A Forrester Total Economic Impact™ Study Prepared For Tufin Software Technologies

The Total Economic Impact Of Tufin's Security Suite

A Large Financial Services Provider Simplified Its Security Operations And Reduced The Risk Of A Security Breach

Project Director: Sebastian Selhorst

March 2013

Headquarters | Forrester Research, Inc.
60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | www.forrester.com

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 www.forrester.com/consulting.

Executive Summary

Security organizations struggle to strike a balance between new and more virulent threats with business expectations and budgetary realities. These organizations are challenged to maintain network security in the most efficient way possible. However, reconciling the constantly growing complexity of access rules with outdated, manual processes and procedures increases the risk of security breaches. In addition, regulators are imposing increasingly rigorous standards of transparency and accountability. Modern security teams need technology that will help them enforce security policies, improve situational awareness, and automate the process steps to limit the risk of security breaches. At the end of the day, the demands on today's security professional are so intense that operational automation must be added to the security equation if the overall security posture of an organization is to be improved.

In January 2013, Tufin commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) enterprises may realize by deploying Tufin's Security Suite.

Tufin Security Suite is an integrated security solution that enables IT organizations to effectively manage the network connectivity and security requirements of their applications across all network devices, including traditional and next-generation firewalls, routers, switches, and load balancers. For a more detailed overview of Tufin's Security Suite, please refer to page 20.

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Tufin's Security Suite on their organizations.

Tufin's Security Suite Enabled A Financial Services Provider To Simplify Security Operations While Reducing The Risk Of A Security Breach

This study illustrates the financial impact — what Forrester calls the Total Economic Impact™ (TEI) — of deploying Tufin's Security Suite at a large European financial services provider. The company provides services in the areas of securities trading, clearing, settlement, financial information, and payment transactions. It has about 1,000 business applications and manages 700 physical and logical firewalls. The complexity of the firewall environment grew constantly and the organization decided to invest in Tufin's Security Suite to reduce this intricacy, gain an overview of the actual configurations, and streamline firewall administration. Our financial analysis found that the scenario described by the interviewed organization has the three-year risk-adjusted ROI, costs, and benefits shown in Table 1.

Table 1
Three-Year Risk-Adjusted ROI[1]

ROI	Payback period	Total benefits (PV)	Total costs (PV)	Net present value
148%	11 months	$3,064,476	($1,238,082)	$1,826,394

Source: Forrester Research, Inc.

- **Benefits.** In conducting in-depth interviews with this existing Tufin customer, Forrester found that this company expects benefits of slightly more than $3 million over a three-year period. In particular, the benefit categories comprise:

> *"Tufin helped us achieve our three goals: to streamline our firewall administration, to increase the visibility of our firewall configurations, and to reduce the complexity of our environment."* (CSO, large European financial services provider)

  - **Productivity gains.** The traditional process for updating firewalls is cumbersome and ineffective. All modern organizations depend so heavily on firewalls that the maintenance of these policies is too time-consuming. The interviewed organization reported that it was able to reduce its efforts with regard to the firewall change management process by 88%. In this case, the productivity gains have an estimated three-year risk-adjusted present value (PV) of approximately $1.25 million.

  - **Hardware cost savings.** The interviewed organization has a rather large and complex firewall environment. The Tufin solution helped the company simplify existing firewall rule sets and to limit and slow the growth of complexity. This has a positive impact on the hardware performance. As a consequence, the company avoided adding extra capacity and can keep the optimized hardware for longer periods of time. For the interviewed company, the resulting cost savings have an estimated three-year risk-adjusted PV of approximately $1.1 million.

  - **Operational cost savings.** The solution simplified the ongoing management of the firewall environment. The interviewed organization was able to reallocate one full-time resource from the firewall management team to other tasks. Labor elasticity is a major issue for many companies, and finding good security professionals is a difficult task. Any time security resources can be reallocated should be considered a major win. The resulting cost savings have an estimated three-year risk-adjusted PV of approximately $565,000.

  - **Audit cost savings.** For the interviewed organization, preparing for a firewall audit used to be a very labor-intensive task. Data from different sources, including firewall configuration files, extracts from an application database, and firewall change request forms, had to be correlated manually, resulting in significant expense. With the Tufin solution in place, the data required for the audit is always readily available. In this case, the audit cost savings have an estimated three-year risk-adjusted PV of approximately $125,000.

  - **Faster incident management.** The interviews organization thinks that cleaner firewall rule sets and the automation of steps in firewall change implementations will result in fewer firewall configuration errors and thus fewer incidents. Moreover, fewer people now need to be involved in root-cause analysis and incident resolution. In this case, the associated cost savings have an estimated three-year risk-adjusted PV of approximately $33,000. Note that fewer incidents might also result in less application downtime, which might result in additional value for organizations. In this case, however, the interviewed organization could not quantify this reduction in application downtime; therefore, it not been included in this business case. The company has very efficient fallback solutions in place that limit the impact of this kind of incidents.

  - **Reduced risk of security breaches.** The Tufin solution helps enforce the organization's security policy across the network. The interviewed organization is now more comfortable with its firewall environment and thinks that the risk of security breaches has been reduced. However, the uncertainty of a security breach and the variability of its potential impact on the organization prevent us from taking it into account in this

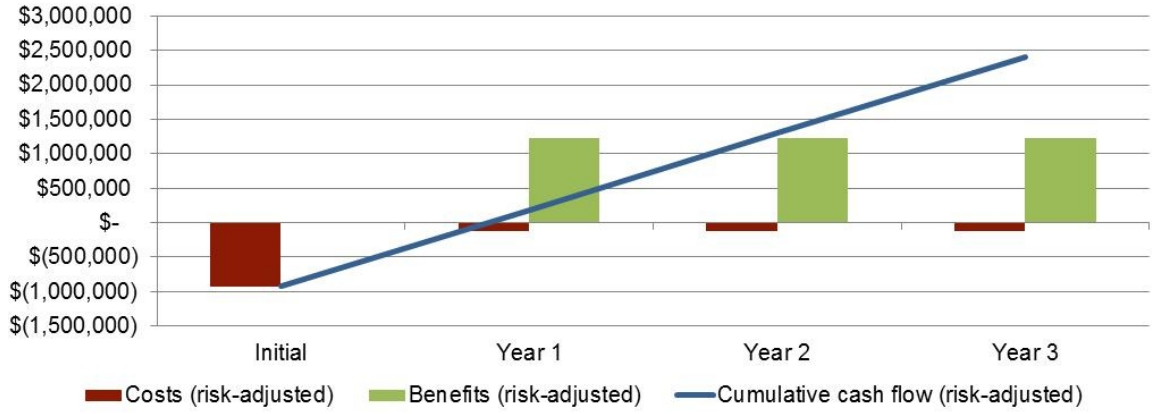
financial business case. The variable direct and hidden costs that can be associated with a security breach can reach from incident response services and regulatory fines to lost earnings, to even changes in stock price. In light of a security breach, simply proactively reducing the attack surface might be invaluable.

"In our industry, we just cannot afford security breaches. Preventing just one case in 50 years would justify the whole investment at once." (Chief security officer (CSO), large European financial services provider)

- **Costs.** To achieve the above benefits, the cost of the Tufin solution is about $1.24 million over a three-year period. Costs included:
    - **Software licensing and maintenance costs.** The organization invested in the full Tufin Security Suite, including SecureApp, SecureChange, and SecureTrack. It licensed about 500 business applications and connected a total of 260 physical and logical firewalls to the Tufin Security Suite. The equivalent price of the software licenses and maintenance costs has a three-year risk-adjusted PV of approximately $943,000.
    - **Setup costs.** The setup costs include professional services costs and internal labor costs for planning, configuring, deploying the Tufin solution. The interviewed organization estimates the internal efforts to about 200 man-days of work. The total setup costs in this case have a three-year risk-adjusted PV of approximately $244,000.
    - **Hardware costs.** The interviewed company chose to run the Tufin solution on dedicated appliances. The resulting hardware and maintenance costs have a three-year risk-adjusted PV of approximately $35,000 in this case.
    - **Training costs.** The seven members of the firewall management team followed the equivalent of two full-day training classes. The associated costs for the organization have a three-year risk-adjusted PV of approximately $15,000.

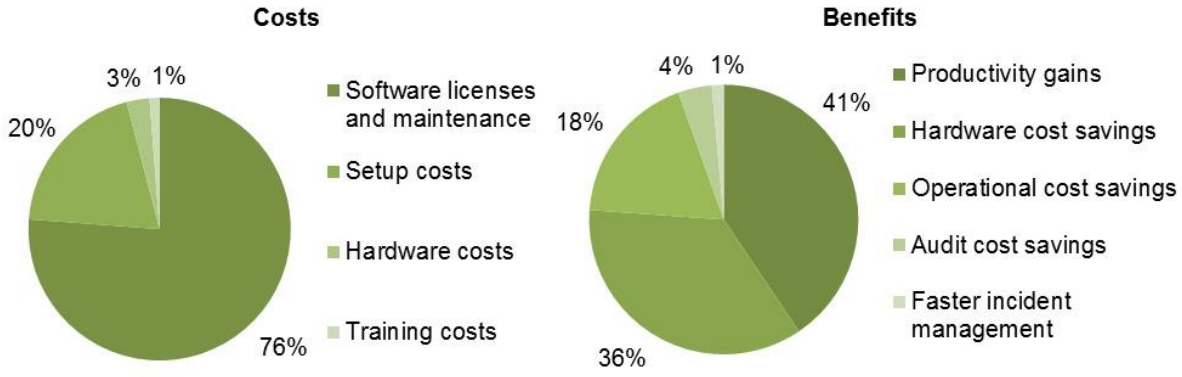
Figure 1 summarizes the yearly and cumulative cash flow; Figure 2 shows the breakdown of the benefit and cost categories for the interviewed organization.

Figure 1
Three-Year Risk-Adjusted Cash Flow



Source: Forrester Research, Inc.

Figure 2
Three-Year Risk-Adjusted Costs And Benefits



Source: Forrester Research, Inc.

Factors Affecting Benefits And Costs

Table 1 illustrates the risk-adjusted financial results that were achieved by the interviewed organization. The risk-adjusted values take into account any potential uncertainty or variance that exists in estimating the costs and benefits, which produces more conservative estimates. The following factors may affect the financial results that an organization may experience:

- **Organization's risk tolerance.** Each organization is unique due to its size, industry, long-term business objectives, and tolerance for risk. A security breach might have very different impacts on organizations, ranging for example from incident response services and regulatory fines to lost revenue from downtime or even changes in stock price. It is therefore understandable that organizations evaluate the value of reduced risk with regard to security breaches very differently.
- **Complexity of organization's firewall environment.** The complexity of an organization's firewall environment defines to what extent it may benefit from security tools such as Tufin's Security Suite. Organizations with a large number of firewalls and complex, distributed business applications are likely to achieve higher value from such an investment than organizations with simpler firewall operations.
- **Agility of organization.** The benefits associated with productivity gains are dependent on how successful each company is at leveraging the functions of Tufin's Security Suite, how many people are concerned, and how effectively firewall engineers can reallocate the freed-up time productively.

Disclosures

The reader should be aware of the following:

- The study is commissioned by Tufin and delivered by the Forrester Consulting group.
- Forrester makes no assumptions as to the potential return on investment 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 Tufin's Security Suite.
- Tufin 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.
- The customer names for the interviews were provided by Tufin.

TEI Framework And Methodology

Introduction

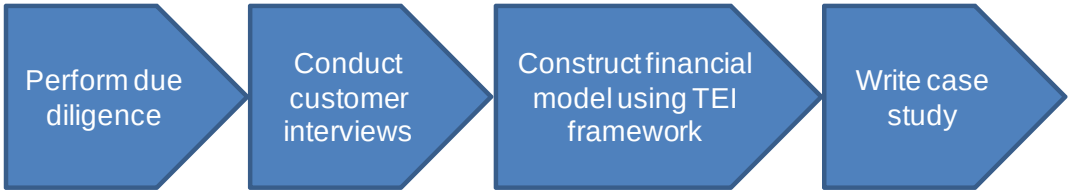
From the information provided in the interviews, Forrester has constructed a Total Economic Impact framework for those organizations considering implementing Tufin's Security Suite. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision.

Approach And Methodology

Forrester took a multistep approach to evaluate the impact that Tufin Security Suite can have on an organization (see Figure 3). Specifically, we:

- Interviewed Tufin's marketing and sales personnel and Forrester analysts to gather data relative to security management tools and the corresponding marketplace.
- Interviewed one organization currently using Tufin Security Suite to obtain data with respect to costs, benefits, and risks.
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews.

Figure 3
TEI Approach



Source: Forrester Research, Inc.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves the purpose of providing a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Analysis

Interview Highlights

Forrester interviewed one organization, a large European financial services provider, for this study. The company employs about 4,000 people in more than 20 countries and provides services in the areas of securities trading, clearing, settlement, financial information, and payment transactions.

Working in the financial services sector, the IT and network security are of course taken very seriously. The company and its clients cannot afford to experience any security breaches or major service disruptions. Furthermore, the company has to comply with a number of security regulations and is frequently audited by regulators.

Ensuring the security of the network is part of the firewall management team consisting of seven full-time engineers. About 1,000 business applications are running on the network which comprises about 700 physical and logical firewalls.

Prior to the investment in the Tufin Security Suite, requesting and implementing changes to the firewall rule set was a very slow and cumbersome process that took one to two weeks on average. Nearly all firewall change requests were related to application changes. The firewall engineers tried to keep track of the changing application connectivity requirements in a database, application owners had nearly no visibility into the existing firewall rules when establishing a new firewall change request, and requests often had to go through several revision cycles and a series of approvals before the changes could be implemented manually and the database updated.

By constantly adding new rules to the existing ones, the complexity of the firewall environment grew steadily, as did the risk of having security holes.

> *"One of the main problems with managing firewalls is that change requests nearly always ask for new ports to be opened, but only rarely to be closed. Application managers are interested in making their applications run but do not necessarily ask for a route to be closed if it is no longer used."* (CSO, large European financial services provider)

Security audits were also a tedious task. Data from various sources, including firewall configuration files, the application database, and the accumulated change request forms, needed to be reconciled manually. In 2011, the company realized that it had to act.

> *"We realized that we had to do something. We could no longer see the big picture. The environment was getting too complex to manage."* (CSO, large European financial services provider)

The company was looking for a tool that would allow it to manage application-related firewall changes from a business process perspective. Following an assessment of the tools that were available in the market, the company decided to invest in Tufin's Security Suite, including SecureApp. The main business objectives for this investment were to:

- Reduce firewall administration efforts.
- Increase the visibility with regard to existing firewall configurations.
- Reduce the complexity of firewall rules.

The Tufin Security Suite was put into production in December 2012. All new change requests now go through this solution; the application database is being phased out. The company has already seen a significant improvement in the firewall change and audit processes and visibility has also increased. Due to the new tool, the company was able to remove 200 "failsafe" rules and has identified that about 10% of existing rules are unused and can be removed in the months to come. Finally, a cleaner firewall environment reduces the risk of a security breach.

> *"We now have cleaner firewall policies — and that is very important to us. It does not necessarily translate into direct cost savings, but it reduces the risk of being hacked. It gives me peace of mind."* (CSO, large European financial services provider)

Framework Assumptions

Please note that this analysis describes the business case of an investment scenario similar to the one of the interviewed organization. In reality, the interviewed organization assisted Tufin with the development and the testing of the SecureApp product. In this analysis, however, we discuss the costs that a company with the same scope would incur and the benefits that it could achieve by investing in the finalized product suite. Table 2 provides the model and salary assumptions that Forrester used in this analysis.

Table 2
Model Assumptions

Ref.	Metric	Calculation	Value
A1	Hours worked per day		8
A2	Average number of working days per year		220
A3	Average fully loaded annual salary rate		$232,000
A4	Average fully loaded daily salary rate (rounded)	A3/A2 rounded	$1,050
A5	Average fully loaded hourly salary rate (rounded)	A3/(A1*A2) rounded	$130

Source: Forrester Research, Inc.

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.

Costs

This section describes and lists the incremental costs over three years incurred by the interviewed organization for deploying and maintaining Tufin's Security Suite.

Software Costs

The interviewed organization runs about 1,000 business applications on the network and has about 100 physical and 600 logical firewalls. It licensed the Tufin solution for about 500 business applications and 260 physical and logical firewalls. The Tufin products SecureApp, SecureChange, and SecureTrack are running on dedicated appliances. While the organization received a special offer from Tufin due to its involvement in the development and testing of the SecureApp product, this analysis uses the price a typical customer would incur. Tufin provided this price for an equivalent scope. The equivalent software license and maintenance costs are indicated in Table 3 below.

Setup Costs

The setup costs include the estimated internal labor and professional service costs that an organization with the same scope would incur for deploying the Tufin security solution in its environment. The internal efforts are estimated to about 200 man-days or $210,000, including resources from the project management team, the engineering team, the firewall management team, and general management. The professional services from Tufin include assistance with the planning, the installation and configuration of the products, the design of some complex workflows and the training. In this case, the professional services costs are estimated at $32,000. The sum of the internal labor and the professional service costs is indicated in Table 3 below.

Hardware Costs

Tufin's solution can be installed on existing servers or Tufin can provide dedicated appliances. In this case, the interviewed organization decided to run the Tufin solution on dedicated appliances. The equivalent appliance and maintenance costs are indicated in Table 3 below.

Training Costs

For the training, we assume that the seven members of the firewall team attend a two-day workshop. The resulting costs to the organization are shown in Table 3 below. Please note that the costs of the trainer are already included in the professional service costs (see Setup Costs section above).

Total Costs

Table 3 summarizes the incremental non-risk-adjusted costs incurred by the interviewed organization for setting up and maintaining Tufin's Security Suite. In total, the interviewed organization spent approximately $1.3 million over three years.

Table 3
Total Costs (Non-Risk-Adjusted)

Ref.	Costs	Initial	Year 1	Year 2	Year 3	Total
B1	Software licenses and maintenance	$630,000	$126,000	$126,000	$126,000	$1,008,000
B2	Setup costs	$242,000	$0	$0	$0	$242,000
B3	Hardware costs	$33,500	$0	$750	$750	$35,000
B4	Training costs	$14,560	$0	$0	$0	$14,560
Bt	Total costs (non-risk-adjusted)	$920,060	$126,000	$126,750	$126,750	$1,299,560

Source: Forrester Research, Inc.

Benefits

The interviewed organization reported quantifiable benefits in terms of productivity gains, hardware cost savings, operational and audit cost savings, and faster incident management. These benefit categories are discussed below.

Productivity Gains

Before the introduction of Tufin's solution the firewall change process was slow and cumbersome. It included a lot of manual tasks, revisions, and authorizations. The interviewed organization estimates that a firewall change request took one to two weeks from request to implementation, with an actual workload of 10 hours. With the Tufin solution, this process has now been streamlined. Both the application manager and the firewall team have a better visibility into the firewall configurations, open routes can be better leveraged and several process tasks are automated. For the interviewed organization, the result is that the required workload for a firewall change request has been reduced by up to 88%, to 75 minutes. This results in significant net time savings for application managers, firewall administrators, and approvers.

However, Forrester assumes that only a portion of the time gained from improved productivity will actually be realized by the organization. In this analysis, we assume that 75% of the time saved will actually be converted into productive output.

With an average of 50 firewall change requests per month, the total three-year, non-risk-adjusted productivity gains can be estimated to approximately $1.5 million, as indicated in Table 4 below.

Table 4
Productivity Gains

Ref.	Metric	Value/ calculation	Year 1	Year 2	Year 3	Total
C1	Average number of firewall change requests per month	50				
C2	Number of firewall change requests per year	600 (C1*12)				
C3	Time required before introduction of Tufin's Security Suite (hours)	10				
C4	Time required after introduction of Tufin's Security Suite (hours)	1.25				
C5	Average fully loaded hourly salary rate (rounded)	$130 (see A5, Table 2)				
C6	Percentage of time saved that actually translates into productive output	75%				
Ct	Productivity gains	C2*(C3-C4)*C5*C6	$511,875	$511,875	$511,875	$1,535,625

Source: Forrester Research, Inc.

Operational Cost Savings

More generally, the whole management of the firewall environment has become more efficient due to Tufin's solution. From an ongoing operations standpoint, the interviewed organization was able to reallocate one full-time employee from the firewall team to other tasks. The resulting cost savings are indicated in Table 5 below.

Table 5
Operational Cost Savings

Ref.	Metric	Value/ calculation	Year 1	Year 2	Year 3	Total
D1	Number of FTEs reassigned to other tasks	1				
D2	Average fully loaded annual salary rate	$232,000				
Dt	Operational cost savings	D1*D2	$232,000	$232,000	$232,000	$696,000

Source: Forrester Research, Inc.

Hardware Cost Savings

The dynamic of constantly increasing data traffic with an ever growing number of firewall rules has a negative impact on firewall performance. To cope with this situation, organizations regularly have to add new capacity. The interviewed organization reports that — due to the Tufin Security Suite — firewall configurations are now cleaner and less complex. New rules are still added, but unused rules are also removed. This results in higher performance, and the interviewed organization estimates that existing firewall can be kept for one to 1.5 years longer and that the company thus saves about $530,000 per year in hardware investments.

Please note that the amount of savings depends largely on the complexity of the firewall environment which in the case of the interviewed organization is rather high. The hardware cost savings for the interviewed organization are indicated in Table 6 below.

Table 6
Hardware Cost Savings

Ref.	Metric	Value/ calculation	Year 1	Year 2	Year 3	Total
E1	Estimated annual hardware cost savings	$530,000				
Et	Hardware cost savings	E1	$530,000	$530,000	$530,000	$1,590,000

Source: Forrester Research, Inc.

Audit Cost Savings

Prior to the introduction of Tufin's Security Suite, a firewall audit took five days on average. Most of the time was spent manually reconciling data from different sources, such as firewall configuration files, extracts from the application database, and firewall change request forms. Now with the Tufin solution, the auditors do not need to correlate this data manually anymore; the interviewed organization estimates that external auditors save up to four days of work. The estimated audit cost savings to the organization are indicated in Table 7 below.

Table 7
Audit Cost Savings

Ref.	Metric	Value/ calculation	Year 1	Year 2	Year 3	Total
F1	Average number of firewall audits per year	4				
F2	External auditor cost per day	$3,200				
F3	Number of days per audit required before introduction of Tufin's Security Suite	5				
F4	Number of days per audit required after introduction of Tufin's Security Suite	1				
F5	Estimated number of auditor days saved per year	16 ((F3-F4)*F1)				
Ft	Audit cost savings	F5*F2	$51,200	$51,200	$51,200	$153,600

Source: Forrester Research, Inc.

Faster Incident Management

The interviewed organization estimates that before the introduction of Tufin's Security Suite, about 20 incidents per year were caused by firewall misconfigurations. Due to the improved visibility with regard to actual firewall configurations and the streamlined firewall change management process, the interviewed organization estimates that the number of such incidents will be reduced by 60%. Furthermore, while the average resolution time will still be four hours, the actual number of people involved to analyze and resolve such incidents is reduced from five to two.

Forrester assumes again that only 75% of the time saved will actually be converted into productive output. The resulting productivity gains are indicated in Table 8 below.

Table 8
Faster Incident Management

Ref.	Metric	Value/ calculation	Year 1	Year 2	Year 3	Total
G1	Number of incidents caused by firewall misconfigurations per year (before introduction of Tufin's Security Suite)	20				
G2	Reduction in number of incidents	60%				
G3	Avoided incidents	12 (G1*G2)				
G4	Hours spent analyzing and resolving incident (before introduction of Tufin's Security Suite)	20 (5 people*4 hours)				
G5	Hours spent analyzing and resolving incident (after introduction of Tufin's Security Suite)	8 (2 people*4 hours)				
G6	Hours saved per incident	12 (=G4-G5)				
G7	Average fully loaded hourly salary rate (rounded)	$130				
G8	Percentage of time that actually translates into productive output	75%				
Gt	Faster incident management	G3*G6*G7* G8	$14,040	$14,040	$14,040	$42,120

Source: Forrester Research, Inc.

Total Benefits

The interviewed organization expects to achieve total benefits of approximately $4 million over the three-year period. Table 9 shows the total non-risk-adjusted benefits that were quantifiable for this study.

Table 9
Total Benefits (Non-Risk Adjusted)

Ref.	Benefits	Year 1	Year 2	Year 3	Total
Ct	Productivity gains	$511,875	$511,875	$511,875	$1,535,625
Dt	Operational cost savings	$232,000	$232,000	$232,000	$696,000
Et	Hardware cost savings	$530,000	$530,000	$530,000	$1,590,000
Ft	Audit cost savings	$51,200	$51,200	$51,200	$153,600
Gt	Faster incident management	$14,040	$14,040	$14,040	$42,120
Ht	Total benefits (non-risk adjusted)	$1,339,115	$1,339,115	$1,339,115	$4,017,345

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 deploy Tufin's Security Suite and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

While Forrester believes organizations can take advantage of these flexibility options, quantification (using the financial industry standard Black-Scholes or the binomial option pricing models) of the additional value associated with these options for this customer would require scenario development and forward-looking analysis, which is not available at this time.

Risk

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 a security tool 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 this security tool, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

Quantitatively capturing investment and impact risk by directly adjusting the financial estimates results in 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 implementation risks that affect costs are identified as part of this analysis:

- The amount of internal efforts required to deploy the security solution depends on the available skills and might be higher than originally estimated.
- The amount that a company needs to invest in new hardware depends for example on the required performance and might be higher than originally estimated.
- The amount of training needed over the three-year period may depend on the employee turnover, and the costs may thus be higher than originally estimated.

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

- Productivity gains depend on the ability of the concerned staff to reallocate their time productively.
- The amount of operational cost savings depends on the ability of the organization to redeploy its resources effectively and might be lower.
- The total amount of hardware cost savings depends on the complexity of the existing firewall environment and might be lower.
- The amount of audit cost savings is based on the assumption that external audit costs can be renegotiated according to the decreased efforts and might be lower.
- Cost savings with regard to faster incident management might be lower depending on the number of actual incidents during the three years of the analysis.

Table 10 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates. The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur within the current environment. The risk-adjusted value is the mean of the distribution of those points.

Table 10
Cost And Benefit Risk Adjustments

Costs	Low	Most likely	High	Mean
Setup costs (low)	98%	100%	105%	101%
Hardware costs (low)	98%	100%	105%	101%
Training costs (medium)	100%	100%	115%	105%
Benefits	**Low**	**Most likely**	**High**	**Mean**
Productivity gains (low)	90%	100%	105%	98%
Operational cost savings (low)	90%	100%	105%	98%
Hardware cost savings (high)	50%	100%	100%	83%
Audit cost savings (low)	90%	100%	105%	98%
Faster incident management (medium)	80%	100%	103%	94%

Source: Forrester Research, Inc.

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 Costs and Benefits sections can be used to determine the three-year return on investment, net present value, and payback period for the organization's investment in Tufin's Security Suite. These are shown in Table 11 below.

Table 11
Cash Flow: Non-Risk-Adjusted

Cash flow: original estimates						
	Initial	Year 1	Year 2	Year 3	Total	PV
Costs	($920,060)	($126,000)	($126,750)	($126,750)	($1,299,560)	($1,234,587)
Benefits	$0	$1,339,115	$1,339,115	$1,339,115	$4,017,345	$3,330,181
Total	($920,060)	$1,213,115	$1,212,365	$1,212,365	$2,717,785	$2,095,594
ROI	170%					
Payback period	10 months					

Source: Forrester Research, Inc.

Table 12 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 10 in the Risk section to the cost and benefits numbers in Tables 3 and 9.

Table 12
Cash Flow: Risk-Adjusted

Cash flow: orisk-adjusted estimates						
	Initial	Year 1	Year 2	Year 3	Total	PV
Costs	($923,543)	($126,000)	($126,758)	($126,758)	($1,303,058)	($1,238,082)
Benefits	$0	$1,232,271	$1,232,271	$1,232,271	$3,696,813	$3,064,476
Total	($923,543)	$1,106,271	$1,105,514	$1,105,514	$2,393,755	$1,826,394
ROI	148%					
Payback period	11 months					

Source: Forrester Research, Inc.

Tufin's Security Suite: Overview

Tufin is a provider of security policy management solutions that enable organizations to take control of their firewalls. According to Tufin, more than 1,100 customers are using Security Suite to assess and mitigate risk in real time, continuously comply with standards, and keep business-critical applications online.

The Tufin Security Suite enables IT to manage security policy across all network devices including traditional and next-generation firewalls, routers, switches, and load balancers. Tufin uses an application-oriented approach to policy management to simplify and streamline firewall operations.

Tufin Security Suite is composed of the following three fully integrated core products:

- **SecureApp for application connectivity management.** Tufin SecureApp enables IT organizations to effectively manage the network connectivity and security requirements of their applications. It provides insight into an application's connectivity needs so that companies can accelerate service delivery, assure business continuity, and monitor compliance. SecureApp is a new approach to managing application connectivity that separates business requirements from the underlying firewall and router policies to simplify operations.
- **SecureTrack for firewall operations, auditing, and compliance.** Tufin SecureTrack is a security operations management solution for network and next-generation firewalls as well as network infrastructure including routers, switches, load balancers, and web proxies. SecureTrack features powerful tools that eliminate routine, manual tasks while assuring security and business continuity for large and small enterprises. Tufin SecureTrack enables organizations to continuously comply with regulatory standards and successfully pass security audits faster.
- **SecureChange for security change automation.** Tufin's SecureChange solution enables companies to automate security change management and risk analysis for the network. With SecureChange, companies can automate business processes to proactively enforce security policies and support governance initiatives.

Appendix A: 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.

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

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.

Risk

Risk measures 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 applies a probability density function known as "triangular distribution" to the values entered. At minimum, three values are calculated to estimate the underlying range around each cost and benefit.

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 in time. However,

having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value.

Appendix B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a 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 organization 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 net present value of cash flows.

Payback period: The breakeven point for an investment. 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 Framework Assumptions section) at the end of the year. Present value (PV) calculations are calculated for each total cost and benefit estimate. Net present value (NPV) calculations are not calculated until the summary tables and are the sum of the initial investment and the discounted cash flows in each year.

Table [Example]
Example Table

Ref.	Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.

Appendix C: Supplemental Material

Related Forrester Research

"Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, Inc., November 15, 2012.

"Determine The Business Value Of An Effective Security Program — Information Security Economics 101," Forrester Research, Inc., October 2, 2012.

"Understand The State Of Network Security: 2012 To 2013," Forrester Research, Inc., September 20, 2012.

"Develop Your Road Map For Zero Trust Network Mitigation Technology," Forrester Research, Inc., May 9, 2012.

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 on Risk, please see page 16.