Information Protection and Governance in Microsoft 365

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Microsoft Purview Information Protection

Microsoft Purview Data Lifecycle Management

Data classification and content explorer

Sensitivity labels and sensitivity policies

Data loss prevention

Retention labels and retention policies

Records management

Microsoft Purview unified data governance

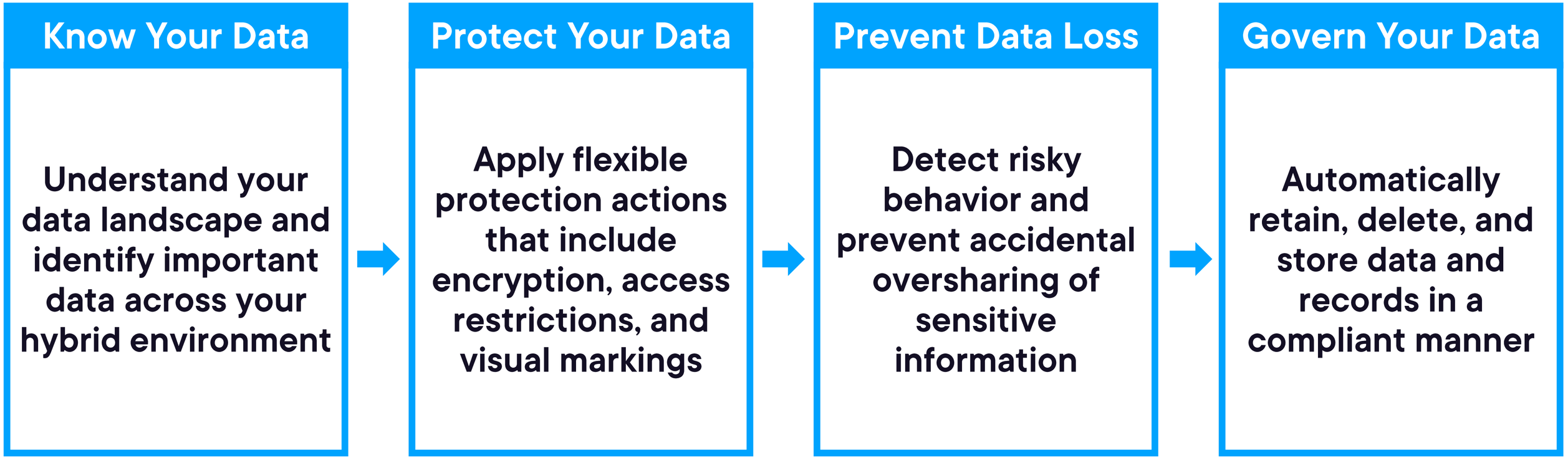
Microsoft Purview Information Protection and Data Lifecycle Management

Microsoft Purview Information Protection

Microsoft Purview Information Protection discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss.

https://learn.microsoft.com/en-us/purview/information-protection

Microsoft Purview Information Protection

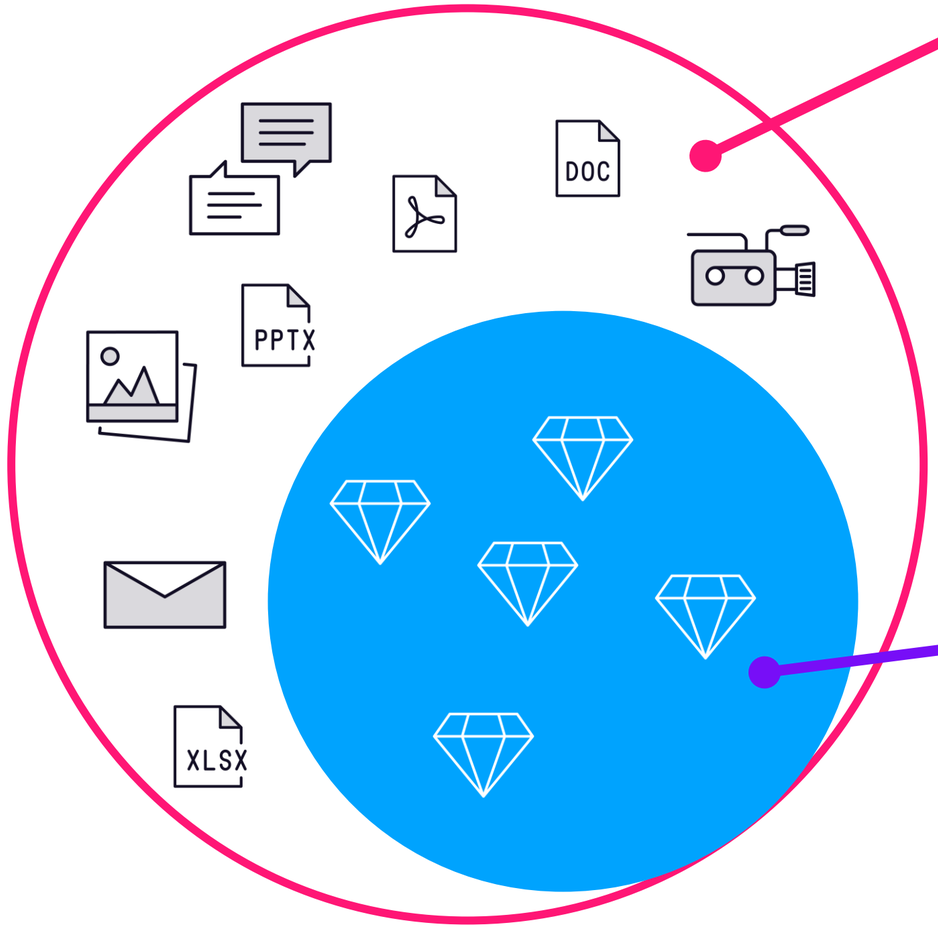


Microsoft Purview Data Lifecycle Management

Microsoft Purview Data Lifecycle Management manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. It gives organizations the capabilities to govern their data, for compliance or regulatory requirements.

https://learn.microsoft.com/en-us/purview/manage-data-governance

Govern Your Data



Microsoft Purview Data Lifecycle Management

Mange risk and liability by only keeping what you need and deleting what you don't across your entire digital estate

Microsoft Purview Records Management

Manage high value content following the specialized workflows required to meet legal, business, or regulatory recordkeeping obligations

Information protection and data lifecycle management work together to classify, protect, and govern your data where it lives, and wherever it goes.

The Features from This Module

Know your data

Sensitive information types

Trainable classifiers

Protect your data

Sensitivity labels

Prevent data loss

Data Loss Prevention

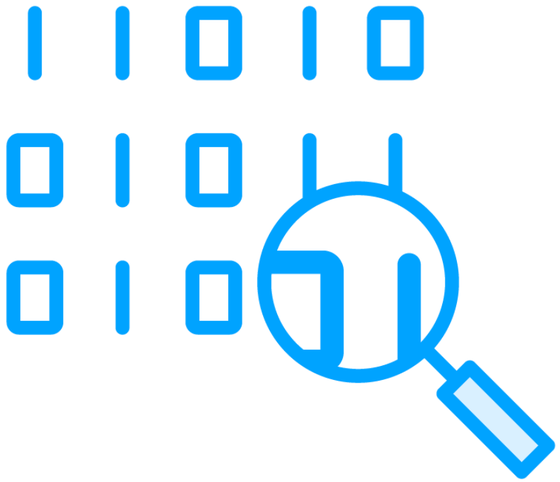
Govern your data

Retention policies

Records management

Data Classification and Content Explorer

Data Classification



Microsoft has a strong classification system that can detect many types of data in your tenant

- Without needing to create any policy

Great way to understand the data you might need to protect as you configure your labels/ policies

Overview Tab

Overview

Get snapshots of how sensitive info and labels are being used across your organization's locations. Learn more

Top trainable classifiers

Trainable classifiers used most in your content

View all trainable classifiers

Top sensitive info types

Sensitive info types used most in your content

View all sensitive info types

Top sensitivity labels applied to content

View all applied sensitivity labels

Top retention labels applied to content

No retention labels detect...

You haven't created any retention labels or they haven't been applied to content yet.

