A Forrester Total Economic Impact™
Study Commissioned By Rapid7
April 2020

The Total Economic Impact™ Of Rapid7 InsightIDR

Cost Savings And Business Benefits Of Rapid7's Cloud-Based SIEM

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.

© 2020, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com.

FORRESTER®

Financial Findings

ROI
445%

Benefits PV
$2,445,343

NPV
$1,996,838

Payback
< 3 months

Executive Summary

Rapid7 provides cloud-based security information and event management (SIEM) in InsightIDR as a part of its comprehensive security offerings. This solution helps customers aggregate security events and provide real-time information and assessment on security threats across the network. Rapid7 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying InsightIDR. This study provides readers with a framework to evaluate the potential financial impact of InsightIDR on their organizations and how it can affect security operations when moving away from legacy on-premises-based SIEMs.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with years of experience using InsightIDR, and whose organizations had used a different SIEM prior to InsightIDR. Our findings revealed that the advanced behavioral analytics and overall presentation of security incidents on the solution vastly improves the ability for organizations to contain and mitigate security issues. In addition, we found the solution to require significantly less security operations (SecOps) FTEs to run and respond in a timely manner. Attributes that are core to the solution are:

- Advanced user- and entity-based analytics (UEBA) to triangulate on potentially harmful activity even without known malicious signatures being detected.
- Immediate visibility to security insights that are often buried in logs that would traditionally require significant SecOps analysis.
- Enablement of SecOps to respond efficiently with human-readable, -actionable, and -correlated data.

Ultimately, the current customers of Rapid7 found that their previous solutions provided limited visibility on the security front and as a result, suffered from a lack of ability to effectively combat threats and reduce risk profiles. Customers often found the insurmountable amount of data in logs to be wasted, as they did not have enough SecOps personnel to process through the logs, causing security incidents to slip through altogether. Other issues with previous SIEMs included: detection against ever-increasing attack vectors, lack of automation, and general upgradeability/scalability concerns of legacy on-premises SIEMs. After adopting InsightIDR, one InfoSec manager stated to Forrester:

- "I use InsightIDR as the backbone to everything that we do. When I look at other security tools, my first question is if InsightIDR can already solve the problem for me, as it does so much for us already."

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

Summary Of Benefits

Faster response efficiency time savings:

$1,227,403

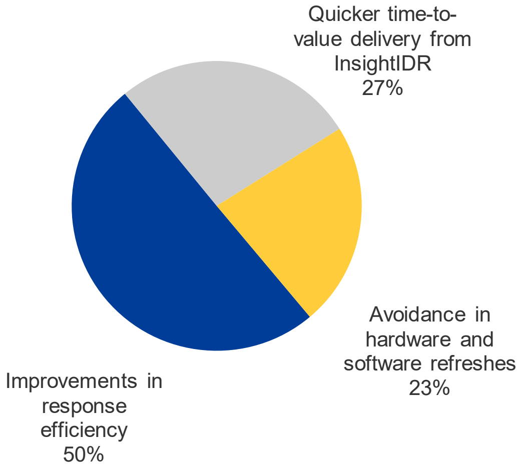
Avoided hardware and software expenditures:

$557,944

Decrease in time to deliver value:

$659,996

Benefits Breakdown



- **Improved security response efficiency, driven by accurate information correlation onto a single pane of glass, produces a time savings equal to $1,227,403 over a three-year period.** Interviewees often praised the incident correlation ability and the effectiveness of the UEBA on InsightIDR. Improved delivery of curated and actionable information led to a drastic drop in the mean-time-to-know (MTTK) and remediation of security incidents.

- **InsightIDR delivered value sooner, through faster implementation times and intuitive delivery of information, leading to a three-year benefit of $659,996.** A single agent working across all network devices makes for faster installation and baselining. The simplicity of the interface and presentation of information also decreased the amount of training SecOps needed to go through with before running at steady state.

- **The cloud-based nature of InsightIDR helped organizations avoid purchasing and refreshing hardware and software associated with a legacy SIEM, bringing a three-year benefit of $557,944.** In relegating the upkeep of the SIEM to Rapid7 on the cloud, organizations save on hardware, software/support licenses, and indirect labor for the maintenance of on-premises infrastructure. The capex savings are ongoing as most legacy solutions require refreshes every two to four years.

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

- **Audits and compliance are easier to prove with a single pane of glass on InsightIDR**. Thorough backtracking of incidents and events make it easy to report on root cause as well as exceptions to compliance policies. External and internal audit efforts can be fast-tracked.

