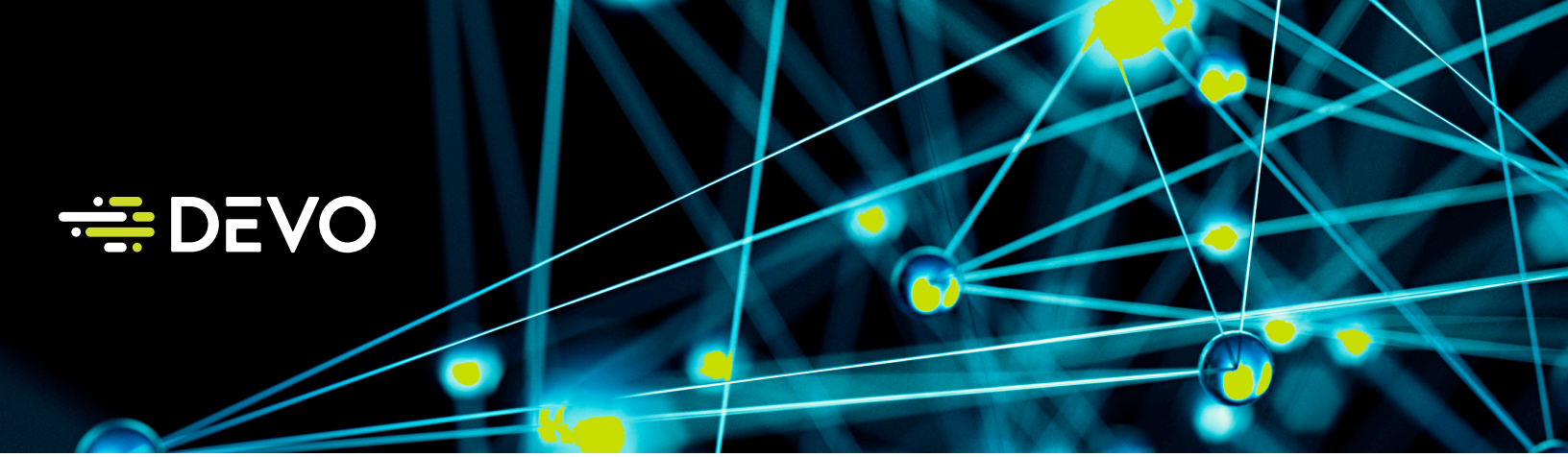

Shifting from Legacy Security Analytics to Devo

A customer case study

Enterprises face a number of challenges with legacy security analytics solutions; they have failed to keep pace with the volume of machine data being generated and the demands being placed on that data. One of our customers – a top 5 clothing retailer – faced these challenges with its existing Splunk Cloud deployment. Data collection constraints forced by Splunk's licensing and data retention limits and poor query performance meant the company struggled to improve its threat detection capabilities. By leveraging the Devo cloud-based security analytics solution for its Security Operations Center (SOC), the retailer was able to move beyond the constraints of its previous solution and improve its security posture.

Why they switched

A confluence of issues led the customer to make the switch. The company's highly-instrumented environment generates 10s of TBs of machine data per day from 100+ data source types. Great demands are placed on this machine data by hundreds of users extracting analytics, from dashboards to ad-hoc queries, as well as applications such as SOAR systems generating queries. Our customer was unable to react to and prevent security breaches fast enough with its previous solution.

Missing data

One major issue the company encountered was incomplete query results. Data was missing from queries for a couple of reasons:

- New product rollouts caused very bursty periods where 2-3TB of data would be generated in 30 minutes. Not only was this data taking hours to appear in their existing solution, but also the company maxed out buffers and dropped data.
- The large deployment meant the company was constantly dealing with indexers going down, which led to incomplete query results being returned – silently and without warning to the user.

INDUSTRY: APPAREL

LOCATION: USA

CHALLENGE

Our customer needed to improve its SOC's security analytics capabilities in order to better protect their business and their brand.

SOLUTION

The Devo Data Analytics Platform allows our customer to collect and make use of all their security relevant data. Devo enables their security analysts to hunt for, detect, and investigate indicators of compromise significantly more quickly and respond to security incidents.

RESULTS

- 100% of security relevant data ingested and queryable
- Query times reduced by up to 98%
- Time-to-alert measured in milliseconds
- All users capable of executing queries in real time
- 400 days of data retained, always hot and encrypted

Inflexible and expensive license costs

The company could not collect all its machine data due to prohibitive licensing costs and capped data at 6TB/day, forcing operations and security staff to make tradeoffs on the data they could ingest. Our customer required that data be retained encrypted and hot for 400 days, increasing costs. Also, during the last contract renewal the customer was discouraged from storing data for longer than 90 days, and were being locked into a longer-term contract – neither of these tradeoffs were acceptable.

Degraded performance

The customer was also disappointed by the performance of built-in alerts, some of which were generated hours after an event condition occurred. The 300 users were straining their previous solution to the point where query performance was degrading, increasing MTTR for security incidents and made threat hunting challenging.

Shifting to Devo

After they migrated to Devo, the difference was stark. Our customer is now able to affordably ingest all its machine data and support all the users and systems who need access to it – all with a significant performance increase and limited data management overhead. Additionally, Devo offers a flexible UI, enabling users to rely on just thirty-one dashboards, instead of the over one hundred previously needed. Additional major benefits included with Devo are:

- 100% of machine data ingested now queryable
- Deployment capable of supporting 10x bursts without dropping an event
- Query times reduced by up to 98%
- Time-to-alert measured in milliseconds
- All users capable of executing queries in real time
- 400 days of data retained, always hot and encrypted

What Devo enabled

Due to the architectural advantages of Devo, for the first time our customer was able to ingest and retain all their data, going from 6 to 10TB/day, currently cresting at 18TB/day. This scaling was possible with no need to re-architect the solution. With just ten Devo Data Nodes the customer can support a 20+TB/day daily ingest rate while supporting 10x bursts, all while responding to thousands of concurrent queries – without dropping an event or waiting long periods for queries to complete.

Not only is Devo able to exceed the needs of this large enterprise customer, it does so with fewer resources and delivers incredible performance, an example of how the Devo no-compromise architecture translates into differentiated capabilities for customers. With these capabilities our customer is able to address the following use cases:

1. Detect DDoS Attacks
2. Detect Brute Force Attacks
3. Provide Data Loss Protection
4. Perform Network Traffic Analysis
5. Implement Bot Monitoring
6. Analyze IP Traffic
7. Enable Malware Detection
8. Monitor Threat Activity