National Business Process Outsourcer Replaces Splunk Cloud with Devo for Modern Security Analytics

CUSTOMER SUCCESS STORY

A national business process outsourcer, turned off by the high cost of its upcoming Splunk Cloud renewal, decided it was time for a change.

In addition to the cost issue, the company wanted to use the opportunity to address other Splunk shortcomings, including ease of use and difficulties with several security use cases.

WANTED: A HIGH-PERFORMANCE, EASY-TO-USE SOLUTION THAT END USERS CAN CUSTOMIZE

A large, national business process outsourcer was approaching its Splunk Cloud renewal date, but the high cost of staying with Splunk Cloud compelled them to seek a true cloud-native alternative.

The company also had been frustrated by several shortcomings of Splunk Cloud. Most significantly, the firm's analysts disliked the Splunk user interface. The frustration of having to manage their workflow across multiple screens caused unacceptable delays. This small team lacked the budget to pay Splunk to customize their screens; but more importantly, they wanted to be able to do it themselves.

Splunk Cloud's poor performance was another major concern for the analysts. Queries took too long to return results, and the product was extremely inflexible and slow to respond to increases in data ingest volumes. Splunk's standard 90 days of data retention severely compromised analysts' investigations, and the cost of a longer retention period exceeded the company's budget.

Additionally, Splunk Enterprise Security never worked adequately to address the company's security use cases, especially threat investigation. Investigations lacked sufficient data, and analysts found it impossible to track down the necessary information within the product. This resulted in unacceptably low SOC performance metrics and fueled frustration among the analysts, leading several to quit.

WHY DEVO

Several critical capabilities made Devo attractive to this customer, including:

- Devo combines at least 400 days of historical hot data with the most recent data, making ad hoc query results across the entire data set virtually instantaneous, compared to waiting more than 24 hours for Splunk's results.

INDUSTRY: Services
HEADQUARTERS: North America

CHALLENGE

The high cost of renewing Splunk Cloud, including paying to extend data retention beyond the Splunk-standard 90 days, caused this large national business process outsourcer to seek an alternative. Frustration with Splunk Cloud's inferior usability, poor performance, and high analyst turnover due to their frustration with Splunk, also drove the decision to find an alternative logging provider.

SOLUTION

Devo delivers at least 400 days of hot standby data with high-performance querying and immediate scaling as data volumes increase. Analysts of all skill levels can use interactive Activeboards, and easily customize them to meet individual preferences.

REQUIREMENTS

- Better query performance, with results returned almost immediately
- More than 90 days of data retention on hot standby, without exorbitant added cost
- Easy-to-use interface, customizable by analysts without requiring professional services engagements
- A 100% SaaS architecture that enables fast and easy scaling as data volumes fluctuate

- High performance; because Devo does not index upon ingest, all data is immediately available for querying.
- The ability to easily scale and manage large volumes of data (e.g., multiple terabytes) and query as needed.
- The ability to easily analyze data, using the built-in Activeboards to bring machine data to life with rich visuals, intuitive dashboards, and interactive capabilities that can be used by both advanced and novice security professionals.
- Devo conducts queries via an easy-to-use graphical user interface, which appeals to casual users. Advanced users can take advantage of the Microsoft LINQ language, which is more widely known and user friendly than Splunk's SPL.
- The ability to ingest machine data in raw format from any source, including cloud provider log files, firewalls, security, as well as governance and compliance solutions.

THE DEVO PLATFORM: CLOUD-NATIVE SIEM, SOAR, UEBA & AI

The Devo Platform delivers a simplified, scalable, and high-performance SIEM solution with integrated behavior analytics, AI, and end-to-end SOAR capabilities. The Devo Platform arms your security team with unparalleled speed and scale, delivering full visibility of your data and risk posture.

- **Zero infrastructure for seamless transfer -** Zero central infrastructure required; quickly ingest any data source with wide ranging OOTB content on Devo Exchange.
- **Outstanding time to value -** We make migration painless and enable your team to start implementing critical security use cases quickly.
- **Preeminent security analytics -** No other SIEM on the market can match our speed and scale when searching data across real-time and historical data.
- **Upskill SOC teams -** The Devo Platform reduces analyst burnout and improves productivity with our at-a-glance visualizations, attack-tracing AI, and response automation.
- **Flexibility and customization -** Devo provides the flexibility to customize your deployment and maximize your existing tools with pre-built integrations.

COLLECT STORE ENRICH

ANALYZE VISUALIZE

Learn more at devo.com

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.