IPSWITCH FILE TRANSFER

IPSWITCH FILE TRANSFER TECHNICAL BRIEF

Security Throughout the File Transfer Life-Cycle:

A Managed File Transfer Imperative

MOVEit®

Security Features of Ipswitch File Transfer's MOVEit, the Trusted Choice for Secure Managed File Transfer

www.IpswitchFT.com

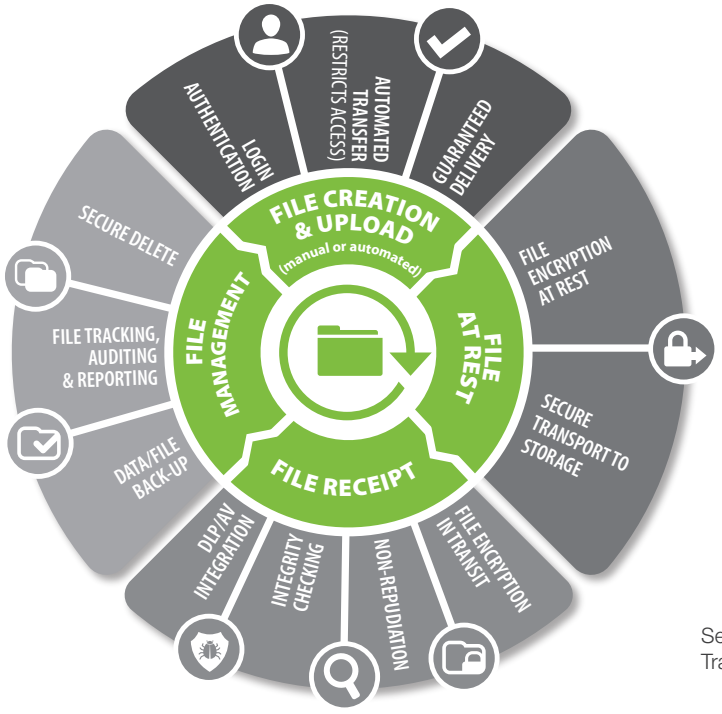
Overview

For those exploring managed file transfer options, security is an important consideration – a consideration that regulatory compliance and best business practices have made an imperative. This document presents Ipswitch's approach to security, and to detail the specific features included in the **MOVEit Managed File Transfer System** – features that have been designed to help IT teams assert control over sensitive data file transfer, helping ensure security.

MOVEit Managed File Transfer Security Features

SECURITY THROUGHOUT THE FILE TRANSFER LIFE CYCLE

MOVEit Managed File Transfer provides security throughout the file transfer life cycle. That life cycle begins when a file is created for automated or manual transmission, and continues through file transport, receipt, and storage or deletion. Throughout the secure managed file transfer life cycle, MOVEit also provides full administrative control over how, where, and by whom files are transferred.



Security throughout the File Transfer Life-Cycle

MOVEit Managed File Transfer is comprised of four functional components. These are explained more fully in the appendix, but for a quick overview, the two core components are MOVEit File Transfer (DMZ) Server, the secure file transfer server, and MOVEit Central, which automates file transfers. The other components, MOVEit Ad Hoc Transfer and MOVEit Mobile are add-ons to MOVEit File Transfer (DMZ). MOVEit can be deployed on-premise or in the cloud.

FILE CREATION AND UPLOAD

Login Authentication

To access file transfer services, MOVEit File Transfer Server requires users to authenticate via login against one or any combination of the following sources.

INTERNAL: MOVEit File Transfer Server has its own secure, built-in user store, and securely encrypts all passwords stored in this database. Internal authentication features include:

INTERNAL AUTHENTICATION	
Password strength	Password complexity is configurable via pre-defined policies.
Password aging	Configurable time period with user email alerts.
Password history	Configurable number of passwords to prevent reuse.
Account lockout	Accounts can be configured for lockout and administrators notified via email.
Blacklist and whitelist	Specific users or classes of users can be restricted to certain ranges of IP addresses and/or hostnames.

