Configuration Manual

MSc Research Project
MSc in Cybersecurity

Dharani Muruga Prasad
Student ID: 22208593

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Dharani Muruga Prasad		
Student ID:	22208593		
Programme:	MSc in Cybersecurity	**Year:**	2023-2024
Module:	Practicum		
Lecturer:	Prof. Vikas Sahni		
Submission Due Date:	12/08/2024		
Project Title:	Implementing a Next Gen CASB for Data Loss Prevention		
Word Count:	1434	**Page Count:**	13

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Dharani Muruga Prasad

Date: 11/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Dharani Muruga Prasad
22208593

1 Prerequisites

The following licenses are the minimum requirements to implement DLP in Microsoft Defender for Cloud Apps by integrating Purview and Defender. Trial versions of the below were used for the project.

- Microsoft 365 E5 Compliance
- Microsoft Defender for Office 365 (Plan 2)
- Office 365 E5 (no Teams)
- Exchange Online Protection

2 Configure and connect portals

1. Create a domain and email address to be used in all the portals.
2. Be a Global Administrator or a Security Administrator to setup Defender for Cloud Apps.
3. Login to the Microsoft Defender Portal[1] and access the Cloud Apps section.

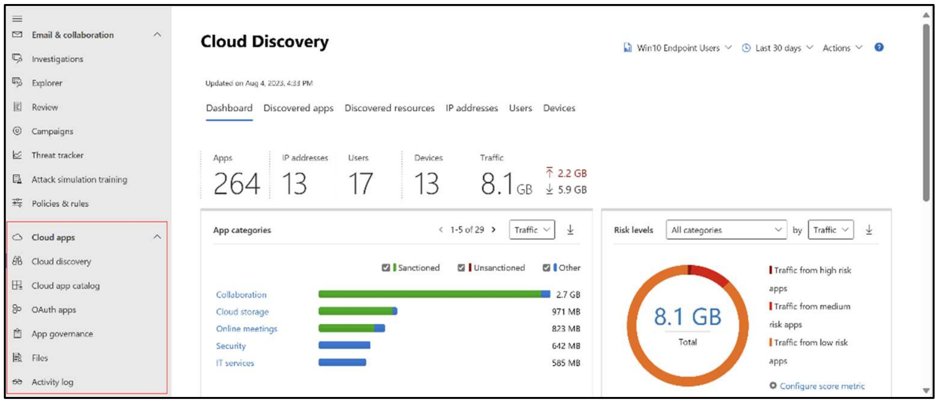


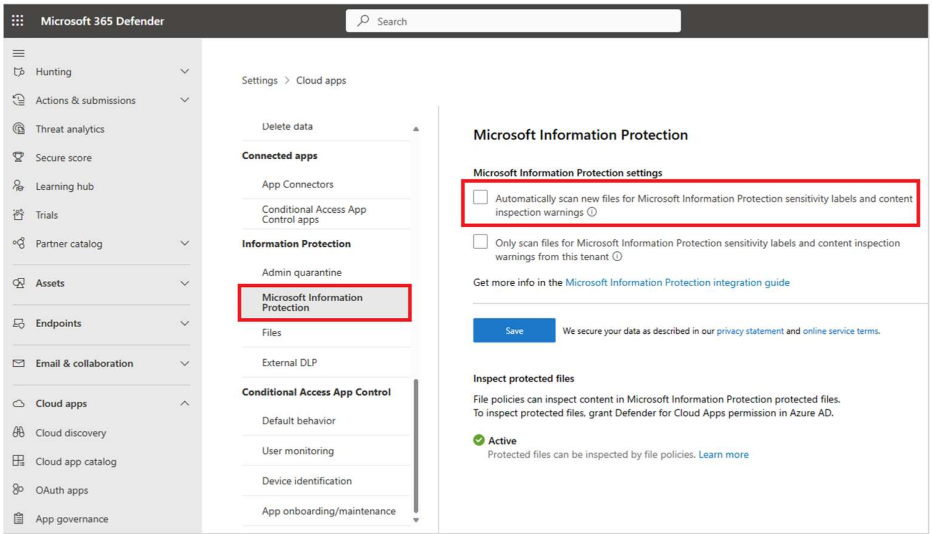
Figure 1: Defender for Cloud Apps (Batami Gold et al., 2024)

2.1 Microsoft Information Protection

1. In the Microsoft Defender Portal, select Settings, choose Cloud Apps, go to Information Protection-> Microsoft Information Protection.

[1] https://security.microsoft.com/

2. Select 'Automatically scan new files for sensitivity labels from Microsoft Purview Information Protection and content inspection warnings', under Information Protection settings.
3. Click on Files, choose 'Enable file monitoring'.(Batami Gold, Jeff Borsecnik, et al., 2023)



Microsoft Information Protection

Microsoft Information Protection settings

□ Automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings ⓘ

□ Only scan files for Microsoft Information Protection sensitivity labels and content inspection warnings from this tenant ⓘ

Get more info in the Microsoft Information Protection integration guide

We secure your data as described in our privacy statement and online service terms.

Inspect protected files

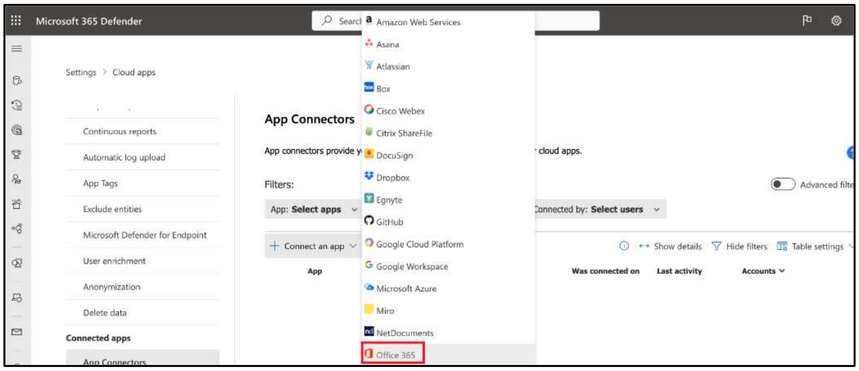
File policies can inspect content in Microsoft Information Protection protected files.
To inspect protected files, grant Defender for Cloud Apps permission in Azure AD.

