







# Identify Cybersecurity Risks at Scale to De-Risk M&A Transactions




## With Horizon3.ai's NodeZero® Platform

Horizon3.ai's NodeZero® autonomous security platform empowers enterprises to swiftly and accurately evaluate the cybersecurity posture of single or multiple independent organizations, making it an indispensable tool for M&A cyber risk assessments.

**During periods of M&A due diligence, organizations can use NodeZero to evaluate potential acquisitions targets with minimal deployment time required. This enables the acquiring organization to:**

-  Autonomously discover and fingerprint network and infrastructure assets without relying on outdated documentation or extensive scoping exercises.
-  Identify security weaknesses caused by misconfigurations, weak or reused credentials, exploitable vulnerabilities, ineffective security controls, and more.
-  Demonstrate and provide proof of exploitability, including potential business impacts such as infrastructure compromise, ransomware exposure, and sensitive data breaches.
-  Reveal systemic issues, allowing the elimination of numerous weaknesses with a single corrective action.

**After the transaction is complete, NodeZero enables the organizations to:**

-  Prioritize remediation efforts based on real-world impact.
-  Follow detailed remediation guidance and conduct follow-up autonomous pentests to confirm fixes.
-  Continuously assess and verify the exploitable attack surface, ensuring ongoing improvements to the security posture.

NodeZero's multi-tenant architecture allows the acquiring organization to maintain oversight over the acquired company. The acquiring organization can also allow the acquired company to independently operate NodeZero and share results and trends.

# Horizon3.ai M&A Engagement Flow

Most enterprises lack the staff to conduct large-scale parallel security assessments, and hiring consultants for manual assessments is costly and time-intensive. Horizon3.ai alleviates this burden by enabling organizations to deploy NodeZero and efficiently assess networks with tens, hundreds, or thousands of endpoints. Here is an example workflow:

Acquiring organization partners with Horizon3.ai and provides contact information for the target organizations.

**1**

Horizon3.ai's Customer Success team manages the process of engaging the target organizations' IT teams, supporting the deployment of the NodeZero host, and empowering the IT admins to launch pentests.

**2**

Pentest results are made available in the NodeZero dashboard for the target organizations to analyze and begin working on any critical remediation activities, while the overall results are reported up to the acquiring organization.

**3**

## Use Case Details

# Multinational Manufacturer Secures M&A Targets With Horizon3.ai

In 2023, an American multinational manufacturer prepared for M&A activity and recognized the need to assess the cyber risk posture of the organizations it planned to acquire.

Partnering with Horizon3.ai, the manufacturer conducted 60 internal pentests across 38,000 hosts in the target organizations' network infrastructures. NodeZero achieved this for less than half the cost of a manual pentest per organization, with simple deployments averaging 15 minutes to set up.

Each pentest concluded with detailed Fix Actions reports providing specific remediation guidance. The acquiring organization gained immediate insights into the impact of each target organization's security weaknesses and drilled into specific findings for further understanding. Following NodeZero's guidance, the organizations could remediate the discovered weaknesses and use the "1-Click Verify" feature to retest and confirm fixes were successful.

