What MFT Is, and How It Applies to You

Thomas Skybakmoen

Gartner clients increasingly ask how to replace existing file transfer solutions to better manage and govern file transfers across application-to-application (A2A), B2B and cloud environments. This research provides a detailed explanation of managed file transfer (MFT) capabilities for CIOs, enterprise technology architects, integration competency center/service-oriented architecture (SOA) center-of-excellence (COE) staff, B2B integration managers and project leaders.

Key Findings

- MFT solutions deliver reliable capabilities to address file transfer across internal A2A, B2B and cloud environments, while providing centralized governance for file transfers across these environments.

- Organizations looking to MFT should expect a differentiated MFT market and vendor diversity for the next two years.

- Organizations are increasingly seeing the value of one solution to facilitate all file transfers, thus increasing end-to-end visibility in business processes.

Recommendations

- Before rolling out MFT projects, IT organizations should take stock of file transfer in their companies, and understand every connection and how it might impact the business. Thus, they need to map governance processes to MFT, and not just rely on MFT software to solve governance.

- When evaluating MFT solutions, IT organizations should bear in mind that they will only find a handful of MFT vendors supporting the full range of MFT applications; thus, large projects often will end up with two solutions.

- Organizations embarking on MFT projects should consult their integration competency centers (ICCs). This is to make sure MFT comes under the same practices, technology architecture standards and governance as other integration efforts.

TABLE OF CONTENTS

Gartner

ANALYSIS

Organizations conduct file transfers between external audiences such as trading partners (through email, File Transfer Protocol [FTP] and, in some cases, B2B gateways) and internally to operating environments and between individuals, for example. However, as organizations face file transfer proliferation, they realize they lack visibility, management and governance across these file transfers.

Traditionally, organizations have used different vendors and custom-built software alongside the proliferation of file transfer technologies, a mixture that has resulted in poor, unconsolidated views of file transfers. Organizations often find that managing these is a resource-intensive task, with operations personnel spending time testing each system to locate the causes of problems in lieu of full, end-to-end traceability. The burden on the operations staff is particularly heavy when file transfers are carried out on a larger scale across many applications, systems and partners, or embedded in the implementation of a service in an SOA application.

Managing these disparate solutions is becoming more resource-intensive, and offers little or no central visibility and governance. Organizations need to evaluate how MFT can help strategic business initiatives and offer consolidated solutions to file transfer. IT should look to deploy MFT through an ICC to establish appropriate best practices and governance (see "Managed File Transfer Offers Solutions for Governance Needs").

Definition of MFT

MFT usually is composed of four components that organizations can implement separately, but often deploy as a suite. These four components are:

- **Server (back end):** This manages all aspects of the file transfer; and supports multiple communication and security protocols and mechanisms, workflow, provisioning, some transformation, APIs and adapters, and streaming input/output.

- **Client (front end):** This is a subset of server technologies, mainly for scheduling, scripting and local reporting. Applications (via APIs) and humans (via a graphical user interface [GUI]) use clients for collaboration, such as large file transfers using email systems.

- **Proxy:** These technologies abstract other elements of the infrastructure, such as a proxy deployed in a demilitarized zone that conceals the true Internet Protocol (IP) addresses and ports of senders and recipients.

- **Application plug-in:** This interoperates or integrates with applications, enabling them to communicate natively with MFT servers, or enabling ad hoc file transfers.

FTP Meets Its Limitations

Organizations continue to make wide use of FTP to move files. Many organizations combine vanilla FTP with Unix/Linux cron scripts or other utilities in combination with monitoring tools to "get the job done." The problem is that these are not integrated MFT tools; they are just locally managed OS-specific scripts. These local solutions do not provide a single-view unified tool, nor do they offer centrally managed security. FTP on its own does not have security features to encrypt or ensure data integrity. Although flexible and easy to deploy, FTP does not provide a viable solution for insight, security and performance and, ultimately, no-risk mitigation.

Gartner

Many Gartner clients report that their FTP solutions often lack central visibility, and do not offer an integrated solution for internal and external file transfer requirements, such as support for multiple protocols and APIs for A2A integration. They also report that their FTP applications are unable to scale to meet modern business demands. Examples range from complex workflows, integration into business applications to perform push and pull of data, increased demand, and segregation of data and users (see "FTP Replacement: Where MFT Makes Sense and Why You Should Care").

FTP often lacks:

- Checkpoint and restart capabilities

- Automated onboarding of users

- Automated rollout to servers for rapid deployment and provisioning

- APIs to integrate with applications, middleware, email and cloud

- Management and security of file movement for collaborative purposes

- Internal connectivity between various operating environments

- Content validation before and after file transfer

- Route files based on policy or content

- Reporting and administration, including user activity, system utilization, scheduling, receipt monitoring, real-time notifications and routing

- Centralized reporting functionality for error reporting or status of all file transfers

- Centralized analytics

- File/data transformation, and file management with versioning capabilities to prevent data duplication or data loss

- Built-in encryption, certification and validation of data

- Workflow rules that dictate file movement from one job to the next and events that would trigger an action

- Metadata to ensure file integrity

Five Key Factors Are Driving Organizations to Adopt MFT

The proliferation of file transfers and repositories presents new challenges for governance and compliance. At the same time, organizations are seeking to lower the cost of staffing and administration for file transfers. MFT aids governance efforts by enabling file transfers to be monitored and managed. Traditional file transfer solutions, such as scripts and FTP, often lack visibility features, and don't have integrated solutions for internal and external file transfer requirements.

The most prominent factors driving organizations to adopt MFT are:

- **File size and volume —** Organizations face ever-increasing demands for larger files (e.g., files containing metadata, video, audio and office documents, such as PowerPoint files that can exceed email attachment limits), more of these large files and more

Gartner

external entities to exchange files with, and finally larger numbers of small files that must be moved around on schedule between many endpoints.

- **Scheduling —** The staffing and administration necessary for FTP and scripts increase with volume and often do not scale from an application and administration point of view. For example, some organizations have to manage 2,000 individuals using file transfer on a daily basis. FTP often struggles to support more than 20 concurrent file transfers per FTP solution, and, in many cases, there is no offloading capability other than the ability to refuse connections, which can increase the volume of requests to the FTP administrator as users are faced with error messages, rather than a message to tell them their transfers are queued.

- **Security —** Businesses often have very strict requirements around their demilitarized zones (DMZs), and most FTP solutions do not provide sufficient capabilities to secure data in transit and at rest.

- **Monitoring/auditability —** Traditional file transfer solutions lack visibility features. MFT will enable businesses to monitor several hundreds or thousands of connections in real time or near real time. Business users, IT and business partners can get access to this information through predefined reporting, and are able to do trend analysis and understand who has access to the files at any given time.

- **Scripting and exception handling —** MFT aids governance efforts by enabling organizations to monitor and manage all file transfers using the same rules. Examples of failures range from attempts to login with the wrong credentials, to packages failing in transfers because of network and/or endpoint failures. It is possible to automate responses, for example, to block IP address ranges to stop failed login attempts, resend packages or produce emails to notify trading partners of endpoint failures.

Therefore, organizations look to MFT to provide a single solution, integrate with internal systems and external partners, and allow the movement of files from a single centralized location.

MFT enables and enhances:

- **Management and security of file movement for collaborative purposes:** Internal and external partners often use email to exchange large files. MFT enables file encryption and secure alternative delivery mechanisms for email. MFT for email comes in the form of plug-ins to integrate MFT with applications that need to move files on and off these systems to provide full governance of file transfers.

- **Internal connectivity between various OSs and hardware:** MFT can secure internal file transfers from A2A, and to and from different files systems. It can also replace unsecured and unmanaged HTTP, FTP or physical media transfers, such as backup tapes.

- **Connectivity with external partners:** Here, MFT generally replaces FTP and email transfers. It provides templates for rapid onboarding and self-service for partners, and reporting and group administration features to manage large groups of users. MFT provides SLA reporting for the business and its partners, which enhances the customer experience. Organizations should be aware that if MFT is used with a B2B technology (e.g., BizTalk Server), then one could be duplicating trading partner information; thus, data consistency across the two technologies should be planned.

Gartner

- **Centralized reporting and analytics:** MFT can monitor internal and external file transfers. This allows for quick identification and resolution. It also helps businesses comply with regulations that apply to their industries.

The Changing Role of File Transfer

Gartner sees a shift from stand-alone file transfer (FTP) and tactical MFT solutions to strategic MFT. This is applicable for clients involved in midsize and large projects, where there is some focus on consolidation and integration. Traditionally, organizations have viewed file transfer solutions as department-level point tools. However, increasing numbers are taking a more holistic approach. This is especially true of larger enterprises, where the number of MFT solutions in use duplicates work and creates compliance issues — for example, some Gartner clients report as many as 10 solutions, ranging from internal scripts to multiple MFT products.

