COALFIRE

CASE STUDY

Payce achieves PCI DSS compliance by utilizing the CoalfireOne℠ scanning platform and Coalfire Labs penetration testing services

AT A GLANCE

Payce, a B2B loyalty rewards and engagement company, wanted to ensure they were protecting consumer credit card data in a manner that complied with the Payment Card Industry Data Security Standard (PCI DSS). To become PCI compliant, Payce decided to conduct various technical testing to determine risks and impact of system vulnerabilities.

CHALLENGE

PCI DSS Requirement 11 entails quarterly vulnerability scanning and an annual penetration test. Understandably, vulnerability scans and penetration tests are thorough security practices for any business, regardless of the PCI DSS. Regular scanning of an environment will proactively identify vulnerabilities, and a penetration test will highlight the complexities of the network to find root causes and prescribe solutions.

Payce understood the severity of protecting consumer credit card information, but experienced difficulty understanding what to do to reach PCI DSS compliance in a technical testing manner. "Prior to obtaining our PCI attestation of compliance (AoSC), we outsourced the payment card information to our network partner, Affinity Merchant Solutions, since they were already PCI compliant," explained Jason Fruge, security data analyst at Payce. "At the same time, I took advantage of the opportunity to research what we needed to do to become PCI compliant."

After speaking with a few vendors, Payce selected Coalfire to provide technical testing services as a result of its cloud expertise and easy-to-use cloud-based scanning platform, CoalfireOne℠. "Affinity Solutions worked with Coalfire in the past and introduced us," said Fruge. "Through our discussions, we learned that Coalfire worked with many Microsoft Azure clients, and since we house our technology in the cloud, that capability alone differentiated Coalfire from the other competitors."

APPROACH

To meet PCI compliance, Payce and Coalfire started the technical testing using a two-phased approach, engaging the CoalfireOne Scanning Services team and Coalfire Labs to conduct PCI-related technical testing. The CoalfireOne Scanning Services team introduced Payce to CoalfireOne℠, Coalfire's cloud-based platform for accessing vulnerability scans and other Coalfire-related projects. Using the tool, Payce learned how to run scans to identify and manage risks and determine the impact of system vulnerabilities – without disrupting network operations – to quickly and easily comply with PCI requirements.

"Coalfire makes vulnerability scanning super simple," says Fruge. "Whether or not you are familiar with networking, the CoalfireOne Scanning platform is easy to use and user friendly."

In the second phase of the engagement, Coalfire Labs conducted internal and external network penetration tests in accordance with PCI DSS requirements. Coalfire had Payce identify and define systems with the goal of finding and safely exploiting vulnerabilities. Coalfire then evaluated attack vectors to determine the path of least resistance and leveraged manual techniques and public exploits to gain a foothold in the environment. "From start to finish, Coalfire's penetration test was very efficient," says Fruge.

RESULTS

Once the penetration tests were complete, Coalfire Labs delivered a custom, detailed report of all in-scope attack vectors to fully meet PCI Security Standards Council (PCI SSC) expectations. The report covered the objective of the test; methods used; and an executive summary of the findings, including severity ratings, vulnerabilities requiring remediation, and remediation suggestions. The penetration test report gave Payce a complete understanding of the exploitable vulnerabilities, as well as a clear, concise remediation strategy to strengthen their cybersecurity posture. Payce quickly remediated the findings, and as a result, in September 2018, received their PCI certification.

"As a result of the technical testing, Payce has significantly reduced business risk and expanded into markets that require PCI certification," stated Fruge. "Additionally, we decreased costs and dependence on vendors by internalizing functions previously outsourced to PCI-compliant vendors."

"Our overall experience with Coalfire was great. Both teams we worked with were knowledgeable about the cloud and truly helped us reduce our business risk."

- JASON FRUGE, SECURITY DATA ANALYST AT PAYCE

COALFIRE

About Coalfire

Coalfire is the 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. **Coalfire.com**

CS_Payce_051419