HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Maximizing MSSP Revenue with NodeZero™: A Four-Pillar Strategy for Comprehensive Security Services

MSSP Revenue

Maximizing MSSP Revenue with NodeZero™: A Four-Pillar Strategy

Executive Summary

The managed security landscape is rapidly evolving, with clients seeking comprehensive, real-time cyber risk assessments to meet compliance, manage risks, and respond to threats. Integrating Horizon3.ai's NodeZero™ autonomous security platform into MSSP service portfolios enables providers to offer a holistic suite of services across four core areas: **Assess, Secure, Defend, and Advise**. These service lines allow MSSPs to meet diverse client needs, from continuous penetration testing and vulnerability remediation to managed detection and response, and strategic advisory with governance, risk, and compliance (GRC) insights.

NodeZero not only enhances operational efficiency for your clients but also empowers MSSPs to build high-margin, sustainable revenue streams models by streamlining client lifecycle management, improving scalability, and delivering executive-level insights that reinforce MSSPs as trusted security partners. The comprehensive business model covered in this white paper positions MSSPs to meet and exceed client expectations, creating sustained growth opportunities in an increasingly competitive market.

This paper is intended for managed security service providers (MSSPs), cybersecurity consultants, and leaders within security-focused organizations aiming to expand their service offerings and enhance revenue streams. It speaks to executives, business owners, and product managers responsible for strategic growth and service innovation, as well as technical and sales teams interested in understanding how autonomous security solutions like NodeZero™, NodeZero Tripwires™, and NodeZero Insights™ can streamline operations, strengthen client relationships, and create high-value, sustainable revenue streams opportunities.

The paper provides actionable insights and practical guidance, helping MSSPs meet the increasing demand for continuous security validation and positioning them as essential partners in their clients' cybersecurity initiatives.

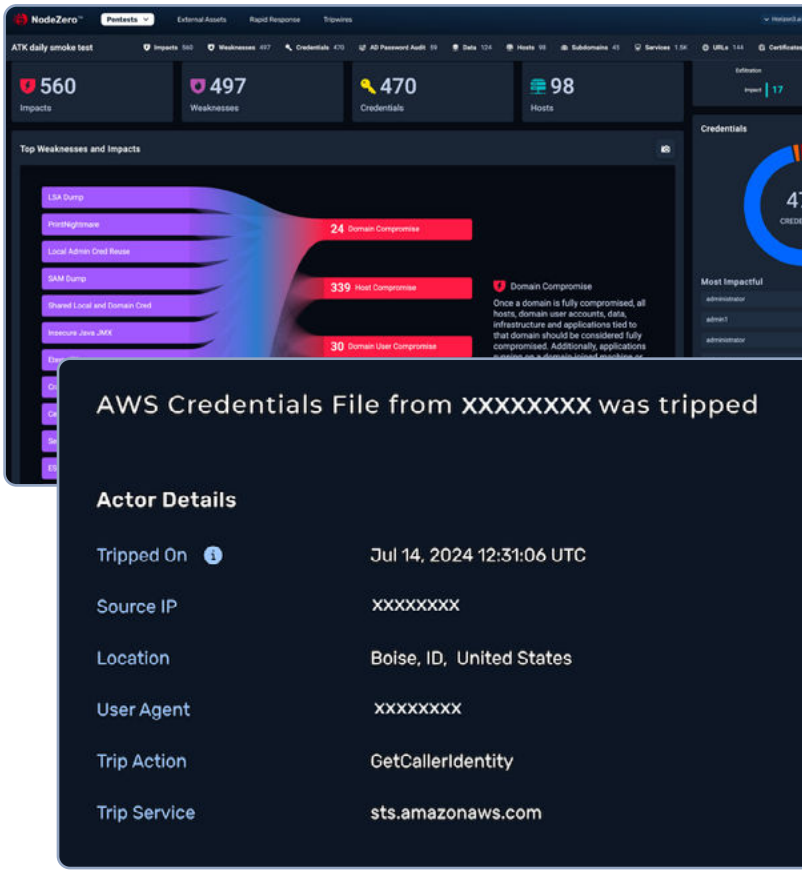
Table of Contents

Horizon3.ai's NodeZero™: Redefining Security for MSSPs

Horizon3.ai's NodeZero™ autonomous security platform redefines how MSSPs deliver comprehensive cybersecurity services. By integrating autonomous penetration testing, threat detection, governance, risk, and compliance insights, and third-party risk management, NodeZero enables organizations to proactively identify and remediate exploitable vulnerabilities.

