Signal Sciences

Defending Remitly with Signal Sciences

CHALLENGE

Remitly enables immigrant communities to send and receive money across borders more simply and at a lower cost. They needed a technology that could satisfy PCI requirements and protect customers' valuable and sensitive transactions through its mobile application.

Remitly is the largest independent digital remittance company headquartered in the United States, transferring over $5 billion in annualized volume from its customers in the United States, United Kingdom, Canada, and Australia to loved ones throughout the world. The company set out to protect its proprietary global transfer network with a web application firewall (WAF) solution that would not only satisfy PCI requirements, but also provide protection against new and emerging attack types, without impacting performance.

Remitly deals with irregular traffic patterns. On one occasion, they observed spike in account transfers all happening from a small network segment on the Pacific coastline of South America. They had to determine if traffic indicated an attack or valid requests, and do so in real time. Allowing the traffic carried the risk that the transactions were malicious, requiring Remitly to reimburse the cost of the fraudulent transfers. A traditional WAF would have no way of distinguishing this traffic, leaving customers frustrated if they chose to blacklist the IP.

> “Protecting customer information to ensure its safety and security is our number one priority. Signal Sciences checked a bunch of boxes for us to achieve this, but we were impressed particularly with their ability to enforce flexible requirements for our business as opposed to old school regex-based enforcement.”
>
> **Kevin Hanaford**, Senior Manager of Security & IT

SOLUTION

With Signal Sciences in place, the security team is able to instrument and defend their web applications and APIs with a solution that doesn't create false positives or block their customers' traffic.

Allow good traffic and block malicious requests coming from the same network

Because Remitly customers are located around the globe—on land and at sea—they needed a solution that was able to only block malicious traffic and allow good traffic through from the same network range or IP. The spike in activity on the Pacific coastline turned out to be requests from their customers who earn their living out at sea. They would come into port and transfer money, all from a small IP network segment. Signal Sciences provided the needed visibility to help the team determine these were legitimate requests, and not an attack.

"Other products would block this traffic—throwing out the good with the bad—or let everything through and therefore subject us to potentially damaging attack traffic. We've noticed that because of the way Signal Sciences responds in a thresholding way, we have far fewer instances of throwing out the good with the bad than we used to," Hanaford explains.

Achieve PCI compliance and more

Remitly knew that they had to have a WAF for PCI compliance, but they wanted to protect the entire site and not just the portion of the application that deals with credit cards. Other solutions required hiring extra headcount and an exorbitant number of hours to manage—Hanaford estimated 30-50% of a security analyst's time, which would grow over time with more signatures and exceptions as the business expands. Instead they needed something that just worked. Signal Sciences Power Rules allowed them to easily add in instrumentation and defense where they needed it without the complex regex rules found in other products.

Flexible across their public and private web applications and API endpoints

Remitly operates public facing endpoints and applications for their customers as well as private endpoints that are for internal employees. Remitly needed to protect both, and couldn't be limited by architectural designs that required chokepoints in networks. Signal Sciences provides a flexible architecture that allows them to get running in production and tie into their proxy layers for both private and public networks with ease.

> " Signal Sciences in three words: Easy. Powerful. Magic. I would absolutely recommend Signal Sciences to other companies looking for a WAF solution that does a great job protecting environments and doesn't require a ton of time and effort to tune and manage. It gets things right the first time. "
>
> **Kevin Hanaford**, Senior Manager of Security & IT