).
- Microsoft Security Copilot assumes the permissions of the user when it tries to access the data to answer the queries. You need to have the required permissions to access the data. You must have at least Security reader role. See [Understand authentication in Microsoft Security Copilot | Microsoft Learn](#) OR be a member of a Security Group with Security Copilot access (Please work with your Microsoft contact if this is needed as it requires a backend change)
 - NOTE: To approve your designated Security Group for Security Copilot access, share the Security Group alias with your Microsoft CXE member

How to get started

- Go to the compliance portal (classic: <https://compliance.microsoft.com/> or new: <https://purview.microsoft.com/>) and sign in with your credentials.
- Go to the Data Loss Prevention solution and navigate to the alerts queue.
- Choose the alert you want to review.
- Click on the “Get a summary from Security Copilot” option on the panel.

The screenshot shows a list of DLP policy matches on the left and a detailed view of a specific alert on the right.

Left Panel (List of DLP policy matches):

- Alert name
- DLP policy match for email with subject 'Interesting news'
- DLP policy match for email with subject 'Request for Project Update'
- DLP policy match for email with subject 'New design spec Process | SpecDis-834'
- DLP policy match for email with subject 'Amanda your file are attached'
- DLP policy match for email with subject 'Review meeting - important!'
- DLP policy match for email with subject 'Could you please do us a small favour?'
- DLP policy match for email with subject 'Amanda do you still would like to work with us?'
- DLP policy match for email with subject 'Follow up - Here is your next Security 101 content'
- DLP policy match for email with subject 'Project status'
- DLP policy match for email with subject 'Request for Invoice Access'
- DLP policy match for email with subject 'Travel itinerary'
- DLP policy match for email with subject 'Interesting news'
- DLP policy match for email with subject 'Cost Analysis Report - 2023-11'
- DLP policy match for email with subject 'Travel itinerary'
- DLP policy match for email with subject 'Project status'

Right Panel (Detailed Alert View):

Alert: DLP policy match for email with subject 'Request for Invoice Access'

Details **Events**

Get a summary from Security Copilot

Alert ID: e00aea5a-5311-884e-5200-08dbe6d3db9c

Alert status: Active

Alert severity: Low

Time detected: Nov 16, 2023 10:47 AM

Number of events: 1

DLP policy matched: Adaptive Protection policy for Teams and Exchange DLP

Locations: Exchange

Users who performed the event:

View details ...

- Alert summary will be generated:

The screenshot shows a list of DLP policy matches on the left and a detailed view of a specific alert on the right.

Left Panel (List of DLP policy matches):

- Export Refresh Set status
- Filter Reset Filters
- Time range: 11/13/2023-12/13/2023
- User: Any
- Alert status: Any
- Alert severity: Any
- Alert name
- DLP policy match for email with subject 'Cost Analysis Report - 2023-11'
- DLP policy match for email with subject 'Travel itinerary'
- DLP policy match for email with subject 'Follow up - Here is your next Security 101 content'
- DLP policy match for email with subject 'Request for Invoice Access'
- DLP policy match for email with subject 'Interesting news'

Right Panel (Detailed Alert View):

Alert: DLP policy match for email with subject 'Request for Invoice Access'

Details **Events**

Security Copilot PREVIEW

Alert summary: Dec 13, 2023 1:18 AM

The low severity DLP (Data Loss Prevention) alert with ID d1e00aea5a-5311-884e-ea00-08dbe7b3ef1e was generated on November 17, 2023 21:26:00 (UTC). The alert is currently in "new" status and is associated with the user jonav@parkcity.alpineskithouse.co.

The email involved in this alert is jonav@parkcity.alpineskithouse.co.

The policy responsible for this alert is named "Adaptive Protection policy for Teams and Exchange DLP" with Policy ID c6fc082d-b1c4-4297-8fd7-49c06937073e. The rule that triggered the alert is "Adaptive Protection audit rule for Teams and Exchange DLP" with Rule ID 98c3fd94-e9e0-4054-a227-b4fee0e3899a. This is related to the workload Exchange.

- You can use the three dots on the top right of the alert summary to copy the response to clipboard, regenerate or open it in the standalone security copilot experience.

Evaluating Security Copilot – Summarize Alert

As you use Security Copilot for evaluating an alert, we encourage you to think about the following questions and scenarios:

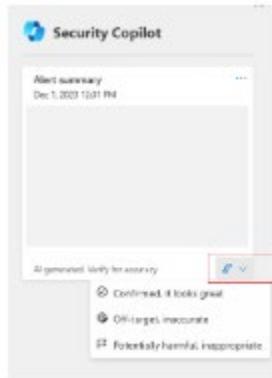
1. How useful was the alert summary for a Data Loss Prevention alert? Did it help reduce the time to action?

2. Are there any improvements you would like to suggest to the alert summary?
3. How would you rate the performance, reliability, and usability of the alert summarization skill?
4. How easy or difficult was it to access and use the alert summarization capability as an embedded experience?

Support and Feedback

We appreciate your participation in the private preview of Security Copilot for Purview, and your feedback will help us in the development of this feature.

To provide feedback, click on the feedback icon on the bottom right (highlighted in red):



Your options:

- **Confirmed:** The results match expectations.
- **Off-target:** The results don't match expectations.
- **Inappropriate:** The results are harmful in some way.

Whenever possible, and when the result is **Off-target**, write a few words explaining what can be done to improve the outcome.

Data processing and privacy

When you interact with the Security Copilot to get Purview data, the Security Copilot pulls that data from Purview. The prompts, the Purview data that's retrieved, and the output shown in the prompt results are processed and stored within the Security Copilot service.

For more information about data privacy in Security Copilot, go to [Privacy and data security in Microsoft Security Copilot](#).

Summarize Insider Risk Management Alerts using Security Copilot

Introduction

Data security teams receive on average over 50 data security alerts per day, but these teams can only review up to 60-70% of these alerts, leaving them exposed to risks. To help with this challenge, we are thrilled to announce the **integration of Security Copilot into Microsoft Purview** in private preview, leveraging the power of generative AI to provide **incident summary that helps accelerate investigations**.

This alleviates the time and effort burden security teams once faced when they had to review a multitude of insights to determine the nature of a potential incident. With this new ability to summarize Insider Risk Management alerts, customers can quickly gain a highlight of the potential incident by identifying critical user details like resignation submissions, exfiltration activities, sequential patterns, user roles and unusual activities that may lead to potential security incidents. This AI-powered summary can help security teams quickly focus on the key leading evidence and locate the critical investigation paths forward.

The screenshot shows the Microsoft Purview Insider Risk Management interface. On the left, there's a navigation sidebar with options like Home, Overview, Alerts (which is selected), Cases, Policies, Users, Notice templates, Adaptive protection (preview), and Solutions. Under Alerts, there are sub-options for Communication compliance, Data Loss Prevention, and Information barriers. The main content area displays an alert titled '(7bbc3040) Data theft by departing users'. It includes sections for 'Activity that generated this alert' (listing 'FileCopiedToRemoteDesktopSession' with a risk score of 87/100 and a creation date of Sept 30, 2023), 'Triggering event' (an HR connector imported a resignation date for this user), 'User details' (user 'jdoe@msftcell.com' from 'rob.dylan@msftcell.com'), and 'User alert history' (a link to view all alert history). Below these are sections for 'Summary', 'Activity explorer', 'User activity', and 'Forensic evidence'. The 'Summary' section contains several charts and tables. A large callout box on the right, titled 'Security Copilot', provides a detailed summary of the alert: 'Alert summary October 1, 2023 2:11 PM. The alert with ID 7bbc3040 is a high-severity Insider Risk Management alert involving user Jane Doe (jdoe@msftcell.com) that was detected on September 30, 2023. The policy "Data theft by departing user" was triggered when the HR connector imported a resignation date for this user on September 25, 2023. The user was involved in activities where files containing sensitive info were copied to a remote desktop session that led to this alert. Getting deeper into the alert, it has a risk score of 87/100 and has 3 alerts and 1 case associated with them. This alert is in a confirmed state and is being investigated by Rob Dylan. The alert also has a case: "DepartingUser_Investigation" associated with it.' At the bottom of the callout, it says 'AI generated. Verify for accuracy.'

Figure 3: Security Copilot provides an incident summary in an alert generated by Insider Risk Management

Prerequisites

- Customer need to be enrolled in the [Microsoft Security Copilot Early Access Program](#).

- Your organization should be onboarded to Microsoft Purview Insider Risk Management and should meet the [licensing requirements](#).
- You must have at least Security reader role. See [Understand authentication in Microsoft Security Copilot | Microsoft Learn](#) OR be a member of a Security Group with Security Copilot access (Please work with your Microsoft contact if this is needed as it requires a backend change)
 - NOTE: To approve your designated Security Group for Security Copilot access, share the Security Group alias with your Microsoft CXE member
- The privacy controls you have set up in the Microsoft Insider Risk Management solution are honored. Alert summary will have anonymized username if pseudo-anonymization is turned ON in your tenant. You can choose to [update your privacy setting](#).

How to get started

- Go to the compliance portal (classic: <https://compliance.microsoft.com/> or new: <https://purview.microsoft.com/>) and sign in with your credentials.
- Go to the Insider Risk Management solution.
- Go to your alerts queue by navigating to the alerts tab.

Insider risk management

Overview **Alerts** Cases Policies Users Reports Forensic evidence Notice templates Adaptive protection (preview)

• Choose the alert you want to review.

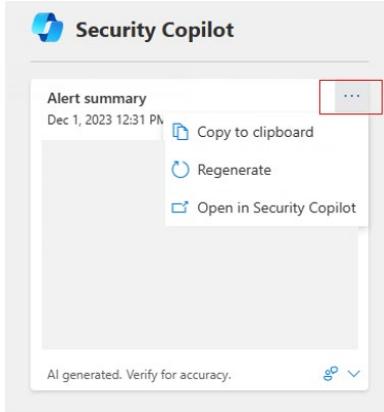
• Click on the summarize alert button on the right.

- Alert summary will be generated:

The screenshot shows the Microsoft Purview Insider Risk Management interface. On the left, there's a navigation sidebar with options like Home, Overview, Alerts, Cases, Policies, Users, Notice templates, Adaptive protection (preview), Solutions, and Related (Communication compliance, Data Loss Prevention, Information barriers). The main content area displays an alert summary for incident ID (7bbc3040) titled "Data theft by departing users". The alert is marked as High severity, Risk score: 87/100, and was created on Sept 30, 2023, as Confirmed. It details an activity where "EpfileCopiedToRemoteDesktopSession" triggered on Sept 28, 2023 (UTC). The triggering event was an HR connector reporting a resignation date for the user. The user details show Bob Dylan (jdoe@edmscontf.onmicrosoft.com). The User alert history section provides a detailed summary of the alert, mentioning Jane Doe (jdoe@edmscontf.onmicrosoft.com) who was deleted on Oct 1, 2023. The alert history notes that Bob Dylan copied files to a remote desktop session on Sept 25, 2023, which triggered the alert. The alert is considered high risk and has 3 alerts and 1 case associated with it. The alert is being investigated by Bob Dylan. The alert also has a case "DepartingUser_investigation" associated with it. The interface includes tabs for Summary, Activity explorer, User activity, and Forensic evidence, along with various charts and tables.

Figure 3: Security Copilot provides an incident summary in an alert generated by Insider Risk Management

- You can use the three dots on the top right of the alert summary to copy the response to clipboard, regenerate or open it in the standalone security copilot experience.



Evaluating Security Copilot – Summarize Alert

As you use Security Copilot for evaluating an alert, we encourage you to think about the following questions and scenarios:

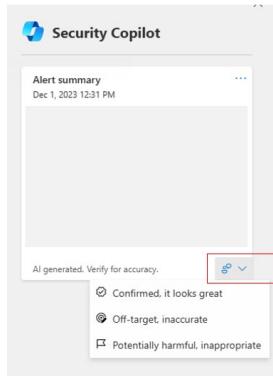
- 1) How useful was the alert summary for an Insider Risk Management alert? Did it help reduce the time to action?
- 2) Are there any improvements you would like to suggest to the alert summary?
- 3) How would you rate the performance, reliability, and usability of the alert summarization skill?

- 4) How easy or difficult was it to access and use the alert summarization capability as an embedded experience?

Support and Feedback

We appreciate your participation in the private preview of Security Copilot for Purview, and your feedback will help us in the development of this feature.

To provide feedback, click on the feedback icon on the bottom right (highlighted in red):



Your options:

- **Confirmed:** The results match expectations.
- **Off-target:** The results don't match expectations.
- **Inappropriate:** The results are harmful in some way.

Whenever possible, and when the result is **Off-target**, write a few words explaining what can be done to improve the outcome.

Data processing and privacy

When you interact with the Security Copilot to get Purview data, the Security Copilot pulls that data from Purview. The prompts, the Purview data that's retrieved, and the output shown in the prompt results are processed and stored within the Security Copilot service.

For more information about data privacy in Security Copilot, go to [Privacy and data security in Microsoft Security Copilot](#).

Security Copilot for Communication Compliance- private preview guide

A step-by-step guide to help you explore the features and capabilities of Security Copilot in Microsoft Purview Communication Compliance

Introduction

Welcome to the private preview of Security Copilot - Purview Communication Compliance

In this guide, you will learn how to access and use Security Copilot in Communication Compliance for the following embedded security copilot experience:

Generate contextual summary of content in a policy

Reviewing communications is an integral part of protecting your organization's communication landscape, but it is also time-consuming to review content that is hundreds of words long or contain attachments on top of that. With Security Copilot, you can now:

1) Get a contextual summary of a message and its attachments in the context of classifier conditions that flagged the message

2) Ask follow-up contextual questions about the message and its attachments

The screenshot shows the Microsoft Purview Communication Compliance interface. On the left, there is a navigation pane with icons for Home, Policies, Regulatory compliance, and other options. The main area shows a list of messages under 'Pending (12)' and 'Resolved (29)'. A search bar and filters for Body/Subject, Date, Sender, and Tags are at the top. The right side features the 'Security Copilot' feature, which is currently active on a message from 'Christophe Fießinger'. The copilot summary indicates 'Conditions detected: Gifts & entertainment (cover the c...)' and provides a detailed breakdown of the sender's strategy and vision. It also lists specific tasks such as developing a company-wide discussion of the vision and managing marketing teams. Below the summary, there are buttons for 'Resolve', 'Summarize', 'Notify', and 'Tag as'. A sidebar on the right contains a 'Copilot' section with a timestamp (Dec 4, 2023, 5:41 PM), a note about potential categories like 'Gifts and Entertainment' and 'Stock manipulation', and a 'Copilot' summary. At the bottom, there are buttons for generating a summary, asking a question, and a note about previous responses.

Prerequisites

Before you start using Security Copilot for Communication Compliance, you need to meet the following prerequisites:

- You need to be enrolled in the [Microsoft Security Copilot Early Access Program](#). To learn how to enroll and get started with Microsoft Security Copilot, please refer to this guide: [Get started with Microsoft Security Copilot Early Access Program | Microsoft Learn](#)
- Confirm that you are part of the Private Preview for Security Copilot for Purview

- You must have [proper licensing to access Communication Compliance](#)
- To get contextual summaries in policies, you must have [Communication Compliance or Communication Compliance Investigator Role](#)
- You must have at least Security reader role. See [Understand authentication in Microsoft Security Copilot | Microsoft Learn](#) OR be a member of a Security Group with Security Copilot access (Please work with your Microsoft contact if this is needed as it requires a backend change)
 - NOTE: To approve your designated Security Group for Security Copilot access, share the Security Group alias with your Microsoft CXE member

Accessing Security Copilot in Communication Compliance

You can access Security Copilot in Communication Compliance as an embedded experience in Microsoft Purview. We do not support a standalone solution as part of this private preview.

- 1) Navigate to Communication Compliance in the compliance portal (<https://compliance.microsoft.com/supervisoryreview?viewid=Overview>). Then navigate to the Policies tab in Communication Compliance

Policy name	New pending today	Total pending	Total resolved	Status	Last modified (UTC)
User-reported messages	0	0	0	Active	Dec 15, 2023 3:10 PM
Insider risk trigger 23-11-29T03:58:37Z	0	0	754	Active	Dec 5, 2023 9:25 PM
Confidential projects	21	1255	286	Active	Dec 4, 2023 10:31 PM
Project Woodgrove	0	0	6740	Active	Nov 28, 2023 4:54 AM
Shared Creds	0	2	62	Active	Nov 29, 2023 3:24 AM
Regulatory compliance	10	30	30	Active	Dec 4, 2023 10:32 PM
Inappropriate Images	0	3	1	Active	Nov 28, 2023 5:08 AM
Inappropriate Text	0	4	0	Active	Dec 4, 2023 10:32 PM

- 2) Navigate to a policy that uses trainable classifiers as part of the policy's configurations.

NOTE: Contextual Summarization currently supports trainable classifiers as context.

The screenshot shows the Microsoft Purview Communication compliance interface. The top navigation bar includes 'WOODGROVE' and 'Microsoft Purview'. Below the navigation is a breadcrumb trail: 'Communication compliance > Policies > Regulatory compliance'. On the right side of the header are links for 'Export files', 'Export report', and 'Download review activity'. The main content area has tabs for 'Pending (30)', 'Resolved (30)', and 'Exports', with 'Pending' being the active tab. A 'Filter' section allows saving, resetting, or applying filters. Below the filter is a table with columns: Escalate, Refresh, Subject, Tags, Sender, Recipients, and Sentiment. The table lists 30 items. One item, a message from 'Christophe Fiessinger' with subject '[EXTERNAL] A Vu... [REDACTED]' and recipient 'WG-WoodgroveCo...', is selected and highlighted with a blue border. To the right of the table is a preview pane titled 'Subject line' with the instruction 'Select an item from the list to preview its content'.

3) Click on a policy match to view message content. You should see a Copilot action in the upper left command bar or a *Summarize* action in the lower right command bar

This screenshot shows the same Microsoft Purview interface as the previous one, but with a different message selected. The message from 'Christophe Fiessinger' is now fully expanded in a large preview pane on the right. The preview pane has tabs for 'Summary', 'Plain Text', 'Conversation', and 'User history', with 'Summary' being the active tab. It displays a yellow banner stating 'Conditions detected: Gifts & entertainment (cover the cost, +2 more), Stock manipulation...' and a 'View all' link. Below the banner is a summary section for 'Christophe Fiessinger' under the heading 'Strategy and Vision'. The summary text reads: 'MD will work with marketing team and upper chain of command to define the upcoming strategy and vision. Pivots in how to approach investors and main responsibilities to be fulfilled include:' followed by a bulleted list of actions. At the bottom of the preview pane are buttons for 'Resolve', 'Summarize', 'Notify', 'Tag as', and 'Escalate'.

- 4) Click on either action to generate a contextual summary of the message and supported attachments (NOTE: Contextual summaries are only eligible for messages and attachments with a combined length of 100 words or more.)

The screenshot shows the Microsoft Purview Communication Compliance interface. On the left, there's a navigation pane with various icons. In the center, a list of messages is displayed under the heading "Pending (30) Resolved (30) Exports". The messages are filtered by "Body/Subject: Any", "Date: Any", "Sender: Any", and "Tags: Any". One message is selected, showing details for "Christophe Fiessinger". The "Summary" tab is active, displaying a summary of his role and responsibilities. To the right, a "Security Copilot" sidebar is open, showing a summary of detected categories: "Gifts & entertainment" and "Stock manipulation". It also includes a timestamp ("Dec 15, 2023, 1:25 PM"), a note about potential matches for these categories, and a list of detected content related to these categories.

- 5) To learn more about the message, explore additional default prompts or type your own question into the text prompt in the Security Copilot side

The screenshot shows the Security Copilot interface. At the top, there are two blue-bordered boxes containing prompts: "What content in the message was flagged as Gifts & entertainment and Stock manipulation categories?" and "Generate a simple summary of this message". Below these is a larger text input field with the placeholder "Ask a question or describe what you'd like to do." and a character count indicator "0/500". At the bottom, a note states "Copilot doesn't reference prior responses when responding to new questions about this message."

- 6) To share feedback on the contextual summary, leverage the feedback mechanism for each Copilot response



Security Copilot Preview

X

'Gifts and Entertainment' and 'Stock manipulation'.

For 'Gifts and Entertainment', the line 'Cover the cost of lodging and traveling for consultant team onsite assisting Contoso' and 'Honor bonus requests such as customized service for offsite business with consultant team' could be seen as offering gifts or entertainment in return for services.

For 'Stock manipulation', the lines 'Allow consultant team to add stocks to investment portfolio related to Contoso Inc's dealings with no dissemination of these dealings' and 'Provide advice for stock trading to exclusive Contoso partners regarding Contoso Inc stocks' could be seen as potential signs of stock manipulation, as they suggest actions that could influence the stock price of Contoso Inc.

AI generated. Verify for accuracy



▼

How's this response?

Looks right

Needs improvement

Inappropriate

?

Generate a simple summary of this message

Ask a question or describe what you'd like to do.

0/500

Copilot doesn't reference prior responses when responding to new questions about this message.

Evaluating Security Copilot in Communication Compliance

As you use Security Copilot in Communication Compliance, we encourage you to think about the following questions and scenarios:

- How easy or difficult is it to access and use Security Copilot in Communication Compliance as an embedded experience in Microsoft Purview?
- How useful or valuable is the information and insights provided by Security Copilot in Communication Compliance?
- How would you rate the performance, reliability, and usability of Security Copilot in Communication Compliance?
- What are the features or capabilities that you like the most or the least about Security Copilot in Communication Compliance?
- What are the features or capabilities that you would like to see added or improved for Security Copilot in Communication Compliance?

Limitations

Please note that Security Copilot in Communication Compliance is currently in private preview and has limitations and unsupported scenarios that you should be aware of:

- Security Copilot is not protected by Purview for AI.
 - Security Copilot interactions are not protected under Communication Compliance policies
- Contextual summary
 - Content summarization length limit 20,000 tokens ~15,000 words
- [Responsible AI FAQ](#)

Support and Feedback

We appreciate your participation in the private preview of Security Copilot for Communication Compliance and we value your feedback. If you encounter any issues or have any suggestions, please use the following channels to contact us:

- To report a bug or request a feature, please use the Feedback button on the bottom right corner of each Security Copilot response (screenshot below for reference) You can also use the Feedback button to rate your experience and share your comments.
- Report any feedback to your designated Microsoft CxE member.

Thank you for your interest and engagement in Security Copilot for Communication Compliance. We look forward to hearing from you and improving the solution based on your feedback.

Security Copilot for Purview eDiscovery (Premium)

A step-by-step guide to help you explore the features and capabilities of Security Copilot - Purview eDiscovery (Premium)

Introduction

Welcome to the private preview of Security Copilot for Purview eDiscovery (Premium).

In this guide, you will learn how to access and use Security Copilot for Purview eDiscovery (Premium) for the following two embedded security copilot experiences.

Scenario 1. Generate an eDiscovery search query with Copilot (Coming Soon)

The first new capability is to help accelerate the query-building experience. Search is one of the most used but highly time-intensive workflows in an investigation. An accurate search is crucial for the success of an investigation. Traditionally, in eDiscovery, a search happens through a condition builder or the input of a query in Keyword Query Language (KQL). While condition builder surfaces most used properties and operators, eDiscovery search is rich in functionality and supports many more properties and operators through the KQL. However, there is a considerable learning curve involved in creating a KQL including learning all supported properties and operators as well the proper format for construction. With Security Copilot, you can now:

- 1) Provide a prompt in natural language and get a query generated in KQL that they can use as-is or build onto their existing query.
- 2) Refine and enhance your natural language prompt for a more accurate KQL.



