A Forrester Total Economic Impact™
Study Commissioned By Splunk
February 2020

The Total Economic Impact™ Of Splunk For Security Operations

Cost Savings And Business Benefits Enabled By Splunk Security Solutions

FORRESTER®

Table Of Contents

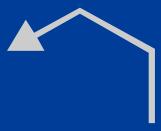
Project Director:
Mark Lauritano

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Benefits



Improved platform uptime:
$1,902,442

Improved compliance efficiency:
$567,002

Savings from security automation:
$520,773

Executive Summary

Built upon Splunk's powerful platform for machine data, Splunk Enterprise Security (ES) and Splunk User Behavior Analytics (UBA) enable IT and security operations centers (SOCs) to identify, analyze, and mitigate advanced cyberthreats. Splunk commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Splunk security solutions. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Splunk ES and UBA on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with years of experience using components of Splunk's security solutions. The combination of advanced security analytics, machine learning, automation, and orchestration technologies increases the efficiency of the SOC's existing security tools and resources while reducing an organization's exposure to risk. In addition, the centralized view of system metrics, logs, and other machine data across the organization enables IT operations teams to detect anomalies and prevent infrastructure problems in real time.

Prior to using Splunk security solutions, the customers struggled to keep up with security monitoring, incident backlogs, and alerts. Attempts to improve performance yielded limited success, because the volume of data was overwhelming and customers lacked the necessary skilled professionals required to analyze incidents and filter out false-positive alerts. These limitations led to poor response times to real threats and greater exposure to operational and security risks.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are for a composite organization that is representative of the benefits experienced by the companies interviewed:

- **Eliminated more than 3.5 hours of platform downtime per year.** The composite organization had become increasingly dependent upon its rapidly expanding digital platform for revenue growth. Needing a better method to monitor the platform's performance and automatically address alerts, the IT operations team deployed the Splunk machine data platform embedded in ES. Over three years, the subsequent improvement in platform uptime was worth more than $1.9 million to the organization.
- **Reduced resources dedicated to security audits and other compliance reporting by 50%.** With Splunk's security solutions, the security team simply granted senior management and auditors access to cyber performance reports and then walked them through the process of viewing the findings. The three-year cumulative savings in resources for the organization totaled $567,002.
- **Decreased the cost of a breach by 37%.** The analytics-driven security information and event management (SIEM) and security orchestration, automation, and response (SOAR) technologies provide an automated response capability that shortens the lifecycle of a breach. By reducing the time to identify and contain a breach, the organization saved $520,773.

ROI
81%

Benefits PV
$3.8 million

NPV
$1.7 million

Payback
<3 months

- **Improved efficiency of threat-hunting tasks by 50%.** The tight integration between Splunk UBA and ES improved customers' advanced and insider threat detection capabilities and reduced the incidence of false positives. The improved efficiencies in threat detection saved the organization $378,380 over three years.
- **Improved efficiency of threat containment tasks by 75%.** The Splunk ES ready-to-use dashboards, correlated searches, automation, and reports in combination with third-party threat intelligence feeds speed up remediation efforts. The three-year savings from improved efficiencies in threat response saved the organization $283,785.
- **Enabled consolidation of existing security products.** After implementing Splunk's security solutions, the organization was able to eliminate some integrated modules from network firewalls, producing a three-year savings valued at $136,822.

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

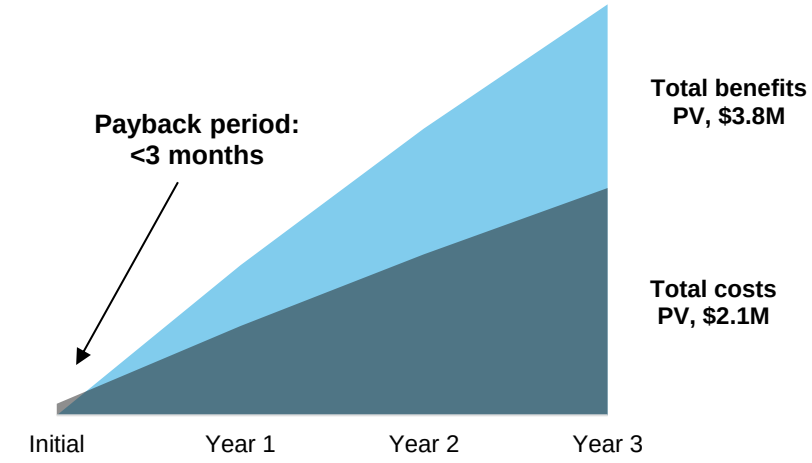
- **Enhanced visibility across the IT infrastructure.** Splunk ES brings together operating system logs, firewall logs, and endpoint alerts into single location. As a result, organizations could more easily correlate searches across multiple areas.
- **Expedited response time for system queries.** The interviewed organizations frequently cited the benefits of the prebuilt dashboards contained in the security solutions. This saved programing resources and improved the security operation teams' ability to respond to queries.
- **Enhanced security infrastructure integration with Splunk Phantom**. Forrester was unable to capture the enhanced automation capabilities introduced by Phantom, as the interviewed customers had yet to deploy this recent addition to Splunk security solutions.

