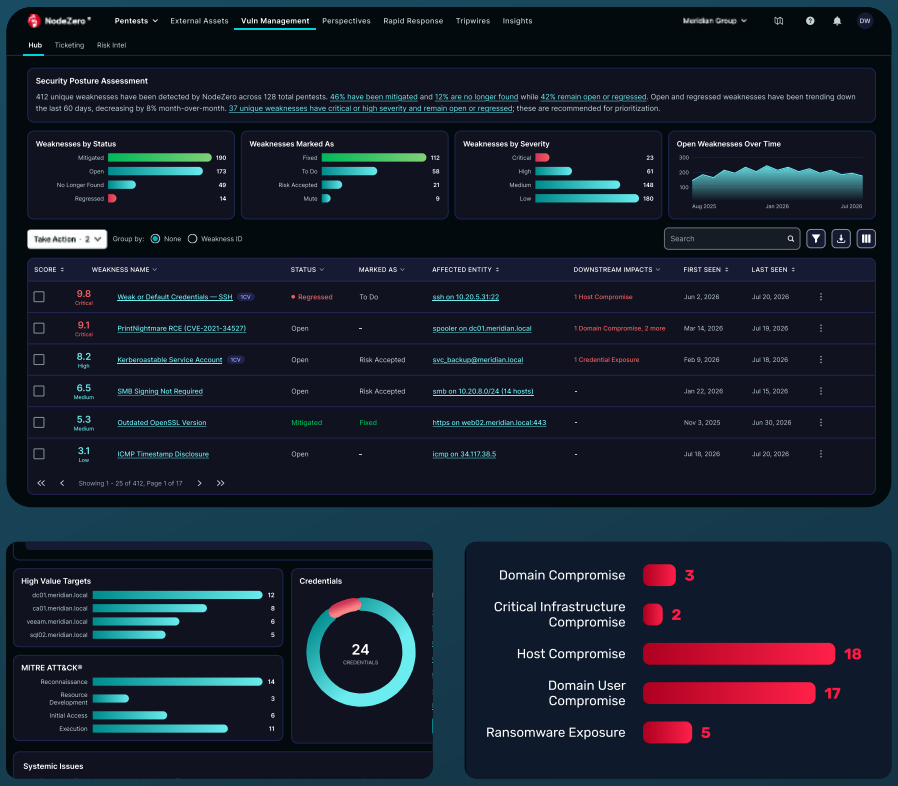
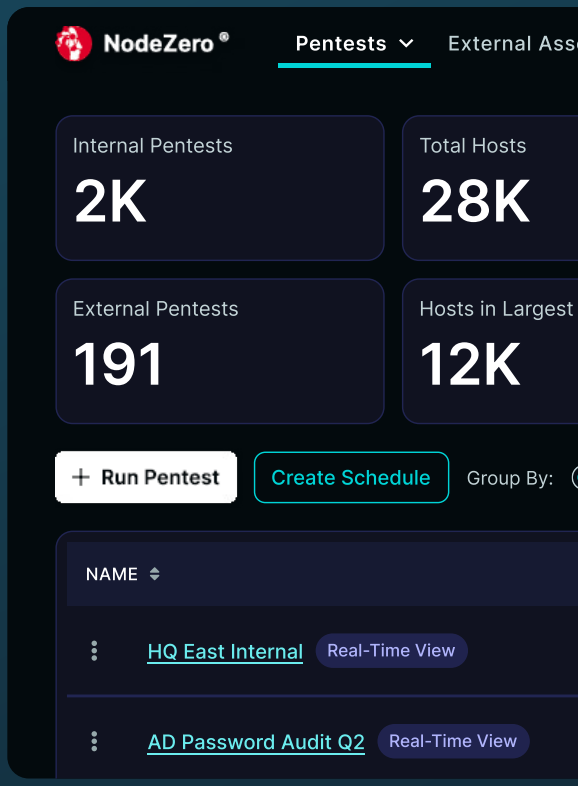
HORIZON3

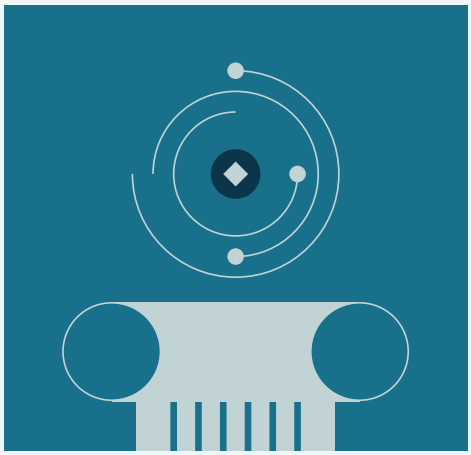
5 Key Benefits of NodeZero® for Enhancing Security in Financial Services Organizations

How Autonomous Security Testing Helps Financial Organizations Manage Risk, Support Compliance, and Improve Operational Efficiency





WHITEPAPER

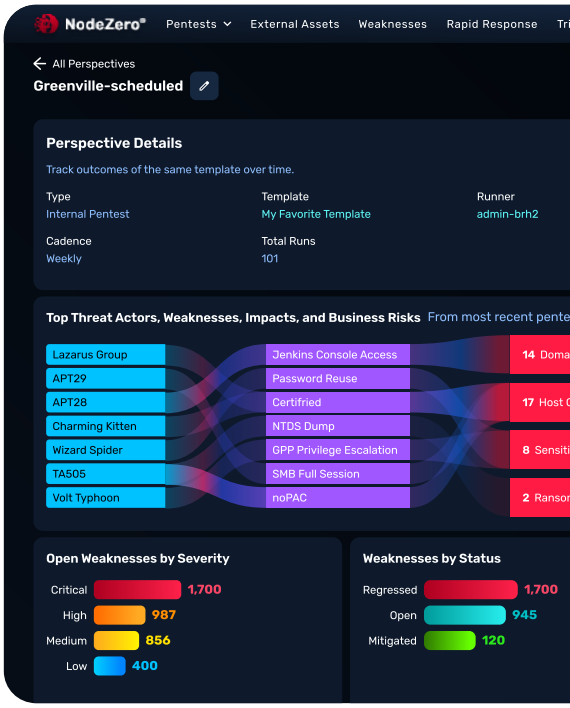


Financial services organizations manage sensitive customer information and process financial transactions across complex, interconnected systems. Their infrastructures span on-premises, cloud, and hybrid environments, often across multiple geographies. Protecting that data and maintaining critical services requires understanding which weaknesses attackers can exploit and how far that access could take them.

Periodic penetration tests and vulnerability assessments provide valuable insights, but their findings reflect the environments assessed at the time. New vulnerabilities, configuration changes, and changes to access permissions can introduce exposure between assessments. Financial organizations need a repeatable way to identify exploitable attack paths and understand their potential consequences, including unauthorized access that could enable fraud, insider abuse, or disruption.

This whitepaper explores how the NodeZero Proactive Security Platform from Horizon3 addresses these challenges through autonomous, production-safe security testing. NodeZero chains exploitable weaknesses into attack paths, demonstrates their impact, and provides actionable remediation guidance. Teams can then implement fixes and retest to verify that those changes closed the identified exposures. This approach helps financial organizations focus resources where they matter most, support compliance activities, and reduce the time and effort spent addressing security weaknesses.

For CISOs and security leaders, the paper explains how NodeZero and NodeZero Insights help track exposure and remediation progress, inform investment decisions, and communicate results to boards. For practitioners, it shows how autonomous testing supports exposure management, prioritizes weaknesses based on demonstrated impact, and verifies that remediation worked. Together, these capabilities connect executive oversight with measurable security improvements.





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 have established requirements and supervisory expectations addressing operational resilience, cyber risk management, or cybersecurity disclosures, depending on the institution and jurisdiction. These obligations reinforce the need for financial organizations to assess exposure regularly, address exploitable weaknesses, and demonstrate measurable progress in reducing cyber risk.

The Limitations of Traditional Cyber Risk Assessments

Many financial organizations rely on periodic penetration tests to assess the security of their IT infrastructures. However, testing annually or quarterly can leave months between assessments, during which new vulnerabilities and other weaknesses can emerge and go unchecked. These gaps create windows of exposure that attackers can exploit.

