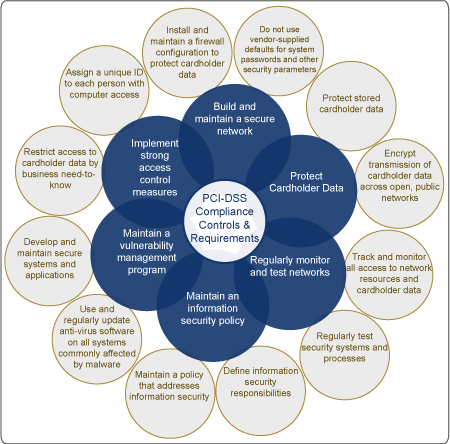
# PCI PAAS requirements

The Payment Card Industry Data Security Standard (PCI DSS) provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed and/or transmitted by merchants and other organizations.

This document details out how our solution helps in meeting these 12 requirements.

The following graphic shows the [objectives of PCI DSS and related 12 requirements](https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf):



Source: http://www.nasi.com/pci-dss-assessment.php

* Build and maintain a secure network
* Protect cardholder Data
* Regularly monitor and test networks
* Maintain an information security policy
* Maintain a vulnerability management program
* Implement strong access control measures

## Requirement 1: Install and maintain a firewall configuration to protect cardholder data

To establish and implement firewall and router configuration standards:

* Our solution identifies all connections between the cardholder data environment and other networks, including any wireless networks.
* It shows all cardholder data flows across systems and networks.
* Firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
* Review firewall and router rule sets at least every six months.

To build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment:

* Restricts inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
* Secures and synchronizes router configuration files.

**Note**: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.

To prohibit direct public access between the Internet and any system component in the cardholder data environment:

* A DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
* Limited inbound Internet traffic to IP addresses within the DMZ.
* Unauthorized outbound traffic is not allowed from the cardholder data environment to the Internet.
* Only “established” connections are permitted into the network.
* System components are placed that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
* No disclosure of private IP addresses and routing information to unauthorized parties.

**Note**: Methods to obscure IP addressing may include, but are not limited to:

• Network Address Translation (NAT)  
• Placing servers containing cardholder data behind proxy servers/firewalls,   
• Removal or filtering of route advertisements for private networks that employ registered addressing,   
• Internal use of RFC1918 address space instead of registered addresses

## Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

To 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.

Sources of industry-accepted system hardening standards may include, but are not limited to:

• Center for Internet Security (CIS)  
• International Organization for Standardization (ISO)  
• Sysadmin Audit Network Security (SANS) Institute  
• National Institute of Standards Technology (NIST).

* Our solution implements only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)  
    
  **Note**: Where virtualization technologies are in use, implements only one primary function per virtual system component.
* Enables only necessary services, protocols, daemons, etc., as required for the function of the system.
* Implements additional security features for any required services, protocols, or daemons that are insecure.  
    
  **Note**: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.
* Configures system security parameters to prevent misuse.
* Removes all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Other features of our solution under this category are:

* Encrypts all non-console administrative access using strong cryptography.  
    
  **Note**: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.
* Ensures that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
* Shared hosting providers protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.