CASE STUDY

LogRhythm Streamlines Compliance and Bolsters Network-Wide Security at Endsleigh

LogRhythm

Organisation
Endsleigh Insurance Services, United Kingdom

Industry
Insurance and financial services

Employees
1000

Log Sources Include
250

Key Impacts
- PCI DSS compliance
- Improved active directory access controls
- Real-time alerting on unusual behaviour across IT systems
- Easier identification of operational inefficiencies

> "We used to collect and manage log data manually, but with LogRhythm we can now automate this process and have a single view of the entire infrastructure. This means we can now spot even the tiniest of events, including those which would have been missed in the past."
>
> *Jason Collins*
> **IT Development Centre Manager**
> **Endsleigh**

Endsleigh Insurance Services had been managing its log data manually for some time but internal business requirements and the increasing complexity of IT systems meant that a more sophisticated solution was required. Primary drivers for this were securing active directory access and ensuring compliance with Payment Card Industry Data Security Standard (PCI DSS) obligations. Since deploying a log management and Security Information and Event Management (SIEM) from LogRhythm, Endsleigh has resolved these challenges as well as boosting security across its networks. Moving forward the system will increasingly be used to identify and eliminate operational inefficiencies.

The Organisation

Originally founded in 1965, Endsleigh has since grown to become one of the UK's leading independent intermediaries. It specialises in providing insurance solutions for career people and aims to develop lifelong relationship with its clients. The company offers a product range that starts with students and continues through to retirement. In order to accommodate the busy lifestyles of its customers, all of its policies are available both online and over the phone. These fully integrated systems ensure that records and client files can be accessed immediately however customers choose to interact with the company.

The Challenge

Endsleigh is subject to a variety of regulations including the Data Protection Act, PCI DSS and Financial Services Authority (FSA) rules – obligations that require ongoing collection and analysis of log data resources. The company had been managing this process manually, however it became clear that it could no longer rely on the log data provided by individual applications and network devices to prove compliance and spot security threats. With a rising number of logs, and with each device and application requiring manual configuration and producing separate log data reports, the overhead of collecting and processing log data was becoming difficult to manage.

In addition to complying with industry regulations, Endsleigh needed to instigate better control processes over its active directory infrastructure. Active directory has a high volume of large log files and the company's external auditors required evidence that privileged user access was being controlled in a structured fashion. This had become quite challenging due to the sheer weight of logs being produced.

The Solution

Endsleigh considered a number of competing solutions, including offerings from LogLogic and ArcSight, but chose to deploy a dedicated log management

and SIEM system from LogRhythm for its scalability, performance specifications, ease-of-use and out-of-the-box functionality.

In contrast to the siloed, manual process that was in place before, the new solution is centralised, automated and able to collect and analyse logs from a wide range of data sources. During the early stages one of Endlseigh's biggest concerns was around the initial setup:

"We wanted a comprehensive solution but we were worried it could take considerable upfront effort to configure specific log settings and alerts," said Jason Collins, IT development centre manager at Endsleigh Insurance Services. "The deal was made via NTS, a partner we had worked with on a number of previous occasions. They provided us with a good introduction to the solution and spent a long time working with us to identify our exact requirements. The joint support provided by LogRhythm and NTS during the initial stages of the deployment was exceptional; both teams were available at all times to help us get the configuration right first time. Once the installation was complete, we have found the solution to be very straightforward – indeed, anyone can use it."

With the LogRhythm solution in place, Endsleigh can now generate reports to prove compliance and act on real-time alerts in case any event takes place that could affect its ability to meet regulations. In the future, Endsleigh intends to use LogRhythm to discover and fix operational inefficiencies, including understanding when remote access connections have failed, or identifying desktops that have not received scheduled software updates.

Collins continued:

"Like so many organisations, Endsleigh faced an uphill challenge to collect, process and store an ever growing number of logs – failure to do so risked non-compliance or a breach. In addition to solving these issues LogRhythm has also given us the ability to pinpoint operational problems and improve the overall efficiency of our entire IT estate.

> "...LogRhythm has also given us the ability to pinpoint operational problems and improve the overall efficiency of our entire IT estate."
>
> *Jason Collins*
> IT Development Centre Manager
> Endsleigh

"Crucially the LogRhythm solution has helped us to meet our two primary objectives – PCI DSS compliance and tightening up active directory control processes. By implementing real-time, ongoing log collection and analysis we comply with PCI. In addition, by automating this process the volume of logs no longer prevents us from being able to demonstrate a best-practice approach to active directory privileged user access."