NEXUSGUARD

White Paper

The Significance of Being a **PCI-Certified Service Provider**

As a PCI-certified Service Provider (Level 1), Nexusguard's infrastructure is guaranteed to offer maximum security for processing, storing and/or transmission of credit card data and sensitive information.

V2.1.1

Introduction

Whether it's banks, e-commerce businesses or gaming websites, given the sensitivity and importance of data they handle, the protection of credit data and sensitive information is of the utmost concern. As many have witnessed through news or even personal experience, the consequences of cardholder data and sensitive information being mishandled, lost, leaked or stolen can be very serious, and that risk is heightened by the increased threat of cyber crime. In view of the growing threat, some regulators[1] have introduced new regulations to strengthen cyber security standards, especially for banks and third-party vendors, in recent months.

Among the many security compliance standards, the Payment Card Industry Data Security Standard (PCI DSS) is regarded as the most stringent compliance standard. No matter how challenging to those being assessed, achieving PCI DSS compliance is a clear indicator of the care merchants and third-party vendors take when handling cardholder and sensitive customer data. While compliance with the PCI DSS is not legally required, achieving the PCI DSS accreditation helps many organisations, especially banks and financial institutions, meet a significant portion of regulatory requirements.

The PCI Security Standards Council recognizes Nexusguard as a PCI-certified service provider (SP) (Level 1) for scenarios in which a merchant processes, stores, and/or transmits credit card data and sensitive information on the Nexusguard infrastructure. Nexusguard's core infrastructure and services are validated by authorized independent QSA to be PCI DSS 3.0 compliant. This article addresses the commonly questions asked by our clients on Nexusguard's PCI DSS assessment, control measures taken, the security of its infrastructure including data centers, as well as the cost-effectiveness for PCI and non-PCI merchants.

[1] For example, the HKMA issued guidelines in October 2014 to banks on how to protect customer data; the New York State Department of Financial Services (NYDFS) has also imposed new cyber security standards for banks and their supply chain in June 2015.

Overview of PCI DSS

Despite the fact that compliance with the PCI DSS is not legally required, it is obvious that some regulations, such as those in some US states, refer directly to the PCI DSS or simply make equivalent provisions. The PCI DSS is regarded as the most widely accepted industry security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The Payment Card Industry (PCI) Council was formed in 2006 by leading credit card companies (American Express, Discover, JCB International, MasterCard, and Visa), who established PCI DSS as a set of rules for payment industries to prevent credit card fraud, hacking and other security threats. These standards apply to any company that stores, processes, or transmits Primary Account Numbers (PANs), cardholder data, expiration codes, or service codes.

These standards apply to all system components such as servers, network components, applications, and all virtualized parts (virtual machines [VMs], hypervisors, and so on). Over time, these standards have also become a reference guide for IT professionals to devise procedures for building safe application infrastructures and ensuring sound data security practices.

PCI DSS consists of 12 standards, of which certain sets of the 12 standards fall under general security requirements. In the 2013 revisions, PCI DSS was updated to include considerations and tools for cloud services, offering ways to measure PCI compliance for specific cloud layers and components. These standards (displayed in the table below) are intended to provide a general framework.

All organizations processing credit card and sensitive information, regardless of their deployment model, are required to be certified. For larger merchants (Level 1 is the largest type), validation by an independent and approved reviewer is required. A PCI Qualified Security Assessor (QSA) is authorized to perform an independent assessment and certify a vendor.

PCI Data Security Standard – High-level Overview

Build and Maintain a Secure Network and System	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. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 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 for all personnel

Nexusguard's PCI DSS assessment

The 2013 PCI Guidelines point out that there are two options for third-party service providers to validate compliance. First, they can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance; or if they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customers' PCI DSS assessments.

Nexusguard implements the first option by undergoing an annual onsite assessment, in which compliance validation is performed on all system components in the cardholder data environment. This way, merchants do not have to engage Nexusguard in their own PCI DSS assessment process every time, but are only required to manage and monitor the PCI DSS compliance of all associated third-party SPs with access to cardholder data.

Nexusguard's PCI DSS compliance

According to the 2013 PCI Guidelines, SPs are organizations that process, store, or transmit cardholder data or sensitive information on behalf of clients, merchants, or other SPs. They may include shared hosting environments in which cardholder data may be stored. Certified credit card merchants must use SPs that are compliant with the PCI DSS.

