How TTEC Turned Hidden Attack Paths Into Audit-Ready Security Validation

In about 20 minutes, Horizon3's NodeZero® scanned several thousand documents, surfaced a few dozen potential usernames and passwords, and helped the team recover most of the roughly 15 percent of annual time it had been spending on a previous penetration testing solution.

TTEC is a global leader in customer experience (CX), operating large contact centers and remote agent programs for some of the world's most recognizable brands. Every interaction depends on a complex mix of telephony, CRM, workforce management, and data systems that must be both available and resilient to attack. To protect that ecosystem, TTEC turned to Horizon3.ai's NodeZero autonomous penetration testing solution.

Customer *snapshot*

CUSTOMER

TTEC

INDUSTRY

CX / BPO, large global enterprise

ENVIRONMENT

Hybrid data centers + cloud; distributed contact centers; remote workforce; fast-growing web app footprint

CHAMPION

Gene Barlow, Penetration Testing & Vulnerability Management

SOLUTION

Horizon3.ai NodeZero autonomous penetration testing and advanced credential discovery

CHALLENGE

Hidden credentials, unknown assets, tougher audits

TTEC is a global provider of next-generation scalable customer experience solutions, operating large contact centers and remote agent programs for some of the world's most recognizable brands across six continents and 50+ languages. With 52K employees supporting their customer needs, every interaction depends on a complex mix of telephony, CRM, workforce management, and data systems that have to stay available while standing up to attack.

That creates a moving target for security leadership. New web applications are launched across the business. Legacy servers and IP ranges are repurposed or brought back online. Administrators and engineers sometimes hard-code credentials into scripts and tools so routine work keeps moving. External attack surface management tools surface new internet-facing entities for the security team to investigate on a regular basis.

The risk was not any single vulnerability in isolation. The larger concern was whether an attacker could land on one overlooked asset, chain together subtle weaknesses, and reach something far more sensitive. That question became more urgent as threat actors moved faster than a traditional vulnerability management program could comfortably match.

WHY NOW

Breakthrough moments with NodeZero

Several experiences with NodeZero pushed the team to expand and deepen its use of the platform.

The first came from Advanced Data Pilfering during a credentialed test. After roughly 20 minutes, NodeZero had scanned several thousand documents and surfaced several dozen potential usernames and passwords, more than previously uncovered over many hours of manual penetration testing. In one case, NodeZero found an account with more permissions than it should have. Further investigation showed that the password it identified was expired, but the account and its new password were still actively used, the account had policy-violating permissions, and both credentials were stored together in documents on a jump server and SCCM servers.

For Gene Barlow and the team, that finding changed the conversation. “It introduced an attack path we never would have found otherwise.” The value was not simply that exposed credentials existed. It was that the team now had clear proof of how an attacker could use them in practice.

A second moment came from a non-credentialed test that used an Active Directory Certificate Services technique the team had not seen in previous assessments. By chaining that misconfiguration into an attack path, NodeZero discovered an Exchange mailbox resource account that had not been used in production for an extended period, still had a guessable password, and was misconfigured in Active Directory as a domain user. The team validated the issue using NodeZero’s recommended commands, and the finding triggered a broader review.

The third breakthrough was operational. When auditors asked for precise evidence showing when vulnerabilities were retested and verified as fixed, the team initially struggled to produce that proof efficiently. NodeZero’s built-in vulnerability management views gave the team concise, time-stamped history by asset. Simple screenshots provided direct, repeatable evidence that issues had been found and re-evaluated after remediation.

The company also gained confidence in running NodeZero during production hours. Over time, several campaigns naturally ran into the workday, and there were no outages or user-visible incidents. Some of the most valuable findings surfaced during those hours, when normal authentication and user activity were at their peak.

WHY HORIZON3

NodeZero as TTEC's offensive security engine

Working with Horizon3, the team made NodeZero a core part of its offensive security and validation program.

The organization needed a platform that could centralize management and reporting, deploy easily, test more devices confidently than the prior solution, and help validate false positives and true positives. NodeZero met those needs and delivered broader operational value.

Much of the roughly 15 percent of annual time the team had been spending on its previous penetration testing solution was recouped after the move to NodeZero. The team now uses Advanced Data Pilfering against high-value systems, tests unfamiliar IPs and hosts with NodeZero first, relies on NodeZero management views to support audit responses, and is extending coverage into web applications while exploring leadership-friendly exposure metrics through NodeZero Insights.

OUTCOMES

Stronger security and clearer stories

Their experience with NodeZero has translated into stronger security and a clearer way to communicate risk.

The security team has identified and removed high-risk credentials from jump servers, SCCM servers, and other administrative systems. It uncovered a previously unknown ADCS-based attack path to a default-password mailbox account behaving as a domain user, and it is surfacing legacy or "zombie" assets faster so forgotten infrastructure is less likely to remain an easy entry point.

Its audit posture is stronger as well. New retesting and verification requirements can now be met with clear, time-stamped evidence from NodeZero. Screenshot-ready views reduce the effort needed to prepare for audits and customer assessments, and continuous testing during real business activity provides a more accurate and defensible picture of risk.

At the program level, the team is building a scalable, attacker-centric validation layer by pairing NodeZero with EASM tools and existing vulnerability scanners. The team can run campaigns as often as needed, prioritize findings based on real exploitability and impact, and communicate emerging patterns more clearly to engineers, auditors, and business leaders.

Looking Ahead

As the company continues to grow its CX services and expand its application and infrastructure footprint, demands from regulators, auditors, and customers will keep rising. With NodeZero, it has moved from point-in-time snapshots to continuous autonomous penetration testing, turning missed credentials, vulnerabilities, and configuration weaknesses into prioritized fixes backed by evidence that stands up with auditors, boards, and prospective clients.

Every NodeZero campaign is a chance to find and close the next unexpected path an attacker might take before someone else does.