HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

5 Key Benefits of NodeZero™ for Enhancing Security in Financial Services Organizations

FinancialServices

5 Key Benefits of NodeZero™ for Enhancing Security in Financial Services Organizations

How Autonomous Security Testing Empowers Financial Organizations to Proactively Manage Risk, Ensure Compliance, and Enhance Operational Efficiency

Financial services organizations manage vast amounts of personally identifiable information (PII) and conduct sensitive financial transactions globally, making them prime targets for cybercriminals. Their infrastructures are often complex, spanning on-premises, cloud, and hybrid environments across multiple geographies. This complexity presents significant challenges in maintaining both security and operational integrity. They face a constantly evolving threat landscape, with risks ranging from external attacks to insider threats.

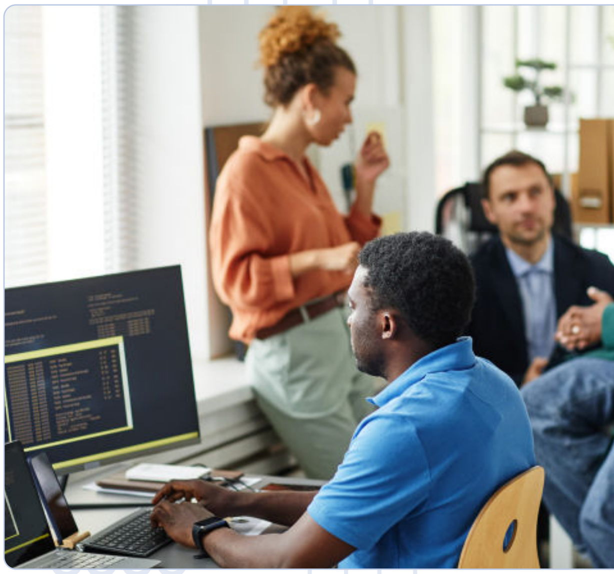
Traditionally, these organizations have relied on periodic risk assessments such as annual penetration tests or sporadic vulnerability scans to measure and document their cyber risk. Whether driven by regulatory requirements, concerns over fraud prevention, or mitigation of insider threats, these episodic assessment approaches have proven inadequate to measure, manage, and mitigate cyber risk. Financial organizations now realize that effective cyber risk management requires real-time assessments rather than infrequent ones.

This white paper explores how **NodeZero™**, the autonomous security platform from Horizon3.ai, addresses these challenges head on by delivering continuous, offensive-based security testing, real time risk-visibility, and actionable executive-level insights. By doing so, NodeZero empowers CISOs and security leaders in financial services to not only measure risk at any given moment, but also reduce it proactively. Through strategic use of NodeZero, organizations can reduce regulatory compliance costs, enhance their security posture, and drastically reduce MTTR (Mean Time to Remediation) by identifying and addressing exploitable attack paths quickly and efficiently.

This white paper serves both security leaders and practitioners within financial services. It offers CISOs strategic insights into how **NodeZero** and **NodeZero Insights™** help track and reduce risk, communicate progress to boards of directors, and meet governance, risk, and compliance initiatives through data-driven assessments. For practitioners, it provides an in-depth look at how NodeZero's autonomous pentesting capabilities streamline vulnerability remediation and ensure that security measures are both strategic and actionable.

Table of Contents

Understanding the Financial Sector's Evolving Cyber Threat Landscape



A successful breach in the financial services industry can lead to significant financial losses, regulatory fines, reputational damage, and potential lawsuits. Regulatory bodies such as the Financial Conduct Authority (FCA) in the UK, the European Central Bank (ECB) in the EU, and the Securities and Exchange Commission (SEC) in the US are enforcing strict requirements for breach notifications, security risk assessments, ongoing risk management, and consumer data protection. Non-compliance with these regulations can result in severe penalties and even personal legal action, highlighting the critical need for advanced, continuous security measures.

The Limitations of Traditional Cyber Risk Assessments

Many financial organizations rely on periodic penetration tests to assess the security risk levels of their IT infrastructures. However, this approach is less than optimal. Traditional penetration testing is typically conducted annually or quarterly, meaning that months can pass between assessments – months during which new vulnerabilities and other weaknesses can emerge and go unchecked. This creates critical windows of exposure where financial organizations are vulnerable to exploitation.

