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 Manager at a manufacturing company with 1,001-5,000 employees

Kevin Merolla

HOW HAS IT HELPED MY ORGANIZATION?

The benefits are almost innumerable. You can't know anything unless you are capturing the data. Once you are capturing the data, you can then make intelligent decisions around what is and is not appropriate, and what is and is not dangerous. It improves the security posture, because you can then know when things are happening that are bad. Before the LogRhythm solution, if someone was trying to login to a server with a local admin account, I would have no way of knowing that. Nothing would log it, audit it, and it would never show up. Now, I get an AIE alarm every time that happens, because it is considered a pass the hash attack. If we know when these things are going on in our environments, we can identify rogue admins doing things that they should not be doing, and the questions can be asked, "Why are you using this process? What's failing you that you have to go around the normal procedure to do this?" Another big one we found was just the ridiculous amount of PSExec running around the environment by non-admins to touch other things, which we have tried to curb. Then, we were able to ingest some custom log sources that have helped us become more proactive in alarming. Some of the stuff that we are using does not do good alerting, or it does not do role-based alerting. So I do not need an IT admin in Georgia to know about a potential issue in China. He does not care. I need that alarm to go to China, and not to Georgia, but some of our solutions will only send their alarms to one source. So, you either send it to the entire IT organization, every time it happens, or you do not send them at all. It has helped us pair down the noise to our site level admins, and give them more actionable intelligence quicker. We are a global company. We have 37 locations. China is one big country in Asia. We are on Australia, North and South America, and in Europe, with about 5,000 full-time employees. For the technology stack, we are running a single LogRhythm LR 6403. 2500 NPS license which we are currently hitting the lid on every day, and running a combination of Trend Micro and Malwarebytes. For endpoint, doing Cisco, Firesight for IPS. We are a Cisco shop, a 100% on the network, and we are a VMware shop, 100% for the servers. Right now, my biggest challenge is distilling the technical data that I am getting out of the LogRhythm appliance, in my reports, and translating that to business value statements to the business units to justify that I need more NPS or I need a bump to NPS, or I need another VX, which is a lot of money to spend. I have to now, instead of making the fear argument of, "Oh my god, the world's on fire." Instead, it is more of, "Here is this device, here is how this solution partners with the business to enable them to make better decisions about risk." Also, they can feel safer in making somewhat more risky decisions, because they know that this solution is behind the scenes, watching, keeping an eye on things, and our team will tell them if something is going wrong.

LogRhythm NextGen SIEM

Read 40 reviews of LogRhythm NextGen SIEM

WHAT IS MOST VALUABLE?

The ability for me to go into the Web UI, and just learn what's going on in my environment. Being able to go in and show our company's management, "Look, this is what we can see. This is what we can now know about our environment." Then, using the past several months to baseline what's normal, it has been invaluable, and we have also been able to stop things that were bad, at the same time. We were able to actually show value, while we were still building out the solution.

WHAT NEEDS IMPROVEMENT?

My biggest challenge always come back to log sources. We are a manufacturing company, so we have a lot of old stuff, and it has been a challenge to get some of our old stuff to light up within LogRhythm in a way that makes sense. I have probably submitted half a dozen log parser requests, and I keep finding more stuff that we need to keep an eye on that doesn't have a definition in LogRhythm. I keep pressing through, and I know they are working hard on it, but that is our biggest challenge.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It has been incredibly stable. I had one minor hardware problem, where it did not reboot at all. It just sat there, but it was just a minor hardware thing, other than that, the software itself has been incredibly stable.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

It is near infinite. We are running a single appliance, but I can, even with my current license, break the Web UI off and put it on a VM if I need to, just to relieve some of the pressure. If I need to bring in another appliance, I can bring in another VX, and cluster those, or I can move AIE off onto another machine, it goes vertical and it goes east-west.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Customer Service:
I can't say enough about LogRhythm's tech teams, the staff, the SEs, and even my CRM. They have all been fantastic. Technical Support:
We are on a first name basis with most of the technical support. My company did not get me professional services, so I deployed LogRhythm by myself, with no knowledge. So I probably opened 50 tickets in the first three or four months. They are amazing. They have an incredible depth of knowledge, even the Level 1 person that answers the phone, and their Level 3 support has been invaluable.

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

LogRhythm is the first SIEM that my company has ever owned. They never owned one before, and it took a lot of convincing to get them to buy it in the first place.

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

Definitely do a PoC. Get an appliance in your system and your company. Get your PoC guys to sign their CTU. Then, truly think through the business case for this device. What is it that the business finds important, and how can this appliance/device enable the business to know more about the solution, and to protect that solution from anything. Because if you start with what we like in the tech industry and what we want to do, you are going to be talking about red team exercises and hacking attempts, and those are all good things to have, but they just do not translate on that initial ask for $100,000s. You really need to target the business, find out what is important to them, then focus that stuff in, and try to answer their questions with the PoC. Then, they will sign any check you hand them.

LogRhythm NextGen SIEM

Read 40 reviews of LogRhythm NextGen SIEM

WHICH OTHER SOLUTIONS DID I EVALUATE?

We were actually dead set on using Splunk. I came from a Splunk shop at my previous job, and I am a big fan, but I had never seen the Web UI before. So, it is a combination of a few things: The web UI, price pressure from the business, and dedicated hardware, which made LogRhythm the overriding choice for us.

WHAT OTHER ADVICE DO I HAVE?

I have seen the features that are coming in 7.3, and they look incredible. It has far exceeded what I thought it was going to do for me in my job role. With the Web UI, over like a Splunk solution, it has actually become a tool that is used outside of security. I do not have to have people who have Lucene SQL Query Syntax memorized in order to get a value out of the system. They can jump in, log in as themselves, point and click, build themselves a query, and everything's great, then they love it.