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

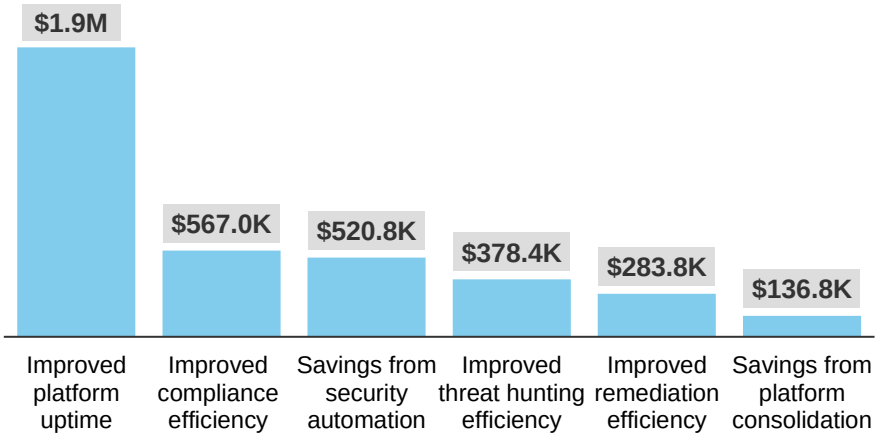
- **Splunk ES and UBA licensing fees over three years, totaling $1.6 million.** Fees are based in part upon the volume of data ingested by the SIEM. The composite organization had provisions for a maximum of 300 GB per day, which increased by 2% each year.
- **Hardware and system software license fees, totaling $391,679 over three years.** The costs are based upon the infrastructure needed to support a Splunk security solutions on-premises implementation.
- **Costs to configure and implement Splunk ES and UBA of $107,856**. The cost included the effort of three employees applying 25% of their time to the project for four weeks.

Forrester's interviews with six existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $3.8 million over three years versus costs of $2.1 million, adding up to a net present value (NPV) of $1.7 million and an ROI of 81%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Splunk security solutions.

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 Splunk ES and UBA can have on an organization:

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

DUE DILIGENCE
Interviewed Splunk stakeholders and Forrester analysts to gather data relative to Splunk security solutions.

CUSTOMER INTERVIEWS
Interviewed six organizations using Splunk ES and UBA 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 Splunk ES and UBA impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Splunk 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 Splunk ES and UBA.

Splunk 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.

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

The Splunk Security Solutions Customer Journey

BEFORE AND AFTER THE SECURITY SOLUTIONS INVESTMENT

Interviewed Organizations

For this study, Forrester conducted six interviews with Splunk ES and UBA customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE	NUMBER OF EMPLOYEES
Government agency	Headquartered in US	SOC lead	4,300
University	Headquartered in UK	Chief information and digital officer	4,500
Healthcare	Headquartered in US	VP and CIO	1,000
Restaurant	Headquartered in US	IT director	65,000
IT service provider	Headquartered in US	CISO	200
IT service provider	Headquartered in US	President and CEO	9

Key Challenges

Prior to implementing Splunk ES and UBA, many of the interviewed customers experienced poor response times to real threats and increasing exposure to operational and security risks. Interviewees attributed those challenges to the following issues:

- **Absence of a unified platform for security analytics.** Customers struggled to ingest and correlate data from disparate sources and then needed additional assistance to build custom reports for threat hunting or forensics. As a result, they couldn't detect modern threats and therefore increased business risks.
- **Limited resources to address security and IT operations monitoring needs.** With security and IT talent at a premium, customers sought a platform that could meet multiple needs: SIEM, operations monitoring, and applications development support. This allowed them to avoid hiring/training specialists for three different toolsets.
- **Poor workflow management and with limited automation.** Interviewees found that their security teams were mostly reactive and spent too many hours combing through logs. To become more proactive, security teams needed better visibility across endpoints, networks, and applications. They also sought to leverage a platform with advanced detection AI and machine learning that supported automation and orchestration capabilities.

