Microsoft Security

Crash Course in Microsoft Purview:

A guide to securing and managing your data estate

Table of Contents

How to secure and manage your crucial data assets 3

1 **Understand and govern your data** 5
Get visibility into all your data and manage assets across your environment

2 **Secure your data** 9
Secure your data throughout its lifecycle across apps, clouds, and devices

3 **Improve your risk and compliance posture** 13
Manage critical risks and regulatory requirements

Secure and govern data in the age of AI with Microsoft Purview 20

How to secure and manage your crucial data assets

Data has become the lifeblood of every business. But to fuel innovation and growth, data must be readily discoverable and understandable by data consumers while being secured and governed by the business.

Organizations must protect their data, close exposure gaps, comply with regulatory requirements, and even manage access controls. Factors like the shift to hybrid work, unprecedented levels of digital and AI transformation, and environments that now span many different devices, apps, and clouds all impact how organizations worldwide protect and govern their data.

The market has responded with a sea of products that address fragments of data security, data governance, and data compliance. But these point solutions typically don't work well together, expose infrastructure gaps, and increase the complexity and costs of management.



Microsoft Purview was designed to meet these challenges. Its platform-based approach enables information protection, data governance, risk management, and compliance across multicloud, multiplatform data estates—in the age of AI.

As a comprehensive solution, Microsoft Purview can simplify vendor management, improve operational efficiency, use AI and automation to eliminate manual work, help overburdened SecOps and DevOps teams, and increase data visibility through a unified management experience. As a result, your organization can leverage that visibility across its environment to protect its data, close exposure gaps, stay up to date with regulatory requirements, and keep its crucial data assets safe.

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

- Get visibility into all your data and manage assets across your environment
- Secure your data throughout its lifecycle, wherever it lives
- Manage critical risks and regulatory requirements

1

Understand and govern your data:

Get visibility into all your data and manage assets across your environment

Data is an organization's unique IP and the key to differentiated innovation. Harnessing the full potential of data requires visibility across your data estate environment—knowing where it lives, where it travels, and how it's being used for analytics and AI.

When business units and individuals can find and access quality data quickly and without advanced technical know-how, they can put their data to work for valuable insights, AI-based app innovation, or generative AI scenarios that drive innovation and growth.

This kind of data innovation begins with the discovery of data from across the data estate, followed by determining the critical data assets that require data quality, lineage, classification, protection, and governance.

With Microsoft Purview, you'll have the tools to activate data for analytics and AI for a modern federated data governance practice through business-friendly interactions, integration across data sources, AI-enabled efficiency, actions, and insights. Learn more with the steps in this section.

Step 1

Create a unified map of all your data

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 to scan and ingest 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 allows data stewards and data owners to curate data assets for governed use in the catalog, which enables data consumers to search for and access data products for use in business innovation. Business-friendly terms, standardized controls, policies, and rules are backed by built-in reports and health actions to help organizations that enable oversight from the data office.

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 Policy 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.

2

Secure your data:

Secure your data throughout its lifecycle across apps, clouds, and devices

Modern organizations create, store, and share vast quantities of data across a variety of platforms, clouds, apps, and devices. Safeguarding that data—whether it is structured or unstructured, in the cloud or on-premises, wherever it lives and travels—requires a structured and automated approach.

Intelligently identifying sensitive and business-critical data, detecting data security risks in a complex threat landscape with multiple exposure points and growing insider risk, and preventing data loss dynamically can ensure better data security while saving time.

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

Step 1

Discover, label, and protect sensitive data across your data estate

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 provides a comprehensive view of the potential risks to your sensitive data. It allows you to automatically discover, label, and protect sensitive data across enterprise apps and services (like Copilot for Microsoft 365), devices, SaaS apps, and both cloud and on-premises environments so you can more effectively manage and reduce overall risk.

The **Microsoft Purview Information Protection SDK** enables organizations to integrate and support Purview labeling and protections natively within their third-party applications and services.

Learn how with Microsoft Purview Information Protection.

Learn how with the Microsoft Purview Information Protection SDK.



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

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 the Microsoft Purview Insider Risk Management.

3

Improve your risk and compliance posture:

Manage critical risks and regulatory requirements

Large data volumes, increasing regulatory requirements, complex data discovery, risk of fines and non-compliance, and too many manual processes are among the factors that can make managing data protection and compliance a massive challenge.

Once you've understood and protected your data, a key step in a comprehensive data protection approach is improving your risk and compliance posture.

With Microsoft Purview, learn how to proactively classify unknown data, assess risks, quickly respond to investigations, and foster safe and compliant communication by detecting sensitive content across your organization. Learn more in the steps in this section.

Step 1

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 a 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.

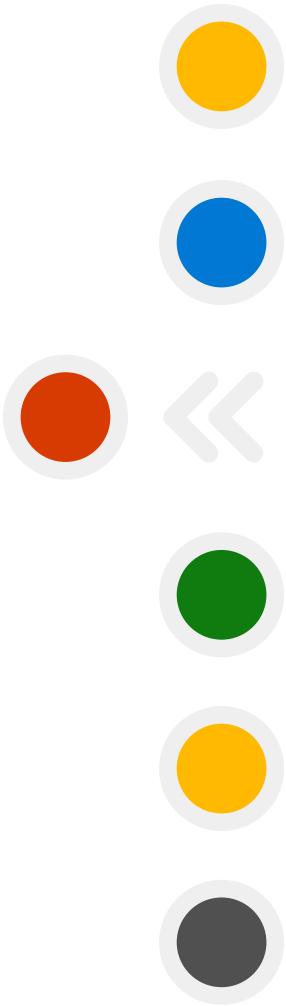
Learn how with Microsoft Purview Data Lifecycle Management.

Step 2

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 3

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, including data spillage scenarios. Intelligent machine learning capabilities such as deep indexing, email threading, and near-duplicate detection can also help you narrow down large volumes of data. Additionally, Copilot for Security in Microsoft Purview offers contextual summaries of review set items, saving reviewers time by quickly identifying relevant information for tagging or exporting.

Learn how with Microsoft Purview eDiscovery.



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

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. Additionally, it extends these capabilities to Generative AI by detecting compliance violations in AI-generated content, including prompts and responses from Copilot for Microsoft 365.

Learn how with Microsoft Purview Communication Compliance.

Step 6

Continuously assess and track your compliance effectiveness

Managing compliance requirements in your data estate 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.

Secure and govern data in the age of AI with Microsoft Purview

Microsoft Purview represents a simplified approach to your data protection strategy, with a unified view across your data estate. 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 Purview, a comprehensive portfolio of products spanning data governance, data security, and data compliance solutions that expand coverage outside of Microsoft 365, including different data types like generative AI data.

With Microsoft Purview, you can close exposure gaps, simplify tasks through automation, and consolidate your existing data protection tools with a single comprehensive approach to help keep your crucial data assets safe.

Learn how >

Microsoft Security

©2024 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.