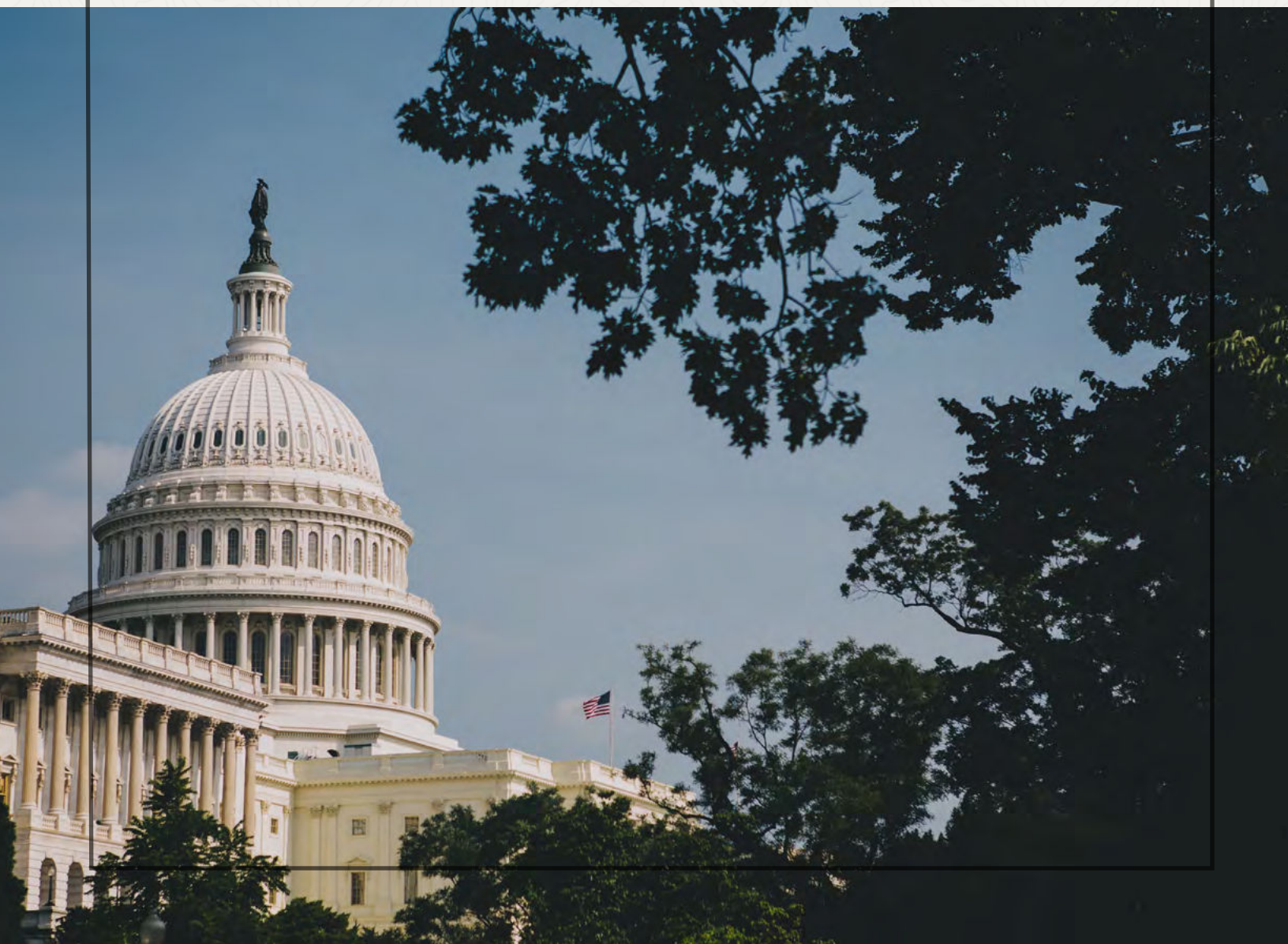
HORIZON3.ai

WHITE PAPER

NODEZERO FEDERAL™ – MISSION PROVEN SECURITY

FEDRAMP® HIGH AUTHORIZED



THE MISSION DOESN'T PAUSE FOR CYBER THREATS. YOUR DEFENSES SHOULDN'T EITHER.

Every system operated by your agency supports functions that directly impact people, services, and national resilience. Whether you're protecting sensitive health data, securing critical infrastructure, or ensuring continuity of government operations, the stakes are too high for assumptions. These environments require more than availability and resilience—they demand proof.

NodeZero Federal™ delivers that assurance. As a FedRAMP High Authorized platform, it enables your teams to continuously validate security from the inside out. Every test is autonomous, proven safe in production, and grounded in real-world attack behavior. In a time when adversaries aim to disrupt, degrade, or control critical systems, readiness must be demonstrated with evidence—not words.

Already powering hundreds of high-impact assessments across national security environments, NodeZero Federal delivers validated, audit-ready results aligned with federal mandates—helping you move from compliance to confidence.

Proven by National Security Missions

The NodeZero® Proactive Security Platform is operationally proven through its support of the NSA's Continuous Autonomous Penetration Testing (CAPT) program, where it helps hundreds of Defense Industrial Base (DIB) suppliers identify, mitigate, and verify exploitable weaknesses have been remediated in their infrastructures.

This large-scale, real-world use case provides concrete validation of NodeZero's safety, scalability, and effectiveness.

CAPT Impact Metrics (as of May 2026):

Metric	Count	Metric	Count
Participants	700+	Pentests Conducted (≥1 host)	23,000+
Endpoints Tested	2,700,000+	Total Weaknesses / Vuln Paths	690,000+
Critical Weaknesses Exploited	29,000+	Critical Weaknesses Mitigated	15,000+
High Weaknesses Exploited	14,000+	High Weaknesses Mitigated	8,000+
Medium Weaknesses Exploited	17,000+	Medium Weaknesses Mitigated	9,000+
Low Weaknesses Exploited	66,000+	Low Weaknesses Mitigated	23,000+
Total NodeZero Pentest Hours	**290,000+**		

CAPT Program Manual Pentest Hours Avoided	
Total NodeZero Pentest Hours Performed	290,000+
Number of Hours Required if Performed by Human Pentesters (x12)	3,400,000+
Average Cost Per Hour for Human Pentesters	$200
Total Cost Avoidance	**$696,000,000+**

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

These results demonstrate that risk wasn't just assessed—it was reduced. Security posture improved significantly, delivering operational impact at scale. That same capability is now available to your agency through NodeZero Federal.

From Point-in-Time to Continuous Assurance

Conventional security practices like vulnerability scans, annual assessments, and manual pentests can no longer match the tempo or tactics of today's adversaries. These methods often produce theoretical findings without context, delay detection of exploitable weaknesses, and fail to confirm whether mitigations actually work.

NodeZero Federal addresses these limitations by continuously emulating adversary behavior in live environments. It chains together real misconfigurations, exposed credentials, and trust boundary violations to reveal how an attacker would gain access, move laterally, and escalate privileges. Each test is credential-optional, and requires no integration, empowering your teams to act swiftly without disruption.

Why Federal Agencies Choose NodeZero Federal

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® PROACTIVE SECURITY PLATFORM

Built on the same platform trusted across 230,0000+ autonomous pentests in commercial, DIB, and federal systems—at scale.

ALWAYS-ON READINESS, NOT ANNUAL SNAPSHOTS

Legacy scans and annual engagements can't keep up with today's adversaries.

NODEZERO FEDERAL

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

Leadership Perspective

"In mission environments, we never assumed security, we validated it. The same principle must apply in cyber. Agencies can no longer rely on hope or paperwork. They need proof," said Snehal Antani, CEO of Horizon3.ai and former CTO in the US Joint Special Operations Command (JSOC).

