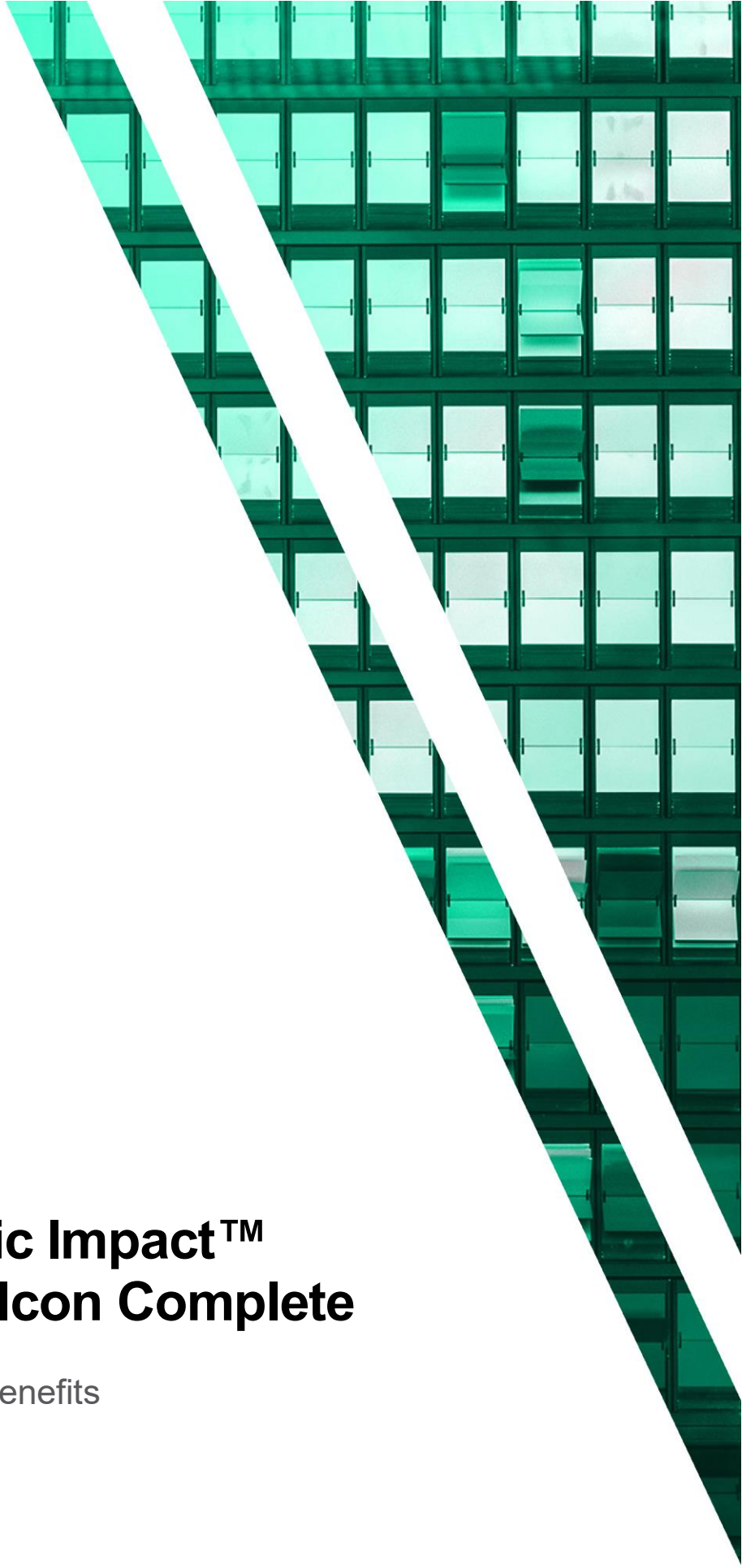
FORRESTER®



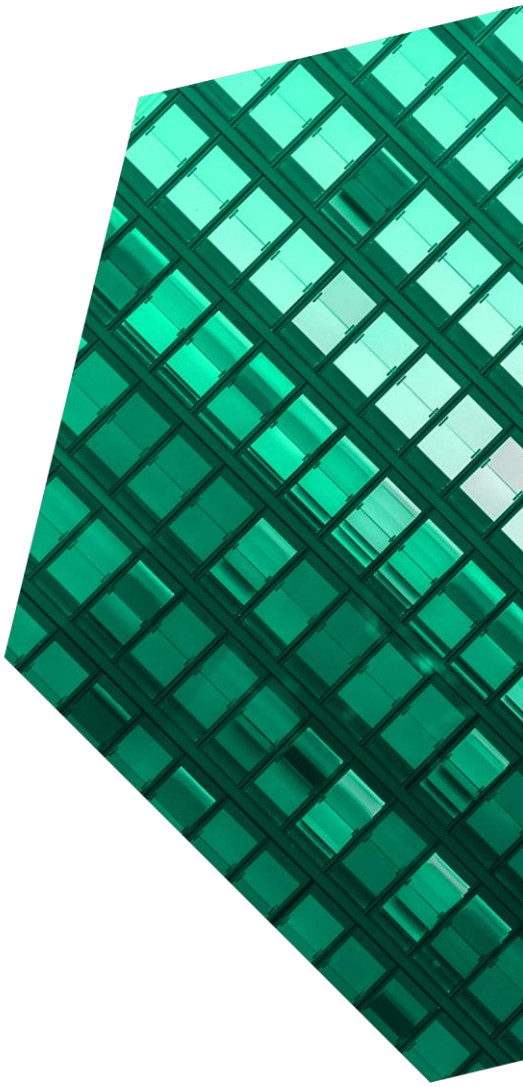
The Total Economic Impact™ Of CrowdStrike Falcon Complete

Cost Savings And Business Benefits Enabled By Falcon Complete

FEBRUARY 2021

Table Of Contents

Consultant Team: Gerry Pape



Executive Summary

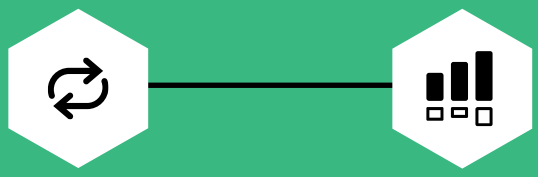
Falcon Complete is a fully managed cybersecurity endpoint protection service that monitors, detects, prevents, and remediates possible breaches and intrusions. Staffed 24/7/365 by CrowdStrike analysts with years of experience using the Falcon Enterprise suite of security modules, Falcon Complete is highly effective at stopping intrusions and reducing risk, while eliminating many of the ever-increasing challenges and burdens of building, staffing, and maintaining your own security operations center.

CrowdStrike commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying CrowdStrike's fully managed endpoint protection service Falcon Complete. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Falcon Complete on their organizations. The CrowdStrike Falcon Complete solution provides full protection of endpoints, minimizes security risk, and solves the problems and burdens of building, staffing, and maintaining your own security operations center (SOC).

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with experience using Falcon Complete. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

Prior to using Falcon Complete, the customer's typical previous state was an assortment of tools and vendor products deployed inconsistently across various divisions and locations of the company. This lack of a coordinated approach to security left the company, its customers, and its partners exposed to threats. Existing tools were sometimes effective at generating security alerts when intrusions occurred, but the fragmented security silos and low staffing levels meant that the security teams were not always able to investigate and respond quickly and consistently.

KEY STATISTICS



Return on investment (ROI)
403%

Net present value (NPV)
$5.81M

In some cases, critical alerts were left unaddressed until after the damage was done, despite the best efforts of security teams. These limitations led to breaches and ransomware attacks. Recovery was expensive, including replacing or reimaging devices. In the worst-case scenario, these intrusions caused business shutdowns, lost revenue, increased audits, and loss of credibility with the company's partners and customers.

After the investment in Falcon Complete, the customers reported full confidence in CrowdStrike and the Falcon Complete team to protect, prevent, and quickly remediate any intrusions. There was generally minimal need for internal resources to work on cybersecurity issues. There was trust and peace of mind that comes with a trusted supplier/partner, and as one customer shared, they were, "100% happy with Falcon Complete."

> **“I’ve looked at a number of them. Falcon Complete is the most complete security model I’ve seen.”**
>
> — CISO, building products

Key results from the investment in Falcon Complete include the savings of: not needing to build a fully staffed SOC; the reduced risk of a data breach; sunsetting redundant tools; the reduced number of security incidents; and more favorable cyberinsurance terms and conditions. The NPV of the Falcon Complete solution over a three-year period for this study exceeded $5.81 million.

KEY FINDINGS

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

- **Operational efficiencies and augmentation of security operations.** Falcon Complete significantly increased the coverage, responsiveness, and overall effectiveness of the interviewed company’s cybersecurity efforts. In more than one instance, customers shared that Falcon Complete not only was effective in augmenting their existing security team, but that it also was able to eliminate the need to build a fully staffed SOC. The customers of CrowdStrike frequently reported they did not have the time or capital budget to build a SOC given the constant threats they were facing. The net benefit of just the salaries required to staff an in-house SOC team with security analysts and threat hunters on a 24/7 basis was a risk-adjusted, three-year PV of over $4.1 million.
- **Reduced risk of data breaches.** Falcon Complete delivered the interviewed organizations superior protection with no major breaches and full remediation of any infected devices. None of the interviewed organizations experienced a single significant intrusion over the course of their engagement with Falcon Complete. In most cases, remediation took place by the Falcon Complete team before the device owner was even aware of a problem. The composite organization of 7,000 employees has an average breach cost of $4.7 million and a one-year breach probability of nearly 15%. This provides a three-year, risk-adjusted benefit of more than $1.5 million.

- **Elimination of redundant and unneeded cybersecurity tools.** Prior to Falcon Complete, the customers had various security providers and an assortment of security tools spread across the enterprise by location and by company business unit. At best, these tools identified possible threats. But they provided little support in identifying real versus false positive threats and minimal assistance with remediation. With Falcon Complete, the composite organization was able to eliminate license fees, associated security tool costs, and IT support to manage these tools and vendors for a risk-adjusted, three-year PV of more than $1 million.

Equivalent staff coverage per year

More than $1.5M

- **Savings attributed to reduction in security incidents.** The interviewed organizations shared that an infected and therefore inoperable device greatly impacted worker productivity. On-site desktop users could experience downtime that lasts one day, while remote laptop users could be negatively impacted by as much as three days. Falcon Complete greatly reduced the incidents of infected and inoperable desktops and laptops. For the composite organization, the reduced worker downtime, along with the reduction in necessary IT resources for remediation, resulted in a three-year, risk-adjusted PV of over $320K. Since remote users typically have longer remediation times for their infected devices, and the COVID-19 pandemic has created the need for more remote workers, the savings due to Falcon Complete's track record of reduced security incidents should increase appreciably.
- **Savings on cyberinsurance.** Falcon Complete includes a Breach Prevention Warranty that covers breach response expenses if there is a security incident within the environment protected by Falcon Complete. This CrowdStrike warranty, as well as the recognized excellent protection afforded by CrowdStrike, assisted the interviewed organizations with savings due to preferred terms and conditions for their cyberinsurance. For the composite organization, these savings amounted to an average of $90K per year and a three-year, risk-adjusted total PV of over $200K.

Unquantified benefits. Benefits that are not quantified for this study include:

- **The confidence, trust, and peace of mind in CrowdStrike and Falcon Complete.** The interviewed customers were consistent in their praise of CrowdStrike and the endpoint protection that Falcon Complete provides. Typical comments included:
    - "[Falcon Complete] lets me sleep far better at night."
    - "They've got my back."
    - "Falcon Complete gives me that confidence."

  These were just a few of the many compliments shared during the four customer interviews. Confidence, trust, and peace of mind are difficult to quantify in dollar terms, but they were abundantly clear for the interviewed customers.
- **Ability to focus on other strategic IT initiatives and activities.** Falcon Complete gave customers the assurance that endpoint security was fully covered and needed little if any oversight. This gave customers the ability and availability to easily direct their IT resources to other IT priorities and projects.
- **Falcon Complete eliminates the need to manage turnover, staffing, and training of**

your own cybersecurity analysts. Previously, it was mentioned that Falcon Complete allows organizations to save upwards of $4 million in not having to staff an in-house SOC. Additionally, and though this was not quantified, Falcon Complete eliminates the challenges and costs associated with turnover, subsequent hiring, and the initial/ongoing training of analysts.

