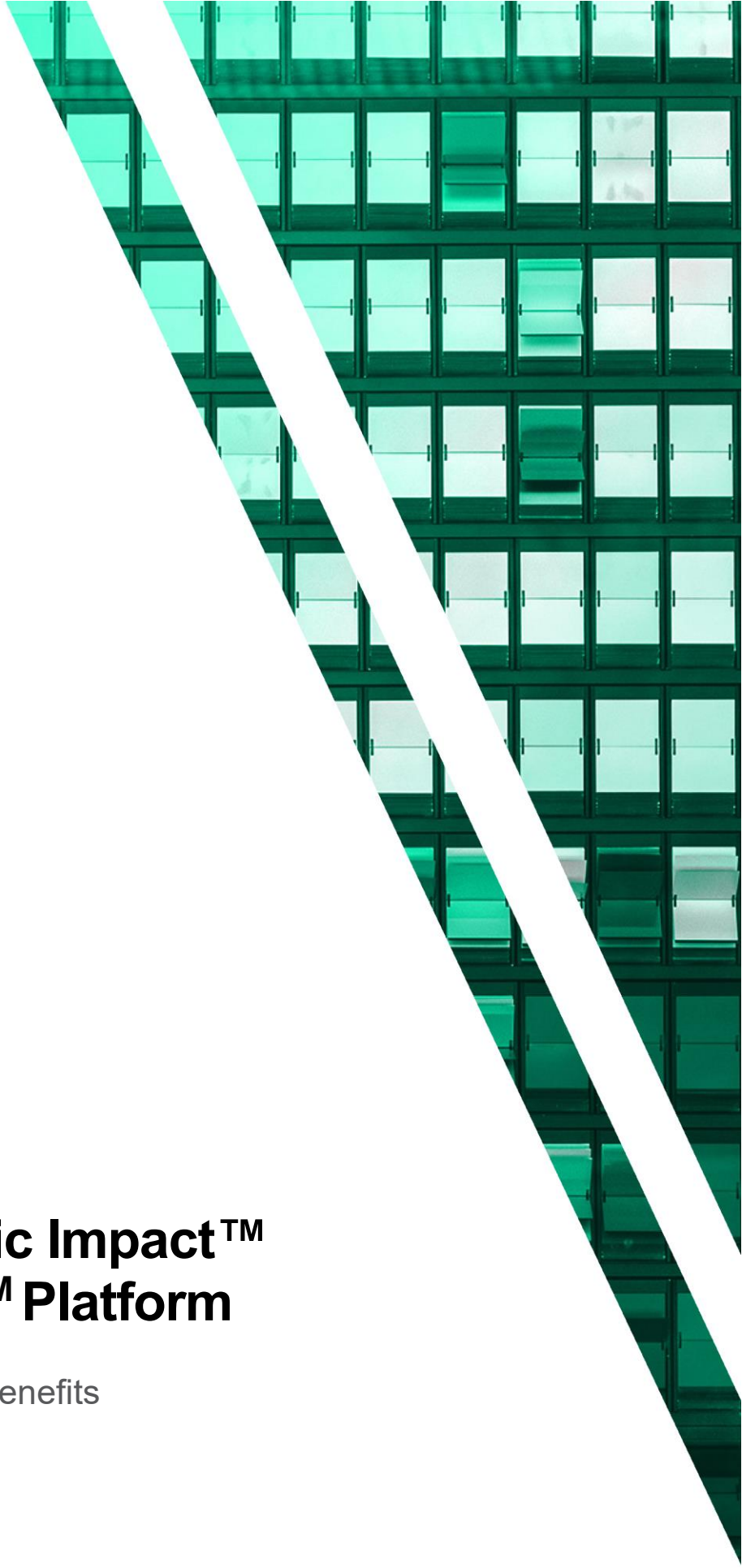
FORRESTER®



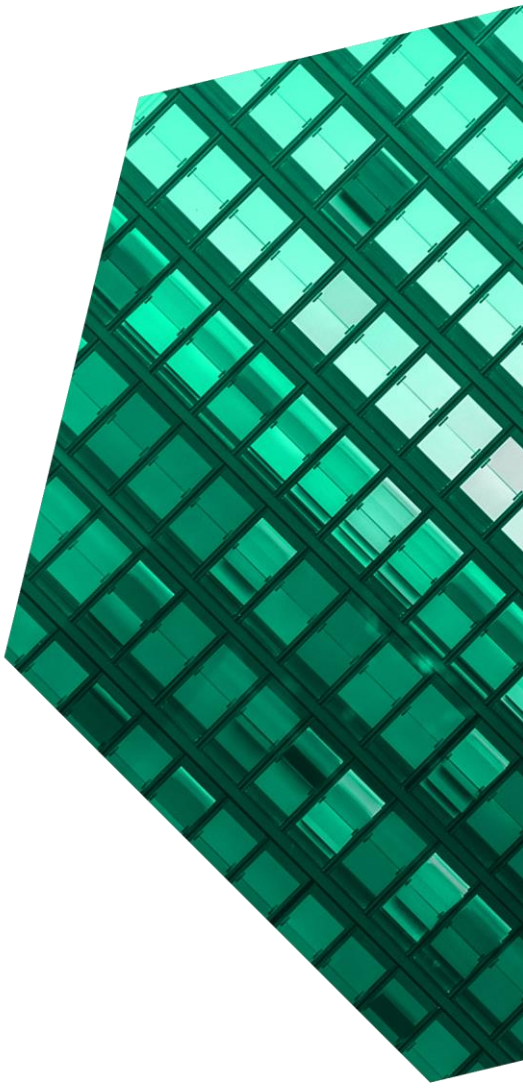
The Total Economic Impact™ Of The NodeZero™ Platform

Cost Savings And Business Benefits Enabled By NodeZero

OCTOBER 2023

Table Of Contents

Consulting Team: Luca Son
Marianne Friis



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

The time and cost involved with manual penetration testing renders organizations unable to test their entire networks, frequently retest, efficiently fix risks, or verify the efficacy of their fixes. For a comprehensive security strategy, organizations must consider a solution that continuously tests attack surfaces that are exploitable, identifies vulnerabilities and attack paths, delivers contextual remediation guidance, and expedites verification that fixes are effective.

The Horizon3.ai NodeZero™ platform is a SaaS platform that provides continuous autonomous penetration testing. NodeZero helps cybersecurity teams proactively find and fix internal and external attack vectors before they can be exploited.

Horizon3.ai commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying NodeZero.[1] This study aims to provide readers with a framework to evaluate the potential financial impact of NodeZero on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives across four organizations with experience using NodeZero. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization, a company based in North America with 2,000 employees and $500 million in annual revenue.

Total time savings across all security operations FTEs with NodeZero

30%

KEY STATISTICS

Return on investment (ROI)
63%

Three-year total benefits
$809K

Prior to using NodeZero, these interviewees noted how their organizations relied on third-party penetration tests and vulnerability scanners to scan for, identify, and provide remediation guidance for vulnerabilities in their attack surface. However, legacy testing and tools were insufficient and led to poor insights. Organizations experienced expensive, inconsistent, and ineffective third-party penetration tests. They had limited insight into vulnerabilities that posed the most significant risk to their organization and spent weeks sorting through lists of false positives, causing security operations and posture to suffer.

