CASE STUDY

JD Williams picks up more than just compliance when selecting LogRhythm

LogRhythm
The Security Intelligence Company

JD Williams
Looking good has never felt so good

Organisation
JD Williams
www.jdwilliams.co.uk

Industry
Retail

Employees
2,500 +

Key Impacts
- Compliance with PCI DSS regulations
- Complements fraud team's analysis
- Identification and closure of unnecessary privileged accounts
- Ability to identify and resolve network issues that are unrelated to security

> "We can rely on LogRhythm's Advanced Intelligence Engine rules and use the web interface for alarm management and more operational information, rather than creating our own dashboards and reports. LogRhythm is an expert in the field and we want to use its knowledge to our advantage."
>
> *Richard Jones*
> Information Security Team Leader
> JD Williams

As a retail organisation, JD Williams is required to protect the data of millions of customers, as well as adhere to stringent industry standards. As such, the organisation sought a solution that would enhance its compliance with regulations, such as PCI DSS. In 2010, the company selected LogRhythm's security intelligence platform due to its position as a leader in the market.

The organisation has since identified further uses of the LogRhythm platform, beyond compliance, and is now using it to add context to information held by its fraud team, as well as identify non-security related issues on the wider network.

The Organisation

JD Williams is a leading internet and catalogue home shopping company, owned by parent company the N Brown Group. The company has over 140 years of experience in the distance shopping market and in 2009 expanded its operation to high-street stores. The multi-channel retailer has 5 million customers worldwide and its brands include Simply Be, Jacamo, Figleaves and Marisota.

The company has a turnover of over £780 million, with more than half of its business generated online. As such, JD Williams is responsible for ensuring the protection of an enormous amount of personal and payment data of its customers.

The Challenge(s)

As a large retail operation with customers across the globe, JD Williams is accountable for safeguarding the personal data and payment information of more than 5 million customers. Processing over 6 million card transactions annually, the retailer is classed as a tier 1 PCI DSS merchant, and is required to meet necessary regulations, including standards for handling log data.

On average, the company processes between 150 and 200 logs per second and required a solution that would enable it to handle this volume of data more effectively. Prior to implementing LogRhythm, all data was dealt with manually, however the team soon recognised that it required a much more efficient system, both to save on costs and ensure it could better comply with regulations.

In 2013/2014, JD Williams leveraged information from the solution that would complement the work of its fraud team; the industry is inherently at risk from nefarious activity.

The Solution

Having identified technology gaps within the organisation, JD Williams shortlisted potential partners based on the 'leaders' in Gartner's Magic Quadrant. The organisation looked at a range of solutions, including IBM's Q-Radar and Splunk, before selecting LogRhythm's Security Information and Event Management (SIEM) platform.

"The Gartner Magic Quadrant is a really important vehicle when venturing into a space that is previously unknown – as SIEM was for us at the time," explains Richard Jones, information security team leader at JD Williams. "LogRhythm ticked all of the boxes for us – it's a leader in its space and the commercials

were very attractive. As well as providing the tools to ensure PCI compliance, it also offered us the ability to manage non-security related events as well, so it made the most sense."

The implementation of LogRhythm's security intelligence platform was carried out by specialist security distributor and LogRhythm partner, Nebulas. Following the initial installation, the system was reviewed in 2013, when the team decided to upgrade to LogRhythm's latest solution.

"Both the original implementation of LogRhythm and the upgrade were straightforward, without any technical issues. The guys from Nebulas were really good and there was barely any disruption when we upgraded," continues Jones. "We've definitely seen a difference since the upgrade. We used to write a lot of rules ourselves, but now we rely on LogRhythm's Advanced Intelligence (AI) Engine rules and use the web interface for more operational information, rather than creating our own dashboards and reports. LogRhythm is an expert in the field and we want to use its knowledge to our advantage."

While JD Williams originally sought a solution to ensure PCI DSS compliance, its use of LogRhythm has expanded to benefit other areas of the business, such as assisting its fraud prevention team. For any retailer, fraud is a very prevalent threat vector and, when suspicious activity is identified, the security team is able to feed information into the LogRhythm platform for it to undertake additional processing. From there, it is able to highlight irregular activity, such as multiple attempts at logging in within a certain time period, which may indicate possible account takeovers. That data is then passed to the fraud team to complement its own information and for investigation.

Jones also says that the security intelligence platform has highlighted the widespread, and unnecessary, use of generic or shared administration accounts within the organisation, and has enabled it to close them down completely.

"Realistically, there is no reason to be logging on as an administrator on any platform. Everyone should have individual log-ins and then assigned pseudo-admin rights," explains Jones. "We can now use rules to highlight where privileged accounts are in use and have subsequently been able to flush most of them out. It's been a huge advantage to use this solution in an area we had not previously considered."

The organisation also uses the LogRhythm platform for non-security related events, such as identifying distressed devices on the network or mis-configured applications.

"Our engineers have been able to isolate and investigate events on the network that are causing problems within hours of identifying an issue," explains Jones. "This has been a huge advantage for the network engineers as they are now able to prevent an incident before it becomes a problem. It's really opened our eyes. There's so much happening on the network that we previously didn't know about, and LogRhythm's security intelligence solution has been exceptional at helping us identify issues and take preventative measures when required."

> "LogRhythm ticked all of the boxes for us – it's a leader in its space and the commercials were very attractive. As well as providing the tools to ensure PCI compliance, it also offered us the ability to manage non-security related events as well, so it made the most sense."
>
> ***Richard Jones***
> **Information Security Team Leader**
> **JD Williams**

Compliance was also a key reason JD Williams selected LogRhythm's platform, with the system now enabling the company to provide proof that it is meeting required standards, such as how frequently logs are checked, which was often hard to do. Now well on its way to achieving what it set out to, the team is considering how it can develop its use of the system further.

"The LogRhythm platform is clearly more than just a tool for compliance, and there is still more we could be using it for. As such, we're starting to explore how we can use the intelligence that LogRhythm provides to improve our security stance even further," concludes Jones.