Brought to you by:

Progress MOVEit

Managed File Transfer

for dummies

A Wiley Brand

Manage file transfers securely

Reduce business risk and ensure compliance

Automate file transfers and save money

Progress MOVEit Edition

Andrew Lorandos, CISSP

About Progress MOVEit

MOVEit is an automated file transfer system that lets you manage, view, secure, and control all file transfer activity through a single system. For any business in any industry, MOVEit provides a secure file transfer solution for meeting security and compliance requirements, while reducing administration time and costs.

MOVEit Managed File Transfer (MFT) software is used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Assure the reliability of core business processes and the secure and compliant transfer of sensitive data between partners, customers, users, and systems with MOVEit. Visit **www.ipswitch.com/moveit** for more information.

Managed File Transfer

Progress MOVEit Edition

by Andrew Lorandos, CISSP

for dummies®
A Wiley Brand

Managed File Transfer For Dummies®, Progress MOVEit Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-71926-7 (pbk); ISBN: 978-1-119-71914-4 (ebk). Some blank pages from the print version may not appear in the ePDF version.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Steve Hayes

Production Editor: Siddique Shaik

Business Development Representative: Molly Daugherty

Table of Contents

INTRODUCTION 1
About This Book 2
Icons Used in This Book 2

CHAPTER 1: **Understanding Managed File Transfer** 3
Understanding What MFT Is 4
Understanding the Requirements and Benefits of MFT 5

CHAPTER 2: **Reviewing the Techniques and Requirements of MFT** 7
Understanding the Various Ways to Transfer Files 7
Email 7
Physical transport 8
File sync and share 8
File transfer clients and servers 8
MFT 9
Looking at MOVEit MFT Solutions 9
MOVEit Transfer 9
MOVEit Cloud 10
MOVEit Automation 10

CHAPTER 3: **Staying Compliant** 11
Data Security 11
Authentication 12
Guaranteed Delivery 12
End-to-End Data Encryption 13
Automation and Control 13
Automating All Methods of File Transfer 14
Considering MFT Security 15

CHAPTER 4: **The Need for Mobile MFT** 17
Understanding Why You Need Mobile MFT 17
Surveying the Professionals 18
Emailing confidential mobile files 18
Thinking you're compliant 18
Being certain you can audit all transfers 19
Having confidence in visibility and control 20
Looking ahead 20

CHAPTER 5: **Seeing MFT in the Real World** 23
Looking at the Healthcare Industry 23
Working with a hospital 23
Working in insurance 25
Sharing with the Government 26
The challenge 26
The solution 27
Handling Critical Finances 27
The challenge 27
The solution 28

Introduction

Moving data securely and reliably to support critical business processes has never been more important — and challenging. Today's digital business processes span the "borderless enterprise" and link business units, partners, agents, contractors, and customers. Sensitive data must be protected in transit and at rest with the proper controls to meet business needs and comply with government and industry regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

Data transfer presents a major challenge for business. Historically, data has been transferred in many ways: File Transfer Protocol (FTP), Electronic Data Interchange (EDI), Value Added Networks (VAN), physical devices such as tapes, DVDs, and thumb drives, email, text messages, shared cloud storage, and Application Integration Middleware. Data is hard to manage because copies are kept anywhere and everywhere with little control.

Managing file transfer risk, time, and cost ensures smooth operations across the supply chain. A strong managed file transfer (MFT) solution can address these needs in a more secure, reliable, compliant, automated manner while being more cost effective and easier to use. Moving data reliably and securely at the right time is a critical success factor in many businesses no matter what form the data may take.

Business agility has become vital to business success. If your existing file transfer systems require scripts to be written and maintained, significant manual activities, and high-touch maintenance to add or change partners or processes, there's a better way. MFT enables both security and full automation, which eliminates errors and reduces costs. Automation is one of the major reasons to embark on an MFT project.

The amount of data stored today has grown hundreds of times over the last five years. Files that contain personally identifiable information (PII) such as credit card numbers or Protected Health Information (PHI) such as medical records are protected by privacy laws. As the digital economy becomes the norm, sensitive files must be transferred securely with full traceability across a growing array of end-point devices. And failure isn't an option. Business leaders' challenges today are security, responsiveness

(or IT agility), and reliability. Protecting data is a major concern, and business systems must exchange or synchronize data across the open Internet with remote locations, while maintaining archives. Making data accessible, while also keeping it secure, is the value of MFT. As data volumes and security concerns grow, MFT has emerged as an indispensable technology.

About This Book

If your business transfers a large number of sensitive files to internal and external parties, this book is for you. *Managed File Transfer For Dummies,* Progress MOVEit Edition, helps you understand best practices for securely and efficiently transferring files to support business critical processes and the risks and costs of unmanaged file transfers.

Icons Used in This Book

I certainly think every word of this book is memorable and valuable, but I highlight extra important content with a few icons in the left margins.

The Tip icon alerts you to pieces of information that may save you time, frustration, or money.

The Remember icon highlights basic MFT rules — information that you should take from the MFT discussion and file away in your brain.

The Warning icon cautions you about serious situations where you can cause personal harm or harm to your work in the context of MFTs.

Sometimes I use techy words or definitions or throw some statistics at you. In these cases, I use the Technical Stuff icon to let you know it's coming. If you have a techy brain, you may love beefing up on these tidbits; otherwise, you can skip this info and not suffer any loss of brain power.

IN THIS CHAPTER

- Knowing what MFT is
- Looking at the requirements and benefits of MFT

Chapter 1
Understanding Managed File Transfer

In this chapter, I give you some insight into why you may need managed file transfer (MFT). To do that, I explain what I mean when I use the term MFT and explain the various requirements and benefits of using MFT.

REMEMBER

Sometimes people use terms differently, so I want to define exactly what I mean when I use the term MFT. The term should be *data transfer* because files are just containers for data, but you will see the words *files* and *data* used interchangeably. And *transfer* means to move data either over a private network in a data center or over the public Internet. For this book, I use the word *managed* to mean "transferred in a controlled way." And then, think of *controlled as scheduled, protected, logged, measured, automated,* and *clearly described*. I usually add the word *secure* to cover the areas of encryption, authentication, and audit. So when I speak about secure MFT, I refer to a set of computer programs that provide security, automation, and management for the transferring of data between multiple entities.

Understanding What MFT Is

You can transfer data in many ways, but most of them are manual, unmanaged, and often insecure. But MFT is managed, secure, and often automated. A server (or multiple servers) is configured and used to control transfers to and from people, systems, and processes.

TECHNICAL STUFF

Automated means that repetitive operations can easily be scheduled to repeat at any interval from minutes to days. (I cover security and compliance in Chapter 3.)

REMEMBER

A good MFT system can often replace all the other methods used to move data, depending on your needs. MFT provides a single solution that mitigates risk and ROI compared to the implementation and maintenance of other solutions for moving files across the borderless enterprise.

MFT is an ideal solution in the following instances:

- Data is moved between people, processes, and combinations of both.
- Data being transferred must be secure and protected.
- Repetitive file transfer tasks are manual or automated by using scripts that take days or weeks to create.

INTEGRATING DATA

Moving data is really about integrating data between business systems to automate business processes. Three common integration patterns that IT architects talk about are messaging, shared database, and file transfer. The messaging infrastructure uses an Enterprise Service Bus (ESB), a software solution that tightly couples all the applications via carefully crafted message formats. This process requires careful planning and is expensive to implement but enables low-latency transactional processing. Another pattern is a shared database, which works well in one location but is a single point of failure and not very scalable. The file transfer pattern can be implemented by using an MFT solution.

- Moving large batch transaction files meets business needs and is less costly than low latency transactional systems.
- Audits of file transfer operations are failure prone or costly.
- Data is transferred over the open Internet with third parties, including vendors, customers, and remote sites.
- Data compliance is an organizational priority.
- Growth of file transfer volume, users, and file size continues to increase year over year.
- Lack of reliability and continuous operations of existing FTP systems negatively impacts the bottom line.
- Troubleshooting file transfer errors and responding to end-user requests for status affect IT responsiveness.

Business runs on data, and this integration of data, people, and processes is the heart of today's enterprise. MFT provides for the automated transfer of large files between people and systems, scaling to the highest volume in a highly secure manner with complete logging and visibility of all activities.

Understanding the Requirements and Benefits of MFT

After you know what an MFT system is, you need to understand the top system requirements and the benefits of deploying such a solution. Each of these requirements is a decision that needs to be made prior to, or during, deployment:

- **Single-system compatibility:** Will your solution be capable of handling all methods of file transfer no matter the size?
- **Integration with IT security infrastructure:** Will your solution be compatible with your existing IT Security Infrastructure and services?
- **Centralized logging:** Will your solution be able to centrally log all file transfer activities, to pass audits and prove compliance?
- **Self-administration:** Will your solution enable users to invite other users to participate in secure file transfers and view the status of file transfers?

