A Forrester Total Economic Impact™
Study Commissioned By Cybereason
May 2020

The Total Economic Impact™ Of Cybereason

Cost Savings And Business Benefits Enabled By The Cybereason Defense Platform

FORRESTER®

Table of Contents

Project Director:
Adrienne Capaldo
Project Support:
Sam Sexton

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Key Benefits

Savings from avoided potential cybersecurity threats:
$3.6 million

Reduction in time spent on detection and response to threats:
93%

Reduction in management required:
75%

Executive Summary

As the security threat landscape continues to grow in complexity, organizations are looking for the best solutions to protect their endpoints without overextending their already overworked security and IT teams. These effective and easy-to-use technologies must be able to assess, prioritize, and respond to threats. Cybereason provides a complete endpoint protection platform that meets these key requirements.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with years of experience using the Cybereason Defense Platform.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Dramatically reduces the likelihood of a cybersecurity breach.** With Cybereason, organizations have significantly better visibility into their endpoints and overall threat landscape, improving their security posture. The Cybereason Defense Platform helps organizations better understand the full context and scope of a threat and automatically uncover attacks, reducing the likelihood of a cybersecurity incident. With the investment in Cybereason, organizations save a three-year risk adjusted total PV of nearly $3.6 million.
- **Improves the efficiency in detection and response to threats by 93%.** Cybereason's easy-to-use user interface (UI) enables organizations to rapidly see a threat, investigate its root cause, and understand the full context of the threat, correlations across threats, how the threat affects the entire endpoint environment across platforms, and finally how to best remediate the situation. With Cybereason, organizations can assess, prioritize, and respond to threats faster, resulting in a three-year benefit of nearly $185,000.
- **Reduces the management of the security platform by 75%.** With the investment in Cybereason, organizations can deploy a single lightweight agent that is managed from one console, drastically minimizing the management required and resulting in a savings of more than $130,000 over three years.
- **Prevents expensive future security analyst hires, resulting in savings of more than $288,000 over three years.** Organizations often selected Cybereason over competitors because its easy-to-use platform enables analysts of all levels of expertise to efficiently and effectively mitigate cybersecurity threats. The intuitive UI makes it easy for all analysts to understand the full context and scope of an attack and how to best remediate the issue, ensuring that L3 SecOps FTEs are reserved for the most important tasks.

FORRESTER®

ROI
308%

Benefits PV
$4.2 million

NPV
$3.2 million

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

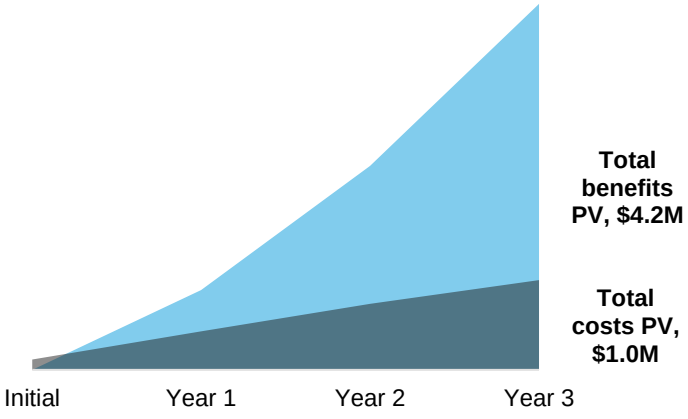
- **Support ticket savings.** Interviewees described how the increased visibility of Cybereason benefits technical support; with SecOps relying less on the help desk to identify and solve issues, the help desk can focus on other tasks. Cybereason helps firms reduce the number of support ticket requests and the time to resolve the issue.
- **Improved compliance and auditing.** Cybereason reduces the time that organizations would otherwise spend on compiling details for audits compared to previous endpoint security solutions.

Costs. The interviewed organizations experienced the following risk-adjusted present value (PV) costs:

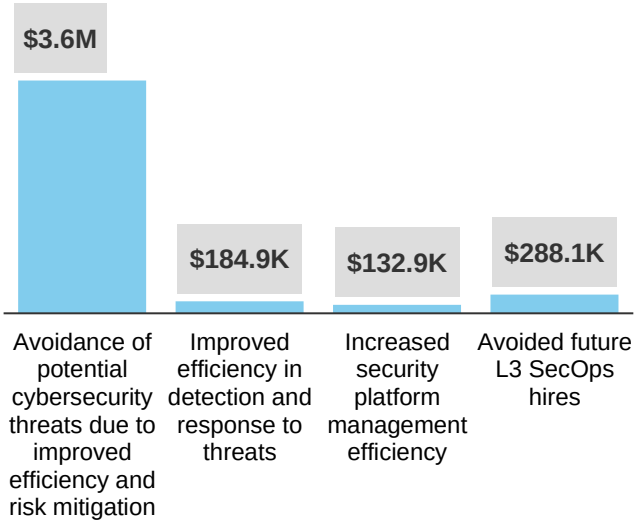
- **Licensing, implementation, management, and training.** These costs look at both the external and internal costs incurred to leverage the Cybereason Defense Platform. This includes licensing costs paid to Cybereason, as well as internal costs for the implementation of Cybereason, ongoing management of the Cybereason platform, and training of the team, resulting in costs of just over $1.0 million for the three years analyzed.

