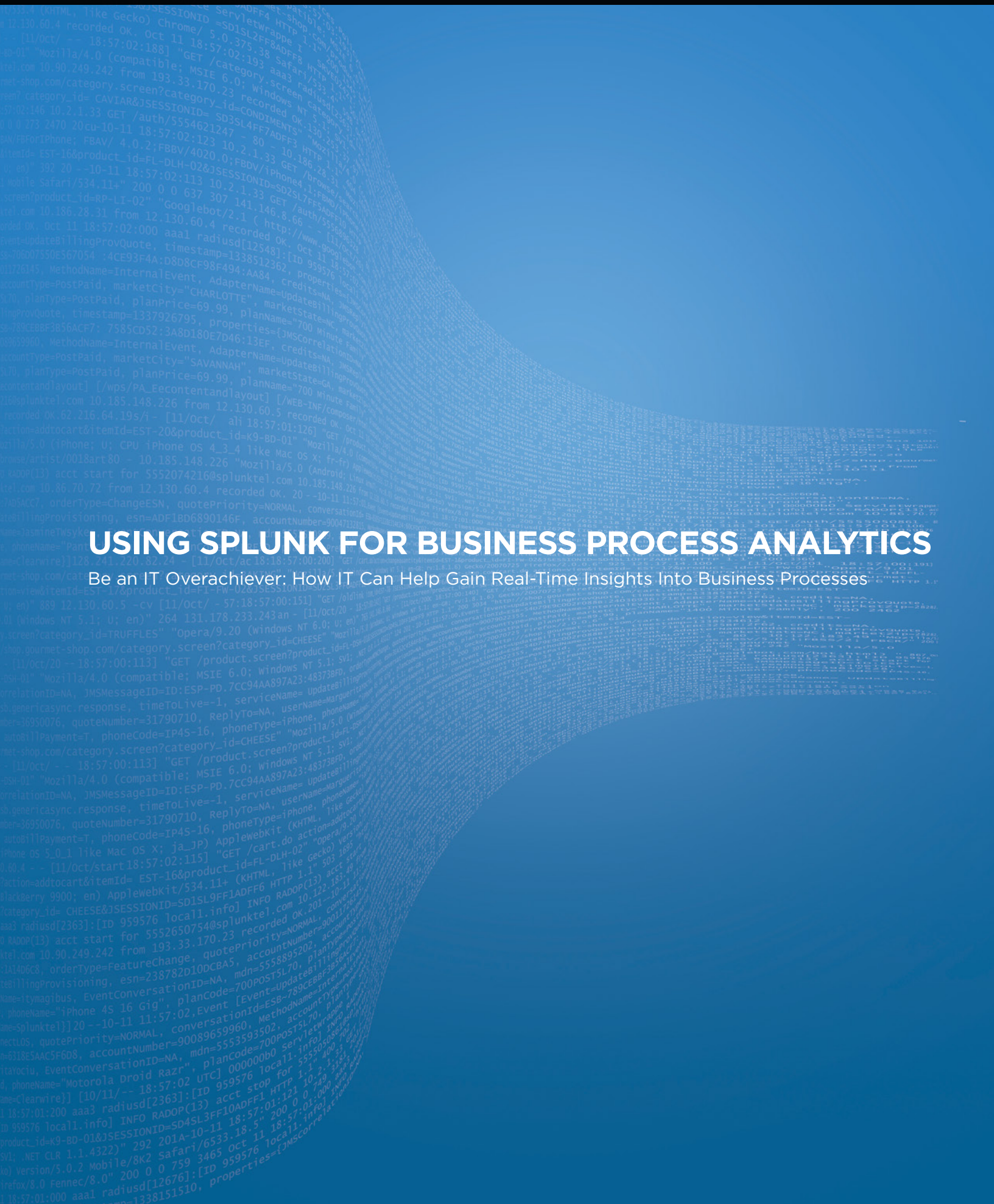
splunk>

GETTING STARTED GUIDE



USING SPLUNK FOR BUSINESS PROCESS ANALYTICS

Be an IT Overachiever: How IT Can Help Gain Real-Time Insights Into Business Processes

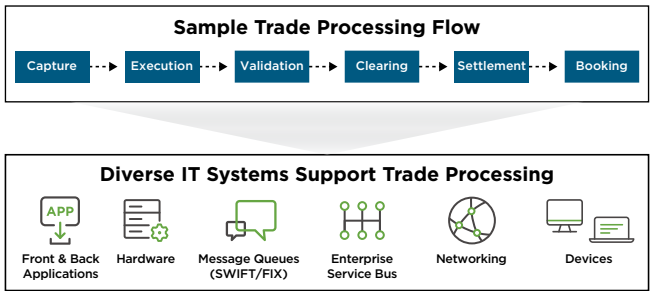
Introduction

Mobility and always-on connectivity means you can interact with businesses anytime, anywhere. That's why companies are digitizing their business processes—to deliver a superior customer experience, improve efficiencies and reduce costs. This provides a huge opportunity for IT to add more value to the business by simplifying increasingly complex IT systems—and leading to improvements in critical business processes.

