FORRESTER®

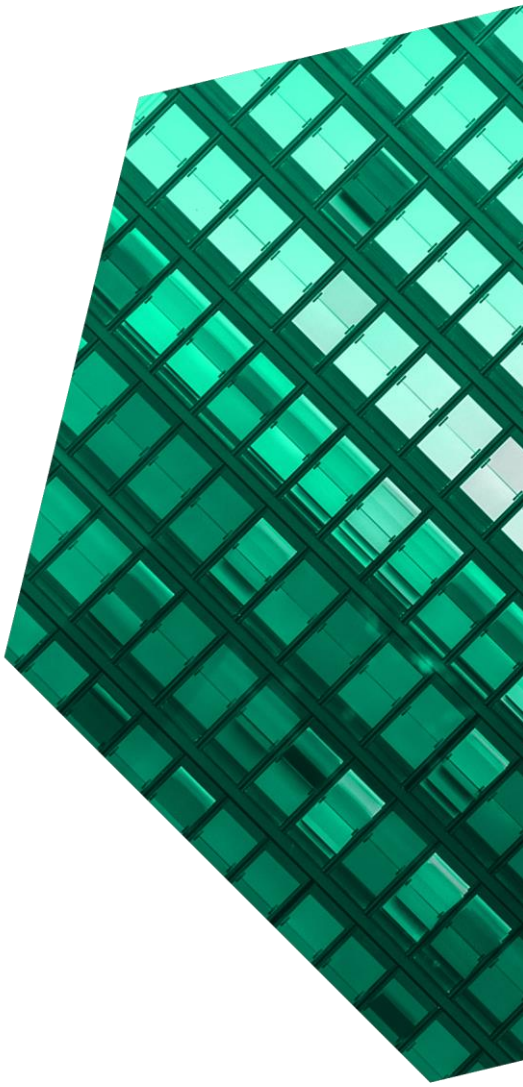
The Total Economic Impact™ Of Rapid7 Threat Command For Digital Risk Protection And Threat Intelligence

Cost Savings And Business Benefits Enabled By Threat Command

January 2023

Table Of Contents

Consulting Team: Rishabh Dua
Tony Lam
Claudia Heaney



ABOUT FORRESTER CONSULTING

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

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

Executive Summary

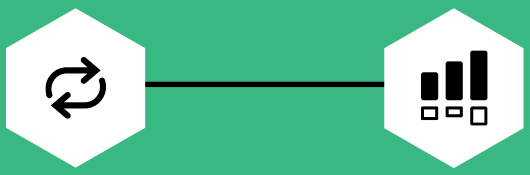
With an increasingly complex threat landscape, security teams require technology solutions and internal processes to manage threat intelligence and effectively protect their security environments. Rapid7 Threat Command is an external threat intelligence solution that helps security teams gain process efficiencies across the entire threat lifecycle, from detection and investigation to remediation. With Rapid7's underlying technology platform and security expertise, Threat Command enhances an organization's security posture.

With the increasing volume of cyberthreats, increasing complexity of digital environments, and expanding attack surfaces for organizations, companies need to enhance their cyberdefenses.[1] In fact, according to Forrester research, 63% of organizations globally were breached in 2021, and security decision-makers were more concerned about external attacks than any other attack vector. [2]

These cyberthreats and compromised data, such as information on end users floating around on the dark web, are pushing organizations to find an external threat intelligence solution that can provide precise visibility into the threats most relevant to their organization and industry and assist in them in staying one step ahead of potential issues. Security teams struggle with the necessary resources, systems, headcount, internal processes for detection and remediation, and data visibility across their security landscape to effectively manage external threats. With external threat intelligence solutions, security teams gain greater visibility into threat intelligence data and swifter, automated remediation that substantially lower the risk organizations face from cyberattacks.

Threat Command is a threat intelligence and digital risk protection solution that reduces an organization's risk exposure from external threats. Threat Command pairs AI and machine learning detections with human intelligence to prioritize alerts relevant for immediate action. Threat Command acts as an extension of an organization's security team, providing expertise on demand and full-service remediation to quickly remove threats impacting it.

