TRUST IN
GERMAN
SICHERHEIT

G DATA Whitepaper

Meet PCI DSS requirements with G DATA

G DATA Software AG | December 2017

Introduction

Information technology has dramatically influenced existing ways of doing business. Digital workplaces, networked point-of-sale terminals and centralized customer databases provide tangible advantages to enterprises and SMBs and their customers, such as increased efficiency and lower costs. However, digitization also comes with its own set of risks. Networked devices enable connected functionality but can also be abused by criminals to gain unauthorized access to internal data. Data theft directly affects customers and business operations and can lead to considerable financial damages.

In order to combat the risks of digital workflows involving credit card data, the major credit card organizations founded the Payment Card Industry Security Standards Council and developed a standard for dealing with credit card data. All companies that process credit card data are bound by the Payment Card Industry Data Security Standard (PCI DSS) and can be found liable in case of a data breach. G DATA solutions assist enterprises that want to protect credit card data and ensure PCI DSS compliance. This whitepaper will discuss the PCI DSS standard and describe how G DATA can help administrators meet PCI DSS requirements.

1. PCI DSS

The PCI DSS standard was first introduced in 2004 by merging the data security policies of the credit card organizations that founded the PCI Security Standards Council. Its goal is to protect account data of credit card holders. PCI DSS explicitly sets a minimum level of requirements. Companies are free to implement additional measures to further increase data protection. The standard does not replace any laws or regulations; its requirements are set in addition to them.

1.1. Scope

Every company that processes credit card data in one form or another falls under PCI DSS requirements. First of all, companies must be aware of the types of data to which PCI DSS applies. The standard distinguishes between two types: cardholder data and sensitive authentication data. Card holder data, which includes the credit card number, cardholder name, service code and expiration date, may be stored. Sensitive authentication data, on the other hand, may be processed but must never be stored. Both are subject to the PCI DSS requirements.

Secondly, the systems that may process card holder data and thus fall within the scope of PCI DSS must be listed. PCI DSS states that its requirements apply to all systems that are connected to or included in the cardholder data environment (CDE). As examples, the standard names servers (such as web servers or mail servers), network components such as firewall and access points, applications, and every other component or device that is connected to the CDE. In practice, this means that the entire IT infrastructure of any company that processed credit card data must comply with PCI DSS standards. Alternatively, the CDE can be limited by performing network segmentation and separating the part of the network that processes cardholder data from the part that does not. Especially in the context of wireless networking, the possible implications of network design for PCI DSS compliance must be evaluated when setting up the infrastructure.

Third-party service providers also fall under the scope of PCI DSS, if a company exchanges cardholder data with them. For example, this may be the case when utilizing a third party to manage the payment process, or when an external party takes care of company hardware or software (such as cloud providers).

1.2. Assessment

Companies that fall within the PCI DSS scope must undergo a regular PCI DSS assessment, which checks whether the company is compliant with the requirements. Assessment parameters depend on the validation level of the merchant and on the credit card provider. For example, a level 4 Visa merchant (processing fewer than 20,000 Visa transactions per year) must at least submit an Attestation of Compliance (AOC) form and complete a yearly Self-Assessment Questionnaire (SAQ) in which they validate their PCI DSS compliance. Larger companies, however, face stricter procedures: level 1 Visa merchants (over 6 million Visa transactions) must file a Report on Compliance, which has to be completed by a Qualified Security Assessor (QSA) or an internal auditor, in addition to the AOC form. The level structure varies between credit card providers, but the AOC and SAQ components are universal. Third party service providers must also validate their PCI DSS compliance, either through an annual assessment of their own or by only carrying out an on-demand assessment when a customer asks for it.

1.3. Structure

The PCI DSS standard has six general categories with altogether twelve requirements, each of which contains a number of individual measures:

- 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

Each requirement lists a number of sub-requirements or measures, which can range from technical configuration to policy and workflow implementations. For each measure, the standard offers additional guidance and testing procedures to make sure compliance exists.

