Microsoft

SC-900

Learning path 4:

Describe the capabilities of Microsoft compliance solutions

SC-900 Course Agenda

Learning Path 1 – Describe the concepts of Security, Compliance, and Identity

Learning Path 2 – Describe the capabilities of Microsoft Entra ID

Learning Path 3 – Describe the capabilities of Microsoft Security Solutions

Learning Path 4 – Describe the capabilities of Microsoft Compliance Solutions

Learning path agenda

- Describe Microsoft's Service Trust portal and privacy capabilities.
- Describe the compliance management capabilities in Microsoft Purview.
- Describe information protection, data life cycle management, and data governance capabilities in Microsoft Purview.
- Describe insider risk capabilities in Microsoft Purview.
- Describe eDiscovery and audit capabilities in Microsoft Purview.

Describe Microsoft’s Service Trust portal and privacy capabilities

Module 1 introduction

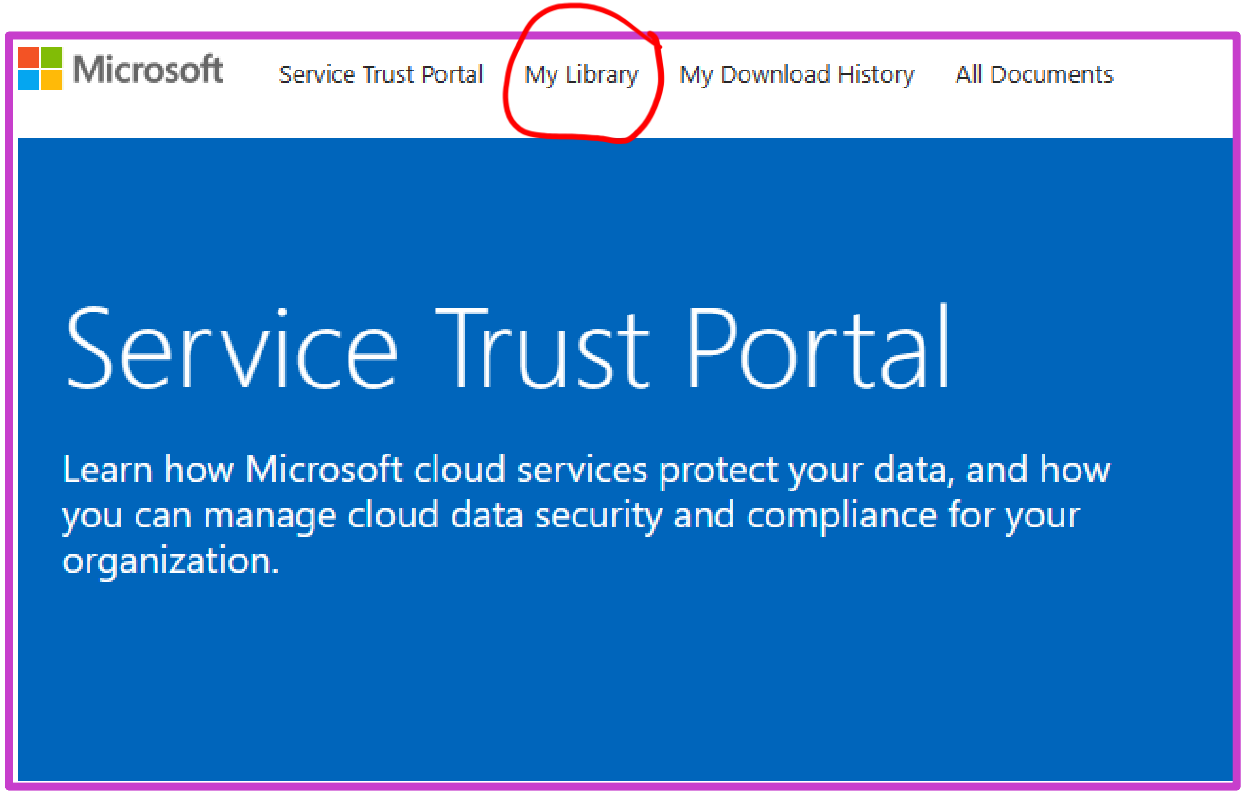
After completing this module, you should be able to:

1. Describe the offerings of the Service Trust Portal.
2. Describe Microsoft's privacy principles.
3. Describe Microsoft Priva.

Microsoft Service Trust Portal

Microsoft's site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services.

- Certifications, regulations and standards.
- Reports, white papers and artifacts.
- Industry and regional resources.
- Resources for your organization.



Service Trust Portal

Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

Microsoft’s privacy principles

1 **Control:** Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.

2 **Transparency:** Being transparent about data collection and use so that everyone can make informed decisions.

3 **Security:** Protecting the data that’s entrusted to Microsoft by using strong security and encryption.

4 **Strong legal protections:** Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

5 **No content-based targeting:** Not using email, chat, files, or other personal content to target advertising.

6 **Benefits to you:** When Microsoft does collect data, it’s used to benefit you, the customer, and to make your experiences better.

