COALFIRE

CASE STUDY

Strategic security-by-design assures public trust for healthcare payments provider's cloud platform

AT A GLANCE

The healthcare payments industry sits in the crossfire between privacy and public trust. Under pressure in the cloud services space, a major FinTech company's executive team intended to position their technology platform ahead of the competition with Coalfire's Strategy+ program and HITRUST CSF® certification.

CHALLENGE

For decision-makers, the mere assumption of safe transactions doesn't cut it anymore, and traditional "security as usual" can't keep up with public demand for operational assurance. With accelerated cybersecurity exposure across expanding attack surfaces, healthcare providers can't easily distinguish between competing technology platforms' value propositions regarding cybersecurity.

Compelled by the increasing number of breaches and negative headlines within the healthcare industry, the company re-evaluated their cyber strategy and looked for ways to elevate their security posture in a thoughtful, strategic way amidst an aggressive M&A strategy.

Moving to the cloud and gaining HITRUST certification were identified as key initiatives for their product. Leadership agreed they needed a way to measure and apply key performance indicators (KPIs) to deliver a more sustainable and adaptable security program.

Protecting the privacy and security of patient data is at the heart of everything we do. Coalfire's Strategy+ gives a higher level of confidence to customers who rely on us to keep sensitive information safe, and of course, HITRUST certification is the gold standard."

– CTO AT THE HEALTHCARE PAYMENTS PROVIDER

APPROACH

Based on Coalfire's experience advising and assessing the top six major cloud providers, the organization determined Coalfire was the right partner to lead them on their journey to a secure cloud, meaningful industry certification, and a long-term cybersecurity strategy.

To ensure a secure migration to the cloud, Coalfire and the client's IT team used the Strategy+ methodology to establish a clear line of sight between the platform's security capabilities and its most critical business outcomes.

Mission-critical considerations – strategy, financials, innovation, regulations, competition, and risk appetite – guided the security program's restructuring. Coalfire's Strategy+ team evaluated the maturity and effectiveness of 12 inclusive domains across three strategic dimensions: business alignment, performance management, and controls discipline. From there, Coalfire modeled the cybersecurity program strategy in four phases:

1. **Define** business context considerations that drive success.
2. **Align** program to business goals and objectives.
3. **Operationalize** cyber plan into a tactical roadmap.
4. **Measure** cyber performance improvements against business objectives.

RESULTS

The company secured their move to the public cloud by integrating security and compliance into the initial design, which will enable future application rollouts into an already secure and compliant environment. The Strategy+ approach positions the cybersecurity program to deliver these additional benefits:

- New revenue streams through innovation
- Strategic risk decisions
- Security as a market differentiator
- Integrated security and resilience

The engagement bridged the gap between M&A disruption and the mature, sustainable security program required to run a unified payments processing platform in the cloud. Leadership's key measurement goals were achieved by:

- Combining compliance and a holistic security program to put a public face on ePHI assurance.
- Using HITRUST and Strategy+ as differentiators within a highly competitive cloud payments environment.
- Achieving security-by-design management objectives.

Stakeholders expect the revenue cycle management platform to become industry standard, but with rising public concerns about privacy, this goal could not be achieved without aligning security and making it part of the company's DNA.

By designing security into platform processes and enterprise operations, every employee can now articulate consistent cyber messaging into RFPs and conversations with customers, prospects, and stakeholders. Even non-technical officers and directors understand and value the company's risk resource allocations and the measurable returns on those investments.

Before partnering with Coalfire, the client was at a crossroads. After a risk assessment and gap analysis, designing security into the cultural fabric became priority. Adherence to regulatory frameworks (SOC 2 Type 2, PCI DSS, and HITRUST) added layers of validation and showcased their commitment to meeting regulatory requirements, managing risk, and protecting sensitive information.

Today, the leadership team maintains dashboard oversight of security posture and controls, with metrics on threat and vulnerability management, remediation performance, provider satisfaction, and patient engagement with the brand.

"This wasn't a laundry-list security program or an exercise in check-the-box compliance. It was a three-dimensional cultural shift, integrating business alignment, performance management, and controls discipline."

– JOHN HELLICKSON, CYBER EXECUTIVE ADVISOR, COALFIRE

COALFIRE

About Coalfire

Leading cloud infrastructure providers, SaaS providers, and enterprises turn to Coalfire for help solving their toughest cybersecurity problems. Through the combination of extensive cloud expertise, technology, and innovative and holistic approaches, Coalfire empowers clients to achieve their business objectives, use security and compliance to their advantage, and fuel their continued success. Coalfire has been a cybersecurity thought leader for 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**

Copyright © 2021 Coalfire. All rights reserved. All trademarks are the property of their respective owners.

CS_AHCpayments_072921