- **Easy deployment:** Will your solution be easy to deploy and configure, initially and long-term?
- **End-to-end encryption:** Will your solution support data encryption on the network and while sitting on storage devices?
- **Guaranteed delivery, non-repudiation, and expiration rules:** Will your network with guaranteed delivery of transferred data, non-repudiation of data received, and expiration rules that expires data after a given date?
- **Deployable in the cloud and on-premises:** Will you require a solution that's accessible by those on a single network or by different organizations at the same time on the same system without any possibility of compromise?
- **Automation:** Will your solution automate your file transfer tasks and eliminate the need to write and maintain scripts and eliminate manual tasks?
- **Scalable with failover capabilities:** Will your solution provide you with the option of spreading the workload across multiple servers automatically ensuring that any transfer jobs would be honored even though there may be a service interruption?

REMEMBER

An MFT solution that's scalable with failover capabilities gives you 24/7 continuous operations and zero data loss with automated failover.

IN THIS CHAPTER

- Taking a look at transferring files
- Examining the requirements of MFT

Chapter 2
Reviewing the Techniques and Requirements of MFT

In this chapter, you explore the various means of file transfers and understand why an MFT solution is preferred. You also take a look into three types of MFT functional options.

Understanding the Various Ways to Transfer Files

You can transfer data in many ways, but most of them are manual, unmanaged, and often insecure. This section gives you the common ways currently in use along with why they aren't good MFT solutions.

Email

The most common way of transferring files is via email attachments. Email is pervasive and well understood by users, but

email was invented to replace "snail mail" letters, not to replace large-scale, managed, secure file transfers. Email is convenient but error-prone due to invalid addresses, delivery failures, and file size limitations. It's also not easily tracked or automated.

Physical transport

You can physically transport data with a thumb drive (also called USB drives, flash drives, jump drives, and so on). Physical transport is best used for the casual transfer, but it has a downside: It's a common vector for virus propagation and can by no means be considered "managed."

File sync and share

With enterprise file sync-and-share (EFSS), users can save files to the cloud or on-premises and then access those files on their desktops and mobile devices. Putting all your critical files on a server and sharing them widely is wildly different from managing the transfer of selected files to selected individuals and systems by using strong encryption, enhanced security, and careful logging, automating workflows, and file processing tasks. Any system that automatically syncs files to unsecured mobile devices is going to be inherently insecure.

REMEMBER

Services like Dropbox, OneDrive, Google Drive, and other file sync and share solutions are popular ways to share files for collaboration between *small* groups of people. If your business is regulated or audited because of credit card, healthcare, financial, or other personal data concerns, make sure that you're even allowed to use public cloud services.

File transfer clients and servers

Another method of file transfer is via File Transfer Protocol (FTP). This method is quite common and may be used explicitly through FTP commands, called through various scripts, or embedded within other programs. FTP has proliferated widely and is used by nearly every business worldwide, but transferring data via FTP is difficult to automate, secure, track, and manage. FTP is inherently not secure.

MFT

MFT is automated and secure. You can certainly automate the other various ways of transferring files, but it's just more work and maintenance. A server (or multiple servers) is configured and used to control transfers to and from people, systems, and processes.


TIP

The reason to choose MFT over the EFSS tool (see the earlier section "File sync and share") is because it has visibility, access control, and authentication.

Looking at MOVEit MFT Solutions

MOVEit MFT software is used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. MOVEit assures the reliability of core business processes and the secure and compliant transfer of sensitive data between partners, customers, users, and systems.

Based on the MOVEit MFT solution, you can configure three optional modules when planning your deployment. The module(s) you decide on determines the features you require.

MOVEit Transfer

MOVEit Transfer enables the consolidation of all file transfer activities to one system to ensure better management control over core business processes. It provides the security, centralized access controls, file encryption, and activity tracking needed to ensure operational reliability and compliance with SLA, internal governance, and regulatory requirements.


REMEMBER

If you decide to leverage another solution, check the latest release notes for your software solution's requirements. Also, ensure that you provide 24/7 technical support in the rare case an issue arises.

If you decide that MOVEit Transfer meets your organization's needs, make sure to address the following requirements:

- **Server software requirements:** Operating system (OS) and database
  - Windows server 2012 R2, 2016, or 2019
  - MySQL (included) or Microsoft SQL Server
- **Server hardware requirements:** Storage, CPU, and memory
  - Quad core CPU
  - 8 gigabyte (GB) RAM
  - 1 terabyte (TB) storage
- **Target SMTP email server requirement:** Email server to relay package notifications
- **Server-side content engine (AV/DLP) compatibility:** Antivirus (AV) and data loss prevention (DLP) engines
- **Client/browser compatibility:** Browser, mobile, and batch clients

MOVEit Cloud

MOVEit Cloud, the MFT-as-a-Service offering, provides full security, reliability, and compliance of MOVEit Transfer with the convenience of a cloud-based service. MOVEit Cloud is auditor certified PCI and HIPAA compliant. Providing the same advanced security controls as MOVEit Transfer, it ensures GDPR compliance in external file transfer activities involving personal data.