This guide shares how you can use multiple sources of machine data for insights that improve your organization's business processes.

Business Processes Analytics—What Is It and Why Should IT Care?

A business process is a complex series of related activities that help accomplish a business goal. Your company's ability to measure, monitor and optimize business processes has a direct impact on revenue and customer satisfaction. Claims processing in healthcare, trade settlements in financial institutions, and new service activation in telecommunications companies are all examples of complex business processes.



Business process analytics is the end-to-end analysis of a business process in real time. The insights organizations gain by monitoring a critical business process can streamline operations. More specifically, real-time, end-to-end visibility into business processes can help you:

- Understand and improve customer experience
- Increase revenue by gaining insight into failed process steps
- Ensure successful business transactions
- Increase efficiency by identifying bottlenecks in business processes and reduce risk
- Comply with government mandates and regulations

IT organizations can play a unique role in helping their company gain real-time visibility into business processes and improve operational efficiency. However, the growing complexity of IT environments has made it increasingly difficult to gain these insights.

If that weren't enough, existing approaches to business process analytics deliver a siloed view into processes—they are not real time; don't correlate business events across business and operations data; and don't deliver a granular view for performing root-cause analysis.

Getting Started with Business Process Analytics

Many IT organizations already use Splunk software for application delivery and IT operations. The same indexed machine data can deliver insights to drive visibility into business processes.

Here is how Splunk can be applied in this use case:

Suggested Data Sources

Data Type	Where to Find It	What It Can Tell You
Application Logs	Local log files, log4j, log4net, Weblogic, WebSphere, JBoss, .NET, PHP	User activity, fraud detection, application performance
Business Process Logs	Business process management logs	Customer activity across channels, purchases, account changes, trouble reports
Call Detail Records	Call detail records (CDRs), charging data records, event data records logged by telecoms and network switches	Billing, revenue assurance, customer assurance, partner settlements, marketing intelligence
Clickstream Data	Web server, routers, proxy servers, ad servers	Usability analysis, digital marketing and general research
Message Queues	JMS, RabbitMQ and AquaLogic	Issues in complex applications and the backbone of logging architectures for applications
Web Access Logs	Web access logs report every request processed by web server	Web analytics reports for marketing
Mobile	SDKs embedded in mobile apps, application and server application logs	Mobile app usage, mobile app crashes, performance, latency, troubleshooting (stack trace) intelligence
Wire Data	DNS lookups and records, protocol level information including headers, content and flow records	Performance and availability of applications, end-user experiences, incident investigations, networks, threat detection, monitoring and compliance

Using Splunk for Business Process Analytics: An Example

Each organization has its own unique business processes—so it will have a unique way of using Splunk software for business process analytics. Never fear! Reading the example below can help shed light on how to analyze business processes for your own company.

This sample focuses on how Splunk software can be used to gain visibility into an order lifecycle—a key business process to understand the various stages of orders. Let's assume the order lifecycle consists of:

- Order capture through an online ecommerce application
- Order entry into an order management system
- Payment verification
- Order release and shipment

The scenario starts with a user noticing a high volume of incomplete orders.

1) Tracing transaction across multiple systems

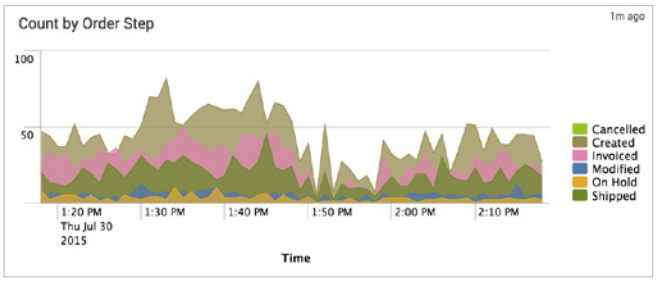
What to Look For?

Combine different custom application logs to gain visibility into how a transaction flows across different systems, action fields like "error codes" and "process step"

Why?

Tracing transaction flow between systems enables quick identification of process step having issues in the order lifecycle

Sample Search: `sourcetype=access_combined | stats count sparkline by order_status`



2) Finding successful transaction percentage

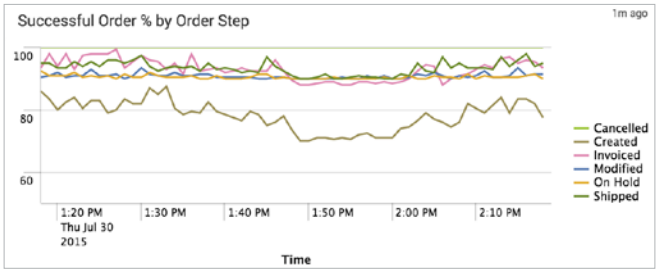
What to Look For?

Action fields like "error code" or "status" or "process step" to capture any issues with specific order process steps

Why?

Errors in processing orders leads to lost revenue

Sample Search: `sourcetype=access_combined | stats count count(eval(status_description="OK")) as count_success by action | eval percent_successful = round(count_success/count*100,0)."%"`



3) Calculating average time the order spends in different process steps

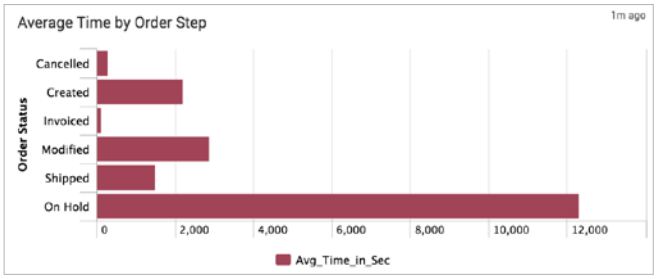
What to Look For?

Combine custom application logs and look for fields like "timestamps" to identify when a transaction crosses the process boundaries

Why?

Understanding how long an order spends in each stage helps identify opportunities for optimizing the business process

Sample Search: `sourcetype=access_combined order_status=* | stats avg(time_taken) as Avg_Time_in_Sec by order_status`



4) Alert on order volume

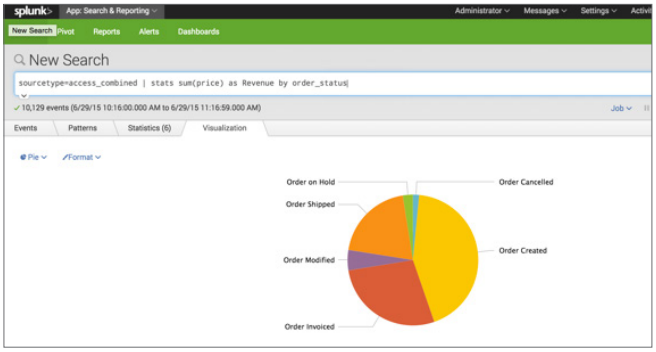
What to Look For?

Action fields like “total price” to gain an understanding of order volume stuck in each process step

Why?

Understand the potential revenue impact by process step due to slow order processing lifecycle

Sample Search: `sourcetype=access_combined | stats sum(price) as Revenue by order_status`



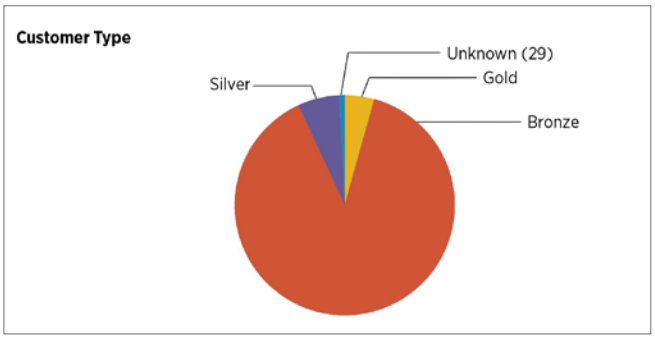
5) Understanding Customer Impact

What to Look For?

Using Splunk DB Connect, enrich machine data with customer profile data (structured data for example from CRM systems) to add additional business context

Why?

Combining order information with customer information reveals the impact of slow performing order lifecycle process on customers



Taking Business Process Analytics to the Next Level

Splunk Apps can add capabilities for business process analytics:

- The Splunk App for Stream (which enables real-time visibility from wire data)
- Splunk DB Connect (which enables integration between machine data in Splunk Enterprise with structured data from traditional relational databases)

Customer Spotlight: Cerner

Starting Out: Splunk for IT Operations

Based in North Kansas City, Missouri, Cerner Corporation is one of the world’s largest healthcare software IT companies. Cerner already had a large Splunk deployment comprised of 600 developers who use the software to enhance application development and management, monitor IT systems, and proactively detect and address issues. The result? Significantly reduced mean time to resolution (MTTR) and improved application performance.

Enter Splunk for Business Process Monitoring

Cerner had mastered the art of quickly identifying and resolving application performance issues by correlating logs across the application, middleware, OS and network to pinpoint issues. In addition to deploying Splunk Enterprise, the Cerner operations team also leveraged the Splunk DB Connect application to combine structured data with machine data to gain new insights into the real-time eligibility process.

Improving Process Efficiencies

Splunk Enterprise empowers Cerner to monitor patient eligibility business processes in a near-real-time manner. They now have views and analytics into data transactions between providers and insurers—enabling them to optimize eligibility verifications, ultimately leading to claims being processed and paid faster. Engineers monitor the data streams via Splunk dashboards, viewing such metrics as transaction volumes at any time, partner response rates and transaction errors. They can also apply filters to view data for specific clients, partners or payers.

When error rates for transactions exceed a threshold, the Splunk platform immediately issues alerts via email. Engineers can then quickly query the data to identify the failed transactions, determine the cause of their failure and take remedial measures. For example, they might detect that one of Cerner’s clients is improperly entering data for submission. Cerner consultants then will work with the client to correct the problem.

Read the Cerner success story.

Learn more about Splunk DB Connect and the Splunk App for Stream.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com