Global Consumer Transportation Company Chooses Devo Over Elastic for Enterprise Log Management and Security

CUSTOMER SUCCESS STORY

A large, multinational consumer transportation company with a 100% remote workforce discovered an employee had downloaded sensitive information they were not entitled to access. As a result, the company prioritized increasing its overall visibility and security posture.

To accomplish this, the firm needed to dramatically improve its ability to ingest and combine data from assorted cloud services and legacy apps relied on by remote workers, which Elastic was unable to do.

WANTED: A SOLUTION TO COMBINE, ENRICH AND QUICKLY ANALYZE CLOUD AND ON-PREMISES DATA

Even before the pandemic, this large, global consumer transportation company's workforce was 100% remote and scattered around the world. As a result, the company relies on a wide variety of cloud services as well as on-premises applications.

The business had been experiencing numerous challenges with its existing vendor, Elastic. But the belated discovery that an unauthorized internal user had downloaded sensitive information drove the company to take decisive action to improve its overall visibility and security posture.

Obtaining greater visibility across the entire attack surface became the highest priority. The business's diverse data needs range from cloud sources such as Amazon GuardDuty, Jamf Pro, Telegraf, Duo, Okta, and G Suite, to legacy on-premises applications.

Such a wide variety of data sources proved too challenging for Elastic to ingest, enrich with third-party intelligence, and analyze quickly. This drove the transportation company to find a new provider.

WHY DEVO

Several critical factors made Devo attractive to the customer, including the ability to:

- Ingest machine data in raw format from any source, combine it with on-premises sources, and centrally manage it.
- Automatically enrich data with third-party intelligence to facilitate analysts' threat-hunting and investigation workflows.

INDUSTRY: Transportation
HEADQUARTERS: United States

CHALLENGE

This global consumer transportation company was struggling with its security solution's inability to ingest and analyze cloud and on-premises log data. When an insider threat was discovered after the fact, the company sought a new provider that would enable the business to be more proactive and accurate.

SOLUTION

The Devo Platform ingests and automatically enriches raw data from both cloud and on-premises sources. Analysts can easily customize their dashboard, and work with the data immediately upon ingest. As a cloud-native solution, scalability and performance are not an issue.

REQUIREMENTS

- Ingest both cloud and on-premises data in raw format
- Centrally manage data, enriched with other intelligence sources
- Visual, easy-to-use interface, which analysts can customize
- Scalability to meet growing data volumes

- Easily analyze machine data, using the built-in Activeboards, and bring it to life with rich visuals, intuitive dashboards, and interactive capabilities.
- Easily scale and manage large volumes of data (e.g., multiple terabytes) and query as needed.
- Attain a lower TCO via significantly reduced hardware costs for compute, storage, and ingress/egress costs because Devo is a true SaaS solution.

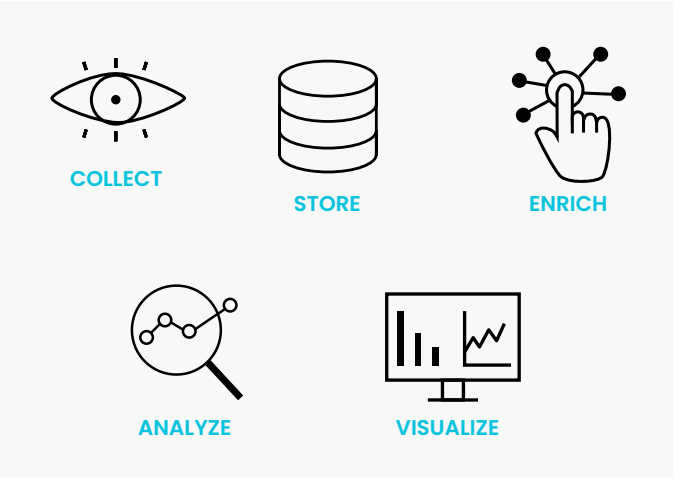
NEXT STEPS

Because Devo is able to centralize data of all types, other groups in the company, such as IT operations and business intelligence are investigating using 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 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 toolswith 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**.