

FORRESTER®

The Total Economic Impact™ Of ExtraHop Reveal(x)

Business Benefits And Cost Savings
Enabled By Reveal(x)

AUGUST 2020

Table Of Contents

Consulting Team: Nick Mayberry

- Executive Summary 1**
- The ExtraHop Reveal(x) Customer Journey..... 5**
 - Key Challenges 5
 - Composite Organization..... 6
- Analysis Of Benefits 7**
 - Improved Time To Threat Detection And Resolution 7
 - Improved Efficiency Responding To Unplanned Network Outages..... 9
 - Improved Time To Troubleshoot Applications..... 10
 - Reduced Cost Of Third-Party Security Solutions . 11
 - Unquantified Benefits 12
 - Flexibility..... 13
- Analysis Of Costs 15**
 - Cost of Licensing Fees, Including Training 15
 - Cost Of Implementation And Deployment..... 16
 - Cost Of Ongoing Management 17
- Financial Summary 19**
- Appendix A: Total Economic Impact 20**



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

© 2020, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

ExtraHop Reveal(x) provides operational and business value for security use cases, while also being leveraged by other groups within IT operations to improve performance and network hygiene. Using Reveal(x), Forrester estimates an **84%** decrease in time to threat resolution, a **50%** decrease in time to threat detection, and a **99.6%** reduction in time to troubleshoot applications. Additionally, some customers were able to save as much as **\$700,000** annually by replacing pre-existing security solutions with Reveal(x).

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

ExtraHop Reveal(x) is a security solution that not only provides threat detection but also broad east-west visibility into traffic flow within network environments. Reveal(x) use cases therefore extend beyond simple threat detection, using machine learning techniques to advance threat hunting and investigation, asset identification, and application and network performance monitoring.

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

Prior to using ExtraHop Reveal(x), the customers were using a combination of packet capture tools, endpoint detection and response (EDR) products, and security information and event management (SIEM) solutions. However, even with all these tools fully operational, significant holes remained in their security posture. Additionally, these organizations needed security analysts and network engineers to

KEY STATISTICS



Return on investment (ROI)
165%



Net present value (NPV)
\$710,154

spend extensive time and effort wading through alerts, researching potential threats, and determining how to properly respond if necessary.

After the investment in ExtraHop Reveal(x), the customers reported significantly enhanced network visibility. This immediate and holistic insight provided the clarity needed not only to detect and respond to security threats at a much faster rate, but also to analyze end-user behavior and detect anomalies that could pose a threat, and to monitor and troubleshoot both application and network performance.

Total Three-Year
Benefits

\$1.1 million



KEY FINDINGS

Quantified benefits. Three-year risk-adjusted present value (PV) quantified benefits include:

- **Improved time to threat detection and resolution worth \$243,401.** ExtraHop Reveal(x) decreased time to threat detection by 50%, and time to threat resolution by 84% from 8 hours to 1.25 hours. In total, time to respond decreased 81%, from 9 hours to 1.75 hours, saving a total of 7.25 hours on each threat detection and resolution process.
- **Improved efficiency responding to unplanned network outages valued at \$159,805.** After implementing ExtraHop Reveal(x), unexpected network outages decreased by 90% and the time to solve any unplanned network outages decreased 92%. The total hours per IT professional spent investigating unplanned outages decreased by 119 hours annually, saving nearly \$12,000 per professional.
- **Improved time to troubleshoot applications worth \$106,975.** ExtraHop Reveal(x) decreased time to troubleshoot applications by 99.6%, from 40 hours to a matter of minutes for each application failure. Assuming there are 12 application failures annually, Reveal(x) would save 478 full time employee (FTE) hours each year.
- **Reduced cost of third-party security solutions valued at \$631,104.** A subset of customers reported the ability to decommission preexisting security solutions, with some of these costing as much as \$700,000 annually.

Unquantified benefits. Benefits that were reported but are not quantified in this study include:

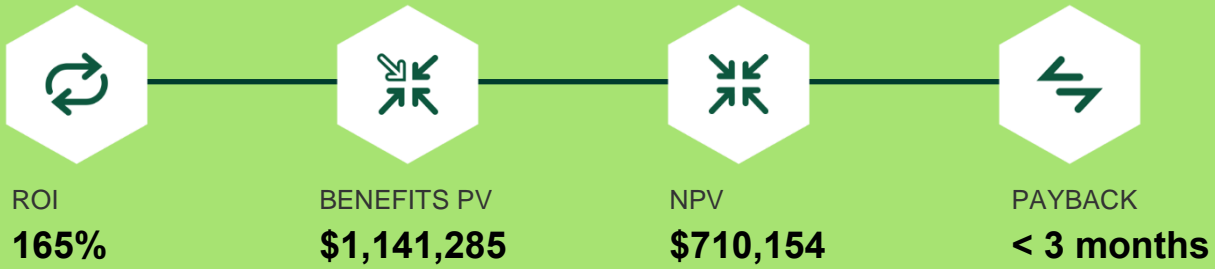
- **Additional revenue and productivity from improved uptime.** Interviewees reported that the additional network and application uptime from ExtraHop Reveal(x) resulted in increases to both revenue and employee productivity.

- **Reduced risk of security breaches.** ExtraHop Reveal(x) helped bolster customer security environments, potentially preventing security breaches worth hundreds of millions of dollars in fines, recovery costs, damage to the brand, and customer goodwill.
- **Reduced product development costs.** For one customer, ExtraHop Reveal(x) was able to reduce product development time, saving a reported 15% of costs and the equivalent cost of three FTEs.

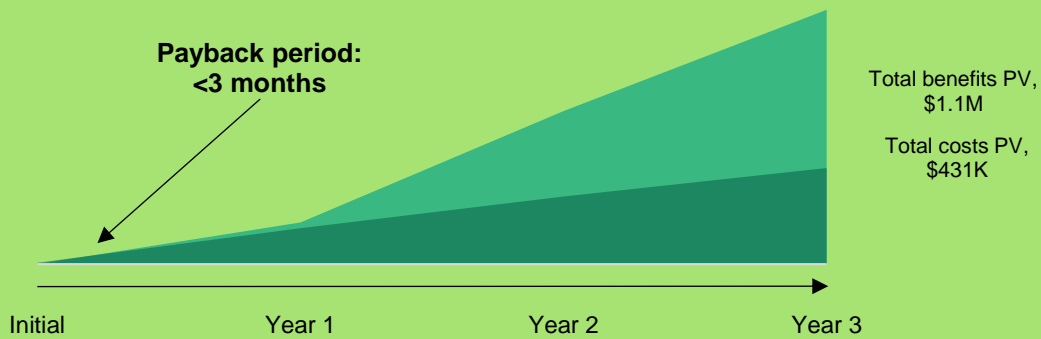
Costs. Three-year risk-adjusted PV costs include:

- **Cost of licensing fees and one-time training costs, totaling \$397,896.** ExtraHop Networks offers Reveal(x) at different tiers, ranging in average selling price (ASP) from \$18,000 to \$450,000 depending on attack surface coverage, number of business-critical devices, and number of clouds and instances. The product is also offered as software as a service (SaaS), however the customers interviewed had not deployed in that model.
- **Cost of implementation and deployment totaling \$5,880.** Customers reported implementation time of three weeks, requiring three FTEs at various utilization rates.
- **Cost of ongoing management totaling \$27,355.** Ongoing management of ExtraHop Reveal(x) required one FTE at 2 hours weekly.

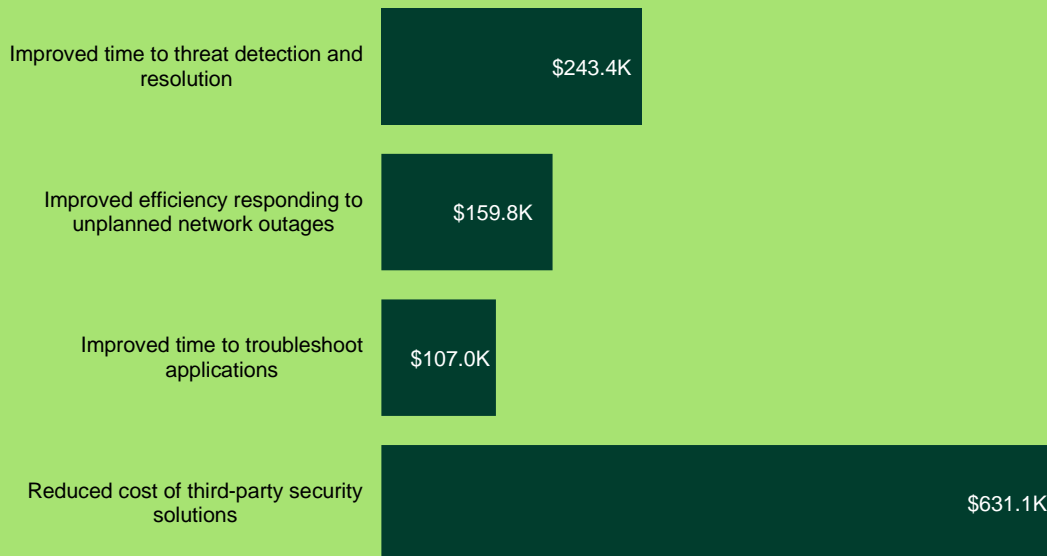
The customer interviews and financial analysis found that a composite organization experiences benefits of \$1,141,285 over three years versus costs of \$431,131, adding up to a net present value (NPV) of \$710,154 and an ROI of 165%.



