Learn about data loss prevention

By chrfox

Archived: 2026-04-05 23:20:46 UTC

Organizations control sensitive information like:

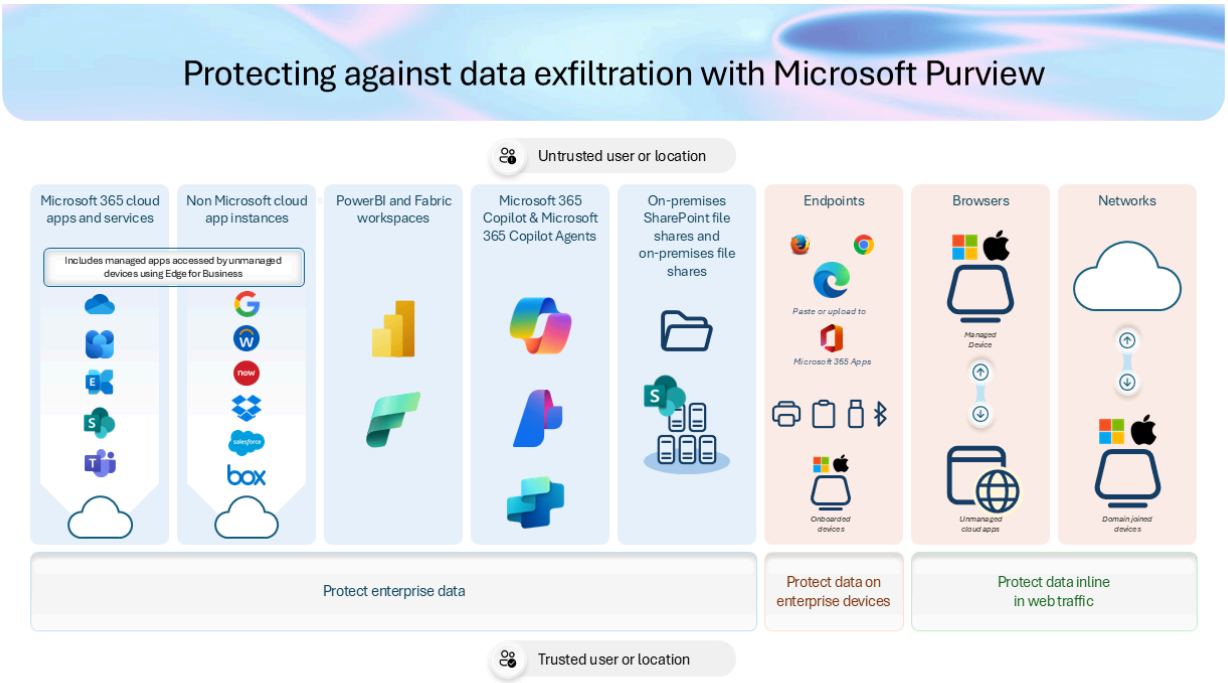
- financial data
- proprietary data
- credit card numbers
- health records
- Social Security numbers

To help protect this sensitive data, and to reduce the risk from oversharing, they need a way to help prevent their users from inappropriately sharing sensitive data with people who shouldn't have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. A DLP policy can help you identify, monitor, and automatically protect sensitive in **Enterprise applications & devices** and **Inline web traffic** data. DLP policies act on a variety of locations, methods of data transmission, and types of user activities.

DLP uses deep content analysis—not a simple text scan. It analyzes content:

- For primary data matches to keywords
- By the evaluation of regular expressions
- By internal function validation
- By secondary data matches that are in proximity to the primary data match
- DLP also uses machine learning algorithms and other methods to detect content that matches your DLP policies
- Inline by Microsoft Edge for business for Windows devices that haven't been onboarded into Microsoft Purview (preview) and Use Network Data Security to help prevent sharing sensitive information with unmanaged AI (preview)



DLP monitors and protects against oversharing in enterprise apps and on devices. It targets Microsoft 365 locations, like Exchange and SharePoint, and locations you add, like on-premises file shares, endpoint devices, and non-Microsoft cloud apps. These locations and sources include:

- Microsoft 365 services, like Exchange, SharePoint, OneDrive accounts, and Teams chat and channel messages
- Office applications, such as Word, Excel, and PowerPoint
- Devices running Windows 10, Windows 11, and the three most recent versions of macOS
- Non-Microsoft cloud apps
- On-premises file shares and on-premises SharePoint
- Microsoft Fabric and Power BI workspaces
- Microsoft 365 Copilot and Copilot chat (preview)
- Managed cloud apps

Create DLP policies for **Enterprise applications & devices** to cover these locations.

