Reference Code: TA001560IMT
Publication Date: January 2009
Author: Chandranshu Singh, and Roy Illsley

Butler Group
a Datamonitor Company

TECHNOLOGY AUDIT

LogRhythm 4.1

LogRhythm Inc.

BUTLER GROUP VIEW

ABSTRACT

LogRhythm 4.1 is an appliance-based solution that combines log and event management into a single product and facilitates collection, storage, analysis, correlation, trending alerting, and reporting of log files and application audit trails. The solution employs rule-based data reduction at multiple levels to segregate log entries of significance from the full volume of logs collected and archived. Butler Group likes the reporting features that include pre-built report packages for many industry and government regulations including GCSx, SOX, PCIDSS, FISMA, GLBA, and HIPAA, among others. The solution also provides tools such as Log Mart for visualisation and trending, and LogRhythm Investigator for rapid drill-down search and analysis. LogRhythm also allows users to view processed log data in real time as it is being handled by the system. LogRhythm should be considered by organisations that generate large amounts of system and application log files, those that need to comply with regulations which mandate the use of automated log management solutions and those that are considering deployment of a security information and event management solution (SIEM).

KEY FINDINGS

- ✓ Rule-based data reduction at multiple levels.
- ✓ Easy to use and powerful GUI.
- ✗ Market in Europe only started in earnest in 2008 with the opening of its UK office.
- ⓘ Reporting features support SOX, PCIDSS, FISMA, GLBA, and HIPAA among others.
- ✓ Ability to prioritise events based on time and date.
- ✓ Role-based access and personalised dashboards.
- ✗ Automated remediation not supported at present, requires manual intervention.
- ⓘ Leverages agent-based and agentless log collection techniques.

Key: ✓ Product Strength ✗ Product Weakness ⓘ Point of Information

LOOK AHEAD

LogRhythm has recognised a gap in the market and is building the capabilities needed to perform baselining of network, system, and application access behaviour to automatically detect and respond to anomalies.

FUNCTIONALITY

IT functions across organisations generate large amounts of operational log data daily. While some organisations have formulated a log management strategy, quite a few are still not clear about what they want to do with their log files. Organisations typically adopt a reactionary approach and look at log files only when an availability, security, performance, or compliance incident gets reported. This approach is no longer tenable as security and regulatory compliance requirements warrant a closer and more proactive monitoring of log data. However, the lack of the appropriate technology and of a structured log management strategy have inhibited such initiatives as IT personnel are faced with the problems of an ever growing volume of data to be managed; tedious and time consuming search operations often do not yield meaningful results. On the technology front, vendors such as LogRhythm have brought to market log and event management products that can handle log collection, storage, monitoring, diagnostic and forensic analysis, log mining, and reporting. Such solutions can help organisations meet security and compliance requirements, as well as help derive operational intelligence from data which, although inherently valuable, typically never gets looked at.

Product Analysis

LogRhythm 4.1 is an appliance-based solution that collects log data from various log sources such as commercial or custom IT systems, devices, and applications; and classifies, stores, and enriches log data for forensic analysis, log data mining, and enterprise/compliance reporting. The appliance is also capable of real-time log monitoring and near real-time event reporting. Events are anomalies in the log data which may potentially represent a security, performance, compliance, or availability issue. The solution generates alarms and notifications for critical events, and also provides out-of-the-box reporting features that address various government and industry regulations.

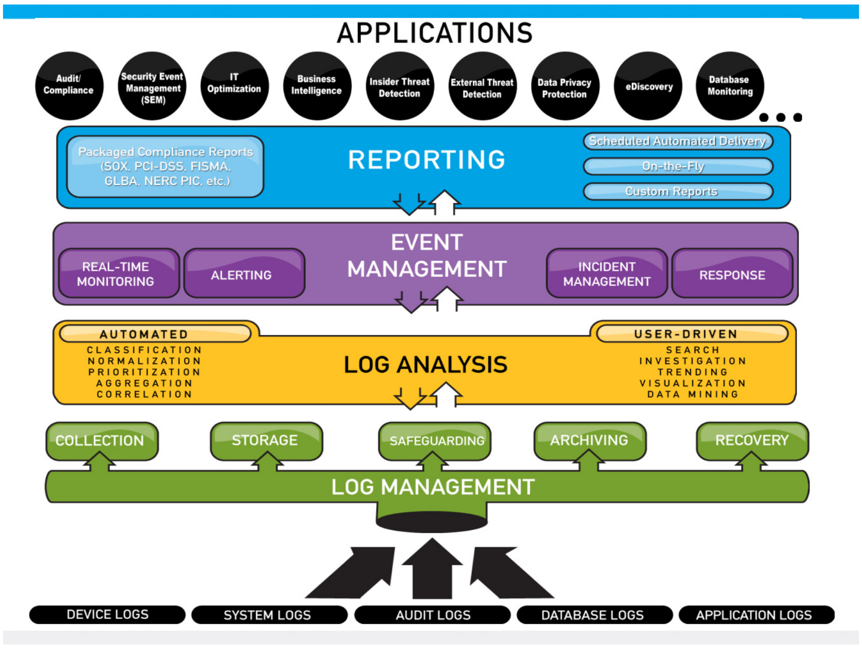
The appliance helps streamline tasks of log collection, storage, analysis, and reporting by automating collection, storage, reporting, and facilitating analysis. Automating even a few aspects of the log and event management processes helps IT achieve operational efficiency, and meet compliance and eDiscovery requirements. Butler Group believes that log and event management can not be viewed in isolation from incident and problem management; LogRhythm 4.1 provides comprehensive incident management features and workflow to help IT operations/support personnel get a holistic view of incidents and resolve support issues quickly. The solution provides a native ticketing system as well as part of the incident management workflow.