Financial Summary



Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in ExtraHop Reveal(x).

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 ExtraHop Reveal(x) can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by ExtraHop Networks 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 report to determine the appropriateness of an investment in ExtraHop Reveal(x).

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



DUE DILIGENCE

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



CUSTOMER INTERVIEWS

Interviewed five decision makers at organizations using ExtraHop Reveal(x) to obtain data with respect to costs, benefits, and risks.



COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed organizations.



FINANCIAL MODEL FRAMEWORK

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



CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The ExtraHop Reveal(x) Customer Journey

■ Drivers leading to the Reveal(x) investment

Interviewed Organizations			
Industry	Region	Interviewee	Revenues and total FTEs
Media and entertainment	US	Chief architect	\$1 billion and 850 FTEs
Healthcare	US	CISO	\$1 billion and 8,500 FTEs
Financial services	US	SVP of global infrastructure	\$1.1 billion and 600 FTEs
Manufacturing	US	Director of technology services	\$1.3 billion and 2,000 FTEs
Financial services	US	VP of network intrusion, detection, and prevention	\$6.7 billion and 20,000 FTEs

KEY CHALLENGES

Before investing in ExtraHop Reveal(x), the interviewed customers were using an array of tools to glean information about the security of their environments, including packet capture, EDR, and SIEM solutions.

The interviewed organizations struggled with common challenges, including:

- **Lack of visibility.** Despite having invested in multiple security solutions, the customers revealed their network security environments were still replete with gaps. For example, they said EDR solutions would stop reporting if CPU usage reached 100%, and SIEM tools were reporting data from logs limited by what developers could predict and code for. The SVP of global infrastructure from the financial services sector said: "The biggest challenge that we had was around getting better visibility into the network as a whole — not just from a security perspective, but from a performance perspective as well."
- **Time-intensive security workflows.** The customers also said their security workflows were too time-consuming before investing in Reveal(x),

"We had SIEM, but there were always holes in that information. We added EDR, and there were still certain bits of information missing. We didn't get the full picture until investing in ExtraHop Reveal(x)."

SVP of global infrastructure, financial services

largely because of limited visibility from packet capture tools and an overabundance of security alerts coming from legacy solutions. The SVP of global infrastructure shared: " We were spending a lot of time in our packet capture tool troubleshooting problems and threat hunting. It was very time-consuming. We needed something that would provide better analytics and be able to help us find problems more quickly." The director of technology services from the manufacturing sector stated: "The added visibility with Reveal(x) is great, but you also get added intelligence about what's important, baked in. Our prior solution was giving us 99% false positives."

COMPOSITE ORGANIZATION

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

Description of composite. This billion-dollar financial services organization serves customers across North America both online and in brick-and-mortar branches. It has 1,000 full-time employees in total, and 20 are responsible for security.

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

Key assumptions

- **\$1 billion in revenue**
- **1,000 FTEs**
- **20 FTEs responsible for network security**

“Whenever ExtraHop throws an alert at us, we pay attention because it’s not just noise. With other tools, there was so much noise. It would have taken us years to make those useful.”

