Sec4good

HORIZON3.ai
~~TRUST~~ BUT VERIFY

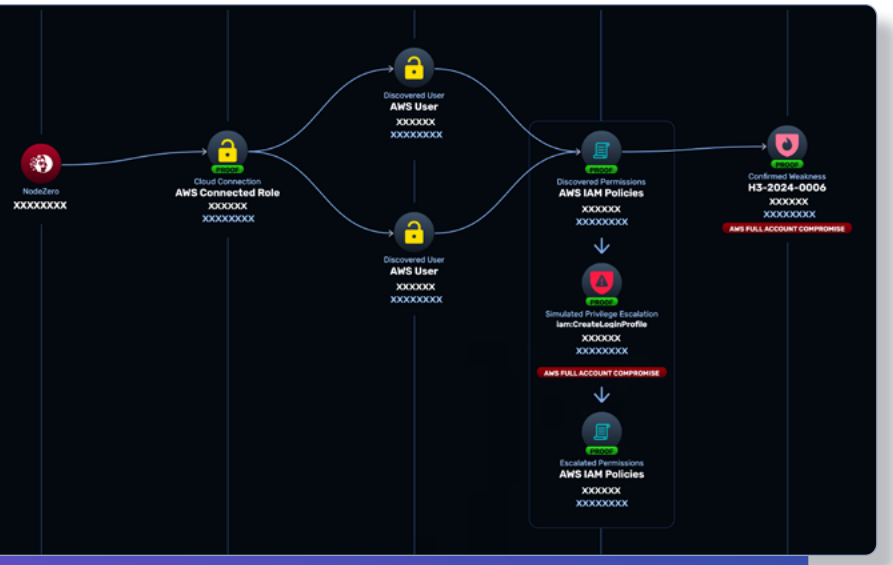
NodeZero

Cloud Pentesting

Unparalleled testing capabilities for cloud and hybrid environments

The NodeZero™ platform delivers autonomous pentests from various perspectives for organizations with cloud or hybrid cloud infrastructures. Taking a comprehensive approach ensures consistent security policy validation and risk assessment across your entire cloud stack.

You can deploy NodeZero from both an internal and external attackers' perspective to rigorously test cloud security controls in the context of your entire digital infrastructure or specifically target identity-based attack surfaces in Amazon Web Services (AWS) or Microsoft Azure Entra ID.



Here NodeZero uses a privileged perspective to delve deeper into an AWS environment.

Internal Pentest: NodeZero's most comprehensive autonomous pentest provides a holistic view of how attackers can chain vulnerabilities across the entire digital infrastructure, identifying complex attack paths and pivoting between on-prem and cloud environments.

External Pentest: Similar to the internal test, but launched from Horizon3.ai's infrastructure to validate the security of public-facing systems.

AWS Pentest: Utilizes AWS CloudFormation to gain a privileged perspective, identifying exploitable vulnerabilities, weak controls, insecure IAM policies, and overexposed assets.

Azure Entra ID Pentest: Targets Azure IAM security (Entra ID) from a privileged perspective, testing susceptibility to Azure-native attacks, and validating the security of applications and services using Microsoft Entra identities.

Use NodeZero to routinely test your cloud security controls from different perspectives:

1 Internal and External Testing:
NodeZero deploys tests either internally or externally to see how an attacker might chain together vulnerabilities and misconfigurations across different environments. This validates the effectiveness of security stacks, highlighting connections between seemingly unrelated assets to escalate privileges and uncover hidden attack paths.

2 Privileged Perspective Testing:
Focusing on specific cloud providers, NodeZero uses a privileged perspective to delve deeper into AWS or Azure environments. This approach surfaces additional vulnerabilities, highlights overexposed or misconfigured assets, and pinpoints abusable IAM policies for privilege escalation. These tests validate defense in depth, reduce potential blast radiuses, and combat insider threats and credentialed attacks.

Here NodeZero uses its privileged perspective to prove that a complex Azure-native attack combined with weak controls allows it to escalate to Entra ID Global Admin.

These capabilities are delivered on the NodeZero architecture designed for scale, speed, and comprehensive coverage of cloud and on-prem environments. NodeZero offers many features that let you replace labor-intensive security activities with its proactive and autonomous approach, from 1-click verify, to your ability to orchestrate concurrent and large-scale pentests in a multi-tenant environment.