After investing in NodeZero, the interviewees improved their security operations productivity and posture, realized cost savings from avoiding third-party penetration tests, and consolidated security technology costs.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Improved security operations productivity by 30%.** NodeZero enables security teams to automate their scanning and testing processes. Teams need less time to filter through false positives and can focus more effort in addressing threats to their sensitive data. NodeZero expedites the research process, allows security teams to understand attack paths and provide guidance to remediation teams. Frequent testing facilitates swift identification of vulnerabilities, preventing incidents and breaches and saving incident response and recovery time. Over three years, improved security operations productivity is worth $348,000.
- **Avoided $255,000 in third-party penetration test costs.** Hiring external security experts can be costly. NodeZero can partially or fully replace third-party penetration tests, allowing organizations to save and reinvest those fees into other security initiatives. NodeZero can also scale the number of tests being run at no marginal cost. This enables continuous real-time insights into the security team's posture and contributes to faster insight and remediation. Over three years, avoided third-party penetration test costs are worth $255,000.
- **Reduced vulnerability scanner cost by $206,000.** NodeZero provides insights that finetune existing security tools and infrastructure. Legacy tools like vulnerability scanners can be ineffective at prioritizing critical vulnerabilities, creating extra work for security teams to understand, triage, and remediate vulnerabilities. Consolidating technology and insights derived with NodeZero empowers organizations to partially replace their legacy vulnerability scanners. Reduced vulnerability scanner costs are worth $206,000 over three years.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Continuous verification of security posture to confirm remediation of weaknesses.**
- **Time savings for remediation guidance.**
- **Identify sensitive data exposure and reduce risk of breaches.**
- **Accurately convey security posture to customers with streamlined reporting.**
- **Accelerate vendor risk assessment.**
- **Streamline mergers and acquisitions with improved security testing and remediation.**
- **Strong vendor partnership and support.**
- **Improved security employee experience (EX).**

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Horizon3.ai's NodeZero subscription fee.** Horizon3.ai charges a subscription fee based on the number of internet protocols (IP) an organization chooses to run its penetration tests and other security operations against. Volume discounts are applied depending on the number of IPs. Implementation and setup time are minimal, and new tests can be set up in minutes. The three-year, total present value of subscription cost is $497,000.

