Top-15 Global Insurance Leader Chooses Devo Achieve Compliance

CUSTOMER SUCCESS STORY

As this top-15 global insurance company was in the midst of its shift to the cloud, it became obvious that its legacy ArcSight SIEM could not handle the transition. The firm had experienced a compliance-audit failure, due primarily to its lack of full visibility into data and events across the global organization.

To comply with data sovereignty regulations, the firm's subsidiaries in Asia and Europe, along with its North America headquarters, have to store data in its country of origin. The inability to securely access all of its data drove the company to address this critical issue by evaluating Splunk vs. Devo.

WANTED: A CLOUD-NATIVE MULTITENANT LOGGING SOLUTION TO PROVIDE UNLIMITED VISIBILITY

This top-15 (by assets) insurance company was beginning its cloud shift transformation project to support business growth objectives and initiatives. As a leader in a highly risk-averse industry and obligated to follow many regulations, the firm was undertaking its cloud shift project very deliberately. However, an audit failure drove the company to accelerate the update of its security operations.

As a worldwide organization with subsidiaries in North America, EMEA and Asia, the firm had petabytes of data stored in many countries to comply with data sovereignty regulations. However, the SOC team at headquarters also needed access to all the data to enable full visibility into the entire threat attack surface. This challenge was the key reason for the compliance-audit failure.

When the security team determined that ArcSight, its legacy SIEM, could not support the cloud-shift project, they searched for a true cloud-native solution, narrowing their search to Splunk and Devo. They identified four key requirements for the new vendor:

- Must be a true cloud-native solution, with a multitenant architecture so each geography
  stores its data locally and global security ops can view everything.

INDUSTRY: Insurance
HEADQUARTERS: North America

CHALLENGE

An insurance leader had to correct an audit failure by ensuring its global subsidiaries could retain data in-country while also enabling secure access for the HQ SOC team. For its shift to the cloud, the firm needed a true cloud-native solution.

SOLUTION

The Devo Platform delivers true multitenancy and high-speed ingestion of all data, makes data available for immediate query, and retains 400 days of hot data for comprehensive, accurate analysis. Built-in security controls—to the data level—help ensure compliance.

REQUIREMENTS

- 100% cloud application with multitenant architecture to keep divisional data separate but still securely viewable by the SOC
- Able to ingest on-premises and cloud app and log data, at scale
- Easy-to-use, modifiable role-based dashboards that only allow authorized data access
- Secure integration with other security apps, such as SOAR
- ML and UEBA to accelerate investigations

- Must be capable of ingesting both on-premises and cloud log and application data
- Must have standard dashboards and be easily modified by SOC analysts without requiring IT involvement.
- Must be able to create specialized, role-based dashboards that ensure each team member only has access to the data they are authorized to view via built-in security provisioning, especially role-based access controls.
- Must be extensible and accessible via secure APIs to facilitate integration with other best-of-breed solutions such as SOAR.

WHY DEVO

Several critical capabilities made Devo attractive to this insurance leader, including:

- Designed 'for the cloud' with a multitenant architecture, Devo enables deployment in all major cloud providers with the ability to maintain separate data sets as necessary, while also allowing a centralized view.
- The ability to easily scale and manage large volumes of data (e.g., multiple terabytes) in raw format—especially unstructured data—from on-premises and cloud sources and query immediately upon ingest.
- Devo combines at least 400 days of 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.
- Easy onboarding of all necessary data sources at a 0% drop rate
- Ability to view logs in 50 ms, enabling faster analysis and threat discovery to achieve compliance
- Queries are conducted via an easy-to-use graphical user interface that is ideal for casual users.
- Using Devo's ML entity models to find hidde and understand behavioral change by cla entity behavior changes over time, while a classifying, predicting, and characterizing hard-to-detect malicious domains.

THE BOTTOM LINE

Devo successfully transitioned this customer off Arcsight to Devo, enabling the team to pass its security audit and address all prior audit failures within the first 90 days of going live.

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.

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**.