A Forrester Total Economic Impact™
Study Commissioned By Proofpoint
October 2019

The Total Economic Impact™ Of Proofpoint Advanced Email Protection

Cost Savings And Business Benefits Enabled By Proofpoint

FORRESTER®

Table Of Contents

Project Director:
Sam Conway

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®

Investment Benefits

Reduced risk of a data breach:
$2,017,857

Avoided headcount to manage email security:
$345,517

"I could sing songs about how you don't know what you've got until it's gone. Basic email protection is like electricity for me in IT: Everyone expects it to be there, but most end users don't understand how complex it is or what is involved."
-CTO, healthcare

Executive Summary

According to Forrester, "Email remains a critical communication medium for organizations of all sizes. However, its ubiquity, combined with the open nature of email itself, also makes it a powerful tool for attackers. Phishing attacks combine technical attacks with social engineering, which makes them difficult to prevent. Proper defense against phishing attacks requires a combination of technologies and techniques — all capabilities that are found in antiphishing technologies."[1] Research shows that 94% of threats start with email.[2] Further, Forrester has found that 27% of external attacks where an enterprise was breached were carried out using stolen credentials — often beginning with a simple phishing email.[3]

Proofpoint provides an advanced email protection suite that helps its customers protect themselves from sophisticated cyberattacks. Proofpoint commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying its email protection products. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Proofpoint email protection on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer with several years of experience using Proofpoint. The organization is a large, US-based healthcare system operator that uses Proofpoint to block spam and malicious content, automate incident response steps, encrypt email data, and improve visibility and forensic capabilities.

Prior to using Proofpoint, the interviewed customer used various vendors for spam protection with limited success and relied on manual capabilities to protect against more sophisticated attacks.

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Reduced the risk of major data breach by 50%.** Implementing automated defense tools has vastly reduced the organization's risk of incurring a major data breach. The organization established automated controls to block malicious spam, attachments, and URLs from reaching end users and to isolate and remove any content that passed through its primary filter. Over a three-year period, the present value (PV) of avoided risk is $2,017,857.
- **Avoided headcount to manage email security.** Proofpoint automatically analyzes any links or attachments in emails prior to delivery, rewriting URLs to provide click-time protection. If Proofpoint deems the contents of an email malicious post-delivery, Proofpoint automatically removes the message from any users who have received it. Before Proofpoint, the organization required email security FTEs to manually analyze and pull emails after threat events. Over a three-year period, the organization saves a PV of $345,517.

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

FORRESTER®

ROI
259%

Benefits PV
$2.4 million

NPV
$1.7 million

Payback
<3 months

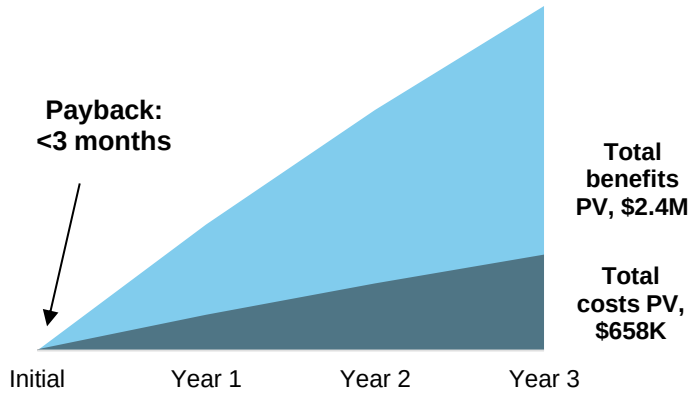
- **Enhanced encryption standards and avoidance of potential fines.** As a healthcare firm, the organization is required to adhere to certain governmental standards such as the Health Insurance Portability and Accountability Act (HIPAA). Using Proofpoint Email Encryption, the organization implemented stringent encryption policies, ensuring that sensitive records are properly protected and no privacy laws are violated.
- **Limited user downtime.** The ability to block spam and malicious messages ensures that users experience limited downtime and provides an overall better user atmosphere.
- **Protected brand image and strengthened marketing efforts.** The organization can use its security track record to assuage patient fears and differentiate from competitors that experience security events.

Costs. The interviewed organization experienced the following risk-adjusted PV costs:

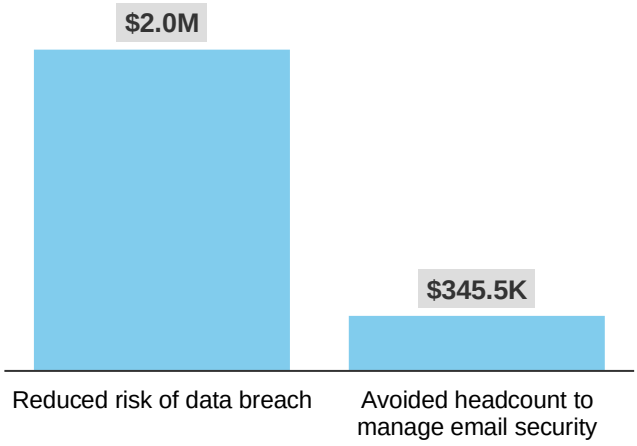
- **Annual Proofpoint fees of $210,000.** The organization has a software-as-a-service (SaaS) deployment of Proofpoint's solutions and pays an annual fee for the use of Email Protection, Targeted Attack Protection, Threat Response, Email Fraud Defense, Email Encryption, and Email DLP.
- **Internal deployment costs of $8,531.** The organization required one FTE for one month of deployment.
- **Ongoing Proofpoint management costs.** The organization has one FTE dedicating 50% of their time to the management of the Proofpoint deployment.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $2,363,374 over three years versus costs of $658,066, adding up to a net present value (NPV) of $1,705,308 and an ROI of 259%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Proofpoint's advanced email security suite.

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 Proofpoint email security tools can have on an organization:

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

DUE DILIGENCE
Interviewed Proofpoint stakeholders and Forrester analysts to gather data relative to Proofpoint's email security products.

CUSTOMER INTERVIEW
Interviewed one organization using Proofpoint to obtain data with respect to costs, benefits, and risks.

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

CASE STUDY
Employed four fundamental elements of TEI in modeling Proofpoint email security impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Proofpoint 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 Proofpoint.

Proofpoint 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.

Proofpoint provided the customer name for the interview but did not participate in the interview.

The Proofpoint Customer Journey

BEFORE AND AFTER THE PROOFPOINT INVESTMENT

Interviewed Organization

For this study, Forrester interviewed a Proofpoint customer:

- The customer is a US healthcare system operating 20 multispecialty care centers. The organization serves roughly 500,000 patients with 1.5 million annual visits.
- The organization employs and protects several thousand users.
- The organization maintains a single data center and has most users running nonpersistent virtual desktops.
- The organization operates Opportunistic Transport Layer Security (TLS) on its exchange servers to enable passive encryption when available.
- The organization uses Proofpoint Email Protection, Targeted Attack Protection, Threat Response, Email Fraud Defense, Email Encryption, and Email DLP.

Using Proofpoint:

Email Protection
Targeted Attack Protection
Threat Response
Email Fraud Defense
Email Encryption
Email DLP

Key Challenges

The organization shared the following challenges, which led to the Proofpoint investment:

- **Limiting user exposure to email attacks.** The organization recognized that email vulnerabilities posed a serious threat to its large user base. Furthermore, attackers have grown more sophisticated and focus more on individuals than infrastructure. The CTO stated: “Given that the majority of threats that enter an organization have the potential to enter through an email, the level of security that you have to provide at the email level is critical. The core functionality of a secure email gateway is the most important aspect of what we have.”
- **Adhering to stringent government regulations.** As a player in the healthcare market, the organization is held to stringent government standards regarding the maintenance and protection of patient information. Violating these policies poses the risk of not only fines, but also damaged reputation and loss of patient trust. Ensuring that communications are encrypted and patient records are not lost to phishing or other malicious attacks was a top priority for the organization.
- **Easily scaling email security operations.** The organization wanted automated and cloud-based tools that could easily scale with its growing operations and email usage. Not having to grow physical deployments or increase the number of FTE assets dedicated to monitoring and maintaining the email security apparatus was a must.

Key Results

The interview revealed that key results from the Proofpoint investment include:

- **Strengthened email security and avoided major data breaches.** The organization has avoided incurring a major data breach, and Proofpoint has been a major factor in that experience. The organization uses Proofpoint to set stringent email controls that automatically block thousands of emails a day and provide automated tools to analyze, provide visibility, and respond to any threats that pass through initial controls. The CTO stated, "Looking at our dashboard and looking at the amount of phishing emails that we turn away, I can say unequivocally that the number of incidents that are blocked by our solutions, particularly Proofpoint, is very high, and it really keeps us from having to deal with any kind of incident management."
- **Enforced stringent encryption policies.** The organization uses Proofpoint to set and enforce stringent email encryption protocols, ensuring that its organization remains in line with government regulations. Users are provided with manual encryption tools prompted by the type of data sent, while the organization also uses Proofpoint DLP to monitor and control the flow of any sensitive data that may have been shared accidentally. The CTO explained: "For an employee to simply assume that we're going to be able to encrypt their email is not a good assumption. We expect them to set the encryption flag, and we give them multiple ways to do that. They can put brackets on the subject, they can mark it is as confidential, whatever. It then goes out through the secure email gateway. That demonstrates to us the willful intent on someone's part to encrypt email."
- **Reduced effort required to maintain email security operations.** By using Proofpoint's automated security capabilities, the organization has greatly reduced the effort required to manage email security operations. The organization can set automated firewall policies, rely on Proofpoint's intelligent threat analysis, and use Threat Response Auto Pull (TRAP) to continuously analyze, block, and remove malicious content. With these tools, the organization has eliminated the need for FTE assets to manually script email harvests, monitor and manage firewall policies, and analyze and update blocked sender lists. The CTO stated: "I would absolutely state that we do see man hours saved because prior to this technology being a core part of Proofpoint's offering, when we had a determination that we had a malicious email, we would have to go and harvest emails containing that content from inboxes. Now that we have that technology enabled, it is a real timesaver for us."

> "The ability to go back historically and manage emails that have become malicious is a great feature."
>
> *CTO, healthcare*

> "We do geographic management of our traffic, so we don't even process messages that come from China or Russia or eastern Europe — areas that are known for notorious activity. We block out 30,000 connections from China every hour."
>
> *CTO, healthcare*

> "[If audited,] we are able to adequately demonstrate through Proofpoint logs that almost all email gets sent and received as encrypted mail."
>
> *CTO, healthcare*

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Reduced risk of data breach	$811,410	$811,410	$811,410	$2,434,230	$2,017,857
Btr	Avoided headcount to manage email security	$138,938	$138,938	$138,938	$416,813	$345,517
	Total benefits (risk-adjusted)	$950,348	$950,348	$950,348	$2,851,043	$2,363,374

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of nearly $2.4 million.

Reduced Risk Of Data Breach

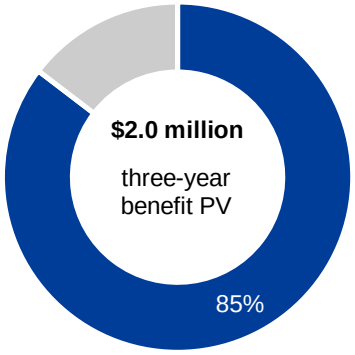
The organization implemented a variety of Proofpoint tools that provide protection at messaging touchpoints. All of these tools combined have enabled the organization to avoid experiencing a major data breach or digital loss event.