KEY STATISTICS



Return on investment (ROI)
311%

Net present value (NPV)
$1.42M

Rapid7 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Threat Command.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Threat Command on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Threat Command. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single global composite organization with 7,500 employees and revenue of $5.7 billion per year.

Prior to using Threat Command, interviewees noted their legacy external threat intelligence solutions were unable to provide them with data relevant to their organization and lacked visibility across all assets. Security team members dealt with information overload and inadequate resources to handle the workload. The security team members manually gathered information across a variety of sources with time-consuming investigations across digital locations such as the dark web. Moreover, the remediation process for actionable alerts was slow and inefficient.

After the investment in Threat Command, interviewees had an efficient solution that monitored and defended against external threats. It provided organizationally relevant data displayed in a single location, saved security analysts' valuable time, and created more efficient processes from investigation to remediation. This strengthened the organizations' security posture for detecting and responding to cyberthreats.

Reduction in time for investigation, threat hunting, and analysis with Threat Command

75%

KEY FINDINGS

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

- **Security-team productivity gains from automation of $496,700 over three years.** Prior to implementing Threat Command, the composite organization has an inefficient process for investigation, threat hunting, analysis, and report creation. By leveraging Threat Command, the composite organization's security team members gain efficiencies across those activities, allowing them to reprioritize more productive and valuable work.
- **Up to 70% reduction in the likelihood of a major security breach.** By implementing Threat Command, the composite organization gains greater efficiency to detect, investigate, respond to, and remediate cyberattacks. For the composite organization, having Threat Command as a part of its security environment has the effect of lowering the likelihood of successful breaches by up to 70% over the course of three years and decreasing the impact of cyberattacks. This results in up to $1.1 million (PV) in savings over three years.
- **Remediation efficiency for the security team.** By implementing Threat Command, the composite organization gains a faster remediation process for actionable alerts due to the automation and access to Rapid7's internal intelligence team. The composite organization avoids the cost of adding one additional security analyst. This results in $302,200 (PV) in savings over three years.

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

- **Proactive processes for external threat intelligence and remediations.** The composite organization gains more efficient security processes from contextualized and relevant alerts on potential threats and the ability to take down malicious accounts and domains before they become larger problems. Implementing Threat Command helps the composite organization become more proactive in dealing with new adverse activity that previously would have gone undetected.

- **Reduction in number of false positive alerts.** By implementing Threat Command, the composite organization realizes a decrease in the number of false positives since the system provides customized, contextualized, and relevant alerts.

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

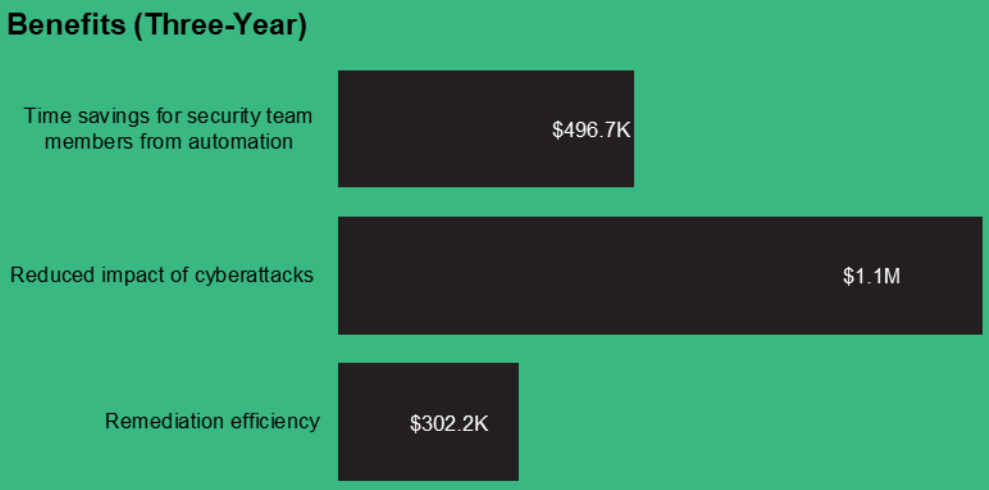
- **Threat Command subscription and remediations fees.** Rapid7 charges the composite organization an annual subscription based on number of assets covered and a supplementary charge for additional remediations, adding up to over $410,300 over three years.
- **Implementation and ongoing costs.** Implementation and ongoing tasks add up to $25,700 over three years.

The representative interviews and financial analysis found that a composite organization experiences benefits of $1.88 million over three years versus costs of $457,000, adding up to a net present value (NPV) of $1.42 million and an ROI of 311%.

ROI
311%

BENEFITS PV
$1.88M

NPV
$1.42M



“Everything was a little bit easier, to navigate and search, and the alerts and the reports that we got on a daily basis were much more fruitful.”

— CIO, airlines

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 Threat Command.

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 Threat Command can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Rapid7 and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Threat Command.

Rapid7 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.

Rapid7 provided the customer names for the interviews but did not participate in the interviews.

The Rapid7 Threat Command Customer Journey

Drivers leading to the Threat Command investment

Interviews

Role	Industry	Region	Revenue	Security Team Size	Named Assets
Principal threat intelligence analyst	Financial services	North America	$18.9 billion	6 team members	7,500
Cyber security and incident response lead	Materials	North America	$1.6 billion	4 team members	500
CISO	Legal	North America	$1.5 billion	5 team members	200
CIO	Airlines	North America	$700 million	8 team members	500

KEY CHALLENGES

Prior to implementing Threat Command, interviewees' organizations worked with limited technology solutions such as open source tools or antivirus software for threat intelligence and were inundated with data. The remediation processes were inefficient. The interviewees noted how their organizations struggled with common challenges, including:

- **Lack of visibility and unactionable data gathered across legacy solutions.** Interviewees noted that there was an immense amount of data to examine with their previous solutions and systems. This resulted in limited visibility into the potential security threats to both interviewees' organizations and their customers. The data the legacy solutions provided was confusing to navigate. There was no singular accounting of assets or solution to provide curated customizable information.
- **Manual and time-consuming process for investigation and analysis.** Interviewees stated that security team members using legacy threat intelligence solutions had to spend hours manually searching through different platforms such as a web-based Git repository or the dark web to investigate all potential threat alerts, and many were irrelevant. This time-consuming process led to additional work, which could have been more efficiently spent on higher-priority security tasks.

> **"We were having a lot of trouble distinguishing relevant threats from noise. It was a manual approach of pulling the information from these sources … It was very reactive."**
>
> *Principal threat intelligence analyst, financial services*

- **Reactive approach to potential cyber incidents.** Interviewees noted that their legacy systems and internal processes led to a reactive approach for their threat intelligence investigations and security responses. Security team members would get alerts from systems or other teams with limited context, which led to

inefficient triage of larger issues. As a result, the teams sacrificed quality for speed.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Provide greater data visibility through a single pane of glass.
- Consolidate information and create a centralized asset list.
- Provide customizable alerts with greater context around the threat intelligence.
- Improve search capabilities across platforms and locations such as the dark web, application marketplaces, and social media.
- Modernize security systems and processes.

"We needed something that gave us the capability to aggregate everything into ... one central platform and bring all of our threat intelligence and curating processes together in a way that it was usable. The solution also had to have the capability of being able to talk to all of our other security technology that could absorb threat intelligence."

CISO, legal

Reduced likelihood of a cyberattack after deploying Threat Command

Up to 70%

COMPOSITE ORGANIZATION

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

Description of composite. The composite organization is a $5.7 billion global enterprise, with 7,500 employees headquartered in North America. The organization has open source tools, antivirus software, and vendor sources for finished intelligence. The security team is comprised of five team members working solely on threat intelligence. The organization has 1000 named assets and monitors a variety of keywords including domains, login pages, brand and company names, social media pages, VIP emails, IP addresses, workstations, and servers. The organization is looking to modernize its threat intelligence and security systems, gain greater data visibility, and create more efficient processes across all stages from threat investigation to remediation. Use cases with Threat Command include, but are not limited to attack mapping, digital risk, brand and fraud protection, vulnerability protection, data and

credential leakage, attack surface monitoring, and phishing protection.