Additionally, manual pentesting can be labor-intensive and constrained by the time and scope of each engagement. While these assessments provide valuable insights, they may examine only portions of the infrastructure or focus on selected critical systems. As a result, exploitable vulnerabilities, software misconfigurations, ineffective security controls, and complex attack paths elsewhere in the environment may remain undiscovered.

Addressing these gaps requires a repeatable testing approach. Before exploring the five benefits for financial organizations, let's examine how NodeZero supports that approach.

Introducing NodeZero: Proactive Security Platform

NodeZero offers financial organizations autonomous, production-safe penetration testing to assess exposure on demand and as environments change. By safely chaining vulnerabilities and other weaknesses into attack paths, it shows teams what attackers can exploit and which systems and data they can reach. NodeZero provides clear remediation guidance, followed by targeted retesting to verify that fixes worked.

Key Capabilities for Financial Services

Autonomous Pentesting: Tests internal, external, cloud, and Kubernetes environments to uncover exploitable weaknesses and demonstrate how attackers could compromise systems and data.

NodeZero WebApp: Tests custom web applications, including authenticated workflows, for exploitable business logic, access control, and session weaknesses. Provides evidence developers can use to investigate and remediate findings.

NodeZero Insights: Consolidates pentest findings into dashboards that help security leaders track exposure, measure remediation progress, and communicate results to executives and boards.

Active Directory Password Audit: Identifies weak passwords, helping teams address credential exposure that could enable unauthorized access to financial systems and customer information.

High-Value Targeting: Identifies high-value accounts and systems and tests whether attackers can reach or compromise them, helping teams prioritize protection of critical financial services assets.

Advanced Data Pilfering: Finds and validates sensitive data exposure, demonstrating which customer records and financial information attackers could access.

Production Safety by Design

For financial institutions, security testing must account for the availability of systems that support transactions, customer access, and daily operations. Production safety has been NodeZero's highest engineering priority since the beginning. Its architecture was built to support autonomous testing against live systems, with a track record of repeated use in real production environments.

That safety is built into how NodeZero selects, constrains, and executes actions. Engineered operational boundaries and guardrails govern routine execution without depending on a person to approve every step. NodeZero uses prevalidated, internally tested actions for exploitation; it does not use generative AI to create or execute exploits.

Within those boundaries, NodeZero combines graph-based reasoning, deterministic logic, machine learning, and generative AI. Graph reasoning supports attack planning, deterministic software provides controlled execution, and machine learning helps classify files and behaviors. Generative AI supports specific tasks such as identifying high-value targets, analyzing exposed data, and explaining findings in business terms, using selected models hosted through Amazon Bedrock for inference rather than training foundation models.

For financial organizations, this approach makes production safety the foundation for repeatable security testing. Teams can assess exploitable exposure as environments change while keeping operational continuity central to the testing approach. The following five benefits show how that capability supports security leadership, remediation teams, and financial services priorities.

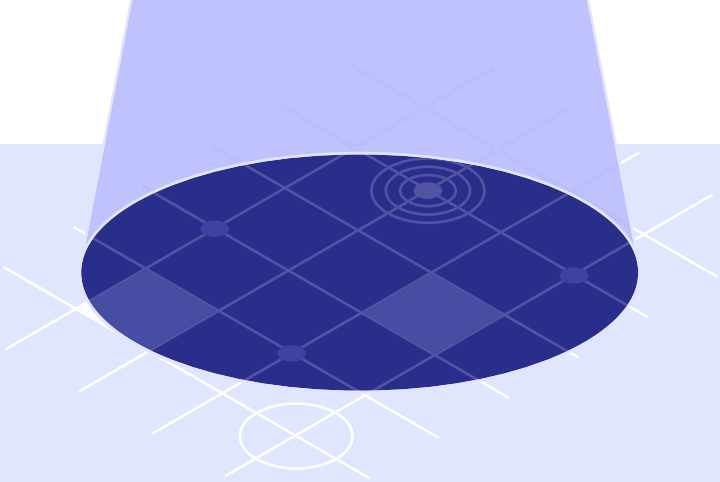


Delivers Executive-Level Visibility for CISOs

NodeZero Insights provides the executive-level visibility CISOs and security leaders need to communicate their organization's security posture. Its dashboards aggregate NodeZero pentest results into reports and visualizations that show exposure, remediation progress, and recurring weaknesses. For financial services leaders, this evidence helps inform security investments and explain progress to boards and other executive stakeholders.

