



HORIZON3.ai

~~TRUST~~ BUT VERIFY

CASE STUDY

NodeZero: Filling a Unique Niche in Cybersecurity

Management Consulting Organization Case Study



Filling a Unique Niche in Cybersecurity

When an IT and cybersecurity team from a U.S.-based management consulting organization were searching for ways to improve their penetration testing, NodeZero and Horizon3.ai were able to answer the call.

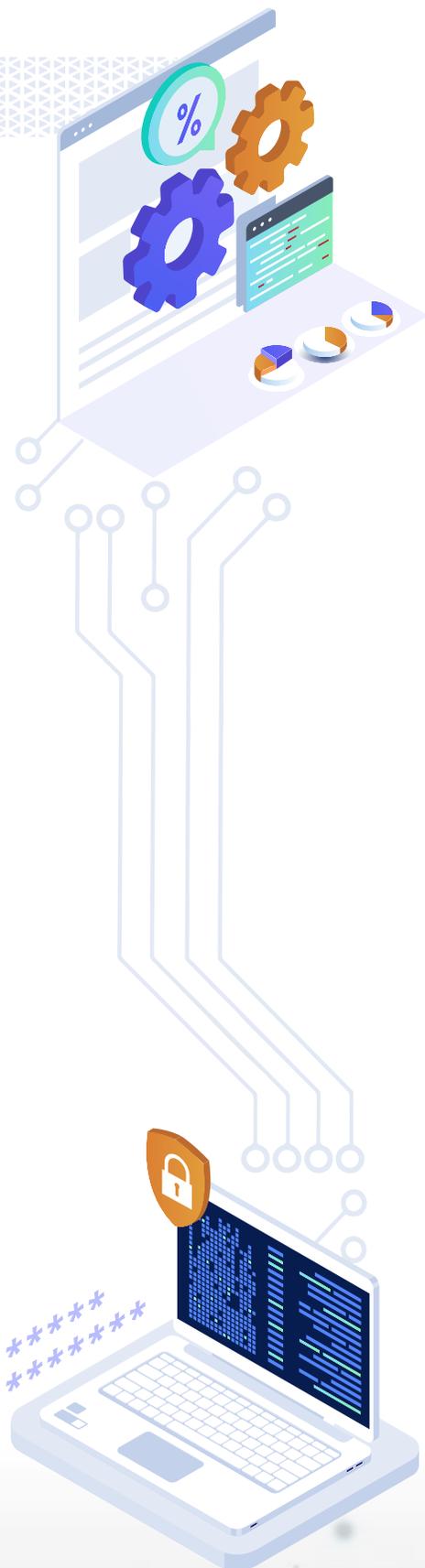
“We’d done some penetration testing in the past, and it was quite expensive,” says the organization’s infrastructure manager. “We were looking to do this on a more regular cadence and looking at different solutions we could implement.”

After running into a team member from Horizon3.ai, they shared a rundown of what they were looking for and felt that NodeZero might be just what the situation called for.

“**I liked the ease of implementation and use of the product,” he says. “And the ability to just do constant scanning and fixes without having to pay for every instance was the biggest appeal.”**

The organization’s director of IT noted that there were solutions he’d encountered that could do external pentesting, but what they really needed at this stage was powerful internal pentesting capabilities.

“Looking at vulnerabilities and criticality was key for us,” he says. “And the biggest thing for me was having a full-package pentest, with all the functionality you needed to really look for and tackle vulnerabilities accordingly.”



The struggle to keep up

The organization's biggest struggle at the time was simply being able to keep up with a small team – they didn't have a dedicated team member to keep up with alerts and investigations.

"We wanted to be able to identify vulnerabilities ahead of time and keep ahead of the game," says their infrastructure manager. "In the past, when we were doing scans, we were able to identify issues – fortunately none required significant time to fix – but being able to identify those things and act on them before they can be exploited is huge for us with a small team."

“In looking at and enforcing our security strategy, we’re trying to implement controls – and with NodeZero, we’re able to implement the right controls and software we need to better our environment,” says their director of IT.

This also helps with various compliance requirements, a key component to the security team's mission, as well as uncover any major vulnerabilities in the environment.

More frequent testing

The team wanted to be able to go in and do internal ops more often, something NodeZero makes uniquely possible.

“Being able to perform on-demand scans is really great – we can scan, make adjustments, and then run another scan to verify we’ve been successful,” says their infrastructure manager.

“We’re taking security to a higher level within the organization to obtain certifications in compliance, and this is going to help with that a lot,” says their director of IT.





Cost effectiveness and efficiency

One of the strongest draws to NodeZero was the ability to run those repeated pentest operations anytime and anywhere they needed them – without incurring additional costs.

“It’s just much more cost effective and easier to deal with the licensing,” says their infrastructure manager.

And to be able to run those operations for internal pentesting set it apart from other options on the market, says their director of IT.

“It’s one thing attacking an organization from the outside, but when attacking from the inside, you need to understand it and have the capabilities to do it,” he says. “I feel NodeZero has the capacity to do that.”

Getting up and running with NodeZero was quick and easy rather than adding cycles to a team that was already running lean.

“Setting up a scan is relatively quick and painless to do,” says their infrastructure manager.

“And even the reports are very intuitive – what the report surfaces and what we need to do to mitigate that,” says their director of IT.

It’s also enabled a frequency of testing they wanted, rather than being limited by the time and cost of standard penetration tests. Before NodeZero, the organization conducted pentests once or twice a year. They already plan to increase this to quarterly, or more – maximizing their return on investment.

NodeZero enables customers to turn a small team into their own seasoned and veteran team.

“It takes a lot of the work our team would have to go through to conduct these investigations, finds vulnerabilities and tells us what needs to happen, and even ranks those vulnerabilities and tells us why something should be considered more urgent than others,” says their infrastructure manager. “It helps prioritize work for optimal impact and address those issues that are going to be critical to our environment soonest.”

“NodeZero, I think, fills a huge missing niche. Not just the skill set or background of company but the actual product, enabling you to do internal and external vulnerability testing to mitigate the issues most people are facing,” says their director of IT.

▶ **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>

