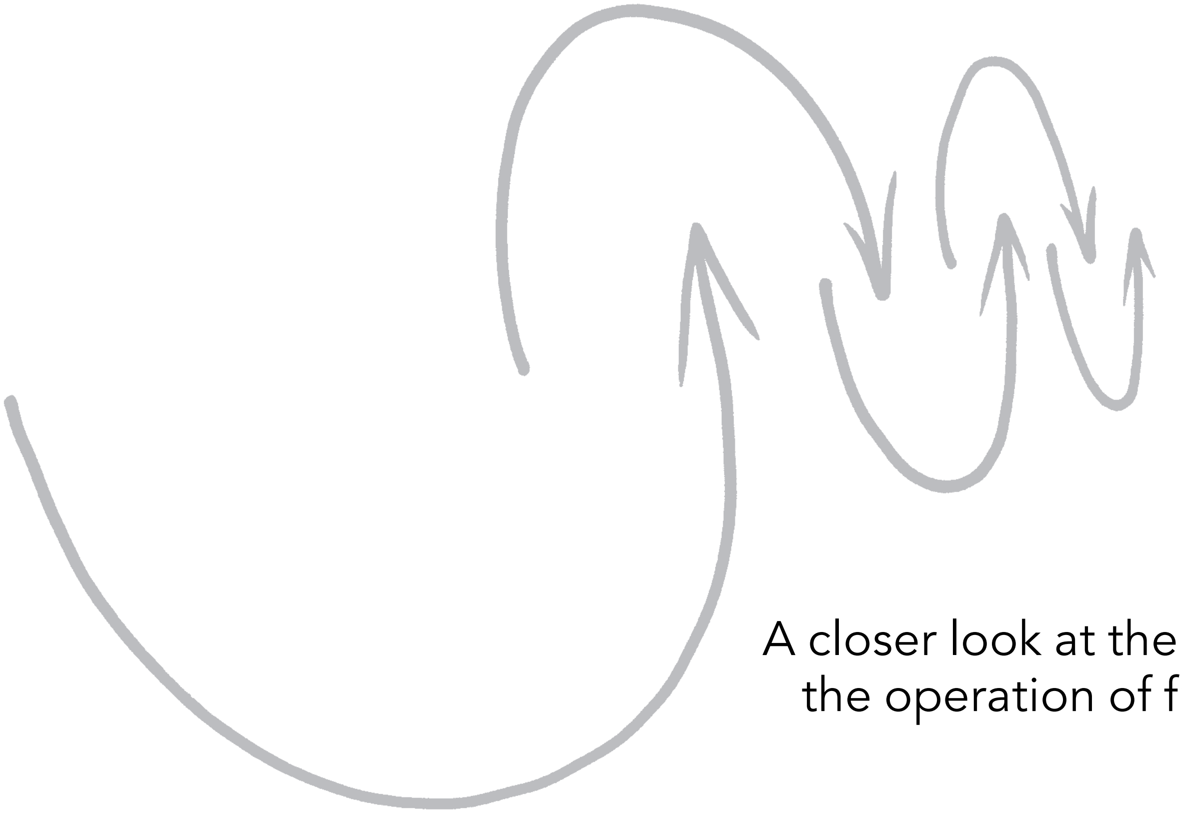
STERLING COMMERCE WHITE PAPER

FTP is Free, but Can You Really Afford It?



A closer look at the total cost of the operation of freeware FTP

Sterling Commerce
An IBM Company

Introduction

File Transfer Protocol (FTP) is a widely used data-movement standard. It provides an unsophisticated and straightforward way to move files to and from remote platforms. Its simplicity of operation, however, comes with a price. This paper examines the hidden costs that result from extended FTP use for critical, production-level data movement.

Large networks are inherently unreliable due to their expanse and complexity. With extended use, the probability of failure increases in proportion to the amount of information that is transmitted. The distributed nature of the Internet, however, tends to hide the overall impact and cost of failures. The decentralized management, security, and performance of the data movement operation generally masks the costs associated with interruptions, rework and security failures. Yet these hidden costs can be exposed dramatically when network failures result in missed processing windows or service levels. Unmanaged use of FTP represents an intolerable risk to the value of the network infrastructure. Companies and organizations that understand the importance of on-time, predictable and secure data movement select products that fit their performance, management and security requirements.

This is not to say that managed FTP does not have a place in every organization. Issues develop when organizations do not match the needs of the business process to the file transfer capabilities for meeting those needs. It is particularly a problem when organizations assume a one-size-fits-all approach with FTP.