A validated SP is one that has undergone an audit by an independent QSA and is found to be in conformity with the PCI security standards as outlined in the latest version of the Data Security Standard published by PCI.

Nexusguard is a PCI-certified SP for scenarios in which a merchant processes, stores, and/or transmits credit card data or sensitive information on the Nexusguard infrastructure. It has built and maintains a secure network environment[2] and operation procedure that have been validated by an independent QSA, allowing merchants to establish a secure cardholder environment and to achieve their own certification, having confidence that their underlying technology infrastructure is compliant.

Nexusguard has been validated as a Level 1 SP[3], meaning that it stores, processes and/or transmits over 300,000 transactions annually. Its core infrastructure and services are PCI DSS 3.0 compliant, including data center locations responsible for delivering the specific services. The compliance has been validated by an authorized independent QSA.

[2] Although Nexusguard's environment is of a virtualized, multi-tenant nature, it has effectively implemented security management processes, PCI controls, and other compensating controls that effectively and securely segregate each customer into its own protected environment.

[3] Level 2: Any service provider that stores, processes and/or transmits less than 300,000 transactions annually.

Cost-saving benefits for PCI merchants

Achieving and maintaining PCI DSS compliance can be time-consuming and costly for merchants. To them, one notable benefit of engaging Nexusguard is that it allows them to reduce the cost of meeting PCI DSS requirements.

Below are a few examples that illustrate how Nexusguard helps merchants achieve and maintain their PCI DSS compliance in a cost-effective manner:

- As required by PCI DSS Requirement 6.6, public-facing web applications are subject to additional controls, to address ongoing threats and vulnerabilities after implementation. Designed to meet this requirement, Nexusguard's web application firewalls (WAFs) are proven to be effective at preventing common web application vulnerabilities that are listed in the requirement.

- As Nexusguard has been certified as Level 1 PCI compliant, a merchant can obtain certification without having to perform a physical walkthrough of its data centers. The merchant's QSA can rely on the work performed by Nexusguard's QSA, which included an extensive review of the physical security of its data centers.

- While all merchants need to manage their own PCI certification, for the portion of the PCI cardholder environment operating through Nexusguard, your QSA can rely on Nexusguard's validated service provider status.

After all, Nexusguard's PCI DSS compliance covers all requirements as defined by PCI DSS for physical infrastructure SPs. Nexusguard can simplify your own PCI compliance by relying on our validated service provider status.

Forensic investigations

If required, Nexusguard can also cooperate with forensic investigations. Nexusguard manages forensic investigations in alignment with DSS requirement A1.4. Customers or their designated Qualified Incident Response Assessors (QIRA) can contact Nexusguard as required to perform forensic investigations.

Benefits for non-PCI merchants

Our PCI compliance further demonstrates our commitment to information security at every level. Compliance with the PCI DSS standard, validated by an independent third-party audit, confirms that Nexusguard's security management program is comprehensive and follows leading practices. This validation provides more clarity and assurance for customers evaluating the breadth and strength of Nexusguard's security practices.

Conclusion

With the PCI DSS accreditation, Nexusguard is committed to maintaining its infrastructure, systems and operation procedure in constant compliance with the latest standards by:

- building/maintaining a secure network environment and operation procedure;
- developing/maintaining secure software systems and application coding security;
- protecting cardholder data and client data privacy;
- implementing strong security measures recognized by international authorities;
- performing required quarterly vulnerability and annual risk assessment; and
- maintaining a stringent and responsible policy that addresses information security.

For financial service, e-commerce and gaming companies maintaining PCI certification, having Nexusguard as their DDoS protection SP ensures the infrastructure and services that process, store and/or transmit their credit card and sensitive information comply with the PCI DSS 3.0 standards. Clients pursuing PCI certification will also find it more cost-effective to integrate Nexusguard's pre-certified components as the required items for assessment.

White Paper

NEXUSGUARD

Founded in 2008, Nexusguard is the global leader in fighting malicious internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats. Headquartered in San Francisco, Nexusguard's network of security experts extends globally.

Twitter twitter.com/nexusguard
Facebook facebook.com/NXG.PR
LinkedIn linkedin.com/company/nexusguard

nexusguard.com
contact@nexusguard.com

20150805-EN-A4