



Zscaler Expands AI-Guardian, Uniting Tech Giants to Secure Enterprise AI at Scale

June 9, 2026

Expanded ecosystem collaboration unites Zscaler's Zero Trust Exchange with leading AI, cloud, and infrastructure technologies enabling interoperability and security signal sharing across AI enterprise interactions

LAS VEGAS, June 09, 2026 (GLOBE NEWSWIRE) -- Zenith Live 2026- [Zscaler, Inc.](#) (NASDAQ: ZS), the cybersecurity platform for the AI era, today announced the next phase of its Project AI-Guardian by expanding the initiative to include technology alliance partners. The expansion broadens the ecosystem collaboration first built with the world's leading global system integrators (GSIs), deepening interoperability across the Zscaler Zero Trust Exchange™ platform and the Company's AI Protect portfolio with complementary partner technologies.

As enterprises adopt generative AI, agentic workflows, and AI-enabled SaaS, no single vendor secures the entire AI estate on its own. Security teams are left stitching together point products that don't share context, leaving blind spots across the rapidly expanding AI attack surface. What organizations need is not another silo, but a comprehensive AI security platform that interoperates with leading and existing technologies to share signals, identity context, and enforcement work.

The expansion of Project AI-Guardian is built around that principle. Through the Zero Trust Exchange, core Zscaler AI services will integrate directly with technology alliance partners. The integration includes the AI Access Graph, which continuously maps how identities, applications, agents, and data connect to AI services; AI attack surface and risk modeling, which discovers and quantifies AI-related exposure across the environment; and additional governance and protection capabilities. Partners both enrich and act on these signals, so insight gathered in one platform can drive enforcement in another.

Because every interaction is brokered through the Zero Trust Exchange, enforcement happens inline and in real time. Access is verified continuously, data is inspected as it moves, and zero trust policy is applied to AI usage the same way Zscaler applies zero trust to users, workloads, and devices today. For customers, interoperability means a consistent control plane for AI without the integration burden of connecting disparate tools. For partners, it means a platform-native path to extend their capabilities across the enterprise AI estate.

Technology alliance partners include: AWS, CoreWeave, Databricks, Deep Cogito, Equinix, Glean, Google Cloud, OpenAI, Saviynt, along with additional GSI Partners Coforge and NTT DATA. These partners join the founding GSI partners (Cognizant, EY, HCLTech, Infosys, TCS, and Wipro) to deliver a comprehensive, end-to-end framework for securing AI.

"AI is creating enormous opportunities for organizations, but it is also reshaping the threat across the security and governance landscape," said Dhawal Sharma, EVP- AI Security and Strategic Initiatives, Zscaler. "Securing AI is an ecosystem effort. With the expansion of Project AI-Guardian through our technology alliance partners, Zscaler is helping customers extend zero trust across enterprise AI interactions so they can adopt AI faster while maintaining the visibility, control, and data protection they need to innovate securely."

Through this expanded initiative, Zscaler and its technology alliance partners will deliver deep integrations across the entire AI pipeline, addressing critical security needs:

- **Zero Trust Controls for AI Workflows:** Enforcing granular policy controls for AI applications, development infrastructures, and workflows designed to prevent unauthorized access and usage.
- **Comprehensive Data Protection:** Helping prevent the leakage of sensitive intellectual property or customer data through prompts, model training inputs, or autonomous AI-to-AI interactions, both inline and out-of-band.
- **Continuous Visibility and Governance:** Delivering a 360-degree view of the organization's AI footprint—including shadow AI apps, model APIs, and cloud-hosted infrastructure—to help ensure alignment with compliance and risk management frameworks.
- **Streamlined Deployment and Time-to-Value:** Providing pre-validated, interoperable partner integrations that simplify deployment and allow security teams to safely accelerate business transformation.

This next phase of Project AI-Guardian reflects Zscaler's vision for secure AI transformation: an open, security-first framework that helps enterprises unlock the value of AI with confidence.

Coforge

"As enterprises accelerate their AI transformation journey and deploy agentic systems at scale, the urgency to secure AI assets from edge to cloud has never been greater. Through Project AI-Guardian, Coforge is uniting Zscaler's AI Asset Management and Zero Trust Everywhere with our Secure Edge2Cloud Solution and Trust AI platform. The combination embeds automated governance, privacy guardrails, and continuous assurance directly into the AI lifecycle — enabling enterprises to discover, secure, and scale their AI deployments without compromising on trust or business velocity," Ashish Kumar, SVP & Global Head - Cloud, AI-Infra & Security, Coforge.

CoreWeave

"As enterprises move AI into production, the attack surface expands at the infrastructure level, beyond just the application layer, said Jim Higgins, Chief Information Security Officer, CoreWeave. "CoreWeave's security is built from the silicon up, and working with Zscaler through Project AI-Guardian means customers will be able to enforce zero trust access controls at every layer of their AI stack, from compute to agent interaction."

Databricks

"Customers consistently tell us they want to route their security data to their Databricks environment and extend their existing security vendor protections to our platform. Our partnership with Zscaler delivers on both fronts. By ingesting Zscaler logs into Databricks and collaborating on Project AI-Guardian, we are helping joint customers safely accelerate their AI initiatives without creating new security silos," Stephen Orban, SVP Product Partnerships & Ecosystem.

Deep Cogito

"Defending against frontier-grade threats requires specialized intelligence models, post-trained on a security team's data and outcomes. Zscaler understood this from the start - going beyond lightweight customization to build specialized intelligence into the model itself," said Drishan Arora, Co-founder and CEO Deep Cogito. "Through Project AI Guardian, we're extending that work to help enterprises adopt AI with the security posture this moment demands."

Equinix

"Equinix is committed to enabling secure, scalable AI innovation across the enterprise," said Maryam Zand, Vice President of Partnerships and Ecosystem Strategy at Equinix. "Our longstanding partnership with Zscaler makes that vision even more powerful, by combining global digital infrastructure with zero trust security to help customers protect their AI interactions. Together, we're giving our joint customers the security controls and infrastructure they need to deploy AI workloads with confidence, at scale."

Glean

"Scaling enterprise AI safely requires both trusted business context and a security ecosystem that can govern how that context is accessed and used," said Sunil Agrawal, CISO, Glean. "Glean helps organizations bring secure, permissions-aware enterprise knowledge directly into AI workflows, and Zscaler's Project AI-Guardian provides an important framework for extending visibility, control, and protection across those interactions. Together, we're helping customers move AI from experimentation to impact while giving security teams greater confidence as adoption scales."

NTT DATA

"As organizations enter the AI execution era, driving a new wave of autonomous enterprise transformation, security must evolve just as rapidly. By collaborating with Zscaler on Project AI Guardian, NTT DATA is combining Zscaler's Zero Trust Everywhere framework with our full-stack Security for AI capabilities to help enterprises prepare for frontier AI risks and accelerate their agentic AI-driven transformation with confidence, resilience and speed," Sheetal Mehta, Global Head of Cybersecurity at NTT DATA, Inc.

OpenAI

"As AI becomes an increasingly important tool for cybersecurity, organizations need systems that are not only capable, but secure, reliable, and aligned with the realities of enterprise risk management. Through our partnership with Zscaler and initiatives like Trusted Access for Cyber and Project AI-Guardian, we're advancing a shared commitment to deploying AI responsibly—combining frontier capabilities with rigorous safeguards, transparency, and human oversight. Together, we're helping security teams strengthen their defenses while building confidence in the safe adoption of AI across the enterprise," Scott Rosecrans, Vice President, Strategic Pursuits, OpenAI.

Saviynt

"AI security is an identity problem first. Zscaler stops threats in motion; Saviynt governs the identities behind them. Together, we give enterprises the control plane they need to adopt AI without losing visibility or governance," Vibhuti Sinha, Chief Product Officer, Saviynt.

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 performance and benefits of Project AI-Guardian and Zscaler's Technology Alliance Partners, including delivering zero trust controls across enterprise AI workflows. 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 achieve partner and customer adoption of Project AI-Guardian and initiatives with Zscaler's Technology Alliance Partners. 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