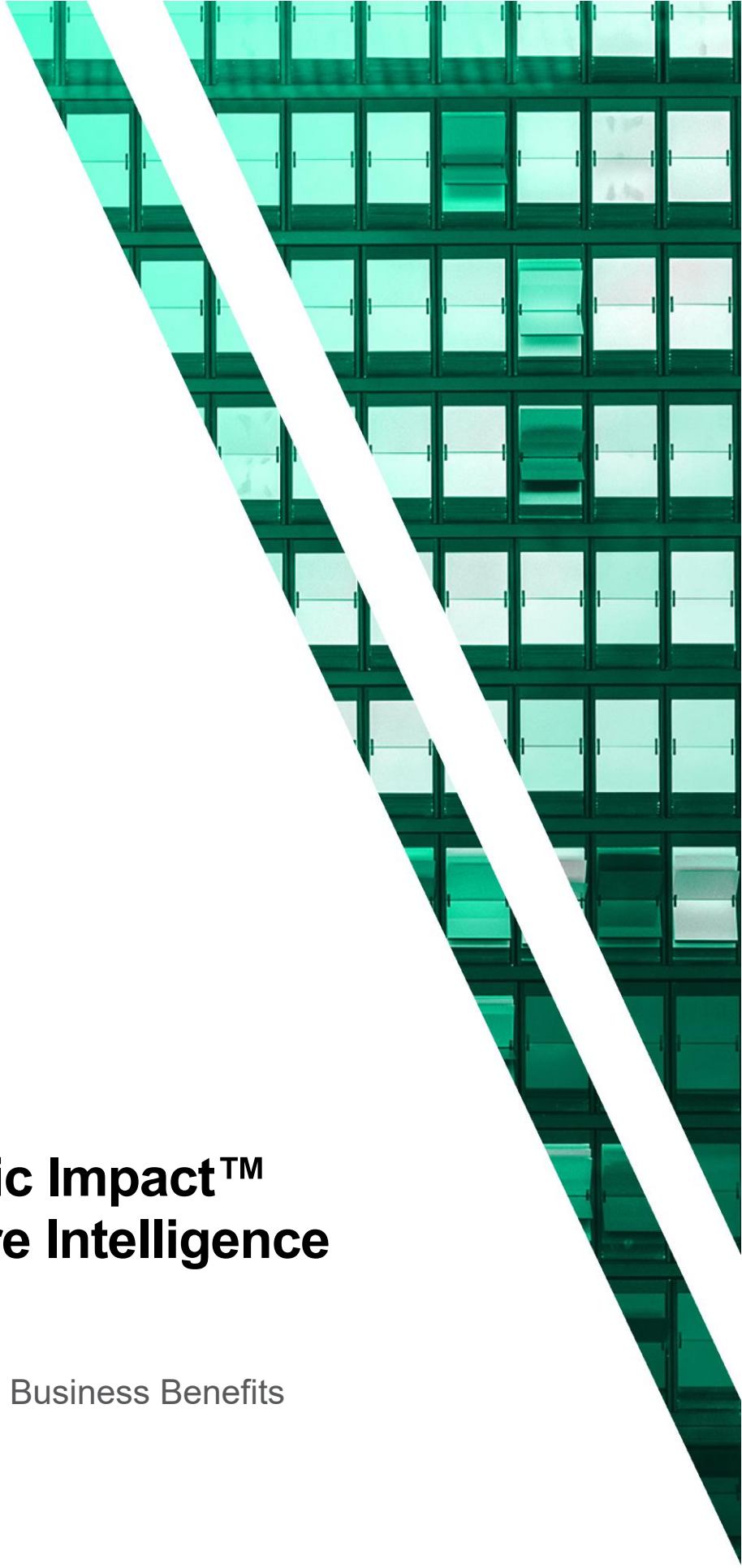
FORRESTER®



The Total Economic Impact™ Of Recorded Future Intelligence Platform

Risk Mitigation, Cost Savings, Business Benefits Enabled By Recorded Future

NOVEMBER 2021

Table Of Contents

Executive Summary 1

The Recorded Future Intelligence Platform Customer Journey 6

Key Challenges 6

Solution Investment Objectives 7

Composite Organization 7

Analysis Of Benefits 8

Security, Risk, And Response Operations Efficiency 8

Breach Loss Avoidance From Early Detection 11

Brand Impact Protection 13

Shift Work To Junior Analysts 14

Unquantified Benefits 16

Flexibility 16

Analysis Of Costs 17

Implementation, Integration, Training, And Ramp Costs 17

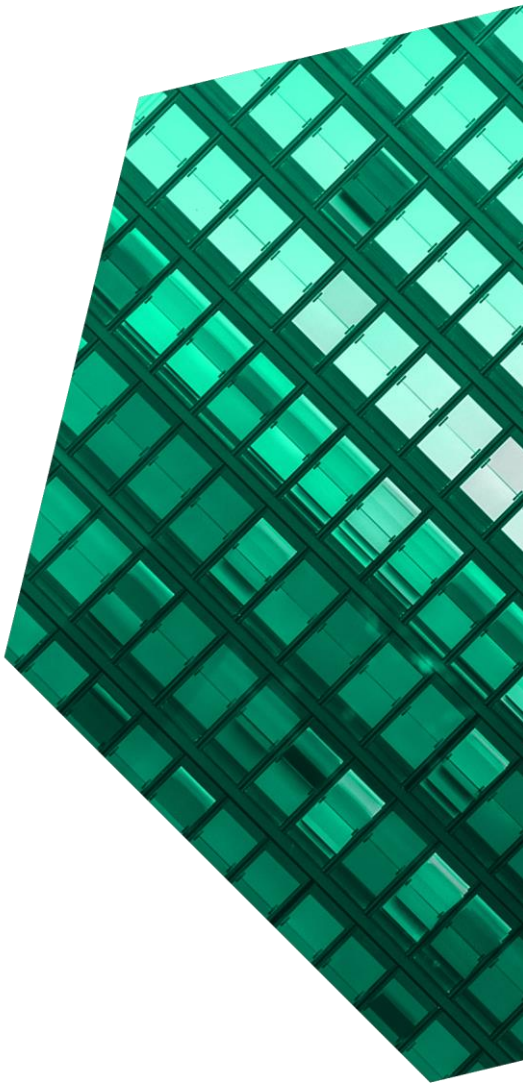
Cost Of Subscriptions 18

Financial Summary 20

Appendix A: Total Economic Impact 21

Appendix B: Endnotes 22

Consulting Team: Henry Huang
Kara Luk



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.

