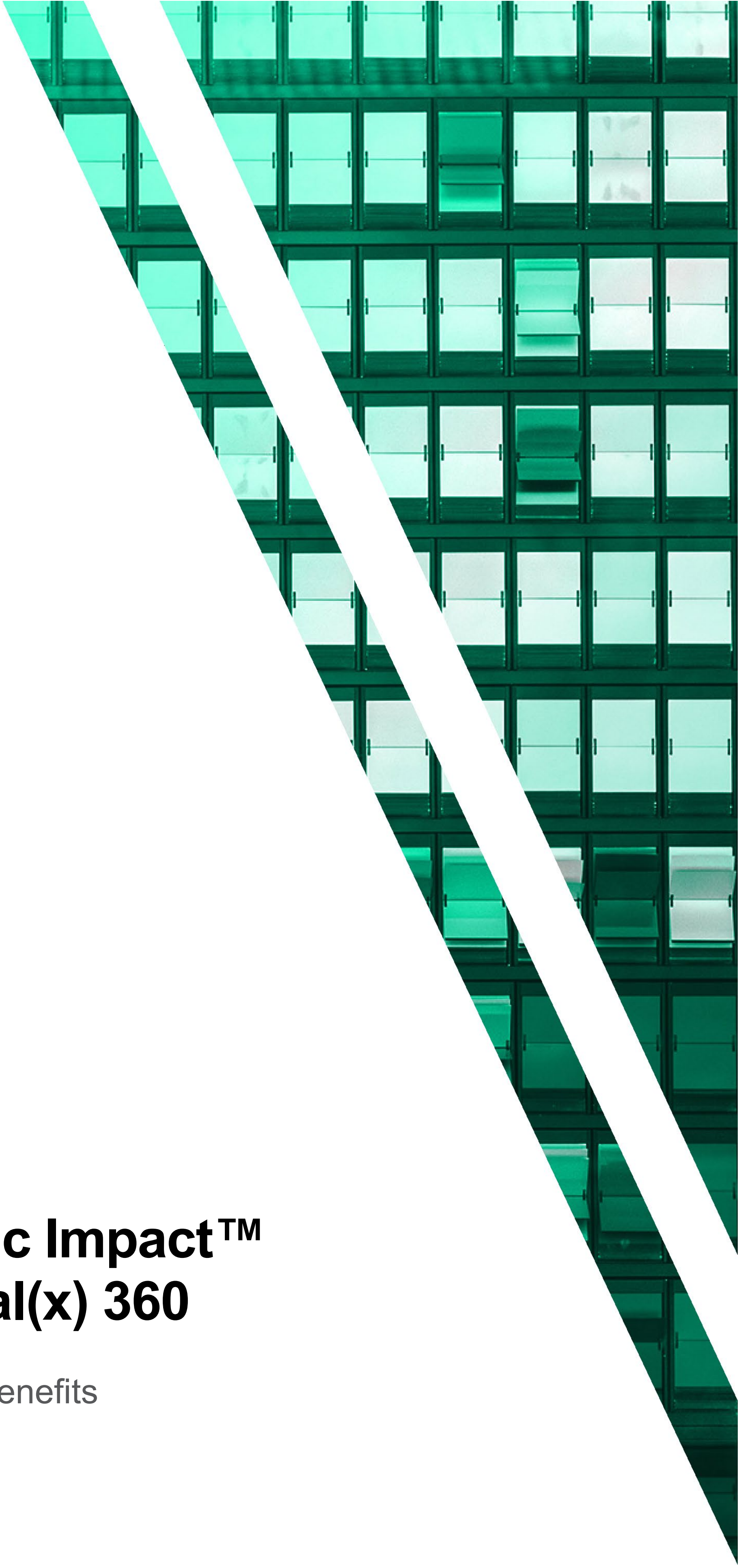
FORRESTER®



The Total Economic Impact™ Of ExtraHop Reveal(x) 360

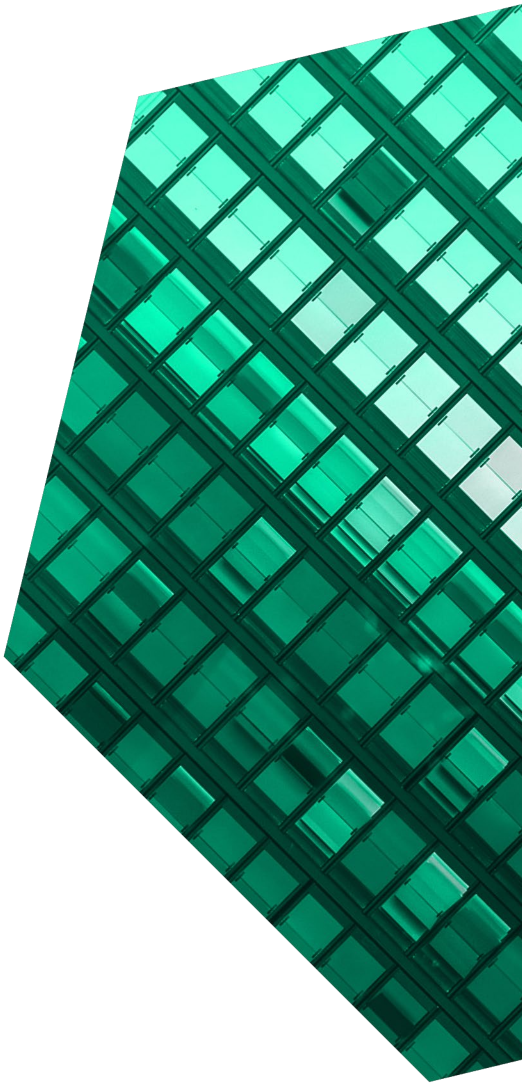
Cost Savings And Business Benefits Enabled By Reveal(x) 360

DECEMBER 2022

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY EXTRAHOP

Table Of Contents

Consulting Team: Sanitra Desai



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Detecting anomalies and enabling response require visibility into the entirety of the data and the totality of the network.[1] ExtraHop Reveal(x) 360 provides rich insight into traffic flow within your environment in both the north-south and east-west corridors to understand your network landscape. Using Reveal(x) 360, Forrester estimates an 86% reduction in time to respond to a threat and 1065 hours saved on responding to an outage per year, alongside improved end user productivity and savings from replacing pre-existing security solutions.

