TOTAL ECONOMIC IMPACT

The Total Economic Impact™ Of ExtraHop RevealX

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY EXTRAHOP, FEBRUARY 2026

COST SAVINGS AND BUSINESS BENEFITS ENABLED BY REVEALX

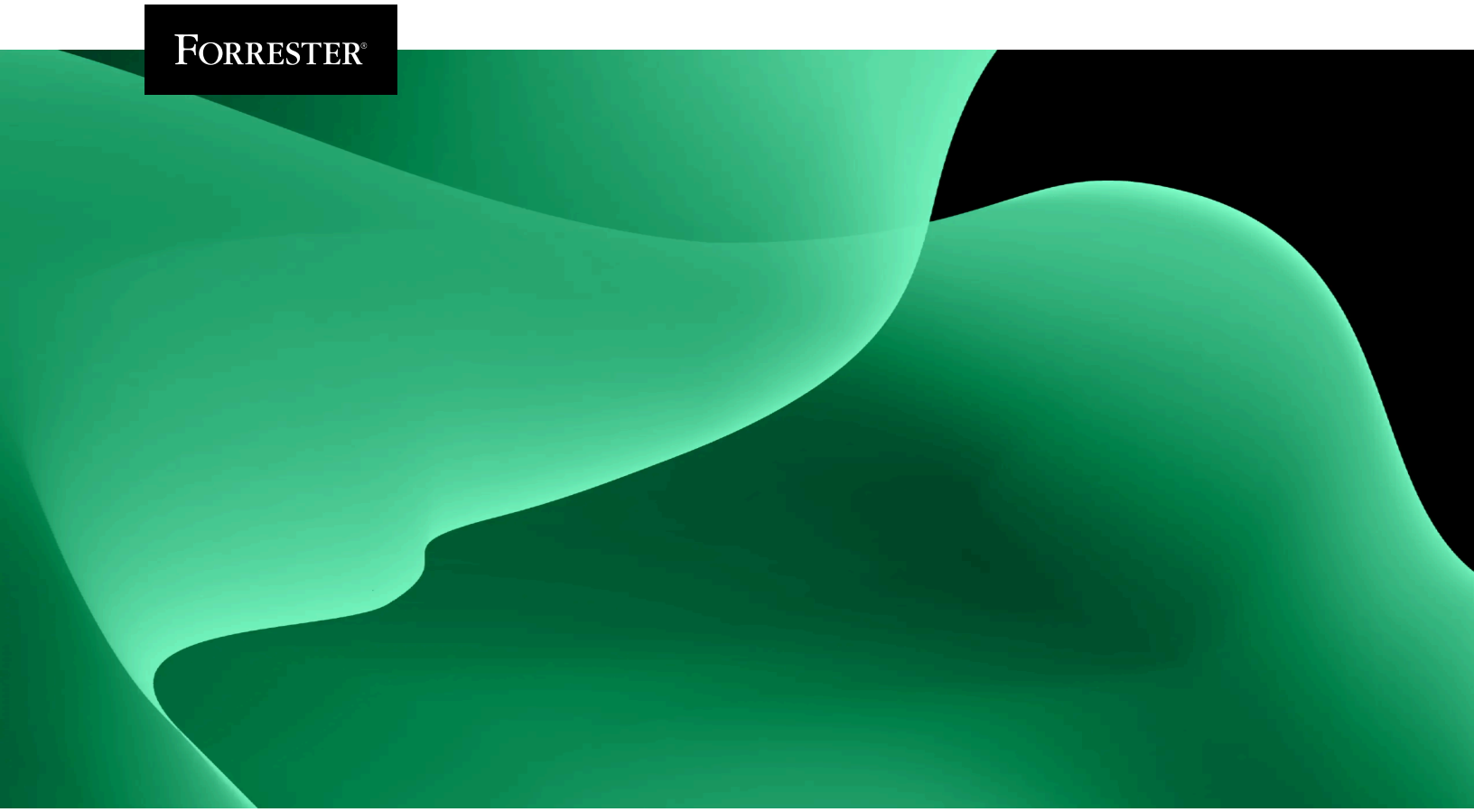


Table Of Contents

Executive Summary

Organizations require deep visibility into encrypted east-west traffic and anomalous network behavior to detect compromises, such as lateral movement and data exfiltration, before significant damage occurs. This security is essential for an organization's Zero Trust journey and in maintaining a strong security posture against evolving threats like ransomware and insider threats. ExtraHop RevealX addresses the need for real-time network analysis and visibility (NAV)/network detection and response (NDR) capabilities to identify and mitigate network threats that bypass traditional security tools.

ExtraHop RevealX is a NAV/NDR solution that continuously decrypts and analyzes all network traffic out of band to identify anomalous activity, zero-day threats, and threats hiding in encrypted traffic. This provides security teams with high-fidelity detections, automated investigations, and forensic evidence to accelerate threat response and secure their environment against lateral movement.

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 RevealX.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of RevealX on their organizations.

155%

Return on investment (ROI)

$3.5M

Net present value (NPV)

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using RevealX. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization that is a global firm with 15,000 employees and $5 billion in annual revenue.

Interviewees said that prior to using RevealX, their organizations used a combination of legacy NDR tools, networking performance monitoring (NPM) tools, and open-source tools for threat detection and analysis. Their legacy NDR tools relied on flow data and metadata but lacked full-packet capture capabilities for in-depth forensic investigation. The interviewees whose organizations had NPM tools in place reported that while the solutions provided network visibility, they lacked the behavioral analytics and security context needed to effectively spot and prioritize covert attacks like lateral movement. Interviewees also reported that their legacy open-source threat detection solutions required extensive manual configuration and lacked centralized management, resulting in delayed incident responses and unnecessarily high alert volumes.

The interviewees used RevealX to replace some of their legacy NDR and open-source tools and supplement their NPM tools. With their updated network security stacks, the interviewees' organizations reduced their risk of security breaches and improved the efficiency of their security teams.

The interviewees shared that RevealX significantly reduced their risk of security breaches by providing them with high-fidelity, real-time threat detection capabilities, allowing analysts to stop threats like lateral movement before they cause damage. They shared that these capabilities led to substantial time savings for their security analysts, while also benefiting auditors by supplying verifiable evidence of security controls and incident response.

