maytech
GLOBAL DATA TRANSFER

Demystifying Managed File Transfer

The Executive Leaders' Guide to Unlocking Security, Transparency, and Compliance

By Chris Thacker, Customer Success Director, Maytech

Contents

← PREVIOUS PAGE
NEXT PAGE →

← CONTENTS

Managed File Transfer: balancing security, compliance, and efficiency

← PREVIOUS PAGE

NEXT PAGE →

“In the face of serious risks and regulations, do you know where your data is – and is it secure at rest and in transit?

With a continual focus on data-driven insights, cloud adoption, and collaborative working, protecting your data remains crucial.

However, mounting public scrutiny, an ongoing focus on cloud services, and a range of international data protection regulations make this no easy task. What's more, a combination of data sprawl – a large amount of volume and variety of data within an organisation – and Shadow IT (unsanctioned tools or software used within companies) can make managing and gaining clear visibility of your data a constant challenge.

The right data management and secure file transfer solution can help find the essential balance that manages the data sprawl challenge effectively. This is the purpose of Managed File Transfer (MFT).

MFT tools enable a critical balance between data protection, regulatory compliance, and operational efficiency. It combines visibility over file transfers with central administration and access management.

For enterprises, this brings unique insights into file transfers, as well as the control needed to ensure data protection both at rest and in transit. This reduces a range of risks, including data breaches and failure to meet compliance.

Read on to learn:

