All-in-One Website Security and PCI Compliance

Protect your site from bots, fake users, and unauthorized transactions — all while making your website faster and ensuring PCI compliance.

PCI

Background /

One important requirement of the Payment Card Industry Data Security Standard (PCI-DSS) is Requirement 6.6. Established in 2008, this requirement originally aimed to address common threats to cardholder data by specifying how to inspect web application access from untrusted environments. At that time, Requirement 6.6 stated that installing a “Web Application Firewall” (WAF) satisfied the requirement to inspect web application traffic.

In 2015, Requirement 6.6 stopped prescribing the use of a WAF and instead specified the use of an “automated technical solution” to ensure adequate inspection of traffic. In doing so, PCI-DSS demonstrated that other “automated solutions” could be adequate and even superior to WAFs in certain capabilities of protecting public facing assets.

Requirement 6.6 now reads as follows:

“For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.”

Source | **PCI - DSS v. 3.2.1**

Satisfaction of Requirement 6.6 /

From the above options, the majority of organizations select the latter as their method of defense. This has generated a significant growth in the technical landscape of web application protection over the past few years. As an advanced web application defense system, Shape Connect provides an inline security device and service that protects web and mobile properties, while meeting all facets of PCI Requirement 6.6 below. Shape Connect is a great addition to other security mechanisms filtering within applications created by developers as well as filtering within the web framework used by developers.

- ✓ Prevents and Detects Web-Based Attacks
- ✓ Sits in Front of Public-Facing Web Applications
- ✓ Configured to Block Web-Based Attacks
- ✓ Actively Running and Up to Date
- ✓ Generates Audit Logs
- ✓ Generates Attack Alerts and Immediate Investigation

Advantages of Shape Connect /

Utilizing a defense strategy differing from those provided by traditional WAFs, Shape Connect is a Level 1 PCI - Certified security-as-a-service solution that actively defends against automated cyber-attacks and vulnerabilities on web applications, including attacks that may evade other legacy security solutions such as WAFs, IPS, and DDoS mitigation tools. Unlike legacy tools whose defense against known application vulnerabilities is often signature based and requires constant manual policy updates, Shape Connect provides defense through an active protection policy that gathers and analyzes telemetry data of web traffic, allowing deeper inspection of malicious activity and adaptive protection.

This customizable protection policy is managed by Shape research experts that arduously study the behavior patterns of malicious activity and threat actors. As more research is completed, the protection policy grows smarter, updates are implemented with faster cycle times, and policy effectiveness is continuously improved in its defense of web properties. This continuous improvement allows Shape Connect to surpass traditional web application defense solutions by providing protections against known AND unknown malicious activity. Additionally, the solution continually analyzes real-time requests from the application at run time instead of utilizing pre-configured rulesets.

OWASP Top 10 /

Shape Connect not only addresses PCI-DSS Requirement 6.6, but also mitigates application exposure to common web application vulnerabilities listed in the Open Web Application Security Project Top 10 vulnerabilities including the following:

- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery
- Broken Authentication

Source | **OWASP Top 10**

OWASP Automated Threats /

The advancement of defense solutions has also persisted the advancement of automated threats. Web applications are subjected to unwanted automated usage daily. Often this traffic attempts to misuse valid functionality, rather than exploit unmitigated vulnerabilities. Most of these problems regularly seen by web application owners are not listed in any OWASP Top 10 or in any other top issue list or dictionary. The OWASP Automated Threats to Web Applications Project completed a review of available security knowledge to identify, name, and classify these ever-emerging automated threats. Resultant from this project was the **OWASP Automated Threat Handbook** including a listing of known threat events.

Through the innovative behavioral analysis of incoming web traffic and continuous expansion of our knowledge base, the Shape Connect solution provides protections against these automated threat scenarios as they continue to evolve. Common automated attacks for which Shape Connect actively protects against include:

- Credential Stuffing
- Credential Cracking
- Account Aggregation
- Carding
- Scraping
- Card Cracking
- Account Creation
- Vulnerability Scanning

Contact Shape /

If you have any additional questions about the Shape Connect solution or its use in fulfilling Requirement 6.6 of PCI-DSS, feel free to contact Shape via the contact us link available on our website.