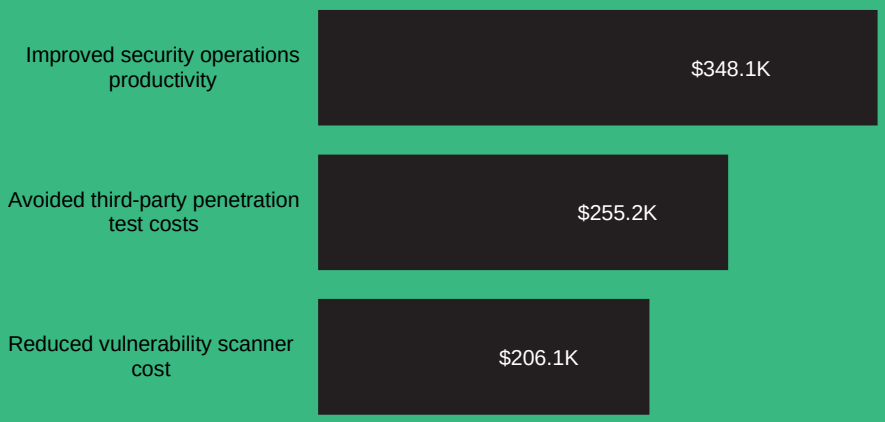
The representative interviews and financial analysis found that a composite organization experiences benefits of $809,000 over three years versus costs of $497,000, adding up to a net present value (NPV) of $312,000 and an ROI of 63%.

ROI
63%

BENEFITS PV
$809K

NPV
$312K

Benefits (Three-Year)



PRESENT VALUE (PV)

Present value (PV) is the current value of a future sum of money or stream of cash flows given a specified rate of return. Future cash flows are discounted at the discount rate, and the higher the discount rate, the lower the present value of the future cash flows.

NET PRESENT VALUE (NPV)

Net present value (NPV) is the difference between the present value of cash inflows and the present value of cash outflows over a period of time. A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

"[An automated pen test solution is] the number one thing I recommend to peers. If you want a valid and modern cybersecurity posture, you must be doing automated pen testing."

— CIO, construction

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in NodeZero.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that NodeZero can have on an organization.

DUE DILIGENCE

Interviewed Horizon3.ai stakeholders and Forrester analysts to gather data relative to NodeZero.

INTERVIEWS

Interviewed six representatives at four organizations using NodeZero to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Horizon3.ai NodeZero Customer Journey

Drivers leading to the NodeZero investment

Interviews

Role	Industry	Region	Revenue
Director of information security	Entertainment	US	$1.5 billion
Director of IT security	Manufacturing	US	$1 billion
• Director of IT • Senior security engineer	Healthcare	US	$500 million
• CIO • Information security engineer	Construction	US	$500 million

KEY CHALLENGES

Prior to their investment in NodeZero, interviewees noted their organizations did not have an automated penetration testing solution. They relied on third-party consultancies to conduct annual penetration tests and relied on vulnerability scanners for their vulnerability management and remediation programs. The interviewees noted how their organizations struggled with common challenges, including:

- **Expensive, inconsistent, and ineffective third-party penetration tests.** Third-party penetration tests were costly and failed to meet the security standards of the interviewees' organizations. The quality of reports ranged amongst providers, as they were often lengthy. Interviewees could not resolve all findings, and were unable to verify the impact of their fixes for the items they did address. The CIO of a construction organization said: "The individual cost to run a pen test was significant. … It wasn't something that we had the luxury of doing whenever we could remediate. The cost of the old model just didn't scale. We couldn't afford to do it three or four times a year."
- **Lack of exploitable vulnerability prioritization.** Third-party penetration tests either failed to accurately categorize exploitable vulnerabilities or listed too many vulnerabilities, overwhelming security and IT teams, leaving them unable to prioritize their efforts to resolve the most critical weaknesses. This created a manual, time-consuming remediation process with little visibility into the efficacy of their efforts. Scarce and expensive security resources compounded the issue and drove the need for a better solution.
    - The CIO of a construction organization stated: "Even with the [third-party] pen test, they would run a myriad of tools, and many of those tools would just give us a ton of false positives. Even though it costs

