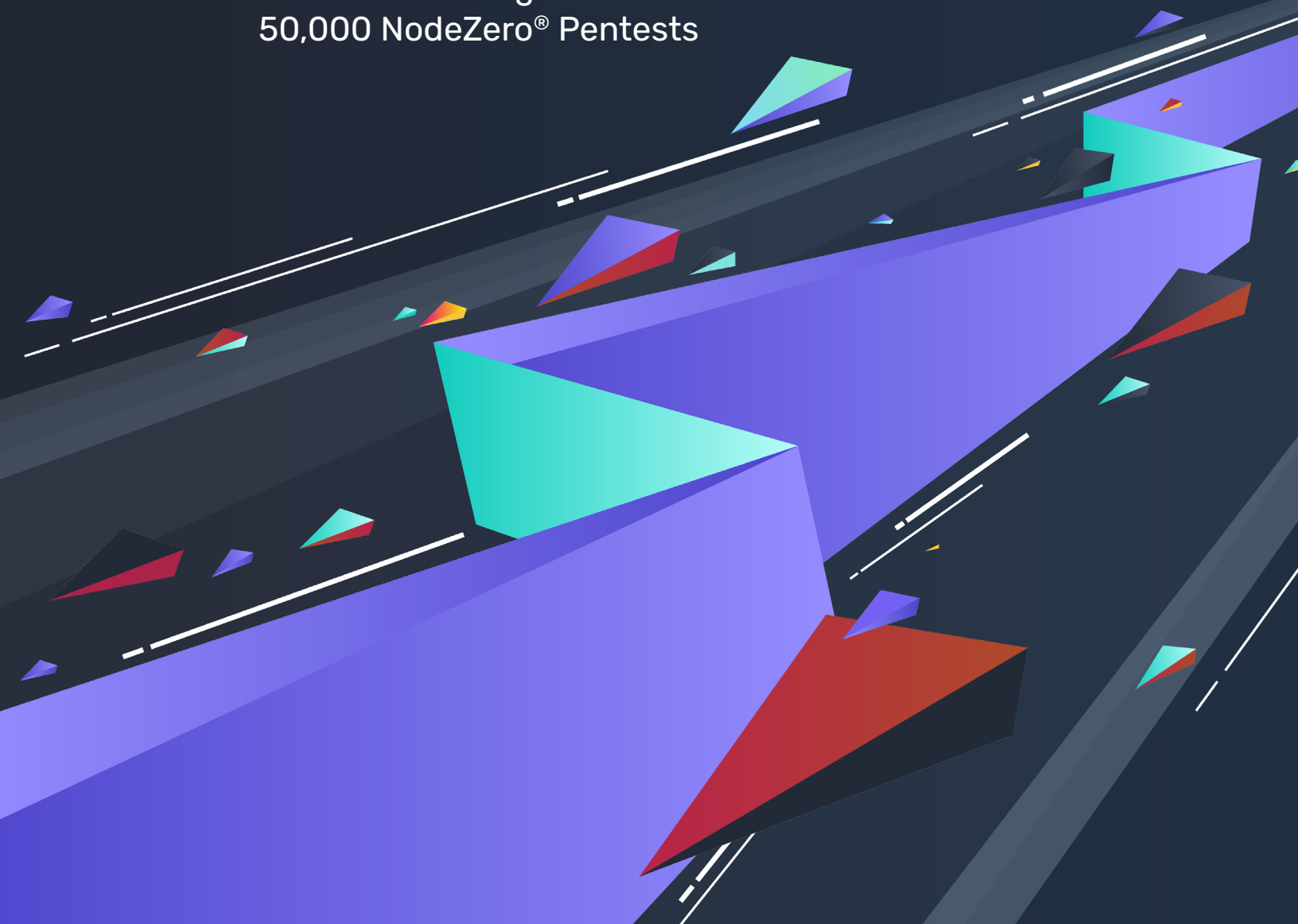
HORIZON3.ai

~~TRUST~~ BUT VERIFY

ANNUAL INSIGHTS REPORT

The State of Cybersecurity in 2025

Data-Driven Insights from Over 50,000 NodeZero® Pentests



Reactive Cybersecurity is Failing

Nearly 25 years have passed since the ILOVEYOU worm infected over 10 million Windows computers on May 5, 2000—one of the first large-scale cyber incidents that jolted the digital world awake. Fast forward to 2025, and cyberattacks are more frequent and widespread. In 2024 alone, the ITRC tracked 3,158 data compromises, resulting in over 1.3 billion notifications sent to affected individuals—a staggering 211% increase from the previous year.[1]

70% Ransomware now accounts for 70% of system intrusions, solidifying its position as the most lucrative and pervasive threat.[2]

71% Credential-based attacks have skyrocketed by 71% year-over-year as attackers continue to exploit stolen user credentials, underscoring one of the most significant challenges in today's hyperconnected landscape.[3]

These numbers paint a grim picture of the current cybersecurity reality.

To get a precise view of cybersecurity in 2024, we looked at data from over 50K penetration tests organizations of all sizes ran in production with NodeZero. The headline? There's a critical disconnect between the perceived and actual state of cybersecurity, emphasizing the urgent need for organizations to shift from compliance-driven checklists to proactive, offense-driven strategies.

The findings in this report are grounded in two powerful sources: deep, high-fidelity 2024 data from Horizon3.ai's NodeZero® Autonomous Security Platform combined with comprehensive data from a survey conducted by Censuswide, which gathered insights from nearly 800 CISOs and hands-on IT practitioners across the U.S., U.K., and EU. These cybersecurity professionals revealed a hard truth that can no longer be ignored:

97% agree that organizations must move beyond compliance-based security and adopt readiness-based assessments to genuinely understand their risk.

39% support the aforementioned approach but acknowledge they lack the resources to execute it.

45% believe that emulating attacker tactics, techniques, and procedures (TTPs) is essential for effective risk assessment.

20% see the value but hesitate to execute it due to perceived operational risks.

[1] https://www.idtheftcenter.org/publication/2024-data-breach-report/
[2] https://www.verizon.com/business/resources/reports/dbir/
[3] https://www.ibm.com/reports/threat-intelligence

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Organizations know they must evolve towards readiness-based security by emulating attacker tactics, yet the gap between intention and execution remains wide—and it's a recurring theme throughout this report. It underscores the critical need for an achievable shift to offensive cybersecurity, embraces an attacker's perspective, challenges conventional defenses, and relentlessly validates security effectiveness.

Purpose Behind This Report

Horizon3.ai created this report to provide real, actionable intelligence that demonstrates how to close security gaps and helps organizations strengthen their defenses to withstand a frontal assault. We've distilled the findings into a set of common gaps and failures, and guidance for what security teams must do to adapt.

The data proves that today's security teams are overwhelmed and falling behind.

In our survey, **36%** of CISOs admit their organization delays patching known vulnerabilities, often because they can't distinguish between those that are exploitable and those that are not. Meanwhile, **41%** of organizations say third-party pentest reports are unreliable, making it difficult to prioritize real risks.

But frontline struggles aren't the only issue—leadership often fails to provide the necessary support to fight back. Nearly half (**48%**) of organizations cite credential-based attacks as a top concern, yet nearly **20%** of CISOs admit they conduct penetration tests only to meet compliance requirements, rather than to improve security.