> "Prior to Splunk, my analysts had 17 nonrelated logins to access the needed data. Now all of our OS logs, all of our firewall logs, everything is going to one place. So, we're able to do correlated searches across multiple areas, and we don't need to have 20 logins."
>
> *SOC lead, government agency*

FORRESTER®

Solution Requirements

The interviewed organizations searched for a solution would be easy to use and familiar to team members and that also could:

- Provide a flexible search capability with the ability to build queries and dashboards quickly.
- Deliver a strong analytic engine for running correlations and that supported AI and machine learning for predictive analysis.
- Offer a central platform for all aspects of security, including single repository-based analytics.
- Run security user behavior analytics for finding malicious insiders and compromised accounts.
- Offer the flexibility to be deployed on-premises, in the cloud, or in a hybrid environment.

> "The flexibility of the search capability was a big driving factor for us. It's really easy to search within Splunk and look for data and quickly identify things."
>
> *SOC lead, government agency*

Key Results

The interviews revealed that key results from the Splunk security solutions investment include:

- **Earlier detection of threats.** The speed of threat detection is critical to organizations, because the longer it takes to discover a threat the more damage it can potentially inflict. The SOC lead shared: "Our security posture has significantly improved because we are able to view activity in near-real time, when it's coming from the servers, and correlate to different data points in one location. Splunk's security solutions make things much, much easier to quickly see and react to things you identify."
- **More rapid response and mitigation of advanced threats.** Interviewees indicated that damage from advanced threats was avoided or limited by leveraging the auto-response and automation capabilities in Splunk ES to disrupt cyberattacks in progress. Using contextual information and visual insights, users were able to prioritize their response to advanced threats.
- **Reduction in false-negative and -positive alerts.** The advanced analytics and machine learning algorithms in Splunk's security solutions enhance the ability to distinguish between normal behavior and anomalies. The VP and CIO for the healthcare company disclosed, "After deploying Splunk ES and UBA, the number of false positives was drastically reduced, leading to a 60% to 80% improvement in meeting our SLAs."
- **Improved efficiency of compliance audits and reporting.** The productivity of customers' compliance activity improved significantly due to the ease of creating ad hoc queries, as well as Splunk ES performance dashboards, historical trend analysis, and post-hoc incident forensics.

> "Our security posture has significantly improved because we are able to view activity in near-real time, when it's coming from the servers, and correlate to different data points in one location. Splunk's security solutions make things much, much easier to quickly see and react to things you identify."
>
> *SOC lead, government agency*

> "After deploying Splunk ES and UBA, the number of false positives was drastically reduced, leading to a 60% to 80% improvement in meeting our SLAs."
>
> *VP and CIO, healthcare*

Composite Organization

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

- In addition to implementing Splunk's security solutions for its security team, the organization's IT operations team leveraged the solutions for network monitoring, performance management, and application analytics and reporting.
- The on-premises deployment was provisioned to ingest a maximum of 300 GB per day, which increased by 2% each year.
- On a scale of 1 to 10, the overall level of security maturity prior to the installation was in the 3-to-4 range.

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	Improved platform uptime	$765,000	$765,000	$765,000	$2,295,000	$1,902,442
Btr	Improved compliance efficiency	$228,000	$228,000	$228,000	$684,000	$567,002
Ctr	Savings from security automation	$209,411	$209,411	$209,411	$628,232	$520,773
Dtr	Improved threat-hunting efficiency	$152,152	$152,152	$152,152	$456,456	$378,380
Etr	Improved remediation efficiency	$114,114	$114,114	$114,114	$342,342	$283,785
Ftr	Savings from platform consolidation	$54,000	$55,080	$56,182	$165,262	$136,822
	Total benefits (risk-adjusted)	$1,522,677	$1,523,757	$1,524,858	$4,571,291	$3,789,204

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of nearly $3.8 million.

Improved Platform Uptime

During interviews, executives told Forrester about how they deployed Splunk as a log management and search tool for infrastructure and IT operations use cases in addition to security use cases. A company with a consumer-facing global digital platform experienced the most significant impact. The company's revenue growth was increasingly dependent upon this rapidly expanding sales channel, and IT operations needed a better solution to gain insights on application performance and platform troubleshooting.

The Splunk solution provided end-to-end insight into all the APIs, all the various cloud resources, and the third-party services that plugged into its digital platform. The customer was now in position to identify specific performance bottlenecks and anomalies. The organization also uses Splunk data to trigger automated actions such as restarting a node or stopping and starting a service. This has taken troubleshooting problems from minutes or even hours down to sub-minutes without operations team direct involvement.

