Learn about Data Security Investigations (preview)

Article • 04/26/2025

Microsoft Purview Data Security Investigations (preview) helps cybersecurity teams in your organization harness generative artificial intelligence (AI) to analyze and respond to data security incidents, risky insiders, and data breaches. Investigations help you quickly identify risks from sensitive data exposure and more effectively collaborate with your partner teams to remediate the issues and simplify tasks that traditionally are time consuming and complex.

https://learn-video.azurefd.net/vod/player?id=cf1d0239-cb00-4db6-a925-dfdb9e605dd2&locale=en-us&embedUrl=%2Fpurview%2Fdata-security-investigations

Analysts can use Data Security Investigations (preview) features in your organization to:

- Quickly and efficiently search, discover, and identify impacted data.
- Use deep content AI analysis to discover exact data risks hidden in data.
- Take action to reduce the impact of data security incidents and quickly mitigate ongoing risks.
- Collaborate with internal and external stakeholders on investigation details.

Check out the Microsoft Mechanics video and the blog post announcement to learn about how Data Security Investigations (preview) can help you respond to data security incidents.

AI integration

Data Security Investigations (preview) uses generative AI to conduct deep content analysis and uncover key security and sensitive data risks for data included in investigations. AI helps analysts quickly analyze large volumes of data with high accuracy, saving critical time for triage, review, and mitigation actions.

There are three main AI-related investigative capabilities:

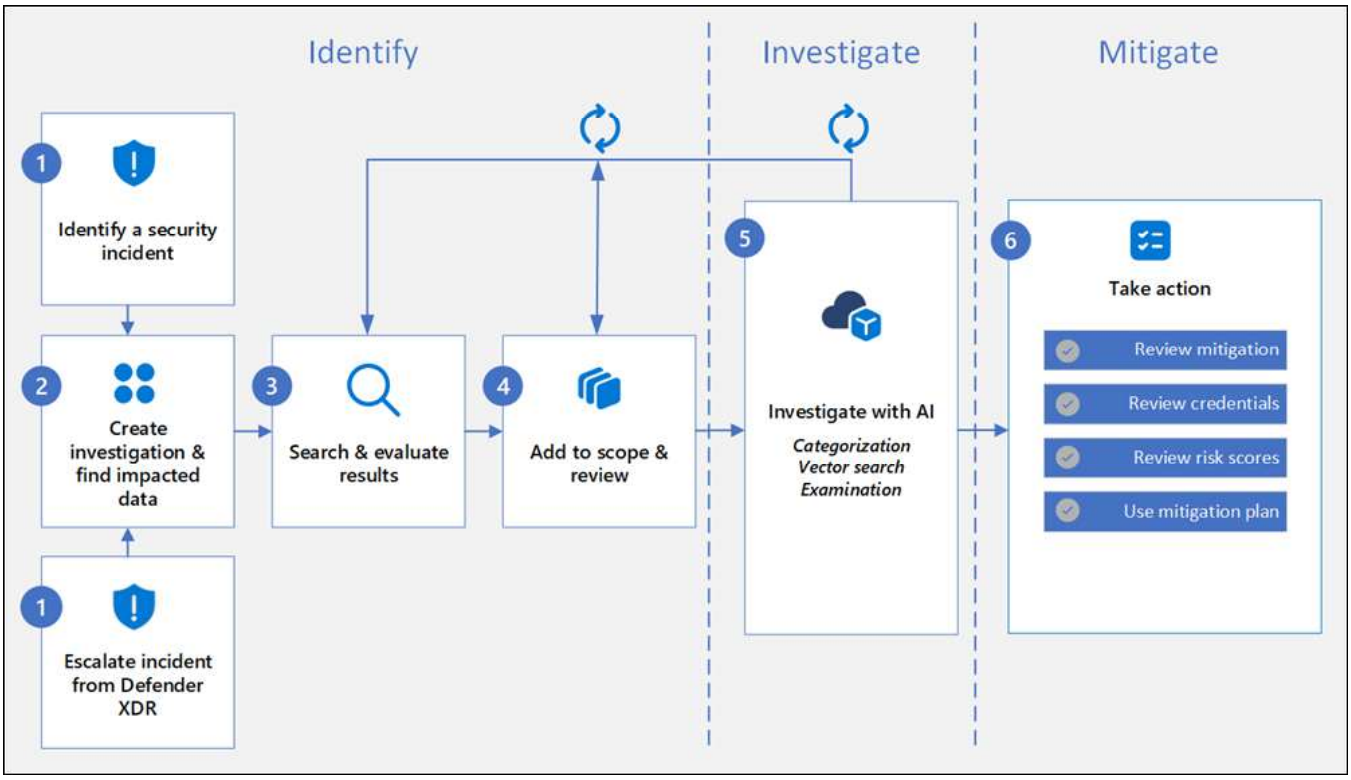
- **Vector search**: Vector-based semantic search enables similarity-based information retrieval and understands user intent beyond literal words. Analysts query impacted data to find all assets related to a particular subject, even if keywords are missing.
- **Categorization**: To get an initial understanding of incident severity, analysts can use AI to categorize impacted data, narrowing focus to high-risk assets. Data Security Investigations (preview) automatically sorts data into default, custom, or AI-suggested categories. Categorized items also including grouping by subject matter and risk level.

Learn about the Data Security Investigations (preview) workflow

Article • 05/05/2025

The Data Security Investigations (preview) workflow helps you quickly identify, investigate, and take action on data associated with security and data breach incidents. This workflow isn't a linear process, it includes significant iteration requirements for several of the steps to fine tune searches, evidence gathering, classification, and investigation using AI and activities.

Identifying and taking action on data and access uses the following workflow:



Step 1: Identify and escalate incidents

Identify a data security incident

Data breaches and other data security incidents require quick action to identify and contain potential risks to your organization. It's critical that you quickly identify these incidents and streamline an integrated response. Investigating a data security incident is daunting, and might include inefficient workflows across multiple tools, manual work, and extra complexity as the investigation grows in size, labor-intensive reviews of impacted data, and increased costs.

Data Security Investigations (preview) helps you investigate and mitigate data security incident and accelerate the time to resolution dramatically. After identifying a data security incident,

Learn about AI analysis in Data Security Investigations (preview)

Article • 04/26/2025

> **Important**
>
> Data Security Investigations uses generative artificial intelligence (AI), large language models, and orchestration in the analysis of data in your organization. Results generated by AI might not always be accurate or complete. While we strive to provide reliable and helpful information, AI systems can produce incorrect or false results. It is important to verify the information and use it with caution. Microsoft makes no warranties, express, implied, or statutory, as to the information provided by AI systems.

Data Security Investigations (preview) uses AI services and tools to help you quickly review and take action on items associated with security incidents. AI-related services include the following tools:

- Vector search
- Categorization
- Examination

Vector search

Vector search in Data Security Investigations (preview) gives you a way to contextually search through data that you add to the investigation scope using advanced orchestration and embeddings. Vector search is a search engine technology that focuses on understanding the meaning and context behind words and phrases in a query, rather than just matching keywords.

Some key aspects of vector search are:

- **Contextual understanding**: Vector search interprets the context of your search terms, considering factors like your organization, search history, and the overall meaning of the query.
- **Intent recognition**: Vector search works to understand your intent, whether you're looking for information, trying to take an action, or seeking a specific type of content associated with a search.
- **Relevance and accuracy**: By focusing on the semantics (the meaning and intent of words in your query), vector search provides more accurate and relevant results and improves the overall search experience.

Get started with Data Security Investigations (preview)

Article • 05/15/2025

Use Data Security Investigations (preview) to identify, investigate, and mitigate data risk either reactively when an incident occurs, or proactively to improve data security hygiene for your organization. Complete the following steps in the workflow to set up prerequisites and configure Data Security Investigations (preview).

