

## Citrix Solutions for Complying with PCI-DSS

ENSURING PROTECTION OF WEB APPLICATIONS AND PRIVACY OF  
CARDHOLDER INFORMATION

---

## **Table of Contents**

<b>2</b>	<b>Overview</b>
2	A Tale of Abandonment, Missed Opportunities and Fraud
<b>2</b>	<b>Guarding Against Credit Card Fraud</b>
<b>3</b>	<b>Whom Does PCI-DSS Apply to?</b>
<b>3</b>	<b>What are the Elements of PCI-DSS?</b>
	<ul style="list-style-type: none"><li>• Build and Maintain a Secure Network</li><li>• Protect Cardholder Data</li><li>• Maintain a Vulnerability Management Program</li><li>• Implement Strong Access Control Measures</li><li>• Regularly Monitor and Test Networks</li><li>• Maintain an Information Security Policy</li></ul>
<b>4</b>	<b>Web Application Controls Specific to PCI-DSS</b>
<b>6</b>	<b>Recommendations</b>
<b>7</b>	<b>Citrix Solutions</b>

## Overview

The Payment Card Industry Data Security Standard (PCI-DSS) is a global standard governed by the major credit card companies. The standard comprises a set of directives for entities that handle credit cards, with the goal of reducing fraud. PCI-DSS presents the framework for protecting sensitive cardholder and authentication data, providing financial benefits to organizations that are in compliance.

Citrix Application Firewall™, along with other Citrix solutions, provide a strong platform for compliance with PCI-DSS application security requirements and overall protection of critical Web applications.

### **A TALE OF ABANDONMENT, MISSED OPPORTUNITIES AND FRAUD**

- 40% of shoppers have abandoned an online transaction due to concerns over credit card fraud. 32% of survey respondents would spend a greater percentage of their holiday shopping budget online if they had greater trust in the retailer (buySAFE, 2006).
- A recent Forrester Research report predicted online holiday spending would rise by 23% in 2006.
- One in three (30%) of online adults, however, said security fears compelled them to shop less online or not at all during the 2006 holiday season. One in five (20%) online adults said Internet security had them “very concerned” or “extremely concerned” during the 2006 holiday season. Those concerns ran highest among those 55 and older (31% said they were “very” or “extremely” concerned) — (Business Software Alliance (BSA), 2006).
- More than half of all Australians say their top security fears are about people accessing or misusing their personal details as well as credit/debit card fraud. (Australian Associated Press, 2006).
- Companies spent nearly \$5 million on average, and 30% more, in 2006 than in 2005 to recover when corporate data was lost or stolen, according to a new study from the Poneman Institute.
- Gartner Group (2006) predicted online retailers would lose nearly \$500 million in sales during the 2006 holiday shopping season due to fraud and suspect transactions.

Fear of credit card fraud keeps consumers from utilizing Web applications for financial transactions and results in reduced sales for retailers. Lack of trust in the Web requires direct human interaction for all sales, resulting in higher transaction costs. Fraud-related costs are a significant drag on profitability and productivity for financial institutions. Any way you look at it, credit card fraud erodes customer confidence, increases costs and diminishes the benefits of ubiquitous e-commerce. It's a problem recognized by the credit card companies and policed by auditors through PCI-DSS v1.1.

## Guarding Against Credit Card Fraud

On September 7, 2006, the leading global Payment Card Industry (PCI) vendors officially joined together to form the PCI Security Standards Council. This council, comprised of American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, is focused on defining security requirements that protect sensitive cardholder data.

---

First introduced in January 2005, the PCI-DSS provides a single global security standard that provides specific technical guidance for protecting cardholder interests. The first initiative of the new PCI Security Standards Council was to update this standard.

Three new significant points have been addressed in PCI-DSS v1.1:

- The unification of PCI vendors to develop a single set of global requirements
- Specific recognition of the unique security needs of Web applications
- Increased requirements for hosting providers

This whitepaper clarifies the newly mandated PCI-DSS requirements for protecting sensitive cardholder data delivered through Web applications.

## Whom does PCI-DSS apply to?

The PCI-DSS standard is aimed at online merchants, financial institutions, credit and debit card processors, card companies and endpoint POS terminals. According to the v1.1 specification:

*“PCI-DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI-DSS requirements do not apply.”* If your organization directly interacts with, or supports, online credit card transactions via a Web-based application or interface, PCI requirements must be complied with.