Module 2: Describe the compliance management capabilities in Microsoft Purview

Module 2 introduction

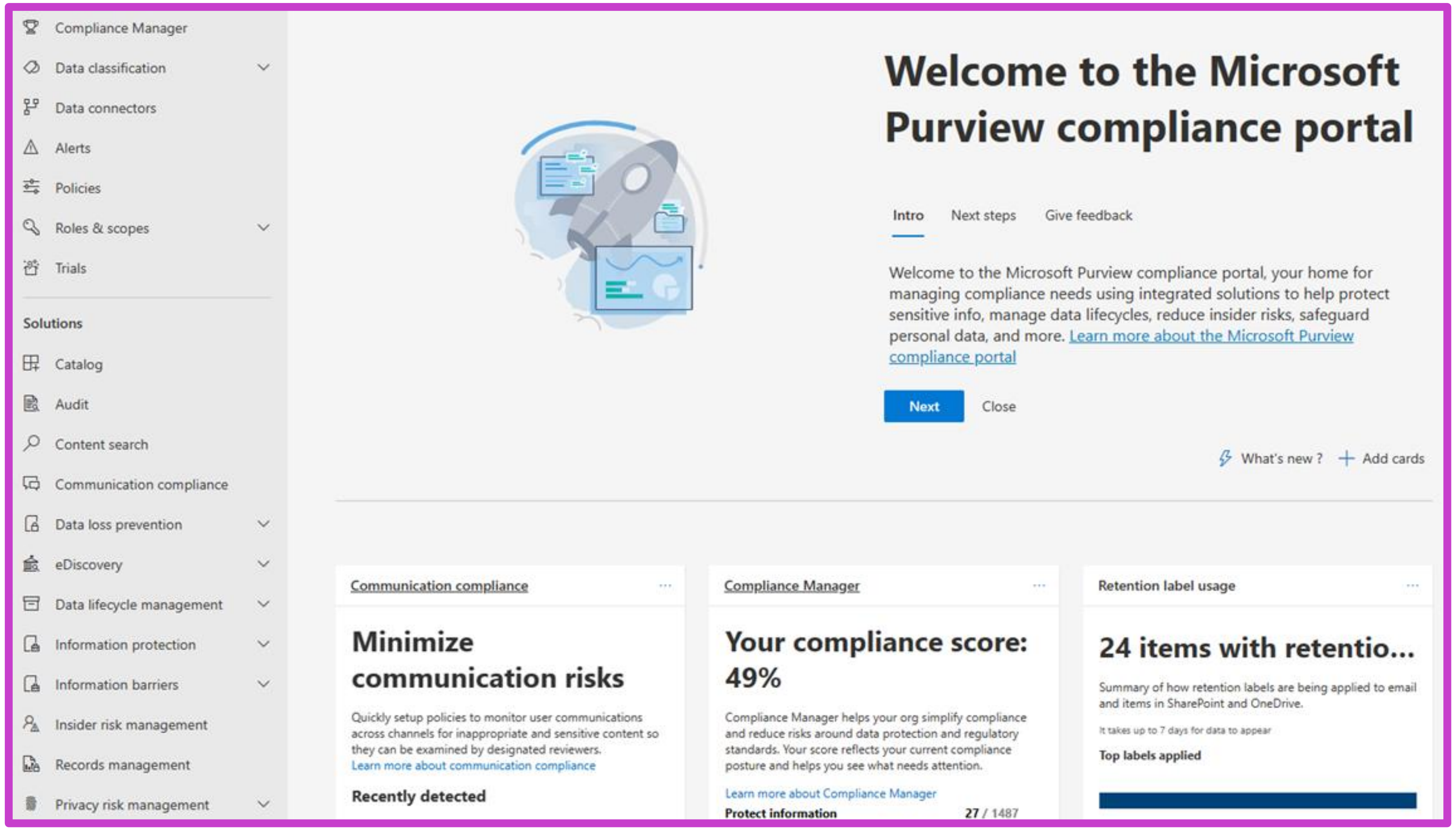
After completing this module, you should be able to:

1. Explore the Microsoft Purview compliance portal.
2. Describe Compliance Manager.
3. Describe the use and benefits of compliance score.

Microsoft Purview compliance portal

Easy access to the data and tools you need to manage to your organization's compliance needs.

- A view to an organization's compliance posture.
- Solutions to help with compliance.
- Customize navigation control.
- And more…



Welcome to the Microsoft Purview compliance portal

Welcome to the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions to help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more. Learn more about the Microsoft Purview compliance portal

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers.
Learn more about communication compliance

Recently detected

Compliance Manager

Your compliance score: 49%

Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information 27 / 1487

Retention label usage

24 items with retentio…

Summary of how retention labels are being applied to email and items in SharePoint and OneDrive.

It takes up to 7 days for data to appear

Top labels applied

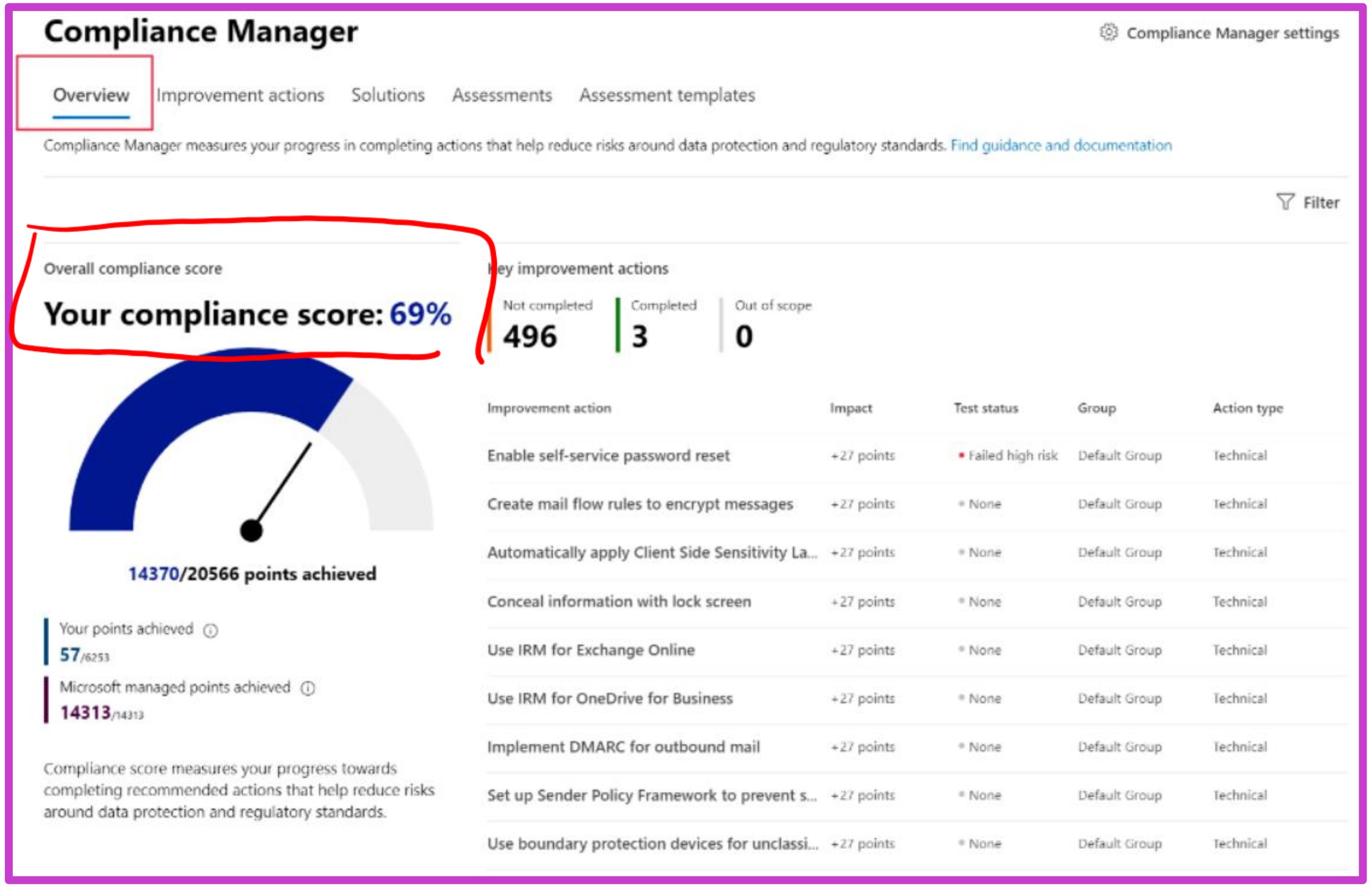
Compliance Manager

Compliance Manager simplifies compliance and reduces risk by providing:

- Prebuilt assessments based on common standards.
- Workflow capabilities to complete risk assessments.
- Step-by-step improvement actions.
- Compliance score that shows overall compliance posture.

Key elements of Compliance Manager

- Controls
- Assessments
- Templates
- Improvement actions



Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. Find guidance and documentation

Overall compliance score

Your compliance score: 69%

14370/20566 points achieved

Your points achieved: 57/6253

Microsoft managed points achieved: 14313/14313

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Key improvement actions

Not completed	Completed	Out of scope
496	3	0

Improvement action	Impact	Test status	Group	Action type
Enable self-service password reset	+27 points	● Failed high risk	Default Group	Technical
Create mail flow rules to encrypt messages	+27 points	● None	Default Group	Technical
Automatically apply Client Side Sensitivity La...	+27 points	● None	Default Group	Technical
Conceal information with lock screen	+27 points	● None	Default Group	Technical
Use IRM for Exchange Online	+27 points	● None	Default Group	Technical
Use IRM for OneDrive for Business	+27 points	● None	Default Group	Technical
Implement DMARC for outbound mail	+27 points	● None	Default Group	Technical
Set up Sender Policy Framework to prevent s...	+27 points	● None	Default Group	Technical
Use boundary protection devices for unclassi...	+27 points	● None	Default Group	Technical

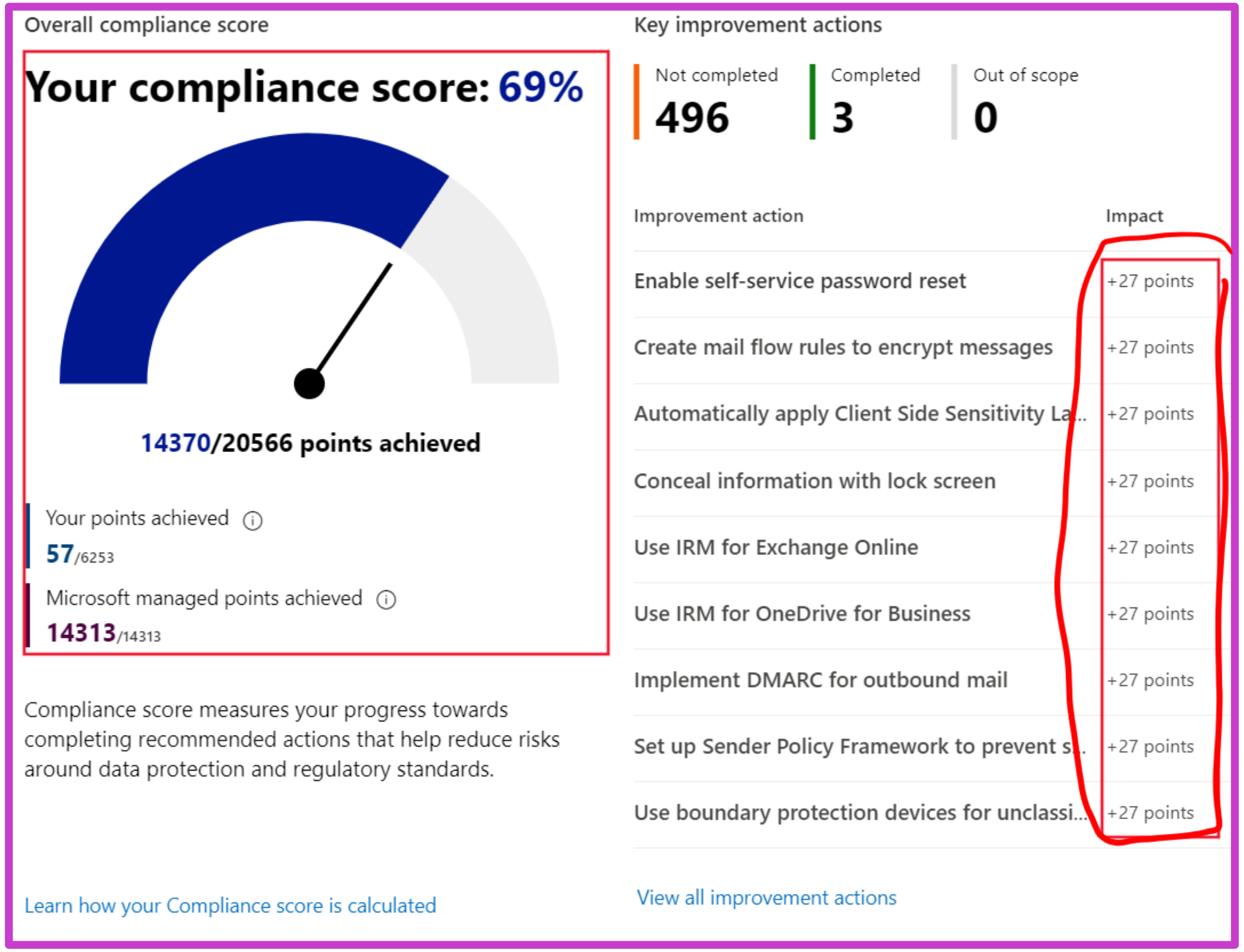
Compliance score

Benefits of compliance score:

- Helps an organization understand its current compliance posture.
- Helps prioritize actions based on their potential to reduce risk.

Understand your compliance score

- Actions
  - Your improved actions.
  - Microsoft actions.
- Action types (and action subcategory)
  - Mandatory (preventive, detective, or corrective).
  - Discretionary (preventive, detective, or corrective).