Key Findings

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

- **Reduction in security breach risk.** RevealX significantly reduces the composite organization's breach likelihood by using machine learning and behavioral analytics to detect security compromises, such as lateral movement and internal reconnaissance, that legacy NDR tools often miss. By providing real-time deep visibility into east-west traffic, decryption, and analysis of all network traffic, the platform eliminates attacker blind spots and allows security teams to intervene before breaches or data exfiltration occurs. Over the course of the three-year analysis, the reduction in breach likelihood is worth a risk-adjusted $2.1 million to the composite organization.
- **Time savings of up to 63% when investigating each network security alert.** RevealX accelerates the composite organization's alert investigation by providing forensic context alongside every detection, including packet data and behavioral analysis, eliminating the need for analysts to pivot to separate tools. Equipped with this forensic data, security teams understand threats faster and more quickly remediate threats. These time savings amount to a risk-adjusted $626,000 in labor cost savings over three years.
- **Productivity lift of 30% on network security auditing work.** With RevealX, the composite organization's internal audit and compliance teams quickly produce the necessary evidence of security controls and incident response procedures required for regulatory mandates. During the three-year analysis, these time savings are worth a risk-adjusted $126,000.
- **Cost savings from retiring legacy network security tools and optimizing cloud costs.** After implementing RevealX, the composite organization retires some of its legacy network security tools and gradually eliminates its prior licensing spend. Additionally, RevealX provides the composite with visibility into its cloud environments, allowing it to monitor and control unexpected consumption or expensive egress points. Over three years, the composite eliminates $2.9 million in legacy system and cloud costs.

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

- **Further efficiencies from RevealX's AI capabilities.** RevealX significantly boosts the efficiency of the composite's security operations center (SOC) through its AI/ML-based threat detection, resulting in additional time savings and risk reduction. Features like Smart Triage prioritize critical threats and cut through alert fatigue, while the AI Search Assistant allows the composite's analysts to use natural language queries for fast threat hunting. These tools streamline detection and investigation, enabling teams to be more productive and focus on the most impactful work.
- **Enhanced cyber insurance process.** By providing enhanced network visibility and detailed network telemetry, RevealX gives the composite organization objective proof of the strong security posture that insurance underwriters require. As a result, the composite can more easily retain its insurance policies and avoid major premium hikes.
- **Easier integration process, simplifying M&A activity.** The composite organization uses RevealX to gain comprehensive visibility into the combined network environments, removing a key hurdle in the M&A process. RevealX ensures rapid asset discovery and inventory across both the composite and the acquired company, quickly identifying all connected devices and accelerating due diligence.

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

- **RevealX subscription and professional services costs.** The composite incurs annual subscription and professional services costs from ExtraHop for the usage of RevealX, as well as a one-time implementation cost. Over three years, these costs amount to a risk-adjusted $2.0 million for the composite.
- **Internal labor for the implementation of RevealX.** The composite dedicates a team of internal employees to managing the implementation of RevealX over the course of the 10-week deployment. These labor costs amount to a risk-adjusted $89,000.
- **Internal labor for ongoing maintenance.** Two of the composite's employees dedicate a portion of their time to managing the RevealX deployment on an ongoing basis. Over the three-year analysis, these labor costs amount to $148,000.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $5.8 million over three years versus costs of $2.3 million, adding up to a net present value (NPV) of $3.5 million and an ROI of 155%.

Reduction in breach risk

Up to 48%

> *"ExtraHop RevealX reduces the risk of breaches and improves the efficiency for our workforce. It leads to cost savings from retiring other technology solutions, and employee satisfaction has also improved. On a scale of one to 10, I'd say ExtraHop is a 10."*
>
> **Head of portfolio management, manufacturing**

Key Statistics

155%

Return on investment (ROI)

$5.8M

Benefits PV

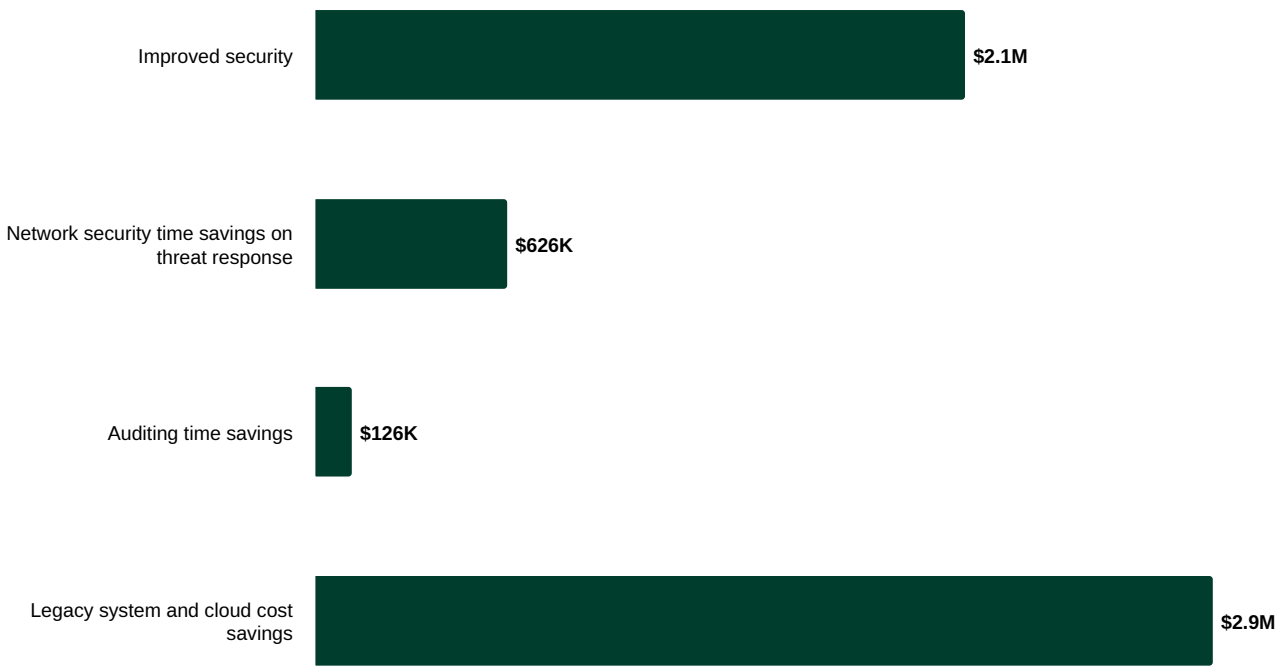
$3.5M

Net present value (NPV)