For more information about how Data Security Investigations (preview) can help you with security incidents in your organization, see Learn about Data Security Investigations (preview).

Step 1: Read and agree to terms

The first time you access Data Security Investigations (preview) in the Microsoft Purview portal, you must read and agree to the terms of the Privacy Statement.

Confirm that you accept the terms and select **Get started**.

Step 2: Billing and usage

To get started with Data Security Investigations (preview), you must configure billing and usage settings for data storage and AI analysis features. Data Security Investigations (preview) uses a payment model based on how much data is added to investigations and how much AI capacity is used for analysis of that data.

For step-by-step guidance, see Billing models in Data Security Investigations (preview).

Step 3. Configure permissions

To allow users to access to Data Security Investigations (preview) tools in the Microsoft Purview portal, you must assign the users the appropriate permissions. The easiest way to assign roles is to use the setup task or add the user the appropriate role group on the **Role groups** page in the Microsoft Purview portal.

For step-by-step guidance, see Assign permissions in Data Security Investigations (preview).

Step 4. Create an investigation

Assign permissions in Data Security Investigations (preview)

Article • 05/05/2025

If you want users to use any Data Security Investigations (preview) capabilities and features in the Microsoft Purview portal, you must assign users the appropriate permissions.

This article describes the permissions required to perform specific Data Security Investigations (preview) tasks. For more information about Microsoft Purview role groups and permissions, see Permissions in the Microsoft Purview portal.

Roles and role groups

> **Important**
>
> After you configure your role groups, it might take up to 30 minutes for the role group permissions to apply to assigned users across your organization.

The easiest way to quickly assign the *Administrator* or *Investigator* roles to users when getting started is to use the **Assign roles to your team members** setup task. Complete the following steps to assign these roles:

1. Go to the Microsoft Purview portal with account with the *Global Administrator* roles assigned.
2. Select the **Data Security Investigations (preview)** solution card and then select **Overview** in the left nav.
3. Select **Assign roles to your team members** in the **Setup tasks** section.
4. On the **Role assignment** flyout pane, select users in the **Administrators** field.
5. Select users in the **Investigators** field.
6. Select **Confirm** to assign users these roles.

You can also add users to appropriate role group on the **Role groups** page in the Microsoft Purview portal. To continue with these configuration steps in the Microsoft Purview portal, you must be assigned to the *Data Security Investigations Admins* role group.

Configure permissions

Depending on how you want to manage Data Security Investigations (preview) workflow and investigations, you need to assign users to specific role groups to manage different sets of Data Security Investigations (preview) features. You have the option of assigning users with

Billing in Data Security Investigations (preview)

Article • 05/13/2025

Billing in Data Security Investigations (preview) is based solely on the combination of the amount of stored data and the associated computing capacity needed for AI analysis, not a dedicated enterprise plan or license.

This billing combination is based on the **storage meter** and **AI capacity** models. The Data Security Investigations (preview) non-AI processing and storage meter allows customers to store data related to an investigation. Security Compute Units (SCUs) are used to measure the computational capacity needed to run the AI analysis within Data Security Investigations (preview).

Storage meter

The storage meter for Data Security Investigations (preview) is based on the pay-as-you-go billing model. Storage is billed on a gigabyte (GB) per month basis for stored data associated with all investigations in your organization.

For example, you have three investigations in your organization that have the following data associated with the items included in the investigation scopes for the current month:

Expand table

Investigation	Items	Total data
Data breach 02/12/2025	3,766	200 GB
Potential data theft 03/03/2025	1,982	10 GB
Risky user activity 04/06/2025	287	5 GB

For the current month, you total storage meter would be 215 GB and you'd be billed for that amount at the current per gigabyte rate. When you delete an investigation, the associated data storage amount is no longer billed and the charges are prorated to the number of days the data was stored in the billing cycle.

Some other important considerations for managing storage charges:

- If you create an investigation, use data storage, and then delete the investigation in a single 24 hour period, you're charged for the storage amount.

