



Four keys to effectively monitor and control secure file transfer



Watson Supply Chain

Four keys to effectively monitor and control secure file transfer

Executive summary

As more information is digitized and more business data is considered critical, you're spending more time than ever managing that information – and its movement within your enterprise, with your partners and with customers.

Can your file transfer infrastructure handle the implications of regulations such as GDPR? Is your network and the data that travels across it secure enough? Can your file transfer operations process the rapidly increasing volumes of digital data across disparate systems, platforms and protocols? How effectively does your file transfer infrastructure enable you to meet and proactively manage service level agreements (SLAs)?

Leading businesses have discovered that ensuring compliance, enabling successful, secure data transfers and managing high volumes of data to meet SLAs all have one thing in common: data must be visible across the organization. After all, you have to know where the data is, and how it got there, to effectively manage it.

When you apply this key learning and the three others described in this paper to effectively manage and monitor the flow of business data, you can dramatically improve the security, auditability, service delivery and scalability of your file transfer operations to deliver on the promise of exceptional customer experiences.

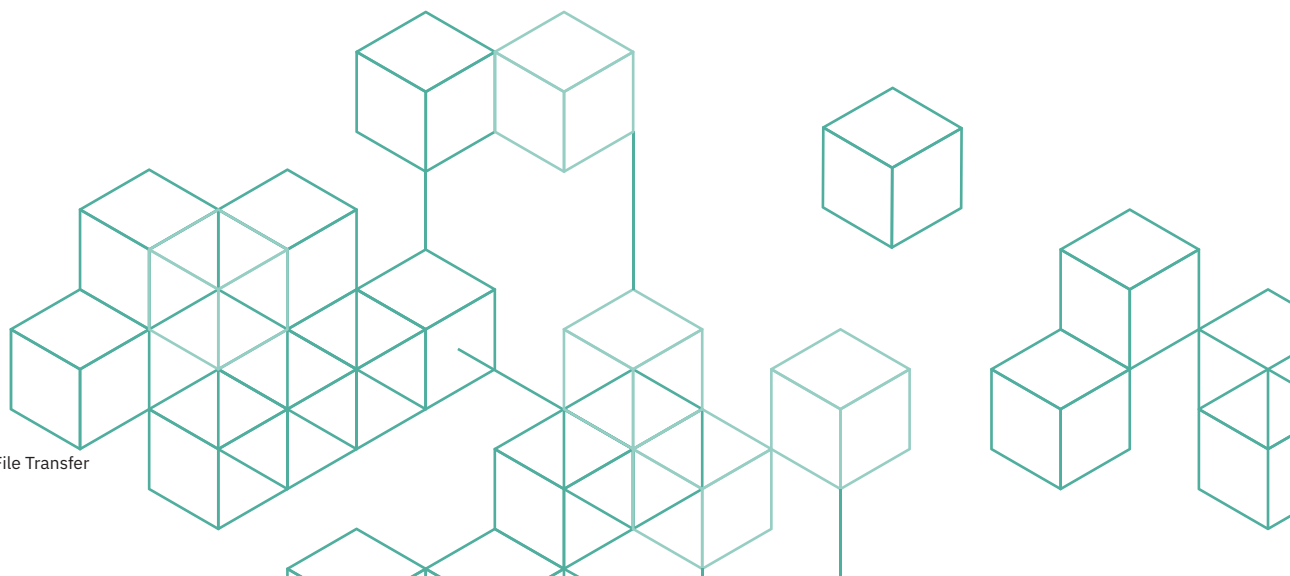
Key #1 – Make your data visible wherever it is in the network

The right file transfer system combines speed, security and reliability with end-to-end data visibility

In today's business environment, how we deliver is as important as what we deliver. Increasing regulations, like GDPR and HIPAA, require auditing and visibility of file transfers – and the cost of non-compliance is high. In addition, ever-stringent SLAs can have a dramatic impact on both business performance and the customer experience.

To deliver on changing customer and market demands, you need visibility into your data from the beginning of a file transfer to the very end. After all, you can't manage what you can't see. A secure file transfer system that moves data quickly and reliably from one application or server to another allows you to comply with increasingly stringent information-security requirements and proactively manage service.

You also need to effectively monitor file transfers and B2B processes. Look for solutions that align server views with operational logic and identify schedules, processes, file names, user roles and security capabilities.



Key #2 – Reduce or eliminate ad hoc use of FTP

Data security should protect the network and the data traveling on it, while simplifying manageability

Many companies move data via File Transfer Protocol (FTP). For those companies, FTP may even be the standard file transfer solution. But using FTP puts data and the network it travels across at risk.

For example, with FTP, client IDs and passwords are transmitted in clear text. Worse, standard FTP commands can be used to create denial-of-service attacks or exploit other network vulnerabilities.

Security risks aside, FTP is difficult to manage because it provides no way for you to see where your critical data is, let alone control its movement or generate an audit trail. Sometimes, in fact, data sent via FTP never reaches its destination, and the sender only knows if the intended recipient manually notifies the sender.

To improve the security of your data and network – and simplify management – it's important to reduce or even eliminate ad hoc use of FTP. Replacing FTP with a standardized platform for secure file transfer enables you to set and enforce security policies throughout your company and with others outside your organization.

Key #3 – Build scalability into your file transfer system

As your company's data volume grows, so should your network's ability to transfer data

The volume of data that companies transfer is growing exponentially. That's because more types of information are being digitized and more companies are expanding trading partner networks. Can your file transfer infrastructure accommodate the growing volume of data?

Banks in the United States are now digitizing checks so that they can be processed faster and more efficiently. If your company is involved in an acquisition or merger, or if your trading partner network is expanding as part of the company's growth strategy, your data volume is growing exponentially too. Trade secrets, such as data-filled documents with product specifications or manufacturing design, move frequently across global supply chains and must also be secured.

A secure file transfer system that easily scales to the size of your needs and accommodates multiple platforms and protocols helps ensure your ability to handle increasing volumes of data.

FTP is difficult to manage because it provides no way for you to see where your critical data is, let alone control its movement or generate an audit trail.

Key #4 – Monitor data transfers from beginning to end

Meet customer demands and SLAs

Time is money. And nothing underscores that more dramatically than the need to quickly process customers' data. Because you have SLAs to meet, you must carefully monitor data transfers from beginning to end – for events and non-events. Can you rely on your file transfer infrastructure to help you manage to service commitments?

A secure file transfer solution enables you to see the data movement in your network. With real-time visibility, you gain more focused insight for resource planning, because the system pinpoints process bottlenecks. It highlights unreliable or inefficient file transfer solutions that need upgrading or replacing. It enables you to customize alerts based on SLAs and to define rules for exception handling. And perhaps most importantly, it enables you to proactively resolve issues before they become failures – ensuring that you meet service commitments.

