info@Horizon3.ai
www.Horizon3.ai
LinkedIn: Horizon3.ai
Twitter: @Horizon3ai

NodeZero

Fix What Matters NOW!

ATTACK AND ASSESS

NodeZero is a fully automated cyber attacker that emulates the tools, tactics, and techniques of real-world attackers, so you can find and **fix what matters NOW.**

PRODUCT DESIGN PRINCIPLES

No Pervasive or Persistent Agents

- ✓ This is true SaaS. NodeZero is an unauthenticated and ephemeral container you spin up. No retention, memory hogging or credential provisioning. Bottom line: no alerts, only results.

1-Click User Experience

- ✓ Zero tuning, zero training and 1-click reporting. From a single machine anywhere in your environment, NodeZero examines and exploits your enterprise, recording a path to your critical assets, identifying vulnerabilities, chaining weaknesses and earmarking precious data. NodeZero validates what an attacker can do and delivers those results to you.

Safe to Run in Production

- ✓ No bruising. Period. You choose the scope and attack parameters. In live production or as code in your development pipeline, NodeZero benignly exploits what is most vulnerable and valuable and provides proof so you and your team are focused on prioritized action.

Painless PenTesting

- ✓ Nobody looks forward to some outside auditor breaching their system and telling them where they are failing. Own it. Literally.

CONTEXT

Your impact, your risk. Every op and every weakness are scored in the context of your environment: what was found and what could be used against you. This is anything but the industry standard.

CHAINING

Attackers chain weaknesses to create an attack vector, taking advantage of ignored misconfigurations, exploiting lower severity vulnerabilities, harvesting default credentials. NodeZero does the same at speed and scale.

PROOF

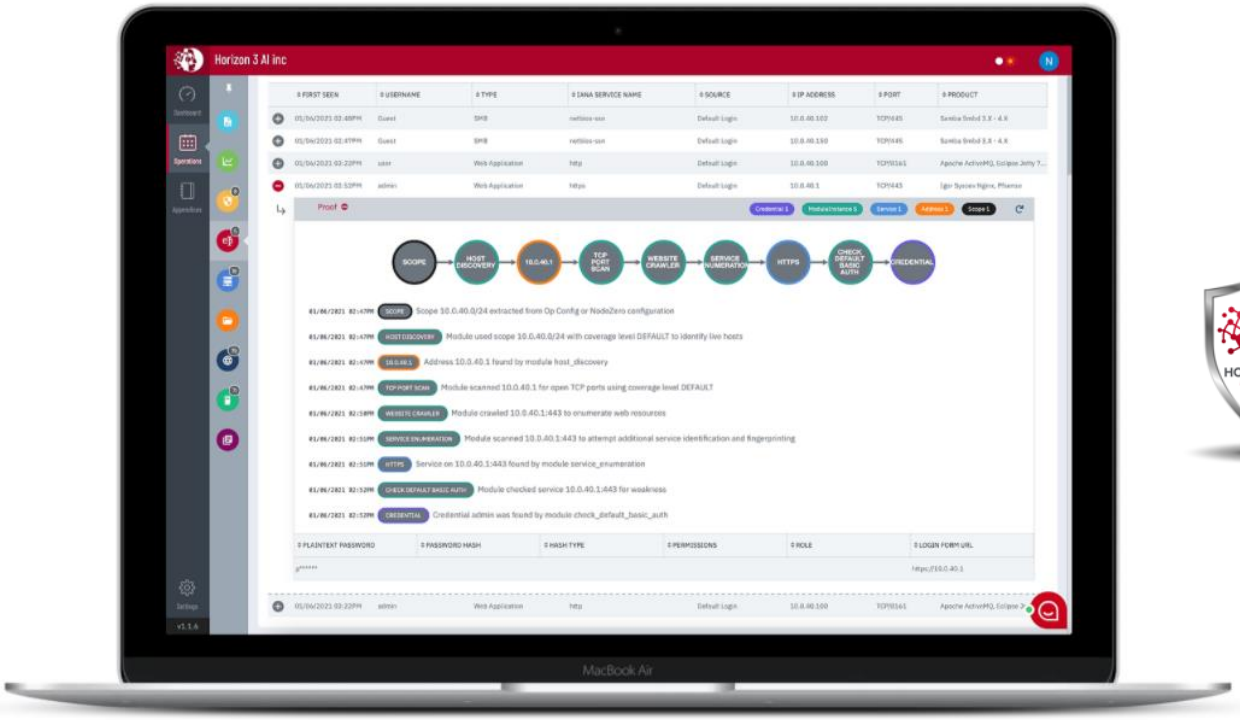
Time and talent are scarce; chasing a false positive is frustrating and wasteful. NodeZero verifies and proves exploitation. There are no alerts, only results.

Automated Pen Testing as a Service (APTaaS™)

NO CHEATING!

NO need to modify your environment. One more reason our attacker's perspective validates your security controls, so you can act on what IS versus what SHOULD BE.

What Matters	**Traditional Approach**	**BETTER Approach**
Effort Required	High (Multi-Team, Coordinated)	Low (Self-Service, On Demand)
Test Frequency	Annual or Quarterly	Agile and Continuous
Total Cost	High for Single Pentest	Low for Unlimited Ops
Time to Value	Weeks to Written Report	Hours to Searchable Results
Coverage	1-2% of Environment	99+% of Environment
Expertise Needed	High to Execute	Low to Execute
Resources	External Professional Services	Internal Purple Team Partner
Ultimate Goal	**Pwn you to demonstrate value**	**Decrease risk to your company**



Our Story

Horizon3.ai is a leader in security assessment and validation enabling continuous security overwatch from an attacker's perspective, so you spend your security resources fixing what matters. Founded in 2019 by former US Special Ops cyber operators, Horizon3.ai is headquartered in San Francisco, CA, and made in the USA.

You Can Try NodeZero for Free

Visit Horizon3.ai for a Free Trial or to Schedule a Demo

NodeZero
Fix What Matters NOW!