Learn more

Daily labeling activity by users

View all activities

Top activities detected

95 activities

67 Auto-labeling simulation
22 DLP rule matched
6 Label applied

View all activities

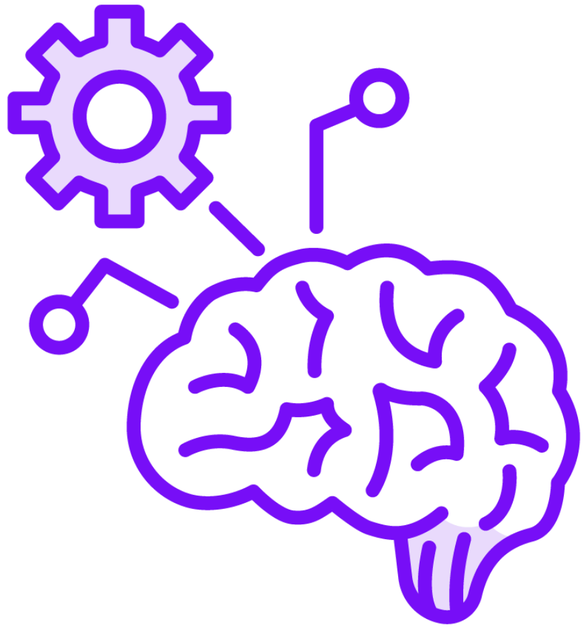
Features You Can Configure

Trainable Classifiers

Sensitive Information Types

Exact Data Matches

Trainable Classifiers

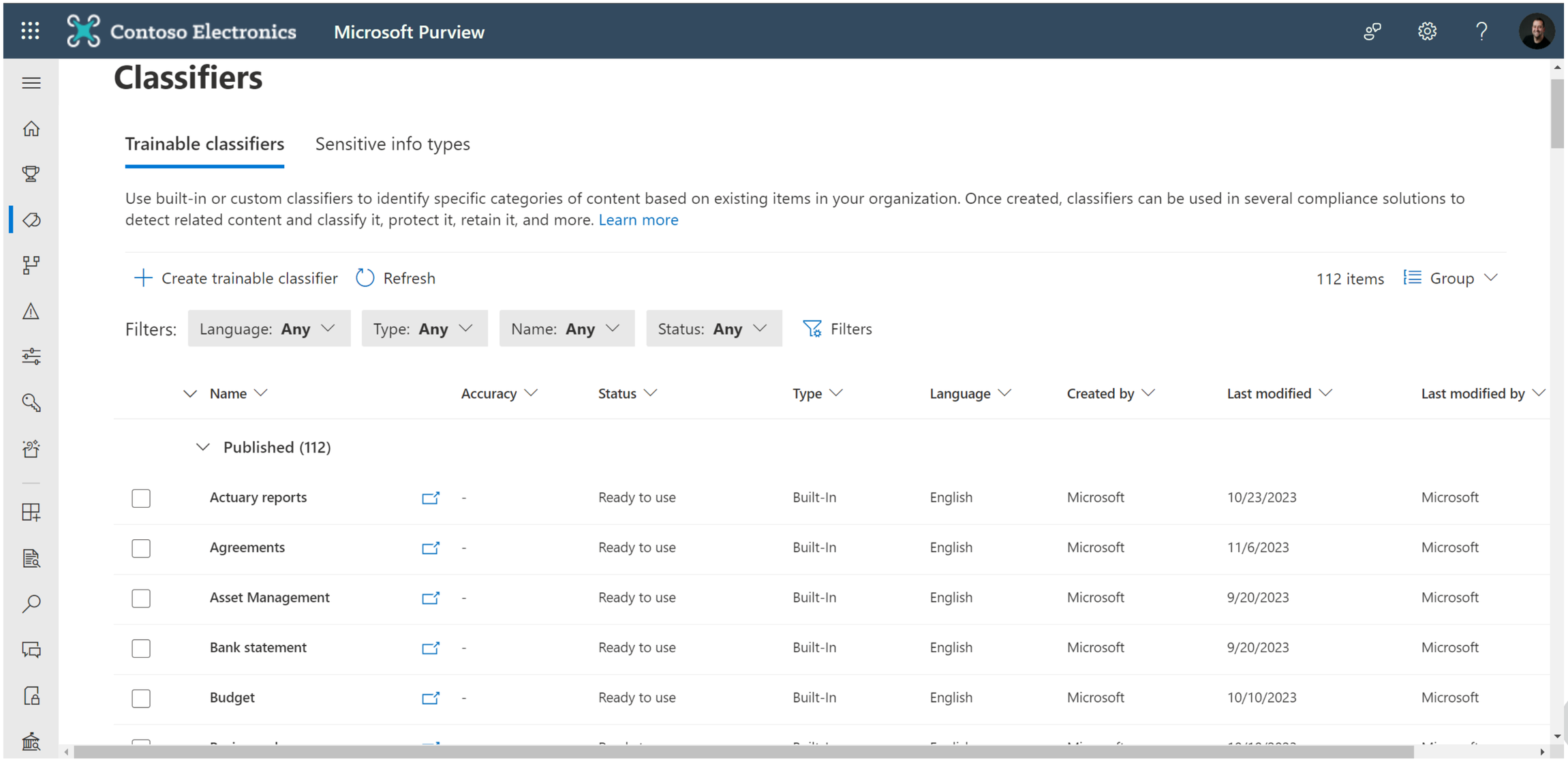


Tool you train to recognize various types of content

- Resume
- Contract
- Source code
- Harassment language

Built-in and custom

Trainable Classifiers



Sensitive Information Types

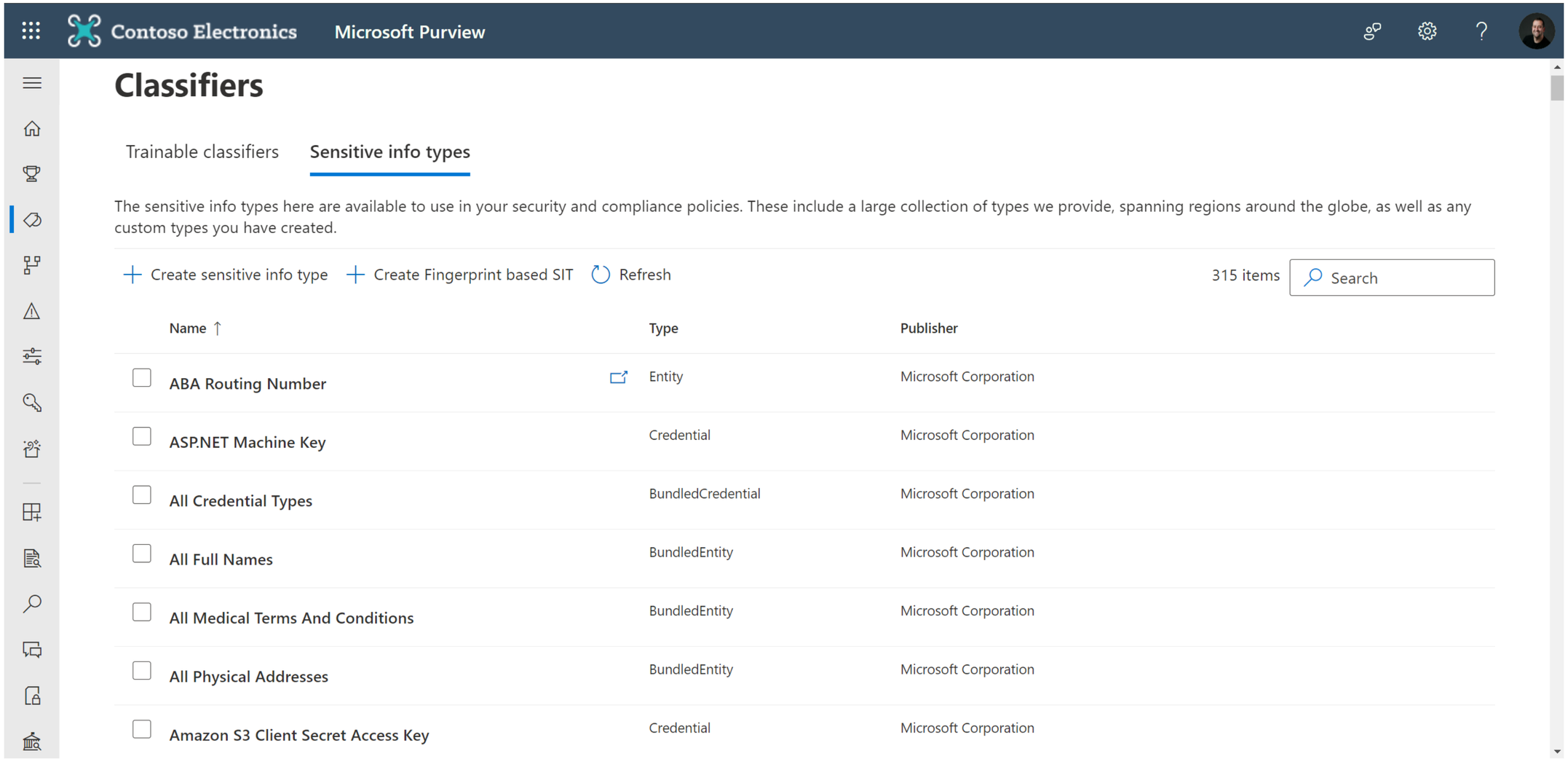
Pattern-based classifiers to detect sensitive information

- Social Security numbers
- Credit cards numbers
- Bank account numbers

Microsoft offers 300+ built-in from around the globe

- You can also create your own

Sensitive Info Types



Exact Data Match (EDM)-based classification

Create custom sensitive information type

- Based on exact data values rather than a pattern

Can have as much as 100 million rows of data

- Refreshed daily

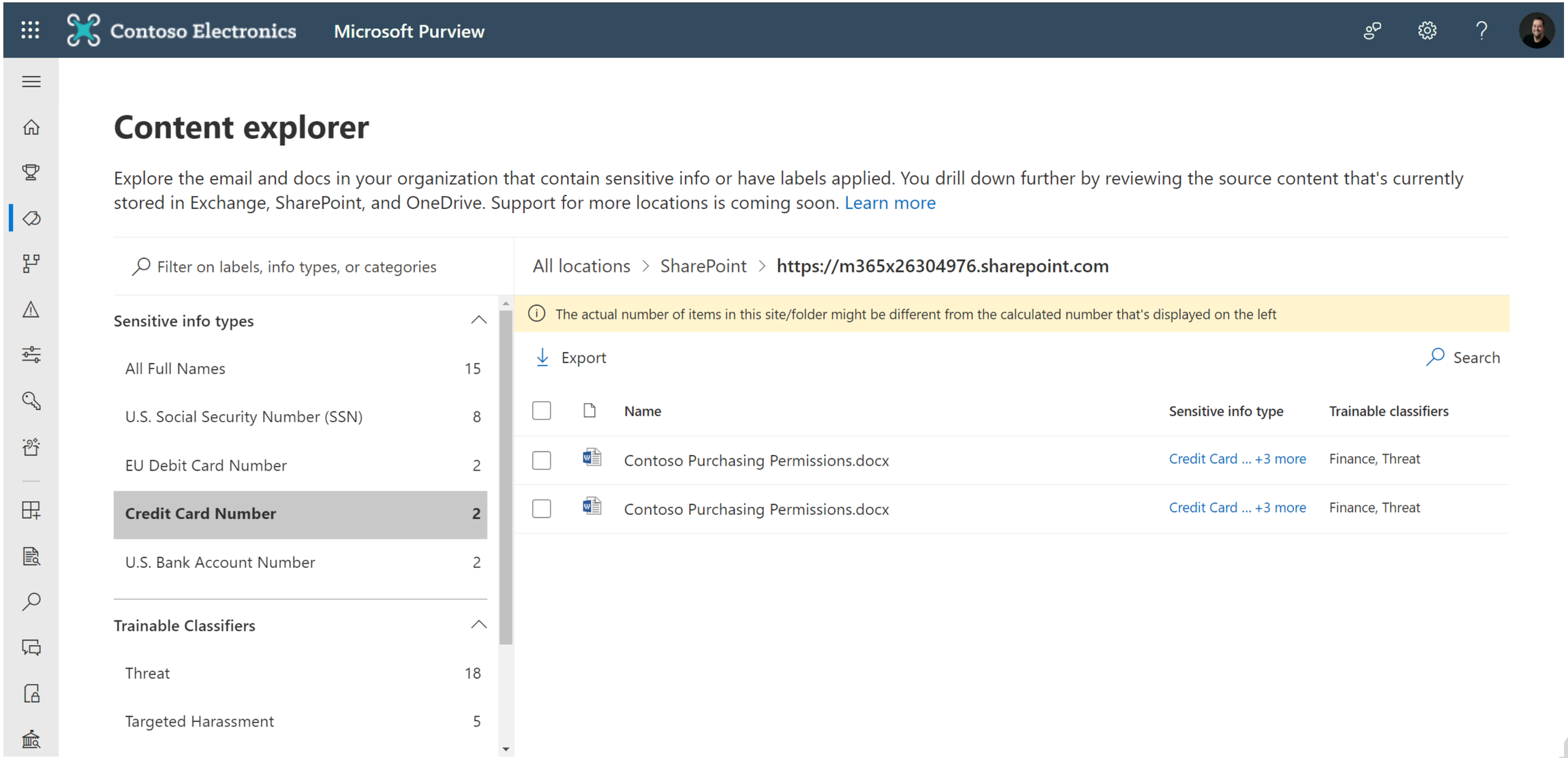
Content Explorer

Snapshot of items that have been labeled or classified

- Sensitive info types
- Trainable classifiers
- Labels applied

Natively view the items

Content Explorer



Activity Explorer

Monitor what's being done with your labeled content

- Read
- Deletion
- Printed
- Copied to network share/USB

Information is collected from the Unified Audit Log

- But in an easier to consume user interface

Activity Explorer

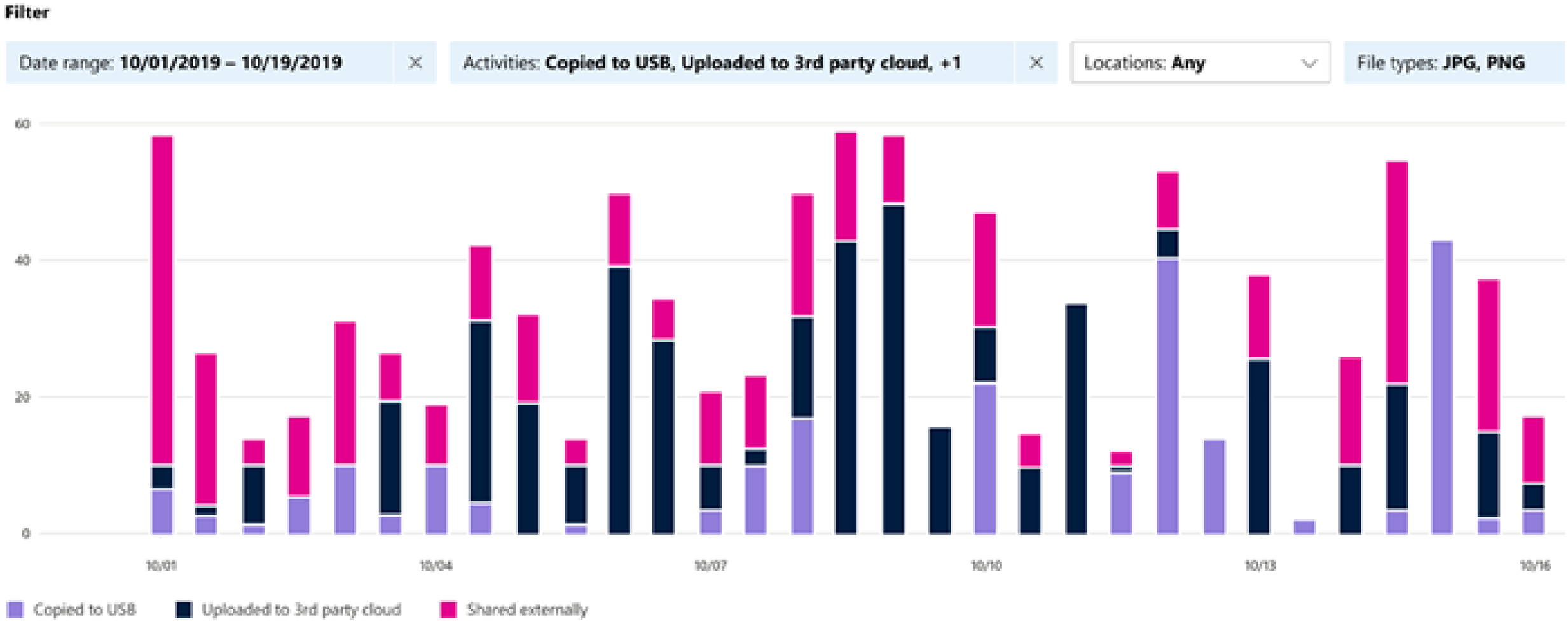


Image: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer

Demo

Exploring files with the content explorer

Sensitivity Labels and Sensitivity Policies

Sensitivity Labels

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered

https://learn.microsoft.com/en-us/purview/sensitivity-labels

Sensitivity Labels Features

Enforce protection settings such as encryption or watermarks on labeled content

Protect content in Microsoft 365 apps across different platforms and devices

Protect content in third-party apps and services

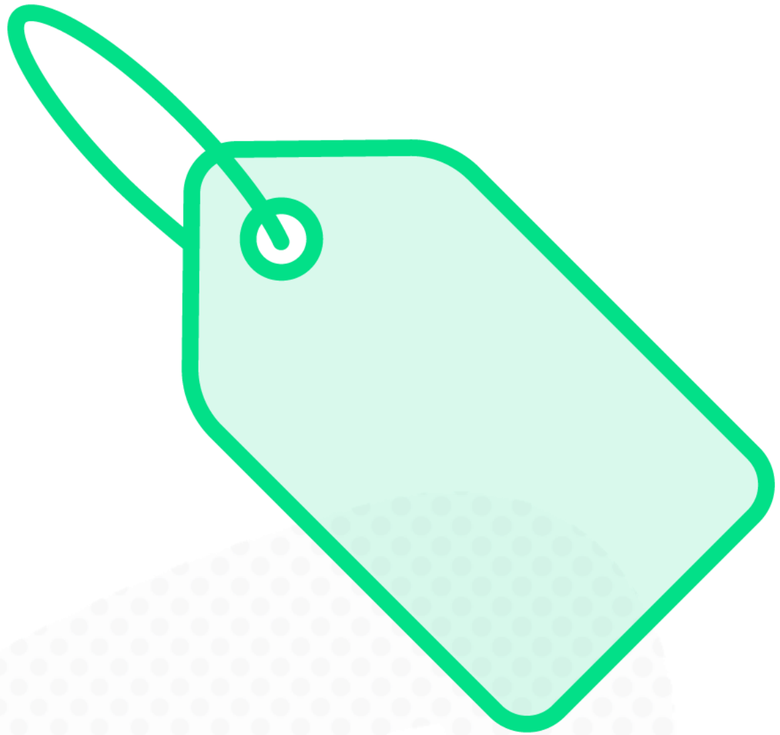
Sensitivity Labels Also Work with Containers

