Multinational Manufacturer Selects Devo to Replace Splunk

DEVO

CUSTOMER SUCCESS STORY

BACKGROUND

This major multinational manufacturer had been using Splunk as its SIEM but lost access to the staff who were familiar with operating the platform. As a result, the company was left with a complex piece of software and no subject-matter experts who could generate insights from the platform and train other team members. It became very cost-prohibitive for the company to continue working this way, and it would have taken too much time and investment to recruit people who knew how to use the solution.

The company was spending an outrageous amount of money for the Splunk license but wasn't deriving value from it. That drove the manufacturer to begin an urgent evaluation of alternatives.

WANTED:

With the company's Splunk renewal looming, the team began assessing SIEM alternatives. They needed a system to seamlessly replace Splunk. The manufacturer wanted a SIEM that could perform as well, if not better, than Splunk but at a lower TCO.

The manufacturer required the following features in a new SIEM:

- A single pane of glass that incorporates all threat feeds
- The ability to ingest SCADA data as well as data from SAP, CrowdStrike, Cylance, Active Directory and OKTA
- The ability to perform "impossible traveler" detection and quickly flag compromised user accounts
- The ability to replicate Splunk PowerConnect functionality for ingesting on-premises SAP data
- A user-friendly system the current staff could implement without having to add headcount

WHY DEVO?

- Multiple critical components and capabilities made Devo attractive to the customer, including:

INDUSTRY: Manufacturing - durables
HEADQUARTERS: North America, Latin America, EMEA, Asia

CHALLENGE

The company lost the team that operated its Splunk Enterprise Security deployment. The manufacturer deemed it too expensive to recruit new Splunk experts. The company decided it needed a new, user-friendly solution with which current staff could quickly become proficient.

SOLUTION

The Devo Platform was a perfect fit as the company's new SIEM. The manufacturer's existing team easily implemented the Devo Platform, eliminating the need to hire outside experts. Devo seamlessly replaced Splunk with improved performance, even detecting — within minutes — a security breach Splunk had missed.

REQUIREMENTS

- A single pane of glass that would incorporate all threats
- The ability to ingest SAP and SCADA data as well as CrowdStrike, Cylance, Active Directory and OKTA
- The ability to detect "impossible traveler" scenarios and flag compromised users
- A user-friendly solution the company's current team could seamlessly integrate

- Devo was able to provide the customer with a flexible license that met the customer's needs better than Splunk.
- Devo is a single platform that combined all threat feeds and provided full visibility.
- The Devo Platform could easily ingest on-premises SAP data.
- The user-friendly platform did not require the manufacturer to hire additional technicians. The current team quickly learned and become proficient Devo users.
- Devo was able to detect an "impossible traveler" within minutes of deploying the proof-of-concept. This revealed a compromised user account that Splunk failed to identify. This demonstrated that Devo was more strategically advanced.
- With Devo, this customer can ingest **2x the data at 25% their allocated budget, resulting in lower TCO.**

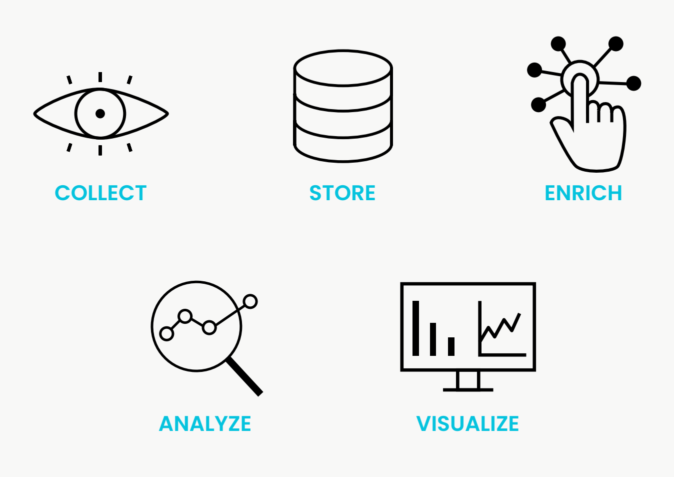
THE BOTTOM LINE

With the Devo Platform, this manufacturer can ingest 2x, increase visibility and better defend the organization at a significantly lower cost.

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**.