> CrowdStrike Falcon Complete consistently offers customers peace of mind and confidence in protection, prevention, and remediation.

- **Near immediate implementation with little cost or risk.** The interviewed customers spoke of near immediate implementation, minimal involvement, and no known issues in the rollout of the CrowdStrike agent on all endpoints. One customer stated, “The actual onboarding was ridiculously easy, and the guys were ridiculously easy to deal with.” This ease in onboarding not only applied to the initial implementation but also to the protection of additional endpoints. In one instance, this unquantified benefit was especially important for merger and acquisition activities.
- **Accurate inventory of all endpoints.** One of the challenges of managing any large corporate network is having an accurate inventory of all the attached devices. In the rollout of loading a single lightweight agent to all devices, CrowdStrike was able to quickly identify those endpoints the customers were unaware of and to immediately bring them into the protected state.
- **A single lightweight agent for all endpoints globally.** The Falcon Complete agent operates without constant signature updates or on-premises infrastructure management. This reduces the burden of open network management and minimizes CPU utilization.

Costs. Risk-adjusted PV costs include:

- **Falcon Complete annual license fees.** For the composite organization, which has 7,000 employees and their associated endpoints, the three-year, risk-adjusted PV was $1.37 million. Falcon Complete pricing is an annual fee based on the total number of protected endpoints.
- **Implementation and administration costs.** The interviewed organizations shared that there was minimal implementation and ongoing support needed. Over the three-year period, this support model reflected modest costs of $72K.

The customer interviews and financial analysis found that a composite organization experiences benefits of $7.25M over three years versus costs of $1.44M, adding up to a NPV of $5.81M and an ROI of 403%.

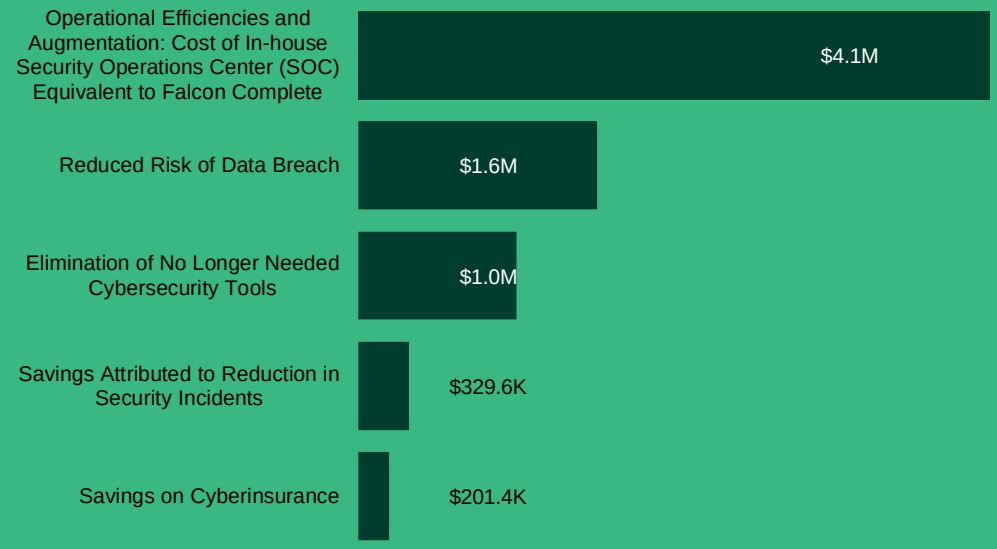
ROI
403%

BENEFITS PV
$7.25M

NPV
$5.81M

PAYBACK
<3 months

Benefits (Three-Year)



> **"I see CrowdStrike Falcon Complete as being a permanent member of my capability."**
> *CISO, building products*

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 Falcon Complete.

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 Falcon Complete can have on an organization.

DUE DILIGENCE

Interviewed CrowdStrike stakeholders and Forrester analysts to gather data relative to the Falcon Complete.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using the Falcon Complete to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

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

The CrowdStrike Falcon Complete Customer Journey

Drivers leading to the Falcon Complete investment

Interviewed Organizations

Industry	Region	Interviewee	Endpoints Managed By CrowdStrike Falcon Complete
Pharmaceuticals	Global – US HQ	Senior director for security operations	22,500
Building products	Europe – UK HQ	Chief information security officer (CISO)	7,700
Infrastructure	Australia/New Zealand	Head of security and risk	4,500
Transportation	Global – US HQ	VP of IT	700

KEY CHALLENGES

Before implementing Falcon Complete, the interviewed customers had multiple tools that identified possible threats and engineered some prevention mechanisms in place. But these tools and procedures were not consistent across the enterprise, leaving a patchwork of protection strategies by region and business unit. Limited IT staff was not able to provide 24/7 monitoring and hunting for any possible threats or intrusions the companies were experiencing. There was limited remediation support provided by the vendors of the tools when a threat or breach was identified. In one case, a ransomware attack had greatly impacted a specific region of the enterprise, limiting business operations for several months.

The interviewed organizations struggled with common challenges, including:

- **Limited staff in size and skills to support cybersecurity threats and activities.** The interviewed customers were limited in both their IT headcounts and staffs' skill sets to properly monitor and act on threats and possible breaches. In most cases, companies were very cost-conscious and averse to adding additional costs. It was equally challenging to provide the necessary training to keep skill sets current with the increasing sophistication of threats and intrusions.
- **Inconsistent and multiple cybersecurity strategies across the enterprise.** The interviewees were brought into their positions to manage the overall corporate cybersecurity effort of their companies. However, these responsibilities did not always include direct budget control of the staff whose responsibility it was to support the security platforms and tools — budgets and staff were under the control of the specific business unit or region. Matrix and dotted-line reporting structures were set up where possible, but even those frameworks still left gaps in security coverage, protection, and remediation.

> **"I am totally confident in their ability to remediate and their ability to respond."**
>
> *VP of IT, transportation*

- **The volume of threats to investigate and the complexity of the threats were increasingly beyond the legacy tools.** Even with tools and staff to monitor and manage possible threats and breaches, the interviewed customers were finding gaps in coverage. The number of threats which needed to be investigated were regularly increasing. The complexity and sophistication of the breaches were outstripping the ability of the legacy security tools to identify and quarantine the threats. These conditions were putting the interviewed leaders of risk and security in very uncomfortable and tenuous positions.
- **Limited time to implement a corporatewide cybersecurity strategy.** With the inadequate and in many cases inconsistent security tools across the organizations, there was a need to quickly roll out a new strategy. There were too many instances of infected or locked out devices that were impacting worker productivity, plus there was the threat of a major breach such a ransomware attack. Once a decision was made on a new security strategy, implementation of that strategy needed to be done efficiently and effectively.

"Falcon Complete is hands down the best product I've ever seen. I'll fight for it."

Senior director for security operations, pharmaceuticals

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewed organizations searched for a solution that could provide:

- A consistent cybersecurity platform across the entire enterprise.
- A fully managed 24/7/365 service to close the gaps in security coverage and eliminate the need to build an in-house SOC.
- A security solution that could be implemented quickly and without creating device and network performance issues.
- A security solution that would require minimal oversight and support from existing IT staff.

While most of the interviewed leaders looked at alternatives to what CrowdStrike offered, the interviewed leaders found that CrowdStrike Falcon Complete offered clear advantages to other options. Therefore, there was not competitive bidding involved in the selection of Falcon Complete for the four interviewed customers.

There were some specific solution requirements that were noteworthy in the selection of Falcon Complete.

- In one case, CrowdStrike was brought in on an emergency basis to remediate a serious breach. This was handled so well that the company contracted with CrowdStrike to provide Falcon Complete across the entire enterprise as their security standard.
- In one instance, one of the interviewed customers proceeded with caution in rolling out Falcon Complete by region over several weeks. Even though the rollout was proceeding without incident, one of the regions yet to implement Falcon Complete had a serious breach and the regional business unit incurred substantial losses. It was clear to the security and risk leader that Falcon Complete would have prevented this breach had it been implemented before the intrusion. After that incident, there were no further delays in the deployment, and Falcon Complete was rolled out immediately to all regions and endpoints.

- In another case, Falcon Complete replaced another managed services cybersecurity provider. Falcon Complete was lower in cost compared to the existing service provider, and it provided full remediation of possible breaches that the exiting provider did not provide.

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 companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global, multibillion dollar business organization provides sales of goods and services serving various industries and markets. Like many global and multinational companies, the composite organization has a strong presence in some markets for certain products it sells, while in other markets the composite company is stronger in the services it provides. It is decentralized in its business approach and allows general autonomy to its business units and regional operations. This autonomy and independence have created a fragmented approach to security and repeated cybersecurity breaches and attempted threats. These conditions plus one notable and damaging ransomware attack have led to the need and implementation of improved defenses and an enterprisewide security strategy.

Deployment characteristics. Falcon Complete was deployed globally in a matter of days, providing coverage for devices for 7,000 employees and 7,500 endpoints. The composite organization has been a user of Falcon Complete for 18 months.

Key assumptions

- **Protects 7,000 employees and 7,500 endpoints**
- **Has been a Falcon Complete customer for 18 months**
- **Manages security operations worldwide**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Operational efficiencies and augmentation: cost of in-house SOC equivalent to Falcon Complete	$1,584,000	$1,663,200	$1,746,360	$4,993,560	$4,126,612
Btr	Reduced risk of data breach	$628,704	$628,704	$628,704	$1,886,112	$1,563,494
Ctr	Elimination of redundant cybersecurity tools	$414,000	$415,620	$417,264	$1,246,884	$1,033,348
Dtr	Savings attributed to deduction in security incidents	$131,760	$132,570	$133,392	$397,722	$329,563
Etr	Savings on cyberinsurance	$81,000	$81,000	$81,000	$243,000	$201,435
	Total benefits (risk-adjusted)	$2,839,464	$2,921,094	$3,006,720	$8,767,278	$7,254,452

OPERATIONAL EFFICIENCIES AND AUGMENTATION: COST OF IN-HOUSE SOC EQUIVALENT TO FALCON COMPLETE

Evidence and data. Companies are responsible for protecting their data and maintaining a secure and stable operating environment. They need to defend themselves from increasingly complex and sophisticated threats, especially those that are advanced enough to remain hidden from security technologies. Firms need to provide that protection across the enterprise regardless of business unit divisions or country boundaries. With the interconnectedness of business, companies also need security solutions that provide protection for their customers, suppliers, and partners. With merger and acquisition activities, the challenges of providing security protection among moving corporate pieces increases even greater.

Given these responsibilities, the following is a summary of the feedback that led to the selection of Falcon Complete versus the build out of an in-house SOC.

- The interviewees were operating with limited staffs, limited budgets, and restrictions on adding costs. In most cases, adding staff was not a likely option. Without 24/7 staff coverage, off-hours operations were left vulnerable to security intrusions and attacks, yet the interviewed customers were charged with enterprisewide cybersecurity prevention and protection. One interviewed leader estimated it would cost more than $1 million per year to add additional staff for a fully operational SOC. Falcon Complete eliminated the need to add additional staff and build a 24/7 fully operational SOC. Falcon Complete not only took those challenges off the table but it also freed up resources to, in the words of one interviewee, “Allow me to focus on other things.”

- It was brought up by the interviewed customers that they were pressed to provide cybersecurity protection in a timely manner. In one instance, the customer was working to recover from a damaging intrusion, and they needed to quickly get all users back to normal operations. Customers needed a much quicker response than expanding any existing SOC capabilities. They found the rollout and implementation of Falcon Complete to be simple and quick. As one security leader shared, "The actual onboarding was ridiculously easy."
- One customer had a major breach, but they did not have the staff nor the tools to remediate the intrusion. They called upon CrowdStrike to provide them remediation. The success of that remediation led to the contracting of ongoing managed support by Falcon Complete.

> **"The biggest positive is not only keeping the business safe but allowing the business to carry on without actually noticing any actions being taken to stop the threat."**
>
> *Head of security and risk, infrastructure*

- Two of the interviewed customers had various legacy security tools for monitoring, protection, and vendor support when called upon. But there was little evidence of prevention measures achieved by these vendor support models. Remediation often took an extended amount of time to be achieved, which affected worker productivity. The standard procedure was to quarantine a device and then address the issue, causing user downtime. Falcon Complete — as a fully managed service with round-the-clock support — provided prevention, transparent remediation when needed, and the elimination of user downtime.

Modeling and assumptions. The alternative to Falcon Complete would be to staff an on-site SOC with the following typical capabilities:

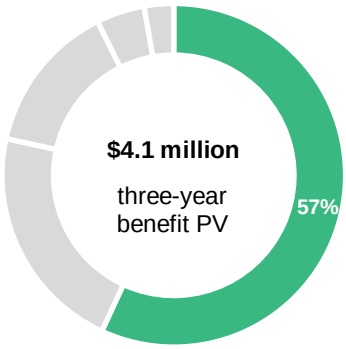
- Global monitoring and response as well as proactive threat hunting on a 24/7/365 basis.
- Support and follow-up investigative actions.
- Full remediation and recovery of systems involved in incidents.
- Platform management and tuning.

When considering a 24/7/365 operation for the composite organization, the SOC staffing model involves five security analysts/responders, five threat hunter specialists, and one supervisor. This staffing level provides the minimum staffing necessary for round-the-clock coverage of security analysis/response and threat hunting. The average fully loaded salary used for a fully trained and competent cybersecurity specialist is $160,000 per year.

Risks. Potential risks can negatively impact benefit categories. Specifically, organizations may realize the following risks:

- The staffing of a SOC could require fewer FTEs than the previously mentioned 10 security specialists and one supervisor.
- The average fully loaded salary of SOC staff could be different than $160,000.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $4,126,612.



Operational Efficiencies And Augmentation: Cost Of In-House SOC Equivalent To Falcon Complete

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	SOC staffing equivalent to Falcon Complete coverage	Composite	11	11	11
A2	Fully loaded salary of SOC staff w/ 5% annual increase	Assumption	$160,000	$168,000	$176,400
At	Operational efficiencies and augmentation	A1*A2	$1,760,000	$1,848,000	$1,940,400
	Risk adjustment	↓10%			
Atr	Operational efficiencies and augmentation (risk-adjusted)		$1,584,000	$1,663,200	$1,746,360
	Three-year total: $4,993,560			**Three-year present value: $4,126,612**	

REDUCED RISK OF DATA BREACH

Evidence and data. The interviewed customers had many experiences with intrusions and breaches prior to the implementation of Falcon Complete. In one case, there was a ransomware attack that had serious negative consequences to a regional business for many months. In other cases, employees were essentially shut down and unable to work if their laptop or desktop was infected. Customers found this was especially troublesome with remote workers who could be out of work by as much as three days until the problems were identified, fixed, or a replacement laptop was sent to them. Two of the interviewed customers spoke of intrusions that not only impacted their own operation but had negative consequences for their customers and partners as well. There were immediate negative impacts on cost and reputation along with the required costs of partner/customer audits and reviews.

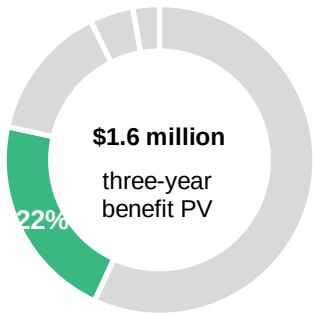
The demands placed on the heads of security and risk were not just to fix and remediate any breach in a timely manner, but to prevent any intrusions and negative impacts to operations and individual worker productivity. Falcon Complete met and exceeded the demands of the business and the requirements of the interviewed customer leaders by providing full remediation and recovery of systems involved in intrusions. As the head of security and risk for one of the customers shared, “The biggest positive with Falcon Complete is not only keeping the business safe but allowing the business to carry on without actually noticing actions being taken to stop a threat.” As another customer relayed, “With Falcon Complete, the problems we had before seemed to just disappear.”

Modeling and assumptions. Reducing the number and severity of breaches saves the composite organization from costly clean-up and recovery, payments of ransomware, and loss of reputation with customers, partners, and even suppliers.

- According to the Ponemon 2020 Cost of a Data Breach report, the average cost of a breach for the 7,000-employee composite organization is $4.72 million.[1]
- Additionally, the probability of a breach over a two-year period, as noted by the Ponemon 2019 Cost of a Data Breach report, is 29.6%.[2]
- The average cost of a data breach by the security automation that Falcon Complete provides would normally give a calculated average reduction in risk of 59.4% per the 2020 Ponemon Report. But with CrowdStrike’s Breach Prevention Warranty, this reduction in risk factor is covered by the warranty leaving only the average cost of a breach and the two-year probability as factors.

Risks. Potential risks can negatively impact benefit categories. Specifically, organizations may realize the following risks:

- Due to the sophistication and increasing number of threats over time, the total costs of a breach will vary by business and region.
- The probability of a breach will be subject to change as new threats emerge and new levels of detection, prevention, and remediation are built.
- The percent reduction in risk will also vary with the effectiveness of the legacy solution and the ability for the solution to adapt and change to meet new types of threats.



To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1,563,494.

Reduced Risk Of Data Breach					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Average cost of breach for 7,000-employee organization	Ponemon	$4,720,000	$4,720,000	$4,720,000
B2	Probability of breach over two-year period	Ponemon; 29.6%/2	14.8%	14.8%	14.8%
Bt	Reduced risk of data breach	B1*B2	$698,560	$698,560	$698,560
	Risk adjustment	↓10%			
Btr	Reduced risk of data breach (risk-adjusted)		$628,704	$628,704	$628,704
	Three-year total: $1,886,112		**Three-year present value: $1,563,494**		

ELIMINATION OF REDUNDANT CYBERSECURITY TOOLS

Evidence and data. With the implementation of Falcon Complete, the interviewed customers reported they were able to eliminate nearly all the prior security tools. The previous tools were not seen as effective as the fully managed service of Falcon Complete. In all cases, the interviewees were able to eliminate license fees, monitoring stations, and other vendor costs associated with security. In one case, a customer initially kept some of the original security tools and monitoring stations, but they soon found the company's prior security tools, support, and strategies to be redundant and ineffective. All the original tools and costs were eliminated.

Staff costs associated with managing endpoint security were also greatly reduced. The customers were able to deploy these resources to other projects and IT priorities. In one instance, the interviewed head of security shared that they had no staff assigned to managing their CrowdStrike solution. This individual was the primary point of contact to CrowdStrike, reviewed any reporting, and was generally available for calls or meetings with the CrowdStrike account team.

Three-year savings from eliminating other security tools

Greater than $1M

The overall response from the interviewed customers can be best summed up with the following feedback: "I'm trying to find some downsides to Falcon Complete. I'm just finding it hard to give you another impression."

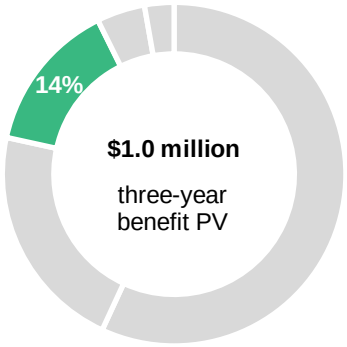
Modeling and assumptions. Based on the experiences and feedback from the interviewed customers, these are the assumptions for elimination of redundant security services:

- Savings from elimination of license fees and software charges result in $300,000 per year.
- Redundant monitoring stations and other hardware costs are $40,000 annually.
- Savings of IT staff support for the previous sets of security tools and processes is modeled as one fully loaded FTE at $120,000 with annual increases of 1.5%.

Risks. Potential risks can negatively impact benefit categories. Specifically, organizations may realize the following risks:

- The sophistication and complexity of new threats may require additional tools and surveillance in other points of a company's IT infrastructure.
- Requirements from interconnected customers, partners, or suppliers may require additional security tools and processes.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1,033,348.



Elimination Of Redundant Cybersecurity Tools

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Elimination of redundant license fees and software	Composite	$300,000	$300,000	$300,000
C2	Elimination of monitoring stations and other hardware tools	Composite	$40,000	$40,000	$40,000
C3	Elimination of one FTE for various cybersecurity tools w/ 1.5% annual salary increase	$120K	$120,000	$121,800	$123,627
Ct	Elimination of redundant cybersecurity tools	C1+C2+C3	$460,000	$461,800	$463,627
	Risk adjustment	↓10%			
Ctr	Elimination of redundant cybersecurity tools (risk-adjusted)		$414,000	$415,620	$417,264
	Three-year total: $1,246,884			**Three-year present value: $1,033,348**	

SAVINGS ATTRIBUTED TO REDUCTION IN SECURITY INCIDENTS

Evidence and data. Endpoint security tools typically identify an issue and require infected devices to be returned to IT to be cleaned and reimaged. In some cases, infected devices could be isolated and remotely fixed. But all of this takes time and results in user downtime and lost productivity. As reported by one of the interviewed customers, some remote workers with laptops could lose as much as three days with contacting the help desk, getting to the appropriate location to receive a replacement, and then going through the setup procedures for the laptop. This same customer shared that on-site desktop users could experience as much as one day of user downtime.

Average annual savings from prevented downtime:

$140,000

Infected devices not only impacted worker productivity but they also put a strain on the IT resources needed to deal with all the issues of an infected device. Isolating an infected device,

replacing, and reimaging devices, maintaining device inventory, and shipping were some of the issues mentioned by the interviewees.

All the interviewed customers provided feedback that Falcon Complete eliminated the occurrences of device infections. They reported the Falcon Complete suite of services — which included 24/7 monitoring, threat identification, prevention, and remediation — was transparent to users. CrowdStrike's remediation processes proved capable of eradicating threats without cumbersome device reimaging or replacement. Since the deployment of Falcon Complete, more than one interviewed customer could not remember a time when an endpoint device was infected and needed replacement.

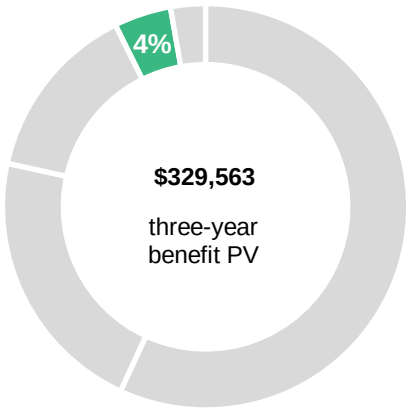
Modeling and assumptions. Based on the information gathered from the interviews, the composite organization is as follows:

- There are on average 18 fewer devices infected and needing remediation per month.
- The average worker downtime and lost productivity per incident is 8 hours.
- The average hourly rate for a worker is $50.
- Fifty percent of one FTE, with a fully loaded salary of $120,000, was saved with the elimination of infected devices.

Risks. Potential risks can negatively impact benefit categories. Specifically, organizations may realize the following risks:

- The average worker's salary will vary.
- The average time it takes for IT to address an infected device and provide the user with a fully operational replacement.
- The prior solution's level of endpoint protection.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $329,563.



Savings Attributed To Reduction In Security Incidents					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
D1	Reduction in worker devices infected per month	Composite	18	18	18
D2	Average hours downtime per infected device	Composite	8	8	8
D3	Number of hours saved per year	E1*E2*12 months	1,728	1,728	1,728
D4	Average hourly rate for a knowledge worker	$104,000/2,080	$50	$50	$50
D5	Reduction in IT resources needed to repair/replace infected devices w/ 1.5 annual increase	$120K*50% of one FTE	$60,000	$60,900	$61,814
Dt	Savings attributed to reduction in security incidents	D3*D4+D5	$146,400	$147,300	$148,214
	Risk adjustment	↓10%			
Dtr	Savings attributed to reduction in security incidents (risk-adjusted)		$131,760	$132,570	$133,392
	Three-year total: $397,722			**Three-year present value: $329,563**	

SAVINGS ON CYBERINSURANCE

Evidence and data. CrowdStrike has demonstrated within the cybersecurity market that it is a top performer among endpoint security suites. In recent Forrester Wave™ evaluations for enterprise detection and response and endpoint security suites, Forrester has rated CrowdStrike as a Leader among its peers due to its strong current offering, strategy, and market presence.[3] With Falcon Complete's Breach Prevention Warranty, broad coverage is provided for breach response expenses if there is a security incident within the environment protected by Falcon Complete.

The interviewed customers which had cyberinsurance shared that they either received preferred terms and conditions from their cyberinsurance provider or they were in the process of negotiating preferred terms and conditions based on their deployment of Falcon Complete.

Modeling and assumptions. Based on the feedback and inputs from the interviews, the following are the assumptions for the composite organization:

- Savings on cyberinsurance due to preferred terms and conditions are $100,000 per year.
- Since there were few security activities at the time of Forrester's analysis, other than the deployment of Falcon Complete and the replacement for other security services, 90% of the savings were attributed to CrowdStrike.

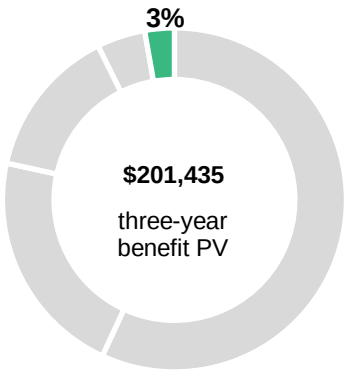
> CrowdStrike's recognition as a leader in cybersecurity, combined with its Breach Prevention Warranty, can provide savings for cyberinsurance.

Risks. The savings on insurance will vary depending on a number of factors, including:

- The level of cyberinsurance protection for the security tools and services prior to Falcon Complete.
- Cyberinsurance coverages may vary according to region or country.

- The technical expertise of the insurance company writing the policy can vary.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $201,435.



Savings On Cyberinsurance

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
E1	Savings on cyberinsurance due to preferred terms and conditions	Composite	$100,000	$100,000	$100,000
E2	Percent attributed to Falcon Complete	Composite	90%	90%	90%
Et	Savings on cyberinsurance	F1*F2	$90,000	$90,000	$90,000
	Risk adjustment	↓10%			
Etr	Savings on cyberinsurance (risk-adjusted)		$81,000	$81,000	$81,000
	Three-year total: $243,000		**Three-year present value: $201,435**		

UNQUANTIFIED BENEFITS

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

- **Confidence and trust customers have in Falcon Complete.** In describing Falcon Complete the interviewed customers used the following phrases:
    - "I'm totally confident."
    - "Lets me sleep far better at night."
    - "Gives me that confidence."

  These are just a few of the many compliments shared by the four leaders in the interviewed organizations. It is difficult to measure in dollar amounts that confidence and trust, but it was repeatedly mentioned throughout the interviews.
- **Ability to focus on other strategic IT initiatives and activities.** Falcon Complete gave customers the assurance that endpoint security was fully covered and needed little if any oversight. This gave customers the ability and availability to easily direct their IT resources to other IT priorities and projects. This was best explained with the following quote from an interviewed customer, "The Falcon Complete product and the comfort and security we get allows my team to focus on other large projects." With cybersecurity handled by CrowdStrike's Falcon Complete, interviewees shared they were able to better manage IT projects such as ongoing network reconfigurations and device upgrades.
- **Elimination of the HR issues of high turnover, hiring, and training.** The savings in terms of salary costs of not having a 24/7/365 fully staffed in-house SOC were identified through the Analysis Of Benefits section. However, the costs

associated with the high turnover normally experienced with SOCs were not included. There is short supply and high demand for trained cybersecurity analysts. This creates an unusually high turnover rate as compared to other IT-related staff. With increased turnover comes hiring and training costs, in addition to possible gaps in cybersecurity coverage and protection. This issue was mentioned in the interviews as another reason for finding a fully managed service, and one that Falcon Complete covers in total.

- **Ease of deployment/time-to-implement.** As in any change and deployment of a new technology platform, customers were initially cautious in the rollout and deployment. In one instance, there were trial period set up for individual endpoints. In another case, the rollout was staged by region. But in all cases when the rollout of Falcon Complete was accomplished it was efficient, effective, and as one customer shared, "seemingly transparent." As another interviewee commented, "Actual onboarding was ridiculously easy, and the guys were ridiculously easy to deal with." As shared before, initial implementation was quick and easy, but it also provided the same quick and easy protection for any changes in endpoints. Quickly providing protection for additional endpoints was noted as a benefit, especially for merger and acquisition activities.
- **Accurate inventory and usage.** Falcon Complete has the flexibility to deploy the agent and identify endpoints that were not previously identified and inventoried. Not only were risks reduced in assuring security coverage for all endpoints, but the usage and changes to the network(s) were also more easily identified. This allowed for better accounting of device counts, capacities, deployments, and licensing fees.
- **A single lightweight agent for all endpoints globally.** The Falcon Complete agent operates without constant signature updates or on-premises infrastructure management. This reduces the burden of open network management and minimizes CPU utilization and perceived delays in device processes. This was especially important for the interviewed security and risk leaders who worked in a decentralized reporting structure.

FLEXIBILITY

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

- **Ability to quickly provide protection to additional endpoints.** Corporations are continually going through changes whether it be growth, relocations, or merger and acquisition activities. Customers of Falcon Complete found that the speed of implementation in the initial rollout also benefited them in quickly adding visibility and protection for the many changes in endpoints.
- **Risk assessment and audit support.** Corporations are interconnected with partners, suppliers, and customers in many ways, including ordering, billing, marketing collateral, and general communication. With those connections come responsibilities to insure secure and safe information flow among all parties. Interviewed customers found Falcon Complete to be a support asset for internal and external audits and in reducing overall risk in general risk assessments.
- **Greater ability than expected to focus on other strategic IT initiatives.** It was shared in earlier sections of this study that Falcon Complete gave interviewed customers the ability to direct their IT resources to other priorities. The feedback also included how often Falcon Complete exceeded customers' expectations in how little involvement they and their staff

required. As one customer related, “What I found most valuable is that we don’t have to get involved in the remediation at all.”

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**
Ftr	CrowdStrike Falcon Complete license fees	$0	$551,250	$551,250	$551,250	$1,653,750	$1,370,877
Gtr	Implementation and admin costs	$5,077	$26,400	$26,796	$27,198	$85,471	$71,657
	Total costs (risk-adjusted)	$5,077	$577,650	$578,046	$578,448	$1,739,221	$1,442,534

CROWDSTRIKE FALCON COMPLETE LICENSE FEES

Evidence and data. Falcon Complete is licensed on a subscription basis per endpoint.

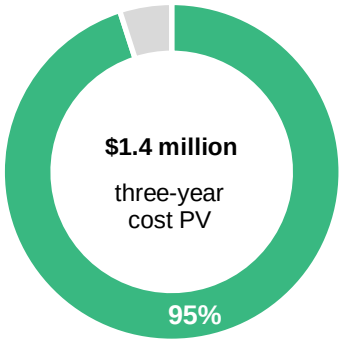
Modeling and assumptions. The costs are based on the following:

- The composite organization has 7,500 endpoints that require protection and monitoring.

Risks. Costs will vary based on:

- The number of endpoints.
- Customer-specific pricing including any discounts.
- The breadth of services contracted.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $1,370,877.



CrowdStrike Falcon Complete License Fees						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Annual license fees	Composite		$525,000	$525,000	$525,000
Ft	CrowdStrike Falcon Complete license fees	Composite	$0	$525,000	$525,000	$525,000
	Risk adjustment	↑5%				
Ftr	CrowdStrike Falcon Complete license fees (risk-adjusted)		$0	$551,250	$551,250	$551,250
	Three-year total: $1,653,750			**Three-year present value: $1,370,877**		

IMPLEMENTATION AND ADMIN COSTS

Evidence and data. The interviewed customers shared that the required staff support for the Falcon Complete deployment and its ongoing administration was minimal. One interviewed customer, a leader of security and risk, shared that they did not assign the ongoing support to anyone on their staff as they were confident in CrowdStrike's performance; this individual did the reviews themselves. Other customers had assigned oversight to their staff, but they felt that minimal ongoing support and involvement was needed.

> **"I've been 100% happy with Falcon Complete. I am happy with the people and happy dealing with the account manager, the regular meetings, and the reports."**
>
> *Senior director for security operations, pharmaceuticals*

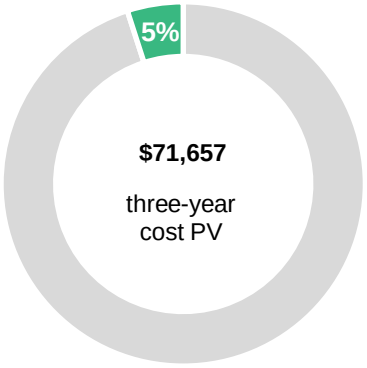
Modeling and assumptions. The costs for the initial deployment of Falcon Complete and the ongoing support for the composite organization are:

- Implementation required 80 hours (two weeks) of support from one FTE.
- Ongoing support is 20% or 416 hours from one FTE.
- The average fully loaded salary for one IT FTE is $120,000.

Risks. Costs for implementation and administration can vary based on:

- The average salary of the assigned staff person to support Falcon Complete.
- The internal reporting and audit requirements of an organization for security and risk reports and general oversight.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $71,657.



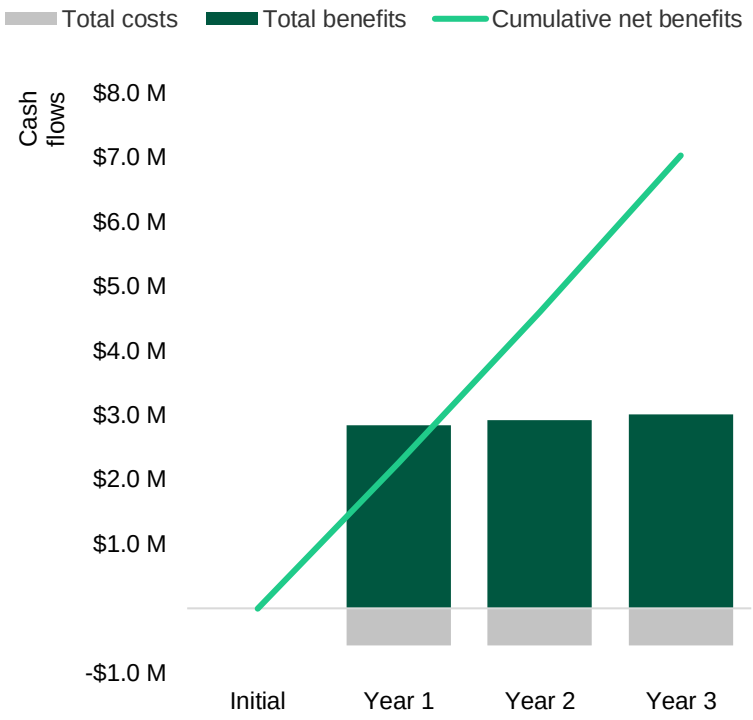
Implementation And Admin Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
G1	Hourly rate of IT staff w/ 1.5% annual increase	$120,000/2,080	$58	$58	$59	$59
G2	Implementation hours	1 FTE for 80 hrs	80	0	0	0
G3	Ongoing admin hours	1 FTE*20%		416	416	416
Gt	Implementation and admin costs	G1*(G2+G3)	$4,615	$24,000	$24,360	$24,725
	Risk adjustment	↑10%				
Gtr	Implementation and admin costs (risk-adjusted)		$5,077	$26,400	$26,796	$27,198
	Three-year total: $85,471		**Three-year present value: $71,657**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($5,077)	($577,650)	($578,046)	($578,448)	($1,739,221)	($1,442,534)
Total benefits	$0	$2,839,464	$2,921,094	$3,006,720	$8,767,278	$7,254,452
Net benefits	($5,077)	$2,261,814	$2,343,048	$2,428,273	$7,028,058	$5,811,918
ROI						403%
Payback period						<3 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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] Source: “Cost of a Data Breach Report 2020,” Ponemon Institute, July 2020.
[2] Source: “Cost of a Data Breach Report 2019,” Ponemon Institute, July 2019.
[3] Source: “The Forrester Wave: Enterprise Detection And Response, Q1 2020” Forrester Research, Inc., March 18, 2020; “The Forrester Wave: Endpoint Security Suites, Q3 2019,” Forrester Research, Inc., September 23, 2019.


FORRESTER®