Enterprise Cloud Data Management and Backup Software Company Jump-Starts its Cybersecurity Initiative with Devo

DEVO

CUSTOMER SUCCESS STORY

A leading enterprise cloud data management and backup software company has seen its growth explode and needed to build an in-house security operations center (SOC) in order to proactively provide world-class security support to its customers.

The team was previously using Elastic but wanted a complete solution that they did not have to build themselves. They turned to in-market solutions that could ingest multiple data sources, especially cloud-based data.

WANTED: A SOLUTION TO BUILD A WORLD-CLASS SOC

This high-growth cloud data management and backup provider was jump-starting its cybersecurity efforts.

The company's cybersecurity staff identified an immediate need for an enterprise log management solution capable of handling large amounts of log data and which would serve as the foundation for the SOC.

The log data was coming from multiple sources, from endpoints to firewalls, as well as cloud and security products. The staff recognized the value of using a proven solution instead of building it themselves—saving considerable time and money for an organization operating in an extremely competitive market segment.

WHY DEVO

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

- Designed 'for the cloud,' Devo enables deployment in Microsoft Azure, Amazon Web Services, and Google Cloud Platform, providing maximum flexibility.
- The ability to ingest machine data in raw format from any source such as cloud provider log files, firewalls, security, as well as governance and compliance solutions.
- The ability to send event data and analysis files via secure API to an MSSP partner so the MSSP can perform Level 1 support.
- The Devo interface with easy to use Activeboards can be used by advanced and novice security professionals.
- Many large enterprises successfully use Devo, demonstrating a proven track record that more than exceeds this company's requirements.

INDUSTRY: High Technology
HEADQUARTERS: North America

CHALLENGE

This enterprise cloud data management and backup provider had an immediate need to establish in-house security capabilities, revolving around its own SOC. They identified a key first step as selecting a complete end-to-end enterprise log management solution.

SOLUTION

The Devo Platform met and surpassed the company's needs by accommodating all three major public cloud providers along with a wide variety of data sources.

REQUIREMENTS

- Enable deployment on the big three public cloud platforms
- Ingest machine data in any format from a variety of sources such as firewalls, endpoints, and other products
- Securely send event data to partners such as an MSSP via API
- Demonstrate proven large-scale capabilities in similar situations
- Be capable of use by select people outside of the security team

THE BOTTOM LINE

Because Devo made it easy to kick off development of its in-house SOC, this company was able to quickly provide additional value to its customers and partners. With Devo, this cloud data management provider is able to consolidate its workload and centralize operations, all while boosting analyst efficiency and improving the team's security posture.

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.

COLLECT STORE ENRICH

ANALYZE VISUALIZE

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**.