How TTEC Brought Web Application Risk Into Continuous 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

Customer experience and business process outsourcing

ENVIRONMENT

52K+ employees, operations across 6 continents and 50+ languages, hybrid data centers and cloud, distributed contact centers, remote workforce, expanding web application estate

CHAMPION

Gene Barlow, Penetration Testing & Vulnerability Management

SOLUTION

Horizon3 NodeZero, WebApp Advanced Data Pilfering, vulnerability management views

CHALLENGE

A broad attack surface, with web applications at the center

TTEC supports many of the world's most customer-centric brands through a global operation spanning more than 52,000 employees, six continents, and 50+ languages. That scale depends on telephony, CRM, workforce systems, remote access infrastructure, and a growing set of web applications that connect customers, agents, and internal teams.

For the security team, the challenge was not any single vulnerability. It was whether an attacker could start from one overlooked host or exposed application, chain together subtle weaknesses, and reach something far more sensitive. New applications appear across the business, legacy infrastructure resurfaces, credentials can end up in scripts and tools, and external discovery platforms keep surfacing new internet-facing assets to investigate. Auditors were also asking for clearer proof that issues had actually been retested and fixed.

WHY NOW

Credential exposure with a provable path to impact

Several NodeZero campaigns pushed the team to deepen its use of the platform. The first came from Advanced Data Pilfering during a credentialed assessment. In roughly 20 minutes, NodeZero scanned several thousand documents and surfaced a few dozen potential usernames and passwords, far more than earlier efforts that had taken many hours. One finding led to an overprivileged account whose expired password had been replaced, yet both the old and current credentials were stored together on a jump server and SCCM systems. As Gene Barlow put it, “It introduced an attack path we never would have found otherwise.”

A subtle identity path the team had not seen before

A second moment came from a non-credentialed assessment that used an Active Directory Certificate Services misconfiguration. By chaining that weakness into a larger attack path, NodeZero uncovered an Exchange mailbox resource account that had gone unused, still had a guessable password, and was misconfigured as a domain user. The team validated the issue using NodeZero’s recommended commands, and the finding triggered a broader review.

Audit proof that stands up to scrutiny

When auditors asked for precise proof showing when issues were retested and verified as fixed, the team initially had no clean way to answer at scale. NodeZero’s vulnerability management views changed that by giving TTEC concise, time-stamped asset history that could be turned into simple, defensible screenshots.

Production-safe testing, and the path to webapp validation

Several campaigns ran into the workday without causing outages or user-visible incidents. Some of the highest-value findings surfaced during those hours, when authentication and normal user activity were at their peak. For a business with an expanding application footprint, that provides a more credible view of risk than limited off-hours testing and a stronger foundation for continuous web application validation.

WHY HORIZON3

One operating model for exploitability, evidence, and scale

TTEC made NodeZero a core part of its offensive security program because it solved practical problems first. The team needed centralized management, easier deployment, broader testing coverage, and faster validation of what was truly exploitable. NodeZero delivered that, and TTEC recovered most of the roughly 15 percent of annual time previously spent maintaining and troubleshooting another penetration testing solution.

Just as important, the platform helped the team focus on the choke point that mattered most. TTEC now uses Advanced Data Pilfering against high-value systems, turns to NodeZero first when unfamiliar IPs or legacy hosts surface, and relies on the platform when audit questions appear.

Extending the model to a growing web application footprint

TTEC is using NodeZero WebApp to bring a growing application portfolio under the same attacker-centric discipline. For a global CX company, that is a strategic shift. Customer experience increasingly depends on web-delivered workflows, and the organization needs to know which application weaknesses can actually be abused, what business consequences they create, and how they connect to identity and infrastructure risk.

VERIFIABLE RESULTS

Reduced exposure, backed by proof

TTEC has identified and removed high-risk credentials from jump servers, SCCM systems, and other administrative assets. It uncovered a previously unknown certificate-related attack path to a default-password mailbox account, and it is surfacing forgotten or legacy infrastructure faster so unfamiliar devices can be patched or decommissioned with clearer priority.

Stronger audit posture with clearer evidence

Retesting and verification requests can now be answered with time-stamped evidence drawn directly from NodeZero. Preparing for audits and customer assessments takes less manual effort, and the results are easier for nontechnical stakeholders to understand.

A scalable path into continuous webapp validation

By pairing NodeZero with external discovery tools and existing scanners, TTEC can run campaigns as often as needed and prioritize remediation based on demonstrated exploitability and impact. That model becomes more valuable as the company extends the same discipline into web applications and builds persistent exposure metrics for leadership.

LOOKING AHEAD

Building continuous validation around the applications the business depends on

TTEC's environment will keep expanding, especially across customer-facing and operational web applications. What has changed is the company's ability to answer that growth with evidence.

With NodeZero, TTEC has moved beyond periodic snapshots and toward continuous security validation grounded in real attack paths, clear retest proof, and safer production testing. As web application coverage expands, the team is in a stronger position to find, prove, and close the next path to material risk before an attacker can use it.