How MFT tools protect data with compliant, secure file-sharing

How COOs can leverage MFT to boost operational efficiency

How MFT tools can demonstrate greater ROI for CFOs

How MFT tools can manage data governance, compliance, and risk

How CMOs can navigate larger file transfers with the need for security

← PREVIOUS PAGE

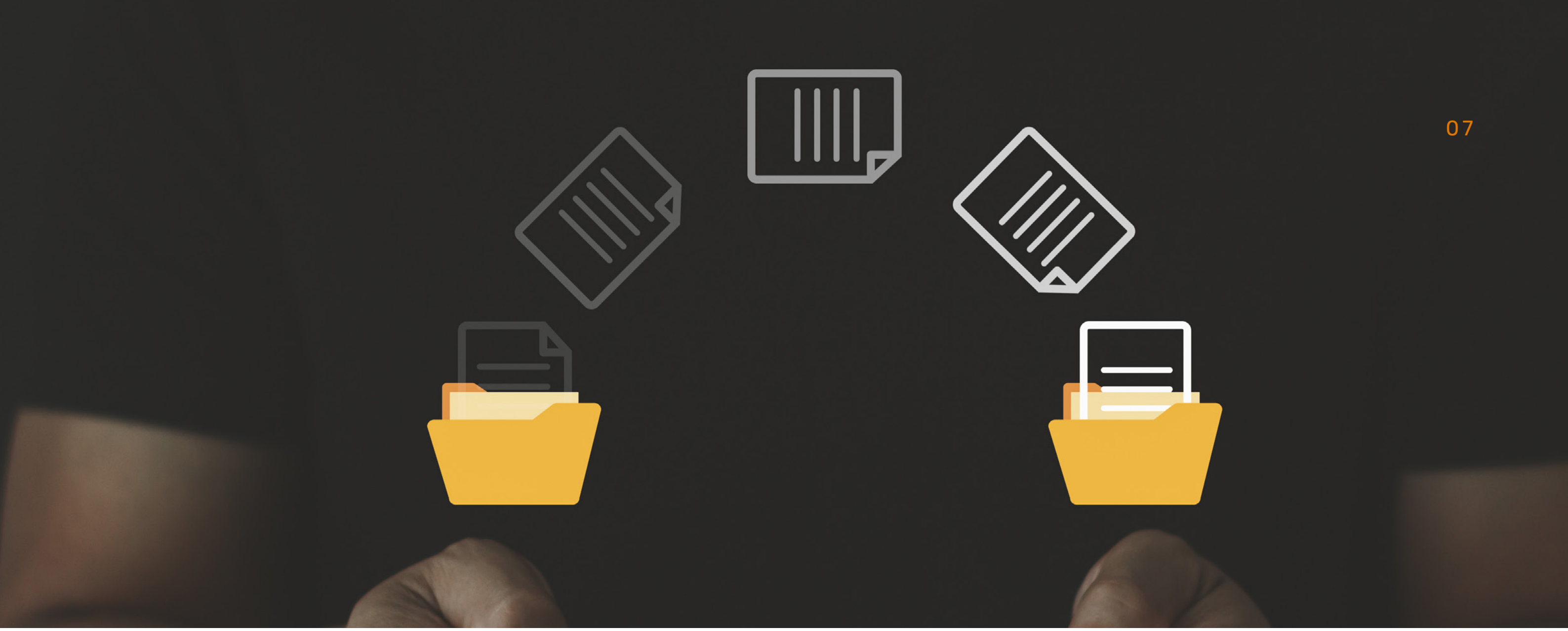
NEXT PAGE →

← CONTENTS

Why your organisation needs a fortified file-sharing solution

← PREVIOUS PAGE

NEXT PAGE →



In 2023, data is the key to continual market growth and development. Between 2022 and 2023, the global data volume rose from 97 to 120 zettabytes (each zettabyte is approximately 1 billion terabytes). With this volume expected to rise to a staggering 181 zettabytes in 2025, and much of this data classified as sensitive in nature, it's important to ensure that it is always protected.

The challenge of data sprawl and the use of Shadow IT in any organisation brings significant risks to unprotected sensitive data, both at rest and in transit.

Catastrophic for both small independent businesses and international organisations, the global average cost of data breaches reached £3.45M in 2022. Even more detrimental is the damage to your business's reputation – as clients, customers, and partners take their business elsewhere to avoid further damage. Taking advantage of a centrally managed, visible, and secure approach is vital to winning and more importantly retaining business.

← PREVIOUS PAGE

NEXT PAGE →

Empowering efficiency for COOs on their digital transformation journey

For Chief Operating Officers, secure and compliant file sharing should be a core consideration in any digital transformation initiative. Introducing this advanced and secure level of file sharing can boost operational efficiency, bring in greater opportunities for productivity, and streamline processes – all while making it simpler to maintain compliance and security.

> If 2022 was the year of hybrid cloud, then 2023 could be the year that businesses come to understand the advantages of diversifying their services across several cloud providers,

Bernard Marr, Forbes 2022.

This trend in diverse cloud adoption within enterprises demonstrates a new attitude to Digital Transformation – one willing to introduce new cloud services if they have a demonstrable value for enterprises. However, as the number of cloud services within an organisation keep growing, so too does the challenge of managing them all.

Increasingly diverse infrastructures brings with them increasingly complex workflows. To navigate this challenge, MFT tools act as a valuable intermediary between endpoint-to-endpoint transfers. Able to centrally aggregate data moving throughout their business and cloud services – COOs can now unlock new avenues to efficiency and greater operational control.

← PREVIOUS PAGE

NEXT PAGE →

← CONTENTS

Streamlining operations with automation

← PREVIOUS PAGE

NEXT PAGE →

Intuitive automation features can also help you to streamline your operations. Offloading repetitive tasks to free up valuable resources, streamlining daily batch transfers, and enhancing scripted home-built environments are all examples of this in motion.

MFT tools allow you to automate a wide range of task, often in flexible, no-code platforms. This gives back valuable time that can be focused on high-value tasks.

Some common automations include:

- Alerting when files arrive or do not arrive
- Out-of-the-box integrations with major cloud apps
- Automating transfers between applications
- Automatic anti-virus scanning
- Managing user access and licences

As well as these applications, automated MFT tools provide companies with a corporate solution for external user-to-user file transfers, as well as a robust method for receiving data from third parties.