To estimate the benefit from real-time IT performance monitoring, including triggers for automated actions, Forrester based its analysis on outages in the composite organization's digital platform. Reducing the length of an outage has a direct result on business revenue, brand reputation, and customer satisfaction. After implementing the Splunk solution, the typical 15-minute outage decreased to seconds.

For the financial model, Forrester also assumes:

- A 15-minute outage in the organization's digital platform reduces business revenues by $60,000.
- Prior to the deployment of the Splunk solution, the digital platform typically experienced 15 significant outages a year.

> "We have far, far better insight into the platform — our digital platform — than we ever had before. It has helped us dispel some previously held myths. It's helped us prove some things that we thought we knew. It's helped us identify problems and resolve them in seconds rather than minutes."
>
> *IT director, restaurant*

FORRESTER®

Because this benefit will apply primarily to organizations that utilize a digital platform as a sales channel and both the impact of an outage and the number of outages varies from across entities, Forrester risk-adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1,902,442.

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

Improved Platform Uptime: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Potential exposure from 15-minute outage in digital platform	Composite	$60,000	$60,000	$60,000
A2	Average number of outages per year	Composite	15	15	15
At	Improved platform uptime	A1*A2	$900,000	$900,000	$900,000
	Risk adjustment	↓15%			
Atr	Improved platform uptime (risk-adjusted)		$765,000	$765,000	$765,000

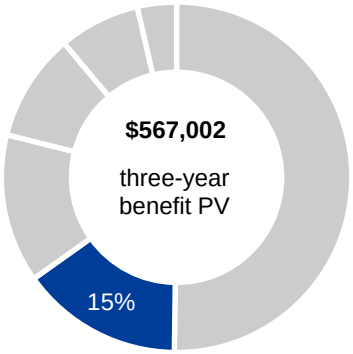
Improved Compliance Efficiencies

A primary need for all the interviewed organizations was to better manage the SOC's growing log data volumes generated by increasingly complex infrastructure. Gathering and storing log data from multiple sources was slowing down response times and impeding compliance-reporting initiatives.

Splunk's security solutions provide log storage in a format that supports compliance reporting across cloud-based and on-premises sources. Having a centralized security analytics platform with powerful search and drill-down capabilities significantly reduced the number of resources required to support compliance and general inquiries from management. The VP and CIO for the healthcare business stated, "All we need to do now is grant auditors and our cybersecurity executives access for various reports and walk them through the process, and that satisfies about 90% of our needs."

For the composite organization, Forrester assumes that two compliance reporting resources (50% of the original team) were freed up following the implementation of Splunk ES and UBA.

While all the interviewed companies use their SIEM to support compliance, the complexity and resources dedicated to compliance reporting varied. To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $567,002.



Improved compliance efficiency: **15%** of total benefits

FORRESTER®

Improved Compliance Efficiency: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Number of workers (saved)	Composite	2	2	2
B2	Yearly rate per person	Assumption	$120,000	$120,000	$120,000
Bt	Improved compliance efficiency	B1*B2	$240,000	$240,000	$240,000
	Risk adjustment	↓5%			
Btr	Improved compliance efficiency (risk-adjusted)		$228,000	$228,000	$228,000

Savings From Security Automation

A major driver for investment in a security analytics platform is the ability to leverage automation tools that help to lower an organization's exposure to risk. Advanced AI and machine learning enable modern SIEMs to recommend next steps and SOAR technologies to automate actions to speed investigations and remediation.

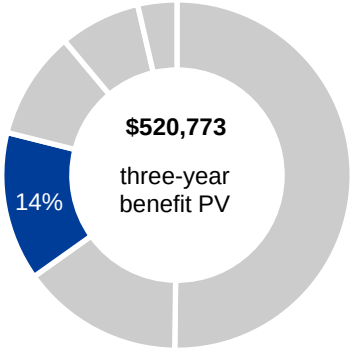
Interviewed customers utilized Splunk ES and UBA to reduce dwell time or the period between malware executing within an environment and its being detected. For example, with Splunk's SOAR technologies, an organization can automate detection and investigation, enabling the system to generate alerts that trigger specified responses. The chief information and digital officer for the university summarized the benefits of automation: "The joy of Splunk is that it's enabling us to automate and ply through data logs at a speed that we'd nowhere be able to do as human beings. By dashboarding, we can see the real key components in our network as they might be starting to fail or suffer from a symptom of a cyberattack."

The Ponemon Institute's 2019 Cost of a Data Breach Report examined the role that security automation plays in the reduction in risk exposure. Among the 507 organizations studied, those that deployed automated security solutions saw significantly lower costs after experiencing a data breach. In fact, organizations that hadn't deployed security automation experienced breach costs that were 95% higher than breaches at organizations with fully deployed automation ($5.16 million average total cost of a breach without automation versus $2.65 million for fully deployed automation).[i]

The Forrester model is based in part on the Ponemon Institute's study of the relationship between the data breach lifecycle (the time elapsed between when an organization is breached and the time the breach is contained) and costs associated with a breach. Security automation plays a direct role in reducing the lifecycle. For the model, Forrester assumes:

- After deploying Splunk's tightly integrated ES and UBA solutions, the composite organization's data breach lifecycle or mean-time-to-detect (MTTD) plus mean-time-to-respond (MTTR) to a breach is less than 200 days. Under the prior environment, the data breach lifecycle was greater than 200 days.
- The average cost of a data breach is as reported by the Ponemon 2019 study, adjusted to match the size of the composite organization.

> "The joy of Splunk is that it's enabling us to automate and ply through data logs at a speed that we'd nowhere be able to do as human beings. By dashboarding, we can see the real key components in our network as they might be starting to fail or suffer from a symptom of a cyberattack."
>
> *Chief information and digital officer, university*



Savings from security automation: **14%** of total benefits

FORRESTER®

› The probability of experiencing a data breach of 30,000 records over the next two years is 14.9%.

The degree of automation put in place will vary from customer to customer as will the length of the data breach lifecycle. To account for this risk, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $520,773 .

Savings From Security Automation: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Average cost of a breach (MTTI + MTTC>200 days)	Ponemon	$5,836,800	$5,836,800	$5,836,800
C2	Average cost of a breach (MTTI + MTTC<200 days)	Ponemon	$4,275,200	$4,275,200	$4,275,200
C3	Average probability of a 30,000-record breach in next 24 months	Ponemon	14.9%	14.9%	14.9%
Ct	Savings from security automation	(C1-C2)*C3	$232,678	$232,678	$232,678
	Risk adjustment	↓10%			
Ctr	Savings from security automation (risk-adjusted)		$209,411	$209,411	$209,411

Improved Threat-Hunting Efficiency

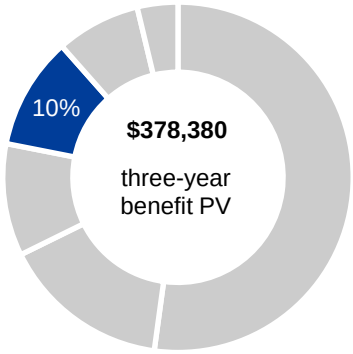
The sooner a threat is detected, the less damage it can inflict on an organization's digital assets. To maximize the effectiveness of threat hunting, security analysts must be able to differentiate real threats from false-positive alerts. In their prior security platforms, customers were getting bogged down addressing false-positive alerts, and they failed to recognize advance threats because their traditional SIEMs generally searched using prebuilt, rigid searches.

Splunk's ES and UBA solutions address these deficiencies by providing comprehensive visibility throughout the enterprise environment in combination with user behavior analytics and machine learning algorithms that correlate anomalous behavior for higher-fidelity behavior-based alerts. This information is then funneled through custom dashboards in real time. The interviewed healthcare organization reported a 60% to 80% drop in its false-positive alert rate.

The deployment of Splunk security solutions completely changed the interviewed university's security posture. In the words of its chief information and digital officer: "Our security posture was very reactive, very boundary-focused. Now, we are proactive, we're looking at all device activity, in a semi predicted matter. That's a huge change for us. We were blind, and now we can see."

In the financial model, Forrester calculates this benefit based upon four full-time equivalents (FTEs) from the security team who realized a 50% reduction in the hours devoted to threat hunting, compared to the previous architecture. The cybersecurity analysts converted 50% of this freed-up time to provide higher-value support to advanced threat hunting. Using an average burdened salary of $160,000, this resulted in an annual productivity benefit of $160,160.

Readers are likely to realize a range of value for this benefit depending on the staffing of their current security platform, the adaptability of the existing SIEM, the ability to view activity across the entire enterprise



Improved threat-hunting efficiency: **10%** of total benefits

"Our security posture was very reactive, very boundary-focused. Now, we are proactive, we're looking at all device activity, in a semi predicted matter. That's a huge change for us. We were blind, and now we can see."

Chief information and digital officer, university

FORRESTER®

environment, and the average salaries in a specific geography. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $378,380.

