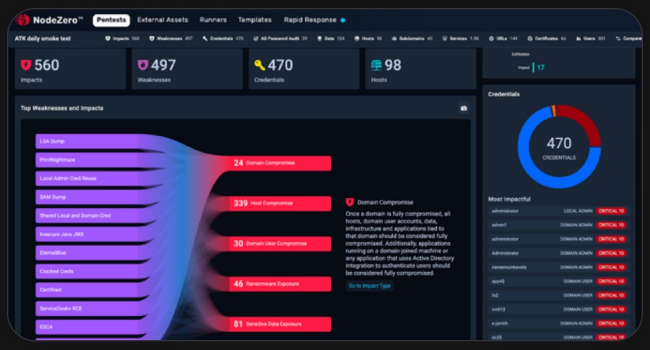
1.01 AUTONOMOUS PENTESTING

NodeZero

Continuously find, fix and verify your exploitable attack surface.

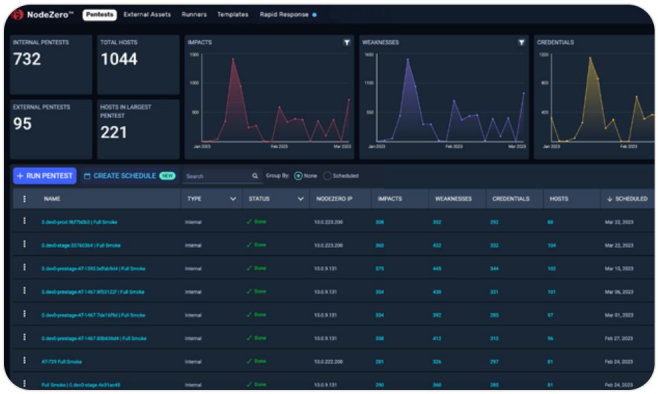
Delivered and supported by Cyber Vigilance's in-house technical team.



See the weaknesses that lead to critical impacts, so you know exactly what to fix to disrupt the kill chain.

The NodeZero™ platform helps your organisation reduce security risk by autonomously finding exploitable weaknesses in your network, giving you detailed guidance on how to prioritise 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: easily compromised credentials, exposed data, misconfigurations, poor security controls and weak policies.



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

1.02 HOW IT WORKS

Thinks like an attacker

NodeZero manoeuvres through your network, chaining weaknesses just as attackers do, then safely exploits them.

Tests at scale

Schedule and run as many pentests as you like against your largest networks, including several at the same time.

Running in minutes

Boost the capacity of your security and IT team, whatever their level of expertise. Your first pentest can start in minutes.

1.03 CONDUCT UNLIMITED TESTS ON

01 On-premises infrastructure

02 Cloud infrastructure

03 Identity and access management

04 Data infrastructure

05 Virtual infrastructure

06 Public-facing assets

2.01 VISIBILITY

Full visibility, from first move to final report

You get full visibility into every action NodeZero carries out. A real-time view shows its exploits as they execute, with the proof, path and impact of each weakness identified.

Final reports are tailored to help you meet internal and external audit requirements, including Executive Summary, Pentest, Fix Actions and Segmentation reports.



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

2.02 KEY OPERATIONS

Assess and validate your posture, autonomously

Internal pentesting

Take an "assume breach" mindset and see your network as an attacker or malicious insider who already has access would. NodeZero prioritises the impacts for you and offers detailed remediation guidance.

External pentesting

Hosted in the cloud with no additional set-up, external pentests quickly and accurately assess your posture from the perspective of an attacker trying to breach your perimeter.

Cloud pentesting

During internal pentests, NodeZero pivots into common cloud environments, finding attack paths to cloud assets and data through misconfigurations and compromised or injected credentials. You can also run dedicated cloud pentests.

Rapid Response and N-Day testing

Real-time threat intelligence on high-profile emerging threats known to affect you, so you can respond pre-emptively and mitigate them before they're exploited in the wild.

Phishing impact test

Discover the damage an attacker could do with phished credentials in your environment. Measure the proven impact of a phishing scam and get recommended controls to reduce your risk.

AD password audit

Attackers don't hack in, they log in. Continually verify the effectiveness of your credential policies, so you're not leaving a welcome mat out for bad actors.

Continuously improve your cyber resilience.

Ask us about a no obligation free trial. Our in-house engineers will help you set up, run and act on your first NodeZero pentest.

Book a demo: www.cybervigilance.uk · +44 (0) 1483 948090 · info@cybervigilance.uk