

# Governance, risk, and compliance overview

Article • 06/20/2024

## How does Microsoft provide effective security governance across the enterprise?

Microsoft understands that effective security policies must be implemented consistently across the enterprise to protect Microsoft information systems and customers. Security policies must also account for variations in business functions and information systems to be universally applicable. To meet these requirements, Microsoft implements a comprehensive security governance program as a part of the Microsoft Policy Framework. Security governance falls under the Microsoft Security Policy (MSP).

The MSP organizes Microsoft's security policies, standards, and requirements so they can be implemented across all Microsoft engineering groups and business units. Individual business units are responsible for specific implementations of Microsoft security policies. For example, Microsoft 365 documents its security implementations in the Microsoft 365 Information Security Policy and the related Microsoft 365 Control Framework. Azure and Dynamics 365 document their security implementations in the Standard Operating Procedures (SOPs) and the Azure Control Framework. These security implementations align with the goals and objectives of the MSP.

Microsoft's security governance program is informed by and aligns with various regulatory and compliance frameworks. Security requirements are constantly evolving to account for new technologies, regulatory and compliance requirements, and security threats. Because of these changes, Microsoft regularly updates our security policies and supporting documents to protect Microsoft systems and customers, meet our commitments, and maintain customer trust.

## How do Microsoft online services implement the Microsoft Security Policy (MSP)?

Microsoft 365 documents security implementations in the Microsoft 365 Information Security Policy. This policy aligns with the Microsoft Security Policy and governs the Microsoft 365 information system, including all Microsoft 365 environments and all resources involved in the collection, processing, maintenance, use, sharing,

dissemination, and disposal of data. Similarly, Azure and Dynamics 365 use the Microsoft Security Policy to govern their information system.

The information systems include the following components governed by the Microsoft 365 Information Security Policy (for Microsoft 365) and the Microsoft Security Policy (for Azure and Dynamics 365):

- Infrastructure: The physical and hardware components of Azure, Dynamics 365, and Microsoft 365 systems (facilities, equipment, and networks)
- Software: The programs and operating software of Azure, Dynamics 365, and Microsoft 365 systems (systems, applications, and utilities)
- People: The personnel involved in the operation and use of Azure, Dynamics 365, and Microsoft 365 systems (developers, operators, users, and managers)
- Procedures: The programmed and manual procedures involved in the operation of Azure, Dynamics 365, and Microsoft 365 systems
- Data: The information generated, collected, and processed by Azure, Dynamics 365, and Microsoft 365 systems (transaction streams, files, databases, and tables)

The Microsoft 365 Information Security Policy is supplemented by the Microsoft 365 Control Framework. The Microsoft 365 Control Framework details the minimum-security requirements for all Microsoft 365 services and information system components. It also references the legal and corporate requirements behind each control. The framework includes control activity names, descriptions, and guidance to ensure effective control implementations by service teams. Microsoft 365 uses the control framework to track control implementations for internal and external reporting. Similarly, Azure and Dynamics 365 record control implementations in the Azure Control Framework.

## **How do online services limit and track exceptions to established policies and procedures?**

All exceptions to the Control Frameworks must have legitimate business justification and be approved by an appropriate governance entity within each online services team. Depending on the scope of the exception and the potential risk it represents, approval for exceptions may need to be obtained from a corporate vice president or higher. Exceptions are managed in a tracking tool where they are reviewed and approved for continued relevance.

# How does Microsoft assess and manage risk across the enterprise?

Risk management is the process of identifying, assessing, and responding to threats or events that can impact Company or customer objectives. Risk management at Microsoft is designed to anticipate new threats and provide ongoing security for our cloud systems and the customers who use them.

Microsoft's risk management aligns to the Enterprise Risk Management (ERM) framework. ERM enables the overall enterprise risk management process and works with management across the enterprise to identify and ensure accountability for Microsoft's most significant risks.



Microsoft ERM enables common risk management principles across the enterprise so business units can independently facilitate consistent and comparative risk assessments. This coordination gives Microsoft the ability to aggregate and report risk information in a consolidated manner for management. ERM provides business units in Microsoft with common methodologies, tools, and goals for the risk management process. Microsoft 365 and other engineering groups and business units use these tools to conduct individual risk assessments as part of their own risk management programs under the guidance of ERM.

# How do Microsoft online services work with ERM?

Each online service follows ERM guidance to manage risks across Microsoft services. The program focuses on aligning the ERM framework with existing Microsoft engineering, service operations, and compliance processes, making the Risk Management program more effective and efficient. Each online service's risk management activities ultimately roll up into and inform the ERM process.

As part of risk assessment activities, each online service analyzes design and operating effectiveness of controls implemented as part of the Microsoft Controls Framework (Framework). The Framework is a rationalized set of controls that, when properly implemented along with supporting compliance activities, allows engineering teams to comply with key regulations and certifications.

## How do online services keep security and compliance requirements updated?

Governance, Risk, and Compliance teams of each online service (GRC) work to maintain the Control Framework on an ongoing basis. Several scenarios may require the GRC team to update the control framework, including changes in relevant regulations or laws, emerging threats, penetration test results, security incidents, audit feedback, and new compliance requirements. When a framework change is required, the Trust team identifies key stakeholders responsible for approving and implementing the change to ensure it is feasible and will not cause unintended issues with Online services. Once the GRC team and relevant stakeholders agree on what the change requires, the workloads responsible for implementing the change set target completion dates and work to implement the change within their respective services. After implementation targets have been met, the Trust team updates the control framework with the new or updated controls.

## Related external regulations & certifications

Microsoft's online services are regularly audited for compliance with external regulations and certifications. Refer to the following table for validation of controls related to governance, risk, and compliance.



### Azure and Dynamics 365

[Expand table](#)

External audits	Section	Latest report date
<a href="#">ISO 27001</a> <a href="#">↗</a> <a href="#">Statement of Applicability</a> <a href="#">↗</a> <a href="#">Certificate</a> <a href="#">↗</a>	A.5: Information security policies A.18.1: Compliance with legal and contractual requirements A.18.2: Information security reviews	November 21, 2024
<a href="#">ISO 27017</a> <a href="#">↗</a> <a href="#">Statement of Applicability</a> <a href="#">↗</a> <a href="#">Certificate</a> <a href="#">↗</a>	A.5: Information security policies A.18.1: Compliance with legal and contractual requirements A.18.2: Information security reviews	November 21, 2024
<a href="#">ISO 27018</a> <a href="#">↗</a> <a href="#">Statement of Applicability</a> <a href="#">↗</a> <a href="#">Certificate</a> <a href="#">↗</a>	A.5: Information security policies	November 21, 2024
<a href="#">ISO 22301</a> <a href="#">↗</a> <a href="#">Certificate</a> <a href="#">↗</a>	6.1.1: Determining risks and opportunities 6.1.2: Addressing risks and opportunities	November 21, 2024
<a href="#">SOC 1</a> <a href="#">↗</a>	IS-1: Microsoft security policy IS-2: Microsoft security policy review IS-3: Security roles and responsibilities	August 16, 2024
<a href="#">SOC 2</a> <a href="#">↗</a> <a href="#">SOC 3</a> <a href="#">↗</a>	C5-1: Standard operating procedures IS-1: Microsoft security policy IS-2: Microsoft security policy review IS-3: Security roles and responsibilities SOC2-14: Confidentiality and non-disclosure agreements SOC2-18: Statutory, regulatory, and contractual requirements SOC2-19: Cross-functional compliance program SOC2-20: ISMS program SOC2-26: Annual risk assessment	February 18, 2025

## Microsoft 365

[Expand table](#)

External audits	Section	Latest report date
<a href="#">FedRAMP</a> 	CA-2: Security assessments CA-5: Plan of action and milestones PL-2: System security plan RA-3: Risk assessment	August 21, 2024
<a href="#">ISO 27001/27017</a>   <a href="#">Statement of Applicability</a>  <a href="#">Certification (27001)</a>  <a href="#">Certification (27017)</a> 	A.5: Information security policies A.18.1: Compliance with legal and contractual requirements A.18.2: Information security reviews	March 2025
<a href="#">SOC 1</a> 	CA-03: Risk management	August 1, 2024
<a href="#">SOC 2</a> 	CA-02: Governance, risk, and compliance team responsibilities CA-03: Risk management CA-11: Policy framework updates CA-17: Microsoft security policy CA-24: Internal risk assessment CA-25: Control framework updates	February 26, 2025

## Resources

- [Microsoft Security Policy](#) 
- [Microsoft Security Program Policy](#) 

## Feedback

Was this page helpful?

 Yes

 No

# Microsoft 365 Risk Management program

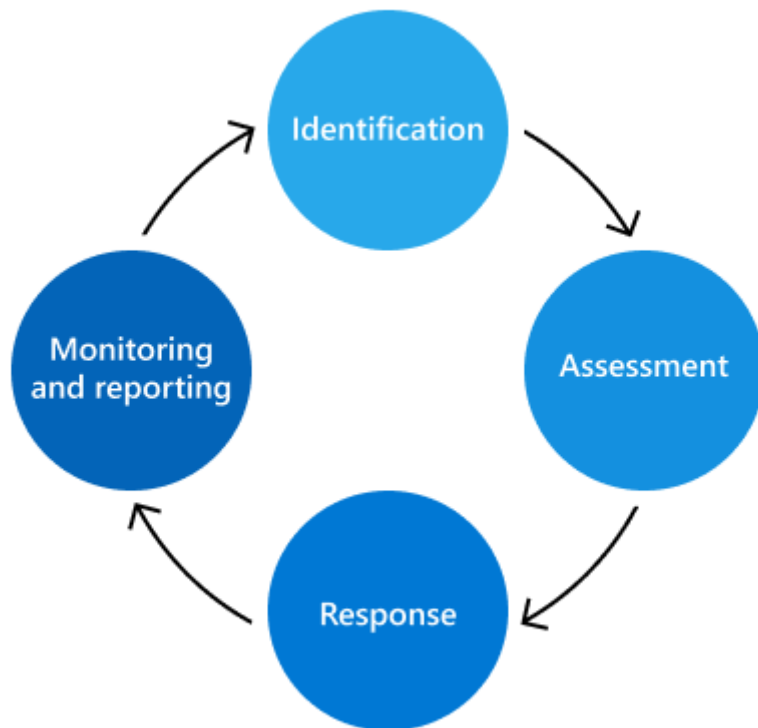
Article • 06/24/2024

The purpose of the Microsoft 365 Risk Management program is to identify, assess, and manage risks to Microsoft 365. Microsoft's top priority is to proactively identify and address risks that could impact our service infrastructure, as well as our customers, their data, and their trust. In addition, a robust risk management program is necessary to meet contractual obligations and maintain public accreditations that our customers rely on to satisfy their own compliance requirements. While the Microsoft 365 Risk Management program functions independently, it aligns with the overarching Enterprise Risk Management (ERM) program's policies, priorities, and methodologies. Working with the ERM program allows for consistent comparison across business units and engineering groups, contributing to a more cohesive approach to risk management across the enterprise.

The Microsoft 365 Trust team is responsible for managing the Microsoft 365 Risk Management program and conducting the activities defined by the ERM program. The Trust team focuses on integrating the risk management framework with existing Microsoft 365 engineering, service operations, and compliance process to make the Risk Management program more effective and efficient.

The Trust team also maintains the Microsoft 365 Controls Framework, a set of rationalized controls that, when properly implemented with supporting compliance activities, allows engineering teams to comply with key regulations and certifications. This framework is continuously updated based on feedback and findings as part of the risk management process.

Risk management activities fall into four phases: identification, assessment, response, and monitoring and reporting.



## Identification

The risk management process starts with identifying all possible risks to all key control areas, internal and external threats, and vulnerabilities in the Microsoft 365 environment. The information guiding this process comes from multiple sources including interviews, vulnerability scans, attack simulation exercises, audit findings, and incident management activities.

The Trust team interviews subject matter experts (SMEs) from multiple service teams on previously identified risks and potential future risks that may be introduced as the services grow. Additionally, SMEs help to validate the accuracy and completeness of risks identified from the other continuous monitoring sources.

The identification phase is also when decision logs, active security and compliance exceptions, and mitigation work from previous risk assessments are reviewed.

## Assessment

Each identified risk is assessed using three metrics: impact, likelihood, and control deficiency.

- Impact refers to the damage that would occur to the service, business, or Microsoft if that risk were to be realized. The impact to Microsoft may include damage to reputation, loss of customers, or legal/compliance implications.



- Likelihood defines the probability of the potential risk being realized and is calculated by analyzing the probability and frequency with which it will occur.
- Control deficiency measures the effectiveness of implemented mitigation controls.

These metrics are used to calculate a risk score that represents the severity of each risk, accounting for existing mitigation strategies. Risks are aggregated and presented to key stakeholders from each service to verify the accuracy and completeness of Microsoft 365's risk posture.

## Response

Using the verified list of risks to Microsoft 365, the Trust team assigns risks to the affected service for risk response. Defined guidelines help determine the appropriate risk response strategy based on the risk score and control effectiveness. Risk response strategies fall into four categories:

- Tolerate: Areas of low-risk exposure with a low level of control.
- Operate: Areas of low-risk exposure where controls are deemed adequate.
- Monitor: Areas of high-risk exposure where controls are deemed adequate and should be monitored for effectiveness.
- Improve: Areas of high-risk exposure with a low level of control that are top priorities in addressing.

The Trust team coordinates with service teams to develop plans for addressing each risk. The severity level determines the appropriate level of review and approval for each plan. For risks that require action, existing engineering bug processes are used for tracking, managing, and making exception decisions. Using a process familiar to the engineering and operation teams makes risk response more efficient and effective.

## Monitoring and reporting

Risks identified as part of the risk assessment are monitored and reported to relevant stakeholders. Monitoring strategies include security monitoring, periodic risk reviews, penetration testing, and vulnerability scanning. These monitoring efforts act as data sources for reporting on key performance indicators, creating dashboards, and developing formal reports, all of which inform future risk decisions.

Multiple times a year, the Trust team meets with risk owners from each service to review risk scores, evaluate the effectiveness of their action plans, and make updates where needed. In addition, Microsoft 365's risk assessment activities contribute to the ERM

program's Enterprise Risk Assessments, which provide a high-level overview of Microsoft's risk posture to Microsoft senior management and the ERM program.

---

## Feedback

Was this page helpful?



Yes



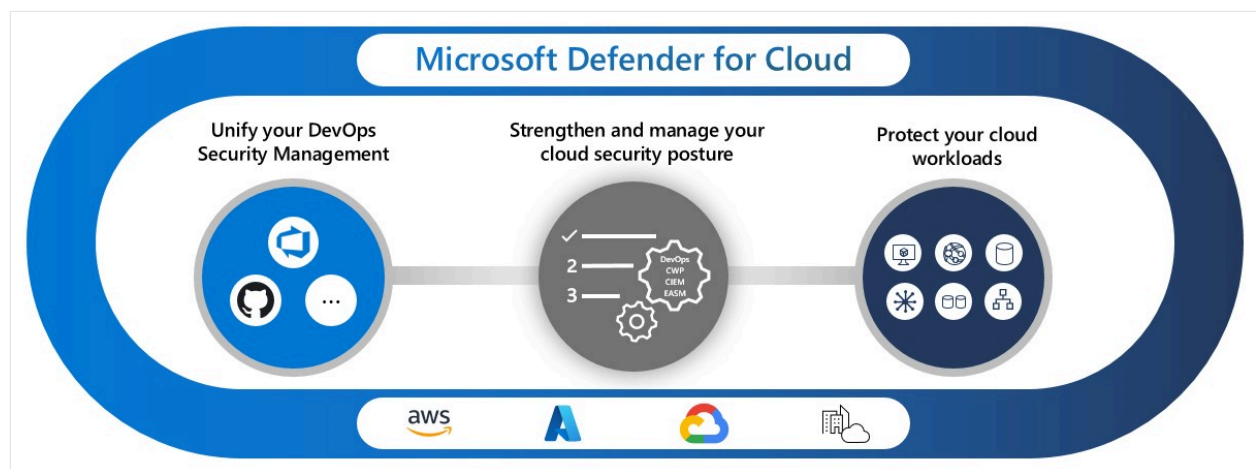
No

# Microsoft Defender for Cloud overview

Article • 02/25/2025

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) that includes security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud includes:

- A development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multi-pipeline environments
- A cloud security posture management (CSPM) solution that identifies actions to prevent breaches
- A cloud workload protection platform (CWPP) with protections for servers, containers, storage, databases, and other workloads



## ⓘ Note

For Defender for Cloud pricing information, see the [pricing page](#).

The Microsoft 365 Defender portal helps security teams investigate attacks on cloud resources, devices, and identities. Microsoft 365 Defender provides an overview of attacks, including suspicious and malicious events in cloud environments. Microsoft 365 Defender achieves this by correlating all alerts and incidents, including cloud alerts and incidents.

Learn more about the [integration between Microsoft Defender for Cloud and Microsoft Defender XDR](#).

## Secure cloud applications

Defender for Cloud helps you incorporate good security practices early in the software development process, or DevSecOps. You can protect your code management environments and code pipelines, and get insights into your development environment security posture from a single location. Defender for Cloud enables security teams to manage DevOps security across multi-pipeline environments.

Today's applications require security awareness at the code, infrastructure, and runtime levels to ensure that deployed applications are hardened against attacks.

[Expand table](#)

Capability	What problem does it solve?	Get started	Defender plan
<a href="#">Code pipeline insights</a>	Empowers security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, including GitHub, Azure DevOps, and GitLab. DevOps security findings, such as Infrastructure as Code (IaC) misconfigurations and exposed secrets, can then be correlated with other contextual cloud security insights to prioritize remediation in code.	Connect <a href="#">Azure DevOps</a> , <a href="#">GitHub</a> , and <a href="#">GitLab</a> repositories to Defender for Cloud	Foundational CSPM (Free) and Defender CSPM

## Improve your security posture

The security of your cloud and on-premises resources relies on proper configuration and deployment. Defenders for Cloud recommendations identify steps to secure your environment.

Defender for Cloud includes free Foundational CSPM capabilities. Enable advanced CSPM capabilities with the Defender CSPM plan.

[Expand table](#)

Capability	What problem does it solve?	Get started	Defender plan
<a href="#">Centralized policy management</a>	Define the security conditions that you want to maintain across your environment. The policy translates to recommendations that identify resource configurations that violate your security policy. The <a href="#">Microsoft cloud security benchmark</a> is a built-in standard that applies security principles with detailed technical implementation	<a href="#">Customize a security policy</a>	Foundational CSPM (Free)

Capability	What problem does it solve?	Get started	Defender plan
	guidance for Azure and other cloud providers (such as Amazon Web Services (AWS) and Google Cloud Platform (GCP).		
<a href="#">Secure score</a>	Summarize your security posture based on the security recommendations. As you remediate recommendations, your secure score improves.	<a href="#">Track your secure score</a>	Foundational CSPM (Free)
<a href="#">Multicloud coverage</a>	Connect to your multicloud environments with agentless methods for CSPM insight and CWP protection.	Connect your <a href="#">Amazon AWS</a> and <a href="#">Google GCP</a> cloud resources to Defender for Cloud	Foundational CSPM (Free)
<a href="#">Cloud Security Posture Management (CSPM)</a>	Use the dashboard to see weaknesses in your security posture.	<a href="#">Enable CSPM tools</a>	Foundational CSPM (Free)
<a href="#">Advanced Cloud Security Posture Management</a>	Get advanced tools to identify weaknesses in your security posture, including: <ul style="list-style-type: none"> <li>- Governance to drive actions to improve your security posture</li> <li>- Regulatory compliance to verify compliance with security standards</li> <li>- Cloud security explorer to build a comprehensive view of your environment</li> </ul>	<a href="#">Enable CSPM tools</a>	Defender CSPM
<a href="#">Data Security Posture Management</a>	Data security posture management automatically discovers datastores containing sensitive data, and helps reduce risk of data breaches.	<a href="#">Enable data security posture management</a>	Defender CSPM or Defender for Storage
<a href="#">Attack path analysis</a>	Model traffic on your network to identify potential risks before you implement changes to your environment.	<a href="#">Build queries to analyze paths</a>	Defender CSPM
<a href="#">Cloud Security Explorer</a>	A map of your cloud environment that lets you build queries to find security risks.	<a href="#">Build queries to find security risks</a>	Defender CSPM
<a href="#">Security governance</a>	Drive security improvements through your organization by assigning tasks to resource owners and tracking progress in aligning your security state with your security policy.	<a href="#">Define governance rules</a>	Defender CSPM

Capability	What problem does it solve?	Get started	Defender plan
<a href="#">Microsoft Entra Permissions Management</a>	Provide comprehensive visibility and control over permissions for any identity and any resource in Azure, AWS, and GCP.	<a href="#">Review your Permission Creep Index (CPI)</a>	Defender CSPM

## Protect cloud workloads

Proactive security principles require implementing security practices to protect your workloads from threats. Cloud workload protections (CWP) provide workload-specific recommendations to guide you to the right security controls to protect your workloads.

When your environment is threatened, security alerts immediately indicate the nature and severity of the threat so you can plan your response. After identifying a threat in your environment, respond quickly to limit the risk to your resources.

 Expand table

Capability	What problem does it solve?	Get started	Defender plan
Protect cloud servers	Provide server protections through Microsoft Defender for Endpoint or extended protection with just-in-time network access, file integrity monitoring, vulnerability assessment, and more.	<a href="#">Secure your multicloud and on-premises servers</a>	Defender for Servers
Identify threats to your storage resources	Detect unusual and potentially harmful attempts to access or exploit your storage accounts using advanced threat detection capabilities and Microsoft Threat Intelligence data to provide contextual security alerts.	<a href="#">Protect your cloud storage resources</a>	Defender for Storage
Protect cloud databases	Protect your entire database estate with attack detection and threat response for the most popular database types in Azure to protect the database engines and data types, according to their attack surface and security risks.	<a href="#">Deploy specialized protections for cloud and on-premises databases</a>	<ul style="list-style-type: none"> <li>- Defender for Azure SQL Databases</li> <li>- Defender for SQL servers on machines</li> <li>- Defender for Open-source relational databases</li> <li>- Defender for</li> </ul>

Capability	What problem does it solve?	Get started	Defender plan
			Azure Cosmos DB
Protect containers	Secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications with environment hardening, vulnerability assessments, and run-time protection.	<a href="#">Find security risks in your containers</a>	Defender for Containers
<a href="#">Infrastructure service insights</a>	Diagnose weaknesses in your application infrastructure that can leave your environment susceptible to attack.	<ul style="list-style-type: none"> <li>- <a href="#">Identify attacks targeting applications running over App Service</a></li> <li>- <a href="#">Detect attempts to exploit Key Vault accounts</a></li> <li>- <a href="#">Get alerted on suspicious Resource Manager operations</a></li> <li>- <a href="#">Expose anomalous Domain Name System (DNS) activities</a></li> </ul>	<ul style="list-style-type: none"> <li>- Defender for App Service</li> <li>- Defender for Key Vault</li> <li>- Defender for Resource Manager</li> <li>- Defender for DNS</li> </ul>
<a href="#">Security alerts</a>	Get informed of real-time events that threaten the security of your environment. Alerts are categorized and assigned severity levels to indicate proper responses.	<a href="#">Manage security alerts</a>	Any workload protection Defender plan
<a href="#">Security incidents</a>	Identify attack patterns by correlating alerts and integrate with Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and IT classic deployment model solutions to respond to threats and reduce risk to your resources.	<a href="#">Export alerts to SIEM, SOAR, or ITSM systems</a>	Any workload protection Defender plan

As of August 1 2023, customers with an existing subscription to Defender for DNS can continue to use the service, but new subscribers will receive alerts about suspicious DNS activity as part of Defender for Servers P2.

## Learn More

For more information about Defender for Cloud and how it works, see:

- A [step-by-step walkthrough](#) of Defender for Cloud
- An interview about Defender for Cloud with an expert in cybersecurity in [Lessons Learned from the Field](#)
- [Microsoft Defender for Cloud - Use cases](#)
- [Microsoft Defender for Cloud PoC Series - Microsoft Defender for Containers](#)
- Learn how [Microsoft Defender for Cloud provides data security](#)

## Next steps

[Enable Microsoft Defender plans](#)

---

## Feedback

Was this page helpful?

 Yes


 No

[Provide product feedback](#) | [Ask the community](#)




# Learn about the new Microsoft Purview portal

Article • 12/05/2024

[Microsoft Purview](#) is a comprehensive set of solutions that can help you govern, protect, and manage data in your organization. The [Microsoft Purview portal](#)  has a streamlined design and unified experience that helps you discover and access data security, data governance, and risk and compliance solutions for all your data, wherever it lives across your data estate. The unified experience streamlines navigation for all Purview solutions and provides a single-entry point for settings, search, and roles and permissions management.

## Getting started with the portal

When you first navigate to and open the [Microsoft Purview portal](#) , a welcome dialog appears that provides a brief overview of the new portal experience. After agreeing to the terms and privacy conditions, select **Get started** to follow teaching bubbles that highlight key areas of the new portal experience.

Microsoft 365 Microsoft Azure Amazon Web Services Snowflake Other cloud platforms & apps

Connected to Microsoft Purview

## Welcome to the new Microsoft Purview portal!

The new Microsoft Purview portal brings together data governance, data security, and compliance solutions to help you quickly discover and protect data stored across platforms and apps including Microsoft 365, Microsoft Azure, Amazon Web Services, Snowflake, and more. [Learn more](#)

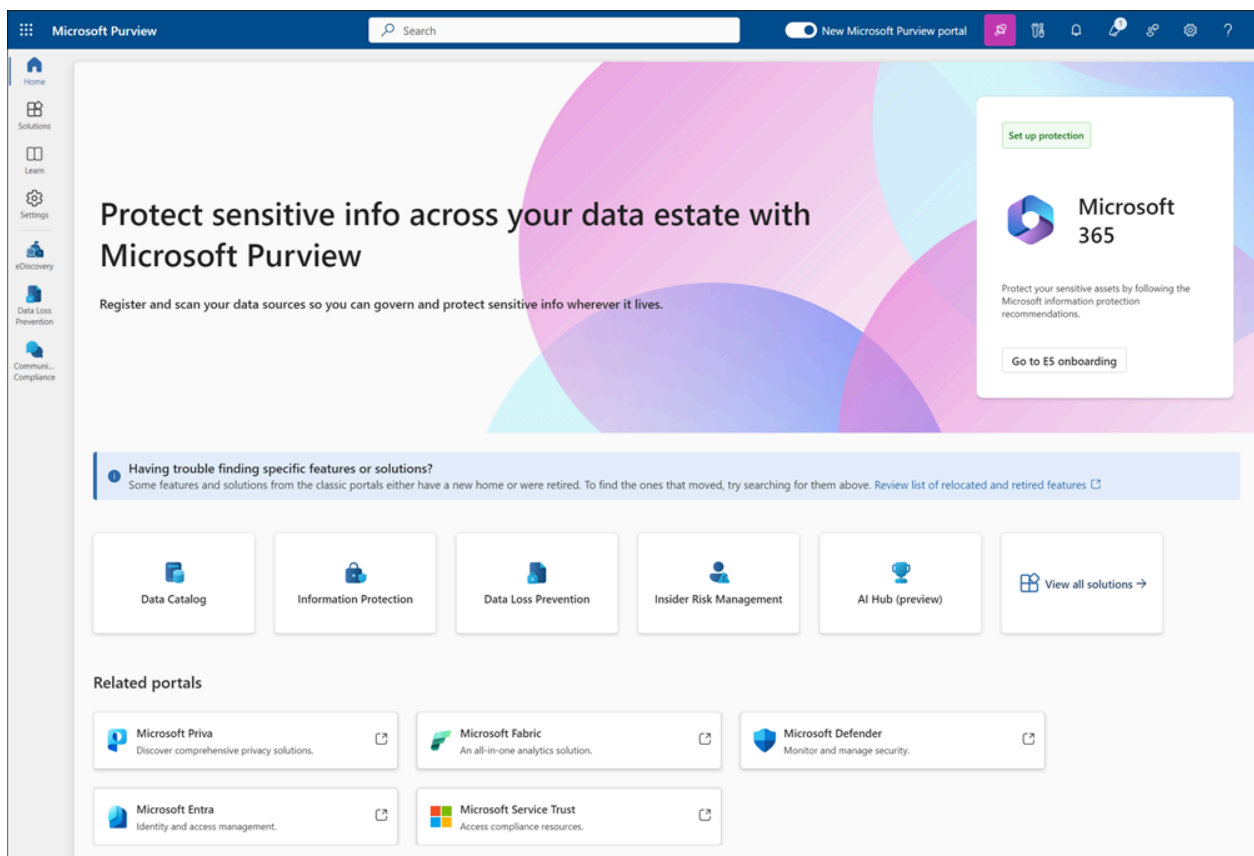
	Protect sensitive info across your data estate	Unified governance & compliance solutions	Upgraded, modern experience
New portal	✓	✓	✓
Classic portals	Limited support	Split between separate portals*	Classic look and feel

\*Microsoft Purview compliance portal and Microsoft Purview governance portal

☒ I agree to the [terms of data flow disclosure](#), and [Privacy Statements](#). \*

[Get started](#) [Go to classic portal](#)

Afterwards, you'll see the new home page displayed. The home page is your starting point for accessing all Microsoft Purview solutions, portal-wide settings, summary information about your data, and more.



## Relocated portal features

Some features and capabilities that you may have been familiar with when using the retired Microsoft Purview compliance portal and the [Microsoft Purview governance portal](#) are relocated or retired in the Microsoft Purview portal.

[Expand table](#)

Feature or capability	Summary of changes
Classification	Classification is renamed to <i>Classifiers</i> and moved to the left-navigation area for each solution.
Content Search	Content Search features are now included as core components in <a href="#">eDiscovery</a> .
Data Asset Search and Browse	Data Asset Search and Browse has moved to <b>Unified Catalog &gt; Data Search</b> .
Data Estate Insights	Data Estate Insights is renamed to <i>Data Estate Health Reports</i> and has moved to <b>Unified Catalog &gt; Data Estate Health &gt; Reports</b> .
Explorers	Explorers have moved to the left-navigation area for each solution.
Glossary	The glossary has moved to <b>Unified Catalog &gt; Business glossaries</b> .

Feature or capability	Summary of changes
Policies	Policies have moved to the left-navigation area for each solution.
Privacy Risk Management	<a href="#">Privacy Risk Management</a> is available in the Microsoft Priva portal.
Reports	Reports moved to the left-navigation area for each solution.
Roles and scopes	Roles and scopes are located in <b>Settings</b> .
Settings	Settings are located in the global left-navigation or at the top command bar of the portal. Select <b>Settings</b> to configure global and solution-level setting options.
Subject Rights Requests	<a href="#">Subject Rights Requests</a> is available in the Microsoft Priva portal.

## Permissions and subscriptions

Depending on your permissions and your Microsoft Purview subscription, you'll see different solutions, home page cards, and features in the portal. For example, if you have permissions and a supported subscription to access a specific data governance or risk and compliance solution (such as **Data Loss Prevention**, **Insider Risk Management**, etc.), you'll see these solution cards on the home page. If you don't have permissions or a supported subscription, you won't see these solution cards on the home page.


### ⓘ Note

Microsoft Purview permissions may be granted through security group membership. If you use Microsoft Entra Privileged Identity Management (PIM) for just-in-time membership for security groups in Microsoft Purview role groups, it could take up to 2 hours after activation for eligible administrators to have effective permissions applied in Microsoft Purview. For more information about PIM, see [What is Microsoft Entra Privileged Identity Management](#).

For more information about permissions and role groups in Microsoft Purview, see:

- [Permissions in the Microsoft Purview portal](#)
- [Roles and role groups in Microsoft Defender for Office 365 and Microsoft Purview portals](#)

For more information about Microsoft Purview subscription requirements, see:







- [Purview compliance solution requirements](#) 
- [Purview governance solution plan requirements](#)

## Global search

Use global search at the top of the portal to search for navigation, users, and resources across all your solutions and data estate. For terms entered in the search bar, you'll see applicable results grouped by the following sections in the search results drop down:

- **Navigation:** Results for items associated with specific Microsoft Purview solutions and solution features.
- **Users:** Results for users included in your organization. User details, including email, role groups, and administrative units assigned, are available when a user is selected. To view role groups for a user, the viewer must have the *Role management* role assigned that isn't restricted to an [administrative unit](#).
- **Resources:** Results for helpful resources associated with the searched term.

To view the consolidated search results page, select the links to view all results at the bottom of any section listed in the search results drop down or select the **Search** arrow on the right side of the search bar. To filter the displayed results by section on the search results page, select the **All**, **Navigation**, **Users**, or **Resources** link at the top of the page. To view all results in each section, select **Show more**.

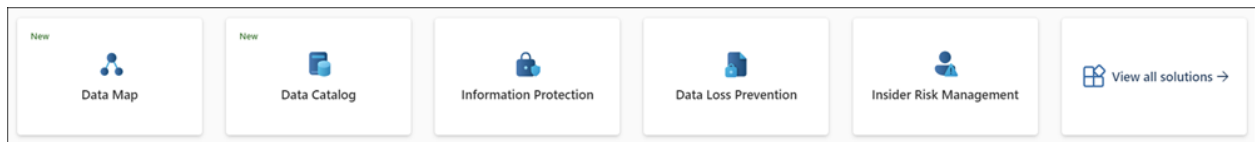
Search results for "data"	
<a href="#">All</a> <a href="#">Navigation (14)</a> <a href="#">Users (0)</a> <a href="#">Resources (80)</a>	
<b>Navigation (14)</b>	
Name	Description
 <a href="#">Solution settings &gt; Data Lifecycle Management</a>	Configure portal and solution settings. These can also be accessed any time from the Settings icon at the top of the portal.
 <a href="#">Solution settings &gt; Data Loss Prevention</a>	Configure portal and solution settings. These can also be accessed any time from the Settings icon at the top of the portal.
 <a href="#">Records Management &gt; Explorers &gt; Data explorer</a>	Automate and simplify the retention schedule for regulatory, legal, and business-critical records.
 <a href="#">Data Lifecycle Management</a>	Manage your content lifecycle so you can keep what you need and delete what you don't.
 <a href="#">Data Lifecycle Management &gt; Explorers &gt; Data explorer</a>	Manage your content lifecycle so you can keep what you need and delete what you don't.
 <a href="#">DSPM for AI &gt; Data assessments</a>	Discover and secure your org's AI data and activity within Microsoft Copilot experiences and other generative AI apps, in one central location.
<a href="#">Show more</a>	

The five most recently entered search terms are retained as quick links in the search bar for quick access to current results for these terms.

## Sections and cards


### Solution cards and the Solutions page


Solution cards on the portal home page allow you to quickly access and open the Microsoft Purview solutions that you have access to. The displayed view for these cards is predefined and can't be customized with specific cards.




To view and manage all solutions you have access to and that aren't listed in the solution card list, select **View all solutions**. From the **Solutions** page, you can select solutions in the **Core** section to set up and configure app experiences across Microsoft Purview or use the **Risk & Compliance**, **Data Governance**, and **Data Security** sections to directly view and manage specific Microsoft Purview solutions. Use the predefined filters to view solutions by area, or use the search box to find a specific solution by keyword. To explore learning materials (documentation, blogs, videos, and tutorials), select **Knowledge Center** in the **Resources** section.


**Core**  
Core capabilities to setting up and configuring solution experiences across Microsoft Purview.


**Audit**  
Search the audit log for user and admin activities across all locations and services.


**Settings**  
Configure portal and solution settings. These can also be accessed any time from the Settings icon at the top of the portal.


**Risk & Compliance**  
Manage critical risks and regulatory requirements.

**Communication Compliance**  
Capture inappropriate messages to help reduce communication risks and take steps to minimize harm.


**Compliance Manager**  
Get insight into your compliance posture and reduce risks with built-in assessments and recommended improvement actions.


**eDiscovery**  
Identify, preserve, and export data in response to legal discovery requests and eDiscovery cases.

**Information Barriers**  
Restrict two-way communication and collaboration to avoid conflicts of interest and safeguard internal info.


**Records Management**  
Automate and simplify the retention schedule for regulatory, legal, and business-critical records.


**Data Governance**  
Govern data seamlessly to empower your organization.


**Data Catalog**  
Find and curate data across your org with this searchable inventory of data assets and metadata.

**Data Lifecycle Management**  
Manage your content lifecycle so you can keep what you need and delete what you don't.

**Data Security**  
Secure data across its lifecycle, wherever it lives.

**Data Loss Prevention**  
Protect sensitive content as it's used and shared throughout your org - in the cloud, on-premises, and on devices.

**Information Protection**  
Discover, classify, and protect sensitive and business-critical content throughout its lifecycle.


**Insider Risk Management**  
Detect risky user activity to help quickly identify and take action on insider risks and threats.


## Related portals


Access related portals and solutions to help you manage all aspects of data analytics, data privacy, user identity, and more in your organization. These cards provide quick access to the following management and resource portals:


- [Microsoft Priva](#)
- [Microsoft Fabric](#)
- [Microsoft Defender](#)
- [Microsoft Entra](#)
- [Microsoft Service Trust](#)


### Related portals

**Microsoft Priva**  
Discover comprehensive privacy solutions.

**Microsoft Fabric**  
An all-in-one analytics solution.

**Microsoft Defender**  
Monitor and manage security.


**Microsoft Entra**  
Identity and access management.

**Microsoft Service Trust**  
Access compliance resources.

## Discover your data

The **Discover your data** card helps you discover your organization's data, see where it's stored, and understand how it's being used. You can use **Search the Unified Catalog** to quickly find the data you're looking for and filter search results by business terms, classifications, and contacts. You can also use **Open Unified Catalog** to open the [Unified Catalog solution](#) to further browse, search, and discover data assets across your organization.


### Discover your data

 Search Data Catalog

**Browse, search, and discover.**  
Understand and manage data across your hybrid data estate, automatic inventory data across the Microsoft Cloud. Use search to find the data you're looking for and filter search results by business terms, classifications, and contacts.

**Open Data Catalog**

### Recently accessed



**No activity yet**

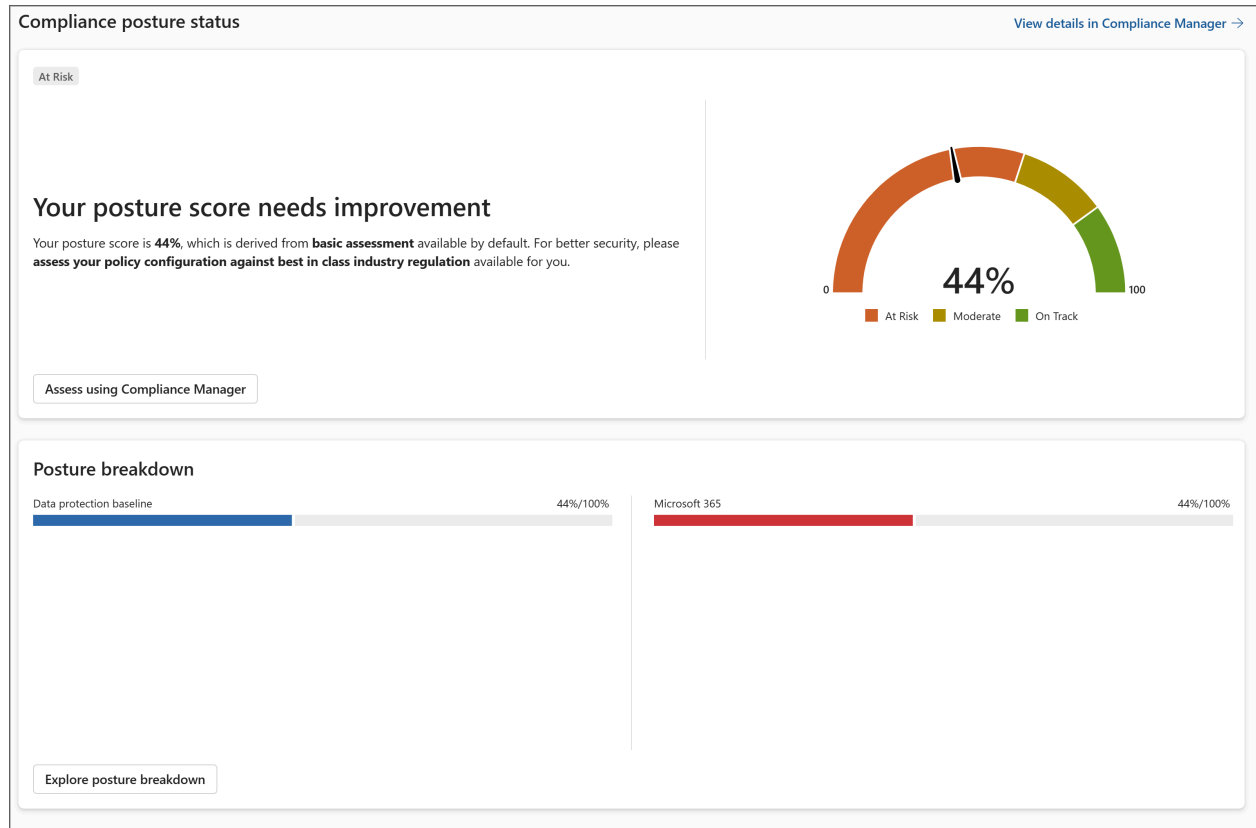
**Start browsing**

## Compliance posture status

This section includes cards that display summary information from the [Compliance Manager solution](#) about your organization's compliance posture. The percentages reflect progress toward completing the requirements of regulatory assessments. The



**Posture breakdown** section highlights completion rates for your organization's top assessments and the services covered by the assessments. Select **Assess using Compliance Manager** or **Explore posture breakdown** to visit Compliance Manager, where you can view, add, and manage assessments.



## Trials and recommendations

The **Trials and recommendations** card displays information and links to help you get started with trial solutions for specific Microsoft Purview solutions. Select **View all trials and recommendations** to discover more security and compliance capabilities in Microsoft Purview you can try for free.

Trials and recommendations [View all trials and recommendations >](#)

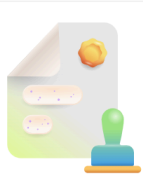
**Microsoft Priva**  
● Your trial is active

### Powerful insights are ready for you

Explore how Priva can help your organization address privacy risks and stay on track with data privacy regulations.

[Visit Priva](#)  
[Trial user guide](#)

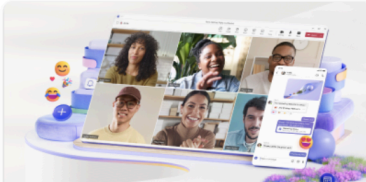
[View purchase options](#) [End trial](#)



### Compliance assessments

Compliance Manager's regulatory assessment templates helps your org assess risks and efficiently respond to national, regional and industry-specific requirements.

[Try now](#) [Learn more](#)



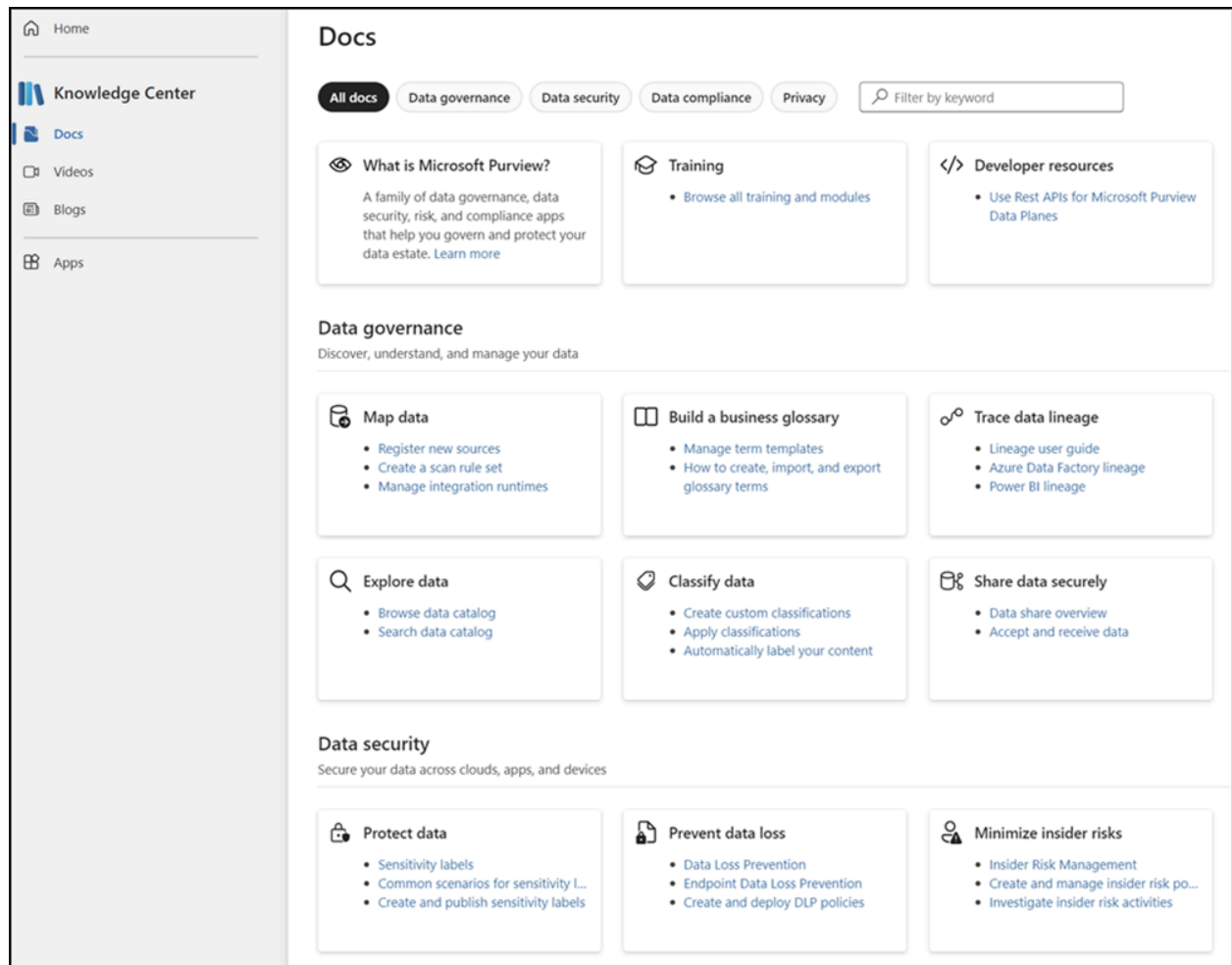
### Microsoft Teams Premium

Built on the familiar, all-in one collaboration experience of Teams, Teams Premium makes every meeting from 1:1s to town halls, virtual appointments to webinars more personalized, intelligent, and protected.

[Try now](#) [Learn more](#)

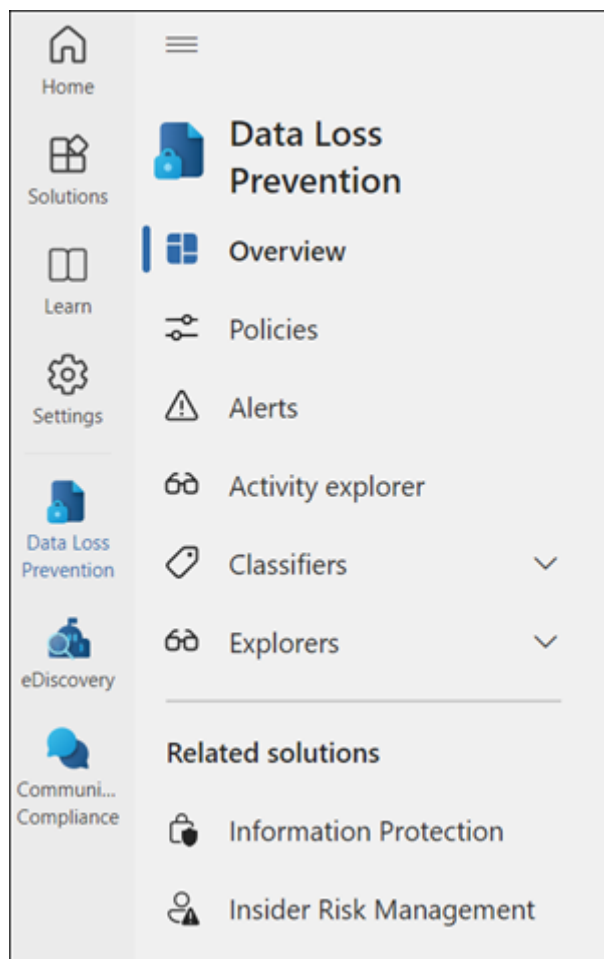
# Knowledge Center

The **Knowledge Center** card highlights articles, product demos, tutorials, and other learning materials to help you succeed with Microsoft Purview. Select **Go to the Knowledge Center** to open the **Knowledge Center** page and to view all available learning materials. Use the predefined filters to view knowledge center items by solution area, or use the search box to find a specific item by keyword.



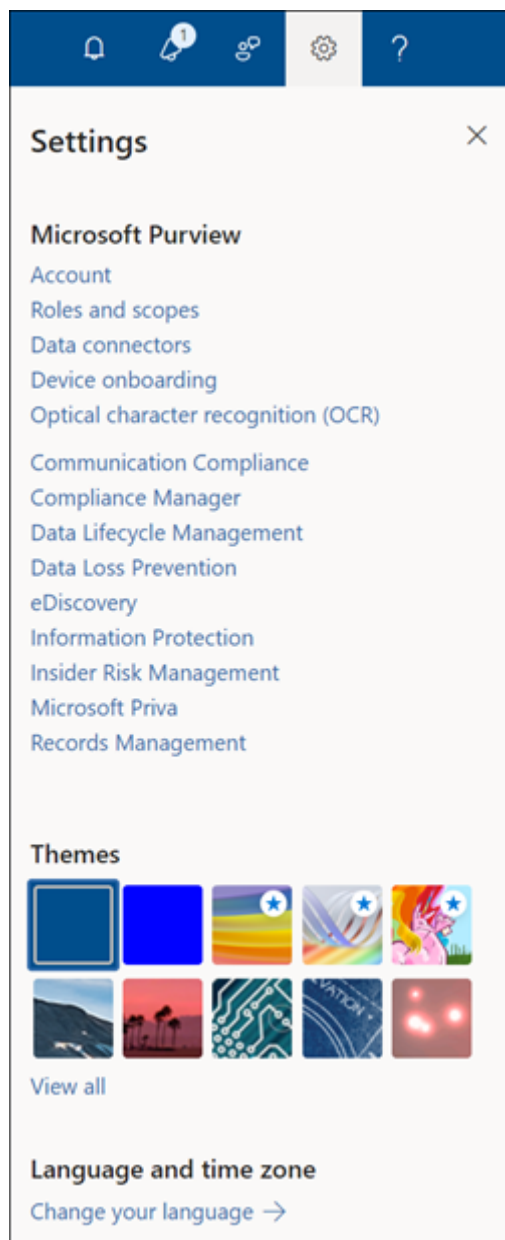
## New left navigation for solutions

When you select a Microsoft Purview solution in the portal, you'll see a solution-specific home page and a new left-navigation experience that allows you to access all solution features, settings, and more. The new left-navigation displays links to the **Home**, **Solutions**, **Learn**, and **Settings** pages for quick and easy access to these areas for managing solutions, learning more about Microsoft Purview, configuring solution settings, and more. Additionally, links to the five most recent Microsoft Purview solutions are also displayed for quick access to these solutions.



