



Crash Course in Microsoft Purview:

A guide to securing and
managing your data estate

Table of Contents

How to secure and manage your most important asset—your data	3
1 Data visibility and governance Discover, understand, and govern data across clouds and platforms	5
2 Data loss prevention Safeguard data wherever it lives	11
3 Data risk management Identify, manage, and reduce insider risk and other potential data vulnerabilities	17
Go beyond compliance with Microsoft Purview	25

How to secure and manage your most important asset—your data

Data has become the lifeblood of every business. But to fuel innovation and growth, data must be readily discoverable, understandable, governable, and safe.

Unfortunately, 42 percent of organizations say at least half of their data is “dark”—that is, unknown or unused for business purposes. This problem has been compounded by the shift to hybrid work, unprecedented levels of digital transformation, and environments that now span many different devices, apps, and clouds.

The market has responded with dozens of products that address fragments of the data protection, governance, and compliance landscape. But these point solutions typically don't work well together, exposing infrastructure gaps and increasing the complexity and costs of management.

Microsoft Purview was designed to meet these challenges. It's a platform-based approach that enables information protection, data governance, risk management, and compliance across multicloud, multiplatform data estates.



As a single, comprehensive solution, Microsoft Purview can simplify vendor management, improve operational efficiency, and use AI and automation to eliminate manual work and help out overburdened SecOps and DevOps teams. All of that means your organization can better contain costs and do more with less. That's always good business, of course, but it's even more important in times of global economic uncertainty.

This e-book will walk you through how Microsoft Purview can help you:



Understand and govern data across clouds and platforms



Safeguard data wherever it lives and prevent exfiltration with Data Loss Prevention (DLP) tools



Identify, manage, and help reduce insider risk and other data vulnerabilities



1

Data visibility and governance

Discover, understand, and govern data across clouds and platforms

If you want to generate data-driven insights and make smart business decisions, the first step is often aggregating and analyzing huge datasets from multiple sources.

To do that, you need visibility across your entire environment—everywhere that data is created, stored, and shared. But with the volume of data growing faster than ever, it's never been harder to understand and govern all that information.

Why is data governance so important? Because it's the key to democratizing data responsibly. Data fuels digital transformation, whether it's coming from products, operations, or employee and customer experiences. But to create value from that data, your employees need the tools and access to work with it safely and confidently, regardless of technical knowhow.

Organizations face many obstacles to this kind of empowering data democratization, but they can start by identifying their data estate end to end, understanding the business context of data, and ensuring data quality.

With Microsoft Purview, you'll have the tools and insights to govern your data at scale by following the steps in this section.



| Step 1

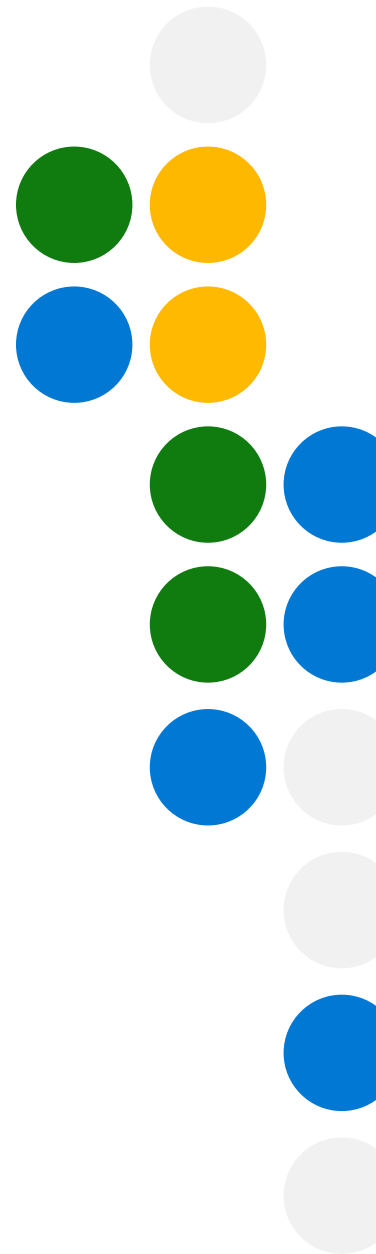
Create a unified map of all your data

The [Microsoft Purview Data Map](#) provides the foundation for effective data discovery, governance, and usage. It captures metadata across analytics, software-as-a-service (SaaS), and operation systems in hybrid, on-premises, and multicloud environments.

The data map stays up to date with built-in capabilities that automatically scan and classify your data. You can also use Apache Atlas APIs to easily integrate all your data catalogs and systems—part of a [collective effort](#) with the open-source community to make it easy to learn and get started with Microsoft Purview.

Learn how with [Microsoft Purview Data Map](#).

Learn more about how data is classified with [Microsoft Purview Information Protection](#).



| Step 2

Make data easily discoverable and maximize its value

To maximize the business value of data for the people in your organization who use it, you need to make that data easily discoverable. Unfortunately, if they don't know exactly how the data estate is structured, users can have a hard time finding something—even if they know exactly what they're looking for.

