ipswitch

Secure. Control. Perform.

AN IPSWITCH WHITEPAPER

How MOVEit Addresses Data Protection Security & Compliance Requirements

ipswitch

Introduction

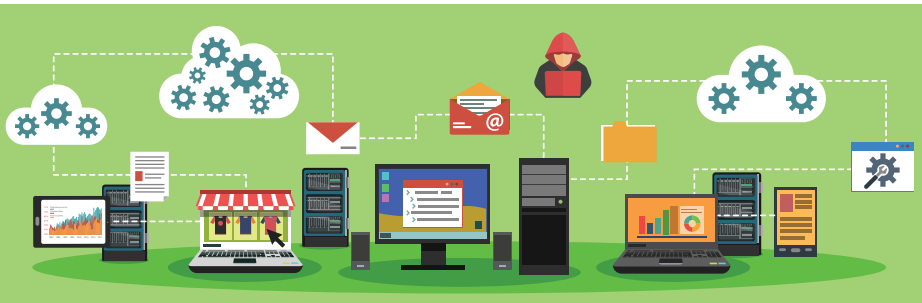
There is no single, holistic solution that can address all data protection compliance and security requirements for a given organization. There are many systems that companies put in place to secure data within the firewall. When sensitive information is contained within an organization, it is much easier for IT to control and manage.

What happens when sensitive data is sent externally – beyond the confines of the firewall? The sensitive data is now vulnerable and can manipulated, stolen or sold on the black market. Your data may end up in the hands of unintended recipients presenting the risk of data theft and regulatory violations.

This is where a secure and reliable Managed File Transfer (MFT) system can prove an invaluable investment for an organization that needs to share sensitive information with 3rd parties. A MFT solution can address many security and compliance protection requirements while giving IT the control, visibility and flexibility to file transfer activities. It enables IT management oversight of day-to-day business operations that involve the transfer of large amounts of data to other organizations, employees, partners and vendors.

In this whitepaper, we will explore the seven key security controls required by data protection regulations and how the suite of MOVEit products (MOVEit Transfer + MOVEit Automation) enables their implementation. Finally, it shows how MOVEit goes above and beyond typical minimum data protection requirements to ensure security, compliance, visibility and control over your most sensitive data.

File Transfer Data Protection



Once sensitive data is outside the firewall, it is exposed to potential theft and misuse.

ipswitch

Compliance Requirements

Assuring external data exchanges are done securely and in compliance with data protection mandates requires careful assessment of your MFT Solution against the following seven security requirements.

Security Requirement		File Transfer Control
1. Compliance	→	Automation
2. Communications Security	→	Control & Visibility
3. Information Security Policies	→	Information Security
4. Access Control	→	Authentication
5. Cryptography	→	Cryptography
6. Physical & Environmental Security	→	Secure Architecture
7. Business Continuity Security	→	Failover

Let's deep-dive into each of these seven file transfer controls and explore how a MOVEit Solution can comprehensively address each of the security requirements outlined above.

AUTOMATION

Automating file transfer operations has multiple benefits. It cuts down on the likelihood of lost revenue from late SLA submissions. It also reduces the risk of violating security requirements required to comply with data protection regulations.

The automation of file-based tasks and business workflows enables IT to:

- Minimize the need to maintain multiple scripts
- Meet service level agreements (SLAs) requirements
- Stay flexible in order to adapt to changing business conditions
- Eliminate the need to manually monitor where files are at any given time.

IT often relies on scripting as a way to transfer files on a regular basis. Maintaining multiple scripts written by different employees in different scripting languages introduces complexity reduces your ability to scale file transfer activities. If the author of a file transfer script leaves the company, the teams ability to make updates or assure effectiveness becomes an issue. Even more problematic is the risk that the scripts become obsolete and no longer work or are insecure and increase the risk of a data breach.

ipswitch

MOVEit Automation makes it easy to schedule the majority of file transfer activities without the need for customized scripts. The easy-to-use setup gives IT the ability to quickly create new tasks and then modify them over time as needed. A built in job scheduler will automatically push and pull files between file share servers, FTP servers or MOVEit Transfer at predefined scheduled intervals assuring their delivery, as required, to the intended recipient.

File transfers can be easily set up to push jobs to multiple systems simultaneously on a regular basis or set up as a one-time batch file transfer transaction. Tasks can be easily created, modified or deleted by any administrator that has been granted access permissions and requires zero scripting capabilities by the user. Even complex, logic-based workflows can be created and modified without the need for advanced programming skills.

MOVEit Automation also supports guaranteed delivery via automatic forwarding and error correction capabilities for all data transfers that take place. Delivery assurance is achieved by MOVEit by automatically resubmitting a failed file transfer activity until it completes successfully. Once the data is delivered, MOVEit provides the sender with a notification confirming that the data was received by the authorized recipient(s).

CONTROL AND VISIBILITY

There is no way to guarantee that an organization's sensitive data is 100% protected from cyber attacks. However, control and visibility over the movement of your data can be effective tools to greatly minimize the chance that hackers gain unauthorized access to your information. By having clear insight into data flows and events taking place, your organization will be able to put effective security procedures in place to protect your data and help assure compliance with data protection compliance regulations.