Key Features of NodeZero Insights:

- → Tracking security trends over time: Visualizes open weaknesses and attack paths by severity and type. Leaders can examine recurring test results to see where exposure is declining and where further action is needed.
- → Measuring remediation progress: Tracks mean time to remediation and the age and severity of open weaknesses, helping leaders identify backlogs and determine where teams may need additional resources.
- → Identifying systemic issues: Highlights patterns such as credential reuse and recurring misconfigurations, helping teams recognize when broader policy or control changes are needed.
- → Reporting to the board: Simplifies executive reporting with summaries and exportable visualizations, helping CISOs communicate demonstrated exposure, remediation progress, and outstanding priorities.



Benefit

2

Identifies Fraud and Insider Threat Risks

Vulnerability management is a core component of financial services security, but vulnerability scans alone do not establish which weaknesses attackers can exploit or what access they could gain. This distinction matters when assessing exposure that could enable financial fraud or insider abuse, where legitimate access and weaknesses in security controls can put sensitive systems and customer data at risk.

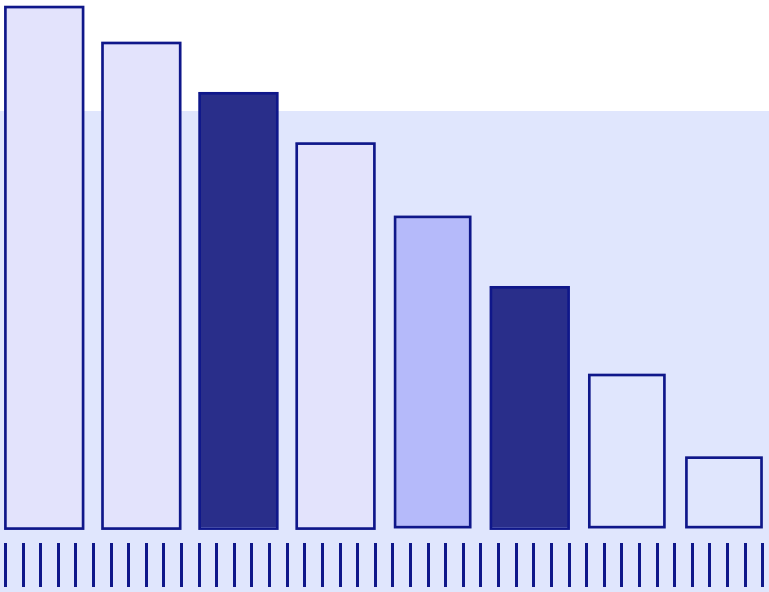
NodeZero helps teams identify these exposures by using attacker tactics, techniques, and procedures to test what is achievable within the environment. It uncovers attack paths involving weak or reused credentials, excessive privileges, and misconfigurations. The resulting evidence shows how an attacker or malicious insider could use available access to reach sensitive systems and data or expand their access through exploitable weaknesses.

These findings help financial organizations prioritize remediation based on demonstrated consequences. A weak credential that enables access to customer records, for example, warrants attention because of what it exposes. High-Value Targeting and Advanced Data Pilfering add context by identifying critical accounts and systems and validating access to sensitive information.

By complementing existing vulnerability management programs with evidence of exploitability and impact, NodeZero helps teams address the security weaknesses that could enable fraud and insider abuse. That evidence supports focused changes to credentials, permissions, and controls, reducing opportunities for unauthorized access.

Benefit

3



Lowers Compliance Costs

Financial services organizations face numerous regulatory requirements and industry standards governing security risk management and customer data protection. Standards such as the Payment Card Industry Data Security Standard (PCI DSS) include penetration testing requirements. Supporting these obligations can involve significant costs, especially when organizations rely on separately scheduled third-party engagements for testing and retesting.

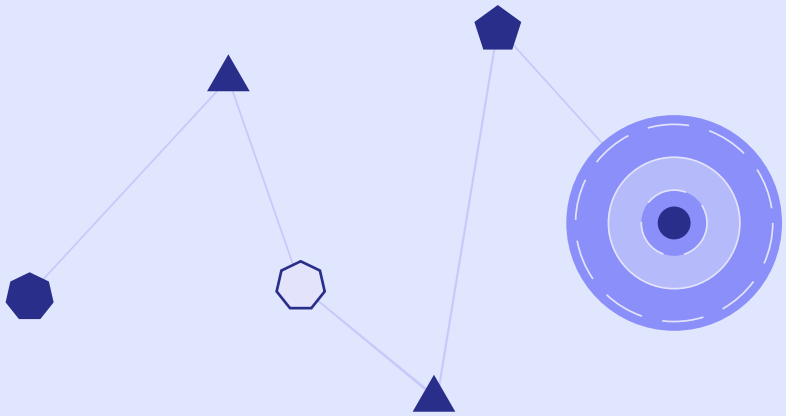
NodeZero helps manage these costs by providing on-demand and scheduled penetration testing. Teams can identify exploitable weaknesses, implement fixes, and verify remediation throughout the year. This reduces reliance on separate engagements for routine testing while complementing assessments that require specific expertise or independence.

This proactive approach also supports the broader objectives of requirements and guidance from bodies such as the Financial Conduct Authority (FCA), the Securities and Exchange Commission (SEC), and the Federal Financial Institutions Examination Council (FFIEC). Although their respective obligations and expectations differ, ongoing testing provides evidence that can inform operational resilience, customer information protection, and security risk management efforts.

By using NodeZero, financial organizations can expand testing frequency and maintain documented findings, remediation guidance, and verification results to support compliance activities. This helps teams use assessment budgets more efficiently and reduce the effort required to prepare evidence for audits and examinations.

Benefit

4



Advances CTEM and ASM Initiatives

As financial services organizations adopt Continuous Threat Exposure Management (CTEM) and Attack Surface Management (ASM) initiatives, NodeZero helps connect discovered exposure to evidence of what attackers can exploit. By uncovering attack paths and demonstrating their impact, it gives teams a practical basis for deciding which weaknesses deserve attention first.

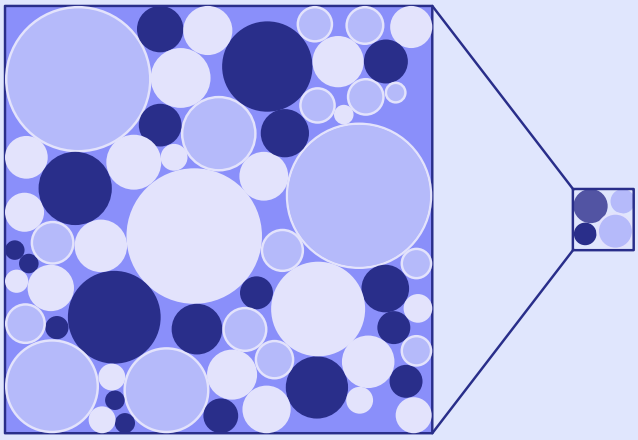
Within CTEM, NodeZero supports validation and impact-based prioritization. Testing reveals how vulnerabilities, misconfigurations, compromised credentials, and ineffective controls can combine to expose critical systems and customer data. This evidence helps financial organizations focus remediation on weaknesses that contribute to meaningful attacker outcomes.

For ASM initiatives, NodeZero complements asset discovery by testing whether exposed systems provide exploitable entry points and where attackers could go next. Across on-premises, cloud, and hybrid environments, this helps teams understand how individual weaknesses connect to broader exposure. Repeated testing allows them to reassess those paths as systems, applications, and access permissions change.

By incorporating NodeZero into these initiatives, financial organizations can connect discovery, validation, prioritization, remediation, and verification in a repeatable process. Teams gain evidence to guide corrective action and confirm whether changes reduced the exposure identified during testing.

