

FORRESTER®

The Total Economic Impact™ Of SentinelOne Cybersecurity Platform

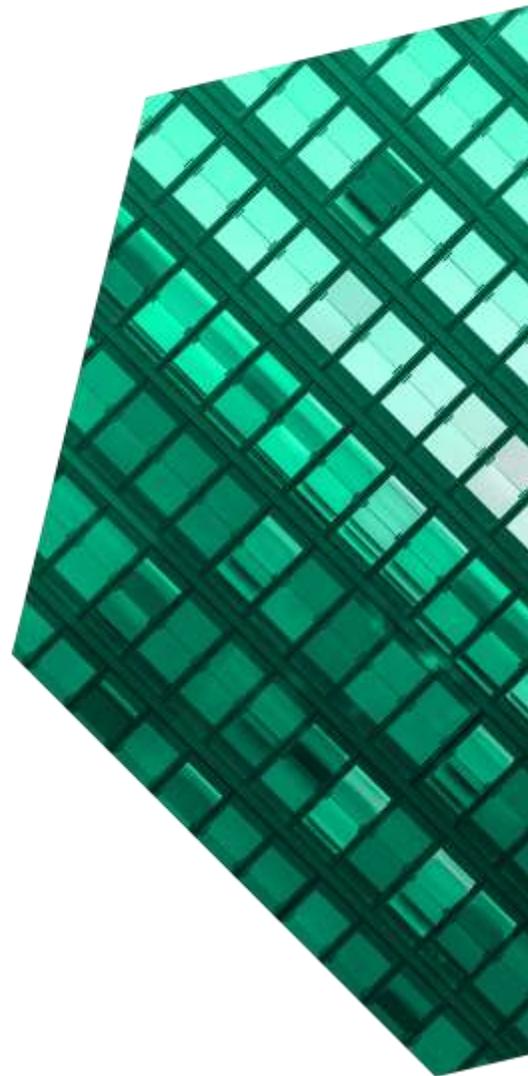
Cost Savings And Business Benefits
Enabled By SentinelOne

OCTOBER 2020

Table Of Contents

Consultant: *Rachel Ballard*

- Executive Summary 1**
- The SentinelOne Customer Journey 6**
 - Key Challenges 6
 - Solution Requirements/Investment Objectives 7
 - Composite Organization 8
- Analysis Of Benefits 9**
 - Gains Through Consolidation With Increased Coverage 9
 - Total Endpoint Issue Resolution Time Saved10
 - Reduced Risk Of Successful Malware And Ransomware Attacks.....12
 - Legacy Solution Maintenance Time Saved.....13
 - Unquantified Benefits.....14
 - Flexibility15
- Analysis Of Costs16**
 - Annual Subscription Fee.....16
 - Initial And Ongoing Costs17
- Financial Summary19**
- Appendix A: Total Economic Impact.....20**



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

© 2020, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

Global enterprises managing thousands of user endpoints across various devices are increasingly susceptible to the rising threat of criminal malware and ransomware activity. Successful attacks can be costly and result in customer data loss, diminished brand reputation, customer attrition, and ultimately loss of revenue. SentinelOne provides a comprehensive solution to protect endpoints by automatically detecting and resolving sophisticated cyberthreats and eliminating vulnerable entry and egress points.

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

SentinelOne is a cloud-based cybersecurity platform that goes beyond providing signature-based protection and offering real-time AI-behavior-related context tracking and detection to proactively prevent threats before they materialize and giving visibility for long-term investigations and incident responses. The solution is an antivirus endpoint protection platform (EPP) partnered with endpoint detection and response (EDR) that significantly expands threat coverage across all endpoints, virtual desktop infrastructure (VDI) workstations, servers, and cloud workloads. In addition, it provides real-time monitoring and automated remediation, which mitigates cyber-risk and allows security and IT staff to focus on higher-level tasks.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with several years of experience using SentinelOne. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single [composite organization](#).

KEY STATISTICS



Return on investment (ROI)

353%



Net present value (NPV)

\$4.1M

Prior to using SentinelOne, the customers relied on on-premises, signature-based antivirus tools that provided 50% coverage because the solutions were reactive instead of preventive. Cybersecurity staff charged with manual and time-consuming threat hunting and remediation had little visibility into their organization's overall threat exposure, leaving their environment susceptible to attack.

Gains through consolidation with increased coverage:

\$3.0 million



KEY FINDINGS

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

- **Gains through consolidation with increased coverage.** The interviewees reported that SentinelOne's consolidated platform increased their coverage from 50% to 100% while simultaneously reducing cybersecurity platform subscription fees. SentinelOne allowed the organizations to replace their various legacy systems with a single-agent solution that doubled their threat coverage to 100%. With an average annual savings of more than \$1 million, the three-year, risk-adjusted present value (PV) of this benefit is nearly \$3 million.
- **Total endpoint issue resolution time saved.** Engineering and IT desktop teams spend less time searching, remediating, and fixing the effects of cyberattacks. When issues are identified, SentinelOne gives visibility to the root cause, including an attacker's ingress, egress, and lateral actions. Attack recovery is simple and designed to be an automated, single-click operation, which promotes efficiencies as coding is not required to replay and reverse an attacker's steps. The combined annual savings is more than \$500,000 per year, resulting in a three-year, risk-adjusted PV of \$1.2 million.

“SentinelOne gives us coverage and visibility across our entire global entity, stopping security threats before they can enter. I’ve been in this business for 25 years, and I’ve never seen anything like it.”

Enterprise security architect, global workforce solution

- **Reduced risk of successful malware and ransomware attacks.** SentinelOne's threat detection through AI-generated behavior analysis

can neutralize many cybersecurity concerns before they enter an organization's digital environment. The EDR component can identify continuously morphing malicious code, providing a second layer of threat protection to a less complex, first-line, signature-based endpoint protection tool. Before adopting the solution, the organizations were left exposed to unpredicted malware and ransomware attacks. Interviewees reported an average of one episode per year, requiring \$300,000 to resolve and resulting in a PV savings of \$671,000 over three years.

- **Legacy solution maintenance time saved.** The legacy solutions the interviewed organizations employed were on-premises, stacked solutions that required frequent, time-consuming upgrades as well as significant management and maintenance time. Most interviewees said they completely replaced their more cumbersome on-premises solutions with SentinelOne's single platform that can be managed with fewer FTE hours. The average savings reported is 300 FTE hours per month, resulting in a risk-adjusted value of approximately \$400,000 over three years.

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

- **Increased cybersecurity team satisfaction.** As SentinelOne's EDR component continuously works to detect, predict, investigate, and remediate attacker behavior, the rate of false positives drops. The result is less mundane cleanup work for the team, allowing it to dedicate its energy to more rewarding, forward-looking security projects. Additionally, remediation can scale because organizations can rectify multiple identical attacks with one click.
- **Tailored, expert customer service.** Interviewees reported high satisfaction with SentinelOne's robust level of support, citing upgrades, troubleshooting, and maintenance

activities as efficient and effective. They added that the platform seamlessly handles seasonal spikes in cyberthreat activity, fluctuating endpoint totals, aging desktop machines, outdated operating systems, and the short-term need to maintain a parallel antivirus legacy solution during SentinelOne deployment.

- **A unified, cloud-based solution.** SentinelOne offers a software-as-a-service (SaaS) solution that allows the customer and its endpoint users flexibility regarding physical location and access while still maintaining vigilance. System updates and access adjustments are streamlined without the need to physically access endpoints.

Costs. Risk-adjusted PV costs include:

- **Annual subscription fee.** The composite organization pays a yearly subscription fee of \$400,000, resulting in a three-year, risk-adjusted PV of \$1 million.
- **Initial and ongoing costs.** Initial costs include internal FTE hours required to manage a pilot program, to implement and roll out the solution, and to train security and IT desktop users within the organization. Ongoing costs include internal management equaling 20% of one FTE. The total three-year, present value of initial and ongoing costs is \$171,000.