Create an investigation in Data Security Investigations (preview)

Article • 04/26/2025

After configuring billing and usage options for Data Security Investigations (preview) and assigning permissions to analysts in your organization that manage investigations, the next step is to create and manage an investigation for collection and analysis activities.

Investigations dashboard

Depending on your permissions, investigations in your organization are displayed on the **Investigations** dashboard in the Microsoft Purview portal. If you're not assigned in the *Data Security Investigations Admin* role group, you can only view investigations you're assigned to as an investigator or reviewer.

The **Investigations** dashboard allows you to quickly see the investigations in your organization that you have access to, the description of the investigations, and important information associated with each investigation.

- **Name**: The name of the investigation. The investigations name must be unique in your organization.
- **Description**: The description of the investigation entered when the case was created.
- **Created on**: The date and time in Coordinated Universal Time (UTC) when the investigation was created.
- **Last modified**: The date and time in Coordinated Universal Time (UTC) when the investigation was last modified.

You can customize the displayed columns and the order of the columns in the **Investigations** dashboard by selecting **Edit columns**. Choose the columns to display or drag and drop columns to reorder.

Investigation templates

Investigation templates allow you to quickly create an investigation based on common data characteristics, data types, and using natural language queries. Only one template per investigation is supported. For the keyword, unique identifier, sensitive information types, and sensitivity labels, you also define the date range, users, and tenant source for the investigation.

The following investigation templates are available:

Create an investigation using full draft mode in Data Security Investigations (preview)

Article • 04/26/2025

Creating an investigation in full draft mode in Data Security Investigations (preview) provides the most flexibility and options for analysts investigating a data security incident. This process allows you to fully customize the data sources and query in your investigation.

Using full draft mode

Complete the following steps to create an investigation and configure the investigation scope using the *full draft mode*. The user who creates the investigation is automatically added as a member. Members of the investigation can access the investigation in the Microsoft Purview portal and perform Data Security Investigations (preview) tasks.

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations (preview) permissions. Members of the *Organization Management* role group can also create investigations.

2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.

3. Select **Create investigation**.

4. On the **Create a investigation** dialog, complete the following fields:

    - **Title**: Give the investigation a name (required). The investigation name must be unique in your organization.
    - **Description**: Add an optional description to help others understand this investigation.

5. Select **Switch to full draft mode**.

6. Select **Add data sources**

7. On the **Manage data sources** flyout pane, search and add data sources for your investigation query. You can filter to scope data sources to help you choose one or more users or group sources to add to the investigation.

    Use one or more of the following options in the **Search for people, groups, locations, or tenant locations** field to select from the following default filters:

Investigation settings in Data Security Investigations (preview)

Article • 04/26/2025

Investigation details allow you to view and update investigation information and to take action on specific investigations.

Investigation details

The following information is displayed for the selected investigation:

- **ID**: Displays the investigation identification number. This ID can be reviewed, but can't be changed once the investigation is created.
- **Investigation name**: Displays the investigation name. This field is required. To change the investigation name, enter the new investigation name and select **Actions** > **Save**.
- **Investigation description**: Displays an optional description to help others understand this investigation. To change the investigation description, enter the new investigation description and select **Actions** > **Save**.
- **Investigation status**: Displays the current investigation status.
- **Investigation created**: Displays the date and time when the investigation was created.

Delete an investigation

You can delete investigations when they're no longer needed for your organization. When you delete an investigation, all components associated with the investigation, such as searches, investigation scopes, and mitigation plans are deleted. You can't recover a deleted investigation.

To delete an investigation, complete the following steps:

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left navigation pane.
3. Select an investigation, the select **Investigation settings**.
4. On the **Investigation settings** page, select **Actions**, and then select **Delete investigations**.

Configure investigation access and permission settings in Data Security Investigations (preview)

Article • 04/26/2025

Access and permission settings in Data Security Investigations allow you to add or remove users to an investigation, manage role group membership for an investigation, and to people outside your organization as guest users for an investigation.

