Horizon3.ai's NodeZero®, the World's Most Experienced AI Hacker, Drives 102% ARR Growth

Tuesday 24 March, 2026

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

ITSecurity :: AI ::

Scan Me:

Best-in-class sales and operational efficiency, with more than 5,200 organisations worldwide relying on NodeZero

London, 24 March 2026 – Horizon3.ai, the AI-native proactive security leader, today announced strong FY2026 growth, with annual recurring revenue (ARR) increasing 102% year over year. This momentum is driven by rapid enterprise and MSSP adoption, as organisations turn to NodeZero to identify and eliminate exploitable attack paths in production environments.

More than 5,200 organisations globally, from Fortune 10 enterprises to local school districts, hospitals, manufacturers, financial institutions, defence contractors, and government agencies, rely on NodeZero to continuously validate and harden their defences in production environments.

Key business and operational metrics include:

- ? 125% Net Dollar Retention, reflecting expansion from pentesting into broader exposure management use cases
- ? 94% Gross Dollar Retention, demonstrating strong customer retention and increasing testing frequency
- ? 32% of Q4 bookings originated by channel partners

Approximately 70% of customers are serviced through Managed Security Service Providers (MSSPs), one of the company's fastest-growing segments. MSSPs are using NodeZero to deliver continuous validation services while expanding into higher-value offerings such as remediation, threat hunting, SOC optimisation, and advisory services.

"MSSPs play a critical role, especially in international markets where local relationships and trust matter," said Snehal Antani, CEO and Co-Founder of Horizon3.ai. "They allow us to scale globally while enabling partners to build high-margin service offerings on top of NodeZero."

"Vulnerability prioritisation has never been more critical," Snehal continued. "AI is accelerating vulnerability research, and defenders are overwhelmed deciding what not to fix. Pentesting remains the most effective way to identify what is actually exploitable and focus remediation on what matters."

"Cybersecurity is currently vital, driven both by the rapid advancement of AI and a more unstable geopolitical landscape," Dan Bird MBE, Field Chief Technology Officer for EMEA at Horizon3.ai added. "Organisations are right to take every possible step to protect their IT environments and critical business services. But the key is focusing on what can actually be exploited, and where teams need to act first."

NodeZero: Built Through Real-World Execution

NodeZero stands apart as the world's most experienced AI hacker, having autonomously executed more than 225,000 production-safe pentests across enterprise environments. These are not simulated or lab-based exercises, but real-world assessments across hospitals, manufacturing environments, financial services networks, and critical infrastructure.

NodeZero continuously chains multi-domain attack paths across web applications, Active Directory, cloud environments, and identity systems, exposing exploitable weaknesses that traditional tools and manual pentesting approaches miss.

"NodeZero has operated at a scale and in environments that others simply have not," Snehal added. "You earn the right to operate in production by delivering results safely and consistently. That experience compounds over time and creates a structural advantage."

Operating in a Rapidly Evolving Threat Environment

This growth comes as organisations face escalating real-world threats, including recent Horizon3.ai guidance on Iranian cyber activity targeting critical infrastructure sectors. NodeZero enables organisations across the Defense Industrial Base, financial services, utilities, telecommunications, and

manufacturing sectors to identify exploitable weaknesses in production environments and disrupt attack paths before nation-state and other adversaries can act.

“The future isn’t humans reacting to AI-driven attacks. It’s AI fighting AI, with humans directing by exception,” said Antani. “We built the most experienced AI hacker first, and we are now using that experience to help organisations defend themselves at machine speed.”

About Horizon3.ai

Horizon3.ai’s AI-native Proactive Security Platform is trusted by four of the Fortune 10, the world’s largest banks, leading global pharmaceutical and semiconductor manufacturers, critical infrastructure operators worldwide, and the U.S. Defense Industrial Base. It enables organisations to proactively hack, fix, verify, and repeat testing on demand, continuously strengthening defences and improving cyber resilience over time.

Recognized as the fastest-growing cybersecurity company in America (Inc 5000 and Deloitte Fast 500), Horizon3.ai was founded by former U.S. Special Operations members and industry experts, and is headquartered in San Francisco.

Follow Horizon3.ai
on LinkedIn
and X.

Further information: Press contact: Stephen Gates - press@horizon3.ai, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Web: www.euromarcom.de, Email: team@euromarcom.com

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