This operational mindset is embedded into the platform itself. NodeZero Federal is currently the only FedRAMP High Authorized platform purpose-built for continuous, autonomous penetration testing, offering a unique capability to federal agencies seeking real-time operational assurance.

> NodeZero Federal enables that proof, continuously, safely, and without slowing the mission.
>
> - Snehal Antani, CEO of Horizon3.ai

Alignment with Federal Cyber Mandates

NodeZero Federal aligns with a comprehensive set of mandates and frameworks, helping your agency meet its regulatory and security obligations with confidence. Its testing and reporting structure support rapid assessments, executive reporting, and technical compliance documentation. NodeZero Federal is designed to help agencies meet many of the requirements below:

Mandate / Framework	Risk Assessments	Penetration Testing	Readiness Exercises
FISMA	Required	Required (via NIST SP 800-53)	Required (via NIST SP 800-53)
OMB M-22-09 (Zero Trust)	Required	Required	Required
FedRAMP Authorized CSPs	Required	Required (annual)	Required (annual)
CMMC 2.0	Required	Required (Level 2 and above)	Required (Level 2 and above)
CISA BOD 23-01	Required	Not specified	Not specified
NIST SP 800-53 Rev. 5	Required	Required (CA-8)	Required (IR-3, IR-4, IR-8)
NIST Cybersecurity Framework (CSF)	Recommended	Recommended	Recommended
NIST SP 800-171 / 172	Required	Required (800-172)	Required (800-172)
NIST SP 800-207 (ZTA)	Recommended	Recommended	Recommended
CORA (DoD Readiness Model)	Required	Required	Required

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, surfacing real-world weaknesses in any 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.

Operational Benefits for Your Agency

NodeZero Federal is designed to enhance—not disrupt—daily operations. It reduces security team workload by focusing only on exploitable risks, and it eliminates the guesswork between remediation and results.

The ability to run safe, repeatable, and autonomous assessments internally gives your agency greater agility, deeper insight, and more control over its risk posture. With no reliance on third-party testers and no delay in reporting and verification, your teams can shift from reacting to leading.

Proving Security Impact When Every Dollar Counts

In an era of tightening budgets and heightened oversight, cybersecurity programs must do more than demonstrate activity—they must justify impact. NodeZero Federal enables that shift by turning penetration testing into a continuous, cost-stable capability that proves readiness at every stage.

Unlike traditional pentesting engagements that rely on external vendors and expensive per-test fees, NodeZero Federal empowers internal teams to run autonomous, production-safe assessments on demand—without added cost, integration work, or scheduling delays.

There are no agents to deploy, no consultants to manage,
no delays in reporting, and no waiting to validate fixes.
It's always available, always safe, and always aligned to the mission.

"NODEZERO FEDERAL DOESN'T JUST HELP YOU FIND PROBLEMS—IT HELPS YOU PROVE VALUE."

Because tests focus only on what's exploitable, teams avoid wasting time on theoretical issues and reduce noise in remediation workflows. One-click retesting confirms whether issues are resolved, enabling faster MTTR and clearer performance metrics. With built-in reporting mapped to federal frameworks, NodeZero Federal also streamlines oversight—reducing friction during audits and reinforcing the maturity of your security program.

When dollars are limited, defensibility matters. NodeZero Federal ensures your security spend results in measurable, mission-aligned outcomes—not assumptions.

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**

Conclusion

Assumed security is no longer acceptable in federal operations. With NodeZero Federal, your agency can transition to a model of continuous, validated readiness—where security decisions are based on fact, not inference, and where the mission remains uninterrupted.

In a time when adversaries move fast and exploit uncertainty, this capability is no longer optional—it's essential.

LEARN MORE ABOUT NODEZERO FEDERAL™

Schedule a Demo

 @Horizon3ai info@horizon3.ai www.horizon3.ai