CASE STUDY

Phoenix Suns Draft LogRhythm to Gain Deep Visibility into IT and Secure Matters

LogRhythm

LogRhythm delivers "the right stuff"

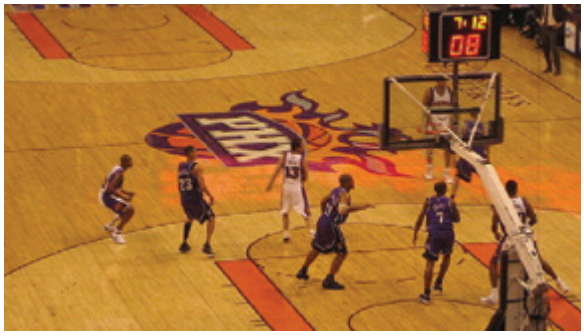
Customer
Phoenix Suns Organization
Phoenix, AZ

Challenges
A small IT team struggling to manage security and operations on the network of a growing infrastructure

Solution
A LogRhythm appliance gathers and distills information all day while only giving IT staff the information they need to analyze security and operational threats and events

Results
Benefits from deployment include:
- Ability to set security levels or important flags about certain issues
- Opportunity to address issues before a server crashes or an attacker compromises IT assets or data
- Small IT group benefited from extra training and support before and after deployment

Future Plans
The Phoenix Suns organization believes LogRhythm is a perfect fit for them now and has the ability to grow with them into the future



The Phoenix Suns IT organization, like the team's professional basketball players, runs lean and mean. Typical of many SMEs, a small datacenter staff of four manages 40 servers and 350 users. Vice President of IT Bill Bolt and another employee who doubles as administrative assistant and help desk manager comprise half the IT team. Bolt's team not only manages IT for the Sun's organization, they also manage IT operations for the US Airways Center, a major multi-use arena, providing support for the WNBA's Phoenix Mercury team and non-basketball events, including music concerts, ice skating shows, theater, comedy, art festivals, and family and community events.

The Challenge
As the Suns' IT infrastructure expanded, the small IT team struggled under the weight of managing security and operations for each server, application, and device on the network. They didn't have the staff to effectively monitor server and application logs for security, programming, and mechanical issues. According to Bolt, "It would take another full-time employee each day just to review the status of stuff, and I was not going to be able to increase our staff."

Bolt added that managing IT is a 24/7 job for companies of his size. "We're employees from 8 to 5 per se, but the reality is we're called on weekends, nights, or whenever. And especially with our sport being basketball, we have games at those times," he said. "I don't want to find out before a 7 o'clock evening game on a Saturday, when one of my employees comes in at 4:30pm, that we've had mechanical problems that prevent us from using some of the technology that would be needed to run that game."

LogRhythm – A First Round Draft Pick
Given the challenges, Bolt kept his ear to the ground for a solution. When he learned about LogRhythm, he realized the automated log and event management system would be like adding extra headcount to his team. LogRhythm's solution would enable his staff to be alerted to security, device, application, and network issues that required their immediate attention. This eagle's eye visibility would enable proactive and pre-emptive IT management. If a server was running out of space, Bolt's team would be alerted by LogRhythm in time to prevent an outage and downtime.

None of LogRhythm's competitors had the functionality Bolt and his team needed,

nor did they have the same ease-of-use or capacity to scale with the Sun's IT environment. It became clear that LogRhythm had the right stuff. Bolt moved quickly to recruit LogRhythm.

He convinced the Suns' CFO and upper management that LogRhythm was "a tool that would act as another person assigned to the department [without] the overhead cost of salary and benefits. In addition, LogRhythm allowed us to be more proactive when it came to our servers and management of IT."

Slam Dunk - Suns Gain Deep Visibility into IT and Security

LogRhythm gathers all the logs from the network – from the backend servers, firewalls, web servers, email servers, and other network devices and applications. The system then normalizes and analyzes the data gathered, monitoring the information for error message codes, rule set violations, and security and operational events and trends. If LogRhythm finds something abnormal, it is set to alert at least two members of Bolt's staff via SMS, email, and phone. Because of LogRhythm, he and his staff are now able to correct problems remotely rather than rushing to the office at all times of the day or night.

> "We're at the beginning levels of its ability. As long as there is a file it can look into. LogRhythm has the ability to pull back any sort of information for you...it doesn't take a vacation either."
>
> **Bill Bolt**
> VP of IT
> Phoenix Suns Organization

From a security perspective, LogRhythm provides invaluable benefits. It delivers early warnings to Bolt and his team on incidents that in the past they would have discovered long after they had occurred. "Unless I had a moment to look at the log file, I might not notice [the attack] for two or three days. Now I'm going to be notified right off the bat when my firewall records that somebody attempted to hack into it," Bolt says. "It gives us another pair of eyes."

LogRhythm provides Bolt and his department unprecedented visibility and real-time knowledge of what is happening in the server room. This allows his team to be proactive in a way that wasn't possible before. "We can set different security levels or important flags about certain issues [so that] we find out about it right away and are able to react to it to prevent outages in our operations," Bolt says. "We're monitoring our payroll system, our accounting databases and sales databases, [among other infrastructure.] All these things we're keeping up on and are aware of the critical issues as soon as they happen."

This visibility has enabled Bolt to add a whole new defensive scheme to his game plan. LogRhythm is gathering and distilling volumes of data every second of every day, and only giving his IT team the information they actually need to analyze security and operational threats and events. This allows the Suns to address issues before a server crashes or an attacker compromises IT assets or data.

Driving Factor - Ease of Installation and Operation

Although cost was an important factor in the Suns' purchase of LogRhythm, its ease of operation was at least equally important. "My employees are very good at what they do, but several of them are younger employees," Bolt explains. "Therefore, I was looking for something that wouldn't require [them] to go offsite an extra two to three weeks just to learn to run the product."

The pain of log and event management was so great and the upside potential of using LogRhythm was so considerable, that the Phoenix Suns did not test the system before dropping it into their network. According to Bolt, "We felt the risk we were taking was minimal because if it didn't perform right, it wasn't going to stop us dead in the water. It just meant we were still going to have to manually look at the logs."

According to Bolt, LogRhythm's installation took only a couple of days and without onsite assistance. "[LogRhythm] actually installed it remotely with us from their offices in Colorado. The device was sent to us, we put it online and got it up and running, and then they went through the first level of training for us over the phone," Bolt explained.

From Day One, LogRhythm performed as promised and delivered crucial security and event information, which was a slam dunk for Bolt's department. "We were suddenly getting results because it came preconfigured with a lot of standard stuff. For example, if somebody were to make a change in our Active Directory to a different security level, that routine is already built in, and we would be notified right away," Bolt said. As the Sun's newest player, LogRhythm gives the Suns a 50,000 foot view of IT and lets them easily drill down where necessary, saving considerable time and cost.

Delivering Results Day In and Day Out

About two months after LogRhythm was installed, one of the Sun's IT staff took advantage of a week-long class at LogRhythm's headquarters in Denver. This training enabled the Suns to learn about and take advantage of some advanced features and capabilities in the LogRhythm product in order to further optimize it for their environment.

In addition to training, LogRhythm is committed to providing world-class technical support. The Suns have noted that LogRhythm's expert staff is easy to work with and has been extremely accessible in helping to address error messages or rule snafus. "They are very responsive to our needs," says Bolt.

Not only is LogRhythm exactly what his IT staff needs today, but Bolt believes that the company will grow with the Suns over time. "We're at the beginning levels of its ability. As long as there is a log file it can look into, LogRhythm has the ability to pull back any sort of information for you." Bolt feels that his first round draft pick has turned out to be a franchise player for the IT department. Bolt added, only half joking, "It doesn't take a vacation, either."

> "LogRhythm is a tool that would act as another person assigned to the department {without} the overhead cost of salary and benefits. In addition, LogRhythm allowed us to be more proactive when it came to our servers and management of IT."
>
> **Bill Bolt**
> VP of IT
> Phoenix Suns Organization