HORIZON3.ai

NodeZero Federal™

MISSION PROVEN SECURITY

FedRAMP® High Authorized

Offensive cybersecurity—now cleared for the most sensitive federal missions.

NodeZero Federal™ is the FedRAMP High Authorized version of Horizon3.ai's proven NodeZero® Offensive Security Platform. Purpose-built for high-security federal use, it enables production-safe, autonomous penetration testing at scale—continuously, safely, and without disrupting operations.

In a time when adversaries don't wait, neither should your defenses. NodeZero Federal replaces guesswork with proof—delivering real, exploitable findings and rapid retest validation so agencies can move from compliance to continuous readiness.

Proven Through National Security Missions

NodeZero powers the NSA's Continuous Autonomous Penetration Testing (CAPT) program, helping over 500 DIB participants stay ahead of evolving threats. This same battle-tested capability is now available to civilian and defense agencies.

CAPT Impact Metrics (as of May 2025):

Metric	Count	Metric	Count
Participants	500+	Pentests Conducted (≥1 host)	6,000+
Endpoints Tested	730,000+	Total Weaknesses / Vuln Paths	229,000+
Critical Weaknesses Exploited	17,000+	Critical Weaknesses Mitigated	5,000+
High Weaknesses Exploited	10,000+	High Weaknesses Mitigated	5,000+
Medium Weaknesses Exploited	8,000+	Medium Weaknesses Mitigated	4,900+
Low Weaknesses Exploited	36,000+	Low Weaknesses Mitigated	11,000+
Total NodeZero Pentest Hours	**64,000**		

CAPT Program Manual Pentest Hours Avoided	
Total NodeZero Pentest Hours Performed	64,000
Number of Hours Required if Performed by Human Pentesters (x12)	768,000
Average Cost Per Hour for Human Pentesters	$200
Total Cost Avoidance	**$153,600,000**

Note: NodeZero Federal™ brings nearly the same capability to federal civilian and defense agencies—cleared for high-security use through its FedRAMP High Authorization.

Why Federal Agencies Choose NodeZero Federal

Always-On Readiness, Not Annual Snapshots:
Legacy scans and annual security assessments can't keep up with today's adversaries.

- Identifies chained attack paths that cross trust boundaries
- Prioritizes only what is actually exploitable
- Validates fixes instantly with one-click retesting
- Produces audit-ready results aligned to federal frameworks

FedRAMP High Authorized: Cleared for use in sensitive federal environments under the FedRAMP High baseline. Delivered as a secure SaaS offering with enforced SSO.

Powered by NodeZero® Offensive Security Platform: Built on the same platform trusted across 150,000+ autonomous pentests in commercial, DIB, and federal systems—at scale.

Operational Proof of Resilience

NodeZero Federal proves how adversaries could compromise your systems. It safely chains together easily compromised credentials, misconfigurations, poor security controls, and weak policies and emulates real-world attacks in your live environment. No agents. No integrations. No assumptions.

Instead of theory, it delivers proof of exploitability—enabling faster fixes, reduced alert fatigue, and a measurable improvement in operational resilience.

From Attack Paths to Actionable Fixes

NodeZero Federal doesn't just identify risk—it shows every exploitable attack path and how adversaries could exploit systems from start to finish, so security teams can act with clarity.

For example:

NodeZero may uncover a misconfigured file share that exposes a private SSH key. That key grants access to a production endpoint, which is then leveraged through cached credentials and misconfigurations to achieve domain-wide compromise.

Or NodeZero might find a weak service account password reused across systems. With that foothold, NodeZero accesses shared drives, uncovers additional secrets, and moves laterally into a sensitive enclave.

Every NodeZero finding is backed by step-by-step remediation guidance and defensible evidence with proof of exploitation, so you know what to fix, why it matters, and how to verify your fix worked.

Mission Outcomes, Not Checklists

Whether validating Zero Trust segmentation, auditing Active Directory hygiene, or testing insider threat scenarios, NodeZero Federal is designed for impact, not checkbox compliance.

It enables:

- Readiness exercises that emulate real attacker TTPs
- Risk assessments that prove what's exploitable across environments
- Fix validation that lets you close tickets with confidence

This isn't snapshot testing—it's continuous operational assurance, delivered on your terms.

Ready for Deployment

See the Service Description here.

Download the Package Request Form here.

Enter this information into the Access Request Form - Name of Package Requested:
Federal High Impact Virtualized Environment

Enter this information into the Access Request Form - Package ID: **FR1802451335**