EXTERNAL: MOVEit File Transfer Server supports any user database accessible via standards-based LDAP, Secure LDAP or RADIUS Server protocols (including Microsoft Active Directory or IAS, Novell Border Manager or eDirectory Sun iPlanet, Tivoli Access Manager, and ODBC-compliant databases).

MOVEit File Transfer Server offers single sign-on capability via standards-based SAML 2.0 integration to Identity Provider (IdP) vendors, including Microsoft ADFS, Onelogin and Shibboleth. This gives IT administrators centralized management of user credentials and enables employees to use a single credential to access multiple desktop and web applications.

Using the internal user store, MOVEit File Transfer Server authenticates users via valid username and any of the following multi-factor authentication combinations: password, certificate or key, and IP address.

Additional options for multi-factor authentication are available via integration to an external IdP vendor. For example, Onelogin enables use of any of the following: their own free Mobile One-Time Password App, PKI certificates or any of the pre-integrated solutions from Duo Security, RSA, Symantec, VASCO and Yubico.

Automated Transfer

Tasks such as pushing and pulling files to and from any FTP/SFTP/HTTPS servers or network shares\UNC paths based on events or schedule; manipulating/transforming file content; and managing files for transfer, storage or deletion can be automated with MOVEit Central. Automating movement of files eliminates external access to the trusted network by pushing encrypted files into the DMZ for external access, and pulling files from external sources.

Guaranteed Delivery

MOVEit File Transfer Server provides non-repudiation and integrity checking. MOVEit also supports file transfer automatic retry and resume on its HTTPS and FTPS interfaces from any clients offering those capabilities, eg MOVEit browser plugins, MOVEit EZ, Xfer, and Freely. In addition to being useful during transfers of multi-gigabyte files, this feature is also secure in the sense that it makes large file transfers less susceptible to denial-of-service attacks.

FILES AT REST

MOVEit File Transfer delivers encrypted storage of data, protection of encryption and decryption keys, generation and use of strong cryptographic keys, secure distribution of keys, cryptographic key rotation based on cryptoperiods, and restricts unauthorized substitution of cryptographic keys. A multi-tier deployment integrating MOVEit File Transfer with existing database servers and SAN/NAS storage servers enables storage of files, logs, keys and configuration data inside the trusted network.

File Encryption at Rest

Traditionally, managing keys for files at rest has been an issue, but MOVEit File Transfer Server handles it transparently. For files at rest, MOVEit uses industry standard AES 256-bit encryption.

MOVEit File Transfer Server is FIPS 197 validated. Within MOVEit, all configuration data (including user authentication information, etc.) is encrypted, ensuring no unencrypted data in the DMZ.

Secure Transfer to Storage

At no point during the transmission or storage of data is it unencrypted in the MOVEit File Transfer Server environment. MOVEit spools parts of files received into much smaller buffers, encrypts them and writes them to disk immediately. Spooling files in this manner reduces overall exposure in two ways: 1) it reduces the amount of information exposed; and 2) it reduces the time information is exposed.

FILE RECEIPT

MOVEit File Transfer Server provides security through file encryption in transit, non-repudiation, integrity checking, and DLP and anti-virus integration.

File Encryption in Transit

MOVEit File Transfer Server supports a number of file transfer protocols, and provides minimum 128-bit encryption, configurable by the MOVEit administrator. In MOVEit Central, all file movements can be optionally PGP encrypted.

ENCRYPTION IN TRANSIT METHODS	
HTTPS	Supports single port (443) access by Web browsers (including Firefox, Internet Explorer, Chrome, and Safari) as well as by the MOVEit File Transfer API Module, and by MOVEit Central, MOVEit EZ and the MOVEit Wizard ActiveX and Java plugins.
SFTP	Used by Secure Shell (SSH) and SCP2 clients. These clients use one firewall port (22) and are often used on UNIX/Linux hosts.
FTPS	Includes all three modes (IMPLICIT, TLS-P, TLS-C) and "firewall-friendly" passive mode transfers.
AS2 (HTTPS) or AS3 (FTPS)	Using the same ports that web and FTPS clients use, automated business-to-business file transfer solutions can send files to MOVEit and receive prompt delivery receipts (requires MOVEit Central).

Non-Repudiation

Tying users to their actions is easy with MOVEit File Transfer Server. This is a security "best practice" and is required by Federal Information Security Management Act (FISMA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and others.

Integrity Checking

MOVEit File Transfer Server uses the cryptographically valid SHA-1 hash capability in its FIPS 140-2 validated cryptographic module to automatically ensure the integrity of the files it stores in its 256-bit AES encrypted file system. All Ipswitch clients support automatic SHA-1 integrity checks with MOVEit File Transfer.

Data Loss/Leak Prevention and Anti-Virus Integration

MOVEit File Transfer Server provides integration to file content scanning software. MOVEit submits incoming files to the scanning systems using the ICAP protocol. DLP solutions enable monitoring and control over movement of all files. Supported solutions include: RSA, Symantec and McAfee. Anti-virus servers scan content for virus and malware. Supported systems include Symantec, Sophos and McAfee. Transferred files can be allowed, blocked or quarantined. All activity is logged and alerts or status are displayed to users, including the malware or virus name if found by your anti-virus solution.

FILE MANAGEMENT

MOVEit File Transfer Server provides secure file management capabilities throughout the file transfer life cycle. Features include policy/rules for the file life cycle, audit and reporting, high availability, failover and disaster recovery.

File Tracking, Auditing and Reporting

MOVEit File Transfer Server maintains application audit logs to support customer recordkeeping and to facilitate daily log review by system administrators or security officers. MOVEit deployed on-premises integrates with a number of log management or SIEM systems. MOVEit offers tamper-evident audit logs.

MOVEit File Transfer Server comes with over 90 pre-defined reports, as well as the ability to create custom reports, all of which can be run against the data that MOVEit automatically logs to its secure, built-in database.

MOVEit Central provides access to current status and recorded statistics in a convenient report format. Different report display types are available, each with user-selectable display and filter options. Report data can be exported to several different formats.

The MOVEit File Transfer Web interface offers easy online access to status and reports. APIs are available to provide access to log data from customer or third party applications. Access is controlled based on user, group or role.

Data Backup

MOVEit File Transfer Server has a flexible architecture designed for high availability, disaster recovery and failover deployments. Disaster recovery and failover are enabled via integration with Neverfail IT Continuity Engine.

Secure Delete

MOVEit File Transfer Server offers the ability to manage administrative policies that improve security. Every folder can have different settings for automatic file deletion. Users accounts can be automatically disabled based on defined criteria such as period of time since last use. In addition, alerts can be set up to warn administrators about potential compliance-related issues, such as failover.

MOVEit CLOUD

MOVEit Cloud is a hosted Managed File Transfer solution. It is deployed in highly protected, redundant data centers (Rackspace), and offers a standard SLA which guarantees 99.9% uptime with high availability.

MOVEit Cloud inherits all of the software-specific security features described above. Since MOVEit Cloud is a managed cloud service, Ipswitch, as the service provider, has control over not only the software, but also the hardware, IT staff, and processes. This broader control enables Ipswitch to take greater responsibility for security compliance. See the appendix for a full list of MOVEit Cloud's unique security features.