NodeZero™ Autonomous Pentesting

NodeZero™ Autonomous Pentesting enables organizations to proactively assess their security posture by performing real-world attacks, just as an adversary would. Unlike traditional methods, NodeZero continuously identifies and validates exploitable vulnerabilities, providing clear proof of their impact. This approach empowers teams to prioritize fixes, streamline remediation efforts, and verify the effectiveness of their security measures. By emulating the tactics, techniques, and procedures of attackers, NodeZero shifts the focus from theoretical risks to actionable, validated threats, ensuring defenses are ready for real-world challenges.



NodeZero Tripwires™

NodeZero Tripwires™ introduces a strategic layer of deception and threat detection, designed to expose malicious activity early and decisively. By planting decoys such as fake credentials and files, and monitoring interaction with these decoys, Tripwires detect unauthorized activity, signaling potential breaches before they escalate. This proactive approach not only enhances situational awareness but also provides MSSPs with actionable intelligence to respond rapidly, ensuring threats are neutralized before causing significant harm.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

NodeZero Insights™

NodeZero Insights™ transforms raw security data into actionable governance, risk, and compliance (GRC) intelligence, empowering MSSPs and their clients to make informed decisions. By aggregating, analyzing, and prioritizing vulnerabilities based on exploitability and impact, Insights equips organizations with clear, real-world perspectives on their security posture. This enables MSSPs to align remediation strategies with client priorities, driving faster resolutions and strengthening long-term defense mechanisms.

For MSSPs, the NodeZero platform is a game-changer. Designed for scalability and easy integration, its multi-tenant architecture empowers MSSPs to efficiently manage multiple client environments, reducing operational overhead while scaling their offerings. This design allows MSSPs to deliver continuous security validation without the resource constraints of manual testing, making NodeZero indispensable for growing their client base and profitability.

NodeZero's autonomous nature enables MSSPs to provide high-margin, recurring services that span assessment, remediation, defense, and advisory functions. This positions MSSPs as proactive, strategic partners in their clients' cybersecurity efforts.

Next, let's dive deeper into the transformative Four-Pillar Strategy that drives these capabilities.

The Four-Pillar Strategy

NodeZero enables MSSPs to offer a comprehensive security solution with four high-value service categories:

Assess:	**Secure:**	**Defend:**	**Advise:**
Continuous Penetration Testing and Compliance Assessments	Vulnerability Remediation and SOC Optimization	Cross-Sell of Managed Detection and Response (MDR) and Overwatch Services	Strategic vCISO Advisory Services Enhanced with NodeZero Insights

Each service line can be developed into a sustainable revenue stream, allowing the MSSP to build long-term client relationships. Table 1 provides a quick overview of the Four-Pillar Strategy.

Table 1

	Sell pentests in the form of: • Compliance Assessments • CISA KEV Assessments • Vendor Risk Assessments • Security Control and SOC Assessments • Cyber Insurance Assessments • M&A Due Diligence Assessments • Purple Teaming Initiatives • Incident Response (IR) Assessments
	• Sell remediation services based on pentest findings • Sell SOC optimization services to improve detection and response times
	• Sell IR services integrated into NodeZero Tripwires • Sell new SOC tools to fill defensive blind spots • Sell MDR services to displace existing SOC or competitor offerings
	• Sell IR services integrated into NodeZero Tripwires

Assess – Penetration Testing and Compliance Assessments

- **Opportunity:** Clients require regular assessments to meet regulatory requirements, validate their security controls, and defend against real-world threats.
- **Revenue Potential:** By offering NodeZero-based assessments listed in Table 1, MSSPs can charge premium, recurring fees.
- **Service Packages:** MSSPs can offer clients quarterly, bi-annual, or continuous penetration testing packages aligned with compliance and operational requirements.