Learn more about the benefits of automation

How MFT tools demonstrate greater ROI for CFOs

Without comprehensive visibility over workflows and processes, understanding how to correctly invest in security tools remains a core challenge – preventing users from determining if tools are overtly costly, if they're limited or redundant in functionality, or if they're inflexible (demanding expensive workarounds as a result).

At the same time, the demand for correct data security has never been more needed, with one recent breach costing an enterprise over $25 million in cleanup. Leveraging the right tools, and taking a centrally managed stance, is essential – but how can CFOs identify the correct data security platforms to invest in?

← PREVIOUS PAGE

NEXT PAGE →

The first steps CFOs can take to understand how to invest in data security

To gain this visibility, and successfully prevent costly risks, CFOs need to begin by questioning their current security and data management processes. Consider questions like:

How secure are the business's file transfer applications – both person-to-person and automated?

This will give you an understanding of the current risk level posed to your file transfer applications and, as a result, your sensitive data. Understanding this current risk level can help inform areas of your business that needs to be strengthened.

Does the business have any legacy systems that might be exploited?

Legacy systems may come with out-of-date encryption ciphers, or other factors that could lead to them being exploited.

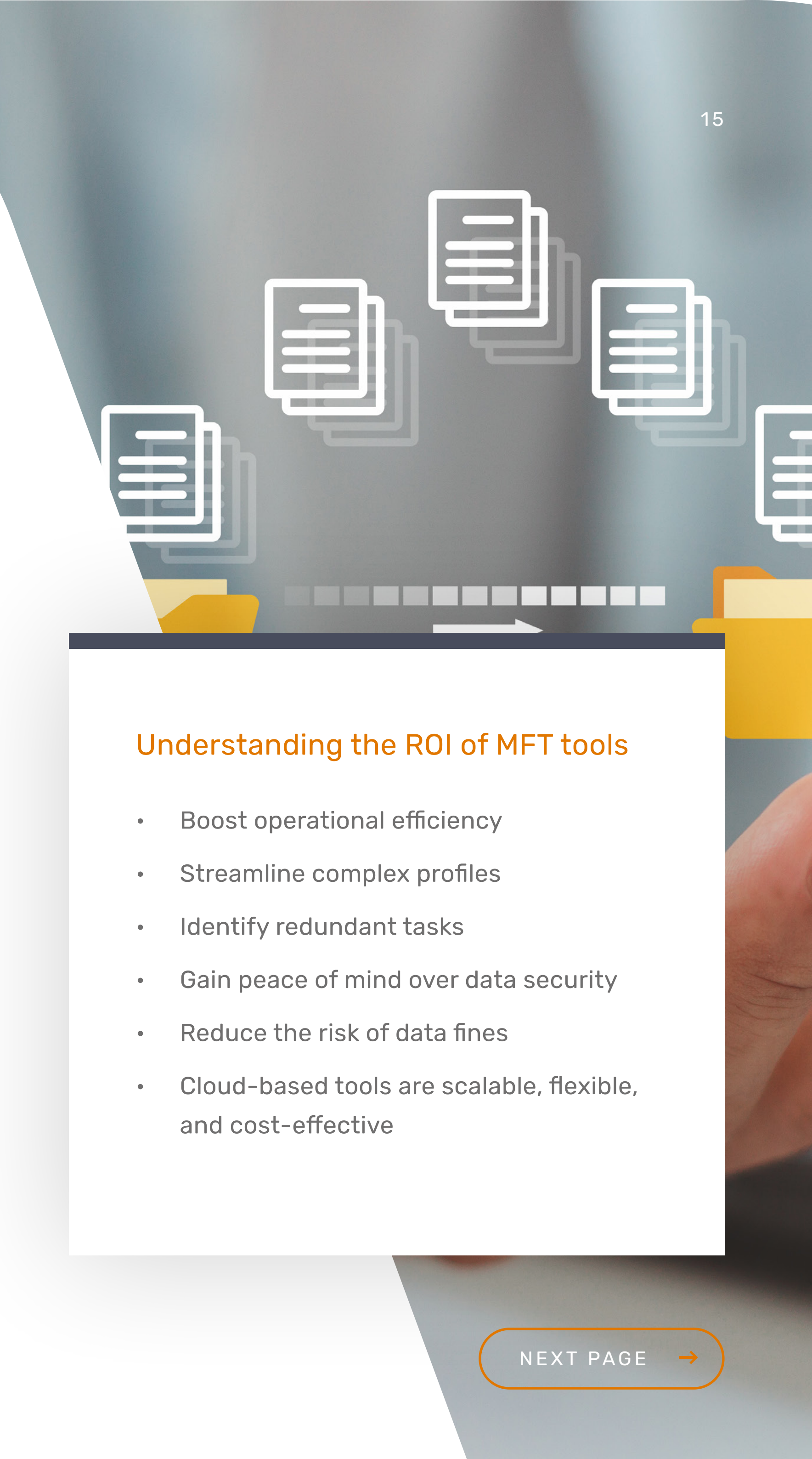
If you do find that your company holds legacy or redundant systems, investing in newer systems can help protect sensitive data and file transfer activity with updated security features. What's more, taking advantage of the cloud helps to ensure up to date technology – preventing the risk of costly incidents affecting your company's growth.