✓ Active
Protected files can be inspected by file policies. Learn more

Figure 2: Microsoft Information Protection

2.2 Microsoft 365

1. To monitor Microsoft 365 activities in Defender for Cloud Apps. Auditing should be enabled in Microsoft Purview.
2. To connect to Microsoft 365, in the Microsoft Defender Portal select Settings. Then choose Cloud Apps. Under Connected apps, select App Connectors.



App Connectors

App connectors provide y cloud apps.

Filters:

App: Select apps

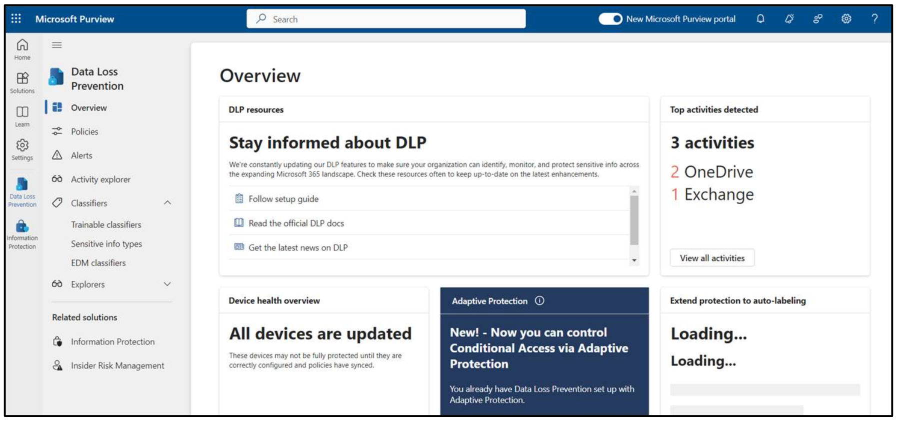
Connected by: Select users

Figure 3: Microsoft Defender

3. On the App connectors page, click on +Connect an app, and then select Microsoft 365 from the drop down.
4. Select the required options on the Microsoft 365 components page and click on 'Connect'.
5. Select 'Connect Microsoft 365', on the 'Follow the Link' page.
6. After Microsoft 365 is displayed as successfully connected, select Done.(Batami Gold, Alex Buck, et al., 2023)

2.3 Microsoft Purview

1. Login to the Purview[2] portal, access ‘Data Loss Prevention’ from Solutions.



Overview

Stay informed about DLP

We're constantly updating our DLP features to make sure your organization can identify, monitor, and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

- Follow setup guide
- Read the official DLP docs
- Get the latest news on DLP

3 activities

2 OneDrive

1 Exchange

All devices are updated

These devices may not be fully protected until they are correctly configured and policies have synced.

New! - Now you can control Conditional Access via Adaptive Protection

You already have Data Loss Prevention set up with Adaptive Protection.

Loading...

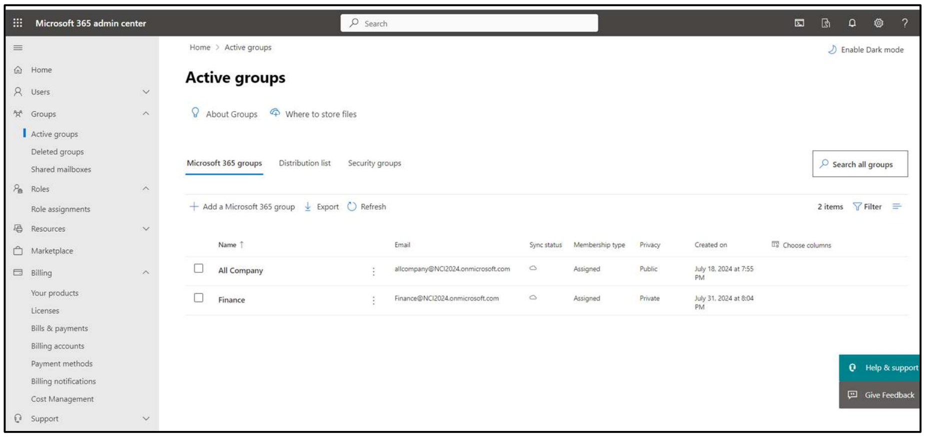
Loading...

Figure 4: Data Loss Prevention

2. Check if there are necessary permissions to create policies

3 Configure environment

1. All information related to licenses assigned to different users, permissions, users and groups, role assignments can be found in the Microsoft 365 admin center[3] portal.
2. Links to other admin center pages can also be found on this page.
3. Users and Groups are created, permissions and licenses are assigned by Least Privilege.



Active groups

	Name ↑	Email	Sync status	Membership type	Privacy	Created on
□	All Company	allcompany@NCI2024.onmicrosoft.com		Assigned	Public	July 18, 2024 at 7:55 PM
□	Finance	Finance@NCI2024.onmicrosoft.com		Assigned	Private	July 31, 2024 at 8:04 PM

Figure 5: Microsoft 365 Admin Centre

4. Distribution lists and shared mailboxes are configured.

4 DLP Planning

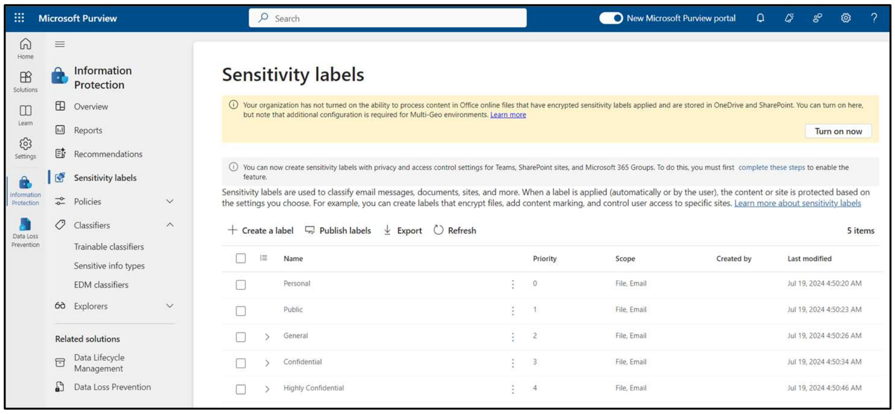
1. Navigate to ‘Information Protection’ on the Purview[4] portal.

