A Forrester Total Economic Impact™ Study

Commissioned By

FireEye

Project Director:
Reggie Lau

May 2016

The Total Economic Impact™ Of FireEye

Efficiently Improving Asset Protection with FireEye Network Security

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Executive Summary

In May 2016, FireEye commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying FireEye. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of FireEye on their organizations.

FireEye provides cybersecurity against both everyday security exploits and targeted attacks by sophisticated cyberadversaries. FireEye offers several solutions covering security related to network, email, mobile, endpoint, forensics and analysis, file system and storage, and threat assessment, training, and response. This case study will be focused on FireEye customers that have deployed the network security solution, NX. Some interviewed customers have also deployed FireEye solutions beyond NX. Those options will be mentioned, but the primary model and financial results are based on the deployment of FireEye Network Security solution, NX.

> *"During our proof of concept, we turned the appliance on, went to lunch, and in 10 minutes, already found malware on the printer. With FireEye now, we don't have to constantly drop everything to fix things, we have more breathing room and we sleep better at night."*
>
> ~ Information security manager, large European imaging company

To better understand the benefits, costs, and risks associated with deploying FireEye NX, Forrester interviewed four existing FireEye customers that have used the technology for more than six months. Prior to deploying FireEye NX, the interviewed customers used various types of endpoint security applications and other ad hoc solutions but did not have any type of advanced threat protection or sandbox-type solution in their security environments. The common themes in objectives of deploying FireEye NX is to provide a higher level of asset protection, increase efficiency in issue resolution and root cause analysis, and reduce the impact to business resources.

FIREEYE IMPROVES AN ORGANIZATION'S ABILITY TO DETECT AND PREVENT BREACHES, LEADING TO IMPROVED ASSET PROTECTION, REDUCED BUSINESS USER DOWNTIME, AND MORE EFFICIENT SECURITY OPERATIONS AND MANAGEMENT

For the purposes of this case study, a composite organization, Ipsum Couture, will be used to represent the composite feedback of interviews. Forrester's interview with four existing customers and subsequent financial analysis found that the composite organization, Ipsum Couture, experienced the risk-adjusted ROI and payback period shown in Figure 1.[1] The analysis points to benefits of $1,264,635 versus costs of $502,082 over three years, adding up to a net present value (NPV) of $762,553.

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results

ROI: 152%	NPV: $762,553	Payback: 9.7 months

Source: Forrester Research, Inc.

› **Benefits.** The composite organization, Ipsum Couture, experienced the following three-year, risk-adjusted, present value benefits:

- **Asset protection value — $1,070,433.** This benefit describes the value of assets that were not lost due to a breach. This benefit category typically takes into account a combination of network downtime (due to different types of breaches including ransomware), lost revenue, refunds and voluntary compensation, regulatory fines and penalties, civil lawsuits and settlements, insurance premiums, and brand reputation. For this case study, Ipsum Couture experienced a breach in a newly acquired subsidiary that required a two-week shutdown of financial systems, which negatively impacted certain orders through its website and reduced the ability of executives to consume financial reports.
- **Detection and resolution efficiency — $194,203.** This benefit focuses on the reduction of labor and effort for remediation activities due to improved detection and fewer infected devices. This benefit affects both the staff involved in reimaging devices and the staff who conduct the investigation and root-cause analysis.
- **Solution cost effectiveness.** This benefit centers on comparing the cost of deploying FireEye with the cost of deploying an alternative solution. As customer interviewees did not provide cost data for alternative solutions, this component is not quantified as part of this study. Readers may still want to consider the price and any incremental training or hiring that may be necessary with an alternative solution.

› **Costs.** The composite organization, Ipsum Couture, experienced the following three-year, risk-adjusted, present value costs:

- **FireEye solution cost — $385,573.** This is the cost of the FireEye NX appliances, related hardware, and recurring maintenance fees.
- **Internal labor and implementation — $116,509.** This cost focuses on the labor and effort related to initial deployment and ongoing operation.
- **Additional hardware.** This cost describes any additional, non-FireEye hardware that needs to be deployed for FireEye NX to work effectively. This category is not quantified for this case study, as only one of the four customer interviewees mentioned this component while also noting circumstances that may be specific to their environment. Readers should consider their own environment and capacity needs and determine whether additional hardware (e.g., aggregation node and cabling) is needed.

Disclosures

The reader should be aware of the following:

- The study is commissioned by FireEye 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 FireEye.
- FireEye 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.
- With permission from its customers, FireEye provided customer names for the interviews but did not participate in the interviews.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering implementing FireEye. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision, to help organizations understand how to take advantage of specific benefits, reduce costs, and improve the overall business goals of winning, serving, and retaining customers.