- **Avoidance of security tool purchases beyond SIEMs are possible after implementing InsightIDR.** The solution goes beyond SIEMs in that it can provide out-of-the-box network traffic analysis, log aggregation, deception technology, and file integrity monitoring.

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

- **License costs are easy to compute, which are based on assets and incur a cost of $402,392 over a three-year period.** Licenses are based on IT assets at list levels, which include support costs, and assessed on a yearly basis.

- **The cost of standing up InsightIDR to a steady state is a strong point of the solution, with costs of testing and tuning requiring $43,917 over a three-year period.** Security posture is a perpetual exercise in motion and the tuning and testing with InsightIDR is no exception. Working in its favor, however, is the ease to stand up the platform and ease of baselining to minimize internal effort.

Forrester's interviews with five existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $2,445,343 over three years versus costs of $448,505, adding up to a net present value (NPV) of nearly $2 million and an ROI of 445%.

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 InsightIDR.

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 InsightIDR can have on an organization:

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

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

CUSTOMER INTERVIEWS
Interviewed five organizations using InsightIDR 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 InsightIDR’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 InsightIDR.

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 InsightIDR Customer Journey

BEFORE AND AFTER THE INSIGHTIDR INVESTMENT

Interviewed Organizations

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

INDUSTRY	FTE COUNT	IT ASSET COUNT	NUMBER OF SECURITY OPERATIONS PERSONNEL
Consumer goods	~10,000	~7,000	Three SecOps and 20 IT incident responders
Industrial supplies	~750	~750	Two SecOps and 14 IT incident responders
Hospitality	~10,000	~2,600	Two SecOps professionals
Media	~7,000	~5,000	Five SecOps professionals
Retail group	~11,000	~30,000	Four SecOps and 60 IT incident responders

Key Challenges

Forrester consistently heard InsightIDR customers coming from environments where it was increasingly difficult to detect a breach. Factors such as a rapid increase in IT assets, growth in transactional data, and difficulty in hiring security professionals contributed to a growing awareness that they were unequipped to detect, contain, and remediate against threats. Previous installs of SIEM tools were unable to provide visibility into the security events and were difficult to leverage. The data generated from these SIEMs provided too little context to act upon and necessitated that organizations throw people resources at cases for hours, if not days. Worse yet, there was the possibility of threats slipping through without detection. We attribute the ineffectiveness of the prior solutions to the following:

> "With three people on our SecOps team trying to monitor 11,000 endpoints, it was a huge challenge; we couldn't achieve any visibility. Now with Rapid7, we are able to do it, and it has reduced the amount of work involved in incident attribution by a large margin."
>
> *Director of infosec, retail group*

- **Legacy SIEMs and logging tools produce a lot of data, often in a non-correlated fashion without context.** Without correlation and context, SecOps spend extraneous effort tracking and verifying root cause of incidents. Basic timestamp and IP evidence was insufficient, as it required SecOps to investigate into logs without directional guidance. Security professionals need quick and insightful data so they can contain and remediate before threats dwell. One interviewee we spoke to cited that they realistically needed an entire team of 10 FTEs to truly leverage its previous SIEM.

- **Some legacy solutions fell short in providing adequate user and entity behavioral analysis.** Holistic views of security events, that include UEBA, help security professionals deterministically identify threats through user account behavior. On some legacy solutions, this crucial security layer was not an available feature.

> "On our old SIEM, we couldn't write queries fast enough to go through and actually make any use of the data that existed. Whereas Rapid7 is more tailored to a small team and gives me a lot of out-of-the-box capability that I could build upon so I don't have to start from scratch."
>
> *Information security manager, consumer goods*

- **Security threats move laterally within the network. Without proper discovery and containment on the first pass, threats may not be discovered until damage is done.** People at resource-constrained organizations are forced to prioritize security investigations, i.e., they aren't able to fully commit their focus onto all incidents, some threats are passed over. For these organizations, the choice comes down to either heavily invest in people, capital, heavy technology, etc., or to face likely security breaches.

Key Results

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

- **Holistic and actionable visibility enabled SecOps to act quickly with high confidence.** One infrastructure security analyst stated, "I'm getting alerts on things I care about, rather than investigating false positives."

  Another security architect said: "We're a small team so anytime a tool can offload tasks from my analysts' plate is a good thing. I can now have my analysts focus on priority issues now — 15 to 20 very high confidence alerts a day, instead of 300."

  Another interviewee regarding the level of granularity InsightIDR can reach stated: "Rapid7 isn't solely just a SIEM to us; it lets us go do deeper dives into investigations by pulling pinpointed logs directly off of boxes. I can also watch process and activities on an individual asset. Put the two together and we can have an accurate read fairly quickly."