Figure 1. GIF of Document summary review using Microsoft Security Copilot including additional prompts.

Scenario 2. Gain contextual summary of items in review sets

We've previously heard from many of you that 60% of eDiscovery admin or managers' time is spent reviewing evidence collected in review sets. With Security Copilot, you can now :

- 1) Get a contextual summary of a single item in a review set
- 2) Ask follow-up contextual questions about the summary

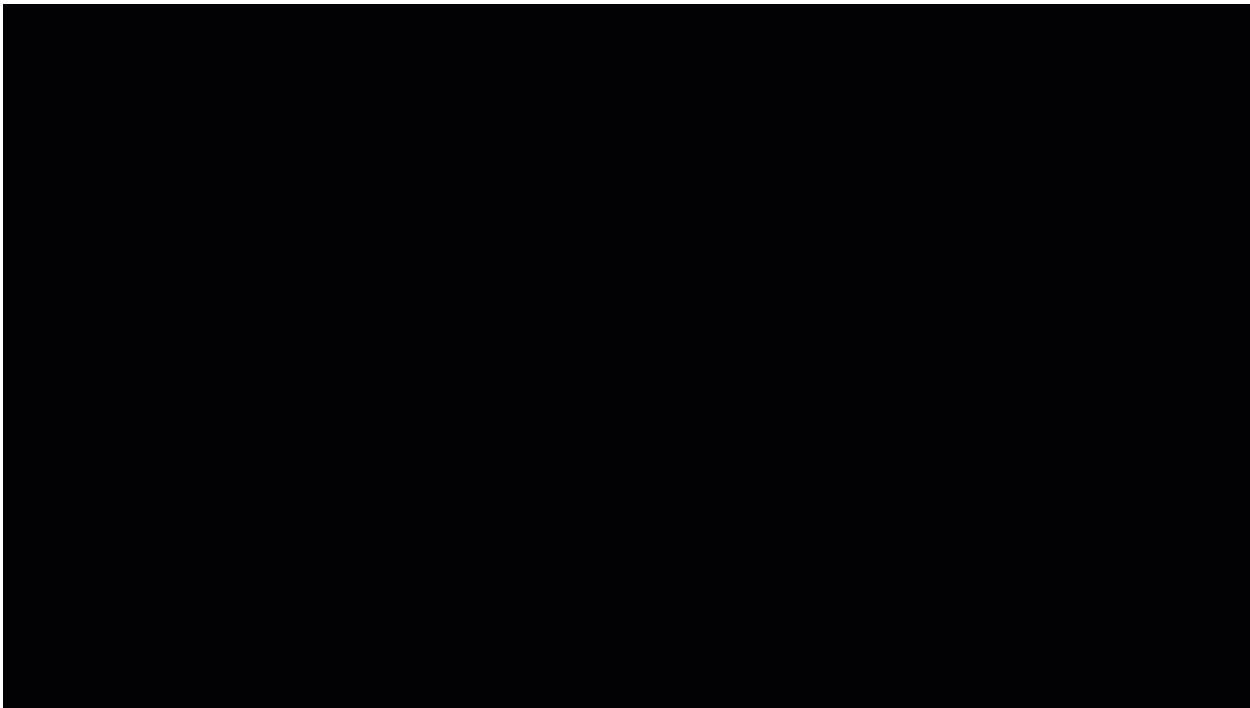


Figure 2. Animated GIF of Natural Language to Keyword Query Language experience in Microsoft Purview

Prerequisites

Before you start using Security Copilot for Purview eDiscovery (Premium), you need to meet the following prerequisites:

- You need to be enrolled in the [Microsoft Security Copilot Early Access Program](#). To learn how to enroll and get started with Microsoft Security Copilot, please refer to this guide: [here](#).
- You must have at least Security reader role. See [Understand authentication in Microsoft Security Copilot | Microsoft Learn](#) OR be a member of a Security Group with Security Copilot access (Please work with your Microsoft contact if this is needed as it requires a backend change)
 - NOTE: To approve your designated Security Group for Security Copilot access, share the Security Group alias with your Microsoft CXE member
- You must have [access to eDiscovery \(Premium\) cases](#).
- To generate a search query with, you must have Purview [Compliance Search role](#).
- To gain contextual summary, you must have Purview [Review role](#).

Accessing Security Copilot - Purview eDiscovery

You can access Security Copilot as embedded experiences within for Purview eDiscovery (Premium). We do not support the standalone solution as part of this private preview.

Gain summary of an item in a review set

- 1) Navigate to the compliance portal (compliance.microsoft.com/advancedediscovery?viewid=Cases) OR the new Purview portal (purview.microsoft.com/ediscovery/casespage) (**Coming Soon**). Then navigate to an eDiscovery (Premium) case.

The screenshots show the Microsoft Purview eDiscovery (Premium) interface. The top screenshot displays the 'eDiscovery (Premium)' dashboard with a list of cases. The bottom screenshot provides a detailed view of one specific case, 'Copilot search test', showing its status as Active and its creation date as Nov 1, 2023 3:30 PM.

Name	Status	Created on	Last modified	Last modified by	Number	Description
Copilot search test	Active	Nov 1, 2023 3:30 PM	Nov 1, 2023 3:30 PM	eDisco Big		
new Exodia case1030copilot	Active	Oct 30, 2023 9:54 AM	Oct 30, 2023 1:25 PM	eDisco Big	1345	test
copilot_new_test	Active	Mar 26, 2023 11:25 PM	Mar 26, 2023 11:25 PM	eDisco Big		Testing the new co...
copilot_new	Active	Mar 26, 2023 10:53 PM	Mar 26, 2023 10:53 PM	eDisco Big		Testing the new co...
copilot_new	Active	Mar 26, 2023 10:46 PM	Mar 26, 2023 10:46 PM	eDisco Big		Testing copilot fe...
copilot_existing	Closing	Mar 26, 2023 10:45 PM	Mar 27, 2023 12:28 AM	eDisco Big		test for copilot

- 2) Navigate to a review set. Please add data to a review set first if you don't see any items. Then open a review set.

