LogRhythm v6.2

Combining SIEM, log management, file integrity monitoring and analytics with powerful forensic tools, LogRhythm v6.2 offers security professionals a powerful monitoring and auditing platform to keep them informed, and an excellent investigatory tool in case things go wrong.

The basic setup is, as it turns out, a little complicated. LogRhythm recommends, and we agree, that purchasers of the product should secure a few hours of deployment assistance. That said, the engineer with whom we worked had our evaluation system up and ready to accept log data in about 15 minutes. Larger deployments – with hundreds of log sources – would obviously take a bit more time, but for our small, all-in-one deployment, it wasn't that bad.

LogRhythm is comprised of a series of modules. The Console provides the user interface and offers a single pane of glass for viewing logs, events, alerts and reports, conducting investigations and managing workflows. Designed to support fast access to millions of records, the console enables users to quickly correlate, search and pivot through their data rapidly. The integrated case management system enables events to be easily assigned to users for later analysis. In addition to the robust installable console, new to v6.2 is an attractive web GUI. While it is obviously in its infancy, it nevertheless enables quick, at-a-glance views of a number of reports and alarms and allows limited investigation. Still, the bulk of an analyst's work needs to be done in the console. The Event Manager provides centralized event and incident management, analysis, reporting and configuration management across the entire deployment.

The Log Manager provides centralized log storage, log processing and archiving functions. The Artificial Intelligence Engine is the analytics platform and is the real meat of the tool. Taking log data from the Log Manager, it performs log correlation, pattern recognition and behavior analysis before sending results to the Event Manager. Finally, the System Monitor Agent does the actual log collection. Installed locally or on remote systems, it provides log collection services to Windows, Linux, AIX, HPUX and Solaris systems. All logs received are parsed and metadata is derived from them, which is then loaded into a database, greatly increasing performance while searching or performing analysis.

Product documentation was done very well. All product features and functions are clearly explained via a series of PDFs. Documentation is also available through LogRhythm's support portal, which contains online versions of those documents, as well as a user support forum.

There are a number of support options offered by LogRhythm. However, the two most common are standard and platinum. The standard tier provides phone, email and web support from 7 a.m. to 6 p.m. Mountain Time. It also includes software updates, a three-year hardware warranty, four-hour response to technical support requests within normal assistance hours, and next-day on-site hardware aid. The platinum tier increases coverage to 24/7, with four-hour technical support response and four-hour on-site hardware help.

LogRhythm starts at $27,500, and the standard support option is priced at 20 percent of the base cost of the product, annually.

DETAILS

Vendor LogRhythm

Price $27,500.

Contact logrhythm.com

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

Strengths Powerful correlation and forensic analysis tools with extensive prepackaged reports.

Weaknesses Complicated install.

Verdict Customers willing to invest in support services will be very pleased with the performance of this product.