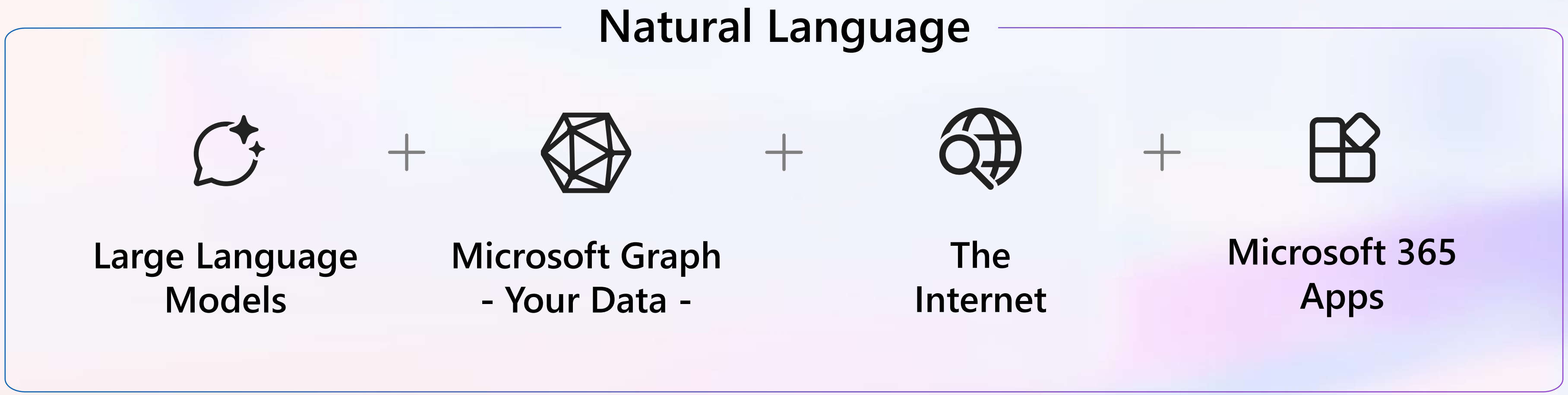
Microsoft 365 Copilot
Data Security & Governance

Fredrik Haventon

Technical Specialist Manager – Security & Compliance

Microsoft 365 Copilot



Natural Language

Large Language Models + Microsoft Graph - Your Data - + The Internet + Microsoft 365 Apps

Microsoft Cloud

Runs on trust

Your data is your data

Your data from any fine-tuning is not used to train the foundation AI models

Your data is protected by the most comprehensive enterprise compliance and security controls

Microsoft 365 Copilot

Protecting sensitive business information

Compliance boundary

Your prompts using Copilot, the data they retrieve, and the generated responses remain within the Microsoft 365 compliance boundary

Data access

Copilot only surfaces organizational data, such as files stored in SharePoint, to which individual users have at least view permissions.

Access controls

Use the same underlying controls for data access used in other Microsoft 365 services to ensure that the right groups and users have access only to the data they're supposed to have access to.

Your tenant

Only the current user's tenant Microsoft 365 cloud content for the current user is surfaced. Copilot won't search other tenants that the user may also be a B2B guest on, or non-current user's tenants that have been set up with either cross-tenant access or cross-tenant sync.

Technical readiness

Recommendations to aid in Microsoft 365 Copilot readiness of data security and governance

ME3

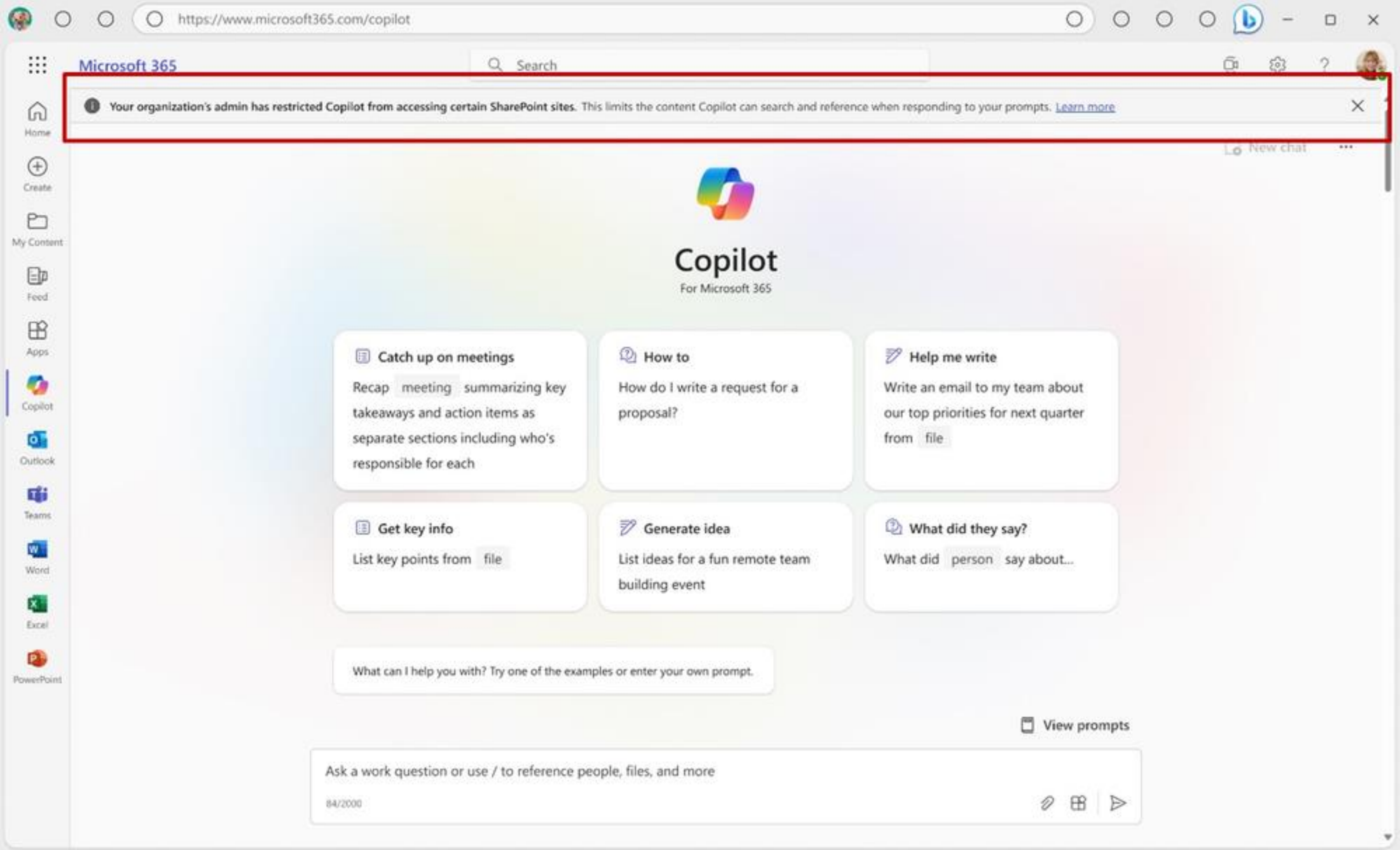
ME5

Add-ons

		Data discovery		Data access		Data protection		Data lifecycle	
Areas of focus		How do I see where sensitive data or risk may exist in my environment today?		How do I rectify any concerning access risks that may exist in my environment today?		How do I protect sites and content that exist in my environment today from being exposed?		How do I retain/dispose/discover content in my environment today and future AI responses?	
		• Permissions • Sensitive Data • Personally Identifiable Data • Data Overexposure • External Sharing		• Remove / Block Access • Change / Modify Access • Enforce Access Reviews • Change / Modify Semantic Search Access		• Protect Sites • Protect Content • Prevent Data Loss		• Retain Content • Dispose / Delete Content • Discover AI Generated Content • Audit AI Activities	
Recommended actions	E3	Review existing permissions of Teams and Sites	Use Content Search / Discovery Standard to discover sensitive information	Manually adjust permissions in Sites and Teams	Remove specific Sites from being included in the Semantic index	Implement data loss prevention policies for mail, files, and Sites	Manually apply sensitivity labels to Microsoft Teams and Sites	Implement location-wide retention and deletion policies	Use Audit Standard to review any Copilot activities
	E5	Use Content Explorer / eDiscovery Premium to identify sensitive content	Identify data exposition with Defender for Cloud Apps	Implement Access Reviews to recertify Teams & Group audience	Refine group expiration policy for inactive Teams & Group sites	Implement data loss prevention policies for Microsoft Teams and third-party cloud apps	Auto-apply sensitivity labels to Microsoft Teams and Sites	Implement adaptive retention and deletion policies (scoped retention)	Implement disposition reviews before deleting content
	Add - on	Identify overshared personally identifiable information with Microsoft Priva	Identify sensitive or overexposed content with SharePoint Premium	Use SharePoint Premium to restrict access to specific Sites		Create data overexposure policies using Microsoft Priva		Use Microsoft Priva to introduce data minimization policies	Use SharePoint Premium to manage Site lifecycle policies

Restricted SharePoint search

[Introducing Restricted SharePoint Search to help you get started with Copilot for Microsoft 365 - Microsoft Community Hub]



Your organization's admin has restricted Copilot from accessing certain SharePoint sites. This limits the content Copilot can search and reference when responding to your prompts. Learn more

Catch up on meetings
Recap meeting summarizing key takeaways and action items as separate sections including who's responsible for each

How to
How do I write a request for a proposal?

Help me write
Write an email to my team about our top priorities for next quarter from file

Get key info
List key points from file

Generate idea
List ideas for a fun remote team building event

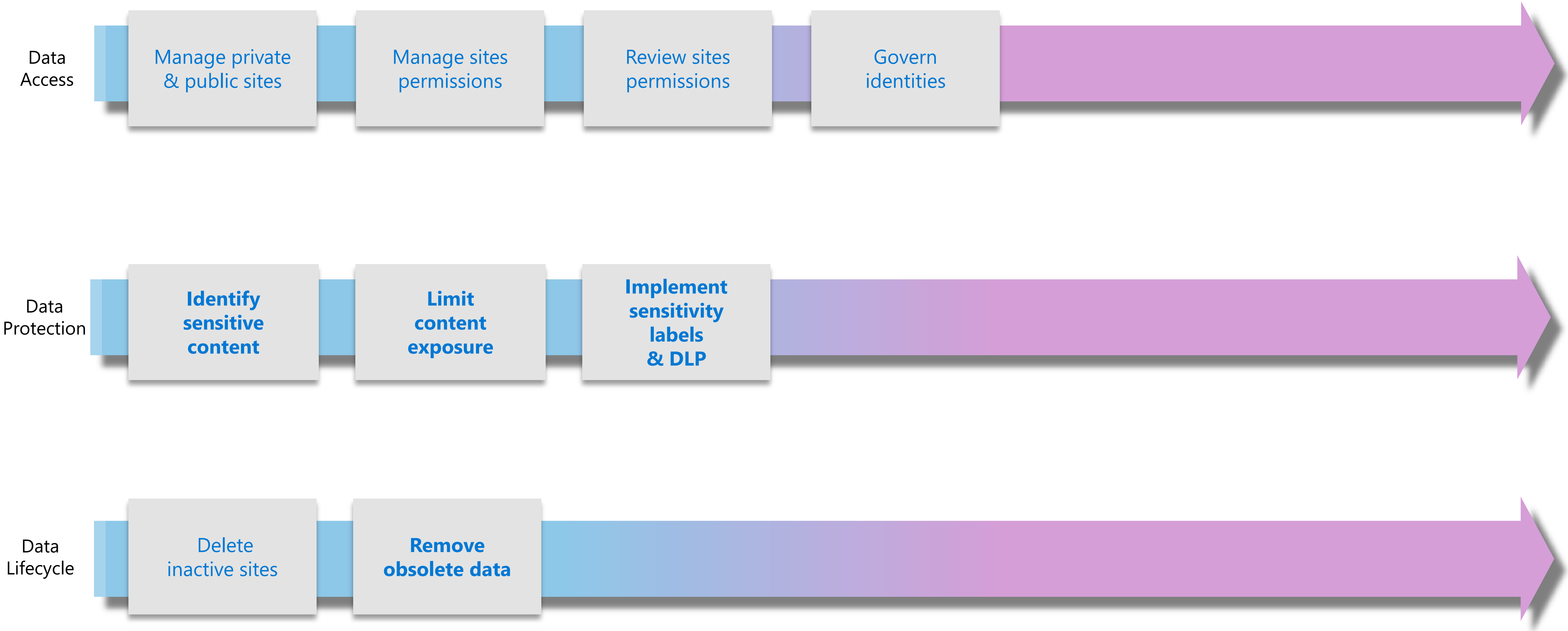
What did they say?
What did person say about...

What can I help you with? Try one of the examples or enter your own prompt.

Ask a work question or use / to reference people, files, and more

Best Practices for Data Security - Overview

It is not a requirement to enable all the features below for Microsoft 365 Copilot. These are recommended to provide optimal data governance.



Data Access

- Manage private & public sites
- Manage sites permissions
- Review sites permissions
- Govern identities

Data Protection

- **Identify sensitive content**
- **Limit content exposure**
- **Implement sensitivity labels & DLP**

Data Lifecycle

- Delete inactive sites
- **Remove obsolete data**

Data lifecycle

Ensure content freshness/up to date and reduce the risk of over exposed aging data.

Recommended approach:

First 30 days

- Identify inactive SharePoint sites & Teams
- Involve sites owners with a data clean up campaign

30 to 90 days

- Implement Inactive Sites policy to report on inactive sites and let owner recertify content
- Consider Site Deletion policies to delete obsolete sites, plus Site Archiving Preview to retain inactive sites by moving it into a cold storage
- Implement Microsoft 365 Group expiration policy to automate the lifecycle of inactive Teams & Group sites

After 90 days

- Refine a comprehensive data lifecycle management strategy to:
  - Keep valuable and regulatory content with retention policies or labels
  - Delete unnecessary and stale content with additional deletion policies or labels

Data overexposure

Focus on overexposed or sensitive content accessible by anyone in the organization without explicit permissions granted.

Recommended approach:

First 30 days

- Identify Sites & Groups with privacy level of Public
- Identify the location of sensitive content based on OOB classifiers via Content Explorer & Content Search
- Identify data exposition with Defender for Cloud Apps
- Change the privacy level of Sites from public to private when necessary
- Exclude temporarily specific Sites from the semantic index
- Involve sites owners with a data permission clean up campaign

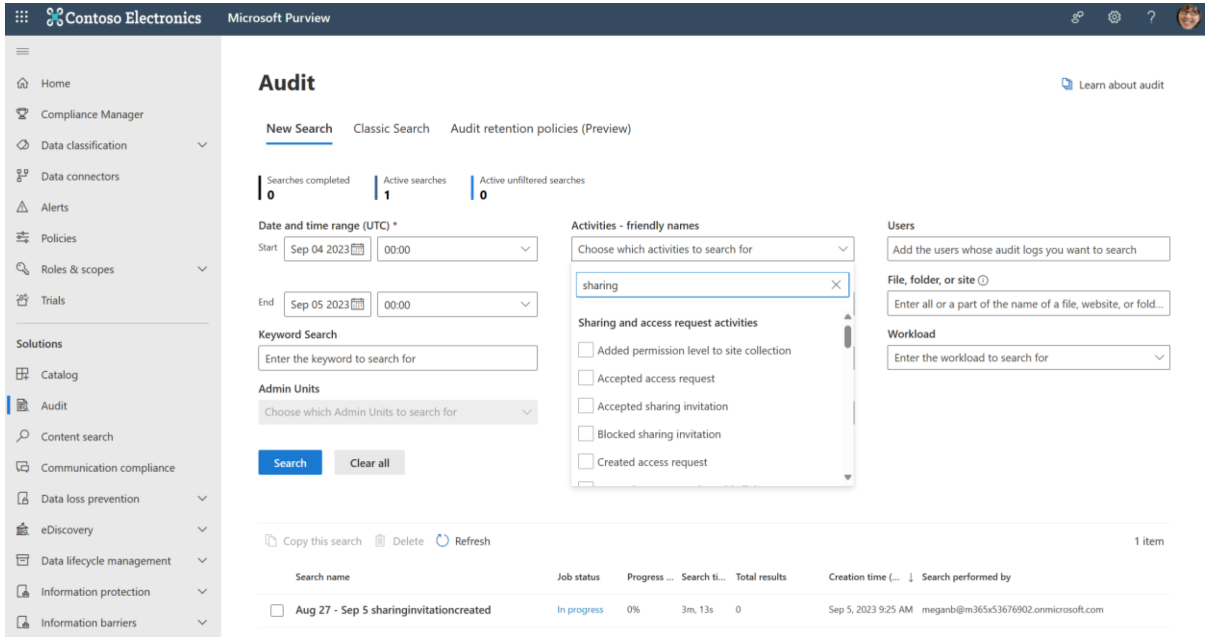
30 to 90 days

- Establish a Sensitivity labels for sites and groups strategy to condition the creation of new public/private sites depending on the sensitivity
- Use data governance access report to identify potential overshared sensitive content to adapt privacy level of existing sites
- Implement Access Reviews to ensure recertification of the audience for Teams & Groups

After 90 days

- Extend Sensitivity label strategy for containers, to:
  - Consider only owners can share content for sensitive sites
  - Adapt the default behavior for sharing links, external sharing control and external user access
- Extend your Sensitivity label strategy for files, by enforcing encryption with ACL, applying it with auto-labeling
- Restrict site access to only Microsoft 365 group owners and members
- Implement Information Barriers in case of specific segregation requirements

Audit Search



Audit

Searches completed 0 | Active searches 1 | Active unfiltered searches 0

Date and time range (UTC) *
Start: Sep 04 2023 00:00
End: Sep 05 2023 00:00

Keyword Search: Enter the keyword to search for

Admin Units: Choose which Admin Units to search for

Activities - friendly names: Choose which activities to search for

sharing

Sharing and access request activities
- □ Added permission level to site collection
- □ Accepted access request
- □ Accepted sharing invitation
- □ Blocked sharing invitation
- □ Created access request