Microsoft Purview

eDiscovery (Premium) > Cases > enron

Overview Data sources Collections Review sets Communications Hold Processing Exports Jobs Settings

Analyze, organize, annotate, redact, and tag collected items for export. [Learn more about review sets](#)

+ Add review set Download list Refresh

Filters: Size: Any Filters

Review set	Size	Created by	Last modified (UTC-12:00)	Modified by	Collections (sources)	Exports	Description
<input type="checkbox"/> Enron RS	190.9 GB	admin@edbig.onmicrosoft.com	Oct 23, 2023 3:42:35 PM	admin@edbig.onmicrosoft.com	2	0	
<input type="checkbox"/> Enron RS - 2	39.16 MB	admin@edbig.onmicrosoft.com	Dec 3, 2023 12:25:16 PM	admin@edbig.onmicrosoft.com	1	0	

Microsoft Purview PREVIEW

Cases > enron

enron Case settings

Searches Hold Policies Review sets

Review sets

Analyze, organize, annotate, redact, and tag collected items for export. [Learn more about review sets](#)

Create review set Download list

Review set	Size	Created by	Last modified (UTC-12:00)	Modified by	Collections (sourc...)	Exports	Description
Enron RS	190.9 GB	admin@edbig.onmicrosoft.com	Oct 23, 2023 3:42:35 PM	admin@edbig.onmicrosoft.com	2	0	
Enron RS - 2	39.16 MB	admin@edbig.onmicrosoft.com	Dec 3, 2023 12:25:16 PM	admin@edbig.onmicrosoft.com	1	0	

Microsoft Purview

eDiscovery (Premium) > Cases > enron

Overview Data sources Collections Review sets Communications Hold Processing Exports Jobs and errors

Analyze, organize, annotate, redact, and tag collected items for export. [Learn more about review sets](#)

+ Add review set Rename review set Options

Filters: Size: Any Filters

Review set

Enron RS

Enron RS - 2

Enron RS

Overview Load sets Exports Jobs and errors

Time zone

Review set name

Enron RS [Edit name and description](#)

Description

-

Created on (UTC-12:00)
Oct 23, 2023 3:42:35 PM

Created by
admin@edbig.onmicrosoft.com

Last modified (UTC-12:00)
Oct 23, 2023 3:42:35 PM

Last modified by
admin@edbig.onmicrosoft.com

Size
190.90 GB

Collections
2

Exports
0

[Open review set](#)

4) Click an item you'd like to summarize from the review set item list page.

The screenshot shows the Microsoft Purview eDiscovery interface. The left sidebar has navigation options like Home, eDiscovery (Premium), Cases, and Enron RS. The main area shows a list of 20 selected items. Item 18 is highlighted with a blue border. The list includes columns for #, Subject/Title, Date (UTC-12:00), Sender/Author, File class, and Message type. Item 18's details are expanded:

Re: gouging

From: Drew Fossum <User6@edbig.onmicrosoft.com> on behalf of Drew Fossum
Sent on: Sunday, November 26, 2000 7:23:00 PM
To: Susan Scott
CC: Kathy Ringblom; Michael Moran
Subject: Re: gouging

Excellent reading of the legal authority issues as well as the political winds. I think your sense of the likelihood of trouble is accurate. I also agree with your implicit premise that if FERC or anyone else wanted to make trouble regarding our negotiated rate deals, the easiest approach, and the most direct one, is to challenge the deals as unjust and unreasonable under NGA section 4/5. To challenge the deals under some state law "gouging" theory would give rise to preemption defenses on our part, etc. I'll talk to you and Kathy further tomorrow AM and then we can grab Mike to discuss. Thanks. DF

5) Click “Summarize”. (Note: Security Copilot can only summarize items with file type with [text extraction support](#))

The screenshot shows the Microsoft Purview eDiscovery interface with a 'Keywords' filter applied: 'unfair advantage of their...'. Item 18 is selected and expanded. The 'Summarize' button is highlighted in blue at the bottom of the list. A 'Security Copilot' panel is open on the right:

Security Copilot

Dec 3, 2023 1:2 PM

The data you provided is a series of email exchanges that relate to potential legal and regulatory challenges associated with high-value transport deals. The discussion primarily revolves around the possibility of these deals being perceived as "unjust and unreasonable" under the Natural Gas Act and Federal Power Act. This could potentially invite intervention from regulatory bodies like the Federal Energy Regulatory Commission (FERC). The conversation also touches upon the political implications of these deals and the necessity to keep a close watch on other pipelines serving California. The participants in the email exchange unanimously agree on the need for caution and further discussion to fully comprehend the depth and potential repercussions of the situation.

AI generated. Verify for accuracy

Please identify key participants
Please identify key topics
Please identify action items

Ask questions and get insights about this message.

Copilot doesn't reference prior responses when responding to new questions about this message.

6) Ask additional questions or click one of the default prompts to gain further insights into the generated summary.

