FORTRA

Managed File Transfer

Ultimate Buyer's Guide

Every day, organizations may exchange a considerable number amount of files with multiple participants. Documents ranging from payment transactions to purchase orders are sent to employees, remote staff, customers, and trading partners. These transfers are an integral part of how each business runs.

Because of the sensitive information often contained in files, data transfers should be protected. Documents, emails, and databases should be encrypted to limit the risk associated with an attack, breach, or user error. Organizations need to consider their network and IT capabilities to achieve a higher level of protection. And they also need to meet the compliance requirements that apply to them, like HIPAA, PCI DSS, and FISMA.

Is it possible to streamline hundreds or thousands of file transfers while still meeting the needs of trading partners, ensuring regulation compliance, and preparing for company audits? Yes.

Consider exploring a solution like secure managed file transfer that does all these tasks—with the aim of making IT and business professionals' lives easier by centralizing the management and encryption of file transfers.



Table of Contents

Getting Started

About this Guide 05

What is Managed File Transfer? 06

Understand the Benefits 07

Pre-Search Considerations

On-Premises or the Cloud 09

Industry-Specific Requirements 10

Cybersecurity & Data Breach Defense 12

Key MFT Features 13

In-Depth Evaluation

Create a Requirements Checklist 15

List Your Compliance Needs 17

Determine Your Budget 18

Find the Solution's ROI 19

Before You Buy

Read MFT Reviews 21

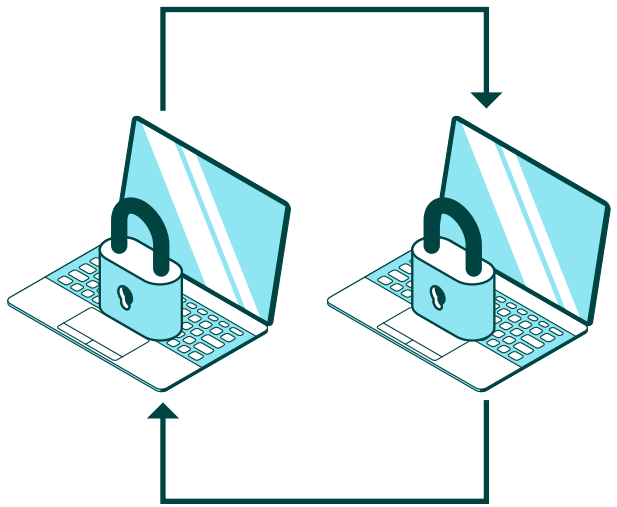
Request a Demo/Trial 22

Study Your Resources 23

After the Sale

Connect with Other Users 25

Receive Product Training 26





Getting Started

Getting Started

About this Guide

Data is a major driver in today's business world, and how a business manages data and data security can drive the bottom line for better or worse. However, finding the right solution for your business isn't always easy. Many details go into choosing the product that'll work best for you: narrowing down your options, researching their unique features, and evaluating them for potential success in your environment are just a few.

This guide strives to help you make a more informed decision by providing you with various buying considerations and explanations, including industry-and compliance-specific concerns.

By the end, you'll have a better grasp of what secure managed file transfer can do for your organization. We've also included a helpful, printable checklist to use when comparing solutions from different managed file transfer vendors.

Have questions? Contact us.



Getting Started

What is Managed File Transfer?

At a minimum, a managed file transfer (or MFT) solution is a product that encompasses all aspects of inbound and outbound file transfers while using industry-standard network protocols and encryption.

What does "managed" in managed file transfer mean? It refers to how the solution can automate and transfer data across your network, systems, applications, trading partners, and cloud environments from a single, central point of administration.

An MFT solution can be used by organizations of all sizes for file transfer needs ranging from a few dozen a week, to a few thousand a day or more. It can replace old technology too, like legacy FTP solutions or time-consuming manual processes like PC tools and legacy scripts, that are still being deployed in organizations. MFT technology is an ideal solution for a business in need of a data management system that can maximize security, compliance, productivity, and value.

MFT technology simplifies data management, providing businesses with the advantage of operational visibility and control so any potential security or efficiency risks can be identified and addressed. It can also provide a centralized and secure system that empowers businesses with the security, visibility, efficiency, and control to manage the flow of data—regardless of size, type, volume, or workflow. When it comes to the compliant management of data, an MFT platform makes things easier for what can often be a complex process. Yet, despite the wide range of MFT products on the market today, the reality is that not all MFT products are created equal.



Getting Started

Understand the Benefits

> Trends in the workplace are making managed file transfer solutions necessary. Employees are sharing a prolific amount of information through their emails [and] only 47 percent of employees think their companies have policies [for file sharing] in place.
>
> — "Select and Implement a Managed File Transfer Solution" Info-Tech Research Group Report

Many organizations struggle to fully protect the data shared by their employees, customers, trading partners, and third-party vendors. Information can easily be sent to the wrong person, stored on the wrong server, or shared with a non-secured application. With these concerns, IT teams are desperately looking for ways to minimize the risks that accompany data exchange.

An MFT solution can help do this by providing the following benefits:

Maintain Strong Cybersecurity Practices

Rely on managed file transfer security settings, including detailed audit trails and segmented groups for multiple security zones, to meet strict in-house policies.

Follow Encryption Protocols

Encrypt and compress your files in transit and at rest with several leading technologies for securing data, including Open PGP, AES, SSL, and SSH.

Meet Compliance Requirements

Secure your data to comply with regulations like PCI DSS, FISMA, HIPAA/HITECH, GBLA, SOX, and the GDPR.

Reduce Your Costs

Eliminate the need for custom scripts and programs, single-function tools, and manual processes, all of which can be costly to maintain.

Improve Your Transfers

Simplify and automate a high volume of file transfers with workflows that are easy to design and process without the use of other tools or programming.

Deploy on Multiple Platforms

Implement your solution on-premises, in the cloud, or in a hybrid environment. Or look for a hosted software-as-a-service (SaaS) solution wherever you need flexibility and scalability to match the growth of your business.

Better Visibility and Control

An MFT solution enables organizations to track data movement, giving you immediate visibility and control. Knowing where data is coming from, where it's going, and who can access it at all times is essential to retain visibility, one of the biggest obstacles to handling data.

Increase Operational Efficiency

Handle manual daily tasks and processes with ease with the data transfer automation capabilities that an MFT solution provides. Productivity can remain steady and reliable, helping to eliminate employee-based limitations such as vacations, turnover, or human error.



Pre-Search Considerations

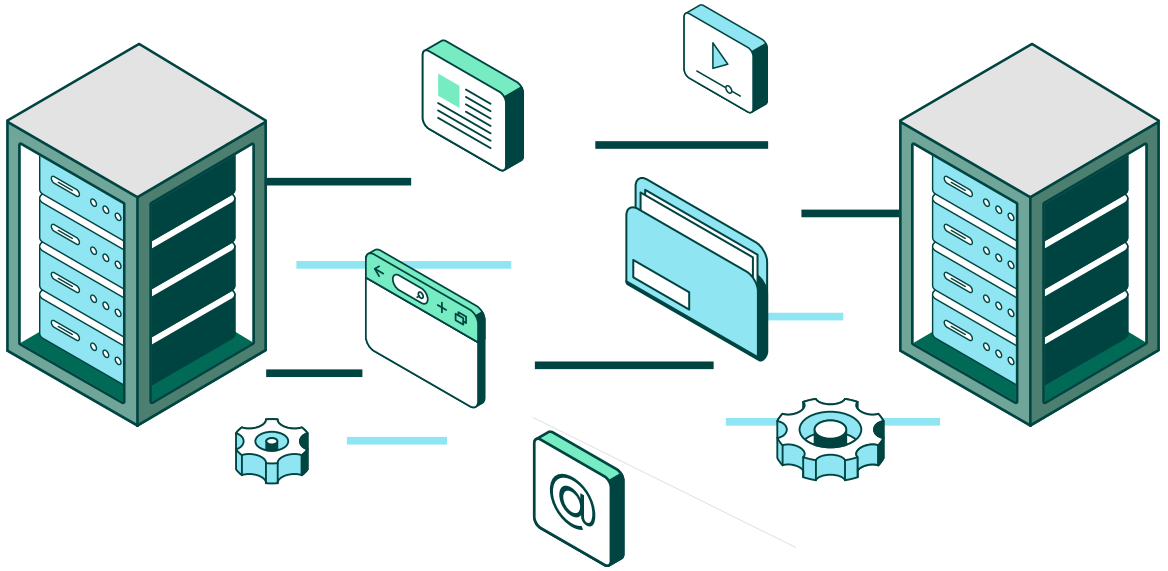
PRE-SEARCH CONSIDERATIONS

On-Premises or the Cloud

In Cybersecurity Insiders' 2021 Cloud Security Report, it was found that 71 percent of organizations are pursuing either a hybrid or multi-cloud strategy. With only 27 percent of companies relying on a single cloud deployment and 76 percent of organizations using two or more cloud providers, the cloud is growing in popularity at a rapid rate.