Additionally, manual pentesting methods tend to be labor-intensive and limited in scope. While they provide valuable insights, they are often narrow in focus, examining only portions of the infrastructure or focusing on critical systems alone. These assessments frequently overlook the broader attack surface and fail to identify causative vulnerabilities, software misconfigurations, ineffective security controls, systemic security weaknesses, and complex attack paths that adversaries can exploit.

The interval between periodic assessments puts financial organizations at risk. Horizon3.ai's NodeZero™ autonomous security platform changes this by modernizing the way cyber risk is measured and managed. Shifting from a defensive posture to an offensive, adversarial strategy allows for a more accurate measurement of risk, which is where NodeZero delivers significant value to the financial services industry. Before exploring the specific benefits for financial organizations, let's first examine the platform's extensive capabilities.

Introducing NodeZero: Autonomous Security Platform

NodeZero offers financial organizations a reliable and continuous solution to penetration testing and cyber risk assessments – one that addresses the shortcomings of all other approaches. By conducting real-time autonomous penetration tests across the entire digital infrastructure of a financial institution, they're provided with ongoing visibility into exploitable vulnerabilities, including those that are unknown or undocumented. Not only does it identify weaknesses, but it shows practitioners where to apply their fixes, followed by a one-click verification process that proves fixes are successful.

Key Features of NodeZero

Here is a list of the key features NodeZero delivers:

- **Internal Pentesting:** Identifies, exploits, and documents vulnerabilities and exploitable attack paths within the organization's internal infrastructure.
- **External Pentesting:** Discovers an organization's footprint on the internet, using tools and methods attackers use to evaluate the security of public-facing systems.
- **Cloud Pentesting:** Extends its penetration testing capabilities to AWS and Azure environments, ensuring that cloud-based assets and IAM configurations are secure.
- **Kubernetes Pentesting:** Deploys NodeZero inside Kubernetes clusters, performing real-world attacks, exposing misconfigurations, RBAC issues, and container escapes.
- **NodeZero Insights:** Equips leaders and practitioners with the tools to track company-wide security initiatives and measures overall security posture over time.
- **NodeZero Tripwires:** Deploys decoys, such as fake files and credentials, along proven attack paths of at-risk assets during NodeZero pentests.
- **Rapid Response Service:** Provides early, actionable intelligence about nascent stage vulnerabilities that are newly discovered and not yet widely known or adequately addressed.
- **AD Password Audit:** Reveals user passwords in an AD environment that are likely targets for credential stuffing, credential abuse, and password cracking attacks.
- **Phishing Impact Testing:** Captures user credentials during simulated phishing attacks and uses them during pentests to understand the broader impact.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

The AI in NodeZero

NodeZero is not built on large language models (LLMs), and no customer data is shared or stored in open-source AI frameworks. Instead, NodeZero's intelligence evolves through continuous reinforcement learning, shadowing, and collective intelligence. Operating as an autonomous agent, it independently executes actions to meet specific penetration testing objectives, such as gaining Domain Admin access, compromising sensitive data, and infiltrating critical systems. Over time, its effectiveness improves as it leverages knowledge graph analytics, inference engines, and iterative learning processes, making it increasingly adept with each test.

In contrast, other **automatic penetration testing solutions** depend on hard coding scripts for every possible attack path – an impractical task given the dynamic nature of modern network environments. The complexity and maintenance burden of such scripts have hindered the scalability of "automated" pentesting solutions. NodeZero's **autonomous** model, delivered via a multi-tenant SaaS platform, eliminates these challenges and serves customers from the Global 100 to SMEs with unmatched efficiency.

Now, let's take a closer look at the five key benefits that NodeZero offers to financial services organizations, demonstrating how it strengthens security, lowers costs, optimizes operational efficiency, and meets the distinct challenges of the industry. These benefits underscore NodeZero's ability to deliver valuable insights, comprehensive protection, and cost-effective solutions tailored to the specific needs of the financial sector.

Latest NodeZero Statistics

NodeZero is purpose-built to assess complex environments at scale, spanning on-premises, cloud, and hybrid infrastructures. Below are key statistics highlighting the increasing adoption of NodeZero in organizations of all sizes.

~ 6,000 tests conducted each month

~ 195 tests run daily

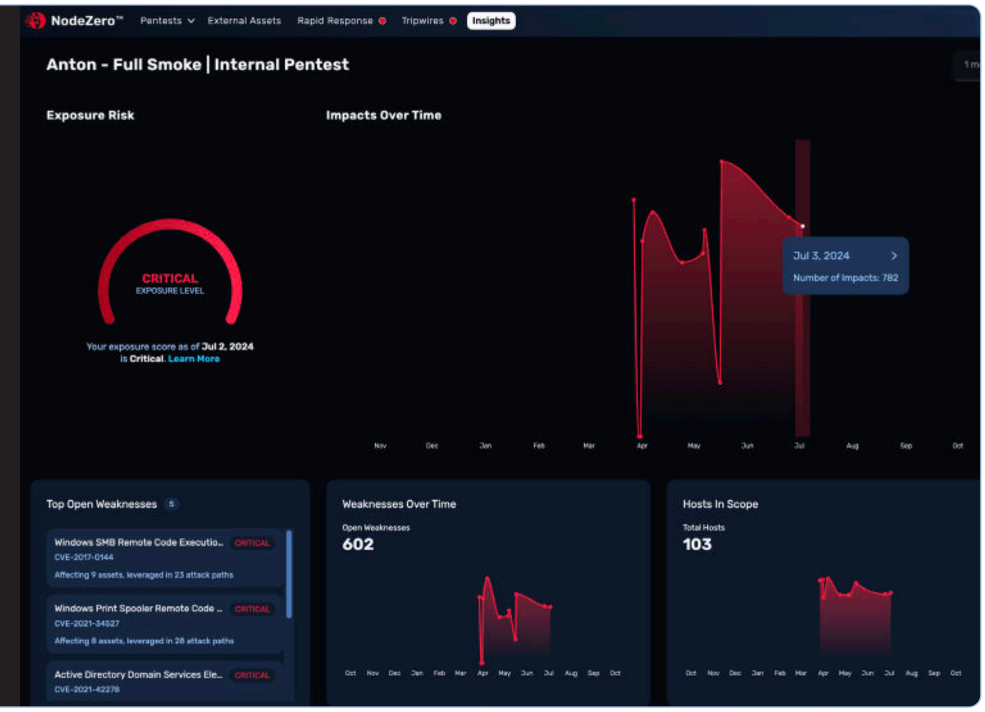
~ 44,000 tests performed in 2024

~ 80,000 tests executed since its launch

~ 100,000 tests projected for 2025, based on current usage trends

Benefits of the NodeZero Platform

Benefit #1: Delivers Executive-Level Visibility for CISOs



Anton - Full Smoke | Internal Pentest

Exposure Risk

Your exposure score as of **Jul 2, 2024** is **Critical**. Learn More

Impacts Over Time

Top Open Weaknesses 5

Windows SMB Remote Code Executio... CRITICAL
CVE-2017-0144
Affecting 9 assets, leveraged in 23 attack paths

Windows Print Spooler Remote Code ... CRITICAL
CVE-2021-34527
Affecting 8 assets, leveraged in 28 attack paths

Active Directory Domain Services Ele... CRITICAL
CVE-2021-42278

Weaknesses Over Time
Open Weaknesses
602

Hosts In Scope
Total Hosts
103

While NodeZero focuses on penetration testing, **NodeZero Insights™** provides the executive-level visibility that CISOs and security leaders need to effectively communicate the state of their organization's security. Through its comprehensive dashboards, **NodeZero Insights** aggregates data from its penetration tests into a single, easy-to-understand interface, offering insights that can be shared with the Board of Directors and other executive stakeholders.

Figure 1: *Example of NodeZero Insights Dashboard*

Key Features of NodeZero Insights

- **Tracking security trends over time:** Enables CISOs to track how their organization's security posture evolves. By visualizing trends, security KPIs, and remediation efforts, leaders can see whether their organization is improving its defenses month-over-month.
- **Remediation velocity:** By measuring how quickly teams are remediating vulnerabilities, NodeZero Insights helps organizations pinpoint areas where additional security investment might be needed. It also ensures that remediation efforts align with strategic goals.
- **Reporting to the board:** Simplifies the reporting process, allowing CISOs to present progress against benchmarks like the MITRE ATT&CK framework. This builds confidence among executive stakeholders that the organization is on track in mitigating their cyber risk.

