Trainable Classifiers

Bringing machine learning to data classification

Know your Data

What methods can I use to classify my data?

Where can I classify my data?

How can I see what happens to my data over its lifecycle?

Flexible options to know your data

Understand what's sensitive, what's business critical & across your environment

Scanner: Spanning on-premises to cloud

Content explorer

Use built-in classification methods

Activity explorer

Auto-classification using trainable classifiers

Trainable classifiers

Leverage machine learning to automatically classify unique data

Built-in

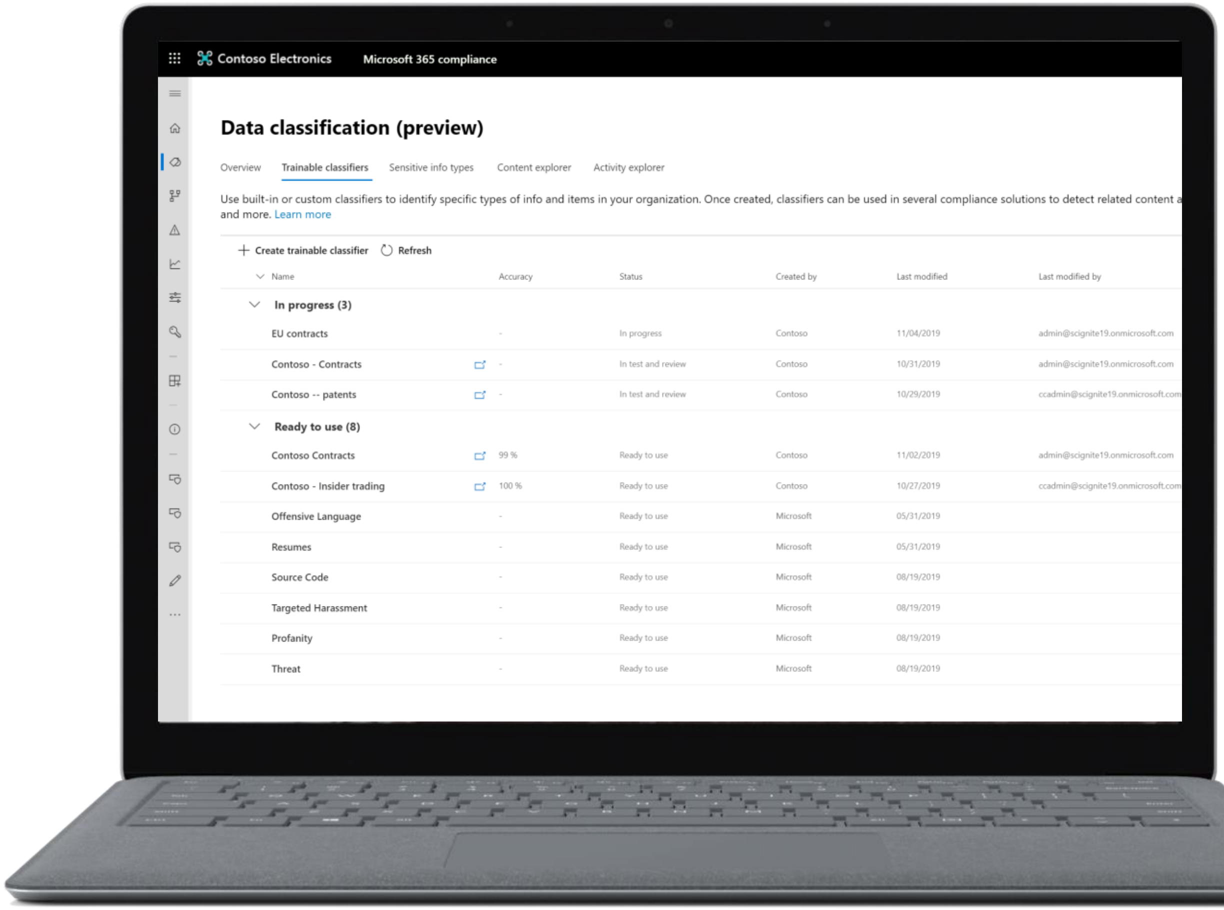
Resume, source code, and more provided out-of-box

Build-your-own

Train the system to look for specific types of data

Integrated

Attach to sensitivity and retention labels and Communication Compliance with associated policies



Data classification (preview)

Use built-in or custom classifiers to identify specific types of info and items in your organization. Once created, classifiers can be used in several compliance solutions to detect related content a and more. Learn more

Name	Accuracy	Status	Created by	Last modified	Last modified by
In progress (3)					
EU contracts	-	In progress	Contoso	11/04/2019	admin@scignite19.onmicrosoft.com
Contoso - Contracts	-	In test and review	Contoso	10/31/2019	admin@scignite19.onmicrosoft.com
Contoso -- patents	-	In test and review	Contoso	10/29/2019	ccadmin@scignite19.onmicrosoft.com
Ready to use (8)					
Contoso Contracts	99 %	Ready to use	Contoso	11/02/2019	admin@scignite19.onmicrosoft.com
Contoso - Insider trading	100 %	Ready to use	Contoso	10/27/2019	ccadmin@scignite19.onmicrosoft.com
Offensive Language	-	Ready to use	Microsoft	05/31/2019	
Resumes	-	Ready to use	Microsoft	05/31/2019	
Source Code	-	Ready to use	Microsoft	08/19/2019	
Targeted Harassment	-	Ready to use	Microsoft	08/19/2019	
Profanity	-	Ready to use	Microsoft	08/19/2019	
Threat	-	Ready to use	Microsoft	08/19/2019	

5 Built-in Classifiers

Resume: Detects written accounts of an applicant's personal, educational, and professional qualifications and experience

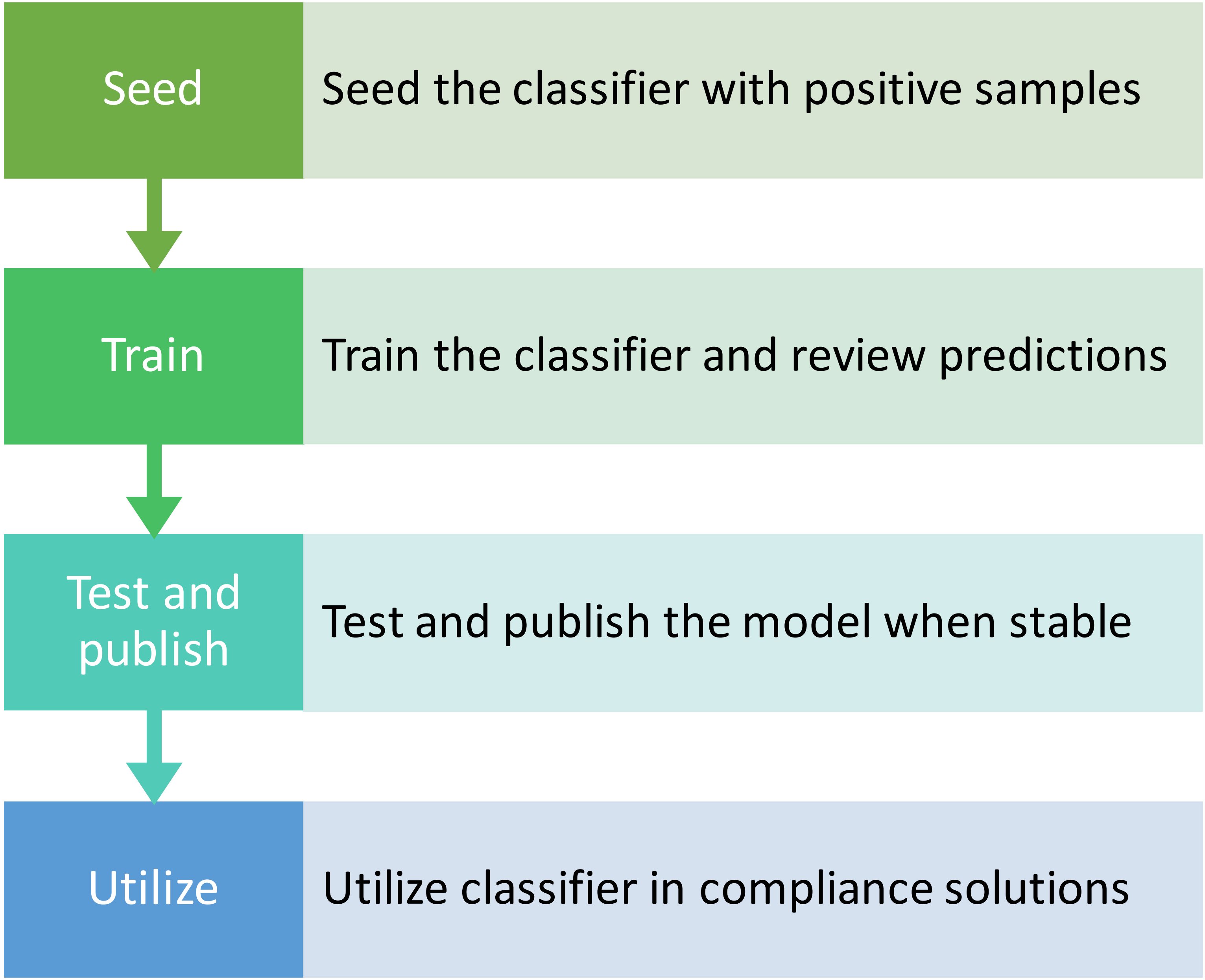
Source Code: Detects a set of instructions and statements written in the top 25 computer programming languages of GitHub

Threat: Detects a specific category of offensive language related to threats to commit violence or do physical harm/damage to a person/property

Harassment: Detects a specific category of offensive language related to offensive conduct targeting one or multiple individuals regarding race, color, religion, national origin, gender, sexual orientation, age, disability and genetic information

Profanity: Detects a specific category of offensive language that contains swear words or vulgar language

Build your own trainable classifier



Seed – Seed the classifier with positive samples

Train – Train the classifier and review predictions

Test and publish – Test and publish the model when stable

Utilize – Utilize classifier in compliance solutions

Sample categories

Legal documents

- Attorney Client Privilege
- Closing Sets
- Statement of Work

Strategic business documents

- Merger & Acquisition
- Deals
- Business plans
- Marketing plans
- Intellectual Property
- Patents
- Database information
- Software design documents

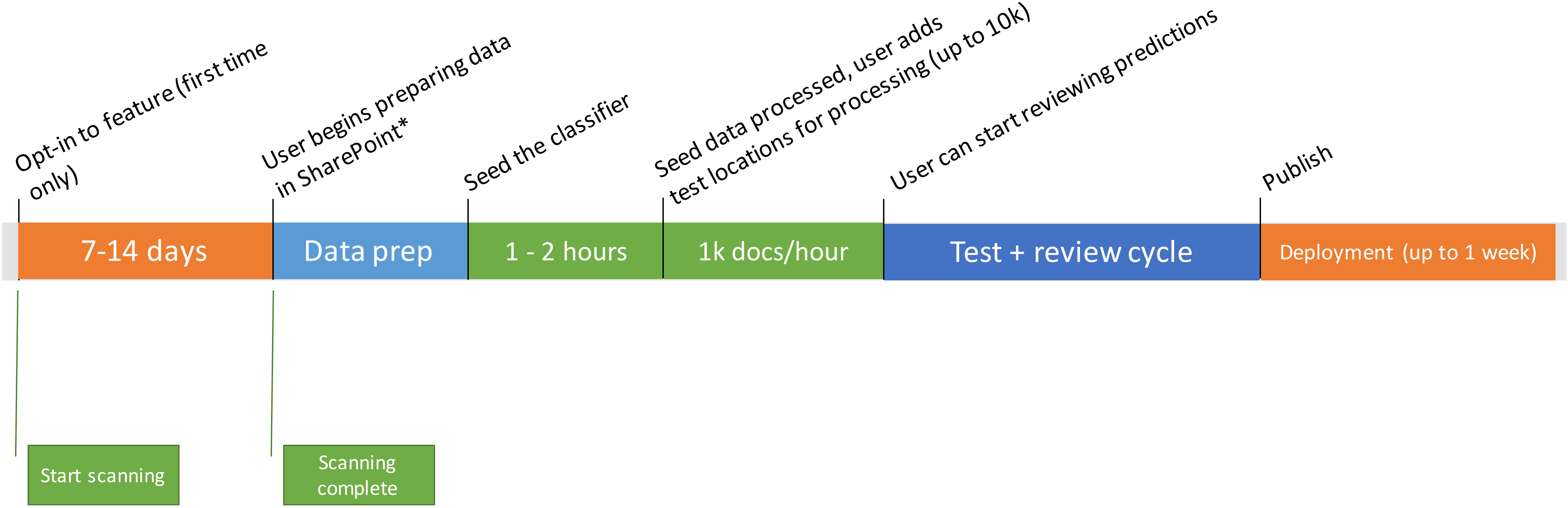
Pricing information

- Quotation
- Work orders
- Bidding documents
- Pricelist

Financial information

- Organizational investments
- Quarterly or annual results

Custom classifier timelines



Opt-in to feature (first time only)

User begins preparing data in SharePoint*

Seed the classifier

Seed data processed, user adds test locations for processing (up to 10k)

User can start reviewing predictions

Publish

7-14 days

Data prep

1 - 2 hours

1k docs/hour

Test + review cycle

Deployment (up to 1 week)

Start scanning

Scanning complete

*During **Data prep**, indexing a new SharePoint site and/or files can take up to 1 day.

Trainable classifiers

Leverage machine learning to automatically classify unique data

Built-in

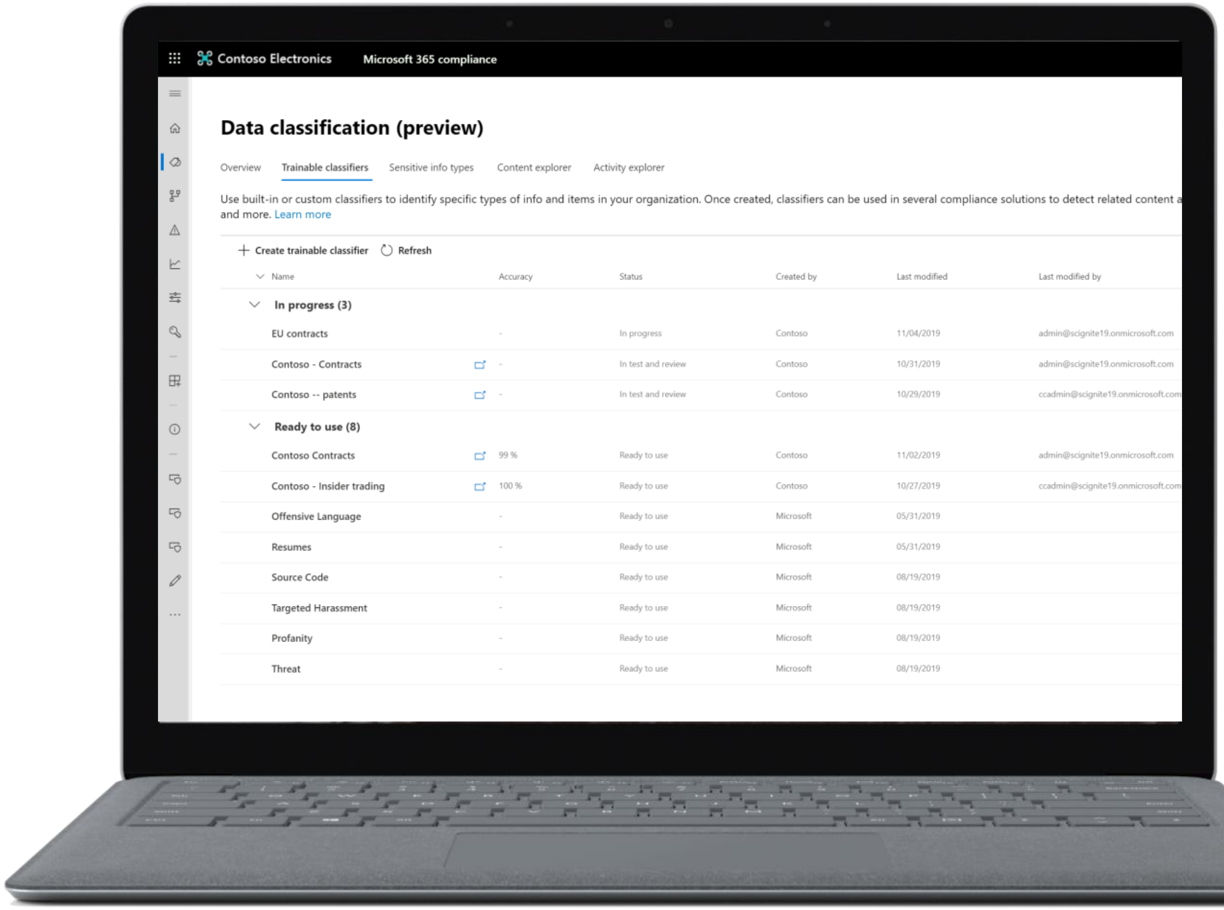
Resume, source code, and more provided out-of-box

