SINGLE SOURCE OF TRUTH

How a Fortune 100 Company Gains Enterprise-Wide Business Visibility by Splunking Multiple Petabytes Per Day

Use Cases

- Improving Operational Efficiencies
- Troubleshooting Services Delivery
- Improving Application Delivery
- Fortifying Internal Security
- Streamlining Regulatory Compliance
Executive Summary

Splunk delivers Operational Intelligence to 85 of the Fortune 100 and drives strong business and IT results at more than 11,000 enterprises worldwide. Regardless of the industry or challenge, Splunk Enterprise enables companies to maintain industry leadership, innovate, manage growth expectations, provide excellent customer service and ensure a solid security posture.

One multinational Fortune 100 technology company with many different lines of business and diversified products and services has been a Splunk customer since 2007. The company began with a 100GB per day Splunk Enterprise implementation for managing endpoints for enterprise resource planning (ERP) systems handling product registration and unique I.D. transactions. The company considered continuing with its own homegrown analysis tools developed by individual groups, but it needed a standard solution across the enterprise that could scale. Since then, this customer has faced many new business and technology challenges and Splunk Enterprise has helped to address them.

The company now has an unlimited Splunk Enterprise license, enabling it to expand its use cases to include security and fraud, business analytics, IT operations, application delivery and Internet of Things (IoT). Splunk Enterprise supports both customer-facing and internal efforts, enabling the company to provide smooth global product launches, gather real-time insights into customer behavior, ensure Payment Card Industry (PCI) compliance, prevent security breaches and maintain a complex IT infrastructure. Today, Splunk Enterprise synchronizes transactions and systems flawlessly and is becoming the data fabric that supports the company’s growth strategy. As a mission-critical application with other mission-critical systems, including the transaction system, the company relies on Splunk Enterprise to ensure uptime and performance.

- **Monitoring IT operations.** Previously, the company had custom-built tools that it used to collect data for product registrations off of its ERP systems. Within days of adopting Splunk Enterprise, the easy-to-use interface began to deliver value. Today, Splunk Enterprise dashboards monitor and provide visibility across applications and infrastructure.

- **Supporting critical security and fraud monitoring; Ensuring PCI compliance.** In the past, the company endured time-consuming security and fraud monitoring and struggled with manual PCI reporting. Splunk Enterprise enables the company to detect and alert on suspicious security and fraud activity, troubleshoot and support case investigation. Automated, continuous PCI monitoring enables the company to meet compliance requirements. With Splunk Enterprise, the company has a solution for company-wide fraud detection and it has reduced the typical fraud report time from eight hours to 20 minutes.

- **Application delivery improvements reduce time-to-market.** Prior to implementing Splunk Enterprise for application delivery, the company relied on homegrown tools. The development teams needed better visibility throughout the development process and now rely on Splunk Enterprise for end-to-end application visibility from development and test to product and operations. Splunk Enterprise has helped improve software quality and reduce time-to-market.

- **Splunk Enterprise provides essential business analytics visibility.** As the company grew its product offerings it looked to real-time analytics with Splunk Enterprise to understand product demand and trends across geographies. Product support page data informs in-house teams about the types of questions customers are most likely to ask so the company can improve documentation quality and provide excellent customer service.
**Business Benefits at a Glance**

<table>
<thead>
<tr>
<th>Challenges</th>
<th>How Value Is Measured</th>
<th>Business Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Committed to build excellent products and provide top-notch services</td>
<td>• Provides visibility across applications and systems</td>
<td>• Provide seamless customer experience with all products and services</td>
</tr>
<tr>
<td>• Lacked a single view across a multi-tiered application and across functions and departments</td>
<td>• Reduces Mean Time to Repair (MTTR)</td>
<td>• Successfully support smooth product launches</td>
</tr>
<tr>
<td>• Needed to collect data in standardized indexes and share data across teams</td>
<td>• Standardized, automated data collection and access</td>
<td>• Easily collect and share data across enterprise</td>
</tr>
<tr>
<td>• Lacked flexible interface to drive alerts and dashboards for multiple personnel</td>
<td>• Provides solution to rapidly create alerts and dashboards</td>
<td>• Alerts and dashboards provide real-time data visibility</td>
</tr>
<tr>
<td>• Struggled with time-consuming fraud investigations, manual PCI monitoring and user authentication</td>
<td>• Real-time monitoring</td>
<td>• Reduce fraud report time from eight hours to 20 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Automated, continuous PCI monitoring meets compliance requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Significant time-savings versus manual user authentication</td>
</tr>
</tbody>
</table>

**Enter Splunk**

The customer employs extremely talented people who are capable of supporting the company’s build versus buy technology approach. However, in 2007, the company realized some of its homegrown tools lacked essential functionality. It also needed a standard solution that could scale with the growing global enterprise as its data volume was projected to reach several terabytes per day in the not-too-distant future.

Splunk Enterprise dashboards now monitor and provide visibility across applications and infrastructure. One dashboard includes a chart that monitors server response time (see Figure 1), providing an engineering team with important visibility into IT operations. This dashboard helps the company monitor the load on the system, determine how the system is keeping up with traffic, troubleshoot or add more capacity, if necessary.

*Figure 1. Standard server response time.*
Improving Application Delivery

Prior to implementing Splunk Enterprise for application delivery, the company relied on homegrown tools that lacked the necessary visibility developers needed. At the time, the company’s “code with purpose” focus meant that developers did not want to be among those who were kicking up many errors. Development teams needed to understand who was writing code and gain insight into how an application was behaving throughout the development process. If any type of issue occurred during development, teams had to scramble to fix it, which slowed time-to-market.

Since the company added an 80GB Splunk Enterprise license for application monitoring and troubleshooting, the company has gained end-to-end application delivery visibility — from development to test to product launch. The company can identify issues early on in the process, as developers have the visibility required to push out good, clean code. With Splunk Enterprise, the company has improved software quality, ensuring smooth product launches and fast time-to-market.

By the time the company had purchased approximately 2TB of Splunk Enterprise software, a team of 15 people worldwide was using it to monitor clusters of an application because staff found that no other technology could provide that level of visibility during a highly critical product launch. Over many years and product launches, Splunk Enterprise has been with the company to provide both questions and answers and support smooth application delivery.

Harnessing Splunk Enterprise for Business Analytics

Soon after its application delivery success, the company identified an additional challenge where Splunk Enterprise could deliver a solution: online transaction business analytics. The company added a 5GB Splunk Enterprise license, which enabled the customer to visualize transactions and run real-time online store analytics successfully during the busy holiday season.

At some point, a technical staff member at the company asked a Splunk representative, “You can click on everything in this interface?” and when the answer was “yes,” the door opened wider for the growth of Splunk Enterprise at the company. The individual who asked this question then admitted that the company was running into some scalability challenges and the vision for a data analytics platform at the company began to materialize.

From there, the company identified another business analytics opportunity when it added a 40GB Splunk Enterprise license to capture retail store data. This enabled the company to understand trends across retail locations, including the number of different products sold. A Splunk Enterprise dashboard shows retail traffic per minute (See figure 2).

![Figure 2. Retail traffic per minute.](image)

Repurposing Data for Customer Demand, Service

One additional business analytics use case provides critical visibility into customer demand for products and services. When the company launches a new product or service, Splunk Enterprise dashboards provide real-time information about demand across geographies. The company is committed to protecting customer privacy and confidentiality, and instead of looking at individual customer behaviors it looks at aggregated trends.

When customers purchase new products, they often consult product support pages. The company now captures product support page data and repurposes it. The data, displayed in a Splunk Enterprise dashboard, informs in-house teams about the types of questions customers are most likely to ask so they can educate themselves about top-selling products, improve documentation quality and provide excellent customer service.
Single Source of Truth
Beyond application delivery and business analytics, Splunk Enterprise also supports critical security, fraud and compliance efforts. When the company had been using Splunk Enterprise actively for three years in various capacities, it discovered a new challenge that it believed Splunk Enterprise could solve. The company had encountered stability issues with its internal user authentication system and had teams monitoring it 24/7 during the busy holiday season. User authentication problems were time-consuming to triage because there were many places to look for issues.

Real-Time Fraud Monitoring; Automated PCI Compliance
Previously, the company had struggled with time-consuming manual PCI reporting. Several years ago, the company began capturing PCI data in Splunk Enterprise indexes. Since the company replaced manual PCI reporting, Splunk Enterprise provides a single place to look across multiple systems. Today, automated, continuous monitoring ensures the company meets PCI mandates.

Another time-consuming challenge in the past was fraud investigation. A typical fraud investigation took up to eight hours. With Splunk Enterprise, the company has a solution for company-wide detection, and a typical investigation takes only 20 minutes. Splunk Enterprise enables the company to detect and alert on suspicious activity, troubleshoot and support case investigation. Today, one group that manages online memberships relies on Splunk Enterprise to identify individuals who are gaming the system. For instance, if a new account is created and used only once for a product recommendation, that account and IP are flagged for immediate review.

Internet of Things Meets Retail
In addition to the many ways Splunk Enterprise solves business and technology challenges, one unique use case is helping to keep things cool – literally. This customer has attractive audiovisual displays in its retail locations designed to help attract walk-in customers. Previously, the audiovisual equipment overheated from time to time, causing it to malfunction. The company wanted to ensure the equipment in retail locations functioned consistently. One of its objectives was to have a dashboard that would provide visibility into the health status of store audiovisual equipment. Today, sensors measure the temperature of audiovisual equipment, the data is sent to Splunk Enterprise, and a dashboard enables employees to continuously monitor the equipment. If there is a problem, staff can jump in and adjust the retail location temperature to prevent the equipment from overheating.

Trillions of Events, Hundreds of Use Cases
In this customer profile, we explored how Splunk Enterprise helps one Fortune 100 customer solve a broad range of challenges. This customer uses Splunk Enterprise to capture all of its data and gain end-to-end visibility across the enterprise. Splunk Enterprise software is mission-critical for everything from business analytics to application delivery, providing a great customer experience and much more. The company leverages domain expertise from different teams in a highly integrated user interface. The easy-to-use interface empowers more than 10,000 users across the organization to identify and solve problems, enabling the company to do more with fewer resources. What began as a 100GB Splunk Enterprise license indexing a few hundred thousand events in 2007 has grown into a solution that analyzes trillions of events and multiple petabytes per day. Splunk Enterprise has proven to be a highly scalable solution that is becoming the company’s mission-critical data fabric across hundreds of use cases.
### About Splunk

Splunk Inc. (NASDAQ: SPLK) is the pioneer in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk provides the enterprise machine data fabric that drives digital transformation. More than 12,000 customers in over 110 countries use Splunk in the cloud and on-premises. Join millions of passionate users by trying a [free trial of Splunk](#).

<table>
<thead>
<tr>
<th>Industry</th>
<th>Splunk Use Cases</th>
<th>Splunk Products</th>
<th>Data Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>• Application delivery&lt;br&gt;• Security, fraud and compliance&lt;br&gt;• Business analytics&lt;br&gt;• IT operations&lt;br&gt;• IoT</td>
<td>Splunk Enterprise</td>
<td>• Application logs&lt;br&gt;• Syslogs&lt;br&gt;• Netlogs&lt;br&gt;• VPN data&lt;br&gt;• Security logs&lt;br&gt;• Authorization logs&lt;br&gt;• CISCO&lt;br&gt;• SAP&lt;br&gt;• NetApp logs</td>
</tr>
</tbody>
</table>