Three significant risks of FTP use and how to overcome them

Management, security and automation

Contents:

1 Make sure your file transfer infrastructure keeps pace with your business strategy

1 The nature of business-critical data – and how you move it – is changing

2 Why FTP might be the biggest threat to your secure file transfer infrastructure

3 How to help ensure best practices for secure file transfer

4 You must bring management, security and control to your secure file infrastructure

Make sure your file transfer infrastructure keeps pace with your business strategy

Making sure your file transfer operations can meet evolving business requirements – today and in the future – is not an easy task. At a very minimum, you must ensure consistent enforcement of security policies, provide audit tracking to prove compliance, proactively monitor and manage data transfer operations to help meet service level agreements (SLAs), and evolve as your business needs change. Your file transfer infrastructure has likely become – or is becoming – a critical linchpin in your organization's business strategy. Does your file transfer infrastructure give you the visibility and control you need to meet these challenges?

Driven by converging trends over the last 10 years, many businesses are reevaluating which data is critical to their core operations and what processes they must implement to protect data that moves across their networks.

As you read further, these trends and how they're reshaping the way businesses think about critical data, will be examined. Further, key best practices that you can apply to ensure the secure and reliable transfer of data across your network, as well as with partners, suppliers and customers outside your corporate walls, will be outlined.

The nature of business-critical data – and how you move it – is changing

For businesses today, the definition of critical data is expanding rapidly. Business-critical data today is about what a company does – its intellectual property and research and development efforts. And it's about what a company knows – customer, partner and employee information. Business-critical data ranges from sensitive, identifiable personal information – such as Social Security and credit card numbers – to human resources information about employees, and even insurance claims.

In addition, more types of data are being digitized, and file sizes are increasing. For example, the Check 21 law in the United States allows banks to digitize checks for faster, more efficient processing. As more data is digitized, demand for access to it increases. And this means you must find ways to move more data, more efficiently and more securely.

With the increasing industrialization of the third world, your trading partner network is probably growing. And more partners, suppliers and customers outside your organization expect to exchange data with you via the Internet despite its notable security flaws. So, while you have more data and more data that's considered critical, you're also likely to move it to more places.

At the same time, your customers, government regulators and even business partners hold you accountable for data loss or theft. In response to some well-publicized security breaches and to the increasing ability of businesses to share information around the world, a growing body of government regulations – such as Sarbanes-Oxley, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Information Practice Act (also known as Senate Bill 1386) – mandate processes for securing data as well as for proving adherence to these standards through audit trails.

Why FTP might be the biggest threat to your secure file transfer infrastructure

File Transfer Protocol (FTP) likely started as a single tactical application. Then, because FTP was easy to use and its costs were perceived to be minimal, its use grew exponentially in many organizations. Yet the purportedly free operation of FTP comes at a high price. It has seen and unseen costs that result from its inherent management challenges, security risks and lack of automation.

Management challenges with FTP

The decentralized management, security and performance of FTP file transfer operations frequently mask the costs associated with interruptions, rework and security failures.

FTP provides no way to control critical file transfer operations or to balance critical transfers with lower-priority work. Both limitations can negatively impact processing windows and service level agreements. FTP places all control with the client, and "first-in" usually wins. Without a way to create an enforceable policy for workload execution – and without a means of controlling priorities and use based on business policies – critical file transfer is threatened.

Security risks with FTP

Open, uncontrolled use of FTP should be considered a serious exposure within the security policies of your organization. That's because security safeguards were not included in the original FTP model. As a result, there are numerous critical security issues.

In FTP sessions, the client must provide an ID and password when initiating a connection to the server, but this security information is transmitted in clear text. The ID and password must be valid on the server, which means that this private information must be distributed to all clients. If a client transmits to multiple servers, the client must have a valid ID and password for each.

Secure FTP does support full, session-level encryption via either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). However, enforcement of encryption during transmission is either left up to the client (explicit) or enforced by the server (implicit). In either case, there is no granularity and no audit trail. It is also possible for the client to be caught in a stand-off situation if the FTP server is configured for implicit security and the client either doesn't support secure FTP or attempts to enforce explicit security.

Security violations are not logged in FTP, and there is no authentication of the client.

Finally, the Computer Emergency Response Team (CERT) has documented hundreds of security issues with the use of FTP, many of which represent serious or catastrophic exposures. For example, using standard FTP commands, someone can create a denial of service situation or exploit known vulnerabilities within the FTP daemons to gain administrative or root access. And because the source code for many FTP implementations is freely available, additional new and creative security attacks are likely. In addition, the CERT advisories themselves represent a source of information that can be used by others in a malicious way to compromise system security through FTP.

Lack of automated operations with FTP

Any outage that occurs with FTP operations must first be discovered and then manually handled, which generally means restarting the failed operation from the beginning. Costs associated with FTP recovery include:

- **Retransmission** – On average, FTP retransmits half of the overall data volume per failure.
- **Delayed restart** – During network resource failure, FTP requires discovery of the failure, which can delay restart and incur additional costs.
- **Duplicate transmission** – Because of incorrect FTP option specifications, duplicate transmissions are a common occurrence. Many FTP transfers were retransmissions of files that resulted from an incorrect option selection. In addition to the cost of retransmission, there is also the cost associated with the delay of discovering that the file is unusable.

The lack of automation in FTP also prevents full utilization of organizational business processes. Costs associated with the lack of FTP automation derive from the following conditions:

- Operations may complete successfully, but the resulting files are not usable since there is no way to validate user-selected (or default) options.
- There is no central control of scheduled activities. Clients can initiate FTP activity regardless of the schedule impact or importance.

Some organizations have built their own automation using FTP commands. However, the costs for development and – especially – maintenance can be quite high.

How to help ensure best practices for secure file transfer

You can proactively counteract the security risks posed by such threats by establishing best practices for secure file transfer to protect your business data today and give you flexibility to adapt to changing requirements in the future:

- Assess your current secure file transfer infrastructure to ensure that it:
  - Permits appropriate security enforcement now and as security standards evolve.
  - Enables enforcement of security policies across your organization and with partners, suppliers and customers.
  - Allows your file transfer operations to fit naturally within the enterprise security policies you establish.
  - Provides support for higher security levels, such as proxy-based security, authentication and configurable encryption.
- Implement a standardized, repeatable process for secure file transfer that provides documentation and ongoing support.
- Provide a predictable and comprehensive end-to-end audit trail through detailed tracking and logging of all file transfer operations. FTP, for example, can only show bytes transferred and the transfer rate calculation from the client's perspective.

- Centralize visibility into every aspect of file transfer with easy-to-use reporting capabilities.
- Define service-level criteria to manage established SLAs.
  - Monitor for events and non-events. For example, failed or omitted file transfers might go unnoticed if you can't monitor for non-events.
  - Ensure the ability to proactively respond, diagnose and repair failures.
- Define and enforce a policy for workload execution.
  - Proactively manage the timing of critical data transfers.
  - Balance critical transfers with lower-priority work. For example, if you have short production windows, features like "checkpoint/restart" are critical when transferring files, especially when dealing with multi-gigabyte file sizes.
  - Balance fluctuating processing loads.
- Ensure that you can access a variety of systems – Windows, UNIX, Linux, mainframe and more – on a wide variety of networking protocols and standards.
- Establish a platform that allows you to grow to support higher volumes, more connections with more partners, and ever larger file sizes.

You must bring management, security and control to your secure file infrastructure

To remain viable in today's rapidly changing business environment, your secure file transfer infrastructure must bring management, security and control to all your file transfer operations. Free and widely available, FTP continues to be used in data transfer operations in many businesses. But to calculate the true cost of FTP, you must consider its inability to provide appropriate levels of security and enforcement of established security policies across your organization, its lack of full audit tracking capabilities to prove compliance, its inability to provide workload monitoring and management to ensure that you can meet service level agreements, and its lack of the flexibility necessary to scale as your business evolves.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
USA

Produced in the United States of America
October 2011

Please Recycle

ZZW03079-USEN-00