

Govern data in Microsoft Fabric with Purview

1. Govern data in the Microsoft Purview hub

<https://learn.microsoft.com/en-us/training/modules/fabric-data-governance-purview/govern-data-purview-hub>

Govern data in the Microsoft Purview hub

Completed

To govern Microsoft Fabric items using Microsoft Purview, you first need to establish a connection between Fabric and Purview. Once connected, the Microsoft Purview hub becomes available within Fabric, offering in-depth analysis and insights into your Fabric items. The Purview Hub acts as a gateway between Fabric and Purview.

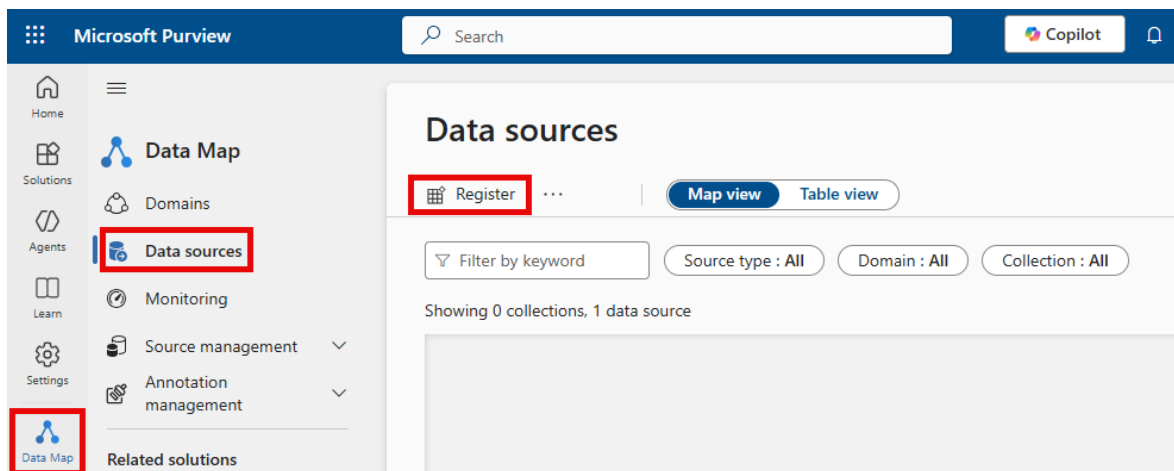
Imagine you're part of a healthcare organization that recently adopted Microsoft Purview. Now, you're ready to connect it to Fabric and explore the insights Purview provides on your Fabric data in the Microsoft Purview Hub.

In this unit, you'll explore the Purview hub.

Connect Purview to Fabric

The stages you must complete to connect Purview to Fabric are:

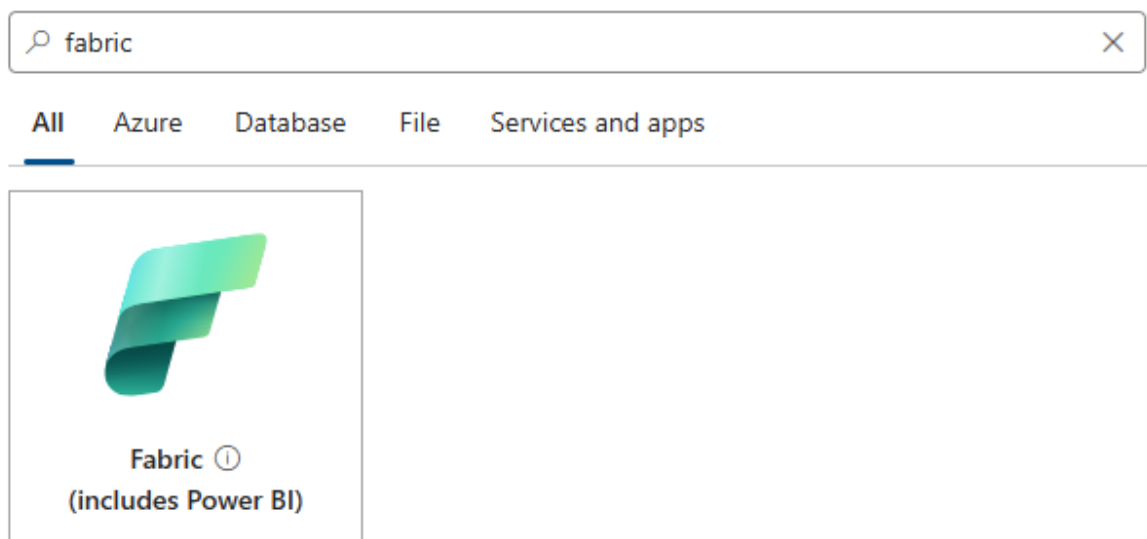
1. In Purview, register your Fabric tenant as a data source from the **Data Map** icon in the left navigation pane:



2. Select Fabric as a data source.

Register data source

Select the type of data source to register. [What data sources are supported?](#)



3. To scan Fabric, Purview needs to authenticate with it. In **Microsoft Entra ID**, configure authentication, using for example, the managed identity of your Purview account.

4. Create a scan in Purview that uses the Fabric data source.

Note

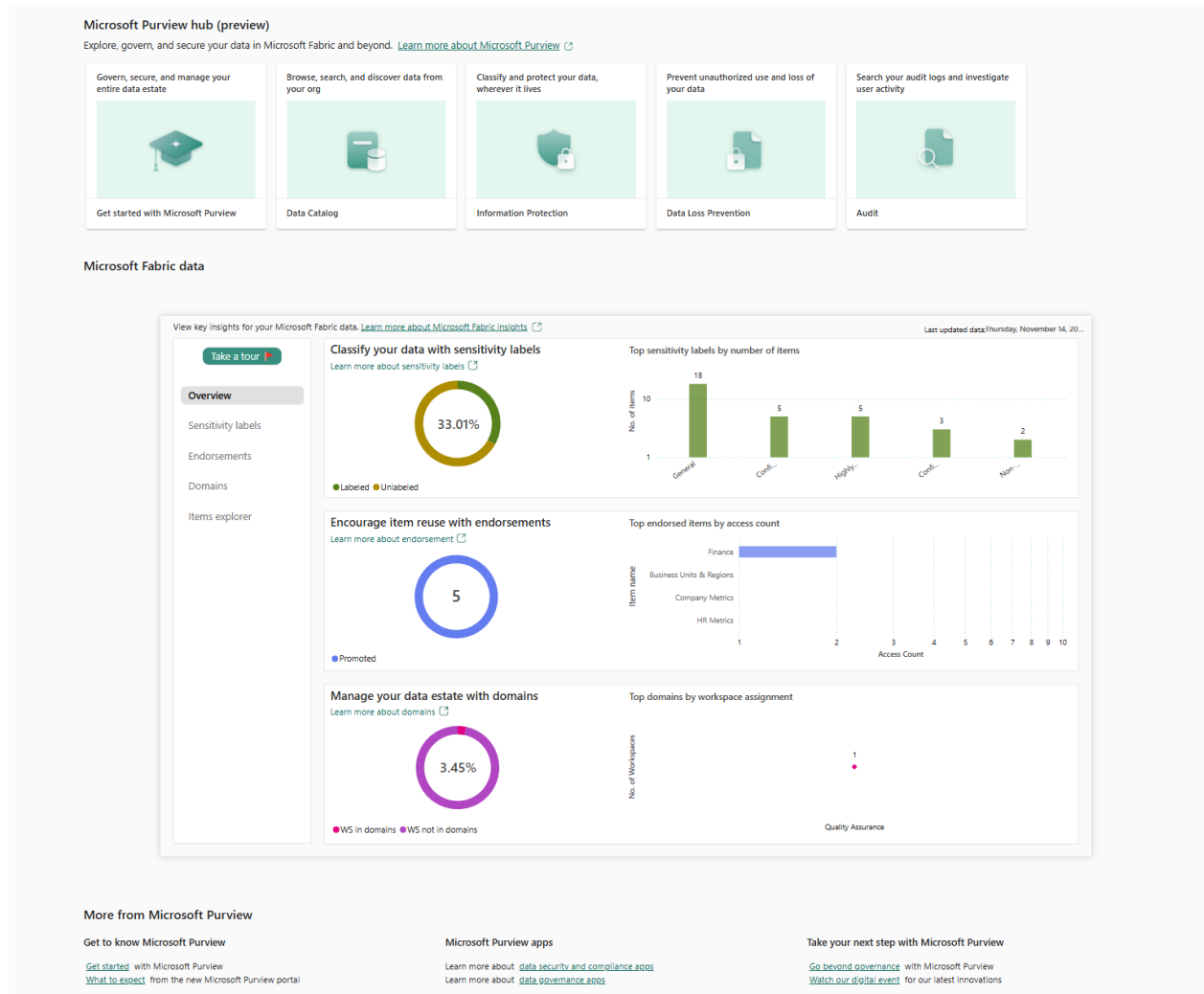
To configure authentication to Fabric from Purview, see

- [Connect to your Microsoft Fabric tenant in the same tenant as Microsoft Purview](#)
- [Connect to your Microsoft Fabric tenant from Microsoft Purview in a different tenant](#)

What is the Microsoft Purview hub in Microsoft Fabric?

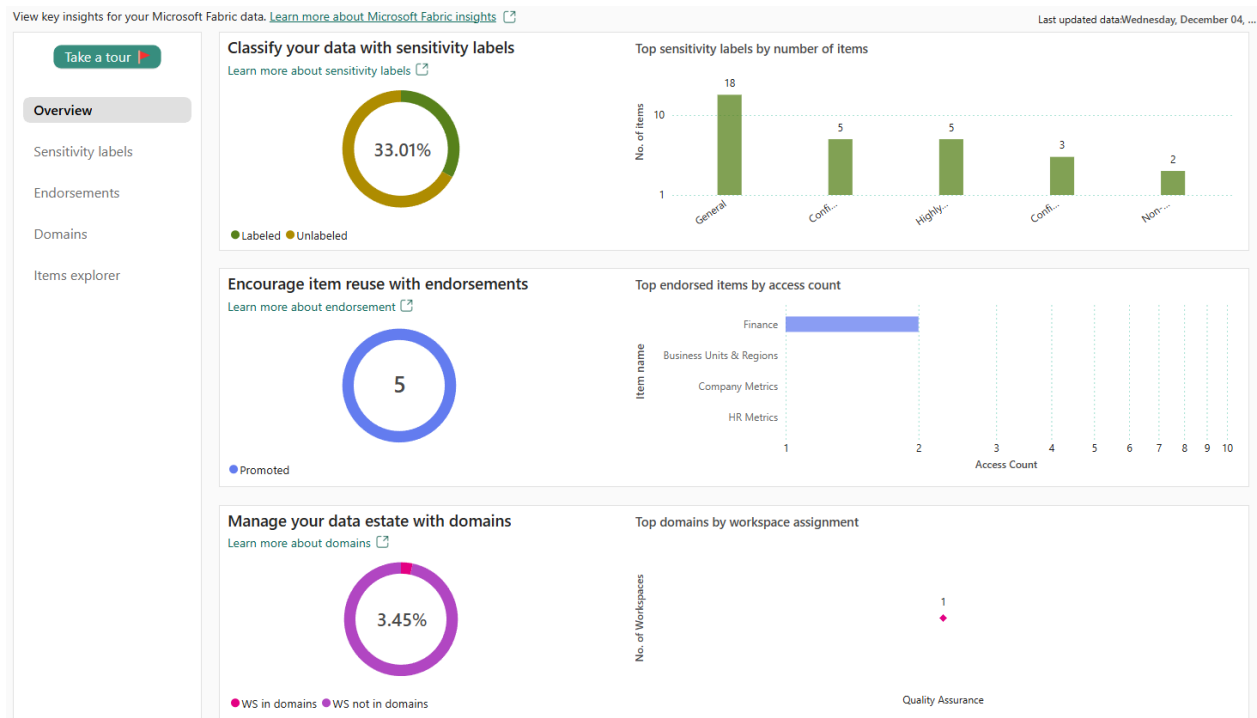
Once Purview and Fabric are connected, the Purview hub in Fabric displays reports and insights about your Fabric items. It acts as a centralized location to begin data governance and acts as a gateway to access more advanced features in Microsoft Purview.

To see the Purview hub, in Microsoft Fabric, open the Fabric settings, and then select **Microsoft Purview hub**.



The tiles at the top of the Purview hub enable you to access advanced governance and compliance capabilities in Purview. The Purview hub report provides dashboards that reflect the security posture of your organization's data estate. Select the following tabs for descriptions of the report pages.

- [Overview](#)
- [Sensitivity labels](#)
- [Endorsement](#)
- [Domains](#)
- [Items explorer](#)



The overview page provides high-level insights about your tenant's data estate. Select the **Take a tour** button in the navigation pane for a quick introduction to the main features of the report.

2. Module assessment

<https://learn.microsoft.com/en-us/training/modules/fabric-data-governance-purview/knowledge-check>

Module assessment

Completed

3. Summary

<https://learn.microsoft.com/en-us/training/modules/fabric-data-governance-purview/summary>

Summary

Completed

In this module, you explored how Microsoft Purview enhances the built-in governance capabilities of Microsoft Fabric to streamline data governance. With tools like the Purview Data Map, Unified Catalog, Information Protection, Data Loss Prevention, and Purview Audit, you can gain comprehensive visibility into your organization's data, safeguard it throughout its lifecycle, manage regulatory and risk requirements, and establish end-to-end governance.

Learn more

- [Microsoft Purview documentation](#)
- [Microsoft Fabric governance documentation](#)
- [Use Microsoft Purview to govern Microsoft Fabric](#)

4. Introduction

<https://learn.microsoft.com/en-us/training/modules/fabric-data-governance-purview/introduction>

Introduction

Completed

Microsoft Fabric is an end-to-end, analytics and data platform that provides a unified solution for data storage, movement, transformation, processing, real-time event routing, and reporting. When working with a large volume of data in Fabric, some of which is highly sensitive, you must ensure that it's accurate, trustworthy, and protected throughout the data lifecycle. Data governance is the set of techniques and tools that you use to implement these requirements.

Microsoft Purview has a data governance solution designed to help you discover, catalog, and manage data assets across your organization. It provides a unified view of your data estate by scanning and cataloging metadata from various data sources, including Microsoft Fabric. Purview has three pillars: data governance, data security, and risk and compliance. In this module, we'll focus on data governance.

Imagine you're in a data stewardship role at a healthcare organization, responsible for managing and safeguarding sensitive patient information. You rely on Microsoft Fabric to store, analyze, manipulate, and report on data, all while ensuring compliance with health data regulations such as HIPAA. Fabric offers built-in data governance capabilities to support these responsibilities. Now, you're looking to explore how integrating Microsoft Purview with Fabric can further enhance your ability to protect sensitive data and maintain regulatory compliance.

In this module, you'll learn how Purview data governance features work with Fabric and how to use them for compliance, security, and discoverability.

5. Govern data in Microsoft Fabric

<https://learn.microsoft.com/en-us/training/modules/fabric-data-governance-purview/govern-data>

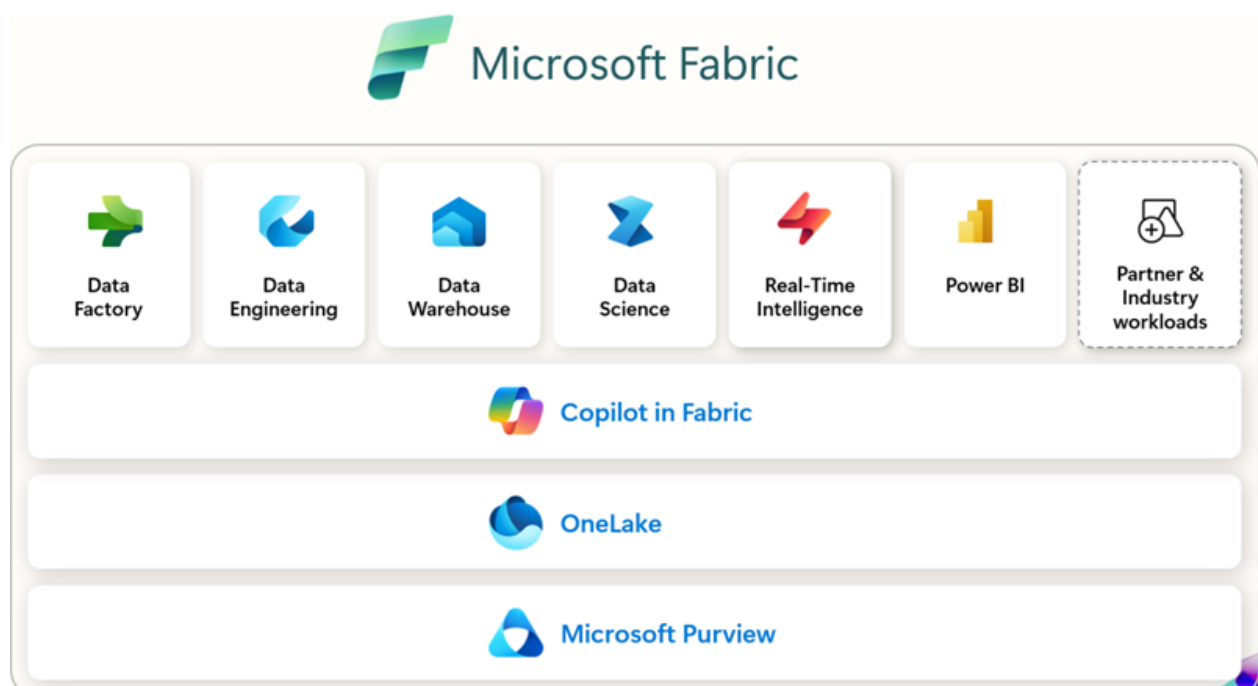
Govern data in Microsoft Fabric

Completed

Microsoft Fabric includes a set of governance and compliance capabilities that might be sufficient for the needs of some organizations. Other governance capabilities can be accessed in Microsoft Purview.

If, for example, you work at a health care company, you have specific data governance needs because of regulatory requirements. In this unit, we'll explore Fabric's governance features so you can assess if they meet your requirements.

What is Microsoft Fabric?



Fabric is Microsoft's end-to-end analytics and data platform. The platform can store, move, process, ingest, transform, and analyze your data regardless of its size and current format. Once you have data in the location and format you need it, advanced business intelligence features can be used to analyze data, and generate insights to support your decision making.

OneLake

In Fabric, all information is stored in a data lake, which can hold both structured and unstructured data. Microsoft's implementation of the data lake is called OneLake and is built on Azure Data Lake Storage (ADLS) generation 2. With all data residing in OneLake, there's a single copy of data that doesn't need to be moved or duplicated. This single underlying storage mechanism helps ensure that policies and security controls are applied universally.

What is data governance?

The data that an organization works with is often business-critical and highly sensitive. Sensitive data must be: held securely, easily available, and processed in compliance with legislation in all the locations where an organization operates.

Data governance is the practice of managing data to ensure the quality, consistency, security, and usability of data. It involves setting up a framework that includes roles, responsibilities, processes, policies, and standards that are used to manage data throughout its lifecycle.

A data governance program usually includes:

- **Auditing:** Recording where data originates and who modifies it.
- **Evaluation:** Assessing the usefulness and accuracy of data.
- **Documentation:** Providing clear descriptions of data to support informed use.
- **Management:** Correcting inaccurate data, fulfilling access requests, and maintaining compliance with data legislation.
- **Protection:** Securing data from unauthorized access, ransomware threats, and other malicious attacks.

Well-governed data is reliable and readily accessible to those who need it.

Tip

In large organizations, data is often stored and managed separately across different business units, creating what are known as data silos. These silos can hinder effective data governance due to inconsistent standards and policies across teams. Breaking down these silos by integrating data—while preserving security and compliance—is essential for establishing a unified and governed data environment.

Implementing data governance can lead to benefits such as:

- A single source of truth that reduces confusion and supports decision making.
- Improved data quality.
- Faster compliance with access requests.
- Reduced data storage and management costs.

Data governance features in Microsoft Fabric

Many data governance tasks can be performed using your Microsoft Fabric license, without the need for an additional Microsoft Purview license. Let's explore some of the built-in data governance capabilities available directly within Fabric.

Managing the data estate

Your organization's data estate encompasses all its data assets. Managing a large data estate can be complex and resource-intensive. Microsoft Fabric simplifies managing your data estate with these tools:

- **The Fabric Admin portal:** control tenant settings, capacities, domains, and other objects, typically reserved for administrators.
- **Tenants, domains, and workspaces:** logical containers that you can use to control access to data and capabilities. Fabric administrators, for example, should have access to all settings in the tenant whereas team level data controllers might only have control of settings on their domain or workspace.
 - Domains group data that is relevant to a single business area or subject field.
 - Workspaces group Fabric items used by a single team or department.
- **Capacities:** These objects limit compute resource usage for all Fabric workloads.
- **Metadata scanning:** Scanning extracts values such as names, identities, sensitivities, endorsements, and so on, from data lakes. You can use this metadata to analyze and set governance policies.

Securing and protecting data

Secure data is safeguarded from unauthorized access and malicious attacks. It's also compliant with data storage regulations applicable in your region. Fabric includes the following tools to secure and protect data:

- **Data tags:** Use tags to identify the sensitivity of data and apply data retentions and protection policies.
- **Workspace roles:** Use roles to define the users who are authorized to access the data in a workspace.
- **Data-level controls:** Use controls at the level of Fabric items such as tables, rows, and columns to impose granular restrictions.
- **Certifications:** Fabric is compliant with many data management certifications, including HIPAA BAA, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27001, and ISO/IEC 27701.

Encouraging data discovery and use

Data only becomes valuable when users can find and analyze it. These Microsoft Fabric features help promote data discovery and encourage meaningful use:

- **OneLake data hub:** This tool makes it easy for users to find and explore the data in your estate.
- **Endorsement:** Users endorse a Fabric item to identify it as of high quality. Endorsements help other users to trust the data that the item contains.
- **Data lineage:** This feature helps users to understand the flow of data between items in a workspace and the impact that a change would have.

Monitoring data usage

Fabric helps users track how data is being used through built-in monitoring tools:

- **Monitoring Hub:** Provides a centralized view of Microsoft Fabric activities. Users can only see activity related to Fabric items they have permission to access.
- **Capacity Metrics App:** Offers insights into Fabric usage and resource consumption, helping teams manage capacity effectively.

Learn more

- [What is Microsoft Fabric?](#)
- [What is data governance?](#)
- [Microsoft Fabric governance documentation](#)

6. Why use Microsoft Purview with Microsoft Fabric?

<https://learn.microsoft.com/en-us/training/modules/fabric-data-governance-purview/why-purview-fabric>

Why use Microsoft Purview with Microsoft Fabric?

Completed

When you need data governance features beyond those built into Microsoft Fabric, Microsoft Purview provides comprehensive data governance capabilities.

In the last unit, we reviewed the built-in governance features of Microsoft Fabric. Let's assume you work for a health care provider and new regulations mean you need stricter governance for data stored in Microsoft Fabric. Now, you want to investigate what features Microsoft Purview includes that can help you comply with new regulations.

