HORIZON3

How a Manufacturer Turned a Password Audit into a Company-Wide Security Reset

A North American manufacturer used NodeZero® to surface 115 added findings, expose 75 critical findings and 75 attack paths across fewer than 120 hosts, and show that 31% of users had crackable passwords, giving the security team the proof it needed to drive action across sites.

Customer *snapshot*

CUSTOMER

North American manufacturer

INDUSTRY

Manufacturing

ENVIRONMENT

Legacy systems, site-level administration, operational environments, distributed local and domain account management

CHAMPION

Security leadership team

SOLUTION

Horizon3 NodeZero

CHALLENGE

This manufacturer operates in the kind of environment many security leaders know well, established systems, local site autonomy, and operational teams that need continuity as much as control. In settings like that, older accounts, service credentials, and legacy defaults can persist longer than anyone would like, especially when they are tied to systems that people rely on every day.

The team was not starting from scratch. They had already been running penetration tests and reviewing the results. What they needed was a clearer way to show operational leaders why certain findings mattered now. The issue was not a lack of awareness. It was a lack of shared urgency across sites. Without a more concrete picture of consequence, known weaknesses could still be treated as isolated technical issues rather than the beginning of a broader attack path.

WHY NOW

The first shift came when the team used stronger credential perspectives and compared the latest results against earlier runs. The updated comparison surfaced 115 added findings, including 75 criticals and 75 attack paths across fewer than 120 hosts. What had previously looked like separate issues now looked like connected paths an attacker could use to move deeper into the environment.

A second moment came from running a AD Password Audit test. NodeZero showed that 31% of users had crackable passwords, including accounts that matched entries from the worst 100 password list. That changed the internal conversation. Weak passwords were no longer a policy concern on paper. They were direct evidence of exposure tied to real accounts and real access.

The turning point was not simply that the platform found more. It was that the team could connect password weakness and legacy account sprawl to actual attack paths. In an environment where older local and domain accounts could still hold more privilege than intended, that proof made the potential blast radius visible. Once the risk was clear, leaders across the organization had a stronger basis to act.

WHY HORIZON3

The company needed more than a testing tool. It needed a way to turn findings into a remediation process the wider organization could understand and repeat. NodeZero gave the team that structure.

They began prioritizing critical findings in Vulnerability Management Hub, starting with the domain and host issues most likely to collapse large concentrations of risk. From there, the plan was to use 1-Click Verify to retest specific attack paths after mitigations were in place. That created a more disciplined operating rhythm, one that helped the security team move from reporting issues to demonstrating whether exposure was actually shrinking over time.

Just as important, the platform helped the team communicate risk in a way that fit the business. Instead of asking site leaders to react to abstract findings, they could show how seemingly routine weaknesses could contribute to a larger compromise path. That made remediation easier to prioritize and easier to defend.

VERIFIABLE RESULTS

The most immediate result was clarity. Stronger credential testing surfaced 115 added findings, 75 critical findings, and 75 attack paths across a limited host scope, giving the organization a more realistic picture of where concentrated risk lived.

The AD Password Audit added another layer of proof. By showing that nearly a third of users had crackable passwords, the team had the evidence needed to begin enforcing password changes and preparing clearer formal password guidance for operational teams.

The broader result was programmatic. Critical-first remediation in Vulnerability Management Hub created a more credible path to reduce exposure, and planned retesting with 1-Click Verify gave the company a way to measure whether fixes were holding. What changed was not just the findings list. The organization now had a stronger process for aligning site leaders, escalating action, and proving progress.

LOOKING AHEAD

The team is now moving from discovery to sustained validation. Next steps include closing the highest-risk weaknesses first, reinforcing password policy across operational teams, continuing to test with stronger credential perspectives, and using regular reviews plus targeted retesting to confirm that exposure is trending down.

That leaves the manufacturer in a fundamentally stronger position, with a clearer view of where risk starts, how it spreads, and how to prove it is being reduced.