CASE STUDY

The Share Centre Chooses LogRhythm to Deliver PCI Compliance and Enhance Data Security

LogRhythm

thesharecentre: simply easier

Organisation
The Share Centre
www.share.com

Industry
Investment and financial services

Employees
150

Log Sources Include
- 100 in total including:
- Windows Event Logs from servers and workstations
- Syslog from firewalls
- Syslog from network switches
- Syslog from IDS
- Event logs from end point protection
- Web Server Logs

Key Impacts
- PCI DSS compliance
- Simplified reporting
- Network visibility
- Real-time alerting on unusual behaviour across the IT system
- Easier identification of operational inefficiencies

> "By implementing LogRhythm's solution, not only have our original goals of improving our security and compliance processes been achieved – it's also enabled us to improve the effectiveness and efficiency of our entire IT operations."
>
> *Giles Roberts*
> IT Infrastructure Manager
> The Share Centre

The Share Centre needed to upgrade its infrastructure due to increasingly complex IT systems and a growing compliance burden, including Financial Services Authority (FSA) and Payment Card Industry Data Security Standard (PCI DSS) regulations. Prior to implementation, the organisation's IT team was required to manually review all log data in order to identify and scrutinise anomalies, as well as work out which data related to which security event.

Since choosing to deploy LogRhythm's log management and Security Information and Event Management (SIEM) solution, the organisation has resolved these challenges and strengthened the security across its networks. Moving forward, the system will ensure The Share Centre continuously improves the effectiveness and efficiency of its entire IT and security system, and will help the company overcome future challenges, such as achieving ISO 27001 compliance and meeting external IT audit criteria.

The Organisation

A member of the London Stock Exchange, The Share Centre was established in 1990 to provide value-for-money share services for private investors. Since then, it has become a multi-award winning leading UK retail stockbroker, with more than 160,000 Share Accounts and ISAs.

Based in Aylesbury, The Share Centre has 150 staff. Its range of services includes buying and selling shares via the Internet, telephone and post, with a comprehensive share administration and safe custody service. In addition, its Advice Team provides comment on market sectors, individual shares and funds online, while account customers can receive individual telephone advice on UK-listed shares and on funds traded via the CoFunds trading platform. Tax-efficient investment 'wrappers' including ISAs, CTFs and SIPPs are also available.

The Challenge

As a retail stockbroker, The Share Centre's reputation depends on its ability to handle confidential information safely, and it is subject to a variety of increasingly stringent regulations including PCI DSS and FSA legislation. These obligations require the company to collect and analyse log data sources constantly, in order to provide a real-time view of what's happening within the network, and the traceability required to connect seemingly unrelated events.

The Share Centre had been managing the process manually, but with a rising number of logs, and with each device and application producing separate log data reports requiring manual configuration, this became increasingly time-consuming and difficult to manage. In order to ensure its IT estate was secure and compliant, whilst still maintaining an effective and efficient infrastructure,

the company needed an intuitive, automated solution capable of providing real-time monitoring as well as a consolidated overview of all events.

The Solution

The Share Centre evaluated several solutions from competing vendors, and LogRhythm's validation in Gartner's Magic Quadrant, together with reseller recommendations, ensured its inclusion on the shortlist. LogRhythm's dedicated log management and SIEM system was eventually chosen following rigorous testing, for its ease of use and ability to deal with a wide range of data sources.

Giles Roberts, IT Infrastructure Manager at The Share Centre explains:

"We were looking for a comprehensive system that would help us stay both compliant and secure, and it was clear that in order to achieve this efficiently, we needed a centralised, intelligent logging solution, with real-time monitoring, and 360 degree visibility across the network. After extensive evaluations, LogRhythm's log management system stood out for its ease of use, while being able to deal with a comprehensive range of data sources. The solution not only met our business requirements, but it also provided all the functionality we needed for generating reports and alerts so that we can act immediately in the case of an incident.

"LogRhythm and its partner supplied us with an outstanding level of assistance in getting the solution set up, from ensuring that it was up and running within a day, through to training our staff. The solution is very easy to use on a day-to-day basis as we can view the entire network infrastructure from one dashboard and easily generate clear, digestible reports. In addition, it correlates all the data relating to an incident, so that we avoid the time consuming process of investigating these logs manually."

With LogRhythm's solution now in place, The Share Centre can also monitor and alert on security events occurring on any part of the network, identifying both potential external and internal breaches – for example, hack attacks, the abuse of access rights or the unauthorised use of flash drives. In the future, The Share Centre intends to use LogRhythm to assist in future goals such as achieving ISO 27001 compliance and meeting external IT audit criteria, as well as improve operational efficiencies.

Roberts continued:

"Crucially, by implementing LogRhythm's solution, not only have our original goals of improving security and compliance processes been achieved – it's also enabled us to gain powerful insight into the whole of our IT operations. LogRhythm provides us with the actionable intelligence required to see where configuration changes need to be made, and this deeper understanding of our infrastructure is helping the company improve the effectiveness and efficiency of our entire IT system, and will also assist us in overcoming future technology and security challenges.""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."

> "We were looking for a comprehensive system that would help us stay both compliant and secure, and it was clear that in order to achieve this efficiently, we needed a centralised, intelligent logging solution, with real-time monitoring, and 360 degree visibility across the network."

Giles Roberts
IT Infrastructure Manager
The Share Centre