Because MOVEit Cloud is offered as a SaaS offering, there are no requirements as far as the server-side is concerned. The only requirement you need to keep in mind is ensuring that your team has the latest client OS running and that each client has a compatible browser running.

MOVEit Automation

MOVEit Automation works with MOVEit Transfer or FTP systems to provide advanced workflow automation capabilities without the need for scripting. MOVEit Automation accelerates the rollout of new services and the onboarding of new external data sharing partners by reducing development time while significantly reducing the likelihood of errors.

IN THIS CHAPTER

- Achieving data security
- Improving agility and productivity
- Looking into data protection and compliance law

Chapter 3
Staying Compliant

Whether by regulation or by a business need, data often needs to be kept secret. Purchasing an MFT solution from a vendor that supports the standards that are important to you is the easiest and most cost-effective way to stay in compliance. This chapter covers the areas that fall under the umbrella of data security.

Data Security

Any MFT solution must also be a security solution and offer standards-based integration to other IT security and user management systems. You should familiarize yourself with the following security protocols:

- Security Assertion Markup Language (SAML) for identity and authentication
- Lightweight Directory Access Protocol (LDAP) for accessing lists of authorized users
- Internet Content Adaptation Protocol (ICAP) for interfacing with virus scanners and content filters

Data loss prevention (DLP) and antivirus software are critical to ensure overall organizational security.

REMEMBER

Carefully consider your security needs. According to the Information Security Institute, unauthorized access to data with Personally Identifiable Information (PII) and Personal Health Information (PHI) for one record or millions of them could result in significant consequences, such as a loss of money, additional fees, and prolonged down time. MFT provides many security mechanisms and offers the flexibility to ensure compliance with data privacy regulations and policies.

Authentication

Authentication is proving who you are. Verifying your identity can involve validating personal identity documents, providing personal credentials, logging into a website with a digital certificate, or making sure that a product or document isn't fake.

TIP

Make sure your MFT solution supports both of the following authentication capabilities:

- **Multi-factor authentication (MFA):** MFA, also referred to as *two-factor authentication* (2FA), is a method of logon verification when you must provide at least two different types of proof to gain access to your email, financial accounts, health records, and so on. This extra security check helps protect your assets and includes not only a password but also a second code that's sent to your email or texted to you.
- **Single sign-on:** Because it's difficult to remember a lot of passwords that may require frequent updates, many companies institute single sign-on, which uses a centralized identity provider system for user management.

Guaranteed Delivery

Guaranteed delivery has three elements:

- **Non-repudiation:** Both parties to a file transfer have been authenticated and authorized.

- **Integrity checking:** Cryptographically validated methods ensure integrity of transferred files, which means that you can be assured that the file securely transferred is precisely the same as the file received.
- **Tamperproof:** This is usually applied to logs, and it ensures that someone can't modify a log record in an undetected way. This, along with integrity checking, prevents data from being modified.

End-to-End Data Encryption

You may also want to protect your data by encrypting it. Most business systems and databases have security controls to protect data within their systems, but data that's exported for transfer is at risk, whether in transit across the Internet or sitting on servers within your network. Malware attacks or disgruntled employees can compromise unprotected data even within your trusted network. Encryption has many standards, and all require key management. Ensure your MFT system can work with them and also has automated key management.

Automation and Control

Beyond security, the value of MFT comes from automation. Automation is simply eliminating the need for manual intervention by having the MFT system execute the steps needed, and its value is reduced errors and labor costs. Costs include troubleshooting errors and lost files; time required to manually transfer files; and the significant skills and costs trying to craft a do-it-yourself automated process with scripts and custom programming.

WARNING

Automation is complex when using older generation file transfer solutions. Custom scripts are difficult and time consuming to create and manage, and other solutions don't offer all-in-one tools to create, schedule, and manage automated tasks without scripting or programming.

With MFT, every repetitive process involving the movement of data can be automated:

- Push files to remote servers across the Internet. For example, securely push financial transaction records in the data center to remote servers at the corporate bank.
- Pull files from remote servers across the Internet. For example, securely pull time-card or payroll data from local worksites into the data center every day at 5:00 p.m.
- Orchestrate movement of files between people and systems. For example, when patient records are received, the data is automatically uploaded into the insurance system, and an email is sent to the insurance agent to process the compensation claim.
- Process (encrypt/unencrypt or translate) and transfer files based on schedule or event. For example, inventory status records are exported from the business system once it goes below a certain level; the file is then translated into the vendor-defined format and securely transferred.

Automating All Methods of File Transfer

MFT automates the movement of files from *process-to-process*, which is how companies use MFT to securely connect systems across the Internet, such as the in-house general ledger system to the banking systems at their corporate bank. Whenever you need copies of files because one process feeds another, the benefit of automated MFT is seen.

In addition to process-to-process file transfers, MFT also automates *process-to-person* transfers. This operation is used, for example, to securely push a sales report to your email or mobile device every day. Another example of process-to-person is a primary care physician who receives daily patient lab reports from local hospital laboratories. Process-to-person is most often used to obtain periodic copies of patient lab findings, management reports, task lists, and other sales and management reports.

A third type of file transfer method is *person-to-system.* A person-to-system operation could be a repair shop owner uploading from a web browser images of a repaired vehicle and text file of itemized costs to the insurance company server. The files can then automatically be uploaded into a back system or moved to storage. A person can put information into a business system with low development costs.

Often, an MFT solution is installed solely for *peer-to-peer (P2P) collaboration*. Peer-to-peer MFT is commonly used to satisfy ad hoc business processes. Maybe a partner or a customer needs a copy of some documents now, so the paperwork is best sent in a secure and logged way. A fully secure and safe system can lead to any number of innovations and make your company much more responsive and agile.

Considering MFT Security

A few major considerations of MFT security revolve around three areas:

- **Compliance:** *Compliance* is conforming to relevant legal, professional, and company standards. Audit teams look at policies and ensure that the actual operations satisfy requirements, often by examining log files and IT systems documentation. Your MFT solution should both specify and prove it's compliant with the standards important to your business.
- **Audit:** An *audit* is a mechanism used to inspect and verify compliance. An audit is used during an investigation to find out how the problem happened, when it happened, and what failed. The best MFT systems provide logging capability and configurable security alerts.
- **Real-time visibility:** Sometimes you need to quickly see what's going on. Your MFT solution should log every event to a central database, whether the event is the start of a transfer, the completion, or errors. That tells you what has just happened in the system, and you may want to watch in real-time to manage performance and investigate various alerts.

IN THIS CHAPTER

- Knowing why you need mobile MFT
- Getting insights from professionals

Chapter 4
The Need for Mobile MFT

Mobile MFT describes a solution that allows users to securely transfer files from their mobile devices with the same protections as their workplace MFT solution. In other words, it extends the capabilities of your core business, on-premises, at-the-office MFT solution to users' smartphones and tablets. While solutions differ in the details, a mobile MFT app should provide key features with the ability to

- Securely sign on with multi-factor authentication (MFA)
- Capture and securely share photos and/or video
- Access and transfer files between people and systems
- Manage files and folders
- Securely share folders

Understanding Why You Need Mobile MFT

Your users are going to use the simplest tool they have for secure transactions and a phone is always going to be more accessible, more connected, and just plain handier than a work laptop. If you don't give them a simple tool that makes it easy to send secure

files the same way they can in the office, you're opening the door to shadow IT and insecure file transfers.

You need mobile MFT because your users are already sending secure files via their mobile devices; they just aren't doing it through *your* MFT. That's a problem because that means you can't track these transfers, they can't be audited, and you have no idea if they were encrypted.


TIP

Look for a mobile app that's fully integrated with your existing MFT solution and then require that your users put it on their mobile devices. The expense will be minimal (and in the case of the free MOVEit Mobile app, nonexistent) but the risk reduction could be worth millions.

Surveying the Professionals

To follow up on the preceding section of why you need MFT, let me show you a survey Progress conducted. This survey of over 100 security professionals in the healthcare and finance industries was conducted to learn more about how mobile users were transferring secure files. The results were eye-opening and further show why you need to start thinking about secure MFT and deploying a solution.


TIP

For the full results of Progress's survey, visit `www.ipswitch.com/mobileMFT`.

Emailing confidential mobile files

Email is an inherently insecure medium for file transfers and doesn't support large files or any type of tamper-evident log. However, people still use it regularly to transfer secure files.


TECHNICAL STUFF

The survey revealed that an incredible 70 percent of healthcare organizations send secure files — such as patient records and insurance claims — via email. Finance professionals reported a slightly better email usage of 51 percent, but in both industries only a minority were using secure file sharing tools.

Thinking you're compliant

When mobile users transfer secure files, do they always encrypt data and comply with security and privacy mandates? The

healthcare and finance industries say yes, most of the time, but if users are sending sensitive information to and from their phones, there's no way this is trackable, compliant, or secure.

Despite the vast majority of confidential files being sent through email, on average, 66 percent of security leaders believe their employees always encrypt data and comply with security and privacy mandates. Executives in the finance industry are more certain their company's mobile file transfers are encrypted than those in the healthcare space, yet in both cases this raises some concerns.

Being certain you can audit all transfers

A huge part of MFT is having an auditable record of transactions you can report on to prove compliance with regulations. And anything less than 100 percent certainty runs the risk of massive regulatory fines or, even worse, an expensive data leak with and an equally expensive bad PR news story.

Take a look at Figure 4-1. Security professionals in the healthcare and finance industries are *not* certain they can audit and report on what their mobile users are transferring. *Not* certain — 91 percent of the time! The vast majority peg their users' abilities to do so as low as half the time.

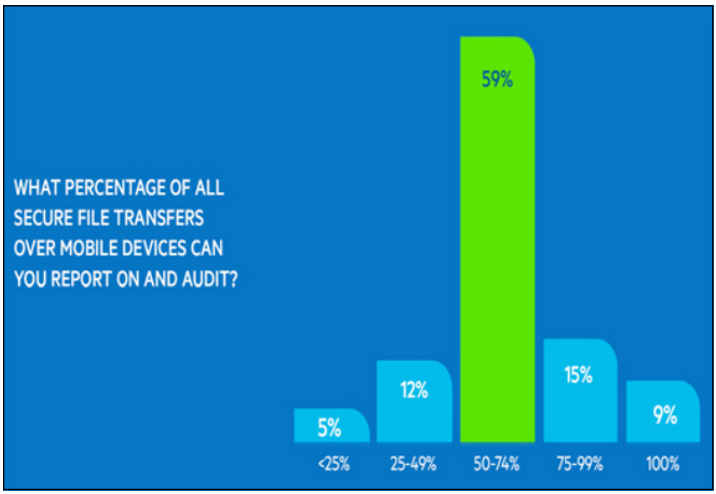

FIGURE 4-1: Only 9 percent of security professionals trust that they can audit and report 100 percent of time.

Having confidence in visibility and control

Despite the inability to audit and report (see the preceding section), an incredibly combined 74 percent of executives think they still have full visibility and control over all mobile file transfers. Healthcare seems to be a bit more realistic at 62 percent, and Finance is a bit optimistic at 86 percent, but neither number coincides with their self-admitted inability to audit all transactions.

So what does this suggest? Execs have a sense of optimism that's not likely backed up by reality. This discrepancy is particularly concerning considering the strict industry regulations like Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and Payment Card Industry (PCI). Healthcare and Finance are the most heavily regulated and should be the most motivated to deploy MFT solutions. Yet they still exclude their mobile users.

Looking ahead

While the COVID-19 pandemic has changed the way people work, the trend toward remote workers is only going to increase as quarantines continue and employers relax requirements for employees to be on site.

When asked how much the frequency of secure mobile file transfers increased during the pandemic, 65 percent of survey respondents said the frequency increased by 6 to 15 percent during the first few months of the pandemic alone. Check out Figure 4-2 for the full results of the pandemic portion of the survey.

And what about access at home versus in the office? Only 22 percent of mobile users can fully access the same file sharing systems at home that they're able to use back at the office. This means that if you have a secure MFT solution, the majority of your remote users aren't able to use it even if they want to. The obvious solution is to provide mobile MFT to all your users to prevent insecure transfers and shadow IT. Without a compatible mobile MFT solution, your risk of regulatory fines, or, worse, security breaches will only increase as more of your users work remotely.

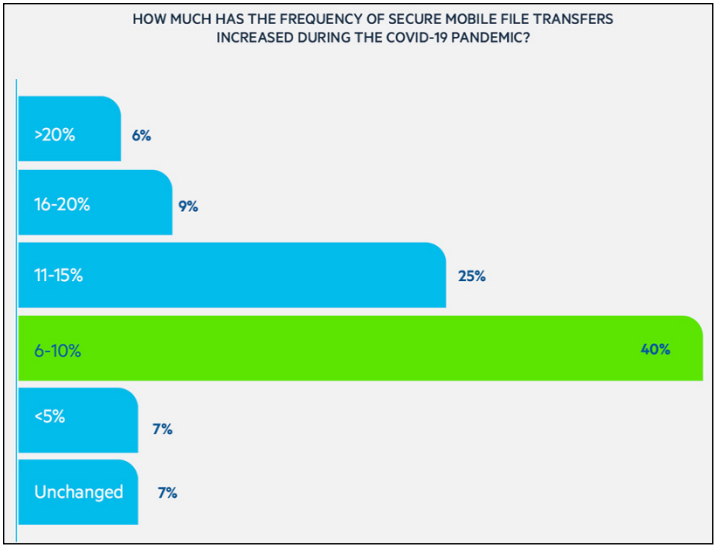

FIGURE 4-2: The secure mobile transfer frequency impacts from COVID-19.

IN THIS CHAPTER

- Recognizing critical business concerns in healthcare
- Solving government problems with MFT solutions
- Reaching into the financial realm

Chapter 5
Seeing MFT in the Real World

Managed file transfer (MFT) comprises three dimensions of value: reducing costs, reducing risks, and improving IT agility, which increases the bottom line. In this chapter, I give you case studies — in healthcare, government, and financial areas — that show you the benefits of deploying MOVEit as your MFT solution.

Looking at the Healthcare Industry

In this section, you examine two cases in the healthcare sector that show how MOVEit is a working MFT solution.

Working with a hospital

A General Hospital in Upstate, New York, handles a full array of medical services. It has tens of thousands of inpatient discharges, 100,000 emergency room visits, and over a million outpatient encounters annually.

The challenge

When faced with a need to exchange patient records and claims information with dozens of insurance companies, health plan providers, and other payer organizations so the hospital could get paid for its services, the hospital needed help. These transfers needed to be both reliable and easy to track so files didn't go missing and delay or prevent payment. Transfers also had to be highly secure to protect patient privacy and ensure compliance with HIPAA and other regulations.

The solution

The hospital's systems engineer (SE) and his team turned to MFT and selected MOVEit after evaluating it against other well-known file transfer products. Key criteria included a solution that

- Was highly secure
- Allowed transfers to be set up quickly and easily
- Handled large files
- Integrated with multiple platforms
- Provided an audit trail
- Confirmed that files had arrived successfully

After carefully evaluating the options available, MOVEit was the best choice for the hospital.

MOVEit's centralized visibility and control gave the IT staff connections with payer organizations and helped manage the transfers. The SE took advantage of MOVEit's point-and-click simplicity to set up, manage, and track more than 70 different file transfer operations between hospital servers and the systems used by payers and outside healthcare providers.

By using MOVEit, the hospital consolidated file transfers between a variety of applications, hardware platforms, and operating systems. MOVEit uploaded files from these hospital servers, encrypted them, and delivered them to third-party systems. Examples include ClaimLogic and SSI ClickON billing systems, Medicare/Medicaid payment systems, EMR systems from McKesson and EpicCare, and practice management systems used by outside physicians.

REMEMBER

Since going live, MOVEit provides the 24/7 reliability that the hospital depends on for its financial health. MOVEit continues to run smoothly, and with over a year of sustained use, the system has never crashed.

Working in insurance

Quickly and securely exchanging sensitive and confidential patient information is a must for a large health maintenance organization responsible for insuring the health of over 100,000 individuals. But this isn't an easy task given the volume and complexity of the information, compounded by the use of cumbersome scripts.

The challenge

While all tasks were "automated" batch jobs, scripting for file transfer job creation and execution is both time consuming and error prone. It's difficult to meet Patient Health Information (PHI) logging requirements. Determining when a file was transferred, where it went, and if it got there requires a lot of tedious backtracking.

Each day, the insurance subsidiary pulls in information from multiple sources: pharmacies, doctors' offices, and Medicare. A complex IT setup includes 13 secure servers and over 200 regularly scheduled tasks, some of which are run as frequently as every 15 minutes, or even minute by minute. Massive amounts of data are also moved each day from an AS/400 COBOL system. A number of these tasks require database lookups and other complex steps that are difficult to code by using scripts.

In addition to performing regular file transfer tasks, the health company's employees did many ad hoc information transfers without proper security, which put confidential files — claims data, pharmacy information, and patient information — at risk of compromise.

The solution

The file transfer challenges directed the insurance company to replace its existing FTP process with one that was easier to use, was highly secure, and would enable employees to securely send and receive zip files whenever they needed.

TIP

There was a better way: MOVEit Cloud Transfer. With this solution, the staff was surprised with how much was possible with MOVEit. Getting a data feed, loading it into the claims engine, and then waiting for the reply file used to be an ugly workflow. MOVEit took care of the whole process — taking something from an FTP site, getting it across, making a backup, loading it on to AS/400, and letting the AS/400 process the files. With MOVEit, all those old batch jobs are pretty much 100 percent automated. The ability to dynamically schedule tasks has also been very beneficial for the health company. And the automation engineer and other IT staffers no longer have to look over the system's shoulder to make sure that jobs have run successfully. MOVEit lets them know when something has worked both in the interface and via email notifications.

Based on the success with MOVEit Transfer for scheduled jobs, the insurance subsidiary decided to also adopt MOVEit Ad Hoc Transfer to manage employee on-the-spot file transfers. MOVEit Ad Hoc Transfer enables direct user file transfer through Microsoft Outlook or web forms. Users can

- Securely transfer sensitive files without worrying about file size or working with unfamiliar, difficult-to-use programs
- Automate task scripting and securely transfer files ad hoc
- Meet Patient Health Information (PHI) logging requirements
- Track file transfers
- Maintain error logs that help staff quickly drill down and identify an error's source
- Get dynamic scheduling and reporting

Sharing with the Government

A county council in the United Kingdom was transferring data between public sector organizations either via the Government Connect Gateway or a generic FTP solution. This clunky and inefficient process was awkward to use.

The challenge

Users noted that there wasn't a way of sharing sensitive information with third parties such as emergency services or housing

associations — which was a frequent requirement. Additional issues included

- Reporting around visibility, control, efficiency, and security
- Connecting with a multitude of systems, servers, and clients used by partners
- Meeting regulatory guidelines

The solution

The government council chose the following solutions:

- MOVEit Transfer server with user-friendly web interface
- MOVEit Ad Hoc for secure, efficient email attachments
- MOVEit Automation for automation of file-based processes

The council uses MOVEit in three ways. The first is to transfer information to third parties that it can't securely connect to using existing government gateways. This information may be a report concerning a member of the public or a contractual negotiation with a supplier. Secondly, MOVEit can be used by anyone wanting to send information to the council. Similar to a self-addressed envelope, a council user simply sends an empty package to the third party, in which she can place her documentation before pushing it back securely. Finally, MOVEit is used for the simple and rapid transfer of large or numerous files to suppliers.

Handling Critical Finances

An international private equity financial institution offers a wide variety of services, such as fixed-term investments, trading of public and private securities, savings accounts, checking accounts, safe deposit boxes, currency exchange, funds transfers, and insurance policies. In addition, the institution provides individual consumer credit through several channels.

The challenge

The bank's operational network includes more than 20 branches within Argentina, intermediate entities, marketers, and an in-house

sales force. With so many locations, the institution faced the following challenges:

- Automating the handling and transfer of critical bank files
- Incorporating a streamlined solution capable of managing the bank's growth and additional services
- Ensuring the integrity and confidentiality of the bank's sensitive information, intermediate entities, marketers, and an in-house sales force

The solution

The international bank chose MOVEit Transfer. With this solution, the institution saw the following results:

- More streamlined processes for information exchange
- Strengthening of security controls
- More robust technology
- File transfer security

Progress® MOVEit®

MANAGED FILE TRANSFER

File Transfer Made Simple and Secure

When secure file transfer becomes mission-critical, IT teams need the power, flexibility and security of MOVEit® Managed File Transfer (MFT). Used by thousands of businesses around the world, MOVEit offers complete visibility and control over file transfer activities.

- **Transfer sensitive information securely with end-to-end encryption**
- **Ensure regulatory compliance with access controls and audit trails**
- **Implement with ease by taking advantage of flexible deployment options**
- **Reduce end-user reliance on IT with an intuitive interface designed for self service**

Simple. Powerful. Intuitive.

Start your free trial and see what MOVEit can do for you today.

https://www.ipswitch.com/forms/free-trials/moveit

Automate your business-critical file transfers

How you protect file transfers in the borderless enterprise is changing. While it's imperative to share data today with customers and business partners, you must deal with the many regulations that protect data and the dangers of insecure files transfers. This book explains the key factors to automate and secure data exchange in the borderless enterprise.

Inside...

- Discover managed file transfer
- Understand a new generation of solutions
- Maintain security in your enterprise
- Learn about data protection requirements
- Examine how to reduce cost
- Increase IT agility
- Automate file transfer tasks

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-71926-7
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.