



# LogRhythm NextGen SIEM

## Review From A Customer



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

---

## Review by a Real User

Verified by IT Central Station



Manager of Information Security at a real estate/law firm with 51-200 employees

**Ashlish Baria**

### **WHAT IS OUR PRIMARY USE CASE?**

The biggest use case is visibility. Because we have a lot of flaws, if you don't have a tool that can bring it all in and give you that visibility, then all that log information is useless. Thus, LogRhythm helps us keep that visibility.

### **HOW HAS IT HELPED MY ORGANIZATION?**

It has definitely improved our security program's maturity, because we have visibility that we didn't have before. We came from another SIEM platform that we had used for over ten years and we completely outgrew that platform. LogRhythm has given us more visibility. It has created more actionable items for us on a day-to-day basis, which gives us more work. At the same time, it has given us more tools than we had before, so that is definitely nice.

### **WHAT IS MOST VALUABLE?**

I wish I could just name one feature! There are so many: The ability to drill down and pivot from an event is one of the biggest advantage the product has compared to other things that I have seen in the market. LogRhythm differentiates itself through its usability. Its simplicity. It can do more than just basic simplicity.

### **FOR HOW LONG HAVE I USED THE SOLUTION?**

Three to five years.

### **WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?**

We have gone through a few versions which has caused a lot of instability. We have logged a lot of hours with professional services. The version that we are currently on is a lot more stable than what we have experienced in the past. So, it is progressively getting better day-by-day. However, we have had some instability in the past.



[Read 40 reviews of LogRhythm NextGen SIEM](#)

#### **WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?**

There are a lot of things that are on our wishlist which I found out about on day one. As far as scalability is concerned, it is good.

#### **HOW IS CUSTOMER SERVICE AND TECHNICAL SUPPORT?**

I would rate the technical support as a nine out of ten. We have had some issues. Though overall, support has been great. The portal and their interaction with us along with their full support has been fantastic.

#### **HOW WAS THE INITIAL SETUP?**

The initial setup is complex, because it's a huge product. LogRhythm is a beast. It can do so much more than just the analytic software, so it is not your typical installation. It's more of a three to four month installation process because you are gradually bringing in logs and fine tuning them. It is not a difficult process, just a lengthy one.

#### **WHAT WAS OUR ROI?**

We have seen a measurable decrease in the mean time to detect and respond to threats. As it comes out new features and new releases, the window is becoming a lot narrower because you can pivot a lot more with the data. Therefore, the new features and enhancements are reducing that.

#### **WHAT OTHER ADVICE DO I HAVE?**

I just found out about the playbooks at the conference. I plan on using them as soon as I get back. We have about 2500 messages per second coming in.

Learn more: [Read 40 reviews of LogRhythm NextGen SIEM](#)