RunSignup

How RunSignup Goes Beyond PCI Compliance with Multi-layer Security

Defense-in-Depth for Payment Security with the VGS Vault

"Small to mid-sized companies can offload some (or all) of their PCI compliance burden by partnering with VGS."

Bruce Kratz,
VP of Development

Background

RunSignup is a swiftly growing company that specializes in developing software for endurance races and ticket events. Their suite of tools covers everything from registration and fundraising to marketing, website development, and business analytics. As a Certified PCI Level 1 Payments Facilitator, RunSignup understands the challenges and risks of security and compliance for sensitive data. They sought an extensible platform built by information security experts and supported by clear documentation to strengthen their security posture and compliance architecture, while simultaneously mitigating myriad threats from hackers and data thieves.

"Companies underestimate the effort it takes to have good security infrastructure. Becoming PCI-certified on your own is a very tall order."

Bruce Kratz, VP of Development at RunSignup

Challenge

RunSignup had already implemented security measures to protect sensitive payment and identity data. However, they recognized the need for a multi-layer approach to further enhance their security posture. They wanted a vault service platform that could process encrypted data streams, including their already encrypted credit card numbers, and seamlessly store this data and retrieve it for later use without ever exposing the original sensitive data. Additionally, they were seeking an easy-to-implement solution that their development team could quickly integrate while maintaining the highest level of security.

Solution

RunSignup discovered a powerful tool in VGS, a robust security and compliance platform that offered an API capable of handling streams of encrypted credit card data. With VGS, RunSignup could store encrypted information in a secure environment, keeping customer data safe from attackers. Payment data is stored separately from user profiles, providing an additional layer of security. Using the VGS API, RunSignup replaced any type of information, including encrypted data streams, with non-relational tokens to maintain the highest level of security. When making the decision of which vault provider to choose, RunSignup appreciated VGS's clear documentation and built-in dashboard. The platform's impressive financial backing from Goldman Sachs, as well as strategic partnership with VISA, further boosted their confidence in the tool.

Result

"Ultimately, the business value is in lowering the risk of exposing sensitive data."

Bruce Kratz, VP of Development at RunSignup

Partnering with VGS has provided several benefits for RunSignup. The VGS platform secures data at rest and in motion, and by partnering with VGS, RunSignup increased its security and privacy while reducing its risk and liability. RunSignup also accelerated its compliance posture toward PCI-DSS, CCPA, GDPR, and more. By adding in VGS's tokenization of encrypted card data, RunSignup ensures the maximum security, flexibility, and portability of sensitive data.

VERY GOOD SECURITY

✉ contact@verygoodsecurity.com

🌐 verygoodsecurity.com