



# Secure Data Transmission: Using a Managed File Transfer

No matter what business you are in, you move data. Every organization has some method of getting files from place to place and person to person, but can they provide an audit trail or confirmation that the files arrived securely?

In this pocket e-guide, get tips on managing secure transmission and exchange of data while keeping operational costs down. Learn Gartner's four components of a well-rounded managed file transfer suite and more about the growing trend of ad-hoc file transfer.

*Sponsored By:*





# Secure Data Transmission: Using a Managed File Transfer

## Table of Contents:

[Using a managed file transfer for secure data transmission, exchange](#)

[Resources from nuBridges, Inc.](#)

---

## Using a managed file transfer for secure data transmission, exchange

by Neil Roiter

Data has to move. Whether you are in manufacturing, financial services, entertainment, government, health care, pharmaceuticals -- whatever your business -- moving files, often big files, to and from departments, business units, partners, customers, etc., is at the heart of your operation.

Every organization has some way of getting files from place to place, person to person. It may be FTP or VPN, probably a home-grown solution using batch scripts, maybe with some file encryption and/or digital signing for some security. That gets you from point A to point B, but where's the audit trail? Where's the accountability? How do you know the files got where they needed to go and to the right people, or if they were even sent?

And how do you manage secure transmission and exchange all this data while keeping operational costs down? Managed file transfer (MFT) software and products have grown into a \$500 million-a-year business to meet the increasing security, compliance and operational demands of moving information.

"It's never just been an issue of security, although security is one of those low-hanging fruits that gets everyone's attention," says Gartner research director L. Frank Kenney. "More companies are affected by a failing audit and the fear of failing audits.

"The bigger issue is can I be assured, can I show, that a file that moves from point A to B has been secured, that the person who sent it had the authority to send it and was authenticated, and that the person who received it had the authority to receive it and was authenticated." Typically, a well-rounded managed file transfer suite should have four components, according to Gartner:

- Server for management of all aspects of file transfer--communications channels, multiple protocols, workflow, provisioning, APIs, etc.
- Client for tight server integration.
- Proxy to conceal IP address and ports.
- Plug-ins to integrate with applications.

The issue covers not only mass file movement but ad hoc transfers between people. So, managed file transfer products need to be able to transparently manage file transfers between people via email and other channels.

"Ad hoc file transfer is an important trend," says John Thielens, VP of technology for Tumbleweed, now part of Axway. "You think of managed file transfer as something scripted or for techies, but there's also file transfer technology for human-to-human collaboration -- Web conferencing, IM, email."

Enterprises buying into this market are typically looking to replace home-grown solutions and/or standardize on one product across the enterprise.

"Most places have home-grown solutions," says Gartner's Kenney. "It's not greenfield; just about everyone has leveraged FTP."

"If you roll your own, the cost is very high," says Proginet CEO Sandy Weil. "And, you don't have a consistent way to manage security around file transfers."

For many enterprises, it's time to herd all the file transfer cats and migrate to a secure Managed File Transfer (MFT) infrastructure. Why? Proving compliance is the most common business driver. And to prove compliance, you need centralized control of file transfer and authentication, visibility into all activity and security event logging.

MFT is also a step in the right (architectural) direction if you're contemplating data loss prevention technologies. And centralized MFT makes it easier and more efficient to support end users, to facilitate ad hoc file transfers, and to share data with authorized people and systems outside the firewall.

## nuBridges Exchange™ helps you put the *managed* in file transfer across the extended enterprise.

nuBridges Exchange™ is a new generation of enterprise MFT software that's easy to implement and administer, reliable, secure and efficient.

### MULTIPLE COMMUNICATION PROTOCOLS

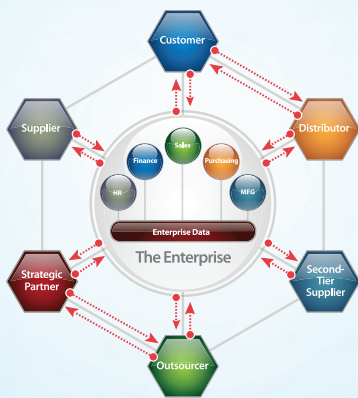
Client and server-side

### SINGLE, WEB-BASED POINT-OF-CONTROL

Server management, user profiles, audit logs and more

### VISIBILITY INTO FILE TRANSFERS

Internal, external, scheduled and ad hoc



Ready to put the *managed* in file transfer for your enterprise? Let's talk.

+1.770.829.2400  
[www.nubridges.com](http://www.nubridges.com)

## Resources from nuBridges, Inc.



### Managed File Transfer Information from nuBridges:

- <http://www.nubridges.com/lp/2010-tech-target/managed-file-transfer/>
- <http://www.nubridges.com/lp/2010-tech-target/managed-file-transfer/white-paper/>

### About nuBridges, Inc.

nuBridges provides technology solutions for extended enterprises that share sensitive data across applications, departments and organizations, and face complex security and compliance mandates. Our innovative data encryption, data tokenization, key management, managed file transfer and EDI solutions help customers get information from point A to point B; do it safely; and prove compliance.

For more information, please visit [www.nubridges.com](http://www.nubridges.com)