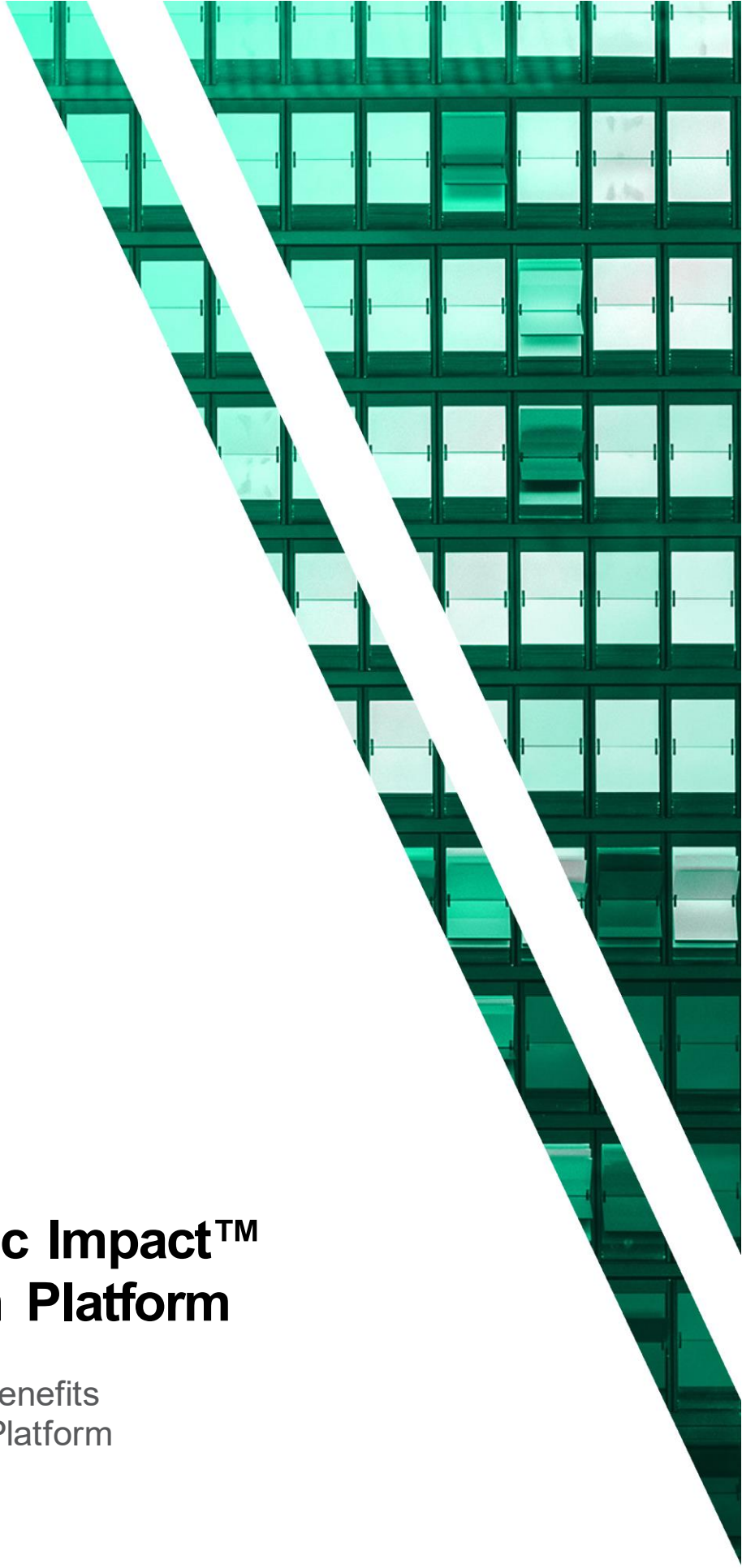
FORRESTER®



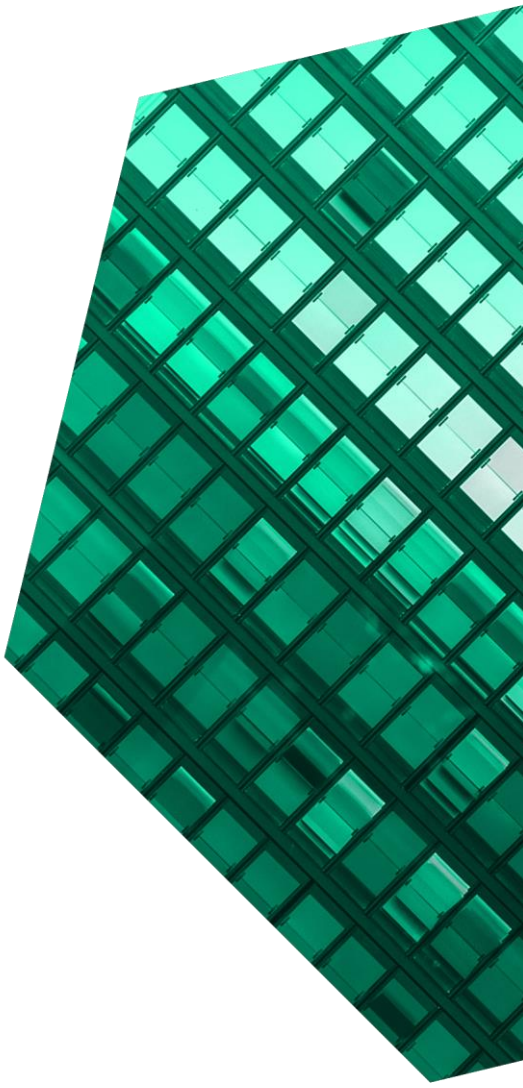
The Total Economic Impact™ Of The LogRhythm Platform

Cost Savings And Business Benefits Enabled By The LogRhythm Platform

JUNE 2021

Table Of Contents

Consultant: Mary Anne North



Executive Summary

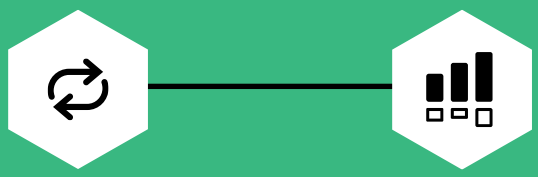
The LogRhythm Platform enables organizations to decrease the number of security alerts and false positives, detect security threats that otherwise might have been missed, prioritize investigation among true positives, and investigate and resolve incidents faster. Quicker resolution shortens the time that an organization is exposed to a threat and reduces the risk of a security breach.