Forrester's interviews with five existing customers and subsequent financial analysis found that a composite organization based on these interviewed organizations experiences benefits of $4.2 million over three years versus costs of $1.0 million, adding up to a net present value (NPV) of $3.2 million and an ROI of 308%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the customer interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering the Cybereason Defense Platform.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision in an endpoint security solution. Forrester took a multistep approach to evaluate the impact that the Cybereason Defense Platform can have on an organization:

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

DUE DILIGENCE
Interviewed Cybereason stakeholders and Forrester analysts to gather data relative to the Cybereason Defense Platform.

CUSTOMER INTERVIEWS
Interviewed five organizations using the Cybereason Defense Platform 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 conservatively 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 Cybereason Defense Platform's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Cybereason Defense Platform Customer Journey

BEFORE AND AFTER THE CYBEREASON DEFENSE PLATFORM INVESTMENT

Interviewed Organizations

For this study, Forrester conducted five interviews with Cybereason Defense Platform customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE	NUMBER OF ENDPOINTS
Food manufacturer	Headquartered in US with global presence	Security IT senior analyst — threat intelligence	72,000 endpoints
Industrial manufacturing	Headquartered in US with European offices	CISO	13,000 endpoints
Health insurance	Headquartered in US	Information security architect	4,300 endpoints
Biotechnology	Headquartered in US, global presence	Information security engineers; Director of security engineering	4,000 endpoints
Retail	Headquartered in UK	Information security manager	5,000 endpoints

Key Challenges

Though interviewed organizations came from a variety of industries and company sizes, they shared similar challenges when it came to protecting their endpoints.

- **Interviewed organizations struggled to gain clear visibility into their endpoints and their threat landscape**. Interviewees noted how their prior solutions created challenges in having a full understanding of what was happening across their endpoints. A senior analyst from the food manufacturer shared: "We were previously using multiple vendors that weren't really EDR [endpoint detection and response]. We were fairly immature. We didn't have a centralized login to see threats." The manufacturer's existing systems often did not provide a cohesive view of the threat landscape, and due to this, the organization lacked the ability to see the full scope of an attack. The retail information security manager explained: "[Our previous system] just really gives an endpoint-centric view such as you see a virus or ransomware or whatever on a single machine and then you see it on another machine and you don't know what's going on between them. It's just not even close to the visibility I require to be able to effectively understand the environment and respond to those kind of threats. We needed something that was far better than what we had." With only limited context into the threat landscape across their endpoints, security teams struggled to accurately assess, prioritize, and respond to threats.

> "Our biggest concern was visibility, especially against advanced threat types."
>
> *CISO, industrial manufacturing*

> "Everything we looked at wanted us to put more and more software packages on our endpoints, which ultimately consumed resources."
>
> *Information security architect, health insurance*

FORRESTER®

- **Inefficient systems and complex workflows further complicated the lack of visibility**. The information security architect from the health insurance organization stated: "Previously, we had several solutions that alerted us of different things that happened. We could see it on one platform, but not all our supported platforms. We had nothing in place to help us understand and trace where it came from or any type of in-depth analysis." The architect added, "Everything we looked at wanted us to put more and more software packages on our endpoints, which ultimately consumed resources." Without proper insights into the full extent of the security threat landscape, the SecOps teams were forced to use inefficient means when faced with a threat. The information security manager at the retail organization summed it up, "We were previously on different tools, different platforms, and we couldn't see or understand how people were working across these tools."
- **Teams struggled to efficiently and effectively manage alerts and incidents**. The lack of visibility and inefficient workflows created inefficiency across the teams. The CISO from the industrial manufacturing organization shared, "Our previous solution was only looking for signature-based threats, and most aren't that anymore because they know they'll be discovered easier." Interviewees noted their previous software solutions involved too much manual effort to understand alerts and investigate threats; solutions required too many resources, creating inefficiencies, bottlenecks, and frustration, leading to slow investigation and remediation and opening the organizations to potential threats. The food manufacturer commented: "We started as a very immature program. We didn't have the systems or workflows in place to support incident response, and we needed to create an incident response program." Without proper visibility and an integrated security stack, organizations struggled to assess, prioritize, and respond to threats in an efficient manner.
- **Overall, organizations needed to better protect the security of their companies and their endpoints**. The key goal across all interviewed organizations was to reduce the risk of a security incident. The biotechnology interviewee shared: "There was stuff we could never detect before, like DNS hijacking and browser hijacking, a bunch of other stuff, and a lot of times that was just never seen. Users had to tell us it was happening. There were times when basically we've had things where we'd find out after a week or two, which is obviously too late again to react quickly — and then we'd actually have to rely on the users to go out and do stuff for remediation, and we would just never get a response from them. It was just too risky." These organizations needed a solution that provided them full visibility into their endpoints, made their teams more efficient, and reduced reliance on complex security systems to reduce this risk.