Improved Threat-Hunting Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Number of FTEs hunting threats	Composite	4	4	4
D2	Hourly rate per person (rounded)	$160,000/2,080	$77	$77	$77
D3	Percent reduction in threat-hunting tasks	Composite	50%	50%	50%
D4	Number of hours saved	D1*2,080*D3	4,160	4,160	4,160
D5	Percent captured	Assumption	50%	50%	50%
Dt	Improved threat-hunting efficiency	D2*D4*D5	$160,160	$160,160	$160,160
	Risk adjustment	↓5%			
Dtr	Improved threat-hunting efficiency (risk-adjusted)		$152,152	$152,152	$152,152

Improved Remediation Efficiency

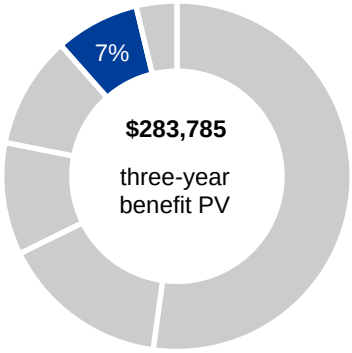
In addition to advanced threat hunting, a security analytics platform must provide the means to quickly contain a cyberattack. Customers expressed a desire for a SIEM that indicated the scope of a threat by identifying where it may have moved after being detected, how it should be contained, and how information about the threat should be shared. In addition, the platform needs to include SOAR capabilities that take SIEM alerts to the next level, analyzing the data and taking remediation steps where necessary.

Interviewees cited several reasons why they felt that Splunk ES improved their response time to attacks, such as its SOAR capabilities that can be used to disrupt cyberattacks in progress. They also appreciated the way Splunk can integrate information from all parts of the enterprise environment, including third-party threat intelligence vendors, as well as apps from Splunkbase. This provided the SOC with the context needed to quickly triage and respond to advanced threats.

The SOC lead for the government agency shared this exact use case, where one of the tools identified a file as malware and Splunk blocked it, and stopped it, and then generated an alert and sent it to another tool. That tool was then able to identify the malware on the different systems, and the agency saw all this in real time in the Splunk dashboard. The SOC lead explained: “Even with only a partial deployment of the solution, we’ve seen a 50% to 60% improvement in the speed to detect and respond to complex attacks. And now it’s going to improve even more so.”

In the financial model, Forrester calculates this benefit based upon two full-time equivalents (FTEs) from the security team who realized a 75% reduction in the hours devoted to remediation, compared to the previous architecture. The cybersecurity analysts converted 50% of this freed-up time to provide higher-value support. Using an average burdened salary of $160,000, this resulted in an annual productivity benefit of $120,120.

Readers are likely to realize a range of value for this benefit depending on the resources currently focused on remediation, the adaptability of the



Improved remediation efficiency: **7%** of total benefits

> “Even with only a partial deployment of the solution, we’ve seen a 50% to 60% improvement in the speed to detect and respond to complex attacks. And now it’s going to improve even more so.”
>
> *SOC lead, government agency*

FORRESTER®

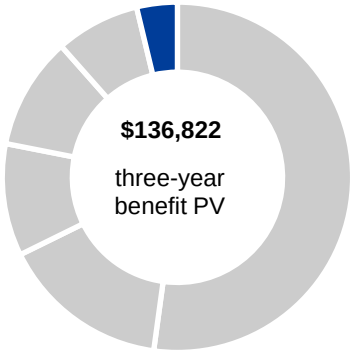
existing SIEM, the ability to view and share information across the entire enterprise environment, and the average salaries in a specific geography. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $283,785.

Improved Remediation Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
E1	Number of FTEs doing remediation	Composite	2	2	2
E2	Hourly rate per person (rounded)	$160,000/2,080	$77	$77	$77
E3	Percent reduction in remediation tasks	Composite	75%	75%	75%
E4	Number of hours saved	E1*2,080*E3	3,120	3,120	3,120
E5	Percent captured	Assumption	50%	50%	50%
Et	Improved remediation efficiency	E2*E4*E5	$120,120	$120,120	$120,120
	Risk adjustment	↓5%			
Etr	Improved remediation efficiency (risk-adjusted)		$114,114	$114,114	$114,114

Savings From Platform Consolidation

Customers found that after deploying Splunk security solutions, some of the SIEM add-ons purchased for existing security tools were no longer needed. The model assumes that the composite organization was able to remove these redundancies, generating a three-year savings equivalent to 10% of its Splunk ES and UBA license, or $152,024. Forrester risk-adjusted this benefit downward by 10% to account for readers who may realize different results. The benefit yielded a three-year risk-adjusted total PV of $136,822.



