

# Information Protection and Governance in Microsoft 365



**Vlad Catrinescu**

Microsoft MVP | Independent Consultant

@vladcatrinescu | [VladTalksTech.com](http://VladTalksTech.com) | [YouTube.com/@VladTalksTech](https://YouTube.com/@VladTalksTech)

## Overview



**Microsoft Purview Information Protection**

**Microsoft Purview Data Lifecycle Management**

**Data classification and content explorer**

**Sensitivity labels and sensitivity policies**

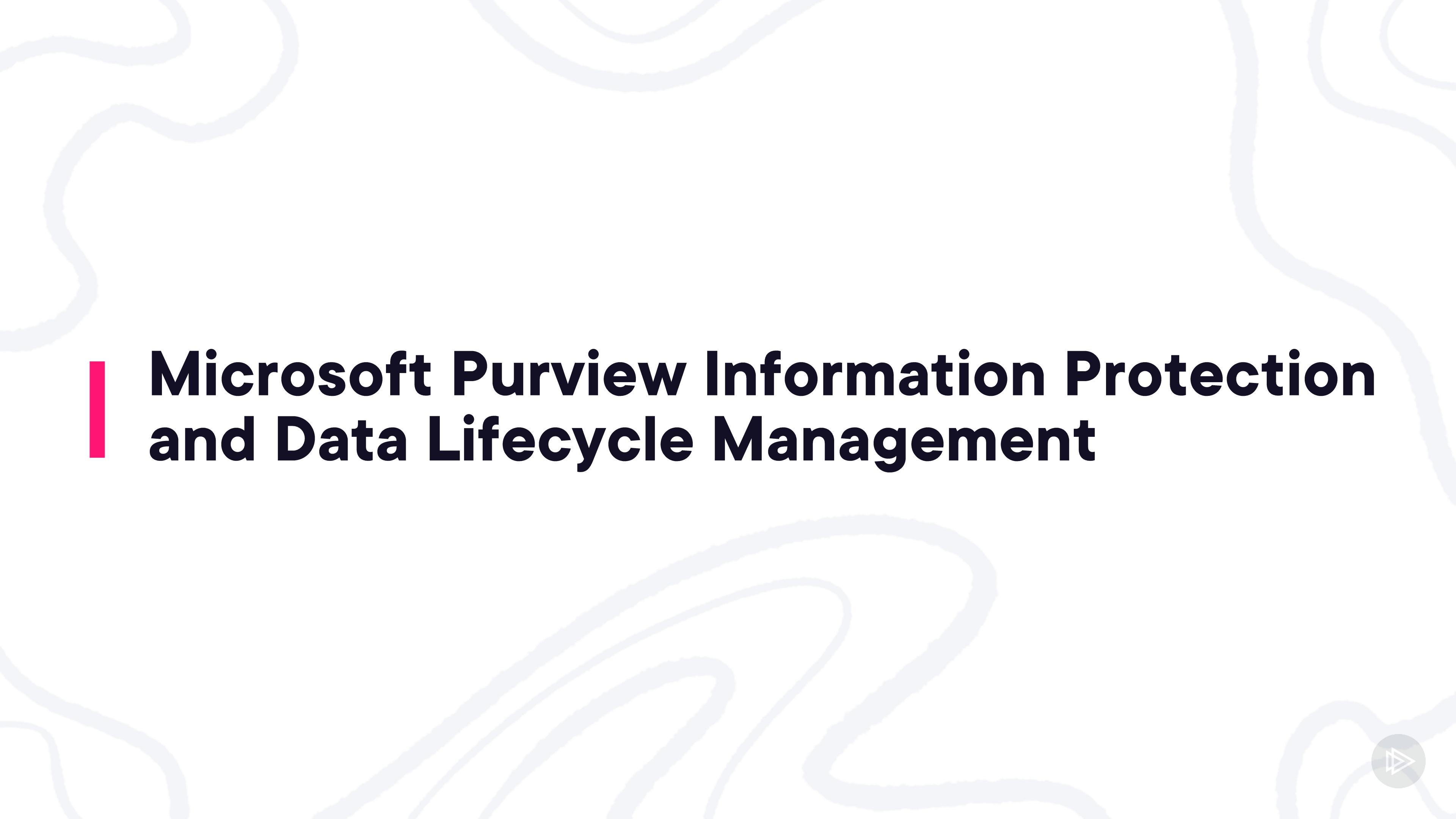
**Data loss prevention**

**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.**



# Microsoft Purview Information Protection

## Know Your Data

Understand your data landscape and identify important data across your hybrid environment

## Protect Your Data

Apply flexible protection actions that include encryption, access restrictions, and visual markings

## Prevent Data Loss

Detect risky behavior and prevent accidental oversharing of sensitive information

## Govern Your Data

Automatically retain, delete, and store data and records in a compliant manner

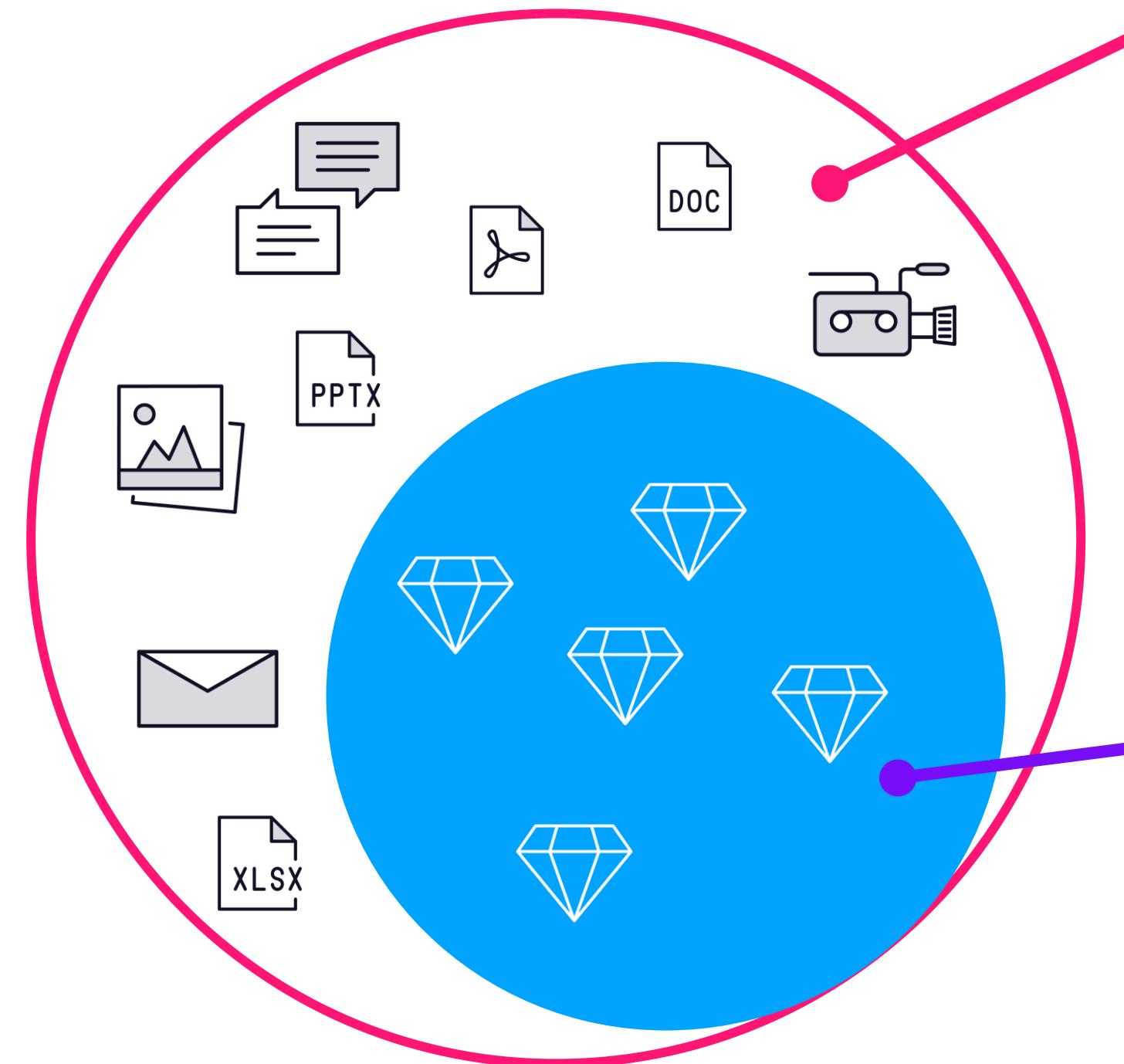


# **Microsoft Purview Data Lifecycle Management**

**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.**



# Govern Your Data



## Microsoft Purview Data Lifecycle Management

Manage 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

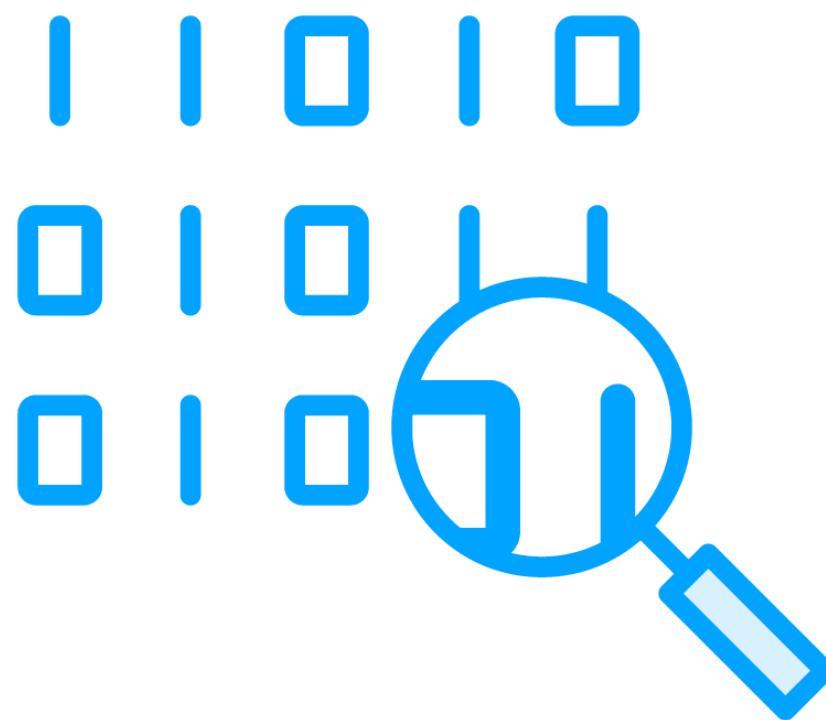
Retention policies  
Records management



# 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](#)

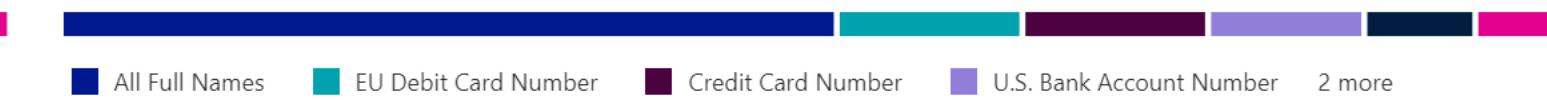
Top trainable classifiers

### Trainable classifiers used most in your content



Top sensitive info types

### Sensitive info types used most in your content



[View all trainable classifiers](#)

[View all sensitive info types](#)

Top sensitivity labels applied to content



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.

[View all applied sensitivity labels](#)

[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

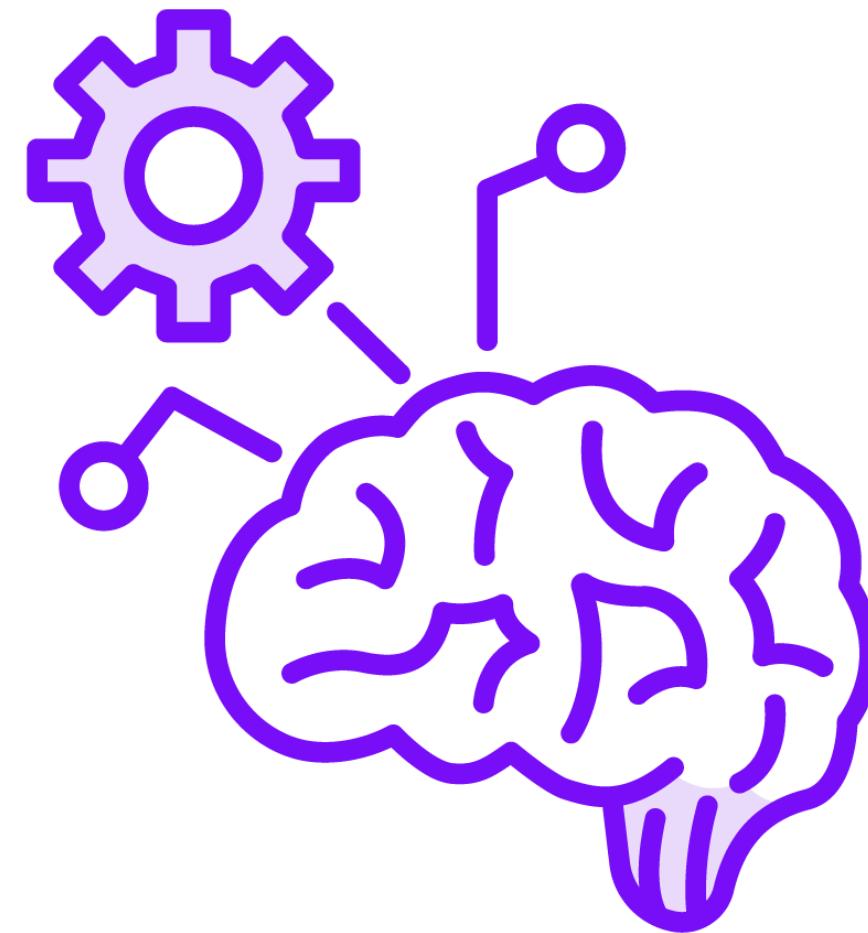
Trainable Classifiers

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

The screenshot shows the Microsoft Purview interface for managing classifiers. The top navigation bar includes the Contoso Electronics logo, the Microsoft Purview title, and various global navigation icons. The main page title is "Classifiers". Below it, there are two tabs: "Trainable classifiers" (which is selected) and "Sensitive info types". A descriptive text block explains the purpose of classifiers and provides a "Learn more" link. On the left, a vertical sidebar contains icons for Home, Recent, Compliance, and other Microsoft services. The main content area displays a table of classifiers with the following columns: Name, Accuracy, Status, Type, Language, Created by, Last modified, and Last modified by. A filter section at the top of the table allows users to refine results by Language, Type, Name, and Status. The table lists five classifiers under the "Published" category:

Name	Accuracy	Status	Type	Language	Created by	Last modified	Last modified by
Actuary reports	-	Ready to use	Built-In	English	Microsoft	10/23/2023	Microsoft
Agreements	-	Ready to use	Built-In	English	Microsoft	11/6/2023	Microsoft
Asset Management	-	Ready to use	Built-In	English	Microsoft	9/20/2023	Microsoft
Bank statement	-	Ready to use	Built-In	English	Microsoft	9/20/2023	Microsoft
Budget	-	Ready to use	Built-In	English	Microsoft	10/10/2023	Microsoft