*Director of technology services,
manufacturing*

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 time to threat detection and resolution	\$97,875	\$97,875	\$97,875	\$293,625	\$243,401
Btr	Improved efficiency responding to unplanned network outages	\$64,260	\$64,260	\$64,260	\$192,780	\$159,805
Ctr	Improved time to troubleshoot applications	\$43,016	\$43,016	\$43,016	\$129,049	\$106,975
Dtr	Reduced cost of third-party security solutions	\$0	\$400,000	\$400,000	\$800,000	\$631,104
Total benefits (risk-adjusted)		\$205,151	\$605,151	\$605,151	\$1,415,454	\$1,141,285

IMPROVED TIME TO THREAT DETECTION AND RESOLUTION

Evidence and data. The interviewed customers experienced substantial time savings to their threat detection and resolution processes using ExtraHop Reveal(x). Before deploying Reveal(x), they used a combination of security solutions that still left gaps in network visibility. Each of these gaps would require significant security analyst effort to validate whether or not a network anomaly was a true security threat and, if it was, to decide how to adequately resolve the threat.

Older, packet-based network security tools in particular added additional workflow inefficiencies by inundating security analysts with alerts, the vast majority of which were benign. The SVP of global infrastructure from the financial services sector said: “Before, we would get thousands of alerts. It was overwhelming. Reveal(x) has done a good job knocking this down to the 25 most important potential threats that we then go and investigate. Because we now have the visibility, we aren’t getting death by alert. We’re truly paying attention to what’s real.” The director of technology services from the

manufacturing industry added: “Whenever Reveal(x) throws an alert at us, we pay attention because it’s not just noise.”

“Within the first three days of the proof of concept, ExtraHop had delivered on 10 different use cases that I had asked all vendors we were considering to provide. I wrote another 10 more, and [ExtraHop] delivered on those as well. I had 20 use cases done in less than 10 days, just from the proof of concept. We hadn’t even purchased yet.”

SVP of global infrastructure, financial services

Modeling and assumptions. Based on the customer interviews, Forrester estimates for the composite organization:

- A single IT professional runs each threat detection and resolution process.
- Three threat detection and response processes run weekly for a total of 150 processes annually.
- A fully burdened hourly rate of \$100 per IT professional.

Risks. The actual improvement in threat detection and resolution time may vary based on:

- The total number of threat detection and resolution processes run annually and the number of professionals performing this function.
- The prior time spent on each threat detection and resolution process.

- The fully burdened hourly rate of the IT professionals tasked with threat detection and resolution processes.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of \$243,401.

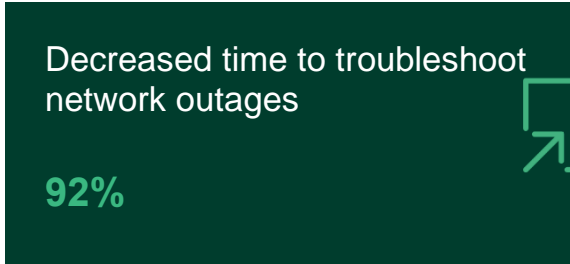
“Our prior solutions provided a lot of alerts, but those don’t mean a whole lot to a human trying to process it. You have to go back and look at the entire conversation to determine what actually happened to determine if it was a true security hit.”

The VP of network intrusion, detection, and prevention, financial services

Improved Time To Threat Detection And Resolution					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Number of IT professionals running threat detection and resolution	Interviews	1	1	1
A2	Number of threat processes per IT professional annually	Interviews	150	150	150
A3	Prior hours to threat detection	Interviews	1	1	1
A4	New hours to threat detection	Interviews	0.5	0.5	0.5
A5	Prior hours to threat resolution	Interviews	8	8	8
A6	New hours to threat resolution	Interviews	1.25	1.25	1.25
A7	Total hours saved per process	A3-A4+A5-A6	7.25	7.25	7.25
A8	IT professional fully burdened hourly rate		\$100	\$100	\$100
A _t	Improved time to threat detection and resolution	A1*A2*A7*A8	\$108,750	\$108,750	\$108,750
	Risk adjustment	↓10%			
A _{tr}	Improved time to threat detection and resolution (risk-adjusted)		\$97,875	\$97,875	\$97,875
Three-year total: \$293,625			Three-year present value: \$243,401		

IMPROVED EFFICIENCY RESPONDING TO UNPLANNED NETWORK OUTAGES

Evidence and data. Although solutions like ExtraHop Reveal(x) are often thought of as security tools first, interviewed customers revealed that many of the benefits they received were broader in scope. One example is the improved operational efficiency customers reported related to responding to unplanned network outages. Thanks to broad network data that Reveal(x) tracks and analyzes coupled with a targeted alert system, network professionals reported the ability to know about a network outage and begin remediating it before external parties notify them of it. The SVP of global infrastructure from the financial services industry said: “We used to average around 20 outages a year that we didn’t know about beforehand. Now, there’s maybe one or two a year that we don’t already know about or are already working on before we get a call.”



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

- Six IT professionals are needed to address each unplanned network outage.
- A fully burdened hourly rate of \$100 per IT professional.

Risks. The improved efficiency responding to unplanned network outages will vary with:

- The number of network outages and the time spent responding to these outages.
- The number of IT professionals responding to network outages.
- The fully burdened hourly rate of the IT professionals responding to network outages.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$159,805.

“We use Reveal(x) for change management to predict potential problems with changes. We use it after the fact to see that it didn’t cause problems. We use it for troubleshooting constantly just to deal with different issues, like [when there’s] a security change, the firewall is causing a problem, or we have this blocker that activated. We can now prove that those things are happening.”

SVP of global infrastructure, financial services

Improved Efficiency Responding To Unplanned Network Outages					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Prior number of outages as reported by the support desk	Interviews	20	20	20
B2	Prior hours spent on researching each outage	Interviews	6	6	6
B3	New number of outages as reported by the support desk	Interviews	2	2	2
B4	New hours spent researching each outage	Interviews	0.5	0.5	0.5
B5	Subtotal hours saved researching outages reported by the support desk	(B1*B2)-(B3*B4)	119	119	119
B6	Number of IT professionals		6	6	6
B7	IT professional fully burdened hourly rate	A8	\$100	\$100	\$100
Bt	Improved efficiency responding to unplanned network outages	B5*B6*B7	\$71,400	\$71,400	\$71,400
	Risk adjustment	↓10%			
Btr	Improved efficiency responding to unplanned network outages (risk-adjusted)		\$64,260	\$64,260	\$64,260
Three-year total: \$192,780			Three-year present value: \$159,805		

IMPROVED TIME TO TROUBLESHOOT APPLICATIONS

Evidence and data. Not only did customers report substantial time savings related to solving unplanned network outages, they also experienced efficiency savings related to troubleshooting application failures. The core driver of this increased efficiency is the at-hand visibility Reveal(x) provides related to application performance with real-time views into all network transactions and decryption of secure sockets layer(SSL)/transport layer security (TLS). The CISO from the healthcare sector elaborated: “We used to spend a large part of our time monitoring application uptime in our prior environment. With the visibility from Reveal(x), we can now work much more efficiently.”

This added visibility translated into customer-reported time savings of 480 times. The SVP of global infrastructure from the financial services industry


detailed: “Now, instead of spending two weeks digging into an application problem, I know within minutes what the issue is and what vendor I need to call to fix things.”

“I would say our number one benefit is being able to identify application or website performance issues.”

VP of network intrusion, detection, and prevention, financial services

Decreased time to troubleshoot applications

99.6%



Modeling and assumptions. Based on the customer interviews, Forrester estimates for the composite organization:

- Twelve application failures requiring troubleshooting annually.
- One IT professional needed to troubleshoot each application failure.
- A fully burdened hourly rate of \$100 per IT professional.

Risks. The actual improved time to troubleshoot applications may vary based on:

- The time spent troubleshooting each application failure.
- The number of application failures requiring troubleshooting annually.
- The number of IT professionals troubleshooting each application failure.
- The fully burdened hourly rate of these IT professionals.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$106,975.

Improved Time To Troubleshoot Applications					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Prior hours spent troubleshooting each application failure	Interviews; 1 week	40	40	40
C2	New hours spent troubleshooting each application failure	Interviews; 10 minutes	0.17	0.17	0.17
C3	Annual application failures requiring troubleshooting	Interviews	12	12	12
C4	Number of IT professionals		1	1	1
C5	IT professional fully burdened hourly rate	A8	\$100	\$100	\$100
Ct	Improved time to troubleshoot applications	$(C1-C2)*C3*$ $C4*C5$	\$47,796	\$47,796	\$47,796
	Risk adjustment	↓10%			
Ctr	Improved time to troubleshoot applications (risk-adjusted)		\$43,016	\$43,016	\$43,016
Three-year total: \$129,049			Three-year present value: \$106,975		

REDUCED COST OF THIRD-PARTY SECURITY SOLUTIONS

Evidence and data. Although some customers deployed ExtraHop Reveal(x) as an additional solution within their security technology stack, others reported that implementing ExtraHop Reveal(x) allowed them to retire a subset of their existing security solutions. For example, the VP of network intrusion, detection, and prevention from the financial services industry reported decommissioning an older

packet-based network security tool, network testing devices, and even a competing solution. Meanwhile, the customer from the media and entertainment industry said their organization retired its vulnerability scanner, and the SVP of global architecture reported decommissioning their firm’s legacy packet-based network security tool alone.

