

PCI COMPLIANCE

SOLUTION PROFILE

Payment Card Industry (PCI) Data Security Standard

Electronic theft of personal and financial data is a growing problem that undermines consumer confidence and loyalty, and drives up costs. In response, the payment card industry has developed the PCI Data Security Standard. This multi-faceted security standard includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

These standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data, and affect all payment channels, including retail (brick-and-mortar), mail/telephone order and e-commerce.

How Third Brigade Helps Companies Achieve PCI Compliance

Third Brigade Deep Security is a best-of-breed, host-based intrusion defense system that brings proven network security approaches — including firewall, intrusion detection and prevention, and application firewall capabilities — down to individual computers and devices. Deep Security has been architected to minimize impact on host and IT operations. It is a non-disruptive and scalable technology that enables immediate, “day-one” deployment, without host interruption or system reboot. Mission-critical servers, applications and data can be quickly and consistently protected, with ongoing security updates, to shield known and unknown vulnerabilities.

Deep Security can accelerate and simplify your PCI audit and help achieve PCI compliance by:

- **Enabling firewall network segmentation** to reduce the scope of the PCI audit.
- **“Virtual Patching”** to comply with requirements for vendor security patches to be applied within one month of release.
- **Detecting and preventing** attacks that target cardholder data, and alerting staff the moment an attack has been attempted.
- **Providing application firewall capabilities** to complement secure coding initiatives and to protect web applications from attacks like SQL injection and cross-site scripting (XSS).
- **Ensuring standard security configurations** are consistently and automatically applied to all appropriate systems, thus reducing the risk of an attack.
- **Providing detailed log information** on who attacked, when they attacked and what they attempted to exploit, and by providing an auditable report of the security posture of a system.



FAILURE TO COMPLY WITH PCI MAY RESULT IN FINES OR RESTRICTIONS IMPOSED BY THE CREDIT CARD COMPANY.

PROTECTION FROM FINES IS TYPICALLY PROVIDED TO MERCHANTS OR SERVICE PROVIDERS THAT HAVE BEEN COMPROMISED BUT FOUND TO BE COMPLIANT AT THE TIME OF THE SECURITY BREACH.

ANY MERCHANT THAT HAS SUFFERED A BREACH THAT RESULTED IN AN ACCOUNT DATA COMPROMISE MAY BE ESCALATED TO A HIGHER VALIDATION LEVEL SUCH AS REQUIRING ANNUAL ONSITE AUDITS.

Which Parts of the PCI Standard Does Third Brigade Deep Security Address:

PCI REQUIREMENT

1.1	Establish firewall configuration standards that include:
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
1.1.5	Documented list of services and ports necessary for business.
1.2	Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.
1.3	Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.
1.3.1	Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters).
1.3.2	Not allowing internal addresses to pass from the Internet into the DMZ.
1.3.3	Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network).
1.3.4	Placing the database in an internal network zone, segregated from the DMZ.
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment.
1.3.7	Denying all other inbound and outbound traffic not specifically allowed.
1.3.8	Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes).
1.3.9	Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
1.4	Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).
1.4.1	Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.
1.4.2	Restrict outbound traffic from payment card applications to IP addresses within the DMZ.
2.0	Do not use vendor-supplied defaults for system passwords and other security parameters.

THIRD BRIGADE DEEP SECURITY ADDRESSES THIS

Third Brigade provides sophisticated, centrally managed stateful firewall. It prevents policy violations, and logs and reports any attempted firewall policy violations.

Third Brigade security profiles contain the firewall configuration policy. Role-based access control capabilities support separation of administrative duties with respect to creating, deploying and auditing firewall policy and events that violate the policies.

Deep Security is used to create and manage sophisticated firewall rules that Allow and Deny appropriate connections with the minimum number of rules and maximum flexibility. Centralized management makes this easy to administer and deploy to the right systems.

Third Brigade Deep Security provides out-of-box reporting capabilities for the creation of reports that detail the hosts' stateful firewall configuration.

Deep Security firewall capabilities can enable network segmentation to isolate systems that store, process, or transmit card holder data from systems that do not. This enables cardholder data environments to be easily defined, reducing the overall scope of the PCI audit.

PCI REQUIREMENT

- 2.1** Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

- 2.1.1** For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

- 2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

- 2.4** Hosting providers must protect each entity’s hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: “PCI DSS Applicability for Hosting Providers.”

- 6.1** Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

- 6.2** Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

- 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.