ExtraHop Reveal(x) 360 helps organizations detect and respond to advanced threats — before they compromise the business. ExtraHop applies cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across multicloud and hybrid environments. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence.

ExtraHop commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Reveal(x) 360.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Reveal(x) 360 on their organizations.

Reduction in time to threat resolution:

87%

KEY STATISTICS

Return on investment (ROI)
193%

Net present value (NPV)
$933K

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives with experience using Reveal(x) 360. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using Reveal(x) 360, interviewees reported that their organizations used a combination of firewalls, endpoint detection and response (EDR) products, security information and event management (SIEM) solutions, and packet capture tools. However, even with these technologies being fully operational, there were significant holes in the reported data. Additionally, with such a high number of tools, the organizations lacked a single source of truth. Security and network teams also had to spend extensive time and effort sifting through alerts, detecting and researching potential threats, and determining how to properly respond.

After the investment in Reveal(x) 360, interviewees' organizations saw a significant improvement in visibility into their network environment. With immediate insight into their network status across all environments, from on-premises to multicloud to distributed workforces and operations, alongside access to AI powered analysis, organizations could detect and respond to security threats at a much faster rate. Passive, ongoing monitoring of the network landscape meant organizations could respond to unplanned outages more efficiently as well as decrease downtime for employees.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Faster threat detection and resolution worth nearly $592,000.** With improved visibility and AI-powered analysis, Reveal(x) 360 decreases time to threat detection by 83% and time to threat resolution by 87%. In total, time to respond decreases 86%, from 11 hours to 1.5 hours, saving a total of 9.5 hours on each threat detection and resolution process.

- **Improved efficiency responding to unplanned outages valued at more than $138,000.** After implementing Reveal(x) 360 to continuously analyze network data and provide one unified view across the network landscape for all IT teams, unexpected outages decrease by 66%, the time needed to solve any unplanned outages decreases 92%, and the number of IT professionals involved in researching an outage decreases by 50%. Overall, the composite organization saves 1,065 hours on investigating unplanned outages.

- **Reduced end user downtime due to widespread unplanned outages resulting in savings worth more than $313,000.** With Reveal(x) 360, end users are less likely to be impacted by widespread unplanned outages that cause downtime, such as a network outage or a failed application, as outages can be troubleshooted and remediated faster. The organization is able to avoid three downtime events per year that result in 3 hours of downtime each for 1,000 end users. This could also decrease damage to the brand and loss of revenue.

- **Savings from retiring legacy security solutions worth nearly $373,000.** After improving network visibility with Reveal(x) 360, organizations are able to retire preexisting security solutions that they no longer needed.

> **"The network is the ground truth. It's what attackers can't avoid. You deploy Reveal(x) 360, [and] now you have the ability to see everything on the network. Without that data, you're operating partially or completely blind. And in my professional opinion, ExtraHop is the best tool to give you that visibility and insight you need to see clearly."**
>
> *Technical director, cybersecurity operations, communications*

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Expanded coverage.** Interviewees' organizations could secure more of their attack surface and monitor more types of attacks, including supply chain, ransomware, and lateral movement, once implementing Reveal(x) 360.

- **Improved communication.** Reveal(x) 360 helped drive alignment and collaboration across security and network teams. With access to one unified view into the network landscape, organizations could remove data siloes, ease the communication process, and be more agile in their response to security vulnerabilities.
- **Reduced risk of security breaches.** Reveal(x) 360 helped bolster customer security environments, potentially preventing security breaches worth millions of dollars in fines.
- **Improved leadership decision-making.** Access to more in-depth insight enabled leadership at the interviewees' organizations to make more informed decisions related to the network landscape in less time.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Fees to ExtraHop, including training and professional services.** ExtraHop offers Reveal(x) 360 at different tiers, ranging in average selling price (ASP) from $15,000 to $450,000 depending on attack surface coverage, number of business-critical devices, traffic throughput requirements, and other factors in the customer environment. Based on the composite organization's usage, this totals $444,000 over three years.
- **Internal implementation and ongoing management.** IT professionals are involved in the deployment and ongoing management of Reveal(x) 360. This costs the composite organization $34,000 over three years.
- **Training costs.** Minimal training is required for IT professionals to become proficient using Reveal(x) 360. This costs the composite organization $5,700 over three years.

