

Barracuda Web Application Firewall Ensures PCI DSS Compliance

Barracuda Web Application Firewalls protect networks against unauthorized access, data leakage, site defacement and other malicious attacks by hackers that compromise both the privacy and integrity of vital data. By installing a Barracuda Web Application Firewall, businesses that store, process and/or transmit credit card numbers can protect their Web applications and achieve PCI DSS compliance in one easy step.

Payment Card Industry Data Security Standard (PCI DSS) Requirements

In response to the increase in identity theft and security breaches, major credit card companies collaborated to create the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. It applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmit cardholder account data.

The 12 PCI DSS requirements are organized into six main categories that prevent credit card fraud through increased controls around data and its exposure to compromise. To be fully compliant, an organization must satisfy all 12 requirements.

Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Controls

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Source: PCI Security Standards version 2.0 - <http://www.PCISecurityStandards.org>

Merchants and organizations should be most concerned with PCI DSS Section 6, which addresses the development and maintenance of secure systems and applications. PCI-DSS compliance requires organizations either submit to code audits or install a Web Application Firewall to secure their public facing Web applications.

RELEASE 2

NOVEMBER 2010

PCI Security Standards Council

Founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to enhance payment account security.

Noncompliance Penalties

While there are no penalties levied by the PCI Security Standards Council responsible for managing the requirements, credit card issuers and financial institutions can enforce PCI DSS compliance by offering incentives and issuing fines.

A code audit places considerable strain on a company with a large quantity of code that needs to be reviewed. This results in a considerable amount of time and cost for each application. Furthermore, code audit provides a point in time protection; quarterly reviews must be maintained to account for any change in the application code. This burdens organizations by constraining their engineering teams to fixing vulnerabilities rather than continuing to innovate and drive companies forward in the marketplace.

Barracuda Networks Enables PCI DSS Compliance



The simpler alternative to satisfy PCI DSS compliance is to invest and implement a comprehensive Web application firewall. Barracuda Web Application Firewalls are designed to be easy and cost-effective solutions for PCI DSS compliance. It protects Web applications from attacks and ensures a layer of security regardless of the underlying code. Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP/S traffic, Barracuda Web Application Firewalls proxy all traffic and insulate Web servers from direct access by attackers. This helps organizations ensure PCI DSS compliance across major requirements categories:

PCI-DSS Requirement	Barracuda Web Application Firewall
3. Protect Data	Proxies all inbound and outbound Web traffic to insulate Web servers from direct access by attackers.
4. Encryption	Provides easy SSL encryption even if the application or server does not enable SSL encryption for inbound and outbound Web traffic.
6. Protect Against Vulnerabilities	Safeguards custom development, legacy and third party applications from known and zero-day attacks as well as the industry-accepted top 10 Web application vulnerabilities.
7. Restrict Access	Utilizes role-based administration to enforce security policies for accessing systems and SSL administration.
10. Track and Monitor Access	Provides logs and reports of application access and security violations.

Barracuda Web Application Firewalls also protect organizations from Top Web Application Threats listed by the PCI Council or other security organizations. These include:

Vulnerability	Description	Barracuda Web Application Firewall Solution
6.5.1 Injection Flaws	Injection flaws are prevalent in Web applications and are often found in SQL queries, LDAP queries, OS commands, and program arguments.	Inspects each client request to the Web application servers for malicious code and blocks any malicious request.
6.5.2 Buffer Overflow	Overloads memory capacity to execute a malicious program to steal passwords, alter system configuration, install backdoors or launch other attacks.	Rejects malformed requests to Web servers and limits total Web form request length.
6.5.3 Insecure Cryptographic Storage	Exploits applications that fail to store sensitive information such as credit card numbers as encrypted fields.	Filters and intercepts outbound traffic to prevent the transmission of sensitive information.
6.5.4 Insecure Communications	Failure by applications to encrypt network traffic containing sensitive communications.	Provides Instant SSL functionality that transforms an HTTP Web site into an encrypted HTTPS site without having to change any code.
6.5.5 Improper Error Handling	Exploits error messages to gather information about the OS and server versions, patch levels, etc. to launch targeted attacks on the server with known platform vulnerabilities.	Cloaks details of the Web application infrastructure and blocks a server's error messages from being sent out to the client. Filters and intercepts outbound traffic to prevent the transmission of sensitive information.

Challenges to an Application Code Audit

- The average security defect takes 75 minutes to diagnose and six hours to fix. (Pentagon Study)
- Every 1,000 lines of code average 15 critical security defects. (US Dept. of Defense)
- The average business application has 150,000-250,000 lines of code. (Software Magazine)

Vulnerability	Description	Barracuda Web Application Firewall Solution
6.5.6 All “High” Vulnerabilities Identified	All “high” vulnerabilities discovered in the vulnerability identification process.	Protects against all of the top threats. Reverse proxy deployment is architecturally superior and more secure than sniffer or bridge solutions.
6.5.7 Cross Site Scripting (XSS)	Injects malicious code from a trusted source to execute scripts in the victim’s browser that can hijack user sessions, deface Web sites, or redirect the user to malicious sites.	Validates user input by terminating session and inspecting incoming requests before forwarding it to the backend servers, blocking it prior to executing within a browser.
6.5.8 Improper Access Control	No credential checks. Failure to restrict URL access, directory traversal.	Provides a granular URL and form-level rules engine that restricts access to unauthorized resources. Sets up and enforces authentication & authorization policies via integrated LDAP, RADIUS, CA SiteMinder and RSA SecurID.
6.5.9 Cross Site Request Forgery (CSRF)	Hijacks a browser from a logged in victim to send forged requests without the victim’s knowledge.	Injects randomized tokens into online forms to authenticate data streams, eliminating unauthorized or malicious requests.

With over a decade of experience in securing Web applications, the Barracuda Web Application Firewall is the proven solution used by organizations of all sizes to secure their valuable assets against Web threats.

For questions about the Barracuda Web Application Firewall, please visit <http://www.barracuda.com/waf> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company’s expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L’Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks’ range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.



Barracuda Networks
 3175 S. Winchester Boulevard
 Campbell, CA 95008
 United States
 +1 408.342.5400
www.barracuda.com
info@barracuda.com