6 Ways FTP/SFTP is Putting Your Business at Risk

Introduction

FTP-based solutions were never designed to handle the exploding need for fast, secure and scalable exchange of digital information.

File Transfer Protocol (FTP) and Secure FTP (SFTP) are among the most widely used methods for file sharing.

Part of the appeal is that they are simple to use and often free or very inexpensive. Typically, organizations get started with FTP because they have an occasional need to send non-sensitive files. The technology works well in these situations, but when used more broadly it can put your business at risk.

Studies show that 88% of organizations have difficulty moving big data quickly and efficiently[1] and the average cost per lost or stolen record is $148.[2] FTP-based solutions were never designed to handle the exploding need for fast, secure and scalable exchange of digital information.

Organizations can't afford to rely on FTP as their "go to" method for demanding workloads. To help you understand its limitations and hidden costs, let's explore six ways FTP can prevent you from reliably connecting with all the people, systems and data that matter to your business.

01
Security weaknesses

Even SFTP lacks security controls to handle today's cyber threats.

Regulatory standards are tightening as large-scale breaches continue to make headline news.

Even minor lapses in security can damage your reputation, send your stock value plummeting and result in massive costs.

Critical data needs to remain secure and under your control, but FTP was not designed with secure file transfer in mind and SFTP lacks security controls to handle today's cyber threats. For example:

- User IDs and passwords to login to FTP servers and send files aren't always protected.
- Encryption is an afterthought requiring extra steps and IT expertise, making it difficult, expensive and time-consuming to send files safely.
- FTP clients are common and free, giving every hacker the tools necessary to attempt to breach your critical systems.
- These security weaknesses and other vulnerabilities make it easy to intercept FTP-based file transfers.

Recent research reveals that more than 400 million files from FTP servers are publicly available online.[3] When files are exposed, FTP doesn't log security violations or authenticate users – basic capabilities you need to help detect and stop breaches.

02
Lack of control

FTP sends files on a first-come, first-served basis.

Seconds count when you're transmitting an order for an annuities trade, payroll information to your processing system or benefits data to meet an enrollment window.

If you can't manage network resources and processing windows based on business priorities, data gets stale and loses value and Service Level Agreements (SLAs) are missed, which can result in fines.

As a solution designed primarily for ad-hoc transmissions, FTP sends files on a first-come, first-served basis. You can't:

- Create enforceable policies to schedule critical transfers above lower-priority work.
- Reserve transmission channels for sensitive transfers based on business requirements.
- Interrupt and re-prioritize transfers on the fly to take advantage of last-minute opportunities or deal with emergencies.

Without these management capabilities you can't prioritize critical transfers, balance processing windows or respond to immediate business needs.

03 Blind Spots

You can't fix what you can't see, and with FTP you only discover failures when you feel the pain.

You don't want to learn about a transmission problem from a partner or customer.

When a file is delayed or isn't transferred at all, you need to be notified in real time so you can proactively correct problems before they impact downstream business activities.

However, FTP can't:

- Instantly notify you when a delay or failure happens.
- Route notifications to team members who can quickly fix the issue.
- Present log file activity across your entire environment so you can proactively address the issue.

You can't fix what you can't see, and with FTP you only discover failures when you feel the pain. Your file transfer system should provide you with full visibility to remove blind spots and address issues across your network before they become a problem.

04 Manual recovery from failures

With FTP, you are often in fire-fighting mode.

FTP was meant for ad-hoc transfers, not data exchanges that the business relies on to generate revenue and remain competitive.

When the size and volume of FTP file transfers grow, so does the probability of failure.

With FTP, you are often in fire-fighting mode because:

- FTP can't recover a failed connection automatically, so you must restart the process manually.
- FTP doesn't include checkpoint restart, requiring you to resend entire files regardless of how much was previously sent.
- You have to discover the failure on your own, which further delays resending the affected files.
- Errors require several calls and emails with multiple parties to correct.

Network outages and errors happen. You need a file transfer technology that helps you automatically handle disruptions reliably and quickly.

05 Unproductive use of resources

IT teams spend hours or days custom coding FTP to deal with challenges.

Clearly, FTP comes up short in meeting the needs of modern business and IT requirements.

Custom scripting, scheduling and integration can help bridge the requirements gap, but it also creates new points of failure, maintenance headaches and wastes valuable resources. Rather than working on more strategic activities, IT teams spend hours or days custom coding FTP to deal with challenges like:

- File transfers that are sent without regard to business priorities.
- Partner onboarding that is complex, labor-intensive and often takes weeks to complete.
- Manual, error-prone processes that increase risk to the business.
- Growing file transfer volumes that FTP isn't intrinsically equipped to handle.

With FTP, file transfer quickly becomes a burden, when it should work seamlessly behind the scenes to power your business.

06
Cost of poor performance

Over time, most organizations realize they can no longer afford their “free” FTP service.

Failure to meet transmission or file transfer SLAs can cost your organization millions of dollars in fees and penalties.

You can even lose business if you develop a reputation for being unreliable. Situations that result in a data breach and non-compliance with security regulations can be even more onerous and costly to address.

FTP solutions don’t provide core capabilities organizations need to monitor performance, such as:

- Transfer confirmations
- Failure notifications
- SLA management tools
- Security alerts
- Detailed and consolidated activity logs

Over time, most organizations realize they can no longer afford their “free” FTP service.

Conclusion

IBM® Secure File Transfer provides simple, secure and scalable file-based transactions, without the hidden costs of FTP/SFTP.

Organizations increasingly rely on digital file transfer solutions to securely exchange growing volumes of sensitive data between people and systems. In fact, more than 50% of all systems integration is still done through file transfer,[1] which is why having a secure, scalable solution that's designed to support your business needs and goals is essential.

IBM's Managed File Transfer solutions provide a battle-tested platform that has the greatest share of the managed file transfer market according to multiple, leading analyst firms. Our IBM® Secure File Transfer offering gives you everything you need to get started quickly and deploy the platform. It provides simple, secure and scalable file-based transactions, without the hidden costs of FTP/SFTP.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
April 2019

Sources:

1. Vanson Bourne, IBM Supply Chain Data Report, Nov 2017
2. Ponemon Institute's 2018 Cost of a Data Breach Study, https://www.ibm.com/account/reg/us-en/signup?formid=urx-33316
3. https://resources.digitalshadows.com/whitepapers-and-reports/too-much-information-misconfigured-ftp-smb-rsync-and-s3-buckets-exposing-1-5-billion-files