Microsoft Security

Top 3 Challenges in Securing and Governing Data for the Era of AI

And how to solve them

Foreword

The rapid advancement of artificial intelligence (AI) is transforming how organizations interact with and manage data, presenting both new opportunities and risks, such as data leakage and oversharing. As organizations navigate this shift, many are recognizing that traditional, fragmented approaches to secure and govern data are not sufficient. Organizations are asking for a way to gain comprehensive understanding of data related risks across their data estate.

Heightened risk in the era of AI is also causing new regulations to emerge and become more stringent, making compliance and privacy not just a priority but a necessity. This is expanding and putting pressure on the responsibilities of security and compliance teams. Meeting these expectations can be complex, particularly when tools, processes, and teams remain siloed.

While evolving data risks can seem daunting, they also present an opportunity: with the right approach, organizations can both strengthen their information governance and create an environment where innovation and compliance work hand in hand.

This paper serves as a resource for understanding the challenges to secure and govern your data in the era of AI—with a solution that fosters resilience, drives efficiency, and paves the way for a more secure future.

Herain Oberoi
GM, Data & AI Security
Microsoft

Methodology overview

To bring to light the challenges and opportunities in securing and governing data, Microsoft partnered with Hypothesis Group, an independent research and strategy agency, to develop this paper, utilizing insights across multiple research initiatives including:

- **Microsoft Secure and Govern AI Whitepaper July 2024**
  A multi-national online survey among over 400 enterprise business IT and data security decision-makers, conducted by MDC Research Group

- **Microsoft Data Security Index Report November 2024**
  A multi-national online survey among 1,376 data security decision-makers, conducted by Hypothesis Group

- **Microsoft Audience Research September 2024**
  4 focus groups + a multi-national online survey among 600 security decision-makers, conducted by MDC Research Group

- **Microsoft Customer Requirements Research December 2024**
  A US/UK-based survey among 400 data security, governance, compliance and privacy tool users, conducted by Hypothesis Group

- **Additional internal and external sources**
  Includes Forbes, Statista, Precisely, Cybersecurity Ventures, Dataversity, and more (Full source list at the end)

Key findings

01

As risks increase in the era of AI, organizations are unprepared to protect their data.

Organizations are utilizing fragmented platforms across security, compliance, and data teams which further exacerbates security outcomes.

02

The regulatory landscape is rapidly evolving due to AI, and organizations are struggling to efficiently comply.

To stay secure and compliant, the responsibilities of security leaders are expanding to include oversight of governance and regulatory requirements.

03

Organizations are indicating a unified platform approach with full visibility of data is crucial to fuel innovation and mitigate risks.

1

As risks increase in the era of AI, organizations are unprepared to protect their data.

Organizations are utilizing fragmented platforms across security, compliance, and data teams which further exacerbates security outcomes.

The AI transformation is happening now, and data risks are rapidly increasing, leaving organizations unprepared

Today, 95% of organizations are either implementing or developing an AI strategy,[1] which is increasing concern for leaders about data risks associated with growing AI use. This AI usage is in part causing enterprise data volume, which stands at an average of 2 petabytes, to grow over 40% year over year.[2]

Because of this, data incidents attributable to AI are on the rise[3] and organizations are struggling to meet this demand, with insufficient permissions, controls, and data hygiene in place to tackle the increase.

Leaders say they are hesitant to fully embrace AI until they adopt a stronger data security posture and data governance structure. Today, 62% admit they don't have a strong data governance structure[5] and only 25% have a global data quality program.[6]

> **"The location where data is stored, and who will access it has complicated the security and management of our AI tools and vendors. We have more than 100 years' worth of data we must protect and govern."**
>
> Information Governance Senior Manager, Manufacturing

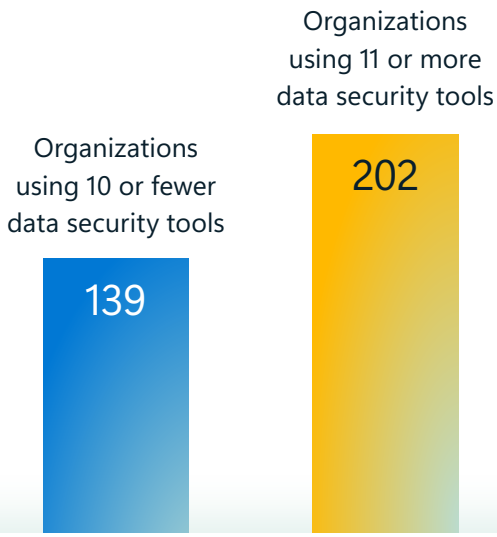
Furthermore, 80% of risk leaders cite leakage of sensitive data as a top AI concern[7] and understand that data generated by AI cannot be trusted without data quality measures in place. Improvements to both data security and governance are critical to help leaders feel more confident with AI adoption, balancing AI innovation with security.

In recognizing that they are unprepared, 53% of security, risk, and data leaders are increasing budgets to address regulatory requirements with AI.[8] With more budget, organizations are making investments to meet growing demand to reduce data risks and ultimately work towards their top priority in securing and governing their data effectively.

Organizations today are using disparate platforms, which is exacerbating AI innovation risks due to limited visibility into the data and associated risks

Today, organizations rely on 11 or more data security tools, and when expanded across governance and compliance platforms, this number increases even further, leading to more fragmentation and disintegration. Specifically, organizations lack visibility into the data and risks across the full data estate. This increases exposure to risks and can lead to more work and higher costs—often, the more tools an organization uses, the more incidents they experience.[3]

Total of data security incidents[3]



This fragmented approach makes it challenging for security, compliance, and data leaders to understand their data posture and mitigate their exposure to potential data risks. In fact, the majority of users are dissatisfied with their disparate platforms and three-quarters are uncomfortable with their experience.[9]

Potential data risk is even further exacerbated as organizations often have siloed teams, disparate workflows, and legacy tools that have not been modernized.

An SVP of IT in Insurance explains the challenge his organization is facing: "Incident management, data sharing, and audit trails rely on multiple standalone platforms **without an end-to-end workflow**," exemplifying the struggle of not knowing how data is being used, who is using it, and where it is going.

With many fragmented platforms, organizations struggle to have an integrated data security and governance posture for their data estate

To try and work securely and productively, teams continue procuring more and more tools, but this ultimately leads to greater inefficiency. The traditional fragmented approach does not have the needed integration to work properly across teams.

This approach falls short of meeting needs because it creates duplicated data, inconsistent data classification, redundant alerts, and siloed investigations. All of this leads to increased data risks, higher costs, ineffective governance, and regulatory non-compliance.

In addition, a third say that managing data across multiple data platforms is a top barrier to collaboration across data security, governance, compliance, and privacy.[9] A VP of Data Security in Healthcare states, "One of the biggest issues is the **lack of interoperability between the platforms used by different teams**, which creates silos and makes it harder to share insights or track data workflows seamlessly."

> **"We have dozens of different systems that don't necessarily communicate with each other. This poses potential gaps for privacy compliance, so having products that make it easier to see the big picture would be a huge improvement."**
>
> Data Protection Officer

A fragmented tooling approach can result in...

Increased data risks

Higher costs

Ineffective governance

Regulatory non-compliance

2

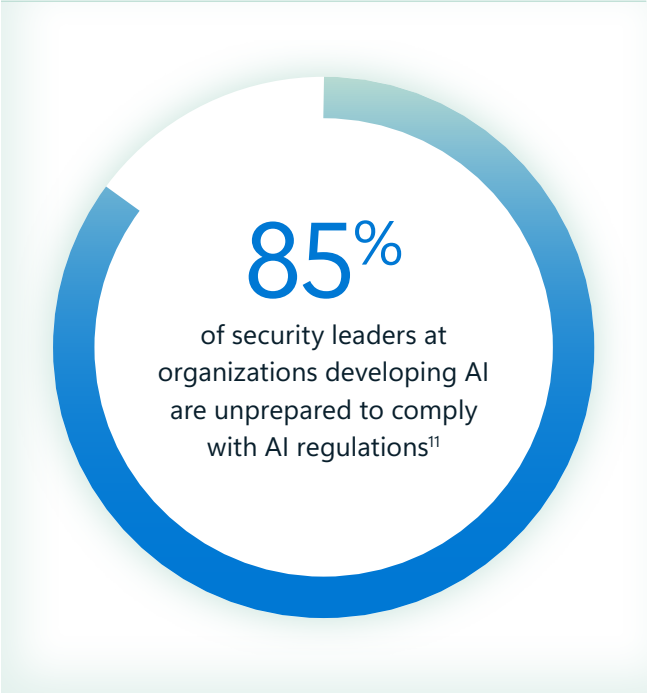
The regulatory landscape is rapidly evolving due to AI, and organizations are struggling to efficiently comply.

To stay secure and compliant, the responsibilities of security leaders are expanding to include oversight of governance and regulatory requirements.

Organizations today are using disparate platforms, which exacerbates AI innovation risks due to limited visibility into data and associated risks

New regulatory requirements are on the rise due to AI. Currently, organizations are facing over 200 daily updates across over 900 regulatory agencies.[10]

With all these new regulations comes fines and the fear of not being able to comply. Leaders acknowledge that compliance is difficult to stay ahead of and they need help figuring out how to make it happen.



A Head of Compliance in Corporate Banking explains his need for unified oversight: "We need an oversight function. When we use different applications at the same time there's different data leaks, so there's not one application or one team or one person who has perfect oversight. This function should have audit trail reporting in case something goes wrong, since it takes a lot of time to investigate what went wrong and which data was leaked from where."

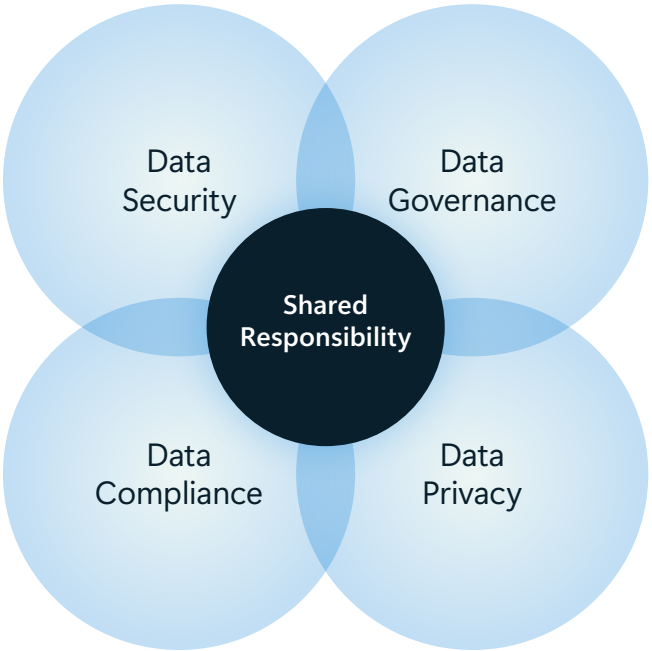
> **"Compliance is binary. You are compliant or you're not. We've got to be compliant in all cases a hundred percent of the time to be auditable. That's where the challenge is since there are a lot of players in our organization involved to keep us compliant."**
>
> Chief Digital & Technology Officer, Hospitality

Organizations are rethinking team responsibilities to remain compliant and secure with their AI innovation

Currently, AI strategy resides across various teams under the CEO and CIO and the associated security and compliance risks gets passed onto the CISO.

To meet the implications of widespread AI adoption, the responsibilities of security leaders are expanding to keep compliance and governance top of mind. This enables leaders to better prepare and protect data across all types of generative AI apps, with governance on AI tools used and data fed into AI systems.

A security leader states, "With AI we will have to find ways in which all offices are responsible for data as a team."



Currently, 87% of data security, governance, compliance, and privacy leaders have responsibilities across multiple areas,[9] showing how these roles are intersecting—a data security leader now needs to care about privacy, compliance and governance, in the same ways those in complementary roles care about all areas of an organization's data.

The increased responsibility for security teams to safeguard AI innovation and comply is creating a need for new roles.

> **"We're specifically adding roles around AI data governance within the security team."**
>
> CTO, Financial Services

3

Organizations are indicating a unified platform approach with full visibility of data is crucial to fuel innovation and mitigate risks.

Leaders want to unify their data security and governance platforms and embrace a unified approach so that data responsibility is shared across the organization

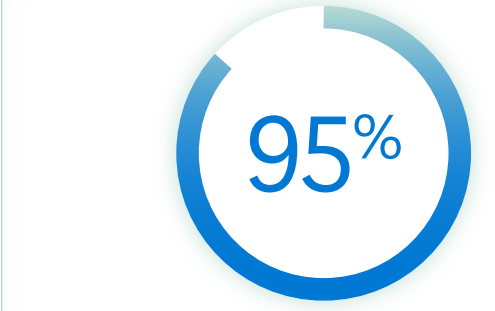
Leaders responsible for securing and governing data are struggling with making data protection a true team sport and need a tool that will allow them to have shared oversight into their data.

In order for security teams to continue innovating, meet privacy and compliance requirements, and protect against risk, organizations want greater tool unification and integration. The majority of organizations believe that a comprehensive approach with integrated solutions is superior to using multiple best-of-breed solutions.[3]

Teams continue to recognize that addressing AI risk and regulatory requirements will demand greater alignment across the organization, which is enabled by unified platforms. **Roughly half of security leaders identify with these top priorities:**[8]

- New tools to adhere to requirements
- Tool consolidation
- Expanded responsibility areas of existing positions

> **"Integration allows us to take a holistic approach to risk management by addressing security, governance, and compliance aspects simultaneously."**
>
> CISO, Healthcare

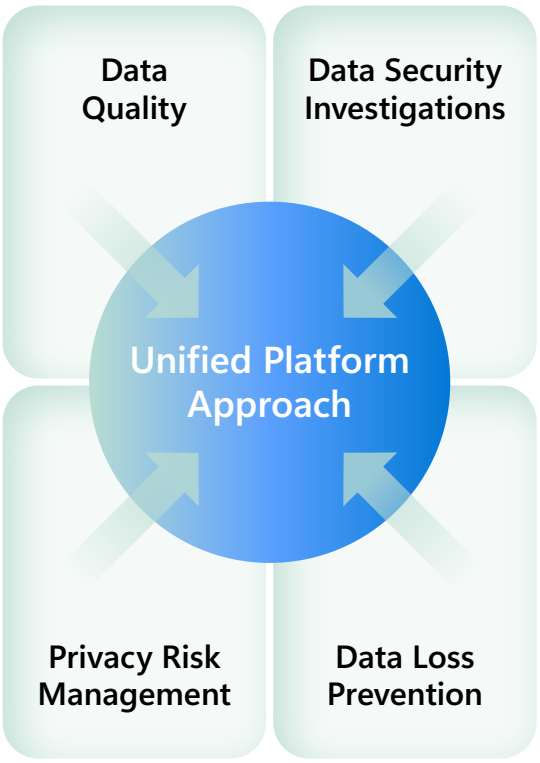


of leaders agree that unifying teams and tools across data security, governance, compliance, and privacy is a priority[8]

Leaders are specifically asking for a unified solution with centralized visibility to identify gaps and risks for region-specific regulatory requirements, all while recommending actions directly in tooling experiences to remain compliant.[9]

They want integrated insights across governance and privacy in addition to data security. To ensure security, teams would only have access to data they need to be exposed to in a unified experience.

The majority seek a solution to increase security and visibility by having the following work together



When asked about the top scenario where unified platforms maximize value, leaders cite a need for data security teams to gain visibility into user risk profiles for all data accessed in a data catalog, which allows for more complete risk profiles across business applications and data catalog tools.[9]

A unified platform approach enables a model where each business unit owns and manages its data, while security and governance teams have centralized oversight and policy adherence of the full data estate. This ensures clean trusted data is used to unlock business innovation. It is no longer enough to keep your data secure; organizations must activate quality data across multiple data sources.

Organizations are ready to adopt a unified platform approach to maximize impact

Organizations might worry about the cost and time needed for a unified platform approach, but security leaders agree that this approach will save time, enhance data security posture, reduce risk exposure, and improve visibility for leadership.[9] These benefits decrease end costs with fewer incidents and greater efficiency.

Contrary to fears, data does not indicate that a unified platform approach will take away jobs. In 2025, there are 3.5 million cybersecurity jobs open globally, representing a 350% increase over the past 8 years.[13] Instead of eliminating jobs, a unified platform is expected to help teams better execute their responsibilities.

Teams with limited time and resources can also bridge gaps in knowledge and skills with AI copilots embedded into unified platform experiences. This reduces the time needed to retrain users on new tooling.

Teams express a need for capabilities that live in a unified platform and offer visibility across their full data estate, but are they ready to adopt? The answer is overwhelmingly yes—over 90% of data security, governance, compliance, and privacy leaders say their organization will adopt a unified solution.[9]

We hope the insights and recommendations in this report help you secure and govern your data in the era of AI.

To learn more about how you can continue to protect your data, visit: **https://aka.ms/secureandgoverndata**

Sources

1. Microsoft, Secure and Govern AI Whitepaper, 2024
2. Statista, Volume of enterprise data worldwide 2020-2022, by location, 2022
3. Microsoft, Data Security Index Report, 2024
4. Forbes, Only 9% Of Surveyed Companies Are Ready To Manage Risks Posed By AI, 2023
5. Precisely, 2025 Outlook: Data Integrity Trends and Insights Report, 2025
6. Data Leaders Guild, Voice of the Chief Data Officer, 2024
7. Information Security Media Group, First Annual Generative AI Study: Business Rewards vs. Security Risks, 2023
8. Microsoft, Audience Research, 2024
9. Microsoft, Customer Requirements Research, 2024
10. Forbes, Cost of Compliance, Thomson Reuters, 2021
11. SAP LeanIX, AI Survey Results, 2024
12. Dataversity, Data Governance Trends in 2024, 2024
13. Cybersecurity Ventures, 2023 Official Cybersecurity Jobs Report, 2023

hypothesis Microsoft Security