

# Microsoft Purview

Microsoft Purview is a comprehensive portfolio of products spanning data governance, information protection, risk management, and compliance solutions.

## Microsoft Purview solutions

Guidance to help you get started with Microsoft Purview solutions in the governance and compliance portals.



### What is Microsoft Purview?

Learn how Microsoft Purview data governance, risk, and compliance solutions can help your organization govern, protect, and manage your data estate.



### Microsoft Purview governance documentation

Learn how to use Microsoft Purview so your organization can find, understand, govern, and consume data sources.



### Microsoft Purview risk and compliance documentation

If your organization needs to comply with legal or regulatory standards, start here to learn about compliance in Microsoft Purview.

## Manage visibility and governance of data assets

Guidance to help you get started with understanding and governing data across your digital estate.

### Microsoft Purview Data Map

Capture metadata about analytics data, software-as-a-service, and in hybrid, on-premises, and multi-cloud environments.

### Microsoft Purview Data Catalog

Find trusted data sources by browsing and searching your data assets, aligning your assets with friendly business terms and data classification.

### Microsoft Purview Data Estate Insights

Gain insights into your data estate, to help you discover what kinds of data you have and where.

# Protect sensitive data across clouds, apps, and devices

Guidance to help you get started with protecting data in your organization.

## Microsoft Purview Information Protection

Discover, classify, and protect sensitive information wherever it lives or travels.

## Microsoft Purview Data Loss Prevention

Use data loss prevention to help prevent accidental sharing of sensitive information.

## Microsoft Purview Message Encryption

Send and receive encrypted email messages to people inside and outside your organization.

## Microsoft Purview Customer Key

Help meet compliance requirements by exercising control over your organization's encryption keys.

## Microsoft Purview Double Key Encryption

Uses two keys together to access protected content. Microsoft stores one key in Microsoft Azure, and you hold the other key.

## Microsoft Purview Data Connectors

Import and archive non-Microsoft data so you can apply Microsoft 365 protection and governance capabilities to third-party data.

## Microsoft Purview Data Lifecycle Management

Retain the Microsoft 365 data that you need to keep, and delete the content that no longer has business value.

## Microsoft Information Protection SDK

Extend sensitivity labels to third-party apps and services.

## Microsoft Purview Customer Lockbox

Maintain control over your content with explicit access authorization for service operations.

# Identify data risks and manage regulatory compliance requirements

Guidance to help you get started with identifying and minimizing risk in your organization.

## Microsoft Purview Insider Risk Management

## Microsoft Purview Communication Compliance

## Microsoft Purview Information Barriers

Detect, investigate, and act on malicious and inadvertent risk activities in your organization.

Detect, investigate, and act on inappropriate and sensitive messages in your organization.

Restrict communication and collaboration among specific groups of users in highly-regulated organizations.

### **Microsoft Purview Privileged Access Management**

Help protect your organization from breaches that use accounts with standing access to sensitive data and critical configuration settings.

### **Microsoft Purview Compliance Manager**

Compliance Manager helps with taking inventory of data protection risks, managing the implementation of controls, staying current with regulations & certifications, and reporting to auditors.

### **Microsoft Purview Records Management**

Manage high-value items for business, legal, or regulatory record-keeping requirements.

### **Microsoft Purview Audit**

Learn about premium and standard audit solutions and tools to help you log and search for audited activities in SharePoint and OneDrive.

### **Microsoft Purview eDiscovery**

Learn about eDiscovery tools that allow you to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams.

### **Microsoft Graph APIs for compliance capabilities**

Adapt, extend, integrate, accelerate, and support compliance solutions with programmatic access.