Although they can offer more flexibility in how data is used, managed, and protected, multi-cloud environments often add complexities and security challenges that must be addressed effectively. As a result, MFT vendors work hard to make sure organizations have the flexibility they need to meet their business requirements. This includes the ability to work in multiple environments, from on-premises to the cloud, to a hosted (SaaS) environment, or to somewhere in between (hybrid). Some even offer cloud versions of the MFT solution alongside vendor-hosted environments.

Determine which environment you plan to integrate your MFT solution in before you start your search. Don't be afraid to ask questions about how a solution works in your chosen environment and check how difficult it may be to migrate if you start on-premises and later want to move to the cloud – or vice versa.



PRE-SEARCH CONSIDERATIONS

Industry-Specific Requirements

What industry are you in? Keeping industry-specific needs in mind when evaluating MFT solutions will make the decision processes much easier, as you'll be able to vet what will and won't work right away. To get you started, here are a few important requirements to consider in the following industries:

Healthcare

Healthcare organizations need to secure their ePHI data and ensure their files are easily transferred and accessible to other locations and departments. The MFT solutions you evaluate should segment users, provide strong authentication methods, offer detailed auditing and reporting for worldwide data protection regulations (like HIPAA in the U.S., the EU's Directive of Data Protection, and Canada's PIPEDA), and coordinate patient data with outside physicians and remote offices.

Logistics

Distribution and warehouse organizations must be able to automate the exchange of orders and EDI documents with their trading partners. Managed file transfer can help ease this burden by securing data for SOX 404 and 409, maintaining records for 21 CFR Part 1.236-1.368, meeting FTC regulations for tax filings and inventory control, generating audit trails, and controlling access to sensitive documents.

Higher Education

Post-secondary schools must protect confidential student information, both university-wide and in the exchange of data with authorized third parties. Managed file transfer can help schools achieve compliance with FERPA, PCI DSS, GLBA, FISMA, and HIPAA, as well as protect student data through encryption, detailed audit logs, centralized user administration, and enforced password policies.

Insurance

The insurance industry must meet onerous compliance burdens and find a way to simplify and automate the data they exchange with business partners. A good MFT solution will help insurance companies meet SOX, GLBA, HIPAA, and HITECH requirements; secure data in compliance with the Dodd-Frank Act; maintain the integrity of files in motion for OIG, Medicare, and Medicaid; transfer data in bulk for ETL and migrations; and more.

Banking and Finance

Banks and financial institutions understand the importance of protecting sensitive data. The right MFT solution will help you achieve PCI DSS and GLBA compliance; provide tracking, auditing, and delivery requirements for Basel III; secure private data for SOX 404 and 409; and secure data in transit and at rest for the Dodd-Frank Act.

PRE-SEARCH CONSIDERATIONS

Industry-Specific Requirements

Manufacturing

Product manufacturing frequently requires the secure exchange of data files between departments, business partners, and (sometimes) government entities. Any MFT solution you consider should secure data for SOX 404 and 409, maintain records for 21 CFR Part 1.236-1.368, meet FTC regulations for tax filings and inventory control, generate audit trails, and control access to sensitive documents.

Public Sector

Government agencies face significant regulations and security policies. In addition to meeting compliance requirements for FIPS 140-2, SOX, GLBA, PCI DSS, and HIPAA, organizations in the public sector are also accountable for FISMA, a mandate that requires them to create, document, and implement a plan to ensure their information systems are secure. In addition, solutions must be secured from the Product Compliant List of the National Information Assurance Partnership's Common Criteria and Evaluation and Validation Scheme (NIAP-CCEVS). The right MFT solution can help with all of this—and more.

Retail

Escalating instances of data theft emphasizes the need for retail locations to safeguard customers' personal data and credit card information. Managed file transfer can help retail companies comply with PCI DSS, SOX, and FTC regulations, implement internal policies that conform to the Non-Bank Financial Services Rule, and control access to documents with enterprise-level security settings (like user and group roles).



PRE-SEARCH CONSIDERATIONS

Cybersecurity & Data Breach Defense

With data breaches rising at an alarming rate across many industries, IT teams are focused on implementing strong cybersecurity practices in their organizations and looking at their third-party applications, software, and networks closer than ever and ensuring they incorporate proper and stringent encryption practices.