Add or remove users from an investigation

You can add or remove users to manage who can access the investigation. However, before a user can access an investigation (and perform tasks in the investigation), you must add the user to the *Data Security Investigations Manager* role group in the Microsoft Purview portal. For more information, see Assign Data Security Investigations (preview) permissions.

Adding users to an investigation

Complete the following steps to add users to an investigation:

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations (preview) permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.
3. Select an investigation, the select **Investigations settings**.
4. On the **Investigation settings** page, select **Permissions**.
5. Under **Users**, select **Add** to add users to the investigation. You can also choose to add a role group to the investigation by selecting **Add** under **Role groups**.
6. In the list of users or role groups that can be added to the investigation, select the check box next to the names of the users or role groups that you want to add.

> **Note**
>
> When adding a role group to an investigation, you can only add the role groups that you're a member of.

Search, review, and refine results in Data Security Investigations (preview)

Article • 04/26/2025

You can use search in Data Security Investigations (preview) to search for Microsoft 365 content such as email, documents, and instant messaging conversations in your organization that are relevant to a security incident. Use search to find content in these cloud-based Microsoft 365 data sources:

- Exchange Online mailboxes
- SharePoint sites
- OneDrive accounts
- Microsoft Copilot prompts and responses
- Microsoft Teams

You can create and run different searches that are associated with an investigation. You use conditions (such as keywords, file types, incidents, etc.) to build search queries that return search results with the data that's most likely relevant to the investigation. You can also:

- View search statistics that might help you refine a search query to narrow results.
- Preview the search results to quickly verify whether the relevant data is being found.
- Revise a query and rerun the search.

When you're satisfied with the results of a search and you're ready to review and analyze the results, you can add them to an investigation scope in the investigation. Adding copies of the original data to an investigation scope also facilitates the AI analysis and review process by providing you with advanced categorization, examination, and vector search tools.

Access search tools

Select the **Summary** from the navigation options at the top of any page within a specific investigation to access search tools.

Search tools include the data source picker, the query builder, and the search by file options. You can refine search query data sources and conditions at any time during the investigation and add the results to an investigation scope.

Data sources

In Microsoft 365, data is stored across three platforms: Exchange, Teams, and SharePoint. These platforms serve as the backbone for organizing and managing data within Microsoft 365

Manage investigation scopes in Data Security Investigations (preview)

Article • 04/26/2025

After adding data items from your search queries to the scope of the investigation, you're ready to start working with your data and validate items before preparing for AI analysis. An investigation scope contains all the data items from your search results that you want to analyze and review. This data is now available for AI preparation and further review by analysts in your organization.

Access the investigation scope

Select the **Analysis** from navigation options at the top of any page within a specific investigation to access the investigation scope. The investigation scope includes a dashboard of scoped items and includes filter and viewer tools to help with item review.

Investigation scope dashboard

The investigation scope dashboard lists all the scoped data items in an investigation. This dashboard allows you to review details about individual data items and displays information about each item.

The investigation scope dashboard contains the following information and controls:

- **Subject/Title**: The subject/title of the data item.
- **Exclude**: The exclude status of a data item. Values are *Yes* or blank.
- **Vectorized**: The vectorization status of a data item. Values are *Yes* or blank.
- **Date**: The date and time the data item was last modified.

To customize the columns display on the investigation scope dashboard, select **Customize columns** to choose the columns to display or drag and drop the columns in the list to reorder.

To download the list of data items and the column information, select **Download list** to create a .csv file containing this information.

Grouping data items

When viewing a large list of data items in an investigation, it's often helpful to group the investigation scope by family or conversations and related items. Select **Group** to group data items by this criteria.

Group and view items in an investigation scope in Data Security Investigations (preview)

Article • 04/26/2025

Data Security Investigations (preview) investigation scopes display content using different grouping options and include specialized viewers that you can use to examine details about individual items.

