Finding Order(s) in the Chaos
How Splunk Software is Used to Troubleshoot Transactions

CUSTOMER PROFILE

Splunk customer profiles are a collection of innovative, in-depth use cases that highlight the value that Splunk customers gain from collecting, analyzing and visualizing the massive streams of machine data generated by their IT systems and technology infrastructures.

Each “real world” customer profile introduces a unique business challenge and shows how leveraging machine data and Splunk software in new and interesting ways has helped drive powerful business and operational outcomes.
Executive Summary

From the simple storefronts and shopping carts of the 1990s, e-commerce has grown into complicated supply chains and partner networks. The capturing, processing and fulfilling of orders has also grown, presenting a unique set of challenges. Losing orders within a complex network of internal and/or partner systems is one of the biggest nightmares for online retailers. Orders that fall between the cracks not only directly impact the revenue stream, they also damage customer satisfaction, the company’s reputation and long-term relationships with consumers.

With a complex stack of dozens of different software components handling up to four million online orders per hour, one Splunk customer, a large online retailer, found that Splunk software provided the visibility into its environment that it required to catch issues with orders before they could affect customers. Founded in the 1980s, this rapidly expanding retailer has $25B in annual revenue and more than 90,000 employees in over 25 countries.

Upon deploying Splunk Enterprise, the customer could visualize its online processes in dashboards for end-to-end visibility into order transactions across the enterprise. Specifically, the retailer defines transactions in Splunk software to monitor customer orders as they travel through the IT data integration backbone, a complex environment which consists of multiple, disparate applications. The retailer also gained visibility into its systems to better understand usage and trends and to enable its support and operation teams to detect problems before they impact customers. As a result, the retailer met its business-critical needs:

- Seeing beyond the complexity of the software stack. The retailer’s multiple, custom-built internal- and external-facing ERP applications do not use a single unique identifier for each transaction to correlate events from one system to another. Consequently, debugging issues that impeded transactions was extremely challenging. The support team learned of problems only when customers called to report unfulfilled orders. Splunk Enterprise now provides comprehensive optics across all systems to track transactions and identify issues.

- Simplify the troubleshooting process. Once an issue was reported, multiple members of the support and operations staff were frequently needed to identify and resolve the problem. This involved tracking, tracing and correlation of data manually through millions of lines of inconsistently formatted log entries, and trying to link unique identifiers from each individual system and silo. Tickets were passed from group to group while customers awaited resolution. Now that Splunk software coheres log events to display both holistic and granular views of the transaction chain, support staff can address issues rapidly and cost-effectively.

- Improve the customer experience. Company executives had been concerned about customer satisfaction issues. Support staff was always in triage mode, fighting fires and never getting ahead of the problem. Now with greater insight into its transaction processing, the retailer has improved the efficiencies of its online business to better meet customer expectations.

The Nightmare of Online Retailing—Orders Lost in the System

To support a business that has grown over the years to millions of transactions per hour, this online retailer built a multi-step, loosely decoupled ordering process and a corresponding IT architecture to underpin it (see Figures 1 & 2).

<table>
<thead>
<tr>
<th>Splunk Value</th>
<th>How Value Is Measured</th>
<th>Business Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-end visibility on customer orders</td>
<td>• Decrease in lost orders</td>
<td>• $900,000 annually in recovered revenue by preventing lost orders</td>
</tr>
<tr>
<td></td>
<td>• Faster resolution when customers inquire about orders</td>
<td>• Higher customer satisfaction and loyalty</td>
</tr>
<tr>
<td>Integrated, yet granular views across siloed systems</td>
<td>• Reduced Mean Time to Repair (MTTR)</td>
<td>• More efficient order fulfillment</td>
</tr>
<tr>
<td></td>
<td>• Reduced SLA violations for order processing and fulfillment</td>
<td>• Issue analysis and resolution accelerated by 25%</td>
</tr>
<tr>
<td></td>
<td>• No IT systems require re-architecting</td>
<td>• Reduction of lost revenue</td>
</tr>
<tr>
<td>High business value, low IT pain</td>
<td>• Rapid ROI via operational efficiencies, recovered revenue and a renewed focus on high value projects</td>
<td></td>
</tr>
</tbody>
</table>
Whenever orders went missing, troubleshooting issues through such a complex stack was a laborious task that required extensive IT resources over long periods of time. Since the IT systems involved—SOA, EAI-connected and platform-based services—were loosely integrated and the underlying data generated was siloed, tracing a particular customer’s transaction end-to-end was nearly impossible. Multiple applications with common fields but different identifiers made it extremely difficult to correlate data, which complicated matters further. As a result, issue tracking and resolution often took weeks or longer, which undermined productivity and customer satisfaction.

Enter Splunk

One reason the retailer sought out Splunk Enterprise as a solution was its desire to minimally impact its loosely coupled IT architecture and its complex, siloed data systems, which had taken years to build. Starting over to create a more tightly integrated system that could easily provide an end-to-end view of business transactions simply was not feasible. Instead, Splunk Enterprise allowed the retailer to leave the existing architecture unchanged while attacking the problem “bottom up” by aggregating, indexing and analyzing machine data across the entire environment (see Figure 3).

For a view of what this data can look like, Figure 4 below is a screenshot from the retailer’s key process orchestration system, the webMethods Service Bus. The top and bottom left are sample webMethods data and fields. The bottom right shows how the Splunk REGEX command pulls out special fields such as `ServiceName` and `OrderNum`, which are particularly useful for tracking orders.

Another key source of data is Tuxedo, a high-performance transaction processing system the retailer uses to commit order data into its ERP order systems. In Figure 5, log messages from
Figure 3. Collecting log data from all systems into Splunk Enterprise.

Tuxedo are in the left column, while the right column shows how the REGEX command extracts important data fields such as the application transaction number \texttt{(appl\_tran\_no)} and transaction error description \texttt{(xtrn\_error\_desc)}.

After pulling relevant data from such separate sources as webMethods and Tuxedo logs, the retailer connects the information using Splunk’s Search Processing Language (SPL™), specifically the transaction command. This step groups events from webMethods and Tuxedo systems together and builds an end-to-end trace for purchase orders.

\begin{verbatim}
> (sourcetype=webMethods\_log OR sourcetype=tux\_log) AND action=purchase | eval order_id = coalesce(orderNum, appl\_tran\_no) | transaction order_id
\end{verbatim}

This particular set of search commands looks through extracted webMethods and Tuxedo logs and informs the system that orderNum from webMethods and \texttt{appl\_tran\_no} from Tuxedo are the same data fields that uniquely identify each order. Splunk Enterprise then coalesces these two fields into a single new field \texttt{order\_id} and, lastly, uses \texttt{order\_id} to group and trace events in webMethods and Tuxedo.

**The Splunk Solution: Complete Order Visualization**

Using Splunk Enterprise to extract and group meaningful data from disparate systems, the retailer then created a number of dashboards that enable its IT and business users to visualize orders as they travel across the production environment.
A dashboard was created for IT operations to monitor transactions going through the retailer's integration backbone system (see Figure 6).

This dashboard shows a pie chart of the count of services that have sent any events in six single value metrics, breaking down the number of transactions versus failures versus SLA violations, as well as a table of these results. The retailer's IT operations team can then drill down into any particular service name in the chart for granular details. From the dashboard above, users can track a specific transaction via a unique transaction ID across all the disparate systems.

Figure 7 represents the transaction path dashboard, which allows a user to view details about a particular transaction. A successful transaction log shows the hops it went through, as well as the raw events. If there was a failure, the dashboard also provides a link to the integration page. This was a huge win for the IT developers because it enabled them to trace any problem to the error origin and even the error cause.

