October 2025
Business Value White Paper
Sponsored by Splunk and AWS

The Business Value of Splunk for Financial Services and Insurance

Stephen Elliot
Group Vice President,
I&O, Cloud Operations, and DevOps, IDC

Jerry Silva
Program Vice President,
Financial Insights, IDC

Megan Szurley
Business Value Manager,
Business Value Strategy Practice, IDC

Table of Contents

Click any title to navigate directly to that page.

Business Value Highlights

Click the to jump to related content. Use "Return to highlights" to get back to this page.

$2.2 million average annual benefit per 10,000 managed endpoints

$15.3 million in average annual benefits per organization

387% three-year ROI

13-month payback on investment

50% more efficient security operations team

86% more threats identified

53% more efficient at incident investigation

51% more efficient at threat response

18% more productive DevOps

Business Value Highlights (continued)

19% less DevOps time spent testing applications

22% more productive IT engineers

74% less time required to search across data

110% more data ingested

56% more environment monitored

Executive Summary

The banking and insurance industries are facing the challenge of managing security, applications, and infrastructure in an increasingly complex financial services environment; the rising demands for business, regulatory compliance, and operational efficiency have never been higher. The integration of security and observability from a single, unified platform supports proactive risk management, faster incident response, and continuous uptime — critical priorities for banking and insurance technology and business executives.

The financial services industry is using Splunk, a Cisco company, to support security operations, infrastructure monitoring, and compliance reporting by aggregating and analyzing machine-generated data across diverse systems to deliver proactive and predictive capabilities across traditionally fragmented processes and data. Its platform capabilities can detect anomalies, investigate incidents, and maintain visibility across complex, hybrid environments. Financial institutions rely on the platform to address challenges such as fraud prevention, regulatory compliance, service performance and availability, and digital resilience amid increasing application transaction volumes and evolving security threats. Splunk's real-time analytics empower banks and insurance clients to detect and remediate malicious activities, optimize customer experience, enable an enhanced security posture, and ensure business continuity.

This document describes the experiences of financial institutions that are using Splunk's unified platform. The report conveys an IDC study that shows how the Splunk platform enables financial organizations to streamline operations, improve incident response times, and reduce the complexity of managing multiple point solutions, creating measurable business value.

IDC conducted research that explored the value and benefits for financial services and insurance (FSI) organizations using Splunk to improve security, observability, resilience, and visibility across their IT environments.

→ Based on an extensive data set and a specialized Business Value methodology, IDC calculates that these customers will achieve benefits worth an annual average of $15.3 million per organization ($2.2 million per 10,000 endpoints managed) and a three-year ROI of 387% by:

- Helping organizations detect and respond to threats faster by improving alert accuracy and reducing false positives

- Providing unified visibility across hybrid infrastructures, enabling efficient monitoring and troubleshooting
- Strengthening fraud detection and insider threat monitoring using behavioral analytics and anomaly detection
- Supporting digital resilience and regulatory compliance by aggregating and analyzing data from diverse sources
- Consolidating legacy tools into a single platform, lowering costs and boosting team productivity

Situation Overview

The financial and insurance industry's siloed and disaggregated legacy infrastructure and application technology have increased the need for a proactive security and observability posture for achieving compliant, secure, and highly performing environments.

The financial and insurance industry's siloed and disaggregated legacy infrastructure and application technology have increased the need for a proactive security and observability posture for achieving compliant, secure, and highly performing environments. Executive pressure to reduce costs, improve efficiency across security and operational teams and processes, and gain value from agentic AI capabilities are core requirements for modern operations.

Financial and insurance organizations face highly regulated, compliance-centric operating models and requirements. These challenges require agentic AI strategies and implementation to focus on data gravity, with strict planning for data collection, access, security, and quality from a vast array of security, operational, application, and infrastructure sources. The need for executives to align agentic AI capabilities with fraud detection and prevention, regulatory compliance and audit readiness, and operational resilience is an opportunity for creating competitive differentiation and delivering personalized customer experiences.

As the rate and pace of technological innovation continue to increase, the need to continuously monitor and audit the operational environment has become paramount to driving revenue, growth, and overall transformation. Using an integrated platform for security and observability enables the streamlining of monitoring, detection, investigation, and incident remediation. This end-to-end visibility drives effective business continuity planning and regulatory alignment across teams, data, processes, and policies.

To help overcome these challenges, Splunk's security and observability solutions are playing an increasingly vital role in the financial services industry, where digital resilience, regulatory compliance, real-time operations, and customer trust are paramount (and regulatory frameworks, such as the EU's Digital Operational Resilience Act and the U.S. SEC's T+1 settlement rule, increasingly mandate them). Splunk provides a real-time monitoring and automation platform for meeting compliance and operational demands in a unified platform that enables financial institutions to detect threats, investigate incidents, and ensure system reliability across complex hybrid environments.

Splunk Overview

Splunk offers a unified security and observability platform to support financial services institutions and insurance organizations in managing increasingly complex legacy and digital infrastructures. The platform integrates observability and security capabilities, enabling organizations to collect, correlate, and analyze data from diverse sources — including metrics, logs, traces, and events — across applications, infrastructure, and networks. This centralized approach facilitates improved visibility, faster incident response, and enhanced operational resilience.

