How SoftControl TPSecure can help with PCI DSS Compliance

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. As a part of this initiative, the council has published a set of standards, called the Payment Card Industry Data Security Standard (PCI DSS). All payment card network members, merchants and service providers that store, process or transmit cardholder data must be able to demonstrate PCI DSS compliance to a PCI DSS Qualified Security Assessor. Non-compliance means risking losing the ability to process payments.

PCI DSS version 2.0, published on Oct 28th 2010, is the latest version of the standard available today. This document describes how SoftControl TPSecure can help you meet the requirements of PCI DSS 2.0 by protecting the integrity of your network.

Benefits of the SoftControl Approach

SoftControl TPSecure helps organizations meet PCI DSS compliance and reduce the risk of financial fraud. Whenever a breach is attempted and blocked, TPSecure issues a real-time alert with a description of where, when and what kind of violation was attempted.

As with all SoftControl solutions, TPSecure has its roots in digital rights management, where the goal is to preserve the integrity of the system rather than try to identify every malicious action attempted on that system. The technology behind this process, VIPO (Valid Inside Permitted Operations), is a unique and highly-effective architecture that monitors and processes all system activity for unexpected and/or unauthorized activities.

Beyond specific compliance benefits, TPSecure also provides:

- Proactive protection against unauthorized data access, file system or registry modifications and software changes, delivering entire system integrity. TPSecure maintains systems in a known-good state by controlling unauthorized launch attempts and all process activities in the system.
- Integration with other security solutions - TPSecure is compatible with most popular corporate security solutions, including antimalware, encryption, and network traffic security, enabling the same policies to be enforced across all endpoints.
- Background monitoring and logging of all system events - Shadow mode provides continuous monitoring of devices using techniques that cannot be detected or tampered with by service personnel. All data movement, including copying to removable media such as skimmers, is monitored and alerts sent to the management console.
- Granular control over access to and use of external USB storage, CDs/DVDs, COM and LPT ports, autorun control and the ability to set exclusions by device type, name, vendor and ID. Protected devices are recognized and accepted, while all others are blocked.
- Centralized management - TPSecure manages client settings, device and application activity rules and updates system profiles centrally/remotely, enabling policy changes to be applied on-the-fly.
- Self-protection system - TPSecure processes cannot be stopped or killed, even with high-level administrative rights. Additionally, the client regularly sends heartbeat status reports to the management console.
- Multiple delivery options - TPSecure can be delivered in various ways, providing flexible integration and deployment capabilities. These include: standard components and settings, custom components and settings based on customer requirements, binary libraries (SDK), or even source code.

PCI DSS Compliance – How TPSecure meets the requirements

Build and Maintain a Secure Network

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

SOFTCONTROL SOLUTION

- TPSecure works with firewall solutions to ensure that application is in a known-good state and keeping it stays that way.
- Access to firewall application data files and registry keys related to all other applications can be disabled. TPSecure ensures that the firewall solution/settings are not tampered with.

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

SOFTCONTROL SOLUTION

TPSecure uses Active Directory synchronization for centralized control of security policies and administrative access protection.

Protect Cardholder Data

3. Protect stored cardholder data

SOFTCONTROL SOLUTION

TPSecure provides protection of stored data, blocking unauthorized access to all sensitive files and folders.

Protect Cardholder Data

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

SOFTCONTROL SOLUTION

Although the standard talks about anti-virus products, it is clear that the intention of this requirement refers to protection against malware — in any shape or form.

TPSecure is recommended not only meets this requirement, but also protects the network from known and unknown threats. TPSecure is unique in that it provides a proactive protection against any malware, including the growing threat of insider attacks. It ensures malware and hackers cannot access or tamper with the way transaction-processing devices function. When deployed, TPSecure creates system profiles using as a base all installed applications or a predefined application set. It also includes the ability to use third-party information regarding legitimate applications during profile creation.

TPSecure controls all attempts to launch applications. All new or changed applications can be blocked from launching if their checksums are not present in the system profile. Specific application activity rules may also be applied.

6. Develop and maintain secure systems and applications

SOFTCONTROL SOLUTION

TPSecure prevents vulnerabilities from being exploited by using the application consistency checks and launching potentially vulnerable applications in a secure environment with limited privileges.

This also means that patching no longer needs to be a real-time activity; all new OS or application patches can be fully tested before being applyed, or avoided altogether, without introducing security risks.

TPSecure preserves device integrity with minimal impact on maintenance tasks and maximum flexibility. The system can be locked down completely, or applications can be executed in a secure environment, or individual or group policies can be applied that enable applications be used for predetermined purposes and/or in predetermined circumstances only.

Regularly Monitor and Test Networks

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

SOFTCONTROL SOLUTION

When a breach is attempted, along with blocking unauthorized activity, TPSecure issues alerts with a description of where, when and what kind of violation was attempted. For every application or process, the entire activity history and shadow copies of the changed files can be created. Every breach can be tracked back to its source.

11. Regularly test security systems and processes

SOFTCONTROL SOLUTION

TPSecure generates alerts on the introduction of unauthorized code or unauthorized file access. The audit log provides easy and timely audit information about endpoint activities. Additionally, TPSecure can send endpoint heartbeats to the management console. If, for any reason, the TPSecure installation is stopped on a remote device, an alert is issued to the management console or to the administrator via e-mail.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel.

SOFTCONTROL SOLUTION

TPSecure contributes to the organization's incident response plan by making alerts on incidents centrally available from across the organization.