Microsoft Purview Data Catalog has a browsing experience that lets users explore all your available data. They can use various filters to search within a given collection, navigate between related collections, or even browse by source type, such as Azure Blob Storage, SQL Server, or Power BI.

Learn how with [Microsoft Purview Data Catalog](#).



| Step 3

Create policies to access, move, and share data

Automated access policies make it easier for everyone in your organization to access the data they need, while still ensuring it stays protected.

Microsoft Purview Data Use Management lets you apply specific policies for accessing, moving, or sharing across various data sources. For example, you might want to create and apply different policies to a particular resource based on who's accessing it—whether that's DevOps, the data owner themselves, or other users looking for self-service access.

Learn how with [Microsoft Purview Data Use Management](#).

| Step 4

Limit the growth of real-time data by eliminating duplicates

Traditional data sharing in most organizations involves a lot of copying, refreshing, and transferring behind the scenes. That usually ends up increasing storage costs, creating many duplicates, and slowing access to time-sensitive data.

Microsoft Purview Data Sharing lets you share all of that data in-place—without moving or copying it—in near real time, within and across organizations.

Learn how with [Microsoft Purview Data Sharing](#).



2

Data loss prevention

Safeguard data wherever it lives

Data is created, stored, and shared across apps, clouds, and devices. Knowing and understanding all that data is critical, but so is the next step of safeguarding it.

The key is a structured and automated approach. That lets you understand what data is sensitive and business-critical, so you can then manage and protect it across your environment.

With Microsoft Purview, you can more effectively safeguard your data—even if it's not stored on Microsoft platforms—by following the steps in this section.

| Step 1

Locate and manage sensitive information, even within unstructured data

Your digital estate likely contains massive amounts of unstructured data—files, documents, emails, messages, and more. To identify potential risks, you need to understand where sensitive data lives, who can access it, what users are doing with it, how it is being shared, and where it is traveling.

Microsoft Purview Information Protection helps you automatically discover and protect sensitive data anywhere it lives, so you can more effectively manage it and reduce overall risk.

Learn how with [Microsoft Purview Information Protection](#).



| Step 2

Deploy DLP policies to restrict data leakage

To protect your most sensitive data, you need to identify and prevent risky or unauthorized sharing, transferring, or using of it across endpoints, apps, services, and on-premises files.

Microsoft Purview Data Loss Prevention helps users understand and take the right actions while using sensitive data, helping balance security and productivity. It helps protect sensitive data from exfiltration across applications, services, and devices, with integrations built on your existing capabilities. It's easy to get started with DLP policies, too, with configuration and deployment that's quick and intuitive.

Learn how with [Microsoft Purview Data Loss Prevention](#).

| Step 3

Build cross-platform support for applying labels and protecting files

A software development kit (SDK) can help you add new capabilities to your applications—and in the case of the Microsoft Purview Information Protection SDK, you can enable your apps to apply labels and protection to files. For example, you might subscribe to services specific to HR or finance, and you want to make sure that data is properly classified when it's exported from those apps.

The **Microsoft Purview Information Protection SDK** makes the labeling and protection services from Office 365 Security and Compliance Center available to third-party applications and services. This lets you apply consistent labels and protection, so applications and services can read and write labels in the same predictable way.

Learn how with the [Microsoft Purview Information Protection SDK](#).



| Step 4

Utilize data connectors to bring in data from external sources

You need to safeguard sensitive data across your entire environment, including non-Microsoft data sources such as messaging or video-conferencing apps.

Microsoft Purview data connectors let you ingest data from a wide variety of sources with high fidelity. Once ingested, data can then be used across multiple solutions including Microsoft Purview Data Lifecycle Management, eDiscovery, Communication Compliance, and Insider Risk Management.

Learn how with [Microsoft Purview data connectors](#).



| Step 5

Automate data classification and governance at scale

You need to manage your records and information lifecycle carefully to meet legal, business, privacy, and regulatory obligations. That involves keeping what you need and getting rid of what you don't need broadly across your organization. Built-in classification and governance can help, by automatically classifying content and applying the appropriate policies. For example, you might automatically apply retention labels to anything with PII (Personally Identifiable Information), such as passport or Social Security numbers.

Microsoft Purview Data Lifecycle Management automates classification and governance at scale, using file properties, pattern recognition, 90+ sensitive info types, and machine learning.

Learn how with [Microsoft Purview Data Lifecycle Management](#).



3

Data risk management

Identify, manage, and reduce insider risk and other potential data vulnerabilities

Managing data protection and compliance can be a massive challenge. And it's made tougher by larger data volumes, increasing regulatory complexity, remote work environments, and growing insider risk.

Once you've understood and protected your data, the final step in a comprehensive data protection approach is reducing your data risk.

With Microsoft Purview, you'll be able to get a better handle on risk by following the steps in this section.

Step 1

Leverage machine learning to identify potential insider risks

The proliferation of digital data and the rise of remote and hybrid work have increased concern around insider risks. Organizations everywhere face real challenges in protecting themselves from harm arising from misuse of authorized access—both accidental and malicious.

Microsoft Purview Insider Risk Management uses machine learning to correlate a broad range of signals to identify potential insider risks, so you can quickly identify and act on them.

Learn how with [Microsoft Purview Insider Risk Management](#).

Step 2

Detect potential violations in communications related to regulatory compliance or business conduct

It's important to foster compliant communications, by protecting sensitive information and detecting inappropriate messages, such as those containing harassing or threatening language or adult content.

Microsoft Purview Communication Compliance provides tools to help organizations identify these kinds of issues, including compliance violations related to regulations like SEC or FINRA. Built with privacy by design, these tools provide role-based access controls, pseudonymize usernames by default, and maintain audit logs to help ensure user-level privacy.

Learn how with [Microsoft Purview Communication Compliance](#).



Step 3

Store and retain core business records

Your organization likely needs to meet regulatory and compliance requirements around records management. You need to be ready at any time to demonstrate compliance with regulations, but ideally you also want to dispose of data that's no longer valuable or no longer required for business or regulatory reasons.

Microsoft Purview Records Management gives you a reliable system to manage and store regulatory, legal, and business-critical records, retaining them in unalterable, compliant formats.

Learn how with [Microsoft Purview Records Management](#).



Step 4

Power forensic investigations with audit-ready reporting and insights

Your organization might need to conduct forensic or compliance investigations at times, especially when researching possible breaches and determining the scope of a compromise. This can require specific information, such as when and what a user searched for, as well as when particular emails were accessed, replied to, or forwarded.

Microsoft Purview Audit makes forensic investigations more productive and efficient. It provides insights on user activity, high-bandwidth data access, and reporting that helps you feel more prepared for audits. It can also help you preserve audit logs to meet regulatory requirements for up to 10 years.

Learn how with [Microsoft Purview Audit](#).



Step 5

Identify legal risks and investigate

If your organization needs to respond to a legal matter or internal investigation, the first step will be discovering where the relevant data lives. You'll need to identify persons of interest and their data sources, apply holds to preserve data, and manage the communication process around legal holds.

Microsoft Purview eDiscovery provides an end-to-end workflow to preserve, collect, analyze, review, and export content for both internal and external investigations. Intelligent machine learning capabilities such as deep indexing, email threading, and near-duplicate detection can also help you narrow down large volumes of data.

Learn how with [Microsoft Purview eDiscovery](#).



Step 6

Continuously assess and track your compliance effectiveness

Managing compliance requirements in a multicloud environment can be challenging. You need to take inventory of data protection risks, deal with complexity when implementing controls, stay current with regulations and certifications, and be ready to report to auditors.

Microsoft Purview Compliance Manager can help you continuously assess and track the effectiveness of your compliance efforts. It has many capabilities that simplify compliance and reduce risk, including pre-built assessments for common standards—for example, around certain industry or governmental bodies. You also get step-by-step guidance on suggested improvements, as well as a risk-based compliance score to help you understand your compliance posture.

Learn how with [Microsoft Purview Compliance Manager](#).

Step 7

Automate workflows and reporting

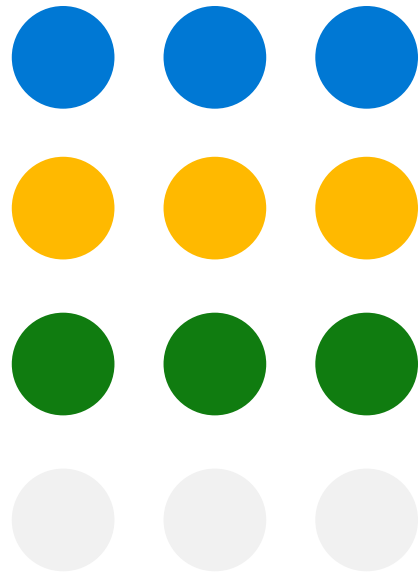
Microsoft Purview has built-in extensibility that can help you adapt, extend, integrate, accelerate, and support your compliance solutions, primarily using data connectors and APIs.

One example is **Microsoft Graph APIs for eDiscovery**. If your organization handles many eDiscovery requests and cases, you know that the associated workflows can be frequent, critical, and high volume. Automation can be a big help, especially with common repeated tasks or large numbers of activities.

Microsoft Graph APIs for eDiscovery provide a scalable way to repeat processes consistently and effectively. By supporting workflows with APIs, you can give yourself flexible options for automation and integration, from upstream processes (such as case creation) to downstream (such as collection, review set queries, or export).

Learn more about [the extensibility of Microsoft Purview](#).

Learn more about [Microsoft Graph APIs for eDiscovery](#).



Go beyond compliance with **Microsoft Purview**

Microsoft Purview represents a new way to approach your data strategy, with a unified view across multicloud, multiplatform environments. Security and compliance leaders can finally bring together the business users of data with the protectors of data.

Every strategy covered in this e-book is available through Microsoft 365 E5 and Microsoft Purview, a comprehensive portfolio of products that spans information protection, data governance, risk management, and compliance.

With Microsoft Purview, you can close exposure gaps, simplify tasks through automation, and control costs so you can do more with less. You can keep your most important asset—your data—safe.

Microsoft Purview can help you consolidate your existing data protection tools with a single comprehensive solution

[Learn how >](#)



©2023 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.