HORIZON3.ai

~~TRUST BUT~~ VERIFY

CASE STUDY

Securing the Move: Cyber Resilience in the Transportation and Supply Chain Industry

@Horizon3ai info@horizon3.ai www.horizon3.ai

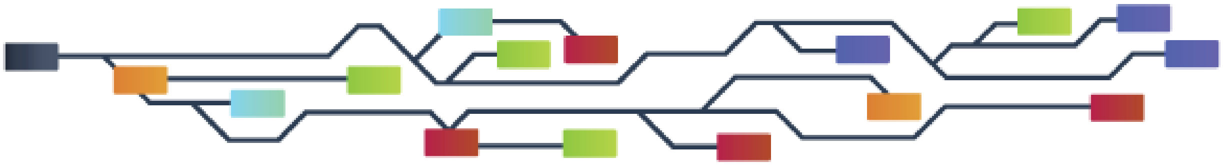
How a Prevailing Transportation Company Modernized Security with NodeZero

Cyber protection is crucial for the transportation industry and the supply chain because it ensures the seamless flow of goods, prevents disruptions, and preserves the integrity of critical data essential for global commerce. Horizon3.ai recently interviewed one of our transportation and logistics customers that is deeply rooted in the fabric of American commerce. As a major player in the national supply chain arena, the customer continues to forge an excellent reputation through their innovative supply chain solutions and commitment to environmentally conscious trucking practices. Embracing innovative technology, they continue to optimize their logistics operations and ensure the seamless movement of goods while reducing their carbon footprint.

Mission:

Addressing their customers' transportation requirements and needs by offering transportation services around the world.

- **Year Founded:** Mid 1900's
- **Number of Employees:** 6,500
- **Operational Reach:** Global



In tandem with their commitment to sustainable logistics, they also remain vigilant in safeguarding their cyber operations against evolving threats. Implementing robust cybersecurity protocols and investing in state-of-the-art technologies that help find threats, fix weaknesses, and verify fixes before they are an issue is paramount. This also allows them to fortify their digital infrastructure to protect sensitive data and ensure uninterrupted operations. By prioritizing cybersecurity measures, the customer not only secures their own network but also upholds the trust and confidence of their clients, reinforcing their position as a reliable and forward-thinking leader in the transportation and logistics landscape.

Too Many Alerts, Not Enough Action

Vulnerability scanners are very good at pointing to and explaining what a vulnerability is, but often lack actionable insights. This leads to an abundance of alerts while also potentially overwhelming teams and impeding effective response. Our transportation client discovered just that. Their existing vulnerability scanning and management tools were insufficient and highly time-consuming, leading to their security teams not knowing which issues were a priority and needed fixed immediately.

The tools created a lot of noise and led to alert fatigue, explained Henry, one of their Cybersecurity Analysts. The scan results mostly pointed to proof of concept (POC) vulnerabilities that **"weren't even things that could be actively exploited,"** he explains. These tools often operate by scanning the client's setup, cross-referencing it with a list of vulnerabilities, and highlighting disparities. However, this approach lacked the essential depth and sophistication (or proof) essential to know what to fix first, requiring their team to spend time researching each vulnerability and how it relates to their environment.

Moreover, it failed to enable them to see and tackle the most critical issues foremost. Henry stresses that beyond identifying vulnerabilities, **"understanding what elements in our environment that are exploitable and having evidence of how these vulnerabilities were exploited [proof] is crucial."** This information is key in effectively prioritizing issues and important in determining which ones to address first.

Vulnerability scanners often offer valuable information but fall short of actionable items for security teams to prioritize and fix. They are great at listing which vulnerabilities exist within your environment, but lack the clarity, explanations, and proof required for action. **"It was hard trying to communicate that to our team,"** Henry adds, saying that **"despite the need to take immediate action, our lack of a clear and actionable plan from our vulnerability scanner left us uncertain about how to prioritize the identified issues and which items needed addressed first."**

> **"I keep going back to the actionable proof, because that has really been the value for us."**

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Happy Cybersecurity, Means Happy Vendors and Clients

Being a leader in the transportation and supply chain industry, protecting sensitive customer information, proprietary logistics and inventory details, financial transactions, route plans, shipment schedules, and operational and communication data is extremely important in maintaining the efficiency and security of the entire supply chain network. Vendors and customers want to know that their sensitive information is safe from cyber criminals and possible cyber-attacks, and that the company has their back. They want to know that the company has their best interests at heart and takes cyber threats seriously by using a proactive approach and maintaining cyber resilience.

How does a company do this? One of the most effective ways to ensure an organization's digital infrastructure is protected and resilient against cyber threats is by implementing an autonomous pentesting solution across their entire environment. Doing this involves integrating tools or platforms that constantly conduct regular and ongoing security assessments, while also falling in line with regulatory compliance standards. Our client understands the need to shift from their current scan and patch (traditional vulnerability scanning tools) mindset and move to autonomous security solutions that *Find, Fix, and Verify* remediations/mitigations immediately and continuously.

Additional to building a cyber resilient digital realm, Henry states that easy and direct access to the precise proof of exploitation is instrumental and allows for immediate sharing with peers and vendors. **"Having that proof comes in really handy when sharing with our vendors to say hey, this wasn't detected [by their software] and is there anything we can do to modify our Indicators of Compromise (IOC) or our Indicators of Attack (IOA) so we can detect this activity in the future?"** he adds. Having direct access to this information allows a client running a continuous pentesting solution the ability to find holes in their current security tools and enables them to contact their third-party vendors to fix gaps and harden security.