<6 months

Payback

Benefits (Three-Year)



The ExtraHop RevealX Customer Journey

Drivers leading to the RevealX investment

Interviews			
Role	**Industry**	**Region**	**Annual Revenue**
Head of portfolio management	Manufacturing	Global	>$20 billion
Director of IT	Healthcare	North America	$800 million
CISO	Software	North America	$5 billion
Managing director	Financial services	Global	>$20 billion

Key Challenges

Interviewees reported that before investing in RevealX, their organizations had a variety of security tools in place, including NPM tools, endpoint detection tools, open-source threat detection tools, and legacy NDR tools. The interviewees whose organizations had legacy NDR tools in place noted that the tools only provided flow data and metadata and lacked full packet capture, limiting the visibility they had into internal network traffic.

Interviewees noted how their organizations struggled with common challenges, including:

- **High breach risk.** Interviewees shared that their organizations' existing security tools frequently failed to detect sophisticated threats like zero-day attacks and fileless malware that bypass traditional defenses. This created an unacceptable level of risk, driving their organizations to search for a tool with deep behavioral analysis to catch threats that other tools miss. The head of portfolio management at a manufacturing firm described the risk: "We had challenges related to data security and privacy. It took us a long time to detect any threats, so it was very high risk. Our sensitive data related to regulatory and compliance requirements was at risk."

  The CISO at a software company also added: "With our legacy product, we didn't have the ability to do full packet capture and see what was happening. There was a lot higher alert volume and most of it was false positives because we didn't know what was in the traffic."
- **Lack of visibility into east-west traffic.** The interviewees reported that their organizations' legacy security stack focused heavily on north-south (in and out) traffic, leaving a dangerous blind spot in east-west (internal) traffic. As a result, their organizations struggled to identify and track threat actors as they moved laterally throughout the network. The CISO at a software company detailed their limitations in identifying and remediating lateral movement: "We had to do a lot of manual alert triage to figure out whether it was a real issue or not. … We had a lot of close calls, meaning we had a threat actor penetrate the perimeter and move laterally within our network, and we weren't able to detect that."
- **Manual alert investigations reduce productivity of security staff.** On top of the breach risks, interviewees noted that their legacy security tools left their network security teams overwhelmed with a flood of alerts from disparate tools. They shared that when a threat actor exhibited lateral movement, stitching together logs and context across multiple systems was time-consuming and error prone. The director of IT at a healthcare organization described their approach prior to RevealX: "Previously, investigating lateral movement was mostly manual. We did a lot of log management and log analysis, so we were taking different data sources and trying to glue the data together. With that approach, you're a bit slower with everything, and

you're also reactive; you're catching the lateral movement after the attack and then it's too late."

The head of portfolio management at the manufacturing firm described a similarly manual approach to threat response: "Prior to ExtraHop [RevealX], we used to call for team meetings with subject matter experts from IT, engineering, R&D, and finance. They used to review a spreadsheet template on an issue, the problem statement, and potential solutions, so they spent a lot of time on investigation and trying to get external IT consulting support. It was a longer process with more people involved and had an added investment on the cost."

- **Inefficient cloud operations lead to spiraling costs.** Some interviewees noted that their organizations faced unpredictable and excessive egress costs stemming from the sheer volume of security logs and metadata being transferred out of cloud environments for analysis. Some also lacked visibility into the costliest network egress points, leading to unnecessarily high cloud costs.

Solution Requirements

The interviewees searched for a solution that could:

- Implement comprehensive and deep network visibility, particularly into east-west traffic, to detect lateral movement and advanced network attacks.
- Reduce mean time to detect (MTTD) and mean time to respond (MTTR) with high-fidelity detections and automated incident context.
- Lower cloud infrastructure costs by minimizing the need for expensive, high-volume log aggregation and egress.
- Introduce AI/ML-driven workflows to automate triage and accelerate investigations, saving security team time and reducing dwell time.
- Maintain compliance with existing and emerging SOC regulations, while saving employee time on preparing for audits.

> *"We do a lot of growth through M&A, and as an organization, we previously did not have centralized visibility or threat detection. We wanted to go to a vendor that gave us that 10,000-foot view overall."*
>
> **Director of IT, healthcare**

> *"It became very obvious that if we are going to have sensitive workloads in the cloud, we really need to make sure that we have good security posture. … We sleep well knowing that we have the right security guardrails and policies in place."*
>
> **Managing director, financial services**

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 interviewees' organizations, 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 composite is a global organization with $5 billion in annual revenue and 15,000 employees distributed around the world. The organization has a hybrid environment with a combination of on-premises, multicloud, and remote sites.
- **Deployment characteristics.** The composite deploys RevealX in Year 1 following a 10-week implementation process. After setting up RevealX, the composite retires NDR tools and devices from its legacy environment. With RevealX, the composite receives 12,000 network security alerts per year, 15% of which require an agent's response.

KEY ASSUMPTIONS

- $5 billion in annual revenue
- 15,000 employees
- Hybrid environment
- 12,000 network security alerts per year, 15% of which require agent action

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Improved security	$809,869	$867,717	$925,564	$2,603,150	$2,148,756
Btr	Network security time savings on threat response	$240,084	$252,720	$265,356	$758,160	$626,484
Ctr	Auditing time savings	$50,544	$50,544	$50,544	$151,632	$125,695
Dtr	Legacy system and cloud cost savings	$900,000	$1,260,000	$1,422,000	$3,582,000	$2,927,874
	Total benefits (risk-adjusted)	$2,000,497	$2,430,981	$2,663,464	$7,094,942	$5,828,809

Improved Security

Evidence and data. The interviewees reported that using RevealX helped reduce breach likelihood by providing real-time network visibility and high-fidelity detection of malicious activity that often bypassed their traditional security tools. The interviewees detailed their specific security improvements, including:

- **Increased visibility into lateral movement with deep traffic analysis.** Interviewees noted that RevealX analyzed both encrypted and unencrypted network traffic in real time to detect threats and anomalous behaviors used by attackers to move laterally across the network. By monitoring east-west traffic and decrypting protocols like TLS, RevealX helped the interviewees' organizations eliminate blind spots and expose activities that traditional security tools may miss. The director of IT at a healthcare organization described the improvement: "With [RevealX]'s visibility into lateral movement, we've been able to better see and deal with credential attempts. We're also able to see what is scanning the network and what is being accessed during these scans. … ExtraHop is stronger than its competition in terms of network visibility."
- **Faster MTTR from automated investigations and context.** Interviewees shared that RevealX accelerated threat response by automatically triaging every detection with an attack timeline, risk score, and all necessary forensic data. This rapid context allowed the interviewees' organizations to quickly scope and contain incidents, stopping a breach before major damage occurs. The CISO at a software company explained the benefit: "RevealX identifies security attacks that are traversing our network as quickly as possible, so that we can triage and guillotine them. It provides the business a reduction in expected losses from a data breach that occurs via the network."

  The managing director at a financial services firm agreed that RevealX both saved employee time and reduced breach risk, noting, "With ExtraHop [RevealX], our mean time to resolution has improved by 60% to 65%."
- **RevealX dashboard capabilities that provide a unified view of network security operations.** Interviewees reported that RevealX's centralized console provided their organizations with real-time visibility into their network, including all assets, transactions, and workloads across multicloud and hybrid environments. They shared that the security dashboards use machine learning to flag high-fidelity alerts, allowing security teams to focus on the most critical threats and better track key security metrics. The head of portfolio management at a manufacturing organization described the effectiveness of RevealX dashboards: "[RevealX's] GenAI dashboard gives us an overview of the number of incidents, the number of issues, resolutions, and identified risks. Because of that, our IT team is well aware before something happens, so they are able to mitigate the risk before any issue happens on the data breaches."
- **Reduction in risk.** Each interviewee estimated their organization's reduction in breach likelihood:

- The head of portfolio management at a manufacturing firm stated, "It is around a **60%** reduction in breach risk with ExtraHop RevealX."
- The managing director at a financial services firm noted, "We estimate that it is between a **50% to 70%** reduction in the likelihood of a breach."
- The CISO at a software firm provided a similar estimate: "We estimate a **50%** reduction in the annual loss expectancy of a data breach related to lateral movement within the network."
- The director of IT at a healthcare organization reported a **15% to 30%** reduction in breach risk from using RevealX.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Based on Forrester's 2025 security survey, an organization of the composite's size expects $4.2 million of annual breach costs per year.[2] Furthermore, 54% of the breaches originate from external attacks targeting organizations and their remote environments.[3]
- With RevealX, the composite reduces the likelihood of a severe data breach caused by an external attack by 42% in Year 1. As the composite finetunes its deployment and security controls, the risk reduction climbs to 45% in Year 2 and 48% in Year 3.

Risks. Improved security will vary depending on:

- An organization's security posture and maturity prior to deploying RevealX.
- Other NDR, NPM, firewalls, or endpoint detection tools that the organization has in place.
- The likelihood and associated costs of security breaches each year.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.1 million.

> *"[RevealX] has become more and more sophisticated and does a great job at being one step ahead of whatever is happening on your attack surface. It allows us to be proactive in identifying lateral threats."*
>
> **Managing director, financial services**

> *"The time it takes to identify threats and to resolve threats is improved drastically. As a result, we are getting a better payback and better ROI from our investment in RevealX."*
>
> **Head of portfolio management, manufacturing**

Improved Security					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Total annual risk exposure to security breaches for the composite organization	Forrester research	$4,201,000	$4,201,000	$4,201,000
A2	Percentage of breaches originating from external attacks targeting organizations and external attacks targeting remote environments	Forrester research	54%	54%	54%
A3	Annual risk exposure addressable with ExtraHop RevealX	A1*A2	$2,268,540	$2,268,540	$2,268,540
A4	Reduced risk of exposure to breach costs with ExtraHop RevealX	Interviews	42%	45%	48%
At	Improved security	A3*A4	$952,787	$1,020,843	$1,088,899
	Risk adjustment	↓15%			
Atr	Improved security (risk-adjusted)		$809,869	$867,717	$925,564
	Three-year total: $2,603,150			**Three-year present value: $2,148,756**	

Network Security Time Savings On Threat Response

Evidence and data. Interviewees shared that RevealX allowed their security teams to reduce the time spent manually investigating and triaging security events through its advanced visibility and threat detection capabilities. With machine learning-based detection and automated decryption, the interviewees' organizations could immediately pinpoint true positive threats, while also accelerating investigation and response times by eliminating the need to manually stitch together fragmented data sources. The interviewees detailed specific efficiencies, including:

- **Automated lateral movement investigation.** The interviewees' organizations were able to significantly cut down the manual labor involved in tracking sophisticated threats, particularly lateral movement across the network. This eliminated the need for analysts to manually piece together evidence from disparate logs and endpoint data, a process that some interviewees' organizations had been performing with manual spreadsheets. The head of portfolio management at a manufacturing organization described the change: "Before RevealX, our teams were working manually using spreadsheets and homegrown templates. After having [RevealX], the process is automated and driven by AI features, so efficiency is improved drastically. … In total, our team spent around 25 employee hours investigating each lateral movement incident, but with RevealX it is now 3 to 4 hours."

  The director of IT at a healthcare firm also reported significant time savings on investigating lateral movement: "On average, it used to take 4.5 hours to investigate an issue, and now it's between 2 to 2.5 hours. … I think it's going to get stronger and more efficient as we move along."
- **Faster forensics and evidence collection.** With RevealX, the interviewees' organizations gained definitive forensic information from the platform's continuous packet capture and streamlined investigation workflow. The interviewees shared that RevealX provided access to transaction records and full-packet level forensic detail all from a single interface, eliminating the time-consuming process of stitching together evidence from multiple tools. The director of IT at a healthcare firm described how the forensics module streamlined their process, stating, "ExtraHop's forensics module is stronger than any tool we had previously because [before], we might have had our own IT response teams or third-party cybersecurity vendor go in and have to figure out what is going on and write a report about what exactly took place."
- **Less time responding to false positives.** By leveraging RevealX, the interviewees' organizations were able to pick up more threats that they otherwise would have missed, while simultaneously bringing down the number of false positives. While the total number of alerts remained similar to their legacy environments, the RevealX alerts were higher fidelity. The managing director at a financial services firm noted the impact: "We've finetuned ExtraHop to distinguish between signal and noise in

our alerts. ... It was an iterative process over the first six or seven months, but we eliminated 60% to 70% of false positives."