[2] https://compliance.microsoft.com/

[3] https://admin.microsoft.com/

[4] https://compliance.microsoft.com/

2. Activate default sensitivity labels (Personal, Public, General, Confidential, Highly Confidential) or create custom labels according to requirements of the organization.



Sensitivity labels

Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but note that additional configuration is required for Multi-Geo environments. Learn more

Turn on now

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

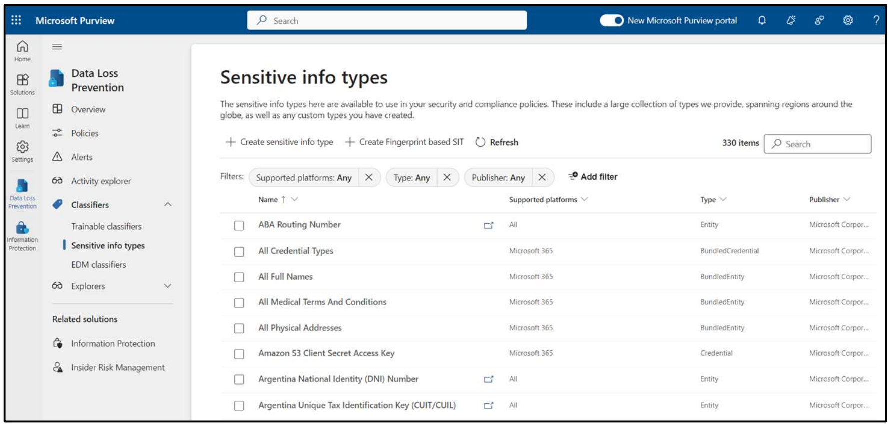
Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

+ Create a label   Publish labels   Export   Refresh   5 items

Name	Priority	Scope	Created by	Last modified
Personal	0	File, Email		Jul 19, 2024 4:50:20 AM
Public	1	File, Email		Jul 19, 2024 4:50:23 AM
General	2	File, Email		Jul 19, 2024 4:50:26 AM
Confidential	3	File, Email		Jul 19, 2024 4:50:34 AM
Highly Confidential	4	File, Email		Jul 19, 2024 4:50:46 AM

Figure 6: Sensitivity Labels

3. Enable sensitivity labels for SharePoint and OneDrive. This step is a prerequisite to use sensitivity labels in Office for the web, and auto-labelling policies for SharePoint and OneDrive
4. Built in Sensitive Information Types (SIT) like PPSN, Driving License for different countries, etc. can be used or if the pre-configured types do not suit the organization's needs, custom SITs can be created.



Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

+ Create sensitive info type   + Create Fingerprint based SIT   Refresh   330 items   Search

Filters: Supported platforms: Any   Type: Any   Publisher: Any   Add filter

Name ↑	Supported platforms	Type	Publisher
ABA Routing Number	All	Entity	Microsoft Corpor...
All Credential Types	Microsoft 365	BundledCredential	Microsoft Corpor...
All Full Names	Microsoft 365	BundledEntity	Microsoft Corpor...
All Medical Terms And Conditions	Microsoft 365	BundledEntity	Microsoft Corpor...
All Physical Addresses	Microsoft 365	BundledEntity	Microsoft Corpor...
Amazon S3 Client Secret Access Key	Microsoft 365	Credential	Microsoft Corpor...
Argentina National Identity (DNI) Number	All	Entity	Microsoft Corpor...
Argentina Unique Tax Identification Key (CUIT/CUIL)	All	Entity	Microsoft Corpor...

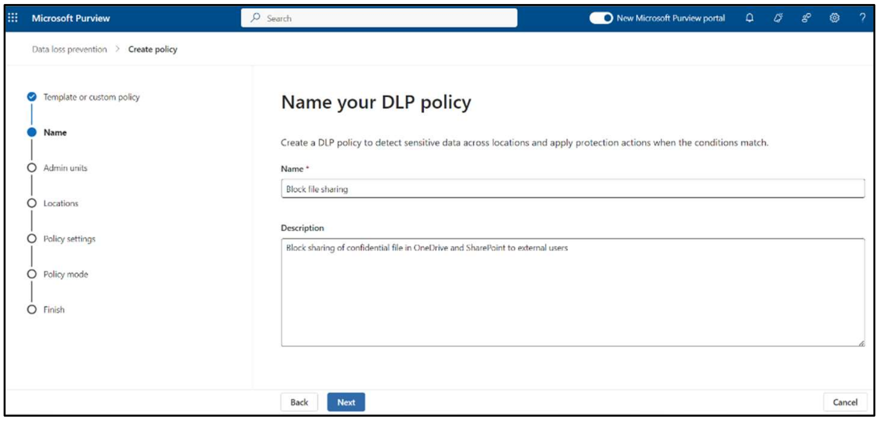
Figure 7: Sensitive Information Types

5 Policy Configuration

Test case – Policy to block sharing of sensitive data with external users via OneDrive and SharePoint.

Requirements – Sharing of files containing confidential data like credit card data, personal data, etc. in OneDrive and SharePoint to all external recipients needs to be blocked. Every time a file is shared, an email notification must be sent to the security team and then blocked. The user should be alerted within the interface.

1. In the Purview portal, select **Data loss prevention**, then **Policies**, next **+Create policy**.



Name your DLP policy

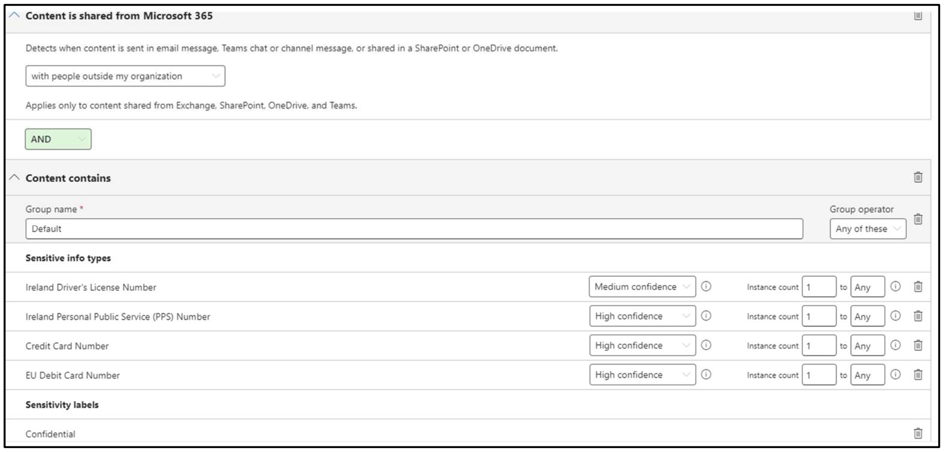
Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *
Block file sharing

Description
Block sharing of confidential file in OneDrive and SharePoint to external users

Figure 8: Create DLP policy

2. From both the **Categories** list and the **Regulations** list, Select **Custom**, click on **Next.**
3. Enter a Name and Description for the policy.
4. On the **Assign admin units** page, let the default set to **Full Directory.**
5. Choose the location where the policy should be applied to.
    - Select OneDrive accounts and SharePoint sites and deselect all other locations.
6. Click on **Done** and **Next**
7. **Create or customize advanced DLP rules** is already selected on the **Define policy settings** page, choose **Next**.
8. Select **+ Create rule** on the **Customize advanced DLP rules** page.
9. Use the following values in the **Add condition** option
    - Choose **Content is shared from Microsoft 365**.
    - Select **with people outside my organization**.
10. Create a second condition, select **Content contains**
11. **Add** > **Sensitivity labels** > and then **Confidential**.



Content is shared from Microsoft 365

Detects when content is sent in email message, Teams chat or channel message, or shared in a SharePoint or OneDrive document.

with people outside my organization

Applies only to content shared from Exchange, SharePoint, OneDrive, and Teams.

Content contains

Group name *
Default

Group operator
Any of these

Sensitive info types

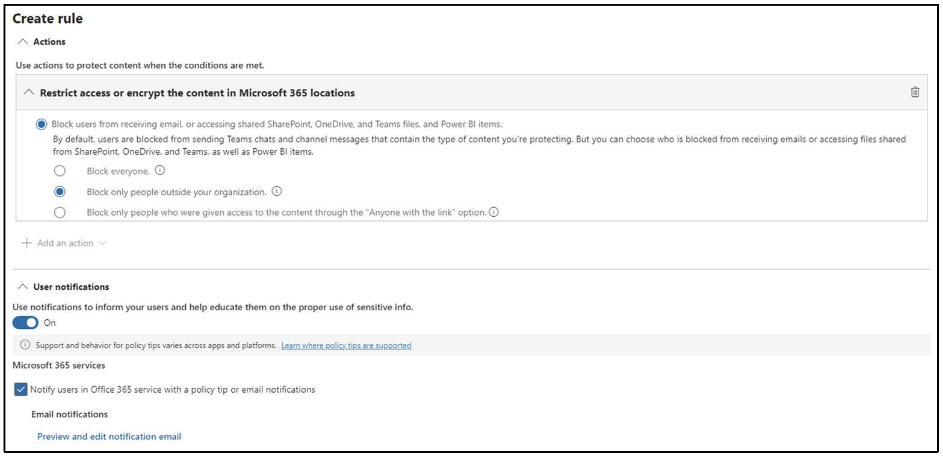
Ireland Driver's License Number	Medium confidence	Instance count 1	to Any
Ireland Personal Public Service (PPS) Number	High confidence	Instance count 1	to Any
Credit Card Number	High confidence	Instance count 1	to Any
EU Debit Card Number	High confidence	Instance count 1	to Any

Sensitivity labels

Confidential

Figure 9: Advanced DLP rules

12. Use the below values in **Actions**
    - **Restrict access or encrypt the content in Microsoft 365 locations**.
    - **Block only people outside your organization**.



Create rule

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

● Block users from receiving email, or accessing shared SharePoint, OneDrive, and Teams files, and Power BI items.
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams, as well as Power BI items.

○ Block everyone.

● Block only people outside your organization.

○ Block only people who were given access to the content through the "Anyone with the link" option.