While attackers move fast, too many organizations are stuck in their own timelines, waiting for the next maintenance window, budget cycle, or breach-driven wake-up call. By then, it's already too late.

Yet, global spending on cybersecurity is projected to reach $212 billion in 2025, a 15% increase from 2024, according to a top U.S. analyst firm.[4] Organizations are spending more than ever, yet attackers are winning. *Something isn't adding up.*

The State of Cybersecurity in 2025

Cybersecurity is pretty much broken—not because defenders don't care, but because they're forced into an asymmetric battle against attackers who innovate faster, exploit weaknesses instantly, have seemingly endless budgets to fund their activities, advance their toolsets daily, and never play by the rules. Meanwhile, too many organizations are stuck in slow patching cycles, reliant on once-a-year pentests, and shackled by ineffective security policies that simply don't stand a chance against today's rapidly evolving threats.

This report isn't just about data points—it's about the real-world impact behind the numbers. For security leaders, it serves as a strategic guide to building stronger defenses. For practitioners, to fight back exists—but only for those bold enough to act before attackers make the choice for them.

[4] https://securityreviewmag.com/?p=27116

Table of Contents

Vulnerability Scanning Isn't Working

Traditional vulnerability scanning is inundating security teams with alerts, delivering more noise than actionable insights. Nearly **98%** of our survey responders use some form of vulnerability scanning solution, but only **34%** consider them highly effective. **36%** report that they're overloaded with false positives and find the tools unreliable.

The result? A growing backlog of questionable vulnerabilities often left unaddressed, leaving organizations exposed. Security teams are caught in a cycle of analysis paralysis, struggling to separate critical risks from insignificant noise. With thousands of alerts but little context, teams waste valuable resources chasing down low-risk issues while real risks remain unchecked.

Attackers exploit the confusion caused by false positives and unprioritized findings, slipping through gaps in overwhelmed defenses. Worse still, the illusion of comprehensive security from vulnerability scanning creates a false sense of confidence, leaving organizations vulnerable to real-world attacks.

> By giving us a prioritized list of real, exploitable vulnerabilities, Horizon3.ai has helped us take a bite-sized approach to remediation.
>
> Instead of getting thousands of vulnerabilities from a typical scan, NodeZero highlights the ones that actually matter—along with fix actions that make them easy to address. Even if it's a vulnerability we're not used to mitigating, NodeZero provides clear guidance on how to fix it."
>
> - Art O'Cain, VP, Incident Response and Disaster Recovery, Airiam

Actionable Recommendation:

Don't get distracted by vulnerabilities without context. Risk comes down to two things: likelihood of exploitation and business impact. Consider how well you can define these two factors, and work to add insight as needed. In a reality of scarce resources, prioritization is king.

How organizations use NodeZero to address this challenge:

By prioritizing real attack paths and delivering detailed proof of compromise, NodeZero empowers security teams to act decisively, ensuring resources are directed toward mitigating the most pressing threats with the greatest potential impact.

In 2024 alone, NodeZero performed over 50,000 pentests, identifying nearly 765,000 critical impacts by successfully exploiting weaknesses within environments to reveal real-world security risks, including:

415,315
Compromised Hosts

Exposing systems that were easily compromised.

174,499
Sensitive Data Exposures

Revealing risks of data breaches and compliance failures.

87,891
Ransomware Exposures

Pinpointing unprotected data that could lead to ransomware attacks.

Additional Risks Discovered:

- **52,761** Critical Infrastructure Compromises – Threatening operational continuity.
- **3,293** Domain Compromises – Allowing attackers to hijack entire domains.
- **21,592** Domain User Compromises – Enabling lateral movement and privilege escalation.
- **206** Perimeter Breaches – Opening the door to external attackers.
- **8,559** Brand Compromises – Undermining brand integrity and trust.
- **129** Business Email Compromises – Facilitating phishing and financial fraud.

Note: Impacts summarize, in business terms, the effects NodeZero was able to achieve as a result of exploiting weaknesses in an environment.

NodeZero empowers security teams to focus on the most critical weakness that can enable compromises and exposures. By mapping real attack paths, providing definitive proof of compromise, and delivering detailed remediation guidance, organizations are quickly resolving what NodeZero discovers.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Weak Credentials and Excessive Permissions Remain a Problem

Attackers aren't just breaking in—they're logging in. **48%** of organizations cite stolen credentials and phishing as among the most dangerous cybersecurity risks.

Our production testing data shows they're right. Across over 50,000 pentests analyzed in 2024, there were 28,866 instances where NodeZero performed successful credential dumping across customer environments. In each instance, NodeZero revealed how attackers exploit credential weaknesses to escalate privileges and move laterally across networks.

In addition, **23%** of organizations specifically cite stolen user and admin credentials as the greatest potential threat they face, highlighting a growing concern. This problem is compounded by poor identity management practices. Weak passwords, password reuse, excessive permissions, and a lack of multi-factor authentication create easy targets. Once attackers gain access, they can escalate privileges, exfiltrate data, or even destroy critical systems, often without triggering a single alarm.

> One of the biggest problems we see—whether in vulnerability assessments or audits—is excessive privilege.
>
> Too many people have too much access. But what NodeZero does really well is not just finding those people—it shows exactly what an attacker could do with those privileges. It finds a user with excessive rights, then maps out all the horrible things they could do to domain controllers, Exchange servers, SQL servers."
>
> - Jon Isaacson, Principal Consultant, JTI Cybersecurity

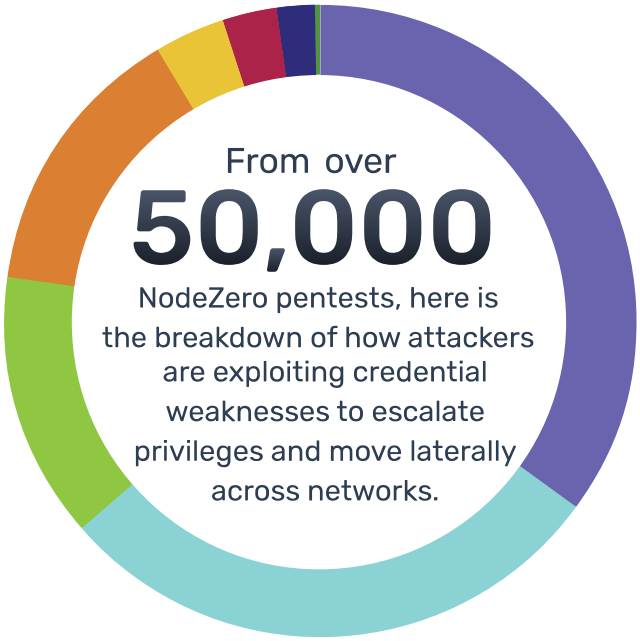
Actionable Recommendation:

Don't assume authentication controls like MFA and FIDO2 are enough—validate them. Organizations need solutions that continuously expose credential-based attack paths—revealing exploitable user and admin accounts, excessive privileges, and credential dumping risks. By proactively testing for these weaknesses and validating remediations, organizations can close these critical gaps before attackers exploit them.

