HORIZON3.ai

~~TRUST BUT~~ VERIFY

NodeZero®

Offensive Security Platform

Cybersecurity From the Attacker's Perspective

Security leaders don't need to find vulnerabilities, they need to prove organizational resilience. The NodeZero Offensive Security Platform reduces risk by validating what attackers can actually exploit. It identifies weaknesses, prioritizes what matters most, provides clear remediation guidance, and verifies that fixes work to continuously fortify your defenses over time.

Uncover blind spots that go beyond known CVEs: compromised credentials, exposed data, misconfigurations, weak controls, and risky policies. NodeZero moves through your network as an attacker would, safely chaining weaknesses into real attack paths.

Continuous, autonomous pentesting validates security posture, prioritizes weaknesses, and gives teams clear proof of potential business impact.

See What Attackers See

NodeZero provides full visibility into every action it takes. Tests explain the proof and impact of each weakness with reports that meet internal and external audit requirements.

Reports include an executive summary, detailed pentest results, fix action plans, and segmentation analysis. Each report provides full visibility into exploit chains, compromised credentials, affected assets, and verified remediations — giving you measurable proof of progress and audit-ready evidence of risk reduction.

Test Across:

- On-premises and virtual infrastructure
- Cloud and hybrid environments — including AWS and Azure
- Identity and access management — including Active Directory, Azure AD, and IAM configurations
- Kubernetes and containerized environments
- Data infrastructure — databases, data stores, and data services
- External, public-facing assets

NodeZero helps you understand the weaknesses that lead to critical impacts, so you know exactly what to fix in order to disrupt the kill chain.

Core Pentesting Capabilities

Internal Pentesting
Reveal and prioritize real internal risks through production safe attacker emulation.

External Pentesting
Assess perimeter resilience directly from Horizon3.ai's cloud with no setup required.

Rapid Response & N-Day Testing
Shrink the window of exposure to high-profile vulnerabilities to hours, providing mitigation before exploits hit the wild.

Phishing Impact Test
Reduce phishing risk and measure the impact of stolen credentials on sensitive systems and data.

Cloud Pentesting
Identify IAM weaknesses and privilege escalation paths that expose critical cloud assets.

AD Password Audit
Reduce credential-based compromise and continuously validate password strength and policy effectiveness.

NodeZero Tripwires™ and AD Tripwires
Reduce attacker dwell time, deploy decoy files and credentials along attack paths. Trigger immediate alerts and speed incident response.

NodeZero Insights™
Consolidate pentest findings into actionable intelligence, helping teams prioritize fixes, track progress, and communicate risk in business terms.

Expanded Capabilities

NodeZero's Offensive Security Platform extends Risk Based Vulnerability Management (RBVM) with advanced capabilities bridging attacker verified offensive insights and defensive priorities:

High-Value Targeting (HVT): Autonomously identify and test access to crown-jewel accounts and systems without manual tuning.

Advanced Data Pilfering (ADP): Find and validate sensitive data attackers could access, showing what can be stolen and the business impact.

Threat Actor Intelligence (TAI): Align risk to real threats, map discovered attack paths to known adversary tactics, techniques, and procedures.

Vulnerability Risk Intelligence (VRI): Enrich scanner data into attacker-validated results that expose what's exploitable and what can be deprioritized.

Threat Informed Perspectives (TIP): Organize targeted assessments by business goals and attacker perspectives evolving pentesting into a measurable, continuous program.

Endpoint Security Effectiveness (ESE): Ensure endpoint defenses are tuned for your environment, validate EDR/XDR tools detect and stop real attacker behaviors in production.

Vulnerability Management Hub (VMH): Integrate directly with ticketing solutions, and track remediation progress to surface proven exploitable weaknesses.

NodeZero MCP Server: Turn natural-language into action to automate remediation and retests while your AI-enabled tools do the work.

Outcome: Stronger Defense, Less Exploitable Risk

NodeZero empowers security and IT teams to:

- Reduce noise and focus on real, exploitable risks
- Validate and prove mitigations and remediations work
- Track progress with measurable results
- Strengthen defenses through attacker-perspective validation

The NodeZero Offensive Security Platform turns offense into the best defense — identifying weaknesses, prioritizing what matters most, providing clear remediation guidance, and verifying fixes work, delivering confidence in your resilience.

 @Horizon3ai www.horizon3.ai