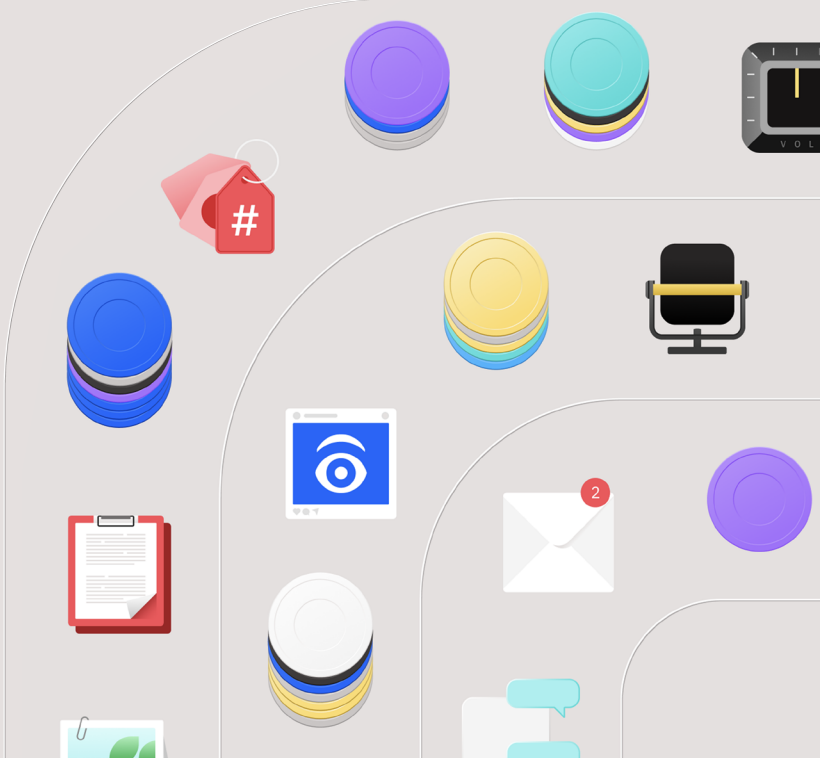
# Unify governance and security for data and AI



AI is evolving fast, and business leaders are leaning into it with bold experimentation and widespread adoption. But with this rapid AI proliferation comes a growing web of risks that originate from a lack of security and governance.

So, while AI does offer a range of benefits, without governance and security in place, even the most advanced AI systems can be in danger of breaches and attacks.

> 25% of enterprise breaches will be linked to misuse of AI agents by both insiders and outsiders by 2028, according to a Gartner prediction.[1]

To scale AI with confidence, you need strong governance and security—working together as a unified force.

## Governance + Security = AI done right

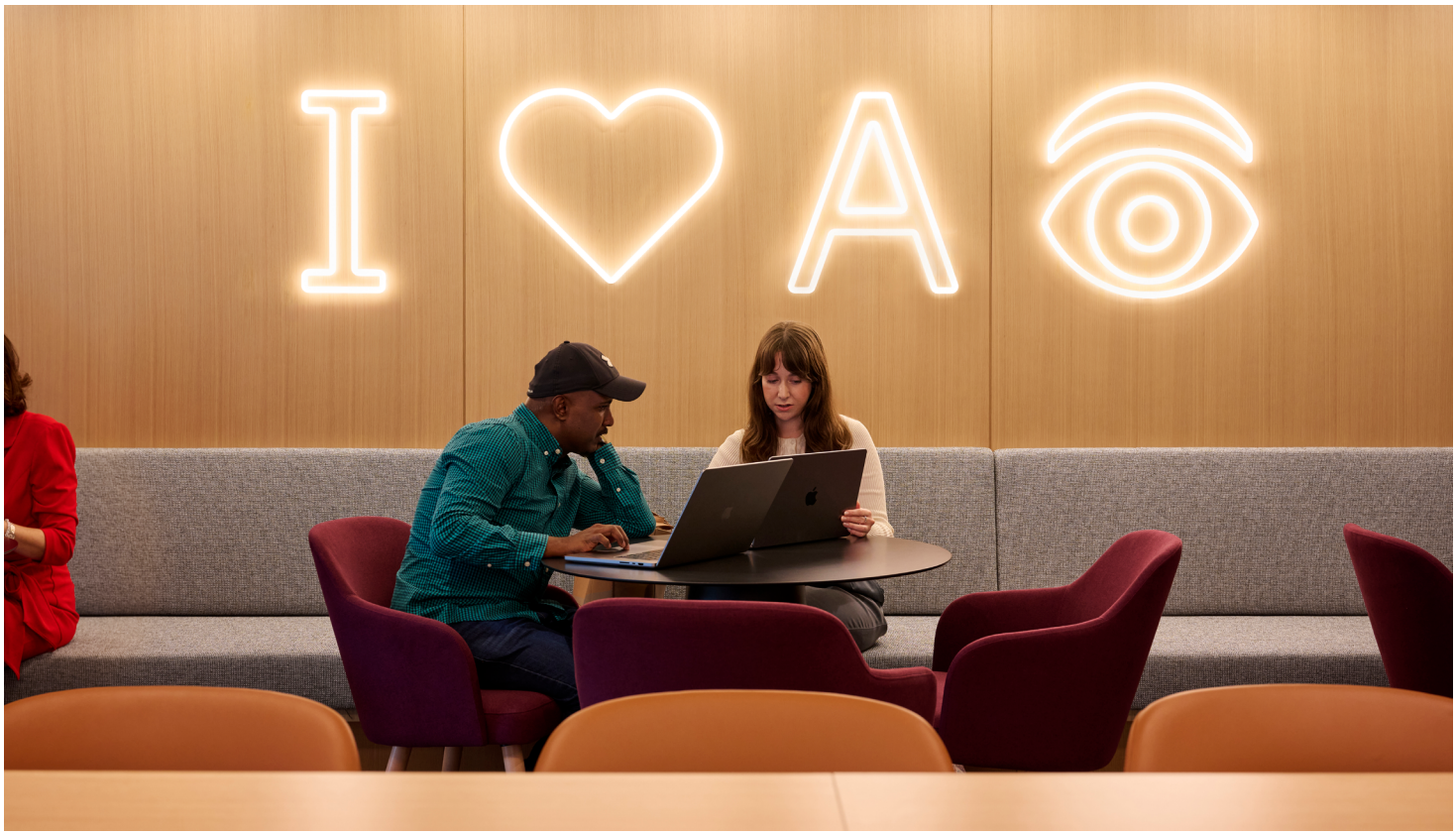
Traditionally, governance and security—policies, compliance measures, threat protection and data defense—have been siloed. This disconnect means many organizations lack a full view of the risks their entire AI tech stack faces.

Merging governance and security turns this fragmented sight into a cohesive view, helping ensure no aspect of AI risk goes undetected. The combination empowers organizations to embed trust and safety into their AI initiatives from day one and to address AI risks holistically.

In the current landscape, no single solution has been able to address both ethical compliance and security risks in AI.

Until now.

IBM




## A unified approach to governance and security

IBM's launch of an offering that unifies AI governance and security in one solution changes the game.

By using the IBM® watsonx.governance® toolkit and the IBM Guardium® AI Security solution in tandem, organizations can now gain unparalleled visibility and risk management for AI in one integrated approach.

Separately, each of these solutions helps protect data and mitigate risks.

- **IBM watsonx.governance** automates policy enforcement, model documentation and compliance workflows, giving risk teams a dynamic view of where AI is used and whether those deployments follow regulations. By baking governance into the AI lifecycle, it builds confidence from day one of an AI project, not just during audit.
- **IBM Guardium AI Security** is designed to proactively monitor, detect and mitigate AI-related risks as they emerge, and to guard sensitive data used and generated by AI to enhance confidentiality, integrity and availability. It also works in real time, so security teams aren't always playing catch-up.

Combined, they provide a single, unified approach to AI governance and security with features vital to protecting data and AI.

- **Unified AI inventory:** View AI model inventory with business and technical users.
- **Proactive risk and compliance management:** Prioritize and monitor alerts across model health, performance and security vulnerabilities.
- **AI usage protection:** Set security and organizational policies to safeguard usage through gateways and guardrails.
- **Integrated operations:** Operationalize across product, risk, compliance and security stakeholders.

Learn more about the only integrated governance and security solution purpose built for AI.

Explore IBM watsonx.governance →

Explore IBM Guardium AI Security →

1. Gartner Unveils Top Predictions for IT Organizations and Users in 2025 and Beyond, Gartner, 22 October 2024.