Microsoft Security

Data Security Index

Trends, insights, and strategies to keep your data secure and navigate generative AI

2024 Report

Foreword

As we embark on our second year of research into the evolving data security landscape, the challenges and opportunities before us have never been more profound. In the past year, the severity of data security incidents has increased. In this data-centric era, the strategies and tools used to keep data protected are evolving at a rapid pace.

This year, we explore a new frontier: the role and impact of generative AI (AI) on data security strategies.

AI is making waves around the world with unprecedented capabilities to unlock more innovation and efficiency. Yet with this enormous potential, organizations are also concerned with data security risks and how that might shape the responsibilities for data security teams. We see AI being an accelerant for organizations to strengthen their foundational data security practices so that they can prepare to minimize the impact of data oversharing and data leaks, and create processes for secure AI adoption. On the other hand, AI can also help organizations enhance their data security practices by identifying hidden risks and gaps in protection, recommending protection policies, as well as helping investigate and remediate security incidents faster.

The goal of our research is to provide data security leaders with actionable insights and guidance to help their teams confidently adapt their data security strategy to effectively protect AI use as well as integrate AI in their data security strategies. While remarkable in its reach and potential, AI is only the latest transformational wave sweeping across enterprises, like hybrid work, cloud, and mobility, that in recent years underscored the timeless need for visibility in their use to mitigate risk and maximize impact. Informed by these learnings, properly securing data used in AI, as well as using AI to enhance data security measures, will enable greater productivity, resilience, and agility as teams navigate future challenges.

We invite you to explore the latest findings and hope that the insights will help you strengthen your data security posture, as well as inspire you to embrace AI and build a comprehensive data security strategy, unlocking more innovation and ensuring a more secure future for us all.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

Introduction

With organizations experiencing an average of 156 data security incidents annually, the impact of these incidents remains a constant concern for data security decision-makers. There's a good reason why: a single incident can cause massive financial and reputational damage, especially in an ever-evolving threat landscape where attackers are exploiting any and all possible vulnerabilities. This is only exaggerated by the rapid adoption of AI, where without adequate protections and security measures, users can accidentally or maliciously put sensitive business critical data (including employee and customer information, intellectual property, financial forecasts, and operational data), at risk. As organizations look for new ways to safeguard this wide range of sensitive data, many decision-makers have turned their attention to the dramatic rise of AI.

The AI challenge is twofold. Given that two-thirds of organizations admit their employees are using unauthorized AI tools, it is critical that they ensure employees use AI tools securely. At the same time, there's an opportunity to wield AI as an effective tool in a sophisticated data security strategy.

AI-powered data security solutions are already playing a critical role in identifying and responding to threats in real time, improving the overall speed and accuracy of data security programs, and providing insights that help prevent data security incidents before they happen. Organizations must manage the risks that AI introduces in addition to harnessing its power to identify patterns that can be challenging for humans to process and analyze at machine speed, and ultimately fight off increasingly sophisticated cyberattacks.

In 2023, Microsoft commissioned an independent research agency, Hypothesis, to conduct a multi-national survey among over 800 data security professionals and embark on a Data Security Index initiative to better serve our partners and customers and help business leaders develop their own data security strategies.

In 2024, this report builds off the prior research with new insights among an expanded multi-national survey of over 1,300 data security professionals. While the data reveals consistent insights and trends across the markets we surveyed, we uncover fresh learnings around the latest data security and AI practices and trends across the globe.

hypothesis Microsoft Security

Key Findings

1

The data security landscape remains fractured, increasing the need for cohesive data security strategies across both traditional and new risks linked to AI use

Organizations report high levels of satisfaction and confidence in their data security measures. However, the severity of data security incidents continues to rise, particularly due to gaps organizations find between their current data security policies and the increased usage/introduction of AI applications. Facing these stakes and imperatives, many organizations still rely on multiple data security tools which can increase their overall vulnerability and risk.

2

As end-users increase their adoption of AI apps, the integrity of organizations' most sensitive data is at greater risk, requiring more visibility and new protection controls

As AI tools become essential to daily work, organizations are concerned about data security risks. They recognize the need to strengthen their defenses and are committed to preventing data security incidents caused by AI — but the unauthorized use of these tools highlights the need for more robust visibility.

3

Decision-makers are optimistic about AI's potential to boost their data security efforts

Organizations are actively investing in data security tools that incorporate AI to improve detection and response capabilities. AI can help detect unprotected data, recommend protection policies, and help investigate and remediate data security incidents faster, ultimately allowing data security teams to focus more time and attention on strategic work. The use of AI also boosts confidence and satisfaction in organizations' overall data security strategy — especially their ability to respond to incidents both quickly and accurately.

1

The data security landscape remains fractured, increasing the need for cohesive data security strategies across both traditional and new risks linked to AI use

There is a disconnect between decision-makers' confidence in their data security practices and the true level of protection of their data

As reported in 2023, the vast majority of decision-makers are confident in their data security strategies, with 74% reporting satisfaction with their current solutions in 2024. They feel secure in their ability to track and manage sensitive data: 88% believe they know where most of their critical information resides, and 85% say their data is properly classified and labeled. Most also trust their defense controls, with 79% confident they can prevent data exfiltration, and 76% describing their approach as proactive rather than reactive.

However, their confidence is being tested as incident severity continues to grow. **The average number of annual data security incidents has remained high from 166 in 2023 and 156 in 2024, and the severity of these incidents has increased from 20% of incidents being severe to 27% in 2024.**

156

data security incidents

27%

of incidents considered severe
(increase from 20% in 2023)

63%

of alerts reviewed per day

"The location where a software platform was established, where its data is stored, and who will access that data complicated the data security and management of our AI tools and vendors. We have more than 100 years' worth of data we must protect and govern in accordance with legal requirements in every jurisdiction we operate in," says a Senior Manager for Information Governance at a heavy equipment manufacturer.

The increase in severity of data security incidents has consequently led to an increase in volume of alerts. **Organizations are facing an average of 66 alerts per day, up from 52 in 2023.** That number varies significantly by organization size, with medium enterprises (500-999 employees) and large enterprises (1,000-4,999 employees) receiving an average of 56 alerts and extra-large enterprises (5,000+ employees) receiving 80 alerts per day on average.

Given the sheer volume of data security alerts, it should come as no surprise that most organizations simply can't keep up. On average, data security teams review 63% of their daily alerts. Thirty-five percent of these alerts turn out to be false positives. This mismatch between perceived control and operational reality leaves data security teams overwhelmed — trying to assess if they have the right protections in place or how to fine tune them, all while being concerned that potentially serious incidents could slip through the cracks.

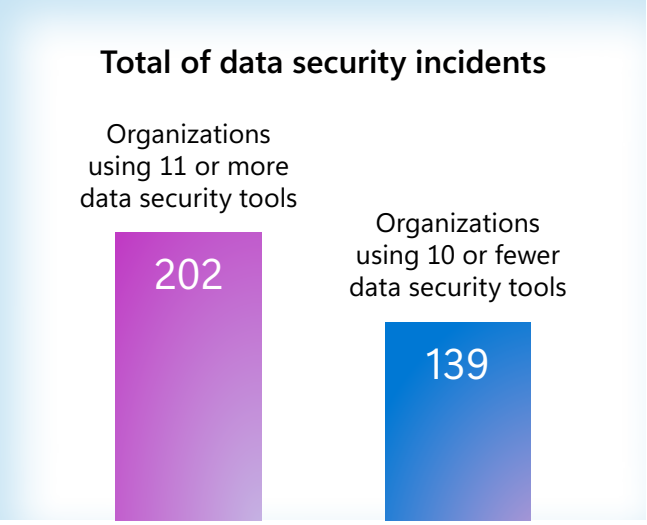
To combat traditional and emerging data risks linked to the use of AI tools, there's a growing need for more robust and cohesive data security strategies

Despite the growing number of tools at their disposal, many decision-makers continue to acknowledge that more isn't always better. In fact, 21% cite the lack of consolidated and comprehensive visibility (and shared understanding of risks) caused by disparate tools as their biggest challenge/risk.[1]

Most decision-makers (82%) agree that a comprehensive, fully integrated platform is superior to managing multiple isolated tools. **On average, they're juggling 12 different data security solutions, creating complexity that increases their vulnerability.** This is especially true for the largest organizations: on average, medium enterprises use 9 tools, large enterprises use 11, and extra-large enterprises use 14.

The data shows a strong correlation between the number of data security tools used and the frequency of data security incidents. Medium and large enterprises report an average of 89 incidents per year, while extra-large enterprises face a staggering 248 incidents annually. This stark difference highlights the high risk larger organizations face, even as they express considerable confidence in their data security measures.

In 2024, organizations using more data security tools (11 or more) experienced an average of 202 data security incidents, compared to 139 incidents for those with 10 or fewer tools.



Fragmented solutions make it difficult to understand data security posture since data is isolated and disparate workflows could limit comprehensive visibility into potential risks. When tools don't integrate, data security teams have to build processes to correlate data and establish a cohesive view of risks, which can lead to blind spots and make it challenging to detect and mitigate risks effectively.

A growing area of concern is the rise in data security incidents from the use of AI applications, which nearly doubled from 27% in 2023 to 40% in 2024. This rise in incidents is fueled by a surge in malware and ransomware attacks, up to 59% from 50% in 2023. Attacks from the use of AI apps not only expose sensitive data but also compromise the functionality of the AI systems themselves, further complicating an already fractured data security landscape. In short, there's an increasingly urgent need for stronger, more cohesive data security strategies that can address both traditional and emerging risks linked to the use of AI tools.

1. September 2024 survey among data security, governance, compliance, and privacy decision makers commissioned by Microsoft from agency MDC Research

The Path Forward

The increase in severity of data security incidents illuminates an opportunity for AI to help. Organizations that are on the cutting edge are implementing AI-powered data security to help with incident prioritization, automate data classification, and identifying ways to fine-tune current protection policies. AI can automatically synthesize the potential severity of incident alerts, providing data security teams with actionable insights for quick response to reduce the time spent on false positives. This streamlines workflows and enables data security teams to focus on more strategic data security improvements and proactive measures.

2

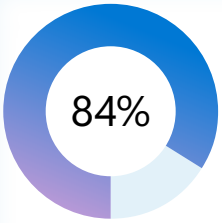
As end-users increase their adoption of AI apps, the integrity of organizations' most sensitive data is at greater risk, requiring more visibility and new protection controls

AI is quickly becoming being essential for day-to-day work — and organizations must embrace and actively adapt to that new reality

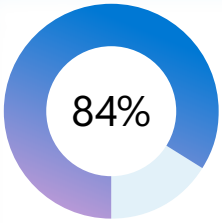
The rapid adoption of AI tools by employees has prompted major changes in organizations' approach to data security. While AI is transforming productivity and workflows, like any emerging technology it can also amplify existing risks or introduce new risks that require a different approach to safeguarding sensitive information. As a result, companies are still finding their footing in a rapidly shifting landscape. A Director of Engineering and Analytics in transportation claims, "we're monitoring data more carefully on the AI side. There's been a tension between productivity and security, preciseness and privacy."

Confidence in securing employees' use of AI remains mixed. A majority (84%) would like to feel more confident about managing and discovering data input. While 22% of organizations feel extremely confident in their ability to keep data secure, most (59%) are only "very confident," indicating there's room for improvement. Most companies (86%) acknowledge that they would like to feel more bullish about managing and discovering data generated by AI tools.

As AI becomes more essential for daily productivity, the use of AI apps has also heightened concerns around data security incidents. **Nearly one-third (31%) of organizations anticipate an increase in data security incidents due to employee use of AI, and 84% admit that they need to do more to protect against these risks.** Such anxieties are especially high among the largest organizations: while 26% of medium enterprises expect to see an increase in AI-related data security incidents and 29% of large enterprises project a rise, a significantly higher group representing 36% of extra-large enterprises foresee an increase.



want to feel more confident about managing and discovering data input into AI apps and tools



agree they need to do more to protect against risky employee use of AI apps and tools

Unauthorized use of AI is widespread

Forty percent report that their AI apps have already been breached or compromised in a data security incident. Again, this figure is higher among larger organizations: medium enterprises report a 36% rate of incidents, large enterprises report 38%, and extra-large enterprises have seen the most occurrences, at 44%.

Unauthorized use of AI often occurs with employees logging in with personal credentials or using personal devices for work-related tasks. **On average, 65% of organizations admit that their employees are using unauthorized AI tools.** Ways in which employees are using unauthorized AI tools include:

- 53% who log in with personal credentials for work purposes
- 48% who use their personal device when using AI for work
- 47% who use their work credentials to use AI for personal purposes

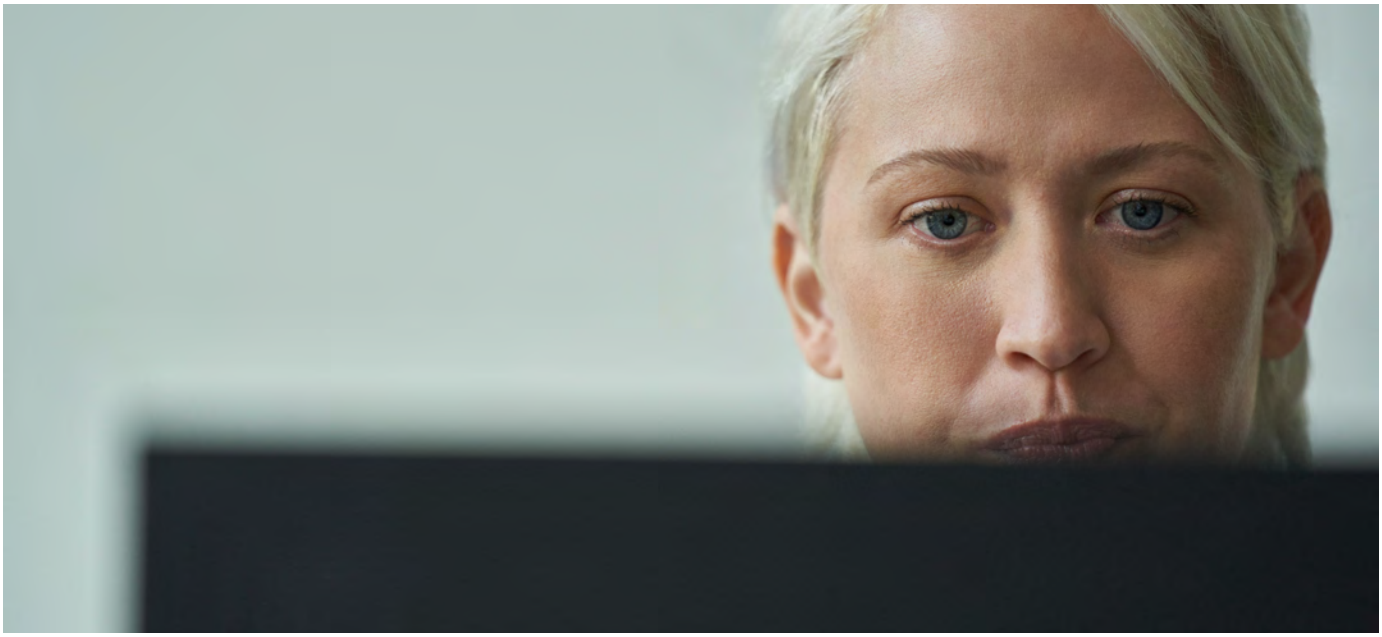
Half of all organizations say they are concerned about a lack of controls to detect and mitigate risks when employees use AI apps in unsafe ways. This figure varies by company size, with 43% of medium enterprises, 50% of large enterprises, and 54% of extra-large enterprises expressing concern about their ability to manage these risks.

Given the increased use of AI, more data security controls are necessary

As AI becomes more embedded in daily operations, organizations recognize the need for stronger protection. **While 96% of companies have concerns about employee use of these tools, nearly as many are willing to invest in solutions to overcome their concerns.**

"The big focus is going to be how do you get ahead of AI? The security focus is about reducing the size of data, monitoring data more carefully. On the AI side, to make your models more representative to identify bias, you need more data. So how do you reconcile?" says a Director of Engineering, Architecture, and Analytics in transportation. The vast majority of decision-makers (87%) are ready to spend both time and money on training employees in secure practices for using AI tools. **That's because 85% say it's critical for employees to use these tools to stay competitive.**

Nearly all organizations (93%) are at some stage of developing or implementing controls around AI usage, but many are still in the early phases. Only 39% have fully implemented data security controls for AI, while 24% have developed policies but haven't yet put them into action. A VP of Data Security in hospitality claims, "we've got to align on controls for AI but are embracing the use of AI in the meantime. It does make life better and helps us be more efficient."



While organizations are taking steps to protect sensitive data from being misused in AI apps, there's a clear need for more comprehensive controls. Currently, 43% of companies are focused on preventing sensitive data from being uploaded into AI apps, while another 42% are logging all activities and content within these apps for potential investigations or incident response. Similarly, 42% are blocking user access to unauthorized tools, and an equal percentage are investing in employee training on secure AI use.

Companies with employees who engage in unauthorized AI usage have a higher need for certain types of controls. **Among those with unauthorized AI usage, 42% need controls to identify risky users based on AI queries, compared to 30% for those without unauthorized use. Moreover, 40% of organizations dealing with unauthorized AI use need controls to manage the lifecycle of data (such as retention and deletion protocols), compared to 27% of companies without this issue.**

Top 5 AI controls needed

Prevent sensitive data from being uploaded to AI	43%
Log all activities and content in AI tools for potential investigations or incident response	42%
Block user access to unauthorized AI tools	42%
Train employees on secure AI tool use	42%
Identify risky users based on queries into AI	41%

The Path Forward

To maintain a strong data security posture, teams need a complete set of controls to discover, protect, and govern their data in AI apps. Here are three key strategies that teams can use:

Increase visibility of AI app usage and data flowing through the app: Utilize data security tools that can detect and use of AI apps. These tools provide insights into a comprehensive list of AI apps being used along with their risk profiles, including details like supported data security controls and compliance with regulations. Use tools that can provide consistent classification for sensitive data in AI interactions, and show trends around how data is flowing through AI apps.

Develop and enforce policies: Create policies based on the insights gained from the analysis. These policies can include guidelines for approved AI apps and procedures for blocking or restricting employee use of unsanctioned apps. Even in sanctioned AI apps, you can create granular policies to allow non-sensitive data to flow through while restricting the use of sensitive and business critical data. This can include blocking certain actions, such as pasting sensitive data into browser-based AI tools to ensure data security.

Regularly assess risks and refine policies: Regularly generate reports that show the risk levels of the AI apps being used, trends on how sensitive data is flowing through these apps, as well as user activity around these apps. This helps in assessing the overall risk landscape and making informed decisions about the most relevant data security policies.

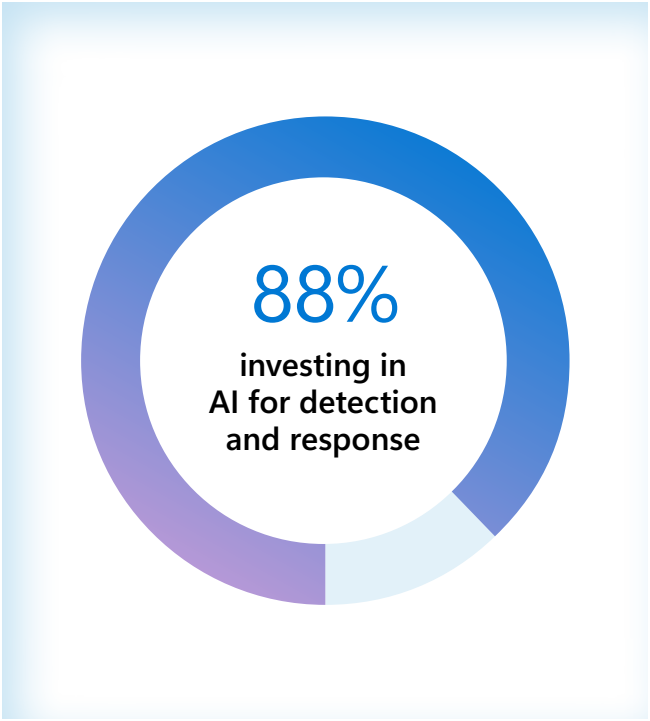
3

Decision-makers are optimistic about AI's potential to boost their data security efforts

Data security investigations rely heavily on AI

The vast majority (88%) of organizations are already investing in AI to improve their detection and response efforts — discovering sensitive data, detecting anomalous activity, and automatically protecting data at risk. **Seventy-seven percent of organizations believe that AI will accelerate these processes, and 76% think it will improve the accuracy of their detection and response strategies.**

While 73% of decision-makers express concerns about using AI to strengthen data security, 50% say it has not inhibited their use of AI to strengthen data security and only 23% say that it has held them back. Altogether, an overwhelming 93% are at least planning to use AI to strengthen data security despite concerns.

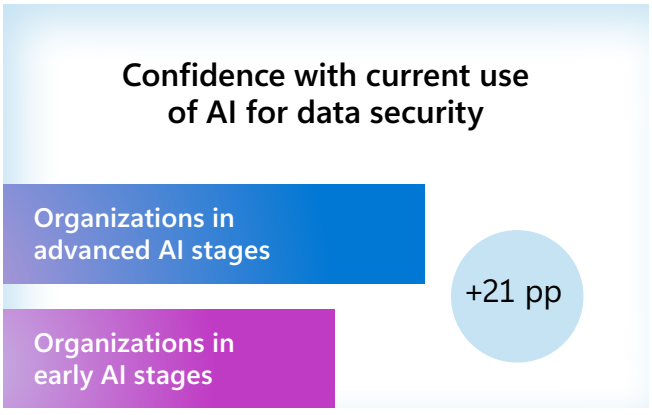


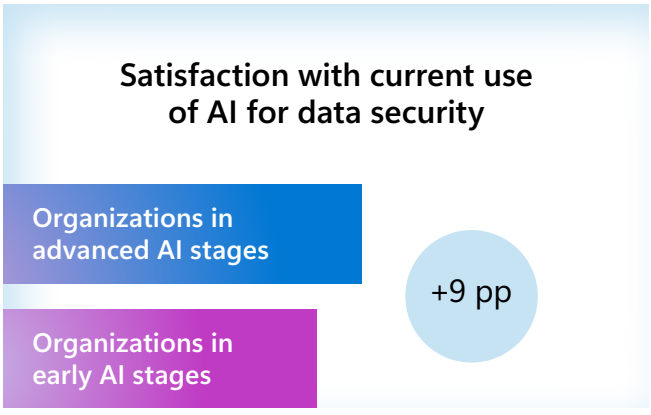
Using AI to strengthen data security increases visibility, confidence, and satisfaction

One of the key benefits of using AI to strengthen data security is its ability to increase visibility across systems, mitigating a prominent concern decision-makers have of knowing where data is stored and how it's classified (20%).[1] 88% of data security decision-makers believe integrating AI into data security solutions will enable teams to have more visibility, which will allow organizations to process and analyze far more data than would otherwise be possible. Medium organizations are primarily focused on reducing short-term risks, such as minimizing human error in their data security processes. In fact, 43% of medium enterprises prioritize reducing risks caused by human error, compared to just 37% of extra-large enterprises.

In contrast, larger enterprises are more advanced in their approach, emphasizing longer-term risks and the need for adaptability. That heightened level of sophistication allows data security teams to better adapt to evolving risks — a top priority for 49% of extra-large enterprises, compared to 43% of medium organizations.

Overall, organizations that are further along in their use of AI to strengthen data security report much higher levels of confidence and satisfaction with their data security strategies. **Among those in the advanced stages of AI implementation, 90% feel extremely or very confident in their use of AI to strengthen data security, compared to 69% in earlier stages. Similarly, 76% of organizations with advanced usage of AI express satisfaction with their data security solutions, while only 67% of those in earlier stages report the same.**





1. September 2024 survey among data security, governance, compliance, and privacy decision makers commissioned by Microsoft from agency MDC Research

Organizations are reducing the number of data security incidents and improving alert management with AI

Organizations using AI to strengthen their data security operations report significantly fewer alerts. **On average, those who have implemented AI-driven data security tools receive 47 alerts per day, compared to 79 alerts for those who have not. And, those using AI are able to review 66% of their daily alerts, while organizations not using AI only manage to review 60%.**

Additionally, those using AI to strengthen data security are more likely to also be using AI to mitigate risks (56% vs. 26%). The reduction in the volume of alerts, along with the increased ability to mitigate them leveraging AI, appears to have had a dramatic impact on the overall number of data security incidents. Organizations that have implemented AI to strengthen data security see a 65% reduction in data security incidents compared to those not using AI to strengthen data security.

AI is expected to have the biggest impact on response

In terms of detection, 33% of decision-makers expect AI to help detect anomalous activity, while 23% believe it will assist in investigating potential data security incidents. Another 22% see the potential for AI to make recommendations for better securing their data environments.

However, response is where decision-makers expect AI to make the most profound impact. Thirty-four percent believe AI could automatically block inappropriate sharing of sensitive data, and 32% say it will protect data at risk. Another 26% see AI helping to mitigate data security risks and apply appropriate controls, while the same number expect AI to automatically flag risky user behavior.

The Path Forward

Integrating AI into data security solutions can help by offering teams real-time guidance, summarization capabilities, and natural language support to spotlight areas that may have otherwise gone overlooked. This can also accelerate investigation and bolster expertise across data security teams. Here's how these capabilities can make an impact:

Alert summarization: Investigations can be daunting due to the volume of sources to analyze and diverse policy rules. By embedding AI in data loss prevention (DLP) and insider risk management (IRM), teams can quickly receive a summary of alerts, including the source, policy rules, and user risk insights to understand what sensitive data was compromised and the associated user risk.

Contextual communications: Organizations must adhere to regulatory requirements around business communications, which often necessitates an extensive review of violations. AI can help data security teams assess content against regulations and corporate policies to highlight high-risk communications that could result in a data security incident.

Natural language to keyword query: Search can be a complex and time-consuming workflow during investigations, typically requiring the use of keyword query language. AI allows data security teams to input search prompts in natural language to streamline the start of the search and enable more advanced investigations.

Final Recommendations

1 Hedge against data security incidents by adopting an integrated platform

Adopting a fully integrated data security platform offers a safer, more streamlined strategy in an increasingly evolving landscape, reducing complexity and increasing visibility while improving protection. An integrated approach can help organizations improve data security posture management by centralizing data security controls and providing unified visibility across data, users, and activities, therefore strengthening and streamlining detection and protection around data risks. With 82% of organizations agreeing that an integrated platform is superior, the move toward consolidation isn't just beneficial — it's essential.

2 Increase visibility into the internal use of AI to assess the necessary controls for employee use of AI that won't impact productivity

As AI becomes more common in the workplace, it can amplify existing risks and introduce new risks. Organizations admit they need to do more to protect against unsafe AI usage. Utilizing built-in controls and visibility into AI apps is critical to maintain data security without disrupting productivity. Training employees on secure AI use can help organizations minimize risky behavior while ensuring that teams continue to benefit from these powerful tools.

3 Uplevel your data security strategy with help from AI

AI allows data security teams to focus on more strategic initiatives instead of reacting to constant threats and a high volume of alerts. Companies in the advanced stages of AI implementation are more confident and more satisfied with their data security solutions than those just starting out. By deploying AI as part of a comprehensive data security strategy, organizations can enhance their visibility, which strengthens their ability to detect and respond to risks, ultimately bolstering their overall data security posture.

Research Objectives

The objectives of the research included:

1. Understand the data security landscape, including priorities and mindsets, challenges, and the cause and effect of data security incidents.
2. Explore the future of data security, including what strategies and innovations are emerging and how organizations intend to invest in the future.
3. Uncover AI's role in enhancing data security and the role AI plays in protecting data.

Methodology

A 20-minute multi-national online survey was conducted August 5–23, 2024 among 1,376 data security decision-makers.

Questions centered around the data security landscape and data security incidents in comparison to 2023. In addition, the survey this year included questions around securing employee use of AI and the use of AI to strengthen data security.

Audience Recruit

To meet the screening criteria, data security decision-makers needed to be:

- CISO and adjacent decision-makers (C-2 and above) with purview over data security
- Work at enterprise organizations (500+ employees; range of sizes)
- Mix of regulated and non-regulated industries (no education, government, or non-profit)

Of the 1,376 data security decision-makers surveyed for the research, completes by country were:

- US: 302
- UK: 305
- India: 301
- Brazil: 158
- France: 156
- Australia: 154

hypothesis Microsoft Security