

# Realizing the benefits of FTP consolidation



How an edge gateway  
can deliver unexpected gains

# Table of Contents

|   |   |
|---|---|
| 3 | Introduction                            |
| 3 | Understanding the challenges            |
| 5 | Identifying opportunities at the edge   |
| 5 | Scalability                             |
| 6 | Rapid onboarding                        |
| 7 | Visibility                              |
| 8 | Bottom line results                     |
| 8 | Cost                                    |
| 8 | Security                                |
| 9 | Going for the benefits of edge gateways |
| 9 | Introducing Sterling File Gateway™      |

**Introduction**

Business organizations today are experiencing a growing demand to move high volumes of data both internally and externally. Accordingly, File Transfer Protocol (FTP) servers are proliferating among individual departments and raising traffic levels with customers and suppliers. As with all technologies that offer easy access to varieties of users, this has created problems as well as benefits. While vital information is flowing, security threats are also increasing dramatically, some of them malicious in the extreme, and the ad hoc nature of internal expansion means that it has become difficult not only to maintain security but to control necessary cost and quality factors.

In response, competitive businesses have identified FTP consolidation as a priority to minimize security risks, reduce costs, and gain better control of their own operations. But there is a larger opportunity at hand, one which can transform the defensive effort to solve file transfer problems into an offensive, strategic move toward vastly improved integration and business responsiveness throughout the business collaboration networks that link enterprises with their key partners.

Explaining and exploring that opportunity is the purpose of this white paper.

**Understanding the challenges**

FTP is not a system. It is a communication protocol that formats data so it can be transmitted and received. Setting up an application that uses FTP is remarkably easy, which is why it has spread through many organizations like the first personal computers did in the microprocessor revolution of the 1980s, creating many of the same kinds of problems. Back then, many IT organizations were caught off guard. Departments and users were suddenly using applications and data over which the technical professionals had no control and little ability to diagnose and prevent errors that could be damaging to the business. Now, just as there were "rogue PCs," there are "rogue FTP servers," which are using one limited and vulnerable tool to perform a huge variety of important, complex, and risky operations that are almost invisible to those who understand the dimensions of those risks.

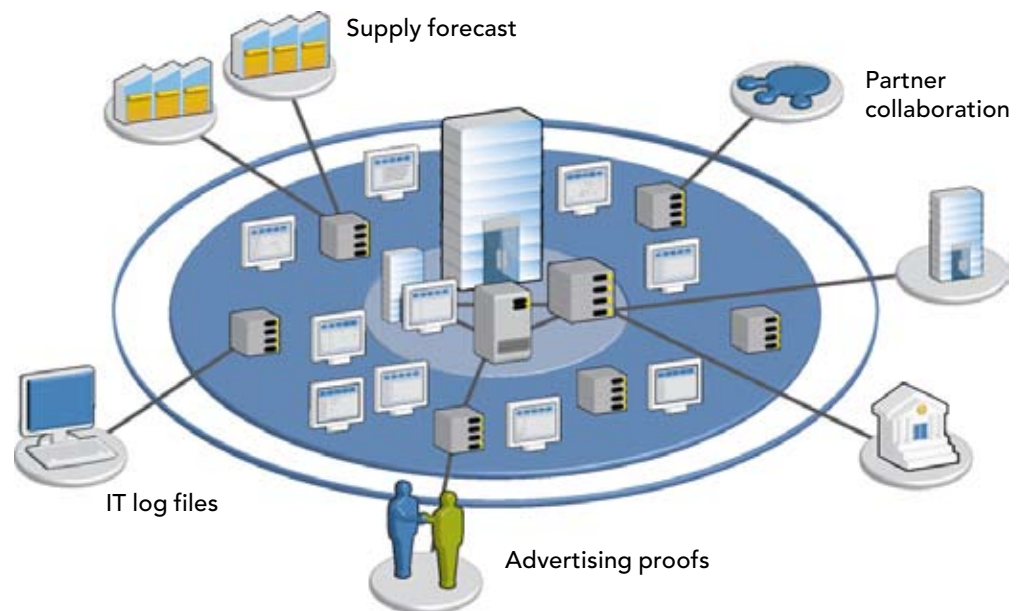
Typically, today's business organizations have multiple departmental FTP servers operating as "silos" throughout the enterprise (see Figure 1). FTP is being used to transmit back office information, including payroll, financial transactions, order administration, production, and other sensitive information. It's being used to convey different kinds of data as well, such as the large graphics-intensive files employed by marketing units. And it's also being used to handle, if not manage, vital business-to-business communications (for example supply chain files, forecasts, and more) with customers and suppliers, in environments in which there may be no visibility into security, as well as operating problems that could jeopardize the organization and the business processes that the files support.

The implications of such spontaneous proliferation of FTP servers are multiple and serious. Administering so many “silos” is time-consuming and difficult. Finding user problems and solving them, patching, and revising them to handle workload changes—all of these factor into the IT downside of keeping up with FTP. Furthermore, automating file transfers requires a good deal of manual scripting.

Maintaining a variety of separately sourced FTP applications is costly and inefficient. Moreover, the potential security liabilities are escalating all the time. There is the constant danger of accidental breaches caused by open text passwords (the rule more than the exception in end-user run organizations), and the unknown “open back door” threat of stolen FTP logins, which are actively hunted by amateur and professional hackers. The damage these can cause is virtually unlimited.

Clearly, there is a critical need, especially in today’s economy, to select the right solution for correcting present problems and preparing the organization for future growth with better control and substantially reduced risk.

Figure 1. Rogue FTP servers are pervasive



**Identifying opportunities at the edge**

Defining the challenge as “consolidating FTP” or “controlling FTP” is too narrow. Reducing the number of independently operating FTP processors does reduce costs and can improve data security. However, that’s not a complete business mission; it’s an IT objective, worthwhile but limited. The real mission—what FTP was procured for in the first place—is facilitating the flow of vital information with any and all security protections that may be required by any business partner or regulating entity. That’s a mission that can’t be fulfilled with a technical communication protocol, an add-on encryption product, or a log file monitor. It requires support for many protocols, encryption schemes, and document formats, as well as tie-ins to existing document management systems and databases. It represents a comprehensive systems approach that, because it is a systems approach, can also provide the flexibility and visibility needed to use such information flows as a strategic competitive advantage in business.

An edge gateway is a unified portal that stands between your enterprise and its external collaboration partners (See Figure 2). Internal departments who send and receive information are participating in an integrated communication network using common tools that automatically perform the necessary steps to format, secure, and route their data in the most efficient and traceable fashion. An edge gateway handles all the technical tasks, and the external recipients receive what they want and need without having to anticipate every detail of the sender’s environment. In essence, business users are no longer grappling with an isolated file transfer application; they are conducting and managing their business operations.

The benefits are manifold. Throughout the organization, collaborative transfers are simplified and automated to a very high degree. Yet because of the integration and unified system controls, communications are also much more visible. It’s easy to identify where and how failures might occur and either prevent them or rapidly fix them after the fact. This is a capability that ensures improved management of information flow and much tighter coordination with both suppliers and customers in the larger business collaboration network.

Even more important in strategic competitive terms are two additional benefits: scalability and rapid onboarding. We’ll take a closer look at these two system-level benefits, as well as the related benefit of visibility.

**Scalability**

Scalability refers to the system’s built-in support for growth and change. A scalable system has an architecture that can operate simply and easily in a small environment, yet accommodate rapid and complex kinds of growth in the volume and variety of communications, providing high performance to expanding numbers and types of users, while smoothly adapting to the increasing sophistication of security requirements.

There are several key variables that define optimum scalability. An edge gateway that can handle all these kinds of change must be designed from the start as an enterprise product, running the gamut from inside small, medium, or large businesses to outside the business-to-business networks. An edge gateway should support varied and dynamic user organizations through both vertical and horizontal clustering, which means that it should be easy to add virtual nodes on existing hardware and new physical nodes on added hardware. It must also provide failover protection; that is, a smooth, automatic transition to a redundant processor without data loss.