DLP, with collection policies, monitors and protects against oversharing to **Unmanaged cloud apps** by targeting data transmitted on your network and in Microsoft Edge for Business. Create policies that target Inline web traffic (preview) and Network activity (preview) to cover locations like:

- OpenAI ChatGPT—for **Edge for Business** and **Network** options
- Google Gemini—for **Edge for Business** and **Network** options
- DeepSeek—for **Edge for Business** and **Network** options
- Microsoft Copilot—for **Edge for Business** and **Network** options
- Over 34,000 cloud apps in the Microsoft Defender for Cloud Apps cloud app catalog—**Network** option only

1. Administrative units
2. Learn about Microsoft Purview Data Loss Prevention
3. Plan for data loss prevention (DLP) - by working through this article you will:
    1. Identify stakeholders
    2. Describe the categories of sensitive information to protect
    3. Set goals and strategy
4. Collection Policies solution overview
5. Collection policy reference
6. Data Loss Prevention policy reference - this article introduces all the components of a DLP policy and how each one influences the behavior of a policy
7. Design a DLP policy - this article walks you through creating a policy intent statement and mapping it to a specific policy configuration.
8. Create and Deploy data loss prevention policies - This article presents some common policy intent scenarios that you map to configuration options, then it walks you through configuring those options.
9. Learn about investigating data loss prevention alerts - This article introduces you to the lifecycle of alerts from creation, through final remediation and policy tuning. It also introduces you to the tools you use to investigate alerts.

For information on licensing, see

- Microsoft 365 Enterprise Plans
- Microsoft 365 Service Descriptions

DLP is just one of the Microsoft Purview tools that you use to help protect your sensitive items wherever they live or travel. You should understand the other tools in the Microsoft Purview tool set, how they interrelate, and work better together. See, Microsoft Purview tools to learn more about the information protection process.

DLP policies monitor the activities that users take on sensitive items and, if the policy conditions are met, take protective actions. For example, when a user attempts a prohibited action, like copying a sensitive item to an unapproved location or sharing medical information in an email, DLP can:

- show a pop-up policy tip to the user that warns them that they might be trying to share a sensitive item inappropriately
- block the sharing and, via a policy tip, allow the user to override the block and capture the users' justification
- block the sharing without the override option
- for data at rest, sensitive items can be locked and moved to a secure quarantine location
- for Teams chat, the sensitive information won't be displayed

All DLP monitored activities are recorded to the Microsoft 365 Audit log by default and routed to Activity explorer.

A DLP implementation typically follows these major phases.

- Plan for DLP

- Prepare for DLP
- Deploy your policies in production

DLP monitoring and protection are native to the applications that users use every day. This helps to protect your organization's sensitive items from risky activities, even if your users are unaccustomed to data loss prevention thinking and practices. If your organization and your users are new to data loss prevention practices, the adoption of DLP might require a change to your business processes, and there will be a culture shift for your users. But, with proper planning, testing and tuning, your DLP policies protect your sensitive items while minimizing any potential business process disruptions.

Keep in mind that DLP as a technology can monitor and protect your data at rest, data in use and data in motion across Microsoft 365 services, Windows 10, Windows 11, and macOS (three latest released versions) devices, on-premises file shares, and on-premises SharePoint. There are planning implications for the different locations, the type of data you want to monitor and protect, and the actions to be taken when a policy match occurs.

DLP policies can block users from performing prohibited activities, like inappropriate sharing of sensitive information via email. As you plan your DLP policies, you must identify the business processes that touch your sensitive items. The business process owners can help you identify appropriate user behaviors that should be allowed and inappropriate user behaviors that should be protected against. You should plan your policies and deploy them in simulation mode, and evaluate their impact, before running them in more restrictive modes.

A successful DLP implementation is as much dependent on getting your users trained and acclimated to data loss prevention practices as it is on well planned and tuned policies. Since your users are heavily involved, be sure to plan for training for them too. You can strategically use policy tips to raise awareness with your users before changing the policy status from simulation mode to more restrictive modes.