APPROACH AND METHODOLOGY

Forrester took a multistep approach to evaluate the impact that FireEye can have on the composite organization, Ipsum Couture (see Figure 2). Specifically, we:

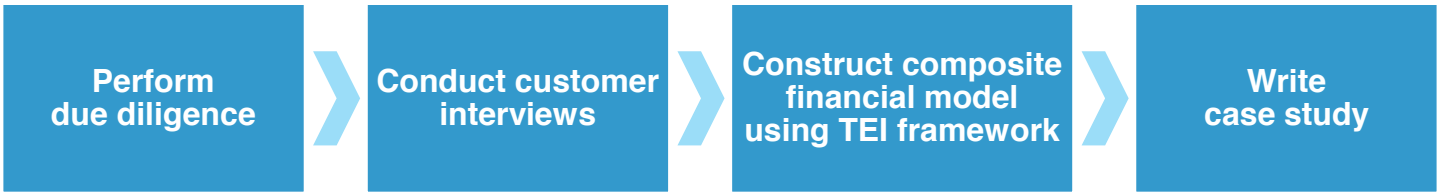
- Interviewed FireEye marketing, sales, and consulting personnel, along with Forrester analysts, to gather data relative to FireEye and the marketplace for advanced cybersecurity solutions.
- Interviewed four FireEye customers to obtain data with respect to costs, benefits, and risks.
- Designed a composite organization to represent the feedback from the interviewed FireEye customers.
- Constructed a composite financial model using the TEI methodology.
- Risk-adjusted the financial model based on issues and concerns the interviewed organizations highlighted in the interview. Risk adjustment is a key part of the TEI methodology. While interviewed organizations provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling the FireEye service: 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 B for additional information on the TEI methodology.

FIGURE 2

TEI Approach



Source: Forrester Research, Inc.

Analysis

COMPOSITE ORGANIZATION — IPSUM COUTURE

For this study, we conducted interviews with four existing customers that have deployed FireEye. A description of the four interviewed customers that contributed to the composite can be found below:

- **A North American bank with over 70,000 staff, 120,000 endpoints, and $35 billion in annual revenue.** This customer has 28 people in its security operations center and assigned three people to deploy and operate the FireEye solution. No specific automated solution for malware mitigation was employed prior to FireEye, and manual work only involved some level of scripting against DNS servers. The necessity for an advanced threat protection solution became prevalent due to news of certain high-profile US financial institutions experiencing major breaches. After conducting tests with five vendors, this customer chose FireEye for its interface, user-friendly deployment, and availability of solutions beyond network security. This customer has since deployed FireEye solutions for email, endpoint, and FireEye as a Service (FaaS), and it has engaged with FireEye security consulting division, Mandiant Consulting, for security assessments.

> *"FireEye detected 20% more [threats], and we reduced device reimaging by 15% to 20%. . . . The solution may cost more than others, but some others would also require us to train and re-tool the staff, which would take time and effort to adopt."*
>
> ~ Information security senior manager, large North American law firm

- **A European subsidiary of a large global imaging company with over 15,000 staff and $8 billion in annual revenue.** This customer has 16 people in its security operations team, which is only responsible for the security of the company's European operations, staff, and offices. Two main events occurred for this customer to deploy FireEye. The first was an almost immediate result in detecting malware on a printer after testing the appliance for 10 minutes. The second was experiencing a major breach with a recently acquired organization that brought down the financial system for two weeks. This made it difficult for executives to consume financial reports, deferred cash flows, and caused unprocessed orders. Since deploying FireEye, the customer has highlighted that the security operations team has more time to plan and execute a strategy as opposed to "putting out fires," and the team lead has less to worry about.

- **A North American food retailer with over 200,000 staff, 100,000 endpoints, 2,000 locations, and $30 billion in annual revenue.** This customer has 85 people on its information security team and six people specifically for security engineering. It also has a team of offshore contractors to assist with operations and support. The customer did not have any advanced threat protection tools prior to FireEye and spent a lot of time and effort reviewing logs and tickets. FireEye was chosen after the customer spoke with references and made comparisons with alternative solutions. The customer noted that reports generated by FireEye are more detailed and have a better description of malware. The FireEye solution also integrates better with the existing security environment, and the customer did not need to hire or train an internal developer, as it may have had to do with other solutions. As this company allows more staff to become remote workers, the customer has started investigating whether to deploy FireEye Endpoint Security solution, HX.

- **A North American law firm with over 1,500 staff and $800 million in annual revenue.** This customer had basic security components for the network, including firewalls and intrusion detection systems (IDS), but it wanted a more advanced, sandbox solution. FireEye was compared with two other solutions, and the customer found that the second best solution had a 10% to 15% false positive rate, which was higher than FireEye. The alternative solution also seemed to require more training and adoption time than FireEye. The customer has experienced a 15% to 20% reduction in device reimaging and estimated an incremental of 20% detections that other components, like antivirus, did not pick up.

Based on these interviews, a composite organization was created to represent the aggregated feedback and quantified experiences. For the purposes of this case study, the composite organization will be known as "Ipsum Couture." Ipsum Couture is a fashion and lifestyle company that has the following high-level characteristics:

> *"In a comparison of five vendors, FireEye was selected for its interface, user-friendly deployment, and they also have an email solution."*
>
> ~ Security operations center manager, large North American bank

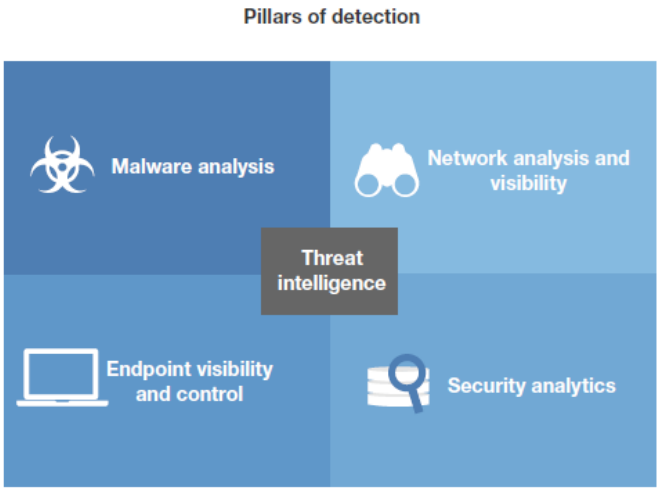
- 8,000 staff, including 500 in consumer-facing roles across its 20 store locations and 7,500 in various office roles, including a 10-person information security team.
- $3 billion in annual revenue from sales at 20 collection stores that feature limited and often seasonal runway-type fashion; website sales featuring primary lines for clothing and licensed lifestyle goods, such as fragrances and home goods; distribution partners and department stores featuring secondary and tertiary lines for clothing; and VIP sales featuring custom designs for high-end customers interested in direct-to-consumer engagement.
- 12,000 endpoints spread across 20 stores, global offices, and remote workers.
- Acquires brands with high potential that fit the company's growth strategy and product portfolio.

Prior to engaging FireEye, Ipsum Couture did not have an advanced threat protection or sandbox-type security solution and relied on endpoint antivirus solutions and the security operations team to review logs and tickets. As the company grew and witnessed high-profile attacks on large consumer brands, Ipsum Couture's executives became concerned with protecting its customer data and avoiding high-profile public relations issues, especially because certain customers are public figures with a high net worth. The security team decided to build out a more comprehensive cybersecurity strategy (see Figure 3) and fill the gaps in each of the technology pillars (see Figure 4).[2] Before the team was able to procure a solution, a small, newly acquired brand experienced a breach, resulting in a shutdown of its financial systems for two weeks. Although the newly acquired brand made up a small portion of Ipsum Couture's business, this hurt the company's sales and reputation, which accelerated the security team's effort to design a strategy and install the necessary technologies.

FIGURE 3
The Targeted-Attack Hierarchy Of Needs

Source: Forrester Research, Inc.

FIGURE 4
Technology Pillars Of Breach Detection



Source: Forrester Research, Inc.

Ipsum Couture started its vendor assessment with five vendors and then narrowed its options down to three. The company's assessment criteria in order of importance were:

- The technology capability and usability as showcased through proof of concept.
- The vendor's reputation through customer references.
- The availability of an expanded solution set to cover beyond network security.
- Investment of capital and training or adoption effort.

Ipsum Couture selected FireEye for its interface, user-friendly deployment process, reputation in the market, availability of email and endpoint solutions, and relatively lower requirement on training and adoption effort. Ipsum Couture engaged FireEye with the following high-level goals:

- Reduce the risk of major breaches and protect the company's assets, especially customer data.
- Prevention when possible; efficient detection otherwise.
- Ensure a low level of false positives and minimal impact to business users.
- Allow the security team to work on enhancing security rather than operating it, through efficient operations management.