Grouping

Use the **Group** control in the command bar of an investigation scope to view review content grouped by the following options:

- **Group by families**: All items related to a specific file are grouped together using the same Group ID. For example, if you have a PowerPoint file in the investigation scope that includes imbedded images or .zip files, these images and files are grouped with the PowerPoint file and shown as nested items with the file in the item list view. Microsoft 365 Copilot and Microsoft 365 Copilot Chat user prompts and responses are also grouped together using the same Group ID when there are multiple prompts and responses associated with a file.
- **Group by conversations**: All email messages, Teams conversations, and Viva Engage conversations are grouped using the same Thread ID and appear as nested items. Additionally, all associated content for these messages and conversations is also grouped together. For example, if you have an email conversation that includes several email messages, some of which include attachments and some that include embedded images, all of the email messages, attachments, and images are grouped together in the investigation scope list view under an applicable item.

Source view

The **Source** viewer displays the richest view of a selected document. It supports hundreds of file types and is meant to display the truest to native experience possible. For Microsoft Office files, the viewer uses the web version of Office apps to display content such as document comments, Microsoft Teams chats, Excel formulas, hidden rows/columns, and PowerPoint notes.

Plain text view

Use AI analysis in Data Security Investigations (preview)

Article • 05/05/2025

After AI preparation and vectorization is complete for your investigation scope, you're ready to review and use AI analytics tools for the data in the investigation. Generative AI processing conducts a deep content analysis of selected items and can uncover key security and sensitive data risks within impacted data.

To get started with AI analysis in an investigation, complete the following steps:

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.
3. Select an investigation, then select **Analysis** on the navigation bar.

Use vector search

Use vector search to describe what you're looking for in the vectorized data items in the investigation scope. Vector-based semantic search enables similarity-based information retrieval and understands user intent beyond literal words. You can query their impacted data to find all assets related to a particular subject, even if keywords are missing. For example, a pharmaceutical company might use vector search to find all emails, documents, Copilot prompts and responses, and Teams messages related to vaccine trials to identify relevant assets that don't mention the words *vaccine* or *trial* but remain pertinent to the investigation.

You can use natural language to ask a question or enter phrases with specific focus to narrow down items for review. There aren't any additional secure compute units (SCU) related capacity costs associated with vector search queries, the previous processing is completed for these scoped items.

To create a vector search, complete the following steps:

> **Important**
>
> You must prepare data for AI analysis before using vector search.

1. In an investigation, select **Analyze** > **Analysis**.
2. Describe what you're looking for in the **Vector search** field.
3. Select **Vector search** or select enter.

Review mitigation recommendations in Data Security Investigations (preview)

Article • 04/26/2025

Analyze data for mitigation information

Complete the following steps to identify risks in data items included in the investigation scope:

> **Important**
>
> You must prepare data for AI analysis before configuring examinations.

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations (preview) permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.
3. Select an investigation, then select **Analysis** on the navigation bar.
4. Use vector search or categorization tools to identify data for credentials examination.
5. Select one or more items, then select **Examine** on the command bar.
6. In the **Examine with AI** dialog, enter name for your examination process in the **Job name** field.
7. Enter a description for the examination process in the **Job description** field.
8. Select *Mitigate: Identify threats and recommended mitigation steps in selected items* in the **Choose a focus area** field.
9. Select **Examine** to start the AI analysis.

> **Note**
>
> The time estimates for the process to complete is based on the amount and size of the selected data. To reduce processing time, filter and exclude data not applicable to the investigation.

Mitigation recommendation report

After the AI processing is completed for the selected data items, you can review the mitigation plan to identify details and recommended mitigation steps for each item.

The mitigation recommendation reports include the following information for each item:

Review credentials examinations in Data Security Investigations (preview)

Article • 04/26/2025

Understanding how credentials and other asset access information is associated with a data security incident is an important part of identifying and mitigation risks.