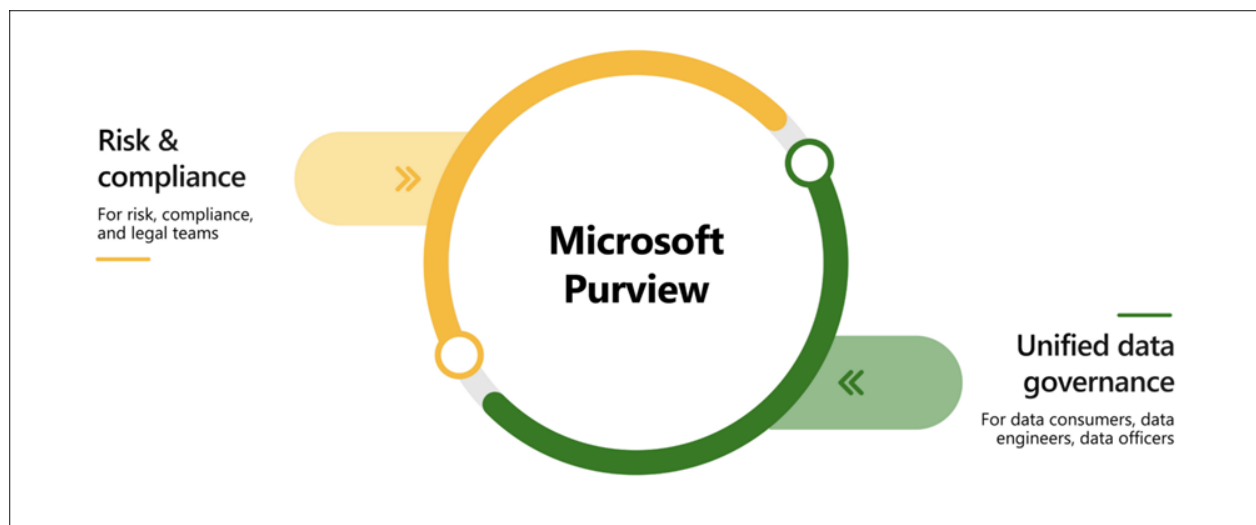
# What is Microsoft Purview?

Article • 02/21/2023 • 2 minutes to read

Microsoft Purview is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate. Microsoft Purview solutions provide integrated coverage and help address the recent increases in remote user connectivity, the fragmentation of data across organizations, and the blurring of traditional IT management roles.

Microsoft Purview combines the former [Azure Purview](#) and [Microsoft 365 compliance](#) solutions and services together into a single brand. Together, these solutions help your organization to:

- Gain visibility into data assets across your organization
- Enable access to your data, security, and risk solutions
- Safeguard and manage sensitive data across clouds, apps, and endpoints
- Manage end-to-end data risks and regulatory compliance
- Empower your organization to govern, protect, and manage data in new, comprehensive ways



For more information about the Microsoft Purview release, see [The future of compliance and data governance is here: Introducing Microsoft Purview](#) security blog announcement.

## Microsoft Purview risk and compliance solutions

Microsoft Purview includes [risk and compliance solutions](#) that support services included in Microsoft 365. These services include [Microsoft Teams](#), [SharePoint](#), [OneDrive](#),

[Exchange](#), and others. These compliance and risk solutions help your organization to:

- Protect sensitive data across clouds, apps, and devices
- Identify data risks and manage regulatory compliance requirements
- Get started with regulatory compliance

## Microsoft Purview unified data governance solutions

Microsoft Purview includes [unified data governance solutions](#) that help you manage data services across your on-premises, multi-cloud, and software-as-a-service (SaaS) estate. That includes [Azure storage services](#), [Power BI](#), databases like [SQL](#) or [Hive](#), file services like [Amazon S3](#), and [many more](#).

These governance solutions are accessible through the Microsoft Purview governance portal, which provides tools to enable your organization to:

- Create an up-to-date map of your entire data estate that includes data classification and end-to-end lineage
- Identify where sensitive data is stored in your estate
- Create a secure environment for data consumers to find valuable data
- Generate insights about how your data is stored and used

## Ready to get started?


- Get started with [Microsoft Purview risk and compliance solutions](#)
- Get started with [Microsoft Purview governance solutions](#)

# Microsoft Purview risk and compliance solutions

Article • 02/21/2023 • 7 minutes to read

[Microsoft Purview](#) risk and compliance solutions help you manage and monitor your data, protect information, minimize compliance risks, and meet regulatory requirements. This article will help you learn about Microsoft Purview risk and compliance solutions and quickly get started with deploying these solutions to meet specific compliance needs for your organization.

## Tip

If you're not an E5 customer, you can try all the premium features in Microsoft Purview for free. Use the 90-day Purview solutions trial to explore how robust Purview capabilities can help your organization manage data security and compliance needs. Start now at the [Microsoft Purview compliance portal trials hub](#) . Learn details about [signing up and trial terms](#).

## Protect sensitive data across clouds, apps, and devices

Your information protection strategy should be driven by your business needs, but every organization has a requirement to protect some or all of its data. Use the capabilities from [Microsoft Purview Information Protection](#) (formerly Microsoft Information Protection) to help you discover, classify, protect, and govern sensitive information wherever it lives or travels.

## Know your data

You have information residing across all the Microsoft 365 services and on-premises. Identifying which items are sensitive and gaining visibility into how they're being used is central to your information protection practice. Microsoft Purview includes:

- [Sensitive information types](#) to identify sensitive items by using built-in or custom regular expressions, or a function.
- [Trainable classifiers](#) to identify sensitive items by using examples of the data you're interested in rather than identifying elements in the item.

- [Data classification](#) provides a graphical identification of items in your organization that have a sensitivity label, a retention label, or have been classified and the actions your users are taking on them

## Protect your data

There are many capabilities that you can use from the Microsoft Purview Information Protection solution to help protect your data, wherever it's stored and however it's accessed. However, sensitivity labels are the foundational capability that both provide protection actions and interact with other Purview solutions and capabilities.

Sensitivity labels provide users and admins with visibility into the sensitivity of the data that they're using, and the labels themselves can apply protection actions that include encryption, access restrictions, and visual markings. For more information about the range of labeling scenarios supported, see the [Common scenarios for sensitivity labels](#) section from the getting started documentation. For more information about sensitivity labels, see [Learn about sensitivity labels](#).

## Prevent data loss

Unintentional sharing of sensitive items can cause financial harm to your organization and may result in a violation of laws and regulations. [Microsoft Purview Data Loss Prevention](#) can help protect your organization against unintentional or accidental sharing of sensitive information both inside and outside of your organization. In a data loss prevention policy, you:

- Define the sensitive information you want to monitor for, like financial, health, medical, and privacy data.
- Where to monitor, like Microsoft 365 services or Windows and macOS devices.
- The conditions that must be matched for a policy to be applied to an item, like items containing credit card, driver's license, or social security numbers.
- The actions to take when a match is found, like audit, block the activity, and block the activity with override.

## Manage your data lifecycle

[Microsoft Purview Data Lifecycle Management](#) (formerly Microsoft Information Governance) provides you with tools and capabilities to retain and delete content across Exchange, SharePoint, OneDrive, Microsoft 365 Groups, Teams, and Yammer. Retaining and deleting emails, documents, and messages are often needed for compliance and

regulatory requirements. However, deleting content that no longer has business value also reduces your attack surface.

For more information, see [Learn about data lifecycle management](#).

## Encrypt your data and control your encryption keys

[Encryption](#) is an important part of your file protection and information protection strategy. The encryption process encodes your data (referred to as plaintext) into ciphertext. Unlike plaintext, ciphertext can't be used by people or computers unless and until the ciphertext is decrypted. Decryption requires an encryption key that only authorized users have. Encryption helps ensure that only authorized recipients can decrypt your content.

[Microsoft Purview Double Key Encryption](#) helps secure your most sensitive data that is subject to the strictest protection requirements. [Microsoft Purview Customer Key](#) helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on.

## Identify data risks and manage regulatory compliance requirements

Insider risks are one of the top concerns of security and compliance professionals in the modern workplace. Industry studies have shown that insider risks are often associated with specific user events or activities. Protecting your organization against these risks can be challenging to identify and difficult to mitigate. Insider risks include vulnerabilities in various areas and can cause major problems for your organization, ranging from the loss of intellectual property to workplace harassment, and more.

Microsoft Purview offers the following compliance solutions to help your organization manage data risk and compliance requirements:

- [Insider risk management](#)
- [Communication compliance](#)
- [Information barriers](#)
- [Records management](#)
- [Audit \(Premium\) and Audit \(Standard\)](#)
- [eDiscovery \(Premium\) and eDiscovery \(Standard\)](#)



## **Detect and act on risk activities with insider risk management**

[Microsoft Purview Insider Risk Management](#) uses the full breadth of service and 3rd-party indicators to help you quickly identify, triage, and act on risky user activity in your organization. By using logs from Microsoft 365 and Microsoft Graph, insider risk management allows you to define specific policies to identify risk indicators. After identifying risky activities, you can take action to mitigate these risks.

## **Detect and act on inappropriate and sensitive messages with communication compliance**

Protecting sensitive information and detecting and acting on workplace harassment incidents is an important part of compliance with internal policies and standards.

[Microsoft Purview Communication Compliance](#) helps minimize these risks by helping you quickly detect, capture, and take remediation actions for email and Microsoft Teams communications. These include inappropriate communications containing profanity, threats, and harassment and communications that share sensitive information inside and outside of your organization.

## **Restrict communication and collaboration between users with information barriers**

[Microsoft Purview Information Barriers \(IB\)](#) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint Online, and OneDrive for Business. Often used in highly regulated industries, IB can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

## **Manage business, legal, or regulatory record-keeping requirements with records management**

[Microsoft Purview Records Management](#) helps an organization manage its legal obligations, provides the ability to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be retained, no longer of value, or no longer required for business purposes. For more information, see [Learn about records management](#).

## Log and search for audited activities in SharePoint and OneDrive with Audit (Premium) or Audit (Standard)

[Microsoft Purview auditing solutions](#) provide integrated solutions to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

For more information about auditing solutions, see [Audit \(Premium\)](#) and [Audit \(Standard\)](#).

## Identify and manage data for legal cases with eDiscovery (Premium) or eDiscovery (Standard)

Electronic discovery, or eDiscovery, is the process of identifying, collecting, and auditing electronic information for legal, regulatory, or business reasons. You can use [Microsoft Purview eDiscovery solutions](#) to search for data and content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results for analysis and review.

For more information about eDiscovery solutions, see [eDiscovery \(Premium\)](#) and [eDiscovery \(Standard\)](#).

## Get started with regulatory compliance

Organizations must comply with a complex and evolving web of policies, industry standards, and regional regulations, and also cope with the increasing cost of potential non-compliance. In fact, there are hundreds of updates per day from thousands of regulatory bodies, making it challenging to keep up to date with the rapidly changing compliance landscape. Microsoft Purview Compliance Manager and a detailed collection of compliance offerings can help your organization manage these regulatory requirements.

## Get started with Compliance Manager

[Microsoft Purview Compliance Manager](#) is a feature in the Microsoft Purview compliance portal that helps you manage your organization's compliance requirements with greater ease and convenience. Compliance Manager can help you throughout your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

## Learn about Microsoft regulatory compliance offerings

Microsoft offers a comprehensive set of [compliance offerings](#) to help your organization comply with national, regional, international, and industry-specific requirements governing the collection and use of data.

## Deploy Purview compliance solutions

Area-specific solutions bring together the technical guidance you need to understand, plan, and implement integrated compliance solutions for secure and compliant data collaboration:

- [Secure data with Zero Trust](#)
- [Deploy an information protection solution](#)
- [Deploy a data governance solution](#)
- [Deploy information protection for data privacy regulations](#)
- [Explore information protection & compliance illustrations](#)

## Next steps for organizations new to risk and compliance solutions

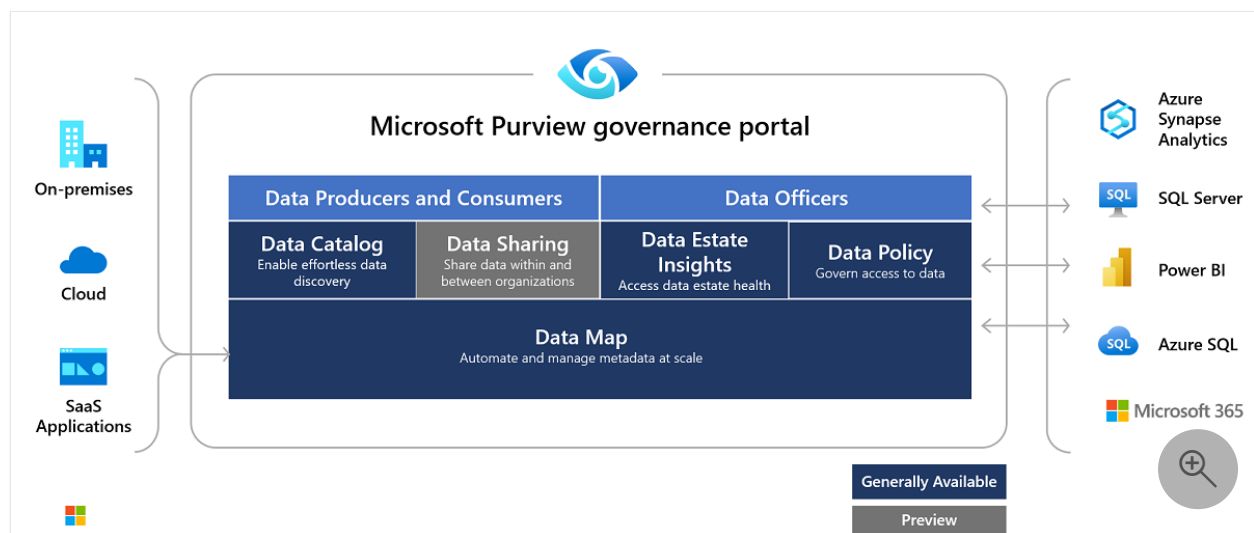
- [Learn about the Microsoft Purview solution trial](#)
- [Quick tasks for getting started with compliance in Microsoft Purview](#)

# What's available in the Microsoft Purview governance portal?

Article • 03/05/2023 • 9 minutes to read

Microsoft Purview's solutions in the governance portal provide a unified data governance service that helps you manage your on-premises, multicloud, and software-as-a-service (SaaS) data. The Microsoft Purview governance portal allows you to:

- Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.
- Enable data curators and security administrators to manage and keep your data estate secure.
- Empower data consumers to find valuable, trustworthy data.



## Tip

Looking to govern your data in Microsoft 365 by keeping what you need and deleting what you don't? Use **Microsoft Purview Data Lifecycle Management**.

## Data Map

Microsoft Purview automates data discovery by providing data scanning and classification for assets across your data estate. Metadata and descriptions of discovered data assets are integrated into a holistic map of your data estate. Microsoft Purview Data Map provides the foundation for data discovery and data governance. Microsoft Purview Data Map is a cloud native PaaS service that captures metadata about enterprise data present in analytics and operation systems on-premises and cloud.

Microsoft Purview Data Map is automatically kept up to date with built-in automated scanning and classification system. Business users can configure and use the data map through an intuitive UI and developers can programmatically interact with the Data Map using open-source Apache Atlas 2.2 APIs. Microsoft Purview Data Map powers the Microsoft Purview Data Catalog, the Microsoft Purview Data Estate Insights and the Microsoft Purview Data Policy as unified experiences within the [Microsoft Purview governance portal](#) [↗](#).

For more information, see our [introduction to Data Map](#).

Atop the Data Map, there are purpose-built apps that create environments for data discovery, access management, and insights about your data landscape.

App	Description
<a href="#">Data Catalog</a>	Finds trusted data sources by browsing and searching your data assets. The data catalog aligns your assets with friendly business terms and data classification to identify data sources.
<a href="#">Data Estate Insights</a>	Gives you an overview of your data estate to help you discover what kinds of data you have and where it is.
<a href="#">Data Sharing</a>	Allows you to securely share data internally or cross organizations with business partners and customers.
<a href="#">Data Policy</a>	A set of central, cloud-based experiences that help you provision access to data securely and at scale.

## Data Catalog app

With the Microsoft Purview Data Catalog, business and technical users can quickly and easily find relevant data using a search experience with filters based on lenses such as glossary terms, classifications, sensitivity labels and more. For subject matter experts, data stewards and officers, the Microsoft Purview Data Catalog provides data curation features such as business glossary management and the ability to automate tagging of data assets with glossary terms. Data consumers and producers can also visually trace the lineage of data assets: for example, starting from operational systems on-premises, through movement, transformation & enrichment with various data storage and processing systems in the cloud, to consumption in an analytics system like Power BI. For more information, see our [introduction to search using Data Catalog](#).

## Data Estate Insights app

With the Microsoft Purview Data Estate Insights, the chief data officers and other governance stakeholders can get a bird's eye view of their data estate and can gain actionable insights into the governance gaps that can be resolved from the experience itself.

For more information, see our [introduction to Data Estate Insights](#).

## Data Sharing app

Microsoft Purview Data Sharing enables organizations to securely share data both within your organization or cross organizations with business partners and customers. You can share or receive data with just a few clicks. Data providers can centrally manage and monitor data sharing relationships, and revoke sharing at any time. Data consumers can access received data with their own analytics tools and turn data into insights.

For more information, see our [introduction to Data Sharing](#).

## Data Policy app

Microsoft Purview Data Policy is a set of central, cloud-based experiences that help you manage access to data sources and datasets securely and at scale.

- Manage access to data sources from a single-pane of glass, cloud-based experience
- Enables at-scale access provisioning
- Introduces a new data-plane permission model that is external to data sources
- It is seamlessly integrated with Microsoft Purview Data Map and Catalog:
  - Search for data assets and grant access only to what is required via fine-grained policies.
  - Path to support SaaS, on-premises, and multicloud data sources.
  - Path to create policies that leverage any metadata associated to the data objects.
- Based on role definitions that are simple and abstracted (for example: Read, Modify)

For more information, see our introductory guides:

- [Data owner access policies](#) (preview): Provision fine-grained to broad access to users and groups via intuitive authoring experience.
- [Self-service access policies](#) (preview): Self-Service: Workflow approval and automatic provisioning of access requests initiated by business analysts that discover data assets in Microsoft Purview's catalog.

- **DevOps policies:** Provision IT operations personnel access to SQL system metadata, so that they can monitor performance, health and audit security, while limiting the insider threat.

Here are the benefits of the Data Policy app:

Principle	Benefit
<i>Simplify</i>	Permissions are bundled into role definitions that are abstracted and consistent across data source types, like Read and Modify.
	Reduce the need of permission expertise for each data source type.
<i>Reduce effort</i>	Graphical interface lets you navigate the data object hierarchy quickly.
	Supports policies on entire Azure resource groups and subscriptions.
<i>Enhance security</i>	Access is granted centrally and can be easily reviewed and revoked.
	Reduces the need for privileged accounts to configure access directly at the data source.
	Supports the Principle of Least Privilege via data resource scopes and common role definitions.

## Traditional challenges that Microsoft Purview seeks to address

### Challenges for data consumers

Traditionally, discovering enterprise data sources has been an organic process based on communal knowledge. For companies that want the most value from their information assets, this approach presents many challenges:

- Because there's no central location to register data sources, users might be unaware of a data source unless they come into contact with it as part of another process.
- Unless users know the location of a data source, they can't connect to the data by using a client application. Data-consumption experiences require users to know the connection string or path.

- The intended use of the data is hidden to users unless they know the location of a data source's documentation. Data sources and documentation might live in several places and be consumed through different kinds of experiences.
- If users have questions about an information asset, they must locate the expert, or team responsible for that data and engage them offline. There's no explicit connection between the data and the experts that understand the data's context.
- Unless users understand the process for requesting access to the data source, discovering the data source and its documentation won't help them access the data.

## Challenges for data producers

Although data consumers face the previously mentioned challenges, users who are responsible for producing and maintaining information assets face challenges of their own:

- Annotating data sources with descriptive metadata is often a lost effort. Client applications typically ignore descriptions that are stored in the data source.
- Creating documentation for data sources can be difficult and it's an ongoing responsibility to keep documentation in sync with data sources. Users might not trust documentation that's perceived as being out of date.
- Creating and maintaining documentation for data sources is complex and time-consuming. Making that documentation readily available to everyone who uses the data source can be even more so.
- Restricting access to data sources and ensuring that data consumers know how to request access is an ongoing challenge.

When such challenges are combined, they present a significant barrier for companies that want to encourage and promote the use and understanding of enterprise data.

## Challenges for security administrators

Users who are responsible for ensuring the security of their organization's data may have any of the challenges listed above as data consumers and producers, and the following extra challenges:

- An organization's data is constantly growing and being stored and shared in new directions. The task of discovering, protecting, and governing your sensitive data is one that never ends. You need to ensure that your organization's content is being shared with the correct people, applications, and with the correct permissions.



