



# How Managed File Transfer Helps Achieve PCI Compliance

White Paper

## Why Is Achieving PCI Compliance Difficult?

Retailers, banks, merchant service providers — any business that handles cardholder information — are required to comply with PCI DSS requirements.

Organizations that don't comply are subject to costly fines from the payment card companies as well as bad publicity and loss of customer confidence.

But achieving PCI compliance — and staying compliant — has proved difficult for many companies. Organizations often have numerous applications and systems, managed by different teams with different goals and security policies. These systems running in silos usually are too disparate to easily comply with PCI requirements, especially when policies for governance and the measures required to enforce them are missing or incomplete.

In many companies, the data security and management approaches used by different teams conflict, wasting resources and greatly delaying the time it takes to get compliant. IT and security personnel are constantly thrashing with questions like: who has access to the files? How are files sent? How, where, and when is data managed? How is it controlled as it moves from one stage to the next? Lack of integration when different applications use the same data creates more conflict and delays. For example, what happens when data flows from a financial system to a CRM system? How do you make that happen as part of an automated and secure workflow?

Acquisitions — of new companies, systems, processes or technologies — restart all of these conflicts, and the cycle repeats. PCI compliance must also be demonstrated periodically, making it an ongoing process, not a one-time event.

## MFT Provides a Holistic Solution for All File Transfer Needs:

- Encrypts the files
- Encrypts the channel that the data or files flow over
- Manages and authenticates individuals, groups, and applications that send and receive files
- Automates file transfers, based on a schedule or event
- Guarantees delivery of files as they move between applications, locations, and/or individuals
- Starts and manages ad hoc file transfers from any device (desktop, email, iPod, Android, etc.)
- Ensures that file-related SLAs are met
- Monitors, reports, and analyzes all file transfer activity
- Integrates easily with other applications and services

# How MFT Enables PCI Compliance

## What Is Managed File Transfer (MFT)?

Managed File Transfer (MFT) is a software application or service that can manage every aspect of file exchange. It has proven to be one of the most effective technologies for achieving PCI compliance, with the agility to keep up with changes to processes and systems, as well as new releases of the standard. It also provides extensive Enterprise Application Integration (EAI) and workflow management capabilities to automate, streamline and secure critical business processes.

An MFT solution provides governance and security that enables PCI compliance throughout your organization, using a central console that provides visibility and control into all files and data. It pulls data from each application into a single encrypted repository where it is managed according to rules you can build and enforce. Whenever data moves through your organization in a batch or flat file, an MFT application manages that data at all times, determining where it needs to go, what encryption level it requires, what applications it interacts with, and who can access it. It also provides a single point for tracking all activity throughout a file's lifecycle and the entire chain of custody, with central reporting and a complete audit trail showing who accessed what files when. This ability to set security rules and policies, and monitor their enforcement, enables organizations to fully meet PCI requirements — as we'll see later in this paper.

With the majority of data moving through an organization comprised of large flat and/or batch files, more and more companies are turning to MFT technologies for the agility, control, and enforcement that PCI requires. Beyond formal compliance, MFT is increasingly seen as a “must-have” to protect sensitive information from security breaches and prevent disruption to the business.

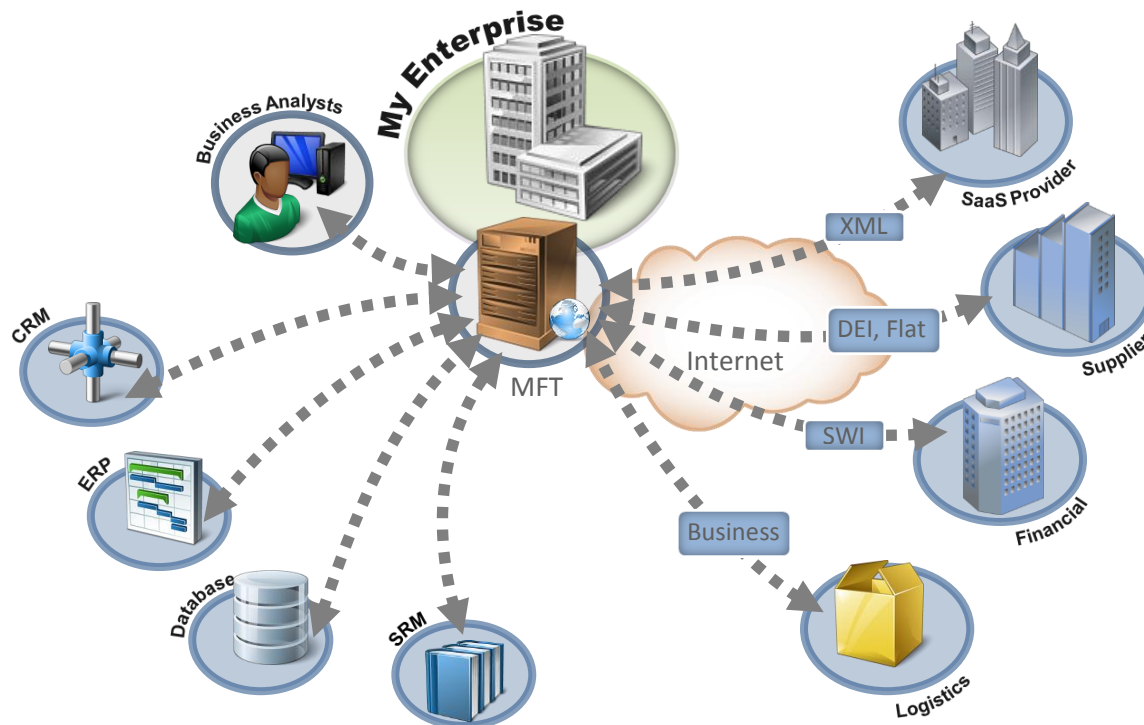
## MFT in Action: PCI Compliance and EAI

MFT manages and integrates disparate applications across an enterprise, providing central governance, visibility and control. An MFT application can function as a flexible EAI tool, bringing together data from many different systems to encrypt files, coordinate file transfers across multiple domains, authenticate users and trading partners, and enforce consistent policies throughout the organization.

In addition to managing data in a single repository, an MFT application can also transform that data as it moves between applications. For example, if data comes from a SaaS provider as an XML file, the MFT application can transform it into

# How MFT Enables PCI Compliance

SWIFT data for a bank or convert it into a format suitable for a CRM or financial system or for a third party database. For analysts or administrators exchanging sensitive information with different internal and external organizations, MFT makes sure the data arrives safely at its intended destination, in the right format.



## How MFT Helps Achieve PCI Compliance

Let's examine the five categories and 12 requirements of the PCI standard and see how an MFT application enables compliance.

### Build and Maintain a Secure Network

Deploying an MFT application is one of the key steps in building and maintaining a secure network. The MFT application securely stores (using encryption) and retrieves all credit card information, and securely transfers that information to and from any valid user and/or application. An MFT application also provides governance for viewing, sending, and receiving files between authorized people, applications, or end points. It manages the transfer of files, tracks the transfer, authorizes and authenticates all users and applications, schedules file transfers, and provides logs and audits of all transfers and transactions.

# How MFT Enables PCI Compliance

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

A two-tiered MFT application, with perimeter servers in the DMZ and the core server and data store in the trusted network, ensures there is a firewall between the internet and cardholder data. Moreover, in a two-tiered application, the MFT application ensures that only transactions specifically intended for the MFT application are allowed through. This is a double means of securing cardholder information. After deploying the firewall and properly segmenting your IT infrastructure, an MFT application helps maintain this requirement by ensuring that no data gets stored in the DMZ. Instead, data is streamed between sending and receiving trading partners and applications.

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

An MFT application helps ensure password security. First, it ensures that the default passwords are changed, and never used. Second, it enforces a set of password rules (e.g., unique passwords in a specific time period or combining letters and numbers to form a unique password). Moreover, the MFT application keeps a history of used passwords to minimize reuse in short periods of time.

## Protect Cardholder Data

Firewalls and encryption are the favored technologies for achieving end-to-end cardholder data protection. Restricting access to card data is the most important PCI DSS requirement, but also the most difficult to achieve because of different technologies used by different teams. In contrast, an MFT application provides one easy-to-use technology that creates a single encrypted repository that all teams can manage from a common dashboard.

✓ **Requirement 3: Protect stored cardholder data**

When the MFT application stores all cardholder data, it encrypts that data so that only authorized users can view or use it. Even system administrators cannot access or view that information. For example, a system administrator cannot copy data from the file system onto a USB key or an iPod because the MFT application encrypts the filenames and contents of the file.

✓ **Requirement 4: Encrypt transmission of cardholder data across an open, public network**

When the MFT application sends cardholder data via a secure file transport protocol (like AS2, SFTP or FTPS), it always encrypts the data while it is in transit. Administrators can select a variety of encryption schemes to ensure the proper combination of security and ease of access by only authorized users.

## Maintain a Vulnerability Management Program

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

By integrating with an anti-virus tool, an MFT application scans files for viruses when they enter its system. If the MFT application finds a virus, it attempts to clean the file. If it cannot clean the file, it notifies the sender and receiver, then securely deletes the file.

### ✓ Requirement 6: Develop and maintain secure systems and applications

An MFT application is one of many secure applications that companies deploy to ensure they can resolve any data breaches. The security built into most MFT applications goes a long way to prevent a data breach: if a determined hacker manages to expose the data, the audit trail in an MFT application will indicate when the breach occurred, who was responsible, and what data was exposed.

## Implement Strong Access Control Measures

Deploying an MFT application in your organization is one of the strongest and best measures you can take to protect sensitive credit card information.

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

An MFT application severely restricts who can view, write, change, or remove cardholder information. You can specify one, many, or groups of users who can access specific cardholder data or sets of cardholder data. In other words, there's plenty of flexibility in how you apply rules that restrict access.

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

The MFT application automatically assigns every user a unique ID. It then tracks all user actions with their unique ID in a tamper-resistant audit file.

### ✓ Requirement 9: Restrict physical access to cardholder data

Given the browser-based design and Service Oriented Architecture (SOA) of an MFT application, no end user or administrator needs physical access to the MFT application. After the initial installation, you can lock or restrict access to the computer. In addition, a properly designed MFT application will encrypt its file repository to prevent anyone from physically accessing the files.

## Regularly Monitor and Test Networks

A properly designed MFT application will help (not hinder) your efforts to monitor for exceptions and test for possible data breaches.

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

An enterprise-class MFT application includes a tamper-resistant audit trail and log. The auditing capability tracks who viewed, updated, added, or removed information; it also tracks when, where, and how that information was viewed, added, changed, or removed. Finally, the auditing tracks what files were changed. Ensuring that the audit trail is resistant to tampering is the most important feature here. “Tamper-resistant” means that the audit trail is always creating a hash of its contents, which is placed into a signed file. If anyone tries to change the contents of the audit file, the hash immediately reports this breach.

- ✓ **Requirement 11: Regularly test security systems and processes**

A properly-designed MFT application lets administrators and security personnel test their designs, flows, and policies before making the system available to end users. This testing helps discover any flaws and gaps in security. The MFT application does this by simulating the flow of the file, file storage, and all file operations (view, add, change, or delete). This simulation produces a detailed log for analysis. The actual data stored on the system is not affected.

## Maintain an Information Security Policy

- ✓ **Requirement 12\*: Maintain a policy that addresses information security for all personnel**

Finally, the organization needs to develop and maintain a policy that addresses all aspects of data security, with rules that govern all your applications and teams. Even though this is the last PCI requirement, it’s actually the first task that your organization needs to complete. (And when developing this policy, remember that MFT addresses all security aspects of your information and data!)

---

\* Refers to a company policy rather than a technology implementation.

## Benefits of Using MFT for PCI Compliance

MFT technology protects sensitive data and improves enterprise-wide compliance, visibility, reporting, and management, all from a single easy to use console. In addition to helping achieve PCI compliance, MFT is one of the most effective technologies for EAI, enabling secure, highly-automated workflows and improved collaboration. Key benefits include:

- **Fast deployment and ROI:** Depending on the size of your organization and the complexity of your solution, an MFT solution can be running and providing value in as little as two hours.
- **Simplified automation and workflow:** Using an administrative console, you can define rules that automate complex, long-running processes where data is shared between applications, locations, users and processes. Workflows and processes can run on a schedule, be driven by events, or on-demand.
- **Governance and control:** An MFT solution can eliminate insecure silos with the ability to manage all data interaction, set rules governing all file activity by users, processes, and applications, and enforce them meticulously.
- **Leverages interoperability standards:** Support for applicable standards and protocols allows data to flow smoothly and securely between disparate systems. Examples include security standards like PGP AES, and AS2, file transfer standards like FTPS or SFTP, banking standards like ACH, and other leading standards.
- **Robust APIs:** A robust set of interfaces and adapters allows rapid integration with applications running within your enterprise.
- **Security Compliance beyond PCI:** By combining EAI with management and enforcement, an MFT application helps secure your data *beyond* PCI to better comply with federal and industry regulations, including GLBA, Sarbanes Oxley, and HIPAA.

## Advanced MFT Technology from Ipswitch

Organizations worldwide depend on MFT solutions from Ipswitch to achieve compliance with the PCI DSS — and stay compliant as new systems and processes are added and the PCI standard evolves. We can help you take effective steps to secure and manage your critical data, as well as the processes and workflows that depend on it. Solutions combine management flexibility, security, and enforcement to provide a level of PCI DSS compliance that other file transfer approaches cannot match.

We offer products that address all levels of the MFT maturity model, from simple person-to-person file transfer through to enterprise-level B2B integration. All offerings are fast to implement, easy to use, and backed by exceptional customer support.

## About Ipswitch File Transfer

Ipswitch File Transfer high-performance integration and managed file transfer (MFT) solutions manage a broad spectrum of business interactions – from enterprise application integration to mission critical data transfers to simple person-to-person file exchanges. Customers worldwide, including more than 90 percent of Fortune 1000 enterprises, the majority of government agencies and millions of users, rely on proven Ipswitch solutions to transform the way they do business. Our customers implement these solutions to facilitate MFT, A2A and B2B integration, collaboration, workflow automation, data transformation, compliance, modernization, consolidation and governance. Ipswitch solutions are interoperable, making them easy to implement and deploy for the industry's fastest time-to-value and accelerated ROI. Learn more at <http://www.ipswitchft.com> or contact us at <http://www.ipswitchft.com/Company/Contact.aspx> or on [Twitter](#).