Please identify key participants

Please identify key topics

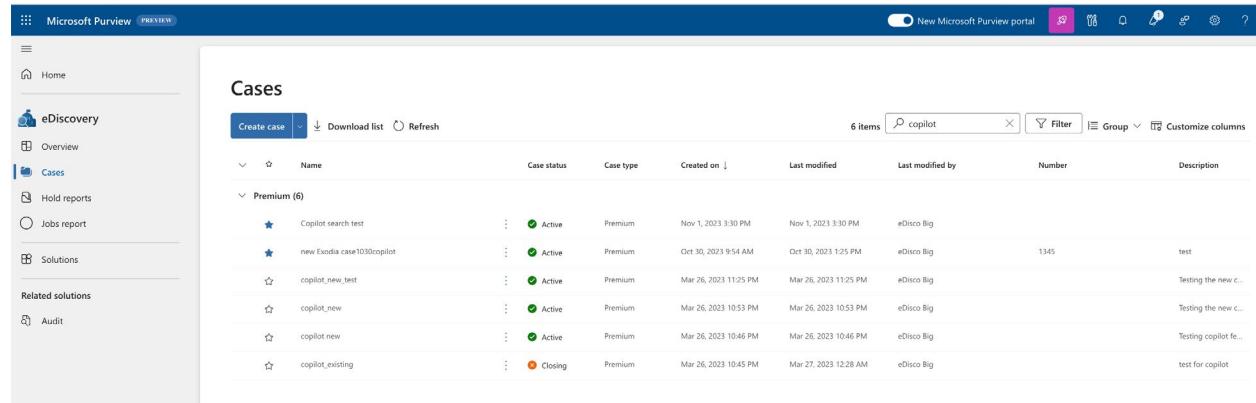
Please identify action items

Does custodian Drew have any action items from this email?

Copilot doesn't reference prior responses when responding to new questions about this message.

Generate a search query using Security copilot (**COMING SOON**)

1) Navigate to the new Purview portal (purview.microsoft.com/ediscovery/casespage)



The screenshot shows the Microsoft Purview eDiscovery interface. On the left, there's a sidebar with 'eDiscovery' selected under 'Overview'. The main area is titled 'Cases' and shows a list of cases. The list includes columns for Name, Case status, Case type, Created on, Last modified, Last modified by, Number, and Description. There are 6 items listed:

Name	Case status	Case type	Created on	Last modified	Last modified by	Number	Description
Copilot search test	Active	Premium	Nov 1, 2023 3:30 PM	Nov 1, 2023 3:30 PM	eDisco Big		
new Exodia case1010copilot	Active	Premium	Oct 30, 2023 9:54 AM	Oct 30, 2023 1:25 PM	eDisco Big	1345	test
copilot_new_test	Active	Premium	Mar 26, 2023 11:25 PM	Mar 26, 2023 11:25 PM	eDisco Big		Testing the new c...
copilot_new	Active	Premium	Mar 26, 2023 10:53 PM	Mar 26, 2023 10:53 PM	eDisco Big		Testing the new c...
copilot_new	Active	Premium	Mar 26, 2023 10:46 PM	Mar 26, 2023 10:46 PM	eDisco Big		Testing copilot fe...
copilot_existing	Closing	Premium	Mar 26, 2023 10:45 PM	Mar 27, 2023 12:28 AM	eDisco Big		test for copilot

2) Navigate to an eDiscovery (Premium) case. Then navigate to searches.

3) Click "Draft with Security Copilot"

The screenshot shows the Microsoft Purview eDiscovery interface. On the left, there's a sidebar with options like Home, eDiscovery (selected), Overview, Cases (selected), Hold reports, Jobs report, Solutions, and Audit. The main area shows a search for 'fabrikam' under 'Cases > enron > Searches > fabrikam'. The search bar contains 'Query: mark 8 (c:s) (c:c)'. Below it are tabs for Query (selected), Statistics, and Sample. A 'Draft with Security Copilot' button is visible. The 'Condition Builder' section shows an AND filter with 'Keywords Equal mark 8 (c:s)'. There are buttons for Run query and Save as draft.

4) Provide your own natural language input or select one of the suggested prompts

Cases > enron > Searches > fabrikam

fabrikam Draft

Query: mark 8 (c:s) (c:c)

Security Copilot Preview

Natural language prompt

Type your search query including user, data source and content details.

Find all emails containing the words budget and finance and have attachments.

Prompt Suggestions

- Find all emails containing the words budget and finance and have attachments.
- Search all chats in the month of January 2020 that contain the word 'financial year'
- Search for files of type .docx that contain the words confidential and budget

Generate KQL

Refine

Suggested prompts

5) (optional) Click “Refine” to optimize your natural language input for Security Copilot. Either accept or discard the suggested refinement.



Security Copilot Preview

Natural language prompt

Type your search query including user, data source and content details.

Find all emails containing the words budget and finance and have attachments.

Generate KQL

Refine

Suggested prompts



Security Copilot Preview

Natural language prompt

Type your search query including user, data source and content details.

Find all emails containing the words budget and finance and have attachments.

Refining prompt...

 Security Copilot [Preview](#)

Natural language prompt

Type your search query including user, data source and content details.

Search for all emails that contain the words 'budget' and 'finance' and also have attachments.

✓ Accept X

AI generated. Verify for accuracy  

6) Click “Generate KQL” to generate a search query from the natural language input.

[Query](#) [Statistics](#) [Sample](#)

 Security Copilot [Preview](#)

Natural language prompt

Type your search query including user, data source and content details.

Search for all emails that contain the words 'budget' and 'finance' and also have attachments.

ⓘ Generate KQL ⓘ Refine ⓘ Suggested prompts

Keyword Query Language (KQL) result

Copy the KQL result generated by Copilot and paste it in your original search query window at the bottom of the page.

Generating KQL...

7) Click “Copy KQL” to copy the KQL result generated by Copilot and paste it in your original search query window at the bottom of the page.

The screenshot shows the Microsoft Security Copilot interface. A modal window titled "Keyword Query Language (KQL) result" is displayed. It contains the generated KQL query: ("budget" AND "finance") AND HasAttachment:true. Below the query is a "Copy KQL" button. To the right of the button, a message says "AI generated. Verify for accuracy" with a small AI icon. The background shows the main Copilot interface with a search bar and some results.

The screenshot shows the Microsoft Security Copilot interface. On the left, there's a sidebar with "Data sources" and a "Start by adding data sources" button. The main workspace has tabs for "Condition Builder" and "Keyword Query Language (KQL)". The KQL tab is active, displaying the query: ("budget" AND "finance") AND HasAttachment:true. Below the query, it says "0 errors detected". At the bottom of the workspace, there are "Run query" and "Save as draft" buttons. The top of the screen shows the Copilot logo and a "Natural language prompt" input field.

