HORIZON3.ai

~~TRUST BUT~~ VERIFY

Healthcare

WHITE PAPER

A Preemptive Approach to **Defeat Ransomware in Healthcare**

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

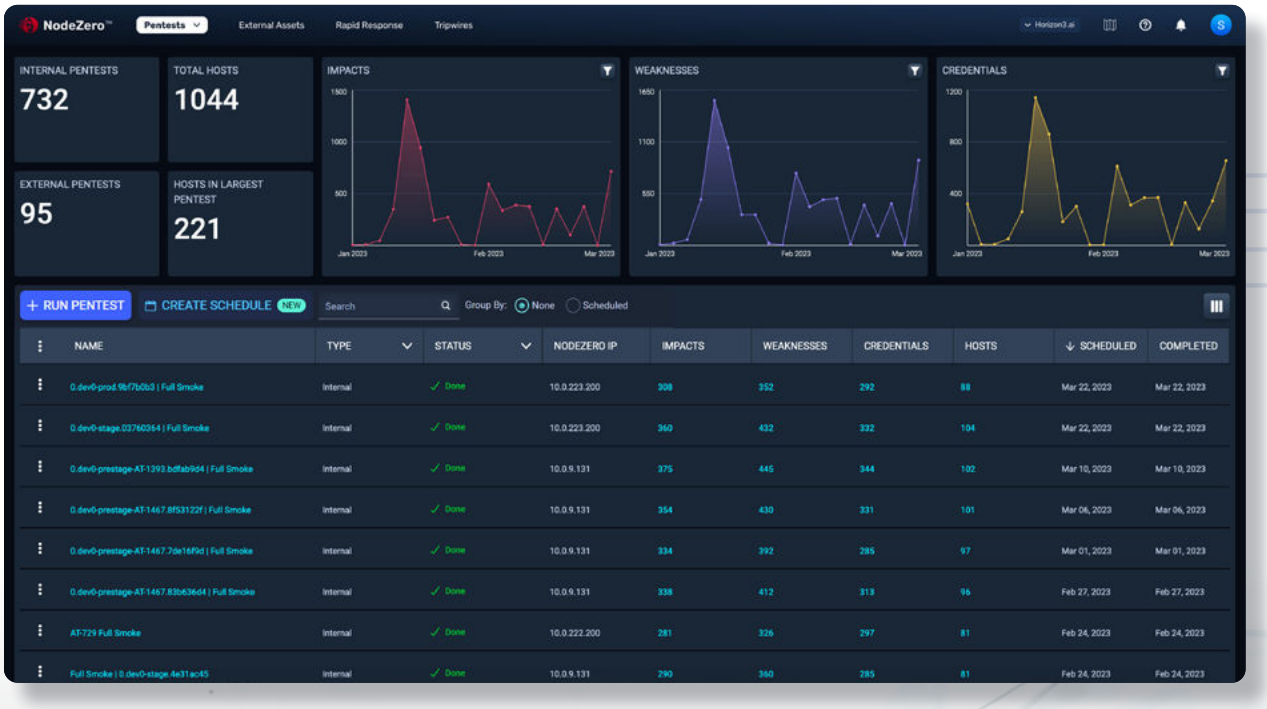
A Preemptive Approach to Defeat Ransomware in Healthcare

Introduction

When thinking about the most damaging cyberattack any healthcare organization could face, ransomware is top of mind. However, the outcome of a successful ransomware attack targeting a healthcare organization, or even worse, a medical facility, is much different than an attack on any other industry. If a bank or large manufacturer gets ransomed, customer satisfaction may plummet, production may be temporarily halted, and revenue may be threatened. Ransomware against the healthcare industry is literally a life-or-death proposition.

The cyber threat landscape is vast, filled with all kinds of threat actors that are fully capable of profiting from those who are unprepared. And today, gaining a foothold in an organization's network, stealing, or encrypting their data, and holding the organization for ransom are the ultimate objectives attackers pursue. The reasons why they use these tactics are simple to understand: They know organizations will pay.

This whitepaper is written for cybersecurity professionals in the healthcare industry. It begins with quickly discussing why a preemptive approach to defeating ransomware is needed, then highlights how NodeZero is becoming an essential part of today's security approaches, and finally, lists multiple healthcare use cases that can help you defeat ransomware attacks.