Sensitivity labels can be applied at the container level

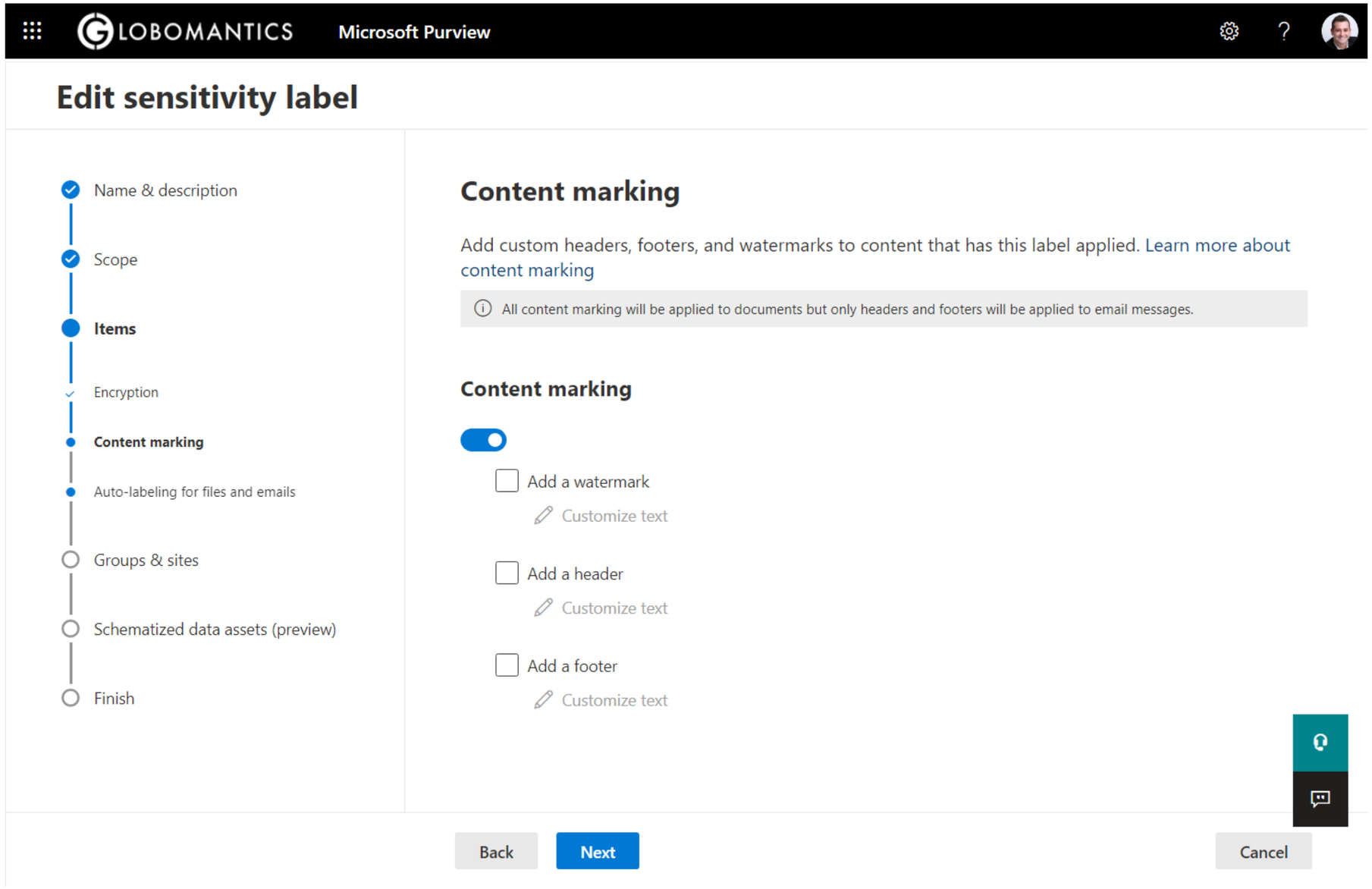
- Microsoft 365 Groups
- Microsoft Teams
- SharePoint sites

Using the label, you can configure

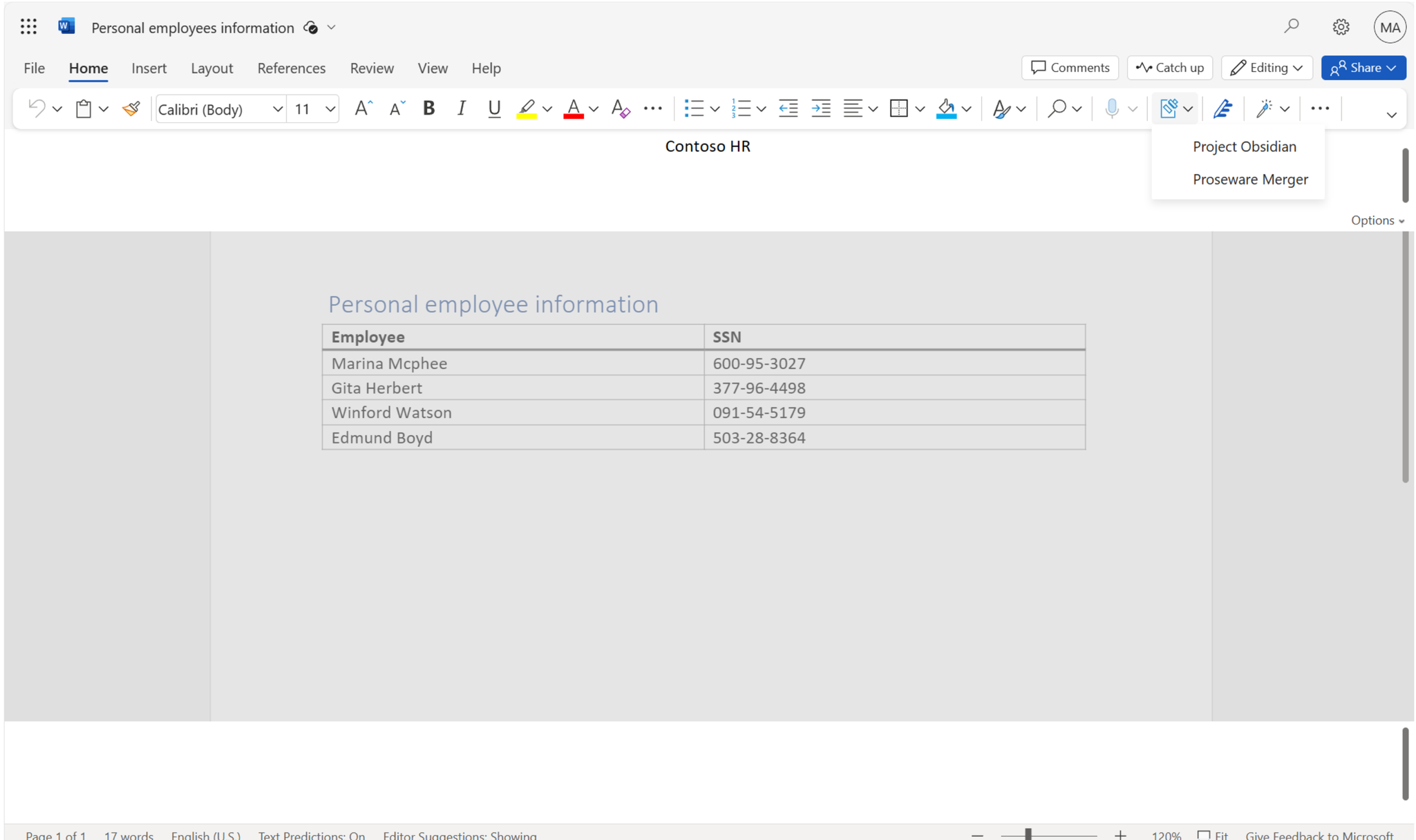
- Privacy (public or private)
- External user access
- Access from unmanaged device



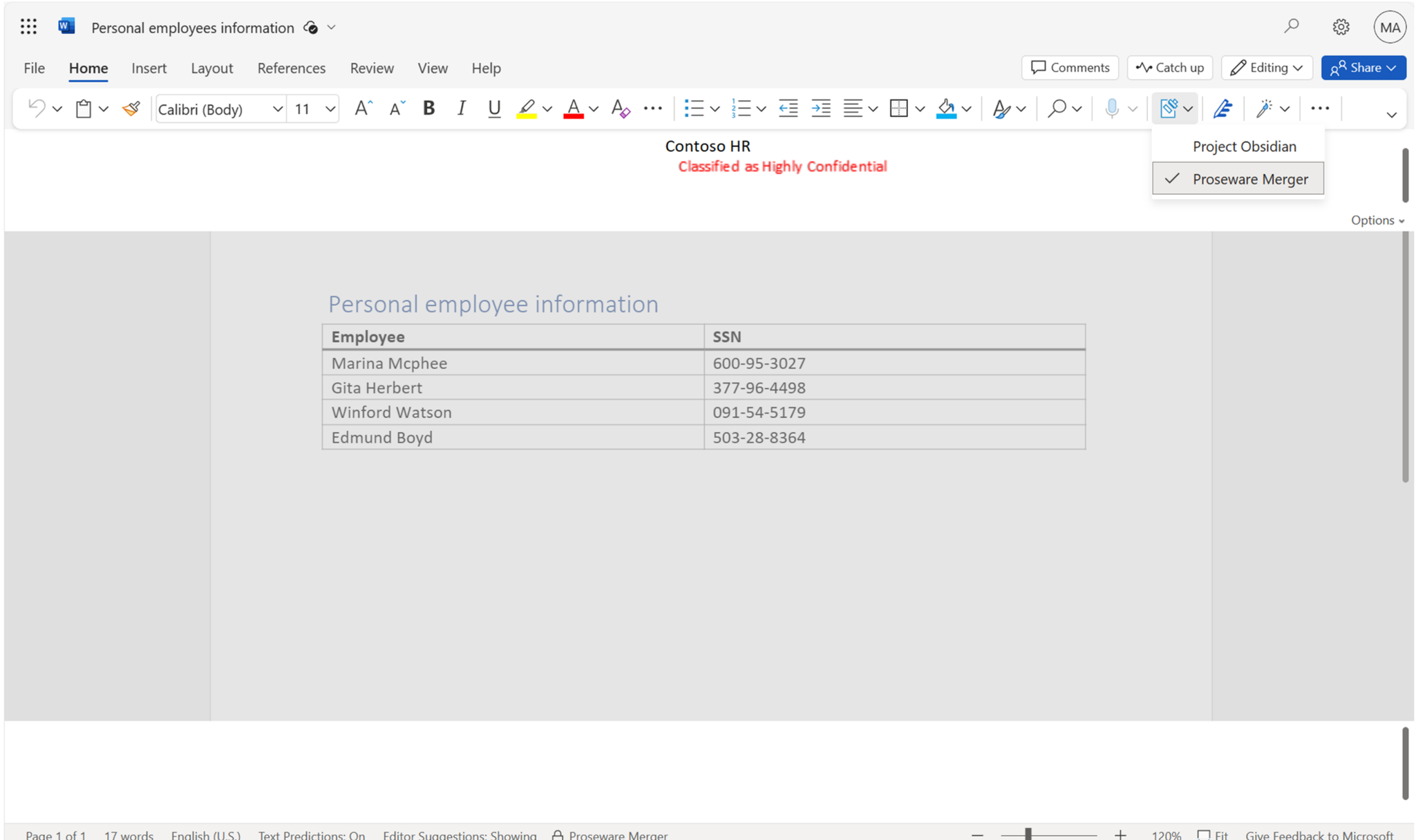
Sensitivity Labels



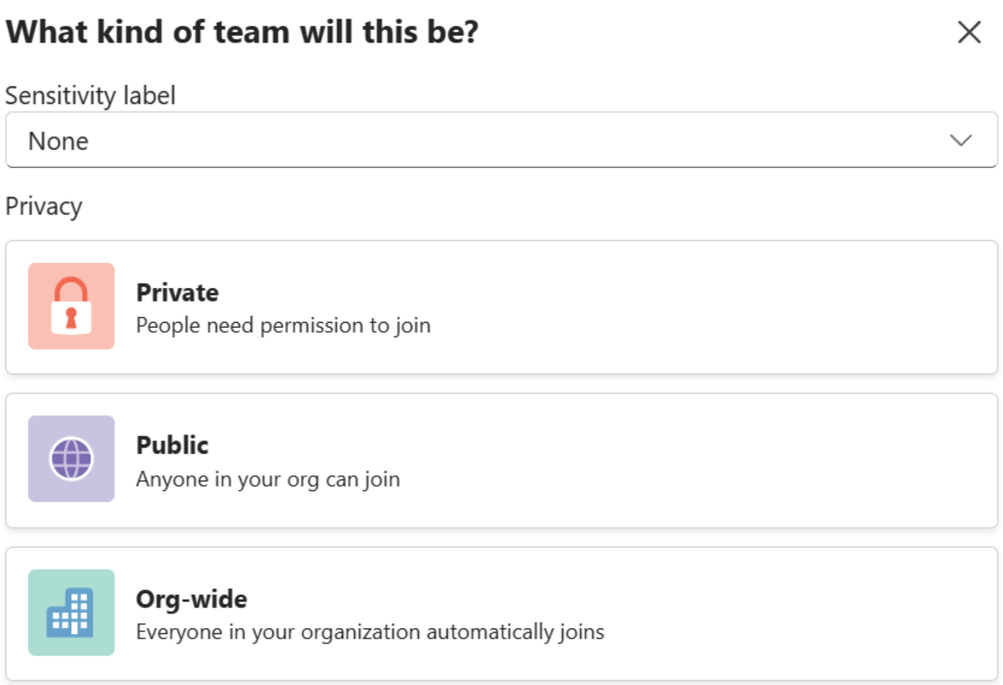
Sensitivity Label: Document without Label

