

PCI

Data security standard and web applications

What you need to know



Introduction

The PCI (Payment Card Industry) Data Security Standard became a global requirement on June 30, 2005, for all entities handling credit card data. Merchants who fail to comply with PCI can face fines or exclusion from processing credit cards.

PCI extensions in the latest revision of the mandate are aimed at protecting credit card data from emerging Web application security threats. Other new rules will require companies to ensure that any third parties that they deal with, such as hosting providers, have proper controls for securing credit card data.

The standard lists 12 broad controls that retailers, online merchants, data processors and other businesses must implement to protect cardholder data. They include technology controls such as data encryption, end-user access control and activity monitoring, as well as procedural mandates.

Most existing PCI requirements focus on security at the network level, but many of the latest threats are at the application level, so it makes sense to update PCI to protect against Web application threats such as SQL injection attacks, cross-site scripting flaws, improper-handling problems and validation errors.

Requirements

Section 6.5 of the PCI mandate requires that “web software and applications are developed based on secure coding guidelines such as the Open Web Application Security Project (OWASP) guidelines.” The OWASP Top 10 represents a broad consensus on what the most critical web applications flaws are today.

Developing secure applications involves a methodology and requires security to be taken care of throughout the entire software development life cycle process. However, faster time to market, richer functionality requirements using new technologies like web services and AJAX, and insecure coding practices do not encourage the development of secure applications. Ultimately this means that unmanaged risks are taken every day by organisations in charge of protecting client information.

When software is not built from the ground up using secure coding principles, it becomes nearly impossible to dynamically manage the risk from a development and patch maintenance perspective. Implementing additional controls, such as web application firewalls to protect and secure the most common vulnerabilities found in web applications is increasingly being looked at as the most effective solution to the problem.

contact@bee-ware.net • www.bee-ware.net
UK : + 44 (0) 207 463 2001 • FRANCE : +33 (0) 174 70 47 11 • BENELUX : + 32 (0) 2427 5302

About Bee Ware:

Bee Ware is the leading provider of appliance based secure web enabled delivery solutions. Built to Open Standards, Bee Ware's award-winning products ensure security, high performance and business continuity for the world's most demanding organisations.

PCI

Data security standard and web applications

Key Points

- i-Sentry acts as a compensating control – helping you achieve PCI compliance AND save time and money in application deployment
- i-Watch in front of your application gives real time assessment of the risks you are running
- ICX technology protects against zero day attacks and undiscovered threats
- Comprehensive logging enhances your PCI reporting capability
- Web application firewalls provide a foundation for business continuity

Solutions

Web application firewalls are a critical component of secure web application architecture. To manage the most important OWASP top 10 vulnerabilities without having to recode the applications a web application firewall presents an effective and economically attractive alternative - from a PCI perspective this is known as a 'compensating control'.

Bee Ware's i-Sentry® is a reverse proxy based web application firewall appliance enabling secure application delivery. i-Sentry employs patented ICX™ technology which uniquely combines intelligent behaviour analysis with positive and negative security models to protect and secure the web application.

Running through the broad spectrum of PCI compliance requirements, it is useful to focus on proven compensating controls capable of satisfying the mandate for information protection and security:

Broad PCI Requirement	Example of Specific Requirement	Compensating Control	Solution	Benefits
3. Protect stored cardholder data.	3.3 Mask PAN* when displayed (the first four and last six digits are the maximum number of digits to be displayed). *Primary Account Number.	Use a Web Application Firewall to rewrite PAN. Use a Web IDS to detect account numbers.	i-Watch detects and alerts on any pattern. i-Sentry can rewrite any pattern, whether inbound or outbound, in the encrypted traffic.	Automation saves time and labour costs and increases productivity. Minimal human intervention for more safety.
4. Encrypt transmission of cardholder data across open public networks.	4.1 Use strong cryptography and encryption techniques to safeguard sensitive cardholder data during transmission over public networks.	Use a Web Application Firewall to enforce SSL strength and usage.	i-Sentry controls, accelerates and terminates encryption strength (cipher) of the SSL connection over public networks.	Protection of cardholder but also of merchant against cardholder fraud.
6. Develop and maintain secure systems and applications.	Work against: 6.5.4 Cross-site scripting 6.5.5 Buffer overflows 6.5.6 Injection flaws (SQL injection) Ensure protection by : 6.6 Installing a web application firewall in front of web facing applications.	Use a Web Application Firewall to detect and block these attacks.	i-Watch detects application vulnerabilities. i-Sentry secures and accelerates your web applications .	Reduced risk and future proof attack management. Increased transaction assurance.
11. Regularly test security systems and processes.	11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. Include: 11.3.2 Application-layer penetration tests.	Use an IDS to continually monitor the application.	i-Watch monitors and analyzes all application use, and reports on attacks and insecure application changes.	Continuous Application Assessment saves on audit and reporting costs.