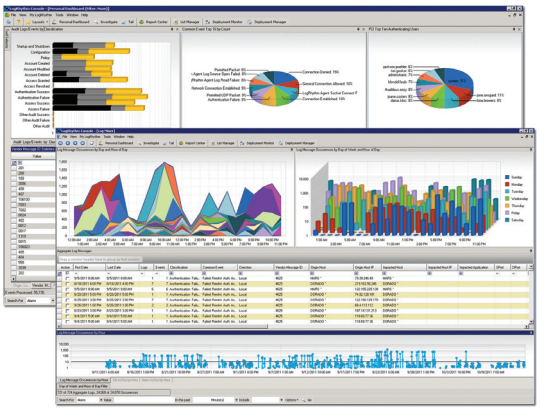
LogRhythm



The LogRhythm appliance goes way beyond traditional security event monitoring and management. This appliance features log and event management functions as with any SIEM, but beyond that it includes advanced correlation and pattern recognition driven by its onboard Advanced Intelligence Engine, with host activity and file integrity monitoring, and drill-down capabilities to get to the raw log data for analysis and forensics.

Overall, we found this product to be easy to set up and manage. The initial setup and deployment of the appliance has changed just slightly, but is still as easy and straightforward as in past appliances that we have seen. To get started with LogRhythm, we had to power on the appliance and allow it to go through a brief initial power-on procedure to set up Windows Server 2008. After the initial start-up process, we were able to set the IP and network settings and we were pretty much done with the initial deployment. All further management is done via a well-designed management interface. We found this to be intuitive to navigate and it includes a multitude of analysis and monitoring tools, including many charts that could be drilled down into for deep event analysis.

This appliance came loaded with monitoring and reporting capabilities. On top of being able to drill down quickly and easily from any event to raw log data, this tool features a lot of automation and compliance reporting functions. The automation aspect includes the LogRhythm SmartResponse, which delivers immediate action on real-world issues, such as when specific cyber threats are detected or compliance-driven policies are violated. This allows for administrators and security managers to focus on the investigation of an incident, rather than trying to plug the hole in a time of crisis. This appliance also came preloaded with a large selection of compliance and predefined reporting templates, making report generation simple and easy right out of the box.

Documentation is included in the management console of the appliance. From the console, administrators can easily access installation and administrator guides for help with advanced configuration or use of product features. We found all documentation to be well-organized and easy to follow owing to many screen shots and the step-by-step instructions.

LogRhythm offers customers 11/5 standard support or 24/7 premium support as part of an annual maintenance contract. Along with phone- and email-based technical assistance, customers also have access to software updates, including all major and minor releases and hardware warranty options. Customers also get access to a portal via the website, which includes a knowledge base, user forums, documentation, support tips, downloads and other resources.

At a price of $25,000, we find this product to be an excellent value for the money. LogRhythm is a powerful yet reasonably priced appliance that includes many excellent features and functions onboard right out of the box. Too, along with powerful functionality, this appliance is easy to use and manage, which makes it an all-around good value and investment for any organization looking to deploy SIEM.

– *Peter Stephenson, technology editor,* SC Magazine

DETAILS

Vendor LogRhythm

Price $25,000

Contact logrhythm.com

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

Strengths Easy to deploy and manage with many reporting and alerting functions built in.

Weaknesses None that we found.

Verdict A solid product with very good value and performance.