Key Assumptions

- **$5.7 billion in annual revenue**
- **7,500 employees**
- **Five threat intelligence team members**
- **1000 named assets**

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	Time savings for security team members from automation	$199,719	$199,719	$199,719	$599,157	$496,672
Btr	Reduced impact of cyberattacks	$366,714	$440,057	$513,399	$1,320,170	$1,082,784
Ctr	Remediation efficiency	$121,500	$121,500	$121,500	$364,500	$302,153
	Total benefits (risk-adjusted)	$687,933	$761,276	$834,618	$2,283,827	$1,881,609

TIME SAVINGS FOR SECURITY TEAM MEMBERS FROM AUTOMATION

Evidence and data. Before implementing Threat Command, interviewees noted that security team members would spend hours searching online on the dark web and investigating potential threats such leaked credit card numbers, credentials, or accounts. For security analysts, this was a time-consuming and extremely manual process, and it limited the time for higher-priority security tasks. With Threat Command, analysts could offload a significant proportion of time devoted to investigation of threats in locations like a web-based Git repository and the dark web. Threat Command scoured through the dark web and other sources for information relevant to interviewees' customers and provided the information in a consolidated platform. Organizations could use Threat Command's intuitive console and user interface to set up automated blocking rules to take immediate action on threats to their environment.

Teams would spend hours creating reports by sifting through various systems to pull data points. With Threat Command, the teams could more easily handle a threat when one was identified, which enabled the team to greatly reduce the amount of time that analysts spent searching the dark web for fraudulent accounts or leaked credentials. Additionally, with greater data visibility, the time to create reports decreased substantially. The improvements with data context and visibility freed up analysts at the interviewees' organizations so they could conduct higher-priority work within the security environment.

- The CIO of an airlines firm estimated the time to research threats for the two team members working on threat investigation decreased by 50%. Additionally, they estimated the time to create quarterly reports decreased from a few hours to 30 minutes. He said: "It's all in one location…making it all a little bit more efficient than me hunting for a couple of hours, looking for that information. Whereas now, it's simply going to a dashboard and I have all the information that I need."
- The principal threat intelligence analyst for a financial services firm estimated that three analysts on the security team saved three to four hours a day running searches across online locations such as a web-based Git repository after implementing Threat Command.
- The cyber security and incident response lead at a materials firm estimated a 50% efficiency gain

for security analysts that researched and created reports more efficiently after implementing Threat Command. They said: “We used to get reports on a daily basis on the number of alerts that had come in. I don’t think we had visibility to that previously. It was a manual process and it would probably take a couple of hours weekly for analysts to go through the reports. Now it’s automated and everything is fast.”

- The CISO for a legal firm said prior to Threat Command, analysts could spend up to three hours investigating potential threats. With Threat Command, they estimated the time to investigate decreased to 30 minutes. They added that the team averaged 10 reports a month and each report could take nearly half a day to complete. With Threat Command, they estimated each report now takes less than 30 minutes to complete.

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

- The intelligence team uses five members.
- A 75% reduction in time for investigation, threat hunting, and analysis attributable to Threat Command.
- The team completes 84 reports annually.
- An 87.5% reduction in time spent on report creation attributable to Threat Command.

Risks. The magnitude of this benefit may vary based on:

- The number of security operations professionals, which may vary by organization size.
- Security analysts’ salaries, which may vary by geographic region.
- Number of reports created annually.
- The increase in efficiency and speed, which may vary based on the overall security posture of the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $496,700.

“I do think Threat Command is a force multiplier for my team at the end of the day because you have one platform to go to.”

CISO, legal

Time Savings For Security Team Members From Automation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of security team members	Composite	5	5	5
A2	Percent of team members working on investigation, threat hunting, and analysis	Composite	80%	80%	80%
A3	Time spent for investigation, threat hunting and analysis prior to Threat Command (hours)	Interview	1,040	1,040	1,040
A4	Reduction in time for investigation, threat hunting, and analysis attributable to Threat Command	Interview	75%	75%	75%
A5	Subtotal: Time savings for investigation, threat hunting, and analysis	A1*A2*A3*A4	3120	3120	3120
A6	Number of reports	Interview	84	84	84
A7	Percent of team members working on reports	Composite	20%	20%	20%
A8	Time spent per report prior to Threat Command	Interview	4	4	4
A9	Reduction in time for reporting attributable to Threat Command	Interview	87.5%	87.5%	87.5%
A10	Subtotal: Time savings for reporting	A6*A7*A1*A8*A9	294	294	294
A11	Hourly fully loaded salary per security team member	TEI standard	$65	$65	$65
At	Time savings for security team members from automation	(A5+A10)*A11	$221,910	$221,910	$221,910
	Risk adjustment	↓10%			
Atr	Time savings for security team members from automation (risk-adjusted)		$199,719	$199,719	$199,719
	Three-year total: $599,157			**Three-year present value: $496,672**	

REDUCED IMPACT OF CYBERATTACKS

Evidence and data. The interviewees' organizations needed to defend themselves and their customers against increased volume of threats, expanded attack surfaces, and expanded locations for attacker tools and exploit code. Limited analyst capacity, disparate data sets across security solutions, and a lack of search accuracy left these organizations vulnerable and more reactive to cyberattacks. With Threat Command, interviewees noted improved security posture for their organizations. Threat Command provided representatives' organizations a more comprehensive security solution with an intuitive user interface to proactively identify and remediate threats before they turned into larger problems. Threat Command provided improved coverage with customizable alerts and dynamic, accurate searches for queries. The user interface presented information in a dashboard that prioritized alerts and lowered the signal-to-noise ratio. This was further enhanced by the ability for organizations to query Rapid7's threat team for more in-depth information on particular alerts/threats with a click of a button within the console. Faster remediation through automated

processes provided a more active response that helped cover more of a security environment. Interviewees' organizations could identify potential threats and investigate and remediate potential threats within the Threat Command console, all of which lowered the impact of cyberattacks.

"We're able to see the vulnerabilities and threats that are coming in with Threat Command, so we can block within our firewall and use email security tools. One less malicious link is one less ability for someone to breach the system."

CIO, airlines

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

- An average of 2.5 cyberattacks per year.[4]
- The average cost per security breach is $654,846.
- There's a 56% degree of coverage from total loss vectors, which includes internal incidents and external cyberattacks.
- With an improving security posture, the reduced likelihood of cyberattacks may decrease by 50% in Year 1 to 70% in Year 3.

Risks. The magnitude of this benefit may vary based on:

- The baseline security posture of the organization.
- The strength and number of cyberattacks and type of exposure.
- The organization's industry and size, because these factors relate to the likelihood of a cyberattack and the potential for losses.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.1 million.

Reduced Impact Of Cyberattacks

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Average number of cyberattacks per year	Forrester research	2.5	2.5	2.5
B2	Reduced likelihood of a cyberattack after deploying Threat Command	Interview	50%	60%	70%
B3	Average cost of a cyberattack	Forrester research	$654,846	$654,846	$654,846
B4	Degree of coverage due to Threat Command from total loss vectors	Forrester research	56%	56%	56%
Bt	Reduced impact of cyberattacks	B1*B2*B3*B4	$458,392	$550,071	$641,749
	Risk adjustment	↓20%			
Btr	Reduced impact of cyberattacks (risk-adjusted)		$366,714	$440,057	$513,399
	Three-year total: $1,320,170			**Three-year present value: $1,082,784**	

REMEDIATION EFFICIENCY

Evidence and data. Interviewees stated that prior to Threat Command, their organizations lacked the required headcount to properly investigate alerts and potential threats. With Threat Command implemented, interviewees' organizations did not need to hire additional headcount. With more comprehensive detection using the underlying technology, analytics platform, and access to Rapid7's internal SOC and remediation teams, interviewee's organizations gained a more efficient process within their security environment. Interviewees found they did not need to hire additional staff having implemented Threat Command.

- The CISO for a legal firm said, "Threat Command definitely cut down on a lot of hours of work for my team in a week. A headcount."
- The CIO for an airline firm estimated the organization did not need to hire an additional security analyst after implementing Threat Command as a part of its security environment.