Benefit

5



Provides Cost Savings Through Reduced MTTR

Reducing mean time to remediation requires teams to balance security priorities with day-to-day operational demands. Weaknesses may span interconnected systems, while legacy infrastructure and change-management requirements can make fixes difficult to implement without disrupting financial services. Limited staff and competing priorities add to the challenge.

Financial organizations cannot afford to spend scarce remediation resources on findings without understanding their significance. NodeZero helps teams focus on exploitable weaknesses and prioritize them based on demonstrated impact. Evidence showing a path to sensitive customer data or privileged access gives teams a concrete reason to act.

NodeZero also provides step-by-step remediation guidance, helping teams determine which changes can disrupt identified attack paths. This reduces the investigation and coordination needed to translate findings into corrective action. Fixes may involve patching software, changing configurations, strengthening credentials, or restricting access.

After teams implement changes, targeted retesting verifies whether the identified weaknesses remain exploitable. Teams can check their work promptly, address unsuccessful fixes, and document verified remediation without waiting for the next scheduled assessment.

Together, focused prioritization, actionable guidance, and verification can reduce the time and effort spent resolving security weaknesses. For financial organizations, that means more efficient use of remediation resources and shorter windows of exposure for critical systems and data.

Real-World Impact: A Financial Services Case Study

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

During its evaluation, the organization launched NodeZero against its infrastructure. Within approximately 16 hours, NodeZero identified an attack path that chained multiple weaknesses together to gain access to sensitive customer information. The test demonstrated how an attacker could move from an insecure configuration to data exposure.

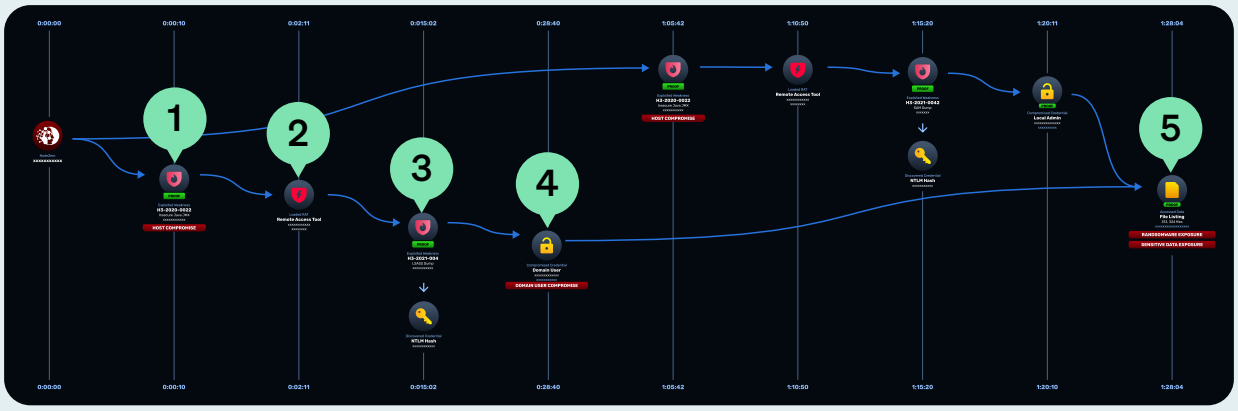


Figure 1: NodeZero Attack Path

Following the attack path from left to right in Figure 1, NodeZero:

1. Exploited an insecure Java Management Extensions configuration to compromise a host.
2. Installed a remote access tool on the compromised host.
3. Dumped the Local Security Authority Subsystem Service process memory and recovered an additional credential.
4. Used that credential to compromise a domain user account and gain access to more than 300,000 files.
5. Accessed customer credit card and Social Security number information stored in those files.

The organization remediated the identified weaknesses and adopted ongoing NodeZero testing to identify and prioritize additional exposures. The findings gave its teams a concrete basis for action: a demonstrated path from initial access to sensitive customer data.

Although Figure 1 shows a relatively straightforward attack path, NodeZero can also combine weaknesses into more complex paths, as illustrated in Figure 2, on the next page.