The solution is particularly relevant in the context of financial services, where institutions face challenges such as legacy technical debt, regulatory pressure, changing customer demands, increasing competition from non-traditional firms, growing data volumes and complexity, and the need for cost control. Splunk's platform supports cross-functional collaboration between IT, security, and compliance teams, helping organizations reduce tool sprawl, streamline workflows, and improve decision-making. Key areas of impact can include fraud detection, risk management, regulatory compliance, and customer experience optimization. The platform's scalability and flexibility position it as a strategic enabler for digital business transformation and operational efficiency in the financial services industry.

The Business Value of Splunk

Study Firmographics

IDC conducted research to explore the value and benefits for FSI organizations using Splunk to improve security, observability, resilience, and visibility across their IT environments. The project included seven interviews with organizations that use Splunk and have experience with and/or knowledge about the benefits and costs of using the platform. During the interviews, IDC asked the companies a variety of quantitative and qualitative questions about the offering's impact on their IT and security operations, core businesses, and costs.

Table 1 (below) presents the firmographics of the seven FSI organizations IDC interviewed for the study. These organizations vary significantly in size, with employee counts ranging from 1,200 to 85,000 and annual revenues between $379 million and $35 billion. On average, they employ 5,637 IT staff and secure over 71,000 IT assets. The companies are geographically diverse, operating in the United States, Germany, Singapore, and the United Kingdom, and all belong to the FSI sector. This diversity provides a broad perspective on how Splunk delivers value across different scales and regions within the industry.

Table 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Minimum	Maximum
Number of employees	29,529	15,000	1,200	85,000
Number of total IT Staff	5,637	5,000	60	15,000
Total number of IT assets secured	71,786	17,000	1,500	250,000
Annual revenue	$7.1B	$3.0B	$379.0M	$35.0B
Countries	United States (4), Germany, Singapore, United Kingdom			
Industries	FSI (7)			

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Choice and Use of Splunk

The organizations that IDC interviewed described the criteria involved in their selection of Splunk. Frontline managers and IT professionals who had direct experience with Splunk's value proposition offered detailed comments about their purchase decision. Study participants consistently cited the need for greater visibility across their IT environments as a primary reason for adoption. Many organizations struggled with fragmented infrastructure, limited observability, and insufficient monitoring capabilities, which hindered their ability to detect and respond to threats effectively. They selected Splunk for its ability to unify data sources, provide real-time insights, and support integrated monitoring across complex hybrid environments. Its scalability and capacity to ingest large volumes of data were especially important for organizations managing terabytes of daily traffic and diverse endpoint ecosystems. Study participants also emphasized the importance of improving incident response times, managing insider threats, and meeting stringent SLAs for both internal and external clients. Several organizations noted that Splunk replaced legacy or internally developed tools that lacked flexibility, automation, and integration capabilities.

Study participants elaborated on these and other selection criteria:

Visibility for entire infrastructure:

"Overall, our infrastructure is divided into three big segments. Each division was using different vendors, but we didn't really have the chance to manage everything or have a clear sense of visibility into the infrastructure and what was going on. That led us to do some homework and decide that Splunk would help us with the challenges we were facing."

Fully integrated monitoring:

"My organization has very complex infrastructure and services and needed a proper monitoring tool. We felt that Splunk would give us that integrated monitoring functionality and enhance performance and security operations."

Scalable insider threat management:

"For my organization, we selected Splunk to manage insider threat. We also liked that it could be part of our data warehouse to manage data collection, applications, and performance. We appreciated that Splunk has the scalability to handle our volume."

Enhanced security and recovery capabilities:
"Meeting SLAs for IT infrastructure for both internal clients as well as external clients was a major challenge that my company was looking to solve with Splunk. We needed a tool that would provide proper observability, performance, scalability, resilience, and reliability. Obviously, security and recovery were key to our decision."

Faster incident response and insights:
"My company needed faster incident response and a SIEM tool that could pull metrics, build dashboards, and assist in investigations. We thought that Splunk would give us the resilience we needed — especially around cybersecurity attacks and IT incidents — along with all-time insights, observability, and faster detection and response."

Improved security and risk management:
"We selected Splunk because it would help us address key challenges during our digital transformation processes by improving security, cybersecurity, and risk management."

Table 2 (below) outlines how the interviewed financial services and insurance organizations were using Splunk across their IT environments. On average, each organization managed over 70,000 endpoints — including servers, virtual machines, and devices — and supported nearly 30,000 employee devices and 3.1 million customer users through business applications. Splunk played a critical role in supporting core operations, with 55% of organizational revenue tied to systems the platform monitors.

Table 2
Organizational Usage of Splunk

Splunk Environment	Average	Median
Total endpoints (servers, VMs, and devices)	70,957	17,000
Employee devices	29,486	5,000
Employees using business applications	28,316	15,000
Customers using business applications	3,104,000	500,000
Revenue supported	55%	70%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Business Value and Quantified Benefits

Participants reported a wide range of benefits from using Splunk for observability and security. The most significant was that the solution enhanced visibility and provided actionable insights across their operational environments. By consolidating data from diverse sources into a unified platform, Splunk enabled real-time monitoring and analysis that supported faster threat detection, streamlined investigations, and enabled more effective incident response. This improved situational awareness helped teams identify control gaps, reduce downtime, and maintain infrastructure performance. The solution ultimately fostered greater resilience and operational confidence across the enterprise.