> "We had three or four different solutions in place, only EPP, and then we acquired a company that had a different EPP [endpoint protection platform] solution. We had no tools that covered the EDR space. We were all over the place. We suffered from lack of forensics, lack of response, and lack of a consolidated platform. We would have users sitting right next to each other being managed by different solutions and different groups."
>
> *Information security engineer, biotechnology*

> "We needed to make sure we didn't introduce any risks that may bring down a factory and cause loss of production. We don't want any of our customers' data to be comprised. We don't want any of our associates' data to be compromised. This is a driving factor for us."
>
> *Security IT senior analyst — threat intelligence, food manufacturer*

> "Cybereason has capabilities to remediate issues and replicate those remediations across the enterprise. We've been able to apply fixes in minutes. The response time from the information security team has increased markedly with Cybereason."
>
> *Information security engineer, biotechnology*

Why Cybereason

The interviewed organizations searched for an endpoint protection vendor that would help them navigate their concerns around security threats, visibility, and efficiency without putting undue burden on their teams. After reviewing and evaluating multiple vendors, the interviewed organizations elected to deploy Cybereason over alternatives for several reasons. Particularly, organizations found the deployment of the solution easy compared to alternatives and appreciated the flexibility of deployment methods, with software-as-a-service (SaaS), on-premises, or

hybrid deployment options. Having one platform that consolidates all EDR and next-generation antivirus (NGAV) capabilities into a single console with an easy-to-use interface reduced stress on the IT and security teams, improving efficiency and productivity. Organizations also found that Cybereason's support across a variety of platforms, including Windows, Mac, Linux, Virtual, iOS, and Android, all within one console, further improved their efficiency. With analytics and machine learning to support enhanced threat detection, interviewed organizations trusted Cybereason to provide complete endpoint protection.

Key Results

The interviews revealed that key results from the Cybereason Platform investment include:

- **Improved visibility into the endpoint threat landscape.** With the Cybereason Defense Platform, all the relevant information to understand an enterprise's endpoints is consolidated into one console to quickly and efficiently understand the scope and impact of threats. The information security manager at the retail organization explained, "Now, with Cybereason, when a Malop [malicious operation] is triggered, I can go and get very, very deep into what was going on at the time, what are the child processes, what are the parent processes, or what files are open, all the rest of the technical information. I would have otherwise had no way of being able to see this."

  Organizations found that with Cybereason, their IT and SecOps teams are no longer bouncing from solution to solution to try to gain a full understanding into an attack; Cybereason provides all the information needed to assess, prioritize, and respond to a threat, requiring significantly less time to investigate and remediate an issue. The director of security engineering at the biotechnology company concluded, "We have more visibility into our security events, which was entirely lacking before."

- **An easier-to-manage platform.** Organizations found that Cybereason is significantly easier to manage than their previous environments or alternative solutions. With cross-platform protection from one console, it allows organizations to more easily protect their endpoints without the need for multiple solutions. The information security architect at the health insurance organization told Forrester, "Cybereason's single agent that had multiple components built into it was very nice feature from our standpoint of having one application to manage, one application to deploy, but yet we got the benefit of multiple components."

  Cybereason is also easy to deploy and provides higher levels of endpoint protection without increased effort. In addition, organizations liked that individuals without specific SecOps training can easily use the platform. An interviewee at the biotechnology company stated: "We needed a solution with an ease of use for the end users because we're going to have people in this that aren't information security engineers. So it had to have a very easy interface to use."

- **Ability to more efficiently assess, prioritize, and respond to threats.** With one console and a single interface to understand alerts and threats, analysts can now better eliminate complex workflows and gain deeper understanding of threats from simplified dashboards. The health insurance interviewee shared: "We're able to spend less time tracking down red herrings or potential false positives because the

> "Having smarter threat detection and visibility across our endpoints with Cybereason aided my operations team to be able to quickly address a situation, triage containment, and jump right into the remediation phase."
>
> *CISO, industrial manufacturing*

> "When we did our PoC, we bounced Cybereason against several other vendors, and the holistic aspect of the application, the fact that it was a single agent that we deployed to each endpoint that had all of these additional capabilities built into it, was beneficial to us."
>
> *Information security architect, health insurance*

> "I would say our reaction time has increased a lot per event with Cybereason. And that has allowed us to mitigate a lot of potential future issues. It allows us to get the root cause quicker and figure out if an alert is due to a malicious file download or something like that; Cybereason makes it easier to pinpoint that. Then we can then analyze it and block future attempts and things like that."
>
> *Information security engineer, biotechnology*

system handles a lot of those false positives for us. It gets rid a lot of the noise. We're able to focus on things that are meaningful that we can evaluate quickly. Just determine, 'Is this a vulnerability that we need to address or not?' And so, it really helps with the management of time." The CISO of the industrial manufacturing organization also revealed how Cybereason changed the firm's ability to more efficiency assess, prioritize, and respond to threats: "Cybereason has changed how we respond, prioritize and categorize our threats. Previously, we had nothing in place. Having the visibility and looking at the different processes running allowed us to have a better grip into what was a true positive, where it came through and why it came through. We were better able to understand the root cause of events."

