Zscaler and OpenAI Partner to Advance the Next Era of Cybersecurity

April 15, 2026

Zscaler is proud to partner with OpenAI as part of their Trusted Access for Cyber (TAC) program, which expands trusted, verified access to advanced AI capabilities for defenders. As part of this program, we plan to use GPT 5.4-Cyber, a TAC-enabled variant of GPT-5.4, to further improve cybersecurity for our Zero Trust Exchange platform and for our customers. GPT 5.4-Cyber will be integrated into our secure Software Development Lifecycle (SDLC) workflows, empowering our teams to instantly detect, triage, and mitigate vulnerabilities earlier and patch security vulnerabilities faster. In addition to safeguarding software, Zscaler has a long history of harnessing OpenAI technology to fight AI-based attacks, including within our AI Red Teaming and Agentic SecOps solutions.

Safeguarding the Zscaler Platform

Secure software development is a business imperative at Zscaler. Participating in Open AI's TAC program enables us to integrate GPT 5.4-Cyber and Codex Security into Zscaler's internal multi -agent security architecture for cyber defenses and product hardening. GPT 5.4-Cyber is a key enabler to offer Security-as-a-Service to our developers throughout the SDLC process, from validating threat models in designs, to assisting with secure code reviews, finding vulnerabilities, and executing black-box testing on built artifacts.

We are approaching TAC with both a defensive and offensive mindset. In addition to improving security through the SDLC, we are leveraging the model to improve cyber readiness by turning large volumes of security signals into actionable intelligence, prioritizing true risk, and accelerating remediations. Moreover, we are relying on the model for offensive-informed posture hardening by modeling adversarial attack paths and highlighting weak controls, which enables us to neutralize exposures at unprecedented speeds.

Combining the frontier OpenAI models with Zscaler's industry -leading Zero Trust architecture leads to better security outcomes for our customers. In addition to leveraging AI to identify and remediate any software vulnerabilities, Zscaler's Zero Trust architecture adds another layer of protection by making critical apps and software invisible to the Internet. This combination provides Zscaler customers superior protection compared to obsolete VPNs and firewalls, maximizing software resiliency while systematically eliminating the internet-facing attack surface.

Harnessing OpenAI for AI Red Teaming

Zscaler has been using OpenAI's 4.x and 5.x models for building advanced capabilities in our AI Red Teaming suite of products to help customers safely build and deploy AI systems, including:

- Continuous Red Teaming
- Prompt hardening
- AI Asset Analysis
- Agentic Radar open source program

Zscaler's AI Red Teaming platform (formerly SPLX) has relied on OpenAI models across the stack since early 2024. Multiple versions of OpenAI models have been central to dynamically generating attack sequences to harden AI systems. With multimodal red teaming (spanning voice and images), OpenAI's image generation, text-to-speech, and speech-to-text capabilities deliver a decisive tactical advantage. Together, these capabilities provide an industry leading solution to strengthen the security of their AI initiatives.

Beyond merely exposing vulnerabilities during red teaming exercises, Zscaler's solution dictates instant remediation in true closed loop fashion by generating optimized system prompts. This serves as the definitive first step AI engineers take to help improve security and safety posture.

Zscaler is also using OpenAI models as part of its AI Asset Analysis solution, which analyzes MCP tools and risks, and provides overall risk analysis for complex AI agents based on source-code scanning. This is an enterprise version of the Agentic Radar open source program, which powered the largest OpenAI hackathon last year in Warsaw, Poland.

Leveraging OpenAI for Agentic SecOps

Zscaler's Red Canary Managed Detection and Response (MDR) service combines AI-powered threat detection with expert security operations in partnership with OpenAI. OpenAI-powered agents work alongside Zscaler experts to handle the tedious context-gathering that traditionally overwhelms SecOps analysts. Elite human analysts dictate workflows, enforce rigid guardrails, and rigorously validate all outputs, maintaining the 99.6% true-positive rate our customers depend on. By pairing OpenAI's adaptive capabilities with Zscaler's data pipelines, expert procedures, and rigorous validation, we deliver faster, more consistent investigations without sacrificing the accuracy that defines the Zscaler Red Canary MDR service.

Building the Right Foundation

AI is fundamentally rewriting the rules of cybersecurity. By partnering with leading vendors like OpenAI, Zscaler is ensuring AI can be used to help improve the overall resilience of our security infrastructure, and mitigate risks from AI-based attacks. We look forward to working with OpenAI as part of their TAC program to improve outcomes for our customers. Enterprise organizations will benefit immensely by using state of the art OpenAI models for better defenses combined with Zscaler's industry leading Zero Trust architecture to minimize the attack surface and assets exposed on the Internet with traditional VPNs and Firewalls.