The LogRhythm appliance combines the log management and event management disciplines. In Butler Group’s experience most available products focus on certain aspects of one of those areas, whereas LogRhythm provides a holistic solution. The solution provides comprehensive search and log-data mining functionality, in addition to trend analysis and visualisation capabilities for historic as well as near real-time data.

The appliance currently provides a rule-based analysis engine. Although the solution provides good workflow capability, it does not provide a complete closed-loop solution in which automated remediation occurs; some amount of manual intervention is required. Overall in Butler Group's opinion LogRhythm 4.1 is a well-rounded offering, and well suited for organisations that generate large amounts of log data on a daily basis.

Butler Group believes that technology alone can not solve the problem of how to extract value from system/application data held in log files. Therefore, if organisations do not have a clear log and event management strategy the technology will help, but it will not provide a complete solution. Organisations also need to estimate the volume of log data that is generated daily, define log retention periods across the enterprise, and define the operations/security/compliance-related reports that they require for all audiences.

Figure 1: Schematic Architecture



Source: LogRhythm Inc. DATAMONITOR

Product Operation

LogRhythm is currently in its 4.1 version, and is classified as an appliance-based solution. The product comprises the Log Manager, monitoring agents, the Event Manager, and a GUI console.

The Log Manager module is responsible for log collection and analysis. The Log Manager processes log messages against the product's rules engine to determine whether they need to be forwarded to the Event Manager as events. System monitoring agents collect logs and forward them to the Log Manager. The solution supports both agent-based and agentless log collection.

The Event Manager receives log messages that are deemed to be important after being processed and evaluated against the rules set by the Log Manager. The Event manager is responsible for processing alarm rules, and issuing notifications and alerts. Only critical events generate alarms; as part of normal operations the Event Manager is responsible for generating reports. The GUI console allows users to interact with the product and also lends itself to administrative tasks.

LogRhythm collects log data from any log source including devices, systems, and applications. The collected logs are normalised to a standard format, and the solution applies a universal time stamp to each log entry for facilitating audit, search, and analysis; thereby handling the difference in time zones common where the log sources are distributed. Log files are classified based upon the nature of the log source into security, operations, or audit categories. Log data is then parsed for useful information such as IP addresses, port numbers, and user IDs.

For analysis purposes, the solution quantifies the criticality of the log entry using a priority number on a scale of one to 100. Event prioritisation takes place based upon the event type, likelihood of occurrence, threat rating of the host that caused the event, and risk rating of the server on which the event occurred. LogRhythm allows for manual risk-based prioritisation as well, through a wizard. Log data from various sources are correlated to provide a holistic view of IT systems in near real time.

Log entries having immediate operational relevance such as security events, audit failures, warnings, and errors are forwarded to the Event Manager based upon a rule set. LogRhythm allows users to modify and create their own rules. The solution incorporates real-time activity monitoring, and can be used to bolster IT support functions such as incident and problem management, as it also contains a comprehensive event management workflow. Automated analysis of log data by the solution involves the aforementioned steps of normalisation, classification, risk-based prioritisation, and log correlation.

The product further enables user-driven analysis and manual search of enriched raw log data. LogRhythm provides tools such as Log Mart and LogRhythm Investigator for facilitating manual search and analysis. Log Mart provides visualisation and trending features. The drill-down capability of the solution enables users to get to the lowest level of granularity. The LogRhythm Investigator enables user-defined search and viewing of user-specified log data; the Investigator also allows for search criteria to be saved for later reuse and reporting.

LogRhythm 4.1 provides real-time activity monitoring and role-based alerting features. Access to the solution and reports is role based; the solution also provides customisable personalised dashboards based upon user roles. LogRhythm dashboards depict statistics about the three event categories identified by the solution, Namely Security, Operations, and Audit; in turn each dashboard has various event categories represented by multi-coloured horizontal bar graphs representing the statistics for the past 24 hours, one hour, and ten minutes respectively. Dashboard entries can also be drilled into to reveal detailed statistics.

