

Learn about Data Security Posture Management (preview)

Article • 01/02/2025

Strengthening data security and minimizing exposure to data risks for sensitive information is often challenging for organizations in the modern workplace. The increasing complexity of data, the variety of data sources and platforms, limited visibility into sensitive data, and fragmented security solutions can pose significant challenges for administrators and data security professionals. Adding multicloud platforms and generative AI applications to these areas makes it even more difficult to assess data security coverage and to correlate insights from user data points. To help discover and mitigate data risks, organizations must address the following questions:

- What is my sensitive data?
- Where is it located?
- What data is currently unprotected?
- How is unprotected sensitive data being handled and accessed?
- How can I help lower the risk and help secure unprotected sensitive data?

Microsoft Purview Data Security Posture Management (DSPM) (preview) allows you to quickly and easily monitor cross-cloud data and user risk through dynamic reports and trend analysis. By processing and correlating across other Microsoft Purview data security and risk and compliance solutions, DSPM (preview) helps you identify vulnerabilities with unprotected data and quickly take action to help you improve your data security posture and minimize risk. DSPM (preview) provides:

- **Data security recommendations:** Gain insights into your data security posture and get recommendations for creating insider risk management and data loss prevention (DLP) policies to help protect sensitive data and to close data security gaps. For example, some recommendations may include creating policies to prevent users from printing sensitive files or to prevent users from copying sensitive files to other network locations.
- **Data security analytic trends and reports:** Track your organization's data security posture over time with reports summarizing sensitivity label usage, DLP policy coverage, changes in risky user behavior, and more.
- **Microsoft Security Copilot:** Use Security Copilot to help you investigate alerts, identify risk patterns, and pinpoint the top data security risks in your organization.



Get started with Data Security Posture Management (preview)

Article • 01/02/2025

Use Data Security Posture Management (DSPM) to quickly identify unprotected sensitive data assets and potentially risky user activities in your organization. Complete the steps in this article to get started with the DSPM (preview) [workflow](#).

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the [Microsoft Purview trials hub](#) [↗]. Learn details about [signing up and trial terms](#).

Subscriptions and licensing

Before getting started with DSPM (preview), you should confirm your [Microsoft 365 subscription](#) [↗] and any add-ons. Depending on the licensing and subscriptions for your organization, you have access to other data security and risk and compliance solutions in the Microsoft Purview portal.

To access and use DSPM (preview), you need a Microsoft 365 E5 or Microsoft 365 E5 Compliance license. Administrators need to verify that their organization has a supported subscription and the appropriate licenses are assigned to users. For more information about subscriptions and licensing, see the [subscription requirements](#) [↗] for DSPM (preview).

Step 1: Assign permissions

Important

If your permissions are restricted in specific administrative units in your organization, you can't access DSPM.

To continue with these configuration steps, you must be assigned to one of the following roles or role groups:

Take action with Data Security Posture Management (preview) recommendations

Article • 01/02/2025

Recommendations in Data Security Posture Management (DSPM) (preview) are generated directly from the processed data, current state of unprotected sensitive assets in your organization and the user activities that put the unprotected sensitive assets at risk. Specific recommendations allow you take action and to quickly create data loss prevention (DLP) and insider risk management policies to help you mitigate data security risks. DSPM (preview) recommendations can also help you identify coverage gaps in existing insider risk management and DLP policies.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the [Microsoft Purview trials hub](#) [↗]. Learn details about [signing up and trial terms](#).

Using recommendations

To display and review recommendations, navigate to **Data Security Posture Management > Overview** or **Data Security Posture Management > Recommendations**.

- From the **Overview** page, you can review the top two data security recommendations or select **View all recommendations** for a complete listing of all recommendations.
- From the **Recommendations** page, you can directly review a complete listing of all recommendations.

Recommendations are generated from the last 30 days of user activity and the state of unprotected sensitive assets. As processing continues, the list of recommendations is automatically updated and the recommendations older than 30 days are removed.