# 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

The screenshot shows the Microsoft Purview interface for managing classifiers. The top navigation bar includes the organization name "Contoso Electronics", the service name "Microsoft Purview", and various global icons. On the left, a vertical sidebar contains a series of icons representing different classification categories. The main content area is titled "Classifiers" and has two tabs: "Trainable classifiers" and "Sensitive info types", with the latter being active. A descriptive text explains that sensitive info types are available for security and compliance policies, including custom types. Below this, there are buttons for "Create sensitive info type", "Create Fingerprint based SIT", and "Refresh". A search bar indicates there are 315 items and provides a search function. The main table lists nine sensitive info types, each with a checkbox, name, type, and publisher:

	Name ↑	Type	Publisher
<input type="checkbox"/>	ABA Routing Number	Entity	Microsoft Corporation
<input type="checkbox"/>	ASP.NET Machine Key	Credential	Microsoft Corporation
<input type="checkbox"/>	All Credential Types	BundledCredential	Microsoft Corporation
<input type="checkbox"/>	All Full Names	BundledEntity	Microsoft Corporation
<input type="checkbox"/>	All Medical Terms And Conditions	BundledEntity	Microsoft Corporation
<input type="checkbox"/>	All Physical Addresses	BundledEntity	Microsoft Corporation
<input type="checkbox"/>	Amazon S3 Client Secret Access Key	Credential	Microsoft Corporation

# 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

Contoso Electronics Microsoft Purview 

## Content explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

Filter on labels, info types, or categories

All locations > SharePoint > <https://m365x26304976.sharepoint.com>

The actual number of items in this site/folder might be different from the calculated number that's displayed on the left

Sensitive info types	Count	Actions	Sensitive info type	Trainable classifiers
All Full Names	15	<a href="#">Export</a>		
U.S. Social Security Number (SSN)	8	<a href="#">Name</a>		
EU Debit Card Number	2	<a href="#">Contoso Purchasing Permissions.docx</a>	Credit Card ... +3 more	Finance, Threat
<b>Credit Card Number</b>	<b>2</b>	<a href="#">Contoso Purchasing Permissions.docx</a>	Credit Card ... +3 more	Finance, Threat
U.S. Bank Account Number	2			

Sensitive info types

Trainable Classifiers

Export

Name

Contoso Purchasing Permissions.docx

Contoso Purchasing Permissions.docx

Credit Card ... +3 more

Finance, Threat

Credit Card ... +3 more

Finance, Threat

Search

Threat

Targeted Harassment

# 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

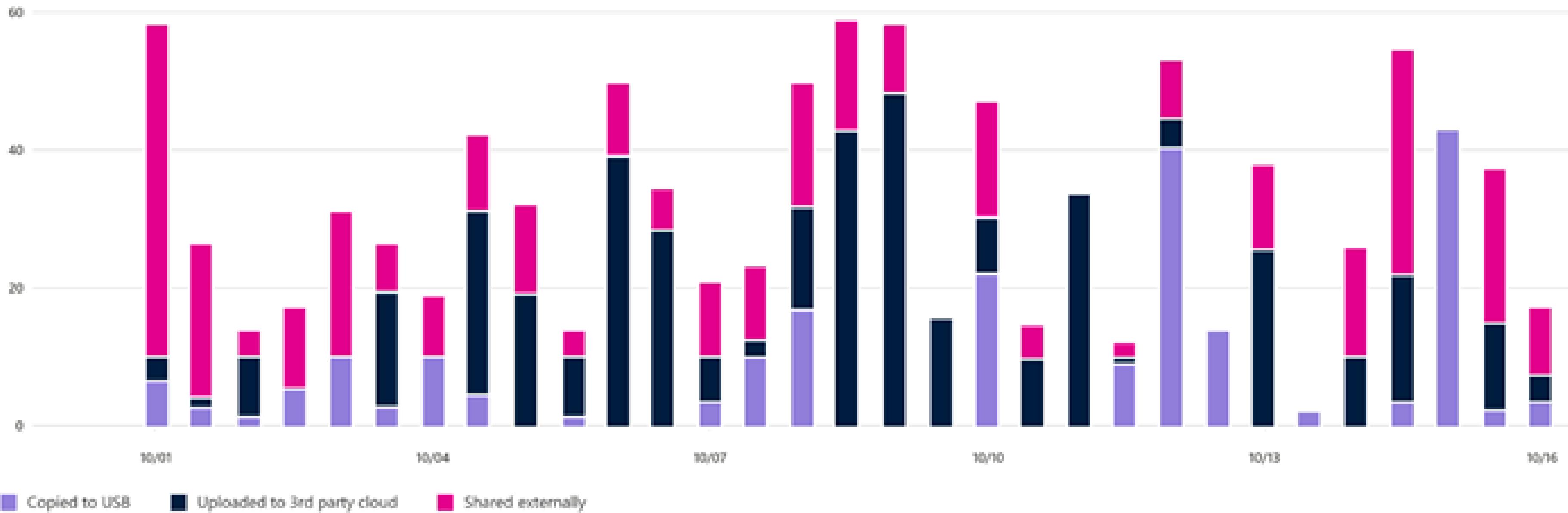
Filter

Date range: 10/01/2019 – 10/19/2019 X

Activities: Copied to USB, Uploaded to 3rd party cloud, +1 X

Locations: Any ▼

File types: JPG, PNG



# 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**



# 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

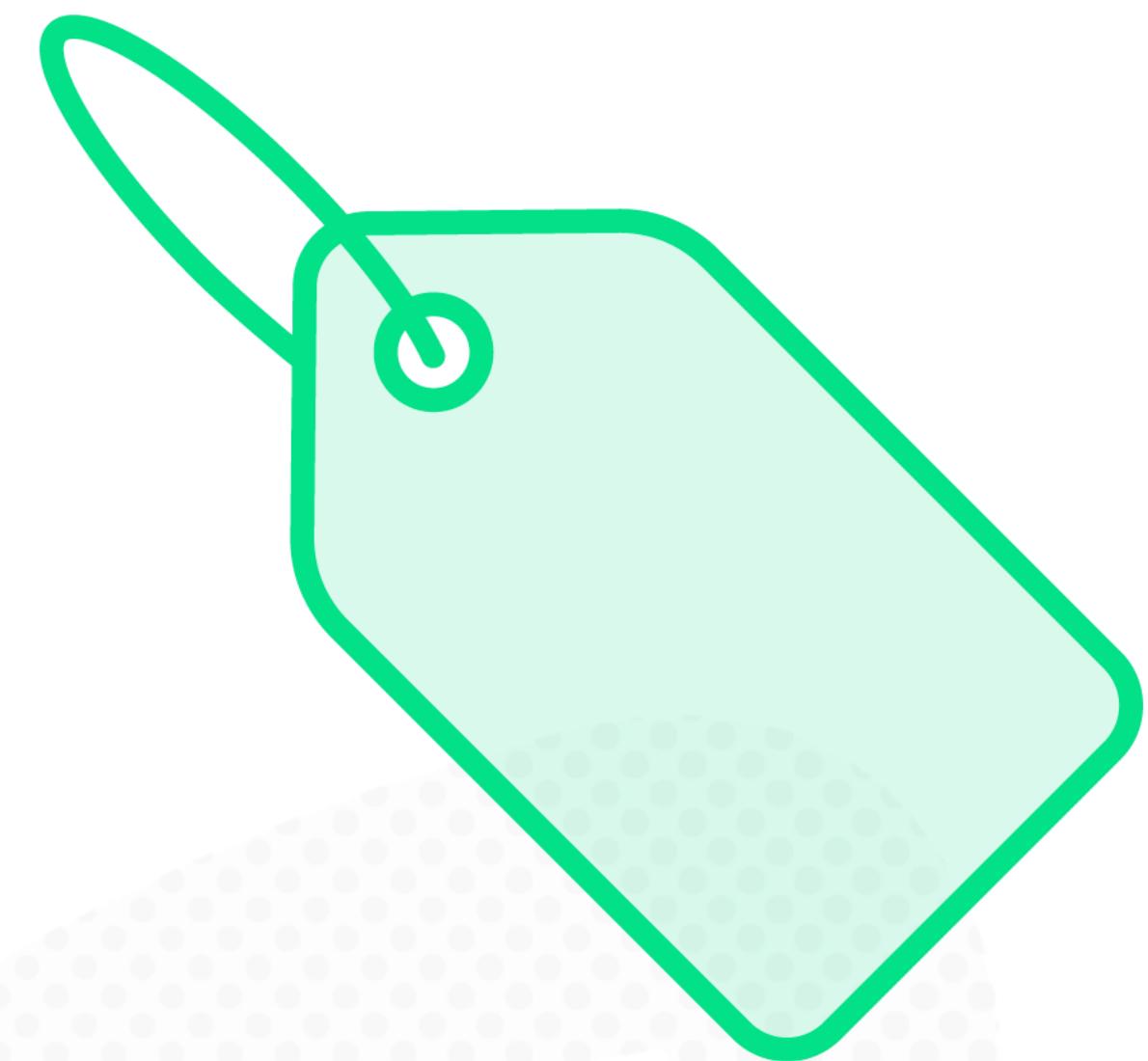
- SharePoint sites

**Using the label, you can configure**

- Privacy (public or private)

