Microsoft Security

Data Security Index

Unifying Data Protection and AI Innovation

2026 Report

Foreword

Over the past year, organizations have been strengthening their foundations to apply data security and governance controls to new AI apps and agents. The rise of generative AI (GenAI) is reshaping how work gets done. According to the 2025 Work Trends Index, the majority of global knowledge workers surveyed report using AI, and more than 70% say they are bringing their own AI tools to work[1]—highlighting a growing trend in AI adoption. But it has also introduced new urgency: visibility, governance, and protection of data are now essential prerequisites for safe and responsible innovation.

In this third edition of the Data Security Index, we explore how generative AI is reshaping data security. Security leaders need a unified view of their data to adopt AI responsibly. In response, organizations are moving beyond fragmented tools toward integrated platforms that deliver continuous visibility and consistent protection—making security and innovation inseparable. To adopt AI confidently, organizations must first establish a unified understanding of their data: where it resides, who can access it, and how it's protected. Fragmented tools and siloed controls are giving way to the goal of integrated platforms that provide continuous visibility and consistent protection across environments.

At Microsoft, we believe that visibility, actionability, and integration are key to unlocking the full potential of AI, facilitated by a unified data security strategy. Integrated solutions that bring together visibility, protection, detection, and investigation capabilities make it possible to scale securely while minimizing complexity. These capabilities not only help detect and mitigate data risks but also enable organizations to embrace AI responsibly and accelerate innovation.

The insights in this paper underscore a clear truth: the organizations best prepared for the future are those investing in integration, intelligence, and responsible AI adoption. These principles form the backbone of a data security strategy that protects today's digital ecosystems and paves the way for innovation tomorrow.

We invite you to explore these insights and apply them to strengthen your security posture while responsibly advancing AI adoption. Together, we can create a security-first foundation for innovation, turning complexity into clarity and setting the stage for a more adaptive, trusted future.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

1. Microsoft, 2025, Work Trends Index

Introduction

In today's rapidly evolving digital ecosystem, organizations must navigate an increasingly complex data security landscape to keep their organization protected and stay ahead of emerging risks. Security teams are under pressure to do more with limited time, resources, and talent, even as the volume of data they must secure grows exponentially. As fragmented tools lead to gaps in visibility, introduce more complexity, and heighten the risks of data exposure, teams are shifting towards tool consolidation and stronger data security posture management to close blind spots, improve efficiency, and build lasting resilience.

Against this backdrop of rising complexity and risk, the latest technologies and tools are reshaping the data security conversation. Among them, generative AI (GenAI) stands out as a positive disruptor driving productivity and innovation. However, as organizations accelerate their GenAI adoption, they're also recognizing the need for increased data controls and governance.

To that end, teams are increasingly using GenAI itself to bolster their data security posture – leveraging it to uncover hidden risks, streamline operations, and effectively investigate their data risks – with AI agents and automation playing a larger role.

ABOUT THE RESEARCH

For the third year, Microsoft commissioned Hypothesis Group, an independent research and strategy agency, to conduct a multi-national survey of over 1,700 data security professionals.

This Data Security Index initiative has now expanded to 10 markets spanning the US, LATAM (Brazil), EMEA (UK, Germany, France), and APAC (India, Australia, Korea, Singapore, UAE) to better understand the needs of partners and customers across the globe as data security leaders develop their own strategies. Also new to the research this year are 10 in-depth interviews with data security leaders in the US and UK to contextualize insights with customer stories.

Key Findings

01
From Fragmented Tools to Unified Data Security

Customers are looking to consolidate solutions for improved data security, visibility, and governance.

Organizations are prioritizing investments in data security, shifting from tool sprawl to integrated platforms. A growing emphasis on Data Security Posture Management (DSPM) is helping teams strengthen visibility, reduce complexity, and move toward proactive data risk management.

86%
of surveyed leaders prefer integrated platforms over fragmented tools, citing better visibility, fewer alerts, and improved efficiency

80%+
of surveyed organizations are implementing or developing DSPM strategies

02
Managing AI-Driven Productivity Securely

As organizations embrace GenAI for productivity, the need for more robust data protection grows.

Organizations are balancing AI innovation with responsibility. Rising incidents linked to unauthorized AI use are driving stronger controls, refined policies, and renewed focus on employee education and secure AI governance.

32%
of surveyed organizations' data security incidents involve GenAI

47%
of surveyed organizations are implementing GenAI controls (+8pp increase vs. 2024)

03
Strengthening Data Security with GenAI

Through agents and automation, GenAI can be leveraged to enhance data security programs.

Data security leaders are increasingly utilizing GenAI to fortify their data security programs – automating detection, streamlining investigations, and enhancing protection. Human oversight remains critical as organizations embrace AI agents and automation to scale securely and intelligently.

82%
of surveyed organizations have developed plans to use GenAI in their data security program (+18pp increase vs. 2024)

39%
of surveyed organizations are using GenAI agents for data security and 58% of surveyed organizations say they are piloting/exploring

1 From Fragmented Tools to Unified Data Security

Customers are looking to consolidate solutions for improved data security and visibility, and governance

Organizations are prioritizing data security more than ever, directing new investment toward strengthening their defenses and enabling secure innovation

88% percent of surveyed decision-makers anticipate their data security and compliance budgets will increase in the next year. Ultimately, the objective behind their investments is to stay ahead of data risks, protect sensitive data, and safeguard responsible GenAI usage – all while continuing to enable innovation.

Top goals for increased data security investments

Among surveyed data security decision-makers

Staying ahead of evolving data security risks	57%
Protecting sensitive data	56%
Enabling secure innovation and adoption of new tech	53%
Ensuring safe and responsible employee use of GenAI tools	52%

> "If my team could do everything in their day-to-day roles in one ecosystem, that would make life a lot easier for us."
>
> Head of IT in Manufacturing

Teams struggle with visibility and governance because they lack a unified view of their data estate

Decision-makers cite that their top challenges with data visibility center around poor integration, lack of a unified view across environments, and disparate tools. One data security leader in Finance and Banking explains, "We have poor tool integration. The tools aren't giving the oversight we need. There's still a lot of false positives and alerts."

These silos make it difficult for teams to connect insights, correlate events, and maintain visibility across workloads.

Top challenges with data visibility

Among surveyed data security decision-makers

Poor integration with data security & management platforms	29%
Lack of a unified view across environments	25%
Disparate tools with no centralized dashboard	23%

Leaders are responding by consolidating tools and investing in unified platforms that simplify operations while improving visibility and control

86% of surveyed decision-makers agree that a comprehensive platform with integrated solutions outperforms managing multiple best-in-breed tools that have to be manually integrated and maintained. The benefits of consolidation are clear: having a unified approach enables improved data risk detection and response, simpler management for data security teams, and better visibility into data risks.

> "We're trying to use fewer vendors. If we need 15 tools, we'd rather not manage 15 vendor solutions. We'd prefer to get that down to five, with each vendor handling three tools."
>
> Global Information Security Director
> Hospitality & Travel

Top benefits of consolidation

Among surveyed data security decision-makers

Improved threat detection and response

Easier for data security team to manage and maintain

Better visibility into data risks across workloads

The drive for integration has accelerated the adoption of Data Security Posture Management (DSPM) strategies

Most organizations surveyed report that they are already developing or implementing DSPM strategies (i.e. frameworks that unify visibility, continuous data risk assessment, and policy enforcement across data environments) including:

Identifying and prioritizing data exposure risks or misconfigurations	82%
Detecting who accesses sensitive data, when, and how	81%
Defining and enforcing data security policies	80%
Discovering and classifying sensitive data across environments	79%

By building integrated ecosystems and embedding DSPM into their core operations, organizations are moving toward a future where data visibility and protection are no longer fragmented efforts, but part of a more cohesive data security strategy.

"I would say we have a pretty good DSPM strategy. We're integrating DSPM with identity management so that not only do we know where the data is, but we can ensure that only the right people have access to it. For us, it's about having a proactive, real-time capability to identify data that requires protection and then applying our control framework on it. DSPM allows us to make the application and management of controls more automated."

Global Information Security Director
Hospitality & Travel

The Path Forward

The proliferation of data and tools has made visibility and governance increasingly complex. To overcome these challenges, organizations must chart a path toward consolidation, integration, and proactive DSPM.

01

Integrate data security, visibility, and governance.

Surveyed leaders overwhelmingly agree that integrated platforms outperform fragmented toolsets. Consolidation simplifies oversight, enhances visibility, and strengthens threat detection and response. Organizations should prioritize building ecosystems where data security, compliance, and IT functions operate from a single, unified framework.

02

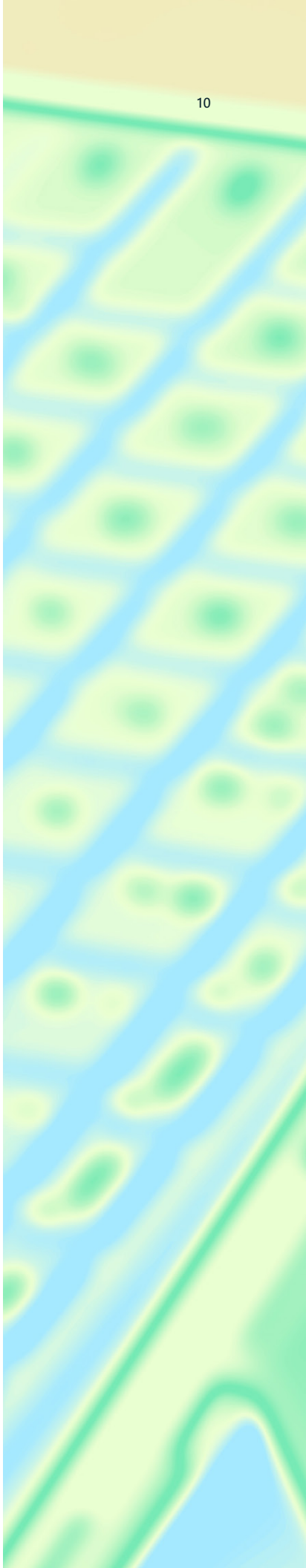
Leverage Data Security Posture Management (DSPM) as a facilitator for greater visibility and protection.

DSPM enables a shift from reactive protection to proactive data risk management. Investing in DSPM strategies allows teams to identify and prioritize data risks, monitor access to sensitive data, and enforce consistent policies across multi-cloud environments.

03

Build shared accountability for data security posture.

Establish clear ownership across IT and security operations to protect sensitive data and coordinate its flow across business units. Collaboration among IT, compliance, and security teams is critical for building lasting resilience in an increasingly complex data landscape.



2

Managing AI-Driven Productivity Securely

As organizations embrace GenAI for productivity, the need for more robust data protection grows

Generative AI (GenAI) is rapidly transforming how employees work, sparking a new wave of creativity, productivity, and innovation – but organizations aren't naïve to the potential data risks, especially from unauthorized GenAI use

Employees are excited to use GenAI; according to the 2025 Work Trends Index, the majority of global knowledge workers surveyed report using AI, and more than 70% say they are bringing their own AI tools to work[1]—signaling a rising trend in AI tool usage at work.

But as adoption accelerates, the conversation is shifting from enablement to responsible use. Leaders understand that the same technologies driving productivity also introduce new data risks – especially when employees experiment with GenAI in unmonitored or unauthorized ways.

70+%

of surveyed global knowledge workers say they are bringing their own AI tools to work[1]

32%

of surveyed organizations' data security incidents involve use of GenAI tools

According to surveyed organizations, a third (32%) of data security incidents involve use of GenAI tools, and 35% of surveyd organizations anticipate a higher volume of incidents in the coming year due to GenAI usage. The biggest concern isn't the technology itself, but how and where employees use it. Many are turning to consumer-grade GenAI tools or logging in with personal credentials, bypassing corporate protections and visibility.

1. Microsoft, 2025, Work Trends Index

Surveyed data security decision-makers mention that:

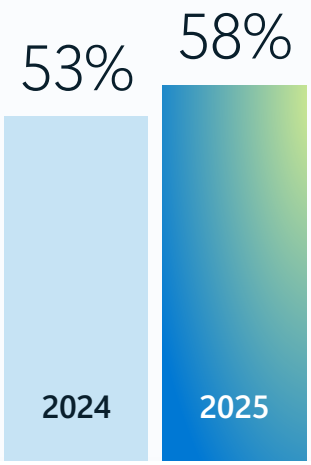
- Employees using personal credentials to access GenAI for work has increased by 5 percentage points year over year.
- Employees using personal devices to access GenAI for work has grown by 9 percentage points year over year.

> "We don't want confidential or restricted data to leave the firewall and it's absolutely doing that if they're using unsanctioned GenAI tools."
>
> Global Information Security Director
> Hospitality & Travel

These behaviors can expose sensitive data to external systems, leaving organizations blind to where information flows and who can access it. The tradeoff between productivity and protection is real – teams want to empower innovation, but not at the expense of data security or compliance.

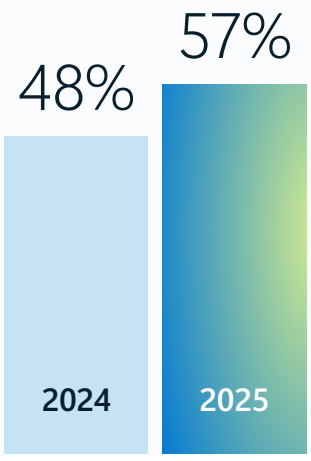
% of employees using personal credentials to access GenAI for work

Among surveyed data security decision-makers



% of employees using personal devices to access GenAI for work

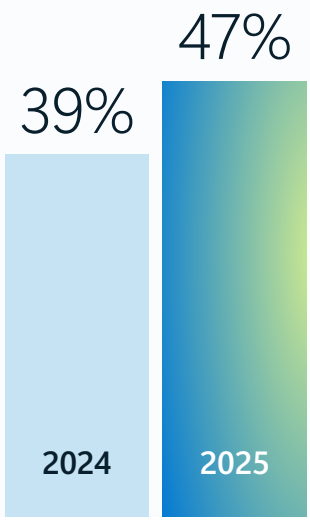
Among surveyed data security decision-makers



Recognizing these challenges, data security teams are taking decisive action to strengthen controls around employee GenAI usage

Nearly half (47%) of surveyed organizations are implementing specific GenAI controls in 2025, up from 39% the previous year – a meaningful jump that reflects growing urgency.

% of surveyed organizations implementing specific GenAI controls



Top priorities for GenAI-related controls

Among surveyed data security decision-makers

Preventing sensitive data from being uploaded into GenAI tools	42%
Training employees on secure use of GenAI tools	38%
Detecting anomalous user activity and identifying risky users	37%
Identifying sensitive data being uploaded to or generated by GenAI tools	37%

> "We're working to block GenAI tools that are not authorized but also increase what is authorized and steer people to that."
>
> CISO in Healthcare and Pharmaceuticals

Having these controls in place ultimately helps data security leaders feel more confident. Beyond the technology itself, decision-makers are encouraging employees to use sanctioned AI tools as well as reinforcing safe practices and building clear approval processes. The message is clear: the goal isn't to slow innovation – it's to enable it safely.

The Path Forward

As GenAI becomes embedded in daily operations, organizations must balance the drive for productivity with robust governance and control. The future of secure AI adoption will depend on visibility, education, and proactive management of data risk.

01

Strengthen visibility and control over GenAI usage.

Organizations should deploy data security tools that can detect and protect the use of GenAI apps across the enterprise, providing insight into which tools are being used, what data flows through them, and where potential risks lie. Continuous discovery ensures security teams can identify unauthorized usage before it escalates into a data incident.

02

Prevent data exposure through proactive protection policies.

Preventing sensitive data from entering GenAI tools is one of the most effective safeguards. Establish policies that restrict what types of data can be processed by GenAI applications and implement automated controls that block risky uploads or actions in real time.

03

Educate and empower employees.

Technology alone cannot solve the governance challenge. Continuous employee education – reinforced with clear guidance on approved tools and practices – helps foster a culture of responsible GenAI use. Transparency builds trust, enabling teams to harness GenAI's full potential without compromising data security.

3

Strengthening Data Security with GenAI

Through agents and automation, GenAI can be leveraged to enhance data security programs

Organizations are accelerating GenAI adoption in data security programs to maximize productivity & efficiency

82%

of surveyed organizations report that they have developed plans to use GenAI within their data security operations (vs. 64% in 2024)

Increasingly, organizations are turning to GenAI to bolster their data security programs – using it to detect risks faster, manage greater volumes of data, and fine-tune protection policies. In 2025, 82% of surveyed organizations report that they have developed plans to use GenAI within their data security operations, a significant increase from 64% in 2024.

The rise in adoption signals growing confidence among leaders that GenAI can help strengthen, not weaken, their overall security posture. Many are deploying GenAI for both proactive use cases, such as assessing & securing data environments and refining data security policies, as well as reactive use cases, like discovering sensitive data, detecting critical risks, and investigating potential data security incidents.

Top areas GenAI is being used in data security

Among surveyed data security decision-makers

Discover sensitive data	44%
Detect critical data security risks	43%
Investigate potential incidents	43%
Assess the security posture of data environments	42%
Secure the data environment	41%
Fine-tune data security policies	38%

> "Our GenAI systems are constantly observing, learning, and making recommendations for modifications with far more data than would be possible with any kind of manual or quasi-manual process."
>
> Director of IT in Energy

> "I would say we reduced manual overhead around our data security program by at least 40%. We improved our processes more than that, probably over 50%. Our GenAI programs are automating routine tasks and learning from evolving risks."
>
> SVP of Cyber, Cloud, and Third-Party Risk Management in Finance and Banking

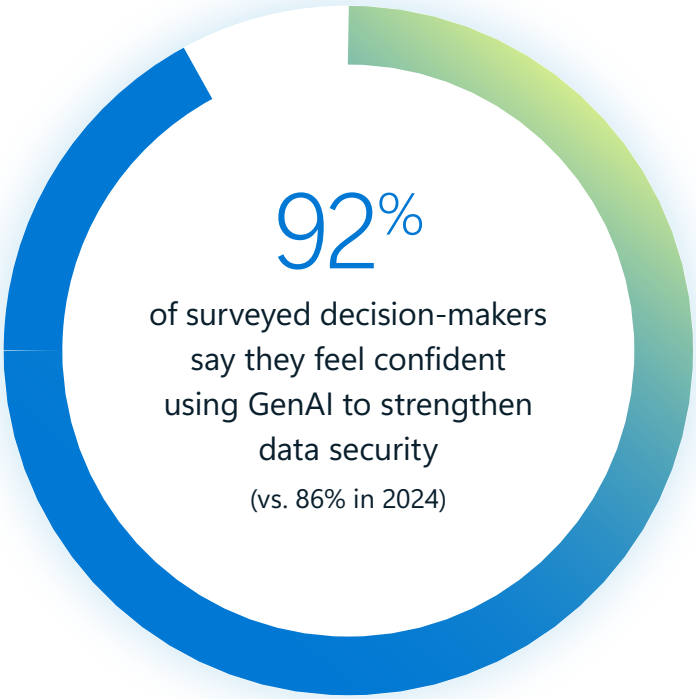
By automating routine data security tasks and helping to accelerate risk detection and response, GenAI empowers teams to do more with fewer resources. Decision-makers cite key benefits including improved efficiency, adapting to evolving risks, freeing up teams for more strategic work, and analyzing more data than traditional tools could handle.

