

# Data Streaming sicuro con Attachmate FileXpress

## Perché è migliore dell'approccio "store and forward"

La necessità di rendere sicuri i dati aziendali durante il trasferimento è ormai una realtà indiscussa, ma che cosa succede alla fine dell'operazione, in quel periodo temporale dai contorni incerti in cui i dati sono in attesa di essere recuperati?

La maggior parte delle soluzioni di trasferimento file basate su Internet utilizza un repository centrale, collocato sulla DMZ, dove vengono depositati i file in entrata e in uscita. Spesso i file rimangono nei repository privi di protezione per ore o giorni, prima di essere recuperate da partner commerciali o clienti. In mancanza di un backup regolare e di adeguate misure di sicurezza, questi repository costituiscono rischi considerevoli per la sicurezza.

Il Data Streaming sicuro elimina questi rischi facendo pervenire i dati direttamente ai server di backend senza soste intermedie in alcun repository. In questo documento vengono analizzati i problemi posti dagli approcci tradizionali di tipo "store and forward" e viene presentata la soluzione fornita dal software Attachmate® FileXpress® che, rendendo sicuro il Data Streaming, può contribuire ad evitarli.

### L'approccio "store and forward": problemi da considerare

La maggior parte delle soluzioni legacy di trasferimento file (compreso l'FTP) utilizza approcci di tipo "store and forward" o basati su repository. Se è stata installata una soluzione "store and forward" o se è allo studio la sua introduzione, sarebbe opportuno porsi le seguenti domande:

1. In che modo si può essere sicuri che il repository non venga manomesso da soggetti esterni o interni, compresi gli amministratori?
2. Nel caso di file di grandi dimensioni, qual è l'aumento di overhead che la doppia scrittura e lettura del file comporta, dapprima nel repository e poi di nuovo verso la destinazione finale?
3. In che modo i dati vengono trasferiti dal repository al sistema di backend? Quale protocollo viene utilizzato? È il sistema di backend che deve dare inizio all'operazione, oppure il repository è in grado di inviare direttamente i dati al sistema di backend? Se è il sistema di backend che deve estrarre i dati dal repository, con quale frequenza quest'ultimo deve eseguire il controllo del sistema alla ricerca di file da recuperare? È necessario ricorrere a uno strumento di terze parti per eseguire il recupero dei file?
4. Quali procedure di backup sono necessarie per il repository?

5. Cosa succede se il repository è temporaneamente non disponibile per ragioni impreviste o per manutenzione del sistema? Sono previste modalità automatiche di passaggio a un sistema alternativo oppure è necessario sospendere tutte le operazioni di trasferimento fino alla riattivazione del repository?
6. Come vengono gestiti i file all'interno del repository, considerando che non possono restarvi indefinitamente per ovvi motivi di disponibilità di spazio? Vengono rimossi automaticamente in base a qualche tipo di configurazione oppure sono previsti interventi manuali periodici di manutenzione del repository?
7. Quanto spazio viene destinato attualmente al repository? In che modo verrà aumentato questo spazio in futuro? Esiste un processo al riguardo? Quali sono i costi?
8. Due eventi distinti intervengono nel trasferimento dei file alla destinazione finale: (1) la scrittura del file nel repository e (2) lo spostamento del file nella destinazione finale (o il sistema remoto per i file in uscita o il server di backend per i file in entrata). Come viene gestito il logging per questi eventi? È semplice controllare entrambe le componenti della transazione per avere una vista completa della stessa?
9. Come vengono gestiti il controllo della versione e l'integrità dei dati? Se alcuni file sono già stati collocati nel repository, è facile eseguire degli aggiornamenti oppure è necessario inviare un secondo set di file da scaricare? Come si può essere sicuri che gli utenti saranno in grado di distinguere le versioni più recenti?

In ultima analisi, la protezione dai rischi e dall'inefficienza di una soluzione "store and forward" è un'operazione costosa e che richiede un alto utilizzo di risorse. Fortunatamente esiste un'alternativa efficace, denominata Data Streaming sicuro.

### L'alternativa rappresentata dal Data Streaming sicuro

Il Data Streaming sicuro elimina la necessità di memorizzare i dati in un repository centrale. I dati in uscita permangono nel sistema di backend (dove sono stati creati) finché non vengono recuperati dal partner commerciale o dal cliente, mentre i dati in entrata sono inviati direttamente al sistema di backend, dove vengono elaborati sulla base delle regole aziendali.

La famiglia di soluzioni Attachmate FileXpress per la gestione del trasferimento file è stata messa a punto per trasferire in sicurezza file di qualsiasi dimensione verso qualunque destinazione da e per tutte le principali piattaforme. FileXpress Internet Server, normalmente installato nella DMZ, mette in sicurezza le connessioni con i client ricorrendo a una vasta gamma di protocolli e creando nuove connessioni distinte verso il o i server di backend interni. I server di backend possono ospitare servizi SFTP, FTPS o FTP oppure utilizzare il FileXpress Platform Server (un altro componente della famiglia FileXpress).

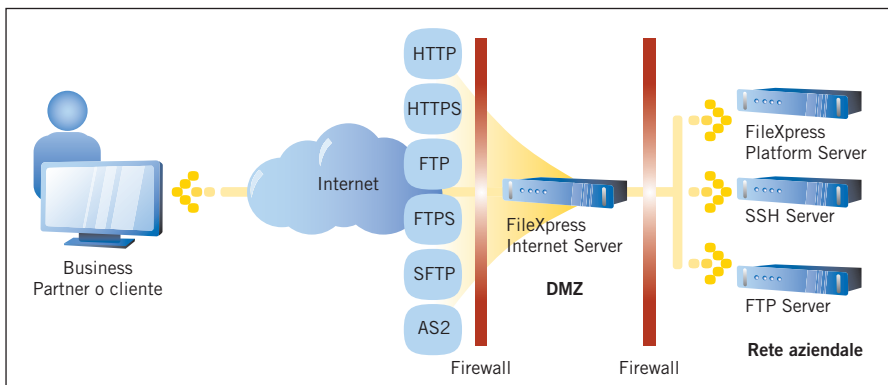
Grazie alle funzionalità di Data Streaming sicuro, FileXpress offre i seguenti vantaggi:

- **Maggiore sicurezza**

Se un hacker riesce a entrare nel repository, probabilmente avrà accesso a tutti i dati in fase di trasferimento. FileXpress Internet Server elimina questo grave punto di esposizione, in quanto costituisce un proxy sicuro che impedisce qualsiasi connessione esterna diretta ai sistemi di backend e nasconde qualunque configurazione interna o topologia di rete.

- **Semplificazione del processo**

Poiché FileXpress Internet Server non impiega un repository centrale, viene meno la necessità di un processo in due fasi, vale a dire scrivere un file nel repository e successivamente trasferirlo nell'ambiente.



FileXpress Internet Server mette in sicurezza le connessioni con i client e, successivamente, crea nuove connessioni distinte verso il o i server di backend interni.

- **Supporto post-elaborazione automatico**

Oltre a risiedere nella DMZ, FileXpress può anche risiedere sul sistema di backend, dove è in grado di elaborare i dati trasferiti sulla base delle regole aziendali definite dall'amministratore (ad esempio l'utente che invia i dati o il tipo di dati trasferito). Si potrebbe ad esempio configurare un intervento post-elaborazione che esegua la procedura di parsing di un file caricato e il successivo aggiornamento di un database con le informazioni memorizzate all'interno del file.

- **Gestione semplificata dello storage**

Con FileXpress, le aziende possono limitarsi ad utilizzare le funzioni di backup e recovery già implementate nei loro sistemi di backend. Non vi è alcuna necessità di installare nuovi sistemi di backup o recovery come quelli che si rendono necessari in presenza di soluzioni che utilizzano repository centralizzati.

In altre parole, FileXpress incrementa la sicurezza e abbatta i costi eliminando la necessità di memorizzare informazioni sensibili nella DMZ e aumentando l'efficienza del processo di trasferimento file.

## Un elevatissimo livello di sicurezza per il trasferimento file

Grazie al data streaming sicuro, FileXpress garantisce la sicurezza del trasferimento di file dall'inizio alla fine del processo. La sua architettura multilivello incrementa ulteriormente la sicurezza tramite le seguenti funzionalità:

- **Reverse proxy con cambiamento di protocollo in-stream**

FileXpress comprende un reverse proxy che funge da broker (intermediario) sicuro tra i file server e i client esterni che tentano di accedervi. Il proxy utilizza una nuova connessione con un protocollo completamente diverso rispetto alla connessione originale, al fine di chiudere le connessioni all'interno della DMZ e creare nuove connessioni verso il server di backend. Così facendo, isola di fatto la rete aziendale dal mondo esterno.

- **Autenticazione avanzata**

FileXpress aggiunge al framework di sicurezza esistente un livello estremamente avanzato di informazioni relative al controllo degli accessi, un livello che fornisce agli utenti permessi specifici per l'invio e la ricezione di dati. Grazie all'integrazione di LDAP e Microsoft Active Directory, FileXpress consente alle aziende di continuare a utilizzare i sistemi esistenti di registro utenti.

- **System obfuscation**

FileXpress è in grado di abilitare la system obfuscation (offuscamento del sistema), una tecnica di sicurezza che occulta i dettagli della configurazione dei sistemi di backend per impedire attacchi esterni. FileXpress può anche essere impostato per la condivisione di file e directory con numerosi sistemi di backend. In questo tipo di scenario, FileXpress presenta un'unica vista logica agli utenti finali, che accedono al FileXpress Internet Server attraverso un file transfer client, un'interfaccia a riga di comando o un web browser.

Con FileXpress è possibile dare a partner e clienti la possibilità di accedere ai file di cui hanno bisogno con la certezza di non rivelare i dettagli dei sistemi interni su cui essi sono memorizzati.

## Prestazioni migliori, costi inferiori, controlli più severi

Il Data Streaming sicuro offre vantaggi notevoli rispetto agli approcci tradizionali di tipo "store and forward". L'eliminazione del repository centrale tipico delle soluzioni di trasferimento file via Internet consente alle aziende di realizzare incrementi significativi dei rendimenti, di abbattere il Total Cost of Ownership (TCO) e di applicare controlli più severi sull'elaborazione dei dati, aumentando nel contempo il livello di sicurezza complessiva.

### La famiglia FileXpress

Attachmate FileXpress è una soluzione enterprise strategica che gestisce ed esegue in sicurezza il trasferimento di file all'interno e all'esterno dell'azienda. La famiglia FileXpress comprende i seguenti prodotti:

- **FileXpress Platform Server** è il motore che alimenta l'infrastruttura di trasferimento file e che fa pervenire in tutta sicurezza file di qualsiasi dimensione su tutte le principali piattaforme.
- **FileXpress Internet Server** è il portale attraverso il quale passano tutti i file che transitano in Internet. Consente di interagire in sicurezza con partner e clienti su scala mondiale.
- **FileXpress Command Center** è il cruscotto digitale per l'intera attività di file transfer, grazie al quale è possibile lanciare, tracciare, registrare, analizzare e supportare da un unico punto centrale tutti gli eventi relativi al trasferimento dati.
- **FileXpress FileShot** è l'agente per il trasferimento di file tra utenti. Grazie alla perfetta integrazione con Microsoft Outlook, è in grado di trasferire file di qualsiasi dimensione, fornire record per gli audit e risolvere i problemi relativi al superamento della dimensione massima delle mailbox.

### Informazioni su Attachmate

Attachmate commercializza soluzioni software avanzate per l'emulazione di terminali, la modernizzazione delle applicazioni legacy, il managed file transfer e la gestione delle frodi aziendali. Grazie alla tecnologia Attachmate, più di 65.000 aziende in tutto il mondo sono ora in grado di far funzionare meglio e in modo più proficuo le proprie risorse IT.  
[www.attachmate.it](http://www.attachmate.it)



**Sede Centrale**  
1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL 206 217 7500  
FAX 206 217 7515

**Sede Centrale EMEA**  
Paesi Bassi  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

**Sede Italiana di Milano**  
TEL +39 02 99060201  
FAX +39 02 99044784

**Sede Italiana di Roma**  
TEL +39 06 45 213 421  
FAX +39 06 45 213 301

WEB [www.attachmate.it](http://www.attachmate.it)  
EMAIL [informazioni.italia@attachmate.com](mailto:informazioni.italia@attachmate.com)

Per le informazioni sulle sedi locali, visitare [www.attachmate.it](http://www.attachmate.it)