A Forrester Total Economic Impact™
Study Commissioned By Rapid7
November 2019

The Total Economic Impact™ Of Rapid7 InsightVM

Cost Savings And Business Benefits Enabled By InsightVM

FORRESTER®

Table Of Contents

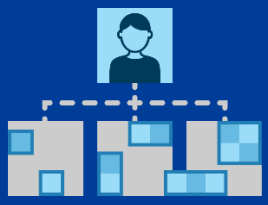
Project Director:
Henry Huang

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

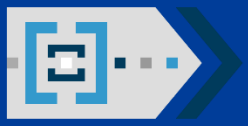
FORRESTER®

Benefits And Costs



Decreased effort to investigate and remediate vulnerabilities:
$397,2000

Scan and report efficiency gains:
$250,672



Avoidance of potential incidents with upfront risk mitigation:
$2,128,950

Executive Summary

InsightVM is a vulnerability management offering that helps its customers find IT vulnerabilities and prioritize risk, allowing customers to be proactive and minimize the impact of risk elements. Rapid7 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying InsightVM. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of InsightVM on their organizations.

Rapid7 offers a range of security solutions and services to help organizations become more secure. InsightVM is at the core of the security equation by providing visibility into vulnerabilities and the associated risks. To better understand the benefits, costs, and variables associated with an investment in this solution, Forrester interviewed several customers with years of experience using InsightVM.

Prior to using InsightVM, the customers already had vulnerability programs in place, using other modern vulnerability management tools. While these tools provided some visibility, aspects like remediation and automation could have been improved upon, leading the customer organizations to initiate proof of concept (PoC) tests on InsightVM. The tests revealed InsightVM to have improved scanning efficacy and accuracy, easier reporting, and better-defined courses of remediation — all while reducing risk. One director of information security expressed to us: “The problem with our old solution was the remediation instructions not being specific. Where InsightVM told us the specific actions for remediation, the old solution would just describe the resolution broadly and send us to articles on the vulnerabilities.” With InsightVM, organizations increased the efficiency of security, network, and development operations dramatically by optimizing the entire vulnerability management program.

Forrester developed a composite organization to reflect the impact InsightVM could have on an organization. The composite is representative of the organizations that Forrester interviewed and is used to present the aggregate financial analysis in this study. All values are reported in risk-adjusted, three-year present value (PV) unless otherwise indicated. (InsightVM will be commonly referred throughout the rest of this study as IVM.)

Key Findings

Quantified benefits. The following benefits reflect the financial analysis associated with the composite organization.

- **The efficacy of InsightVM reduces the manual effort to investigate as well as remediate vulnerabilities by 33%.** Accurate analyses of IT assets lead to fewer false positives, fewer investigations, and often time-consuming triage sessions. The accuracy and fidelity additionally provide for a much easier exercise on the remediation end. The combination of fewer investigations and quicker remediations provide a benefit value of $397K over three years.
- **Scanning and reporting of the IT stack was less tedious — this leads to a value gain of $250K over three years.** Usage of InsightVM reduces the time spent to scan and report on vulnerabilities. The tediousness of creating different reports is eased without losing fidelity. On average, security teams are able to shave 40% to 50% off time spent reporting activities.

FORRESTER®

ROI
342%

Benefits PV
$3 million

NPV
$2.3 million

Payback
<6 months

- **Patching automation and improved workflows reduce manual effort to patch by 60%.** InsightVM integrates with popular patching software like BigFix or SCCM, folding into the workflow so that much of the vulnerability patching process becomes automated. Savings over three years are $188K.
- **Earlier detection, especially on development efforts avoids future incidents and events, leading to savings of $2.1 million over three years.** Incorporation of the highly effective InsightVM engine early in the development cycle, and on changing infrastructure, avoids remediation and redevelopment efforts later in time. Security, network, and development operations teams save up to 30% in people resources.

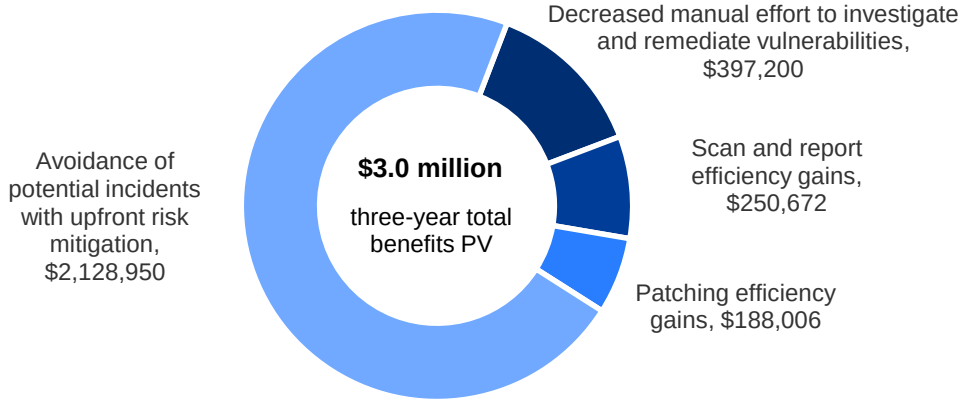
Unquantified benefits. The interviewed organizations experienced the following benefits, which are not quantified for the composite:

