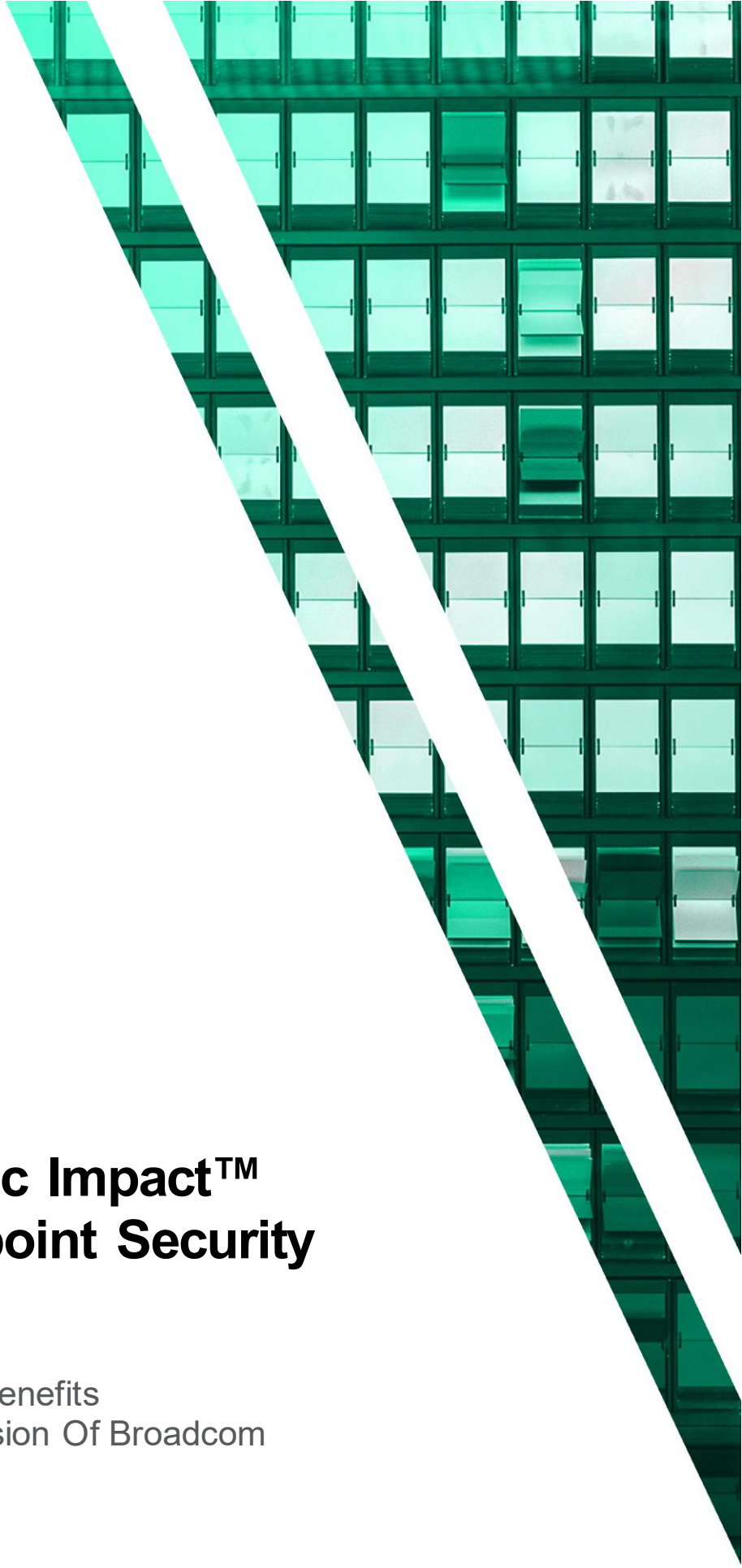
FORRESTER®



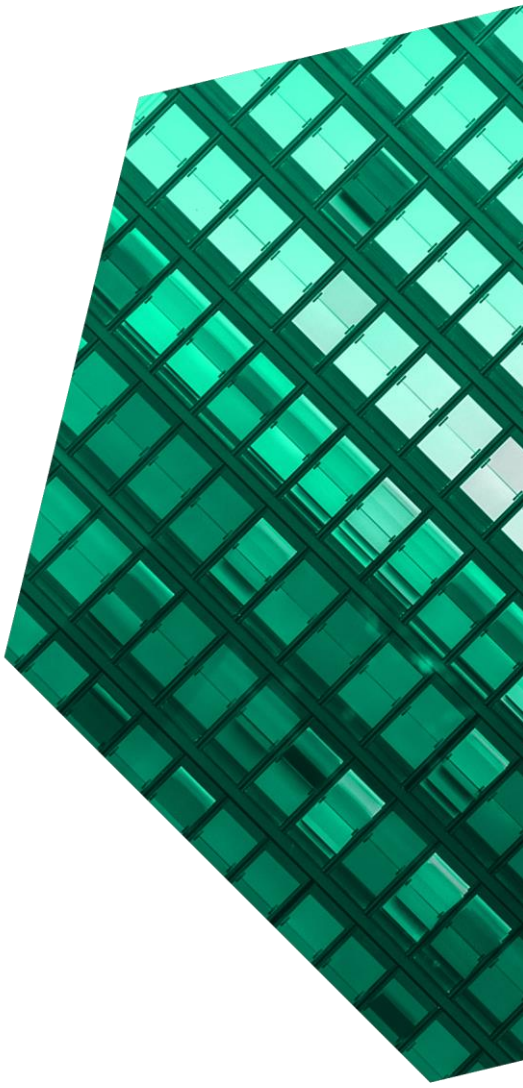
The Total Economic Impact™ Of Symantec Endpoint Security Complete

Cost Savings And Business Benefits Enabled By Symantec, A Division Of Broadcom

SEPTEMBER 2021

Table Of Contents

Consultant: *Rachel Ballard*



Executive Summary

Managing endpoint protection is a vital task for today's security analysts. Large enterprises often have thousands of endpoints to monitor and protect, and they need accurate assessments in real time to best eliminate cyber threats before they become attacks. A comprehensive strategy with broad coverage, centralized control, and efficient remediation is essential to protect against the increasing incidences and sophistication of malware and ransomware.

Symantec Endpoint Security (SES) Complete offers endpoint protection against malware and ransomware attacks with a centralized, user-friendly platform that can be managed as on-premises, cloud-based, or as a hybrid solution. The single agent solution provides protection, detection, and response across a broad range of virtual and physical devices. The IT security team can monitor thousands of endpoints and customize application configurations, while leveraging multiple layers of protection. Detected threats are quickly contained and remediated, and historical and ongoing security assessments provide users with relevant information for both internal and external audits.

Deploying an effective security plan gives customers and stakeholders confidence and serves as a tool for attracting new investment. The streamlined user interface and increased efficiencies allow security and IT staff to focus on higher-level tasks.

Total cost avoidance of a security breach:

$3.5 million

KEY STATISTICS

Return on investment (ROI)
437%

Net present value (NPV)
$4.4M

Broadcom commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Symantec Endpoint Security Complete.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of SES Complete on their organizations.

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

With SES Complete, we're seeing a whole heap of activity that we never knew was even happening. We have at least 1,000% improvement in terms of visibility and detection.

— Managing director, consumer credit company

Prior to using SES Complete, the interviewees noted how their organizations relied on on-premises or software-as-a-service (SaaS) solutions with signature-based protection combined with manual threat hunting and remediation. They lacked the efficiencies needed to manually cover the large number of endpoints and growing risk of sophisticated threats.

After the investment in SES Complete, the interviewees' organizations have greater protection with an automated, streamlined, and effective endpoint solution. Key results from the investment include the cost avoidance of a security breach, the consolidation and simplification of the organization's security stack, and efficiencies in remediation time.