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

- By implementing Threat Command, the composite organization avoids hiring one security analyst.
- A security analyst's annual fully loaded salary is $135,000.

Risks. The magnitude of this benefit may vary based on:

- The size of the organization.
- The level of security coverage required.
- Security analysts' salaries, which may vary by geographic region.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $302,200.

> **"Before Threat Command, if I needed to do a domain takedown, I had to dig up where it was registered. Taking down a fake social network profile or domain is painful, and it can take months of communication. Now I upload it, hit the remediation button, and Threat Command does the hard work in the background."**
>
> *CISO, legal*

Remediation Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Avoided headcount	Interview	1	1	1
C2	Average annual fully loaded salary for security analyst	TEI standard	$135,000	$135,000	$135,000
Ct	Remediation efficiency	C1*C2	$135,000	$135,000	$135,000
	Risk adjustment	↓10%			
Ctr	Remediation efficiency (risk-adjusted)		$121,500	$121,500	$121,500
	Three-year total: $364,500			**Three-year present value: $302,153**	

UNQUANTIFIED BENEFITS

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

- **Proactive approach to potential threats.** Interviewees described more efficient security processes. They fine-tuned searches for themselves and their customers, gained personalized alerts on potential threats, took down accounts and domains off the dark web before they became larger problems, and had a greater accounting of all their digital assets. With these new processes, interviewees noted they moved from a reactive to a proactive approach with threat intelligence and threat remediations. One interviewee even reported learning of threats to the organization's customer before being informed by the customer.
    - The principal threat intelligence analyst for a financial services firm said: "Threat Command helped us become more proactive in a way that we otherwise couldn't. By the time somebody is asking you the question, it's too late to do all the work to fix a problem."
    - The CIO of an airline firm said: "We're more proactive now based upon some of the information we see within Threat Command. So there have been several instances where we received information from Threat Command before our customer even notified us."
- **Decrease in false positives.** Interviewees noted there was a decrease in the number of false positives after implementing Threat Command. Since the systems filters out information and only provides relevant and customized alerts, teams were able to focus on alerts that required further investigation rather than chase down potential alerts that led nowhere.

FLEXIBILITY

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

- **Continued threat protection.** Interviewees expressed continued confidence in Threat Command's ability to identify and help protect their organizations against future threats utilizing the most up-to-date threat intelligence. This may result in improved business continuity and risk avoidance.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Subscription costs	$0	$165,000	$165,000	$165,000	$495,000	$410,331
Etr	Implementation effort	$25,740	$0	$0	$0	$25,740	$25,740
Ftr	Maintenance effort	$0	$8,580	$8,580	$8,580	$25,740	$21,337
	Total costs (risk-adjusted)	$25,740	$173,580	$173,580	$173,580	$546,480	$457,408

SUBSCRIPTION COSTS

Evidence and data. Interviewees said they paid for an annual subscription fee for Threat Command and for a set of additional remediations. The subscription fees were based on the number of named assets and the remediations pricing was based on number of additional remediations purchased.

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

- Subscription fee of $140,000 is for 1,000 named assets.
- Additional remediations for use anytime is $10,000.

Risks. The pricing will vary based on:

- The number of assets being covered.
- The number of additional remediations purchased.
- Any discounts negotiated with or offered by Rapid7.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $410,300.

Subscription Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Subscription cost	Composite		$140,000	$140,000	$140,000
D2	Additional remediation request costs	Composite		$10,000	$10,000	$10,000
Dt	Subscription costs	D1+D2	$0	$150,000	$150,000	$150,000
	Risk adjustment	↑10%				
Dtr	Subscription costs (risk-adjusted)		$0	$165,000	$165,000	$165,000
	Three-year total: $495,000			**Three-year present value: $410,331**		

IMPLEMENTATION EFFORT

Evidence and data. Interviewees described a straightforward implementation process for Threat Command. Team members worked to integrate and connect Threat Command into their security environment from servers to firewalls. They also uploaded lists of named assets such as domains and accounts.

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

- The involvement of three security team members.
- Implementation takes 120 hours to complete.
- A security team member's hourly fully loaded salary is $65.

Risks. The costs may vary due to:

- The systems and named assets that need to be connected and uploaded to Threat Command.
- Time required to complete implementation.
- The number of security team members dedicated to the implementation of Threat Command, which may vary by organization size.
- Security team member's salaries, which may vary by geographic region.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $25,700.

Implementation Effort

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Number of security team members	Composite	3			
E2	Time for implementation of Threat Command (hours)	Interview	120			
E3	Hourly fully loaded salary	TEI standard	$65			
Et	Implementation effort	E1*E2*E3	$23,400	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Implementation effort (risk-adjusted)		$25,740	$0	$0	$0
	Three-year total: $25,740			**Three-year present value: $25,740**		

MAINTENANCE EFFORT

Evidence and data. Interviewees described minimal efforts to maintain the system. This included tasks such as updating the asset lists and connecting new security technologies to Threat Command.

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

- The involvement of two security team members.
- Maintenance tasks take 5 hours a month to complete.
- A security team member's hourly fully loaded salary is $65.

Risks. The cost may vary based on:

- The number of security team members, which may vary by organization size.
- Time required for maintenance tasks
- Security team member's salaries, which may vary by geographic region.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $21,300

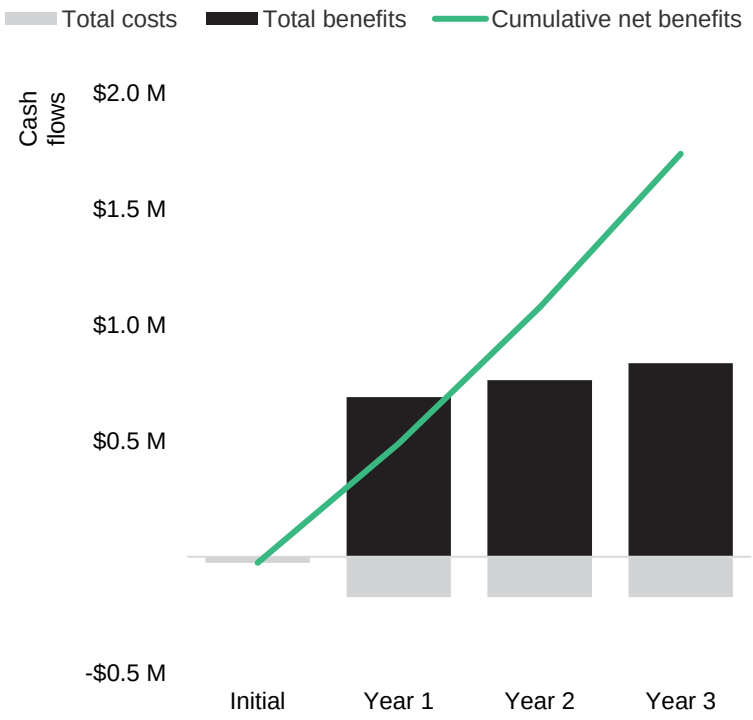
Maintenance Effort

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Number of security team members	Composite		2	2	2
F2	Hours for ongoing work per month	Interview		5	5	5
F3	Hourly fully loaded salary	Forrester standard		$65	$65	$65
Ft	Maintenance effort	F1*F2*F3*12	$0	$7,800	$7,800	$7,800
	Risk adjustment	↑10%				
Ftr	Maintenance effort (risk-adjusted)		$0	$8,580	$8,580	$8,580
	Three-year total: $25,740			**Three-year present value: $21,337**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($25,740)	($173,580)	($173,580)	($173,580)	($546,480)	($457,408)
Total benefits	$0	$687,933	$761,276	$834,618	$2,283,827	$1,881,609
Net benefits	($25,740)	$514,353	$587,696	$661,038	$1,737,347	$1,424,201
ROI						311%

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%.

Appendix B: Endnotes

[1] Source: “The 2021 State Of Enterprise Breaches,” Forrester Research, Inc., April 8, 2022.

[2] Ibid

[3] 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.

[4] Source: “Forrester Consulting Cost Of A Cybersecurity Breach Survey,” Q1 2021.


FORRESTER®