- **Organizational specific risk scoring helps organizations address the most important risks first, rather than throw resources at the entire risk surface.** IT assets don't always carry the same risk. For example, patient records or HR servers, at the perimeter, can carry a much higher risk. InsightVM scores risk with business context so that organizations can prioritize what matters most..
- **One single lightweight agent for multiple solutions reduces the parasitic drag on IT asset performance.** End users are kept happy with negligible performance degradation, and administrators appreciate that the single agent also provides data for other Rapid7 platforms such as incident detection on InsightIDR.

Costs. The composite organizations experienced the following risk-adjusted PV costs:

- **Direct costs of Rapid7 and external implementors.** Rapid7 charges for the InsightVM offering on a subscription basis. Beyond the costs paid to Rapid7, costs are paid to third-party implementors for integration to other IT services. Three-year costs amount to $442K.
- **Internal costs of integration and training.** To fully leverage automation and optimize workflows, the composite integrates InsightVM with various platforms and point solutions to leverage security orchestration automation and response (SOAR). Total effort, including training, carries a cost of $227K over three years.

Forrester's interviews with five existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $2,964,828 over three years versus costs of $670,123, adding up to a net present value (NPV) of $2,294,705 and an ROI of 342%.



FORRESTER®

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Rapid7 InsightVM.

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 Rapid7 InsightVM can have on an organization:

DUE DILIGENCE
Interviewed Rapid7 stakeholders and Forrester analysts to gather data relative to InsightVM.

CUSTOMER INTERVIEWS
Interviewed five organizations using InsightVM to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Rapid7 InsightVM's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Rapid7 and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Rapid7 InsightVM.

Rapid7 reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Rapid7 provided the customer names for the interviews but did not participate in the interviews.

The InsightVM Customer Journey

BEFORE AND AFTER THE INSIGHTVM INVESTMENT

Interviewed Organizations

For this study, Forrester conducted five interviews with Rapid7 InsightVM customers. Interviewed customers include the following:

INDUSTRY	LOCATION & REVENUE	INTERVIEWEE	IT ASSETS
Financial services	North America/$1B+	Infosec manager	5,000
Healthcare	North America	Director of infosec	1,700
IT services	Global/$1B+	Infosec team lead	40,000
Education	North America	Deputy CISO	15,000
Transportation	Global/$10B+	Security manager	10,000

Key Challenges

Keeping data secure is a tough job, and the promise of compliance to constituents, customers, and ever-increasing regulatory measures only add to that difficulty. To the customers, understanding their assets and the risks that they carry are paramount. One manager of infosec stated: "The goal was to at least understand all of our assets. We had machines off the network for extended periods of time so a quick scan wouldn't work. We needed an agent that would report back as soon as the machine hit our network." Without such a feedback loop providing visibility, risk cannot be accurately measured or dealt with.

Other challenges existed as well, such as the ability to provide meaningful contextual information to both executives, who needed to understand risk levels, and to security and the broader IT group, to act with efficiency. The most glaring of the challenges are as follows:

- **Visibility without context isn't always actionable due to the lack of depth in information provided.** Some of the products tested by the customers provided meaningful visibility, but they lacked the ability to deliver actionable advice. One customer thought of this as analogous to application performance monitoring and logging platforms, where superfluous data straddled operators with more analytical work on the path to remediation. Simply put, actionable insights were more valuable to this customer, instead of more data.

  Another interviewee said: "Our old vulnerability management platform used to say, 'Hey, there's this new system and it has this vulnerability over here.' And in the beginning, that was helpful. But quite frankly, it didn't really give me the in-depth east-west visibility that I really wanted."

- **Triage sessions, especially on false positives were a tremendous resource drain.** Working with thousands of vulnerabilities that appear, investigative work required significant people resources. While some false positives were easily addressed, complex situations required triage between various groups within IT, taking away precious time for threat hunting.

> "With vulnerabilities, it all comes down to risk. CVSS scores were a problem because they're static. The InsightVM Real Risk scoring really has allowed me to prioritize for what matters to our specific business."
>
> *Infosec manager, financial services org*

> "InsightVM really reduces the amount of work that my team has to do. Before, a lot of it was working with application and server owners to provide them reports, then do the scans, etc. — it was major time sink. Now the platform is mostly self-service giving infosec hours back that we can apply elsewhere."
>
> *Director of infosec, healthcare*

FORRESTER®

- **Common vulnerability scoring system (CVSS) risk scoring was too generic for the diverse nature of organizations and the regulatory measures that they operate with.** The inability for some organizations to decipher which vulnerabilities are important to their specific business compounds the issue of false positives. The CVSS scoring system is a broad guideline that does not always lead security professionals to the vulnerability that needs addressing most urgently.
- **Off-network devices are not always accounted for, nor are they regularly scanned with existing systems.** One interviewee lamented at the fact that previous vulnerability management agents required access that made their team uncomfortable, leading to a lapse in vulnerability assessment. They said: "A big part of our issue was the off-network assets, because 90% of our workforce will never connect to the network. With our old [vulnerability management] platform, these systems never got touched and we couldn't get the vulnerability data from those machines easily without opening security holes."
- **Reporting was a burdensome task for security professionals.** Prior to Rapid7, many of the organizations used security professionals — a consistently scarce resource — to produce vulnerability reports for a wide range of constituents. Network and development operations teams required reports to start working on specific jobs while management and compliance officers needed the information to assess risk and complete audits. There was a lack of automated distribution or easily deciphered dashboarding. In one of the organizations, three FTEs spent the vast majority of their year on generating the reports needed within the organization.

"The dashboards and reports in InsightVM are very flexible. We're able to present the material in any number of different ways, so it's nice. The C-level, like the executive summaries and everyone else, is getting the exact information that they need."

Director of infosec, healthcare

Key Results

The interviews revealed that key results from the InsightVM investment include:

- **The beneficiaries of InsightVM's ability to detect and present findings effectively includes not only security teams, but also network and development operations, the rest of IT, and management.** With InsightVM, security and development teams avoid investigating extraneous false positives, while IT operations and DevOps spent less time rectifying issues due to actionable remediation with a few clicks. Realtime dashboards tracked the progress of vulnerabilities – making it a bit easier for team leads and management to sleep.

  At an IT services company, the interviewee reported that their remediation efforts needed two less FTEs, allowing them to concentrate on other activities like threat hunting. Separately, a director at a healthcare organization explained: "The remediation instructions coming from [the previous solution] were not close to what was coming out of InsightVM. The InsightVM output was very specific."

"InsightVM's reporting capability is huge. The biggest problem in security is not about, 'Hey, there's an issue here,' but rather it's about telling the story about it, what it means to the business, and how to remediate it. With InsightVM, I can tell a huge part of the story from one place."

Infosec manager, financial services org

- **Real risk scoring was brought to the customers, in context of what mattered to their organizations.** Assets like customer records are always important to protect, but carry different significance between organizations such as healthcare and professional services. By intelligent weighing of factors that are most relevant, it was easier prioritize resource allocation in a world where vulnerabilities surface regularly. Risks and vulnerabilities will always be present, which one interviewee stated to be similar to "whack a mole, where they keep popping up." Limited resources were able to be aimed at true risk factors – ones that had the potential to affect the business most.
- **Automation brought about significant operator efficiencies.** Once integrated with patching programs and other workflows within IT, InsightVM was able to direct remedial instructions to the appropriate parties requiring minimal human input. Workflows were streamlined effectively reducing work effort across operations. An infosec team lead said, "The [old] solution needed a lot of massaging of the data and essentially made for a very manual remediation process."
- **High satisfaction in overall value.** The Deputy CISO at an educational organization stated: "We have grown substantially in the past 10 years without really growing cost, while continuing to mitigate risk in the threat environment quickly. The security checks within the [InsightVM] product are kept up extremely well, especially with zero-days. When we called their support to talk about creating some custom checks on our dashboard following a week full of zero-days, there was no fee for the help from Rapid7. To me, that's value."

> "What we really like about Rapid7 is the reporting. Our teams get their own different reports from the system and they can see which hosts have issues and which of those hosts are most severe. The nice touch on top is that the report tells us how to fix those issues."
>
> *Infosec team lead, IT services*

Composite Organization

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

Description of composite. The composite organization is based on a global enterprise that complies to the Payment Card Industry Data Security Standard (PCI-DSS) and the General Data Protection Regulation (GDPR), as well as other requirements set forth by select clients. Vulnerability management has always been taken seriously by this organization and they have previously deployed a non-Rapid7 vulnerability management platform. As a best practice, this organization regularly performs PoCs and tests to ensure that they are using the very best in technology — it's especially necessary to extract the most of its lean security team. Objectives for a new platform include increased scanning efficacy and extensions to automate remedial activities.

Deployment characteristics. The security operations team at the composite organization consists of 10 people, of which a handful concentrate on vulnerability management. These operators are involved with an initial deployment of InsightVM following a successful PoC bake-off. A rollout of InsightVM is completed in approximately six months, accounting for planning, integrating, and baselining the IT assets.

Key assumptions:

- Global enterprise
- 12,000 IT assets
- Has internal security operations team of 10 FTEs
- Develops significant internal custom apps and functionality
- Desires to integrate InsightVM with other IT tools

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	Decreased manual effort to investigate and remediate vulnerabilities	$159,720	$159,720	$159,720	$479,160	$397,200
Btr	Scan and report efficiency gains	$100,799	$100,799	$100,799	$302,397	$250,672
Ctr	Patching efficiency gains	$75,600	$75,600	$75,600	$226,800	$188,006
Dtr	Avoidance of potential incidents with upfront risk mitigation	$739,200	$864,000	$988,800	$2,592,000	$2,128,950
	Total benefits (risk-adjusted)	$1,075,319	$1,200,119	$1,324,919	$3,600,357	$2,964,828

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of nearly $3 million.

Decreased Manual Effort To Investigate And Remediate Vulnerabilities

Interviewed organizations described the following insights on the decrease of investigation and remediation efforts with InsightVM:

- A primary challenge for many of the customers was the investigative work required once vulnerabilities were found. Vulnerabilities that were high on the risk score dictated immediate attention from multiple groups that would triage to investigate the issue. This time-consuming exercise was compounded by a high false-positive rate, which averaged 20% greater than what they found with InsightVM.
- In addition to the unnecessary investigative work, remediation efforts outside of simple patching were also drawn out efforts. Lacking sufficient actionable insights from previous vulnerability management solutions, these organizations needed nearly twice the security professionals as with InsightVM. Multiple organizations praised the specificity of remedial action on InsightVM, leading to faster remediation.
- Effectively, InsightVM helped organizations reduce vulnerabilities faster while requiring less people resources.

According to the director of infosec in the healthcare industry: “Looking back to when we switched to InsightVM, for the app dev team, we had around 6,000 critical vulnerabilities and 2,000 severe vulnerabilities.” The question was not whether the organization wanted to remediate the vulnerabilities, but rather a matter of people resources to analyze and tackle the problems. The director continued: “So with the same team, we’ve got 46 critical and 200 severe vulnerabilities today. A lot of that comes by not only from having the right team and tool, but also giving them digestible information to handle the holes.”

Modeling after the interview results, the composite organization assumes the following:

Customers consistently reported risk scores that decreased 50% or greater after implementing InsightVM.

FORRESTER®

- False positives are reduced by 22%, eliminating a portion of the investigative work by security operations.
- The effort to remediate decreased across multiple groups. We assume that security, development, and network operation teams all benefit, as complex remediations are commonly achieved through inter-team efforts. By providing the context and action steps, teams were allowed to remediate 33% faster.
- Not modeled here is the resulting decrease in risk score for the composite organization. The value of decreased risk is explained further in the Unquantified Benefits section further below.

Over a three-year projection period, Forrester forecasts this benefit to be worth a risk-adjusted total PV of $397,200.

Decreased Manual Effort To Investigate And Remediate Vulnerabilities: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Number of FTEs dedicated to vulnerability management on prior solution		5	5	5
A2	Percentage of time spent on investigating and triaging vulnerabilities		20%	20%	20%
A3	Decrease in false positive detection on InsightVM		22%	22%	22%
A4	Security, development, and network operations FTE effort responsible for remediation	Combined effort equivalent to 3 FTEs	3	3	3
A5	Average annual compensation of vulnerability investigation and remediation FTEs	$110K*1.2x benefits modifier	$132,000	$132,000	$132,000
A6	Decrease in effort to remediate vulnerabilities due to contextual and actionable reporting		33%	33%	33%
At	Decreased manual effort to investigate and remediate vulnerabilities	(A1*A2*A3*A5)+(A4*A5*A6)	$159,720	$159,720	$159,720
	Risk adjustment	0%			
Atr	Decreased manual effort to investigate and remediate vulnerabilities (risk-adjusted)		$159,720	$159,720	$159,720

Scan And Report Efficiency Gains

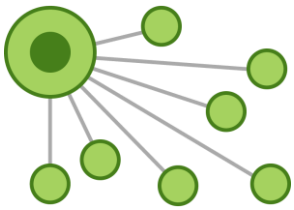
Scan efficacy and report generation were common pain points for the interviewed organizations. One customer vocalized that because the existing solution missed a number of nodes and endpoints on scheduled scans, manual scans were often required. Further still, some customers found that some vulnerabilities were missed when doing head-to-head tests, leading them to question the effectiveness of the previous solution's agent. For another customer, the fact that the competition's scanning agent required deep-level credential access was a non-starter, as it would present a new risk for his organization. With InsightVM, the agent reported back quickly, enabling a more up-to-date assessment of the environment.

Reporting became a more positive experience for multiple interviewees. Drawing from fresh agent data, dashboards were near real time while reports could be pulled with ease. Time savings on producing reports — whether it was for audits, management, or general IT purposes resulted in nearly 90% for the interviewed transportation company. The security manager explained: "Back in the day, we had a team of three people who spent a majority of their time generating vulnerability reports. As we moved forward [with InsightVM], the work has greatly reduced. We've gone from three people to nearly no one on reporting duty."

For the composite organization, Forrester anticipates that:

- It spent the equivalent of 1.5 FTEs on vulnerability scanning and reporting prior to using InsightVM.
- Time savings on scanning and reporting are both significant, based primarily on the effectiveness on the scans and the ease of report production.
- Automation is a contributor to the scan and report process, particularly on scheduled scans and reports.

Comprehensively for scans and reports, Forrester estimates this benefit to yield a three-year, risk-adjusted total PV of $250,672.



During a PoC bake-off, InsightVM detected nearly twice as many vulnerabilities as another solution.

"InsightVM has been transformational for us. It's allowed us to bring the stakeholders into the process. Due to the ease of InsightVM, stakeholders can run their own reports or scans whenever they want. As a result, they've now taken ownership of issues and are now helping to drive down risk."

Director of infosec, healthcare

FORRESTER®

Scan And Report Efficiency Gains: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
B1	Security operations FTE time spent on manual scanning and reporting, in hours		1,040	1,040	1,040
B2	Security operations FTE time spent on automated scanning and reporting, in hours		2,080	2,080	2,080
B3	Security operations effort reduction on ad hoc manual vulnerability scans and reporting		40%	40%	40%
B4	Security operations effort reduction on scheduled vulnerability scans and reporting, due to automation		50%	50%	50%
B5	Security operations FTE hourly cost	$120K*1.2x benefits modifier/2,080 hours	$69.23	$69.23	$69.23
Bt	Scan and report efficiency gains	B5*((B1*B3)+(B2*B4))	$100,799	$100,799	$100,799
	Risk adjustment	0%			
Btr	Scan and report efficiency gains (risk-adjusted)		$100,799	$100,799	$100,799

Patching Efficiency Gains

Patching is a common form of remediation for vulnerabilities. And while these are often simple in nature, they are often required, especially with today's frequency of software releases. Customers of InsightVM appreciated the out-of-box linkage to patching software like SCCM and BigFix, as the linkage provided a level of automation that streamlined the entire vulnerability patching process. While the customers made no indication that the automation was to be a complete hands-off solution, they did indicate that many of the repetitive tasks such as information collection, requests to system administrators, and validation of patching were reduced or consolidated.

For the composite organization, Forrester anticipates that the organization leverages 1.5 FTEs for vulnerability patching. With an effective decrease of 60% in patching effort, the savings is equivalent to a PV of $188,006 over a three-year period.

Vulnerability related patching requires 60% less effort with InsightVM automation.

Patching Efficiency Gains: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	IT operators in charge of patching and maintenance		1.5	1.5	1.5
C2	Decrease in patching effort in workflow due to automation		60%	60%	60%
C3	IT operator annual salary	$70K*1.2x benefits multiple	$84,000	$84,000	$84,000
Ct	Patching efficiency gains	C1*C2*C3	$75,600	$75,600	$75,600
	Risk adjustment	0%			
Ctr	Patching efficiency gains (risk-adjusted)		$75,600	$75,600	$75,600

Avoidance Of Potential Incidents With Upfront Risk Mitigation

The interviewed organizations all follow the best practice of scanning and testing new introductions to the corporate network, to avoid potential vulnerabilities and incidents once in production. Two of the interviewees went further by introducing vulnerability testing during internal development cycles. For these customers:

- The early introduction of vulnerability testing in the software development lifecycle reduces development rework and additional test cycles, effectively shifting left on the vulnerability issue. By programming in this workstream, developers were able to save 10% to 15% in time over the long run.
- Incident responders, security professionals, and developers all reaped the benefits of shifting left, with two groups earlier avoiding potential incidents and vulnerabilities that may have arisen when in production. By the customer's estimation, one security professional, multiple incident responders, and several help desk personnel were reallocated to other duties.

Based on the interview findings, the Forrester composite model assumes the following:

- Forty developers (or one-third of the entire developer group) leverage this development model. Not all development efforts are applicable. Development efforts increase on this model year-over-year as they become more acclimated to developing in this manner.
- Developer effort savings are conservatively estimated at 10%.
- Security operations FTE usage decreases by one for incident/event/vulnerability.
- General IT personnel usage decreases by two FTEs.

Some potential variability exists however, especially as some organizations outsource their development. Additionally, developers may take an extended period of time to ramp up. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $2,128,950.

Shift left on vulnerability management in dev cycles to avoid potential incidents in the future.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Avoidance Of Potential Incidents With Upfront Risk Mitigation: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
D1	Security operations FTE reallocated from decreased incident rate		1	1	1
D2	IT FTEs reallocated due to decreased incident rate		2	2	2
D3	Development operations FTEs engaged in testing vulnerabilities up front		40	50	60
D4	Reduction of development operations effort with dev/test once, rather than multiple efforts		10%	10%	10%
D5	Security operations FTE annual salary	$110K*1.2x benefits modifier	$132,000	$132,000	$132,000
D6	IT operations FTE annual salary	$70K*1.2x benefits modifier	$84,000	$84,000	$84,000
D7	Development operations FTE annual salary	$130K*1.2x benefits modifier	$156,000	$156,000	$156,000
Dt	Avoidance of potential incidents with upfront risk mitigation	(D1*D5)+(D2*D6)+(D3*D4*D7)	$924,000	$1,080,000	$1,236,000
	Risk adjustment	↓20%			
Dtr	Avoidance of potential incidents with upfront risk mitigation (risk-adjusted)		$739,200	$864,000	$988,800