For example, if you discover credentials within impacted data associated with the data security incident, a Microsoft Entra admin in your organization can join the investigation, securely view the extracted credentials, and take necessary next steps to reset the accounts. You can also use investigation learnings to refine existing account management policies to strengthen your organization's security practices.

Analyze data for credentials and asset access information

Complete the following steps to identify credentials and asset access data in items included in the investigation scope:

> **Important**
>
> You must prepare data for AI analysis before configuring examinations.

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations (preview) permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.
3. Select an investigation, then select **Analysis** on the navigation bar.
4. Use vector search or categorization tools to identify data for credentials examination.
5. Select one or more items, then select **Examine** on the command bar.
6. In the **Examine with AI** dialog, enter name for your examination process in the **Job name** field.
7. Enter a description for the examination process in the **Job description** field.
8. Select *Credentials: Extract credentials and access assets in the selected items* in the **Choose a focus area** field.
9. Select **Examine** to start the AI analysis.

> **Note**

Review risk examinations in Data Security Investigations (preview)

Article • 04/26/2025

By examining impacted data for security risks, you can find network risks or data that presents continued security risks in your organization. Risk examinations provide reasoning for risk scores and recommended mitigation steps for each item so you can take the appropriate mitigation steps. Scores and explanations are summarized for the risk focus areas.

Analyze data for risk information

Complete the following steps to identify risks in data items included in the investigation scope:

> **Important**
>
> You must prepare data for AI analysis before configuring examinations.

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.
3. Select an investigation, then select **Analysis** on the navigation bar.
4. Use vector search or categorization tools to identify data for credentials examination.
5. Select one or more items, then select **Examine** on the command bar.
6. In the **Examine with AI** dialog, enter name for your examination process in the **Job name** field.
7. Enter a description for the examination process in the **Job description** field.
8. Select *Risk: Analyze and score all active risks in selected items* in the **Choose a focus area** field.
9. Select **Examine** to start the AI analysis.

> **Note**
>
> The time estimates for the process to complete is based on the amount and size of the selected data. To reduce processing time, filter and exclude data not applicable to the investigation.

Risk examinations include the following information for each item:

Use the mitigation plan in Data Security Investigations (preview)

Article • 04/26/2025

The mitigation plan helps connect analysis to specific mitigation actions from examination tools and analyst reviews. The mitigation plan is like a to-do list that you can use to help manage and track data risk mitigation actions in your investigation. This plan helps analysts centralize all items that require attention or action to mitigate risks associated with the investigation and data security incident.

Mitigation plan dashboard

All items added to the mitigation plan in your investigation are displayed on the **Mitigation plan**. This view allows you to quickly see the all the items that need action in your investigation, the status for each item, and other important information about each item in the plan.

- **Name**: The subject or title of the data item.
- **Type**: The file type of the data item.
- **Description**: The description of the data item.
- **Status**: The current status of the data item. Values include *In-progress* or *Complete*.
- **Last modified by**: The name of the analyst or investigator that last updated information about the data item.
- **Last updated (UTC)**: The date and time in Coordinated Universal Time (UTC) that the data item was last updated.

You can customize the displayed columns and the order of the columns in the mitigation plan by selecting **Customize columns**. Choose the columns to display or hide. To filter items in the mitigation plan, select **Add filter** and choose an available filter.

To download the list of data items and the column information in the mitigation plan, select **Download list** to create a .csv file containing this information.

Item detailed view

Analysts can view details about each data item included in the mitigation plan as part of the review and evaluation process. After you select a data item, an item summary and viewers are available for the analyst to view metadata, source, and other information.

Update item status

Use the Activity history in Data Security Investigations (preview)

Article • 05/06/2025

The Activity history for Data Security Investigation displays information about activities performed in each area of your investigation. Activities associated with searches, investigation scopes, AI analysis, and mitigation activities are included in the Activity history.

