Another Bank Moving to the Cloud Jettisons Splunk in Favor of Devo to Modernize and Scale Operations

CUSTOMER SUCCESS STORY

This large bank, while in the early stages of a cloud migration project, began searching for an alternative for its IT operations application monitoring needs. Having used Splunk on-prem for years, the team considered Splunk Cloud, but the combination of its price and the bank's dissatisfaction with Splunk's past performance drove them to look elsewhere.

A key to the bank's successful migration would be the ability of the solution to ingest multiple data types, from on-premises as well as cloud applications, since the transformation was expected to take several years and the team envisioned some applications never migrating to the cloud.

WANTED: A SOLUTION TO HANDLE DIVERSE DATA TYPES AND PROVIDE AN EASY-TO-USE ANALYST INTERFACE

A large, well-established bank in the U.S. was in the midst of its multiyear cloud migration and was not pleased with the high price of Splunk Cloud, especially given the performance challenges they experienced with on-prem Splunk over the years.

The bank's use cases centered around monitoring its IT operations banking application. Their goal was to centralize monitoring between cloud and on-premises data sources, since they were not initially going to be 100% cloud-based, with some applications never migrating to the cloud.

A key requirement was the ability to support the plethora of data sources—from simple to complex—that would span both environments, including: syslog, data sent via Windows Agents, MS-SQL databases, HTTP API calls, HTTP streams, Rabbit MQ, and Tibco Enterprise Service Bus.

Another essential need was the ability to scale to more than 1TB per day of ingestion volume, with the data available for instant query. The bank also was frustrated with how long it took to spin up historic data in its Splunk installation, and were eager for a faster solution.

Ease-of-use for analysts was also high on the bank's list. First, the new solution had to re-create the Splunk environment to which analysts were accustomed, to ensure a smooth transition. The bank also wanted analysts to have the ability to create their own individual and custom dashboards, but did not want them to have to learn a complex programming language to accomplish this.

INDUSTRY: Financial Services
HEADQUARTERS: United States

CHALLENGE

The high cost of Splunk Cloud led this bank to seek an application monitoring alternative in the midst of its cloud migration. The solution needed to meet the bank's data ingestion and immediate access requirements, while scaling to terabytes per day over time. Ease-of-use and the ability to customize dashboards were also priorities.

SOLUTION

The Devo Platform ingests all data types regardless of location, with immediate query capabilities and hot access to 400 days of historic data, while easily scaling data ingestion.

REQUIREMENTS

- Ingest many data types from both on-prem and cloud apps
- Query data immediately upon ingest, and have historic data available without delay
- Ability to scale and ingest multiple terabytes per day
- Easy for analysts to customize their dashboards

WHY DEVO

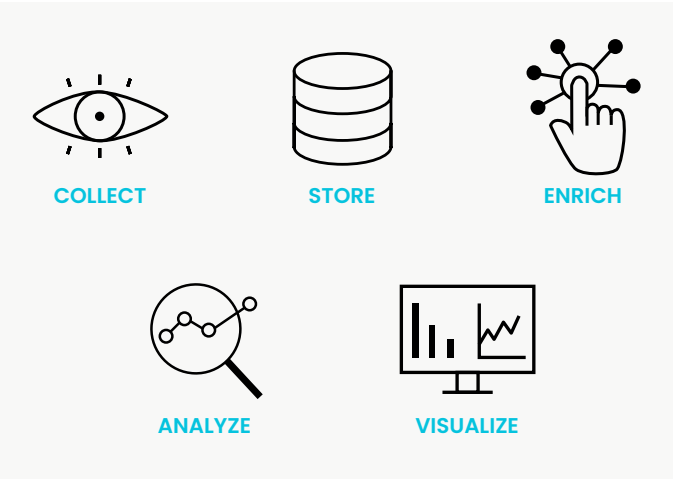
Several critical capabilities made Devo attractive to the bank, including:

- The ability to easily scale and manage large volumes of data (e.g., multiple terabytes) and instantly query as needed. Also, the ability to have at least 400 days of hot historic data, with no access delay to bring it into an investigation.
- The ability to ingest machine data in any format—especially unstructured data—from on-premises and cloud sources simultaneously.
- The Devo interface, with easy-to-use Activeboards, can be used by advanced and novice IT professionals. Using Activeboards, Devo was able to replicate the Splunk functionality while significantly reducing the complexity of the analysts' interaction with the system. For example, some activities that required more than 30 steps in Splunk now took less than five steps in Devo.

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.



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**.