Sterling Commerce provides the management capability, auditing features, security enforcement and workload balancing that organizations need to address the inherent complexity and unreliability of networks. The temptation to compare software license costs with free or low-cost FTP acquisition is fallacious, since this represents but a small fraction of the overall cost of operation for FTP. IBM® Sterling Managed File Transfer has the ability to enforce security, balance the use of network resources, and automatically recover from the interruptions that invariably occur. FTP, by comparison, does none of these. A careful evaluation of the relative ability of Sterling Managed File Transfer and FTP to ensure the timely and reliable delivery of critical business information strongly favors the use of Sterling Managed File Transfer. A key component of the Sterling Managed File Transfer solution, IBM® Sterling Connect:Direct® allows organizations to automate the data exchange between mission-critical applications regardless of platform. Many businesses have made the same calculations in favor of Sterling Connect:Direct, and today it runs on over 45,000 servers.

Consistent management of data movement operation and use of network resources

As data movement grows within and between enterprises, it is becoming more important to effectively manage data transmission operations according to business priorities. Unmanaged data movement can result in unproductive utilization of network resources. In catastrophic cases, unimportant or duplicate bulk data movement can impact critical data delivery.

Inability to prioritize and control use based on business policies threatens the data movement infrastructure. FTP provides no way to control critical data movement or balance it against lower-priority work that can impact processing windows. Massive, unmanaged data movement can delay and slow critical deliveries. FTP places all control in the hands of the client, and the first job usually wins. FTP also lacks the ability to create an enforceable policy for workload execution. Over time, this frequently results in chaos.

Sterling Connect:Direct gives each process a work-queue priority and a session class. Priorities are used to determine when processes run, and session classes are used to reserve transmission channels for critical transfers. These can be set up and enforced in accordance with business requirements. Users' requests are always accepted, but the actual operation of the request is scheduled according to the business policy that drives the priority and class structure.

This accomplishes the goals of the user as well as those of the business. Without queuing, scheduling and management capabilities, it is impossible to control the data movement workload.

In addition, these capabilities give the enterprise a way to manage work when exceptions or high-priority work suddenly occur. The data-movement workload can be suspended, re-prioritized and restarted dynamically. This allows for continuous exception management as unplanned business priorities arise. FTP just does not have the management infrastructure to be able to respond to real-time business needs.

Consistent security enforcement

Security concerns are not a part of the FTP model. The client must supply an ID and password upon opening the connection to the server, but this security information is transmitted in open text. The ID and password must be valid on the server, which means that this security information must be distributed to all clients. If a client needs to transmit to many servers, the client must have a valid ID and password for each.

Security violations are not logged in FTP. Moreover, there is no authentication of the client. Encryption—if it's done at all—must be an offline process.

As a result of the inability to enforce security policies with FTP use, many enterprises have chosen to ban it from production level use completely. The risk of security compromise is too great.

There is another, and possibly catastrophic, set of security exposures with the use of FTP. These are documented on the CERT Web site (www.cert.org), and include the ability to use standard FTP commands to create a denial of service situation or exploit known vulnerabilities within the FTP daemons to gain administrative or root access. Since the source code for many FTP implementations is freely available, expect additional new and creative security attacks.

Sterling Managed File Transfer offers multiple choices, ranging from securing FTP traffic to robust security, which allow the data movement operation to fit naturally within enterprise security policies. If support of FTP traffic is required, the data flow can be encrypted. If higher security levels are required, proxy-based security, coupled with authentication and configurable encryption, can be implemented within the Sterling Managed File Transfer deployment.

The value of these safeguards can be enormous. Even minor lapses in security can be expensive in terms of response and containment. In order to assess vulnerability, many enterprises are expanding the security perimeter testing to include penetration test cases. The exposure created by open, uncontrolled use of FTP should be understood as an exposure within the security policies of an organization.

Consistent notification

In addition to consistent management, organizations need a structured level of notification that enables real-time adjustments to the data movement infrastructure. The enterprise requirements for notification are:

- Instantaneous notification of critical exception and error conditions
- Flexibility in the routing of notifications
- Integration of data movement notification with the Enterprise Systems Management (ESM) structure
- Historical logging of data movement activities

Sterling Managed File Transfer answers all these requirements by providing notification and logging as a natural part of the data movement operation. Notification can be routed, using a variety of platform capabilities, to operation and monitoring staff. Alerts represented by SNMP traps can be directed to ESM systems for proactive action at the network level. And all file transfer activity, including finely grained operational detail, is logged continuously.

FTP provides none of these capabilities. It is very difficult, if not impossible, to determine previous FTP activity. Any action that is required must be performed by the client/user. This makes for an inconsistent and unresponsive data movement infrastructure. Therefore, the cost associated with the use of FTP must include the inherent delays in exception discovery.

Consistent recovery

As the size and volume of data movement uses grow, so does the likelihood of failure. A robust data movement infrastructure requires numerous hardware and software resources. The reliability of the entire structure that is needed for data movement operations is the multiplicative product of the reliability of each component. That is to say, if there are 50 components, and each component has a reliability of .9999, then the reliability of the entire infrastructure is .995. This means that there are five chances in 1,000 of a failure for each operation.