INTERVIEW HIGHLIGHTS

The customer interviews revealed the following themes:

- **Organizations should not wait until a major event before building a business case for an advanced threat solution.** Of the four interviewed customers, only one had experienced a major breach and was able to build a business case based on actual lost value. Two of the customers built business cases based on recent events of peer companies in finance and retail. And one of the customers in the legal industry works with clients that have been in lawsuits related to data breaches. It highlighted that the organization holds an ethical responsibility to follow the advice that it provides to clients. Regardless of their industry, customers highlighted that targeted and nontargeted attacks will occur; thus, the potential lost value in a scenario that has never happened to the organization is not as far-fetched anymore. The question is not "if" but "when" and "what are our capabilities to respond." These questions became drivers for these organizations to at least explore the technology options and costs and prepare a business case in light of competing technology priorities.
- **FireEye network security is part of a layered approach.** Customers highlighted that whether they have a multivendor or single-vendor strategy, their organizations use a layered approach to cover each component of their environments (e.g., network, email, end-user devices) and offer redundancy as a risk mitigation plan. One customer used "overlap" and the logging of a single threat in multiple security components as a key metric. This theme is also a reason that some customers selected FireEye as the vendor offered solutions beyond network security. They had plans to expand their network security solution into FireEye email and endpoint solutions and leverage Mandiant Consulting's security assessment and threat response offerings.
- **Post-investment justification is not just about potential lost value multiplied by the probability of a breach.** Similar to other types of technology deployments, organizations can track efficiency metrics in addition to primary KPIs like "lost value avoidance." For example, an organization's primary method of measuring a salesperson is how much the salesperson has sold. However, there are also important yet perhaps secondary efficiency metrics like the volume of cold calls completed in an hour or the pipeline built without manager guidance. In the case of FireEye, users may want to measure items like the ratio of preventions to detections, time to detection, the time and effort to operate and manage the solution, comparisons of operational overhead due to false alerts, or even FireEye's response time to service requests. Measuring these actuals may aid in post-investment justification in addition to potential lost values in hypothetical scenarios.

BENEFITS

The composite organization, Ipsum Couture, experienced three benefits in this case study:

- Asset protection value.
- Detection and resolution efficiency.
- Solution cost effectiveness.

Asset Protection Value

Ipsum Couture acquired a smaller brand around the same time the security team started to redesign the company's security strategy and technology needs. The brand experienced a breach that resulted in the financial systems being shut down for two weeks. Twenty-five percent of online orders were cancelled, and the remaining orders were given a 20% discount for the delay in processing and delivery. Users building a business case may also want to adjust for the probability of a breach — a 25% probability was used for this model.[3]

Along with the lost productivity for executives who are highly dependent on financial reporting, the combined asset protection value is approximately $1.3 million over three years after adjusting for risk, as shown in Table 1.

TABLE 1
Asset Protection Value

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Average orders per month	Year 1: composite Year 2 and 3: $A1_{py}$*110%	75,000	82,500	90,750
A2	Average order value	Year 1: composite Year 2 and 3: $A2_{py}$*110%	$75	$83	$91
A3	Downtime avoided (months)	Composite	0.5	0.5	0.5
A4	Order cancellations	Composite	25%	25%	25%
A5	Discounts offered for late delivery	Composite	20%	20%	20%
A6	Order cancellation value	A1*A2*A3*A4	$703,125	$850,781	$1,029,445
A7	Late delivery discount value	A1*A2*A3*(1-A4)*A5	$421,875	$510,469	$617,667
A8	Total staff	Year 1: composite Year 2 and 3: $A8_{py}$*110%	240	264	290
A9	Executive ratio	Composite	10%	10%	10%
A10	Executives consuming reports	A8*A9	24	26	29
A11	Monthly hours dedicated to consuming reports	Composite	4	4	4
A12	Executive annual salary	Year 1: assumption Year 2 and 3: $A12_{py}$*103%	$175,000	$180,250	$185,658

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A13	Executive report consumption value saved	A10*A11*A3*(A12/12)	$700,000	$793,100	$898,582
A14	Breach probability	Assumption	25%	25%	25%
At	Asset protection value	(A6+A7+A13)*A14	$456,250	$538,588	$636,424
	Risk adjustment	↓20%			
Atr	**Asset protection value (risk-adjusted)**		**$365,000**	**$430,870**	**$509,139**

Source: Forrester Research, Inc.

Detection And Resolution Efficiency

Beyond the value saved from major breaches, Ipsum Couture is able to quantify the efficiencies captured from smaller threats. The company estimates 30 device reimaging requests each month in its previous environment. The organization has experienced a 20% reduction in these requests after deploying FireEye. It typically takes 1 hour for IT to reimage the device and then another half an hour to 1 hour for the business resource to personalize it to their preferences.

Furthermore, for each issue avoided, an investigation that involves three security staff can also be avoided. Altogether, the combined three-year risk-adjusted value of reducing device reimaging is $234,715, as shown in Table 2.

