Solution Brief

Addressing PCI DSS Compliance with Enterprise Security from Broadcom® Software

Challenge

PCI DSS compliance has become a business requirement for any company involved in processing credit card information. It requires strong security controls over all systems and applications that process or store cardholder information. These controls serve to enforce rights to all confidential information, and to identify and remediate areas of potential exposure of customer credit card information.

Opportunity

Broadcom® Software provides strong controls over access to your network, applications, and data, no matter where they reside or how they are accessed. Using proven security solutions, Broadcom Software helps organizations achieve PCI DSS compliance by ensuring the privacy of all confidential cardholder information, and identifying and prioritizing areas of potential exposure.

Benefits

PCI DSS compliance requires comprehensive security across a range of systems and applications. Embracing the principals of Zero Trust and Secure Access Service Edge (SASE), Broadcom Software delivers a comprehensive security approach to help address PCI DSS compliance. Our security solutions can protect cardholder data regardless of where it is used or stored: on the mainframe, on-premises, or in the cloud. Our solutions also leverage security data to build intelligent usage patterns that improve threat detection for users and devices attempting to access this data.

The Payment Card Industry Data Security Standard (PCI DSS) mandates controls over card holder data to reduce the chances of credit card fraud. Although compliance became mandatory in 2018, Verizon[1] found that only 27.9% of organizations achieved 100% compliance during their 2019 interim compliance validation.

Overview

PCI DSS was first introduced in 2004. Originally it was considered best practices to implement, but in February 2018 the standard became a mandatory requirement for any organization processing credit card payments. Validation is required annually, and over the years, the standard has evolved with new revisions. The latest version 4.0 was released as a draft in 2020 for comment, and is expected to be published in early 2022.

Although PCI DSS does not mandate specific technologies or products, it does define how credit card information should be handled, communicated, and stored in order to reduce the probability of unauthorized access to that information. Many of the requirements relate to strengthening the perimeter to ensure “bad guys” don’t get access to internal systems or data. In addition, there are also a number of requirements whose sole purpose is to limit the access of employees to guard against both accidental breaches and malicious insider attacks.

There are six major categories of goals in the standard, each of which has a small number of key requirements, as shown in the table on the following page. These requirements are further delineated into a large set of specific statements defining what is needed for compliance. At a high level, these requirements address a broad range of security measures. This brief will describe how the Broadcom Software Enterprise Security solutions can help achieve compliance with these relevant major categories.

The Broadcom Software Security Portfolio

Security is a significant component of today’s IT infrastructures. In a dynamic computing environment with a variety of assets that need to be protected, as well as a large and diverse user population, it is critical to ensure the following (also continued on the following page):

- Protection of critical assets and endpoints from malicious code, such as viruses, worms, keyloggers and rootkits, as well as malware and ransomware
- Proactive risk mitigation by identifying and remediating system vulnerabilities

1: Verizon Payment Security Report, 2020.

Category	PCI-DSS Requirements
Build and Maintain a Secure Network and Systems	• Install and maintain a firewall configuration to protect cardholder data. • Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	• Protect stored cardholder data. • Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	• Protect all systems against malware and regularly update anti-virus software or programs. • Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	• Restrict access to cardholder data by business need-to-know. • Identity and authenticate access to systems components. • Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data. • Regularly test security systems and processes.
Maintain an Information Security Policy	• Maintain a policy that addresses information security for all personnel.

- Centralized enforcement of access policies for protection of cloud, virtual, and hybrid environments, as well as the applications and data that run or reside in these environments
- Automated provisioning and governance of digital identities to ensure least privileged access
- Improved authentication to ensure that users and devices are whom they claim to be
- Integrated analytics to monitor user activities and automatically trigger mitigating actions when unusual or risky behavior is detected

Broadcom Software leads the industry by providing an integrated set of security management solutions that includes the following:

- API Security to integrate apps, mobile, and IoT—bringing security, single sign-on, and identity management to the latest connected devices
- Endpoint Security to safeguard your laptops, desktops, mobile devices, servers, applications, cloud workloads, containers, and storage devices
- Identity Security to enforce granular security policies to stop unauthorized access to sensitive resources and data while providing seamless access to trusted users
- Information Security to protect your users, applications, and data everywhere with the most comprehensive data access and protection platform
- Mainframe Security to deliver identity and access management, compliance and data protection on the system that stores and processes the majority of PCI data
- Network Security to stop inbound and outbound threats that target your users, information, and key infrastructure while enabling quick access to data and applications wherever they reside
- Payment Security to reduce CNP fraud with the largest global e-commerce authentication network, industry-leading data science and patented analytics

These solutions help you determine and control who has access to applications and systems storing and processing cardholder data, determine what is happening in your environment, and combat major categories of online threats. In this way, they can help you achieve operational efficiencies and regulatory compliance, as well as contain costs, mitigate risk, and ensure continuous business operations.

