HORIZON3.ai
TRUST BUT VERIFY

GALIX

What We Do:

The NodeZero™ platform, delivered in collaboration between Galix and Horizon3, empowers your organization to continuously discover, remediate, and validate your exploitable attack surface across your entire digital infrastructure. Together, we help reduce your security risk by autonomously identifying real-world exploitable weaknesses that extend beyond known CVEs and patchable vulnerabilities. This includes risks such as easily compromised credentials, exposed sensitive data, misconfigurations, ineffective security controls, and weak security policies—ensuring a more comprehensive and proactive approach to cybersecurity.

Autonomously Chains Attack Vectors

- NodeZero manoeuvres through your cloud and on-premises environments, chaining weaknesses together just as an attacker would and then safely exploits them.

Provides Path, Proof, and Impact

- NodeZero shows you the actual attack paths in your environment for every weakness it discovers, showing the proof of where it was able to get past your defences. Weaknesses are ranked based on their impact on your organization.

Breadth of Coverage

- NodeZero offers a growing list of operations to help you assess your onprem infrastructure, external attack surface, cloud infrastructure, identity and access management infrastructure, data infrastructure, blast radius from phished credentials, and more.

Prioritises and Streamlines Remediation

- NodeZero shows you what weaknesses are truly exploitable in your network, and which have the most critical impacts so you can prioritize your work. It delivers detailed remediation guidance, including fixes for systemic issues that will eliminate many weaknesses. Use 1-click verify to confirm your fixes are effective.

Pre-emptive Threat Intelligence

- Alerts from the Horizon3.ai Attack Team about emerging threats that are proven to impact your organization enable you to mobilize your defenses in the NodeZero Rapid Response center.

Early Threat Detection

- Early Threat Detection: NodeZero TripwiresTM enables you to rapidly respond to active threats in highrisk areas of your environment. NodeZero automatically deploys decoys along proven attack paths. You're alerted when malicious activity is detected.

Continuous, Unlimited, and Orchestrated Deployments

- Continuously improve your effectiveness. Include a very broad scope in a single test, orchestrate 100+ concurrent tests, and simultaneously test your enterprise from different attacker perspectives.

Requires No Agents or Special Hardware

- NodeZero is a true self-service SaaS offering that is safe to run in production. No hardware or software to maintain; no persistent or credentialed agents required.

HORIZON3.ai
TRUST BUT VERIFY

GALIX

Capability Statement

Value of the NodeZero Platform

1. Continuous Vulnerability Detection: Deploy NodeZero across your infrastructure to continuously monitor and identify exploitable vulnerabilities. Upon detection, NodeZero provides immediate notification and detailed reports, prompting your security team to begin remediation immediately. This workflow helps reduce your attack surface and the time-to-remediate.

2. Efficient Remediation Verification: After your team applies a fix to address a detected vulnerability, use 1 click verify to retest the area and verify the effectiveness of the remediation. This quick verification process can reduce the likelihood of leaving unresolved or insufficiently addressed vulnerabilities.

3. Prioritization of Vulnerabilities: Use NodeZero to rank identified vulnerabilities based on severity, exploitability, and potential impact on your business. This can guide your team in prioritizing remediation efforts, ensuring that the most critical vulnerabilities are addressed first.

4. Pre-emptively Respond to Emerging Threats: Use the NodeZero Rapid Response center to streamline your response to emerging threats. Receive real-time alerts when the Attack Team identifies a nascent threat that impacts your organization. Monitor the status of the vulnerability and learn how to mitigate or remediate as appropriate. Gain access to early exploits to quickly assess your assets and prioritize your activities.

5. Early Threat Detection: Routinely use NodeZero TripwiresTM with your NodeZero pentests. During testing, NodeZero automatically drops appropriate tripwires when it exploits a vulnerability, adding protection before the pentest event is complete. NodeZero alerts you when there are attempts to run tripwire processes or use tripwire credentials.

6. Continuously Measure and Report on Overall Security Posture: NodeZero Insights provides an uninterrupted, comprehensive view of your organization's security posture as it evolves. This includes tracking trends in weaknesses, open attack paths, key performance indicators (like mean-timeto- remediation), and the results of ongoing pentests across all potential attack vectors. With this level of insight, security leaders can continually evaluate the effectiveness of their remediation efforts, while company executives can effectively communicate the business implications of their exploitable attack surface to the board and other key stakeholders.

7. Validate the Effectiveness of your Cloud IAM policies: Identify cloud-based IAM weaknesses by launching a pentest from a privileged perspective for added visibility. NodeZero will surface vulnerabilities, overexposed or misconfigured public assets, and highlight IAM rules that can be abused for privilege escalation.

8. Cross-Platform Daisy Chaining: NodeZero identifies exploitable vulnerabilities that expose credentials, intelligence, and additional visibility, then chains them together to show how attackers could use these to pivot across on-prem, cloud, or hybrid environments. This provides a true assessment of the security risks from interconnectivity and availability of assets.

9. Understand a Credential's Blast Radius: Use the Phishing Impact test to understand the blast radius of phished credentials. NodeZero will attempt to escalate privileges, gain lateral movement within the network, and access sensitive data.

10. Verify EDR and SIEM Effectiveness: After deploying a NodeZero pentest, monitor the alerts and responses from your EDR and SIEM systems. If these tools are detecting and responding to NodeZero effectively, they are functioning as expected. If not, it indicates tuning or upgrades are warranted.