First, the organization uses Proofpoint policy settings to set up robust policies at the first step in email routing. The organization automatically blocks emails from specific geographic regions and senders with a known reputation for malicious activity. This approach allows the organization to block known historical threats from reaching its users. Furthermore, the organization harnesses Proofpoint's Stateful Composite Scoring (SCCS) to dynamically identify emerging email threats and block email fraud. The CTO explained: "There's a whole bunch of stuff that gets knocked down before even getting to our environment, and that same reputation handling is being done by Proofpoint. To some extent, we are vicariously benefiting by Proofpoint's own statistics of all the stuff that they knock down that they never even bring to our gateway."

The organization also uses Proofpoint Targeted Attack Protection (TAP) to quarantine messages with malicious attachments or URLs not caught by its initial firewall; these emails messages frequently lack malware or are not malicious at the time of delivery, which makes initial discovery difficult. The organization uses Proofpoint to automatically scan embedded attachments and URLs for threats and filter user clicks as well as monitor suspicious login attempts. The organization has set a policy for users where if a potentially malicious URL is clicked, their password is automatically reset. The CTO explained: "If somebody actually clicks on a phishing email, we immediately reset their password and they have to call in to the help desk to get a new password. They cannot reset it themselves; they have to make a phone call to do that."

The organization use Proofpoint's Threat Response Auto-Pull (TRAP) to analyze and quarantine messages after delivery. This quarantine can be initiated by Proofpoint's post-delivery analysis or from user prompts. The tool allows the organization to quickly react to threatening messages in users' inboxes. The CTO stated: "If Proofpoint later determines that a link or an attachment is malicious, that it had a timebomb in it, we have the ability to go and remove that from our mailboxes. That's a very cool capability."

Finally, the organization harnesses Proofpoint's Email Encryption and



Reduced risk of data breach: **85%** of total benefits

FORRESTER®

DLP to ensure that any user messages containing sensitive content cannot be accidentally exposed.

For the analysis, Forrester assumes that:

- Using Ponemon Research estimates, the average US company has a 29.6% probability of experiencing a data breach.[4]
- The average value of a breach for a US healthcare firm is $6.45 million.[5]

Forrester recognizes that readers are likely to experience a wide range of results based on several risk factors. Specific risk considerations include:

- Geographic location of firm, size, and industry vertical.
- Baseline security tools and training.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $2,017,857.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Reduced Risk Of Data Breach: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Average cost of US healthcare data breach	Ponemon research	$6,450,000	$6,450,000	$6,450,000
A2	Average risk of data breach occurring	Ponemon research	29.6%	29.6%	29.6%
A3	Annual risk value	A1*A2	$1,909,200	$1,909,200	$1,909,200
A4	Attribution of risk avoidance to Proofpoint		50%	50%	50%
At	Reduced risk of data breach	A3*A4	$954,600	$954,600	$954,600
	Risk adjustment	↓15%			
Atr	Reduced risk of data breach (risk-adjusted)		$811,410	$811,410	$811,410

Avoided Headcount To Manage Email Security

With the ability to automate many aspects of its email security apparatus, the organization has avoided the need for additional headcount. Some tasks, such as pulling malicious emails post-delivery, would previously have required manual work. Other features of Proofpoint had no direct analog at the time of inception but would have required adding FTE assets to attain the same capabilities.

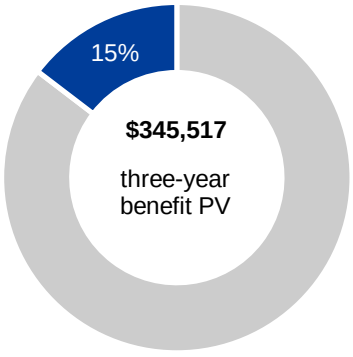
The CTO for the organization explained: “With Proofpoint, all somebody really needs to do is occasionally look through the Proofpoint dashboard to see what’s going on and see if there’s anything happening. It’s a massive timesaver when the tools are there to simply pull up and look at. I currently attribute a full FTE to the overall responsibility of overseeing our email protection program. But if we didn’t have the kinds of tools that we have with Proofpoint, that would be two to three FTEs.”