The CISO at a software company agreed that their team spent less time responding to false positives, allowing them to more quickly address more critical alerts: "Our alert volume is less than what it was previously, and these alerts are high-fidelity. When it tells us something, something is happening. ... It's an 80% reduction in false positives [with RevealX]."

- **Overall security team time savings.** Interviewees expressed that using these capabilities from RevealX allowed them to avoid increasing security headcount and reallocate staff teams to new initiatives. The CISO at a software company estimated the impact: "It reduced network security work so we used that additional bandwidth to monitor additional alert types. If we had not repurposed our security team, we could have reduced them by 25%."

  The managing director at a financial services firm estimated that RevealX boosted the efficiency of their organization's 75-person SOC team by 40% to 60%.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization receives 12,000 network security alerts per year, 15% of which require a response from their security team.
- The composite dedicates 5 FTE hours to investigating and responding to each alert that requires action.
- With RevealX, the composite organization reduces the FTE time required for each alert investigation by 57% in Year 1. As the deployment becomes more mature and the composite gathers more historical alert data, the efficiency increases to 60% in Year 2 and 63% in Year 3.
- The fully burdened hourly rate for a security FTE is $65.
- An 80% productivity recapture is applied since not all time savings are redeployed productively.

Risks. Threat response time savings will vary depending on:

- The volume of network alerts an organization has in its legacy environment.
- The number of FTE hours required for each alert response prior to deploying RevealX.
- The average fully burdened hourly rate for a security FTE.

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 $626,000.

Up to 63%

Productivity lift on investigating alerts

> *"Before we had ExtraHop [RevealX], it could take us between 10 to 48 hours to even figure out the issue. With ExtraHop, in 90% of the time, we are able to pinpoint the issue and figure out what's happening in less than an hour."*
>
> **Managing director, financial services**

Network Security Time Savings On Threat Response					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Network security alerts per year	Composite	12,000	12,000	12,000
B2	Percentage of alerts that require agent action	Composite	15%	15%	15%
B3	Alerts requiring network security team response with ExtraHop RevealX	B1*B2	1,800	1,800	1,800
B4	FTE time required to investigate and respond to each alert before ExtraHop RevealX (hours)	Interviews	5	5	5
B5	Investigation efficiency gains with ExtraHop RevealX	Interviews	57%	60%	63%
B6	FTE time required to investigate and respond to each alert with ExtraHop RevealX (hours)	B4*(1-B5)	2.15	2.00	1.85
B7	Time savings on threat response with ExtraHop RevealX (hours)	(B3*B4)-(B3*B6)	5,130	5,400	5,670
B8	Fully burdened hourly rate for a network security employee	Composite	$65	$65	$65
B9	Productivity recapture	TEI methodology	80%	80%	80%
Bt	Network security time savings on threat response	B7*B8*B9	$266,760	$280,800	$294,840
	Risk adjustment	↓10%			
Btr	Network security time savings on threat response (risk-adjusted)		$240,084	$252,720	$265,356
	Three-year total: $758,160			**Three-year present value: $626,484**	

Auditing Time Savings

Evidence and data. When evaluating NDR vendors, the interviewees' organizations sought a solution that could ensure compliance with their existing compliance regulations, such as SOC policies, NIST, and PCI DSS. Interviewees shared that RevealX allowed their organizations to maintain their existing compliance and streamline the process of manually collecting and parsing data for audits. RevealX provided their organizations with automated asset discovery and classification, full-scale network visibility, and a complete and untampered record of network activity, saving hours of employee time. Interviewees described a range of ways that RevealX made their internal audit teams more efficient:

- Interviewees reported that prior to using RevealX, it was very labor-intensive to pull network security data to prove their network security compliance. The CISO at a software firm stated: "We have a lot of audits, including seven SOC-1 audits. … It's definitely reduced the amount of time that it takes for us to produce evidence of network security monitoring. Before, it was really difficult to get data from our network security tool to show the auditors that we were following our processes for alert triage for network security alerts. It's reduced that time by about 30%."
- Other interviewees praised RevealX's dashboards, which helped them gather data for their compliance tasks faster. The head of portfolio management at a manufacturing firm reported: "When we have a half-yearly audit by third parties, they refer to the dashboard available on ExtraHop. They are able to reduce the physical audit time to go to each of the functional areas."

  This interviewee went on to say that: "We also monitor the compliance initiatives on a monthly and quarterly basis, which we report to government agencies to meet our target audit requirements. Since the process got automated with ExtraHop [RevealX], we are able to save around 40% of our time on measuring compliance, regulatory, and sustainability requirements."
- The managing director at a financial services firm agreed that RevealX made it easier for them to prove their security posture for auditors: "Every month, we have to generate reports on how many types of network alerts we got, and the auditors will do their own analysis on our security posture and reputational risk. Without ExtraHop [RevealX], our internal audit team would have to spend 20% to 30% more time gathering that information and validating it. With all the dashboards and details we have, they're saving all that time."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization has 12 internal employees involved in network security audits. Each of these 12 employees dedicate 25 hours per month to these audits.
- With RevealX, these employees complete network security auditing tasks, such as asset discovery and data gathering, 30% faster than with their legacy toolset.
- The fully burdened hourly rate for an employee involved in network security auditing is $65.
- A productivity recapture of 80% is applied to account for the fact that not all hours saved are redeployed productively.

Risks. Audit time savings will vary depending on:

- Specific audit and compliance regulations that an organization is required to meet.
- The number of internal staff involved in the audit process.
- The fully burdened hourly wage of FTEs involved in auditing.

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 $126,000.

30%

Time savings on preparing for network security audits

> *"One of the key metrics for our evaluation was if onboarding ExtraHop could save our audit and compliance teams' time. We wanted to save at least 20% of their time on audits, and we have more than achieved that."*
>
> **Managing director, financial services**

Auditing Time Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Internal employees involved in auditing process	Composite	12	12	12
C2	Time dedicated to network security audits per employee per month before ExtraHop RevealX (hours)	Composite	25	25	25
C3	Network security audit efficiency improvement with ExtraHop RevealX	Interviews	30%	30%	30%
C4	Time dedicated to network security audits per employee per month with ExtraHop RevealX (hours)	C2*(1-C3)	17.5	17.5	17.5
C5	Annual time savings on network security auditing with ExtraHop RevealX (hours)	C1*(C2-C4)*12 months	1,080	1,080	1,080
C6	Fully burdened hourly rate for an internal employee involved in network security auditing	Composite	$65	$65	$65
C7	Productivity recapture	TEI methodology	80%	80%	80%
Ct	Auditing time savings	C5*C6*C7	$56,160	$56,160	$56,160
	Risk adjustment	↓10%			
Ctr	Auditing time savings (risk-adjusted)		$50,544	$50,544	$50,544
	Three-year total: $151,632			**Three-year present value: $125,695**	

Legacy System And Cloud Cost Savings

Evidence and data. Interviewees reported that implementing RevealX allowed their organizations to retire some of their existing security tools, including legacy NDR tools and open-source threat detection tools. Those interviewees' organizations that implemented RevealX alongside ExtraHop's NPM module were also able to retire legacy NPM tools. In addition, interviewees shared that RevealX optimized cloud costs by providing full network visibility to identify unauthorized, runaway, or misconfigured workloads that drive unnecessary consumption and compute charges.

- The director of IT at a healthcare organization described how their organization uncovered net savings from replacing some of its legacy tools with RevealX: "We have been able to consolidate the number of tools we have. The cost with our previous solution was $250,000 higher than our ExtraHop costs. It is around a 35% savings than had we scaled out our legacy solution."
- In addition to legacy security software, the CISO at a software firm shared that RevealX helped their organization optimize its cloud spend: "RevealX helps us identify network flows that are more cost-effective. At times, it helped us identify that we've got traffic flowing from this cloud to this on-premises location with expensive network egress costs, so we moved those application to the cloud or on-premises. It's hundreds of thousands in savings from decreasing our egress costs." The interviewee went on to estimate that the annual cloud cost savings were at least $750,000 and expected them to grow.
- The managing director at a financial services firm described how scaling out RevealX led to their organization uncovering cost savings: "On a yearly basis, we go through our stack of vendors and we ramp some down. With RevealX, we ramped down two vendors. It was easily over $500,000 in annual cost savings." The managing director went on to add that RevealX contributed to hundreds of thousands of dollars in additional cloud cost savings.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization begins retiring its previous tools in Year 1 and can fully retire those tools by Year 2, with $500,000 of tool costs avoided in both Year 2 and Year 3.
- The composite also uses RevealX to optimize its cloud egress spend, leading to $750,000 of cloud costs being eliminated in Year 1. As the composite's deployment becomes more mature, the composite's annual cloud savings increases to $900,000 in Year 2 and $1.08 million in Year 3.

Risks. The avoided legacy costs will vary depending on:

- The specific network security tools that an organization has in its legacy suite.
- The speed at which an organization can retire its legacy costs and right size its cloud spend.
- An organization's legacy cloud deployment and total cloud spend.

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 $2.9 million.

Over $1M

Cloud cost savings in Year 3

> *"The cost with our previous solution was $250,000 higher than our ExtraHop costs. It is around a 35% savings than had we scaled out our legacy solution."*
>
> **Director of IT, healthcare**

Legacy System And Cloud Cost Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Cost savings from retiring legacy network detection tools and devices	Composite	$250,000	$500,000	$500,000
D2	Cost savings from optimizing cloud costs	Composite	$750,000	$900,000	$1,080,000
Dt	Legacy system and cloud cost savings	D1+D2	$1,000,000	$1,400,000	$1,580,000
	Risk adjustment	↓10%			
Dtr	Legacy system and cloud cost savings (risk-adjusted)		$900,000	$1,260,000	$1,422,000
	Three-year total: $3,582,000		**Three-year present value: $2,927,874**		

Unquantified Benefits

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

- **Further efficiencies from RevealX's AI capabilities.** Interviewees said RevealX enhanced the operational efficiency of their organizations' SOC by integrating sophisticated AI and ML capabilities, yielding substantial gains in time savings and overall risk reduction. The platform's Smart Triage feature intelligently prioritized alerts for the interviewees' organizations by correlating events and calculating a risk score, effectively filtering out noise and combating alert fatigue. Furthermore, the AI Search Assistant empowered the interviewees' organizations' analysts to perform rapid threat hunting using natural language queries rather than specialized coding. These integrated AI tools collectively accelerated the entire security workflow, from detection and prioritization to deep investigation.

Voice Of The Customer

RevealX AI Capabilities

Interviewees reported several emerging ways RevealX's AI features were changing their security operations:

"We're seeing that initial triage time is significantly reduced with Smart Triage. We're seeing the time to triage go from 9 minutes to 4 to 4.5 minutes with these tools because they do a lot of the legwork that was manually done before." — CISO, software

"We are using ExtraHop's AI assistant to identify issues and to search for predetermined solutions. We can compare an issue with any historical issue to see how it was solved, so we have a path forward and can mitigate issues faster and more accurately." — Head of portfolio management, manufacturing

"ExtraHop has natural language search, which we have started to use more and more frequently to get more detail on security events." — Managing director, financial services

"They're continuously improving their generative AI [genAI] features, and they're doing a good job. ... They're very serious about their AI features. They're not just trying to make it look like they have a genAI thing." — Managing director, financial services

- **Enhanced cyber insurance process.** According to interviewees, RevealX streamlined their organizations' cyber insurance procurement and renewal processes by offering objective evidence of their network security posture. Consequently, the interviewees noted their organizations could more easily satisfy insurer requirements, enabling them to secure new policies, retain existing coverage without excessive scrutiny, and potentially mitigate drastic premium increases because the documented risk profile was demonstrably lower. The director of IT at a healthcare organization reported how RevealX has improved their insurance process: "We're able to show ExtraHop RevealX to our cyber insurance risk agency and say, 'Hey, we have these new controls in place and we're following best practices now.' So, in theory, we can save some dollars off of the total cost that goes into our insurance plan."
  The managing director at a financial services firm added, "We aim to increase our security posture and decrease our cyber insurance premiums, and RevealX is one of the key ingredients in that."

