CASE STUDY

# LogRhythm Helps Mutual Fund Administrator Reap Big Returns with SIEM 2.0

LogRhythm

ALPS

**Organisation**
ALPS
www.alpsinc.com

**Industry**
Financial Services

**Employees**
300+

**Solution Deployed**
- Log Management and SIEM 2.0
- File Integrity Monitoring

**Log Sources Included**
- Servers
- Routers
- Switches
- Firewalls
- Custom Applications

**Log Sources Included**
- GLBA compliance
- Detection of login exceptions
- Flexible log reporting
- Powerful investigation and root cause analysis tools

> "LogRhythm stood out from the other solutions by how easy the solution lets us investigate log activity. We simply pull a group of logs and then filter them on the fly."
>
> *Pete Blood*
> IT Security Professional
> ALPS

Established in 1985 with headquarters in Denver and branch offices in Boston, New York and Seattle, ALPS offers a full-service partnership approach to a select group of mutual fund clients. The company offers turn-key capabilities that anchor all of the diverse resources needed to run a mutual fund company and has become a leader in the mutual fund service provider industry by continually providing exceptional customer service. ALPS has provided services for nearly 25 years, and as of December 31, 2010, the firm manages more than $2.7 billion in assets and provides servicing to more than $288 billion in client assets.

## The solution

As a financial services firm required to remain in compliance with the Gramm-Leach-Bliley Act (GLBA), ALPS needs to monitor and accurately report on log activity across its two data centers that contain close to 200 servers and are protected by multiple firewalls. "It allows us to retain log activity in compliance with our retention policy," said Pete Blood, IT Security Professional for ALPS. "Our previous solution was sufficient in providing security but was not as strong on log retention. We needed to improve on our retention capability to stay compliant."

On a daily basis, the ALPS IT team needs to review system logs, NetFlow traffic and DHCP logs from servers throughout the company, along with logs from the firewalls and a custom application through which ALPS provides mutual fund back-end processing to customers via the Internet. "Monitoring logs for this application is particularly critical since it's our primary platform for providing services," Blood said. "Our customers rely on the application to access data related to mutual fund accounting, transactions, and compliance. We also need to view logs from a second custom web application that provides shareholder services."

ALPS found its previous log monitoring system difficult to maintain, and pulling logs back into the system from the archive to perform historical reviews was particularly challenging. In searching for a solution with better reporting capabilities, ALPS required technology that worked with industry standard database servers. Blood also wanted a solution that would make it easier to be more self-sufficient.

"We need the ability to write rules for DHCP logs on our own so that if any unknown system shows up, we know about it right away," Blood said. "We have auditors that come in on a regular basis, so it's good to know when someone plugs in somewhere they should not.".

## The Challenge

While researching various solutions, ALPS found several positive reports in security journals on the LogRhythm Log Management and SIEM 2.0 solution. "We also considered other solutions, but LogRhythm was the best fit for our environment," Blood said. "They stood out from the other solutions by how easy the solution lets us investigate log activity. We simply pull a group of logs and then filter them on the fly. We can also move columns around

and manipulate data exactly the way we want to for our environment, and LogRhythm provides the ability to create our own rules specifically for our custom applications."

The LogRhythm deployment went smoothly with an on-site system engineer from LogRhythm assisting ALPS by adding the custom application logs to the system. "They showed us how to get the queries correct to allow us to pull in logs located in a database," Blood said. "With the LogRhythm Universal Log Adapter, it's just a matter of setting the command line correctly with the proper spaces, quotes, and returns."

LogRhythm also provided a training course on expression writing, which allowed ALPS to write rules for DHCP logs so if any unknown system shows up the ALPS network, the IT staff knows about it right away. Thanks to LogRhythm's intuitive user interface, ALPS has needed very little help since the initial deployment except for occasional questions. "With LogRhythm, we always get someone on the phone right away, and within a matter of minutes we have an answer," Blood said.

According to Blood, LogRhythm further set itself apart from competing solutions with its strong log collection and reporting—not just for daily reporting but also for its ability to retain log activity in compliance with our retention policy. LogRhythm allows ALPS to easily store and review all log activity. ALPS currently maintains log archives on the LogRhythm appliance but will eventually move these onto network attached storage (NAS) for historical reporting.

Another LogRhythm capability that ALPS has found extremely valuable is having visibility into the source and origin of connections into its network and applications. "We plan to use the geolocation component for viewing network connections and process monitoring," Blood said. "LogRhythm offers a service for populating geo IP that we have not implemented but want to look into soon."

In addition to setting alerts for specific conditions, such as when an unexpected or unauthorized IP address or system name accesses the system, ALPS also conducts proactive daily investigations, which now require much less time. "That's because we generate results faster," Blood said. "And we quickly find bad login attempts, multiple user IDs from the same IP address, and symptoms that show someone is trying to get into the system. It's very simple to check the Windows, firewall and custom application logs, which is an important benefit—if someone is trying to get into the system, we need to know."

> "With LogRhythm we generate results faster, and we quickly find bad login attempts, multiple user IDs from the same IP address, and symptoms that show someone is trying to get into the system. It's very simple to check the Windows, firewall and custom application logs, which is an important benefit—if someone is trying to get into the system, we need to know."

*Pete Blood*
IT Security Professional
ALPS

ALPS has deployed the LogRhythm File Integrity Monitoring (FIM) module which will monitor critical files. FIM sends alerts when key files are viewed, deleted or modified and when group ownership of files is changed. "We want to gain these capabilities to be aware of files changing that we don't expect to change within our core applications," Blood said. "We also want to make sure files are in the state that they should be at all times and be sure that application executable changes go through the proper procedure."