appgate

WHITEPAPER

MEET PCI DSS CONTROLS WITH SDP

INTRODUCTION

In April 2016, PCI DSS version 3.2 became effective. It expanded upon the previous 3.0 version released in January 2015 that made compliance an even more demanding task for organizations that handle payment card data. At the same time, continuing cyber-attacks have demonstrated that compliance alone is no guarantee that data is secure. To succeed in this environment, organizations need to abandon the uphill struggle of attempting to tackle both new PCI requirements and emerging cyber threats using traditional, inflexible network and information security solutions.

Appgate SDP can address some of the challenges of PCI compliance, when used by the enterprise with other specifically designed tools and as part of an overall enterprise information security vision.

This document demonstrates how a properly installed, configured and maintained Appgate SDP solution can be used to aid a customer in achieving PCI compliance.

PCI SECTION OVERVIEW SUMMARY

PCI DSS is divided into 12 sections, with three appendices for service providers. The following table is a breakout of the sections of the PCI DSS where Appgate SDP can help with compliance.

The following paper describes how Appgate SDP is applied to the latest compliance standards.

REQUIREMENT	DESCRIPTION	ADDRESSED BY APPGATE SDP
1	Install and maintain a firewall configuration to protect cardholder data	Yes
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	No
3	Protect stored cardholder data.	No
4	Encrypt transmission of cardholder data across open, public networks.	Yes
5	Protect all systems against malware and regularly update anti-virus software or programs.	No
6	Develop and maintain secure systems and applications.	No
7	Restrict access to cardholder data by business need to know	Yes
8	Identify and authenticate access to system components.	Yes
9	Restrict physical access to cardholder data.	No
10	Track and monitor all access to network resources and cardholder data.	Yes
11	Regularly test security systems and processes.	No
12	Maintain a policy that addresses information security for all personnel.	No

SECTION 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

SUMMARY

Firewalls control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the internet as e-commerce, employee internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement .

APPGATE SDP APPLIED

While having many of the same features of a firewall, Appgate SDP is not a firewall solution or replacement. It is a security tool that can be used in concert with an enterprise-grade firewall to control user access to network resources. With Appgate SDP properly configured, a user accessing an allowed network resource would never know that a separate, controlled network resource with cardholder data existed. Moreover, a user on a public network would need to authenticate with Appgate SDP before being allowed to access a resource containing cardholder data.

PCI CONTROLS ADDRESSED	
1.1 Establish and implement firewall and router configuration standards that include the following:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Appgate SDP can be used in conjunction with an enterprise class firewall system to provide additional security to networks and enterprise infrastructure. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.
1.1.4 Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone.	Using Appgate SDP to control every internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.
1.1.5 Description of groups, roles, and responsibilities for management of network components.	Access to network resources is controlled by granting user entitlements to resources via policy. This is part of the Appgate SDP Admin GUI. In Appgate SDP, administrative responsibilities can also be segregated and divided through multiple means, including a trouble ticket.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 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.	It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Appgate SDP is a the perfect tool to act as a trust between trusted and untrusted networks—only granting users access to resources (networks) in which they have specific reasons (entitlements) to access. For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity's network.

PCI CONTROLS ADDRESSED	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Appgate SDP only allows access to specific resources, and restricts all other traffic from access.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include, but is not limited to, corporate networks, retail stores, guest networks, warehouse environments, etc. Appgate SDP treats wireless networks as it would treat any other network—as part of an infrastructure in which a user must authenticate and be granted access before accessing the resource.
1.3 Prohibit direct public access between the internet and any system component in the cardholder data environment. 1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. 1.3.2 Limit inbound internet traffic to IP addresses within the DMZ. 1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. 1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the internet. 1.3.5 Permit only "established" connections into the network. 1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. 1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	Properly configured, a user accessing a public network would never know that a network with cardholder data existed. Moreover, a user on a public network would need to authenticate with Appgate SDP before being allowed to access a resource containing cardholder data.

SECTION 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

SUMMARY

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

APPGATE SDP APPLIED

Appgate SDP protects all the networks connected to an enterprise. Information is protected by the latest TLS encryption (section Appendix A2 is not required).

PCI CONTROLS ADDRESSED	
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to: • The internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS) • Satellite communications	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted.

SECTION 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

SUMMARY

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. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

APPGATE SDP APPLIED

Appgate SDP has a granular, principle of least privilege approach to user access. Users and administrators only have access to resources for which they are specifically authenticated.

PCI CONTROLS ADDRESSED	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	To limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, these roles can be assigned in Appgate SDP when the resource is defined and can be assigned to the individual user/groups accordingly
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges").For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Entitlements can be strictly controlled and enforced at a granular level, with administrators only having access and administrative rights to resources they are directly responsible for.
7.1.3 Assign access based on individual personnel's job classification and function. 7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: 7.2.1 Coverage of all system components 7.2.2 Assignment of privileges to individuals based on job classification and function. 7.2.3 Default "deny-all" setting.	Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access in Appgate SDP according to their job classification and function by using the already-created roles. Without a mechanism like Appgate SDP to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access control systems to manage user access.

SECTION 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

SUMMARY

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

APPGATE SDP APPLIED

Appgate SDP has a granular, principle of least privilege approach to user access. Users and administrators only have access to resources for which they are specifically authenticated.

PCI CONTROLS ADDRESSED	
8.1 Define and implement policies and procedures to ensure proper user identification management for nonconsumer users and administrators on all system components as follows: 8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Appgate SDP ensures that each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	Appgate SDP has a lockout mechanism to limit repeat failed access attempts. Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	If an account is locked out due to someone continually trying to guess a password, Appgate SDP can be configured to delay reactivation of these locked accounts and prevent the malicious individual from continually guessing the password. The account lock out can be reset in the Appgate SDP admin GUI by an administrator/ help desk.
8.1.8 If a session has been idle for more than 15 minutes, require the user to reauthenticate to re-activate the terminal or session.	Appgate SDP has a session timeout setting that can be configured by the administrator. When users walk away from an open machine with access to critical system components or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. Appgate SDP can also be configured to require periodic user re-authentication based on a variety of criteria, configurable by the system administrator.

PCI CONTROLS ADDRESSED	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	Multi-factor authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Appgate SDP uses a unique ID plus a token, in addition to apassword for user authentication.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. 8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including thirdparty access for support or maintenance) originating from outside the entity's network.	Multi-factor authentication is used by Appgate SDP to gain access to protected resources. It requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted.

SECTION 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

SUMMARY

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

APPGATE SDP APPLIED

Appgate SDP is not a logging tool nor a Security Information and Event Management (SIEM) solution. But—as all enterprise grade tools and solutions—Appgate SDP does have extremely robust logging and monitoring capabilities that can integrate with most third party SIEM tools.

PCI CONTROLS ADDRESSED	
10.1 Implement audit trails to link all access to system components to each individual user.	It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual user accesses to cardholder data 10.2.2 All actions taken by any individual with root or administrative privileges 10.2.3 Access to all audit trails 10.2.4 Invalid logical access attempts 10.2.6 Initialization, stopping, or pausing of the audit logs 10.2.7 Creation and deletion of system-level objects	Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Appgate SDP logs events applicable to system, user and resources that are controlled by Appgate SDP. Further, these logs can be used with a SIEM tool for event reconciliation and management.
10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.5 Origination of event 10.3.6 Identity or name of affected data, system component, or resource.	By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how. Appgate SDP logs can be used (in part) to track users, type of access, date and time, status of authentication (failed, successful, etc), where the user tried to authenticate from (device, etc.), and resources that the user authenticated to.