LogRhythm NextGen SIEM Review From A Customer

IT Central Station
Unbiased reviews from the tech community

LogRhythm NextGen SIEM

Review by a Real User

Verified by IT Central Station

Security Analyst at a financial services firm

it_user756411

WHAT IS MOST VALUABLE?

The most valuable part of the solution is being to view all of the logs whenever you want. Any time an issue comes in or something that needs to be researched, I have the logs there. I can go in, run an investigation. It's pretty much at my hands. Information is available on demand. I feel like I'm in control of it, which gives me warm, fuzzy feeling.

HOW HAS IT HELPED MY ORGANIZATION?

Pro's and con's I would say. We are short staffed, like the majority of the people are here at the LogRhythm World conference. We have a lot of alarms that get overlooked, there's not a lot of prominence to them. So our SLAs are over extended. But other than that, we're getting alerted on things that we need to quickly look at, glance, and see what needs our attention right away. Usually, anything that's really hot, urgent, rated 90 or above, we answer those right away, and get those tasks completed.

WHAT NEEDS IMPROVEMENT?

If they continue to do innovation, and listen to their customers, then they'll move forward, and I think that will be the best thing for all parties involved.

WHAT WAS MY EXPERIENCE WITH DEPLOYMENT OF THE SOLUTION?

One thing that surprised me was how many logs were being generated by our environment and how many logs are just a waste of time, looking at them. They're just there. It's just logging information, and we were able to reduce. Deployment, I believe, took about two weeks, and going from, let's say, a 100 logs, we were able to reduce to about half of those logs in terms of what we're reviewing.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

Stability is perfect. We have had no issues whatsoever with the servers, or with the Web Console or anything else.

LogRhythm NextGen SIEM

Read 49 reviews of LogRhythm NextGen SIEM

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

The scalability is awesome. Initially, when we first purchased LogRhythm, we purchased only about 20 lite agents. Then we realized, as we were looking for additional log sources, we needed more. Pretty much within a day, we were able to purchase additional licenses and get them rolled out to our organization.

HOW IS CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Tech support is amazing. They always follow up with a document on how to do something and if you still need further assistance, they're willing to get on the phone with you, without any doubt.

WHICH SOLUTIONS DID WE USE PREVIOUSLY?

We were using a different vendor and we decided to go against it. We wanted to bring this in, in-house. We were using Dell SecureWorks, and we were just not satisfied with their ability to give us reporting and information on a timely manner.

HOW WAS THE INITIAL SETUP?

It was a little complex, I did not have training prior to, so it was more of a hands-on learning, which I appreciate. I prefer to do hands-on. It's easier for me to learn that way. It was complex but at the same time it was educational. It had benefits.

WHAT OTHER ADVICE DO I HAVE?

Being at this conference I learned a lot. For example, I haven't been using the Web Console to the extent that I should be using it, and I think going back I'll be using that a lot more. It's extremely important for a solution to be a unified, end-to-end platform. In terms of criteria when selecting a vendor, we look at it as a relationship between our organization and LogRhythm. We want them to work with us and we're willing to work with them to fit what's best for our environment. I gave it seven out of 10 because we've only used the product for about a year and a half and it's still a building process, and I think it will always be a building process. You're always tweaking things. I can't imagine the company being the best at one specific thing, and then if you're the best at it, then there's no room for improvement. But I know as an organization, we are extremely happy, with LogRhythm. I would definitely tell colleagues to at least PoC LogRhythm, and see for themselves what their getting in their environment and what other vendors might be missing.

Read 49 reviews of LogRhythm NextGen SIEM