



**ICSA Labs
Product Capability Assurance Report
Payment Card Industry
Data Security Standard v.2.0**

Imperva, Inc.

**SecureSphere Web Application Firewall X Series
7.5.0.7564**

November 19, 2010

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

PCIW-IMPERVAINC-2010-1119-01



**Imperva SecureSphere Web Application Firewall X Series
Product Capability Assurance Report**

Table of Contents

Executive Summary 1
PCI DSS and ICSCA Labs Testing 1
Product Description 1
 Hardware 2
 Software 2
ICSCA Labs Certifications 2
Summary of Findings 2
Testing Information 5
 Lab Report Date 5
 Test Location 5
 Product Developer’s Headquarters 5

Executive Summary

The Payment Card Industry (PCI) Data Security Standard (DSS) was written by the payment card industry to help merchants worldwide to better safeguard cardholder data. Its requirements apply to merchant environments and any third-party service providers where cardholder data is processed, stored, or transmitted.

Merchants and service providers must comply with the PCI DSS standard. They are faced with purchasing and deploying computer and network security products that help them achieve and demonstrate compliance with PCI DSS requirements, or to develop and document appropriate compensating controls. Qualified Security Assessors (QSAs) likewise need assistance in understanding whether or not products in the cardholder data environment have the capacity to assist the merchant in achieving compliance with the PCI DSS.

This report helps both merchants and QSAs by identifying where a specific product or family of products has the capability to satisfy or help to satisfy one or more of the individual PCI DSS requirements. Armed with this information, merchants and QSAs can better determine where additional products or compensatory controls may be required.

PCI DSS and ICSA Labs Testing

The PCI DSS version 2.0, dated October 2010, is a set of 12 groups of requirements. These groups of requirements establish minimum security standards for merchant and service provider environments where sensitive payment cardholder data is processed, stored, or transmitted.

Within the 12 requirements there are mandates that merchants deploy several computer and network security components. There is a corresponding certification testing program at ICSA Labs for each of the five security components below which are mandated by the PCI DSS:

1. Firewalls (PCI DSS also refers to these as “network firewalls” or “perimeter firewalls”)
2. PC Firewalls (PCI DSS refers to these as “personal firewalls”)
3. Web Application Firewalls
4. Anti-virus Products
5. Network Intrusion Prevention Systems (IPS)

Beyond requiring that the security components above be present in the merchant environment, the PCI DSS imposes policy and configuration requirements as well. Policy requirements cannot be met by a product.

Statements of a product’s capability to satisfy individual PCI DSS requirements as made in this report are based on ICSA Labs’ knowledge of the product or product family. Product knowledge comes from successful certification testing in the program(s) identified in the *ICSA Labs Certifications* section below. The product may employ additional capabilities that could be relevant to PCI DSS, but these may not have been tested by ICSA Labs.

Product Description

This report is valid only for the product(s) and version specified below. The report makes no claims regarding previous or subsequent versions of this product or product family.

Hardware

Imperva, Inc. provided ICSA Labs with the following hardware listed below:

- SecureSphere X1000
- SecureSphere X2000
- SecureSphere X2500
- SecureSphere X4500
- SecureSphere X6500
-

Software

- Version 7.5.0.7564

ICSA Labs Certifications

The product or product family listed above is currently certified in the following ICSA Labs certification testing program(s):

- Web Application Firewall Testing & Certification Program

Details on ICSA Labs certification testing programs, including lists of certified products and certification testing reports are available on the ICSA Labs web site:

<http://www.icsalabs.com>

Summary of Findings

The PCI DSS is comprised of requirements that may be met by one or more products as well as requirements that are purely policy oriented (i.e., requirements to maintain a policy, often with specific required elements). Of those PCI DSS requirements that are product related, no single product can meet them all. However, a product can satisfy or help satisfy one or more of them. Only a subset of the product-related requirements were tested and reported on below.

Table 1 below lists the specific version 2.0 requirements which the product is capable of satisfying. PCI DSS 1.2 policy-only requirements and requirements the product cannot satisfy are omitted.

The “ID” identifies the requirement number as referenced from the PCI DSS version 2.0. A “Yes” in the “Compliant?” column indicates that based on knowledge gained through the course of ICSA Labs certification testing, the product is capable in whole or in part of satisfying the PCI DSS requirement in question. The “Notes” column includes any additional information that may be of interest

Paragraph Number	Text	Compliant	Note
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for webbased management and other non-console administrative access.	Y	

Imperva SecureSphere Web Application Firewall X Series Product Capability Assurance Report



Paragraph Number	Text	Compliant	Note
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Y	
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	Y	
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Y	
6.5.2	Buffer overflow		
6.5.3	Insecure cryptographic storage		
6.5.4	Insecure communications		
6.5.5	Improper error handling		
6.5.7	Cross-site scripting (XSS)	Y	
6.5.8	Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal	Y	
6.5.9	Cross-site request forgery (CSRF)	Y	
6.6	Installing a web-application firewall in front of public-facing web applications	Y	
7.2	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:		
7.2.1	Coverage of all system components	Y	
7.2.2	Assignment of privileges to individuals based on job classification and function	Y	
7.2.3	Default "deny-all" setting	Y	
8.1	Identify all users with a unique ID before allowing them to access system components or cardholder data.	Y	
8.5.15	If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	Y	
10.2.2	All actions taken by any individual with root or administrative privileges	Y	
10.2.3	Access to all audit trails	Y	
10.2.4	Invalid logical access attempts	Y	
10.2.5	Use of identification and authentication mechanisms	Y	

Imperva SecureSphere Web Application Firewall X Series Product Capability Assurance Report



Paragraph Number	Text	Compliant	Note
10.2.6	Initialization of the audit logs	Y	
10.2.7	Creation and deletion of system-level objects.	Y	
10.3	Record at least the following audit trail entries for all system components for each event:		
10.3.1	User identification	Y	
10.3.2	Type of event	Y	
10.3.3	Date and time	Y	
10.3.4	Success or failure indication	Y	
10.3.5	Origination of event	Y	
10.3.6	Identity or name of affected data, system component, or resource.	Y	
10.4	Synchronize all critical system clocks and times.	Y	
10.5.2	Protect audit trail files from unauthorized modifications	Y	

Testing Information

This report is issued by the authority of the Managing Director, ICSA Labs. Tests are done under normal operating conditions.

Lab Report Date

November 19, 2010

Please visit www.icsalabs.com for the most current information about this and other products.

Test Location

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050



Product Developer's Headquarters

Imperva, Inc.
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
United States



The certification test methods used to produce this report are accredited and meet the requirements of ISO/IEC 17025 as verified by the ANSI-ASQ National Accreditation Board/ACLASS. Refer to certificate and scope of accreditation number AT – 1423.

Copyright 2010 Cybertrust. All Rights Reserved. Testing reports shall not be reproduced except in full, without prior written approval of ICSA Labs.