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

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Why Ransomware? Why Now?

Historically speaking, the healthcare industry has not been severely impacted by ransomware attacks like other industries. In the past, most attackers shied away from attacking this industry due to its humanitarian purposes. Although attackers have often stolen healthcare records for the purpose of identity theft, as demonstrated by several extremely high-profile breaches, taking a hospital offline due to a ransomware attack was typically beyond the "code of ethics" of most attackers. However, that has changed.

Attackers are now putting healthcare organizations in the ransomware crosshairs for three reasons:

1. Ransomware attackers are being emboldened to perform more attacks since they are rarely arrested and/or prosecuted for such crimes.

2. Ransomware attackers know that healthcare facilities are highly likely to pay the ransom to keep critical, life-saving systems, technologies, and networks online.

3. Other organizations are actively paying the demands of attackers, further incentivizing new actors to use this extremely profitable attack vector at everyone else's cost.

At the time of this writing, open-source reporting indicates that cyber threat actors are actively exploiting or seeking to exploit a vulnerability in Progress' MOVEit software (CVE-2023-34362) in real-world scenarios. The CISA #StopRansomware campaign highlights the ransomware group CL0P as the initial group to exploit this vulnerability.

CL0P has targeted the healthcare sector, in which nearly 4 million individuals' personal and health records were breached. The CL0P group is notorious for being a "big game hunter" that targets organizations with large budgets by issuing proportionally large ransom demands – some have been as high as $20 million. However, CL0P also hones and sharpens their skills by targeting smaller organizations.

Horizon3.ai proactively warns customers about potential zero-day and n-day ransomware attacks and impacts so customers can take immediate action to fix potential vulnerabilities and mitigate possible threats.

https://www.horizon3.ai/insight-moveit-zero-day-reminds-us-yet-again-to-be-diligent-in-monitoring-our-it-infrastructure/

2020

Additionally, CL0P has been known to target the public health and healthcare industry in the past. Some examples include:

- **April 2020:** ExecuPharm, Inc.
- **May 2020:** Carestream Dental LLC
- **November 2020:** Nova Biomedical

2022

More recent reporting points to other healthcare industry targets such as:

2023

- **May 2023:** John Hopkins All Children's Hospital
- **May 2023:** UT Southwestern Medical Center (~100k patients information compromised)
- **June 2023:** Harris Health Systems (~225k patients information compromised)
- **Aug 2023:** Colorado Department of Health Care Policy & Financing (~4M patients information compromised)

Exploitation by any cyber threat actor poses a significant risk to businesses relying on applications such as MOVEit for file transfer operations.

Key impacts on businesses include:

- Data breaches and intellectual property theft (e.g., current, and former employee data)
- Operational disruption and downtime
- Manipulation of file transfers
- Reputational damage and legal consequences

Enter NodeZero™

An Essential Security Ally for the Healthcare Industry

NodeZero, with its continuous, autonomous penetration testing capabilities, takes an offensive approach to discover and prove where your greatest vulnerabilities exist. It extends beyond traditional vulnerability assessment tools by probing systems in the same way an attacker would, identifying exploitable vulnerabilities that pose a real-world risk.

Horizon3.ai specifically developed NodeZero so organizations can discover what would happen next if an attacker gained a foothold in their networks. NodeZero highlights the attack paths an attacker could take to discover and exploit the unknown vulnerabilities and weaknesses in your networks that could lead to compromise, or even worse, ransomware. NodeZero safely attacks you, then explains how to fix the issues it discovers. Once you take action to remediate what NodeZero discovers, it allows you to verify your fix worked.

In addition, healthcare organizations use NodeZero to significantly strengthen their security posture by reducing their exploitable attack surface, enhancing the return on investment (ROI) for their security tools, and validating the effectiveness of their Security Operations Centers (SOCs). Healthcare organizations must understand that NodeZero goes way beyond the capabilities of common vulnerability management tools because it shows you which vulnerabilities are actually exploitable.

For example, the Director of Security Engineering with Cross Country Healthcare, Mike MacNeill, gave us his thoughts on vulnerability management solutions.

> **Some of the biggest challenges with vulnerability management solutions is that we're just overloaded with information. We were working with these products that have dashboards that are just telling you you've got hundreds of thousands of vulnerabilities you need to fix. So, where do you begin when you have that kind of an overwhelming sense of doom and gloom? That was one of the biggest challenges. Another is how do I present the success of a vulnerability management program to the executive leadership? When they're looking at a dashboard that's showing a large number, they expect that number to go down and, and in vulnerabilities, that's not always the case."**

In the Gartner® Hype Cycle for Security Operations[1], 2023, NodeZero is classified as an automated penetration testing and red teaming technology. In other words, NodeZero is a pentesting solution that allows organizations to continuously assess the security posture of their internal, external, and cloud infrastructures in a completely autonomous fashion. Beyond red teams, Figure 1 shows how other teams use NodeZero.

Figure 1

ITOps proactively fixes security issues within their infrastructure

Security Teams respond immediately to n-day crises

SecOps uses NodeZero as a sparring partner to tune their security tools

Large Organizations assess and reduce supply-chain and subsidiary risks

MSSPs and MSPs can run assessments, tune their services, and provide strategic insights

Pentesters use NodeZero to attack at-scale so humans can be scalpels

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

HORIZON3.ai
~~TRUST BUT~~ VERIFY

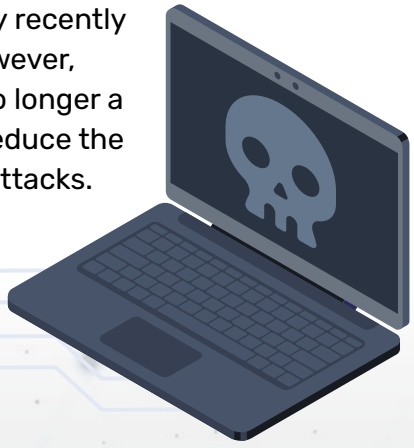
1. Gartner, Hype Cycle for Security Operations, 2023, Jonathan Nunez, Andrew Davies, 20 July 2023.

Autonomous Pentesting: Critical to Identifying and Reducing Your Ransomware Risk

Healthcare organizations recognize they need a preemptive approach to help them discover their truly exploitable vulnerabilities, show them how to fix the issues at hand, then verify their fix worked. They also understand this type of approach is the best way to discover exploitable vulnerabilities, misconfigurations, and oversights they previously knew nothing about.

Too often in the fight against cybercrime, healthcare organizations think "more" defenses are the best approach. However, they are now adopting a continuous assessment approach using autonomous pentesting to meet healthcare industry information security standards. This approach allows healthcare organizations to see their networks through the eyes of an attacker by using the same tactics, techniques, and procedures (TTPs) that attackers use. Simply put, the only way to reduce the risk of ransomware is to know where you're vulnerable – and fix it. And healthcare organizations are using NodeZero to do just that.

Too often in the fight against cybercrime, security teams focus solely on known-vulnerability management and patching systems impacted by recently publicized CVEs. However, many agree this is no longer a viable approach to reduce the risk of ransomware attacks.



NodeZero safely identifies and reduces your ransomware risk as follows:

- Discovers and exploits your unknown vulnerabilities that could lead to compromise
- Uses misconfigurations and dangerous product defaults to advance its attacks
- Identifies poor credential policies and credential reuse to take over systems
- Chains weaknesses together to compromise hosts and domains
- Pivots from one system to another to discover additional attack paths
- Finds your data and determines if it can be accessed, stolen, and ransomed
- Performs phishing simulations, harvests credentials, and shows what happens next
- Highlights software that is still exploitable even after patches have been applied
- Proves what it discovered by showing commands, exploit code, and outcomes

The whole point of performing autonomous pentests is to identify and reduce your exploitable attack surface, and in doing so, reduce the risk of a successful ransomware campaign. Organizations of all sizes are pointing, clicking, and digitally firing NodeZero at themselves to see what it discovers. They know that in doing so, it will accelerate the find, fix, and verify cycle that measurably reduces the risk of ransomware.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

