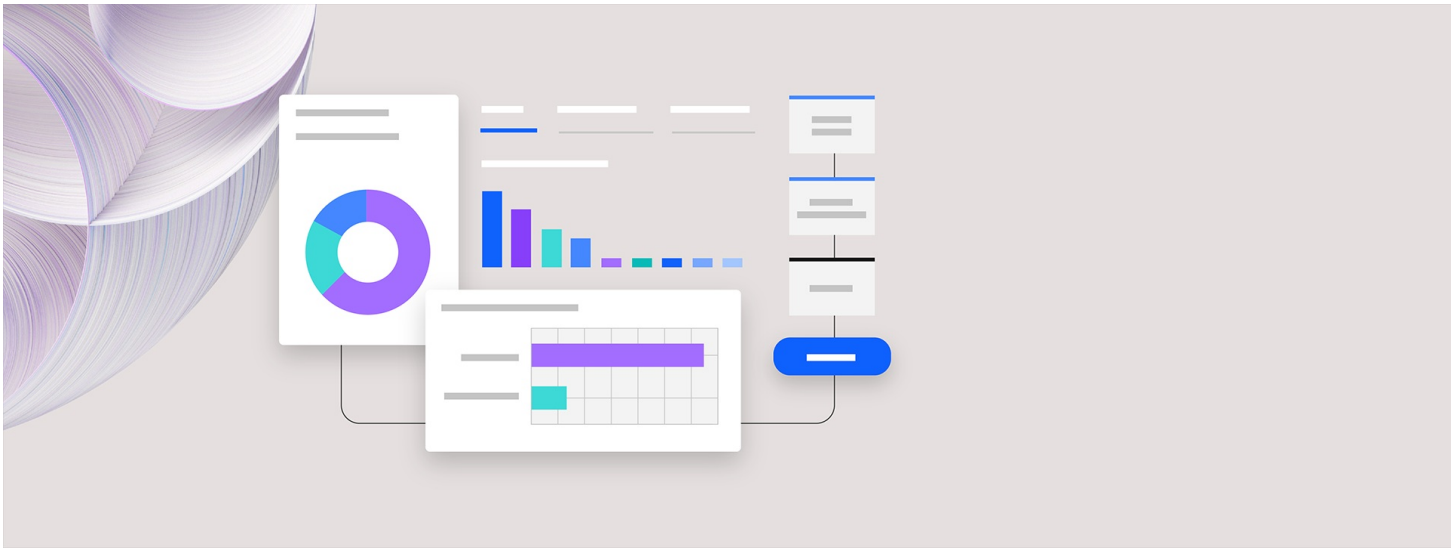
IBM Newsroom

IBM Introduces Industry-First Software to Unify Agentic Governance and Security

New IBM integrations to help businesses keep their agentic AI – and other generative AI systems –secured and responsible at scale

Enterprises can red team agents, audit agents, detect shadow agents, and more



ARMONK, N.Y., June 18, 2025 /PRNewswire/ -- Today, as enterprises scale AI agents across their organizations, IBM (NYSE: IBM) is announcing the industry's first software to bring AI security and AI governance teams together and provide a unified view of enterprises' risk posture.

The new capabilities enhance and integrate watsonx.governance and Guardium AI Security to help clients keep their AI systems, including agents, secured and responsible at scale. Watsonx.governance is IBM's end-to-end AI governance tool and Guardium AI Security is IBM's tool for securing AI models, data, and usage.

"AI agents are set to revolutionize enterprise productivity, but the very benefits of AI agents can also present a challenge," said **Ritika Gunnar, General Manager, Data and AI, IBM** "When these autonomous systems aren't properly governed or secured, they can carry steep consequences."

Today's new offerings include:

Integrating and Automating Agentic AI Security

IBM is enhancing the integration of IBM Guardium AI Security and watsonx.governance, providing enterprises with the first unified solution to manage security and governance risks associated with AI use cases. The integration supports users' processes to validate compliance standards against 12 different frameworks, including the EU AI Act and ISO 42001.

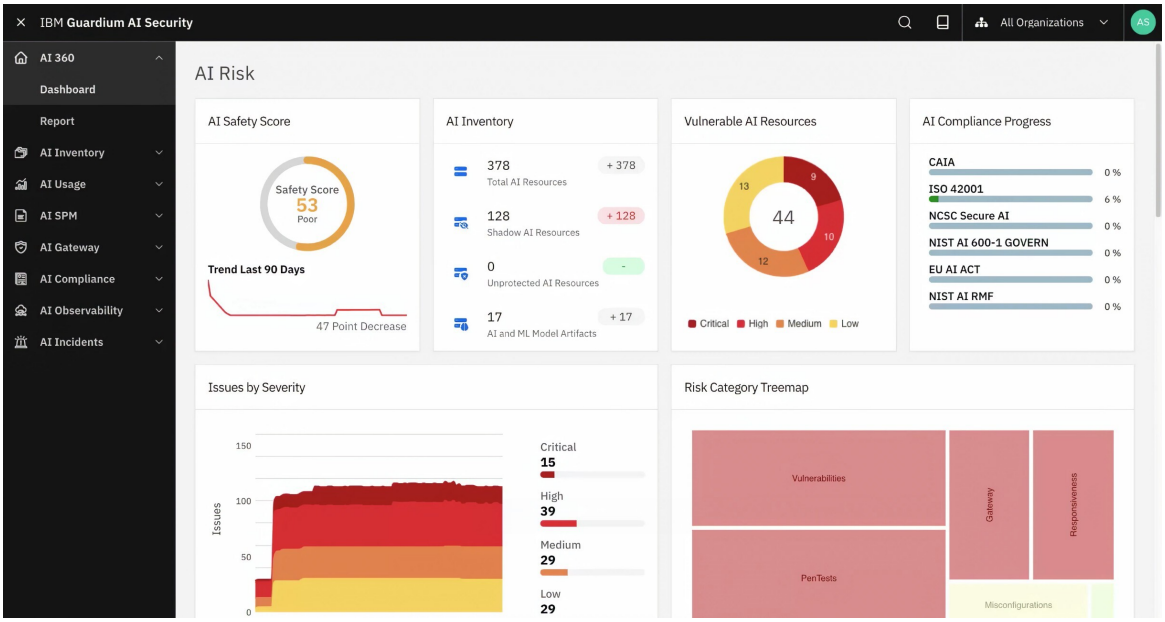
IBM is also introducing new capabilities to Guardium AI Security through a collaboration with AIlTrue.ai, including the ability to detect new AI use cases in cloud environments, code repositories, and embedded systems –providing broad visibility and protection in an increasingly decentralized AI ecosystem. Once identified, IBM Guardium AI Security can automatically trigger

appropriate governance workflows from watsonx.governance.

Recent updates to IBM Guardium AI Security also include automated red teaming to help enterprises detect and fix vulnerabilities and misconfigurations across AI use cases. And to help mitigate risks such as code injection, sensitive data exposure, and data leakage, the tool enables users to define custom security policies that analyze both input and output prompts. These features are available now in IBM Guardium AI Security, and their integration with watsonx.governance will roll out throughout the remainder of the year.

"The future of AI depends on how well we secure it today. Embedding security from the start is essential to protecting data, supporting compliance obligations, and building lasting trust," said **Suja Viswesan, Vice President, Security and Runtime Products, IBM**.

"One of the biggest challenges for security teams is translating incidents and compliance violations into quantifiable business risk. The rapid adoption of AI and agentic AI amplifies this issue," said **Jennifer Glenn, Research Director for the IDC Security and Trust Group**. "Unifying AI governance with AI security gives organizations the necessary context to find and prioritize risks, as well as the information to clearly communicate the consequences of not addressing them."



Enhanced Agentic AI Evaluation and Lifecycle Governance

IBM watsonx.governance can now monitor and manage AI agents across their entire lifecycle, from development to deployment. Evaluation nodes can be built directly into agents, allowing users to carefully monitor metrics like answer relevance, context relevance, and faithfulness – and help identify the root cause of poor performance. Planned future capabilities also include agent onboarding risk assessment, agent audit trails, and an agentic tool catalogue, which are expected to be available June 27.

Off-the-Shelf Compliance Capabilities

IBM watsonx.governance Compliance Accelerators provide select pre-loaded regulations, standards, and frameworks from around the globe, enabling users to identify relevant obligations and map them onto their own AI use cases. Content covers key regulations like the EU AI Act, the U.S. Federal Reserve's SR 11-7, and New York City Local Law 144, along with global

standards like ISO/IEC 42001 and frameworks like the NIST AI RMF. Watsonx.governance Compliance Accelerators is available now as an add-on.

Expertise to Scale AI Responsibly

To help clients scale AI responsibly, IBM Consulting Cybersecurity Services is introducing a new set of services that brings together data security platforms, like IBM Guardium AI Security, with deep AI technology and domain consulting. The new services will support organizations through their AI transformation journey: from discovering AI deployments and potential vulnerabilities, to implementing secure-by-design practices across AI layers, to governance guidance for a constantly evolving regulatory landscape. The new services build on IBM Consulting's experience helping hundreds of clients worldwide on AI strategy and governance, including Nationwide Building Society and e&.

To provide AWS clients with increased value and convenience, watsonx.governance is now also available on AWS data center in India with enhanced model monitoring capabilities.

Today's new capabilities and integrations give businesses the comprehensive governance and security they need to thrive in the agentic AI era. The innovations also dovetail with IBM's broader suite of IBM watsonx AI solutions, built to help companies accelerate the impact of generative AI, responsibly and securely.

About IBM
IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs, and gain a competitive edge in their industries. Thousands of governments and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently, and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity, and service. Visit www.ibm.com for more information.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Media contacts:

Michele Brancati
Communications, IBM Software
Mbrancati@ibm.com

Kevin Zawacki
Communications, IBM Software
kevin.zawacki@ibm.com

SOURCE IBM

Additional assets available online: 

https://stage.mediaroom.com/ibmnewsroom/2025-06-18-ibm-introduces-industry-first-software-to-unify-agentic-governance-and-security