Arriva Trains Achieves New Level of Security and Addresses PCI DSS Compliance with Internal Visibility

ARRIVA
Trains Wales
Trenau Arriva Cymru

Highlights

Company: Arriva Trains Wales

Industry: Transportation

Location: Europe

About the Customer

Arriva Trains Wales is part of the Arriva Group, a part of Deutsche Bahn (DB), one of the largest providers of passenger transport in Europe, employing more than 55,000 people and delivering more than 2.2 billion passenger journeys across 14 European countries each year. The Arriva train network extends throughout Wales and the border counties of England, providing local and long distance services to destinations including major cities such as Swansea, Cardiff, Newport, Birmingham, Chester and Manchester. It has over 2,200 employees and a fleet of 128 trains and 247 stations.

> **"Magna could tell us straightaway if something was wrong on our network... it could clearly show us what was going on."**
>
> - Paul Stern, IT Network and Security Manager, Arriva Trains

The Need

Committed to the highest levels of quality and reliability for its customers, Arriva Trains Wales wanted to protect its business systems and its financial and customer data from a potential breach. Paul Stern, IT Network and Security Manager, understood that traditional security was no longer enough to detect a would-be attacker and that eventually one would gain access to the network. "If an attacker wants to get into a network, there are a million ways and eventually they will succeed," said Mr. Stern. "It's the new reality of security."

The Results

Addressing PCI DSS

The firm's Qualified Security Assessor (QSA) for PCI compliance put the problem simply to Stern, "If you had an attacker on your network, how would you be able to detect it?" At the same time, the parent company was driving adherence to the PCI DSS (Payment Card Industry Data Security Standard). "We budgeted for PCI DSS and started looking for the best solution out there to give us visibility inside our network," said Mr. Stern.

Using Behavior as the Basis for Detection

"We looked at two behavioral analysis type solutions," said Mr. Stern. "We picked LightCyber because it could clearly show us what was going on." The other solution had a futuristic interface that was appealing but could not clearly show the real issues. In contrast, "Magna could tell us straightaway if something was wrong on our network," explained Mr. Stern. Another important consideration was having integrated visibility of both the network and the endpoints to provide a high level of accuracy and actionability. During the evaluation, Magna even found ransomware files on a host that had not yet fired and stopped the threat even before it started.

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP

Key Challenges

- Improve ability to quickly detect internal and external attackers
- Address a PCI DSS requirement to detect security events on their internal network
- Avoid the damage and disruption of a data breach

Key Results

- Visibility of network and endpoints in one integrated system
- Low number of daily alerts, with high accuracy
- "Audit tool for the network"
- Ransomware alerts allowed Arriva to quickly quarantine an infected computer
- Unauthorized and risky employee activities uncovered

About LightCyber

LightCyber is a leading provider of Active Breach Detection solutions that accurately detect active cyber attacks that have circumvented traditional threat prevention systems. The LightCyber Magna platform is the first security product to simultaneously profile both network traffic and endpoint state in order to accurately detect compromised user accounts and devices early in the attack lifecycle, and to enable security operators to remediate breaches and stop attacks before real damage is done. Founded in 2011 and led by world-class cyber security experts, the company's products have been successfully deployed by top-tier customers around the world in the financial, legal, telecom, government, media and technology sectors.

Indispensable from the Start

Arriva did an initial evaluation by deploying the LightCyber Magna solution in their network. During the evaluation, they became accustomed to looking at Magna every day to know the status of their network and see other discoveries it made, including finding operationalized malware that escaped perimeter security and was communicating with sites or other software. It also uncovered risky behavior that could compromise the network. Some of the findings included some unauthorized remote access tools and also IT applications that were out-of-date. "After the month evaluation, LightCyber took Magna out and we immediately missed it. It was easy to establish a business case for it, so we purchased the product."

No Configuration Process – It Just Works

Setting up the Magna appliance was astonishingly easy. "It worked almost right out of the box," said Mr. Stern. Magna immediately started learning the Arriva environment. "It really didn't have to be taught or configured," said Mr. Stern. "There's not enough of us to have to invest time to try to make something work. There can't be any of this messing around."

Confidence to Find Attacks Quickly

"Magna is kind of an audit tool for our network," said Mr. Stern. "We deployed a tool from one of our partners, and Magna showed that it was port scanning the network and pinging various internal IP addresses. We never would have known this without Magna. It gives me confidence when I see how it finds various activities on the network. I know Magna will find any active attacks if and when they occur."

Magna found other irregularities. At one point it highlighted unusually high traffic utilization from some devices. It turned out that an employee was uploading video from company CCTV camera to his Facebook account. While this was not a strict security issue, it was in violation of company policies, and the incident was curtailed.

Low Number of Alerts

Generally, Magna produces 4-5 alerts per day for Mr. Stern's team. The number is easily manageable, and Arriva Trains can review all them and prioritize their response. No staff time is involved with trying to sort through a voluminous number of alerts that are mainly comprised of false positives.

The Power of Visibility

Having a new approach to security based on behavioral profiling has been critical to fulfilling PCI responsibilities and protecting the integrity of the company. "Our executives watched as the CEO of TalkTalk went on national television and had to explain about their recent data breach," said Mr. Stern. "Right then we decided that we never wanted to be in that position. That's why we have LightCyber."

> **"Magna is kind of an audit tool for our network… It gives me confidence when I see how it finds various activities on the network. I know Magna will find any active attacks if and when they occur."**
>
> - Paul Stern, IT Network and Security Manager, Arriva Trains

LIGHTCYBER
5050 El Camino, Suite 226
Los Altos, CA 94022
Ph: (844) 560-7976
www.lightcyber.com

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP