DynaTech | Systems

Accelerate Business

What Sets Us Apart

DynaTech's Competitive Advantage

Backed by years of expertise and a team of skilled professionals, DynaTech Systems stands at the forefront of the IT services industry. Our extensive portfolio includes cutting-edge solutions in cloud, ERP and CRM implementation, data analytics, artificial intelligence, and more.

We prioritize long-term partnerships built on collaboration and trust, delivering innovative, scalable, and secure solutions to keep our clients ahead in a rapidly evolving landscape.

AICPA Service Organization Control Reports AICPA SOC 2 Formerly SAS 70 Reports

Microsoft Solutions Partner

Great Place To Work® Certified FEB 2025-FEB 2026 INDIA

DUN & BRADSTREET D-U-N-S® REGISTERED™

ISO 9001:2015

CMMI level 3

150+

Global Projects

100+

Happy Clients

420+

Expert Minds

DynaTech | Systems

DynaTech

AI - Led Microsoft Cloud Capabilities

Microsoft Cloud & Low Code

- Azure Infra
- Azure Services
- Logic Apps
- Service Bus
- Event Grid
- API Management
- Synapse Analytics
- Load Testing
- Functions
- Data Factory
- Power Pages
- Power Automate
- Power Apps
- AI Builder
- Azure FHIR

Agentic AI Business Applications

- Sales
- Finance
- SCM
- Project Operations
- Customer Service
- Field Service
- Customer Insights & Marketing
- Human Resources
- Commerce

Data & AI

- Fabric
- Copilot
- Power BI
- Data Warehouse
- OneLake
- Data Lake
- Data Factory
- Data Science
- Lakehouse
- Real-Time Intelligence
- Data Engineering
- Dataverse
- Microsoft Purview
- Databases
- Azure AI Foundry
- Copilot Studio

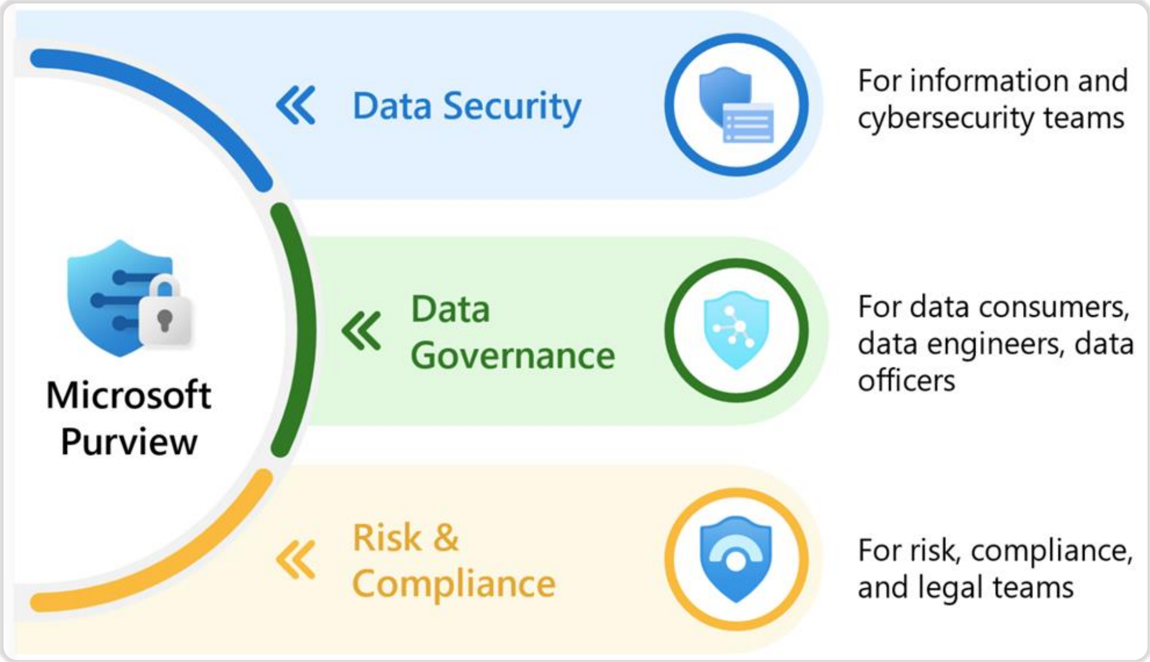
DynaTech | Systems

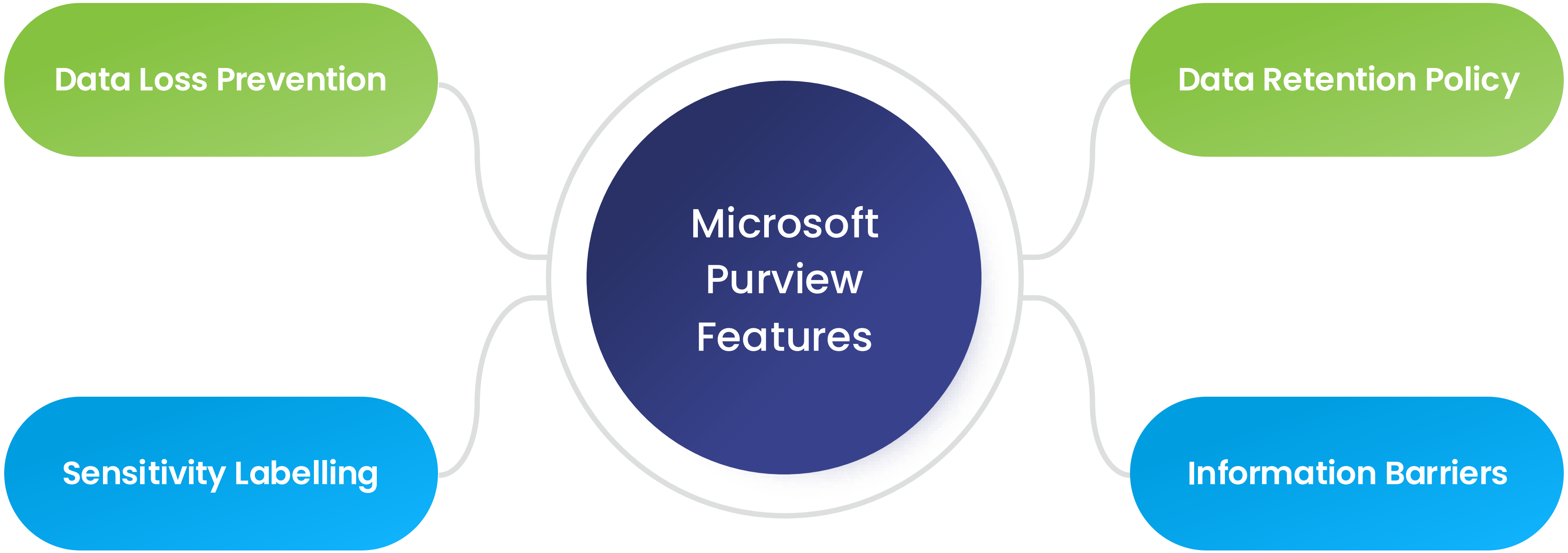
Microsoft Purview

Features

Microsoft Purview is a comprehensive set of solutions that can help your organization govern, protect, and manage data, wherever it lives. Microsoft Purview solutions provide integrated coverage and help address the fragmentation of data across organizations, the lack of visibility that hampers data protection and governance, and the blurring of traditional IT management roles.

- Gain visibility into data across your organization
- Safeguard and manage sensitive data across its lifecycle, wherever it lives
- Govern data seamlessly in new, comprehensive ways
- Manage critical data risks and regulatory requirements


Microsoft Purview
Data Security
For information and cybersecurity teams
Data Governance
For data consumers, data engineers, data officers
Risk & Compliance
For risk, compliance, and legal teams



Microsoft Purview Features

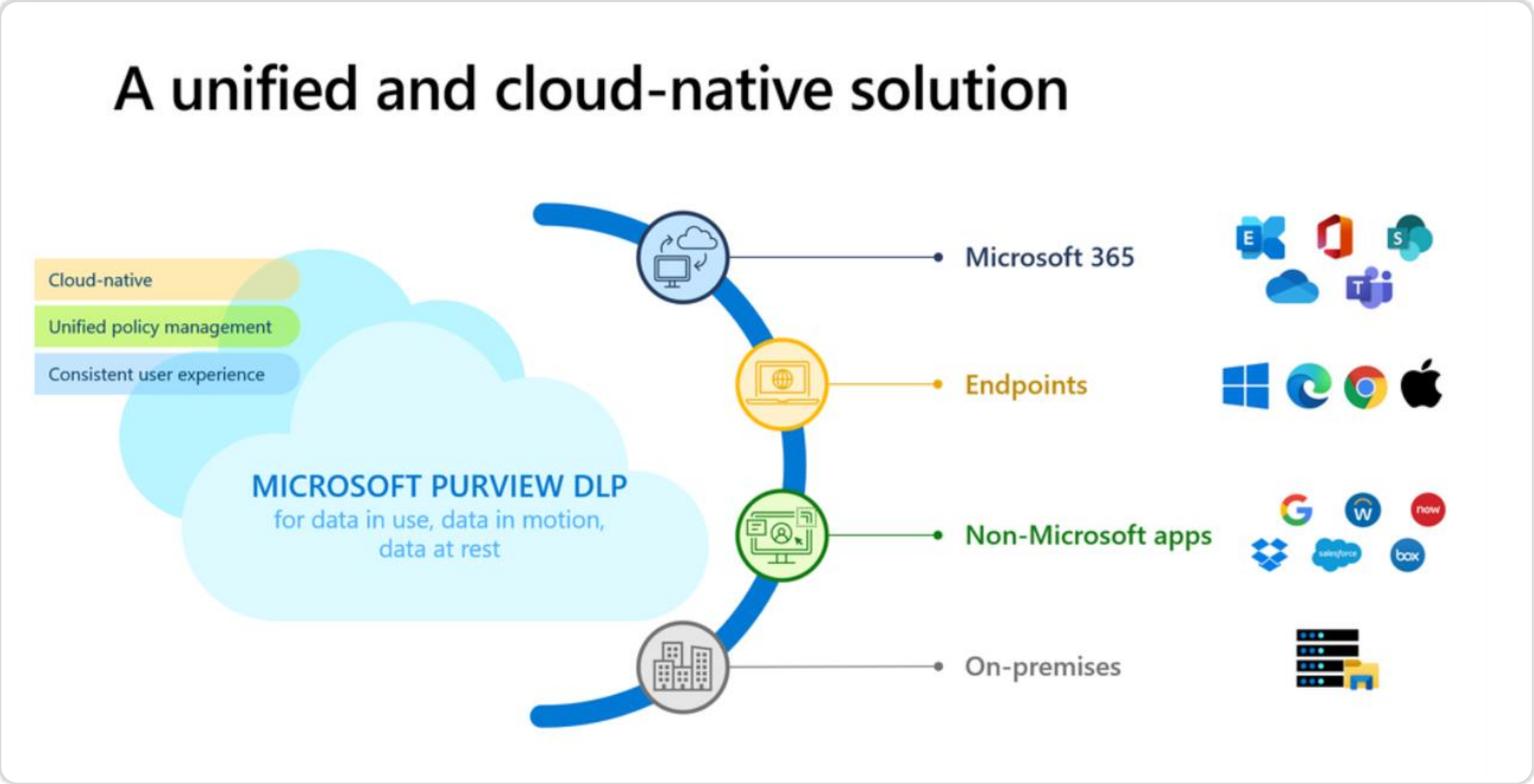
Data Loss Prevention

Data Retention Policy

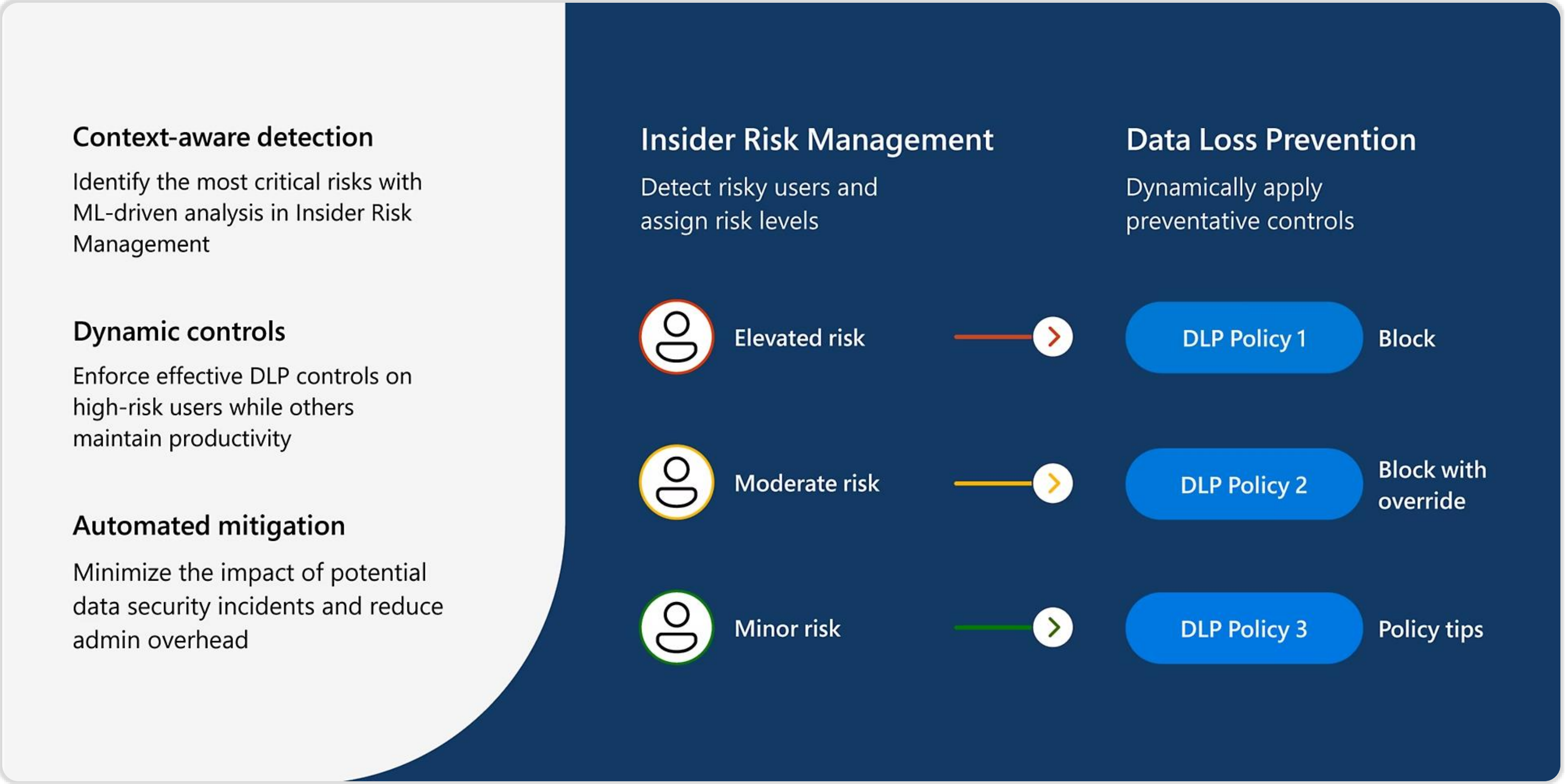
Sensitivity Labelling

Information Barriers

Microsoft Purview DLP is a unified, cloud-native solution for safeguarding data across Microsoft 365 endpoints, non-Microsoft apps, and on-premises environments. It offers unified policy management and a consistent user experience. protecting data in use, motion, and at rest. The solution covers popular platforms like Windows, macOS, Google Workspace, and Salesforce, ensuring comprehensive data protection across different environments.


