Global Retail and Commercial Bank Chooses Devo for Centralized SIEM Solution

CUSTOMER SUCCESS STORY

After spending more than two years and several million dollars, a large global retail and commercial bank realized its security incident response efforts were still failing to ingest all of the structured and unstructured data from both on-premises and cloud sources. This left the bank vulnerable to data breaches and compliance failures due to its inability to adequately analyze threats.

Digital transformation is one of the bank's key strategic business objectives. The CISO determined that more than 80 percent of its security technology was not designed to run in the cloud. The bank knew it had to bring in a trusted partner that could provide a solution to support both structured and unstructured data from any source.

WANTED: A SOLUTION TO BRIDGE THEIR CLOUD MIGRATION

While many customers today are undergoing digital transformation, the reality is that a large number of key applications, especially security, were designed for on-premises use only and will never migrate to the cloud.

The bank employs a wide variety of security solutions—from endpoint to network—to help protect against cyberattacks. The institution had been attempting to implement a SIEM solution to provide centralized data collection and analysis. But despite investing large sums of money on multiple solutions, its efforts were fruitless.

Each SIEM solution had its drawbacks; some could only work with on-premises security solutions, while others were limited to working with cloud-based solutions. A SIEM solution the bank acquired more than two years ago promised to support both on-premises and cloud data sources, but failed to deliver.

The bank has more than 100 different data source types, comprising both structured and unstructured data, which is why it long sought a single solution to provide SIEM functionality.

Another of the bank's key requirements was performance. On a daily basis, terabytes of data need to be quickly ingested for analysis.

After spending millions of dollars with the aforementioned vendor, the bank was looking for a company that could be trusted to deliver the urgently needed results.

INDUSTRY: Financial Services
HEADQUARTERS: North America

CHALLENGE

This global bank needed to shut down a failed, multi-year SIEM project and centralize its log management across on-premises and cloud security sources, ingesting copious amounts of unstructured and structured data—while also supporting its ongoing digital transformation initiative.

SOLUTION

The Devo Platform easily ingests all of the bank's data from any source in any format, providing real-time insights that help improve performance, security, and protection from cyber threats at scale.

REQUIREMENTS

- Daily ingestion of more than 3TB of data from more than 100 data source types
- Unified collection of structured and unstructured data for improved efficiency and security
- Simultaneous support for on-premises and cloud data sources
- Cost-effective data infrastructure well-suited for peak demand while delivering a lower TCO

WHY DEVO

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

- The ability to consolidate 3-4 SIEMs into one global solution.
- Designed 'for the cloud' with a multitenant architecture, Devo enables deployment in any cloud-provider.
- The ability to smoothly ingest large volumes of data (e.g., multiple terabytes) and query as needed.
- The ability to ingest over 100 different data sources — especially unstructured data—from any source.
- Lower TCO via significantly reduced hardware costs for both computing and storage by keeping cloud data in the cloud and on-premises data on premises, which cuts ingress/egress costs.
- The Devo team's willingness to partner with the bank to solve its needs, in contrast with previous vendors' "take it or leave it" approaches.

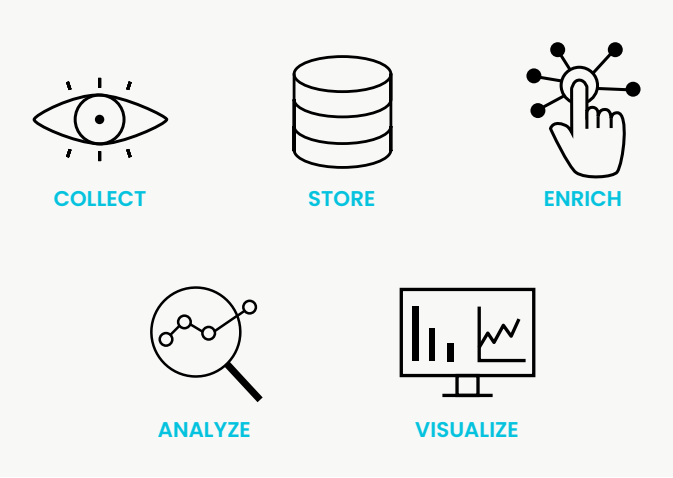
THE BOTTOM LINE

By implementing a single solution that enabled both unstructured and structured data from on-premises and cloud sources, the bank is able to provide more effective threat detection and response by quickly analyzing cybert hreats. And doing this with a lower TCO has facilitated its digital transformation and migration to the cloud while also helping to meet its regulatory requirements.

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**.