You can apply DLP policies to data at rest, data in use, and data in motion in locations such as:

- Exchange Online email
- SharePoint sites
- OneDrive accounts
- Teams chat and channel messages
- Instances: Microsoft Defender for Cloud Apps
- Devices: Windows 10, Windows 11, and macOS (three latest released versions)
- On-premises repositories
- Fabric and Power BI workspaces
- Microsoft 365 Copilot (preview)

Each one has different prerequisites. Sensitive items in some locations, like Exchange online, can be brought under the DLP umbrella by just configuring a policy that applies to them. Others, such as on-premises file repositories, require a deployment of Microsoft Purview Information Protection scanner. You'll need to prepare your environment, code draft policies, and test them thoroughly before activating any blocking actions.

Start by defining your control objectives, and how they apply across each respective workload. Draft a policy that embodies your objectives. Feel free to start with one workload at a time, or across all workloads - there's no

impact yet. For more information, see Create and deploy data loss prevention policies.

Evaluate the impact of the controls by implementing them with a DLP policy in simulation mode. Actions defined in a policy aren't applied while the policy is in simulation mode. It's ok to apply the policy to all workloads in simulation mode, so that you can get the full breadth of results, but you can start with one workload if you need to. For more information, see Policy Deployment.

While in simulation mode, monitor the outcomes of the policy and fine-tune it so that it meets your control objectives while ensuring you aren't adversely or inadvertently impacting valid user workflows and productivity. Here are some examples of things to fine-tune:

- Adjust the locations and people/places that are in or out of scope
- Tune the conditions that are used to determine if an item and what is being done with it matches the policy
- Refine the sensitive information definitions
- Add new controls
- Add new people
- Add new restricted apps
- Add new restricted sites

Note

Stop processing more rules doesn't work in simulation mode, even when it's turned on.

Once the policy meets all your objectives, turn it on. Continue to monitor the outcomes of the policy application and tune as needed.

Note

In general, policies take effect about an hour after being turned on.

You have flexibility in how you create and configure your DLP policies. You can start from a predefined template and create a policy in just a few clicks or you can design your own from the ground up. No matter which you choose, all DLP policies require the same information from you.

1. **Choose what you want to monitor** - DLP comes with many predefined policy templates to help you get started or you can create a custom policy.
    - A predefined policy template, such as Financial data, Medical and health data, Privacy data all for various countries and regions.
    - A custom policy that uses the available sensitive information types (SIT), retention labels, and sensitivity labels.
2. **Choose administrative scoping** - DLP supports assigning Administrative Units to some **Enterprise applications & devices** policies. Administrators who are assigned to an administrative unit can only create and manage policies for the users, groups, distribution groups, accounts, and sites that they're assigned to. So, policies can be applied to all users, groups, and sites by an unrestricted administrator, or they can be

scoped to administrative units. See, Policy Scoping for more DLP specific details. See, Administrative units for the details on administrative units across Microsoft Purview Information Protection.

3. **Choose where you want to monitor** - You pick one or more locations that you want DLP to monitor for sensitive information. You can monitor:

location	include/exclude by
Exchange email	distribution groups
SharePoint sites	sites
OneDrive accounts	accounts or distribution groups
Teams chat and channel messages	account or distribution group
Windows 10, Windows 11, and macOS (three latest released versions) devices	users and groups + devices and device groups
Microsoft Cloud App Security	instance
On-premises repositories	repository file path
Fabric and Power BI	workspaces
Microsoft 365 Copilot (preview)	account or distribution group

Note

The users and groups mentioned above should be Online users and M365, Exchange online, and Microsoft Entra groups

4. **Choose the conditions that must be matched for a policy to be applied to an item** - You can accept preconfigured conditions or you can define custom conditions. Some examples are:
    - item contains a specified type of sensitive information that is being used in a certain context. For example, 95 social security numbers being emailed to recipient outside your org.
    - item has a specified sensitivity label
    - item with sensitive information is shared either internally or externally
5. **Choose the action to take when the policy conditions are met** - The actions depend on the location where the activity is happening. Some examples are:
    - SharePoint/Exchange/OneDrive: Block people who are outside your organization from accessing the content. Show the user a tip and send them an email notification that they're taking an action that is prohibited by the DLP policy.
    - Teams Chat and Channel: Block sensitive information from being shared in the chat or channel.

    - Windows 10, Windows 11, and macOS (three latest released versions) Devices: Audit or restrict copying a sensitive item to a removable USB device.
    - Office Apps: Show a popup notifying the user that they're engaging in a risky behavior and block or block but allow override.
    - On-premises file shares: move the file from where it's stored to a quarantine folder.

  Note

  The conditions and the actions to take are defined in an object called a *rule*.

All DLP policies are created and maintained in the Microsoft Purview portal. See, Create and Deploy data loss prevention policies for more information.

After you create a DLP policy, it's stored in a central policy store, and then synced to the various content sources, including:

- Exchange, and from there to Outlook on the web and Outlook
- OneDrive
- SharePoint sites
- Office desktop programs (Excel, PowerPoint, and Word)
- Microsoft Teams channels and chat messages

After the policy is synced to the right locations, it starts to evaluate content and enforce actions.

DLP reports a vast amount of information to Microsoft Purview from monitoring policy matches and actions, to user activities. You need to consume and act on that information to tune your policies and triage actions taken on sensitive items. The telemetry goes into the Microsoft 365 audit Logs first, is processed, and makes its way to different reporting tools. Each reporting tool has a different purpose.

The DLP **Overview** page gives you quick access to important information about your DLP policies, including:

- **Policy sync status**
- **Device status**
- **Top activites detected**
- **Device overall health**

You can investigate incidents for Microsoft Purview Data Loss Prevention (DLP) from the Microsoft Defender portal **Incidents & alerts** > **Incidents**. See Investigate data loss incidents with Microsoft Defender XDR and Investigate alerts in Microsoft Defender XDR.

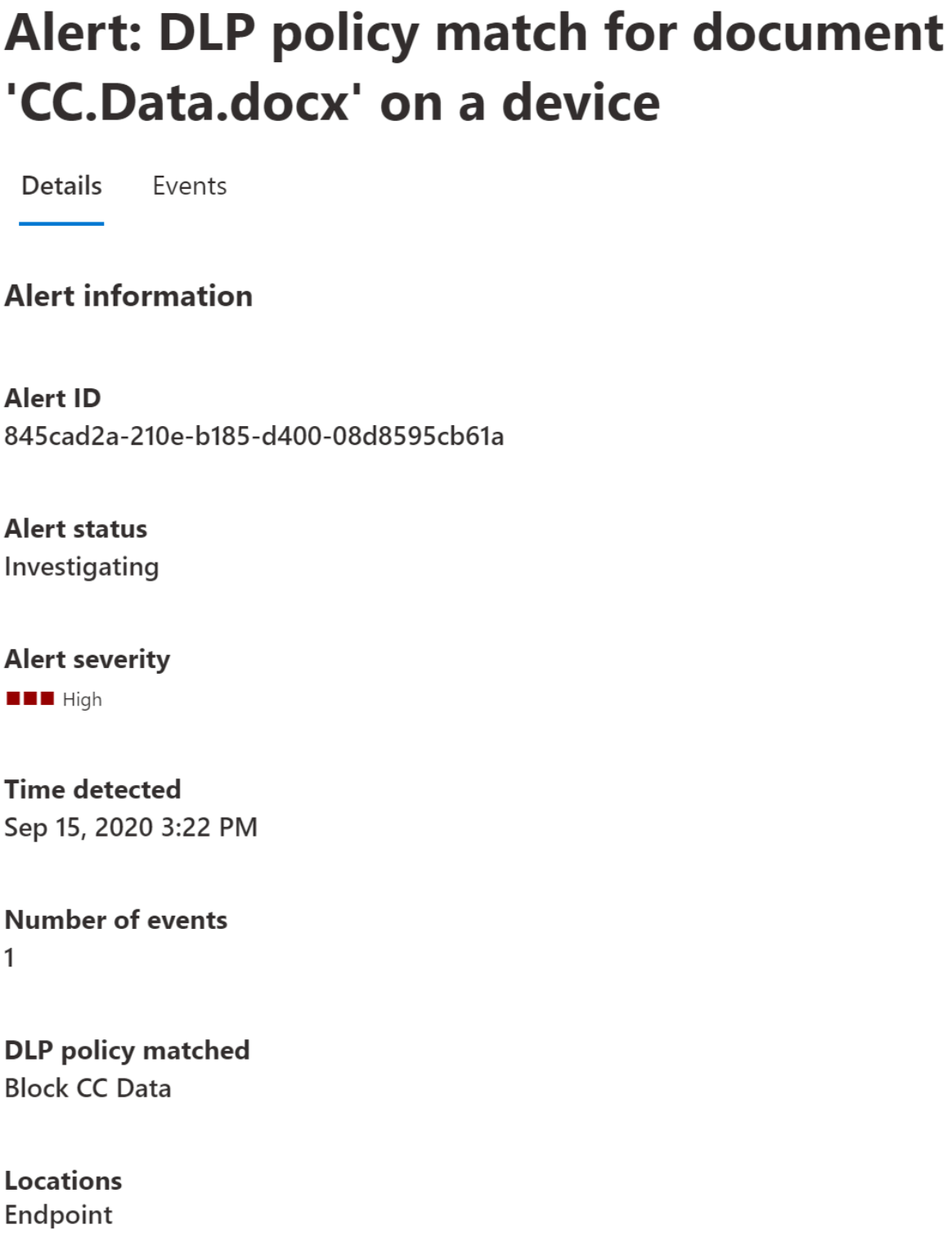
DLP can generate alerts when a user(s) performs an activity that meets the criteria of a rule in a DLP policy, and you have incident reports configured to generate alerts. Depending on your subscription level, alerts can be aggregated on a time window/rule basis or on a time windows/user basis(preview).

