HORIZON3.ai

~~TRUST BUT~~ VERIFY

NodeZero

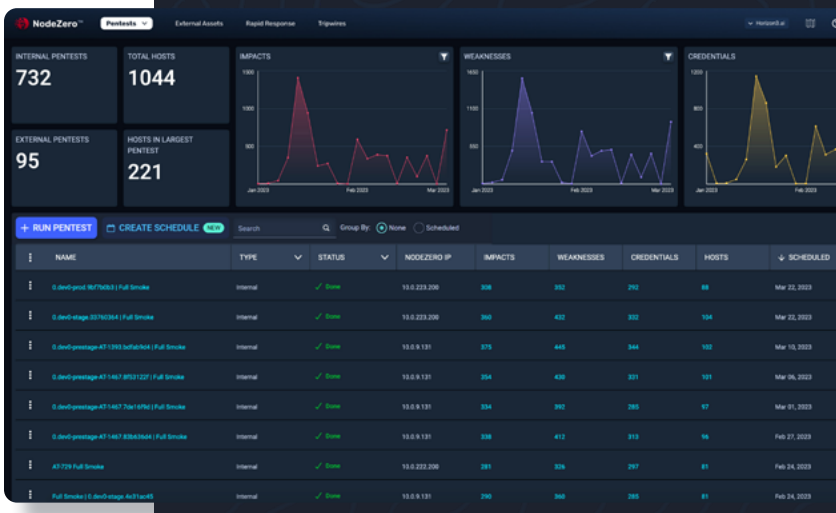
Continuously find, fix, and verify your exploitable attack surface

The NodeZero™ platform empowers your organization to reduce your security risk by autonomously finding exploitable weaknesses in your network, giving you detailed guidance about how to prioritize and fix them, and helping you immediately verify that your fixes are effective.

Uncover—and quickly remediate—blind spots in your security posture that go beyond known and patchable vulnerabilities, such as easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies.

Maneuver through your network, chaining weaknesses just as attackers do, and then safely exploits them.

Schedule and run as many pentests as you want against your entire digital infrastructure and run multiple pentests at the same time.

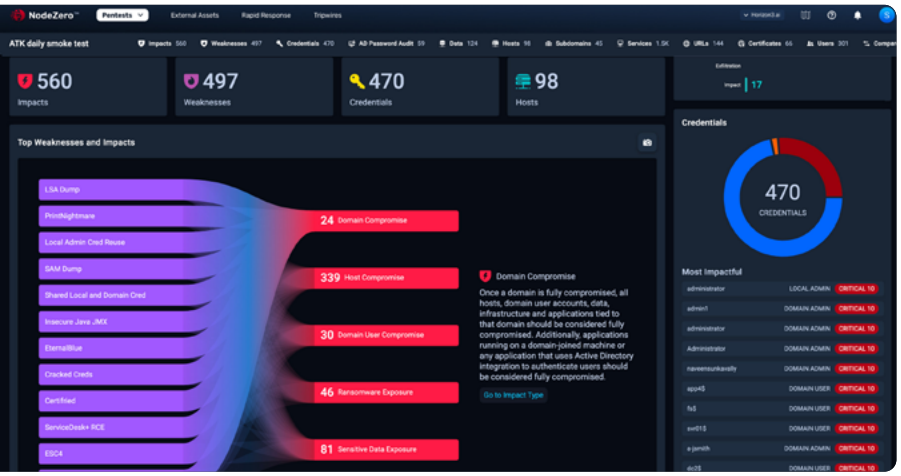


▲ The dashboard prioritizes your highest risks and helps you monitor your progress over time.

Improve the capacity of your security and IT team members, regardless of their level of expertise. You can set up and start your first NodeZero in minutes.

Conduct unlimited tests on:

- On-premises infrastructure
- Cloud infrastructure
- Identity and access management infrastructure
- Data infrastructure
- Virtual infrastructure
- Public facing assets



▲ NodeZero helps you understand the weaknesses that lead to critical impacts, so you know exactly what to fix in order to disrupt the kill chain.

You have full visibility into the actions carried out by NodeZero. Real-time view gives you visibility into NodeZero exploits as they are executing. You can see the proof, path, and impact of each weakness identified.

The final reports are tailored to help you meet your internal and external audit requirements. They include Executive Summary, Pentest, Fix Actions, Segmentation reports and more.

▲ This attack path shows how NodeZero was able to compromise sensitive data from over 76,000 files stored in Amazon Web Services (AWS) via a compromised credential.

NodeZero autonomously executes these key operations for assessing and validating your security posture:

Internal Pentesting

Take an "assume breach" mindset to reveal the perspective of an attacker or malicious insider who has already gained access to your internal network. NodeZero prioritizes the impacts for you and offers detailed remediation guidance.

Rapid Response & N-Day Testing

The one-of-a-kind Horizon3.ai Rapid Response service provides NodeZero users with real-time threat intelligence about high-profile emerging threats known to impact them, enabling you to use the intel in the Rapid Response center to mitigate threats before they are exploited in the wild.

Phishing Impact Test

Discover the damage an attacker can do with phished credentials in your environment. NodeZero helps you measure and understand the proven impact of a phishing scam and recommends controls to mitigate your risk.

External Pentesting

Launched from Horizon3.ai's cloud environment with no additional set up, external pentests quickly and accurately assess your security posture from the perspective of an attacker trying to breach your perimeter.

Cloud Pentesting

NodeZero provides a variety of methods to test cloud environments. Users can test their cloud security with the context of the entire digital infrastructure, target only cloud environments, or even use a privileged perspective to test for attack paths stemming from weak identity and access management.

AD Password Audit

Attackers don't hack in, they log in. Compromised credentials underpin a high percentage of cyberattacks. Continually verify the effectiveness of your credential policies to ensure you're not leaving a welcome mat out for bad actors.

Continuously improve your cyber resilience.

NodeZero is available on aws marketplace

Start your free trial now.

https://www.horizon3.ai/trial

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

HORIZON3.ai
~~TRUST BUT~~ VERIFY