Signal Sciences

PCI Compliance FAQ

What Is PCI DSS Compliance?

According to the American Bankers Association, it is estimated that there are 10,000 payment card transactions made every second around the world. With this kind of transaction volume and with cyber criminals constantly finding new ways to acquire sensitive cardholder data, payment card security breaches are a growing concern for many organizations. In order to protect cardholder data, the Payment Card Industry (PCI) Security Standards Council (SSC) created the Data Security Standard (DSS). PCI-DSS compliance is required by all major credit card brands for any organization that processes payment cards or transfers and stores payment card data.

As organizations take advantage of wireless technology to improve operations and gain a competitive advantage, PCI DSS requires organizations to extend the same level of security from the wired network to the wireless network and provides specific guidelines as to how to protect point-of-sale data over the wireless network.

Why are web application firewalls important in PCI-DSS?

Web application firewalls filter and block non-essential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured. This can be achieved through a combination of technology and process. Process-based solutions must have mechanisms that facilitate timely responses to alerts in order to meet the intent of this requirement, which is to prevent attacks.

PCI-DSS requirement 6.6 requires either doing a web application vulnerability assessment on every change to the application or by using a web application firewall. Most organizations choose to run a web application firewall which is why PCI-DSS 6.6 is often referred to as the WAF requirement.

Does Signal Sciences Next-Generation WAF meet PCI-DSS 6.6 and fulfill the need for a web application firewall?

Yes! Signal Sciences provides a solution that can be used fulfill PCI requirement 6.6 as a control for a Web Application Firewall. Not only does Signal Sciences meet PCI-DSS 6.6, we have helped many customers complete a full PCI-DSS audit using our product to meet PCI-DSS 6.6.

How does Signal Sciences meet the PCI Requirement 6.6?

Signal Sciences ensures that public-facing web applications are protected against known attacks. This includes web-based attacks like XSS and SQLi but Signal Sciences goes above and beyond PCI requirements and helps prevent business logic attacks and account takeover attacks.

Do you have any compliance standards met on your own platform?

Yes. Signal Sciences is SOC 2 Type 2 compliant.

Request a demo

Request a demo and we'll get you set up with one of our experts.

The World's Top Companies Trust Signal Sciences

DOORDASH

Glossier.

DUO

vimeo

tenable®

SHINOLA
DETROIT

UNDER ARMOUR

one medical

Any App

Cloud, Containers, PaaS, and Serverless

Web Servers and Languages

Gateways and Proxies

Any Attack

OWASP Top 10

Application DoS

Brute force attacks

+ MORE

Any DevOps Toolchain

Slack

Datadog

Webhooks

Splunk

SIEM/SOC tools via APIs

+ MORE