2. Meet PCI DSS requirements with G DATA

G DATA business solutions can help enterprises to sustainably meet PCI DSS requirements by supporting workflows and policies and implementing technical measures. Compliance is an ongoing process: infrastructure or personnel changes can affect its status. G DATA software offers functionality that helps administrators to implement and monitor the status of compliance.

The individual PCI measures are a mixture of technical measures and policy-making decisions. Not all measures can be supported by security software. For that reason, this whitepaper only offers general guidance on the areas of PCI DSS that G DATA can help with. To achieve full compliance and to ensure that the proper measures have been implemented, it is recommended to engage specialized PCI DSS consultancy services.

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

G DATA Client Security Business, Endpoint Protection Business and Managed Endpoint Security contain a client firewall, which helps provide security for networked endpoints (requirement 1.4). It can be configured to restrict traffic with the CDE to the necessary minimum (requirement 1.2). The firewall protects desktops as well as laptops, allowing flexible rules for devices that are used within as well as outside the corporate network. G DATA solutions can also be deployed in DMZ scenarios (requirement 1.3). The product documentation provides a clear overview of port and protocol configuration that is required to deploy G DATA solutions (requirement 1.1).

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

G DATA solutions can be configured using a comprehensive dashboard. This helps administrators quickly adapt protection settings to their needs (requirement 2.1). The clearly grouped and documented configuration modules enable administrators to quickly obtain information that is required by security policies and operational procedures (requirement 2.5). The solutions support the development of configuration standards by offering various deployment scenarios and by allowing administrators to configure machines based on group settings (requirement 2.2). Through the integration with existing Active Directory services as well as the comprehensive hardware and software inventory, administrators are always informed about components that may be in the scope of the PCI standard (requirement 2.4).

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

G DATA solutions provide endpoint protection for a wide range of operating systems including Windows, Mac, Linux, Android and iOS (requirement 5.1). Regular updates can be configured, as well as periodic scans, with logs being available through a clear console (requirement 5.2). By default, protection components cannot be disabled by the end user. Only if an administrator explicitly allows changes, security settings can be configured on the endpoint itself (requirement 5.3). The administrative dashboard offers a clear overview of settings and tasks, which supports the documentation of security policies and operational procedures. In addition, the ReportManager module allows administrators to regularly create tailor-made reports about the security status and configuration (requirement 5.4).

Requirement 6: Develop and maintain secure systems and applications

Requirement 6 focuses on making sure security vulnerabilities cannot be abused to gain access to systems, both technically and by using policies. A process for security vulnerability identification (requirement 6.1) can be set up in conjunction with G DATA Advanced Analytics, which offers consultancy services. With the help of the Patch Management module, patch testing and deployment can be automated, making sure that systems are protected from known vulnerabilities (requirement 6.2).

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

Access control measures can be implemented by creating a comprehensive policy and implementing technical measures using tools such as the PolicyManager module of G DATA Endpoint Protection Business and Managed Endpoint Security. For example, using Application Control, access to specific applications can be granted to only those employees who need access in order to carry out their job (requirements 7.1 and 7.2). The integrated dashboard of G DATA solutions supports the documentation of access control measures.

Requirement 8: Identify and authenticate access to system components

User account management of G DATA solutions is based on Windows credentials, which allows for fine-grained password-based user management (requirements 8.1 and 8.2). Alternatively, an integrated authentication system can be used.

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

Using the Network Monitoring module of G DATA solutions, administrators can stay on top of infrastructure events. Network Monitoring keeps track of a wide range of statistics on infrastructure components, such as CPU load, network traffic or runaway processes, in order to support administrators with identifying suspicious activity (requirement 10.6). The endpoint security components provide historical logs, which are available for immediate analysis (requirement 10.7).

Requirement 11: Regularly test security systems and processes

Similar to the identification of suspicious activity, Network Monitoring can be used to implement SNMP monitoring measures to check network infrastructure itself (requirements 11.1 and 11.4). Further tests, such as vulnerability scans and penetration tests can be implemented per separate agreement with G DATA Advanced Analytics (requirements 11.2 and 11.3). Change detection mechanisms are present to ensure the integrity of the G DATA endpoint security components (requirement 11.5).

Please note that this paper is not meant to replace seeking legal advice.