splunk> listen to your data™

CASE STUDY

Splunk at Nexa Technologies

Improved Response and Increased Service

nexa Technologies

"Splunk helps us improve customer service. We're closing queries almost as fast as we open them. With customer support handling most inquiries, our system administrators have gained about two hours of productivity per day."

Matt Easley
Customer Support Manager

OVERVIEW

INDUSTRY

- Financial Services - Trading Platforms

SPLUNK USE CASES

- Application Management
  Transaction Tracing
- Security
  Incident Investigations

BUSINESS IMPACT

- Standardized production team's efforts on centralized, secure system with automated transaction record reporting and monitoring
- Enabled system managers to gain two hours per day in time saved using Splunk
- Reduced customer request response time for urgent issues by an hour or more.
- Reduced broker response times on non-urgent requests from more than a day to minutes on the phone.

DATA SOURCES

- Syslog from hosts via a central forwarder
- Syslog from custom applications
- Financial Industry Exchange Logs (FIX)

The Business

Founded in 1999, Nexa Technologies' origin as an online brokerage firm makes it an ideal provider of brokerage and trading applications because its complete line is deployable in any market, any language and any currency. Today Nexa both develops and hosts browser-based trading solutions, direct access trading platforms, trade management and order routing systems as well as back-office and account management applications. With its common architecture and products designed by traders, Nexa helps brokerage firms around the world increase their market presence through improved compliance, client management and operational efficiency.

Challenges

Before Splunk, the brokerage support team relied solely on two very busy system administrators to access the activity logs containing official records of exchange settlements and other trading events. Even for these experts, finding a trade confirmation executed at the right price and confirming if the trader had enough buy power was a cumbersome process that took, at best, five minutes. This process involved running a homegrown script to retrieve a file of log events covering a specific time range and it needed to match specific criteria.

Since all 50 servers running the trading software generate a single log, retrieving the file from the production systems was only the first step. The file contained records that looked like:

8=FIX.4.19=6135=A49=INVMGR56=BRKR34=152=2000042

6-12:05:0698=0108=3010=157

Since the data was so cryptic, the support team needed the system administrators to grab the relevant information.

Using a command line text editor, this manual search took at least another five minutes. And if they didn't get the right data or if the trade they were looking for didn't occur within the specified time window, the system administrators would have to go back to the production system and begin again. In cases like this, the requests took up to an hour.

Since accessing information on the production systems was only a secondary part of their jobs, only the most urgent requests were responded to immediately. And although the highly skilled administrators spent one to two hours per day handling up to 15 requests, most of the time, they couldn't respond to the support team in less than a day.

Enter Splunk

The Nexa team first discovered Splunk Enterprise in 2005 when they downloaded a 30-day trial version. They rolled out Splunk 2.0 in early 2006, modifying the trading application to use Kiwi, a third-party Windows logging utility that provides a .DLL library that records log events. Kiwi runs locally on each Nexa Windows server, forwarding events in syslog UDP format to a central Linux server that runs Splunk.

Application Management

Rather than having system administrators run the homegrown script on their production systems, the Nexa support team now uses Splunk. The support team now securely accesses transaction records directly—saving valuable time.

When a broker wants to verify that a trade took place, the Nexa support person adds a specific order ID to a canned Splunk search to find the FIX settlement event. While brokers remain on the phone the support person can confirm whether or not it actually happened. If customers need details about their orders, support can search using Splunk by order ID and send the results via email.

Brokers also contact the support team with questions about their buy power, which Nexa calculates during the course of a day based on the broker's account activity. If a broker did not have enough buy power when an order was placed, the support person uses Splunk's View Source to find the three buy power calculations associated with the order ID in question. With this information, the support person can explain to the broker exactly what happened.

Security

Splunk also is also used for security incident investigations. If a user is concerned that their account has been compromised, the security team can easily check the logs to see if an unauthorized user or foreign IP address has accessed the account.

Breakthroughs

Splunk has helped Nexa streamline operations and improve their customer experience. Today they are using Splunk for common broker requests which significantly reduces the load on system administrators. Nexa estimates they have streamlined operations with 50% less labor time for 80% of the validation requests requiring a single pass through production data. They have further streamlined operations with approximately 80% less labor time for 20% of the validation requests requiring multiple passes through production data.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 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.