How Kyocera AVX Built a Global Security Validation Program from Zero

In roughly three years, Kyocera AVX remediated more than 30,000 vulnerabilities and misconfigurations, deployed NodeZero across most manufacturing sites in one to two years, and established a testing cadence four times higher than the industry norm.

CASE STUDY

Customer *snapshot*

CUSTOMER

Kyocera AVX Corp (KAVX)

INDUSTRY

Global electronic components manufacturing

ENVIRONMENT

Approximately 15,000 employees, 33 manufacturing sites worldwide, complex global infrastructure, and production environments with OT-adjacent considerations

CHAMPION

Russell Charles, Global Risk & Compliance, Information Security Manage

SOLUTION

Horizon3 NodeZero, continuous pentesting, 1-Click Verify runs, Fix Actions reports, Splunk integration, and NodeZero Tripwires™ / deception tokens

CHALLENGE

A global manufacturing environment without a formal validation program

Kyocera AVX uses technology to address critical needs across automotive, information and communications, environment and energy, and medical and healthcare, guided by its mission: "Now and In the Future." With global manufacturing sites, the company operates a complex environment where security decisions must account for business continuity and production safety.

Before NodeZero, KAVX had no formal vulnerability management or pentesting program. There was no consistent scanning process, no regular pentest cadence, and limited visibility into how weaknesses could combine into an end-to-end attack path. IT operations teams were understandably sensitive to tools perceived as invasive, especially around production systems.

"Without an attacker's view, it was difficult to know which misconfigurations and weaknesses really mattered most in a complex manufacturing environment such as ours," says Russell Charles, Global Risk & Compliance, Information Security Manager.

That gap created the need for a program that could show practical risk without compromising the environments that kept the business running.

WHY NOW

Moving from theoretical findings to demonstrated risk

Russell first encountered NodeZero through a trusted cybersecurity podcaster, someone he describes as a “top 30 cybersecurity guy” who rarely recommends products. That endorsement prompted deeper research, including due diligence conversations with traditional vendors such as Rapid7, Nessus, and Qualys.

The distinction that stood out was NodeZero’s exploit-based approach. Instead of stopping at theoretical vulnerabilities, the platform could prove exploitability by chaining weaknesses into real attack paths. The KAVX team needed attacker context, and NodeZero showed how misconfigurations, domain compromise, lateral movement, and credential abuse could connect.

By 2022, the Infosec team made the call: NodeZero would become the engine behind a new global vulnerability management and pentesting program.

Early campaigns changed the team’s view of production risk

As the first pentests began in production, KAVX refined its rules of engagement with internal teams, MDR providers, and EDR teams, especially in an OT-adjacent environment. The goal was to allow continuous pentesting while minimizing possible disruption to production.

The findings quickly made the risk tangible. At one key production site, NodeZero demonstrated eight different ways to compromise the domain. Credential dumping emerged as a major early finding, prompting the KAVX team to work with its EDR team and external SOCs to tune detections and mitigations. In subsequent tests, credential dumping largely disappeared. Without NodeZero, the team would not have known that exposure existed.

The platform also surfaced common misconfigurations and challenged long-standing assumptions, including the belief that changing certain settings would break operations. Those findings led to an update of the company’s password policy and a significant reduction in credential exposure risk.

WHY HORIZON3

A faster path to scale, with findings IT could act on

Many tools in KAVX's environment historically took four to five years to deploy across global sites. NodeZero reached most sites in roughly one to two years, the fastest deployment Russell had seen during his eight years at the company.

That speed came with operational discipline. KAVX codified engagement rules, refined how MDR and EDR tools responded to testing, and adapted the program to production realities. Russell recalls waking up during early campaigns and checking his phone and laptop to see compromises appear in real time. Compared with static reports, the findings were immediate, specific, and difficult to dismiss.

The Fix Actions report became especially important because it gave IT and security a tangible list of changes to make rather than abstract severity scores. Today, approximately 34 NodeZero hosts support regular assessments across the global footprint. KAVX runs about four pentests per site each year, compared with the industry norm of roughly one, and adds 1CV runs for urgent validations.

The operating model extends beyond testing. Each week, vulnerabilities are distributed to IT by severity, progress is tracked, and results are reported to executives. Using the Horizon3 API, the team built a custom NodeZero app in Splunk to visualize global and per-site vulnerabilities, monitor trends, and communicate risk in terms leaders can understand.

VERIFIABLE RESULTS

From zero formal coverage to measurable risk reduction

In approximately three years, KAVX remediated more than 30,000 vulnerabilities and misconfigurations across its global environment. Russell describes remediation as "a never-ending process," but the scale of the work represents a substantial reduction from a baseline with essentially no formal vulnerability management or pentesting program.

Faster deployment and more frequent validation

NodeZero reached most manufacturing sites in one to two years, compared with the four to five years typically required to fully roll out comparable tools. KAVX now has a repeatable rhythm of weekly vulnerability metrics, quarterly site pentests, and targeted retesting managed by Kaleb Keith.

NodeZero is, by nature, the "most noisy and invasive" tool in the stack. Yet the risks it exposed also made it the fastest security tool to roll out in Russell's nearly eight years at the company. The value was clear enough to overcome the initial pushback.

Executive visibility that changes priorities

Splunk dashboards, NodeZero findings, and Fix Actions reports give IT and executives a shared view of what matters and what needs to change. Russell's counterfactual is direct: without NodeZero, KAVX would likely be living with at least 30,000 more weaknesses today.

LOOKING AHEAD

Expanding validation and making small controls count

KAVX is exploring Tripwires and deception tokens, with approximately 8,000 potential placements identified across the environment. The team also is considering more frequent testing to tighten the window in which weaknesses remain open.

Russell's advice to peers is practical: expect pushback, be patient, educate the organization, and adapt the program so pentesting and operations can coexist. When leaders and IT teams can see real attack paths and understand how to fix them, priorities change.

KAVX has moved from having no formal vulnerability management program to operating a global, evidence-driven security validation practice that makes risk visible, actionable, and harder to ignore.