Overall compliance score

Your compliance score: 69%

14370/20566 points achieved

Your points achieved ⓘ
57/6253

Microsoft managed points achieved ⓘ
14313/14313

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how your Compliance score is calculated

Key improvement actions

Not completed	Completed	Out of scope
496	3	0

Improvement action	Impact
Enable self-service password reset	+27 points
Create mail flow rules to encrypt messages	+27 points
Automatically apply Client Side Sensitivity La...	+27 points
Conceal information with lock screen	+27 points
Use IRM for Exchange Online	+27 points
Use IRM for OneDrive for Business	+27 points
Implement DMARC for outbound mail	+27 points
Set up Sender Policy Framework to prevent s...	+27 points
Use boundary protection devices for unclassi...	+27 points

View all improvement actions

Module 3: Describe information protection, data life cycle management, and data governance capabilities in Microsoft Purview

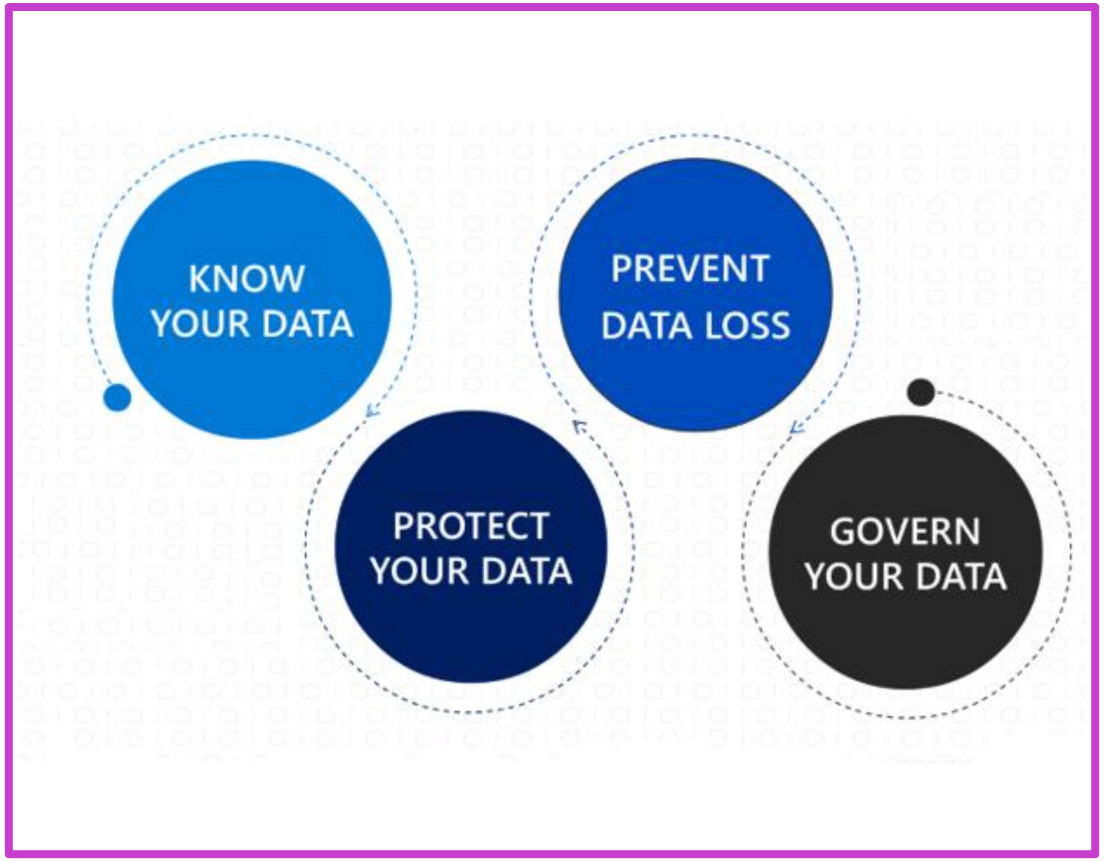
Module 3 introduction

After completing this module, you should be able to:

1. Describe the data classification capabilities of Microsoft Purview.
2. Describe data loss prevention in Microsoft Purview.
3. Describe records management in Microsoft Purview.
4. Describe the unified data governance solutions of Microsoft Purview.

Know your data, protect your data, and govern your data

- **Know your data:** Understand your data landscape and identify important data across on-premises, cloud, and hybrid environments.
- **Protect your data:** Apply flexible protection actions including encryption, access restrictions, and visual markings.
- **Prevent data loss:** Detect risky behavior and prevent accidental oversharing of sensitive information.
- **Govern your data:** Automatically keep, delete, and store data and records in a compliant manner.



Data classification capabilities of the compliance portal

1. Sensitive information types. → Label
2. Trainable classifiers: Pretrained classifiers and custom trainable classifiers.
3. Understand and explore the data.
4. The content explorer: Gain visibility into the content that has been summarized in the overview pane.
5. The activity explorer: Monitor what's being done with labeled content across the organization.