Savings from platform consolidation: **4%** of total benefits

Savings From Platform Consolidation: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
F1	Prior SIEM costs eliminated by Splunk ES and UBA (% of Splunk license)	Composite	10%	10%	10%
Ft	Savings from platform consolidation	F1*Gt	$60,000	$61,200	$62,424
	Risk adjustment	↓10%			
Ftr	Savings from platform consolidation (risk-adjusted)		$54,000	$55,080	$56,182

FORRESTER®

Unquantified Benefits

In addition to the benefits outlined above, the interviewed executives shared other benefits that did not have specific financial implications. Specifically, the companies benefited in the following ways:

- **Enhanced visibility across the IT infrastructure.** Splunk security solutions bring together operating system logs, firewall logs, and endpoint alerts into a single location. This visibility into the entire enterprise environment provides organizations the ability to quickly correlate searches across multiple areas and respond to queries. The healthcare executive shared: “My team members would say that the biggest advantage of Splunk ES is the way you can drill down through various data log sources and get what you need. Splunk has a fantastic drill-down approach.”
- **Expedited response time for system queries.** The interviewed organizations frequently cited the benefits of the prebuilt dashboards contained in Splunk ES, as well as the ability to build custom dashboards. The government agency SOC lead said: “I asked my team to build a couple of dashboards, and they were built within a day. That flexibility to work off a variety of sources paired with being able to export the data quickly, visualize it, graph it, and do stat counts in real time — just makes life easier.”
- **Enhanced security infrastructure integration with Splunk Phantom.** The study was unable to capture the enhanced automation capabilities introduced by Phantom, as the interviewed customers had yet to deploy this recent addition to Splunk security solutions.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Splunk security solutions and later realize additional uses and business opportunities, including:

- **Integrating new data and applications.** Customers indicated that the ability to expand the data and applications linked to Splunk helps to ensure that they will obtain future value. The government agency SOC lead said: “Splunk security solutions will provide benefits in the future, because you can bring new things in and they’ll integrate with ES. There are a lot of built-in or easy-to-add applications that will work with a whole bunch of products. So, you don’t need to buy a particular product’s logging solution.”
- **Evolving product strategy.** Interviewees anticipate receiving future value from Splunk based upon its corporate leadership and strategy. The president and CEO of a service provider stated: “Splunk has an evolution strategy, and they’re intending to be No. 1 forever. Their investment in product and talent acquisition gives me great confidence that things are going to continuously get better.”

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a 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.

> “Splunk has an evolution strategy, and they’re intending to be No. 1 forever. Their investment in product and talent acquisition gives me great confidence that things are going to continuously get better.”
>
> *President and CEO, service provider*

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
Gtr	License fees	$0	$630,000	$642,600	$655,452	$1,928,052	$1,596,252
Htr	Hardware and software license fees	$0	$157,500	$157,500	$157,500	$472,500	$391,679
Itr	Implementation costs	$107,856	$0	$0	$0	$107,856	$107,856
	Total costs (risk-adjusted)	$107,856	$787,500	$800,100	$812,952	$2,508,408	$2,095,787

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of $2.1 million.

License Fees

The interviewed organizations operate Splunk ES and UBA under a consumption-based pricing model. License fees are based in part upon the volume of data ingested by the SIEM. The composite organization implemented an on-premises version of the security solutions and had provisions for a maximum of 300 GB per day, which increased by 2% each year.

The final license fees will vary across organizations depending on the method of implementation and volume of data ingested by the SIEM. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $1.6 million.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

License Fees: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	License fees	Composite		$600,000	$600,000	$600,000
G2	Yearly percent increase in data	Composite		2%	2%	2%
Gt	License fees	Y1: G1 Y2/Y3: Gt_{PY}*(1+G2)	$0	$600,000	$612,000	$624,240
	Risk adjustment	↑5%				
Gtr	License fees (risk-adjusted)		$0	$630,000	$642,600	$655,452

Hardware And Software License Fees

For on-premises deployment, Splunk security solutions need to be treated like an enterprise database and software installations that require dedicated resources at all times. Forrester assumes the licensing fees for the added servers and storage to the composite organization's data center totaled $150,000 per year.

To account for any risk in variation that readers may experience in the configuration of their hardware and software running Splunk ES and UBA, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $391,679.

