LOG MANAGEMENT

LogRhythm

REVIEWED BY GARY MOSER

LogRhythm
www.logrhythm.com
Price: **Starts at $20,000**

LogRhythm is a cross-platform log management program that provides a multitude of functions to manage audit files and IT security management processes. It's well crafted to meet IT industry trends aimed at increased enterprise efficiency, security and governmental/industry compliance standards.

Configuration/Installation B+

While the configuration of data sources initially seemed a daunting task, the installation documentation guided the process in a step-by-step format that was easy to follow and manageable.

However, actually deploying log management in an enterprise is hardly plug-and-play, and prospective buyers with complex IT infrastructures may want to consider onsite installation and training.

LogRhythm is a cross-platform tool, with out-of-the box configuration settings to bring in data for many sources, including Linux syslog, Cisco NetFlow, Snort, Blue Coat Web proxy, and all ODBC-compliant databases.

LogRhythm also supports application logs, such as Apache, IIS, DNS and DHCP.

Dashboard B+

We were impressed with the configurable dashboard, with plenty of options to monitor network activity in a real-time, visual interface. The display is set up to show near real-time activity in a graphic format in operations, security and audit panels.

The dashboard can be configured to display pertinent critical data based on any aggregated data variables. Further log management functions are started from the main console, with clearly defined dropdown menus.

Testing methodology: We tested a LogRhythm appliance connected to a lab environment with multiple syslog sources.

Monitoring/Analysis A

LogRhythm's aggregator can be configured to collect data at variable intervals to minimize bandwidth concerns. Queries can then be run on the aggregated data to drill down to find specific information. Setup wizards facilitate step-by-step development of queries and reports.

LogRhythm is remarkably configurable, which enables rapid development of queries to correlate, filter and find data quickly. Its ability to filter and correlate data provides a fantastic forensic analysis tool, which can be finely tuned to examine any details users need to look at, cross-referencing multiple sources.

For example, we were able to quickly see anomalous activity on our network by examining trends in login failures and after-hours activity, easily focusing our search to identify specific users.

The ability to save complex queries for future use will prove especially efficient in fast-paced IT data centers, particularly for incident response situations, where time is a critical factor. The graphic presentation of the data queries was impressive, one of the best we've seen, painting a clear picture of large and complex data sets.

The custom alarm rule setting function provides in-depth functionality in categories of classification, events, login and service rules. Varying thresholds and time requirements can also be set, like number of events before an alarm is triggered, and how often to report. Alarms can be delivered via email, SNMP or in the console.

Reporting A

Reporting is outstanding for its range of templates, output formats and exceptional graphic displays.

The reporting functions provide templates to meet most commonly used industry compliance standards for data collection and auditing purposes, such as PCI, SOX, GLBA and HIPAA. The output formats included Crystal Reports, which enables a host of additional options. The graphics formats visually depicting the data correlation were particularly impressive at summarizing trend data in easy-to-digest format.

Verdict

LogRhythm is an outstanding and affordable log management tool, with many uses to fit any enterprise IT management tasks, and particularly useful in forensic analysis.