Microsoft Security

Discover, protect, and manage sensitive data across your digital estate

Your enterprise generates, stores, and shares a huge amount of data every day. A comprehensive data security strategy requires visibility into that data, as well as intelligent detection of risk, sensitive data protection, and prevention of data loss.

Microsoft Purview Information Protection is an integrated, comprehensive security solution that enables you to quickly **discover and protect your organization's most important sensitive data** while also **making it easy for employees to collaborate securely.** This is more important than ever, as many organizations are now using generative AI tools to create content based on information accessible on their network.

Why protecting business data is critical

137

out of 194 countries, **with legislation in place to protect data.**[1]

$4.45 million

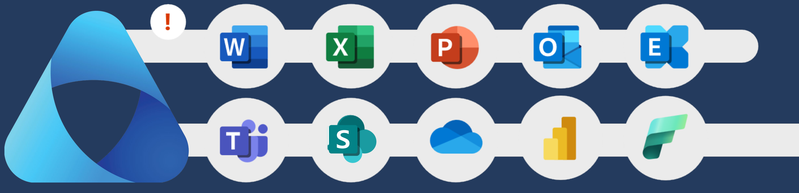
Is the **global average cost of a data breach** in 2023, a 15% increase over the past 3 years.[2]

6%

of employees have **pasted sensitive data into GenAI tools**, and 4% of employees have pasted sensitive data on a weekly basis. [3]

1. UNCTAD Data Protection and Privacy Legislation Worldwide web page 2. IBM 2023 Cost of Data Breach report 3. LayerX Revealing the True GenAI Exposure Risk research report, June 2023

When Information Protection detects sensitive data across your data estate, it can automatically classify, label and protect it in Microsoft 365 apps and supported security solutions.



Information Protection is also tightly integrated with Microsoft Purview Data Loss Prevention. Its policies prevent unauthorized access and oversharing sensitive files and content and can automatically block pasting sensitive data into specific websites for supported browsers, generative AI prompts, or personal email.

Integration with Microsoft Purview Insider Risk Management provides insights to help identify potentially risky activity that may lead to data security incidents, and with Adaptive Protection, you can dynamically adjust DLP controls to prevent use of sensitive data based on a user's risk level.

Together, these integrated data security solutions secure your data and address your organization's most critical data risks, and protect corporate personally identifiable information (PII), intellectual property (IP), and company trade secrets for industry regulations.

In addition to this suite of data security solutions, Information Protection is also natively integrated with Microsoft Copilot for Microsoft 365. Sensitivity labels and label inheritance are supported by Copilot, which helps prevent data overexposure to unauthorized users. Copilot responses will not summarize or include information from protected, referenced files for which a user doesn't have permissions.

Comprehensive discovery with best-in-class classification technology

Information Protection provides over 300 ready-to-use Sensitive Information Types (SITs), the ability to define custom SITs, and AI-powered trainable classifiers that can identify sensitive data in common business categories (legal, finance, intellectual property and trade secrets, etc.).

- Sensitive information types
- Named entities
- Exact data match
- Optical character Recognition (OCR)
- Trainable classifiers
- Credentials SITs
- Fingerprint SITs
- Context-based classification

Once classified, the sensitivity label and any associated protection or encryption stay with the document regardless of where it travels. The data is secured across Microsoft services, and even across non-Microsoft apps and services.

Learn more about Microsoft Purview

- See Information Protection, Data Loss Prevention, Insider Risk Management, and licensing options.
- Watch mechanics videos about data classification, AI-powered classification, and an overview of Microsoft Purview Information Protection.