COALFIRE

CASE STUDY

Bank deploys “secure-by-design” microservices architecture in PCI-compliant hybrid cloud

AT A GLANCE

A Global 500 bank migrated legacy applications from in-house data centers to a hybrid cloud to save money and reduce the scope of its Payment Card Industry (PCI) environment. The bank engaged Coalfire to design and advise on a microservices architecture that nearly 300 different applications would use, taking advantage of PCI-compliant cloud services and reducing its in-scope environment by up to 50%.

CHALLENGE

Like many other enterprises, this bank was in the process of migrating as many applications as possible to the cloud to reduce operating expenses, simplify compliance, and improve its ability to support the business.

Many applications targeted for migration contained cardholder data (CHD), which means the bank has to continuously demonstrate compliance with the PCI Data Security Standard (PCI DSS). The chief technology officer and chief information security officer seized this once-in-a-generation opportunity to reduce PCI compliance scope while simultaneously capturing development efficiencies through the use of a microservices library that could be shared by multiple development teams and applications.

To make this vision a reality, the bank needed a partner with deep skills in cloud computing, software engineering, and the PCI DSS. According to the project’s executive sponsor, the bank solicited proposals from a number of firms and selected Coalfire for three reasons:

1. Compliance-in-the-cloud expertise, demonstrated by the fact that Coalfire assesses PCI compliance for several major cloud providers, including the leading cloud service providers.
2. Cloud computing skills, demonstrated by the deep experience of the assigned project team and references on similar and successful projects.
3. The collaborative, flexible work approach, which included both concrete deliverables as well as ad-hoc advisory and support services that brought much-needed skills to bear on the initiative upfront and during the project.

APPROACH

Coalfire's dedicated team of cyber engineers looked across the bank's hundreds of development teams and applications and thousands of developers to help create a sustainable, secure-by-design, PCI-ready assessment architecture program.

Coalfire started the engagement by discussing and examining the bank's architectural development process and its implementation status. Coalfire used this time with the organization to respond to design and implementation questions. Then, Coalfire provided guidance on constructing the architecture with the bank's cloud service provider, Amazon Web Services (AWS), effectively building the environment to be amendable to other IT or regulatory frameworks outside of PCI DSS.

Coalfire was instrumental in helping the bank craft an approach for using a single microservices "core" to securely process PCI requests from a variety of dissimilar payment applications. Use of end-to-end encryption (E2EE) technology delivered from this central "core" enabled many of these applications to operate from zones outside the CHD trusted zone, thereby reducing scope, cost, and system complexity.

As an added bonus, Coalfire assisted the bank in creating an AWS "playbook" to serve as a useful tool for future payment card projects. By using the design patterns and guidelines suggested in the playbook, new applications may be crafted to have similar security by design and take advantage of scope-reducing methodologies.

RESULTS

The project was a huge success and continues to create significant cost savings and efficiency improvements for the bank. Using this new microservices architecture, the bank has eliminated redundant development efforts and dramatically reduced the scope of its PCI environment. In addition, the bank's development team is now vastly more nimble and responsive to new requests from the business.

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 more than 17 years and has offices throughout the United States and Europe. **Coalfire.com**