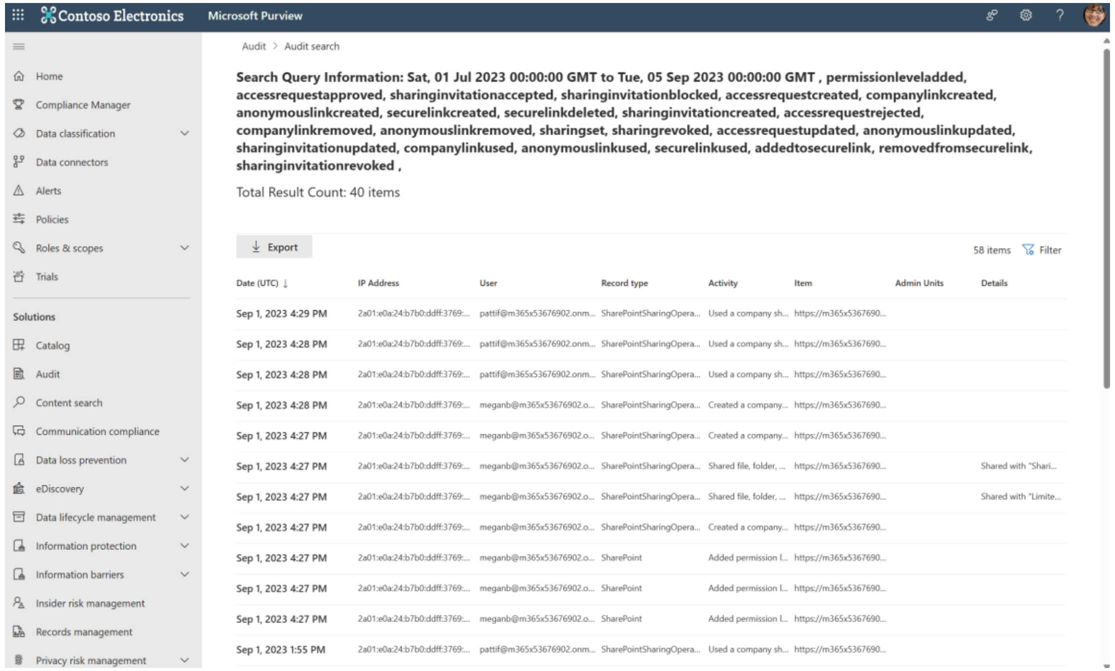
Users: Add the users whose audit logs you want to search

File, folder, or site: Enter all or a part of the name of a file, website, or fold...

Workload: Enter the workload to search for

1 item

	Search name	Job status	Progress ...	Search ti...	Total results	Creation time (... ↓	Search performed by
□	Aug 27 - Sep 5 sharinginvitationcreated	In progress	0%	3m, 13s	0	Sep 5, 2023 9:25 AM	meganb@m365x53676902.onmicrosoft.com



Search Query Information: Sat, 01 Jul 2023 00:00:00 GMT to Tue, 05 Sep 2023 00:00:00 GMT , permissionleveladded, accessrequestapproved, sharinginvitationaccepted, sharinginvitationblocked, accessrequestcreated, companylinkcreated, anonymouslinkcreated, securelinkcreated, securelinkdeleted, sharinginvitationcreated, accessrequestrejected, companylinkremoved, anonymouslinkremoved, sharingset, sharingrevoked, accessrequestupdated, anonymouslinkupdated, sharinginvitationupdated, companylinkused, anonymouslinkused, securelinkused, addedtosecurelink, removedfromsecurelink, sharinginvitationrevoked ,

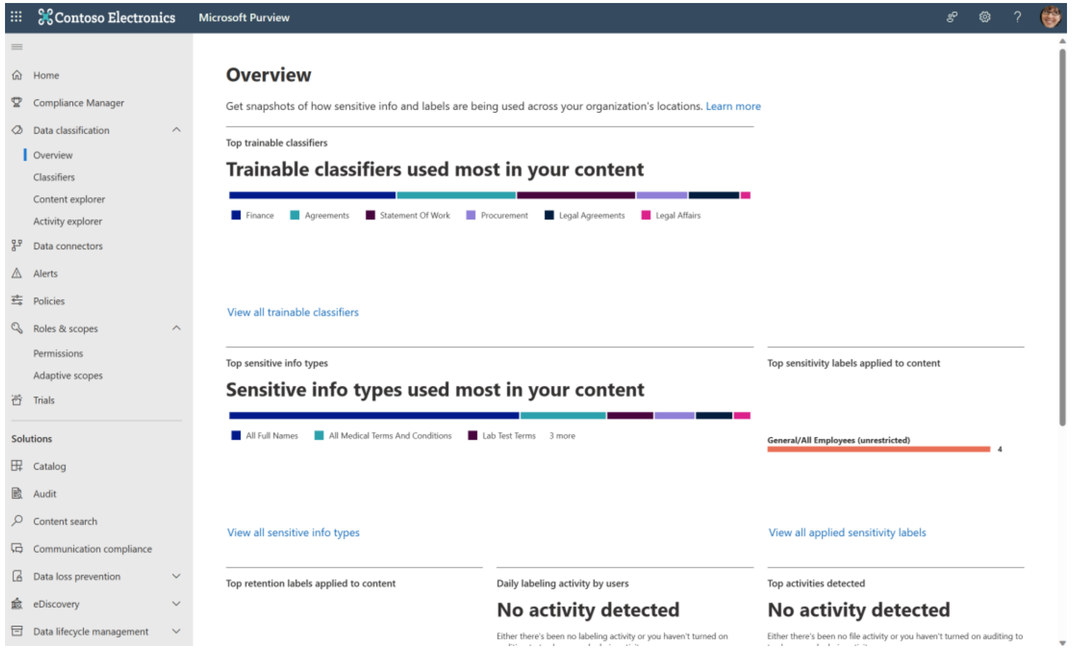
Total Result Count: 40 items

58 items

Date (UTC) ↓	IP Address	User	Record type	Activity	Item	Admin Units	Details
Sep 1, 2023 4:29 PM	2a01:e0a:24:b7b0:ddff:3769:...	pattif@m365x53676902.onm...	SharePointSharingOpera...	Used a company sh...	https://m365x5367690...		
Sep 1, 2023 4:28 PM	2a01:e0a:24:b7b0:ddff:3769:...	pattif@m365x53676902.onm...	SharePointSharingOpera...	Used a company sh...	https://m365x5367690...		
Sep 1, 2023 4:28 PM	2a01:e0a:24:b7b0:ddff:3769:...	pattif@m365x53676902.onm...	SharePointSharingOpera...	Used a company sh...	https://m365x5367690...		
Sep 1, 2023 4:28 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePointSharingOpera...	Created a company...	https://m365x5367690...		
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePointSharingOpera...	Created a company...	https://m365x5367690...		
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePointSharingOpera...	Shared file, folder, ...	https://m365x5367690...		Shared with "Shari...
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePointSharingOpera...	Shared file, folder, ...	https://m365x5367690...		Shared with "Limite...
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePointSharingOpera...	Created a company...	https://m365x5367690...		
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePoint	Added permission l...	https://m365x5367690...		
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePoint	Added permission l...	https://m365x5367690...		
Sep 1, 2023 4:27 PM	2a01:e0a:24:b7b0:ddff:3769:...	meganb@m365x53676902.o...	SharePoint	Added permission l...	https://m365x5367690...		
Sep 1, 2023 1:55 PM	2a01:e0a:24:b7b0:ddff:3769:...	pattif@m365x53676902.onm...	SharePointSharingOpera...	Used a company sh...	https://m365x5367690...		

Using Audit Logs, you can view specific activities in your tenant (180 days – up to 365 days with E5). Such as the sharing and access request activities.

Data Classification / Content Explorer



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

Daily labeling activity by users

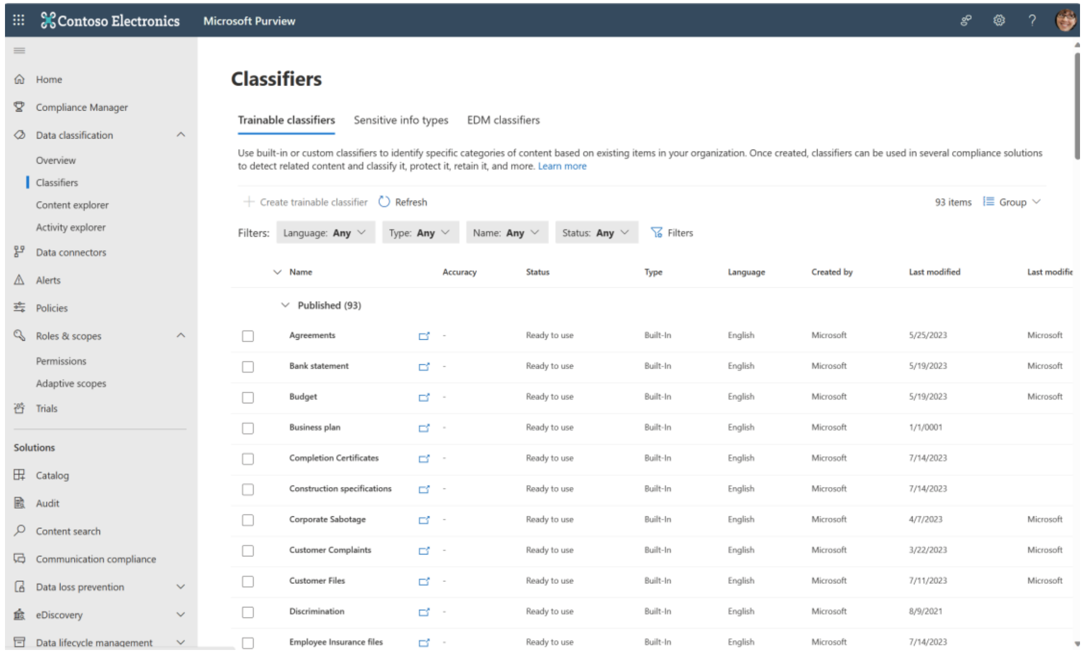
No activity detected

Either there's been no labeling activity or you haven't turned on

Top activities detected

No activity detected

Either there's been no file activity or you haven't turned on auditing to



Classifiers

Trainable classifiers | Sensitive info types | EDM classifiers

Use built-in or custom classifiers to identify specific categories of content based on existing items in your organization. Once created, classifiers can be used in several compliance solutions to detect related content and classify it, protect it, retain it, and more. Learn more