Summary: Ipswitch MOVEit Security

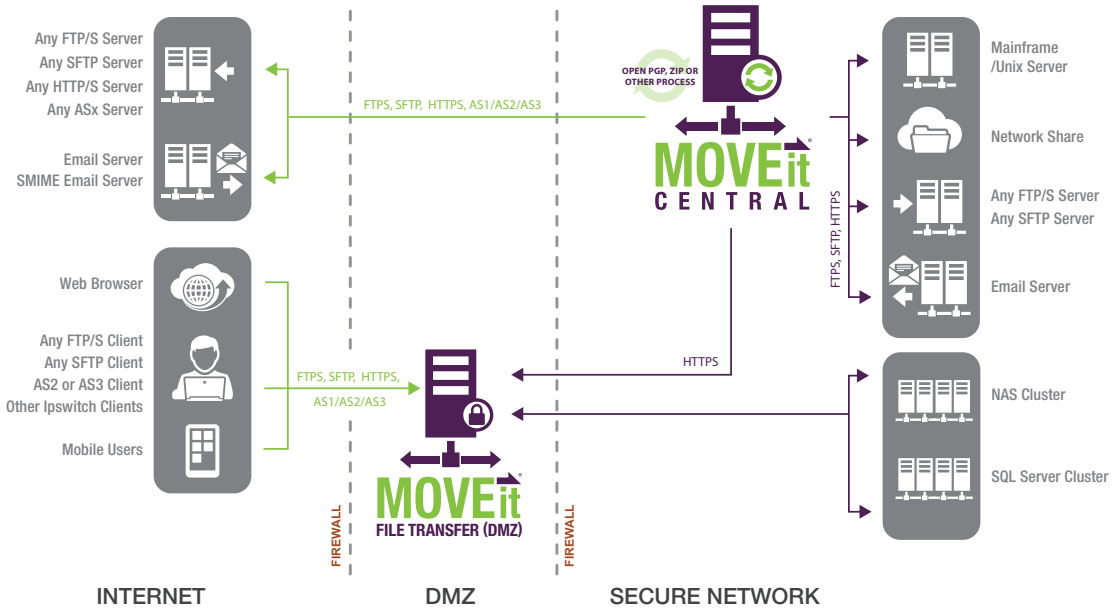
MOVEit Managed File Transfer's security features are born out of a holistic approach to security that provides security throughout the file transfer life cycle. Ipswitch products are developed, architected, and deployed so that highly secure file transfers can be offered to your stakeholders without the complexity or cost of other technology and vendor choices.

SECURE SOFTWARE DEVELOPMENT

Software engineering at Ipswitch follows a development process that enables Ipswitch to build more secure software and address security-related compliance requirements. This process is formally known as the secure Software Development Life Cycle (SDLC). By rigorously following the SDLC, Ipswitch addresses security in every phase of training, requirements, design, implementation, verification, release, and response. Static and dynamic code analysis and penetration testing are routinely performed for all major releases of MOVEit Managed File Transfer, ensuring product integrity. When high-risk security flaws are discovered in Ipswitch products, as part of its continuous testing, patches are crafted and tested, and customers notified.

Ipswitch takes vulnerability management seriously, following secure coding best practices as defined by the Open Web Application Security Project. OWASP is a worldwide organization focused on improving the security of software. Ipswitch adheres to the OWASP top 10 list and other guiding principles, such as requiring third-party security training for all engineering and technical support staff, and maintaining a regularly-updated security knowledge base.

SECURE ARCHITECTURE



Typical deployment architecture for MOVEit Managed File Transfer

MOVEit Managed File Transfer is architected to integrate with existing security infrastructure, policies, and applications, ensuring that there is no unencrypted data in the DMZ. MOVEit offers the ability to automate the transfer of files outside the inner firewall, eliminating external access to trusted networks. MOVEit is used by IT staff to automate the pulling, processing and pushing of files between internal business and storage systems, MOVEit servers, and remote systems and users.

MOVEit's tiered architecture enables deployment in a distributed configuration, with the application, database, and file system running on different machines. This configuration is flexible and can expand to provide increased file transfer performance and availability.

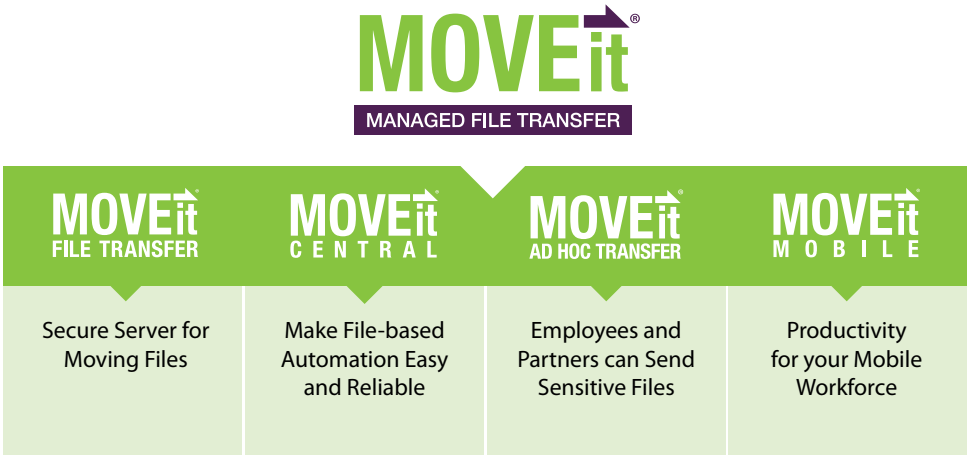
SECURE DEPLOYMENT

Security is a shared responsibility, so MOVEit includes tools that help guide IT administrators to choose the appropriate settings to meet their security policies. Ipswitch provides a proprietary hardening security tool that runs on installation, assisting the setting of security policies, disabling services, and performing other security-related tasks. Out-of-the-box MOVEit default installation options provide a responsible level of security, eliminating implicitly weak default options (e.g., plain text FTP, which has inherent vulnerabilities), and encourages administrators to go through all of the security options during initial installation.

APPENDICES

MOVEit MANAGED FILE TRANSFER PRODUCT OVERVIEW

Ipswitch MOVEit Managed File Transfer is composed of four functional components. (Shown in the figure below.) At the core are MOVEit File Transfer (DMZ) and MOVEit Central, two independent but tightly integrated applications that facilitate all types of file transfers, whether your partners pick up data from you, you collect data from their systems, your employees need to send a large file securely, or you are implementing automated file transfers between systems or people. MOVEit Ad Hoc Transfer and MOVEit Mobile are add-on components to MOVEit File Transfer (DMZ).



MOVEit Managed File Transfer has four functional components

MOVEit File Transfer (DMZ)

MOVEit File Transfer (DMZ) is a secure file transfer server for storing and managing sensitive information accessible by internal systems and external entities. Web browsers and no cost/low cost secure FTP clients can securely exchange files with MOVEit over encrypted connections using HTTPS, FTPS, and SFTP protocols. All files received by MOVEit are securely stored using FIPS 140-2 validated AES encryption, the U.S. Federal and Canadian government encryption standard.

MOVEit provides flexible configuration. In MOVEit File Transfer, individual end-user members of a group can be designated as group admins. These users are then able to administrate the users, folder permissions and address books in their group, subject to various parameters set by organization administrators.

MOVEit Central

MOVEit Central securely and automatically transfers files to and from FTP, FTPS, and SFTP servers, the local file system, network folders, email servers, and MOVEit File Transfer servers. MOVEit Central can also send or receive files in an AS1, AS2 or AS3 trading partnership. PGP encryption/decryption, zip operations, command-line applications and anti-virus integration are also built in, and usually requires no additional software. (MOVEit Central PGP Module license is required.)

MOVEit Central protects sensitive access to information with powerful encryption, local files with NIST 800-88 compliant data erasure, and configuration channels with SSL. Remote access (to Central) is restricted via local or AD domain group. Group membership can also provide or restrict access to particular tasks/jobs, external or internal file transfer servers, and encryption keys stored in MOVEit Central's secure key stores.

