The Total Economic Impact™ Of The ThreatConnect Platform

Cost Savings And Business Benefits Enabled By ThreatConnect
Table Of Contents

Executive Summary 1
  Key Findings 1
  TEI Framework And Methodology 4
The ThreatConnect Platform Customer Journey 5
  Interviewed Organizations 5
  Key Challenges 5
  Key Results 6
  Composite Organization 6
Analysis Of Benefits 8
  Savings From Automated Triage Of Alerts 9
  Savings From Automated Triage Of Phishing Emails 10
  Savings From Curating Threat Intelligence Feeds And Identifying Redundant Security Tools 11
  Improved Organizational Security 12
  Unquantified Benefits 13
  Flexibility 14
Analysis Of Costs 16
  Software Fees 16
  Implementation And Training 16
  Cost Of Ongoing Work Performed In ThreatConnect 17
Financial Summary 19
The ThreatConnect Platform: Overview 20
Appendix A: Total Economic Impact 21
Appendix B: Endnotes 22

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.

© 2019, 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, RoleView, TechRadar, 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

According to Forrester Analytics’ Global Business Technographics® Security Survey, 2018, 50% of global network security decision makers report that their organizations experienced at least one breach in the previous 12 months.¹ Security teams are often ill-equipped to detect and respond to breaches: Analysts process alerts manually, which slows them down, increasing the dwell time of the threat. Not surprisingly, 62% of global security technology decision makers at enterprises said that using automation and orchestration tools to improve security operations is a high or critical priority.²

ThreatConnect provides an intelligence-driven security operations platform that helps its customers integrate disparate security technologies, automate workflows and establish process consistency, measure the effectiveness of the security programs, and improve organizational security. ThreatConnect 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 ThreatConnect Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the ThreatConnect Platform on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers using ThreatConnect to build more integrated and cost-efficient security programs across their enterprises.

Prior to using ThreatConnect, the customers struggled with a lack of a single security management interface, faced an overwhelming volume of incoming security signals that required manual processing, and failed to establish connections between security teams.

With the investment in ThreatConnect, organizations gained the ability to introduce Playbooks to triage alerts, indicators of compromise (IOCs), and phishing emails, saving thousands of hours’ worth of analysts’ time every month. A consolidated view of the security tools and intelligence feeds revealed that teams were using redundant and, in some cases, non-value-add products. Organizations stopped paying unnecessary license fees, reducing the cost spent on security data. Previously disconnected, security teams received a platform to interact on through ThreatConnect Communities.

“With ThreatConnect, I was able to consolidate all the tasks that were spread across different tools into one place,” said the director of cybersecurity and analytics development at a security infrastructure company. “Now, we only have one tool, and it has an enterprise-grade user interface.”

Key Findings

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

- Savings from automated triage of alerts: $3 million
- Savings from automated triage of phishing emails: $252,200
- Savings from curating threat intelligence feeds and identifying redundant security tools: $111,900
The Total Economic Impact™ Of The ThreatConnect Platform

» **Saved $3 million by automating triage of alerts.** Prior to using the ThreatConnect Platform, security teams were overwhelmed by quantities of alerts and the number of threat intelligence feeds to process. Analysts were stretched thin, and a significant portion of the incoming security information went unaddressed due to the lack of capacity. Each interviewed organization used ThreatConnect to automate workflows and free up limited security and threat intelligence resources for cases where a deeper investigation was required.

» **Saved $252,171 by automating triage of phishing emails.** Organizations received thousands of phishing emails per month, each of the emails requiring analysts’ review to identify if it was malicious. ThreatConnect automated the initial email diagnostics, including verification of multiple parameters, such as IP address, email address, or URL, to prioritize the ones that had a higher likelihood of posing a threat. The analysts then only spent valuable time on the emails that were flagged by ThreatConnect as “risky.”

» **Saved $111,908 by curating threat intelligence data feed and identifying redundant security tools.** Prior to ThreatConnect, companies lacked a single management interface that integrated all available security data, which, in some cases, resulted in redundant licenses and fees. ThreatConnect provided a single view of the security information available to organizations, helping them to reassess the value of the subscriptions and to retire the redundant or non-value-add ones.

» **Improved organizational security by 5%.** Before ThreatConnect, enterprise security teams lacked full visibility of the security landscape. They struggled to consolidate the information from disparate security tools and spent most of their time manually analyzing the incoming alerts. As a result, potentially critical security threats could go uninvestigated and unaddressed longer, exposing the organization to greater risk. ThreatConnect lifted a burden of manual work and provided security teams with the bigger picture view, allowing them to prioritize the actions to defend the organization.

