maytech
A Kiteworks Company

UNDERSTANDING
MANAGED FILE TRANSFER (MFT)

A Buyer's Guide to Modern MFT

v 1.1 2023

Contents

Executive Overview

For IT leaders, MFT offers better service, an improved security posture and a positive return on investment.

File transfer is the lifeblood of many organisations.

Secure and reliable file transfer is one thing, but to maintain this over time requires significant and sustained effort.

MFT does the heavy lifting of development, maintenance and security, managing the dual risks of data leaks and hard operational failure on your behalf.

For organisations in regulated industries, it offers simplified compliance with standards including GDPR, ISO 27001, SOC2 and PCI-DSS.

When you consider the total cost of ownership, the time and cost savings are typically substantial, providing a solid return on investment.

MFT also offers a valuable human benefit at a time of growing complexity and increasing security threats, reducing the workload placed on under pressure IT professionals.

This is highlighted in Splunk's 2022 State of Security report, in which 70% of respondents said that the increase in their workload over the last year had led them to consider looking for a new role.

Operationally, it is easier to work with one centralised platform which handles all file transfers. No more wondering what script does what, or which team set up an automated process.

Built-in monitoring and audit capabilities provide enhanced control and visibility making it simple to provision, manage and debug services.

In summary, MFT offers:

- Improved security and compliance
- More efficient, cost effective and reliable file transfers
- Centralised administration for better control, monitoring and governance
- Reduced workload and Improved working environment for IT professionals

This guide is for prospective MFT buyers, to empower them with the information required to specify, evaluate and select a modern MFT solution that meets their organisation's requirements.

Managed vs. Unmanaged

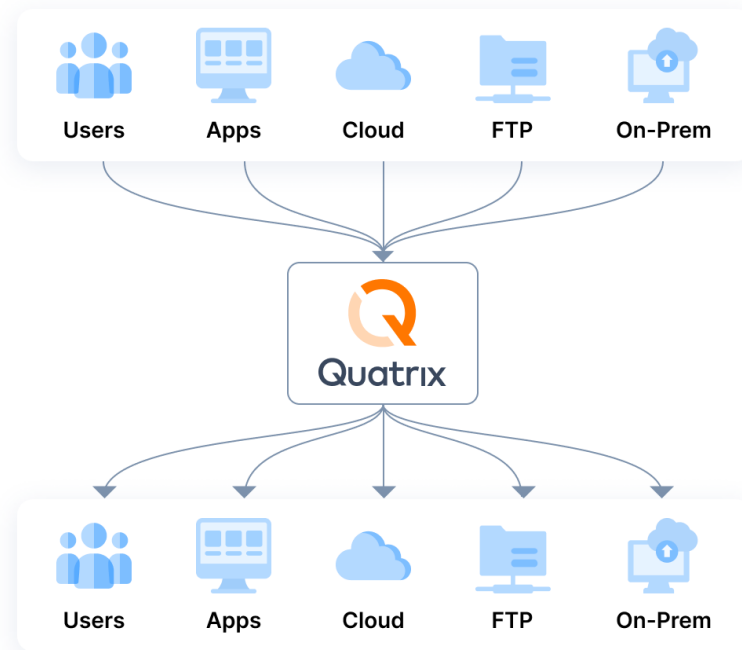## Managed File Transfer Brings Order to Chaos

Unmanaged:

- Insecure & unsanctioned file sharing
- Scripts to develop and maintain
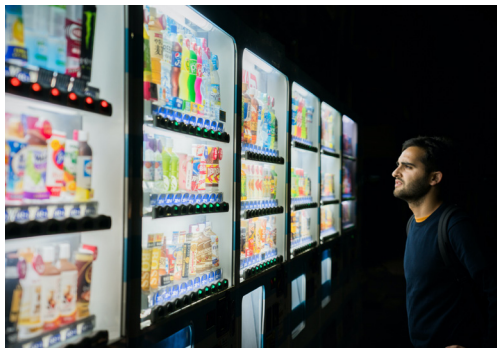- Multiple points of failure
- Difficult to debug
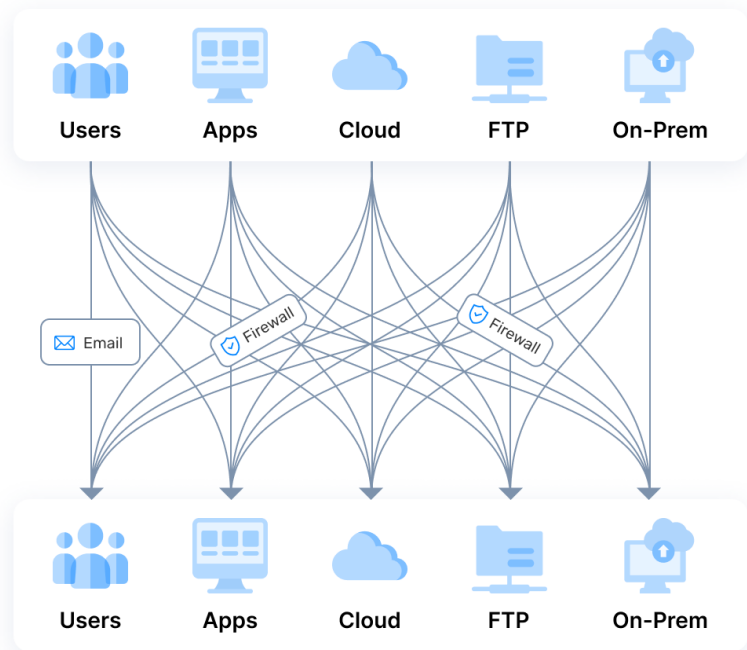
Managed:

- Centralised control and management
- Visibility of file transfers and workflows
- Single, secure, specialist application
- High availability with alerting

Modern MFT Solutions

The MFT marketplace is crowded, making it challenging to select and evaluate solutions.

This is not helped by the many adjacent, overlapping and complementary technologies:

- Enterprise File Sync & Share (EFSS)
- Document Collaboration
- IPaaS / API
- FTP / SFTP / FTPS
- Robotic Process Automation (RPA)
- Electronic Documentation Interchange (EDI)
- Secure Email
- Extreme File Transfer

Secure homegrown file transfer solutions are highly challenging to build and maintain, which is why most organisations opt for purpose-built software.

Realising the complexity and breadth of the market, they often turn to consultants to help them to navigate it.

The key requirements of MFT are typically:

- Security
- Compliance
- Reliability
- Automation
- Vendor support

But buyers also need to consider:

- Cost / contract length
- SLAs
- Ease of use / time to deploy
- Cloud vs. On-premises / Hybrid
- Connectivity options
- Integration capabilities

A key consideration for modern MFT buyers is the broader trend of cloud adoption, with all the commonly attributed benefits of improved security, compliance and reduced cost.

Established MFT players with legacy on-premises software recognise this and have responded by developing cloud offerings.

Their implementations are however often hampered by extensive legacy functionality and high existing license costs, which can make them less cost effective than new, more nimble cloud-native solutions.

This is recognised in Gartner's "Market Snapshot: Managed File Transfer, Worldwide, 2020", which identified MFT Platform as a Service (MFTPaaS) offerings as the fastest growing market segment.

04 Enhanced Security

MFT provides enhanced security, reducing the risk of data loss.

"Unmanaged" file transfers leave organisations open to risk:

- Multiple file sharing tools used by different parts of an organisation, each requiring ongoing security configuration, maintenance, patching and monitoring creates a much larger attack surface
- FTP (SFTP / FTPS) server software lacks centralised controls, encryption at rest, logging, anti-virus scanning, enterprise authentication (SAML / AD) and 2-factor authentication
- With no officially sanctioned method of sharing files, users can turn to third party tools and file sharing over email, which is a huge risk.

In Netenrich's Global 2021 Survey of IT and Security Professionals, when asked how to improve organisational security posture, the top answer was "upgrading tools" (67%).

They also reported that this was an effort being thwarted by integration difficulties, lack of expertise and the sheer number of tools to manage.

And IT staff are feeling the pressure. Splunk's State of Security 2022 report shares that:

- 73% say that workers have resigned, citing burnout
- 70% say increases in their workload have led them to consider looking for a new role
- 76% say team members have been forced to take on responsibilities they aren't ready for
- 68% report that talent shortages directly led to the failure of one or more projects / initiatives.

Outsourcing security to experts and relieving pressure on internal teams has become more and more desirable, adding to the case for MFT.

And MFTPaaS is the easiest way to achieve this, while also benefiting from the efficiencies and high availability of the cloud.

Regulatory Compliance

In the event of a data leak, the consequences of not taking all possible measures to protect data, or being found to be non-compliant are severe.

All organisations handle personally identifiable information (PII) and need to manage at least some compliance.

Once organisations identify and document all their global requirements for compliance, this becomes a daunting task to implement. It also requires regular auditing to ensure standards do not slip.

MFT software simplifies this process by handling compliance on behalf of organisations, including varying degrees of support offered by software vendors to assist with the management of compliance and audit programmes.

In the EU, the General Data Protection Regulation (GDPR) governs the collection, use and management of PII covering all types of data for EU citizens.

After Brexit, GDPR still applies to UK citizens. The Data Protection Act 2018 also applies and there are likley to be UK-specific amendments to GDPR.
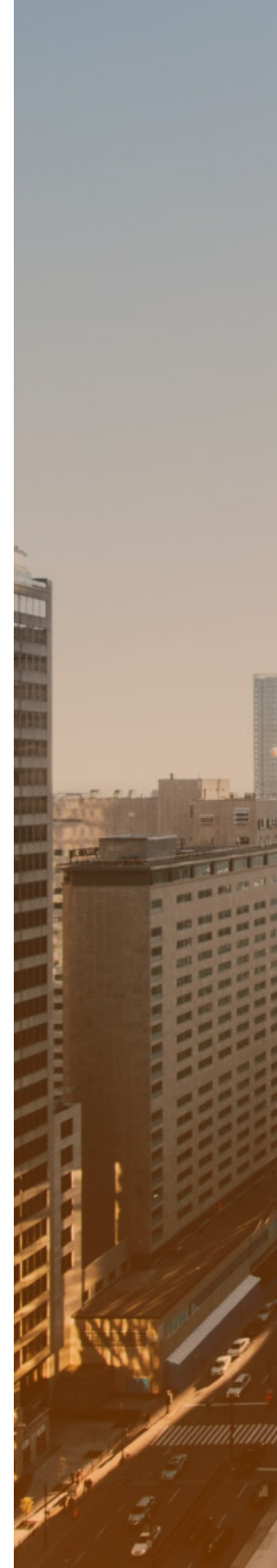
In the US, legislation is currently at a state level, with California and Massachusetts legislating independently, along with a patchwork of 14 other states. Certain data is also covered by specific legislation:

- US Privacy Act 1974 for data held by government agencies
- Health Insurance Portability and Accountability Act 1996 (HIPAA) for health data
- Gramm-Leach-Bliley Act (GLBA) for financial data.

In summary, MFT software:

- Simplifies and ensures compliance with global security standards such as GDPR, ISO 27001, SOC2 and PCI-DSS.
- Simplifies reporting to prove governance and regulatory compliance to the board and auditors.
- Provides alerting and audit trails to enable faster, more effective responses to security incidents.

And, as with security, MFTPaaS is the easiest way of implementing and maintaining compliance for MFT.

CERTIFIED LR ISO/IEC 27001

GDPR Compliant

PCi DSS COMPLIANT

HIPAA COMPLIANT

Government Procurement Service *Supplier*

Reliability for Critical Transfers

When pay slips, stock updates or daily bank transfers silently fail, the first an organisation likely knows about it is when it's already become an issue.

And when the workflow can't be easily restored, it quickly becomes an even bigger problem.

Devastating operational failures are all too often the reason organisations recognise the need for a more secure and robust method of transferring files, leading them to MFT.

Scripts are often how organisations start out with secure file transfers and automated workflows.

Then as requirements grow, scripts become more and more costly to maintain and risky to operate.

Debugging becomes easier too, because there is a centralised audit log and specialist technical support is on hand, provided by the vendor.

With MFT, an organisation is alerted when transfers fail and can investigate and resolve issues before becoming an issue.

Debugging becomes easier too, because there is a centralised system with an audit log, and specialist technical support is provided by the vendor.

Through the cloud, MFTPaaS offers superior networking and systems availability, further improving reliability.

07 Automating Repetitive Tasks & Workflows

With automation, the possibilities are truly endless. But the basic premise is that a file is received, then something happens to it, then it arrives at its destination.

Automation enables organisations to quickly react to events, build robust, set and forget workflows and offload repetitive tasks.

It can also help enforce governance and compliance by managing granular file permissions, deleting files for GDPR, managing user access and providing detailed audit trails.

Common automations include:

- Files placed into the right folders, with the right permissions
- Alerting when files arrive
- Alerting when expected files do not arrive
- Renaming of files
- Deleting files
- Actions based on file attributes; size, type, date created, name
- Taking an action after a period of time
- Automatic anti-virus scanning
- Managing user access and licences

Given the endless possibilities, completing a requirements analysis prior to selecting or evaluating a system is critical.

Independent file transfer consultants and vendor customer success teams will be able to support you in defining your use case and specifying the most appropriate and cost-effective solution.