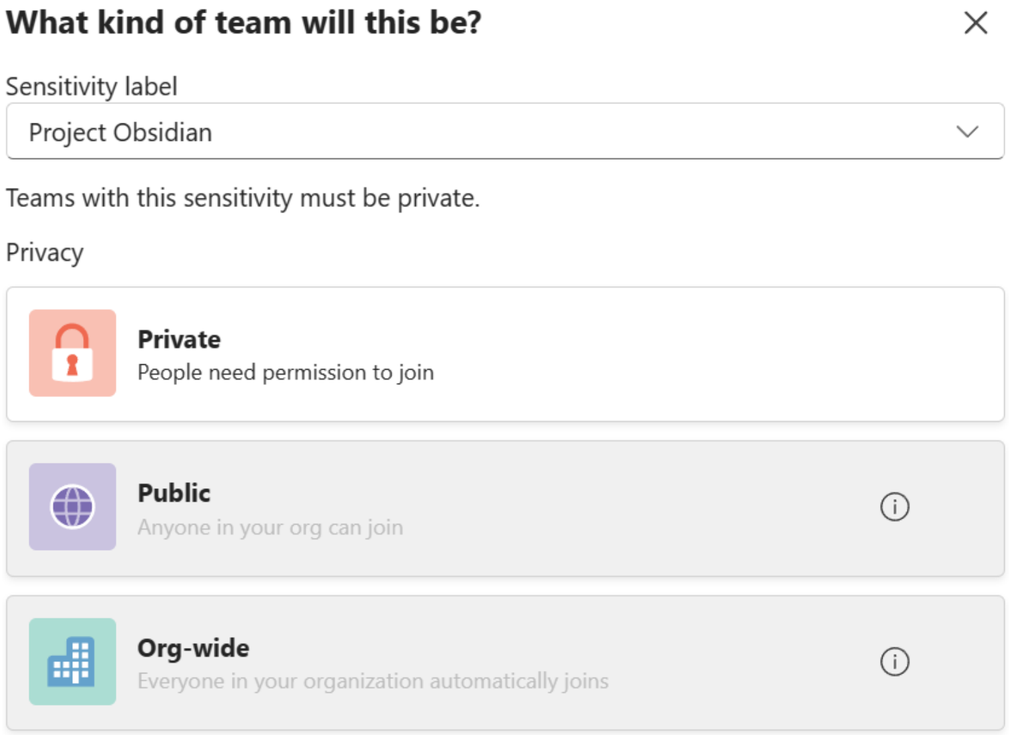


Sensitivity Label: Document with Label

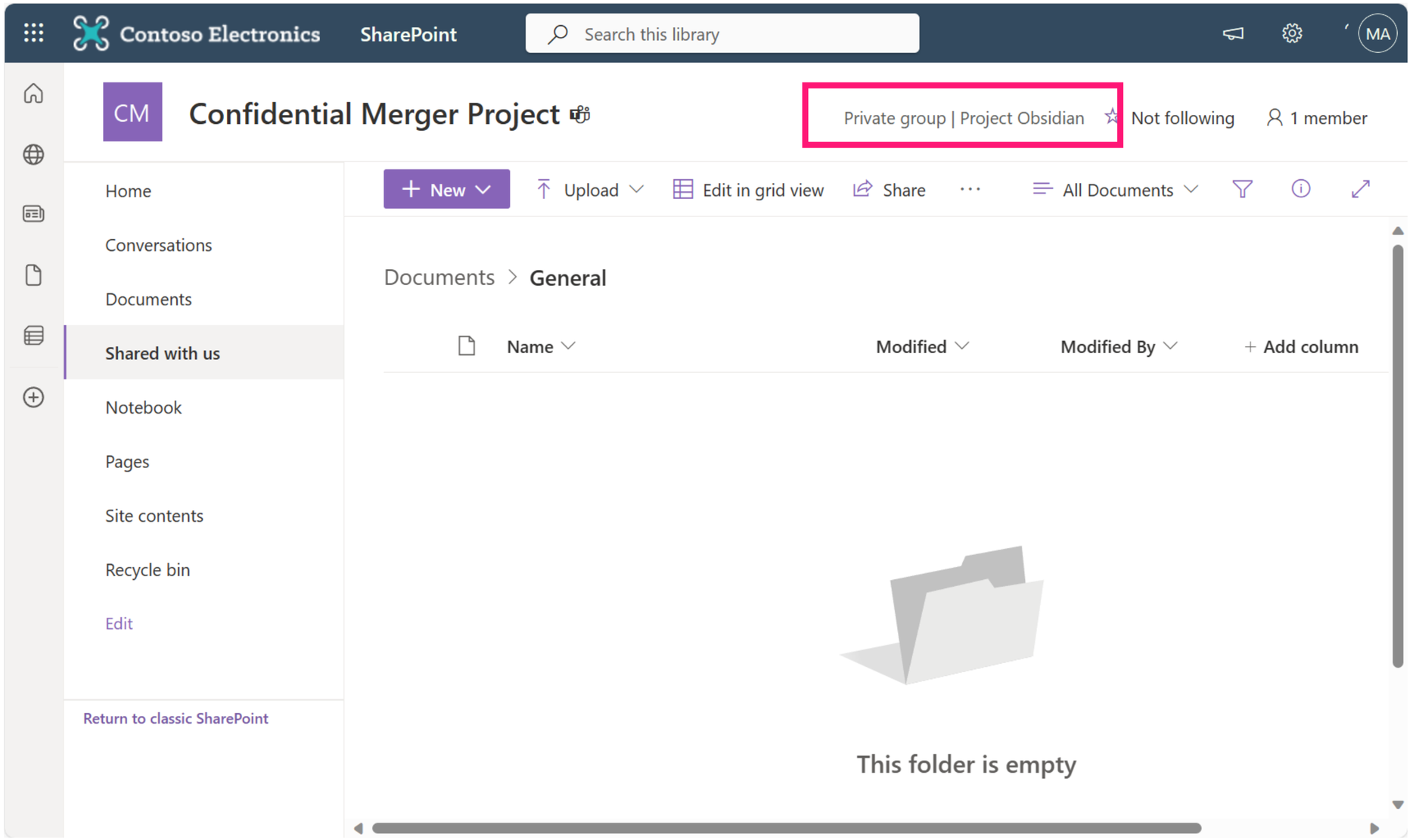


Sensitivity Labels: Teams Creation Experience

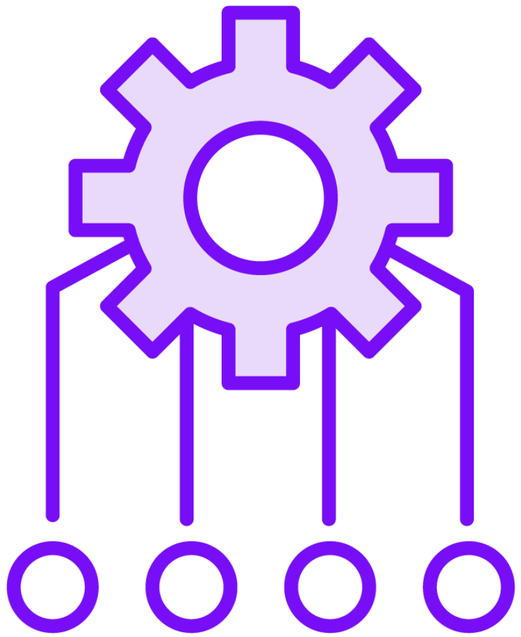




Sensitivity Labels: Teams Display Experience



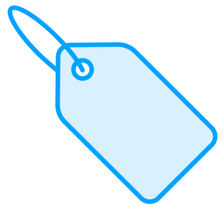
Sensitivity Labels Policies



Sensitivity labels need to published using policies

- Which users and groups can see specific labels
  - User(s)
  - E-mail enabled security groups
  - Distribution groups
  - Microsoft 365 Groups

Other Label Policy Settings



Apply a default labels to new e-mails/documents by those users

Require justifications for label changes

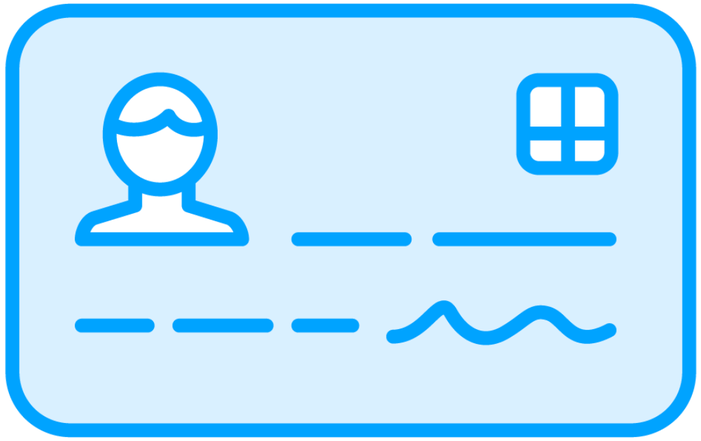
Require users to apply a label (mandatory labeling)

Demo

Sensitivity labels in action

Data Loss Prevention

Data Loss Prevention (DLP)



