Global Automotive Supplier Chooses Devo Over Splunk Cloud to Get Security Analytics Back on Track

DEVO

CUSTOMER SUCCESS STORY

A top global automotive supplier dropped Splunk Cloud in favor of LogLogic a few years ago due to high costs. But they became so fed up with its inability to deliver results they considered a return to the prior vendor.

During the reevaluation, the team remembered how unhappy they were with the interface. So they expanded their search to include Devo. Another major issue they had was how difficult—if not impossible—it was to search easily and quickly across multiple data sources.

WANTED: A SOLUTION TO CENTRALLY MANAGE GLOBAL DATA THAT PROVIDES ANALYSTS WITH EASY VISIBILITY INTO THE ENTIRE DATA SET, AND CAN SCALE TO TENS OF TERABYTES PER DAY

A member of the Fortune Global 500, this North American automotive supplier with major facilities in EMEA and Asia had booted Splunk Cloud a couple of years ago due to its high costs.

Analysts were frustrated with how difficult it was to tie together all data sources, search across multiple sources, and obtain results quickly.

First, the company replaced Splunk Cloud with LogLogic, but the effort was unsuccessful. Because the automotive supplier has major operations in EMEA and Asia, it needs to centrally manage, enrich, and analyze across the entire data set, even when it is stored in other locations, to comply with data sovereignty requirements.

This specific need, along with numerous LogLogic shortcomings, raised concerns about compliance risks if the company couldn't manage and search all of its global data. So they jettisoned that solution and began a new search, revisiting their prior vendor while also examining Devo.

WHY DEVO

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

- 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.
- A much easier way to search across multiple data sources and support for use of subqueries, and searching by user name and host name.

INDUSTRY: Automotive Supply
HEADQUARTERS: Global

CHALLENGE

After dumping Splunk Cloud due to high costs and poor user interface and query performance, this top automotive supplier tried LogLogic, without success. It was eager to improve its ability to centralize data collection from EMEA and Asia, and upgrade analysts' ability to query the full data set. So, the team revisited their prior vendor and also considered Humio and Devo.

SOLUTION

Devo delivers the ability to ingest, store, and instantly query at least 400 days of hot historical data of any type in any location. Devo also gives analysts a user-friendly interface. This enables them to easily customize and execute queries and subqueries across multiple data sources using a single filter and get immediate results. The company's data volume is expected to spike sharply from connected vehicles, and Devo showed it can handle tens of TBs of daily volume.

REQUIREMENTS

- Easy data analysis, with intuitive dashboards analysts can customize without professional services help
- A much simpler way to ingest, centrally consolidate, and manage data from multiple sources, with the ability to easily query all the data and obtain fast results
- Certified for deployment on all major cloud providers, e.g., AWS, Microsoft Azure, and Google Cloud Platform
- Be scalable to immediately accommodate high-volume data bursts in the range of terabytes per day

- Devo conducts queries via an easy-to-use graphical user interface, which appeals to casual users. More advanced users can use the Microsoft LINQ language, which is more widely known and easier to use than SPL.
- Designed 'for the cloud' with a multitenant architecture, Devo enables deployment in all major cloud providers—including Microsoft Azure, Amazon Web Services, and Google Cloud Platform—for maximum flexibility.
- The ability to easily scale, ingest, and manage large volumes of data (e.g., multiple terabytes), regardless of geographic location, into a single, centrally managed data source that could scale to more than 50TB per day
- Because it doesn't index data upon ingest, Devo delivers high parsing performance with all data available for immediate query.
- 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 more than 24 hours for Splunk.

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 across real-time and historical data.
- Upskill SOC teams - Devo 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

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**.