

Multinational Credit Reporting Agency Replaces Splunk with Devo to Accelerate Cloud Shift



CUSTOMER SUCCESS STORY

BACKGROUND

A leading credit reporting agency was using Splunk on-premises and wanted to shift its data to the cloud. Splunk proposed a cloud transition solution, but it came with a very high TCO and additional post-purchase costs. This left the door open for competitors, including Devo, to propose a better approach.

With the agency's contract renewal fast approaching, they were seeking a replacement that could be deployed quickly and operational by the next fiscal year. The credit reporting agency determined that Splunk was not the right vendor for this cloud transition because the costs would be far too high.

WANTED: A CLOUD-NATIVE SECURE LOGGING SOLUTION THAT OFFERED MORE STORAGE AND COULD KEEP DATA HOT AT A LOWER TCO

This multinational credit reporting agency was looking to move from maintaining its data on-premises to a cloud-native SIEM. As the company continued growing, transitioning its SIEM to the cloud became urgent. The agency had been using Splunk's on-prem solution and considered converting to the Splunk Cloud license model. However, Splunk Cloud didn't offer sufficient flexibility. The agency kept searching for a solution that could safely move its SIEM to the cloud while providing access to essential baseline features for which Splunk would have charged an excessive amount.

The agency wanted to maintain the same amount of storage it had with Splunk while driving down its TCO. Because they had a great deal of historical data, they also were seeking a solution that would allow for a smooth transition of their data into the cloud platform they chose.

Once the customer determined they were ready to move their SIEM to the cloud, they narrowed their options to Splunk Cloud and The Devo Platform.



INDUSTRY: Financial services
HEADQUARTERS: North and Central America

CHALLENGE

This top credit reporting agency had been using Splunk in an on-premises deployment. But the agency — and its data needs — were growing rapidly. So, the company decided to optimize its operations by shifting to the cloud. The organization initially considered migrating to Splunk Cloud. However, the licensing model was inadequate for its needs. The agency's TCO analysis confirmed this transition would be cost-prohibitive, for example, the license only allowed for 90 days of hot data, leading the company to seek a different cloud-based SIEM.

SOLUTION

Devo provided the customer with a comparable amount of data storage at a 50% annual cost savings and enabled them to maintain 400 days of always-hot data. Devo also delivered a query speed that far surpassed that of Splunk and other competitors. Ultimately, Devo provided the best licensing model and storage plan for the credit reporting agency at a very reasonable cost.

REQUIREMENTS

- A cloud-based SIEM solution
- At least 90 days of hot data storage
- A smooth transition of historical data to the cloud
- An attractive licensing model and pricing

WHY DEVO

- Several critical components and capabilities made Devo attractive to the customer, including:
 - Devo could provide the same amount of storage to the customer (1 Petabyte) at half the cost of Splunk.
 - Devo provides at least 400 days of always-hot data. Splunk was only providing the credit reporting agency with 90 days of hot data, making it much harder to retrieve and query it.
 - Devo could easily migrate historical data into the cloud quickly and efficiently.
 - The Devo Security Operations application includes threat detection and hunting and threat investigation in the baseline cost. Devo detects and alerts on compromises before any damage occurs.
 - With Devo, the agency can run high-performance queries and have total real-time visibility of its cloud data from all sources.
 - The Devo licensing model is flexible, meeting both the agency's data demand and alerting needs. Splunk offered a cloud license model that failed to meet the organization's needs.

- **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.



Learn more at devo.com

NEXT STEPS

The multinational credit agency is confident in implementing Devo to carry out its cloud-based SIEM transition.

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.



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

© 2022 Devo All Rights Reserved

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.