KEY FINDINGS

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

- **Avoided security breach costs of nearly $3.5 million.** The interviewees reported that the consolidated platform of SES Complete and its robust suite of features, including multiple technologies for attack prevention, endpoint detection and response (EDR), active directory threat defense, threat hunter, and adaptive protection, allows their organizations to replace multiple manual processes and provide greater coverage and protection. With a breach sometimes costing an organization several million dollars, Forrester calculated that the increased efficacy of the SES Complete solution allows an organization to avoid an average of $1.25 million per year. The three-year risk-adjusted present value (PV) of this benefit totals nearly $3.5 million.
- **A consolidated and simplified security stack, leading to savings of over $1.1 million.** Upon adoption of the SES Complete solution, add-on endpoint protection tools were no longer required. Since the implementation of SES Complete, interviewees commented that their organizations now spend 10% less on other security application licenses. With an average total spend of $5 million, the annual savings is $500,000 per year. The three-year, risk-adjusted PV of this benefit is just over $1 million.

- **Increased efficiencies in remediation time, leading to a savings of over $775,000.** With the improved automation the EDR feature provides, information bottlenecks caused by the need for manual attention and intervention are greatly reduced. This automation means only the highest priority threats require intervention. Additionally, the solution's visibility and analytics addresses issues proactively, allowing security and IT team members to focus on more strategic tasks. The combined annual savings is more than $300,000 per year, resulting in a three-year, risk-adjusted PV of over $775,000.

Consolidation and simplification of security stack:

$1 million

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

- **Increased employee empowerment.** The security team members experience an increased satisfaction while performing their jobs after the SES Complete investment. The solution provided them with more valuable information with which to work, allowing them to proactively react in the areas of threat identification and remediation.
- **The ability to contain new types of threats.** SES Complete has the ability to monitor unknown threats, suspicious behavior, exploits, and potential breaches. These abilities allow the team to effectively detect attack vectors and address suspicious security activity before they become successful ransomware attacks.
- **Improved visibility.** SES Complete offers consolidated platform management that supports organizations across the entire endpoint environment. Security teams can see broad endpoint activity and take actionable steps in real time as needed.

Costs. Risk-adjusted PV costs include:

- **Annual subscription fee costs of under $1 million.** SES Complete customers pay an annual subscription fee based on the number of managed endpoints. For the composite organization, the annual $400,000 subscription cost results in a three-year, risk-adjusted PV of under $1 million.
- **Initial and ongoing costs of less than $10,000.** Initial costs include implementing new features and training team members accordingly. Ongoing costs include internal management of one FTE for an average of one day per month. The total three-year PV of initial and ongoing costs equals less than $10,000.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $5.4M over three years versus costs of $1.0M, adding up to a net present value (NPV) of $4.4M and an ROI of 437%.

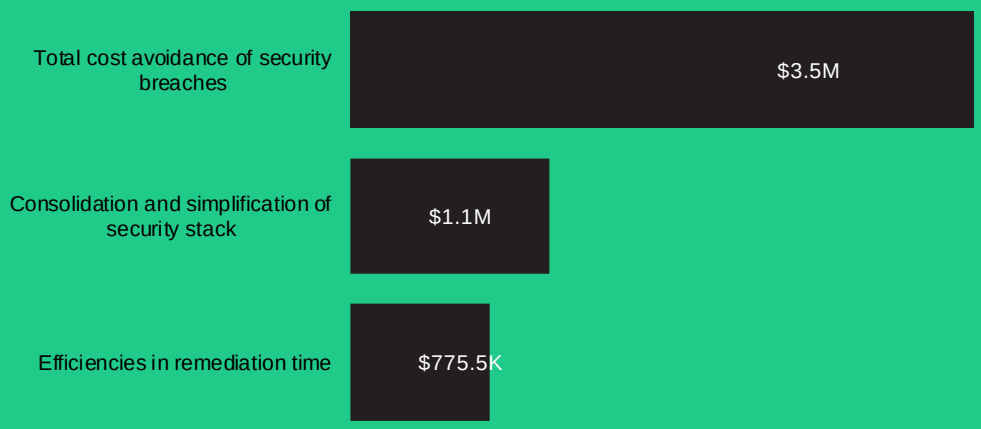
ROI
437%

BENEFITS PV
$5.4M

NPV
$4.4M

PAYBACK
<6 months

Benefits (Three-Year)



Greater endpoint coverage protects organizations from real, embedded risks such as direct financial loss, damaged brand reputation, lost productivity, and fractured regulatory relationships.