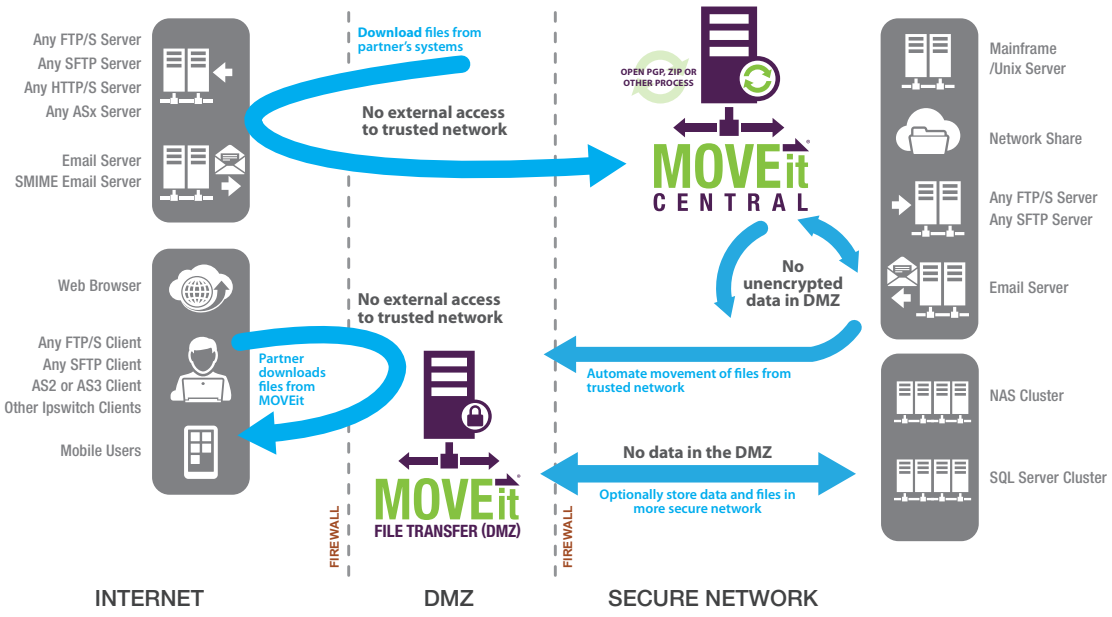
MOVEit Ad Hoc Transfer

The MOVEit Ad Hoc Transfer module supports sending and receiving files and messages between individuals and groups using Outlook or a simple browser interface, meeting employees' needs for convenience and ease of use.

MOVEit Mobile

MOVEit Mobile module supports sending and receiving files by individuals using mobile devices, providing security and productivity to mobile workers.

HOW MOVEit'S FUNCTIONAL COMPONENTS WORK TOGETHER



MOVEit Managed File Transfer Architecture

MOVEit Managed File Transfer's architecture provides robust file transfer services to employees and partners, while restricting external access to the trusted network. MOVEit Central automates the movement of files. Files can be automatically transferred to partners' systems or to MOVEit File Transfer Server, where partners can access files without accessing systems in the trusted network. MOVEit File Transfer Server encrypts data stored in the DMZ, or can optionally be configured to enable storage of files in a secure network such as a 'data zone', ensuring no storage of data or files in the DMZ.

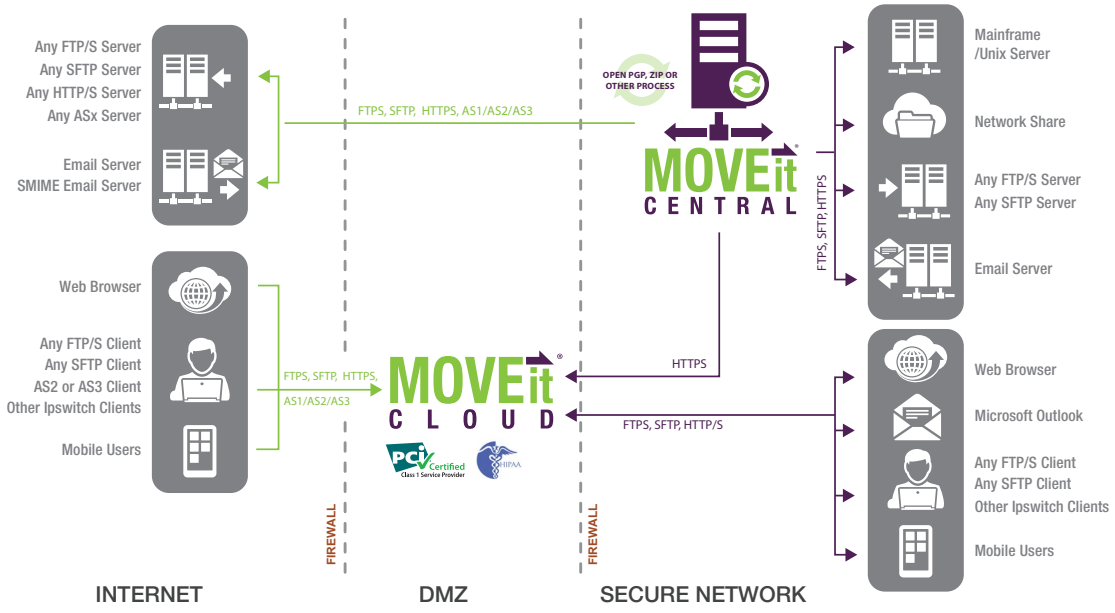
SECURITY-RELATED FEATURES UNIQUE TO MOVEit CLOUD

MOVEit Cloud is available with three purchase options, each with unique capabilities.

MOVEit® CLOUD

SECURE EMAIL ATTACHMENT	PROFESSIONAL	PREMIUM
Employees and partners can send sensitive files	Transfer sensitive files using folders from anywhere, including mobile devices	Access all features in *Secure Email Attachment Professional* options

Deploying MOVEit Central with MOVEit Cloud provides the same security and architectural advantages described above when deployed with MOVEit DMZ, MOVE Ad Hoc Transfer and MOVEit Mobile on-premises.



MOVEit Cloud Architecture

MOVEit Cloud is deployed in a data center that has undergone an SSAE-audit and received Type II SOC 1, 2 and 3 reports. MOVEit Cloud is validated through an independent, third-party assessor firm as PCI DSS, HIPAA, FFIEC and GLBA compliant.

Physical and logical access to the MOVEit Cloud environment is limited to authorized Ipswitch and Rackspace employees based on their organizational role. MOVEit Cloud Operations personnel who require remote access to the customer's cloud environment must use two-factor authentication (named user ID and unique complex password). Non-console access to the servers is secured by a Virtual Private Network (VPN) connection that is further protected by hardware tokens. Privileged access, including custodial responsibility for cryptographic keys, is further restricted to a subset of authorized Ipswitch employees. Ipswitch conducts criminal, education and employment background checks on new employees, where permitted by law, to further minimize security risks.

MOVEit Cloud's security features include:

Secure System Configuration: Ipswitch maintains an approved, hardened configuration profile for each system component. The system undergoes periodic review to find and fix any deviations from the documented standards.

Intrusion Detection System (IDS): MOVEit Cloud leverages an integrated Rackspace service that analyzes network traffic for attack signatures. Some events lead to immediate blocks at the firewall per Ipswitch directives.

Vulnerability Scanning: Ipswitch conducts quarterly PCI-compliant vulnerability scanning using an Approved Scanning Vendor (ASV). Identified vulnerabilities are remediated immediately.

Penetration Testing: Ipswitch uses a third-party qualified security vendor to perform penetration testing on an annual or as-needed basis to check for additional vulnerabilities that involve advanced exploit techniques.

Risk Assessment: Ipswitch conducts an annual risk assessment of the hosted Cloud environment to determine if the control framework achieves the data privacy and data security objectives.

Incident Management: Ipswitch maintains a highly evolved plan for responding to security incidents. The plan outlines specific procedures for shutting down the security-related event and notifying appropriate Ipswitch staff and customer contacts. The security event is worked to resolution—with urgency and expediency—and a root-cause analysis is performed.

Data Destruction: Customer data in the MOVEit Cloud environment is owned by the customer and may only be destroyed upon authorization by the customer. Any data devices taken off line are destroyed using the DoD 5220.22-M data sanitization method.

Log Management: For MOVEit Cloud, a dedicated log management system saves a read-only record of system and application logs to serve as a tamper-proof audit trail.

Ipswitch File Transfer provides solutions that move, govern and secure business information between employees, business partners and customers. The company's proven solutions lead the industry in terms of ease of use, allowing companies of all sizes to take control of their sensitive and vital information and improve the speed of information flow. Ipswitch lets business and IT managers govern data transfers and file sharing with confidence and enable compliance by balancing the need for end user simplicity with the visibility and control required by IT. Ipswitch File Transfer solutions are trusted by thousands of organizations worldwide, including more than 90% of the Fortune 1000, government agencies, and millions of prosumers. For more information on Ipswitch File Transfer and its products, go to www.IpswitchFT.com.

IPSWITCH FILE TRANSFER