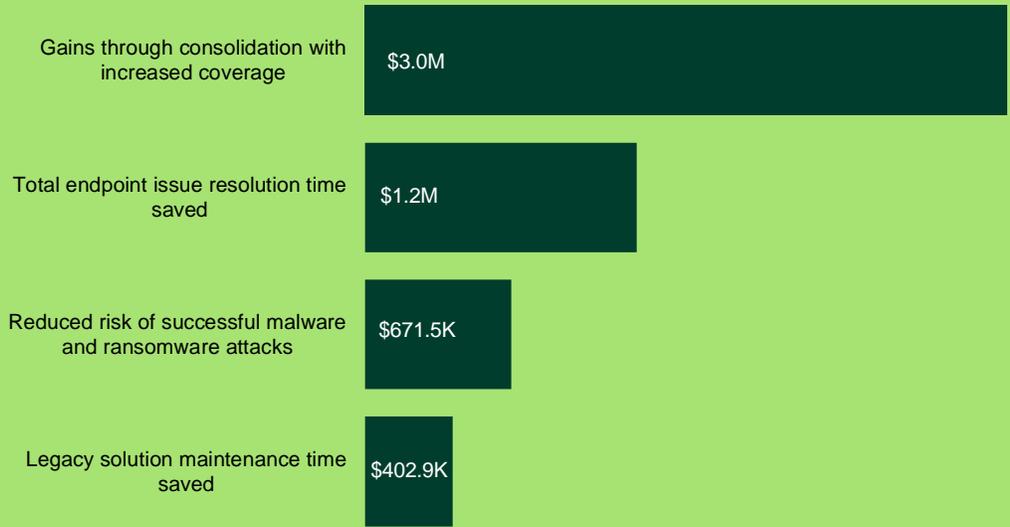
Total endpoint issue resolution time savings:


\$1.2 million

The customer interviews and financial analysis found that the composite organization would experience benefits of \$5.3 million over three years versus costs of \$1.17 million, adding up to a net present value (NPV) of \$4.1 million and an ROI of 353%.



Benefits (Three-Year)



Composite organization doubled its total threat coverage.

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 SentinelOne.

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 SentinelOne can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by SentinelOne 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 SentinelOne.

SentinelOne 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.

SentinelOne provided the customer names for the interviews but did not participate in the interviews.



DUE DILIGENCE

Interviewed SentinelOne stakeholders and Forrester analysts to gather data relative to the investment.



CUSTOMER INTERVIEWS

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



COMPOSITE ORGANIZATION

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



FINANCIAL MODEL FRAMEWORK

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



CASE STUDY

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

The SentinelOne Customer Journey

■ Drivers leading to the SentinelOne investment

Interviewed Organizations		
Industry	Interviewee title	Organization description
Digital learning platform	Security engineering manager	Operating in more than 20 countries
Global workforce solution	Enterprise security architect	41,000 employees worldwide
International restaurant group	CSO	More than 570 restaurants worldwide
Government contractor	CISO	More than \$2 billion in annual revenue

KEY CHALLENGES

The interviewed organizations previously managed cybersecurity in a reactive and localized manner that lacked centralized visibility and control. They met threat alerts after the fact with manual remediation that required unnecessary cybersecurity team and IT desktop resolution time while still leaving the organization exposed to the relentless morphing of cyberthreats. Interviewees said their organizations sought expanded detection and coverage through behavior-based analyses to complement signature-based detection.

The interviewed organizations struggled with common challenges, including:

- **Decentralized cybersecurity control centers.** With various antivirus security tools deployed across a global organization, it was difficult for a single cybersecurity team to identify, remediate, and manage all security threats and breaches. Many endpoint protection tools were physically on-premises in different stacked server locations, and each required physical space, maintenance, and regular updates.
- **Lack of automated threat detection and response.** Identified digital attacks required many internal FTE hours to locate and remediate manually. The lack of automation consumed the

security team's attention for needless hours that could have been spent performing more sophisticated cybersecurity projects.