Interviewed customers described their most significant benefits in detail below:

Increased visibility:

"Splunk has provided visibility into what's going on in our environment, which was our primary challenge before deployment. We didn't have a one-stop shop before, and Splunk helped us correlate and see where incidents are coming from and what their intention is."

Deeper insights:

"Splunk enhanced our operational intelligence and resilience by providing real-time, actionable insights from machine-generated data. It aggregates data from networks, cloud services, and servers, making it searchable and analyzable, helping us prepare for, respond to, and recover from cyber and non-cyber incidents."

Identification of control gaps:

"The biggest benefit of using Splunk is that it has allowed my organization to define and identify gaps in our controls and detect suspicious behavior, either malicious or the result of a compromise."

Quicker detection:

"Splunk has significantly improved our mean time to detect across a range of issues — from downtimes and server monitoring to security analytics and insider threats. It's helping us in a lot of areas right now."

Minimized downtime impact:

"Splunk helps my organization detect threats earlier and remediate those issues quickly. Importantly, this minimizes the downtime impact of our business applications."

Improved availability and performance:
"The most significant benefit of Splunk is felt in our security operations center (SOC). It is heavily used to monitor our infrastructure and services. As a result, we have improved our uptime, availability, and performance. This is incredibly important because this industry is heavily regulated."

Improved customer experience:
"Splunk has helped improve our customer services and applications because we have better response time, uptime, and availability. This has really improved customer experience."

Using its standard ROI methodology, IDC quantified the benefits across the categories of application management, security, IT operations, and business enablement. **Figure 1 (next page)** presents IDC's calculations of cumulative customer benefits after the adoption of Splunk.

As shown, the average annual benefits totaled $15.3 million per organization in the following categories:

Application management benefits:
Improved application performance and reliability by enabling proactive monitoring, anomaly detection, and streamlined DevOps workflows

Security and compliance benefits:
Enhanced threat detection, incident response, and regulatory compliance through real-time analytics, behavioral monitoring, and automated reporting

IT benefits:
Boosted IT operational efficiency by consolidating tools, increasing infrastructure visibility, and reducing search and maintenance time

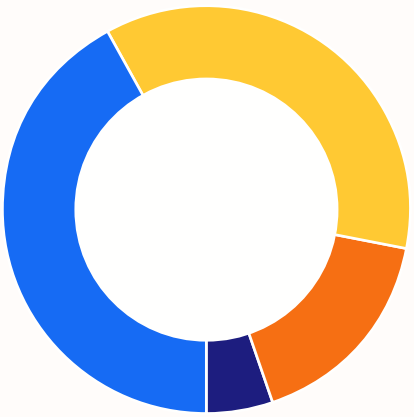
Business enablement benefits:
Enabled greater end-user productivity by minimizing downtime and improving the availability and performance of business-critical applications

Figure 1

Average Annual Benefits Per Organization

See Figure 1 data in an accessible table format.

($ per interviewed organization)



- $6,468,100 Application management
- $5,515,366 Security and compliance
- $2,570,342 IT
- $767,568 Business enablement

$15.3 million

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Security and Compliance Benefits of Splunk

IDC used its Business Value methodology to evaluate a series of specific benefits related to security and compliance. Study participants reported that Splunk significantly enhanced their overall security posture by improving threat detection, reducing false positives, and accelerating incident response. Organizations noted that Splunk's ability to ingest and correlate data from diverse sources enabled faster identification and triage of genuine threats. The platform's scalability and integration with existing security tools allowed teams to manage large volumes of data efficiently, while features such as risk-based alerting and real-time monitoring supported more proactive and precise threat management. Several organizations also highlighted substantial cost savings from retiring legacy security tools and reducing reliance on external threat intelligence services.

On the compliance front, Splunk helped financial institutions meet regulatory requirements more effectively by providing robust reporting capabilities, audit trails, and dashboards tailored to frameworks such as MAS TRM and PDPA. Participants emphasized that Splunk enabled faster turnaround during regulatory examinations and improved visibility into compliance metrics, contributing to reduced fines and penalties.

The tool's ability to centralize and standardize data access and reporting also supported board-level oversight and improved organizational confidence in meeting evolving compliance demands.

Study participants elaborated on these and other benefits:

Increased visibility:
"Splunk gives us full visibility by aggregating log data from the network, storage, and application layers in real time. This helps us query alerts and determine whether they're genuine threats or false positives."

Quicker threat identification and response:
"Splunk has helped us better identify threats by improving data visualization, early detection, response, and ingestion. With built-in alerts and observability, we can detect, respond, and rectify issues quicker."

Reduced time to identify threats:
"Splunk has significantly reduced the time it takes us to identify threats — what used to take up to an hour now happens three to five times faster, thanks to replacing manual tools with Splunk's automated capabilities."

Notable generation:
"One of Splunk's standout features is its notable generation, which drastically reduced our daily alerts from over 500 to just 30–40, allowing us to focus on true positives. It's also highly scalable and integrates easily with existing security tools — something many other solutions can't do."

Severity and criticality ratings:
"Splunk helps us triage more effectively by providing severity and criticality ratings, response times, and prioritization. We now have better control over how we manage and respond to alerts."

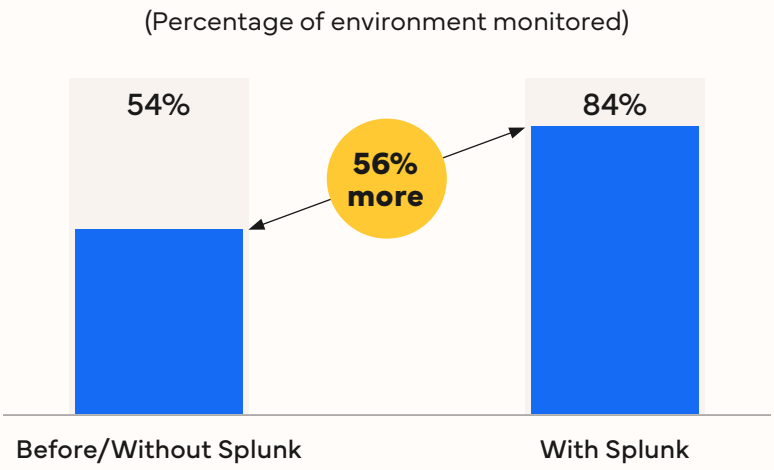
Behavioral analytics:
"Splunk allows our SOC to monitor behavioral analytics on individuals for insider threats, potential fraud, and system availability."

Compliance reports:
"Splunk helps us generate outage reports that align with compliance frameworks like GDPR, PCI DSS, and others. These reports give us a clear picture of our compliance posture and help demonstrate that we're meeting regulatory requirements whenever an issue arises."

IDC validated this anecdotal reporting by quantifying the benefits, beginning with the impact of Splunk on environment monitoring. **Figure 2 (below)** highlights the improvements that stemmed from Splunk's scalability in terms of data ingestion and integration. Interviewed organizations reported significant improvements in their ability to consolidate monitoring tools and expand visibility across their IT environments. On average, participants were able to monitor 56% more of their total environment using Splunk, demonstrating its effectiveness in enhancing operational oversight and infrastructure coverage.

Figure 2

Environment Monitoring Impact



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Table 3 (next page) highlights the efficiency gains that SOC teams achieved through their use of Splunk. Interviewed organizations benefited from Splunk's ability to consolidate data sources, reduce alert noise, and accelerate threat detection and response using features such as notable event generation, risk-based alerting, and integrated dashboards. As a result, the SOC was able to work with 50% greater efficiency, meaning it needed 65 fewer FTEs to manage its environment in comparison to its previous monitoring tools. This freed up the time of highly skilled individuals to focus on other important security initiatives for the organization. IDC valued this efficiency gain at $6.5 million per year.

Table 3

Security Operations Team Efficiency Gain

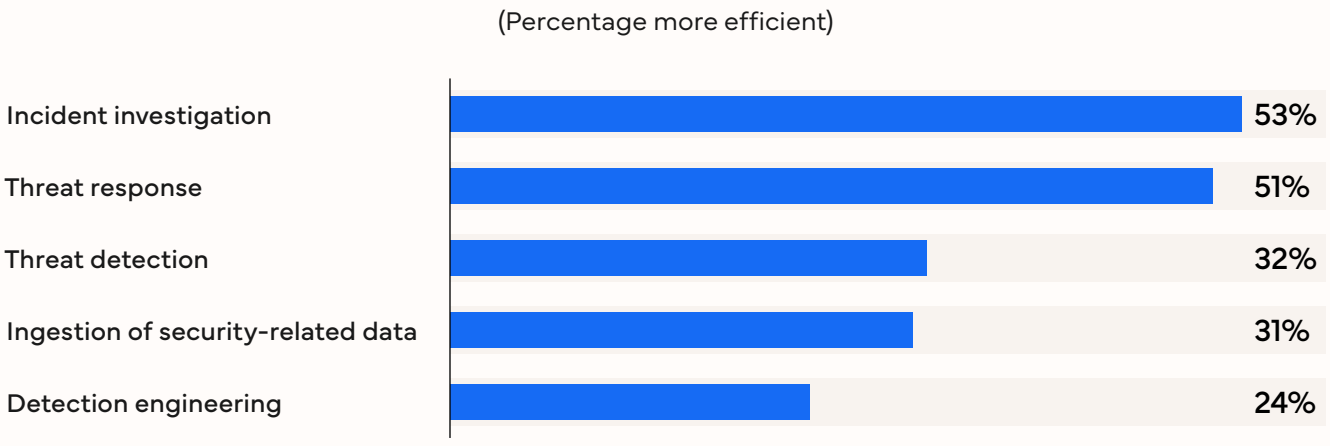
Efficiency Gain	Before Splunk	With Splunk	Difference	Benefit
Total FTE count	128.9	63.9	65.0	50% gain
Value of staff time per year	$12,893,852	$6,391,667	$6,502,185	50% gain

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IDC then evaluated the improvements Splunk delivered to core security operations tasks. Study participants reported **measurable efficiency gains** across five key areas: detection engineering (24%), data ingestion related to security (31%), threat detection (32%), threat response (51%), and **incident investigation (53%)** **(Figure 3 below).** Splunk's automation capabilities, streamlined data workflows, and advanced analytics made these enhancements possible, which collectively enabled security teams to respond faster, reduce manual effort, and improve the overall effectiveness of their threat management processes.

Figure 3

Security Task-Related KPIs



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Splunk also had measurable impacts on threat and alert identification or investigation. The results below underscore Splunk's effectiveness in enhancing visibility, streamlining alert workflows, and accelerating investigations, ultimately strengthening overall security posture and alert response.

Respondents saw the following positive impacts of Splunk:

- 43% increase in fidelity alerts
- 27% reduction in alerts
- 52% more threats and alerts handled with Splunk
- **86% more threats identified with Splunk**
- 60% less time required to identify potential threats
- 47% reduction in impactful security incidents

Table 4 (below) outlines how organizations reduced their reliance on third-party threat intelligence services. By centralizing threat detection and response within their own environments and automating key security tasks, organizations were able to eliminate costly external vendor contracts. On average, this shift resulted in $800,000 in annual cost avoidance.

Table 4

Reduction in Third-Party Threat Intelligence Services

Cost Reduction	With Splunk
Annual cost avoidance	$800,000

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IDC then looked at the impact of Splunk on compliance teams. Splunk's ability to automate compliance reporting, enhance visibility into regulatory data, and streamline audit workflows enabled productivity improvements. As a result, organizations not only improved operational efficiency but also reduced their risk of serious breaches or data loss by 28%, a critical outcome in the highly regulated financial services and

insurance sectors. As shown in **Table 5 (below),** these improvements helped the team improve their productivity by 16%, meaning teams of 44.7 FTEs could work with the equivalent speed of having an additional 7.3 FTEs on staff. IDC valued this productivity gain at $509,743 per year.

Table 5

Compliance Team Productivity Gain

Productivity Gain	Before Splunk	With Splunk	Difference	Benefit
Equivalent productivity level, FTEs	44.7	52.0	7.3	**16% gain**
Value of staff time per year	$3,130,000	$3,639,743	$509,743	**16% gain**

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Application Management Benefits of Splunk

Study participants reported substantial application management benefits from the deployment of Splunk. The solution provided improved application performance and reliability by enabling proactive monitoring, anomaly detection, and streamlined DevOps workflows. Splunk's real-time monitoring capabilities enabled teams to proactively identify performance bottlenecks and application failures, thereby minimizing downtime and improving service availability. Participating organizations also highlighted the value of Splunk's observability features, which provided end-to-end visibility across hybrid environments and supported faster root cause analysis.

Study participants discussed these and other key benefits:

Improved visibility:

"Splunk has helped our DevOps team manage databases and applications more smoothly by providing better visibility into how the environment operates."

Streamlined workflows:

"Splunk supports our DevOps and application managers in daily operations, maintenance, troubleshooting, and incident response by streamlining workflows and improving visibility."

Anomaly detection:

"Splunk's robust monitoring capabilities allow DevOps to set dynamic thresholds and receive immediate alerts when patterns are breached or nearing a breach. Its anomaly detection helps identify potential issues before they impact the environment."

Automated reports and testing:

"Splunk has enabled our DevOps team to do more with automation; they are integrating it with their toolsets to generate automated reports and streamline testing."

Robust dashboards:

"Splunk dashboards and reports help our IT engineers support and troubleshoot applications by identifying issues like missing logs or latency. At the application level, Splunk IT Intelligence and real user monitoring also help us track SLA breaches and downtime."

IDC applied its Business Value methodology to quantify application management benefits, beginning with DevOps productivity. Enhanced observability across the application life cycle increased productivity. This enabled faster troubleshooting, proactive anomaly detection, and streamlined automation through integrated dashboards and dynamic alerting. Additionally, organizations experienced a **19% reduction in time spent testing applications** and a 22% decrease in time spent troubleshooting application problems, underscoring Splunk's role in accelerating DevOps workflows and improving operational efficiency.

Table 6 (below) highlights the improvements that DevOps teams achieved through the use of Splunk. Interviewed organizations reported an 18% increase in productivity, which helped teams of 367 work at the equivalent productivity level of having an additional 67.8 FTEs on staff. IDC valued this gain at approximately $6.8 million.

Table 6

DevOps Productivity Gain

Productivity Gain	Before Splunk	With Splunk	Difference	Benefit
Equivalent productivity level, FTEs	367.0	434.8	67.8	**18% gain**
Value of staff time per year	$36,700,000	$43,475,108	$6,775,108	**18% gain**

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IT engineers also saw productivity gains from the deployment of Splunk. Organizations attributed these gains to Splunk's real-time observability across complex environments, which enabled faster detection of application issues, more reliable code deployments, and improved operational workflows. Additionally, organizations were able to detect application problems 70% quicker and had a 19% higher success rate for production code changes.

Table 7 (below) quantifies the productivity enhancement that came from the previously mentioned improvements. As shown, interviewed organizations reported a **22% increase in IT engineers' productivity levels.** This gain helped teams of 108.5 FTEs work as the equivalent productivity level of having 23.9 additional FTEs, which IDC valued at $6.8 million per year.