DLP posts the alert for investigation in the DLP Alerts dashboard. Use the DLP Alerts dashboard to view alerts, triage them, set investigation status, and track resolution. Alerts are also routed to Microsoft Defender portal where you can do all the alert dashboard tasks plus more.

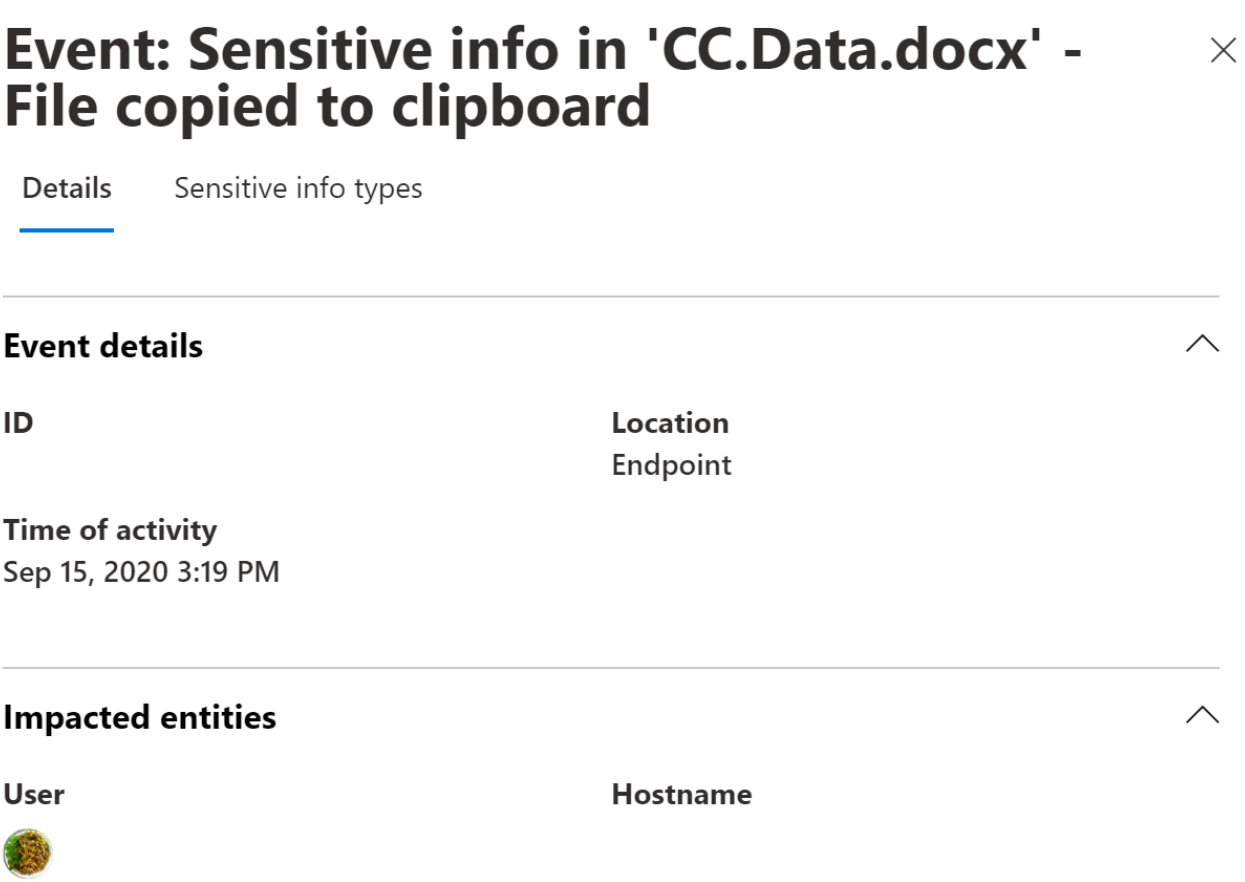
DLP alerts are available in the Microsoft Defender portal for six months. They're only available in the Microsoft Purview DLP alerts dashboard for 30 days.

