maytech
GLOBAL DATA TRANSFER

www.maytech.net

7 Key Principles to **Control** and **Secure** your External **File Sharing**

V 1.0 March 2020

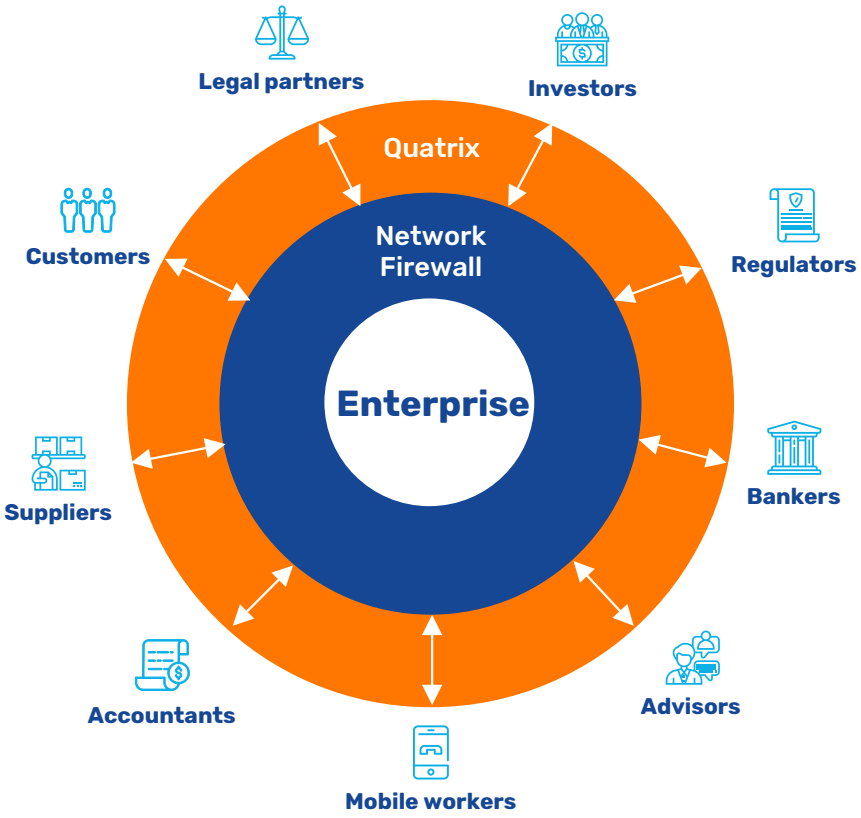
Introduction

John Lynch
CEO, Maytech

I'd like to personally thank you for your interest in our whitepaper.

Maytech has provided secure file sharing to organisations across 60 industries and 35 countries through our enterprise-grade SaaS solutions since 2006.

This document summarises the key principles of keeping your most sensitive data safe and under your own control, when sharing with third parties.



Our Solution

Quatrix® has been developed for enterprise-grade performance and security, providing compliance and safeguarding controls for sensitive or critical data while in transit and at rest.

It has a user-friendly HTTPS portal, SFTP connectivity and a secure API, all of which are delivered over our uncongested global network, to ensure that files are delivered securely, reliably and fast while avoiding opening up the corporate network.

Quatrix

1 Exploit the advantages of the cloud

A cloud solution provides many benefits, which is why so many organisations are migrating services to the cloud. For file sharing, the main benefits are:

- Delivering services more efficiently, allowing IT resources to be freed up and to be deployed on higher priority tasks.
- Accessing data over the internet, removing the requirement of using a VPN connection or installing software prior to exchanging files. This is especially important when working with third parties who might not have access to the same systems as your own organisation.
- For larger data sets, preventing internal network congestion by sending and receiving files over an uncongested global network.
- Avoiding the requirement to open the corporate firewall.

2 Cater for common user requirements

External file sharing takes many different forms. Consider which use cases you require and whether they are covered in a solution without the need to source, procure and manage additional suppliers:

Person to person sharing:

- **HTTPS / Web Access:** for accessing files directly in a web browser, providing mobile access and removing the requirement to install software. This is key to working with external partners with disparate systems who can readily access your specified platform.
- **Email integration:** for sending attachments of any size securely.
- **Automated rules:** so that files can be distributed quickly and efficiently, with appropriate notifications and automated processing events so users and systems receive the data they require, when they require it.
- **Collaboration features:** for users inside and outside of the network to allow them to access and work on files remotely.
- **Data acquisition:** via secure online forms to control ad hoc incoming files.