Organizations increasingly want consolidated management and visibility capabilities to better manage customer experiences and expectations (SLAs) across the business. In B2B, trading partners demand better visibility and capabilities that contain not only management, but also solutions that enable file transfers to be monitored and to ensure that files are secured with their partners.

The traditional deployment scenario for MFT was to replace FTP. However, MFT's role has been expanded to include a range of integration efforts, from internal A2A, SOA and data integration initiatives to external B2B and cloud computing projects. MFT also helps govern files in applications such as email programs (Outlook, for example), collaboration tools (such as Documentum) and application development tools. We still see many organizations that require only basic MFT functionality, such as secure, reliable, high-performance large-file transport; checkpoint/restart to work around unreliable networks and connections; and multithreading to increase performance, compared with traditional file transfers, which is one of the primary reasons for considering MFT solutions.

MFT is evolving into a holistic solution that includes a set of services that work to enable various governance processes and policies relating to the management, coordination and trust of file transfers. As the MFT market evolves and solutions mature, it is important that organizations understand that implementing MFT integration projects without a coherent, holistic strategy generally leads to inefficiencies and vulnerabilities associated with individual IT groups implementing MFT projects with different approaches and technologies. The MFT integration project should be defined in light of other relevant IT strategies for internal integration, A2A, B2B, SOA, cloud computing, software as a service (SaaS) and business process management (BPM). Failure to do so will lead to the proliferation of files moving outside the MFT technology, such as via unsupported FTP, which will increase the possibility that compliance efforts will not achieve their aim, and could lead to complete failure of the MFT project.

Consider the Following Functionalities in MFT

Currently, Gartner tracks more than 45 vendors in the MFT market. Many vendors have specific solutions, such as file transfer acceleration, support for tablets, collaboration (e.g., SharePoint), and others support specific OSs. However, there are some key functions to consider (see "How to Distinguish and Choose Between MFT Solutions").

Functions to consider include:

- **Secure multiprotocol communication:** Organizations will find that some vendors support a range of protocols; other will only support a few. Examples of supported protocols include FTP, FTPS, HTTP, HTTPS, SSH/SFTP, SSH/SCP, AS1, AS2, AS3,

Gartner

IBM Sterling Connect:Direct, WebDAV, SOAP, ODETTE, ebMS, OFTP, OFTP 2 and MQSeries.

- **Different Use Scenarios for MFT:** Understand the different use scenarios for MFT. Gartner has identified five:

  1. **Ad hoc file transfer:** MFT is used to provide mechanisms for sending large files through either email or a Web interface, for example, to an individual.

  2. **Accelerated transfer (i.e., UDP):** When performing file transfer over large distances, or where there are issues with routing of files, data transfer latency often increases. UDP provides mechanisms to speed up the file transfer, often 10 times faster than normal protocols.

  3. **A2A:** MFT will integrate with existing applications through APIs and software development kits (SDKs), as well as support multiple operating environments.

  4. **B2B:** MFT will secure existing file transfers, such as FTP, and support a range of protocols (i.e., AS2 and OFTP), while providing visibility into SLAs with business partners, to name a few.

  5. **Cloud to on-premises and vice versa:** MFT can be used to back up files in the cloud, and facilitate synchronization of data between on-premises applications and off-premises applications (e.g., salesforce.com).

  6. **SOA:** MFT supports SOA through APIs and SOAP calls, as well as through integration. MFT can integrate with existing governance processes and tools. Examples are MFT vendors that use registries and repositories to store metadata about file transfers.

- **Provisioning:** Rapid deployment to meet the demands of your business and the marketplace.

- **Transformation:** File/data transformation, and file management with versioning capabilities to prevent data duplication or data loss.

- **Security technologies:** Encryption, certification and validation of data.

- **Checkpoint and restart capabilities:** Failed file transfers are automated and mechanisms exist to facilitate alternatives, such as email notifications when files have failed a certain number of times.

- **Workflow:** Rules that enable file movement from one job to the next, events that would trigger an action and metadata to ensure file integrity.

- **Reporting and administration:** User activity, system utilization, scheduling, receipt monitoring, real-time notifications and routing.

- **Active Directory and LDAP integration:** Users are given access to the MFT tool through their regular login and permissions.

- **Storage area network/network-attached storage support:** Provide easy backup and access to files.

- **Mechanisms for securing FTP:** Existing and new connections, by adding encryption while the file is in transit and at rest.

Gartner

- **Support for local languages:** Many MFT solutions will only support a limited number of languages, because the majority of vendors are U.S.-based. However, there are some exceptions.

