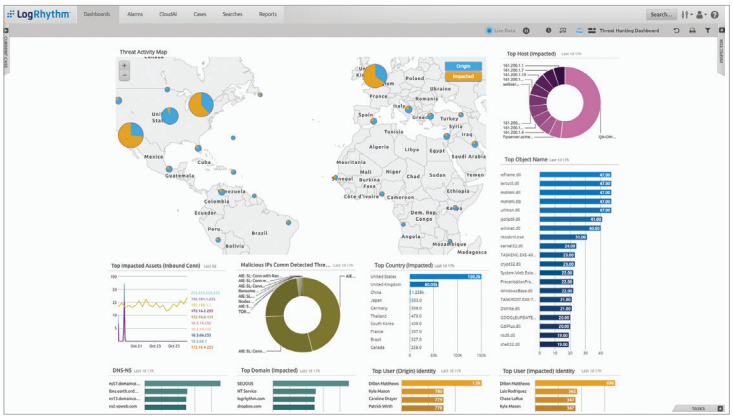

DETAILS

Vendor LogRhythm

Price Starts at $28,080 for the software. $35,400 for the appliance option.

Contact logrhythm.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★½
Ease of use	★★★★½

OVERALL RATING ★★★★¾

Strengths Very well polished and usable toolset. Very configurable and easy to use.

Weaknesses Setup wasn't as smooth as we'd like to see, but documentation was put together very well.

Verdict LogRhythm has always been one of the top names in this space, and the new version continues to showcase why it needs to be considered part of your SOC.

LogRhythm
The Security Intelligence Company

4780 Pearl East Circle
Boulder, CO 80301
1-866-384-0713
www.LogRhythm.com

LogRhythm
LogRhythm Platform

When security professionals talk about SIEMs, LogRhythm is a name that gets brought up as one of the tools to look at. The company has a long history as a leader in this space by providing a log correlation solution that utilizes security analytics, automation and artificial intelligence. LogRhythm prides itself on accurately detecting a wide range of early attack behaviors enabling your security analysts to take the quick action to prevent data breaches before they happen.

BEST BUY

LogRhythm offers a software-only solution as well as a physical appliance. For our testing, LogRhythm supplied the complete appliance. We slid it into the rack and it was quickly up and going. There was very little configuration needed to connect to the network and operating, however getting data into LogRhythm was a little more challenging. But the documentation and support communities got us up and running in no time.

Once up and running, the system dashboard is a thing of beauty. The dashboard looks clean and with deep black, gray and blue accents, information just pops out at you. The dashboard is very customizable; we felt right at home navigating through the alerts. The system was responsive and easy to work with. LogRhythm has the capacity to handle large amounts of encrypted log data for forensic analysis and packs the horsepower to search quickly across large data sets to identify what's needed. The Elasticsearch utilized for indexing data, allows LogRhythm to scale for large enterprises and assists with search reliability.

The Dashboards can be customized for any user with access, supporting a broad spectrum of needs ranging from security analysts to high-level executives. It manages to provide just the right amount of insight to enhance an individual's job function. Reports are detailed and customizable. Predefined reports in the reporting dropdown that cover a range of topics.

LogRhythm's platform isn't just your everyday SIEM, it includes many additional features that others in this space do not, making it one of the more complete packages for your enterprise. LogRhythm offers reporting on user behavioral analytics, however we were unable to provide enough input to get valid results to share. LogRhythm employs one of the industry's broadest set of threat detection methods, employing techniques well-suited to the detection and prioritization of a wide range of suspicious behavior.

A stand-out feature is the integrations with other players in the security space. LogRhythm has many vendor-specific APIs to work with existing security products as well as cloud-based APIs to capture events from a cloud footprint. It supports several threat feeds to keep your analysts up-to-date.

LogRhythm's basic 11x5 support includes access to its knowledgebase and quick response times. 24x7 support costs extra.

– Michael Diehl with Dan Cure; tested by Matt Hreben and Michael Diehl