News AI and machine learning Microsoft Purview

11 min read

New Microsoft Purview features use AI to help secure and govern all your data

By Herain Oberoi, General Manager, Data Security, Compliance, and Privacy, Microsoft

December 7, 2023

Data security

Security operations

Microsoft Copilot for Security

Microsoft Purview Communication Compliance

Microsoft Purview Data Loss Prevention

Microsoft Purview eDiscovery

Microsoft Purview Information Protection

Microsoft Purview Insider Risk Management

In the past few years, we have witnessed how digital and cloud transformation has accelerated the growth of data. With more and more customers moving to the cloud, and with the rise of hybrid work, data usage has moved beyond the traditional borders of business. Data is now stored in multiple cloud environments, devices, and on-premises solutions, and it's accessed from multiple locations, both within and outside of corporate networks. More than 90% of organizations use multiple cloud infrastructures, platforms, and services to run their business, adding complexity to securing all data.[1] Microsoft Purview can help you secure and govern your entire data estate in this complex and changing environment.

As many of you look to AI transformation to drive the next wave of innovation, you now also **need to account for data being both consumed and created by generative AI applications**. The risks that come with implementing and deploying AI are not fully known, and it is only a matter of time before you start to see broader regulatory policies on AI. According to Gartner®, by 2027 at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation.[2] **AI will be a catalyst for regulatory changes, and having secure and compliant AI will become fundamental.**

With these trends converging all at once, securing and governing all your data is a complex and multifaceted undertaking. You need to secure and govern different types of data (structured, unstructured, and data generated by AI). You need to secure and govern it in different locations across multiple clouds, and you need to account for existing and future data security, governance, and AI regulations.

Most organizations experience an average of 59 data security incidents per year and use an average of 10 solutions to secure their data estate.[1] This fragmented approach requires many of you to stitch together multiple tools to address data security and governance, which can lead to higher costs and difficulty in both procurement and management. The lack of integration between the disparate tools can cause unnecessary data transfers, duplicate copies of data, redundant alerts, siloed investigations, and exposure gaps that lead to new types of data risks and ultimately worse security outcomes.

A simpler approach: Microsoft Purview

To address these challenges, you need a simplified approach to data security, governance, and compliance that covers your entire data estate. Microsoft Purview is an integrated solution that helps you understand, secure, and manage your data—and delivers one unified experience for our customers.

With Microsoft Purview, you can:

- **Gain end-to-end visibility** and understanding of your entire data estate, across on-premises, multicloud, and software as a service (SaaS) environments, and for structured, unstructured, and data created by generative AI applications.
- **Apply comprehensive data protection** across your data estate, using AI-powered data classification technology, data maps, extensive audit logs and signals, and management experience.
- **Improve your risk and compliance posture** with tools to identify data risk and manage regulatory requirements.

Microsoft Purview

Help keep your organization's data safe with a range of solutions for unified data security, data governance, and risk and compliance management.

What's new in Microsoft Purview?

In this blog post, we will outline some of the exciting new capabilities for Microsoft Purview that we announced at Microsoft Ignite 2023.

Expanding data protection across the data estate

As we unveiled earlier this year, Microsoft Purview is expanding the sphere of protection across your entire data estate, including structured and unstructured data types. We are excited to share some of the next steps in that journey by providing you with:

- **A unified platform** that enables you to discover, label, and classify data across various data sources, including Microsoft Fabric, Microsoft Azure, Amazon Web Services (AWS), and other cloud environments.
- **Consistent protections** across structured and unstructured data types such as Azure SQL, Azure Data Lake Storage (ADLS), and Amazon S3 buckets.
- **Expanded risk detections** enabling signals from infrastructure clouds and third-party apps such as AWS, Box, DropBox, and GitHub.

With these capabilities, you can gain visibility across your data estate, apply consistent controls, and ensure that your data is protected and compliant across a larger digital landscape. For example, you can scan and label your data in Microsoft Azure SQL, Azure Data Lake Storage, and Amazon S3 buckets, and enforce policies that restrict access to sensitive data based on data labels or user roles from one control plane—just like you do for Microsoft 365 sources. Check out this short Microsoft Mechanics video covering an end-to-end scenario. To learn more, we invite you to read the "Expanding data protection" blog.

Securing AI with Microsoft Purview

We are committed to helping you protect and govern your data, no matter where it lives or travels. Building on this vision, Microsoft Purview enables you to protect your data across all generative AI applications—Microsoft Copilots, custom AI apps built by your organization, as well as more than 100 commonly used consumer AI apps such as OpenAI's ChatGPT, Bard, Bing Chat, and more.[3] We announced a set of capabilities in Microsoft Purview to help you secure your data as you leverage generative AI. Microsoft Purview will provide you with:

- **Comprehensive visibility** into the usage of generative AI apps, including sensitive data usage in AI prompts and total number of users interacting with AI. To enable customers to get these insights, we announced preview of AI hub in Microsoft Purview.
- **Extensive protection** with ready-to-use and customizable policies to prevent data loss in AI prompts and protect AI responses. Customers can now get additional data security capabilities such as sensitivity label citation and inheritance when interacting with Copilot for Microsoft 365 and prevent their users from pasting sensitive information in consumer generative

AI applications.

- **Compliance controls** to help detect business violations and easily meet regulatory requirements with compliance management capabilities for Copilot for Microsoft 365.

Copilot for Microsoft 365 is built on our security, compliance, privacy, and responsible AI framework, so it is enterprise ready. With these Microsoft Purview capabilities, you can strengthen the data security and compliance for Copilot. **The protection and compliance capabilities for Copilot are generally available, and you can start using them today.** To learn more, read the Securing AI with Microsoft Purview blog.

Supercharge security and compliance effectiveness with Microsoft Security Copilot in Microsoft Purview

Microsoft Purview capabilities for Microsoft Security Copilot are now available in preview. With these capabilities you can empower your security operations center (SOC) teams, your data security teams, and your compliance teams to address some of their biggest obstacles. Your SOC teams can use the standalone Security Copilot experience to analyze signals across Microsoft Defender, Microsoft Sentinel, Microsoft Intune, Microsoft Entra, and Microsoft Purview into a single pane of glass. Your data security and compliance teams can use the embedded experiences in Microsoft Purview for real-time analysis, summarization, and natural language search, for data security and compliance built directly into your investigation workflows.

Microsoft Purview capabilities in Security Copilot

To help your SOC team gain comprehensive insights across your security data, Microsoft Purview capabilities in Security Copilot will provide your team with data and user risk insights, identifying specific data assets that were targeted in an incident and users involved to understand an incident end to end. For example, in the case of a ransomware attack, you can leverage user risk insights to identify the source of the attack, such as a user visiting a website known to host malware, and then leverage data risk insights to understand which sensitive files that user has access to that may be held for ransom.

Security Copilot embedded in Microsoft Purview

We’ve also embedded Security Copilot into Microsoft Purview solutions to help with your data security and compliance scenarios. You can now leverage real-time guidance, summarization capabilities, and natural language support to catch what others miss, accelerate investigation, and strengthen your team’s expertise. Here’s where these capabilities will light up:

- **Summarize alerts in Microsoft Purview Data Loss Prevention:** Investigations can be overwhelming for data security admins due to the large number of sources to analyze and varying policy rules. To help alleviate these challenges, Security Copilot is now natively embedded in Data Loss Prevention to provide a quick summary of alerts, including the source, attributed policy rules, and user risk insights from Microsoft Purview Insider Risk Management. This summary helps admins understand what sensitive data was leaked and associated user risk, providing a better starting point for further investigation. Learn more in our Microsoft Purview Data Loss Prevention announcement.
- **Summarize alerts in Microsoft Purview Insider Risk Management:** Insider Risk Management provides comprehensive insights into risky user activities that may lead to potential data security incidents. To accelerate investigations, Security Copilot in Insider Risk Management summarizes alerts to provide context into user intent and timing of risky activities. These summaries enable admins to tailor investigations with specific dates in mind and quickly pinpoint sensitive files at risk. Learn more in our Microsoft Purview Insider Risk Management announcement.
- **Contextual summary of communications in Microsoft Purview Communication Compliance**: Organizations are subject to regulatory obligations related to business communications, requiring compliance investigators to review lengthy communication violations. Security Copilot in Communication Compliance helps summarize alerts and highlights high-risk communications that may lead to a data security incident or business conduct violation. Contextual summaries help you evaluate the content against regulations or corporate policies, such as gifts and entertainment and stock manipulation violations. Learn more in our Microsoft Purview Communication Compliance announcement.
- **Contextual summary of documents in review sets in Microsoft Purview eDiscovery:** Legal investigations can take hours, days, even weeks to sift through the list of evidence collected in review sets. This often requires costly resources like outside council to manually go through each document to determine the relevancy to the case. To help customers address this challenge, we are excited to introduce Security Copilot in eDiscovery. This powerful tool generates quick summaries of documents in a review set, helping you save time and conduct investigations more efficiently. Learn more in our Microsoft Purview eDiscovery announcement.
- **Natural language to keyword query language in eDiscovery:** Search is a difficult and time-intensive workflow in eDiscovery investigations, traditionally requiring input of a query in keyword query language. Security Copilot in eDiscovery now offers natural language to keyword query language capabilities, allowing users to provide a search prompt in natural

language to expedite the start of the search. This empowers analysts at all levels to conduct advanced investigations that would otherwise require keyword query language expertise. Learn more in our Microsoft Purview eDiscovery blog.

To learn more about Security Copilot and Microsoft Purview, read our Microsoft Security Copilot in Microsoft Purview blog.

Additional product updates

New Microsoft Purview Communications Compliance capabilities

Copilot for Microsoft 365 support introduces an advanced level of detection within Communication Compliance, allowing organizations to identify and flag risky communication, regardless of source. Investigative scenarios across various Microsoft applications, including Outlook, Microsoft Teams, and more, showcase the precision of this feature, identifying patterns, keywords, and sensitive information types. With additional features for policy creation and user privacy protection, administrators can also fine-tune their management strategy, ensuring secure, compliant, and respectful communications. Integration with Security Copilot further enhances data security and regulatory adherence, providing concise contextual summaries for swift investigation and remediation. Leveraging AI technology, Communication Compliance detects and categorizes content, prioritizing content that requires immediate attention. Reporting inappropriate content within Microsoft Viva Engage and ensuring compliance in Microsoft Teams meetings further strengthens the multilayered compliance defense. Stay ahead of compliance challenges and embrace these innovative features to secure, comply, and thrive in the digital age.

Learn more in our Microsoft Purview Communication Compliance announcement.

New to Information Protection in Microsoft Purview

As organizations prepare to use generative AI tools such as Copilot for Microsoft 365, leveraging Microsoft Purview Information Protection, discovery and labeling of sensitive data across the digital estate is now even more important than ever. New releases to Microsoft Purview Information Protection include intelligent advanced classification and labeling capabilities at an enterprise scale, contextual support for trainable classifiers that improve visibility into effectiveness and discoverability, better protection for important PDF files, secure collaboration on labeled and encrypted documents with user-defined permissions, as well support for Microsoft Fabric, Azure, and third-party clouds.

You can learn more about the new Information Protection capabilities in the Information Protection announcement.

New Microsoft Purview Data Loss Prevention capabilities

We are excited to announce a set of new capabilities in Microsoft Purview Data Loss Prevention (Purview DLP) that can help comprehensively protect your data and efficiently investigate DLP incidents. Our announcements can be grouped into three categories:

- **Efficient investigation**: Capabilities that empower admins by making their everyday tasks easier, including enriching DLP alerts with user activity insights from Insider Risk Management, DLP analytics to help find the biggest risk and recommendations to finetune DLP policies, and more.
- **Strengthening protection**: Capabilities that help protect numerous types of data and provide granular policy controls, including predicate consistency across workloads, enhancements to just-in-time protection for endpoints, support for optical character recognition (OCR), and performance improvements for DLP policy enforcements.
- **Expanding protection**: Capabilities that extend your protection sphere to cover your diverse digital estate, including support for Windows on ARM and several enhancements to macOS endpoints.

Purview DLP is easy to turn on; protection is built into Microsoft 365 apps and services as well as endpoint devices running on Windows 10 and 11, eliminating the need to set up agents on endpoint devices.

Learn more in our Microsoft Purview DLP blog.

New Microsoft Purview Insider Risk Management and Adaptive Protection capabilities

To secure data in diverse digital landscapes, including cloud environments and AI tools, detecting and mitigating data security risks arising from insiders is a pivotal responsibility. At Microsoft Ignite, we made a few exciting announcements for Insider Risk Management and Adaptive Protection:

- **Intelligent detection across diverse digital estate**: Insider Risk Management will now detect critical data security risks generated by insiders in AWS, Azure, and SaaS applications, including Box, Dropbox, Google Drive, and GitHub. Additionally, security teams can also gain visibility into AI usage with our new browsing to generative AI sites indicator.

- **Adaptive data security from risk detection to response**: User context can help security teams make better data security decisions. Security teams can now gain user activity summary when a potential DLP incident is detected in Microsoft Purview DLP and Microsoft Defender portal. With this update and Adaptive Protection, user risk context is available from DLP incident detection to response, making data security more effective. In addition, security teams can now leverage human resources resignation date to define risk levels for Adaptive Protection, addressing common incidents, such as potential data theft from departing employees.
- **Streamlined admin experience for effective policies**: To enable better policies management experience, Insider Risk Management will support admin units and provide recommended actions to fine tune policies and receive more high-fidelity alerts.

Learn more details about all these announcements in our Microsoft Purview Insider Risk Management blog.

Get started today

These latest announcements have been exciting additions to help you secure and govern your data, across your entire data estate in the era of AI. We invite you to learn more about Microsoft Purview and how it can empower you to protect and govern your data. Here are some resources to help you get started:

- Watch the Microsoft Purview on-demand sessions from Microsoft Ignite, outlined in this guide.
- Try Microsoft Purview for free.
- Read the Data Security Index report.
- Visit the Microsoft Purview website.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

[1] Microsoft Data Security Index: Trends, insights, and strategies to secure data, October 2023.

[2] Gartner, Security Leader's Guide to Data Security, Andrew Bales. September 7, 2023.

[3] Microsoft sets new benchmark in AI data security with Purview upgrades, VentureBeat. November 13, 2023.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads