Zscaler Unveils New Product Innovations to Secure Agentic AI

June 9, 2026

Delivers Industry's First Complete Zero Trust Platform for Agentic AI with Comprehensive Protection for How Agents Access Data, Interact with Systems, and Operate Across the Enterprise

LAS VEGAS, June 09, 2026 (GLOBE NEWSWIRE) -- Zenith Live 2026 -- Zscaler, Inc. (NASDAQ: ZS), the cybersecurity platform for the AI era, today announced major innovations to extend the Zscaler Zero Trust Exchange™ platform to secure AI Agents–how they connect, access data, and run on devices. With these innovations, Zscaler is delivering the industry's first complete Zero Trust platform for Agentic AI.

Today, enterprise security is undergoing a shift from human users to autonomous agents. Traditional security tools were designed around known human identities and predictable access patterns. Autonomous AI agents change that model. They operate on a user's behalf as well as autonomously and at machine speed, creating ephemeral identities, spawning sub-agents and tasks, and exercising permissions in ways that traditional security tools cannot fully see or control. While they can deliver significant efficiency gains, AI agents also introduce new gaps in visibility, access, and governance, obscuring agent risk and making data flows difficult to track at scale. As AI becomes more deeply embedded in software development, endpoints are also increasingly exposed to malicious agents, tools, and plugins that many legacy endpoint security solutions were not designed to detect.

To help companies adopt agentic AI more securely, Zscaler is introducing the next evolution of its Zero Trust Exchange with new solutions that expand protections across the AI ecosystem – helping organizations put agentic AI to work with stronger security and greater confidence. These include two key advances:

- **Zscaler AI Broker** helps secure agentic communications through MCP and A2A brokers. With an integrated Agent Registry, it helps organizations understand what each agent is allowed to access and apply fine-grained access across enterprise AI agents.
- **Zscaler Endpoint AI Security** helps customers find and stop AI-related threats on employee devices, including risks hidden in browsers, plugins, extensions, and local AI tools. This capability reaches into the browser, extension, and plugin layers that traditional endpoint security tools miss. Now Zscaler can enforce policies to secure AI everywhere including endpoint and cloud.

Introducing Zscaler AI Access Graph: Connecting the dots of Data and Identity lineage with AI for enhanced security and governance of Agentic AI

An important element of agentic security is understanding which agents, users, and identities are communicating with which models, applications, and data sources. Powered by Zscaler's recent acquisition of Symmetry Systems, Zscaler AI Access Graph maps how identities, applications, and other data sources connect across the enterprise. The integration of this technology with Zscaler's Zero Trust Exchange enables organizations to understand and then enforce policies, reduce unnecessary access and risk, and track data lineage in real-time across every channel.

Building on **Zscaler AI Protect** launched in January 2026, Zscaler is also delivering major new enhancements across AI Protect's three core use cases:

- **AI Asset Management** (visibility into AI assets, usage, and risk) gains new capabilities to discover embedded AI in SaaS and internet traffic, identify AI agents and MCP servers in public cloud environments, uncover risks in agentic codebases through code scanning, and extend visibility to AI activity on endpoints.
- **Secure Access to AI** (safe, governed access to sanctioned AI tools) expands controls for AI interactions with prompt extraction across more than 250 GenAI apps and adds full conversational views, support for Anthropic and OpenAI Compliance APIs, and intent-based guardrails for multi-turn conversations.
- **Secure AI Infrastructure and Apps** (protection for AI apps across the development and runtime lifecycle) introduces AI red teaming for MCP servers, a standalone prompt hardening service, and compliance heat maps to strengthen AI governance.

"Traditional security was never designed for millions of autonomous agents that act and reach sensitive data at machine speed," said Jay Chaudhry, Chairman and CEO of Zscaler. "We pioneered Zero Trust Exchange to secure users, branches and cloud workloads and now we are innovating to extend the Zero Trust security to AI Agents. Now Enterprises are not held back from rolling out agents everywhere."

"Managing data security is no longer just about building high walls; it is about scaling visibility and treating data as a highly active, strategic asset," said John Israel, Global CISO at KPMG, who joined Zscaler as a guest speaker to discuss the launch. "As businesses scale their use of AI agents to optimize operations, having a unified, zero-trust framework to trace data lineage and govern agent-to-agent interactions is paramount to maintaining trust, compliance, and competitive advantage."

Together, these innovations deliver a comprehensive framework for securing agentic AI – built on Zscaler's Zero Trust Exchange platform to protect enterprises today and into the future. By safeguarding agents with comprehensive security controls, organizations can now accelerate their AI adoption with confidence.

For more information on the latest Zenith Live announcements, please visit: http://www.zscaler.com/events/zenithlive2026

About Zscaler
Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world's largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across 160+ data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

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 the expected development, integration, adoption, performance and benefits of Zscaler's new AI Security Platform offerings and Zscaler AI Protect enhancements. 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 Zscaler's ability to develop, deliver and achieve customer adoption of these AI security solutions and platform enhancements. Additional risks and uncertainties are set forth in our most recent Quarterly Report on Form 10-Q filed with the Securities and Exchange Commission ("SEC") on May 26, 2026, which is available on our website at ir.zscaler.com and on the SEC's website at www.sec.gov. Any forward-looking statements in this release are based on the limited information currently available to Zscaler as of the date hereof, which is subject to change, and Zscaler will not necessarily update the information, even if new information becomes available in the future.

Media Contact
Nick Gonzalez, Director of Global Public Relations, press@zscaler.com