The LogRhythm Platform is a security information and event management (SIEM) solution that provides a single integrated platform for rapid detection, response, and neutralization of security threats. It improves organizations' visibility of threats, provides insights needed to make better decisions about those threats, and accelerates and reduces the effort needed for threat investigation and response. The platform can be deployed in the cloud, on-premises, or in a hybrid environment.

LogRhythm commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the LogRhythm Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the LogRhythm Platform on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers utilizing LogRhythm deployed in the cloud or on-premises. Calculations used in this study were based on the customers' own experiences with LogRhythm, including the stated benefits and costs articulated in the interviews. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization. The calculations of benefits and costs are from the perspective of that composite organization. Forrester also used outside industry metrics, such as those from Ponemon, for salaries and data breach costs in the calculations. For more details on Forrester's methodology, see Appendix A.

KEY STATISTICS



Return on investment (ROI)
258%

Net present value (NPV)
$2.24M

Prior to deploying LogRhythm, the interviewees' organizations used an entirely manual approach to monitor security alerts, address security incidents, and manage incident cases. These limitations resulted in lack of visibility to the full security picture and prolonged the mean time to detect (MTTD) and mean time to respond (MTTR). This increased the risk of a security breach and made it difficult to prioritize investigation and resolution of security incidents and comply with security standards.

After investing in LogRhythm, the organizations not only reduced analyst effort per incident but also prioritized their highest risk threats for response.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits applied to the composite organization and totaled over three years include:

- **Improved ability to prioritize investigation and resolution, valued at $816,827.** With LogRhythm, the composite organization reduces its overall number of alerts, decreases the percentage of those alerts that are false positives, and cuts the amount of time an analyst requires to deem an alert either true positive or false positive. In addition, the platform categorizes and prioritizes alerts and calculates a risk score for each alert. These changes collectively save many hours of security analyst effort each year and greatly improves the SOC team's ability to prioritize alerts for investigation and resolution.

Reduction in investigation and resolution time

90%

- **Faster investigation and resolution, valued at more than $1.7 million.** The composite organization reduces its average time to investigate and resolve a true positive incident by 90%. The greatest time savings are seen with asset lookup and manual enrichment. Analysts can quickly identify affected assets and no longer have to manually pull activity data from multiple sources. Correlation across sources and time indicates where to troubleshoot. Automation of parts of the investigation and resolution, along with case management capabilities, further decreases analyst effort.
- **Reduced risk of security breach, valued at $504,447.** Deploying LogRhythm enabled interviewees' organizations to investigate and resolve security incidents faster, therefore reducing the risk of a security breach. That reduction in analyst time (and also elapsed time) to investigate and resolve an incident shortened the time that an organization was exposed to a threat.

> **"We have more evidence to look at, faster, to determine if it's a false positive. And we have a place to tune out those false positives, so they don't happen again."**
>
> *Cybersecurity engineer, media company*

- **Decreased staffing costs of $63,760.** Over time, the composite organization includes less senior (and less expensive) security analysts on its SOC team because it can provide security analysts with detailed playbooks and other guidance, and also automate certain efforts. Instead of relying on what was in each analyst's memory about incident response, the composite organization captures and codifies that expertise in the platform and augments it with industry content from LogRhythm Labs. That content includes out-of-the-box templates and preconfigured blueprints for investigation and response constructed for different compliance mandates.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Maturing an organization's security operations and freeing up analyst time for more strategic needs.** Interviewees saw deploying and then optimizing their organizations' use of LogRhythm as an important part of maturing their security operations. With less time needed to investigate and resolve an incident — and some of that effort shifted to more junior

analysts — organizations' senior analysts had more time for threat hunting, adding new use cases, and tracking trends.

- **Detecting threats that may have been overlooked otherwise and reducing MTTD and dwell time.** LogRhythm enabled organizations to aggregate and correlate alerts and log sources that previously had been reviewed in isolation. It revealed the full scope of an attack instead of leaving an analyst to piece together disparate parts. This helped organizations detect threats that otherwise may have been overlooked and reduce their MTTD and dwell time.
- **Improved ability to comply with regulatory standards.** LogRhythm helped organizations comply with regulatory standards more easily and then meet an audit's compliance requirements by monitoring and reporting on their adherence to those standards.
- **Flexible pricing model and scalability.** The LogRhythm pricing model allowed organizations to readily accommodate acquisitions and organic growth by leveraging existing use cases, adding more log sources, and increasing the level of messages per second (MPS) covered by their LogRhythm subscription fees.
- **Additional analyst productivity improvement via more consistent and/or automated incident response and simplified collaboration and incident management.** In addition to decreasing the average time an analyst needed to investigate and resolve a security incident, LogRhythm improved analyst productivity by increasing the consistency of incident response, fully automating the response to certain incidents, and reducing the time analysts spent managing the incident and collaborating with others.
- **Ease of implementation and use.** Organizations valued LogRhythm's straightforward implementation process and user experience.
- **Improved access to and cost of cybersecurity insurance.** Organizations mentioned that the ability to show proof of using an established SIEM, such as LogRhythm, helped them access cybersecurity insurance and do so at a lower cost.
- **Security becoming a brand enabler.** The organizations' use of LogRhythm enabled them to attract and retain incremental revenue by building confidence in customers and prospects that their data would be protected.
- **Better security analyst experience and retention.** By contributing to an environment of growth and innovation, LogRhythm helped improve analyst morale and retention.

