



03

Prioritize data security as you prepare for AI

07

Bring the power of next-generation AI to work

09

Use case – Mitigate insider risk and prevent data loss

10

How to get your data ready for M365 Copilot

12

Why Microsoft for Data Security

16

Get started with Microsoft Purview for your organization





Prioritize data security as you prepare for AI

The next generation in how we work is coming. Is your data prepared?

With the introduction of AI into your business model, there are perks of balancing engagement and productivity. Employees can avoid spending too much effort on tasks that zap their time, creativity, and energy by utilizing the power of next-generation AI.

But this change comes with concerns about data security and governance. For many organizations, content oversharing, and data governance can already be a challenge. With the addition of AI, you need to ensure your data is shared safely.

Keep reading to see how you can enhance your data security and governance practices to get ready for the next transformation in how we work.

Data security incidents can happen anytime, anywhere

As the volume and sophistication of cyber-attacks increase, organizations of all sizes across industries are prioritizing processes and tools that secure data. You must know what kind of data you have, where it's stored, who has access to it, and how they are using it. A comprehensive, integrated approach is critical. A patchwork of disparate or siloed data security and governance solutions leaves infrastructure exposed, creating threats that are costly and difficult to manage.

To effectively protect against leaks and breaches, organizations need a holistic approach that encompasses data security, compliance, and employee productivity to:

- Maintain control of your data throughout its lifecycle
- Minimize risks without compromising collaboration or user experience
- Keep up with evolving industry regulations and standards
- Identify and mitigate intentional and unintentional insider risks
- Innovate data protection and automation
- Reduce cost and complexity



66% of consumers say retailers are responsible for data security²

93% of polled patients said they would switch providers if their patient privacy was undermined³

At **\$14.5 million**, companies in financial services experience the highest total cost of insider security incidents⁴

27,000 sensitive files including financial and business-critical information is available to everyone⁵

90% of government IT employees believe that specialized software and tools are important to battle ransomware⁶

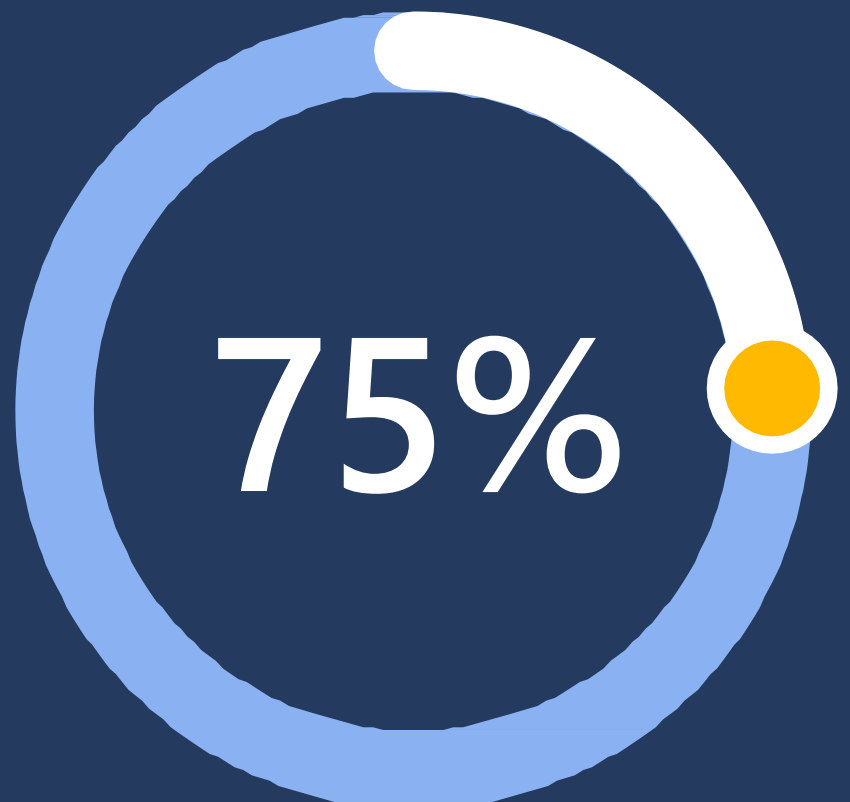
The best way to prepare for AI is to prepare your data security and governance practices first

Organizations like yours can achieve things like never before using AI to unleash creativity and accelerate productivity. Employees can jump-start their creative process, lighten their workload to focus on what really matters, and uplevel their skills or quickly master what they've yet to learn.

Before you get started with AI in your workplace, take a moment to determine:

- How do you manage data throughout its lifecycle?
- Do you have measures in place to prevent data loss or oversharing of sensitive data?
- What steps are you taking to mitigate the impact of an insider event that may lead to leak or breaches?

By 2023, inadequate management of identities, access, and privileges will cause 75% of cloud breaches¹



¹ CISO Insider Issue 3

Perform faster with AI without compromising your data security



Safeguard data wherever it lives. Protect your data with industry leading enterprise data security and governance solution.



Secure data with comprehensive permissions model. Fortify data security with content classification, sensitivity labelling, and the 'just enough access' principle.



Establish strong foundations. Power collaboration and productivity with integrated data security, governance, privacy, and responsible AI.

Bring the power of next-generation AI to work



Microsoft 365 Copilot is designed to help you radically accelerate employee productivity and capability by leveraging its transformational AI without compromising your data security.

Copilot automatically inherits your organization's security, compliance, and privacy policies for Microsoft 365. Permission models within Microsoft 365 services, including Copilot, ensure appropriate access for users/groups.

Proper content classification and labeling of sensitive information blocks restricted data to avoid content oversharing and data privacy issues. Unrestricted information is still utilized to enable users to synthesize data and conduct tasks at speed.

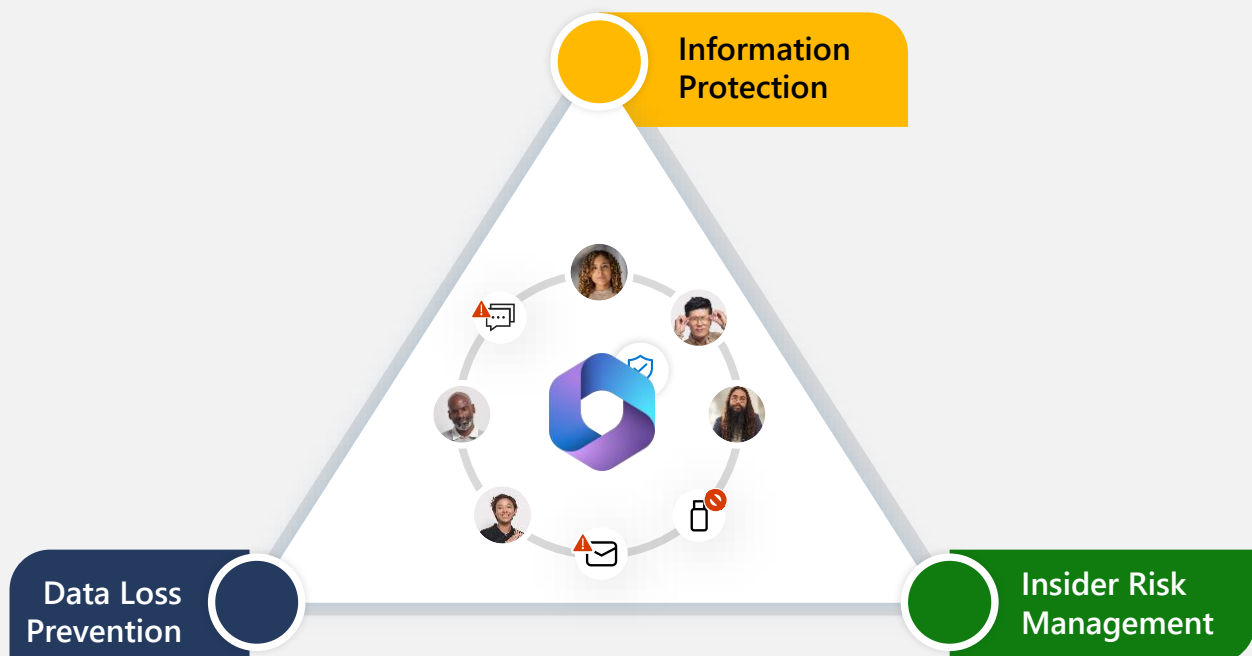
Our efforts are guided by our AI principles and Responsible AI Standard and are built on decades of research on grounding and privacy-preserving machine learning. Copilot is the AI solution you can trust.



Leverage Microsoft 365 Copilot and Microsoft Purview for productivity and security

While Microsoft 365 Copilot has inbuilt security, you can leverage the Purview to provide an additional layer of security and governance to your organizational data. We've designed an experience that prioritizes human agency, putting the user in control while maintaining data governance and security. There are several opportunities to leverage Purview and security best practices.

- Data discovery is the first step to solid data governance. Use MIP Scanner to discover oversharing and important data types within your file ecosystem so you can strategically decide which protections to apply.
- By implementing 'just enough access' principles, Copilot users can leverage the proper files in Microsoft Teams, SharePoint sites, OneDrive, email, and chat conversations to work more efficiently than ever before.
- Harness Adaptive Protection to leverage Insider Risk Management machine learning to understand user interaction with data, identify risky activities, then automatically tailor Data Loss Prevention (DLP) controls based on the risk detected.
- Semantic Index for Copilot analyzes your data in Microsoft Graph and uses a Large Language Model (LLM) to map the relationships between you and your content to find the most relevant results in milliseconds.





Mitigate insider risks and prevent data loss

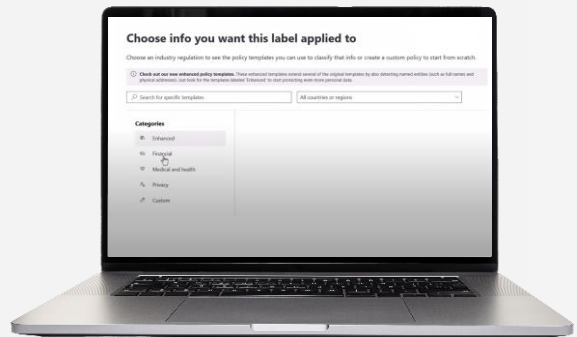
Some businesses need to outsource more than a quarter of their daily business tasks, giving suppliers access to their business data¹. This may introduce a multitude of data security and governance risks such as:

- Intentional or unintentional insider risks
- Over-extended permissions to accommodate faster onboarding
- Leaks and breaches of sensitive business-critical information
- Scattered customer information across multiple devices
- Inadequate implementation of policies and controls
- Noncompliant data security and governance practices

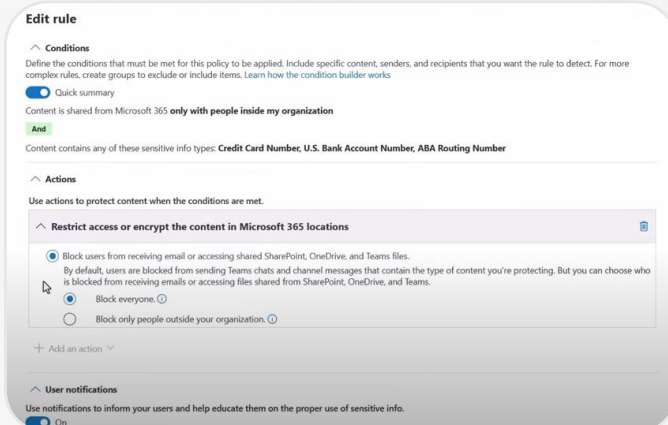
¹ [CISO Insider: Issue 1](#)

How to your information ready for M365 Copilot

If a user has access to most, if not all the information within an organization, then they can retrieve any information by simply using search. Solving this information access challenge is not unique for M365 Copilot. The recommended approach here to have just enough access for users as needed to perform their work.



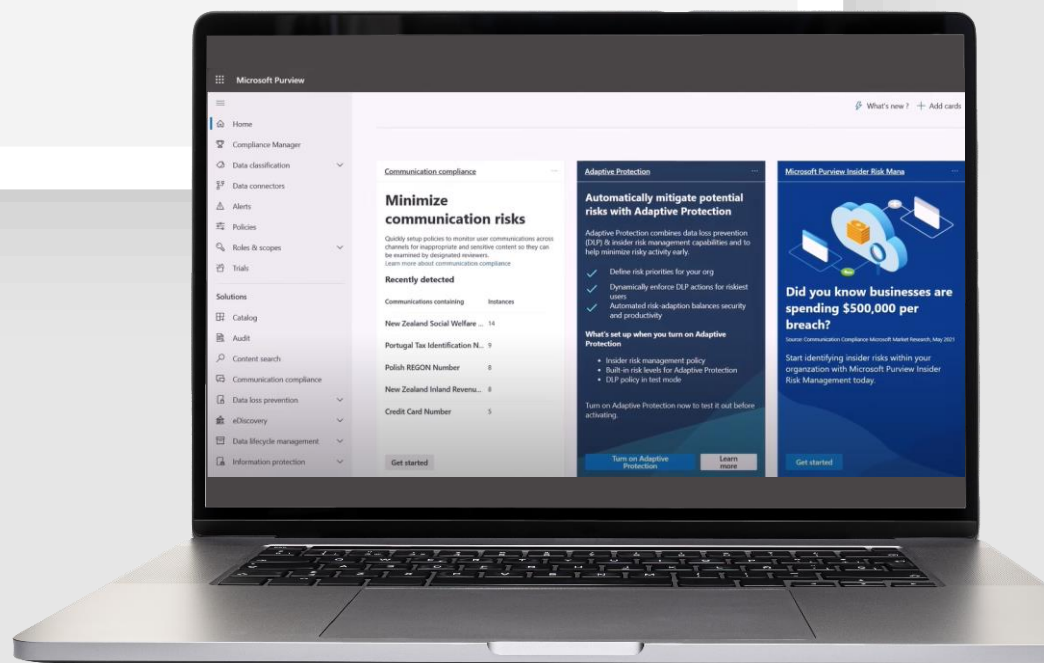
M365 Copilot will only retrieve information that each user explicitly has access to so prepare your data for search within the organization.



Place automated controls in place to get the right level of access and stop oversharing using Microsoft Purview Information Protection and Data Loss Prevention before you deploy M365 Copilot.

How to mitigate risks associated with overshared information

If you have concerns about the users have too much access to sensitive information, Microsoft Purview Information Protection along with its data classification controls and integrated content labelling and corresponding Data Loss Prevention policies can help you identify files in Microsoft Teams, SharePoint sites, OneDrive locations, and within email and chat conversation either containing sensitive information or classified content and automatically apply controls to limit their access.





Built on Microsoft's security approach

The security landscape continues to evolve, and organizations are facing a variety of risks beyond traditional cybersecurity. That's why we believe in a comprehensive approach to data security, governance, and compliance. A holistic approach to data protection can help your organization adapt to changes in your risk landscape.

Microsoft is committed to providing solutions that help you defend against threats across your entire digital estate. For your team, that means securing your multicloud, multiplatform environment, getting complete visibility into threats, and investigating and responding faster.

Microsoft E5 Compliance, which includes an intelligent suite of products and features, can make this process easier, all on a single platform. Avoid the difficulties of aligning governance, security, and compliance in an environment of bespoke applications.

