



WHITE PAPER (GLOBALSCAPE)

# Streamlining Business Operations: Harnessing the Power of MFT



We're continually learning about data breaches impacting even prominent and well-secured organizations around the world. Despite their advanced security measures and intrusion detection systems, one significant vulnerability lies in the way data is shared.

Traditional file transfer methods, such as File Transfer Protocol (FTP) and email, go hand-in-hand with a number of challenges regarding security, control, scalability, and compliance.

File transfer protocols, such as FTP and HTTP, transmit user credentials and files without encryption, leaving them vulnerable to interception. This lack of security is prompting companies to seek alternatives to their unsecured file transfer methods.

## The Danger of Outdated Protocols

The reliance on [outdated protocols like FTP](#) and email exposes companies to security vulnerabilities due to a lack of robust protocols to protect sensitive information from interception and possible exploitation.



**Native FTP does not encrypt data:** Traditional FTP lacks built-in encryption mechanisms, meaning that data transferred via FTP is sent in an unencrypted format. This makes it highly susceptible to interception and eavesdropping by malicious actors, potentially compromising sensitive information.



**User names and passwords are transferred in clear text:** During the login process, FTP transmits user credentials (username and password) in clear text format, making those credentials vulnerable to interception. This lack of encryption means that anyone with access to the network traffic can easily capture and decipher the login credentials, putting the data at significant risk.



**FTP scripts and batch files expose user IDs and passwords:** Scripts and batch files used for automated FTP processes often contain plaintext user IDs and passwords. Storing sensitive information in this way exposes them to unauthorized access and exploitation by hackers or malicious software. Even if the FTP server is secure, leaving credentials in scripts widens the attack surface and compromises security.



**FTP does not meet compliance regulations when used alone:** Most industries and organizations are subject to regulatory requirements regarding data security and privacy, particularly those in heavily regulated industries such as healthcare and financial services. Due to its inherent lack of encryption and vulnerability to data breaches, FTP alone may fail to meet these compliance standards.



**Transferred data could "stray" to a remote computer:** In some cases, particularly when FTP connections are improperly configured or intercepted, data intended for transfer may be redirected to another destination by mistake. This could happen due to network misconfigurations, unauthorized access, or malicious actions. Unauthorized redirection exposes sensitive data to unsanctioned parties and increases the risk of data breaches.



**Conventional FTP does not maintain a record of file transfers:** Unlike more advanced file transfer solutions, traditional FTP lacks built-in logging and auditing capabilities. This absence of comprehensive logging makes it difficult for administrators to track and monitor file transfer activities, root out suspicious behavior, or investigate security incidents. Without proper records, it's hard to maintain accountability and ensure compliance with security policies and regulations.

Considering these challenges, organizations must rethink their approach to file transfer. The global file transfer landscape requires modern solutions which prioritize security, automation, scalability, and compliance to meet the evolving needs of data-driven businesses.

## The High Cost of Insecure File Transfer Solutions

Inefficient file transfer methods can take a significant financial and operational toll on businesses. One of the most tangible consequences is the risk of data breaches. When files are transmitted using outdated protocols or insecure channels, they become vulnerable to interception by threat actors. The fallout from a data breach can be extensive, resulting in financial losses, damage to reputation, loss of customer trust, and legal liabilities.

File transfer software handles a wide range of data, including sensitive and proprietary information, such as financial records, trade secrets, and personal data. This information is typically entrusted to the software for secure transmission between parties. However, if the security of the file transfer software is compromised, it can endanger the confidentiality and integrity of the stored data.

One key concern is the potential for the file transfer software to become a single point of failure within an organization's security infrastructure. As a central hub for data exchange, a breach in the software can grant unauthorized access to all the information contained within it. If attackers successfully breach the software's defenses, they could gain access to a wealth of sensitive data, which could have severe consequences for the affected entity.

Furthermore, the compromise of file transfer software can have broader implications beyond the immediate data loss. It can erode trust among stakeholders, damage the organization's reputation, and lead to legal and regulatory repercussions. The fallout from a breach may also require significant resources to investigate, remediate, and recover from, further exacerbating the impact on the organization.

## Potential Costs Over and Above Breach Mitigation

Regulatory fines can run into the millions, representing a substantial cost for organizations that fail to comply with data protection regulations. In industries governed by strict privacy laws, such as healthcare (HIPAA), finance (PCI DSS), and the European Union's General Data Protection Regulation (GDPR), non-compliance can result in hefty penalties. These fines can escalate rapidly, especially in the event of a data breach caused by insecure file transfer practices.

For instance, in 2023, Meta Platforms in Ireland was fined a [staggering €1.2bn](#), when it was found to have mishandled personal data when transferring it between Europe and the United States. Two years earlier, Amazon Europe received a [€746m fine](#) for non-compliance with general data processing principles.

Lost productivity is another consequence of inefficient file transfer practices. Manual processes, errors, and delays can impede workflows, causing employees to waste time navigating cumbersome systems or troubleshooting transfer issues. This not only hampers productivity but erodes employee morale and engagement.

Given the critical role that file transfer software plays in facilitating business operations and communication, its security must be a priority for organizations. File transfer solutions that employ robust security measures, such as encryption, access controls, and regular security audits can help mitigate the risk of breaches and safeguard the confidentiality of sensitive data.

## Rise Seen in Attacks Targeting File Transfer Apps

Over recent years, the number of cyberattacks targeting widely used file transfer applications has risen. These incidents have underscored the critical need for secure file transfer solutions to protect sensitive data and ensure operational continuity for businesses of all sizes.

One prominent attack exploited a previously unknown SQL injection vulnerability in a popular file transfer solution, impacting nearly 1,000 organizations worldwide, including high-profile entities and various government agencies. The attackers accessed and potentially manipulated files stored in the repositories.

In another incident, threat actors began exploiting a critical vulnerability in another centralized file exchange application that large enterprises use to transfer large files or large volumes of files at very high speeds. Interestingly, the attackers actively exploited the vulnerability almost four months after the patch was initially released.

This incident highlighted the vulnerability of such systems and the importance of robust security measures.

## MFT Addresses the Challenge of Outdated FTP Methods

To meet the challenge of outdated FTP methods, robust Managed File Transfer (MFT) solutions are being adopted by organizations to securely and reliably exchange files both internally and externally. MFT solutions provide a centralized platform for managing, monitoring, and controlling file transfers across various networks, including cloud, on-premises, and hybrid environments.

MFT systems typically offer encryption, authentication, audit trails, scheduling, and automation to ensure files are transferred safely and efficiently while adhering to compliance requirements and organizational policies. This helps mitigate risks associated with data breaches, ensures data integrity during transmission, and gives organizations greater visibility and control over their file transfer operations.

## Core Features and Benefits of Comprehensive MFT Solutions

### Enhanced Security

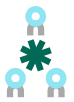
Enhanced security is a critical aspect of comprehensive MFT solutions to safeguard sensitive data and mitigate the risks associated with file transfers. This encompasses several key security features:



**Encryption:** MFT solutions employ robust encryption algorithms to secure files during network transmission. These solutions typically use industry-standard encryption techniques, such as Advanced Encryption Standard (AES), RSA Security, or Triple Data Encryption Algorithm (Triple DES), to encrypt data, ensuring it remains confidential and unreadable to unauthorized parties. Encryption converts plaintext data into ciphertext, making it indecipherable without the corresponding decryption key. Encrypting files during transmission keeps sensitive information safe from interception or eavesdropping by malicious actors, maintaining data confidentiality and integrity.



**User Authentication:** A modern solution will also enforce stringent user authentication mechanisms to verify the identity of individuals accessing the system. This usually requires users to authenticate themselves using credentials like usernames, passwords, or multi-factor authentication (MFA) methods. These solutions may also integrate with existing identity management systems to centralize user authentication processes and ensure consistency across the business. This helps to prevent unsanctioned individuals from gaining entry to sensitive data, reducing the risk of data breaches and unauthorized access.



**Access Control:** Another crucial feature of any robust MFT solution is granular access control mechanisms that enable businesses to define and enforce file access permissions. Administrators can specify access rights and privileges on a per-user or per-group basis, determining who can view, modify, or delete files and directories. Access controls help businesses enforce the principle of least privilege, granting users only the permissions strictly necessary to do their jobs. Specific MFT solutions also support role-based access control (RBAC), allowing administrators to assign users roles with predefined permissions based on their job roles or responsibilities.

### Improved Visibility and Control

Improved visibility and control are another compelling benefit of MFT solutions, as it is crucial for organizations looking to enhance oversight, security, and efficiency in their file transfer operations. This includes:



**Monitoring:** Robust real-time monitoring capabilities allow administrators to track file transfer activities closely across the company's network. Through intuitive dashboards and customizable alerts, administrators can get instant visibility into file transfer operations, including transfer status, file sizes, transfer rates, and the parties involved. Real-time monitoring facilitates timely resolution of issues such as failed transfers, bottlenecks, or unusual activities, helping administrators take immediate corrective actions and minimize disruptions.



**Audit Trails:** By maintaining comprehensive audit trails to capture detailed information about every aspect of file transfers, essential metadata such as timestamps, user identities, file names, source and destination addresses, and transfer protocols are recorded. Additionally, audit trails document system events, configuration changes, and security-related activities, providing a complete historical record of file transfer operations. These serve as valuable forensic evidence in investigations of security incidents or compliance audits, helping firms demonstrate adherence to regulatory requirements and internal policies.



**Automated Workflows:** Through the automation of repetitive tasks and workflows, MFT solutions empower organizations to streamline file transfer processes. Administrators can define automated workflows that specify the sequence of actions to be taken during file transfers, such as encryption, decryption, compression, file validation, and routing, based on a predefined set of criteria. Automated workflows also allow businesses to schedule transfers at certain times or in response to trigger events, such as the availability of new files or changes in data conditions.

## Increased Scalability and Reliability

Increased scalability and reliability are other benefits of modern MFT solutions. This is critical for organizations dealing with soaring volumes of data and growing demands for efficient file transfer operations. To realize these benefits, the MFT solution should feature the following:



**Centralized Management:** A centralized platform for managing all aspects of file transfer operations helps save time and resources. Instead of relying on disparate tools and manual interventions scattered across various departments or locations, companies can consolidate their file transfer processes into one unified system. This approach streamlines management tasks, cuts complexity, and enhances visibility and control over file transfer activities. Administrators can set standardized policies, access controls, and monitoring parameters from a central console, ensuring consistency and compliance across the organization.



**Bandwidth Optimization:** A robust MFT solution will incorporate advanced techniques to optimize bandwidth usage during file transfers. One of these techniques is data compression, which reduces the size of files before transmission, minimizing the amount of data transferred over the network and speeding up transfer times. Some solutions implement bandwidth throttling mechanisms to regulate the data transmission rate, preventing network congestion, and ensuring bandwidth-hungry file transfers do not disrupt critical business processes. MFT will also feature high availability and clustering techniques, to ensure efficient resource utilization and uninterrupted access to services by distributing network traffic across redundant systems. This enhances reliability and performance in critical applications.

## Streamlined Compliance

Another benefit is efficiently and effectively managing regulatory requirements within an organization, particularly in the context of file transfer activities. This approach has two key components:



**Automated Reporting:** A good MFT solution will feature robust reporting capabilities that automatically generate detailed insights into file transfer activities, compliance status, and security incidents. By automating the reporting process, companies can save time and resources, as manual reporting tasks are prone to errors and can be labor-intensive.



**Support for Industry Standards:** Any solid MFT tool will have been designed to adhere to various industry protocols and standards such as SFTP, FTPS, PGP, HTTPS, AS2/AS3/ AS4. By aligning with these standards, organizations can ensure that their file transfer processes meet their industry's legal and regulatory requirements. This includes implementing encryption protocols, access controls, audit trails, and other security measures mandated by regulatory bodies.

## MFT Meets Evolving Business Needs

Managed File Transfer solutions offer comprehensive features and benefits that enable organizations to securely exchange files, improve operational efficiency, and maintain compliance with regulatory requirements.

By adopting robust MFT solutions, organizations can mitigate security risks, enhance visibility and control, and optimize file transfer processes to meet the changing needs of their business operations.

## About Globalscape

Globalscape Enhanced File Transfer (EFT) is a complete MFT platform that streamlines and encrypts the exchange of data between systems, employees, customers, and trading partners. Administration is easy, yet detailed enough for complete control of your file transfer system.

### How much could your organization benefit from secure file transfers?

Explore managed file transfer's many features and security settings with a personalized demo of our enterprise-level solution, Globalscape EFT.

[www.globalscape.com/demo](http://www.globalscape.com/demo)

[www.globalscape.com](http://www.globalscape.com)



#### **About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at [fortra.com](https://fortra.com).