

© Copyright Microsoft Corporation. All rights reserved.

FOR USE ONLY AS PART OF MICROSOFT VIRTUAL TRAINING DAYS PROGRAM. THESE MATERIALS ARE NOT AUTHORIZED FOR DISTRIBUTION, REPRODUCTION OR OTHER USE BY NON-MICROSOFT PARTIES.



# Microsoft Security Virtual Training Day: Protect Data and Manage Risk

# **Information protection and governance in Microsoft 365**

# Lesson: Introduction to information protection and governance in Microsoft 365

# Lesson Agenda



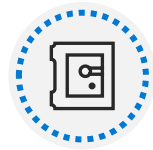
Discuss information protection and governance and why it's important.



Describe Microsoft's approach to information protection and governance.

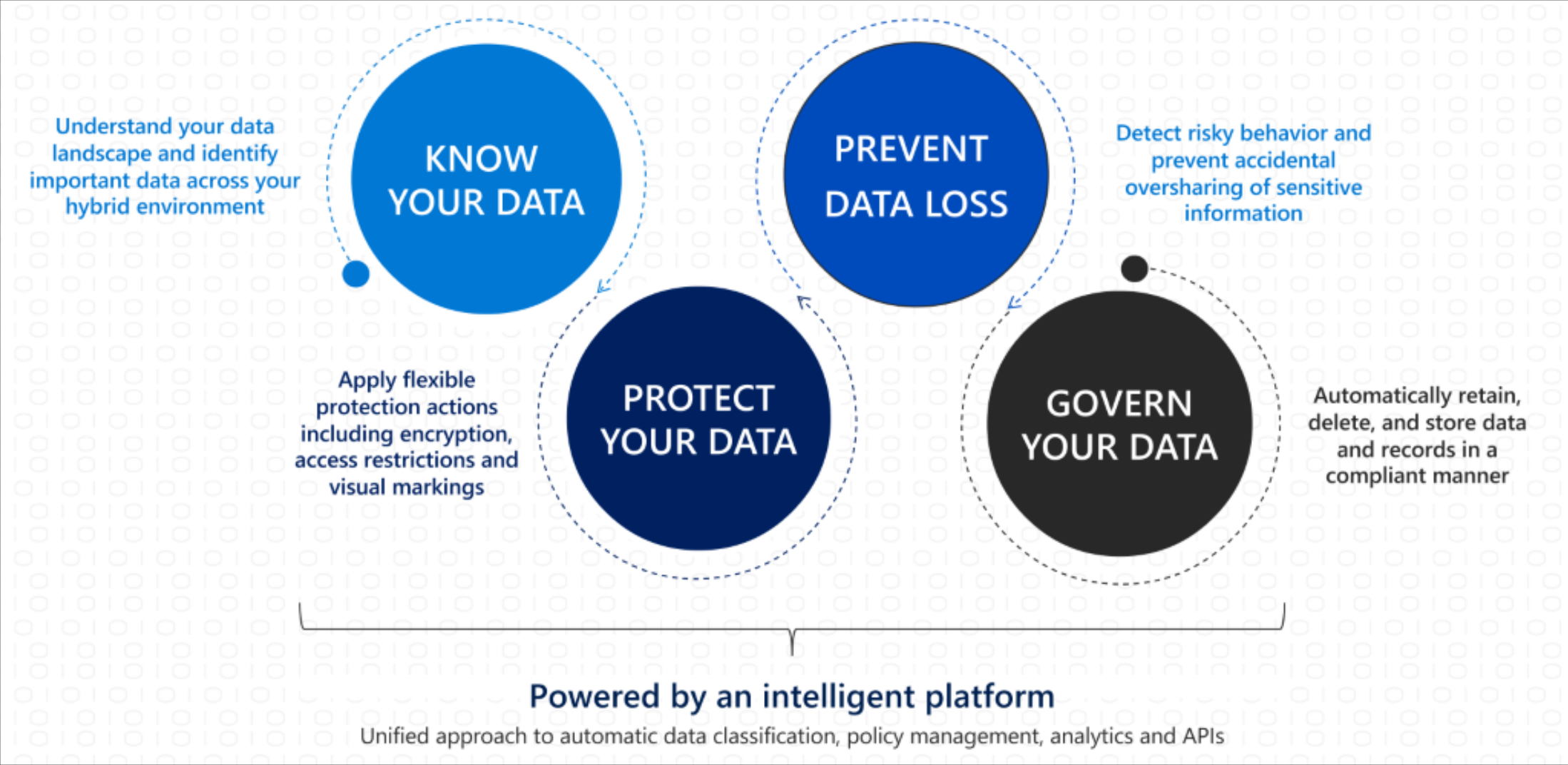


Define key terms associated with Microsoft's information protection and governance solutions.



Identify the solutions that comprise information and governance in Microsoft 365

# Basics of information and governance in Microsoft 365



# Know your data

Data classification concepts, apply one or more of the following to your data:



Sensitive information types

---



Trainable classifiers

---



Labels

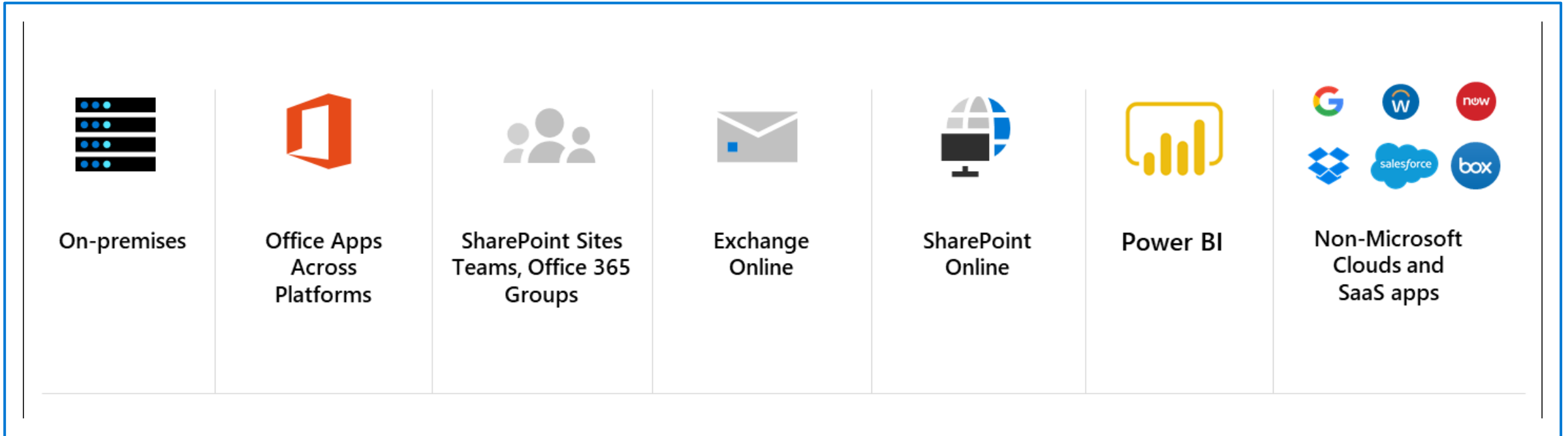
---



Policies

# Protect your data

Information protection is integrated into Microsoft 365 apps and services like:





# Prevent data loss

## Secure Data

- Enforce conditional access to sensitive data
- DLP action to block sharing
- Encrypt files and emails based on sensitivity label
- Prevent data leakage through DLP policies based on sensitivity label
- Business data separation on devices
- Secure email with encryption & permissions

## Enable productivity

Manually apply sensitivity label consistently across applications and endpoints

Show recommendations and tooltips for sensitivity labels with auto-labeling and DLP

Visual markings to indicate sensitive documents across apps and services (like watermarks, lock icons, sensitivity column in SharePoint Online)

Co-author and collaborate with sensitive documents

Enable searching of encrypted files in SharePoint

Allow users to open and share encrypted PDF files in Edge in addition to Adobe Acrobat Reader

# Govern your data

Themes of the Microsoft solutions for governing your data:



Streamlined administration

---



Automation at scale

---



Tailored workflows

---

**Lesson: Classify data for protection and governance**

# Lesson Agenda



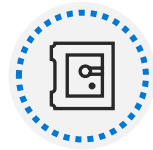
List the components of the data classification solution.



Identify the cards available on the Data Classification overview tab.



Explain the Content explorer and Activity explorer.



Describe how to use sensitive information types and trainable classifiers.

# Basics of data classification

## Microsoft 365 data classification components:

### **Overview**

Provides snapshots of how sensitive information types and labels are being used.

### **Content explorer**

Explore the email and documents in your organization that contain sensitive information or have labels applied.

### **Activity explorer**

Review activity related to content containing sensitive info or has labels applied, such as what labels were changed, files were modified, and more.

### **Sensitive info types**

Manage the built-in and custom sensitive information types available to classify data.

### **Trainable classifiers**

Manage the classifiers used to identify content based on what the item is, not by the elements in the item.

# Classify data using sensitive information types

Information protection and governance solutions and where in those solutions you can use sensitive information types:



**Information protection:** Sensitivity label auto-labeling policies

---



**Data loss prevention (DLP):** DLP policies

---



**Information governance:** Retention policies and retention label auto-apply policies

---

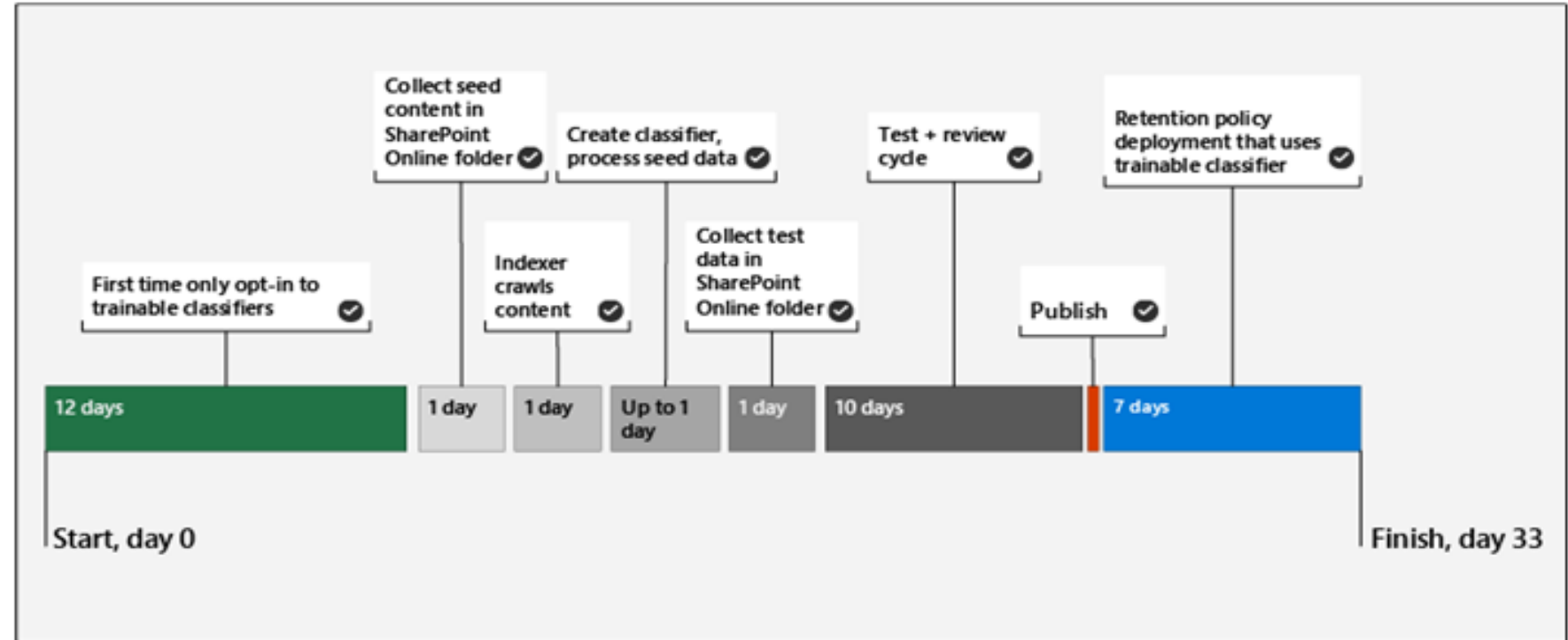


**Records management:** Retention label auto-apply policies

# Classify data using trainable classifiers

Training includes several steps:

1. Items of a type added to a SharePoint library.
2. Train until the classifiers do not request additional training documents.
3. Review items to improve the classifier accuracy.



# Classify data using trainable classifiers (continued)

Classifiers separate into default classifiers, custom trainable classifiers, and retrained classifiers.



## **Built-in or default classifiers**

Classification for basic use or testing: Offensive Language, Resumes, Source Code, Targeted Harassment, Profanity and Threat.

---



## **Custom classifiers**

- Must be activated, which requires 7-14 days for basic analytics.
- Training requires 50-500 positive samples of seed data.
- Up to 24 hours of seed data to be processed.
- Up to 10,000 positive and negative samples for testing.



# Review sensitive information and label usage

**The Overview page can answer questions like:**

- What sensitive data is out there?
- What labels are being used the most?
- Is sensitive data being copied or shared outside the organization?

