



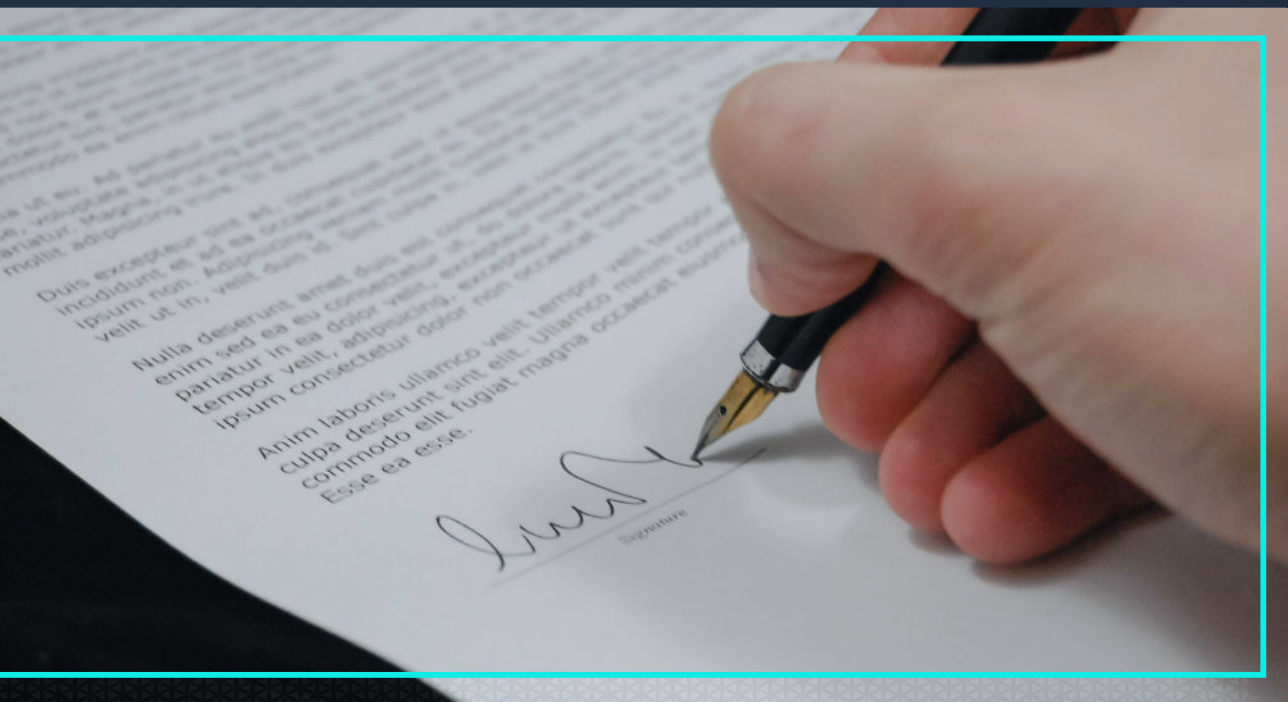
HORIZON3.ai

~~TRUST~~ BUT VERIFY

WHITE PAPER

Demonstrating DORA Resilience in the Legal Sector

How Legal Firms Can Support Financial Clients with
a CTEM-Driven, Proof-Based Security Strategy



DORA Resilience

A New Level of Scrutiny

The EU's **Digital Operational Resilience Act (DORA)** has redefined how financial institutions must manage cyber risk—not only within their own organisations but across their third-party ecosystem. As custodians of privileged information and enablers of high-value transactions, legal firms are now a critical part of that equation.

Under DORA, financial entities are expected to ensure that vendors with ICT access are resilient, secure, and continuously tested. For legal service providers, this represents a significant shift—from occasional due diligence to ongoing validation.

It's no longer acceptable to simply assert that protections are in place. Clients expect evidence, and regulators increasingly require it. Legal firms that want to remain trusted partners must demonstrate their ability to withstand the tactics, techniques, and procedures that today's attackers are actively using.

This is no longer theoretical. [Legal firms have experienced high-profile breaches](#) involving the exposure of confidential client data, privileged case files, and internal communications—many of which stemmed from phishing, insider misuse, or gaps in third-party vendor controls.

From Point-in-Time to Continuous Assurance

The heightened scrutiny of legal vendors isn't just driven by regulation—it reflects the changing nature of modern threats. Legal firms often operate with distributed access, hybrid workforces, and third-party collaboration tools, all of which expand the exploitable attack surface.

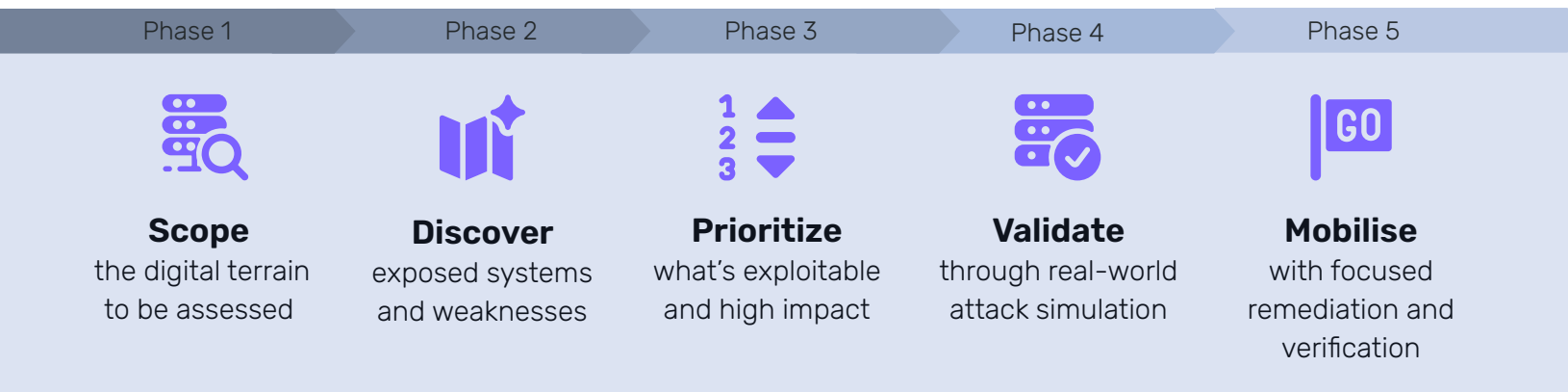
Misconfigured access controls, unsegmented internal networks, reused or compromised credentials, and phishing susceptibility have become common entry points for adversaries. Moreover, attackers often see legal firms as easier targets than the highly regulated banks and investment firms they serve.

Moreover, attackers often see legal firms as easier targets than the highly regulated banks and investment firms they serve. And regulators are taking notice: [some firms have already received formal reprimands](#) or financial penalties for failing to enforce basic cyber hygiene—particularly when outsourced IT providers or insufficiently monitored processes were involved.

To stay ahead, firms must move beyond traditional audits and vulnerability scans. What's needed is continuous, attacker-informed testing that shows what can actually be exploited—not just what might be vulnerable. That's the essence of Continuous Threat Exposure Management (CTEM).

CTEM: The Strategy Behind Real-World Resilience

Continuous Threat Exposure Management (CTEM), as defined by Gartner®, is a programme model that enables organisations to discover, validate, and reduce real-world security exposure. It's a strategic, iterative approach made up of five key phases:



For legal firms, CTEM provides a blueprint for proving resilience—not just achieving compliance. It aligns perfectly with DORA's focus on ICT risk management, operational continuity, and continuous security testing. A sound CTEM programme answers the questions regulators and clients are already asking:

- Are your vulnerabilities actually exploitable?
- Can an attacker escalate privileges or move laterally?
- What would be the impact of compromised credentials?
- Is your environment being tested regularly and realistically?
- Can you produce verified evidence of security performance?









This is where the NodeZero® platform becomes indispensable.

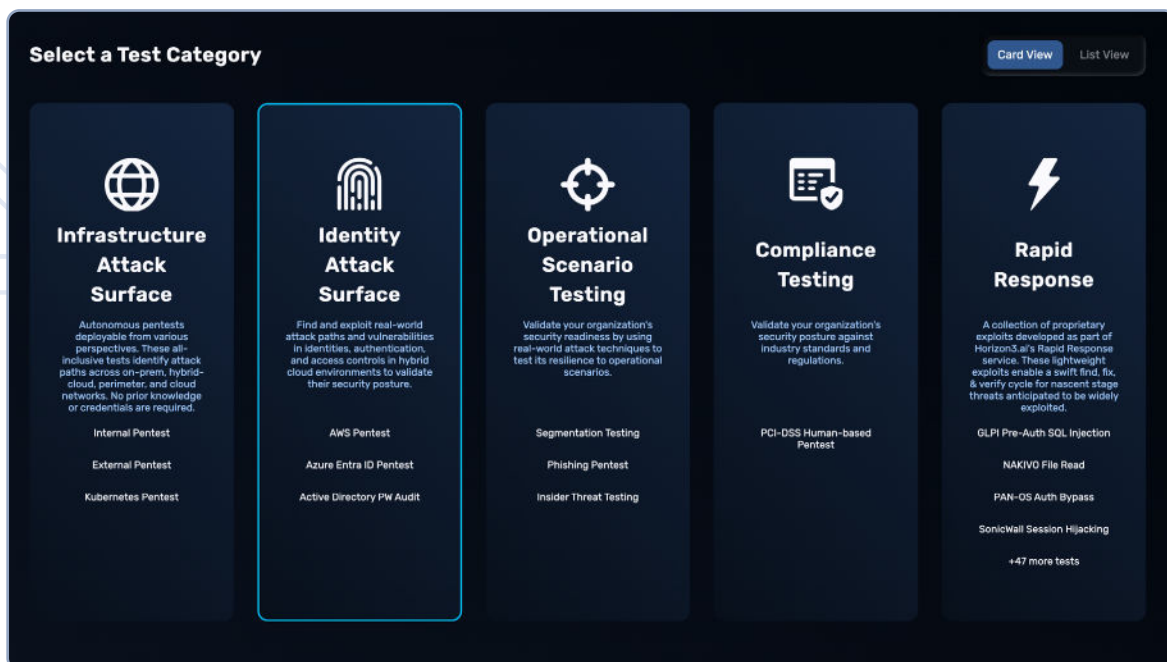
NodeZero®: Autonomous Proof of Security

NodeZero by Horizon3.ai is an autonomous penetration testing platform that behaves like an attacker—chaining together weak credentials, poor segmentation, exposed services, and unmonitored admin access to show precisely how a breach could occur.

Unlike traditional assessments, NodeZero does not rely on assumptions. It delivers proof, path, and impact for every issue it uncovers—and it does so continuously, safely, and without requiring third-party consultants or special software agents. NodeZero helps legal firms:

-  Simulate real-world attacker behaviour within their own infrastructure
-  Identify exploitable gaps in privilege escalation, segmentation, or credential reuse
-  Prioritise remediations based on actual business impact
-  Retest fixes instantly to verify effectiveness
-  Produce evidence-backed reports for audits, clients, and internal stakeholders
-  Validate outsourced IT services and managed security providers by testing their controls and processes directly

Whether identifying lateral movement opportunities after a phished login or testing segmentation between file shares and core infrastructure, NodeZero gives firms a repeatable, defensible approach to risk reduction.

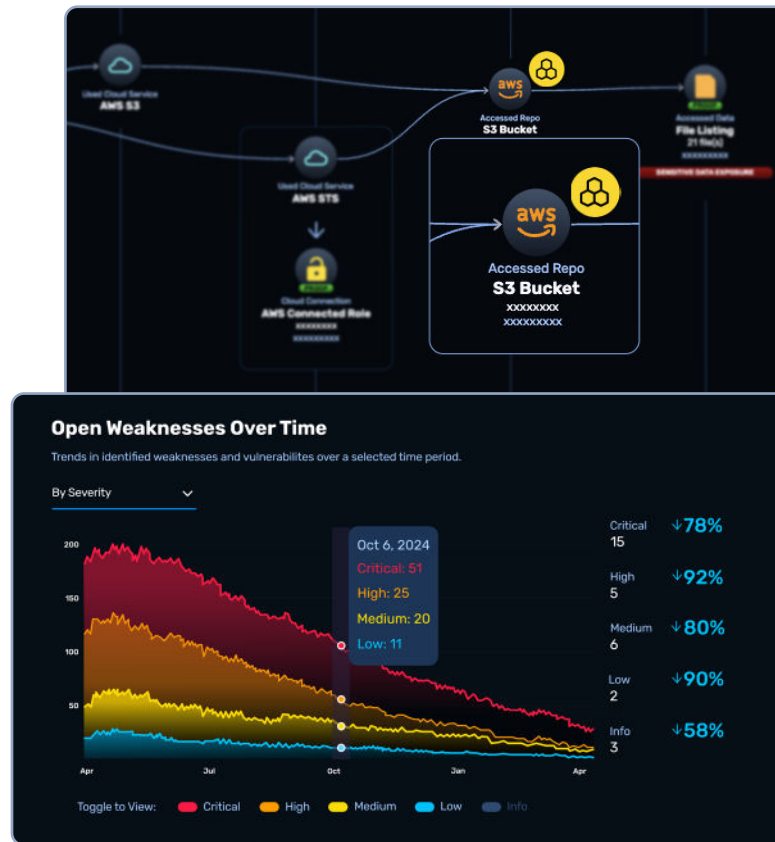


Advanced Capabilities That Raise the Bar

Several advanced features make NodeZero uniquely valuable to legal providers supporting financial institutions:

Tripwires™ deploy deception artefacts—such as fake credentials or files—along discovered attack paths. If an attacker or malicious insider interacts with these decoys, NodeZero sends immediate alerts with minimal false positives.

NodeZero Insights™ converts detailed findings into board-ready dashboards and KPIs. Security leaders can monitor trends like mean-time-to-remediation, open exploit paths, and systemic issues—providing clear visibility into progress over time.



Move Beyond Compliance. Deliver Confidence.

Legal firms are no longer adjacent to financial sector resilience—they are central to it. As DORA takes hold, firms must be able to prove their readiness to clients and regulators alike.

NodeZero makes that possible—offering continuous, autonomous validation of security posture through adversary simulation and real-world testing. It allows legal teams to move from theoretical risk assessments to actionable proof of resilience.

840
Impacts

677
Weaknesses

706
Credentials

1K
Protected Data Items

84
Compromised Hosts

In doing so, NodeZero helps legal providers not just maintain compliance, but earn trust, win business, and play a proactive role in safeguarding their clients' operations.

