

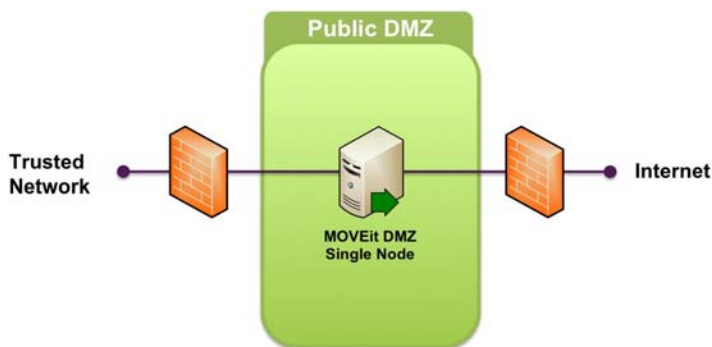
Servidor para Gerenciamento de Transferência de Arquivos

O MOVEit DMZ é um servidor de transferência de dados altamente seguro que acelera a transferência e o armazenamento encriptado de dados e arquivos de ponta-a-ponta, entregando uma poderosa administração e relatórios detalhados.

O MOVEit DMZ melhora a produtividade e colaboração entre funcionários, parceiros e clientes, permitindo a troca de dados sensíveis de negócios de forma rápida, fácil e segura através de mensagens encriptadas como também por transferência de arquivos sem a necessidade de adquirir licenças por usuário, instalar software em estações de trabalho, gerenciar chaves de encriptação, sobrecarregar sistemas de e-mail, ou ainda ter que permitir anexos de e-mails através de firewalls.

O MOVEit DMZ fica residente em um servidor seguro em uma "Zona Desmilitarizada" também conhecida como DMZ anexa ao seu firewall. Isto permite que seja acessado através do firewall de ambos os lados (de dentro e de fora) de sua rede para as seguintes transferências de dados:

- Usuário Final para Usuário Final
- Usuário Final para Sistemas e Servidores
- Sistemas e Servidores para Sistemas e Servidores



O MOVEit DMZ pode ser utilizado por uma grande variedade de agentes (também chamados de clients) normalmente instalados em desktops e laptops, servidores Unix/Linux e Windows, e Mainframes IBS, incluindo:

Navegadores: Firefox, Internet Explorer, Mozilla, Netscape, Opera, e Safari via HTTPS (HTTP Seguro).
Uso de Java, Active-ex, plugins ou aplicações de encriptação de terceiros como PGP. Os assistentes gratuitos (wizards) do MOVEit podem ser utilizados com navegadores para fornecer funcionalidades avançadas de transferência de arquivos, incluindo verificação de integridade de arquivos SHA1 (para não repudição), continuidade de transferência a partir de uma interrupção (resume) e novas tentativas (retry) para garantir a entrega de um arquivo, e muito mais.

Clients Seguros de FTPS como o WS_FTP Professional, MOVEit Central e uma variedade de produtos de terceiros para FTP através de SSL (Secure Sockets Layer) que suportem qualquer um dos 3 modos de FTP sobre SSL (IMPLICIT, TLS-P, TLS-C) como também transferência de arquivos, o que o MOVEit DMZ faz utilizando apenas 4 portas abertas no firewall. FTPS clientes são normalmente utilizados em sistemas Windows e são nativos para o IBM z/OS mainframes.

Clients Seguros de SFTP Clients como WS_FTP Professional, [MOVEit Central](#) e outros clients Seguros de terceiro para FTP sobre SSH (Secure Shell) e clients SCP2.

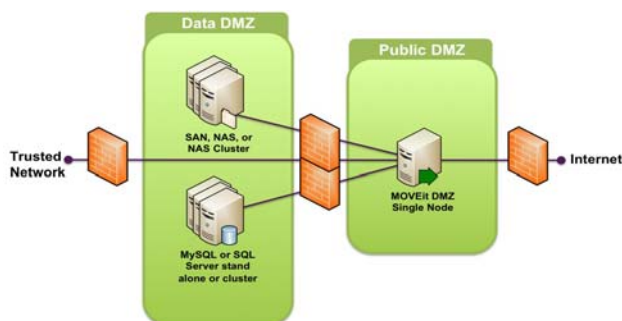
Clients MOVEit HTTPS incluindo APIs do [MOVEit DMZ](#), os clients [MOVEit EZ](#) Windows e o MOVEit Xfer agente para execução de linha de commando (gratis), sendo que todos podem ser utilizados para troca de arquivos automaticamente com o MOVEit DMZ.

Clients AS2 e AS3 Clients tais como [MOVEit Central](#) e clients de terceiro com suporte a transferência segura de arquivos por AS2 e AS3.

Para mais informações sobre Clients compatíveis com o MOVEit DMZ [clique aqui \(em inglês\)](#).

MOVEit DMZ foi projetado desde o início para ser uma solução segura e para suportar uma grande variedade de protocolos públicos e os padrões. Ele não é um servidor FTP com características de segurança adicionadas e também não é um programa proprietário seguro para transferência de arquivos com padrões abertos embutidos. Aqui estão alguns exemplos das características únicas, defesas fortemente construídas que fazem do servidor MOVEit DMZ “seguro por arquitetura”:

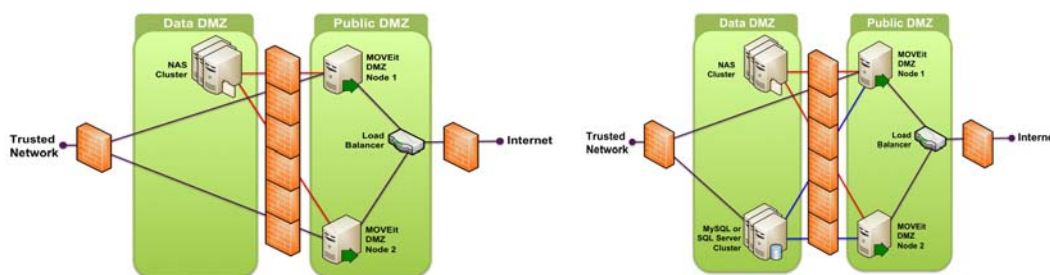
- [FIPS 140-2 Validated Cryptography](#), incluindo encriptação 256-bit AES que é utilizada para armazenar cada arquivo e formulários web recebidos. O MOVEit DMZ suporta transferência e armazenamento encriptados de ponta-a-ponta, sem a necessidade de utilizar programas de terceiros, tais como PGP.
- [OS Independent Security](#) Uma vez que o MOVEit DMZ fornece suas próprias capacidades de permissão e segurança, tem como resultado que hackers não conseguem acessar os dados que o MOVEit DMZ manipula, mesmo que subvertam a camada de segurança do Sistema Operacional. A segurança do MOVEit DMZ não depende da segurança do sistema operacional no qual está executando.
- O MOVEit DMZ não inicia transferência, portanto as portas do firewall não necessitam ser abertas a partir do segmento DMZ da rede.



Adicionalmente para suportar criptograficamente validação de checagem de integridade arquivos para SHA-1, compressão em tempo real e reinício de transferências interrompidas em NAT e FTPS, o servidor MOVEit DMZ oferece um conjunto de características corporativas que fornece integração avançada e flexibilidade operacional.

- Arquitetura em camadas permite que múltiplos nós DMZ sejam montados em forma de “web farm”. Os administradores podem instalar o MOVEit DMZ em um servidor, os dados encriptados em um Segundo servidor e o banco de dados de configuração em um terceiro servidor. Esta flexibilidade melhora o desempenho, disponibilizada e a segurança das soluções MOVEit DMZ.
- Integra com SQL Server. Administradores tem a opção de utilizar o banco de dados próprio do MOVEit ou integrar com Microsoft® SQL Server ou Microsoft SQL Server Express para autenticação e configuração do sistema, tais como controle de acesso, permissão ao usuários e política de senha.
- Autenticação Multi-Factor contra o banco de dados do MOVEit DMZ's utilizando dois out res fatores, incluindo senha, certificados de hardware e software SSL, chaves públicas de SSH (“fingerprints”), e/ou endereços de IP. O MOVEit DMZ exceed os parâmetros de autenticação emitidos pelo FFIEC utilizados por instituições financeiras e supervisionado pelo US FDIC, FRB, NCUA, OCC e OTS.
- Opção de autenticação externa permite ao MOVEit DMZ autenticar usuários contra qualquer combinação de LDAP, Secure LDAP, RADIUS Server ou banco de dados ODBC adicionalmente ou substituindo seu próprio banco de dados.

- Utilização de política de antiguidade pode desativar automaticamente usuários (inclusive excluí-los depois de um período), baseado em número de dias depois da sua criação ou depois de seu último acesso ao MOVEit DMZ, ou após uma quantidade de logons, ou ainda por calendário.
- [File Non-Repudiation](#) A habilidade de provar quem enviou o arquivo, quem recebeu e que não foi corrompido ou modificado durante a transferência. (Requer o uso de FTP, ou o MOVEit client, incluindo o MOVEit Wizard com um navegador).
- Garantia de entrega com segurança incluindo retomada, tentativas, transferências e armazenamento encriptados e File Non-Repudiation.
- Opção de mensagem segura permite aos usuários a troca de mensagens sem a movimentação de arquivos através do servidor MOVEit DMZ utilizando navegadores existentes.
- Notificação por email alertando usuários quando arquivos ou mensagens chegaram, foram vistas, excluídas, downloads e sobre eventos de administração (expiração de senha, trava de usuários, etc.)
- Auditoria baseada em banco de dados padrão aberto via ODBC, que contém registro de atividades de cada usuário, arquivo, mensagem e postagem de web forms, como também todas as atividades dos administradores.
- [Relatórios](#) Inclui mais de 90 relatórios pré-definidos (além de poder construir seus próprios relatórios) cobrindo transferência de arquivos, mensagens seguras, status dos usuários, desempenho do sistema, status de armazenamento e segurança, que podem ser executados sob demanda ou através de agendamento, gerando arquivos CSV, HTML, ou XML.
- [API Interface](#) Opção que fornece acesso programático baseado em HTTPS, para acessar o MOVEit DMZ, trocando e excluindo arquivos e mensagens seguras, criar, gerenciar e excluir pastas, usuários e permissões.
- [Integração com aplicação Web](#) incluindo como portais e programas web podem utilizar os serviços de transferência de arquivos, mensagem seguras, armazenamento encriptado de arquivos e serviços de banco de dados.
- [Alta disponibilidade](#) Opção que entrega uma arquitetura flexível para disponibilizar serviços 24/7 sem interrupções através de uma configuração de “auto-failover”. O MOVEit DMZ pode ser configurado com aplicações de terceiros para carga balanceada e clustering para garantir a instalação de múltiplos MOVEit DMZ Servers em uma “web farm”.



O licenciamento de um MOVEit DMZ permite o software ser executado em um único servidor em ambiente de produção e um em ambiente de não produção, ou seja desenvolvimento, QA e backup). A licença permite um número ilimitado de usuários trocar e armazenar arquivos e opcionalmente ilimitadamente mensagens.