Top activities detected

**1169810 activities**

**753.8K** File created

**288K** File copied to clipboard

**94.2K** File printed

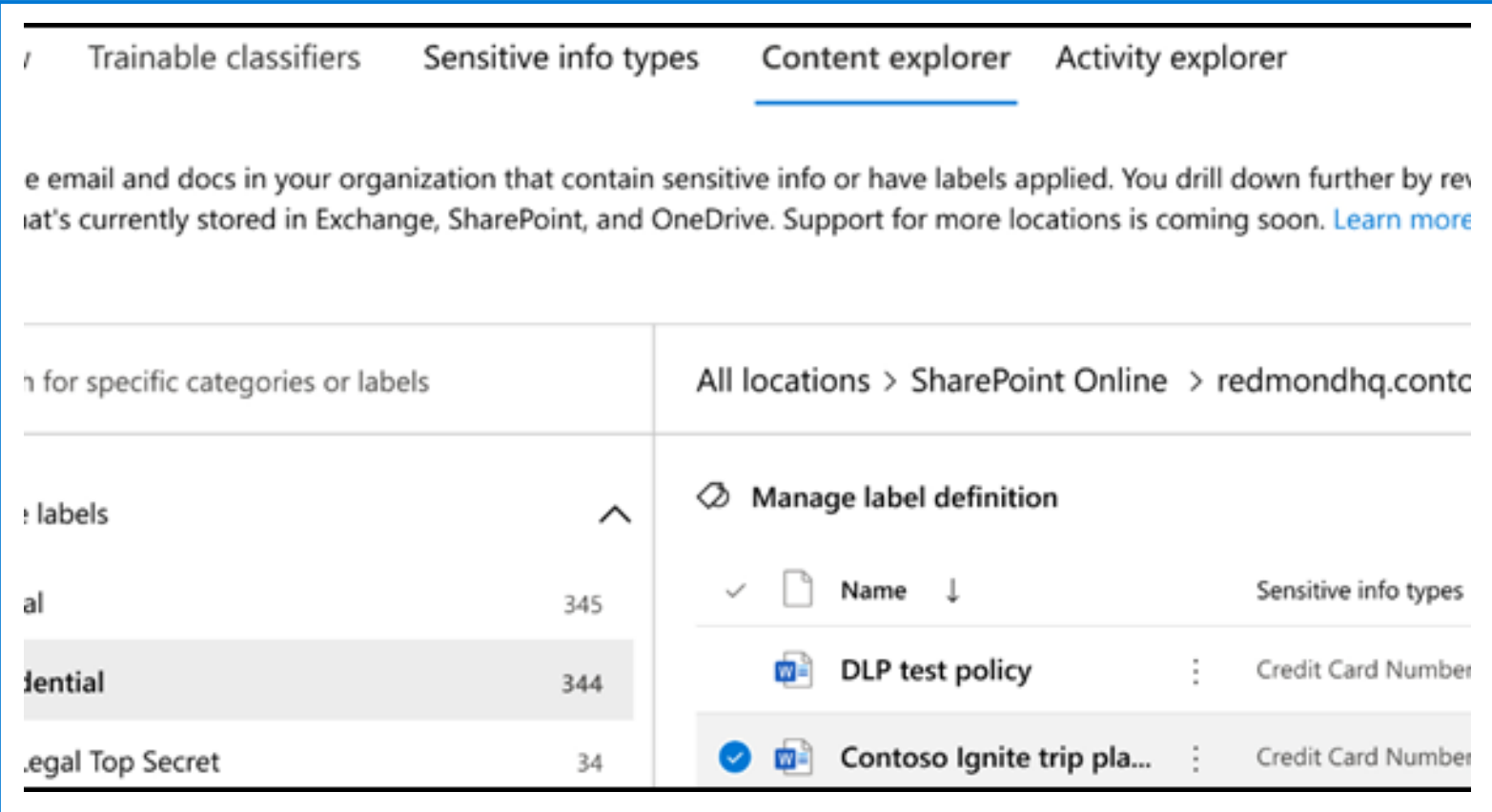
# Explore labeled and sensitive content

## Here is a summary of what the content explorer provides:

Visibility into the amount of sensitive data in a document that triggered the classification to be applied.

Ability to filter by label or sensitive information type to get a detailed view of the locations where the data is stored.

Integrated viewer to display documents, providing context for the circumstances in which sensitive information is being detected.



The screenshot shows the Microsoft Content Explorer interface. At the top, there are navigation tabs: Trainable classifiers, Sensitive info types, Content explorer (selected), and Activity explorer. Below the tabs, there is a brief description: "View email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing what's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)".

The main content area is divided into two sections. On the left, there is a list of labels with their counts:

Label	Count
Confidential	345
Legal Top Secret	344
Other	34

On the right, there is a detailed view for the "Confidential" label. It shows the breadcrumb "All locations > SharePoint Online > redmondhq.conto". Below this, there is a "Manage label definition" section with a table of sensitive information types:

Name	Sensitive info types
DLP test policy	Credit Card Number
Contoso Ignite trip pla...	Credit Card Number

# Activities related to your data

Activity explorer provides the following:



Visibility into document-level activities like label changes and label downgrades.

---



Ability to filter to see all the details for a specific label including file types, users, and activities.

---



Understand a broad-spectrum of sensitivity label activities across Microsoft 365.

**Lesson: Create and manage sensitive information types**

# Lesson Agenda



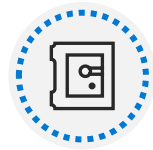
Recognize the difference between built-in and custom sensitivity labels.



Configure sensitive information types with exact data match-based classification.



Implement document fingerprinting.



Create custom keyword dictionaries.

# Compare built-in versus custom sensitive information types

## Built-in Sensitive Information Types

- More than 100 built-in sensitive information types.
- Includes default patterns managed by Microsoft.
- Fulfills basic protection of common information types.
- Starting point for implementations.

## Custom Sensitive Information Types

- Allows to detect business individual sensitive information.
- Consists of customized patterns.
- Provides several special features:
  - Exact Data Match (EDM)-based classification
  - Document Fingerprinting
  - Keyword dictionaries

# Create and manage custom sensitive information types

## Sensitive Information Type parts



### **Primary pattern**

Search pattern for detection, consisting of keywords or regular expressions.

---



### **Additional evidence**

Second search pattern for higher matching accuracy of the primary pattern, consists of keywords.

---



### **Character proximity**

Detection window in characters of primary patterns and additional evidence.

---



### **Confidence level**

Supporting level of pattern and evidence matching accuracy.

# Describe custom sensitive information types with exact data match

Sensitive information type based on database matching:

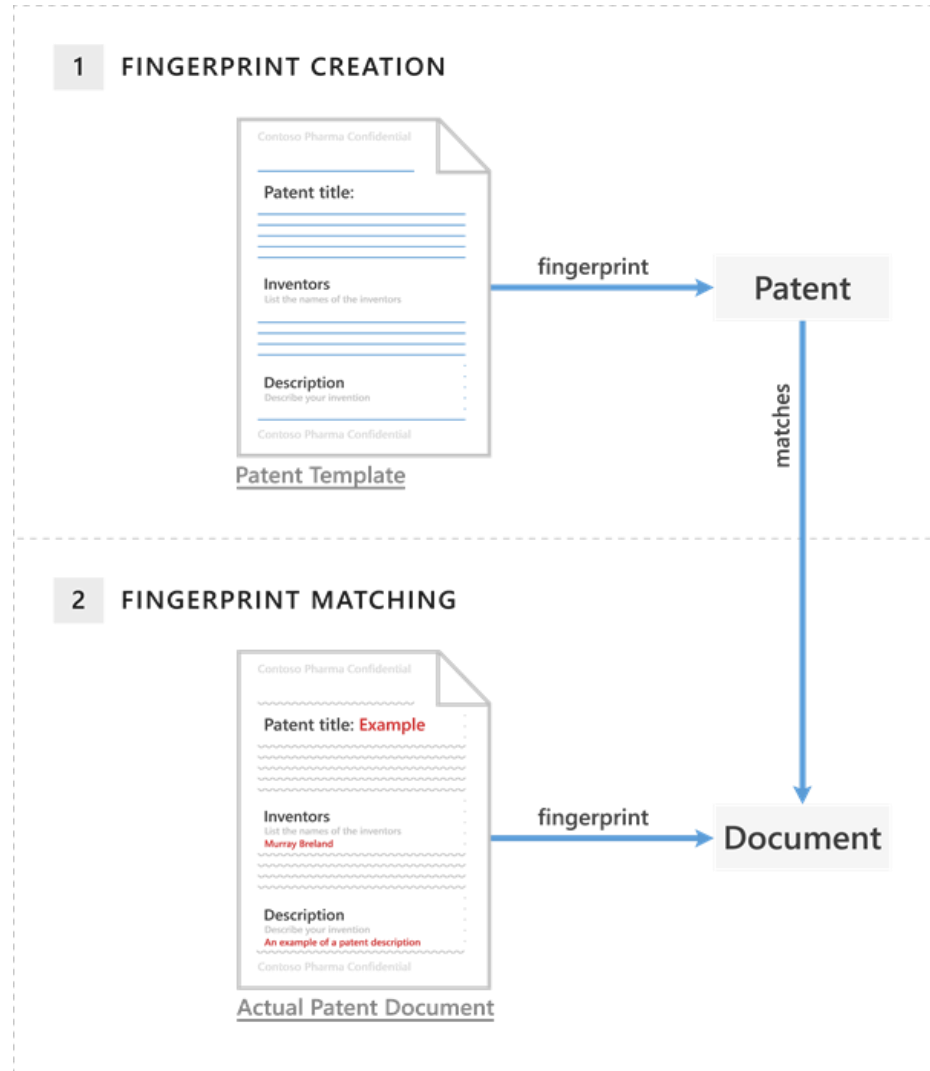
- Supports up to 100 million rows of sensitive data, 32 columns (fields) per data source and up to 5 columns (fields) marked as searchable.
- Additional license requirements
- Configuration done in three steps:  
Step 1: Set up EDM-based classification  
Step 2: Hash and upload the sensitive data  
Step 3: Use EDM-based classification in policies

Phase	Requirements
<b>Step 1: Set up EDM-based classification</b>	<ul style="list-style-type: none"><li>• Read access to the sensitive data</li><li>• Database schema in XML format</li><li>• Rule package in XML format</li><li>• Admin permissions to the Security &amp; Compliance Center</li></ul>
<b>Step 2: Hash and upload the sensitive data</b>	<ul style="list-style-type: none"><li>• Custom security group and user account</li><li>• Local admin access to machine with EDM Upload Agent</li><li>• Read access to the sensitive data</li><li>• Process and schedule for refreshing the data</li></ul>
<b>Step 3: Use EDM-based classification in policies</b>	<ul style="list-style-type: none"><li>• Microsoft 365 subscription with DLP</li><li>• EDM-based classification feature enabled</li></ul>



# Implement document fingerprinting

- Digital fingerprint from empty template document.
- Detection of documents created from a template.
- Requires all fields from the original template document.
- Exchange Online only.
- Password protected files are not supported, as well as documents containing images.



# Create a keyword dictionary

Efficient way to manage large lists of words that are regularly subject to changes

- Supports up to 100KB of terms after compression.
- Source can be cleartext files such as .txt and .csv files.
- Keyword Dictionary Creation Best Practices:

For a school, get together with a class of students to find words and phrases you don't want in an education environment. For companies, use various options to collect keywords:

- Search typical words from some departments e.g., using Microsoft Forms.
- Information from employees e.g., from HR or legal to create a list of typical words.
- Create an employee audit and then create the list out of the outcome.

# Manage Sensitive Information Types

## **Scenario:**

Contoso Ltd. previously had issues with employees accidentally sending out personal information from customers when working on support tickets in the ticketing solution. To educate users in the future, a custom sensitive information type is required to identify employee IDs in emails and documents.



# Manage sensitive information



# Lesson: Configure sensitivity labels

# Lesson Agenda



Discuss the information protection solution and its benefits.



List the customer scenarios the information protection solution addresses.



Describe the information protection configuration process.



Explain what users will experience when the solution is implemented.

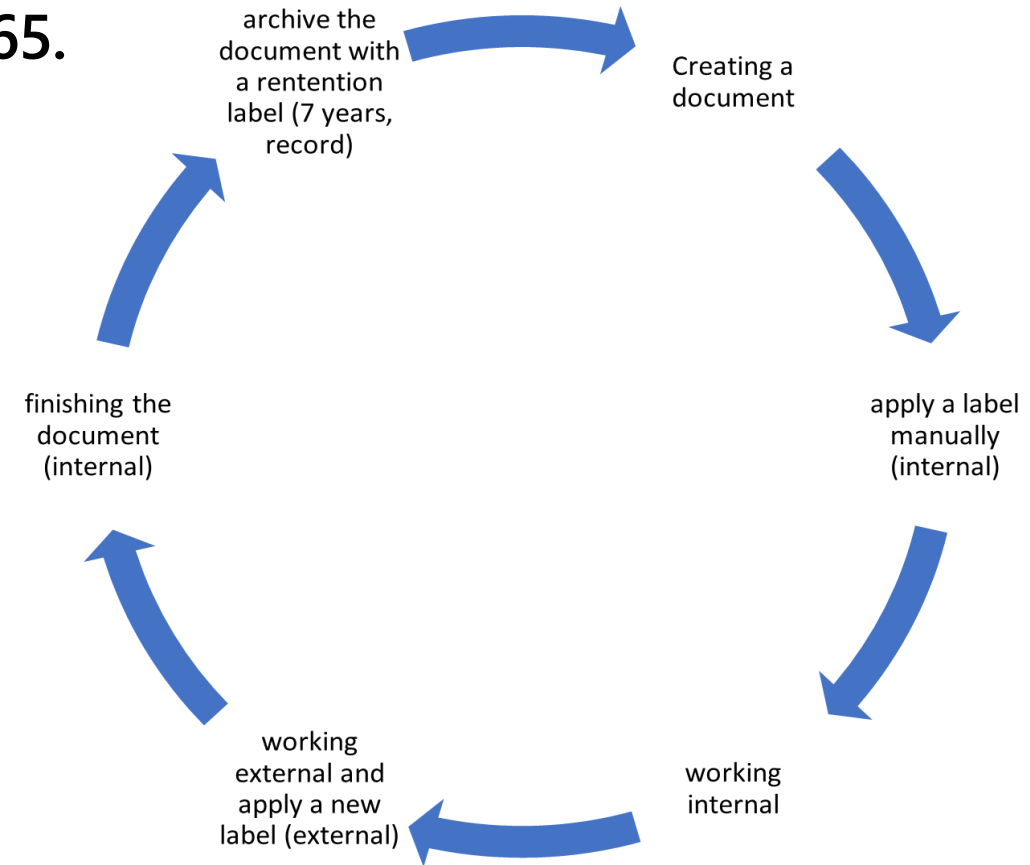


Articulate deployment and adoption best practices.