“We wanted to move to a next-generation antivirus, anti-malware solution that would be more effective than the old signature base.”

CISO, outsourcing company

- **Limited threat coverage.** The legacy antivirus solutions were limited to signature-based detections to identify attacks. Upon detection, signature updates were triggered, which created gaps of time between identification and remediation when an organization could be exposed to further attacks.

“The nice thing with SentinelOne is that it’s watching for behavior, and it’s also doing files malware. That is huge because attacks keep getting more sophisticated, and those tend to be more damaging.”

*Manager of security engineering,
education and technology enterprise*

SOLUTION REQUIREMENTS/ INVESTMENT OBJECTIVES

The interviewed organizations searched for a solution that could:

- Provide a cloud-based solution.
- Unify EPP with EDR.
- Provide deep visibility into an attacker's behavior through remote access to user and server endpoints.

COMPOSITE ORGANIZATION

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

- The multinational organization is headquartered in the US and does business in multiple countries.
- Operations include an extensive digital network with thousands of employee and third-party endpoints connected on various devices, requiring vigilant monitoring against cyberthreats, attacks, and breaches.
- A chief information security officer (CISO) and a team manage the cybersecurity efforts across the global organization.

Key assumptions

- **Multinational corporation managing thousands of endpoints**
- **50% coverage with legacy solution**
- **100% coverage with SentinelOne**
- **Cybersecurity engineering team of 12**
- **IT desktop resolution team of 55**
- **One successful, malicious digital attack per year before the adoption of SentinelOne**

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	Gains through consolidation with increased coverage	\$1,188,000	\$1,188,000	\$1,188,000	\$3,564,000	\$2,954,380
Btr	Total endpoint issue resolution time saved	\$502,200	\$502,200	\$502,200	\$1,506,600	\$1,248,897
Ctr	Reduced risk of successful malware and ransomware attacks	\$270,000	\$270,000	\$270,000	\$810,000	\$671,450
Dtr	Legacy solution maintenance time saved	\$162,000	\$162,000	\$162,000	\$486,000	\$402,870
	Total benefits (risk-adjusted)	\$2,122,200	\$2,122,200	\$2,122,200	\$6,366,600	\$5,277,597

GAINS THROUGH CONSOLIDATION WITH INCREASED COVERAGE

Evidence and data.

- By implementing SentinelOne’s single-console solution, the organization was able to increase its protection level with fewer technology and labor resources. Legacy platforms became obsolete within a reasonable period, reducing the company’s total annual cybersolution subscription fees.
- Other than SentinelOne, the organization did not require other new to meet its EPP and EDR needs, avoiding additional fees. In fact, it was able to eliminate some third-party endpoint agents to simplify the security stack.
- One interviewee noted: “SentinelOne is collecting a lot more information now than just virus activity. We can internally monitor and widely protect. . . . We know where a user is going because SentinelOne is tracking the websites they’re visiting and the processes that are running.”

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

- The legacy system’s annual subscription cost totaled \$660,000 at 50% threat coverage.

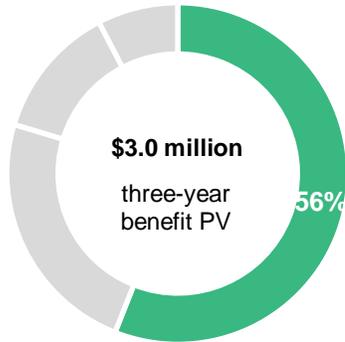
Risks. The subscription fee savings and coverage gains will vary with:

- The annual cost of an organization’s legacy cybersecurity solutions.
- The level of coverage the legacy cybersecurity solutions provided.
- The organization’s size, industry, and location.

“SentinelOne enabled us to get rid of legacy systems and have a more effective, consolidated platform with fewer associated costs.”

CSO, restaurant group

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of \$2,954,380.



Gains through consolidation with increased coverage

Gains Through Consolidation With Increased Coverage					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Cost of legacy solution at 50% coverage	\$660,000/50%	\$1,320,000	\$1,320,000	\$1,320,000
At	Gains through consolidation with increased coverage	B1	\$1,320,000	\$1,320,000	\$1,320,000
	Risk adjustment	↓10%			
Atr	Gains through consolidation with increased coverage (risk-adjusted)		\$1,188,000	\$1,188,000	\$1,188,000
Three-year total: \$3,564,000			Three-year present value: \$2,954,380		

TOTAL ENDPOINT ISSUE RESOLUTION TIME SAVED

Evidence and data.

- SentinelOne eliminated considerable time spent by security engineers and IT desktop staff resolving detected endpoint issues. One interviewee said: “The problems we used to have required a lot more hands-on work than SentinelOne requires. SentinelOne only lets issues through that really need our direct attention.”
- Interviewed organizations increased their endpoint visibility globally, allowing them to respond to real-time alerts that required corrective action. A security team member stated: “When suspicious activity is flagged, I can see its entire history. SentinelOne is a phenomenal tool.”
- The interviewees said they saved a significant number of FTE endpoint resolution hours across the security engineering and IT desktop teams. A security engineering manager said: “We spend significantly less time now that we have SentinelOne. [We spend] 75% to 85% less time

chasing down people on the desktop team to research and clean the infected device. We just don't need to do that anymore.”

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

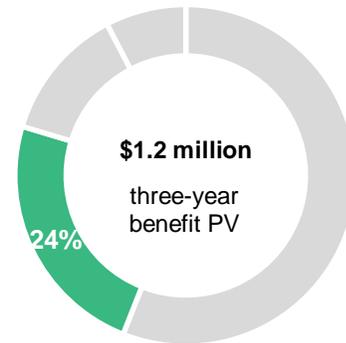
- Twelve security engineering FTEs with an average salary of \$95,000 save 20% of their time due to efficiencies gained.
- Fifty-five IT desktop support team members with an average salary of \$60,000 save 10% of their time due to efficiencies gained.

Risks The total endpoint issue resolution time saved will vary with:

- The skill level and experience of security engineers and IT desktop support staff.

- The salary levels of security engineering and IT desktop staff, depending on skillset or geographical location.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$1,248,897.



Total endpoint issue resolution time saved

Total Endpoint Issue Resolution Time Saved					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Number of security engineering FTEs		12	12	12
B2	Reduction in security engineering time resolving endpoint issues		20%	20%	20%
B3	Fully loaded security engineer salary		\$95,000	\$95,000	\$95,000
B4	Total security engineering time saved	B1*B2*B3	\$228,000	\$228,000	\$228,000
B5	Number of IT desktop support FTEs		55	55	55
B6	Reduction in IT desktop support time resolving endpoint issues		10%	10%	10%
B7	Fully loaded IT desktop support salary		\$60,000	\$60,000	\$60,000
B8	Total IT desktop support time saved	B5*B6*B7	\$330,000	\$330,000	\$330,000
Bt	Total endpoint issue resolution time saved	B4+B8	\$558,000	\$558,000	\$558,000
	Risk adjustment	↓10%			
Btr	Total endpoint issue resolution time saved (risk-adjusted)		\$502,200	\$502,200	\$502,200
Three-year total: \$1,506,600			Three-year present value: \$1,248,897		

REDUCED RISK OF SUCCESSFUL MALWARE AND RANSOMWARE ATTACKS

Evidence and data.

