White Paper

Solving E-Mail Attachment and FTP Challenges with Managed File Transfer

BluePoint Associates

www.bluept.org • 978-993-4403

.

Solving E-Mail Attachment and FTP Challenges with Managed File Transfer

The problem of transferring files from one place to another is one that continues to plague both IT and the company. Issues around file transfer are not new to IT, but the sheer volume of business conducted over the network and the increasing number of corporate users who transfer information as a regular part of their work places new emphasis on monitoring and controlling the methods used to transfer files. The simple process of transferring a file from one user to another can have a profound impact on IT resources and the infrastructure. It may also have an impact on the company in the form of lost data or by compromising the company's intellectual property.

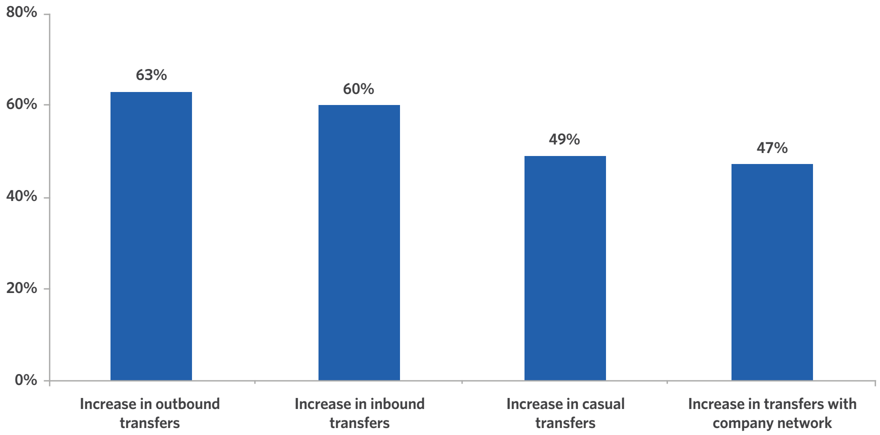
This paper will examine some of the methods currently used to transfer files and detail the issues they present both for IT and for the company. It will present the case for a managed file transfer solution, one that is easy to use, integrates with email clients and applications found on the end user's desktop, and which provides IT and the organization with the security and accountability needed in today's business climate.

Business Context

Who transfers files over the network? The answer is: almost everyone in the organization—though end users may not think of them as "files", but rather as PDFs, documents, presentations, pictures, MP3s, videos, and so on. Since email became the ubiquitous desktop application, perhaps rivaled only by the Internet browser, most end users employ email as a way of moving files from sender to recipient.

How big a problem does this create for IT? Research conducted by Osterman Research showed that a typical corporate user sends and receives an average of 44,700 emails per year, 29% of which have file attachments. The number of files transferred both within and outside the company network is increasing according to the Aberdeen Group (see Figure 1). Note that the percentages for inbound (63%) and outbound (60%) are nearly identical.

Figure 1: Companies report increasing use of file transfers.



IT administrators are well aware of the demands placed on the network and the mail infrastructure. Email attachments not only affect network performance, they also consume large amounts of storage.

This was not always the case. The venerable FTP (file transfer protocol) was the preferred method of moving files from one place to another. FTP was invented nearly 40 years ago as a way to move files from a client computer to a server across a LAN. When it was designed, FTP had no notion of an "internetwork" or of the need for security, as it was correctly assumed that the local network wouldn't be connected to the outside world (the technology existed, but only for the military).

As a network service, FTP was designed to be used by system administrators, not end users, and so it had a rather terse command line interface. More recent versions have added a graphical interface, but FTP is not a file transfer method designed for the casual computer user. Other problems with FTP include:

- Most users need to be trained in how to use FTP, whether they are sending or receiving a file.
- The recipient's computer or a local server has to be running the FTP service in order to establish a connection with the sender's computer.
- Once the files are delivered, they must be explicitly deleted by the recipient or by the sender.

All of these issues involve the participation of IT, for training, help desk support, or file maintenance. It's no wonder, then, that email has become the most widely used method of transferring files – the simplicity of attaching a file to an email and pressing "send" means that even a casual computer user can send files.

The Problems with Email

Attaching files to emails is convenient for the sender and the recipient, but its use in a corporate setting creates a number of IT problems which most end users never see. A sender might see an email with a large attachment bounced back by the local email server because of file size limits within the mail server itself – many companies won't allow files larger than 4 megabytes to pass through the mail infrastructure, simply because of the impact on overall performance. Remember we're not talking about one email with an attachment – depending on the size of the company we could be talking about hundreds or thousands of attachments per day. If the attachment arrives at the recipient's mailbox then it has to be stored either on that user's computer or on an email server, but even if the attachment never gets delivered, it still consumes storage for the sender.

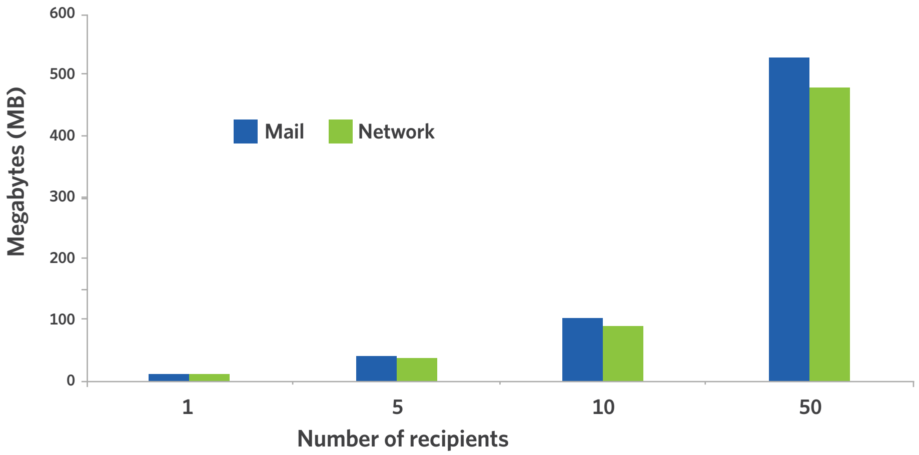
Even if an email with a 10 megabyte attachment gets through the outbound server, it still has to travel through the Internet and arrive at the recipient's email server, which may also impose restrictions on incoming file attachments. If the attachment is too large, the recipient's email server may send an error message back to the send, but more often than not, the mail and the attachment just "disappear" – they are disposed of by the incoming mail server.

IT administrators are well aware of the demands placed on the network and the mail infrastructure. Email attachments not only affect network performance, they also consume large amounts of storage. Nearly all attachments are stored along with the email in the mail server's data store.

A typical email user generates some 44,700 emails per year, 29% of which have files attached and 19% of these attachments are 5 megabytes or greater in size.

Figure 2 shows the effect on network performance and storage requirements as the number of recipients for a single email with an attachment increases. This is because a copy of the email and the attachment are stored for every recipient, either on the mail server's data store or a local drive depending on how mail is configured.

Figure 2: The multiplicative effect of email attachments.



This example only depicts the effect of one email attachment sent to multiple recipients. Depending on the size of the company there could be hundreds or even thousands of attachments being sent every day. As we noted earlier, a typical email user generates some 44,700 emails per year, 29% of which have files attached and 19% of these attachments are 5 megabytes or greater in size. Using these numbers as a starting point, the number of email mailboxes in an organization has a substantial effect on infrastructure resources (see Table 1).

Table 1: An example of how email attachments consume infrastructure resources.

Number of users	Average messages per year	29% with attachments	19% with attachments >= 5MB	Storage consumed by attachments
1	44,700	12,963	2,463	12.3 GB
10	447,700	129,630	24,630	123.1 GB
50	2,235,000	648,150	123,149	615.7 GB
100	4,470,000	1,296,300	246,297	1.2 TB
500	22,350,000	6,481,500	1,231.485	6.2 TB

Source: Osterman Research, Inc, 2008

If we use the storage consumed for the number of mailboxes from Table 1 and combine that with the number of recipients, the amount of resources consumed grows even larger (see Figure 2).

The amount of resources may differ according the kind of emails being sent – document attachments would consumer far less resources than video attachments, for example – but even in mid-size organizations, staying ahead of the demand for email resources is difficult and consumes IT effort and time.

The pervasive use of the network for nearly every business process has accelerated the speed and efficiency with which businesses conduct daily business, but this same networking capability has exposed companies to greater risk.

Table 2: The effect of combining attachments with the number of recipients.