In this unit, you'll learn what capabilities Microsoft Purview adds to the built-in data governance and compliance capabilities available in Microsoft Fabric.

What is Microsoft Purview?

Microsoft Purview is a set of solutions that you can use to govern, protect, and manage data wherever it resides. It has three pillars: data governance, data security, and risk and compliance. Purview includes data governance tools for data discovery, classification, and cataloging and can be used to gain a clear understanding of your data landscape. Purview automates the identification of sensitive information and provides a centralized repository for metadata. Use it to find, manage, and govern data across various environments, both on-premises and in the cloud.

Purview also supports data security and risk and compliance management with features that monitor regulatory adherence and assess data vulnerabilities. It integrates with other Microsoft services and third-party tools. By streamlining data access controls, enforcing policies, and delivering insights into data lineage, Purview can help you maintain data integrity, comply with regulations, and use data effectively for strategic decision-making.

The Purview solutions can be accessed via the Microsoft Purview Portal.



What are some of the Purview tools?

Microsoft Purview enables you to discover, manage, and protect Fabric data using Purview tools. Purview can be configured to scan your Fabric item and present data governance findings in the Purview Hub located in Fabric or in Purview itself. To unlock the following capabilities, register your Fabric tenant in Microsoft Purview.

Microsoft Purview Data Map

Data Map can be used to scan all of your data assets, to capture metadata about them and to identify sensitive data. It captures metadata about data in existing analytics, software-as-a-service, and operational systems in hybrid, on-premises, and multicloud environments. There's a built-in scanning and classification system that keeps the Data Map updated.

Microsoft Purview Unified Catalog

The Purview Unified Catalog is a searchable catalog of your scanned data where you curate, grant access to and, improve the health of your data.

In the Purview Unified Catalog, you can inventory of all your data assets, their metadata, and their lineage so you can understand the topography of your data estate. You can search for and browse datasets, and view metadata, data lineage, classification, and sensitivity labels. The Unified Catalog promotes collaboration because users can annotate datasets with tags to improve discoverability.

Suppose you work at a health care provider and regulations require you to control who can access patient records. In the Unified Catalog, users and administrators can:

- Discover where patient records are held by searching for keywords.
- Label documents and items as patient records to differentiate them from other, less sensitive information.
- Use access policies to manage self-service access requests to patient records.

Microsoft Purview Information Protection

Information Protection is used to classify, label, and protect sensitive data throughout your organization. By applying customizable sensitivity labels, you can classify records. Then policies can define access controls and enforce encryption. These labels follow the data wherever it goes, whether in emails, documents, or cloud storage, and integrate with other tools like Data Loss Prevention (DLP) to prevent unauthorized sharing. This helps organizations meet compliance requirements while safeguarding data against accidental exposure or malicious threats.

If, for example, you worked as a data steward at a health care provider, you could use Information Protection to:

- Identify data items that contain patient information, even when item titles don't identify them as patient records.
- Train classifiers to spot patient records automatically.
- Protect records with policies to encrypt data and impose Information Rights Management (IRM).

Microsoft Purview Data Loss Prevention (DLP)

DLP helps protect sensitive information with policies that automatically detect, monitor, and control the sharing or movement of sensitive data. Administrators can customize rules to block, restrict, or

alert when sensitive data is transferred to prevent accidental or malicious data leaks.

If you worked at a health care provider, you would need to ensure that users don't share patient records with external parties, either accidentally or maliciously. DLP can prevent such transfers on information labeled as patient records.

Microsoft Purview Audit

Auditing solutions in Purview are used to search for activities performed in Microsoft services by users and admins. User activities such as creating files or accessing Fabric items are automatically logged and appear in the Purview audit log.

Thorough auditing is an important protection for the policies you apply to patient records. For example, if a malicious administrator changes DLP policies so that they can copy a patient record to a USB device, this change is recorded and can be identified during later investigations.

Learn more

- [Use Microsoft Purview to govern Microsoft Fabric](#)
- [Learn about Microsoft Purview](#)