Codesealer

WHITE PAPER

PCI DSS V4.0

HOW CODESEALER HELPS STREAMLINE REGULATORY COMPLIANCE

Adhering to new PCI DSS standards for web application security can be complex. Codesealer simplifies this challenge by providing a clear solution for meeting new PCI DSS requirements and enhancing web application security.

BROUGHT TO YOU BY CODESEALER

www.codesealer.com

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Although PCI DSS version 4.0 was released in April 2022, meeting its updated requirements and guidelines—which aim to enhance payment security, address emerging threats, and provide greater flexibility for achieving compliance—presents significant challenges for organizations.

In today's digital landscape, the security of web applications is paramount. Traditional web security methods often focus solely on threat detection and blocking, leaving vulnerabilities exposed. Enter Codesealer, a leading cybersecurity solution.

Codesealer is unique in the industry for its ability to encrypt APIs and JavaScript in transit and secure it at runtime, aligning with PCI DSS requirements for protecting payment card data. This innovative approach not only strengthens defense mechanisms but also reduces the attack surface, enhancing security.

Codesealer's technology surpasses traditional security measures by encrypting sensitive data and application logic even in the client environment. This proactive strategy helps conceal vulnerabilities and mitigate risks before they can be exploited, offering unparalleled protection against a wide range of cyber threats.

PCI DSS 6.4: Public-facing web applications are protected against attacks

Public-facing web applications are those accessible to the general public, not just for internal use. These applications are prime targets for attackers, and inadequately coded web applications offer an easy entry point for attackers to access sensitive data and systems.

What's addressed?

Requirements 6.4

6.4.1: Public-facing web applications are protected against ongoing threats and known attacks with automated solutions that detect, prevent, and log web-based attacks, ensuring real-time alerts or blocking.
6.4.2: An automated, real-time solution detects and prevents web-based attacks on public-facing applications, ensuring active monitoring, logging, and immediate alert investigation.
6.4.3: Payment page scripts are managed with authorization, integrity checks, and an inventory with justifications for each script.

Codesealer ensures that only scripts originating from the company's web server can run within the browser application. This approach leverages the authorization, ownership, and change management practices the company has implemented to protect its production web application. Additionally, the integrity of each script is maintained through tamperproof end-to-end encryption, from the server-side to the secured execution of the script.

Codesealer protects your public-facing web applications against formjacking, data skimming, and Magecart attacks by extending encryption into the client. Your source code and APIs are fully encrypted, leaving attackers no way to intervene with the client-side scripts. Codesealer also provides a Web Application Firewall (WAF) to protect your web applications, which functions in addition to Codesealer's other groundbreaking web application protection techniques. The payment page upholds all integrity under full protection, out of attackers' sight. Inventory management is an upcoming feature.

new

PCI DSS 11.6: Unauthorized changes on payment pages are detected and responded to

Many web pages now rely on assembling objects, including active content like JavaScript, from various internet sources. Additionally, content management and tag management systems define much of this content, making it difficult to monitor with traditional change detection methods. As a result, the most effective place to detect changes or indicators of malicious activity is within the consumer's browser, as the page is constructed and all JavaScript is interpreted.

What’s addressed?

Requirement **11.6.1**

- Alert personnel to any unauthorized modifications (including signs of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as they are received by the consumer's browser.
- Evaluate the received HTTP headers and payment pages for any potential tampering.

Codesealer prevents modifications to HTTP headers and all payment page contents by sealing them in the client's browser. Built-in mechanisms in the handshake and execution flow of the bootloader detect tampering attempts. Codesealer can also be configured to alert on all attempts to tamper with or change the Codesealer-protected scripts, ensuring that only scripts originating from the authorized web server are executed.

PCI DSS 5: Protect All Systems and Networks from Malicious Software

Newly discovered vulnerabilities in previously secure systems are constantly being targeted by attacks. Without a regularly updated anti-malware solution, new types of malware can infiltrate systems, disrupt networks, or compromise data.

What's addressed?

Requirement **5.2.2**

- Alert personnel to any unauthorized modifications (including signs of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as they are received by the consumer's browser.
- Evaluate the received HTTP headers and payment pages for any potential tampering.