Key Monetizable Assessments

In the context of assessments, MSSPs can generate revenue by providing:

- **Compliance Assessments:** For clients needing to meet regulations *(e.g., PCI-DSS, SOC2, NIS2, GDPR, HIPAA, CMMC)*, NodeZero's pentests provide the required compliance reports and proof of security assessment. MSSPs can offer these compliance-oriented assessments as a recurring service, driving long-term revenue and customer retention.
- **CISA KEV Assessments:** Given the high risk associated with CISA's Known Exploited Vulnerabilities (KEVs), MSSPs can offer dedicated assessments to confirm clients are not vulnerable to these emerging threats, making this a high-impact, recurring service offering.
- **Vendor Risk Assessments:** MSSPs can assist clients in meeting third-party risk requirements by performing regular pentests of their supplier environments. This service helps clients maintain trust and security assurance with their own customers and partners.
- **Security Control and SOC Assessments:** NodeZero can validate the efficacy and effectiveness of the SOC in the context of deployed security controls like SIEMs, EDR, and broader security policies. MSSPs can monetize these services by aligning them with board or CISO priorities, providing actionable insights and reporting to demonstrate security control effectiveness.
- **Cyber Insurance Assessments:** MSSPs can help clients meet the penetration testing and risk assessment requirements mandated by cyber insurance providers, allowing clients to reduce premiums and meet policy requirements.
- **M&A Due Diligence Assessments:** For clients engaged in mergers or acquisitions, MSSPs can perform comprehensive pentests to identify security risks and vulnerabilities, crucial for reducing risk and protecting the valuation.

- **Purple Teaming Initiatives:** As more CISOs focus on purple teaming to improve collaboration between offensive and defensive teams, MSSPs can monetize purple team exercises using NodeZero to drive security enhancements and identify potential gaps in both detection and response.
- **Incident Response (IR) Assessments:** MSSPs can test their clients' IR processes to validate their effectiveness during an attack. Using NodeZero, they can run simulations that help identify weaknesses, refine processes, and improve response readiness.

Secure – Remediation Services and SOC Optimization Services

- **Opportunity:** MSSPs can provide remediation consulting to clients based on NodeZero's remediation insights and guidance. This service line can include vulnerability remediation and SOC optimization to tune detection and response mechanisms.
- **Revenue Potential:** MSSPs can charge for each remediation engagement, with additional consulting fees for SOC optimization based on pentest findings.
- **Service Packages:** MSSPs can offer ad-hoc remediation services, fixed-scope remediation retainers, or SOC consulting packages.

After completing assessments, MSSPs can generate revenue by providing:

- **Remediation Services:** MSSPs can directly fix critical vulnerabilities identified in NodeZero assessments. This includes consulting on or performing patching, reconfiguring security policies, and implementing controls to eliminate or reduce exploitable weaknesses.
- **SOC Optimization:** NodeZero can help MSSPs identify areas for optimizing existing Security Operations Centers (SOCs). MSSPs can offer specialized consulting to improve SOC performance, including optimizing alert settings, enhancing detection accuracy, and reducing false positives, driving operational efficiencies.

By bundling NodeZero-based assessments with remediation and SOC consulting, MSSPs create value-driven packages that deepen client relationships and drive incremental revenue.

Defend – MDR, SOC-as-a-Service, and Overwatch Services

- **Opportunity:** NodeZero's pentesting results reveal security gaps, presenting an opportunity to cross-sell the MSSP's own MDR or SOC-as-a-Service offerings.

- **Revenue Potential:** MSSPs can charge subscription fees for continuous MDR/SOC services and add specialized services like Overwatch Services for a premium.
- **Service Packages:** MSSPs can offer comprehensive MDR packages, SOC-as-a-Service plans, and dedicated Overwatch Services.

NodeZero's pentesting results open cross-sell opportunities for MSSPs to strengthen clients' defense posture:

- **Managed Detection and Response (MDR):** MSSPs can leverage NodeZero findings to promote their own MDR or SOC-as-a-Service offerings, positioning them as a natural next step for clients needing continuous detection and response after identifying vulnerabilities.
- **Overwatch Services Using NodeZero Tripwires:** MSSPs can add value by providing an Overwatch Service that rapidly responds to NodeZero Tripwires alerts. By monitoring and responding to these alerts in real-time, MSSPs create an enhanced layer of security for clients that require quick action on detected threats.
- **Security Tool Resale:** Based on NodeZero's assessments, MSSPs can identify gaps in the client's security architecture and recommend solutions (e.g., firewalls, IDS/IPS systems, endpoint security solutions). MSSPs can partner with vendors to resell these tools, generating additional revenue streams while enhancing the client's security capabilities

These offerings provide MSSPs with a steady flow of recurring revenue from managed services and security product resale, creating a comprehensive, multi-layered approach to client defense.

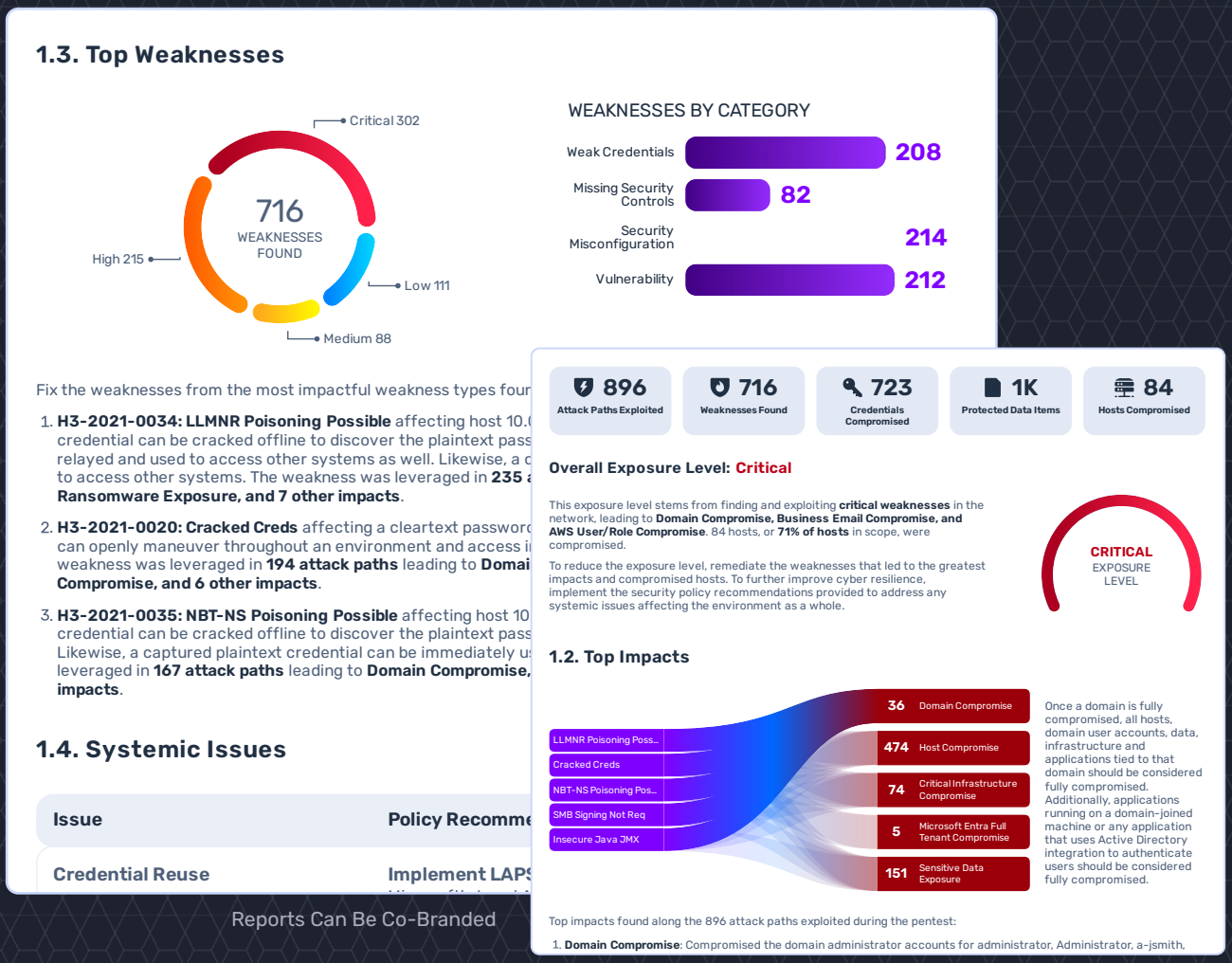
Advise – Strategic vCISO Services with NodeZero Insights

- **Opportunity:** MSSPs can offer executive-level advisory services based on NodeZero Insights and the narratives it provides. This includes regular security posture reports for boards and tailored vCISO services.
- **Revenue Potential:** Advisory services are high-margin offerings, particularly valuable to C-suite and boards requiring strategic guidance on security.
- **Service Packages:** MSSPs can offer monthly, quarterly, or annual vCISO retainer services, augmented with NodeZero Insights for ongoing strategic advisories.

With NodeZero Insights, MSSPs can offer higher-margin advisory services that deliver long-term value and strategic insights:

- **vCISO Services:** MSSPs can position themselves as virtual CISOs, delivering periodic advisory sessions based on pentest results over time. NodeZero's continuous assessments allow MSSPs to provide data-backed recommendations, aligning security actions with the client's business goals and security strategy.
- **NodeZero Insights and Narratives:** With NodeZero Insights, MSSPs can deliver periodic reports and Board presentations using NodeZero Insights. By leveraging pentest data, user annotations, and analysis over time, MSSPs can offer insights and reports tailored to Boards or C-suite needs, demonstrating security progress and areas of improvement.

By providing these advisory services, MSSPs create trusted relationships with executive stakeholders, allowing them to position as strategic partners and open new revenue channels through high-value consulting engagements.



Reports Can Be Co-Branded

Competitive Advantages of NodeZero for MSSPs

NodeZero provides MSSPs with a range of competitive advantages that streamline operations, enhance scalability, and drive exceptional client value:

Scalability to Serve Large Enterprises:

NodeZero is designed to scale effortlessly across vast and complex enterprise environments, making it ideal for MSSPs targeting large clients with distributed networks and diverse asset types. The platform's robust automation can handle high-volume, high-velocity internal, external, cloud, and Kubernetes penetration testing requirements, enabling MSSPs to efficiently serve large enterprises while ensuring consistent coverage and thoroughness. This scalability differentiates NodeZero from traditional penetration testing tools that struggle with large-scale deployments, allowing MSSPs to take on bigger clients and high-margin contracts confidently.

Multi-Tenant SaaS Architecture for Simplified Client Lifecycle Management:

NodeZero's multi-tenant architecture is purpose-built for MSSPs, providing streamlined management of multiple clients from a single interface. This multi-tenant design makes client lifecycle management more efficient, ultimately lowering the cost per client served and enabling MSSPs to expand their client base without overburdening internal teams. This architecture reduces operational overhead and simplifies crucial client lifecycle activities, such as:

- **Enrollment and Onboarding:** MSSPs can onboard new clients quickly, benefiting from NodeZero's structured setup and configuration options that minimize the time and effort required for client intake.
- **Utilization Management:** NodeZero's dashboard provides insights into each client's pentest status and activity level, enabling MSSPs to optimize engagement by easily identifying underutilized licenses and maximizing ROI for both the MSSP and the client.
- **License and Entitlement Management:** MSSPs can efficiently allocate and track licenses across clients, ensuring accurate entitlement and enabling seamless scalability without administrative complexity.
- **Client Offboarding:** When a client relationship concludes, NodeZero's multi-tenant model enables MSSPs to swiftly handle data and access de-provisioning while maintaining compliance, reducing potential security risks and preserving MSSP resources.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Continuous and Autonomous Pentesting:

Unlike traditional penetration testing services that provide only point-in-time insights, NodeZero's autonomous platform allows MSSPs to deliver continuous penetration testing as a service. This approach gives clients near-real-time visibility into their security posture and enables MSSPs to offer a premium, recurring service that aligns with clients' ongoing security needs.

Seamless Integration with MSSP Offerings:

NodeZero's insights can directly inform and enhance other MSSP offerings, such as Managed Detection and Response (MDR) and vCISO advisory services. NodeZero Tripwires' alerts integrate seamlessly into security operations, allowing MSSPs to cross-sell monitoring and rapid-response services. The result is a cohesive and comprehensive portfolio that addresses client needs across assessment, remediation, defense, and advisory.

Enhanced GRC and Compliance Reporting:

With NodeZero Insights, MSSPs can deliver executive-ready reports that satisfy governance, risk, and compliance requirements, demonstrate security control efficacy, and provide strategic insights for C-level stakeholders. This reporting capability differentiates MSSPs by enabling them to translate technical findings into actionable business intelligence, adding significant value for clients.

White-Labeling and Co-Branding Capabilities for Enhanced Client Engagement:

NodeZero allows MSSPs to white-label or co-brand reports, making it easy to present penetration testing results and insights as an integrated part of their own service offerings. This flexibility enhances the MSSP's brand visibility and credibility, positioning them as the primary provider of security expertise to their clients. With NodeZero's custom-branded reports, MSSPs can deliver a consistent, branded experience that reinforces their value and builds stronger client loyalty. This capability also supports co-branded engagements, where MSSPs can leverage Horizon3.ai's reputation alongside their own to boost client confidence and establish authority, particularly in highly regulated or large enterprise environments.

