

Secure Data Streaming with Attachmate FileXpress

Why it's better than the store-and-forward approach

The need to secure business data in motion is a given. But what happens at the end of the line—in that uncertain space of time when the data just sits, waiting to be picked up?

Most Internet-based file transfer solutions employ a central repository, situated in the middle of the DMZ, where incoming and outgoing files are stored. Files often linger unprotected in these repositories—for hours or days—before being retrieved by business partners or customers. Without constant backup and the proper safety measures, these repositories introduce untold security risks.

Secure data streaming removes these risks by delivering data directly to backend servers, without stopping at any repository. This paper examines the issues presented by traditional store-and-forward approaches and explains how secure data streaming with Attachmate® FileXpress® software can overcome them.

The Store-and-Forward Approach: Issues to Consider

Most legacy file transfer solutions (including FTP) deploy store-and-forward—or repository-based—approaches. If you have deployed, or are considering, a store-and-forward solution, you will want to answer the following questions:

1. How will you ensure that the repository won't be compromised by internal or external parties, including administrators?
2. For large files, what is the increased overhead of having to read and write the file two times—first to the repository and again at the final destination?
3. How is data moved between the repository and the backend system? What protocol is used? Does the backend system have to initiate all the movement or can the repository send the data directly to the backend system? If data has to be pulled out of the repository by the backend system, how often must it poll the system for files to pull? Will you require a third-party scheduler to perform these pulls?
4. What backup procedures will you need for the repository?
5. What happens if the repository goes offline—either for unplanned reasons or for system maintenance? Are there automated ways to roll over to a mirrored system or will all transferring need to be suspended?

6. How will you manage the files in your repository (since they cannot be stored indefinitely)? Can you automatically remove them, based on some configuration, or are there steps you must perform regularly to maintain the repository?
7. How much space is needed for the repository today? How will you add space in the future? Is there a process? A cost factor?
8. Two separate events move data to the ultimate location: (1) the writing of the file to the repository, and (2) the moving of the file to its ultimate destination (either the remote system for outgoing files or the backend server for incoming files). How is logging handled for these events? Is it easy to map both ends of the transaction to have a full view of the transaction?
9. How will you handle version control and data integrity? If you have already posted files to the repository, can you easily make updates or do you need to post a second set of files for download? Can you ensure that the users will be able to sort out the most recent versions?

Ultimately, guarding against risk and inefficiency with a store-and-forward solution is a costly, labor-intensive proposition. The good news is that there is an effective alternative. It's called secure data streaming.

The Secure Data Streaming Alternative

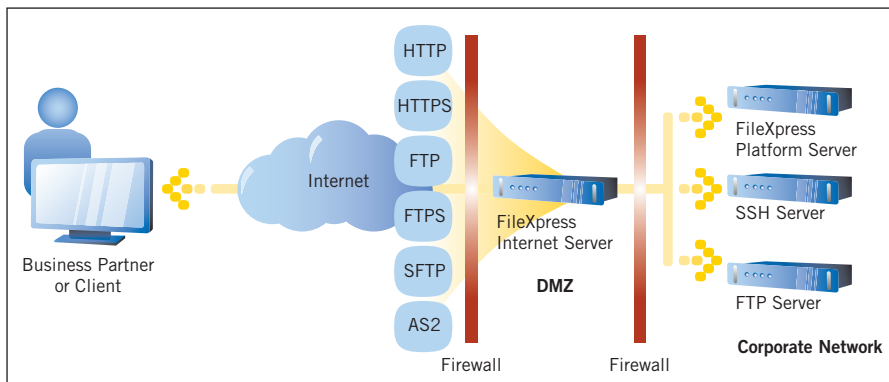
Secure data streaming eliminates the need to store data in a central repository. Instead, outbound data resides on the backend system (where it was created) until your business partner or customer retrieves it. Inbound data is delivered directly to the backend system, where it is processed according to business rules.

Attachmate FileXpress software, a family of managed file transfer solutions, is built to securely transfer files of any size, across all major platforms, to any location. The FileXpress Internet Server, which resides in the DMZ, securely brokers connections from clients, using a

wide range of protocols, and then makes new, separate connections to the internal backend server(s). Those backend servers could be hosting SFTP, FTPS, or FTP services, or they could be running the FileXpress Platform Server (another member of the FileXpress family).

With its secure data streaming capabilities, FileXpress provides the following benefits:

- **Stronger security**
If a hacker breaks into your repository, he can probably gain access to all the data being transferred. FileXpress Internet Server eliminates this serious point of exposure. It provides a secure proxy that prevents any direct outside connection to the backend systems and isolates any inside configuration or network topology.
- **Streamlined process**
Because FileXpress Internet Server does not employ a central repository, you do not need to follow the two-step process of writing a file to the repository and then moving it into the corporate environment.



The FileXpress Internet Server securely brokers connections from clients and then makes new, separate connections to the internal backend server(s).

- **Automated post-processing support**
In addition to residing in the DMZ, FileXpress is able to reside on the backend system where it can process data based on business rules defined by the administrator (such as the user sending the data or the type of data). For example, a post-processing action might be configured to run the procedure for parsing an uploaded file and updating a database with the information stored within it.
- **Easy storage management**
With FileXpress, organizations can leverage the backup and recovery functions that have already been implemented on their backend systems. There's no need to deploy new backup or recovery systems, such as those required for solutions that use centralized repositories.

In short, FileXpress enhances security and lowers costs by eliminating the need to store sensitive information in the DMZ and improving the efficiency of file transfer workflow.

Extra-Strength Security for File Transfers

With secure data streaming, FileXpress keeps transfers safe from start to finish. Its multi-tiered architecture strengthens security further with these capabilities:

- **Reverse proxy with in-stream protocol switching**
FileXpress includes a reverse proxy that acts as a secure broker between file servers and the external clients who attempt to access them. The proxy uses a new connection, with a completely different protocol from the original connection, to terminate connections in the DMZ and establish new connections to the backend server. In this way, it effectively isolates the outside world from the corporate network.

- **Strong authentication**
FileXpress adds a robust layer of access control information on top of your existing security framework. This layer of information grants users specific permissions for sending or receiving data. With LDAP and Microsoft Active Directory integration, FileXpress allows organizations to leverage their existing user registry systems.

- **System obfuscation**
FileXpress is built to enable system obfuscation, a security practice that hides backend system configuration details from users in order to prevent socially engineered attacks. FileXpress can even be

set up to share files and directories with a number of backend systems. In this scenario, FileXpress presents a single logical view to end users accessing the FileXpress Internet Server through a file transfer client, command line, or web browser.

With FileXpress, you can give partners and customers access to the files they need—confident that you are not exposing details about the internal systems that store them.

Better Performance. Lower Costs. Tighter Controls.

Secure data streaming offers compelling advantages over traditional store-and-forward approaches. The elimination of the central repository typically found in Internet file transfer solutions enables organizations to achieve significant performance improvements, lower the total cost of ownership, and enforce tighter controls over data processing—all while improving overall security.

The FileXpress Family

Attachmate FileXpress is a strategic enterprise solution that manages and executes the secure transfer of files inside and outside your organization. The FileXpress family includes these products:

- **FileXpress Platform Server** is the engine that powers your file transfer infrastructure. It securely delivers files of any size, across all major platforms, to any location.
- **FileXpress Internet Server** is the portal through which all Internet-traveling files flow. It lets you safely interact with partners and customers around the globe.
- **FileXpress Command Center** is your digital dashboard for all file transfer activity. Transfer-related events can be initiated, tracked, logged, audited, and supported from one central location.
- **FileXpress FileShot** is your go-to agent for user-to-user file transfers. Working seamlessly with Microsoft Outlook, it transfers files of any size, provides audit records, and eliminates mailbox congestion.

About Attachmate

Attachmate delivers advanced software for terminal emulation, legacy modernization, managed file transfer, and enterprise fraud management. With our technologies, more than 65,000 businesses worldwide are putting their IT assets to work in new and meaningful ways. www.attachmate.com



Corporate Headquarters
1500 Dexter Avenue North
Seattle, Washington 98109
TEL 206 217 7500
800 872 2829
FAX 206 217 7515

EMEA Headquarters
The Netherlands
TEL +31 172 50 55 55
FAX +31 172 50 55 51

Asia Pacific Headquarters
Australia
TEL +61 3 9825 2300
FAX +61 3 9825 2399

Latin America Headquarters
Mexico
TEL +52 55 9178 4970
FAX +52 55 5540 4886

WEB attachmate.com
E-MAIL info@attachmate.com

For regional office information, visit www.attachmate.com.