TENEX.AI Partners with Google Cloud on Google AI Threat Defense

TENEX.AI partners to deliver Google Cloud's new autonomous, continuous security platform at enterprise scale

SARASOTA, FL, UNITED STATES, May 27, 2026 /EINPresswire.com/ -- TENEX.AI, the AI-native, human-led Agentic SOC company, today announced its expanded partnership with Google Cloud to deliver Google AI Threat Defense, a newly announced automated security system designed to continuously monitor for and outpace AI-driven attacks.

Announced today, Google AI Threat Defense fuses the reasoning power of Gemini and other frontier models, the contextual risk prioritization of Wiz, the code remediation capabilities of CodeMender, and the frontline expertise of Mandiant, operationalized through a four-step framework: Prepare, Scan and Prioritize, Remediate, and Monitor.

This announcement arrives as AI-driven attacks can exploit vulnerabilities at unprecedented speeds, outpacing security teams' ability to prevent them. Google Cloud is delivering AI Threat Defense to help organizations outpace AI-enabled adversaries and stop threats before impact.

TENEX.AI's role is to help operationalize and deliver this new architecture inside enterprise customer environments, turning autonomous platform capabilities into verified, remediated code integrated continuously with a real-time, AI-native, human-powered SOC.

"Every CISO I talk to is being asked the same question by their board: how will the security team keep up when adversaries become autonomous? Google AI Threat Defense gives them a credible answer at the platform layer; TENEX gives them the delivery model that turns it into measurable outcomes. That is the combination enterprises are asking for, and it is a core thesis behind our investment in TENEX." — Greg Clark, Founder & Managing Partner, Crosspoint Capital Partners

What Google AI Threat Defense Delivers

Google's new AI Threat Defense delivers:
- Mapping the attack surface across multicloud, multi-AI, code, SaaS, and hybrid environments via Wiz
- Deep vulnerability hunting through AI security agents (including CodeMender) drawing on

multiple frontier models via the Gemini Enterprise Agent Platform
- Exploitability validation by enriching findings with live architectural and runtime context, filtering theoretical flaws down to reachable, business-critical risk
- Autonomous remediation at machine speed, generating, testing, and applying patches directly in developer IDE/CLI workflows and across live production environments
- Continuous monitoring through Google Security Operations SOC capabilities and Wiz's agents
The full announcement is available at the Google Cloud blog.

TENEX.AI's Role: Turning the Platform into an Outcome

Most enterprise security organizations, particularly in regulated industries, lack the engineering bandwidth to translate these new AI-driven capabilities into measurable risk reduction. TENEX.AI is built to close that gap.

To support Google AI Threat Defense, TENEX.AI has built a dedicated delivery offering for the platform, available as a standalone service for any enterprise through TENEX.AI's AI-native, human-led SOC and through its MDR and service offerings where customers need a fully integrated and unified AI security workflow.

As a Google AI Threat Defense partner, the TENEX.AI offering includes:
- Rapid validation engagements to demonstrate for customers what Google AI Threat Defense will actually deliver against their specific codebase, infrastructure, and threat model: measured outcomes, not slideware.
- Direct TENEX.AI AI-driven SOC and MDR integration into Google AI Threat Defense to feed verified, exploitable findings as enriched application telemetry directly into Google Security Operations playbooks from TENEX.AI's automated triage agents, surfacing AI-detected, code-level risk in the same workflow as runtime detection, not in a separate ticket queue.
- High-fidelity, exploitability-validated triage with elite human analysts on the loop to funnel the large volume of model findings down to verified, reachable, exploitable flaws - eliminating the false-positive overhead that has historically kept AppSec tooling off engineering roadmaps.
- TENEX.AI-engineered drafts and patches, using deep, AI-driven structural code context, shipped alongside customer engineering teams to fulfill customers' workload-side obligations under the Google Cloud Shared Fate Model.
- Custom data-boundary maps for proprietary middleware. TENEX.AI creates bespoke architectural maps for in-house and proprietary middleware that commercial scanners typically miss, helping ensure AI Threat Defense covers the code that is uniquely yours and is uniquely prioritized.

"AI Threat Defense gives enterprises a real shot at outpacing AI-driven adversaries - but a platform isn't an outcome, and most security organizations don't have the engineering bandwidth to bridge that gap on their own. That's the work TENEX is built for: showing customers proof of value on their own code and infrastructure, triaging findings down to verified, exploitable risk, drafting and shipping patches alongside engineering teams, and closing

the loop back into our MDR so code-level risk surfaces in the same workflow as runtime detection." — Eric Foster, Founder & CEO, TENEX.AI

"Legacy MDR was built around a human-speed model of security operations with alerts, escalations, investigations, and response queues. AI is changing the pace of the threat landscape faster than most organizations can adapt. The next generation of cybersecurity will come from combining autonomous security platforms with an MDR built around AI from the start. That's what Google AI Threat Defense and TENEX bring together for enterprise customers, and it's why I'm proud to chair this company."" — Elias "Lou" Manousos, Chairman, TENEX.AI

About TENEX.AI
TENEX.AI: The AI SOC Company. The AI-native, human-led AI SOC and Managed Detection and Response (MDR) provider led by operators who've built and scaled MDR before, with founding engineers from the hyperscalers and leading AI labs. Recently named the #1 fastest-growing cybersecurity company in the country by IT-Harvest's 2026 Cyber 150, TENEX.AI serves enterprise customers across Google and Microsoft security ecosystems. TENEX.AI's platform triages, investigates, hunts, and responds to threats autonomously, with elite human analysts always in the loop, combining the speed and scalability of AI with the accountability of human-led security operations. Backed by Crosspoint Capital Partners, Shield Capital, DTCP, Deepwork Capital, and the Florida Opportunity Fund, with its seed round led in 2025 by Andreessen Horowitz (a16z), TENEX.AI is headquartered in Sarasota, FL with offices in Overland Park, San Jose, and Phoenix. Learn more at TENEX.ai.

TENEX.AI PR
TENEX.AI
+1 650-605-7865
email us here
Visit us on social media:
LinkedIn
Facebook
X