HORIZON3

When the Vulnerability Backlog Stops Calling the Shots

Six daily NodeZero® tests helped a major international law firm complete more than 500 tests in eight months, cut active impacts from more than 90 to two, and fixed 530 weaknesses.

CASE STUDY

Customer *snapshot*

CUSTOMER

A major international law firm

INDUSTRY

International business law

ENVIRONMENT

More than 1,800 lawyers, over 20 offices across EMEA, clients in more than 100 countries, and a hybrid Azure and on-premises technology estate

CHAMPION

Cyber Security Lead

SOLUTION

Horizon3 NodeZero, distributed internal penetration testing, targeted retesting, exploitability prioritization, and Power BI reporting

CHALLENGE

For a firm whose service depends on trusted access to information, security risk has a direct business dimension.

Leadership needed to know which weaknesses could create material exposure, where remediation would make the greatest difference, and whether the firm's defenses were improving in practice.

The firm already had a mature security program, including Microsoft Defender, Nessus, external testing, and periodic internal penetration testing. The gap was operational: valuable findings still had to be translated into a clear order of work. As the firm's Cyber Security Lead described the previous process, results could become an exported list that teams hoped someone would review or turn into ServiceNow tickets. The organization wanted prioritization backed by evidence of real-world impact.

WHY NOW

Making testing part of the daily rhythm

The first breakthrough came when the firm made testing routine

The team moved to six NodeZero tests each day and completed at least 500 tests in eight months. That cadence gave the firm a more current view of exposure than a periodic assessment could provide, while targeted retesting showed whether remediation had changed what an attacker could do.

Turning evidence into remediation priorities

A second moment came from making the evidence useful beyond the security team. The Cyber Security Lead built a Power BI dashboard that combined Nessus, Defender, and NodeZero findings with affected devices and remediation context. An exploitability filter allowed infrastructure teams to start with weaknesses NodeZero had verified, rather than working through a broad list based only on severity. Tier 3 remediation teams could use the view themselves, without having to interpret a penetration-test report or become attack-path specialists. “You need to prioritize these ones because they are exploitable,” the Cyber Security Lead said.

“It’s already helping us prioritize what we’re trying to fix first before the other stuff.”

Tracing findings to the control gap

The third breakthrough was seeing how continuous validation could improve a control, not only identify an individual issue. Testing indicated that password spraying could compromise an Active Directory account and also surfaced an old computer-account credential. Investigation found that a blocked-password list was missing from newly created domain controllers after upgrades. The firm changed affected account passwords and began implementing Entra-based password controls, addressing the deployment gap that allowed the weakness to persist.

WHY HORIZON3

A fit with the existing security program

The firm chose NodeZero because it connected attacker validation to the security program the organization already trusted. The team could deploy runners in its hybrid environment, run autonomous internal tests at a cadence manual testing could not sustain, and bring the results into the same reporting and remediation workflows used by infrastructure teams. NodeZero became a practical decision system: it showed which weaknesses were exploitable, which devices were affected, and whether corrective action had changed the outcome.

A governed model for wider coverage

That operating model gave the firm a governed path to scale. Security leadership could establish a daily testing rhythm, make evidence available to remediation owners, and build the case for additional runner deployments across international sites. The team is also exploring broader application testing as more business services move through cloud and web-based delivery. The firm is extending coverage without separating security assurance from the operational controls that make a global professional-services organization dependable.

VERIFIABLE RESULTS

Reduced exposure with proof

Active impacts identified through testing fell from more than 90 to two, while 530 weaknesses were fixed. The team also completed 281 verification tests, giving remediation owners evidence that fixes had changed the result rather than simply closed a ticket.

A more scalable remediation model

Six daily tests and targeted retesting created a repeatable flow of evidence for security and infrastructure teams. The Power BI view connected exploitability to devices and corrective actions, making risk easier to prioritize and explain to leadership.

Stronger control assurance

The password-policy investigation showed the value of testing assumptions after infrastructure changes. The firm found a gap between the control it expected to be deployed and the control its upgraded domain controllers were enforcing, then extended remediation to the underlying process.

Together, these changes have shifted the firm from periodic assurance toward continuous, evidence-led security operations. Security can now show leadership where exposure is concentrated, remediation teams know what deserves attention first, and verification demonstrates whether the risk has actually moved.

Looking Ahead

The firm is extending the model across its international sites and considering how the same discipline can support its expanding application estate.

It has moved from asking which vulnerabilities exist to asking which risks are demonstrably actionable, who needs to act, and whether the fix worked. That is the foundation of a security program built to keep pace with a changing business, before an attacker finds the next path first.