The purpose of all these architectural features is that the population of users consists of business people, not computer operators. Marketing professionals, cost accountants, and functional managers are not technical experts. If the system handles the tasks as it should, the system can grow very large indeed, to handle hundreds of thousands of files and users. This is the definition of a high-performance system.

The final key characteristic of scalability is support for changing customer requirements, which are typically industry or general technology needs. For example, it is now common for specific industries to require additional layers of encrypting, not just at the network level but at the payload level. These generally require new protocols to be added over time, and a truly scalable system will be able to incorporate such additions as they occur.

### **Rapid onboarding**

The term refers to the speed and ease with which it is possible to add new external partners to the collaboration network. The system's built-in support for many protocols, encryption schemes, and security provisions vastly reduces the effort required to integrate with trading partners, regardless of how small and unsophisticated, or how large and complex.

The key to rapid onboarding is very simple; it means not having to say "no." Whether a customer prefers SSL or FTP or SSH or IBM® Sterling Connect:Direct®, integrating that customer into your B2B network should be easily accomplished as seamlessly as possible.

Getting up to speed with new partners also means having the ability to identify problems and correct them during implementation and beyond, as well as handling specialized needs which can add value to the relationship. That's why another critical component of onboarding is a system attribute described more briefly earlier: visibility.

**Visibility**

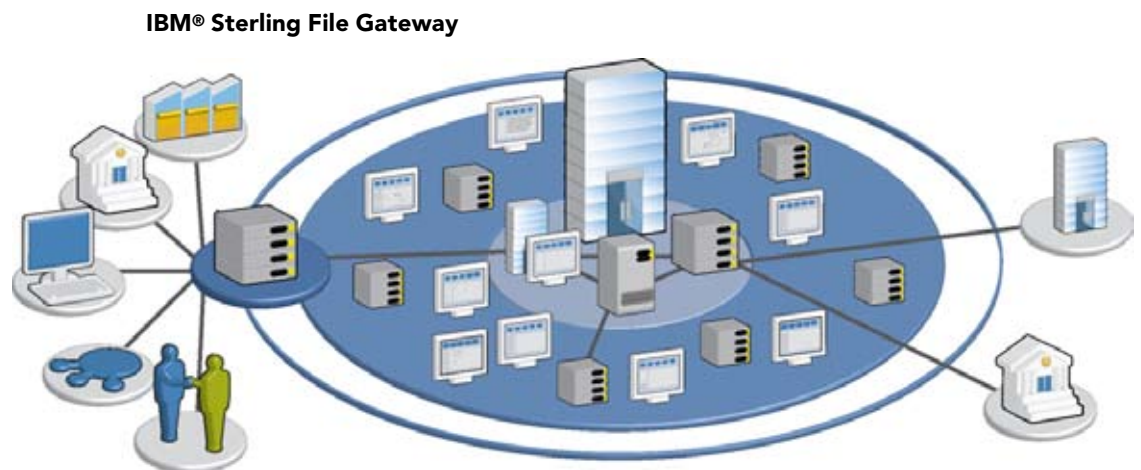
In the collaborative network that includes an enterprise and all its partners, incorporating suppliers and customers, visibility should address all communication transactions. Consider the following example:

A file comes out of a back-end system using one protocol, and one security system. The file is generated, it is passed to the gateway, and goes on to the trading partner. Next it has to be extracted, encrypted, or uncompressed or unencrypted, and maybe file names need to be changed. Perhaps a date/time stamp needs to be inserted into the file name. Perhaps the file needs to be opened because it contains critical information. Then the file has to be delivered to the customer, using a different protocol and encryption method.

With so many operations, it's always possible there will be a problem. When the trading partner calls and says "Where's my file?," visibility means being able to give the answer. This is information which can potentially save countless dollars for the transmitting organization. The ability to answer this question involves more than knowing where the file is in the system. It means knowing what happened to the file within the system, and even knowing what did not happen to the file, which makes it far easier to identify a problem source outside the system (for an expired security certificate) beyond your or the customer's control.

This kind of visibility is not just a protection of your performance with the partner. It can be a benefit of doing business with you that competitors cannot match. It becomes a competitive advantage.

Figure 2. Edge gateways have advantages



**Bottom line results**

There are opportunities in business. And there are requirements. Controlling the cost and security problems of rogue FTP servers has become a requirement. This white paper describes the benefits which might be achieved by enterprises that have the resources to invest in an offensive strategy in business communications. Yet, the economic climate today is challenging and difficult in the extreme.

Every business, however stressed, should be alert to the need for preventing the limitless downside to the proliferation of FTP servers in departments without the expertise to manage and control them properly. The two issues that make change an imperative in this area are cost and security.

**Cost**

When any business enterprise contains numerous FTP servers, it adds (and in some cases multiplies) the costs of IT resources required to keep them both operational and secure. The application programs, interfaces, and other technical requirements associated with departmental FTP communications may vary considerably, and it's always expensive when IT professionals have to react to situations after the fact.

The IT professionals become firefighters called into action when their proper role is as architects of smoothly-functioning facilities that cannot fall prey to accidents. The inevitable result of responding after the fact is wasted resources and, unfortunately, occasional business that is lost because of the second indispensable requirement—security.

**Security**

Ad-hoc computer implementations initiated and run by business people who are IT amateurs represent an open door to business competitors, amateur vandals, and professional thieves who have the power to do significant damage. Preventing this kind of potential security breach is not a risky investment in the future. It's a necessary insurance against disaster. It's the kind of disaster that's happening every day to businesses who never fully comprehended the risks. Loss of data. Theft of customer records. Open-ended liabilities that seem impossibly reckless risks only after the worst comes to pass.

All this can and must be prevented. The good news is that it's possible to turn this possibly limitless liability into a strategic competitive advantage at the same time, with exactly the same commitment to long-term business success.



## **Going for the benefits of edge gateways**

The discussion here has moved far beyond the gains to be achieved by consolidating decentralized FTP implementations within business organizations seeking cost, security and administrative improvements. These are worthy objectives on their own, of course, but there is a significantly greater opportunity to be derived.

For those willing to look farther down the road, an edge gateway approach opens the door to a host of business-level savings and performance improvements, including scalability, high performance business-to-business collaboration networks, rapid onboarding of new business, and the strategic advantage of end-to-end process visibility.

## **Introducing IBM Sterling File Gateway**

Our own edge gateway product is the IBM® Sterling File Gateway. Built on a Service Oriented Architecture (SOA) Sterling File Gateway is a component of our IBM® Sterling Managed File Transfer solution. Sterling File Gateway offers a feature-rich set of capabilities to manage the most demanding edge-based file transfer environments.

These include:

- Re-usable templates to facilitate trading partner onboarding
- A scaleable architecture for business growth and performance
- A self-service portal that offers users and IT real-time visibility of file transfer activity
- Support for all major communication and security protocols
- Intelligence driven file routing
- A business process framework for the setup and administration of process flows

Collectively, these capabilities allow companies to take complete control over all edge-based file transfer activity. Companies deploying Sterling File Gateway recognize an accelerated time to revenue, a lower cost of ownership and improved trading partner satisfaction.

## **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](http://www.sterlingcommerce.com).

**Sterling Commerce**  
An IBM Company

---

For all Sterling Commerce offices worldwide,  
visit [www.sterlingcommerce.com](http://www.sterlingcommerce.com)

©2009 – 2010, Sterling Commerce, Inc.  
All rights reserved. Sterling Commerce and the Sterling Commerce logo are trademarks of Sterling Commerce, Inc. or its affiliated companies. All products referenced are the service marks, trademarks, or registered marks of their respective owners. Printed in U.S.A.  
SC0760 11/10