> **"The [third-party pen test] methodology and reporting was always different. The quality of reporting ranged widely. I got terrible reports, and I got some excellent reports. But the good reports were few and far between."**
>
> *Director of IT, healthcare*

a lot, the value proposition wasn't great. We'd get a 150-page report and have to spend days trying to find out what's real or not. Then, if we didn't use the same provider year after year, they would usually have different toolsets that would tell us different things."

"When we had [third-party penetration testers], it would take four to six weeks to figure out exactly what we would work on in what order, and we would never be able to do everything. We would target 33% to half of the report, and what would happen is maybe two-thirds of the things we thought we addressed were fixed, but a third of them would reappear on the report the next year. Meaning that even though we thought we resolved it, we really didn't."

CIO, construction

- **Siloed or underperforming security tools led to poor insights.** Interviewees stated that before using NodeZero, they struggled to understand the efficacy of their other security tools and where there was room for finetuning. The director of IT security at a manufacturing organization shared: "[Our legacy vulnerability scanner] will basically just look at the CVEs [common vulnerabilities and exposures]. When it gives you back 4,000 criticals, where do you start? Then, when you start digging, it's not necessarily exploitable stuff."

"[Our security operations and workflows] are a lot more repeatable with NodeZero and we don't have a single distracting project. It now becomes operationally focused. We get the scan, we fix things, we get another scan, we fix things every time. We're getting better."

CIO, construction

WHY HORIZON3.AI NODEZERO

The interviewees' organizations searched for a solution that could:

- Improve security posture by automating penetration testing and broadening penetration testing coverage.
- Continuously test and verify environments and scale penetration test cadence from once a year to dozens of times yearly.
- Prioritize exploitable vulnerabilities to remediate the most critical issues faster.
- Improve the efficiency of security operations.
- Finetune and improve the effectiveness of existing security tools and processes.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four organizations and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a company based in North America with 2,000 employees, a security team of four people, and $500 million in annual revenue.

Deployment characteristics. The security team in the composite organization conducts weekly tests of its internal environment and monthly tests of its external environment across a total of 5,000 IPs. The four security FTEs review and act on the results after each test, identifying and prioritizing exploitable vulnerabilities, verifying past fixes, and routing tickets to teams responsible for remediation.

Key Assumptions

- **Annual revenue of $500 million**
- **Total of 5,000 IPs**
- **A security team of four FTEs**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Improved security operations productivity	$139,968	$139,968	$139,968	$419,904	$348,080
Btr	Avoided third-party penetration test costs	$102,600	$102,600	$102,600	$307,800	$255,151
Ctr	Reduced vulnerability scanner cost	$82,875	$82,875	$82,875	$248,625	$206,098
	Total benefits (risk-adjusted)	$325,443	$325,443	$325,443	$976,329	$809,329

SECURITY OPERATIONS PRODUCTIVITY

Evidence and data. Horizon3.ai's NodeZero allowed interviewee organizations to automate their scanning and testing process, reducing the need for manual, time-consuming tasks. As NodeZero identifies attack paths and prioritizes exploitable vulnerabilities, organizations spent less time filtering through false positives and could focus more effort in addressing the vulnerabilities that posed the largest threat to their sensitive data. NodeZero's remediation guidance expedited the research process and allowed security teams to provide quicker guidance to remediation teams. More frequent testing meant security teams could identify vulnerabilities more quickly, preventing incidents and breaches and saving incident response and recovery time.

- Interviewees used NodeZero to automate red teaming activities, allowing their security teams to reallocate time to other strategic tasks. The senior security engineer in a healthcare organization noted: "It's hard to curate exploits and stay on top of emerging threats. It's hard to measure, but [NodeZero] easily avoids having to hire one or two people that would do specifically red teaming or purple teaming."
    - The director of IT security in a manufacturing organization stated: "[NodeZero] probably saves us two to three FTEs a year, just in terms of efficiency."
- NodeZero enabled interviewees to automate and increase the complexity of their tests without demanding more time from their security practitioners. The senior security engineer in a healthcare organization shared: "We could automate many of the functions that we would like to spend more time on but didn't have time to. NodeZero allowed us to do more complex scans and things without learning other vulnerability programs."
- Interviewees used NodeZero to improve time to value. The information security engineer of a

"By having NodeZero in place and constantly running, you can constantly take care of updates and fixes."

Director of IT security, manufacturing

construction organization said: “The key thing about NodeZero is that the pen test is fast. It gets it done within half a day at most. Another key factor is that it provides fix action reports that you can take immediately from the completed pen test. The moment it’s done, you already have solutions you can implement. If you never had NodeZero, you would probably spend 40 hours a week trying to figure out solutions to specific vulnerabilities.”

- Interviewees reported saving time understanding remediation guidance and implementing fixes. The information security engineer of a construction organization stated: “Horizon3.ai has already solved the first portion of figuring out a remediation tactic. Fifty percent of the work is already done for us — I already know exactly what I need to implement, where I need to go, and all the settings I need to change. For us, where the bulk of the remediation takes place is making sure that we take the adequate steps to implement the solution NodeZero provided us, but doing it in a controlled state where we’re not causing any downtime with our production server.”

Modeling and assumptions. In modeling the composite organization, Forrester assumes:

- There are four security operation FTEs who work across various responsibilities (e.g., vulnerability management, attack surface management, and penetration testing).
- The average fully burdened rate for a security operation FTE is $162,000, which includes a 1.35 multiplier on the fully burdened rate.
- The security operations FTE recaptures 80% of their time savings and dedicates that to other productive activities.

Risks. The expected financial impact is subject to risks and variation based on several factors, including:

- Number of security operations FTEs.
- Level of expertise and range of responsibilities.
- Varying labor rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $348,000.

Improved Security Operations Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of security operations FTEs focused on vulnerability prioritization, understanding, and triaging	Composite	4	4	4
A2	Time savings with Horizon3 NodeZero	Interviews	30%	30%	30%
A3	Fully burdened rate per security operations FTE	Composite	$162,000	$162,000	$162,000
A4	Productivity recapture	Composite	80%	80%	80%
At	Improved security operations productivity	A1*A2*A3*A4	$155,520	$155,520	$155,520
	Risk adjustment	↓10%			
Atr	Improved security operations productivity (risk-adjusted)		$139,968	$139,968	$139,968
	Three-year total: $419,904			**Three-year present value: $348,080**	

VOICE OF THE CUSTOMER - BENEFITS

Interviewees shared:

- "[Horizon3 NodeZero] is crystal clear and accurate. As security practitioners, we all have very limited resources. Being able to employ those as effectively as possible will allow us to secure our environment or keep it secure most rapidly, and Horizon3 does that near flawlessly, better than any solution that I am aware of."
- "Some of the things we've caught super early on, before it was even problematic, were all put in place because of alerts we've developed around Horizon3.ai. We're able to find problems before they become a problem. … It absolutely has helped us set up a lot of our alerting and refine our alerting for what to look for. It absolutely has contributed to our overall security posture."

  – Director of IT security, manufacturing

- "Anything critical – the team will concentrate on those, get that fixed, and then go back and click verify, which is amazing. To me, that alone, on top of everything that [Horizon3.ai] offers, is priceless. Because it's super-fast, and it's pinpointing exactly what I want to look for. Instead of running a five-day test, I can run [NodeZero] probably within the hour and I can get an answer."
- "You can do a nice asset discovery with the tool. It saves tons of time because if I didn't have this tool, I would need to go out and hire someone every time to do a pen test and verify everything, and that would take a lot of time."

  – Director of information security, entertainment

- It gave us a lot of insight into [our environment] that we probably never knew about before. We were able to gain insights, find devices, and implement policies much faster. It reduced the amount of time that we would have to spend on analyzing and remediation so that we can work on newer projects and start making our leaps to technology better."

  – Information security engineer, construction

- "The nice thing that Horizon3.ai does is that you can run ad hoc as many scans as you want. I can run a scan every day if I want to. That's a beautiful thing about it."

  – Director of information security, entertainment

- "Without NodeZero, we would have had these ticking time bombs in our environment. NodeZero has provided a layer of decision-making and justifications for our decisions that we wouldn't have been able to do before…. But the reality is our peers in the construction industry consistently have cyber events that we do not have, and NodeZero is the number one thing that has improved our cybersecurity posture."

  – CIO, construction

- "We got eyes on trends regarding patching vulnerabilities, and we were able to see those trends downward. So, overall, I would say, that our risk posture has improved quite a bit with the combination of the vulnerability management program and Horizon3.ai."