Build-your-own

Train the system to look for specific types of data

Integrated

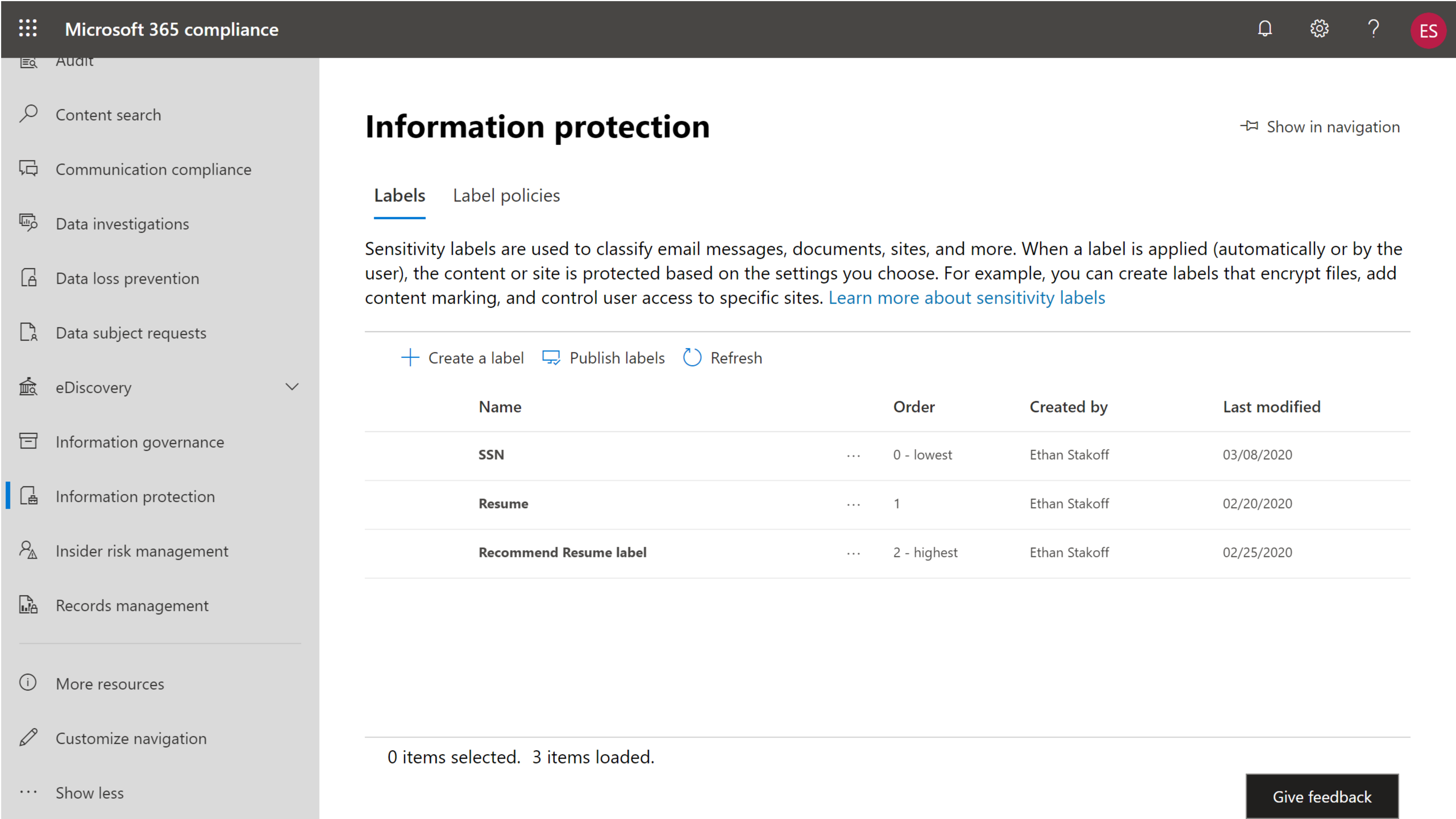
Attach to sensitivity and retention labels and Communication Compliance with associated policies



Data classification (preview)

Use built-in or custom classifiers to identify specific types of info and items in your organization. Once created, classifiers can be used in several compliance solutions to detect related content a and more. Learn more

Name	Accuracy	Status	Created by	Last modified	Last modified by
In progress (3)					
EU contracts	-	In progress	Contoso	11/04/2019	admin@scignite19.onmicrosoft.com
Contoso - Contracts	-	In test and review	Contoso	10/31/2019	admin@scignite19.onmicrosoft.com
Contoso -- patents	-	In test and review	Contoso	10/29/2019	ccadmin@scignite19.onmicrosoft.com
Ready to use (8)					
Contoso Contracts	99 %	Ready to use	Contoso	11/02/2019	admin@scignite19.onmicrosoft.com
Contoso - Insider trading	100 %	Ready to use	Contoso	10/27/2019	ccadmin@scignite19.onmicrosoft.com
Offensive Language	-	Ready to use	Microsoft	05/31/2019	
Resumes	-	Ready to use	Microsoft	05/31/2019	
Source Code	-	Ready to use	Microsoft	08/19/2019	
Targeted Harassment	-	Ready to use	Microsoft	08/19/2019	
Profanity	-	Ready to use	Microsoft	08/19/2019	
Threat	-	Ready to use	Microsoft	08/19/2019	

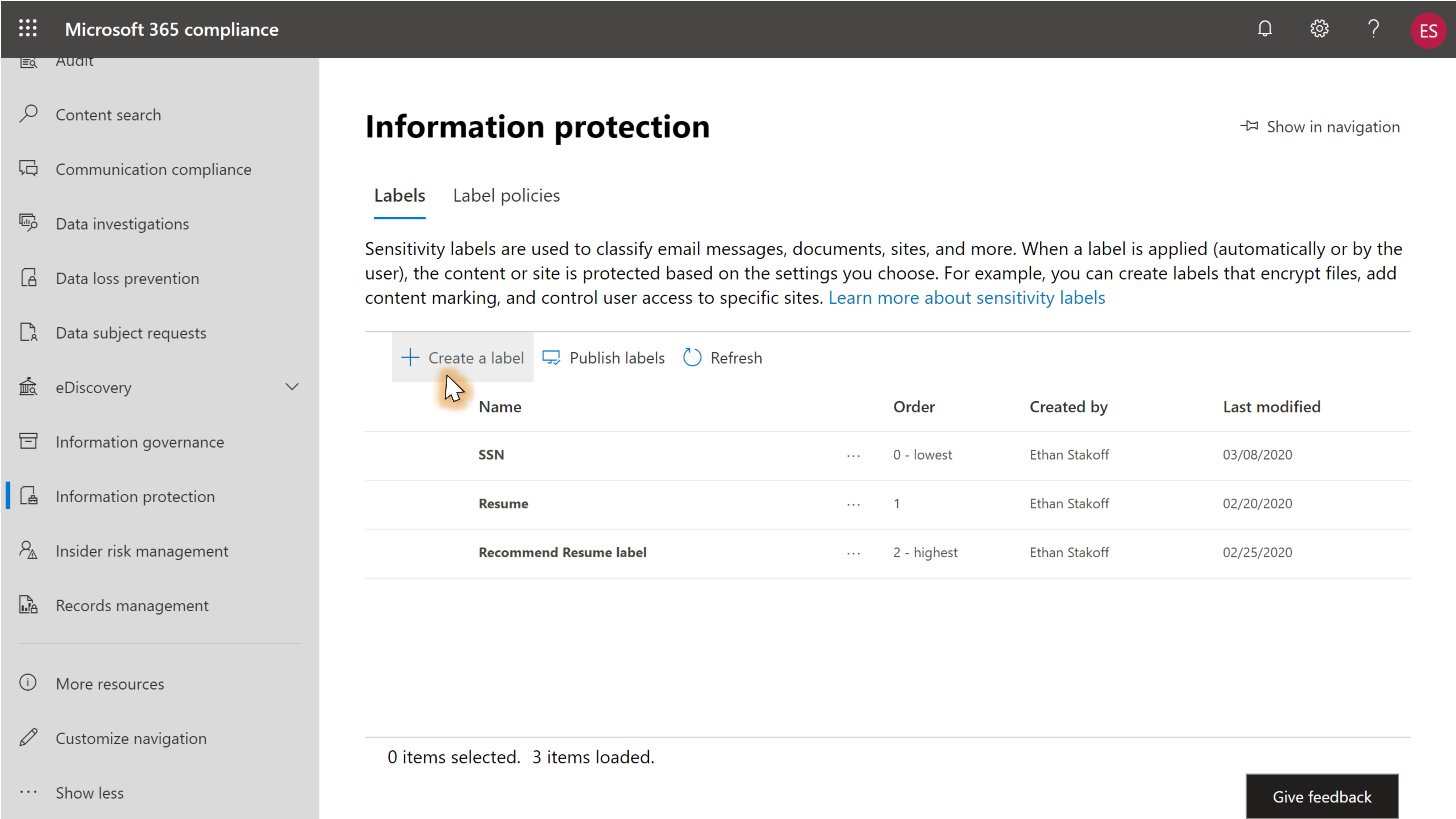


Information protection

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

Name		Order	Created by	Last modified
SSN	···	0 - lowest	Ethan Stakoff	03/08/2020
Resume	···	1	Ethan Stakoff	02/20/2020
Recommend Resume label	···	2 - highest	Ethan Stakoff	02/25/2020

0 items selected. 3 items loaded.