Without doing this, you could end up purchasing a solution which does more than you need, and paying more than necessary as a result.
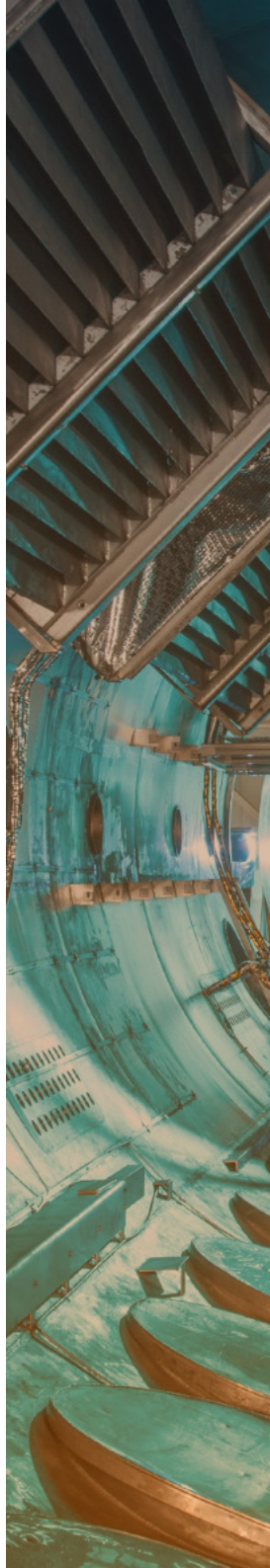
08 Vendor Selection and Support

What support is provided, on what terms, and what happens when things (inevitably) go wrong?

Vendor selection has never been more important.

The Splunk State of Security 2022 found that cloud-hosted applications are increasingly performing business-critical functions, with 66% of respondents reporting that the majority of their business-critical apps are now cloud-hosted, up from 41% a year ago.

And when organisations need support for their cloud-hosted applications, they turn to vendors for assistance.

A vendor that provides world class support and acts as a value added partner rather than "just" a supplier is invaluable.

A lot can be determined through the RFQ (Request for Quote) and RFP (Request for Proposal) process, including the vendor's reputation, capabilities and track record.

Support received early on should provide a good indication of how well you will be supported ongoing, but the best vendors should also be happy to provide references from existing customers to back this up.

Contract negotiations should include SLAs detailing any additional support requirements such as 24x7 or 5x24 support and whether it is for administrators only or is also for end users.

Payment terms and length of contract will also be discussed during negotiations. A longer commitment should provide more room for negotiation, as will added support options.

Ideal characteristics for an MFT provider:

- Established, with a track record of working with organisations in similar industries and with similar requirements
- Named account manager and responsive customer service
- Support available during your preferred hours
- ISO 27001 or similar (not just compliant, but audited and certified)
- Regular pen testing
- Option for a data centre location in a jurisdiction of your choosing
- Ongoing development, including bespoke requests
- Resilient hosting and network infrastructure with high availability, redundancy and backup SLAs.

Alternatives to MFT

MFT provides a complete solution for secure, automated, point to point file transfer.

A common misconception is that MFT competes with platforms such as DropBox, WeTransfer, Microsoft 365 or even ESB or IPaaS software such as Mulesoft or Boomi.

MFT is a specialist application which focuses on file transfer. Other applications without this specialist focus leave the door open to misconfiguration and inadvertent human error.
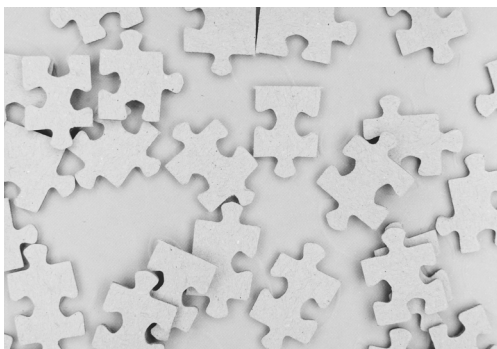
For example, in MS 365, OneDrive alone has 75 settings associated with data security, scattered across 15 different locations, which can make it hard to secure and manage, increasing the risk of data loss.

Cloud data services such as AWS, Azure and GCP provide the benefits of the cloud, but security and compliance is left up to the organisation.

They also lack the centralised control, security and audit capabilities built into MFT software which must be installed, configured and maintained.

Integration Platform as a Service (IPAAS) or Enterprise Service Bus (ESB) applications focus on the integration of disparate systems. By turning to MFT whenever file transfer is required as part of a workflow, organisations are able to utilise pre-configured endpoints.

Using MFT in this way enables quick and easy connections and the secure, compliant transfer of data.

Specialist MFT software provides:

- Ongoing future proofing for new technologies
- Ongoing future proofing for security and compliance
- Specialist technical and operational support
- Data acquisition from end users
- Data acquisition from third party systems
- Support for specific connector types
- Support for specific file types
- Very large file transfers
- Scalability to avoid congestion or latency issues
- Compatibility with legacy systems

Return on Investment (ROI)

On purchasing an MFT solution, organisations can eliminate existing costs.

When compared with achieving the same outcomes in-house, MFT typically produces a cost saving and a positive ROI.

To achieve greater ROI, organisations should audit existing tools to avoid duplication and consolidate applications to avoid unnecessary spending.

An indirect benefit is the improved speed of deployment, which can provide a competitive advantage.

For MFT, there are four different types of file transfer, which can lead to application proliferation:

- Human to Human
- Human to Machine
- Machine to Human
- Machine to Machine

From an ROI perspective, a solution which provides for all four types can potentially replace more applications.

From a human perspective, Jumpcloud's 2022 IT Trends report found that 69.1% of respondents prefer a single tool to do their job versus a handful of tools.

Delivering an improved working environment can in turn deliver substantial savings from lower recruitment and training costs, so it's unsurprising this is a desirable outcome.

As well as the cost savings, cloud-hosted MFTPaaS solutions reduce hardware requirements, leading to smoother Capital Expenditure (CapEx).

They also offer instant scalability and tighter budgetary controls.

Unlike mass-market tools, specialist MFT software vendors can typically provide customisations, support and consultancy which won't break the budget.

And unlike on premises software, it is easy to deploy updates and bespoke product customisations over MFTPaaS, so product update cycles are typically faster and less costly.
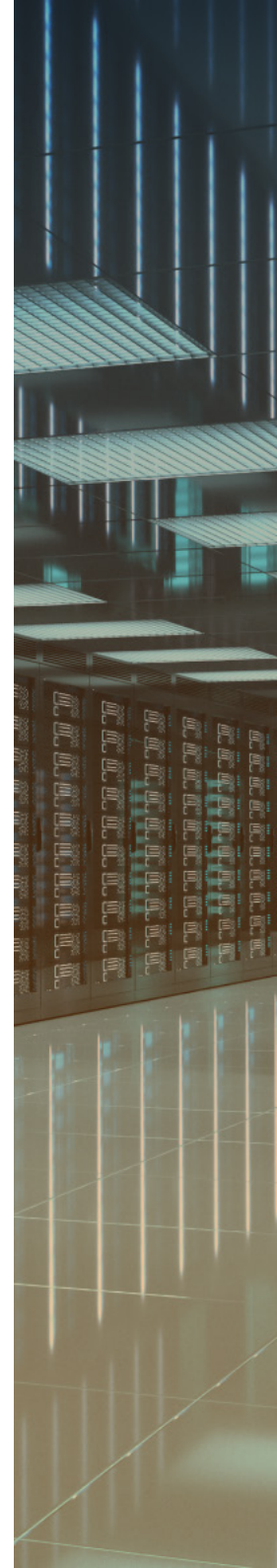
About Quatrix

Quatrix® is a proven, cloud-native solution trusted by leading organisations across the globe in industries including finance, banking, healthcare and government.

It offers quick, easy deployment and management of MFT (MFTPaaS), user to user file sharing, SFTP and secure data acquisition in one cost-effective SaaS platform.

With access to Enterprise-level features, a named account manager, responsive customer support and a knowledgeable customer success team, Maytech is a valued partner, not "just" a vendor.

To see whether Quatrix could work for you, request a demo or take a 14-day free trial online at www.maytech.net.

ORACLE®   NOVARTIS   xerox   MOLSON Coors   DURACELL®

"We wanted to keep it controlled, rather than relying on whatever external organisations were using, so we looked for a secure external file sharing solution we could own and control.

Not only were we impressed with the solution, but from the perspective of customer service and being easy to work with, Maytech is the best supplier we have ever had. I wouldn't hesitate to recommend their services."

CISO, Global Fashion House - Case Study

"One problem with many other solutions is that they aren't secure "out of the box", requiring a lot of time and effort to secure. With Quatrix, I didn't even need to read the manual - everything was simple and easy to set up and immediately secure.

There are videos to help guide me through some of the more advanced configurations, and the team is super responsive to any support questions, so I know I will be well supported."

Ross Argent, Director of Technology, ARZO - Case Study

"Our main priority was the transfer of data via SFTP but as we've gone along, we've uncovered other features that are really useful, such as the ability to make data requests, to set expiry links for files, or to be notified of downloads.

When it comes to support, Maytech has been second to none. We're very impressed with the level of service and whenever we request support, it's pretty much done within five seconds. The response is really quick."

Gareth Young, Systems Administrator, Trust Payments - Case Study