Enterprise Strategy Group™
by TechTarget

ECONOMIC VALIDATION

Analyzing the Economic Benefits of Splunk Security

Mitigate Business Risk, Enhance Operational Efficiency, and Increase Insights Into the Business, All While Delivering an ROI of 267%

By Jennifer Duey
Enterprise Strategy Group

This Enterprise Strategy Group Economic Validation was commissioned by Splunk and is distributed under license from TechTarget, Inc.

Contents

Introduction 3
Challenges 3
The Solution: Splunk Security 4
Enterprise Strategy Group Economic Validation 6
Splunk Security Economic Overview 7
Reduced Business Risk 7
Improved Security Team Operational Efficiency 8
Improved Insights 8
Enterprise Strategy Group Analysis 9
Issues to Consider 11
Conclusion 11

Enterprise Strategy Group by TechTarget — Economic Validation: Key Findings Summary

Validated Benefits of Splunk Security (versus alternative security solutions)

- **Up to 30% improvement in security team productivity**
- **50% increase in alert fidelity**
- **267% return on investment (modeled)**

- **Mitigate Risk:** Splunk Security empowers security teams to improve the time to detect, triage, investigate, and remediate, reducing risk to the organizations.
- **Enhance Operational Efficiency:** Splunk optimized customers' security operations, leading to cost reductions and simplified processes. As a result, customers found that their security teams could accomplish more with a leaner team.
- **Increase Insights:** Customers were able to quickly implement, integrate, and scale their Splunk solutions into their evolving environments and processes, providing insight across the data environment.

Introduction

This Economic Validation from TechTarget's Enterprise Strategy Group is focused on the quantitative and qualitative benefits organizations can expect by using the technologies that make up Splunk Security rather than using multiple alternative point security products.

Challenges

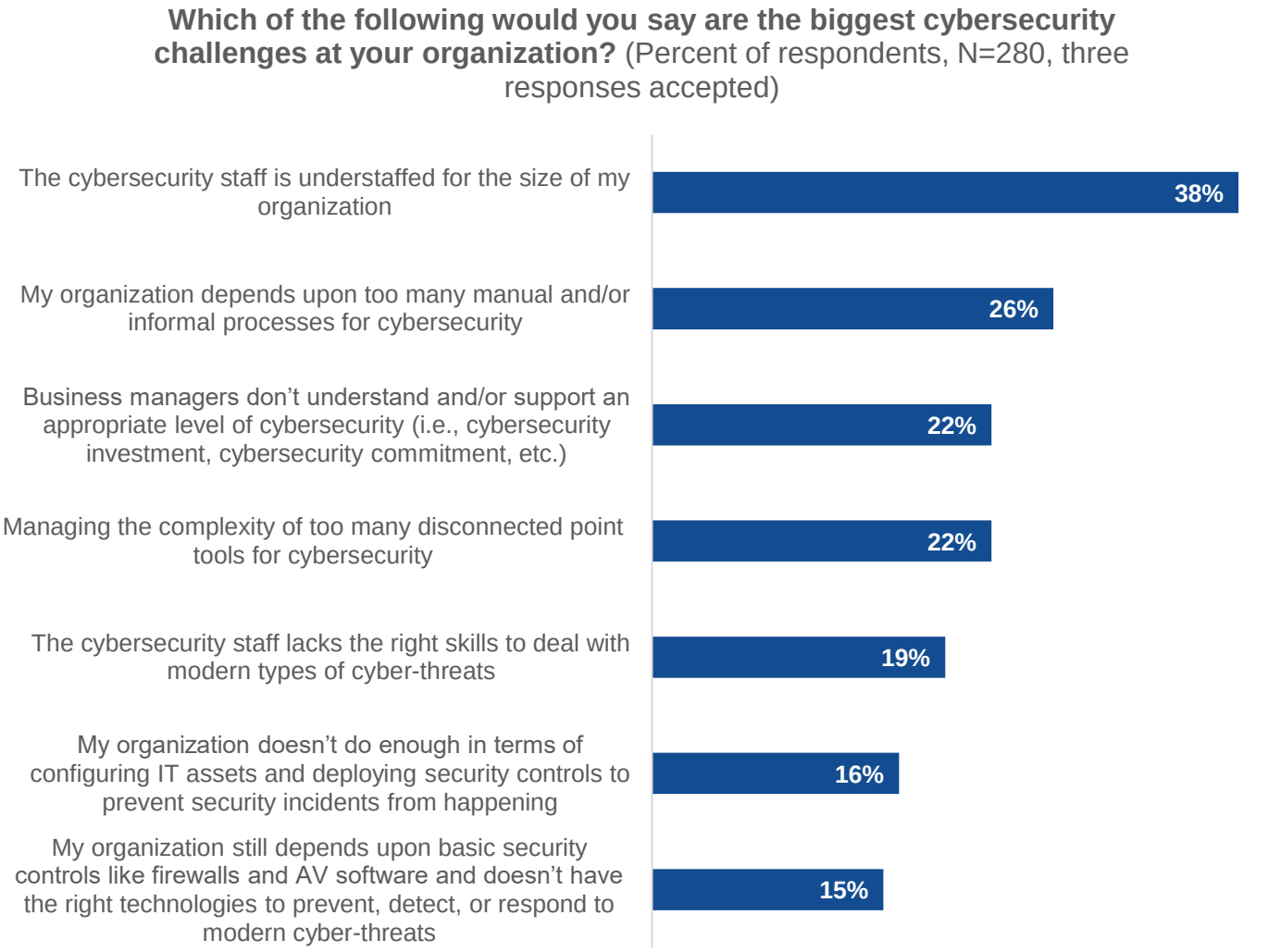
According to Enterprise Strategy Group research, 52% of surveyed respondents believe that security operations are more difficult today than they were two years ago.[1] This is no surprise, as the quantity, type, and sophistication of cyberthreats have evolved, increasing the attack surface and making it difficult for cybersecurity professionals to keep up with the pace of change. Security operations centers (SOCs) are left overwhelmed by the number of alerts received, making thorough investigations and analysis virtually impossible and delaying detection, response, and remediation. The need for skilled cybersecurity professionals leaves SOCs understaffed and open to further vulnerabilities.

