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 Architect at a leisure / travel company

it_user756300

HOW HAS IT HELPED MY ORGANIZATION?

We used to use a third-party vendor. We migrated to an in-house security operation center, so it's been a big difference.

WHAT IS MOST VALUABLE?

We're doing almost 10,000 EPS right now and we have anywhere between 5000 and 6000 servers, and a couple thousand network devices more or less. Our goal is pretty much to gather all those logs. Keeping track of when new servers are deployed and new network equipment gets put out there and then have them report to LogRythm. That's mainly the biggest challenge so far. Mostly for us the most valuable feature is its aggregation of all the logs into a single platform, and then doing the real-time monitoring based on that. Also, the real-time monitoring piece of it, that's extremely valuable. Plus you can tweak a lot of their settings while other systems don't really let you.

WHAT NEEDS IMPROVEMENT?

Dashboards, reports. Right now I know there's a big issue with reporting. It's challenging, at least for us, to do some of the reporting within the system itself. Hopefully that's something that gets improved. Also, when you're reaching out to any other solution out there, any third party, most of them have integrations with Splunk; that's something that it's lacking on the LogRythm side. They're lagging behind when it comes to integration to main platforms. So hopefully, with the help of the entire community, we can build something a little bit more flexible when it comes to integrations.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

We had some issues. Unfortunately, it was not sized properly from the beginning. But now with the additional boxes on everything, so far it's pretty solid.

LogRhythm NextGen SIEM

Read 40 reviews of LogRhythm NextGen SIEM

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

They're pretty good. Sometimes I wish they would be a little bit quicker getting back to you, at least when you open a ticket, but apart from that they're pretty good. We usually do reach the right person within the SLAs they have.

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

We were using a third party, Dell SecureWorks. We wanted to go away from that and go into more of a centralized system in-house. We went through a bunch of factors and LogRhythm came out on the top.

HOW WAS THE INITIAL SETUP?

It was good. We have a lot of collectors, we ended up having almost 50 collectors in total, so it was a little bit challenging, but it's not bad.

WHICH OTHER SOLUTIONS DID I EVALUATE?

Curator Security Splunk ArcSight We took it as far as they were able to help us with very specific things we do as a company, and LogRhythm came out on top.

WHAT OTHER ADVICE DO I HAVE?

We're migrating to a dumb-terminal type of environment. That's the end goal that we have, because we have noticed that there's no way for us to secure everything. There's really no way. So having the users centralized into one location, it makes a big, big difference. So far it's working fine. Like I said, we had some little things here and there but we've revised the architecture and now it's good. For selecting a vendor we had a matrix. There were a bunch of points that we were trying to cover. How easy is it to use? For Roger's group, for example, to see how easy it was to adapt from the GUI base to the console. In terms of a unified, end-to-end platform, I'd say we're not married to specific vendors or companies, that's the nature of our business, at least how we run. But it's good to have everything in one solution. If I had a colleague at another company researching this and other SIEM security tools, I would give him my matrix.

Learn more: Read 40 reviews of LogRhythm NextGen SIEM