The upshot is that errors, exceptions and disruptions should be taken into account as a natural part of the business contingency plan. Just as the backup policy is an essential part of any production server, the ability to deal with network disruptions must be an essential element of the data movement infrastructure.

FTP does not provide an automated way to recover from network errors. Any outage that occurs with FTP operations must first be discovered and then handled manually. This generally means restarting the failed operation from the beginning.

The costs associated with FTP recovery are:

- Retransmission due to networking resource failure. On average, FTP will need to retransmit half the overall data movement volume per failure. Sterling Managed File Transfer recovers the network connection and requires no retransmission

- During a network-resource failure, FTP use requires discovery of the failure. This delay in restart represents cost. Sterling Managed File Transfer will automatically sense network failures and retry the operation. In most cases the recovery will be automatic. In the case of a permanent outage, notification is provided to enable rapid resolution

- Duplicate transmission due to incorrect FTP option specification is a common occurrence. One study found that 10 percent of FTP transfers were retransmissions of files that resulted from an incorrect option selection (e.g., binary). In addition to the retransmission, there is cost in the delay to discover that the file is unusable

Importance of automation

Through the use of scripting, scheduling, and application integration, automation can ensure that proven business processes can continue to be successful by eliminating human error. With processes that require human interaction, errors and unintended activity can be introduced into a process flow. Many times such an error will not be discovered until much time has passed.

The costs associated with the lack of FTP automation include:

- Operations that complete successfully but are not usable since there is no way to validate user selected (or defaulted) options
- No central control of scheduled activities. Clients can initiate FTP activity regardless of its importance or impact on schedule

Total cost of operation and ownership

In order to quantify the overall cost associated with FTP operations, each of the following categories should be considered:

- Server Administrative Costs – Costs to administer the FTP servers, manage exceptions, and onboarding of new connections/partners
- Security/Risk Management Related Costs – Estimated costs to the company resulting from FTP usage and unencryption
- Facilities Related Operating Expenses – Costs associated with operating the datacenter (electricity and server space) and administering server downtime

For example, estimates for each of the previously identified areas are given below. This example is based on a file transfer network containing 100 FTP servers. It is based on experience within the Sterling Commerce trading community exchange, but this is just an example. The assumptions used for this example as well as a breakdown within each cost category can be found in the appendix.

The cost of FTP (100 servers)	
Server administrative costs	$676,487.53
Security/Risk management related costs	$241,062.50
Facility related operating expenses	$ 47,818.54
Total cost of ownership (1 year)	$965,368.57

What this example provides is a baseline from which you can derive the overall impact and costs associated with FTP. While FTP is easily attainable and free from a licensing perspective, this paper identifies the hidden cost categories all companies should consider when selecting the freeware. Don’t forget to ask yourself:

- How will FTP impact my server administrative costs? What could a breech potentially cost my company from a security and risk management perspective?
- What other facility related, inherent costs are associated with operating the additional servers?

The overall impact to each organization is unique, and the true cost of FTP can be estimated only by applying firsthand knowledge of the activity required to operate and manage it. If your company uses or is considering using FTP for data movement, use this example as a baseline for calculating your own total cost of ownership. Take those costs into consideration along with your other performance, management, and security requirements when deciding the best option for on-time, predictable, and secure data movement.

Appendix

FTP – Total cost of ownership example

Assumptions

Number of servers	100
Number of file transfer partners (connections)	3000
Number of transfers per partner (connection)	300
% of transfers that have exceptions	8%
Annual cost per IT staff (fully loaded)	$125,000
Per incident cost of data breach (Ponemon Study)	$6.65M

Server watts/system	280
Server operating hours per year	8736
$/kW-Hr (power)	$0.10
$/kW-Hr (cooling)	$0.05
$/ft2 (datacenter)	$21
ft2/server	1.2
Amount of TCO attributed to downtime	18% - 35%
Weekly overhead to manage FTP server by IT	1 hour

Annual costs for operating 100 FTP servers

Server administrative costs	
Managing exceptions	$355,393.78
Onboarding new connections	$8,593.75
FTP administration	$312,500.00
Subtotal – Administration cost savings	$676,487.53
Security/Risk management related costs	
Estimated risk from FTP usage	$124,687.50
Estimated risk from unencryption	$116,375.00
Subtotal – Security costs	$241,062.50
Facility related operating expenses	
Power	$24,460.80
Cooling	$12,230.40
Datacenter	$2,520.00
Downtime (20% of total Op Ex)	$8,607.34
Subtotal – Facilities costs	$47,818.54
Total cost of ownership	**$965,368.57**

About Sterling Commerce

Sterling Commerce, an IBM® Company, helps organizations worldwide increase business agility in their dynamic business network through innovative solutions for selling and fulfillment and for seamless and secure integration with customers, partners and suppliers. More information can be found at **www.sterlingcommerce.com.**

Sterling Commerce
An IBM Company

For all Sterling Commerce offices worldwide,
visit **www.sterlingcommerce.com**

SC0378 11/10