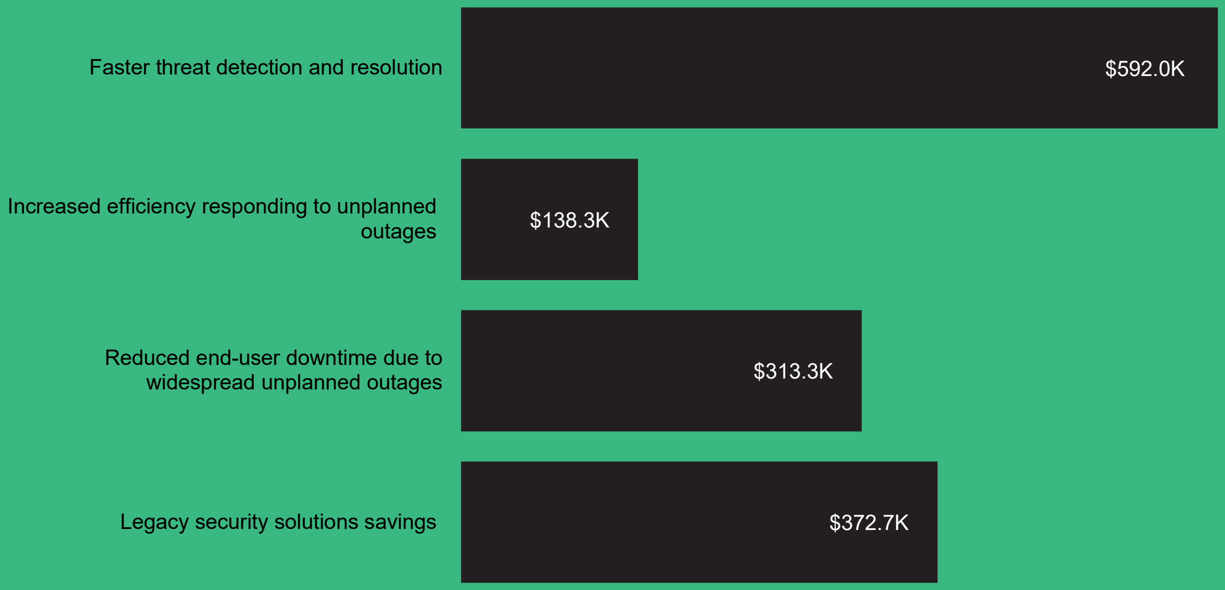
The representative interviews and financial analysis found that a composite organization experiences benefits of $1.42 million over three years versus costs of $484,000, adding up to a net present value (NPV) of $933,000 and an ROI of 193%.

ROI
193%

BENEFITS PV
$1.42M

NPV
$933K

Benefits (Three-Year)



> **“Because we have more visibility, we have a better understanding of what’s happening and what we can do. The Reveal(x) 360 platform has shifted our attitude from reactive to proactive.”**
>
> — Director of cybersecurity, financial services

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 Reveal(x) 360.

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 Reveal(x) 360 can have on an organization.

DUE DILIGENCE

Interviewed ExtraHop stakeholders and Forrester analysts to gather data relative to Reveal(x) 360.

INTERVIEWS

Interviewed five representatives at organizations using Reveal(x) 360 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 interviewees.

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 ExtraHop 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 Reveal(x) 360.

ExtraHop 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.

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

The ExtraHop Reveal(x) 360 Customer Journey

🟩 Drivers leading to the Reveal(x) 360 investment

Interviews

Role	Industry	Region	Revenue	Full-Time Employees
VP, IT risk management	Retail	North America	$9 billion	40,000
IT support analyst	Retail	North America	$9 billion	40,000
Director of cybersecurity	Utilities	North America	$5 billion	5,000
Technical director, cybersecurity operations	Communications	Global	$2 billion	6,000
Director of cybersecurity	Financial services	North America	$1 billion	1,000

KEY CHALLENGES

Prior to the investment in Reveal(x) 360, the interviewees' organizations used myriad tools to protect and glean insights into the status of their environments such as firewall, EDR, SIEM, and packet capture solutions. However, as organizations expanded their attack surface through scaling their business and introducing cloud applications and bring-your-own-device (BYOD) policies for hybrid remote workforces, IT teams were unable to keep up with the growing number of alerts and potential threats.

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

- **A complex environment lacking a single source of truth.** As potential threats continued to evolve and organizations expanded their environment to include more devices and on-premises and cloud workloads, IT teams found themselves with a collection of both security and network tools acquired over time for various functions and goals. This increased the operational complexity within their IT landscape.

  Organizations looked to create a more integrated and cost-effective environment. However, they also lacked a solution that could provide a single source of truth to begin the consolidation process and increase collaboration and trust across IT teams. The director of cybersecurity at a financial services organization said: "We lacked a common communication platform with a single view of our whole environment. We had network folks, security folks, application folks, and administration folks looking at their little piece of the puzzle. Getting everyone on the same page was impossible."

> **"We liked that Reveal(x) 360 could be used by the network team and security team. Also, their user interface is clean and extremely intuitive."**
>
> *Director of cybersecurity, utilities*

- **Limited visibility.** The interviewees' organizations had invested in multiple security solutions but still saw gaps at the network security level. Existing network tools focused on data on the availability side of the house, and existing security tools did not monitor the network layer. Additionally, organizations faced a visibility gap related to lateral movement, an increasingly prominent threat as attackers become more sophisticated. According to the technical director, cybersecurity operations, at a communications organization: "Our environment is fairly large and has a lot of bandwidth. With workloads both on-premises and in the cloud, we had more segmented visibility capabilities that were used by various operational teams throughout the organizations to examine and monitor their little piece of the pie. There was no real network or security analytic capability that could track an entry to exit of our network at scale."

> **"We could see the endpoints and we could see our servers, but we couldn't see anything in between. We needed Reveal(x) 360 to gain that visibility and ramp up threat response."**
>
> *Director of cybersecurity, financial services*

- **Inefficient security workflows.** Interviewees reported that their security workflows were extremely time-consuming in their legacy environment, largely due to limited visibility and an overabundance of security alerts and false positives hindering threat detection coupled with mostly manual investigation and remediation processes. The director of cybersecurity at a utilities organization said: "Our IT team was constantly frustrated because most of the alerts we would get were false positives, and there were so many alerts that our small team couldn't possibly sift through them all. We had no way of knowing what we actually needed to investigate." The VP, IT risk management at a retail organization stated, "It would take us days or even weeks to respond to an actual threat because we didn't have the AI/ML capabilities to find the threat quickly, classify how serious it was, establish the root cause, and respond intelligently across our entire network, from on-premises data centers to store locations to cloud workloads."

> **"We did a comparison, and ExtraHop outperformed everybody. They had the scaling capabilities we needed and the alert accuracy, granularity, and AI analytics capabilities we wanted. Reveal(x) 360 allows us to get complete visibility of the ground truth for our full network environment and make the right call when it came to identifying and removing bad traffic."**
>
> *Technical director, cybersecurity operations, communications*

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Provide a single source of truth across all assets in the enterprise, from cloud to on-premises to endpoints, as the organization scales.

- Improve visibility across the entire network, with the ability and added intelligence to detect advanced attacks and lateral movement.
- Introduce advanced AI/ML capabilities to ease the threat detection, investigation, and remediation processes for security teams.

> **"ExtraHop's platform enables us to deliver exceptional and secure customer experience at scale, with better visibility, detection, and investigation capabilities across our hybrid environment."**
>
> *Director of cybersecurity, financial services*

- Simplify IT management while encouraging communication and collaboration across IT teams with a cloud-based solution.

COMPOSITE ORGANIZATION

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

Description of composite. The multibillion-dollar organization serves customers both online and in brick-and-mortar branches. It has 5,000 employees consisting of remote workers and those distributed across its numerous locations. Of these, 25 use Reveal(x) 360, and users primarily consist of employees from the network and security teams.

Deployment characteristics. The organization previously deployed a packet-based network security tool and firewalls, an endpoint detection and response product, and a SIEM solution. However, it still struggled to gain full visibility into its hybrid environment and into east-west traffic to detect and respond to threats. Additionally, the organization saw an opportunity to save time remediating network outages by investing in a solution that can provide both broad and deep network visibility.

Key Assumptions

- **$5 billion annual revenue**
- **Widespread organization with distributed workforces and operations**
- **Hybrid environment (on-premises, multicloud, remote site)**
- **25 FTEs using Reveal(x) 360**
- **40 threats analyzed per month**

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	Faster threat detection and resolution	$238,032	$238,032	$238,032	$714,096	$591,950
Btr	Increased efficiency responding to unplanned outages	$55,593	$55,593	$55,593	$166,779	$138,252
Ctr	Reduced end-user downtime due to widespread unplanned outages	$126,000	$126,000	$126,000	$378,000	$313,343
Dtr	Legacy security solutions savings	$0	$160,000	$320,000	$480,000	$372,652
	Total benefits (risk-adjusted)	$419,625	$579,625	$739,625	$1,738,875	$1,416,197

FASTER THREAT DETECTION AND RESOLUTION

Evidence and data. With Reveal(x) 360 in place, organizations gained the visibility and AI-powered analysis needed to substantially decrease the time it took to detect, investigate, and resolve actual threats.

Before deploying Reveal(x) 360, the security solutions in place at the interviewees' organizations left gaps in network visibility. Additionally, older, packet-based network tools and firewall logs flooded security analysts with alerts, many of which were benign or false positives. These issues lengthened the threat remediation process, as it would require significant analyst effort to sift through alerts, validate whether or not a network anomaly was a true security threat, and if it was, decide how to adequately resolve the threat.

Conversely, Reveal(x) 360 passively observes everything on the network and instantly detects malicious activity like lateral movement, command and control, and privilege escalation, using cloud-scale machine learning and global threat intelligence. The platform provides high-fidelity, contextual alerts to prioritize the highest-risk threats and keep teams focused on what really matters.

> **"ExtraHop prioritizes alerts based on their potential risk and provides detailed information around each one. This allows us to really understand what's happening in our network to act and help us evolve our network landscape over time."**
>
> *Director of cybersecurity, utilities*

- According to the director of cybersecurity at a financial services company: "Detection went down from hours to days to hours to minutes because we can see things immediately on the console, instead of waiting for logs from the SIEM to get indexed and create the alert. We could be more proactive instead of reactive."
- Similarly, a communications organization decreased the time it took to detect an issue from multiple hours to seconds and minutes. "Pulling data, processing, transforming, and analyzing it

to detect something was a manual process, and it took hours. Meanwhile, the ExtraHop platform operates in real time," said the technical director, cybersecurity operations, at a communications organization.

- The IT support analyst at a retail organization said: "We used to get thousands of alerts per day with no context, and we couldn't even dig through them all because there were so many. And of the ones we did look at, a lot of them were false positives. We're now getting closer to 150 alerts per day, and these are more targeted, so we can detect an issue faster and take action."

Through access to the platform's cloud-based record store with 90-day lookback and intuitive investigative workflows, analysts could get answers quickly and plan their response. Native integrations enabled automated action on compromised workloads, domains, and IP addresses, which ultimately led to faster threat resolution. Additionally, a cloud-hosted control panel provided a unified view into a hybrid enterprise, which further accelerated the threat remediation process.

- The communications organization was able to stop attacks while they were happening instead of identifying attacks after the fact. The technical director, cybersecurity operations, explained: "The delay in our previous setup meant that often, by the time we were able to see something bad was happening, the attacker had switched, so everything we did was basically a waste. ExtraHop's passive detection capability allows us to craft detections with enough information to understand the mitigation action that needs to take place. Integrations allow us to resolve an attack within seconds."

- The VP, IT risk management, at a retail organization said: "The ExtraHop platform has been a huge time-saver. We now have all the data we need in one spot instead of having to go from system to system and using spreadsheets to map all the data points together."

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

- The composite organization detects and resolves 40 threats per month.
- The organization saves 2.5 hours on the threat detection process and 7 hours on the threat remediation process with Reveal(x) 360.
- The fully burdened hourly rate of an IT professional is $58.

> **"Previously, when we got an alert, an analyst would have to manually dig into it and figure out how to resolve it. It could take days, if not longer. Now, instead of having to look in a dozen systems and try to put data together to make a decision, it's one. Also, the data is more trustworthy. Reveal(x) 360 adds rich context to the threats it catches. It presents a better risk story to the analyst, allowing them to confidently respond."**
>
> *Technical director, cybersecurity operations, communications*

Risks. The improvement in threat detection and resolution time may vary depending on the following:

- The total number and complexity of threats detected and resolved annually.

