Log & Event Management: LogRhythm

The value of log & event management solutions

There are three major benefits to be derived from log and event management solutions (sometimes referred to as SIEM, security information and event management). In the first case, these solutions provide real-time identification and alerting against external and internal security threats. Secondly, they provide compliance monitoring and reporting and, thirdly, they offer forensic environments for root cause analysis and fraud detection. There are also secondary benefits in that this sort of software can be used to support network performance monitoring and analysis and, with appropriate facilities, can be used for data retention purposes in the telecommunications sector. A possible extension environment is to support the collection and filtering of data retrieved from various types of industrial and other sensors. For good reason, log and event management solutions are often referred to as "business intelligence for IT".

Requirements for log and event management

There are a large number of log and event management solutions within the market—more than 20—and they by no means all offer comparable capabilities. The sorts of features to look for include:

Integration

There are literally hundreds and hundreds of different sources of data that may need to be monitored, depending on your environment, ranging from device support through mainframes, databases, applications and security software to things like vulnerability data. Moreover, it is not simply a question of what sources you support but also how you support them. In most cases an agentless approach is to be preferred because there is no performance impact on the source system. On the other hand, if you want to filter events at source or encrypt them then you will need an agent-based approach. However, integration is not limited to source systems but to other enterprise applications such as network monitoring, help desk software and others.

Real-time analysis

This requirement involves recognising a threat, identifying what sort of a threat it is and then taking appropriate action. Since hackers may disable logging it will be useful if the software can monitor configuration, vulnerability and similar data. Identifying a threat is typically provided through correlation engines that recognise patterns of activity and exceptions. Taking action will not just mean raising alerts but may also involve initiating appropriate remedial processes such as turning off port 80.

Forensics and compliance monitoring

As far as compliance monitoring is concerned it will be useful if the vendor provides out of the box dashboards for such things as Sarbanes-Oxley, PCI DSS and HIPAA compliance, as well as internal corporate compliance requirements such as ITIL. For forensics generally, most suppliers offer a large number of reports and analytics capabilities. It may be useful if SQL is supported so that you can use a third party business intelligence or data mining tool. It may also be helpful to support PMML (the industry standard for porting data mining models) in order to support both forensics and real-time pattern analysis. As log data is typically opaque you will normally require data to be normalised (put into a standard format) and presented in a more user friendly fashion.

Infrastructure

Both appliance and software-only solutions are available as well as outsourced options. In the case of appliances some vendors offer distributed environments for large implementations. Compression is de rigueur because of the large quantities of data that need to be stored, often for prolonged periods—for which reason, lifecycle management capabilities will be an advantage—and, obviously, the greater the compression the better. For this reason many vendors have developed their own data storage technologies, either based on file systems or column-based technology: as a general rule, standard row-based relational databases will not be efficient enough in this regard. A further requirement is the ability to tamper-proof the data for evidentiary purposes. Typically this will mean support for write-once read-many (WORM) storage.

Performance and scalability

In some instances it may be necessary to process billions of events per day. Moreover, the more events you are processing the more you will need to store. So there will be a premium on performance, throughput and storage capacity (and compression). In multi-national organisations with distributed IT systems, log and event management may also need to be distributed. Also, as data volumes increase it will be important to be able to incrementally add more hardware resources to support increased processing requirements. Support for distributed environments may help here as will support for virtualisation.

Optional features for log and event management

EU Data Retention Directive

Some log and event management suppliers also support, for example, the EU Data Retention Directive for recording and storing call detail records and IP detail records. This requires not only high throughput capability but also the provision of a search interface, preferably with self-service capabilities so that law enforcement agencies can make their own (subject to appropriate authorisation) enquires against your stored records. Support for lawful intercepts may also be required.

Other security applications

There is a trend towards making log and event management more inclusive. For example, including database activity monitoring (DAM) and/or risk management as a part of, or complementary to, the same system. We expect this trend to accelerate and we anticipate a trend towards broader platform provision.

LogRhythm 5.0

Background

LogRhythm does not use the term 'log' just to refer to IT-based logs (database logs, syslogs, network logs, web logs and so forth) but to refer to anything that generates a record of activity. Thus, for example, the product supports physical security devices such as badge readers, call detail records, RFID readers, GPS, ANPR (automated number plate recognition) and SCADA sensors, which all generate log data in a similar way. The product does not, however, provide native interfaces to leading application package (ERP, CRM and so forth) and database products (though ODBC and JDBC are supported). There is also a Data Loss Defender option, which protects customer systems by independently auditing and logging data transfers to USB thumb/hard-drives, memory cards and CD/DVDs.

In terms of events LogRhythm defines these as being log data that is of interest to the business, regardless of whether these are security events, performance related events or whatever. In practice, the company focuses particularly on automated compliance, security event management and IT operations management. In the case of compliance this would include PCI DSS, Sarbanes-Oxley, HIPAA, GLBA, CoCo and other such regulations.

LogRhythm is available either as an appliance (there are several options), a combination of appliances (to support either failover and/or distributed environments) or as software only. The company also has partners that provide its software via a SaaS model. Raw log data is stored in its original, unaltered form in archives that use binary files that are stamped with a digital fingerprint (sha-1 hash) to ensure tamper proofing. At the same these archives are created, a user-friendly form of the data is created in stored in a Microsoft SQL Server database for query and reporting purposes. This has the advantage that you can use SQL and SQL-based tools (and you can import data mining models) to access the data in addition to the out-of-the-box facilities provided by LogRhythm.

Log and event management optional features

EU Data Retention Directive	Relevant features are provided though this is not a focus area
Other applications	Not generally available though the product's file integrity monitoring is a notable feature not available in most other products.

Focus

LogRhythm targets companies of all sizes and it tends to focus on use cases rather than vertical sectors. While some of these overlap, for example ePHI (electronic protected health information) in the healthcare sector, others are more generic, including privileged user monitoring, zero-day investigations, operating cost management and change control auditing and governance, as well as compliance monitoring and reporting.

Services

Outside the United States, LogRhythm has a European headquarters based in the UK and an Asia-Pacific office in Hong Kong. The company has been growing aggressively outside the US recently, trebling its staff numbers over the last year. The company uses both direct and channel (in Latin America as well as the other regions mentioned) sales models and offers the usual professional services and support

Company Details

LogRhythm Inc.
3195 Sterling Circle, Suite 100
Boulder
CO 80301, USA

Phone: +1 303 413 8745
Web site: www.logrhythm.com
Email: info@logrhythm.com

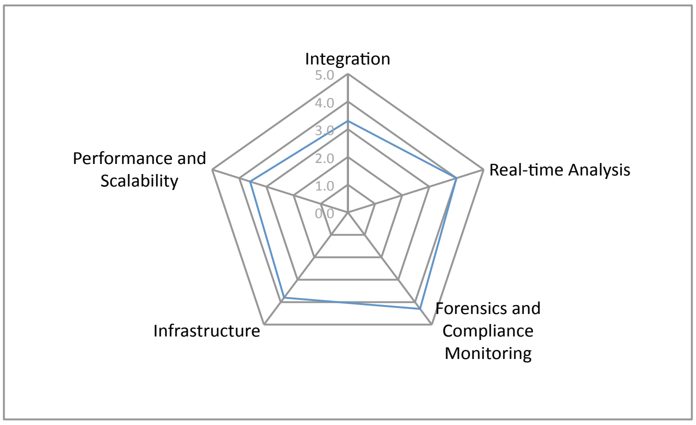

Figure 1: Log & Event Management Requirements (scale 0 to 5)

Customers

LogRhythm has some 350 customers of which roughly two-thirds are in North America, a quarter in Europe and the rest in Asia-Pacific. Customers include Time Warner, Bank of America, Cardiff City Council, the US Department of Defense, Camelot and Fortis Bank.

Summary

LogRhythm scores highly across the board and it is particularly strong for its front-end capabilities, with its combined coverage for real-time analysis, forensics and compliance monitoring being the best we have seen. One concern, common to many vendors, is the use of what is essentially a transactional database (in this case SQL Server). This is fine for ingesting, storing and reporting on the data but may not be ideal when ad hoc and complex analytics are required (for example, for fraud investigation). While LogRhythm has implemented specialised in-memory cache techniques in order to improve database read performance, a more specialised analytic warehouse would be preferable for this purpose. Fortunately, Microsoft will be releasing SQL Server Parallel Edition later in 2010, which should provide such capabilities. Leaving this aside, LogRhythm clearly represents one of the most technically advanced products on the market.

Philip Howard—*Research Director, Data Management*