HORIZON3

Trading Maintenance for Momentum: Scaling Security Validation Across 230+ Sites

By replacing hardware maintenance fatigue with autonomous validation, an automotive manufacturer saved four days of weekly operational overhead, cut test times in half, uncovered critical missed vulnerabilities, and maximized ROI for a lean security team.

CASE STUDY

Customer *snapshot*

CUSTOMER

Global automotive technology manufacturer

INDUSTRY

Automotive technology and manufacturing

SIZE

>100,000 employees

SOLUTIONS

Horizon3 NodeZero Internal Pentest

Threat Informed Perspectives

Insights

Rapid Response

1-Click Verify (1CV)

CHALLENGE

A global automotive technology manufacturer operates across factories, offices, data centers, and cloud environments that must remain available while security teams test them.

A global automotive technology manufacturer operates across factories, offices, data centers, and cloud environments that must remain available while security teams test them. More than 200 sites, multiple network segments, centralized identity infrastructure, and a distributed operating model created a difficult validation problem: the team needed recurring evidence of exploitable risk without building and maintaining a large testing appliance footprint at every location.

This organization had already built a substantial automated validation program with an incumbent autonomous pentesting solution, but the operating model required significant ongoing effort and was difficult to scale across its distributed environment. The team ran roughly 22 site tests each week, maintained a main node and 12 appliances, managed VPN tunnels, and built an internal orchestration layer to schedule campaigns and move results to local IT teams. The team estimated that launch, update, and troubleshooting work could consume roughly four days each week. Coverage also stopped short of parts of the data center and cloud environment.

That created a moving target for security leadership. The program was producing useful evidence, but the cost of operating it made broader, more frequent validation difficult. The Exposure Management experts operating the program had turned into technicians troubleshooting legacy appliances 2 days out of 5, which was seen by the management as a waste of talent and resources. The customer selected NodeZero for the initial like-for-like migration of internal pentesting from their previous platform. Broader external testing and Rapid Response were planned as follow-on use cases.

WHY NOW

A comparison that changed the decision

The first proof point came from a side-by-side evaluation against the incumbent solution. For the first time ever, the customer was able to cover north of 80K assets in a single assessment, overcoming their usually fragmented view of risk, caused by the computing limitations of legacy appliances. On top of giving a complete picture, the comparison also exposed a meaningful coverage gap: NodeZero uncovered many relatively new vulnerabilities (2026) that the incumbent had not surfaced, largely due to the dependency on manual content updates The finding reached the CISO quickly because it represented a concrete difference in what the two platforms could prove, not a difference in dashboard design.

A rollout built for scale

A second moment came from the scale of the environment. Moving from maintenance heavy, large footprint appliances, to lightweight plug-and-play virtual machines, the team found that NodeZero could operate almost at zero-touch and with minimal footprint rather than requiring hands-on maintenance and troubleshooting at every site. The architecture preserved the customer's existing tunnel-based approach while making any lightweight runner available to any site. That flexibility mattered in an environment where installing and maintaining hundreds of powerful appliances would have been impractical.

A production lesson that strengthened the program

The third breakthrough was operational. As the rollout moved into production, the team connected NodeZero findings to its own portal and local remediation process. It classified findings, routed site-specific tickets, and used 1CV to determine whether fixes held. The team also ran Rapid Response checks against newly relevant vulnerabilities, including external assets, instead of waiting for the next full testing window.

WHY HORIZON3

Centralized testing without hardware and operational overhead

NodeZero fits the team's goal of running more validation without recreating the hardware and maintenance burden of the prior platform. The initial production model used a centralized pool of 16 NodeZero virtual machines and VPN tunnels into sites, supported by existing local tunnel infrastructure. The team could deploy quickly, use the same runner for different sites, and keep scheduling and ticket routing connected to its existing operational systems.

One view from testing to remediation

The platform also gave the central vulnerability team a common view across site assessments. Perspectives and Insights helped the team track coverage and trends, while vulnerability management views consolidated findings across tests. The result was a program that could be operated centrally while still sending local teams only the actions relevant to their sites.

As the vulnerability management lead put it, "I think this will honestly be much less of a headache than trying to launch a test every week on the old platform because that was really hard. I think it will be an easy life for us going forward."

VERIFIABLE RESULTS

Broader coverage at a repeatable cadence

The program expanded from a recurring schedule of site-by-site campaigns into a centralized rollout. The team reported over 190 of the 230+ sites onboarded, a target cadence of about 22 sites per week, representing 82% coverage during the initial pass. It also used the results to change how remediation was managed, rather than treating each pentest as a report that disappeared after delivery.

Comparable test runtime was reduced by 50% and double the number of weaknesses identified. This is seen as a key enabler for allowing increased test cadence.

Hundreds of tests were run within the first 2 months of production service.

.

Remediation that could be verified

That workflow produced measurable follow-through. The team reported more than 1,200 remediation tickets, 300+ 1CV's, over 250 remediation cases confirmed with only about 60 still open after verification. Findings could be prioritized by downstream attack paths and business impact, giving local IT teams a clearer reason to fix an issue and a repeatable way to confirm the result.

A program designed to keep scaling

The broader change was structural. The security team moved from maintaining a complex testing operation toward continuously validating a large, changing environment through a central program. NodeZero added broader exploitability evidence, newer vulnerability coverage, external testing, and a path to include data centers and cloud environments in the same security conversation.

Looking Ahead

The team is extending the program beyond local site testing to data centers, the external perimeter, cloud environments, and Rapid Response for faster validation of newly published vulnerabilities.

The organization's security program is becoming easier to scale because each campaign can do more than produce a report. It can show what an attacker could reach, direct the right team to the fix, and prove whether the path is closed before the next test begins.