# Basics of sensitivity labels

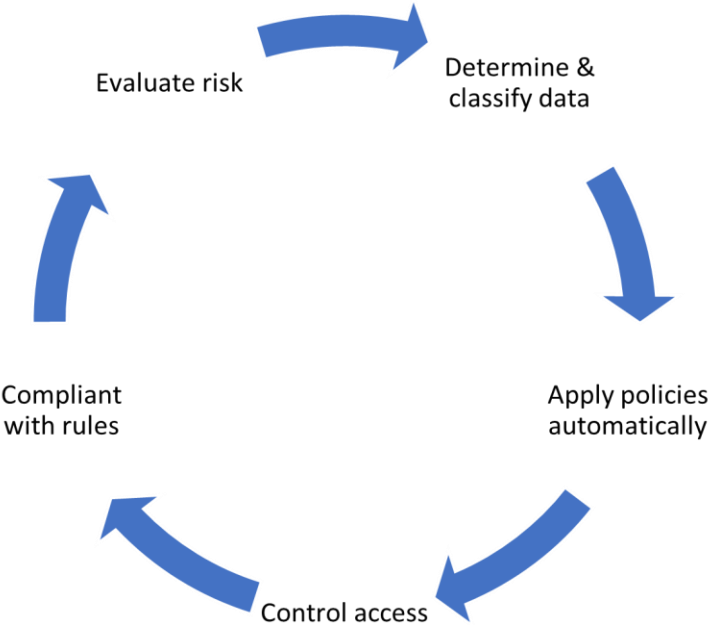
Sensitivity Labels are a solution to handle the lifecycle of company data with classify, encryption, and access management in Microsoft 365.

- Sensitivity Labels move with a labeled document and can be applied to locations such as SharePoint sites, Microsoft 365 groups, documents, and e-mails or may be applied to Azure Purview assets.

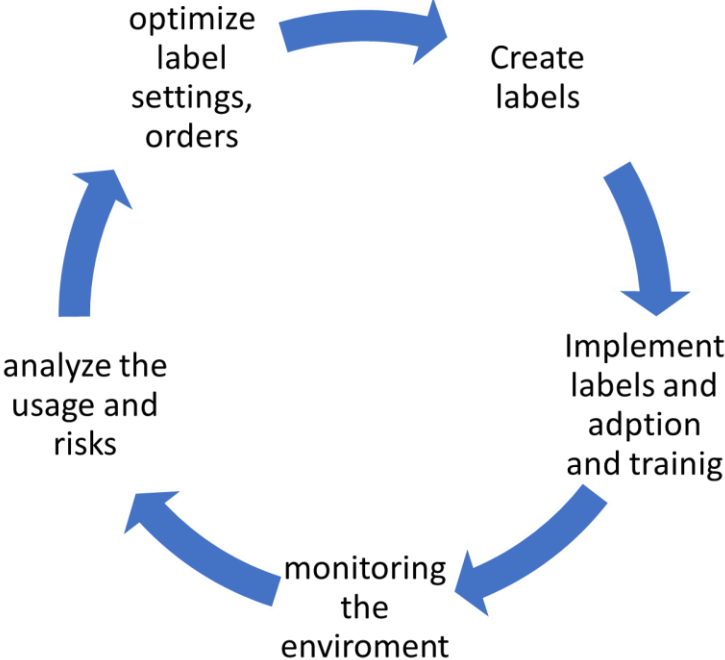


# Administer the sensitivity labeling lifecycle

The lifecycle of the sensitivity labeling for the administrator:



The lifecycle of the sensitivity label:

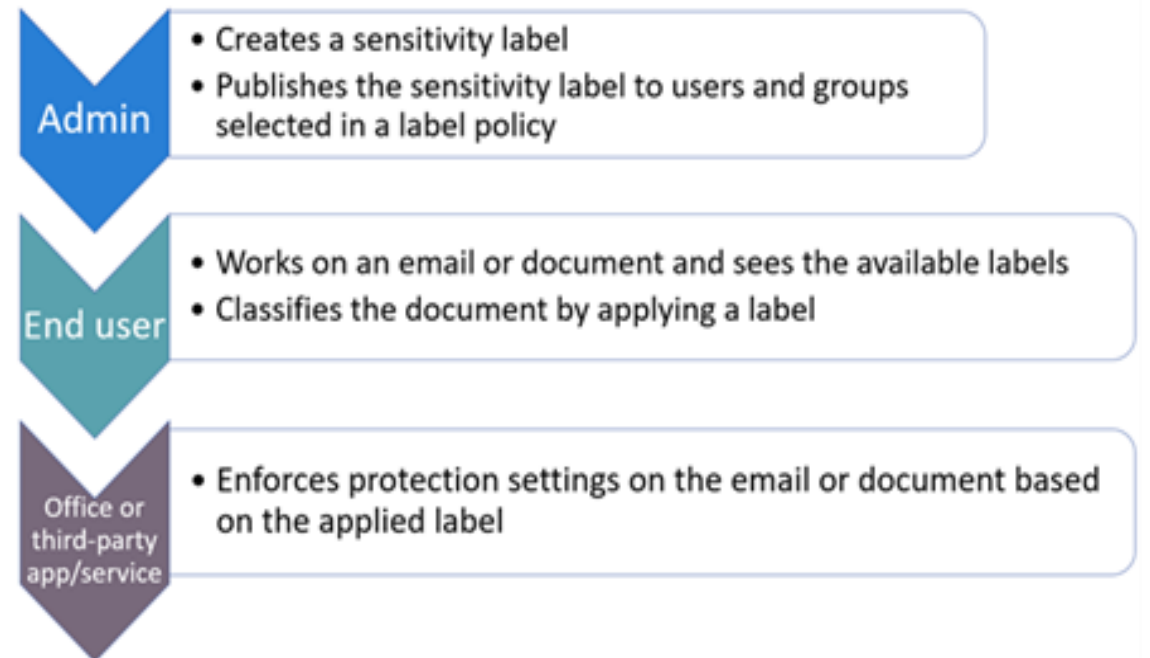




# Configure sensitivity labels

Sensitivity labels can be created by an admin through either the Compliance Center UI or PowerShell.

- Select a scope of either Files & emails, Group & sites or Azure Purview assets.
- Items can be auto-labeled on either Sensitive info types or trainable classifiers.
- PowerShell provides additional options for multilanguage support.



# Configure sensitivity label policies

- Sensitivity labels must be published before they can be applied to items.
- Groups must be email enabled like security groups or distribution lists.
- Microsoft Teams is a use case.
- It is a best practice to name the sensitivity label using a naming guideline (like "2021-Jan-HR-HRLabels-RK").

# Configure auto-labeling policies

The Microsoft 365 compliance center includes options to configure and publish auto-labeling policies.

- The option is provided through the *create a label* wizard and allows the label to be automatically assigned based on conditions set by the administrator.
- You can select up to 20 sensitive information types from a list.

## Auto-labeling for files and emails



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

### ^ Detect content that matches these conditions ⓘ

+ Add condition ▾

### When content matches these conditions ⓘ

Automatically apply the label ▾

Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. [Learn more](#)



## Lesson: Apply and manage sensitivity labels

# Lesson Agenda



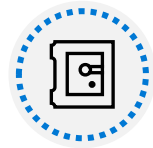
Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.



Monitor label usage using label analytics.



Configure on-premises labeling.



Manage protection settings and marking for applied sensitivity labels.



Apply protections and restrictions to email and files.

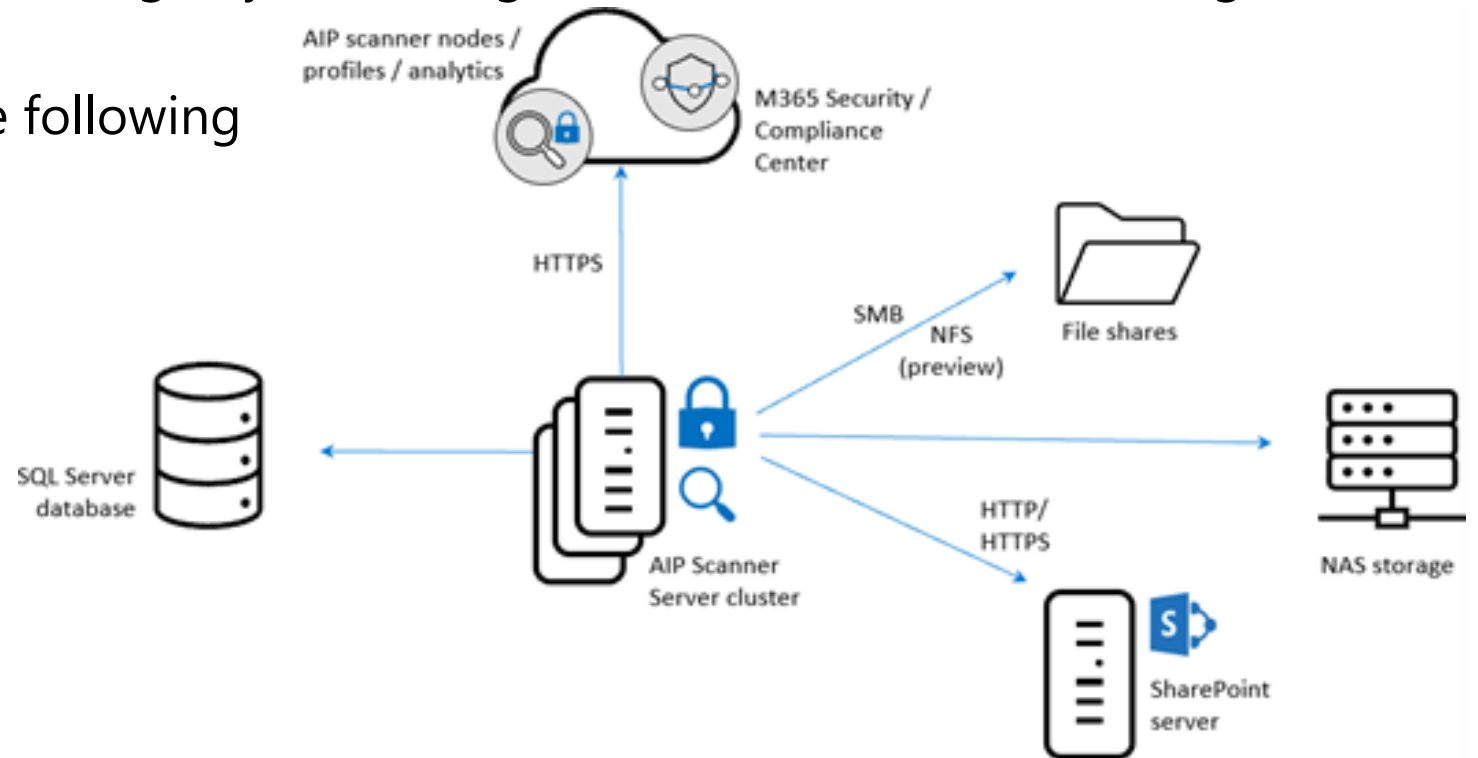
# Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites

- Labels may be published for use in Microsoft 365 Groups, Microsoft Teams, Yammer communities and SharePoint sites.
- You must activate labels in the tenant level via the Azure AD PowerShell module before they can be used.
- Sensitivity labels can be manually assigned to SharePoint Sites and Teams sites through the creation settings.
- Labels can be changed through the properties of existing SharePoint sites or Microsoft Teams.
- A sensitivity label is applied to a Group in the Azure portal through Azure services > Groups > properties.

# Plan on-premises labeling

The sensitivity labels functionality is natively only available in the user context or in the Microsoft 365 services for auto-labeling

- This can be expanded to on-premise through hybrid configuration of the Unified Labeling Scanner.
- The Unified Labeling Scanner has the following requirements for setup:
  - Windows server 2016 / 2019 with UI
  - A SQL server installation
  - An Azure AD token
  - AD Service accounts



# Configure on-premises labeling for the Unified Labeling Scanner

The Unified labeling scanner can be used for different operational scenarios, some of them include:



**Scan for a report only to know your data:** Run the scanner in discovery mode only to create reports that check to see what happens when your files are labeled.

---



**Run the scanner to find and discover files with sensitive information:** Run the scanner to discover files with sensitive information, without configuring labels that apply automatic classification.

---



**Run and apply labels:** Run the scanner automatically to apply labels as configured.

---



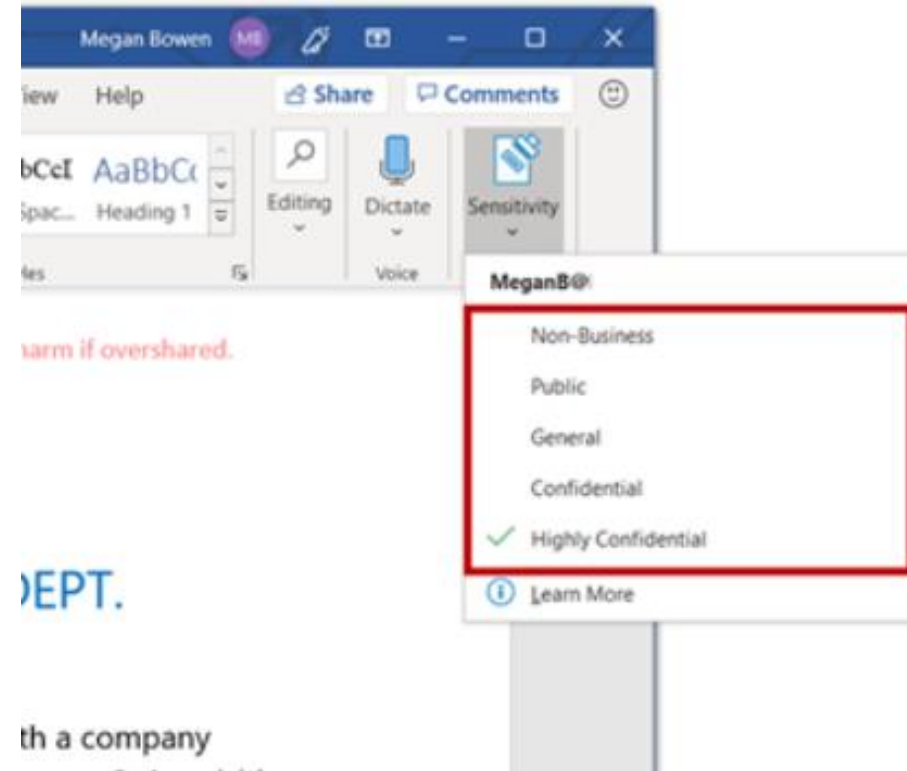
**Specific scan only a few files types:** Define a file types list to specify specific files to scan or to exclude.