For the interviewed organization, Forrester assumes that:

- The fully burdened salary of an email security FTE is $97,500.

The reduction in security management expense will vary with:

- Size and complexity of organization.



Avoided headcount to manage email security: **15%** of total benefits

FORRESTER®

› Geographic location and prevailing local labor rates.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $345,517.

Avoided Headcount To Manage Email Security: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	FTE equivalent avoided		1.5	1.5	1.5
B2	Fully loaded salary		$97,500	$97,500	$97,500
Bt	Avoided headcount to manage email security	B1*B2	$146,250	$146,250	$146,250
	Risk adjustment	↓5%			
Btr	Avoided headcount to manage email security (risk-adjusted)		$138,938	$138,938	$138,938

Unquantified Benefits

The interviewed organization experienced the following benefits, which are not quantified for this study:

- **Regulatory compliance and avoidance of fines.** The organization utilizes Proofpoint to enact and enforce user rules and adhere to federal data regulations.
- **Improved user uptime.** Improved blocking of spam and malicious emails limits user downtime.
- **Improved marketing.** The organization uses its security strength and track record as a differentiator.

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Annual Proofpoint fees	$0	$210,000	$210,000	$210,000	$630,000	$522,239
Etr	Internal deployment cost	$8,531	$0	$0	$0	$8,531	$8,531
Ftr	Ongoing Proofpoint management cost	$0	$51,188	$51,188	$51,188	$153,563	$127,296
	Total costs (risk-adjusted)	$8,531	$261,188	$261,188	$261,188	$792,094	$658,066

Annual Proofpoint Fees

The organization pays an annual license fee for the use of its cloud-deployed Proofpoint suite. Solutions in this organization's deployment include Email Security, Targeted Attack Protection, Threat Response, Email Fraud Defense, Email Encryption, and Email DLP.

Readers may experience varying Proofpoint fees based on license type and usage. Proofpoint offers a number of deployment and solution options as well as variable discounts.

To account for these risks, Forrester has adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $522,239.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of $658,066.

Annual Proofpoint Fees: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Annual Proofpoint fees		$0	$200,000	$200,000	$200,000
Dt	Annual Proofpoint fees	D1	$0	$200,000	$200,000	$200,000
	Risk adjustment	↑5%				
Dtr	Annual Proofpoint fees (risk-adjusted)		$0	$210,000	$210,000	$210,000

Internal Deployment Cost

The organization spent one month fully implementing its Proofpoint deployment. During this period, the organization dedicated a single FTE resource to overseeing the implementation.

In modeling this cost, Forrester assumes a fully burdened salary of $97,500 for the FTE managing implementation.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates. Implementation time and recognition of benefits may vary based on an organization's size and specific network characteristics. Geographic location and local labor rates may also differ.

To account for these risks, Forrester adjusted this cost upward by 5%,

One month
Total implementation and deployment time

FORRESTER®

yielding a three-year risk-adjusted total PV of $8,531.

Internal Deployment Cost: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	FTE required for deployment		1			
E2	Time dedicated to deployment (months)		1			
E3	Annual fully burdened salary		$97,500			
Et	Internal deployment cost	E1*E2*(E3/12)	$8,125	$0	$0	$0
	Risk adjustment	↑5%				
Etr	Internal deployment cost (risk-adjusted)		$8,531	$0	$0	$0

Ongoing Proofpoint Management Cost

The organization dedicates a single FTE, who spends 50% of their time to the ongoing management of its Proofpoint deployment.

In modeling this cost, Forrester assumes a fully burdened annual salary of $97,500.

The costs associated with managing a Proofpoint deployment may vary due to specific use cases and tools deployed, size and scope of operations, and prevailing local labor rates.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $127,296.

One FTE
spends 50% of their time on ongoing management of Proofpoint.

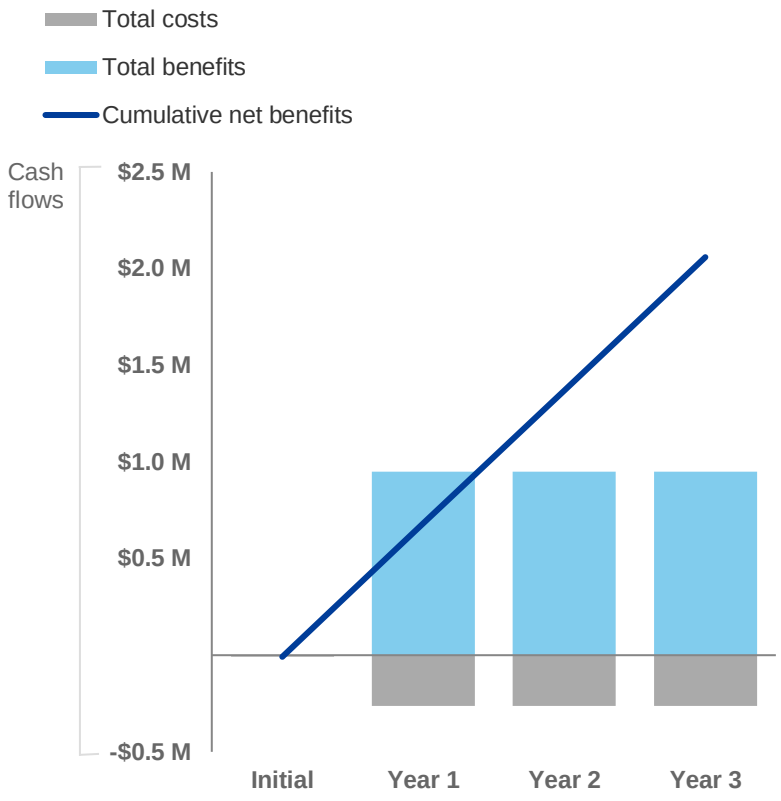
Ongoing Proofpoint Management Cost: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
F1	FTE required for ongoing email security management			1	1	1
F2	Percentage of time dedicated to Proofpoint			50%	50%	50%
F3	Annual fully burdened salary			$97,500	$97,500	$97,500
Ft	Ongoing Proofpoint management cost	F1*F2*F3		$48,750	$48,750	$48,750
	Risk adjustment	↑5%				
Ftr	Ongoing Proofpoint management cost (risk-adjusted)		$0	$51,188	$51,188	$51,188

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 interviewed 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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($8,531)	($261,188)	($261,188)	($261,188)	($792,094)	($658,066)
Total benefits	$0	$950,348	$950,348	$950,348	$2,851,043	$2,363,374
Net benefits	($8,531)	$689,160	$689,160	$689,160	$2,058,949	$1,705,308
ROI						259%
Payback period						<3 months

FORRESTER®

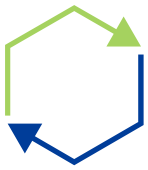
Appendix A: Total Economic Impact

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: “Now Tech: Antiphishing Solutions, Q1 2019,” Forrester Research, Inc., January 8, 2019.
[2] Source: “2019 Data Breach Investigations Report,” Verizon, 2019.
[3] Source: “The Forrester Wave™: Enterprise Email Security, Q2 2019,” Forrester Research, Inc., May 16, 2019.
[4] Source: “2019 Cost of a Data Breach Report,” Ponemon Institute, 2019 (https://www.ibm.com/security/data-breach).
[5] Ibid.

FORRESTER®