By incorporating NodeZero into their offerings, MSSPs gain the ability to serve complex, large-scale enterprises efficiently while benefiting from streamlined client management, consistent service delivery, and high margins. This combination of scalability, multi-tenant architecture, and comprehensive reporting creates a powerful, competitive advantage in the managed security market.

Example Implementation Plan

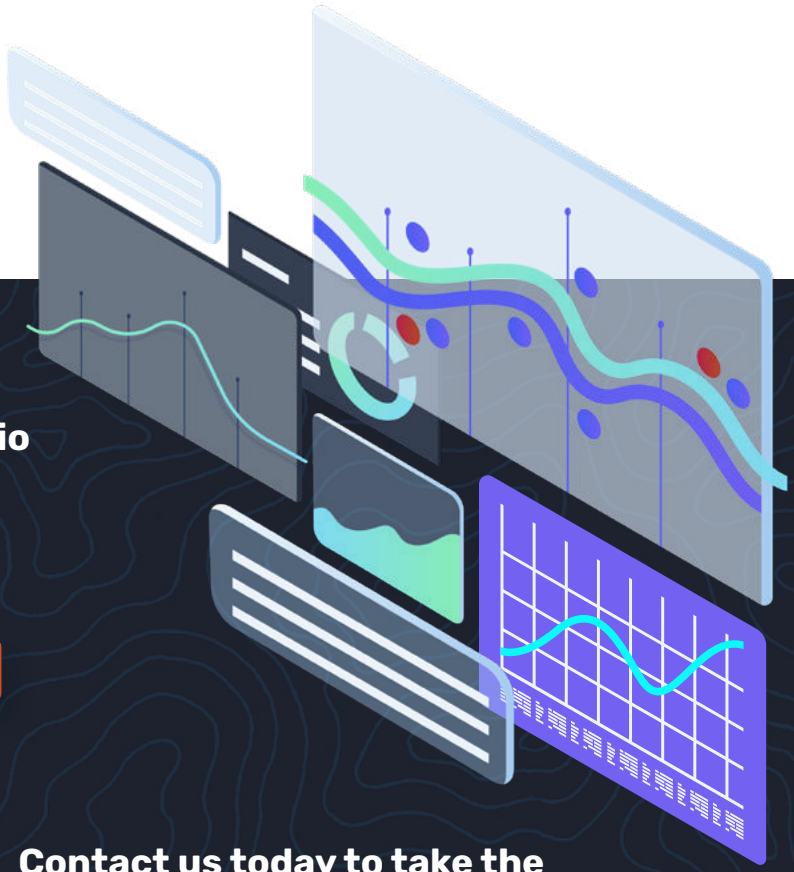
To maximize the potential of NodeZero, MSSPs should follow this structured implementation plan:

1. **Pilot Program:** Start with a select group of clients and offer a NodeZero-based assessment. Gather feedback, refine the service, and build internal expertise.
2. **Service Development:** Define each service line clearly, including pricing, deliverables, and timelines. Bundle assessment, remediation, MDR, and advisory offerings into cohesive packages.
3. **Sales and Marketing Alignment:** Develop go-to-market messaging focusing on NodeZero's unique advantages. Train the sales team to educate clients on the benefits of autonomous pentesting and continuous security validation.
4. **Client Engagement Strategy:** Begin with pentesting as an entry point and then expand the client relationship by cross-selling remediation, MDR, and advisory services based on assessment results.

Offering	Description	Features
Essential Security Validation	Basic package for compliance assessments	• Quarterly Penetration Tests
Advanced Continuous Pentesting & Defense	Continuous pentesting, advanced threat response, and advisory services	• Monthly Pentests • Rapid Response CISA KEV Testing • NodeZero Tripwire Overwatch • ~40 hours Remediation Consulting per Quarter • vCISO Quarterly Advisory

Conclusion

NodeZero enables MSSPs to create a high-margin business model by addressing client needs across assessment, remediation, defense, and strategic advisory. By embedding NodeZero's autonomous penetration testing capabilities into their service offerings, MSSPs can offer high-impact assessments, leverage actionable remediation, strengthen defense capabilities, and deliver executive-level insights that deepen client relationships and increase sustainable revenue streams potential. This holistic approach allows MSSPs to maximize client lifetime value, positioning themselves as essential partners in the client's security journey.



- **Explore how NodeZero can transform your service portfolio and position your organization as a leader in the competitive managed security market.**

https://www.horizon3.ai/trial

- **Contact us today to take the next step in revolutionizing your business.**

https://www.horizon3.ai/demo