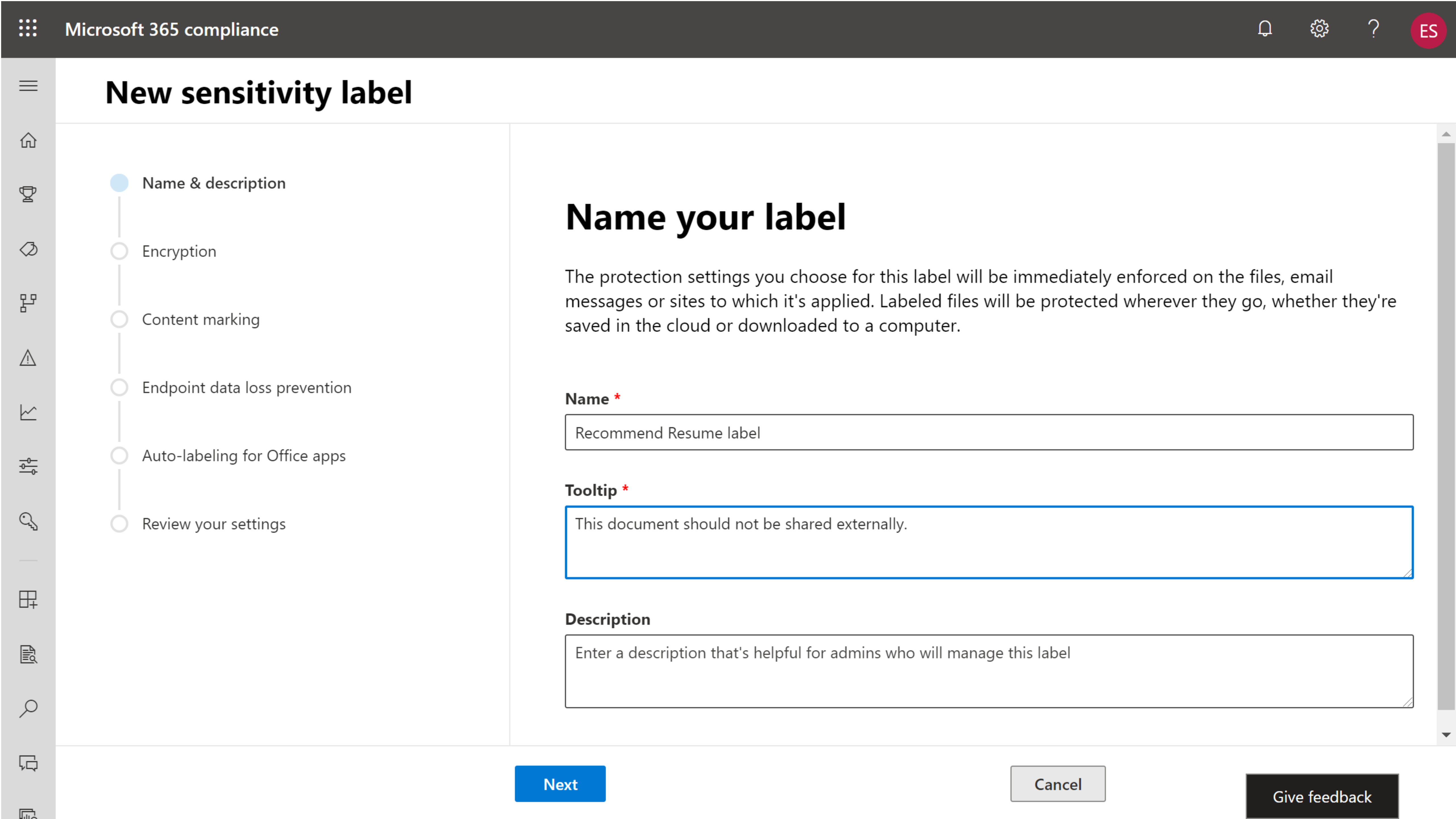


Information protection

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

Name		Order	Created by	Last modified
SSN	···	0 - lowest	Ethan Stakoff	03/08/2020
Resume	···	1	Ethan Stakoff	02/20/2020
Recommend Resume label	···	2 - highest	Ethan Stakoff	02/25/2020

0 items selected. 3 items loaded.



New sensitivity label

Name your label

The protection settings you choose for this label will be immediately enforced on the files, email messages or sites to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name *

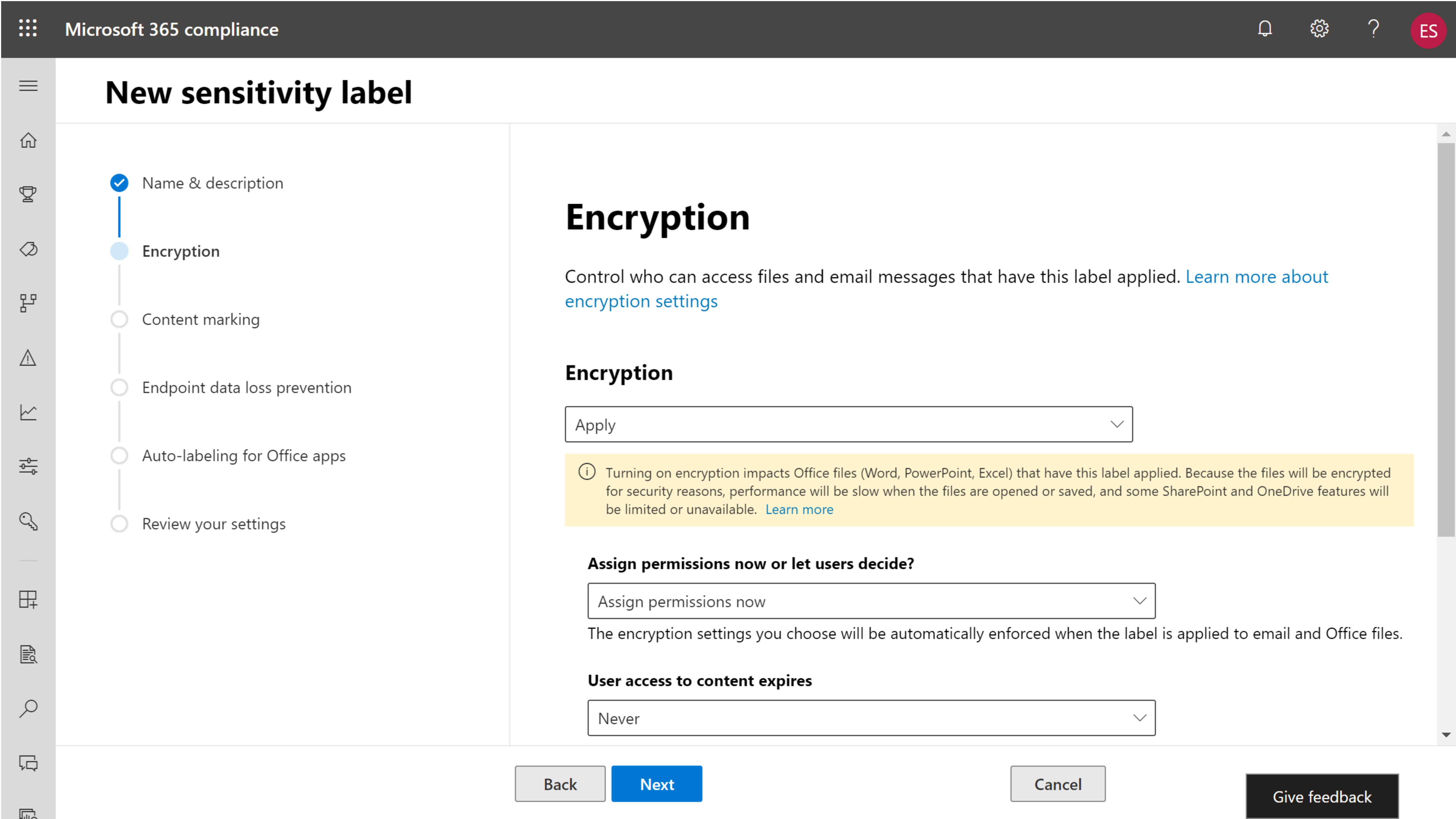
Recommend Resume label

Tooltip *

This document should not be shared externally.