If you're an administrative unit restricted admin, you'll only see the DLP alerts for your administrative unit.

Here's an example of alerts generated by policy matches and activities from Windows 10 devices.



You can also view details of the associated event with rich metadata in the same dashboard.



Note

Alerts are generated differently for emails than they are for SharePoint or OneDrive items. In SharePoint and OneDrive, DLP scans existing items as well as new ones and generates an alert whenever a match is found. In Exchange, new email messages are scanned and an alert is generated if there's a policy match. DLP ***does not*** scan or match previously existing email items that are stored in a mailbox or archive.

For more information on Alerts, see:

- Alerts in DLP policies: Describes alerts in the context of a DLP policy.
- Get started with data loss prevention alerts: Covers the necessary liscensing, permissions, and prerequisites for DLP alerts and alert reference details.
- Create and deploy data loss prevention policies: Includes guidance on alert configuration in the context of creating a DLP policy.
- Learn about investigating data loss prevention alerts: Covers the various methods for investigating of DLP alerts.
- Investigate data loss incidents with Microsoft Defender XDR: How to investigate DLP alerts in Microsoft Defender portal.

The Activity explorer tab on the DLP page has multiple filters you can use to view DLP events. Use this tool to review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and matched a rule.

You can view the last 30 days of DLP information in Activity Explorer using these preconfigured filters:

- Endpoint DLP activities
- Files containing sensitive info types
- Egress activities
- DLP policies that detected activities
- DLP policy rules that detected activities

To see this information	Select this activity
User overrides	**DLP rule undo**
Items that match a DLP rule	**DLP rule matched**

You can also access DLP report using via these cmdlets in the Security & Compliance PowerShell.

1. Connect to Security & Compliance PowerShell

Use these cmdlets:

- Get-DlpDetailReport
- Get-DlpDetectionsReport
- Get-DlpSiDetectionsReport

However, DLP reports need to pull data from across Microsoft 365, including Exchange. For this reason, the following cmdlets for DLP reports are available in Exchange PowerShell. To use the cmdlets for these DLP reports, take the following steps:

1. Connect to Exchange PowerShell

Use these cmdlets:

- Get-DlpDetailReport

- Get-MailDetailDlpPolicyReport

You can see the text that surrounds the matched content, like a credit card number in a **DLPRuleMatch** event in Activity explorer.

DLPRuleMatch events are paired with user egress activities such as "CopyToClipboard" or "CloudEgress". They should be right next to (or at least very close to) each other in Activity explorer. You want to look at both because the **user activity** contains details about the matched policy and the **DLPRuleMatch** event contains the details about the text that surrounds the matched content.

For endpoint, be sure that you have applied KB5016688 for Windows 10 devices and KB5016691 for Windows 11 devices or above.

For more information, see Get started with activity explorer.

To learn more about Microsoft Purview DLP, see:

- Learn about Endpoint data loss prevention
- Learn about the default data loss prevention policy in Microsoft Teams (preview)
- Learn about data loss prevention on-premises scanner
- Learn about the Microsoft Compliance Extension
- Get started with the data loss prevention Alerts dashboard

To learn how to use data loss prevention to comply with data privacy regulations, see Deploy information protection for data privacy regulations with Microsoft Purview (aka.ms/m365dataprivacy).
