Organizations Overlook AI Risk as Governance Fails to Keep Up

TrendAI™ research reveals pressure to deploy AI for business speed is outpacing control, visibility and accountability

DALLAS, March 25, 2026 /PRNewswire/ -- TrendAI™, the enterprise AI security leader fromTrend Micro Incorporated (TYO: 4704; TSE: 4704), has published new research revealing that organizations worldwide are pushing ahead with AI deployment despite known security and compliance risks.

To read the full report visit:https://www.trendmicro.com/explore/trendai-global-ai-study/

The new global study of 3,700 business and IT decision makers found that 67% have felt pressured to approve AI despite security concerns, with one in seven describing those concerns as "extreme" but overridden to keep pace with competitors and internal demand.

Rachel Jin, Chief Platform & Business Officer, Head of TrendAI:"Organizations are not lacking awareness of risk, they're lacking the conditions to manage it. When deployment is driven by competitive pressure rather than governance maturity, you create a situation where AI is embedded into critical systems without the controls needed to manage it safely. This research reenforces our focus on helping organizations drive solid business outcomes with AI while still managing business risk."

The risk of pressure-driven AI rollout is exacerbated by governance inconsistencies and unclear responsibility for AI risk that are becoming widespread. The same is true for security teams working on a reactive basis to top-down AI rollout decisions, which often leads to workarounds and increased use of unsanctioned or "shadow" AI tools.

Recent TrendAI™ threat research reinforces this shift, showing how attackers are already using AI to automate reconnaissance, accelerate phishing campaigns and lower the barrier to entry for cybercrime, increasing both the speed and scale of attacks.

AI adoption is outpacing control
Organizations are deploying AI faster than they can manage the associated risks, creating a widening gap between ambition and oversight. 57% say AI is advancing more quickly than they can secure it, while more than half (64%) report only moderate confidence in their understanding of the legal frameworks governing AI.

Governance maturity remains low. Only around a third (38%) of organizations have comprehensive AI policies in place, with many still drafting them, and 41% cite unclear regulation or compliance standards as a barrier. In practice, AI is being operationalized before the rules governing its use are fully established.

Trust in autonomous AI remains uncertain
Confidence in more advanced, autonomous systems is still in the maturing phase. Less than half (48%) believe agentic AI will significantly improve cyber defense in the short term, with ongoing concerns around data access, misuse and lack of oversight.

The data shows where those concerns are landing. More than four in ten organizations (44%) say AI agents accessing sensitive data is their biggest risk. Over a third (36%) warn malicious prompts could compromise security, while one in three (33%) point to a growing attack surface for cyber criminals. A similar proportion (33%) fear abuse of trusted AI status and risks linked to autonomous code deployment.

At the same time, nearly a third (31%) admit they lack observability or auditability over these systems, raising serious questions about how organizations can control or intervene once agents are deployed.

Around 40% of organizations support the introduction of AI "kill switch" mechanisms to shut down systems in the event of failure or misuse, while nearly half remain unsure. This lack of consensus highlights a deeper issue. Organizations are moving towards autonomous AI without agreement on how to retain control when it matters most.

"Agentic AI is moving organizations into a new risk category," added Rachel Jin. "Our research shows the concerns are already clear, from sensitive data exposure to loss of oversight. Without visibility and control, organizations are deploying systems they don't fully understand or govern, and that risk is only going to increase unless action is taken."

About TrendAI™
TrendAI™, a global leader in AI security, empowers enterprises to innovate fearlessly by securing AI, cloud, networks, endpoints, and data across the modern attack surface. At the core is TrendAI Vision One™, a unified cybersecurity platform that centralizes cyber risk exposure management and security operations to protect the entire AI lifecycle from infrastructure to models to users. The platform is fueled by world-class threat intelligence and insights that protect organizations from hundreds of millions of threats every day. With 6,000 TrendAI™ experts across 75 countries, TrendAI™ empowers security leaders to stay ahead of threats, driving proactive security outcomes across the entire attack surface. This includes critical environments like AWS, Google, Microsoft, and NVIDIA. AI Fearlessly.

SOURCE TrendAI

For further information: TrendAI Communications, 817-522-7911, media_relations@trendmicro.com

https://newsroom.trendmicro.com/2026-03-25-Organizations-Overlook-AI-Risk-as-Governance-Fails-to-Keep-Up,1