Description

Enter a description that's helpful for admins who will manage this label



New sensitivity label

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

Encryption

Apply

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) 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

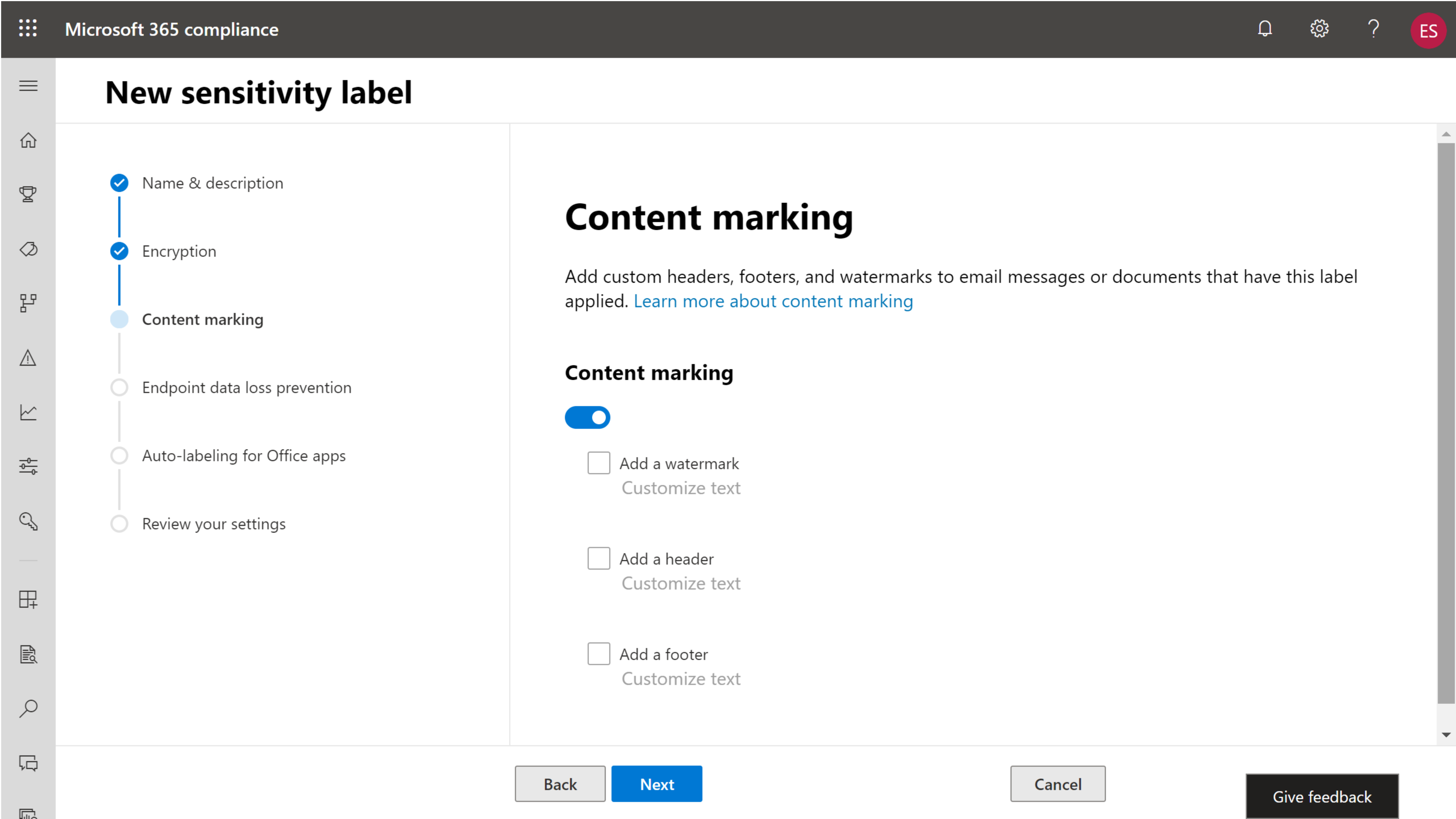
Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Never



New sensitivity label

- ✓ Name & description
- ✓ Encryption
- ● Content marking
- ○ Endpoint data loss prevention
- ○ Auto-labeling for Office apps
- ○ Review your settings

Content marking

Add custom headers, footers, and watermarks to email messages or documents that have this label applied. Learn more about content marking