The retailer also uses Splunk Enterprise to aggregate transactional data for real-time optics into the volume of orders going through the system. Figure 8, for example, is an executive dashboard featuring a stack chart broken out by orders over a 30-day period by geography and business unit.

In addition, Splunk Enterprise has helped IT monitor the overall trends and health of the entire stack. The trends dashboard (see Figure 9) shows comparisons of services between days of the week, for entire weeks, and quarterly, as well as a stack chart of all the services during the previous month. When executives request this type of information, it can be made available instantly, enabling them to holistically view service levels and anticipate future needs.

Orders Found, Time and Revenue Regained

As retailers grow, they inevitably reach a stage where there are multiple in-house and partner systems that integrate to fulfill customer orders. One by-product of this growth and these multiple systems is order loss due to complex data integration. Order loss can significantly impact a retailer in terms of reduced revenue and customer satisfaction as well as expensive technical troubleshooting involving numerous resources and man-hours.

Rather than go through the costly, lengthy and unpredictable process of tightening systems integration or data warehousing, this particular retailer deployed Splunk Enterprise to trace orders throughout their life cycle. As with most Splunk customers, the retailer saw immediate value from Splunk software. By using the solution to track customer orders, the retailer has prevented up to 100 lost orders per week, with a corresponding $900,000 in annual revenue recovery. In addition, the retailer has enhanced
operational efficiency, saving numerous man-hours for the IT Support and Development Operations teams involved in troubleshooting. Since deploying Splunk software, these teams have found and addressed issues up to 25% faster, freeing up time for higher value projects.

Splunk software not only allows this retailer to extract critical business insights out of its application and systems data, the solution also enables the customer to improve overall operational efficiency and increase customer satisfaction.

With Splunk, They Found Order(s) in Chaos

In this use case, we explored how Splunk software can enable operational intelligence for a classic transaction/workflow challenge. Despite a daunting stack of dozens of different software components handling four million orders per hour, an online retailer has the optics to figure out when something has gone wrong and how to fix it. This use case demonstrated:

- **Elimination of data silos.** Because Splunk software indexes all kinds of machine data, the customer’s reams of siloed data no longer hinder its ability to quickly find lost orders and rectify underlying issues.

- **Correlations drive analytics.** Because Splunk software correlates different types of data, the customer links error messages in one system's logs to useful evidence in other logs to resolve issues.

- **Flexible analytics powered by a read-time schema.** Because Splunk software keeps the data unstructured, the customer views the data through the lens that matters at the time it queries the data, not the lens that mattered to the system at the time it generated the event.

- **Significantly reduced manual intervention and labor cost.** Because Splunk Enterprise provides real-time visibility of end-to-end data flow through the customer’s business process, the retailer tracks orders across disparate systems and reduces MTTR.

**One Splunk. Many Uses.**

While the business problems discussed in this case were specific to this customer and their industry, and the solution made creative use of Splunk Enterprise’s features to solve these particular problems, the underlying theories are applicable to a variety of single-path workflows.
With the right sets of data, Splunk can trace the time it takes for a specific file to go through a series of compression processes, which steps in an online purchase stymie the most customers, or which coupon-downloaders actually go into the store to buy the product.

While the possibilities are endless, the process is simple.

**Next Steps**

To learn more about Splunk customer success, customer snapshots, ROI stories, customer profiles and more, please visit: [http://www.splunk.com/view/customer-case-studies/SP-CAAABB2](http://www.splunk.com/view/customer-case-studies/SP-CAAABB2)

Splunk software is also available as a free download. Download Splunk Enterprise and get started today: [http://www.splunk.com/download](http://www.splunk.com/download)

If you would like to speak to a salesperson, please use our online form: [http://www.splunk.com/index.php/ask_expert/2468/3117](http://www.splunk.com/index.php/ask_expert/2468/3117)

**Free Download**

Download Splunk for free. You’ll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.