THIRD BRIGADE DEEP SECURITY ADDRESSES THIS

- Custom filters can be used to detect and prevent the use of default passwords.

- Where applicable, Deep Security can be used to perform network segmentation such that wireless environments cannot access payment systems thereby eliminating wireless environments from the scope of the PCI Audit.

- Security profiles can be used to specify configurations for specific server functions (i.e. a DNS, Web or Database Server), and restrict or prevent access to services and protocols.

- Third Brigade can also help Hosting providers with Appendix A requirements by providing virtual network segmentation of the cardholder data environment and role-based access control (RBAC) for delegated administration capabilities to enforce separation of duties.

- Deep Security Virtual Patching protects systems and data until patches can be deployed and can act as a compensating control for systems that cannot be patched within the 30-day time frame specified. Deep Security can also shield systems in the case of a known vulnerability where the vendor patch is not available; or in the case of custom applications where source code changes are required to remediate vulnerabilities.

- Third Brigade monitors a wide range of vulnerability research sources to identify and deliver new filters to customers. The deployment of new security filters can be completely automated such that the download and installation of new security filters to the appropriate systems occurs without administrative intervention. Deep Security also supports the ability to schedule (one time only, daily, weekly, etc.) automatic scans of host systems and makes recommendations on the appropriate security filters to protect these hosts.

- Third Brigade complements secure coding initiatives by providing strong detection and prevention capabilities that address these attacks (6.5.1 to 6.5.10):
 - **Detection:** It is important to detect attacks, even if an application is not susceptible to a specific attack or class of attack, because it identifies the attacker before they can find other potential vulnerabilities.
 - **Prevention:** Third Brigade shields web application vulnerabilities, preventing security breaches, until the underlying flaw(s) can be addressed

PCI REQUIREMENT

6.5.8	Insecure storage.
6.5.9	Denial of service.
6.5.10	Insecure configuration management.
6.6	Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: <ul style="list-style-type: none"> ➤ 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.
7	Restrict access to cardholder data by business need-to-know.
10	Track and monitor all access to network resources and cardholder data.
10.3	Record at least the following audit trail entries for all system components for each event: User identification; Type of event; Date and time; Success or failure indication; Origination of event; Identity or name of affected data, system component, or resource.
10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.
11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.
12.9.5	Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

APPX B Compensating Controls for Encryption of Stored Data.

CONTACT

Corporate Headquarters:	US Headquarters:	European Headquarters:
40 Hines Road Suite 200 Ottawa, Ontario, Canada K2K 2M5 +1.866.373.6977	11710 Plaza America Drive Suite 2000 Reston, Virginia, USA 20190 +1.866.373.6977	Fetcham Park House Lower Road Fetcham, Surrey, UK KT22 9HD +44 (0)1372 371210
www.thirdbrigade.com		

THIRD BRIGADE DEEP SECURITY ADDRESSES THIS

Third Brigade's advanced deep packet inspection engine provides application layer firewall protection for web applications. It monitors incoming and outgoing application traffic for protocol deviations, content that signals an attack, or policy violations. When necessary, Deep Security intervenes and neutralizes the threat by blocking the malicious traffic.

Third Brigade firewall capabilities (logical access control) are one way to enforce network access to host resources, on a machine (IP or MAC) basis.

Third Brigade Deep Security logs are part of an effective audit trail and can be used to track and monitor access. Detailed logging and reporting capabilities are an effective way to record, track and monitor cardholder data system access and use. Deep Security can be configured to store logs for the appropriate retention period and/or forward them to a security information and event management (SIEM) application or log management system.

Third Brigade Deep Security is a host-based intrusion detection and prevention system. It monitors traffic, prevents intrusions, and alerts personnel to suspected compromises. Security updates that shield newly discovered vulnerabilities are automatically delivered to customers and hosts.

Deep Security's "recommendation scan" feature identifies applications running on hosts that may be vulnerable, and recommends which filters should be applied to these hosts, ensuring the correct protection is continuously in place, with minimal effort.

Deep Security provides alerts that are integral to a security incident response plan. And because it can prevent attacks as well, Deep Security reduces the number of incidents that need to be responded to.

Third Brigade's integration with leading SIEM vendors enables organizations to receive a consolidated view of security incidents.

If for some reason, a company is unable to encrypt cardholder data, Third Brigade Deep Security alone, or in combination with other security mechanisms, can provide the necessary compensating controls.