

Attain EL3 Compliance — Without Busting Your Budget



PUBLIC SECTOR

Drowning in the cost of storing log data? Struggling to move to ELI? You now have options.

Do you need to ingest log data to meet the EO M-21-31 logging requirement? Then you need Devo.

Devo is a cloud-native logging and security analytics platform that enables you to ingest and query legacy on-premises data as easily and quickly as you can access real-time streaming cloud data. Devo provides deeper insights that improve security and enhance operations at half the cost of legacy solutions.

Splunk customers pay a high cost to consume, ingest and store all of the data required for proper cyber analysis. Devo provides a variety of deployment options to meet your individual needs:

OPTION 1:

- Keep Splunk as the front-end analysis tool for the first 90 days and move the rest of your data to the Devo Platform for analysis and compliance. This would keep your security operations center (SOC) team focused on immediate threats with no transition/training, satisfy the mandates, and provide less short-term risk. By switching to Devo for logs past 90 days customers typically save between 25% and 50% of what they're paying for Splunk on the licensing cost alone. Since Devo is built for the cloud and doesn't require in-house maintenance, SMEs, or infrastructure, you could save up to 80% of what you're currently paying. Because Devo includes 400 days of always-hot data in the price, your cost of storage will decrease by 50%.

OPTION 2:

- Deploy Devo on the front end and get 400 days of always-hot data in the cloud. You can move the rest of your data into Splunk for historical analysis. This would reduce the total cost of ownership for your self-managed solution by up to 50% while allowing you to collect and store the data you need for regulatory compliance. In addition, it would allow your Splunk-trained team to continue using Splunk while your SOC analysts focus on immediate security challenges without needing to be Splunk Query Language experts.

OPTION 3:

- For data that you aren't collecting in Splunk, you can deploy Devo to pick up logs that are 'being dropped on the floor.' This will eliminate visibility gaps in your environment for items such as DNS, NetFlow, SCADA, IoT, VPC flow logs, and more. Devo can easily collect, store, analyze and safeguard microservices in the cloud, including containers and serverless technology.

OPTION 4:

- Replace Splunk with Devo. This would save you the most money, enable you to achieve compliance, and support future growth. We are confident you will accomplish this with minimal risk. We can show you what your savings will be after discussing the details of your environment.



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

© 2022 Devo All Rights Reserved

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.