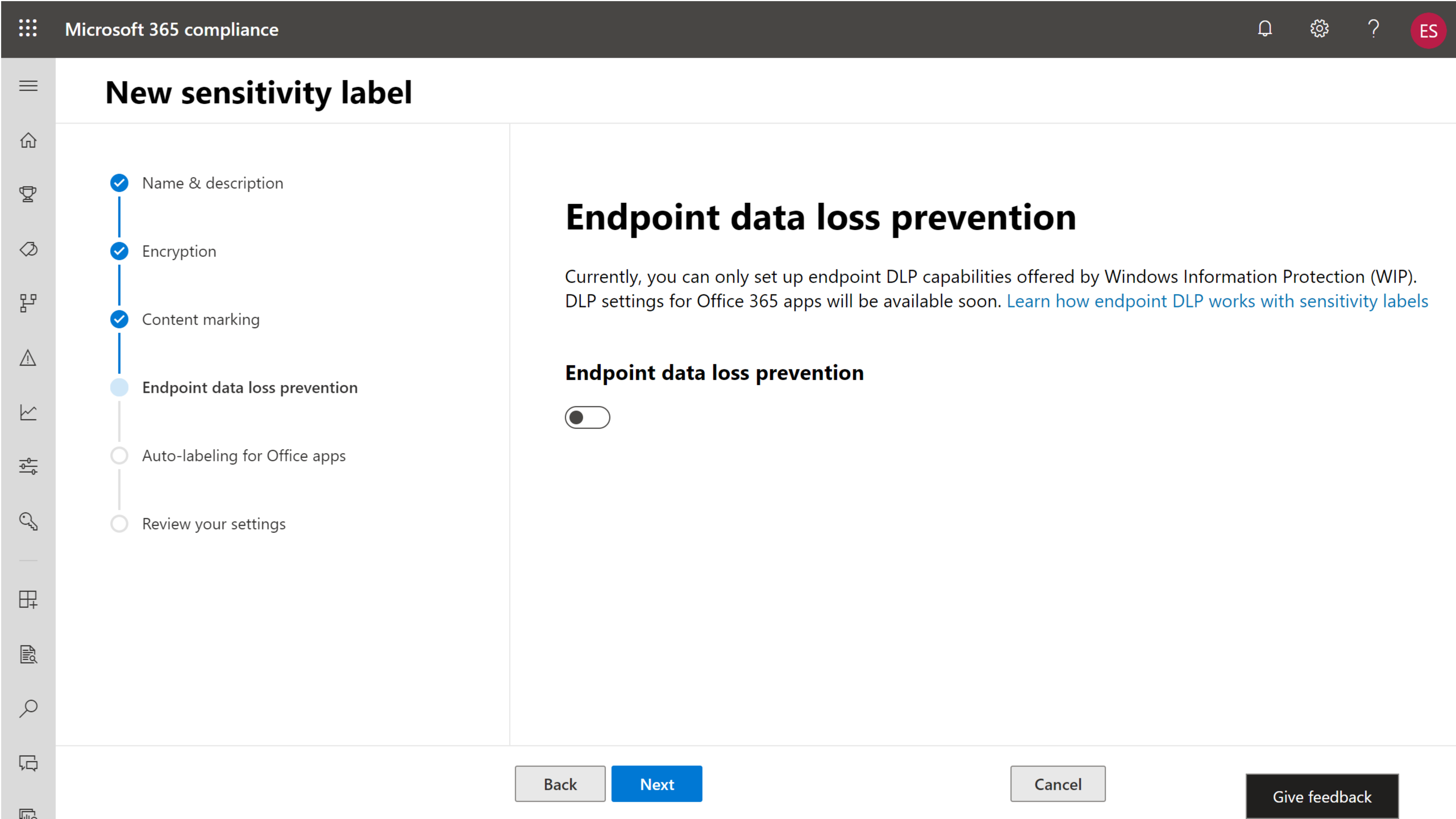
Content marking

● On

□ Add a watermark
Customize text

□ Add a header
Customize text

□ Add a footer
Customize text



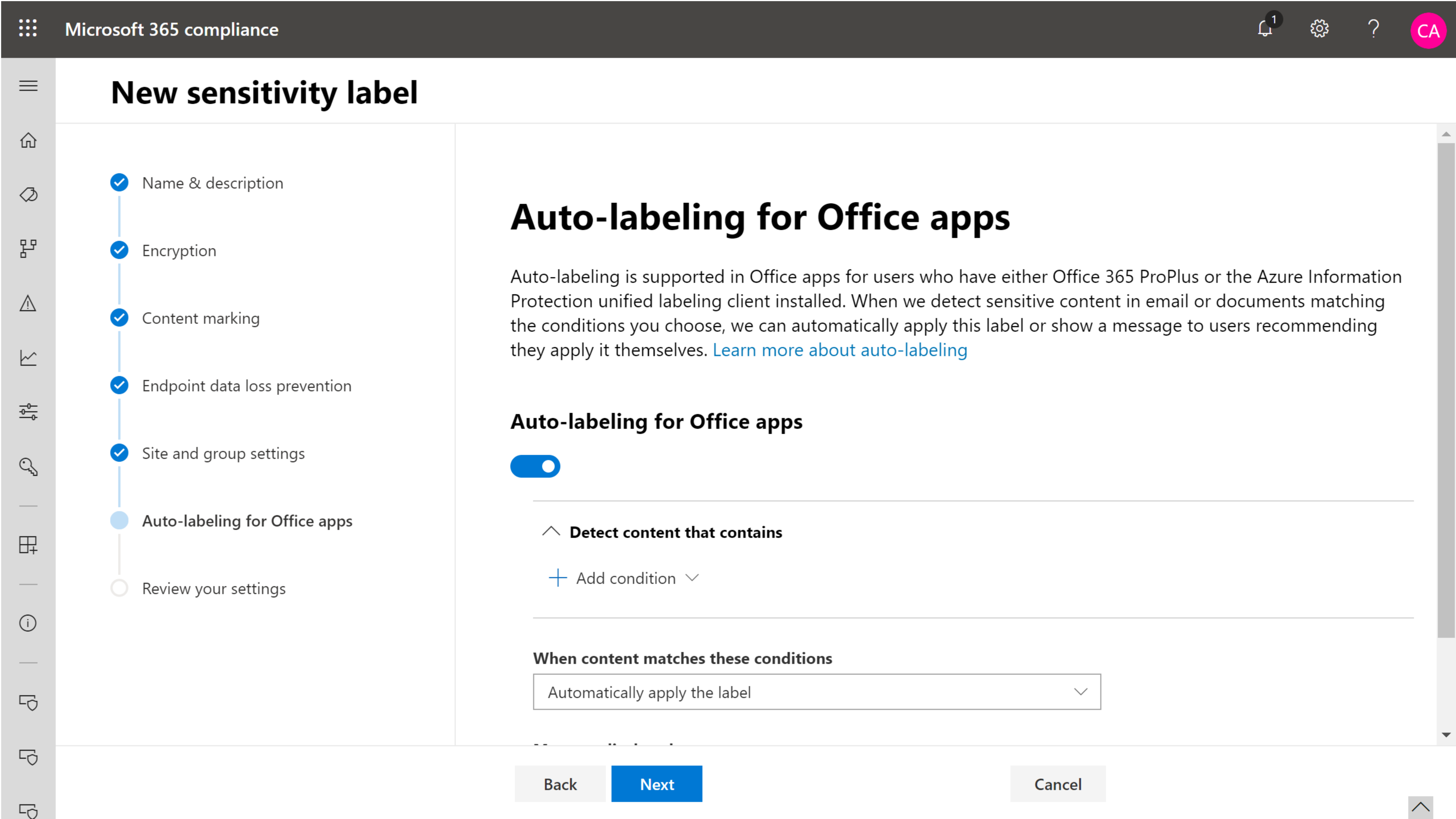
New sensitivity label

Endpoint data loss prevention

Currently, you can only set up endpoint DLP capabilities offered by Windows Information Protection (WIP). DLP settings for Office 365 apps will be available soon. Learn how endpoint DLP works with sensitivity labels

Endpoint data loss prevention

○ Off



Microsoft 365 compliance

New sensitivity label

- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ✓ Endpoint data loss prevention
- ✓ Site and group settings
- ● Auto-labeling for Office apps
- ○ Review your settings

Auto-labeling for Office apps

Auto-labeling is supported in Office apps for users who have either Office 365 ProPlus or the Azure Information Protection unified labeling client installed. When we detect sensitive content in email or documents matching the conditions you choose, we can automatically apply this label or show a message to users recommending they apply it themselves. Learn more about auto-labeling

Auto-labeling for Office apps

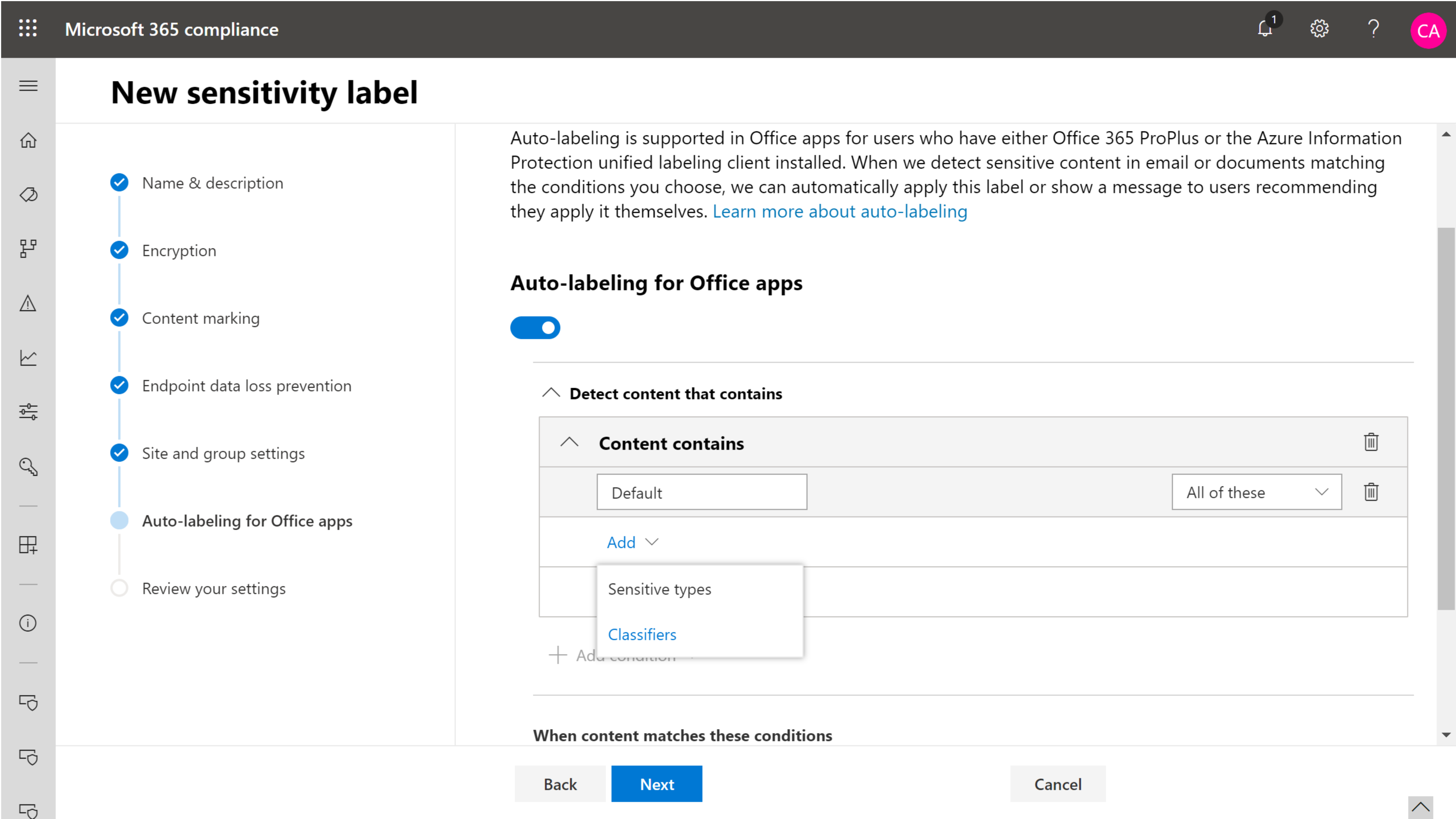
●

Detect content that contains

+ Add condition

When content matches these conditions

Automatically apply the label



New sensitivity label

- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ✓ Endpoint data loss prevention
- ✓ Site and group settings
- ● **Auto-labeling for Office apps**
- ○ Review your settings

Auto-labeling is supported in Office apps for users who have either Office 365 ProPlus or the Azure Information Protection unified labeling client installed. When we detect sensitive content in email or documents matching the conditions you choose, we can automatically apply this label or show a message to users recommending they apply it themselves. Learn more about auto-labeling

Auto-labeling for Office apps

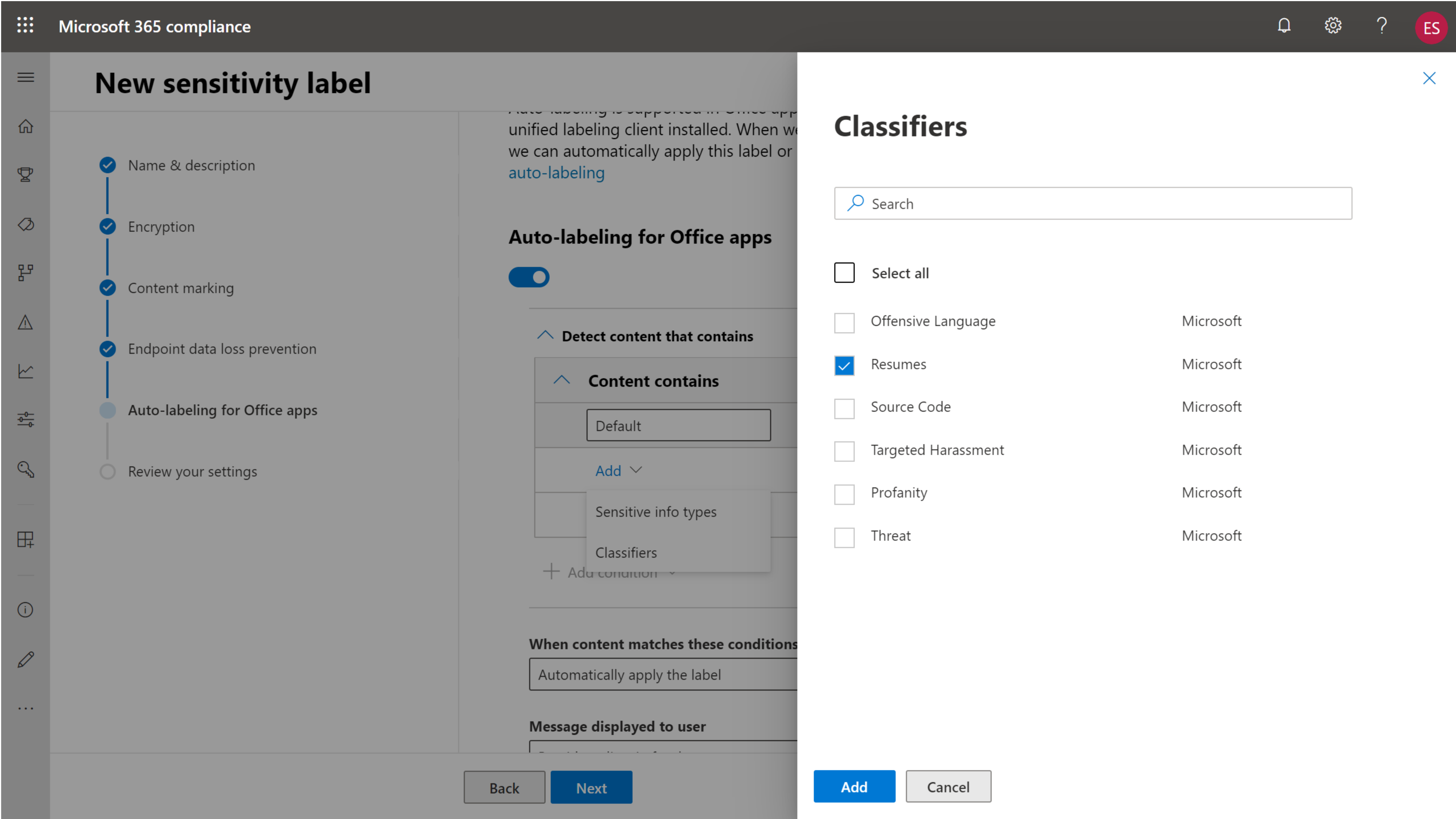
Detect content that contains

Content contains

Default

All of these

When content matches these conditions



Microsoft 365 compliance

ES

New sensitivity label

- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ✓ Endpoint data loss prevention
- ● Auto-labeling for Office apps
- ○ Review your settings

Auto-labeling is supported in Office app
unified labeling client installed. When we
we can automatically apply this label or
auto-labeling

Auto-labeling for Office apps

Detect content that contains

Content contains

Default

Add

Sensitive info types

Classifiers

+ Add condition

When content matches these conditions

Automatically apply the label

Message displayed to user

Back

Next

Classifiers

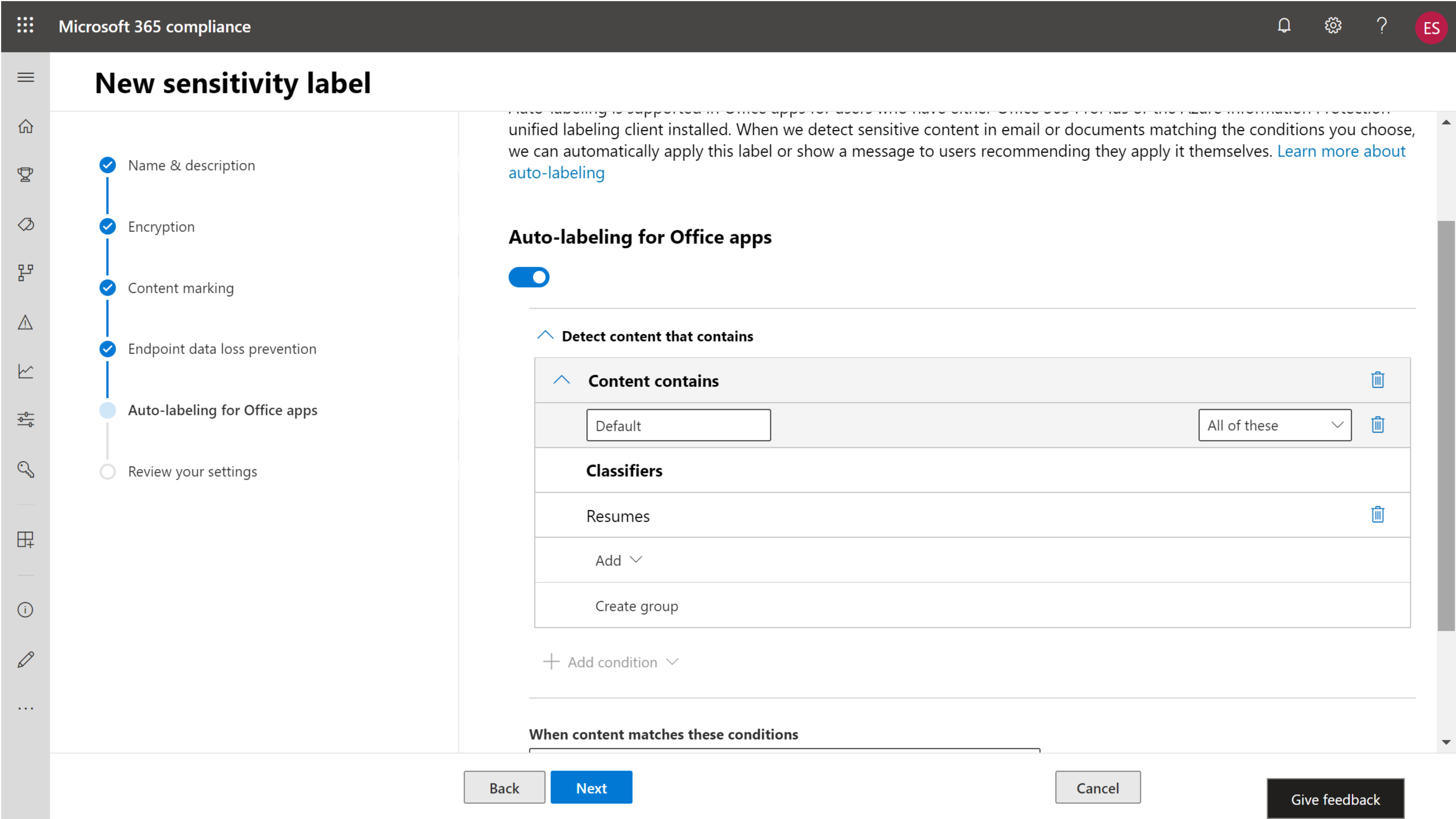
Search

□ Select all

□	Offensive Language	Microsoft
☑	Resumes	Microsoft
□	Source Code	Microsoft
□	Targeted Harassment	Microsoft
□	Profanity	Microsoft
□	Threat	Microsoft

Add

Cancel



New sensitivity label

- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ✓ Endpoint data loss prevention
- ● Auto-labeling for Office apps
- ○ Review your settings

Auto-labeling is supported in Office apps for users who have either Office 365 ProPlus or the Azure Information Protection unified labeling client installed. When we detect sensitive content in email or documents matching the conditions you choose, we can automatically apply this label or show a message to users recommending they apply it themselves. Learn more about auto-labeling

Auto-labeling for Office apps

● On

Detect content that contains

Content contains

Default — All of these

Classifiers

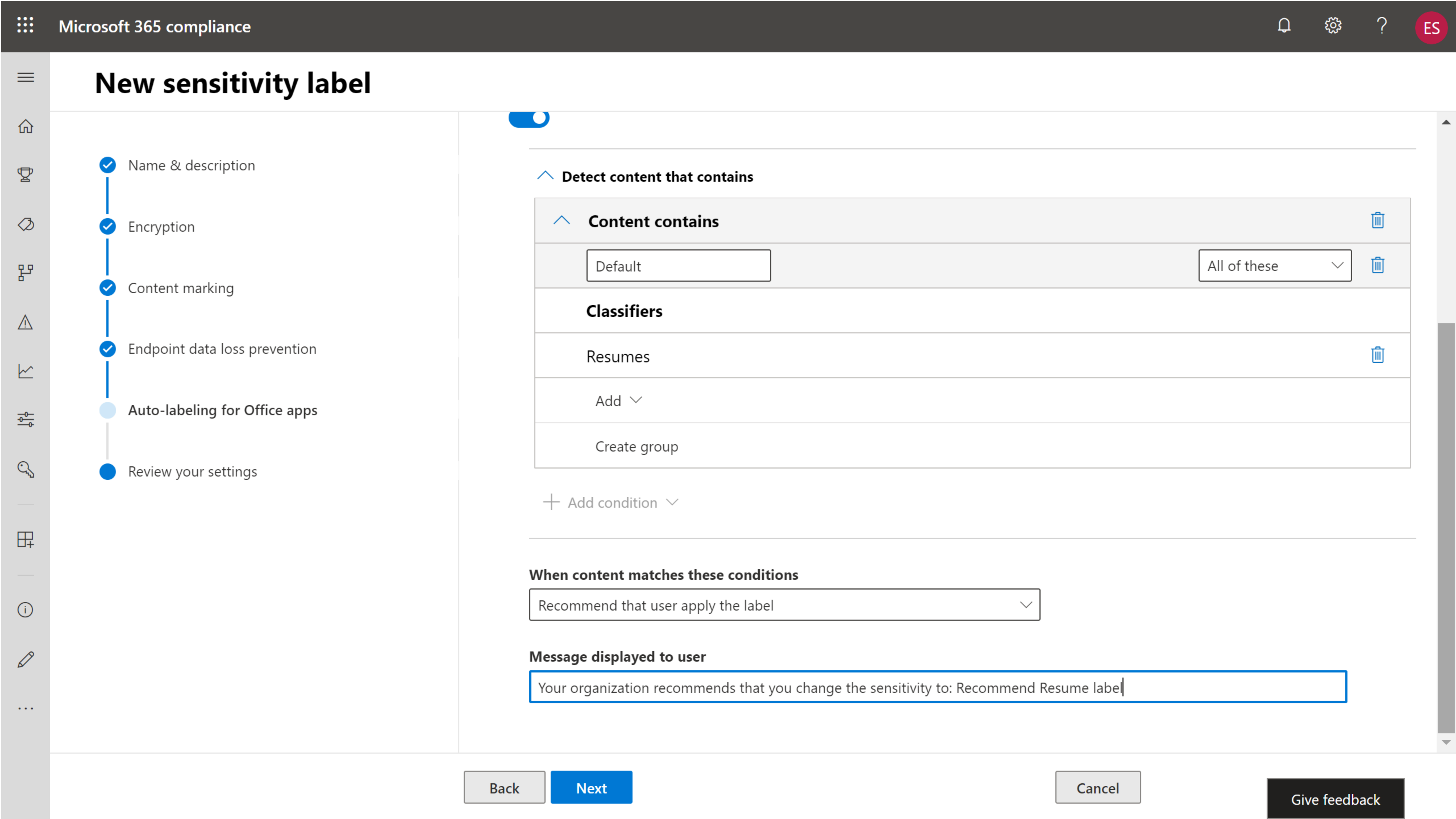
Resumes

Add

Create group

+ Add condition

When content matches these conditions



New sensitivity label

Detect content that contains

Content contains

Default — All of these

Classifiers

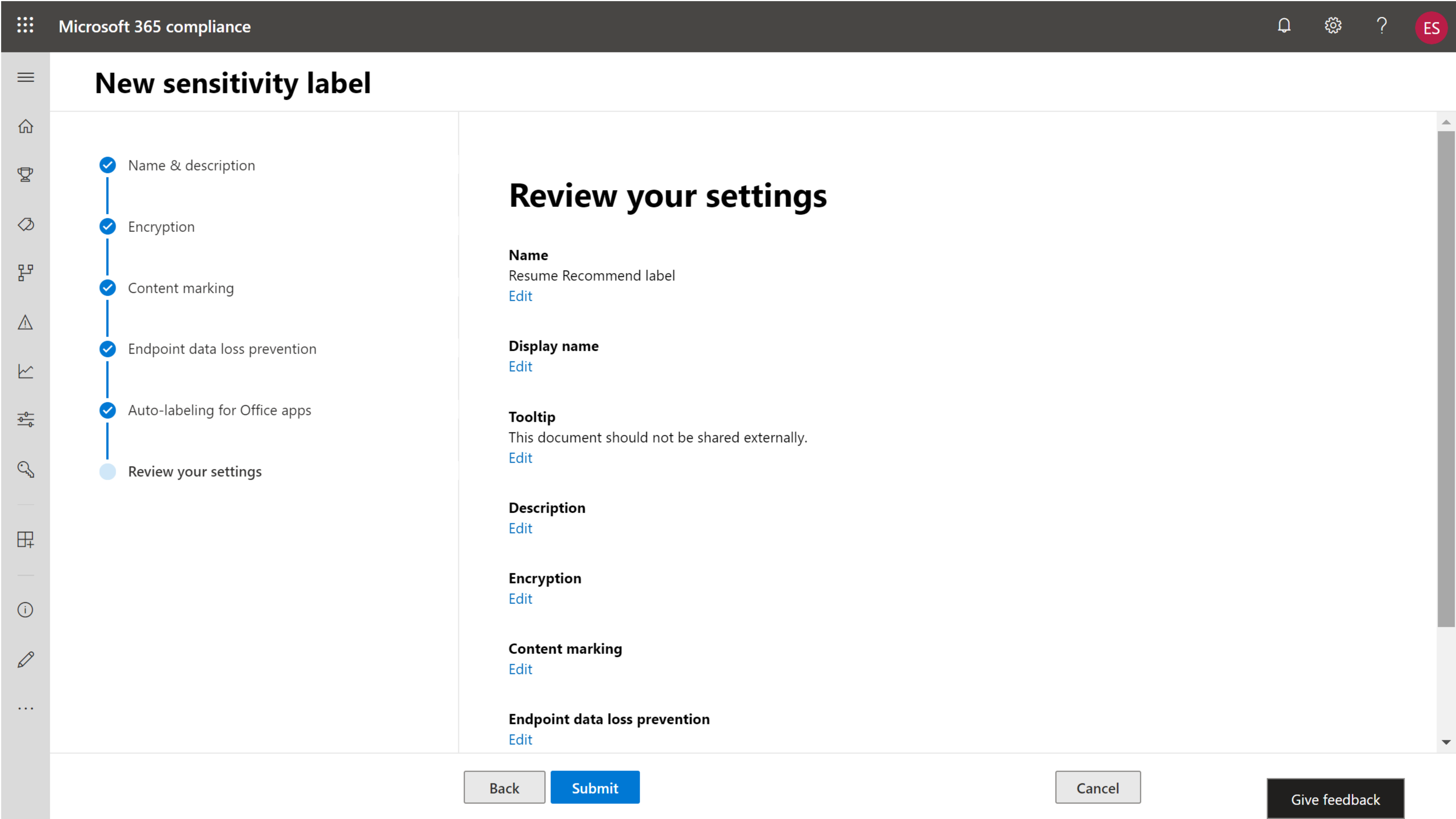
Resumes

When content matches these conditions

Recommend that user apply the label

Message displayed to user

Your organization recommends that you change the sensitivity to: Recommend Resume label



New sensitivity label

Review your settings

Name
Resume Recommend label
Edit

Display name
Edit

Tooltip
This document should not be shared externally.
Edit

Description
Edit

Encryption
Edit

Content marking
Edit

Endpoint data loss prevention
Edit

Microsoft

What’s in it for customers?

Show slides on how the classifier is used in Comms Comp, Retention labels, Sensitivity labels, and Analytics

Microsoft

Join private preview for trainable classifiers in MIP

Fill out the survey here: https://aka.ms/MLSensitivityLabelsPreviewConsent
Follow MIP previews: https://aka.ms/MIPC/Previews
Tech Community Resources: https://aka.ms/MIPC/TechCommunity
Follow us on Twitter @MIPnews