A unified and cloud-native solution
Cloud-native
Unified policy management
Consistent user experience
MICROSOFT PURVIEW DLP
for data in use, data in motion, data at rest
Microsoft 365
Endpoints
Non-Microsoft apps
On-premises

Microsoft Purview DLP uses Insider Risk Management to detect and assign risk levels (elevated, moderate, and minor) to users based on behavior. It features context-aware detection with machine learning, dynamic controls that enforce tailored DLP policies depending on user risk level, and automated mitigation to reduce admin overhead while maintaining productivity. Policies dynamically apply preventative controls, such as blocking actions or offering policy tips based on the user's risk profile.



Context-aware detection

Identify the most critical risks with ML-driven analysis in Insider Risk Management

Dynamic controls

Enforce effective DLP controls on high-risk users while others maintain productivity

Automated mitigation

Minimize the impact of potential data security incidents and reduce admin overhead

Insider Risk Management

Detect risky users and assign risk levels

Data Loss Prevention

Dynamically apply preventative controls

Insider Risk Management	Data Loss Prevention	
Elevated risk	DLP Policy 1	Block
Moderate risk	DLP Policy 2	Block with override
Minor risk	DLP Policy 3	Policy tips

Sensitive Information Identification

- Detect and classify sensitive data (e.g., credit card numbers, SSNs, health records).
- Create and use custom sensitive information types specific to your organization.

Policy Enforcement

- Block, restrict, or monitor data sharing based on DLP policies.
- Provide users with policy tips and notifications for education and awareness.
- Enable users to override policies with justification if allowed.

Data Protection Across Environments

- Apply DLP policies to protect data in Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Fabric and Microsoft Teams.
- Prevent and notify unauthorized sharing or transmission of sensitive data.

Automatic Remediation Actions

- Automatically block or encrypt sensitive information.
- Notify administrators and users of policy violations.
- Trigger alerts for suspicious activities.

Compliance and Regulatory Adherence

- Ensure compliance with regulations like GDPR, HIPAA, etc.
- Use pre-configured templates for industry-specific compliance requirements.

Monitoring and Reporting

- Track and monitor data usage and policy violations.
- Generate detailed audit logs and compliance reports.
- Use dashboards for a quick overview of policy effectiveness and incidents.

Integration with Other Microsoft Solutions

- Leverage Microsoft Information Protection (MIP) for labelling and encryption.
- Extend DLP capabilities to third-party cloud apps via Microsoft Cloud App Security (MCAS).

Collaboration Control

- Manage and protect sensitive data shared via Microsoft Teams and SharePoint.
- Apply DLP policies to collaboration activities, such as file sharing and messaging.

Adaptive DLP Policies

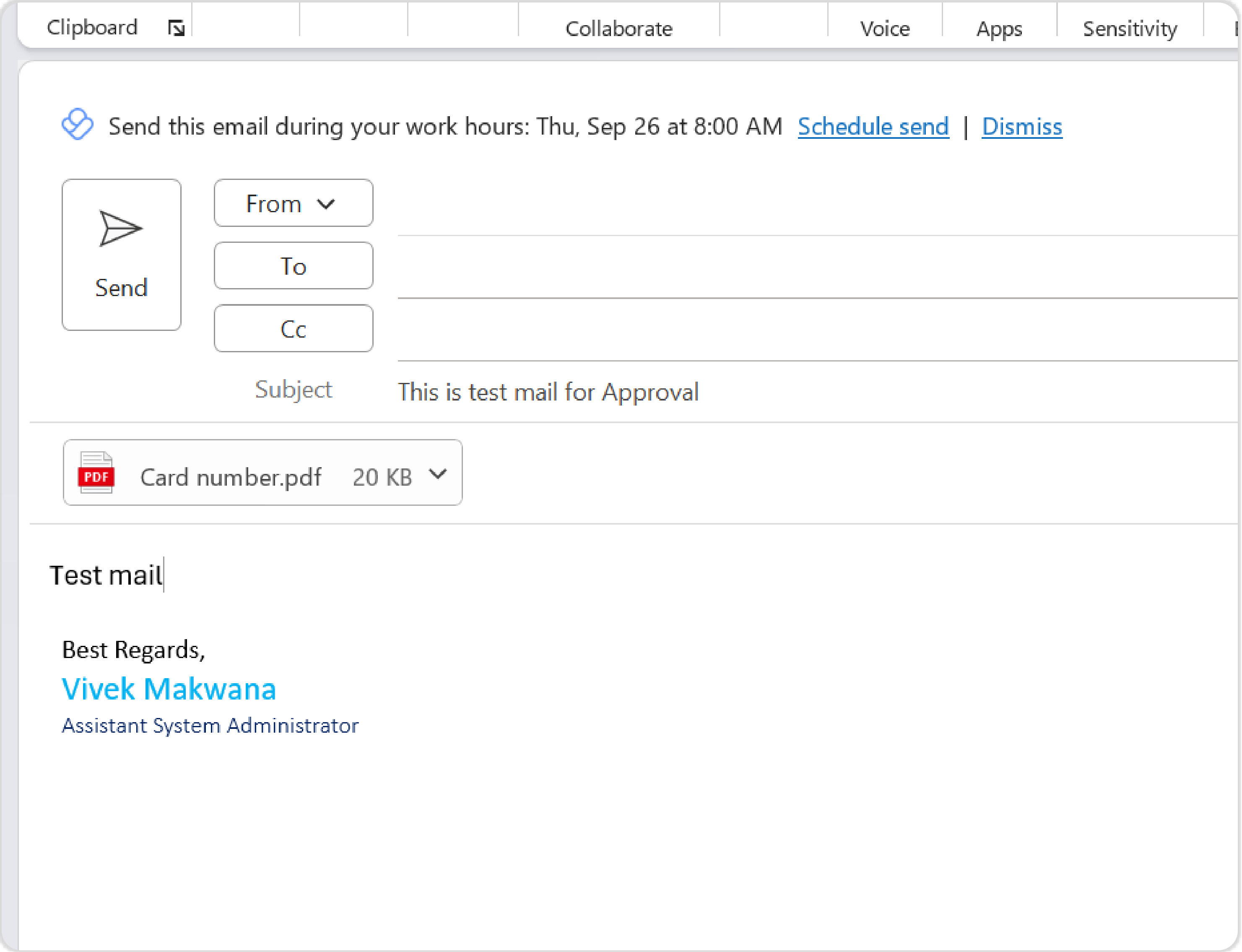
- Apply DLP policies dynamically based on user, location, device, and other attributes.
- Customize policies for specific user groups, data locations, and scenarios.

Governance and Lifecycle Management

- Integrate DLP with data governance for secure data handling throughout its lifecycle.
- Manage data retention and deletion based on compliance policies.

We have configured the policy as below:

- We have mentioned the File extension
- If any file is sent outside the organization via email, a notification will be sent to the approval authority for review and approval.
- Once approved then mail has been sent



Send this email during your work hours: Thu, Sep 26 at 8:00 AM Schedule send | Dismiss

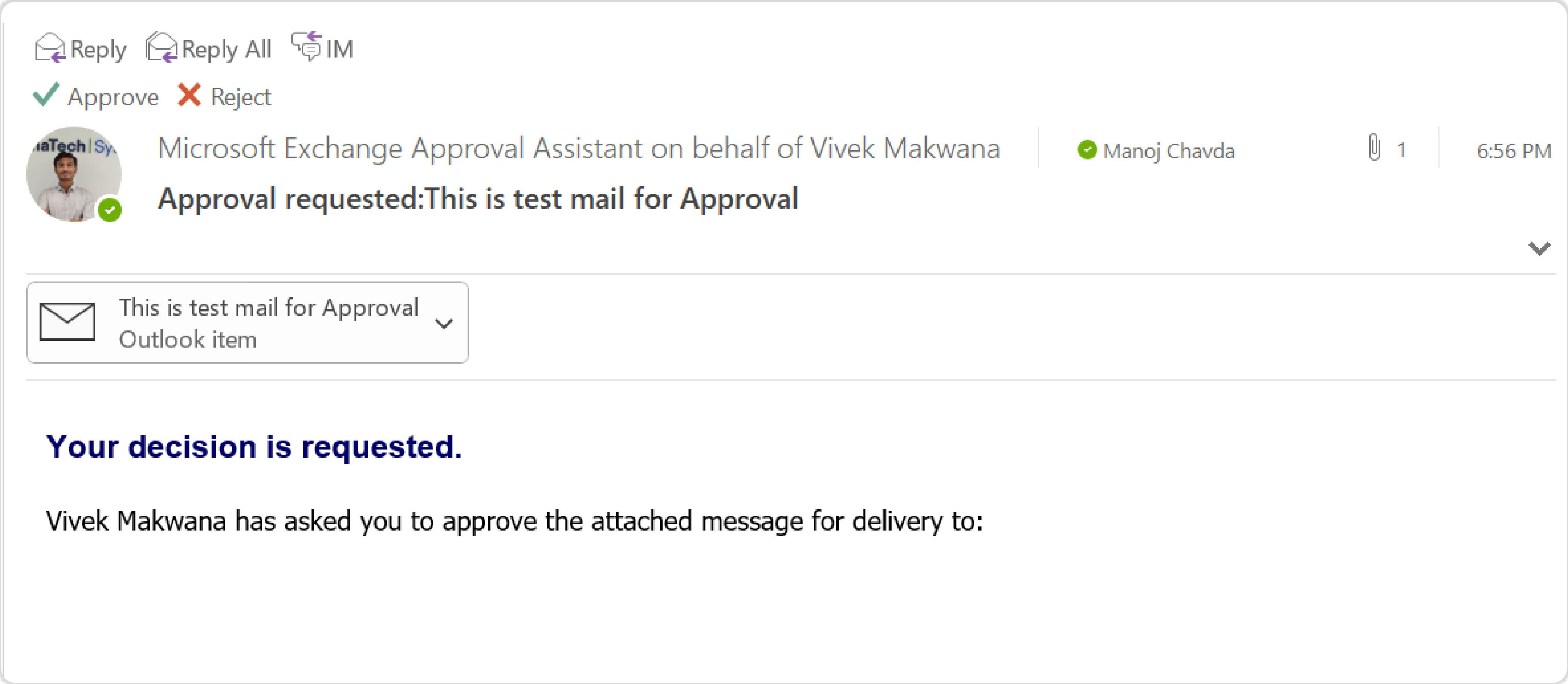
Subject This is test mail for Approval

Card number.pdf 20 KB

Test mail

Best Regards,
Vivek Makwana
Assistant System Administrator

Approval mail has been delivered to approval authority.



Microsoft Exchange Approval Assistant on behalf of Vivek Makwana

Manoj Chavda

1

6:56 PM

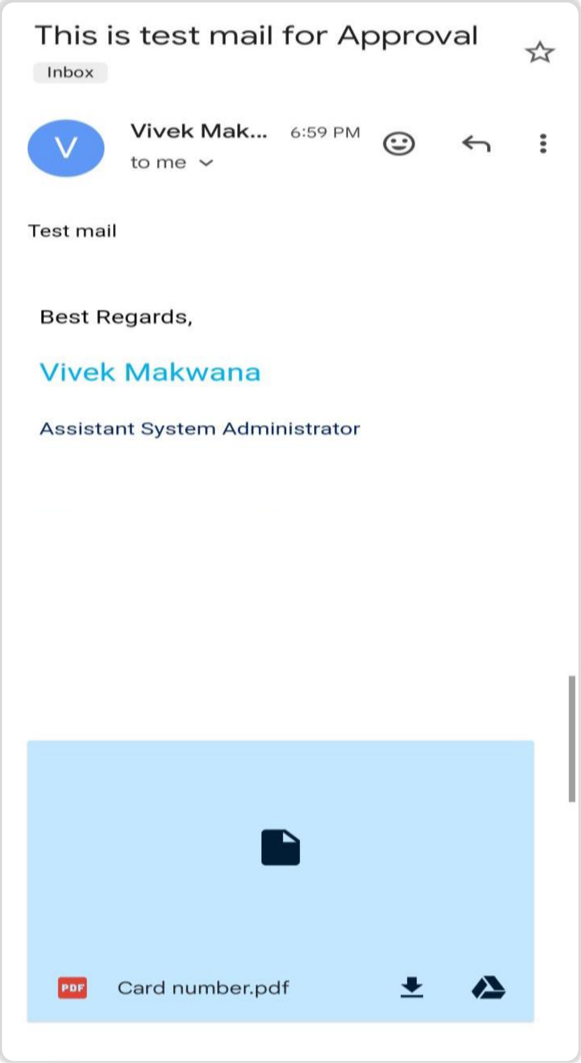
Approval requested:This is test mail for Approval

This is test mail for Approval
Outlook item

Your decision is requested.

Vivek Makwana has asked you to approve the attached message for delivery to:

After Approval mail has been sent to specified recipient.



This is test mail for Approval

Vivek Mak... 6:59 PM

to me

Test mail

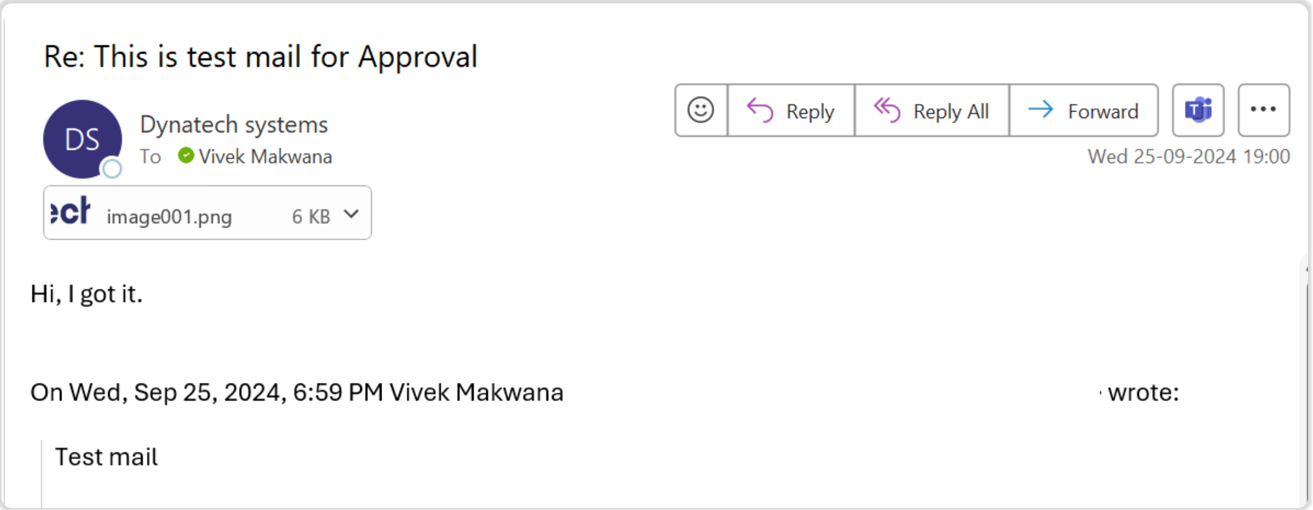
Best Regards,

Vivek Makwana

Assistant System Administrator

Card number.pdf

Also, sender getting the response after approval.