When evaluating managed file transfer solutions, consider what vendors offer for security and data breach defense. Make sure they're putting security first and ask how they'll work with you to protect the sensitive information you share on a daily basis.

Here are a few questions to get you started:

- What types of encryption standards are supported?
- Does it use FIPS 140-2 validated encryption ciphers?
- Can I authenticate users against LDAP or Active Directory?
- Can I segment my organization into multiple security zones?
- Can I define various permissions for separation of duties?
- Can I perform multi-factor authentication?
- Can I restrict users to specific directories and subfolders?
- Does this solution offer notifications (email and/or SMS) for login failures, rejected files, and other irregular activity?
- Does this solution track all user events and file activity?
- Can I generate management reports of trading partner activity?
- Will the solution block brute-force and DoS attacks?
- Does the solution meet the security standards required for Common Criteria certification?



PRE-SEARCH CONSIDERATIONS

Key MFT Features

There are several MFT solutions on the market. How should you determine which is best for your organization? When exploring your options, here are some features to look for:

Auditing and Reporting

Audit logs help you monitor the activity in your environment for all movement of files. Reporting metrics provide statistical details, graphs, and charts of this activity.

Cloud Support

Cloud deployment gives you the flexibility to automate and secure file transfers in the cloud, no matter where those files reside. Look for a solution that scales with your organization and works with popular cloud computing platforms like Amazon Web Services and Microsoft Azure.

Some MFT solutions also offer built-in integrations for popular web and cloud applications like Salesforce, SharePoint, and Microsoft Dynamics 365. These integrations make it easy to move files to and from the services you use every day.

Remote Agents

Remote agents can automate file transfers and workflows on systems throughout your enterprise. They are managed by a central deployment of the product, allowing you to run processes and transfers across multiple locations.

Automation

A MFT solution with batch automation will allow you to determine when your file transfers perform. Look for an option that can execute multiple transfers concurrently, trigger when another process completes, and comes with a builtin scheduler, which eliminates the need for other tools or software to launch your workflows.

Data Loss Prevention Integration

Enhance your MFT infrastructure by integrating a Data Loss Prevention (DLP) solution. With DLP, you can detect, inspect, and secure critical data across email, web, and the cloud. You can also minimize your risk of accidental data loss, data exfiltration, and cyberattacks – plus, reduce the impact on day-to-day operations.

Extensive Security Controls

Enterprise-level security will help you meet stringent in-house policies and compliance requirements. Make sure the MFT solution you evaluate comes with features that safeguard your data and restrict users to only the areas of the product they need.

Secure Email Capabilities

A solution that offers a secure way to send email will help ensure the security of your messages and files by turning them into encrypted packages. These packages can then be downloaded through a protected HTTPS connection.

Flexible Web Client

A browser-based interface allows you and your trading partners to perform file transfers through HTTPS. This type of interface may give your team the best flexibility because it doesn't require a desktop client installation.

Additionally, look for a solution with good mobile support, so you can check your file transfer metrics and system activity on-the-go from any device, including tablets and smartphones.

Load Balancing & Clustering

Load balancing allows you to process high volumes of file transfers by spreading the workload across multiple systems. Clustering (active-active) allows the automatic failover to another system if a server in the cluster goes down.

EDI File Translation

Many traditional EDI tools are complex and time consuming to configure. A robust solution with EDI file translation should support critical X12 and EDIFACT standards and combine file transfer and EDI into one, easy-touse solution for reading, writing, and mapping X12 and XML files between databases.



In-Depth Evaluation

IN-DEPTH EVALUATION

Create a Requirements Checklist

Once you've identified the features you want in an MFT solution and have an idea of what your organization needs in terms of deployment, industry, and cybersecurity, it's helpful to create a checklist of requirements that you can easily refer to when evaluating different MFT solutions.

Here's an example requirements checklist to get you started:

Requirement	Vendor #1	Vendor #2	Vendor #3
I can administer file transfers without having to install software on my PCs.			
The solution can run on _____ platforms (e.g. Windows, IBM i, Linux, Microsoft Azure).			
The solution has role-based administration that allows for separation of duties.			
The solution can help guarantee the delivery of file transfers.			
The security standards I need, like _____(e.g. OpenPGP, SFTP, FTPS, and AS2), are supported by the solution.			
The solution lets me encrypt data with FIPS 140-2 validated algorithms.			
The solution produces detailed audit trails of all activity and supports SYSLOG feeds.			
I am able to compress and decompress files using ZIP, GZIP, and TAR.			
The solution can extract data from a database and convert it to popular file formats.			
The solution allows me to translate/parse received files directly into a database.			
The solution has configurable error handling (auto-retry, continue, send email alert, etc).			
The solution includes an integrated scheduler for automatically running future transfers.			
The solution monitors folders for new files and can call workflows to process those files.			
The solution includes integrated key and certificate management tools.			
The solution allows users to securely create ad-hoc file transfers.			
The solution has a DMZ gateway that allows sensitive files to be kept in the internal network (out of the DMZ), without needing to open inbound ports into that internal network.			