Unquantified Benefits

Forrester's interviews with Rapid7 customers revealed that while there are very tangible and quantifiable benefits to using InsightVM, there is also a benefit that cannot be quantifiably portrayed in a one-size-fits-all model. Specifically, we noted the different prioritization of risk elements based upon the business's needs and industry can affect the potential monetary assignments to breaches. Readers are advised to consider their own calculations on their risk-tolerance and the possible cost ramifications of breaches.

Due to a weighted risk scoring system that allows organizations to move beyond CVSS, organizations using InsightVM are at a lower risk of suffering losses when breached because of prioritization of vulnerabilities on the network map that are critical to that specific business. Security operations no longer need to investigate all items that are deemed important on the CVSS rating, but instead focus efforts on assets that matter more in the situation.

One infosec manager stated: "CVSS is stale and static, and what's more is that not every audience is looking for the same thing. I can change the weighed scale on the fly and let different groups know what's important, so that they too can prioritize."

Risk carries a different meaning for every organization. InsightVM helps contextualize risk scores for relevance to individual organizational tolerances.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement InsightVM and later realize additional uses and business opportunities, including:

- **Augmentation of existing security operations center (SOC) with Rapid7 managed detection and response (MDR).** In speaking with the interviewees, it was clear that experienced security analysts were a difficult commodity to hire. Rapid7 has the flexibility to provide MDR, off-handing some of the traditional responsibilities of security operations to bring together a flexible and effective secondary team.

  An interviewee from a healthcare organization said: "I put their SOC services through the ringer during our PoC. I ran them through a couple of red team exercises and I think on the first red team exercise I got; they called my phone in minutes. And I was doing a very serious recon, trying to be very stealthy, and we got a call and stick to minutes and it was like, 'Damn, all right, good for you.'"
- **Addition of services without adding additional agents.** The Insight Agent used for InsightVM is the same agent that works across all Rapid7 offerings, which means that potentially adding Rapid7 incident detection or log management would bring about little additional load to IT assets.
- **Connectivity is king.** InsightVM has built-in connectivity with popular ticketing platforms. The flow of information between InsightVM, the configuration management database (CMDB), and ticketing platform enables automated workflow assignments that are distributed to proper teams. A RESTful API is also available, but readers are advised to consider the cost of integration/customization on the recipient side of the API.

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

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
Etr	Direct costs of Rapid7 and external providers	$92,000	$125,718	$171,718	$125,718	$515,154	$442,659
Ftr	Integration and training costs assigned internally	$159,158	$72,598	$2,792	$0	$234,548	$227,464
	Total costs (risk-adjusted)	$251,158	$198,316	$174,510	$125,718	$749,702	$670,123

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of $670K.

Direct Costs Of Rapid7 And External Providers

Interviewed organizations described the following as direct costs that were paid to Rapid7 and their external service partners.

- The subscription license for Rapid7 InsightVM was straightforward and based upon assets managed and charged on a yearly rate.
- Additional external costs, beyond the Rapid7 licensing costs, were incurred as customers desired deeper integrations to other security and IT platforms.
- All support costs were included with the Rapid7 licenses, with several customers being extremely positive on the support they had received.

Based upon the customer interviews, Forrester estimates for the composite organization:

- All assets are covered under Rapid7 InsightVM licenses, to a gross figure of $109,320 per year.
- Two custom integrations are done at the onset of adoption by an external partner, with an additional integration done on Year 2. All integrations are designed to increase automation and operational efficiency.

The cost of custom integration can vary however, depending on the application stack already in place. Organizations are advised to assess their own security program and the level of integration that they need, especially if SOAR is already in place or on the roadmap.

To account for this risk of additional integrations, Forrester adjusted this cost bucket upward by 15%, yielding a three-year, risk-adjusted total PV of $442,659.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Direct Costs Of Rapid7 And External Providers: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Rapid7 InsightVM license cost			$109,320	$109,320	$109,320
E2	External professional service assisting in integration work		$80,000		$40,000	
Et	Direct costs of Rapid7 and external providers	E1+E2	$80,000	$109,320	$149,320	$109,320
	Risk adjustment	↑15%				
Etr	Direct costs of Rapid7 and external providers (risk-adjusted)		$92,000	$125,718	$171,718	$125,718

Internal Integration And Training Costs

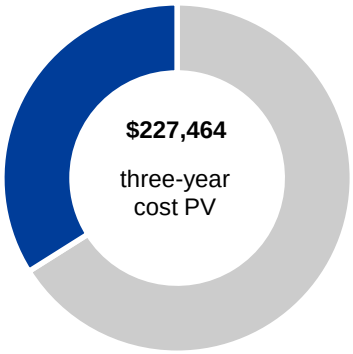
Interviewed organizations described the following costs that were assumed internally, as indirect costs:

- Integration to the existing IT stack required internal resources in addition to the external service provider. A small team of development, security, and network operators spent three months for each manual integration that was performed.
- In addition to integration, the effort and time to baseline and customize workflows to fit within compliance policies were also accounted for in the initial implementation phase.
- Installation and initial deployment absent of the two terms stated above required minimal effort or time.

Based on the customer interviews, Forrester estimates the following for the composite organization:

- Two manual integrations are performed during the initial implementation phase, resulting in two FTEs expending a total of six months of effort.
- Several other integrations were also performed, however, they required built-in direct integration between the applications such as Microsoft SCCM. These integrations are supplied out-of-the-box and hence require a very small amount of effort.
- Training is supplied to security personnel, but given that all customers praised the interface, actual training effort and time was minimal. The expected training per FTE is one week, spread across initial months.

In some instances, organizations may require additional integration effort due to more complex IT stacks. Additionally, onboarding/training may extend to DevOps and bring about a degree of uncertainty in the costs accrued. To account for this risk, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $227,464.



Internal integration and training costs: **34%** of total costs

Six months
of total implementation and deployment time.

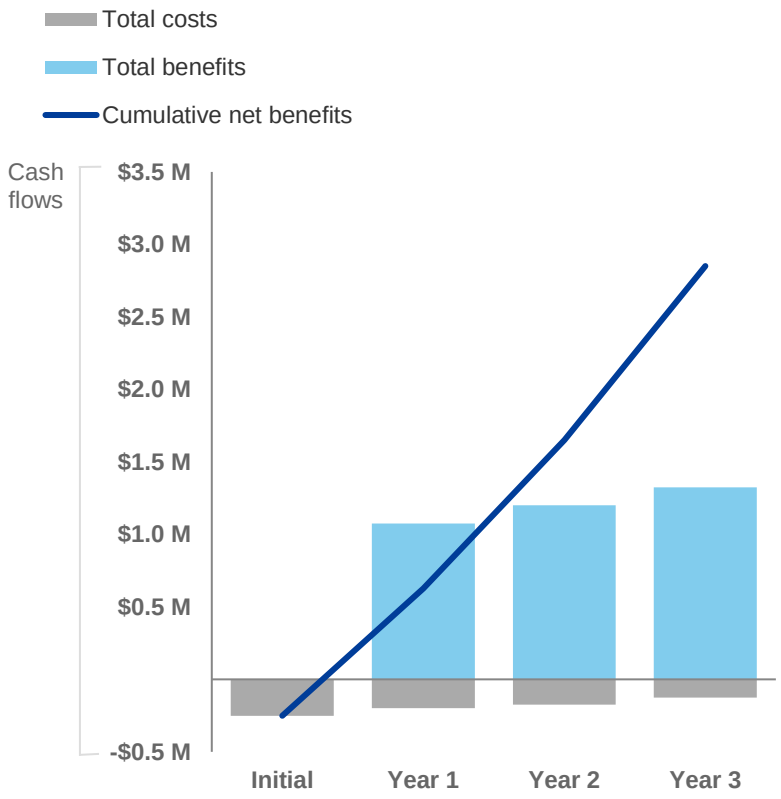
FORRESTER®

Internal Integration And Training Costs: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	Integration, development efforts, and baselining by development and security operators, in hours	2 FTE at 3 months per manual integration	2,080	1,040		
F2	Hourly cost per development and security operations FTE or equivalent, fully loaded	$110K*1.2x benefits/ 2,080 hours	$63.46	$63.46	$63.46	$63.46
F3	Training and onboarding to InsightVM	5 FTE for 1 week at $63.46 per hour	$12,692		$2,538	
Ft	Internal integration and training costs	F1*F2+F3	$144,689	$65,998	$2,538	$0
	Risk adjustment	↑10%				
Ftr	Internal integration and training costs (risk-adjusted)		$159,158	$72,598	$2,792	$0

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($251,158)	($198,316)	($174,510)	($125,718)	($749,702)	($670,123)
Total benefits	$0	$1,075,319	$1,200,119	$1,324,919	$3,600,357	$2,964,828
Net benefits	($251,158)	$877,003	$1,025,609	$1,199,201	$2,850,654	$2,294,705
ROI						342%
Payback period						<6 months

FORRESTER®

Rapid7 InsightVM: Overview

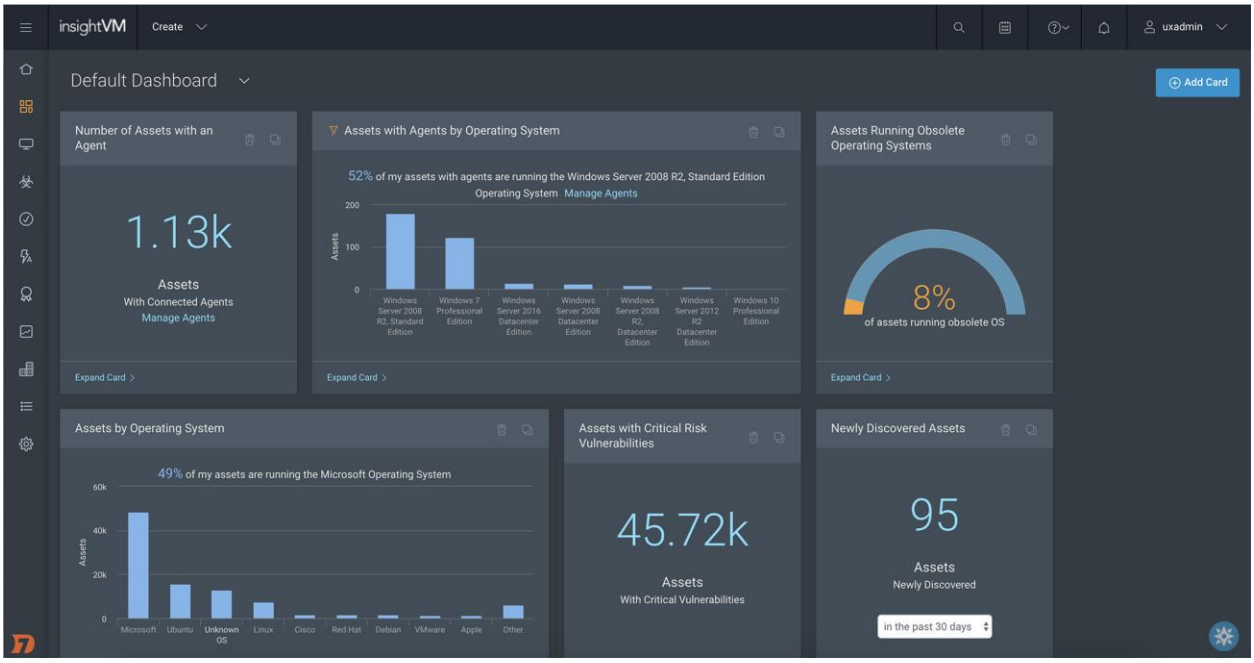
The following information is provided by Rapid7. Forrester has not validated any claims and does not endorse Rapid7 or its offerings.

Utilizing the power of the Rapid7 Insight cloud, InsightVM is the industry-leading vulnerability management solution for your modern environment. With InsightVM, you can:

Gain Clarity Into Risk
InsightVM not only provides visibility into the vulnerabilities in your modern IT environment, but also clarity of shared work and objectives. With a deeper understanding of risk, cross-functional teams can work in lockstep towards common goals.

Extend Security's Influence
InsightVM is not a silver bullet. Instead, it is a foundation for security leaders to expand their influence and eliminate silos by sharing a common language and objectives with technical teams.

See Shared Progress
InsightVM is not another reactive security tool. It's designed to support proactive security programs with tracking and metrics that create accountability across teams and recognize shared progress and impact.



FORRESTER®

How exactly does InsightVM do this in your environment?

- **Clear Risk Assessment and Prioritization**
  InsightVM identifies vulnerabilities across your modern IT infrastructure, from local to remote, and cloud to containerized assets. Capabilities like Attack Surface Monitoring with Project Sonar, Container and Cloud Assessment, Threat Feeds, and our proprietary Real Risk Score offer insight into how those vulnerabilities translate into business risk, and which are most likely to be targeted by attackers.

- **Remediation with Impact and Influence**
  InsightVM provides the shared view needed to align traditionally siloed teams and drive impact with features such as Live Dashboards, IT-Integrated Remediation Projects, Automation-Assisted Patching, and Automated Containment. Its Goals and SLAs feature supports a proactive approach to vulnerability management with tracking and metrics that create accountability for remediators, demonstrate impact across teams, and celebrate progress.

- **Unified Endpoint Assessment**
  The Insight Agent is a universal, lightweight agent that collects data across the Rapid7 Insight cloud, including InsightVM and our leading cloud SIEM, InsightIDR. With it, you can get live intel into both network and user risk on your endpoints.

- **Maximization of Your Tech Stack**
  Point solutions are a thing of the past. Rapid7's dedicated integrations team ensures that InsightVM is a foundational source of intelligence for the rest of your security program, helping all your products, like InsightIDR, work better together to collectively improve ROI. InsightVM not only integrates with 40+ other technology solutions, but also offers a fully documented RESTful API that makes it easy to automate virtually any aspect of vulnerability scanning.

Knowing your risk is just the beginning: Prioritize work, align teams, and see progress with InsightVM.

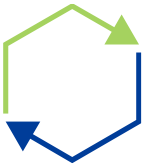
Appendix A: Total Economic Impact

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.