- **Easier integration process, simplifying M&A activity.** RevealX significantly accelerated and derisked the interviewees' organizations' M&A processes by instantly providing deep visibility across the merging IT environments. Instead of relying on slow, incomplete reports from the acquired entity, the interviewees said their organizations used RevealX to achieve rapid asset discovery and inventory for every connected device in both networks. The director of IT at a healthcare firm described how this applied to their own organization's M&A activity: "Another benefit is ExtraHop's ability to connect different data. Being in an M&A environment, hospitals and clinics are typically siloed from each other, but not from the enterprise. The time it takes to gather the information we need for either pre-M&A or post-M&A tasks has improved with ExtraHop."

> *"The future is with AI search and Smart Triage capabilities because as the complexity of our ecosystems increases, it's very difficult for people to synthesize that information. Instead, they want to use natural language prompts."*
>
> **Managing director, financial services**

Flexibility

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

- **Using the RevealX NDR module alongside additional modules, such as NPM, to reduce internal and customer-impacting downtime.**Interviewees reported that their organizations used ExtraHop's NPM to unify security and operations visibility and significantly decrease downtime. The integrated platform monitored all network and application activity in real time, allowing their IT teams to instantly pinpoint the root cause of performance issues — whether it was a slow application, a misconfigured network device, or a security attack — without having to switch between disparate tools.
  The head of portfolio management at a manufacturing firm described the impact of the broader ExtraHop suite on improving reliability: "Previously, the networks would go down as well as our network performance monitoring solution. Our network detection and response module would go down, and the communication from our ERP [enterprise resource planning] to our different finance systems, supply chain systems, and manufacturing systems would not work. ... If I compare our prior situation of having ExtraHop and our current situation, there is a 10-to-12-hour reduction in downtime per month. Per hour, our downtime costs $65,000."
  Prior to implementing ExtraHop, the CISO from the software firm said they dealt with rare but extremely costly customer-facing downtime. They reported a marked reduction, partially driven by the implementation of RevealX: "We also use ExtraHop's network performance management module, which helps reduce network downtime. Our overall network downtime has come down about 35% since implementing the network performance monitoring piece. ... Our [customer-impacting] downtime costs approximately $1.2 million a minute, so those minutes are meaningful."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

> *"ExtraHop gives us better visibility into our entire network across the M&A environment that we're in. It helps us manage risk, respond to that risk, and consolidate away from legacy tools that weren't giving us information we needed and were potentially going to cost the organization more money. It's paid for itself a few times over."*
>
> **Director of IT, healthcare**

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	ExtraHop RevealX subscription costs	$143,000	$715,000	$770,000	$825,000	$2,453,000	$2,049,198
Ftr	Implementation and training costs	$80,080	$3,432	$3,432	$3,432	$90,376	$88,615
Gtr	Ongoing management costs	$0	$59,400	$59,400	$59,400	$178,200	$147,719
	Total costs (risk-adjusted)	$223,080	$777,832	$832,832	$887,832	$2,721,576	$2,285,532

ExtraHop RevealX Subscription Costs

Evidence and data. Interviewees reported that their RevealX costs were typically structured on a per-device basis with additional charges for support and professional services. Pricing may vary. Contact ExtraHop for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes that the composite incurs annual subscription costs of $650,000 in Year 1; these costs include licensing, support, and professional services. As the composite grows and more devices are onboarded, the costs grow to $700,000 in Year 2 and $750,000 in Year 3. The composite also incurs a one-time fee of $130,000 for professional services during the implementation process.

Risks. The impact of this cost will vary depending on:

- The number of devices protected by RevealX.
- The level of professional services support required by an organization.
- Pricing changes and contract terms.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.0 million.

ExtraHop RevealX Subscription Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	ExtraHop RevealX licensing and professional services costs	Composite	$0	$650,000	$700,000	$750,000
E2	One-time professional services costs during implementation	Composite	$130,000	$0	$0	$0
Et	ExtraHop RevealX subscription costs	E1+E2	$130,000	$650,000	$700,000	$750,000
	Risk adjustment	↑10%				
Etr	ExtraHop RevealX subscription costs (risk-adjusted)		$143,000	$715,000	$770,000	$825,000
	Three-year total: $2,453,000			**Three-year present value: $2,049,198**		

Implementation And Training Costs

Evidence and data. Interviewees shared that during the implementation process, their organizations dedicated a small team of FTEs to deploying RevealX. Implementation tasks consisted of meeting with ExtraHop, deploying sensors in their network, and configuring the product to determine how alerts will be handled and which type will be escalated. In addition to the deployment process, interviewees reported that some employee time was required for training during the implementation process.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization deploys RevealX over the course of 10 weeks.
- The composite has a team of four people that dedicate 50% of their time to the implementation process during the 10-week period.
- During the initial period, 20 employees are trained on using RevealX with training taking 16 hours per employee. To account for new hires and churn, three employees are trained on using RevealX in the following years.
- The fully burdened hourly rate for a security employee is $65.

Risks. Implementation and training costs will vary depending on:

- Implementation delays.
- The fully burdened hourly rate for an FTE involved in implementation and training.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $89,000.

Implementation And Training Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Internal employees dedicated to implementing ExtraHop RevealX	Composite	4			
F2	Time spent on implementation process (weeks)	Interviews	10			
F3	Percentage of time dedicated to implementation process	Interviews	50%			
F4	Total implementation time (hours)	F1*F2*F3*40 hours per week	800			
F5	Fully burdened hourly rate for an FTE	Composite	$65	$65	$65	$65
F6	**Subtotal: Internal labor costs for ExtraHop RevealX implementation**	**F4*F5**	**$52,000**			
F7	Employees trained to use ExtraHop RevealX	Composite	20	3	3	3
F8	Training time for a new user (hours)	Composite	16	16	16	16
F9	**Subtotal: Internal training costs**	**F7*F8*F5**	**$20,800**	**$3,120**	**$3,120**	**$3,120**
Ft	Implementation and training costs	F6+F9	$72,800	$3,120	$3,120	$3,120
	Risk adjustment	↑10%				
Ftr	Implementation and training costs (risk-adjusted)		$80,080	$3,432	$3,432	$3,432
	Three-year total: $90,376			**Three-year present value: $88,615**		

Ongoing Management Costs

Evidence and data. Interviewees reported that some employee time was dedicated to managing the RevealX deployment, with tasks consisting of meeting with ExtraHop, reviewing network performance, and handling any updates or maintenance.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization has two FTEs in charge of managing the platform, with each FTE dedicating 20% of their time to RevealX management work.
- The average fully burdened annual salary for a security employee is $135,000.

Risks. Ongoing management costs will vary depending on:

- The level of skill and internal effort per resource dedicated to managing RevealX.
- The average fully burdened annual salary for a RevealX platform manager.

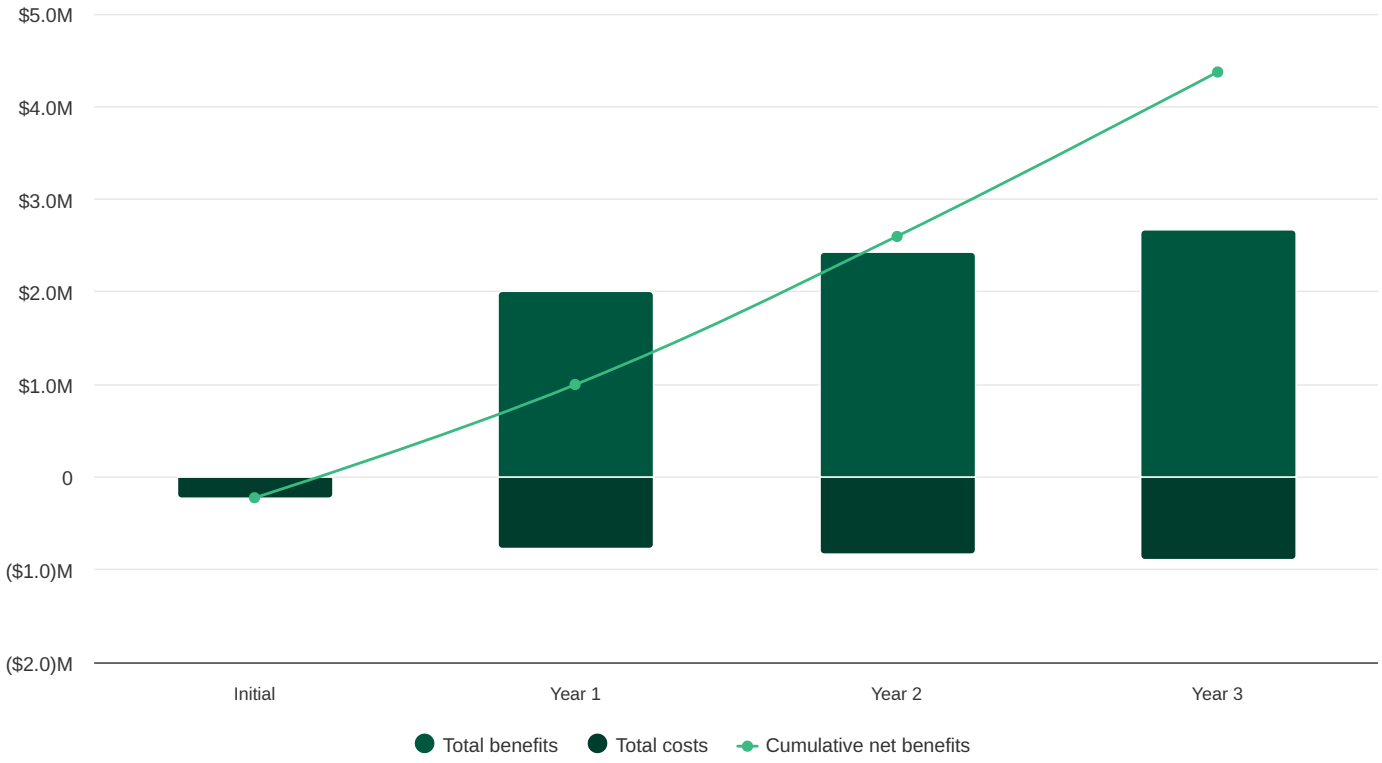
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $148,000.

Ongoing Management Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Employees dedicated to managing ExtraHop RevealX	Composite		2	2	2
G2	Percentage of time dedicated to managing ExtraHop RevealX	Composite		20%	20%	20%
G3	Fully burdened annual salary for an ExtraHop RevealX platform manager	Composite	$135,000	$135,000	$135,000	$135,000
Gt	Ongoing management costs	G1*G2*G3	$0	$54,000	$54,000	$54,000
	Risk adjustment	↑10%				
Gtr	Ongoing management costs (risk-adjusted)		$0	$59,400	$59,400	$59,400
	Three-year total: $178,200			**Three-year present value: $147,719**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($223,080)	($777,832)	($832,832)	($887,832)	($2,721,576)	($2,285,532)
Total benefits	$0	$2,000,497	$2,430,981	$2,663,464	$7,094,942	$5,828,809
Net benefits	($223,080)	$1,222,665	$1,598,149	$1,775,632	$4,373,366	$3,543,277
ROI						155%
Payback						<6 months

Please Note

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

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

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.

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 RevealX.

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 RevealX can have on an organization.

Due Diligence

Interviewed ExtraHop stakeholders and Forrester analysts to gather data relative to RevealX.

Interviews

Interviewed four decision-makers at organizations using RevealX to obtain data about 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.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

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

Risks

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."

Financial Terminology

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PVs 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

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

Appendixes

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

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

[2] Source: Cumulative breach costs are computed using the composite organization's size (revenue or number of employees) as an input to a regression analysis of reported total cumulative costs for all breaches for organizations that experienced at least one breach in the past 12 months. Source: Forrester's Security Survey, 2025, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,740 global security decision-makers who have experienced a breach in the past 12 months. The cumulative breach cost is then multiplied by a 67% likelihood for organizations to experience one or more breaches in a given year. Source: Forrester's Security Survey, 2025, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,643 global security decision-makers.

[3] Source: Percentage of breaches by primary attack vector, as reported by security decision-makers whose organizations experienced at least one breach in the last 12 months. Source: Forrester's Security Survey, 2025, "Of the times that your organization's sensitive data was potentially compromised or breached in the past 12 months, please indicate how many of each fall into the categories below." Base: 1,766 global security decision-makers who have experienced a breach in the past 12 months.

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 RevealX.

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.

Consulting Team:
Matt Dunham

PUBLISHED
February 2026