Requirement	Vendor #1	Vendor #2	Vendor #3
The solution allows me to trade with an unlimited number of trading partners for one price.			
I can install and start using the solution without assistance from the vendor's technicians.			
The solution helps my organization comply with critical industry and governmental regulations.			
I can create file transfers and business processes that I want to perform without creating a script.			
I can set password policies and expiration intervals for the product.			
I can authenticate users against _____ (e.g. LDAP or AD).			
The solution offers notifications for login failures, rejected files, and other unusual activity.			
The solution allows me to segment my organization into multiple security zones (with features like users, groups, roles, and domains).			
The solution allows me to track all user events and file transfer activity.			
I can generate activity reports for trading partners.			
I can authenticate server connections with a combination of passwords, SSH keys, and SSL certificates.			
I can easily integrate with the web and cloud applications I use every day (e.g. Salesforce or SharePoint).			
I can monitor file transfer metrics and system activity anywhere from any device (including smartphones and tablets).			
The solution has customers or contacts I can talk to and/or the vendor can provide links to third-party sites where their customers have submitted product reviews.			
The vendor offers 24/7 software support (including weekends).			
The vendor has professional services (e.g. product training, project consulting, migration assistance) to help me get the most out of the product.			
The solution offers flexible deployment: on-premises, in the cloud, Saas or hybrid.			
The vendor invests in the product through frequent enhancements and support.			
The vendor is Common Criteria-certified or is listed on the Product Compliant List of the NIAP-CCEVS.			

Helpful Tip: If you have questions about any of these items, contact the vendor's support team or your sales representative. Pay special attention to their response time and what kind of answer you get. A vendor that is helpful during the evaluation period will also likely be helpful after purchase.

IN-DEPTH EVALUATION

List Your Compliance Requirements

The MFT solution you're evaluating may seem perfect on the surface, but you'll want to make sure that it also meets your compliance requirements.

Compliance regulations have been established to help organizations better protect people by ensuring that they retain their right to data privacy, which is critical in today's current high risk, data transfer landscape. For many organizations, compliance mandates are the baseline for the development of a secure and compliant IT infrastructure.

See what resources the solution offers for compliance. Do they have data sheets, checklists, or a FAQ that describes how their product helps organizations meet certain regulation requirements? When you combine a comprehensive strategy that prioritizes data security and data management, then the process of meeting and maintaining compliance is simplified. A MFT product designed with enterprise level security technologies can make the process of compliance achievable and more manageable. Be sure that your MFT software delivers enterprise level security for your organization's most sensitive data and supports compliance mandates for your industry.

Beware of vendors who have labeled their MFT solution as certified: i.e., "HIPAA Certified" or "GDPR Certified. "

Most compliance regulations do not offer these certifications. Furthermore, a vendor can never guarantee their product will make your organization compliant; they can only help you take steps toward compliance. Ultimately, the responsibility to become and remain compliant rests on you and your organization.



IN-DEPTH EVALUATION

Determine Your Budget

Secure managed file transfer solutions come in all sizes and packages, from small, free FTP tools to enterprise-sized solutions that cost hundreds of thousands of dollars.

When determining how much you want to spend on an MFT solution, consider what is—and isn't—included in the price. Questions to ask the vendor's sale team include:

- Can I license specific modules?
- Are clustered and load balancing licenses discounted?
- Do you discount non-production licenses?
- Can I lease the software?
- Do you offer user- or vendor-based licensing, or are users and vendors unlimited?

Beyond initial software licenses, most buyers purchase a support package and annual maintenance, so they can upgrade to the latest product version as soon as it's available.

Also consider any optional investments you'd like to put into the product, such as professional services (e.g. migration and implementation assistance, software training) or add-on modules that expand what you can do with your MFT solution.



IN-DEPTH EVALUATION

Find the Solution's ROI

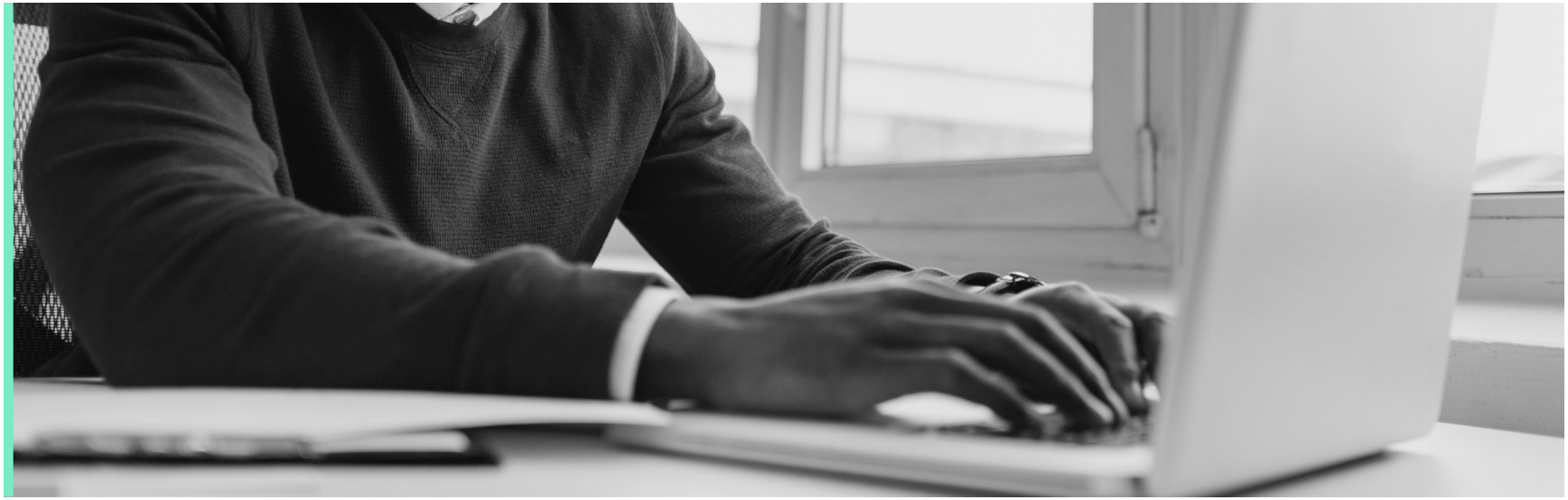
Aside from its ability to secure and automate file transfer tasks, one of the most attractive aspects of implementing an MFT solution is the positive return on the investment (ROI). This ROI varies, as the amount you can save depends on the vendor and product.

When evaluating solutions, look to see if the vendor has an ROI tool or resource that will calculate how much your organization stands to save after replacing your legacy products, manual file transfers and scripts, and homegrown workflows. A MFT technology that is designed to scale with your growing business needs will save you time, money, and most of all—it will save you the headache.

In general, MFT can help IT teams:

- Respond quickly to new security requirements without creating additional work.
- Save time by eliminating labor-intensive processes like scripting and programming.
- Grow with the needs of the organization as its data requirements become more complex.
- Avoid unplanned and unnecessary system downtime by keeping file transfers running.
- Scale with any nodes, systems, and networks added to an environment over time.





Before You Buy

BEFORE YOU BUY

Read MFT Reviews

At this point, you've hopefully filled out your requirements checklist, detailed which features are important to you, determined how much you can spend, and stacked each of these up against potential MFT solutions.

Once you've narrowed down the search, look at reviews to see what customers are saying. Are they happy with the MFT solution you're considering? What do they think the product's strengths and weaknesses are? Pay special attention to the "cons" customers mention. Is there a trend among reviewers? Is the perceived negative a dealbreaker for you?

Some good software review websites for MFT solutions are:

Capterra

PeerSpot

SoftwareReviews

G2



BEFORE YOU BUY

Request a Demo/Trial

After reading reviews, request a demo or trial for your top-identified solutions. Choosing a demo or trial (or both) fully depends on how much time you have during your evaluation period.

A demo is a live, one-on-one meeting with the vendor's product experts that usually lasts an hour, giving you time to ask any questions you have that haven't been answered by previous research. It also lets the vendor show you areas of the product you're especially interested in, so you can see the solution in action.

A trial is usually a 14- to 30-day period that allows you to use the product and see how it performs, how long it takes to set up a file transfer, what the encryption process looks like, and more. A trial is more hands-on than a demo, allowing you to explore features in your own time on your own system. This is often what professionals need to go from "considering buying" to "invested in buying."

How should you approach demos and trials?

To avoid getting overwhelmed with different solution details, we recommend first attending a demo with two or three of your top vendor choices. Setting up a trial in your environment can be time consuming; a demo will help you determine which solutions appear to be the best fit for your organization.

Once you've narrowed your options to one or two vendors, use the trial period to set up some file transfers, test encryption methods, and make sure the solution works for you.



BEFORE YOU BUY

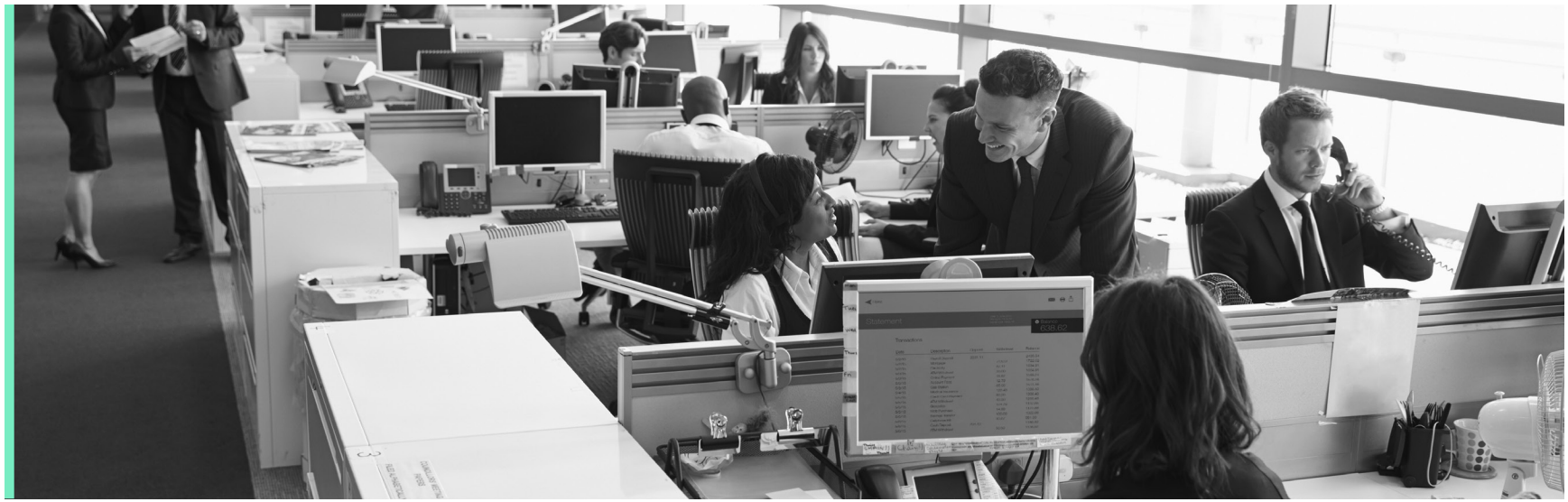
Study Vendor Resources

Finally, take some time to explore the vendor's MFT resources. Good resources, like online documentation and educational videos, tell you that the vendor is not only dedicated to developing powerful software, they're also dedicated to helping you understand everything the product can do for your organization.

Look for materials like these. They should be easy to locate:

- White papers
- Product videos
- Support forms
- Training resources
- Professional services
- On-demand webinars
- Case studies and user testimonials
- A blog with helpful, up-to-date information
- Product documentation (user guides, support articles)





After the Sale

AFTER THE SALE

Connect with Like-Minded Customers

Congratulations! You've successfully purchased an MFT solution. Once the software is up and running in your environment, you might think the process is over… but it doesn't have to be.

If you want to maximize your new investment, consider connecting with other like-minded customers who use MFT or your chosen vendor.

Some vendors offer a customer portal that gives access to community forums, where you can brainstorm with other customers over questions you might have, suggest enhancements and fixes you'd like to see in the product, and share any templates or workflows you create with others.

You might also learn how others have tackled specific MFT projects on websites like:

Stack Overflow | Reddit



AFTER THE SALE

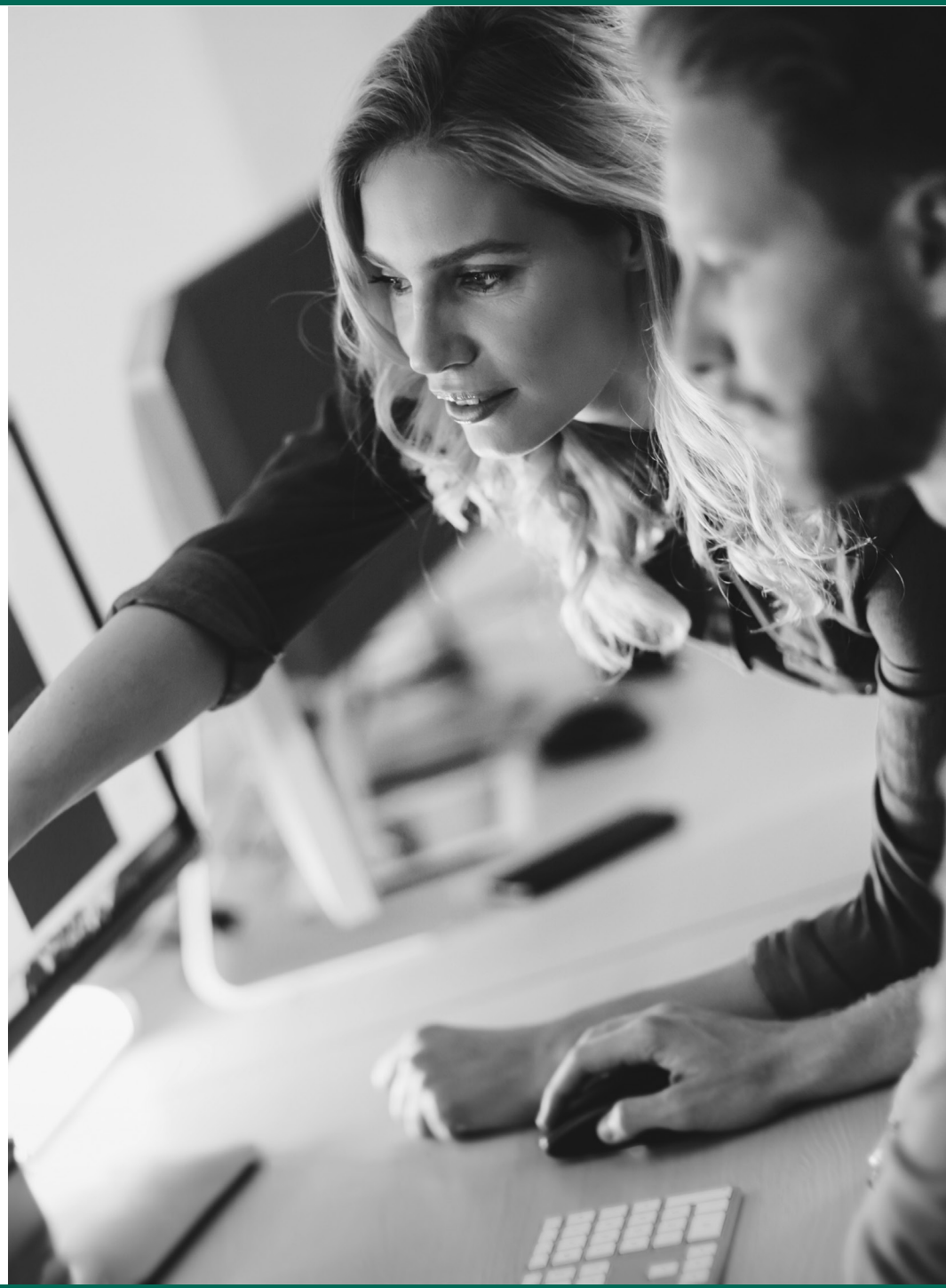
Receive Product Training and Services

Some MFT vendors offer product training and professional services, both online and on-site, for a fee. When choosing an MFT solution, see if the vendor offers training and services to help your team get proficient with the solution and put it into production in a timely manner.

Training should give you in-depth knowledge of the solution. When you request training details, consider asking the vendor the following questions:

- Are the training costs the same regardless of how many people attend the session?
- Is the training interactive or demonstrated by the trainer?
- Are there course outlines you can review before purchasing the sessions?
- Can you customize what will be covered in training?

Professional Services usually provide integration, development, and consulting services. If you don't have the resources needed to implement the solution, or you'd like to have the vendor help with the migration to the new solution, be sure to ask the vendor if those services are available.





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.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

fta-gs-gd-1022-r1-79d