Netskope Unveils Netskope One AI Security, Delivering High-Performance Protection Across the Entire AI Ecosystem

March 11, 2026

Netskope One AI Security secures AI agents, AI applications and data, AI tools, and users across public SaaS, enterprise, and privately hosted AI, as well as agentic workflows, all from a single unified platform

SANTA CLARA, Calif., March 11, 2026 (GLOBE NEWSWIRE) -- Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, today announced Netskope One AI Security, a suite of AI security capabilities that protect, make visible, and accelerate the entire AI ecosystem, unified within the Netskope One platform. Netskope One AI Security introduces new products to power and enable the AI era, alongside a brand new, first-of-its-kind AI Index, which provides global tracking of AI adoption and emerging risks.

New products include:

- **Netskope One Agentic Broker:** Providing visibility and control over all MCP transactions whether sanctioned or unsanctioned - enabling organizations to secure agentic AI interactions.
- **Netskope One AI Guardrails:** Preventing AI-specific threats, including prompt injection and jailbreaking, and providing LLM content moderation to enable responsible AI use.
- **Netskope One AI Gateway:** Inspecting and enforcing security policies for private AI apps and/or LLMs organizations host or build themselves.
- **Netskope One AI Red Teaming:** Simulate adversarial attacks, uncover weaknesses, and assess safety risks of LLMs and AI applications.

Enterprise investment in AI continues to grow at a rapid rate: according to IDC, enterprise AI spending worldwide rose to $241.8B in 2025, and it is projected to pass $867.3B by 2029[1]. This rapid AI adoption has also created significant security gaps: organizations using legacy security products lack visibility into the ways their data is being used across AI based applications, private and public AI models, and AI agents and tools, with AI systems often bypassing security and introducing risks including data exfiltration, manipulative prompts, and inappropriate usage.

Netskope One AI Security provides comprehensive discovery, visibility and real-time control of AI applications, models, agents and tools in use, analyzes their specific risks, and accelerates secure AI adoption across the entire ecosystem, within a fully unified and integrated platform. Customers additionally benefit from Netskope NewEdge AI Fast Path, the set of capabilities that efficiently optimize latency to their AI destinations. Combining the high-performance access of NewEdge AI Fast Path with the intelligent, context-aware zero trust controls of Netskope One AI Security provides fully optimized and integrated performance, resilience, and security for enterprise AI.

“The AI Supercycle is here, demanding a new standard for high-performance security and networking. We believe the next decade will be defined by an intelligent edge. Our Netskope One platform combined with our NewEdge network is exactly that: a structural architecture built specifically for the requirements of an autonomous, agentic economy. This architecture provides an AI-native foundation with the innate ability to secure the complex data flows that power the modern AI ecosystem,” said Sanjay Beri, Co-Founder and CEO of Netskope. “With the launch of our new AI Security products and our AI Fast Path infrastructure, we are delivering deep, real-time protection at the speed of inference. By unifying high-speed performance with the active context of trillions of transactions, Netskope is providing the essential, adaptive fabric for the modern AI enterprise.”

Alexander Schuchman, CISO and SVP Global Network Engineering and Operations at Colgate-Palmolive Company said, “Colgate-Palmolive’s 220-year history of innovation is the foundation of our company’s purpose as a caring, innovative growth company that is reimagining a healthier future for all. We leverage technology solutions, including Artificial Intelligence, to drive creativity, efficiency and scale. AI systems offer powerful means for enhancing our business processes, improving customer and consumer experiences, and driving innovation across our operations. That said, technology comes with responsibilities, which is why we are guided by our employee Code of Conduct and AI Governance structure. We ensure the responsible deployment and use of AI systems by prioritizing good judgment, adherence with applicable laws and regulations, and ethical considerations to mitigate any unintended consequences. Colgate-Palmolive continues to partner with Netskope to provide data protection associated with our AI systems and associated use cases."

New Capabilities

Netskope One Agentic Broker:

- Provides unified visibility and real-time protection for the autonomous AI ecosystem by decoding and securing MCP traffic

between AI agents and data sources.
- Delivers real-time monitoring and governance over how AI agents interact with enterprise data sources.
- Ensures a consistent security posture that protects sensitive corporate data while enabling the speed and scale of agentic automation.

Netskope One AI Guardrails:

- Protects against emerging AI attacks including jailbreaking and prompt injection by acting as a real-time content moderator for every user and automated agent interaction.
- Seamlessly integrates with Netskope One DLP and Threat Protection within a single cohesive view, allowing security teams to understand the context of detections without managing fragmented alerts.
- Automatically detects and blocks discriminatory, copyrighted, and inappropriate content that creates legal and reputational risk for the enterprise.
- Maps detections to MITRE ATLAS and OWASP Top 10 for LLMs to stay ahead of adversary tactics.

Netskope One AI Gateway:

- Extend Netskope AI security controls to secure agentic communications in private AI environments (on-premises, virtual private cloud) that don't go through the cloud for inspection, centralizing authentication, traffic management, and content inspection.
- Enables organizations to secure interactions between apps and LLMs and ensure autonomous agentic data flows remain governed and secure.

Netskope One AI Red Teaming:

- Extends Netskope protection into the development cycle to proactively prevent and remove vulnerabilities in private AI deployments.
- Exposes AI models to thousands of simulated attacks, identifying where complex multi-turn attacks could bypass default AI model guardrails, stopping performance drift.

Netskope One Agentic Broker, Netskope One AI Gateway, Netskope One AI Guardrails, and Netskope One AI Red Teaming are all generally available today. Read more about securing agentic AI and securing private AI on the Netskope blog. Visit Netskope.com/AI for the latest updates on AI security, performance, and analytics from Netskope.

Netskope will be demonstrating the full Netskope One platform at RSA Conference in San Francisco, March 23-26, 2026. Engage with Netskope at RSA Conference by visiting booth #1127 in Moscone South, scheduling a session with Netskope experts, and joining Netskope speaking sessions and social events.

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 beliefs and assumptions and on information currently available to us. These forward-looking statements include the growth of AI and the impact of AI on enterprises. 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 adoption of AI and our customers' purchasing decisions. Any forward-looking statements in this release are based on the limited information currently available to Netskope as of the date hereof, which is subject to change, and Netskope will not necessarily update the information, even if new information becomes available in the future.

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