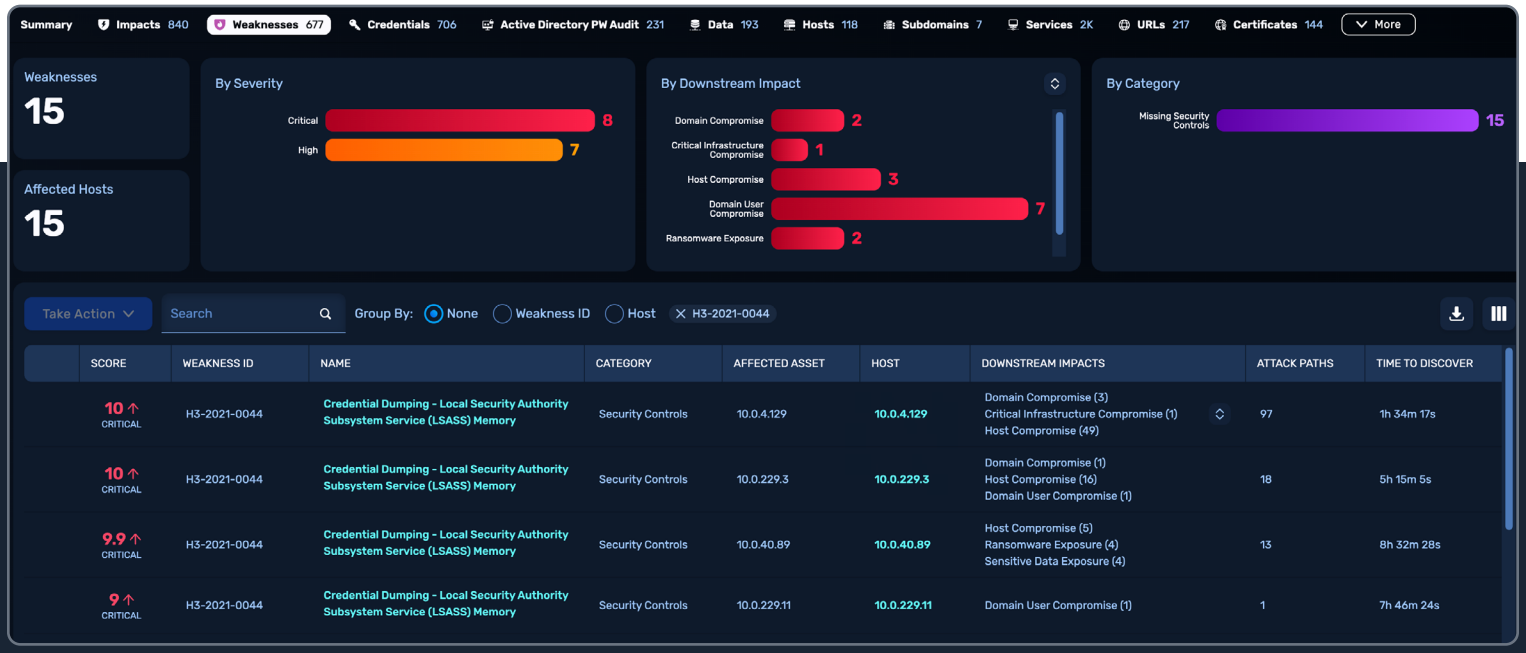
How organizations use NodeZero to address this challenge:

With NodeZero, organizations identify and remediate exploitable credential weaknesses at scale and continuously. By emulating real-world attacks, NodeZero reveals how attackers leverage weak credentials and excessive permissions to escalate privileges and move laterally.

NodeZero includes specific rules designed to detect and alert on any form of successful credential dumping, ensuring comprehensive visibility into credential risks.



- **Security Account Manager (SAM): 32.7%**
  revealing widespread exposure to SAM-based credential theft.
- **Local Security Authority Subsystem Service (LSASS) using ProcDump: 26.6%**
  indicating prevalent use of ProcDump to steal credentials from LSASS.
- **Local Security Authority Subsystem Service (LSASS) using MiniDump: 12.6%**
  demonstrating the effectiveness of MiniDump techniques for harvesting credentials.
- **Data Protection API (DPAPI): 13.2%**
  highlighting risks associated with encrypted data extraction.
- **/etc/shadow File: 3.3%**
  revealing exposure to Unix-based password hashes.
- **Office365 Application Memory: 2.6%**
  demonstrating risks in cloud-based application memory dumps.
- **Active Directory Services Database (NTDS.dit): 1.9%**
  exposing vulnerabilities in Active Directory credential storage.
- **Active Directory Services Database (NTDS.dit): .07%**
  exposing vulnerabilities in Active Directory credential storage.



NodeZero customers successfully remediated **95%** of credential dumping instances—as verified on subsequent retests—with **27,297** out of **28,866** detected cases marked as "Mitigated," demonstrating organizations' ability to rapidly resolve credential exposure risks.

These findings reinforce the fact that credential dumps to escalate privileges within a network are easily discovered by NodeZero, often bypassing endpoint detection and response (EDR) systems altogether.

HORIZON3.ai
~~TRUST~~ BUT VERIFY

Patch Overwhelm is Extending Attackers' Window of Opportunity

Attackers don't wait—but too many organizations do. Over **53%** of practitioners and **36%** of CISOs admit to delaying patches, either waiting for scheduled maintenance windows or patching when they can. This gives attackers ample time to exploit weaknesses, often with devastating consequences. Notably, **22%** of practitioners recognize unpatched but known vulnerabilities as one of their greatest potential threats, highlighting the critical need for proactive remediation strategies.

Every day a known vulnerability remains unpatched is another day for attackers to exploit it, especially for those assigned and catalogued by trusted organizations like MITRE and CISA.

By the time vendor patches are released, attackers have already weaponized exploits, rapidly scanning for unpatched systems to breach with ease. This risk is amplified by organizations clinging to rigid patching schedules and outdated vulnerability management practices, leaving critical gaps in their defenses.

> This kind of capability is truly actionable—it allows us to stay left of boom.
>
> **In today's world, where vulnerabilities are discovered and exploited in near real-time, having immediate visibility is critical.**
>
> The fact that we can receive an alert that something we rely on—despite being fully patched—is now vulnerable, empowers us to take swift, decisive action before an issue escalates."
>
> - Senior Network Architect, Electronics Manufacturing DIB

Actionable Recommendation:

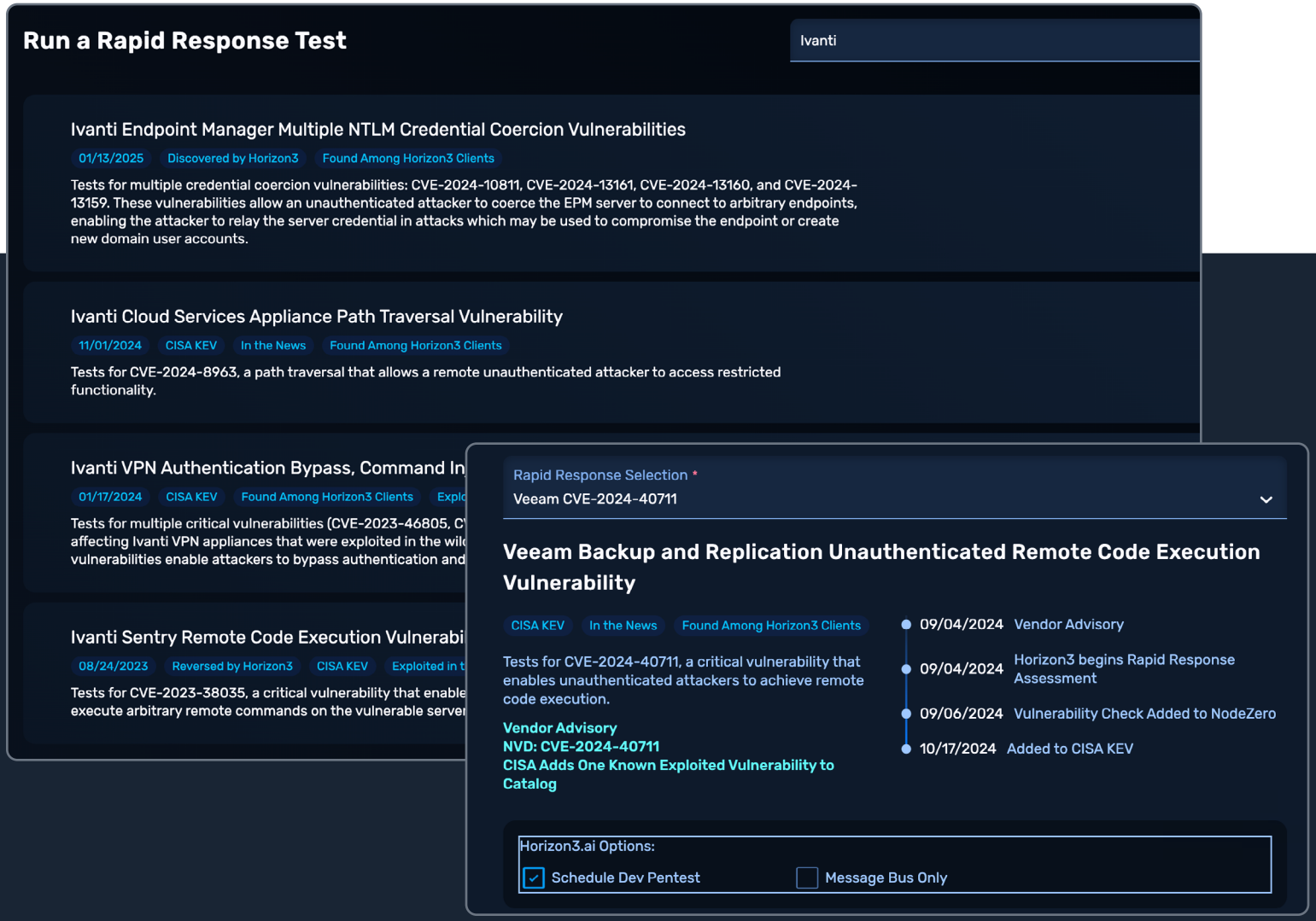
When a new vulnerability is announced, validate whether it is actually exploitable in your environment—don't assume you're at risk based on CVSS severity scores alone. Once validated, take immediate mitigation and/or remediation action and confirm that patches effectively close potential attack paths.

How organizations use NodeZero to address this challenge:

Rather than scanning for every possible vulnerability, Horizon3.ai's top-tier attack team researches what vulnerabilities are likely to be easily exploited, and to what potential impact. These are built into core NodeZero tests.

In 2024, NodeZero exploited **229** known vulnerabilities (CVEs) a staggering **99,924** times within customer environments, demonstrating the scale of the slow patching dilemma. Of these, **170** CVEs were on the CISA KEV, highlighting that organizations were running known vulnerable software that was already being widely exploited on a global scale. These included critical vulnerabilities identified by Horizon3.ai's Attack Team and others known to be actively targeted.

To bring even faster coverage to the most nascent zero- and N-day vulnerabilities, NodeZero Rapid Response added more than 50 new rapid tests with custom exploits in 2024. Many of these emerging vulnerabilities were discovered and reported by the Horizon3.ai Attack Team.



Customers are proactively alerted if NodeZero Rapid Response was able to exploit their environments, empowering them to stay ahead of emerging threats.

HORIZON3.ai
~~TRUST~~ BUT VERIFY

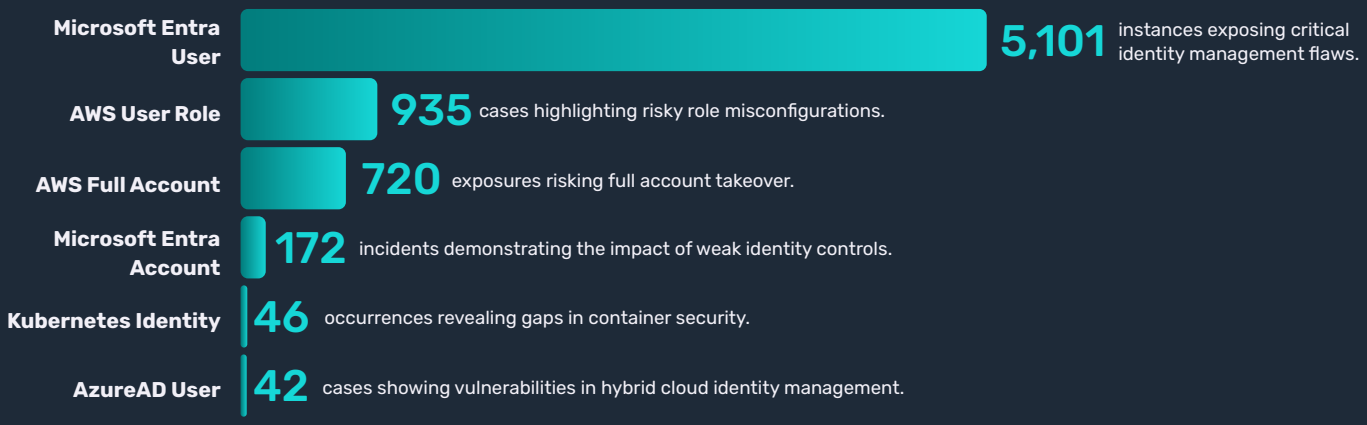
Poor Security is Plaguing Cloud Infrastructure

Over **40%** of organizations either don't regularly test their cloud environments or struggle to find an effective solution. Even more concerning, **31%** of cloud users skip security-focused pentests altogether, leaving critical applications and sensitive data exposed.

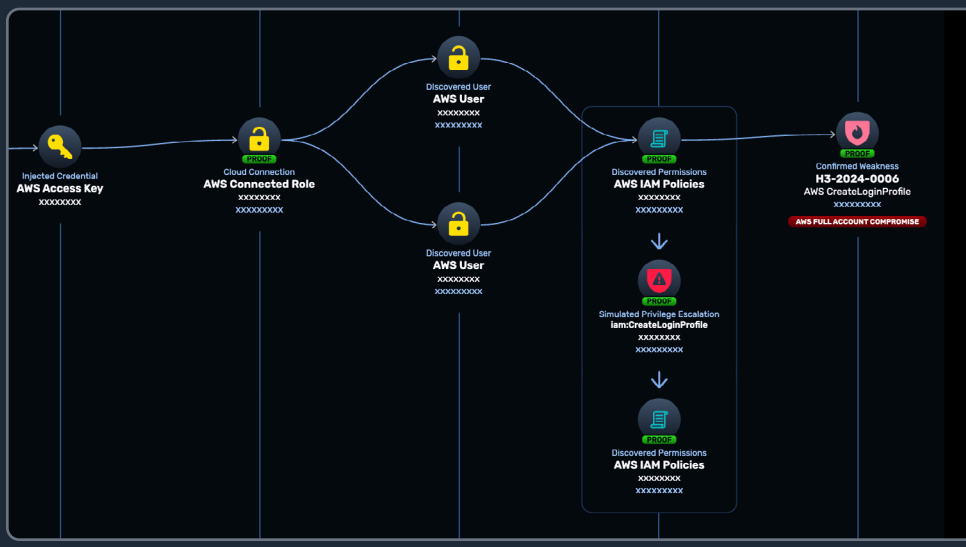
Cloud environments host everything from financial data to customer information and mission-critical applications. The lack of rigorous security testing creates dangerous blind spots.

In 2024, NodeZero uncovered **7,016** actionable weaknesses across production cloud environments, the lionshare, **72%**, stemming from Microsoft Entra User compromise.

NodeZero: Exploited Weaknesses Across Production Environments



Just like NodeZero, attackers are actively exploiting these misconfigurations, weak identity and access controls, and unpatched vulnerabilities in cloud systems.



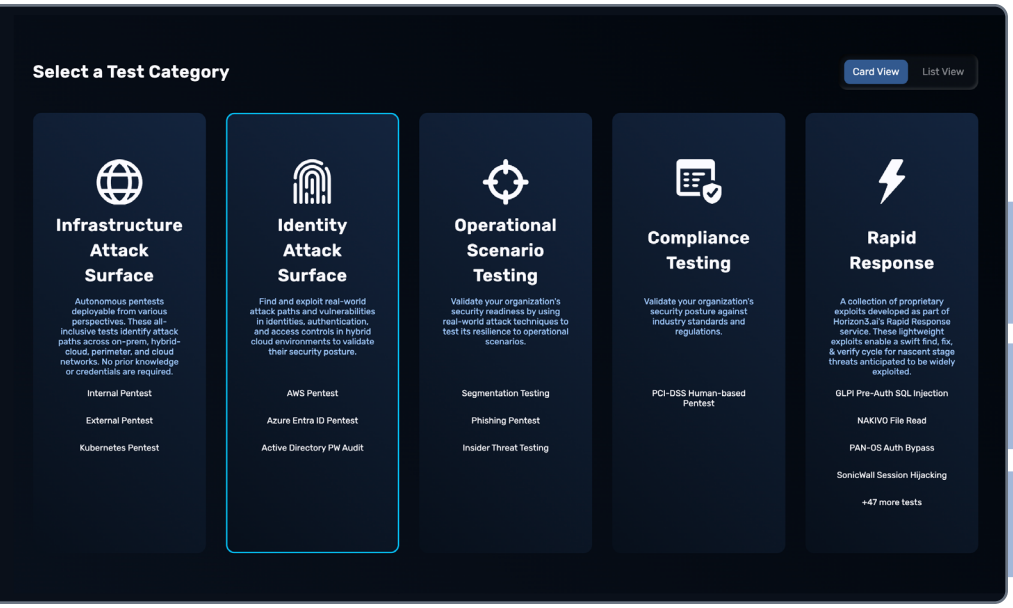
Many organizations struggle to find effective cloud security testing solutions, with a considerable portion of CISOs and practitioners stating they haven't found a tool that truly meets their needs. Overstretched IT and operations teams—often lacking cloud-specific security expertise—are forced to fill the gap, leading to visibility blind spots, inconsistent security policies, and a higher risk of human error.

Actionable Recommendation:

For teams without capacity, the highest return on your time is often focusing on identity and access (IAM) management. A first step is to audit user accounts and make sure access is appropriate. Where you find users with excessive permissions, reach out and validate whether there's a business case to warrant their access. And check with your cloud provider—most offer some free tools to support auditing.

How organizations use NodeZero to address this challenge:

NodeZero customers choose from a suite of tests that provide coverage across their cloud, on-prem, and hybrid environments. They get specific proof of exploitable cloud weaknesses so they know where to focus remediation.



These tests combine strategies that are often otherwise siloed, labor intensive, or out of reach entirely, for example:

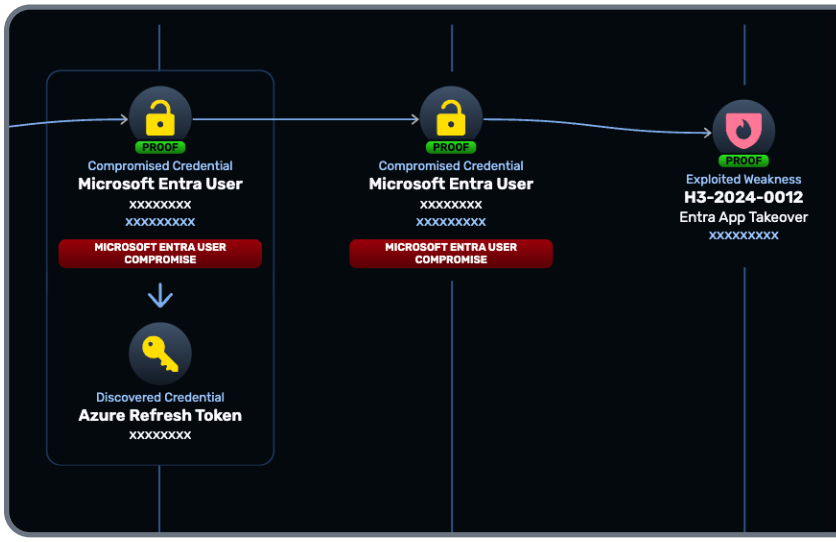
Mapping attack paths using BloodHound to map and analyze Active Directory (AD) and Azure environments.

Identifying excessive privileges and exploitable accounts via audits.

Simulating real-world attacks in production.

Proactive, continuous testing is essential to identify and remediate IAM misconfigurations, excessive permissions, vulnerabilities, and cloud security gaps before attackers can exploit them.

NodeZero pinpoints specific, exploitable cloud weaknesses, enabling security teams to focus on remediation that truly matters. Proactive, continuous cloud testing is essential to identify and remediate IAM misconfigurations, excessive permissions, vulnerabilities, and security gaps before attackers can exploit them.



HORIZON3.ai
~~TRUST BUT~~ VERIFY

Teams Failing to Reduce Mean Time to Remediation

61% of organizations acknowledge the importance of Mean Time to Remediation (MTTR), with **30%** considering it extremely important for both improving security and reducing costs. Yet, **31%** struggle with remediation due to resource constraints, and **16%** deprioritize remediation altogether.

By failing to prioritize MTTR, organizations are essentially leaving the door open for attackers, relying on hope rather than action to defend critical systems. Doing so jeopardizes compliance, threatens brand reputation, increases the likelihood of financial losses, and exposes organizations to legal consequences.

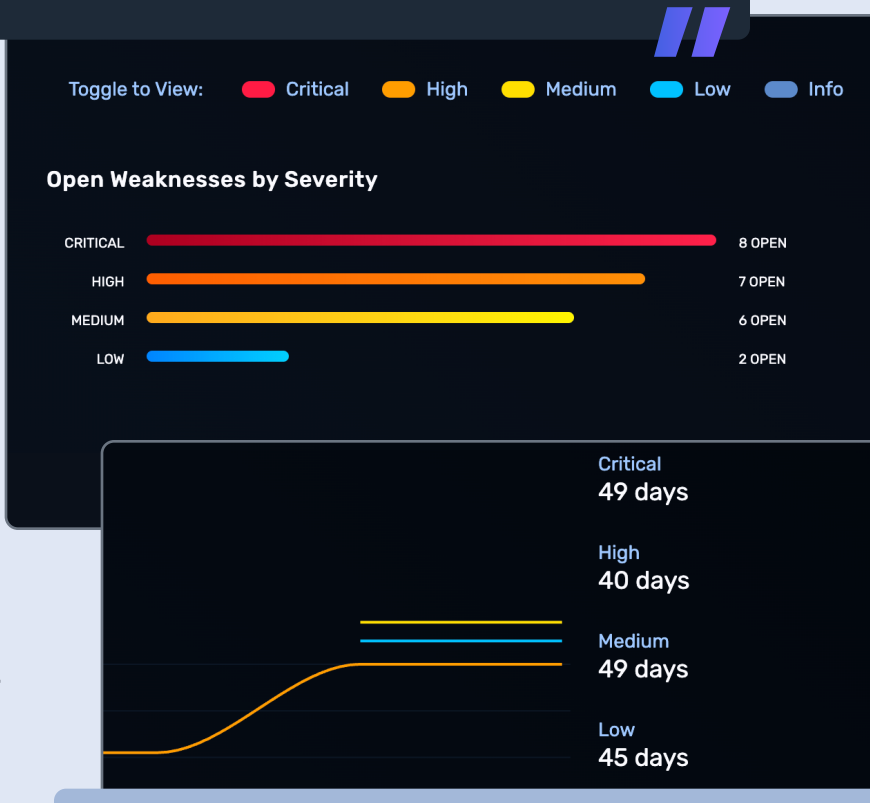
> Here's the thing though (about NodeZero). You test, identify, remediate and then just run the test again to make sure the remediation is successful.
>
> You're not capped on the number of or frequency of tests, and it only takes a couple of minutes to set up....Winner!"
>
> - Anthony Owen, Senior Security Solutions Specialist, CAE Technology Services

Actionable Recommendation:

Start by measuring your MTTR for your most critical weaknesses. Understanding your baseline and setting goals for improvements among this subset will help cross-functional teams better sense their impact. It will also focus business stakeholders on your most meaningful remediation.

How organizations use NodeZero to address this challenge:

First, with NodeZero, customers think about MTTR in terms of what's most likely to be exploited and cause material business impact. They use this priority to make progress where it matters most, and can track their MTTR accordingly.



NodeZero Insights™ shows MTTR trends over time with filters for weakness criticality and CISA KEV status.

CASE STUDY

Major national materials provider serving the aerospace, marine, military, and medical sectors.

During their first uncredentialed internal pentest using NodeZero in May 2024, NodeZero:

- Compromised a domain, revealing critical security gaps.
- Gained access to **23%** of their user accounts, demonstrating the impact of weak credentials.
- Discovered **2 million** sensitive resources vulnerable to ransom-based attacks.

Recognizing the severity of these exposures, they hardened their infrastructure and remediated the weaknesses identified. When they conducted a follow-up internal pentest they verified the following improvements:

285 weaknesses mitigated

151 critical and high severity vulnerabilities mitigated

	Critical Impacts	Overall Weaknesses	Compromised Credentials	Compromised Hosts	
First Test with NodeZero	477	483	893	84	First Test with NodeZero
Follow-Up Test Results	56	377	225	13	Follow-Up Test Results

This study demonstrates how an iterative cycle of testing, remediation, and verification, enables organizations to continuously strengthen their security posture and reduce MTTR.

HORIZON3.ai
~~TRUST~~ BUT VERIFY

Low Trust Undermines Manual Pentests

Traditional manual pentesting is leaving organizations dissatisfied, unsure, and exposed:

- **41%** of organizations feel third-party pentest reports are filled with suspect results, making it difficult to prioritize remediation.
- **27%** of organizations report that pentesters often don't fully understand their infrastructure, resulting in potential false positives, false negatives, and a disconnect between testing and real-world risks.
- **24%** say the reports don't provide guidance on how to remediate critical issues, leading to remediation paralysis.

> "I ran NodeZero on one of our organizations, and it uncovered a vulnerability in a roundabout way—one issue exposed another, which led to compromised credentials and access to something even more critical.
>
> **That kind of insight has been a godsend for us.**
>
> It takes a lot of time and energy off my pentesters' plates, allowing them to focus on more complex challenges rather than repetitive manual tasks."
>
> - Brian Beckwith, Chief Technology Officer, Intuitus

Over **40%** of organizations report their pentest results are invalid due to environmental changes between when the test was run and the report delivered. In real-world environments, configurations change, new vulnerabilities emerge, and user access shifts constantly. Organizations are left with exploitable blind spots, giving attackers a predictable window to strike.

In the end, only **11%** of organizations report no challenges with traditional pentesting. The high costs, limited scope, and slow nature of traditional pentesting simply don't meet the needs of modern security teams facing agile, persistent attackers.

Actionable Recommendation:

Replace point-in-time assessments with continuous pentesting to detect and eliminate threats in real-time. Look for SaaS solutions that provide actionable insights and clear remediation guidance. This shift from static, snapshot-based assessments to dynamic, adaptive security testing will empower you to stay ahead of attackers and protect critical assets with confidence.

How organizations use NodeZero to address this challenge:

NodeZero delivers autonomous pentesting at scale, executing dynamic attack paths that mimic real-world adversaries to identify exploitable weaknesses. With the ability to test tens of thousands of hosts in a single operation, it ensures no part of the network is left untested. Organizations can schedule recurring tests to continuously validate security fixes, ensuring defenses remain resilient against evolving threats.

NodeZero demonstrates that continuous validation must operate at breakneck speed to enable truly proactive cybersecurity. Unlike traditional pentesting—where human testers take breaks, stop for the day, or juggle multiple tasks—NodeZero operates without interruption. This relentless, autonomous approach matches the speed and sophistication of modern attackers.

In an analysis of **50,000 NodeZero pentests**, the results were striking:

- The fastest path to a critical impact, such as attaining domain admin access, was achieved by NodeZero in just **60 seconds**, underscoring the speed at which it can compromise high-value assets.
- On average, it took NodeZero **14 hours** to reach a critical impact.
- Manual pentests take **5–10 days** for networks under 500 hosts and over four weeks for larger networks with thousands of hosts.

Search | Critical Infrastructure Compromise

SCORE	NAME	TYPE	HOSTS	TIME TO COMPROMISE
10 CRITICAL	GitLab ExifTool Remote Code Execution Vulnerability (CVE-2021-22205)	Critical Infrastructure Compromise	10.2.51.107	47m 58s
9.8 CRITICAL	VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985)	Critical Infrastructure Compromise	10.0.4.29	3m 10s
9.8 CRITICAL	Zoho ManageEngine Desktop Central Authentication Bypass Vulnerability (CVE-2021-44515)	Critical Infrastructure Compromise	10.0.4.22	1h 40m 27s
9.8 CRITICAL	VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972)	Critical Infrastructure Compromise	10.0.4.29	3m 7s
9.8 CRITICAL	VMware vRealize Network Insight Remote Code Execution Vulnerability (CVE-2023-20887)	Critical Infrastructure Compromise	10.0.4.26	2m 57s
9.8 CRITICAL	Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass Vulnerability (CVE-2022-40684)	Critical Infrastructure Compromise	10.0.4.25	18m 20s

These findings underscore the importance of continuously validating defenses and mimicking real-world attacker behavior. It demonstrates that effective security validation isn't just about speed, but about persisting until the comprehensive scope of risk is understood.

Security Leaders Settling for Annual Pentests

84% of organizations were impacted by a cyberattack in the past year, partly due to the fact that only **26%** conduct pentests more than once annually—and nearly **20%** of CISOs said they only do so because of mandates, regulations, or policies. This infrequent testing leaves exploitable gaps open for months, giving attackers a predictable window to strike.

Attackers exploit predictable pentest cycles like those mandated by PCI DSS, which requires testing only once a year—giving attackers a clear window to strike. While security teams face ever-changing attack surfaces and new vulnerabilities, regulations like NIS 2 and DORA push for more frequent security assessments. It's only a matter of time before PCI DSS and other standards follow suit.

Actionable Recommendation:

Organizations must move beyond doing the bare minimum to meet compliance and adopt a proactive, high-frequency assessment model to stay ahead of evolving threats. Regulatory requirements set a baseline, but true security demands continuous validation of security posture. By going beyond compliance mandates with continuous risk assessments, organizations can strengthen their defenses, stay ahead of emerging threats, and easily prove their security posture to auditors—reducing compliance burdens and avoiding costly penalties.

How organizations use NodeZero to address this challenge:

An analysis of how often organizations run NodeZero pentests, based on a review of over 50,000 customer-run tests in 2024, revealed:

- The average interval between two tests was approximately **10 days**, indicating that organizations using NodeZero are consistently validating their security posture.
- The median interval was **6 days**, indicating that many organizations are adopting near-daily testing to continuously evaluate and strengthen their defenses.
- The longest interval was **315 days**, highlighting that some organizations are stuck in the once-per-year mindset, exposing themselves to extended windows of risk.

By validating fixes immediately after remediation, organizations reduce exposure windows and ensure vulnerabilities remain closed.

This commitment to continuous assessments is reflected in customer behavior. **82%** of Horizon3.ai customers have increased their testing frequency to monthly, with **40%** testing weekly or more, proving that frequent validation leads to stronger security outcomes.

> We provide this as an ongoing service, and we're seeing far more traction than with traditional penetration testing. In fact, we pivoted our own approach—we now pentest ourselves every week, instead of waiting for an annual test.
>
> That shift has given us far better visibility into what's happening in our environment in real time."
>
> - Calvin Engen, Chief Technology Officer, F12.net

Organizations Stuck in Reactive Security Mode

30% of organizations admitted they only perform cyber risk assessments after an attack has occurred. Only **8%** of organizations conduct year-round continuous cyber risk assessments, a practice widely regarded as the cornerstone of effective cybersecurity across every known security framework.

This isn't just a security failure—it's a strategic failure. Reactive security limits visibility, slows down remediation, and increases the cost and impact of infrastructure and data breaches. Organizations stuck in this cycle of reactivity are exposing themselves to operational disruptions, financial losses, regulatory penalties, reputational damage, and legal repercussions.

> We run four different test scenarios—starting in the middle of the network where full access is possible, then moving to different populations. We conduct both black-box attacks and injected credential tests.
>
> It's eye-opening to see how NodeZero works in those scenarios."
>
> - Jim Beers, DIrector of Information Security, Moravian University

Actionable Recommendation:

Move from reactive firefighting to proactive security operations. Instead of waiting for an incident to reveal security weaknesses, security teams need tools to continuously probe for newly emerged attack paths, identify critical exposures, and take action before threats materialize. A proactive security model ensures that defenses are always ahead of adversaries.

How organizations use NodeZero to address this challenge:

In January 2025 alone, Horizon3.ai's customers conducted **6,342** testing operations (Ops), demonstrating their proactive commitment to securing their infrastructures.

- **Internal Pentest – 3,628 Ops:** Credentialed and non-credentialed internal pentests to uncover internal risks like misconfigurations.
- **External Pentest – 1,389 Ops:** Real-world external attacks to validate perimeter defenses.
- **External Asset Discovery – 556 Ops:** Mapping external attack surfaces to identify exposed assets.
- **Active Directory (AD) Password Audit – 314 Ops:** Assessing credential security and identity management within AD environments.
- **Network Enumeration – 278 Ops:** Mapping network devices, services, and attack paths.

Cloud Security Operations:

46 Ops
Azure Pentest

41 Ops
AWS Pentest

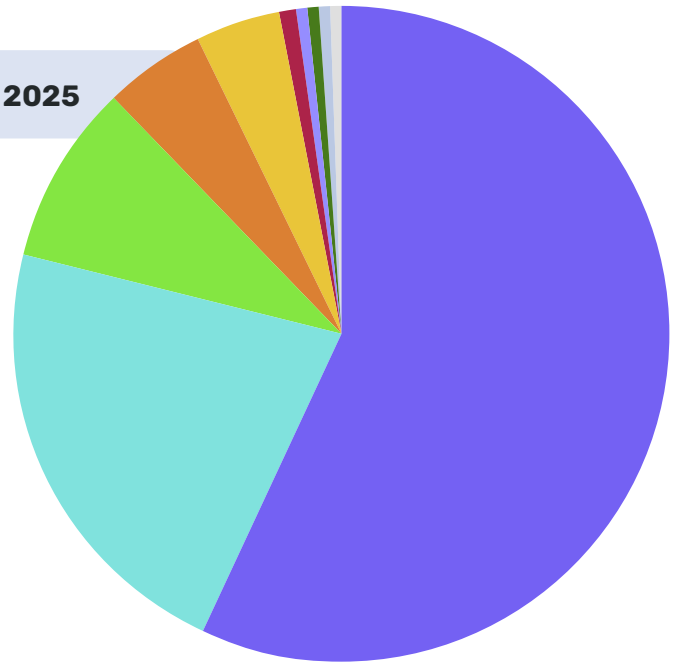
27 Ops
Kubernetes (K8) Ptentest

Social Engineering and Insider Threat Simulation:

Phishing
36 Ops
Testing user awareness and mapping the blast radius of phished credentials.

Insider Threat
27 Ops
Validating internal security controls against privilege misuse.

Distribution of Security Operations in January 2025



This number of NodeZero operations isn't just a metric. It's a testament to the industry-wide shift toward proactive cybersecurity. Organizations that embrace continuous validation aren't just improving security; they're ensuring their defenses evolve faster than adversaries can adapt.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Failure to Adopt Offensive Exercises

27% of organizations experienced operational disruptions like downtime and outages due to cyberattacks. Yet, only **18%** of companies are investing in proactive security measures, such as offensive exercises, to measure resilience before they're attacked.

The reluctance to adopt offensive security exercises isn't due to a lack of awareness. As mentioned in the beginning of this report, **97%** of security leaders agree that organizations must start using the same TTPs as attackers to adequately assess their risk. However, **39%** admit they lack the resources to implement such tactics, and **18%** are hesitant because of the perceived risks associated with offensive approaches. Despite these challenges, **45%** believe that leveraging manual and automated adversarial techniques is necessary to adequately assess their risk, underscoring the growing recognition that defense alone is not enough.

This strategic oversight is compounded by a lack of actionable, forward-looking intelligence. **41%** of CISOs want to know which assets attackers are most likely to target first, indicating a strong need for early-warning signals and precise risk prioritization. This highlights a significant gap in predictive intelligence—one that offensive security exercises can help fill by exposing the attack paths that adversaries are most likely to exploit.

Meanwhile, **37%** of CISOs are seeking clearer ways to communicate current risk levels to leadership and the board, revealing a lack of insights into the current state of their security posture. Offensive security exercises provide definitive, proof-based insights that accurately assess vulnerabilities and expose exploitable attack paths.

Actionable Recommendation:

The Department of the Navy[5] and the Joint Force Headquarters–Department of Defense Information Network (JFHQ-DODIN)[6] have transitioned from compliance-based assessments to readiness-based. Their approach integrates adversarial exercises that blend manual expertise with automation, acknowledging that true readiness is only measurable through real-world attack scenarios. Organizations should adopt this model by performing regular offensive security exercises and red team operations to uncover hidden attack paths, validate security controls, and assess SOC effectiveness.

> Continuous visibility and continuous penetration testing will be the new standard to ensure security effectiveness—regardless of what technology stack an organization is using.
>
> Larger companies are waking up to the fact that security testing can't just be an annual checkbox for compliance.
>
> It has to be done on a recurring basis to be defensible and to ensure the right protections are in place before they become a target."
>
> - Calvin Engen, Chief Technology Officer, F12.net

[5] https://media.defense.gov/2023/Nov/21/2003345095/-1/-1/0/DEPARTMENT%20OF%20THE%20NAVY%20CYBER%20STRATEGY.PDF

[6] https://www.cybercom.mil/Media/News/Article/3689870/jfhq-dodin-to-officially-launch-its-new-cyber-operational-readiness-assessment/DEPARTMENT%20OF%20THE%20NAVY%20CYBER%20STRATEGY.PDF

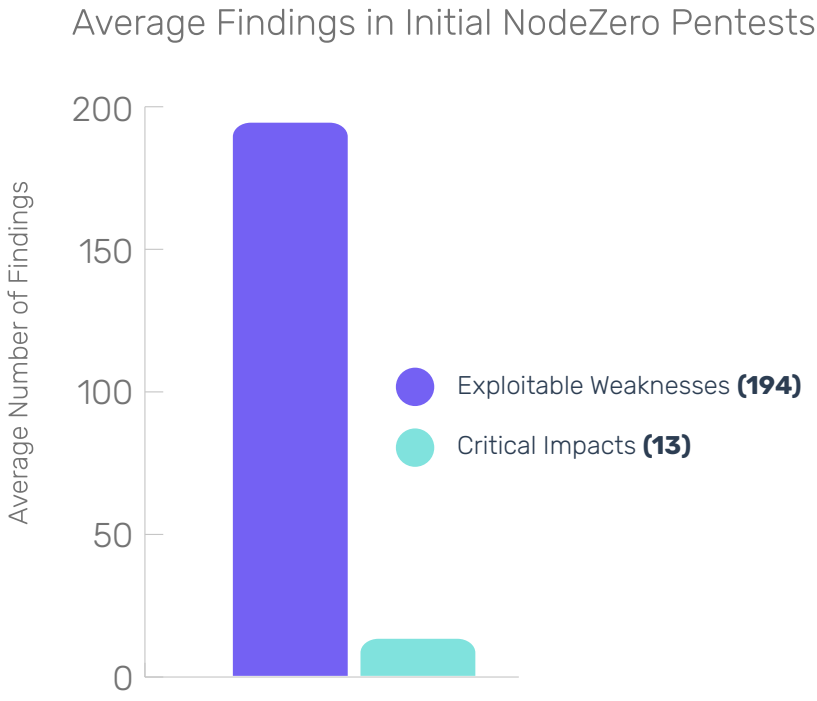
How organizations use NodeZero to address this challenge

NodeZero extends and enhances offensive expertise for any organization, whether security is managed by the IT team alone or there's an advanced red team in house. This approach:

- Makes offensive exercises accessible for IT-teams on the hook for security.
- Empowers blue teams building their offensive skills.
- Frees red teams to focus on the most advanced cyber security risks.

Not only does NodeZero continuously deliver new attack content across a suite of test types, with every test, it "shows its work". This means teams gain transparency and learn from every exploit with:

- Detailed attack paths that led to business impacts.
- Commands to replicate attacks.
- Detailed explanations of weaknesses and impacts.
- Precise, instructive fix actions.



Organizations using NodeZero report a nearly **100%** chance of discovering critical vulnerabilities, exploitable weaknesses, and data at risk within their networks **on the first run.** NodeZero consistently uncovers dozens of exploitable attack paths often missed by traditional pentests.

Data from nearly **120,000** all-time NodeZero pentests provides undeniable evidence of its effectiveness. In initial assessments of large-scale networks, an average of **132** to **256** exploitable weaknesses were uncovered. Moreover, each test revealed between **5** and **21** critical impacts—potentially severe attack paths that conventional security assessments often overlook.

Despite widespread agreement that organizations must test their defenses like real attackers would, many still hesitate due to resource constraints or perceived risks.

Yet, the data is clear—organizations leveraging offensive security exercises gain critical insights that traditional assessments fail to provide.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Conclusion: The Inevitable Cybersecurity Shift

The old adage “the only constant in life is change” couldn’t be more applicable to cyber security. Defenders are fighting an uphill battle against adversaries who innovate relentlessly, adapt instantly, and exploit gaps faster than security teams can react.

Yet, many organizations rely on vulnerability scans, conduct infrequent risk assessments, trust untested defenses, and often treat compliance as the ultimate goal instead of a baseline. Meanwhile, threats evolve daily, exposing critical gaps that attackers are ready to exploit.

Even with cybersecurity budgets projected to hit $212 billion in 2025, the current strategy is failing. Risk assessments are still being performed only once a year—or worse, after an incident—leaving organizations vulnerable for months at a time. This status quo isn’t just ineffective. It’s a liability.

Cybersecurity’s old playbook is obsolete. The choice is no longer about improving defenses—it’s about going on the offense.

Be proactive or be breached.

Attack yourself or be attacked.

Those who embrace this shift today will be the ones who survive tomorrow. The battlefield has already changed.

> This report is a wake-up call: the reactive approach to cybersecurity is failing.
>
> Attackers move at machine speed, chaining weaknesses for maximum impact, while organizations remain stuck in outdated, compliance-driven security. We need to stop playing defense and start thinking like the adversary. The only way to win is to attack yourself before attackers do—proving resilience through continuous, real-world validation.”
>
> - Snehal Antani, CEO of Horizon3.ai

About the Survey

The survey highlighted in this report was conducted by Censuswide | Research Consultants. Censuswide is an international market research consultancy headquartered in London, with offices in New York, Dubai, Bristol, and Glasgow. Censuswide strictly adheres to the MRS Code of Conduct and ESOMAR principles and is a member of the British Polling Council, reinforcing a commitment to ethical research practices and data integrity.

Who Was Surveyed

- 375 CISOs and CIOs in the UK, USA, France, Spain, Germany, and Italy from October 15-30, 2024.
- 379 IT Practitioners in the UK, USA, France,Germany, Italy, and Spain from October 15-31, 2024.

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

HORIZON3.ai
~~TRUST~~ BUT VERIFY