



WEBDEFEND®: YOUR PCI COMPLIANCE SOLUTION

WHAT IS THE PCI DSS?

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of security requirements established by the leading payment brands. These requirements are designed to protect sensitive account data such as credit card numbers, customer names and contact information.

MUST I COMPLY?

Any organization that “stores, processes or transmits” credit, debit or other payment card information must comply with the PCI DSS.

WHY SHOULD I BE CONCERNED?

Non-compliance with the standard may result in data breaches, fines and fees, lawsuits, federal oversight and lost customers.

Breach Security’s next-generation WebDefend web application firewall appliance offers the industry’s most accurate attack detection and prevention, as well as the best data leakage protection for payment card information. Praised in reviews by *SC Magazine* and *Information Security* magazine for its targeted PCI features, WebDefend provides real-time, continuous web application integrity, security and compliance.

WEBDEFEND FACILITATES COMPLIANCE WITH 10 OF 12 PCI DSS REQUIREMENTS

Requirement 2

Blocks known vulnerabilities through signatures developed and updated by Breach Security Labs.

Requirement 3

Stops all cardholder data, including magnetic stripe data, from leaking from web applications.

Requirement 4

Ensures SSL strength when sensitive information is legitimately transmitted through web applications and discovers hidden attacks in SSL traffic without compromising performance.

Requirement 5

Detects web application access by and upload of Trojan horses and backdoor viruses.

Requirement 6

Learns each protected application and adapts its protection as changes to the application are released. Identifies security defects—such as unvalidated input fields, insecure configuration, weak cryptography and poor session management—and acts as a “virtual patch,” preventing them from exploit.

Requirement 7

Permits organizations to apply appropriate policies to different sites to enforce unique settings.

Requirement 8

Ensures that unique IDs and passwords are assigned and used correctly by the application.

Requirement 10

Includes PCI-specific reports which show details of payment card data use for audit purposes as well as the system’s overall level of compliance.

Requirement 11

Assesses inbound and outbound application traffic to detect security and application integrity issues, including improper error messages, leakage of system and user information, missing or broken links and other coding flaws which can lead to lost revenues or negative user experiences.

Requirement 12

Ensures protected applications are in compliance with the PCI DSS and enables policy-setting for web application protection across the organization.

© 2009 Breach Security, Inc. All rights reserved. Breach Security is a trademark and WebDefend is a registered trademark of Breach Security, Inc. All other brand, product and service names are the trademarks, registered trademarks or service marks of their respective owners. 0808

ABOUT BREACH SECURITY™

Breach Security, Inc. is the leading provider of real-time, continuous web application integrity, security and compliance that protects sensitive web-based information. Breach Security’s products protect web applications from hacking attacks and data leakage and ensure applications operate as intended. The company’s products are trusted by thousands of organizations around the world, including leaders in finance, healthcare, ecommerce, travel and government.

Contact Us Today for a Complimentary PCI Web Application Security Assessment

(866) 205-7032 (toll-free)

(760) 268-1924

info@breach.com

www.breach.com/pci-webdefend