Costs. Risk-adjusted PV costs applied to the composite organization and totaled over three years include:

- **LogRhythm fees of $710,355.** LogRhythm subscription or license fees vary depending on the MPS ingested by the platform and include a standard level of support. LogRhythm provides implementation assistance and training for the composite organization at one-time costs of $15,000 and $5,000, respectively.
- **Internal labor of $159,209 for implementation, management, and support.** Initial internal labor costs for the composite organization include 30 hours of security engineer time for technical implementation of cloud-based LogRhythm and 24 hours of training per person for that engineer and four security analysts. Ongoing costs include training for an additional analyst in Year 2 and 130 hours of security engineer time annually to manage the platform and support end users. In addition, the analysts spend 20% of their time during the first six months and 5% of their

ongoing time on baselining the organization's security operations.

The customer interviews and financial analysis found that a composite organization experiences benefits of $3.11M over three years versus costs of nearly $870K, adding up to a net present value (NPV) of $2.24M and an ROI of 258%.

We can get to more incidents and make our response smarter.

— IS security director, healthcare

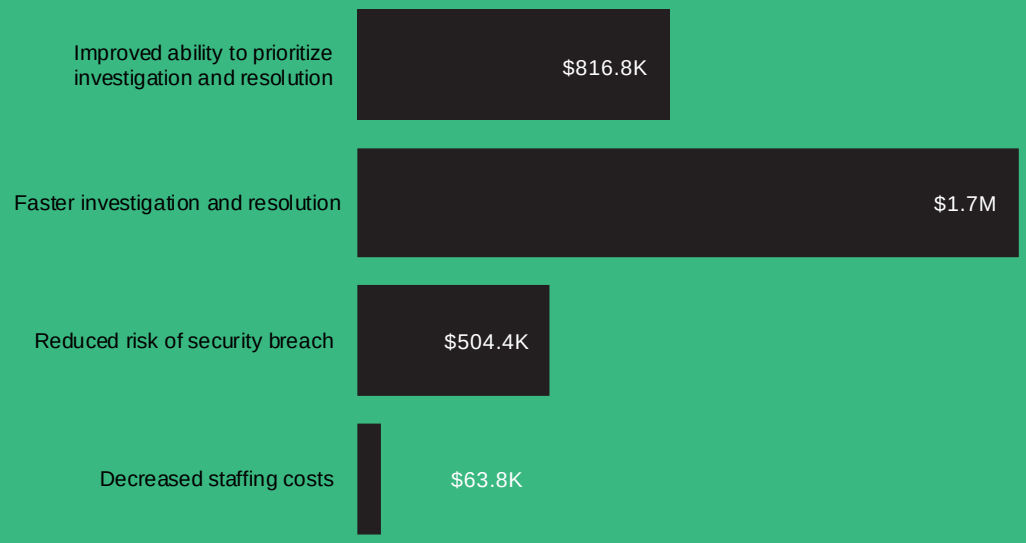
ROI
258%

BENEFITS PV
$3.11M

NPV
$2.24M

PAYBACK
<6 months

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

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

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 the LogRhythm Platform can have on an organization.

DUE DILIGENCE

Interviewed LogRhythm stakeholders and Forrester analysts to gather data relative to the LogRhythm Platform.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using the LogRhythm Platform 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 the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The LogRhythm Platform Customer Journey

Drivers leading to the LogRhythm Platform investment

Interviewed Organizations			
Industry	**Region**	**Interviewee**	**Revenue**
Healthcare	North America	IS security director	$8.6 billion
Media	Global	Cybersecurity engineer	$2 billion
Real estate	Asia Pacific	IT compliance manager	$100 million
Healthcare	North America	VP, information security	$2 billion

KEY CHALLENGES

Before investing in LogRhythm, the interviewees' organizations monitored security alerts and addressed security incidents with a manual approach. The analysts in their security operations center (SOC) had to log into individual security tools or try to make sense of email notifications, with no SIEM or any other correlation solution to help. Case management was equally manual, typically consisting of a shared document that listed incidents with no tools for managing an incident and working collaboratively if needed.

> **"We had no SIEM and no correlation solution. We had to log into individual security tools to check this here and check that there."**
>
> *Cybersecurity engineer, media*

Interviewees described a range of challenges that prompted their organizations to deploy LogRhythm, including:

- **Lack of visibility to the full security picture.** Interviewees cited challenges around ingesting many different log sources and easily aggregating and correlating various risk items to gain better and more complete visibility to emerging security threats and trends across the organization. The IT compliance manager for a real estate company explained: "We couldn't put the pieces together to get the full picture. We needed to improve the quality and scope of our rules for aggregation and correlation, across time and across sources."
- **Prolonged MTTD and MTTR.** The lack of visibility, inability to aggregate and correlate risk items from multiple sources, and absence of both a uniform process for handling incidents and a case management tool all combined to prolong the organizations' MTTD and MTTR.

  Longer MTTD increased the dwell time for threats and thus increased the risk and potential harm of a security incident. As the cybersecurity engineer at a media company explained: "A threat could have been there for an hour, or it could have been there for three weeks. Unless an analyst logged into something and happened to see an alarm there, who knew?"

  The amount of analyst time needed to investigate and resolve each security incident once it was detected further increased the risk of damage

and limited the number of incidents each security analyst could address.

"Reducing the time to detect and respond to a security incident, in order to reduce the damage, was our top challenge. During an incident, time is of the essence. Many bad things can happen, and you can't go back in time after the damage is done."

VP information security, healthcare

- **Inability to prioritize investigation and resolution.** The interviewees' organizations were unable to focus on critical threats because they were overwhelmed with alerts and could not discern among them. They experienced a high rate of false positive alerts, estimated by interviewees to range from "most" to "probably 99%." Their security analysts spent considerable time determining whether incoming alerts were true positives that needed to be resolved or false positives that could be safely ignored.

  This could involve logging into multiple security tools and also multiple individual systems that had been impacted. A VP of information security at a healthcare company observed: "It could take 24 to 48 hours to determine what's going on and if something is even a problem."

  The interviewees' organizations also experienced numerous other alerts that, although valid, did not necessarily warrant action or could be addressed with an automated response. However, the organizations lacked the ability to distinguish among alerts on these factors.

  The organizations' resulting attempts to address every incoming alert, with no ability to prioritize those efforts, created alert fatigue and burdened the security analysts. That left the organizations at risk of a slow response — or no response — to their high-risk alerts. The IS director at a healthcare company explained: "I can't tell you the number of times that our email inboxes blew up. We didn't know if there were any threats out there because we'd have a thousand emails with no way to get through them all."

"We knew we were missing things. Because our security analysts were overwhelmed with false positives, they wouldn't get to the true positives."

IS security director, healthcare

- **Difficulty becoming and remaining compliant with security standards.** The organizations struggled to attain, maintain, and indicate continuous compliance with regulatory standards around information security, or even to understand what compliance required. Depending on an organization's location and industry, those standards ranged from broadly applicable ones like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), General Data Protection Regulation (GDPR), Personally Identifiable Information (PII), and Payment Card Industry Data Security Standard (PCI DSS), to industry- or location-specific standards and also international standards.

  The IS security director for a healthcare company said, "We had a big blind spot with our audits." That director described an audit's compliance requirements, such as having a SIEM, indicating what logs are monitored, and providing evidence of appropriate security operations. The director observed, "Our not being able to check that box on an audit compliance list would result in a

higher risk rating score and a red comment on an audit compliance finding."

COMPOSITE ORGANIZATION

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

Description of composite. The composite organization is a $3 billion company in a highly regulated industry. It has around 9,500 employees and operates across the US. Its applications and data are hosted both on-premises and in public or private clouds. Approximately 10,000 endpoints need monitoring. The organization needs to address varied security incidents including suspicious login attempts, unauthorized access, compromised credentials, malware infections on endpoints, brute-force attacks, and phishing emails. It must account to multiple national- and state-level regulatory bodies and adhere to numerous regulatory standards.

Deployment characteristics. The organization deploys the cloud version of LogRhythm, integrating it with its security tools, log sources, and external threat intelligence feeds. Internal staff handle implementation in collaboration with LogRhythm's professional services team. End users receive several days of initial training and coaching and continue to build their skills over the first few months.

The organization uses a wide range of LogRhythm's capabilities, including dashboards, analytics, reporting, AI engine rules, and security incident case management. It leverages diverse LogRhythm Labs content to inform its security operations. As the organization continues to mature its security operations, it integrates additional security tools and adds new use cases and log sources.

Key assumptions

- **$3 billion in revenue**
- **9,500 employees**
- **Highly regulated industry**
- **Data on-premises and in the cloud**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Improved ability to prioritize investigation and resolution	$462,000	$251,513	$251,513	$965,026	$816,827
Btr	Faster investigation and resolution	$670,208	$709,632	$709,632	$2,089,472	$1,728,910
Ctr	Reduced risk of security breach	$195,548	$207,050	$207,050	$609,649	$504,447
Dtr	Decreased staffing costs	$0	$32,640	$48,960	$81,600	$63,760
	Total benefits (risk-adjusted)	$1,327,756	$1,200,835	$1,217,155	$3,745,746	$3,113,944

IMPROVED ABILITY TO PRIORITIZE INVESTIGATION AND RESOLUTION

Evidence and data. After deploying LogRhythm, the interviewees' organizations reduced their overall number of alerts, decreased the percentage of those alerts that were false positives, and cut the amount of time an analyst required to deem an alert either true positive or false positive. The platform also categorized and prioritized alerts and calculated a risk score for each alert. These changes collectively saved many hours of security analyst effort each year and greatly improved the organizations' ability to prioritize alerts for investigation and resolution.

LogRhythm enabled the interviewees' organizations to reduce both their overall number of alerts and the percentage of false positives that their log sources generated. By capturing and consolidating logs and alerts data, adding context to those alerts through integrated scripting and playbooks, processing logs for correlation according to risk, and providing analytical tools, the platform helped the organizations gain a deeper understanding of the nature of their alerts and pinpoint what caused their false positives. They could then adjust the underlying rules set within the platform to tune out certain alerts and generate fewer false positive alerts.

LogRhythm also reduced the amount of time an analyst needed to determine if an incoming alert was a false positive or a true positive, via playbooks, automations, and integrated scripting. The VP of information security for a healthcare company said: "It definitely reduces the time to distinguish false positives. Within minutes, I can run an investigation and validate if something happened that I should be concerned about."

> **"We now have the power to weed out false positives, focus on the alerts we have prioritized, and quickly identify and escalate the important alerts."**
>
> *IS security director, healthcare*

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The annual number of alerts is 10,000 in Year 1, decreasing to 5,000 in Years 2 and 3.
- Prior to the organization's deployment of LogRhythm, 90% of its alerts are false positives.

After LogRhythm, this decreases to 60% in Year 1 and 50% in Years 2 and 3.

- The amount of time a security analyst spends to determine if an incoming alert is a true or false positive drops from 60 minutes prior to use of LogRhythm to 15 minutes in Year 1 and 10 minutes in Years 2 and 3
- Given the repetitive and relatively structured nature of incident response, 100% of the saved time gets recaptured for productive use.

Risks. Risks that may affect an improved ability to prioritize investigation and resolution include:

- Number of security tools and log sources connected to the SIEM.
- An organization's risk tolerance.
- The extent to which an organization tunes its alert criteria, rules, and thresholds.
- The extent to which an organization has leveraged the platform's capabilities and matured its overall security operations.
- Security analyst experience and capabilities.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $816,827.

Improved Ability To Prioritize Investigation And Resolution

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Annual number of alerts	Interviews	10,000	5,000	5,000
A2	Percentage of alerts that were false positives before LogRhythm	Interviews	90%	90%	90%
A3	Time required to determine if alert is true or false positive before LogRhythm (minutes)	Interviews	60	60	60
A4	Analyst time spent on false positives before LogRhythm (hours)	(A1*A2*A3)/60	9,000	4,500	4,500
A5	Percentage of alerts that were false positives after LogRhythm	Interviews	60%	50%	50%
A6	Time required to determine if alert is true or false positive after LogRhythm (minutes)	Interviews	15	10	10
A7	Analyst time spent on false positives after LogRhythm (hours)	(A1*A5*A6)/60	1,500	417	417
A8	Reduction in analyst time spent on false positives (hours)	A4-A7	7,500	4,083	4,083
A9	Security analyst fully burdened compensation, per hour	Assumption: $160,000/2,080	$77	$77	$77
A10	Productivity recapture	Assumption	100%	100%	100%
At	Improved ability to prioritize investigation and resolution	A8*A9*A10	$577,500	$314,391	$314,391
	Risk adjustment	↓20%			
Atr	Improved ability to prioritize investigation and resolution (risk-adjusted)		$462,000	$251,513	$251,513
	Three-year total: $965,026		**Three-year present value: $816,827**		

FASTER INVESTIGATION AND RESOLUTION

Evidence and data. By deploying LogRhythm, the interviewees' organizations reduced their average time to investigate and resolve a true positive incident. Before LogRhythm was deployed, the average time for an analyst to investigate and resolve a true positive incident ranged from 240 minutes to 2,160 minutes. After deployment, the range was 7.5 minutes to 90 minutes. As a percentage for each interviewees' organization, that reduction ranged from 62.5% to 99.7%.

LogRhythm enabled faster investigation and resolution in a number of ways:

- Because data from multiple log sources is aggregated, correlated, and presented in a single dashboard, analysts can run an investigation from a single place and act from within LogRhythm. The IS security director for a healthcare company said: "It takes less time because all the data is right there to look at and act on. You don't have to grab the logs from some other system or log into another system."

> **"Because all of our log sources are in a single place, we're well positioned to respond immediately."**
>
> *VP information security, healthcare*

- Of the steps typically involved with investigating and resolving an incident, the most time was saved on asset lookup and manual enrichment. Analysts could quickly identify affected assets and no longer had to manually pull activity data from endpoints, external networks, VPN logs, DNS records, and network infrastructure.
- Correlation across log sources and across time provided visibility to a threat's origins, apparent targets, and spread, and helped a security team know where to troubleshoot.
- Automation of parts of the investigation and resolution (e.g., via SmartResponses) further decreased analyst effort.
- LogRhythm's case management capabilities made it easier for teams to collaborate on and share information about incident response. They could create, share, and access reports about incidents and incident responses, faster and with less effort.
- In addition to factors that broadly improved security analyst productivity, LogRhythm saved security analysts' time in diverse ways specific to the nature of an incident.
- The difference between the organization's number of alerts and its number of incidents that need to be manually investigated and resolved depends on how many of those alerts either are false positives or can be automatically addressed.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The organization manually investigates and resolves 1,600 incidents each year.
- Prior to the organization's deployment of LogRhythm, each true positive incident requires approximately 480 minutes of analyst time to investigate and resolve (whether by one analyst or several). This decreases to 72 minutes in Year 1 and 48 minutes in Years 2 and 3.
- Given the repetitive and relatively structured nature of incident response, 100% of the saved time is recaptured for productive use.

Risks. Risks that may affect faster investigation and resolution include:

- An organization's prior state for investigation and resolution of security incidents.

- Nature of an organization's security incidents and resulting per-incident analyst time to address.
- Number of incidents.
- Extent to which an organization has automated its responses to certain types of alerts.
- The extent to which an organization has leveraged LogRhythm's capabilities and matured its overall security operations.
- Security analyst experience and capabilities.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1,728,910.

Faster Investigation And Resolution

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Annual number of security incidents that need manual investigation and resolution	Interviews	1,600	1,600	1,600
B2	Analyst time to investigate and resolve an incident before LogRhythm (minutes)	Interviews	480	480	480
B3	Reduction in time needed to investigate and resolve an incident after LogRhythm	Interviews	85%	90%	90%
B4	Analyst time to investigate and resolve an incident after LogRhythm (minutes)	B2*(1-B3)	72	48	48
B5	Annual time savings (hours)	(B1*B2*B3)/60	10,880	11,520	11,520
B6	Security analyst fully burdened compensation (hourly)	Assumption: $160,000/2,080	$77	$77	$77
B7	Productivity recapture	Assumption	100%	100%	100%
Bt	Faster investigation and resolution	B5*B6*B7	$837,760	$887,040	$887,040
	Risk adjustment	↓20%			
Btr	Faster investigation and resolution (risk-adjusted)		$670,208	$709,632	$709,632
	Three-year total: $2,089,472		**Three-year present value: $1,728,910**		

REDUCED RISK OF SECURITY BREACH

Evidence and data. Deploying LogRhythm helped organizations investigate and resolve security incidents faster, reducing their risk of a security breach. That reduction in analyst time and elapsed time to investigate and resolve an incident shortened the time that an organization was exposed to a threat. Reduction in MTTD/dwell time further decreased risk exposure, as did the ability to prioritize incident response based on risk scores.

The VP of information security for a healthcare company indicated that the improved visibility to threats and faster resolution of them helped reduce the damage if an incident did occur, such as files being encrypted due to ransomware, unauthorized configuration changes, or a vulnerability emerging on a system that holds protected health information. That VP also gave the example of a phishing incident where upon detection the security team can run a scan, use file integrity monitoring detail that goes into LogRhythm from two different log sources to determine if files were actually encrypted, and if so, validate whether those files should be rolled back.

> **"Our chance of being compromised has been reduced, and we are more confident that if a malicious attacker did get in, we would detect the activity."**
>
> *IS security director, healthcare*

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The average cost of a data breach is over $3.8 million.[1]
- The likelihood of a 30,000-record data breach in a given year is 7.45%.[2]
- Prior to the organization's deployment of LogRhythm, each true positive incident requires approximately 480 minutes of analyst time to investigate and resolve (whether by one analyst or several). This decreases to 72 minutes in Year 1 (an 85% reduction) and 48 minutes in Years 2 and 3 (a 90% reduction).

> **"The big cost savings is in the ability to respond quickly to the incident and thus minimize damage."**
>
> *VP information security, healthcare*

Risks. Risks that may affect reduced risk of security breach include:

- The prevalence and average cost of security breaches in an organization's industry.
- The extent to which an organization has leveraged LogRhythm's capabilities and matured its overall security operations.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $504,447

Reduced Risk Of Security Breach					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
C1	Analyst time to investigate and resolve an incident before LogRhythm (minutes)	B2	480	480	480
C2	Analyst time to investigate and resolve an incident after LogRhythm (minutes)	B4	72	48	48
C3	Decrease in vulnerability window from using LogRhythm	B3	85%	90%	90%
C4	Average cost of data breach (global)	Ponemon	$3,860,000	$3,860,000	$3,860,000
C5	Likelihood of a 30,000-record breach (within 2 years/2)	Ponemon	7.45%	7.45%	7.45%
C6	Expected annual average cost of a breach	C4*C5	$287,570	$287,570	$287,570
Ct	Reduced risk of security breach	C3*C6	$244,435	$258,813	$258,813
	Risk adjustment	↓20%			
Ctr	Reduced risk of security breach (risk-adjusted)		$195,548	$207,050	$207,050
	Three-year total: $609,649		**Three-year present value: $504,447**		

DECREASED STAFFING COSTS

Evidence and data. Over time, LogRhythm enabled organizations to include less senior/less expensive security analysts on their incident response teams because they could provide those analysts with detailed playbooks and other guidance and automate certain efforts. Instead of relying on what was in each analyst's memory about incident response, the organizations captured and codified that expertise in LogRhythm and augmented it with content from LogRhythm Labs. That content includes out-of-the-box templates and preconfigured blueprints for investigation and response constructed for different compliance mandates.

The organizations typically kept a consistent number of security analysts focused on investigating and resolving incidents but could shift some of the more senior analysts' time to other security efforts like threat hunting.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- A total of four security analyst FTEs investigate and resolve incidents in each of Years 1, 2, and 3.
- Over time, the organization shifts a percentage of that effort to analysts with less experience and lower compensation. The percentage is 20% in Year 2 and 30% in Year 3.
- The organization saves 30% on compensation for a less experienced analyst.

> **"If you have the playbooks defined and the alerts tuned correctly, a junior analyst can jump in, be trained quickly, and figure it out. They can triage events and escalate as needed, but you've reduced the cost of looking."**
>
> *IS security director, healthcare*

Risks. Risks that may affect decreased staffing costs include:

- The nature and extent of security analyst experience and expertise.
- The extent to which an organization has leveraged LogRhythm's capabilities and matured its overall security operations.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $63,760.

Decreased Staffing Costs

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Baseline number of security analysts investigating and resolving incidents	Interviews	4	4	4
D2	Security analyst baseline fully burdened compensation (annual, rounded)	B6*2080	$160,000	$160,000	$160,000
D3	Percentage of analyst effort shifted to less experienced analysts	Assumption	0%	20%	30%
D4	Anticipated compensation savings for each less experienced analyst	Interviews	30%	30%	30%
Dt	Decreased staffing costs	D1*D2*D3*D4	$0	$38,400	$57,600
	Risk adjustment	↓15%			
Dtr	Decreased staffing costs (risk-adjusted)		$0	$32,640	$48,960
	Three-year total: $81,600		**Three-year present value: $63,760**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Maturing the organization's security operations and freeing up analyst time for more strategic needs.** Interviewees viewed deploying and optimizing their organizations' use of LogRhythm as an important part of maturing their security operations. The IS security director in a healthcare organization said, "LogRhythm enables us to do a lot of new things that add value to our security program like building more playbooks, adding new and unique use cases, and tracking our incident trends."

  These improvements freed up security analyst time for other needs. With less time needed to investigate and resolve an incident and some of that effort shifted to less senior security analysts, organizations' senior security analysts had more time for threat hunting and maturing the organization's security operations. In addition, the media organization increased the time that its analysts spent on in-house training programs.

- **Detecting threats that may have been overlooked otherwise and reducing MTTD and dwell time.** LogRhythm enabled the interviewees' organizations to aggregate and correlate alerts and log sources that previously had been reviewed in isolation. It revealed the full scope of an attack instead of leaving an analyst to piece together disparate parts. This helped organizations detect threats that otherwise may have been overlooked and reduce their MTTD and dwell time.

  Although the interviewees lacked data to determine their MTTD prior to deploying LogRhythm, they believed their MTTD had decreased from days — if not weeks, or never — to minutes.

  The IS security director of a healthcare organization said: "LogRhythm is doing the job it's supposed to do, by bringing attention to malicious activities so we can stop and remediate that attack. We have a pen test at least once a year. Since deploying LogRhythm, we've caught the pen tester every time. And, because of all the things we've been able to do with the platform, we reduced the time to detection of a malicious attacker from 180 days to two days. If it had been there for 180 days, there would have been a breach. They would have had access to all the data. And we would have had an investigation and fines."

> **"If someone clicked on a phishing email and I find out a day later, it's a huge difference as opposed to finding out in five minutes."**
>
> *VP information security, healthcare*

  By aggregating and correlating alerts and log sources that previously had been reviewed in isolation — if at all — LogRhythm enabled organizations to detect threats they might have missed in the past. The cybersecurity engineer at a media company said: "We have a lot more flexibility in alerts and incident detection that we had before. Previously, each security tool could alert only on its own scope. Now that we have LogRhythm, I can build an alert that looks at multiple different activities to fire an alert."

- **Improved ability to comply with regulatory standards.** LogRhythm enabled organizations to comply with regulatory standards more easily and then meet an audit's compliance requirements by monitoring and reporting on their adherence to those standards.

  The VP of information security at a healthcare company said: "One of the things LogRhythm

does particularly well is to map their alerting and their rules directly to the different regulatory standards. It's done the homework for us, and that's provided tremendous value." That VP continued: "For instance, if I know we need to be PCI compliant, I can go into LogRhythm and identify the rules that indicate how we get PCI compliant in terms of monitoring and alerts."

"In the past we couldn't proactively audit ourselves and find the gaps. Now we can, instead of finding out from the auditors."

VP information security, healthcare

- **Flexible pricing model and scalability.** The VP of information security for a healthcare company cited LogRhythm's pricing model as one of the reasons for purchasing the platform, noting the resulting ability to ingest as much data as possible. The IS security director at a healthcare organization noted the ease with which LogRhythm could be scaled to accommodate acquisitions and organic growth by leveraging existing use cases, adding more log sources, and increasing the level of MPS covered by its LogRhythm subscription fees.
- **Additional analyst productivity improvement via more consistent and/or automated incident response and simplified collaboration and incident management.** In addition to decreasing the average time an analyst needed to investigate and resolve a security incident, LogRhythm improved analyst productivity in other ways.

  LogRhythm increased the consistency and repeatability of incident responses across security professionals with varied levels of experience and expertise. The IS security director for a healthcare organization said: "We have playbooks and formalized programs built around the different kinds of incidents, and those steps are baked into LogRhythm, so analysts know what to do next. Some of those are automated, some aren't, but they're all baked in."

  LogRhythm also enabled organizations to fully automate their response to certain incidents. The VP of information security for a healthcare company explained how its security team could ingest threat intelligence feeds into LogRhythm for correlation and then — where indicated — trigger an automated response. For instance, that organization uses LogRhythm to automatically block and then trigger blocklisting for IP addresses known to be malicious. That automation eliminates the need for the company's security team to create an alert that would detect those IP addresses and then subsequently investigate those alerts.

  In addition, the case management tools within LogRhythm reduced the time analysts spent managing the incident and collaborating with others.

"User interface and resource ramp were big reasons why we picked LogRhythm. LogRhythm's interfaces are easier to understand than other platforms. We can hand out passwords to our team members and have them immediately get value from it. Other products we considered require users to understand a lot more about generating syntax and how to search for things. LogRhythm does a lot of that for you, and makes it look pretty."

IS security director, healthcare

- **Ease of implementation and use.** The IT compliance manager for a real estate company noted: "The straightforward user experience out of the box was a big consideration in selecting LogRhythm. It's easy to navigate. And we don't need advanced technical skills to tweak or configure it."
- **Improved access to and cost of cybersecurity insurance.** Although not unique to LogRhythm, several organizations mentioned that the ability to show proof of using a SIEM helped them access cybersecurity insurance and do so at lower cost. The IS security director of a healthcare organization said, "I would expect that if we didn't have that SIEM box checked, our cyberinsurance costs would be higher." The VP of information security for a healthcare organization said, "We have several client requirements to have a SIEM, so if we didn't have one, we probably would not have been able to get insured."
- **Security becoming a brand enabler.** The organizations' use of LogRhythm enabled them to attract and retain incremental revenue by building confidence in customers and prospects that their data would be protected.

  The cybersecurity engineer at a media company said that customers and prospects, in deciding whether to do business with it, were starting to ask whether the company used a SIEM. The IS security director for a healthcare organization noted: "Our improved security maturity has translated into awards for our organization. It's a reputational thing to say our security program got an award. And a big part of that program involved using the SIEM."

  The IT compliance manager for the real estate company explained that the ability to demonstrate to customers that their data is safeguarded created a better perception of the company that attracted more customers. The VP of information security for a healthcare company indicated: "We have extensive security requirements for our clients, who need to be comfortable with our security profile. LogRhythm provides a significant capability for us. Without it, we probably would get 10% to 15% less new business each year."
- **Better security analyst experience and retention.** The IS director of a healthcare organization said: "A mature and well-used SIEM attracts good employees. We continue to improve our security program using LogRhythm, and our team has stated they like to work in an environment like ours where they can be innovative. I know that we have been able to keep people on the team because of the SIEM and because we have a program that encourages growth and innovation. If we can retain employees longer, it reduces our costs. So that increase in morale is huge."

FLEXIBILITY

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

- **Integrating additional security tools from LogRhythm or its partners and additional log sources.** Although the interviewees' organizations integrated their most critical tools and log sources into LogRhythm during implementation, they subsequently added more. Data from these new sources enabled organizations to further enhance their security programs.
- **Providing access to other groups within the organization.** Several interviewees indicated that their organizations either had provided additional groups (e.g., help desk, infrastructure, and audit

staff) with access to LogRhythm or were considering doing so.

The IT compliance manager at a real estate company described two opportunities: enabling the company's risk management department to comply with a new central bank framework around risk management for IT, by using a specific dashboard provided within LogRhythm; and using LogRhythm to create an internal dashboard for the audit team that would provide real-time data and simplify audit and reporting efforts for compliance parameters.

- **Applying LogRhythm to additional use cases.** LogRhythm can also be applied to other use cases including additional aspects of cybersecurity, fraud, disaster recovery, or physical security. The IS security director for a healthcare organization said, "Having the platform gives us a lot more options and growth opportunities that wouldn't exist without this investment."
- **Moving from on-premises to the cloud**. An interviewee, whose organization uses LogRhythm on-premises, indicated the organization will be looking at the cloud version in a few years to reduce infrastructure complexities and costs.

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**
Etr	LogRhythm fees	$21,000	$277,200	$277,200	$277,200	$852,600	$710,355
Ftr	Internal labor for implementation, management, and support	$13,524	$104,650	$33,102	$30,976	$182,252	$159,290
	Total costs (risk-adjusted)	$34,524	$381,850	$310,302	$308,176	$1,034,852	$869,645

LOGRHYTHM FEES

Evidence and data. LogRhythm fees include subscription or license fees that vary depending on the messages per second (MPS) LogRhythm ingests. Many customer-specific factors affect an organization's MPS volume and thus its fees. Consult with LogRhythm for pricing that is specific to your organization when conducting your own analysis. Subscription fees for cloud licenses and maintenance fees for perpetual licenses include a standard level of support.