- **The time to containment or remediation greatly improved with InsightIDR, significantly lowering risk profiles of organizations.** With greater visibility and contextual information, SecOps is able to pass remedial instructions to an IT responder or execute directly and avoid becoming a bottleneck at the investigation step. One interviewee cited: "We're able to take the information and take actions. It gives us actionable intelligence into the environment and [allows us to] pass it to someone to execute on that. We've been able to reduce the remediation time probably tenfold."

  Another interviewee added: "Rapid7 is at least twice as fast [as our previous solution], maybe even faster to correlate. Before, we didn't have the ability to actually understand the problem with any speed; it would have taken weeks."

- **Security operations accomplished more without increasing people resources.** Many organizations described the Rapid7 solution as extremely suitable for teams with constrained resources. The infrastructure security analyst at an industrial supplies organization said:

  "Where we really succeeded with the tool is that we've been able to make it work to produce the level of visibility with just me as the security guy here. I'm now able to distill down 18 million alerts and prioritize who handles what."

- **Increased usage due to ease of use.** "To be completely honest with you, I think we as a security team have significantly increased our efficiency because of the InsightIDR intuitiveness vs our previous solution. InsightIDR has become our go-to primary tool for the security team and where [the previous solution] was the very last tool we used."

> "Rapid7 is at least twice as fast [as our previous solution], maybe even faster to correlate. Before, we didn't have the ability to actually understand the problem with any speed; it would have taken weeks."
>
> *Senior security professional, industrial supplies*

> "Who was this? Where were they going? What was our user doing at the time? All the contextual questions are there in Rapid7 — you have it all."
>
> *Security engineer, retail group*

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. This a large North American enterprise that has been making steady progress to migrate services and infrastructure to the cloud. To keep pace with organizational growth, the organization intends to increase spend on IT security especially as it requires PCI-DSS and SOX compliance and is aware of the growing prevalence of corporate breaches. While the organization has a dedicated security operations team and a complementary assortment of security technology, the team has not been able to adequately respond to security incidents. Additional characteristics are as follows:

- It has three SecOps FTEs, which serve as the first line of defense. A large portion of remedial tasks are then passed onto the IT incident responders. Hiring additional SecOps FTEs has been a challenge, given the demand for these professionals.
- It has a legacy on-premises SIEM and logging software, but its ability to sort through data and identify incidents is limited, especially given the size of its SecOps team.
- It is currently due for a hardware refresh cycle for the SIEM, with a three-year cycle similar to other infrastructure assets.
- It has multiple office locations, which complicates many types of security upgrades — something that is cloud-based would be preferred.

Prior to selecting Rapid7 InsightIDR, the organization questioned whether the number of incidents were actually higher than what had been detected. Because detection and queries were extremely slow, lingering threats could already be spreading laterally across its network. The organization considered implementing a fully managed detection and response (MDR) solution, greatly increasing hiring, or replacing its SIEM — the Rapid7 SIEM solution was selected as being the most cost-effective and scalable solution.

✓

Key assumptions:

- 5,000 IT assets
- 8,000 employees
- Three SecOps FTEs
- Prior state: Legacy on-premises SIEM

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	Improvements in response efficiency	$461,214	$485,784	$541,242	$1,488,240	$1,227,403
Btr	Quicker time-to-value delivery from InsightIDR	$563,112	$93,852	$93,852	$750,816	$659,996
Ctr	Avoidance in hardware and software refreshes and purchases	$294,400	$184,000	$184,000	$662,400	$557,944
	Total benefits (risk-adjusted)	$1,318,726	$763,636	$819,094	$2,901,456	$2,445,343

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 more than $2.4 million.

Improvements In Response Efficiency

Forrester observed that many of the interviewed organizations' existing SIEM solutions produced alerts, data, and visibility, but these functionalities were only of limited use. A level of security maturity was evident at these organizations, but often their ability to respond was hampered by three main factors on the legacy tools:

- Visibility was available, but without sufficient correlation and context SecOps professionals had to invest significant time into digesting the data. And as a result, they were unable to do meaningful investigations. When investigations were carried through, triage was a protracted process.
- Due to the lack of clarity on incidents, the SecOps team was unable to forward remedial actions to the broader IT and incident response team.
- Legacy SIEMs required entire teams to be dedicated to monitoring. With security professionals being both difficult and expensive to hire, the organizations could not spare sufficient people resources to the task.

Prior to using InsightIDR, delayed response times were common for organizations. False alerts and superfluous amounts of log data also contributed to an increased workload for SecOps teams. Following the investment in InsightIDR, these organizations found that they were able to achieve more with just a few security professionals. This is attributable to the contextual visibility and user behavior analytics that reduced both the MTTK by as much as 50% and the total incident management time by up to 40%.

For the composite organization, we assume that:

- SecOps personnel spent 40% of their time on detection and incident management activities when using the legacy SIEM.
- A limited base of IT and incident response FTEs spent 50% of their time on response and remediation when using the legacy SIEM.
- False positives decreased by 27%, removing these incidents from the investigation pool.
- All remaining cases and incidents required 38% less time to manage, benefiting both SecOps and IT responder groups.

Incident management effort reduction: **38%**

False positives are reduced by **27%** using InsightIDR

Cumulatively, the composite organization is able to recoup over $500K annually in time spent on incident management, freeing individuals to perform value-add activities such as threat hunting. Net returns to the organization over a three-year period are $1.3 million, PV. Forrester recognizes that some organizations may employ or have decreased utilization of incident responders. In accounting for this possible variance, we have adjusted the three-year benefit downward to a risk-adjusted PV of $1,227,403.

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.

Improvements In Response Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Security operations FTE involved in detection		3	3	4
A2	IT operations involved in incident response and remediation		15	16	17
A3	Percentage of time expended on detection and SIEM activities - SecOps		40%	40%	40%
A4	Percentage of time expended on response – IR team		50%	50%	50%
A5	Reduction in time expended on incident management, as a percentage		38%	38%	38%
A6	False positive reduction impact on detection and response teams, as a percentage		27%	27%	27%
A7	SecOps FTE annual salary, on average fully loaded	$110K*1.2X benefits multiplier	$132,000	$132,000	$132,000
A8	ITOps FTE annual salary, on average fully loaded	$70K*1.2X benefits multiplier	$84,000	$84,000	$84,000
At	Improvements in response efficiency	((A1*A3*(A5+A6))*A7)+ ((A2*A4*(A5+A6))*A8)	$512,460	$539,760	$601,380
	Risk adjustment	↓10%			
Atr	Improvements in response efficiency (risk-adjusted)		$461,214	$485,784	$541,242

Quicker Time-To-Value Delivery From InsightIDR

Interviewed organizations emphasized a great importance in being able to quickly realize value from their SIEM solution. Our findings revealed that when these organizations implemented their previous solutions, or investigated some other solutions available on the market, the complexity and on-premises nature of these alternatives led to long protracted deployments and extended time to baseline. In order to derive meaningful value from other solutions, these organizations had to apply more resources over a longer implementation period, often between six months and one year. Whereas with Rapid7, these same organizations were able to find value within two months of the solution's deployment.

An infrastructure security analyst from a consumer goods company stated the following on their experience with the implementation:

"You can have this up in less than two weeks. I mean the cloud interface is really nice, really simple. The query language that you use to write custom alerts is very straightforward, easy to pick up. Overall, I think you can be pretty well-tuned in two months."

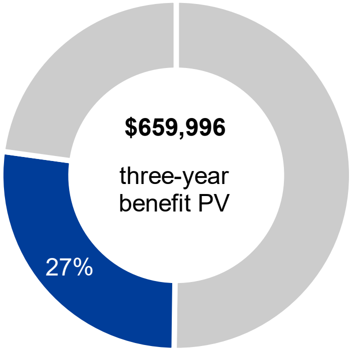
Some observations made are:

- Deployment times typically took two weeks.
- Proper baselining took an additional month on average.
- SecOps personnel required three times less overall training to become proficient with InsightIDR, as compared to other solutions.
- Fine-tuning following the deployment stage is an ongoing refinement process and generally a constant between the various solutions.
- Due to the complexities of some alternate solutions, organizations reported that they were not able to digest and leverage the data that the alternative SIEMs generated, even after eight months following deployment.

For this study, we've taken these findings and applied the following to the composite organization:

- Fewer SecOps personnel were needed to learn and become proficient in SIEM monitoring on InsightIDR.
- A total period of 1.5 months were required to reach a steady state on InsightIDR, as compared to the seven months needed for a legacy SIEM. This is a 79% reduction in time to be operationally ready.
- Determined for labor savings that the delta in *time to achieve steady state* multiplied by the labor rate of $63.46 per hour on an annual rate of $132,000 (fully loaded).
- An assumption of FTE turnover and retraining adds incremental time-to-value savings in Years 2 and 3.

The accelerated basis of deployment and rollout of the platform equates to a present value of $733,329 over a three-year period. We also expect that there can be some variability in the degree of baselining and tuning required between different organizations. As such, we have risk-adjusted the value of this benefit downward by 10%, resulting in a final three-year PV of $659,996.



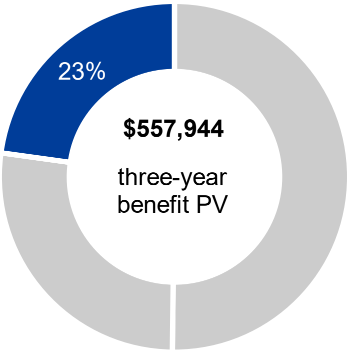
Quicker time-to-value delivery from InsightIDR: 27% of total benefits

- **Two weeks** to deploy and baseline
- One month to achieve steady state
- Achieves value **79%** faster than legacy SIEMs

Quicker Time-To-Value Delivery From InsightIDR: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	SecOps involved in InsightIDR SIEM activities	A1*A3	1.2	0.2	0.2
B2	Additional SecOps necessary with alternate competitive SIEM solution	B1*4	4.8	0.8	0.8
B3	Time to deploy with InsightIDR, in months		0.5	0.5	0.5
B4	Additional time to reach high efficiency with InsightIDR, in months		1	1	1
B5	Months to deploy and reach high efficiency with competitive SIEM		7	7	7
B6	Reduction in time to deploy and run at steady state with alternative SIEM		79%	79%	79%
B7	Cost of SecOps FTE annually, on average fully loaded		$132,000	$132,000	$132,000
Bt	Quicker time-to-value delivery from InsightIDR	(B1+B2)*B6*B7	$625,680	$104,280	$104,280
	Risk adjustment	↓10%			
Btr	Quicker time-to-value delivery from InsightIDR (risk-adjusted)		$563,112	$93,852	$93,852

Avoidance In Hardware And Software Refreshes And Purchases



Avoidance in hardware and software refreshes and purchases: 23% of total benefits

Many of the interviewed organizations stated that their IT strategy was to shift their infrastructure footprint to the cloud, where costs are more predictable and scalability is not an issue. In the past, many of these organizations had implemented on-premises SIEM tools, but these implementations were difficult to maintain, difficult to integrate with newer cloud-based applications, and not updated with regularity. Compounding these issues, the parabolic growth in data storage and processing required that infrastructure be refreshed so that the SIEMs could collect and effectively analyze the data.

In transitioning to Rapid7, the organizations saved in the following hardware and software areas:

- Hardware refreshes on the infrastructure, typically once every three years.
- Software licenses, including that of upgrades.
- Support plans and indirect maintenance costs, with some customers listing their costs as high as 20% when labor costs are included.

For the composite organization, we assume that:

- Major hardware refreshes amounting to $120K once every three years can be avoided by moving to the cloud-based InsightIDR.
- Software licenses cost $200K per year, based on the cost of an alternative SIEM.
- A 15% maintenance charge on the total cost of hardware and software.

In aggregate, the composite organization avoids $697,431 over a three-year period. Understanding that there are some solutions that may have a lower cost, at the expense of capability, we've risk-adjusted the benefit down by 20%, for a total PV of $557,944.

Avoidance In Hardware And Software Refreshes And Purchases: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Cost of hardware refresh		$120,000	-	-
C2	Legacy software costs		$200,000	$200,000	$200,000
C3	Ongoing support contract costs of legacy hardware and software	15% of legacy hardware + software	15%	15%	15%
Ct	Avoidance in hardware and software refreshes and purchases	(C1+C2)+((C1+C2)*C3)	$368,000	$230,000	$230,000
	Risk adjustment	↓20%			
Ctr	Avoidance in hardware and software refreshes and purchases (risk-adjusted)		$294,400	$184,000	$184,000

Unquantified Benefits

Forrester's interviews with Rapid7 customers pointed to an additional benefit that could not be reasonably quantified, due to the variance between the customers and their respective business activities.

- **Audit- and compliance-related activities were much easier to prove with InsightIDR.** Traceability and the presentation of evidence were centralized on the Rapid7 platform, serving as a single pane of glass. For some organizations that are subjected to heavy regulations or partner-required compliance measures, time savings are recognized by both IT professionals and auditors multiple times per year. For one organization, their supply chain mandated certain controls to maintain certain portions of their business relationship, making InsightIDR a crucial part of proving compliance.

  An information security manager expressed to us its experience with presenting compliance information from InsightIDR: "We were able to meet all of the compliance requirements from a solution perspective through our IDR reports. It delivered on what we needed and it certainly made us look better in terms of our level of sophistication because it is simply a better solution. We have far more information than we've ever had before. We certainly don't need to jump through hoops like before to collect the information."

- **Avoidance of security tool purchases beyond SIEM technology are possible after implementing InsightIDR.** Multiple functions of InsightIDR can replace alternative tools, especially in an environment where people resources are constrained. Log aggregation, deception detection, and newly released network traffic analysis are components that are all pieces which can supplement existing services or hardware, leading to additional savings of averted purchases in the security segment. Traditionally, the task of aggregating logs and deciphering key information in itself has been a monumental task for security professionals.

Flexibility

The value of flexibility is 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 InsightIDR and later realize additional uses and business opportunities, including:

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.

- **The Rapid7 single agent system applies to InsightVM as a single orchestrator to InsightConnect, enabling organizations to further add capabilities in the future without increasing resource overhead.** Interviewees stated that while InsightIDR carried its own benefits, they also considered future build-out capabilities of the platform. Specifically, with the platform residing in the cloud and using a single agent across vulnerability management and SIEM, scaling capabilities and improving security automation would be an easier effort with fewer infrastructure changes.

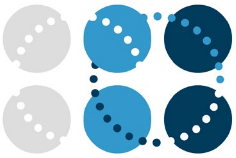
  An infosec manager stated to us that:

  “We’re leveraging some SOAR functionality, specifically within our email environment. One of the reasons that we chose IDR was because it was cloud-hosted and scalable. We knew about the InsightConnect platform and while it was on our radar, we knew we weren’t quite ready at that time — that left the door open though. Now that we are at the point of wanting to leverage more automation and orchestration so that we can be more efficient as a team, the Insight platform ability to integrate easily really allows us continue to grow, scale, and really give us a lot more capabilities.”

- **Beyond upgradability and scalability, interviewees also cite the responsiveness and speed at which Rapid7 incorporates new functionality and enhancements on a regular basis.** Being nimble and responsive to the needs of the modern customer, Rapid7 is described by its customers to be transparent on its roadmap and quick to fulfill customer-desired functions. Updates and functional features are rolled out seamlessly on the cloud platform.

  An infosec manager said:

  “We had a wish list of enhancement requests with Rapid7, and I would say to date, everything that was on our list has come to fruition as part of either a request that we have directly made, or because it was already part of their roadmap and was something they were actively working on.”



Rapid7’s cloud platform is constantly improved with new features in response to customer feedback and asks — without the need for customers to manually perform upgrades.

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	Cost of licenses	$149,250	$0	$156,713	$164,548	$470,511	$402,392
Etr	Internal testing and tuning costs	$40,646	$0	$3,465	$3,465	$47,576	$46,113
	Total costs (risk-adjusted)	$189,896	$0	$160,177	$168,013	$518,087	$448,505

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 approximately $449K.

Cost Of Licenses

Customers of Rapid7 pay for InsightIDR licenses in terms of assets under coverage and pricing could possibly be negotiated if additional protection mechanisms are bundled. However, for the purposes of this study, we assume that pricing is based on list pricing, without any bundling incorporated. The interviewed customers saw the cloud-based Rapid7 solution as an affordable and very predictable cost, even as they expanded their network and physical footprint.

Over the course of three years, the composite organization grows 5% year over year in IT assets, resulting in small increases in overall license costs. Through the three-year period, the full license and support cost of the InsightIDR solution is $402,392, PV.

Licensing and support costs are wrapped into a simple line item that is determined by the number of IT assets under coverage.

Cost Of Licenses: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Number of assets under coverage, inclusive of VMs and cloud		5,000	-	5,250	5,513
D2	InsightIDR license cost per asset		$29.85	$29.85	$29.85	$29.85
Dt	Cost of licenses	D1*D2	$149,250	$0	$156,713	$164,548
	Risk adjustment	0%				
Dtr	Cost of licenses (risk-adjusted)		$149,250	$0	$156,713	$164,548

Internal Testing And Tuning Costs

Most interviewed customers noted that the initial deployment of agents and the cloud solution took a small amount of time, often within the frame of one week. Following the initial implementation, the organizations applied effort to test and tune the security posture so that alerts would be meaningful based on their security tolerances. For the composite organization, the following factors were included in our analysis:

- Ninety (90) hours of SecOps effort are required to implement and test InsightIDR across an enterprise of 5,000 IT assets.

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.

- Tuning and refinement of the detection and alerting will be an ongoing effort, but to reach a state of normal operation will take approximately 520 hours.
- Incremental hours are spent on tuning in Years 2 and 3 to maintain alignment on the detection and alerting with security policies.

The time and effort applied have been intentionally over-estimated in this financial model due to the possibility that some organizations undertake a greater effort on the refinement of their settings to optimize security operations and response management. Effectively, a PV sum of $43,917 in labor costs are incurred for initial testing and tuning of InsightIDR.