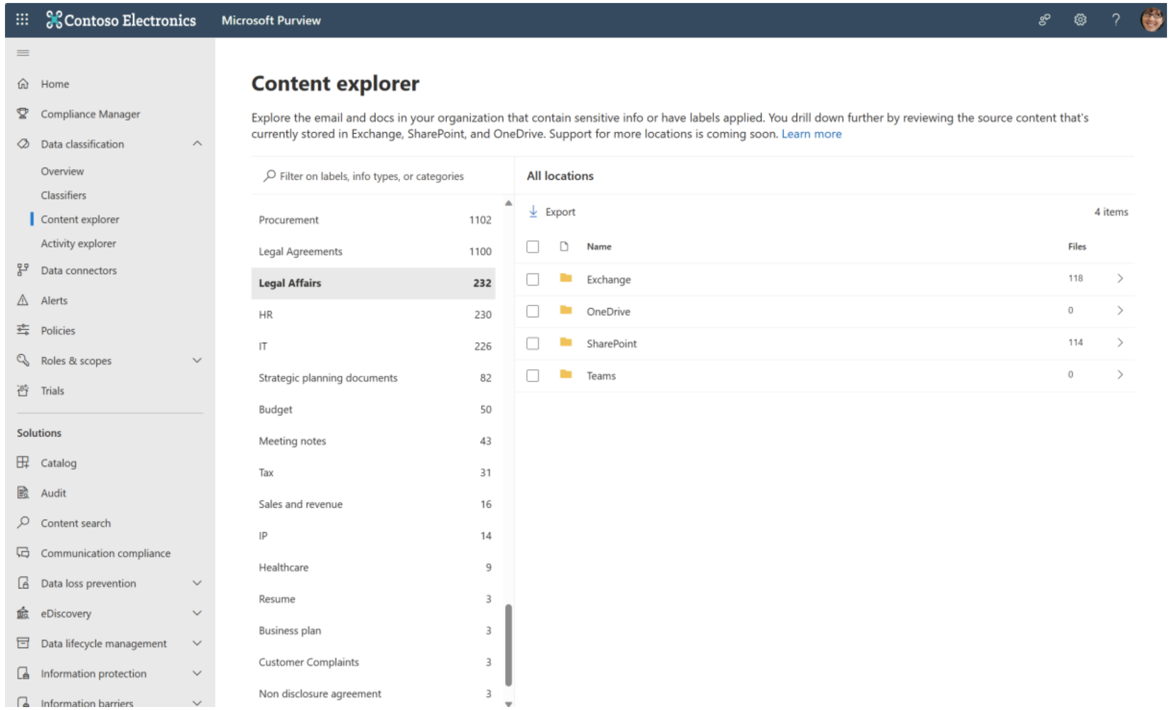
Filters: Language: **Any** Type: **Any** Name: **Any** Status: **Any** Filters

Published (93)

	Name	Accuracy	Status	Type	Language	Created by	Last modified	Last modifie
□	Agreements	-	Ready to use	Built-In	English	Microsoft	5/25/2023	Microsoft
□	Bank statement	-	Ready to use	Built-In	English	Microsoft	5/19/2023	Microsoft
□	Budget	-	Ready to use	Built-In	English	Microsoft	5/19/2023	Microsoft
□	Business plan	-	Ready to use	Built-In	English	Microsoft	1/1/0001	
□	Completion Certificates	-	Ready to use	Built-In	English	Microsoft	7/14/2023	
□	Construction specifications	-	Ready to use	Built-In	English	Microsoft	7/14/2023	
□	Corporate Sabotage	-	Ready to use	Built-In	English	Microsoft	4/7/2023	Microsoft
□	Customer Complaints	-	Ready to use	Built-In	English	Microsoft	3/22/2023	Microsoft
□	Customer Files	-	Ready to use	Built-In	English	Microsoft	7/11/2023	Microsoft
□	Discrimination	-	Ready to use	Built-In	English	Microsoft	8/9/2021	
□	Employee Insurance files	-	Ready to use	Built-In	English	Microsoft	7/14/2023	

In Data Classification, you can see the different classifiers (E5): out-of-the-box classifiers or trainable classifiers (custom)

Data Classification / Content Explorer



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

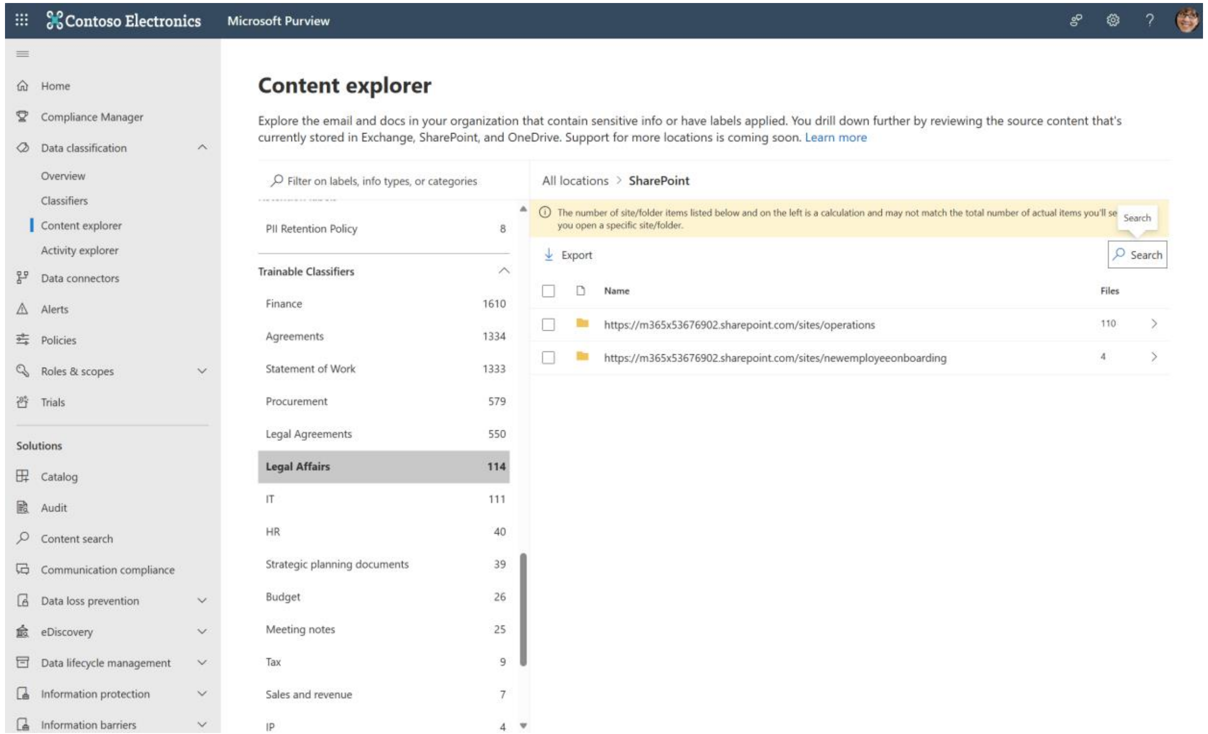
Filter on labels, info types, or categories

Procurement	1102
Legal Agreements	1100
Legal Affairs	**232**
HR	230
IT	226
Strategic planning documents	82
Budget	50
Meeting notes	43
Tax	31
Sales and revenue	16
IP	14
Healthcare	9
Resume	3
Business plan	3
Customer Complaints	3
Non disclosure agreement	3

All locations

Export — 4 items

Name	Files
Exchange	118
OneDrive	0
SharePoint	114
Teams	0



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

PII Retention Policy	8
Trainable Classifiers	
Finance	1610
Agreements	1334
Statement of Work	1333
Procurement	579
Legal Agreements	550
Legal Affairs	**114**
IT	111
HR	40
Strategic planning documents	39
Budget	26
Meeting notes	25
Tax	9
Sales and revenue	7
IP	4

