Zscaler Unveils New Innovations to Secure Enterprise AI Adoption

January 27, 2026

New Capabilities Empower Organizations to Gain Visibility into, and Securely Build, Deploy, and Use AI Applications Across the Enterprise

SAN JOSE, Calif., Jan. 27, 2026 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced new AI security innovations designed to empower enterprises to secure the fast growing use of AI, while maintaining visibility, control, and governance. As organizations today adopt generative AI and prepare for the use of agentic AI, they face rising risk of cyberattacks and data loss because traditional security models weren't designed to secure AI. The Zscaler AI Security Suite eliminates the trade-off between AI innovation and risk, providing the visibility and controls needed to securely build, deploy, and govern AI at enterprise scale.

Most enterprises lack a complete view of the AI applications and services in use, including GenAI tools, AI development environments, embedded AI in SaaS, models, agents, and underlying infrastructure. This limits their ability to understand AI exposure, data access, and risk. Organizations also struggle to control access and enforce policy as AI traffic shifts to new protocols and non-human patterns that traditional security tools cannot govern. In fact, in the ThreatLabz 2026 AI Security Report published today, Zscaler experts found most enterprise AI systems could be compromised in just 16 minutes with critical flaws uncovered in 100% of systems analyzed.

Zscaler's new innovations provide enterprises with a comprehensive inventory and dependency map of their AI footprint, spanning GenAI services, embedded AI SaaS, AI development environments, MCP servers, agents, models, and AI infrastructure. The solution correlates asset discovery, access relationships, data lineage, runtime behavior, and security posture, enabling organizations to adopt AI faster while maintaining security, governance, and control.

"AI is changing how businesses operate, but traditional security approaches were not designed to secure AI," said Jay Chaudhry, CEO, Chairman, and Founder of Zscaler. "Business leaders are looking for a comprehensive solution - not more point products. At Zscaler, we're providing the security necessary for leaders to move forward with confidence and embrace the full spectrum of AI. We aren't just securing the AI era; we're accelerating it."

Revolutionizing AI Security Across Three Core Enterprise Use Cases

The new Zscaler AI Security suite addresses enterprise AI security challenges in three critical ways:

- **AI Asset Management** gives CISOs, IT, and governance teams a comprehensive inventory of AI apps, models, infrastructure, agents, and usage, helping them detect shadow AI, understand what data AI touches, and prioritize risk by providing visibility on AI usage.
- **Secure Access to AI** helps security architects and IT admins safely enable sanctioned AI services like developer tools and AI models with Zero Trust controls, inline inspection, and prompt classification to reduce data loss and misuse while preserving productivity.
- **Secure AI Infrastructure and Apps** equips application teams to protect AI development across the lifecycle with automated AI red teaming, prompt hardening, runtime guardrails and continuous risk posture assessment from build to runtime.

"The industry is currently struggling with a massive visibility gap because AI traffic doesn't behave like traditional web traffic," said Zeus Kerravala, Principal Analyst, ZK Research. "It's faster, non-human, and uses protocols that most security stacks simply can't see. What's important here isn't just another security tool; it's the shift toward a Zero Trust framework that actually understands the context of an AI conversation. Without this level of deep inspection and automated guardrails, enterprises are essentially flying blind into the most significant technology transition of our lifetime."

Governance, Partnerships, and Supplemental Controls

To simplify global AI adoption, Zscaler now supports customers in aligning their security programs with frameworks such as the NIST AI Risk Management Framework and the EU AI Act. This governance is paired with CXO-level reporting on GenAI usage and deep ecosystem integrations with OpenAI, Anthropic, AWS, Microsoft, and Google. Additionally, Zscaler is expanding its defense capabilities with a new MCP gateway for secure automation and AI Deception to divert and neutralize model-based attacks.

To dive deeper into the latest advancements to the Zscaler AI Security suite, please read the following blog - *Accelerating AI Initiatives with Zero Trust*.

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 benefits of the expansion of our AI Security portfolio and the solutions and protections offered to our 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 our ability to successfully integrate new features of our product offerings into our AI Security portfolio and the business impact additional offerings may have for our customers. 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 November 25, 2025, 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 more than 160 data centers globally, 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