Table Of Contents

Executive Summary **1**
- Key Findings 1
- TEI Framework And Methodology 4

The QRadar Customer Journey **5**
- Interviewed Organization 5
- Key Challenges 5
- Solution Requirements 5
- Key Results 6

Analysis Of Benefits **8**
- Benefit 1: Improved Speed And Effectiveness In Threat Detection 8
- Benefit 2: Improved Speed In Threat Response 9
- Benefit 3: Reduced Investigative Workload 10
- Benefit 4: Compliance Reporting Efficiency 11
- Benefit 5: Legacy Security Solution Savings 12
- Flexibility 12

Analysis Of Costs **14**
- Cost 1: IBM QRadar License Cost 14
- Cost 2: Implementation And Deployment Cost 15
- Cost 3: Cost Of SOC Resources 16

Financial Summary **18**

IBM QRadar: Overview **19**

Appendix A: Total Economic Impact **20**

Appendix B: Supplemental Material **21**

Project Director:
Sean McCormick

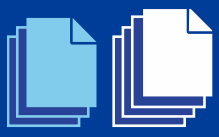
ABOUT FORRESTER CONSULTING

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

FORRESTER®

Benefits And Costs

Improved threat detection:
$1,631,344



Reduced investigative workload:
$2,025,461

IBM QRadar license costs:
$5,048,986

Executive Summary

IBM provides a cybersecurity intelligence platform that enables its customers to strengthen their security processes while improving their ability to detect and act upon threats. IBM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying QRadar. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of QRadar on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer with several years of experience using QRadar. IBM QRadar Security Intelligence Platform is a family of offerings that includes QRadar and a unified architecture that integrates security information and event management (SIEM), anomaly detection, incident forensics, incident investigation, and vulnerability management. QRadar natively takes feeds from 450 data sources and can be deployed on-premises, in the cloud, and via software-as-a-service (SaaS). The advanced security analytics engine is included as part of the base offering to detect advanced threats. QRadar User Behavior Analytics is available as an app to monitor user behavior. Some case management workflows are included, and additional automation and orchestration is available through IBM's recent acquisition of Resilient.[1]

Prior to using QRadar, the interviewed customer was utilizing a non-IBM managed security service provider (MSSP) for security monitoring and response. However, after many years, the MSSP was not meeting their needs and the customer still required a lot of internal resources to ensure logs were provided to the MSSP accurately. More importantly, security threats were being missed, thereby leaving the customer exposed to incidents that they would have to deal with alone. The interviewed customer said: “There was a lot of true positives being missed. For every one identified, two or three were missed.” After deciding to insource their security monitoring and response, the interviewed organization adopted IBM QRadar as it met all their requirements and was more flexible with its standard capabilities. They soon found that QRadar was much more effective at detecting threats and enabling their security operations center (SOC) to act upon these threats much faster, saying: “ . . . previously, we were detecting 30 incidents per day, many of which were false positives. Now we see 50 per day, but they are much more concrete and actionable.”

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **IBM QRadar improves the speed and effectiveness of detecting threats.** With IBM QRadar, the interviewed organization was able to detect more incidents faster than with their previous solution, helping to reduce the overall risk of a large incident or breach from occurring. The organization told Forrester that, on average, three out of four threats were going undetected with their previous solution, but with QRadar, nearly 75% more incidents were being detected and an even higher percentage were actionable threats. Over three years, this resulted in a risk avoidance of over $1.6 million for the interviewed organization.

FORRESTER®

ROI
35%

Benefits PV
$14.1 million

NPV
$3.6 million

Payback
17 months

- **With more information in one place, QRadar helped improve incident response times by 75%.** Prior to adopting QRadar, the interviewed organization only had access to simplified view of the MSSP's tool and therefore did not have all the information needed to appropriately respond to incidents. In addition, insourcing their monitoring and response activities enabled them to have a 24x7 internal monitoring and response team within their SOC. Altogether, this helped improve their incident response time by 75% leading to $656,000 of annual risk avoidance.
- **Fewer endpoint forensic investigations were required saving $2 million over three years.** Due to the improved detection and response times, fewer endpoint forensic investigations were needed. With a team of 16 FTEs, this meant they were able to focus their time on other value-added tasks, like further refinement and definition in security rules. Overall, it was estimated that there was a 50% reduction in these types of investigations resulting in $2 million of savings over three years.
- **Compliance reporting became more efficient with IBM QRadar leading to $135,019 in productivity savings.** The interviewed organization was responsible for quarterly Sarbanes-Oxley (SOX) audits as well as an external compliance audit that lasted two months every three years. It was stated that with IBM's built-in reporting, the interviewed company was able to satisfy the compliance requirements with half the resources. This led to $135,019 in savings over three years.
- **Legacy technology cost savings of $8.7 million.** The interviewed organization was able to avoid spending nearly $8.7 million with their former MSSP after adopting IBM QRadar and insourcing their monitoring and reporting tasks.

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

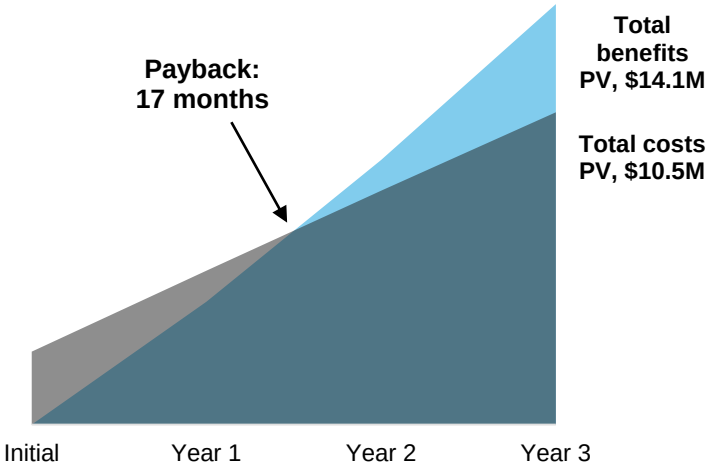
- **Improved effectiveness and maturity in cybersecurity processes.** The interviewed organization was able to leverage IBM QRadar to improve their cybersecurity processes and be more effective in threat detection and incident response. Based on a maturity assessment conducted after the adoption of IBM QRadar, it was reported that security maturity increased from 2.1 to 3.3 on a scale of 5.
- **Integration with other third-party apps helps improve productivity and automate response.** QRadar has pre-built integrations with many third-party apps, giving the customer the ability to visualize their entire environment in one system. The interviewee said, "we've found a lot of useful apps running with QRadar which has given us better visibility into offenses across our entire network."

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

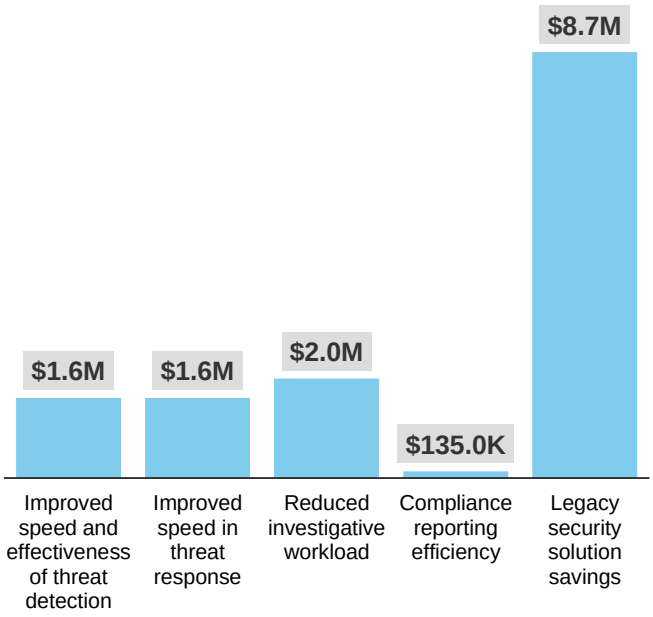
- **IBM QRadar initial license, add-on licenses, and ongoing support and maintenance fees for a large customer resulted in $5 million of expense over three years**. As one of IBM's largest customers, an initial purchase of appliances and licensing to support 50,000 events per second was made. This grew in years 2 and 3 to 100,000 events per second and along with a further investment that included 1.9 million flows per minute with IBM QFlows, resulted in additional costs of $1,000,000 per year. In addition, IBM provides annual support and maintenance to their customers at a cost of roughly 20% of the initial license fee. Over three years, the interviewed organization paid $5,048,986 to IBM for QRadar. A typical deployment for small customers would cost roughly $155,000 over three years, while a midsize deployment would equate to $645,000 million over three years.
- **Professional services costs during implementation and deployment resulted in $701,250.** Implementation and deployment took approximately five months. During this time, IBM Global Services was hired to help develop monitoring and response procedures, runbooks, and training. In total, $550,000 was paid to IBM for implementation and an additional $151,250 was incurred for internal resources to support the deployment.
- **Fourteen additional security resources were added to insource monitoring and response.** When the decision was made to insource monitoring and response activities in lieu of the MSSP, the interviewed organization needed to hire additional resources. Three security engineers and 11 security analysts of varying experience were hired at an average fully loaded salary of $110,000. Over three years, the interviewed organization incurred $4.6 million in added headcount expense.

Forrester's interview with the customer and subsequent financial analysis found that the interviewed organization experienced benefits of $14.1 million over three years versus costs of $10.5 million, adding up to a net present value (NPV) of $3.6 million and an ROI of 35%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

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

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 IBM QRadar can have on an organization:

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

DUE DILIGENCE
Interviewed IBM stakeholders and Forrester analysts to gather data relative to QRadar.

CUSTOMER INTERVIEW
Interviewed one organization using QRadar to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organization.

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

The QRadar Customer Journey

BEFORE AND AFTER THE QRADAR INVESTMENT

Interviewed Organization

For this study, Forrester interviewed one of IBM's largest QRadar customers:

- A US-based utility company with more than $20 billion in annual revenue.
- They employ 32,000 people including contractors.
- Operate a corporate network with 30,000 workstations and an operational network linking industrial control systems and other utility systems.
- They have 150 employees in the security operations center (SOC), with a team of 35 dedicated to security monitoring and incident response. This team is the main user of IBM QRadar.

Key Challenges

Prior to adopting QRadar, the interviewed organization utilized a managed security service provider for security monitoring and experienced the following challenges:

- **Inflexible service with a lack of understanding for their business.** The MSSP used a pre-built set of security monitoring use cases and had a minimal ability to customize to the needs of the interviewed organization. In addition, they lacked an understanding of their business as they had no specific skills or expertise in operational control systems. This meant they couldn't understand how and why devices (endpoints) and firewalls behaved the way they did leading to more false positive alerts than what was acceptable.
- **Poor threat detection led to attack vulnerability.** Even though there was a high degree of false positive alerts, the MSSP was missing a lot of true positive threats. According to the interviewee, only about one out of four true positives were being detected. This left the interviewed organization vulnerable to attacks and escalating incidents.
- **High degree of internal resource support.** With so many false positives and escalating attacks, the interviewed security leader still needed resources to respond and follow-up on alerts and incidents. The security team of 16 devoted considerable time to performing on-site investigations and forensics. The security team lacked visibility to log data needed for investigations and didn't have access to detailed security context in tickets which were created by the MSSP. This made incident investigations challenging and inefficient.

> "There were a lot of true positives being missed. For every one identified, two or three were missed."
>
> *Cybersecurity director, utility company*

Solution Requirements

The interviewed organization searched for a solution that could:

- Enable them to insource their security monitoring and response using mostly out-of-the-box rules and use cases that don't require much customization and tuning.
- Detect threats better than their existing MSSP.

- Flexibly meet their needs.

After an extensive RFP and business case process evaluating five to seven leading SIEM vendors, the interviewed organization chose IBM QRadar and began deployment.

- Initially, the interviewed organization hired 14 security FTEs. Three security engineers helped bridge the gap between system admins and security analysts. These engineers helped to define monitoring and response use cases, develop rules and configurations, and identify log and event sources. In addition, 11 monitoring and response analysts were hired; the harder role to fill. This effort took approximately two months and required the cybersecurity director to partner with HR to draft job descriptions, review resumes, and interview candidates. The interviewee estimated this took about 20% of his time, however, there was always about a 10% vacancy due to turnover which required 10% of his time in an ongoing capacity.
- IBM Global Services was hired to provide professional service support throughout the implementation and deployment of QRadar. IBM developed monitoring and response procedures, runbooks, training materials, and introduced proper change management practices. In total, IBM Global Services engaged the interviewed organization for five months.
- In addition to the professional service support, three internal FTEs spent six months focused on integration, deployment, and configuration of the QRadar appliances. This included the build-out of business specific customizations to enhance security and reduce false positives.

Key Results

The interview revealed that key results from the QRadar investment include:

- **Improved threat detection and speed in detection.** With the adoption of IBM QRadar, the interviewed organization was able to improve the number of threats detected, i.e., the amount of true positives, while reducing the number of false positives. Prior to adopting QRadar, the MSSP was detecting an average of 30 incidents per day, which were mostly false positives, known anomalous activity, or not always actionable incidents. QRadar improved the interviewed organization's ability to customize rules to their business allowing them to reduce the false positives all the while improving their ability to detect threats. Furthermore, the interviewed organization integrated QRadar QFlow, a layer 7 network activity monitoring capability. Adding QFlow gave analysts additional visibility into network and application behavior beyond what is captured in log data. This additional visibility enhanced threat detection and the analysts' ability to quickly respond to threats. The interviewed organization reported that this combination enabled them to detect an average of 50 incidents per day that were much more actionable than the 30 incidents detected by the MSSP.

> "Our response is much more effective with QRadar. We can now work the incident through until closure quicker and more effectively by leveraging QRadar."
>
> *Cybersecurity director, utility company*

- **Faster incident response time reducing the risk of escalating incidents.** Prior to insourcing their security monitoring and response, the MSSP provided high-priority incident escalation 24x7, but the internal SOC only operated on a 40-hour workweek. Through the insourcing effort, the interviewee was able to establish a 24x7 internal SOC team. This helped them to improve incident response SLAs. Formerly, they operated on an eight-hour SLA and averaged four hours for incident response. With the 24x7 SOC, and the data available in IBM QRadar, they were able respond to incidents within one hour on average. Incident response was also more effective as more detailed threat information, which included the incident description, the log data or flow data, and threat intelligence, was available to analysts. The interviewee stated, "QRadar sped up and improved our ability to respond to incidents as the log and flow data is right there in QRadar." Previously, with the MSSP, the analysts didn't have access to the full tool and only had a simplified view through the vendor's ticket portal. The portal only contained recent log files the MSSP thought would be useful, but the analysts weren't able to access the incident in the tool. The interviewee said: "Our response is much more effective with QRadar. We can now work the incident through until closure quicker and more effectively by leveraging QRadar." Overall, they were able to improve their time to respond by 75% reducing the risk of small incidents escalating into large incidents.
- **Efficiencies in investigations and compliance reporting.** With the improved threat detection and response, and the ability to analyze logs and network flows in IBM QRadar, the interviewed organization was able to reduce the amount of local inspections and endpoint forensic investigations by 50%. This allowed FTEs to investigate twice the number of incidents as they could previously. Ultimately, this enabled the interviewed organization to create new rules providing better coverage and more depth in their detection rules. Furthermore, as a heavily regulated organization, the interviewed company experienced improvements in compliance reporting. With greater visibility into network flows and log files, data needed for internal SOX controls and regulation evidence was easily supplied on an ongoing basis. About once every three years, a two-month special audit was performed. This took quite a bit more effort during that time frame, but it was assumed to be 50% more efficient with IBM QRadar. As mentioned by the interviewee, "We heavily use QRadar for compliance, it's really helped speed up our SOX audits by making it quicker and easier to gather the evidence needed."
- **Improved security maturity with added capabilities.** With the investment in IBM QRadar came new capabilities and increased flexibility in rule definitions. The interviewee said, "QRadar gave us more flexibility with the standard capabilities in which rules are in place and how configurations are tuned." QRadar also has apps that can run on top of it allowing the interviewed organization to gain better visibility into their environment from a single interface. In addition, they could now incorporate anomaly detection capabilities allowing them to dynamically build baselines and set alerts to be generated when activity exceeds baselines. With QRadar, the interviewed organization was able to improve their security processes. A maturity assessment was performed before and after adoption of QRadar. The results demonstrated an improvement from 2.1 to 3.3 on a 5-point scale. The interviewee said, "With QRadar, we were much more effective for the same amount of money."

"We heavily use QRadar for compliance, it's really helped speed up our SOX audits by making it quicker and easier to gather the evidence needed."

Cybersecurity director, utility company

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Improved speed and effectiveness of threat detection	$655,988	$655,988	$655,988	$1,967,963	$1,631,344
Btr	Improved speed in threat response	$655,988	$655,988	$655,988	$1,967,963	$1,631,344
Ctr	Reduced investigative workload	$792,000	$815,760	$840,233	$2,447,993	$2,025,461
Dtr	Compliance reporting efficiency	$49,500	$61,182	$52,515	$163,197	$135,019
Etr	Legacy security solution savings	$2,375,000	$3,562,500	$4,750,000	$10,687,500	$8,672,051
	Total benefits (risk-adjusted)	**$4,528,475**	**$5,751,417**	**$6,954,722**	**$17,234,614**	**$14,095,219**

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of more than $14.1 million.

Benefit 1: Improved Speed And Effectiveness In Threat Detection

With IBM QRadar, security analysts have access to more information in a single interface. This allows them to further refine and develop new rules to increase the effectiveness and speed in which threats are detected. A 75% improvement in threat detection was reported by the interviewed organization after implementing QRadar. This helped the organization lower the probability of an incident becoming a breach.

To model the value of this benefit, the following assumptions were made:

- The average cost of a breach or large incident involving 10,000 records or more is $7,350,000. This is specific to US-based companies published by Ponemon in their 2017 study.[2]
- The probability for an average organization of experiencing a breach or large incident involving 1,000 records or more is 14% in a given year. [3]

The improvement in threat detection can vary with:

- The types of threats and the effectiveness of the previous solution to detect those threats.
- The industry in which an organization operates, as some industries have higher probabilities and breach costs.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $1,631,344.

IBM QRadar improves threat detection by 75%.

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

Improved Speed And Effectiveness In Threat Detection: Calculation Table					
REF.	**METRIC**	**CALC./SOURCE**	**YEAR 1**	**YEAR 2**	**YEAR 3**
A1	Average cost of breach or large incident	Ponemon study	$7,350,000	$7,350,000	$7,350,000
A2	Average probability of breach or large incident	Ponemon study	14%	14%	14%
A3	Percentage improvement in detecting threats with QRadar		75%	75%	75%
At	Improved speed and effectiveness in threat detection	A1*A2*A3	$771,750	$771,750	$771,750
	Risk adjustment	↓15%			
Atr	**Improved speed and effectiveness in threat detection (risk-adjusted)**		**$655,988**	**$655,988**	**$655,988**

Benefit 2: Improved Speed In Threat Response

Secondary to detection of threats is the response time. The interviewed organization was able to improve their time to respond to threats by up to 75%. With a 24x7 SOC, the analysts had faster access to the data that mattered. This helped reduce the average response time to an incident from four hours down to one hour.

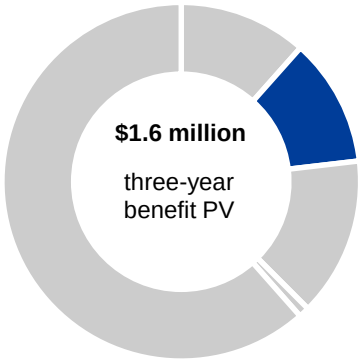
For the interviewed organization, Forrester assumes that:

- The average cost of a breach or large incident involving 10,000 records or more is $7,350,000. This is specific to US-based companies published by Ponemon in their 2017 study.[4]
- The probability of an average organization experiencing a breach or large incident involving 1,000 records or more in a given year is 14%.[5]
- By adopting IBM QRadar, the interviewed organization saw a 75% improvement in threat response time. This helped the organization lower the probability of an incident escalating and helped reduce the overall cost of incidents.

The reduction in software development expense will vary with:

- The types of threats and the availability of data with the previous solution.
- The industry in which an organization operates, as some industries have higher probabilities and breach costs.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $1.6 million.



Improved speed in threat response: **12%** of total benefits

FORRESTER®

Improved Speed In Threat Response: Calculation Table					
REF.	**METRIC**	**CALC./SOURCE**	**YEAR 1**	**YEAR 2**	**YEAR 3**
B1	Average cost of breach or large incident	Ponemon study	$7,350,000	7,350,000	7,350,000
B2	Average probability of breach or large incident	Ponemon study	14%	14%	14%
B3	Percentage improvement in response time to threats with QRadar		75%	75%	75%
Bt	Improved speed in threat response	B1*B2*B3	$771,750	$771,750	$771,750
	Risk adjustment	↓15%			
Btr	**Improved speed in threat response (risk-adjusted)**		**$655,988**	**$655,988**	**$655,988**

Benefit 3: Reduced Investigative Workload

With improvements in threat detection and response, the interviewed organization was able to reduce the number of forensic investigations by 50%. This allowed the interviewed organization to further allocate their resources' time to improving rules and configurations, ultimately creating a more secure environment. This cycle repeats itself, saving more time and enabling analysts to be proactive rather than reactive.

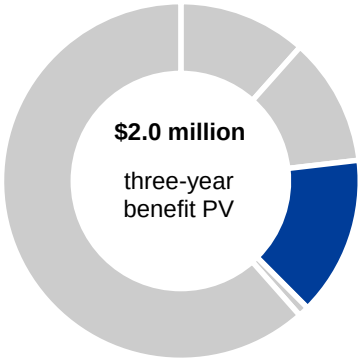
For the interviewed organization, Forrester assumes that:

- Sixteen FTEs were involved in endpoint forensics and localized response activities.
- The cost of an average security analyst FTE, fully loaded, is $110,000 per year.
- IBM QRadar helps reduce the number of investigations by 50%.

The reduction in investigative workload can vary by:

- The amount of investigations initially taking place and the location of devices.
- The number of resources dedicated to investigations.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $2,025,461.



Reduced investigative workload: **14%** of total benefits

Reduced Investigative Workload: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
C1	Number of FTEs involved in investigations		16	16	16
C2	Percent of investigations avoided		50%	50%	50%
C3	Average cost per FTE		$110,000	$113,300	$116,699
Ct	Reduced investigative workload	C1*C2*C3	$880,000	$906,400	$933,592
	Risk adjustment	↓10%			
Ctr	**Reduced investigative workload (risk-adjusted)**		**$792,000**	**$815,760**	**$840,233**

FORRESTER®

Benefit 4: Compliance Reporting Efficiency

Being in a heavily regulated industry, the interviewed organization had to satisfy ongoing SOX audits and a once every three-year industry-specific audit. Historically, this was a resource and time-intensive process as the interviewee would have to request specific data from the MSSP to satisfy the tests. With IBM QRadar, not only could analysts quickly and easily access the information they needed, but reports were developed as evidence to satisfy auditors' requirements.

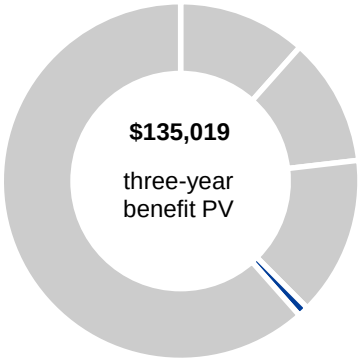
For the interviewed organization, Forrester assumes that:

- One FTE was used prior to investing in QRadar for ongoing SOX audits and an additional FTE was needed for two months during the industry-specific audit.
- The interviewed organization was able to improve compliance reporting efficiency by 50%.

The efficiency gained in compliance reporting can vary with:

- The historical ability to access required information and the sophistication of existing reporting.
- The industry in which an organization operates as some industries have different regulations that need to be met.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $135,019.



Compliance reporting efficiency: **1%** of total benefits

Compliance Reporting Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Ongoing quarterly compliance reporting (FTE)		1.0	1.0	1.0
D2	Effort for three-year audit (FTE)	One FTE/12 months *2 months	0.00	0.20	0.00
D3	Compliance reporting efficiency gain		50%	50%	50%
D4	Average cost per FTE		$110,000	$113,300	$116,699
Dt	Compliance reporting efficiency	(D1+D2)*D3*D4	$55,000	$67,980	$58,350
	Risk adjustment	↓10%			
Dtr	**Compliance reporting efficiency (risk-adjusted)**		**$49,500**	**$61,182**	**$52,515**

FORRESTER®

Benefit 5: Legacy Security Solution Savings

While there are many organizations that utilize a MSSP in conjunction with QRadar, the interviewed company chose to insource their security operations after adopting IBM QRadar. Historically, they had used a non-IBM MSSP that cost them $2.5 million per year. While there is an offsetting cost to hire resources in order to take the place of the MSSP, the interviewed organization found it to cost less than paying an MSSP. In addition, they now had more control over their data and security.

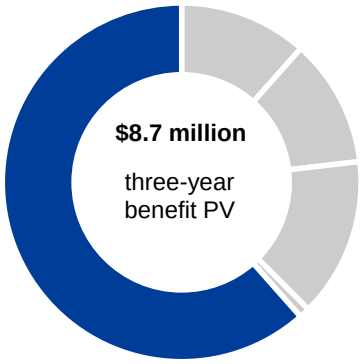
For the interviewed organization, Forrester assumes that:

- After discontinuing the use of an MSSP, $2.5 million was avoided in the first year.
- The cost avoidance for the MSSP would have grown based on the consumption demands similar the IBM QRadar license costs.

The reduction in legacy security solution savings can vary with:

- The amount of data consumed by the MSSP and the pricing model of the MSSP.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $8,672,051.



Legacy security solution savings: **61%** of total benefits

Legacy Security Solution Savings: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
E1	Annual cost for legacy security solution (MSSP)		$2,500,000	$2,500,000	$3,750,000
E2	Annual demand growth rate			50.0%	33.3%
Et	Legacy security solution savings	E1*(1+E2)	$2,500,000	$3,750,000	$5,000,000
	Risk adjustment	↓5%			
Etr	**Legacy security solution savings (risk-adjusted)**		**$2,375,000**	**$3,562,500**	**$4,750,000**

Flexibility

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

- **IBM QRadar Advisor with Watson enables organizations to accelerate incident analysis and rapidly respond to threats.** With IBM Watson, artificial intelligence (AI) can be applied to proactively analyze threats, determine the threat's relevance, and provide additional context about the threat to the analyst. This additional analysis and context gathering speeds investigations and gives analysts a guide for incident handling. Given the skills shortage in the security space, organizations have the option to utilize IBM Watson to reduce false positives, increase analyst efficiency, and increase response times.

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

FORRESTER®

- **With IBM's User Behavioral Analytics (UBA) organizations can gain visibility into behavioral anomalies that may signal insider threats.** UBA helps security teams analyze user activity and find out if insiders are behaving in a suspicious or potentially malicious manner. Combining UBA with log, event, and flow data gives analysts the ability to detect suspicious behavior and conduct an efficient investigation. Behavioral analysis also detects activities that may be missed by a rules-only approach.

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

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ft	IBM QRadar license cost	$1,400,000	$1,280,000	$1,480,000	$1,680,000	$5,840,000	$5,048,986
Gtr	Implementation and deployment cost	$731,500	$0	$0	$0	$731,500	$731,500
Htr	Cost of SOC resources	$313,133	$1,709,400	$1,760,682	$1,813,502	$5,596,718	$4,684,754
	Total costs (risk-adjusted)	**$2,444,633**	**$2,989,400**	**$3,240,682**	**$3,493,502**	**$12,168,218**	**$10,465,240**

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of less than $10.5 million.

Cost 1: IBM QRadar License Cost

The interviewed organization purchased IBM QRadar for an initial cost of $1.4 million. As one of the largest IBM customers, this license was a consumption-based license covering 50,000 events per second. Over the course of the following three years, the interviewed organization's demand grew to over 100,000 events per second. Additionally, a further investment in IBM QFlow was made to analyze their network data. This license covered 1.9 million flows per minute.

For the interviewed organization Forrester assumed:

- An annual support and maintenance charge of 20% of the original license cost would be assessed.
- Initial licensing included QRadar SIEM appliances with high availability (HA), event processing with HA, and 50,000 events per second.
- Additional licenses included more data nodes, QRadar Incident Forensics including full packet capture, and an additional 50,000 events per second.
- Licensing for 1.9 million flows per minute with IBM QFlows.

The cost of licenses will vary with the number of events per second and flows per minute needed. In addition, the interviewed organization was much larger than the average customer. For a typical organization with 2,500 events per second, the initial licensing cost would be closer to $77,040. For a typical organization with 10,000 events per second and 200,000 flows per minute, the initial licensing cost would be closer to $359,500. The table below illustrates the costs for a typical small and midsize deployment over three years.

IBM QRadar Typical License Costs For Small Organizations						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
X1	Events per second		2,500		2,500	
X2	Flows per minute					
X3	License and infrastructure cost paid to IBM		$77,040		$35,400	
X4	Ongoing maintenance and support cost	$20\%*X3_{previousyear} + X4_{previousyear}*1.1$		$15,405	$16,949	$25,724
Xt	**IBM QRadar license cost for small organizations**	**X3+X4**	**$77,040**	**$15,405**	**$52,349**	**$25,724**

IBM QRadar Typical License Costs For Midsize Organizations						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
Y1	Events per second		10,000	5,000		
Y2	Flows per minute		200,000			
Y3	License and infrastructure cost paid to IBM		$359,500	$70,800		
Y4	Ongoing maintenance and support cost	$20\%*Y3_{previousyear} + Y4_{previousyear}*1.1$		$71,900	$93,250	$102,575
Yt	**IBM QRadar license cost for midsize organizations**	**Y3+Y4**	**$359,500**	**$142,700**	**$93,250**	**$102,575**

IBM QRadar License Cost: Calculation Table For Interviewed Organization						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	License and infrastructure cost paid to IBM		1,400,000	1,000,000	1,000,000	1,000,000
F2	Ongoing maintenance and support cost	$20\%* Sum(F1_{initial} :F1_{previous year})$		280,000	480,000	680,000
Ft	**IBM QRadar license cost**	**F1+F2**	**$1,400,000**	**$1,280,000**	**$1,480,000**	**$1,680,000**

Cost 2: Implementation And Deployment Cost

The interviewed organization spent six months implementing QRadar. They had three FTEs working internally to support the deployment and hired IBM Global Services for five months to help define rules and configure the system.

Forrester assumed the following for the interviewed organization:

- IBM professional services cost of $100,000 per month for five months.
- The cost of an average security analyst FTE, fully loaded, is $110,000 per year.

The implementation and deployment costs vary with:

- The complexity of the deployment and the amount of configurations required.

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

- The third-party professional service hired, and the quality of service provided.
- The amount of internal resources versus third-party effort.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $731,500.

Implementation And Deployment Cost: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	IBM Professional Services cost per month		$100,000			
G2	Months required for implementation and deployment		5			
G3	Internal resources required for implementation (FTEs)		3			
G4	Average cost per FTE		$110,000			
Gt	Implementation and deployment cost	G1*G2+(G3*(G4/12*6))	$665,000	$0	$0	$0
	Risk adjustment	↑10%	□			
Gtr	**Implementation and deployment cost (risk-adjusted)**		**$731,500**	**$0**	**$0**	**$0**

Cost 3: Cost Of SOC Resources

The interviewed organization insourced monitoring and response activities after adopting IBM QRadar and discontinuing services with their former MSSP. The director of the SOC spent two months initially hiring analysts and engineers to build out his team. Overall, the director hired fourteen security personnel. While maintaining a full SOC is a never-ending battle, the interviewee said they usually run at 90% capacity as they have consistent turnover.

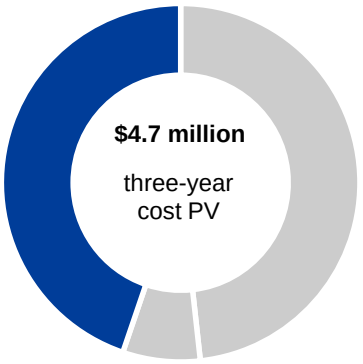
Forrester assumed the following for the interviewed organization:

- Initial hiring of 20% FTE and ongoing hiring of 10% FTE effort required by the director.
- The cost of an average security analyst FTE, fully loaded, is $110,000 per year. The cost of an average hiring manager, fully loaded, is $140,000 per year.
- Fourteen incremental resources were required to support the security insourcing effort.

The cost of resources and effort in hiring resources fluctuates with:

- The job location and local competitive salaries.
- The scarcity of resources and the level of expertise required.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $4,684,754.



Cost of SOC resources: **45%** of total costs

FORRESTER®

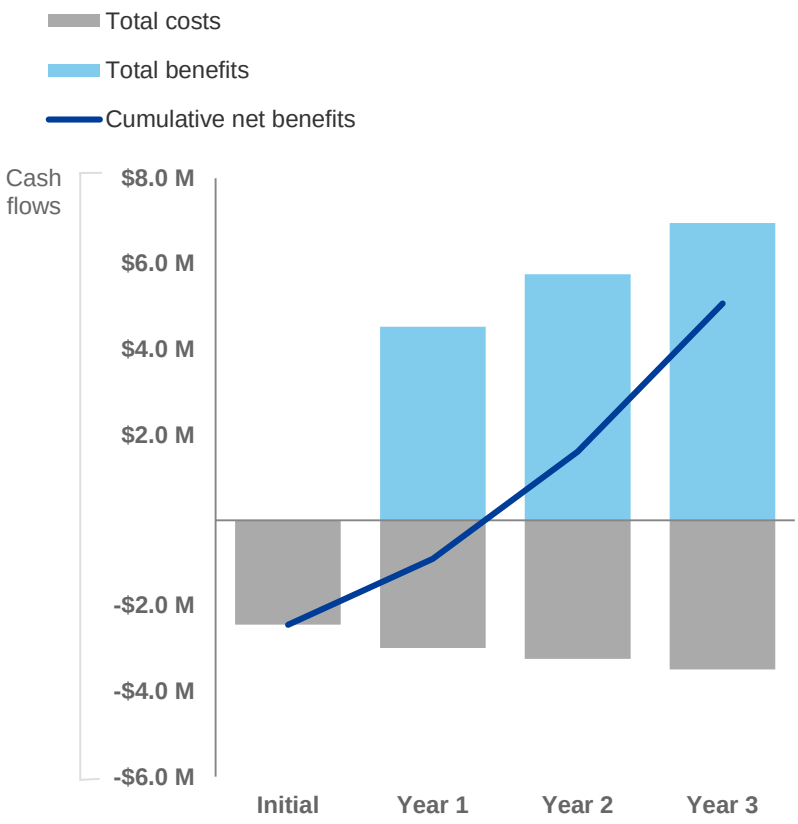
Cost Of SOC Resources: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
H1	Resources required for initial hiring and ongoing hiring (FTEs)		0.2	0.1	0.1	0.1
H2	Average cost per hiring FTE		140,000	140,000	144,200	148,526
H3	Cost of hiring SOC resources	H1*H2	$28,000	$14,000	$14,420	$14,853
H4	Additional resources required for SOC		14	14	14	14
H5	Months resources were required		2	12	12	12
H6	Average cost per FTE		$110,000	$110,000	$113,300	$116,699
H7	Cost of additional resources	H4*H5*H6	$256,667	$1,540,000	$1,586,200	$1,633,786
Ht	Cost of SOC resources	H3+H7	$284,667	$1,554,000	$1,600,620	$1,648,639
	Risk adjustment	↑10%				
Htr	Cost of SOC resources (risk-adjusted)		$313,133	$1,709,400	$1,760,682	$1,813,502

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 interviewed organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($2,444,633)	($2,989,400)	($3,240,682)	($3,493,502)	($12,168,218)	($10,465,240)
Total benefits	$0	$4,528,475	$5,751,417	$6,954,722	$17,234,614	$14,095,219
Net benefits	($2,444,633)	$1,539,075	$2,510,735	$3,461,220	$5,066,397	$3,629,979
ROI						35%
Payback period						17 months

FORRESTER®

IBM QRadar: Overview

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

The IBM QRadar Security Intelligence Platform is a comprehensive security analytics solution designed to help organizations filter through the network noise to gain real-time, actionable insight into risks and threats in their environment.

At the core of the solution is QRadar Security Information and Event Management (SIEM), which collects vast amounts of network, asset, cloud and user data and applies a series of advanced analytics to identify threats and uncover anomalies that may indicate an attack. The flexible platform can be deployed on-premises, in a public cloud, or consumed as SaaS. Optional components can easily be added to extend monitoring capabilities and address new use cases without making major infrastructure changes. Optional components include:

- **QRadar User Behavior Analytics:** seamlessly layers on top of QRadar SIEM to detect anomalous user activities that may indicate an insider has turned malicious or had their credentials compromised.
- **QRadar Advisor with Watson:** uses AI to automate steps in the investigation process and accelerate time-to-remediation by quickly uncovering the root cause and scope of a threat, as well as providing insight into the threat actors, likely end goals, and related observables that may be elsewhere in the environment.
- **QRadar Vulnerability Manager:** enriches the results of vulnerability scans by mapping vulnerability data to assets and asset configuration information to help organizations prioritize remediation efforts.
- **QRadar Network Insights:** inspects network activity in real-time to detect attacks, such as phishing schemes, lateral movement, and data exfiltration, and reconstructs session content to provide insight into application-level activity and aid in forensic investigations.
- **QRadar Incident Forensic:** retraces an attacker's actions step-by-step using full packet capture data, enabling analysts to more easily conduct in-depth forensic investigations.
- **QRadar Data Store:** serves as a log data lake, normalizing and storing log data and enabling security analysts to run advanced search queries and optionally use the QRadar SDK to develop their own custom analytics.

Components of the IBM QRadar Security Intelligence Platform are fully integrated, enabling customers to start as small or large as they choose and easily scale up or down as their needs change. With over 500 validated out-of-the-box integrations and preconfigured rules, customers can get up and running quickly and easily add on new capabilities through the IBM Security App Exchange. Learn more at www.ibm.com/qradar.

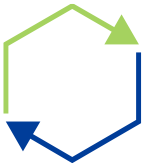
Appendix A: Total Economic Impact

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: Supplemental Material

Related Forrester Research

[1] Source: "Vendor Landscape: Security Analytics (SA)," Forrester Research, Inc., November 15, 2016.

Online Resources

[2] Source: Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN).
[3] Source: The True Cost of Compliance with Data Protection Regulations (https://www.ponemon.org/news-2/80).
[4] Source: Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN).
[5] Source: The True Cost of Compliance with Data Protection Regulations (https://www.ponemon.org/news-2/80).