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported

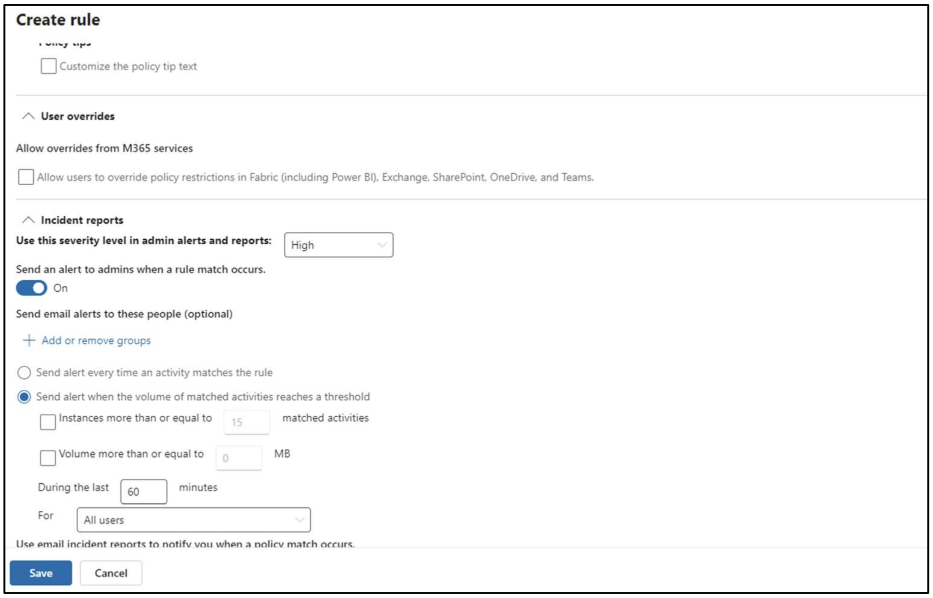
Microsoft 365 services

☑ Notify users in Office 365 service with a policy tip or email notifications

Email notifications

Figure 10: Actions

13. Toggle **User Notifications** on.
14. Choose **Notify users in Office 365 services with a policy tip** and then select **Notify the user who sent, shared, or last modified the content**.
15. Make sure **Allow override from M365 services** is not selected under **User overrides.**



Create rule

Policy tips

□ Customize the policy tip text

User overrides

Allow overrides from M365 services

□ Allow users to override policy restrictions in Fabric (including Power BI), Exchange, SharePoint, OneDrive, and Teams.

Incident reports

Use this severity level in admin alerts and reports: High

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

○ Send alert every time an activity matches the rule

● Send alert when the volume of matched activities reaches a threshold

□ Instances more than or equal to 15 matched activities

□ Volume more than or equal to 0 MB

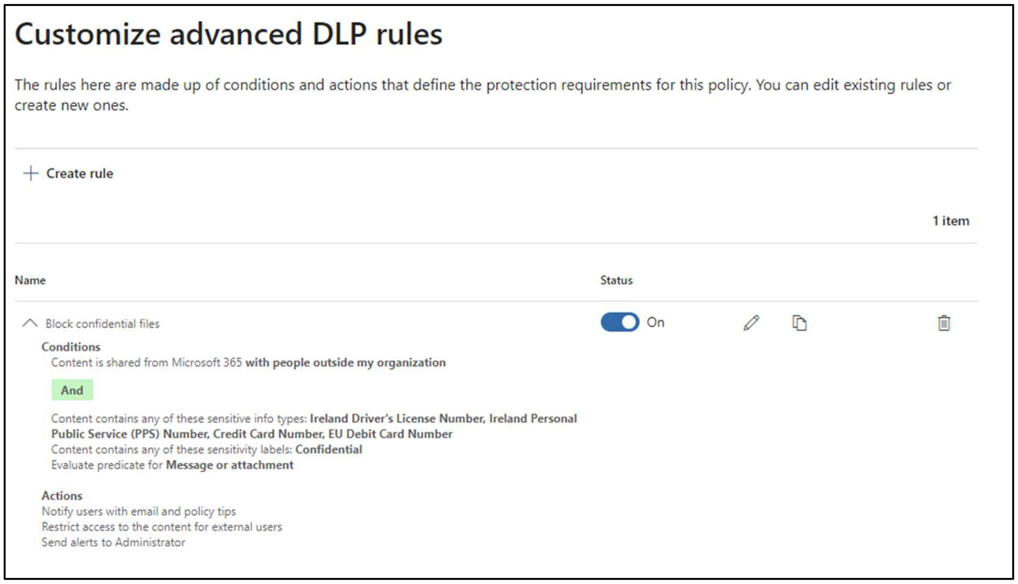
During the last 60 minutes

For All users

Use email incident reports to notify you when a policy match occurs.

Figure 11: Send alert

16. In **Incident reports**:
    - Set **Use this severity level in admin alerts and reports** to **High**.
    - Toggle **Send an alert to admins when a rule match occurs** to **On**
17. Select **Save** and **Next.**



Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

Block confidential files — On

Conditions
Content is shared from Microsoft 365 **with people outside my organization**

And

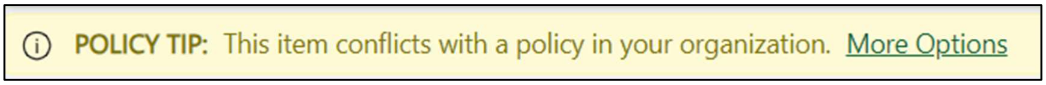
Content contains any of these sensitive info types: **Ireland Driver's License Number, Ireland Personal Public Service (PPS) Number, Credit Card Number, EU Debit Card Number**
Content contains any of these sensitivity labels: **Confidential**
Evaluate predicate for **Message or attachment**

Actions
Notify users with email and policy tips
Restrict access to the content for external users
Send alerts to Administrator

Figure 12: Rule page

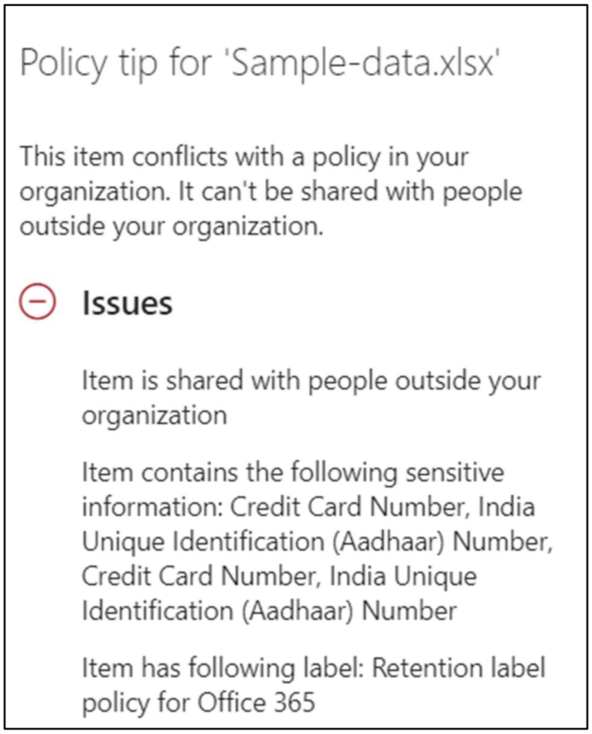
18. Choose the required **Policy mode, Next** and **Done.** (Chris Fox MSFT, Katy Koenen and Robert Mazzoli, 2024)

6 Alerts



POLICY TIP: This item conflicts with a policy in your organization. More Options

Figure 13: Policy tip



Policy tip for 'Sample-data.xlsx'

This item conflicts with a policy in your organization. It can't be shared with people outside your organization.