Decreased time to remediate a security threat:

86%

- The prior time spent on each threat detection and resolution process.
- The skill level, efficiency, and salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of nearly $592,000.

Faster Threat Detection And Resolution

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of threats analyzed by an IT professional	Composite	480	480	480
A2	Mean time to detect: prior environment (hours)	Interviews	3	3	3
A3	Mean time to detect: new environment (hours)	Interviews	0.5	0.5	0.5
A4	Mean time to resolution: prior environment (hours)	Interviews	8	8	8
A5	Mean time to resolution: new environment (hours)	Interviews	1.00	1.00	1.00
A6	Subtotal: hours saved per threat	A2-A3+A4-A5	9.50	9.50	9.50
A7	IT professional hourly rate (fully burdened)	TEI standard	$58	$58	$58
At	Faster threat detection and resolution	A1*A6*A7	$264,480	$264,480	$264,480
	Risk adjustment	↓10%			
Atr	Faster threat detection and resolution (risk-adjusted)		$238,032	$238,032	$238,032
	Three-year total: $714,096		**Three-year present value: $591,950**		

INCREASED EFFICIENCY RESPONDING TO UNPLANNED OUTAGES

Evidence and data. Access to continuously and passively analyzed broad network data coupled with a targeted alert system through Reveal(x) 360 enabled network professionals to become aware of unplanned outages and begin remediating them before external parties notified them.

- The director of cybersecurity at a financial services organization said: “The number of outages we had that we didn’t know about before decreased substantially once we implemented Reveal(x) 360. Now, there’s less than five per year. Additionally, we’ve been able to identify exact causes with having three to six people involved in the conversation, instead of 10 to 20, in minutes instead of hours.

Additionally, one unified view across the network landscape for both network and security teams meant that organizations could involve fewer IT employees in the research effort and respond to outages faster.

- The same interviewee said: “Beforehand, understanding and responding to outages got whole teams involved, up to 20 people. Network folks would look at one system, security folks at others, and everyone would have their own opinion on what the problem was. Arguing back and forth would take hours. Now, we have a system that is providing everyone with the same point of view. We can all see the problem, pinpoint the reason behind it, and agree on how to resolve it in minutes. Reveal(x) 360 has established trust within our organization. Now, not only can we involve less people in the problem — we now just need three to six people in the conversation — we can also spend less time taking care of it.”

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

- The composite organization experienced 15 unplanned outages in its previous environment. Twelve IT professionals were needed to address each outage, and it took 6 hours to research the issue.
- Once the organization implements the Reveal(x) 360 platform, the number of unplanned outages, the amount of time spent researching each outage, and the number of people needed to address each outage decreases to five, 30 minutes, and six, respectively.
- The fully burdened hourly rate of an IT professional is $58.

> **“The ExtraHop platform was able to identify the reason behind different issues in minutes compared to 4 to 8 hours. It’s easier for us to troubleshoot and prove the cause behind our network going down.”**
>
> *VP, IT risk management, retail*

Risks. The increased efficiency in responding to unplanned outages may vary depending on the following:

- The total number, complexity, and time spent responding to unplanned outages.
- The number of people involved in responding to these outages.
- The skill level, efficiency, and salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $138,000.

Increased Efficiency Responding To Unplanned Outages

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of outages: prior environment	Composite	15	15	15
B2	Time spent researching outages: prior environment (hours)	Interviews	6	6	6
B3	Number of IT professionals involved: prior environment	Interviews	12	12	12
B4	Subtotal: FTE hours spent researching outages: prior environment	B1*B2*B3	1,080	1,080	1,080
B5	Number of outages: new environment	Interviews	5	5	5
B6	Time spent researching outages: new environment (hours)	Interviews	0.5	0.5	0.5
B7	Number of IT professionals involved: new environment	Interviews	6	6	6
B8	Subtotal: FTE hours spent researching outages: new environment	B5*B6*B7	15	15	15
B9	IT professional hourly rate (fully burdened)	TEI standard	$58	$58	$58
Bt	Increased efficiency responding to unplanned outages	(B4-B8)*B9	$61,770	$61,770	$61,770
	Risk adjustment	↓10%			
Btr	Increased efficiency responding to unplanned outages (risk-adjusted)		$55,593	$55,593	$55,593
	Three-year total: $166,779		**Three-year present value: $138,252**		

REDUCED END-USER DOWNTIME DUE TO WIDESPREAD UNPLANNED OUTAGES

Evidence and data. A decrease in unplanned outages also resulted in a reduction in end-user downtime. Prior to implementing Reveal(x) 360, when the network went down or an application failed, interviewees' organizations did not have the necessary visibility to troubleshoot the issue and fix it quickly. It took organizations hours to days to resolve the outage, which resulted in downstream implications for the business such as loss of productivity and loss of revenue. With Reveal(x) 360, end users are less likely to be impacted by outages resulting in downtime, as IT teams have better visibility to quickly address the issue.

- According to the IT support analyst at a retail organization: "Anytime the network at a distribution center goes down, our employees can't send products to the stores or through e-commerce, and we just have people standing around doing nothing and product getting stuck. We have other instances where we would get a delay every night at 1 a.m. that was crippling production. People would say it was a network issue, but through the ExtraHop platform, we could prove that it was actually a database backup that was happening at 1 a.m. We were able to adjust it in minutes and save it from dragging on for months based on what ExtraHop was able to find."
- For a financial services organization, having Reveal(x) 360 in place improved system uptime by 99% compared to what it was before, as security teams were instantly able to pinpoint issues affecting performance. The director of cybersecurity shared: "Without the controls and monitoring we get with Reveal(x) 360, our landscape was like the Wild West. Now, we could figure out which machines were being underpowered in their production environments or whatever issues we were having. If I'm seeing a database starting to get overloaded, I can start seeing that happening before hearing anything from end users. This improves reliability and removes any excuses of 'I couldn't do my job because of X.'" They continued: "Also, it keeps us in good standing with our customers. Thousands of dollars come through our system every minute, and any one of these outages can stop the money from flowing. ExtraHop really prevents our reputation from getting tarnished."

> **"The ExtraHop platform allowed us to show the application team that a problem we were facing was with an application and not the network. We could also show them exactly what the issue was. They were able to fix the application code faster, allowing us to keep our business flowing."**
>
> *IT support analyst, retail*

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

- The composite organization avoids three widespread outages per year. A widespread outage is defined as one that affects a large group of people rather than a specific workgroup or a specific system. These may include downtime due the network crashing, issues with cloud connectivity, or issues in performance in highly used applications. These outages affect 1,000 users at the composite organization and cause an average of 3 hours of downtime per outage.
- The fully burdened hourly rate of an end user is $35.

- Forrester conservatively estimates that 50% of the total time saved per end-user FTE is applied directly back to value-generating tasks, and it is therefore included in the benefit calculation. Individual employees may apply additional time savings toward professional development, training, and work-life activities, which were not included in the benefit analysis.

Risks. The reduction in end-user downtime may vary depending on the following:

- The number and duration of widespread outages causing end-user downtime.
- The number of end users affected per outage.
- The salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $313,000.

Reduced End-User Downtime Due To Widespread Unplanned Outages

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average number of end users affected per event	Composite	1,000	1,000	1,000
C2	Number of downtime events per year	Composite	3	3	3
C3	Average end-user downtime per event (hours)	Interviews	3	3	3
C4	Average end-user hourly rate (fully burdened)	TEI standard	$35	$35	$35
C5	Productivity recapture	TEI standard	50%	50%	50%
Ct	Reduced end-user downtime due to widespread unplanned outages	C1*C2*C3*C4*C5	$157,500	$157,500	$157,500
	Risk adjustment	↓20%			
Ctr	Reduced end-user downtime due to widespread unplanned outages (risk-adjusted)		$126,000	$126,000	$126,000
	Three-year total: $378,000		**Three-year present value: $313,343**		

LEGACY SECURITY SOLUTIONS SAVINGS

Evidence and data. Numerous interviewees reported that they were able to retire a subset of their existing security solutions once they had implemented Reveal(x) 360.

- A financial services organization was able to decommission 20% of its security stack overtime, which resulted in six-figure savings for the enterprise. The director of cybersecurity said: "We have been able to simplify our stack because we now have a platform where everyone can communicate. Therefore, tools that just the network team or just the systems team was using are no longer used as much. They just kind of died out, so I don't have to renew their licenses and can get rid of their infrastructure."
- The IT support analyst at a retail organization stated: "We were able to consolidate tooling. Particularly, we were able to get rid of our IDS/IPS [intrusion detection system/intrusion prevention system] solution once implementing our ExtraHop solution because it wasn't able to do as much for us as ExtraHop can in terms of pinpointing network and security issues."

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

- One third-party security solution costing $200,000 annually is fully retired by Year 2.
- The organization is able to retire additional solutions in Year 3, totaling $400,000 worth of retired tools.

> **"We were able to decommission a few homegrown solutions and some network analytics sensors. We're also looking to retire some tools our operations team uses for visibility over the next year. This could lead to savings in the millions."**
>
> *Technical director, cybersecurity operations, communications*

Risks. Legacy security solutions savings may vary depending on the following:

- The number of security solutions decommissioned.
- The total annual cost of decommissioned security solutions.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $373,000.

Legacy Security Solutions Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Total annual license cost savings from decommissioning redundant legacy security solutions	Interviews	$0	$200,000	$400,000
Dt	Legacy security solutions savings	D1	$0	$200,000	$400,000
	Risk adjustment	↓20%			
Dtr	Legacy security solutions savings (risk-adjusted)		$0	$160,000	$320,000
	Three-year total: $480,000		**Three-year present value: $372,652**		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Expanded coverage.** Reveal(x) 360 cloud-based machine learning enables the interviewees' organizations to secure more of their attack surface and discover attack attempts not monitored by EDR, SIEM, or other methods, such as exploitation, lateral movement, command and control, and sophisticated ransomware.
  - A communications organization saw a 3x expansion in coverage across its on-premises and cloud environment and noted that ExtraHop's platform was the only solution that could scale to the volume of traffic being pushed through it. The technical director, cybersecurity operations, explained: "We generate about 150 billion work events per day and had about 100 billion that we couldn't do anything about before. ExtraHop allows us, through automated orchestration, to do something about all those events if necessary. We were able to expand our ability to detect phishing and spam, detect ransomware, and detect rogue systems and compromised clients with their device discovery and enumeration capability. Additionally, we have pushed around 450,000 blocks to lateral movement over the last 18 months. We make a lot of determinations based on the additional visibility we get through Reveal(x) 360."
  - A retail organization had 85% of its environment covered with ExtraHop across on-premises, the cloud, and their thousands of stores and distribution centers. The VP, IT risk management, said, "Thanks to ExtraHop, we have a great baseline of what our systems normally do, so deviations from the norm are easy to catch."

> **"When a major supply chain attack happened, ExtraHop had a dashboard for us almost immediately, so we could see any devices that may have been affected by that. ExtraHop spins up dashboards so we can capture vulnerabilities before they become issues."**
>
> *VP, IT risk management, retail*

- **Improved communication.** Reveal(x) 360 drove alignment and efficiency across security and IT operations — the organization as a whole — with shareable and intuitive dashboards. The director of cybersecurity at a financial services organization noted: "Having a tool where we can all communicate has been key. If I see a threat, I am now able to communicate not only with the people who will be fixing it but also with management to say, 'This is my proof, this is what we're going after, this is what we're trying to lock down.' Reveal(x) 360 has been great for security maturity."

- **Reduced risk of security breaches.** Interviewees shared that Reveal(x) 360 helped them achieve a better security posture due to faster threat detection and remediation, reducing risk to the organizations. The technical director, cybersecurity operations, at a communications organization said: "The Reveal(x) 360 platform gathers a lot of information for us instantly. And with the ability to put our behavioral models and our intelligence models directly into the system and customize the risk scores that the system produces, we can much more quickly respond to things that we see as a greater degree of risk than without it. This definitely recused the deeper and more collateral damage that could occur and probably saves us millions.”

> **“Before, you could see 15% or 20% of everything, maybe you [could] get another 15% or 20% by looking at a dozen different systems. Now, you can see it in one standardized, centralized fashion, and everyone who needs to can see all of it — the full picture. And now we know how to steer the ship.”**
>
> *Technical director, cybersecurity operations, communications*

- **Improved decision-making by leadership.** With the added insight the Reveal(x) 360 platform provided, organizations could make more informed decisions in less time. According to the director of cybersecurity at a financial services organization: “We’ve been able to create security overview presentations to communicate with executives that are much more streamlined and provide more in-depth value because of the platform’s dashboards and reporting capabilities. We have been able to cut the time those presentations take by 60%, while giving leadership all the information they need to make important decisions such as showing traffic to inform cyber insurance renewals or understanding resource utilization to see where we may need more CPUs, RAM, or bandwidth.”

> **“The data that the ExtraHop platform provides us tells us everything that’s happening to the wire. That enables us to be extremely dynamic because we now have the information to act. Reveal(x) 360 lets you react significantly faster because you have the visibility you need and the understanding of what’s going on, and you're not acting on unknowns anymore. You’re actually responding to known issues, known suspicions that are on the network, and you can very quickly prioritize what’s important.”**
>
> *Technical director, cybersecurity operations, communications*

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Reveal(x) 360 and later realize additional uses and business opportunities, including:

- **Further increasing coverage.** Organizations using Reveal(x) 360 to monitor a majority of their network landscape looked to expand their coverage to 100% in the future. The technical director, cybersecurity operations, at a communications organization said, “We have multiple cloud environments, and we’re hoping to deploy Reveal(x) 360 in all of them.”
- **Expanding usage to different teams.** With the expansive visibility the Reveal(x) 360 platform

provides, interviewees noted that the information the platform relays could be beneficial to other teams within their organizations. The technical director, cybersecurity operations, at a communications organization explained: “We want to get our compliance teams and traffic policing and optimization teams on the platform. Reveal(x) 360 gives us visibility into data that’s unencrypted that shouldn’t be or what systems are getting network requests that shouldn’t be. This is all valuable information for our compliance teams as they can become more aware of events that may concern them. Meanwhile, our traffic policing and optimization teams are vetting some of their use cases with the ExtraHop platform and are trying to get more information on their downstream traffic. We’re hoping to fully implement this for them within the next year.”

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

Analysis Of Costs

🟩 Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	Fees to ExtraHop, including training and professional services	$0	$178,500	$178,500	$178,500	$535,500	$443,903
Ftr	Internal implementation and ongoing management	$2,297	$12,760	$12,760	$12,760	$40,577	$34,029
Gtr	Training costs	$2,552	$1,276	$1,276	$1,276	$6,380	$5,725
	Total costs (risk-adjusted)	$4,849	$192,536	$192,536	$192,536	$582,457	$483,657

FEES TO EXTRAHOP, INCLUDING TRAINING AND PROFESSIONAL SERVICES

Evidence and data. ExtraHop offers several levels of Reveal(x) 360 subscriptions tailored to fit customers with varying levels of security maturity. The service is priced depending on attack surface coverage, number of hosts, workloads, instances, traffic throughput requirements, and other factors in the customer environment. Sensors are free, and physical appliances are available at an additional cost, with enterprise appliances scaling from 1 Gbps to 100 Gbps. The average selling price for the various configurations ranges from $15,000 to $450,000 annually.

> **"ExtraHop is always offering to help us if we experience problems. They are amazing partners and did a lot of work to ensure we are successful."**
>
> *VP, IT risk management, retail*

> **"Training was part of the package, and they customized it to our needs."**
>
> *Technical director, cybersecurity operations, communications*

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

- The organization purchases a "medium" configuration supporting the high end of the configuration range at 25 Gbps of throughput and approximately 35,000 devices. The organization spends $170,000 annually for the high end of the ASP range.
- This configuration includes cloud-based threat detection, investigation capabilities through global search and indexing, decryption, on-demand and event-triggered packet capture, and discovery and classification of all devices, including internet of things (IoT), in the organization's environment.

- Pricing may vary. Contact ExtraHop for additional details.

Risks. Fees to ExtraHop may vary depending on the following:

- The attack surface coverage.
- The number of hosts, workloads, and instances.
- The amount of throughput required for the physical devices.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $444,000.

Fees To ExtraHop, Including Training And Professional Services

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Annual cost of licensing fees with training and professional services included		$0	$170,000	$170,000	$170,000
Et	Fees to ExtraHop, including training and professional services	E1	$0	$170,000	$170,000	$170,000
	Risk adjustment	↑5%				
Etr	Fees to ExtraHop, including training and professional services (risk-adjusted)		$0	$178,500	$178,500	$178,500
	Three-year total: $535,500		**Three-year present value: $443,903**			

INTERNAL IMPLEMENTATION AND ONGOING MANAGEMENT

Evidence and data. Interviewees said the implementation and ongoing management of Reveal(x) 360 was simple and required relatively minimal time investments.