## What are the Elements of PCI-DSS?

The PCI-DSS defines 12 high-level requirements in the following six categories:

### **BUILD AND MAINTAIN A SECURE NETWORK**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

### **PROTECT CARDHOLDER DATA**

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

### **MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM**

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

**IMPLEMENT STRONG ACCESS CONTROL MEASURES**

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

**REGULARLY MONITOR AND TEST NETWORKS**

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

**MAINTAIN AN INFORMATION SECURITY POLICY**

Requirement 12: Maintain a policy that addresses information security

PCI-DSS presents the framework and standard for protecting cardholder and sensitive authentication data with the ultimate goal of limiting access, controlling fraud and providing financial benefits to organizations that are in compliance.

## Web Application Controls Specific to PCI-DSS

To support the specific interests and unique risks associated with Web applications, PCI-DSS v1.1 expands on existing requirements and introduces new requirements. The following considerations highlight several of the requirements and proposed controls specific to web application environments.

*1.1.6 – Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN).*

The PCI-DSS mandates that organizations build and maintain a secure network by using core Web protocols and VPN technologies to deliver and secure cardholder data across networks. Citrix Application Firewall and Citrix® NetScaler® appliances restrict access to applications and data by allowing only the use of approved protocols and methods.

*3.3 – Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).*

Citrix Application Firewall is easily configured to mask individual and multiple Primary Account Numbers. Citrix Application Firewall prevents the leakage of sensitive cardholder data, regardless of programmer oversight, logic flaws or targeted attacks. It masks or blocks the PAN, preventing it from ever being returned to the user, maliciously or accidentally.

*3.5 – Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.*

*3.5.1 – Restrict access to keys to the fewest number of custodians necessary.*

*3.5.2 – Store keys securely in the fewest possible locations and forms.*

The protection of encryption keys is paramount to maintaining the confidentiality of encrypted cardholder data. If an encryption key can be uncovered, all previous, current and future transactions that use the key can be decrypted and disclosed as clear text.

---

Citrix NetScaler, Citrix Application Firewall and Citrix Application Gateway™ solutions securely maintain the certificates and encryption keys used for SSL/TLS, and can SSL-enable applications that were not designed to use secure network protocols. Cryptographic protection standards such as FIPS 140-2 have proven to be a best practice for financial organizations that require strong key protection, and will be a consideration in PCI-DSS compliance. All Citrix appliances are available in FIPS 140-2-compliant versions.

*4.1 – Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.*

In addition to the protection of encryption keys, Citrix Application Firewall inspects the contents of SSL/TLS-encrypted sessions, ensuring session validity and blocking attacks -Network firewalls and Intrusion Protection Systems (IPS) cannot see inside an SSL session.

*5.2 – Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*

When using technologies that provide direct access to applications, especially client/server applications, it is imperative that the client machine be free from malware. Before access is allowed, Citrix SmartAccess™ automatically assures that minimum defined client security requirements have been met, contextually allowing application usage by clients that have been determined through policy to be trusted.

*6.5 – Develop all Web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:*

*6.5.1 – Unvalidated input*

*6.5.2 – Broken access control (for example, malicious use of user IDs)*

*6.5.3 – Broken authentication and session management (use of account credentials and session cookies)*

*6.5.4 – Cross-site scripting (XSS) attacks*

*6.5.5 – Buffer overflows*

*6.5.6 – Injection flaws (for example, structured query language (SQL) injection)*

*6.5.7 – Improper error handling*

*6.5.8 – Insecure storage*

*6.5.9 – Denial of service*

*6.5.10 – Insecure configuration management*

Secure coding practices and code review are core elements of a security-oriented application development lifecycle. However, they're not enough.

The threat vectors and application-layer attacks presented in Section 6 are common vulnerabilities that competent application developers have known how to prevent for years. But these common vulnerabilities continue to be regularly discovered — even in major commercial applications.

Human error, rushed patches, application interoperability, new attack methods and constantly evolving best practices make it highly likely that a critical vulnerability exists within a complex and highly customized Web application. And all it takes is one vulnerability to cause devastating data loss and compromise.

Citrix Application Firewall blocks these common vulnerabilities in both well-characterized and custom applications, complementing and enforcing secure coding best practices. Since Citrix Application Firewall only allows known good behavior, even new attacks are blocked without requiring new signatures or updates. Your data remains protected while other vendors scramble to release patches and hotfixes.

*6.6 – Ensure that all Web-facing applications are protected against known attacks by applying either of the following methods:*

- *Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security*
- *Installing an application layer firewall in front of Web-facing applications.*

*Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.*

Today's highly dynamic and complex Web applications require the protection of Citrix Application Firewall. While code review is always recommended, it is important to remember that the results of a code review are only valid until: a) the code changes in any way; or b) a new attack vector leads to an update of code review best practices.

The active protection afforded by Citrix Application Firewall prevents both known and unknown attacks, and is proven to be the most efficient and cost-effective means for protecting custom Web applications. This is why the PCI-DSS specification is mandating the implementation of an application-layer firewall as of June 30, 2008 and recommending it as a best practice today.

In addition, the requirements for strong access control and audit information presented in *Requirement 8: Assign a unique ID to each person with computer access* can be fulfilled and enforced through the implementation of Citrix Application Firewall.

## Recommendations

Organizations subject to compliance with PCI-DSS v1.1 should take the following steps to ensure conformance of Web application interests:

- Review the objectives of the PCI Security Standards Council and the PCI-DSS standard at <https://www.pcisecuritystandards.org/>
- Discuss governance, risk and compliance objectives with auditors, risk management and security officers, business-line management, Information Technology management and senior organizational management
- Institute recommended best practices for compliance with PCI-DSS requirements, including the installation of Citrix Application Firewall in front of Web-facing applications
- Perform active assessments and review audit logs to assure that policy objectives are being complied with

---

## Citrix Application Firewall

Citrix Application Firewall is a high-performance, hardened security appliance that blocks all known and unknown attacks against Web and Web Services applications. Citrix Application Firewall enforces a positive security model that permits only correct application behavior, without relying on attack signatures. Application Firewall analyzes all bi-directional traffic, including SSL-encrypted communications, protecting against 16 classes of Web application vulnerabilities without any modification to applications. Citrix Application Firewall is available as a family of purpose-built appliances that meet any deployment need, and in two software editions offering upgrade options as threats, applications and defenses become more complex.

Application Firewall is deployable alone or with Citrix NetScaler application delivery systems to deliver the combined benefits of application optimization and comprehensive protection.

## Citrix NetScaler

Citrix NetScaler optimizes the delivery of web applications — improving performance up to 5x, increasing security, and increasing web server capacity with lower costs — ensuring the best total cost of ownership (TCO), security, availability, and performance for web applications. Citrix NetScaler combines high-speed load balancing and content switching with state-of-the-art application acceleration, layer 4-7 traffic management, data compression, static and dynamic content caching, SSL acceleration, numerous network optimizations, and robust application security into a single, tightly integrated solution. Deployed in front of both web- and application servers, Citrix NetScaler significantly reduces processing overhead, reducing hardware and compresses data, reducing bandwidth costs.

## Citrix Access Gateway

Citrix Access Gateway products are universal SSL VPN appliances providing a secure, always-on, single point-of-access to an organization's applications and data. A comprehensive range of appliances and editions allow Access Gateway to meet the needs of any size organization, from small businesses to the most demanding global enterprises.

## Citrix Worldwide

### WORLDWIDE HEADQUARTERS

#### **Citrix Systems, Inc.**

851 West Cypress Creek Road  
Fort Lauderdale, FL 33309 USA  
Tel: +1 (800) 393 1888  
Tel: +1 (954) 267 3000

### EUROPEAN HEADQUARTERS

#### **Citrix Systems International GmbH**

Rheinweg 9  
8200 Schaffhausen  
Switzerland  
Tel: +41 (52) 635 7700

### ASIA PACIFIC HEADQUARTERS

#### **Citrix Systems Hong Kong Ltd.**

Suite 3201, 32nd Floor  
One International Finance Centre  
1 Harbour View Street  
Central  
Hong Kong  
Tel: +852 2100 5000

### CITRIX ONLINE DIVISION

5385 Hollister Avenue  
Santa Barbara, CA 93111  
Tel: +1 (805) 690 6400

[www.citrix.com](http://www.citrix.com)

### NOTICE

The information in this publication is subject to change without notice. THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. THE USE CASES IN THIS PAPER ARE PROVIDED ONLY AS POTENTIAL EXAMPLES AND YOUR ACTUAL COSTS AND RESULTS MAY VARY.



Best Access Experience. Anytime. Anywhere.

**About Citrix:** Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 180,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the *Fortune* 100 companies and 98% of the *Fortune* Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Annual revenue in 2006 was \$1.1 billion. Learn more at [www.citrix.com](http://www.citrix.com).

©2007 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler®, Citrix Application Firewall™, Citrix SmartAccess™ and Citrix Application Gateway™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. UNIX® is a registered trademark of The Open Group in the U.S. and other countries. Microsoft®, Windows® and Windows Server™ are registered trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.