FORESITE CYBERSECURITY

The Needle They Almost Missed

Foresite Cybersecurity

When a clean pentest is not a clean environment

Autonomous Penetration Testing Case Study

Revised: June 05, 2026

Version: 26.06.05

Executive Summary

A healthcare organization that handles regulated member data ran annual penetration tests for more than a year. Every one came back clean. The compliance boxes were checked, the program was well run, and by every available indicator the environment was secure.

Then Foresite ran an internal test using the NodeZero autonomous penetration testing platform. In 17 hours, with no human attacker and no prior knowledge of the environment, NodeZero exploited 254 attack paths, compromised 319 credentials, and accessed 739 items of protected personally identifiable information, including Social Security Numbers and Individual Taxpayer Identification Numbers.

The exposure was not new. It had been reachable from any foothold inside the network through every prior clean test. This case study examines what NodeZero found, why more than a year of testing missed it, and why the only reliable answer is to test as often as possible.

254 attack paths. 319 credentials. 739 PII items.

17 hours. One autonomous platform. No human attacker.

Overall exposure level: HIGH, confirmed via Foresite NodeZero internal pentest

The Needle in the Haystack Problem

Why clean tests are not the same as a clean environment

A clean penetration test means the weakness was not found inside that engagement window. It does not mean the weakness is not there.

Traditional testing, even strong manual testing, works within constraints. Testers operate inside a defined scope and time window and follow established methodologies. No tester can simultaneously evaluate every credential, every protocol, every relay opportunity, and every attack-chain combination across roughly 100 hosts in a single engagement.

The weaknesses NodeZero surfaced were not recent. SMB signing had not been required for years. Shared service account passwords had not been rotated. The NTLM coercion attack surface had existed since the domain was built. What changed was the tool used to look, and its ability to chain conditions together autonomously that a human tester might evaluate individually but never connect.

The rescan that disappeared

After reviewing the findings, the organization ran a follow-up scan two weeks later without remediating anything. It came back clean. No critical findings, no compromised credentials, no path to host compromise. Nothing had been fixed.

NodeZero's NTLM relay chains depend on timing, active sessions, and the real-time availability of relay targets. A domain controller processing authentication at the right moment on day one was not doing so on day fifteen. The attack path closed temporarily. The underlying misconfiguration was completely unchanged.

This is exactly how real attackers behave. They do not run one scan and accept a clean result. They probe continuously, wait, and try again when conditions shift.

The frequency argument

Point-in-time testing, regardless of quality, is structurally incapable of catching conditions that are transient, timing-dependent, or that require chaining a large number of simultaneous variables. The reliable answer is frequency.

Running weekly rather than annually means sampling 52 sets of conditions a year instead of one. For timing-dependent chains like NTLM relay, frequency is the mechanism by which the platform works.

What NodeZero Found

NodeZero did not find one catastrophic flaw. It found three systemic weaknesses that amplified each other, the same pattern a capable attacker would identify and chain. Each is manageable alone. Together they produced full domain-level access to live PII in under 17 hours.

Root cause 1: Weak and reused credentials

NodeZero cracked 32 credentials with standard dictionary attacks, including cleartext passwords on accounts named after internal business units and partners. Three domain service accounts responsible for database replication, scheduled jobs, and backups shared a single password. One privileged account was cracked in under eight minutes, and that one compromise led directly to domain user compromise, ransomware exposure on two file stores, and sensitive data access across seven assets.

- 32 credentials cracked via dictionary attack
- 3 domain service accounts confirmed sharing one password
- 140 instances of local credential reuse across database infrastructure
- 1 shared local administrator account working across unrelated hosts
- 1 privileged account cracked in under 8 minutes

Root cause 2: SMB signing not required, combined with NTLM coercion

NodeZero confirmed three NTLM coercion techniques against the domain controllers: Authenticated PetitPotam (MS-EFSRPC), DFSCoerce (MS-DFSNM), and PrinterBug (MS-RPRN). Each forced a domain controller to authenticate back to NodeZero, handing over its machine account hash. Because SMB signing was not required on 76 services across the environment, those hashes were relayed straight to other hosts with no password cracking needed.

Several of these protocols are designated no-fix issues by Microsoft. The defense is configuration, not patching: enforce SMB signing environment-wide and apply RPC filters. Neither had been done. The attack surface had been present and exploitable through every prior clean test.

- 76 services found with SMB signing not required
- 3 domain controllers confirmed vulnerable to NTLM coercion
- Machine account credentials for all three domain controllers captured via relay
- 19 hosts compromised through relay attack alone

Root cause 3: Inadequate endpoint security controls

NodeZero acquired 137 credentials through OS credential dumping, reaching the Windows Security Account Manager database and LSASS memory on compromised hosts. Endpoint detection and response was either absent or insufficiently tuned to block common credential harvesting. Even after passwords are reset, an environment without effective EDR will have its credentials harvested again within hours of the next attacker foothold.

The Data Exposure That Makes This a Breach Scenario

NodeZero accessed 739 items of personally identifiable information, specifically Social Security Numbers and Individual Taxpayer Identification Numbers, via compromised credentials on SMB file shares. One share held more than 51,000 files with read, write, and delete permissions accessible to a single compromised service account.

Under HIPAA, unauthorized access to protected health information is a breach that triggers notification to affected individuals, to the Department of Health and Human Services, and in some cases to the media. NodeZero showed that access was not only possible but trivially achievable from any foothold inside the network, and that it had been achievable throughout more than a year of clean testing.

Had this been a real attacker rather than an autonomous platform, the organization likely would not have known until members reported identity theft or a ransom note appeared on the file servers. The prior clean tests would have given no warning.

Why Frequency Changes Everything

The vCISO lesson

Foresite serves clients as a virtual CISO, providing strategic leadership, program oversight, policy development, and compliance guidance. The program here was well run by any reasonable standard. The exposure existed anyway.

No program, however well designed, can compensate for testing that samples conditions once or twice a year. The vCISO provides strategy, governance, and program architecture. Continuous autonomous validation provides the ground truth about whether that program is actually working at any given moment.

Compliance vs actual security posture

Annual penetration testing satisfies the HIPAA Security Rule requirement for technical evaluation. It produces a report, a finding list, and a remediation plan, all of which satisfy an auditor. None of it prevented this organization from carrying exploitable access to 739 PII items through more than a year of compliant testing.

Compliance and security are not the same thing. This engagement is the proof. Continuous autonomous validation is what closes the gap between them.

Recommended Remediation Path

Foresite built a prioritized roadmap that addresses root causes in order of leverage. Each fix reduces the blast radius of the rest.

Immediate

- Rotate every compromised credential identified in the findings
- Enable and require SMB signing via Group Policy across all domain-joined systems
- Apply RPC filters for MS-EFSRPC and MS-DFSNM on domain controllers
- Disable the Print Spooler service on all non-print servers

Short term, within 30 days

- Migrate service accounts to Group Managed Service Accounts to eliminate shared and manually managed passwords
- Deploy LAPS for all local administrator accounts
- Enforce a 12-character minimum password length via domain policy
- Verify EDR deployment and enable credential-harvesting prevention on every host

Ongoing

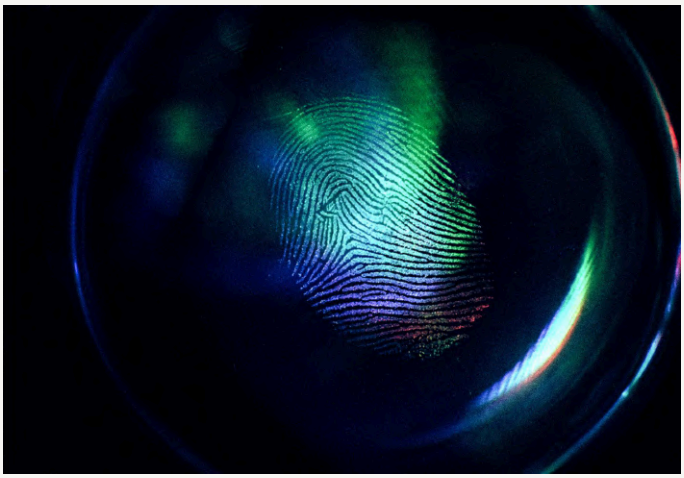
- Enable Extended Protection for Authentication on AD CS
- Disable NTLM where possible and audit NTLM usage
- Run NodeZero on a continuous schedule, weekly at minimum, to catch configuration drift and verify closure
- Establish a formal fix, rescan, document workflow so every remediation is verified before it is closed

The Foresite and NodeZero Difference

Foresite delivers NodeZero-powered autonomous penetration testing as part of its vCISO and continuous security validation services. The combination provides what neither delivers alone: strategic security leadership grounded in real-time, proven evidence of what is actually exploitable right now.

The value is not the report. The value is the loop. Find, fix, verify, repeat, running continuously while the vCISO program focuses on strategy, governance, and the bigger picture.

- Autonomous internal and external testing powered by NodeZero
- Proof-of-exploit documentation for every finding, not theoretical risk scores
- Immediate rescan after remediation, no scheduling and no waiting
- Continuous coverage that catches what annual tests miss
- vCISO integration, so strategy and ground truth work together
- Aligned to HIPAA, SOC 2, ISO 27001, and NIST CSF validation requirements



Foresite, Award-Winning Security

To see what continuous security validation finds in your environment, contact us at soc@foresite.com or visit foresite.com to learn more about Autonomous Penetration Testing.

NodeZero BY HORIZON3.ai