

YOU INHERITED A FILE TRANSFER SYSTEM. *NOW WHAT?*

WHAT TO DO WITH YOUR HAND-ME-DOWN
FILE TRANSFER SYSTEM



GLOBALSCAPE

INTRODUCTION

When you become the new owner of an organization's file transfer system, it can quickly complicate your responsibilities in a number of ways. Here is a look at a few common situations:

- ✓ **Outdated managed file transfer (MFT) software** are often vulnerable to a variety of bugs, patches, or processes limitations. Outdated software can expose an organization to a security breach.
- ✓ **Homegrown file transfer systems** come in all shapes and sizes. Sometimes they are made up of various file transfer protocols and the often come with little to no documentation. Sometimes they are highly customized with no backup if a script breaks.
- ✓ **Disparate file transfer systems** are sometimes a combination of several technologies, systems and applications, both old and new. They often have multiple logins, no centralized dashboard for management, and little visibility, which makes them tedious and high maintenance to manage.

Oftentimes when an existing platform is outdated, homegrown, or cobbled together from many different components, they lack the security, reliability, and efficiency capabilities required by today's organizations. They can also be high maintenance and a constant drain of resources.

According to a [Harvard Business Review Analytic Services study](#), more than a third of surveyed IT respondents believe that "current IT systems make it difficult or time-consuming for employees to access core business data and apps without help." They were also "too busy supporting legacy tech" to spend time improving systems for employees.





"The average private sector employee in the UK who uses IT systems and reports wasted time at work said they waste an average of nearly 6% of that time due to technology problems. ... The top three IT issues faced by workers were slow-running systems and equipment (65%), connection failures (54%), and outdated software (32%)." (TechRepublic, "IT failures cost UK companies £35B per year in lost productivity")

IT COMPLICATES EVERYTHING

Not only do these types of systems complicate how you manage your IT infrastructure, they also complicate other business initiatives. When other departments or lines of business within your organization rely on various workflows and processes, you need a secure, reliable, and efficient platform to do the job.

CUSTOM SCRIPTS, CUSTOM RISK

If you are running customized scripts, processes, or workflows on your existing file transfer system and you have no documentation to reference, then you may have to try the "sit-and-wait approach" hoping that nothing breaks. However, the sit-and-wait approach is not conducive to a secure, reliable, and productive IT ecosystem.

SECURITY RISKS INCREASE, COMPLIANCE IS MORE DIFFICULT

An outdated, disparate, or homegrown file transfer system can create unnecessary security and compliance vulnerabilities for your entire network. For instance, if you have an old and unmanaged application that was sitting in a dark corner of your organization, then it likely has not been updated in years. This would leave a glaring opportunity for malicious actors to use old Java or SSL exploits to infiltrate your network.

Additionally, while the security components of a file transfer system play a crucial role within any compliance initiative, so do the reliability and efficiency components. If your system is difficult to maneuver around, or if it is unreliable or inefficient, then it is not likely to get easier when you are required to provide proof of compliance. In most cases, when a system has issues with efficiency or reliability, security issues are not too far off.

IT IS A PRODUCTIVITY KILLER

The effect of an inherited existing homegrown or legacy system can have a ripple effect across the organization, causing poor or delayed transfers of sensitive, mission-critical data. These outdated solutions can also cause a business to default on service level agreements (SLAs) that directly tie to work with customers or partners.

MAKING LIFE BETTER WITH MFT

Modern managed file transfer (MFT) software provides a centralized mechanism for users to manage their file transfers with greater efficiency, reliability, and security. Compared to homegrown or outdated file transfer systems, a modern MFT platform provides a higher degree of governance and control, enabling low-code (or no code with some MFT platforms) automation for complex workflows and operational visibility. MFT users can manage their IT productivity and compliance requirements more efficiently with respect to business resources and business demands. Adding further benefit, using a modern MFT platform helps:

1. Provide multi-layered security, reducing your security vulnerabilities and risks
2. Streamlining complex file transfer workflows and processes
3. Increase IT flexibility and responsiveness
4. Facilitate security compliance

WHAT TO LOOK FOR

With the right MFT platform and security strategy, you can have a stronger and more secure IT infrastructure. A strong MFT platform provides proactive and preventative security measures to mitigate external attacks or internal mishaps, while also enabling an organization to facilitate compliance.

1. CENTRALIZED DASHBOARD

Using a decentralized file transfer process makes it more difficult to manage compliance. Auditing various applications and systems without a comprehensive perspective of your IT system is very time consuming and error prone.

If your IT system is disparate or comprised of multiple FTP servers, then you are likely experiencing issues and facing many risk factors. You may have data silos that cause various challenges for employees that need timely access to data for data-driven business decisions. You may also find that you are spending more time logging into various systems and platforms, troubleshooting, or doing other related maintenance tasks.

By consolidating your systems into one centralized managed file transfer platform, IT oversight and management is easier. Monitor and track all file transfer activity in near real-time from start to finish. Control all user access and permissions. You can consolidate your efforts and configure your necessary patches, upgrades, and workflows, supporting your productivity and compliance initiatives.

With a centralized dashboard you can get the drill down granular details of a file transfer status, monitor activity between internal or external partners, create reports or charts, track various key performance indicators (KPIs) such as the percentage of failed or successful file transfers, most active partners, transaction trends, and more.

2. SECURITY

You need to understand your overall security posture. In addition to establishing how your existing system or processes supports your security and compliance needs, you want to determine whether your platform is conducive to supporting employee needs and IT needs. If shadow IT practices are causing problems or you are using less secure methods of file transfer, like FTP, to move secure data, then your security or noncompliance risks will be higher.

Data privacy requirements continue to become stricter. A preventative approach will save you from the heartache of a data leak or security breach. Be sure to examine two areas: encryption and data wiping.

Encryption: To safeguard data at rest, a combination of strong public-key and symmetric cryptography can provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures.

If PGP is not available, Microsoft's Encrypting File System (EFS), included in Microsoft Server operating systems, can be enabled to transparently encrypt files during disk read/write. Data is encrypted while it is being written to disk, and decrypted prior to transferring.

An effective MFT allows you to monitor and control each of those systems and security layers all in one location. Managing activity on your network, such as allowing or blocking IP addresses, multi-factor authentication, encryption, real-time reporting, email alerts, and other active security measures can all be done with an MFT platform that sits inside your network.

Data Wiping: Your MFT solution should have the option to configure data sanitization/ data wiping options to securely delete or purge the files by writing over the initial data using encrypted and/or pseudorandom data. Many government regulations and standards require data wiping to ensure the deleted data does not end up in the wrong hands.



3. AUTOMATION

Many IT teams turn to methods such as HTTP web-based transfers, Windows Task Scheduler, and outsourced data management to automate data transfers. Yet, each of these methods have limitations that modern MFT doesn't.

When you have a higher volume of file transfers or complex workflows to configure and manage, customized or homegrown scripts may have seemed like the right fit. However, if you are holding your breath, wondering which script will break and when, then it is just not worth it!

When you use an MFT platform with advanced automation features like Event Rules, you can establish controlled and automated processes for key data transfer tasks, whether they are system to system, person to system or person to person.

In addition to ensuring the controlled and secured movement of data, MFT with automation helps with data security, compliance mandates, and employee productivity. Unlike many of the common methods of data automation, an MFT platform with automation can provide multi-layered security capabilities and enhance employee productivity in a high-volume, enterprise environment.



DIFFERENT FLAVORS OF MFT

Deployed on-premises, in the cloud, both (hybrid), or as a managed service, MFT platforms are helping organizations move away from legacy system challenges and toward a modern IT infrastructure.

Here's a high-level look at the different MFT deployment models:

On-premises MFT deployments – Deploying MFT on-premises gives organizations a high degree of control, governance, and visibility. On-premises deployments of MFT are often the first choice for organizations that are required to manage sensitive data and strict compliance regulations.

Cloud MFT deployments – Deploying MFT in the cloud gives organizations a high degree of flexibility in both budget and capabilities. Cloud MFT deployments enable greater agility, helping organizations respond faster to market demand, all while supporting their security and efficiency needs.

Hybrid On-premises and Cloud MFT deployments – Hybrid deployments of MFT give organizations the best of both worlds. If they are not ready or prefer not to “go all in” with a cloud platform just yet, a hybrid platform can help with the transition from on-premises to cloud, or it can be project-specific.

SaaS or Managed Services MFT – While cloud deployments provide many benefits, many organizations lack the expertise or resources to manage a cloud infrastructure efficiently. A SaaS-based platform allows organizations the opportunity to outsource the management of underlying infrastructure, like application updates, capacity planning, and other ongoing maintenance.

➤ **MFT PLATFORMS ARE HELPING ORGANIZATIONS MOVE TOWARD A MODERN IT INFRASTRUCTURE**



PROTECT YOUR NETWORK AND PREVENT SENSITIVE DATA

EFT: AN AWARD-WINNING MFT PLATFORM

Globalscape's award-winning [MFT platform, Enhanced File Transfer™ \(EFT™\)](#), provides enterprise-level security for collaboration with business partners, customers, and employees, while automating the integration of back-end systems.

Built-in regulatory compliance, governance, and visibility controls help keep your data safe, while outstanding performance and scalability help boost operational efficiency and maintain business continuity.

Administration is easy, yet granular enough to provide complete control of your file transfer system. With EFT, you can:

- Use industry-standard secure protocols to secure your file transfers
- Monitor file movement and user activities on your network
- Create a multi-layered security solution for data storage and retrieval, authentication, and firewall traversal with Globalscape DMZ Gateway®
- Use data wiping to thoroughly delete data
- Use malware prevention and IDP tools to protect your network and prevent sensitive data from leaving the network
- Encrypt stored data
- Merge or replace legacy file transfer systems
- Automate workflows and integrate systems

Security, reliability, and efficiency are foundational needs and should be core elements of your IT infrastructure. They are also core elements of a strong MFT solution, like EFT. We can work with you and your unique business and file transfer needs.

[Download a Free Trial of EFT Today at www.globalscape.com/try-globalscape-software.](http://www.globalscape.com/try-globalscape-software)

MAKE BUSINESS FLOW BRILLIANTLY

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit www.globalscape.com or follow the blog and Twitter updates.

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249, USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support
© 2018 GlobalSCAPE, Inc. All Rights Reserved

GLOBALSCAPE