All locations > SharePoint

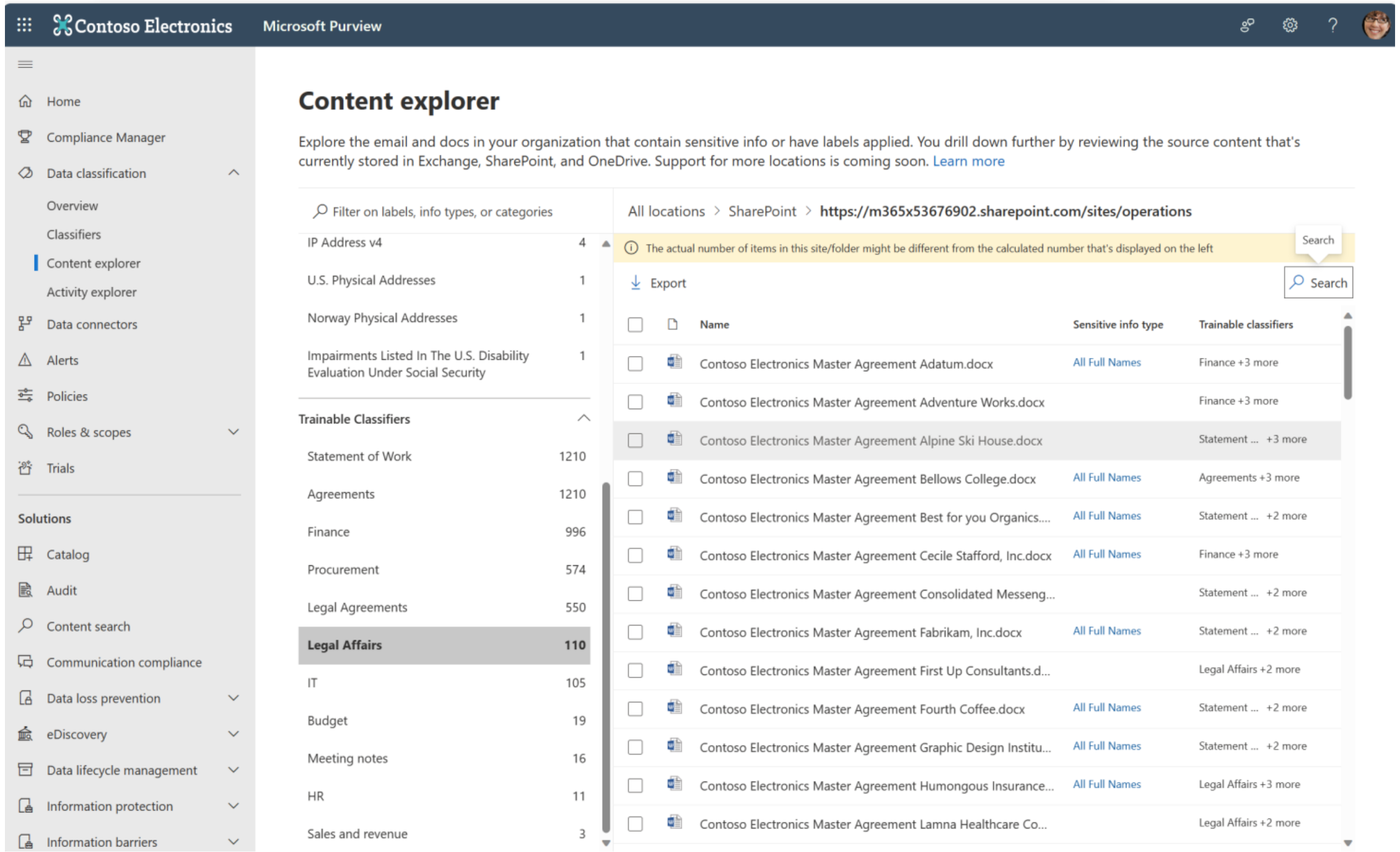
The number of site/folder items listed below and on the left is a calculation and may not match the total number of actual items you'll se you open a specific site/folder.

Export — Search

Name	Files
https://m365x53676902.sharepoint.com/sites/operations	110
https://m365x53676902.sharepoint.com/sites/newemployeeonboarding	4

Select a specific classifier, and open it to view how much your content is mapped to this classifier. Check especially the ones in SharePoint Online locations.

Data Classification / Content Explorer



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

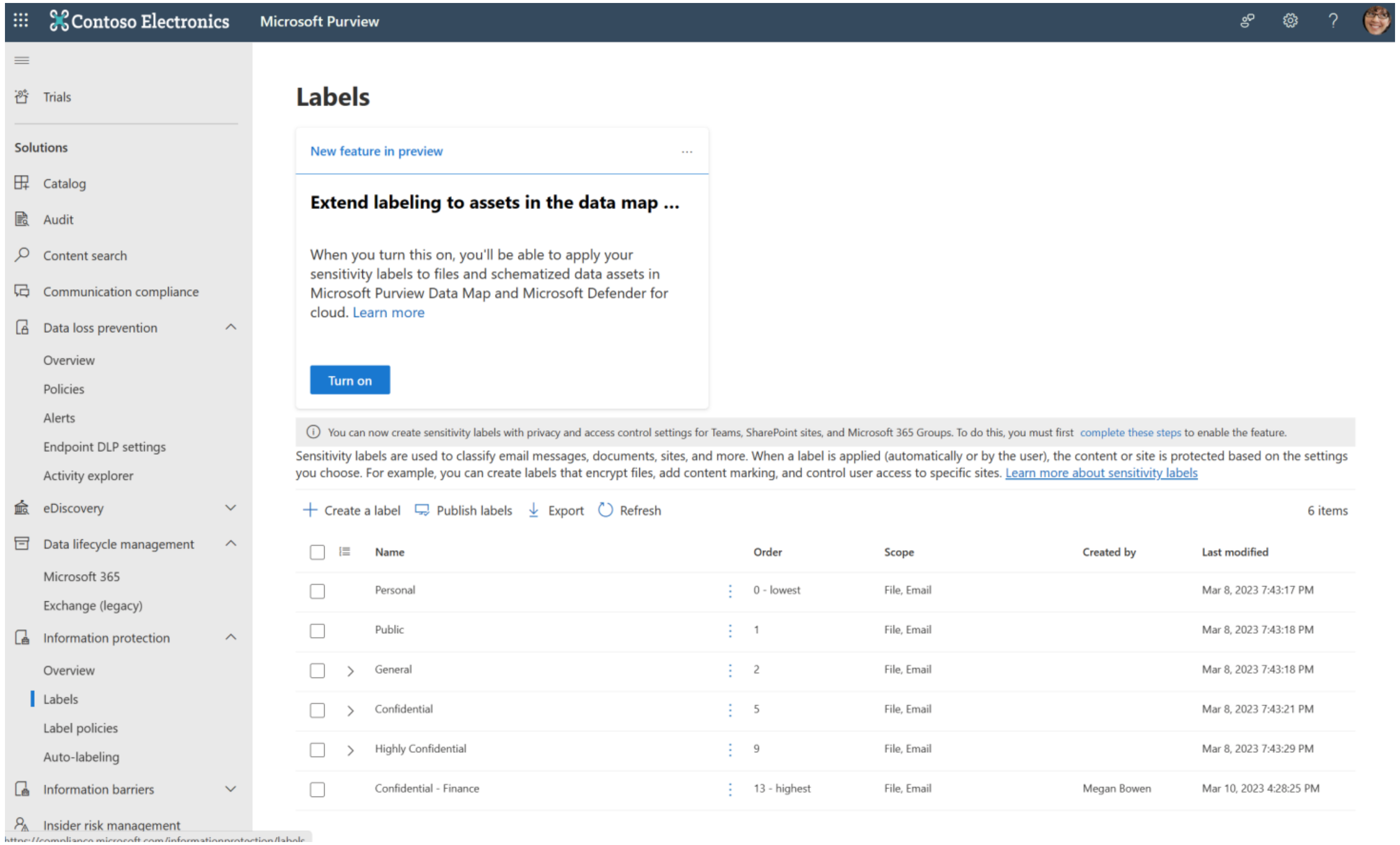
IP Address v4	4
U.S. Physical Addresses	1
Norway Physical Addresses	1
Impairments Listed In The U.S. Disability Evaluation Under Social Security	1
Trainable Classifiers	
Statement of Work	1210
Agreements	1210
Finance	996
Procurement	574
Legal Agreements	550
Legal Affairs	**110**
IT	105
Budget	19
Meeting notes	16
HR	11
Sales and revenue	3

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

Name	Sensitive info type	Trainable classifiers
Contoso Electronics Master Agreement Adatum.docx	All Full Names	Finance +3 more
Contoso Electronics Master Agreement Adventure Works.docx		Finance +3 more
Contoso Electronics Master Agreement Alpine Ski House.docx		Statement ... +3 more
Contoso Electronics Master Agreement Bellows College.docx	All Full Names	Agreements +3 more
Contoso Electronics Master Agreement Best for you Organics....	All Full Names	Statement ... +2 more
Contoso Electronics Master Agreement Cecile Stafford, Inc.docx	All Full Names	Finance +3 more
Contoso Electronics Master Agreement Consolidated Messeng...		Statement ... +2 more
Contoso Electronics Master Agreement Fabrikam, Inc.docx	All Full Names	Statement ... +2 more
Contoso Electronics Master Agreement First Up Consultants.d...		Legal Affairs +2 more
Contoso Electronics Master Agreement Fourth Coffee.docx	All Full Names	Statement ... +2 more
Contoso Electronics Master Agreement Graphic Design Institu...	All Full Names	Statement ... +2 more
Contoso Electronics Master Agreement Humongous Insurance...	All Full Names	Legal Affairs +3 more
Contoso Electronics Master Agreement Lamna Healthcare Co...		Legal Affairs +2 more

You can see a list of the documents associated to this classifier.
You can export a list of the documents, or the sites matching the classifier.
Then, use SharePoint Online or Teams Admin center to review the visibility or the permissions applied

Information Protection / Labels



Labels

New feature in preview

Extend labeling to assets in the data map ...

When you turn this on, you'll be able to apply your sensitivity labels to files and schematized data assets in Microsoft Purview Data Map and Microsoft Defender for cloud. Learn more

Turn on

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.