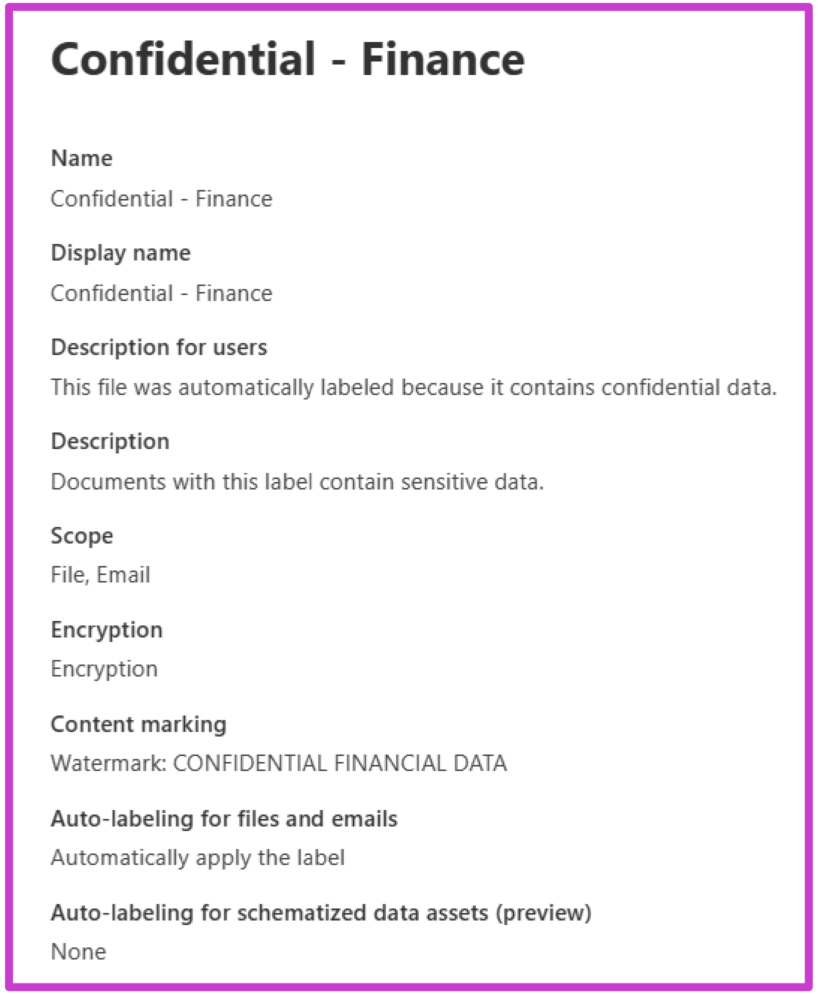
Sensitivity labels and policies

Sensitivity labels

- Customizable
- Clear text
- Persistent

Label policies

- Choose the users and groups that can see labels.
- Apply a default label to all new emails and documents.
- Require justifications for label changes.
- Require users to apply a label (mandatory labeling).
- Link users to custom help pages.



Confidential - Finance

Name
Confidential - Finance

Display name
Confidential - Finance

Description for users
This file was automatically labeled because it contains confidential data.

Description
Documents with this label contain sensitive data.

Scope
File, Email

Encryption
Encryption

Content marking
Watermark: CONFIDENTIAL FINANCIAL DATA

Auto-labeling for files and emails
Automatically apply the label

Auto-labeling for schematized data assets (preview)
None

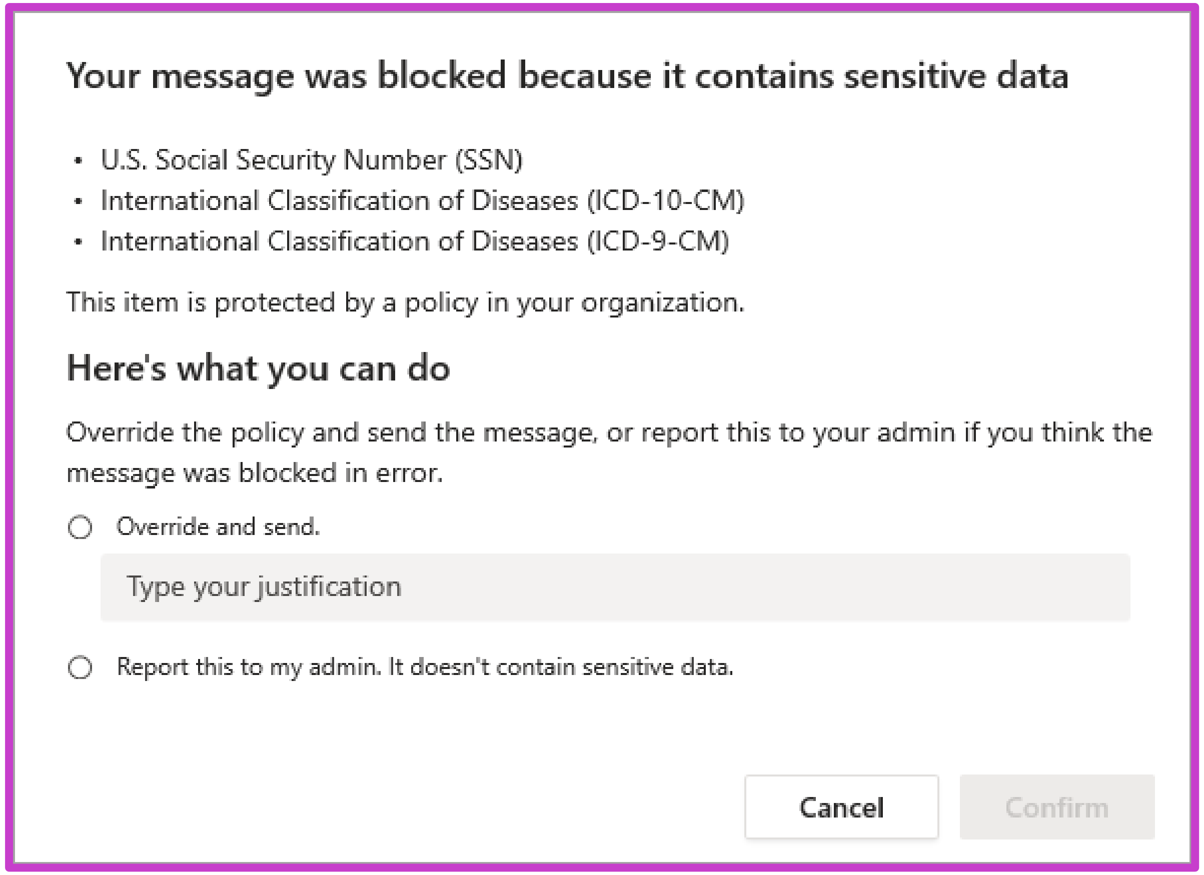
Data loss prevention (DLP)

Identify, monitor, and automatically protect sensitive items across:

- Microsoft 365 services – OneDrive for Business, SharePoint Online, Exchange Online, Office 365 applications.
- Microsoft Teams – Teams chat and channel messages.
- Devices – Windows 10, Windows 11, macOS.
- Microsoft Defender for Cloud Apps.
- On-premises repositories.
- Power BI.

Protective actions that DLP policies can take:

- Show a pop-up policy tip.
- Block the sharing with or without the override option.
- Move data at rest to a secure quarantine location.
- For Teams chat, sensitive information won't be displayed.



Your message was blocked because it contains sensitive data

- U.S. Social Security Number (SSN)
- International Classification of Diseases (ICD-10-CM)
- International Classification of Diseases (ICD-9-CM)

This item is protected by a policy in your organization.

Here's what you can do

Override the policy and send the message, or report this to your admin if you think the message was blocked in error.

○ Override and send.

Type your justification

○ Report this to my admin. It doesn't contain sensitive data.

Retention labels and policies

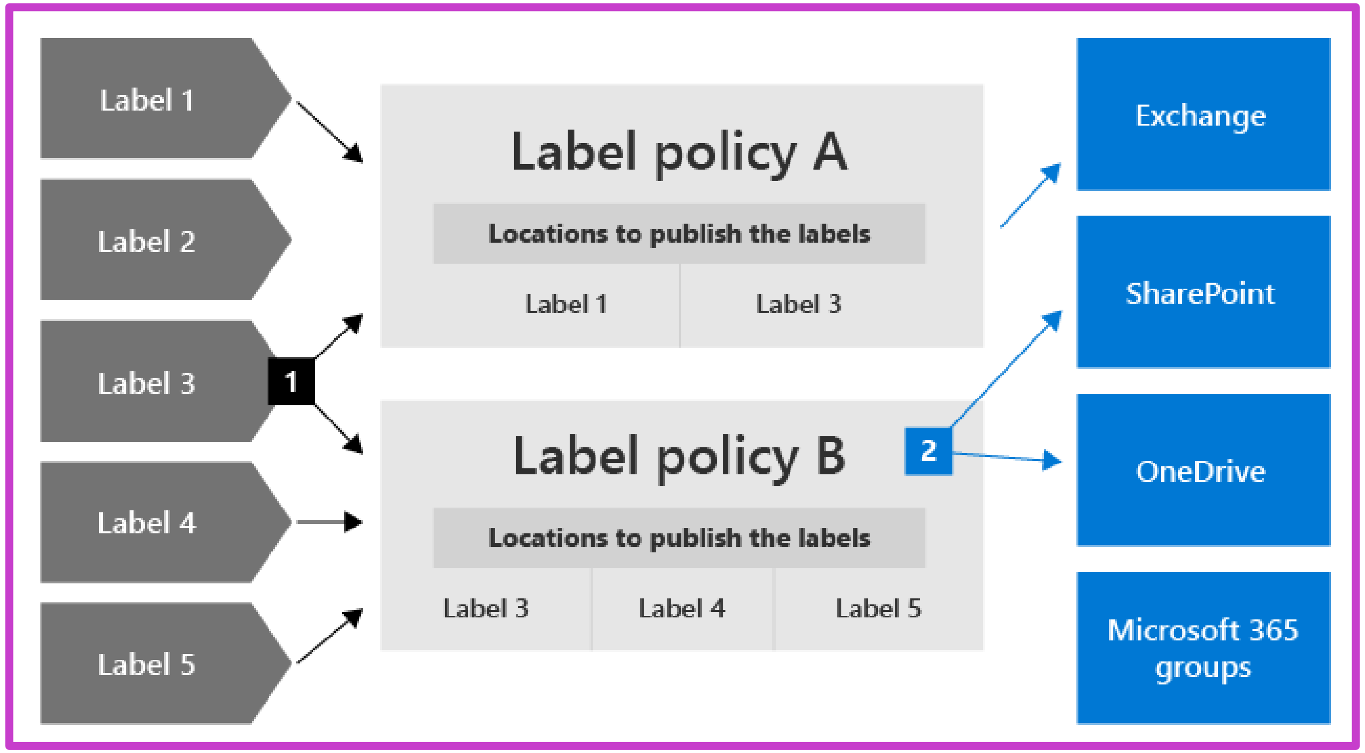
Manage and govern information by ensuring content is kept only for the required time.

Retention labels:

- Assigned at an item level.
- Only one label can be assigned at a time.
- Retention settings travel with the content.
- Can be applied automatically.
- Support disposition review.
- Published through label policy.

Retention policies:

- Assigned at a site level or mailbox level.
- A single policy can be applied to multiple locations, or to specific locations or users.
- Items inherit the retention settings from their container.



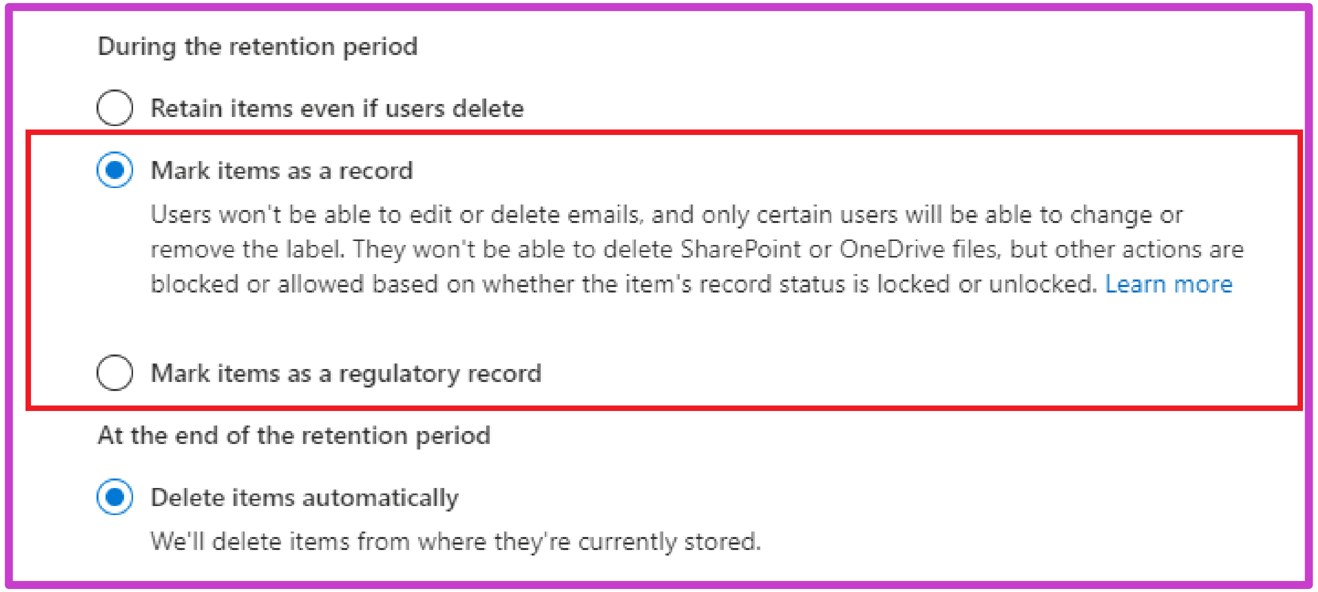
Records management

Helps an organization look after their legal obligations and helps to demonstrate compliance with regulations.

For content labeled as a record:

- Restrictions are put in place to block certain activities.
- Activities are logged.
- Proof of disposition is kept at the end of the retention period.

