McColl's Retail Group remains PCI compliant with the LogRhythm NextGen SIEM Platform

Convenience retailer McColl's realised it needed to change its business payment model when its customers were increasingly choosing to pay for their goods using bank cards instead of cash. This resulted in McColl's becoming a level one card merchant, which required the highest standard of compliance to the Payment Cards Industry (PCI) regulations.

To ensure they stayed compliant, McColl's shortlisted three security organisations, with LogRhythm proving to best suit the retailer's needs. LogRhythm created a bespoke commercial strategy for McColl's, which utilised its NextGen SIEM Platform to create personalised security alerts, helping McColls keep its high volumes of transactions safe.

The Organisation

McColl's Retail Group is a British convenience store and newsagent operator, trading under the names of McColl's, Martins, and RS McColl for stores in Scotland. There are 1,600 stores across England, Scotland and Wales. McColl's uses a flexible business model and is focused on bringing the best product offer, and convenient services, to all the local communities it serves so it can achieve its vision to be the neighbourhood's favourite shop.

The Challenge

McColl's, which began operating in the early 1970s, has seen its business evolve over time. In 2011 it recognised a shift in how customers wanted to pay for their goods, which resulted in the company becoming a level one card merchant. This meant McColl's needed to comply with PCI regulations, which requires organisations to independently audit systems, processes and procedures to ensure they are compliant with the data security standard. A large portion of these requirements relate to centralising the secure logging of security events, which is why McColl's Retail Group needed to find a suitable security solution.

However, at that time not many companies were proactively pursuing PCI compliance. Security logging systems were mainly adopted by legal firms and financial corporations and there were no cost effective solutions available for retail businesses with large estates of EPOS tills to manage. McColl's processes over 5.5m customer transactions per week. As a convenience business the average transaction value is low at £5.62, so commercials based on value as opposed to volume was of importance – something which was foreign for security logging systems at the time.

Organisation
McColl's Retail Group plc

Industry
Retail – Convenience

Employees
22,000

Key Impacts

- Achieved the required PCI compliance
- Mean time to detect (MTTD) and mean time to respond (MTTR) has been reduced
- Ability to create personalised alerts to detect threats

The Solution

In order to remain PCI compliant, McColl's set out to identify what was available to satisfy its need. Through the help of a channel partner, it shortlisted three organisations; one of them being LogRhythm. While all three were strong candidates, there were features of the LogRhythm offering that stood out.

"Features including the file integrity monitoring and strong traceability between the logging systems meant LogRhythm was steps ahead of what we were seeing in the marketplace. With PCI requirements so stringent, these features made staying compliant much easier," said Peter Gore, development & compliance manager at McColl's.

At the time, McColl's had 1,200 stores which they needed to ensure were compliant; and therefore worked with LogRhythm to find a strategy that best suited them. "We were able to create a commercial strategy that worked for every McColl's store," said Gore. "We were not the regular customer for security firms at the time, but LogRhythm worked with us instead of forcing us into a solution that would not be of use."

Presently McColl's logs over 13.5m events using LogRhythm per day.

Having been PCI compliant since 2013, McColl's is also seeing the other benefits of LogRhythm's solution. "Not only do we have a centralised logging system; we also have a system that monitors every potential security threat and can design personalised alerts within it. We need to respond to alerts that are relevant, instead of wading through the huge volumes of information. LogRhythm enables us to do that, saving us time and allowing us to respond to actual threats. Even now that there is a new P2Pe payment system solution in place which reduces the scope of PCI significantly, we still see LogRhythm as a good business investment. It's a tool that gives us peace of mind. If the worst were to happen, the forensic examiners would have the right data to analyse in order to prevent any further and future damage. Without LogRhythm, it would be a near impossible task."

> **"LogRhythm is a good business investment and a tool that gives us peace of mind. If the worst were to happen, the forensic examiners will have relevant data to analyse in order to prevent any further and future damage. If we didn't have LogRhythm, it would be a near impossible task."**
>
> – Peter Gore, development & compliance manager at McColl's