Machine to machine sharing:

- **SFTP connectivity:** a common requirement - often used to quickly and easily share data or as part of an automated workflow.
- **API:** for machine-to-machine systems integration and custom automations.

3 Adhere to legal and regulatory compliance

Compliance with data protection and security requirements is a non-negotiable part of running a modern organisation. Failure to adhere to security, privacy and regulatory obligations can be seriously damaging, due to loss of income from negative PR and serious financial penalties.

While compliance is your responsibility, suppliers should be accountable to you and be able to prove that they conduct their operations in line with your compliance requirements.

Here are some of the key facts around compliance for external file sharing:

- ISO 27001 certification is a highly regarded international standard that proves an organisation has robust information security management practices. Certification requires regular auditing, so request a copy of the certificate and check it is issued by a reputable auditor.
- Choose a platform that complies with your obligations under global privacy laws including the General Data Protection Regulation (GDPR) in the EU and California Consumer Privacy Act (CCPA) for US operations. Under the GDPR, the EU requires you to have a Data Processing Agreement (DPA) in place between you and your supplier if sharing Personally Identifiable Information (PII). If you will be handling PII, ask your supplier whether they can provide you with a DPA they are willing to sign.
- Depending on your industry, your suppliers should also be compliant with standards such as HIPAA for US medical records, PCI-DSS for credit card processing and any other industry-specific requirements you have. Check with your supplier which standards they are compliant with, and find out whether they will support you in the process of proving compliance.
- Ask where your data will physically be stored. You should opt for data residency in the country or region your business operates in so that it is within the same jurisdiction.

4 Demand enterprise level security

Enterprise security is a combination of policies, processes and proactive management. Key things to consider when choosing a solution are:

- **Security-First:** choose a security-focused, enterprise-specific solution, as opposed to a consumer-grade solution that also targets the enterprise market.
- **Strong Encryption:** use strong encryption to prevent files from being accessed in transit and at rest, including monitoring and deprecation of insecure cyphers.
- **2FA:** specify two-factor authentication to lock down access and prevent unauthorised use of login credentials.
- **IP Restricted Access:** prevent unauthorised access by providing access to specific IP addresses.

5 Prevent the use of shadow IT

Unfortunately, users at all levels of seniority don't always follow corporate policies. They find the easiest way to achieve their objective, which is often as simple as sharing some files with another person as part of an everyday workflow. Preventing users from doing this requires some consideration.

- Introduce a solution that meets their needs, with rapid adoption, fast deployment and superior service levels to prevent users from bypassing it or seeking alternatives.
- Provide training documentation to quickly provide an overview of the platform.
- Block consumer grade platforms using your corporate firewall.

6 Require centralised administration

Centralised administration will allow you to quickly and easily manage your service settings. Key aspects to consider are:

- Easy-to-use service settings and granular user access controls that provide a simple and fast way to self-manage your external services.
- Modern, passwordless authentication using Single sign-on (SSO), managed within existing infrastructure.
- Ability to jail users to specific folders and secure spaces, with the ability to apply this to teams and projects for collaboration with third parties.
- Access to a comprehensive audit trail for compliance purposes and to ensure you know where your data is and who has access to it at all times.
- Applying site-wide or folder-specific rules for automatic deletion to prevent sensitive data from persisting in external cloud locations.

7 Know your Supplier

Working with a trusted partner will ensure smooth operation of your service and fast responses to issues. Key aspects to consider are:

- **Trust:** when working with a cloud solution, you want to know exactly who you are dealing with when commissioning services to handle your organisation's most sensitive data. Some organisations run pen testing and background checks as part of their procurement process before they will engage with a supplier.

- **Support:** an extension of your team, your supplier will be operating a critical business function. Support staff should be responsive, knowledgeable and experienced, so that as and when you do require assistance, you are provided with an efficient and professional service.
- **Flexibility:** a consumer-grade platform is highly unlikely to be appropriate for your organisation. The same solution is offered to every customer and there is no incentive to service bespoke development. A specialist solution provides more flexibility and an opportunity to influence the product roadmap.

Talk to one of our team of specialists for more information on how Maytech can support your organisation with the management of secure external data transfer. Get in touch through our website at www.maytech.net, where you can also access a free 14-day trial of Quatrix, our easy-to-use file-sharing platform.

Some of the customers Maytech provides solutions for