 **60**

**BUSINESSES  
PENTESTED**

 **15 MINS**

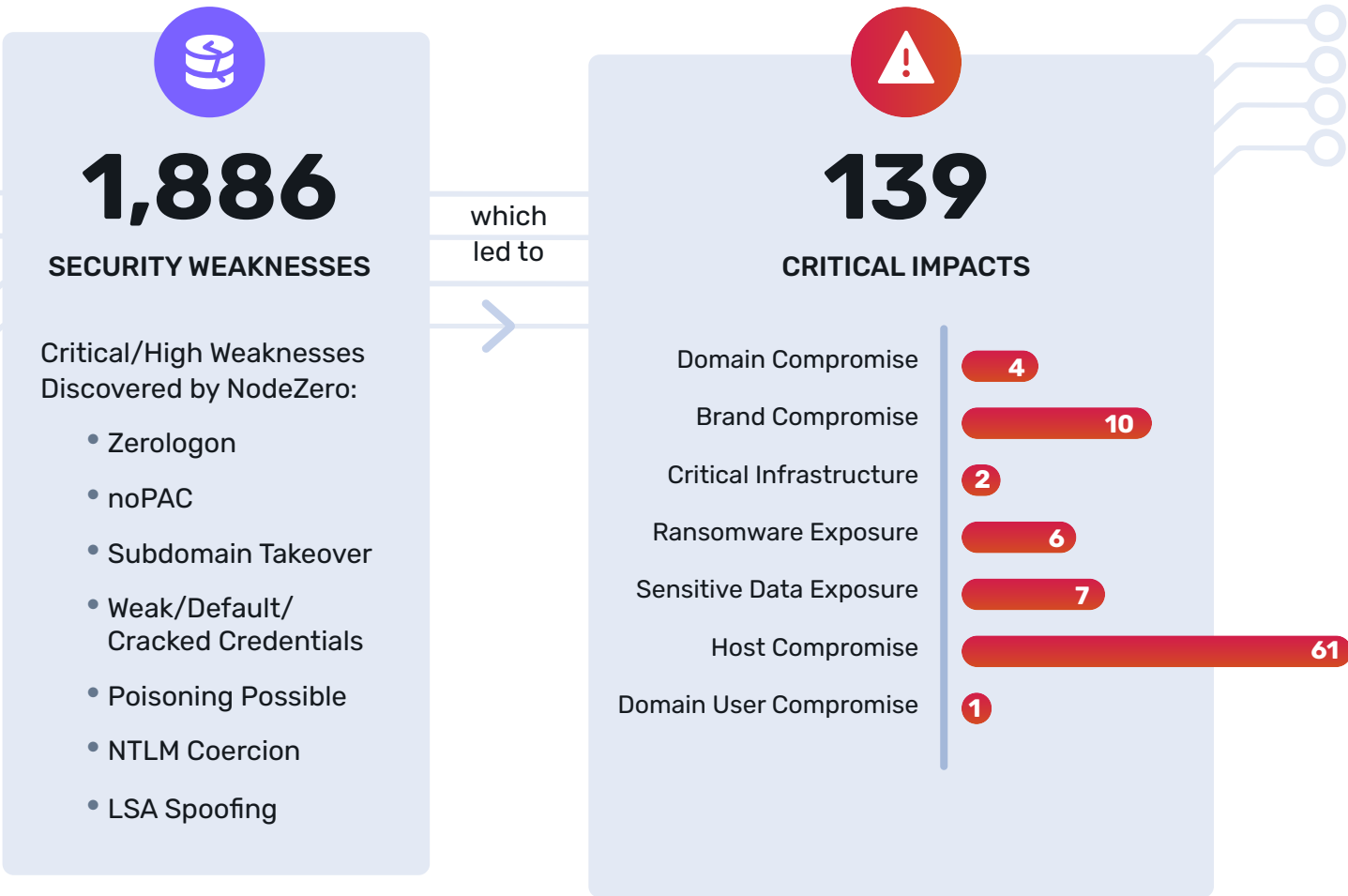
**AVERAGE DEPLOYMENT  
TIME PER BUSINESS**

 **38,000**

**TOTAL HOSTS  
PENTESTED**

# Overall Results Across 60 Target Business

In total, Horizon3.ai helped the manufacturer to identify and prioritize thousands of security weaknesses, many of which were demonstrated to have critical impacts to the businesses when exploited.



## Illustrative Results From One Target Business

While findings differed at each of the businesses where NodeZero was deployed for autonomous pentesting, here is how the results from one of those businesses looked:

### PROCESS

On Sept 11, 2023, the acquiring organization began a series of pentests of one of the target organizations by first conducting a network enumeration of all reachable assets at this location. On Sept 18, 2023 a baseline pentest was conducted which lasted for 2 hours.

INITIAL RESULTS

As shown in **Figure 1**, the results of this pentest proved 71 impacts and 79 weaknesses, across 27 credentials, 22 protected data items, and 29 compromised hosts. This uncredentialed pentest revealed four unique attack paths to domain compromise via Zerologon and noPAC weaknesses.

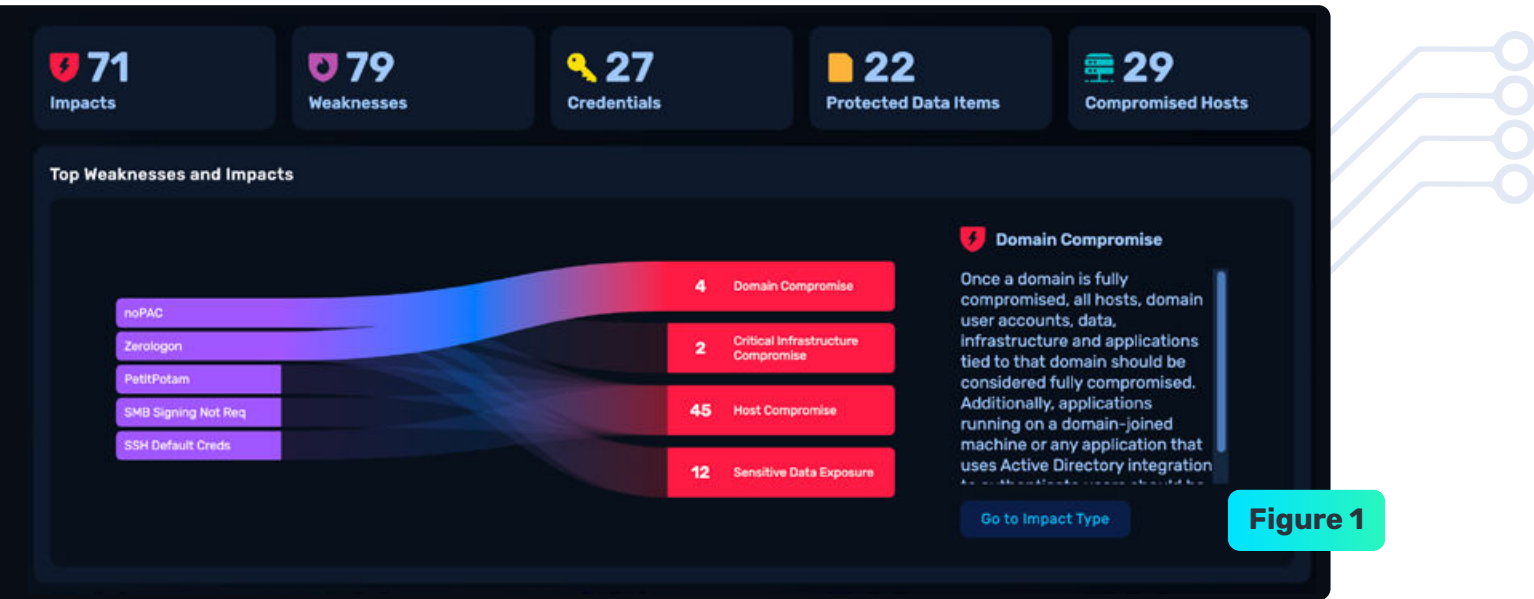


Figure 1

As shown in **Figure 2**, the domain compromise led to a Ransomware Exposure of over 195k sensitive data resources, including possible PII exposure.

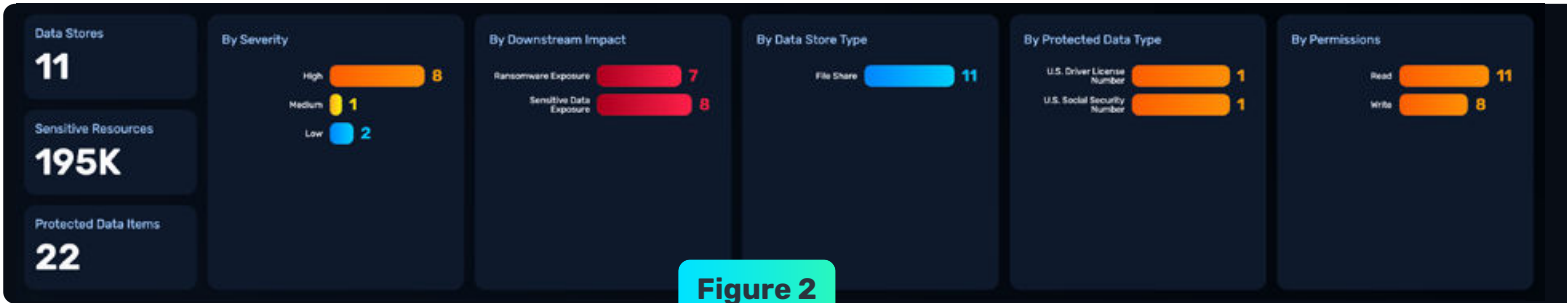


Figure 2

As shown in **Figure 3**, NodeZero followed this attack path as it discovered and exploited several weaknesses until ultimately gaining a Critical Impact: Domain Compromise in ~30 minutes. NodeZero provided the path, proof, and impact for every attack path it found.

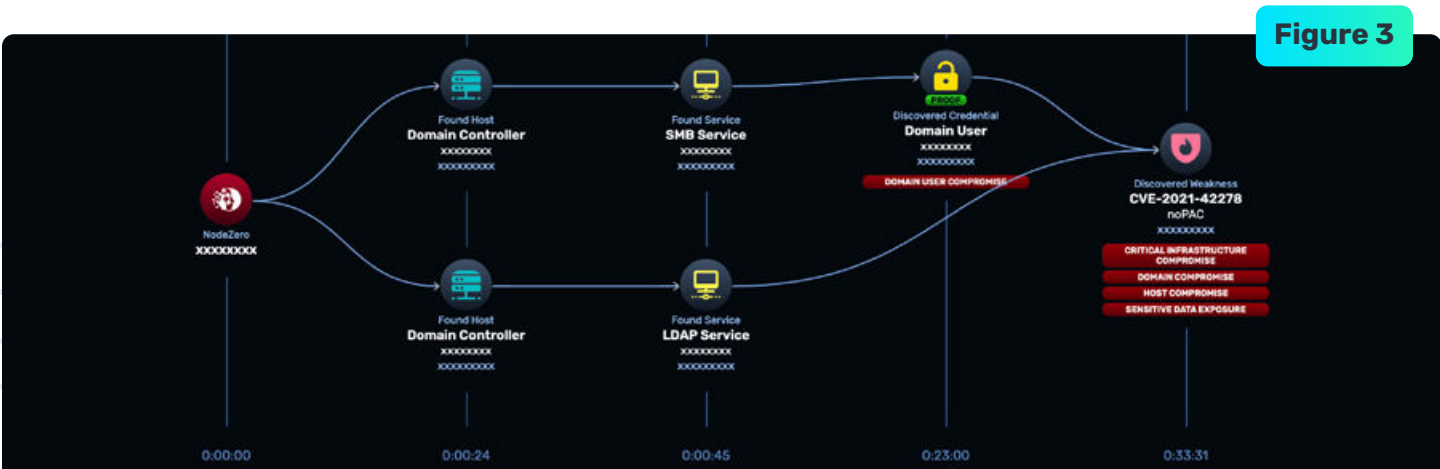


Figure 3

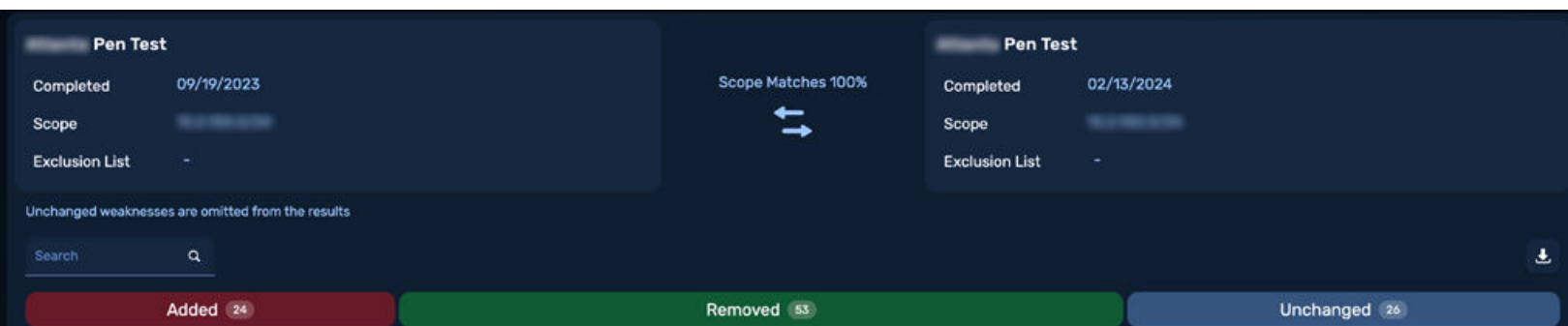
## ACTIONS AND OUTCOMES

These high-level findings were extremely useful for assessing the cyber risk of the potentially acquired company during the due diligence process. In addition, now that the target company had visibility into these security weaknesses and impacts, they could begin prioritizing and fixing them.

Immediately following the first baseline test, the target company's security team followed NodeZero's step by step Fix Actions guidance, and prioritized remediation of the most critical weaknesses first.

After successful remediation, the team used NodeZero's 1-Click Verify to conduct a targeted validation pentest of the same environment as shown in Figure 4.

The targeted validation pentest provided proof that the team had successfully mitigated all paths to domain compromise and removed 53 additional weaknesses in the process. Additionally, the pentest also provided insight into 24 new weaknesses based on infrastructure changes that occurred since the first pentest was completed.

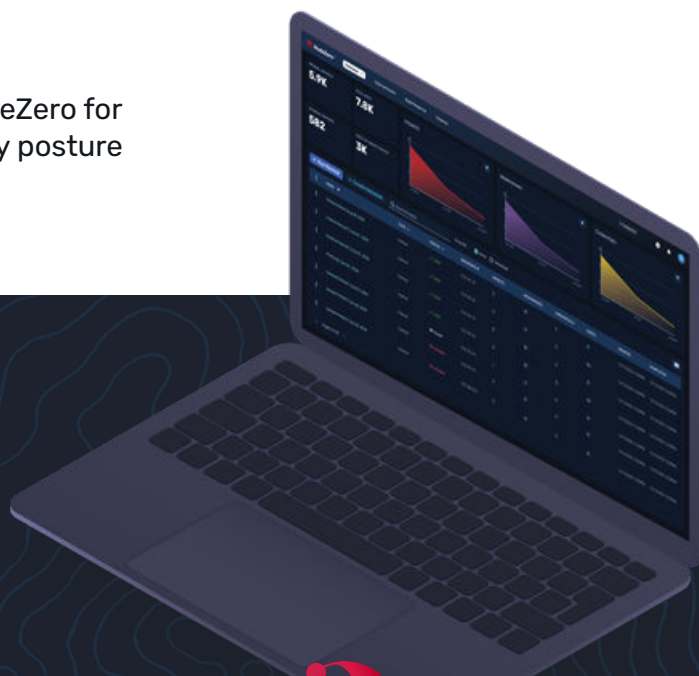


## CURRENT STATUS

The acquiring organization regularly uses NodeZero for continuous security assessments and security posture improvements as part of their M&A playbook.

- Discover how NodeZero™ can de-risk your M&A transactions—schedule a demo today.

<https://www.horizon3.ai/demo>



**HORIZON3.ai**  
TRUST BUT VERIFY