- SentinelOne enabled the detection of more previously undetectable threats through its AI-powered behavior analyses that can predict and prevent malware and ransomware attacks.
- After implementing SentinelOne, the interviewed organizations were no longer at risk of a successful, costly cyberattack. All the interviewees reported they have not had cybersecurity incidents, malware, or ransomware since adopting SentinelOne’s solution. A security engineering manager said, “I can now see exactly what is happening across the enterprise, and we’ve not had a single issue since implementation.”

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

- The organization previously experienced one successful malware or ransomware attack per year before adopting SentinelOne.
- Each successful attack costs the organization \$300,000 to resolve. Note that while the composite organization incurred the cost of \$300,000 to remediate the successful attack, regulatory fines and other types of breaches can potentially cost a target organization millions of dollars.

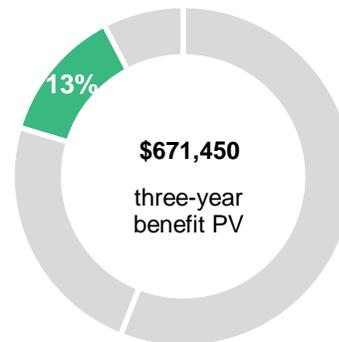


Cost to remediate a successful malware attack: \$300K

Risks. The total reduced attack risk will vary with:

- The size and sophistication of the attack.
- The skill level and experience of the cross-departmental resolution team.
- The capabilities of the legacy systems and solutions in the previous environment.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$671,450.



Reduced risk of successful malware and ransomware attacks

Reduced Risk Of Successful Malware And Ransomware Attacks

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Number of yearly malware attacks in previous environment	Interviews	1	1	1
C2	Average cost to remediate	Interviews	\$300,000	\$300,000	\$300,000
Ct	Reduced risk of successful malware and ransomware attacks	C1*C2	\$300,000	\$300,000	\$300,000
	Risk adjustment	↓10%			
Ctr	Reduced risk of successful malware and ransomware attacks (risk-adjusted)		\$270,000	\$270,000	\$270,000
Three-year total: \$810,000			Three-year present value: \$671,450		

LEGACY SOLUTION MAINTENANCE TIME SAVED

Evidence and data.

- The internal FTE hours required to maintain and upgrade the on-premises legacy EPP solution were eliminated upon the adoption of SentinelOne.
- Updates can now be pushed directly from the application, requiring less FTE time and allowing the organization to perform them more frequently. One CISO commented, “Not only are lots of hours saved, but we used to update less often because it was tedious and hard to do.”
- SentinelOne manages all maintenance and updating. A security team manager said, “All I have to do is make sure that our environment is running clean, which saves us 3,600 hours a year.”

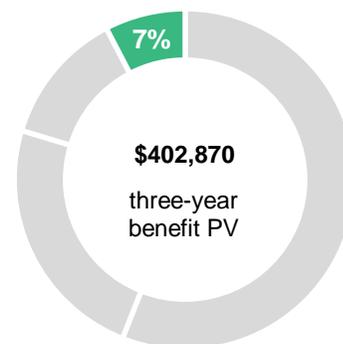
Modeling and assumptions. For the financial analysis, Forrester assumes that:

- Twelve security engineering employees save 25 maintenance hours per month each, totaling 3,600 hours saved per year.
- The security engineer's average hourly rate is \$50.

Risks. The total legacy solution maintenance time saved will vary with:

- The maintenance requirements of the previously implemented legacy solutions.
- The salary levels of security engineers, depending on their skillset or geographical location.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$402,870.



Legacy solution maintenance time saved

Legacy Solution Maintenance Time Saved					
Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Number of annual security engineering hours previously required to maintain on-premises solution	12 FTEs*25 hours per month*12 months	3,600	3,600	3,600
D2	Security engineer hourly rate		\$50	\$50	\$50
Dt	Legacy solution maintenance time saved	D1*D2	\$180,000	\$180,000	\$180,000
	Risk adjustment	↓10%			
Dtr	Legacy solution maintenance time saved (risk-adjusted)		\$162,000	\$162,000	\$162,000
Three-year total: \$486,000			Three-year present value: \$402,870		

UNQUANTIFIED BENEFITS

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

- Increased cybersecurity team satisfaction.** With the reduction in false positives and the increased automated detection and remediation of real threats, a security team member said cybersecurity team members are “able to dedicate more time to exciting projects that they care about in lieu of mundane tasks.” security Another interviewee said, “Our staff is very, very happy with the solution.”
- Tailored, expert customer service.** Interviewees noted that in addition to providing a smooth, simple transition to its solution, SentinelOne continuously incorporates customer feedback to improve and expand its offerings. A chief security officer said: “I think they're thoughtfully listening to their customers to see what other features we need. These efforts are perpetually enriching our security capabilities.”
- A unified, cloud-based solution.** As SentinelOne eliminates the need for an on-premises server, the security tool is accessible from anywhere. A cybersecurity manager can quickly access SentinelOne’s activity reports for

the organization, review potential weaknesses, and make strategic decisions regarding the security of the organization’s digital environment. As one executive mentioned: “That’s the beauty of it. For as large as my organization is, it can now really be done by one person.”

FLEXIBILITY

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

- **Time reclaimed for higher-level cybersecurity strategic planning and preparation.** With the efficiencies gained in the adoption of SentinelOne, the composite organization's cybersecurity team is now able to focus proactively on future malicious cyberattack methods and prevention, mitigating future vulnerabilities.
- **Continuous improvements in functionality.** Interviewees reported that SentinelOne is responsive to their evolving cybersecurity needs, frequently providing updates with problem-solving functionality. For example, an interviewee discussed his organization's partnership with the solution provider and commented, "With SentinelOne . . . we have seen the product mature over the years and, in turn, our metrics continue to improve."

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
Etr	Annual subscription fee	\$0	\$400,000	\$400,000	\$400,000	\$1,200,000	\$994,741
Ftr	Initial and ongoing costs	\$105,012	\$26,400	\$26,400	\$26,400	\$184,212	\$170,665
	Total costs (risk-adjusted)	\$105,012	\$426,400	\$426,400	\$426,400	\$1,384,212	\$1,165,406

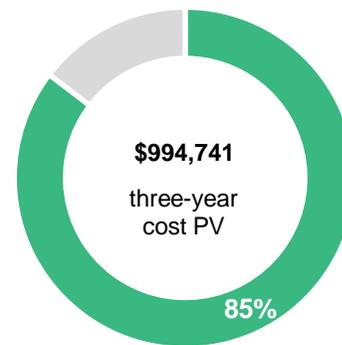
ANNUAL SUBSCRIPTION FEE

Evidence and data.

- For a large, multinational organization with thousands of endpoints, the annual subscription fee totals \$400,000.

Risks.

- Given SentinelOne's pricing structure, Forrester did not risk-adjust this cost, which yielded a three-year total PV of \$994,741.



Annual subscription fee

Annual Subscription Fee						
Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Annual subscription fee			\$400,000	\$400,000	\$400,000
Et	Annual subscription fee	E1	\$0	\$400,000	\$400,000	\$400,000
	Risk adjustment	0%				
Etr	Annual subscription fee (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.

- Initial costs included a one-month pilot program to fully understand the solution’s features and to tailor the tool to the organization’s specific security needs. Initial costs also entailed an implementation and rollout period of three months, as well as an 8-hour end-user training for a combined IT desktop and security engineering group.
- Ongoing maintenance of the SentinelOne platform required 10% of the time of one full-time security engineer.

“SentinelOne covers our whole environment. We’re seeing a lot more data for a lower price than our legacy system.”

Manager of security and engineering, education and technology enterprise

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

- The SentinelOne pilot program, or proof of concept (POC) period, calls for 50% dedicated time of six security engineer FTEs earning a fully loaded annual salary of \$110,000 each.
- The implementation and rollout phase is three months, and it requires 50% dedicated time of

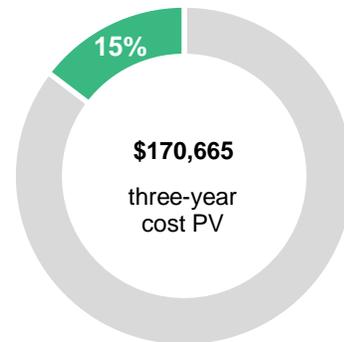
three security engineer FTEs earning a fully loaded annual salary of \$110,000 each.

- A cybersecurity engineering team of 12 and an IT desktop resolution team of 55 earning a weighted average rate of \$35 per hour receive 8 hours of SentinelOne user training.
- Ongoing management of the solution necessitates 20% of the time of one security engineer earning a fully loaded annual salary of \$110,000.

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 20%, yielding a three-year, risk-adjusted total PV of \$170,665.



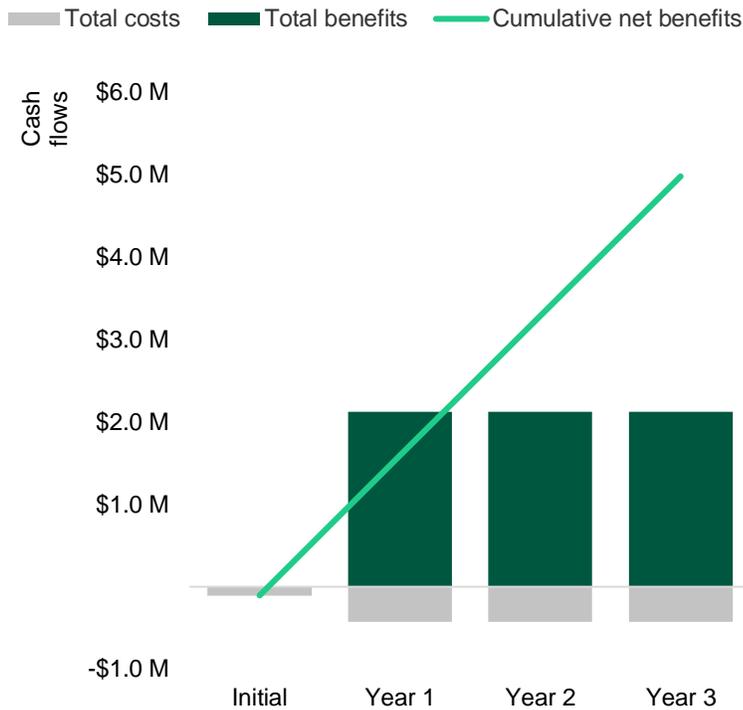
Initial and ongoing costs

Initial And Ongoing Costs						
Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Pilot	1 month per 12 months*6 FTEs*\$110,000 per year*50% time	\$27,500			
F2	Implementation and rollout	3 months per 12 months*3 FTEs*\$110,000 per year*50% time	\$41,250			
F3	Training	67 security and IT desktop support staff*8 hours*\$35 per hour	\$18,760			
F4	Ongoing management	1 FTE* \$110,000 per year* 20% time		\$22,000	\$22,000	\$22,000
Ft	Initial and ongoing costs	F1+F2+F3+F4	\$87,510	\$22,000	\$22,000	\$22,000
	Risk adjustment	↑20%				
Ftr	Initial and ongoing costs (risk-adjusted)		\$105,012	\$26,400	\$26,400	\$26,400
Three-year total: \$184,212			Three-year present value: \$170,665			

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	(\$105,012)	(\$426,400)	(\$426,400)	(\$426,400)	(\$1,384,212)	(\$1,165,406)
Total benefits	\$0	\$2,122,200	\$2,122,200	\$2,122,200	\$6,366,600	\$5,277,597
Net benefits	(\$105,012)	\$1,695,800	\$1,695,800	\$1,695,800	\$4,982,388	\$4,112,191
ROI						353%
Payback period (months)						<3

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.

FORRESTER®