Set of tools to identify sensitive data from being shared

- Credit card number
- Social Security number
- Passport number

You can also create custom sensitive information

- Client case numbers
- Patient number

Microsoft Purview Data Loss Prevention

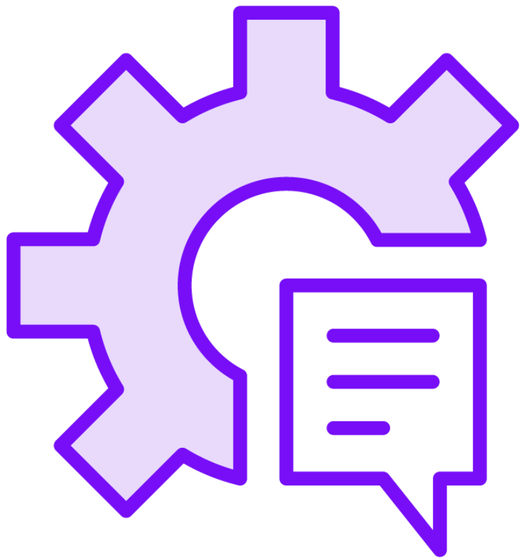
Can identify information across

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams

Also works with non-cloud services

- On-premises SharePoint Server
- File shares

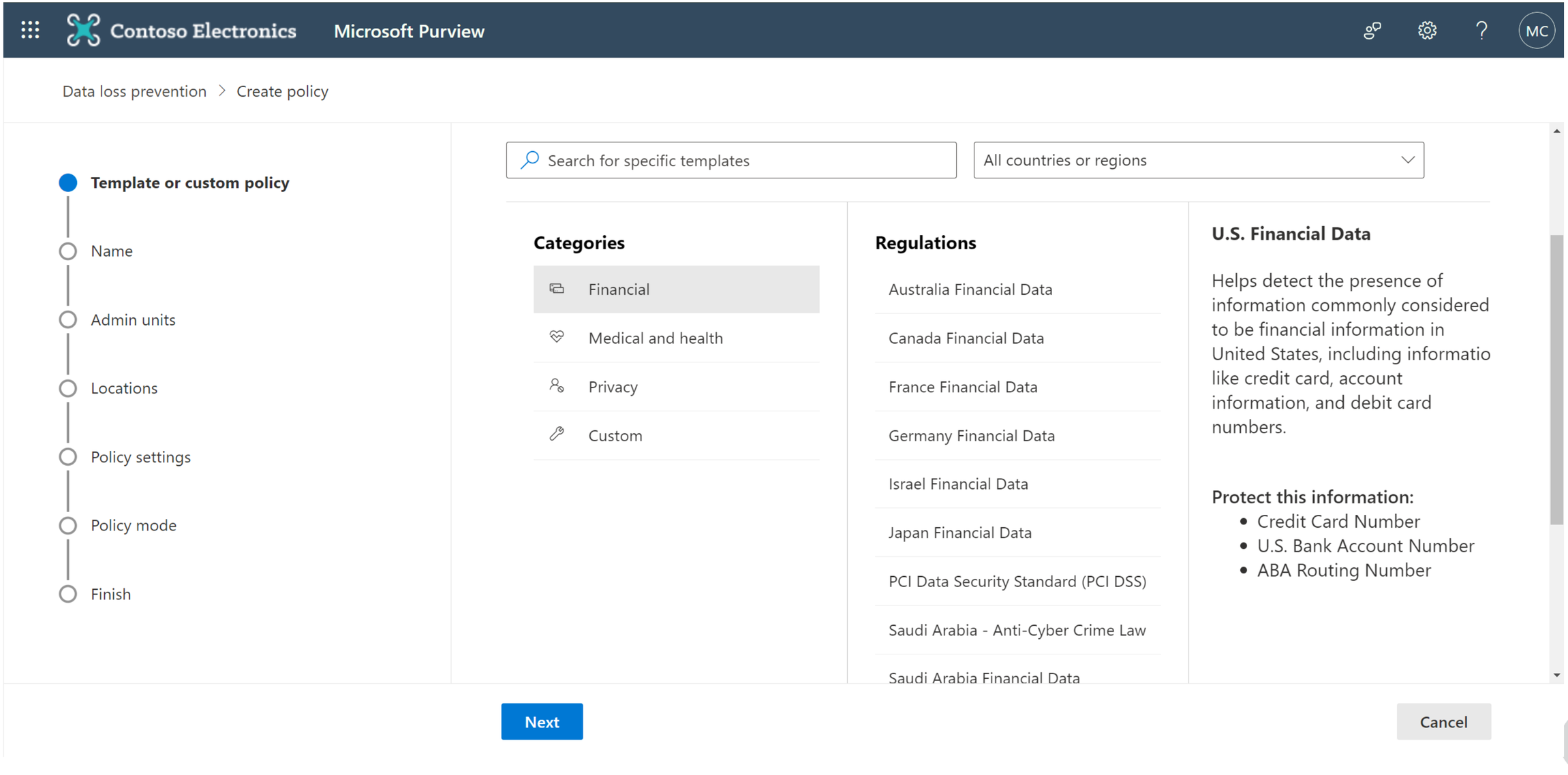
Data Loss Prevention Policies



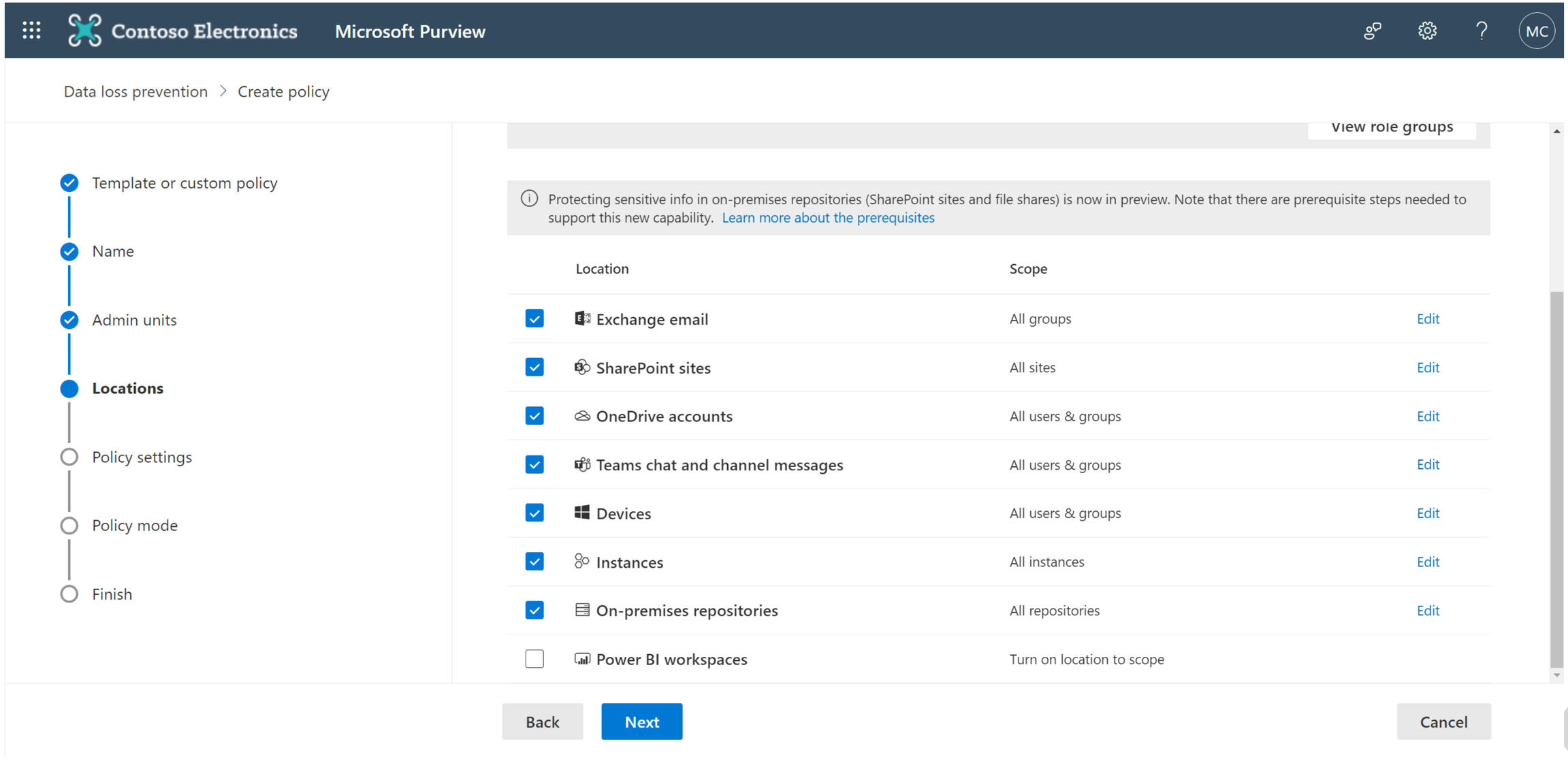
You create different policies for the type of content you want to protect

- Type of sensitive information
- Locations to check
- Action to do if sensitive information found
  - Show a pop-up warning
  - Block the sharing
  - Lock and move content to a quarantine location