Benefit #2:
Identifies Fraud and Insider Threat Risks

Vulnerability management is the cornerstone of any strong cybersecurity program; NodeZero significantly enhances this process by providing continuous vulnerability data. While many financial organizations rely on vulnerability scanning tools, these tools often struggle to differentiate between theoretical vulnerabilities and those that are truly exploitable, including risks tied to financial fraud and insider threats. Financial organizations are particularly vulnerable to these risks, as they involve misuse of legitimate access and exploitation of systemic weaknesses.

NodeZero addresses these challenges by focusing on vulnerabilities that pose immediate threats to the organization's security, including those that could be leveraged in fraudulent activities or by malicious insiders. By using the same tactics, techniques, and procedures (TTPs) attackers use, NodeZero helps security teams identify internal weaknesses stemming from poor password policies, weak or reused credentials, risky privileged accounts, and unnecessary insider access. This enables organizations to focus their remediation efforts more effectively, ensuring that high-risk, fraud-related, and insider threat vulnerabilities are addressed first.

NodeZero's ability to seamlessly integrate with vulnerability management programs and complement existing vulnerability scanning tools makes it a vital asset to any security strategy. By providing actionable intelligence on vulnerabilities with the potential for financial fraud and insider attacks, it allows financial organizations to maximize the value of their existing security tools while significantly reducing risks. The added context of specific risks helps to improve the organization's resilience against both external and internal attackers, enhancing overall security postures.

Benefit #3:
Lowers Compliance Costs

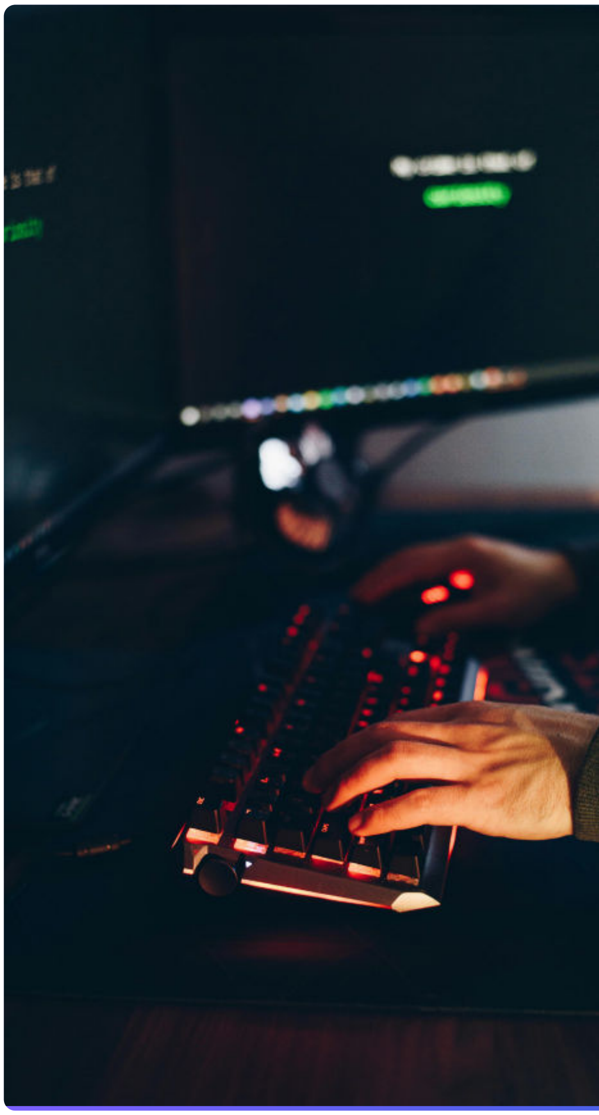
Financial services organizations face numerous regulatory requirements that mandate regular cyber risk assessments. Regulations such as GDPR and GLBA, and standards like PCI DSS require financial institutions to conduct regular assessments of their security posture. Compliance with these regulations often involves significant costs, especially when relying on third-party penetration testing services.

NodeZero offers a cost-effective alternative to traditional third-party assessments by providing on-demand and scheduled penetration testing. Unlike third-party pentesters who conduct assessments annually or quarterly, leaving months between evaluations, NodeZero enables unrestricted assessments, often for less cost than a single penetration test. By reducing the reliance on external pentesting services, financial organizations can significantly lower the costs associated with compliance while still meeting regulatory requirements for ongoing risk assessments.