Number of users	Number of Recipients			
	5	10	20	50
1	61.6 GB	121.3 GB	246.3 GB	615.7 GB
10	615.7 GB	1.2 TB	2.5 TB	6.2 TB
50	3.1 TB	6.2 TB	12.3 TB	30.8 TB
100	6.2 TB	12.3 TB	24.6 TB	61.6 TB
500	30.8 TB	61.6 TB	123.1 TB	307.9 TB

Another issue that troubles IT departments is that there isn't an easy way to manage the problem of email attachments. By its nature, email use is unscheduled and casual. Demand for email may follow the same patterns as overall computer use, with heavier demand at the start and the end of the working day, but otherwise is mostly unpredictable. As with the demand for storage, the use of email continues to grow.

Security and Governance

The security of company computing resources, networks, and intellectual property is an ongoing concern for organizations of all sizes. IT regularly invests heavily in hardware and software to prevent all manner of viruses, malware, root kits, and spam from penetrating company firewalls. As it happens, attachments to email or the email themselves may contain links or executables that can spread easily once inside the network. Even the corporate use of anti-virus and malware detection software doesn't preclude malicious intent— in all likelihood, if someone you know sends you an email with an important contract attached or pictures of their recent vacation, chances are good you'll open the attachment. The pervasive use of the network for nearly every business process has accelerated the speed and efficiency with which businesses conduct daily business, but this same networking capability has exposed companies to greater risk. According to the Aberdeen Group, companies report that not only employees, but also other groups outside of the company have increasing access to company data (Figure 3).

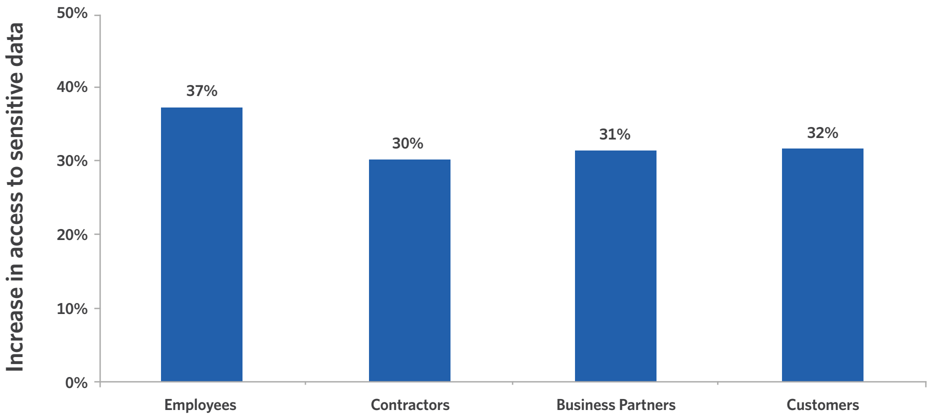


Figure 3: Companies report increasing access to sensitive data..

The network is not the only problem. As we noted earlier, FTP presents a usability challenge for most users and corporate email servers usually impose limits on the size of attachments, so employees may turn to other solutions to get their jobs done, including:

- alternate email services such as Hotmail or Gmail,
- removable devices such as thumb drives, memory sticks, and even iPods, or
- removable media such as CD-R, or DVD-R.

These solutions present problems for both the company and IT. It's unlikely that the files put onto a thumb drive or CD have been encrypted, which exposes the company to the risk of data loss or intellectual property theft. And unless the media is delivered by hand, moving the media to its destination incurs additional expense through delivery by Federal Express, UPS, or a courier service. Most of these ad hoc file transfers occur without IT's knowledge or consent. Unless the company uses some kind of device management solution that monitors or prevents the use of removable media, there isn't any easy way for IT to audit the movement of files.

In additional to the risk posed by data or intellectual property loss, companies have increasing exposure to legal discovery. The 2006 Federal Rules for Civil Procedure (FRCP) hold companies liable for providing documents or emails in response to a legal discovery request and can impose large penalties for failing to provide this information in a timely fashion. Companies that use email as the primary way of distributing files to customers and partners are doubly at risk, unless they have the means to trace email distributions and to find all of the email and documents relating to the legal matter.

Companies that use email as the primary way of distributing files to customers and partners are doubly at risk, unless they have the means to trace email distributions and to find all of the email and documents relating to the legal matter.

Many companies also need to comply with the Health Insurance Portability and Accountability Act (HIPAA) or with Sarbanes-Oxley (SOX). Insecure and unencrypted transfer of medical information, such as through an email system, exposes companies to the risk of lawsuits or regulatory penalties for violating HIPAA regulations.
The inability to provide auditable financial systems under SOX regulations can also put many companies of all sizes at risk of regulatory action, especially when traditional email and file transfer methods don't provide encryption or a high degree of security.