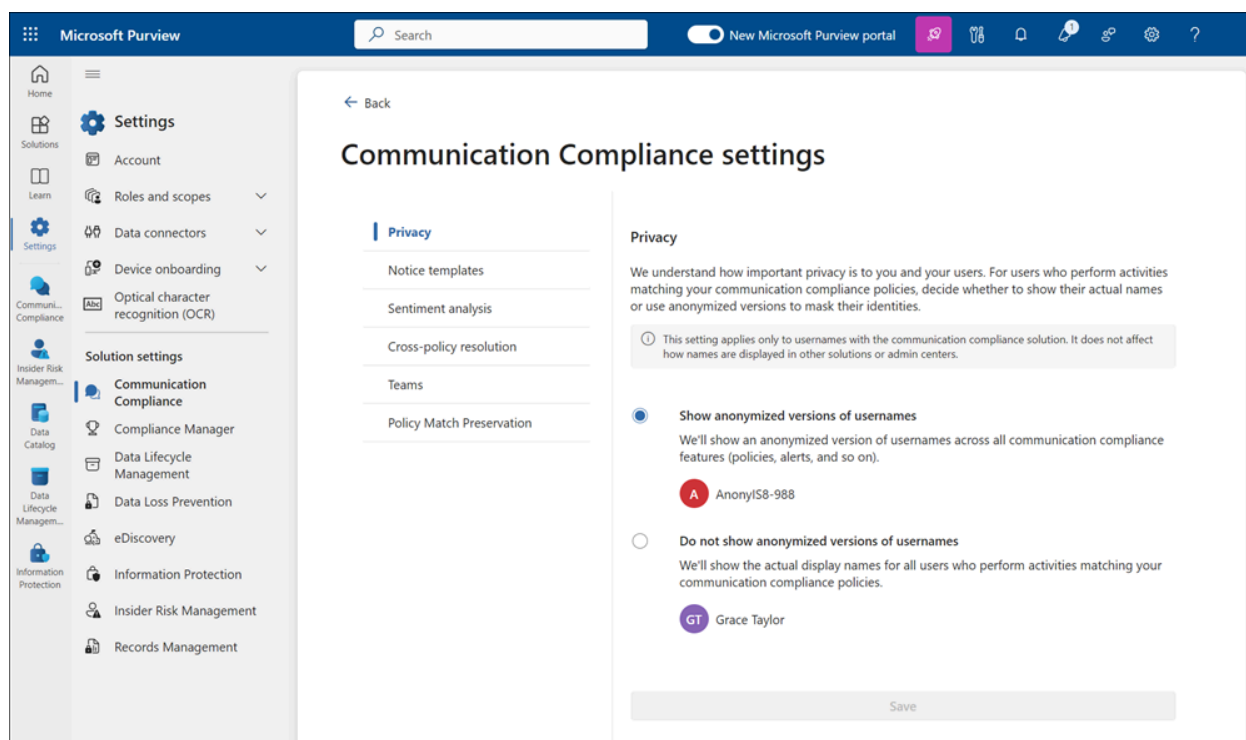
## Settings in the portal

Settings in the Microsoft Purview portal are now centralized and persist in one location at the top of the portal page. By selecting the **Settings** icon in the left navigation or at the top of the page, you can quickly manage solution and global portal-wide settings, no matter where you are in the portal.



To view and manage portal-wide settings, select options in the **Themes**, **Language and time zone**, **Password**, and **Contact preferences** sections.

To view and manage solution settings, select a solution. This opens the settings page for the solution where you can update settings for the selected solution. From any solutions settings page, you can also select other Purview solutions in the **Solution settings** area in the left navigation to view and update settings in these solutions. To view and manage account settings, select **Account**.



## Release notes and updates

View the latest release notes for Purview solutions in a centralized location by selecting the **Release notes & updates** icon in the top right command bar. You can view [Message center](#) announcements for solutions that give you a high-level overview of a planned update or change and how it may affect your users or organization. Select the associated **Learn more** link to view the announcement and more details on the Message Center.

## Help and support

Select the **Help** icon in the top right command bar to access specific help and support options for Microsoft Purview solutions:

- **Guided tours:** Start an integrated dialog driven overview of key features and capabilities in the Microsoft Purview portal.
- **Knowledge Center:** Quick access to the Knowledge Center that contains highlights articles, product demos, tutorials, and other learning materials to help you succeed with Microsoft Purview.
- **Need help?:** Select specific solution areas for self-help or share what you need help with so we can get you the right help and support.

For solution-specific help and support, we recommend selecting a specific solution in the drop-down field in the **Need help** section and selecting **Get help**. For example, if

you need help with data loss prevention (DLP) policies, you'd select *Data Loss Prevention*, then **Get help**. On the **Help** tab, enter the details for your help request.

Self Help

Contact Support

Support History

## How can we help?

Tell us your problem so we can get you the right help and support.

How do I configure DLP policies

X

→

AI-generated content ⓘ

To configure DLP policies, please follow these steps:

1. Go to [Configure endpoint DLP settings](#) <sup>[1]</sup> and follow the instructions provided.
2. To learn more about conditions and actions for the devices supported, see [Data Loss Prevention policy reference](#) <sup>[1]</sup>.
3. Endpoint DLP supports monitoring of the file types through policy. For more info, see [Monitored files](#) <sup>[1]</sup>.
4. For more information, see [Learn about Endpoint data loss prevention and Get started with Endpoint data loss](#)

Show more

Is this helpful?

Yes

No

More Help

Create and deploy a data loss prevention policy | Microsoft...

MICROSOFT SUPPORT

Data Loss Prevention policy reference - This article introduces all the components of a DLP policy and how each one influences t...

Configure endpoint DLP settings | Microsoft Learn

MICROSOFT SUPPORT

To work with the DLP alert management dashboard: In the Microsoft Purview portal, navigate to Data loss prevention > ...

Contact support

ⓘ **Note**

AI and article suggestions in help and support may not be available for some Purview solutions. Check back frequently for updates about upcoming availability for these solutions in help and support.

## Submit feedback about the new portal

Select the **Feedback** icon in the top right command bar to provide your feedback to Microsoft about the new Microsoft Purview portal. Provide as much detail as you'd like, but don't include any private or sensitive information. After entering your feedback, select **Submit** to send your suggestions to Microsoft to help improve the portal experience.

## Get started with data governance solutions

Getting started with data governance solutions in the Microsoft Purview portal depends on your organization's current relationship with Microsoft Purview data governance solutions.

- If your organization hasn't created a Microsoft Purview account in the Azure portal, [read about the new experience here](#).
- If your organization has Microsoft Purview accounts in the Azure portal, [read about the new experience here](#).

## New experience for new customers

If your organization doesn't have any Microsoft Purview accounts in any subscriptions under your Microsoft Entra tenant, you can get started with our governance solutions right away. Use the new [Microsoft Purview portal](#) <sup>↗</sup> to start your journey with the free version of Microsoft Purview.

## Free version of Microsoft Purview data governance solutions

If you're new to Microsoft Purview data governance solutions, you'll start in the [free version](#) of Microsoft Purview.

Only a core subset of Microsoft Purview's governance solutions with limited capabilities are currently available in the free version:

- [Catalog](#): Browse and search for your data assets.
- [Data Map history](#): A log of updates made to assets.

Currently, the free version of Microsoft Purview governance solutions supports these governance data sources using [live view](#):

- Azure Blob Storage
- Azure Data Lake Storage Gen 2
- Azure SQL Database
- Azure subscriptions

- [Microsoft Fabric](#)

You can annotate and curate assets that are available via [live view](#), or [use our APIs to create new entities](#).

The free version is limited; therefore it's recommended only for initial evaluation, development, and test scenarios. If you want to use all of Microsoft Purview's data governance features, it's recommended to [upgrade to the enterprise version](#).

For more information about limitations in the free version of Microsoft Purview, see our documentation on [what's in the free version of Microsoft Purview data governance solutions](#). To try out Microsoft Purview and get started on your data governance journey, see our [guide to getting started with the free version of Microsoft Purview data governance solutions](#).

## Enterprise version

You can get started with the enterprise version of Microsoft Purview by [upgrading from the Microsoft Purview portal](#). Upgrading to enterprise gives you and your user's access to all of Microsoft Purview's data governance features, including:

- [All of Microsoft Purview's supported governance sources](#) - manage data sources across your multicloud environment
- [Collections](#) - fine grained access control for users across your environment
- [Scanning](#) - gather your sources' technical metadata and lineage information
- [Automatic classification](#) - classify your data to identify important and sensitive information
- [Microsoft Purview policies](#) - govern data at the source from Microsoft Purview
- [All reports in Data Estate Insights](#) - understand your data estate at a glance
- [Workflows](#) - automate governance in your environment
- etc.

For more information about Microsoft Purview's governance solutions, [see our overview article](#).

## New experience for existing data governance customers

The new experience is an enhancement to the current Microsoft Purview data governance experience, and doesn't impact the information already stored in your accounts or your ability to use our APIs. When you upgrade to the new experience, you'll have automatic access to the enterprise version of Microsoft Purview, which has all the features you already use, and these new features:



- [This new Microsoft Purview portal](#): the latest platform to manage your organization's data governance.
- [Live view](#): view your Azure data assets in the Microsoft Purview Unified Catalog automatically and in real time with no need to register or set up a scan for the source.
- [Tenant-level administration](#): we've added roles that give you the ability to delegate administration from the tenant level, while maintaining fine-grained access control options to limit permissions by role and collections. This gives your team flexibility when managing access and responsibilities.
- [Data map history](#): a log of updates made to data assets, so you can audit changes in your data map.

To get started in this new experience, see our [guide to getting started with data governance in the new Microsoft Purview portal](#).

---

## Feedback

Was this page helpful?

 Yes

 No