# Apply protections and restrictions to email and files

It is important to apply a sensitivity label to an email as well as the contained files.

- The email is only the container of the files with it's own separate protection configuration for the attachments.
- You can apply a sensitivity label to an email manually in the Outlook Desktop app. Create an email and before sending the email an option is available in the ribbon menu to assign a sensitivity label.
- You can create a default sensitivity label for both the documents and emails using auto-apply publishing through the Compliance center.



# Apply protections and restrictions to email and files (continued)

**It's possible to apply a sensitivity label to a file through the following options:**

- Unified Labeling Client (Windows, Mac), Native Office Desktop Apps (limited), Mobile Office Apps (iOS, Android)
- You can:
  - choose a label for external and internal sharing
  - Assign a label without a Microsoft Office client
  - Apply a default sensitivity label to a SharePoint document library
  - Set a default label via sensitive information
  - Apply sensitivity labels with MCAS

# Monitor label performance using label analytics

**The sensitivity labels reports are available in the Security or the Compliance Center.**

- Available reports include:
  - DLP policy
  - DLP Incidents
  - DLP false positives and overrides
- **The Label analytics tool is provided through the Azure Portal and requires an Azure subscription.**
- **Monitoring and analysis is also available through Azure Sentinel.**

## Manage sensitivity labels

### **Scenario:**

Your organization is based in Rednitzhembach, Germany and is currently implementing a sensitivity plan to ensure that all employee documents in the HR department have been marked with a sensitivity label as part of your organizations information protection policies.



# Message encryption in Office 365



Lesson : Describe Microsoft 365 encryption

# Lesson Agenda



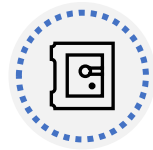
Explain how encryption mitigates the risk of unauthorized data disclosure.



Describe Microsoft data-at-rest and data-in-transit encryption solutions.



Explain how Microsoft 365 implements service encryption to protect customer data at the application layer.



Describe the differences between Microsoft managed keys and customer managed keys for use with service encryption.

# Basics of Microsoft 365 encryption

What is encryption in Microsoft 365?

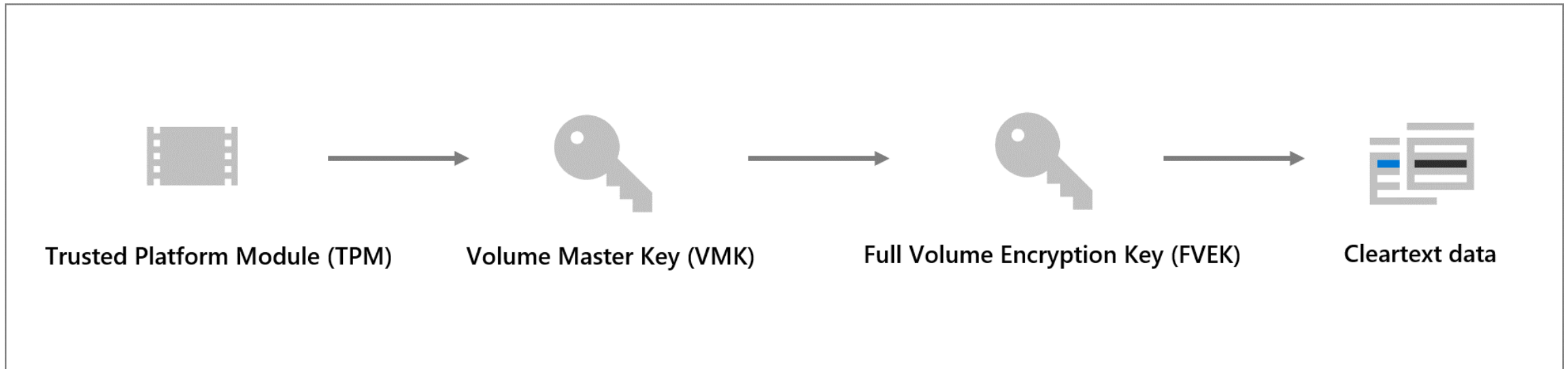
- Encoding plain text into cipher text.
- Decryption requires encryption keys.
- Control access to authorized users or machines only.
- Differentiation between 'data at rest' and 'data in transit'

- Data at rest
- Files saved on computers and mobile devices
- Documents and files saved in SharePoint Online and OneDrive for Business
- Mails saved in Mailboxes in Exchange Online

- Data in transit
- Documents and files accessed in SharePoint Online and OneDrive for Business
- Mails transported between servers
- Shared files and conversations in Teams meetings



# Learn how BitLocker encrypts data-at-rest



- A flow diagram depicting the chain of trust for BitLocker encryption.

# Service encryption in Microsoft 365

Available encryption options:

## Service Encryption, Azure RMS, and S/MIME

- Service Encryption, optionally with Customer Key
  - Encryption of all data saved in a Microsoft 365 tenant.



- Information Rights Management (IRM) with Rights Management Service (Azure RMS)
  - Protection of individual documents, files and emails



- Secure/Multipurpose Internet Mail Extensions (S/MIME):
  - Encryption and digital signing of email messages and attachments only



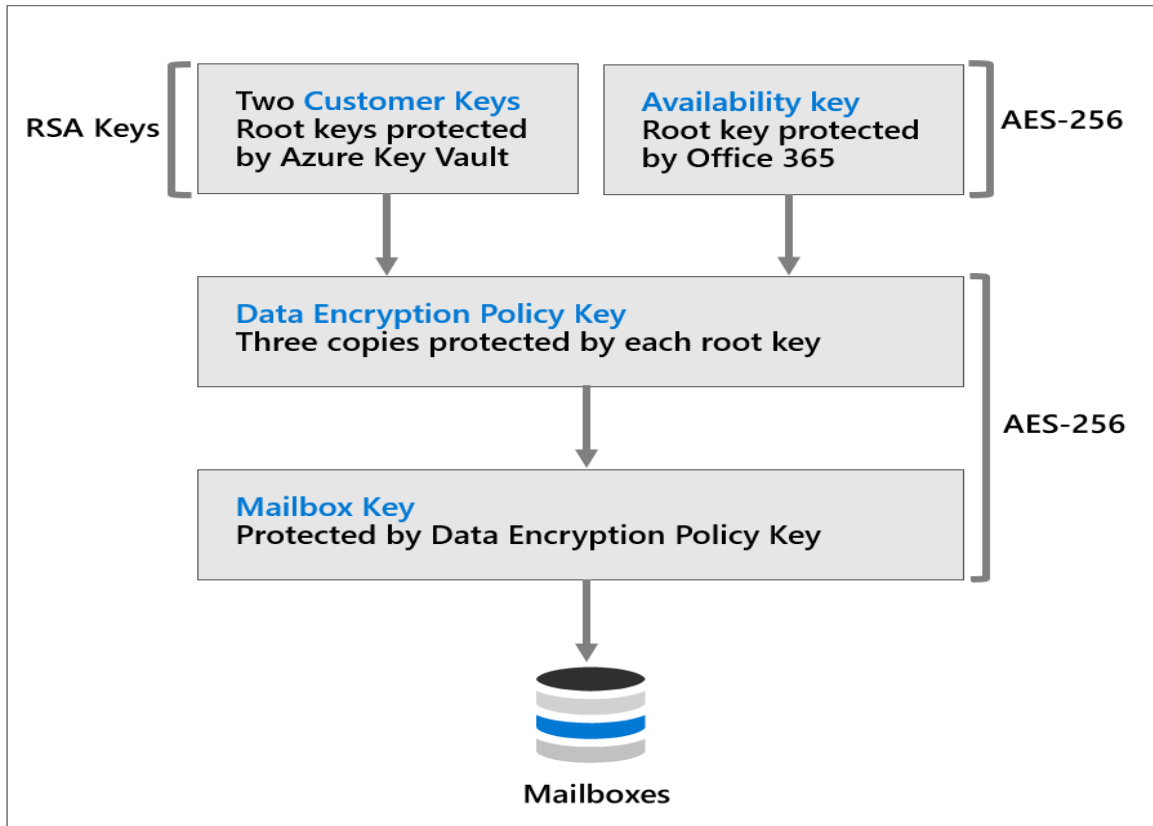
Encryption Key Management:

- Service Encryption - Microsoft managed Keys or Customer Keys
- Azure RMS - Microsoft managed Keys, BYOK, DKE, or HYOK

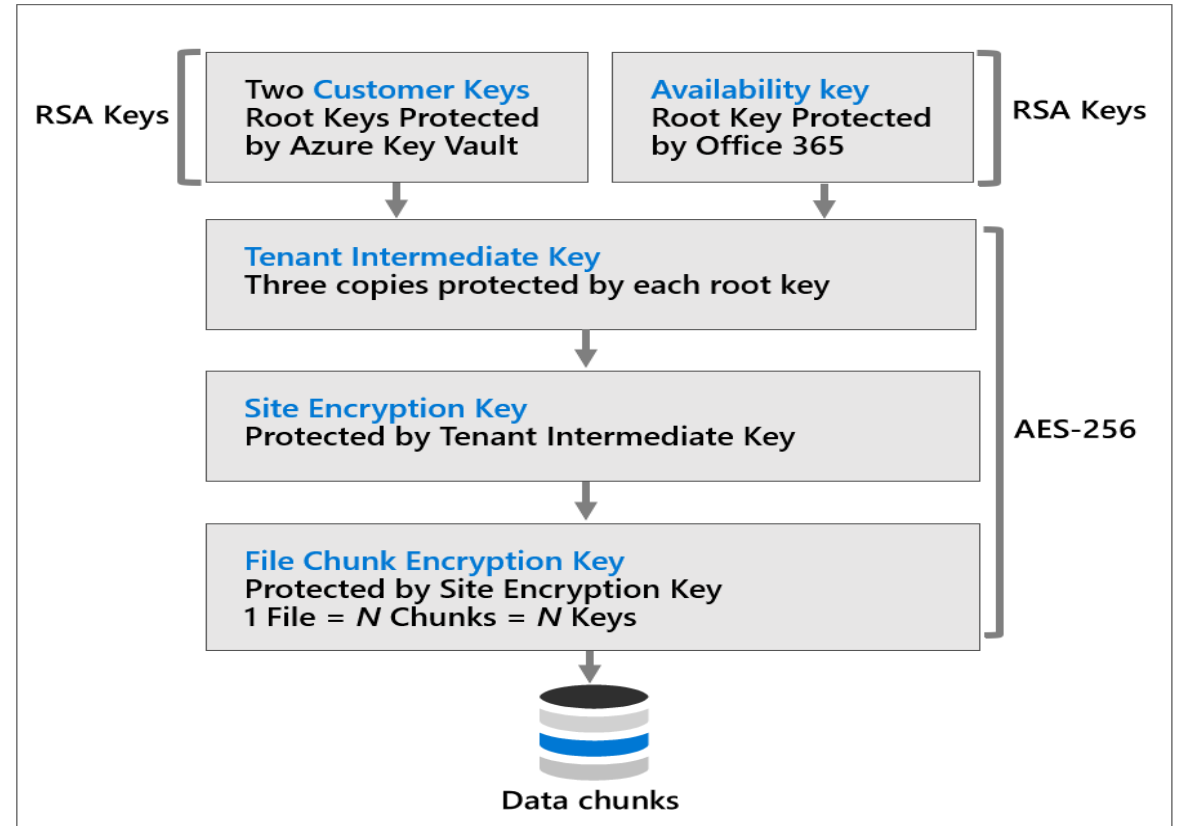
# Customer key management using Customer Key

## Customer Key hierarchy

### Exchange Online



### SharePoint Online, OneDrive for Business, Microsoft Teams files



# Encrypted data in transit

- Data-in-transit scenarios include:



When a client machine communicates with a Microsoft server.

---



When a Microsoft server communicates with another Microsoft server.

---



When a Microsoft server communicates with a non-Microsoft server (for example, Exchange Online delivering email to a third-party email server).

---



# Lesson: Deploy message encryption in Office 365

# Lesson Agenda



Configure Office 365 Message Encryption for end users.



Implement Advanced Office 365 Message Encryption.

# Implement Office 365 Message Encryption

Office 365 Message Encryption (OME) uses IRM and RMS templates

## Default configuration

- Default configuration named “OME Configuration” is available
- Modifications apply to all users
- Customization of OME portal and functionality is possible

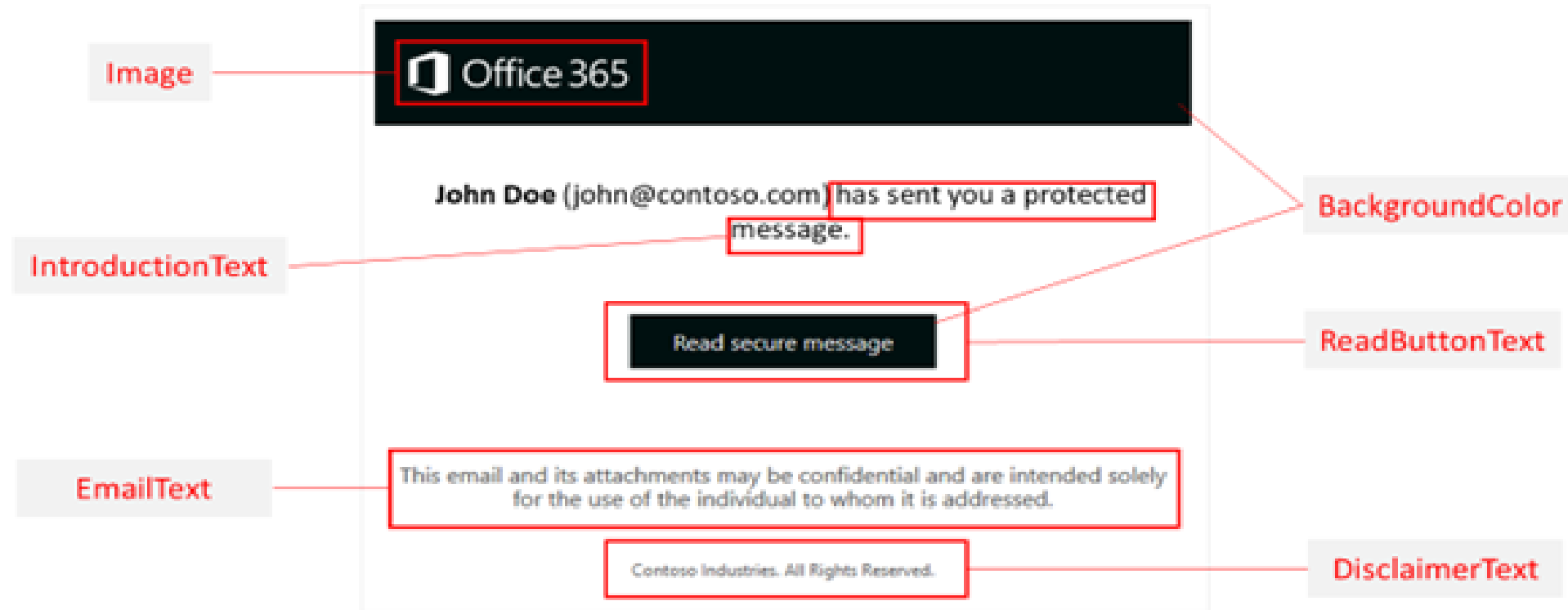
## Branding templates

- Only one branding template is available for all with basic OME

# Implement Office 365 Advanced Message Encryption

## Additional Features

- Multiple branding templates
- Message Expiration added (1 – 730 days)
- Customized templates for different groups of users





# Use Office message encryption templates in mail flow rules

## Configuration via Mail Flow Rules

- Different OME configurations are assigned via mail flow rules
- Possible use cases:
  - Individual departments.
  - Different products.
  - Different geographical regions.
  - Determine whether emails can be revoked.
  - Determine whether emails sent to externals expire after several days.

Demo

# Manage Office 365 message encryption

## **Scenario:**

You will modify the default Office 365 Message Encryption template and create a new branding template. You will then test the OME functionality with their accounts.

# **Data Loss Prevention in Microsoft 365**

# Lesson: Prevent data loss in Microsoft 365

# Lesson Agenda



Discuss the data loss prevention solution and its benefits.



Describe the data loss prevention configuration process.



Explain what users will experience when the solution is implemented.

# Basics of data loss prevention

Each DLP policy contains:

## Where to protect the content

Content is protected in locations like SharePoint Online, Exchange Online, OneDrive for Business accounts, Microsoft Teams chat and channel messages, and Windows 10 devices.

## When and how to protect the content

When and how to protect the content is defined by enforcing rules. A policy contains one or more rules, and each rule consists of conditions and actions at a minimum.



# Identify content to protect

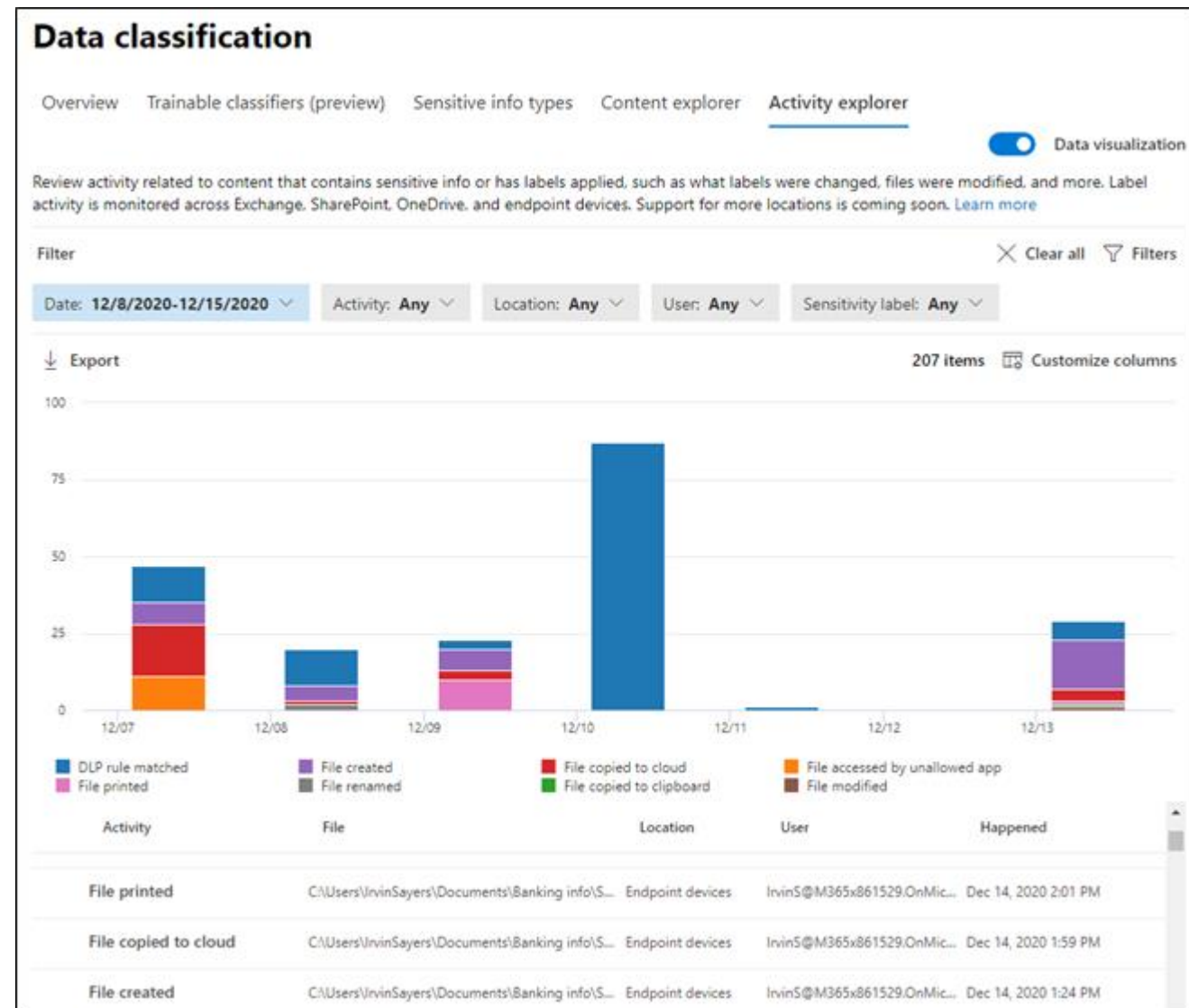
Use the following to identify content:

## Content explorer

Content explorer identifies the email and documents in your organization that contain sensitive information.

## Activity explorer

Activity explorer includes information on activity related to content that contains sensitive information, which can also inform what should be protected by DLP policies. The top portion of the screen includes a histogram of various activities over time, while the bottom portion lists each recorded activity.



# Initiate policy creation workflow

To create a DLP policy go to the **Microsoft 365 compliance center**

## Data loss prevention policy configuration





# Choose the information to protect

DLP policy templates consist of one or more sensitive info types grouped into categories:

- **Financial**
- **Medical and health**
- **Privacy**

**Choose the information to protect**

- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

## Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

Search for specific templates:  All countries or regions:

Categories	Templates	U.K. Financial Data
<input checked="" type="radio"/> Financial	Canada Financial Data	<p>Helps detect the presence of information commonly considered to be financial information in United Kingdom, including information like credit card, account information, and debit card numbers.</p> <p><b>Protect this information:</b></p> <ul style="list-style-type: none"><li>• Credit Card Number</li><li>• EU Debit Card Number</li><li>• SWIFT Code</li></ul>
<input type="radio"/> Medical and health	France Financial Data	
<input type="radio"/> Privacy	Germany Financial D...	
<input type="radio"/> Custom	Israel Financial Data	
	Japan Financial Data	
	PCI Data Security Sta...	
	Saudi Arabia - Anti-...	
	Saudi Arabia Financi...	
	U.K. Financial Data	

# Choose locations to apply the policy

Locations are places or service the DLP policy will apply to:

- **Exchange Online email**
- **SharePoint Online sites**
- **OneDrive for Business accounts**
- **Microsoft Teams chat and channel messages**
- **Windows 10 devices**
- **Third-party apps/services with MCAS**

**Choose locations to apply the policy**

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

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All <a href="#">Choose distribution group</a>	None
<input checked="" type="checkbox"/> On	SharePoint sites	All <a href="#">Choose sites</a>	None
<input checked="" type="checkbox"/> On	OneDrive accounts	All <a href="#">Choose account</a>	None
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All <a href="#">Choose account</a>	None
<input checked="" type="checkbox"/> On	Devices	All <a href="#">Choose user or group</a>	None
<input checked="" type="checkbox"/> On	Microsoft Cloud App Security	All <a href="#">Choose instance</a>	None

# Define policy settings

DLP policy rules include:

## Conditions

Determine what types of information you are looking for, and when to take an action.

## Exceptions

Prevents the application of a rule for content matching the exceptions.

## Actions

When content matches a condition in a rule, you can apply actions to automatically protect the content.

## User notifications

Use notifications to educate your users about DLP policies and help them remain compliant without blocking their work.

## User overrides

Allows the user to override the policy and share the content.

## Incident reports

When a rule is matched, you can send an incident report to your compliance officer (or any people you choose) with details of the event.

## Test or turn on the policy

- Use test mode to gauge impact before policy activation.
- Policy matches will be reported to you in emails or through DLP reports.
- Test mode allows you to activate policy tips without enforcing protective actions.
- Policy tips allow users to flag false positives.
- Configure exceptions to the policy to reduce false positives.

## Manage DLP policies

### **Scenario:**

You are the newly hired Compliance Administrator for Contoso Ltd. tasked to configure the company's Microsoft 365 tenant for data loss prevention. Contoso Ltd. is a company that offers driving instruction in the United States and you need to make sure that sensitive customer information does not leave the organization.

**Lesson: Implement Endpoint data loss prevention**

# Agenda



Prepare your environment for Endpoint DLP



Onboard devices to Endpoint DLP



Configure global Endpoint DLP settings

# Prepare for Endpoint DLP

- Endpoint DLP extends the protection of your DLP policies to Windows 10 devices
- File type limitations exists  
Unsupported file types can create opportunities for data loss
- Management of Endpoint DLP policies can be completed by a Compliance Admin
- Devices are monitored by Microsoft Defender
- Devices onboarded for Defender are automatically also onboarded for Endpoint DLP



# Prepare for Endpoint DLP (continued)

## Endpoint DLP only protects data on Endpoints

- All Endpoint DLP policies end at the border of the device
- Policies allow you to restrict:
  - Uploading to cloud service domains
  - Access by unallowed browsers
  - Copying to the clipboard from protected items
  - Copying protected items to USB removable media
  - Copying to network shares
  - Access by unallowed apps
  - Printing protected items

The screenshot shows the 'Create policy' page in the Microsoft 365 DLP console. The main heading is 'Customize access and override settings'. Below this, there is a paragraph explaining that by default, users are blocked from sending email and Teams chats containing protected content, but users can be allowed to share files. Two radio buttons are present: 'Restrict access or encrypt the content in Microsoft 365 locations' (unchecked) and 'Block users from accessing shared SharePoint, OneDrive, and Teams content' (checked). Below this, a section titled 'Audit or restrict activities on Windows devices' is checked. It lists several activities with checkboxes and dropdown menus for their enforcement: 'Upload to cloud service domains or access by unallowed browsers' (checked, dropdown: Block), 'Copy to clipboard' (checked, dropdown: Audit only), 'Copy to a USB removable media' (checked, dropdown: Block with ov...), 'Copy to a network share' (checked, dropdown: Audit only), 'Access by unallowed apps' (checked, dropdown: Audit only), and 'Print' (checked, dropdown: Audit only). Each activity has an information icon (i) to its right.

# Onboard devices for Endpoint DLP

The onboarding feature is turned off by default and needs to be turned on first

## **Local Script**

Use a local script to onboard a maximum of 10 devices for testing purposes

## **Group Policy**

Use this method if you are looking to mass onboard devices for Endpoint DLP and you do not plan on using Configuration Manager or an MDM solution.

## **Configuration Manager**

Use this method if you are looking to mass onboard devices for Endpoint DLP if you do not plan on using an MDM solution.

## **MDM/Intune**

Use this method if you are looking to mass onboard devices for Endpoint DLP and do not plan on using Configuration Manager.

## **VDI Scripts**

Use this method if you need to onboard VDI clients. The provided scripts work for more than 10 devices.

# Configure global Endpoint DLP settings

Endpoint DLP settings create a framework in which Endpoint DLP policies work

## File path exclusions:

- Are applied to all Endpoint DLP policies
- Allow you to limit where your policies are in effect

## Unallowed apps:

- Are applied when a policy blocks unallowed apps
- Allow you to limit where you can work with protected files

## Unallowed Browsers/Service Domains:

- Are applied when a policy blocks unallowed browsers
- Allow you to limit where you can share protected files

# Manage Endpoint DLP

## **Scenario:**

You are the newly hired Compliance Administrator for Contoso Ltd. tasked to configure the company's Microsoft 365 tenant for data loss prevention. Contoso Ltd. is a company offering driving instruction in the United States and you need to make sure that sensitive customer information does not leave the organization. For this reason, you decide to not only implement Microsoft 365 DLP policies but extend this protection to devices in your organization.

# Lesson: Configure DLP policies for Microsoft Cloud App Security and Power Platform

# Agenda



Configure data loss prevention policy and rule priorities



Implement DLP policies in test mode



Configure Data loss prevention policies in Power Platform



Integrate DLP Policies into MCAS for advanced functionality

# Configure DLP policies for Microsoft Power Platform

- Microsoft Power Platform DLP policies restrict communication between connectors.
- Policies can be configured on a tenant or environment level.
- Connectors can be sorted into three groups and only reside in one at a time:
  - Business
  - Non-business
  - Blocked
- Certain connectors cannot be sorted into the blocked group
- Connectors can only communicate with other connectors in their group

# Combine DLP with Microsoft Cloud App Security

Create file policies in MCAS and use the Data classification service:

- You need to enable file monitoring
- File policies allow you more granular control over Microsoft cloud apps

Create DLP policies in the Compliance Center and select MCAS as a location:

- DLP policies monitor third party apps you connected to MCAS (Box, Dropbox, Salesforce, etc.)
- Protective actions are limited by the API of the third-party app



# Configure file policies in Microsoft Cloud App Security



File policies can use the MCAS DLP engine or the same Data Classification Services as DLP policies

---



You can configure real-time alerts or review alerts via reports

---



File policies are configured in the Microsoft Cloud App Security portal

---



There is no test mode for file policies, actions will be applied as soon as the policy exists

---



Use the preview functions to see the files your policy would match if you saved it

# Manage DLP violations in Microsoft Cloud App Security

- Violations of file policies only show up in the MCAS dashboard and the individual policy matches overview.
  - Use the policy overview to review matches of the policy and fine tune your filters.
  - Get a history of past matches to see where your policy had an effect.
  - Use the quarantine view to see files that have been quarantined because of governance actions.
- Modify file policy filters and review the effects your policy changes have on your environment before committing to them by using the preview function.

# Lesson: Manage DLP policies and reports in Microsoft 365

# Agenda



Review and analyze DLP reports



Manage permissions for DLP reports



Identify and mitigate DLP policy violations



Configure DLP for policy precedence

# Manage DLP policy alerts

## DLP Reports

Provides an overview of DLP violations

Contains DLP policy matches, DLP incidents, and DLP false positives and user overrides reports

Used to fine tune your policies and identify problematic configurations or business processes

Can take up to 24h to update

## DLP Alerts Dashboard

Provides a deeper insight into DLP violations

Displays individual alerts

Can aggregate alerts to spot patterns more easily

## MCAS Dashboard

Displays alerts of MCAS file policies

Shows alerts of all your MCAS DLP policies

Drill down to specific policies and review only a single policy's matches

Provides a match history and quarantine views

# View DLP reports

- DLP reports can be broken down by affected service, enforced action, or applied policy.
- Use filters to restrict the displayed information to specific policies and time slots.

The **DLP policy matches** report is used for identifying matches with specific rules and fine tuning DLP policies, to increase the accuracy of the policies matching a company's individual data shared on a regular basis.

The **DLP incidents** report is used for identifying specific pieces of content that are problematic for your DLP policies and to identify groups of items that may require additional protective actions.

The **DLP false positives and user overrides** report should be used to identify the accuracy of the existing DLP policies, to be able to react fast when suddenly large numbers of faulty matches occur.

# Manage permissions for DLP reports

- Any role group with the View-Only DLP Compliance Management role can view DLP reports
- The Security Reader (Azure AD) role group can view all Security and Compliance related topics
- The Security Reader (Exchange) role group is synchronized with the Security Reader (Azure AD) role group
- Use the Security & Compliance Center to assign permissions
- Exchange role groups can sound similar to Azure AD role groups but have different scopes

# Configure DLP for policy precedence



Policies and rules are processed in priority order

---



Only the highest priority rule of the highest priority policy is applied

---



More restrictive rules/policies should be prioritized above less restrictive rules/policies

---



All processed matches are logged, even if the rule/policy is not applied



# Manage and respond to DLP policy violations

- DLP policies do not make decisions about the validity of a policy violation.
  - Compliance officers have the task of monitoring reports and need to decide if violations require technical or organizational actions.
  - Compliance admins should be aware of escalation processes and contacts in other departments to coordinate a unified response to violations.
- Use Exclusions in your DLP rules to limit the amount of false positives you get.
- Allow users to override the protective actions of specific DLP policies if you identified legitimate use cases in past responses to policy violations.

# **Information Governance in Microsoft 365**

# Lesson: Govern information in Microsoft 365

# Agenda



List the customer scenarios the information governance solution addresses.



Explain what users will experience when the solution is implemented.

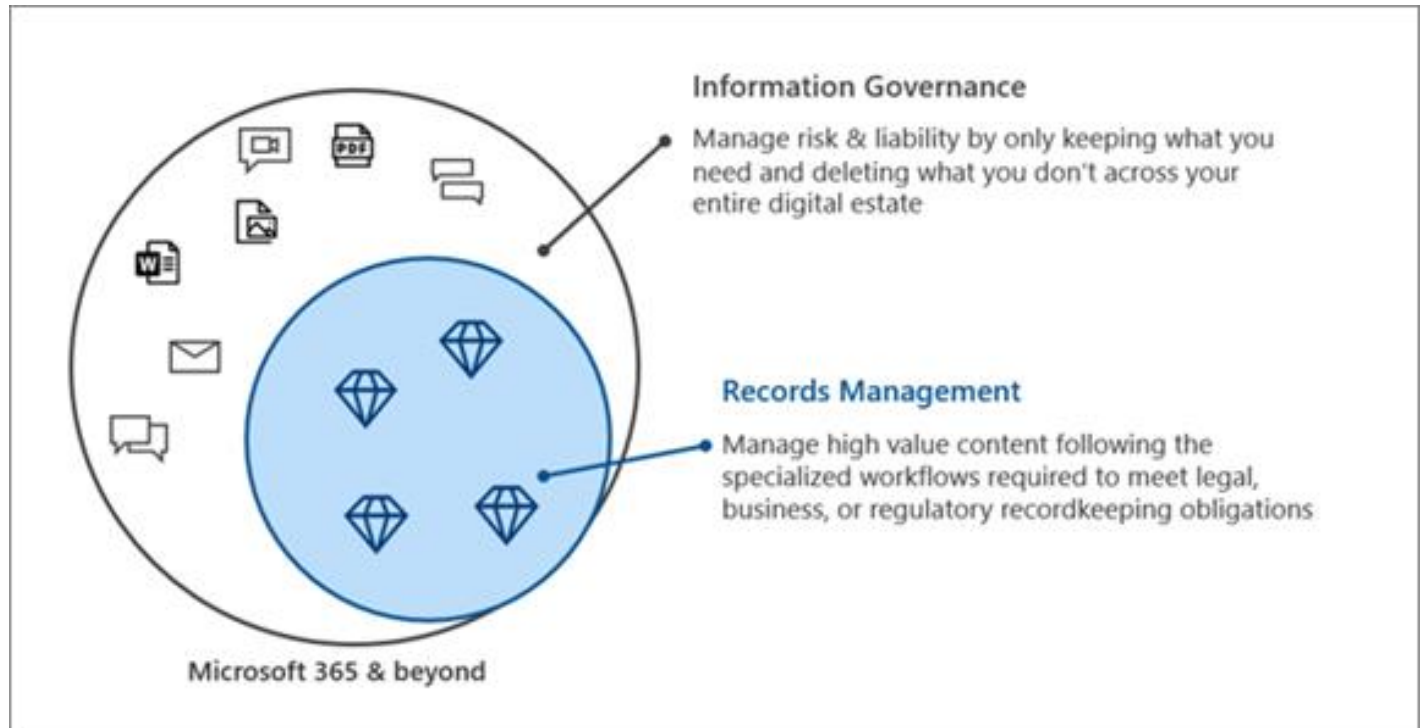


Articulate deployment and adoption best practices.

# Basics of information governance

## Retention is a part of Microsoft Information Governance in Microsoft 365

- Information Governance manages risk & liability by retaining or deleting company data across the entire digital estate.
- Different time periods for different retention requirements.
- Retention is not a backup.



# Basics of information governance (continued)

## Retention Strategy

- The goal of a retention strategy is to fulfill the requirements of laws, internal compliance policies and business regulations.
- Creating a strategy includes several steps:
  1. Know the data for an organization.
  2. Know the requirements an organization must fulfill.
  3. Create a retention plan.

Category	Examples
Personal data	Name, e-mail address, telephone number
Sensitive personal data	HR data, Health data, ethical origin, Union membership
Product data	Brand, pictures, tenders, product descriptions, internal IP
Authentication data	System generated data like username, MAC address, IP-address
Log files with system accesses	License data, log files, Telemetry, diagnostic data

# Configure retention policies and labels

## Differences between retention policies and retention labels

- Retention Policies are focused on service locations.
- Retention Labels are focused on individual items.
  - Retention labels are created for certain kinds of business data.
  - Label policies are used to publish retention labels.

Type	Based on	Travel with the document	Data lifecycle	examples
<b>Retention Policy</b>	Location, product	no	yes	Teams Chat, Junk Folder, SharePoint Site
<b>Retention Label</b>	Single file or email, library, or list	yes	yes, better	Email, document in a library

# Configure retention policies and labels (continued)

## Retention period calculation

- Retention label count starts when a label is applied.
- Several legal and regulatory requirements start at the end of a year.
- Exact requirements must be known to fulfil them with required accuracy.
- A combination of retention labels and retention policies is required.

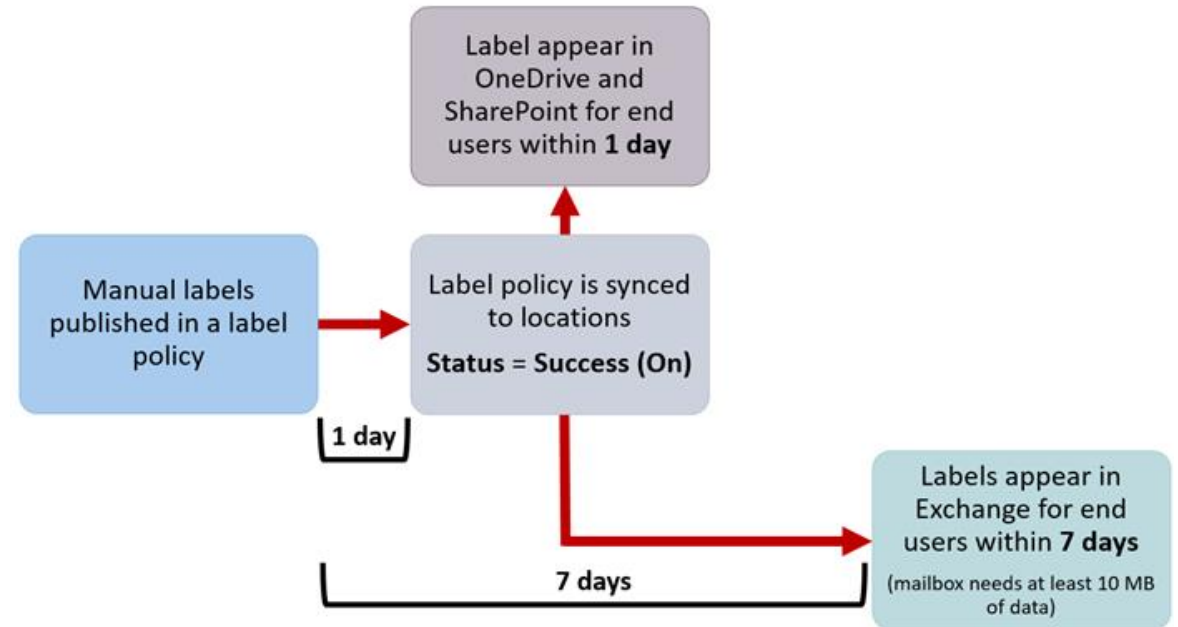
Document	Label	Method	Deletion	False
Invoice	6 years + delete	Last modified on 1. May 2020	Delete after 6 years in May 2026	The file will be deleted 6 months too early.
Invoice	7 years + delete	Last modified on 1. May 2020	Delete after 7 years in May 2027	The file will be deleted 5 months later. But it's stored for the full time to fulfill the legal requirement.



# Configure manual retention label policies

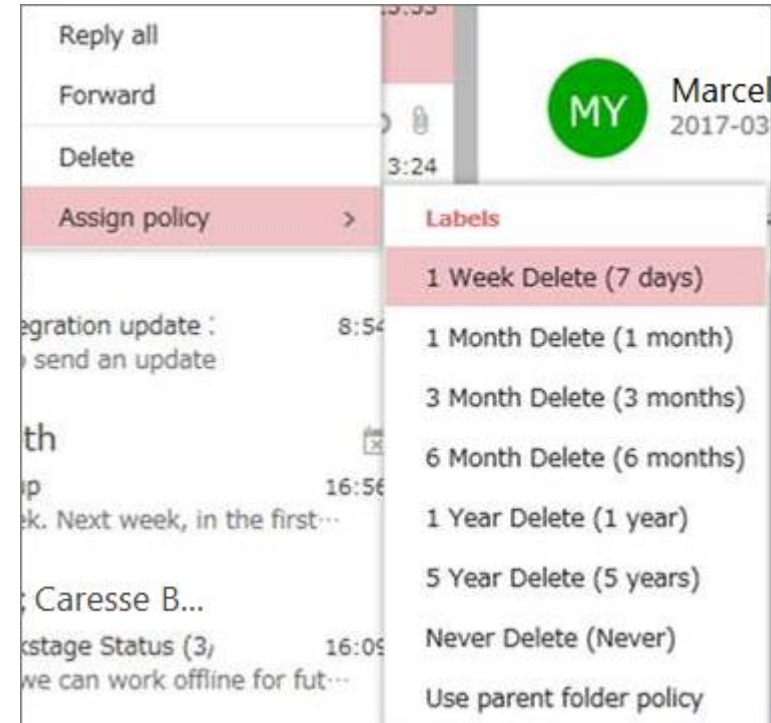
Published labels will be available at the published location to be assigned manually.

- These locations include:
  - Exchange mail
  - SharePoint sites
  - OneDrive accounts
  - Microsoft 365 Groups
- Exchange public folders, Skype for Business, Teams, and Yammer messages **do not** support retention labels.



# Configure manual retention label policies (continued)

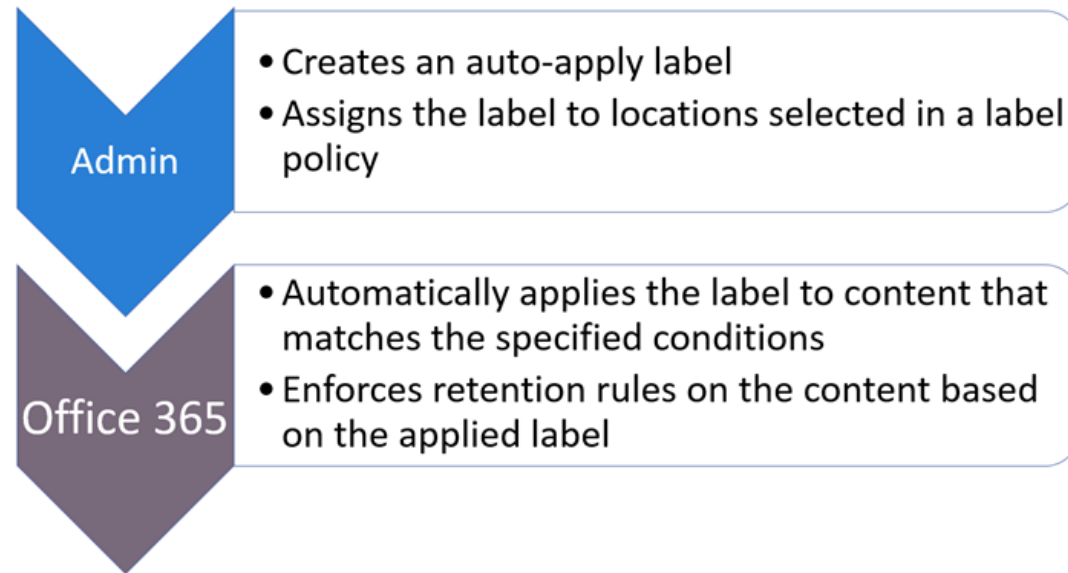
- Within Outlook a retention label can be assigned to an email through the *assign policy* ribbon
- The retention label is then visible within the email
- You can set the default retention label for an entire Outlook folder through the folder's properties
- Within SharePoint you can set the retention label to a file through the file/folder/document libraries properties
- Retention labels for Onedrive can be set through the web version through the file properties



# Configure auto-apply retention label policies

## Auto-apply labels can apply retention labels automatically to:

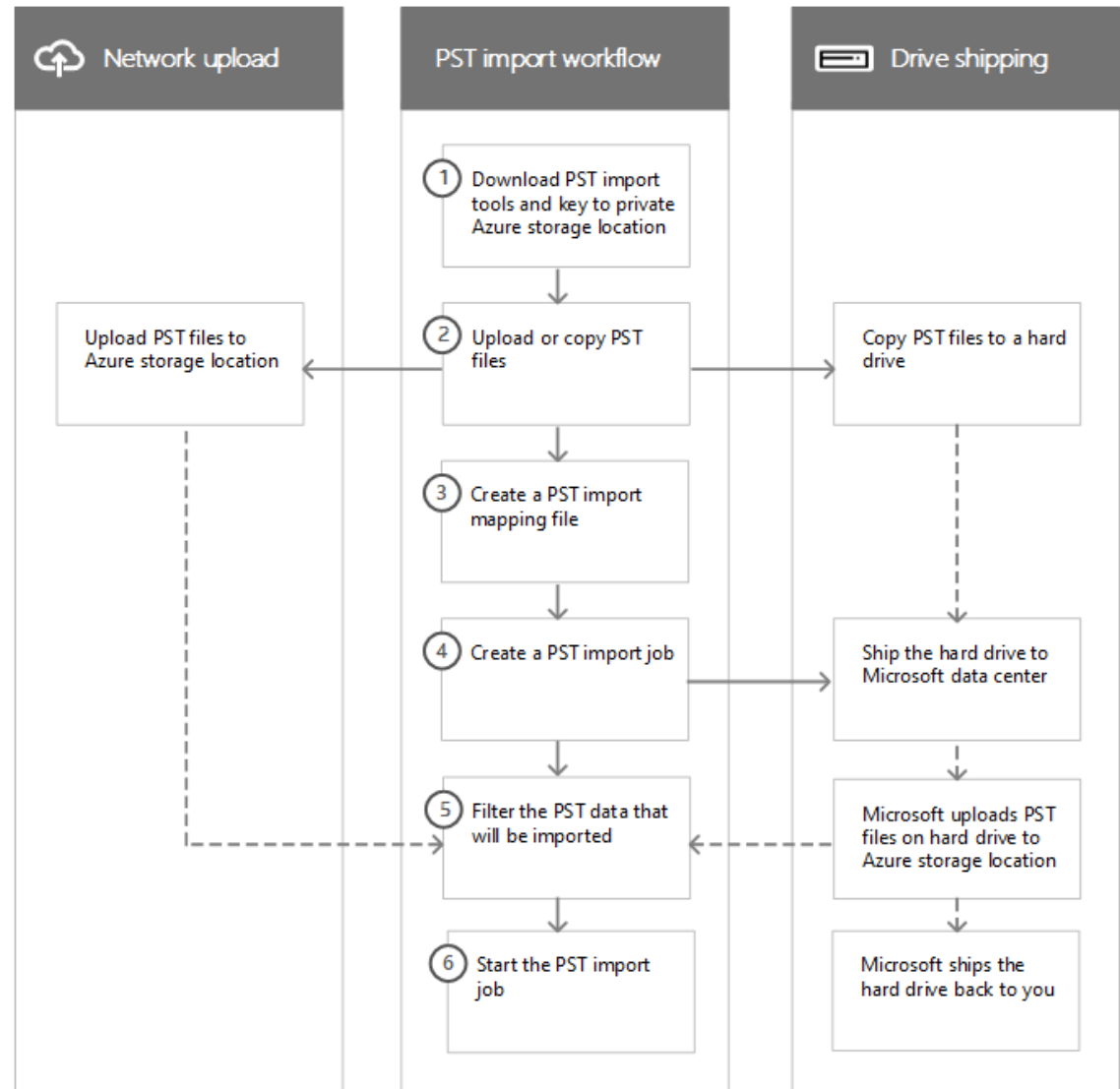
- Content that contains sensitive information that match sensitivity templates.
- Content that contains specific words or phrases, or properties. This is specified by the Keyword query language.
- Or trainable classifiers such as source code, offensive language or resumes.



# Import data for information governance

There are two ways to import PST files to Office 365:

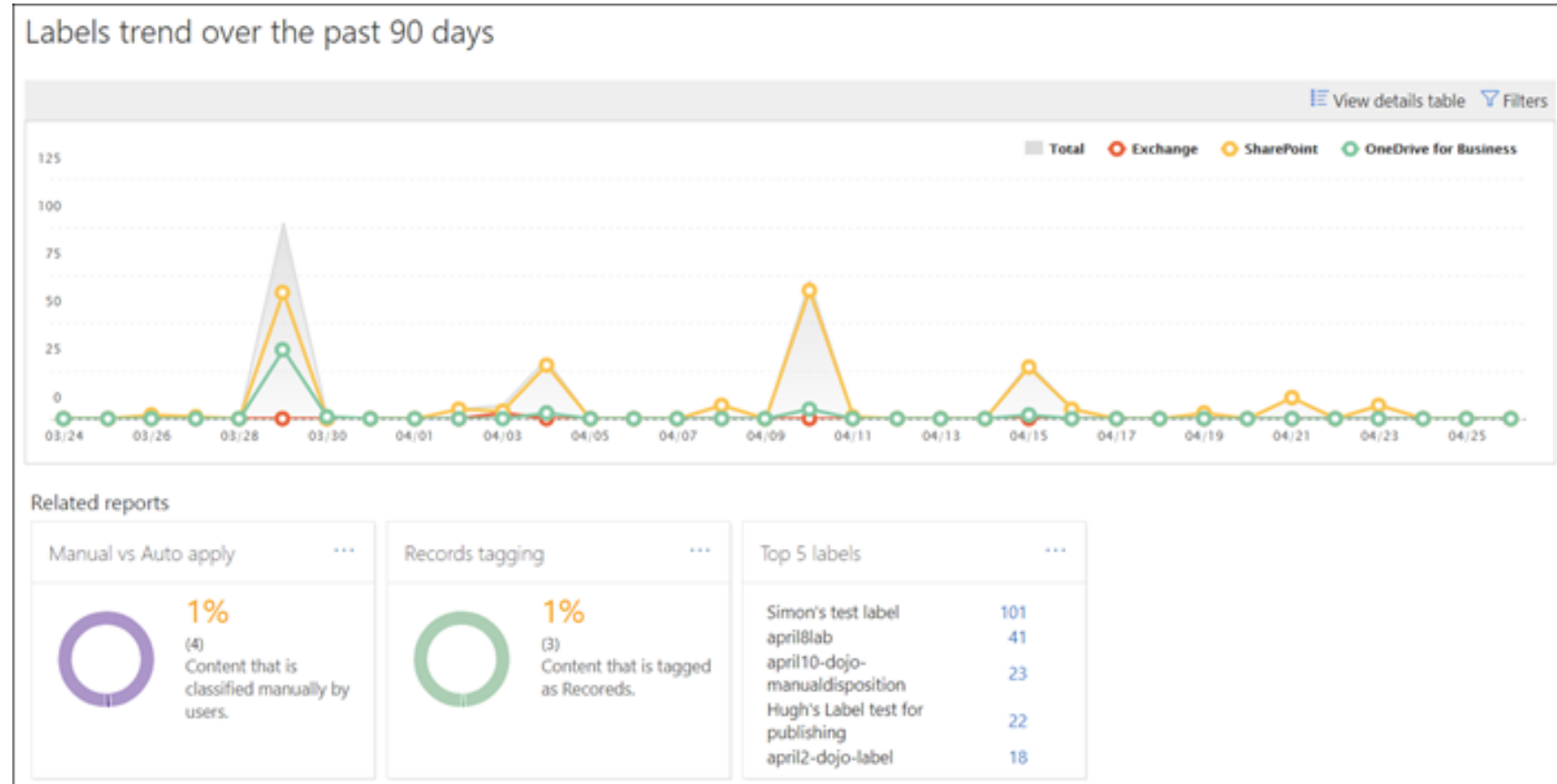
- Network upload
- Drive shipping



# Manage, monitor, and remediate information governance

## Data governance cards on the Data classification page:

- Top sensitive info types
- Top retention labels applied to content
- Locations where retention labels are applied



# Lesson: Manage data retention in Microsoft 365 workloads

# Agenda



Describe the retention features in Microsoft 365 workloads.



Configure retention settings in Microsoft Teams and SharePoint Online.



Recover content protected by retention settings.



Implement retention for Exchange Mailbox items.



Apply mailbox holds on Exchange Mailboxes.



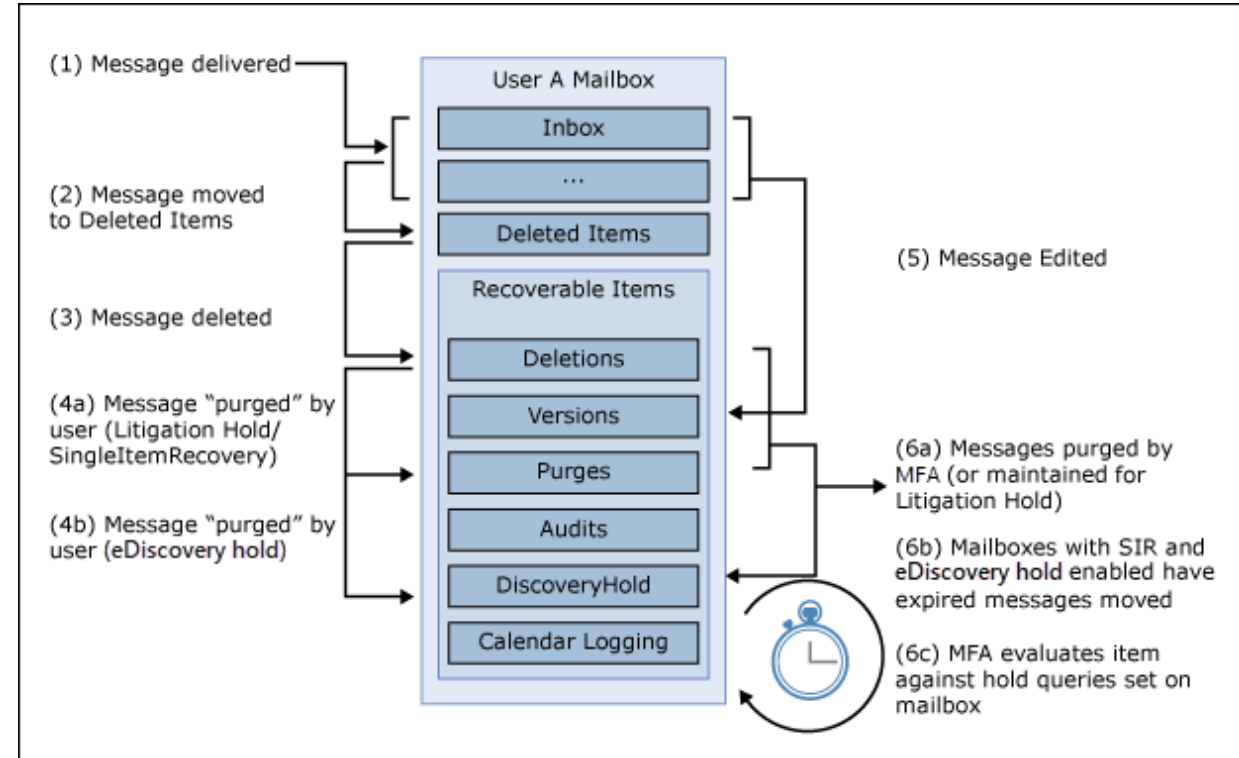
Regain protected items from Exchange Mailboxes.

# Explain retention in Exchange Online

## Hidden Recoverable Items Folders

- Not visible for users in mailboxes.
- Contains deleted mail messages and versions.
- Processed by Managed Folder Assistant (MFA).
- Access possible via
  - eDiscovery cases
  - Compliance Searches

Administrators must consider legal restrictions when accessing user mailboxes in some instances.

