HORIZON3

FedRAMP

PLATFORM ONE

NodeZero® Proactive Security Platform

For Mission and Program Leaders

Mission success depends on uninterrupted operations, and adversaries are targeting that foundation. They're no longer probing for weaknesses; they're executing, using automation and AI to move faster than traditional defenses. NodeZero gives leaders the power to continuously validate readiness, prove resilience, and maintain mission continuity using the same playbook adversaries rely on.

Why It Matters

Legacy security assessments and annual compliance reviews were built for paperwork, not resilience. Adversaries chain misconfigurations, credentials, and policy gaps to achieve persistence and disruption. Leaders need a way to see what attackers see and prove that defenses can stop them.

Readiness must be measurable.

NodeZero safely performs readiness assessments to expose exploitable attack paths, validate controls, and prove resilience across the organization.

Prove Mission Readiness

NodeZero gives leaders defensible insight into how systems perform under real attack conditions, showing not just where gaps exist but how they affect mission continuity.

Actionable Intelligence:

- → See how attackers would pivot through your environment and what assets they'd target.
- → Identify systemic weaknesses where one fix mitigates multiple risks.
- → Use verified outcomes to brief leadership, auditors, and interagency partners with confidence.

Command-Level Validation

Continuous Autonomous Pentesting

NodeZero uses attacker TTPs to move through internal, external, cloud, and Kubernetes environments, revealing the true paths to compromise before adversaries do.

Risk Based Exposure Management (RBEM)

Stop managing vulnerabilities by volume. NodeZero identifies which weaknesses are exploitable, quantifies their mission impact, and tracks progress using MTTR, MTTM, and ROR.

FixOps for Operational Readiness

Bridge the gap between security and IT. NodeZero verifies that remediations work through instant retesting, turning response into measurable, repeatable progress.

Aligned to Federal Frameworks

NodeZero supports and accelerates alignment with FISMA, NIST 800- 53, OMB Zero Trust, CDM, and CORA (CCRI), producing evidence of operational assurance, not just compliance.

Expanded Capabilities

NodeZero's Offensive Security Platform extends Risk Based Exposure Management (RBEM) 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 Prioritization (VP):
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, External Pentesting, Phishing Impact Testing, Network Segmentation Testing, Insider Threat Testing, NodeZero Insights, VMH, HVT, ADP, and ESE.

Operational Superiority, On Demand

Find Attack Paths Before Adversaries Do
Launch autonomous tests in minutes without disruption or dependency on external consultants.

Anticipate Lateral Movement and Mission Risk
See how real attackers would chain weaknesses, escalate privileges, and threaten continuity.

Understand the Impact
NodeZero shows how gaps translate into data loss, domain control, or operational disruption.

Prioritize Fixes That Matter
Focus on the most critical weaknesses and accelerate time to mitigation.

Validate and Report with Confidence
Run targeted retests instantly and report verified improvements to stakeholders and oversight bodies with reports that show measurable improvement.

NodeZero® *transforms* compliance-driven testing into evidence of readiness.

Prove resilience, outpace the adversary, and command the risk before it commands you.