- Understanding the risk levels in your organization's data requires diving deep into your content, looking for keywords, RegEx patterns, and sensitive data types. For example, sensitive data types might include Credit Card numbers, Social Security numbers or Bank Account numbers. You must constantly monitor all data sources for sensitive content, as even the smallest amount of data loss can be critical to your organization.
- Ensuring that your organization continues to comply with corporate security policies is a challenging task as your content grows and changes, and as those requirements and policies are updated for changing digital realities. Security administrators need to ensure data security in the quickest time possible.

## Microsoft Purview advantages

Microsoft Purview is designed to address the issues mentioned in the previous sections and to help enterprises get the most value from their existing information assets. The catalog makes data sources easily discoverable and understandable by the users who manage the data.

Microsoft Purview provides a cloud-based service into which you can register data sources. During registration, the data remains in its existing location, but a copy of its metadata is added to Microsoft Purview, along with a reference to the data source location. The metadata is also indexed to make each data source easily discoverable via search and understandable to the users who discover it.

After you register a data source, you can then enrich its metadata. Either the user who registered the data source or another user in the enterprise can add more metadata. Any user can annotate a data source by providing descriptions, tags, or other metadata for requesting data source access. This descriptive metadata supplements the structural metadata, such as column names and data types that are registered from the data source.

Discovering and understanding data sources and their use is the primary purpose of registering the sources. Enterprise users might need data for business intelligence, application development, data science, or any other task where the correct data is required. They can use the data catalog discovery experience to quickly find data that matches their needs, understand the data to evaluate its fitness for purpose, and consume the data by opening the data source in their tool of choice.

At the same time, users can contribute to the catalog by tagging, documenting, and annotating data sources that have already been registered. They can also register new data sources, which are then discovered, understood, and consumed by the community of catalog users.

Lastly, Microsoft Purview Data Policy app provides a superior solution to keep your data secure.

## In-region data residency

Microsoft Purview processes data and stores metadata information, but does not store customer data. Data is processed in its data region, and customer metadata stays within the region where Microsoft Purview is deployed. For regions with data residency requirements, customer data stays within its region, and customer metadata is always kept within the same region where Microsoft Purview is deployed.

## Next steps

### Tip

Check if Microsoft Purview is available in your region on the [regional availability page](#) <sup>↗</sup>.

To get started with Microsoft Purview, see [Create a Microsoft Purview account](#).

---

## Additional resources

### Documentation

#### [Elastic data map - Microsoft Purview](#)

This article explains the concepts of the Elastic Data Map in Microsoft Purview

#### [Microsoft Purview security best practices - Microsoft Purview](#)

This article provides Microsoft Purview best practices.

#### [Understand data classification in the Microsoft Purview governance portal - Microsoft Purview](#)

This article explains the concepts behind data classification in the Microsoft Purview governance portal.

#### [Understand Insights reports in Microsoft Purview - Microsoft Purview](#)

This article explains what Insights are in Microsoft Purview.

#### [Microsoft Purview Data Map supported data sources and file types - Microsoft Purview](#)

This article provides details about supported data sources, file types, and functionalities in the

Microsoft Purview Data Map.

## **Deployment best practices for Microsoft Purview (formerly Azure Purview) - Microsoft Purview**

This article provides best practices for deploying Microsoft Purview (formerly Azure Purview) in your data estate. The Microsoft Purview Data Map and governance portal enable any user to register, discover, understand, and consume data sources.

## **Prerequisites to successfully deploy a Microsoft Purview (formerly Azure Purview) account - Microsoft Purview**

This tutorial lists a prerequisite checklist to deploy a Microsoft Purview (formerly Azure Purview) account.

## **How to: browse the Data Catalog - Microsoft Purview**

This article gives an overview of how to browse the Microsoft Purview Data Catalog by asset type

[Show 5 more](#)

## **Training**

Learning path

### **Govern data across an enterprise - Training**

Govern data across an enterprise

Certification

### **Microsoft Certified: Azure Enterprise Data Analyst Associate - Certifications**

Azure enterprise data analysts perform advanced data analytics at scale, such as cleaning and transforming data, designing and building enterprise data models, incorporating advanced analytics capabilities, integrating with IT infrastructure, and applying development lifecycle practices.