Evaluating Security Copilot - Purview eDiscovery

As you use Security Copilot - Purview eDiscovery, we encourage you to think about the following questions and scenarios:

- How easy or difficult is it to access and use Security Copilot for Purview eDiscovery as an embedded experience within Microsoft Security Copilot?
- How useful or valuable is the information and insights provided by Security Copilot for Purview eDiscovery?
- How would you rate the performance, reliability, and usability of Security Copilot - Purview eDiscovery?

- What are the features or capabilities that you like the most or the least about Security Copilot for Purview eDiscovery?
- What are the features or capabilities that you would like to see added or improved in Security Copilot for Purview eDiscovery?

Limitations and known issues

Please note that Security Copilot - Purview eDiscovery is currently in private preview and has some limitations and unsupported scenarios that you should be aware of:

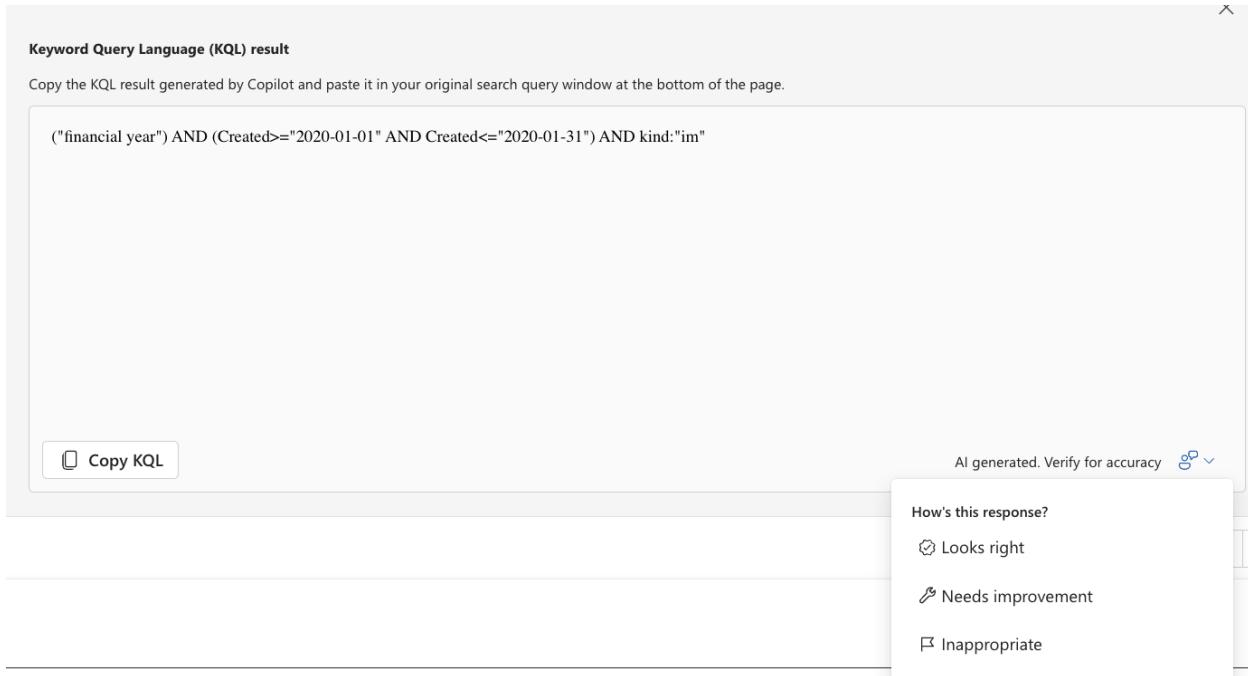
- Security Copilot activities are not protected by Purview.
 - No audit activities are available for Security copilot activities.
 - Security copilot activities are not discoverable in Purview eDiscovery. You can't search and preserve Security copilot activities.
 - Not covered under M365 copilot protections, [Microsoft Purview data security and compliance protections for Microsoft Copilot | Microsoft Learn](#)
- Security Copilot is not available in eDiscovery (Standard) cases.
- Contextual summary
 - Security Copilot can summarize up to 15,000 words (20,000 tokens). Please reference the "word count" metadata field value to check if an item will hit the word count limit.
 - Security Copilot only support single-item summary. This private preview version does not support multi-item summary for family or conversation groups.
 - Supported file type: plaintext view must be available. Security Copilot can only summarize items with file type with [text extraction support](#).
 - Security Copilot doesn't reference prior responses when responding to new questions about this message.
- Generate an eDiscovery search query with Copilot
 - This experience is only available on the [new Microsoft Purview portal \(preview\)](#).
 - Your organization must be enrolled to eDiscovery private preview for the new Microsoft Purview portal (preview)
 - Security Copilot generated search queries are subject to [existing query limits](#).
- [Responsible AI FAQ](#)

Support and Feedback

We appreciate your participation in the private preview of Security Copilot for Purview eDiscovery and we value your feedback.

Security Copilot and Purview eDiscovery uses AI and machine learning to process data and generate responses for each of the key features. However, AI might misinterpret some data, which sometimes cause a mismatch in responses. Providing your feedback about the generated responses enable both Security Copilot and Purview eDiscovery to continuously improve delivery of more accurate responses in the future.

All key features have an option for providing feedback. To provide feedback, perform the following steps:



1. Select the down arrow beside the face icon located at the bottom of any response card in the Security Copilot pane.
2. Select Confirmed, it looks great if the results are accurate based on your assessment. When results are confirmed, you can provide more information in the next dialog box.
3. Select Off-target, inaccurate if any detail is incorrect or incomplete based on your assessment. You can provide more information about your assessment in the next dialog box and submit this assessment to Microsoft.
4. You can also report the results if it contains questionable or ambiguous information by selecting Potentially harmful, inappropriate. Provide more information about the results in the next dialog box and select Submit.

Thank you for your interest and engagement in Security Copilot for Purview eDiscovery (Premium). We look forward to hearing from you and improving the solution based on your feedback.