Where GenAI delivers the biggest impact in data security programs

Among surveyed data security decision-makers

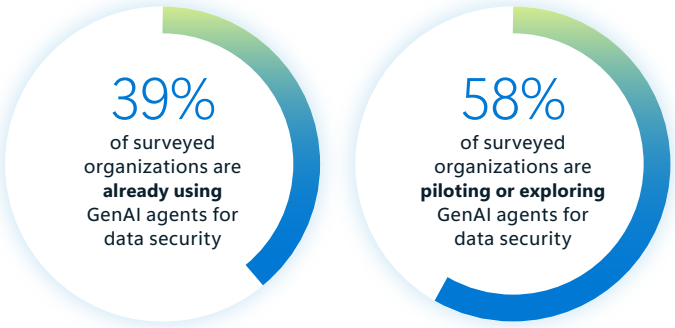
Automate routine security tasks to improve efficiency	38%
Improve our ability to adapt and learn from evolving risks	36%
Help our data security team spend more time on strategic work	35%
Analyze more data than would be possible with other solutions	35%

Confidence in GenAI-driven security is rising fast. Ninety-two percent of surveyed decision-makers say they feel confident using GenAI to strengthen data security – an increase from 86% in 2024.



GenAI agents are seen as a key opportunity for data security programs but must include human oversight

The momentum around GenAI in data security programs extends to the rise of GenAI agents, intelligent systems capable of detecting critical risks, automatically classifying or protecting data, and recommending controls in real time. 39% of surveyed organizations say they're already using GenAI agents for data security, while another 58% report they are piloting or exploring them.



> "We have Agentic AI embedded in some of our security tooling today. Our phishing awareness and tester training solution uses Agentic AI to look at emerging real-time threats, as well as user behaviors."
>
> Global Information Security Director
> Hospitality & Travel

Top Agentic AI data security use cases

Among surveyed data security decision-makers

Detect critical risks	**40%**
Automatically protect, block, flag, and classify data	**36%**
Investigate potential data security incidents	**35%**
Make recommendations to better secure data environments	**35%**
Reduce false positive alerts	**35%**

Still, even as organizations embrace these capabilities, leaders emphasize the importance of keeping humans in the loop. 38% of surveyed decision-makers are concerned about employees using GenAI agents without proper approval or human oversight.

A Director of Global Cybersecurity in Manufacturing explains, "We have GenAI agents for different purposes, but there's still a human in the loop directing the activities and reviewing data that is output."

Automation and GenAI agents are already reshaping data security—not by replacing human judgment, but by amplifying it. They extend the reach of security teams to empower them to respond faster and adapt to evolving risks. But as these capabilities scale, strong guardrails are essential to ensure speed doesn't compromise security or trust.

The Path Forward

Organizations are embedding GenAI into the foundation of their data security programs. The next phase of maturity lies in using GenAI to automate and enhance protection and accelerate investigations – helping teams scale securely and stay ahead of evolving risks.

01

Integrate GenAI into the data security workflow.

Embedding GenAI into detection, investigation, and policy workflows enhances visibility, prioritization, and response speed. GenAI can prioritize alerts, correlate events, and surface insights that help teams focus on the most critical threats.

02

Use GenAI agents to accelerate response and reduce noise.

GenAI agents offer scalable automation for data discovery, protection, and remediation. When deployed thoughtfully, they can help reduce manual effort and improve consistency without compromising control.

03

Maintain human oversight to stay in control.

Human expertise remains essential for guiding, validating, and improving GenAI-driven outcomes. Clear governance frameworks and human review processes are critical to ensuring accuracy, fairness, and trust in GenAI-enabled data security operations.

Final Recommendations

Integration for Greater Visibility: Integrated platforms as the key to stronger protection

As data volumes continue to expand, visibility remains one of the greatest challenges in protecting sensitive information. Organizations can no longer afford to manage dozens of disconnected tools that introduce blind spots and increase operational drag. Moving toward an integrated platform, supported by DSPM, provides the unified visibility and control needed to reduce complexity and strengthen protection. A consolidated, cohesive approach helps organizations not only streamline management but also helps improve detection and response – turning visibility into resilience.

Stay Productive, Stay Protected: Mastering the GenAI security balance

As GenAI becomes a fixture of everyday work, the challenge for organizations is not whether to use it, but how to use it securely. The rise in unauthorized or unmanaged GenAI usage highlights the need for greater oversight and governance. Implementing controls that prevent sensitive data from entering GenAI tools, identifying GenAI usage across environments, and training employees on secure practices are critical steps to mitigating risk. By putting the right controls in place, GenAI can continue to drive innovation without compromising data security or compliance.

Smarter, Faster, Safer: Reinventing data security with GenAI

GenAI is rapidly transforming how organizations detect, respond to, and prevent data risks. Integrating GenAI into security workflows allows teams to automate routine tasks, analyze complex data faster, and help perform more advanced investigations. As organizations adopt GenAI agents and automation to scale their data security programs, human oversight remains essential. The strongest data security strategies will combine GenAI's analytical power with human judgment to move faster, cut through noise, and reduce exposure risks.

Research Objectives

Understand the data security landscape, including priorities and mindsets, challenges, and the cause and effect of data security incidents.

Explore the future of data security, including what strategies and innovations are emerging and how organizations intend to invest in the future.

Uncover how employee use of GenAI is impacting data security and how teams are using GenAI in their data security program.

Methodology

A 25-minute multi-national online survey was conducted from July 16–August 11, 2025 among 1,725 data security leaders.

Questions centered around the data security landscape, data security incidents, securing employee use of GenAI, and the use of GenAI in data security programs to highlight comparisons to 2024.

One-hour in-depth interviews were conducted with 10 data security leaders in the US and UK to garner stories about how they are approaching data security in their organizations.

Audience Recruit

To meet the screening criteria, data security leaders 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 1,725 data security leaders surveyed for the research, completes by country were:

- US: 300
- UK: 300
- India: 300
- France: 150
- Germany: 150
- Brazil: 150
- Australia: 150
- UAE: 75
- Korea: 75
- Singapore: 75

Appendix

Unifying Data Protection and AI Innovation by Region

Across the globe there are unique differences in confidence, readiness, and expectations around GenAI and data security

US

Need support amid growing pressure

+9%
Outsized pressure to prove ROI of data security

+15%
Anticipate more data security incidents due to employee use of GenAI

+6%
More challenged with inaccurate/incomplete data classification

+5%
More challenged in managing DSPM due to too many disconnected tools

LATAM

Embracing growth with controls

+7%
More likely to anticipate an increase in data security budgets

+14%
More likely to have a fully implemented DSPM strategy

+7%
More controls around employee use of GenAI

EMEA

Less mature in governing GenAI data risks and leveraging Agentic AI

-5%
Less concerned about inability to protect data that goes into GenAI apps/tools

-4%
Less likely to have controls around identifying risky users of GenAI apps/tools

-4%
Less use of GenAI agents for data security

APAC

Grappling with high incident rates

+45
More data security incidents in past 12 months

+4 days
More time to detect and respond

+5%
More demand for data security staff to effectively manage responsibilities

+5%
GenAI apps more often compromised in data security incidents

Gaps shown represent regional vs. global data