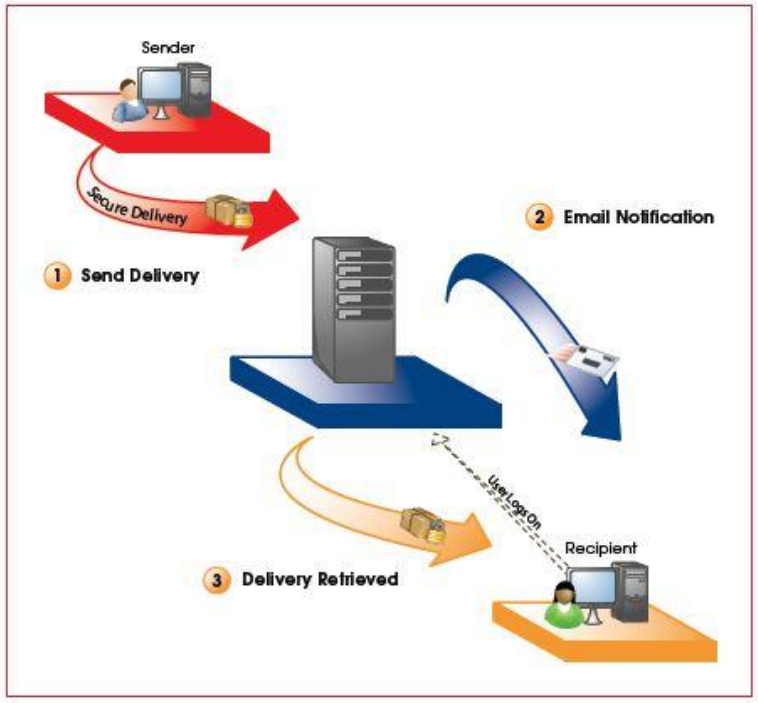
Top 10 Questions to Ask when Choosing a Secure File Transfer Solution

Companies that have made an investment in a Secure File Transfer (SFT) solution have discovered how it can become a central component of their communications and network infrastructure. Asking the right questions before investing in an SFT solution can help ensure you choose one that can handle both your immediate needs and future requirements.

BISCOM

Transferring, securing and collaborating on large files and documents in today's business environment has led users to demand that IT departments provide better file transfer methods than the traditional ones: FTP, email, physical media, and courier services. In response to such demands, IT staffs are looking for SFT solutions that fit into their current IT infrastructure and have built-in scalability to support a growing user population.

Secure File Transfer (SFT), also known as Managed File Transfer (MFT), helps people send electronic files and documents to other people easily and with confidence. The increasingly digital nature of documents, media, and messaging requires better, faster, and easier ways to deliver these electronic files. As file sizes increase, security concerns intensify, and pressure from users to have an easy-to-use application rises, secure file transfer becomes a high priority need. The media has reported on several high profile companies that have lost important data or sensitive customer information. These reports have detailed the hard costs associated with a data breach: identifying and notifying affected parties, resolving the breach, monetary fines, implementing a SFT or MFT solution, and legal fees, not to mention negative publicity and a harm to the brand.



Secure File Transfer

1. Why is secure file transfer becoming so important?

Data, documents, multimedia files, software, and other digital files are getting bigger. Users who were satisfied with eighty gigabyte hard drives a few years ago now need half-terabyte drives or larger. The introduction of iTunes, video, eBooks, and other traditional media are taking up larger portions of hard drives. Transferring these bigger and more numerous files is becoming a major issue – how are large files delivered? Will people be able to easily retrieve the files? Do the files need to be sent securely?

The two primary complaints about sending large files are of users having technical problems with complex software clients, and inadequate tracking of the success or failure of the delivery. Current methods for delivering files, such as FTP, email, and burning a DVD to send in the mail, have serious drawbacks and limitations. Today's users want a tool that is simple to use, provides needed security, and has the real-time notification and reporting that enables them to track the progress of their deliveries.

2. What's wrong with sending email?

Email is a great way to send messages and small files quickly and easily. Email does have many limitations, however. From a security standpoint, email is equivalent to sending a postcard in the mail – if you don't care who sees the contents of your message, email is a great solution. If your attachments have low potential for being rejected as too large or a restricted file type, then email works well in this case also.

Email administrators are constantly battling larger mail stores, viruses, and spam, and are implementing increasingly strict protocols that block many messages based on content, attachment size, and attachment

© Biscom Inc. All rights reserved. SFT is a trademark of Biscom Inc. All other registered trademarks are property of their respective owners. Specifications subject to change without notice.

type. Many companies impose five megabyte attachment limits, restrict compressed, executable, and script-based attachments, and use aggressive content filters. These restrictions result in problems with sending and receiving legitimate messages and files. In many cases, senders do not realize their intended recipients have not received their message.

3. *What about FTP or burning a CD or DVD?*

FTP has been around for over thirty years – one of the first protocols available to transfer files. It was designed when security, automation, and management were not pressing requirements. As a mostly free server application, FTP is used by many companies and organizations. In today's world, however, data management, security/access control, and automation are important. Whether it's clear text passwords, painful user management and permissions, unsecure transmission, or unintentional access to others' files, FTP has numerous security issues.

Delivering large files by burning them to physical media, such as a CD or DVD, and mailing them requires time, equipment, and know-how. The sender needs access to CD or DVD burning hardware and software, some level of technical knowledge, and time to write the disc, package it up, address the envelope, and mail it out. Physical delivery is slow, cannot be tracked in real time, and the package can be lost in transit.

4. *Is it easy to use?*

Technology and applications that are hard to use won't get used – that's a big complaint from the business and operations groups who must use applications for compliance or other policies required for secure data transmission. For people who are used to sending emails to anyone in the world with a few clicks of a mouse, adding complexity to this task can inhibit use. Ensuring proper usage means making sure the application's user interface is simple and easy to understand, and also meets the requirements for security and tracking.

5. *How should data be secured?*

When looking at secure file transfer products, it is important to evaluate how their deployment can affect security. A model proven to be secure is a multi-tier architecture that supports separation of the presentation layer, business logic, and data layer. With such a separation, the presentation and business logic layers do not contain any user data. Since the presentation layer is often placed in the demilitarized zone or DMZ in order to provide wide access, it is necessarily exposed to unwanted admission. Users interact with the presentation layer, making requests that are passed from the presentation layer back to the business logic layer. The business logic layer enforces the parameters around valid usage, such as validating data before storing it, controlling user access, tracking transactions, reporting, and managing and allocating back end resources. Once the request and associated data is deemed authentic, the business logic layer can pass the information to the data layer or to other protected resource and information management systems. Each layer should thus be deployed in progressively more secure areas of your network, utilizing firewalls, IP, port, user, and protocol restrictions. All communication between the application and the end user should be done over an encrypted channel such as SSL or TLS.

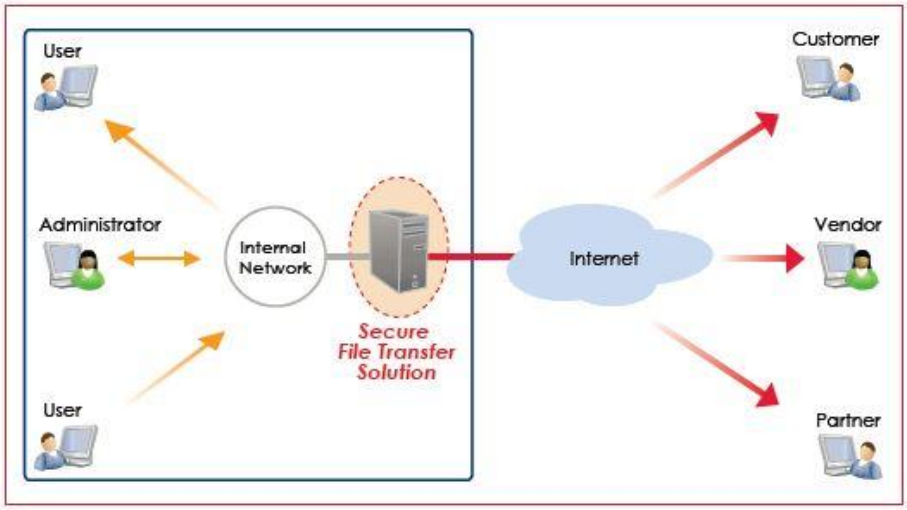
6. *Can I easily deploy it to a large number of users?*

Managing a large number of users can be tedious, and if you have to manage those users through multiple mutually exclusive interfaces, it can be very tiresome. LDAP and Active Directory are popular directory services that simplify and centralize user management and access to resources. Accordingly, any SFT applications should support directory services to consolidate management tasks.

© Biscom Inc. All rights reserved. SFT is a trademark of Biscom Inc. All other registered trademarks are property of their respective owners. Specifications subject to change without notice.

7. *Can it integrate with my network, other applications, and legacy systems?*

Companies fall into two categories – homogeneous, or heterogeneous, operating environments, where a homogeneous environment is typically Windows or Unix/Linux. An SFT application should be comfortable fitting into single as well as mixed-mode environments for front end and back end application components. Having an application that can run on multiple hardware and operating systems is even better, as it gives IT managers the flexibility to deal with any shift in the technology stack and run applications on hardware and software they are most familiar with.



Secure File Transfer Workflow

Web-based technologies that support HTTP and Web services is a must-have these days. The ubiquity of Web access through browsers almost guarantees your files can be accessed by practically anyone without any special client software.

Once an SFT application is deployed, leveraging it for use with other applications or legacy systems can speed up your return on investment. Open standards-based APIs that are platform and language neutral allow integration with a diverse application pool – standardized communications is achievable when there is no proprietary or language-specific interface. APIs enable developers to build business applications without having to worry about the implementation details of file transfer, security, user management, and storage.

8. *What else should I consider before implementing a secure file transfer system?*

Scalability is a critical feature of any production file transfer system. What works today may not be adequate for future needs. Being able to scale up the application to handle additional users, storage requirements, and bandwidth seamlessly is a must, and particularly important when initial load and usage estimates may be too low. Savvy buyers want to pay only for what they need and look for a cost effective upgrade path. If you've bought into proprietary hardware, or a system that your IT department doesn't normally support, expect to invest in additional training, make more support calls, and spend more time deploying and maintaining the product. Using familiar hardware and operating systems you already know how to support enables you to upgrade the components and performance on your schedule, as you see fit.

9. *What about building this system on my own?*

The build-versus-buy decision is a frequently asked question. The standard response usually references the primary business of the company – is file delivery the primary business or simply part of the business process? More questions than answers usually ensue – who is developing the application? Is it his or her primary job at the company? How long will it take the person to develop the application and have it running in production? Will it scale to handle my entire organization? How easy is the system to administer? How configurable and customizable is the application? Has the software gone through a rigorous QA cycle? Is there documentation?

© Biscom Inc. All rights reserved. SFT is a trademark of Biscom Inc. All other registered trademarks are property of their respective owners. Specifications subject to change without notice.

How often is the software updated with new features? How long does it take to get something fixed? What happens if that person leaves the company? Ultimately, are the time and resources needed going to be more or less than buying a purpose-built solution?

10. How experienced/credible is the company that developed the product, and how does the company support the product?

For experienced buyers, confidence in the vendor is common sense. How long has the vendor been in business? How many customers do they support? Do they have experience working with and supporting enterprise accounts with mission critical applications? Will they continue to support the product? How will I be treated after I buy the product? Are they responsive to suggestions and feature requests? Having a good relationship with your vendor, and being comfortable with their post-sales support, is key to choosing the right product.

While you may have already considered many of these questions in your search for a Secure File Transfer solution, it is hoped that raising and answering them here has helped you focus your inquiry. In addition, there may be additional questions specific to your particular industry/market segment, the answers to which can help you make sure you choose the right SFT product. Because many companies who have acquired an SFT solution for a single use have come to see it can meet multiple business communication needs, it's more important than ever that the solution be one that can handle your immediate, as well as future, requirements.

Need More Information?

To learn more about Biscom secure file transfer please contact us at:

Toll Free: 800-477-2472
Email: sales@biscom.com
Web:www.biscom.com/secure-file-transer/sft

© Biscom Inc. All rights reserved. SFT is a trademark of Biscom Inc. All other registered trademarks are property of their respective owners. Specifications subject to change without notice.