

safend

Securing Your Endpoints



Achieving PCI Compliance with the Safend Solution

This paper introduces you to the PCI compliance requirements and describes how the Safend Solution can enable you to comply with these regulatory requirements in your organization. It provides an overview of the threats posed by new technologies to PCI regulated organizations, how to prepare for them, and how the Safend Solution helps you address these threats.

Introduction

The PCI Security Standards Council is "an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection". The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard, and Visa. The council issues security compliance requirements to merchants that process, store, or transmit cardholder information. The PCI Data Security Standard (DSS) v1.2 published in November 2008 contains the current set of requirements for credit card merchants.

Specifically, the PCI DSS control objectives ensure that compliant organizations build and maintain a secure network; protect cardholder data; maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy. Ensuring security at the endpoints within a network that processes cardholder data is one of the issues that must be addressed by PCI-compliant organizations.

The Safend Solution enables you protect your sensitive data. By providing built-in security policies designed specifically for PCI compliance, it helps you achieve compliance, while at the same time maintaining the flexibility and granularity needed

to run your network smoothly. The solution's built-in policies allow single-click implementation, and are fully customizable to suit your exact needs.

PCI Compliance Requirements

PCI compliance requirements are probably the most detailed and specific compliance requirements currently published. Compared to HIPAA, SOX, or GLBA they have very specific requirements about the specific data that needs to be protected, as well as the recommended (or required) way to protect it. The requirements are divided into 12 main categories, which are further divided into sub-requirements. This paper will provide an overview of the requirements, and will detail the way in which the Safend Solution makes you compliant, where applicable. The first step in understanding the requirements is recognizing the type of data PCI-DSS is trying to protect and why. Table 1 includes data from the PCI DSS "Understanding the intent of the requirements" document.

	Data Element	Storage permitted	Protection required	PCI DSS Requirements 3,4
Cardholder Data	Primary Account Number	Yes	Yes	Yes
	Cardholder Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

It should be noted that sensitive authentication data should not be stored anywhere, under any circumstance. Cardholder data can be stored, but it must be protected. The nature of protection required for cardholder data, and the protection offered by the Safend Solution to answer those requirements, are both detailed in the sections that follow.

The Safend Solution Built-in PCI Compliance Feature

The Safend Solution helps organizations address the 12 PCI sub-requirements by providing built-in security policies designed specifically for PCI compliance. This feature includes detailed guidelines on how to configure, operate, and maintain the product for PCI compliance. The built-in policies include the recommended settings for PCI compliance that can be applied "as is" with a single click or can be modified to better accommodate your organization's specific security and business needs. To assist with this customization of policy settings, the Safend Solution includes detailed guidance, explaining the specific impact of the policy security settings and the associated mapping of these settings to regulatory policy statements.

The built-in compliance feature helps your organization readily achieve compliance while at the same time maintaining the flexibility and granularity needed to run your network smoothly.

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

This requirement refers first and foremost to a network level firewall to protect against hackers infiltrating your network. The requirement describes defining and managing a firewall policy, both on the endpoint and on the Enterprise routers.

However, sub-requirement 1.1.2 refers to maintaining a stable network topology diagram, without which the various firewall zones could be rendered useless.

Safend Protector, a component of the Safend Solution can help with this requirement since it offers a feature that blocks bridging of networks between WiFi, Bluetooth, or 3G Modems and the fixed enterprise network. Wireless bridging completely alters the network topology since it can connect two previously separate parts of the network, and create gaping holes in otherwise secure segments of the network.

This feature helps an organization avoid breach of PCI requirements, and maintain good security practices by turning off non-secured wireless access, so that TJX-like vulnerability is no longer available to a would-be attacker.

Requirement 2: Do not use vendor-supplied defaults for system passwords/security parameters.

This requirement applies to all systems, including the Safend Solution. In an age when doing a web search for "Default Password" yields close to 1M results, and the top 5 Google first page results are each compilations of at least 1000 different equipment types, The Safend Solution has no users or passwords that are hardwired or even pre-defined. Authentication is based on Active Directory groups, users and roles.

The default settings of Windows for device and port connections are all open by default. Installing Safend Protector provides a base policy where many of those ports

are only selectively enabled, thereby significantly decreasing the attackable footprint of the protected system. Safend Protector can block WiFi, Bluetooth, FireWire, USB and many other ports and override the default Windows settings.

Requirement 3: Protect stored cardholder data.

Cardholder data stored inside the organization must be protected. This protection must combine multiple layers of defense. The innermost layer is encryption of data on the hard drive itself. Section 3.4 in the PCI document details the recommended features for an encryption solution.

Stored cardholder data is protected by Safend Encryptor, a component of the Safend Solution, by encrypting the hard drives and removable storage devices where the data resides. Safend Encryptor encrypts all data on the drive using file based industry standard AES256 encryption, and safely stores the keys in a central location to allow recovery, if needed.

The recovery is possible only with the right administrator credentials, in agreement with requirement 3.6

The next layer of protection keeps the data from being removed from its protected endpoint. Safend Protector's Granular Port and Device control will allow only specific users to take out specific data from specific machines.

If Data has to be physically transferred, removable storage is a common way to backup and transmit large amounts of data to partners. Safend Protector automatically and seamlessly encrypts any removable media connected to a computer. Safend Protector creates a full usage trail of the encrypted transferred files, and maintains control of the data, even when the removable storage is used outside the organization by a partner, or remote worker.

Safend Protector also enables tagging of specific CDs, and can limit access to tagged CDs only, thereby blocking the connecting of any other CD or rewritable DVD, while still allowing encrypted burning of CDs and DVDs.

The Safend Solution's unique Content Inspection Integration component allows administrators to leverage existing 3rd party Content Monitoring and Filtering systems for controlling file transfers to external storage devices. With this technology, each file that is downloaded from an endpoint to an external storage device can be inspected to determine whether it contains any credit card data.

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

This requirement is best handled by using link-level encryption, such as TLS. In networks in which some of the data is physically transferred on CD, DVD or USB memory sticks, Safend Protector provides secure measures to protect any data transferred physically, by utilizing AES 256 bit encryption for removable media.

Safend Protector also enforces secure usage of WiFi networks, by limiting access to WiFi networks by type, by MAC and by SSID. The type of network (encrypted, non-encrypted, Infrastructure/Peer to Peer) can be enforced, as can be white listing of certain MAC addresses or SSID networks.

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

An anti-virus solution is important to make sure that no malware finds its way into the internal network, and that any malware that does end up there, is quickly removed. Malware today is capable of extracting sensitive data and sending it back to the Malware's distributors, and is often used to harvest personal information and specifically credit card numbers.

Safend Protector supplements solutions from vendors such as Symantec or McAfee by completely blocking the transfer of executables from and to removable storage devices. This protection enables blocking any USB borne threat, even if it is not yet recognized by the established vendors at the time of the attack.

Furthermore, it can granularly limit U3 autorun support further enhancing the granularity of control over USB originating Malware.

Requirement 6: Develop and maintain secure systems and applications.

This requirement refers to internal IT systems and applications. Safend Protector is an external application, so it does not contribute to this requirement. The thorough penetration and security testing performed on The Safend Solution, ensures that at least that part of a complete solution is secure.

The Safend Protector is certified by Common criteria to EAL2, and is currently in the "Coordination" stage in FIPS 140-2 certification.

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

7.2.2 Discusses assigning rights to access data based on job function, as defined in the infrastructure. For most organizations this is usually Microsoft's Active Directory, with a minority of cases using other LDAP-based infrastructure from Novell. Safend Protector supports seamless synchronization of roles and groups from these systems, and the recommended best practice is to assign each group its own policy.

7.2.3 Recommends a restrictive ("deny-all") default policy. In Safend's best practices document [1] there are two recommended policy layers. The lower layer is the machine policy, and the higher one is the user policy. The default policy if no known user is logged into the machine, is the machine policy which is very restrictive – blocking all devices and logging all access attempts.

Once a user logs in, a more permissive policy can be applied, on a need-to-know, need-to-use basis.

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

Safend Protector maintains unique IDs for computers, users, removable storage devices and even individual files, in all its logs, so that auditing is greatly enhanced and simplified. Any administrative access to the Safend Management Server requires membership of the admin group and is logged separately with the user ID.

Those unique IDs are protected from thieves using hardware keyloggers by Safend Protector. Hardware keyloggers are inline devices which connect to input devices such as keyboards, keypads, or credit card readers, and record all keystrokes between the input device and the target computer. Most hardware key loggers are no bigger than two AAA batteries, as seen below:



All hardware keyloggers contain the following two components:

- **Microcontroller** – interprets and processes the electrical signal from the input device and records it in memory
- **Non-volatile memory** – usually flash storage, stores the data from the microcontroller and retains it even if power is lost

They collect all transmitted data including users, passwords, and credit card numbers, and can later replay the information back to a potential thief.

Safend Protector blocks or detects those devices, rendering them useless and protecting the unique IDs as required by PCI DSS.

Requirement 9: Restrict physical access to cardholder data.

Physical access is just that – do not allow physical access to physical entry points (doors, buildings) and also to the machines containing the sensitive data, or machines that can access them. Toward this end, Safend Protector can block the connecting of any non-authorized USB devices to any physical machine that is able to access cardholder data, so that cardholder data is secure.

The recommendation of PCI DSS 1.2 only refers to network ports in requirement 9.1.2, but the very same requirement applies to USB ports. Requirement 9.9 refers to the inventory of removable media. Safend Protector can encrypt and keep track of all such media.

The keyloggers referred to in section 8 may also be used by would-be attackers to eavesdrop in the communication between credit card readers and their host computers, therefore stealing full CC data for each device they are connected to. The measures described in section 8 are also applicable to securing the connection of Credit Card readers.