Re: This is test mail for Approval

Dynatech systems

To Vivek Makwana

Wed 25-09-2024 19:00

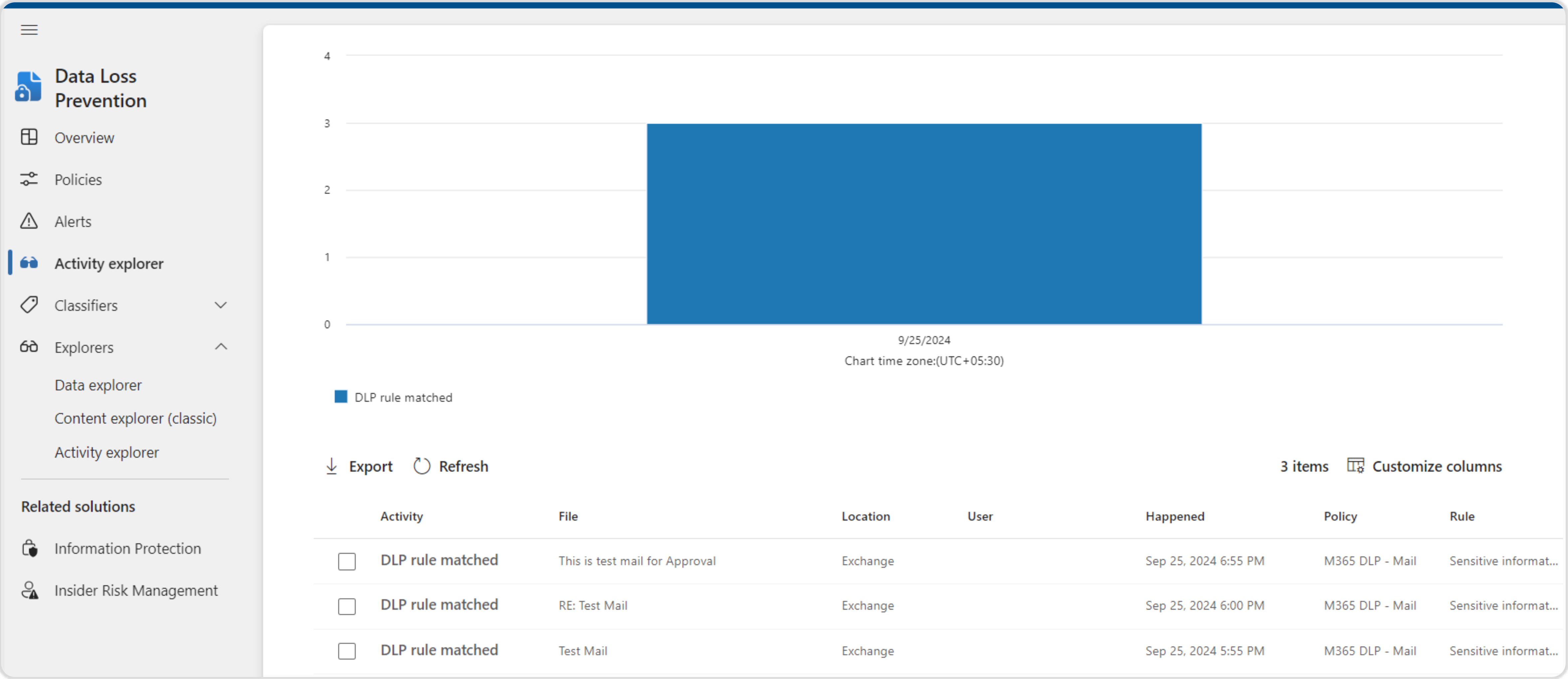
image001.png 6 KB

Hi, I got it.

On Wed, Sep 25, 2024, 6:59 PM Vivek Makwana · wrote:

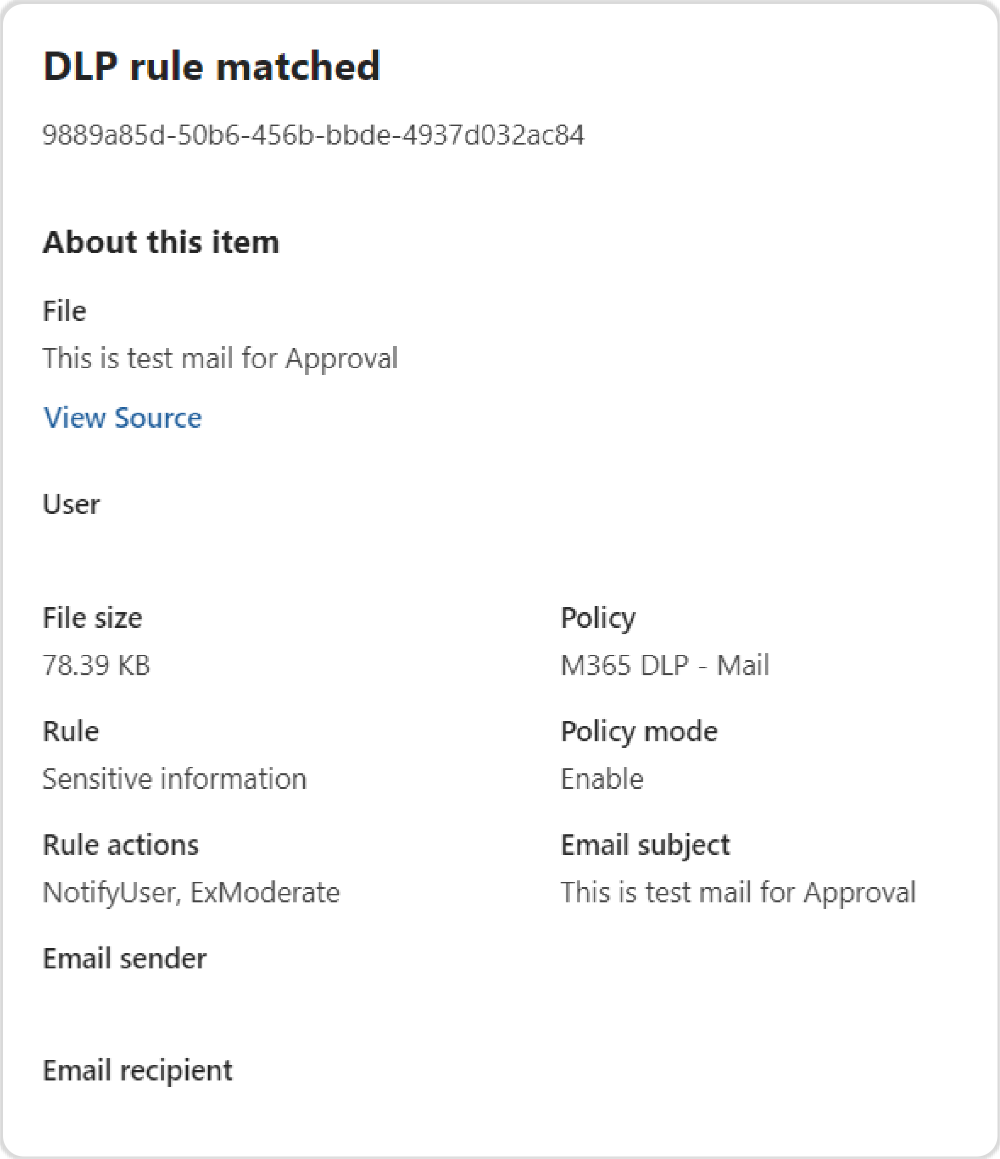
Test mail

Alert Logs.



	Activity	File	Location	User	Happened	Policy	Rule
☐	DLP rule matched	This is test mail for Approval	Exchange		Sep 25, 2024 6:55 PM	M365 DLP - Mail	Sensitive informat...
☐	DLP rule matched	RE: Test Mail	Exchange		Sep 25, 2024 6:00 PM	M365 DLP - Mail	Sensitive informat...
☐	DLP rule matched	Test Mail	Exchange		Sep 25, 2024 5:55 PM	M365 DLP - Mail	Sensitive informat...

Alert Logs.



DLP rule matched

9889a85d-50b6-456b-bbde-4937d032ac84

About this item

File
This is test mail for Approval

View Source

User

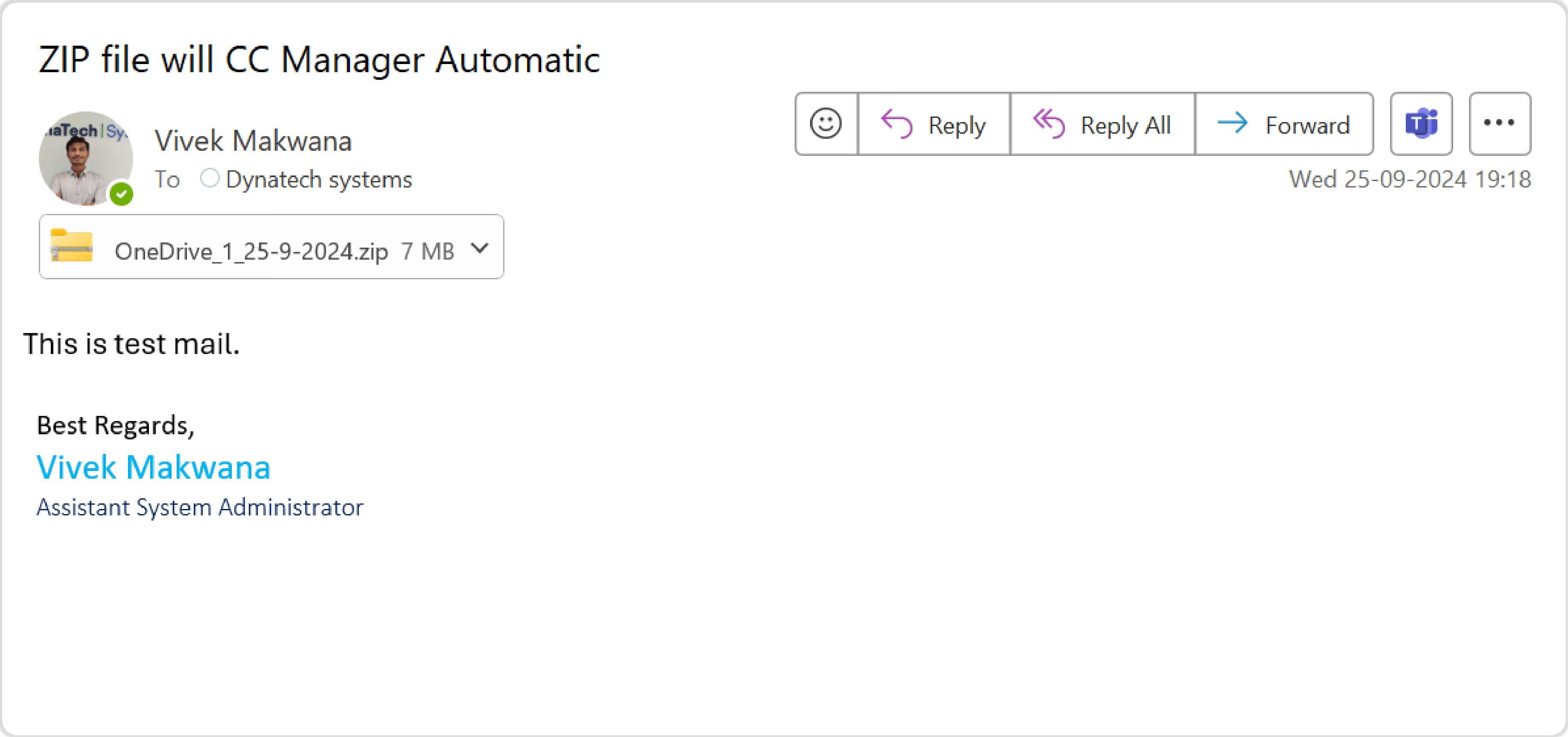
File size 78.39 KB	Policy M365 DLP - Mail
Rule Sensitive information	Policy mode Enable
Rule actions NotifyUser, ExModerate	Email subject This is test mail for Approval
Email sender	

Email recipient

In this policy we have mention below criteria:

- File extension is .Zip
- If a user sends an email outside the organization with the specified file extension, the conditions will be met, and their manager will be automatically added to the CC.

Sender



ZIP file will CC Manager Automatic

Vivek Makwana

To ○ Dynatech systems

Wed 25-09-2024 19:18

OneDrive_1_25-9-2024.zip 7 MB

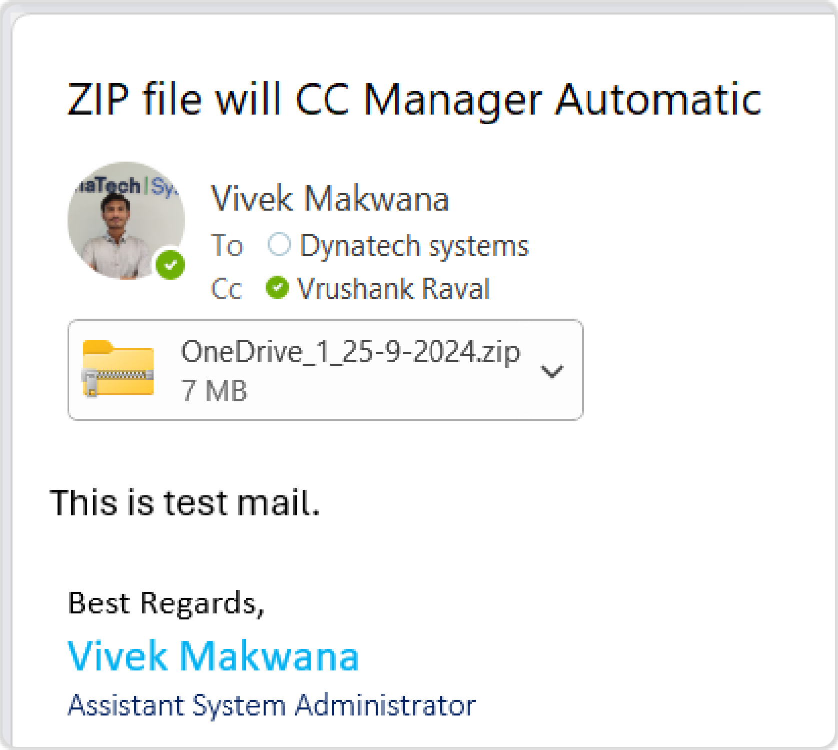
This is test mail.

Best Regards,

Vivek Makwana

Assistant System Administrator

Manager will receive the mail automatically.



ZIP file will CC Manager Automatic

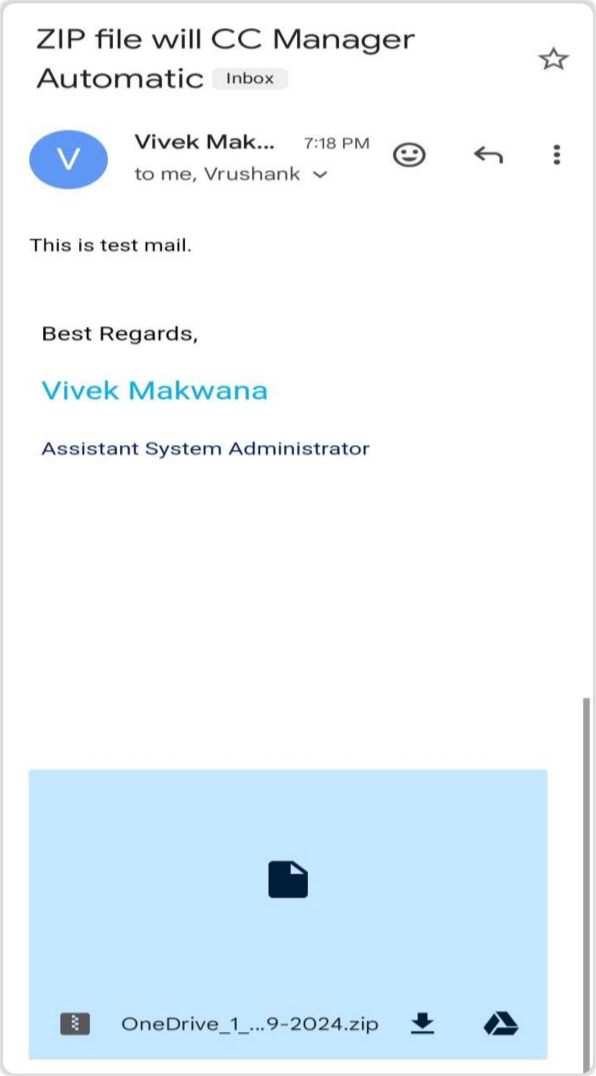
Vivek Makwana
To ○ Dynatech systems
Cc ✓ Vrushank Raval

OneDrive_1_25-9-2024.zip
7 MB

This is test mail.

Best Regards,
Vivek Makwana
Assistant System Administrator

Recipient Mail



ZIP file will CC Manager Automatic Inbox

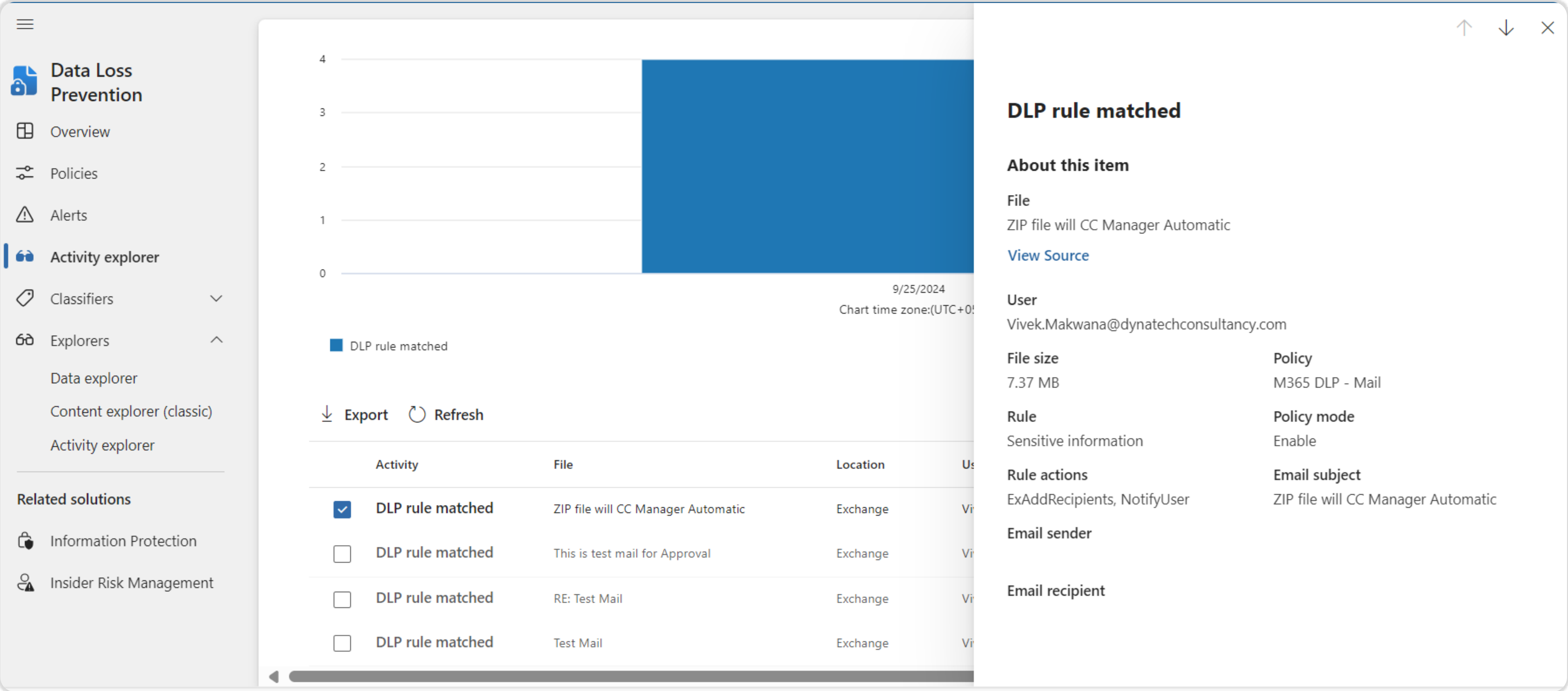
Vivek Mak... 7:18 PM
to me, Vrushank

This is test mail.

Best Regards,
Vivek Makwana
Assistant System Administrator

OneDrive_1_...9-2024.zip

Alert and Log.



	Activity	File	Location	Us
☑	DLP rule matched	ZIP file will CC Manager Automatic	Exchange	Vi
□	DLP rule matched	This is test mail for Approval	Exchange	Vi
□	DLP rule matched	RE: Test Mail	Exchange	Vi
□	DLP rule matched	Test Mail	Exchange	Vi

DLP rule matched

About this item

File
ZIP file will CC Manager Automatic
View Source

User
Vivek.Makwana@dynatechconsultancy.com

File size
7.37 MB

Policy
M365 DLP - Mail

Rule
Sensitive information

Policy mode
Enable

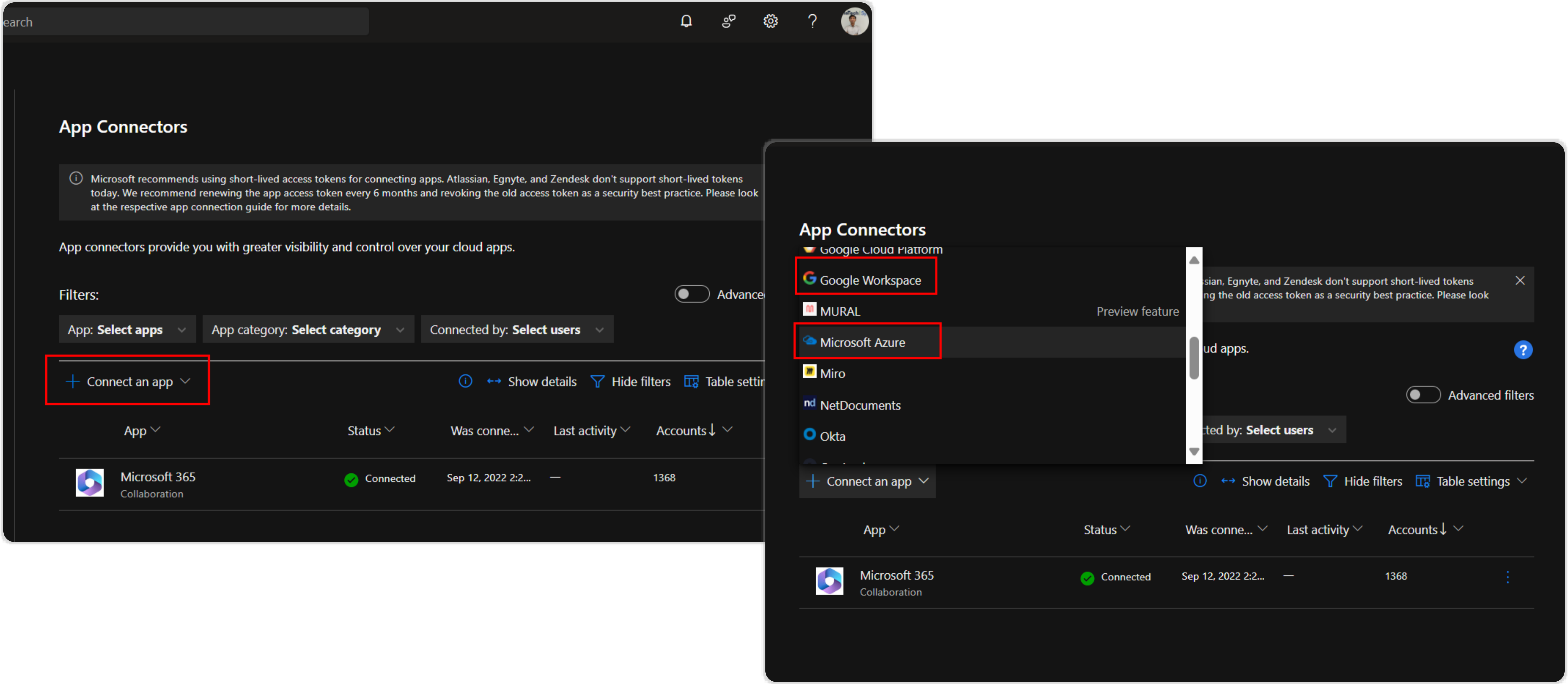
Rule actions
ExAddRecipients, NotifyUser

Email subject
ZIP file will CC Manager Automatic

Email sender

Email recipient

For third party platform integration the app must be connected to Microsoft Defender for Cloud Apps.



App Connectors

Microsoft recommends using short-lived access tokens for connecting apps. Atlassian, Egnyte, and Zendesk don't support short-lived tokens today. We recommend renewing the app access token every 6 months and revoking the old access token as a security best practice. Please look at the respective app connection guide for more details.

App connectors provide you with greater visibility and control over your cloud apps.

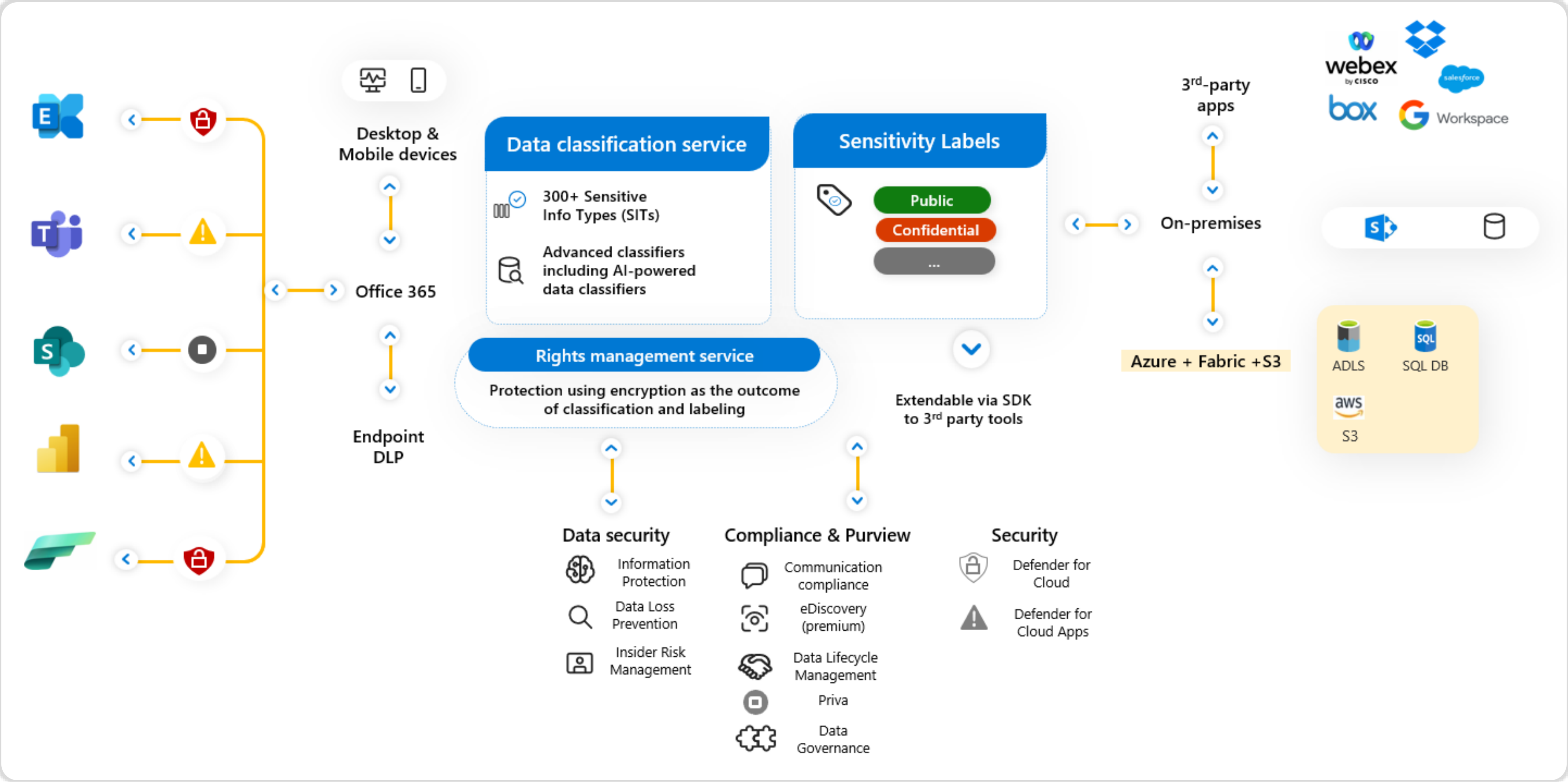
Filters: App: Select apps | App category: Select category | Connected by: Select users | Advanced filters

+ Connect an app

App	Status	Was conne...	Last activity	Accounts
Microsoft 365 Collaboration	Connected	Sep 12, 2022 2:2...	—	1368

What is Sensitivity Labelling?

Sensitivity Labeling in Microsoft Purview is a critical feature that allows organizations to classify and protect sensitive information across their Microsoft 365 environment. Sensitivity labels help identify, categorize, and protect data based on its level of sensitivity, and apply policies to safeguard it accordingly.



Data Classification and Sensitivity Labelling

- Classify and tag data based on sensitivity levels (e.g., Public, Confidential, Highly Confidential).
- Apply sensitivity labels manually or automatically to documents, emails, and other content.
- Create and use custom labels tailored to organizational needs.
- Automatically apply labels based on content, such as keywords or sensitive information types.

Policy Enforcement and Compliance

- Enforce data handling policies based on labels (e.g., block sharing, require encryption).
- Support compliance with regulations like GDPR, HIPAA, and others through proper data labelling.
- Generate audit logs and compliance reports to monitor label application and data handling.

Data Protection and Encryption

- Encrypt labelled documents and emails to secure them from unauthorized access.
- Apply rights management controls, such as restricting who can view, edit, or share labelled content.
- Add visual markings like watermarks, headers, and footers to indicate sensitivity levels.

Integration with Other Microsoft Solutions

- Use sensitivity labels across Microsoft 365 apps (Word, Excel, Outlook, PowerPoint).
- Integrate with Data Loss Prevention (DLP) and Azure Information Protection (AIP) for enhanced data protection.
- Extend labelling to third-party environments via connectors and integrations.

User Awareness and Education

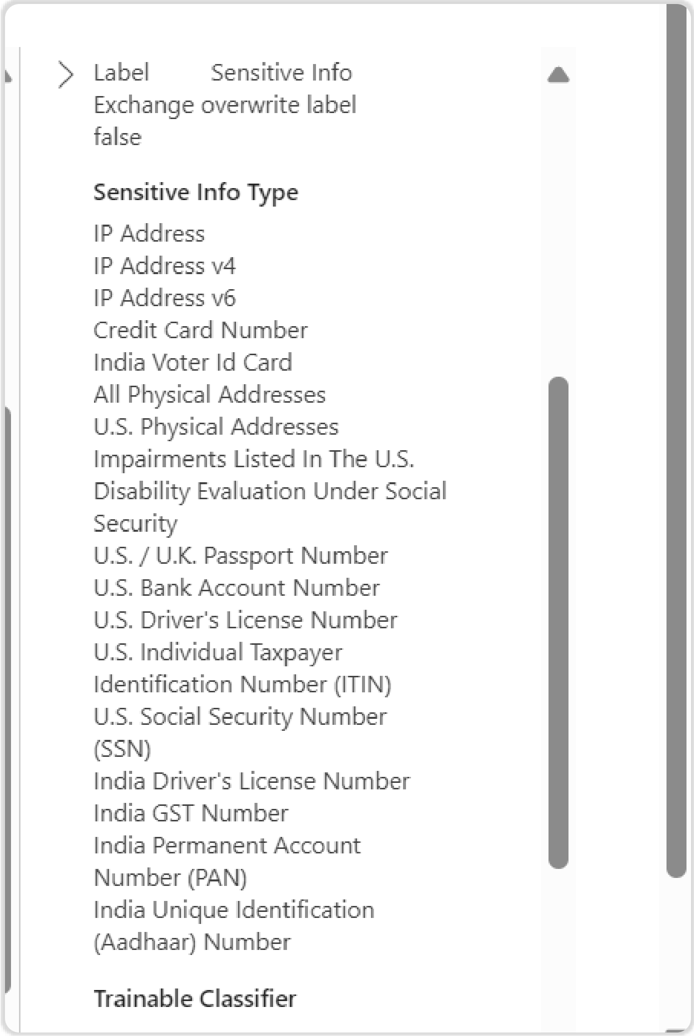
- Provide label recommendations based on content analysis.
- Display tooltips and descriptions to educate users on label usage and impact.
- Enable users to manually label content when needed.

Microsoft Purview Feature

Sensitivity Labelling – Test Case

DynaTech | Systems

We have created the Policy as an Auto labelling and Sensitive information type is as below:



Label Sensitive Info

Exchange overwrite label

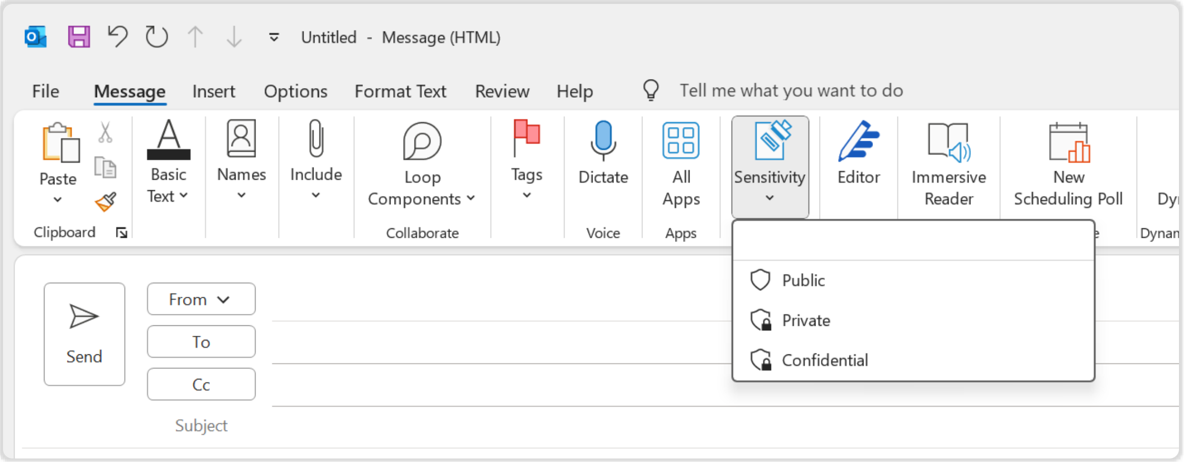
false

Sensitive Info Type

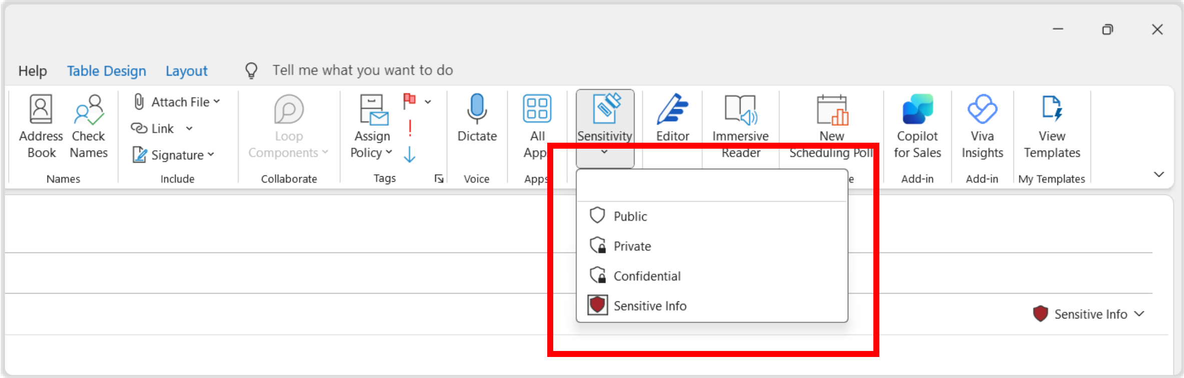
IP Address
IP Address v4
IP Address v6
Credit Card Number
India Voter Id Card
All Physical Addresses
U.S. Physical Addresses
Impairments Listed In The U.S. Disability Evaluation Under Social Security
U.S. / U.K. Passport Number
U.S. Bank Account Number
U.S. Driver's License Number
U.S. Individual Taxpayer Identification Number (ITIN)
U.S. Social Security Number (SSN)
India Driver's License Number
India GST Number
India Permanent Account Number (PAN)
India Unique Identification (Aadhaar) Number

Trainable Classifier

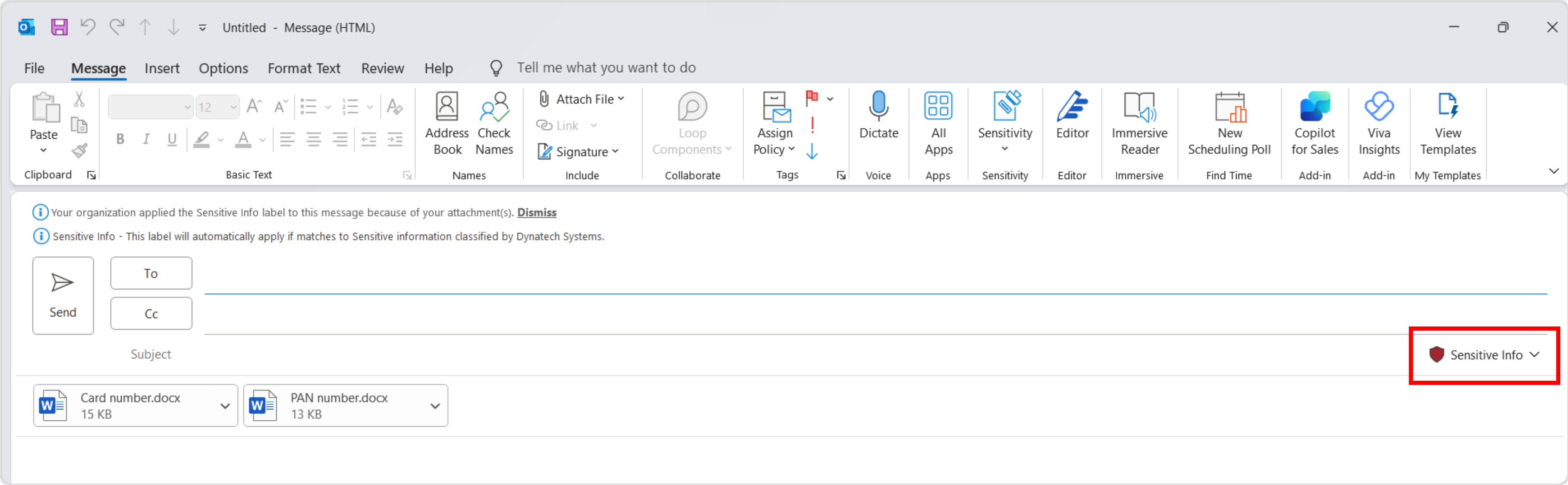
Before Auto labelling policy turn on the labels are as below mentioned screen shot:



After the reflecting the policy the new label which is Sensitive Info are added in the label list.



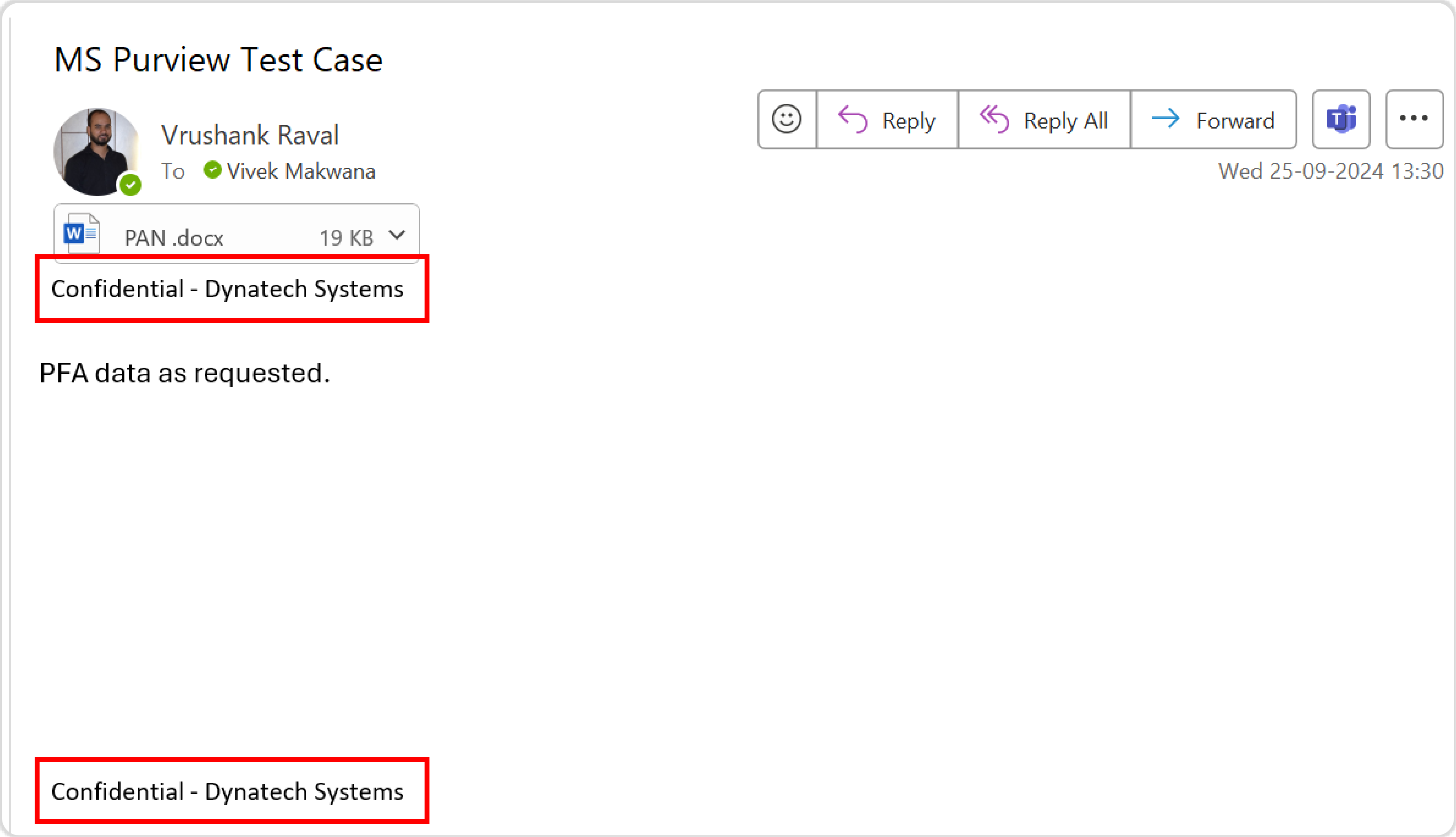
When the content of the files is matched the sensitivity information type then label is automatically taken.



Your organization applied the Sensitive Info label to this message because of your attachment(s). Dismiss

Sensitive Info - This label will automatically apply if matches to Sensitive information classified by Dynatech Systems.

Receiver side the recipient is getting mail with labelling.



MS Purview Test Case

Vrushank Raval

To Vivek Makwana

Wed 25-09-2024 13:30

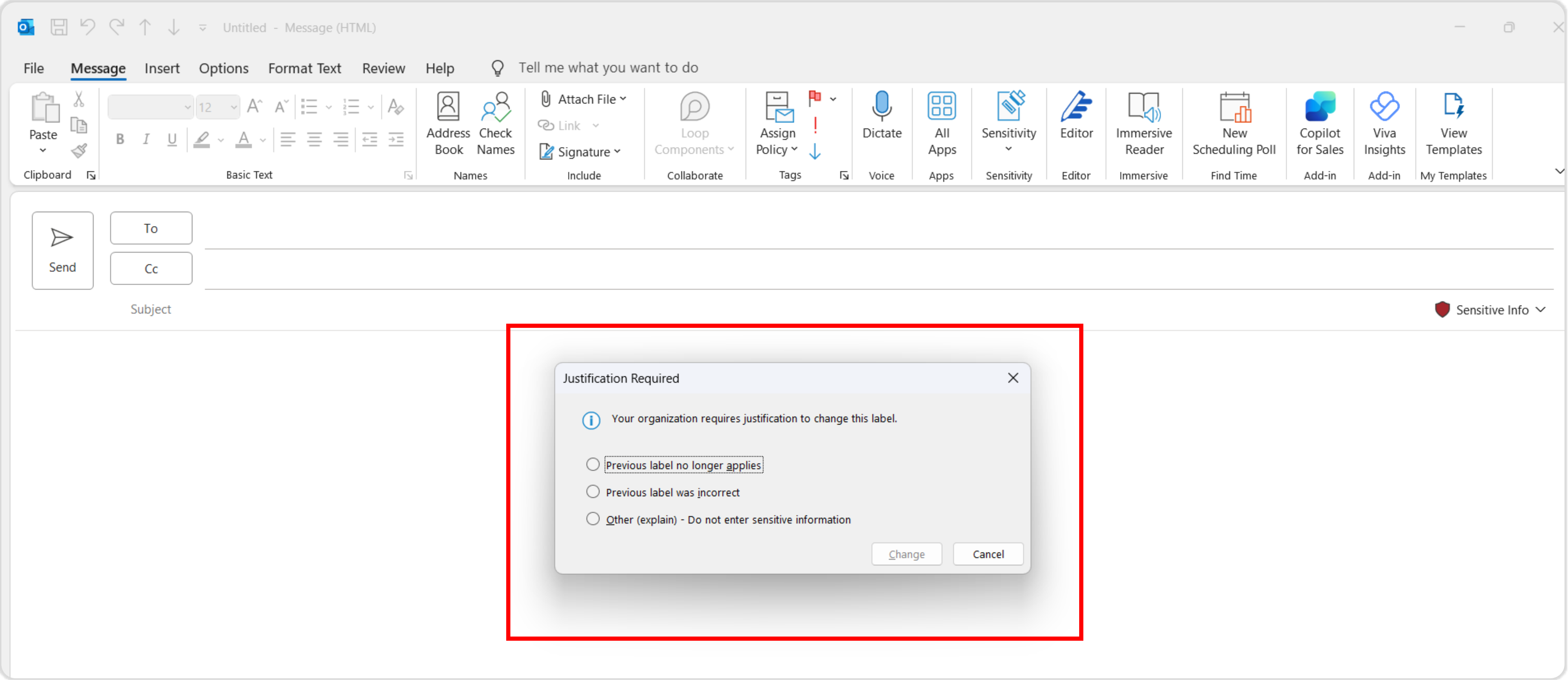
PAN .docx 19 KB

Confidential - Dynatech Systems

PFA data as requested.

Confidential - Dynatech Systems

If end user is trying to remove the label, then needs to provide the justification, Based on the label you can control the access as well.



Justification Required

Your organization requires justification to change this label.

○ Previous label no longer applies

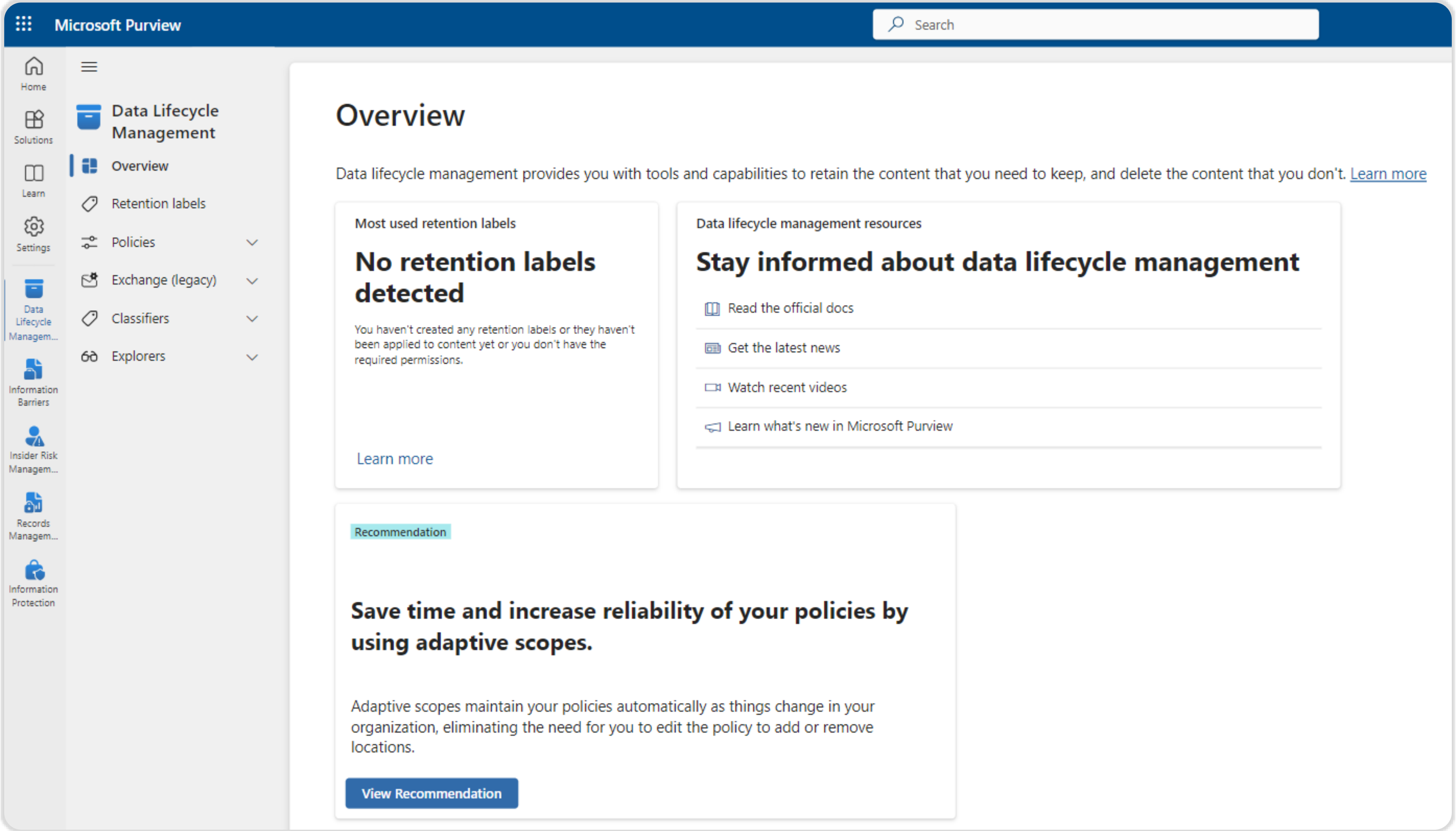
○ Previous label was incorrect

○ Other (explain) - Do not enter sensitive information

Change | Cancel

What is the Retention Policy?

A retention policy in Microsoft Purview helps manage the lifecycle of your data by specifying whether to retain content, delete content, or retain and then delete content after a certain period.



Overview

Data lifecycle management provides you with tools and capabilities to retain the content that you need to keep, and delete the content that you don't. Learn more

Most used retention labels

No retention labels detected

You haven't created any retention labels or they haven't been applied to content yet or you don't have the required permissions.

Learn more

Data lifecycle management resources

Stay informed about data lifecycle management

- Read the official docs
- Get the latest news
- Watch recent videos
- Learn what's new in Microsoft Purview

Recommendation

Save time and increase reliability of your policies by using adaptive scopes.

Adaptive scopes maintain your policies automatically as things change in your organization, eliminating the need for you to edit the policy to add or remove locations.

View Recommendation

Data Retention and Deletion

- Automatically retain data for a specified period, ensuring it is preserved for legal, regulatory, or business requirements.
- Automatically delete data after a specified period to reduce storage costs and minimize risk exposure.
- Apply "retain and delete" actions, keeping data for a specific duration and then deleting it after.

Centralized Management

- Manage retention policies for various content types (emails, documents, chats, etc.) across Microsoft 365 from a central location.
- Apply policies to different locations such as Exchange Online mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams.

Compliance and Regulatory Adherence

- Ensure compliance with regulations and organizational policies that mandate data retention (e.g., GDPR, HIPAA, financial regulations).
- Meet legal hold requirements by preserving data indefinitely until the hold is removed.
- Simplify regulatory audits and eDiscovery processes with consistent data retention and deletion practices.

Granular Policy Control

- Apply retention policies based on different criteria, such as specific keywords, content types, labels, or user groups.
- Create custom retention labels for specific business requirements and apply them to content manually or automatically.
- Exclude specific content or locations from retention policies as needed.

Retention Across Multiple Environments

- Apply retention policies across cloud and on-premises environments using Microsoft 365 compliance features.
- Ensure consistent data retention and deletion policies across various data sources, including SharePoint, OneDrive, and Teams.

Data Lifecycle Management

- Automate data lifecycle management by transitioning content based on its age, location, or other attributes.
- Retain important content for organizational knowledge management while ensuring outdated information is deleted.
- Support defensible deletion practices, reducing the risk of keeping unnecessary data.

Minimizing Risk and Reducing Storage Costs

- Reduce the risk of keeping data longer than necessary by enforcing automatic deletion of outdated information.
- Save on storage costs by systematically deleting data that is no longer needed.

Preservation of Business Records

- Preserve business-critical records and documents for specified durations, ensuring their availability for audits and compliance checks.
- Prevent unauthorized edits or deletions of important records during their retention period.

Integration with eDiscovery and Litigation Hold

- Integrate with eDiscovery to facilitate data searches and exports for legal and compliance investigations.
- Apply legal holds to content, preventing deletion during legal proceedings or investigations, overriding standard retention settings.

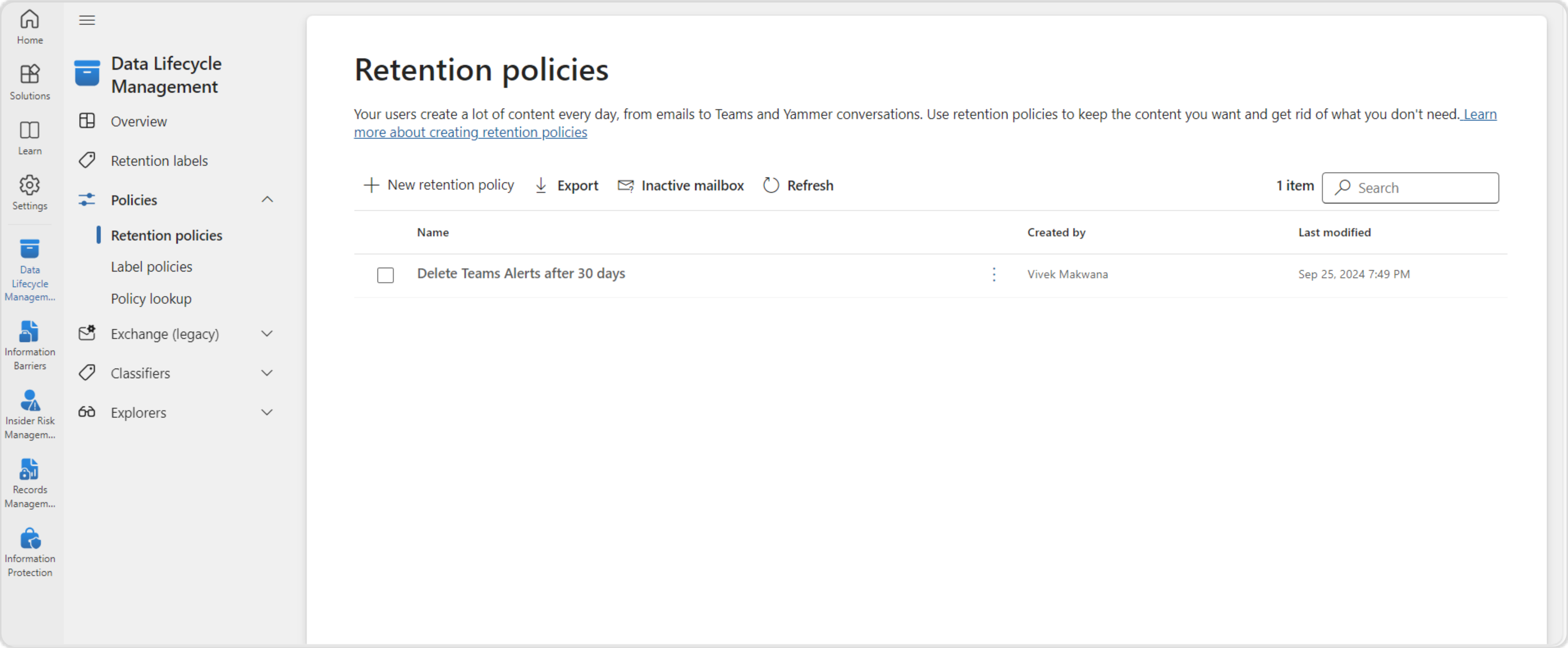
Data Retention Policy Configuration Steps

Step 1: Access the Microsoft Purview Compliance Portal

1. Log in to Microsoft 365 with admin credentials.
2. From the admin center, open the Microsoft Purview Compliance portal.

Step 2: Navigate to Data Lifecycle management

1. Select Retention Policy.



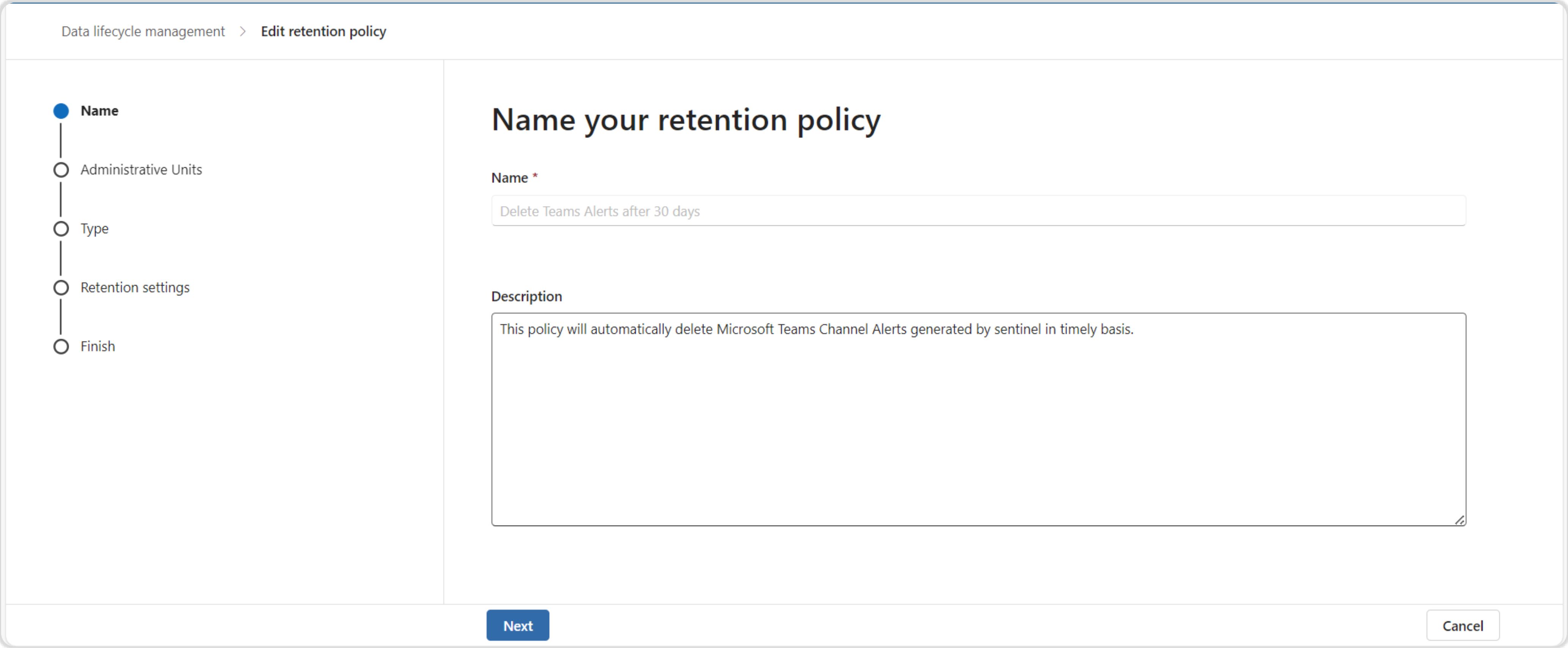
Retention policies

Your users create a lot of content every day, from emails to Teams and Yammer conversations. Use retention policies to keep the content you want and get rid of what you don't need. Learn more about creating retention policies

	Name	Created by	Last modified
□	Delete Teams Alerts after 30 days	Vivek Makwana	Sep 25, 2024 7:49 PM

Step 3: Create a New Retention Policy

1. Select + New retention policy to create a new policy.
2. Name your policy, e.g., "Teams Channel Deletion After 30 Days.“
3. Add an optional description for clarity.



Name your retention policy

Name *

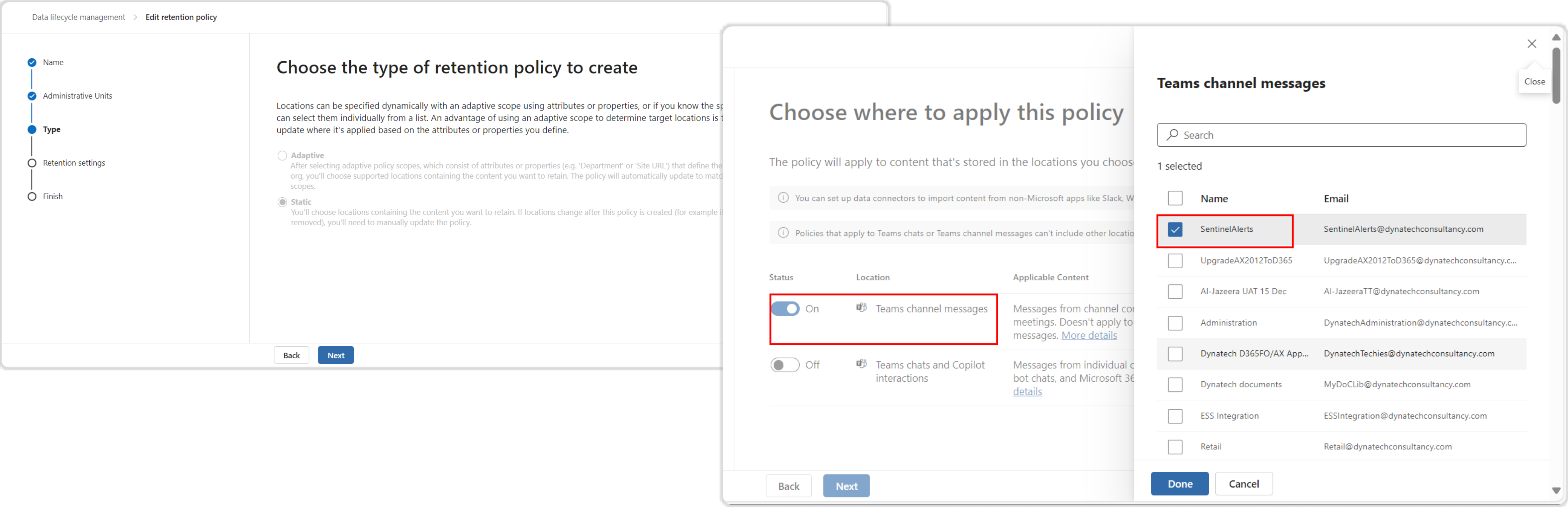
Delete Teams Alerts after 30 days

Description

This policy will automatically delete Microsoft Teams Channel Alerts generated by sentinel in timely basis.

Step 4: Apply Policy to Teams Locations

1. You will now choose where the retention policy will apply. Select Teams channel messages.
   - Make sure you don't select Teams chats if you only want the policy to apply to channel messages.
2. You can choose to apply the policy to:
   - All Teams in the organization, or
   - Specific Teams if you need more granular control.



Choose the type of retention policy to create

Locations can be specified dynamically with an adaptive scope using attributes or properties, or if you know the sp
can select them individually from a list. An advantage of using an adaptive scope to determine target locations is t
update where it's applied based on the attributes or properties you define.

○ Adaptive
After selecting adaptive policy scopes, which consist of attributes or properties (e.g. 'Department' or 'Site URL') that define the
org, you'll choose supported locations containing the content you want to retain. The policy will automatically update to matc
scopes.

● Static
You'll choose locations containing the content you want to retain. If locations change after this policy is created (for example i
removed), you'll need to manually update the policy.

Choose where to apply this policy

The policy will apply to content that's stored in the locations you choos

You can set up data connectors to import content from non-Microsoft apps like Slack, W

Policies that apply to Teams chats or Teams channel messages can't include other locatio

Status	Location	Applicable Content
On	Teams channel messages	Messages from channel co meetings. Doesn't apply to messages. More details
Off	Teams chats and Copilot interactions	Messages from individual c bot chats, and Microsoft 36 details

Teams channel messages

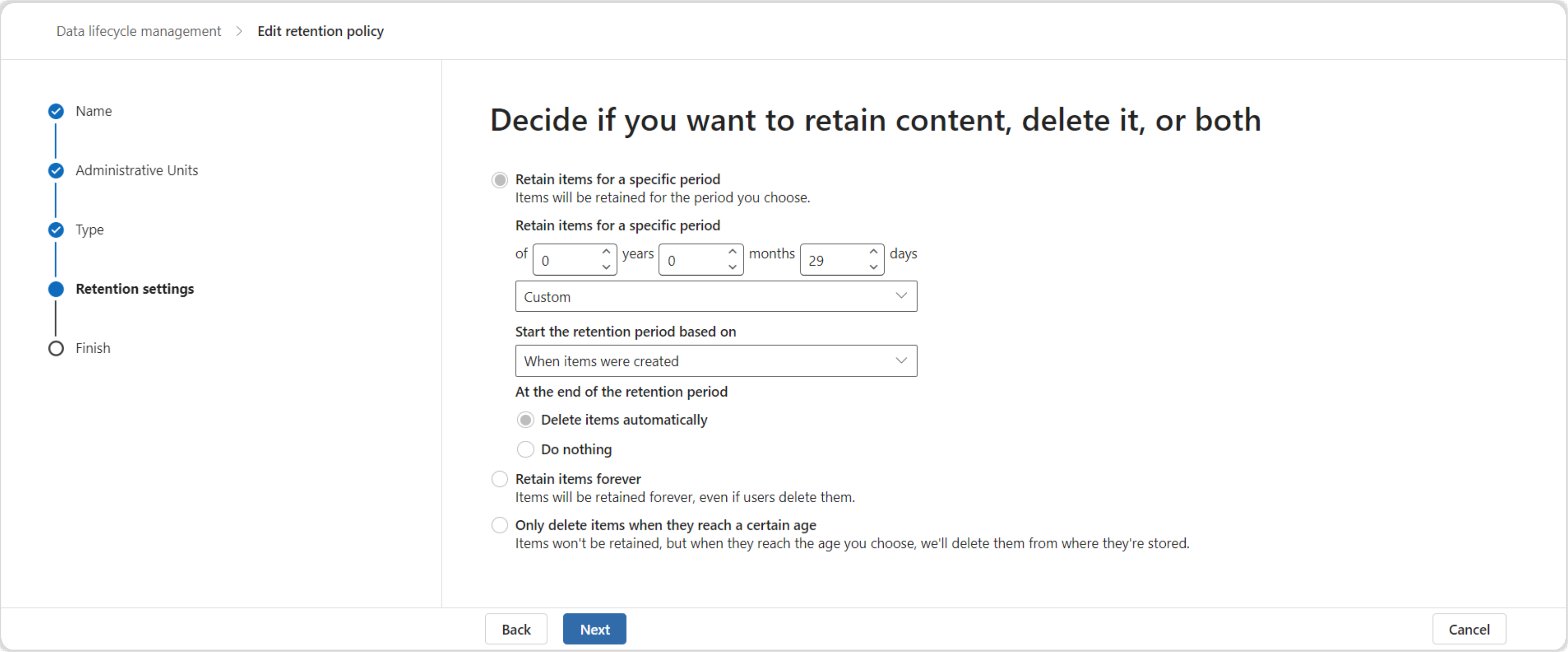
Search

1 selected

□	Name	Email
☑	SentinelAlerts	SentinelAlerts@dynatechconsultancy.com
□	UpgradeAX2012ToD365	UpgradeAX2012ToD365@dynatechconsultancy.c...
□	Al-Jazeera UAT 15 Dec	Al-JazeeraTT@dynatechconsultancy.com
□	Administration	DynatechAdministration@dynatechconsultancy.c...
□	Dynatech D365FO/AX App...	DynatechTechies@dynatechconsultancy.com
□	Dynatech documents	MyDoCLib@dynatechconsultancy.com
□	ESS Integration	ESSIntegration@dynatechconsultancy.com
□	Retail	Retail@dynatechconsultancy.com

Step 5: Define Policy Settings

1. In the next step, you'll configure policy settings:
    - Choose "Retain item for specific period".
    - Select the option "Delete items after a specific period".
    - Set the duration to 30 days.
2. In the section "When should we start the retention period?", select "When items were created" to start the 30-day countdown from the creation date of the message or item.



Decide if you want to retain content, delete it, or both

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

Retain items for a specific period

of 0 years 0 months 29 days

Custom

Start the retention period based on

When items were created

At the end of the retention period

● Delete items automatically

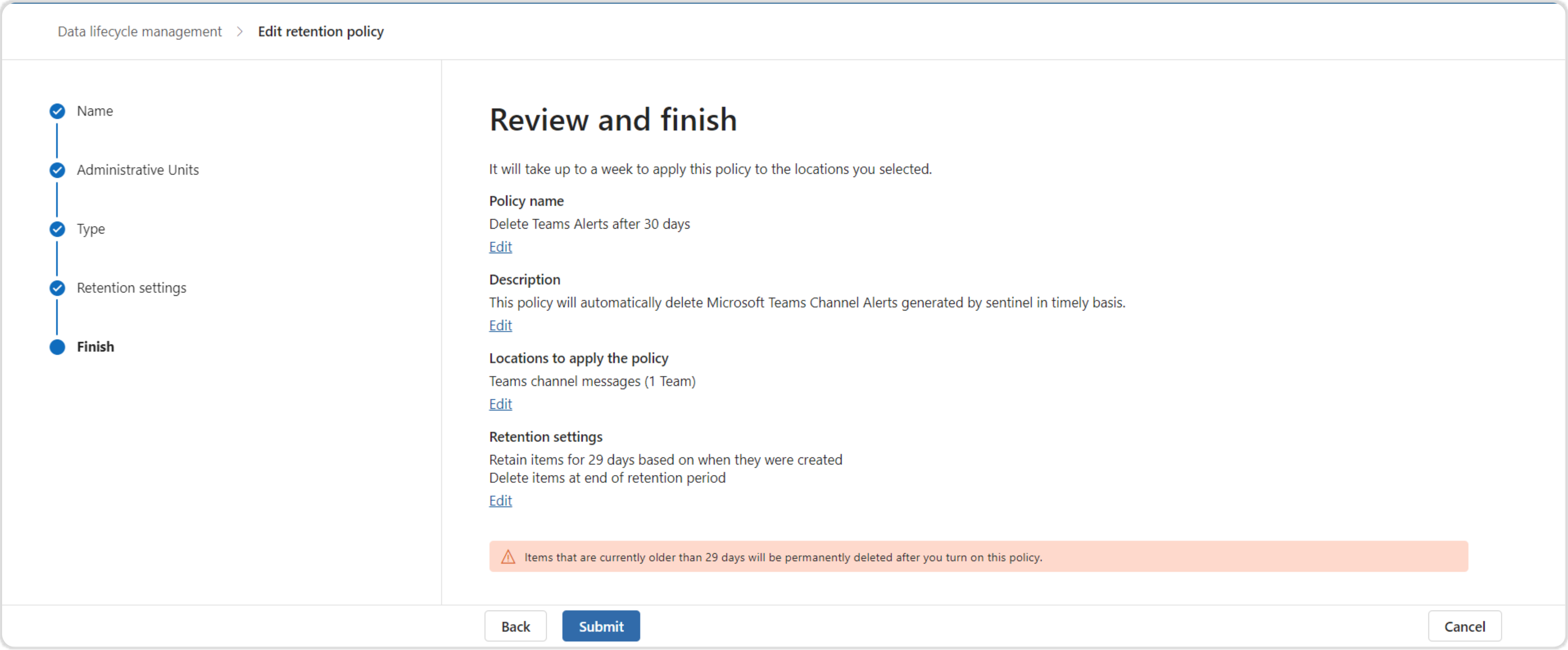
○ Do nothing

○ Retain items forever
Items will be retained forever, even if users delete them.

○ Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Step 6: Review and Save the Policy.

1. Review your settings, making sure the retention period is set to 30 days and applies to Teams channel messages.
2. Once confirmed, select Submit to save the policy.



Review and finish

It will take up to a week to apply this policy to the locations you selected.

Policy name
Delete Teams Alerts after 30 days
Edit

Description
This policy will automatically delete Microsoft Teams Channel Alerts generated by sentinel in timely basis.
Edit

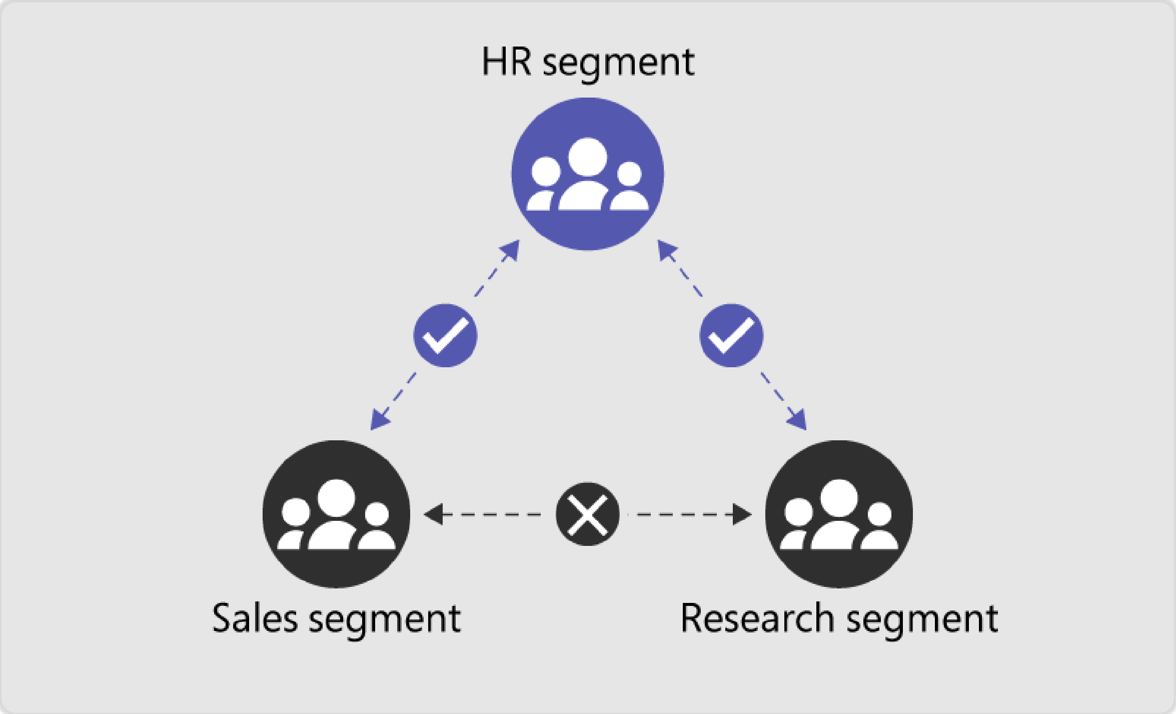
Locations to apply the policy
Teams channel messages (1 Team)
Edit

Retention settings
Retain items for 29 days based on when they were created
Delete items at end of retention period
Edit

⚠ Items that are currently older than 29 days will be permanently deleted after you turn on this policy.

Information Barriers in Microsoft Purview are compliance features designed to prevent unauthorized communication and collaboration between specific groups or individuals within an organization. They help organizations enforce policies that restrict communication to avoid conflicts of interest, protect sensitive information, and comply with regulatory requirements.

The following example illustrates three segments in an organization: HR, Sales, and Research. An information barrier policy has been defined that blocks communication and collaboration between the Sales and Research segments. These segments are incompatible.



With SharePoint information barriers, a SharePoint Administrator or Global Administrator can associate segments to a site to prevent the site from being shared with or accessed by users outside the segments.

Up to 100 compatible segments can be associated with a site. The segments are associated at the site level (previously called site collection level).

The Microsoft 365 group connected to the site is also associated with the site's segment.

Prevent Unwanted Communication and Collaboration

- Restrict communication and collaboration between specific groups or individuals within the organization to prevent conflicts of interest.
- Block certain users or groups from communicating through Microsoft Teams, SharePoint, OneDrive, and other Microsoft 365 services.

Conflict of Interest Management

- Manage conflicts of interest by preventing specific groups (e.g., investment banking and retail banking teams) from interacting with each other.
- Enforce ethical walls within the organization to avoid situations where information should not flow between different teams or departments.

Regulatory Compliance

- Ensure compliance with industry regulations like the Financial Industry Regulatory Authority (FINRA), SEC regulations, and GDPR.
- Enforce legal and regulatory requirements by separating teams, departments, or business units that should not communicate or collaborate.

Flexible Policy Management

- Create and manage custom policies to define who can communicate and collaborate with whom based on user attributes like department, location, or role.
- Use a combination of allow and deny policies to set up complex information barriers that suit specific business needs.

Safeguard Sensitive Information

- Prevent unauthorized access and sharing of sensitive or confidential information between restricted groups.
- Protect intellectual property, trade secrets, and other sensitive information by restricting who can access, view, or share content.

Controlled Access to Resources

- Restrict access to specific SharePoint sites, OneDrive accounts, or Teams based on information barrier policies.
- Prevent users in restricted groups from searching for or discovering other users, files, or sites they are not allowed to access.

Integration with Compliance and Security Solutions

- Use information barriers in conjunction with Microsoft Compliance Centre tools like Data Loss Prevention (DLP), Insider Risk Management, and eDiscovery.
- Ensure information protection and compliance across all layers of data security and management.

User Search and Discovery Restrictions

- Block users in restricted segments from finding each other in directory searches or viewing each other's presence status.
- Prevent users from adding members of restricted groups to Teams, meetings, or chat conversations.

Enhanced Privacy and Security

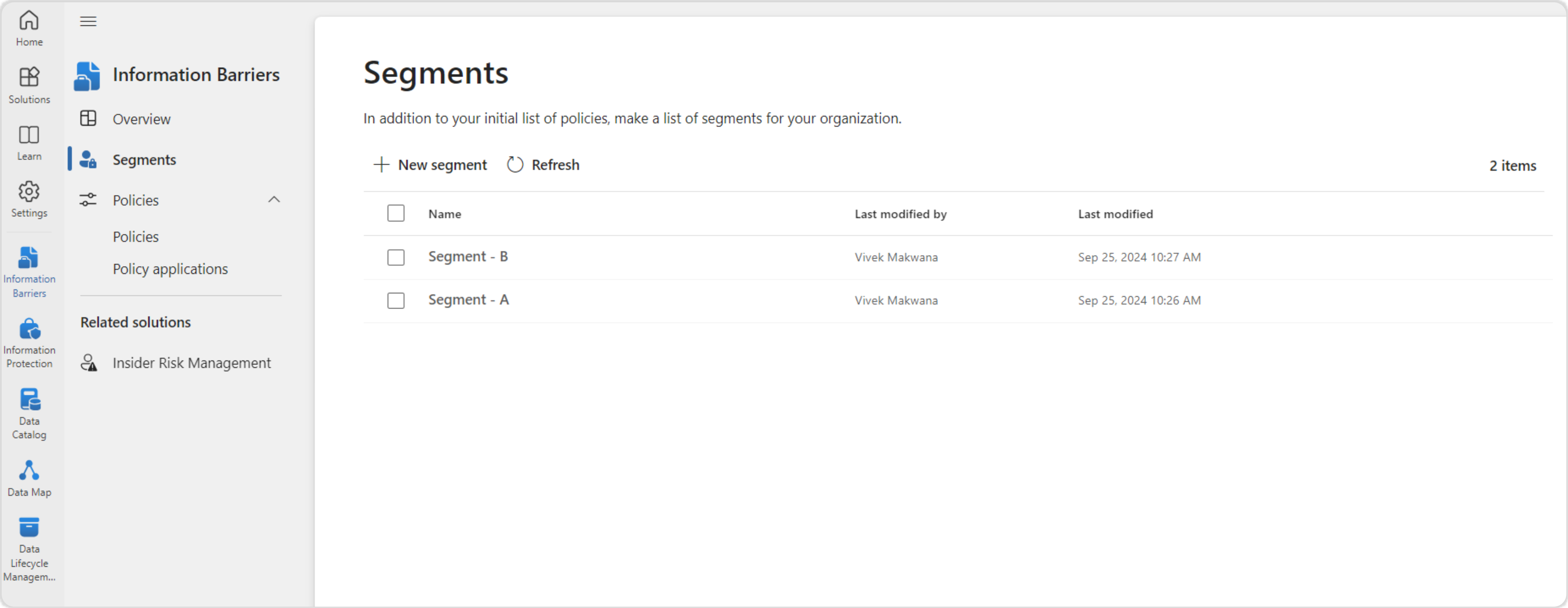
- Protect sensitive projects or initiatives by isolating specific teams and restricting their interactions with other parts of the organization.
- Reduce the risk of accidental data leaks or unauthorized disclosures by limiting communication paths.

Monitoring and Compliance Reporting

- Monitor information barrier policy violations and generate alerts for attempted or successful violations.
- Generate reports and logs to demonstrate compliance with information barrier requirements during audits or reviews.

Access Microsoft Purview Compliance Portal

1. Go to Microsoft 365 Compliance Center at: https://compliance.microsoft.com.
2. From the left-hand navigation pane, click on Information Barriers.



Segments

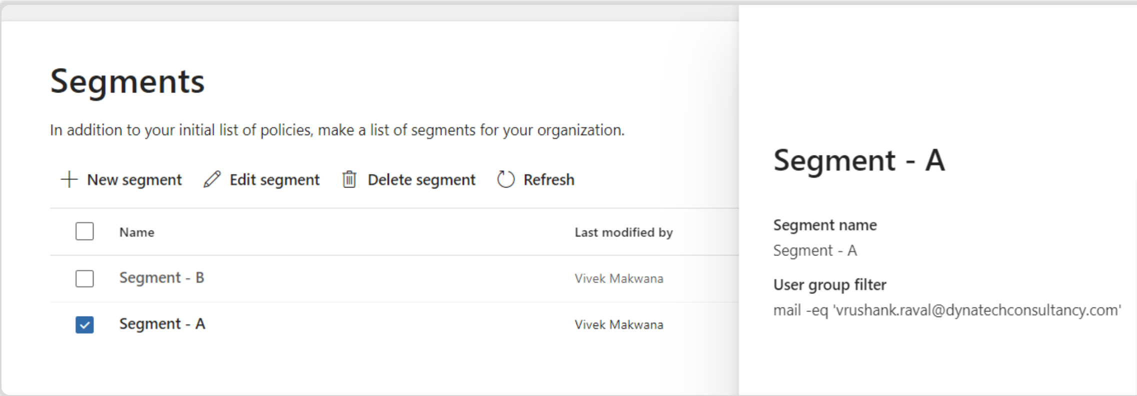
In addition to your initial list of policies, make a list of segments for your organization.

2 items

□	Name	Last modified by	Last modified
□	Segment - B	Vivek Makwana	Sep 25, 2024 10:27 AM
□	Segment - A	Vivek Makwana	Sep 25, 2024 10:26 AM

Set Up Segments

1. Segments are used to define user groups within the organization that can communicate or must be isolated from others.
2. Navigate to Information Barriers → Segments.
3. Click Create a segment.
4. Define the segment by adding a name and specifying the criteria (based on Azure Active Directory attributes, like Department, JobTitle, etc.).
    - Example: Segment Name: Finance with criteria Department = Finance.



Segments

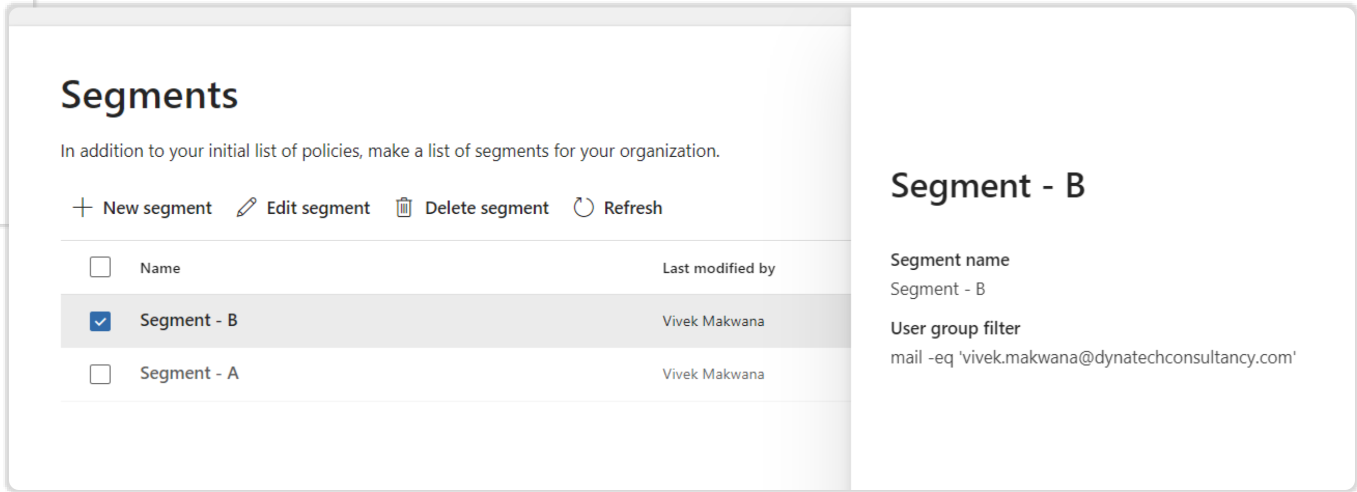
In addition to your initial list of policies, make a list of segments for your organization.

	Name	Last modified by
□	Segment - B	Vivek Makwana
☑	Segment - A	Vivek Makwana

Segment - A

Segment name
Segment - A

User group filter
mail -eq 'vrushank.raval@dynatechconsultancy.com'



Segments

In addition to your initial list of policies, make a list of segments for your organization.

	Name	Last modified by
☑	Segment - B	Vivek Makwana
□	Segment - A	Vivek Makwana

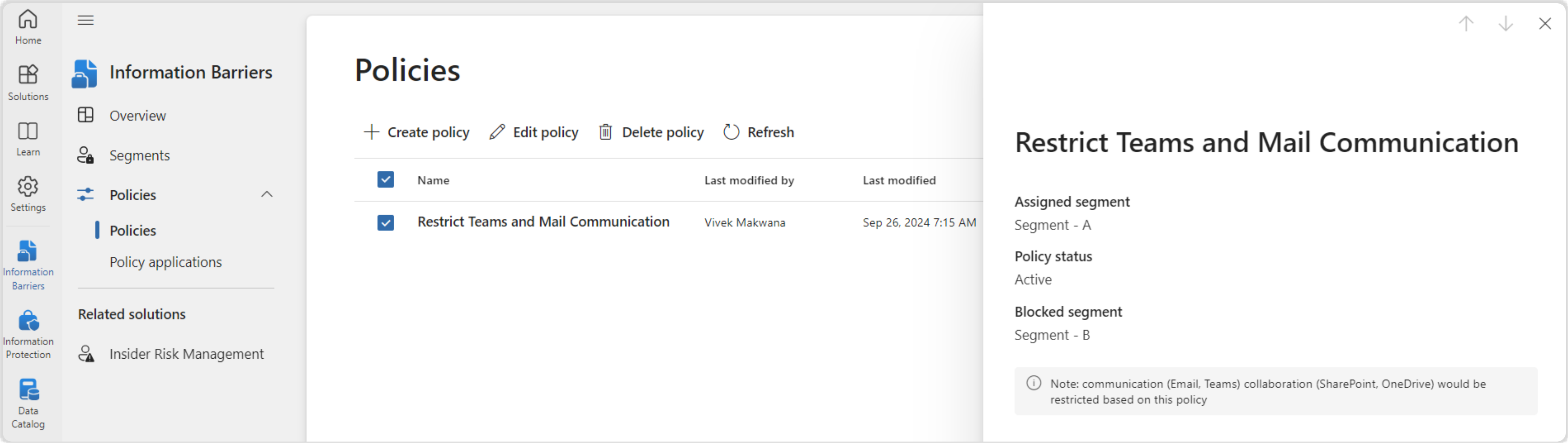
Segment - B

Segment name
Segment - B

User group filter
mail -eq 'vivek.makwana@dynatechconsultancy.com'

Create Policies

1. After creating segments, you need to define policies that specify how these segments can interact.
2. Go to Information Barriers → Policies.
3. Click Create a policy.
4. Provide a Name and Description for the policy.
5. Choose the Segment that the policy applies to (e.g., Finance, Legal, etc.).
6. Set Allow or Block rules to control how communication and collaboration between the selected segment and other segments should behave.
   - Example: Block communication between the Finance segment and Marketing segment.



Policies

☑	Name	Last modified by	Last modified
☑	Restrict Teams and Mail Communication	Vivek Makwana	Sep 26, 2024 7:15 AM

Restrict Teams and Mail Communication

Assigned segment
Segment - A

Policy status
Active

Blocked segment
Segment - B

ⓘ Note: communication (Email, Teams) collaboration (SharePoint, OneDrive) would be restricted based on this policy

Define Communication Restrictions

1. Choose the users or groups who are restricted from communicating with each other.
2. You can block communication across services like Microsoft Teams, SharePoint, OneDrive, and Exchange Online.
3. Set the rule to Block or Allow communication between specific segments.

Review and Submit

1. Once you have set the policies and restrictions, review your settings.
2. Click Submit to create the policy.

Policy Activation

1. The policy you created will not be active immediately. You need to activate it.
2. To activate, select the policy in the Information Barriers → Policies section and click Activate.
3. Activation can take some time depending on the size of the organization and the complexity of the policy.

User Access and Role Management

- Role granularity: While Purview has role-based access controls (RBAC), fine-grained permission management might be limited for some enterprise-scale scenarios.

Cross-Platform Support

- Multi-cloud complexity: Though it integrates with Azure, AWS, and other cloud platforms, managing governance across multi-cloud environments can introduce additional complexity and may require custom configurations.

Integration Limitations

- Limited support for certain data sources: While MS Purview integrates with many data sources (on-premises, cloud-based, and SaaS applications), there are some proprietary or lesser-used data sources that may not be supported directly.

Data Retention and Archiving

- Retention policies: While Purview provides capabilities to manage retention, it may not fully meet all enterprise needs around long-term archival and retrieval in certain jurisdictions.

DynaTech | Systems

Want to know more?

Contact Us!

DynaTech Systems has proudly served clients seeking advanced tech solutions across the globe with top-notch precision and excellence.

Locations

USA, Canada, UK, India

Mail Us

sales@dynatechconsultancy.com

Phone

+1 844 787 3365

Visit Our Website

www.dynatechconsultancy.com