Additionally, the comprehensive and automated nature of NodeZero ensures that financial services organizations can address vulnerabilities as they arise, rather than waiting on third-party assessors. This proactive approach aligns well with regulatory standards such as those enforced by the Financial Conduct Authority (FCA), the Securities and Exchange Commission (SEC), and the Federal Financial Institutions Examination Council (FFIEC), all of which mandate regular risk assessments and security management practices.

By utilizing NodeZero, financial organizations can achieve the same, if not higher, levels of compliance at a lower cost, as the platform can be continuously used to identify exploitable vulnerabilities across the entire digital infrastructure. This not only saves the direct costs of third-party assessments but also reduces the risk of non-compliance fines and penalties, ultimately delivering a significant return on investment.

Benefit #4:
Advances CTEM and ASM Initiatives



As financial services organizations move toward adopting Continuous Threat Exposure Management (CTEM) and Attack Surface Management (ASM) initiatives, NodeZero becomes an essential tool in enhancing both strategies. CTEM requires organizations to continuously assess and manage risks across their entire environment, ensuring constant visibility into potential threats. NodeZero seamlessly integrates into this process by uncovering real-world attack paths and identifying truly exploitable vulnerabilities in real time. This instantaneous insight ensures financial organizations stay ahead of emerging threats and adjust their security defenses as needed to mitigate risks quickly.

In the context of ASM, NodeZero's capabilities play a pivotal role in identifying, mapping, and securing the organization's attack surface. Financial services organizations, with their complex and interconnected environments, are particularly vulnerable to potential security gaps across on-premises, cloud, and hybrid systems. NodeZero autonomously scans the full attack surface and provides deep visibility into every part of the infrastructure, ensuring that no critical assets or network segments are left unchecked. This comprehensive visibility ensures that financial organizations can proactively manage their attack surface, reducing the risk of exploitation.

By adopting NodeZero as part of their CTEM and ASM strategies, financial organizations can focus their efforts into remediating what is actually exploitable. NodeZero's ability to validate security controls and test for real-world vulnerabilities allows organizations to remain resilient and ensure business continuity while helping them comply with strict regulatory requirements.

Benefit #5:
Provides Cost Savings Through Reduced MTTR

The Mean Time to Remediation (MTTR) for vulnerabilities, often ranging between 30 to 90 days[1][2], stems from a combination of factors. First, many organizations face a resource shortage, both in terms of personnel and tools, which slows down the identification and remediation process.

Vulnerabilities are often spread across complex, interconnected systems, requiring teams to prioritize critical patches while balancing day-to-day operational demands. Additionally, legacy systems and technical debt contribute to delays, as older infrastructure is harder to patch without causing disruption to the business.

Since the time between a vulnerability being announced and it actively being exploited in the wild (often known as time-to-exploit (TTE)) continues to shorten, organizations can't waste valuable time chasing low-risk vulnerabilities. They must focus their efforts on fixing what matters most. This is where NodeZero excels in the context of reducing MTTR.

Human-led pentests often rely on manual processes, leading to delays between identifying vulnerabilities, reporting on what was discovered, then allowing teams to address the issues found. The industry must shorten the time between identifying and remediating exploitable vulnerabilities. Not doing so only serves to widen the window of opportunity for attackers.

With NodeZero, vulnerabilities are not only found quickly but are also prioritized based on the risk they pose to the organization.

This enables security teams to focus on the most critical issues first, streamlining the process of remediation and minimizing exposure windows.

NodeZero streamlines the remediation process by offering clear, step-by-step guidance, eliminating the guesswork and back-and-forth typically associated with patching. This ensures that the right fixes are applied efficiently, precisely where they are needed most.

In addition to identifying and fixing vulnerabilities, NodeZero plays a crucial role in verifying that risks have been effectively mitigated. After remediation steps are implemented, NodeZero can automatically retest specific areas or systems to confirm that vulnerabilities have been successfully patched and that no new risks have emerged.

The NodeZero platform integrates seamlessly with existing vulnerability management workflows, allowing security teams to act fast. This equates to significant cost savings in the context of reducing the amount of time and effort it takes to remediate issues. This in turn shortens the vulnerability window attackers look to exploit.

This continuous validation process provides assurance that remediation efforts are being streamlined. This closed-loop process of finding, fixing, and verifying that vulnerabilities no longer exist helps organizations maintain a stronger security posture with minimal delay.

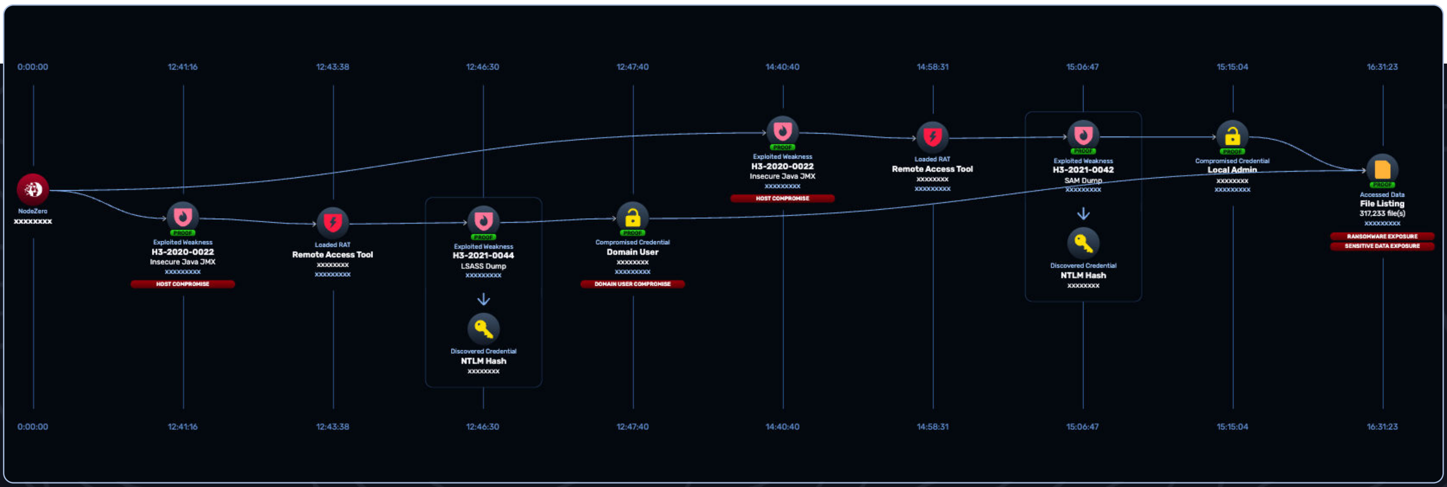
[1] https://info.edgescan.com/vulnerability-statistics-li23

[2] https://www.qualys.com/forms/tru-research-report/

Real-World Impact: A Financial Services Case Study

A large financial services organization committed to helping their clients improve their long-term financial success recently implemented NodeZero to pentest its complex environment. Previously, the organization relied on annual penetration tests, but they felt this approach left significant gaps in coverage.

During an evaluation of how NodeZero could help secure their organization, they launched NodeZero against their entire infrastructure. Within ~16 hours, NodeZero identified a critical attack path by exploiting multiple weaknesses. If the organization had left these weaknesses unresolved, they would have exposed themselves to a potential breach that could have resulted in a ransom demand. Let's look a little closer at how NodeZero easily compromised their environment.



▲ ***Figure 2:*** *NodeZero Attack Path*

Looking at the attack path from left to right in Figure 2, NodeZero:

- Discovered an Insecure Java JMX Configuration and compromised that host.
- Installed a Remote Access Tool (RAT) on that compromised host.
- Performed a LSASS Dump and then discovered another privileged credential.
- Using that credential, it compromised the Domain User's account and then gained access to over 300,000 files.
- Gained access to customer credit card and social security number information stored in those files.

Since adopting NodeZero, the financial organization has not only remedied the situation above, but now has continuous visibility into its infrastructure and is able to identify and prioritize critical vulnerabilities for faster remediation.

Although Figure 2 is a relatively simple attack path, NodeZero is fully capable of combining vulnerabilities and other weaknesses that often result in increasingly complex attack paths as shown in Figure 3.