Hardware And Software License Fees: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
H1	License fees	Composite	$0	$150,000	$150,000	$150,000
Ht	Hardware and software license fees	H1	$0	$150,000	$150,000	$150,000
	Risk adjustment	↑5%				
Htr	Hardware and software license fees (risk-adjusted)		$0	$157,500	$157,500	$157,500

Implementation Costs

The organization employed three administrators who spent 25% of their time over four weeks integrating the data from various sources and setting up dashboards. In addition, the organization availed itself of professional services totaling $75,000 to optimize the on-premises installation.

To account for any risk in variation that readers may experience in the time required to implement Splunk security solutions, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $107,856.

Three FTEs
spent 25% of their time over four weeks implementing Splunk security solutions.

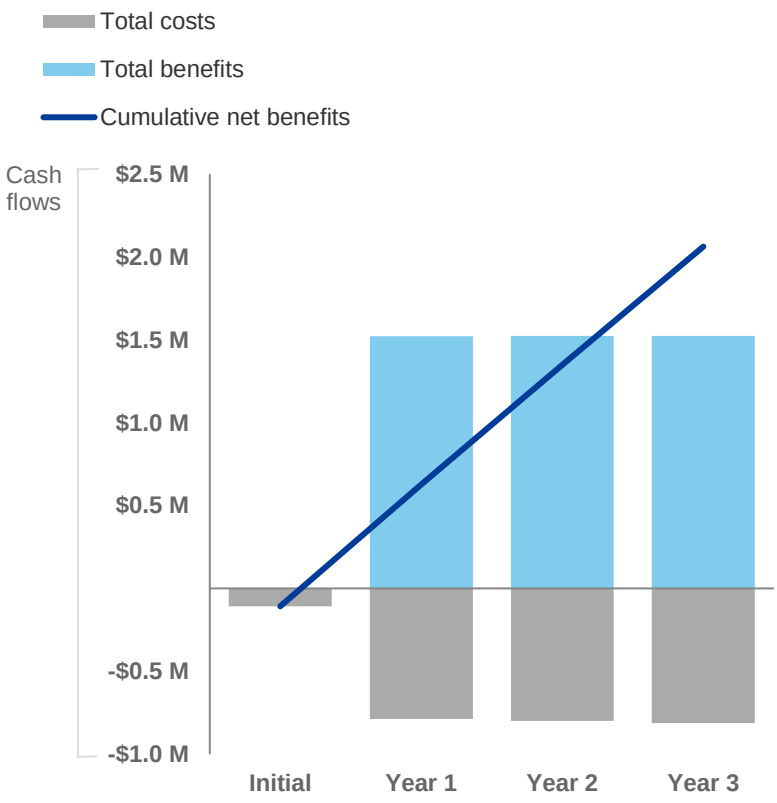
Implementation Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
I1	Number of people	Composite	3			
I2	Hourly rate per person (rounding)	$160,000/2080	$77			
I3	Hours	I1*160*25%	120			
I4	Professional services	Composite	$75,000			
It	Implementation costs	I4+I1*I2*I3	$102,720	$0	$0	$0
	Risk adjustment	↑5%				
Itr	Implementation costs (risk-adjusted)		$107,856	$0	$0	$0

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.

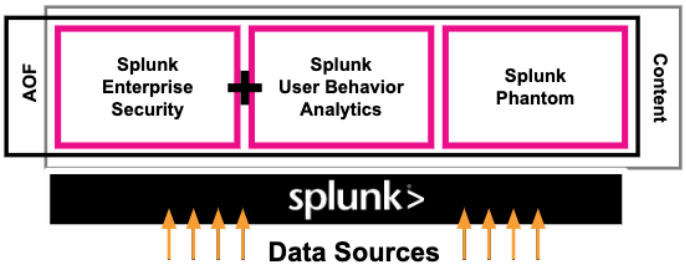
Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($107,856)	($787,500)	($800,100)	($812,952)	($2,508,408)	($2,095,787)
Total benefits	$0	$1,522,677	$1,523,757	$1,524,858	$4,571,291	$3,789,204
Net benefits	($107,856)	$735,177	$723,657	$711,906	$2,062,883	$1,693,417
ROI						81%
Payback period						<3 months

FORRESTER®

Splunk Security Solutions: Overview

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



***AOF** = Adaptive Operations Framework*

***Content** = Pre-packaged security content (searches, detection models, automation playbooks)*

The only **integrated suite** with industry-leading **SIEM**, **UEBA** and **SOAR** solutions that utilize a market-proven, scalable **big data platform**, continually augmented with actionable use case content.

splunk> turn data into doing

FORRESTER®

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[i] Source: “Cost of a Data Breach Report 2019,” a Ponemon Institute Study, Commissioned by IBM Security, 2019