LogRhythm provides multiple report formats out of the box, including compliance and audit reports specific to various government and industry regulations such as PCIDSS, SOX, GLBA, FISMA, and HIPAA. The solution allows users to generate reports for any investigation on the fly, and vice versa; i.e., enabling users to drill down from the report to the root cause. Users can schedule creation and delivery of reports, and also create custom reports.

Product Emphasis

LogRhythm 4.1 has been designed to handle high log volumes, and support trending, analysis, and mining of log data. LogRhythm enables near real-time correlation and reporting of log data, as well as historic trending, visualisation, user-driven search, and reporting features.

The log management and security event/information management have traditionally been disparate market segments. LogRhythm 4.1 combines the two interrelated areas. Other vendors in this area are now adopting the combined approach, but their solutions are new to the market and not as well established as LogRhythm 4.1. Log management is a new market where the larger enterprise software vendors are absent; however, Butler Group believes that log management technology will find its way into IT Services/Systems/Security Management suites in the next few years.

DEPLOYMENT

Resource requirements for the deployment project vary depending upon the scope of implementation. Solution implementation can involve a single LogRhythm engineer, IT security experts for the client-side aspects, UNIX or Windows administrators, and Firewall administrators. According to LogRhythm the average time taken for implementation is two days.

However, the solution can be deployed using a modular approach as LogRhythm is an appliance-based solution and does not charge separately for optional components; the company provides three hardware variants and three software variants of its appliances. Hardware variants are designed to accommodate different requirement levels and various deployment scopes. Software variants on the other hand define the appliance functionality. Software variants include Log Manager devices (LM), Event Manager devices (EM), and devices housing both the modules in the same appliance (XM). Organisations can take the modular approach to deployment by installing one XM device, and increasing the number of devices as their log and event management requirements grow.

Average maintenance requirements of the solution are approximately three hours per month. Maintenance package includes product upgrades, patches, addition of new log sources, and new automated report schedules. The company provides a Virtual Administrator Service (VAS) which helps LogRhythm engineers remotely maintain the solution. The company provides training courses aimed at all levels of users, but advanced user training courses include advanced end-user training, LogRhythm administrator training, and advanced rule-development training. Training courses are held at the company premises; LogRhythm also offers training courses at customer sites if so requested. LogRhythm offers technical support globally. Standard support is eight hours by five days a week (8x5) over e-mail and phone; however, customers can also visit the online customer service portal which provides technical help. LogRhythm can provide 24x7 support if required.

The solution is available on Windows 2003 Enterprise Edition (EE) R2 platform. The company offers system monitor agents that run on Windows, Linux, Solaris, AIX and AS/400(System i) platforms for log collection and forwarding. The solution is delivered as an appliance in most cases, but the company provides software-only options as well. The product does not depend on any third-party software that is not bundled with the solution. Internally the solution leverages Windows Server 2003 Enterprise Edition R2, in addition to MS SQL Server Enterprise Edition, and the Microsoft .NET runtime.

The solution is also capable of legacy integration; it can import log data from legacy systems provided that the legacy log files are in a supported format such as ASCII text files.

The solution can be integrated into existing business processes at the client organisation, and can help to streamline such processes further. LogRhythm does not foresee any changes to business procedures as a result of the deployment project. The company, however, highlights the lack of management sponsorship as a potential risk that may cause any deployment project to fail.

PRODUCT STRATEGY

LogRhythm's appliance is a horizontal solution which can prove useful for all organisations with high daily log volumes. In testament to this horizontal nature the company's clients come from many industry sectors including retail, financial services, government, utilities, manufacturing, eCommerce, aerospace, transportation, hospitality, and education. LogRhythm states that its strategy is targetting organisations with compliance requirements, as compliance has become a major driver of adoption of such automated log management suites. In terms of company size, LogRhythm primarily targets medium to large enterprises with more than 500 employees while still offering a valuable and easily deployable solution for the Small to Medium-sized Enterprise SME market.

LogRhythm claims that the solution's Return on Investment (ROI) is usually realised in less than 12 months after deployment, and ROI accrues from cost savings related to the audit, compliance, security, and operations related areas.

LogRhythm sells directly to customers and also through a network of value added resellers, referral partners, and system integrators in the USA. In EMEA, the company leverages a network of distributors, value added resellers, referral partners, and system integrators, whereas in APAC LogRhythm sells only through local reseller partners. LogRhythm's business partners include McAfee, CSC, HP/EDS, and PowerTech. The company has many technical partners including Avaya, Barracuda, BlueCoat, Checkpoint, Cisco, Dell, Enterasys, Fortinet, HP, IBM, Juniper, McAfee, Microsoft, NetApp, RedHat, Sonicwall, and Sun; and strategic technology relationships with Dell, McAfee, Microsoft, and PowerTech.