**Benefits (Three-Year)**

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saved from automated triage of alerts</td>
<td>$3.0M</td>
</tr>
<tr>
<td>Saved from automated triage of phishing emails</td>
<td>$252.2K</td>
</tr>
<tr>
<td>Saved from curating threat intelligence feeds and identifying redundant security tools</td>
<td>$111.9K</td>
</tr>
<tr>
<td>Improved organizational security</td>
<td>$407.5K</td>
</tr>
</tbody>
</table>

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

» **ThreatConnect provided opportunities for collaboration.** Security and threat intel communication was previously shared via email, which was inefficient and took a long time. With ThreatConnect, security teams received access to an easy-to-use platform to quickly share knowledge, ask for advice, or solve a problem.
Dashboards and reports helped monitor and evaluate security operations and intelligence. Several interviewed organizations used ThreatConnect dashboards to see in one place what was happening in their environments in real time. Senior leadership looked at dashboards to assess the big picture of the threats faced by the organization, while program managers tracked the utilization and effectiveness of the ThreatConnect Playbooks to identify opportunities for training and new automations.

Better visibility into internal security practices led to user education. One organization identified users who frequently submitted phishing emails that were, in fact, non-malicious. The organization used Playbooks to automatically assign phishing email training to those employees. As a result, the organization reduced the number of phishing emails reported by users by more than 60%, while users also became significantly better at identifying and reporting true phishing attempts.

Easy integration with security tools provided a unified view of the security technology stack. Each interviewed organization used a variety of security technologies provided by different vendors. Before ThreatConnect, the tools did not exchange data with each other. Companies found it easy to onboard new security tools onto the ThreatConnect Platform, while enjoying the benefit of a single management interface.

Costs. Each interviewed organization expended costs and resources associated with annual license fees, implementation and training, and ongoing management and development costs. The associated software fees and resources required vary greatly depending on the security team size and specific organizational needs. For more information regarding the ThreatConnect Platform, please contact your ThreatConnect representative.

ThreatConnect license fee. The interviewed organizations incurred annual license fees for the ThreatConnect Platform. ThreatConnect pricing is based on the number of users and the type of the subscription.

Cost of implementing and training. Implementing and configuring ThreatConnect required involvement from different groups, including database administrator (DBAs), network specialists, and security team members, for a duration ranging from one week to several months. Interviewed organizations paid a flat implementation fee to ThreatConnect.

Ongoing management and development costs. The interviewed organizations incurred ongoing costs of development and product management. Several developers dedicated a portion of their time to building automations in ThreatConnect. Director-level security professionals analyzed data within ThreatConnect, planned the automation roadmap, or built reports for senior management.

Forrester’s interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $3.7 million over three years versus costs of $888,213, adding up to a net present value (NPV) of $2.8 million and an ROI of 320%.

“ThreatConnect provided security teams with the bigger picture view and a better understanding of the threat landscape, so that they can better prioritize the actions they take to defend the enterprise.”

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

**TEI Framework And Methodology**

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

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 ThreatConnect can have on an organization:

- **DUE DILIGENCE**
  Interviewed ThreatConnect stakeholders and Forrester analysts to gather data relative to the ThreatConnect Platform.

- **CUSTOMER INTERVIEWS**
  Interviewed four organizations using ThreatConnect to obtain data with respect to costs, benefits, and risks.

- **COMPOSITE ORGANIZATION**
  Designed a composite organization based on characteristics of the interviewed organizations.

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

- **CASE STUDY**
  Employed four fundamental elements of TEI in modeling the ThreatConnect Platform 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.

**DISCLOSURES**

Readers should be aware of the following:

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

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

ThreatConnect 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.

ThreatConnect provided the customer names for the interviews but did not participate in the interviews.
The ThreatConnect Platform Customer Journey

BEFORE AND AFTER THE THREATCONNECT INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with ThreatConnect customers. Interviewed customers include the following:

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>REGION</th>
<th>INTERVIEWEE</th>
<th>TYPE OF IMPLEMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security infrastructure</td>
<td>Headquartered in the US</td>
<td>Director, cybersecurity analytics development</td>
<td>Dedicated cloud</td>
</tr>
<tr>
<td>Defense</td>
<td>Headquartered in the US</td>
<td>Director, information sharing and analysis center</td>
<td>Dedicated cloud</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Headquartered in the US</td>
<td>Senior IT security analyst</td>
<td>On-premises</td>
</tr>
<tr>
<td>Financial services</td>
<td>Headquartered in the US</td>
<td>Security intelligence team lead Security intelligence analyst</td>
<td>On-premises</td>
</tr>
</tbody>
</table>

Key Challenges

The interviewed organizations shared the following challenges leading up to decision to invest in ThreatConnect:

› **Security data residing in multiple systems.** Prior to ThreatConnect, the organizations had to manage security data from disparate security systems and feeds and had no centralized console to get the overall picture. Lack of transparency often resulted in teams duplicating work in silos and paying license fees for redundant tools.