Each time an activity is created or requested in a workflow area, specific activities are automatically started and logged in the Activity history. For example, if you search for data and select **Estimate scope* in an investigation, *Generate statistics* and *Generate sample* activities are listed in the Activity history list for the investigation.

To view and manage activities, complete the following steps:

1. Go to the Microsoft Purview portal and sign in using the credentials for a user account assigned Data Security Investigations (preview) permissions.
2. Select the **Data Security Investigations (preview)** solution card and then select **Investigations** in the left nav.
3. Select an investigation, then select the **Activities** tab.

Activity history dashboard

The Activity history dashboard lists all the activities for an investigation and contains the following information for each activity:

- **Activity type**: The type of activity.
- **Status**: The status of the activity.
- **Export name**: The name of the export. For nonexport activity types, this value is blank.
- **Created**: The date and time the activity was created.
- **Completed**: The date and time the activity was completed.
- **Duration**: The duration of the activity.
- **Created by**: The user that created the activity.

To customize the columns display for the Activity history, select **Customize columns** to choose the columns to display or drag and drop the columns in the list to reorder. To download the list of activities and the column information, select **Download list** to create a .csv file containing this information.

Grouping activities

Responsible AI FAQ for Data Security Investigations (preview)

FAQ

What is Data Security Investigations (preview)?

Microsoft Purview Data Security Investigations (preview) is a tool for cyber security professionals to quickly and thoroughly analyze their organization's data after a data security incident. Each investigation includes the specific organizational data (files, emails, messages, etc.) an investigator decides to include. It then uses AI to generate data categories to drive search, risk identification and ratings to aid in prioritization, and recommendations at the end of the process to help mitigate the breach.

What can Data Security Investigations (preview) do?

Data Security Investigations (preview) has AI functionality in three main areas:

- **Vector search**: Data Security Investigations (preview) uses artificial intelligence to create vector search embeddings on user data. Vector search allows users to use context and meaning to improve the relevance of search results.
- **Categorization**: Once users identify data for their investigation, Data Security Investigations (preview) provides functionality to categorize data with AI. With this functionality, users select categories they deem as relevant to their investigation. Once some vector searches are completed, users are presented with AI-suggested categories. These categories also include risk and impact scoring to help prioritize the investigation.
- **Examination**: After filtering investigation data with analysis tools, users choose from several built-in Large Language Model (LLM) features to get a deeper understanding of potential risks in their data.

What is the intended use for Data Security Investigations (preview)?

Data Security Investigations (preview) is intended to be used as a post-breach investigation and mitigation product. Data security analysts can also use Data Security Investigations (preview) to understand content risk around risky insiders, data over-sharing, or spillage events

Privacy FAQ for Data Security Investigations (preview)

FAQ

How is my data stored in Microsoft Purview Data Security Investigations (preview)?

When you use Data Security Investigations (preview), Microsoft copies user queried organization data from the Microsoft 365 application storage to tenant-isolated regional investigation storage. This data is stored until Data Security Investigations (preview) administrators or investigators delete the investigation. Only Data Security Investigations (preview) Administrators, Investigators, and Reviewers have access to this data in your organization.

How is my data processed for Data Security Investigations (preview) AI features?

Data Security Investigations (preview) partners closely with Microsoft Security Copilot platform to power Data Security Investigations (preview) AI features. This means that data leaves Data Security Investigations (Microsoft 365 compliance area) and travels to Microsoft Security Copilot (Microsoft Azure compliance area) for up to 48 hours and return with AI generated content and insights. This generates the vector embeddings for vector search, category and subject generation, and examination results.

To ensure user privacy, all data sharing, logging, and scanning is turned off by default for Microsoft Security Copilot processing of Data Security Investigations (preview) data. For more information on Microsoft Security Copilot, see Privacy and data security in Microsoft Security Copilot

What feedback information does Data Security Investigations (preview) collect?

Data Security Investigations (preview) collects customer feedback to enhance its AI features and improve user experience. This feedback is gathered during the public preview stage and includes specific metrics related to the AI features' inputs and outputs.