The AI security balancing act: From risk to innovation

A CISO's guide to mastering the risk and potential of AI

With insights based on NTT DATA's 2025 Global GenAI Report

Soaring investment in AI is already transforming industries and affecting the way we work.

The increasing adoption of AI goes hand in hand with new and evolving cyberthreats.

CISOs acknowledge the need for a modern, integrated cybersecurity posture.

of CEOs are planning further GenAI investments.

of CEOs say GenAI is causing them to invest more in cybersecurity.

But how do CISOs help their organizations tap into the potential of AI while also protecting their digital assets from the risks?

We call this the AI security balancing act.

1. Is your cybersecurity strategy ready for the AI era?

While AI is transforming industries and empowering cybersecurity to combat both traditional and evolving AI-driven cyberattacks, it also exposes businesses to new security risks.

GenAI has the potential to transform businesses

95%

of C-suite leaders say that GenAI is driving a new level of innovation in their organizations.

Top 3

Organizations list improved security as one of the top three outcomes they have seen as a direct result of their GenAI deployments.

But progress comes with new security risks

88%

of organizations are highly concerned about the security risks associated with GenAI deployments.

Yet, only 24%

of CISOs strongly agree that their organization has a robust framework for balancing risk with value creation.

2. Understanding AI-related risks

The rapid integration of AI technologies expands attack surfaces and introduces sophisticated threats, making cybersecurity a critical business imperative.

Common types of AI attacks

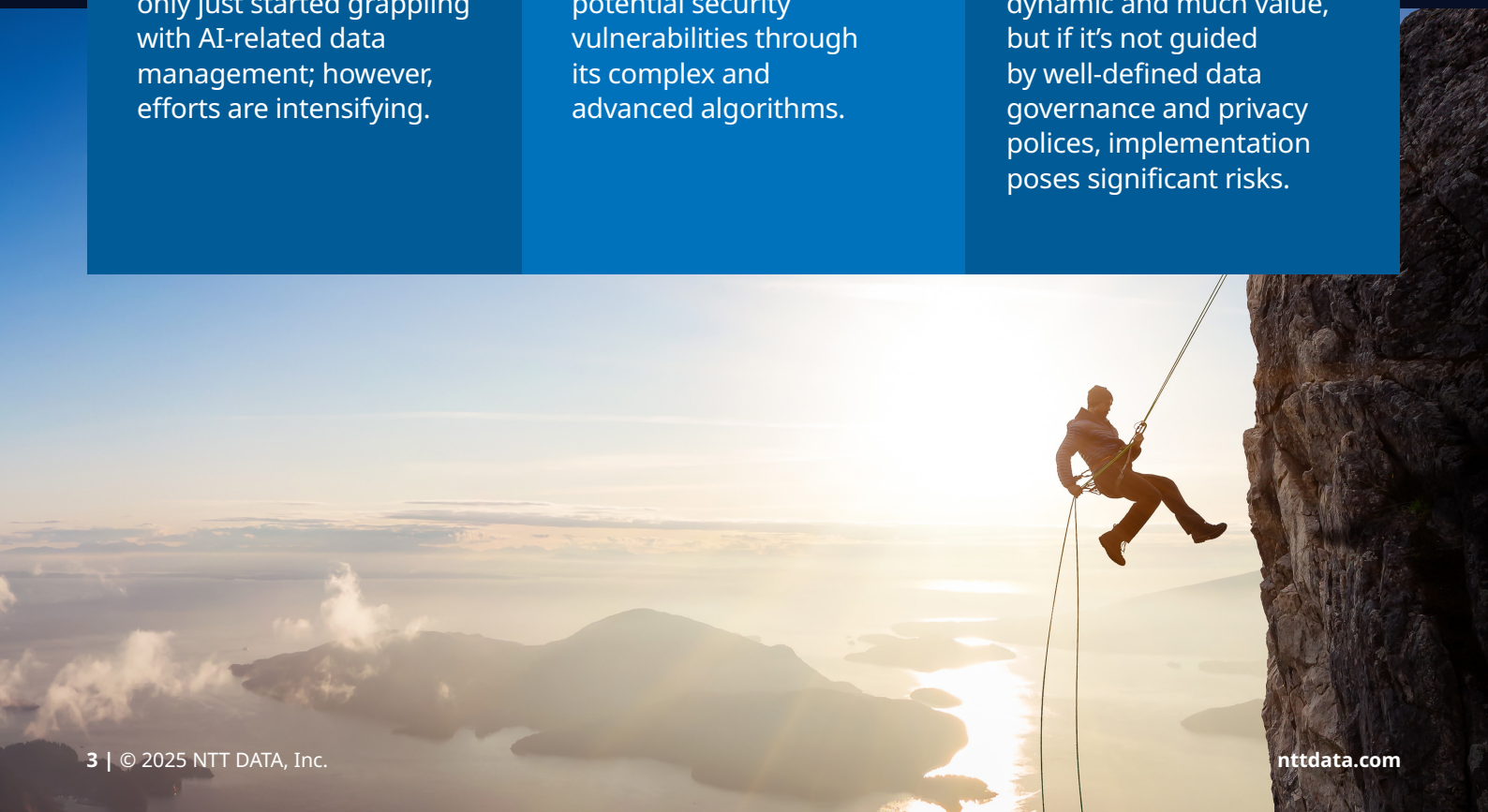
- Adversarial attacks
- Data poisoning
- Algorithmic bias

Data management, GenAI and agentic AI

Many organizations have only just started grappling with AI-related data management; however, efforts are intensifying.

GenAI also introduces potential security vulnerabilities through its complex and advanced algorithms.

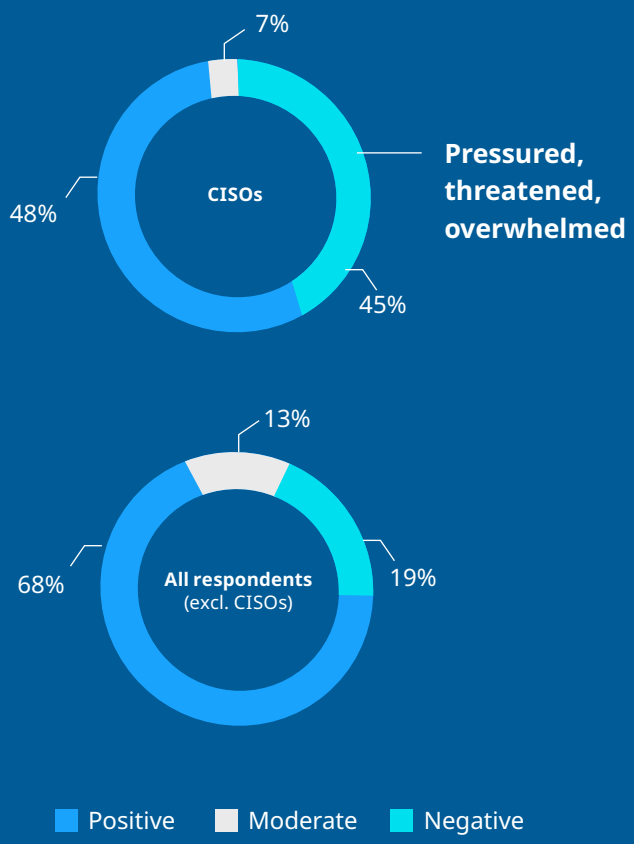
Agentic AI will add a new dynamic and much value, but if it's not guided by well-defined data governance and privacy polices, implementation poses significant risks.



3. AI and security: CISOs must balance opportunity and risk

There is a notable disconnect between the strategic goals of the C-suite and the operational hurdles that CISOs face when striving to responsibly maintain security, privacy and compliance in AI deployments.

Strongest sentiment about GenAI



54%

of CISOs say internal guidelines or policies on GenAI responsibility are unclear, yet only 20% of CEOs share the same concern.

Only 38%

of CISOs agree strongly that there is alignment between their organization's GenAI and cybersecurity strategies, while 51% of CEOs say the same.

Adding to the challenge...

The CISO challenge is compounded by aging, absent or unintegrated infrastructure

71%

of CISOs indicate their organization lacks clear direction from leaders on how to maintain responsibility.

87%

believe that legacy infrastructure is holding back their GenAI progress.

69%

admit that their teams lack the skills to work with this fast-evolving technology.

86%

say the cloud environment is the optimal infrastructure for efficiently and cost-effectively scaling GenAI.

Yet, despite feeling cautious about the deployments of GenAI, security leaders acknowledge its business value.

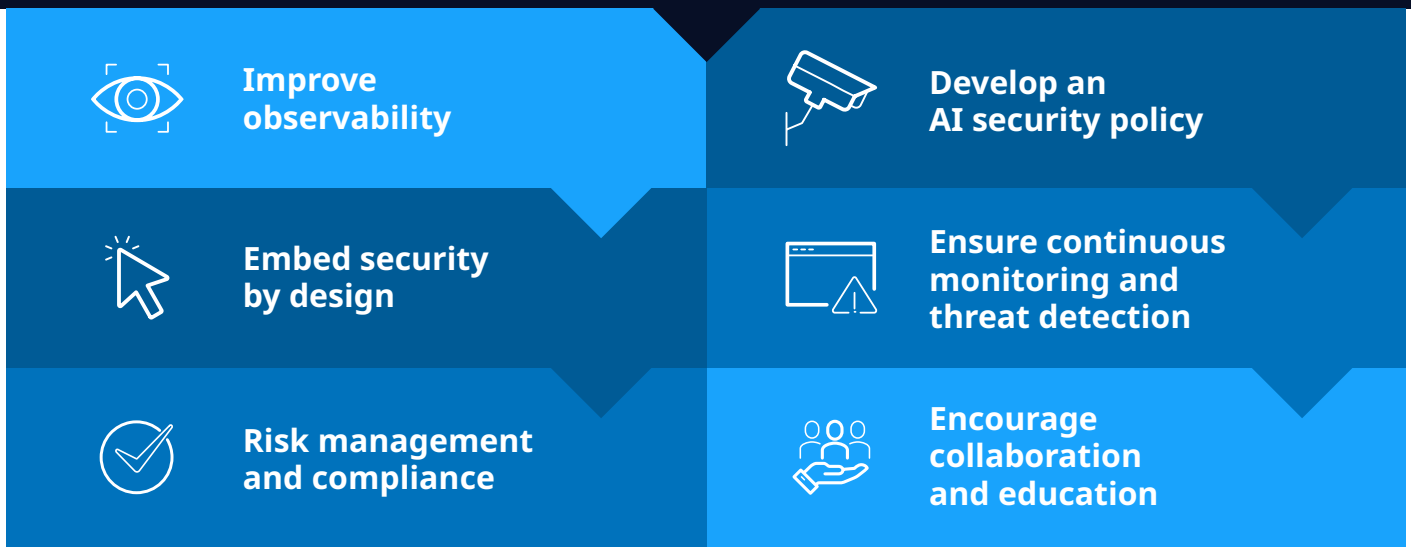
81%

of senior IT security leaders with negative sentiments about GenAI still agree that the technology will boost efficiency and improve the bottom line.

4. How CISOs can manage AI-related risks

Co-innovation and an end-to-end GenAI service offering are CISOs' top ranked factors for deployment and assessing GenAI partners.

Key areas for managing AI risks with a multilayered approach



An AI-led, platform-first approach to cybersecurity will strengthen your organization's defenses in an evolving threat landscape and turn cybersecurity into a strategic advantage that enables innovation and drives a competitive edge.

NTT DATA empowers organizations to innovate safely through AI-driven solutions, and secure business growth.

Contact an AI and security expert

Get the full report

Visit nttdata.com to learn more.

NTT DATA is a global innovator of digital business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.