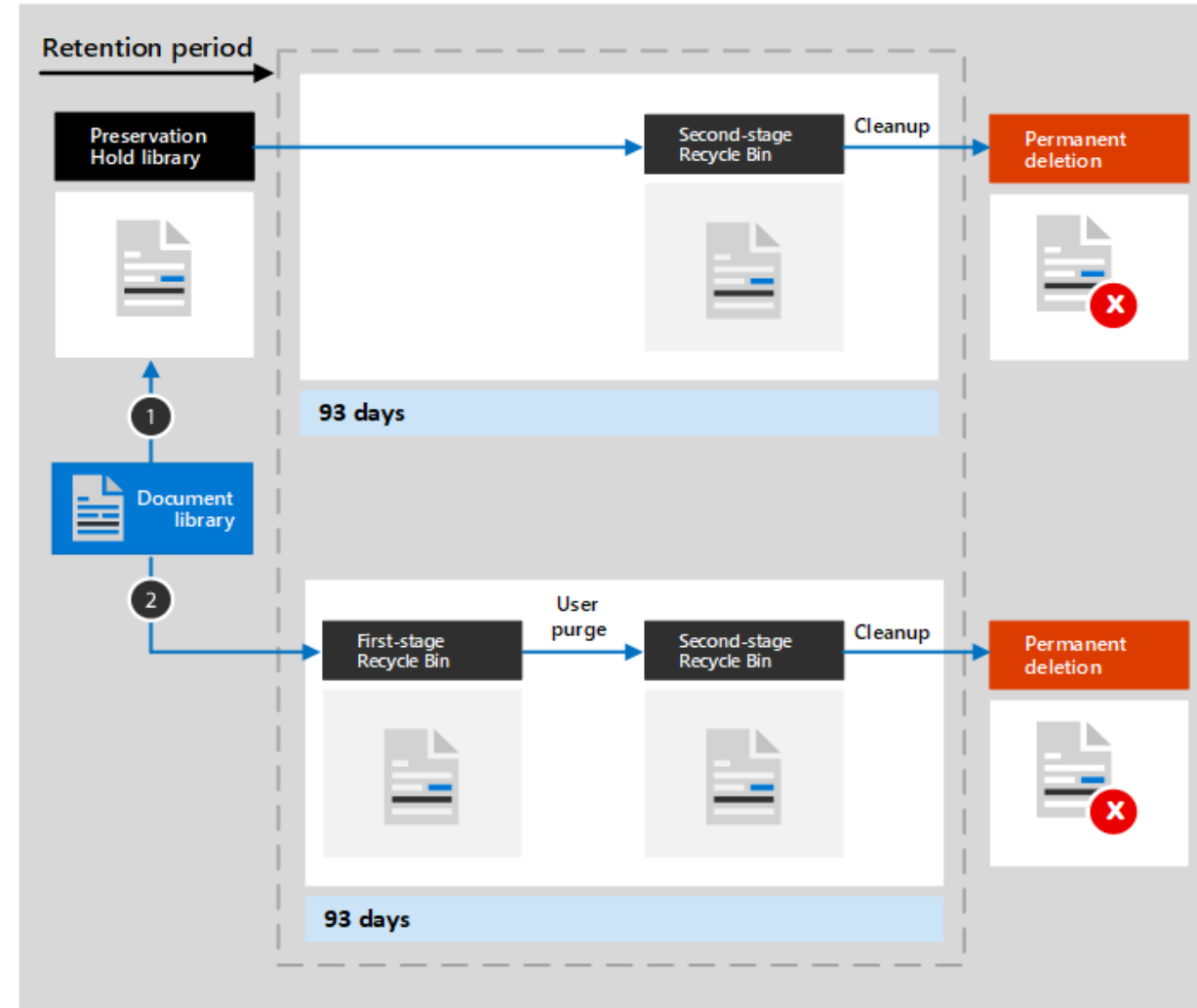




# Explain retention in SharePoint Online and OneDrive for Business

## Preservation Hold Library

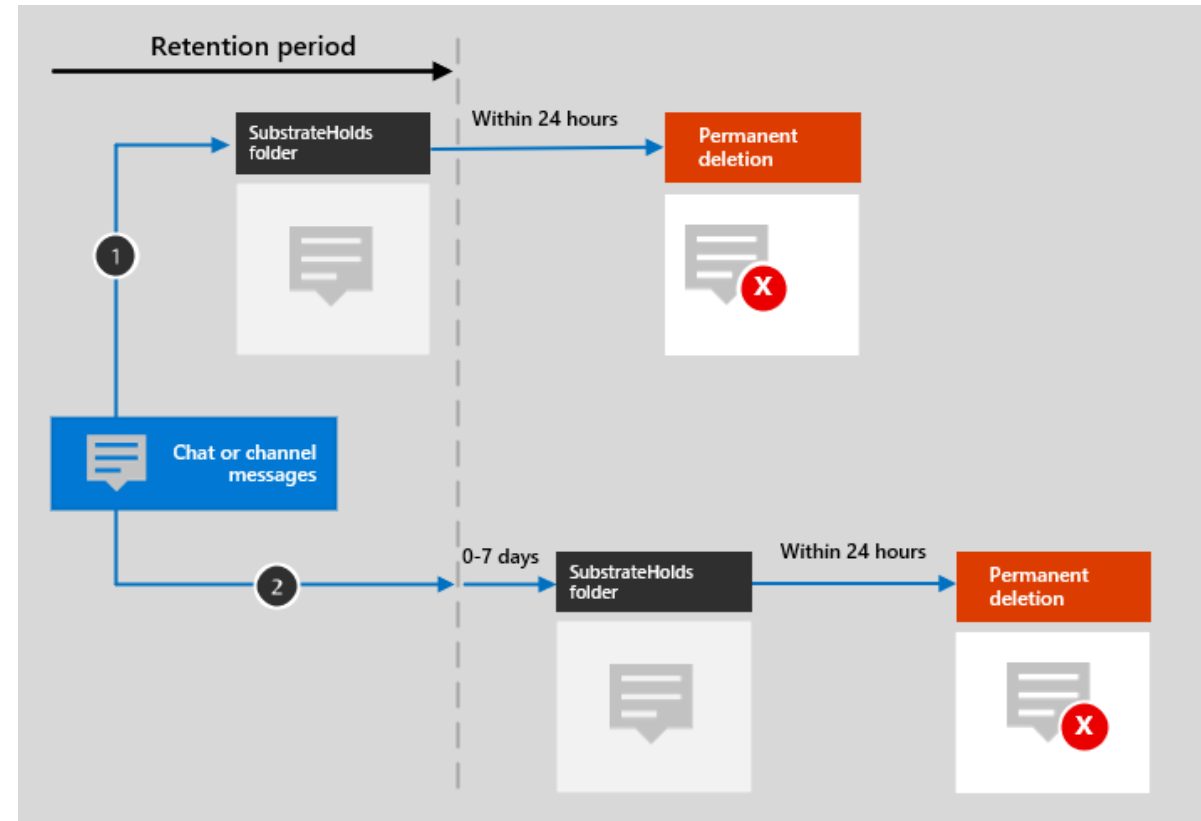
- Site specific document libraries
- Used to preserve documents and versions
- Can be accessed by administrators



# Explain retention in Microsoft Teams

## Azure Cosmos DB to SubstrateHolds

- Compliance copy of data into mailboxes.
- Hidden folder in folder structure.
- Administrators must know storage locations to configure correct retention features.



# Recover content in Microsoft 365 workloads

## Recovery options for users and administrators

- Users can recover documents and files in OneDrive via their recycle bin.
- Users can restore items on SharePoint Online document libraries via the recycle bin.
- Users can restore versions in the SharePoint Online and OneDrive for Business portal.
- Users can restore versions via Office Online or via Microsoft 365 apps for enterprise.
- Users can restore their entire OneDrive for Business content.
- Administrators can access the preservation hold libraries and recover data.

# Implement retention policies and tags in Microsoft Exchange

## Messaging records management (MRM)

- Former feature for retention in Exchange
- Used for archiving of mailbox content
- Consists of different features:
  - **Retention policies** to publish retention tags to use.
  - **Retention policy tags (RPTs)** for default folders.
  - **Default policy tags (DPTs)** for all untagged items.
  - **Personal tags** for manual assignment.
- Mailbox Folder Assistant (MFA) processes retention tag actions.

## Archive Mailboxes

- Additional mailbox for archiving.
- Retention tags move items to archive.

# Apply mailbox holds in Microsoft Exchange

## Mailbox Holds target Exchange Mailboxes

- Protect content of Exchange mailboxes against deletion.
- Two types of mailbox holds available:
  - Litigation Holds set on a mailbox level to protect all content from deletion.
  - eDiscovery Holds created in cases to prevent mailbox content matching search criteria from deletion.

# Recover content in Microsoft Exchange

## Exchange Mailbox content recovery with eDiscovery cases

- Recovery of content from active and inactive mailboxes.
- Results can be previewed and exported in .pst files.
- Different eDiscovery permissions required for case creation, preview and export.

## Configure retention labels

### **Scenario:**

Your organization is based in Texas and wants to implement retention policies to adhere to state laws which stipulate that records may be deleted after three years without constituting a violation.

# Lesson: Manage records in Microsoft 365



# Agenda



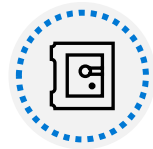
Explain the records management solution and its benefits.



Describe the records management configuration process.



Explain what users will experience when the solution is implemented.



Articulate deployment and adoption best practices.

# Basics of records management

A record is a document or other electronic or physical entity in an organization that serves as evidence of an activity or transaction performed by the organization and requires retention for some time period.

- Different actions that possibly needs to be prevented:
  - change the assigned Retention Label of an item
  - change of the content of an item or it's metadata
  - deletion of a file or remove a retention label from a file
  - moving a file between containers (SharePoint libraries for example)
- Four steps to plan and decide:
  - Decide to add a Record to a label or not
  - Decide to add a Record or a Regulatory Record to a label
  - Configure the Record to a label
  - Decide to have an auto labeling functionality and configure it

# Import a file plan

File plans group the creation of labels, auto-apply label policies and additional metadata tags together.

---

A file plan can help you manage how to dispose of files after the retention period


---

Export file plans as CSV-files and import them into other tenants

---

Use trainable classifiers to identify content it should match

When ready, simply upload the completed plan to Microsoft **Export** then publish or auto-apply

+ Create a label    Publish labels    Import    Export    Refresh

# Configure retention labels

## Retention Labels used for Records Management.

- Activation of records management via PowerShell required.
- Different options available to configure retention labels after activation.

Option	Use to..
<b>Without a Record</b>	Does not add a record to a retention label.
<b>With a Record</b>	A simple record on a retention label restricts options for users to modify labeled items.
<b>With a Regulatory Record</b>	A regulatory record restricts options for users to modify labeled items more strictly. A warning will be displayed when a regulatory record is created and when the retention label will be applied to a file.

# Configure event driven retention

## Building blocks of event-driven retention

**Event Types** group up labels under one banner (e.g. Product lifetime)

---

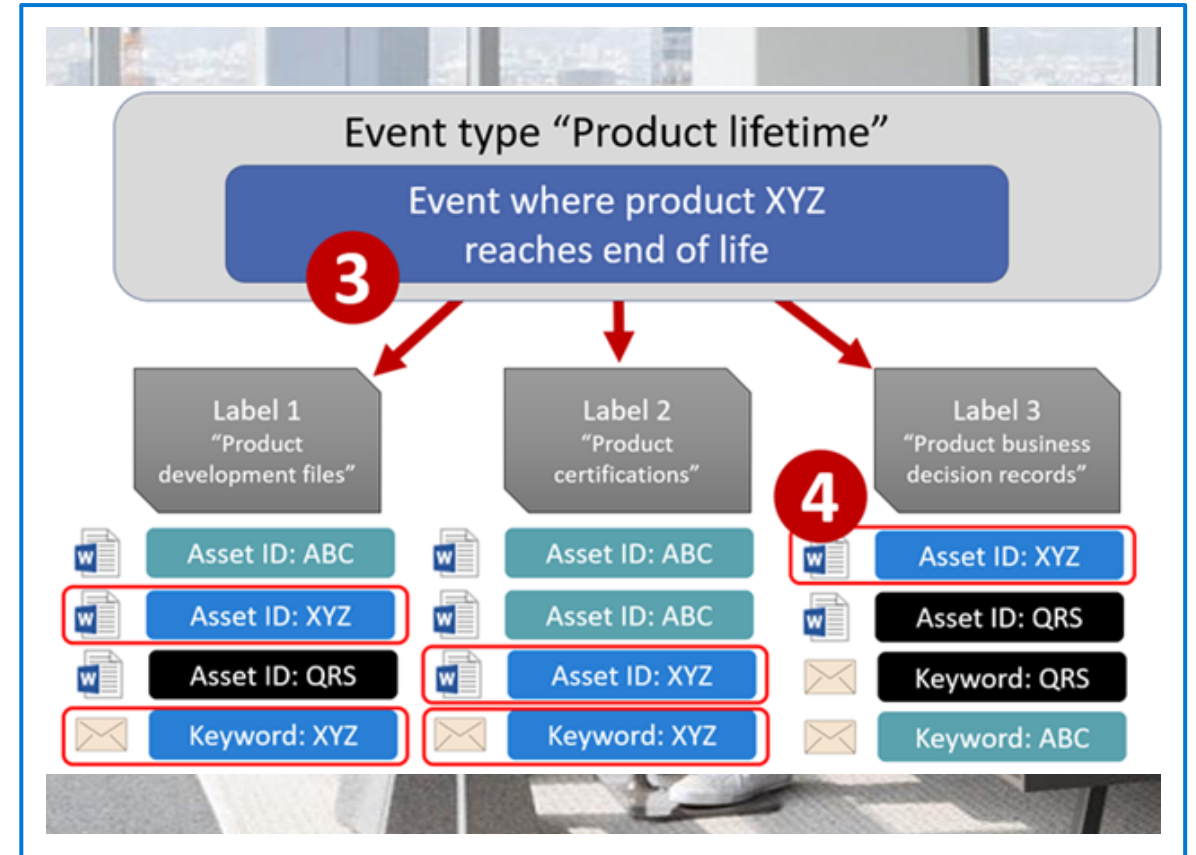
**Labels** are added to content, but the retention period does not start immediately.

---

**Asset IDs** are unique to each product and have to be assigned by users.

---

**Events** can be triggered to start the retention period for all content containing the specified Asset IDs and the applied labels of the event type you selected.



# Configure event driven retention (continued)

**1**

Create labels and decide if you want your labels to mark records or even regulatory records

---

**2**

Use the file plan to publish your labels

---

**3**

Create event types specific to your retention strategy

---

**4**

Trigger events for your event types when your retention strategy calls for them

## Demo

# Configure Records Management

### **Scenario:**

Regulatory requirements for your organization include having a definitive copy of the employee provided health insurance information available when your company discusses the insurance costs. You are tasked with making sure the records are kept.