Achieving PCI DSS Compliance with Enterprise Security from Broadcom Software

Compliance with PCI DSS requires the implementation of stronger controls on any system that is processing or storing credit card holder data. Some of these requirements are purely process-related, but most can be either achieved or aided through the use of technology in addition to improved security processes. The following sections describe how the various Broadcom Software security solutions can address the major requirements of the PCI DSS standard.

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect data

The traditional approach to securing the network and systems was to install and maintain a firewall, and while this is still a critical technology, the network perimeter has been rendered obsolete by a perfect storm of mobile users, remote workforce, cloud applications and infrastructure, and evolving security threats. Network and security teams need solutions that protect credit

card and cardholder data and payment applications that can exist outside their own data center around the clock, but still be accessed and used from any location.

Symantec® Secure Access Service Edge (SASE) helps organizations to achieve all the benefits of digital transformation and addresses these security challenges by converging network and security-as-a-service into a cloud-delivered service model that provides a complete range of integrated, best-in-class network security capabilities for low-latency cloud and Internet access. The heart of our SASE solution is the Symantec Web Security Service, which includes a secure web gateway, software defined perimeter, anti-virus scanning, sandboxing, web isolation, data loss prevention, and email security. This cloud-delivered network security service enforces comprehensive Internet security and data compliance policies, regardless of location or device.

2. Do not use vendor-supplied defaults for system passwords and other security parameters
Many organizations do change vendor-supplied defaults for system passwords, however, these credentials are still often shared and known by multiple internal, and sometimes external, individuals who need access to these accounts to perform key activities. These accounts generally provide elevated and unrestricted access that, if compromised, would enable a malicious user to access and steal card holder data. Even worse, cloud-based and virtualized environments, combined with the adoption of continuous delivery, have exponentially expanded the number of privileged accounts that could be compromised.

Symantec Privileged Access Management (PAM) allows organizations to create and enforce controls over users, accounts, and systems that have elevated or "privileged" entitlements by vaulting these credentials and forcing users to uniquely identify themselves before gaining access to them. Our solution can enforce policies to ensure users can only use those credentials they are authorized to access and provide a complete audit trail of all activities performed by each user while they had access to a privileged credential. The solution can also continuously monitor privileged activity to assess risk based on unusual behavior and trigger automatic mitigations actions when risk thresholds are exceeded. Additionally, Symantec PAM can serve as the jump host into PCI environments, covering many access and logging requirements downstream by requiring two-factor authentication, recording the privileged sessions, and preventing leapfrog connections.

Protect Cardholder Data

3. Protect stored cardholder data
The primary objective of PCI DSS is to protect stored credit card holder data, so the first question is: what data needs to be protected and what data can be stored? The standard allows for the following data elements to be stored: Primary Account Number (PAN), Cardholder Name, Service Code, and Expiration Date. The following data cannot be stored, but is often used in authentication so is captured and processed: Full Track Data (from magnetic strip), Security Code (CAV2/CVC2/CVV2/CID3), and PIN/PIN Block. Most of this data is directly from the credit card; however, cardholder name may be stored in multiple systems, and therefore must be protected everywhere (in addition, this data is often covered as PII data under most data privacy laws).

Symantec Information Security secures data stored on-premises and in the cloud. It provides total visibility and control of data flowing in, out, and across your organization's extended perimeter. Our leading DLP solution integrates with CASB, web, and email gateway technologies to find data stored on endpoints, servers, file shares, databases, SharePoint, and more. Underpinning the integration is a single data protection policy giving you consistent and up-to-the-minute protection, avoiding the hassle of policy duplication. Additionally, many financial institutions still process and store cardholder data on their mainframes, and our mainframe identity, access, and data compliance solutions can safeguard this data.

4. Encrypt transmission of cardholder data across open, public networks
Symantec Encryption solutions protect cardholder data—wherever it is. Symantec Endpoint Encryption protects sensitive information and ensures regulatory compliance by encrypting all files on the hard drive, sector-by-sector, for maximum security. It supports Windows, macOS, tablets, self-encrypting drives, and removable media (USB drives, external hard drives, and DVDs). For maximum flexibility, Symantec Endpoint Encryption also manages BitLocker and FileVault-protected devices. Symantec Email Encryption protects card holder data by encrypting emails from the client, mobile devices, or at the gateway, ensuring that this data remains encrypted while in transit or when it is stored on the mail server, backup server, and storage systems. Finally, Symantec File Share and Command Line Encryption can ensure that files remain encrypted if moved, copied, or distributed, and can protect data when used in large batch jobs.

Another point of attack is the communications between devices and corporate applications and resources, which are predominantly done using APIs. Symantec addresses this threat vector with its Layer7 API Management solution, which is a lightweight, low-latency mobile gateway with integrated security and management controls designed to help enterprises safely and reliably expose internal assets to developers and remote apps as mobile APIs. Additionally, it is FIPS 140-2 out of the box, and can be configured for both FIPS 140-3 and PCI-DSS compliance.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs

The heart of any vulnerability management program is to use and regularly update anti-virus software or programs because properly protecting endpoint devices addresses one of the primary beachheads used by external hackers to initiate a breach. Symantec Endpoint Security meets this challenge through innovative technology that addresses the entire attack chain: attack surface reduction, attack prevention, breach prevention, and detection and response.

Symantec defends endpoints proactively with advanced policy controls and technologies that scan for vulnerabilities and misconfigurations across applications, Active Directory, and devices connecting to the endpoint, and then it proceeds with hardening the system and locking down processes and behaviors to render many attacker tactics and techniques ineffective. Symantec also stops attacks during the initial infection attempt by quickly identifying threats and blocking these attacks to prevent infection, maintain endpoint integrity, and avoid compromise.

6. Develop and maintain secure systems and applications

Another critical aspect of vulnerability management is to ensure that all system components have the latest vendor-supplied patches and are configured to industry best practices. To help accomplish this, Symantec Control Compliance Suite automates IT assessments through agent and agentless scanning with 15,000+ configuration checks for over 75 platforms so you can quickly identify and prioritize misconfigurations so that they can be quickly remediated. It automates assessments of technical controls that require secure configuration settings by using network and asset discovery—including for third-party systems such as POS. A single IT assessment can be mapped to numerous regulations, with audit-ready reports and dashboards included to show auditors. Additionally, Control Compliance Suite also automates the ability to demonstrate compliance through pre-package support for over 100 regulations, mandates, and best practice frameworks, including GDPR, HIPAA, NIST, PCI DSS, and SWIFT.

Furthermore, Symantec IT Management Suite helps manage, patch, and remediate application and OS configurations on desktops, laptops, and servers throughout their lifecycle to strengthen endpoint security and maximize user productivity. Our solutions are extremely versatile with support for all major operating systems, real-time and persistent management of endpoints inside and outside the perimeter, and extensive deployment, asset management, and patch management capabilities.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know

Access to systems, applications, and data that are storing and processing cardholder data must be tightly restricted to only individuals who have a clearly defined need to obtain this information. Although one of the shorter sections in the entire PCI standard, it is very broad in its scope and its compliance may require the most effort of any requirement in the entire standard.

One approach that has gained popularity recently that ensures that access to all systems, applications, and data is tightly restricted to only those people who have a clearly defined need is Zero Trust. Achieving Zero Trust is a journey and requires the integration of many types of security tools that have traditionally operated in their own silos. Many of these tools may already exist within your enterprise, some delivering value but likely with the potential to deliver even more. Customers need a partner to weave all of these disparate systems together—a partner who can also help fill in the gaps where they exist. Broadcom is that strategic partner. Our Symantec security portfolio delivers endpoint, network, information, and identity security across on-premises and cloud infrastructures, to provide the most complete and effective Zero Trust solution in the industry. Our Integrated Cyber Defense technology can weave these products and your existing security solutions into a platform that can secure your workforce, your data, and your workloads to deliver superior visibility and control.

The Zero Trust approach is focused primarily on enforcing controls over which users, applications, and devices are allowed to connect to the network and access sensitive data, in this case, card holder data.

But they do not often ask the question – is this access really needed and should it have been given in the first place. To address these questions, organizations need to periodically review and certify that users' access entitlements are necessary to do their jobs. Symantec IGA addresses this challenge by automatically gathering user access rights, either for all systems or just those covered by regulations such as PCI DSS, and presents this data to reviewers in an easy-to-use and customizable interface. Reviewers can then easily review and certify or reject this access. Additionally, risk-level contextual information is provided to help reviewers focus their attention riskier users first, and all rejected access can be immediately removed and all decisions are logged to support compliance audits.

8. Assign a unique ID to each person with computer access

This section of the standard includes a number of specific identity security requirements that can be summarized as follows: All actions taken on cardholder data and payment systems are performed by, and can be traced to, known and authorized users. In general, enterprise identity and access management systems, such as SiteMinder, are already providing these controls and addressing these requirements for your business users already. For example, SiteMinder can identify all users with a unique username/ID and track all activity back to this ID, even if their username differs from app to app or system to system. SiteMinder can also enforce a variety of authentication methods based on the sensitivity of the application or the data being accessed. Symantec VIP provides strong authentication through transparent risk analysis and software-based or hard token 2FA credentials. And once authenticated, SiteMinder can manage the user's session, terminating it based on defined time limits or inactivity.

Where this requirement often becomes difficult is with shared or system accounts as the user's identity is often masked and audited simply as root or superuser. Symantec PAM can help to address this issue by forcing users to first authenticate to PAM before granting access to these accounts. In this way, Symantec PAM can link the user's actual identities to the account and ensure that all privileged activities that they perform can be traced to their actual identity to ensure full accountability.

9. Restrict physical access to cardholder data

In general, most organizations have physical access control systems (PACS) that restrict physical access to critical infrastructure, such as servers running or processing cardholder data. However, the third principle of Zero Trust is to assume breach, which should be interpreted to assume that the PACS can and will be breached. This would give an unauthorized and potentially malicious user direct physical access to cardholder data. Symantec PAM can address this concern through its server control agents, which provide host-based access control.

Server Control agents are installed directly on the servers they protect, and therefore cannot be bypassed if a malicious user gains direct access to a physical server. Symantec PAM server control agents provide file, directory, and resource-specific, kernel-level controls, registry protection, and other localized granular controls to ensure that high-value assets and resources hosted on critical servers are protected from damages caused either by malicious or accidental insider actions. These controls cannot be stopped or bypassed, even by a superuser.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

Your network is the lifeblood of your organization. In the cloud, on-premises, or both, you must stop inbound and outbound threats that target your end users, information, and key infrastructure. One wrong click can put your network at risk. Symantec Network Security protects it with comprehensive, advanced web and email security solutions. Additionally, as organizations have shifted their applications to cloud environments, security concerns have been raised. And although most cloud infrastructure puts strong safeguards in place to help protect customer privacy, there is often a lack of visibility into who is using the cloud and how they are using it, especially when it comes to large workloads of sensitive data that may be stored and/or processed in the cloud.

Symantec CloudSOC CASB empowers organizations to confidently enable cloud applications and services while helping them stay safe, secure, and compliant with the following benefits:

- Monitoring, logging, and analyzing user and admin activity
- Enforcing access controls to prevent misconfigurations
- Detecting and remediating risky exposures in different cloud instances
- Defending cloud storage from advanced malware and APTs
- Detecting compromised accounts with user behavior analytics
- Detecting and restricting misuse and "shadow" cloud instances

Finally, Symantec Security Analytics provides complete visibility and advanced network traffic analysis to enable real-time threat detection. With enriched, full-packet capture, Symantec Security Analytics can monitor all network traffic, including thousands of applications, dozens of file transports, all flows, and all packets—including encrypted traffic when deployed with Symantec SSL Visibility. The total forensic data analysis of your network traffic yields actionable intelligence so you can quickly shut down exposure and mitigate ongoing risk.

Summary

Compliance with the requirements of the PCI standard has become a business imperative for firms processing significant numbers of credit card transactions, or providing any type of credit card services to another organization. Although these requirements are based on industry best practices, it is unlikely that most organizations would comply with this standard without improvements to their IT security processes and systems.

Compliance with PCI requires a concerted effort, typically involving multiple groups within the organization. Although changes to various IT processes are usually involved, the adoption of specific technology solutions can greatly aid the compliance effort. And it should be noted that many of the requirements of the PCI standard are reflected in other emerging compliance mandates; the data that needs to be protected may change, but key requirements are identical in many cases, so addressing PCI compliance will help the organization to be in a better position to address GDPR, HIPAA, and so on.

Broadcom Software is a world leader in business-critical software, modernizing, optimizing, and protecting the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

BROADCOM® SOFTWARE

For more product information: broadcom.com

PCI-DSS-Compliance-SB100 January 11, 2022