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in SES Complete.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that SES Complete can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DUE DILIGENCE

Interviewed Broadcom stakeholders and Forrester analysts to gather data relative to SES Complete.

DECISION-MAKER INTERVIEWS

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

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

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

The Symantec Endpoint Security Complete Customer Journey

Drivers leading to the Symantec Endpoint Security Complete investment

Interviewed Decision-Makers		
Interviewee	**Industry**	**Organization description**
Consulting security architect	Retail banking	Annual revenue of over $2 billion
Senior IT security consultant	International department of finance	Annual budget of over $61 billion
Managing director	Consumer credit	Manages credit information for more than 1 billion people and businesses
Chief manager, cyber and information security division	National bank	Maintains 180 million customers

KEY CHALLENGES

The interviewees previously secured their organizations' endpoints with a combination of third-party tools and in-house solutions. Many threats required manual attention for assessment and remediation. They sought greater coverage, streamlined and automated management, and a more efficient method for remediation.

The interviewees noted how their organizations struggled with common challenges, including:

- **Lack of automated detection and remediation processes.** The decision-makers reported their organizations used various systems to identify potential threats in their previous endpoint environments. Often, by the time an issue was detected, several days had passed and then several additional days were required to properly assess and rectify any damage. Even for the organizations that had not yet fallen victim to an attack or breach, without sufficient visibility and control needed for adequate protection, security teams operated in constant fear of a crippling attack.
- **Decentralized endpoint protection management.** As potential threats continued to evolve, security teams found themselves with a collection of tools acquired over time for various endpoint management functions and goals. Organizations lacked a single console from which the greater endpoint environment could be managed. As security teams gradually migrated their endpoint security programs to the cloud, organizations needed a single, consolidated platform that could effectively monitor all endpoints during the transition. The complexity of the required oversite across multiple decentralized platforms proved inefficient and was difficult to effectively manage.
- **Need for accurate and timely data.** The interviewees reported that their organizations lacked the ability to capture a clear, real-time picture of their security postures as required by compliance, regulatory, and internal security policies.

"We needed a single pane of glass from which we could manage the configuration, as well as see all the alerts, remediations, and activities."
Consulting security architect, retail banking

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Provide a single agent endpoint management tool.
- Offer an automated threat detection and remediation solution for an enterprise organization, eliminating most manual processes.
- Expand visibility, coverage, and security event prevention.
- Facilitate shift to cloud-based monitoring.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Deployment characteristics. The composite organization is a multinational financial services corporation protecting 25,000 endpoints. Its operations include an extensive digital network with over 20,000 employees, contractors, and connected third parties.

Key assumptions

- **Global financial services organization**
- **25,000 endpoints**
- **90 real threats identified per year**
- **2.5 days saved per real threat**

"Symantec offers us all the features that we need in a very solid form. We get complete information reports from endpoint to source, as well as excellent real-time detection and response. When a threat is identified, we can address it from one centralized location for all of our endpoints."
Senior IT security consultant, international department of finance

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Total cost avoidance of security breaches	$1,405,574	$1,405,574	$1,405,574	$4,216,722	$3,495,454
Btr	Consolidation and simplification of security stack	$450,000	$450,000	$450,000	$1,350,000	$1,119,083
Ctr	Efficiencies in remediation time	$311,850	$311,850	$311,850	$935,550	$775,525
	Total benefits (risk-adjusted)	$2,167,424	$2,167,424	$2,167,424	$6,502,272	$5,390,062

TOTAL COST AVOIDANCE OF SECURITY BREACHES

Evidence and data. The massive volume of proprietary data enterprise organizations receive requires constant monitoring for suspicious activity. Automating the monitoring process with SES Complete saves time and resources. Potential threats are identified more quickly, and the events that are handled automatically are assessed and rectified in real time.