An Example Attack Path
Discovered in a Healthcare Organization

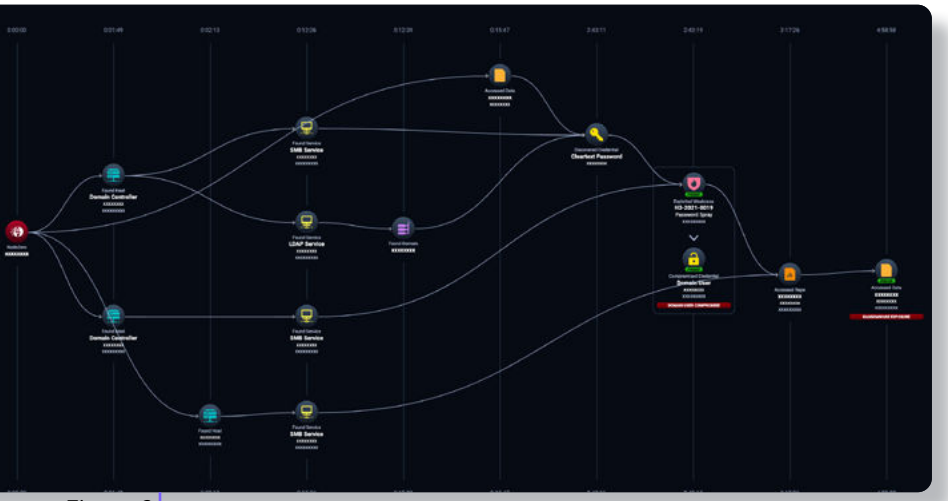


Figure 2

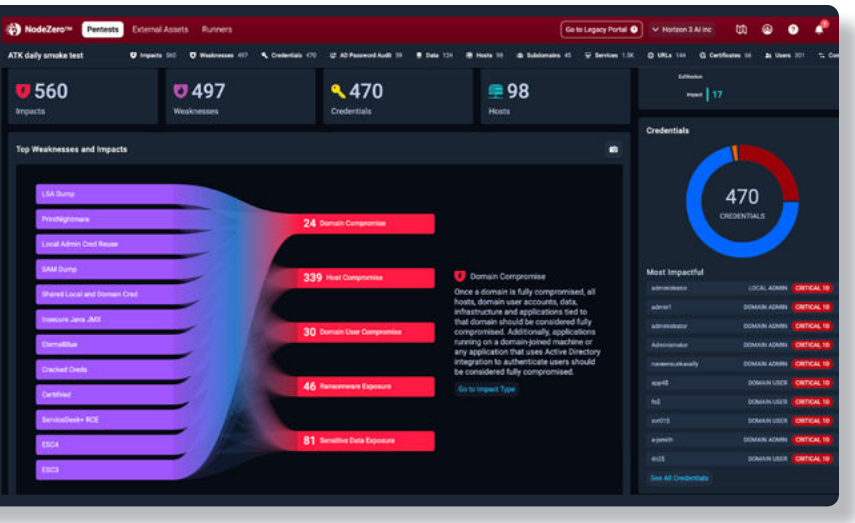
In the context of cybersecurity, attack paths provide a graphical representation of the possible paths an attacker can take to exploit weaknesses in your computers, servers, applications, infrastructure, and security controls. Figure 2 shows an example attack path discovered by NodeZero during an autonomous assessment in a physical healthcare facility that is a customer of Horizon3.ai. This attack path could have led to a successful ransomware attack.

Here are the steps NodeZero took that identified RANSOMWARE EXPOSURE (far right)

- NodeZero was launched from host x.x.x.x on Aug 4, 2023
- NodeZero discovered 250+ verified usernames
- NodeZero discovered a cleartext password for USER1 while accessing the SMB service on domain controller DC1
- NodeZero discovered and verified H3-2021-0019: Weak or Default Credentials - Password Spray affecting the credential for USER1 in DOMAIN1 on the SMB service on domain controller DC2
- NodeZero discovered file share DATA1 using the credential for USER1 in DOMAIN1
- NodeZero enumerated 200+ highly sensitive files in file share DATA1 on FILESERVER1 using the credential for USER1 in DOMAIN1

In less than five hours, NodeZero was able to discover 250+ usernames, determine there was a cleartext password in use, leveraged a password spraying technique to see if credentials were in use elsewhere, verified the discovered credential had access to other systems, and easily accessed a file share with highly sensitive data in it. Then NodeZero enumerated more than 200 files in the file share which could have been stolen, encrypted, and ransomed by an attacker. Using the compromised credential, NodeZero determined the credential could be used in 70+ other attack paths within the same network, eventually leading to domain compromise.

NodeZero Lowers the Risk of Ransomware – and More



Healthcare organizations who have adopted NodeZero as part of their continuous assessment process, and added it into their cybersecurity programs, experience the following benefits:

- Identify attack vectors before they're exploited through easy-to-understand attack paths. Proactively identifies weaknesses and provides top-level views of larger systemic issues, and how to address them at a macro level for long-term cyber resilience.
- Obtain a prioritized list of what needs fixing most urgently. Eliminates time-consuming false positives and improves the capacity of security and IT teams regardless of the level of expertise or size of the overall team.
- Eliminate risks and validate security with continuous assessments. Provides proof of current security levels, highlights effective remediations, tracks improvement over time, and generates reports that analysts and auditors understand.
- Improve security performance and visibility of risk level. Delivers reports that leaders will appreciate and verifies risks are identified, prioritized, and addressed — justifies their investment and proves its effectiveness.
- Perform assessments on demand. Allows teams to find, fix, and verify as often as they like – and even concurrently – without additional costs while reducing the need to hire third party assessors and penetration testers.

What NodeZero discovers daily in networks just like yours confirms what we have always known. To fully understand what would happen if an attacker gained a foothold in your network, you must continually attack your own environment the same way they would. NodeZero enables organizations of all sizes to safely attack their production networks, no matter what time of day or night, and as often as they like.

"NodeZero has been very good at finding things we didn't expect it to find, and it's not just about computers and software weaknesses. For example, IP-based telephones having a default password used to configure them, or the conference room gear that you never think of when someone plugged it in, and nobody ever changed the default password… it's amazing what NodeZero finds way beyond just your typical computer or application", says Mike at Cross Country Healthcare.

NodeZero helps you tune your defenses to enhance security tool ROI

Investing in security tools is a necessity, but ensuring their efficacy is critical to maximizing ROI. Acting as a sparring partner, NodeZero can help teams better tune security tools, including Endpoint Detection and Response (EDR) solutions like CrowdStrike Falcon Complete and Security Information and Event Management (SIEM) systems like Splunk. By executing autonomous pentests, NodeZero exposes any gaps in detection and response, providing actionable insights to fine-tune these tools, thereby improving their overall effectiveness and ROI.

NodeZero helps verify your SOC effectiveness

The effectiveness of a healthcare organization's SOC is critical in managing and mitigating cyberattacks. NodeZero can serve as a vital tool in verifying SOC effectiveness by executing realistic attacks that allow organizations to assess their detection and response capabilities. For instance, using a NodeZero attack mimicking a user or domain compromise, or even a ransomware takeover, allows you to accurately assess your SOC's ability to identify and respond to any one of these attacks.

NodeZero assists blue teams and red teams

In the context of blue teams, NodeZero can assist them in identifying and prioritizing exploitable vulnerabilities. Following a NodeZero pentest, blue teams can remediate identified vulnerabilities and re-run the test with a One-Click Verify™ to validate their remediation actions were successful.

NodeZero can also act as a force multiplier for red teams. It can autonomously execute pentests, freeing those teams to focus on more sophisticated, pinpointed attacks. The insights from NodeZero can help red teams better understand an organization's exploitable attack surface so they know where to focus their efforts, becoming more like human scalpels instead of using "spray and pray" TTPs.

Healthcare Ransomware and Security Breaches

Let's look at two use cases where NodeZero could have helped the following organizations avoid the attacks they fell victim to:

Use case 1:

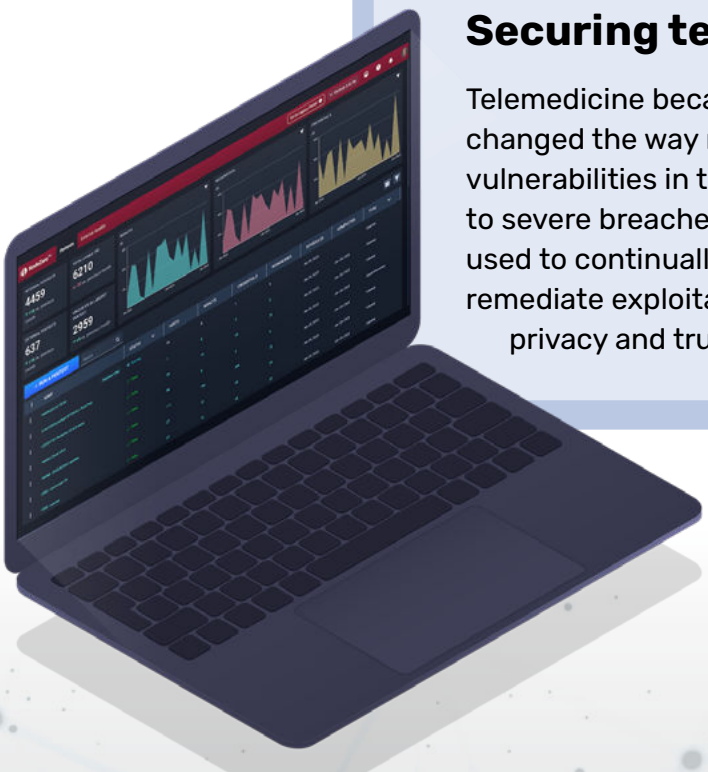
Guarding against ransomware attacks

NodeZero can help healthcare organizations prepare for ransomware attacks, similar to the recent attack on Prospect Medical Holdings that has impacted healthcare services in at least three states. By autonomously pentesting healthcare networks and infrastructure, NodeZero identifies vulnerabilities an attacker could exploit to inject ransomware, allowing for timely remediation before an incident occurs.

Use case 2:

Securing telemedicine platforms

Telemedicine became a lifeline during the pandemic and has changed the way many receive healthcare today. However, vulnerabilities in the software behind these services can lead to severe breaches, like the Cerebral breach. NodeZero is being used to continually test telemedicine platforms to identify and remediate exploitable vulnerabilities, thereby enhancing patient privacy and trust.



10 Scenarios Where NodeZero Can Help Healthcare Organizations

When considering the various scenarios that could lead to compromise, NodeZero helps identify the following risks, and more:

1 Unpatched Software

NodeZero identifies unpatched or outdated software versions within the infrastructure, exploits CVEs and unknown weaknesses, and demonstrates what attackers could do next.

2 Misconfigured Network Devices

Misconfigured firewalls and other security controls can expose internal services to the internet. NodeZero highlights misconfigurations and product defaults to help with remediation efforts.

3 Weak or Reused Passwords

Weak or reused passwords make credential-based attacks easy to execute. NodeZero uses password guessing techniques against service accounts to discover weak passwords.

4 Exposed RDP Services

Open RDP ports can be exploited by credential stuffing attacks. NodeZero identifies open RDP ports and attempts to authenticate with harvested or guessed credentials.

5 Lateral Movement

NodeZero executes lateral movement attacks, such as Pass-the-Hash or Pass-the-Ticket, to detect excessive trust relationships within the network.

6 Lack of Multi-factor Authentication (MFA)

By attempting to authenticate to services that should be protected by MFA, NodeZero identifies services where MFA is not enforced, helping to prevent breaches.

7 Excessive User Credential Privileges

NodeZero pinpoints user or system credentials that enable excessive privileges by attempting to access resources typically restricted to high-privilege accounts and displays the exposed data impacts.

8 Unsecured Network Shares

NodeZero finds unsecured network shares that can be accessed without credentials, helping to prevent data theft and ransomware incidents.

9 Exploitable SMB Protocols

By attempting exploits like EternalBlue against systems running SMBv1, NodeZero recognizes those systems susceptible to this and other SMB attack vectors.

10 Unencrypted Network Traffic

NodeZero identifies the usage of unencrypted protocols (HTTP, FTP, Telnet) within the network that can be intercepted and exploited by attackers.

Conclusion

Since today's attackers fully understand common security approaches and are often experts on the same security tools organizations use, they know how to sidestep your defenses to reach their objectives. And as the cyber threat landscape widens, and threat actors continue to modernize and evolve, healthcare organizations must keep up by adopting a preemptive approach to defeating ransomware. NodeZero has become a critical, offensive-based solution for healthcare organizations worldwide.

Using NodeZero to continuously assess themselves, it helps organizations of all sizes find their unknown weakness and remediate their issues before attackers can exploit them. By reducing the exploitable attack surface, maximizing security tool ROI, and reinforcing SOCs, NodeZero empowers healthcare organizations to better protect their patients, data, and services while significantly reducing the possibility of ransomware-related outages.

To learn how NodeZero can help secure your healthcare business, schedule a demo today.

https://www.horizon3.ai/demo