EPC Uses LogRhythm's Insight and Actions to Improve IT Operations

EPC Inc. has been in business since the dawn of the personal computer era. Founded in 1984 to provide sales and services of PCs, today EPC is one of the premier IT asset recovery solution providers in the United States. The company owns numerous processing facilities in the U.S. and Canada, and it partners with companies providing IT asset disposition (ITAD) services in Europe, Asia, and Central and South America.

In addition to asset recovery, the company specializes in qualified and responsible end-of-life IT asset handling. Banking and healthcare are among the industries that EPC serves—the types of clients whose computer hard drives might contain sensitive and regulated data. EPC secures, processes, and thoroughly wipes client devices before repurposing or de-manufacturing according to local and ISO 14001 environmental standards.

The Business Challenge

Troubleshooting Operational Issues with Limited Information

With a lean group that oversees IT operations for nine dedicated production facilities, corporate offices, 40+ workers in the field, and numerous international partners, keeping everything running smoothly was a daily challenge.

Difficult-to-troubleshoot operational issues were constantly coming up. The team had insufficient information about the events, which hindered their ability to determine the root cause of the problems. The operations team could resolve the issues, but they had little insight as to why the failures occurred so often and how to prevent them from happening again.

For example, EPC's remote access system (based on Microsoft Terminal Server) is critical to business operations. It's heavily used by traveling employees, as well as partner companies from around the world who must access EPC's inventory system and tools. These servers would go down frequently, grinding work to a halt for the remote users. The operations team lacked the insight to know when and why the servers would fail.

For EPC, the server room was one area that was especially problematic. As more and more equipment was installed in this room, it became more challenging to effectively dissipate the heat the computers generate and maintain proper environmental temperatures.

To add to the challenge, the climate control system included two aging air conditioning units known to be particularly cantankerous. If the data center was not properly cooled, computers could fail or would require shutdown to allow the room to cool. This was unacceptable, as critical applications were unable to run due to the stoppage.

epc
Secure IT Asset Recovery
resell · recycle · relax

Organization
EPC Inc.

Industry
Computer sales, service and disposition

Locations
Dozens of processing facilities and offices around the world

Key Impacts

- Proactive monitoring of environmental conditions
- Improved operations and decreased downtime of facilities
- More reliable access for remote users via web services
- Correlation of operational activities and employee presence
- Documented compliance for PCI DSS, HIPAA and SOC 2
- Enhanced operational visibility overall

> *"I'm a big fan of both the product and the LogRhythm people. The support we get is awesome. This product and the people make my team's job much easier."*
> – Michael Sweeney,
> IT manager, EPC Inc.

The Solution

Operational Innovation for Improved Reliability and Efficiency

EPC deployed LogRhythm in 2012 to meet security and compliance needs. But after seeing LogRhythm in action, Michael Sweeney, IT manager, dug in to see how he could use the platform to improve operational processes.

"Plain and simple, we needed a better way to troubleshoot IT issues," says Sweeney. "Prior to using LogRhythm for correlating our system activities related to operations, we probably had 10 different tools for reading logs. It was painful to sift through all the logs to get an understanding of what was going on with our systems."

Now the IT group feeds every possible source of activity logs from all around the world into the centralized LogRhythm security intelligence and analytics platform. LogRhythm gives the IT team all the data it needs in one place to troubleshoot operational issues. Even more important, the team has been able to set up alerts that indicate an emerging situation before it turns into a real issue.

The most critical example of an early warning alert comes from the server room and the troublesome A/C units. Sweeney pushes the syslog output from the system that monitors the temperature in the data center into LogRhythm. If the room temperature starts to increase, an alert goes off, triggering an email to the on-call team. Someone can quickly respond to the situation before the rising room temperature can cause an outage. With automated alerts from LogRhythm, EPC now has confidence that servers will not fail due to unauthorized temperature fluctuations.

Beyond the temperature issues in the server room, the IT operations team also uses the data they've collected to analyze when they should be scheduling the maintenance, service and planned shutdowns of servers and other equipment. By optimizing the maintenance schedule, the team is able to not only decrease downtime, but also save time and money.

The insights from LogRhythm has also enabled the team to address their other operational challenges. Sweeney says the data backups fail from time to time, and LogRhythm provides the necessary information to figure out exactly why a failure has occurred. The same is true for user lockouts. "People call the help desk all the time to report they can't log in to a system," says Sweeney. "We go to the LogRhythm console to see what is causing the lockout so we can fix it."

Additionally, LogRhythm now provides critical insight to help keep the terminal servers running properly. It turns out that these externally facing servers have been experiencing numerous and frequent cyber attacks for years. "We knew the servers were being overwhelmed, but we didn't know why or where," says Sweeney. "We just weren't getting good enough information about what was happening."

LogRhythm now alerts on any unusual or suspicious activity with these servers so that attacks can be rebuffed and outages prevented. Sweeney says, "We have actually decreased downtime because we now have alerts and good insightful data. We've stopped attacks on our terminal servers because of alerts generated from LogRhythm as precursors to bad stuff happening."

Due to the versatility and effectiveness of LogRhythm, the operations team actively looks for other creative ways to use the platform—beyond their original challenges. Since their original project, they've set up a process to capture and correlate employee badge information. As people swipe their badges through readers on the EPC premises, that data is matched to their activities in the work processes. "The badge system data is used in various ways, especially by HR," says Sweeney. "For instance, we can correlate badge data with the production line data to associate the work done on products to a specific person. If there's ever a question about work tasks, we know who to talk to."

"The visibility into the infrastructure and being able to see what events are widespread is so helpful," says Sweeney. "LogRhythm has shown us things that we didn't know before. It has shed light into areas that we have now been able to improve."

"LogRhythm has shown us things that we didn't know before. It has shed light into areas that we have now been able to improve."

– Michael Sweeney, IT manager, EPC Inc.

Looking Forward

Increased Adoption of AI Engine and SmartResponse for a Reduced Manual Burden on the Team

EPC just updated its LogRhythm license to include advanced correlation functionality, and Sweeney plans to "use the heck out of AI Engine" in the months ahead. "We're using AI Engine to get rid of the false positives, and that has been so wonderful. Our false positive alarms have dropped significantly," says Sweeney.

The team has just started experimenting with Smart**Response**™ to do automatic remediation of various issues. Smart**Response** is a feature of the LogRhythm platform that automates incident response. "We want to set up an automated response that will restart the backup or reset a user's account under certain conditions. This should help to eliminate even a small amount of downtime for individuals and free up time for the help desk people."

"I feel like we've already come so far with LogRhythm, but there's still more we can do to create more efficiencies in our operations," says Sweeney. "Now we get the insight we need to troubleshoot problems and fix recurring issues. We're going to automate as much as we can to free up people from manual tasks, and AI Engine will reduce our alerts so we can focus on the most critical situations and keep our business humming."

> “Now we get the insight we need to troubleshoot problems and fix recurring issues. We're going to automate as much as we can to free up people from manual tasks, and AI Engine will reduce our alerts so we can focus on the most critical situations and keep our business humming.”
>
> – Michael Sweeney, IT manager, EPC Inc.