HORIZON3

From Lockout to Insight: How a Large Real Estate Company Turned NodeZero® Findings into Immediate Action

A testing issue with a locked SQL sa account led this U.S. real estate company to a deeper privilege path, exposed risky service-account patterns through NodeZero's AD Password Audit, and helped the team move from symptom to remediation with clear ownership.

CASE STUDY

Customer *snapshot*

CUSTOMER

Large U.S. real estate company

INDUSTRY

Real estate

CHAMPION

Security and infrastructure team

SOLUTION

Horizon3 NodeZero and AD Password Audit

CHALLENGE

For a real estate company with roughly 900 employees, core business systems depend on stable identity, database, and administrative infrastructure. That creates a practical challenge for security teams. They are not only defending internet-facing assets or user endpoints, they are also responsible for the quieter layers of privilege that support line-of-business systems behind the scenes.

That tension surfaced during testing when the team noticed a SQL sa account was getting locked out. On its face, it looked like the kind of issue a team might work around to keep a test moving. Instead, they treated it as a signal. NodeZero showed that the lockout was only the symptom. The more important issue was an attack path involving an overprivileged ADFS-related account that allowed access to the SQL sa hash. What first appeared to be test friction was evidence of a real privilege problem with clear implications for identity security and lateral movement.

WHY HORIZON3

The value of NodeZero here was not simply that it found weaknesses. It showed the team how those weaknesses connected. By validating that a SQL lockout pointed to a deeper privilege issue, the platform helped the organization avoid treating the symptom as the problem. That matters in mature environments, where teams often have no shortage of alerts but still need proof of which conditions create meaningful attack paths.

NodeZero also gave the team a practical way to extend that same logic into credential risk. The AD Password Audit translated weak and repeated service-account passwords into findings the team could act on immediately. For a technical security audience, that is the operational difference that matters most: evidence tied to exploitability, clear prioritization, and findings specific enough that owners can move without another round of interpretation.

VERIFIABLE RESULTS

The most credible result was the speed and clarity of response.

Before NodeZero, testing had surfaced symptoms, but the root cause behind the SQL issue was still unclear. After NodeZero, the team understood that the lockout pointed to an exploitable privilege path involving an overprivileged ADFS-related account and access to the SQL sa hash.

Before the password audit, service-account password risk had not been exposed in a way that forced action. After the audit, the team could see crackable passwords, repeated patterns, shared credentials, and high-risk service accounts with domain admin rights. That visibility translated directly into prioritization.

Most importantly, the organization moved quickly from finding to ownership. Instead of debating whether the issue mattered, the team assigned remediation responsibility in the moment and began addressing the highest-risk accounts right away. That is a meaningful shift in program maturity. The security team was no longer reacting to isolated indicators, it was using attacker-valid evidence to drive faster, more accountable remediation.

LOOKING AHEAD

For this organization, the next step is not simply to repeat the same tests. It is to keep using attacker-grounded validation to uncover privilege relationships and credential exposures before they become larger incidents.

The team has already shown the mindset that matters most: when a symptom appears, they follow it to the underlying path, assign ownership fast, and fix what an attacker could actually use.