



BLACK CELL
Protecting critical infrastructures

Compliance in Microsoft Purview Whitepaper



Table of Contents

1. Introduction	3
1.1. Information protection.....	3
1.2. Data life cycle management	3
1.3. Data loss prevention	4
2. Configuring a custom DLP policy	5
2.1. First steps.....	5
2.2. Choose the information to protect.....	6
2.3. Name your policy.....	7
2.4. Location to apply the policy	7
2.5. Policy settings	8
2.6. Advanced DLP rules.....	8
2.6.1. Conditions	8
2.6.2. Actions.....	9
2.6.3. User notifications.....	10
2.6.4. User overrides	10
2.6.5. Incident reports.....	11
2.7. Test or turn on the policy.....	11
2.8. After the test.....	12
3. Executive summary	12
4. References	12

1. Introduction

Microsoft Purview is a comprehensive set of data management solutions to govern, protect, and manage an organization's entire data estate. Among its many features the document introduces three with special focus on data loss prevention.

1.1. Information protection

Information protection is the process of safeguarding information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information protection is important to preserve confidentiality, integrity, and availability. To achieve these goals, information protection employs security solutions like encryption and other technologies, as well as policies and processes.

Microsoft Purview Information Protection (formerly Microsoft Information Protection) provides the tools you need to discover, classify, and protect sensitive information by using labels and label policies. In essence you create a label and you set your conditions and restrictions on that label after assigning that label to a label policy, a group of users or group of devices.

1.2. Data life cycle management

Data management is a critical part of any software platform. Data is generated from many sources, such as business processes, network operations centres, mobile devices, social media sites, and other data-sharing environments. This data must be managed effectively to keep the customer safe and meet internal compliance requirements. Data lifecycle management (DLM) is a best practice approach that covers all stages of the data life cycle, from production to data destruction, data management, data protection, and data governance. By following DLM principles, businesses can establish that the correct data is at the place where it is supposed to be, enabling them to capitalize on data insights and create new opportunities. A more holistic view of data usage could then be gained by applying data science techniques through the various phases of the client's journey, allowing them to detect breaches or other potential misuse.



In Microsoft Purview Data lifecycle management, there are important tools like retention polices. The difference between backup and retention is that backup is used for operational and disaster recovery purposes, whereas retention is for compliance and legal reasons.

1.3. Data loss prevention:

Data is the key for information-based organizations nowadays. Have you ever wondered what would happen to your business if your data leaked? Your business could be destroyed. Amidst data breaches, cyberattacks, corporate espionage and data privacy regulations, data loss prevention (DLP) technologies have become an essential component of today's business.

DLP is a set of products, strategies, technologies, and techniques to prevent unauthorized access to sensitive data. The main causes of data loss are accidental deletion, data migration, accidental overwrite, external hackers or malware, and malicious network insiders.

Recently, the adoption of cloud-based SaaS applications, such as Microsoft 365 has increased. That's why continuously more data is being stored in the cloud. However, the cloud is not immune to data loss, therefore we need the best settings to keeping our data safe.

Organizations have sensitive files to handle. For instance, proprietary data, credit card numbers, health records, financial data, or social security numbers. How Microsoft deals with this obstacle? Microsoft Purview Data loss prevention is capable of preventing users from accidentally or intentionally sharing sensitive content, identify sensitive information (Exchange Online, SharePoint Online, OneDrive, Microsoft Teams, Windows devices), and monitor and protect confidential files (Excel, PowerPoint, Word and Outlook). Microsoft Purview has features like DLP alerts and reports which can be customized according to your company policies.

