SYNERGY
FOR
FUTURE

Identifying and Protecting Sensitive Data at Enterprise Scale

Meet the Microsoft Purview family

DATA SECURITY

Secure data across its lifecycle, wherever it lives

Data Loss Prevention
Insider Risk Management
Information Protection

DATA GOVERNANCE

Govern data seamlessly to empower your organization

Data Map
Data Catalog
Data Estate Insights

DATA COMPLIANCE

Manage critical risks and regulatory requirements

Compliance Manager
eDiscovery
Audit
Communication Compliance
Data Lifecycle Management
Records Management

Unstructured & Structured data

Traditional and AI generated data

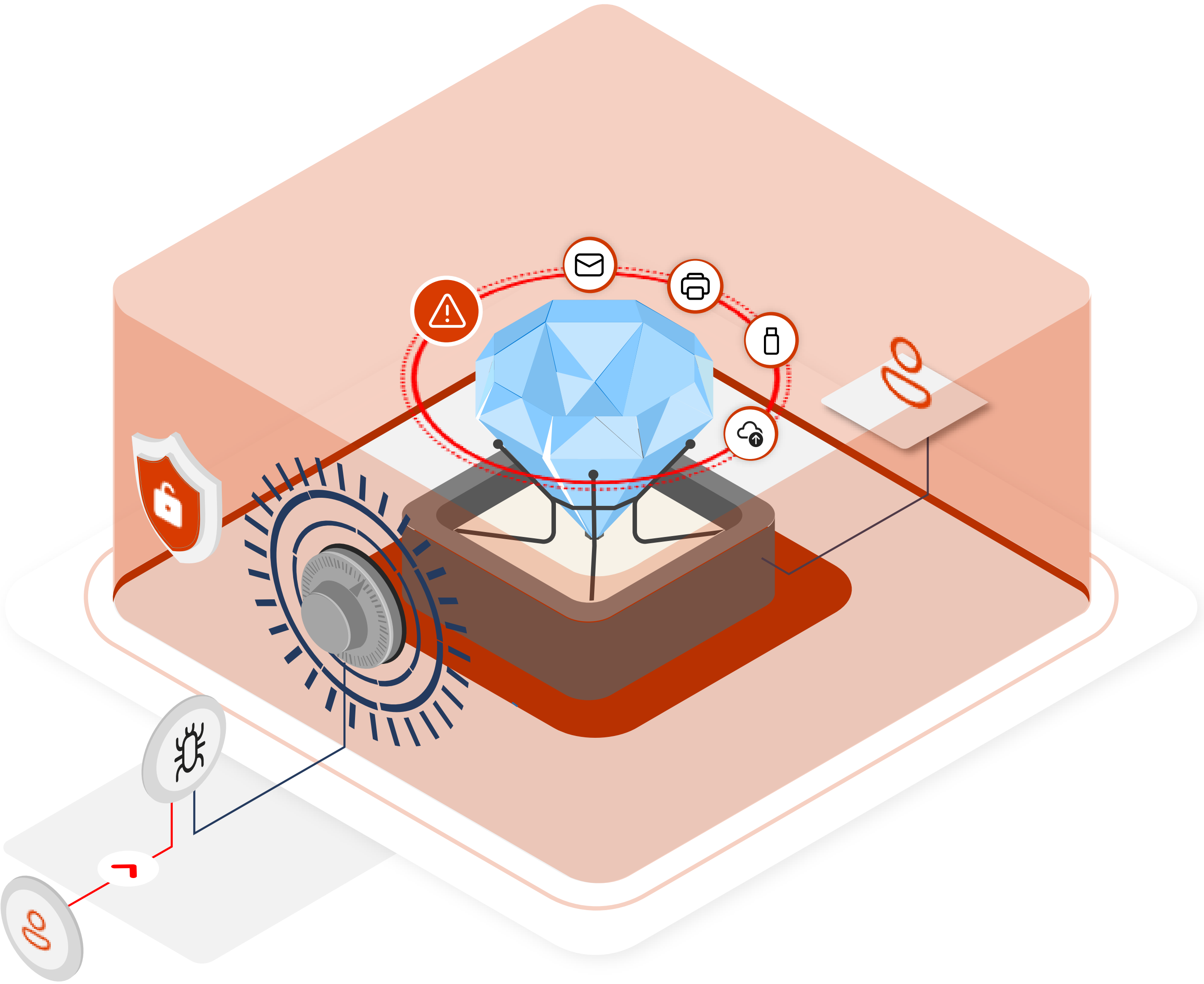
Microsoft 365 and Multi-cloud

Shared platform capabilities

Fidelis

The most urgent data security challenges

- Discover sensitive data, whether structured or unstructured, on-premises or in the clouds
- 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 incidents can happen anytime, anywhere

Data at risk of misuse if organization has no visibility into their data estate

1

User falls prey to phishing attack, compromises user credentials

Data compromise by external threat

2

User copies file to a USB, then uploads to a personal Dropbox

Data theft by malicious insider

3

User negligently shares sensitive data in generative AI apps

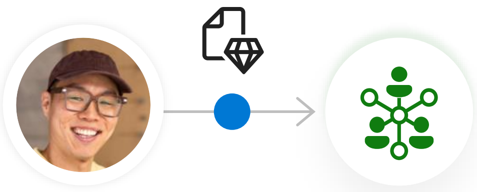
Data exposure by negligent insider

Security concerns associated with AI usage

Insufficient visibility into the usage of AI applications can result in security and compliance challenges.

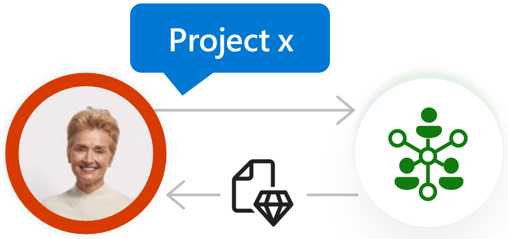
1

Data leak:
Users may inadvertently leak sensitive data to AI apps



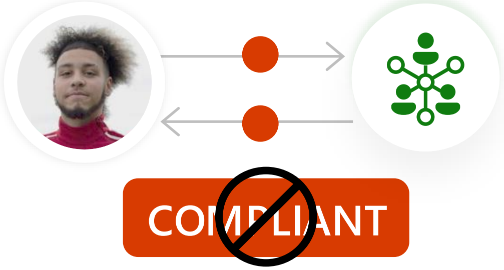
2

Data oversharing:
Users may access sensitive data via AI apps they are not authorized to view or edit



3

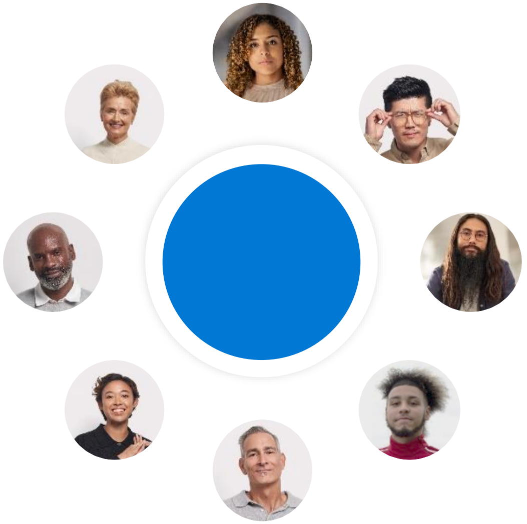
Non-compliance usage:
Users use AI apps to generate unethical or other high-risk content



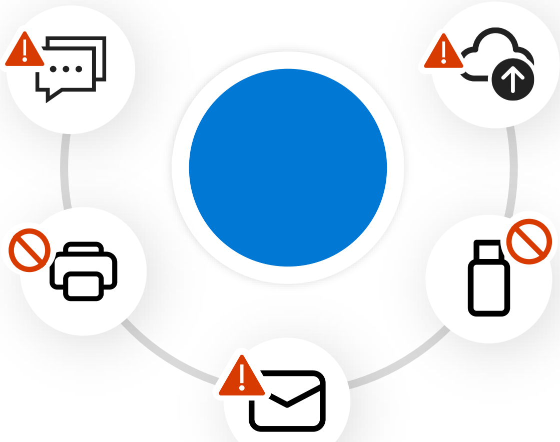
Organizations need to...

Discover and protect sensitive data throughout its lifecycle

Understand user activity context around the data and identify risks



Prevent data from unauthorized use across apps, services, and devices



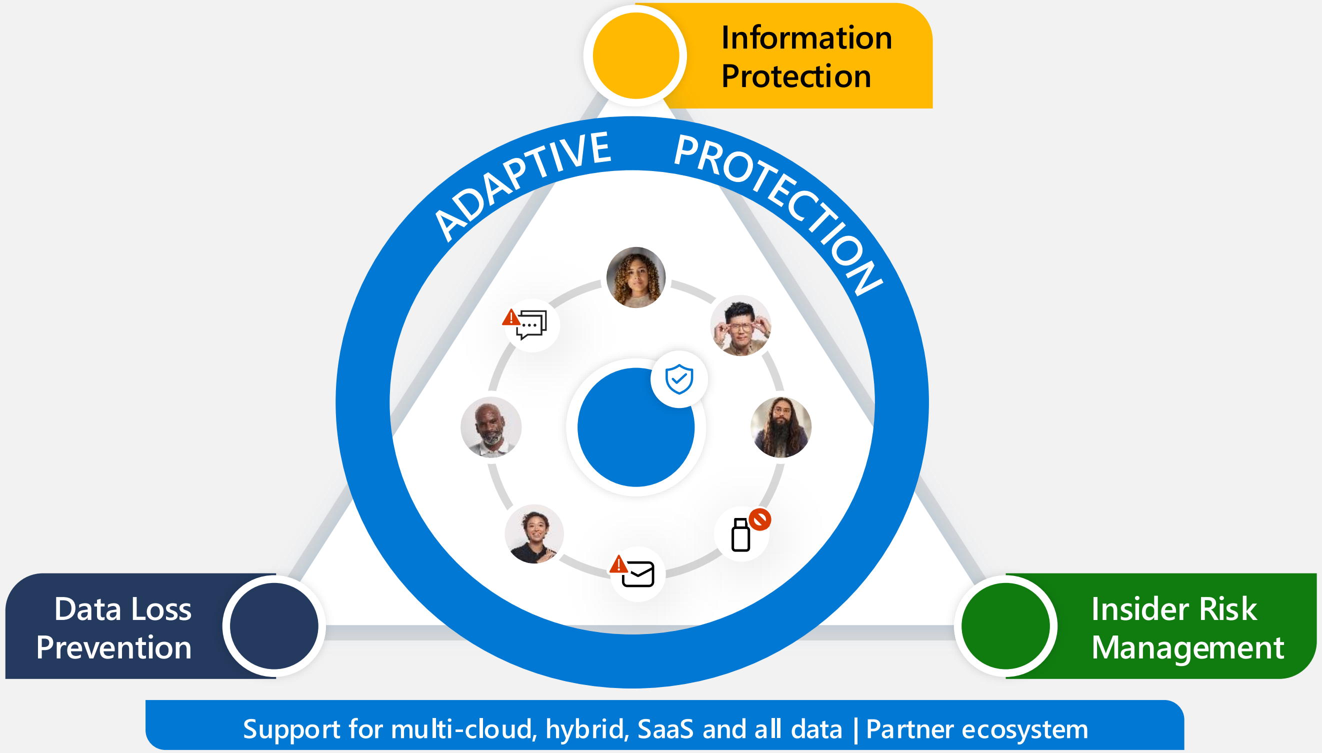
Balance data security and productivity

Fortify data security with an integrated approach

Discover and auto-classify data and prevent it from unauthorized use across apps, services, and devices

Understand the user intent and context around sensitive data to identify the most critical risks

Prevent data from unauthorized use across apps, services



Information Protection

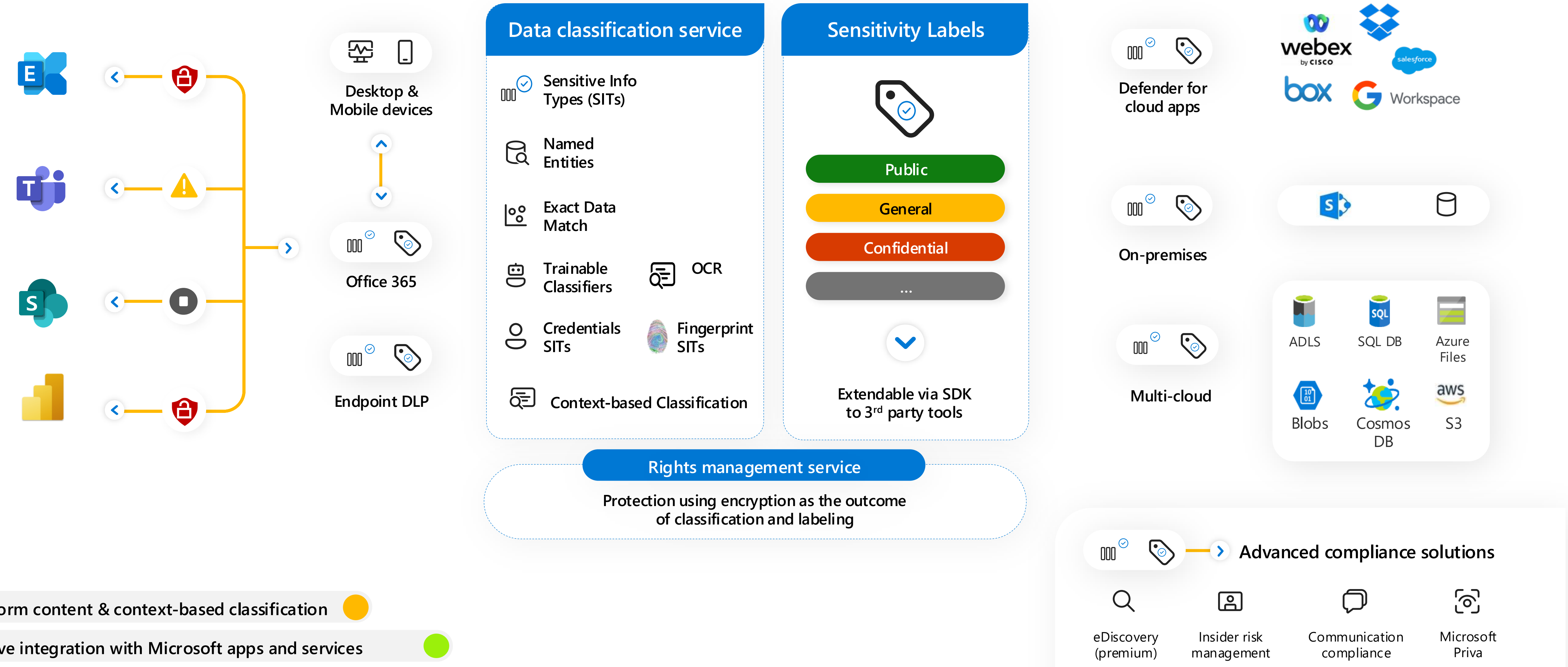
ADAPTIVE PROTECTION

Data Loss Prevention

Insider Risk Management

Support for multi-cloud, hybrid, SaaS and all data | Partner ecosystem

Microsoft Purview Information Protection



Desktop & Mobile devices

Office 365

Endpoint DLP

Data classification service

Sensitive Info Types (SITs)

Named Entities

Exact Data Match

Trainable Classifiers

OCR

Credentials SITs

Fingerprint SITs

Context-based Classification

Sensitivity Labels

Public

General

Confidential

...

Extendable via SDK to 3rd party tools

Rights management service

Protection using encryption as the outcome of classification and labeling

Defender for cloud apps

On-premises

Multi-cloud

Advanced compliance solutions

eDiscovery (premium)

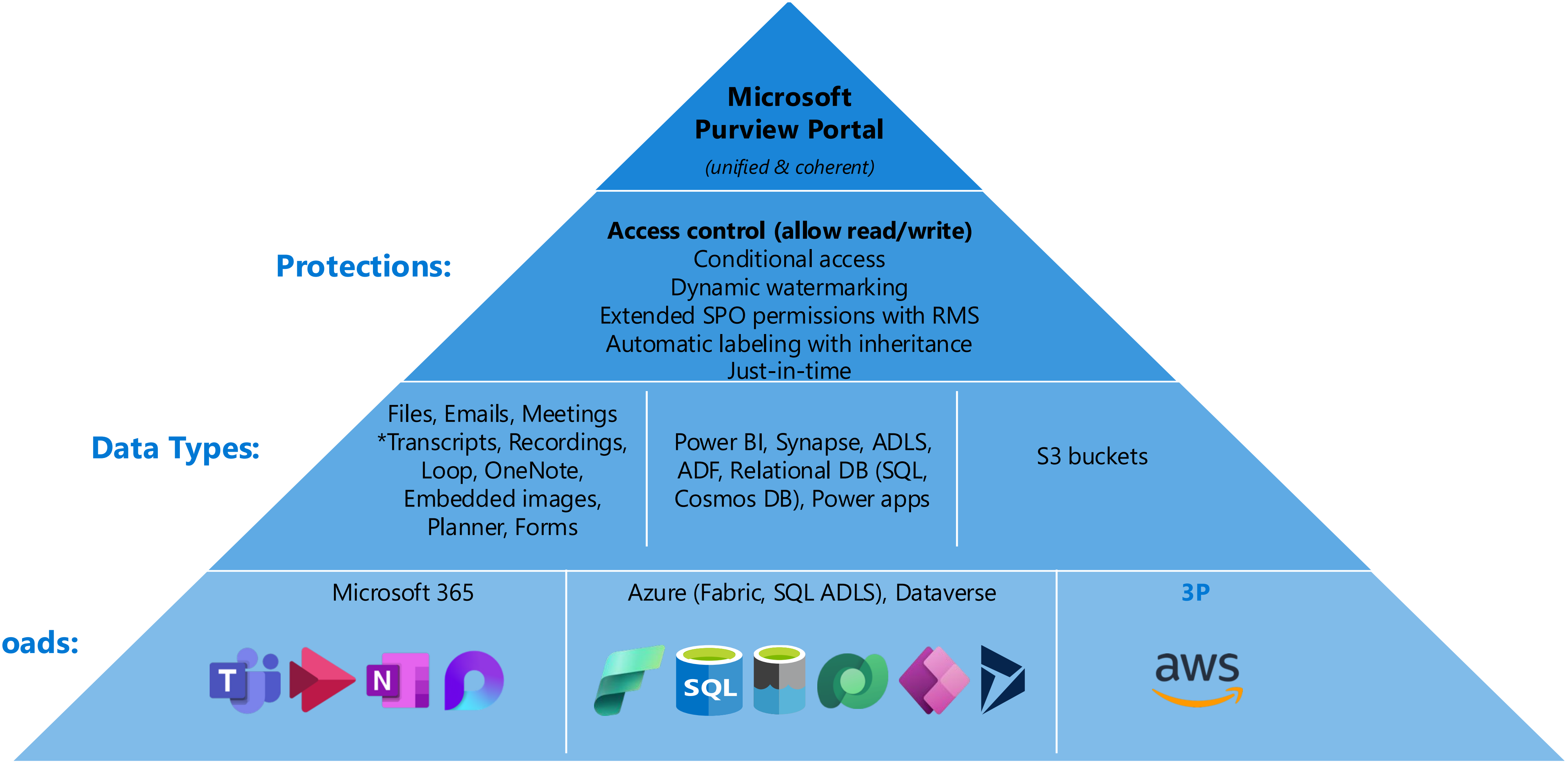
Insider risk management

Communication compliance

Microsoft Priva

- Uniform content & context-based classification 🟠
- Native integration with Microsoft apps and services 🟢
- Broad support with 3rd party solutions, data repositories, and LOB applications 🔵

Our focus is to expand Purview to more workloads, new data types, with more protection capabilities



Microsoft Purview Portal
(unified & coherent)

Protections:

Access control (allow read/write)
Conditional access
Dynamic watermarking
Extended SPO permissions with RMS
Automatic labeling with inheritance
Just-in-time

Data Types:

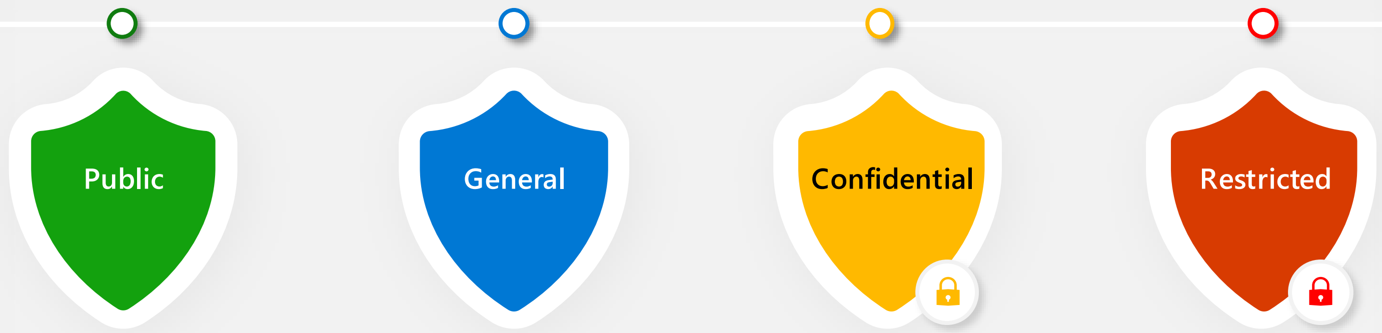
Files, Emails, Meetings *Transcripts, Recordings, Loop, OneNote, Embedded images, Planner, Forms	Power BI, Synapse, ADLS, ADF, Relational DB (SQL, Cosmos DB), Power apps	S3 buckets

Workloads:

Microsoft 365	Azure (Fabric, SQL ADLS), Dataverse	**3P**

Sensitivity labels span your entire data estate

- They are a representation of your information taxonomy.
- They describe the priority assigned to your categories of sensitive information.



Content labels

Applied To: Office apps, Power BI reports, Azure Data

Protections: Encryption and visual markings

Automation: Can be applied either manually by users or automatically based on classification

Container labels

Applied To: SharePoint sites, Teams channels, Microsoft 365 groups

Protections: Access control, privacy settings, conditional access

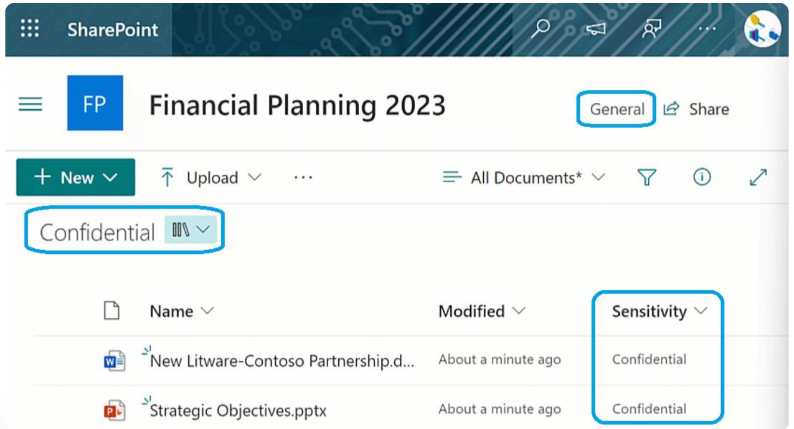
Automation: Can be applied manually by site/Team or group owners

Powerful controls that ensure labels are applied where needed

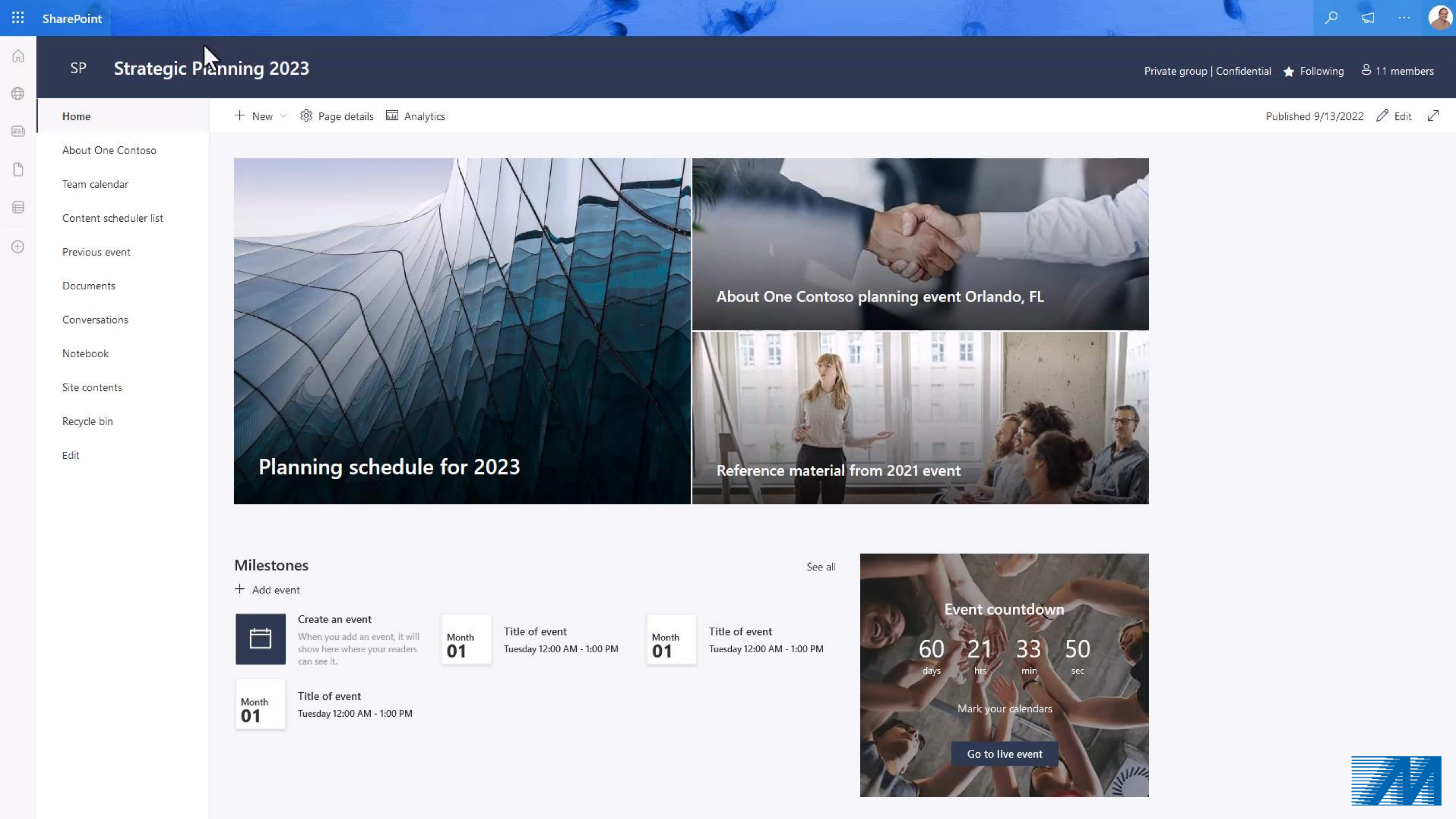
Apply labels by default, make them mandatory, prevent label downgrades

Default sensitivity labels

- Secure SharePoint and OneDrive document libraries with default sensitivity labels (Office files and PDFs)
- Classify and protect Document Libraries, within a site, with labels-based policies



Name	Modified	Sensitivity
New Litware-Contoso Partnership.d...	About a minute ago	Confidential
Strategic Objectives.pptx	About a minute ago	Confidential



Strategic Planning 2023

Published 9/13/2022

Planning schedule for 2023

About One Contoso planning event Orlando, FL

Reference material from 2021 event

Milestones

Create an event
When you add an event, it will show here where your readers can see it.

Month 01 — **Title of event** — Tuesday 12:00 AM - 1:00 PM

Month 01 — **Title of event** — Tuesday 12:00 AM - 1:00 PM

Month 01 — **Title of event** — Tuesday 12:00 AM - 1:00 PM

Event countdown

60 days 21 hrs 33 min 50 sec

Mark your calendars

Best-in-class classification technologies

Sensitive info types

300+ out of the box info types like SSN, CCN

Clone, edit, or create your own

Supports regex, keywords, and dictionaries

Named entities

50+ entities covering person name, medical terms, and drug names

Best used in combination with other sensitive info types

Exact data match

Provides a lookup to exactly match content with unique customer data

Supports 100m rows and multiple lookup fields

Optical Character Recognition (OCR)

Expanded OCR for EXO, SPO, ODB, Teams & endpoint devices

Supports over 150 languages

Supports image files and images embedded in PDFs

Trainable classifiers

35+ pre-trained ready-to-use trainable classifiers

Create your own classifier based on business data

Credentials SITs

42 new SITs for digital authentication credential types

Use in auto-labeling and DLP policies to detect sensitive credentials in files

Fingerprint SITs

Detect exact or partial matching of sensitive intellectual property

Use in Exchange, SharePoint, Teams and Devices

Context-based classification

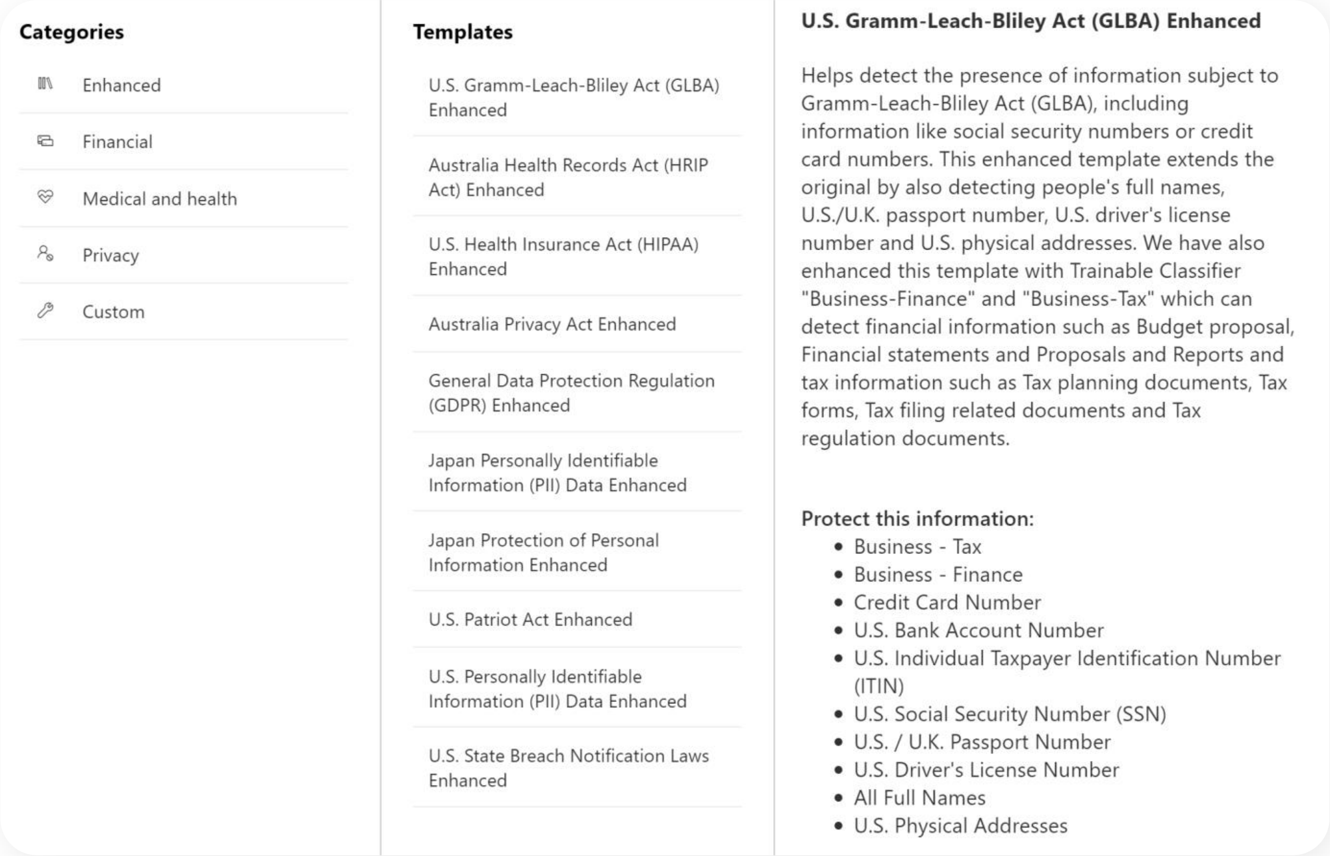
ODSP default site label

Service-side auto-labeling

- File extension
- Document name contains word
- Document property is
- Document size greater than
- Document created by

Templates

- Provide pre-defined policies that use available classifiers
- Cover multiple industry and geographical regulatory requirements
- Easily customizable, can be edited to meet customer needs
- Get started easily with simulations, rerun as needed to fine tune



Categories

- Enhanced
- Financial
- Medical and health
- Privacy
- Custom

Templates

- U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced
- Australia Health Records Act (HRIP Act) Enhanced
- U.S. Health Insurance Act (HIPAA) Enhanced
- Australia Privacy Act Enhanced
- General Data Protection Regulation (GDPR) Enhanced
- Japan Personally Identifiable Information (PII) Data Enhanced
- Japan Protection of Personal Information Enhanced
- U.S. Patriot Act Enhanced
- U.S. Personally Identifiable Information (PII) Data Enhanced
- U.S. State Breach Notification Laws Enhanced

U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced

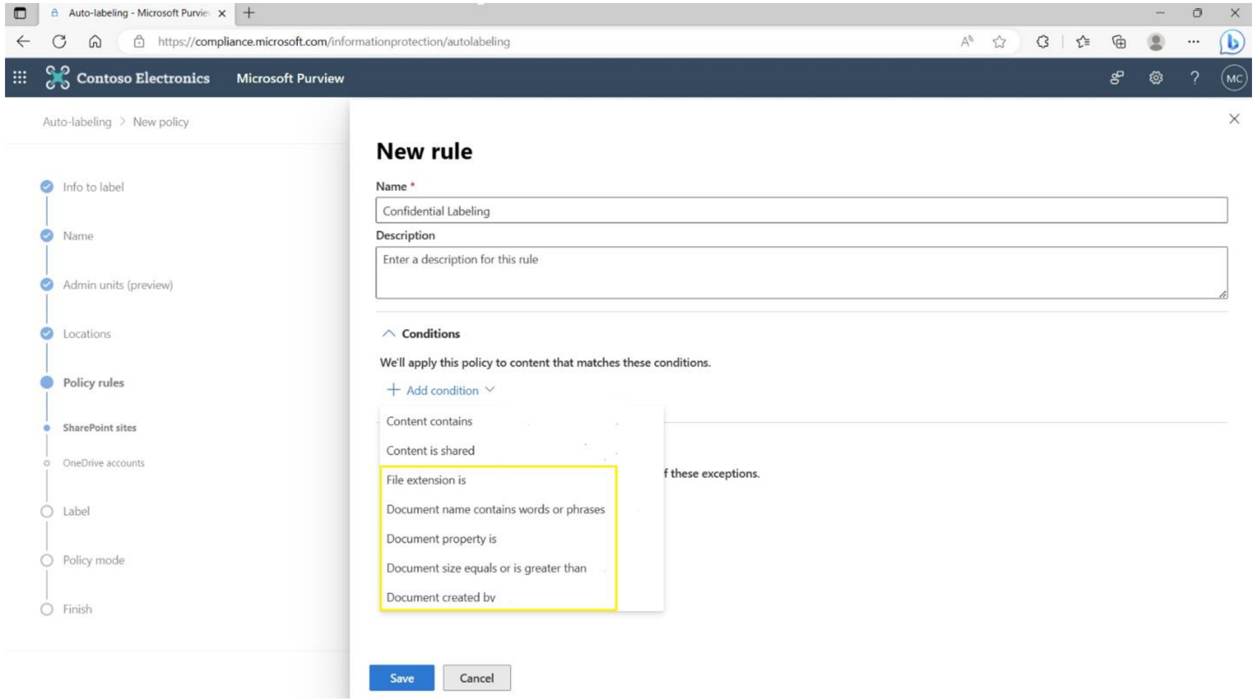
Helps detect the presence of information subject to Gramm-Leach-Bliley Act (GLBA), including information like social security numbers or credit card numbers. This enhanced template extends the original by also detecting people's full names, U.S./U.K. passport number, U.S. driver's license number and U.S. physical addresses. We have also enhanced this template with Trainable Classifier "Business-Finance" and "Business-Tax" which can detect financial information such as Budget proposal, Financial statements and Proposals and Reports and tax information such as Tax planning documents, Tax forms, Tax filing related documents and Tax regulation documents.

Protect this information:

- Business - Tax
- Business - Finance
- Credit Card Number
- U.S. Bank Account Number
- U.S. Individual Taxpayer Identification Number (ITIN)
- U.S. Social Security Number (SSN)
- U.S. / U.K. Passport Number
- U.S. Driver's License Number
- All Full Names
- U.S. Physical Addresses

Context-based classification

- New contextual predicates in service-side auto-labeling
- Supports the following new contextual based predicates



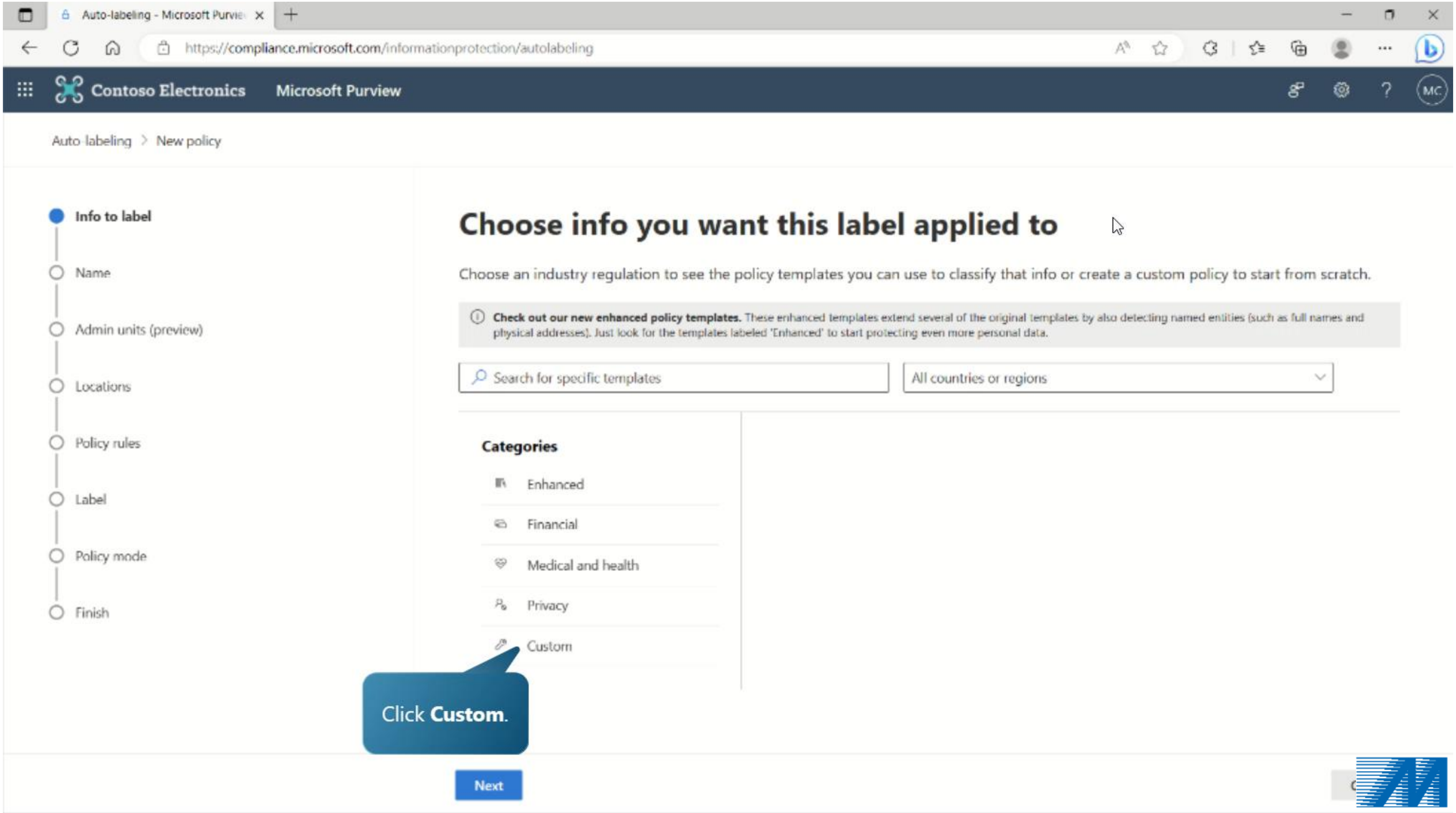
New rule

Name *: Confidential Labeling

Description: Enter a description for this rule

Conditions

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


Auto-labeling - Microsoft Purvie
https://compliance.microsoft.com/informationprotection/autolabeling
Contoso Electronics
Microsoft Purview
MC

Auto labeling > New policy

- ● **Info to label**
- ○ Name
- ○ Admin units (preview)
- ○ Locations
- ○ Policy rules
- ○ Label
- ○ Policy mode
- ○ Finish

Choose info you want this label applied to

Choose an industry regulation to see the policy templates you can use to classify that info or create a custom policy to start from scratch.

ⓘ **Check out our new enhanced policy templates.** These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

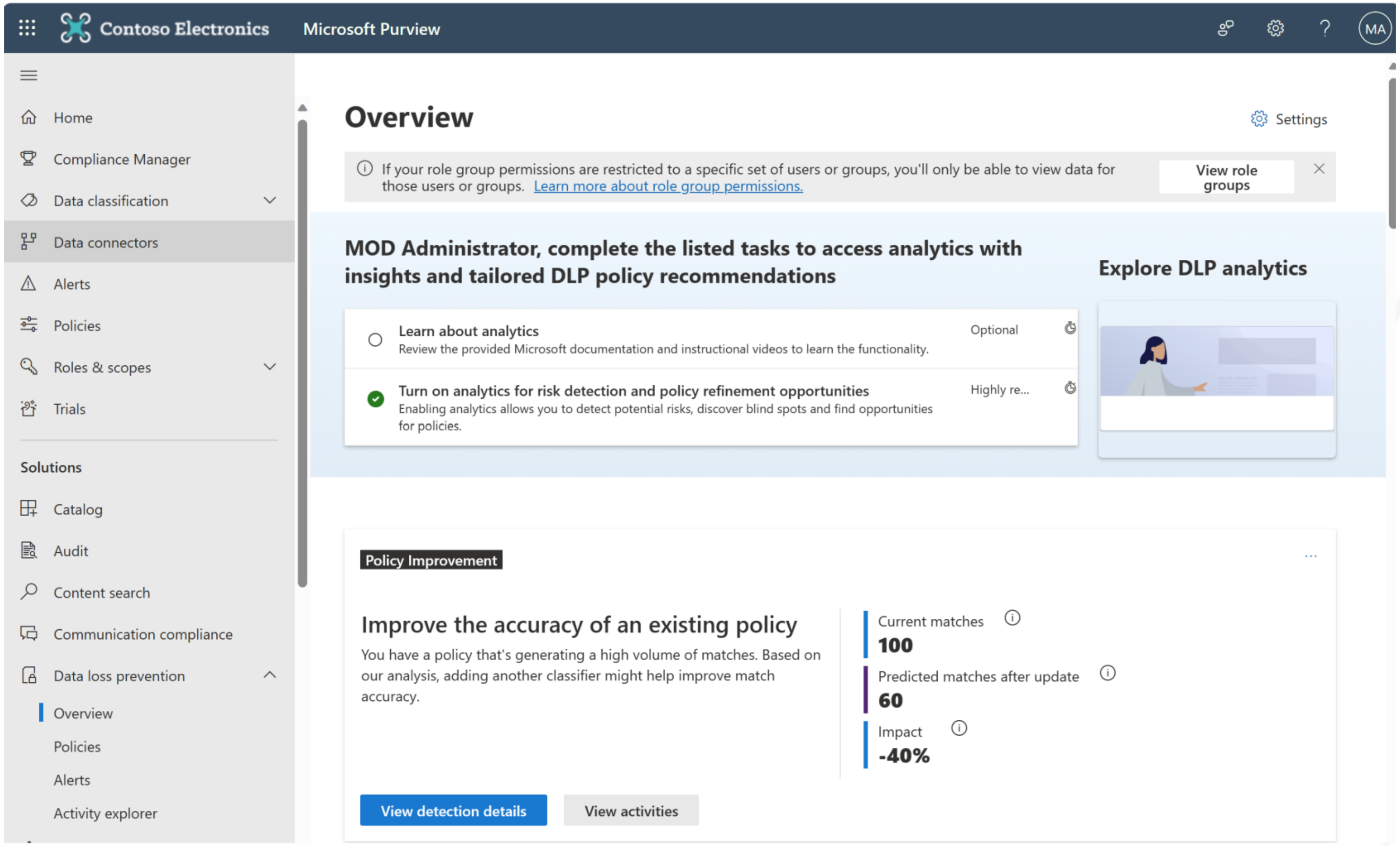
Categories

- Enhanced
- Financial
- Medical and health
- Privacy
- Custom

Click **Custom**.

Next

MIP and DLP Analytics Page



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.

MOD Administrator, complete the listed tasks to access analytics with insights and tailored DLP policy recommendations

○ Learn about analytics
Review the provided Microsoft documentation and instructional videos to learn the functionality.

✓ Turn on analytics for risk detection and policy refinement opportunities
Enabling analytics allows you to detect potential risks, discover blind spots and find opportunities for policies.

Improve the accuracy of an existing policy

You have a policy that's generating a high volume of matches. Based on our analysis, adding another classifier might help improve match accuracy.

Current matches
100

Predicted matches after update
60

Impact
-40%

Policy simulation

1

Pick your scope

- Option 1: ALL – SharePoint sites, OneDrive accounts and Email users
- Option 2: Subset of sites or accounts – Can use PowerShell for longer lists

Supported in auto labeling and DLM today, DLP by Jun’23

2

Simulate in your production environment

- Simulation is fast – It normally takes a few hours to run depending on the size of your tenant
- Simulation is not intrusive – No actions are applied
- Simulation for EXO triggers in near real time on email activity (not emails at rest)
- Simulation for ODSP triggers on files at rest
- Insights are best achieved on real production data

3

Gain confidence in your protection policy

- Review simulation results (both aggregate and sample files)
- Iterate and experiment to improve accuracy

4

Turn on protection policies after validating simulation results

- Existing Office Files at rest (Word, Excel, PowerPoint) in OneDrive & SharePoint are automatically protected
- New files added after the policy is enforced are also protected
- Emails in transit are automatically scanned for sensitive information and protected
- *Cold data crawl: private preview coming in Q3’23*

Labeling data at scale – Guiding principles

Apply labels by default using Label Policy

- When content is created or accessed, set a default label for
  - Files
  - Emails
  - Meetings
  - PBI Reports
  - Containers
  - …

Apply labels based on context

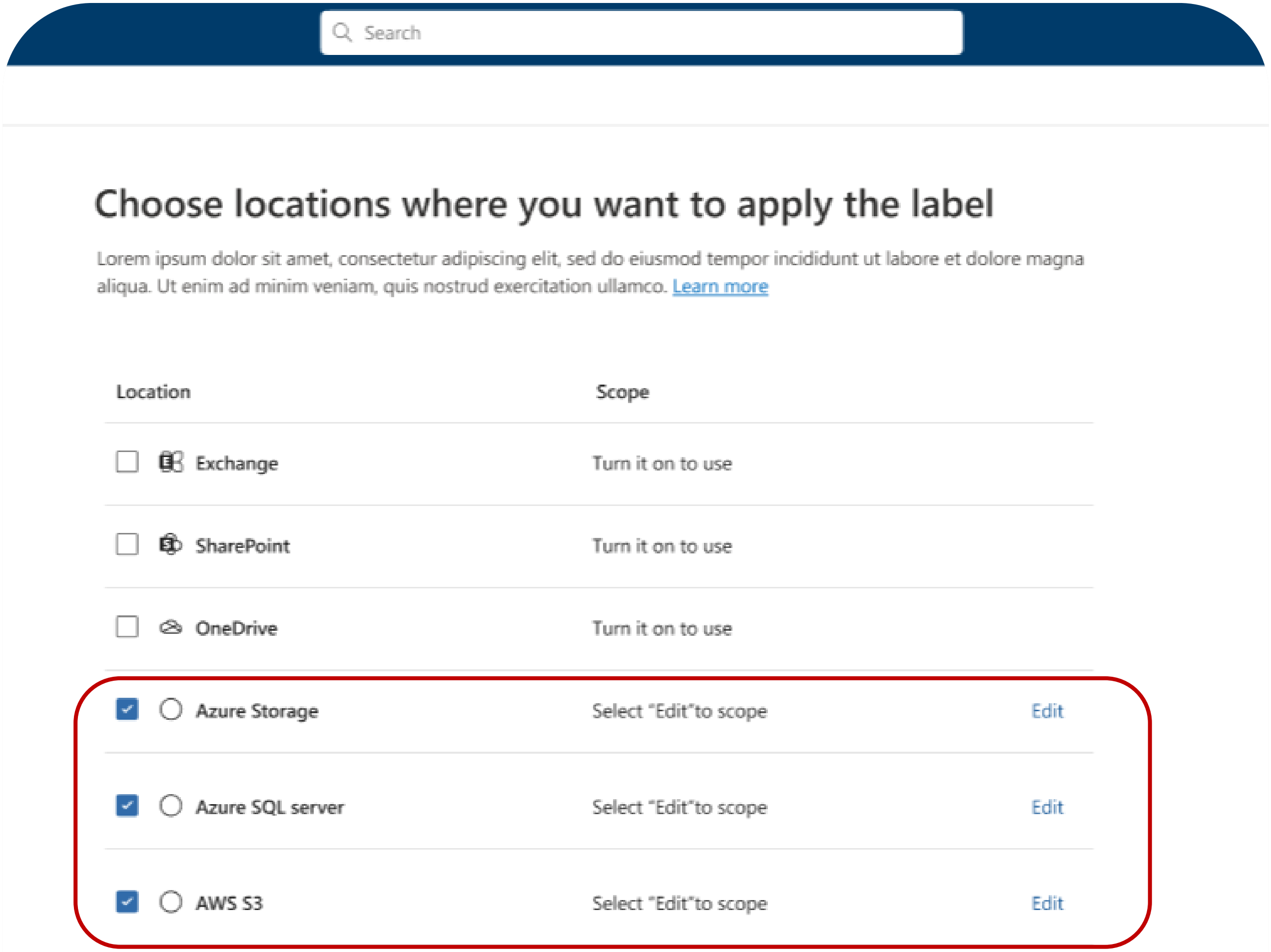
- By location, for sensitive SPO libraries, site owners can set a default label per library
- For documents at rest
  - Use service-side auto labeling by file size, extension, properties …
  - Use SetLabel Graph API to label specific files based on your criteria
- For emails in motion
  - Use service-side auto labeling to trigger labels based on predicates like sender, recipient, domain, …

Apply labels automatically based on content

- Client-side auto-labeling for content when files are in-use and mails are being composed
- Service side auto-labeling policy for files at-rest in SPO, ODB and mails in-transit in Exchange

Expanding auto-labeling

1. **New actions & workloads:** Configure auto-labeling policies for Azure, ADLS, and AWS S3 individually.
2. **New workloads:** Granular scoping allows admins to confidently enable auto-labeling in SQL, ADLS, & AWS S3 without impacting existing workloads.
3. **Coherence:** Single location to author auto-labeling policies for all workloads.



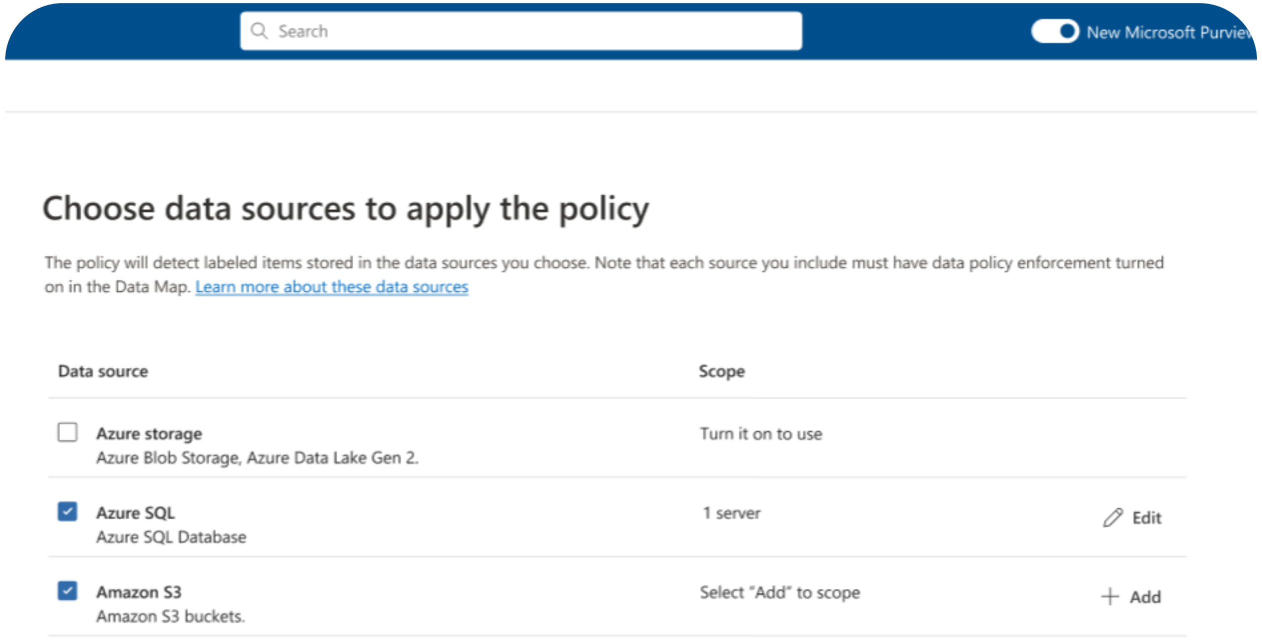
Choose locations where you want to apply the label

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco. Learn more

Location	Scope	
☐ Exchange	Turn it on to use	
☐ SharePoint	Turn it on to use	
☐ OneDrive	Turn it on to use	
☑ ○ Azure Storage	Select "Edit"to scope	Edit
☑ ○ Azure SQL server	Select "Edit"to scope	Edit
☑ ○ AWS S3	Select "Edit"to scope	Edit

Label-based access in Azure SQL, ADLS, & AWS S3

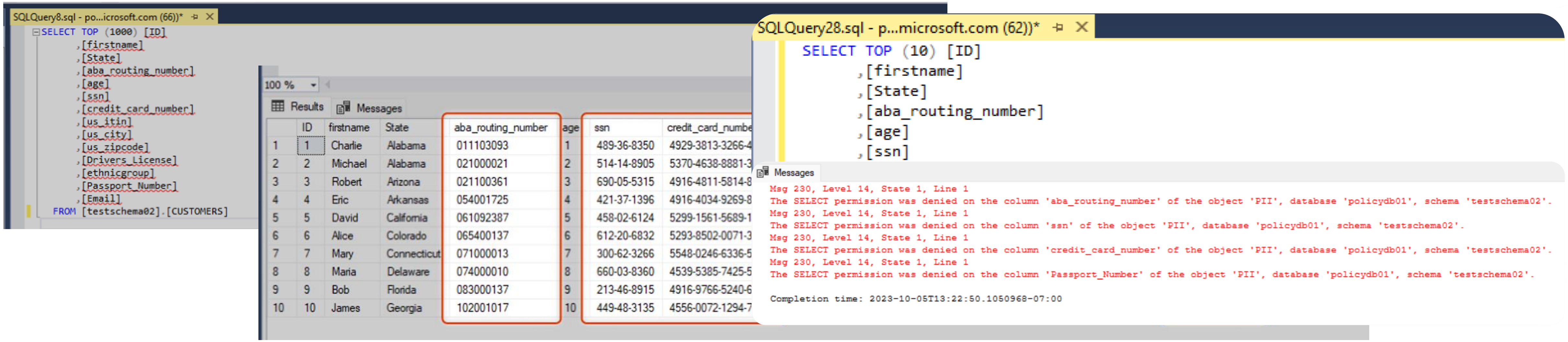
1. **New workloads:** Labeling and classification available across Azure SQL, ADLS, & AWS S3.
2. **New protection actions:** Enforce protection actions (access) for Azure SQL, ADLS, & AWS S3.
3. **Coherence:** Configure unified policies, allowing comprehensive visibility of sensitive data from single control plane.



Choose data sources to apply the policy

The policy will detect labeled items stored in the data sources you choose. Note that each source you include must have data policy enforcement turned on in the Data Map. Learn more about these data sources

Data source	Scope	
☐ **Azure storage** Azure Blob Storage, Azure Data Lake Gen 2.	Turn it on to use	
☑ **Azure SQL** Azure SQL Database	1 server	Edit
☑ **Amazon S3** Amazon S3 buckets.	Select "Add" to scope	+ Add



```sql
SELECT TOP (1000) [ID]
      ,[firstname]
      ,[State]
      ,[aba_routing_number]
      ,[age]
      ,[ssn]
      ,[credit_card_number]
      ,[us_itin]
      ,[us_city]
      ,[us_zipcode]
      ,[Drivers_License]
      ,[ethnicgroup]
      ,[Passport_Number]
      ,[Email]
  FROM [testschema02].[CUSTOMERS]
```

	ID	firstname	State	aba_routing_number	age	ssn	credit_card_numbe
1	1	Charlie	Alabama	011103093	1	489-36-8350	4929-3813-3266-4
2	2	Michael	Alabama	021000021	2	514-14-8905	5370-4638-8881-3
3	3	Robert	Arizona	021100361	3	690-05-5315	4916-4811-5814-8
4	4	Eric	Arkansas	054001725	4	421-37-1396	4916-4034-9269-8
5	5	David	California	061092387	5	458-02-6124	5299-1561-5689-1
6	6	Alice	Colorado	065400137	6	612-20-6832	5293-8502-0071-3
7	7	Mary	Connecticut	071000013	7	300-62-3266	5548-0246-6336-5
8	8	Maria	Delaware	074000010	8	660-03-8360	4539-5385-7425-5
9	9	Bob	Florida	083000137	9	213-46-8915	4916-9766-5240-6
10	10	James	Georgia	102001017	10	449-48-3135	4556-0072-1294-7

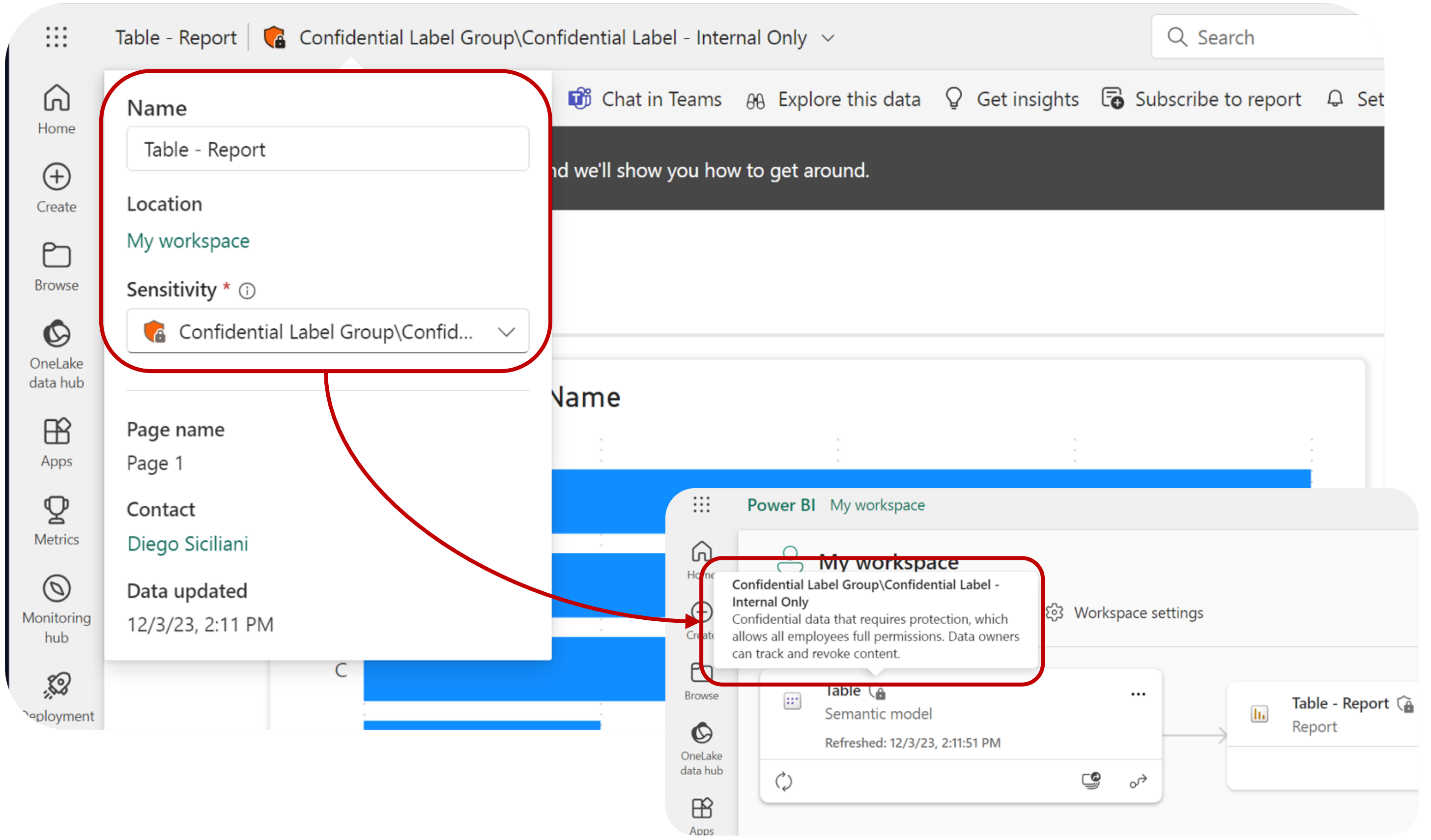
```sql
SELECT TOP (10) [ID]
      ,[firstname]
      ,[State]
      ,[aba_routing_number]
      ,[age]
      ,[ssn]
```

```
Msg 230, Level 14, State 1, Line 1
The SELECT permission was denied on the column 'aba_routing_number' of the object 'PII', database 'policydb01', schema 'testschema02'.
Msg 230, Level 14, State 1, Line 1
The SELECT permission was denied on the column 'ssn' of the object 'PII', database 'policydb01', schema 'testschema02'.
Msg 230, Level 14, State 1, Line 1
The SELECT permission was denied on the column 'credit_card_number' of the object 'PII', database 'policydb01', schema 'testschema02'.
Msg 230, Level 14, State 1, Line 1
The SELECT permission was denied on the column 'Passport_Number' of the object 'PII', database 'policydb01', schema 'testschema02'.

Completion time: 2023-10-05T13:22:50.1050968-07:00
```

MIP and DLP for Fabric

1. **New Protection Policy actions:** As a result of applying labels, admins can set MIP Protection Policies for items in Fabric (Allow read, Allow write).
2. **Extend label protection actions:** Extend Power BI Desktop protection actions to match Office protections more closely (Open, Edit, Republish)
3. **New DLP Policy:** Customers will be able to apply DLP policies (Policy Tips & auditing) and scope to specific Fabric workspaces (available in Power BI).



Name
Table - Report

Location
My workspace

Sensitivity *
Confidential Label Group\Confid...

Page name
Page 1

Contact
Diego Siciliani

Data updated
12/3/23, 2:11 PM

My workspace

Confidential Label Group\Confidential Label - Internal Only
Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.

Table
Semantic model
Refreshed: 12/3/23, 2:11:51 PM

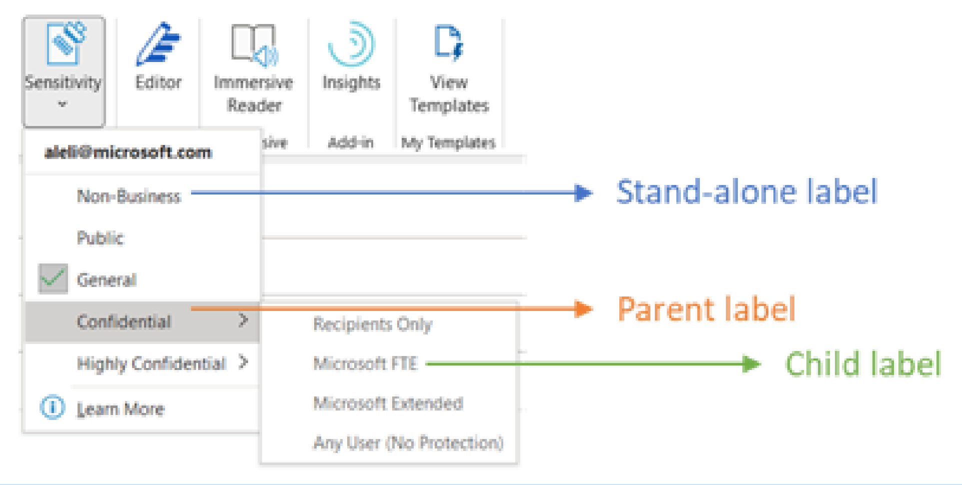
Table - Report
Report

Label Scheme Modernization

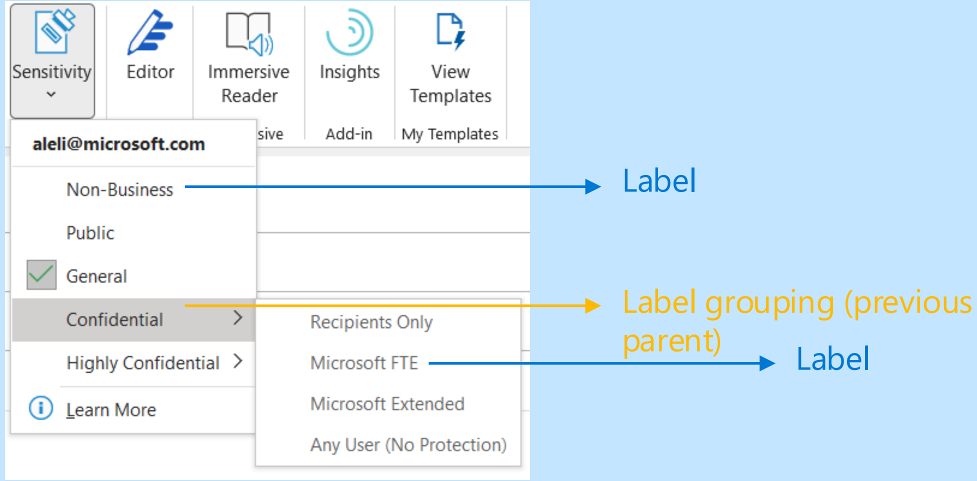
- Goal is to reduce confusion and complexity of label hierarchy configuration for admins and users:
  - Inconsistent user experience across apps when parent labels are published without any sub labels
  - Prevent orphaned labels – as requirements evolve, adding a sub label to a standalone causes all prior data assets to be orphaned

- Stand-alone and child labels will remain as-is today.
- Label Groups (what used to be Parent labels) will represent a group of labels.
- With proposed change, there will only be two types of entities:
  - Label group (new)
  - Labels (includes standalone & child labels)

Today (Before)



Proposal (After)



Label scheme modernization: Pre-Migration Readiness

Parent labels do not have any conditions or actions

Parent labels have the right scope (superset of their child label scopes).

Parent labels are published with child labels

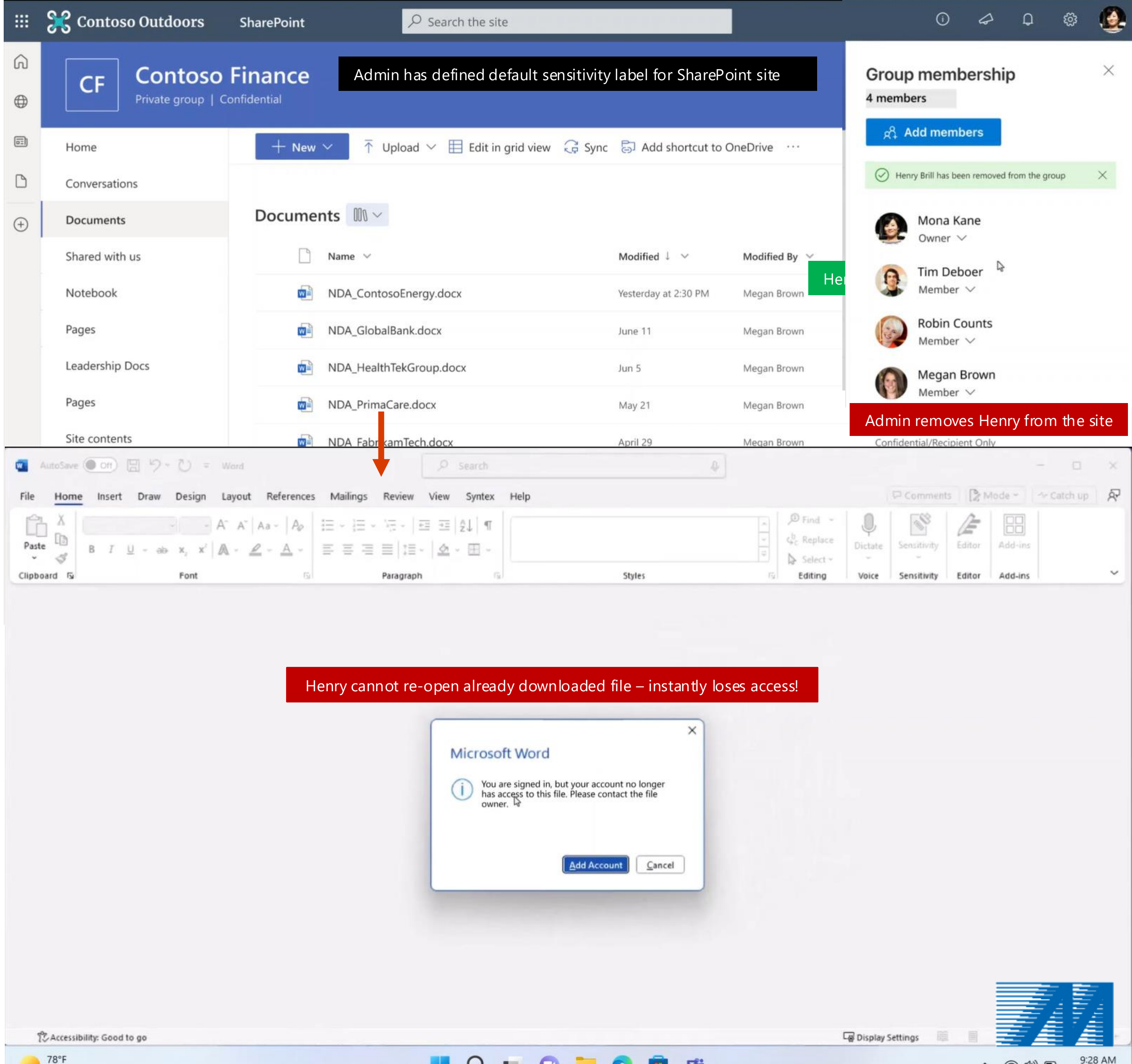
- They are not published by themselves.

Parent labels are not used as defaults, recommended, or in Auto-labeling, Protection, or DLP policies.

Extended SharePoint Permissions with RMS

Brings together permissions in SharePoint Online and Microsoft Purview Information Protection.

- ACLs for MIP encrypted docs are inherited from the SPO site – **fewer access issues to debug** [2 ACLs → 1 ACL].
- Managing ACLs is delegated to the site admin (== data owner) **– less overhead for the compliance admin**
- Simple and consistent enforcement of access to encrypted data – **makes online and offline/downloaded files instantly inaccessible when user is removed from the site**
- No need to create a label per project/site - **Prevents label sprawl**



Admin has defined default sensitivity label for SharePoint site

Admin removes Henry from the site

Henry cannot re-open already downloaded file – instantly loses access!

Henry Brill has been removed from the group

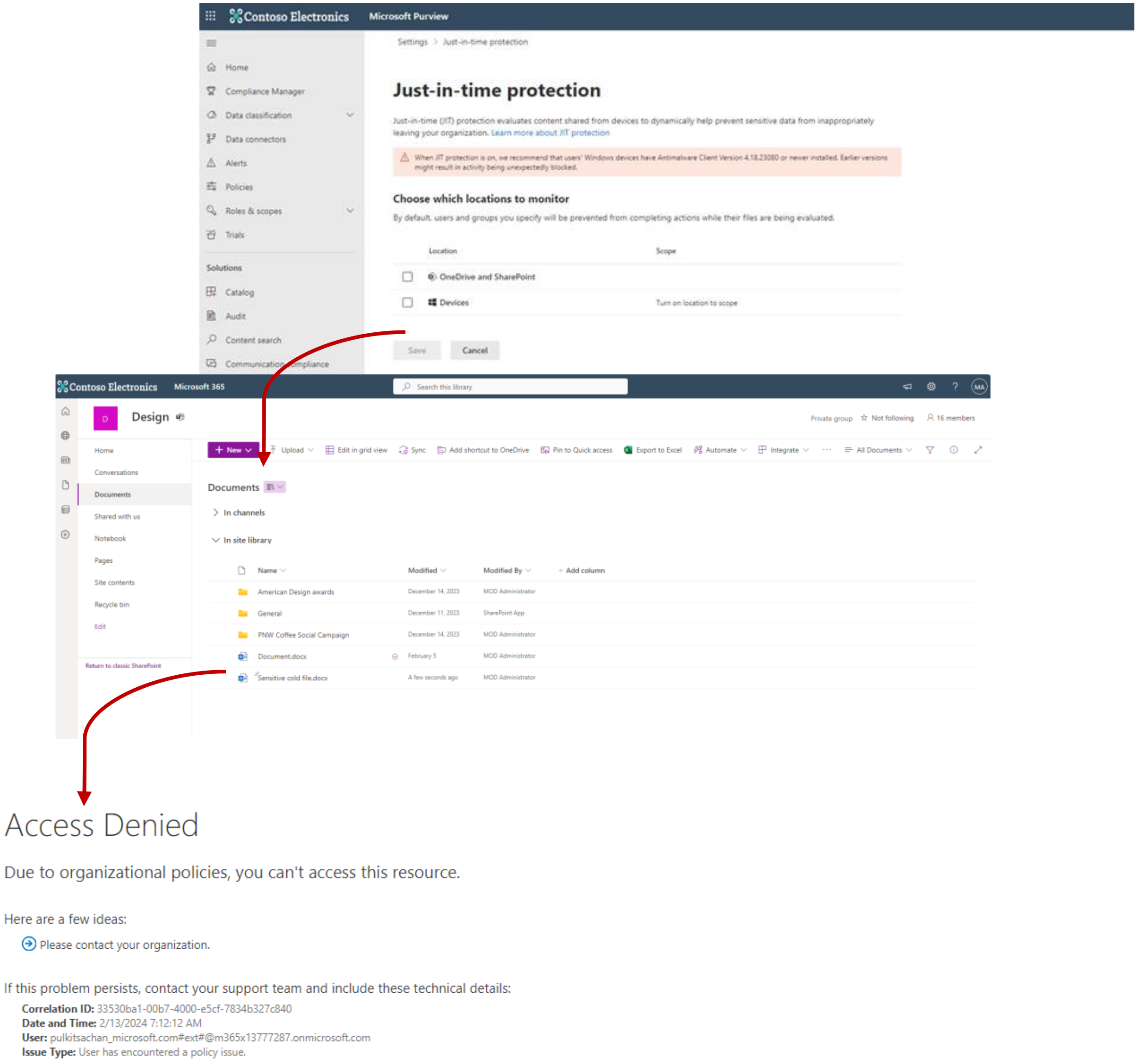
Microsoft Word

You are signed in, but your account no longer has access to this file. Please contact the file owner.

Just-in-time on SPOD

With Just in time protection Admins can be sure that each file will be evaluated and protected by DLP on the latest policy posture

- Admin can turn on JIT for both OneDrive and SharePoint.
- A cold file which hasn't been evaluated by DLP will appear as non-sensitive to both internal and external user
- With JIT protection on – every access will be evaluated and enforced as per the latest policy posture



Just-in-time protection

Just-in-time (JIT) protection evaluates content shared from devices to dynamically help prevent sensitive data from inappropriately leaving your organization. Learn more about JIT protection

When JIT protection is on, we recommend that users' Windows devices have Antimalware Client Version 4.18.23080 or newer installed. Earlier versions might result in activity being unexpectedly blocked.

Choose which locations to monitor

By default, users and groups you specify will be prevented from completing actions while their files are being evaluated.

	Location	Scope
☐	OneDrive and SharePoint	
☐	Devices	Turn on location to scope

Name	Modified	Modified By	+ Add column
American Design awards	December 14, 2023	MOD Administrator	
General	December 11, 2023	SharePoint App	
PNW Coffee Social Campaign	December 14, 2023	MOD Administrator	
Document.docx	February 5	MOD Administrator	
Sensitive cold file.docx	A few seconds ago	MOD Administrator	

Access Denied

Due to organizational policies, you can't access this resource.

Here are a few ideas:

Please contact your organization.

If this problem persists, contact your support team and include these technical details:

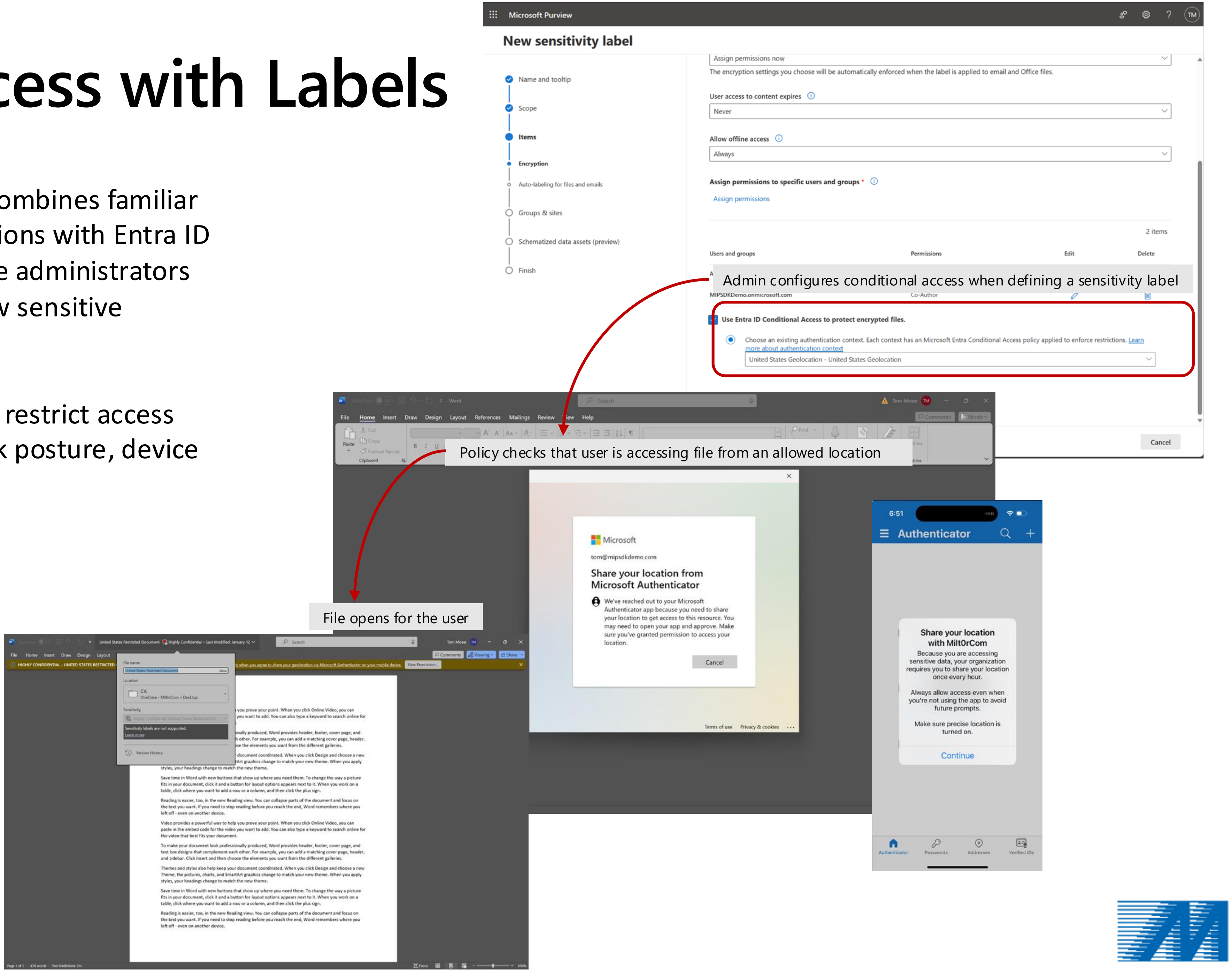
Correlation ID: 33530ba1-00b7-4000-e5cf-7834b327c840
Date and Time: 2/13/2024 7:12:12 AM
User: pulkitsachan_microsoft.com#ext#@m365x13777287.onmicrosoft.com
Issue Type: User has encountered a policy issue.

Conditional Access with Labels

- Label-Based Conditional Access combines familiar sensitivity labeling-based protections with Entra ID Conditional Access policies to give administrators more control over where and how sensitive information can be accessed.
- Label policies can be extended to restrict access based on user attributes, user risk posture, device status, user location, and more.

Scenario in which a user is granted access:
A user trying to access Swiss customer data from **Switzerland** will be granted access to files labeled as “Confidential\Swiss Customer Data”

Scenario in which a user is denied access:
A user trying to access Swiss customer data from **Germany** will be denied access to files labeled as “Confidential\Swiss Customer Data”



New sensitivity label

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

Allow offline access: Always

Assign permissions to specific users and groups *

Assign permissions

2 items

Users and groups	Permissions	Edit	Delete
MIPSDKDemo.onmicrosoft.com	Co-Author		

☑ Use Entra ID Conditional Access to protect encrypted files.

● Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. Learn more about authentication context

United States Geolocation - United States Geolocation

Admin configures conditional access when defining a sensitivity label

Policy checks that user is accessing file from an allowed location

Microsoft

tom@mipsdkdemo.com

Share your location from Microsoft Authenticator

We've reached out to your Microsoft Authenticator app because you need to share your location to get access to this resource. You may need to open your app and approve. Make sure you've granted permission to access your location.

Cancel

Share your location with Milt0rCom

Because you are accessing sensitive data, your organization requires you to share your location once every hour.

Always allow access even when you're not using the app to avoid future prompts.

Make sure precise location is turned on.

Continue

File opens for the user

United States Restricted Document · Highly Confidential · Last Modified: January 12

HIGHLY CONFIDENTIAL - UNITED STATES RESTRICTED … when you agree to share your geolocation via Microsoft Authenticator on your mobile device.

File name: United States Restricted Document.docx

Location: CA — OneDrive - Milt0rCom » Desktop

Sensitivity: Highly Confidential\United States Restricted Inf...

Sensitivity labels are not supported.
Learn more

Version History

Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it and a button for layout options appears next to it. When you work on a table, click where you want to add a row or a column, and then click the plus sign.

Reading is easier, too, in the new Reading view. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off - even on another device.

Video provides a powerful way to help you prove your point. When you click Online Video, you can paste in the embed code for the video you want to add. You can also type a keyword to search online for the video that best fits your document.

To make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you can add a matching cover page, header, and sidebar. Click Insert and then choose the elements you want from the different galleries.

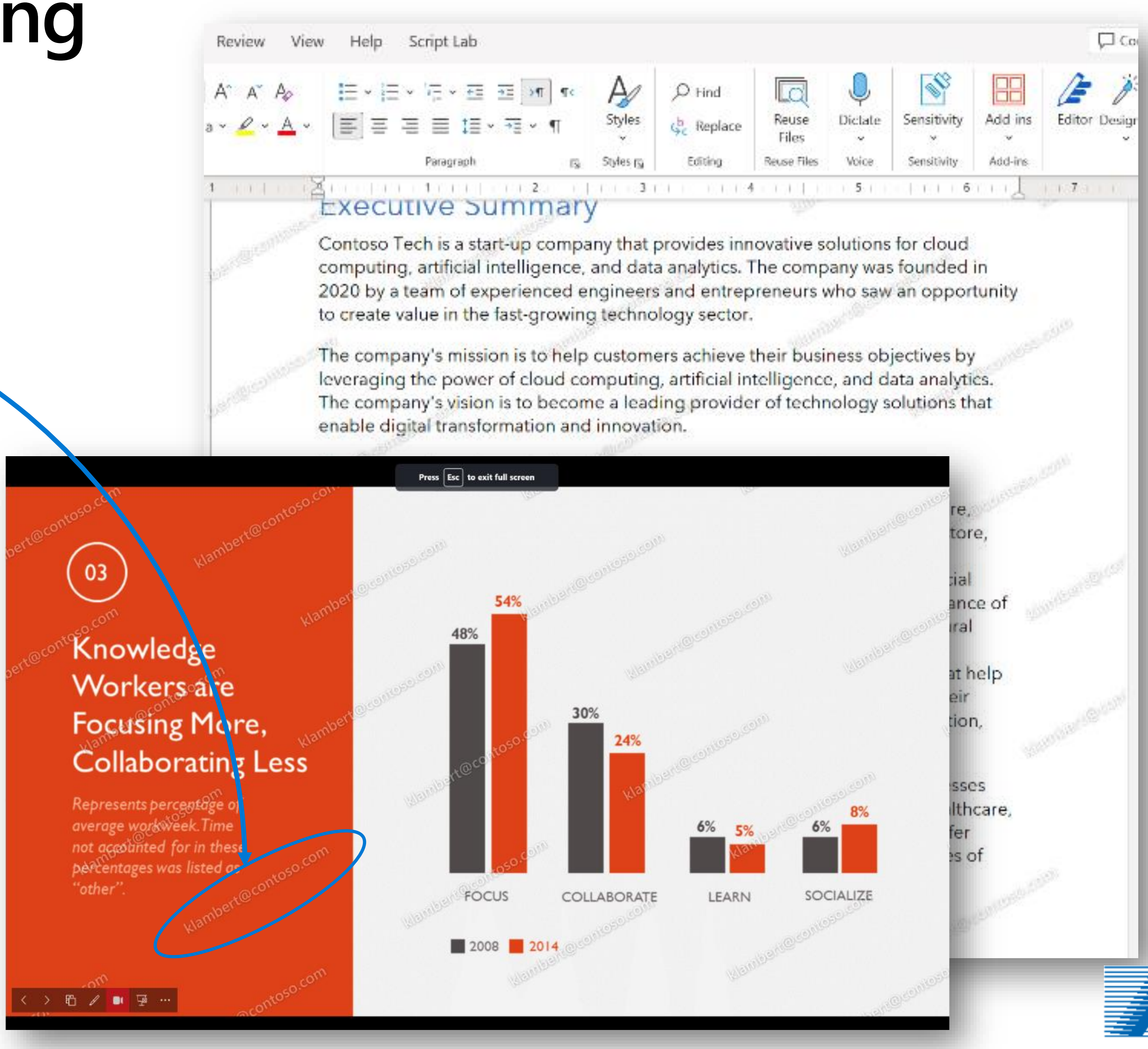
Themes and styles also help keep your document coordinated. When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you apply styles, your headings change to match the new theme.

Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it and a button for layout options appears next to it. When you work on a table, click where you want to add a row or a column, and then click the plus sign.

Reading is easier, too, in the new Reading view. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off - even on another device.

Dynamic Watermarking

- Dynamic watermarking provides customers with the controls to require virtualized watermarks on labeled documents.
- Renders user's email address across the document.
- Discourages unauthorized photos and sharing in Teams.



Executive Summary

Contoso Tech is a start-up company that provides innovative solutions for cloud computing, artificial intelligence, and data analytics. The company was founded in 2020 by a team of experienced engineers and entrepreneurs who saw an opportunity to create value in the fast-growing technology sector.

The company's mission is to help customers achieve their business objectives by leveraging the power of cloud computing, artificial intelligence, and data analytics. The company's vision is to become a leading provider of technology solutions that enable digital transformation and innovation.

03

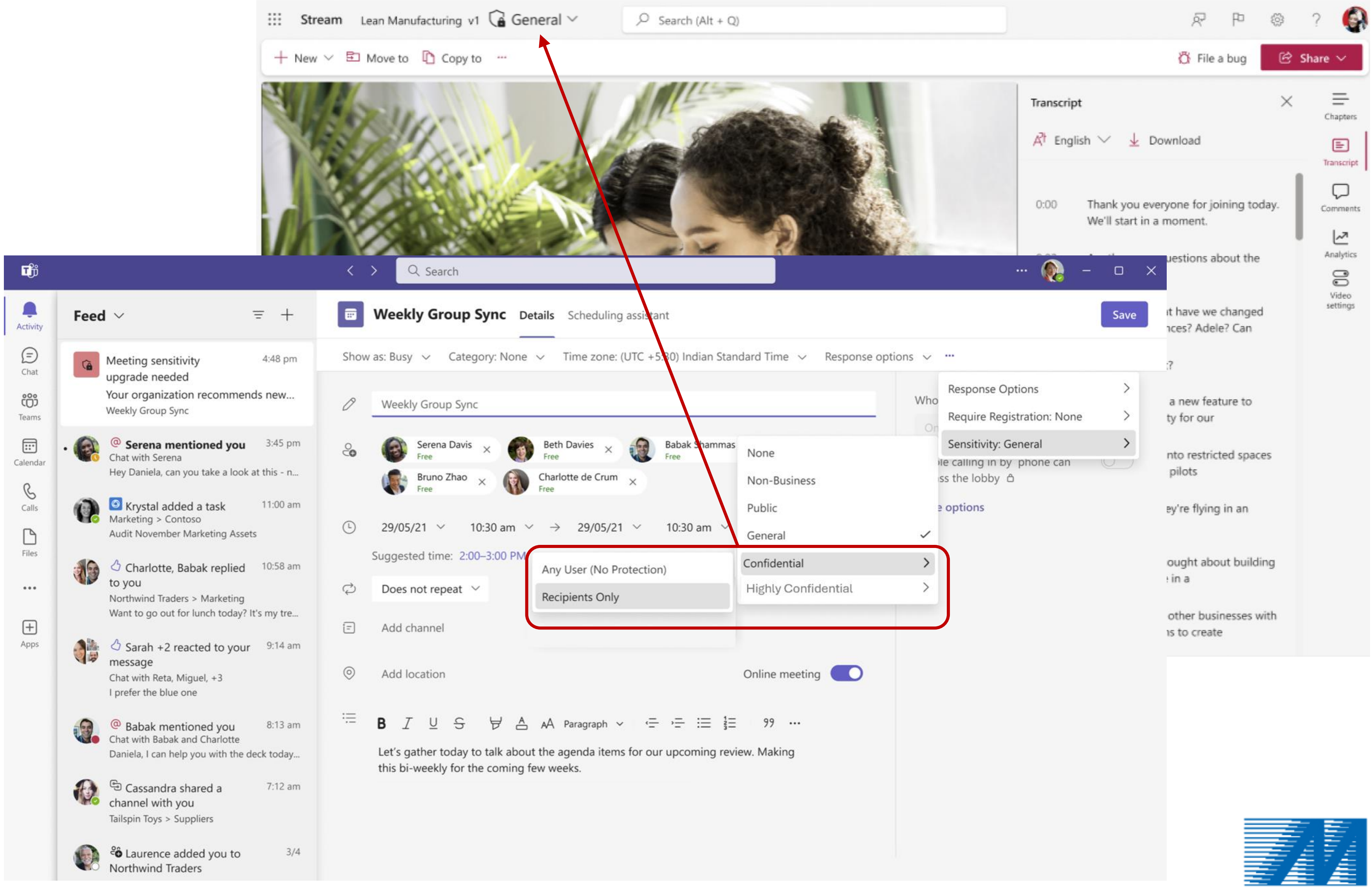
Knowledge Workers are Focusing More, Collaborating Less

Represents percentage of average workweek. Time not accounted for in these percentages was listed as "other".

Labeling meetings recordings, transcripts with inheritance

Labeled meetings will automatically inherit the label to meeting artifacts:

1. Support labeling for recording and transcripts
2. Meeting recording and transcripts inherit the same label after a meeting is finished
3. Labeled recordings can be protected from oversharing by preventing file download
4. Labeled transcripts can restrict sensitive chats from being processed by Copilot



0:00 Thank you everyone for joining today. We'll start in a moment.

Meeting sensitivity upgrade needed 4:48 pm
Your organization recommends new...
Weekly Group Sync

Serena mentioned you 3:45 pm
Chat with Serena
Hey Daniela, can you take a look at this - n...

Krystal added a task 11:00 am
Marketing > Contoso
Audit November Marketing Assets

Charlotte, Babak replied to you 10:58 am
Northwind Traders > Marketing
Want to go out for lunch today? It's my tre...

Sarah +2 reacted to your message 9:14 am
Chat with Reta, Miguel, +3
I prefer the blue one

Babak mentioned you 8:13 am
Chat with Babak and Charlotte
Daniela, I can help you with the deck today...

Cassandra shared a channel with you 7:12 am
Tailspin Toys > Suppliers

Laurence added you to Northwind Traders 3/4

Weekly Group Sync

Show as: Busy | Category: None | Time zone: (UTC +5:30) Indian Standard Time | Response options

Weekly Group Sync

Serena Davis Free, Beth Davies Free, Babak Shammas Free, Bruno Zhao Free, Charlotte de Crum Free

29/05/21 10:30 am → 29/05/21 10:30 am

Suggested time: 2:00–3:00 PM

Does not repeat

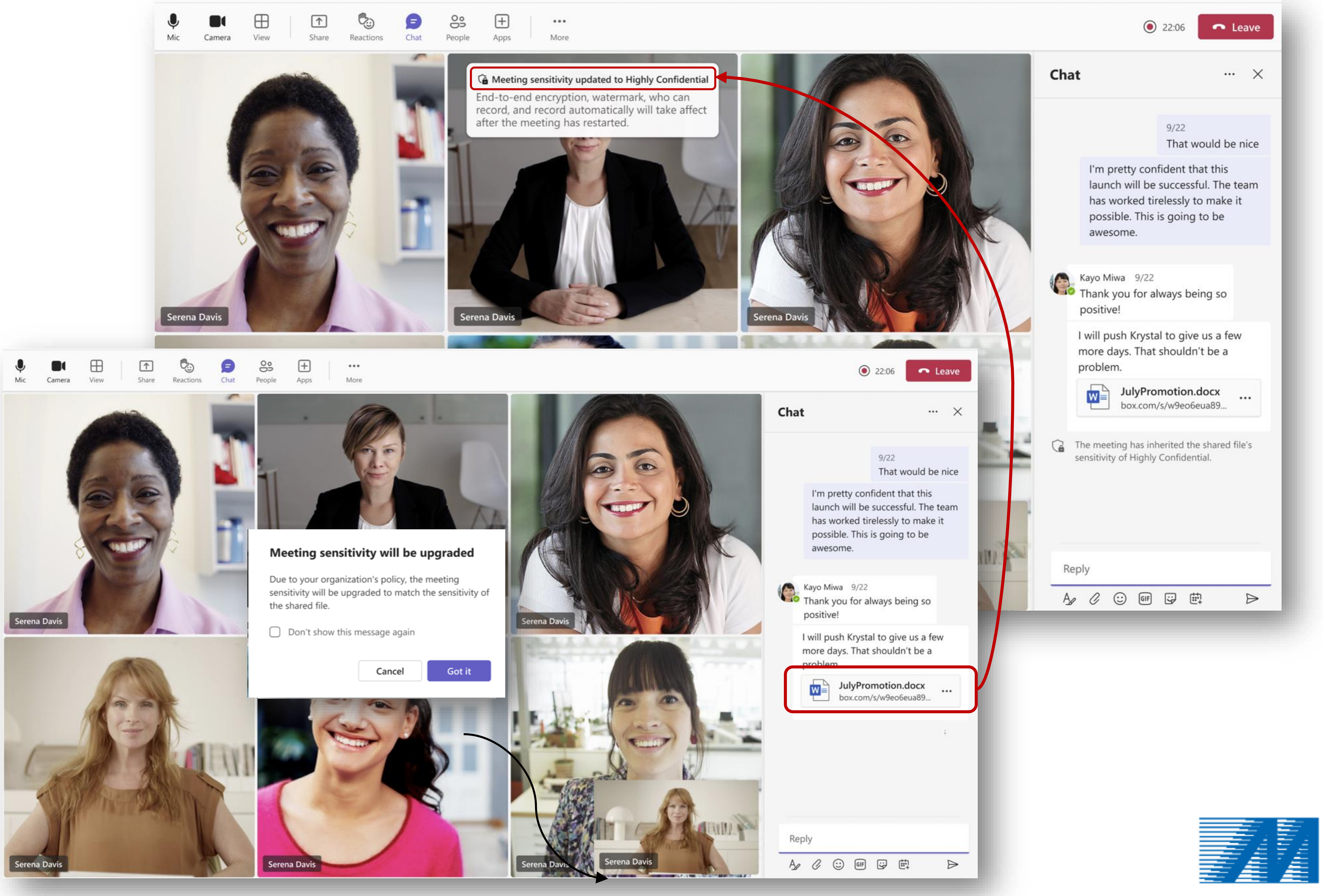
Sensitivity: General

Let's gather today to talk about the agenda items for our upcoming review. Making this bi-weekly for the coming few weeks.

Automatic labeling of meetings from sensitive docs

Protected meeting will automatically label based on the most sensitive shared content:

1. Labeled documents shared through chats or windows share can upgrade label on meeting
2. Labels can be recommended or automatically applied to meeting from shared documents



Meeting sensitivity updated to Highly Confidential

End-to-end encryption, watermark, who can record, and record automatically will take affect after the meeting has restarted.

9/22
That would be nice

I'm pretty confident that this launch will be successful. The team has worked tirelessly to make it possible. This is going to be awesome.

Kayo Miwa 9/22
Thank you for always being so positive!

I will push Krystal to give us a few more days. That shouldn't be a problem.

JulyPromotion.docx
box.com/s/w9eo6eua89...

The meeting has inherited the shared file's sensitivity of Highly Confidential.

Meeting sensitivity will be upgraded

Due to your organization's policy, the meeting sensitivity will be upgraded to match the sensitivity of the shared file.

☐ Don't show this message again

9/22
That would be nice

I'm pretty confident that this launch will be successful. The team has worked tirelessly to make it possible. This is going to be awesome.

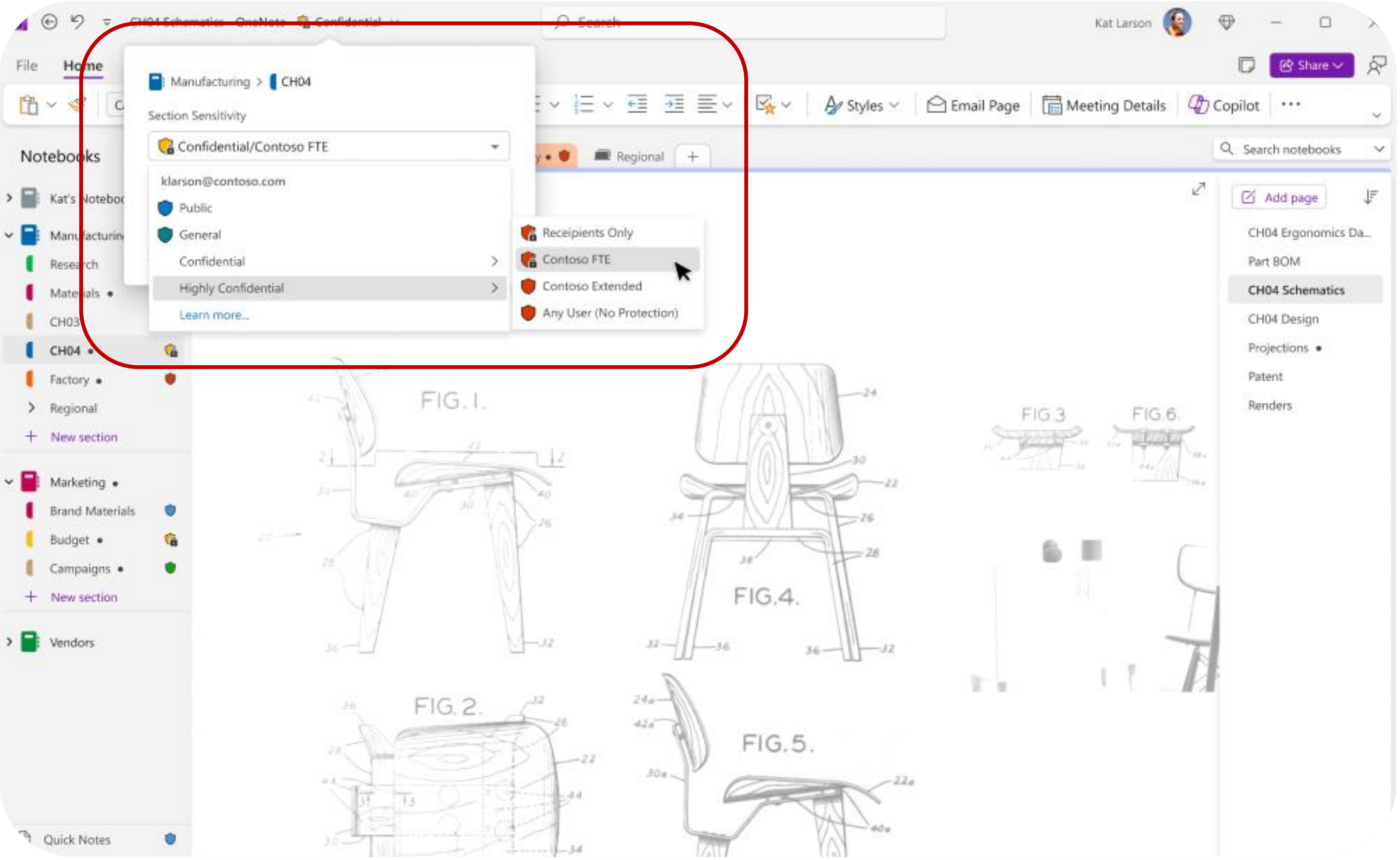
Kayo Miwa 9/22
Thank you for always being so positive!

I will push Krystal to give us a few more days. That shouldn't be a problem.

JulyPromotion.docx
box.com/s/w9eo6eua89...

Labeling in OneNote

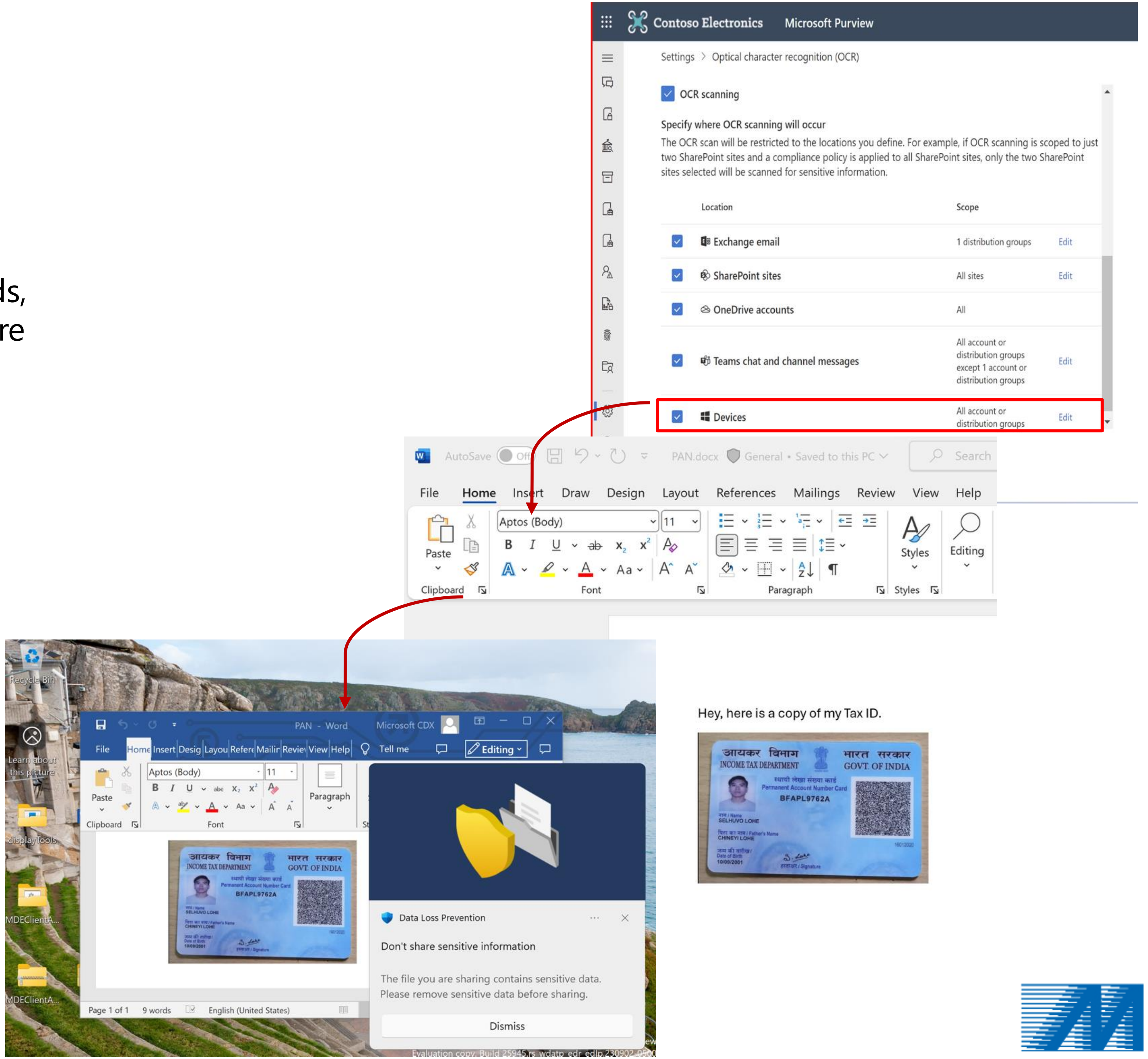
- Extending OneNote to support sensitivity labeling and protection.



Section Sensitivity: Confidential/Contoso FTE

Embedded OCR

- With embedded OCR support across workloads, customers will be able to scan images which are embedded inside office and archive files
- Images inside hybrid PDF files which contain images as well as searchable text will also get scanned using OCR.
- No admin intervention: The existing OCR settings will seamlessly extend and apply to embedded images



Settings > Optical character recognition (OCR)

☑ OCR scanning

Specify where OCR scanning will occur

The OCR scan will be restricted to the locations you define. For example, if OCR scanning is scoped to just two SharePoint sites and a compliance policy is applied to all SharePoint sites, only the two SharePoint sites selected will be scanned for sensitive information.

	Location	Scope	
☑	Exchange email	1 distribution groups	Edit
☑	SharePoint sites	All sites	Edit
☑	OneDrive accounts	All	
☑	Teams chat and channel messages	All account or distribution groups except 1 account or distribution groups	Edit
☑	Devices	All account or distribution groups	Edit

Data Loss Prevention

Don't share sensitive information

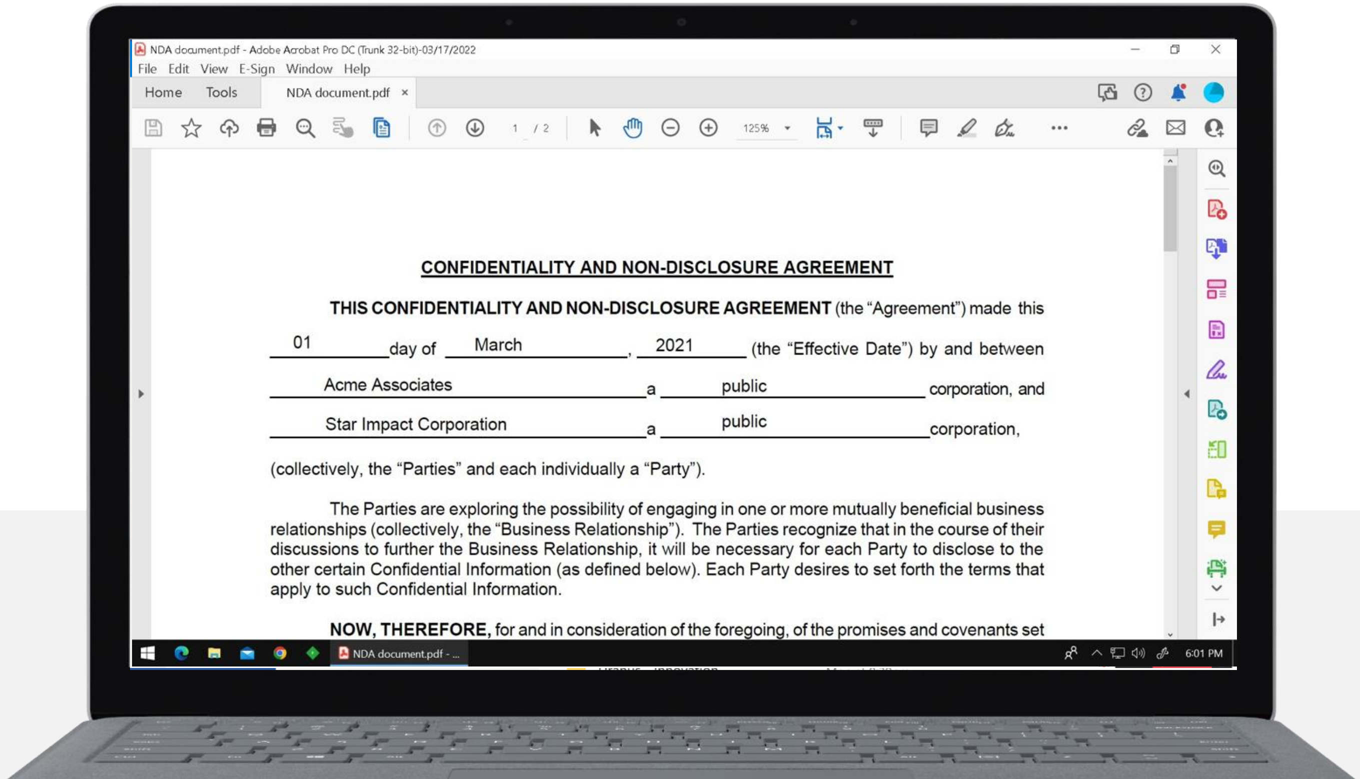
The file you are sharing contains sensitive data. Please remove sensitive data before sharing.

Dismiss

Hey, here is a copy of my Tax ID.

Protect your most important PDF files

1. Office PDF support
2. SharePoint renders protected PDFs
3. SharePoint auto-labeling support for PDF
4. Adobe Acrobat native support for labels


NDA document.pdf - Adobe Acrobat Pro DC (Trunk 32-bit)-03/17/2022
File Edit View E-Sign Window Help
Home
Tools
NDA document.pdf ×
1 / 2
125%
NDA document.pdf - ...
6:01 PM

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT (the "Agreement") made this 01 day of March, 2021 (the "Effective Date") by and between Acme Associates a public corporation, and Star Impact Corporation a public corporation,

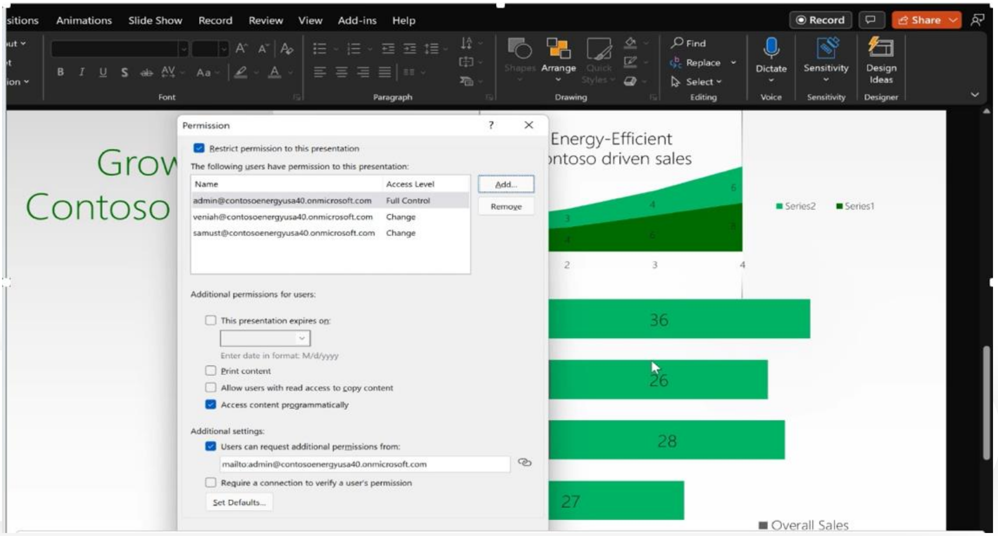
(collectively, the "Parties" and each individually a "Party").

The Parties are exploring the possibility of engaging in one or more mutually beneficial business relationships (collectively, the "Business Relationship"). The Parties recognize that in the course of their discussions to further the Business Relationship, it will be necessary for each Party to disclose to the other certain Confidential Information (as defined below). Each Party desires to set forth the terms that apply to such Confidential Information.

NOW, THEREFORE, for and in consideration of the foregoing, of the promises and covenants set

User-defined permissions for secure collaboration

- Users can choose specific users/groups for read/change permissions at the file level (no need for admins to create labels)
- Protection travels with the document, no matter where and how the document travels
- Co-authoring support of encrypted Office files with user-defined permissions in SharePoint



Permission

☑ Restrict permission to this presentation

The following users have permission to this presentation:

Name	Access Level
admin@contosoenergyusa40.onmicrosoft.com	Full Control
veniah@contosoenergyusa40.onmicrosoft.com	Change
samust@contosoenergyusa40.onmicrosoft.com	Change

Additional permissions for users:

☐ This presentation expires on:

Enter date in format: M/d/yyyy

☐ Print content

☐ Allow users with read access to copy content

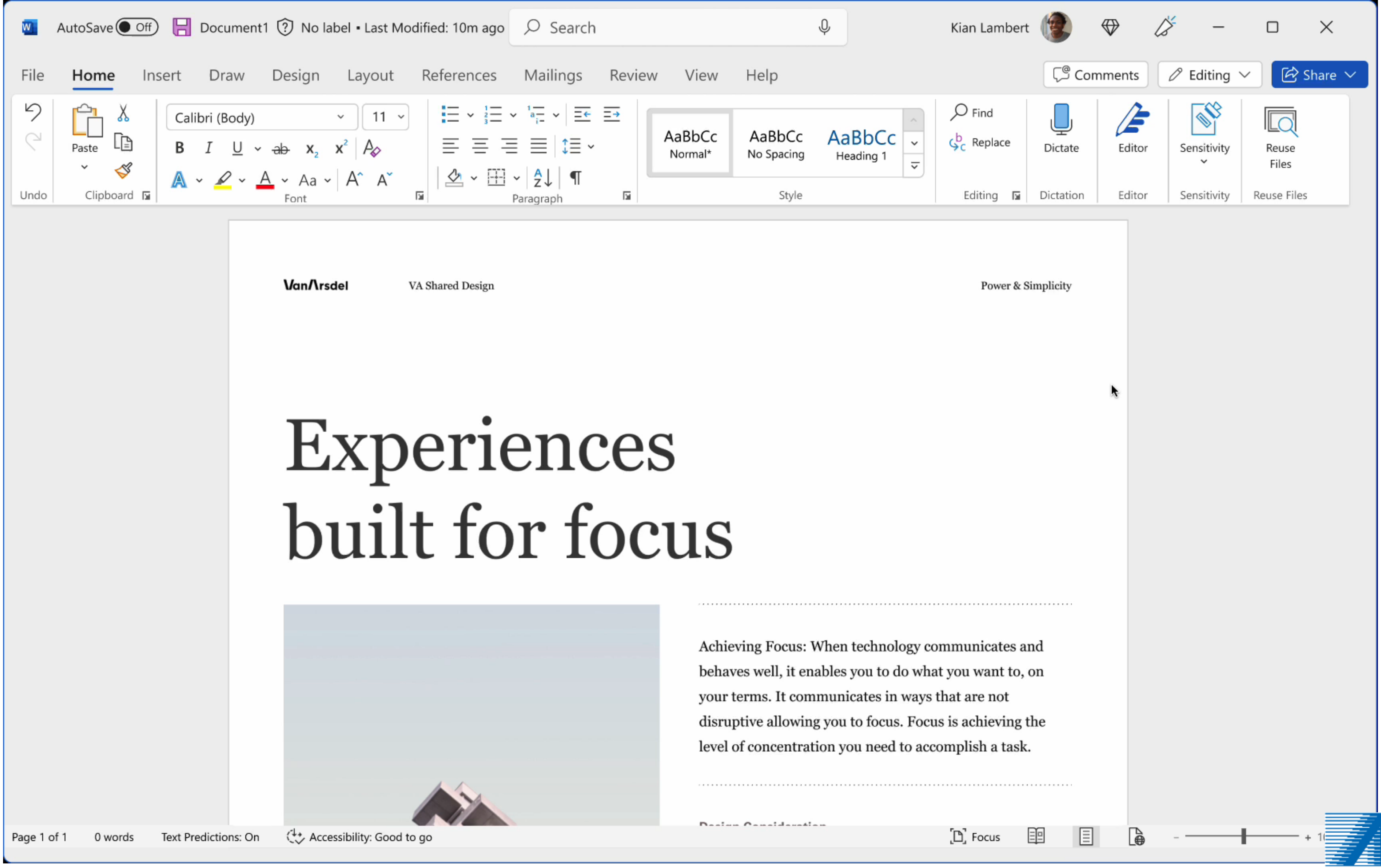
☑ Access content programmatically

Additional settings:

☑ Users can request additional permissions from:

mailto:admin@contosoenergyusa40.onmicrosoft.com

☐ Require a connection to verify a user's permission



VanArsdel VA Shared Design Power & Simplicity

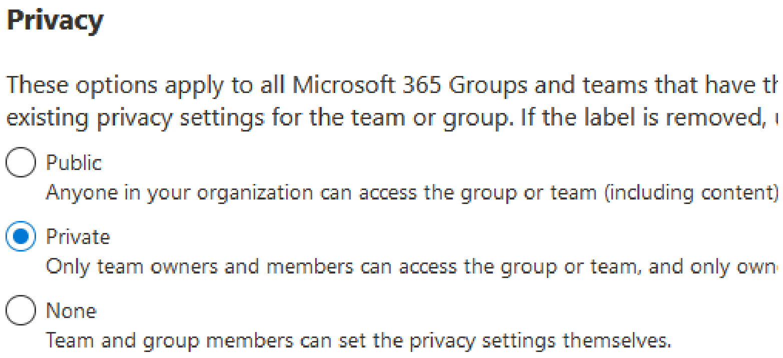
Experiences built for focus

Achieving Focus: When technology communicates and behaves well, it enables you to do what you want to, on your terms. It communicates in ways that are not disruptive allowing you to focus. Focus is achieving the level of concentration you need to accomplish a task.

Design Consideration

Sensitivity labels to protect Microsoft Teams shared channels

- Private Teams discoverability control
- Shared channel controls provide access controls to shared channels based on the label applied to the Team: internal only, same team only (internal), or private Teams only.



Privacy

These options apply to all Microsoft 365 Groups and teams that have t
existing privacy settings for the team or group. If the label is removed,

○ Public
Anyone in your organization can access the group or team (including content)

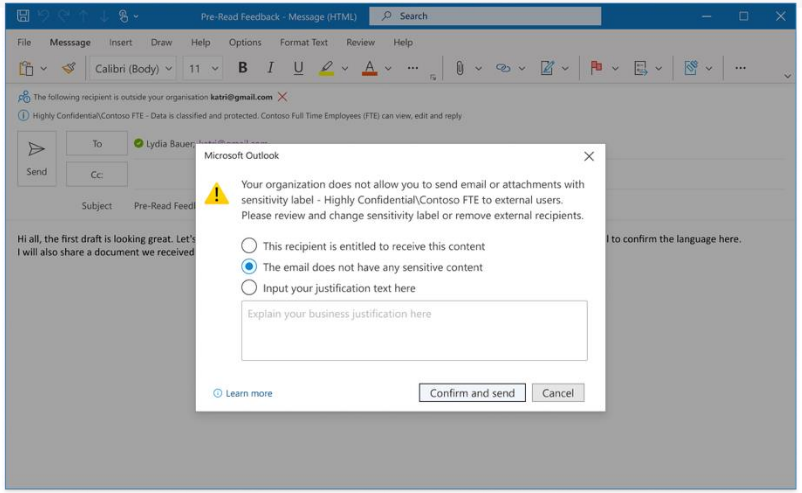
● Private
Only team owners and members can access the group or team, and only own

○ None
Team and group members can set the privacy settings themselves.

Configure policy tips as popups for labeled emails and attachments

- Configure DLP rules that display warnings in a popup dialog before sending emails.
- Admins can set up rules to provide warnings, require business justifications, or request explicit acknowledgements before sending emails

Generally available in Office version v2302



The following recipient is outside your organisation **katri@gmail.com**

Highly Confidential\Contoso FTE - Data is classified and protected. Contoso Full Time Employees (FTE) can view, edit and reply

Hi all, the first draft is looking great. Let's … I to confirm the language here.
I will also share a document we received …

Microsoft Outlook

Your organization does not allow you to send email or attachments with sensitivity label - Highly Confidential\Contoso FTE to external users. Please review and change sensitivity label or remove external recipients.

○ This recipient is entitled to receive this content
● The email does not have any sensitive content
○ Input your justification text here

Explain your business justification here

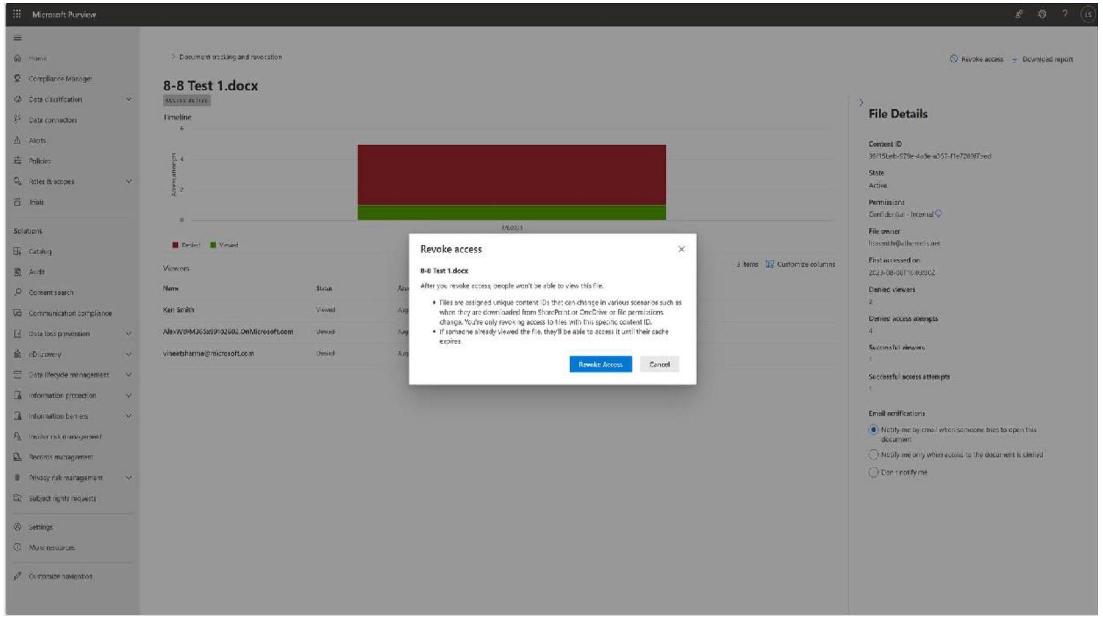
Double Key Encryption (DKE)

- Use double-key encryption to protect your most sensitive files and emails in Microsoft 365 Apps on Windows with built-in labeling
- With DKE, Microsoft stores one key in Microsoft Azure and you hold the other key, ensuring that only you can ever decrypt protected content, under all circumstances

Tracking and Revocation

Native in Information Protection

- Users can access the Microsoft Purview compliance portal to check who has tried accessing their sensitivity labeled and encrypted local Office files and revoke access when needed



8-8 Test 1.docx

Viewers

Name	Status
Ken Smith	Viewed
AlexW@M365x09102602.OnMicrosoft.com	Denied
vineetsharma@microsoft.com	Denied

Revoke access

8-8 Test 1.docx

After you revoke access, people won't be able to view this file.

- Files are assigned unique content IDs that can change in various scenarios such as when they are downloaded from SharePoint or OneDrive or file permissions change. You're only revoking access to files with this specific content ID.
- If someone already viewed the file, they'll be able to access it until their cache expires.

File Details

Content ID

State: Active

Permissions: Confidential - Internal

File owner

First accessed on

Denied viewers: 2

Denied access attempts: 4

Successful viewers: 1

Successful access attempts: 1

Email notifications

● Notify me by email when someone tries to open this document

○ Notify me only when access to the document is denied

○ Don't notify me

Growing ecosystem

200+ Purview and Priva partners

75 MISA partners

111 MISA products and services

> *"MISA transformed our ability to deliver a premium solution to our clients quickly by enriching our solution through integrations with Information Protection and Defender for Cloud Apps, allowing us to focus on our AI designed to automate Microsoft security tools."*
>
> Ami Marueli, Chief Technology Officer & Cofounder, Cognni

17a-4 LLC
ABLEINFO
ACTIVE CYPHER
ACTIVENAV
Adobe
AvePoint
ATAKAMA
BDO DIGITAL
box
Check Point SOFTWARE TECHNOLOGIES LTD.
cognni
DATA 443
DATAGUISE
dathena
DIGITALGUARDIAN
epiq
e-share
EY
FORCEPOINT
Gimmal
GTB Technologies Data Security that Works
HELUX
edgile a wipro company
Infotechtion
Informatica
KPMG
LIGHTHOUSE
netskope
nviso
nitro
xillio
opentext
paloalto NETWORKS
PKWARE
protiviti
Relativity
SECUDE
SecuPi
SECURITI.ai
SPIRION
servicenow
SUMMIT7
TeleMessage
VERITAS

Microsoft Purview Information Protection SDK

- Cross-platform SDK
- Extend classification, labeling, and protection
- Broadens the reach of information protection capabilities
- Used in Microsoft Purview Information Protection solutions
- Graph (REST) endpoint for Policy API

Platforms

Mac OS

iOS

Languages

.NET

Graph Service

Components of the SDK

File SDK

Abstraction of **Policy** and **Protection** API

Can **read** labels from supported files

Can **apply** labels to supported files

“Supported” files can be **expanded**

Policy SDK

Useful for **client** applications

Exposes policy for current user

Exposes **actions** for each label

Protection SDK

Protects plaintext content

Decrypts protected content

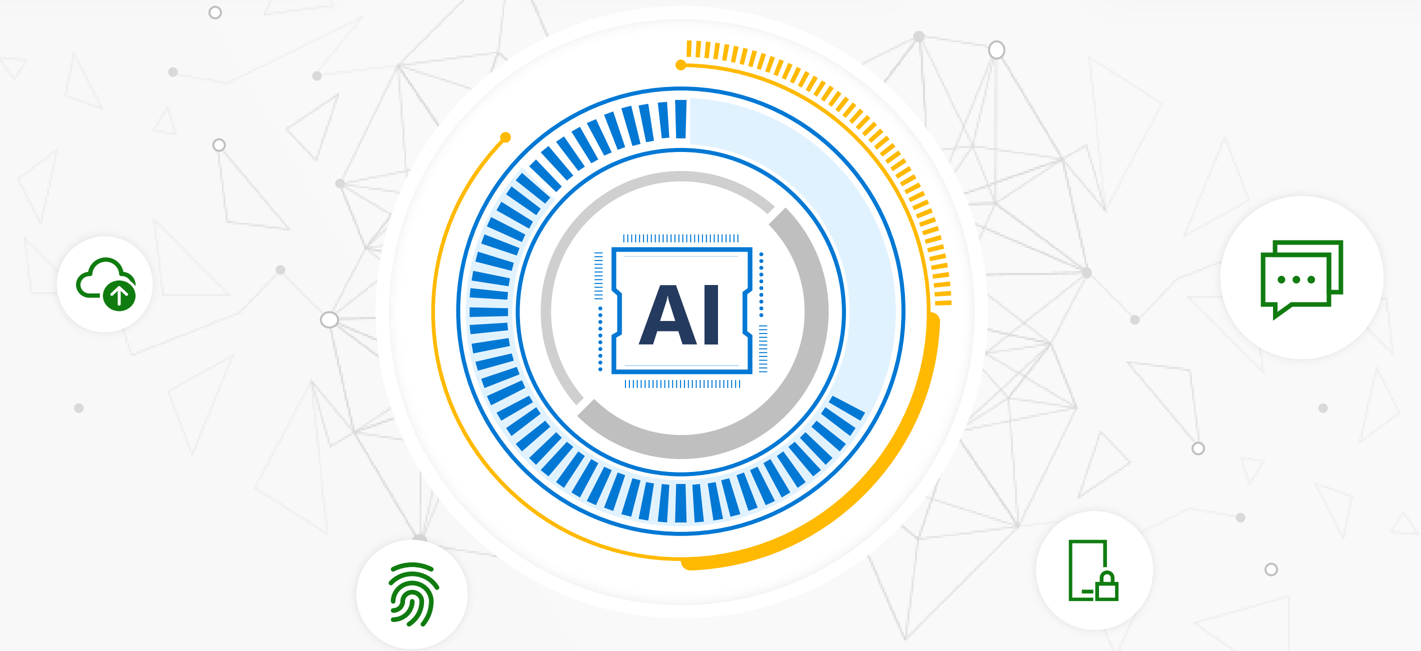
Rights enforcement is up to the developer

Information Protection and Microsoft 365 Copilot

[AI-powered data classification]

Microsoft Copilot for Microsoft 365

BRK298H Security for AI: Prepare, protect, and defend in the AI era

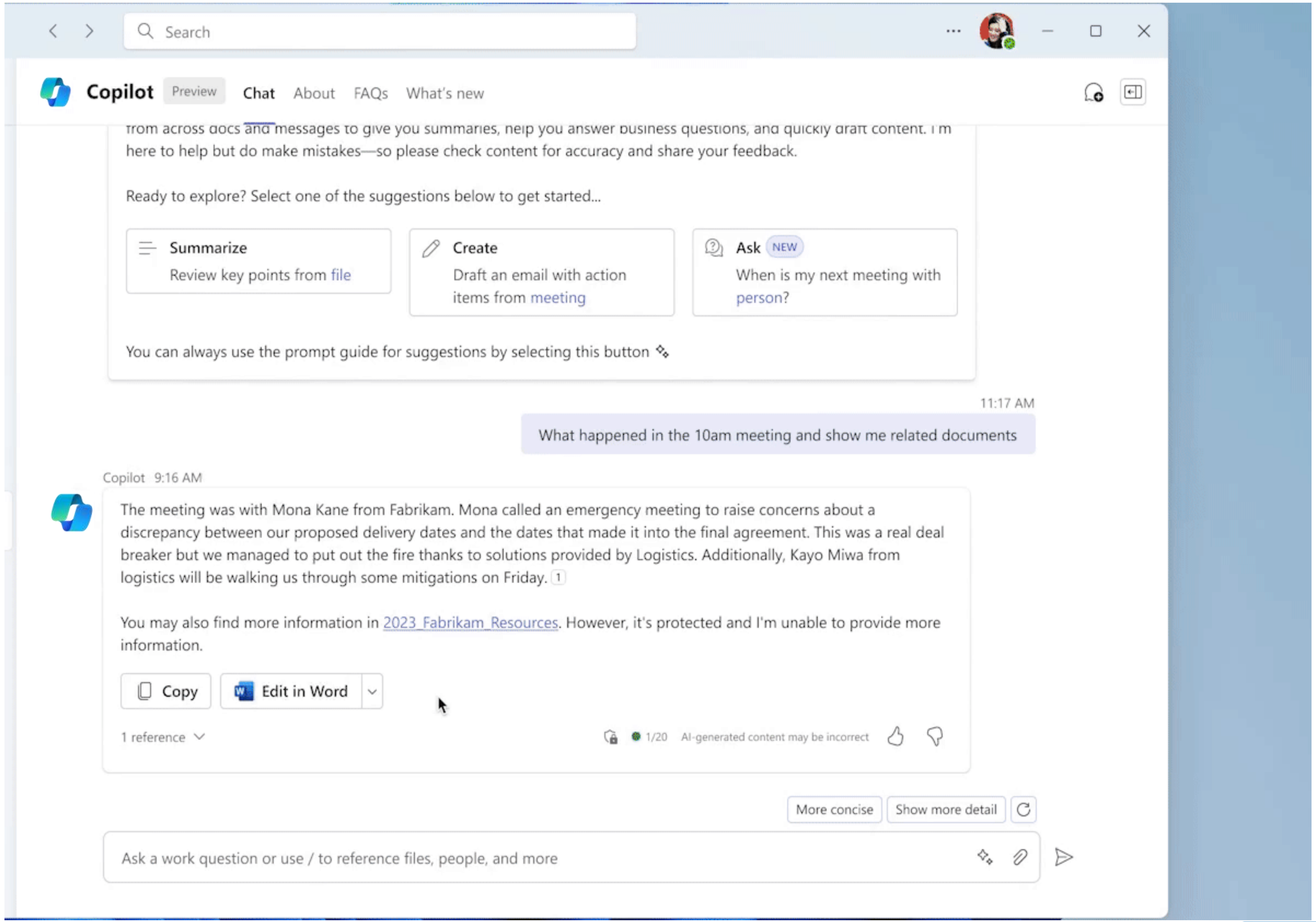


Copilot will honor access control restrictions on labeled content

Only content from references where the user has appropriate RMS permission will be included in responses.

If a user lacks the right RMS permissions, Copilot will inform the user and provide a link, but will not include the content for generating responses.

Copilot will not include information from referenced files where the user does not have appropriate access rights.


Search
Copilot
Preview
Chat
About
FAQs
What's new

from across docs and messages to give you summaries, help you answer business questions, and quickly draft content. I'm here to help but do make mistakes—so please check content for accuracy and share your feedback.

Ready to explore? Select one of the suggestions below to get started...

Summarize
Review key points from file
Create
Draft an email with action items from meeting
Ask NEW
When is my next meeting with person?

You can always use the prompt guide for suggestions by selecting this button

11:17 AM

What happened in the 10am meeting and show me related documents

Copilot 9:16 AM

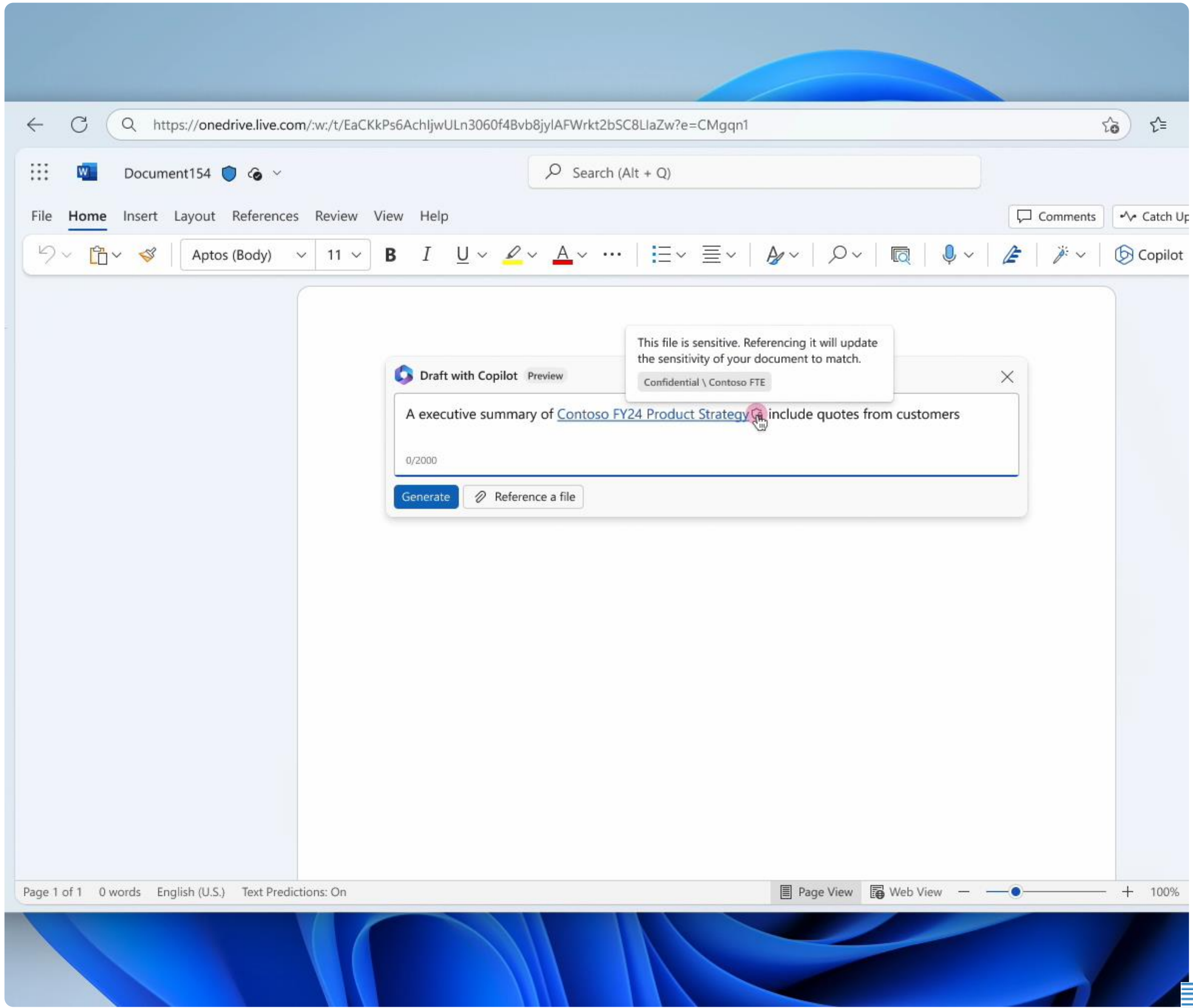
The meeting was with Mona Kane from Fabrikam. Mona called an emergency meeting to raise concerns about a discrepancy between our proposed delivery dates and the dates that made it into the final agreement. This was a real deal breaker but we managed to put out the fire thanks to solutions provided by 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.

Copy
Edit in Word
1 reference
1/20
AI-generated content may be incorrect
More concise
Show more detail
Ask a work question or use / to reference files, people, and more

Copilot can reason over data sensitivity

Users can see the sensitivity of the document that they reference within the Copilot prompt



This file is sensitive. Referencing it will update the sensitivity of your document to match.

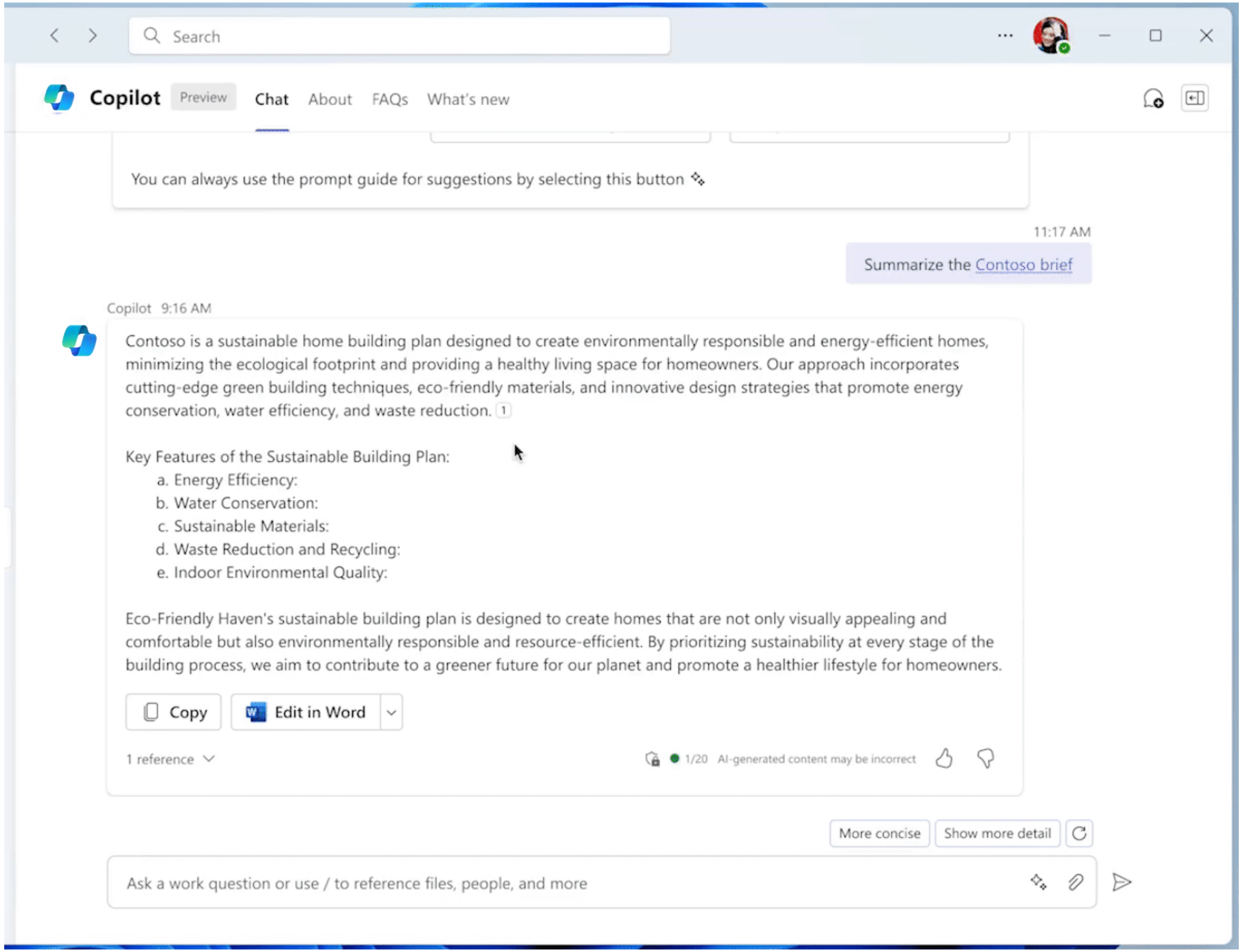
Confidential \ Contoso FTE

A executive summary of Contoso FY24 Product Strategy include quotes from customers

0/2000

Copilot can reason over data sensitivity

Users can see the sensitivity of the document that they reference within the citations of the Copilot output


Search
Copilot
Preview
Chat
About
FAQs
What's new
Copy
Edit in Word
1 reference
1/20
AI-generated content may be incorrect
More concise
Show more detail
Ask a work question or use / to reference files, people, and more

You can always use the prompt guide for suggestions by selecting this button

11:17 AM

Summarize the Contoso brief

Copilot 9:16 AM

Contoso is a sustainable home building plan designed to create environmentally responsible and energy-efficient homes, minimizing the ecological footprint and providing a healthy living space for homeowners. Our approach incorporates cutting-edge green building techniques, eco-friendly materials, and innovative design strategies that promote energy conservation, water efficiency, and waste reduction. [1]

Key Features of the Sustainable Building Plan:

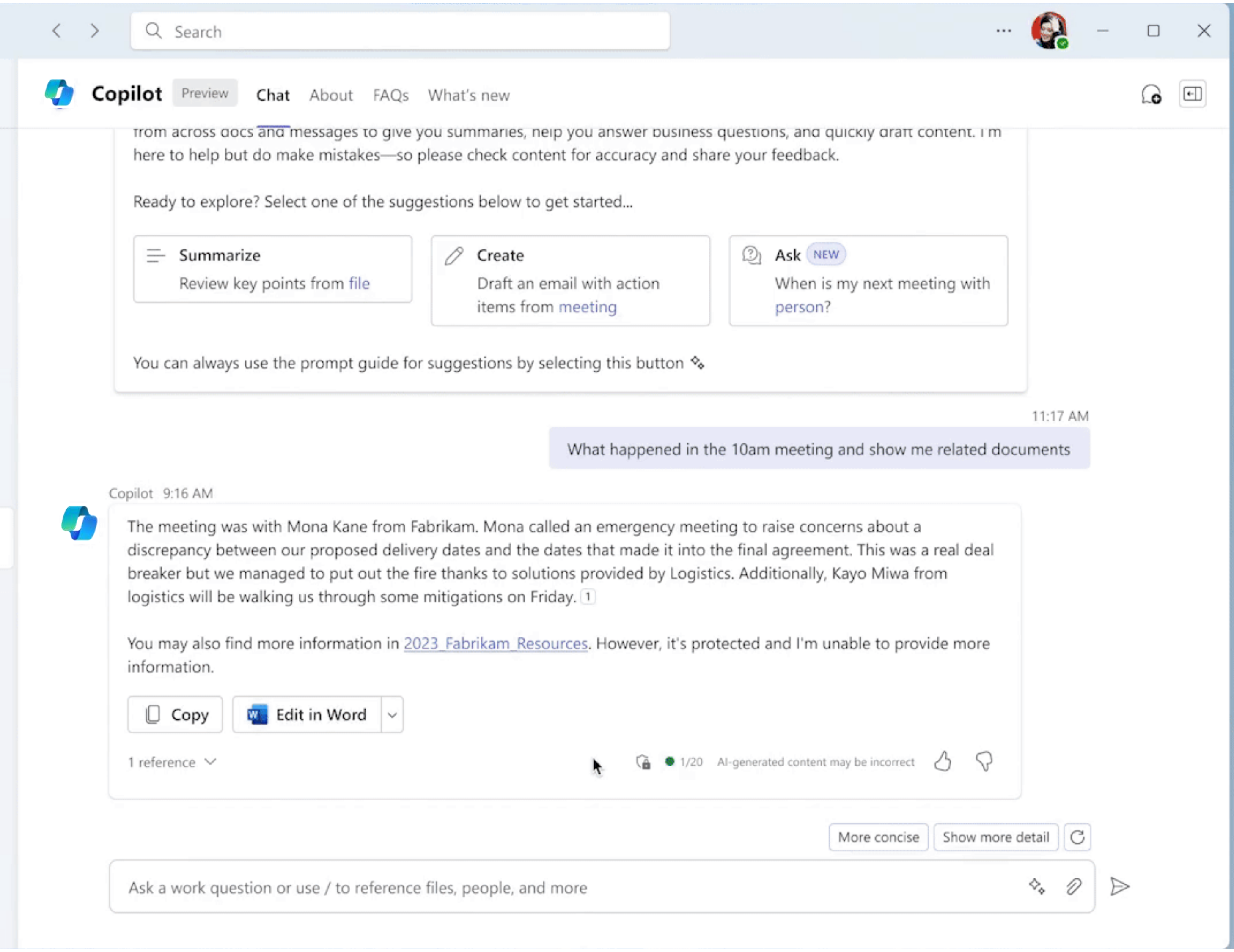
a. Energy Efficiency:
b. Water Conservation:
c. Sustainable Materials:
d. Waste Reduction and Recycling:
e. Indoor Environmental Quality:

Eco-Friendly Haven's sustainable building plan is designed to create homes that are not only visually appealing and comfortable but also environmentally responsible and resource-efficient. By prioritizing sustainability at every stage of the building process, we aim to contribute to a greener future for our planet and promote a healthier lifestyle for homeowners.

Copilot can reason over data sensitivity

A sensitivity label applies to the entire conversation.

Conversations inherit the most restrictive sensitivity labels from the references used to formulate a response.


Search
Copilot
Preview
Chat
About
FAQs
What's new

from across docs and messages to give you summaries, help you answer business questions, and quickly draft content. I'm here to help but do make mistakes—so please check content for accuracy and share your feedback.

Ready to explore? Select one of the suggestions below to get started...

Summarize
Review key points from file
Create
Draft an email with action items from meeting
Ask NEW
When is my next meeting with person?

You can always use the prompt guide for suggestions by selecting this button

11:17 AM

What happened in the 10am meeting and show me related documents

Copilot 9:16 AM

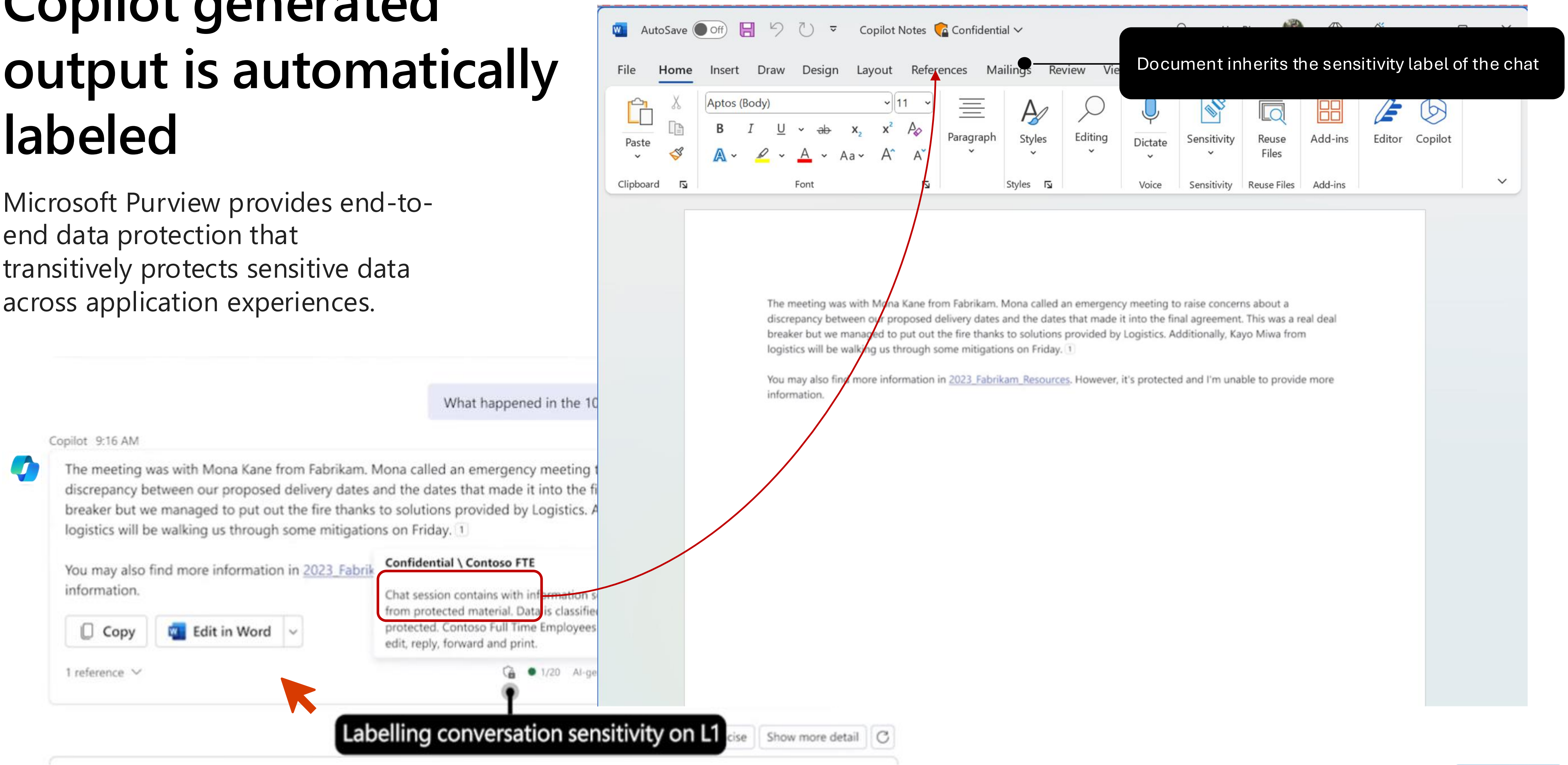
The meeting was with Mona Kane from Fabrikam. Mona called an emergency meeting to raise concerns about a discrepancy between our proposed delivery dates and the dates that made it into the final agreement. This was a real deal breaker but we managed to put out the fire thanks to solutions provided by 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.

Copy
Edit in Word
1 reference
1/20
AI-generated content may be incorrect
More concise
Show more detail
Ask a work question or use / to reference files, people, and more

Copilot generated output is automatically labeled

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.

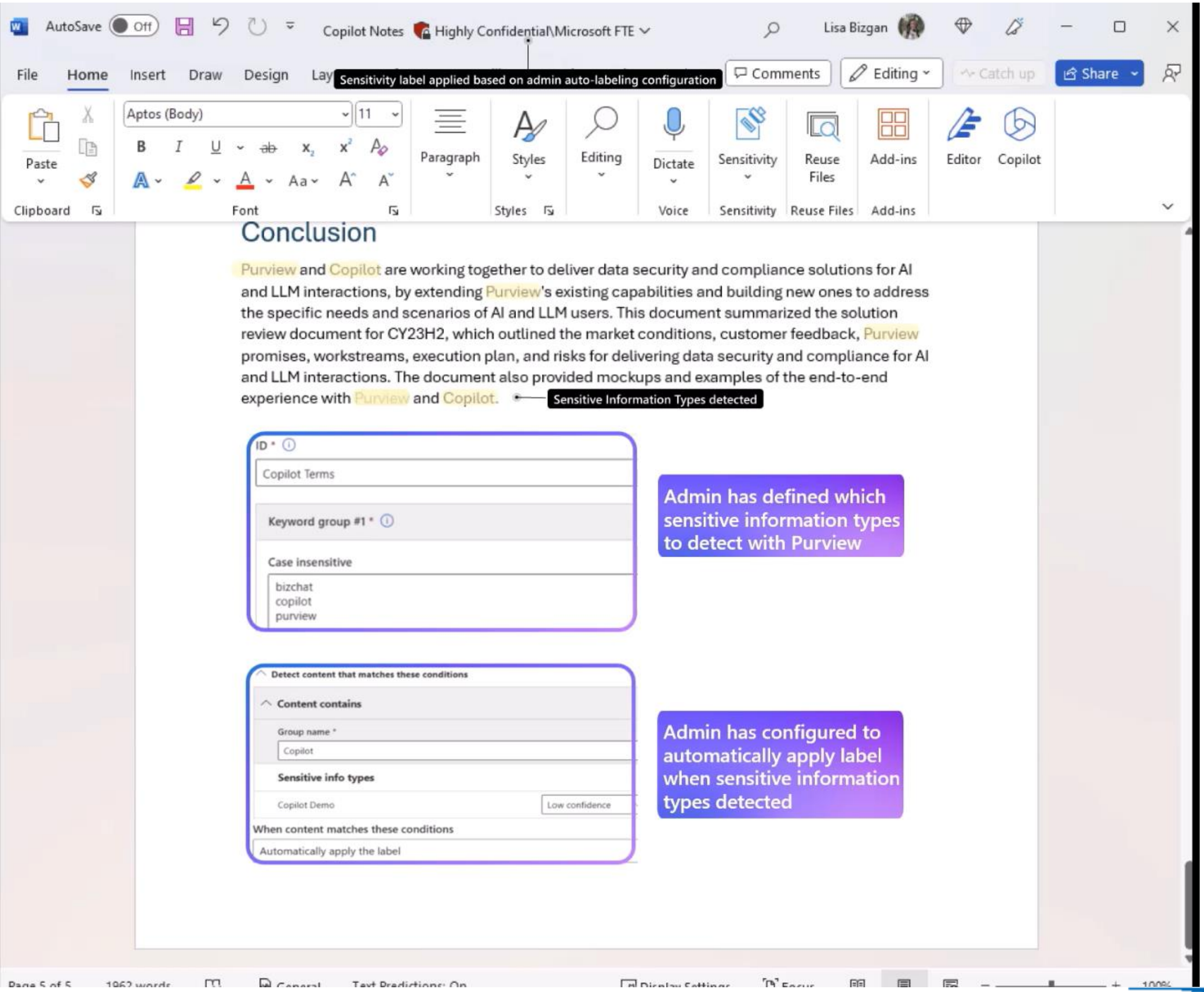
Confidential \ Contoso FTE

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 auto-matically labeled

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

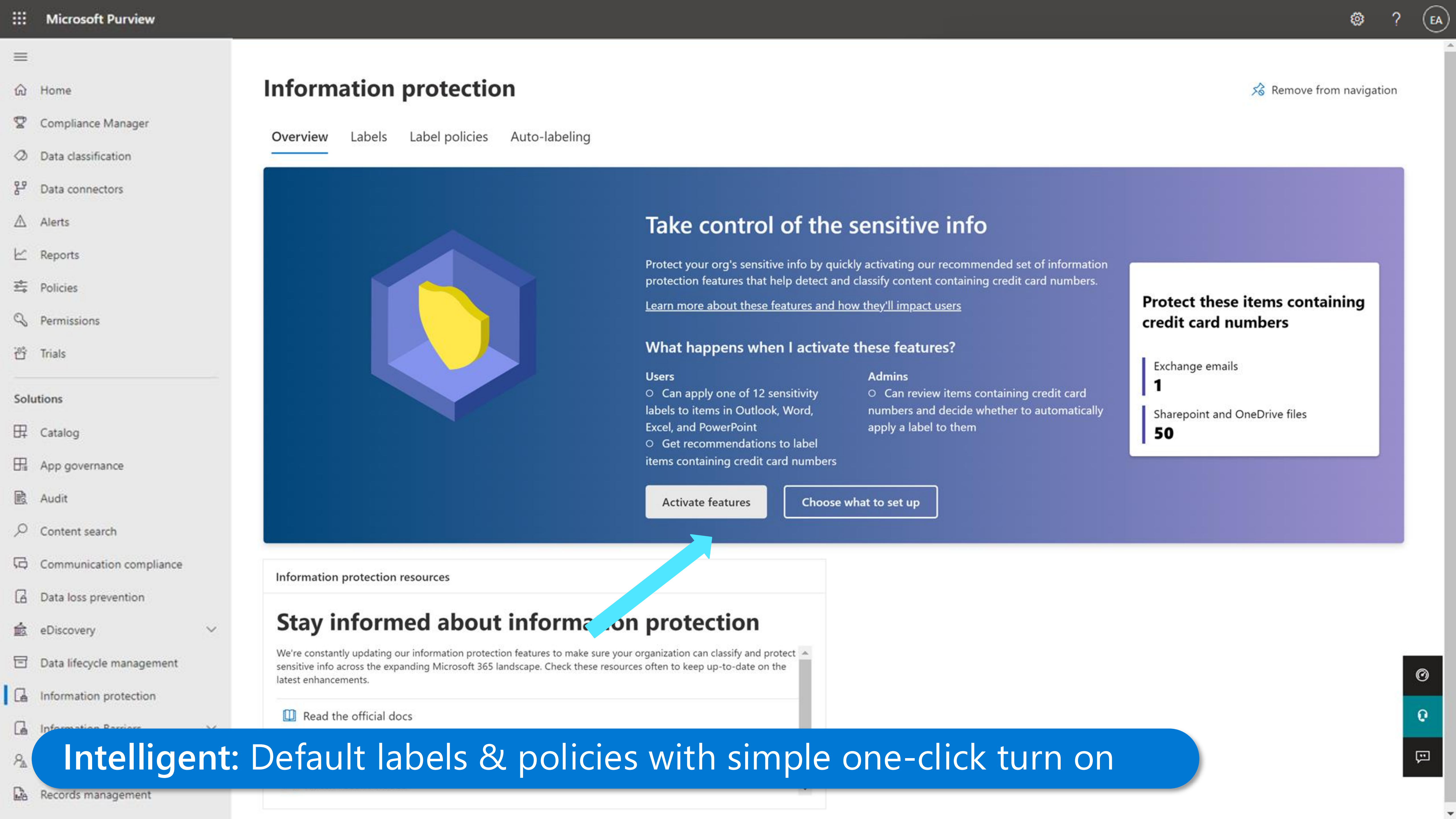
Sensitive info types

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



Information protection

Take control of the sensitive info

Protect your org's sensitive info by quickly activating our recommended set of information protection features that help detect and classify content containing credit card numbers.

Learn more about these features and how they'll impact users

What happens when I activate these features?

Users

- Can apply one of 12 sensitivity labels to items in Outlook, Word, Excel, and PowerPoint
- Get recommendations to label items containing credit card numbers

Admins

- Can review items containing credit card numbers and decide whether to automatically apply a label to them

Protect these items containing credit card numbers

Exchange emails
1

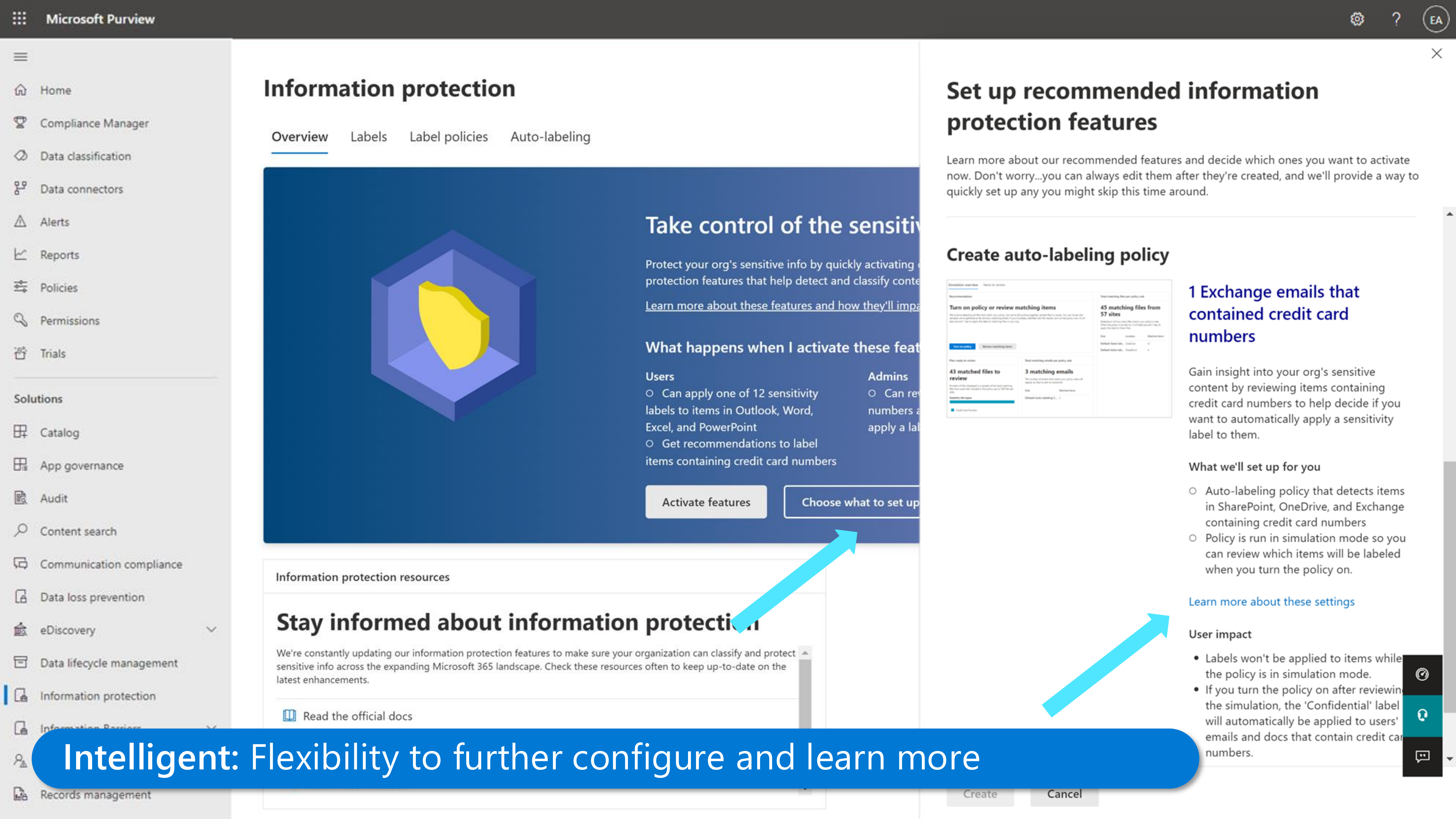
Sharepoint and OneDrive files
50

Information protection resources

Stay informed about information protection

We're constantly updating our information protection features to make sure your organization can classify and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

Intelligent: Default labels & policies with simple one-click turn on



Information protection

Take control of the sensitiv

Protect your org's sensitive info by quickly activating
protection features that help detect and classify conte

Learn more about these features and how they'll impa

What happens when I activate these feat

Users

- ○ Can apply one of 12 sensitivity labels to items in Outlook, Word, Excel, and PowerPoint
- ○ Get recommendations to label items containing credit card numbers

Admins

- ○ Can re
numbers a
apply a lab

Information protection resources

Stay informed about information protecti

We're constantly updating our information protection features to make sure your organization can classify and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

Set up recommended information protection features

Learn more about our recommended features and decide which ones you want to activate now. Don't worry...you can always edit them after they're created, and we'll provide a way to quickly set up any you might skip this time around.

Create auto-labeling policy

1 Exchange emails that contained credit card numbers

Gain insight into your org's sensitive content by reviewing items containing credit card numbers to help decide if you want to automatically apply a sensitivity label to them.

What we'll set up for you

- ○ Auto-labeling policy that detects items in SharePoint, OneDrive, and Exchange containing credit card numbers
- ○ Policy is run in simulation mode so you can review which items will be labeled when you turn the policy on.

Learn more about these settings

User impact

- Labels won't be applied to items while the policy is in simulation mode.
- If you turn the policy on after reviewin the simulation, the 'Confidential' label will automatically be applied to users' emails and docs that contain credit ca numbers.

Intelligent: Flexibility to further configure and learn more

Metro Systems Corporation Public Company Limited
400 Chalermprakiat Rama IX Road, Nong Bon, Prawet, Bangkok 10250 Tel: +662 089 – 4000

Thank You