TrendAI™ Secures the OpenClaw-Driven AI Era

Introducing new security solution designed for the rapidly emerging era of agentic AI

DALLAS, March 24, 2026 /PRNewswire/ -- TrendAI™, the enterprise AI security leader, today introduced**TrendAI™ Agentic Governance Gateway**, a new security solution engineered to give organizations visibility and control over autonomous agent interactions to strengthen security where systems interact across data, tools, and environments with increasing autonomy.

To learn more about TrendAI™ and TrendAI™ Agentic Governance Gateway, visit:
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/from-anarchy-to-authority-closing-the-governance-gap-in-agentic-ai

Rachel Jin, CPBO and Head of TrendAI™:"Tools like OpenClaw show just how powerful and accessible this new model has become. Organizations need to deploy these systems to unlock the next wave of productivity, and many already are, often without centralized oversight. TrendAI™ Agentic Governance Gateway enables this by providing visibility, control, and confidence."

Traditional cybersecurity is built to protect endpoints, networks, and applications. In contrast, agentic AI systems operate across dynamic chains of interaction where agents, models, APIs, and data continuously exchange information and trigger actions.

Eva Chen, CEO of Trend Micro:"As AI systems become more autonomous, security must evolve from protection to governance. This is the next frontier of cybersecurity and the focus of TrendAI™."

TrendAI™ Agentic Governance Gateway is a new way to address the emerging security gap created by agentic AI systems, such as OpenClaw, where autonomous agents act across enterprise environments without clear security control points. This was demonstrated last week at NVIDIA GTC, where a fundamentally new attack surface was highlighted - one that traditional security models were not designed to control: Autonomous agentic frameworks, such as OpenClaw, accelerating enterprise adoption of AI systems capable of planning, executing, and coordinating actions across workflows at machine-speed. There has never been a more critical business-level need than understanding and governing how agentic systems behave, and what actions they are taking. The orchestration required to monitor this attack surface created complex, multi-step workflows across enterprise systems until now.

According to Forrester, "AI agents are proliferating across workflows, but security programs built for human-centric architectures fail in agentic environments. These agents operate with dynamic reasoning, ephemeral identities, and goal-driven autonomy, creating unpredictable attack paths. Risks to agentic architectures include intent hijacking and cascading hallucinations that extend beyond confidentiality to integrity and availability. Without guardrails, enterprises risk regulatory violations, financial loss, and disclosure events from agentic security issues." [1]

TrendAI™'s Agentic Governance Gateway allows enterprises to focus on the behavior, interactions, and outcomes of AI systems in real-world environments. TrendAI™ Agentic Governance Gateway is delivered through the TrendAI Vision One™ platform, building on TrendAI™'s existing strengths, including AI-driven analytics to detect anomalous behavior and emerging threats, and a unified approach that correlates context across endpoints, cloud, applications, and AI systems.

TrendAI™'s Agentic Governance Gateway enables enterprises to:

- Gain visibility into how agents interact across systems
- Understand the context and intent behind agent communications to identify risky or unintended actions
- Enforce policy and control over agent-driven actions
- Introduce human oversight at critical decision points
- Simulate governance decisions before deployment — previewing the full policy impact without executing it
- Stage, preview, and roll back governance changes through a managed lifecycle

With these new advanced capabilities, TrendAI™ is enabling organizations to secure the critical interaction layer - the dynamic communication fabric where autonomous systems coordinate, make decisions, and drive enterprise actions. By establishing robust oversight and control at this pivotal layer, TrendAI™ ensures that agentic interactions are visible, governed, and trusted, effectively closing the security gap in agent-driven AI environments.

TrendAI™ is the enterprise business unit of Trend Micro Incorporated (TYO: 4704; TSE: 4704).

1: The AEGIS Agent-On-A-Page Template For Agentic Security, Forrester Research, Inc., Feb 13, 2026.

About TrendAI™

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

---