Central visibility can alert IT to unusual file access activity or file transfer patterns. MOVEit provides a large set of authentication controls manage when and for how long users are authorized to access sensitive data. These include user and group provisioning, user account access, permissions and quotas as well as defining file access expiration rules. IT can also set password policies and is able to blacklist and whitelist users as required. Any violations to these set policies and controls alert IT to unauthorized access or possible cyber attacks and enable them to respond to these security concerns quickly and effectively.

Control over logging and reporting simplifies the audit process and assures the integrity of audit trails. System logs provide valuable insight into the file transfer process by keeping track of when a file is transferred, if it was received by the right part and whether or not it was subsequently deleted. If these logs are tampered with, the integrity of the entire file transfer process is compromised. MOVEit prevents this from happening with cryptographic tamper-evident logging, ensuring file transfer logs are not altered

in any way.

Another way MOVEit assists in the audit trail process is with predefined and customizable reports. A simple user interface makes it easy to view and pull reports. A consistent report format across all the FTP servers in the system makes it easy for auditors to review, compare and contrast all the available file activity information.

INFORMATION SECURITY

Important file transfer compliance requirements include file integrity checks, data deletion after receipt, non-repudiation and guaranteed delivery. These information security safeguards ensure sensitive data in transit is protected from being altered by a third party or incorrectly delivered to an unintended recipient.

Getting your data where you want it to go sounds easy, but requires a lot of back-end protections built into your file transfer methodology to keep your sensitive data safe. Man in the middle attacks occur when an attacker maliciously alters the direct communication between two parties. MOVEit's non-repudiation data integrity feature ensures that the sender and the receiver are both authorized and authenticated to access the data. In other words, only the sender and receiver have permissions to access the data that is being transmitted. If a third party somehow manages to intercept this transmission, they will not be able to read or alter any of the data. MOVEit uses SHA1 and MD5 algorithms when conducting file integrity checks to ensure that the data that is originally sent is the same data that is eventually delivered to the intended recipient.

MOVEit enables the protection of sensitive data with the option to set controls to automatically delete data at a set time (e.g. 1 hour, 1 day, 1 week, etc) or limit the number of times a file can be downloaded after it is received by the recipient. Data deletion and file download limits help to assure that files are not inadvertently left exposed to unauthorized access by a third party.

Another great feature of MOVEit is that you know where your files are at all times. Guaranteed delivery ensures your files are indeed sent to your intended destination. MOVEit automatically resends a failed file transfer activity until it completes successfully. Once the data is delivered, MOVEit provides the sender with a notification confirming that the data was received by the authorized recipient(s).

AUTHENTICATION AND AUTHORIZATION

One of the first layers of defense for meeting data security and compliance requirements can be put in place before information is even accessed. By controlling access to your systems and data, you can assure only authorized users have direct contact with your organization's most sensitive data.

MOVEit enables the ability for administrators to authenticate users against multiple authentication sources such as the local user database, external directories via LDAP or RADIUS and external IdP's via SAML/SSO.

For example, active directory (AD), Microsoft's implementation of the LDAP directory services, is a database that keeps track of all the user accounts and passwords in your organization. Administrators can tap into AD to easily implement enterprise-wide policies, credentials and security. Using AD limits the numbers of user names and logins for end users to remember, reduces the number of accounts that IT has to create and manage and increases security since all data is stored in one protected location. Integrating access control with AD ensures only already authenticated users in AD or LDAP have access to the file transfer system. There is no need for IT to monitor this process, once it is in place, as the system will be able to keep up with, and provide appropriate access to, changes in employee status (i.e. new or fired employees).

Multi-factor authentication is supported through SSL/TLS certificates for HTTPS and FTPS as well as SSH client keys for SFTP. This provides another layer of authentication designed to help ensure that the person trying to access the MOVEit system does indeed have the permissions to do so.

Once a user has been granted access to the MOVEit server, built-in authorization controls provide security to protect sensitive data from being viewed by unauthorized parties. Users are, by default, assigned access rights based on the principal of least privilege meaning they have no access or visibility until permissions are granted. In other words, each user's files are protected from being viewed or altered by unauthorized individuals. MOVEit provides system administrators with flexibility and granularity to adjust authorization controls as needed. Administrators can grant users individual permissions or a set of permissions via a Group. Group membership can be synchronized with AD via LDAP or SAML. This enables the system administrators to have clear control over what users can and cannot access when logged onto a MOVEit server.

CRYPTOGRAPHY

Compliance standards often mandate a certain level of data security protocols be put in place to prevent sensitive information from ending up in the wrong hands, stolen and sold on the black market. The intentions of these compliance regulations are good, but often, encryption algorithms get updated at a more rapid pace than can be kept up with by these mandates. Encryption algorithms have a limited shelf life. Your systems should be continuously updated to ensure the most up-to-date encryption protection available for data both in transit and at rest.

MOVEit uses FIPS 140-2 validated algorithms such as AES-256 encryption to protect data at rest. Even if someone is able to hack into your system, any data stored on the MOVEit Transfer server will be encrypted and inaccessible to the intruder. They will not be able to 'break the code', so to speak, and gain access to your sensitive files.

MOVEit also protects data in transit using secure file transfer protocols SFTP (SSH), FTPS (SSL/TLS) and HTTPS (SSL). These protocols are continuously updated in

MOVEit to adhere to the latest industry standards, ensuring your data is always safe.

SECURE ARCHITECTURE

A robust and secure MFT solution not only has safeguards in place to protect data both at rest and in motion, but it also delivers a system architecture with additional layers of security to physically separate data marked for transit from internal file databases.

The MOVEit Transfer server acts as a temporary repository for data that needs to be shared with third parties. It sits outside of an organization's firewall so data stored on it can be accessed by external parties without exposing the rest of the organization's network. All data stored on MOVEit Transfer is protected with AES-256 encryption ensuring that is no unencrypted data within the DMZ.

Ipswitch Gateway adds yet another layer of protection to your file transfer solution architecture. It sits within the DMZ and provides termination of inbound requests for authentication and data transfers. It also acts as a proxy between inbound connections from the public network and an organization's internal trusted network. This configuration enables MOVEit Transfer to be deployed behind the firewall providing additional layers of security and minimizing the risk of exposure to secured network resources, sensitive data and authentication services by unauthorized third parties and hackers.

FAILOVER

Business continuity is a very important aspect for any organization that must exchange sensitive data, both within and outside the confines of its firewall. When you need to protect your data in motion and ensure it does not get "lost in a void" somewhere during a natural disaster, power outage or period of high transfer volume within your organization, confidentiality, integrity and availability of file transfer activities become top priorities.

MOVEit's flexible and scalable architecture enables high availability by improving the network's file transfer performance. High availability can be gained by eliminating single points of failure with the implementation of a distributed web farm deployment of MOVEit Transfer components. The MOVEit Transfer web farm operates as single MOVEit Transfer system that handles all client requests and distributes the MFT system load across multiple nodes. This distributed architecture ensures the most efficient distribution of file transfer activities for your system and enables IT to scale availability and increase performance by simply adding more application nodes to the web farm.

Automatic, secure failover plays a big role in ensuring file transfer activities are successful 100% of the time. MOVEit's failover option ensures files are either successful or continuously restarted until completed, even during a disaster or outage. It ensures reliable 24/7 file transfer operations with zero downtime and secures against data loss to assure regulatory and policy compliance.

Combining MOVEit's high availability and failover options ensures that your MFT system is ready, available and equipped to provide secure and guaranteed delivery of all your data when it needs to be transferred.

ipswitch

Summary of Ipswitch MOVEit Data Protection Security and Compliance Features

MOVEit is a MFT system that lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations.

With MOVEit your IT team can:

- **Control** movement of critical data between partners, people and systems to assure data security and regulatory compliance
- **Simplify** the creation of automated workflows to improve reliability, security and compliance
- **Automate** performance, SLA and compliance monitoring

From a compliance perspective MOVEit delivers on many data protection concerns:

- **Data Protection Safeguards:** MOVEit was designed to excel at implementing data protection safeguards: encryption at rest, secure delete, file transfer integrity (non-repudiation), unique user IDs, automatic log off
- **Access Control:** MOVEit allows admins to configure and automatically enforce a strong access control policy for internal users who access ePHI
- **Logging and Reporting:** MOVEit produces detailed audit logs to support user activity reviews, including login activity
- **Disaster Recovery:** Ipswitch Failover for MOVEit removes a lot of the complexity involved in a technical implementation of contingency planning required for critical ePHI data

ipswitch

Frost & Sullivan has awarded Ipswitch MOVEit their 2016 Secure File Transfer Product Leadership Award.

In the course their industry Best Practices Research, MOVEit was found to best address the key customer and industry needs of security, flexibility and scalability while ensuring an unrivaled customer experience and ease-of-use.

The following table summarizes how a MOVEit MFT Solution compares to other file transfer implementations available on the market.

SECURITY AREA	FTP SERVERS	CLOUD FILE SHARE	EMAIL SERVERS	MOVEit MFT SERVERS
Workflow Automation	◑	○	◔	●
Control and Visibility	◔	◑	◑	●
Information Security	◕	◕	◑	●
Authentication	◔	◕	◑	●
Cryptography	◑	◕	◑	●
Secure Architecture	◑	◑	◕	●
Failover	◑	◕	●	●

About Ipswitch

Ipswitch helps solve complex IT problems with simple solutions. The company's software is trusted by millions of people worldwide to transfer files between systems, business partners and customers; and to monitor networks, applications and servers. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices throughout the U.S., Europe and Asia.

For more information, visit **www.ipswitch.com**.

ipswitch

Download your 30-Day FREE TRIAL of Ipswitch MOVEit ›