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

- One third-party security solution at \$500,000 annual cost is fully retired by Year 2.

Risks. The reduced cost of third-party security solutions will vary with:

- The number of security solutions decommissioned or retired.

- The total annual cost of decommissioned or retired third-party security solutions.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of \$631,104.

Reduced Cost Of Third-Party Security Solutions					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Annual cost of retired packet capture tool	Interviews	\$0	\$500,000	\$500,000
Dt	Reduced cost of third-party security solutions	D1	\$0	\$500,000	\$500,000
	Risk adjustment	↓20%			
Dtr	Reduced cost of third-party security solutions (risk-adjusted)		\$0	\$400,000	\$400,000
Three-year total: \$800,000			Three-year present value: \$631,104		

UNQUANTIFIED BENEFITS

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

- **Additional revenue and productivity from improved uptime.** Because ExtraHop Reveal(x) provided customers the visibility needed to resolve both network and application outages more quickly than in their prior environment, customers reported an increase in employee productivity as well as revenues from this increased uptime. The director of technology services from the manufacturing sector stated: “As soon as our systems are unavailable, all of our associates working on the shop floor stop. They’re not able to produce. The immediate impact is opportunity cost related to all the salaries of those people on the shop floor who are now unable to actually be productive and produce products for the company.”

In terms of revenue, the VP of network intrusion, detection, and prevention shared: “When our site is down, customers can’t get to our sales channel to sign up additional services. That delivers a potential revenue loss we avoid with ExtraHop.”

“What’s been interesting is the revenue savers or cost avoidance that have been application-related. We found big problems with important applications that we never knew existed thanks to Reveal(x)’s added visibility.”

SVP of global infrastructure, financial services

- **Reduced risk of security breaches.** Customers shared that ExtraHop Reveal(x) helped them achieve a better security posture thanks to faster threat detection and remediation. This had knock-on benefits of preventing potential loss to brand value and customer goodwill, as stated by the media and entertainment customer. Similarly, the manufacturing firm was able to reduce its cybersecurity insurance premium because of Reveal(x)'s higher compliance with its policy provider's standards. Lastly, the CISO from the healthcare industry reported potentially saving "multiple millions of dollars" thanks to additional risk mitigation from Reveal(x).

"We have a lot of personally identifiable information from our users and are subject to both the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR). Reveal(x) is helping us avoid a security breach that could cost us hundreds of millions of dollars in fines alone, not to mention the cost to our brand reputation."

Chief architect, media and entertainment

- **Reduced product development costs.** Interestingly, the media and entertainment firm also reported achieving substantial cost reductions to its product development process from ExtraHop Reveal(x). Before implementation, the organization would have to test and validate every feature release both within the development studio and by the security team. With Reveal(x) the studio team can handle this on its own, increasing the frequency of feature releases from one every three days, to two to three features every day. The chief architect of the firm detailed: "We're saving 15% of product

development costs with Reveal(x) and saving the equivalent of three full-time roles at a total of \$600,000 annually."

FLEXIBILITY

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

- **Flexibility in times of crisis.** Customers reported ExtraHop Reveal(x) enabled them to mitigate friction in the transition from an in-office environment to a work-from-home environment during the COVID-19 pandemic. For example, the VP of network intrusion, detection, and prevention from the financial services sector was able to get visibility into why employees were having difficulty accessing certain applications over VPN from home, and quickly troubleshoot solutions to these issues. The CISO from healthcare shared: "Working from home increases our risk profile significantly. East-west visibility from Reveal(x) helps to mitigate this."

"We were able to optimize that work-from-home network environment to make it all work much more efficiently so that we're not double-dipping on net flows going in and back out of the core data center."

VP of network intrusion, detection, and response, financial services

- **Targeted use cases.** Interviewed organizations relayed that ExtraHop helped them build custom triggers and dashboards into ExtraHop Reveal(x) that address unique aspects of the different customer environments. One of the financial services firms "worked extensively with ExtraHop to build custom triggers for some of our [domain

service] integrations, our email, and brute force detection.” The manufacturing interviewee said their firm worked with ExtraHop to build “dashboards specific to some critical applications that run our manufacturing process that focus on all the components of those applications.”

