Payment Card Industry Data Security Standard (PCI DSS)

Requirements and Security Assessment Basics – PCI DSS v3.2.1

The payment card industry compliance and validation regulations apply to financial institutions, Internet vendors and retail merchants. The rules spell out what security measures must be taken to protect the private information of customers, employers and employees during any transaction occurring with the use of a payment card. They also require certain auditing procedures. The Payment Card Industry (PCI) Data Security Standard (DSS) is used by all card brands to assure the security of the data gathered while an employee is making a transaction at a bank or through a participating vendor.

In the wake of high-profile identity theft and fraud concerns, VISA and MasterCard are now requiring organizations that process cardholder data to comply with their PCI DSS standards. PCI details twelve key requirements designed to reduce the risk from the electronic transmission of cardholder data and devotes substantial focus on the development and maintenance of secure systems and applications.

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data.

Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1 – May 2018

The PCI DSS version 3.2.1 is the global data security standard adopted by the card brands for all organizations that process, store or transmit cardholder data. It consists of common-sense steps that mirror best security practices.

PCI Data Security Standard – High Level Overview

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

PCI DSS Standards Overview

PCI DSS comprises a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. PCI DSS requirements apply to organizations and environments where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted.

Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no Primary Account Number (PAN) in the environment.

How Blue Ridge Assists with PCI DSS Compliance

Blue Ridge Networks Inc.'s LinkGuard Secure Cloud Defined Network ("SCDN") products, coupled with its managed services, support complying with PCI DSS Requirements as noted within this document. The Blue Ridge statements can assist in describing Compensating Controls for requirements where necessary.

The LinkGuard SCDN product line prevents external network breaches with an affordable solution that is simple to implement, easy to deploy, and doesn't force organizations to constantly react to cyber threats. Even the most complex systems can be up and running in minutes — with little to no augmentation of your existing system structure.

SCDN outperforms complex and insecure solutions like firewalls, conventional VLAN segmentation, and traditional VPNs like TLS or IPsec. LinkGuard has been heavily tested, protecting both U.S. national security assets as well as commercial entities for well over 20 years with no confirmed security breaches of the LinkGuard solution, using its devices and technology.

LinkGuard products are Type 1 Encryptors that create secure tunnels between configured LinkGuard endpoints, and only those endpoints.

The results are secure layer 2 network segments within a secure boundary termed the Enclave network. These SCDN devices are deployed as a simple overlay of the existing network with little to no configuration changes required to the underlying system network.

The LinkGuard SCDN Encryptors (BorderGuard and RemoteLink components) are neither routers nor firewalls. Network traffic only passes through the secure tunnels. LinkGuard devices do not provide a routable path to an untrusted external LAN or WAN. By adding a Blue Ridge managed Firewall/Gateway to the Enclave network(s) approved network, traffic can be permitted to specified destinations while preventing ingress/egress of unapproved network traffic.

The SCDN solution dramatically reduces attack surfaces by eliminating ingress/egress between the trusted Enclave network(s) and the underlying LAN/WAN through the use of Blue Ridge Networks' patented proprietary encryption model that eliminates man in the middle vulnerabilities of traditional VPN solutions like TLS/IPSEC.

PCI Requirements Detail: Blue Ridge LinkGuard SCDN and Managed Service Value

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

Blue Ridge Networks LinkGuard SCDN Solution Value:

LinkGuard SCDN components are Type 1 Encryptors that create secure tunnels between configured endpoints. The results are secure layer 2 networks with a secure boundary termed the Enclave Network. The LinkGuard SCDN Encryptors (BorderGuards and RemoteLinks) are not routers or firewalls. Network traffic only passes through the secure tunnels. There is no path to an external LAN or WAN.

This requirement states that other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls in this requirement. This design meets and/or exceeds the protection offered by traditional firewalls and/or existing network segmentation strategies.

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

Blue Ridge Networks SCDN Solution Value:

LinkGuard products are shipped pre-configured and are not configurable in the field through any web or console-based method. Encryption is handled by pre-placed encryption keys that do not rely on any passwords at all, therefore meets the requirement to restrict passwords from being determined via public information.

Requirement #3: Protect cardholder data

Blue Ridge Networks LinkGuard Solution Value:

LinkGuard devices will only establish secure encrypted tunnels with other LinkGuard devices. All data traversing through SDCN tunnels is fully protected. LinkGuard devices will ignore all attempts to penetrate the network, whether malicious or not.

Requirement #4: Encrypt transmission of cardholder data across open, public networks

Blue Ridge Networks LinkGuard SCDN Solution Value:

LinkGuard devices will only establish secure encrypted tunnels with other LinkGuard devices. All data traversing through LinkGuard tunnels is fully protected. The LinkGuard system uses AES256 encryption, HMAC-SHA256 integrity checking, and 2048-bit RSA keys. These protocols meet or exceed this requirement for encrypted transmission of cardholder data.

Requirement #5: Protect all systems against malware and regularly update anti-virus software or programs

Blue Ridge Networks LinkGuard SCDN Solution Value:

LinkGuard devices will only establish secure tunnels with other LinkGuard devices. LinkGuard SCDN products do not present any attack surface to malware and viruses, and do not contain any operating systems. Rather, LinkGuard components contain proprietary firmware which Blue Ridge maintains. No signatures, scanning, or updates are needed to continue to provide protection against malware.

Requirement #6: Develop and maintain secure systems and applications

Blue Ridge Networks LinkGuard SCDN Solution Value:

Blue Ridge Networks LinkGuard products have zero external attack surfaces. By design they will not interoperate nor establish any communication or security association with third-party products. The LinkGuard encryption model does not possess any of the remote exploit or man-in-the-middle attack surfaces of TLS and/or IPSEC based solutions. The identity of the remotely connecting LinkGuard device is guaranteed by the pre-placed encryption keys on both the local and remote LinkGuard devices. These cannot be altered in the field after deployment by anyone.

Requirement #7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. PCI compliance requires that the cardholder data from the PoS device is encrypted on the local area network. SCDN augments this security and enhances it across the company's wide area network. No unauthorized user is allowed to enter the secure network segment created by the SCDN device.

Requirement #8: Identify and authenticate access to system components

Blue Ridge Networks Managed Service Value:

Managed Service Head Equipment is housed within locked cages in secure data center facilities. Access to the data center facility requires multi-factor and biometric identification for physical access. Access is restricted to authorized Blue Ridge Secure Operations Center ("SOC") personnel. Managed Service System Access from the Blue Ridge Secure Operations Center to the data center facility is over encrypted SSH or TLS communication protocols. All routing of SOC to data center network traffic is secured by LinkGuard encrypted tunnels adding and additional encryption layer when accessing Managed Service Systems. There is no capability for unauthorized access to the Managed Service Systems.

Requirement #9: Restrict physical access to cardholder data

Blue Ridge Networks Managed Service Value:

Managed Service Head Equipment is housed within locked cages in secure data center facilities. The access to the data center facility requires multi-factor and biometric identification for physical access. Access is restricted to authorized Blue Ridge SOC personnel. There is no capability for unauthorized access to the Managed Service Systems.

Requirement #10: Track and monitor all access to network resources and cardholder data

Blue Ridge Networks Managed Service Value:

Blue Ridge monitors and logs access to the devices under its administrative control.

Requirement #11: Regularly test security systems and processes

Blue Ridge Networks Managed Service Value:

Regular vulnerability and threat assessments are performed on managed service environments to ensure the integrity of the security configuration. These environments include both remote site locations as well as the secure collocation facilities.

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

It is up to the company to create and maintain employee security policies that address internal information security. Blue Ridge Networks maintains information security policies for its personnel.

What's Next?

PCI DSS 4.0 will be released sometime in late 2020, with the basic 12 requirements expected to remain. Credit card data security standards are predicted to tighten in four specific areas. Blue Ridge will help you map to these possible areas of change:

1. Authentication – Deeper focus on NIST MFA/Password guidance
2. Encryption – Broader applicability on trusted networks
3. Monitoring – technology advancement requirements
4. Critical control testing and frequency methods – possible inclusion of Designated Entities Supplemental Validation requirements

Be sure to check with Blue Ridge and determine how LinkGuard SCDN can help you keep up.

Blue Ridge Networks Contact Information

Blue Ridge Networks, Inc.
14120 Parke Long Court #103
Chantilly, VA 20151
USA
800-722-1168
www.BlueRidgeNetworks.com
sales@blueridgenetworks.com