Can the business consolidate applications that perform the same function

A common side effect of mergers and acquisitions is that organisations often end up with redundant tools. Several internal departments within the same company may choose to introduce a wide range of applications to accommodate their file sharing requirements, without communicating their use to other departments.

However, while these applications can suit the needs of the user at the time, this approach can compromise overall visibility – possibly introducing vulnerabilities that threaten overall data security.

Instead, businesses should seek to consolidate multiple applications into a single standardised tool used throughout the company. This can provide the centralised, universal approach needed to reduce risks such as data breaches, while providing users with the visibility needed to always ensure compliant practices.



Understanding the ROI of MFT tools

- Boost operational efficiency
- Streamline complex profiles
- Identify redundant tasks
- Gain peace of mind over data security
- Reduce the risk of data fines
- Cloud-based tools are scalable, flexible, and cost-effective

← PREVIOUS PAGE

NEXT PAGE →

Transparent governance, compliance, and risk for CTOs, CIOs, and CISOs

Managing data can seem an endless challenge. This is where Managed File Transfer can help – combining compliant file sharing with centralised control.

The core benefits of MFT tools

Rapid deployment:

An effective MFT solution will possess a range of key features, from pre-built connectors to a robust API, that ensure a rapid go-live date with little operational delay or disruption.

Elevated cyber security maturity level:

Leverage MFT tools to rapidly elevate your organisation's Cyber Security Maturity Level, demonstrating a proactive approach to safeguarding sensitive data and mitigating risks.

Supporting file sharing and security policies:

Managed File Transfer serves as an ideal solution to enforce an organisation's file sharing and security policies, ensuring confidentiality and compliance.

Avoiding Shadow IT:

Standardising MFT tools can help mitigate the risks associated with Shadow IT, promoting a centralised and controlled environment for file exchange.

Streamlined operations:

MFT tools enable efficient collaboration and secure data exchange while maintaining a strong focus on data protection and regulatory compliance.

← PREVIOUS PAGE

NEXT PAGE →

Answering the most common questions about Maytech's MFT tools

Q: Have your information security controls been assessed by an external auditor or certification body?

Yes. Maytech are ISO 27001 certified since 2013 and are audited twice a year by Lloyd's Register Quality Assurance – one of the leading business assurance providers in the world.

Q: Are your information security controls regularly assessed by an internal audit team?

Yes, we conduct thorough internal audits which cover core aspects of the ISMS throughout the year. Results available on request.

Q: How do you monitor the security of your infrastructure?

Firewalls, weekly external vulnerability scanning (McAfee) daily internal vulnerability scanning (Vuls) and Annual Penetration Testing.

→ Check out our security and compliance FAQs to learn more

> “One of the most significant advantages of deploying MFT is its ability to reduce a lot of the risks that come with sharing or accessing sensitive data. We put access control, secure encryption, and full data residency in the hands of our users – helping make sure that any sensitive data remains managed and compliant at all times.”

Mike Futerko, Chief Technical Officer at Maytech

← PREVIOUS PAGE

NEXT PAGE →

Making data security easier for CMOs

Handling videos, images, content, confidential press releases, and stakeholder information, CMOs balance compliance and security protocols for several sensitive data types.

Managed File Transfer offers an alternative to the common hazardous approach of using Shadow IT software (software not internally approved for use). Instead, all departments can make use of a consistent framework for internal file sharing. This allows marketing teams to protect sensitive assets without interrupting workflow, and enabling sales, HR, and other departments to do the same.

An MFT approach forges a strong relationship between departments such as marketing and security teams. MFT tools ensure that security requirements are met and evidenced – offering full transparency while allowing for the easy file sharing needed to accelerate marketing strategies.

The result? Uninterrupted, secure workflows that keep all teams satisfied. Everyone can access the content they need or even connect to additional sources, without any worry about data security.

← PREVIOUS PAGE

NEXT PAGE →

Our MFT tools in action: securing data transfer for fintech provider Intelliflo

“One of our key responsibilities is to migrate data securely into Intelligent Office from the systems a financial advisory firm had before acquiring our software.

Previously, we were zipping up files and sending them using a solution similar to Dropbox or any other FTP protocol, but there wasn’t the level of encryption we were looking for as a minimum. Our obligations under the DPA and GDPR led us to look for something more robust and secure, that’s where Maytech and Quatrix came into the picture.

It’s been working fantastically. One of the key selling points from a GDPR standpoint is the ability to send a secure link to one individual. If that individual then decides to share that link with somebody else it becomes null and void, or if the email then gets intercepted it lessens the ability for someone to perform malicious activity and obtain the data.”

See secure external file sharing in action

Closing thoughts

At Maytech, our mission is to make file sharing simple and secure.

We believe in the capabilities of Quatrix to enhance the role and responsibility of the full C-Suite. With Quatrix, users have a platform trusted by international enterprises and governments. Regularly tested, evaluated, and updated, its capabilities come complete with 24/7 customer support. As a result, we can give our clients the tools needed to maintain compliance with local and international data regulations – and reduce common data risks.

With multiple certifications, our MFT solutions demonstrate our commitment to creating compliant and secure tools that can embed themselves enterprise-wide, bringing stark benefits and greater value to almost any level.

Our Credentials

Government Procurement Service *Supplier*

HIPAA COMPLIANT

GDPR Complaint

CERTIFIED LR ISO/IEC 27001

PCI DSS COMPLIANT

SKYHIGH ENTERPRISE-READY

CYBER ESSENTIALS CERTIFIED PLUS

To learn more, why not book a complimentary discovery call and a free 14-day trial? Here, we can discuss the unique requirements of your industry, and explore how our SaaS tools can provide an all-in-one intelligent solution.

→ Book a discovery call today

← PREVIOUS PAGE

NEXT PAGE →

maytech
GLOBAL DATA TRANSFER

Email support

Support: support@maytech.net

Sales: sales@maytech.net

Billing: billing@maytech.net

Telephone support

International: +44 189 286 1222

US and Canada: 1 800 592 1906

UK: 01892 861 222

Correspondence address

Maytech Communications Ltd
40 Gracechurch Street
London, EC3V 0BT
United Kingdom

Registered address

Maytech Communications Ltd
4 Mount Ephraim Rd
Tunbridge Wells, TN1 1EE
United Kingdom