HORIZON3.ai

# Third-Party Risk Management Program

## Proactively Secure Your Supply Chain with NodeZero®

The cybersecurity risk you inherit from your suppliers is no longer theoretical—it's verifiable, and increasingly weaponized. **Horizon3.ai's NodeZero® Proactive Security Platform** gives you the power to hack, fix, verify, and repeat to discover third-party risks before they disrupt your operations. Traditional approaches to assessing third-party exposure, like self-attestation questionnaires or external ratings agencies rely on assumptions and probability models.

Modern attackers increasingly target small and mid-sized suppliers who lack the staff, tools, or budget to adequately defend themselves. NodeZero closes this blind spot with autonomous pentesting that continuously uncovers and validates exploitable attack paths, with no agents, credentials, or integrations required.

## NodeZero for Supplier Security Posture Management

A turnkey approach for organizations that need proof, not promises, from their third parties.

- Run autonomous pentests against supplier environments
- Discover attack paths fueled by credential weaknesses, shadow IT, vulnerable software
- Regularly retest to verify mitigations and confirm a measurable reduction in exploitable attack surface
- Receive executive-ready reports for compliance and board-level oversight

**NodeZero is not a questionnaire. It's a test your suppliers can pass—or fail.**

## Business Impact for Executives and Risk Leaders

- **Continuity —** Prevent avoidable disruption by verifying supplier resilience
- **Efficiency —** Cut reliance on costly, slow third-party risk assessments
- **Compliance —** Prove you're meeting due diligence and assurance requirements
- **Reputation —** Avoid the headlines by stopping breaches before they start
- **Trust —** Integrate assessments into supplier onboarding to validate security posture prior to production integration

## Horizon3.ai's TPRM Program Proven Effective: NSA's CAPT Program

The National Security Agency (NSA) selected NodeZero to power the Continuous Autonomous Penetration Testing (CAPT) program—delivered through its Cybersecurity Collaboration Center. CAPT provides no-cost offensive security assessments to eligible Defense Industrial Base (DIB) suppliers using NodeZero.

| CAPT Program Manual Pentest Hours Avoided | |
|---|---|
| **Total Number of DIB Participants** | **700+** |
| **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: Figures as of May 2026*

# How The TPRM Program Works

## A Repeatable, Scalable Model for Third-Party Risk Validation

**1. Identify and Prioritize Suppliers by Risk**

Map and tier your supplier ecosystem by focusing on three key groups: critical suppliers essential to operations, high-risk suppliers with suspected security gaps, and new suppliers recently onboarded through contracts or acquisitions.

**2. Distribute NodeZero Through a Buyer-Led Program**

Organizations initiate the program by allocating NodeZero access to selected suppliers. Horizon3.ai handles the logistics, ensuring each supplier is supported through onboarding, host deployment, and test execution.

**3. Launch Safe, Agentless Autonomous Pentests**

Suppliers deploy NodeZero in under 15 minutes with no agents, credentials, or integrations required. Tests emulate real-world attacker behavior, safely identifying exploitable weaknesses within live production environments.

**4. Surface Impact, Fix Weaknesses, and Verify Remediation**

Each test produces detailed, proof-based findings showing exploitable attack paths, impacted systems, and data at-risk. NodeZero provides prioritized remediation guidance, and suppliers can retest instantly to confirm issues are resolved.

**5. Track and Improve Security Across Your Ecosystem**

The parent organization receives centralized reports and visibility through NodeZero's dashboards, prioritizing critical and high-risk weaknesses, monitoring verified fix rates over time, and ensuring systemic and recurring issues are identified and addressed.

**6. Supplier Enablement and Shared Visibility**

The parent organization gains a high-level view across their supplier base without needing direct access to sensitive vendor data. Horizon3.ai's Customer Success team facilitates engagement throughout the program.

## What Do Suppliers Say?

Suppliers say yes to NodeZero because it's fast to deploy, safe to run in live production, and smart in how it prioritizes real, exploitable risk—not just theoretical CVEs. But the biggest reason they participate is access to high-quality pentest results they can reuse for their own compliance needs, including SOC 2, ISO 27001, and other regulatory audits. The platform also reduces the burden of questionnaires and manual assessments while enabling secure reporting that protects sensitive data. As vendor assurance becomes a requirement, participating is no longer optional—it's a strategic advantage.

## Stop Inherited Risk Before It Spreads

The mission of the TPRM program is to break the cycle of inherited risk. When suppliers fail, the consequences hit upstream—impacting your operations, customers, and reputation. NodeZero enables you to verify resilience, demand accountability, and ensure that third-party cyber risk stays where it belongs: *outside your business.*

## Ready to take control of third-party risk?

Schedule a demo at **www.horizon3.ai/demo.**