

## MOVEIT DMZ: FILE SECURITY V. OS SECURITY

This document describes two things: how secure file transfer servers, and the files they handle, can often be vulnerable to unauthorized access and misuse by hackers, and why this is not the case with the MOVEit DMZ secure file transfer and storage server software by Ipswitch.

**The Problem.** Every computer operating system (OS) has flaws. Hackers exploit these flaws to take remote control of computers and their applications, and to access the files stored on them. This means the security of programs and files often depends on the security (or lack thereof) of the underlying OS. This is one reason for the ongoing debate about which OS is more secure.

Most secure file transfer servers — and the files they store — depend on the OS being secure. This is because they use authentication and/or access control capabilities provided by the OS. It is also because most lack the ability to provide encrypted storage of the files they receive. By subverting the OS, hackers may gain the opportunity to do the following with such servers.

**Read and Alter Files.** Confidential data in unencrypted files stored by the server can be read and/or changed, and this may not be discovered right away, if ever.

**Delete or Replace Files.** Files stored by the server can be destroyed, or replaced by new files that may have similar characteristics, and this may also be hard to discover.

**Upload and Store Files.** A hacker-controlled server can become a safe haven for porn, stolen software, and malware (viruses, scripts, Trojans, etc.) for attacking other systems.

**Distribute Files.** Hackers can turn such a server into their personal distribution system, giving their associates file upload/download permissions, and even administrative rights.

**Compromise Other Systems.** Malware can be placed in the folders of legitimate users, who may then download it and unknowingly compromise their own systems, files and data.

In addition to operational and security problems, these activities can create legal liabilities.

**The Solution.** Use a MOVEit DMZ secure file transfer and storage server. The security of MOVEit DMZ, and every file it stores, is totally independent of the security of the OS it runs on. This is a result of the following features that were designed into MOVEit DMZ from the beginning.

**Permissions System.** MOVEit DMZ has its own built-in authentication and access controls. The former enables MOVEit DMZ to independently regulate exactly who can login to it. The latter uses the MOVEit DMZ virtual interface and permissions database to control what each user can see and do in regards to files, folders, logs, other users, and commands.

**Encrypted Storage.** MOVEit DMZ has its own built-in, FIPS 140-2 validated 256-bit AES encryption that it uses to automatically safeguard each file it receives. Each encrypted file has its own key, which is also encrypted. Hackers cannot access files stored by MOVEit DMZ.

MOVEit DMZ supports end-to-end secure file transfer — and storage — without fear of OS flaws.

Please contact the Ipswitch File Transfer division for MOVEit DMZ technical, evaluation and licensing information. For additional information about security and operational differences between MOVEit DMZ and other servers, download the “MOVEit DMZ v. Secure FTP Servers” pdf document from our website [www.ipswitchft.com](http://www.ipswitchft.com) or click on the purple link below for more contact information.



Contact Ipswitch's File Transfer Division