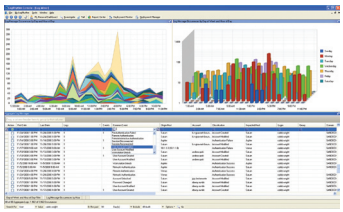
Valuable data resides in a number of locations throughout the digital continuum, but an interdisciplinary approach is required to find and interpret it, says Keith Gilbert.

Gone are the days in which conducting a forensic analysis meant pulling the plug and imaging the hard drive. We now know that valuable investigative data resides in a large variety of locations throughout the digital continuum. A successful investigation may rely on the ability to find and interpret a variety of data from these multiple locations.

As a result, the number of tools being designed and marketed with forensic capabilities is growing. The traditional media analysis tools definitely still have a firm place in the investigative process, but they now often include the ability to carry out all the traditional tasks over the network. Adding to those traditional tasks, some of these tools also include the ability to complete a live analysis of a target system over the network as well. Once you've moved past the more traditional products, they become more specialized, and in some cases, less obvious.

LR-1000-XM



Vendor	LogRhythm
Price	starts at $20,000
Contact	www.logrhythm.com

The LogRhythm LR-1000-XM system is a power log aggregation tool available in hardware and software platforms, although the appliance is the most common deployment and the one we tested. It can collect information off of a number of open and closed platforms, including Unix system logs, Windows event logs and Cisco logs. Its search capabilities make it a powerful network forensic tool.

SC MAGAZINE BEST BUY

Collection also can be done using customized agents on the monitored systems giving the product an impressive range of systems it can monitor. It also has built-in features to assist with regulatory compliance. LogRhythm is capable of displaying an array of reports from a general aggregated overview down to the individual events collected from logs. Many of the features are readily available and easy to use in a very clear and easy to analyze format.

The LogRhythm console starts up in a customizable interface with three main zones of focus: operational, security and audit events. The Tail tool provides the ability to scan logs in near real time for suspicious changes, and the product features a digital fingerprinting system for authenticity verification. It can also analyze long-term trends with the one year of log data it stores by default. With almost any tool in the suite that is accessible from the console, you can quickly drill down to individual events.

The appliance features dual quad-core Xeon CPUs and a RAID array [redundant array of independent disks] stocked with drives to deliver top performance even when handling large data sets. Despite warnings contained with the appliance, setup was relatively painless.

Locating the documentation was a bit of a challenge as it is solely available from LogRhythm's support site and covers the gamut of their products. The documentation itself is well-written and clear as to what procedures need to occur for proper use and customization.

The support system is top notch with setup assistance options and personable staff. LogRhythm can be easily reached on the phone, by email or using their help forum system. Starting at $20,000, depending on which LR model selected, this product is a very good value, especially considering its powerful network forensic capabilities.

SC MAGAZINE RATING

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

Strengths Easy to use with strong reporting capabilities.
Weaknesses None that we found.
Verdict Powerful product with plenty of easy-to-use features, this one is our Best Buy.

LogRhythm®
COMPLY. SECURE. OPTIMIZE.

LogRhythm
3195 Sterling Circle, Suite 100
Boulder, CO 80301
303-413-8745 (phone)
303-413-8791 (fax)
www.logrhythm.com

SC MAGAZINE Reprints

Powerful product with plenty of easy-to-use features, this one is our Best Buy.

Keith Gilbert

Copyright Haymarket Media, Inc.