SHIELDX

PCI DSS: Meeting The 3.2.1. Standard

For companies that handle credit card data, the Payment Card Industry Data Security Standard (PCI DSS) governs how cardholder data is stored, processed and transmitted. All major players in the credit card ecosystem support PCI DSS and, if your organization accepts payment cards, you are required to comply.

THE 12 PCI DSS REQUIREMENTS

There are six overarching objectives in the PCI DSS standard that are in turn spelled out in 12 groups of requirements. Meeting the requirements can be a challenge**,** but one strength of PCI DSS is that it allows organizations to manage compliance according to their specific IT and business needs. ShieldX provides several key capabilities that help organizations reach PCI compliance using technologies that are uniquely suited to today's data center architecture.

Here are the six objectives and twelve underlying requirements:

Build and Maintain a Secure Network and Systems

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

HOW SHIELDX APPLIES TO PCI DSS

Today, complying with PCI becomes especially complicated when moving data centers to cloud/ virtualized environments. There is a lack of visibility into PCI applications—their size and structure—forcing security teams to create increasingly larger PCI "zones" that result in dramatic increases in cost, management and audits**,** while also compromising an environment's security posture. By using automation, ShieldX reduces the cost and manual effort as well as time to value to pass PCI audits.

ShieldX uniquely ensures isolation of an organization's cardholder data environment with a robust set of natively integrated security capabilities, including:

- Visibility. Enhanced visibility of East-West traffic, and asset as well as application and connection discovery. ShieldX discovers and identifies business logic tiers—not just ports and protocols—within a network, to provide a full picture of all workloads across a multi-cloud. Even as your infrastructure changes, ShieldX continuously discovers all changes—large or small.

- Advanced Security to Layer 7. Control of all traffic at the application level (Layer 7 of the OSI Model). The ShieldX Elastic Security Platform relies on innovative deep packet inspection (DPI) technology to accurately identify and classify all traffic by its corresponding application, regardless of ports and protocols, evasive tactics such as port hopping, or encryption. In sensitive or specialized zones of the network, this provides the best possible control by allowing security administrators to deny all traffic except the few applications that are explicitly allowed.

- Least Privilege Model. ShieldX employs least privilege access control across the network. This enables organizations to tightly control access to cardholder data environments based on an extensive range of business-relevant attributes, including the specific application and individual functions being used, and the specific elements of data being accessed (e.g., credit card or social security numbers). The result is a definitive implementation of Zero Trust, where administrators can create security rules based on business logic to allow only the absolute minimum, legitimate traffic in a zone while automatically denying everything else.

- Advanced Threat Protection. ShieldX provides a combination of antivirus/malware, intrusion prevention, and advanced threat prevention technologies that filter all allowed traffic for both known and unknown threats.

- Multi-Cloud Orchestration. ShieldX simplifies manage-ment of multi-cloud and virtualized data center environments via a single management console, reducing the risk of misconfiguration, while adapting to your existing business processes using business logic-based policy.

PCC DSS REQUIREMENTS V3.2	SUPPORTED SUBSECTIONS	DESCRIPTION
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.2 1.2.1 1.2.3 1.3.4 1.3.5 1.3.6	ShieldX Elastic Security Platform enables zero trust or the principle of least-privileged access control (i.e., deny all applications and content except for that which is necessary) for all networks involving cardholder data. Our microsegmentation supports all sub-requirements pertaining to network zoning, application tiering and microsegmentation intended to prohibit public access and direct access between the workloads and cardholder application tiers.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	2.1.1 2.2 2.2.1 2.2.2 2.4	The intent behind Requirement 2 is to implement sufficient preventive controls to reduce the attack surface. These controls include changing vendor passwords; enabling only necessary services, protocols and daemons; and removing unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and web servers. For a relatively complex cardholder data environment, there are potentially thousands of instances in which unnecessary services, unnecessary functionality, and insecure services could operate. The ShieldX ESP leverages deep packet inspection and integration with leading vulnerability management solutions to detect threats targeting your systems containing sensitive PCI data. Our patented technology inspects content as it traverses the network, identifying ports, protocols and applications.
Requirement 3: Protect stored cardholder data	n/a	This requirement focuses on reducing the amount of cardholder data stored and ensuring stored data is appropriately masked and encrypted. Microsegmentation inherently restricts access to containers (including database services) to the entities that should be working with them. The architecture also has the enormous advantage of giving you visibility into East-West traffic, so that attacks that are attempting to pivot through the data center can be detected and blocked before they make progress.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	n/a	

Requirement 5: Use and regularly update anti-virus software or programs	n/a	The ShieldX containerized microservices-based architecture builds the DPI-enabled security controls including threat and malware prevention, content inspection, URL filtering, TLS inspection, virtual patching and more.
Requirement 6: Develop and maintain secure systems and applications	6.4.1 6.4.3 6.4.5.3 6.6	As a fully application-aware solution, the Elastic Security Platform is capable of preventing a wide range of application-layer attacks that have, for example, taken advantage of improperly coded or configured web apps. As part of DevOps, developers tag workloads by business function which will be applied automatically. ShieldX provides a security policy definition language that uses the native tagging scheme while offering a more robust user defined tagging scheme. Upon discovering the tagged workload, ShieldX automatically deploys the appropriate security controls in accordance with policy. ShieldX also provides a unique virtual patching capability that integrates directly with industry-leading vulnerability scanners from vendors such as Rapid7.
Requirement 7: Restrict access to cardholder data by business need to know	7.2.1 7.2.3	Granular, policy-based control over applications and content, enables organizations to implement a Zero Trust policy, limiting access to cardholder data systems based on business need with deny all policy for everything else.

Requirement 8: Assign a unique ID to each person with computer access	n/a	
Requirement 9: Restrict physical access to cardholder data	n/a	
Requirement 10: Encrypt transmission of cardholder data across open, public networks	10.1 10.2 10.2.1 10.2.2 10.2.3 10.2.4 10.2.5 10.2.6 10.2.7 10.3 10.3.1 10.3.2 10.3.3 10.3.4 10.3.5 10.3.6 10.4 10.6 10.6.1 10.6.2 10.6.3	ShieldX Elastic Security Platform maintains extensive logs/audit trails for configurations, system changes, alerts, traffic flows, threats and URL filtering. The solution also supports both daily and periodic review of log data with both native, customizable reporting capabilities and the ability to write log data to a syslog server for archival and analysis by third-party solutions (including popular security event and information management systems, such as Splunk®).
Requirement 11: Regularly test security systems and processes	11.4	ShieldX Elastic Security Platform fully inspects all allowed communication sessions for threat identification and prevention. A single, unified threat engine delivers intrusion prevention, stream-based anti-malware prevention, and blocking of content. Our cloud-based file analysis engine extends these capabilities further by identifying and working in conjunction with on-premise components to prevent unknown and targeted malware and exploits. The net result is comprehensive protection from all types of threat in a single pass of traffic.

Requirement 12: Maintain a policy that addresses information security for all personnel	n/a	

CONTROLLING PCI DSS SCOPE

The PCI Security Standards Council information supplement "Guidance for PCI DSS Scoping and Network Segmentation" makes it clear that organizations should give serious consideration to which elements of their business systems are within scope. The guidance puts it succinctly: "when properly implemented, network segmentation is one method that can help reduce the number of system components in scope for PCI DSS."

The ShieldX Elastic Security Platform are embedded in the pathways among application components and these pathways are controlled to provide separation among components. The scaling advantages of the cloud are preserved without sacrificing security and while maintaining isolation of individual tiers in the architecture. If you place your in-scope PCI workloads in specific tiers, other tiers can be clearly shown to be out of scope for compliance.

If you want to reduce the complexity of your PCI assessments, reducing the number of network segments where PCI compliance is required accomplishes this in one broad stroke.

Compliance is a universally challenging element of security operations, but ShieldX believes that establishing the right framework for security within the data center gives you an advantage that makes several fundamental requirements inherently built-in from day one.

ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110 USA

+1 408.758.9400
info@shieldx.com
www.shieldx.com

October 2019