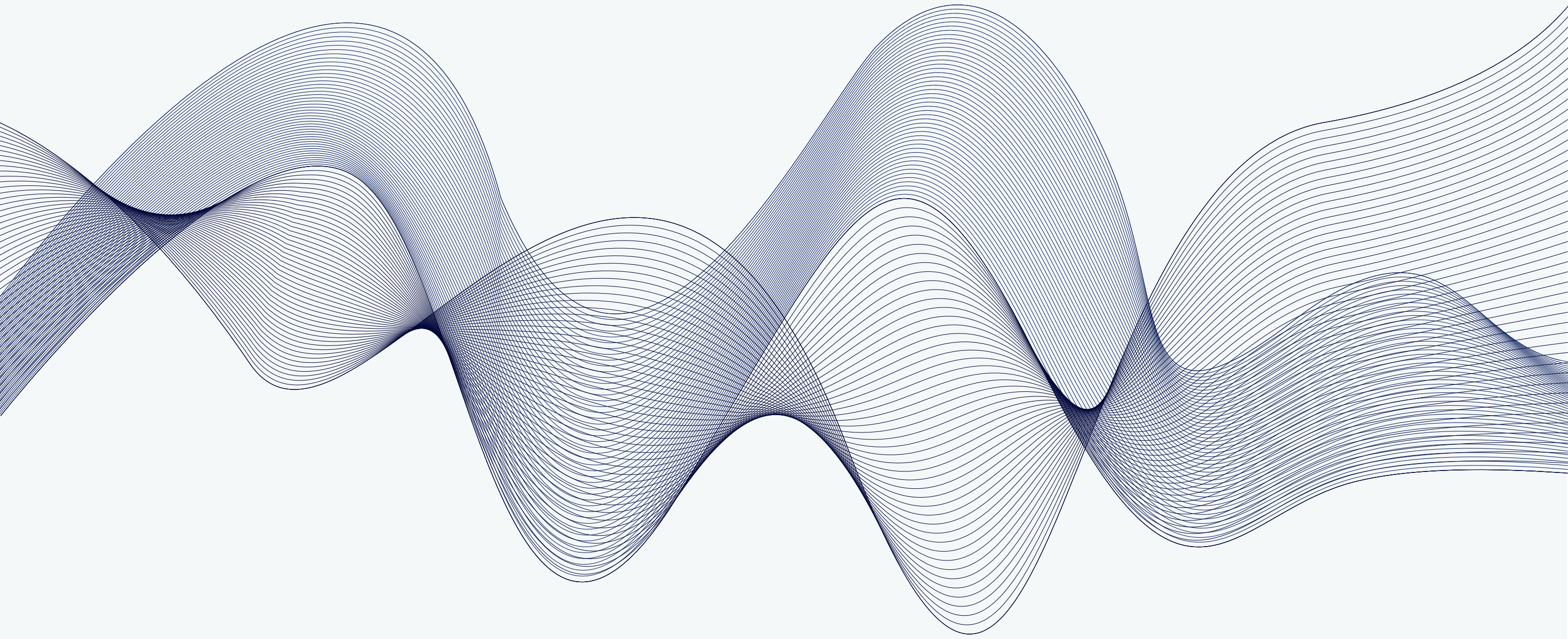
Codesealer protects browser-based applications by blocking malware and disrupting its behavior on web pages. Many types of malware work by injecting malicious JavaScript into web pages. Advanced attacks, such as bypassing signatures, changing payment data elements, or hijacking links, rely on interacting with existing JavaScript to make subtle changes that trick servers into accepting malicious actions as legitimate.

Codesealer safeguards all intentional JavaScript through encryption and controlled initiation while detecting and blocking unwanted additions and injections. This results in controlled responses, from blocking the attack to sending alerts based on administrator settings. By doing so, Codesealer prevents any malware, even unknown types, from successfully attacking the web page.

Ready to secure your PCI DSS compliance ?

Reach out to our team today to learn more about Codesealer's API protection features and discover how we can fortify your web applications against evolving cyber threats. It's extremely easy (and free) to run a test with us on any existing URL, ensuring that you can see the benefits without any time-consuming setup. Schedule a consultation or request a demo to witness the transformative impact of Codesealer firsthand.

info@codesealer.com
Codesealer A/S
Njalsgade 76, 3rd Floor
2300 Copenhagen S
CVR 39228920



Codesealer

www.codesealer.com