Enter NodeZero™

Our client wanted to get away from basic vulnerability scanners and adopt something that emulated attacks across their environment. After doing open-source research, Henry and his team ran across NodeZero on LinkedIn™ and started watching Horizon3.ai videos on YouTube™.

What impressed him the most was that our

> **CEO was very active, and he knew the product very well, which really stood out.**

So, they booked a demo.

Henry mentions that some of our competitors were reluctant to schedule a Proof of Value (POV), and that our onboarding/POV process was transparent, which was the main driving factor for going with Horizon3.ai. Furthermore, initial real-world impressions highlighted that the NodeZero interface was sleek and easy to use, especially when compared to traditional manual pentest and vulnerability scanning tools. Running a pentest was "quick and there are multiple methods for the reporting, which is really valuable to us" he mentions.

Not just for the Vulnerabilities

Henry says that NodeZero has **"everything, from the reporting to the one click verify, being able to quickly identify if we remediated this or not [vulnerabilities],"** adding that, **"those things really help outshine some of the other competitors."** NodeZero allows customers to see a prioritized list of vulnerabilities, proof of exploitation (if available), and highlights notable events to enable customers to fix what matters first, and to verify those fixes.

NodeZero also provided detailed attack paths that enable customers to walk through how an attack could be carried out through the Eyes of an Attacker, while also showing which vulnerabilities led to specific downstream impacts and what to fix to mitigate other issues throughout the environment. He says that everything NodeZero provides is **"really, really helpful, and showing the top weaknesses in our environment with proof of exploitation so that me and my team could manually run the commands was really impressive."**

Furthermore, **"the fix actions report is super helpful because I was able to attach it to a ticket and send it off"** saving Henry valuable time from calling multiple people and walking them through how to do fix the issue and remediate the vulnerability. NodeZero reports not only give the customer step-by-step instructions, but also provides multiple options to fix the same problem. **"Being able to mitigate this in multiple ways really cuts down on me having to do research on the back end,"** he adds.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Filling the gaps, Hardening policies

After the first few pentests, Henry mentions that the results weren't too shocking, especially when NodeZero found multiple weak credentials, as they had just done a pentest from another vendor a few weeks prior. However, after the third week of using NodeZero, it was able to escalate its privileges to become domain admin, effectively taking over the domain because a temporary account was created with default credentials. He was surprised by how quickly NodeZero was able to "shed light on the issue and provide immediate remediation instructions."

Additionally, this issue prompted his team to not only quickly remediate but help fine tune their parent company's current Identity and Access Management (IAM) policies and guidelines, in addition to their own. Although the temporary account was created by a systems admin, NodeZero finding the vulnerability allows for visibility and mitigation to ensure compliance with System and Organization Controls (SOC) and future audits. He also mentions that "they [him and his team] got to actually see domain admin compromise and what that would look like, as well as what sort of things [downstream impacts] would be pivoted into from obtaining those escalated privileges, which was very interesting."

This example illustrates that, even if a company thinks they are complying and adhering to their current policies, there can still be gaps and credentials that get through the cracks. Henry emphasized that they thought they were doing a good job by following established IAM guidelines and policies. However, when NodeZero was introduced into their environment, they quickly discovered **"that's not necessarily true and some things like service accounts and similar had slipped through the cracks."** Furthermore, he goes on to say that these types of IT department and admin level accounts **"were not subject to quarterly password resets, so NodeZero helped us figure out those accounts, keeping us in the know."**

Reducing Cost, Increasing Business Operations

As many of our customers have highlighted after switching over to NodeZero from traditional annual and/or manual pentesting is the significant reduction in per pentest cost. As Henry describes, "we are well below the cost of just a single annual pentest and are getting way more pentests per year, which is somewhere near 90% cost effectiveness and that NodeZero has more than paid for itself already." He goes on to say that "only a few things from our previous annual pentest were solved because the report wasn't good [lacked effective fix actions] or not many people were tracking it, so there just wasn't a lot of helpful information."

As a result, NodeZero has helped Henry and his team accelerate, justify, and steer their company into additional cyber operations that they otherwise wouldn't have been able to do with a once-a-year annual pentest. **"This not only helps us reduce risk, but has also helped us make better investment decisions,"** he mentions.

> Even if you're not going with NodeZero, I would highly recommend that you do.

NodeZero revolutionizes the landscape for organizations seeking an autonomous pentesting solution, empowering a proactive and preemptive strategy to illuminate how an attacker sees your environment and reinforce resilience against cyber threats. Henry says that **"even if you weren't going with NodeZero, you need to get some kind of attack emulation exercise going, because we didn't realize that we needed that until we had it."**

Subsequently, Henry and his team realized how valuable it is to see things from an attacker's perspective, as well as gaining a lot more perspective into their defensive and offensive posture. **"We like seeing how NodeZero moved like an attacker through our environment, as well as the narrative and context that it provided, allowing us to actually determine what is more likely to happen, and more likely not to happen,"** says Henry.

Some organizations don't realize the value of continuous pentesting until it's too late and they have a breach or are paying millions of dollars in ransom. For the transportation and supply chain industry, recognizing this importance is critical as it helps proactively identify and address vulnerabilities, preventing potential disruptions, financial losses, and safeguarding the integrity of their intricate and interconnected operations across the globe.

To try NodeZero for yourself, you can sign up for a free trial
https://www.horizon3.ai/demo