HORIZON3.ai

Introduction to Horizon3.ai and NodeZero®

Horizon3.ai helps organizations validate security based on how real attackers operate. Our platform, NodeZero, autonomously performs penetration testing across external, internal, cloud, identity, and application attack surfaces to determine what is actually exploitable in live environments.

NodeZero is designed for security teams that need high confidence results. Instead of generating large volumes of theoretical findings, NodeZero validates exploitability, captures proof, and shows impact. This allows customers to prioritize remediation based on demonstrated risk rather than scanner output or point in time assessments.

NodeZero Web Application Pentesting

NodeZero Web Application Pentesting brings the attacker's perspective to custom web applications. It is built to safely test production applications and answer a simple but increasingly challenging question: **can an attacker actually exploit this application in a production, development, or staging environment?**

During a Web Application Pentest, NodeZero autonomously performs the following steps:

1. **NodeZero maps the application by crawling reachable routes, forms, and endpoints.** This creates an accurate view of the application surface as it exists at test time, without requiring manual route enumeration. Authentication, parameter, check, and session support are built into NodeZero dynamically allowing it to traverse all relevant paths aligned to the initial scope.
2. **NodeZero executes controlled exploit attempts against high impact vulnerability classes.** These include injection flaws and broken access control scenarios that reflect how attackers target real applications. Testing can be performed with or without authentication, depending on configuration, to validate both unauthenticated and authenticated attack paths. Supported vulnerability classes include injection (e.g. XSS, SQLi, SSTI), broken access control, auth bypass, XXE, LFI, redirects, uploads, among others. NodeZero also attempts post-exploitation to achieve persistence by landing RCE and remote access tools, where possible and production safe.
3. **Finally, when exploitation and/or post-exploitation is successful, NodeZero captures replayable proof.** This includes the payload used, the request and response evidence, and a clear description of what access or impact was achieved. Findings are validated by exploitation, not inferred by pattern matching. NodeZero benchmarks on a <5% potential false positive rate compared to the 30-50% rates seen by many leading DAST tools.

All testing is production safe by default. NodeZero applies guardrails around rate limiting, payload selection, and destructive actions to ensure business operations are not disrupted. Customers maintain control over scope through route level inclusion and exclusion rules and can re-test individual findings to verify that fixes fully resolve the issue.

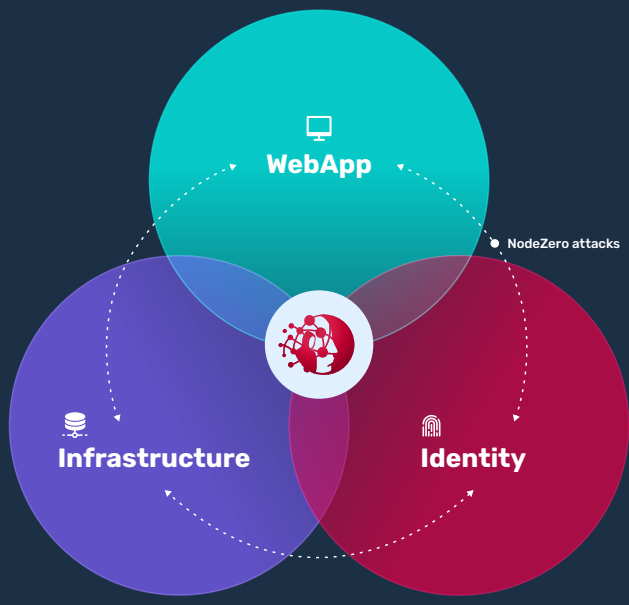
Web application findings integrate into existing security workflows. Results can be reviewed alongside other NodeZero findings through vulnerability management hub, shared with application owners via notes and ticketing integrations, and tracked through remediation and verification without requiring a full retest.

NodeZero Vision for Web Application Security

At Horizon3.ai, we believe web application security cannot be effective if it is treated as a standalone problem or evaluated only at fixed points in time. Applications change constantly, and attackers continuously test for new ways in. Point in time assessments leave long gaps in coverage and create false confidence that quickly erodes as code, configurations, and dependencies evolve.

Effective defense requires continuous testing across all relevant attack surfaces. Web applications, infrastructure, cloud resources, and identity systems are tightly connected in real environments, and attackers routinely move across these boundaries. A weakness in a web application often becomes the entry point that enables credential abuse, privilege escalation, or downstream access to internal and cloud systems.

The vision for NodeZero is to continuously test across the entire technology stack as a single attack surface, using the same attacker driven methodology everywhere. Web applications are treated as first class entry points, evaluated not in isolation but in the context of the infrastructure and identities they interact with. Validated exploits show proof for how an attack could progress, what systems are exposed, and where real business impact emerges.



NodeZero is the only AI-Powered platform that autonomously attacks WebApps, Infrastructure, and Identities.

By combining autonomous execution, exploit validation, and unified visibility across web applications, infrastructure, and identity, NodeZero aims to replace fragmented security programs with a single offensive security platform. The outcome is **clearer prioritization, faster remediation, and confidence** that critical applications and systems are not the path attackers will use to compromise the business.

Join the Waitlist

NodeZero Web Application Pentesting is currently available to a limited set of early adopter customers. Join the waitlist to request early access and help shape a more effective, attacker driven approach to web application security.