Netskope Announces AI Guardrails Solution Powered by Google Cloud TPUs to Help Secure High-Performance AI Workflows at Scale

April 22, 2026

SANTA CLARA, Calif., April 22, 2026 (GLOBE NEWSWIRE) -- Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, today announced an expanded partnership with Google Cloud to deliver performance and security for AI workflows. The new solution uses Netskope One AI Guardrails to enable enterprise deployment of high-performance generative AI and autonomous agentic workflows at scale on Google Cloud. By leveraging Netskope capabilities, the solution improves the safety of those workflows and the data they use.

Enterprise investment in AI is expected to rise beyond $867.3B worldwide by 2029.[1] As organizations transition from simple chatbots to autonomous AI agents that execute tasks independently, the need for real-time, agent-native protection has become critical. As part of Netskope One AI Security, Netskope One AI Guardrails protects data, stops AI-specific threats, and provides content moderation to enable responsible AI use.

Hardware-Accelerated Responsible AI

- By using Google Cloud Tensor Processing Units (TPUs), Netskope aligns with some of the industry's most cost-efficient and high-throughput inference infrastructure, helping to ensure that security keeps pace with the fastest AI workloads.
- With this solution, safety checks can happen quickly on optimized TPU instances. By processing in-line with the model's native speed, Netskope can offer very low latency, without compromising performance.
- Utilizing Google Cloud's Vertex AI platform to perform real-time moderation allows Netskope One AI Guardrails to leverage the same specialized accelerator architecture that supports Google Cloud's AI services.

Enablement for Secure Agentic and Generative AI Ecosystems

- Netskope One capabilities secure autonomous agents, helping to ensure that when an agent calls a tool, interacts with an MCP server, or executes an autonomous task, every step is verified against enterprise policy in real time.
- The solution detects and breaks unintended recursive loops or malicious "ghost" commands that can lead to resource exhaustion or unauthorized system modifications on Google Cloud.
- The solution enforces real-time safety checks for categories such as hate speech and discrimination, criminal activity, suicide and self-harm, piracy and copyright, and requests for sensitive data.

Real-Time Behavioral Protection Against Multi-Vector AI Threats

- While traditional security focuses on data at rest, Netskope proactively identifies and blocks AI-specific threats, including prompt injection and jailbreaking, before they can compromise model integrity.
- As agents increasingly use MCP, APIs, and other tools, Netskope inspects the data passed between the agent and the tool to prevent indirect prompt injection and malicious execution.
- All detections are mapped to industry-standard frameworks like MITRE ATLAS™ and the OWASP Top 10 for LLMs, providing security teams with a clear and cleanly auditable risk posture.

Native Data Sovereignty and Compliance

- The solution from Netskope is deployed directly within a customer's Google Cloud instance, helping to ensure that sensitive prompts and responses are scanned locally, and that data doesn't leave the governed tenant.
- Customers can more easily meet stringent requirements like GDPR, HIPAA, and the EU AI Act by enforcing consistent policy across all AI communications.

"Netskope and Google Cloud's collaboration helps bring the best of AI innovation from Google Cloud and enterprise security from Netskope," said Vineet Bhan, Director of Security and Identity Partnerships, Google. "Netskope One AI Guardrails works with Vertex AI and TPUs to enable the secure deployment of both generative AI and autonomous agents. Together, we are helping organizations build the future of their business on a foundation of trust."

"As a global leader in AI-ready security and networking, Netskope provides critical capabilities required for the safe, high-performance adoption of modern AI workflows," said Sanjay Beri, CEO and Co-Founder, Netskope. "We are proud to collaborate with Google Cloud to help ensure that customers can confidently pursue their AI goals."

Netskope products are available on Google Cloud Marketplace.

About Netskope
Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for the AI ecosystem inclusive of agents, applications, tools, LLMs, people, devices, and data. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications – providing security and accelerating performance without trade-offs. Learn more at netskope.com, Netskope.ai, on LinkedIn, and Instagram.

Forward-Looking Statements
This press release contains forward-looking statements that are based on our management's beliefs and assumptions and on information currently available to our management. These forward-looking statements include enterprise investment in AI, demand for security solutions, and the expected benefits of new solutions offered to customers. These forward-looking statements are subject to the safe harbor provisions created by the Private Securities Litigation Reform Act of 1995. A significant number of factors could cause actual results to differ materially from statements made in this press release, including those factors related to customer adoption of new solutions and the impact new offerings may have for customers.

Media Relations Contact:
press@netskope.com

Investor Relations Contact:
ir@netskope.com

---

[1] IDC, Worldwide Artificial Intelligence ITSpending Forecast, 2025–2029, August 2025, IDC #US53688725