Executive Summary

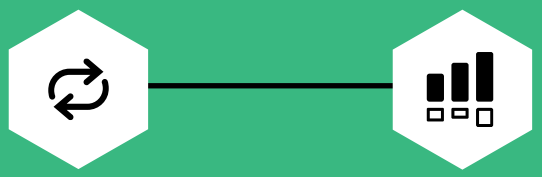
Cyberthreat actors and their attack vectors are growing increasingly complex. Organizations are also growing, adding expansive attack surfaces that create a need for better intelligence and more data to protect themselves. While technology has made it easier for organizations and threats to scale, human capital has not, which makes threat intelligence and outwards visibility more important from cyberintelligence sources like Recorded Future.

The Recorded Future Intelligence Platform provides deep-level cyberthreat visibility and intelligence with actionable insights that enable and empower security operations and incident responders to act more quickly, be more proactive, and remediate cyberthreats faster. Intelligence is sourced from open-source mediums, social forums, technical data sources, and the dark web, and is then structured upon both artificial and human analysis to provide up-to-date contextual information. The result is the ability to decrease both manual and automated investigative efforts. Ultimately, the platform reduces cybersecurity-related risk and protects organizations and their brands from potential harm.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using the Recorded Future Intelligence Platform. For the purposes of this study, Forrester aggregated the interviewees' experiences s and combined the results into a single composite organization.

KEY STATISTICS



Return on investment (ROI)
245%

Net present value (NPV)
$3.74M

Prior to using the Recorded Future Intelligence Platform, the interviewees' organizations relied on manual intelligence collection or point solutions for threat intelligence. Manual aggregation was slow and point solution data was labor intensive to correlate and provide meaningful guidance, leaving organizations with extended processes to piecemeal investigations. The limitations created caused long lead times before indicators of compromise (IOC) were determined, leading to a lack of action and extended remediations or worse — missed remediations.

Following the investment in Recorded Future, the interviewees' organizations acquired deeper intelligence, including information from the far reaches of the dark web and social channels. Interviewees' organizations also integrated Recorded Future to other segments of the security stack like their security information and event management

(SIEM) and security orchestration automation and response (SOAR) systems to improve their ability to thwart threats. Key results from the investment include greater security operations efficiency, greater proactive measures to stay ahead of threats, and better defense of brand value.

Forrester findings on the aggregate of the interviewed organizations are compiled and delivered quantitatively as follows through a composite of the interviewed organizations.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Improved security, risk, and response operations efficiency with security operations (SecOps) reducing investigation effort by 40%.** The comprehensiveness of data collection and data extrapolation were two anchors that fed SecOps and incident responders with the know-how to act on alerts and incidents. The two items were not mutually exclusive, as there was a huge log of event data, which without the analyses and enrichment, was often not useable. In total, the composite organization sees a $2.66 million benefit over three years in efficiency gains.
- **Increased material security breach avoidance due to early detection of nearly $1.46 million over a 3-year span.** Added visibility and early detection of potential threats contributed better securing interviewees' organizations against material breaches. Interviewees revealed that their organizations preemptively detected possible breaches and detected up to 20% more threats, thus reducing the likelihood of a breach by being proactive. Findings are based upon a combination of Forrester internal research and empirical customer feedback.
- **Improved brand impact protection savings of more than $638,000.** Brand erosion costs matriculated in various ways with customer reacquisition and retention costs as main headliners in the field. Forrester Consulting's Cost Of A Security Breach survey from 2020 points to a cost of $950,000 per year on these costs for the composite organization.[2] With the addition of Recorded Future, interviewees noted their organizations avoided some of this cost through early identification of brand misuse. For the composite, the total amount of brand-impact-related cost savings amounts to a PV of $638,000 over three years for brand impact related costs.
- **Deeper level insight and context around intelligence allows for a shift to use more junior SecOps workforce.** Deeper and more contextual insights allowed security operations and incident responders to work faster, eliminating a significant portion of investigative and triage work. Enriched with improved insights, organizations shifted investigation and triage work to more junior-level analysts, which was helpful in the current environment where security analysts come at a premium and are hard to retain. The composite organization recognizes a savings of over $510,000 in three years.

Savings due to advanced work shifted to junior analysts

$510,000

Unquantified benefits and Flexibility elements. Benefits that are not quantified for this study include

- Vulnerability identification comes faster than with traditional vendor releases. Understanding what vulnerabilities threat actors are exploiting allows security professionals to stay ahead and proactively mitigate the risk of a breach. Recorded Future provides both machine

analytics as well as an additive layer of human analytics to ensure that information is delivered fast and accurately.

- Reduction of friendly fraud with early identification in social channels. Friendly fraud consists of up to 60% of losses at retail organizations. Organizations could save millions if they recognize friendly fraud activities, such as abusing coupons before they are used. One interviewee's organization saved nearly $3 million from a single leaked coupon code.

Costs. Risk-adjusted PV costs include:

- **Implementation, integration, and ramp up costs that amount to just over $90,000.** Forrester observed that organizations required a lead time to integrate threat feeds and information so that the Intelligence Platform could be fully integrated with other systems, such as SIEMs. Additionally, interviewees noted a short period of time was needed to acclimate to the Recorded Future platform and execute upon new threat intel.
- **Subscription licensing costs at list levels amount to an average of $577,500 per year.** Threat and intelligence feed pricing is straightforward. Pricing is based on the intelligence modules needed to consume the data. Integration APIs were priced per connection, allowing for organizations to share the data with multiple platforms and the people working on those platforms. Costs in this category also included managed takedowns of potentially harmful material on the web.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $5.27 million over three years versus costs of $1.53 million, adding up to a net present value (NPV) of $3.74 million and an ROI of 245%.

"Recorded Future enriched intelligence to enable automation, provide operational lift, and enable our team to think deeper about threats and how they affect the organization. Recorded Future's augmentation represents at least a few threat intelligence analysts for us."

— Director of cyberintelligence, hospitality

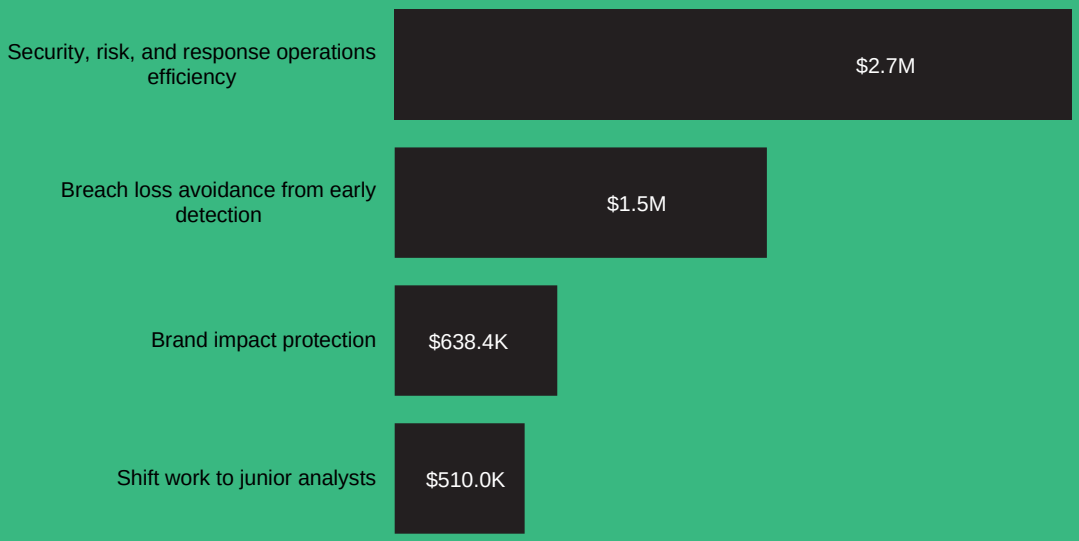
ROI
245%

BENEFITS PV
$5.27M

NPV
$3.74M

PAYBACK
<6 months

Benefits (Three-Year)



Investigation, triage, and response times were each reduced by as much as 40% with the use of Recorded Future.

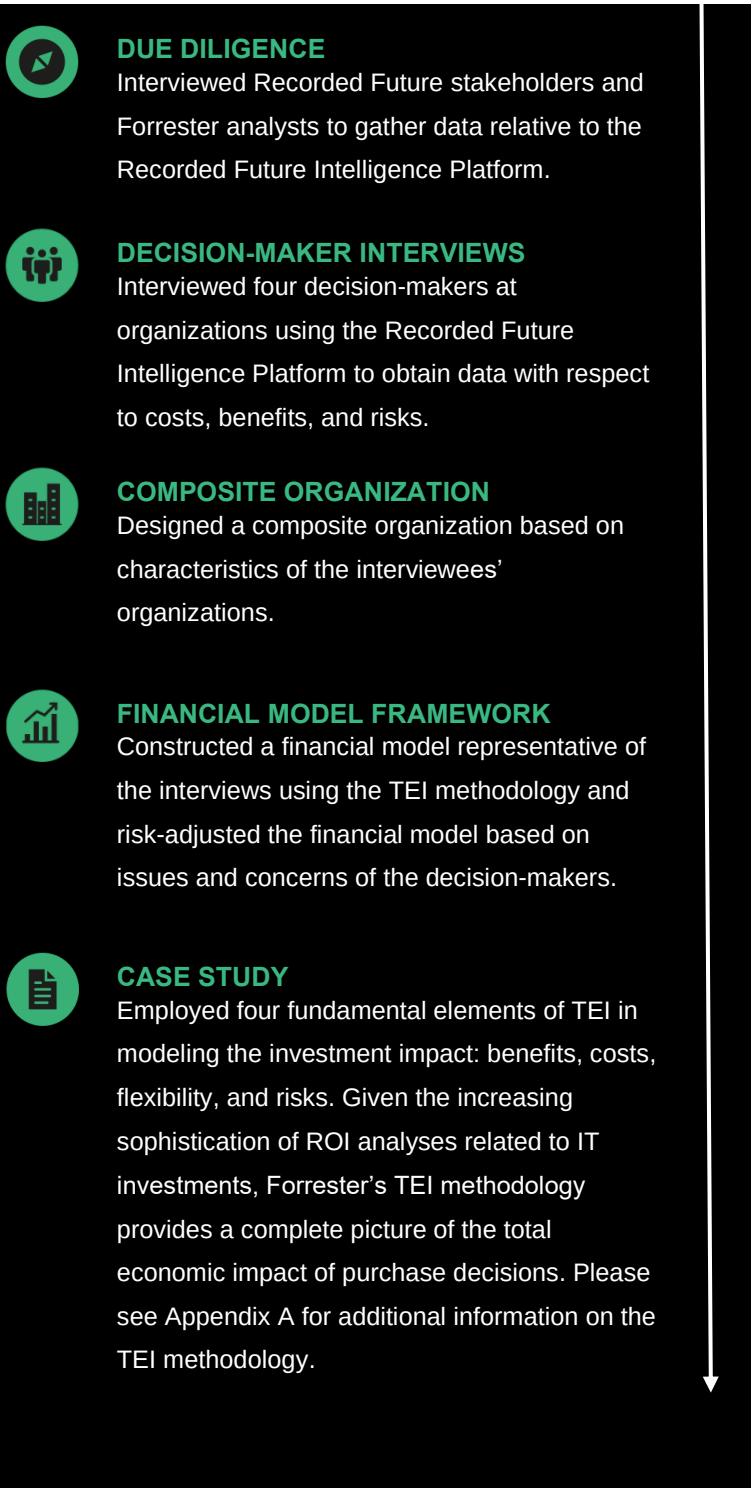
Not sure of an alert? Recorded Future reduced false positive identification times by 50% from an hour, typically to half an hour.

Global enterprises reallocated on average two threat intel resources by utilizing Recorded Future.

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 the Recorded Future Intelligence Platform.

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 the Intelligence Platform can have on an organization.



The Recorded Future Intelligence Platform Customer Journey

Drivers leading to the Recorded Future Intelligence Platform investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Revenue
Global cyberthreat leader	Manufacturing and chemicals	Global	$10+ billion
Deputy chief information security officer (CISO), Cyber intelligence lead	Payment technologies	Global	$1+ billion
Director of cyber intelligence	Hospitality	Global	$10+ billion
Threat intelligence manager	Retail	North America	$10+ billion

KEY CHALLENGES

Forrester interviewed and surveyed over 3,500 organizations in December of 2020 to determine their approach and experience with various cyber threat intelligence organizations and determined that the need for intelligence feeds have gone up from 4.2 in 2018 to an average of 7.5 in 2021, based on the need to cover the growing threat streams.[3] The emphasis is that intelligence vendors need to present not only broader, but also deeper level analyses to cover the different tactics used by would-be attackers.

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

- **Inadequate threat intelligence from existing sources to counter modern threat actors.** Interviewees spoke of the rapid increase in threats that proliferated across landscapes — commonly ones that did not present as a first strike. As a result, the mass of threats bore threats that potentially amounted to greater financial loss.
- **Using multiple threat sources was problematic in delivering data that is useable across the organization.** Using multiple sources of threat intelligence presented intel from broad ends of the spectrum, but it was difficult to bring that data together and have it correlated, creating more work for threat intelligence analysts.
- **Hampered visibility without integration into the greater security stack.** Using threat intelligence feeds from many feeds was difficult to organize into a central platform, such as a SIEM. Further, collating and disseminating the data was a tedious and fairly manual task, and using an immense amount of threat feeds added coverage but created exponentially more work for threat analysts. Where integrations between feeds and the security stack introduced disparate and unlinked data points for later analysis, some feeds were not easily integrated with the entirety of the stack, limiting visibility and actions.

> **"Because our business is so diversified, the market offerings were not picking up all of the data streams to suit our needs. For instance, our other threat intelligence platform just wasn't digging deep enough on the dark web. We had to peel back the onion to get what we needed."**
>
> *Deputy CISO, payment technologies*

SOLUTION INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Attain broader views on the areas where potential threats were brewing while reducing the number of threat intel feeds. Dark web and other non-public forums were top of mind for these organizations and was an absolute requirement, especially as it came to protecting their brand.
- Develop a deeper perspective on threats to proactively prepare and protect against them before attacks happen.
- Bring contextualized data into the security stack so that automation could relieve some of the threat hunting, effectively reduce investigational work and introducing operational efficiency downstream with incident response (IR).
- Curate threats to present what was important, so the noise was filtered to some degree before reaching the organization.
- Potentially provide vulnerability identification, especially in areas that traditional scanners could not pick up or help prioritize new or discovered vulnerabilities related to an organization's unique environment.

"We have vendors that help us provide intelligence around endpoints. We have information coming through for email and email activities. But really what Recorded Future has done is provide a wide base of knowledge, a wide base of information to help enrich both at the UI level and technical level."

Threat intelligence manager, retail

Key assumptions

- **Enterprise with 32,000 FTEs**
- **Six threat intelligence analysts**
- **50+ incident responders and security analysts**
- **Three security stack integrations**
- **Utilizes multiple threat intel feeds for 360-degree coverage**

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 four decision-makers 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. The composite organization is a global enterprise servicing both B2C and B2B customers. Its revenues are in the billions, and it has spent extensively in the past to develop its brand, so protection of its brand is crucial. To secure its global operations, there is both a distributed incident response force as well as a central security operations center (SOC). It employs six dedicated threat intelligence operators and more generalized security analysts and incident responders. In its current state, the composite's security stack is well developed and it leverages data from multiple threat intelligence feeds. The composite organization recognizes increasing and more sophisticate threats inhabit the deeper segments of the web, creating a need for a more holistic and far-reaching intelligence source.

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	Security, risk, and response operations efficiency	$1,068,622	$1,068,622	$1,068,622	$3,205,865	$2,657,504
Btr	Breach loss avoidance from early detection	$587,019	$587,019	$587,019	$1,761,058	$1,459,830
Ctr	Brand impact protection	$256,697	$256,697	$256,697	$770,091	$638,368
Dtr	Shift work to junior analysts	$205,081	$205,081	$205,081	$615,244	$510,007
	Total benefits (risk-adjusted)	$2,117,419	$2,117,419	$2,117,419	$6,352,258	$5,265,709

SECURITY, RISK, AND RESPONSE OPERATIONS EFFICIENCY

Evidence and data. Speed, breadth, depth, and most importantly, actionable data is what is expected of threat intelligence providers. Recorded Future met the interviewees' requirements for combinations that most other services cannot provide. The resulting combination nullified threats increased the efficiency of the security operations center (SOC), and reduced threats quicker. Some highlights from interviewees are as follows:

- The global cyberthreat leader at a manufacturing and chemicals company note, "We accumulated a number of threat intelligence programs from mergers and acquisitions, but many of them merely gave indicators. Recorded Future is so much more of a full service with a true intelligence team that adds a layer to the AI processing."
- The threat intelligence manager at a retailer noted that only Recorded Future fulfilled the collection requirements that the organization had. The requirements extending across network infrastructure, deep and dark web discussions, data exposure, domain chatter, and more.
- The director of cyberintelligence at a hospitality organization noted that it saw a double digit percentage reduction in time savings needed for triage and analyst support when responding to incidents.

> **"One of the hardest things about responding is the triage when we get an alert. It can take a really long time but, when we use Recorded Future, it takes a lot less time because of all the indicators and depth of information."**
>
> *Global cyberthreat leader, manufacturing and chemicals*

- The deputy CISO at a payment technologies organization suggested that as much as 45% of threat intelligence investigative times were eliminated, while incident responders saw a deflection of 10% of false alerts thereby eliminating the need for those responses altogether.

  Considering that incident responses required 3.7 hours per incident, the averted hours amounted to the tens and hundreds of thousands of hours

saved given the number of responses required at the interviewees' organizations.

- Recorded Future's direct intel feed via API led to the need for fewer intel solutions but provided wider and deeper coverage. This decreased the amount of correlation work and overall noise in SIEM environments. The net effect was greater overall efficiency within the threat intelligence team, SecOps, and incident responder groups due to greater information availability to all. When integrated into the clients' SOAR solutions, manual effort was further reduced.

Modeling and assumptions. The modeling basis Forrester has taken is predicated on the following:

- The composite organization is fairly mature in their security practice but desires additional security feeds that can facilitate automation and integration into SIEM and SOAR platforms.
- The organization uses multiple threat feeds but, as Recorded Future covers threats at a broad/deep level, the threat intelligence team leans on Recorded Future more heavily than some of the other intelligence providers.
- Based on interview results, threat intelligence operators save 40% of their time investigating threats that Recorded Future presents.

"Recorded Future is a force multiplier for our security team to do much more than our current headcount."

Deputy CISO, payment technologies

- Incident responders also save time through the deflection of false alerts along with decreased triage times.

  False positive alerts are reduced by 10%, which in turn decreases the work for incident response teams. Forrester research points to research and investigation times adding up to 3.7 hours per incident. Because the composite investigates 98,165 alerts per year, a 10% reduction is a substantial number of hours.

- Audit, compliance, and managerial reporting add to a substantial amount of time for security operations. With the need for evidence-based reporting, audit trails, and root cause analyses on incidents, hours add up quickly. Interview data indicates that control owners in the field will save 40% in time for reporting.

"There's workflows provided by Recorded Future to help my team of threat hunters, but its ability to push across all our tools democratizes the threat intel to be usable by others in security operations."

Cyber intelligence lead, payment technologies

Risks. Forrester identified risks that could potentially change the benefit value calculated, including:

- Varying coverage of previously deployed threat intelligence feeds. These feeds can vary depending on the breadth of sources and collection methods. Depending on the scope of existing threat intelligence feeds, the benefit listed can vary. Organizations should note that threat intelligence feeds — specifically end-point centric feeds versus dark web-focused feeds — are different but a degree of overlap in information can shift the business value equation.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of nearly $2.67 million.

Security, Risk, And Response Operations Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Hours spent on investigation, threat hunting, and triage work in prior environment	9 analysts*2,080 hours	18,720	18,720	18,720
A2	Work done using Recorded Future data, present state	Interviews	33%	33%	33%
A3	Reduction in investigation and threat hunting due to Recorded Future context and correlations	Interviews	40%	40%	40%
A4	SecOps hours saved on reduced triage and related work	A1*A2*A3	2,471	2,471	2,471
A5	Average fully burdened salary: Security engineer (hourly)	$126,785/2,080 hours	$60.95	$60.95	$60.95
A6	Subtotal: SecOps efficiency savings	A4*A5	$150,607	$150,607	$150,607
A7	Number of security alerts	Forrester internal research	98,165	98,165	98,165
A8	Incident responses deflected by Recorded Future as false positives	A7*10%	9,817	9,817	9,817
A9	Time spent on remediation efforts and additive investigation by incident response team (hours/response)	Forrester internal research	3.7	3.7	3.7
A10	Average fully burdened salary: Incident response analyst (hourly)	$99,419/2,080 hours	$47.80	$47.80	$47.80
A11	Subtotal: Incident response deflected work savings	A8*A9*A10	$1,736,235	$1,736,235	$1,736,235
A12	Hours spent on governance, risk management, and compliance (GRC) analysis and reporting in prior environment	10 control owners at 20 hours per quarter	800	800	800
A13	Reduction in manual GRC work with Recorded Future	Interviews	40%	40%	40%
A14	Time savings from Recorded Future intelligence (hours)	A12*A13	320	320	320
A15	Average fully burdened salary: GRC analyst (hourly)	$139,167/2,080 hours	$66.91	$66.91	$66.91
A16	Subtotal: GRC efficiency savings	A14*A15	$21,411	$21,411	$21,411
A17	Productivity recapture on time saved	Forrester assumption	70%	70%	70%
At	Security, risk, and response operations efficiency	A17*(A6+A11+A16)	$1,335,777	$1,335,777	$1,335,777
	Risk adjustment	↓20%			
Atr	Security, risk, and response operations efficiency (risk-adjusted)		$1,068,622	$1,068,622	$1,068,622
	Three-year total: $3,205,865			**Three-year present value: $2,657,504**	

BREACH LOSS AVOIDANCE FROM EARLY DETECTION

Evidence and data. Based on Forrester's Cost of a Security Breach survey data from Q4 of 2020 with 351 mid to large enterprise respondents, Forrester estimates most enterprise organizations will suffer on average 2.5 breaches per year.[4] Interviewees for this study found that the intelligence Recorded Future provided enabled their organizations to anticipate and avoid breaches in the following ways:

- Earlier detection from broader/deeper sources let threat intel analysts and SecOps stop threats early.
- The weaponized exploit indication feature in Recorded Future gave SecOps and network operations (NetOps) better insight as to the potential danger of threats and exploits. The global cyberthreat leader at a manufacturing and chemicals organization stated: "Using our other data source was like flipping a coin on the level of importance. Recorded Future figures out if the threats have been weaponized and their degree of impact then directs our team's prioritization."
- The cyber intelligence lead at a payment technologies organization shared, "Greater accuracy on whether threats and indicators of compromise were real [or false alerts] helped stop real incidents from becoming large scale breaches."

Modeling and assumptions. The modeling basis Forrester has taken is predicated on the following:

- The composite organization faces 2.5 material breaches per year.[5]
- Breach costs avoided include:
  - Customer and vendor compensation.
  - Regulatory fines.
  - Compliance costs.

> **"Really what it's doing is it's preventing us from experiencing certain threats that would have a huge monetary impact on our stock price, our customers. Really, that's the cost of doing business. You have to monitor these things. This is the landscape we're in, but it's helping us prevent from being on the first page of the Wall Street Journal."**
>
> *Threat intelligence manager, retail technologies*

- The composite organization uses Recorded Future in conjunction with multiple threat intelligence feeds, as customers interviewed stated that no single threat feed can cover the entire spectrum. The majority of threat intelligence platforms in place at the organizations do not cover the most crucial threat elements. Thus, Recorded Future data is more apt to help the composite organization avoid a breach. Recorded Future provides broader and deeper intelligence which shines a light on a greater number of critical vulnerabilities and threats thus play a larger role in breach prevention.
- When using Recorded Future in the incident responder capacity, the composite organization obtains greater visibility on threats and context on alerts. This includes attribution back to who the threat actors are, their importance, and how to approach a security incident. Correlation often means everything in addressing incidents at their core and interviewees noted that capability as a highlight.
- Interviewees noted their governance, risk, and compliance personnel found that reporting and providing an evidential trail to the sources was

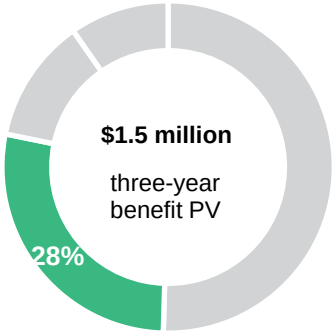
important not only to internal and external auditors, but also management. Savings were seen across control owners and auditors.

Risks. Forrester identified risks that could potentially change the benefit value calculated, including:

- Organizations of differing industries may see different levels of alerts and incidents. For instance, the Forrester Q4 2020 survey indicated that financial services organizations were twice as likely to be met with a breach, even while operating advanced security programs.
- Incident response rates vary and can be fewer for some industry verticals which may affect the savings on overall resolutions.
- Existing security stack architecture. Depending on the level of integration within the stack and the tools deployed, such as SIEMs and SOAR, the mean time to identify and resolve can change the equation.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of nearly $1.46 million.

Breach cost avoidance from early detection



Breach Loss Avoidance From Early Detection

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Average number of data breaches per year	Forrester research	2.5	2.5	2.5
B2	Average potential cost of data breach ($30.81 per employee) exclusive of internal-user downtime	Forrester research	$986,076.71	$986,076.71	$986,076.71
B3	Increased visibility to potential threats by Recorded Future	Interviews	20%	20%	20%
B4	Reduced likelihood of a breach attributable to Recorded Future	Interviews	60%	60%	60%
B5	Subtotal: Avoided costs of remediation, customer resolution, regulatory fines, revenue loss from business downtime, and all other external-facing costs	B1*B2*B3*B4	$295,823	$295,823	$295,823
B6	Number of internal business users	Composite	32,000	32,000	32,000
B7	Average burdened salary: Business user (hourly)	$50,000*1.35/2,080 hours	$32.45	$32.45	$32.45
B8	Diminished/eliminated internal-user productivity hours per breach	Forrester research	3.6	3.6	3.6
B9	Average percentage of employees affected per breach	Forrester research	56%	56%	56%
B10	Productivity capture	Assumption	70%	70%	70%
B11	Subtotal: Cost of reduced internal productivity	B1*B4*B6*B7*B8*B9	$437,951	$437,951	$437,951
Bt	Breach loss avoidance from early detection	B5+B11	$733,774	$733,774	$733,774
	Risk adjustment	↓20%			
Btr	Breach loss avoidance from early detection (risk-adjusted)		$587,019	$587,019	$587,019
	Three-year total: $1,761,058			**Three-year present value: $1,459,830**	

BRAND IMPACT PROTECTION

Evidence and data. Recorded Future's Brand Intelligence module specifically identified any threats that relate or are tied into an organization's brand before material harm can be done. Essentially, this was what gives organizations the ability to take proactive measures to prevent domain abuses, privileged impersonation, or leaked credentials found on the dark web so that actions could be taken to mitigate harm to their brand.

- Interviewees noted their organizations' priorities with Recorded Future were to go one layer deeper than what other threat intelligence services offered, delving into areas like the dark web and those within the criminal underground that are typically closed off to most other intelligence services.
- Customers stated multiple ways in which they benefited, which included website name infringement/typosquatting prevention, avoidance of credential leaks that might be offered for sale, and managed takedowns of offenders. These threats were typically mitigated before they proliferated and caused extensive brand damage.
- The director of cyberintelligence at a hospitality organization stated that once enabled, Recorded Future sent an automated alert that a threat actor was selling a coupon used by a partner. It had been exploited for months and caused $2.9 million dollars in damage. Had it gone on, the damage would have been far worse.

"We have found success around monitoring the leaked credentials on the deep and dark web on Recorded Future, which helped mitigate the impact to our reputation. We've also identified third-party breaches for our suppliers using the solution as well. They've been very helpful. It's been a win in my book."

Threat intelligence manager, retail

Modeling and assumptions. The modeling basis Forrester has taken is predicated on the following:

- Brand impact is predicated on a set of factors that Forrester has determined to have lasting effect. The factors include but are not limited to:
    - Brand reputational damage and the cost to recuperate it.
    - Cost of customer reacquisition.
    - Customer lawsuits and compensation.
- Factored against the average rate of a material security breach, Forrester estimates that an average of nearly a million dollars is at stake.
- Due to the fact that Recorded Future makes up only a portion of the entire security stack, Forrester estimates that 12 % of loss prevention is attributed specifically to Recorded Future based on the combination of the interviewees' reported statistics and Forrester's internal Cost Of A Security Breach survey.[6]

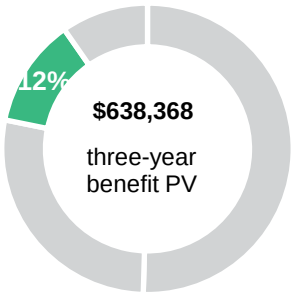
Recorded Future reduced negative brand impact monetarily by **$212,666** annually.

Risks. Forrester identified risks that could potentially change the benefit value calculated, including:

- The subjectivity and variation on the immediacy of brand impact depending on B2B or B2C emphasis.
- The expectation that B2C organizations realize higher losses on brand exposures, while B2B organizations experience a longer-lasting detriment to their brand.

Results. To account for these risks, Forrester adjusted Brand Impact Protection benefit downward by 10%, yielding a three-year, risk-adjusted total PV of over $638,000.

Recorded Future reduces negative brand impact



Brand Impact Protection

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average number of breaches per year	Forrester research	2.5	2.5	2.5
C2	Average potential cost of brand impact per breach ($29.71 per employee)	Forrester research	$950,728.95	$950,728.95	$950,728.95
C3	Reduced likelihood of a breach attributable to Recorded Future	Interviews	12%	12%	12%
Ct	Brand impact protection	C1*C2*C3	$285,219	$285,219	$285,219
	Risk adjustment	↓10%			
Ctr	Brand impact protection (risk-adjusted)		$256,697	$256,697	$256,697
	Three-year total: $770,091			**Three-year present value: $638,368**	

SHIFT WORK TO JUNIOR ANALYSTS

Evidence and data. Interviewees cited that Recorded Future allowed their organizations to do more with less, largely contributed by the context and depth of information Recorded Future provided. The result was a shift to move some segments of the security operations to a more junior level of analysts.

- In large, interviewees said their organizations moved some aspects of threat hunting and security operations to junior employees, enabling senior-level analysts to focus on more difficult tasks. As the deputy CISO of a payment technologies company put it, “The data is democratized to our entire group in a usable form so that people who aren’t threat intel specialists can take action and not overutilize our threat intelligence team.”
- Not only did junior analysts comprehend the data flows easier with Recorded Future, but they were also better able to take action resulting in a quicker remediation time, benefiting end-user productivity.
- Interviewees mentioned that a range of 35% to 70% of analyst/senior analyst-level work shifted to junior analysts.

Shifted advanced security work to junior analysts by as much of **50%** of total tasks.

Modeling and assumptions. The modeling basis Forrester has taken is predicated on the following:

- The composite organization uses a 33%-to-67% split of senior analysts to junior analysts, respectively.

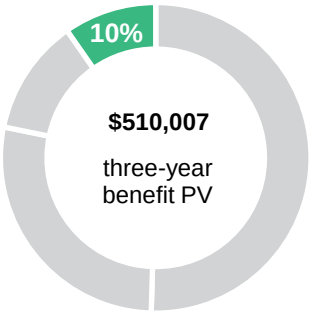
- While Recorded Future's intelligence helps security professionals reach a safer state faster, the composite does not use only Recorded Future. In the composite's current state, Recorded Future is one of four threat intelligence feeds. Overlaps do occur but the timeliness and the correlated intelligence that Recorded Future provides is critical and otherwise hard to source from alternative feeds, thus the attribution to Recorded Future on feed dependency is 33%, based upon interviewees' statements.
- The savings found here by shifting work to a junior group is mutually exclusive from the savings that IR groups recognize from simpler data correlation.
- With everything considered between the impact of Recorded Future data and the number of workflows that depend on the data, the composite organization reallocates up to 50% of senior analyst work to more junior staff. Senior analysts are now free to do additive threat hunting and new implementations.

Risks. Forrester identified risks that could potentially change the benefit value calculated, including:

- Organizations leveraging managed detection and response (MDR) services could benefit from the data but may not see the savings from the MDR provider. MDR costs are often billed by the size of interviewees' organizations and can thus provide no hard savings. Dependency on MDR may also affect the savings realized as some MDR solutions are an extension of the security team while, in other instances, they replace the greater majority of the internal team.
- An organization's willingness to use junior analysts, who might require longer training and ramp times to become effective.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $510,000.

Advanced security work shifted to junior analysts



Shift Work To Junior Analysts

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Hours spent on threat intelligence and subsequent SecOps workflows in prior environment	Interviews	50960	50960	50960
D2	Work attributed to Recorded Future data in present state	Interviews	33%	33%	33%
D3	Percent of work shifted to junior analysts	Interviews	50%	50%	50%
D4	Average burdened salary: Senior security analyst (hourly)	$132,636.15/2,080 hours	$63.77	$63.77	$63.77
D5	Average burdened salary: Junior security analyst (hourly)	$76,269.60/2,080 hours	$36.67	$36.67	$36.67
Dt	Shift work to junior analysts	D1*D2*D3*(D4-D5)	$227,868	$227,868	$227,868
	Risk adjustment	↓10%			
Dtr	Shift work to junior analysts (risk-adjusted)		$205,081	$205,081	$205,081
	Three-year total: $615,244			**Three-year present value: $510,007**	

UNQUANTIFIED BENEFITS

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

- **Friendly fraud and coupon abuse.** Friendly fraud represents as much as 60% of overall fraud loss, and organizations were perplexed as to how to reduce this loss figure as it meant the possibility of losing customer loyalty and potential sales.
- Coupon abuse has become rampant with digitally focused retailers. In a single instance, the threat intelligence manager at a retailer noted the organization lost nearly $3 million via a leaked coupon code. Even worse, threat actors resold these coupon codes for their benefit at the expense of the interviewee's organization. Recorded Future scans the corners of the web to surface where the organization's brand might surface so that unnecessary loss can be curtailed.

FLEXIBILITY

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

- **Vulnerability management proactiveness.** Multiple interviewees expressed that the combination of threat intelligence and vulnerability intelligence assisted their organizations in plugging and preventing vulnerabilities before they could be exploited. For these organizations, this meant keeping threat actors out from the beginning, rather than being reactive and recoding after breaches have occurred.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Implementation, integration, training, and ramp costs	$56,262	$2,296	$20,296	$20,296	$99,149	$90,371
Ftr	Cost of subscriptions	$0	$577,500	$577,500	$577,500	$1,732,500	$1,436,157
	Total costs (risk-adjusted)	$56,262	$579,796	$597,796	$597,796	$1,831,649	$1,526,528

IMPLEMENTATION, INTEGRATION, TRAINING, AND RAMP COSTS

Evidence and data. Implementation was the first step to getting started on Recorded Future. Secondarily, integrations to SIEMs, endpoints, and SOARs progressively added value to the solution. Costs, such as deployment, integration, and training were covered in this area.

- Interviewees spoke of extreme fast deployment times for the Recorded Future platform and its modules.
- Areas that were more difficult were related to integrations with the other pieces within the security stack. However, the interviewees stated that difficulties typically arose from homebrew systems and heavily modified public applications.
- A level of baselining and acclimation to the organizations was necessary and varied depending on the needs of the organization. Primarily, this was for the fine-tuning of threat intelligence incorporation into the existing security stack.

Modeling and assumptions. The modeling basis Forrester has taken is predicated on the following:

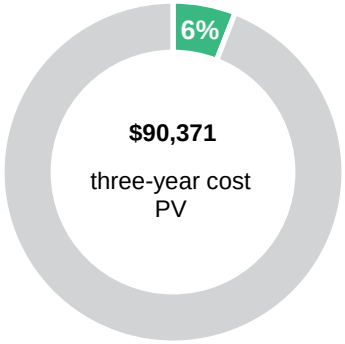
- Pricing for the composite organization is based on the characteristics of interviewees and list level pricing from Recorded Future.
- The majority of costs are borne internally and are not directly attributable to Recorded Future. Costs, such as internal configuration and training, are highly variable with most organizations, but overall, findings indicate that a composite organization assumes very few hours on the actual deployment of the Recorded Future solution.
- Integrations matter. The tie-ins with various other security programs allow the consumption of data and insights Recorded Future produces in other platforms, where workflows continue in the security response lifecycle. To that end, the composite organization's integration costs depend on the complexity and level of modification to existing platforms that ingest Recorded Future data.
- Training and ramp times are minimal but need to be taken into account for turnover in the larger security group.

Risks. Potential risks that can negatively affect the cost basis reflected in this group are as follows:

- The level of modifications to existing security platforms.
- The level of automation and orchestration desired that originates from Recorded Future data.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of over $90,000.

Implementation and training costs



Implementation, Integration, Training, And Ramp Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Internal configuration and implementation hours, total	Composite	80	10	10	10
E2	Average burdened salary: Security analyst (hourly)	$132,636.15/2,080 hours	$63.77	$63.77	$63.77	$63.77
E3	Hours of effort required for integration with third parties	80 hours per integration*3 integrations	240			
E4	Number of security analysts requiring training	Composite	9	1	1	1
E5	Hours required for training and to achieve proficiency with platform per analyst	Interviews	20	20	20	20
E6	Professional services	Interviews	$15,000		$15,000	$15,000
Et	Implementation, integration, training, and ramp costs	E2*(E1+E3+E4+E5)+E6	$46,885	$1,913	$16,913	$16,913
	Risk adjustment	↑20%				
Etr	Implementation, integration, training, and ramp costs (risk-adjusted)		$56,262	$2,296	$20,296	$20,296
	Three-year total: $99,149			**Three-year present value: $90,371**		

COST OF SUBSCRIPTIONS

Evidence and data. The cost of Recorded Future Threat Intelligence, Brand Intelligence, and SecOps Intelligence were based on current list pricing as of September 2021.

- Organizations should think of Recorded Future capabilities as per module with each providing a different set of intelligence to help specific groups within an organization optimize their work within the security, compliance, IT, or vulnerability teams.
- There may be additional discounts available when purchasing multiple modules. Contact Recorded Future or one of their partners for more information.
- Subscriptions are based on the intelligence modules licensed within the platform, although the majority of Recorded Future intelligence is

exported via APIs (at a cost) to different security platforms for use without the need for additional licenses. Threat hunting is frequently completed through Recorded Future and all other relevant data is relayed to incident responders and other security analysts for remediation and investigations.

Integrations from platforms such as a SIEM with Recorded Future provided information for all integrated users.

Modeling and assumptions The modeling basis Forrester has taken is predicated on the following:

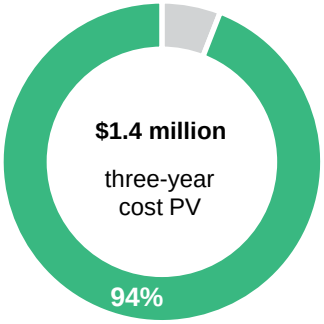
- The modeling assumes that threat intelligence analysts and SecOps personnel sometimes own multiple Recorded Future licenses, for instance the SecOps module license as well as the Threat intelligence modules.
- The composite organization leverages multiple integrations of data flow from Recorded Future, piping the data into its SIEM and SOAR platforms for automation.
- Costs are not scaled across a three-year span, and it would be presumptuous to state it as the current state of corporate growth is in fluidly changing due to economic conditions.

Risks. Risk can fluctuate for the business as it relates to licensing costs; this is due to the level of integration and number of licenses each organization requires.

- If used in sole capacity as threat hunting tool without aggregation to other security platforms, costs can go down.
- If purchasing in lesser amounts, costs of licensing can vary.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of under $1.44 million.

Subscription costs



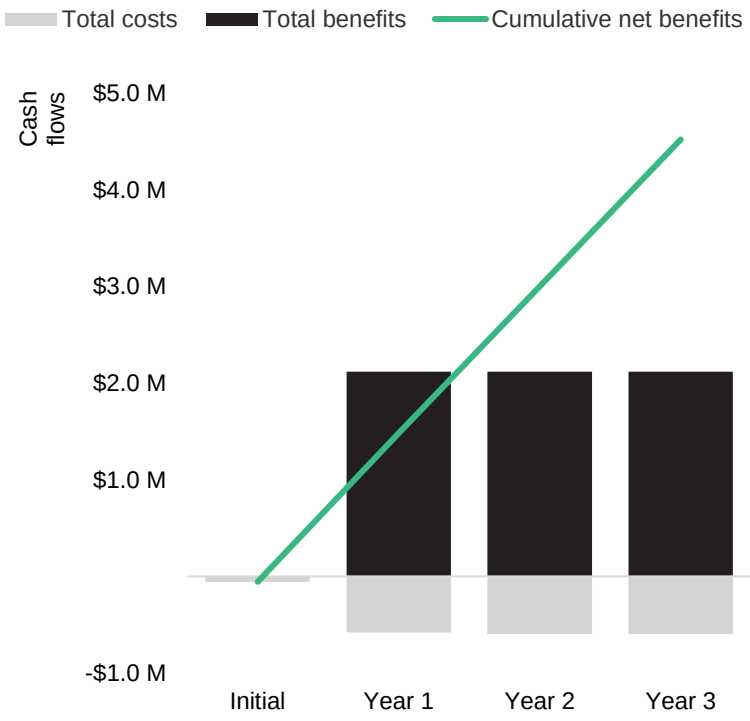
Cost Of Subscriptions

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Number of Recorded Future users	Composite		9	9	9
F2	Cost for brand, threat intelligence, and SecOps intelligence, inclusive of managed takedowns	List pricing		$405,000	$405,000	$405,000
F3	Number of API integrations	Composite		3	3	3
F4	Cost of data integration licenses	Interviews		$120,000	$120,000	$120,000
Ft	Cost of subscriptions	F1*F2+F3*F4	$0	$525,000	$525,000	$525,000
	Risk adjustment	↑10%				
Ftr	Cost of subscriptions (risk-adjusted)		$0	$577,500	$577,500	$577,500
	Three-year total: $1,732,500			**Three-year present value: $1,436,157**		

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	($56,262)	($579,796)	($597,796)	($597,796)	($1,831,649)	($1,526,528)
Total benefits	$0	$2,117,419	$2,117,419	$2,117,419	$6,352,258	$5,265,709
Net benefits	($56,262)	$1,537,623	$1,519,623	$1,519,623	$4,520,608	$3,739,181
ROI						245%
Payback period						< 6 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."

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] 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

[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[3] Source: "The Forrester Wave™: External Threat Intelligence Services, Q1 2021," Forrester Research, Inc., March 23, 2021.

[4] Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[5] Source: Ibid.

[6] Source: Ibid.


FORRESTER®