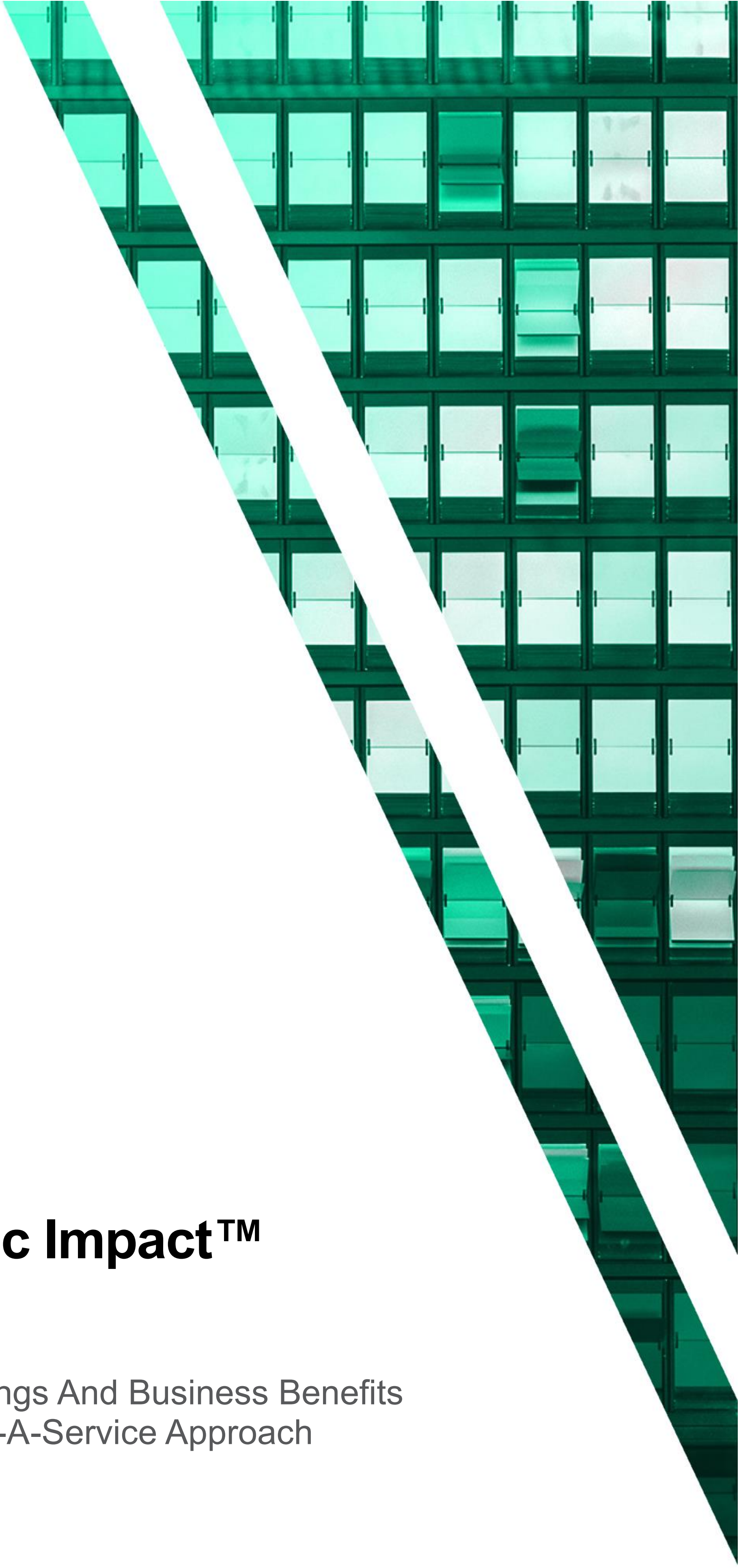
FORRESTER®



The Total Economic Impact™ Of ReliaQuest

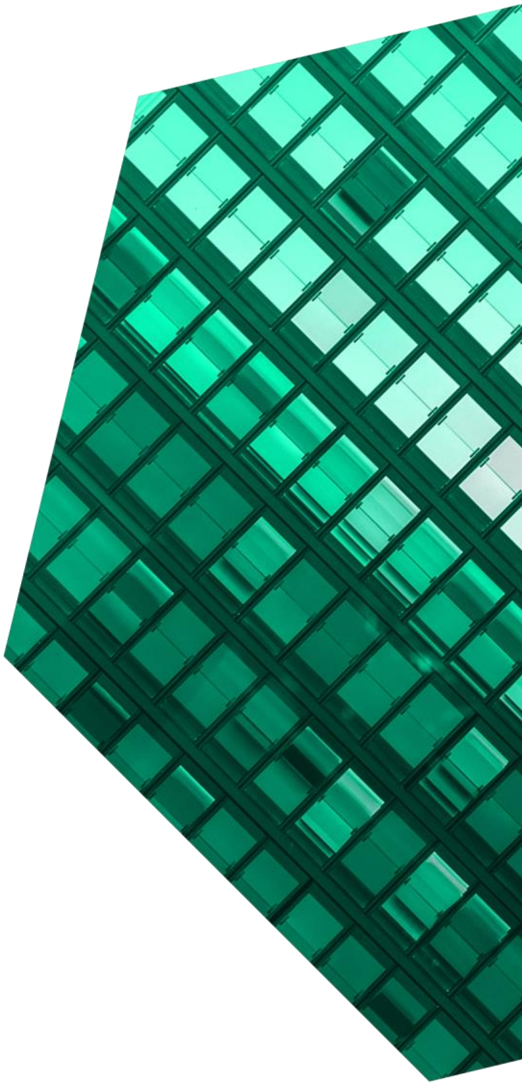
Customer-Realized Cost Savings And Business Benefits Enabled By An Open XDR-As-A-Service Approach

OCTOBER 2021

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY RELIAQUEST

Table Of Contents

Consulting Team: Connor Maguire
Benjamin Corey



Executive Summary

Organizations spend years and hundreds of thousands of dollars deploying strategies and frameworks that don't ultimately drive their desired outcomes. But security leaders are getting closer to achieving those goals by blending services, technology, and best practices with curated integration and detection content. ReliaQuest delivers an open XDR cloud-native platform, 24/7/365 expertise and best practices to make desired security outcomes possible.

ReliaQuest delivers its services through a cloud-native Open XDR platform designed to bring together data from across a company's security ecosystem into a single view to quickly detect, investigate, and remediate threats. Compiling data from various security tools and cloud or hybrid data sources in one place provides the foundation for situational awareness, faster time-to-insights, and quicker responses to cybersecurity threats. This ultimately gives organizations the ability to manage and communicate risk to the business.

ReliaQuest commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by engaging ReliaQuest.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of ReliaQuest on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using ReliaQuest's cloud-native Open XDR platform. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using ReliaQuest, these interviewees noted how their organizations used a combination of security platforms from disparate vendors and in-house solutions to fill in coverage gaps. However, prior attempts yielded limited success, leaving them with challenges like supporting necessary staff for 24/7 security monitoring and inefficient manual processes that constrained interviewees' organizations' resources. These limitations led to untenable false positive rates and the need for increased headcounts to monitor security systems and correlate security relevant data from cloud applications across the business

KEY STATISTICS

Return on investment (ROI)
350%

Net present value (NPV)
$5.51M

After the investment in ReliaQuest, the interviewees' organizations have been able to offload threat detection and response responsibilities to ReliaQuest security experts and automate many of their processes from detection, investigation, response, and resilience through ReliaQuest. Key results from the investment include increased coverage from cybersecurity threats, avoided additional headcount, and time savings from reducing the mean-time-to-resolve (MTTR).

> **For me as the manager of the team, I don't have to hire new analysts and then train them up. We're using ReliaQuest to do those things. They're hiring the new analysts and they're going to train them** — Associate VP of cybersecurity, retail

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Increased risk coverage reduced the likelihood of a breach by 20%.** Implementing ReliaQuest allows for improved automatic threat detection and reduces response time when a threat is discovered. By integrating tools, organizations realize ROI on existing investments while reducing risk. Furthermore, awareness of risk helps security leaders advise the business when launching new initiatives or budgeting for additional staff or tools — from cloud to go-to-market models, to opening new regions, and more. By avoiding a breach, organizations can avoid costs associated with customer notification, fines, and damage to their brand image, as well as reduced employee productivity from disruptions caused by the breach. This reduction produced a three-year present value of $2.7 million for the composite organization.
- **Reduced headcount expenses by $1.2M over three years for the composite organization.** Before adopting ReliaQuest, interviewees' organizations required additional staffing for their security support centers, security operations center (SOC) maintenance, and analysis. By utilizing the capabilities of the ReliaQuest platform, the organizations were able to focus existing resources on the most relevant security issues and avoid the burden of hiring and onboarding additional headcount.
- **Reduced the number of incidents requiring analyst response by 90%.** Prior to investment in ReliaQuest, incidents were frequent, totaling 400 per month. Improved incident management reduced incident totals to 30 per month while ReliaQuest's offering reduced the MTTR by 50%. These process improvements for the composite organization resulted in a three-year present value of over $2.2 million.
- **Reduced false positives by 90% with the improved incident accuracy provided by ReliaQuest.** Prior to investment, false positives were rampant, totaling 100 per month. ReliaQuest's ability to integrate disparate tools

and cascade detection content across them led to more accurate alerting capabilities and reduced this monthly average to 10. The time saved by reducing investigations into false positives resulted in a three-year present value of $348K for the composite organization.

- **Saved $200,000 annually for the composite organization by retiring legacy tooling.** The interviewed decision-makers' organizations were able to scale back their investments in security solutions with offerings made redundant by the features of ReliaQuest. Over the three-year analyzed period, this benefit to the composite organization created more than $440K in savings.
- **Reduced the need to review legacy MSSP/MDR incidents.** The interviewed organizations found that in their legacy states they had limited to no visibility into the operations of their managed security services provider (MSSP) or managed detection and response (MDR) provider operations. This led to investing resources in auditing log data and double checking the work of these providers to ensure that their environment was properly secured. Investing in ReliaQuest gave these organizations increased visibility into the workings of their security environments and allowed them to reallocate these resources to more business-critical tasks. This saved the composite organization $123K over the modeled period.

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

- **Increased effectiveness of security tools.** The interviewed decision-makers found that eliminating many of the manual tasks associated with cyber hygiene allowed their organizations to better use existing security data and tools. These interviewees said that this enabled their teams to improve the return on investment they received from those products.
- **Negotiated lower insurance premiums.** Several interviewees noted that their organizations' investment in ReliaQuest caused the brokerage firms who issue cyber insurance to look more favorably on their organizational security. This enabled the decision-makers' organizations to lower the cost of their premiums, leading to additional cost savings.

Costs. Risk-adjusted PV costs include:

- **$528,000 in risk-adjusted combined subscription costs.** Interviewees stated that their organizations paid an annual fee to ReliaQuest for use of their solution. These fees are typically broken up into different levels (Managed, Extended, Automated) based on the features and services required. Several of the decision-makers also reported investing in engagements with the ReliaQuest services team to extend the use of its product.
- **Implementation and training carried three-year present costs of $132,000.** ReliaQuest users spend time planning and implementing the solutions across their organizations and training users on the best way to integrate the solution into their typical workflows.
- **Employee management costs total $48,000 annually.** Finally, all interviewees' organizations dedicated partial resources to the ongoing management and maintenance of the relationship.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $7.09 million over three years versus costs of $1.58 million, adding up to a net present value (NPV) of $5.51 million and an ROI of 350%.

