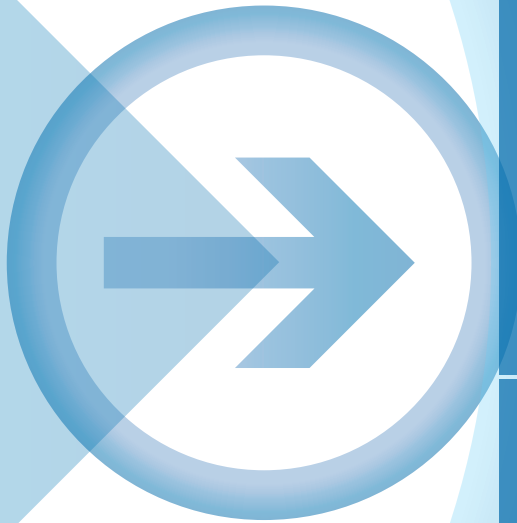




End-to-end Processing with TIBCO Managed File Transfer (MFT)[™]

Improving Performance and Security
during Internet File Transfer



Abstract: *File-transfer technology has become increasingly critical to the enterprise business process as companies look to integrate with customers and business partners and drive global data movement strategies using the Internet. The need to secure business data in motion is a given but what happens when it reaches its destination? Many file-transfer solutions (not to mention FTP) deploy repository-based approaches, which introduce untold security risk at either end. End-to-end processing eliminates this risk by delivering data right into back-end applications (no repository required). This Brief looks at the major benefits of end-to-end processing, particularly security, control, and efficiency.*

Introduction

Users opting to deploy TIBCO's Managed File Transfer (MFT)™ end-to-end processing will see significant performance improvements, tighter controls over the processing of the data and lower total cost of ownership (TCO).

Typically, Internet file-transfer solutions can not match this level of integration or efficiency. Most applications typically deploy a central repository where files coming in and out of the organization are stored. Files sit in these repositories as they wait for business partners to download. These repositories are also the staging area for incoming files. Administrators need to be concerned with maintaining and managing these repositories, ensuring proper backups, and taking the appropriate steps to ensure that these repositories never get compromised.

The Advantages of End-to-end Processing

With end-to-end processing, TIBCO MFT eliminates the need to store data in a central repository and allows the data to reside on the backend system (where it was created) until the business partner initiates a download. Incoming data is delivered directly to the backend system that will be processed based on business rules. In addition business partners do not have to come to retrieve the data; MFT's end-to-end processing function allows your organization to send the data directly to the business partner – without manual intervention.

There are a number of other benefits to end-to-end processing, including:

- » **Post-processing Support:** automated data processing on the backend system. Because MFT resides on these systems, it can process the data upon receipt based on business rules defined by the administrator (such as the user sending the data or the type of data).
- » **Maximized Security:** having no central repository eliminates a serious point of exposure. TIBCO's view is that data at rest is data at risk. If a hacker is able to compromise the data repository, they can potentially gain access to all data being transferred with the file-transfer solution. MFT eliminates this possibility by provid-

ing a secure proxy, preventing any direct outside connection as well as isolating any inside configuration or network topology. This eliminates the possibility of socially-engineered attacks.

- » **Improved Performance:** MFT provides a significantly more efficient and streamlined process. This is a key performance issue and an important differentiator because MFT eliminates the step of writing to a central repository and then performing a second step to move it into the corporate environment.
- » **Tighter Integration:** finally, by leveraging the backend systems, organizations are able to leverage their existing backup and recovery systems. This eliminates any requirement to have to deploy new backup or recovery systems such as those required for solutions that use centralized repositories. End-to-end processing brings many significant benefits to any MFT deployment but that is not where the benefits end: MFT adds a multi-tiered security architecture that ensures the highest level of security. These capabilities include:
 - » **Reverse Proxy with In-stream Protocol Switching:** MFT's Reverse Proxy securely isolates backend servers from direct Internet access, acting as a secure broker between Web servers and the external clients who attempt to access them. Reverse Proxy is an industry standard and a way of terminating connections in the DMZ and establishing new connections to the backend server. This approach is used by other Internet file transfer solutions to secure their data repository; however, MFT adds an additional level of security by utilizing not only a new connection, but a new connection that uses a completely different protocol from the original connection. This adds an additional, and critical, level of isolation between the outside world and the corporate network.
 - » **Strong Authentication:** MFT provides a robust authentication model that leverages an organization's existing security framework to control user access. On top of the existing infrastructure we add an additional layer of access control information that requires a user to be granted specific permissions to any data they may want to send or receive. This combination includes two or more of the following, depending on the environment: Operating System Security, LDAP Directories, Business Rules, and Web SSO solutions.
 - » **System Obfuscation:** MFT never reveals any details of the internal configuration or layout of the backend systems to the end user. This prevents the potential that a user will be able to use such information for a socially-engineered attack. This is a common security practice referred to as obfuscation. The system can even be set up to share/distribute information across a number of backend systems with the user in no way aware that it is not sitting on the local system where the MFT Internet Server is running.

Some Things to Consider

Organizations considering a solution that does not provide end-to-end processing will need to understand the following:

1. What security is in place to ensure that the repository cannot be compromised by internal or external parties?
2. Do administrators of the Internet file-transfer systems have access to files stored within the repository? Does this open up any security exposure for sensitive files?
3. For large files, what is the increased overhead of having to read and write the file a second time (once to the repository and again at the final destination).
4. How is the data moved between the backend system and the repository?
 - a. What protocol is used?
 - b. Does this comply with security standards for internal movement of data within the organization?
 - c. Does the backend system have to initiate all the movement or can the repository send the data directly to the backend system?
 - d. 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 or are these capabilities delivered as part of the solution? Is there any significant overhead to the polling process?
5. What backup procedures will you need in place for the repository? Are there any special needs?
6. What happens in the event of the data repository being offline whether it is unplanned or for system maintenance? Are there automated ways to roll over to a mirrored system or will all transferring need to be suspended?
7. How do you manage the files stored within the repository? They cannot be stored indefinitely. Are they automatically removed based on some configuration or are there steps that the administrator must perform regularly to maintain the data repository?
8. Based on your understanding of the volume, how much space will be needed for the data repository? If your needs increase in the future, what is involved in increasing the amount of storage? Is there a process? A cost factor?
9. There are two separate events to move data to the ultimate location: first the writing of the file to the data repository, then the moving of it to the ultimate destination location (either the remote system for outgoing files or the backend server for incoming files). How is logging handled for this? Is it easy to map both ends of the transaction to have a full view of the transaction?
10. What are the implications in terms of version control and data integrity? If you have already posted files to the data repository, and you need to make updates before the user downloads them, can you easily make updates or do you need to just post a second set of files for download? Can you ensure that the users will be able to sort out the most recent versions?

Clearly, there are many issues to consider if you are evaluating file-transfer systems for use in your organization. In our experience, many of the systems currently on the market do not offer end-to-end processing.



Conclusion

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

TIBCO Software Inc. (NASDAQ: TIBX) is a provider of infrastructure software for companies to use on-premise or as part of cloud computing environments. Whether it's efficient claims or trade processing, cross-selling products based on real time customer behavior, or averting a crisis before it happens, TIBCO provides companies the two-second advantage™ - the ability to capture the right information, at the right time, and act on it preemptively for a competitive advantage. More than 4,000 customers worldwide rely on TIBCO to manage information, decisions, processes and applications in real-time. Learn more at www.tibco.com.



Global Headquarters
3303 Hillview Avenue
Palo Alto, CA 94304

Tel: +1 650-846-1000
+1 800-420-8450
Fax: +1 650-846-1005

www.tibco.com