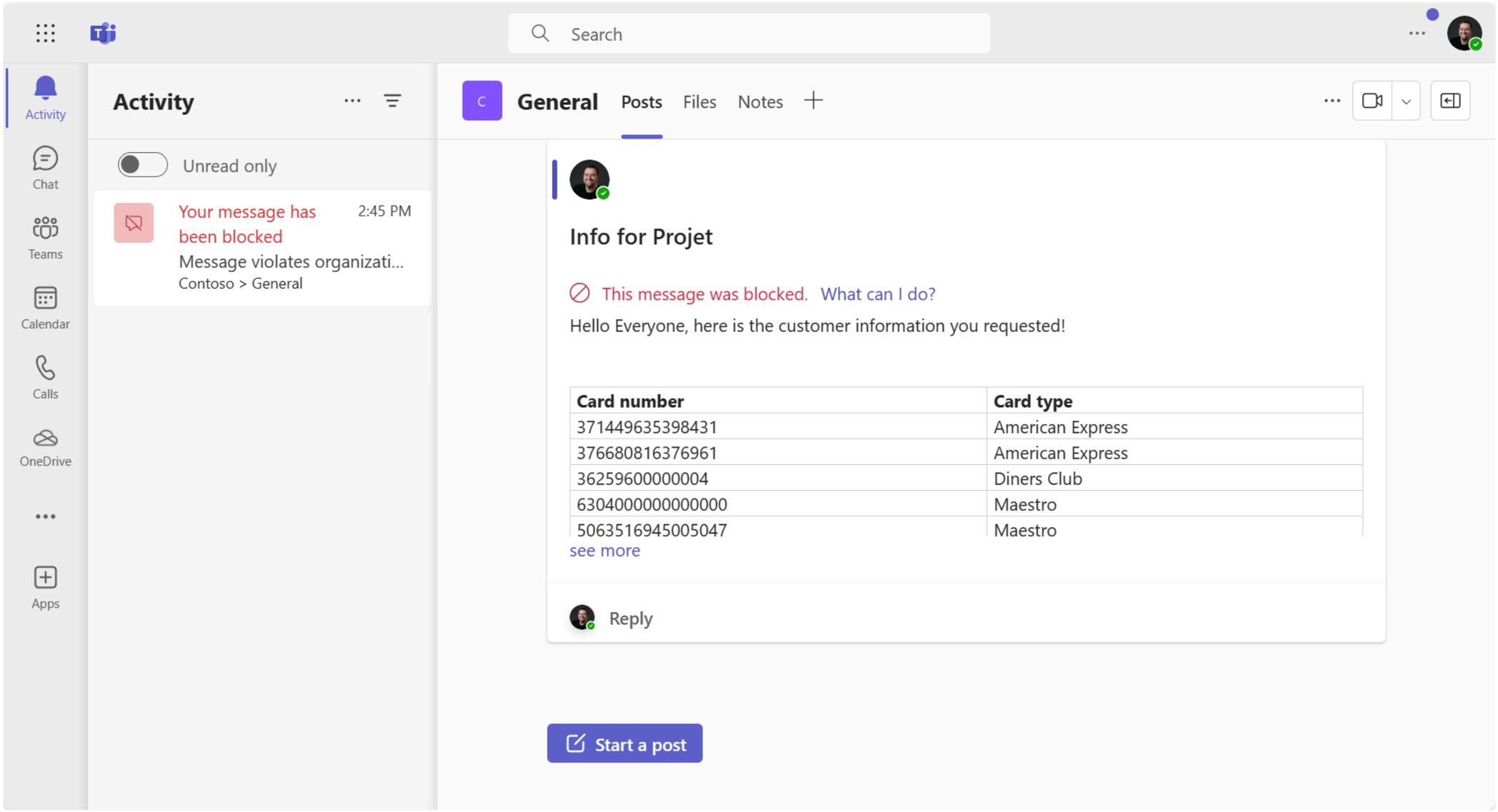
Data Loss Prevention Policy



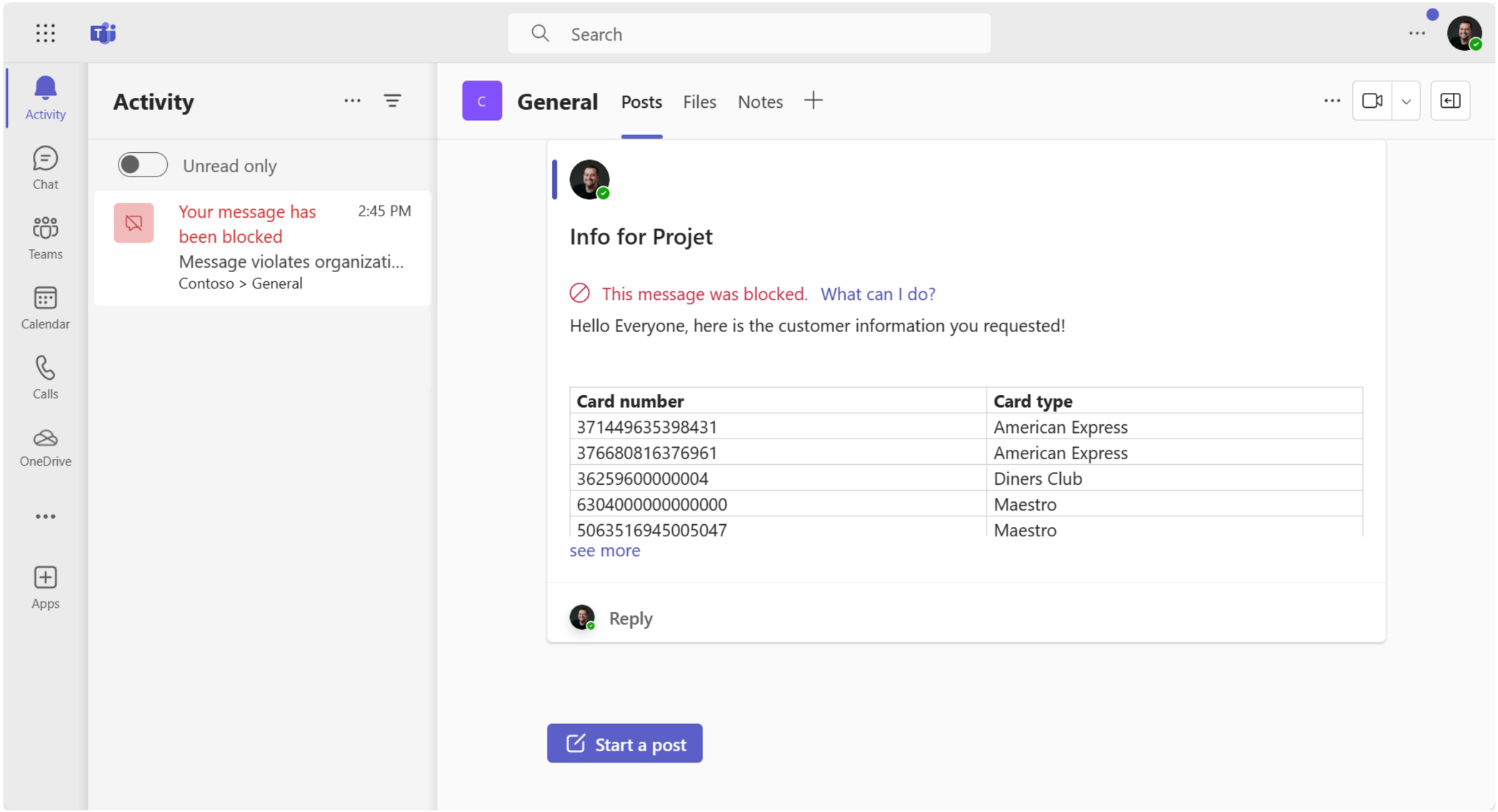
DLP Policy Locations



Data Loss Prevention Inside Microsoft Teams



Data Loss Prevention Inside Microsoft Teams



Policy Tip

Your message was blocked due to organization policy

- Credit Card Number

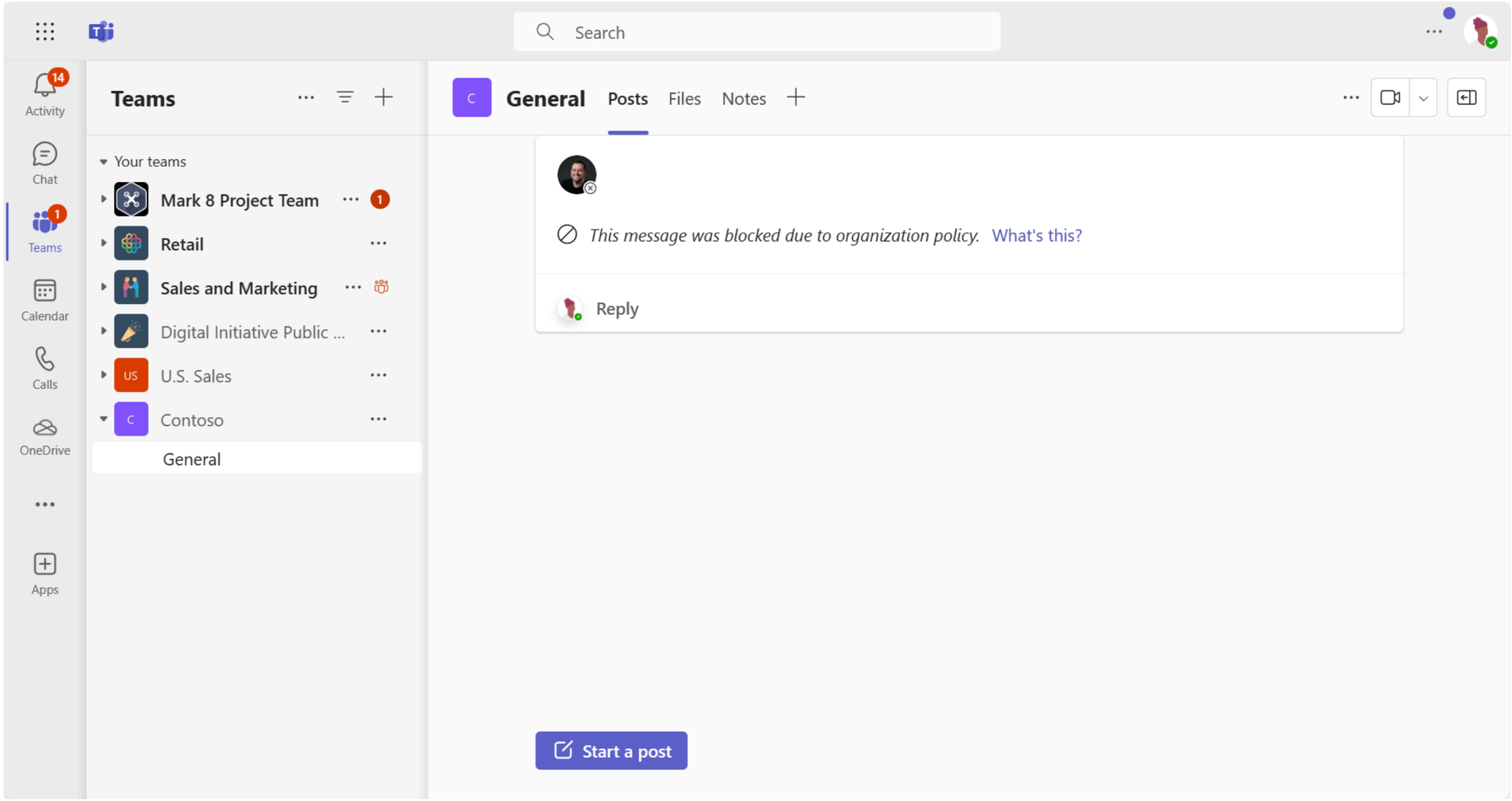
This item conflicts with a policy in your organization.

Here's what you can do

If you think the message was blocked in error, report it to your admin. Reporting won't send the message.

Cancel Report

Data Loss Prevention: Other Users View



Retention Labels and Retention Policies

Retention Policies

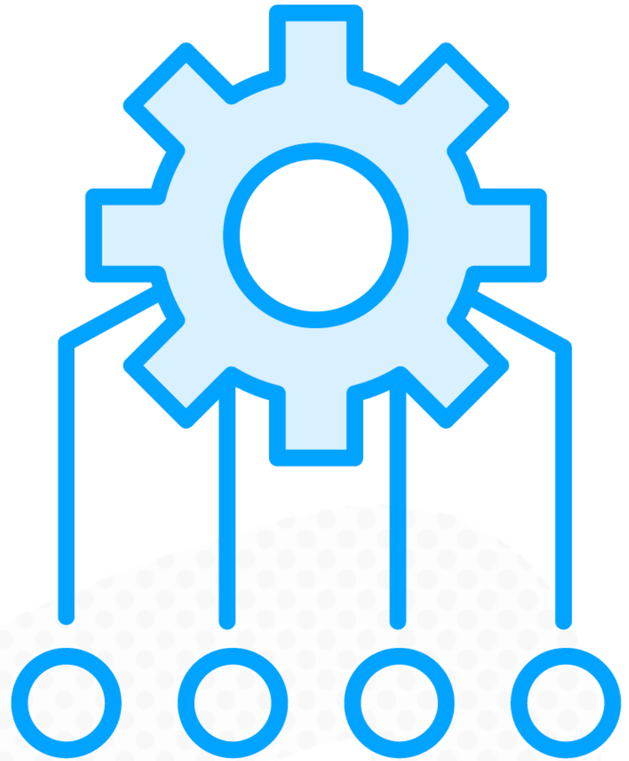
Retention policies help you to more effectively manage the information in your organization. Use retention policies to keep data that's needed to comply with your organization's internal policies, industry regulations, or legal needs, and to delete data that's considered a liability, that you're no longer required to keep, or has no legal or business value.

https://learn.microsoft.com/en-us/microsoftteams/retention-policies

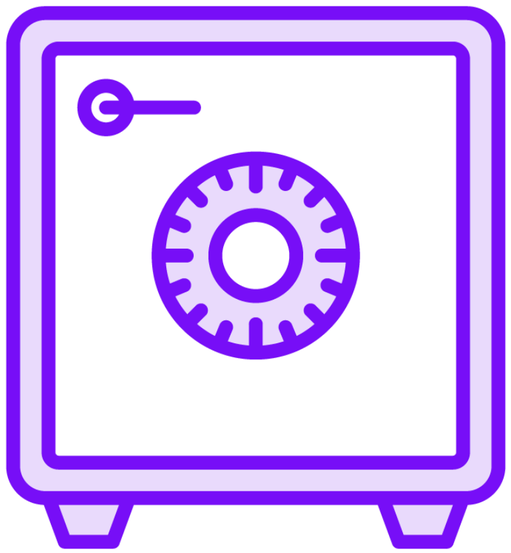
Retention in Microsoft 365

Retention in Microsoft 365 works with:

- SharePoint Online
- OneDrive for Business
- Microsoft Teams
- Microsoft 365 Groups



Retention Actions: Retain Data



Ensure data is retained for a specified period of time

- Regardless of what happens in the user app

Data is available for eDiscovery

You can decide what to do with the data after the specified period

- Do nothing
- Delete the data

Retention Actions: Delete Data

Retention policies can be used to delete data after a certain period of time

- Permanently deleted from all storage locations on the service

Retention Actions and Microsoft Teams Example

Retain Teams chats and/or channel messages for a specified duration and then do nothing

Retain Teams chats and/or channel messages for a specified duration and then delete the data

Delete Teams chats and/or channel messages after a specified duration

Retention Policies vs. Retention Labels

Retention Policies	VS	Retention Labels
Retention policies are used to assign the same retention settings to content at a site level or mailbox level		Retention labels are used to assign retention settings at an item level, such as a folder, document, or email
A single policy can be applied to multiple locations, or to specific locations or users		An email or document can have only a single retention label assigned to it at a time
Items inherit the retention settings from their container specified in the retention policy		Retention settings from retention labels travel with the content if it's moved to a different location

View all details: https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden#compare-capabilities-for-retention-policies-and-retention-labels

Scenario 1

If all documents in a SharePoint site should be kept for five years, it's more efficient to do so with a retention policy than apply the same retention label to all documents in that site

https://learn.microsoft.com/en-us/purview/retention

Scenario 2

If some documents in a SharePoint site should be kept for five years and others for 10 years, you'd need to apply a policy to the SharePoint site with a retention period of five years. You'd then apply a retention label to the individual items with a retention setting of 10 years.

https://learn.microsoft.com/en-us/purview/retention

You need to use retention label policies to make them available

Retention label policies configure locations that labels are available

A label can exist in more than one policy

You can create auto-apply retention label policies

- Automatically apply when a condition is met

Image Source: https://learn.microsoft.com/en-us/purview/retention

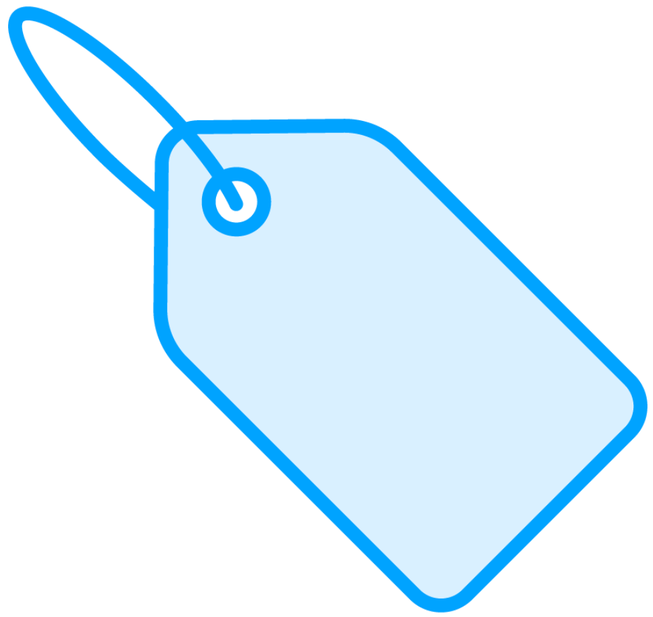
Records Management

Records Management

Records management (RM) is the supervision and administration of digital or paper records, regardless of format. Records management activities include the creation, receipt, maintenance, use and disposal of records. Documentation may exist in contracts, memos, paper files, electronic files, reports, emails, videos, instant message logs or database records.

https://searchcompliance.techtarget.com/definition/records-management

Microsoft Purview Records Management



Microsoft Purview Records Management leverages retention labels

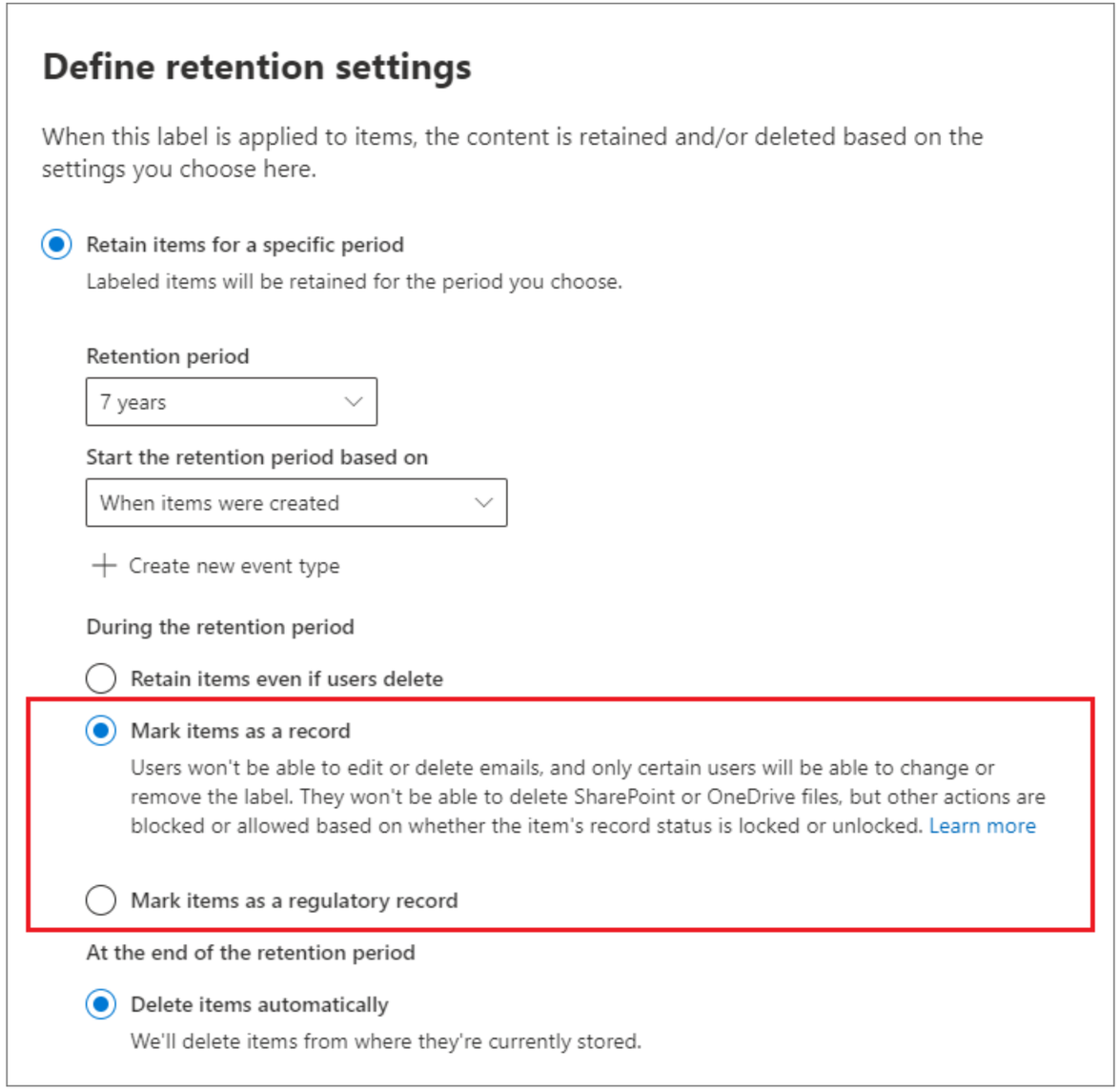
Behavior is different from a user experience/ feature point of view

Retention labels keep a copy of the content hidden from the user

- User is allowed to delete/ modify content from the user interface

Records also block actions in the user interface

Configuring Retention Labels to Declare Records



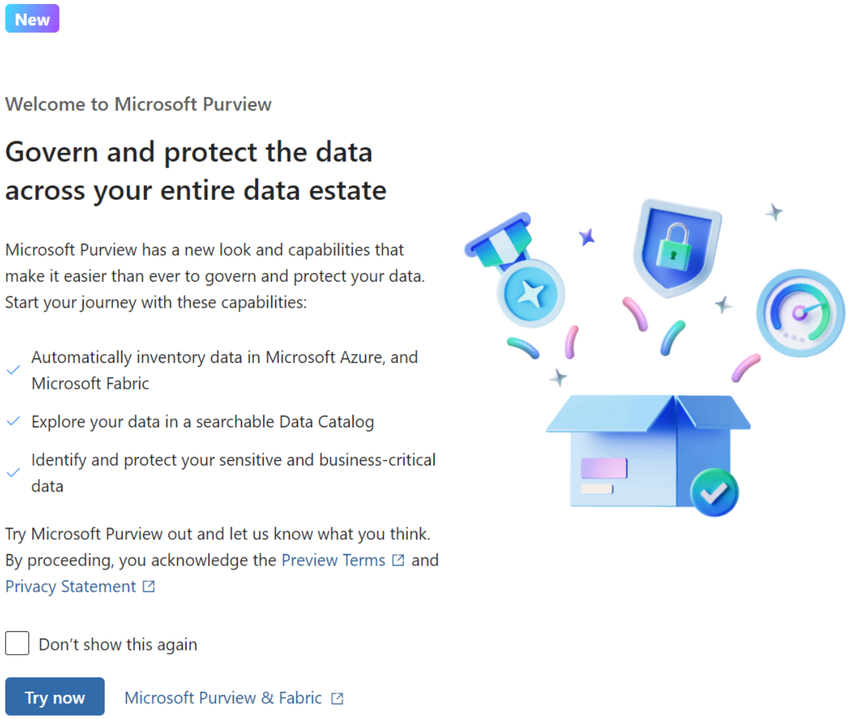
Retention Labels vs. Records

Action	Retention label	Record	Regulatory record
Edit contents	✓	✗	✗
Edit properties/ rename	✓	✓	✗
Delete	✓	✗	✗
Copy	✓	✓	✓
Move across containers	✓	✗	✗
Open/Read	✓	✓	✓
Change label	✓	✓	✗
Remove label	✓	✓	✗

The most important difference for a regulatory record is that after it is applied to content, nobody, not even a global administrator, can remove the label

Microsoft Purview Unified Data Governance

Microsoft Purview Unified Data Governance



Many organization have data outside of Microsoft 365

- SQL Servers
- Blob Storage
- Amazon S3
- Etc.

Microsoft Purview unified data governance enables you to inventory, identify, and protect your business-critical data wherever it is

Data Map

Automates data discovery across all registered sources

Classify data using built-in and custom classifiers

Label sensitive data across SQL Server, Azure, Microsoft 365

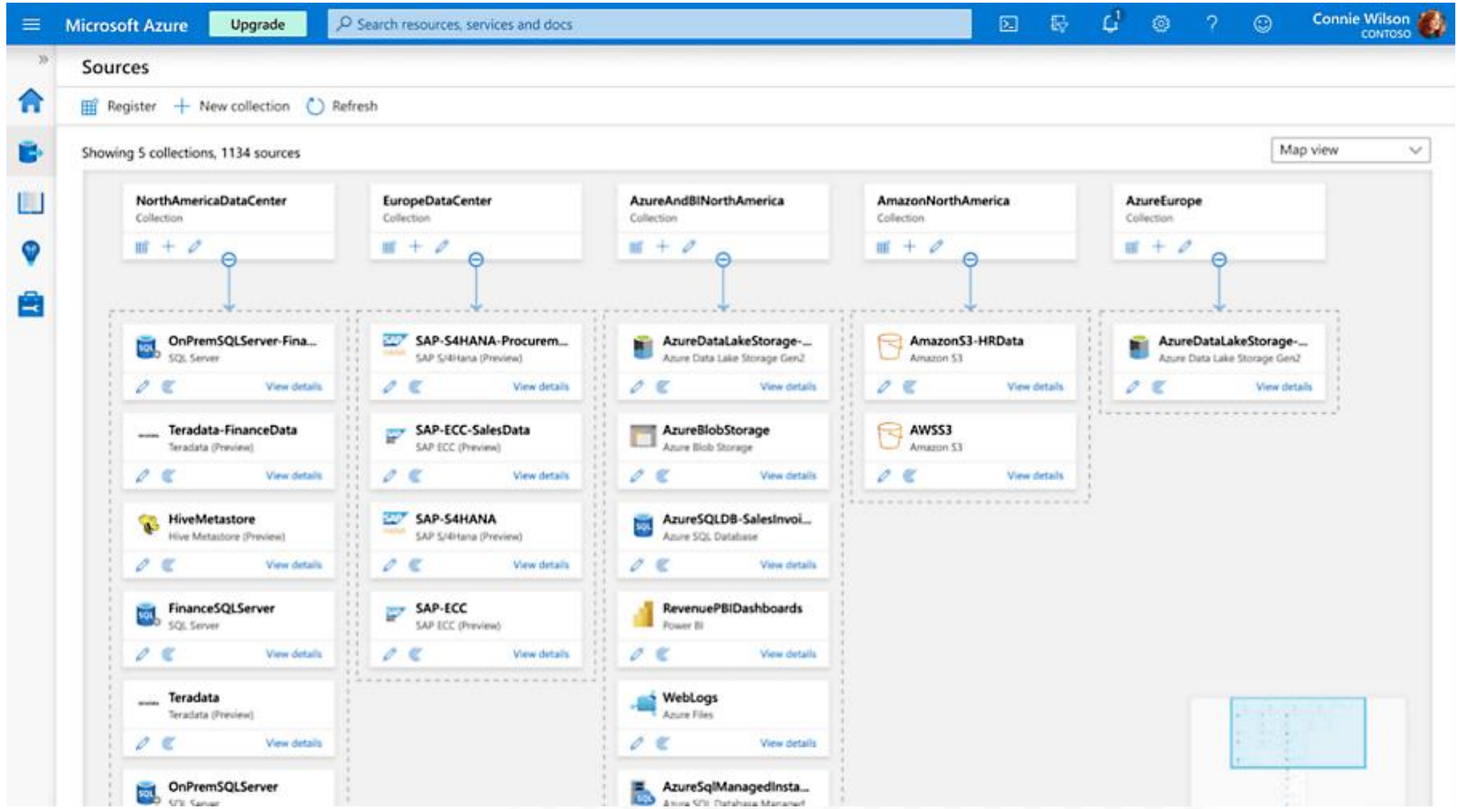


Image Source: https://azure.microsoft.com/products/purview

Data Catalog

Make data easily discoverable

Create an enterprise grade business glossary

Understand origin of your data with data lineage visualisation

Provide data scientists with data they need for BI, AI, and machine learning

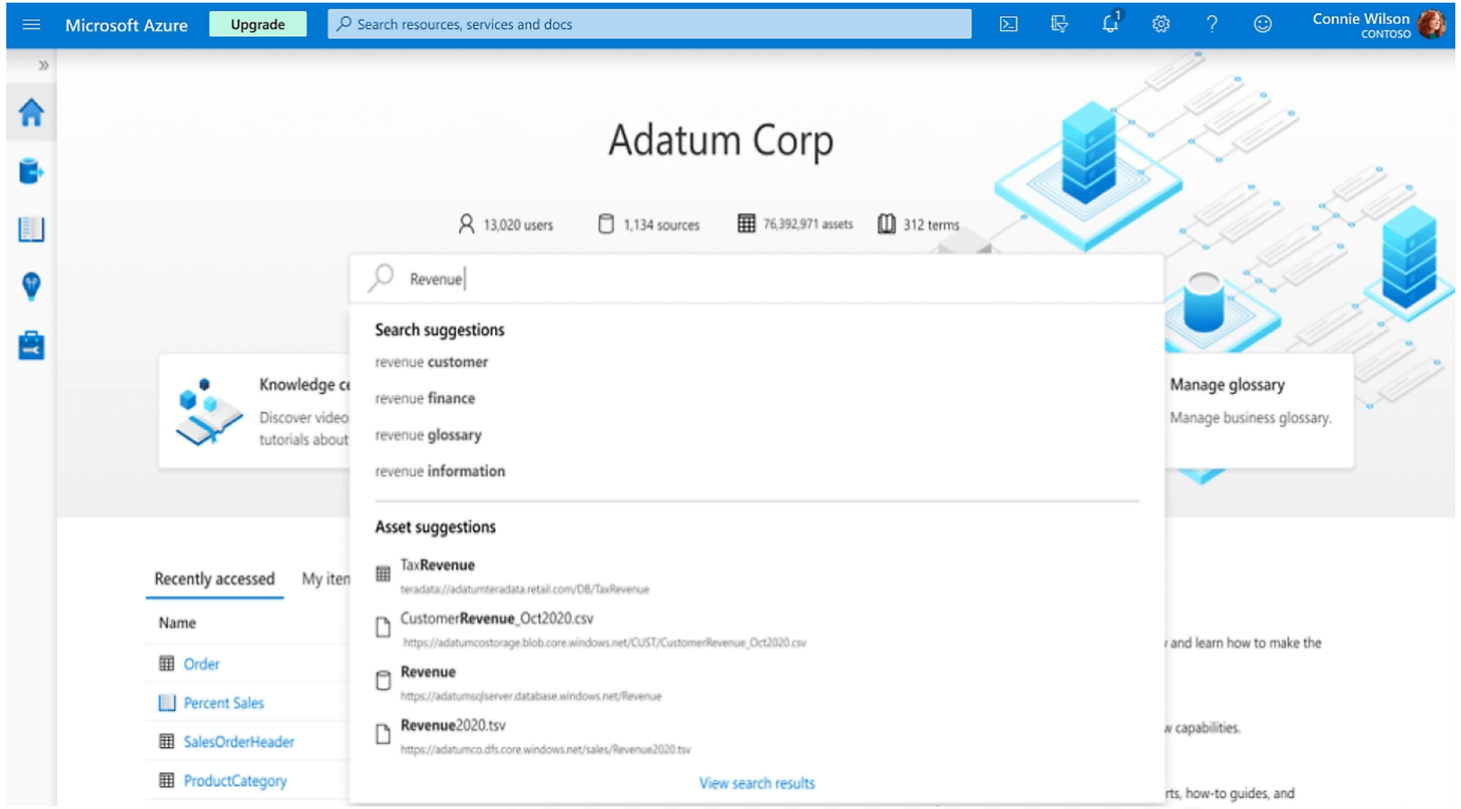


Image Source: https://azure.microsoft.com/products/purview

Data Estate Insights

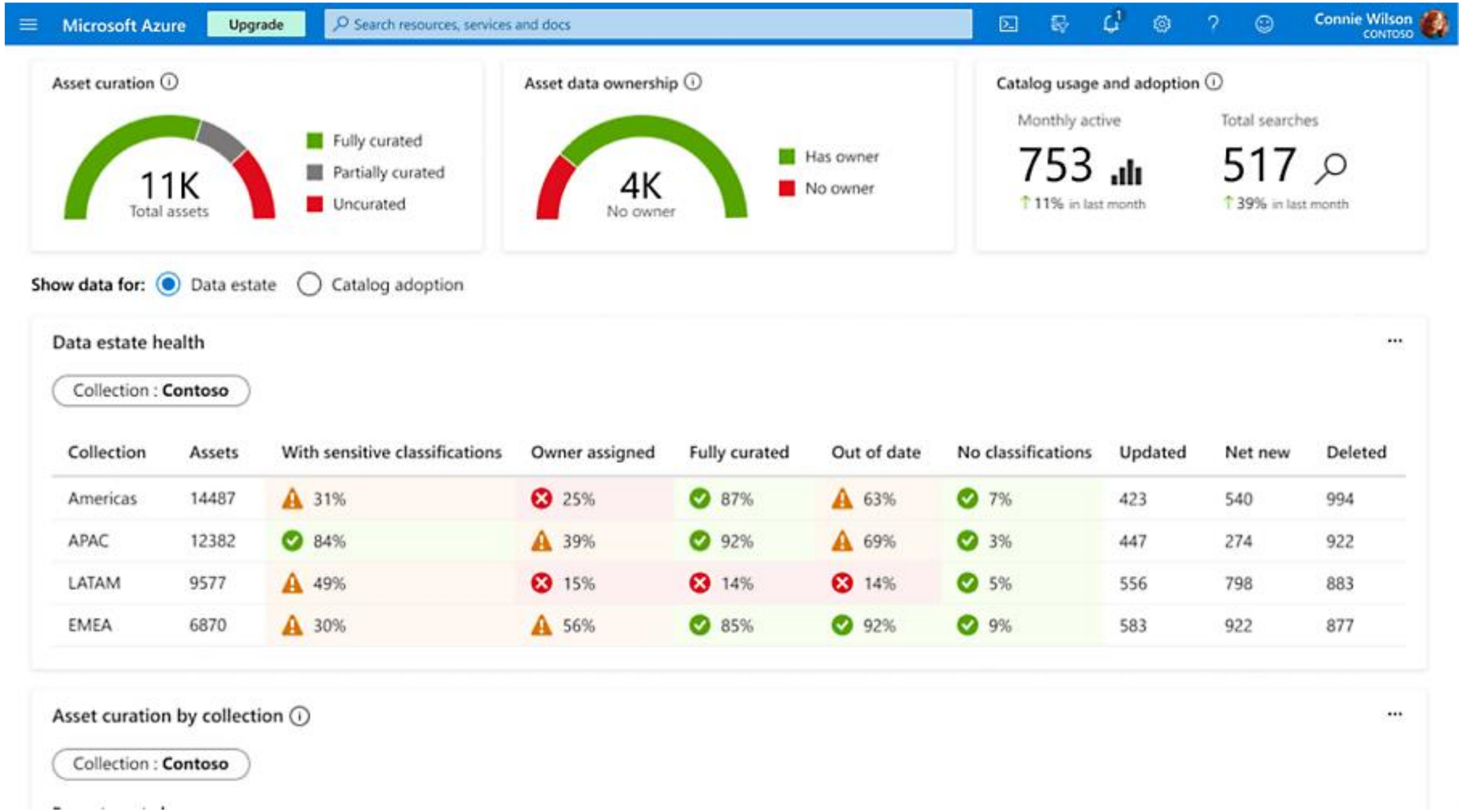


Image Source: https://azure.microsoft.com/products/purview

Data Sharing

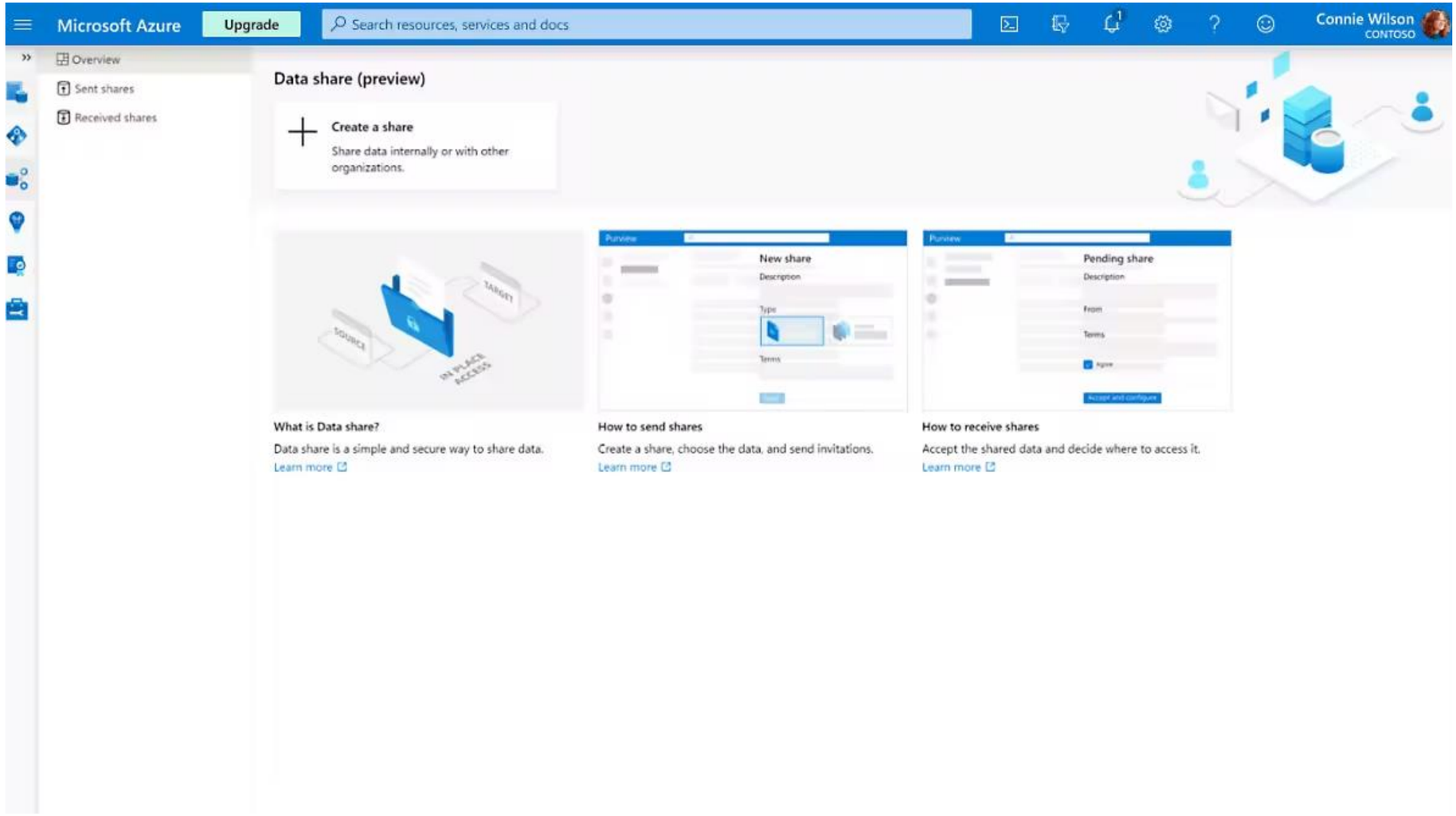


Image Source: https://azure.microsoft.com/products/purview

Data Policy

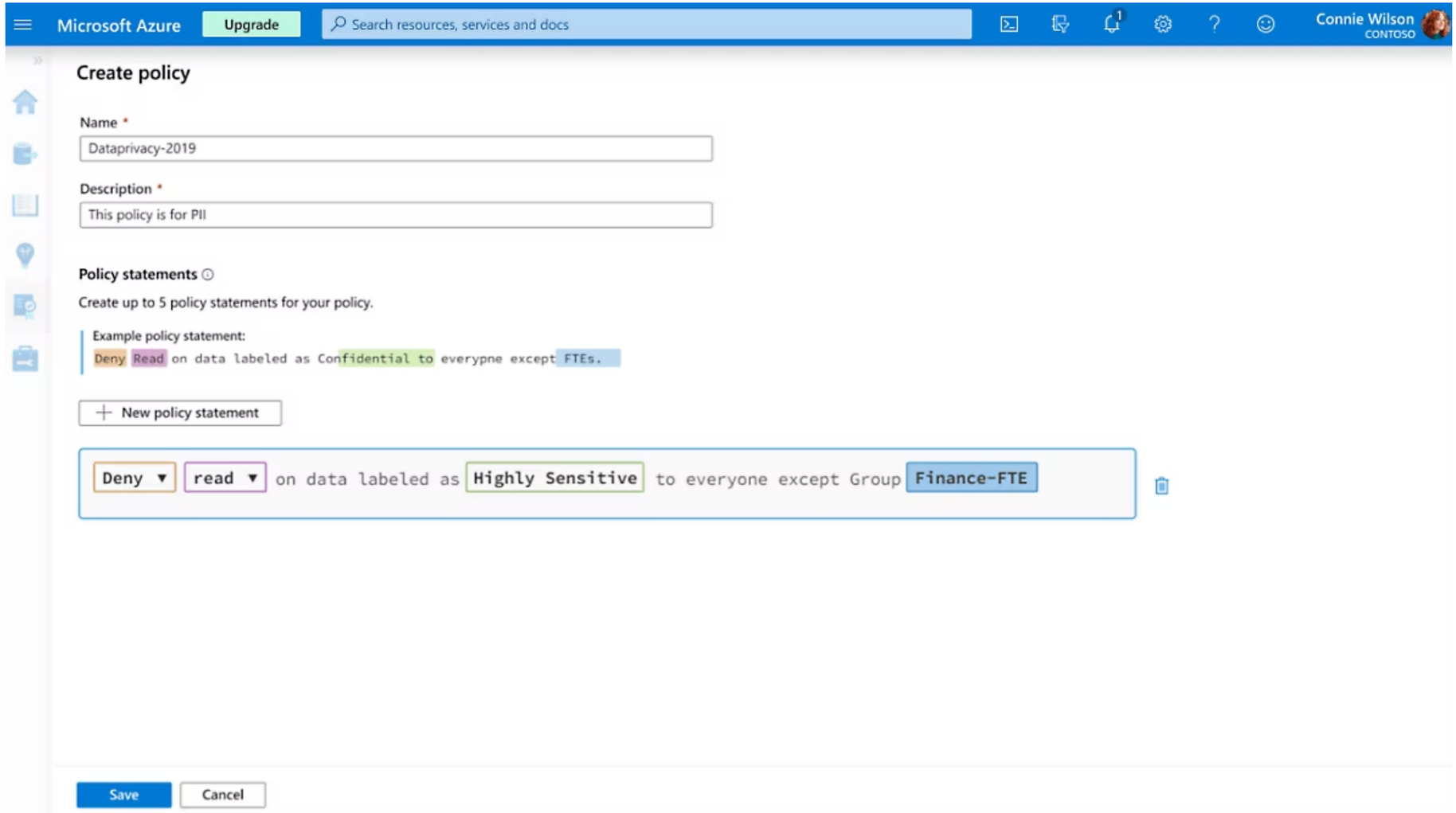


Image Source: https://azure.microsoft.com/products/purview

Module Conclusion

Introduced Microsoft Purview Information Protection and Data Lifecycle Management

Data classification and content explorer

Sensitivity labels and sensitivity policies

Data loss prevention

Retention labels and retention policies

Records management

Microsoft Purview unified data governance

Up Next:

Protecting from Insider Risk in Microsoft 365