HORIZON3.ai

~~TRUST BUT~~ VERIFY

CASE STUDY

Healthcare Staffing Organization Puts Cybersecurity Best Practices in Place with NodeZero

Healthcare Staffing Organization Puts Cybersecurity Best Practices in Place with NodeZero

The director of security engineering at a national healthcare staffing organization grew up wanting to be a hacker, and he found that NodeZero's ability to provide the attacker's perspective to help better protect his organization was a perfect fit for keeping his organization safe.

"Security has always been on my mind. Protecting company assets have always been on my mind. We'd reached a point where our organization is big enough, people are working remotely, and I wanted to split off some of my roles and be ultimately dedicated to security," he says.

One of the challenges he has faced over the years has been convincing the c-suite to focus on security. They always had compliance in mind and policies in place, but the organization struggles with aging software without a development cycle or vendors who didn't support software when it aged out or broke down.

As a publicly traded company, they ran their annual penetration tests on their roughly 900-1,200 hosts and performed well – they had a strong firewall in place protecting them from outside threats.

"But we have ancient software inside, and one of the great things about NodeZero is that it's internally focused. In my mind, that's where the threats will come from," he says.

The first time he ran NodeZero, it was able to obtain domain admin access in 17 minutes via an overlooked machine that shared a password with other machines. It also surfaced risks and vulnerabilities that those aging machines and systems internally may have otherwise made difficult to find.

> **We have folks, who have come and gone, who may have built servers I'm not aware of, that we don't know about until NodeZero finds them, finds the misconfigurations, and helps us remediate them,"** he says.

HORIZON3.ai ~~TRUST BUT~~ VERIFY

Immediate, actionable results

Before NodeZero, the organization would run one external pentest and one scan to check on their remediation actions. The pentest would, regardless of vendor, use the same tools.

“You get a PDF telling your execs how you suck, and 99 percent of the stuff that says you suck are things that are such low priority you don’t care about them,” he says. **“I love that with NodeZero, those are identified as low-priority, such as expired SSL certs, very minor things.”**

Because other options all felt cookie cutter, with no difference in quality, leadership simply wanted the cheapest, easiest option to check that box. Cost was always a struggle – with security being seen as an annoying expense – until a key leader re-joined the company having survived a ransomware attack with his previous organization who now had security at top of mind.

“He asked, what are you missing? I told him endpoint protection, and we had the contract signed the next day,” he says.

When it came time for addressing pentesting, there was some pushback between the dev and infrastructure teams, but once they ran a demo of NodeZero, the teams fell in line.

> **I showed the demo to our network guy, who’s as big a cynic as I am and he was blown away, saying ‘this is what we need,’”** he says.

This was all happening right around the time the Log4Shell vulnerability was the talk of the cybersecurity world.

“Log4j was everywhere,” he says, but running NodeZero offered actionable mitigation right away, whereas other tools they were using at the time had a lag time of weeks.

From once a year to once a month

The organization now runs NodeZero once a month, and then retests mid-month. With NodeZero they're able to show progress better than ever before.

"Audit and compliance guys would look at the number of vulnerabilities in a 90-day period and say the numbers have gone up, you haven't fixed anything," he says. "But we're able to show them that these are new weaknesses, and that new vulnerabilities come up all the time. We're not being measured against those 90 days, and we can compare in the middle of the month to see what's been fixed."

In fact, with NodeZero running, the only issues his team has not fixed are due to manpower, not because of testing.

"Honestly, anything that hasn't been addressed is a resource issue on our side," he explained.

And, NodeZero has helped improve their results from other tools and resources. They were able to improve notification of attacks from their MSSP from four hours to fifteen minutes and validated their endpoint protection by verifying that the pentests are immediately detected and alerts issued – all enabling them to get more out of existing expenditures.

NodeZero has improved their overall accuracy, such as identifying a false positive that came up time and again with Adobe Flash that was no longer being used but could not be removed from some older machines.

Doing things other vendors don’t

“I don’t think you have any other competitors,” he says. “I’d a have to go out and get a red team to do what NodeZero does, and it would cost twice as much for one scan.”

He also appreciates that NodeZero doesn’t just stop when it finds a vulnerability – it keeps digging.

> **It chains attacks, which other pentesters don’t do,” he says. “Hackers don’t say hey, I got access to this, I’ll stop here. That’s not how they operate.”**

As a once-aspiring hacker himself, their director of security engineering knows that anyone who says they are 100% secure is either dishonest or naïve.

“You are going to get breached. It’s going to happen,” he says. “But the more you understand, the better you can lock things down and limit the blast radius.”

How NodeZero Can Help

- **If you’d like to see how NodeZero works with your organization, have our experts walk you through a demo**
  https://www.horizon3.ai/demo

HORIZON3.ai ~~TRUST BUT~~ VERIFY