Table 7
IT Engineers' Productivity Gain

Productivity Gain	Before Splunk	With Splunk	Difference	Benefit
Equivalent productivity level, FTEs	108.5	132.3	23.9	**22% gain**
Value of staff time per year	$10,846,667	$13,232,933	$2,386,267	**22% gain**

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IT Benefits of Splunk

IDC found that interviewed organizations experienced significant IT benefits, particularly in improving scalability, observability, and operational resilience. Splunk enabled real-time monitoring and analysis of machine-generated data across networks, cloud services, and servers. Splunk's centralized platform supported standardization and consolidation of IT tools, streamlining workflows and improving data management. Organizations appreciated the actionable insights that Splunk provided, which empowered teams to make faster, more informed decisions. These capabilities translated into more efficient IT operations, reduced downtime, and improved overall system performance across complex hybrid environments.

Study participants offered these detailed comments:

Single pane of glass visibility:
"Splunk's data correlation and dashboard capabilities give us a single pane of glass to monitor all company assets. With features like summary indexing, we can quickly identify issues — whether it's CPU spikes, unusual login activity, or server performance problems — and respond faster with greater accuracy."

Less manual work:
"Splunk has had a big impact on our IT operations and management team. It tells them exactly where to fix issues, provides detailed reports, and eliminates the need for them to investigate or analyze problems themselves."

Reduced maintenance requirements:
"For infrastructure teams, Splunk reduces time spent on maintenance and hardware upkeep — especially tasks like patching and managing server hardware."

Environment investigations:
"Splunk enables our IT team to investigate the availability and integrity of both applications and platforms."

Reduced search time:
"Splunk has dramatically reduced search times across our data environment — from several hours previously, down to just a few minutes. Before Splunk, data was scattered across multiple tools with no centralized portal, making searches slow and unclear. Now, with native and ingested data consolidated in Splunk, everything is searchable in one place."

Increased data ingestion:
"My organization has increased data ingestion and utilization a lot with Splunk; we ingest about 67% more data per year."

Less expensive data ingestion:
"To match our current level of data ingestion with Splunk using our old tools, we'd be paying at least 30% more."

Study participants reported that their IT infrastructure teams achieved significant efficiency gains. Driving these gains were Splunk's ability to consolidate monitoring tools, enhance visibility, automate workflows, and improve data searchability and data ingestion. Notably, organizations experienced a **74% reduction in the time required to search across data.** Interviewed organizations reported a 22% improvement in team efficiency, which IDC valued at $2.6 million per year **(Table 8, next page).**

Table 8

IT Infrastructure Teams' Efficiency Gain

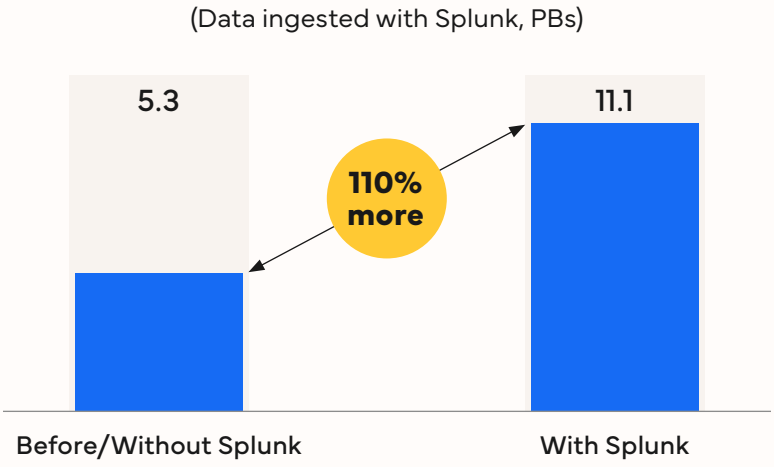
Efficiency Gain	Before Splunk	With Splunk	Difference	Benefit
Total FTE count	121.2	95.0	26.2	**22% gain**
Value of staff time per year	$12,118,451	$9,500,000	$2,618,451	**22% gain**

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IDC then looked at the influence of Splunk on data ingestion. Interviewed organizations found that they were able to increase their data ingestion by 110% with Splunk **(Figure 4, below).** Driving this increase was Splunk's ability to consolidate ingestion pipelines, automate data collection, and support scalable, high-volume environments.

Figure 4

Data Ingestion Impact



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Additionally, by leveraging Splunk's unified platform for data ingestion, correlation, and analysis, these FSI organizations were able to eliminate redundant monitoring solutions, reduce storage expenses, consolidate legacy systems, and streamline their IT operations. One participant emphasized the transformation, stating: "*Splunk has enabled us to eliminate legacy tools and save approximately $2 million annually. Our previous solutions were ineffective, and the level of visibility and integration we now have with Splunk simply wasn't possible before. It's become an industry standard — and if we didn't have it, we'd be in panic mode.*" This resulted in the organizations reducing their IT costs by $721,667 annually **(Table 9, below).**

Table 9

Annual IT Cost Reduction/Avoidance

Cost Reduction/Avoidance	With Splunk
Annual cost avoidance from tool consolidation and storage avoidance	$721,667

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Business Benefits of Splunk

Splunk's impact extended beyond IT operations to support broader business goals and drive measurable value across FSI organizations. The solution empowered organizations to make more informed strategic decisions by delivering actionable insights from data. Several interviewees highlighted improvements in customer experience and investor confidence, attributing these gains to enhanced system reliability and performance. Additionally, there was a general sentiment that Splunk reduced the risk of financial and reputational losses by improving overall resiliency.

Study participants offered these comments:

Improved application performance:

"Application performance has improved by roughly 25% for end users because Splunk's analytics capabilities have helped us identify and resolve issues more effectively."

Less downtime end-user impact:

"Our end users are less impacted by downtime, security incidents, and performance degradation because of Splunk."

Strengthen security posture:

"Splunk helps my company reduce risk and strengthen our security posture and resilience. This is especially important in the financial industry because it minimizes potential financial and reputation losses."

Table 10 (below) outlines the business enablement benefits that interviewed organizations achieved in terms of end-user productivity improvements. Splunk's ability to reduce downtime, minimize performance degradation, and enhance application availability and responsiveness drove these gains. This ultimately enabled end users to work more effectively and with fewer disruptions. In fact, the organizations interviewed reported a 5% increase in end-user productivity. Factoring in a 15% operating margin, this meant that internal application users could work with the equivalent speed and productivity level of having 15.5 additional FTEs on staff. IDC valued this gain at $1 million per year.

Table 10

Business Enablement — End-User Productivity Gain

Productivity Gain	Before Splunk	With Splunk	Difference	Benefit
Equivalent productivity level, FTEs	1,986.0	2,089.0	103.5	5.0% gain
Equivalent productivity level, FTEs net	1,986.0	2,001.0	15.5	0.78% gain
Value of staff time per year	$139,000,000	$140,087,179	$1,087,179	0.78% gain

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

ROI Summary

IDC's three-year ROI analysis of Splunk usage among financial services and insurance organizations revealed a substantial economic impact. On average, participating organizations realized $35.1 million in discounted benefits over three years, compared to $7.2 million in discounted investment costs, resulting in a net present value (NPV) of $27.9 million. This translates into a 387% ROI, with a payback period of just 13 months. These findings underscore Splunk's ability to deliver significant value through improved security, operational efficiency, and cost savings **(Table 11, below).**

Table 11

Three-Year ROI Analysis

ROI Analysis	Per Organization	Per 10,000 Managed Endpoints
Discounted benefits	$35,117,000	$4,949,044
Discounted investment	$7,211,300	$1,016,290
NPV	$27,905,700	$3,932,754
ROI	**387%**	**387%**
Payback	**13 months**	**13 months**
Discount factor	12%	12%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Challenges/Opportunities

Splunk's unified security and observability platform offers significant value to financial services organizations, but like any enterprise solution, it faces certain adoption hurdles. Integration can be complex, especially in environments with legacy systems, siloed technology teams, and often competing budgets from the lines of business that each have their own priorities. Splunk claims that they have addressed many of these challenges in order to make deployment and interoperability more straightforward. Platform implementation still requires cross-functional collaboration between technology and security teams, as well as a partnership with lines of business and the C-suite for a strategic deployment.

The AI revolution is causing budget pressures in the financial services industry, with many traditional projects at risk of being cut to fund AI projects, particularly generative and, more recently, agentic initiatives. While Splunk's licensing model reflects the depth and scalability of its capabilities, it may be perceived as a challenge in such budget-conscious environments where hard choices must be made. Some institutions may view a Splunk implementation as a way to overcome infrastructure challenges that are getting in the way of AI deployment and, in that way, allocate some AI investment dollars toward a Splunk solution.

Additionally, competitive dynamics are evolving rapidly. In observability, Splunk competes with more narrowly focused or cloud-native tools that may appear more agile for specific use cases. However, as the infrastructure at the institution grows and becomes more complex, there will be a growing need to move to a unified approach for performance, stability, reliability, and cost efficiency. In the security space, the SIEM market is shifting toward automation and AI-driven insights. To stay ahead, Splunk needs to differentiate through its performance, scalability, and ability to unify workflows across IT and security operations specific to financial services, demonstrating real business value that demands investment.

Conclusion

Moving to and adopting cloud and new AI platforms is increasing the already siloed and complex financial services infrastructure, adding risks to the resiliency, security, compliance, and scalability of institutions' operations. To address the growing complexity and risk in financial services and insurance IT environments, organizations face challenges such as fragmented infrastructure visibility, slow incident response, and regulatory compliance pressures. To help address these challenges, Splunk offers a unified platform that enhances observability, security, and operational resilience. Splunk enables real-time monitoring, automated threat detection, and centralized data analysis across hybrid environments — empowering IT, security, and compliance teams to respond faster, reduce downtime, and meet regulatory requirements more effectively.

IDC's analysis found that Splunk delivers substantial business value both quantitatively and qualitatively. Organizations reported improved productivity across DevOps, IT, and security teams, reduced reliance on third-party services, and enhanced customer experience through better application performance. On average, organizations realized $15.3 million in annual benefits, including cost savings, efficiency gains, and risk reduction. The ROI metrics are compelling: a 387% three-year ROI and a 13-month payback period. These quantitative results are in addition to the qualitative benefits of improved resiliency and controlled scalability.

Appendix 1: Financial Summary

Table 12 (below) presents a summary of IDC's Business Value calculations as fully described in the previous sections, with total average benefits of $15.3 million per organization accruing annually.

Table 12

Specific Calculations: Benefits from the Use of Splunk

Category of Value	Average Quantitative Benefit	15% Margin Applied	Calculated Average Annual Value*
IT annual cost reductions	$721,667 in annual IT cost reductions	No	$721,667
IT infrastructure team — admin and management efficiency gains	22% higher efficiency worth 26.2 FTEs, $100,000 salary	No	$1,848,675
Security operations team efficiency gain	50% higher efficiency worth 65 FTEs, $100,000 salary	No	$4,590,663
Reduction in third-party threat intelligence services	$800,000 in annual savings from services reduction	No	$564,815
Compliance team productivity gain	16% higher productivity worth 7.3 FTEs, $70,000 salary	No	$359,888
DevOps productivity gain	18% higher productivity worth 67.8 FTEs, $100,000 salary	No	$4,783,352

Table 12 continued next page

Appendix 1: Financial Summary (continued)

Table 12 continued

Category of Value	Average Quantitative Benefit	15% Margin Applied	Calculated Average Annual Value*
IT engineers' productivity gain	22% higher productivity worth 23.9 FTEs, $100,000 salary	No	$1,684,748
Business enablement — end-user productivity gains	0.78% higher net productivity worth 15.5 FTEs, $70,000 salary	Yes	$767,568
Total average annual benefits	**$15.3M per organization per year**		

*includes 10.6 months deployment time in year 1
n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Appendix 2: Methodology

IDC utilized its standard ROI methodology for this project, which involved gathering data from current users of Splunk as the foundation for the model.

Based on interviews with organizations using Splunk, IDC performed a three-step process to calculate the ROI and payback period:

1. **IDC gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Splunk.** In this study, the benefits included IT cost reductions and avoidances, staff time savings and productivity benefits, and revenue gains.
2. **IDC created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Splunk and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **IDC calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Splunk over a three-year period. ROI is the ratio of the NPV and the discounted investment. The payback period is the point at which the cumulative benefits equal the initial investment.

IDC based the payback period and ROI calculations on the following assumptions:

- Time values multiplied by burdened salary (salary + 28% for benefits and overhead) quantify efficiency and productivity savings. For this analysis, IDC used the assumptions of an average fully loaded $100,000 per year salary for IT staff members and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumed that employees work 1,880 hours per year (47 weeks x 40 hours).
- IDC calculated the net present value of the three-year savings by subtracting the amount that organizations would have realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for the assumed cost of money and the assumed rate of return.
- Further, because Splunk requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC pro rates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

Appendix 3: Accessible Data Table

This appendix provides an accessible version of the data for the complex figure in this document. Click "Return to figure" to get back to the original figure.

Figure 1 Accessible Data

Average Annual Benefits Per Organization

Benefits	$ Per Interviewed Organization
Application management benefits	$6,468,100
Security and compliance benefits	$5,515,366
IT benefits	$2,570,342
Business enablement benefits	$767,568
Total	**$15.3 million**

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Return to figure

About the IDC Analysts

Stephen Elliot

Group Vice President, I&O, Cloud Operations, and DevOps, IDC

Stephen Elliot manages multiple programs spanning IT operations, enterprise management, ITSM, agile and DevOps, application performance, virtualization, multi-cloud management and automation, log analytics, container management, DaaS, and software-defined compute. Elliot advises senior IT, business, and investment executives globally in the creation of strategy and operational tactics that drive the execution of digital transformation and business growth.

More about Stephen Elliot →

Jerry Silva

Program Vice President, Financial Insights, IDC

Jerry Silva is vice president for IDC Financial Insights and is responsible for the Global Retail Banking practice. Silva's research focuses on technology trends and customer expectations and behaviors in retail banking worldwide. Silva draws upon over 35 years experience in the financial services industry to cover a variety of topics, from the back office to customer channels to governance in the technology shops at financial institutions.

More about Jerry Silva →

About the IDC Analysts (continued)

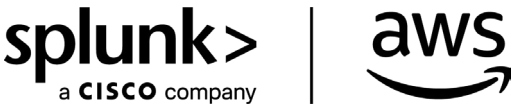
Megan Szurley

Business Value Manager, Business Value Strategy Practice, IDC

Megan Szurley is manager for the Business Value Strategy practice, responsible for creating custom business value research that determines the ROI and cost savings for enterprise technology products. Szurley's research focuses on the financial and operational impact of these products for organizations once deployed and in production. Prior to joining the Business Value Strategy practice, Szurley was a consulting manager within IDC's Custom Solutions division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Szurley partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

More about Megan Szurley →

Message from the Sponsor



Splunk for Financial Services

Splunk helps financial leaders protect revenue, maintain trust, meet evolving regulatory demands by delivering real-time visibility through advanced AI-driven analytics. From proactive AI-enhanced detection of financial crime and AML risks to continuous monitoring for fraud and payment anomalies, Splunk enables rapid investigation and resolution before issues impact payments, customers or compliance. Splunk's predictive AI analytics turn complex financial data into clear, actionable intelligence—strengthening payment integrity, ensuring regulatory readiness, and driving confident, compliant growth in the digital finance ecosystem.

For more information, visit: www.splunk.com/fsi

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

idc.com @idc @idc

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.