



HORIZON3



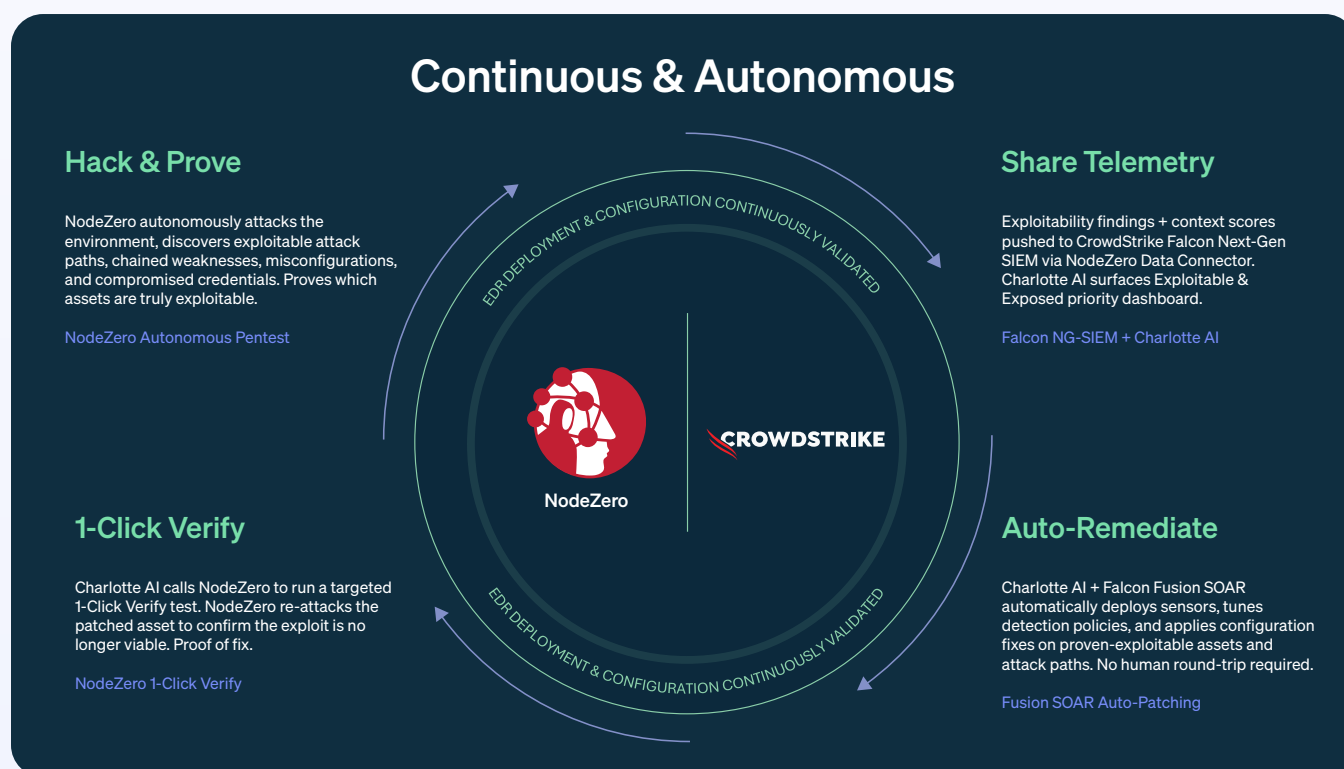
CROWDSTRIKE

Prove your security from the attacker's perspective.

Horizon3 and CrowdStrike have partnered to bring NodeZero's exploitability intelligence from autonomous pentesting into CrowdStrike NG-SIEM and Fusion SOAR workflows in a continuous loop of proving, prioritizing, remediating, and verifying. Together, the integration helps organizations prioritize the risks that matter most.

PROVE. PRIORITIZE. VERIFY.

This closed loop carries proof of exploitability into the Falcon platform your team already uses, helping security and IT teams avoid alert fatigue and manual triage by providing proof of exploitability, remediation and verified closure in minutes. Scanners flag what might exist. CVSS scores estimate severity in the abstract. Endpoint protection helps defend the environment. None of these tools on their own can tell you what an attacker can actually reach in your environment right now. NodeZero exposes actual attack paths, sending verified proof of exploitability into CrowdStrike NG-SIEM to turn threat noise into prioritized defense.



The security gap

<2%

of published CVEs are ever actually exploited, yet most teams still triage by severity score alone.

88%

of organizations haven't validated their EDR effectiveness in the past three months.

70%

patch a vulnerability and assume the fix held, without ever retesting it.

More vulnerabilities. Less time to decide.

In 2025, more than 50,000 CVEs were published. Frontier AI is also collapsing exploit weaponization timelines from weeks to as little as one to two days.

The challenge is not simply volume. Teams need a reliable way to determine which findings represent a real attack path in their environment, then move from proof to action without losing time between tools.

Siloed visibility

Siloed security data, spanning vulnerability, identity, cloud, network, and endpoints, lacks the visibility to reveal exploitable attack paths, while scanners and CVSS scores only identify theoretical weaknesses.

Alert fatigue and false positives

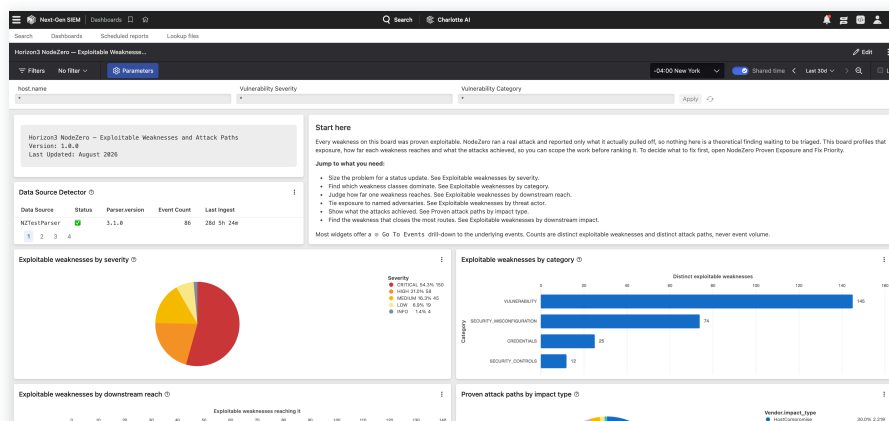
Security teams work with large volumes of telemetry and alerts, while fewer than 2% of published CVEs are ever actively exploited.

Manual bottlenecks

Remediation and verification often require multiple handoffs. A fix may be applied without confirming that the attack path is closed, leaving teams to rely on assumptions instead of evidence.

Stretched teams

The pace of change continues to increase while security and IT teams must make decisions with finite time and resources. Teams need to reduce manual correlation and quickly get the context needed to act.



NodeZero + CrowdStrike Falcon: Prove. Prioritize. Verify.

NodeZero, Horizon3's autonomous AI pentesting platform, combines with CrowdStrike NG-SIEM and Fusion SOAR workflows to connect exploitability proof to prioritization, remediation, and verification.

NodeZero proves what is exploitable. Falcon brings that proof into the workflows teams already use. Configured response workflows can act on the findings, and NodeZero can verify whether the fix closed the path.

Once NodeZero sends exploitability intelligence to CrowdStrike NG-SIEM, it can flow into the native CrowdStrike workflows customers already use, like Fusion SOAR & Charlotte AI.

What this means for you

Benefit	What it means for your team
Fix what an attacker can use	Findings are ranked by environment-specific context and blast radius, helping teams focus on exploitable paths rather than a long CVSS list.
Keep each team in its workflow	Pentest and vulnerability management teams run NodeZero. Findings and remediation context surface in NG-SIEM as an event, where the SOC can use them without opening NodeZero.
Verify the fix	Use the Fusion SOAR workflow to automatically trigger NodeZero 1-Click Verify retests on the exact weakness. Close detection cases with verification, not assumption.
Track exploitable exposure in a unified location	Findings stream into Falcon NG-SIEM, normalizing results into a single Exploitable & Exposed dashboard, eliminating the need to switch tools.
Continuously validate	Manage real-world attacks, chaining vulnerabilities and misconfigurations, on CrowdStrike managed production assets.
Remediation faster and automatically	Remediation time is cut from weeks to minutes when Falcon Fusion SOAR triggers instant playbooks scoped to specific hosts and techniques uncovered by NodeZero.

Project QuiltWorks:

From AI discovery to proven protection

Frontier AI is changing how quickly vulnerabilities can be discovered and weaponized. Project QuiltWorks brings together the capabilities needed to assess those findings, prioritize what matters, guide remediation, and continuously validate protection.

How NodeZero extends QuiltWorks

1. Discover

QuiltWorks surfaces vulnerabilities through frontier AI research and coalition discovery efforts, including Project Glasswing and Anthropic's Mythos.

2. Prove

NodeZero autonomously tests the relevant assets across infrastructure, identity, cloud, web applications, and endpoints. It chains vulnerabilities, misconfigurations, and exposed credentials into real attack paths, confirming what can be exploited in the customer's environment.

3. Prioritize

NodeZero's proven exploitability integrates natively with CrowdStrike. By surfacing evidence directly in existing workflows, such as Next-Gen SIEM and Charlotte AI, teams can prioritize action based on real attack paths and business impact, rather than just abstract severity scores.

4. Fix and verify

Teams remediate using existing tools. Falcon Fusion SOAR triggers playbooks for proven findings, while NodeZero's 1-Click Verify confirms the path is closed.

The Outcome

QuiltWorks accelerates discovery, NodeZero confirms actual exploitability, and CrowdStrike Falcon drives remediation and verification.

Together, CrowdStrike and NodeZero deliver the complete cycle:
Prove. Prioritize. Verify.

Get *started*

To request a Joint Assessment, please contact:

partners@horizon3.ai

or visit horizon3.ai to deploy the integration directly within NodeZero, available now in the CrowdStrike Marketplace.