Organizations found that with the intuitive platform, analysts, particularly those who may have less technical skills, can do a deep dive to truly understand threats and lower investigation times. In fact, the senior analyst of security IT from the food manufacturing organization reported: "Cybereason's detection is particularly valuable to us. [The interface and machine learning] correlate and nest alerts together; this allows any analyst, regardless of skill, to not miss an alert and be able to understand what's taking place across the entire attack." Cybereason's easy-to-use platform also means that every analyst, regardless of level of expertise, becomes more effective, helping organizations avoid the need for expensive L3 hires.

> "It's really easier to tell what's going on with an attack in Cybereason's UI, and because of that, we don't have to invest in higher-skilled analysts, and we're getting more bang for our buck with the product."
>
> *Security IT senior analyst — threat intelligence, food manufacturer*

- **Reduced risk against threats**. The Cybereason Defense Platform provides the interviewed organizations with a complete solution that improves their security posture. The information security architect at the health insurance organization stated: "I would say that Cybereason is protecting us against some things that our previous security control did not cover us on. So we wanted to leverage Cybereason proprietary components of behavioral analytics to protect us."

  Cybereason has helped organizations understand and stop a variety of attacks, including viruses, ransomware, and fileless attacks, as well as unknown attacks. With machine learning, Cybereason analyzes potential attacks and enables organizations to reduce risk through identifying threats in real time. The food manufacturer interviewee put it bluntly: "Cybereason has helped us detect some really nasty stuff." Additionally, organizations found that with Cybereason's cross-machine correlation, they can remediate threats on all machines quickly and easily; for one organization, this meant it no longer relies solely on wiping a machine and can now dig deeper to truly understand the risk and reduce the impact on the organization. "With Cybereason, we reduced the need for reimaging laptops from multiple times a week to less than a dozen, maybe only six, in the past year." Finally, automation across the platform has enabled teams to swiftly react to threats, without requiring advanced skills or slow-moving investigations.

> "I am able to give the business a much better state of mind in terms of security across the enterprise and across all our platforms that we have with Cybereason. Without Cybereason, we would not be able to have the visibility into our risk that we have now."
>
> *Information security manager, retail*

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated 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 that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. The composite organization is a US-based organization with a global presence. The organization has a total of 7,500 employees. Across those employees, there are a total of over 9,000 endpoints, growing to more than 10,000 by Year 3 of the study.

Deployment characteristics. The composite organization purchases the Cybereason Defense Platform to protect each of its endpoints, which increase at 10% each year. Prior to investment in Cybereason, the composite organization used multiple solutions to manage security but specifically found their EDR and NGAV capabilities lacking.

Key assumptions

- US-based organization
- 10,000+ endpoints protected by Year 3
- 7,500 employees

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE ORGANIZATION

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Avoidance of potential cybersecurity threats due to improved efficiency and risk mitigation	$874,800	$1,443,420	$2,117,016	$4,435,236	$3,578,727
Btr	Improved efficiency in detection and response to threats	$74,229	$74,364	$74,498	$223,091	$184,911
Ctr	Increased security platform management efficiency	$52,397	$52,397	$52,397	$157,192	$130,304
Dtr	Avoided future L3 SecOps hires	$0	$147,488	$221,231	$368,719	$288,105
	Total benefits (risk-adjusted)	$1,001,427	$1,717,669	$2,465,143	$5,184,238	$4,182,047

Avoidance Of Potential Cybersecurity Threats Due To Improved Efficiency And Risk Mitigation

Prior to their investment in the Cybereason Defense Platform, organizations struggled with visibility into their endpoints and their overall threat landscape.

With multiple disparate solutions that did not provide the level of EDR and NGAV capabilities the organization required, the composite struggled to gain a true understanding of its security risk posture. With the implementation of Cybereason, the composite organization now has a clear view into its endpoints within one console. Cybereason provides the organization with visibility across all endpoints, regardless of platform, allowing the SecOps team to more efficiently get a deeper understanding of the threat landscape, with all relevant information in one place.

The composite organization can now see where potential security threats are coming from, the scope of the threats, and how to best protect its endpoints. With Cybereason, the organization can now stop a variety of known and unknown attacks. Cybereason's analytics and machine learning also ensure the composite organization reduces its security risk through analyzing and identifying threats in real time. With Cybereason, the composite organization can now more efficiently and effectively avoid potential threats.