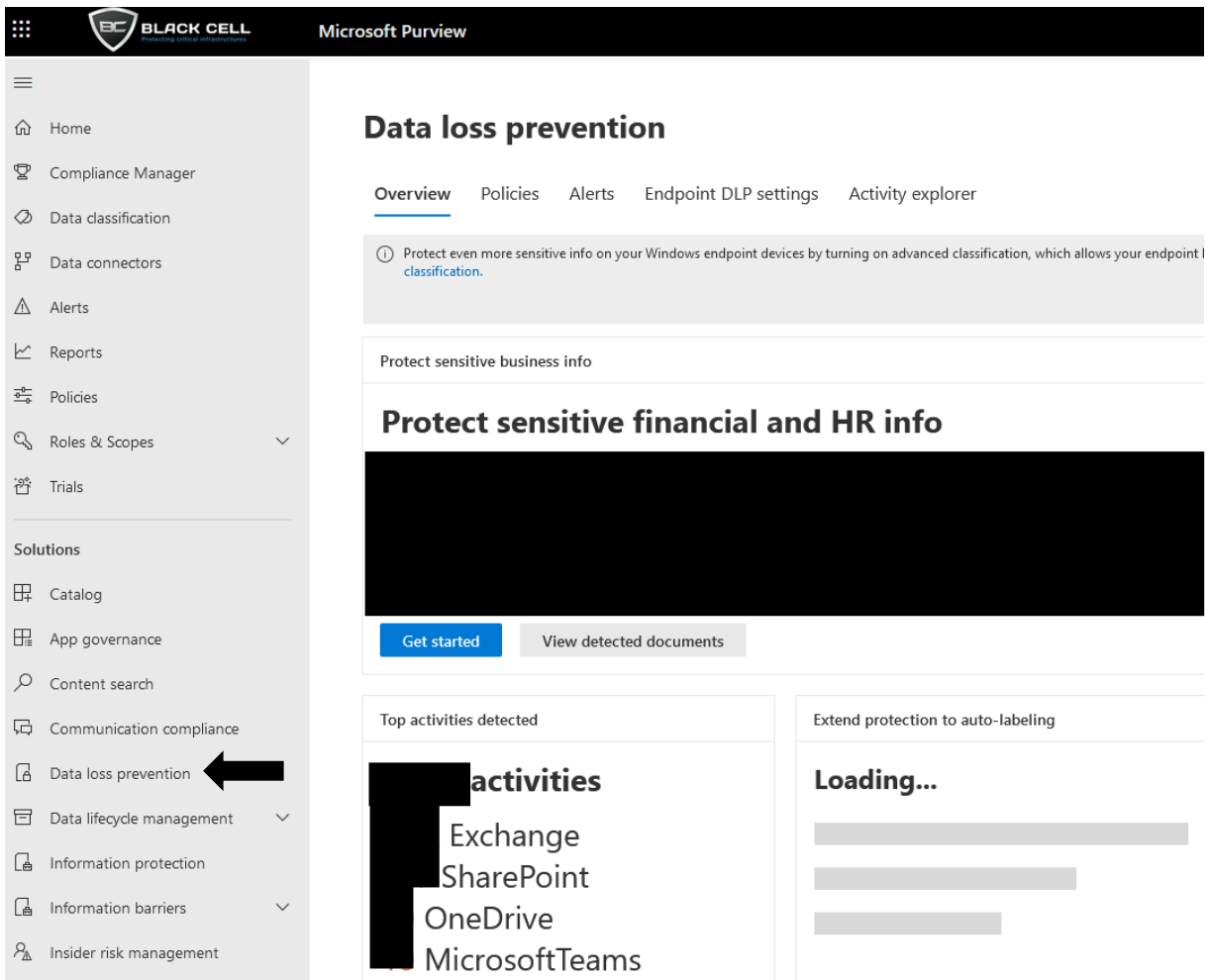
2. Configuring a custom DLP policy:

One of the most important aspects of security and compliance is data loss prevention. In the following section we are going to create an example policy that will prevent external users from accessing financial and tax related sensitive data.

2.1. First steps

Log into Microsoft Purview on the following website: <https://compliance.microsoft.com> or on <https://admin.microsoft.com>, below *Admin centers* select *Compliance* blade.

On Microsoft Purview select Data loss prevention blade.



The *Overview* page gives us information about our organization data loss prevention, such as *Top activities detected* on OneDrive, SharePoint, OneDrive, and Microsoft Teams.

To define a new policy, click *Policies* and then *Create policy* in the menu at the top.

Microsoft Purview

Data loss prevention

[Overview](#) [Policies](#) [Alerts](#) [Endpoint DLP settings](#) [Activity explorer](#)

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example y

Automatically configure Teams DLP policies to protect files shared in team messages
 Want to make sure all existing and future policies that protect Teams chats and channel messages also protect any files shared automatically be included in all Teams DLP policies.

↓

+ Create policy ↓ Export ↻ Refresh

<input type="checkbox"/>	Name	Order
--------------------------	------	-------

2.2. Choose the information to protect

Policies can be created by choosing a basic template which can be modified easily or by creating our own custom policy.