Next step – Evaluate your file transfer operations

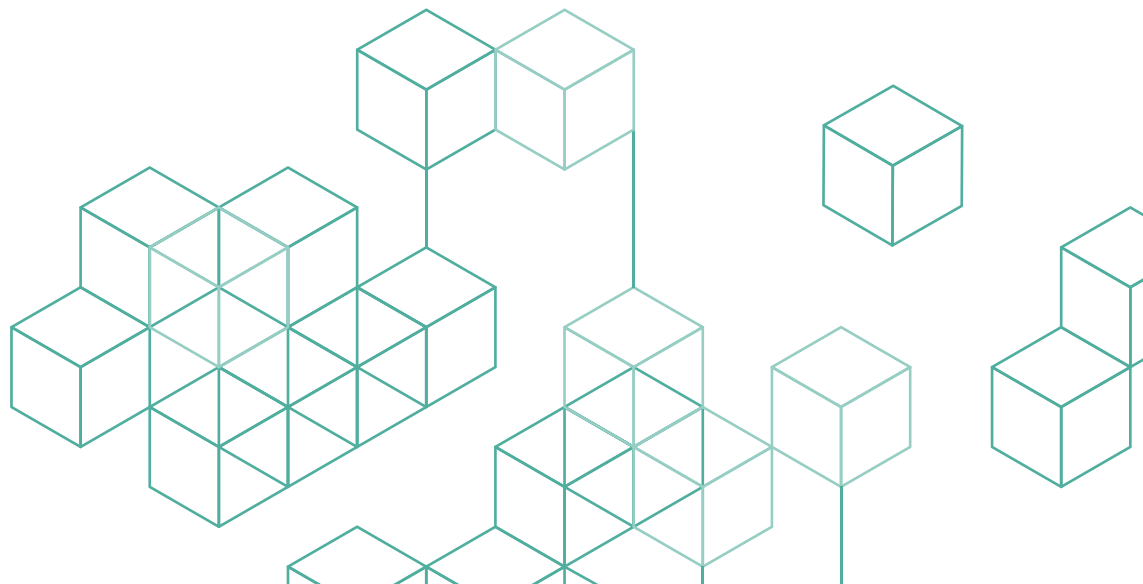
Is *your* file transfer infrastructure equipped to meet today's business demands? The answer lies in its ability to let you see data everywhere in the network. Because your organization's business processes reach across a vast network within and beyond your four walls, data sharing plays an integral role in your company's success. Existing enterprise applications, like enterprise resource planning and departmental FTP servers, enable these processes.

It's important to evaluate the impact – and the cost – that unmanaged file transfers place on your business. Begin by answering these questions:

Do you have business processes based on rapidly recurring file transfers at predictable or unpredictable intervals?

Do you have business processes that depend on the transfer of especially large files that often exceed a gigabyte in size?

The only way your file transfer infrastructure can meet your evolving business demands is if it lets you see data everywhere in the network.



Do you have business processes that rely on the transfer of data among hundreds or thousands of partners or customers?

Do you have multiple lines of business using different, disparate applications?

Can those applications effectively exchange data to enable seamless business processes?

Do you face corporate or regulatory mandates that require you to track and monitor data transfers?

Can you generate the reports those mandates require?

Do you want to make IT more strategic to the organization?

Do you wonder whether your enterprise data transfers are secure and working correctly?

Answering “yes” to any of these questions underscores the need to act quickly to improve your file transfer operations to better prove compliance with government regulations, secure your data and network, manage the increasing volumes of data, and meet service level agreements.

Your answers to the following two questions may very well define how fast you must act:

How much revenue does your company lose if it takes weeks or months to extend strategic multi-enterprise business processes to new partners or customers?

How long do you want other departments within your company to continue establishing and using rogue systems to enable file transfer?

Help ensure security-rich, reliable data movement with solutions from IBM.

Secure file transfer solutions from IBM establish enterprise-wide control over your data transfer processes. They provide the visibility and tools you need to help ensure that data is safeguarded, its delivery is reliable and auditable, and the file transfer infrastructure can accommodate growing data volumes.

For example, deploying IBM® Connect:Direct® supports your efforts to comply with government regulations and safeguard the data that moves across your network. And IBM® Control Center gives you the visibility you need to better manage data and proactively manage to service level agreements.

IBM knows file transfer. Our solutions span from managed file transfer all the way to B2B collaboration. We can help you establish better enterprise-wide control over your data transfer processes. Our products provide the visibility and tools you need to help ensure that data is safeguarded, its delivery is reliable and auditable, and your file transfer infrastructure can scale to meet your company’s needs today – and provide a solid foundation to meet the demands of tomorrow.

You need to act quickly to improve your file transfer operations to better prove compliance with government regulations, secure the data and the network, manage the increasing volumes of data and meet service level agreements.



© Copyright IBM Corporation 2018

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America

November 2018

All Rights Reserved

IBM, the IBM logo, ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice.

IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at

IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.

Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results.

ZZW03064-USEN-00