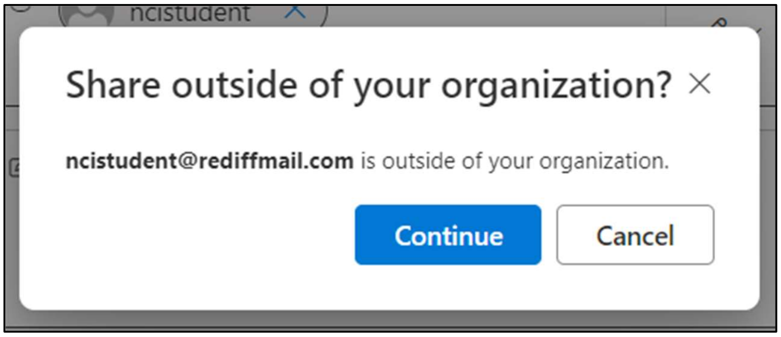
Issues

Item is shared with people outside your organization

Item contains the following sensitive information: Credit Card Number, India Unique Identification (Aadhaar) Number, Credit Card Number, India Unique Identification (Aadhaar) Number

Item has following label: Retention label policy for Office 365

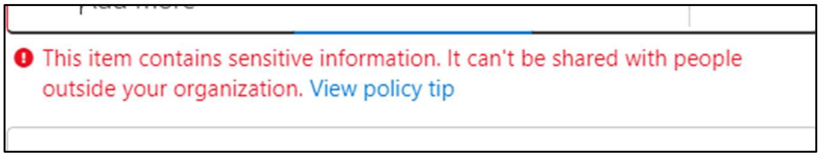
Figure 14: More Options for policy tip



Share outside of your organization?

ncistudent@rediffmail.com is outside of your organization.

Figure 15: Popup

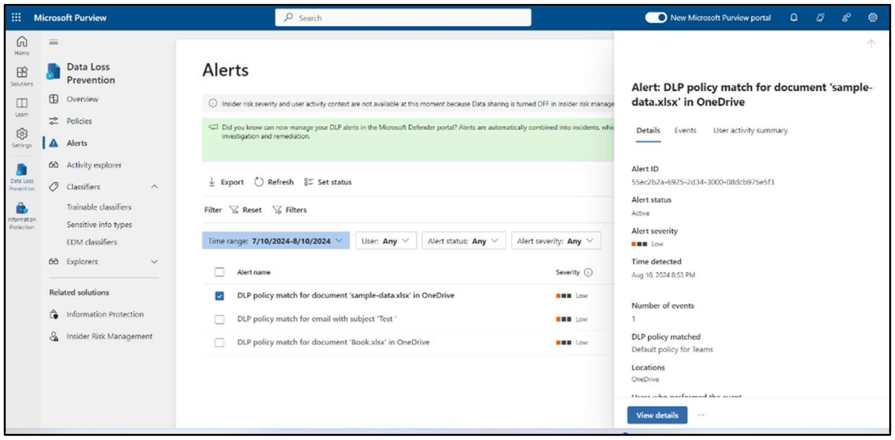


This item contains sensitive information. It can't be shared with people outside your organization. View policy tip

Figure 16: Alert when trying to share

7 Alert Dashboard/Notification

1. Alerts can be viewed in the Purview Dashboard



Alerts

Insider risk severity and user activity context are not available at this moment because Data sharing is turned OFF in Insider risk manage

Did you know can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically combined into incidents, whic investigation and remediation.

Time range: **7/10/2024-8/10/2024** User: **Any** Alert status: **Any** Alert severity: **Any**

	Alert name	Severity
☑	DLP policy match for document 'sample-data.xlsx' in OneDrive	Low
□	DLP policy match for email with subject 'Test '	Low
□	DLP policy match for document 'Book.xlsx' in OneDrive	Low

Alert: DLP policy match for document 'sample-data.xlsx' in OneDrive

Details | Events | User activity summary

Alert ID
55ec2b2a-6925-2d34-3000-08dcb975e5f3

Alert status
Active

Alert severity
Low

Time detected
Aug 10, 2024 8:53 PM

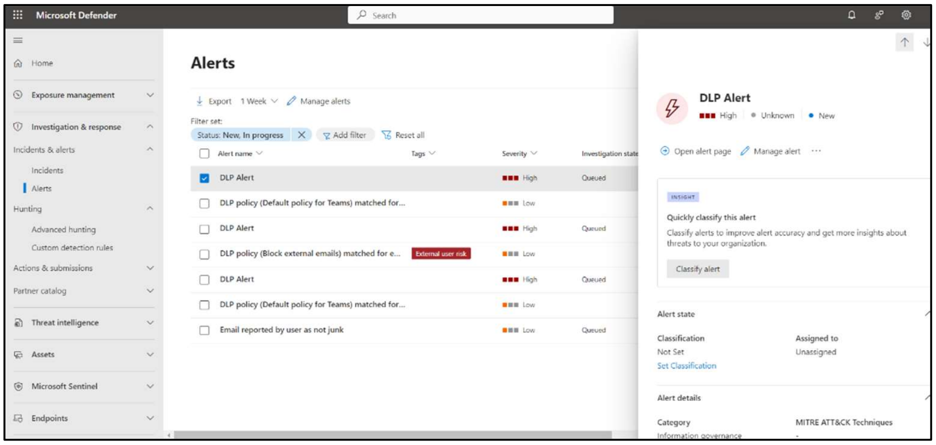
Number of events
1

DLP policy matched
Default policy for Teams

Locations
OneDrive

Figure 17: Purview Alert Dashboard

2. Since Defender is connected, alerts can also be viewed there



Alerts

Filter set: Status: New, In progress

	Alert name	Tags	Severity	Investigation state
☑	DLP Alert		High	Queued
□	DLP policy (Default policy for Teams) matched for...		Low	
□	DLP Alert		High	Queued
□	DLP policy (Block external emails) matched for e...	External user risk	Low	
□	DLP Alert		High	Queued
□	DLP policy (Default policy for Teams) matched for...		Low	
□	Email reported by user as not junk		Low	Queued

DLP Alert

High | Unknown | New

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Alert state

Classification: Not Set

Assigned to: Unassigned

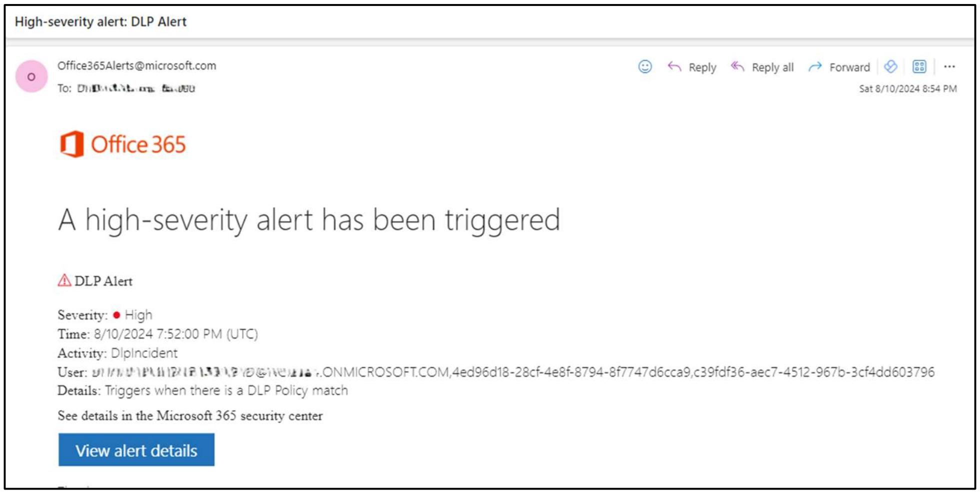
Alert details

Category: Information governance

MITRE ATT&CK Techniques: -

Figure 18: Defender Alert Dashboard

3. Email notification is also received if an alert is triggered.



High-severity alert: DLP Alert

Office365Alerts@microsoft.com
To: [redacted]
Sat 8/10/2024 8:54 PM

A high-severity alert has been triggered

⚠ DLP Alert

Severity: ● High
Time: 8/10/2024 7:52:00 PM (UTC)
Activity: DlpIncident
User: [redacted].ONMICROSOFT.COM,4ed96d18-28cf-4e8f-8794-8f7747d6cca9,c39fdf36-aec7-4512-967b-3cf4dd603796
Details: Triggers when there is a DLP Policy match

See details in the Microsoft 365 security center

Figure 19: Email notification

8 Advanced Threat Hunting

KQL queries can be used to view raw data and proactively detect threats. It also provides more details about the activity.

Test case – Identify if a document was accessed by a user on OneDrive/SharePoint
The time range specified in advanced hunting will determine the information that is returned by this query from OneDrive for Business and SharePoint Online. Verify with whom certain files have been shared for SharePoint and OneDrive DLP alerts, and it provides external access and file sharing history.

1. In the Defender portal, select **Advanced Hunting,** under **Hunting.**

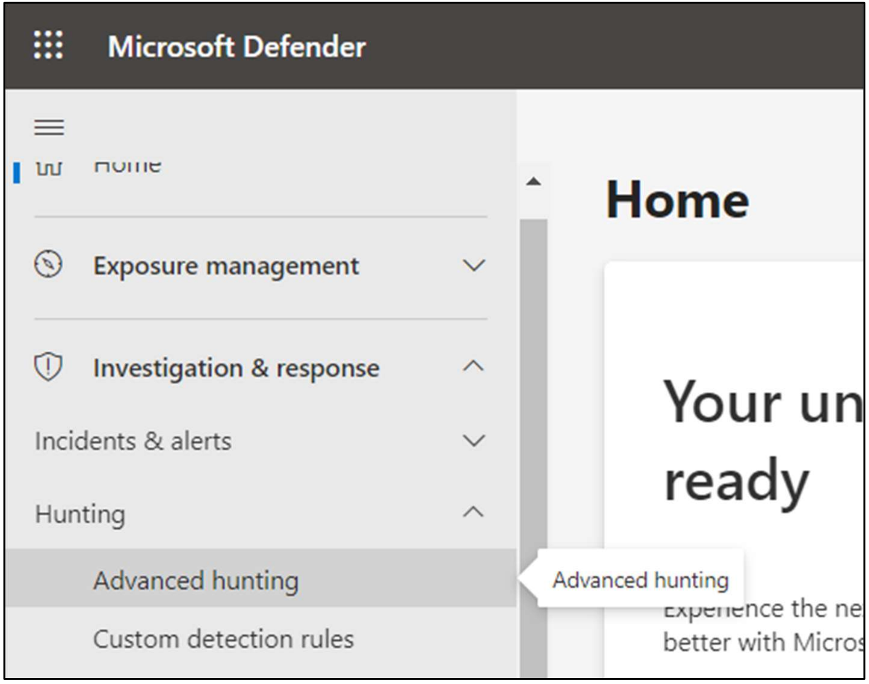
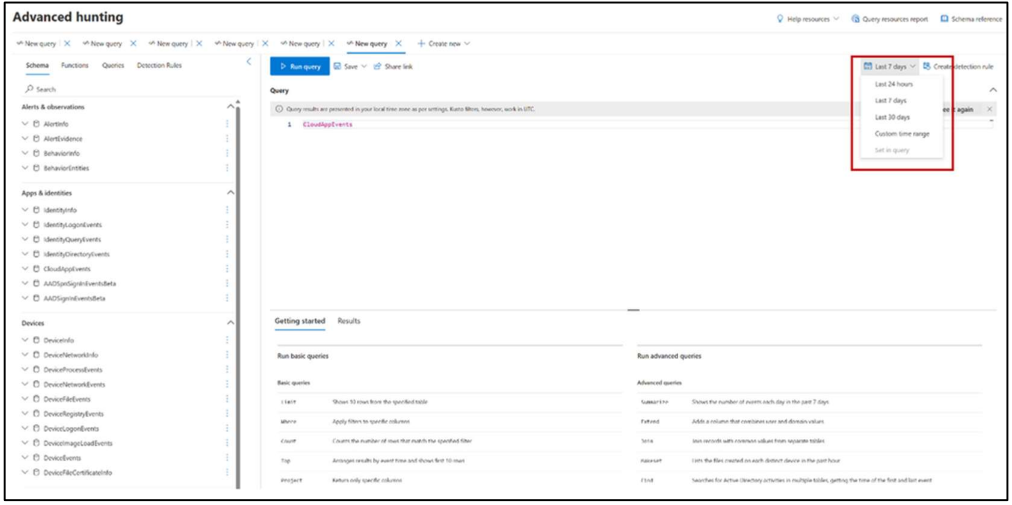