In this tutorial, select *Financial* category and from the template list U.S. Financial Data.

Data loss prevention > Create policy

Choose the information to protect

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

United States of America

Categories	Templates	
<ul style="list-style-type: none"> <input type="checkbox"/> Enhanced <input checked="" type="checkbox"/> Financial <input type="checkbox"/> Medical and health <input type="checkbox"/> Privacy <input type="checkbox"/> Custom 	<ul style="list-style-type: none"> PCI Data Security Standard (PCI DSS) <input checked="" type="checkbox"/> U.S. Financial Data U.S. Federal Trade Commission (FTC) Consumer Rules U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced 	<p>U.S. Financial Data</p> <p style="font-size: 0.8em;">Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.</p> <p>Protect this information:</p> <ul style="list-style-type: none"> • Credit Card Number • U.S. Bank Account Number • ABA Routing Number

More details about DLP policy templates can be found under the following link:
<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide>

Click Next.

12

TLP:CLEAR

2.3. Name your policy

Provide a name for the policy. A detailed description is highly recommended.

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy**
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

Name your DLP policy

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

Name *

Description

Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.

Click Next.

2.4. Location to apply the policy

Choose the Location to apply the policy to. By default, everything will be selected, and groups or users can be excluded. The purpose here is to select the locations with the highest risk such as Exchange email, SharePoint sites, OneDrive, etc.

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy**
- Policy settings
- Test or turn on the policy
- Review your settings

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

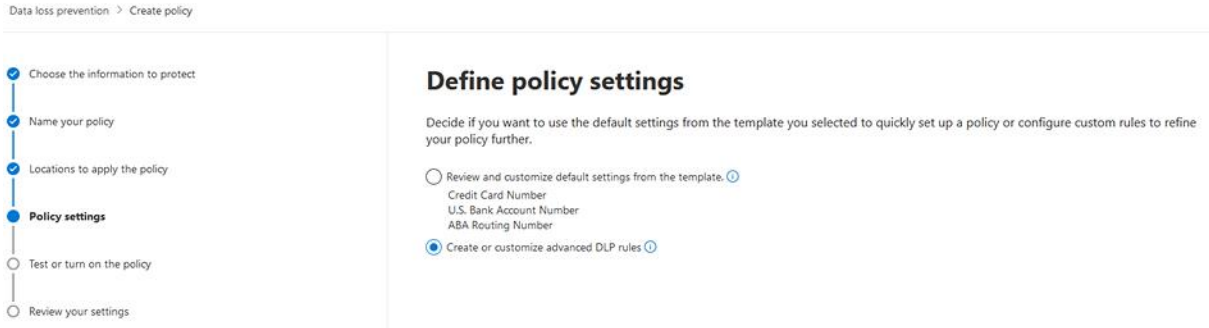
ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input type="checkbox"/> Off	Devices		
<input type="checkbox"/> Off	Microsoft Defender for Cloud Apps		
<input type="checkbox"/> Off	On-premises repositories		

Click Next.

2.5. Policy settings

At this step, the default settings from the template are displayed. Select *Create or customize advanced DLP rules*, where rules can be added to the policies.



Data loss prevention > Create policy

Choose the information to protect
 Name your policy
 Locations to apply the policy
Policy settings
 Test or turn on the policy
 Review your settings

Define policy settings

Decide if you want to use the default settings from the template you selected to quickly set up a policy or configure custom rules to refine your policy further.

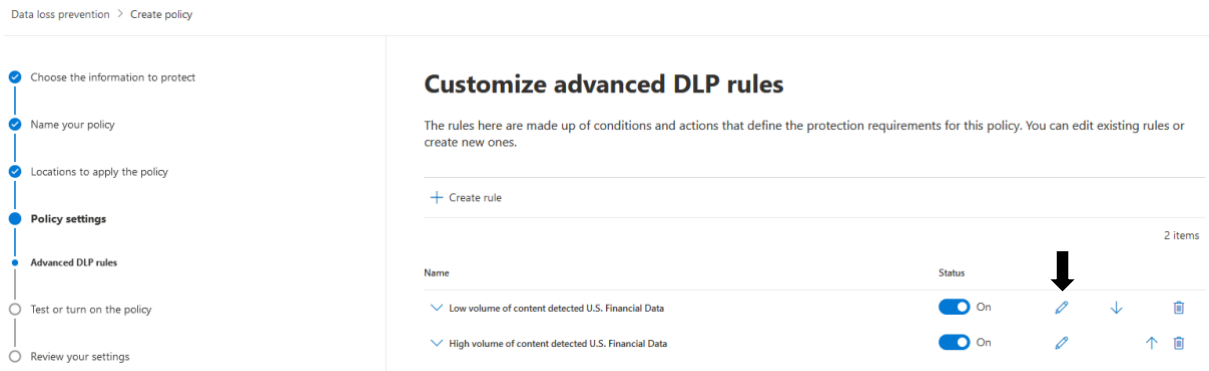
Review and customize default settings from the template. ⓘ
 Credit Card Number
 U.S. Bank Account Number
 ABA Routing Number

Create or customize advanced DLP rules ⓘ

Click Next.

2.6. Advanced DLP rules

From the list choose Low volume content detected U.S Financial Data and click on pencil icon to edit the DLP rule.



Data loss prevention > Create policy

Choose the information to protect
 Name your policy
 Locations to apply the policy
Policy settings
 Advanced DLP rules
 Test or turn on the policy
 Review your settings

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.

+ Create rule

2 items

Name	Status			
Low volume of content detected U.S. Financial Data	On			
High volume of content detected U.S. Financial Data	On			

2.6.1. Conditions

In section *Content is shared from Microsoft 365*, choose the option *with people outside my organization*. This condition will affect users outside of the organization. More sensitive information types can be added with the confidence level selected. Click *Add*.

Edit rule

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Group name * Group operator

Sensitive info types

Credit Card Number Instance count to

U.S. Bank Account Number Instance count to

ABA Routing Number Instance count to

Add

Create group

AND

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.

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

Choose sensitive info types, scroll down, and pick out U.S. Individual Taxpayer Identification Number (ITIN).

Edit rule

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Group name *

Sensitive info types

Credit Card Number

U.S. Bank Account Number

ABA Routing Number

Add

Sensitive info types

Trainable classifiers

Sensitive info types

1 selected

Name	Publisher
U.K. National Insurance Number (NINO)	Microsoft Corporation
U.K. Physical Addresses	Microsoft Corporation
U.K. Unique Taxpayer Reference Number	Microsoft Corporation
U.S. / U.K. Passport Number	Microsoft Corporation
U.S. Bank Account Number	Microsoft Corporation
U.S. Driver's License Number	Microsoft Corporation
<input checked="" type="checkbox"/> U.S. Individual Taxpayer Identification N...	Microsoft Corporation
U.S. Physical Addresses	Microsoft Corporation

Click Add.

2.6.2. Actions

Click *Add an action* and choose *Restrict access or encrypt the content in Microsoft 365 location*.

Edit rule

Actions

Use actions to protect content when the conditions are met.

+ Add an action

Restrict access or encrypt the content in Microsoft 365 locations

Apply this action only people outside your organization.

^ Actions

Use actions to protect content when the conditions are met.

^ Restrict access or encrypt the content in Microsoft 365 locations 🗑️

Restrict access or encrypt the content in Microsoft 365 locations

Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
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.

Block everyone. ⓘ

Block only people outside your organization. ⓘ

2.6.3. User notifications

In this section, how to notify the users about an action was taken can be defined. Under *Policy tips*, check the box next to *Customize the policy tip text*. If a file contains Personally Identifiable Information (PII) a notification will be sent to the user in a pop-up window. These notifications help to keep users informed and educated about organization's DLP policies.

Edit rule

^ 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

Email notifications

Notify the user who sent, shared, or last modified the content.

Notify these people:

The person who sent, shared, or modified the content

Owner of the SharePoint site or OneDrive account

Owner of the SharePoint or OneDrive content

Send the email to these additional people:

[Add or remove people](#)

Customize the email text

Customize the email subject

Policy tips

Customize the policy tip text



This file conflicts with a policy in your organization.

2.6.4. User overrides

Choose *Require a business justification to override* to mandate users to provide a rationale for deviating from the policy rule. For example, a salesperson may be allowed to override this policy with a proper business justification.

^ User overrides

Allow overrides from M365 services

- Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.
- Require a business justification to override
- Override the rule automatically if they report it as a false positive

2.6.5. Incident reports

Various options are available for generating reports on policy rule matches. An alert to an admin or to any optional groups of users can be sent if a rule match occurred. Number of alerts can be limited based on customizable thresholds. The priority of the alert can be set.

