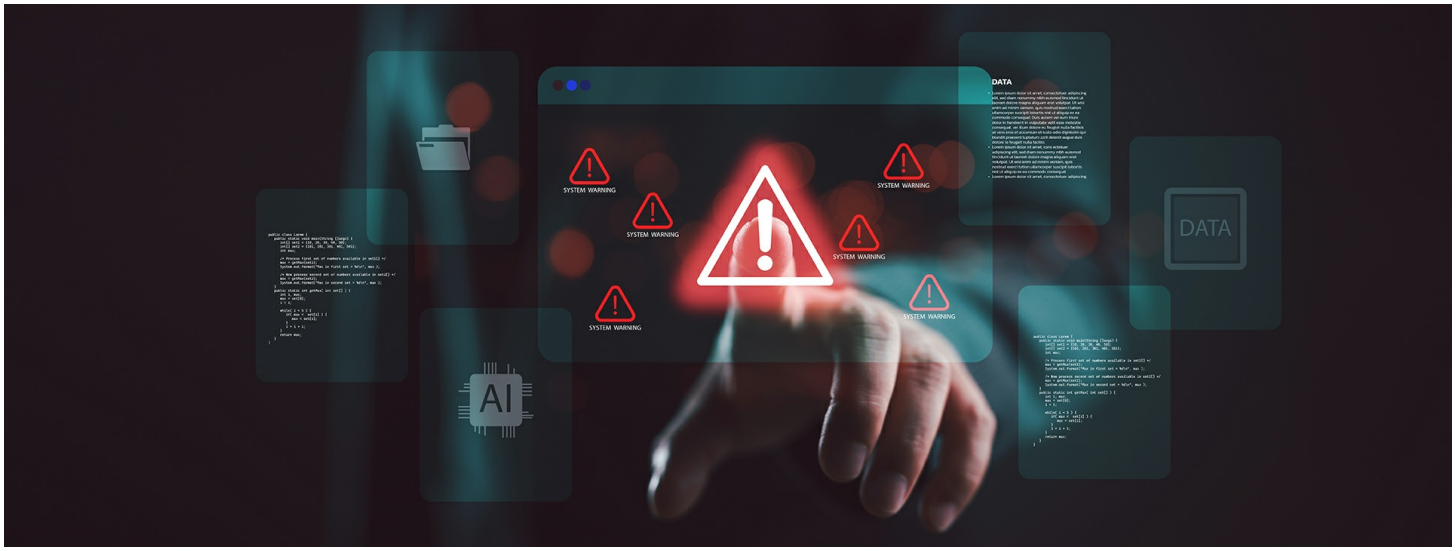
IBM Newsroom

IBM Announces New Cybersecurity Measures to Help Enterprises Confront Agentic Attacks

• New IBM cybersecurity assessment helps enterprises identify and measure new risks introduced by frontier AI models capable of vulnerability discovery and autonomous attacks

• IBM Autonomous Security, a new machine speed service composed of IBM AI agents, helps automate vulnerability remediation at a pace humans alone cannot sustain



ARMONK, N.Y., April 15, 2026 /PRNewswire/ -- IBM (NYSE:IBM) today announced new cybersecurity measures designed to help organizations counter a new generation of cyber threats as attackers begin weaponizing frontier AI models.

Attackers are already using frontier AI models to accelerate every phase of the attack lifecycle. These models represent a step change in offensive capability, which can dramatically lower the time, cost, and expertise required to carry out sophisticated attacks and push organizations toward continuous business disruption. As attacks move at machine speed, security programs built on fragmented tools and manual processes are increasingly outmatched. Defending against agentic adversaries will require security programs that are autonomous and coordinated at scale.

Enterprise Cybersecurity Assessments for Frontier Model Threats

Enterprises operate sprawling, complex IT estates that are hard to codify, creating ideal conditions for frontier models to identify weaknesses and rapidly turn them into attack paths. To address this challenge, IBM Consulting is offering a new cybersecurity assessment to help enterprises evaluate their readiness for agentic enabled threats. The assessment will be delivered by IBM together with its technology partners to help customers get the support they need across their environments.

The assessment provides deep visibility into security gaps, policy weaknesses, AI-specific exposures, and potential exploit paths. It also delivers prioritized mitigation guidance, including interim safeguards where no immediate software fix exists. In addition, the assessment highlights opportunities for enterprises to accelerate their detection and response through improved automation and architectural alignment.

IBM Introduces IBM Autonomous Security

Recognizing that enterprises must now match the speed and sophistication of AI-generated attacks, IBM today introduced IBM Autonomous Security—a multi-agent-powered service designed to deliver coordinated decision making, response and intelligence at machine speed.

IBM Autonomous Security brings together interoperable, vendor-agnostic digital workers that operate across an organization's full security stack, enabling security programs to act as a system rather than a collection of disconnected tools. The service is designed to fundamentally rearchitect how security programs operate as threats become increasingly autonomous and self-optimizing.

Using coordinated AI agents, the service analyzes software exposures and runtime environments to understand exploit paths, improve hygiene, enforce security policies across the applicable security tools, detect anomalies, and contain threats with minimal human intervention. Insights flow directly into governance and risk systems enabling up-to-date security and compliance posture – helping to reduce exposure windows and accelerate containment of high velocity attacks.

By extending security into identity, risk, and governance functions and connecting with AI systems across IT, OT, and business processes, IBM Autonomous Security helps organizations transform detection to remediation, strengthen compliance outcomes, reduce operational friction, and improve resiliency.

"Frontier models are creating a new category of enterprise threat that is fast moving, systemic and increasingly autonomous," **said Mark Hughes, Global Managing Partner of Cybersecurity Services, IBM Consulting** "Meeting that threat requires a systemic defense. AI powered offense demands AI powered defense. That's what IBM is delivering."

In an agentic threat environment, defensive advantage no longer comes from individual tools, but from how quickly and coherently security programs can act. IBM is committed to helping organizations prepare for this critical inflection point in cybersecurity where resilience must match machine speed.

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 the 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 effect 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.

Media Contacts:

Elizabeth Brophy
IBM
Elizabeth.Brophy@ibm.com

Michele Brancati
IBM
mbrancati@ibm.com

SOURCE IBM

---

https://stage.mediaroom.com/ibmnewsroom/2026-04-15-ibm-announces-new-cybersecurity-measures-to-help-enterprises-confront-agentic-attacks