› **Manual ingestion, triage, and processing of alerts.** Organizations struggled to keep up with the growing number of alerts analysts needed to process manually. Even better trained or more experienced security professionals spent time on manual instead of proactive work.

› **Lack of a single monitoring interface for security operations and intelligence.** Prior to ThreatConnect, companies lacked a single 360-degree view of all available security data, which resulted in redundant licenses and fees.

› **Inefficiencies in communication across security teams.** Security-related communication was previously conducted via email, which was inefficient and took a long time. Security teams and individuals felt disconnected and had no visibility into each other’s work streams and priorities.

› **Unaddressed security threats.** The volume of threats that faced the organizations was far greater than the current capacity to process them. Threat prioritization was also a challenge for the security operations center (SOC) analysts as a result of the volume.

“All security teams were collecting, generating, and analyzing intelligence on their own, and some of them had built internal tools to do so. We were looking for a centralized platform that was generally acceptable to everyone within the organization.”

*Director of cybersecurity analytics development, security infrastructure*
Key Results

The interviews revealed that key results from the ThreatConnect investment include:

› **Lowered barriers to collaboration.** Using a single platform brought security teams closer together and encouraged analysts to spread awareness or share experiences with a broad audience to speed up resolution. “Because of the ease of setting up Communities in ThreatConnect, we’ve had instances where we’ve had an emergency, an incident, and we quickly stood up a Community that we put a lot of folks in so they could collaborate securely, and they managed to find the solution quickly,” said the director of information sharing and analysis center at a defense company.

› **Automated ingestion of intelligence data.** Interviewed organizations automated a significant portion of the triage for alerts, IOCs, vulnerabilities, and phishing emails, freeing up experienced analysts to do more proactive and specialized work.

› **Significant and ongoing cost avoidance and cost reduction.** With the trackable metrics described above, the organizations can report on cost avoidance and cost reduction by task and by security team. They can identify redundant or non-value-add intelligence feeds and security tools that could be retired for additional savings.

› **Trackable metrics.** The organizations can now track not only the type and frequency of threats they face, but also the outcomes of their automation efforts, such as: how many times any given Playbook has been run or how much time the organization has saved by implementing an automated workflow.

› **Improved organizational security.** By investigating previously unaddressed threats while at the same time giving their analysts more time to proactively search for threats, the organizations are better protected against vulnerabilities and threats.

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 four 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.** It is a global, multibillion-dollar enterprise. The organization has a strong brand and a large customer base. The organization is geographically distributed and has several security-focused teams. No specific threat intelligence platforms or security automation and orchestration solutions were deployed prior to ThreatConnect. Before investing in the ThreatConnect Platform, the organization conducted a comprehensive vendor selection process. The driving factors were automation and orchestration capabilities, integrations with existing systems, deep understanding of threat intelligence, and the ability to bring all security information under one roof.

**Deployment characteristics.** The organization uses ThreatConnect in its operations across all security teams.

Key assumptions

- $5 billion in revenue
- 20,000 employees
- 5,000 alerts per week
- 750 phishing emails per week
Systems that integrate with the ThreatConnect Platform.
ThreatConnect integrates with the following systems: third-party threat intelligence providers, security information and event management (SIEM), network security, endpoint security, malware analysis, incident response and ticketing, vulnerability management, enrichment, and analysis.
The Total Economic Impact™ Of The ThreatConnect Platform

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

<table>
<thead>
<tr>
<th>REF.</th>
<th>BENEFIT</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
<th>TOTAL</th>
<th>PRESENT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atr</td>
<td>Savings from automated triage of alerts</td>
<td>$982,800</td>
<td>$1,202,947</td>
<td>$1,431,507</td>
<td>$3,617,254</td>
<td>$2,963,138</td>
</tr>
<tr>
<td>Btr</td>
<td>Savings from automated triage of phishing emails</td>
<td>$85,925</td>
<td>$102,251</td>
<td>$119,195</td>
<td>$307,370</td>
<td>$252,171</td>
</tr>
<tr>
<td>Ctr</td>
<td>Savings from curating threat intelligence feeds and identifying redundant security tools</td>
<td>$45,000</td>
<td>$45,000</td>
<td>$45,000</td>
<td>$135,000</td>
<td>$111,908</td>
</tr>
<tr>
<td>Dtr</td>
<td>Improved organizational security</td>
<td>$154,400</td>
<td>$164,282</td>
<td>$174,796</td>
<td>$493,477</td>
<td>$407,460</td>
</tr>
<tr>
<td></td>
<td>Total benefits (risk-adjusted)</td>
<td>$1,268,125</td>
<td>$1,514,479</td>
<td>$1,770,498</td>
<td>$4,553,102</td>
<td>$3,734,677</td>
</tr>
</tbody>
</table>

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $3.7 million.
Savings From Automated Triage Of Alerts

Each interviewed organization used ThreatConnect to automate workflows and free up limited SOC and threat intelligence resources for cases where a deeper investigation was required. Prior to using the ThreatConnect Platform, security teams were overwhelmed by quantities of alerts to process and the number of threat intelligence feeds to check against. The senior IT security analyst at the healthcare company summarized the situation, “It was impossible for analysts to check all the alerts we receive without any kind of automation.” Forrester research shows that manual activities and alert fatigue make the security teams slower to respond to security events, leaving organizations vulnerable.4

› To reduce the load on its security and IT staff, the healthcare company used ThreatConnect to introduce more than 60 workflow automations with Playbooks, saving $1.3 million per year in labor costs.

› Similarly, the defense company implemented nearly 40 Playbooks to automate repeatable analyst actions and saved thousands of hours’ worth of analyst time. The director of information sharing and analysis center said: “We’ve taken a couple of the typical analyst use cases and put them into Playbooks. And while we lowered the costs, our main goal was to put the decision makers where they needed to be — at the top of the cognitive triangle.”

› The security infrastructure company used automation enabled by ThreatConnect to enrich the alert data received by analysts, shortening time spent on research. For example, a network threat protection team received between 10 and 100 alerts each day, and it took a senior FTE 30 minutes to an hour to resolve an alert. With ThreatConnect, the time has been reduced to several minutes, and the ability to respond is no longer limited to senior professionals, freeing them from spending time on manual and tedious work.

Forrester assumes that:

› The composite organization receives, on average, 5,000 alerts every week, and the number grows by 2% each year.

› It takes an analyst, on average, 15 minutes to review an alert.

› The automations built with ThreatConnect Playbooks help the organization reduce the burden on the analysts by 50% in the first year. As the organization introduces more and fine-tunes the current workflow automations, the number increases by 10% every year.

› Seventy percent of the time saved is productive time.

› An analyst’s annual burdened compensation is $100,000.

The efficiency gains from workflow automation will vary with:

› An organization’s commitment to building and using Playbooks for saving time and manual labor.

› Employees’ fully loaded compensation.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $3 million.
### Savings From Automated Triage Of Alerts: Calculation Table

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Number of alerts reported each week</td>
<td>Includes a 2% YoY growth</td>
<td>5,000</td>
<td>5,100</td>
<td>5,202</td>
</tr>
<tr>
<td>A2</td>
<td>Time to manually process alerts (hours)</td>
<td>15 min</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>A3</td>
<td>Percentage of alerts automatically processed in ThreatConnect that no longer require analyst attention</td>
<td>50%</td>
<td>60%</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td>Time saved by processing alerts in ThreatConnect (hours)</td>
<td>A1<em>A2</em>A3*52 weeks</td>
<td>32,500</td>
<td>39,780</td>
<td>47,338</td>
</tr>
<tr>
<td>A5</td>
<td>Analyst hourly rate (rounded)</td>
<td>$100,000/2,080 hours</td>
<td>$48</td>
<td>$48</td>
<td>$48</td>
</tr>
<tr>
<td>A6</td>
<td>Productivity recapture</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>At</td>
<td>Savings from automated triage of alerts</td>
<td>A4<em>A5</em>A6</td>
<td>$1,092,000</td>
<td>$1,336,608</td>
<td>$1,590,564</td>
</tr>
</tbody>
</table>

Risk adjustment: ↓10%

| Atr  | Savings from automated triage of alerts (risk-adjusted) | $982,800 | $1,202,947 | $1,431,507 |

### Savings From Automated Triage Of Phishing Emails

Interviewed organizations described triage to user-reported phishing emails as an important use case for the ThreatConnect Platform. One interviewee received several thousand phishing email notifications every month. Each reported email demanded attention and time from the IT and security teams to determine whether the email was malicious and required further investigation or could be deemed as "false positive." The organization used ThreatConnect to automate the initial email diagnostics, including verification of multiple parameters, such as IP and email addresses or URLs, to prioritize the ones that had a higher likelihood of posing a threat. The analysts then only needed to spend time on the emails that were flagged by ThreatConnect as "risky." One interviewee told Forrester: "When a user reports a legitimate email, instead of me handling it, the automation responds back to that user from ThreatConnect and says, ‘You reported a legitimate email.’ And then, autodeletes it from the system. I don’t even see it. I just get the metrics."

For the composite organization, Forrester assumes that:

- Users report, on average, 750 phishing emails per week.
- Ninety percent of the reported phishing emails are not malicious and should be considered false positive.
- On average, it takes an analyst 10 minutes to review one reported email.
- Fifty percent of the time saved is productive time.
- An analyst’s annual burdened compensation is $100,000.

The efficiency gains from automated triage of the phishing emails will vary with:

- The number of phishing emails reported by users every week.
- The time needed to review a reported email.
The proportion of true phishing emails that would require further investigation post- triage.

The analyst fully loaded compensation.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $252,171.

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>Number of phishing emails reported per week</td>
<td>Includes a 2% YoY growth</td>
<td>750</td>
<td>765</td>
<td>780</td>
</tr>
<tr>
<td>B2</td>
<td>Percent of falsely reported phishing emails that are filtered out by ThreatConnect</td>
<td>60%</td>
<td>70%</td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td>B3</td>
<td>Average time to manually process a phishing email (hours)</td>
<td>10 min</td>
<td>0.17</td>
<td>0.17</td>
<td>0.17</td>
</tr>
<tr>
<td>B4</td>
<td>Analyst hourly rate (rounded)</td>
<td>$100,000/2,080 hours</td>
<td>$48</td>
<td>$48</td>
<td>$48</td>
</tr>
<tr>
<td>B5</td>
<td>Productivity recapture</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Bt</td>
<td>Savings from automated triage of phishing emails</td>
<td>$95,472</td>
<td>$113,612</td>
<td>$132,439</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td>↓ 10%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Btr</td>
<td>Savings from automated triage of phishing emails (risk-adjusted)</td>
<td>$85,925</td>
<td>$102,251</td>
<td>$119,195</td>
<td></td>
</tr>
</tbody>
</table>

Savings From Curating Threat Intelligence Feeds And Identifying Redundant Security Tools

Prior to ThreatConnect, all interviewed companies used multiple security tools and intelligence feeds; however, they lacked a single management interface that would integrate all available security data. In some cases, different security teams within the organizations could unknowingly be using the same software and paying the license fee twice. ThreatConnect provided a single view of the intelligence available to organizations and helped them reassess the use and the value of the software and intelligence feeds, saving costs on redundant or low-value products.

Once the defense company started using ThreatConnect, it found that several units within the organization were subscribed to the same security software through separate independent contracts, which resulted in extra license costs for the organization.

The security infrastructure company found that before ThreatConnect, teams did not coordinate their selection and onboarding of new security tools. “We used to have two to three different teams investigating vendors on their own. And in some cases, even picking competitive vendors. However, it’s cheaper for us if we buy one big license versus two smaller licenses. Now we are saving between 10% and 30% of the costs as the scale discount,” said the director of cybersecurity analytics development.
Several interviewed organizations used ThreatConnect to determine the value of the intelligence feeds they subscribed to and scale back on the use of resources that provided commodity, duplicate, or irrelevant information.

Forrester assumes that:

- After evaluating the quality of the data received from multiple intelligence feeds with ThreatConnect, the composite organization cancels its subscription to one of the resources, saving $50,000 per year.

Savings from curating the intelligence data feeds could differ based on:

- The organization’s effort to identify redundant or inefficient software and intelligence data subscriptions across multiple teams.

- The number and the cost of the subscriptions the organization eliminates as a result of the assessment.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $111,908.

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Savings from curating threat intelligence feeds and identifying redundant security tools</td>
<td></td>
<td>$50,000</td>
<td>$50,000</td>
<td>$50,000</td>
</tr>
<tr>
<td>Ct</td>
<td>Savings from curating threat intelligence feeds and identifying redundant security tools</td>
<td>C1</td>
<td>$50,000</td>
<td>$50,000</td>
<td>$50,000</td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td></td>
<td>↓10%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ctr</td>
<td>Savings from curating threat intelligence feeds and identifying redundant security tools (risk-adjusted)</td>
<td></td>
<td>$45,000</td>
<td>$45,000</td>
<td>$45,000</td>
</tr>
</tbody>
</table>

**Improved Organizational Security**

Before ThreatConnect, the enterprise security teams did not have a “single pane of glass” view of their threat intelligence feeds, often felt overwhelmed by the disparate security tools and data sources, and spent time manually analyzing the incoming alerts. As a result, potentially critical security threats could go uninvestigated and unaddressed longer, exposing the organizations to greater risk. “ThreatConnect provided security teams with the bigger picture view and a better understanding of the threat landscape, so that they can better prioritize the actions they take to defend the enterprise,” said the security intelligence team lead at the financial service organization.

- Automating tasks like context gathering and lookups in ThreatConnect enabled the threat hunting team to offload IOC review to the security intelligence team. “Our hunting team was bogged down with looking at IOCs, but since we moved to ThreatConnect, they have been able to actually hunt for things. That’s a big win for us,” said the security intelligence team lead at the financial service organization.

- The analyst at the healthcare company told Forrester that ThreatConnect had a major impact on the company’s vulnerability management program. Full visibility into the organization’s security landscape allowed the vulnerability management team to identify actively exploited vulnerabilities faster and prioritize addressing them weeks sooner than they would have without ThreatConnect.
With its former tool, the defense company downloaded its IOC report every 24 hours. ThreatConnect allowed the company to report on and triage IOCs every hour, significantly shortening time-to-detection.

For the composite organization, Forrester assumes that:

- The average cost of a security breach is $3.86 million per the 2018 Ponemon Institute survey.\(^5\)
- The average cost of a data breach increases at 6.4% per year.
- With ThreatConnect, the organization takes measures to integrate disparate security technologies, automate workflows, shorten time-to-detection, and enable analysts to focus on proactive work such as threat hunting. As a result, the organization reduces the risk of a breach by 5%.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $407,460.

### Improved Organizational Security: Calculation Table

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>Average cost of a data breach</td>
<td>Increasing at 6.4% per year</td>
<td>$3,860,000</td>
<td>$4,107,040</td>
<td>$4,369,891</td>
</tr>
<tr>
<td>D2</td>
<td>Reduced risk of a breach with ThreatConnect</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dt</td>
<td>Improved organizational security</td>
<td>D1*D2</td>
<td>$193,000</td>
<td>$205,352</td>
<td>$218,495</td>
</tr>
<tr>
<td>Dtr</td>
<td>Improved organizational security (risk-adjusted)</td>
<td>↓20%</td>
<td>$154,400</td>
<td>$164,282</td>
<td>$174,796</td>
</tr>
</tbody>
</table>

### Unquantified Benefits

The companies that Forrester interviewed shared the following benefits from using the ThreatConnect Platform that affected their organizations, but are not quantified in this study:

- **ThreatConnect provided opportunities for collaboration.** Security and threat intel communication was previously facilitated via email, which was inefficient and took a long time. With ThreatConnect Communities, security teams received access to an easy-to-use mechanism for fast information sharing. “We love the way analysts can post and chat, and they like the interface and its simplicity,” said the director of the information sharing and analysis center at the defense company. “Communities have been adopted by a hundred different folks inside the company. So it’s now an established channel they use to spread awareness or share experiences with a broad audience.”
Dashboards and reports helped monitor and evaluate security operations and intelligence. Several interviewed organizations used ThreatConnect dashboards to see in one place what was happening in their environments in real time, whereas previously, gathering the data from multiple sources could take days. Senior leadership looked at dashboards to assess the big picture of the threats faced by the organization and the overall trends in malware. Program managers looked more specifically at the utilization and effectiveness of the ThreatConnect Playbooks to identify opportunities for training and new automations. One director told Forrester: “When I see Playbooks that are underutilized that I think should be used more, I reach out to the business units and say, ‘Do you know about it? How can I make it easier to use? Do you need additional training?’ and that typically solves the issue.”

Better visibility into internal security practices led to user education. The organization that used ThreatConnect to manage user-reported phishing emails identified users who frequently submitted phishing emails that were, in fact, nonmalicious. The organization used Playbooks to automatically reach back out to those users and assign phishing email training to them. As a result, in the course of several years, the organization reduced the number of phishing emails reported by users by more than 60%. At the same time, users became significantly better in identifying and reporting true phishing attempts.

Easy integration with security tools provided a unified view of the security technology stack. Each interviewed organization used a variety of security technologies provided by different vendors. Before ThreatConnect, the tools did not exchange the data with each other or have a shared management interface. Interviewed organizations have found it easy to onboard new security tools onto the ThreatConnect Platform. One interviewee said: “We run the gamut, and that’s what I liked about ThreatConnect. It’s got really good integrations with a lot of great products that we’ve been picking up on.”

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 ThreatConnect and later realize additional uses and business opportunities, including:

Expanding the use of automation and orchestration to incident response. All interviewees talked about the benefits of automating workflows to identify threats and discussed plans for new Playbooks. One of the areas where organizations expect to see additional benefits is through new automations when incidents occur.

“It is intangible, but ThreatConnect brings the analysts together where they can see and chat with each other, breaks down the walls. I measure by the number of posts I see each month. It makes us a closer-knit community. We don’t talk on the phone often enough with the analysts, but I’d say there’s some pretty spirited communication going on inside the posts.”

Director, information sharing and analysis center, defense

As a result of user education enabled by ThreatConnect, one organization reduced the number of phishing emails reported by users by over 60%, while increasing the accuracy of reports.
Building a connected security organization. Several interviewees described security teams within their organizations as being siloed, following inconsistent processes, duplicating efforts, and sometimes using redundant tools. ThreatConnect provided organizations’ leadership with a unified view of the security environment and inspired organizationwide initiatives aimed at getting alignment on security processes and collaboration across teams. The security intelligence team lead at the financial company said, “ThreatConnect brought everyone together and reminded us about the ‘one-team-one-fight mentality’ where before, it was easier to be in silos, not because people were hoarders, but because we didn’t have an environment.”

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

<table>
<thead>
<tr>
<th>REF.</th>
<th>COST</th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
<th>TOTAL</th>
<th>PRESENT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Etr</td>
<td>Software fees</td>
<td>$0</td>
<td>$170,000</td>
<td>$170,000</td>
<td>$170,000</td>
<td>$510,000</td>
<td>$422,765</td>
</tr>
<tr>
<td>Ftr</td>
<td>Implementation and training</td>
<td>$52,382</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$52,382</td>
<td>$52,382</td>
</tr>
<tr>
<td>Gtr</td>
<td>Cost of work performed in ThreatConnect</td>
<td>$0</td>
<td>$166,100</td>
<td>$166,100</td>
<td>$166,100</td>
<td>$498,300</td>
<td>$413,066</td>
</tr>
<tr>
<td></td>
<td>Total costs (risk-adjusted)</td>
<td>$52,382</td>
<td>$336,100</td>
<td>$336,100</td>
<td>$336,100</td>
<td>$1,060,682</td>
<td>$888,213</td>
</tr>
</tbody>
</table>

Software Fees

For the composite organization, the annual price of ThreatConnect amounts to $170,000. Software fees depend on a variety of factors and will change based on specific organizational needs. For more information regarding the ThreatConnect Platform pricing, please contact your ThreatConnect representative.

Forrester did not risk-adjust this cost because it was provided for the composite organization by ThreatConnect. The three-year risk-adjusted total PV is $422,765.

Software Fees: Calculation Table

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>ThreatConnect license fee</td>
<td></td>
<td>$170,000</td>
<td>$170,000</td>
<td>$170,000</td>
<td></td>
</tr>
<tr>
<td>Et</td>
<td>Software fees</td>
<td>E1</td>
<td>$0</td>
<td>$170,000</td>
<td>$170,000</td>
<td>$170,000</td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td></td>
<td>0%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etr</td>
<td>Software fees (risk-adjusted)</td>
<td></td>
<td>$0</td>
<td>$170,000</td>
<td>$170,000</td>
<td>$170,000</td>
</tr>
</tbody>
</table>

Implementation And Training

Interviewed organizations described ThreatConnect implementation as a gradual process that required:

- Involvement from different groups, including DBAs, network specialists, and security team members for a duration ranging from one week to several months.
- A flat implementation fee paid to ThreatConnect.

For the composite organization, Forrester assumes:

- The implementation takes one month.
- A cross-functional team of DBAs, network specialists, and security team members is involved in the implementation; they dedicate 30% of their time to the related activities.
The average burdened annual salary for the cross-functional team is $112,000.

To equip the composite organization with the necessary knowledge about the platform, ThreatConnect delivers training to five key users. The training costs the organization $20,000 and takes four days to complete.

The cost of training and implementation will vary based on:

- The complexity of the existing security landscape and the team’s dedication to implementation activities.
- The number and salaries of FTEs involved in implementation.
- The number and salaries of the FTEs who need to be trained to use ThreatConnect.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $52,382.

### Implementation And Training: Calculation Table

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Installation and implementation fee</td>
<td>$5,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F2</td>
<td>Implementation time (months)</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F3</td>
<td>Number of cross-functional FTEs involved in implementation</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F4</td>
<td>Percent of FTEs’ time dedicated to ThreatConnect implementation</td>
<td>30%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5</td>
<td>FTEs’ average burdened monthly salary (rounded)</td>
<td>$112,000/12 months $9,333</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F6</td>
<td>Training fee</td>
<td>$20,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F7</td>
<td>Number of FTEs trained on ThreatConnect</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F8</td>
<td>Time to train the platform owners (days)</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F9</td>
<td>Platform owners’ average burdened daily rate (rounded)</td>
<td>$112,000/260 $431</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fₜ</td>
<td>Cost of implementation and training</td>
<td>(F₁+(F₂<em>F₃</em>F₄*F₅)<em>F₆+(F₇</em>F₈))</td>
<td>$47,620</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td>↑10%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fₜᵣ</td>
<td>Cost of implementation and training (risk-adjusted)</td>
<td>$52,382</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
</tbody>
</table>

### Cost Of Ongoing Work Performed In ThreatConnect

Interviewed organizations dedicate comparable resources to the ongoing platform management. Based on the interviews, Forrester assumes for the composite organization:

- Two developers spend 50% of their time building automations in ThreatConnect.
- A developer’s annual burdened salary is $91,000.
Two director-level security professionals dedicate, on average, 20% of their time to analyzing data within ThreatConnect, planning the automation road map, and building reports for senior management.

An average senior security professional’s annual burdened compensation is $150,000.

The costs will vary based on:

- The organization’s need for new and improved workflow automations and the number of developers building them.
- Senior security professionals’ interest in using ThreatConnect for reporting, further automation, and new initiatives.
- Annual compensation for developers and senior security team members.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $413,066.

### Cost Of Ongoing Work Performed In ThreatConnect: Calculation Table

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>Number of developers building new automations with ThreatConnect</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G2</td>
<td>Percent of developers’ time dedicated to ThreatConnect</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G3</td>
<td>Developer average burdened annual salary</td>
<td>$91,000</td>
<td>$91,000</td>
<td>$91,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G4</td>
<td>Number of senior security/operations professionals working in ThreatConnect</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G5</td>
<td>Percent of senior staff’s time dedicated to ThreatConnect</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G6</td>
<td>Senior security professionals’ annual burdened salary</td>
<td>$150,000</td>
<td>$150,000</td>
<td>$150,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gt</td>
<td>Cost of work performed in ThreatConnect</td>
<td>G1*G2*G3+G4*G5*G6</td>
<td>$0</td>
<td>$151,000</td>
<td>$151,000</td>
<td>$151,000</td>
</tr>
<tr>
<td>Gtr</td>
<td>Cost of work performed in ThreatConnect (risk-adjusted)</td>
<td>↑10%</td>
<td>$166,100</td>
<td>$166,100</td>
<td>$166,100</td>
<td></td>
</tr>
</tbody>
</table>
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 Table (Risk-Adjusted)**

<table>
<thead>
<tr>
<th></th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
<th>TOTAL</th>
<th>PRESENT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total costs</td>
<td>($52,382)</td>
<td>($336,100)</td>
<td>($336,100)</td>
<td>($336,100)</td>
<td>($1,060,682)</td>
<td>($888,213)</td>
</tr>
<tr>
<td>Total benefits</td>
<td>$0</td>
<td>$1,268,125</td>
<td>$1,514,479</td>
<td>$1,770,498</td>
<td>$4,553,102</td>
<td>$3,734,677</td>
</tr>
<tr>
<td>Net benefits</td>
<td>($52,382)</td>
<td>$932,025</td>
<td>$1,178,379</td>
<td>$1,434,398</td>
<td>$3,492,420</td>
<td>$2,846,464</td>
</tr>
<tr>
<td>ROI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>320%</td>
</tr>
</tbody>
</table>
The ThreatConnect Platform: Overview

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

Intelligence, Automation, Analytics, And Workflows In A Single Platform

With ThreatConnect, you are able to centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness all in one place.

Make your security operations and analysts more efficient, while providing real-time insights to security leaders to make better business decisions.

With ThreatConnect’s intelligence-driven security operations platform, your team has the ability to leverage threat intelligence, automation, and orchestration directly from one platform. Automation or orchestration informed by threat intelligence makes your preexisting technology investments and your entire security team — including security operations and incident response — more efficient and more effective.

ThreatConnect enables you to gain visibility into threats and understand their relevance to your organization, as well as increase efficiency with automation, task management, and orchestration. With ThreatConnect, every member of your security team — including leadership — benefits from using the same platform. A centralized system of record, ThreatConnect can measure the effectiveness of your organization with cross-platform analytics and customizable dashboards.

Product Capabilities

✓ Collaborate with other users in Common Community
✓ Query indicators and reports from 100+ OSINT sources and industry blogs
✓ Export intel as PDFs or Signatures
✓ Automate with Playbooks
✓ Create and manage your own intelligence
✓ Validate “on-the-ground” threats with CAL™ data
✓ STIX/TAXII support
✓ Integrations with premium feed providers
✓ Automated email import and triage
✓ Incident, task, and workflow management
✓ Custom dashboards
✓ User access management
✓ Build custom applications with our App Builder, SDK, and App Framework
✓ Connect your tools via API or Playbooks
✓ Measure ROI and other metrics
✓ Advanced Quality of Service and scaling options
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

3 A ThreatConnect Community is a tightly administered group of ThreatConnect users. A Community can be designated as either Private or Public depending on the purpose of the Community. Members can contribute intelligence to the Community, vote on indicator ratings, and have collaborative discussions. Oftentimes a Community will rally around a common purpose, such as an industry sector, a current event, or a geopolitical region.