HORIZON3.ai
~~TRUST BUT~~ VERIFY

FedRAMP

PLATFORM ONE

NodeZero® Offensive Security Platform

For Practitioners and Defenders

When attackers move fast, your response has to move faster. You don't have time to fix what doesn't matter or wonder whether your fix worked. NodeZero gives you the proof you need, not promises. It continuously exposes real attack paths, validates your defenses, and confirms that your fixes actually worked.

Why It Matters

The fight is asymmetric. Adversaries have automation, scale, and patience, and often, your teams don't. You need to know what's exploitable, what's fixed, and what's still exposed. NodeZero helps you stay ahead by performing real attacks safely, chaining misconfigurations, credentials, and policy gaps to show how an adversary would move through your environment.

You can't defend what you don't validate.

NodeZero gives you actionable proof of where you're exposed and how to close the gap fast.

Stay Ahead of the Threat

NodeZero helps you detect, validate, and respond faster, turning findings into operational advantage.

Actionable Outcomes:

- Eliminate guesswork with proof of exploitation.
- Validate controls and verify remediation instantly.
- Detect lateral movement during and after testing with NodeZero Tripwires™.
- Test for newly weaponized threats using Rapid Response.

Built for Practitioners Who Live in the Fight

Continuous Autonomous Pentesting

Launch your first pentest in minutes. No agents, no consultants, no training curve.

Results arrive in hours, prioritized by exploitability with step-by-step fix guidance.

Risk-Based Vulnerability Management (RBVM)

NodeZero focuses your efforts on what's actually exploitable.

Track MTTR, MTTM, and ROR to see real improvement over time.

FixOps in Action

Close the loop between finding and fixing.

With one-click retesting, NodeZero verifies that mitigations worked and that nothing new broke in the process.

Adversary Emulation

NodeZero behaves like a real attacker, dynamically chaining weaknesses to reveal complete attack paths across internal, external, cloud, and Kubernetes environments.

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.

NodeZero Federal™

NodeZero Federal provides a FedRAMP® High authorized deployment of the NodeZero Offensive Security Platform.

Current Capabilities Include: Internal Pentesting, Phishing Impact Testing, Network Segmentation Testing, Insider Threat Testing, NodeZero Insights, VMH, HVT, ADP, and ESE.

External Pentesting is not currently available but will be launched for GA by 1 FEB 2026 upon authorization by FedRAMP PMO.

Hash Cracking will be available before 20 DEC 2025.

Prove the Fix

1-Click Verification
Re-test exactly where a fix was applied and instantly confirm it's resolved.

Continuous Validation
Run recurring tests to stay ahead of misconfigurations and regressions.

Evidence-Based Confidence
Each result includes proof of exploitation, remediation guidance, and audit-ready reports that show measurable improvement.

NodeZero turns security operations into proof of resilience.

Find what matters. Fix it fast. Prove it worked.