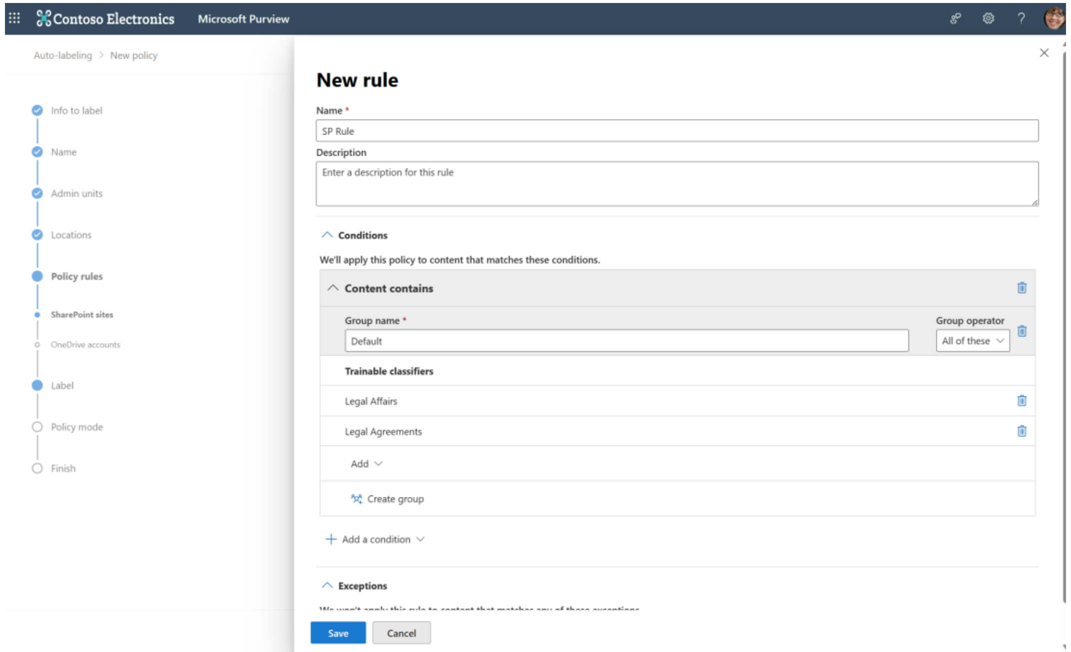
Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access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

+ Create a label   Publish labels   Export   Refresh   6 items

Name	Order	Scope	Created by	Last modified
Personal	0 - lowest	File, Email		Mar 8, 2023 7:43:17 PM
Public	1	File, Email		Mar 8, 2023 7:43:18 PM
General	2	File, Email		Mar 8, 2023 7:43:18 PM
Confidential	5	File, Email		Mar 8, 2023 7:43:21 PM
Highly Confidential	9	File, Email		Mar 8, 2023 7:43:29 PM
Confidential - Finance	13 - highest	File, Email	Megan Bowen	Mar 10, 2023 4:28:25 PM

Copilot will respect labels applied to your content. Consider this option to create more granular controls over who can access a content based on the applied labels, or its content (matching a sensitive info type), rather than global permissions.

Information Protection / Labels



Contoso Electronics Microsoft Purview

Auto-labeling > New policy

- Info to label
- Name
- Admin units
- Locations
- Policy rules
  - SharePoint sites
  - OneDrive accounts
- Label
- Policy mode
- Finish

New rule

Name *

SP Rule

Description

Enter a description for this rule

Conditions

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

Content contains

Group name *: Default

Group operator: All of these

Trainable classifiers

Legal Affairs

Legal Agreements

Add

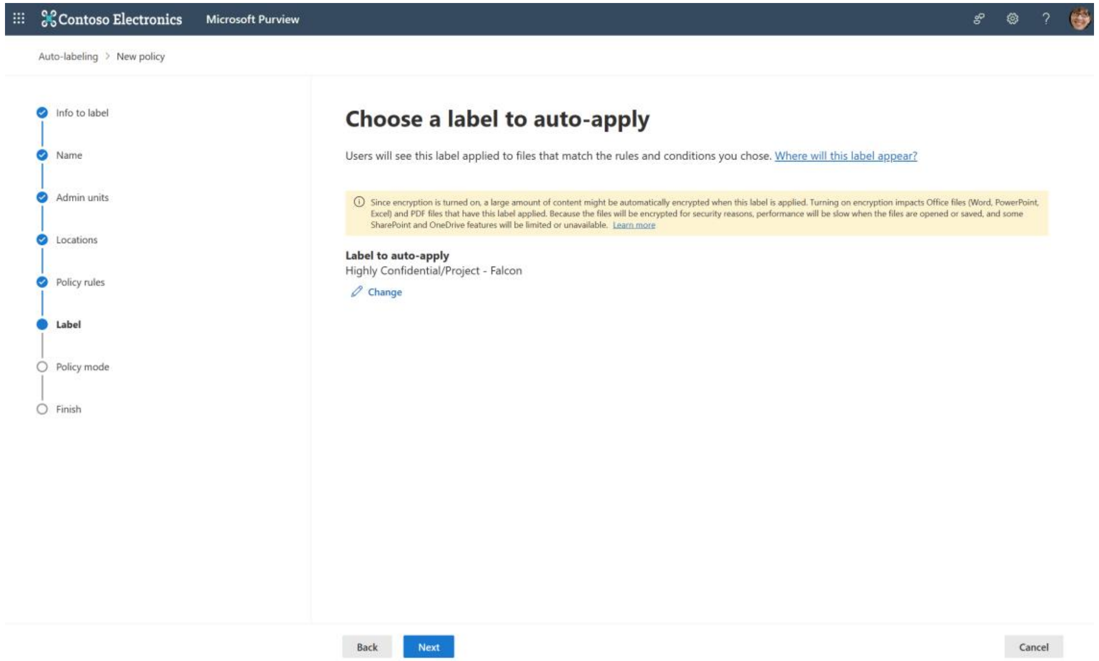
Create group

Add a condition

Exceptions

We won't apply this rule to content that matches any of these exceptions

Save Cancel



Contoso Electronics Microsoft Purview

Auto-labeling > New policy

- Info to label
- Name
- Admin units
- Locations
- Policy rules
- Label
- Policy mode
- Finish

Choose a label to auto-apply

Users will see this label applied to files that match the rules and conditions you chose. Where will this label appear?

ⓘ Since encryption is turned on, a large amount of content might be automatically encrypted when this label is applied. Turning on encryption impacts Office files (Word, PowerPoint, Excel) and PDF files that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Label to auto-apply

Highly Confidential/Project - Falcon

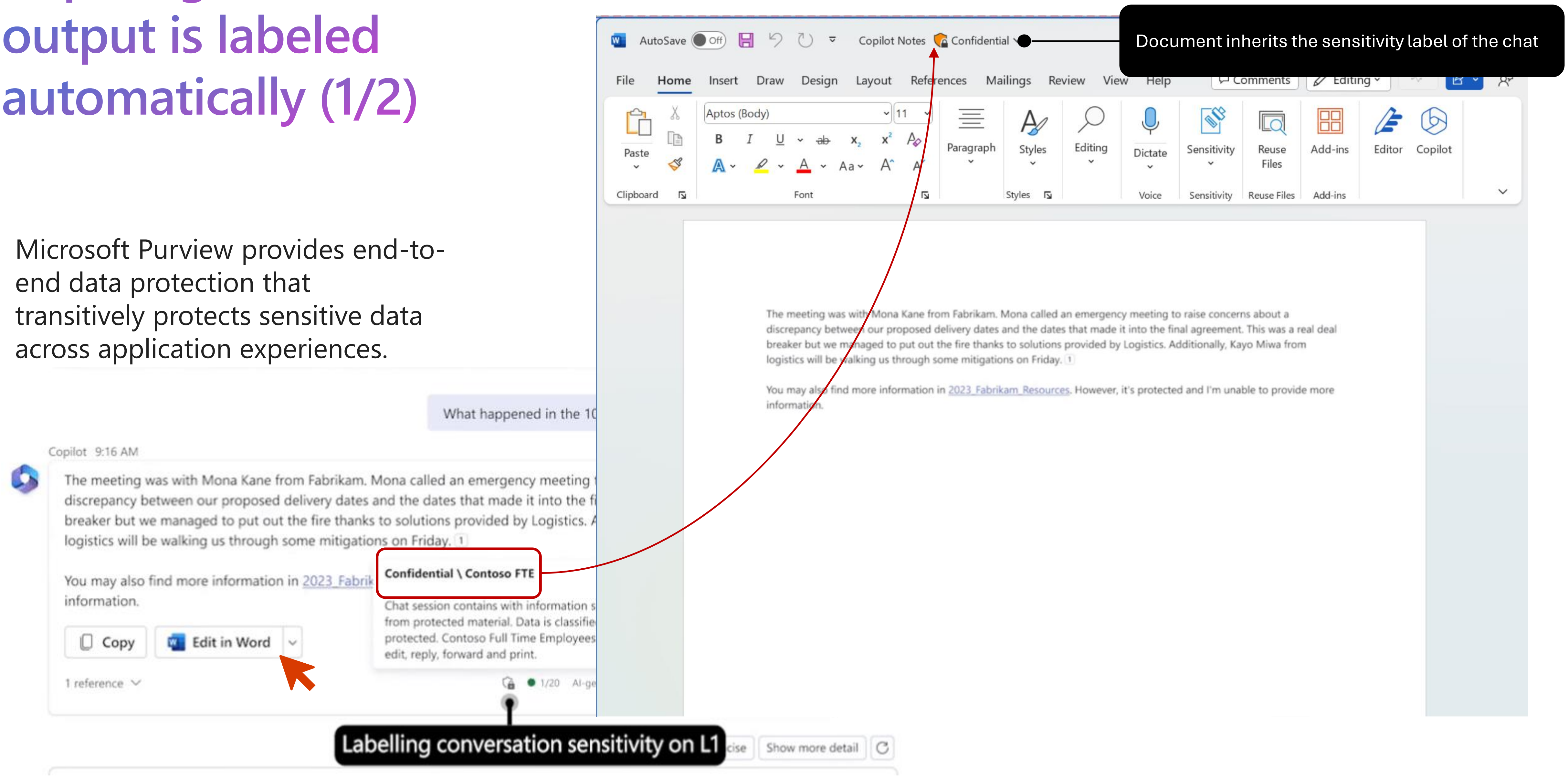
Change

Back Next Cancel

Use auto-labeling (E5) to automatically apply a label based on the content of documents (keyword, sensitive info type, trainable classifiers) to protect sensitive content.

Copilot generated output is labeled automatically (1/2)

Microsoft Purview provides end-to-end data protection that transitively protects sensitive data across application experiences.



Document inherits the sensitivity label of the chat

The meeting was with Mona Kane from Fabrikam. Mona called an emergency meeting to raise concerns about a discrepancy between our proposed delivery dates and the dates that made it into the final agreement. This was a real deal breaker but we managed to put out the fire thanks to solutions provided by Logistics. Additionally, Kayo Miwa from logistics will be walking us through some mitigations on Friday. 1

You may also find more information in 2023_Fabrikam_Resources. However, it's protected and I'm unable to provide more information.

What happened in the 10

Copilot 9:16 AM

The meeting was with Mona Kane from Fabrikam. Mona called an emergency meeting t
discrepancy between our proposed delivery dates and the dates that made it into the fi
breaker but we managed to put out the fire thanks to solutions provided by Logistics. A
logistics will be walking us through some mitigations on Friday. 1

You may also find more information in 2023_Fabrik
information.

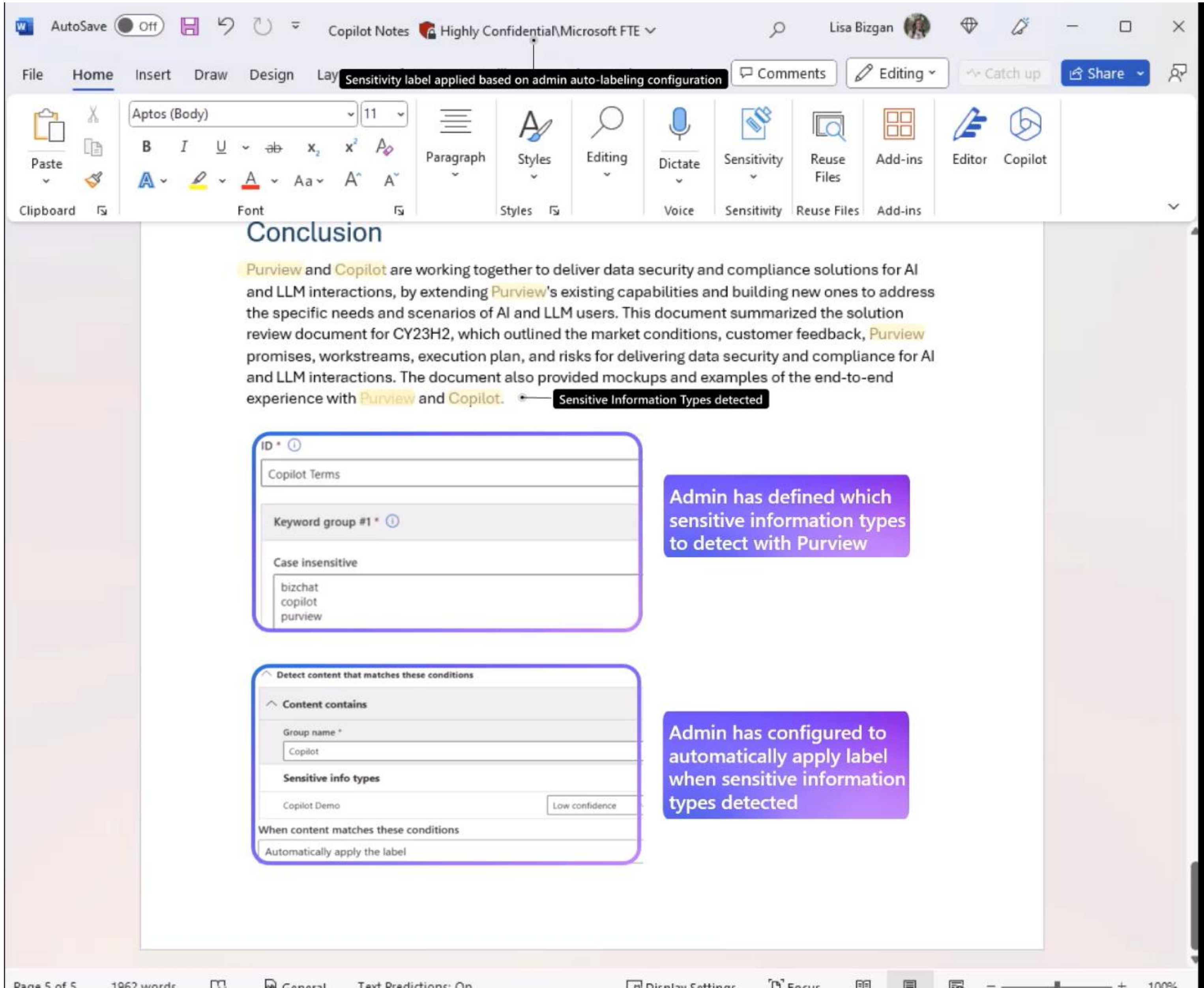
Confidential \ Contoso FTE

Chat session contains with information s
from protected material. Data is classifie
protected. Contoso Full Time Employees
edit, reply, forward and print.

Labelling conversation sensitivity on L1

Copilot generated output is labeled automatically (2/2)

Use existing Microsoft Purview auto-labeling rules and admin-defined sensitive information types to detect sensitive content and automatically label the files/emails.



Sensitivity label applied based on admin auto-labeling configuration

Conclusion

Purview and Copilot are working together to deliver data security and compliance solutions for AI and LLM interactions, by extending Purview's existing capabilities and building new ones to address the specific needs and scenarios of AI and LLM users. This document summarized the solution review document for CY23H2, which outlined the market conditions, customer feedback, Purview promises, workstreams, execution plan, and risks for delivering data security and compliance for AI and LLM interactions. The document also provided mockups and examples of the end-to-end experience with Purview and Copilot.

Sensitive Information Types detected

ID *

Copilot Terms

Keyword group #1 *

Case insensitive

bizchat
copilot
purview

Admin has defined which sensitive information types to detect with Purview

Detect content that matches these conditions

Content contains

Group name *

Copilot

Sensitive info types

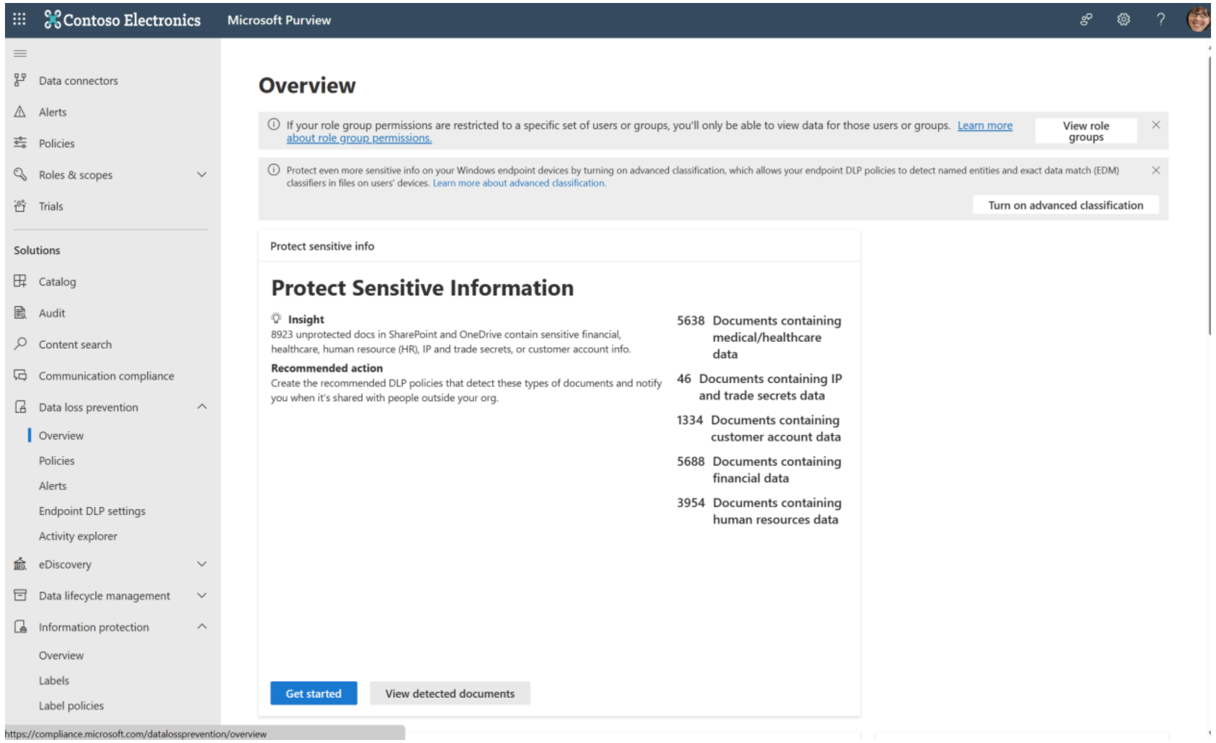
Copilot Demo — Low confidence

When content matches these conditions

Automatically apply the label

Admin has configured to automatically apply label when sensitive information types detected

Data Loss Prevention



Overview

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to view data for those users or groups. Learn more about role group permissions.

Protect even more sensitive info on your Windows endpoint devices by turning on advanced classification, which allows your endpoint DLP policies to detect named entities and exact data match (EDM) classifiers in files on users' devices. Learn more about advanced classification.

Protect sensitive info

Protect Sensitive Information

Insight

8923 unprotected docs in SharePoint and OneDrive contain sensitive financial, healthcare, human resource (HR), IP and trade secrets, or customer account info.

Recommended action

Create the recommended DLP policies that detect these types of documents and notify you when it's shared with people outside your org.

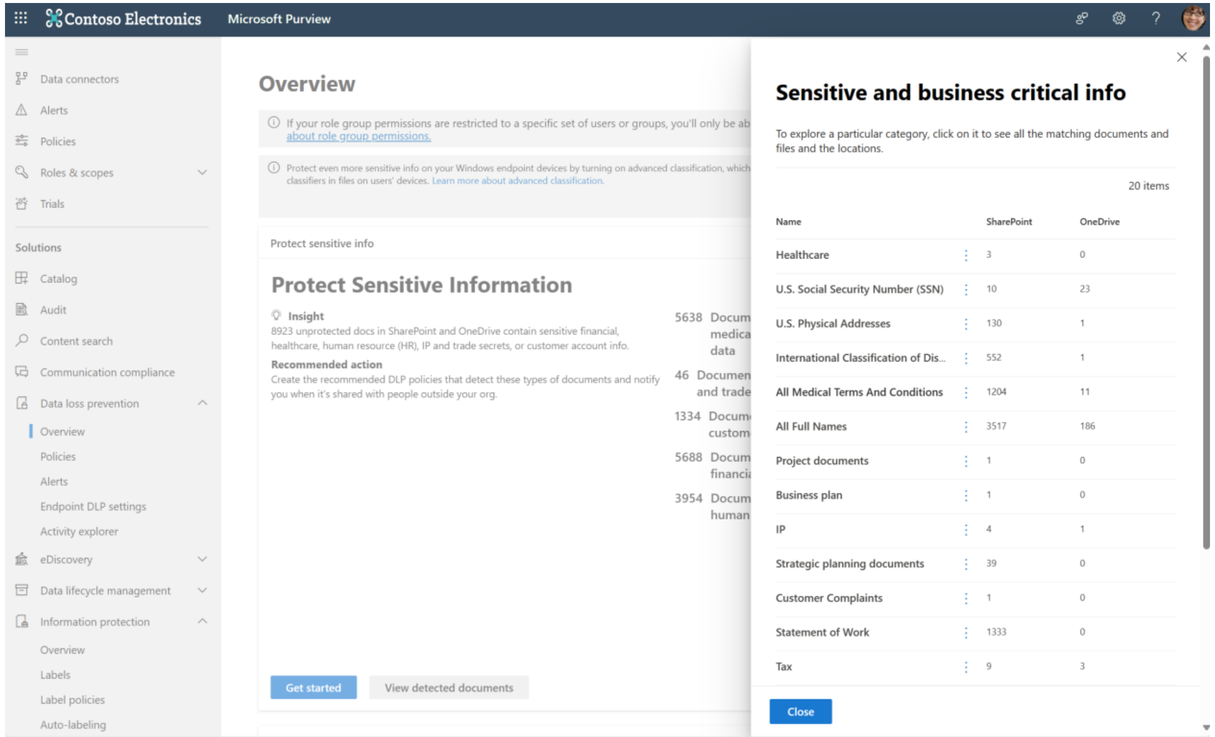
5638 Documents containing medical/healthcare data

46 Documents containing IP and trade secrets data

1334 Documents containing customer account data

5688 Documents containing financial data

3954 Documents containing human resources data



Sensitive and business critical info

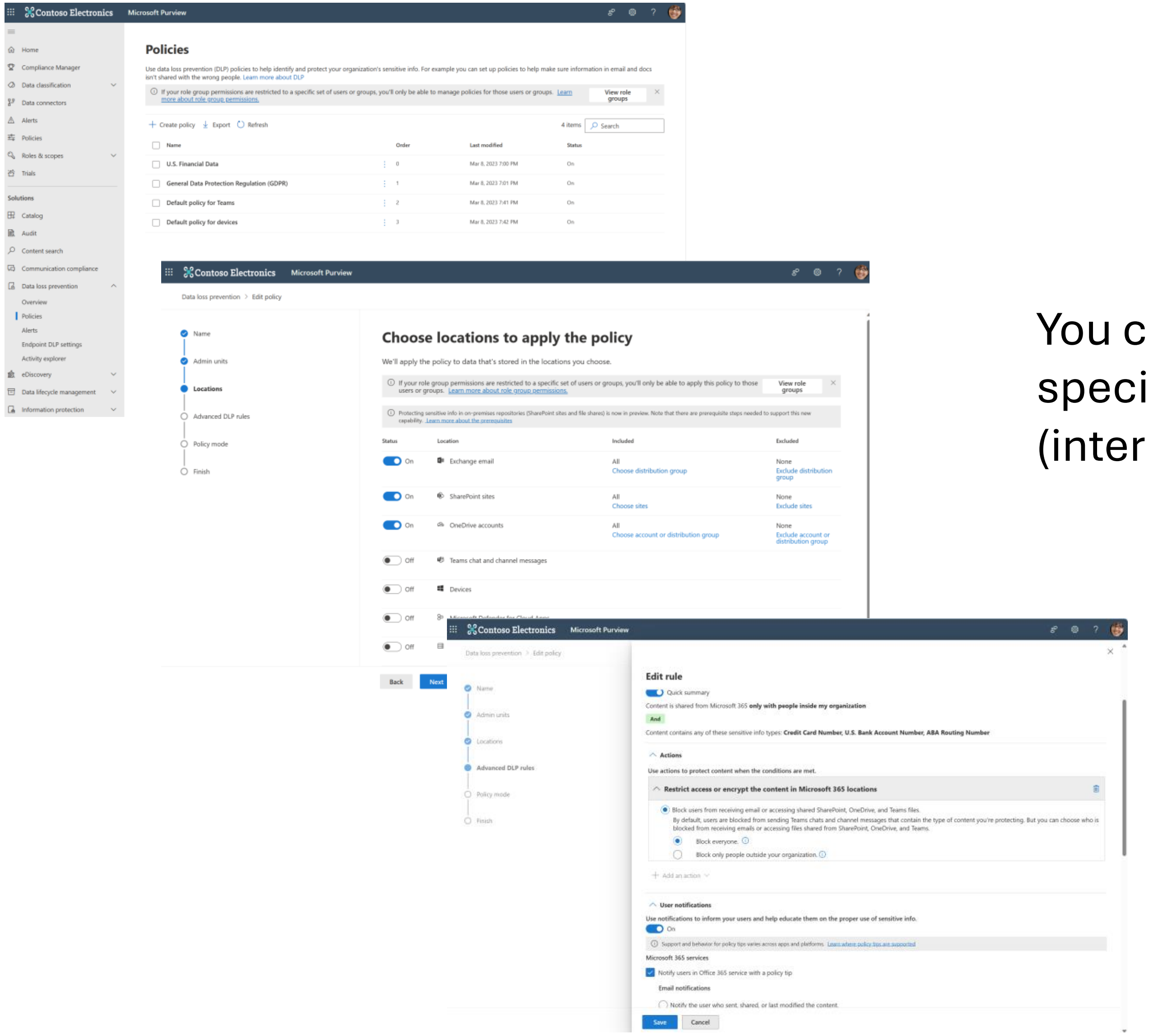
To explore a particular category, click on it to see all the matching documents and files and the locations.

20 items

Name	SharePoint	OneDrive
Healthcare	3	0
U.S. Social Security Number (SSN)	10	23
U.S. Physical Addresses	130	1
International Classification of Dis...	552	1
All Medical Terms And Conditions	1204	11
All Full Names	3517	186
Project documents	1	0
Business plan	1	0
IP	4	1
Strategic planning documents	39	0
Customer Complaints	1	0
Statement of Work	1333	0
Tax	9	3

In Data Loss Prevention, you can also review the content associated to sensitive info types.
You can explore the content associated to each sensitive info type (redirecting to the content explorer of Data Classification)

Data Loss Prevention



Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

4 items

Name	Order	Last modified	Status
U.S. Financial Data	0	Mar 8, 2023 7:00 PM	On
General Data Protection Regulation (GDPR)	1	Mar 8, 2023 7:01 PM	On
Default policy for Teams	2	Mar 8, 2023 7:41 PM	On
Default policy for devices	3	Mar 8, 2023 7:42 PM	On

Choose locations to apply the policy

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

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. Learn more about role group permissions.

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
On	Exchange email	All Choose distribution group	None Exclude distribution group
On	SharePoint sites	All Choose sites	None Exclude sites
On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
Off	Teams chat and channel messages		
Off	Devices		
Off	Microsoft Defender for Cloud Apps		
Off			

Edit rule

Quick summary

Content is shared from Microsoft 365 **only with people inside my organization**

And

Content contains any of these sensitive info types: **Credit Card Number, U.S. Bank Account Number, ABA Routing Number**

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.
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.

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.

You can use Data Loss Prevention policies to apply specific rules when a sensitive content is shared (internally or externally), like blocking the content sharing

Microsoft 365 Copilot
Data Security & Governance

Fredrik Haventon

Technical Specialist Manager – Security & Compliance