Some organizations retained professional services from LogRhythm or third parties to help with implementation and training. While interviewees deemed LogRhythm easy to use, manage, and support, several worked with a LogRhythm Analytics Co-Pilot or Technical Account Manager for ongoing support around maximizing their use of the platform and maturing their overall security operations.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The organization pays $264,000 annually for subscription fees.
- The organization purchases $15,000 of implementation services.
- The organization pays LogRhythm $5,000 to train four security analysts and a security engineer who provides technical support.

Risks. Risks that may affect LogRhythm fees include:

- Number of security tools and log sources connected to the platform.
- The organization's preferences around third-party advisory services.
- The number of staff members trained.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $710,355.

LogRhythm Fees						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	NextGen SIEM Platform subscription	Composite		$264,000	$264,000	$264,000
E2	Professional services	Composite	$15,000			
E3	Training	Composite	$5,000			
Et	LogRhythm fees	E1+E2+E3	$20,000	$264,000	$264,000	$264,000
	Risk adjustment	↑5%				
Etr	LogRhythm fees (risk-adjusted)		$21,000	$277,200	$277,200	$277,200
	Three-year total: $852,600			**Three-year present value: $710,355**		

INTERNAL LABOR FOR IMPLEMENTATION, MANAGEMENT, AND SUPPORT

Initial costs. The composite organization requires 30 hours of security engineer time for technical implementation of cloud-based LogRhythm, including creating user accounts and roles, onboarding log sources, defining networks and IP ranges so the platform would recognize what was internal, and configuring the platform to accept the log sources. Training for the security engineer and four security analysts consists of an eight-hour training session followed by two days of getting comfortable with the system.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- A security engineer spends 30 hours on technical implementation.
- The security engineer and four security analysts each spend 24 hours in training.

Ongoing costs. To capitalize on the functionality of LogRhythm and enable the benefits described earlier in this study, security analysts needed to invest time baselining their organization's security operations. This consists primarily of two steps: 1) Understanding what the baseline should be, which involves getting a better understanding of how certain applications or users behave and indicating to the platform what is normal; and 2) establishing rule sets, writing scripts (or using those provided), and creating reports.

Baselining took around 20% of the analysts' time during their first six months of using LogRhythm and 5% of their time on an ongoing basis. Their ongoing efforts included determining how to address new activities and emerging threats, incorporating new log sources, and determining how to filter and capitalize on the additional data from those sources.

In addition, a security engineer needed to integrate additional security tools, onboard new log sources, and adjust alert rules.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- Four security analysts spend 20% of their time for the first six months of Year 1, and 5% of their time thereafter, for baselining and ongoing adjustments.
- A security engineer spends 130 hours annually to manage the platform and support end users.
- An additional security analyst is trained in Year 2.

Risks. Risks that may affect internal labor for implementation, management, and support include:

- The prior state of an organization's security operations and its vision for the future state.
- Whether the deployment is in the cloud or on-premises.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $159,290.

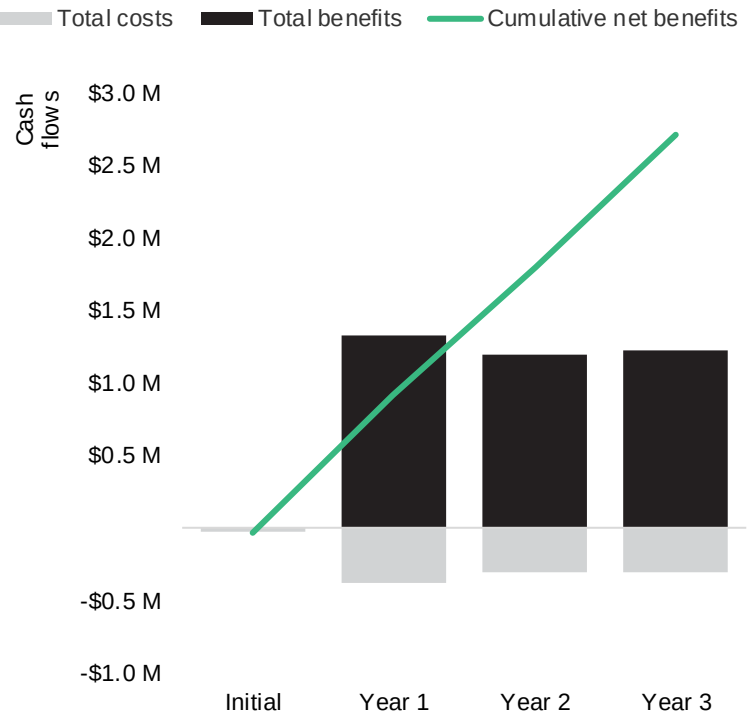
Internal Labor For Implementation, Management, And Support

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Security engineer combined total hours required for technical implementation and ongoing management and support	Interviews	30	130	130	130
F2	Security engineer fully burdened compensation (hourly)	Assumption: $174,720/2,080	$84	$84	$84	$84
F3	Security analyst combined total hours for baselining and ongoing adjustments	Interviews		1,040	208	208
F4	Security analyst fully burdened compensation (hourly)	B6		$77	$77	$77
F5	Number of staff members trained	Interviews	5		1	
F6	Hours spent in training per person	Interviews	24		24	
F7	Security analyst fully burdened compensation (hourly)	B6	$77	$77	$77	$77
Ft	Internal labor for implementation, management, and support	(F1*F2)+(F3*F4)+(F5*F6*F7)	$11,760	$91,000	$28,784	$26,936
	Risk adjustment	↑15%				
Ftr	Internal labor for implementation, management, and support (risk-adjusted)		$13,524	$104,650	$33,102	$30,976
	Three-year total: $182,252		**Three-year present value: $159,290**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($34,524)	($381,850)	($310,302)	($308,176)	($1,034,852)	($869,645)
Total benefits	$0	$1,327,756	$1,200,835	$1,217,155	$3,745,746	$3,113,944
Net benefits	($34,524)	$945,906	$890,534	$908,979	$2,710,894	$2,244,299
ROI						258%
Payback period						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: “Cost of a Data Breach Report 2020,” Ponemon Institute, April 2020.
[2] Source: “Cost of a Data Breach Report 2019,” Ponemon Institute, April 2019.


FORRESTER®