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

Manager Security Operations Center at a leisure / travel company

ManagerSc364

HOW HAS IT HELPED MY ORGANIZATION?

Our key challenges in security include standardizing our policies having the end user population be aware on the security side of things. And the solution, LogRhythm, is helping us today to enforce it. We see now what it is that we're trying to propagate into the environment, based on the policies that we're monitoring today. The goal is to 100% enforce our policies. It has improved things tremendously. Going from a third-party vendor to an in-house solution, such as the LogRhythm solution, has given us visibility into the entire organization, compared to the limitations, based on budget and whatnot, from a third-party vendor. Absolutely, we have a lot more visibility now. I can tell you that having the ability to monitor the semi-subsidiaries that are a part of our organization, is huge in that sense. We have 10,000 EPS, as it is. And we have between about 500 and 1500 incidents daily.

WHAT IS MOST VALUABLE?

One of the most valuable features is the investigation tab. It allows us to dig in deeper into the alerts that we receive today, based on the policies, that get triggered by our end-user population.

WHAT NEEDS IMPROVEMENT?

I think a must-have feature would be better reporting. Today, as you can imagine, the organization would like to see what is happening in our environment, and the reporting feature within LogRhythm, I would say, is very limited. The reports do not provide information such as, who are your top ten end users generating the most activity within the environment, or appliances, per se, so that's very limited.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

So far, from my end, I haven't experienced any challenges. We are able to integrate all of the solutions that we have out there: our antiviruses, our data-loss prevention tools, and even our web browsing filtering. At this point, I really don't have any challenges. Maybe the architectural team has different ones for integrations, but no issues on my end.

LogRhythm NextGen SIEM

Read 40 reviews of LogRhythm NextGen SIEM

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

I have not used technical support, as I do not troubleshoot the application itself. We are technically just administrators of it, monitoring.

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

Because the organization wanted to have an in-house solution, when we looked at what was out there, we thought that LogRhythm, based on the user interface that was somewhat easier to follow compared to the competition, was a must for our security analysts. And the additional features within the investigation side of it, to dig deeper into what's going on out there. Those were two big selling factors for us.

WHICH OTHER SOLUTIONS DID I EVALUATE?

Curator Splunk Dell SecureWorks We chose LogRhythm because, as I said before, the user interface was really a plus for us. It was easier to understand, compared to the competition. And the ability to dig in deeper in the investigation tab, those were the two major selling points.

WHAT OTHER ADVICE DO I HAVE?

The most important criterion, when selecting a vendor, is how easy it is to adapt to the solutions we have in house. Every organization, I understand, is different, but based on what we required, for the most part I'd say about 85% of our needs were met with LogRhythm, compared to all other competitors. It's very important for our solution to be a unified, end-to-end platform because the organization might adapt new technologies. Our security architect needs to have the ability to integrate them. If it's a challenge then, definitely, that's going to be a downside for us. If a colleague at another company was doing a SIEM solution comparison with this and similar solutions, I would say to give LogRhythm a shot and, if the possibilities are there, to implement a PoC to understand how the solution can help them.

Learn more: Read 40 reviews of LogRhythm NextGen SIEM