Sumo Logic

Review From A Customer

Sumo Logic

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

AWS Operations Engineer at MR

AwsOpera2176

WHAT IS OUR PRIMARY USE CASE?

We use it for ingestion of VPC flow logs, CloudTrail logs, and config logs from AWS.

HOW HAS IT HELPED MY ORGANIZATION?

We also use it to ingest Windows domain controller logs. We use this to monitor if anyone is placed in particular administration groups that potentially shouldn't be. It helps us keep track of people.

WHAT IS MOST VALUABLE?

The dashboards are great. We use them for monitoring certain events when they happen to see if we want to act upon them. The monitoring pages and the alerting pages are also very handy.

WHAT NEEDS IMPROVEMENT?

If you want to up your subscription through the AWS Marketplace, it can be difficult. You can't just go back to the AWS Marketplace, and say, "I want a bigger one now." You have to contact the sales team, then they do it on the back-end. This could definitely be improved. If they could do something about this, it would be nice.

FOR HOW LONG HAVE I USED THE SOLUTION?

One to three years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It is very stable. I've never really seen it have bad performance issues. As long as you're using optimized queries, then it always performs very well.

Sumo Logic

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

I don't think I have ever had a performance problem with it. The scalability is good. We have multiple different customers who ingest different amounts based on their workloads and environments. We have ten customers with our biggest customer ingesting around 18G a day. Across all our customers, we might be ingesting around 50G a day.

HOW IS CUSTOMER SERVICE AND TECHNICAL SUPPORT?

The support team at Sumo Logic is great. They have great people. They give good support when and if we need it.

HOW WAS THE INITIAL SETUP?

The integration and configuration of Sumo Logic into our AWS environment was easy and great.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

Purchasing the solution through the AWS Marketplace is very easy. We chose to go through the AWS Marketplace because it makes it a lot easier when we bill our customers. Rather than having to get multiple different sources of information then correlate a monthly bill for our customers, it is just included in the AWS usage charges. Thus, it's convenient. The AWS Marketplace pricing is fairly reasonable for what it does. Compared to the other tools that do it as well, it's reasonable. I wouldn't call it expensive, but I wouldn't call it cheap. It is pretty good.

WHAT OTHER ADVICE DO I HAVE?

We love the product and haven't had any bad experiences with it. We integrated it with Windows Active Directory. With one of our customers, we integrated it with some security software. It was some antivirus platform. We worked with their security team to ingest some logs that they used at the time and queried the data that they ingested. It integrates easily with other products. You just have to install the Collector. Then, as long as you know what the format of your logs are like, you can write your field extraction rules, and away you go. As long as you know what you're doing, and as long as you are familiar with the logs that you're ingesting, then it is easy. We ultimately use it because we are a managed services partner of Amazon, and we need to do it for our ordering purposes. It's just something that we have to have to be able to look at our logs in a dated manner. I would tell people to not get Sumo Logic if you are looking for a traditional monitoring software, because that was not the purpose it was written for. They should get it if they are looking for a log ingestion and aggregation system. We use the AWS version of the product.