“We replaced a lot of our homemade scripts with custom triggers from Reveal(x), which makes everyone sleep a little better at night.”

VP of network intrusion, detection, and response, financial services

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

- **Transition to the cloud.** Although most customers reported plans to use ExtraHop Reveal(x) as an important security tool for their planned use of cloud services in the future, the customer from the media and entertainment industry already implemented the cloud use case. The chief architect shared: “Because Reveal(x) has the ability to see into the different major cloud environments, our studio developers can choose to leverage whatever service works the best for them. I don’t have to hold them back. And the business does not have to spend another \$2 million on port costs and add six weeks to the development timeline. We can just plug it in and go.”

“We expect it to be a key cloud security architecture component to help us trust and verify as we make the transition to cloud services.”

Director of technology services, manufacturing

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	Cost of licensing fees, including training	\$0	\$160,000	\$160,000	\$160,000	\$480,000	\$397,896
Ftr	Cost of implementation and deployment	\$5,880	\$0	\$0	\$0	\$5,880	\$5,880
Gtr	Cost of ongoing management	\$0	\$11,000	\$11,000	\$11,000	\$33,000	\$27,355
	Total costs (risk adjusted)	\$5,880	\$171,000	\$171,000	\$171,000	\$518,880	\$431,131

COST OF LICENSING FEES, INCLUDING TRAINING

Evidence and data. ExtraHop offers different levels of Reveal(x) subscriptions to customers of varying security maturity levels. The service is priced based on attack surface coverage, number of business-critical devices, and software as a service (SaaS), if required. Both virtual and physical sensors (appliances) provide coverage for the attack surface, with enterprise appliances scaling from 1 Gbps to 100 Gbps.

“We did one on-site, 4-hour training with ExtraHop, and six of us have been through their entire virtual training package All of this is included in our licensing.”

SVP of global infrastructure, financial services

The average selling prices (ASPs) for the various configurations range from \$18,000 to \$450,000 annually.

Modeling and assumptions. Forrester estimates for the composite organization include:

- The organization purchases a “medium” configuration supporting the high end of the configuration range at 25 Gbps of throughput and approximately 35,000 devices.
- 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.
- The organization pays the high end of the ASP range of \$160,000 annually.

Risks. The cost of licensing fees will vary with:

- The amount of throughput required for the physical appliances.
- The number of business-critical devices supported.

As Forrester priced the composite organization directly with ExtraHop, this cost has not been adjusted for risk, yielding a three-year total PV (discounted at 10%) of \$397,896.

Cost Of Licensing Fees, Including Training						
Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Annual cost of licensing fees with training included		\$0	\$160,000	\$160,000	\$160,000
Et	Cost of licensing fees, including training	E1	\$0	\$160,000	\$160,000	\$160,000
	Risk adjustment	↑0%				
Etr	Cost of licensing fees, including training (risk-adjusted)		\$0	\$160,000	\$160,000	\$160,000
Three-year total: \$480,000			Three-year present value: \$397,896			

COST OF IMPLEMENTATION AND DEPLOYMENT

Evidence and data. Customers reported a simple implementation process with time to deployment dependent on a number of factors, most notably the organization’s own conservativeness in moving from proof of concept (POC) to deployment. Another factor affecting implementation and deployment was whether or not the organization had already deployed strategic network taps to capture and inspect network traffic at scale. The SVP of global infrastructure from the financial services sector said: “Because we already had some taps in place and some of the equipment in place from our previous packet capture system, Reveal(x) was deployed in less than 24 hours.”

“One of the key differentiators for Reveal(x) is that its engineering talent is crazy. They are some of the most knowledgeable IT people of any IT vendor I’ve come across. Both the pre-sales and post-sales teams are very, very high caliber.”

Director of technology services, manufacturing

Implementation teams typically consisted of a handful of IT professionals from the server, network, and security teams.

Modeling and assumptions. Forrester estimates for the composite organization include:

- A full working week of 40 hours to implement the solution.
- Three IT professionals needed for implementation, one at 100% of time and two at 20% of time each.
- A fully burdened hourly rate for these IT professionals of \$100.

Risks. The cost of implementation and deployment will vary with:

- The number of IT professionals needed to implement the solution.
- The share of time required for each professional for implementation.
- The fully burdened hourly rate of pay for these IT professionals.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of \$5,880.

