# CASE STUDY: TRAINLINE

### *KEEPING CLIENTS ROLLING AND SECURE*

## *ACHIEVING PCI COMPLIANCE ON AWS*

Mieke Kooij, Trainline's Security Director, described, "We are a one-stop-shop for train travel, bringing together major train companies and providing our customers with a complete set of travel options. We're all about bringing best-in-class technology to rail, to make it easy for travelers to find the best price for their journey."

The Trainline website receives 30 million visits per month and the company is experiencing 100% year-on-year growth in app transaction volumes. Trainline sells a ticket every three seconds and manages an equally massive number of credit card transactions coming from all over Europe. The Trainline team is aware of the responsibilities that come with handling this volume of sensitive information. Kooij noted, "We're trusted with a huge amount of personal data and it's imperative that we put security first."

True to its reputation of being one of the industry's leading innovators, Trainline recently moved its portfolio of applications to Amazon Web Services (AWS), decommissioning its legacy bricks-and-mortar production data center in the process.

The transition to AWS provided benefits with agility, efficiency, and economy but also necessitated a change in the company's approach to security. Trainline leveraged this move to ensure security was built in to their foundations.

trainline

### ABOUT

Trainline is Europe's leading independent retailer of train tickets. Now owned by KKR, it sells tickets worldwide on behalf of 48 train companies, helping customers make more than 100,000 smarter journeys every single day in and across 24 countries, generating £2.3 billion (US$3.0 billion) in annual revenues.

### SOLUTIONS

**ALERT LOGIC® PROFESSIONAL**

An integrated suite of intrusion detection, vulnerability scanning and log management for the cloud, on-premises, hosted, and hybrid infrastructures.

"Executing in the cloud requires a totally different mindset: You can't just deploy a traditional layered architecture and expect to be protected. Being virtual turns things on their head, you need new ways to gain visibility and ensure the right level of control," explained Kooij. "We jumped at the opportunity to implement an entirely new security architecture," she added.

## WHY ALERT LOGIC?

Jerry Wozniak, Application Security Lead for Trainline, recounted, "There are not a lot of cloud solution providers for either intrusion prevention systems (IPS) or intrusion detection systems (IDS). Functions such as file integrity monitoring, or even vulnerability scanning, are more challenging in a virtual environment. We looked for solutions that were designed from the ground-up to work in the cloud and that leverage advanced APIs to fully understand the infrastructure, rather than relying on the old approach of discovery via network scans."

A security architect on the Trainline team already had familiarity with the Alert Logic suite of solutions and based on those positive experiences recommended Alert Logic® Professional.

> ***"WHAT REALLY IMPRESSED US WAS THAT ALERT LOGIC WAS OUT THERE AT THE FOREFRONT FROM THE BEGINNING; PROVIDING VISIBILITY INTO TRAFFIC AND SERVICES TO HELP ITS CLOUD-BASED CUSTOMERS DELIVER BOTH SECURITY AND COMPLIANCE WITH KEY REGULATIONS SUCH AS PCI DSS [PAYMENT CARD INDUSTRY DATA SECURITY STANDARD.]"*** - Mieke Kooij, Security Director for Trainline

The Alert Logic solutions proved to be straightforward to implement, Wozniak reflected, "Deployment is very easy: Alert Logic Professional just about configures itself out of the box. It saves us a lot of time and troubleshooting, we appreciate how well it works." Kooij concurred, "The company's solutions are specifically engineered for cloud deployments instead of taking older architectures and forcing them to work – this is exactly what we were looking for."

## THE RESULTS

Trainline has deployed Alert Logic Professional across multiple infrastructures; not only for AWS-based applications but also running in one of their management data centers.

Trainline's impressive year-after-year growth means that security measures have to scale accordingly to keep pace with the increasing volumes of data. With a back-end team that provides continual monitoring, Alert Logic delivers the required scalability and provides Trainline with the critical proof points required to maintain PCI DSS compliance. "With the managed, outsourced nature of the Alert Logic service, we don't have to spend time or worry about hiring additional resources to maintain coverage," asserted Wozniak.

Kooij added, "The Alert Logic team's analysis of our logs has really helped us to understand what our applications are telling us, and what 'normal' and 'good' states look like, which is a view that we didn't have before. It's great working with a specialist and leader in this space who provide continuous monitoring and visibility."

Wozniak added, "We have a very close relationship with our account manager and all of our questions and concerns are dealt with very professionally and quickly. I'm very happy with how the Alert Logic solutions work and the support we receive: The relationship has been going very well."

Trainline's is also working to ensure compliance with the General Data Protection Regulation (GDPR) introduced by the European Commission to strengthen and unify data protection for individuals within across Europe. "The GDPR is about far more than your technical controls, but it's great to know that we have the right security foundations." commented Kooij.