Microsoft Security

Securing Your Data in the Age of Generative AI

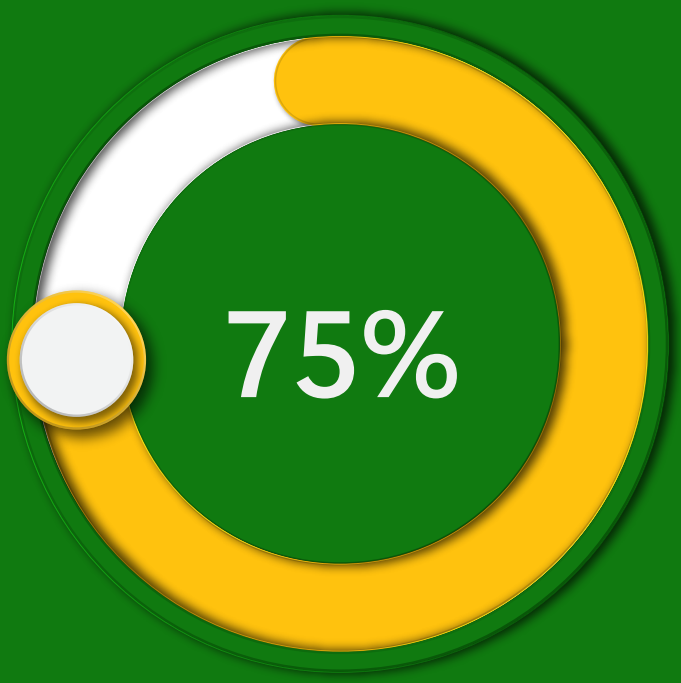
Insights and Strategies for CISOs

Table of Contents

Introduction

Data security is shifting with the adoption of Generative AI

Generative AI creates new content from existing data, empowering organizations to transform operations, drive innovation, delight customers, and enhance productivity. However, maximizing the value of this exciting new technology requires effective data security to combat data oversharing, leaks, and noncompliance. Integrated data security, governance, and compliance tools help mitigate these risks and support the safe deployment of Generative AI technology.



of knowledge workers use Generative AI at work today, saying it helps them:

- Save time (90%)
- Focus on their most important work (85%)
- Be more creative (84%)
- Enjoy their work more (83%)[1]

[1]GenAI at Work Is Here. Now Comes the Hard Part

Three areas of Generative AI risk to consider

Data leaks: Users might expose sensitive data, such as customers' personal information, when interacting with Generative AI applications through chat, form submissions, or document uploads. Detecting and controlling these interactions can help ensure sensitive data stays secure.

Data oversharing: Misconfigured permissions or access controls can expose sensitive data to unauthorized parties through Generative AI applications.

Non-compliant usage: Without the right guardrails, individuals can use Generative AI tools to create unethical or high-risk material.

Addressing new and existing data security challenges with an integrated solution

The need for integrated data security solutions has never been greater. The datasphere doubles every four years. The rapid adoption of Generative AI will further fuel the data explosion. Rapidly growing data stores make it more important—and more challenging—to prevent data security incidents.

To prevent business-critical data and safeguard their competitive edge, reputation, and customer loyalty, organizations need to secure their data with a comprehensive approach that combines data and user context across their estate, devices, and Generative AI applications.

However, many organizations continue to use disparate data security solutions, which can increase the cost and risk of these activities. They create silos that leave gaps in protection, leading to vulnerabilities and inefficiencies.

By choosing an integrated data security platform, organizations can unify policies, visibility, and enforcement across the entire data ecosystem. This approach reduces complexity, lowers costs, and strengthens defenses against emerging risks, helping to enhance data security wherever data lives.

Customer Story:

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 uses 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 >

Chapter 1

A three-pronged strategy

Secure data with a comprehensive approach across your estate, devices, and Generative AI applications. In this section, we examine three critical components to data security: discovering data risk, preventing data loss, and responding to security incidents.

Discover hidden risks to data wherever it lives or travels

Uncover hidden risks to your data using AI-driven aggregated insights with correlated data and user context. Understanding the location and volume of sensitive data enables better protection and management.

- **Gain visibility:** Understand where sensitive data lives across files, documents, emails, messages, devices, databases, and more.
- **Classify and protect:** Use intelligent classifiers to find and secure sensitive information quickly.
- **Detect insider risks:** Employ machine learning to surface threats without manual intervention.

More than 30 percent of decision-makers say they don't know where or what their business-critical data is.[2]

[2] Data Security Index | Microsoft Security

Protect and prevent data loss across your data estate

Flexible controls help protect data across on-premises, cloud, and hybrid environments, diverse devices, and applications while balancing security and productivity.

- **Manage DLP policies centrally:** Choose a solution that enables data security teams to create and administer comprehensive DLP policies within a single tool.
- **Apply for adaptive protection:** Dynamically tailor protection controls based on user risk level. DLP controls can be automatically applied more stringently to higher-risk users.
- **Extend DLP policies across the application landscape:** Choose solutions that apply protections to the broadest range of applications, including SaaS.

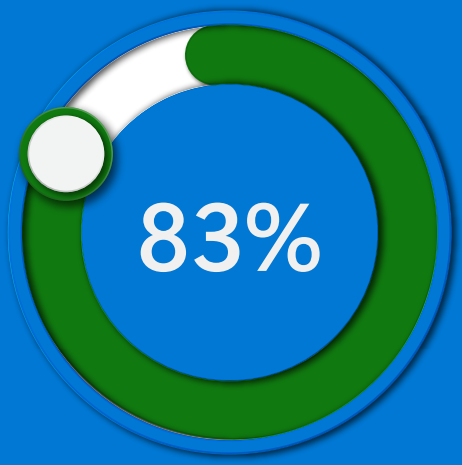
of security leaders say sensitive data leakage is their primary concern.[2]

[2]Data Security Index | Microsoft Security

Quickly investigate and respond to data security incidents

Respond to data security incidents at machine speed using AI insights correlated across an integrated set of products.

- **Enhance DLP investigations:** Improve understanding of DLP incidents with a full picture of user and content context, including where the files originated and actions the user took.
- **Empower investigators with unified tools:** Choose solutions that provide comprehensive alert triaging, management, and remediation in one place.
- **Resolve cases faster:** Accelerate time to action with intuitive investigation tools that empower investigators to efficiently review content, examine forensic evidence, and escalate cases to eDiscovery.



of organizations experience more than one data breach in their lifetime.[2]

[2]Data Security Index | Microsoft Security

Chapter 2

Addressing Generative AI–specific challenges

To fully capture the value of Generative AI investments, organizations should choose an integrated data security solution that incorporates purpose-built Generative AI security and governance features. Such tools can offer a view into data flows, risks, and governance efficacy. Here are three categories of Generative AI–specific capabilities to consider when building a data protection strategy.

Discover Generative AI application usage

Understanding sensitive data flow and interactions allows teams to pinpoint vulnerabilities and target security strategies. Security tools can offer real-time visibility into Generative AI application usage, alerting administrators to unauthorized access or use.

- **Analyze usage:** Security tools make it easy to see which information is shared with Generative AI applications, helping assess risks accurately.
- **Identify critical risks:** Data discovery solutions prioritize sensitive data, preventing oversharing and ensuring better protection.
- **Detect unethical interactions:** Detection systems spot regulatory violations, money laundering, and targeted harassment, enabling prompt action.

Protect sensitive data

Tools such as encryption, role-based access, and automated labeling help reduce the likelihood and severity of data breaches.

- **Implement data security controls:** Technologies like encryption, watermarking, and auto-labeling support appropriate access measures to ensure Generative AI is honoring permissions in files it references.
- **Prevent data leakage in third-party apps:** Dynamic protection measures can help prevent the pasting of sensitive data into Generative AI prompts, reducing leakage risks.
- **Apply adaptive protection: Tailored** security measures based on user risk levels help support flexible policies.

Govern Generative AI usage

Navigating the regulatory landscape for Generative AI requires comprehensive governance and integrated compliance tools. Adopting robust frameworks and ensuring data visibility simplifies adherence to evolving standards. Integrated tools track Generative AI interactions and enforce policies, helping avoid legal penalties and showing a commitment to ethical AI practices. Proactive compliance supports confident innovation and stakeholder trust.

- **Detect Generative AI interactions:** Logging and auditing tools capture and review Generative AI prompts and responses, offering the ability to review and improve company practices and policies.
- **Detect and mitigate risks:** Advanced classifiers and machine learning identify and block or otherwise mitigate unethical Generative AI prompts.
- **Streamline legal responses:** eDiscovery solutions efficiently preserve and collect relevant Generative AI data, minimizing legal exposure.

Address emerging GenAI regulatory compliance needs

Evolving Generative AI regulations require robust strategies that align with both current and emerging standards. Relevant tools can help promote ethical Generative AI use, foster trust, and support confident innovation within regulated environments.

- **Comply with Generative AI regulations:** Assessment templates and compliance management tools help organizations align with standards like the EU AI Act and NIST AI RMF.
- **Strengthen compliance controls:** Continuous risk detection and auditing assist with regulatory adherence.
- **Reduce compliance risks:** Deploy tools for data visibility to help prevent unauthorized sharing to or from AI applications.

Chapter 3

Empowering data security professionals with Generative AI

Comprehensive governance and Generative AI protections help address emerging security challenges. In addition, Generative AI has the potential to put new capabilities in the hands of security teams, redefining how they approach the protection of sensitive information.

For example, Generative AI helps identify and prioritize security risks by improving the understanding of intent and context, making it easier to address potential threats. It accelerates and simplifies investigations for administrators and empowers security operations center (SOC) analysts with enhanced intelligence and data, elevating their capabilities.

of organizations report that their data security team needs more people to manage critical responsibilities effectively.[3]

[3]Data Security Index | Microsoft Security

Benefits of Generative AI for security

Efficiency: Generative AI helps prioritize and automate security tasks to improve productivity.

Speed: Generative AI helps people understand unique cyber threats in real time, speeding detection and response.

Scale: Generative AI processes large volumes of data efficiently, making it possible to manage extensive and complex security environments.

How Generative AI can enhance data security capabilities

Alert summarization: Generative AI summarizes data loss prevention (DLP) and insider risk management alerts, enabling security teams to quickly understand the nature and severity of potential threats without manually sifting through extensive logs.

Automated triage: By prioritizing alerts based on risk, Generative AI enables security professionals to focus on the most critical issues. This triage process helps distribute resources efficiently and accelerates breach response times to potential breaches.

Data insights and analysis: Generative AI can analyze vast amounts of data to identify patterns and correlations that might indicate security risks. This analysis includes examining user behavior and communication patterns to detect anomalies indicative of insider risks or exfiltration attempts.

Interactive prompting: Interactive prompts allow security professionals to ask specific questions and receive details about their security and compliance status. Queries like "Summarize the DLP alert with ID 12345" or "Show me the top five Insider Risk Management alerts from the past 24 hours" provide immediate actionable information.

Compliance and policy management: Generative AI can support more effective compliance by summarizing policy matches based on trainable classifiers. This capability supports continuous detection of issues and enforcement of standards.

eDiscovery and legal hold: Generative AI provides contextual summaries for eDiscovery cases, efficiently grouping and reviewing documents. This feature helps legal teams manage data for litigation or regulatory inquiries.

A comprehensive approach to data security

Microsoft security solutions enhance your organization's ability to secure data across your entire estate, devices, and Generative AI applications. Microsoft Purview offers a unified suite of tools to govern, protect, and manage your data, no matter where it lives. By providing integrated coverage, Microsoft Purview increases visibility for better protection and governance and adapts to the evolving roles within IT management.

- 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 the rest of the Microsoft Security ecosystem to help your team:

- Quickly investigate and respond to data security incidents, with Microsoft Security Copilot.
- View data security incidents in context using Microsoft Defender XDR.
- Allow or deny users access to applications where data resides, with Adaptive Protection integrated with Microsoft Entra Conditional Access.

Additionally, with Microsoft Purview Copilot, organizations can revolutionize their data security and compliance using AI-powered insights and automation. By integrating Copilot, teams can quickly investigate and respond to data security incidents and gain a deeper understanding of their data through interactive summaries and risk analysis. This enables a more streamlined and effective approach to managing risk and protecting sensitive information.

Why Microsoft for Generative AI data security?

Microsoft offers an integrated approach to data security built on a trusted platform with tools that address existing and emerging challenges while maximizing productivity and efficiency. As part of the Microsoft security ecosystem, Purview and Security Copilot empower you to strengthen your data protection framework so your business can harness the full potential of Generative AI. With the right approach, Generative AI itself can be a powerful ally in safeguarding your data.

Learn more about Microsoft data security solutions and how they empower your team in the era of Generative AI.

Microsoft