TABLE 2
Detection And Resolution Efficiency

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Devices reimaged prior to FireEye per month	Composite	30	30	30
B2	Reduction due to incremental prevention	Composite	20%	20%	20%
B3	Device reimaging avoidance per month	B1*B2	6	6	6
B4	Hours for IT to reimage device	Composite	1	1	1
B5	Hours for user to personalize device	Composite	0.5	0.5	0.5
B6	IT and user annual salary	Year 1: assumption Year 2 and 3: $B6_{py}$*103%	$65,000	$66,950	$68,959
B7	IT and user value avoided	(B4+B5)*(B6/2,080)*B3*12	$3,375	$3,476	$3,581
B8	Security operations staff to investigate breach	Composite	3	3	3
B9	Days of investigation	Composite	3	3	3
B10	Time dedicated per staff	Composite	25%	25%	25%
B11	Security operations staff annual salary	Year 1: assumption Year 2 and 3: $B11_{py}$*103%	$130,000	$133,900	$137,917

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B12	Breach investigation cost avoided	(B11/260)*B8*(B9*B10)*B3 *12	$81,000	$83,430	$85,933
Bt	Detection and resolution efficiency	B7+B12	$84,375	$86,906	$89,513
	Risk adjustment	↓10%			
Btr	**Detection and resolution efficiency (risk-adjusted)**		**$75,938**	**$78,216**	**$80,562**

Source: Forrester Research, Inc.

Solution Cost Effectiveness

Solution cost effectiveness compares the cost for initial deployment, recurring maintenance, ongoing labor, and any training and adoption effort between FireEye and alternative solutions. Although this benefit category is not quantified as part of this case study, we included it because one customer interviewee noted a lower training and adoption barrier for FireEye. Readers may want to quantify this component as part of building a tailored business case after speaking with multiple vendors.

Total Benefits

Table 3 shows the total of all quantified benefits, as well as present values (PVs) discounted at 10%. Over three years, the composite organization, Ipsum Couture, expects risk-adjusted total benefits to be a PV of $1,264,635.

TABLE 3
Total Benefits (Risk-Adjusted)

Ref.	Benefit	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Asset protection value	$0	$365,000	$430,870	$509,139	$1,305,009	$1,070,433
Btr	Detection and resolution efficiency	$0	$75,938	$78,216	$80,562	$234,715	$194,203
	Total benefits	**$0**	**$440,938**	**$509,086**	**$589,701**	**$1,539,724**	**$1,264,635**

Source: Forrester Research, Inc.

COSTS

The composite organization, Ipsum Couture, experienced three costs in this case study:

- FireEye solution cost.
- Internal labor and implementation.
- Additional hardware.

FireEye Solution Cost

The solution cost includes the initial cost for the FireEye appliance and the ongoing maintenance fees. For this case study, an estimate of $250,000 was used to cover six network security (NX) appliances and one central management (CM) device. A 20% ratio was used to estimate the annual maintenance fee. This results in a three-year risk-adjusted solution cost of $412,000, as shown in Table 4.

TABLE 4
FireEye Solution Cost

Ref.	Cost	Calculation	Initial	Year 1	Year 2	Year 3
C1	NX appliances	Composite	6	-	-	-
C2	CM device	Composite	1	-	-	-
C3	Hardware investment	Composite	$250,000	-	-	-
C4	Annual maintenance and license ratio	Assumption	-	20%	20%	20%
C5	Annual maintenance fee	$C4*C3_{initial}$	-	$50,000	$50,000	$50,000
Ct	FireEye solution cost	C3+C5	$250,000	$50,000	$50,000	$50,000
	Risk adjustment	↑3%				
Ctr	**FireEye solution cost (risk-adjusted)**		**$257,500**	**$51,500**	**$51,500**	**$51,500**

Source: Forrester Research, Inc.

Internal Labor And Implementation

Ipsum Couture budgeted three months to procure, deploy, integrate, test, and monitor FireEye before stabilizing. During this period, four staff dedicated 25% of their time to the effort. Post deployment, the ongoing operations fell to one of the four staff and required 25% of that staff's time. The total three-year risk-adjusted value is $134,368, as shown in Table 5.

