AWF SERIES SOLUTION BRIEF

WAF for PCI-DSS Compliance

AWF Series Web Application Firewall helps meet PCI DSS standard, protecting cardholder data, reducing fraud and mitigating security vulnerabilities

Background

The Payment Card Industry Data Security Standard (PCI DSS) was instituted more than a decade ago to specify the minimum levels of security for storing, processing and transmitting credit cardholder data. Any type of business that wishes to accept major credit cards, such as MasterCard, Visa, American Express and others, is required to comply with PCI DSS in order to obtain or maintain membership status.

The stakes are high for merchants – failure to comply with PCI DSS, and a subsequent breach of cardholder or transaction data, can result in substantial fines and/or the revocation of the right to accept credit card payments, not to mention the potential for a class-action lawsuit by the credit cardholders themselves or by a government entity.

The PCI DSS requirements apply to all network components, servers and applications included in or connected to the cardholder data environment. The standard sets out six key control objectives and twelve requirements that members must adhere to – and larger entities must be externally validated for compliance.

Solution Overview

Array's AWF Series Web application firewalls provide industry-leading Web application attack protection, ensuring continuity and high availability of Web applications while reducing security risks. The AWF Series not only detects the complex Web application attacks of today, but also blocks attack traffic in real time without affecting the normal flow of traffic. In addition, the AWF Series provides extremely fine-grained attack detection and analysis capabilities while protecting against a broad spectrum of Web application attacks.

Deployed in the datacenter or enterprise network, the AWF Series includes a powerful suite of features to assist in attaining and maintaining PCI compliance.

The majority of the PCI DSS requirements, and the specific ways in which the AWF Series can help achieve compliance, include:

- **Install and maintain a firewall configuration to protect cardholder data.** The AWF Series Web application firewall protects back-end Web servers from attacks. It includes a predefined attack signature library that helps block common attacks, and in addition the administrator can define customized rules to prevent new attacks.
- **Do not use vendor-supplied defaults for system passwords and other security parameters.** AWF Series allows the administrator accounts' passwords to be changed, and all remote administrative access is encrypted via SSL.
- **Protect stored cardholder data.** The AWF Series itself does not store cardholder data, and a reverse proxy mode can be utilized to protect Web servers from being directly accessed by attackers.
- **Encrypt transmission of cardholder data across open, public networks.** Array's AWF Series supports secure transmission of data via SSL, and does not provide a wireless network interface.
- **Protect all systems against malware and regularly update antivirus software or programs.** The AWF Series' core operating system is proprietary, and security hardened to protect against malicious attacks. In addition, the built-in attack signature library can be updated as needed to counter the latest attacks.
- **Develop and maintain secure systems and applications.** Protection is provided against SQL injection, buffer overflow, server information leaks, and known vulnerabilities, as well as XSS, CSRF and other attacks. Vulnerability pattern can be easily updated as needed. Access control lists help assure that administrators and auditors can access only the appropriate data.
- **Restrict access to cardholder data by business need to know.** As mentioned previously, the AWF Series provides role-based administrative rights. Administrator accounts are restricted to configuration tasks; account manager accounts are restricted to managing the administrators and their sessions; and the audit accounts are restricted to auditing the administrators' activities and system logs. None of these accounts has access to cardholder data.
- **Identify and authenticate access to system components.** In addition to authenticating and restricting access for multiple management account types, the AWF Series sets up an individual session each time an administrator accesses the system, and all user types' accesses are logged.
- **Track and monitor all access to network resources and cardholder data.** The AWF Series maintains a log system which maintains access logs, attack logs, audit logs, webkeeper logs and backup logs.
- **Regularly test security systems and processes.** A scanning function is included in the AWF Series, allowing administrators to define automatic scan tasks to regularly scan destination URLs to ensure the security of back-end applications.
- **Maintain a policy that addresses information security for all personnel.** As mentioned previously, the AWF Series provides role-based authentication and access for administrators, account managers and auditors. In addition, all access activities and operations are recorded in logs for auditing purposes.

AWF Series Benefits

- Operates on multiple levels to protect Web servers and applications
- Continuous scanning for vulnerabilities and for SQL injection or cross-site scripting and other threats within applications
- DDoS protection via brute force attacks mitigation
- Active incident response with detection, blocking and prevention of attacks, including zero-day detection
- Post-incident diagnosis and analysis to reduce overall security risk
- Highly refined rules library includes sophisticated protections
- Comprehensive Layer 1 through 7 protection for Web servers at the network and application level
- Web page tamper-proofing through centralized management and control of all Web tamper-proofing endpoints
- Customizable feature library and flexible configuration model
- Guided configuration to reduce installation complexity and errors
- Comprehensive management portal with visualized monitoring

Summary

With the exception of restricting physical access to cardholder data, Array's AWF Series Web application firewall can help enterprises and other entities meet the requirements for PCI DSS compliance, while protecting cardholder data, reducing fraud exposure, and mitigating security risks.

For more information about how Array Networks can help you meet the requirements of the PCI DSS standard, visit us at www.array-networks.co.in or send us an email at sales-india@arraynetworks.com.