- External user access

- Access from unmanaged device



# Sensitivity Labels

GLOBOMANTICS Microsoft Purview   

## Edit sensitivity label

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

(i) All content marking will be applied to documents but only headers and footers will be applied to email messages.

Content marking

Add a watermark 

Add a header 

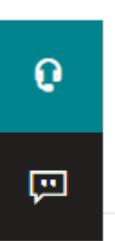
Add a footer 

Groups & sites

Schematized data assets (preview)

Finish

Back Next Cancel



# Sensitivity Label: Document without Label

Personal employees information

Contoso HR

Project Obsidian

Proseware Merger

Options ▾

Personal employee information

Employee	SSN
Marina Mcphee	600-95-3027
Gita Herbert	377-96-4498
Winford Watson	091-54-5179
Edmund Boyd	503-28-8364

Page 1 of 1 17 words English (US) Text Predictions: On Editor Suggestions: Showing

120% Fit Give Feedback to Microsoft

# Sensitivity Label: Document with Label

The screenshot shows a Microsoft Word document titled "Personal employees information". The ribbon menu is visible at the top, showing tabs like File, Home, Insert, Layout, References, Review, View, and Help. The Home tab is selected. The ribbon also includes sections for Comments, Catch up, Editing, and Share.

In the center of the document, there is a red watermark-like text that reads "Contoso HR" and "Classified as Highly Confidential".

The main content of the document is a table titled "Personal employee information". The table has two columns: "Employee" and "SSN". The data in the table is as follows:

Employee	SSN
Marina Mcphee	600-95-3027
Gita Herbert	377-96-4498
Winford Watson	091-54-5179
Edmund Boyd	503-28-8364

At the bottom of the screen, there is a circular icon with a play symbol (▶) and some status text: "Page 1 of 1 17 words English (U.S.) Text Predictions: On Editor Suggestions: Showing Proseware Merger".

# Sensitivity Labels: Teams Creation Experience

What kind of team will this be?

X

Sensitivity label

None

Privacy



**Private**

People need permission to join



**Public**

Anyone in your org can join



**Org-wide**

Everyone in your organization automatically joins

What kind of team will this be?

X

Sensitivity label

Project Obsidian

Teams with this sensitivity must be private.

Privacy



**Private**

People need permission to join



**Public**

Anyone in your org can join

(i)



**Org-wide**

Everyone in your organization automatically joins

(i)



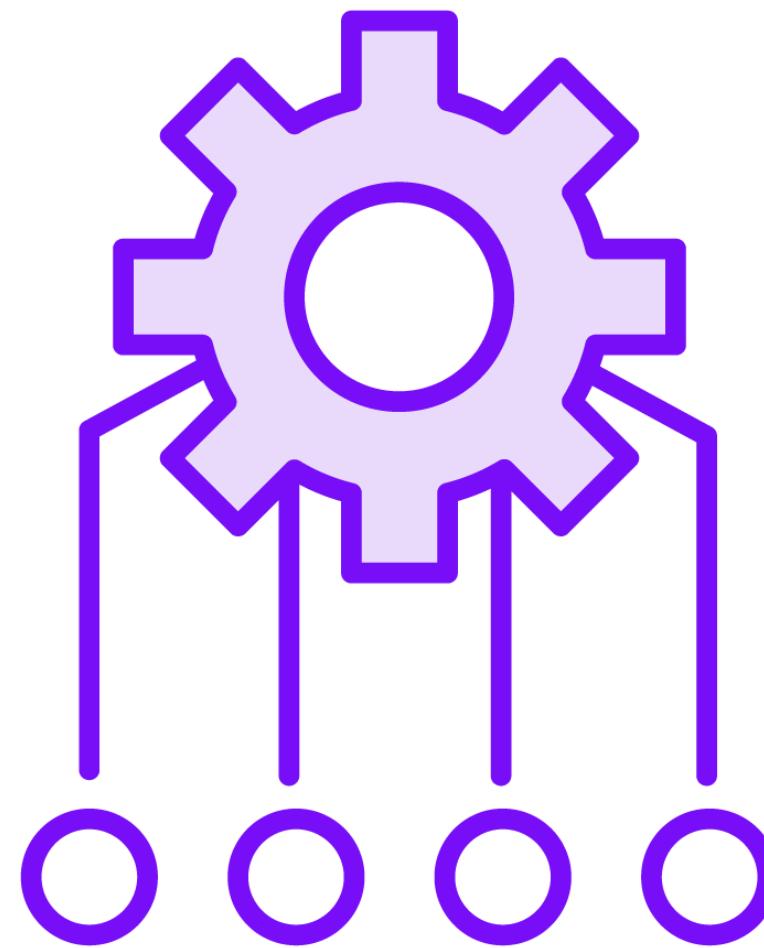
# Sensitivity Labels: Teams Display Experience

The screenshot shows a SharePoint library interface with the following elements:

- Header:** Contoso Electronics SharePoint. A search bar says "Search this library". A user icon shows "MA".
- Title:** Confidential Merger Project
- Permissions:** Private group | Project Obsidian (highlighted with a red box), Not following, 1 member.
- Toolbar:** Home, + New, Upload, Edit in grid view, Share, All Documents, Filter, Help.
- Breadcrumb:** Documents > General
- Table Headers:** Name, Modified, Modified By, + Add column.
- Content:** A large folder icon with the text "This folder is empty".
- Left Navigation:** Home, Conversations, Documents, Shared with us (selected), Notebook, Pages, Site contents, Recycle bin, Edit, Return to classic SharePoint.



