

Protect your data with Microsoft Purview Information Protection and Data Loss Prevention



Ehsan Eskandari

Microsoft Azure MVP

Metro Toronto Azure Community October 5, 2023 Microsoft Canada

About me: Ehsan Eskandari



Senior Consultant

B.S. & M.Sc. Software Engineering



http://passionatecoder.ca



@EhsanEskandarim



Ehsan. Eskandari@BuildOnCloud.net



Microsoft Microsoft

Solutions Developer

Azure Solutions Architect

Solutions Expert

Cloud Platform and Infrastructure

Specialist

Developing Microsoft Azure Solutions



Az-220, Az-203, Data Analyst



Part of Azure Tech Communities - 222 groups

Metro Toronto .NET User Group

(Toronto, ON

2,807 members · Public group @

Organized by Ehsan E. and 6 others

Share: 🚹 🄰 🛅



Part of .NET Foundation - 354 groups

Toronto .NET Meetup

(Toronto, ON

2,496 members · Public group @

Organized by Luca G. and 5 others

Share: 🚹 🍏 🛅

Microsoft Security

| SC-200 | Microsoft Security Operations Analyst | SC200WATERLOO |
|--------|---|---------------|
| SC-300 | Microsoft Identity and Access Administrator | SC300VANDALIA |
| SC-400 | Microsoft Information Protection Administrator | SC400EMPORIA |
| SC-900 | Microsoft Security, Compliance, and Identity Fundamentals | SC900TUPELO |



OR



OR



Take one exam

CERTIFICATION EXAM

Microsoft Cybersecurity Architect



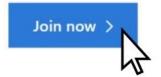
EXPERT CERTIFICATION

Microsoft Certified: Cybersecurity Architect Expert

Development

Microsoft 365

Join the Microsoft 365 Developer Program today!



TRenewable E5 subscription

Expires on Jan 23, 2022

Administrator
ContosoDev@12345.onmicrosoft.com



Users 25 user licenses

Go to subscription

ቆ Sample data packs



Users



Mail & Events

ofi

Microsoft Teams 1년

SharePoint



SharePoint

The most urgent data security challenges





Discover your most valuable asset, your data

Secure configuration to prevent sophisticated attacks

Detect how users are interacting with data and identify insider risks

Ensure your data remains **secure** from **data leakage** and **data exfiltration** activities

Data Security



Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

Fortify data security with Microsoft Purview

Information Protection

- Discover, classify, and protect data at scale, using automation and ML
- Productivity tools with built-in userselectable sensitivity labels for precise controls
- Data is protected (encrypted) across environments, throughout its lifecycle

Insider Risk Management

- Leverage analytics, machine learning, sequencing to understand user context and intent
- Investigate potential incidents with curated, high-quality, and enriched alerts and evidence
- Ensure user privacy while identifying highest risk users

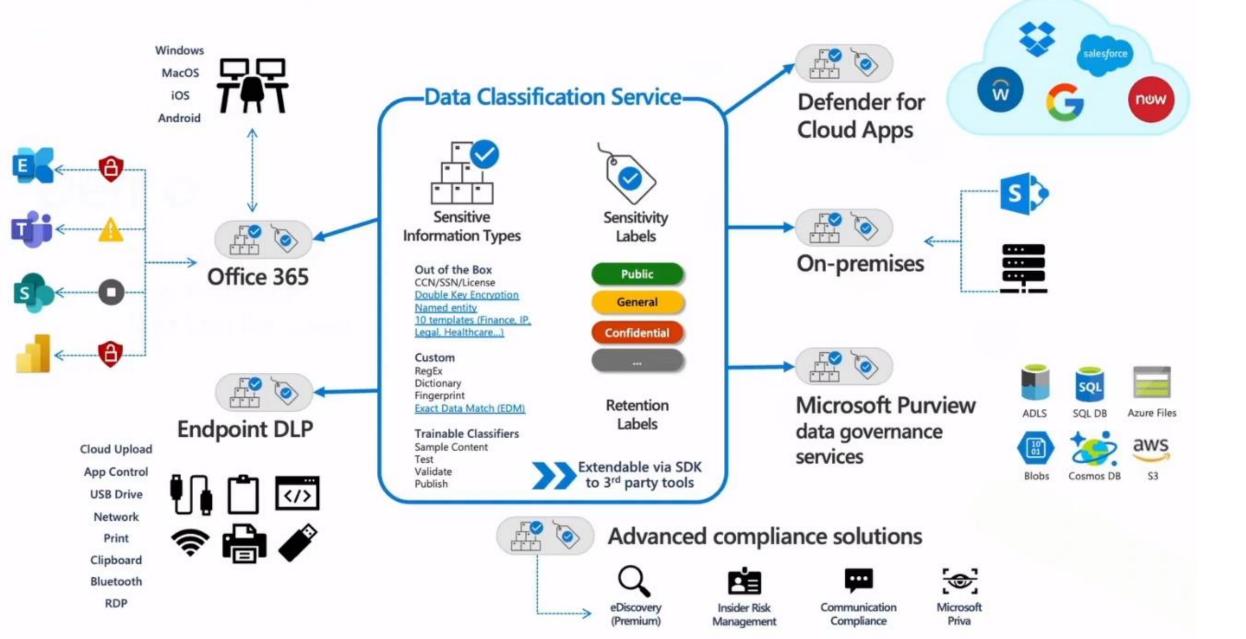
Data Loss Prevention

- Prevent unauthorized use, like improperly saving, storing or printing sensitive data
- Create, deploy, and manage
 DLP policies across all cloud, apps,
 and devices from a single location
- Leverage data classification, labeling, and user insights
 to finetune and adapt DLP policies

Adaptive Protection

Dynamically adjust data security controls based on user risk level

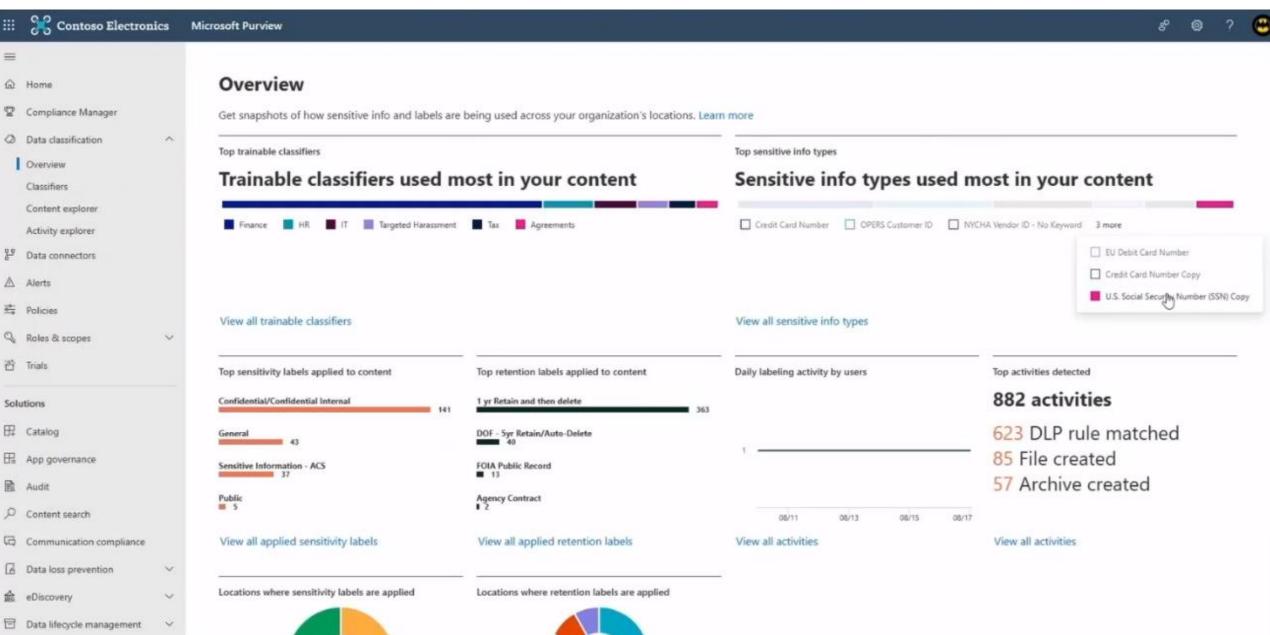
Data Security in Microsoft Purview



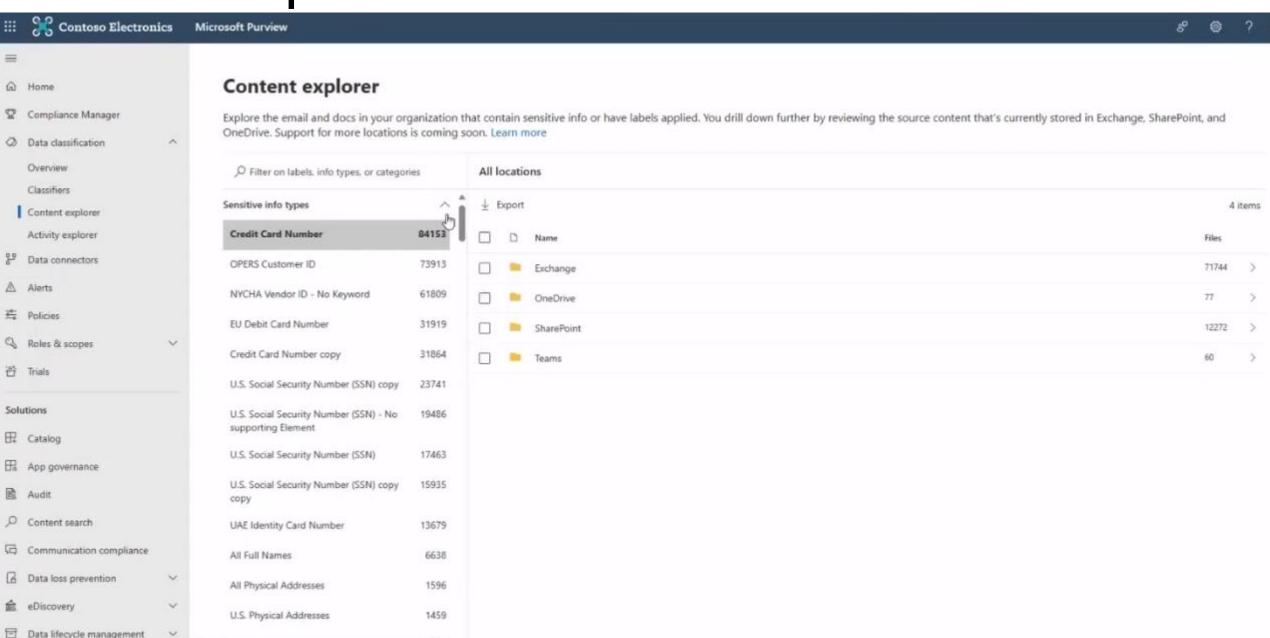
Compliance Portal



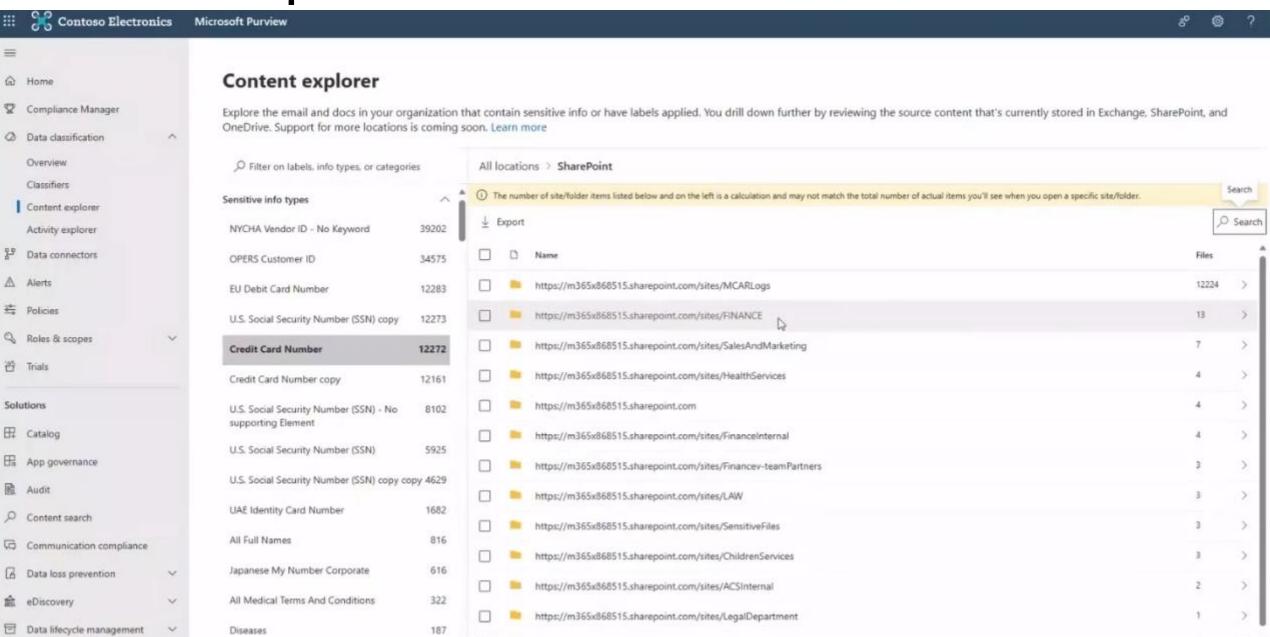
Data Classification Overview



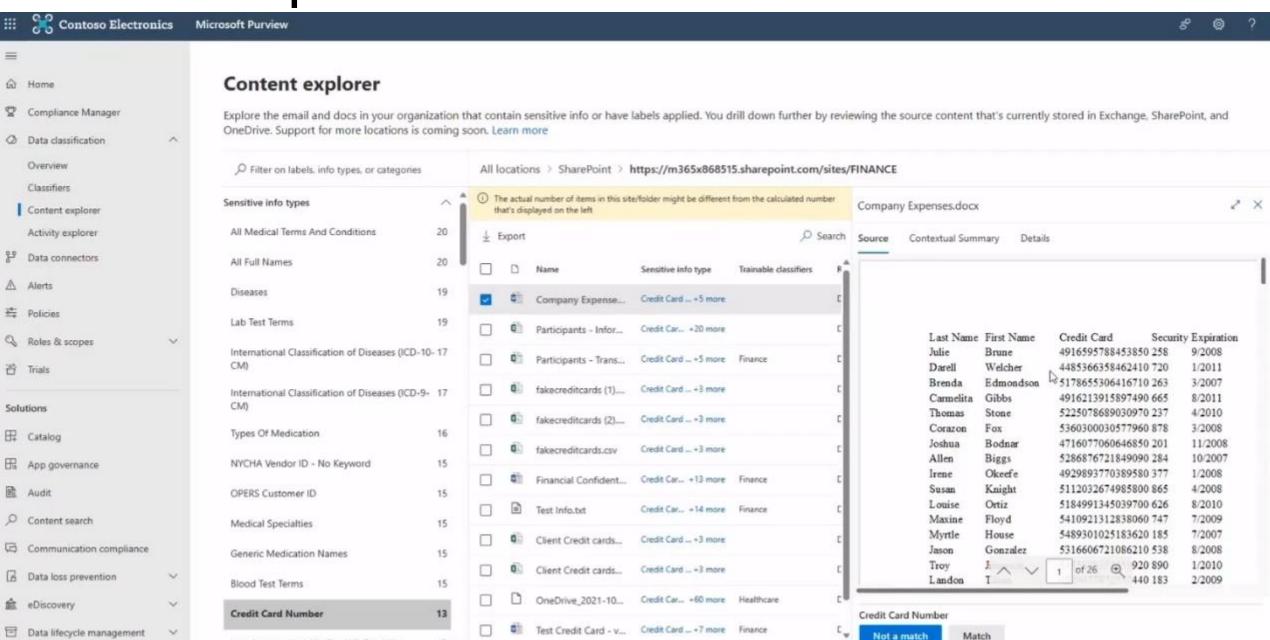
Content Explorer



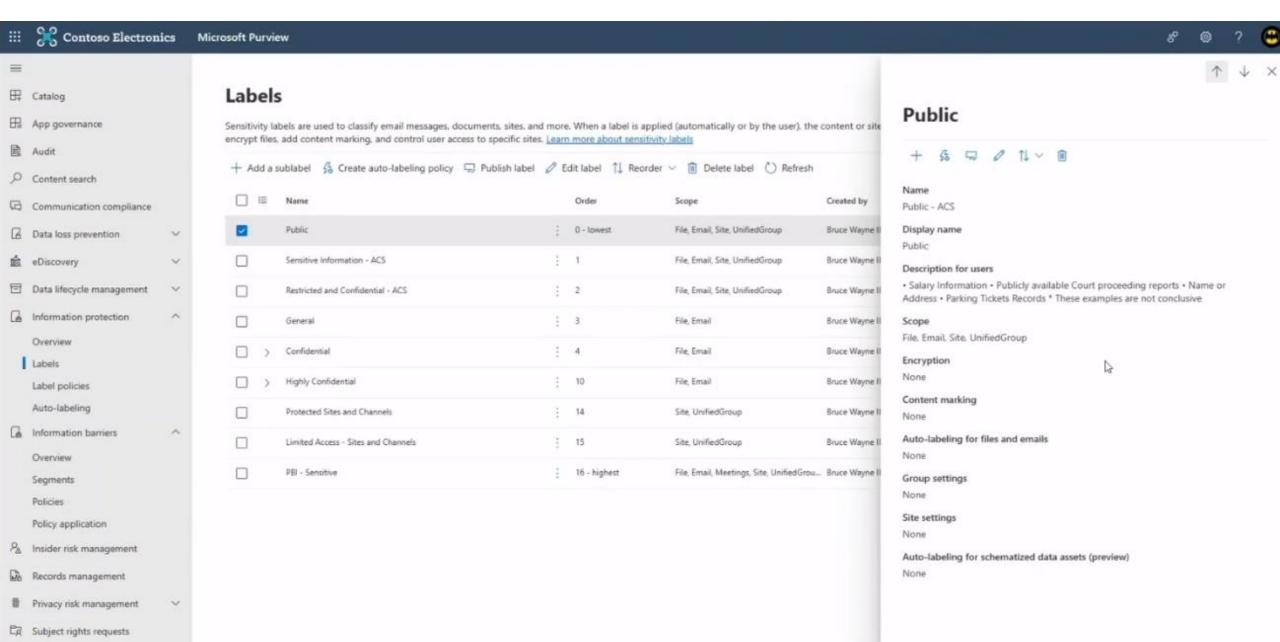
Content Explorer



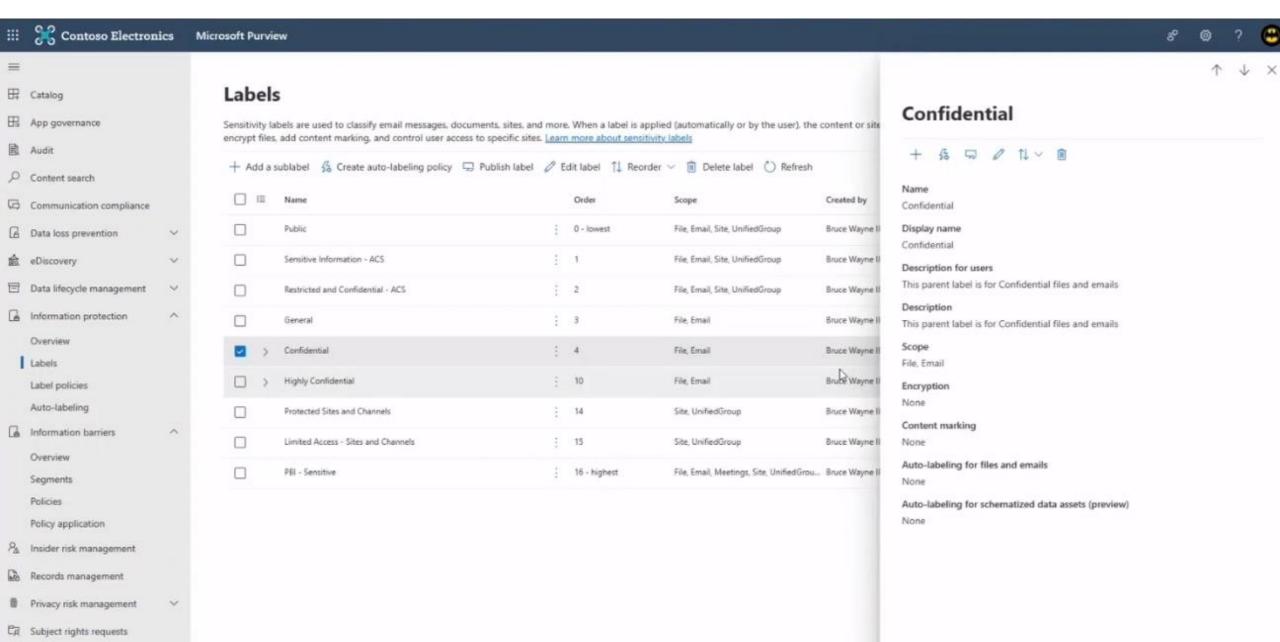
Content Explorer



Information Protection: Public Label



Information Protection: Confidential Label





O Groups & sites

O Finish

Schematized data assets (preview)

| Parent label | |
|--|--|
| Confidential | |
| | |
| Name * ① | |
| Confidential Internal | |
| | |
| Display name * ① | |
| Confidential Internal | |
| Description for users * ① | |
| This label is for internal emploinstances of sensitive informat | byces only. The content will be encrypted and can only be decrypted by internal employees. Content that contains more than the contains more than also will automatically be encrypted. In ployees will be able to access Teams and SharePoint sites. |
| This label is for internal emploinstances of sensitive informat | |
| This label is for internal emploinstances of sensitive informal Additionally, ONLY internal en | tion will automatically be encrypted. |
| This label is for internal emploinstances of sensitive informal Additionally, ONLY internal en | tion will automatically be encrypted. |
| This label is for internal emploinstances of sensitive informal Additionally, ONLY internal en | tion will automatically be encrypted. Inployees will be able to access Teams and SharePoint sites. |
| This label is for internal emploinstances of sensitive informal Additionally, ONLY internal en | tion will automatically be encrypted. Inployees will be able to access Teams and SharePoint sites. |

Information Protection: Edit Label 2



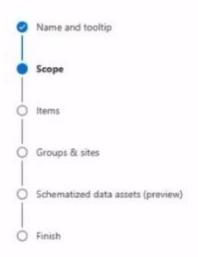
Contoso Electronics

Microsoft Purview

8



Edit sensitivity label



Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

Items

Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. Learn more

✓ Files

Protect files created in Word, Excel, PowerPoint, and more.

Emails

Protect messages sent from all versions of Outlook.

Meetings

Protect calendar events and meetings scheduled in Outlook and Teams.

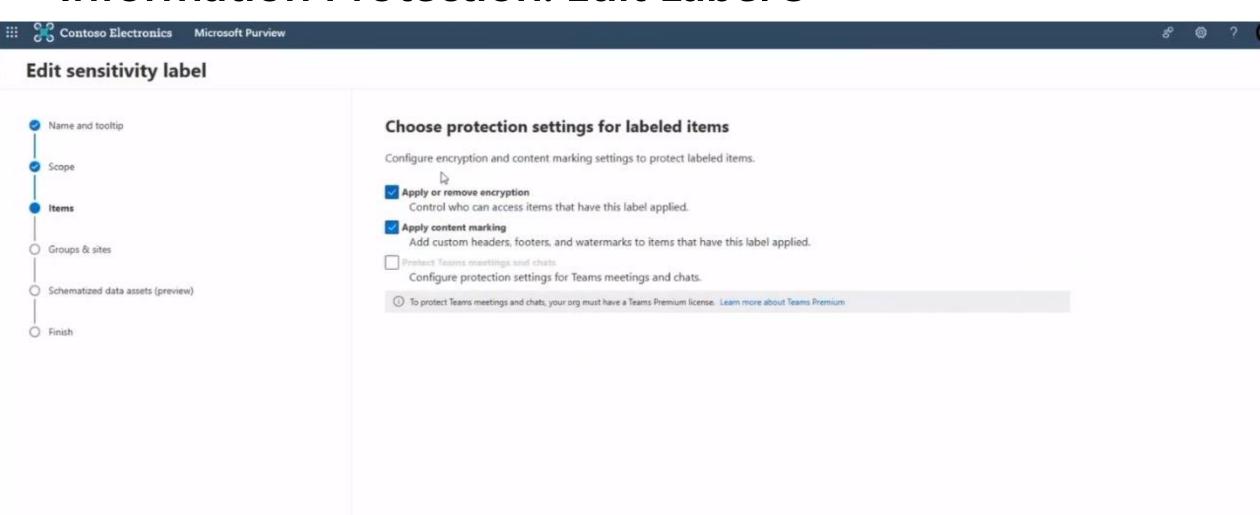
Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

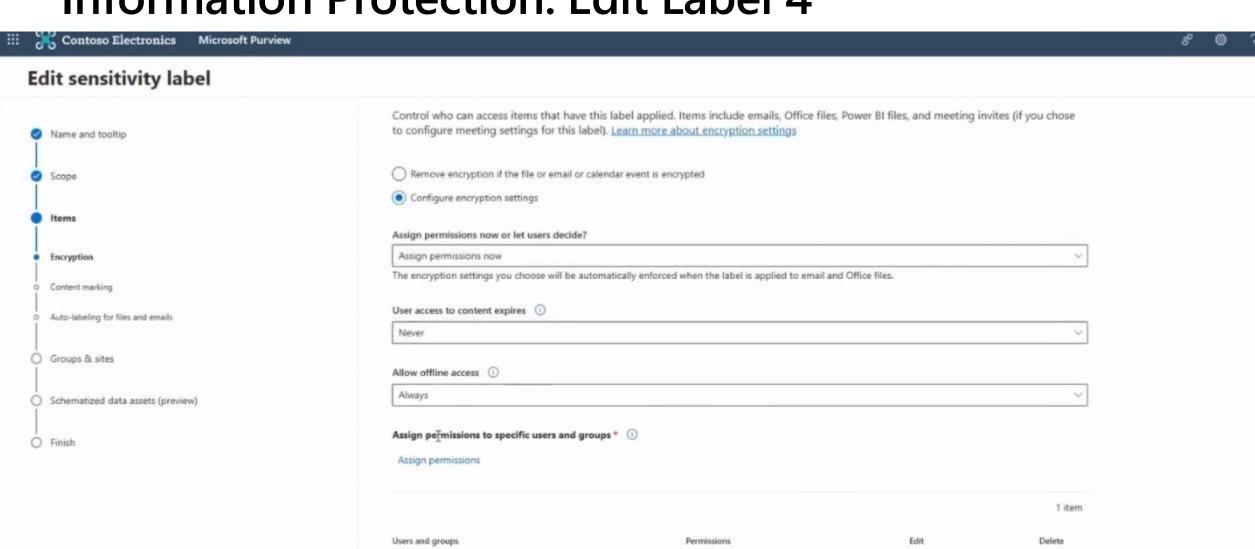
Schematized data assets (preview)

Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Information Protection: Edit Label 3



Information Protection: Edit Label 4



Co-Author

Back

M365x868515.onmicrosoft.com

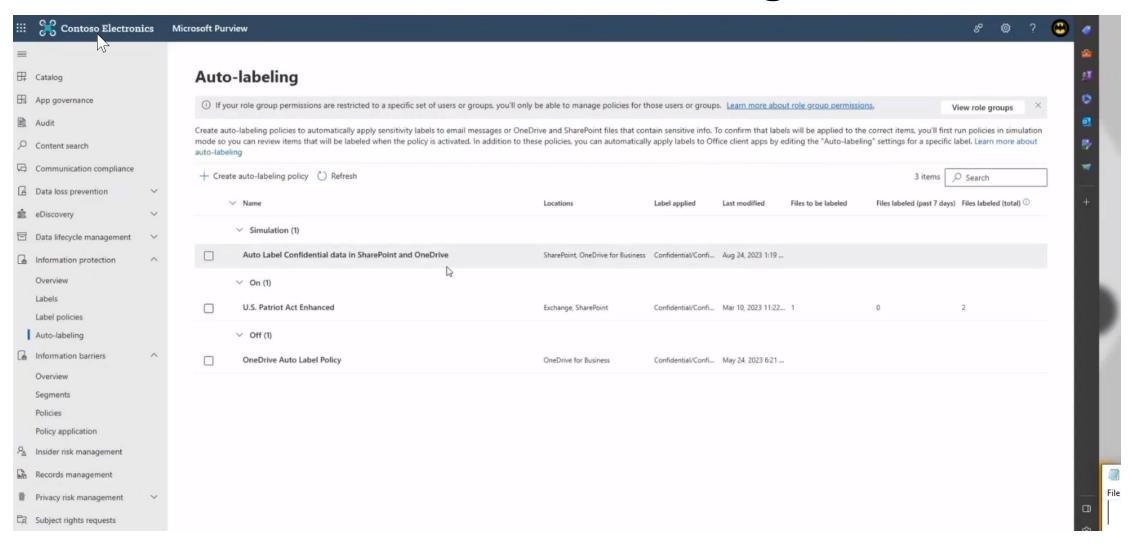
Use Double Key Encryption ①

闸

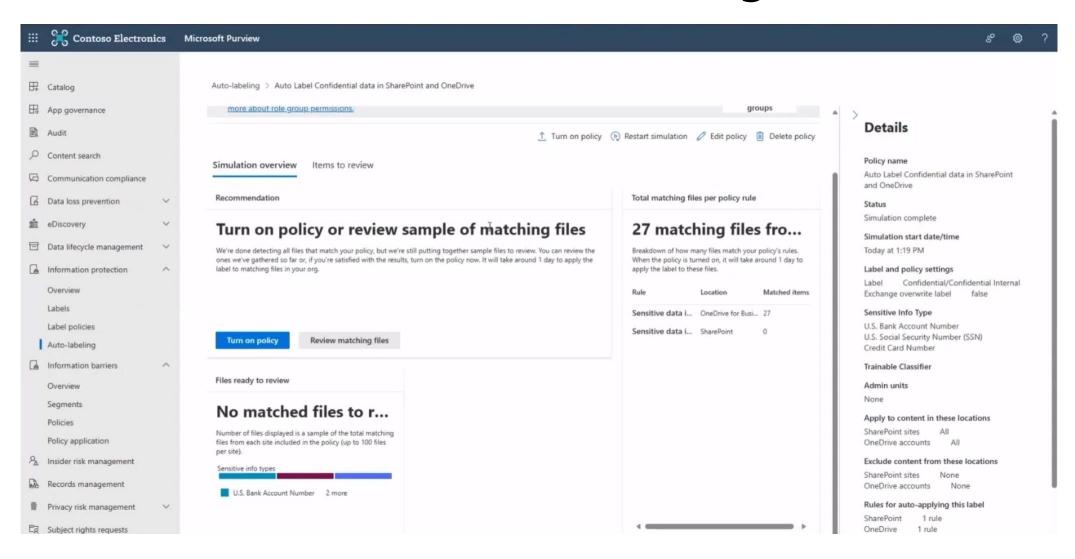
Demo

- -Microsoft 365 Admin portal
- -Compliance Portal Overview
- -Confidential Internal Word Document Not Accessible outside Organization
 - 1.Define a Label for Files: File-Label-Confidential-Internal
 - 2. Publish label for all users: Confidential Internal Only Files
 - 3.create document with internal account and label it with the label
 - 4.the document is not accessible with other org accounts: if you email it to
- Ehsan. Eskandari @Build On Cloud. Net for example you can not open this document.

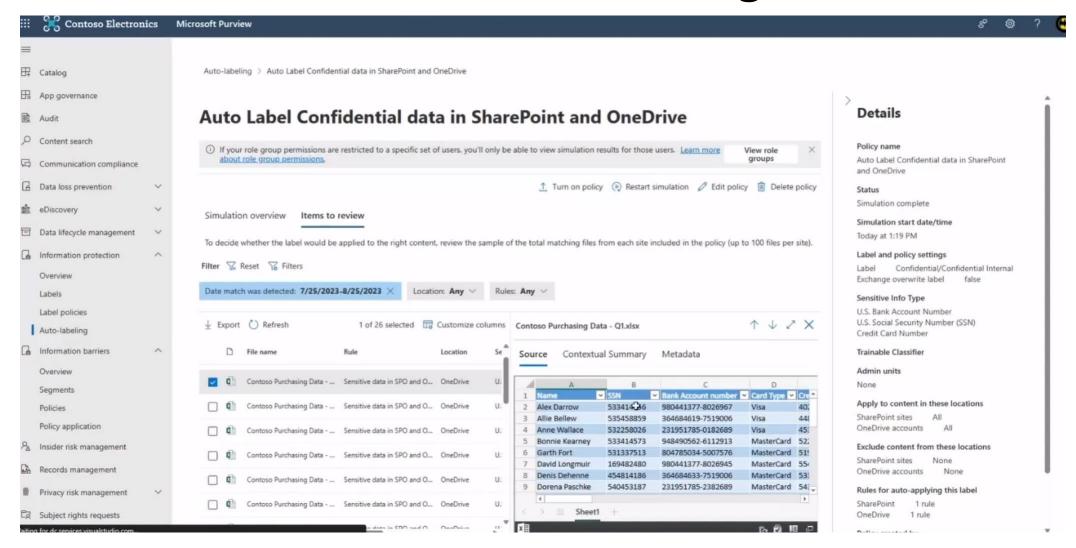
Information Protection: Auto Labeling



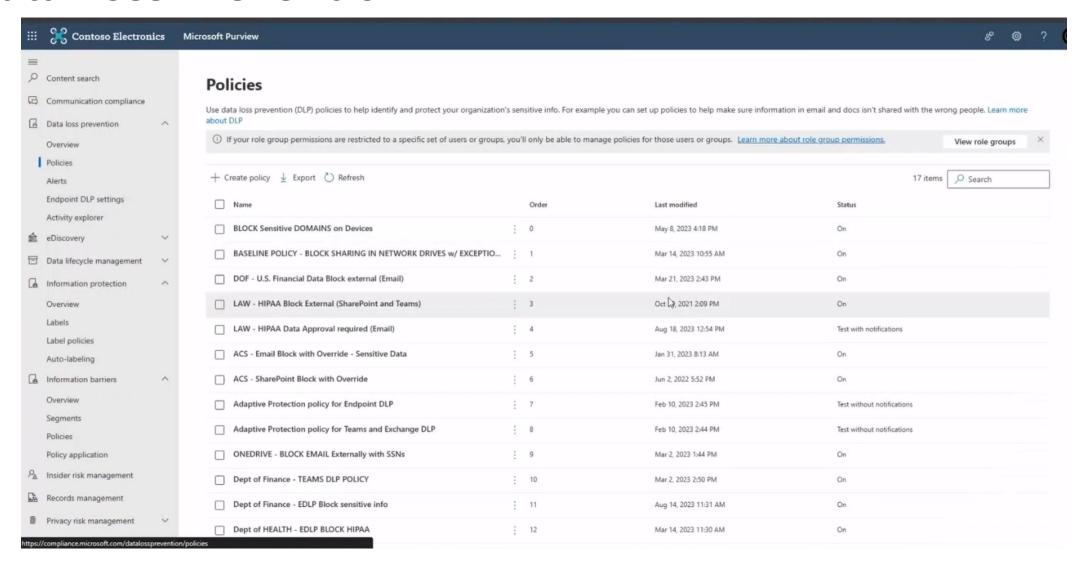
Information Protection: Auto Labeling

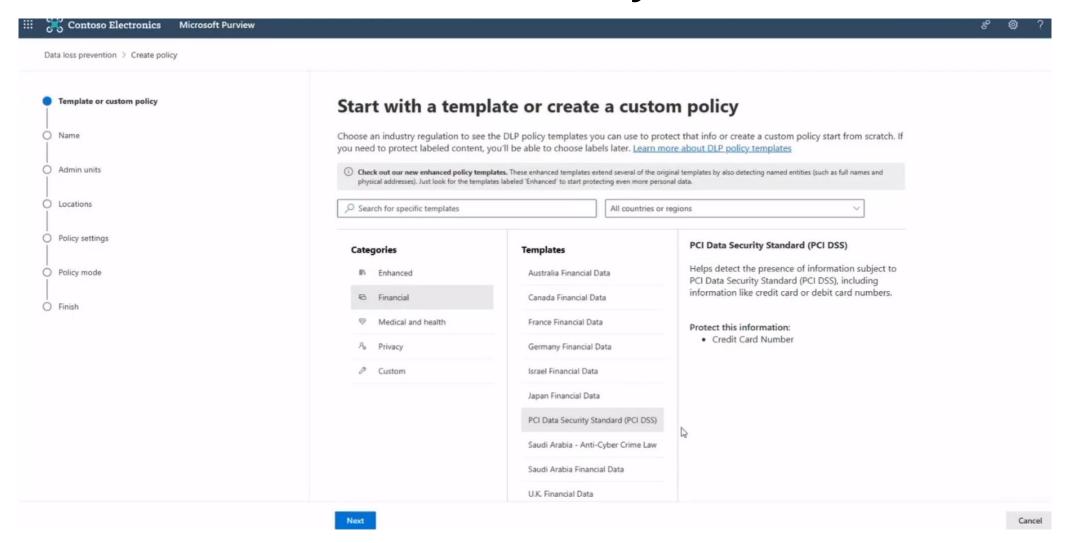


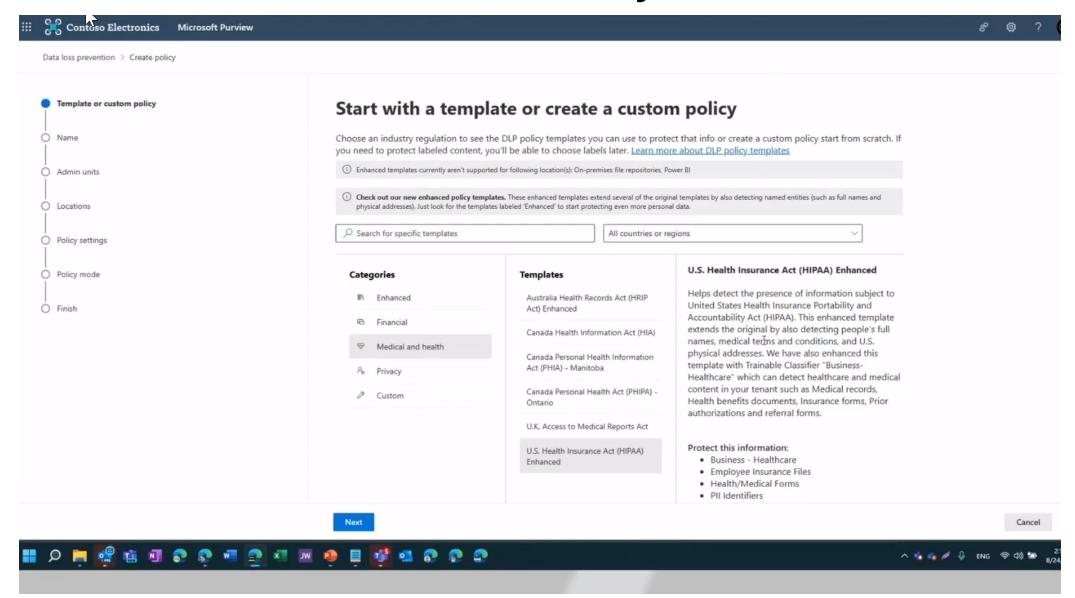
Information Protection: Auto Labeling

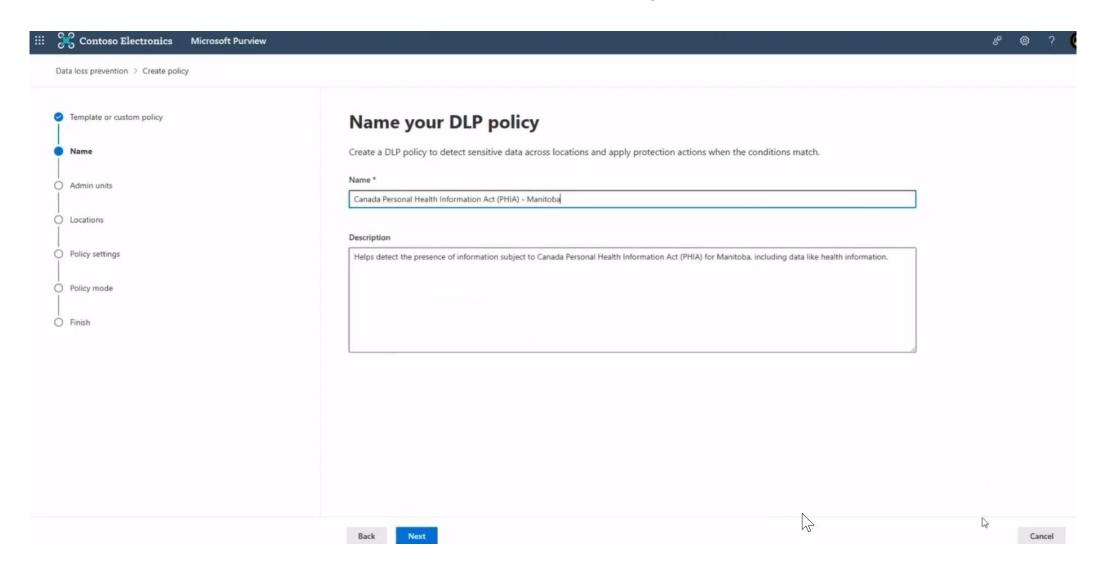


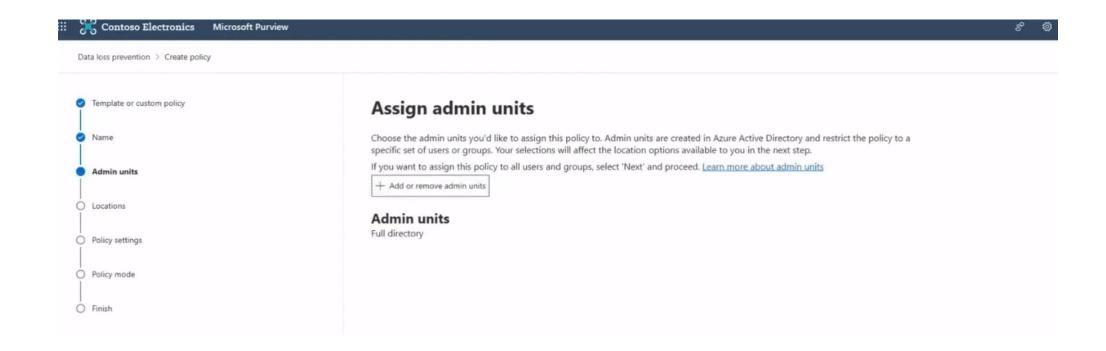
Data Loss Prevention

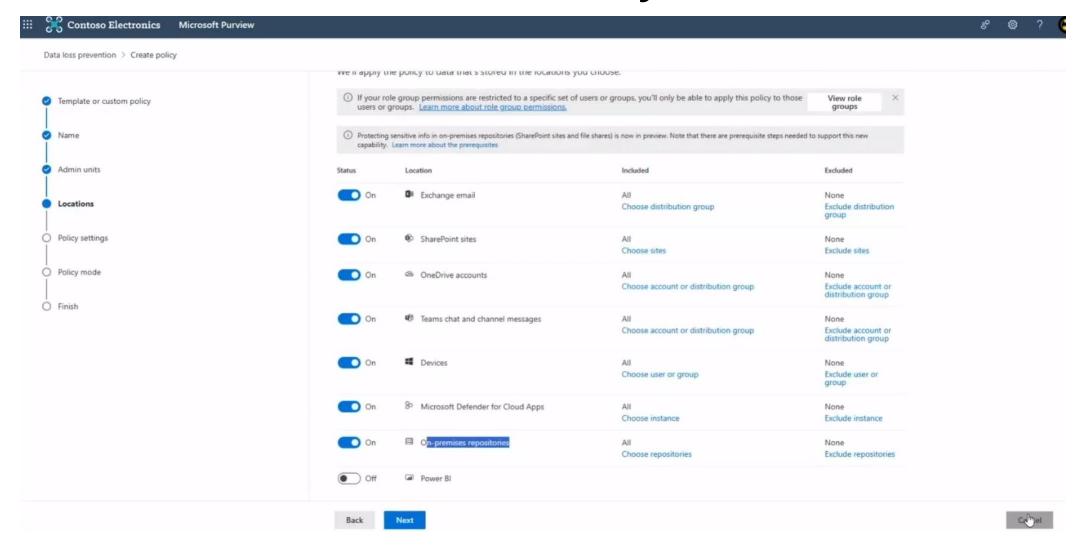














Thank You