Horizon3.ai Raises $100M to Cement Leadership in Autonomous Security

Wednesday 11 June, 2025

Related Sectors:

Computing & Telecoms ::

Related Keywords:

AI :: IT Security :: Software ::

Scan Me:

- **“The future of cybersecurity is AI vs. AI, and Horizon3.ai is leading the way,” said Snehal Antani, CEO and Co-Founder of Horizon3.ai.**
- **The new funding will be used to strengthen Horizon3.ai’s leadership in autonomous cybersecurity.**
- **Interview requests with Snehal Antani: Please contact team@euromarcom.com to arrange an interview.**

London, 11 June 2025 – Horizon3.ai, the company behind the NodeZero® Autonomous Security Platform, has announced a $100 million Series D funding round led by NEA, with participation from SignalFire, Craft Ventures and 9Yards Capital. As part of the investment, Lila Tretikov, Partner and Head of AI Strategy at NEA and former Deputy CTO of Microsoft, will join the Horizon3.ai Board of Directors.

NodeZero is a cloud-based platform that enables organisations and public institutions to launch internal attacks on their own IT infrastructure in order to assess their cyber resilience—known as penetration testing or pentesting. Thanks to its cloud-based model, costs remain low, making regular pentesting accessible even for mid-sized companies.

Snehal Antani: “Hacking with AI Is No Longer Science Fiction”

“Over the past four years, we’ve proven that using AI to hack companies isn’t science fiction—it’s real, and it’s delivering measurable results at scale. There are now over 3,000 organisations using NodeZero globally to conduct penetration tests. We’re sustaining 100%+ year-over-year ARR growth, and we are now Rule of 40-positive, which means we’re not just growing—we’re growing efficiently,” said Snehal Antani, CEO and Co-founder of Horizon3.ai. “This raise marks the next chapter in our mission to lead the Autonomous Security category.”

The Rule of 40 is a benchmark for software-as-a-service (SaaS) companies that balances growth and profitability. It states that the sum of annual recurring revenue (ARR) growth (in percent) and EBITDA margin (in percent) should be at least 40. A company is considered "Rule of 40 positive" when this sum is 40 or higher, indicating a healthy combination of growth and profitability.

“Security teams are tired of chasing CVEs, false positives, and compliance checkboxes. They want to find and fix what actually matters, verify it’s resolved, and go home early,” said Antani. “The hardest part of the job as a CIO is deciding what not to fix. The second hardest part is proving to the board that your security initiatives are meaningfully reducing risk. NodeZero plays a critical role in reducing your threat exposure over time.”

Targeting an $80B Total Addressable Market: Autonomous Security

The cybersecurity market is undergoing a generational shift. NodeZero successfully compromised a bank in 4 minutes with no humans required, far faster than the reaction time of the bank’s security team and their best-in-class tools. Similarly, adversaries are leveraging AI to exponentially increase the sophistication, complexity, speed and scale of attacks. The Horizon3.ai thesis is simple: the future of cyber will be algorithms fighting algorithms—at machine speed—with humans by exception. This requires a fundamental rebuild of every part of the cybersecurity stack. And to do so effectively, you need a deep understanding of how attackers operate—and an AI system that can use offensive insights to drive defensive improvements. Horizon3.ai is leading this shift.

“Horizon3.ai has already realised what others are just beginning to imagine. NodeZero is a fully autonomous security system operating in live production environments—executing real attacks, uncovering real risk and delivering real results,” said Antani.

Powered by reinforcement learning, graph reasoning, and AI, NodeZero doesn't simulate adversaries—it thinks and acts like one. Each cyber attack against production systems executed by NodeZero collects training data used to improve its algorithms, creating a compounding data advantage that no other platform can match. This is the foundation for the next era of cybersecurity, where AI doesn’t just find risk, but continuously improves defences. Horizon3.ai isn’t chasing the future—it’s building it.

Expanding the Partner Ecosystem and Driving Product Innovation

With this funding, Horizon3 is accelerating across three strategic fronts:

? **Scale through partners** – Doubling down on its partner ecosystem to meet growing demand across the Americas, EMEA, and APAC.

? **Product innovation** – Expanding into web application pentesting, vulnerability management, and precision defence, where NodeZero can remediate findings and tune defensive tools.

? **Winning the federal market** – Scaling its success with the Defence Industrial Base through the NSA's Continuous Autonomous Pentesting (CAPT) program, accelerating FedRAMP High usage, and expanding into Secret and Top Secret workloads to help secure the nation's most mission-critical systems.

What the Investors Are Saying

"What drew us to Horizon3.ai is the clarity of their mission and the speed at which they're executing it," said Aaron Jacobson, Partner at NEA. "They are defining a new security category—autonomous security—and are already the go-to solution for red and blue teams alike. We're thrilled to lead this round and support the company's next phase of growth."

"Snehal and the Horizon3.ai team are tackling one of the biggest problems in cybersecurity: automating both sides to ensure maximum defensibility against automated and AI-driven attacks," said Lila Tretikov, Partner and Head of AI Strategy at NEA. "Their customers love NodeZero, and the team has proven to operate with excellence at scale, which is why Horizon3.ai is transforming how security is done. I'm excited to join the board and help shape this next chapter."

The impact is immediate and measurable. In one recent pentest, NodeZero gained access to sensitive US aircraft carrier design data through a third-party supplier. No humans were involved in the pentest. The platform autonomously compromised the network, gained access to sensitive data, and then guided defenders on exactly what to fix to prevent a breach.

"My old boss used to say, 'don't tell me we're secure, show me, then show me again tomorrow, and again next week, because our environment is always changing and the enemy always has a vote,'" said Antani.

To learn more about NodeZero visit www.horizon3.ai.

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to simulate self-attacks on their IT infrastructure to assess their cyber resilience through penetration testing (pentesting). Thanks to its cloud model, the platform offers affordable, regular pentesting, making it accessible to mid-sized companies. Horizon3.ai continuously monitors the cybercrime landscape to ensure that newly discovered vulnerabilities are swiftly integrated into the cloud system. NodeZero not only identifies security flaws but also offers tailored recommendations for remediation. Through this platform, Horizon3.ai helps organisations meet rising regulatory demands for cyber resilience in Governance, Risk & Compliance (GRC), with guidelines recommending an internal self-attack at least once a week.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information: Horizon3.AI Europe GmbH, Prielmayerstrasse 3, 80335 Munich, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Tel. +49 611 973150, Web: www.euromarcom.de, E-Mail: team@euromarcom.de

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk