Qualpay chooses Coalfire to validate security and achieve PCI DSS compliance to maximize market adoption.

AT A GLANCE

For Qualpay, achieving a Payment Card Industry Data Security Standard (PCI DSS) Report on Compliance (ROC) in a timely manner was critical to maintaining business. As a leading provider of integrated, omnichannel payment solutions, Qualpay knew it needed an experienced expert to efficiently assess and validate its PCI DSS efforts while protecting the security of its payment platform.

CHALLENGE

Qualpay needed to achieve PCI compliance and ensure its cloud-based payment platform was secure. However, taking a security-first approach couldn't put its deadline at risk or overburden internal resources.

After its previous Qualified Security Assessor (QSA) firm replaced personnel mid-engagement and travel expenses grew too high, Qualpay started looking for a QSA firm with cloud expertise that would assign a senior-level assessor for the entire engagement and would provide support as its infrastructure and environment evolved.

"Our previous vendor was based in Atlanta, which meant travel expenses for on-site visits were quite high," explained Qualpay's CIO. "During our short engagement with that vendor, our original assessor left the company, leaving us in the care of a more junior member. The assessor we worked with knew PCI DSS requirements quite well, but clearly was inexperienced in performing client assessments and lacked necessary cloud knowledge."

Having partnered with Coalfire at a previous employer, Qualpay's CIO recommended the firm. "Coalfire's experience assessing companies using cloud infrastructure, such as Amazon Web Services (AWS), was one of the many reasons we chose Coalfire for our PCI DSS ROC."

APPROACH

As the go-to cybersecurity advisor, Coalfire leveraged its PASS+R methodology and deep technical expertise with PCI DSS and cloud services to assess and validate Qualpay's environment. Coalfire used this approach:

- **Pre-assessment and analysis:** Coalfire conducted a project charter call to determine timelines, resource allocations, and scheduling for the on-site assessment. The secure, powerful CoalfireOne^{SM} platform was used to gather, retain, and review evidence in accordance with PCI DSS standards. Qualpay's CIO and his team uploaded high-level system and business information, allowing Coalfire to examine the cardholder data environment in its entirety and efficiently move to the on-site phase.

- **Sampling and testing:** Coalfire performed a comprehensive on-site assessment at Qualpay's Bay Area headquarters, which included a physical walkthrough of the facility. Coalfire and Qualpay then conducted configuration checks on system components, including network devices and servers located within the payment processor's production facility hosted on AWS.
- **Remediation and submission:** Coalfire prepared a remediation action item list (RAIL) that detailed the data requests and remediation needed for a successful revalidation of PCI DSS compliance. By leveraging CoalfireOne's task assignments, dashboards, document management, and tracking features, the combined team efficiently and easily resolved the RAIL requirements. As a result, Coalfire validated Qualpay's remediation efforts and prepared a ROC.

How were AWS services a part of the solution?

According to Qualpay's CIO, "We used AWS services extensively to achieve compliance, often with much less effort than would have been required in a traditional data center infrastructure." The services used were:

- CloudWatch for monitoring API calls for suspicious activity
- Key Management Service (KMS) for managing encryption keys
- Amazon Virtual Private Cloud (VPC) for network isolation
- VPC flow logs for validating traffic within the VPC, which allows for identification of unexpected or suspicious activity
- Security groups for controlling access among resources within AWS
- AWS Inspector to determine whether resources used within AWS are configured correctly from a security perspective

RESULTS

With extensive PCI experience and a team of skilled assessors, Coalfire has served as Qualpay's partner, helping the company reduce risks and achieve compliance over the past three years. "Coalfire helped us remain PCI complaint in the cloud as we continued to innovate our payments platform and grow our business," explains Qualpay's CIO.

"We must remain PCI-compliant each year to continue doing business in our industry," said the CIO. "Achieving this compliance is a complex effort, requiring disparate types of evidence and policies. Coalfire does an excellent job by efficiently walking us through the requirements one by one so we're confident in the security of our platform and don't put our compliance validation at risk."

> *"I'm impressed by the breadth of knowledge that Coalfire assessors have shown regarding PCI DSS requirements and how they apply to our environment. The assessors know the requirements in detail and can readily speak to how implementation of particular processes and methodologies in our cloud-based environment satisfy those requirements."*
>
> – QUALPAY'S CIO

COALFIRE

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**