  – Senior security engineer, healthcare

- "The new scheduling functionalities have started to free up some of our time, so we don't have to worry about kicking off new pen tests; we can have them automatically start as needed on whatever schedules we want."

  – Director of IT, healthcare

AVOIDED THIRD-PARTY PENETRATION TEST COSTS

Evidence and data. Third-party penetration tests can be costly, as they involve hiring external security experts. Interviewees shared that they either partially or fully replaced third-party penetration tests with NodeZero, allowing them to save and reinvest in further security initiatives. All interviewees also scaled the number of tests they can run at no marginal cost. This enabled continuous real-time insights into their security posture and contributed to faster insight and remediation time to value.

- The director of IT in a healthcare organization shared: "We're required to have a third party do a pen test. Those pen tests would be between $60,000 and $120,000 a year, depending on who you purchased them from. These were network pen tests and did the same thing NodeZero is doing. Now, [Horizon3.ai] does our third-party pen testing. We were able to benefit quite a bit out of that."
- The information security engineer of a construction organization shared: "We are no longer doing third-party pen tests. We are in a less regulated industry from a government compliance standpoint, but we work for customers who might be in highly regulated industries. We do get the typical vendor assessments and we use NodeZero for most questions related to vulnerabilities, patching, and verification because we have so much data that we can easily prove that we have a process in place. We have a set of reports that show our processes are in control."

Modeling and assumptions. In modeling the composite organization, Forrester assumes:

- It spends $120,000 annually with a third-party service to conduct one penetration test prior to using NodeZero.
- It replaces third-party penetration testing entirely with NodeZero and attributes 5% of this benefit to internal labor and process improvements.

Risks. The expected financial impact is subject to risks and variation based on several factors, including:

- Cost and frequency of third-party penetration tests.
- Some organizations may elect to continue employing third-party penetration tests on an annual or biennial cadence.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $255,000.

Avoided third-party penetration test costs

95%

Avoided Third-Party Penetration Test Costs					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Cost of third-party penetration tests	Interviews	$120,000	$120,000	$120,000
B2	Avoided third-party penetration test attribution to NodeZero	Interviews	95%	95%	95%
Bt	Avoided third-party penetration test costs	B1*B2	$114,000	$114,000	$114,000
	Risk adjustment	↓10%			
Btr	Avoided third-party penetration test costs (risk-adjusted)		$102,600	$102,600	$102,600
	Three-year total: $307,800			**Three-year present value: $255,151**	

REDUCED VULNERABILITY SCANNER COST

Evidence and data. NodeZero provided insights that helped interviewees finetune their existing security tooling and infrastructure. They reported that tools in their prior environment (e.g., their vulnerability scanners) were ineffective at prioritizing critical vulnerabilities and created extra work for security teams to understand, triage, and remediate vulnerabilities. They either fully or partially replaced their legacy vulnerability scanners with NodeZero. Interviewees also actioned insights derived from NodeZero to assess the coverage and gaps from their other security tools and gave them evidence to further finetune tooling efficacy and negotiate rates.

- The director of information security in an entertainment organization stated: "[Our vulnerability scanner] was $120,000 a year. … [With Horizon3,] I would say it's like a 90% replacement, which is good enough to get rid of the tool and exercise those savings."
- A construction organization used NodeZero to identify infrastructure and edge devices that they could decommission. The CIO from the construction company noted, "From a hardware perspective, we've probably saved a very small amount, maybe 5% to 10%, because we've been able to turn so many things off that we weren't using, but didn't have justification for turning them off [previously]."

Modeling and assumptions. In modeling the composite organization, Forrester assumes:

- It spends $150,000 annually on its vulnerability scanner licensing costs prior to using NodeZero.
- Their reliance on their vulnerability scanner vendor is reduced, and thus their overall licensing spend is lowered by 65%. This is realized as a direct technology cost saving.

Risks. The expected financial impact is subject to risks and variation based on several factors, including:

- Cost of legacy vulnerability scanner.
- Ability to decommission or reduce vulnerability scanner licensing.

Reduced vulnerability scanner cost

65%

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $206,000.

Reduced Vulnerability Scanner Costs					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Cost of legacy vulnerability scanner	Interviews	$150,000	$150,000	$150,000
C2	Reduced vulnerability scanner reliance and licensing cost due to Horizon3 NodeZero	Interviews	65%	65%	65%
Ct	Reduced vulnerability scanner cost	C1*C2	$97,500	$97,500	$97,500
	Risk adjustment	↓15%			
Ctr	Reduced vulnerability scanner cost (risk-adjusted)		$82,875	$82,875	$82,875
	Three-year total: $248,625			**Three-year present value: $206,098**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Continuous verification of security posture to confirm remediation of weaknesses.** Running multiple six-figure third-party penetration tests a year was cost prohibitive and unrealistic for interviewees. With NodeZero, interviewees noted their organizations could orchestrate additional penetration tests at no marginal cost, allowing them to continuously verify their security posture and proactively work to fix exploitable vulnerabilities. The information security engineer of a construction organization shared: "To put numbers to that, Horizon3.ai indicates each vulnerability on a scale from 0 to 10, 10 being the most critical. When we first started off, we were averaging numbers between 6 to 8. Right now, our highest vulnerability is a 0.1."
- **Time savings for remediation guidance.** Interviewees noted the remediation guidance given with NodeZero saved their organization time on research and remediation. The information security engineer of a construction organization said, "[Horizon3.ai] gives me a better idea of what to focus on. … [NodeZero] reduces my actual remediation time by almost 50% because I don't have to go out and do as much research as I used to do. I already have the

"Horizon3 is one of the exceptional vendors we've worked with in that they provide us the vulnerability or the exploit they found and remediation steps. We're not just getting, 'hey, this part sucks, good luck fixing that.' … we have the remediation steps in the report as well."
Senior security engineer, healthcare

solutions in play. I just have to validate that those work in our environment and fix it right then and there."

  - The director of IT security in a manufacturing organization echoed, "[Horizon3.ai] has made a ton of additional enhancements, and when you get the vulnerability, you just look at it, and all the details are there: 'Here's the CVE, here's the link.' It'll tell you how to fix it, and give you the details: 'Here's how you fix it.', 'Here's a couple of different options.' I would say the product is pretty much plug and play."

- **Identify sensitive data exposure and reduce risk of breaches.** Interviewees shared that NodeZero was an integral solution in their security strategy to decrease the risk of a data breach and downstream costs such as remediation, downtime, lost productivity, legal fines, and brand damage. The director of IT security at the manufacturing organization shared: "If our initial risk of getting attacked is 100%, it's 25% now. The probability of getting an attack is down by 75%."
- **Accurately convey security posture to customers with streamlined reporting.** NodeZero reporting helped interviewees convey security posture to internal teams, executives, partners, customers, and in mergers and acquisitions. The CIO of a construction organization said: "The wonderful thing with NodeZero is now, on every single section that has to do with patching vulnerability scanning, penetration testing, and external scanning, I can just attach the reports right out of the system and never have a follow-up question from the security teams. It ensures that [our organization] is still on the good list for the cybersecurity teams of major Fortune 100 companies."
- **Accelerate vendor risk assessment.** NodeZero expedited the vendor risk assessment for several interviewees. The director of IT in a healthcare organization shared: "The [NodeZero] reports have been used, not only with our C-level folks, but we also have shared the executive report findings with potential customers and other customers if they are doing a review of our vendor status."
- **Streamline mergers and acquisitions with improved security testing and remediation.** NodeZero was instrumental in ensuring the success of the manufacturing organization's acquisition that doubled its company size. The director of IT security in a manufacturing organization estimated that without NodeZero, securing the environment of the company their organization had acquired would have taken triple the number of security professionals twice as long, or 18 FTEs across five months. With NodeZero, it took six FTEs two months to remediate their organization's additional environment.

  - The director of IT security shared: "[NodeZero] allowed us to prioritize those vulnerabilities and determine where to focus. You can imagine as you're going through an integration, there's a ton of stuff that you need to be thinking about, like email and access to file shares and network integration, Wi-Fi, guest Wi-Fi, and so on… it would allow us to highlight blind spots and gaps. Then allowing you to fix it most efficiently was instrumental in securing that integration."

- **Strong vendor partnership and support.** Interviewees noted their positive sentiment, relationship with Horizon3.ai, and the solution's efficacy. The director of IT security at the manufacturing organization said: "We use [NodeZero] very heavily and regularly. It is an

incredible tool. … Horizon3.ai is an absolutely phenomenal vendor. They're just constantly exceeding my expectations. It's a great product, it's a great team, and it massively helped us secure both our company and when we did an acquisition about a year ago."

  - The same interviewee stated: "We started early with [NodeZero], and the continuous enhancements and evolution we've seen has just been fantastic. It's just gotten better and better. It continues to evolve and improve, and it's already doing an amazing job. I'm super happy with that."

- **Improved security EX.** Interviewees shared that as NodeZero streamlined their operations and productivity, it also improved their overall security EX. The director of IT security in a manufacturing organization shared how they reduced time spent on tedious tasks: "We were able to create templates and occasionally, we might go on and modify those templates a little bit. But that is pretty much the scope for those tests with NodeZero… it's just a few minutes instead of hours of reviewing our inventory. We saved at least 20 man hours going over details for every scope we have to do for an external company."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement NodeZero and later realize additional uses and business opportunities, including:

- **Improved cybersecurity insurance rate.** One interviewee told Forrester that contrary to their peers and industry, they saw a decrease in their cybersecurity insurance rate after implementing NodeZero.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	NodeZero subscription cost	$0	$200,000	$200,000	$200,000	$600,000	$497,370
	Total costs (risk-adjusted)	$0	$200,000	$200,000	$200,000	$600,000	$497,370

HORIZON3.AI NODEZERO SUBSCRIPTION FEE

Evidence and data. Horizon3.ai charges a subscription fee based on the number of IPs an organization chooses to run penetration tests against. Volume discounts are applied depending on the number of IPs. Implementation and setup time are minimal, and new tests can be set up in minutes.

- The information security engineer of a construction organization told Forrester: "It takes around 25 to 30 minutes to fully implement a NodeZero container or NodeZero image in our environment. … In 'executive speak', it's instantaneous."

Modeling and assumptions. In modeling the composite organization, Forrester assumes:

- The composite organization pays $40 per IP across 5,000 IPs.
- Prices shown are for informational purposes only. Contact Horizon3.ai for additional details on pricing.

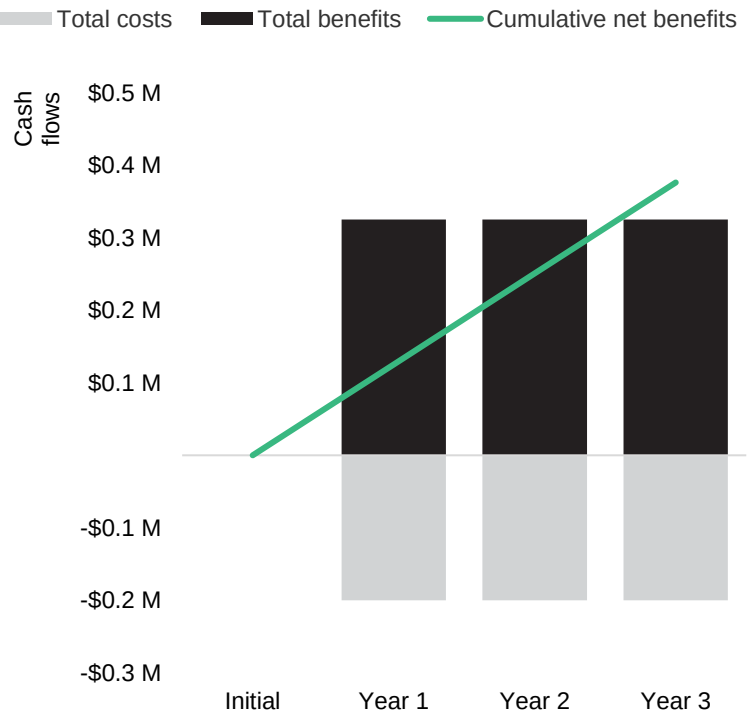
Results. Forrester did not risk-adjust the Horion3.ai NodeZero subscription fee as the pricing mechanisms are directly based on a per-IP cost with little to no implementation investment. The total three-year PV (discounted at 10%) cost is $497,000.

NodeZero Subscription Cost						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Number of IPs	Composite	$0	5,000	5,000	5,000
D2	Cost per IP	Composite	$0	$40	$40	$40
Dt	NodeZero subscription cost	D1*D2	$0	$200,000	$200,000	$200,000
	Risk adjustment	0%				
Dtr	NodeZero subscription cost (risk-adjusted)		$0	$200,000	$200,000	$200,000
	Three-year total: $600,000			**Three-year present value: $497,370**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	$0	($200,000)	($200,000)	($200,000)	($600,000)	($497,370)
Total benefits	$0	$325,443	$325,443	$325,443	$976,329	$809,329
Net benefits	$0	$125,443	$125,443	$125,443	$376,329	$311,959
ROI						63%
Payback period						0 months

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.


FORRESTER®