LogRhythm

Back again this year is one of the most powerful SIEMs that we have seen, and it is more powerful than ever with the new version 6. To start, the LogRhythm appliance combines log management, SIEM, file integrity monitoring and host activity monitoring into a single integrated platform. From there, all these functions use the advanced intelligence engine to provide full correlation and pattern recognition to stay on top of security threats throughout the enterprise.

SC MAGAZINE BEST BUY

From beginning to end this appliance is easy to deploy and configure. The first thing that needs to be done is to get the appliance up and running. The tool is pretty much ready to go out of the box, but does need some initial configuration. At first boot the appliance will run through a short Windows setup wizard where networking and other settings can be configured. After the appliance is up and running, all management is done via a powerful management console application. Overall, we found the management console to be easy to navigate, as well as intuitive to use. We also liked that the interface can be highly customized to meet the needs of the user and is not a one-size-fits-all layout.

The management interface has a plethora of features and functions. Some of these include fully customizable dashboards – along with predefined dashboards that offer specific information at a glance, many graphs and charts that can be drilled down into all the way to the raw log data if needed, and quick navigation controls for easy movement throughout the interface. Aside from all of the management capability, this product also features many strong compliance functions, including a brand new SmartResponse system. Security administrators can use this to deploy instant and automated remediation of common alerts. The final strength of this product is a solid rule engine. While the appliance comes preloaded with many rules out of the box, creating custom rules for alerts is as easy as dragging and dropping the parts of the rule using the rule builder interface. Finally, in terms of performance and flexibility, the appliance has the ability to collect data and logs. The LogRhythm appliance is able to gather and analyze logs with or without the use of agents, depending on the type of log and needs of the environment.

The LogRhythm documentation set is included in the management console and can be easily accessed if needed. It features installation, configuration and administrator guides. We found all documentation to be well-organized and easy to follow, with many screenshots and step-by-step configurations.

LogRhythm provides both eight-hours-a-day/five-days-a-week and 24/7 support options for customers. Support must be purchased as part of an annual agreement and includes access to phone- and email-based technical help. Customers also can access a large support portal via the website, which includes a full knowledge base and FAQ section, along with other resources.

At a price of around $25,000, this LogRhythm solution is an excellent value for the money. The appliance offers a lot of functionality, along with many easy-to-use features and pre-built dashboards, making it a very powerful SIEM appliance.

– Peter Stephenson, technology editor

DETAILS

Vendor	LogRhythm
Price	$25,000
Contact	logrhythm.com
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Highly customizable SIEM with many pre-built policies and dashboards backed by a powerful correlation engine.

Weaknesses None that we found.

Verdict One terrific product and an equally terrific value. We make it our Best Buy.

LogRhythm®
COMPLY. SECURE. OPTIMIZE.

LogRhythm
4780 East Pearl Circle
Boulder, CO 80301
866-384-0713
www.logrhythm.com