- **Database support:** MFT often comes with a database, or will allow you to integrate the MFT with existing databases. This is for reporting purposes, logging and compliance, to name a few.

- **Support for several OSs:** If you have requirements for file transfer on OSs such as AS/400, make sure the OSs are listed, as the number of vendors supporting this feature is limited.

- **How the MFT tool is accessed:** Some vendors will provide more than one way to access the MFT solution; some vendors will provide Java clients, thus supporting multiple OSs; and others will only give access to MFT through an HTML client (browser), Windows (ActiveX) client, Windows (.NET) or a command line, to mention a few options. Some MFT tools can also be accessed through mobile phones and tablets.

MFT Is Not Always a Stand-Alone Technology

MFT is just one category of back-end integration technology. Others include an enterprise service bus (ESB) for B2B gateway software, integration brokerages, cloud services brokerages (CSBs) and integration-platform-as-a-service (iPaaS) offerings.

What differentiates MFT from other forms of infrastructure are:

- MFT's unique focus on particularly large files, and the scheduling and management of moving very large numbers of files and bulk data between applications and businesses.

- The movement of files and data in usage scenarios that many integration solutions do not typically address, such as enhancing the performance of file attachments in email.

Note, however, that all integration solutions are rapidly converging so that, for example, MFT solutions continue to incorporate more-general-purpose integration capabilities, such as ESBs or B2B gateways, and vice versa (see "Gartner 2011 Research Outlook on Managed File Transfer").

MFT Helps With Governance and Compliance

MFT includes the capability to provide a set of services that works to enable various governance processes and policies related to the management, coordination and trust of the file transfer.

These governance services are:

- **Visibility:** Enables the organization to examine file transfers, processes, transactions, systems, and the people who interact with messages and files.

- **Monitoring:** Enables the tracking of messages, files and transactions as part of a larger governance initiative.

- **Security:** Integrates with solutions, such as B2B, A2A and middleware, to enable full governance to address risk, identity, access and authentication issues.

- **Reporting and auditing:** Enables companies to compile and assemble data related to all aspects of file transfers; in existence with other tools, this enables a complete audit and reporting capability.

Gartner

- **Adaptability:** Provides companies with the opportunity to connect with existing, as well as new, systems and infrastructures.

- **Provisioning:** Enables enterprises to rapidly onboard systems, companies and individuals, and to continually manage change in these environments.

- **Workflow and automation:** Enables companies to design, test and execute the processes associated with file transfers.

MFT Is Not Just About Technology

Stage 1

You need to understand how files move, and how files are transferred in and out of the business. The IT department needs to identify and understand what file transfers take place. Without this effort, MFT will not help manage governance issues related to file transfer. IT organizations should consult their ICCs. MFT will often come under the same practices, technology architecture standards and governance as other integration efforts.

Stage 2

Once a clear understanding exists of what transactions take place internally and externally (such as HTTP calls, FTP transactions, message queue transactions, ad hoc email and collaboration file transfers), IT can use this to build a foundation to improve visibility and governance, as risks surrounding file transfers are identified, and define policy.

Stage 3

Approach the governance of file transfers as an ongoing program. All file transfers should undergo continuous tracking to ensure that they are visible, governed and part of MFT solutions to enforce policy based on risk. Consider MFT disciplines essential for your organization, and likely part of your COE for integration, ICC, SOA or BPM. File tracking can take several months to complete; however, once you have the expertise, individuals will manage file transfer governance on a continuous basis, which will reward you with reusability and reuse.

Look at the degree of control required to enforce governance of data movement throughout the organization. It is possible to integrate MFT with existing data transfer solutions, to ensure you can monitor all file transfers and enforce governance policies as part of the COE. Because organizations consistently need to enforce governance, regardless of technical physical domains, all attributes and policies should be available to an administrator, regardless of the type of file transfer and where file transfers are taking place. This is to provide administrators, process owners and policy owners with visibility and assurance that the proper policy was enforced (see "Managed File Transfer Offers Solutions for Governance Needs").

RECOMMENDED READING

Some documents may not be available as part of your current Gartner subscription.

"Platform as a Service: Definition, Taxonomy and Vendor Landscape, 2011"

"How to Distinguish and Choose Between MFT Solutions"

"Taxonomy, Definitions and the Vendor Landscape for Application Integration Solutions, 2011"

"Gartner 2011 Research Outlook on Managed File Transfer"

Gartner

"Managed File Transfer Offers Solutions for Governance Needs"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner