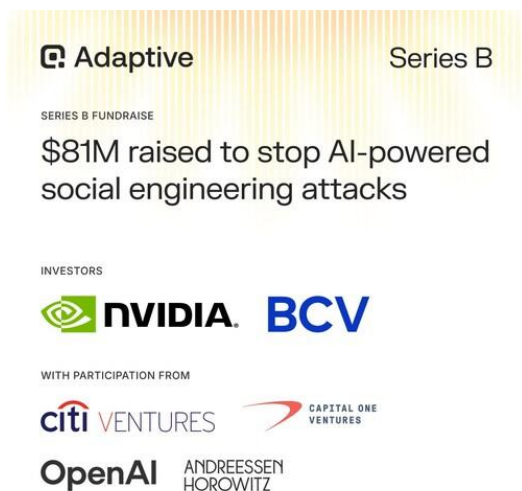


Adaptive Security Raises \$81 Million Series B to Stop AI-Powered Cyber Threats

NEW YORK, Dec. 16, 2025 /PRNewswire/ -- **Adaptive Security** today announced it has raised an \$81 million Series B funding round led by Bain Capital Ventures, with participation from NVentures (NVIDIA's venture capital arm), OpenAI Startup Fund, Andreessen Horowitz (a16z), Abstract Ventures, Capital One Ventures, and Citi Ventures. The investment is Adaptive's third financing announcement this year and brings the firm's total capital raised to \$146.5 million.

In April, the Company announced a \$43 million Series A led by OpenAI Startup Fund and Andreessen Horowitz, making it OpenAI's first and only cybersecurity investment. The OpenAI Startup Fund later led an additional \$12 million follow-on investment announced in September.



Adaptive's rapid fundraising activity reflects rising investor and customer concern over AI-powered cyber threats. In less than one year since its public launch in January 2025, Adaptive has grown to more than 500 enterprise customers and reports a world class NPS score of 94. Customers include PayPal, Xerox, Bose, the National Hockey League, the Professional Golfers' Association, Figma, Ramp, Vimeo, TaylorMade Golf, and Perplexity, among others.

AI Impersonation Threats Accelerate

Adaptive was founded by Brian Long and Andrew Jones after they saw AI-enabled impersonation move quickly from a niche risk to a practical problem for

companies, employees, and consumers. The two entrepreneurs, who previously founded and grew Attentive to \$500 million in annual revenue, started the company because legacy security training was not built for cutting-edge generative AI deception.

"Over the past year, we have watched AI impersonations evolve from experimental to everyday," said Brian Long, CEO and co-founder of Adaptive Security. "A few seconds of audio or a short video clip is now enough for anyone to generate a convincing clone. That shift forces organizations to prepare for scenarios where even familiar voices, faces, or messages can no longer be taken at face value."

Social engineering accounts for more than 95% of successful cyber breaches and traditionally came through email. In recent years, malicious activity over phone calls, text messages and video chat has surged. Deepfake incidents grew 17 times from 2023 to 2024, with more than 100,000 occurring in the U.S. alone. In 2025, Adaptive reported a rise in AI deepfake activity and said more than half of its customer discussions included reports of deepfake incidents. These incidents affect employees across all levels of an organization and increasingly affect consumers through cloned voices, fabricated videos and personalized scams.

Deepfake Phishing Simulations and AI Security Awareness

The company uses AI to simulate deepfake and impersonation scenarios across voice calls, text messages, video and email. These simulations identify where existing controls are likely to break down and provide individualized training based on employee responses. The platform also includes automated threat triage and AI-driven executive risk scoring to help organizations identify their most exposed teams and processes.

"Our task is to give organizations clarity in a landscape that is changing extremely quickly," Long said. "The threat is evolving in real time. Our responsibility is to move at least as fast."

Leading AI Companies and Investors Support Adaptive's Approach to Next-Gen Security

With support from NVIDIA, Adaptive is advancing efforts to secure AI systems and protect the people who work with them. OpenAI Startup Fund's continued participation reflects growing attention among leading AI researchers to the security and safety implications of generative models. Together, the investors point to a widening consensus that AI impersonation is becoming a mainstream risk for businesses and consumers.

"Brian and Andrew have been longtime members of the Bain Capital Ventures portfolio spanning TapCommerce, Attentive and now Adaptive, and we have deep conviction in their ability to build and scale category-defining products," said Enrique Salem, partner at Bain Capital Ventures. "The surge in AI-enabled threat vectors has elevated human-layer security to a board-level priority, and Adaptive is emerging as the platform organizations rely on to stay ahead of these threats. We are proud to support this team as they tackle one of the most important challenges facing businesses and consumers today."

About Adaptive Security

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

For more information, visit [**www.adaptivesecurity.com**](https://www.adaptivesecurity.com)

Media Contact:

[**media@adaptivesecurity.com**](mailto:media@adaptivesecurity.com)