

Four keys to effectively monitor and control secure file transfer

Explore the four keys you can apply to improve the security, auditability, service delivery and scalability of your file transfer operations to deliver on the promise of exceptional customer experiences.

Highlights

- File transfer landscape
- Make your data visible wherever it is in the network
- Reduce or eliminate ad hoc use of FTP
- Build scalability into your file transfer system
- Monitor data transfers from beginning to end
- Evaluate your file transfer operations



File transfer landscape

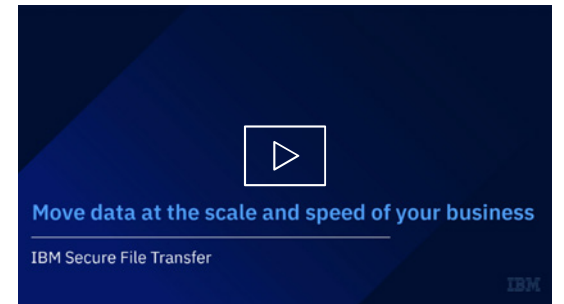
As more critical business information is digitized, you're spending more time than ever managing that information and its movement within your enterprise and with your partners and customers.

Can your file transfer infrastructure handle the implications of different data privacy regulations? Is your network and the data that travels across it secure enough? Can your file transfer operations process the rapidly increasing volume 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.



Watch: Learn how you can drive out complexity and enable simple, secure and scalable file-based transactions

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 BCBS 239 and HIPAA, require auditing and visibility of file transfers – and the cost of non-compliance is high. In addition, ever-demanding SLAs can have a dramatic impact on both business performance and 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 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.

Learn 6 ways FTP is putting your business at risk and how you can overcome them

[Explore the ways](#)

Key #3: Build scalability into your file transfer system

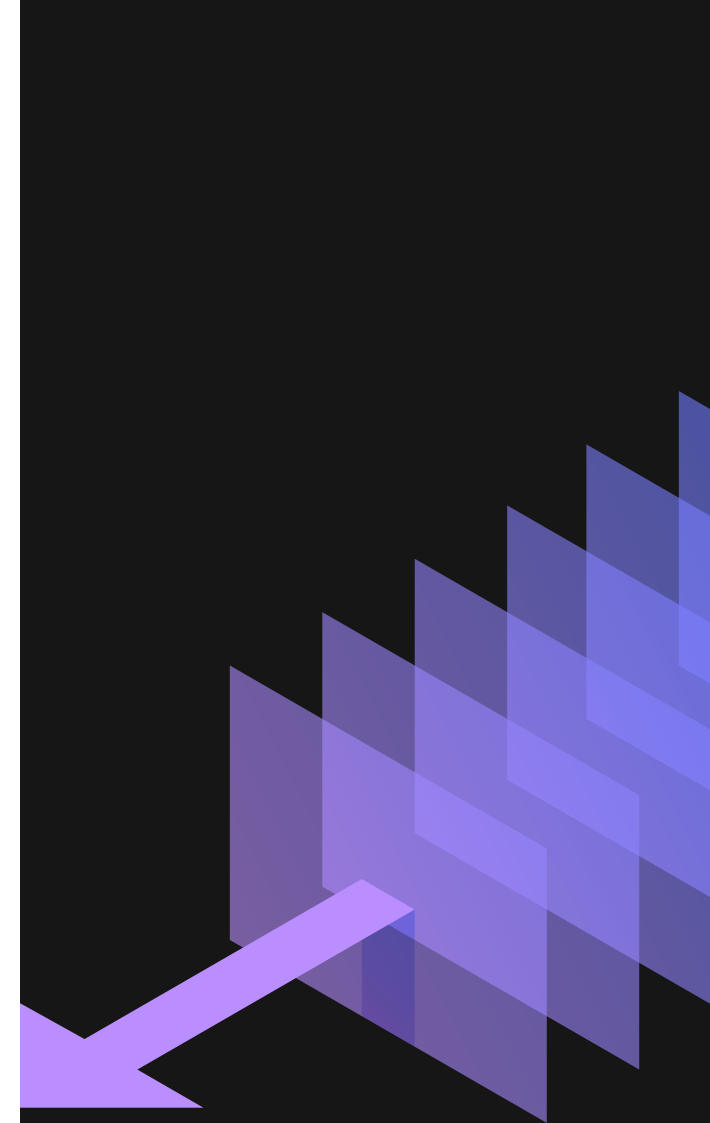
As your company's data volume grows, so should your network's ability to transfer data

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.



Key #4: Monitor data transfers from beginning to end

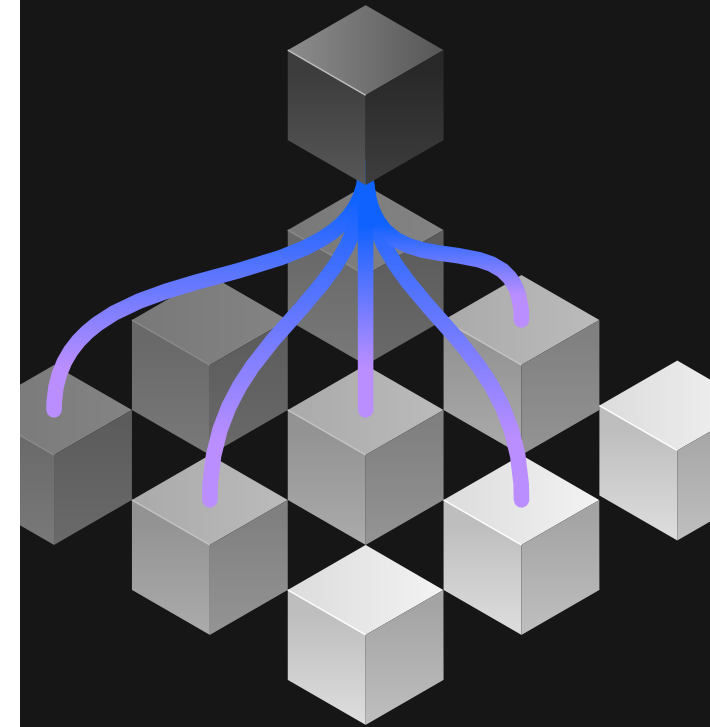
Meet customer demands and SLAs

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.

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



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:

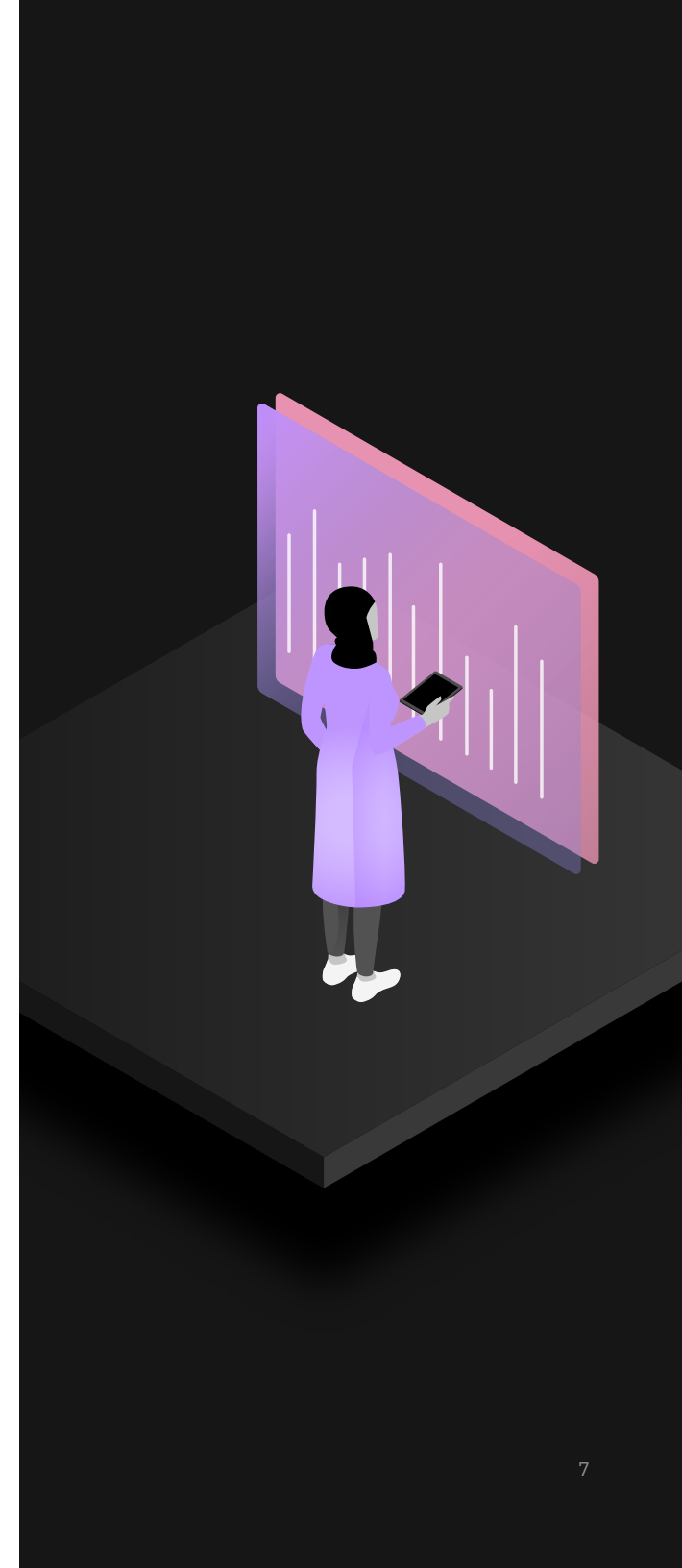
- Do you have business processes based on rapidly recurring file transfers at predictable or unpredictable intervals?
- Do you have business processes that depend on the transfer of especially large files that often exceed a gigabyte in size?
- Do you have business processes that rely on the transfer 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?



Next step: Evaluate your file transfer operations

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.

For example, deploying [IBM Sterling Connect:Direct](#) supports your efforts to comply with government regulations and safeguard the data that moves across your network. [IBM Sterling Control Center](#) gives you the visibility you need to better manage data and proactively manage to service level agreements. And [IBM Sterling Control Center Director](#) makes it faster and easier for you to centrally update and

configure IBM Sterling Connect:Direct nodes — and scale your managed file transfer environment easily.

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.

IBM Sterling Secure File Transfer

Securely move data at the scale and speed of your business.

[Learn how](#)

Next steps



Solve the secure file transfer puzzle

Overcome the challenges of file transfer security and visibility by modernizing your approach to data exchange.

[Read the blog](#)



IBM Sterling Secure File Transfer

IBM Sterling Secure File Transfer provides a unified file transfer platform so you can securely share and track mission-critical information movement within your enterprise and across your partner network.

[Read solution brief](#)



Speak with an expert

Learn how IBM can help you achieve simple, secure and scalable file-based transfers.

[Request a consultation](#)



© Copyright IBM Corporation 2020

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
January 2021

IBM, the IBM logo, ibm.com, and TRIRIGA are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at <http://www.ibm.com/legal/us/en/copytrade.shtml>

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The information in this document is provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.