This approach is at the foundation of Microsoft 365 Copilot and Microsoft Purview, so you can be confident about your data security.

Go beyond data protection with Microsoft Purview

We've all seen how the ongoing shift to hybrid and multicloud environments is changing how organizations collaborate and access data. It's easy to see how the massive volume of data generated and stored today could create business liability.

Our customers have been clear in voicing their need for a unified, comprehensive solution for data security and management—one that's as scalable as their business needs.

Microsoft Purview can provide you with better visibility, secure data management practices, and take you beyond compliance. Our comprehensive solutions for information protection, data governance, risk management, and compliance can help you safeguard all your data across platforms, apps, and clouds.

 **41.6B**

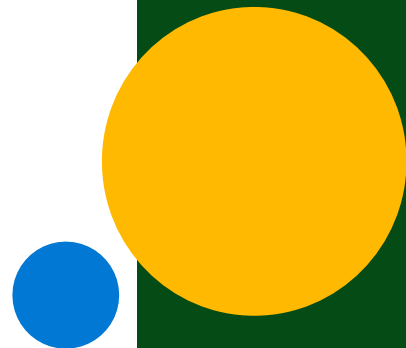
The number of global IoT (internet of things) devices is projected to reach 41.6 billion by 2025, creating an expanded attack surface for attackers who use such devices as entry points for cyber-attacks.¹

¹ International Data Corporation (IDC) via [MSFT's CISO Insider: Issue 3](#)

Understand and govern data

Safeguard data wherever it lives

Improve risk and compliance posture



Discover the product suite

Make data security a top priority with these unified solutions.

Information Protection

Discover, identify, classify, and protect sensitive data that is business critical, then manage and protect it across your environment.

[Learn more](#)

Insider Risk Management

Detect, investigate, and take action on critical risks in your organization, including data theft, data leaks, and security policy violations.

[Learn more](#)

Data Loss Prevention

Automatically protect sensitive information from risky and unauthorized access across apps, services, endpoints, and on-premises files.

[Learn more](#)

Adaptive Protection

Leverage machine learning to dynamically identify and mitigate the most critical risks using the most effective protection controls, saving security teams valuable time while ensuring better data security.

[Learn more](#)

Choose a holistic and comprehensive approach

Microsoft offers comprehensive compliance and data governance solutions to help your organization manage risks, protect and govern sensitive data, and respond to regulatory requirements. By implementing Microsoft Purview and its well-established data security strategy, you can form a solid foundation prior to adding Microsoft 365 Copilot.

As the landscape continues to evolve with the introduction of next-generation AI, data security and governance will always be a top priority. While Copilot adheres to Microsoft's strong approach to security, Purview can upgrade your organization's overall security plan.





Next steps you can take today

Uplevel your data estate, then bring the power of next-generation AI to work



Get ready for Microsoft 365 Copilot and upgrade from ME3 to [ME5](#) or get [E5 Compliance](#).



If you have ME5, [deploy Microsoft Purview Information Protection \(MIP\) and Data Loss Prevention \(DLP\)](#) so your organization can find its data, choose a governance strategy, and define user access levels.



Ready to take the next step? Contact your Microsoft Representative today!

Resources

What is Microsoft 365 Copilot?

- [Microsoft 365 Copilot](#)
- [The Copilot System](#)
- [ChatGPT vs. Microsoft 365 Copilot: What's the difference?](#)
- [Semantic Index for Copilot: Explained by Microsoft](#)
- [Data privacy and security for Microsoft 365 Copilot](#)

How Microsoft 365 Copilot works

- [How Microsoft 365 Copilot works: Microsoft Mechanics video](#)
- [How to get ready for Microsoft 365 Copilot](#)



We live in an era where security is a key enabler of technological success. Innovation and enhanced productivity can only be achieved by introducing security measures that make organizations as resilient as possible against modern attacks.



Bret Arsenault

*Chief Information Security Officer,
Microsoft*