# Sensitivity Labels Policies

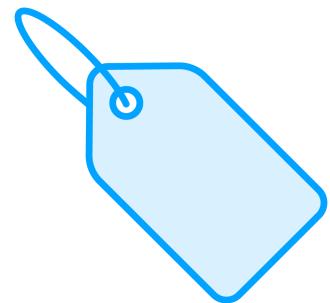


**Sensitivity labels need to published using policies**

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



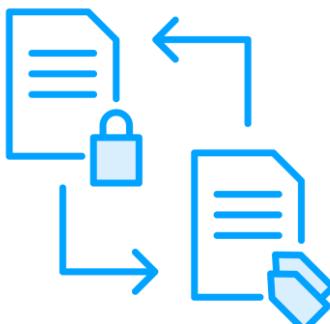
# Other Label Policy Settings



**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

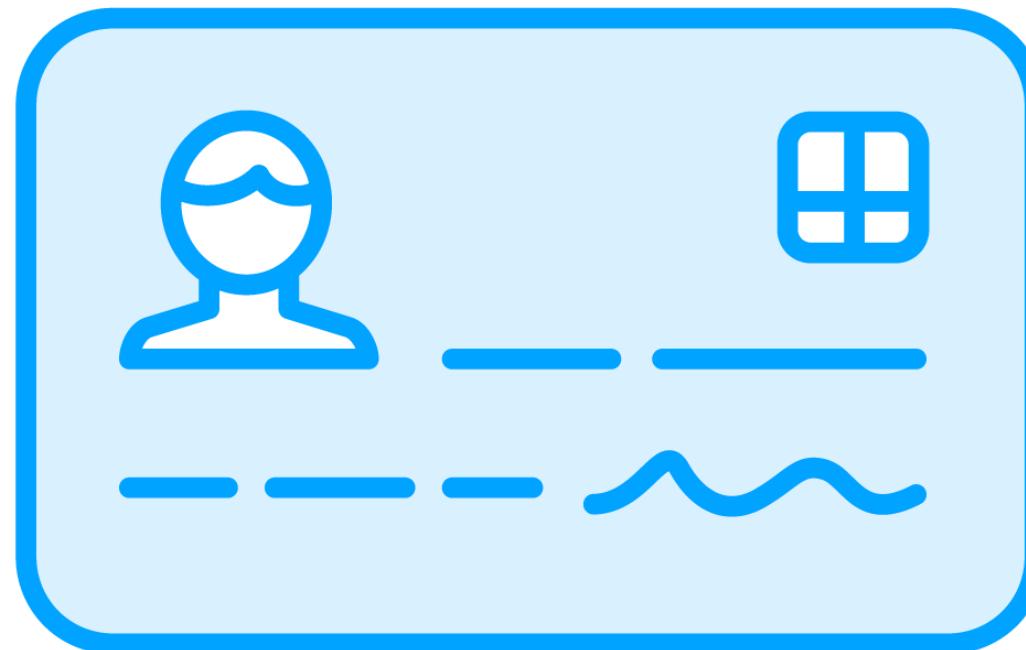




# Data Loss Prevention



# 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

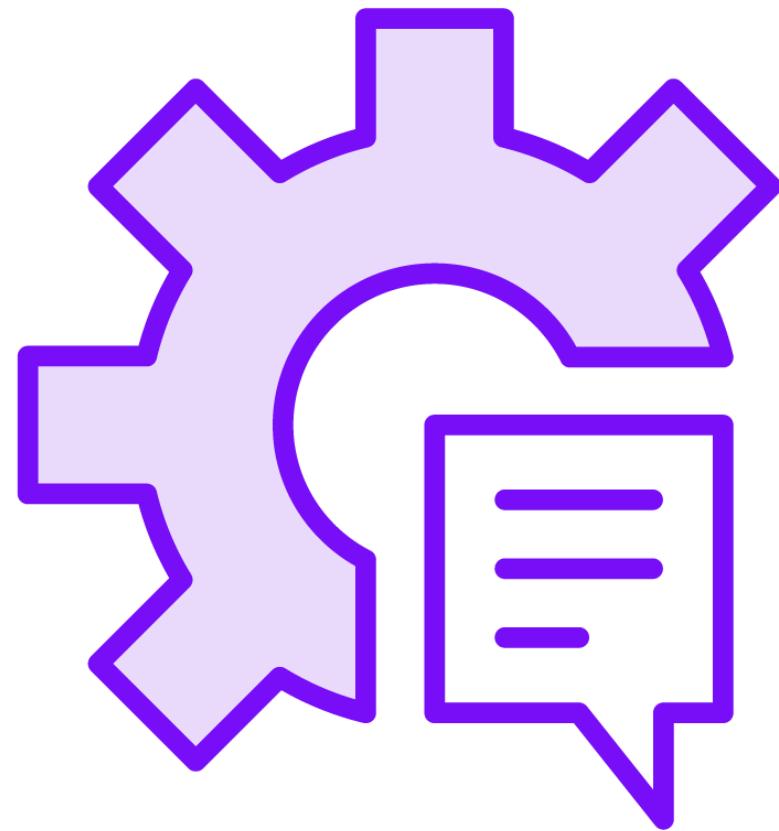
**Also works with non-cloud services**

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

Contoso Electronics Microsoft Purview ⚙️ 🌐 ? MC

Data loss prevention > Create policy

**Template or custom policy**

- Name
- Admin units
- Locations
- Policy settings
- Policy mode
- Finish

Search for specific templates All countries or regions

Categories	Regulations	U.S. Financial Data
Financial	Australia Financial Data	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.
Medical and health	Canada Financial Data	
Privacy	France Financial Data	
Custom	Germany Financial Data	
	Israel Financial Data	
	Japan Financial Data	
	PCI Data Security Standard (PCI DSS)	
	Saudi Arabia - Anti-Cyber Crime Law	
	Saudi Arabia Financial Data	

**Next** **Cancel** 

# DLP Policy Locations

Contoso Electronics Microsoft Purview

Data loss prevention > Create policy

View role groups

Template or custom policy

Name

Admin units

**Locations**

Policy settings

Policy mode

Finish

(i) 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](#)

Location	Scope	
<input checked="" type="checkbox"/> Exchange email	All groups	<a href="#">Edit</a>
<input checked="" type="checkbox"/> SharePoint sites	All sites	<a href="#">Edit</a>
<input checked="" type="checkbox"/> OneDrive accounts	All users & groups	<a href="#">Edit</a>
<input checked="" type="checkbox"/> Teams chat and channel messages	All users & groups	<a href="#">Edit</a>
<input checked="" type="checkbox"/> Devices	All users & groups	<a href="#">Edit</a>
<input checked="" type="checkbox"/> Instances	All instances	<a href="#">Edit</a>
<input checked="" type="checkbox"/> On-premises repositories	All repositories	<a href="#">Edit</a>
<input type="checkbox"/> Power BI workspaces	Turn on location to scope	

Back Next Cancel

# Data Loss Prevention Inside Microsoft Teams

The screenshot shows a Microsoft Teams channel named "General". On the left, the "Activity" sidebar indicates an "Unread only" message from a user named "Contoso". The message content is as follows:

Your message has been blocked  
Message violates organization policy  
Contoso > General

A red warning icon is present next to the message. Below the message, a note states: "This message was blocked. What can I do? Hello Everyone, here is the customer information you requested!"

On the right, a table displays sensitive card numbers and their types:

Card number	Card type
371449635398431	American Express
376680816376961	American Express
36259600000004	Diners Club
6304000000000000	Maestro
5063516945005047	Maestro

A "see more" link is available at the bottom of the table.

At the bottom of the screen, there is a "Start a post" button.



# Data Loss Prevention Inside Microsoft Teams

The screenshot shows a Microsoft Teams channel named "General". On the left, the "Activity" sidebar indicates an "Unread only" status. A red notification bubble appears, stating "Your message has been blocked" at 2:45 PM, with the reason "Message violates organization's data loss prevention policy". The message content reads: "Hello Everyone, here is the customer information you requested!" Below the message is a table showing card numbers and their types:

Card number	Card type
371449635398431	American Express
376680816376961	American Express
36259600000004	Diners Club
6304000000000000	Maestro
5063516945005047	Maestro

A "see more" link is available to view additional cards. At the bottom of the message card is a "Reply" button.

**Start a post**



# 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

The screenshot shows the Microsoft Teams interface. On the left is the navigation bar with icons for Activity (14 notifications), Chat, Teams (1 unread), Calendar, Calls, OneDrive, and Apps. The main area shows the 'Teams' tab selected, listing 'Your teams': Mark 8 Project Team, Retail, Sales and Marketing, Digital Initiative Public ..., U.S. Sales, and Contoso. The 'Contoso' team is expanded, showing its 'General' channel. The 'General' tab is selected in the channel header, which also includes 'Posts', 'Files', and 'Notes'. A message from a user with a green profile picture is displayed, showing a crossed-out icon and the text: *This message was blocked due to organization policy.* A link to 'What's this?' is provided. Below the message is a 'Reply' button. At the bottom of the channel view is a blue 'Start a post' button. The top right corner of the screen shows a user profile picture with a green checkmark.





# 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.**



# Retention in Microsoft 365

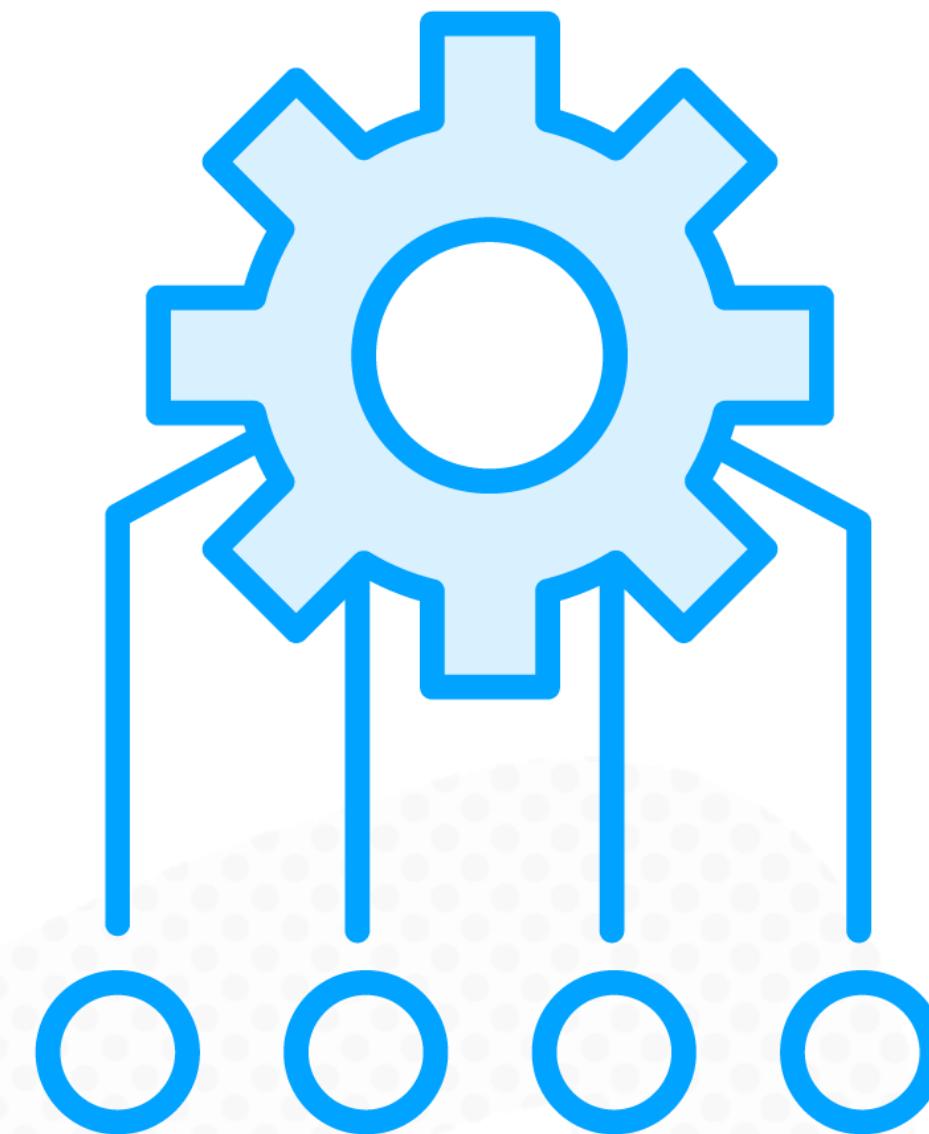
**Retention in Microsoft 365 works with:**

SharePoint Online

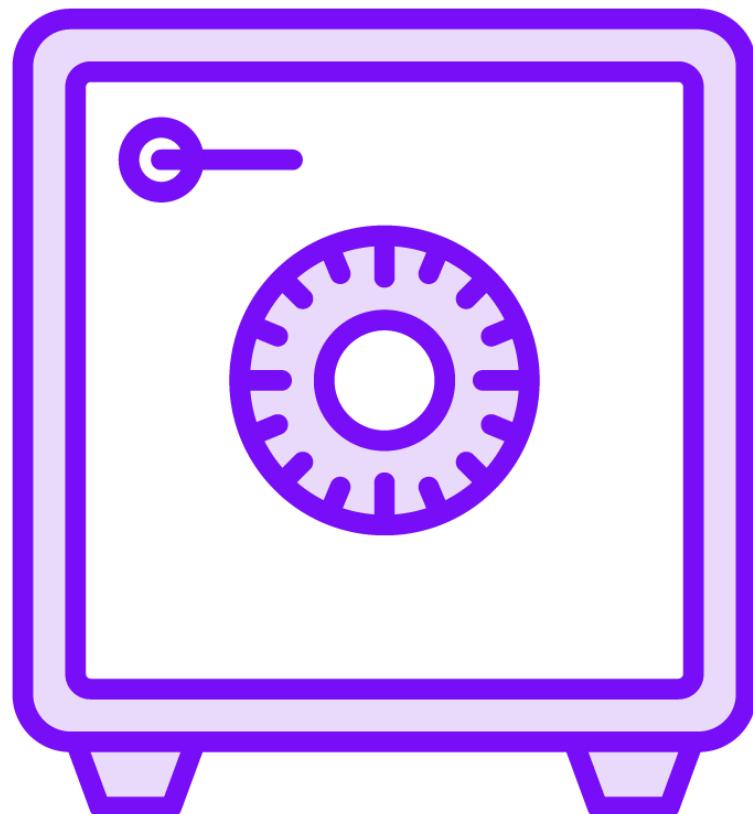
OneDrive for Business

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

DELETE



# 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

A single policy can be applied to multiple locations, or to specific locations or users

Items inherit the retention settings from their container specified in the retention policy

Retention labels are used to assign retention settings at an item level, such as a folder, document, or email

An email or document can have only a single retention label assigned to it at a time

Retention settings from retention labels travel with the content if it's moved to a different location



# 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**



# 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.



**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





# Records Management

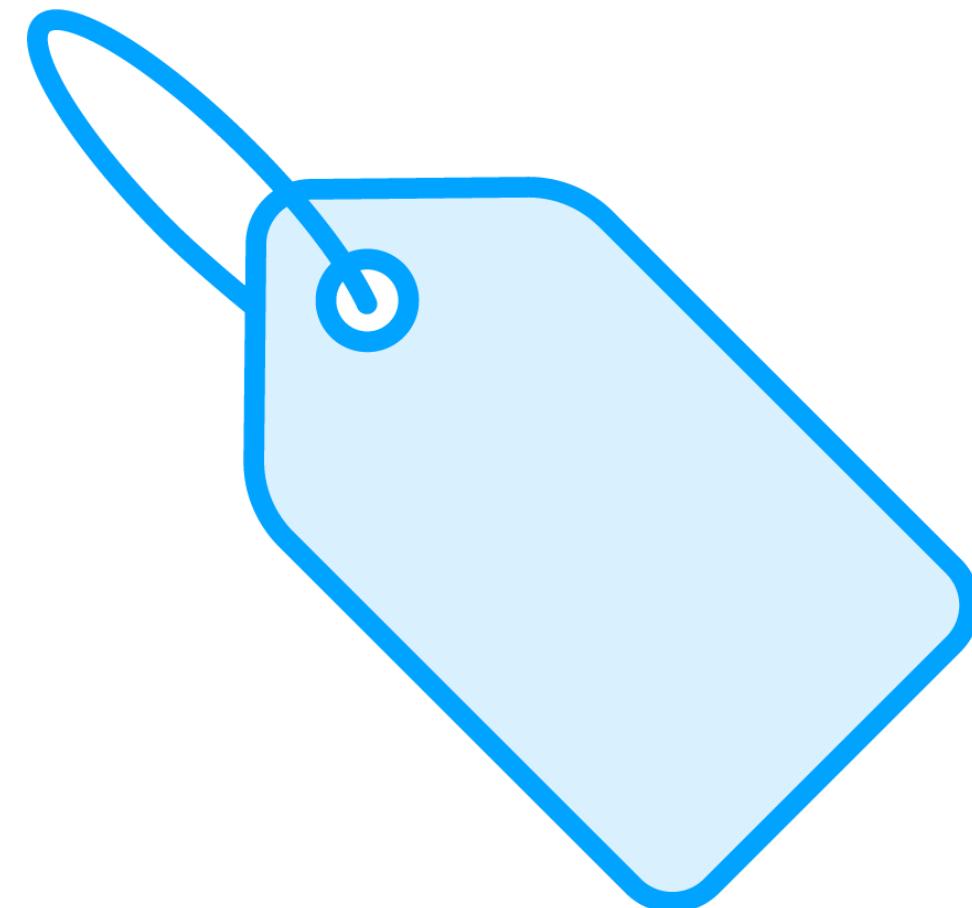


# Records Management

**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.**



# 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

## Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

Retain items for a specific period  
Labeled items will be retained for the period you choose.

Retention period

Start the retention period based on

+ Create new event type

During the retention period

Retain items even if users delete

Mark items as a record  
Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. [Learn more](#)

Mark items as a regulatory record

At the end of the retention period

Delete items automatically  
We'll delete items from where they're currently stored.



# 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

New

Welcome to Microsoft Purview

Govern and protect the data across your entire data estate

Microsoft Purview has a new look and capabilities that make it easier than ever to govern and protect your data. Start your journey with these capabilities:

- ✓ Automatically inventory data in Microsoft Azure, and Microsoft Fabric
- ✓ Explore your data in a searchable Data Catalog
- ✓ Identify and protect your sensitive and business-critical data



Try Microsoft Purview out and let us know what you think. By proceeding, you acknowledge the [Preview Terms](#) and [Privacy Statement](#)

Don't show this again

Try now

Microsoft Purview & Fabric

**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**

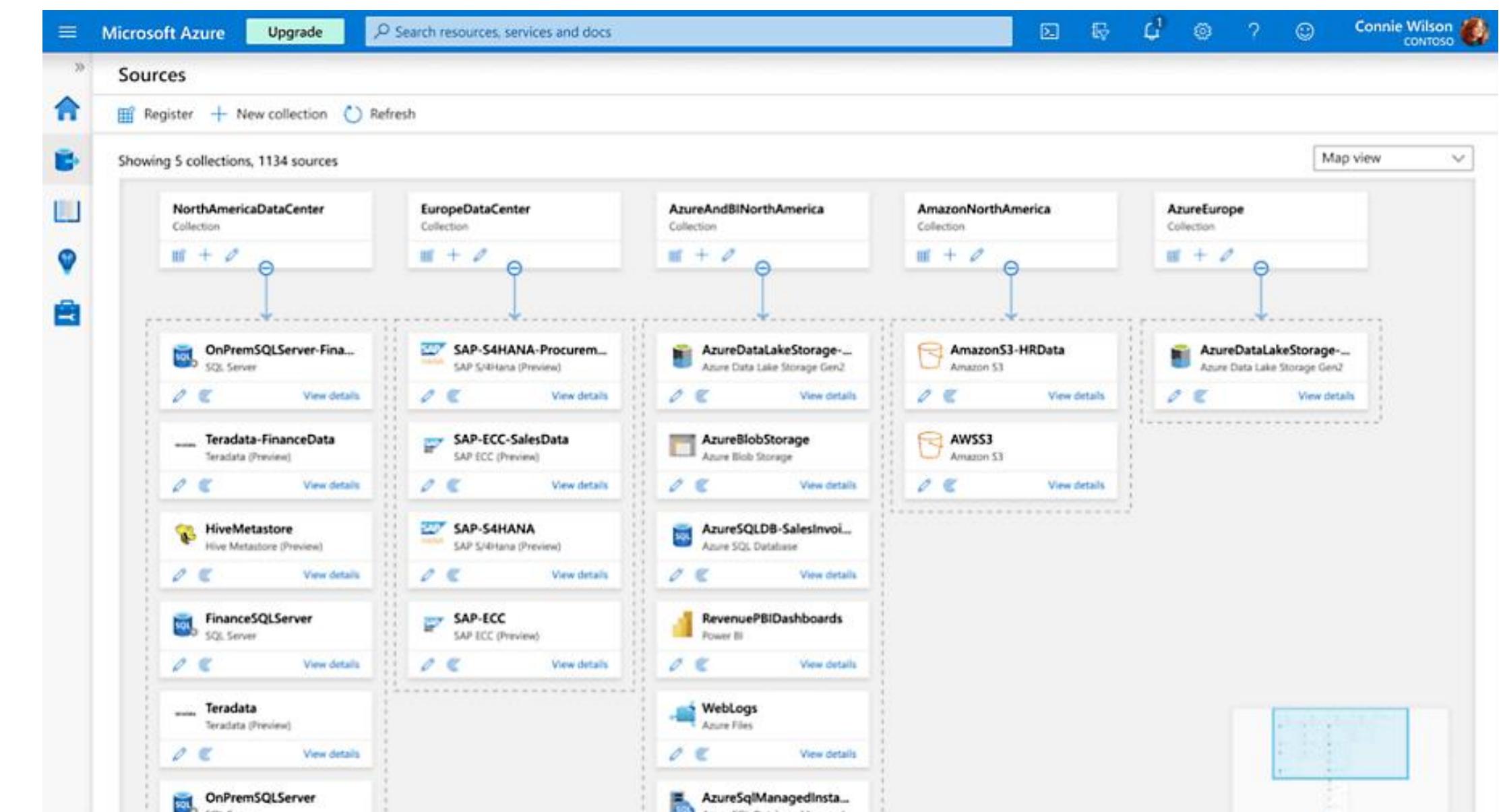


Image Source: <https://azure.microsoft.com/products/purview>



# 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

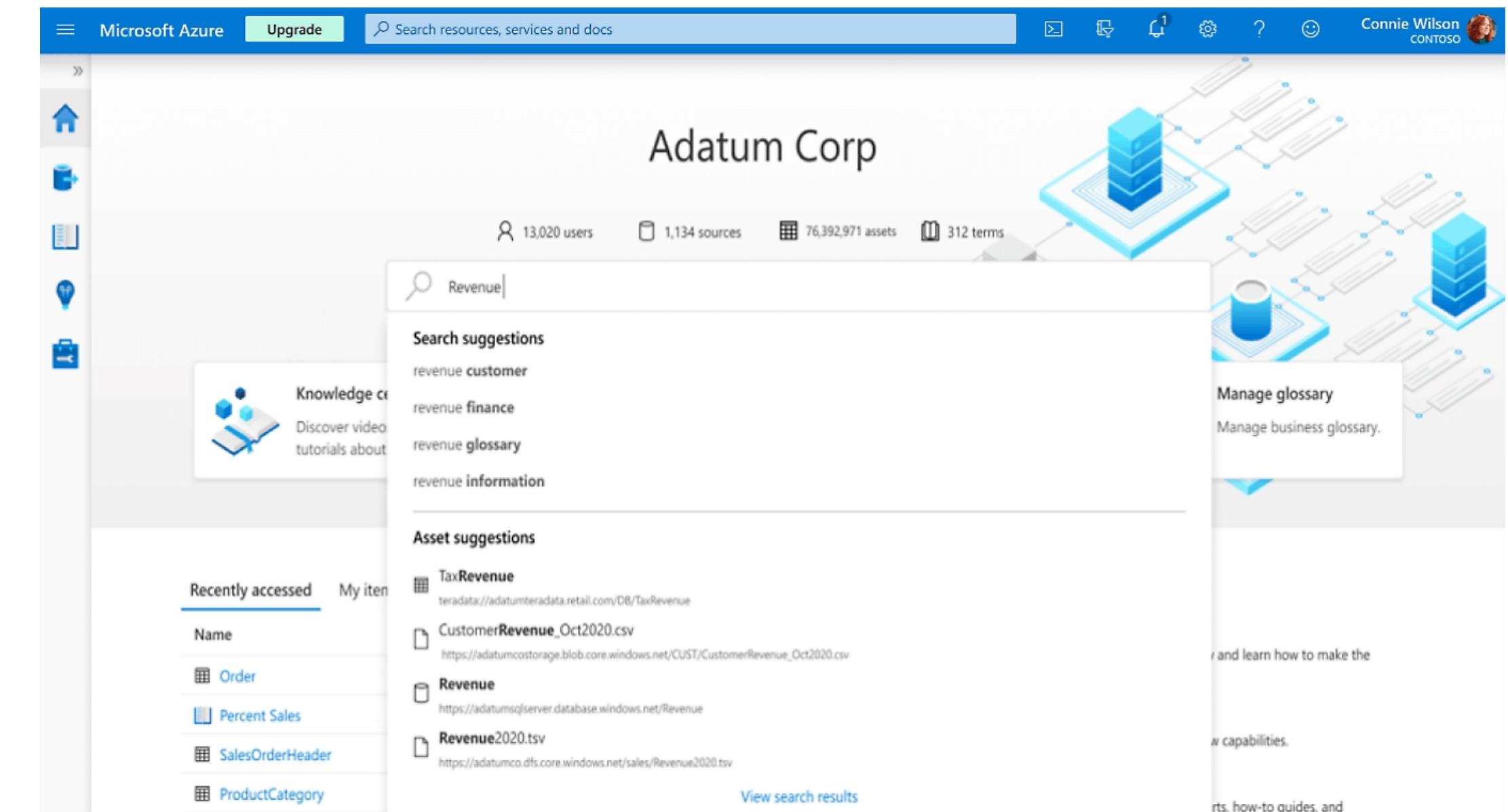


Image Source: <https://azure.microsoft.com/products/purview>



# Data Estate Insights

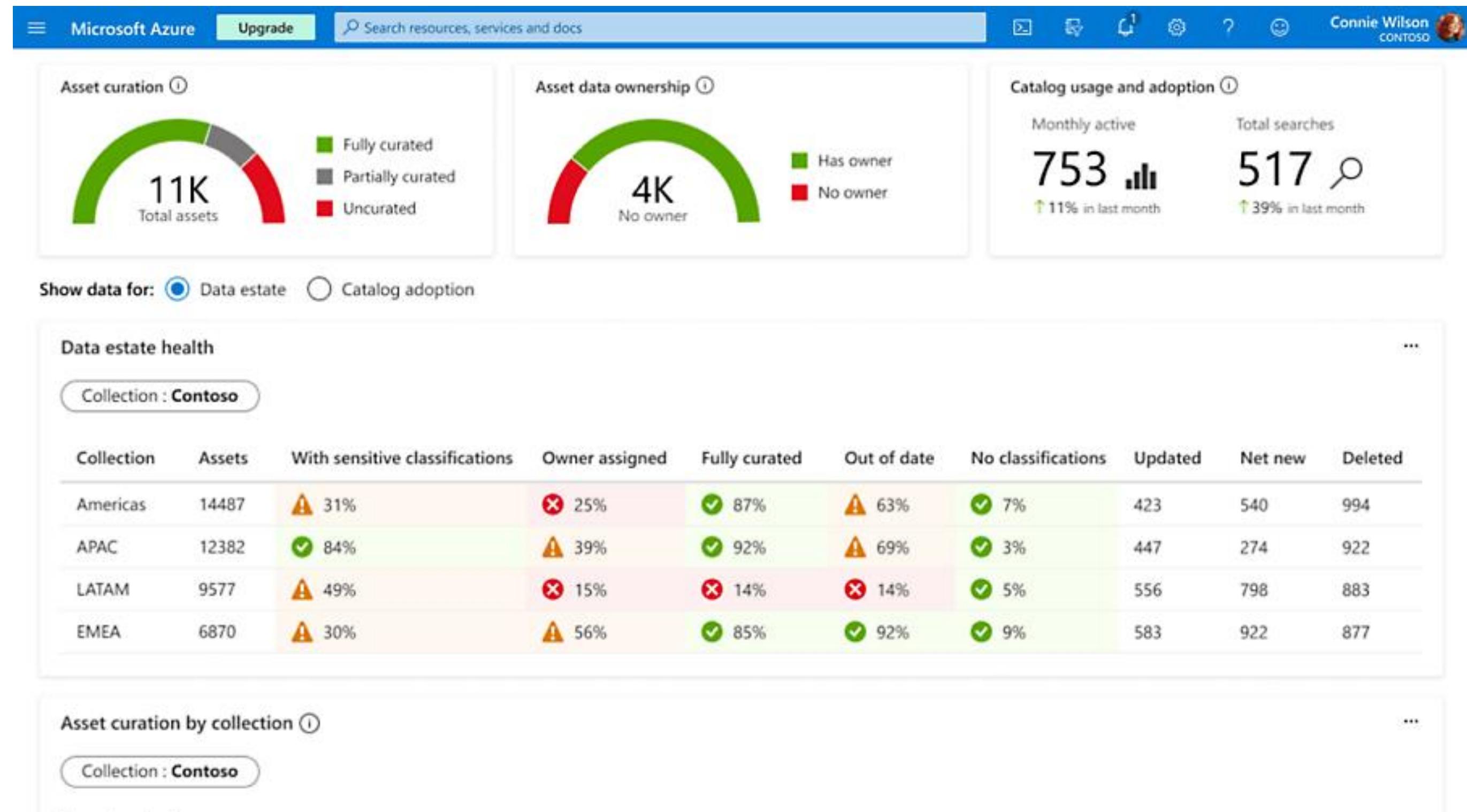


Image Source: <https://azure.microsoft.com/products/purview>



# Data Sharing

The screenshot shows the Microsoft Azure Purview Data Share (preview) interface. At the top, there's a navigation bar with 'Microsoft Azure' and 'Upgrade' buttons, a search bar, and a user profile for 'Connie Wilson CONTOSO'. The main area has a title 'Data share (preview)' and a large callout box for 'Create a share' with the sub-instruction 'Share data internally or with other organizations.' Below this are two side-by-side preview cards: 'New share' (left) and 'Pending share' (right), each with fields for 'Description', 'Type', 'From', 'Terms', and 'Accept and configure'. To the left of these cards is a diagram showing a 'Source' icon pointing to a 'TARGET' icon with the text 'in place access'. Below the diagram are sections for 'What is Data share?' (described as a simple and secure way to share data), 'How to send shares' (create a share, choose data, send invitations), and 'How to receive shares' (accept shared data and decide where to access it). A large graphic on the right depicts a network of people and data flows.

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



# Data Policy

The screenshot shows the 'Create policy' page in the Microsoft Azure Purview portal. The top navigation bar includes 'Microsoft Azure', 'Upgrade', a search bar, and user profile 'Connie Wilson CONTOSO'. The main form has sections for 'Name' (Dataprivacy-2019), 'Description' (This policy is for PII), and 'Policy statements'. An example statement is provided: 'Deny Read on data labeled as Confidential to everyone except FTEs.' A new statement is being added, showing 'Deny read on data labeled as Highly Sensitive to everyone except Group Finance-FTE'. At the bottom are 'Save' and 'Cancel' buttons.

Name \*  
Dataprivacy-2019

Description \*  
This policy is for PII

Policy statements ⓘ  
Create up to 5 policy statements for your policy.

Example policy statement:  
Deny **Read** on data labeled as **Confidential** to everyone except **FTEs**.

+ New policy statement

Deny **read** on data labeled as **Highly Sensitive** to everyone except Group **Finance-FTE**

Save Cancel

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**

---

