Microsoft Security

Secure your data

Secure data in the age of AI with a comprehensive approach

Microsoft Security provides a comprehensive solution that combines data and user context across your estate, devices, and generative AI applications. This integrated solution can help:

- **Discover hidden risks to data** wherever it lives or travels by leveraging AI-powered aggregated insights.
- **Protect and prevent unauthorized use of data** across cloud, devices, and generative AI applications with flexible controls that help balance protection and productivity.
- **Investigate and respond** to data security incidents at the speed of AI by leveraging insights correlated across an integrated set of products.

Tackle growing complexity in data types and sources with a multilayered approach to data security

Generative AI is enabling organizations to transform and generate novel solutions to complex problems at an accelerated rate by leveraging data in new ways—all while enhancing human capabilities and experiences. That means it's more important than ever for organizations to safeguard their competitive edge, reputation, and customer loyalty by preventing business-critical data from being compromised.

Recent Microsoft research shows that 89 percent of decision-makers consider their data security posture critical to overall success in protecting their data[1]. Of those same respondents, 80 percent agree that comprehensive, integrated solutions are superior to manual, best-of-breed solutions—and yet, organizations use an average of 10+ data security tools. Those with the most tools experience more data security incidents.

80%
of decision-makers agree that comprehensive, integrated solutions are superior to manual, best-of-breed solutions

To get the most out of data and to confidently adopt AI, organizations using an integrated, multilayered approach to data security can address the following concerns:

Gain visibility

Gain visibility into the location, volume, and type of sensitive data in the digital estate. More than **30 percent**[1] of decision-makers say they don't know where or what their business-critical data is. Organizations need tools that can help discover, classify, and label sensitive data.

Understand user context

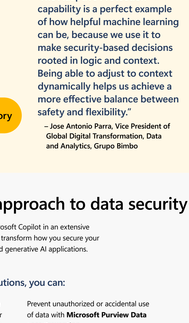
Over a third, **35 percent, of decision-makers**[1] hope to shore up defenses against malicious insiders and compromised accounts, and a third are concerned with inadvertent insider incidents. Malicious insiders rank second among the types of incidents that decisions-makers feel least prepared to prevent. Understanding user activity and context around the data movement helps identify risks and create policies to mitigate them.

Prevent data loss

Over **80 percent of leaders**[1] said that the potential for sensitive data leakage is their primary concern. Ensuring users can access data to get their work done is critical. Organizations need flexible security to strike a balance between protection and productivity. Applying restrictive policies only to users with high risk allows other users to maintain productivity.

These different layers—combining the data context with the user context to apply flexible and dynamic policies—are what a comprehensive approach to data security looks like. Wherever organizations start on this journey, it is critical that they build out each layer of protection.

Seamlessly integrating AI with security products helps discover hidden risks to your data no matter where it lives or travels; balance security and productivity with flexible controls that detect, protect data, and prevent loss; and investigate and respond to data security incidents at the speed of AI.



Defend against real-world data security incidents

Let's examine a situation that actually occurred. While working at a Fortune 500 company, over a period of years Jane Doe managed to upload sensitive files to her personal cloud storage, then download proprietary information to a personal hard drive.

With processes in place to understand how users are interacting with data, Jane's company could have avoided data theft. Here's how a comprehensive data security program could have helped detect risky data movement that resulted in a data security incident and better protect the company:

- **Microsoft Purview Information Protection** would have let the company employ ready-to-use, trainable classifiers for visibility into sensitive data and enforce encryption policies to restrict file access to specific users.
- **Microsoft Purview Insider Risk Management** would have helped identify Jane as a high-risk user and detect activities that could lead to data security incidents. Insider Risk Management could have assigned Jane an elevated-risk level in **Adaptive Protection** and prevented her from exfiltrating data through any channel with **Microsoft Purview Data Loss Prevention**.
- All of Jane's user activities could have been detected and evidence collected for appropriate insider risk investigations. The enriched and curated insights derived would have allowed security teams to expedite the investigation, minimizing impact.

Grupo Bimbo turns to Microsoft Security to take a proactive approach to data security

Faced with the complex task of understanding how sensitive data is flowing through their organization, where it resides, and how to protect and prevent exfiltration of that data, Grupo Bimbo leveraged Microsoft Security for its data security needs:

"We're using Microsoft Purview to keep Grupo Bimbo data more secure, more proactively than ever before."

– **Alejandro Cuevas, Global Director of Information Technology, Risk, and Compliance, Grupo Bimbo**

"The Adaptive Protection capability is a perfect example of how helpful machine learning can be, because we use it to make security-based decisions rooted in logic and context. Being able to adjust to context dynamically helps us achieve a more effective balance between safety and flexibility."

– **Jose Antonio Parra, Vice President of Global Digital Transformation, Data and Analytics, Grupo Bimbo**

Read Grupo Bimbo's story

A comprehensive approach to data security

Microsoft's Security solutions integrates Microsoft Copilot in an extensive product range to deliver capabilities that will transform how you secure your organization's data across estate, devices, and generative AI applications.

With Microsoft Security solutions, you can:

Discover, classify, and protect sensitive data throughout its lifecycle, no matter where it lives or travels with **Microsoft Purview Information Protection**.

Understand user activity and context around the data and identify risks with **Microsoft Purview Insider Risk Management**.

Prevent unauthorized or accidental use of data with **Microsoft Purview Data Loss Prevention**.

Dynamically tailor protection controls based on user risk level with **Adaptive Protection in Microsoft Purview**.

And Microsoft Purview integrates with Microsoft Security solutions to:

Quickly investigate and respond to data security incidents with **Microsoft Copilot for Security**.

View data security incidents in context of security incidents in **Microsoft Defender XDR**.

Allow or deny users access to applications where data resides with **Adaptive Protection** integrated with **Microsoft Entra Conditional Access**.

And more...

Secure your data in the age of AI

Secure your data with a comprehensive approach that combines data and user context across your estate, devices, and generative AI applications. Speak with a representative and put Microsoft's data security solutions to work helping you get the most out of your data and confidently adopt generative AI.

Connect with a representative and put Microsoft Security solutions to work.

Get started

Microsoft Security

1. Data Security Index, September 2023, Microsoft Security https://info.microsoft.com/ww-landing-data-security-index.html