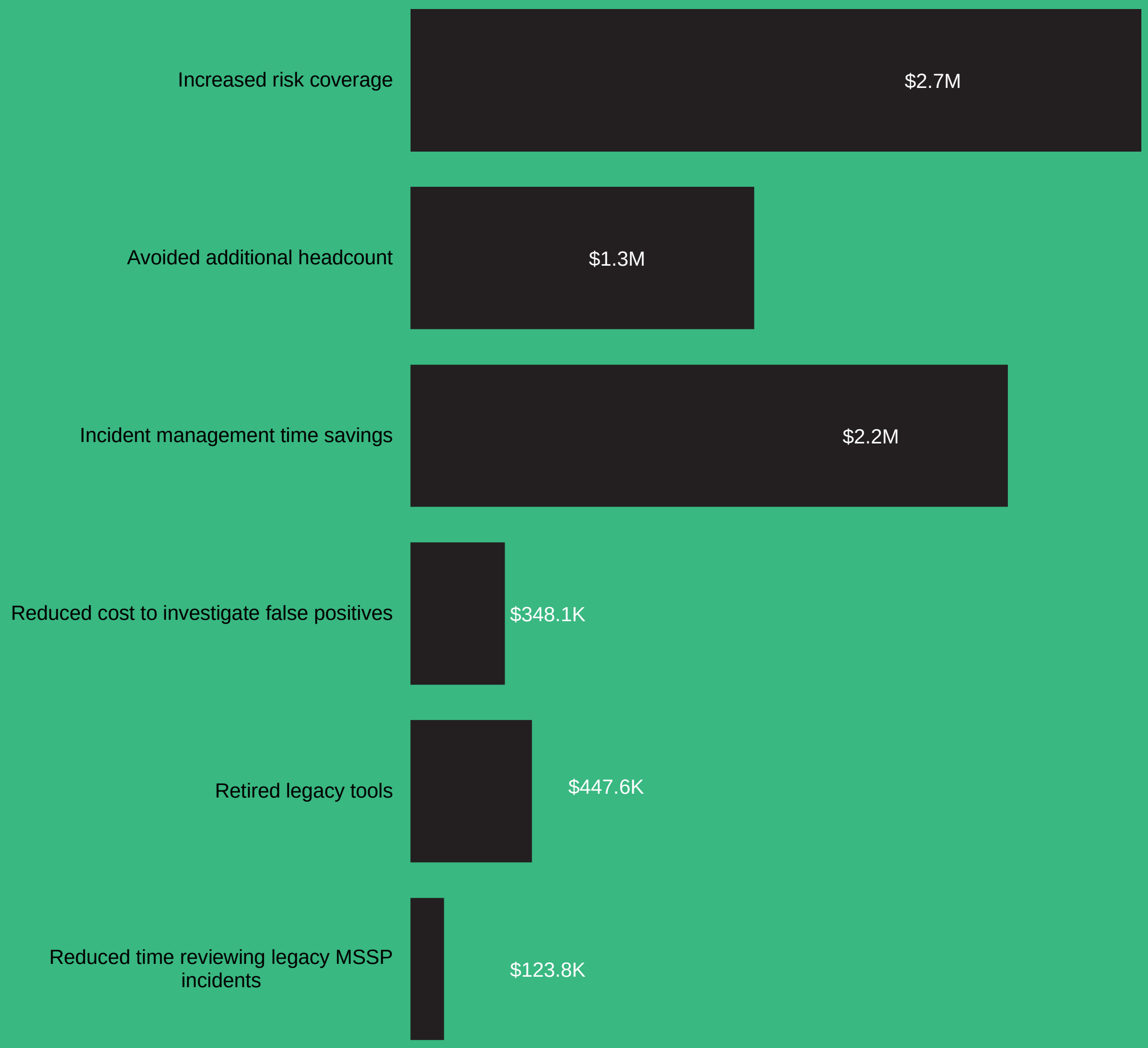
ROI
350%

BENEFITS PV
$7.09M

NPV
$5.51M

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 ReliaQuest.

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 ReliaQuest can have on an organization.

DUE DILIGENCE

Interviewed ReliaQuest stakeholders and Forrester analysts to gather data relative to ReliaQuest.

DECISION-MAKER INTERVIEWS

Interviewed four decision-makers at organizations using ReliaQuest to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by ReliaQuest 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 study to determine the appropriateness of an investment in ReliaQuest.

ReliaQuest 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.

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

The ReliaQuest Customer Journey

🟩 Drivers leading to the ReliaQuest investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Annual Revenue
Chief information security officer	Retail	Headquartered in the US	$3B
Chief security officer	Law	Headquartered in the US	$5B
Associate vice president of cybersecurity	Retail	Headquartered in the US	$13B
Chief information security officer	Banking	Headquartered in the US	$30B

KEY CHALLENGES

Prior to investing in ReliaQuest the interviewed decision-makers described legacy states that depended on multiple point solutions with neither a common connection nor a MSSP or MDR provider that provided security teams with actionable insights into the threats their environment faced.

The interviewees noted how their organizations struggled with common challenges, including:

- **Need for 24/7/365 monitoring.** All interviewees wished to provide 24/7/365 security monitoring and support to their organization. Legacy systems restricted their ability to do so by requiring these organizations to either pay a premium for this level of monitoring or staff the monitoring centers internally. This proved to be both an expensive and risky endeavor, as those who chose not to invest in vendor coverage often left their monitoring centers unattended for several hours. One interviewee described this challenge by saying: “The hackers don’t sleep so we can’t. So, there’s the basic challenge of how do you set up a 24/7/365 support with high reliability and redundancy? You need people, processes, and technology, and building this out comes with a whole bucket of challenges there. You can buy these packages, or other kinds of automated testing systems, but these cost hundreds of thousands of dollars.”
- **Desire to build out more mature security systems and processes.** Many of the legacy service providers that the interviewees previously relied upon were very rigid and could not be easily adapted to meet the dynamic needs of business and security environments. This was frustrating for the interviewed decision-makers as it often forced their organizations to invest in additional technology to patch up holes that emerged in their environments.
- **Need to eliminate noise from legacy systems and focus on key security alerts.** Finally, the interviewees found that legacy incident management systems escalated a vast number of alerts to their security teams. These left analysts overwhelmed by the number of manual investigations they were required to perform and pulled them away from higher-value security work. Often these investigations found either false positive alerts or very low priority security incidents. The interviewees strove to implement a solution that could reliably filter out this unnecessary noise.

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 decision-makers 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 representative of a multibillion-dollar global organization with 20,000 employees, including a team of 20 security analysts dedicated to incident monitoring and response. The composite organization previously relied on a series of endpoint monitoring solutions as well as an MSSP/MDR to monitor and respond to security events. The composite organization struggles with the same challenges as the interviewees' organizations and prioritizes reducing noise across its security environment and increasing overall endpoint security. Prior to investing in ReliaQuest, the composite used legacy systems which would escalate an average of 400 events per year. After investigation, it is determined that 100 of these events are false positives. These incidents took an average of 2 hours to investigate and resolve.

Deployment characteristics. The composite organization deploys ReliaQuest to monitor its Tier 1 support, content creation, security information and event management (SIEM), and endpoint detection and response (EDR) engineering. The composite customer represents 50% of organizations on the Extended plan and 50% of organizations on the Automated plan. Additionally, the organization integrates ReliaQuest with many of the solutions that it uses to secure its environment. The organization uses the ReliaQuest services team to implement preliminary threat hunting workflows and plans to work with this team to help it expand the use of ReliaQuest to Tier 2 and 3 support.

Key assumptions

- **20,000 employees**
- **400 total incidents investigated**
- **100 false positives**
- **2-hour MTTR**

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	Increased risk coverage	$1,084,160	$1,084,160	$1,084,160	$3,252,480	$2,696,145
Btr	Avoided additional headcount	$510,000	$510,000	$510,000	$1,530,000	$1,268,295
Ctr	Incident management time savings	$886,464	$886,464	$886,464	$2,659,392	$2,204,505
Dtr	Reduced cost to investigate false positives	$139,968	$139,968	$139,968	$419,904	$348,080
Etr	Retired legacy tools	$180,000	$180,000	$180,000	$540,000	$447,633
Ftr	Reduced time reviewing legacy MSSP incidents	$49,766	$49,766	$49,766	$149,299	$123,762
	Total benefits (risk-adjusted)	$2,850,358	$2,850,358	$2,850,358	$8,551,075	$7,088,420

INCREASED RISK COVERAGE

Evidence and data. The interviewed decision-makers' organizations found that their legacy security systems were often disjointed and difficult to manage. Security analysts spent considerable time addressing a myriad of security incidents with little to no ability to classify and prioritize these events. The situation forced employees to pull information from multiple sources and attempt to decipher the extent and severity of incidents across these different areas. This led to slow incident response times, causing untimely delays in incident response for higher priority tasks.

The resulting security environment was stuck in a perpetually reactive state. Analysts had limited ability to research new and emerging threats and could not perform any threat hunting or other higher-tier security actions. The interviewees required a solution that could help automate aspects of their security support workflows for them to ensure that no potential threats were being overlooked.

Using ReliaQuest allowed the interviewees' organizations to automate portions of their security response workflows, enabling analysts to focus on higher priority threats and leading to a more secure environment.

Customers also saw ReliaQuest as a trusted partner who could help them make improvements to their security environment and reduce risk. One interviewee highlighted this by saying: "ReliaQuest gives us suggestions on what data sources we should have if we need that data to address a particular risk. So that helps reduce our risk landscape as well as making sure that the content is covering relevant MITRE ATT&CK techniques and Kill Chain frameworks."

The decision-makers' organizations worked in partnership with the ReliaQuest services teams to build out advanced workflows and techniques that can aid in reducing the risk of a potentially harmful breach. As the CSO for a North American law firm described: "Securing our data has been easier than we expected, and this is because we were leveraging ReliaQuest's experience and expertise which has been a major benefit. They have people that know our systems better than we did and they were able to say: 'Well, based on our experience, we'll do it this way.' Great! They improved our SIEM deployment, and those improvements that they brought to our environment helped ease all management and support work. I think that they have provided better visibility into things in our environment, and they point out what [actions] we need to take actions to remediate [issues]. That allows us to be informed on where we need more visibility, where we need a project or capability we don't have today. It's helped drive our strategy as to what we need to do to continue to improve our environment's security."

The combination of increased automation and the insights and capabilities provided by the ReliaQuest services teams allowed the interviewees' organizations to reduce the risk their environments face. This enabled them to avoid security breaches and mitigate the potentially profound financial impacts these incidents can have. An interviewee expressed this by saying: "Our time to resolve is now fast enough that we are able to react extremely quickly. We've shut down malware before it became a breach, so we are experiencing extreme savings there. We are a lot more likely to identify a breach earlier into detection, which can result in cheaper incident response. Whether it's for notification, containment, or quickly starting a forensics investigation, all those pieces of our incident response are cheaper the earlier in an incident you detect it. So that's the primary value derived from having broader coverage."

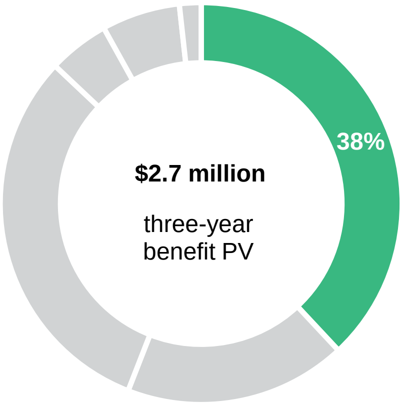
Modeling and assumptions. For the composite organization Forrester assumes:

- Through an extensive survey of vendors, Forrester determined that on average an organization can expect to experience 3.2 breaches per year. These breaches have an average potential cost of $53 per person (exclusive of the cost of downtime).
- Automating lower-tier incidents and utilizing the insights and capabilities provided by ReliaQuest allows customers to expand their risk coverage. This reduces the likelihood of a breach by 20%.
- In addition to the costs associated with a breach, the employees of the composite organization could experience extended periods of downtime. This leads to lost productivity for workers affected by a breach. Per the aforementioned survey, Forrester found that on average 20% of the employee population will experience downtime and the affected employees experienced an average of 3.6 hours of downtime.
- The average hourly salary for all employees affected by downtime associated with a breach is $47.

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

- The importance of the data at the composite organization, relative to organizations in other verticals, can materially affect the cost of a breach.
- The severity of breaches (such as east-west proliferation or critical application services) can affect internal business users.

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 almost $2,700,000.



Increased Risk Coverage

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average number of breaches per year	Forrester survey	3.20	3.20	3.20
A2	Average potential cost of a data breach ($53 per employee) exclusive of internal downtime	Forrester survey	$1,060,000	$1,060,000	$1,060,000
A3	Reduced likelihood of a breach	Interviews	20%	20%	20%
A4	Subtotal: Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external facing costs	A1*A2*A3	$678,400	$678,400	$678,400
A5	Number of internal employees	Composite	20,000	20,000	20,000
A6	Average hourly salary for business users	Assumption	$47	$47	$47
A7	Diminished/eliminated internal user productivity (hours)	Forrester survey	3.6	3.6	3.6
A8	Average percentage of employees affected per breach	Forrester survey	20%	20%	20%
A9	Subtotal: Cost of reduced internal productivity	A5*A6*A7*A8	$676,800	$676,800	$676,800
At	Increased risk coverage	A4+A9	$1,355,200	$1,355,200	$1,355,200
	Risk adjustment	↓20%			
Atr	Increased risk coverage (risk-adjusted)		$1,084,160	$1,084,160	$1,084,160
	Three-year total: $3,252,480		**Three-year present value: $2,696,145**		

AVOIDED ADDITIONAL HEADCOUNT

Evidence and data. The interviewed organizations noted that a major benefit of using ReliaQuest was it gave them the ability to avoid staffing increases or maintaining a 24/7/365 security support operation.

The interviewees described that, prior to using ReliaQuest, they typically attempted to build and maintain a support center internally. This proved to be an expensive and risky task as they either needed to hire two teams to provide true 24-hour support or offer support for a limited time. The more affordable option left their environment vulnerable during off hours. Investing in ReliaQuest allowed these organizations to offload the burden of maintaining these support centers to the ReliaQuest services team and the capabilities of the platform. This allowed the organizations to offload the cost of these services and avoid the expense associated with this level of support. As one interviewee noted: "If we were looking for a support center for a company of our size], we would be talking about six to 12 full-time folks just to cover all those 24/7/365 incidents."

In addition to avoiding the cost of support, the interviewed organizations also found that the expertise provided by the ReliaQuest team allowed them to sidestep investing in additional resources dedicated to creating rules, policies, and other content within their established security systems. An interviewee highlighted this by saying: "We would have needed another group of people setting up rules and policies or creating and updating content within our other solutions. To achieve the value that we are getting with ReliaQuest we would need to buy new tools or hire new team members to recreate these capabilities."

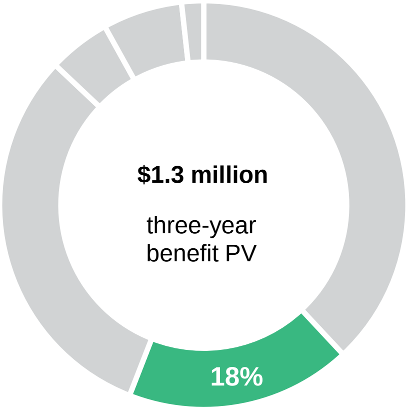
Modeling and assumptions. For the composite organization Forrester assumes:

- Without investing in ReliaQuest, the composite organization would need a dedicated a team of eight employees for Tier 1 security support. The annual salary of these employees is $50,000 each.
- In addition to avoiding the cost of hiring additional support employees, the composite organization avoids the need to hire additional employees to perform maintenance and analysis on their established solutions. Without ReliaQuest, the composite organization would need to dedicate two employees to these tasks. The average salary of these employees is $100,000 each.

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

- Legacy support workflows and deployments can affect the need to invest in additional resources.
- Regional variation in salaries will affect the extent of savings generated by this benefit.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of over $1,200,000.



Avoided Additional Headcount

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Employees required to staff support center	Interviews	8	8	8
B2	Annual salary of support employees	Assumption	$50,000	$50,000	$50,000
B3	Subtotal: Cost required to staff support center without ReliaQuest	B1*B2	$400,000	$400,000	$400,000
B4	Employees required to perform legacy security solution maintenance and analysis	Interviews	2	2	2
B5	Annual salary of employees working on legacy security solution	Assumption	$100,000	$100,000	$100,000
B6	Cost required to perform legacy security solution maintenance and analysis	B4*B5	$200,000	$200,000	$200,000
Bt	Subtotal: Avoided additional headcount	B3+B6	$600,000	$600,000	$600,000
	Risk adjustment	↓15%			
Btr	Avoided additional headcount (risk-adjusted)		$510,000	$510,000	$510,000
	Three-year total: $1,530,000		**Three-year present value: $1,268,295**		

INCIDENT MANAGEMENT TIME SAVINGS

Evidence and data. As previously discussed, a major challenge all interviewees faced in their legacy security states was alert volume. The interviewees all had various security solutions that produced a variety of alerts for investigation daily. This led to security teams being overwhelmed by the number of investigations they were expected to investigate. This feeling was exacerbated by the fact that incident investigation was a lengthy process and legacy solutions often could not properly filter out false positives, which extended incident resolution time. One interviewee described their organization's situation by saying: "In our prior state we were getting thousands of events a month because the place was so dirty and messy. Investing in ReliaQuest was the only way to be successful. Otherwise we were getting too much noise in the environment. If you don't clean the junk, eventually you trip on it. So, now, in the time [we've been with ReliaQuest], we've cleaned up so many events that were just garbage."

With ReliaQuest, the decision-makers' organizations automated incident response processes, allowing their security analysts to focus on a select number of high-priority incidents. Reducing noise across security environments has the added benefit of reducing the average time spent remediating each incident, as analysts no longer perform lengthy investigations on false positives (which will be modeled in the next benefit section). One interviewee described the efficiency gain they experience from their ReliaQuest deployment by saying: "Our MTTR has been reduced significantly, down to a few hours. In under 24 hours, we've gotten information back on what we need to confirm. Thank goodness, a lot of them end up being policy violations."

Modeling and assumptions. For the composite organization Forrester assumes:

- Prior to investing in ReliaQuest the composite organization experiences 400 events that its security analyst team investigate manually. 100 of these incidents are determined to be false positives and are included in the next benefit.
- The composite organization dedicates 3 analysts from its security team to incident investigation and resolution. Prior to working with ReliaQuest, these investigations lasted for an average of 2 hours.
- The average hourly salary for employees involved in these workflows is $48.
- Automating incident response and removing the burden of lower-tier incident response from security analysts enabled the composite organization to reduce the number of manual incident investigations it performs to 30. Additionally, the composite can reduce the time required to investigate each incident by 1 hour.

Reduced MTTR by:

50%

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

- Established incident management solutions will affect the extent to which ReliaQuest can reduce manual investigations.
- Incident response management workflows will vary by organization and vertical.

Incident Management Time Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Security incidents responded to prior to investing in ReliaQuest (monthly)	Interviews	300	300	300
C2	Security individuals involved in incident response process	Interviews	3	3	3
C3	Time spent investigating and resolving incidents prior to investing in ReliaQuest (hours)	Interviews	2	2	2
C4	Hourly salary of employees involved in incident response and resolution workflows	Assumption	$48	$48	$48
C5	Subtotal: Total cost to investigate security incidents prior to investing in ReliaQuest	C1*C2*C3*C4*12	$1,036,800	$1,036,800	$1,036,800
C6	Security incidents investigated with ReliaQuest (monthly)	Interviews	30	30	30
C7	Time spent investigating and resolving incidents with ReliaQuest	Interviews	1	1	1
C8	Cost to resolve incidents with ReliaQuest	C2*C3*C4*C6*12	$51,840	$51,840	$51,840
Ct	Incident management time savings	C4-C8	$984,960	$984,960	$984,960
	Risk adjustment	↓10%			
Ctr	Incident management time savings (risk-adjusted)		$886,464	$886,464	$886,464
Three-year total: $2,659,392		**Three-year present value: $2,204,505**			

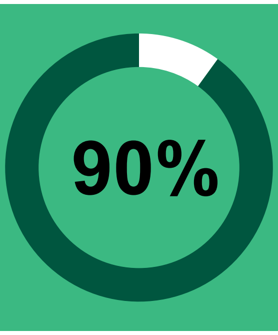
Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of over $2,200,000.

REDUCED COST TO INVESTIGATE FALSE POSITIVES

Evidence and data. In conjunction with a reduction in event investigations, the interviewed decision-makers stated that their organizations also saw a reduction in the number of false positives their security teams investigated.

In their legacy states, security solutions frequently escalated incidents for review that were deemed to be false positives. Typically, these reviews required analysts to perform a significant portion of an incident investigation before flagging the alert as a false positive. ReliaQuest applied machine learning to filter out false positives, greatly reducing the number of incidents that analysts investigate. As one interviewee shared: “It's been at least a 70% reduction in false positive rate. You start filtering down events and within that quarter, we had a massive cleansing of data. There is a significant cost savings associated with this.”

Reduced false positives by:



Modeling and assumptions. For the composite organization Forrester assumes:

- The composite organization investigates 100 incidents that are deemed to be false positives. These investigations typically last an hour and involve three individuals.
- The average hourly salary for individuals involved in these workflows is $48.
- Implementing ReliaQuest allowed these customers to reduce the number of false positives investigated by 90%.

Risks. The following risk factors may affect the extent to which an organization experiences these benefits.

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

Reduced Cost To Investigate False Positives

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	False positives manually investigated prior to investing in ReliaQuest (monthly)	Interviews	100	100	100
D2	Security individuals involved in incident investigation process	Interviews	3	3	3
D3	Time spent investigating false positives prior to investing in ReliaQuest	Interviews	1.0	1.0	1.0
D4	Hourly salary of employees involved in incident investigation	Assumption	$48	$48	$48
D5	Cost to investigate false positives prior to investing in ReliaQuest	D1*D2*D3*D4*12	$172,800	$172,800	$172,800
D6	Reduction in the number of false positives investigated	Interviews	90%	90%	90%
Dt	Reduced cost to investigate false positives	D5*D6	$155,520	$155,520	$155,520
	Risk adjustment	↓10%			
Dtr	Reduced cost to investigate false positives (risk-adjusted)		$139,968	$139,968	$139,968
	Three-year total: $419,904		**Three-year present value: $348,080**		

RETIRED LEGACY TOOLS

Evidence and data. The interviewees' organizations used the capabilities of the ReliaQuest platform to scale back investment in existing security solutions. The interviewees found that the capabilities of the ReliaQuest platform were often superior to those of their legacy MDR and MSSP providers. Additionally, some organizations were able to avoid purchases of threat intelligence or breach and attack simulation tools because those components are included as part of the ReliaQuest platform. The interviewed CISO of a global retail company explained how ReliaQuest has replaced other managed service providers by saying, "We do have some managed contracts for tool maintenance and optimization for things that we might have as one-offs, but ReliaQuest serves as our primary SOC and Tier 1 provider for response." They went on to describe how their team was able to reinvest these savings into further improvements for their operations team.

Modeling and assumptions. For the composite organization Forrester assumes:

- The composite organization invests $200,000 annually in solutions and product features that are included in their investment in ReliaQuest.
- Investing in ReliaQuest allows these organizations to avoid all the costs associated with these products and features (these could be threat intelligence, breach and attack simulation, or threat hunting platforms).

Reduced annual spending on legacy tools by:

$200,000

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

- The amount organizations spend on legacy vendors.
- The capabilities of those vendors.
- The extent to which customers choose to deploy ReliaQuest.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of almost $447,6700.

Retired Legacy Tools

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Cost of retired legacy tools	Assumption	$200,000	$200,000	$200,000
Et	Retired legacy tools	E1	$200,000	$200,000	$200,000
	Risk adjustment	↓10%			
Etr	Retired legacy tools (risk-adjusted)		$180,000	$180,000	$180,000
	Three-year total: $540,000		**Three-year present value: $447,633**		

REDUCED TIME REVIEWING LEGACY MSSP AND MDR INCIDENTS

Evidence and data. Finally, several interviewed decision-makers stated that ReliaQuest provides transparency not available from MSSP or MDR providers, allowing them to avoid the need to audit the work of their legacy providers. The interviewees described that with legacy providers they had little to no visibility into incidents that were being deflected by their legacy MSSP. This caused them to spend time auditing and testing the system, taking up resource time that could be better spent elsewhere.

With ReliaQuest, the interviewees' organizations were able to gain increased visibility into all aspects of their security environments, including the events that were being automatically resolved by

> **“ReliaQuest is providing more coverage, which lets us focus less on constantly testing and validating to see if our service provider is doing their job and just trusting the process and working with what they find.”**
>
> *CISO, retail*

ReliaQuest. This gave the interviewees’ organizations an increased sense of trust that their environment was secure and that systems were working as intended. This also allowed these organizations to reallocate employee time previously dedicated to auditing established systems to more business-critical activities.

Modeling and assumptions. For the composite organization Forrester assumes:

- With legacy MSSP/MDR solutions the composite organization dedicated three employees to auditing their legacy incident management tactics. These staffers spent 32 hours each month performing these tasks.
- The average hourly salary of employees involved in these workflows is $48.
- By transitioning to ReliaQuest the composite organization can eliminate all legacy workflows associated with auditing legacy MSSP/MDR solutions.

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

- Organizations whose legacy state does not include an MSSP/MDR will not recognize this benefit.
- Not all organizations choose to perform audits on their legacy security environments and will not recognize these savings as a result.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of almost $123,800.

Reduced Time Reviewing Legacy MSSP And MDR Incidents

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Time spent reviewing MSSP work in legacy state (monthly)	Interviews	32	32	32
F2	Number of employees involved in these workflows	Interviews	3	3	3
F3	Hourly salary of employees involved in incident investigation	Assumption	$48	$48	$48
Ft	Reduced time reviewing legacy MSSP and MDR incidents	F1*F2*F3*12	$55,296	$55,296	$55,296
	Risk adjustment	↓10%			
Ftr	Reduced time reviewing legacy MSSP incidents (risk-adjusted)		$49,766	$49,766	$49,766
	Three-year total: $149,299		**Three-year present value: $123,762**		

UNQUANTIFIED BENEFITS

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

- **Increased effectiveness of security tools.** Using ReliaQuest to automate manual processes, analysts at the interviewed decision-makers' organizations could look at their existing technology solutions and find features or capabilities of these products that they did not utilize before. This allowed analysts to drive additional efficiencies through these tools and enabled them to get more value from their tools.

- **Cyber insurance premium reductions.** The interviewees found that investing in ReliaQuest enabled them to lower their insurance premiums. Insurance providers saw adding ReliaQuest to their security suites provided more protection against threats, which resulted in additional cost savings for the interviewees. The associate VP of cybersecurity at a global retail organization described how improving their security posture helped when it came time to negotiate security insurance premiums. They explained: "It always puts us in a very good position with our cyber insurance auditors. When they hear that we're using ReliaQuest and doing the right things, it puts us in a better light, and we save money."

FLEXIBILITY

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

- **Expanding use case to include additional cloud-based sources of telemetry.** The interviewees noted that they planned to expand their use of ReliaQuest to include sources of cloud-based telemetry. This could provide additional efficiencies for employees and would increase the risk coverage to include their cloud-based logs. One interviewee elaborated: "Where the world is going and where we're going with ReliaQuest is to other data sources—behavior-based data and logs and telemetry from various cloud services. We have a gap when it comes to certain cloud-based data and detection that ReliaQuest is helping to patch for us."

- **Easier onboarding of new tools.** Interviewees also noted that they could rely on their partnership with the ReliaQuest team to help vet new vendors. The expertise provided by the individuals on the ReliaQuest team helped customers understand what security solutions work well with their current environment and provided insights on the fastest and most secure ways to get these solutions up and running.

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**
Gtr	License and services costs	$0	$528,000	$528,000	$528,000	$1,584,000	$1,313,058
Htr	Implementation and training costs	$81,664	$20,416	$20,416	$20,416	$142,912	$132,436
Itr	Employee management time	$0	$52,800	$52,800	$52,800	$158,400	$131,306
	Total costs (risk-adjusted)	$81,664	$601,216	$601,216	$601,216	$1,885,312	$1,576,800

LICENSE AND SERVICES COSTS

Evidence and data. ReliaQuest customers pay for the ongoing use of the platform. In addition, most customers chose to invest in professional services to tailor the solution to their individual needs and integrate the solution with their legacy telemetry sources.

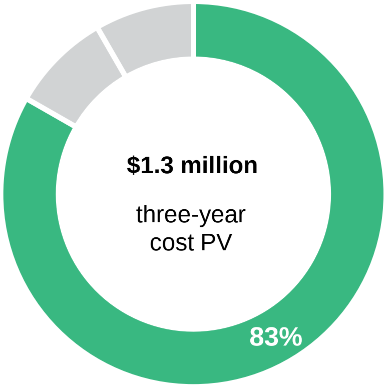
Modeling and assumptions. For the composite organization Forrester assumes:

- The composite organization pays $400,000 annually for use of ReliaQuest.
- The organization invests $80,000 annually in professional services engagements with ReliaQuest.

Risks. The following risk factors may affect the extent to which an organization experiences these costs:

- Individual licensing costs will vary based on the number of data sources ReliaQuest monitors.
- The need to deploy professional services will vary on an organizational basis.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of more than $1,313,000.



License And Services Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	License costs	Interviews		$400,000	$400,000	$400,000
G2	Services costs	Interviews		$80,000	$80,000	$80,000
Gt	License and services costs	G1+G2	$0	$480,000	$480,000	$480,000
	Risk adjustment	↑10%				
Gtr	License and services costs (risk-adjusted)		$0	$528,000	$528,000	$528,000
	Three-year total: $1,584,000		**Three-year present value: $1,313,058**			

IMPLEMENTATION AND TRAINING COSTS

Evidence and data. The interviewed organizations incurred indirect costs for internal labor to deploy ReliaQuest. The interviewees' organizations spent time researching ReliaQuest, planning for the implementation, and executing the plan.

The decision-makers' organizations also stated that users typically spent time in training on how to best use the ReliaQuest platform and how to integrate existing security systems with ReliaQuest. There is no charge for this training, and ReliaQuest provides free training on many SIEM and EDR platforms.

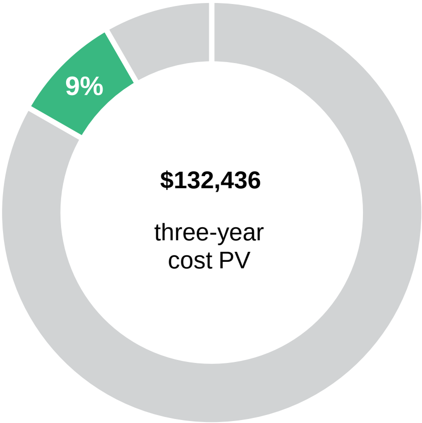
Modeling and assumptions. For the composite organization Forrester assumes:

- The composite organization has a team of three employees who spend a collective 160 hours planning for and implementing ReliaQuest.
- The hourly salary of the individuals involved in these workflows is $58.
- The 20 members of the composite organization's security team participate in 40 hours of training as the organization first introduces ReliaQuest. In subsequent years, these analysts spend 16 hours annually refreshing their skills on the platform and learning how to best make use of new features and functionalities.

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

- Implementation and training times will vary based on established organizational practices and workflows.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of more than $132,000.



Implementation And Training Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Employees involved in implementation	Assumption	3			
H2	Time spent implementing ReliaQuest	Interviews	160			
H3	Hourly salary for employees involved in implementation	Assumption	$58			
H4	Subtotal: Cost to implement ReliaQuest	H1*H2*H3	$27,840			
H5	Number of individuals trained on ReliaQuest	Assumption	20	20	20	20
H6	Time spent training on ReliaQuest	Interviews	40	16	16	16
H7	Cost to train users on ReliaQuest	H5*H6*H3	$46,400	$18,560	$18,560	$18,560
Ht	Implementation and training costs	H4+H7	$74,240	$18,560	$18,560	$18,560
	Risk adjustment	↑10%				
Htr	Implementation and training costs (risk-adjusted)		$81,664	$20,416	$20,416	$20,416
	Three-year total: $142,912		**Three-year present value: $132,436**			

EMPLOYEE MANAGEMENT TIME

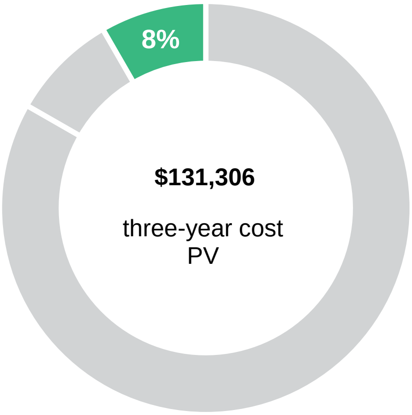
Evidence and data. Interviewees noted that management of ReliaQuest was typically minimal and consisted of communication with ReliaQuest representatives, planning for and making required systems updates, and onboarding new users.

Modeling and assumptions. For the composite organization Forrester assumes that the composite organization dedicates two product managers to handle all aspects of platform management. These employees spend an average of 20% of their time attending to tasks associated with ReliaQuest and their average annual salary is $120,000.

Risks. The following risk factors may affect the extent to which an organization experiences these benefits:

Internal management costs will vary based on organizational polices around system upgrades and the number of new users onboarded to ReliaQuest each year. This difference could change the costs associated with the solution.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of approximately $131,000.

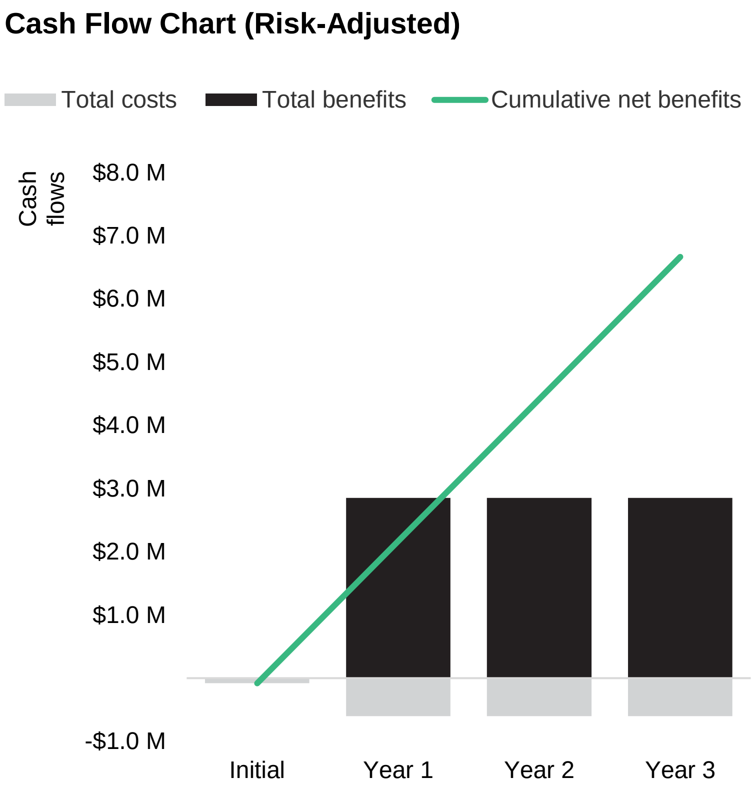


Employee Management Time

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	Number of employees tasked with managing ReliaQuest	Assumption		2	2	2
I2	Percent of time spent managing ReliaQuest	Interviews		20%	20%	20%
I3	Fully burdened compensation for employees tasked with managing ReliaQuest	Assumption		$120,000	$120,000	$120,000
It	Employee management time	I1*I2*I3	$0	$48,000	$48,000	$48,000
	Risk adjustment	↑10%				
Itr	Employee management time (risk-adjusted)		$0	$52,800	$52,800	$52,800
	Three-year total: $158,400		**Three-year present value: $131,306**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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	($81,664)	($601,216)	($601,216)	($601,216)	($1,885,312)	($1,576,800)
Total benefits	$0	$2,850,358	$2,850,358	$2,850,358	$8,551,075	$7,088,420
Net benefits	($81,664)	$2,249,142	$2,249,142	$2,249,142	$6,665,763	$5,511,620
ROI						350%
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] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

FORRESTER®