NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com September 02, 2011

Sister organizations pool their resources to share SIEM and logging

Only LogRhythm provided the group with two options.

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

You've heard the expression, "Two can live as cheaply as one." Sometimes that old adage applies to IT solutions as well. Five of the nine member clubs of the Canadian Automobile Association (CAA) pooled their funds to buy and share one instance of a high-end logging and SIEM system. It was either that or each club spending separately to buy their own solutions that offered fewer features and capabilities.

I mention this because it's unusual that a vendor would allow -- much less encourage -- sister companies to share a single solution. Most vendors would prefer to sell a separate product to each company and earn a bigger paycheck. The lesson here is, you never know what kind of deal a vendor is willing to give you until you ask.

Paul Schubert is director of technology services for CAA Saskatchewan, one of the five clubs involved in the deal. Schubert says his organization, along with CAA Manitoba, CAA Atlantic, CAA Niagara and CAA North & East Ontario, all needed to deploy logging for PCI compliance. "We all needed the same functionality, but the cost of each club purchasing its own product just didn't make sense," Schubert says.

Schubert said the group contacted several log management vendors with their plan to go in together on a purchase. Only LogRhythm provided the group with two options: Each club could separately install its own log management system with a small feature set (what every other vendor proposed); or the five clubs could act as a single entity and implement one larger, more feature rich system.

With each club contributing one-fifth of the purchase price, all five clubs would gain the use of a much more robust system at the same cost of each club buying its own basic tool.

The LogRhythm multi-tier architecture, which is designed to support multiple branch offices and remote locations, is what enabled the CAA clubs to share the solution. Schubert's club, CAA Saskatchewan, hosts the LogRhythm servers in its data center. Schubert created an isolated segment of his network to host the LogRhythm environment and VPN tunnels to the four other club locations.

The remote clubs all have an agent that collects the local logs and feeds them to the central servers in Saskatchewan where the data is analyzed. If the data warrants a security or operational alert, it is sent via email to the appropriate club where action can be taken as needed.

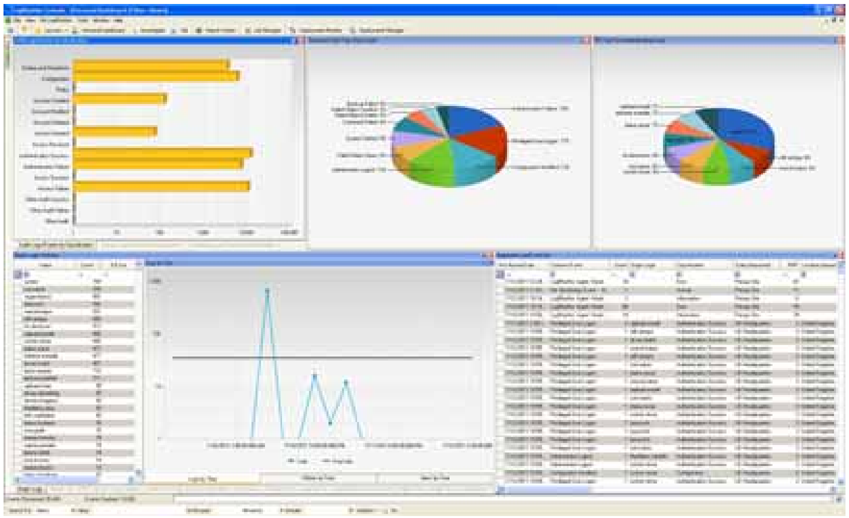
Schubert says the clubs are logging everything with the exception of one isolated application. "We are logging the complete environment, from end to end -- firewalls, virtual machine hosts, servers, IPSs. Everything, both physical and virtual."

The commingling of the clubs' data is not an issue for PCI compliance, largely because the individual clubs are part of the same parent organization and they have

Copyright 2011 by Network World, Inc., 118 Turnpike Road, Southborough, MA 01772.
This article originally appeared in the Network World IT Best Practices newsletter, September 02, 2011.
Reprinted with permission from Network World.

contractual agreements among themselves to address privacy and other data issues. "We reviewed our implementation with our PCI QSA (Qualified Security Assessor), and the QSA believes we are in compliance with the regulation," Schubert says. At some future point, the clubs may decide to restrict access to only their own data, which LogRhythm can also accommodate if needed.

In addition to meeting the logging requirement for PCI compliance, the five CAA clubs enjoy the benefit of being able to look at central logs for security and operational issues. For example, Schubert says instead of having to correlate 60 server logs manually (if that even is possible), users now go to one service that aggregates and correlates all the information and allows them to generate reports as needed. The clubs also appreciate the audit trails that LogRhythm generates.



Implementation time and effort was another important selection criterion for the CAA clubs. "With LogRhythm, we got the complete package without the need for customization," Schubert says. "Other products would let us do what LogRhythm does, but we would have had to spend too much time and too many resources in setting up the data capture, getting the logs into a central system, and developing the reports we need. We were also concerned about unsupported devices."

In contrast, Schubert says the LogRhythm implementation was easy. He says the five clubs together spent a total of about 40 man-hours in deployment and getting the system to do everything they need it to do.

Now that all the clubs are up and running, the next big step will be to use the LogRhythm correlation and alerting capabilities to streamline troubleshooting and reduce the overall problems in their respective environments. The clubs expect to be able to fix a lot of little problems faster and to detect other hidden problems they don't even know about yet.

For these five automobile clubs spread across Canada, a little bit of collaboration on IT operations is paying off big. Without LogRhythm's multi-tier architecture and the vendor's willingness to view five individual clubs as one entity, each club might still be struggling to implement its own isolated log management system.

LogRhythm®
COMPLY. SECURE. OPTIMIZE.

3195 Sterling Circle
Suite 100
Boulder, CO 80301
303-413-8745
www.logrhythm.com