Each recommendation provides a short description of the risky activity or state of the unprotected sensitive asset and includes a recommended policy to configure to help mitigate ongoing and future data security risks. Metrics for the number of activities, the

Use Data Security Posture Management analytics (preview) trends and reports

Article • 01/02/2025

Data security posture management (DSPM) (preview) analytics trends and reports help provide a quick view into the unprotected and protected sensitive assets and potentially risky user activities in your organization.

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the [Microsoft Purview trials hub](#) [↗]. Learn details about [signing up and trial terms](#).

Working with reports

For each report, use the following features to help filter, review, evaluate, and export DSPM insights:

- **Charts:** Hover on specific areas of report information for metrics and more details about insights.
- **Customize columns:** Select **Customize columns** to add or remove columns and associated information from a report.
- **Export:** Select **Export** to create a .csv file that contains the values included in a report.

Analytics reports


- **Unprotected sensitive assets across data sources:** This report displays the location of sensitive assets containing one or more classifiers (sensitive information types, exact data match classifiers, trainable classifiers) and:
 - Aren't protected by a data loss prevention (DLP) policy that restricts exfiltration activities.
 - Don't have a sensitivity label applied that controls access.
- **Users performing top risk-related activities on unprotected sensitive assets:** This report displays the number of users flagged by [insider risk management](#) (departing

Use Microsoft Security Copilot with Data Security Posture Management (preview)

Article • 01/02/2025

Use Microsoft Security Copilot and Data Security Posture Management (DSPM) (preview) to quickly dive into the details and get answers about unprotected sensitive data assets and potentially risky user activities in your organization. Data security insights are generated from scanned data across data loss prevention (DLP), information protection, and insider risk management solutions.


Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the [Microsoft Purview trials hub](#) . Learn details about [signing up and trial terms](#).

Get started with Copilot

After you [configure DSPM \(preview\)](#), [onboard your organization](#) to Security Copilot, and the automated scanning has completed, you can use suggested or customized prompts in Copilot to quickly learn more about your data security posture.

To get started with Copilot, complete the following steps:

1. Go to the [Microsoft Purview portal](#)  and sign in using the credentials for a user account assigned DSPM (preview) permissions.
2. Select the **Data Security Posture Management** solution card and then select **Overview** in the left nav.
3. Select one of the suggested prompts for Security Copilot:
 - a. **Prioritize alerts:** See which alerts were triggered in the last 30 days for users leaving your organization.
 - b. **Detect sensitive data leaks:** See which sensitive files were shared outside of your organization from SharePoint in the last week.
 - c. **Find devices at risk:** See which devices were involved in exfiltration activities in your organization.

Responsible AI FAQ for Data Security Posture Management

FAQ

What is Data Security Posture Management and Copilot?

[Data Security Posture Management \(DSPM\)](#) provides data security admins with a holistic view and insights of their sensitive data landscape. This includes visibility into new risks and vulnerabilities and contextual recommendations to optimize your organization's data security posture. The Copilot experience in DSPM is an open-ended prompt experience which uses generative AI to provide responses to help accelerate time to action and help data security analysts with their data security investigations.

What can the DSPM and Copilot do?

DSPM highlights data and user risk insights through dynamic reports and trend analysis. View your top data security risks and explore recommendations to enhance protections in your organization. With Copilot embedded into the experience, you can use the quick start prompts in data-security-posture-management to launch Copilot or select **Copilot** in the portal shell and ask questions in natural language about data security.

What are DSPM and Copilot's intended uses?

DSPM is an in-product experience in the [Microsoft Purview portal](#) that provides customer insights, reports, and recommendations across several data security solutions in Microsoft Purview. A Copilot experience is embedded in DSPM where you can ask detailed questions using an open-prompt free text in natural language about the data in DSPM and about other data security solutions in Microsoft Purview.

From the DSPM, you can also launch Copilot via quick start prompts. If you have how-to or troubleshooting questions, Copilot can answer these questions based on public documentation in relevant areas. The DSPM Copilot experience includes suggested prompts to assist you when asking follow-on questions. This feature significantly expedites data security investigations, enabling the swift identification and comprehension of hidden vulnerabilities.