Zscaler launches Agentic SOC to contain AI-Driven Threats

September 9, 2026

Unifying exposure management and SOC workflows with Zscaler telemetry and specialized AI agents that detect, investigate, and respond to threats at machine speed

SAN JOSE, Calif., Sept. 09, 2026 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the cybersecurity platform for the AI era, today announced Zscaler Agentic SOC, a new approach to security operations built to proactively reduce exposures, scale human expertise and stop AI-driven attacks at machine speed. In today's threat landscape, simply layering in AI capabilities onto the existing security stack will not provide the protection needed. Zscaler is delivering a new solution to the security operations center (SOC), purpose-built from the ground up with an AI-first approach to detect, investigate, and stop threats at machine speed.

Today's threat landscape is defined by speed and stealth as AI-driven attacks move faster than SOC teams can manually correlate, analyze, and remediate. Threatlabz, Zscaler's global research team, is also seeing a rise in evasive tactics, including the use of trusted sites to host attacks, abuse of legitimate remote management tools, and browser-based attacks. Zscaler Agentic SOC is built to meet that challenge by combining unique Zscaler telemetry, the world's largest decoy mesh network, expert-validated agents, integrated Zscaler Zero Trust controls, and customers' third-party controls to detect threats earlier and automate containment at machine speed.

To power Agentic SOC, Zscaler has partnered with leading frontier AI labs, including Anthropic and OpenAI. By integrating their frontier models alongside Zscaler's proprietary threat intelligence and zero trust telemetry, Zscaler is able to deliver AI agents that reason with greater depth, accuracy, and explainability than any single model or approach could achieve alone. This extends beyond threat detection, with Zscaler's open platform approach enabling direct integration with frontier models, allowing security teams to ingest vulnerability findings and operationalize them within their SOC workflows. This collaboration reflects Zscaler's commitment to building on the best available AI that includes speed, reliability and transparency that security operations demand.

"AI-driven attacks are moving faster than traditional SOC models were ever designed to handle," said Deepen Desai, Executive Vice President of Cybersecurity at Zscaler. "Agentic SOC is a fundamental rethinking of security operations, built with agentic capabilities at its core to reduce exposures proactively, extend human expertise with AI agents and contain threats at machine speed. With unmatched inline telemetry, specialized AI agents and closed-loop remediation, Zscaler is giving security teams the visibility and control they need to outpace modern attackers."

"The past year has made one thing clear: AI attacks are fundamentally changing the threat landscape, operating at a speed, scale, and level of adaptability that looks very different from traditional human-led activity," said Allie Mellen, principal analyst and author of Code War: How Nations Hack, Spy, and Shape the Digital Battlefield. "To defend effectively, organizations must double down on the fundamentals — Zero Trust principles, preventing data exfiltration, limiting access, and making AI attacks as expensive as possible."

Reimagining SecOps: The Zscaler Differentiation

- **Unified exposure and threat management:** Zscaler connects proactive attack surface reduction with reactive threat defense in a single platform, enriching context and accelerating protection.
- **Unmatched zero trust telemetry:** Zscaler sits inline, capturing network, identity, endpoint, cloud and AI insights across its 750 billion daily zero trust transactions that security teams can operationalize for real-time detection and response.
- **Specialized AI agents built on frontline experience:** Zscaler AI agents have been trained and continuously tuned on more than 10 years of frontline SOC, managed detection and response and threat-hunting experience, informed by threat intelligence derived from thousands of customer environments globally.
- **Closed-loop inline remediation:** Zscaler automatically contains threats at machine speed with native inline controls that can isolate compromised users, block command-and-control communications, and cut off lateral movement. Integrations with customers' third-party tooling provide increased options for nuanced responses to active threats.

"Our team was drowning in alert noise, forcing top analysts into triage instead of proactive threat hunting," said Andrea Liccardi, Sr. Cybersecurity Manager, Maire Tecnimont. "Zscaler Agentic SOC gives us full attack-path context using telemetry we already had in place, helping our team move from fragmented signals to faster, more informed decisions. Zscaler has proven to be one of our most valuable cybersecurity partners, continuously helping us improve operational efficiency, visibility, and our ability to focus our analysts on what really matters."

Open Platform Integration
Zscaler Agentic SOC seamlessly integrates with your existing security ecosystem, pulling in third-party data to contextualize risks and threats. By triggering automated outbound actions, it proactively eliminates exposures and contains attacks at machine speed.

Key Features of Zscaler Agentic SOC

- **Data-rich context graph:** Correlates real-time zero trust telemetry with third-party data to map, prioritize and investigate complex incident chains.
- **Specialized AI agents:** Autonomous agents perform dedicated roles across triage, root-cause investigation, assigning verdicts, and triggering response workflows, reducing analyst workload and accelerating defenses.
- **Advanced detections informed by threat intelligence:** Applies frontline threat research and rich telemetry to identify

sophisticated attacks earlier and with greater precision.
- **Continuous threat hunting and expert support:** Combines AI speed with seasoned human judgment from Zscaler and Red Canary security experts.

Availability and Additional Information
Zscaler Agentic SOC is available globally today. To learn more, register for the global launch webinar or visit zscaler.com/solutions/agentic-secops.

Follow Zscaler on LinkedIn, X, 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 the expected adoption, performance and benefits of Zscaler Agentic SOC, including its AI agents, third-party integrations and automated threat-containment and remediation capabilities. 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 deliver and achieve customer adoption of Zscaler Agentic SOC and the performance and effectiveness of its AI-driven and automated capabilities. Additional risks and uncertainties are set forth in our most recent Annual Report on Form 10-K filed with the Securities and Exchange Commission ("SEC") on September 3, 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.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across over 200 public data centers globally and thousands of private sites at the edge, the SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

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