FORTRA

PCI DSS Compliance with Managed File Transfer

Executive Summary

PCI DSS compliance requirements will continually evolve under the auspices of the PCI Security Standards Council. This means that the security “tweaks” that IT implements today for PCI DSS may be inadequate to handle the data security requirements of the next version of the standard.

However, by rethinking the use of underlying components that IT uses in its data transfer arsenal, forward-thinking IT shops are arming themselves to meet the changing requirements of PCI DSS and other compliance requirements. With better tools with more configuration options, these professionals are building new technology strategies to meet and/or exceed the compliance requirements for today and tomorrow.

Introduction

Some IT groups are taking a new and creative path towards PCI DSS compliance. Instead of struggling to meet compliance requirements with legacy data transfer tools, they are implementing managed file transfer solutions that include DMZ Secure Gateways.

This unique and cost-effective strategy provides better, more configurable tools to help IT organizations achieve PCI DSS compliance more easily, while laying a good foundation for future security enhancements.

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is the information security standard for organizations that handle payment card processing which includes merchants, processors, service providers, acquirers, and issuers. It's defined by the Payment Card Industry Security Standards Council as a method to increase security controls over cardholder data and reduce credit card fraud due to accidental or deliberate exposure.

The Danger of Non-Compliance

If your organization experiences a security breach, the lack of compliance will result in fines and penalties from the payment card brand (Visa, MasterCard, etc.). The fines are not trivial and could result in termination of your merchant account by the bank.

Therefore it's imperative that IT professionals become well-versed in PCI DSS to learn how to most efficiently implement its technical compliance requirements in their organizations.

The Impact of PCI DSS on IT

PCI DSS is a broad-reaching security standard with many requirements and recommendations. At first glance, the IT elements for achieving PCI DSS compliance may not appear too onerous. Some are common sense requirements, such as enforcing password policies, locking down networks and restricting access to systems that store PCI data. All require testing and validation on a scheduled basis. But, like many compliance regulations, the devil is in the details.

For some IT shops, the technical elements of PCI compliance may already be in place as a part of an organization's information security framework. But for others, the stricter security focus of PCI DSS will necessitate a thorough technical review of the existing IT infrastructure and validation processes including:

- Infrastructure reconfiguration
- New equipment or software investment
- New and/or extended auditing processes

Legacy file transfer tools make it difficult to comply with PCI DSS.

A New Technical Strategy for Compliance

As companies develop their strategy to comply with the PCI DSS standard, many have chosen to shift the compliance efforts of their IT staff. They have learned that it's no longer cost-effective to "tweak" an existing aging security infrastructure – especially where critical and confidential data is being transferred to other entities.

Instead, these IT organizations are building a technical strategy within the IT infrastructure that can evolve easily to accommodate new compliance demands as they are defined.

How are IT shops developing such a technical strategy? One key component being used by leading edge IT shops is the implementation of a managed file transfer solution.

What is Managed File Transfer?

Managed File Transfer (MFT) is a comprehensive, centrally controlled software solution that facilitates and secures the movement of data between systems across internal networks, trading partners, and the Internet.

MFT solutions move file transfer activities into a controlled environment with oversight, authentication, encryption, role based administration, auditing, and reporting.

An effective MFT solution does all of the following:

- Automates file transfer processes between trading partners and internal systems including detection and handling of failed transfers
- Supports multiple file transfer standards including FTP, FTPS, SFTP, SCP, AS2, and HTTPS
- Protects transmissions over public and privatem networks using secure protocols (e.g., TLS 1.2 and 1.3, SSH)
- Provides strong authentication schemes using multifactor authentication.
- Protects files while at rest using strong encryption methods such as AES 256 and OpenPGP
- Integrates with existing applications using documented APIs
- Generates detailed reports on user and file transfer activity

MFT solutions resolve many of the known security limitations normally associated with FTP while permitting IT to automate and validate the file transfer processes. Most importantly for PCI DSS compliance, MFT solutions protect sensitive cardholder data so that exposure to threats due to attacks or user errors can be minimized or eliminated. By utilizing the flexible and configurable components of MFT, an organization will decrease its exposure, increase the success rates of file transfers, and remove many of the obstacles that are common with business-to-business transfers.

Implementing a typical MFT solution doesn't satisfy PCI DSS data security requirements by itself. To help achieve compliance, a DMZ Secure Gateway is also needed.

Managed File Transfer solutions help organizations achieve PCI DSS compliance.

How MFT Addresses PCI Requirements

The right MFT solution will address many PCI DSS requirements through features such as encryption, role-based security, and audit logs. As you evaluate MFT software, make sure the solution offers these capabilities.

	PCI DSS	Corresponding GoAnywhere Feature
Required Standards	**Requirement 1: Install and Maintain Network Security Controls** Applicable Requirements: 1.3.1, 1.3.2, 1.4.1, 1.4.2, 1.4.4, 1.4.5	IP addresses and ports are customizable in GoAnywhere, allowing flexibility with firewalls. Description fields make it easy to document why connections are used. Combined with GoAnywhere Gateway, full separation of internal data, DMZ, and public networks is simplified.
	Requirement 2: Apply Secure Configurations to All System Components Applicable Requirements: 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.7	The GoAnywhere Security Settings Audit report provides a detailed list of GoAnywhere security defaults, enabled services, and configured security features. Using HTTPS will ensure that all administrative access is encrypted.
	Requirement 3: Protect Stored Account Data Applicable Requirements: 3.2, 3.5.1, 3.6.1.3, 3.7.5	With GoAnywhere, your files are protected at rest using strong encryption methods like AES and OpenPGP. It also provides cryptographic key management. Data retention can also be automated.
	Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks Applicable Requirements: 4.2.1	GoAnywhere protects transmissions over public and private networks using secure protocols including SFTP, FTPS, AS2, and HTTPS. TLS 1.2 and 1.3 are fully supported.
	Requirement 5: Maintain a Vulnerability Management Program	GoAnywhere can run on systems with 3rd party anti-virus solutions. It also supports ICAP integration for external scanning and data loss prevention.
	Requirement 6: Develop and Maintain Secure Systems and Software Applicable Requirements: 6.2.4, 6.3.3, 6.4.1, 6.4.2	GoAnywhere provides various security configurations to support the secure implementation of the environment.
	Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know Applicable Requirement: 7.2.2	GoAnywhere provides role-based security so each user only has access to the information they need.
	Requirement 8: Identify Users and Authenticate Access to System Components Applicable Requirements: 8.2.2, 8.2.6, 8.2.8, 8.3.1, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.5.1, 8.6.3	GoAnywhere has full individual account management features. It can also integrate with LDAP and external 2-factor authentication to satisfy all account requirements in PCI DSS.
	Requirement 9: Restrict Physical Access to Cardholder Data	GoAnywhere's multi-platform and virtual environment flexibility will allow you to run software and store data in your secure location.
	Requirement 10: Log and Monitor All Access to System Components and Cardholder Data Applicable Requirement: 10.5.1	With detailed audit logs, GoAnywhere makes it easy to monitor all activity on the system. Integration with external logging solutions is built in.

MFT solutions have resolved security issues associated with FTP while automating and validating data transfers.

What is a DMZ Secure Gateway?

A DMZ Secure Gateway is designed to add an extra layer of security to the company's network. It is configured to reside in the public-facing segment of a company's network called the demilitarized zone (DMZ).

By acting as a reverse proxy, a DMZ Secure Gateway prohibits direct public access from the Internet to any systems in the company's private network. At the same time, it can serve as a forward proxy by passing transfer requests from the private network out to the Internet, coordinating these transfers with the MFT software in the company's internal network.

By implementing a DMZ Secure Gateway solution, the IT staff can quickly configure and automate data transfers, eliminating the complexity of staging files in the DMZ.

Strategic Tools for Compliance

Managed File Transfer, in tandem with a DMZ Secure Gateway, enhances the overall information security framework by bringing the day-to-day tasks of data exchange into a configurable, scalable system that can meet or exceed the requirements of PCI DSS.

MFT dovetails with the current IT requirements for PCI DSS, while positioning the organization to meet new requirements down the road. This is why it is such an effective technical strategy for compliance.

Therefore, a managed file transfer solution, combined with a DMZ Secure Gateway, accomplishes the following goals:

- Centralizes the control and management of file transfers
- Provides role-based administration and permissions for separation of duties
- Institutes secure connections for the transmission of sensitive data
- Provides strong encryption key management
- Closes inbound ports into the private network to prevent unwanted intrusion
- Provides detailed audit logs for reporting and audit reduction

Organizations who want to ensure PCI DSS compliance find that MFT allows IT administrators to control and secure the day-to-day data exchange activities, boosted by DMZ Secure Gateways that extend that security to the network itself.

Using this MFT strategy, IT groups can reduce the amount of time required to implement PCI DSS, increase the security of the network, and control the access to cardholder data while providing a future-proof technical strategy that is robust, scalable, predictable, and secure.

Are your file transfers PCI DSS compliant?

The GoAnywhere PCI Security Audit Report tests 100+ file transfer settings against PCI requirements and provides recommended actions to help achieve compliance. Request a demo to see it in action.

Request a Demo
Visit goanywhere.com/demo

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.