- SES Complete gives organizations a comprehensive and real-time snapshot of endpoint activity. One managing director noted: "The detect capability is many times stronger than what we had before. The visibility we have now compared to what we had before shows just how shockingly compromised we were from a risk perspective. SES Complete is a game changer for us when it comes to preventing future breaches."
- The same interviewee noted: "With SES Complete, we are aware of the snooping type of malware that we could not see previously. Not only can we see it now, but we can also understand the full extent of the threat and how to eliminate it."

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization employs 20,833 FTEs.
- The composite organization manages 25,000 endpoints.
- Forrester's proprietary, internally developed security model calculates the average cost of a security breach to total $1,260,968.[2]

"Since implementing SES Complete, we are saving millions of dollars through added efficiencies, removal of manual processes, and the general reduction of resources needed to run the security operations."
Consulting security architect, retail banking

Risks. The total cost avoidance of a security breach will vary with:

- The baseline security strength, exposure, and posture of the organization.
- The skill and salary levels of the organization's security team.
- The organization's size, industry, and location.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of nearly $3.5 million.

Total Cost Avoidance Of Security Breaches

Rf.	Metric	Source	Year 1	Year 2	Year 3
A1	Total FTEs	Composite	20,833	20,833	20,833
A2	Total endpoints	Composite	25,000	25,000	25,000
A3	Base cost of breach, adjusted for composite size	Forrester research	$1,260,968	$1,260,968	$1,260,968
A4	Subtotal: Total external cost of a security breach	A3	$1,260,968	$1,260,968	$1,260,968
A5	Time required to secure endpoints	Assumption	0.25	0.25	0.25
A6	Fully loaded annual salary of a cybersecurity analyst	Assumption	$100,100	$100,100	$100,100
A7	Subtotal: Total internal cost of productivity loss	A2*(A5/2080)*A6	$300,781	$300,781	$300,781
At	Total cost avoidance of security breaches	A4+A7	$1,561,749	$1,561,749	$1,561,749
	Risk adjustment	↓10%			
Atr	Total cost avoidance of security breaches (risk-adjusted)		$1,405,574	$1,405,574	$1,405,574
	Three-year total: $4,216,722		**Three-year present value: $3,495,454**		

CONSOLIDATION AND SIMPLIFICATION OF SECURITY STACK

Evidence and data. Prior to implementing SES Complete, interviewees used a combination of resources for endpoint protection. SES Complete allowed the security team to eliminate the need for other tools, significantly reducing its annual security spend.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The previous annual spend on endpoint security solutions totaled $5 million.
- The composite organization realized 10% in savings after implementing SES Complete.

Risks. The total consolidation and simplification of the security stack benefit will vary with:

- The desired endpoint protection and coverage.
- The number of legacy tools.
- The cost of legacy tools.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of over $1.1 million.

Consolidation And Simplification Of Security Stack

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Previous annual license spend	Interviews	$5,000,000	$5,000,000	$5,000,000
B2	Percent decrease in license spend	Interviews	10%	10%	10%
Bt	Consolidation and simplification of security stack	B1*B2	$500,000	$500,000	$500,000
	Risk adjustment	↓10%			
Btr	Consolidation and simplification of security stack (risk-adjusted)		$450,000	$450,000	$450,000
	Three-year total: $1,350,000			**Three-year present value: $1,119,083**	

EFFICIENCIES IN REMEDIATION TIME

Evidence and data. In its previous environment, most threats required manual intervention and often required work on individual endpoints. With the SES Complete EDR feature, threats are detected and remediated automatically. They are then rated and triaged based on the organization's configuration. Only those requiring high-level attention are flagged for team review, while the lesser threats are captured and handled without the need for attention.

- With immediate access to all information surrounding the threat, the security team can expedite the remediation process. One interviewee noted: "With fewer potential threats requiring attention, we have eliminated the detection and remediation bottleneck that existed in our previous system. Now, only the highest priority threats require attention, indicated along with the relevant analytics that make the remediation process much more efficient and effective."

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization receives 7.5 real threats per month.
- The composite organization saves 2.5 days in the remediation process.
- Four security analysts are required to remediate each real threat.
- The fully loaded, annual salary of a security analyst totals $100,100.

Risks. The total efficiencies in remediation time will vary with:

- The skill level, efficiency, and salaries of analysts.
- The security posture and exposure of the composite organization.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of nearly $776,000.

Efficiencies In Remediation Time

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of real threats per year	7.5 per month*12 months	90	90	90
C2	Time saved per real threat (days)	Assumption	2.5	2.5	2.5
C3	Number of cybersecurity analysts required per real threat	Interviews	4	4	4
C4	Fully loaded annual salary of a cybersecurity analyst	Assumption	$100,100	$100,100	$100,100
Ct	Efficiencies in remediation time	C1*(C2/260)*C3*C4	$346,500	$346,500	$346,500
	Risk adjustment	↓10%			
Ctr	Efficiencies in remediation time (risk-adjusted)		$311,850	$311,850	$311,850
	Three-year total: $935,550			**Three-year present value: $775,525**	

UNQUANTIFIED BENEFITS

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

- **Increased employee empowerment.** With SES Complete's powerful suite of features, the security team is more proactive and effective. The IT security consultant noted: "We have moved from 68% to 83% in terms of employee empowerment. Employees feel like they are no longer running blind and are not just completely reactive. The employees are also having more time to train and study for additional security certifications, which will likely lead to another significant increase in employee satisfaction."
- **The ability to contain new types of threats.** In their previous environments, interviewees noted that their organizations could only block known threats using signature-based protections. Now with SES Complete, organizations gain visibility in all the attack vectors and, in doing so, proactively block unknown threats using new tactics, techniques, and procedures. Some examples of these threats include ransomware, zero-day attacks, black-listed IP addresses, and hash values. Features like Adaptive Protection help the organization to adapt its defense posture against the latest threat in real time and without increasing the burden on operators.
- **Improved visibility.** SES Complete enables the organization to see potential threats across all endpoints from a single dashboard. As the managing director emphasized: "Our detection is probably 1,000 times better than it was previously because of enhanced visibility."

FLEXIBILITY

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

- **Enhanced proactivity.** With increased coverage and visibility, SES Complete allows organizations to be a step ahead regarding endpoint protection. A managing director reported: "We can now avoid being worried about things that we don't need to worry about, and instead focus on the issues that really matter. We now have the visibility necessary to make strategic decisions to detect, inform, protect, and contain in less time. Those savings are immediately reinvested, allowing our security team to be proactive."
- **Continued investment and innovation.** Interviewees reported that SES Complete provides the functionality needed to operate in an increasingly cloud-based environment. A consulting security architect commented: "SES Complete's suite of features is at the forefront, and they are constantly making improvements. They are moving in the right direction in terms of innovation, roadmap, reputation, cost, and otherwise."
- **Strengthened external stakeholder relationships.** Having a strong security strategy in place helps organizations solidify their reputations with external stakeholders, such as customers and regulatory partners. The managing director noted: "The ability to quantify and qualify what is being done by the firm to protect the firm's assets enables us to enhance our brand as one that is mature and safe. This enhanced data also allows us to stay on the right side of our internal and external audit and regulatory friends."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Annual subscription cost	$0	$400,000	$400,000	$400,000	$1,200,000	$994,741
Etr	Initial and ongoing costs	$7,277	$970	$970	$970	$10,187	$9,689
	Total costs (risk-adjusted)	$7,277	$400,970	$400,970	$400,970	$1,210,187	$1,004,430

ANNUAL SUBSCRIPTION COST

Evidence and data. The interviewees revealed the following about their organizations' use of SES Complete:

- The annual subscription cost totals $400,000.
- The composite organization manages 25,000 endpoints.

Risks. The total annual subscription cost will vary with:

- The size of the enterprise and number of endpoints the enterprise manages.
- The type and extent of endpoint coverage an organization seeks.

Given Broadcom's simple pricing structure, Forrester did not risk-adjust this cost category, which yielded a three-year, total PV (discounted at 10%) of under $1 million.

Annual Subscription Cost						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Number of protected endpoints	Interview		25,000	25,000	25,000
D2	Cost per endpoint per year	Interview		$16	$16	$16
Dt	Annual subscription cost	C1*C2	$0	$400,000	$400,000	$400,000
	Risk adjustment	0%				
Dtr	Annual subscription cost (risk-adjusted)		$0	$400,000	$400,000	$400,000
	Three-year total: $1,200,000			**Three-year present value: $994,741**		

INITIAL AND ONGOING COSTS

Evidence and data. The interviewees revealed the following about their organizations' use of SES Complete:

- Initial costs the composite organization incurs included the internal labor required for implementation and the training of the team on new product features.
- Ongoing costs include management of the SES Complete platform and relationship.

> **"With SES Complete, we are able to do more with less. We are realizing a significant productivity gain."**
>
> *Managing director, consumer credit company*

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The implementation of SES Complete features requires one FTE for one full day.
- Seventeen team members spent one full day on initial training.
- Ongoing management requires one day per month for one FTE with a fully loaded salary of $100,100.

Risks. Initial and ongoing costs will vary with:

- The skill level and experience of the security engineering and IT teams.
- The salary levels, depending on skillset or geographical location.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of under $10,000.

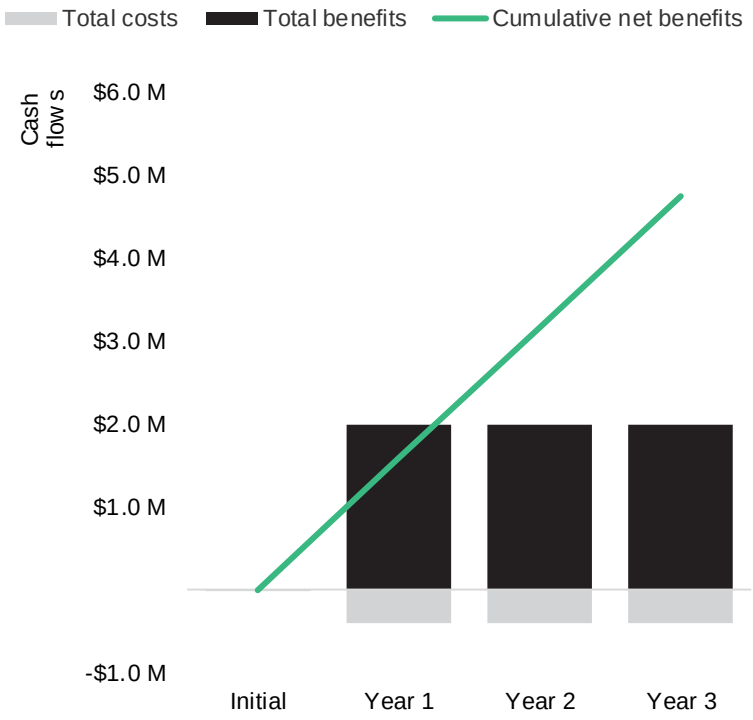
Initial And Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Implementing new features	(1 day/260)*$100,100 salary	$385			
E2	Alerting and training team members on new features	(1 day/260)*17 team members*$100,100 salary	$6,545			
E3	Ongoing management	((1 day per month*12 months)/260)*$100,100 salary*20%		$924	$924	$924
Et	Initial and ongoing costs	E1+E2+E3	$6,930	$924	$924	$924
	Risk adjustment	↑5%				
Etr	Initial and ongoing costs (risk-adjusted)		$7,277	$970	$970	$970
	Three-year total: $10,187		**Three-year present value: $9,689**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash flow analysis (risk-adjusted estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($7,277)	($400,970)	($400,970)	($400,970)	($1,210,187)	($1,004,430)
Total benefits	$0	$2,167,424	$2,167,424	$2,167,424	$6,502,272	$5,390,062
Net benefits	($7,277)	$1,766,454	$1,766,454	$1,766,454	$5,292,085	$4,385,632
ROI						437%
Payback period (months)						<6

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."

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: Endnote

[1] 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.
[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.


FORRESTER®