To enable items to be marked as records, an administrator sets up retention labels.



During the retention period

○ Retain items even if users delete

● Mark items as a record

Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. Learn more

○ Mark items as a regulatory record

At the end of the retention period

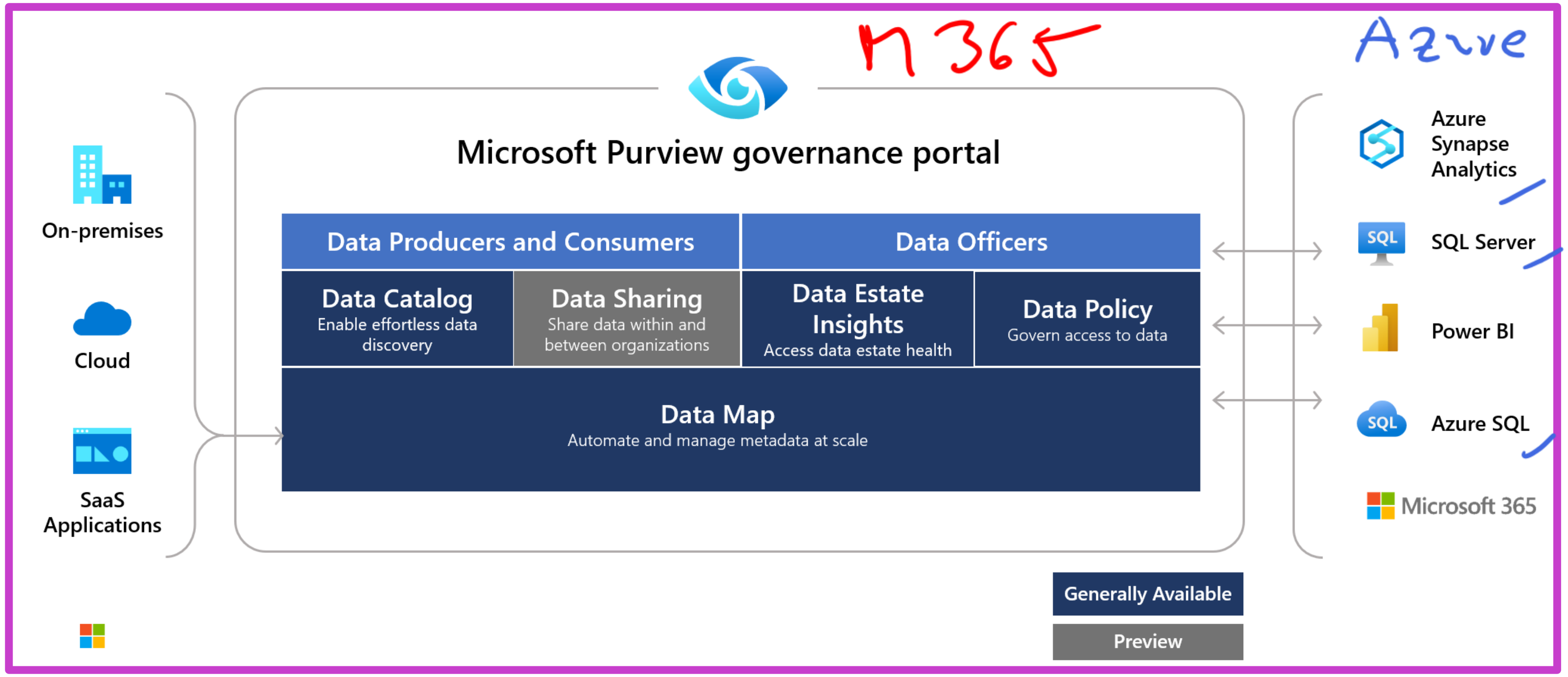
● Delete items automatically

We'll delete items from where they're currently stored.

Microsoft Purview unified data governance

A unified data governance service that helps organizations manage and govern their on-premises, multicloud, and SaaS data.

- **Data Map** – identify and classify sensitive data.
- **Data Catalog** – quickly and easily find relevant data.
- **Data Sharing (preview)** – share data within and between organizations.
- **Data Estate Insights** – know where sensitive data is, and how it moves.
- **Data Policy** – govern data access.



Module 4: Describe insider risk capabilities in Microsoft Purview

Module 4 introduction

After completing this module, you should be able to:

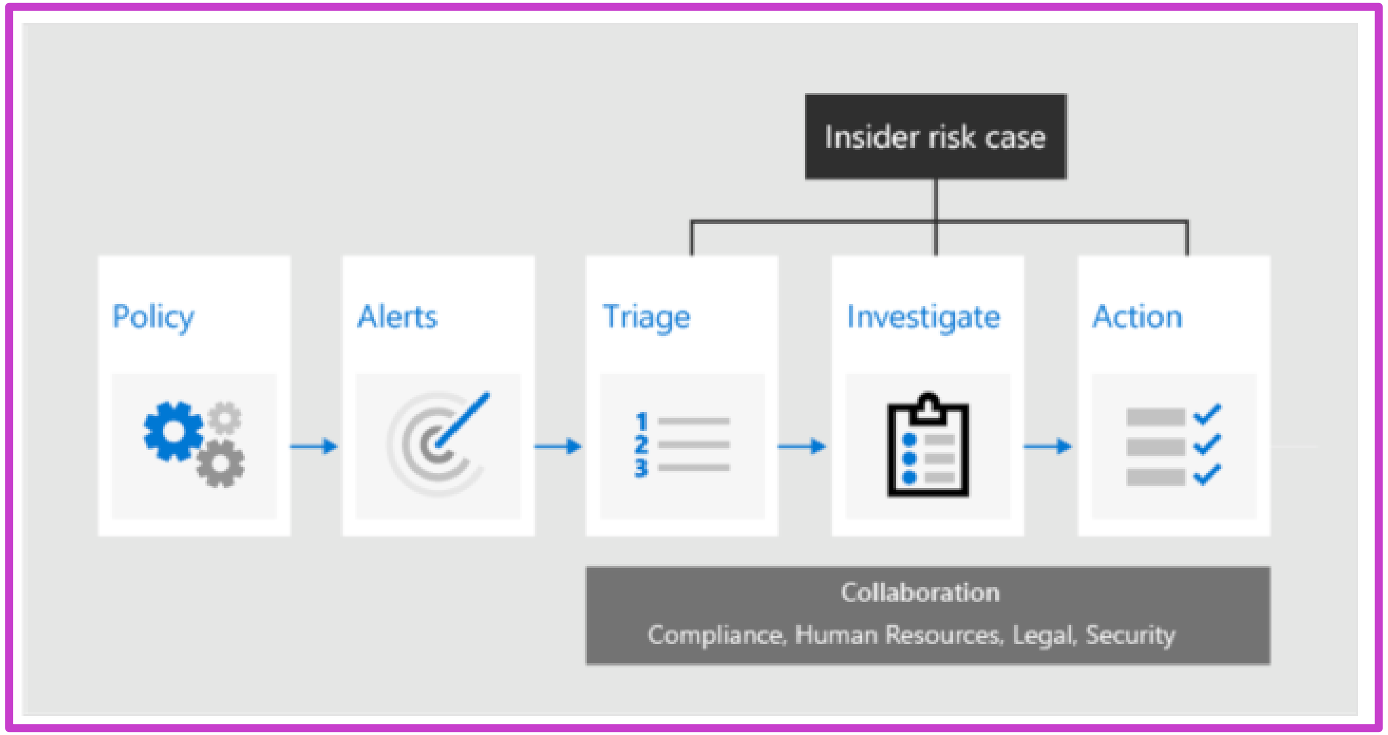
1 Describe how Microsoft Purview can help organizations identify insider risks and take appropriate action.

Microsoft Purview Insider Risk Management

Helps organizations to identify, investigate, and address internal risks such as data leaks, intellectual property theft, fraud, insider trading, and more.

Insider risk management workflow:

- Create ***policies*** to define what risk indicators are examined.
- ***Alerts*** automatically generated by risk indicators that match policy conditions.
- ***Triage*** alerts with a needs review status.
- Cases are created for alerts that require deeper review and ***investigation***.
- Reviewers can quickly take ***action*** to resolve the case.



Module 5: Describe eDiscovery and audit capabilities in Microsoft Purview

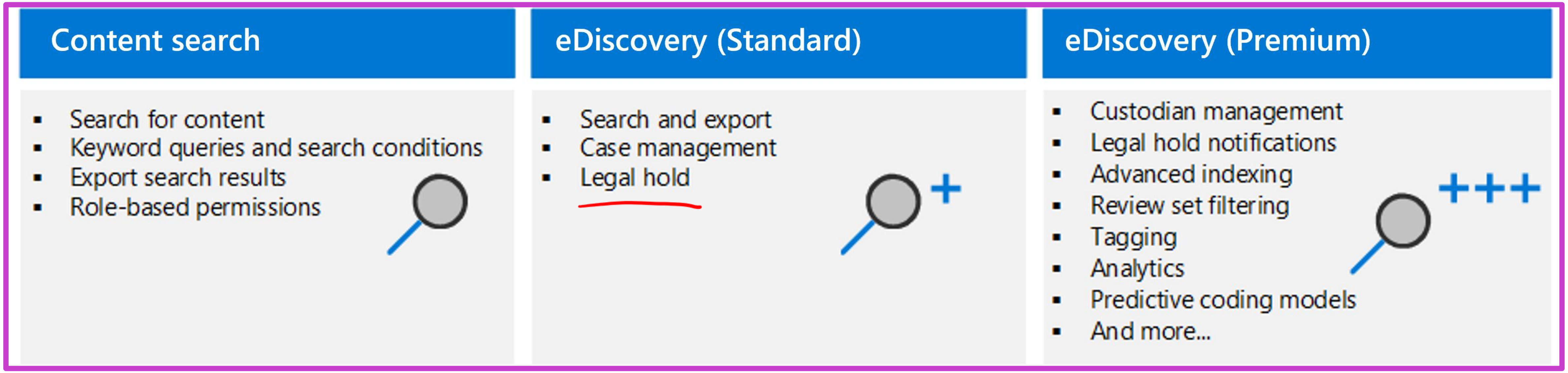
Module 5 introduction

After completing this module, you should be able to:

1. Describe the eDiscovery capabilities of Microsoft Purview.
2. Describe the auditing capabilities of Microsoft Purview.

Microsoft Purview eDiscovery

The process of identifying and delivering electronic information that can be used as evidence in legal cases.



Content search

- Search for content
- Keyword queries and search conditions
- Export search results
- Role-based permissions

eDiscovery (Standard)

- Search and export
- Case management
- Legal hold

eDiscovery (Premium)

- Custodian management
- Legal hold notifications
- Advanced indexing
- Review set filtering
- Tagging
- Analytics
- Predictive coding models
- And more...

Microsoft Purview Audit

Help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.

Audit (Standard)

Log and search for audited activities:

- Enabled by default
- Thousands of searchable audit events
- 90-day default retention period
- Accessed by GUI, cmdlet, and API

Audit (Premium)

Builds on the capabilities of Audit (Standard) with:

- 1 year default retention period
- Customized retention policies
- Intelligent insights
- Higher bandwidth access to API

Learning path summary

Describe the capabilities of Microsoft compliance solutions.

In this learning path, you have:

- Learned about the Service Trust Portal and privacy with Microsoft.
- Learned about the compliance management capabilities in Microsoft Purview, including the compliance portal, Compliance Manager, and Compliance Score.
- Learned about the information protection, data life cycle management, and data governance capabilities of Microsoft Purview.
- Learned about insider risk capabilities in Microsoft Purview.
- Learned about eDiscovery and audit capabilities of Microsoft Purview.

Knowledge check

Privacy and how private data is handled are top concerns for organizations and consumers. Microsoft helps organizations meet these challenges, through capabilities offered through two solutions. What are those solutions?

A. Microsoft Purview eDiscovery and Microsoft Purview Audit.

B. Priva Privacy Risk Management and Priva Subject Rights Requests.

C. Microsoft Purview Insider Risk Management and Microsoft Purview Communication Compliance.

Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained?

A. Controls that both external regulators and Microsoft share responsibility for implementing.

B. Controls that both your organization and external regulators share responsibility for implementing.

C. Controls that both your organization and Microsoft share responsibility for implementing.

Knowledge check continued

Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented?

A. Use the content explorer.
B. Use sensitivity labels.
C. Use records management.

The compliance admin for the organization wants to explain the importance of insider risk management, to the business leaders. What use case would apply?

A. To identify and protect against risks like an employee sharing confidential information.
B. To identify and protect against malicious software across your network, such as ransomware.
C. To identify and protect against devices shutting down at critical moments.

Microsoft