LogRhythm devices are sold with a perpetual licence, the prices of these appliances range from UK£14,900 to UK£44,600. Average project value for a LogRhythm deployment is around UK£50,000, including LogRhythm implementation services that range from UK£1,475 to UK£2,500; standard annual maintenance and support is provided at 20% of the price. LogRhythm partners also offer a range of implementation, training and support services to complement what is available from LogRhythm. LogRhythm releases one major version and one or two minor updates every 12-18 months. The company plans to add more advanced correlation to the solution and a Heuristics-based anomaly detection engine is on the product roadmap.

Log Management is a relatively new market segment and has not yet attracted the large IT infrastructure management vendors. The recent growth in organisations' security and compliance requirements, and clauses in some regulations are the major drivers that have mandated adoption of automated log management suites. Butler Group believes that log and event management is an area where IT systems/security/risk/services management market segments overlap. Although log management functionality is currently absent from IT management suites which address the aforementioned markets, Butler Group expects it to be incorporated in such products in the next few years.

LogRhythm's market strategy is fairly simple, straightforward, and in line with the current market scenario. Most organisations treat log management as primarily a compliance-driven initiative. This view has created the need for add-on solutions which are quick to deploy, meet the requirements well, and do not disrupt the existing order in the IT organisation. The company provides an appliance-based log and event management solution which can meet the requirements, and easily fit into the IT environments of Small to Medium-sized Enterprises (SMEs) as well as larger enterprises. Butler Group believes that LogRhythm has gauged the market sentiment well, and will continue to grow in the foreseeable future. It will also be interesting to see when this nascent market attracts the large enterprise software vendors.

COMPANY PROFILE

LogRhythm was founded in 2003 to take advantage of the unmet need for an integrated log and event management solution. The company is headquartered in Boulder, Colorado, USA; and runs its EMEA operations from offices in Maidenhead, U.K. LogRhythm is a privately held company that has attracted venture capital from High Country Venture, Access Venture Partners, and Croghan Investments. The company has nearly 50 employees on its payroll; most of the employees are based in the USA office in Boulder with the rest operating out of the U.K. offices. Nearly 40% of the company's employees are engaged in research and development activities, 35% in sales and marketing functions, 15% in support and service roles, and the remaining 10% in administration. LogRhythm expects its head count to increase by 25-50% over the next year.

The company's customers include Royal London Mutual Insurance, Asent Media, Retail Decisions, Cardiff County Council, PetCo, General Dynamics, Amtrak, U.S. Department of the Interior, Real Networks, Singapore Government, Kroger Corporation, Red Cats, and Regis Corp. LogRhythm has around 200 customers globally. The company does not disclose financial information.

SUMMARY

LogRhythm has combined the log and event management disciplines to bring to market a solution that is currently in its fourth version. The solution manages the log data value cycle from log collection to extraction of operational intelligence, and log/event-data based reporting. The solution also includes pre-built compliance/audit reports for various industry/government regulations and incorporates rules-based data reduction at multiple levels, which is used to identify events of significance and generate alerts/notifications and reports against them. Most of the log management vendors have not combined log and event management into a single solution, the prime barrier to which is the inability to reduce log data to manageable proportions. Some vendors have launched products based on this approach recently but the market readiness of these new solutions needs to be carefully assessed.

Butler Group's opinion is that LogRythm 4.1 is a well-rounded offering that provides IT with tools to derive value from huge amounts of daily log data, which due to its sheer volume has often been ignored. Butler Group believes LogRhythm to be suitable for organisations of all sizes that need to meet regulatory compliance requirements, or just want to extract more value from the wealth of information contained within its log file estate. While LogRhythm has been traditionally focused on the North America market, its expansion into EMEA and APAC over the past two years has led to the establishment of EMEA headquarters in the UK at the beginning of 2008.

Table 1: Contact Details

LogRhythm Inc.

3195 Sterling Circle
Boulder,
CO 80301
USA

Tel: +1 (303) 413 8745

Fax: +1 (303) 413 8791

www.logrhythm.com

LogRhythm Inc.

Siena Court
The Broadway
Maidenhead
Berkshire, SL6 1NJ
U.K.

Tel: +44 (0) 1628 509 070

Fax: +44 (0) 1628 509 100

www.logrhythm.com

Source:LogRhythm Inc.

DATAMONITOR

Headquarters

Shirethorn House,
37/43 Prospect Street,
Kingston upon Hull,
HU2 8PX, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Butler Direct Pty Ltd.

Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

Butler Group

245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684

For more information on Butler Group's Subscription Services please contact one of the local offices above.

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.