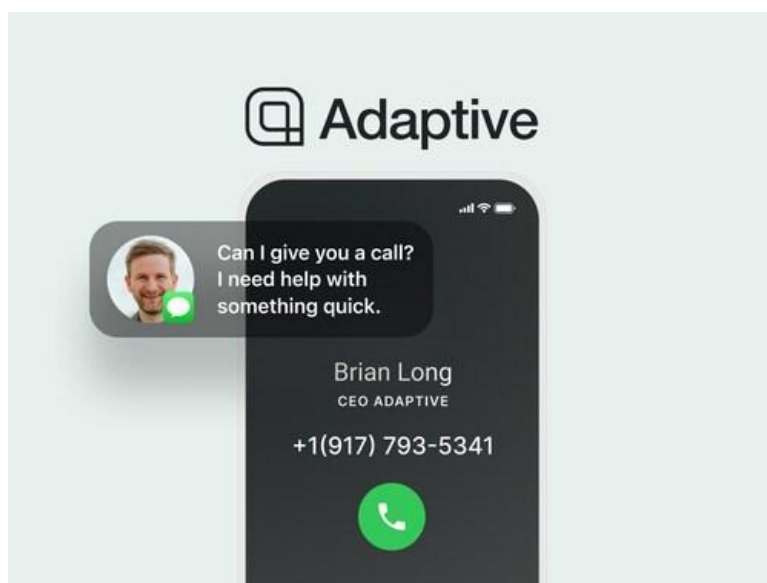


Adaptive Security Raises \$43M from a16z and OpenAI Startup Fund to Combat AI-Powered Cyber Attacks Including Deepfakes, Vishing and Smishing

NEW YORK, April 2, 2025 /PRNewswire/ -- Adaptive Security, the leading provider of AI-powered social engineering prevention solutions, today announced a \$43 million funding round led by Andreessen Horowitz (a16z) and the OpenAI Startup Fund, marking OpenAI's first investment in a cybersecurity startup. Additional participating investors include Abstract Ventures, Eniac Ventures, CrossBeam Ventures and K5, along with executives from Google, Workday, Shopify, Plaid, Paxos and others. The funding will accelerate Adaptive's development of solutions to defend against AI-powered social engineering attacks.



Most companies aren't prepared for deepfake personas and GenAI attacks

Today, cybercriminals can easily create deepfake AI personas that closely mimic real individuals, attacking over real-time phone calls, video chats and emails. Open-source intelligence models give attackers powerful tools to impersonate an individual's responses in a real-time, realistic manner.

According to Entrust, a deepfake attack attempt occurred every five minutes in the U.S. in 2024 — suggesting more than 100,000

incidents across the year. Sumsb reported a 17-fold year-over-year increase in deepfake attacks in the U.S., fueled by new open-source large language models (LLMs) that provide cheap AI with limited safety controls.

These sophisticated deepfake persona attacks are no longer limited to high-profile executives — deepfake personas can now be generated for nearly anyone in seconds, using open-source intelligence to create hyper-realistic AI clones.

Deepfake attacks have reached a new level of sophistication and boldness. In one instance, a convincing video call featured an AI-generated impersonation of Ukraine's foreign minister speaking with U.S. Sen. Ben Cardin — an attempt to manipulate U.S. foreign policy (New York Times). In Hong Kong, criminals used AI-generated voices in a video call to trick a bank manager into wiring \$25 million (CNN). Even cybersecurity executives are being targeted — Wiz CEO Assaf Rappaport reported that attackers cloned his voice in a sophisticated deepfake attack aimed at deceiving his team (TechCrunch). These incidents signal a disturbing shift in the threat landscape.

Protecting the future of cybersecurity

"The rise of AI-powered social engineering represents one of the most urgent cybersecurity threats of our time," said Brian Long, CEO and co-founder of Adaptive Security. "Deepfake phone calls, AI-generated emails and SMS phishing are evolving rapidly. Attackers can now create AI personas of anyone, turning routine communications into sophisticated fraud attempts. Our platform is designed to protect companies at every stage of the attack cycle — from simulated AI attacks to employee training and automated risk mitigation. With this new investment from a16z, the OpenAI Startup Fund and other top-tier partners, we are scaling our technology to stay ahead of the next generation of cyber threats."

"Adaptive Security is solving one of the most urgent challenges in cybersecurity today: defending against AI-powered social engineering," said Zane Lackey, general partner, Andreessen Horowitz. "As threats grow more sophisticated, Adaptive's AI-native platform gives organizations the tools to proactively train employees, simulate real attacks, and respond in real time. This is a critical inflection point for new threats, and we're proud to back Brian, Andrew and the team as they build defenses for the AI era."

"AI is reshaping the cybersecurity threat landscape faster than most organizations can respond," said Ian Hathaway, partner at the OpenAI Startup Fund. "Adaptive is building exactly what the industry needs — an AI-native defense platform that evolves as fast as the attackers. We're proud to support them as they lead this critical shift."

A complete solution against AI-powered social engineering attacks

Adaptive Security provides next-generation AI designed to prevent, detect and mitigate AI-driven social engineering attacks:

- **AI deepfake persona attack simulations** test organizations by deploying realistic deepfake persona attacks across real-time voice phone calls, SMS and GenAI email. Failed simulations help security teams identify vulnerabilities while providing users with individualized training to prevent future breaches. Employees who fall for simulated attacks are automatically enrolled in tailored remediation training.
- **AI security training** educates employees on emerging and traditional security threats with hundreds of high-quality, mobile-friendly, expert-vetted training modules. In addition to security content, Adaptive also offers HR content such as compliance training. Employees consistently rate Adaptive Training 4.8 out of 5 stars.
- **GenAI content generation** enables the creation of new training modules in seconds, using any topic or existing source materials. GenAI content includes text, images and videos.
- **Real-time threat triage** allows employees to report suspected phishing attacks, which are automatically scanned and mitigated by Adaptive AI.

- **AI-driven risk scoring** provides real-time risk assessments at the individual, departmental and organizational levels. This enables security professionals to focus on the most at-risk areas and proactively strengthen defenses.

About Adaptive Security

Adaptive Security is the leading provider of AI-powered social engineering prevention solutions, specializing in protection against deepfake persona attacks, AI-driven phishing and multi-channel social engineering threats. By combining advanced AI simulations, real-time risk assessment and security training, Adaptive empowers organizations to proactively defend against emerging cyber threats.

For more information, visit www.adaptivesecurity.com.

Media Contact:

Joshua Thompson

josh@adaptivesecurity.com

Cell: 716-864-4429

Website: www.adaptivesecurity.com