

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
-

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

Pro Sports League leverages Devo to unify all its data and leverage its increasing volumes of data and use the insights gleaned to improve operations and security posture.

THE DEVO PLATFORM: CLOUD-NATIVE SIEM, SOAR, UEBA & AI

Devo's cloud-native architecture allows Pro Sports League to collect 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.

- **Zero infrastructure for seamless transfer** Devo's cloud-native architecture allows Pro Sports League to collect 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.
- **Outstanding time to value** Devo's cloud-native architecture allows Pro Sports League to collect 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.
- **Preeminent security analytics** Devo's cloud-native architecture allows Pro Sports League to collect 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.
- **Upskill SOC teams** Devo's cloud-native architecture allows Pro Sports League to collect 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.

A A



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.