- As a cloud-native, SaaS-based platform, Reveal(x) 360 was extremely easy for organizations to deploy. According to the technical director, cybersecurity operations, at a communications organization: "Deployment and getting it turned on took maybe a day. We had multiple hundreds of gigs of data being pushed into the system within 48 hours. An on-premises system may have taken the better part of a year just to get all the approvals."
- Interviewees cited the Reveal(x) 360 command center as a huge time-saver for ongoing management of the solution and their network environments. The same interviewee said: "With the deployment of the command center, we could aggregate multiple deployed sensors into a single location. The detection, the triggers, the API calls, everything goes to one place now versus individual systems. Therefore, we can push out intelligence and detections and pull data across multiple networks — whether deployed in the cloud or on-premises — much quicker."
- Implementation teams typically consisted of a handful of IT professionals from the network and security teams. IT professionals on the network team were typically in charge of ongoing management.

Total implementation and deployment time:

3 days

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

- Three IT FTEs participate in the initial implementation for three working days. After implementation, two IT FTEs dedicate 2 hours of their time per week to manage the system.
- The fully burdened hourly rate of an IT FTE is $58.
- A year contains 50 work weeks.

> **"We were up and running with Reveal(x) 360 in less than a day, and we were getting viable network information right away. We'd never had this level of visibility before and were able to strengthen our security posture on day one."**
>
> *Director of cybersecurity, financial services*

Risks. Internal implementation and ongoing management may vary depending on the following:

- The complexity of the organization's network security environment.
- The number of FTEs dedicated to the implementation and management of the solution.
- The salaries of FTEs.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $34,000.

Internal Implementation And Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	IT FTEs involved in implementation and ongoing management	Composite	3	2	2	2
F2	Time spent on initial implementation (hours)	Interviews	24	0	0	0
F3	Percentage of IT FTEs' time dedicated to implementation	Interviews	50%	0%	0%	0%
F4	Time spent on ongoing management per week (hours)	Interviews	0	2	2	2
F5	IT professional hourly rate (fully burdened)	TEI standard	$58	$58	$58	$58
Ft	Internal implementation and ongoing management	(F1*F2*F3*F5)+ (F1*F4*F5*50)	$2,088	$11,600	$11,600	$11,600
	Risk adjustment	↑10%				
Ftr	Internal implementation and ongoing management (risk-adjusted)		$2,297	$12,760	$12,760	$12,760
	Three-year total: $40,577		**Three-year present value: $34,029**			

TRAINING COSTS

Evidence and data. The training time needed to understand how to use Reveal(x) 360 was minimal. Interviewees noted that it only took hours for users to become proficient in using the solution.

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

- Twenty-five IT FTEs are onboarded onto the Reveal(x) 360 platform over three years. It takes them 4 hours to become proficient in using the solution.
- The fully burdened hourly rate for an IT FTE is $58.

Risks. Training costs may vary depending on the following:

- The number, skill set, and prior experience of users being trained to use Reveal(x) 360.
- The salaries of FTEs.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $5,700.

> **"We use a proprietary search language; it does a bunch of really cool stuff, but when we put someone on it that's never used it before, it takes six months for them to be useful. Reveal(x) 360 was the complete opposite of that. Really easy-to-use UI, really robust documentation, really simple to search for things. Anyone with network experience had at most two 1-hour sessions with ExtraHop."**
>
> *Technical director, cybersecurity operations, communications*

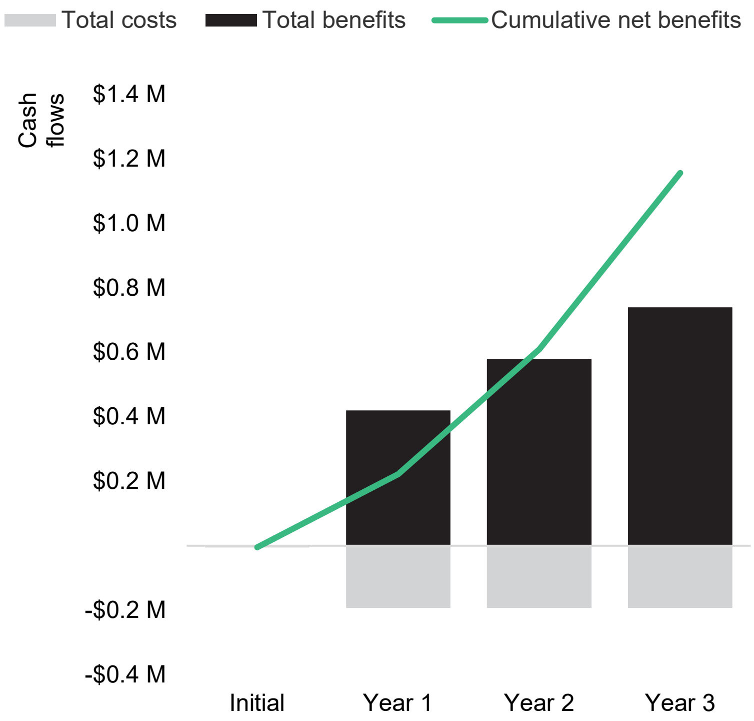
Training Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of IT FTEs (net new)	Interviews	10	5	5	5
G2	Hours of training per IT FTE	Interviews	4	4	4	4
G3	IT professional hourly rate (fully burdened)	TEI standard	$58	$58	$58	$58
Gt	Training costs	G1*G2*G3	$2,320	$1,160	$1,160	$1,160
	Risk adjustment	↑10%				
Gtr	Training costs (risk-adjusted)		$2,552	$1,276	$1,276	$1,276
	Three-year total: $6,380			**Three-year present value: $5,725**		

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 and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI and NPV 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	($4,849)	($192,536)	($192,536)	($192,536)	($582,457)	($483,657)
Total benefits	$0	$419,625	$579,625	$739,625	$1,738,875	$1,416,197
Net benefits	($4,849)	$227,089	$387,089	$547,089	$1,156,418	$932,540
ROI						193%

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: “Mitigating Ransomware With Zero Trust,” Forrester Research, Inc., August 20, 2021.

[2] 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®