

27.08.2024 – 09:00 Uhr

Horizon3.ai Launches NodeZero™ Cloud Pentesting to Transform Cloud Security

Horizon3.ai Launches NodeZero™ Cloud Pentesting to Transform Cloud Security

Advanced Solution Identifies Complex Vulnerabilities Across AWS and Azure Environments, Ensuring Comprehensive Cloud Security for Organisations of All Sizes

London, 27 August 2024 – Horizon3.ai, a leading provider of autonomous security solutions, today announced the launch of NodeZero™ Cloud Pentesting. This innovative solution helps organisations identify and resolve complex exploitable vulnerabilities and hidden attack paths in their cloud environments. Horizon3.ai offers the most comprehensive autonomous penetration testing solution, enabling both public and private sectors to thoroughly assess and secure their cloud environments across AWS and Azure.

Dennis Weyel, International Technical Director responsible for Europe at Horizon3.ai, explains: “This is a dream come true for many IT managers: pentesting in the cloud with Horizon3.ai. We know that many users have been waiting for this functionality for some time. So we are prepared for the onslaught.”

As organisations expand their digital presence in the cloud, managing security and addressing the unique requirements of each cloud environment becomes increasingly complex for already overburdened security teams. Concurrently, attackers are intensifying their efforts with more frequent and sophisticated attacks. Many organisations struggle to identify and remediate vulnerabilities in both cloud environments and on-premises systems.

NodeZero Cloud Pentesting offers unparalleled testing capabilities for both cloud and hybrid environments. It identifies and chains together exploitable vulnerabilities, security weaknesses, and software misconfigurations, ensuring continuous validation of security programs and compliance initiatives. The solution can also pivot to on-premises networks, to emulate the true behaviour of an attacker. This allows organisations to prioritise the remediation of complex attack paths that could be exploited by attackers, significantly reducing cyber risk.

“To empower organisations to better secure their entire digital ecosystem, NodeZero Cloud Pentesting features the most advanced cloud-focused attack content ever developed,” states Snehal Antani, CEO and Co-founder of Horizon3.ai. “By emphasising identity as a cornerstone of cloud security, NodeZero provides deeper insights into exploitable risks in AWS and Azure environments than any other penetration testing solution available today. Organisations can schedule and launch on-premises and cloud-focused penetration tests at their convenience and we encourage them to compare our solution against any other cyber risk assessment approach they currently use.”

Organisations can comprehensively assess their cloud and hybrid environments using the advanced capabilities of NodeZero by conducting both internal and external pentests, along with operations such as AD Password Audits and Phishing Impact tests. The solution uncovers previously unknown cloud security weaknesses, highlights overexposed or misconfigured assets, and identifies exploitable identity and access management (IAM) policies that could lead to privilege escalation. This comprehensive testing ensures effective defence in depth, reduces potential attack blast radiuses, and helps organisations mitigate the risks of insider threats and credential-based attacks.

NodeZero Cloud Pentesting Key Features

Internal Pentests: NodeZero’s internal pentests provide a holistic view of how attackers can chain together exploitable vulnerabilities across the entire digital infrastructure, identifying complex attack paths and pivoting between on-premises and cloud environments.

External Pentests: Similar to the internal tests but launched from Horizon3.ai’s cloud infrastructure, this pentest uncovers externally exposed weaknesses and validates the security of public-facing systems.

AWS Pentests: This pentest utilises AWS CloudFormation to gain a privileged perspective, identifying exploitable vulnerabilities, weak controls, insecure IAM policies, and overexposed assets.

Azure Entra ID Pentests: This pentest targets Microsoft Entra ID from a privileged perspective, testing susceptibility to Azure-native attacks, and validating the security of applications and services using Microsoft Entra identities.

Designed by Horizon3.ai’s world-renowned attack team and certified offensive security engineers, NodeZero Cloud Pentesting includes safe and effective purpose-built exploits, advanced remote access tools, and an array of attacks designed to leverage lateral movement and privilege escalation. With over 65,000 autonomous penetration tests performed and tens of thousands of on-premises and cloud terrains fully mapped, NodeZero significantly enhances security and reduces risk for organisations of all sizes. With NodeZero’s find, fix, and verify capabilities, no other pentesting solution matches the power, efficacy, and effectiveness that NodeZero delivers.

To learn more about NodeZero Cloud Pentesting please visit [here](#).

These two videos explain the functions of NodeZero in more detail.

This demo shows how quick and easy it is to set up an internal, external, and cloud test with NodeZero.

<https://youtu.be/En4prKyrggY?feature=shared>

This demo shows the NodeZero analyses that a user would see after completing a cloud test.

<https://youtu.be/5FCsq1thmhM?feature=shared>

About Horizon3.ai: The NodeZero™ platform empowers organisations to continuously find, fix, and verify exploitable attack surfaces. It is the flagship product of Horizon3.ai, founded in 2019 by former industry and U.S. National Security veterans. Our mission is to help organisations see their networks through the eyes of the attacker and proactively fix problems that truly matter, improve the effectiveness of their security initiatives, and ensure that they are prepared to respond to real cyberattacks. Follow Us: Horizon3.ai: [LinkedIn](#) and on [X](#), formerly known as Twitter.

Trademark notice : NodeZero is a trademark of Horizon3.ai

Further information: Horizon3.AI Europe GmbH, Sebastian-Kneipp-Str. 41, 60439 Frankfurt am Main, Web: www.horizon3.ai

Media Contact: euromarcom public relations GmbH, Web: www.euromarcom.de, Email: team@euromarcom.de

Diese Meldung kann unter <https://www.presseportal.de/en/pm/163532/5851498> abgerufen werden.