Secure File Transfer

Understanding and Selecting the Right Secure File Transfer Solution for your Organization

www.biscom.com

321 Billerica Road, Chelmsford, MA
phone: 978-250-1800
email: sales@biscom.com

Any investment in a security-centric application that involves sending confidential information outside an organization's borders must be vetted from both a business as well as a technology perspective. The goal of this document is to help educate both the business and technology decision makers by:

- Examining the challenge of sending and sharing large or confidential files with external parties
- Illustrating the benefits of a secure file transfer (SFT) solution
- Outlining the various aspects and implications of introducing SFT technology into an organization's existing processes and infrastructure
- Identifying key issues and questions that need to be addressed in order to maximize the advantage of a SFT deployment

OUTLINING THE PROBLEM

The increased need in today's global economy to transfer and collaborate on large files or sensitive documents with external individuals and groups has motivated users to demand better, more manageable file transfer solutions that are easy to use and that satisfy the increasing security concerns and regulatory requirements which many companies face. Healthcare, financial services, education, government agencies, and many other segments have stringent data delivery and sharing needs. Does your organization have a way to share sensitive information in a secure manner? If not, many users may be resorting to methods that are unsecure, incapable of being tracked, slow, expensive, or require significant IT time and attention. Email, FTP, peer-to-peer file sharing, and overnight services may not meet the security, data payload, speed, cost, and reporting requirements that companies call for.

BUSINESS BENEFITS OF SECURE FILE TRANSFER

Ideally, a SFT solution will require very little training, have minimal impact on existing user behavior, and operate transparently to speed the adoption of any new processes or policies. Identifying the groups and individuals who regularly interact with external parties (customers, partners, consultants, contractors, etc.) and who would benefit from a SFT solution is the first step in the requirements phase of selecting a SFT vendor. Understanding the types of files and documents that will be shared is a second step to ensure that the confidentiality and file sizes being transferred is supported by the SFT solution. Documents that include personal information such as social security numbers, financial data, and other confidential information can be sent safely and securely via SFT without the vulnerability inherent in email and FTP. And files that may exceed email attachments limits can be sent effectively through a SFT solution.

Above and beyond meeting security requirements, the business benefits of SFT include:

- Providing a self-service application for non-technical users
- Cost savings over other methods such as overnight deliveries
- Tracking and reporting capabilities for compliance and auditing purposes

TECHNOLOGY FIT

Any new system or process introduced into a company's technology infrastructure must work well with existing applications, support integration with legacy applications, adhere to existing security designs, scale to support small departments to large or organization-wide deployments, and leverage existing infrastructure when possible, such as virtualized environments, enterprise storage systems, and Web components already in place. When evaluating any technology, the emphasis should be on solutions that adapt to your existing infrastructure, and not on applications that require significant systems re-architecture and design modifications to meet the application's requirements.

Secure file transfer applications can be broken down into five main categories which are addressed below:

- Security
- Architecture
- Features and ease of use
- Reporting
- Licensing and total cost of ownership

SECURITY

Because data exiting an organization's boundaries may contain sensitive or confidential information, locking down this data and being able to identify and ensure that only intended recipients actually receive the information should be considered critical criteria. A security assessment involves multiple views into a product, including the overall architecture, storage and protection of data, user authentication, how permissions and roles are handled, policies that administrators can define, and even how well an application can be supported on the underlying platform and existing security configuration.

Questions to ask about a solution's security:

- How is data secured while at rest (i.e., on disk)?
- How is data secured while being transmitted (i.e., over public networks like the Internet)?

- Is data encryption a standards-based algorithm (e.g., AES)?
- Are there key management utilities to manage the encryption?
- How is user authentication handled?
- Can specific collections of files be password protected?
- Can you restrict specific domains or recipients from accessing the system?
- Can you restrict certain file types from being delivered?
- Can you define user quotas?
- Can you set user expiration?
- Can you define password strength requirements?
- Can you define retention policies for deliveries?

ARCHITECTURE

A solution's overall architecture and design approach can tell a significant amount about the planning and forethought a vendor has put in their product. Good product developers build for today's needs, but design in anticipation of tomorrow's requirements. When reviewing any secure file transfer architecture, note how the vendor addresses encryption, flexibility, scalability, support for extremely large files, network interruptions, policies, ease of integration and extension of existing applications, customizability, performance, user and system administration, platform support, and programmatic interfaces (APIs) into the product. Is the application designed logically? Do components fit well with each other? Will the application fit into your existing infrastructure?

Questions to ask about a solution's architecture:

- Does the application integrate with my directory service (e.g. LDAP, Active Directory)?
- Does it support at least three tiers to separate the presentation layer, the application logic, and the data?
- Does it run on my platform (e.g., Windows, Linux, Solaris)?
- Does it support a heterogeneous or mixed computing environment?
- Does the product run on my existing hardware or does it need specialized hardware?
- Can the application be load balanced?
- Does the application allow me to leverage my existing investments in storage, Web technologies, and application servers?
- Does the application run in a virtual environment? (And, are there any artificial governors that might not leverage the underlying compute power?)
- Does it support a services oriented architecture (SOA)?

- Is an API available that works with my applications, preferably a Web services-based, language neutral API?
- Can the application be scripted?

FEATURES AND EASE OF USE

A well thought out user interface is critical to the successful and effective adoption of any technology. The less intrusive and overbearing a system, the more likely it will be used. This applies to both the internal senders as well as the external recipients. Important elements in a highly usable interface include clean and uncluttered screens, intuitive controls, thoughtful and meaningful text, and overall consistency in look and feel. This directly affects adoption, and the tools easiest to use will most likely receive the most acceptance from end users:

- Does it integrate with email clients like Microsoft Outlook?
- Are prompts customizable?
- Is the look and feel customizable?
- Can the application be branded?
- Does the application support internationalization and localization?
- Are time-saving features, such as auto-complete and drag-and-drop supported?
- Is special client software needed to receive files or is a ubiquitous Web-based application available?

ADMINISTRATION

A well thought out user interface is critical to the successful and effective adoption of any technology. The less Two major aspects of administering a SFT solution are user management and system configuration. Some user management imperatives to keep in mind are: minimize duplication of information (e.g. multiple user databases), leverage existing identity and access management databases, and automate when possible to have the SFT system run without constant IT intervention. System configuration and default settings enable companies to more closely match and support existing policies and procedures:

- Is there support for using existing directory services such as LDAP and Microsoft Active Directory?
- Can user registration assign default roles and permissions, and is it domain sensitive?
- Can it handle the occasional versus regular user?
- Is there granularity to configure users globally as well as individually or in groups?
- Is system administration accessible remotely (e.g. through a Web interface)?
- Are there multiple administration levels (i.e. user manager, system administrator, and super user)?

REPORTING

Once a SFT solution is in place, reporting becomes an important tool in understanding adoption, utilization, trends, and auditing support. Compliance requirements may require report generation to satisfy state and federal regulations or to meet internal usage guidelines and corporate governance:

- Can you determine which users are the most active?
- Can you determine which files have been downloaded?
- Can you determine which deliveries and files are the most popular?
- Can you determine bandwidth used?
- Can you search and filter transactions to reduce the data set?
- Are transactions tracked granularly enough?
- Can reports be exported?
- Can a compliance officer perform regular or impromptu checks?
- Can reports be automated and emailed out?

LICENSING AND TOTAL COST OF OWNERSHIP

Adding SFT to an organization's toolbox gives users new options to send sensitive files and data through a secure channel. While this functionality may fill the immediate needs of certain individuals or departments initially, the SFT implementations often grow organically. Ideally, SFT would be accessible to every individual in an organization, but budgetary constraints may limit usage to satisfy the most affected individuals and groups. Different licensing approaches exist but look for the most cost effective ones that don't penalize you for growing or scaling the solution as adoption and demand grow. Also, from a financial standpoint, total cost of ownership should be calculated over a number of years to better compare vendor offerings:

- Is licensing annual or perpetual? What is total cost of ownership over 2-5 years?
- What kind of upgrade policy exists? Will you get full credit for your existing users?
- If the solution is hardware-based, how are components upgraded? What happens if you exceed the system capacity?
- Are features and modules purchased à la carte or bundled and all inclusive?
- Are upgrades included in the support agreement?
- Are there licensing costs associated with recipients or infrequent users?
- For hardware-based solutions and appliances, what are the costs for upgrading or scaling beyond capacity?

FREQUENTLY ASKED QUESTIONS

Q: I already have a secure email solution in place? Why do I need a secure file transfer solution?

A: SFT complements secure email in many ways – secure email solutions often have the same limitations that standard email servers have – that is, there may be limitations on the size and file type of attachments. The capability to re-route large or sensitive file attachments through a SFT solution maintains the security requirements, but also enables content sharing that was not available through email. Also, if your SFT solution integrates with your email client, sending large files is seamless.

Q: My FTP server seems to be running fine. Isn't that sufficient?

A: File transfer protocol (FTP) was developed in the early 1970s when security concerns and usability were less important than getting data from one place to another. Most end users were Department of Defense or university researchers exchanging data across a very limited network and user population, and may not have minded sending clear text passwords. FTP hasn't changed much in over 30 years which is a testament to the original design, but today's world has new concerns and requirements that didn't exist back then. Security, ease of use for the less technical users, and reporting requirements have made FTP a less-than- ideal solution for many people. The administration and IT involvement needed to send a file is a manual, tedious, and error-prone process. If not set up correctly, people may have access to files that were not intended for them.

Q: What's so important about scalability?

A: Scalability is important for any application because small deployments often grow and large deployments grow even more. Scalability, or the inability to scale, depends on several factors, such as a well-designed architecture, modular coding, standards-based component support, well-defined APIs, and platform neutrality. Support for load balancing becomes important when deployments grow beyond the departmental level, for both performance and availability reasons. Look for solutions that were designed from the ground up to be enterprise solutions.

Q: What are the differences between hardware-based and software-based solutions?

A: Some SFT vendors are appliance-based solutions and others are software-only solutions. Appliances are useful in situations when deployed at network edges, such as a firewall or network switch, but because potentially sensitive data is being stored and transferred through a SFT application, software solutions are often more flexible and secure. For external facing applications, such as SFT, placing an appliance in a public-accessible location such as the DMZ potentially exposes corporate data to the world. Hackers are constantly exploiting vulnerabilities, and patches are usually one or two steps behind most intrusions; any system that has openings to the public Internet is susceptible to being attacked, and there is significant potential for your data to be accessed.

Software solutions, especially those that support multiple tiers, can simply expose the presentation layer in the DMZ without compromising sensitive data, which can be stored (and encrypted ideally) in a more secure part of an organization's private network. Also, since most IT departments have standardized hardware and operating systems, software that runs on supported platforms is easier to install and maintain. And security patches can be applied globally as the rule rather than exception-based patching for unique hardware systems.

Hardware-based solutions also face the inherent risk of obsolescence. The pace of CPU advances and a declining price/performance ratio means hardware becomes outdated even more quickly today than in years past. Proprietary appliances may be harder and more expensive to upgrade than standard servers, and if increased user demands require scaling, you may be forced to replace the appliance hardware rather than go a more cost-effective upgrade route.

Q: Why should I consider buying a solution when I can build one myself?
A: Many companies can provide similar functionality by putting together their own FTP server and develop custom software and scripts to facilitate usage. For very small companies, this might be a feasible endeavor. But some questions you must ask are:

- Is software development or developing secure file transfer solutions your core business?
- How long will it take to build this system? Who will build it? While they're building the system, what other job functions and responsibilities are being pushed off or forgotten?
- Do you want to dedicate precious IT or development resources to maintaining and supporting a home-grown solution?
- Has it been tested and deployed in large production environments?
- Does it provide adequate tracking, and can you easily generate activity reports for audits?
- Will you see new features and functionality at regular intervals?
- Will the person writing the software and scripts and maintaining the system be around for the long haul? Will he or she be able to fix any bugs in a timely manner?
- Will the system scale to handle more users or increased load?
- How much will it cost you in people, time, and resources to build and maintain this system?

ABOUT BISCOM DELIVERY SERVER

Biscom Secure File Transfer (SFT) is an enterprise managed file transfer (MFT) solution that enables users to send files, documents, and messages securely while maintaining a complete transaction and audit trail. SFT provides you with all you need to manage large file transfers and comply with increasingly strict state and federal regulations, all in an easy-to-use package that ensures widespread adoption by employees, customers, partners, and others.

ABOUT BISCOM

Biscom was founded in 1986 and pioneered the fax server marketplace, providing many of the world's largest organizations with its award-winning FAXCOM fax servers. In addition to enterprise fax server products, Biscom also offers hosted fax services, secure file transfer and messaging solutions, file conversion software, and document workflow and automation tools. The company is headquartered in Chelmsford, Massachusetts.

CONTACTS

- Visit www.biscom.com
- Call 800-477-2472. Ask for a SFT representative
- Send an email to sales@biscom.com