To consider how this improved visibility, efficiency, and risk mitigation help the composite organization avoid potential cybersecurity threats, Forrester assumes that:

- Each endpoint across the organization has access to 150 sensitive data assets, with an average value of $12 per data asset.
- The likelihood of a breach without Cybereason is 30%. This number will vary based on industry and location, among other factors.

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10% to take into account the time value of money, as described in Appendix A. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of nearly $4.2 million.

"There's that constant struggle when you look at managing and protecting those endpoint devices around ransomware, malware, those complex components that show up in almost every avenue of our daily lives as we work through utilizing technology. We are looking at ways to enhance our security controls and better understand our risk posture by leveraging Cybereason."

Information security architect, health insurance

› With the investment in Cybereason, the composite organization reduces the likelihood of a breach by 20% in Year 1. As the SecOps team becomes more efficient at utilizing the Cybereason Defense Platform, this improves to 40% by Year 3.

To calculate the value of the benefit, we consider the potential cost of a breach without Cybereason versus the cost of a breach with Cybereason.

When weighing the value of this benefit for your organization, consider the value of your data assets and the number of data assets that are at risk on any given endpoint. Also consider the potential extent of costs beyond the value of the asset, such as impact on your organization's brand perception, how this may affect customer churn, and other business cost impacts.

The value of this benefit can vary due to a variety of factors, including:

The size, industry, region, and other factors of an organization that may impact the value of their data assets or the likelihood of a cybersecurity event.

› The severity of a security event.

› How the organization leverages Cybereason to reduce the risk associated with cyberthreats.

To account for these risks and maintain a conservative approach, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of nearly $3.6 million.

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

Avoidance Of Potential Cybersecurity Threats Due To Improved Efficiency and Risk Mitigation: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
A1	Number of endpoints		9,000	9,900	10,890
A2	Data assets protected	150 sensitive data assets per endpoint	150	150	150
A3	Average value of data asset		$12	$12	$12
A4	Potential impact of breach without Cybereason	A1*A2*A3	$16,200,000	$17,820,000	$19,602,000
A5	Likelihood of breach without Cybereason		30%	30%	30%
A6	Potential cost of breach without Cybereason	A4*A5	$4,860,000	$5,346,000	$5,880,600
A7	Reduction in likelihood of incident due to Cybereason		20%	30%	40%
At	Avoidance of potential cybersecurity threats due to improved efficiency and risk mitigation	A6*A7	$972,000	$1,603,800	$2,352,240
	Risk adjustment	↓10%			
Atr	Avoidance of potential cybersecurity threats due to improved efficiency and risk mitigation (risk-adjusted)		$874,800	$1,443,420	$2,117,016

Improved Efficiency In Detection And Response To Threats

Cybereason dramatically cuts the time required to detect and remediate potential threats. Prior to its investment in Cybereason, the composite organization struggled to truly understand the full scope of a potential threat; the organization had limited visibility into the root cause of a problem or the full extent of the problem, resulting in a significant amount of time spent detecting, investigating, and remediating the issue. In its previous implementation, the organization also spent wasted time dealing with false positives, which required expensive resources to resolve.

With Cybereason, the composite organization greatly improves its efficiency in detecting and remediating threats. With an easy-to-use UI, the organization can rapidly see a threat, investigate its root cause, and understand the full context of the threat, how it automatically correlates across threats, how the threat effects the entire endpoint environment across platforms, and how to best remediate the situation. Cybereason reduces the number of false positives the organization sees compared its previous endpoint security platform, reducing the noise and ensuring the team is not wasting time on unnecessary tasks. With Cybereason's console, the composite organization can now assess, prioritize, and respond to threats faster than before.

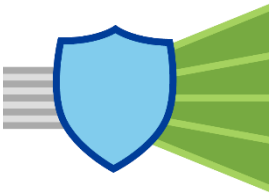
For the composite organization, Forrester assumes that:

- The organization sees an average of three attacks per day.
- Previously, the composite organization's SecOps team spent an average of 15 hours on detection and response to a threat.
- With Cybereason, the SecOps team can react to threats in a fraction of the time: In Year 1, it reduces the time to 5 hours, and by Year 3, as the team has become more proficient utilizing the solution, this reduces to 1 hour.

The improved efficiency in detection and response to threats will vary with:

- The number of threats per day, as well as their severity.
- The time an organization took in its previous solution to detect and respond to threats.
- How an organization leverages Cybereason to reduce the risk associated with cyberthreats.
- The fully loaded compensation of the SecOps team.

To account for these risks and take a conservative approach to understanding the value of this benefit, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $184,911.



93%
Reduction in time to detect and remediate threats by Year 3

Improved Efficiency In Detection And Response To Threats: Calculation Table					
REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
B1	Frequency of attack	Three a day	1,095	1,095	1,095
B2	Time-to-detect and -remediate before Cybereason (hours)		15	15	15
B3	Time-to-detect and -remediate after Cybereason (hours)	Interviews	5	3	1
B4	Reduced time-to-detect and -remediate	B2-B3	10	12	14
B5	Average hourly rate for SecOps required		$74.64	$74.64	$74.64
Bt	Improved efficiency in detection and response to threats	(B1+B4)*B5	$82,477	$82,626	$82,775
	Risk adjustment	↓10%			
Btr	Improved efficiency in detection and response to threats (risk-adjusted)		$74,229	$74,363	$74,498

Increased Security Platform Management Efficiency

Prior to the implementation of Cybereason, the composite organization used many different security solutions on disparate platforms. IT and SecOps teams had to try to piece together multiple security solutions to protect the organization. However, they found that not only did this method not provide visibility and context into threats, but it was also difficult to manage. With Cybereason, the organization has deployed a single lightweight agent that is managed from one console, drastically minimizing the management required.

To calculate this benefit, Forrester assumes that:

- The composite organization previously had one FTE managing its security platforms for 50% of their job.
- With Cybereason, this is reduced by 75%.

The value of this benefit can vary due to a variety of factors, including:

The time spent managing the previous security environment.

- How efficiently the organization manages Cybereason.
- The salary of security platform management.

To account for these risks and continue a conservative approach, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $130,304.

75%
Reduction in management required

Increased Security Platform Management Efficiency: Calculation Table					
REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
C1	Person-hours spent on security management	50% of 1 FTE''s time	1,040	1,040	1,040
C2	Reduction in management required with implementation of Cybereason		75%	75%	75%
C3	Total management hours saved as a result of implementing Cybereason	C1*C2	780	780	780
C4	Hourly salary	B5	$74.64	$74.64	$74.64
Ct	Increased security platform management efficiency	C3*C4	$58,219	$58,219	$58,219
	Risk adjustment	↓10%			
Ctr	Increased security platform management efficiency (risk-adjusted)		$52,397	$52,397	$52,397

Avoided Future L3 SecOps Hires

All IT and security teams within organizations face a complex challenge: finding the right skills to ensure their organizations are protected against threats. One benefit that organizations found particularly useful from Cybereason compared to alternative solutions: The easy-to-use platform enabled security analysts of all levels of expertise to efficiently and effectively mitigate cybersecurity threats.

The intuitive UI made it easy to empower all analysts at the composite to understand the full context and scope of an attack and how to best remediate the issue, ensuring that expensive, difficult-to-find L3 SecOps FTEs were reserved for the most important tasks. With Cybereason, the composite organization can look at and recalibrate its future hiring needs.

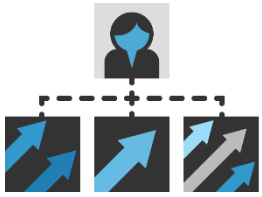
For the composite organization, Forrester assumes that:

- The SecOps team begins using the Cybereason Platform in Year 1.
- Without Cybereason, the composite organization would require at least one L3 analyst FTE in Year 2 and another 1.5 FTEs in Year 3 to manage endpoint security within the organization.
- With the investment in Cybereason, the composite organization avoids the need for these additional L3 analyst headcounts, starting in Year 2.

The cost avoidance associated with this benefit will vary with:

- The size of the organization and how many L3 analysts the organization believes it would require to manage endpoint security within the organization.
- The fully loaded salary of L3 analysts.

To account for these risks and maintain the conservative approach to understanding the benefit, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $288,105.



Avoids 1.5 new hires
by Year 3

Avoided Future L3 SecOps Hires: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
D1	Avoided L3 hires due to improved efficiency/ease of use with Cybereason			1.0	1.5
D2	Annual fully loaded salary			$155,250	$155,250
Dt	Avoided future L3 SecOps hires	D1*D2	$0	$155,250	$232,875
	Risk adjustment	↓5%			
Dtr	Avoided future L3 SecOps hires (risk-adjusted)		$0	$147,488	$221,231

Unquantified Benefits

In addition to the benefits outline above, the interviewed organizations shared other benefits that were not included as part of this financial model. Specifically, the companies saw the following unquantified benefits:

- **Support ticket savings.** Organizations described how the increased visibility of Cybereason benefits technical support; with SecOps relying less on the help desk to identify and solve issues, the help desk can focus on other tasks. In addition, for those issues still requiring help desk support, Cybereason shortens the amount of time required to find information and hastens the resolution of security issues, decreasing the mean-time-to-respond.

  One of the interviewees was impressed with how well Cybereason supported the relationship between SecOps and the help desk: "When help desk tickets come in, you can automatically go back into Cybereason and do the investigation, and then it automatically tracks the incident throughout its entire lifecycle. The incident stays with us, so we only send the task to the correct person, and then we can say whether the incident has been remediated or not." Organizations found that Cybereason reduces the number of support ticket requests that come in and the time to resolve the issue.
- **Improved compliance and auditing.** Regular and surprise audits require visibility into the network and the ability to rapidly pull up and present information. Organizations dealing with HIPAA, HITECH, GDPR, and other regulations found the added visibility of Cybereason helpful to meet compliance and audit requirements in a timely fashion. One interviewee noted: "By implementing Cybereason, it provided us the rest of the coverage that we need to fall into compliance. . . . So it kind of got us the rest of the way to ensure compliance and regulations are being met." Cybereason reduced the time that would have been spent on compiling details for audits compared to previous environments.

Unquantified Benefits:

- Support ticket savings
- Improved compliance and auditing

Flexibility

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

- **Adding on additional Cybereason services**. In addition to its platform, Cybereason offers a wide array of services, ranging from security assessments to managed detection and response to aiding directly in the event of a breach. These services can dramatically expand an organization's security awareness and capability without requiring corresponding hires. With Cybereason services, an organization can utilize Cybereason as an extension of its SecOps program to better protect, detect, contain, and respond to security incidents. Cybereason services help to augment and improve an organization's risk posture.

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

- **Expansion to more endpoints**. As organizations continue to grow, companies can continue to expand the use of Cybereason to protect new endpoints across the organization, further improving security and enabling safer growth. Cybereason enables organizations to scale easily as they grow and are looking for both EDR and NGAV capabilities.

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

Analysis Of Costs

QUANTIFIED COST DATA AS APPLIED TO THE COMPOSITE ORGANIZATION

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	Licensing, implementation, management, and training	$116,903	$355,734	$380,304	$361,593	$1,214,535	$1,026,269
	Total costs (risk-adjusted)	$116,903	$355,734	$380,304	$361,593	$1,214,535	$1,026,269

Licensing, Implementation, Management, And Training Costs

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than $1.0 million.

This cost analysis looks at both the external and internal costs incurred to leverage the Cybereason platform. The model first considers the external costs paid directly to Cybereason for use of the platform. Costs for licensing vary based on number of endpoints in any given year. Next, the model considers internal costs associated with implementation, ongoing management, and training on the platform. Based on feedback from the interviewed organizations, the composite organization's implementation takes groups of employees several months working part-time. Maintaining and managing the platform requires relatively little effort. Finally, the composite organization spends time training its Cybereason users as a best practice to ensure they understand how to get the most out of the platform.

For the composite organization, Forrester assumes:

- Based on feedback from interviewed organizations, Forrester assumes it takes about 690 resource-hours for implementation, with a fully loaded hourly rate of $64 for IT staff. This equates to one full-time resource working for a bit over four months, but many organizations have more than one resource working on implementation.
- As a best practice, 75 employees are trained on Cybereason, with 12 hours of initial training to prepare them to use the platform and 16 hours of additional training each year to ensure they understand new features and continue to learn new aspects of the platform.
- For ongoing maintenance and management, the composite organization spends 204 resource-hours each year to keep Cybereason up and running.

These costs can vary with:

- The size of the deployment, which will affect licensing costs and may require more implementation and support hours.
- The average hourly salary of IT and SecOps personnel.

To account for these risks and look at the costs conservatively, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $1,026,269.

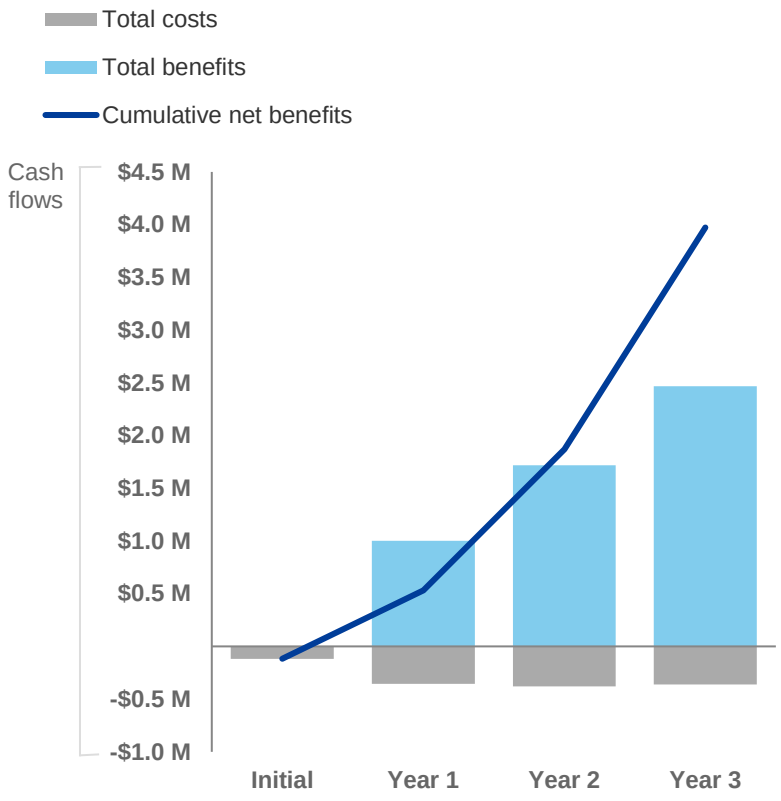
Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Licensing, Implementation, Management, And Training: Calculation Table						
REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Licensing costs			$234,000	$257,400	$239,580
E2	Implementation	Resource-hours	690			
E3	Fully loaded hourly rate of IT		$64			
E4	Implementation costs	E2*E3	$44,160			
E5	Number of employees trained on Cybereason		75	75	75	75
E6	Hours trained annually		12	16	16	16
E7	Ongoing management	Resource-hours		204	204	204
E8	Hourly rate of SecOps		$74.64	$74.64	$74.64	$74.64
E9	Total training and ongoing management costs	((E5*E6)+E7)*E8	$67,176	$104,795	$104,795	$104,795
Et	Licensing, implementation, management, and training	E1+E4+E9	$111,336	$338,795	$362,195	$344,375
	Risk adjustment	↑5%				
Etr	Licensing, implementation, management, and training (risk-adjusted)		$116,903	$355,734	$380,304	$361,593

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	($116,903)	($355,734)	($380,304)	($361,593)	($1,214,535)	($1,026,269)
Total benefits	$0	$1,001,427	$1,717,669	$2,465,143	$5,184,238	$4,182,047
Net benefits	($116,903)	$645,692	$1,337,364	$2,103,549	$3,969,703	$3,155,778
ROI						308%

FORRESTER®

Cybereason Defense Platform: Overview

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

A COMPLETE ENDPOINT SECURITY SOLUTION

The Cybereason Defense Platform delivers a complete and integrated endpoint security solution via a single agent. It combines prevention with endpoint detection and response (EDR), along with threat hunting across all endpoints and devices. It's ideal for enterprises that are looking to stop all types of cyberattacks before they can do damage while reducing their security risk.

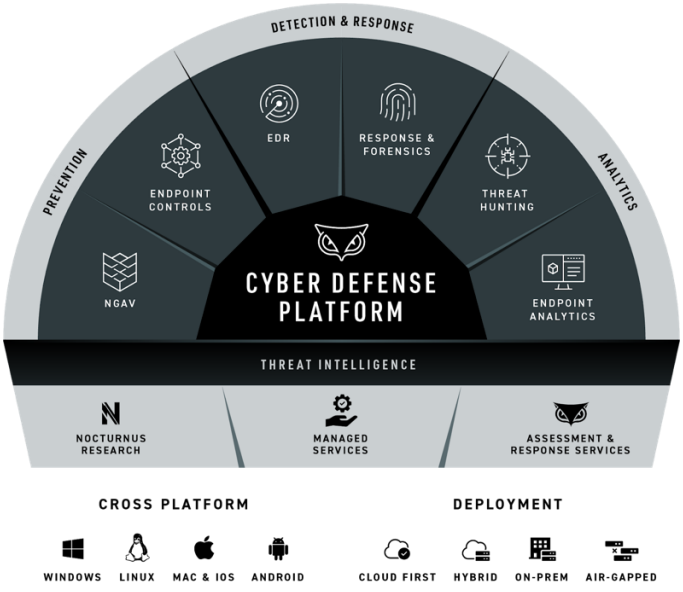
THE VISIBILITY TO EMPOWER YOUR SECURITY TEAM

Cybereason empowers analysts of any skill levels to rapidly investigate incidents and easily respond to alerts. Your security team can view the entire attack lifecycle within a single screen; view a complete timeline of events for all malicious activity, across every impacted device and every process, all within a single platform without having to switch back and forth between different screens or systems. Investigations are visual based and easy to use allowing you to "up-level" your security analysts.

The Cybereason Defense Platform gives your analysts a clear understanding of even the most complex attacks, at a glance, so they can take action quickly. This reduces the time required to triage and accelerates prioritization and remediation. Upon receiving an alert, your analysts can assess and quickly kill processes, quarantine files, remove persistence mechanisms, prevent file execution, and isolate machines.

SAVE PRECIOUS TIME, FOCUS ON WHAT IS MOST IMPORTANT

Cybereason automates threat detection and remediation to save your analysts time and effort. Automatically uncover attacks and hunt for malicious activities and TTPs used by attackers in real-world campaigns without spending weeks to configure and tune rules. Your security team can get a complete story automatically and see all related attack elements, including the root cause, all affected machines and users, incoming and outgoing communications, and a timeline of an attack. Your team will have full context of an incident without the "noise" of false positives so they can instantly understand an attack and focus on what matters most.



FORRESTER®

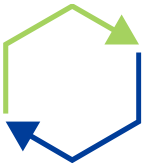
Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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



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

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

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

Present value (PV)

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

Net present value (NPV)

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

Return on investment (ROI)

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

Discount rate

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

Payback period

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