LogRhythm Brings Time Savings, Improved Network Visibility and Operational Efficiencies to Commidea

:::LogRhythm™

Organisation
Commidea Ltd
www.commidea.com

Industry
Credit Card Processing

Employees
135

Log Sources Include
• Routers
• Windows 2003, Windows 2008
• Custom applications
• VMware
• ESX servers
• Firewalls
• Switches
• Remotely managed PDUs
• SQL server databases

Key Impacts
• Reduction by hours of daily log data audits
• Simplified log data analysis
• Improved visibility of data centre activity
• New network management efficiencies
• Optimum levels of security resulting in improved customer service

> ❝ LogRhythm has brought an integrated SIEM and File Integrity Monitoring solution to the market which is unlike any other. ❞
>
> **Marc White**
> Head of Security and Compliance
> Commidea

When Commidea first became Payment Card Industry Data Security Standard (PCI DSS) compliant in 2004, technology restrictions meant that it had to install two separate systems to meet the stipulated log data requirements. These systems were complex and time consuming to use. However, since installing a new integrated log management & SIEM 2.0 solution (log and event management, file integrity monitoring, and network and user monitoring in a single offering) from LogRhythm, Commidea is experiencing new efficiencies by having an unprecedented view of data centre activity and superior log data analysis capabilities.

The Organisation

Commidea is a market leader in the development of card payment solutions. The company provides a range of high performance systems and tailor-made solutions for almost every industry and market sector. Established for over 17 years, Commidea has been at the forefront of pushing the boundaries of card payment technology. In October 2009, Commidea launched Ocius Sentinel, the UK's first card payment processing solution to offer true end-to-end dual encryption of card holder data.

The Challenge

Due to the quantity of credit card transactions it processes, Commidea is classed by the Payment Card Industry Data Security Standard (PCI DSS) as a level one processor. Commidea has been fully compliant with PCI DSS since 2004 when the regulations were first established and its compliance is checked annually by an independent third party QSA.

The PCI DSS has specific requirements relating to how log data is handled which includes storing the logs in a central repository and in an accessible format. This also applies to files which are unlikely to be altered but still have to be monitored to protect against tampering.

In 2004 when Commidea was considering how best to meet the log data requirements of PCI DSS, the only technology available comprised of two separate solutions – a File Integrity Monitoring solution and a Security Information Event Management (SIEM) system. Marc White, head of security and compliance, Commidea, explains:

"When we first embarked on our PCI DSS programme, there simply wasn't a great deal of choice so our hands were tied in terms of what SIEM and File Integrity Monitoring solution we could implement. While the original solutions that we installed back then ensured PCI DSS compliance, having to access two systems, firstly to view the logs in one and then secondly identify file changes in another, was an incredibly time consuming task."

The Solution

When Commidea decided to open a new data centre in 2009 it triggered an opportunity to investigate what alternative log data management solutions were available. The company carried out an extensive assessment of a number of vendors before choosing LogRhythm, the company that makes log data useful.

Marc White continues, "In the past few years, technology has advanced considerably. In particular, the introduction of LogRhythm has brought an integrated SIEM and File Integrity Monitoring solution to the market unlike any other. We were attracted to the fact that whilst there is lot of preconfigured options straight from the box, dramatically speeding up implementation time, it has the flexibility and ease of use to meet our user specific requirements. Additionally, LogRhythm allows log data to be interrogated by drilling through from one single interface which considerably simplifies the process."

Implementation of LogRhythm was straight forward. Commidea provided the team with basic details of its log sources in advance so that when the LogRhythm solution was delivered and installed into the new data centre, it became operational immediately - bringing an early return on investment.

As well as supporting PCI DSS compliance, Commidea is using LogRhythm for a number of additional activities, resulting in a greater return on investment. The IT Systems team utilises LogRhythm to track and trace all traffic in and out of the data centres, ensuring that all services are fully functional with no technical difficulties.

Elsewhere, the Security & Compliance team runs its daily auditing checks on LogRhythm, for example, seeing if any unauthorised changes have been made. Because LogRhythm stores all of the log data in one central resource, the team only needs to go to one interface to access the information, reducing analysis time significantly.

LogRhythm also developed a specific application which simplifies how Commidea monitors the activity of its remote engineers centrally, including when, and where from, they

> " LogRhythm provides us with much greater visibility of all data centre activity from a single interface, something we never previously had. "
>
> **Marc White**
> **Head of Security and Compliance**
> **Commidea**

log-in and out of the data centre. This added visibility ensures that Commidea is notified of any unusual behaviour which it can then address immediately.

Marc White continues: "LogRhythm is just a joy to use and provides us with much greater visibility of data centre activity from a single interface, something we never previously had. But technology is only part of the story; you still need to have strong people and support behind it. The team at LogRhythm is one of the most professional that I have encountered. They are always willing to take on feedback and enhance the solution to ensure that we are getting the most out of it. LogRhythm is now playing a critical role in our auditing and investigation processes and we have recently invested in an additional appliance to meet our continued company expansion and development."