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

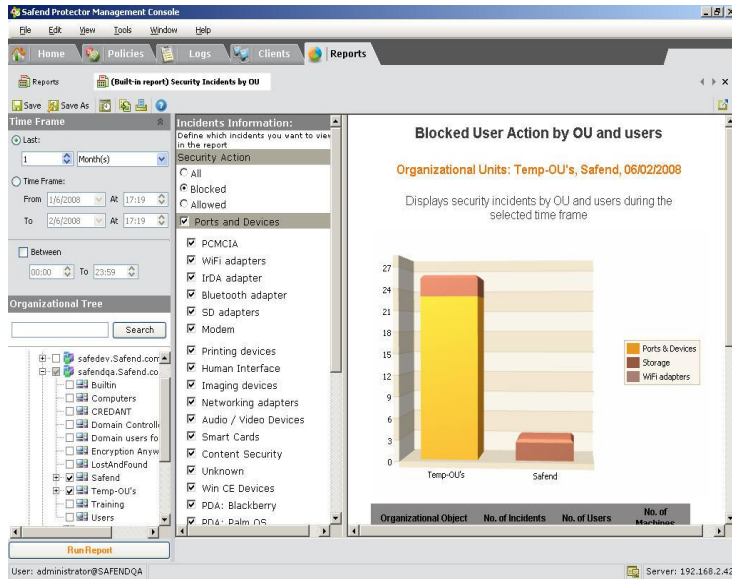
Access monitoring should include systems, endpoints, removable devices, and network resources. Safend Protector monitors closely all removable storage access by machine, user, device, file type and even content. Safend Protector monitors all access to cardholder data files on PC (10.2.1), and has an extensive anti-tampering mechanism that warns administrators of any attempt to change or erase logs (requirements 10.2.3, 10.2.6, 10.2.7).

Logging and monitoring user activity not only can be used to track down incidents when they occur; it can also help detour users from inappropriate actions. Users with administrative privileges, especially those with root or full system access privileges, require special consideration. The Safend Solution works to establish automated audit trails to reconstruct user actions, such as copying data based on the record,

the user's actions with a device, date and time and file properties information. These capabilities are provided by Safend Protector.

File Shadowing can establish a detailed audit trail for questionable file transfer. It includes a copy of the transferred file in the incident data for that transfer. Any data on each of the inbound and outbound channels can be shadowed including shadowing for specific file types. Collected shadow files are securely stored in a central repository and available for review by authorized administrators.

Requirement 11: Regularly test security systems and processes.



Continuous testing and auditing can be done easily with the Safend Solution. Safend Reporter, a component of the Safend Solution, can generate historical and graphical statistical data for reporting purposes.



Regular audits to discover devices should be scheduled. Safend Auditor enables security administrators to check either on-demand, or during set intervals, for the existence of current device connections and/or all historic device connections on

network endpoints. This data can be used immediately to improve security levels, where needed. Just as important as the deploying of security defenses, is the regular testing of the effectiveness of those defenses. Using Safend Solution enables a security team to continuously improve device and data leakage protection, during normal security improvement efforts. Most organizations regularly test security controls and processes to ensure they are in use and are implemented properly. Safend's technology strengthens a security team's ability to perform a security "self audit" and uses regular scanning and management programs to pro-actively prepare for audits, as well as protect the network and sensitive data assets. The Safend Solution performs these functions, as part of its on-going use as a security tool.

Requirement 12: Maintain an information security policy for employees and contractors.

Ultimately the standard on record is the documented information security policy. This establishes the standard that is expected of employees and contractors regarding the use of company resources, protection of company and customer data, and the methods for gaining approvals and access to these resources. Additionally, establishing an incident alert and management process to monitor, escalate and respond to violations of policies and to enforce actions taken when these situations occur. The Safend Solution enables all of these procedures for the use of devices within an organization user environment. The Safend Solution has an easy to follow workflow and documentation process, so that policy enforcement and policy changes can be easily created, modified, and documented.

Conclusions

Mobile technologies have created new challenges for IT departments. Traditional security has serious limitations — an information perimeter with localized access control points no longer meets PCI requirements. Newer technologies have been able to leapfrog this barrier and transfer information without defined access controls.

The Safend Solution augments PCI safeguards and integrates with existing organizational access privileges, to control the flow of information from endpoints. It tackles the difficult job of making sure that data leakage has minimal impact on PCI compliance. The Safend Solution also provides tools to manage the protective aspects and the auditing requirements of the regulation. Plus, the technical controls can easily be integrated into existing policies and procedures — controls which can be quickly deployed. Without these types of security counter measures, organizations face serious cracks in any infrastructure designed to be PCI compliant.

References

[1] Safend Protector best practices www.safend.com

[2] PCI –Understanding the intent of the requirements

https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf