25.02.2025 – 15:15 Uhr

Horizon3.ai Achieves 101% YoY Revenue Increase and Sets New Record in Q4 Performance

Horizon3.ai Achieves 101% YoY Revenue Increase and Sets New Record in Q4 Performance

London, 25 February 2025 – Horizon3.ai, a global leader in autonomous security solutions, continues to set new industry benchmarks, achieving 101% year-over-year revenue growth and exceeding 150% of Q4 pipeline targets in FY25. With demand accelerating for real-world, offense-driven security, organisations are rapidly adopting NodeZero® to continuously find, fix, and verify exploitable weaknesses—before attackers can.

This record-breaking momentum is further validated by 100,000+ autonomous pentests completed to date, solidifying NodeZero as the industry's most scalable security validation platform.

Partner-Driven Growth & Market Expansion

Horizon3.ai's partner-first strategy is fuelling its rapid growth by leveraging an extensive partner network to make offense-driven security accessible to organisations of all sizes. This approach is accelerating adoption across industries faster than ever before and solidifying Horizon3.ai's leadership in autonomous security solutions.

- **111% YoY Growth in Customer Expansion Revenue** – Demonstrating high retention, increasing adoption, and expanding use cases, solidifying market leadership.
- **72% YoY Growth in Q4 Performance** – Driven by strong demand and strategic investment in NodeZero's capabilities, underscoring its competitive differentiation.
- **106% YoY Growth in Partner-Sourced Pipeline** – Proving the effectiveness of channel partners and MSSPs in driving market penetration and customer acquisition.
- **80% of Horizon3.ai's 3,000 Customers Fully Serviced by MSSPs** – Reflecting the strength and scale of its partner ecosystem in delivering autonomous security solutions.
- **Industry-Leading NPS of 88** – Highlighting exceptional customer satisfaction and trust, reinforcing Horizon3.ai's commitment to customer-centric innovation.

Scaling Cyber Resilience Across Industries

As cyber threats escalate, organisations across enterprise, government, and critical infrastructure are turning to Horizon3.ai for proactive security validation. By working with the NSA Cybersecurity Collaboration Center, Horizon3.ai is expanding the reach of autonomous security validation, ensuring DoD suppliers can proactively harden their defences.

As Bailey Bickley, Chief DIB Defense at the NSA Cybersecurity Collaboration Center, recently posted on her LinkedIn account:

"Pen testing is a really valuable tool for network defenders, but can be costly and time consuming, making it challenging for some small businesses to take advantage of.

The CAPT service, offered by the NSA Cybersecurity Collaboration Center through Horizon3.ai, is designed to make pen testing easy and accessible for critical DoD suppliers. Our goal is to rapidly scale cybersecurity benefits across the Defense Industrial Base and protect sensitive DoD information that sits on privately owned and managed networks from IP theft by our adversaries."

Through partnerships like these, Horizon3.ai continues to drive the industry shift from compliance-based security to offense-driven resilience. Traditional pentesting firms still control a sizeable portion of the market, yet their outdated, manual approaches can't match NodeZero's scalable, automated, and repeatable security validation.

Customer Validation: The Impact of Autonomous Pentesting

"Our customers are proving every day that offense is the best defence," said Snehal Antani, CEO & Co-Founder of Horizon3.ai. "By continuously attacking themselves with NodeZero, they're ensuring that security teams aren't just checking boxes—they're closing real security gaps before attackers can exploit them."

This impact is echoed by Rick MacKirdy, CEO of Modus Advanced, Inc.:

"We pride ourselves on maintaining a strong security posture, which is why we partner with NodeZero for pentesting. Within hours of running NodeZero internal pentesting, our MSP was able to quickly review the findings and remediate the weaknesses. As a member of DIB, it's my personal responsibility to help protect our nation's secrets. With Horizon3.ai and NodeZero verifying our system security at a regular cadence, I'm confident we're well positioned to handle the critical data ultimately supporting our troops."

Horizon3.ai: Defining the Future of Cybersecurity

As Horizon3.ai accelerates toward market dominance, the company remains focused on scaling adoption, expanding partnerships, and enabling organisations to outpace attackers. The demand for offense-driven security isn't just growing—it's becoming the new standard.

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to run production safe 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 autonomous pentesting, making it accessible from small to mid-sized, to large enterprises. 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.

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

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

- - - -