

## MOVEIT DMZ: VERSUS SECURE FTP SERVERS

MOVEit DMZ is a highly secure enterprise Managed File Transfer server which boasts end-to-end encrypted transfer and storage of data and files and delivers powerful administration and reporting capabilities.

MOVEit DMZ delivers many advanced in-depth security capabilities that are essential for the safe and reliable operation of an Internet-facing server. The following is a partial list of these capabilities — the ones that are typically lacking in most secure FTP servers. If your requirements include any of the following security capabilities, then you probably need a MOVEit DMZ.

**FIPS 140-2 VALIDATION.** Files, messages, passwords and other sensitive data handled by MOVEit DMZ are protected by its built-in FIPS 140-2 validated cryptography that has been rigorously inspected by a US and Canadian government-approved testing lab to insure that each of its algorithms are properly implemented, all sensitive data is securely erased, and there are no hidden “back doors”. FIPS 140-2 validation is the cryptographic “Gold Standard” and MOVEit DMZ earned it in 2003 — most secure ftp servers still have not.

**ENCRYPTED STORAGE.** Every file and message uploaded to a MOVEit DMZ is securely stored, until deleted, using the strong FIPS 140-2 validated 256-bit key AES encryption that is built-in to every MOVEit DMZ. Encryption/decryption is done in tiny chunks so the entire file or message is never in the clear in either memory or on disk, and each file and message has its own encryption key — which is also encrypted. MOVEit DMZ provides encrypted storage because data is much more vulnerable “at rest” than in transit. Most secure ftp servers lack encrypted storage, while some depend on the underlying OS to provide this. The rest provide no “at rest” file security, forcing everyone to encryption their files with programs like PGP.

**END-TO-END ENCRYPTION.** The combination of SSL and SSH encrypted transfer and AES encrypted storage means files and messages exchanged through MOVEit DMZ will be encrypted from sender to recipient — without any end-user involvement, and without any need to use third-party encryption programs like PGP.

**PERIMETER SECURITY.** MOVEit DMZ can be deployed in a high security perimeter architecture without resorting to “pass-through proxies,” proprietary VPNs, odd firewall rules, or other methods that employ non-standard network entities. MOVEit products can be used to provide a complete enterprise-level secure data transfer, processing, and storage solution.

**SECURE PERMISSIONS SYSTEM.** MOVEit DMZ has its own built-in secure commercially licensed database, which is used to safeguard its system settings as well as its user authentication and permissions data. Most secure ftp servers lack this, relying instead on the underlying operating system to provide this.

**OS SECURITY INDEPENDENCE.** Hackers exploit OS flaws to gain access to systems, applications and files, but MOVEit DMZ’s unique combination of encrypted storage and secure permissions means that the security of its

settings, files and messages does not depend on the underlying OS always being secure. This is in stark contrast to the OS security dependence of most secure ftp servers.

**INTEGRITY CHECKING.** MOVEit DMZ performs cryptographically valid integrity checks on every file it handles (both when uploaded and downloaded) using the SHA1 algorithm in its FIPS 140-2 validated cryptography. Many secure ftp servers still do integrity checks using the error-prone and easily subverted XCRC algorithm, which is not FIPS approved, lacks cryptographic validity, and should not be used for integrity checking.

**NON-REPUDIATION.** This is the ability to prove who sent a file, who received it, and that the file sent and the one received are exactly the same. Non-repudiation is a security “best practice” as well as required for FISMA, GLBA, HIPAA, PCI DSS, MA 201 CMR 17 and SOX compliance. MOVEit DMZ does the authentication, logging and integrity checking needed for Secure FTP servers that use XCRC cannot do this.

**GUARANTEED DELIVERY.** To provide this, servers must support file Non-Repudiation as well as file transfer retry and (Checkpoint) resume. MOVEit DMZ provides Guaranteed Delivery; servers that use XCRC cannot.

**NO PUSH VULNERABILITES.** Hackers exploit push capabilities to send malware to remote file transfer servers, and into the local trusted network. Despite this, many secure ftp servers feature scriptable Move/Copy file transfer client capabilities. MOVEit DMZ does not have such capabilities, by design.

**TAMPER-EVIDENT AUDIT TRAIL.** A chain of cryptographic hashes protects the secure audit database in MOVEit DMZ, which automatically sends an email alert if records are subsequently altered or deleted.

**ONSCREEN KEYBOARD.** MOVEit DMZ Web login and password change pages have mouse-clickable keyboards for entering authentication data. This helps prevent identity theft by key logging programs that may have been installed on PCs at Internet cafés, business centers, public kiosks — and on home computers.

MOVEit DMZ’s virtual interface and least privilege permissions’ policy also helps protect the data being handled (and the privacy of its users) by providing tight administrative control over exactly what each and every user can and cannot see and do in terms of command options, files, messages, folders, logs, and other users.

In addition to being secure by design, MOVEit DMZ secure file and message transfer and storage servers include all of the following operational advantages — which are typically lacking in most secure ftp servers.

**WEB BROWSER SUPPORT.** Firefox, Internet Explorer, Mozilla, Netscape, Opera and Safari can be used to securely exchange files and messages via MOVEit DMZ, and also to securely administer it (use of Java, ActiveX, plugins, or third-party encryption applications like PGP is not required). AS2, AS3, FTP SSL (FTPS), FTP SSH2 (SFTP/SCP2) and MOVEit HTTPS clients are also supported.

**HIGH AVAILABILITY OPTION.** MOVEit DMZ has a flexible architecture that can ensure 24/7 uninterrupted service through its out-of-the-box high-availability, auto-failover configuration. MOVEit DMZ can also be configured with third party applications for load balancing and clustering to ensure smooth deployment of multiple MOVEit DMZ Servers in your web farm.

**TIERED ARCHITECTURE DEPLOYMENTS.** Distributed architecture enables the deployment of multiple DMZ nodes in the form of a web farm. Administrators can now deploy MOVEit DMZ on one server, the encrypted data store on a second server, and the configuration database on a third server. This flexible architecture extends the performance, availability and security of MOVEit DMZ solutions

**FILE NON-REPUDIATION AND GUARANTEED DELIVERY.** The former is the ability to prove who sent and who received a specific file, and that the file sent and the file received are absolutely identical. The latter requires file transfer retry, resume and non-repudiation. MOVEit DMZ supports both (requires use of a MOVEit client, including the free MOVEit Wizard browser plugins).

**EMAIL NOTIFICATION.** MOVEit DMZ can automatically alert users when files or messages arrive and have been system and user events like password expirations and lockouts.

**ADVANCED USER MANAGEMENT.** MOVEit DMZ supports user groups and group administrators for simplified, decentralized management, and enables user aging, cloning and customized profiles.

**AUDIT TRAIL.** Detailed data is automatically recorded in MOVEit DMZ's secure, tamper-evident database for each user, file, message, Web form posting and for each administrative action.

**EXTENSIVE REPORTING.** MOVEIT DMZ includes over 90 pre-defined, customizable reports that can be run against its database, from which data can be automatically extracted and exported in CSV, fixed-width and XML formats for use by third-party reporting and billing/tracking programs.

**API INTERFACE OPTION.** Provides third-party programs, including Web apps, with programmatic access to MOVEit DMZ file and message transfer, encrypted storage and user database services.

**EXTERNAL AUTHENTICATION OPTION.** Allows MOVEit DMZ to also authenticate users against one or more external sources (like Active Directory) via LDAP, secure LDAP and RADIUS Server protocols.

**INTEGRATES WITH SQL DATABASE.** Administrators have the option to either use the embedded MOVEit database or integrate with Microsoft® or Microsoft Express for both user authentication and server system configurations such as access controls, user permissions, and password policies.

**SECURE MESSAGING OPTION.** Enables authorized users with Web browsers to create and exchange messages and ad-hoc file transfers with other authorized users of the same MOVEit DMZ.

**USER INTERFACE LANGUAGE OPTIONS.** Enables users to select English, French or Spanish versions of the MOVEit DMZ Web, secure FTP, and Secure Messaging user interfaces and Help files.

**MULTIPLE ORGANIZATIONS OPTION.** Enables a single copy of the software to host two or more MOVEit DMZ “orgs” — each with its own URL, branding, admins, users, files, folders, audit trail, etc.

**OTHER FREE CLIENTS.** MOVEit DMZ licensees have the right to use and distribute the MOVEit Wizard plugins for Web browsers and the MOVEit Xfer command-line clients. These are commercially supported Java and Windows clients that use firewall friendly HTTPS encrypted transport and provide automatic SHA1 file integrity checking, transfer retry and resume, and other features.

For additional information about the MOVEit DMZ managed file transfer solution, including licensing and pricing as well as demonstration and evaluation options, please contact Ipswitch directly.



Contact Ipswitch's File Transfer Division