

TrendAI™ Ranks First on CyberGym Agentic AI Security Benchmark

The 97% success rate places TrendAI™ ahead of all other entrants on the AI security benchmark

DALLAS, Aug. 26, 2026 /PRNewswire/ -- The TrendAI™ agentic exploit-remediation engine, codename AESIR, achieved the top position on CyberGym, an independent evaluation benchmark for AI-driven security tooling.

The 97% success rate from TrendAI™ surpassed all other entrants currently on the leaderboard and is nearly 4 percentage points higher than the former leader, who posted a 93.2% score on Aug. 8, 2026.

CyberGym, a University of California, Berkeley benchmark, evaluates AI security tooling against 1,507 confirmed vulnerabilities drawn from 188 large open-source software projects that run in every enterprise.

Rachel Jin, Chief Platform and Business Officer, Head of TrendAI™: "CyberGym's validation changes what's possible for enterprises adopting AI. The race isn't to find first. It's to close the exposure window. Cybersecurity has been defined by the scramble from discovery to exploitation; our job is to make that gap meaningless by compressing exposure time towards zero. Our advantage is turning validated vulnerability intelligence into effective risk reduction faster."

TrendAI™ leverages seven AI models across four providers (Anthropic, DeepSeek, Google, and OpenAI) to maximize detection and remediation accuracy, and it powers a system built around one objective: close the exposure window faster than attackers can exploit it. It begins with discovery, powered by AI-scale identification of weak spots that static approaches miss. Each finding is then validated and turned into a working proof of concept, so teams understand exploitability and true business risk before the noise drowns out the signal. Only then does TrendAI rapidly reduce the risk, translating validated vulnerability intelligence into detection and virtual patches without waiting for the normal patching cycle.

That last step is what makes our approach and usage of agentic security different. This capability is built on more than 20 years of vulnerability research and exploit intelligence from TrendAI™ ZDI, giving the system a deep foundation of real-world knowledge about how vulnerabilities are discovered, validated and exploited. AI is compressing the time from discovery to exploitation, so risk reduction must move faster than the patch cycle, not wait on it. By converting validated intelligence into virtual patching, TrendAI™ shrinks the exposure window from weeks to as close to zero as possible, turning vulnerability management from reactive patching into proactive defense.

The TrendAI™ agentic exploit-remediation engine also powers dynamic discovery of threat actors actively exploiting vulnerabilities in the wild, giving security teams visibility into live exploitation in real time. Our real-world threat-intelligence layer supports the same goal: reduce exposure before attackers can exploit it.

TrendAI™ has published a technical blog post on the CyberGym methodology. For more information, please visit: <https://www.trendaisecurity.com/en-us/resources-insights/trendai-security-blog/trendai-first-on-cybergym-top-exploit-benchmark>

About TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities, to infrastructure, to data. Global Fortune 500 companies rely on TrendAI™ to cut risk and stop threats up to three months earlier, powered by world-leading threat and attack intelligence. AI Fearlessly.

SOURCE TrendAI

For further information: Media Contact: TrendAI™, media_relations@trendmicro.com

<https://newsroom.trendmicro.com/2026-08-26-TrendAI-TM-Ranks-First-on-CyberGym-Agentic-AI-Security-Benchmark>