LogRhythm

Security Intelligence Platform

It feels as if these folks have been around forever. They started life as a SIEM with a heavy emphasis on log management. Today they are all that plus a solid suite of next-generation attributes. They have many of the attributes of next-gen SIEMs: artificial intelligence, sophisticated log correlation, sophisticated pattern recognition and behavioral analysis. Their strength is, as it always has been, log management. But "log management" has taken on an entirely new dimension with this product. As is absolutely necessary today, it has the intelligence to analyze, correlate and make sense of huge amounts of data.

It can take input from almost any device and any log type you can imagine – the list ran to 14 single-spaced pages – and it has an excellent UI that makes analysis if not intuitive at least very straightforward. To support that, LogRhythm has first-rate documentation with lots of detail and step-by-step lists. We do wish for some clarification on what the rear panel ports mean. On our unit they were labeled a bit ambiguously and a call to support provided the explanation quickly. The company pointed out that the product typically is deployed with the assistance of a professional services engineer. We decided to bite the bullet and go it alone. The results, after the first start-up hiccups, were quite satisfactory.

Everything starts with the IP address configuration. Instructions for that came with the product and once we figured out where to plug what, we were up in no time. Next comes configuration and that is where it can become a bit more difficult. The centerpiece for that set of tasks is the Deployment Manager. That has a menu that is about as straightforward as a menu can be and still be a GUI. Just about anyone who ever has set up a security device will feel comfortably at home with the Deployment Manager tabs.

There are data processors, data indexers, agents and log sources among others that all need to be configured and added. We recommend that you read the manual before you even apply power to the box if you want the kind of analytical power that the tool offers. It probably is worth noting that the first 720 pages of the manual are devoted to deployment and other administrative tasks while much of the rest of the 1,220 pages are a user guide. The user guide assumes a configured device in production and the power of the device – buried by deployment details in the first part of the manual – really becomes evident. We would like to see, at least, a mini-support portal open to the public where one could access technical details during the decision-making phase of buying the tool. This is a very pricey device, but it offers a lot as well. For a SIEM of this quality, we believe that its cost is reasonable.

– Peter Stephenson, technology editor

DETAILS

Vendor LogRhythm

Price $32,000, plus 20 percent for annual maintenance.

Contact logrhythm.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths The most complete pure-play SIEM we've seen with the added benefit of many next-gen features and superlative correlation and analytics.

Weaknesses Some minor hiccups in the documentation at the getting started point.

Verdict This is a heavy duty tool made for a demanding large environment. It is scalable and complete with the largest list of supported connectors we've yet seen. For all of that we make it our Recommended product.