Cost Of Implementation And Deployment						
Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Hours to implement and deploy	Interviews; 1 week	40			
F2	Number of FTEs needed for implementation and deployment, full time	Interviews; 1 FTE at 100% of time	1			
F3	Number of FTEs needed for implementation and deployment, partial time	Interviews; 2 FTEs at 20% of time	0.4			
F4	IT professional fully burdened hourly rate	A7	\$100			
Ft	Cost of implementation and deployment	$F1*(F2+F3)*F4$	\$5,600	\$0	\$0	\$0
	Risk adjustment	↑5%				
Ftr	Cost of implementation and deployment (risk-adjusted)		\$5,880	\$0	\$0	\$0
Three-year total: \$5,880			Three-year present value: \$5,880			

COST OF ONGOING MANAGEMENT

Evidence and data. Interviewed organizations also reported incurring ongoing management costs. The manufacturing firm had three FTEs spend 15% of their time using ExtraHop Reveal(x), while the VP of network intrusion, detection, and response had a single FTE spend approximately 2 hours per week with the solution.

Modeling and assumptions. Forrester estimates for the composite organization include:

- One FTE spending 2 hours per week with the solution.
- A fully burdened hourly rate for this FTE of \$100.

Risks. The cost of ongoing management will vary with:

- The number of FTEs managing the solution on an ongoing basis.
- The annual time spent for each FTE on managing the solution.
- The fully burdened hourly rate of these FTEs.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of \$27,355

Ongoing Management

1 FTE

2 hours weekly

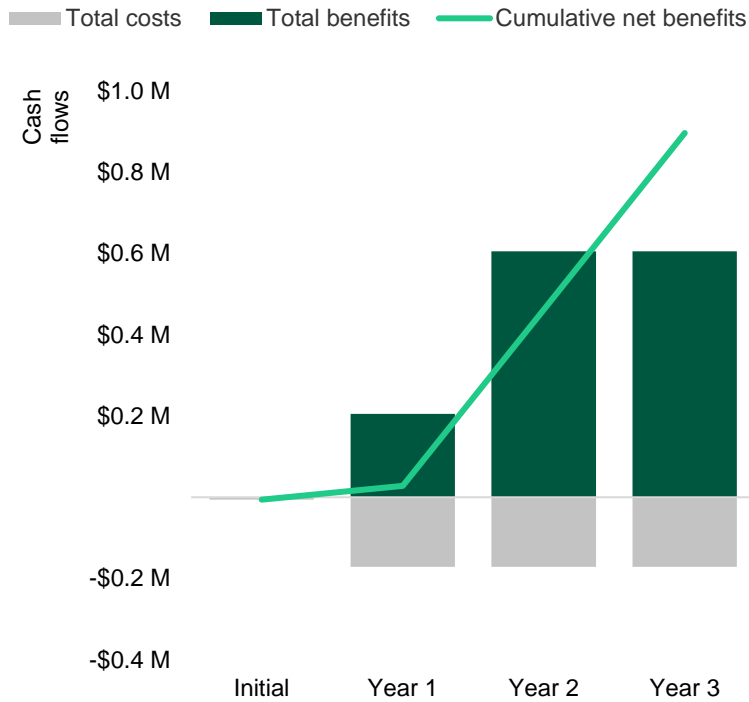
Cost Of Ongoing Management

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
G1	Number of FTEs needed for ongoing management	Interviews		1	1	1
G2	Hours spent weekly on ongoing management	Interviews		2	2	2
G3	IT professional fully burdened hourly salary	A8		\$100	\$100	\$100
Gt	Cost of ongoing management	$G1 * G2 * 50 * G3$	\$0	\$10,000	\$10,000	\$10,000
	Risk adjustment	↑10%				
Gtr	Cost of ongoing management (risk-adjusted)		\$0	\$11,000	\$11,000	\$11,000
Three-year total: \$33,000			Three-year present value: \$27,355			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	(\$5,880)	(\$171,000)	(\$171,000)	(\$171,000)	(\$518,880)	(\$431,131)
Total benefits	\$0	\$205,151	\$605,151	\$605,151	\$1,415,454	\$1,141,285
Net benefits	(\$5,880)	\$34,151	\$434,151	\$434,151	\$896,574	\$710,154
ROI						165%
Payback						< 3 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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



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.

FORRESTER®