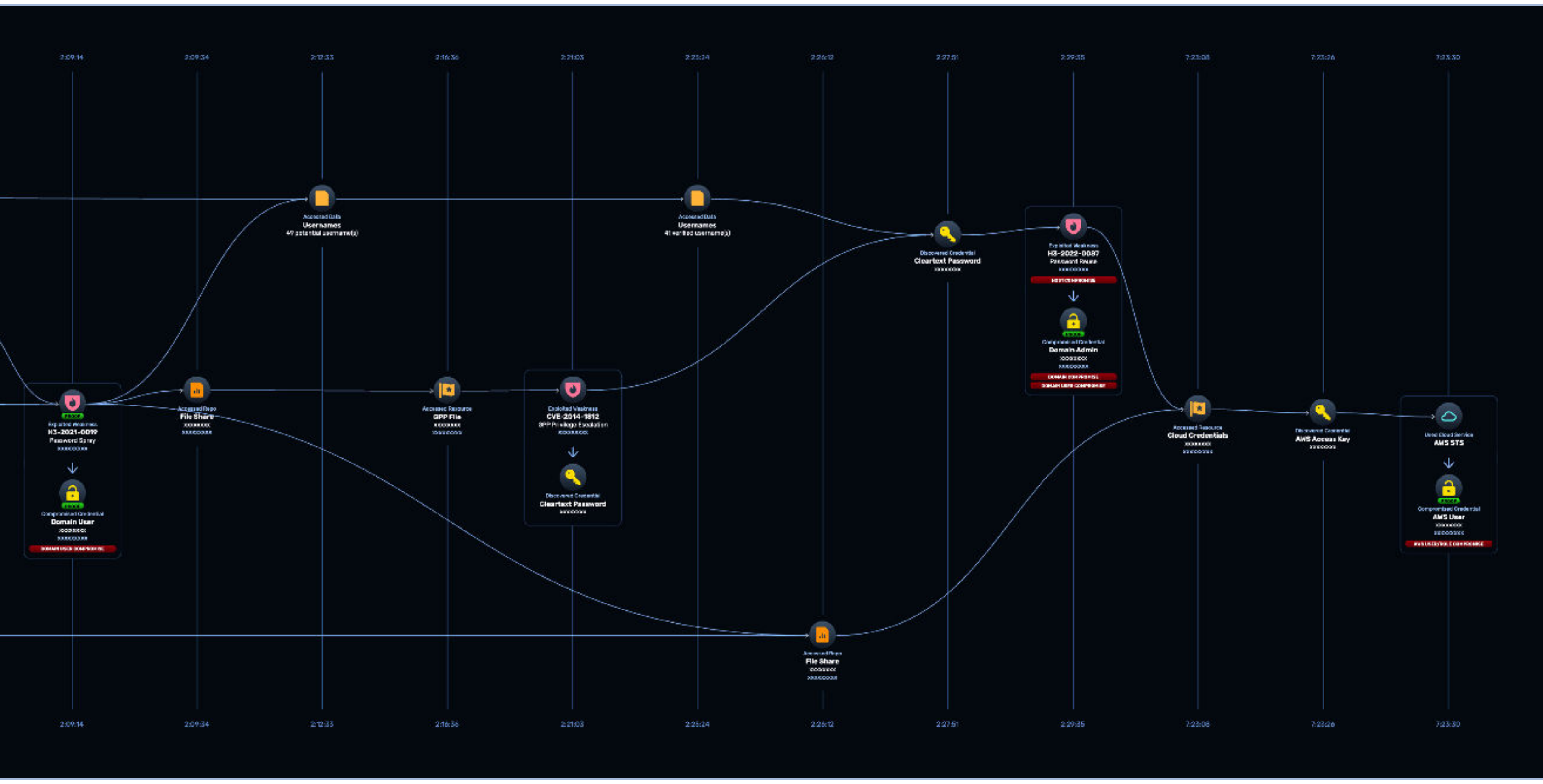


Figure 3: *More Complex NodeZero Attack Path*

NodeZero safely identifies vulnerabilities, misconfigurations, and insufficient security controls, chaining these weaknesses together to uncover very complex attack paths that manual penetration testing often overlooks. By using real-world adversarial behavior, NodeZero goes beyond isolated findings, mapping out multi-step attack scenarios that span on-premises, cloud, and hybrid environments.

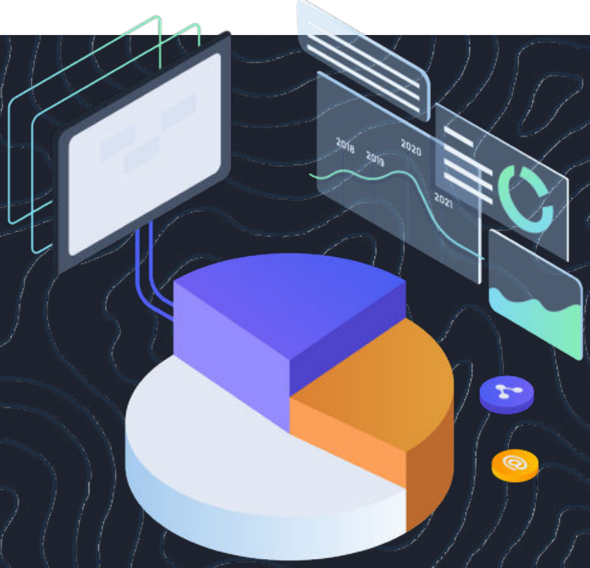
This capability enables organizations to proactively address hidden risks and strengthen their overall security posture. For each weakness discovered, NodeZero provides easy-to-follow remediation steps regardless of attack path complexity. Often, remediating a critical vulnerability or weakness can disrupt NodeZero's ability to exploit these complex attack paths, preventing potential breaches before they occur.

Conclusion: Securing the Future of Financial Services with NodeZero

As financial organizations navigate an increasingly sophisticated and volatile cyber threat landscape, defensive security measures alone are no longer enough to keep pace with today's risks. Periodic assessments, manual testing, and reactive security measures leave critical gaps that adversaries are exploiting. In a sector where data breaches can lead to significant financial and reputational losses, as well as compliance penalties, the need for continuous, real-time cybersecurity assessments is more urgent than ever.

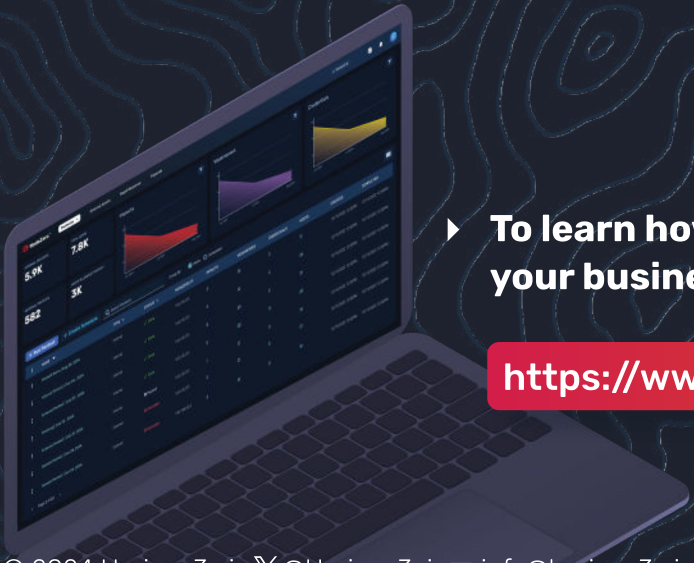
NodeZero and NodeZero Insights provide the comprehensive solutions financial organizations need - to move from reactive to proactive security. For financial services organizations, the benefits of adopting NodeZero are clear. By providing unmatchable visibility, lowering fraud and insider risks, reducing compliance-related costs, managing attack surfaces continuously, and shortening MTTR, organizations can not only lower their cyber risk but also reduce costs while doing so.

NodeZero is more than just a cybersecurity tool – it is an essential part of forward-looking, offensive-based readiness initiatives. Its ability to integrate seamlessly with vulnerability management programs and support continuous threat monitoring ensures that financial organizations remain resilient against evolving threats. By embracing NodeZero, financial organizations can secure both their infrastructure and their reputations, while ensuring long-term protection against the threats of tomorrow.



- **To test drive NodeZero in your own environment, sign up for a free trial.**

https://www.horizon3.ai/trial



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

https://www.horizon3.ai/demo

HORIZON3.ai
~~TRUST BUT~~ VERIFY