Security teams need to move fast to identify, investigate, and remediate threats. However, a combination of limited security resources, too many tools, and complex workflows result in limited visibility into the attack surface, making it harder to get to the root cause. Enterprise Strategy Group research identified that some of the top cybersecurity challenges that IT teams face today include that they are understaffed for the size of their organization and have too many manual and/or informal processes for cybersecurity. Diving deeper into this list reveals that these teams are also struggling with the management of multiple point tools for cybersecurity, their staff lacking the right skills, and being dependent on basic security tools that don't have the right technologies to prevent, detect, or respond to modern cyber threats (see Figure 1).[2]

[1] Source: Enterprise Strategy Group Research Brief, *Security Operations Managed Services*, March 2023.
[2] Source: Enterprise Strategy Group Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

© 2023 TechTarget, Inc. All Rights Reserved.

Figure 1. Top 7 Cybersecurity Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To address these challenges, 40% of security leaders have identified improving cybersecurity as a top consideration for justifying IT investments over the next 12 months.[3] In an attempt to become more effective and provide adequate visibility into their IT environment, a SOC may look to integrate with various other tools and systems within an organization, such as identity and access management systems, network and application performance monitoring tools, and incident management tools. However, running multiple tools can become too costly and complex for a SOC to maintain. Effectively automating and unifying security operations enable security teams to overcome these challenges. Implementing a comprehensive and flexible security platform with automation is a requirement for the modern SOC and a sure way to strengthen its cybersecurity posture.

The Solution: Splunk Security

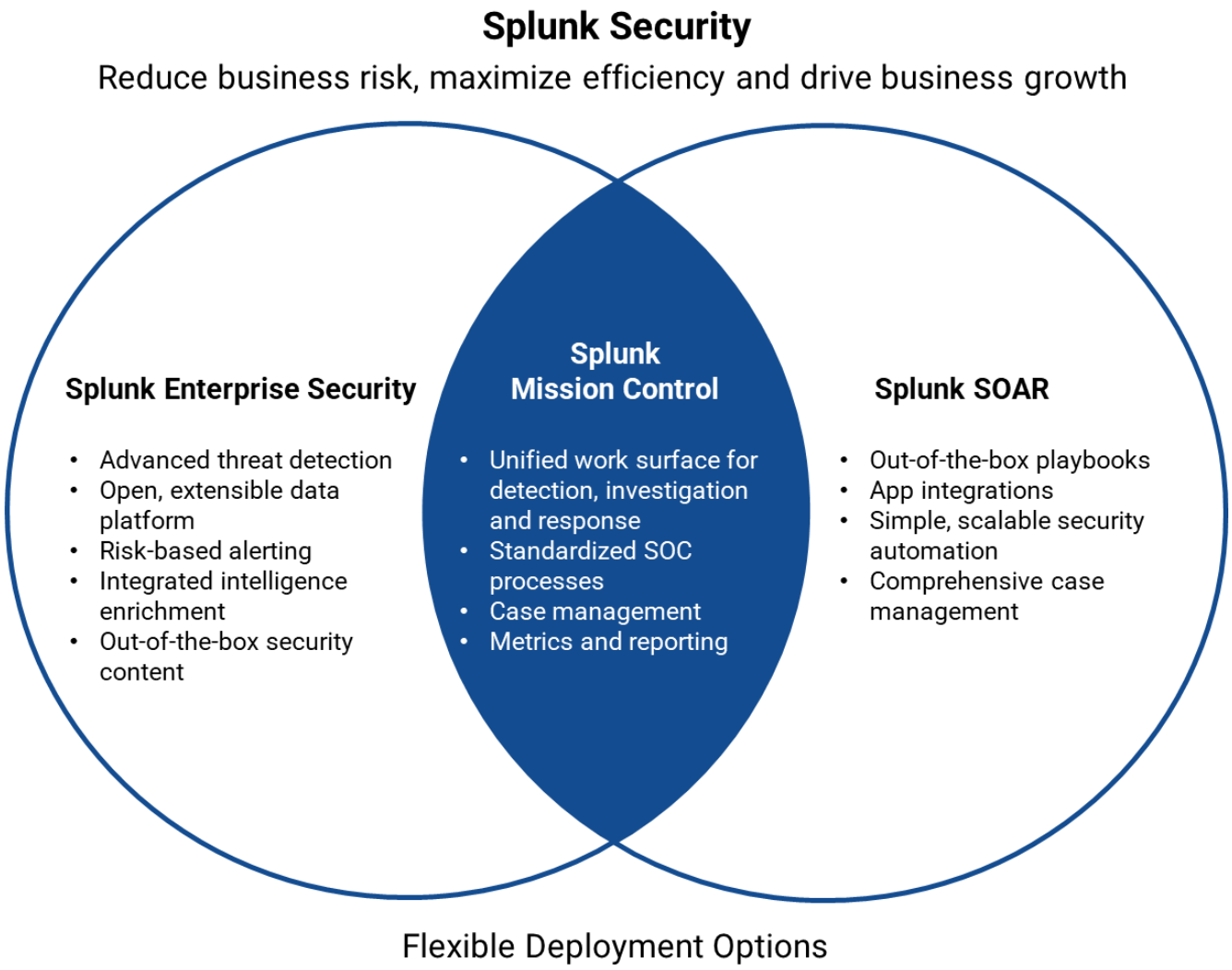
Splunk Security provides SOCs with a unified work surface to accelerate threat detection, investigation, and response. At the core is an extensible data platform for end-to-end visibility of an organization's security posture. By

[3] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

combining Splunk's security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities and workflows into a simplified security operations experience, organizations can achieve efficient integration and process execution across cloud, on-prem, and hybrid environments. This Enterprise Strategy Group analysis focuses on the following components of Splunk Security (see Figure 2):

- **Splunk Enterprise Security.** Splunk's SIEM offering is built on the Splunk platform that can ingest, normalize, and analyze at-scale data from all enterprise data sources—not only security tools but also IT and enterprise systems—so no "weak" signals are missed. Splunk Enterprise Security delivers data-driven insights for full-breadth visibility into an organization's security posture, so the organization can protect its business and mitigate risk at an enterprise scale. The risk-based alerting approach in Splunk Enterprise Security reduces alert volume and empowers security analysts to prioritize their attention on the primary targets of attackers: users and machines. With incomparable search and reporting capabilities, advanced analytics, integrated intelligence, and pre-packaged security content, Enterprise Security accelerates threat detection and investigation, letting organizations determine the scope of high-priority threats to their environment so they can quickly take action.
- **Splunk Mission Control.** An included capability of Splunk Enterprise Security, Mission Control brings order to the chaos of an organization's security operations by enabling its SOC to detect, investigate, and respond to threats from one modern and unified work surface. It unifies an organization's security operations experience across Splunk's industry-leading security technologies and partner ecosystem in one work surface. This enables organizations to better understand business risk by seeing the entire picture of security insights and trends in order to detect what matters, investigate holistically, and respond intelligently. With Splunk Mission Control, organizations can streamline their security operations by improving SOC process adherence and scale their team's productivity by fusing Splunk Enterprise Security insights with security automation.
- **Splunk SOAR.** This Splunk Security component provides security orchestration, automation, and response capabilities that enable security analysts to work smarter by automating repetitive tasks; respond to security incidents faster with automated alert triage, investigation, and response; increase productivity, efficiency, and accuracy; and strengthen defenses by connecting and coordinating complex workflows across their team and tools. Splunk SOAR also supports a broad range of SOC functions, including event and case management, integrated threat intelligence, collaboration tools, and reporting.

Figure 2. Splunk Security Overview



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group (ESG) completed a quantitative analysis of Splunk Security. ESG's process is a proven method for understanding, validating, quantifying, and modeling the value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation.

ESG conducted in-depth interviews with end users to better understand and quantify how the use of Splunk Security has impacted their organizations, particularly in comparison with previously deployed and/or experienced security solutions. ESG reviewed vendor-created technical documentation, existing case studies, and third-party analyses and leveraged our own expert analyst opinions and knowledge of the industry, markets, and alternative technologies. The qualitative and quantitative findings around time and effort savings were then used as the basis for a simple economic analysis predicting the potential operational cost savings and reduced risk for an organization.

Splunk Security Economic Overview

Enterprise Strategy Group's economic analysis revealed that by using Splunk Security, customers saw significant savings and benefits in the following categories:

- **Reduced Business Risk.** Splunk Security strengthens an organization's security posture through vigilant monitoring and adept management of its digital ecosystem, thereby reducing business risk.
- **Improved Security Team Operational Efficiency.** Splunk Security offers continual monitoring, automation, and streamlined resource utilization, improving operational efficiency.
- **Improved Insights.** Splunk Security offers the insight and automation required to provide a deeper understanding of their digital landscape.

Reduced Business Risk

By using Splunk Security, businesses can bring in information (logs) from vast sources and use machine learning to analyze and detect advanced threats. Organizations can quickly identify and mitigate cyber threats and incidents by utilizing out-of-the-box detections, reducing business risk. Customers reported savings and benefits in the following categories:

- **Faster time to detect threats.** Through Splunk's advanced analytics and real-time monitoring of capabilities, organizations found that they were able to significantly lower the mean time to detect threats. Splunk identifies anomalies, patterns, and potential threats in near real time by quickly aggregating and analyzing substantial volumes of data from various sources.

> **"With Splunk, we've achieved a remarkable mean time to detection (MTTD) of just 7 minutes - from the moment an alert is triggered until we have triaged and are taking action."**

- **Faster time to triage threats.** Splunk Security categorizes and prioritizes potential threats based on severity and relevance by rapidly comparing and analyzing diverse data streams. Intelligent automation enables security teams to focus on the most critical issues, simplifying the triage process and enabling faster decision-making and response to emerging threats. Furthermore, risk-based alerting with Splunk has increased alert fidelity and reduced alert fatigue. Customers reported that ***false positives were reduced by 50%*** since transitioning to risk-based alerting. This enables security teams to allocate resources to investigate and resolve the most crucial security incidents rather than spend time on unnecessary alert triage.

> **"We saw major improvements in alert fidelities when we implemented the first round of risk-based alerting. It's been amazing!"**

- **Faster time to investigate and remediate threats.** With the robust search capability and ability to aggregate and correlate data with Splunk, customers could quickly assemble relevant information from various sources, creating a cohesive context for security incidents. Customers reported their security teams could quickly identify the root cause of threats and determine the appropriate remediation actions ***90% faster than with their previous solution***. Additionally, customers found that Splunk's automation capabilities facilitated faster investigation and remediation by making the response process easier. When a threat is detected, Splunk SOAR can be configured to execute pre-defined response actions, eliminating manual intervention and enabling immediate and consistent efforts to mitigate threats. Customers used Splunk playbooks to expedite investigation and remediation by providing structured, predefined workflows for responding to

> **"Before Splunk, an incident could drive on for days. As we've matured with Splunk, we can seamlessly search through data at our scale without encountering delays. We can make decisions quickly, which helps us to remediate much faster."**

specific types of threats. By following these established processes, security teams can quickly and consistently address threats with precision, minimizing the impact of a security event.

