

# Eventbrite: Strengthen Security Posture and PCI Compliance

## CHALLENGE

Eventbrite had lost confidence in their security vulnerability scanner's ability to identify malicious code or backdoors attackers could leverage, and needed a comprehensive solution to protect their global sites and M&A properties.

Eventbrite was facing two key challenges during a critical time of the business. To fulfill PCI 6.6 requirements they had been using a variety of security vulnerability assessment tools (scanners) to protect their applications against the OWASP Top 10. But even with ongoing configuration, these scanners were providing spotty coverage and failing to spot inherent security weaknesses in the codebase of their global properties.

Additionally, Eventbrite was building their security strategy for securing acquired properties. They needed a vendor that could install easily, provide security coverage quickly, and provide effective web layer security for any future merger or acquisition activity with a single solution.

Eventbrite had never utilized a web application firewall (WAF) as part of their security stack: the team was hesitant about the performance, tuning, and maintenance issues that are common with legacy WAFs. But they reached a breaking point with vulnerability scanners and needed a vendor that would restore confidence in their security posture.



“ Signal Sciences is a simple but effective solution that required minimal upfront configurations and next to zero on-going babysitting. ”

**Paul Pieralde**, Director of Security



## SOLUTION

Signal Sciences provides complete web application layer attack coverage for Eventbrite's global properties with minimal tuning and maintenance.

After deploying Signal Sciences, Eventbrite experienced how our next-gen WAF surpasses what legacy WAF vendors and scanners provide. Not only does our technology block SQL Injection, XSS, and other attacks against their six global properties, but does so before these malicious requests reached Eventbrite's application servers, inherently freeing up resources for legitimate traffic.

### **Flexible Installation and Customizable Deployment**

Eventbrite needed a solution that would work for their architecture. They had NGNIX and HAProxy load balancers routing to EC2 servers running multiple apps and containers, so they wanted custom deployments without painful workarounds. "Signal Sciences provides several installation options, allowing us the flexibility to install where it makes the most sense for our platforms," said Peralde.

### **Fast Time-To-Value with Minimal Maintenance**

Although Eventbrite had used multiple scanners over the years, they were still seeing attacks coming through. During the Signal Sciences pilot, Eventbrite went from "monitoring" to "blocking" mode in less than 30 days. They experienced firsthand how easy it was to set up and use, and became a customer quickly after. Peralde noted, "It's a simple solution that required minimal upfront configurations and next to zero on-going babysitting."

### **Restored Trust and Peace of Mind**

Eventbrite's unreliable vulnerability scanners created an untenable working environment for their security team, who needed 100% confidence to operate effectively. Signal Sciences dashboard and alerting features gave the security team complete visibility into what was happening across their applications and APIs.

The Eventbrite logo is displayed in a bold, lowercase, orange sans-serif font.

“ Signal Sciences provides several installation options, allowing us the flexibility to install where it makes the most sense for our platforms. ”

**Paul Peralde**, Director of Security