^ Incident reports

Use this severity level in admin alerts and reports: Low v

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

[Add or remove groups](#)

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 A single user v

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

Off

Click save and next.

2.7. Test or turn on the policy

It is recommended that you test the policy first to make sure that it is set up correctly.

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy**
- Review your settings

Test or turn on the policy

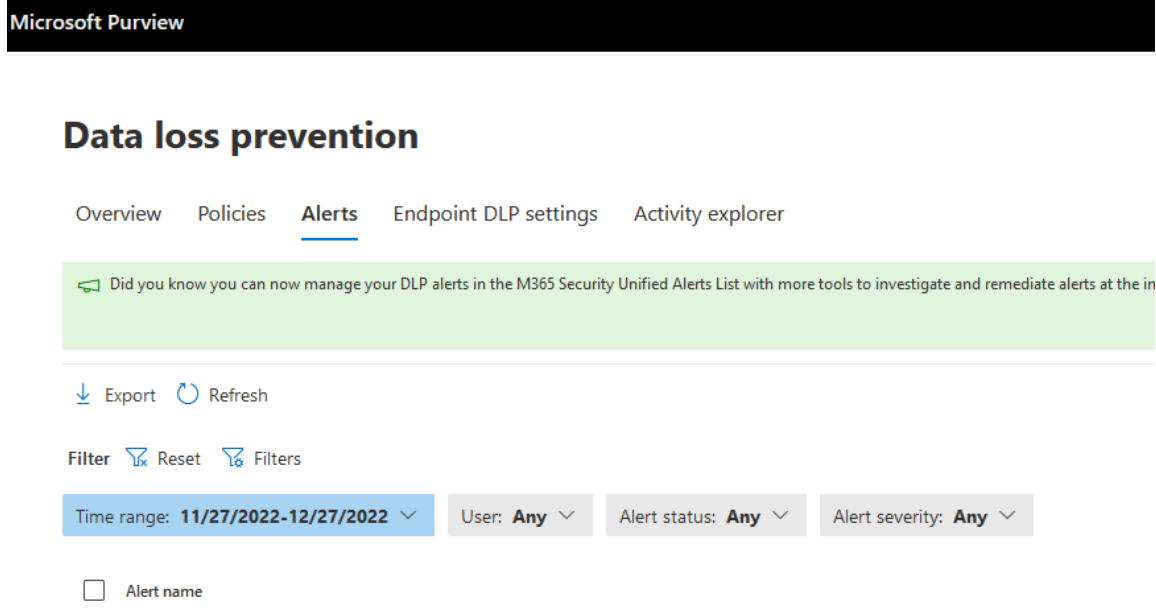
Decide whether you want to turn the policy on right away or test it out first.

- Test it out first**
 You'll be able to review alerts to assess the policy's impact. Any restrictions you configured won't be enforced. [Learn more about test mode](#)
 - Show policy tips while in test mode
- Turn it on right away**
 After the policy is created, it'll take up to an hour for it to take effect.
- Keep it off**
 You'll be able to test it out or turn it on later.

Click Next. Review your settings and select Submit.

2.8. After the test

If everything went fine and the policy is active, under the *Data loss prevention* blade, *Alerts* tab or *Activity explorer* can be checked to see if the policy generated any alerts.



The screenshot shows the Microsoft Purview interface for Data loss prevention. At the top, there is a navigation bar with tabs for Overview, Policies, Alerts (which is selected), Endpoint DLP settings, and Activity explorer. Below the navigation bar, there is a green notification banner that says "Did you know you can now manage your DLP alerts in the M365 Security Unified Alerts List with more tools to investigate and remediate alerts at the in". Underneath the banner, there are buttons for Export and Refresh. Below that, there is a Filter section with a Reset button and a Filters button. There are four filter dropdown menus: Time range (set to 11/27/2022-12/27/2022), User (set to Any), Alert status (set to Any), and Alert severity (set to Any). At the bottom, there is a checkbox labeled "Alert name".

3. Executive summary

Microsoft Purview provides numerous opportunities to keep our data safe. These options are essential for organisations to protect against hackers and malicious actors. The Data loss prevention feature enables high level of customization for setting rules in the data protection policies and can play a vital role in the organization's data lifecycle management.

4. References

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

<https://azure.microsoft.com/en-gb/products/purview/>