



# GETTING MORE FOR LESS AS LOG MANAGEMENT AND SIEM CONVERGE

AN IANS INTERACTIVE PHONE CONFERENCE

FEBRUARY 11, 2009

CHRIS PETERSON, CTO, FOUNDER, LOGRHYTHM  
NICK SELBY, IANS FACULTY

---

SUMMARY OF FINDINGS

Underwritten By:

The LogRhythm logo features a stylized icon of three horizontal bars of varying lengths above the word 'LogRhythm' in a bold, sans-serif font. A small 'TM' trademark symbol is located at the end of the word.

LogRhythm™

**Chris Peterson, LogRhythm**  
CTO, Founder

Chris brings a unique and diverse background in information security, audit, product development, and product management to his role as Chief Technology Officer/Founder of LogRhythm. Chris has spoken at numerous conferences, been quoted in numerous publications, and was a faculty member with IANS. Chris has a degree in Accounting/Information Systems from Colorado State University.

**Nick Selby**  
IANS Faculty

Nick is a member of the IANS faculty. He has worked as an IT security consultant to small and mid-sized firms subject to regulatory compliance and strict confidentiality. He has also covered emerging technologies such as open source, wireless, and software piracy when based in Europe and Eastern Europe. He was editor-at-large for Amsterdam-based Tornado Insider/Tornado Investor, and reported for the International Herald Tribune.

Selected statements by Chris Peterson of LogRhythm

## Context

In this Interactive Phone Conference, IANS faculty member Nick Selby moderated a conversation with LogRhythm CTO/Founder Chris Peterson about the evolution toward one product addressing both log and event management needs. Chris also responded to numerous phone and email questions from participants.

## Briefing Summary

- The market is demanding a single solution for both log and event management.
- A single solution has lower investment and maintenance costs as well as faster incident response. Also, reporting is faster and less expensive. A single solution supports forensics and e-discovery.
- LogRhythm is unique in that it was created to provide a single log and event management solution. Its architecture has separate collection and processing layers.
- LogRhythm has several differentiating capabilities. These include the collection infrastructure, the correlation capabilities, the online and archiving abilities, the sharing and visualization capabilities, and the ability to access logs in custom applications.
- The future of log and event management will focus on analysis. More robust analytical capabilities will derive even greater value from the logs and data that are collected, bringing greater insights to problems such as insider threats.

## Overview

Log management and event management have evolved as separate and distinct solutions. But customers would prefer and are demanding a single log and event management solution. A single solution would cost less to implement and maintain, would provide faster incident response, and would result in better reporting (among other things).

LogRhythm is the single solution that the marketplace is looking for. It is a best-of-breed log management solution and a very good event management solution. LogRhythm is unique in that from its inception it was designed to be both a log and an event management solution. The result: LogRhythm's architecture has separate collection and processing layers, which provides multiple benefits. LogRhythm is highly scalable, has a great user interface, and has many other unique and differentiating capabilities.

## Key Points

- **Instead of separate log and event management solutions, the market is demanding one solution that does both.**

The problem SIEM was invented to solve was data overload, primarily from IDSs. The idea was take IDSs, firewall logs, and more pieces of data and boil this information down into a highly correlated single event. "Boiling down" has great value, but in this data reduction process SIEMs threw away a lot of valuable forensic material; the information was simply discarded. It was lost and not available to a SIEM user.

*"Customers are smart and are asking, 'Why should I deploy two technologies?'"*

*"The ability to corroborate high-level events against lower-level log data enables much more effective 'truth in corroboration' in terms of understanding 'What just happened here?'"*

*"Wouldn't it be nice if a single solution could identify what I care about in real time when an event occurs, and could also provide the ability to immediately access other log data to help corroborate or understand other information around that attack?"*

In contrast to SIEM, log management was developed to collect and store all of the underlying forensic information, and to have this data available. Keeping all of the log data in its original, unfiltered, unmodified state—which SIEM solutions don't do—also has tremendous value.

What evolved were two different types of solutions: log management solutions that collect and store logs in their original form, and event management solutions (SIEMs) that boil information down to view a single event. Yet increasingly users are asking, "Why should I deploy two technologies and two infrastructures that collect the same data?" Customers are saying that they would prefer one product that collects and keeps all of their logs, provides a correlated view of events, and allows access to the raw data when it is needed.

By having a single solution, when an IDS alarm goes off, it is possible to then pull all of the raw logs from a web server around that attack and corroborate what the IDS is saying.

- **A single solution that combines log and event management has many advantages.**

Among the many advantages of a single log and event management solution are:

- **Lower investment.** Instead of investing to implement and maintain two separate solutions, just one is needed, lowering the upfront investment and ongoing maintenance expenses.
- **Faster incident response time.** By having one solution with normalized data, incident response time related to operations, compliance, and security issues should be significantly reduced.
- **Lower system downtime.** The ability to respond to intrusions faster and more effectively will decrease system downtime, which will lower costs.
- **Decreased reporting costs.** The automated capabilities of a single solution support reporting associated with compliance and do so in a low-cost way.
- **Support for forensic investigations.** Access to raw log data supports after-the-fact forensic investigations. It provides the ability to get to log data that is needed whenever it is needed.
- **Easier e-discovery.** As with forensics, the ability to access vast amounts of log data in one system makes the entire e-discovery process easier.

- **LogRhythm is unique in that it was created as a single solution.**

When LogRhythm was founded, the basic premise was to integrate log management and SIEM in a single solution. In some ways, LogRhythm had an advantage in that it was late to market. The company had the

*"We architected a solution where we separated the collection layer and the processing layer."*

*"If you are a log management vendor, you need to keep the log in its original state." That is something the SIEM vendors have not done."*

*"Our solution is the best of both worlds. You have the original or raw log, which is critical to keep, plus you have all of the metadata for correlation, analysis, and more effective reporting."*

opportunity to observe and learn from the existing players in the market—all of which were either pure SIEM or log management solutions.

LogRhythm was unique in embracing a "single solution" philosophy. This philosophy led the company to architect a solution which separated the collection layer and the processing layer.

- **Collection layer.** Any type of log data can be collected in its native, raw form. This raw data is not modified, but it is normalized and time stamped. It is then stored within a log manager which is a general purpose data repository and managed effectively for compliance purposes.
- **Processing layer.** On top of the collection layer is a separate processing layer. Processing is done through a rules engine that has the ability to look at any type of log data. This has broader capabilities than a typical SIEM. Specifically, this means looking into a log message text and identifying metadata.
- **LogRhythm has several differentiating characteristics.**

Unlike most of the other players in the space, which started as SIEM solutions and over time have tried to add log management capabilities, LogRhythm was focused on having both capabilities from its outset. Because of this, LogRhythm's technology is more effective in terms of delivering an integrated platform.

While this was the company's vision, most of the company's early R&D investments were focused on log management. As a result, LogRhythm is a true "best-of-breed" solution for log management, with very good event management capabilities.

Among LogRhythm's differentiating capabilities are:

- **The collection infrastructure.** How LogRhythm collects data is different from other solutions, and much more flexible. LogRhythm has extensive agentless collection capabilities, collecting logs from Cisco, Netflow, Windows event logs, and more. These agentless capabilities allow for the remote collection of logs such as database logs, Cisco IDS logs, and Checkpoint logs.

In addition, LogRhythm also has agents, which make sense in some cases. For example, if a retailer has a POS system in its remote stores, it can be valuable to put an agent on the POS. The agent can reach out and pull logs from the POS and send data to a datacenter over SSL communications in compressed form. That is very valuable in providing an extension to the data collection infrastructure that is managed and maintained by the same vendor.

Having the ability to use an agent is a distinct advantage for LogRhythm versus vendors that are 100% agentless. In the POS example above, a customer that used an agentless solution would have to find some open source software or shareware to get the POS

*"I consider LogRhythm to be best in class."*

*"Having both agentless and agents when they're required is really a big differentiator for us."*

*"It's pretty easy to get to any data regardless of the age."*

*"We win a lot of business because of our user interface. It seems like once people see our UI, we're immediately short-listed."*

data to them. So, they would still be using agents but the agents would not be managed by the log management solution.

- **Correlation.** A LogRhythm user can create an alarm rule on any of the fields that the solution parses out, and can correlate on any of the roughly 35 metadata fields. Also, LogRhythm can take multiple alerts on the same event and correlate these into a single event.
- **Online data.** Data is kept online as long as a user wants; 90 days is common. When data is online it is immediately accessible through analysis, tools, and reports. When the data expires it gets purged, which keeps the database at a reasonable size.
- **Archiving.** When data is no longer accessible online, it is still archived. LogRhythm has a unique log data management archiving technology. Every log is collected and is written into a purpose-built archiving system. This is a file-based archiving solution where a file contains a log source and log messages for that day, and all files are compressed and cryptographically sealed. This makes it possible to verify that a file hasn't been tampered with.

All log data is kept in the archives for as long as the user wants it there. The archived data can be written to an appliance or a SAN, or to wherever the user wants to write it.

LogRhythm has developed an archive search tool called Second Look. This tool finds any logs that meet specific criteria and pulls these logs back online.

- **Collecting and accessing logs in custom applications.** This is another big advantage of the separation in the collection and processing layers. For a custom application, as long as data can be received through a collection interface, the data can come into LogRhythm. This means that if an application logs to a flat file, if it will send out via SysLog, if it writes to a database, or if it writes to Windows Event Log, then the data can be collected in LogRhythm.

When logs from custom applications are brought in, LogRhythm has no idea what the logs mean. But LogRhythm has the ability to bring these logs into a tool called Investigator. This provides the ability to look at the logs and copy them into a rule builder where a user can write their own rules.

- **User interface and visualization.** LogRhythm uses a great deal of visualization. These capabilities complement what is seen as a great user interface.
- **Data sharing.** LogRhythm has created a capability for users who want to take the data that is collected and build their own visualization, or share data with other users. This capability is called Log Distribution Services. LogRhythm wants to be the infrastructure for data management, but recognizes there are other uses for data that require sharing.

*"We want to be the infrastructure in terms of log data management."*

*"Solutions like LogRhythm that bring in all of this data are the key to identifying some of the things that we just cannot detect today."*

- **The future for log and event management will focus on analysis.**

When asked about his vision for the future of log and event management, Chris Peterson said, "I think analysis is still the key in terms of where a lot of innovation will occur. Analysis will continue to be more important."

The value of collecting huge amounts of data doesn't reside in the act of collection; it is in the analysis of what has been collected. Effective analysis and algorithms will enable looking for anomalous things, such as insider threat.

### Other Important Points

- **Scalability.** LogRhythm's "sweet spot" tends to be enterprises with 500 to 5,000 servers. Not many customers have fewer than 500 servers. Many started with 500 and then added more servers over time. An important consideration when evaluating log and event management solutions is how well and how easily they scale. Users should look for a "building block" architecture that they can continue to build on. LogRhythm is highly scalable; scaling simply entails adding log managers.
- **Time required.** Typically it takes 1-2 weeks to implement LogRhythm. The ongoing maintenance time varies based on exactly what a user wants to do. Roughly 1 to 2 days per month of maintenance wouldn't be an unreasonable amount of time.
- **Usage auditing.** One participant mentioned that many log and event management products fail to have an ability to demonstrate (for compliance purposes) that people are actually going in and looking at the logs. LogRhythm implemented a feature called Usage Auditing to address this specific need. Everything that a user does is logged—every report that is run, every search, every alarm that is drilled down on. That information is available in Usage Auditing reports.
- **A process, not a tool.** Log and event management is not a product; it is an operational process. A tool will only do so much. Tools make the processes possible and more efficient, but they are just tools. A complete solution involves tools, processes, and people.

### **About LogRhythm**

LogRhythm provides a comprehensive, fully integrated, enterprise-class log management, log analysis, and event management solution that empowers organizations to comply with regulations, secure their networks, and optimize IT operations.

By automating the collection, organization, analysis, archival, and recovery of all log data, LogRhythm enables enterprises to easily comply with log data retention regulations while simultaneously gaining valuable, timely, and actionable insights into security, availability, performance, and audit issues within their infrastructure. LogRhythm solutions are noted for their completeness, useful analytics, ease of use, and rapid time to value.

Learn more at [www.logrhythm.com](http://www.logrhythm.com)

### **About IANS**

IANS is the premier membership organization for practicing information security professionals. IANS' mission is to provide key technical and business insights to help members solve their most pressing professional challenges. IANS achieves this mission through a broad offering of services provided to its members—insightful events, thought-provoking publications, best-practice research, and unique networking opportunities.

Learn more at [www.ianetsec.com](http://www.ianetsec.com)