Pro Sports League Unlocks Power of All Machine Data Sources with Devo

CUSTOMER SUCCESS STORY

When one of North America's major professional sports leagues realized that its existing open-source security analytics solution, Graylog, couldn't scale to meet its growing needs, the league began scouting for a high-powered replacement.

The league's head of IT and security saw this as an opportunity to bring in a solution that could leverage the massive volumes of machine data generated across the league from enterprise applications, game operations, broadcasting and merchandising.

WANTED: A SOLUTION TO HANDLE DIVERSE DATA TYPES

Like most professional sports leagues, this organization doesn't own the sites where franchise teams play their games. That's why it's critical the technology the league uses must be capable of working in diverse data environments, e.g., Checkpoint at one site, Palo Alto at the next, etc. It also must be able to scale up to handle the peak amounts of data generated during games.

Unlike most businesses, where network load is relatively consistent from day to day, a professional sports league operates on a vastly different schedule. When there are no games being played, the network load is relatively minimal. But at game time the league needs 100 percent capacity as game operations, broadcasting and related activities ramp up. Traffic levels spike 500 percent when the action begins, and that continues for the duration of each game. That's why this pro sports league needed a no-compromise data architecture.

WHY DEVO

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

- The ability to work with a wide range of IT and security infrastructure
- The ability to ingest machine data in raw format from any source
- The ability to smoothly handle performance peaks during games

INDUSTRY: Professional Sports
HEADQUARTERS: North America

CHALLENGE

This professional sports league needed to improve upon the performance of the open-source security operations solution it was using, while also fully leveraging all of its operational data.

SOLUTION

The Devo Platform easily ingests all of the league's data, to provide real-time insights that help improve operations and security.

REQUIREMENTS

- Daily ingestion of up to 2TB of data from more than 100 sources
- Unified collection of operations and security data for improved operations and security
- Cost-effective data infrastructure well suited for peak demand during games and minimal usage at other times
- Real-time insights into enterprise applications

THE RESULTS

Devo gathers and centralizes up to 2TB of data each day for the league—from more than 100 data sources. Previously, 80 percent of the data the league collected for network and IT monitoring was also collected by the security team, using separate solutions, which added unnecessary cost and complexity.

Devo made it easy to unify all the data so the league could collect it once for use by analysts in various groups. This greatly enhances efficiency and responsiveness, as the same data is used for many use cases.

The league relies on Devo for logging, threat hunting, application monitoring, and network infrastructure monitoring. The organization now collects 100 percent of its security-relevant data for security operations center (SOC) analysts to query. The time to alert is measured in milliseconds, greatly improving the league's security posture.

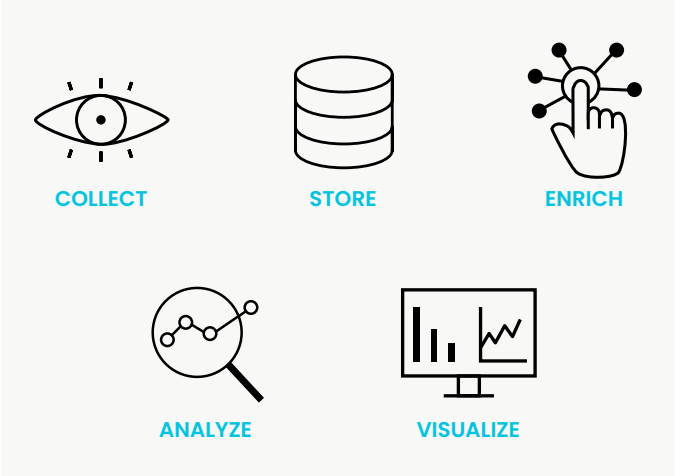
BOTTOM LINE

This professional sports league has been able to ingest all necessary data and action upon it at scale with Devo. The team has been able to leverage its increasing volumes of data and use the insights gleaned to improve operations and security for all teams under its umbrella.

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**.