COALFIRE

CASE STUDY

Global network and enterprise security company navigates FedRAMP with Coalfire's help

AT A GLANCE

A global network and enterprise security company that provides protection against cybersecurity breaches to tens of thousands of worldwide organizations chose Coalfire to perform a FedRAMP gap analysis. The client lacked in-house FedRAMP experience, and knew they needed an expert advisor to help them prepare for the rigors of the FedRAMP authorization process.

CHALLENGE

The client had developed a new SaaS offering that could potentially support many federal and Department of Defense (DoD) agencies. The client knew their SaaS solution needed to achieve FedRAMP authorization so it could be offered to the federal government, but they lacked the in-house expertise required to navigate the FedRAMP requirements and determine the best path forward based on their organizational goals and current and planned customer base.

"We had a manual process of control review and comparison between product management and DevOps that left many questions unanswered due to the lack of in-house experience," according to a product manager at the organization. "We compared three vendors in this field for about three months," explained the organization's VP of sales and federal and product management teams. "Ultimately, we selected Coalfire because they led the industry in FedRAMP certifications and had impressive client feedback." Once engaged, Coalfire immediately helped the client down the path to achieving FedRAMP authorization.

APPROACH

As the market leader in the FedRAMP program, Coalfire leveraged its experience and deep technical understanding of FedRAMP requirements to help the client develop a strategy for successfully achieving compliance with the FedRAMP control framework. Coalfire aligned four different organizations within the client – all with competing priorities and objectives – to establish an efficient, cost-effective roadmap to FedRAMP authorization. Coalfire's comprehensive capabilities were key to helping the client navigate the authorization process. Coalfire started the engagement by:

- Identifying and verifying the boundary for the client's SaaS offering. Coalfire's FedRAMP subject matter experts reviewed network diagrams and interviewed system stakeholders to identify key components, interconnections, and control responsibility, and then determine where federal data was processed, stored, or transmitted by the SaaS offering.
- Performing a detailed gap analysis of the SaaS offering against the FedRAMP moderate controls (NIST SP 800-53 r5) and DISA/DoD IL4. Coalfire reviewed the client's existing security documentation for their SaaS offering to determine if any content could be reused when developing the FedRAMP documentation package.
- Developing a comprehensive report with the necessary preparation steps for a FedRAMP assessment, security documentation and control review results, and technical recommendations for remediating non-compliant controls, emphasizing those controls required to achieve FedRAMP Ready status. Coalfire presented the findings to system stakeholders and executive management, and discussed recommended next steps to achieve FedRAMP compliance.

"The Coalfire team delivered quality feedback while demonstrating their expertise in a way that didn't make control review feel tedious and dry."

– PRODUCT MANAGER AT THE GLOBAL NETWORK AND ENTERPRISE SECURITY COMPANY

RESULTS

Through extensive FedRAMP experience and a team of highly skilled professionals, Coalfire helped the organization understand how their SaaS offering aligned with FedRAMP requirements.

"The review decreased the time needed to understand the FedRAMP requirements, and the walkthrough of the control implementation was invaluable, allowing us to save substantial workforce time," according to the product manager. Coalfire helped:

- Simplify the FedRAMP process.
- Identify key controls that were lacking.
- Identify solutions for control gaps.

CS_FEDRAMP_092717

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 more than 16 years and has offices throughout the United States and Europe. **Coalfire.com**