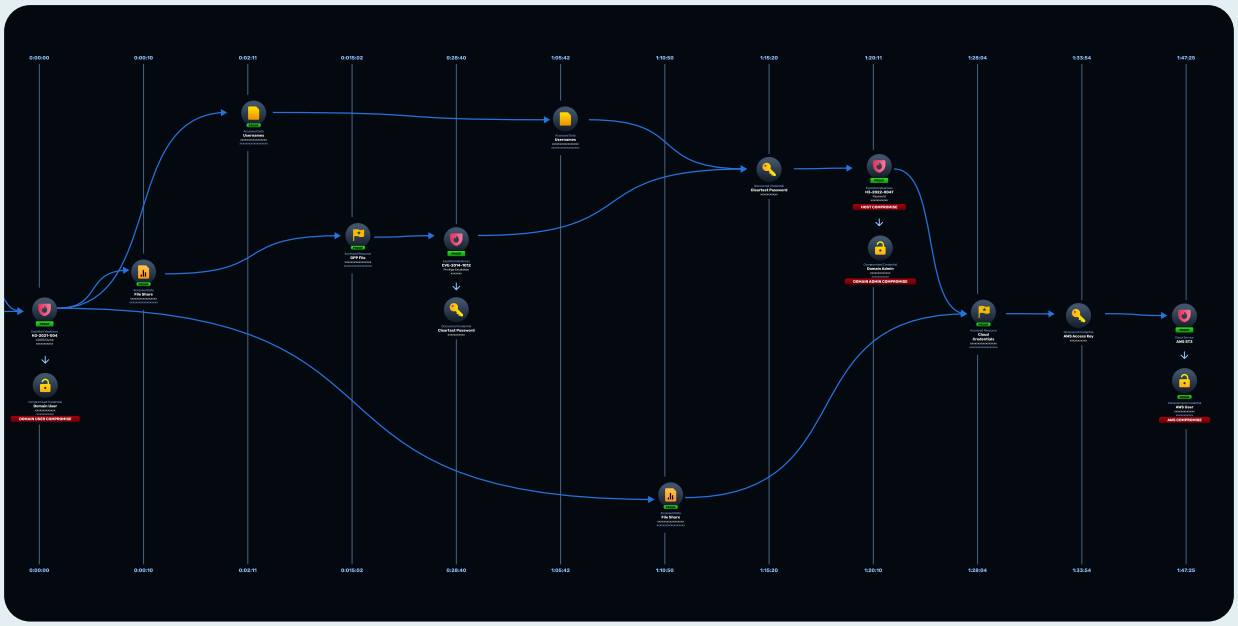


Figure 2: More Complex NodeZero Attack Path

NodeZero chains vulnerabilities, misconfigurations, and gaps in security controls to reveal how attackers could move through an environment. This helps teams understand the relationships between weaknesses that might otherwise appear to be isolated findings.

For each identified weakness, NodeZero provides remediation guidance. Addressing a weakness that supports multiple attack paths can disrupt several routes to compromise, helping teams focus their efforts where a change can have broader impact. Retesting then verifies whether the remediation closed the identified exposure.

Conclusion:

Securing the Future of Financial Services with NodeZero

Financial organizations must protect sensitive customer information and maintain essential services as their environments and threats evolve. Periodic assessments remain valuable, but the gaps between them can leave exploitable weaknesses undiscovered. Repeatable security testing helps teams identify those exposures and address them before attackers take advantage.

NodeZero and NodeZero Insights connect testing evidence with the decisions financial organizations need to make. Together, they provide executive visibility, identify weaknesses that could enable fraud and insider abuse, support more efficient compliance activities, strengthen exposure management, and help reduce remediation time and effort.

By incorporating autonomous testing into their security programs, financial organizations can make these benefits part of their ongoing operations. Leaders gain evidence to guide investments and communicate progress. Practitioners gain clear priorities, remediation guidance, and a way to verify that fixes worked. The result is a repeatable approach to reducing exposure and strengthening the protection of critical systems and customer data.

To learn how NodeZero can help secure your organization, schedule a demo today.

https://horizon3.ai/schedule-demo