Figure 20: Advanced Hunting

2. Select time range for query

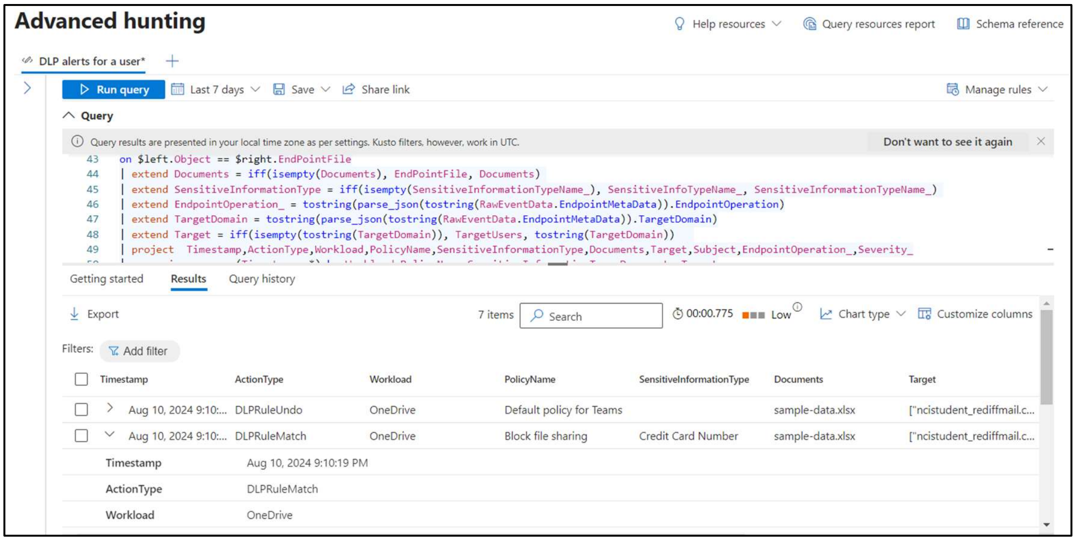


Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
CloudAppEvents
```

Figure 21: Query editor

3. There are tables available on the left side to query data.
4. Queries in advanced hunting are based on Kusto Query Language(KQL)
5. Run the query once inserted, to see the results.



Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
on $left.Object == $right.EndPointFile
| extend Documents = iff(isempty(Documents), EndPointFile, Documents)
| extend SensitiveInformationType = iff(isempty(SensitiveInformationTypeName_), SensitiveInfoTypeName_, SensitiveInformationTypeName_)
| extend EndpointOperation_ = tostring(parse_json(tostring(RawEventData.EndpointMetaData)).EndpointOperation)
| extend TargetDomain = tostring(parse_json(tostring(RawEventData.EndpointMetaData)).TargetDomain)
| extend Target = iff(isempty(tostring(TargetDomain)), TargetUsers, tostring(TargetDomain))
| project  Timestamp,ActionType,Workload,PolicyName,SensitiveInformationType,Documents,Target,Subject,EndpointOperation_,Severity_
```

Timestamp	ActionType	Workload	PolicyName	SensitiveInformationType	Documents	Target
Aug 10, 2024 9:10:...	DLPRuleUndo	OneDrive	Default policy for Teams		sample-data.xlsx	["ncistudent_rediffmail.c...
Aug 10, 2024 9:10:...	DLPRuleMatch	OneDrive	Block file sharing	Credit Card Number	sample-data.xlsx	["ncistudent_rediffmail.c...

Timestamp	Aug 10, 2024 9:10:19 PM
ActionType	DLPRuleMatch
Workload	OneDrive

Figure 22: Results

References

Batami Gold, Alex Buck, et al. (2023) How Defender for Cloud Apps helps protect your Microsoft 365 environment, Microsoft Learn. Available at: https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365 (Accessed: 10 August 2024).

Batami Gold, Jeff Borsecnik, et al. (2023) Integrate Microsoft Purview Information Protection, Microsoft Learn. Available at: https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration (Accessed: 10 August 2024).

Batami Gold et al. (2024) Get started with Microsoft Defender for Cloud Apps, Microsoft Learn. Available at: https://learn.microsoft.com/en-us/defender-cloud-apps/get-started (Accessed: 9 August 2024).

Chris Fox MSFT, Katy Koenen and Robert Mazzoli (2024) Create and Deploy data loss prevention policies.