TABLE 5
Internal Labor And Implementation

Ref.	Cost	Calculation	Initial	Year 1	Year 2	Year 3
D1	Initial deployment staff	Composite	4			
D2	Dedicated time to deployment	Composite	25%			
D3	Deployment weeks	Composite	12			
D4	Initial deployment cost	(D7/52)*D3*D1*D2	$30,000			
D5	Ongoing operations staff	Composite		1	1	1
D6	Dedicated time to operations	Composite		25%	25%	25%
D7	Security operations staff annual salary	Initial and year 1: assumption Year 2 and 3: $D7_{py}$*103%	$130,000	$130,000	$133,900	$137,917
D8	Ongoing operations cost	D7*D6*D5		$32,500	$33,475	$34,479
Dt	Internal labor and implementation	D4+D8	$30,000	$32,500	$33,475	$34,479
	Risk adjustment	↑3%				
Dtr	**Internal labor and implementation (risk-adjusted)**		**$30,900**	**$33,475**	**$34,479**	**$35,514**

Source: Forrester Research, Inc.

Additional Hardware

Additional hardware is not quantified in this case study, as three of the four interviewees did not give any indication that additional hardware was a necessary investment. One of the interviewees did invest in a port aggregator for traffic and packets but also noted that it may be specific to their environment's capacity and age. Readers should take into consideration any additional hardware that may be needed to effectively incorporate the FireEye appliance into their respective environments.

Total Costs

Table 6 shows the total of all costs, as well as present values (PVs) discounted at 10%. Over three years, Ipsum Couture expects risk-adjusted total costs to be a PV of $502,082, as shown in Table 6.

TABLE 6
Total Costs (Risk-Adjusted)

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ctr	FireEye solution cost	$257,500	$51,500	$51,500	$51,500	$412,000	$385,573
Dtr	Internal labor and implementation	$30,900	$33,475	$34,479	$35,514	$134,368	$116,509
	Total costs	**$288,400**	**$84,975**	**$85,979**	**$87,014**	**$546,368**	**$502,082**

Source: Forrester Research, Inc.

FLEXIBILITY

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement FireEye and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project.

As Ipsum Couture continues to grow as a company and increases its use of cloud applications, it may need to invest in upgrading or incremental FireEye NX appliances to address growing capacity demands. Furthermore, per Ipsum Couture's reasoning for selecting FireEye, the company may expand its footprint with the FireEye email and endpoint solutions. The email solution will assist in filling in any remaining gaps, and the endpoint solution will address the company's growing remote worker program. Lastly, after the email and endpoint solution deployments, Ipsum Couture plans to engage Mandiant Consulting for an assessment to review if there are any further gaps to fill.

RISKS

Forrester defines two types of risk associated with this analysis: "implementation risk" and "impact risk." Implementation risk is the risk that a proposed investment in FireEye may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in FireEye, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 7
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Asset protection value	↓ 20%
Detection and resolution efficiency	↓ 10%
Costs	**Adjustment**
FireEye solution cost	↑ 3%
Internal labor and implementation	↑ 3%

Source: Forrester Research, Inc.

Quantitatively capturing implementation risk and impact risk by directly adjusting the financial estimates results provides more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as "realistic" expectations since they represent the expected values considering risk.

The following impact risks that affect benefits are identified as part of the analysis:

- Attempting to customize the sandbox image according to the standard image for the organization.
- Configuring correctly to avoid any delays or impact to the business.
- Aligning standard FireEye reporting with the organization's reporting needs.

The following implementation risks that affect costs are identified as part of this analysis:

- Increased bandwidth demand.
- Lack of a cybersecurity strategy, leading to increasing hiring or training costs.

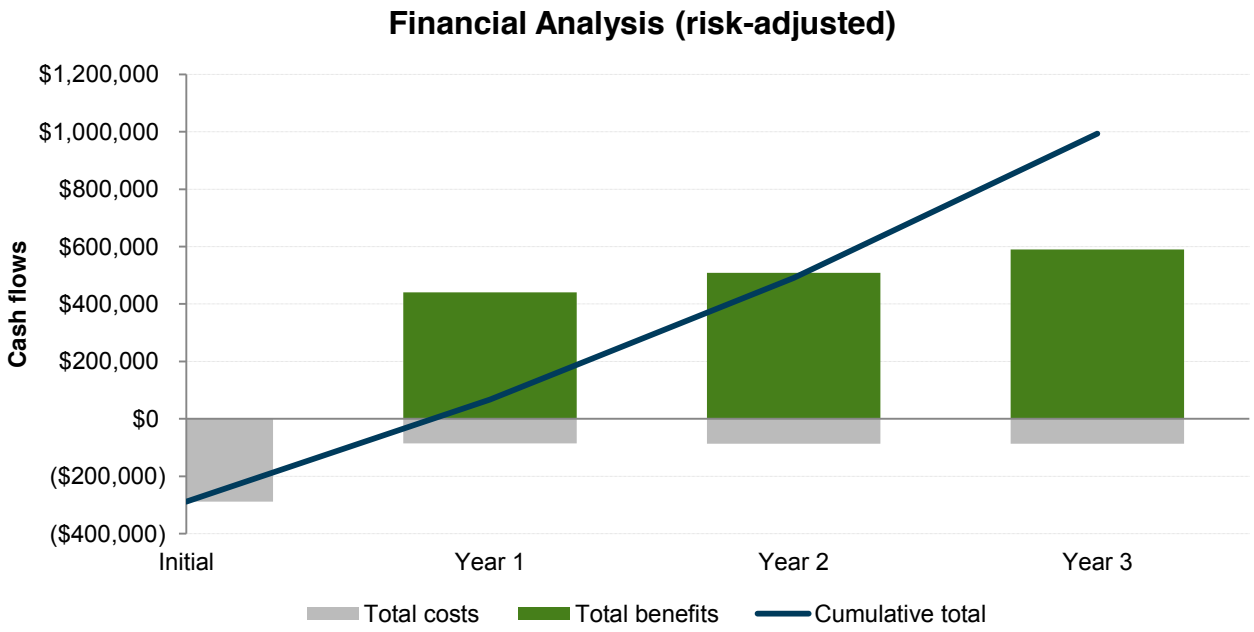
Table 7 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the composite organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for Ipsum Couture's investment in FireEye.

Table 8 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 7 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 5
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 8
Cash Flow (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	($288,400)	($84,975)	($85,979)	($87,014)	($546,368)	($502,082)
Benefits	$0	$440,938	$509,086	$589,701	$1,539,724	$1,264,635
Net benefits	**($288,400)**	**$355,963**	**$423,106**	**$502,687**	**$993,356**	**$762,553**
ROI			152%			
Payback period			9.7 months			

Source: Forrester Research, Inc.

FireEye: Overview

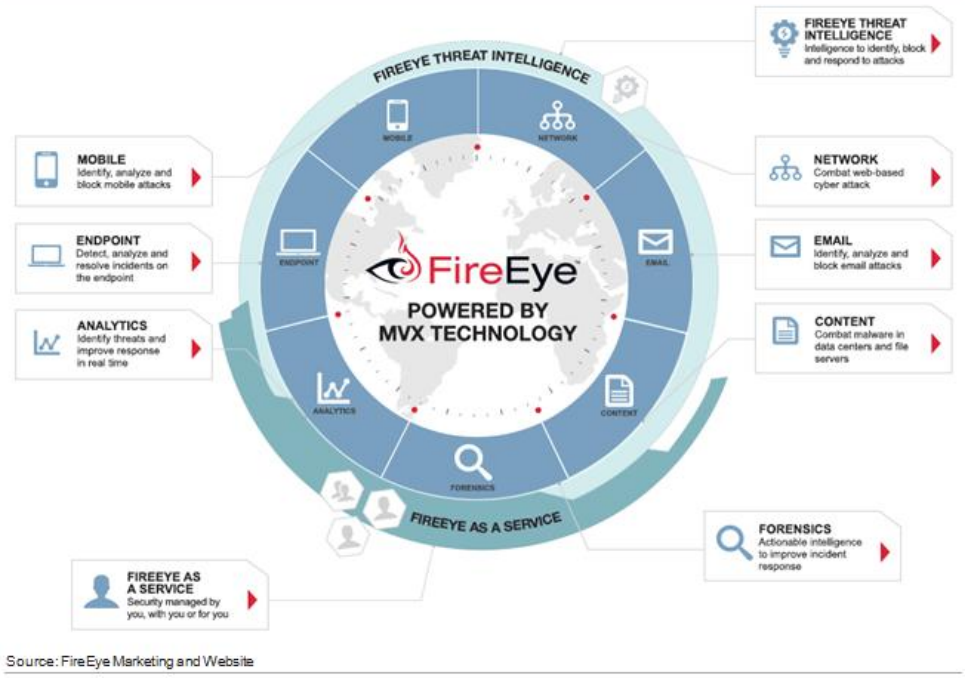
The following information is provided by FireEye. Forrester has not validated any claims and does not endorse FireEye or its offerings.

FireEye cybersecurity products combat today's advanced persistent threats (APTs). As an integral piece of an adaptive defense strategy, the FireEye state-of-the-art network security offerings protect against cyberattacks that bypass traditional signature-based tools such as antivirus software, next-generation firewalls and sandbox tools.

The FireEye product portfolio includes:

- Network security.
- Email security.
- Content security.
- FireEye-as-a-service.
- Enterprise forensics.
- Endpoint forensics.
- Endpoint security.
- Malware analysis.
- Mobile security.
- Threat analytics platform.
- Central management.
- Orchestration
- Threat intelligence.

FIGURE 6
FireEye Product Portfolio



Source: FireEye Marketing and Website

For more information on FireEye, please go to https://www.fireeye.com.