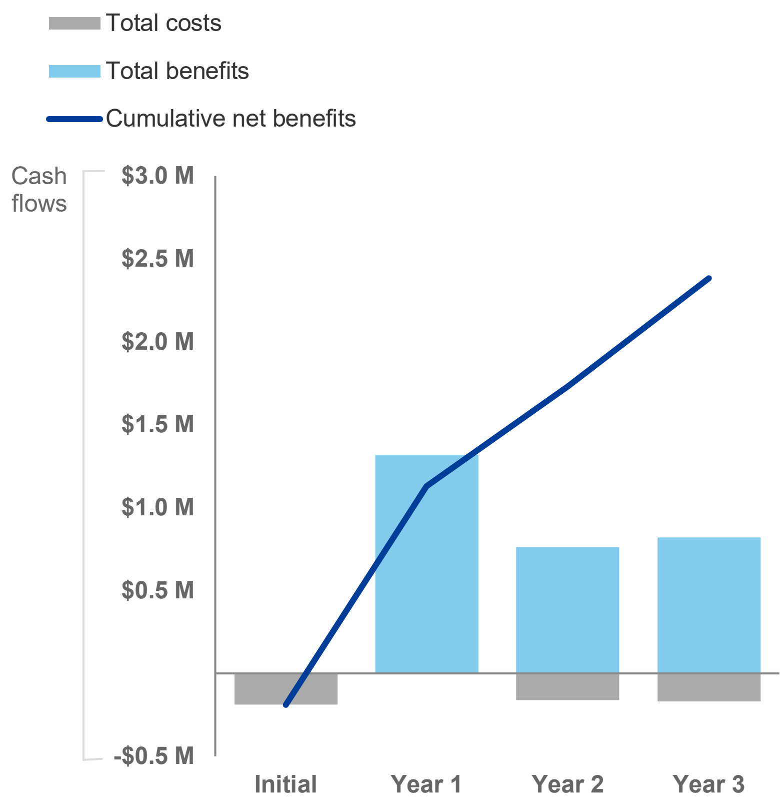
Internal Testing And Tuning Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Internal SecOps hourly rate	$110K*1.2X benefits modifier/2,080 hours	$63.46	$63.46	$63.46	$63.46
E2	Hours required for testing and initial deployment		90	-	-	-
E3	Hours required for tuning and refinement of detection functions		520	-	52	52
Et	Internal testing and tuning costs	E1*(E2+E3)	$38,711	$0	$3,300	$3,300
	Risk adjustment	↑5%				
Etr	Internal testing and tuning costs (risk-adjusted)		$40,646	$0	$3,465	$3,465

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)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($189,896)	$0	($160,177)	($168,013)	($518,087)	($448,505)
Total benefits	$0	$1,318,726	$763,636	$819,094	$2,901,456	$2,445,343
Net benefits	($189,896)	$1,318,726	$603,459	$651,081	$2,383,369	$1,996,838
ROI						445%
Payback period						< 3 months

Rapid7 InsightIDR: Overview

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

Rapid7 provides a complete approach to threat detection and response. InsightIDR — Rapid7's cloud SIEM — provides a balance of technology and service expertise to enable security leaders to cut through clutter and complexity, protect their organizations, and build a foundation for success.

Accelerate Detection and Response with Accessible Expertise

Whether you integrate and manage our agile SIEM, or leverage the full force of our elite MDR team, you'll have access to and insights from the experts and research driving the industry forward. This includes a robust library of out-of-the box detections curated from our global managed SOC team, plus insights from Rapid7's global threat intelligence network.

Realize Faster Time to Value with Natively Cloud Infrastructure

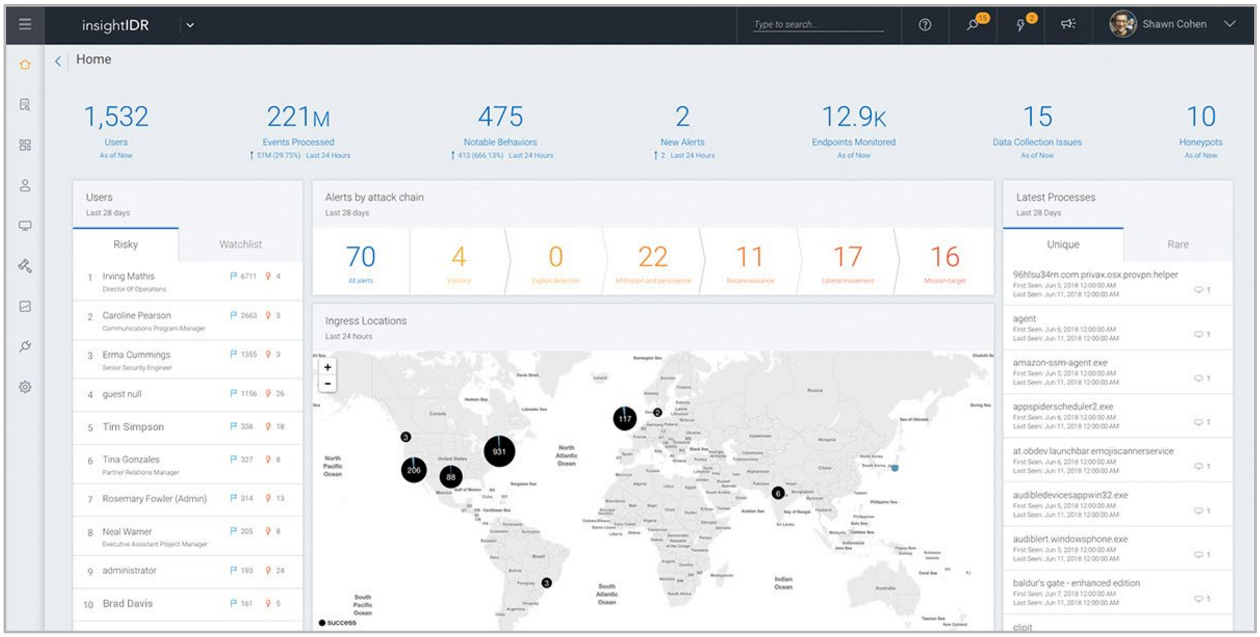
With its cloud infrastructure and intuitive software-as-a-solution interface, InsightIDR is built to help you get up and running quicker than ever, while continuously up-leveling your capabilities. By eliminating the deployment, management, hardware maintenance, and upgrade processes that bog teams down, analysts can focus their energy on what matters most and collaborate more easily across their team.

Eliminate Blind Spots with Coverage Across Modern Environments

InsightIDR collects, aggregates, analyzes, and correlates data across diverse sources to provide actionable insights that teams can feel confident taking action on. Prescriptive collection guides and built-in analysis enable teams to quickly get meaningful insights across logs, UEBA, endpoint, cloud, and network data.

Unlock the Focus and Efficiency Needed for Successful Security

Our detection and response mission is anchored in eliminating complexity and giving teams the information and tools they need to focus on the most critical threats. With deep correlations and attribution, visual investigation timelines, and in-product automation and enrichment, teams can measurably accelerate their response.



1,532 Users As of Now

221M Events Processed ↑ 51M (29.75%) Last 24 Hours

475 Notable Behaviors ↑ 413 (666.13%) Last 24 Hours

2 New Alerts ↑ 2 Last 24 Hours

12.9K Endpoints Monitored As of Now

15 Data Collection Issues As of Now

10 Honeypots As of Now

Users
Last 28 days

1	Irving Mathis Director Of Operations	6711	4
2	Caroline Pearson Communications Program Manager	2663	3
3	Erma Cummings Senior Security Engineer	1355	3
4	guest null	1156	26
5	Tim Simpson	338	18
6	Tina Gonzales Partner Relations Manager	327	8
7	Rosemary Fowler (Admin)	314	13
8	Neal Warner Executive Assistant Project Manager	205	8
9	administrator	193	24
10	Brad Davis	161	5

Alerts by attack chain
Last 28 days

All alerts	Visibility	Exploit detection	Infiltration and persistence	Reconnaissance	Lateral movement	Mission target
70	4	0	22	11	17	16

Ingress Locations
Last 24 hours

Latest Processes
Last 28 Days

96hlsu34rn.com.privax.osx.provpn.helper
First Seen: Jun 5, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

agent
First Seen: Jun 6, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

amazon-ssm-agent.exe
First Seen: Jun 5, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

appspiderscheduler2.exe
First Seen: Jun 6, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

at.obdev.launchbar.emojiscannerservice
First Seen: Jun 6, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

audibledevicesappwin32.exe
First Seen: Jun 5, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

audiblert.windowsphone.exe
First Seen: Jun 5, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

baldur's gate - enhanced edition
First Seen: Jun 7, 2018 12:00:00 AM
Last Seen: Jun 11, 2018 12:00:00 AM
1

clipit

InsightIDR's flexible, intelligence-infused approach helps you make the most of your resources, so you'll always know you're covered and know what to do next.

Learn more at rapid7.com/insightidr

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.