IT Infrastructure Cost

Cost is almost always a primary concern of IT. Cost was the predominant factor driving IT decision-making in a series of surveys conducted by the author at the Aberdeen Group in 2008 on a diverse set of IT topics ranging from disaster recovery to virtualization to green IT. Larger companies tend to be more sophisticated in budgeting for and allocating costs, but even small companies need to understand the sources and components of infrastructure— as the axiom goes: "you can't manage what you can't measure."

As we noted in earlier sections, transferring files is an activity that is both difficult to measure and to manage because of its unpredictable, ad hoc nature. It requires not only physical infrastructure resources in the form of storage and network bandwidth, but also administrative resources to manage email servers, storage systems, and to provide help desk support to end users.

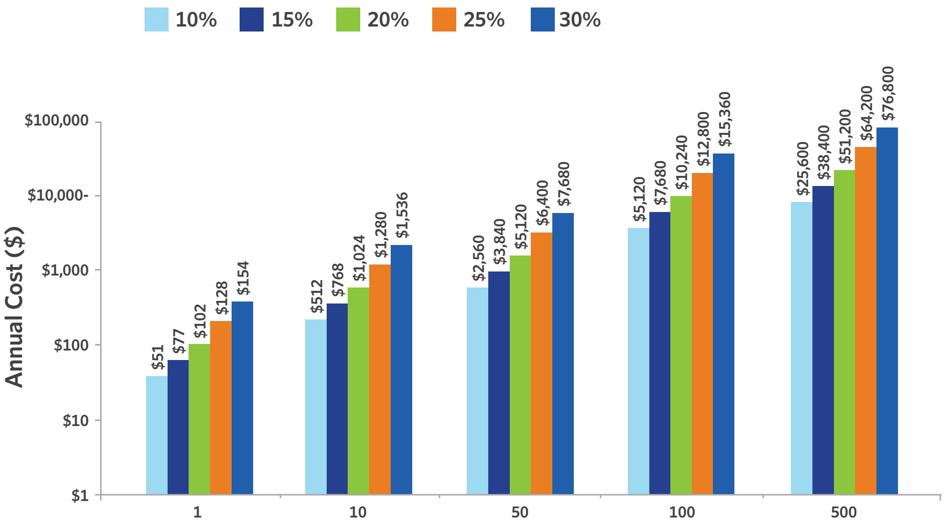
The actual cost of transferring files is difficult to determine, since it is comprised of some portion of the infrastructure resources consumed and the administrative time needed to train end users, manage servers, network and storage. In addition, the cost will vary widely based on what methods of file transfer are used, number of users engaged in the transferring files, and so on.

As an example, consider the infrastructure costs of maintaining an FTP server (or in a large organization, servers). These costs would include the server hardware, dedicated storage, administrative and operations costs, and some portion of the data center costs for power, cooling, floor space, and so on. It would also include the network bandwidth required to move data to and from the FTP infrastructure. At one company of 7,000 employees it was estimated that the monthly FTP costs were more than $14,000 per month.

Even at a small percentage, handling file attachments through emails can be an expensive part of the total cost of email.

If the predominant method of transferring files is through company email, we may correctly assume that the cost of file transfer is some percentage of the annual cost of owning and maintaining the email infrastructure. Recent research suggests that the average annual cost of a Microsoft Exchange mailbox is $512.00 per user. Based on this cost, an organization with 50 email users which allocates 20% of the total cost per user to handling email attachments would have a total annual cost of $5,120. Figure 4 summarizes the annual costs based on the percentage allocated to managing file attachments.

Figure 4: Cost of email attachments as a percentage of total annual email cost per user.



The costs shown in Figure 4 don't include the amount of time users waste dealing with issues related to sending file attachments, such as attachments that are over server limits or are undeliverable at the recipient's mail server. It's easy to see that even at a small percentage, handling file attachments through emails can be an expensive part of the total cost of email.

The Solution: Managed File Transfer

The preceding sections of this paper have enumerated the problems with transferring files and how existing technologies such as email attachments to transfer files place a burden on the IT infrastructure both in terms of resources and administrative cost. In addition, these solutions don't provide companies with the security and accountability that is essential at a time when companies are conducting more and more of their business on the Internet. What is needed is a solution that allows companies to continue to transfer files as part of their daily business process by using a technology that provides an easy to use, secure, affordable managed solution such as the one developed by YouSendIt.