Improved Security Team Operational Efficiency

Splunk Security enables security teams to handle large volumes of data efficiently, quickly detect threats, automate routine tasks, and implement effective response strategies. This holistic approach results in a more optimized and responsive team, resulting in a proactive approach to safeguarding the organization's digital environment.

- **Automation of manual tasks.** Manual tasks, such as alert triage, data enrichment, and incident response, can be time-consuming and repetitive. Automation enables these tasks to be executed rapidly and consistently, freeing up valuable time for the security team to focus on more strategic activities. Customers reported that ***with Splunk SOAR, they were able to save 90%*** of the time that was typically spent on routine tasks. With this time savings, customers could allocate their security professionals to do more strategic and complex activities that require human expertise, ultimately maximizing the value of the security team.

> **"We were able to increase our service offerings without the need to scale up our team. We've effectively accomplished more using the same resources."**

- **Reduced operational complexity.** Customers discovered that integrating Splunk led to a ***30% increase in their operational efficiency***, achieved through the reduction of operational complexity. Customers reduced their operational complexity by integrating their existing security infrastructure with Splunk and creating a unified platform for data aggregation, analysis, and automation. By funneling data from various security tools into Splunk, organizations eliminate data silos and gain a comprehensive view of their security landscape. This consolidation reduces the need to manage multiple standalone systems, optimizing security processes and resulting in improved operational efficiency, faster incident response times, and better overall security management.
- **Streamlined workflows.** Customers found that operational workflows were simplified with Splunk by arranging a centralized platform that consolidates data, analytics, and automation. By ingesting data from various sources across the digital landscape, Splunk creates a single source of truth for security-related information. The orchestration of predefined playbooks enables customers to develop repeatable processes, helping security teams identify threats faster.

> **"Splunk has simplified everything for us so much so that we have saved over 1,000 person-hours on tasks we no longer have to do."**

Improved Insights

Splunk Security delivers enhanced insights to organizations by providing advanced analytics and comprehensive data collection. This enables businesses to gain a deeper understanding of their digital environment and make informed decisions to address potential challenges and optimize their overall security posture proactively. Customers reported savings and benefits in the following categories:

- **Improved flexibility.** Customers utilized the flexibility of Splunk by leveraging its adaptable architecture and multifaceted features. Customizable dashboards and visualizations empower users to tailor insights to their specific needs, accommodating different use cases and requirements. As a result, customers were able to derive actionable insights relevant to their unique goals.
- **Improved visibility.** Splunk can ingest data from a wide variety of devices, systems, applications, and sources, including logs, events, metrics, and even structured or unstructured data. This universal data ingestion capability ensures that data from all devices is collected and made available for analysis.

"We didn't have to look in so many places anymore. Splunk allowed us to consolidate what we had and combine the telemetry from these different tools into a single view. We could see everything from network to endpoint and everything else we were building."

- **Consolidated tools.** Splunk helps its customers streamline operations by centralizing various systems into a unified platform, eliminating the need to manage multiple disparate systems. Customers reported that they were able to ***discontinue the use of approximately two or three different products*** that were previously managed manually. This eased the security infrastructure and reduced the operational burden on the security team.

Enterprise Strategy Group Analysis

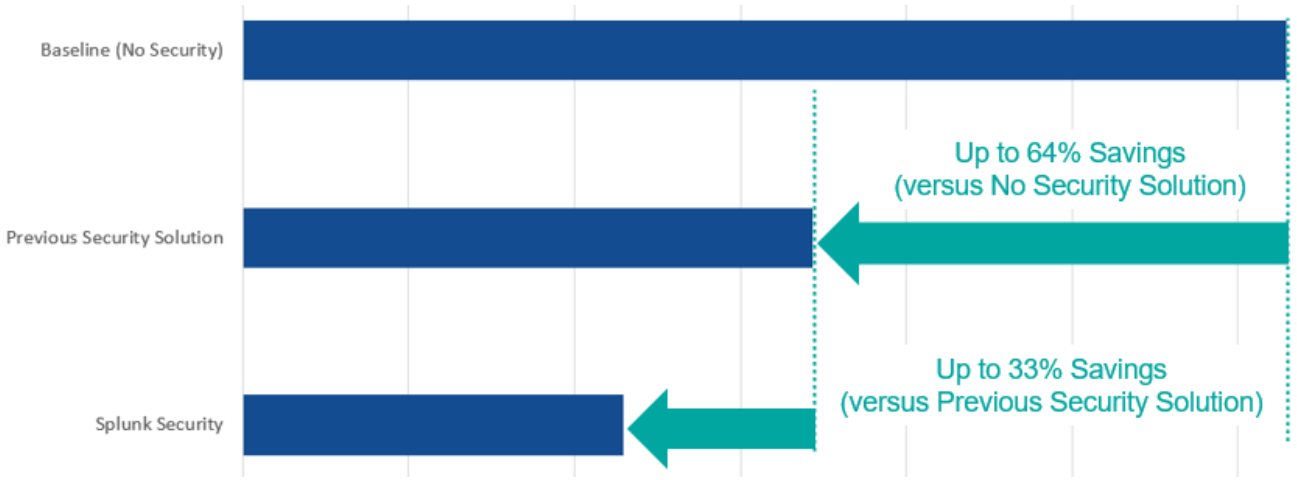
Enterprise Strategy Group (ESG) leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to report and model the expected savings and benefits customers could expect by using Splunk Security. ESG's interviews with customers who have recently made the transition, combined with experience and expertise in economic modeling and technical validation of security products, helped to form the basis for our modeled scenario.

Why This Matters

In today's rapidly evolving threat landscape, where cyber attacks are becoming more sophisticated, an effective security solution is essential for businesses to manage and mitigate security risks effectively. With the right solution, organizations can detect threats faster, respond more efficiently, maintain a strong security posture, and realize cost reductions.

ESG created a model to measure the expected costs and savings by implementing Splunk Security rather than continuing to use multiple alternative point security products. We formulated our assumptions on the premise of a composite organization that maintains an 8-person security team and processes daily data ingestion of 1TB. Based on our interviews, customers expressed that without utilizing any security solution, they would need to more than double the size of their security team. Furthermore, customers indicated that previous security solutions would require a 1/3 increase in the security team. By projecting the operational cost reductions, Splunk demonstrated potential savings of up to 64% compared to the baseline (no security solution) and a 33% cost reduction compared to an alternative security solution (see Figure 3).

Figure 3. Expected Operational Savings



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

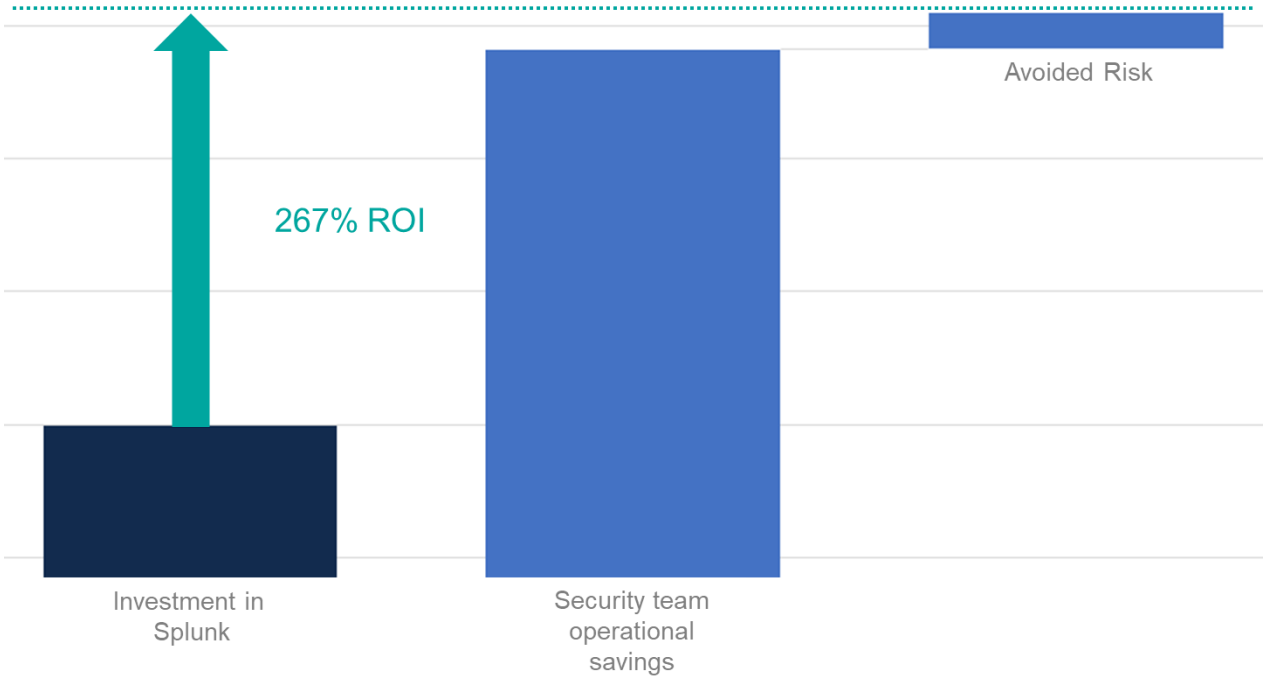
Although we could not gather specific risk reduction metrics from customers, we leveraged our proprietary models to predict a very conservative reduction in risk facilitated by Splunk compared to alternative security solutions. This reduction stems from the capability to aggregate additional data sources, extend data retention, and expedite search processes and ongoing investigations. In assessing the risk of a cybersecurity event, ESG factored in a 5% enhancement beyond the assumed 90% improvement from the previous security solution. This adjustment takes into consideration enhanced custom alerts, reduced downtime, and accelerated search capabilities. When analyzing the risk of non-compliance, ESG considered a 3% enhancement over a 20% improvement assumption from using the previous security solution based on the ability to conduct faster searches and alerting benefits. While evaluating the risk of IT downtime, ESG assumed a 10% improvement over the 50% improvement assumptions, taking into account the benefits of accelerated searches, custom alerts, and easier integrations (see Table 1).

Table 1. ESG's Modeled Expected Annual Risk

	Risk of Cybersecurity Event	Risk of Non-Compliance	Risk of IT Downtime	Splunk Security Avoided Risk
Baseline (No Security Solution)	$1.3M	$945K	$750K	
Alternative Security Solution	$128.8K	$756K	$375K	
Splunk Security	$64.3K	$728K	$300K	
Splunk Security Reduction in Risk (vs. Alternative Security Solution)	**$64.4K**	**$28.4K**	**$75K**	**$167.8K**

Combining these factors, ESG formulated an anticipated annual ROI for Splunk Security in comparison to other security solutions. The resulting ROI of 267% includes the potential benefit of avoided risk (see Figure 4).

Figure 4. Expected Return on Investment



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Issues to Consider

While Enterprise Strategy Group (ESG)'s models are built in good faith upon conservative, credible, and validated assumptions, no single modeled scenario will ever represent every potential environment. The costs and benefits received from a Splunk Security deployment will depend on the details of an organization's requirements and practices. ESG recommends that organizations perform their own analysis of available products and consult with their Splunk representative to understand and discuss the differences between the solutions through their own proof-of-concept testing.

Conclusion

Security stands as a paramount priority for all organizations. The rising spectrum of threats and an ever-expanding attack landscape pose significant challenges for security teams. With constrained budgets, attracting and retaining skilled security personnel becomes a formidable task. Therefore, it is imperative for organizations to channel investments into tools and services that mitigate risks and enable security teams to optimize efficiency and productivity within existing resource limitations.

Enterprise Strategy Group (ESG) validated through custom research and interviews with Splunk customers that Splunk Security delivers on this requirement. Our validation with Splunk Security customers revealed that, when compared to their previous security solutions, Splunk delivered cost savings, streamlined operational processes, and mitigated risk. ESG's modeled scenario predicts that Splunk Security can be effectively managed by teams up to 33% smaller compared to other alternative security solutions. Moreover, our model shows an ROI of 267%.

If your organization is looking to improve threat detection, response times, operational efficiency, and the ability to manage complex security landscapes, ESG recommends that you evaluate whether Splunk Security is right for your organizational needs.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com