Appendix A: Composite Organization — Ipsum Couture

Based on these interviews, a composite organization was created to represent the aggregated feedback and quantified experiences captured during the interviews. For the purposes of this case study, the composite organization will be known as "Ipsum Couture." Ipsum Couture is a fashion and lifestyle company that has the following high-level characteristics:

- 8,000 staff, including 500 in consumer-facing roles across its 20 store locations and 7,500 in various office roles, including a 10-person information security team.
- $3 billion in annual revenue from sales at 20 collection stores that feature limited and often seasonal runway-type fashion; website sales featuring primary lines for clothing and licensed lifestyle goods, such as fragrances and home goods; distribution partners and department stores featuring secondary and tertiary lines for clothing; and VIP sales featuring custom designs for high-end customers interested in direct-to-consumer engagement.
- 12,000 endpoints spread across 20 stores, global offices, and remote workers.
- Acquires brands with high potential that fit the company's growth strategy and product portfolio.

Prior to engaging FireEye, Ipsum Couture did not have an advanced threat protection or sandbox-type security solution and relied on endpoint antivirus solutions and the security operations team to review logs and tickets. As the company grew and witnessed high-profile attacks on large consumer brands, Ipsum Couture's executives became concerned with protecting its customer data, especially because certain customers are public figures with a high net worth. The security team decided to build out a more comprehensive cybersecurity strategy (see Figure 3) and fill the gaps in each of the technology pillars (see Figure 4)[4]. Before the team was able to procure a solution, a small, newly acquired brand experienced a breach, resulting in a shutdown of its financial systems for two weeks. Although the newly acquired brand made up a small portion of Ipsum Couture's business, this hurt the company's sales and reputation, which accelerated the security team's effort to design a strategy and install the necessary technologies.

Ipsum Couture started its vendor assessment with five vendors and then narrowed its options down to three. The company's assessment criteria in order of importance were:

- The technology capability and usability as showcased through proof of concept.
- The vendor's reputation through customer references.
- The availability of an expanded solution set to cover beyond network security.
- Investment of capital and training or adoption effort.

Ipsum Couture selected FireEye for its interface, user-friendly deployment process, reputation in the market, availability of email and endpoint solutions, and relatively lower requirement on training and adoption effort. Ipsum Couture engaged FireEye with the following high-level goals:

- Reduce the risk of major breaches and protect the company's assets, especially customer data.
- Prevention when possible; efficient detection otherwise.
- Ensure a low level of false positives and minimal impact to business users.
- Allow the security team to work on enhancing security rather than operating it, through efficient operations management.

FRAMEWORK ASSUMPTIONS

Table 9 provides the model assumptions that Forrester used in this analysis.

The discount rate used in the PV and NPV calculations is 10%, and the time horizon used for the financial modeling is three years. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their respective company's finance department to determine the most appropriate discount rate to use within their own organizations.

TABLE 9
Model Assumptions

Ref.	Metric	Value
X1	Hours per week	40
X2	Weeks per year	52
X3	Hours per year (M-F, 9-5)	2,080
X4	Hours per year (24x7)	8,760
X5	Annual organization/budget growth	10%
X6	Annual salary/wage growth	3%
X7	IT security annual salary	$130,000
X8	Executive annual salary	$175,000
X9	Average nontechnical resource annual salary	$65,000
CY/PY	Current/prior year	

Source: Forrester Research, Inc.

Appendix B: Total Economic Impact™ Overview

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. TEI assists technology vendors in winning, serving, and retaining customers.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

BENEFITS

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place 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. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

COSTS

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

FLEXIBILITY

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections and 2) the likelihood that the estimates will be measured and tracked over time. TEI risk factors are based on a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the risk factor around each cost and benefit.

Appendix C: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

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.

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.

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.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A NOTE ON CASH FLOW TABLES

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until 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.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.

Appendix D: Endnotes

[1] Forrester risk-adjusts the summary financial metrics to take into account the potential uncertainty of the cost and benefit estimates. For more information, see the section on Risks.

[2] Source: “Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Advanced Capabilities,” Forrester Research, Inc., July 24, 2014.

[3] Twenty-five percent probability is derived from a 22% probability noted in a 2015 Ponemon Institute study and a 25% probability suggested in a study by FireEye. Source: “2015 Cost of Data Breach Study: Global Analysis,” Ponemon Institute, (https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf) and “The Business Case For Protecting Against Advanced Attacks,” FireEye, (https://www2.fireeye.com/WEB-2015WPBusinessCaseforFaaS.html).

[4] Source: “Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Advanced Capabilities,” Forrester Research, Inc., July 24, 2014.