CASE STUDY

Combining PCI DSS Compliance with Unprecedented IT System Analysis Capabilities

LogRhythm

ventura Outsourcing Experts

Organisation
Ventura
Leeds, United Kingdom

Industry
Customer management outsourcing

Employees
8,000

Log Sources Include
- Windows, Unix, Linux
- Database
- Intrusion Protection System (IPS)
- 2-factor authentication
- Webserver
- Firewalls
- Custom log sources
- VPNs
- Anti-virus software

Key Impacts
- PCI DSS compliance
- Reduced time for trouble-shooting
- Real-time alerting on unusual behaviour across the IT system

> "LogRhythm has given us network visibility, transforming how we monitor and manage our IT infrastructure and applications."
>
> *Mark Wityszyn*
> IT Security Manager
> Ventura

Like it does with most organisations who must comply, the Payment Card Industry Data Security Standard (PCI DSS) triggered a review of how Ventura, one of the UK's largest customer management outsourcers, handled its log and event data. Since installing an integrated Security Information Event Management (SIEM) solution from LogRhythm, Ventura can carry out complex analyses of log and event information as well as identify any anomalies in real-time.

The Organisation

Ventura, a subsidiary of Next Group, is one of the UK's leading outsourcers, employing over 8,000 people throughout its onshore and offshore operations. The company provides customer management, debt management, sales and revenue generation, document management, IT services and business solutions to an array of blue chip and government organisations, including O2, Sky and the Department for Work & Pensions (DWP).

The Challenge

Accessing log and event data for compliance or security investigation purposes had always been a laborious and time-consuming task for Ventura. This was because log and event data were held in heterogeneous formats on each of the various IT systems in operation, requiring separate analysis to be accessed. The company recognised the value that an integrated Security Information Event Management (SIEM) solution would offer in terms of simplifying and reducing the time taken to access and analyse log data.

As 90 per cent of Ventura's clients are impacted by the PCI DSS regulations, it means that Ventura must also be compliant due to the information that is effectively going through Ventura systems on its clients' behalf. PCI DSS has specific requirements around log data centralisation, archiving, monitoring and reporting for security and auditing. As such, in 2009, when Ventura embarked on its PCI DSS compliance programme, it triggered an assessment of how log and event data is handled at the company.

The Solution

After assessing a number of competitive solutions, Ventura chose to implement LogRhythm. Mark Wityszyn, IT security manager, Ventura explains the choice:

"We'd gone as far as installing a demo system from one organisation before evaluating LogRhythm. However, after trialling LogRhythm for just 30 minutes, it became apparent that LogRhythm was a more powerful yet simpler to use solution - especially as I was able to subsequently fully demonstrate it to colleagues that same day. While the primary driver behind installing

LogRhythm was PCI DSS compliance, we specifically wanted a solution which would transform the log data and event management processes at Ventura. We were particularly impressed with how LogRhythm allowed us

> “Today we can carry out full and detailed log analysis within a couple of hours. Previously this was just unthinkable.”
>
> *Mark Wityszyn*
> IT Security Manager
> Ventura

to analyse data by a straight forward click through to the original source message. For this analysis capability, and the simplicity of the system, we chose to implement LogRhythm.”

Implementation of LogRhythm at Ventura took just two days which meant that within 48 hours, the company was already getting a return on investment from the solution.

Installing LogRhythm has helped ensure that Ventura is fully compliant with the monitoring and alerting requirements of PCI DSS.

Beyond PCI DSS compliance, Ventura is using LogRhythm to monitor activity on the separate systems it operates on behalf of its clients. LogRhythm correlates and consolidates the information for each system, identifying any unusual behaviour, giving Ventura’s IT security team full insight into IT system activity for each client. Not only does LogRhythm alert on any anomalies and produce easily interpreted reports, it also provides reassurance to Ventura’s clients that the company is monitoring its IT systems in an efficient and effective manner.

Wityszyn continues:
“LogRhythm has given us network visibility, transforming how we monitor and manage our IT infrastructure and applications. The visibility it offers is unlike anything that we had previously, giving us greater confidence and protection. By continually monitoring network activity and flagging potential problems as and when they occur, LogRhythm assures us that there are no network issues of which we are not aware. Today we can carry out full and detailed log analysis within a couple of hours.

Ventura has started to extend the use of LogRhythm beyond the IT security team to its network administrators. They have been using the solution to profile firewall rule bases which makes it quicker and easier to identify which rules aren’t in use or which ones need updating – helping to keep the firewall as effective and efficient as possible.

This roll out is only the start as Wityszyn concludes:
“In the coming months we will be focused on tweaking LogRhythm to bring even more efficiencies and reduce log analysis time to under an hour. Also, Ventura does a considerable amount of internal web development. I see

> “... after trialling LogRhythm for just 30 minutes, it became apparent that LogRhythm was a more powerful yet simpler to use solution - especially as I was able to subsequently fully demonstrate it to colleagues that same day.”
>
> *Mark Wityszyn*
> IT Security Manager
> Ventura

LogRhythm being extended to these teams so that they can evaluate their developments as they go along. This would mean that any issues can be flagged and addressed there and then, and not at the end of the development cycle, resulting in considerable time savings and a more straight forward development process.”